Rappels sur TCP/IP

Damien Gros

CEA

3 octobre 2021

Plan du cours

Plan du cours

Définitions

- Revenir sur les principaux points qui font les réseaux
- Procooles étudiés :
  - Les protocoles : DNS, DHCP, SMTP (un peu), HTTP
- Principes de commutation (ethernet et réseau sans fil)

Plan du cours

Un peu d'histoire

- TCP/IP : protocole actuellement utilisé sur Internet ;
- Internet : Interconnexion de réseau, aussi appelé Réseau des réseaux ;
- En 1980 : quelques dizaines d'hôtes ;
- En 1995 : 4 850 000 machines/71 000 réseaux ;
- En 1996 : +12 millions de machines/500 000 réseaux ;
- Plusieurs millairds de device connectés

Utilité des réseaux

- Mettre en relation des machines entre elles ;
- Dialoguer, partager, déplacer....
- Qu'est-ce qu'on partage/déplace ?
  - Des données : mails, documents, etc.
  - Des ressources : `cloud`, calcul, capacités de stockage...
- Vouloir accéder à tout depuis n'importe (quelque soit le moyen)

Qu'est-ce qu'une topologie réseau ?

- Manière dont sont connectés les éléments qui composent notre réseau
- Disposition physique, logique
- Moyen d'interconnexion
- Choix du routage, de la technologie, etc.
- etc.

Définitions

Réseau local

Dans un réseau local, les équipements réseau communiquent en utilisant les **adresses MAC** (couche 2 du modèle OSI). Ces communications s'effectuent en **broadcast**

- Le **broadcast** ou diffusion :
  - Une machine émet un paquet sur le réseau ;
  - Dans ce paquet est contenu l'adresse du destinataire ;
  - Toutes les machines du réseau reçoivent le paquet ;
  - Seule la machine destinatrice traite le paquet.

Définitions

Réseau "Internet"

Lorsque l'on sort du réseau local, la communication s'effectue grâce aux couples IP et TCP/UDP. Ces communications s'effectuent de **point-à-point**.

- Le point à point :
  - Communication entre 2 machines ;
  - Cette communication doit passer entre des machines intermédiaires.

Commutation de paquets

Commutation de paquets

Découper les données en petite taille pour réduire dans le but de faciliter les échanges dans les milieux hétérogènes.

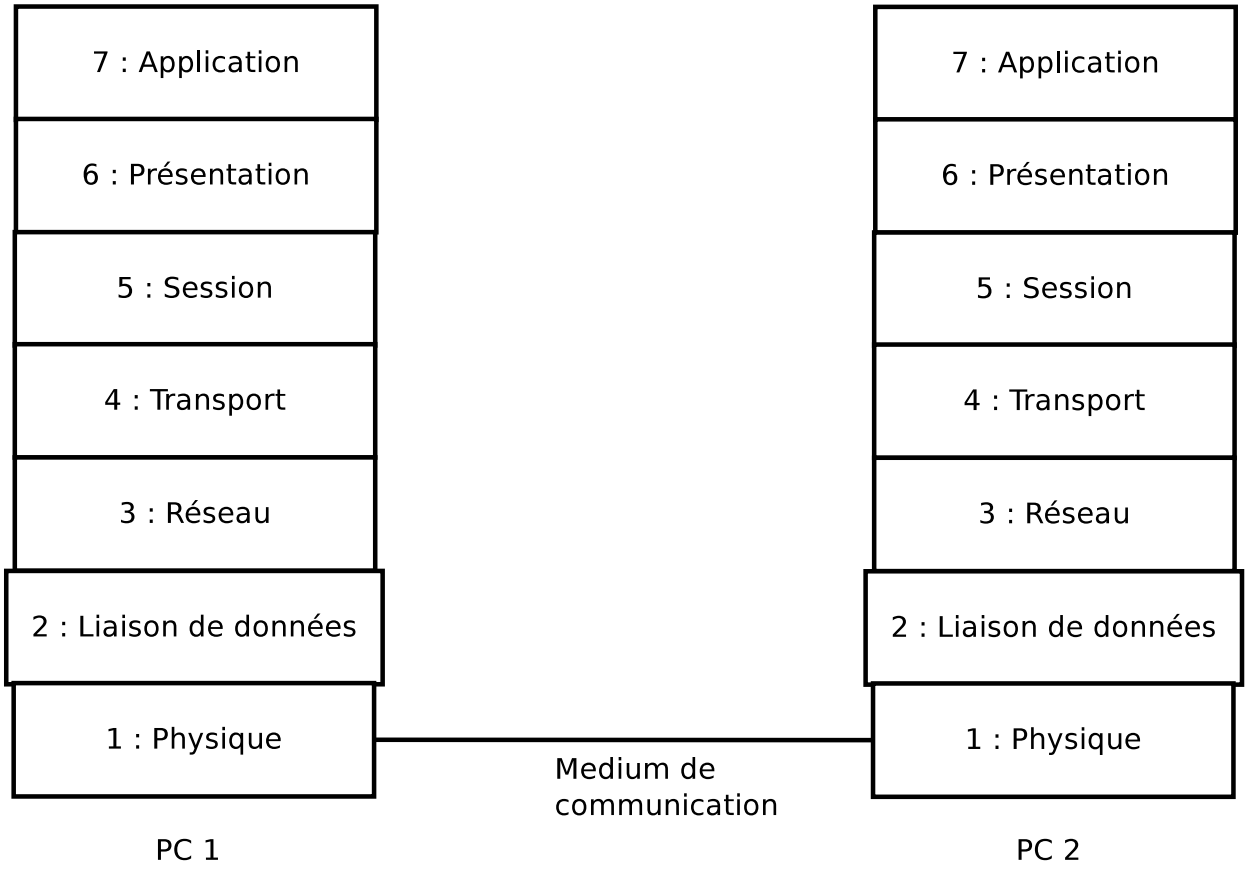
- Chaque bloc contient l'adresse du destinataire ;
- Les blocs sont réassemblés par le destinataire.

Plan du cours

Modèle OSI de l'ISO

- ISO : International Standards Organisation ;
- OSI : Open Systems Interconnection Reference Model ;
- Modèle ouvert servant souvent de référence ;
- Modèle constitué de 7 couches ;
- A chaque couche correspond une fonction précise ;
- **Une couche ne définit pas un protocole mais un service** $\rightarrow$
  Ainsi une couche peut contenir plusieurs protocoles tant que ceux-ci fournissent le service du modèle

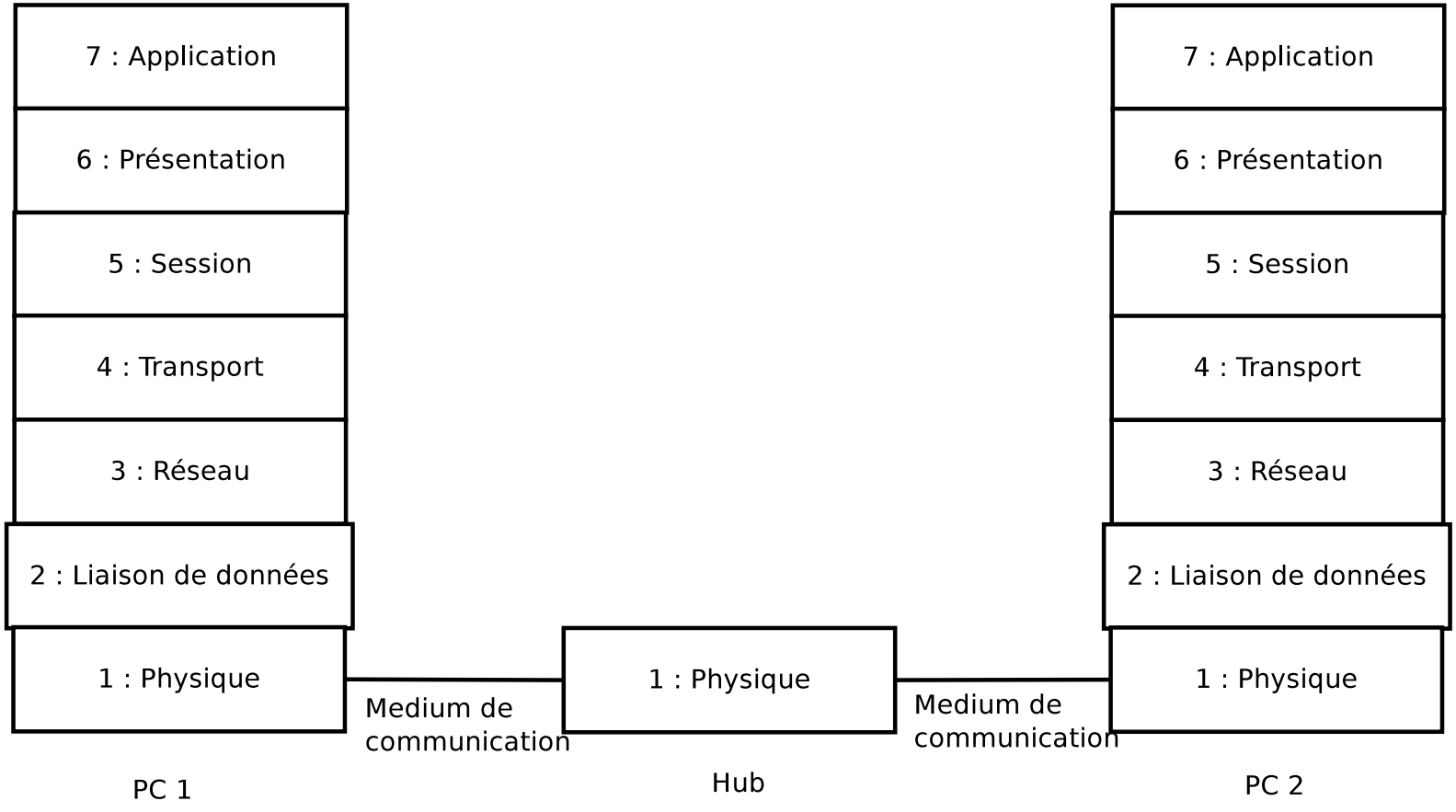
Les différentes couches du modèle OSI



La couche physique

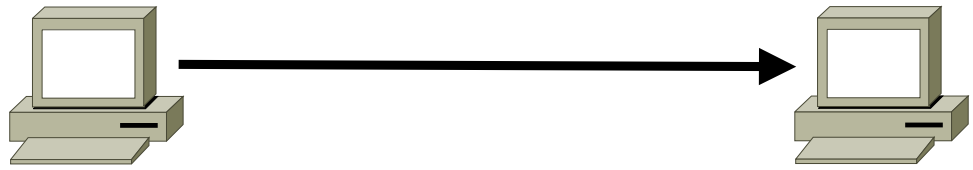
- Moyens électriques/mécaniques nécessaires à l'activation/maintien/désactivation de la connexion ;
- Conduire les éléments binaires ;
- Minimiser le coût de la communication ;
  - Les câbles : coaxiaux, ethernet, etc
  - La fibre
  - Les ondes

Ajout d'un HUB



Les méthodes d'accès

- SIMPLEX

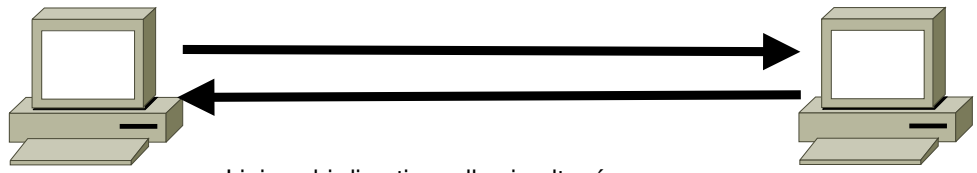


Une seule extrémité émet l'autre, l'autre reçoit
(liaison unidirectionnelle)

- HALF-DUPLEX

Liaison bi-directionnelle par alternat

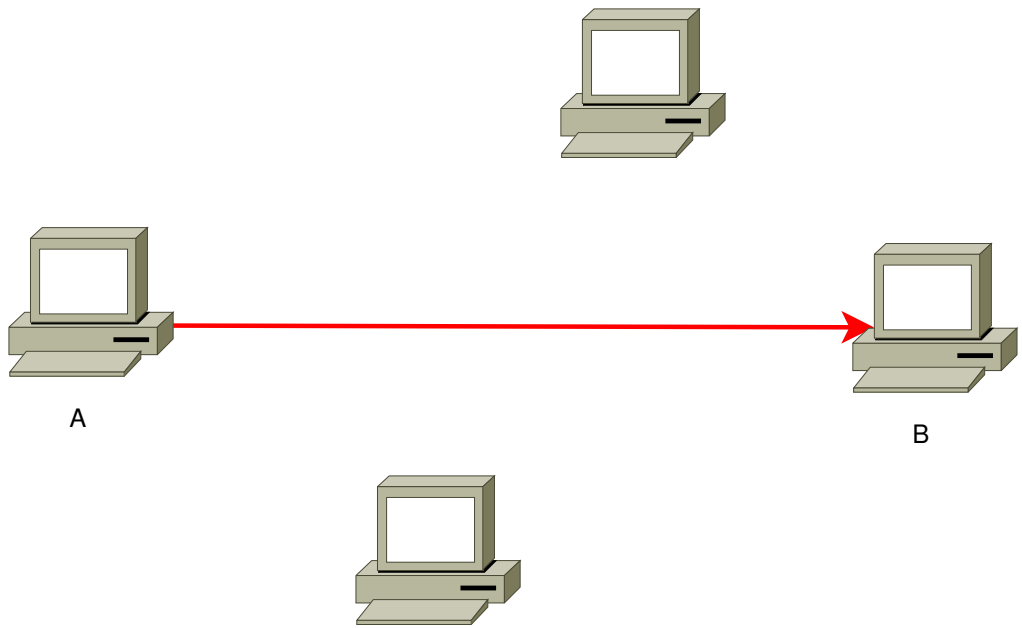
- FULL-DUPLEX



Liaison bi-directionnelle simultanée

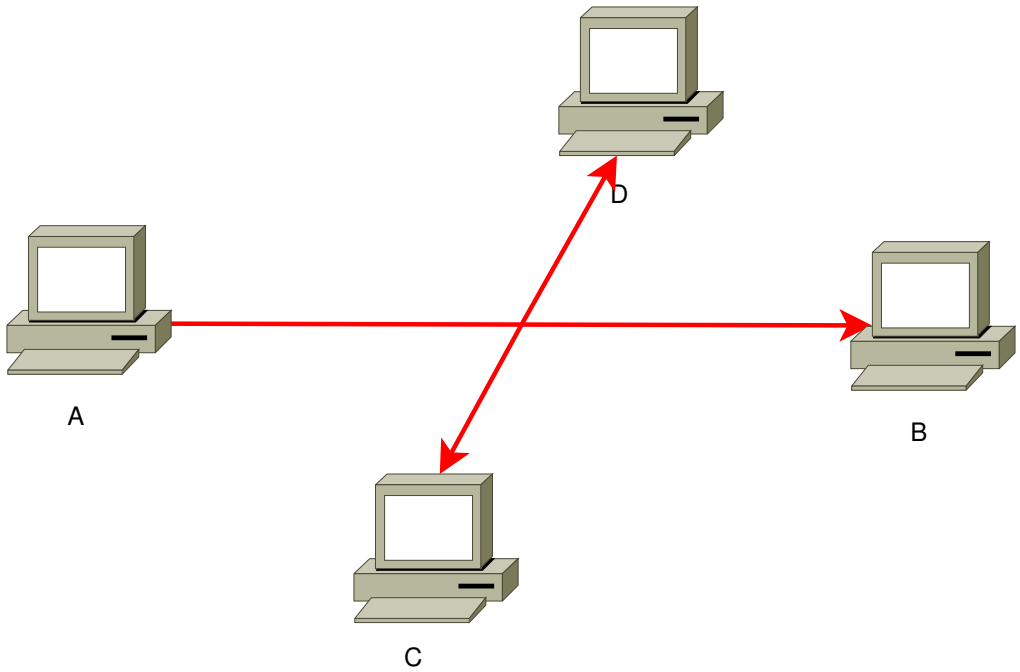
Les modes de diffusion

- UNICAST : A $\Rightarrow$ B



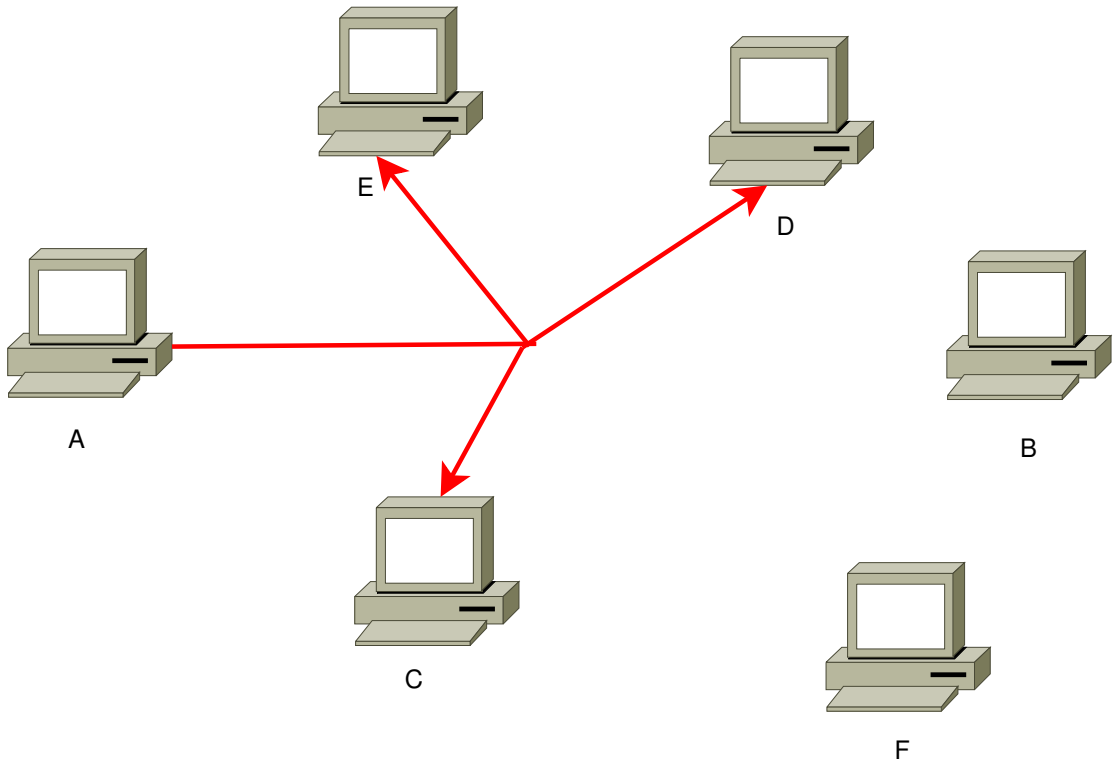
Les modes de diffusion

- BROADCAST : A $\Rightarrow$ All



Les modes de diffusion

- MULTICAST : A $\Rightarrow$ {Ensemble de destinataires}



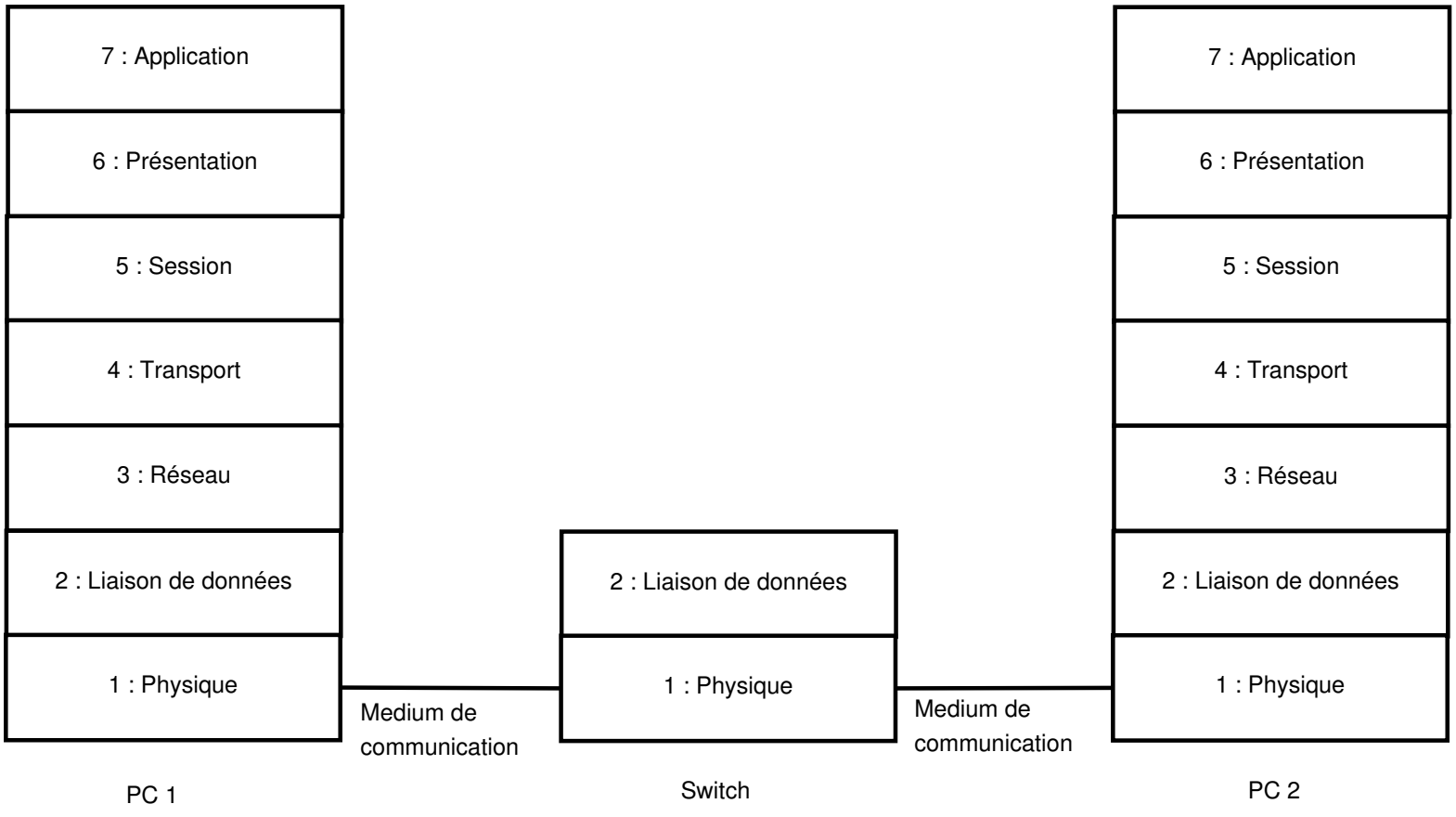
La couche de liaison de données

- Règle les conflits d'accès du canal de transmission
- Classiquement : **Ethernet**
- 802.2 : CSMA/CD (Carrier Sense, Multiple Access with Collision Detection)
  1. La station écoute le support physique de liaison pour déterminer si une autre station transmet (niveau tension électrique).
  2. Si pas de signal, elle émet.
  3. Si plusieurs stations émettent au même moment $\Rightarrow$ collision
  4. Les stations écoutent aussi les collisions, elles réémettent après un délai aléatoire.

La couche de liaison de données

- Réseaux sans fil : 802.11 CSMA/CA (Carrier Sense, Multiple Access with Collision Avoidance)
  1. La station voulant émettre écoute le réseau.
  2. Si le réseau est encombré, la transmission est différée.
  3. Dans le cas contraire, si le média est libre pendant un temps donné (DIFS pour Distributed Inter Frame Space), alors la station peut émettre.
  4. La station transmet un message appelé Ready To Send (RTS) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission.
  5. Le récepteur répond un Clear To Send (CTS), puis la station commence l'émission des données.
  6. A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK).
  7. Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

Ajout d'un SWITCH



Les modes de diffusion sur un réseau local

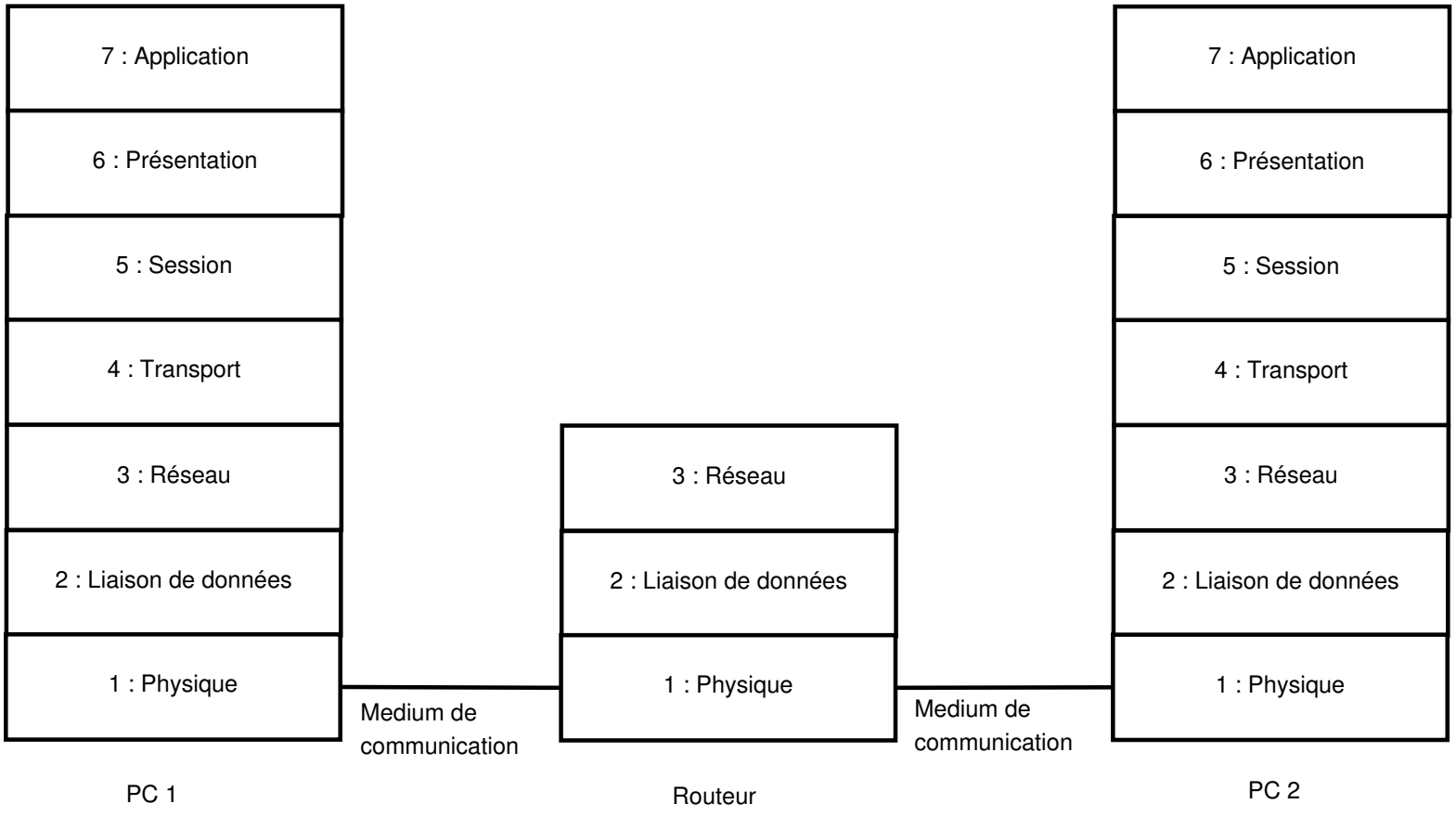
- UNICAST : Communication directe vers une seule machine, Adresse MAC paire
- BROADCAST : Communication avec toutes les stations : FF-FF-FF-FF-FF-FF
- MULTICAST : Communication vers un groupe de machines : Adresse Impaire sur le 1 er octet (01-00-5E-XX-XX-XX)

La couche réseau

- Résout les problèmes de routage ;
- Assure le traitement entre les couches basses et les couches hautes ;
- Détaillé plus tard dans le cours.

- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)

Ajout d'un ROUTEUR



Les boucles locales

La boucle locale

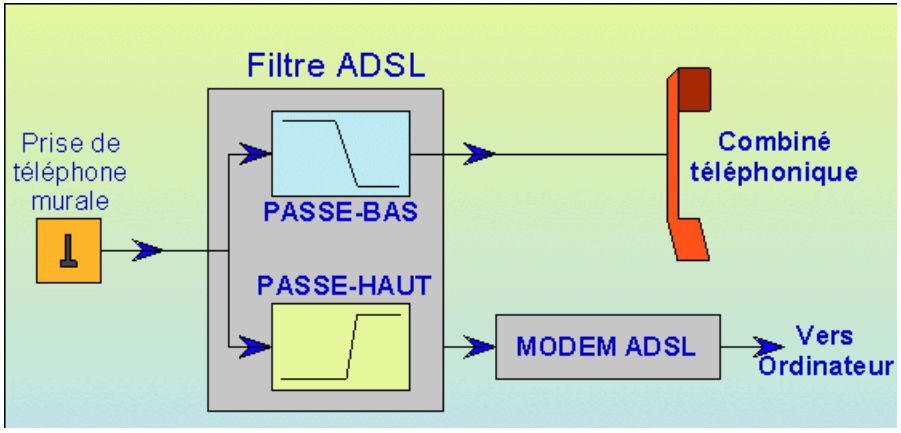
La boucle locale représente ce qui relie un utilisateur à l'équipement du réseau de son Fournisseur d'Accès à Internet (FAI). Peut être physique : paires torsadées, fibres, ou immatériel (Wifi, WIMAX, GSM, etc)

- Filaire : xDSL (Digital Subscriber Line)
- Fibre : FTTx
- Electromagnétique : WIMAX et GSM

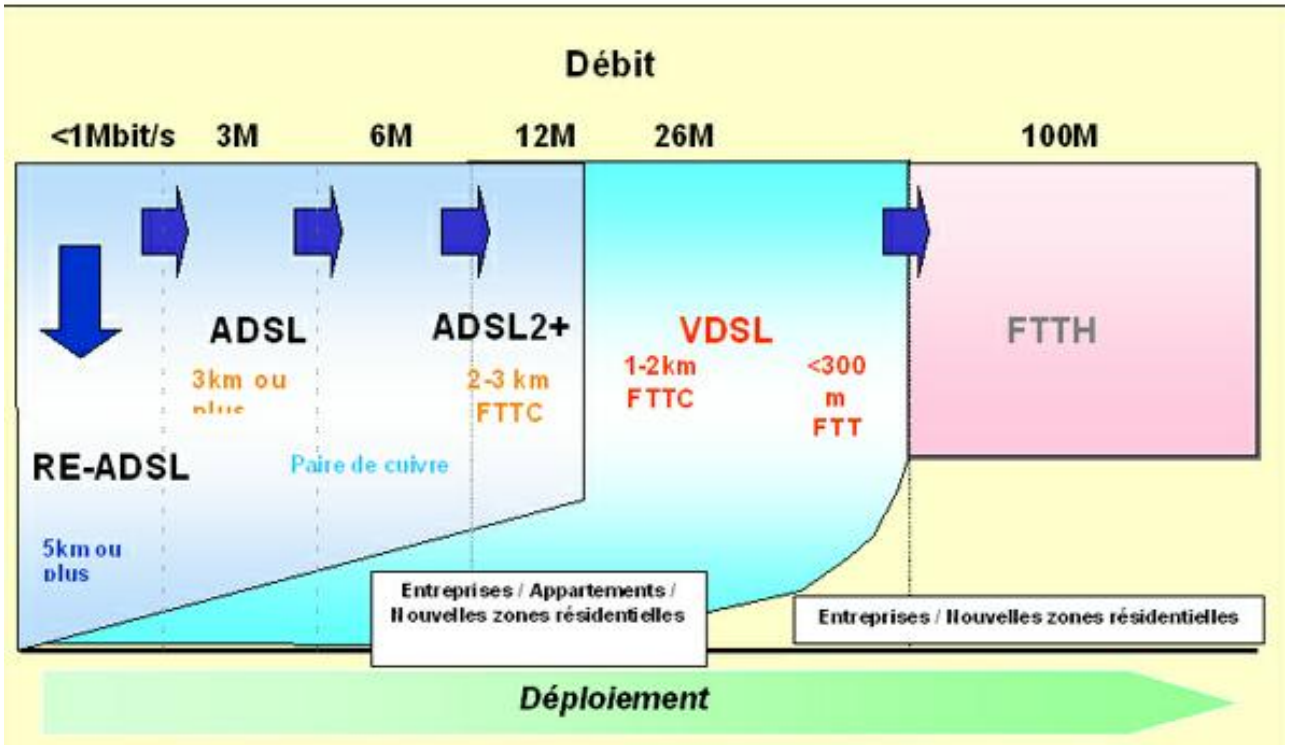
Les technologies DSL

Nom	Définition	Mode	Down (Mb/s)	Up (Kb/s)	Distance (Km)
HDSL	High datarate DSl	Symétrique	1.5-2	1.5-2	3.6
SDSL	Single Line SDL	Symétrique	0.7	0.7	3.6
ADSL	Asymetric DSL	Asymétrique	0.1-8	0.0016-07	5.4
ADSL2+	ADSL-V2	Asymétrique	0.1-24	0.016-1	5.4
RE-ADSL	Reach Extended ADSL	Asymétrique	0.5	0.1	8
VDSL	Very high datarate DSL	Asymétrique	15-30	1.5-2.3	1.3
VDSL2	VDSL-V2	Asmyétrique	jusqu'à 100	jusqu'à 40	0.8

ADSL

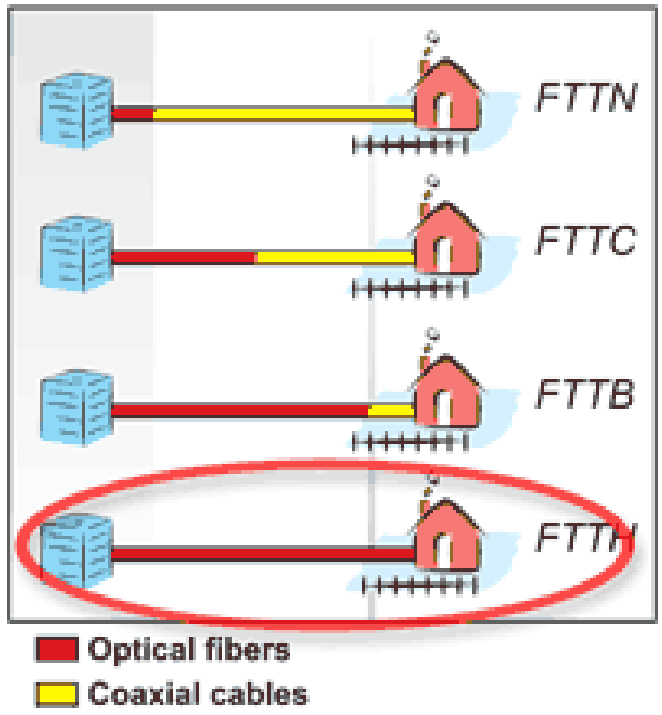

Filtre ADSL
Prise de téléphone murale
PASSE-BAS
PASSE-HAUT
Combiné téléphonique
MODEM ADSL
Vers Ordinateur

ADSL


Débit
<1Mbit/s
3M
6M
12M
26M
100M
ADSL
3km ou
ADSL2+
2-3 km
FTTC
VDSL
1-2km
FTTC
<300
m
FTT
FTTH
RE-ADSL
Paire de cuivre
5km ou
plus
Entreprises / Appartements /
Nouvelles zones résidentielles
Entreprises / Nouvelles zones résidentielles
Déploiement

FTTx

- FTTx : Fiber To The "fibre jusqu'à"
  - au quartier : FTT Neighborhood ou au trottoir FTT Curb
  - au pied de l'immeuble : FTT Building
  - au domicile : FTT Home



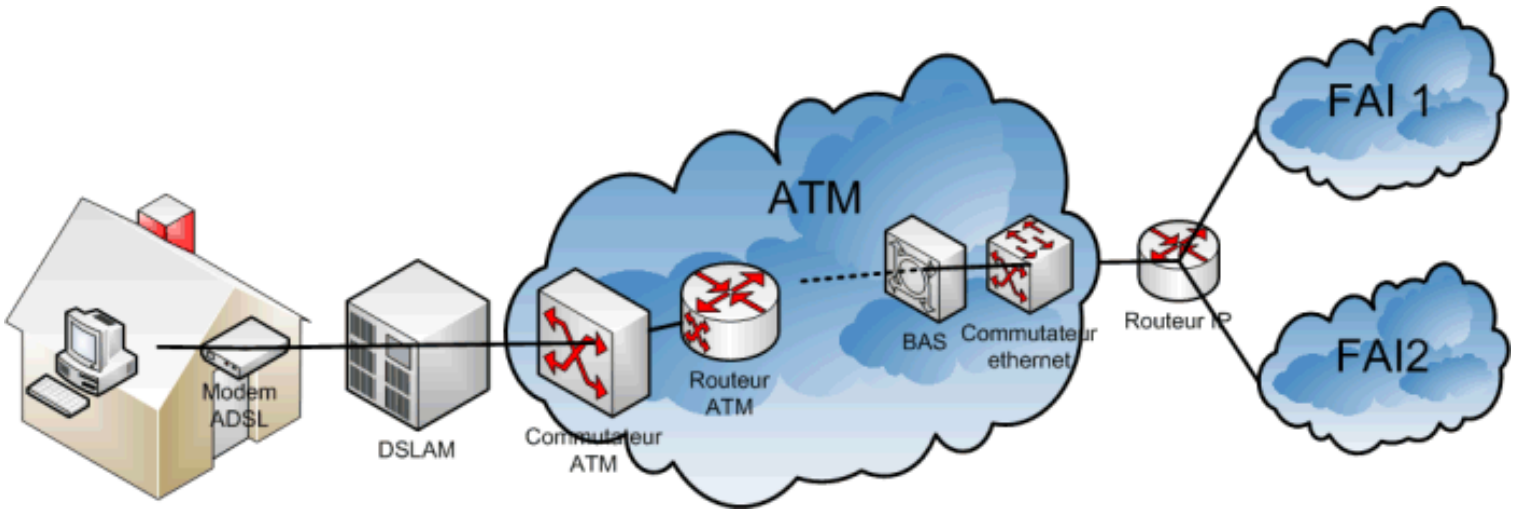
Architecture d'opérateur

- BOX Boîtier usager servant à transférer les données du réseau local de l'abonné (Ethernet/WIFI/CPL) ainsi que la bande de fréquence utilisée par la voie au répartiteur téléphonique. Il joue le rôle de MODEM DSL. Les BOX intègrent aujourd'hui un grand nombre d'autres fonctionnalités (serveur multimédia, VoIP, etc.).
- DSLAM : Digital Suscriber Line Access Module (800 à 2500 abonnés) Ce commutateur DSL se situe à la frontière entre la boucle locale et le réseau de collecte (backbone) de l'opérateur. Il permet aussi de concentrer les canaux de télévisions pour les distribuer vers l'abonné. Le choix des chaînes se faisant à son niveau. Il sépare les flux IP de la bande passante téléphonique. Cette dernière est redirigée vers le Réseau Téléphonique Commuté.

Architecture d'opérateur

- BAS : Broadband Access Server (serveur d'accès à la bande passante). 250 000 connexions simultanées. Il concentre le trafic venant des DSLAM. Il achemine le trafic Internet (routeur IP). Coté DSLAM, il alloue les @IP aux Box. Il sert aussi de serveur d'authentification, d'autorisation, de comptage et de taxation entre les abonnés et la base de données usagés situé dans les locaux du FAI.
- RBCI : Réseau Backbone de Collecte Internet, transport des flux internet
- FAI : Fournisseur d'accès à internet

Architecture d'opérateur



Un dernier point

- Les FAI paient une redevance (entre 6 et 9 euros) à l'opérateur historique pour pouvoir exploiter la ligne téléphonique reliant leurs DSLAM à l'abonné.

La couche transport

- Grâce à la couche **transport** nous avons une communication de bout en bout
- Assurer une certaine qualité sur la transmission :
  - contrôle de flux
  - séquencement
  - acquittement de messages
  - multiplexage d'applications
- TCP : Transmission Control Protocol
  - Protocole avec connexion
  - "On est sûr que l'information arrive au destinataire" (dans une certaine mesure)
- UDP : User Datagram Protocol
  - Protocole avec non connecté
  - "On **n'est pas** sûr que l'information arrive au destinataire"

La couche session

- Offre des services orientés utilisateur :
  - gestion des dialogues,
  - synchronisation des échanges,
  - allocation de ressources.

La couche présentation

- Les couches "basses" gèrent des bits $\rightarrow$ cette couche gère des objets (caractères, structures, etc) ;
- Permet l'adaptabilité en fonction des machines : Big-endian, Little-endian ;
- Permet de *présenter* les données.

Exemple : eXternal Data Representation (XDR) est un standard de la couche de présentation.
Utilisation de plus en plus importante de XML et JSON

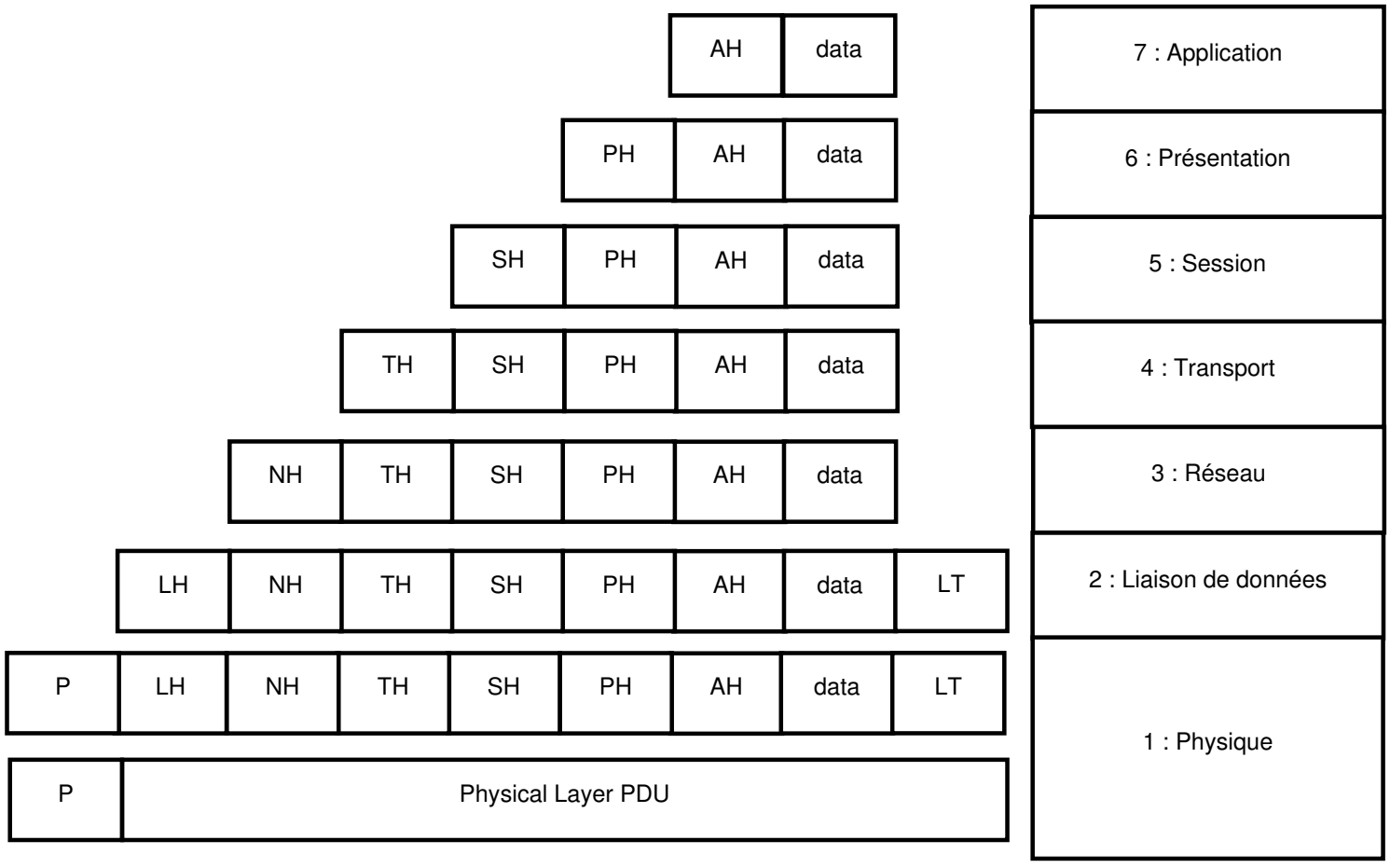
La couche application

- Constitué des programmes/services ;
- Messagerie, transfert de fichiers, navigateur web etc.

Le mécanisme d'encapsulation

- Chaque couche du modèle OSI ajoute des informations au message à destination de la même couche mais chez le récepteur ;
- Ces informations ne concernent que la couche du récepteur, en aucun cas les couches du dessus ou du dessous ne sont concernées par ces informations ;
- La couche transport va ajouter l'entête TCP ou UDP ;
- La couche réseau va ajouter l'entête IP ;

Schéma d'encapsulation



L'encapsulation

Émetteur :

- Une couche ne communique qu'avec la couche qui la précède et qui la suit (exception faite pour les couches 1 et 7) ;
- Lors de l'émission d'un message depuis la couche 7, chaque couche ajoute "son élément" propre ;
- Cet élément sera "lu" par la couche correspondante du destinataire ;
- $\Rightarrow$ Encapsulation !

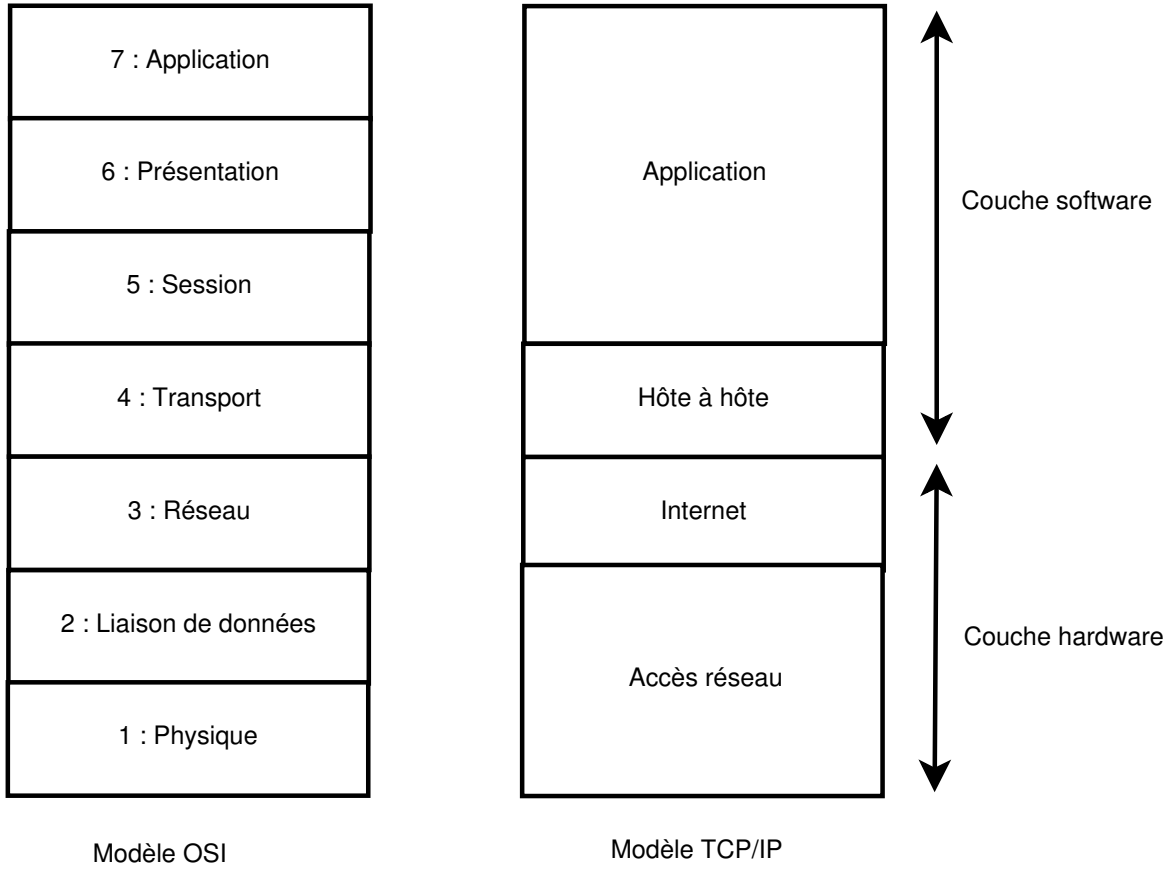
Destinataire :

- Le message arrive par la couche 1 pour aller à la couche 7 ;
- Chaque couche que le message traverse "récupère" l'information qui lui est propre ;
- $\Rightarrow$ Désencapsulation !

Modèle TCP/IP

- Modèle DOD (Department Of Defense)
- 4 couches :
  - Couche application
  - Couche transport
  - Couche internet
  - Couche accès réseau

Comparaison entre le modèle OSI et TCP/IP



Plan du cours

Les réseaux locaux

- A ce niveau, on parle de **trame ethernet** ;
- Les machines émettent des trames en **broadcast** ;
- Chaque trame est donc reçue par l'ensemble des équipements situés sur le même lien ;
- Ces trames ont une taille limite MTU : *Maximum Transmission Unit* ;
- Les équipements réseau sont identifiés par leur interface (carte éthernet, carte wifi, etc) ;
- Chaque interface du réseau possède une adresse MAC *Medium Access Control*
- *presque* unique de 6 octets (écrits en hexadécimal)
- Les 3 premiers octets identifient le constructeur de la carte.

Affichage et manipulation de l'adresse MAC

Afficher son adresse MAC :

```
damien@ossus:% ifconfig enp0s25 | grep eth
        ether 00:0f:fe:dc:b5:15  txqueuelen 1000  (Ethernet)

damien@ossus:% ip link show dev enp0s25
2: enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
     state UP mode DEFAULT qlen 1000
    link/ether 00:0f:fe:dc:b5:15 brd ff:ff:ff:ff:ff:ff
```

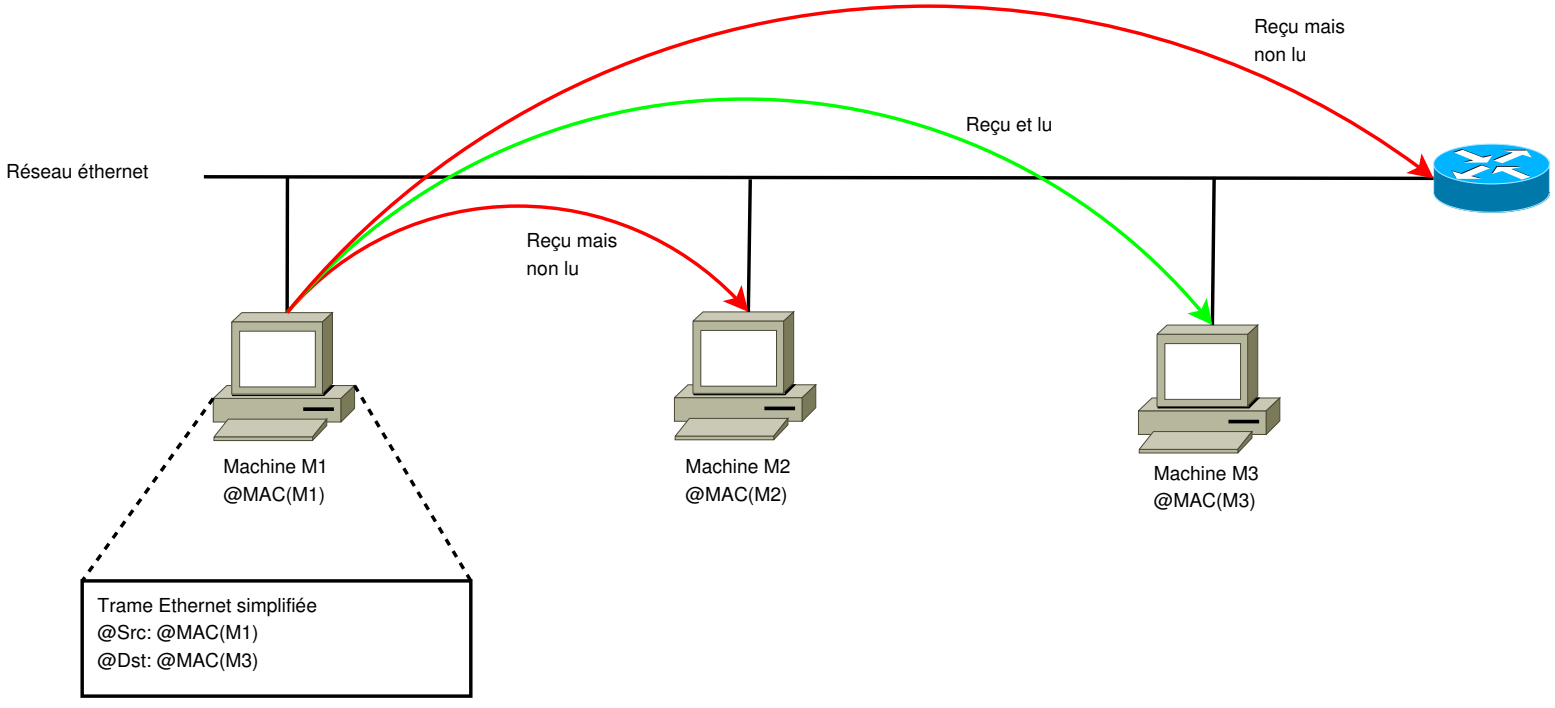
Changer son adresse MAC :

```
sudo ifconfig enp0s25 ether 00:01:02:03:04:05
```

Communication sur les réseaux locaux

- On utilise les adresses MAC pour communiquer sur les réseaux locaux
- Principe d'une communication :
  - Broadcast de la trame avec pour destinataire l'adresse MAC de la machine cible ;
  - Tous les équipements réseau réceptionnent la trame, seule la machine cible lit cette trame ;
  - La machine cible répond (et on recommence le processus).

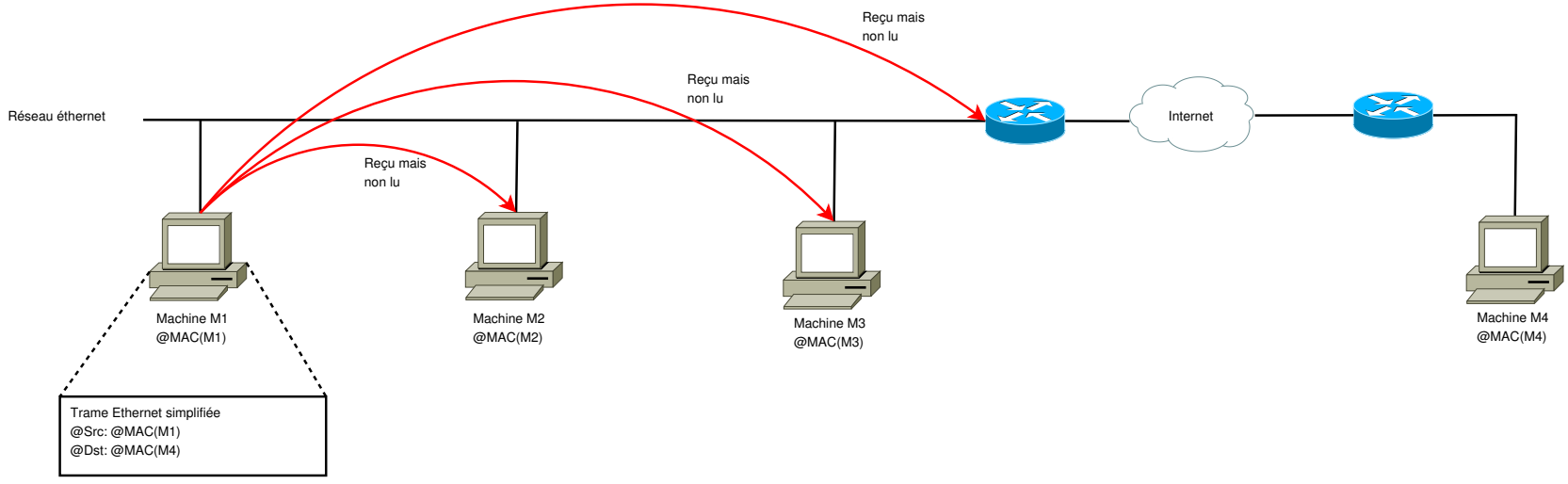
Communication sur les réseaux locaux



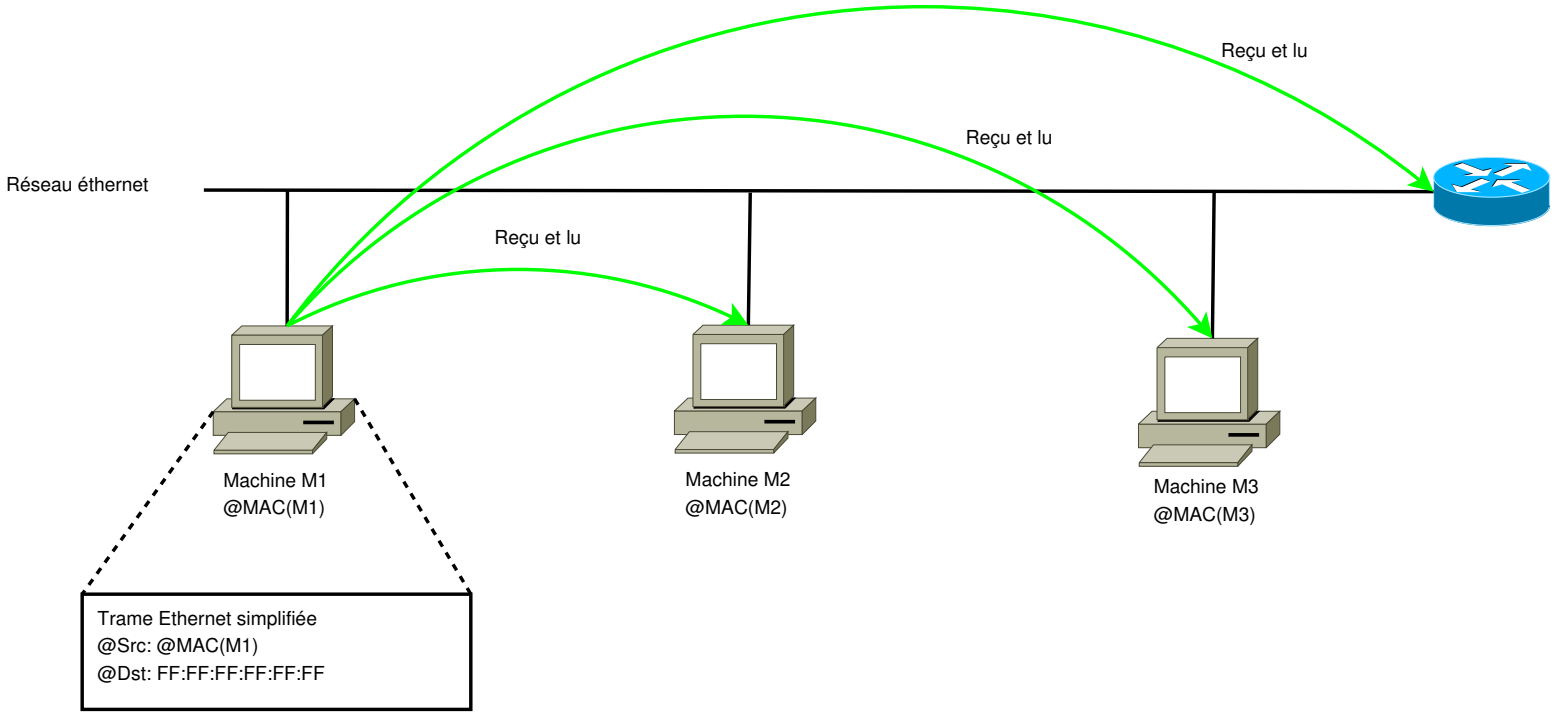
Communication sur les réseaux locaux

- Que se passe-t'il si on met une adresse MAC d'une machine qui n'est pas sur le même réseau que nous ?
- La trame n'arrive pas et elle est perdue.

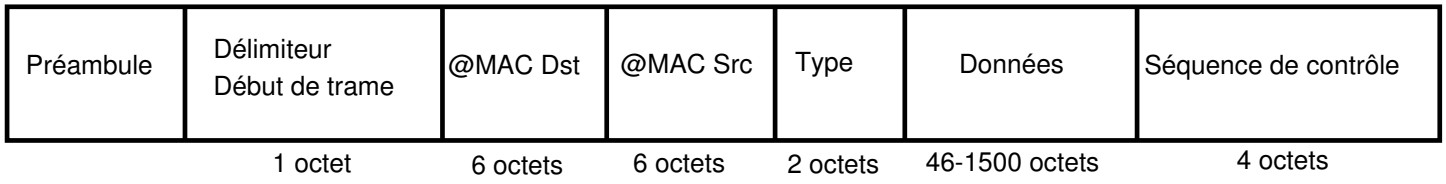
Communication sur les réseaux locaux



Communication sur les réseaux locaux



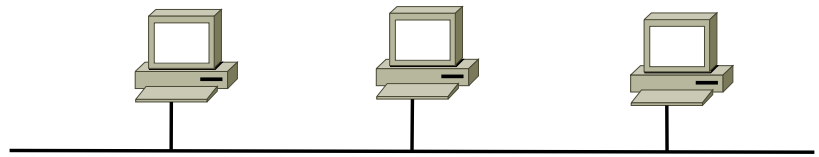
Trame Ethernet

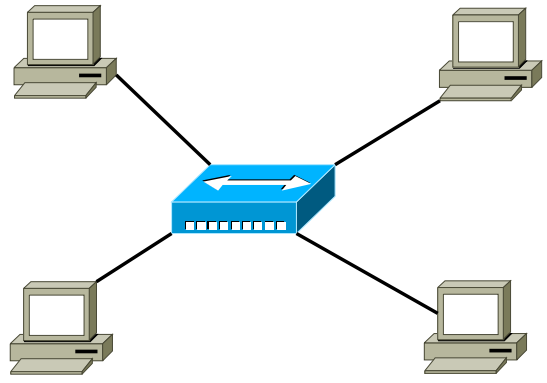


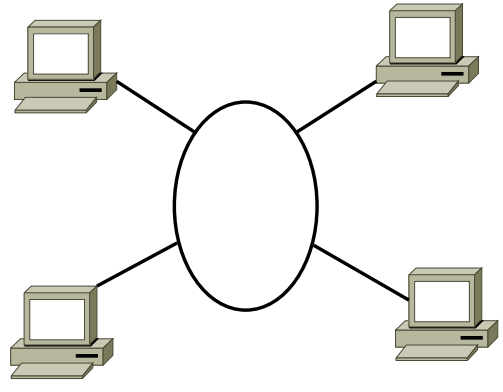
Les types d'architecture

- Réseau en bus ;
- Réseau en étoile ;
- Réseau en anneau.

Topologie des réseaux







De Ethernet à IP

- Problèmes à résoudre :
  - Communiquer avec tout le monde, n'importe où, n'importe comment ;
  - Accessible par tout le monde ;
  - Une machine doit pouvoir être identifiée par :
    - Un nom (pour les humains) ;
    - Une adresse "unique" ;
    - Une route pour y accéder.

$\Rightarrow$ Adresse binaire et utilisation de noms

De Ethernet à IP

- Une personne normalement constituée retient des noms et des un certain nombre de chiffres/nombres ;
- La problématique des noms est résolu grâce au DNS ;
- L'utilisation de nombre $\Rightarrow$ Utilisation des adresses IP ;
- On se concentre sur les adresses IPv4 dans ce cours ;
- On verra les adresses IPv6 au cours de cette année.

MAC vs IP

- Une adresse MAC identifie une interface sur un réseau local
  - Plus ou moins unique ;
  - C'est une adresse **physique** (ie : reliée à une interface physique)
- Une adresse IP identifie une machine sur un réseau (quelque soit le réseau)
  - Aucune dépendance vis-à-vis du matériel ;
  - C'est une adresse **logique** (positionne une machine dans un réseau)
- On n'agit pas sur les mêmes couches des modèles OSI/(TCP/IP).

Qu'est-ce qu'une Adresse IPv4 ?

- Une suite de 4 "mots" écrits en décimal ;
- Adresse IPv4 : 32 bits : 4 octets ;
- Adresse IPv4 : 4 octets entre 0 et 255.
- Une paire (netid,hostid) ;
- Netid : identifie le réseau ;
- Hostid : identifie la machine sur ce réseau.

Adresses IPv4 remarquables

- 127.X.X.X (127.0.0.1) : localhost/boucle locale ;
- Privé : 10.0.0.0/8 192.168.0.0/16 : non routés
- Adresse de broadcast : dernière adresse du réseau.
- On reviendra dans le cours 5 sur les notions de masque et de routage statique.

Le besoin :

- La communication entre machines ne peut s'effectuer qu'à travers l'interface physique ;
- Les applicatifs ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique ?
- Les machines sur un réseau local ne communiquent que par Ethernet.

Address Resolution Protocol

La solution : ARP

- Mise en place dans TCP/IP d'un protocole de bas niveau appelé Adress Resolution Protocol (ARP) ;
- Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IPv4 de la machine destinatrice.

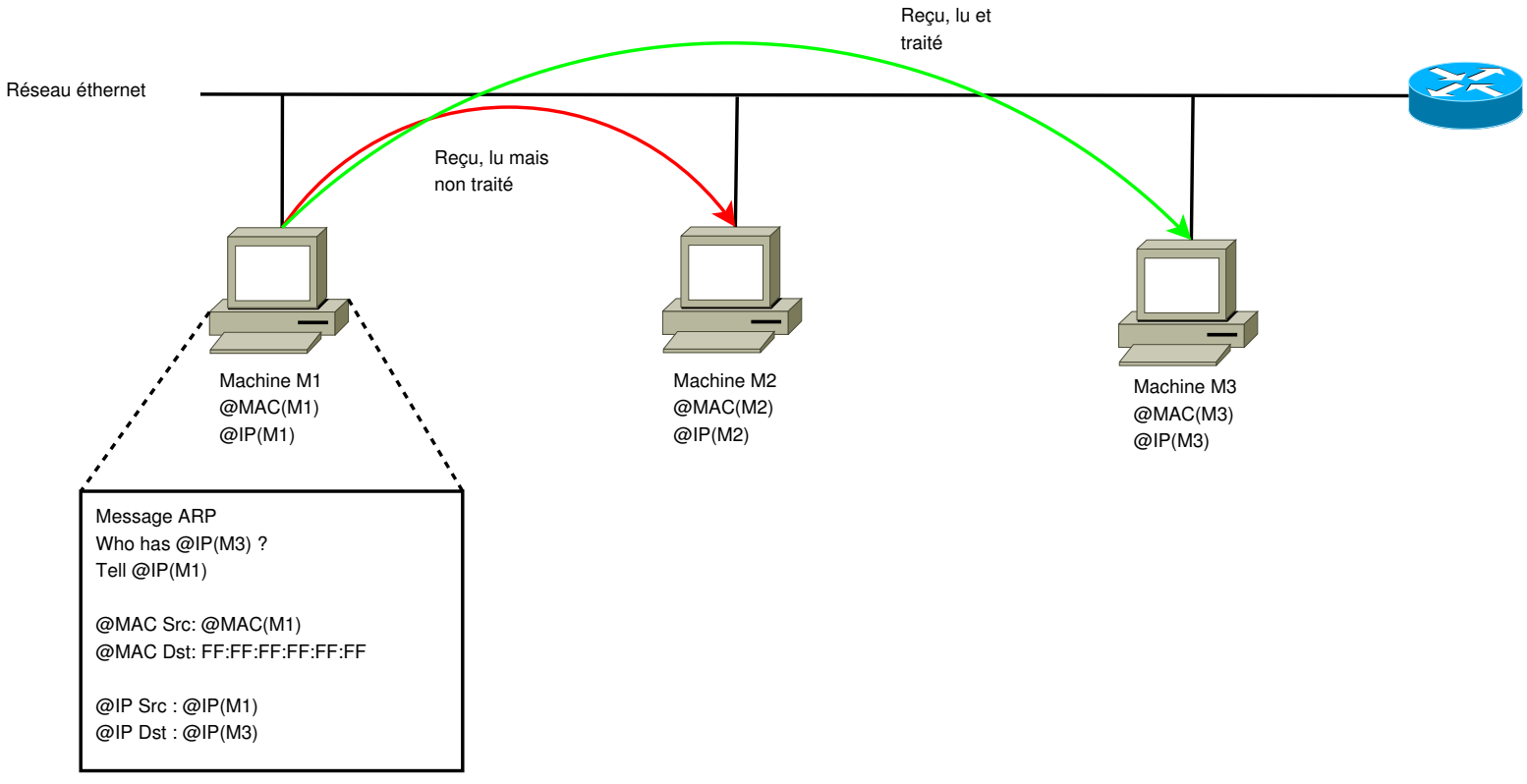
La technique :

- Diffusion d'adresse sur le réseau physique ;
- La machine d'adresse IPv4 émet un message contenant son adresse physique ;
- Les machines non concernées ne répondent pas ;
- Gestion cache pour ne pas effectuer de requête ARP à chaque émission.

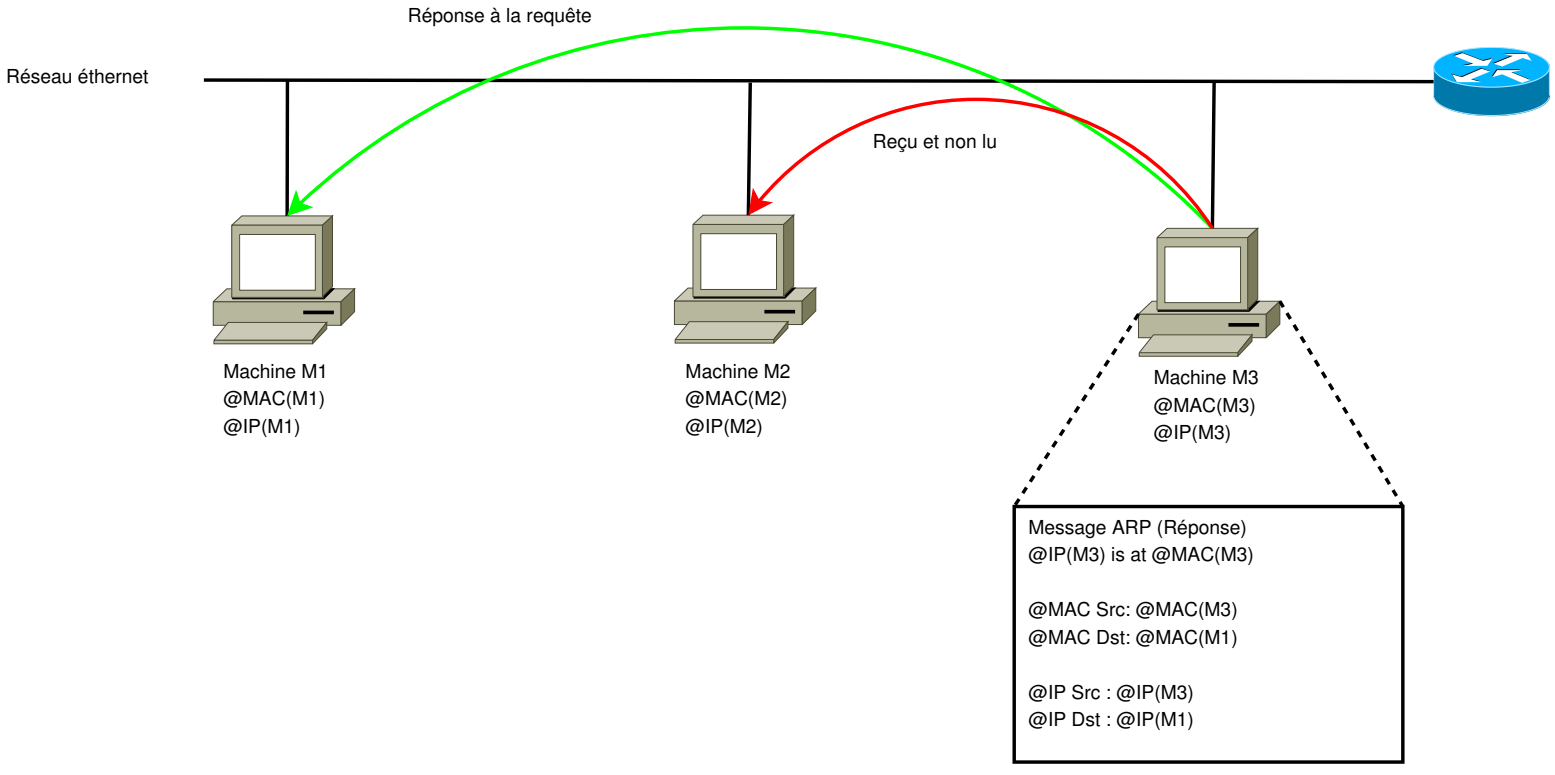
Address Resolution Protocol

- Exemple : A cherche à contacter C.
- Message de A (par diffusion) : Question : étant donné IPv4 (C), que vaut Eth (C) ?
- Message de C à A : Réponse : voici mon adresse Ethernet.

Requête ARP


Reçu, lu et
traité
Réseau éthernet
Reçu, lu mais
non traité
Machine M1
@MAC(M1)
@IP(M1)
Machine M2
@MAC(M2)
@IP(M2)
Machine M3
@MAC(M3)
@IP(M3)
Message ARP
Who has @IP(M3) ?
Tell @IP(M1)
@MAC Src: @MAC(M1)
@MAC Dst: FF:FF:FF:FF:FF:FF
@IP Src : @IP(M1)
@IP Dst : @IP(M3)

Réponse ARP


Réponse à la requête
Réseau éthernet
Reçu et non lu
Machine M1
@MAC(M1)
@IP(M1)
Machine M2
@MAC(M2)
@IP(M2)
Machine M3
@MAC(M3)
@IP(M3)
Message ARP (Réponse)
@IP(M3) is at @MAC(M3)
@MAC Src: @MAC(M3)
@MAC Dst: @MAC(M1)
@IP Src : @IP(M3)
@IP Dst : @IP(M1)

Address Resolution Protocol

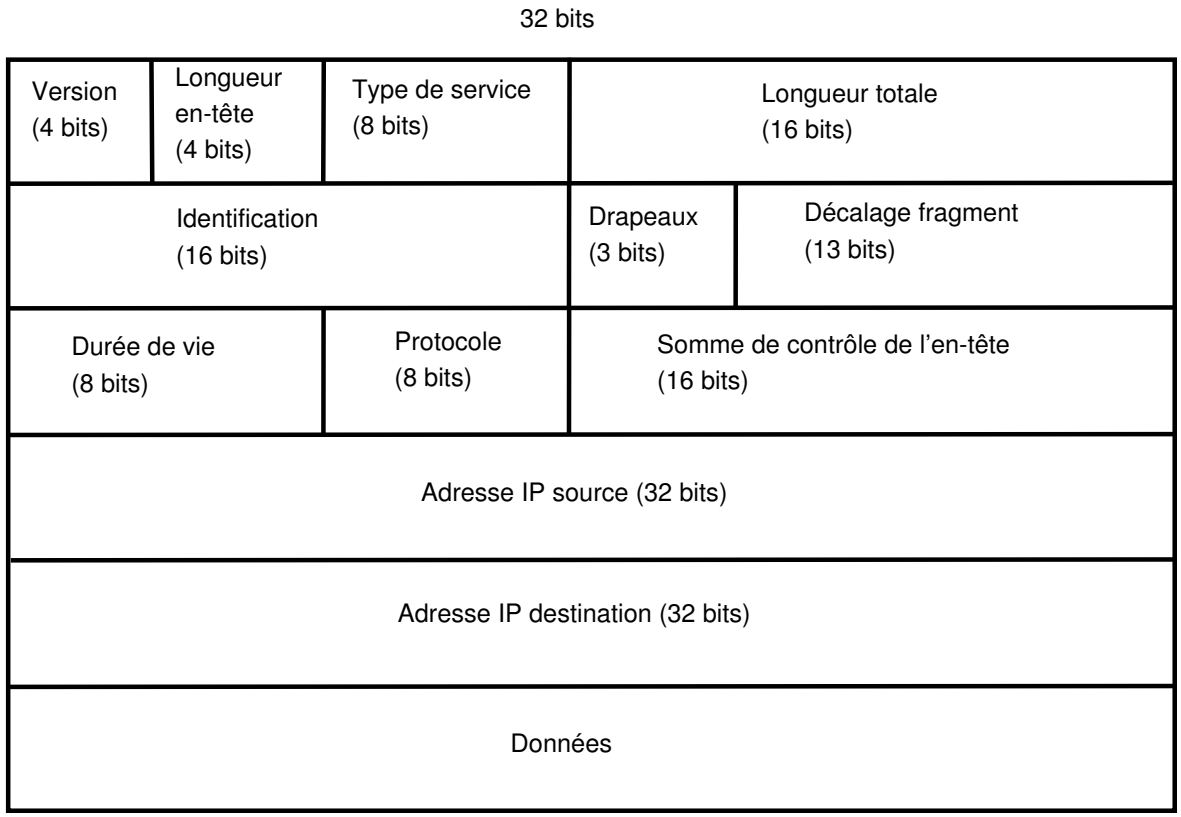
- Naïvement : pour chaque paquet IPv4 on ferait un échange ARP (en diffusion) ;
- Problème : trafic énorme !
- Solution : chaque machine conserve les dernières transactions dans un cache (table ARP).

```
damien@debian :~% arp -a
Freebox-Server.local (192.168.3.254) at f4:ca:e5:5f:84:db [ether] on eth0
? (192.168.3.87) at 00:0f:fe:dc:b4:cd [ether] on eth0
? (192.168.3.44) at 00:18:f8:bc:95:48 [ether] on eth0
? (192.168.3.12) at 00:12:79:6b:2f:81 [ether] on eth0
? (192.168.3.13) at 00:12:79:6b:2f:a5 [ether] on eth0
```

Internet Protocol

- Le protocole IP définit :
  - l'unité de donnée transférée dans les interconnexions (datagramme),
  - la fonction de routage,
  - les règles qui mettent en œuvre la remise de paquets en mode non connecté
- Un datagramme IP peut être découpé en plusieurs morceaux = fragment

Datagramme IP



Datagramme IP

- Version : numéro de version du protocole utilisé (4 ou 6)
- Longueur de l'en-tête uniquement
- Type de service : défini le type d'acheminement (le protocole encaspulé : ICMP, TCP, UDP, etc).
- Longueur totale : taille du fragment et non pas celle du datagramme initial,
  - On peut déterminer la taille du datagramme initial grâce au dernier fragment.
- IDENTIFICATION : entier qui identifie le datagramme initial (utilisé pour la reconstitution à partir des fragments qui ont tous la même valeur).

Datagramme IP

- FRAGMENT OFFSET, FLAGS, IDENTIFICATION : les champs de la fragmentation.
  - Le MTU (*Maximum Transmission Unit*) définit la taille maximale d'un datagramme véhiculé sur le réseau physique.
  - Lorsque le réseau physique vers lequel est routé le paquet possède un MTU plus petit que le MTU courant, la passerelle fragmente le datagramme IP.
  - Si un seul des fragments est perdu, le datagramme initial est considéré comme perdu : la probabilité de perte d'un datagramme augmente avec la fragmentation.
- FRAGMENT OFFSET : indique le début du fragment courant (par rapport au datagramme entier).

Datagramme IP

- Drapeaux : contient des informations sur la fragmentation
  - Réservé : 0
  - DF (Don't Fragment) : lorsque le drapeau est à 1, le datagramme ne peut être fragmenté
  - MF (More Fragment) : tant que ce drapeau est à 1, cela signifie qu'il existe des fragments qui arrivent.
- Durée de vie
  - Ce champ indique en secondes, la durée maximale de transit du datagramme sur le réseau. La machine qui émet le datagramme définit sa durée de vie.
  - Les passerelles qui traitent le datagramme doivent décrémenter sa durée de vie du nombre de secondes (1 au minimum) que le datagramme a passé pendant son séjour dans la passerelle ; lorsque celle-ci expire le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.

Datagramme IP

- Protocole : ce champ identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du datagramme :
  - 6 : TCP,
  - 17 : UDP,
  - 1 : ICMP.
- Somme de contrôle de l'en-tête
  - Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme. Le total de contrôle d'IP porte sur l'en-tête du datagramme et non sur les données véhiculées. Lors du calcul, le champ HEADER CHECKSUM est supposé contenir la valeur 0.

La fragmentation IP

- Considérons un datagramme IP de 5000 octets(ou bytes) avec un MTU de 1500.

1. Le premier fragment est créé en prenant les 1480 premiers bytes de données du datagramme initial.
2. On lui ajoute les 20 bytes de l'entête IP : IP source, destination.
3. La taille totale est mise à 1500 bytes.
4. Le champ identification est copié du datagramme original,
5. MF est mis à 1
6. DF est mis à 0
7. Offset (décalage) à 0.

La fragmentation IP

1. Le second fragment est crée avec les 1480 prochains bytes de données (de 1480 -> 2960).
2. On lui ajoute les 20 bytes de l'entête IP : IP source, destination.
3. Le champ identification est copié du datagramme original,
4. MF est mis à 1
5. DF est mis à 0
6. Offset (décalage) à 185 = 1*(1500-20)/8 (signifiant que ce fragment commence à la position 1480 du datagramme initial).

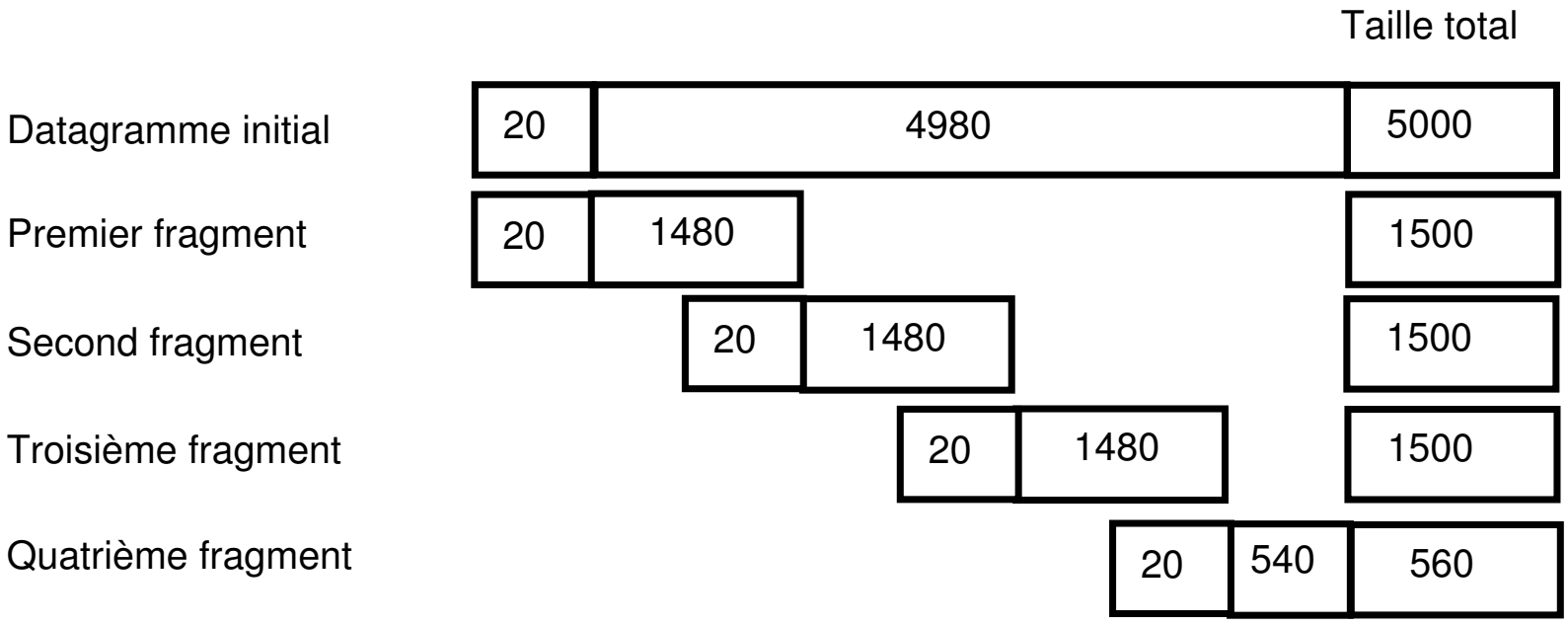
La fragmentation IP

1. Le troisième fragment est crée avec les 1480 prochains bytes de données (de 2960 -> 4440).
2. On lui ajoute les 20 bytes de l'entête IP : IP source, destination.
3. Le champ identification est copié du datagramme original,
4. MF est mis à 1
5. DF est mis à 0
6. Offset (décalage) à 370 = 2*(1500-20)/8 (signifiant que ce fragment commence à la position 2960 du datagramme initial).

La fragmentation IP

1. Le quatrième fragment est crée avec les 1480 prochains bytes de données (de 4440 -> 5920).
2. On lui ajoute les 20 bytes de l'entête IP : IP source, destination.
3. Le champ identification est copié du datagramme original,
4. MF est mis à 0 (On a dépassé le taille du datagramme initial donc tout est envoyé)
5. DF est mis à 0
6. Offset (décalage) à 555 = 3*(1500-20)/8 (signifiant que ce fragment commence à la position 4440 du datagramme initial).

Fragmentation IP



ICMP

Internet Control Message Protocol : RFC 950

- IP ne vérifie pas les erreurs ;
- ICMP est un mécanisme de contrôle des erreurs au niveau IP ;
- La couche application peut aussi avoir un accès direct à ce protocole ;
- Numéro de protocole : 1.
- Les messages ICMP sont encapsulés dans les datagrammes IP
- Ce n'est pas un protocole de couche supérieur !

ICMP

Chaque message ICMP caractérise un problème qu'il signale :

- TYPE : contient le code d'erreur ;
- CODE : complète l'information du champ TYPE ;
- CHECKSUM : ne porte que sur le champ ICMP.

ICMP

- Echo Request (T : 8), Echo reply (T : 0) : ping !
- Destination Unreachable (T : 3) :
  - 0 " Network unreachable "
  - 1 " Host unreachable "
  - 2 " Protocol unreachable "
  - 3 " Port unreachable "
  - 4 " Fragmentation needed and DF set "
  - 5 " Source route failed "

UDP

- User Datagram Protocol : RFC 768 "paquet UDP"
- Rappel : Au niveau de la couche Internet les datagrammes sont routés d'une machine à une autre en fonction des bits de l'adresse IP qui identifient le numéro de réseau.
- Lors de cette opération aucune distinction n'est faite entre les services ou les utilisateurs qui émettent ou reçoivent des datagrammes.
- La couche UDP ajoute un mécanisme qui permet l'identification du service (niveau Application). En effet, il est indispensable de faire un tri entre les divers applications (services) : plusieurs programmes de plusieurs utilisateurs peuvent utiliser simultanément la même couche de transport et il ne doit pas y avoir de confusion entre eux.

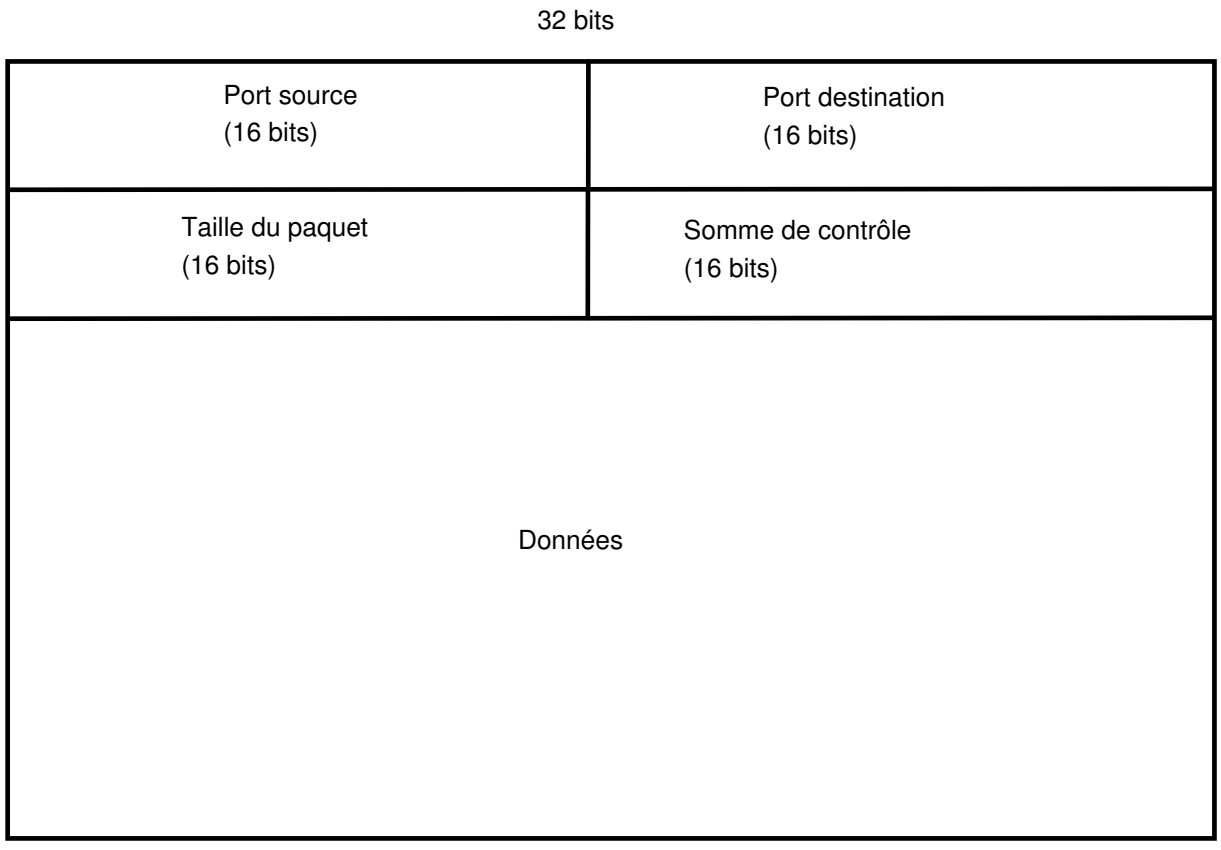
UDP

- Associer la destination à la fonction qu'elle remplie ;
- Utiliser un entier positif appelé **port**
  - Le système d'exploitation local a à sa charge de définir le mécanisme qui permet à un processus d'accéder à un port.
  - La plupart des systèmes d'exploitation fournissent le moyen d'un accès synchrone à un port.
  - Ce mécanisme doit alors assurer la possibilité de gérer la file d'attente des paquets qui arrivent, jusqu'à ce qu'un processus (Application) les lise.
  - A l'inverse, le système d'exploitation bloque un processus qui tente de lire une donnée non encore disponible (ou qui ne lui est pas destiné).

UDP

- Protocole en **Mode déconnecté**
- Ports 1 à 1024 : accessible uniquement aux programmes Root/Administrateur
- 49152, 65535 : ports dynamiques (ouverts par les applications)
- Les ports sont référencés dans /etc/services
  C :\Windows\System32\drivers\etc\services

Datagramme UDP

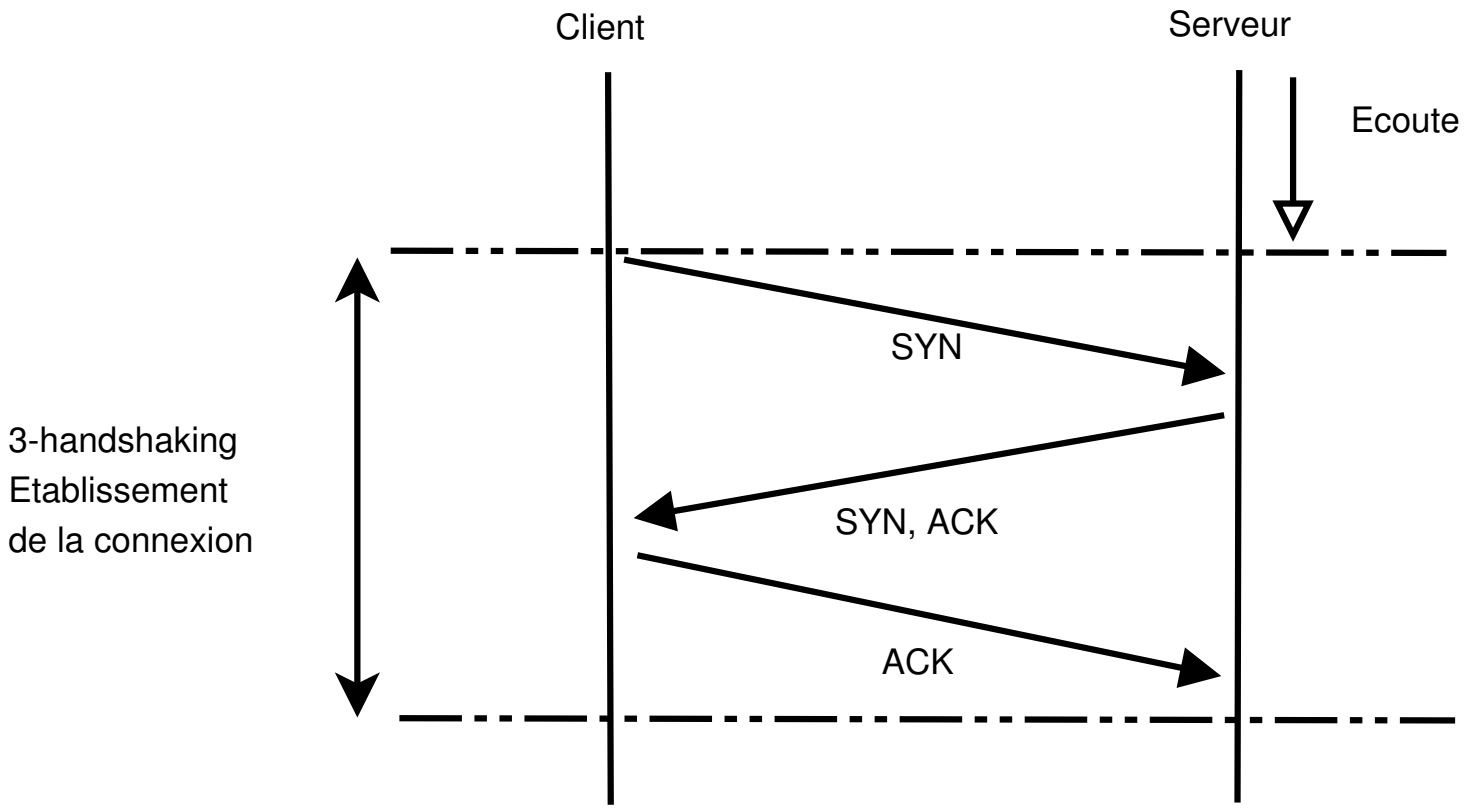


TCP

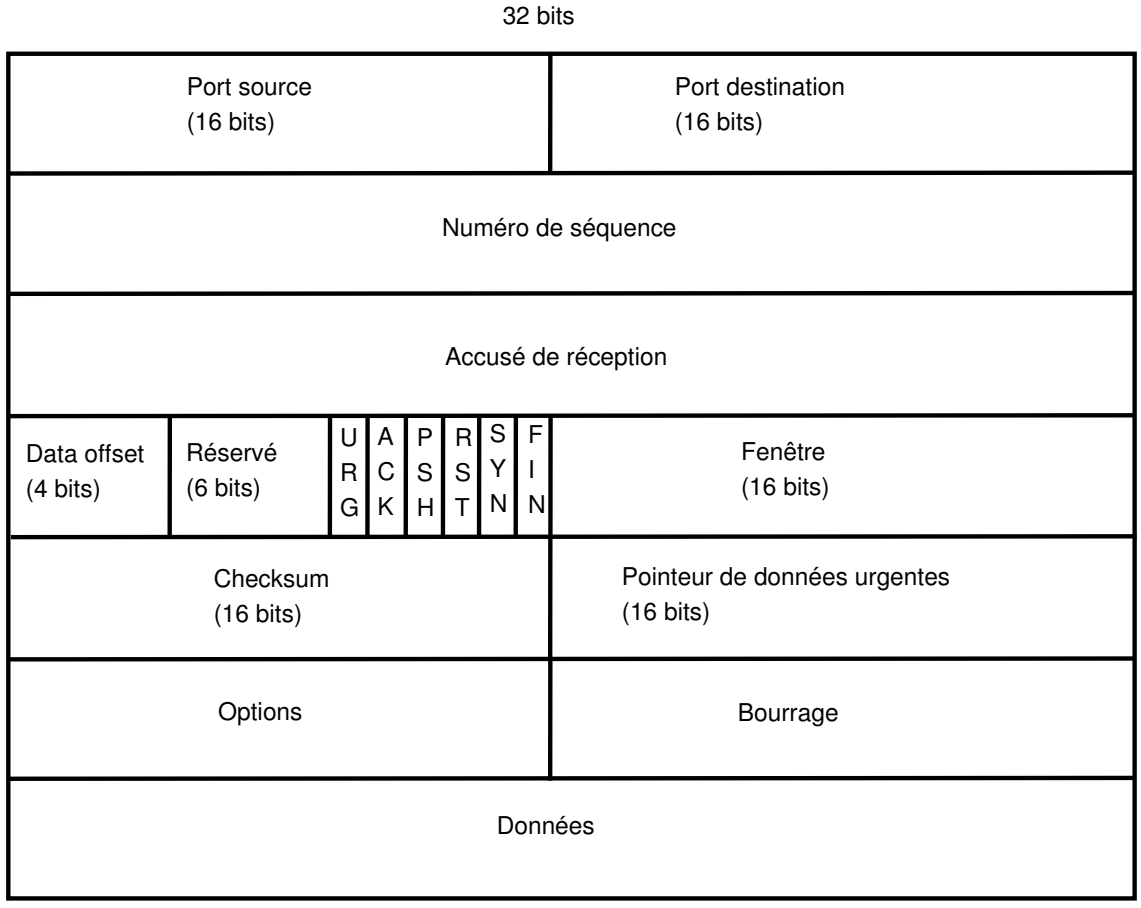
Transmission Control Protocol : RFC 793 : "paquets TCP"

- contient un mécanisme pour assurer le bon acheminement des données ;
- fonctionne en mode connecté ;
- 3-handshaking !

Établissement d'une communication TCP



En-tête TCP


32 bits
Port source
(16 bits)
Port destination
(16 bits)
Numéro de séquence
Accusé de réception
Data offset
(4 bits)
Réservé
(6 bits)
URG
ACK
PSH
RST
SYN
FIN
Fenêtre
(16 bits)
Checksum
(16 bits)
Pointeur de données urgentes
(16 bits)
Options
Bourrage
Données

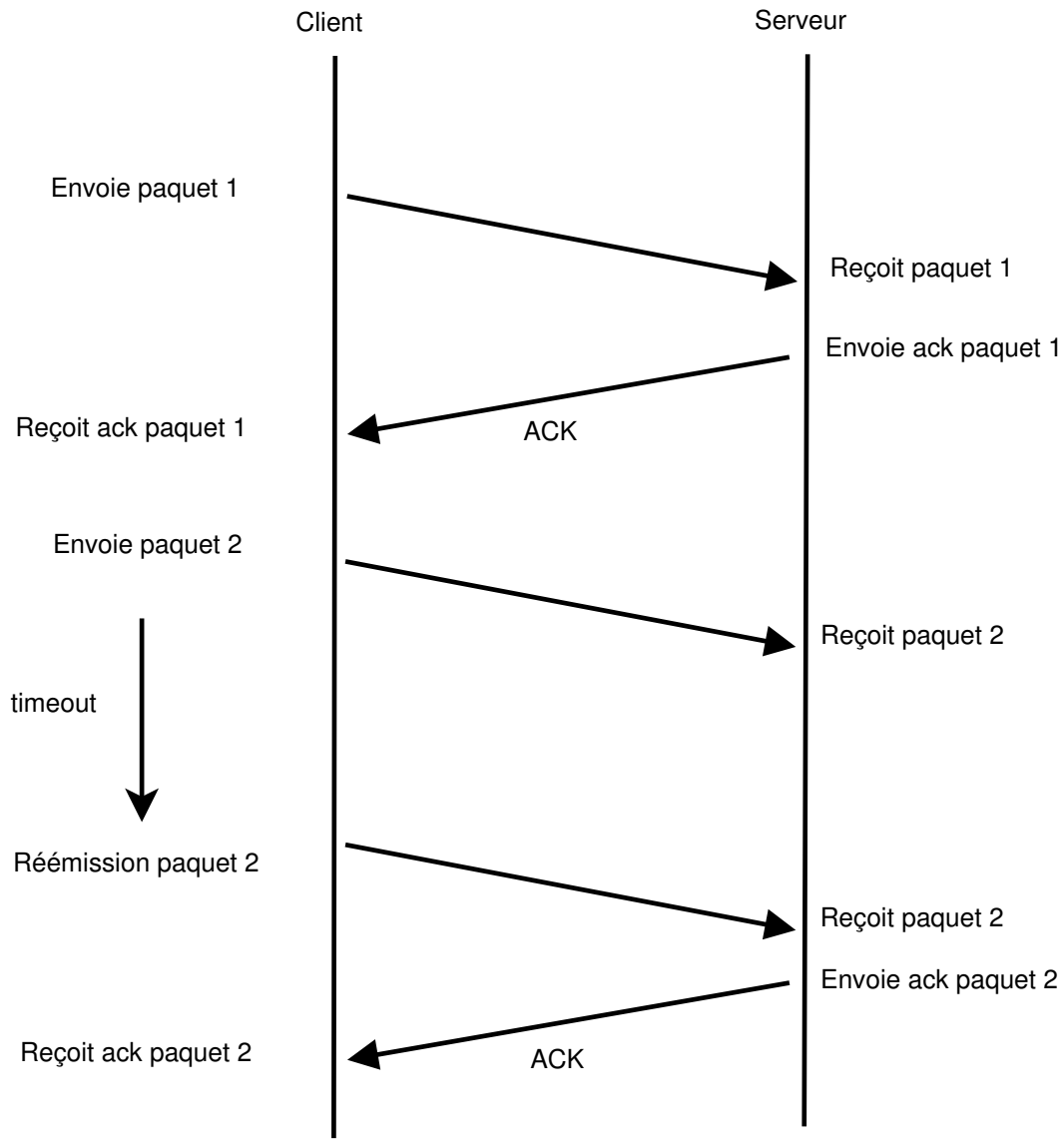
Numéro de séquence

- Numéro de séquence : Il donne la position du segment dans le flux de l'émetteur.
- Numéro d'acquittement : numéro de séquence attendu, soit donc le numéro du dernier octet reçu incrémenté de 1 (les paquets de numéros inférieurs ayant donc tous été reçus).
- Fenêtre : nombre d'octets à transmettre sans nécessité d'accusé de réception ;

Flags TCP

- flags (6) : bits de contrôle ;
  - URG, URGent (1) : utilisation du champ pointeur d'urgence, 1 ;
  - ACK, ACKnowledgment (1) : validation du champ numéro d'acquittement, 1 ;
  - PSH, PuSH (1) : livraison instantanée des données à l'application sans mise en mémoire tampon demande d'acquittement, 1 ;
  - RST, ReSeT (1) : demande de réinitialisation de connexion, 1 ;
  - SYN, SYNchronisation (1) : synchronisation des numéros de séquence, 1 ;
  - FIN, FINalize (1) : fin de la transmission, 1.

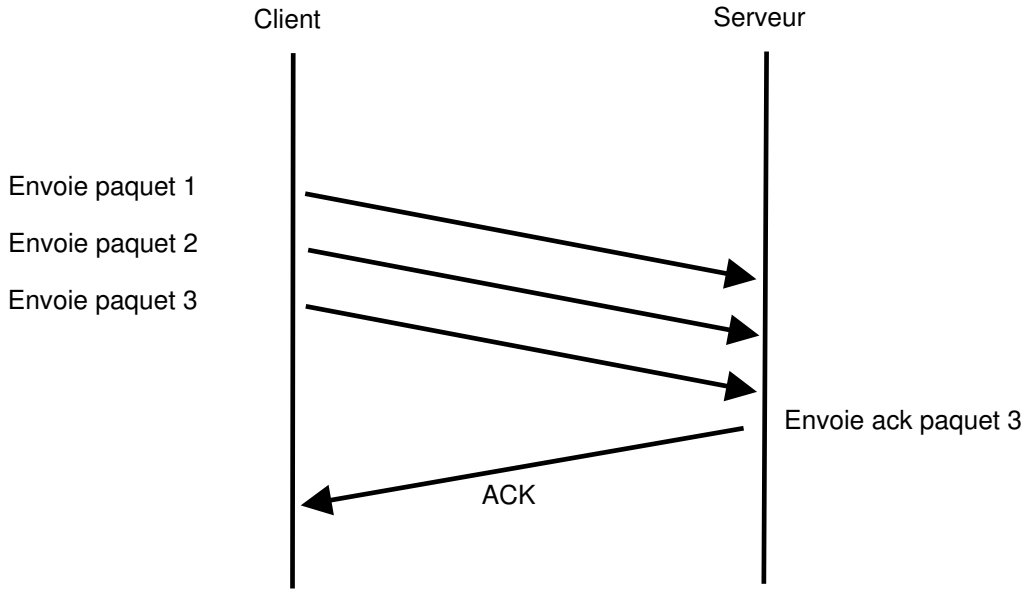
Acquittement



TCP fenêtre glissante

- Le client envoie N paquets sans attendre l'ACK du serveur ;
- Le serveur n'a besoin d'acquitter que le dernier paquet de la fenêtre pour acquitter l'ensemble des paquets envoyés dans cette fenêtre.

TCP fenêtre glissante



TCP fermeture de connexion