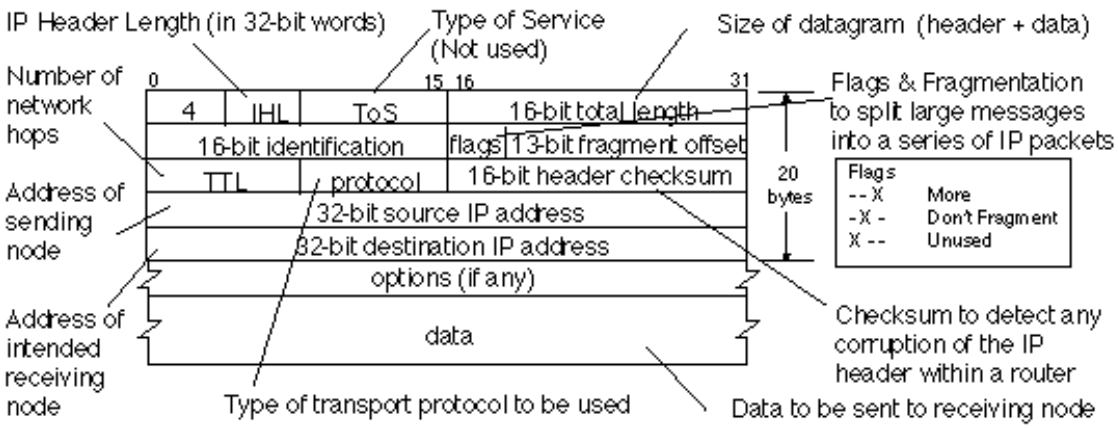
Protocole IP

- Constitution des datagrammes et routage
- Sans connexion, ni contrôle d'erreur, ni contrôle de flux, ni remise en ordre des datagrammes … (pas de garantie de remise)
- Chaque datagramme est traité indépendamment des autres
- Aucune sécurité
- Les services non assurés sont laissées à la charge de la couche supérieure

Protocole IP



Protocole IP

- Version (always set to the value 4 in the current version of IP)
- IP Header Length (number of 32 -bit words forming the header, usually five)
- Type of Service (ToS), now known as Differentiated Services Code Point (DSCP) (usually set to 0, but may indicate particular Quality of Service needs from the network, the DSCP defines the way routers should queue packets while they are waiting to be forwarded).
- Size of Datagram (in bytes, this is the combined length of the header and the data)
- Identification (16-bit number which together with the source address uniquely identifies this packet - used during reassembly of fragmented datagrams)
- Flags (a sequence of three flags used to control whether routers are allowed to fragment a packet (i.e. the Don't Fragment, DF, flag), and to indicate the parts of a packet to the receiver)
- Fragmentation Offset (a byte count from the start of the original sent packet, set by any router which performs IP router fragmentation)
- Time To Live (Number of hops /links which the packet may be routed over, decremented by most routers - used to prevent accidental routing loops)
- Protocol (Service Access Point (SAP) which indicates the type of transport packet being carried (e.g. 6 = TCP; 17= UDP).
- Header Checksum (Used to detect processing errors)
- Source Address (the IP address of the original sender of the packet)
- Destination Address (the IP address of the final destination of the packet)
- Options (not normally used, but, when used, the IP header length will be greater than five 32-bit words to indicate the size of the options field)

Routage

- **Intra-Net** ou **Le routage direct**
  - Il s'agit de délivrer un datagramme à une machine raccordée au même LAN.
  - Protocole ARP.
- **Inter-Net** ou **Le routage indirect**
  - Le destinataire n'est pas sur le même LAN
  - Cette opération est beaucoup plus délicate que la précédente car il faut sélectionner une passerelle.

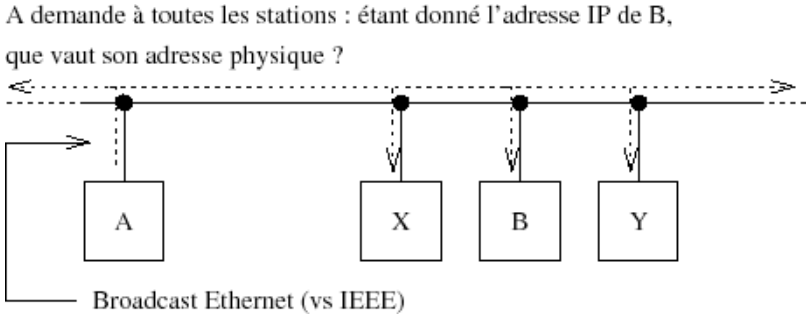
Protocole ARP

- ARP est l'acronyme de "Address Resolution Protocol", il est définie dans la RFC 826.
  - Le problème à résoudre est issu de la constatation qu'une adresse IP n'a de sens que pour la suite de protocole TCP/IP ; celle-ci étant indépendante de la partie matérielle il faut avoir un moyen d'établir un lien entre ces deux constituants.
  - L'usage de ARP est complètement transparent pour l'utilisateur.

Protocole ARP

- la station Ethernet A (I_A, P_A) a besoin de connaitre l'adresse physique de la station Ethernet B (I_B, P_B)

ARP question

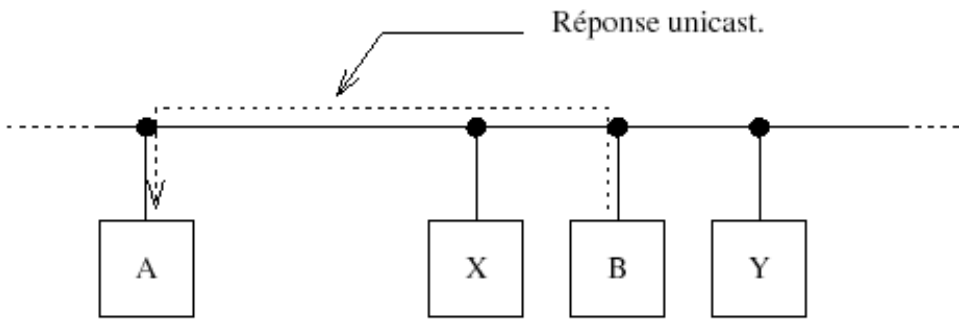


Protocole ARP

- Toutes les machines du LAN écoutent cet échange et peuvent mettre à jour leur table de conversion (adresse IP adresse Ethernet) pour la machine A.
- la réponse de B est du type “unicast”.
  - Remarque : quand une station Ethernet ne répond plus il y a suppression de l'association adresse IP - adresse MAC.

Protocole ARP

ARP answer



B répond directement à A en lui communiquant son adresse physique.

Protocole ARP

- Il n'est pas besoin d'utiliser ARP préalablement à chaque échange, car heureusement le résultat est mémorisé.
- En règle générale la durée de vie d'une adresse en mémoire est de l'ordre de 20 minutes et chaque utilisation remet à jour ce compteur.

Protocole ARP

- La commande arp -a sous Unix permet d'avoir le contenu de la table de la machine sur laquelle on se trouve, par exemple :
- $ arp -a
- soupirs.chezmoi.fr (192.168.192.10) at 8:0:9:85:76:9c
  espoirs.chezmoi.fr (192.168.192.11) at 8:0:9:85:76:bd
  plethore.chezmoi.fr (192.168.192.12) at 8:0:9:a:f9:aa
  byzance.chezmoi.fr (192.168.192.13) at 8:0:9:a:f9:bc
  ramidus.chezmoi.fr (192.168.192.14) at 0:4f:49:1:28:22 permanent
  desiree.chezmoi.fr (192.168.192.33) at 8:0:9:70:44:52
  pythie.chezmoi.fr (192.168.192.34) at 0:20:af:2f:8f:f1
  ramidus.chezmoi.fr (192.168.192.35) at 0:4f:49:1:36:50 permanent
  gateway.chezmoi.fr (192.168.192.36) at 0:60:8c:81:d5:1b

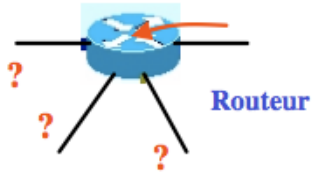
Routage Indirecte

- Le service offert par la couche Réseau (protocole IP) est l'acheminement des datagrammes d'une station connectée au réseau à une autre station, sans connexion.
- Chaque datagramme IP est traité individuellement et aiguillé par une stratégie de routage préalablement définie.
- Principal inconvénient : le risque d'arrivée dans le désordre des différents paquets d'une communication.
- Principal avantage : l'adaptation rapide au trafic et aux différents problèmes qui peuvent survenir dans un réseau (équipement en panne, saturation...).

Routage Indirecte

- Terminologie
  - “routeur” : capable de transmettre un datagramme d'un interface à un autre
  - “hôte” n’est pas capable de transmettre un datagramme d'un interface à un autre et pas le deuxième

Routage



- table de routage contient :
  - l'adresse du destinataire à atteindre (adresse de station, adresse d'un réseau) et le prochain équipement (nexthop) à atteindre sur ce «chemin».
- Aiguiller c'est engager le paquet sur le chemin le plus court en matière de distance, ou parfois de temps, ou sur des chemins définis.
- Plusieurs stratégies de routage :
  - statiques: la mise à jour des tables de routage est établie par les administrateurs des différents équipements de l'Internet (Stations, passerelles...);
  - dynamiques: la mise à jour est faite automatiquement en fonction de mesures de trafic ; Les différents équipements peuvent s'échanger des informations de routage (ex: RIP).

Table de Routage

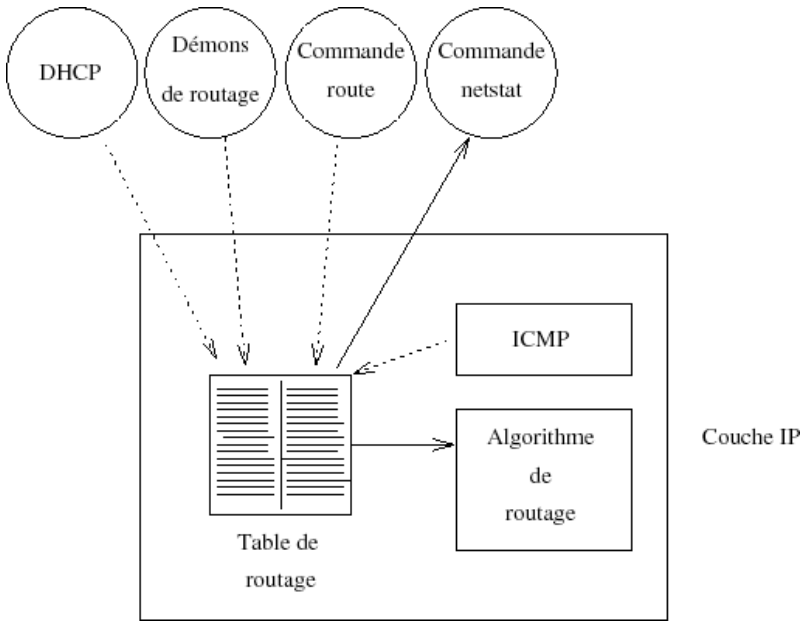


Table de Routage

- **Comment est-elle crée ?**
  - Au démarrage avec la commande route, invoquée dans les scripts de lancement du système
  - Manuellement avec la commande route, à partir du shell (administrateur système uniquement).
  - Dynamiquement avec les démons de routage *routed* ou *gated* (la fréquence de mise à jour est typiquement de l'ordre de 30 sec.).
  - Par des messages "ICMP redirect".

Table de Routage

- La commande netstat -rn permet de la visualiser au niveau de l'interface utilisateur.

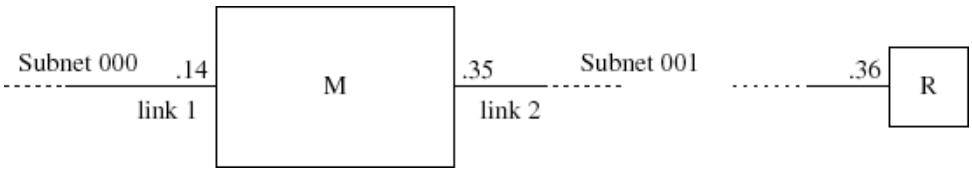
```
$ netstat -rn
Routing tables

Internet:
Destination          Gateway            Flags
default              192.168.192.36     UGS
127.0.0.1            127.0.0.1          UH
192.168.192/27       link#1             UC
192.168.192.10       8:0:9:85:76:9c     UHLW
192.168.192.11       8:0:9:85:76:bd     UHLW
192.168.192.12       8:0:9:88:8e:31     UHLW
192.168.192.13       8:0:9:a:f9:bc      UHLW
192.168.192.14       0:4f:49:1:28:22    UHLW
192.168.192.15       link#1             UHLW
192.168.192.32/27    link#2             UC
192.168.192.33       8:0:9:70:44:52     UHLW
192.168.192.34       0:20:af:2f:8f:f1   UHLW
192.168.192.35       0:4f:49:1:36:50    UHLW
192.168.192.36       link#2             UHLW
```

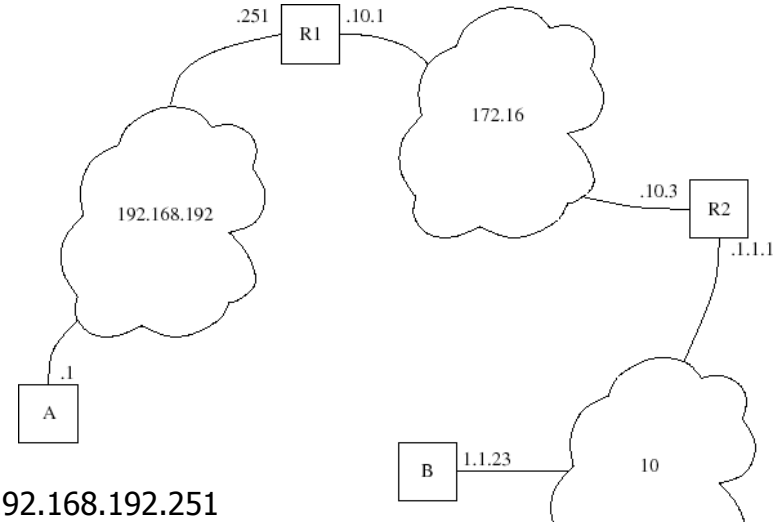
Table de Routage

C c	La route est générée par la machine, à l'usage.
D	La route a été crée dynamiquement (démons de routage).
G	La route désigne une passerelle, sinon c'est une route directe.
H	La route est vers une machine, sinon elle est vers un réseau.
L	Désigne la conversion vers une adresse physique (cf ARP).
M	La route a été modifiée par un `` redirect ''.
S	La route a été ajoutée manuellement.
U	La route est active.
W	La route est le résultat d'un clônage.

Table de Routage



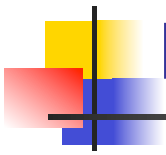
Routage Statique



Machine A default : 192.168.192.251
Machine B default : 10.1.1.1
Routeur R1 10 : 172.16.10.3
Routeur R2 192.168.192 : 172.16.10.1

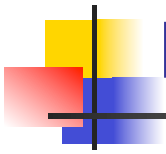
Routage Dynamique

- 2 principaux types d'algorithme de routage (routage dynamique) :
  - vecteur de distance (distancevector) => protocole RIP
    - table de routage basée "coût" (nombre de sauts) de chacune des routes
    - échange de table entre routeurs adjacents
  - état des liens (linkstaterouting) => protocole OSPF (Open Shortest Path First)
    - écoute en continu et recensement des différents éléments autour
    - table de routage basée sur les plus courts chemins (en temps) vers les autres routeurs
    - diffusion de cette information (aux voisins) sous formes de paquets de mise à jour.



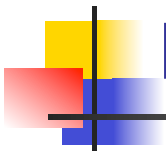
Protocole RIP

- basé sur des vecteurs de distances pour comparer mathématiquement des itinéraires :
  - métrique utilisant le nombre de sauts (hop count) entre la source et la destination : chaque saut sur le chemin vaut 1 => identification du «meilleur chemin» d'un point de départ à une destination donnée.
- messages de mise àjour :
  - périodiques (intervalles réguliers, toutes les 30 secondes)
  - apériodiques (lorsque la topologie du réseau change), propagés aux voisins



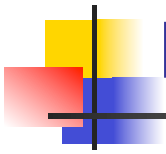
Protocole RIP

- Stabilité et particularité du protocole RIP
  - empêche les boucles de routage de continuer indéfiniment : le nombre maximal de sauts permis entre la source et la destination est 15.
  - si nbresauts >15, la destination du réseau est considérée comme inaccessible (infinie). limite le diamètre maximal d'un réseau RIP àmoins de 16 sauts (0..15).
  - exécute le Split Horizon: principe qui empêche d'envoyer des informations concernant une route dans la direction par laquelle elle est venue



Protocole RIP

- Principe de fonctionnement Réception (par un routeur) d'une mise à jour
- Elle induit un changement si l'itinéraire est :
  - Nouveau (nouvelle destination) ⇒nouvelle entrée dans la table de routage
  - Meilleur (valeur métrique plus basse) ⇒modification de l'entrée existante, mise à jour de l'entrée de sa table de routage pour refléter cet itinéraire, avec incrémentation (+1) de la valeur métrique et avertissement de l'expéditeur, Après cette mise à jour de sa table de routage, propagation aux routeurs adjacents pour transmettre les mises à jour (indépendamment des mises à jour régulières)



Protocole RIP

- Compteurs utilisés
  - «routing-update»…pour l'intervalle entre les mises à jour périodiques. 30 secondes, avec un petit temps aléatoire ajouté à chaque remise à 0 pour empêcher la congestion du réseau (pb si tous les routeurs essayaient simultanément de mettre à jour leur table).
  - «route-timeout»…pour la validité de chaque entrée de la table (par défaut à180 secondes). si cpteur expire ⇒itinéraire invalide, mais est conservé dans la table tant que pas «route-flush»
  - «route-flush »…pour suppression d'une route (par défaut à 240 secondes).

Exemple

Illustration RIP *(Routing Information Protocol)*

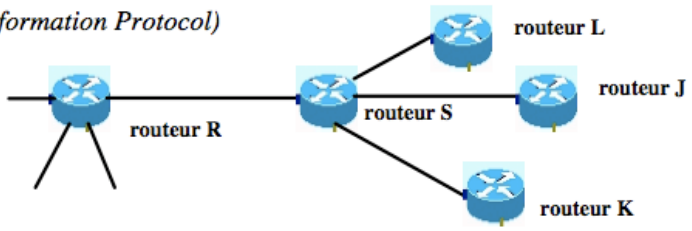


Table 1 (émise par routeur R)	
destination	distance
Réseau 1	0
Réseau 2	1
Réseau 6	1
Réseau 9	2
Réseau 14	4
Réseau 23	3
Réseau 25	6
Réseau 34	*15*

Table 2 (appartenant au routeur S)		
destination	distance	Route
Réseau 1	0	Directe
Réseau 2	0	Directe
Réseau 6	2	Routeur R
Réseau 9	1	Routeur J
Réseau 11	3	Routeur K
Réseau 14	4	Routeur R
Réseau 23	6	Routeur L

Table 2 actualisée		
destination	distance	Route

Exemple

Illustration RIP *(Routing Information Protocol)*

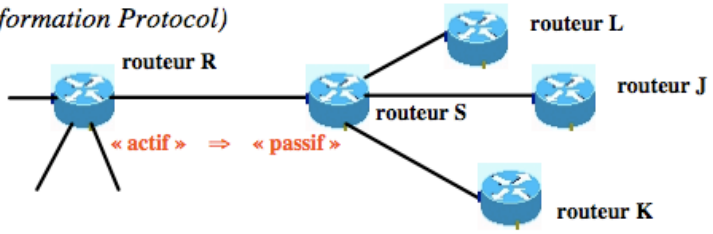


Table 1 (émise par routeur R)	
destination	distance
Réseau 1	0
Réseau 2	1
Réseau 6	1
Réseau 9	2
Réseau 14	4
Réseau 23	3
Réseau 25	6
Réseau 34	*15*

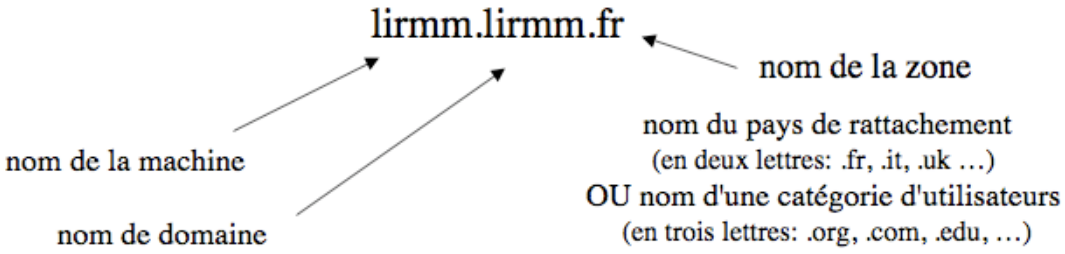
route infinie pour S (15+1 > max)

Table 2 (appartenant au routeur S)		
destination	distance	Route
Réseau 1	0	Directe
Réseau 2	0	Directe
Réseau 6	2	Routeur R
Réseau 9	1	Routeur J
Réseau 11	3	Routeur K
Réseau 14	4	Routeur R
Réseau 23	6	Routeur L

Table 2 actualisée		
destination	distance	Route
Réseau 1	0	Directe
Réseau 2	0	Directe
Réseau 6	2	Routeur R
Réseau 9	1	Routeur J
Réseau 11	3	Routeur K
Réseau 14	**5**	**Routeur R**
Réseau 23	**4**	**Routeur R**
Réseau 25	**7**	**Routeur R**

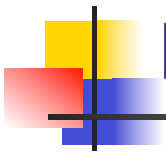
Nom et adressage IP

- Routage IP, basé sur l'adresse IP, impose une correspondance entre le nom et l'adresse : la résolution de nom
- Un nom se compose de plusieurs parties séparées par un point ex. lirmm.lirmm.fr
- C'est un nom hiérarchique. Il se lit de droite à gauche.



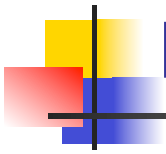
Nom et adressage IP

- Résolution réalisée :
  - soit à travers un fichier " hosts " local
  - soit à travers un serveur de noms, DNS (Domain Name Server/System), auquel on envoie une requête de demande d'adresse IP.
- Système d'annuaire distribué. Si le serveur de noms DNS ne trouve pas la correspondance, il transmet la demande à un serveur autorisé.
- Pour améliorer les performances, un système de cache (mémorisant les résolutions précédentes) est mis en place permettant d'éviter au maximum le trafic.



La couche Transport

- Protocole TCP (Transport Control Protocol) Transmission fiable des données et Distribution des connexions IP aux applications (couche supérieure)
  - orienté connexion
  - contrôle d'erreur, contrôle de flux, remise en ordre des datagrammes…

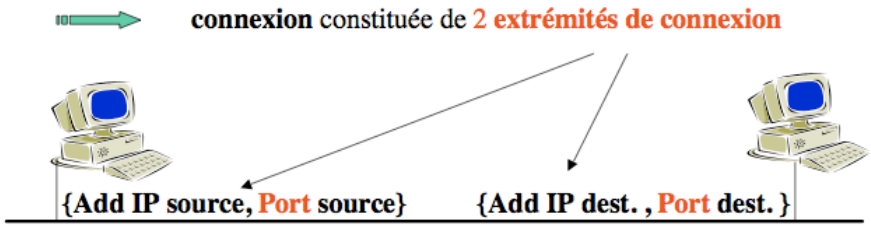


La couche Transport

- Protocole UDP (User Datagram Protocol)
  - sansconnexion, sans garantie

Protocole TCP

- permet aux deux entités connectées de savoir qu'elles sont présentes et en relation avant d'échanger,
- permet éventuellement d'assurer un contrôle de flux en fonctiondes ressources allouées (zones mémoires, files d'attente, etc.).



Services de transmission de données de bout en bout

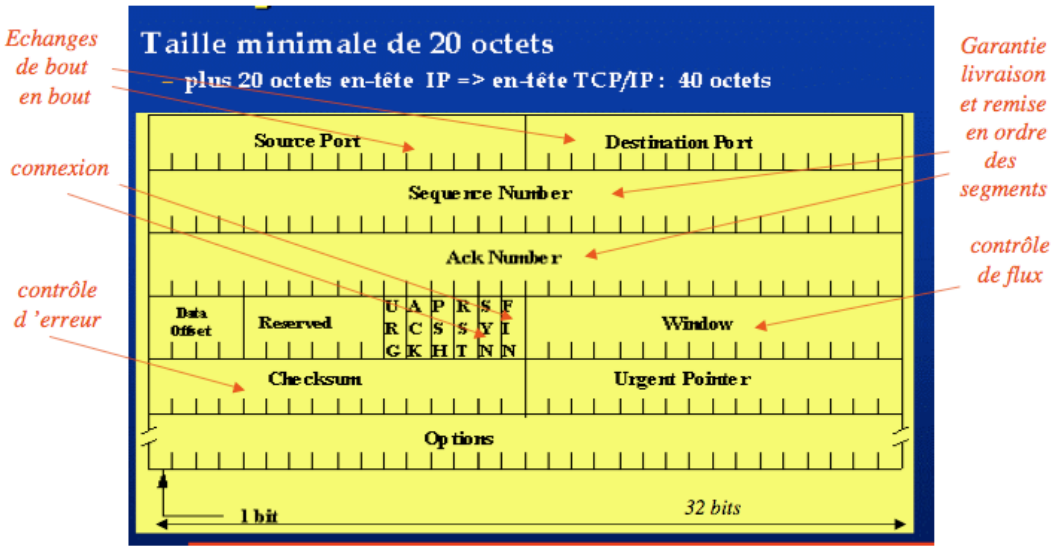
entre applications ⇨ *entre les Ports via lesquels les applications échangent*

Le couple "extrémités de connexion" est unique pour une connexion donnée.

Protocole TCP

- Notion de Port= «porte d'entrée/sortie» d'un processus de la couche application
- Attribution des numéros de Port
  - internationalement «assignés» < 1023 (ex: FTP ports 20 & 21, TELNET port 23, etc.)

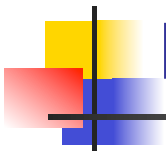
Header TCP



Source : www.urec.cnrs.fr

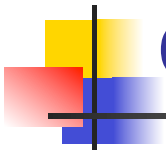
Header TCP

- Port source et destination: permet d'identifier l'application émettrice et réceptrice.
- Numéro de séquence: numérote la séquence, en identifiant la position de l'octet dans le flux de données.
- Numéro d'acquittement: numéro de séquence plus 1 de la dernière séquence TCP reçue avec succès. Ce champ n'est valide que si le flag ACK=1.
- longueur en-tête: c'est le nombre de mots de 32 bits figurant dans l'en-tête. Il permet de déterminer la présence d'options.
- URG: Le Pointeur Urgent est valide (ex: cas du Ctrl C dans application Telnet).
- ACK: Le numéro d'acquittement est valide.
- PSH: Le récepteur devrait passer cette donnée à l'application le plus tôt possible.
- RST: Réinitialise la connexion.
- SYN: Synchronise les numéros de séquence pour initialiser une connexion. SYN=1 lorsqu'une
- nouvelle connexion est en train de s'établir.
- FIN: fermeture de connexion.
- taille de fenêtre: taille de la zone tampon pour chaque émission (en octets).
- somme de contrôle: recouvre l'en-tête et les données TCP (si erreur détectée pas d'ACK délivré).
- options: un exemple est la taille maximale du segment que le récepteur peut recevoir (MSS), cette option est utilisée lors de l'ouverture de connexion.
- Données données à transmettre.



Protocole TCP

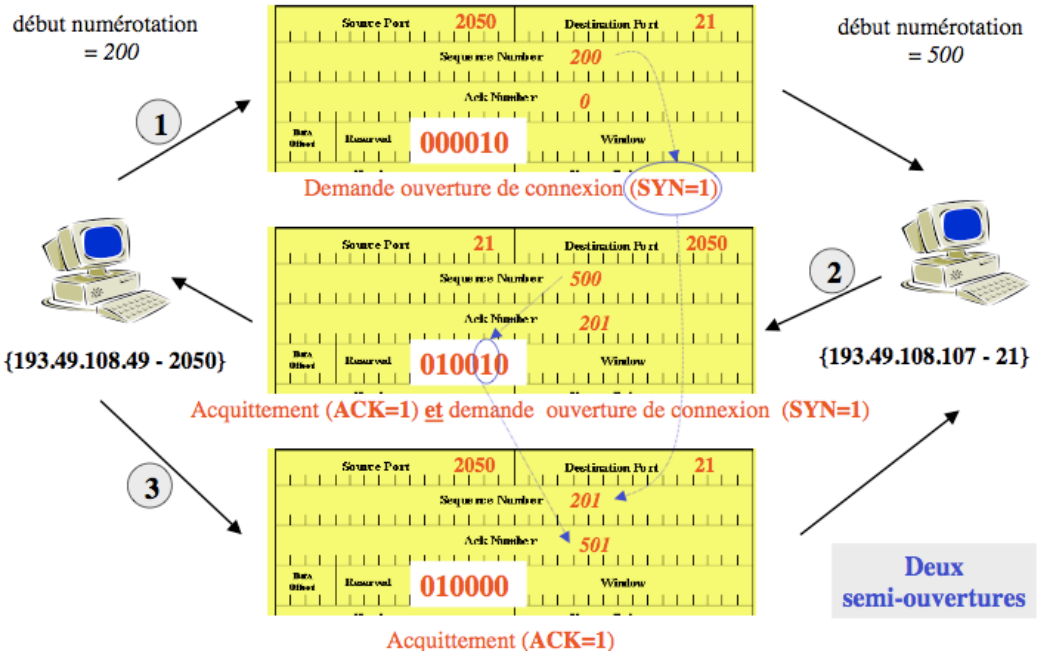
- Connexion
- Echange des données
- Fermeture de connexion



Connexion

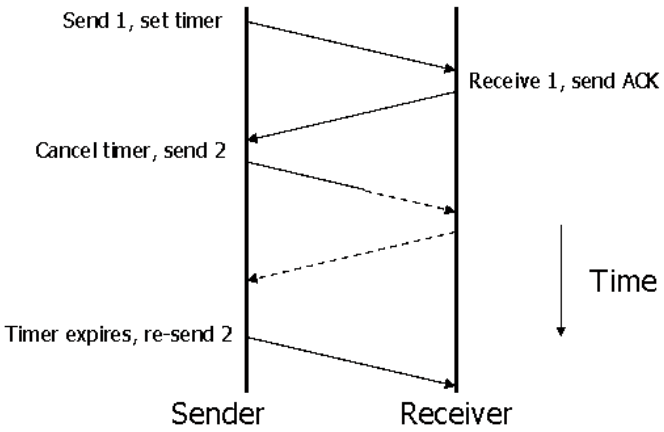
- Séquence d' ouverture (3 way handshake):
  - demande d'ouverture de connexion par l'entité source
    - SYN message + sequence number + port
  - réponse de l'entité cible sous forme de demande de connexion
    - (SYN+ACK) + server sequence number
  - confirmation de connexion de la source à la cible
    - ACK

Connexion



Echange des données

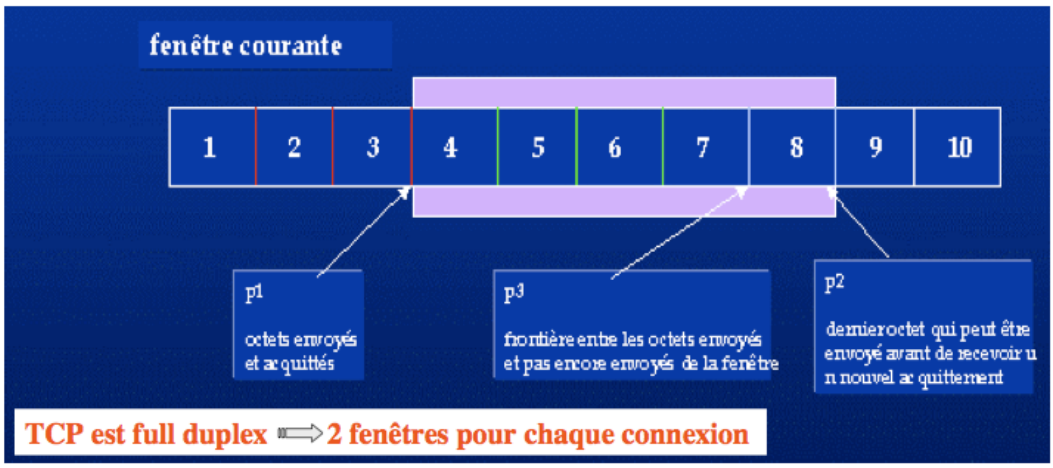
- simplex stop-and-wait



Echange des données

- sliding windows
  - protocole **go-back-N**
  - protocole **selective reject**

Fonctionnement basé sur 3 pointeurs



Fermeture de connexion

- 2-way handshake
  - Message FIN (client ou server)
  - ACK du FIN: le client ou server considère la connexion fermée, mais il peut encore recevoir des données
  - Le client ou server envoi FIN de qu' il as terminé d' envoyer des données et il attende l' ACK