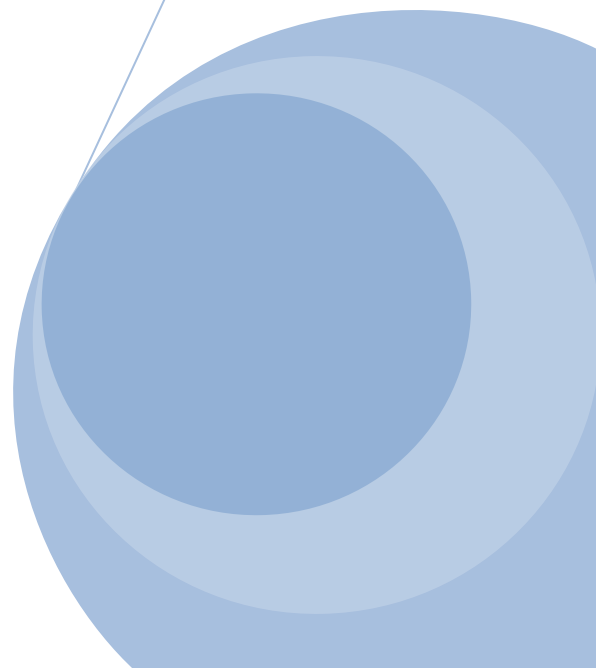


LES RESEAUX



Sommaire:

1. Objectifs et utilisation des réseaux.....	5
1.1. Partage des ressources.....	5
1.2. Augmentation de la fiabilité et des performances.....	5
1.3. Réduction des coûts.....	5
1.4. Accès à l'information et au courrier.....	5
1.5. Autres utilisations.....	5
2. L'avenir des réseaux.....	6
3. Que signifie réseau.....	6
4. Différents types de réseaux.....	6
5. Composants actifs:.....	9
5.1. Répéteur.....	9
5.2. HUB.....	9
5.3. Switch.....	9
5.4. Routeur.....	10
5.5. Carte Réseau.....	10
6. TCP/IP.....	12
6.1. IP.....	12
6.2. La couche IP comprend plusieurs protocoles :.....	13
6.2.1. Scénario typique de l'utilisation d'ARP (couche 3).....	13
6.2.2. RARP (pour Reverse ARP) :.....	13
6.2.3. ICMP (Internet Control Message Protocol -couche 3).....	14
6.2.4. Le routage IP.....	14
6.2.5. Les ports.....	15
6.3. UDP (User Datagram Protocol).....	16
6.4. TCP.....	17
6.5. Les adresses TCP/IP :.....	19
6.5.1. Les classes d'adresses :.....	19
6.5.2. Etendue de chaque classe :.....	19
6.5.3. Le masque de sous réseau :.....	20
7. Le modèle O.S.I.....	24
7.1. La couche physique 1.....	24
7.2. La couche de liaison de données 2.....	24
7.3. La couche réseau 3.....	25
7.4. La couche transport 4.....	25
7.5. La couche session 5.....	25
7.6. La couche présentation 6.....	26
7.7. La couche application 7.....	26
7.8. L'encapsulation.....	26
8. Le modèle OSI et TCP/IP.....	27
8.1. En résumé :.....	28
9. Les topologies.....	31
9.1. Le BUS.....	31
9.1.1. Avantages.....	31
9.1.2. Inconvénients.....	31
9.1.3. Conclusions.....	31
9.2. L'étoile.....	32
• Principe.....	32
9.2.1. Avantages.....	32
9.2.2. Inconvénients.....	32
9.3. Les réseaux en anneau.....	33
10. Architecture des réseaux.....	33
10.1. Poste à poste.....	33
10.2. Client serveur.....	33
10.2.1. Avantages de l'architecture client/serveur.....	34

10.2.2. Inconvénients du modèle client/serveur	34
11. Les systèmes serveurs	34
11.1. Basés sur trois protocoles :	34
• NetBEUI	34
• IPX/SPX	35
• TCP/IP	35
11.2. Communication client / serveur	35
11.3. Exemple de Communication Internet	35
Consultation de page WEB	35
Ethernet	36
12. ETHERNET	37
12.1. Historique	37
12.2. Le support physique	37
12.2.1. Ethernet 10 base 5	37
12.2.2. Ethernet 10 base 2	38
12.2.3. Réseau 10 Base T :	38
13. Méthode d'accès au support	39
13.1. Deux problèmes à résoudre	39
13.2. Parler et se faire entendre...	39
13.3. La liberté dans l'auto discipline (Ethernet)	39
13.3.1. Avantages	39
13.3.2. Inconvénients	39
13.4. L'organisation déterminée (Token Ring)	40
13.4.1. Avantages	40
13.4.2. Inconvénients	40
13.5. Enfin, une solution chère mais efficace (ATM)	40
13.6. Accès aléatoire Ethernet	40
13.6.1. Protocole d'accès au média CSMA/CD	40
13.6.2. Principe du CSMA/CD	41
• Les collisions	41
13.6.3. Vitesse de propagation, temps d'aller-retour	42
13.6.4. Performances	42
14. Trame Ethernet	43
14.1. Le préambule	43
14.2. Start Frame Delimiteur	43
14.3. Adresse destination et adresse source (MAC)	43
14.1. Le champ longueur / type	44
14.2. Les données	44
14.3. Le champ de contrôle	44
14.4. Le temps inter-trame	44
15. Ressource et références :	45

Objectif et utilisation des réseaux

1. Objectifs et utilisation des réseaux

Les réseaux ont été et sont toujours développés pour un certain nombre de raisons. Il y en a en fait 4 principales.

1.1. Partage des ressources

Les réseaux permettent de rendre accessible un certain nombre de ressources (logiciels, bases de données, imprimantes...) indépendamment de la localisation géographique des utilisateurs.

.....

.....

Le partage des données commerciales d'une entreprise en est une illustration : chaque employé d'une multinationale peut accéder aux derniers comptes de résultat de l'entreprise.

1.2. Augmentation de la fiabilité et des performances

Les réseaux permettent par exemple de dupliquer en plusieurs endroits les fichiers vitaux d'un projet, d'une entreprise ; en cas de problème, la copie de sauvegarde est immédiatement disponible.

.....

.....

L'augmentation des performances vient également du fait qu'il est relativement facile d'augmenter les performances d'un système en réseau en ajoutant tout simplement un ou deux autres ordinateurs supplémentaires. Ce dernier point associé à un constat économique (voir objectif suivant) rend presque obsolètes les grosses installations.

1.3. Réduction des coûts

En effet, les ordinateurs individuels coûtent bien moins cher que les gros systèmes centralisés (1000 fois moins environ), et ce pour une baisse des performances d'à peine un facteur 10.

1.4. Accès à l'information et au courrier

Avec les réseaux et en particulier **Internet**, il est très facile de s'informer sur toute sorte de sujets très rapidement. Ce dernier objectif joue en fait un rôle capital dans l'utilisation que les gens ont des réseaux. C'est peut-être même l'utilisation principale aujourd'hui.

1.5. Autres utilisations

Au delà de ces quatre points, il existe quelques autres objectifs aux réseaux, mais ces objectifs sont apparus récemment avec la démocratisation des réseaux et l'émergence d'Internet notamment, et ne correspondent pas véritablement à un besoin des professionnels.

Les réseaux vont servir par exemple de support pour des jeux interactifs et autres divertissements, ainsi que de médium de communication.

.....

.....

2. L'avenir des réseaux

Les réseaux et toutes les technologies environnantes sont en pleines expansions.

Augmentation de la bande passante, de plus en plus d'utilisateurs, autant d'éléments motivant les entreprises dans la réalisation de solutions techniques innovantes.

Le but n'est plus de proposer un moyen de connecter les gens, **il est de fournir la meilleure connexion et le meilleur service possibles au moindre coût.**

.....

3. Que signifie réseau

Le terme réseau en fonction de son contexte peut désigner plusieurs choses.

Il peut désigner l'ensemble **des machines, ou l'infrastructure informatique d'une organisation avec les protocoles**

.....

qui sont utilisés, ce qui 'est le cas lorsque l'on parle de Internet.

Le terme réseau peut également être utilisé pour décrire **la façon dont les machines d'un site sont interconnectées**

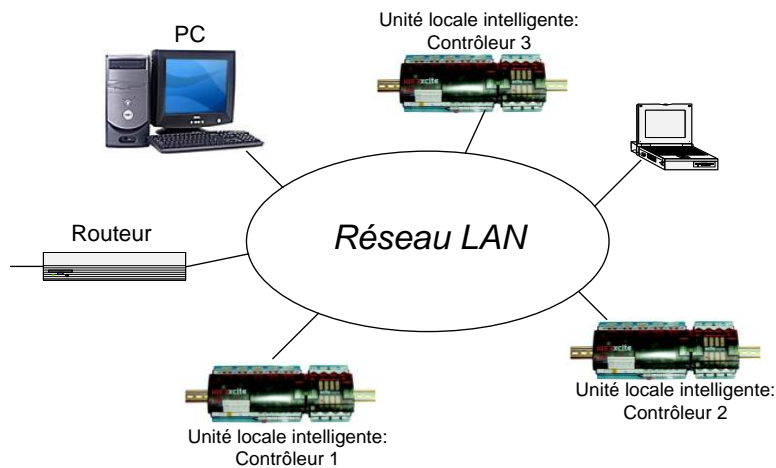
C'est le cas lorsque l'on dit que les machines d'un site (sur un réseau local) sont sur un réseau **Ethernet, Token Ring, réseau en étoile, réseau en bus,**.....

Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent. On peut parler de réseau TCP/IP, NetBeui (protocole Microsoft) DecNet (protocole DEC), IPX/SPX,...

4. Différents types de réseaux

Il existe différents types de réseaux ; suivant la localisation, les distances entre les systèmes informatiques et les débits maximum, on peut distinguer trois types de réseaux.

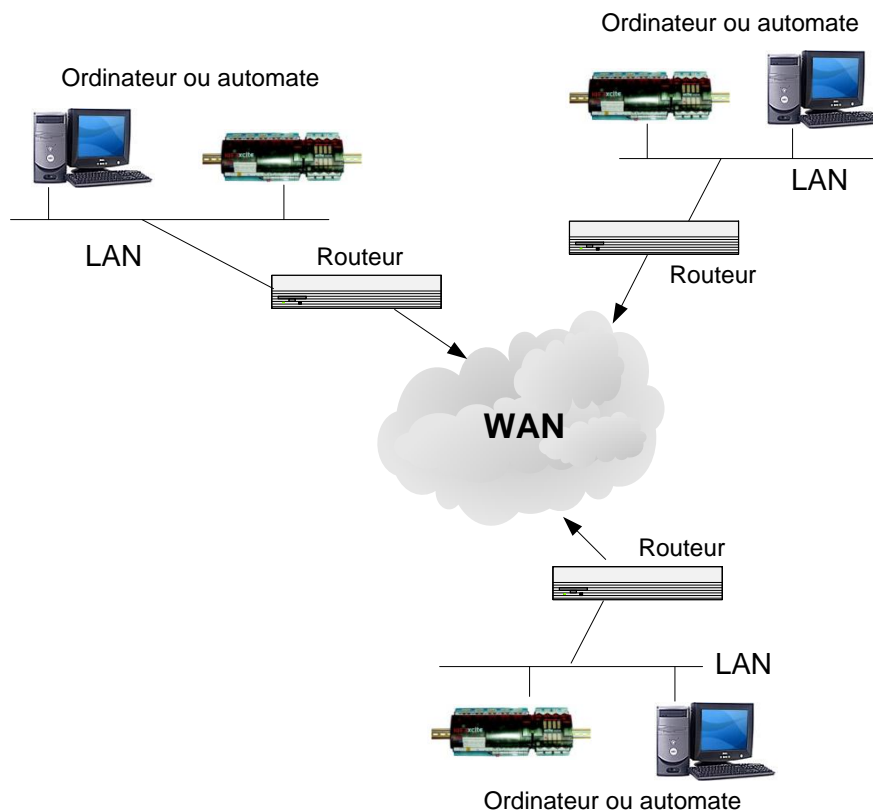
- Les *réseaux locaux* ou **LAN (Local Area Network)**qui correspondent par leur taille aux réseaux intra-entreprise et qui permettent l'échange de données informatiques ou le partage de ressources (Ethernet, Token ring, ATM).



➤ Les réseaux métropolitains ou MAN (Metropolitan Area Network)

➤ Les réseaux longues distances ou **WAN** (Wide Area Network), généralement publics (Renater), et qui assurent la transmission des données numériques sur des distances à l'échelle d'un pays. Le support utilisé peut être terrestre (réseau maillé de type téléphonique ou ligne spécialisée) ou hertzien (transmission par satellite).
Types de réseaux Wan : ADSL

Dans une grande entreprise, un réseau est généralement une combinaison plus ou moins complexe de Lan et de Wan.

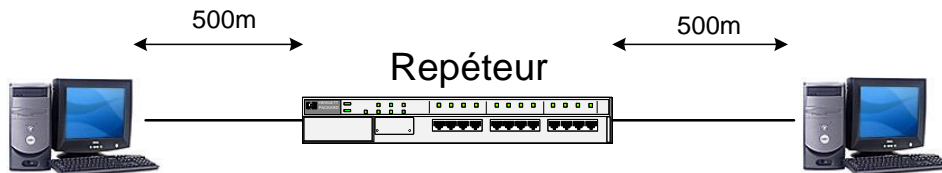


Les composants

5. Composants actifs:

5.1. Répéteur

Un **répéteur** reçoit des informations et les retransmets en régénérant un signal. Un répéteur permet de connecter 2 segments Ethernet dans un LAN.



Un réseau 10Base T peut utiliser des « **HUBs** » comme répéteurs.

5.2. HUB

Un Hub récupère les **trames Ethernet en provenance d'un port et les renvoie vers tous les autres ports.**

.....
Toutes les trames en provenance d'une interface Ethernet sont envoyées à toutes les autres interfaces présentes sur ce HUB.

Ainsi on est 'sur' que le destinataire recevra l'information.

Inconvénients : toutes les interfaces pour lesquelles la trame n'est pas destinée la recevront également.

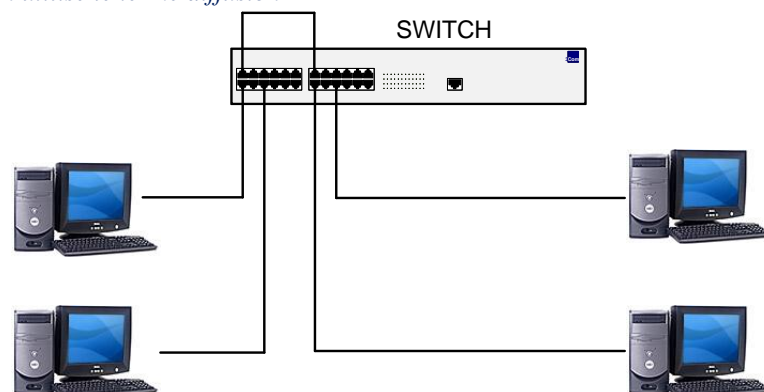
Cela génère beaucoup de trafic inutile sur le réseau, il y a risque **de saturation.**

5.3. Switch

Alors que les Hubs ne font que transférer, **de façon aveugle,** les trames à travers le réseau, les **switchs** sont capables **de connaître la destination en consultant** dans chaque trame l'adresse MAC de l'expéditeur et du destinataire.

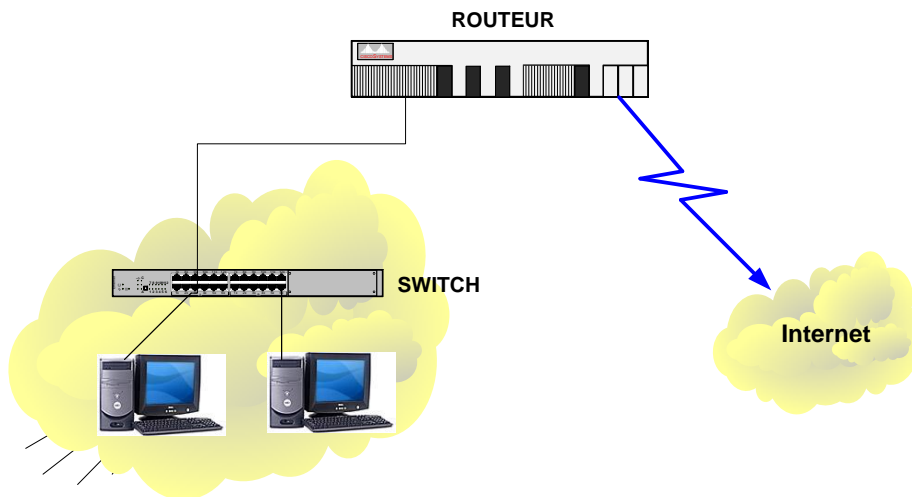
En conservant la trace de ces adresses MAC dans sa table d'adresse, un switch est capable de transférer exactement la trame sur le port où est raccordé le destinataire (sauf les trames de Broadcasts).

Nota : Le broadcast est un terme anglais définissant une diffusion de données à un ensemble de machines connectées à un réseau. En français on utilise le terme diffusion



5.4. Routeur

C'est une passerelle entre le LAN (réseau local) et un autre réseau (Internet par exemple). Ils sont employés pour relier 2 réseaux ensemble et diriger le trafic des réseaux basés sur les adresses IP. Beaucoup de routeurs sont employés pour créer **Internet**.



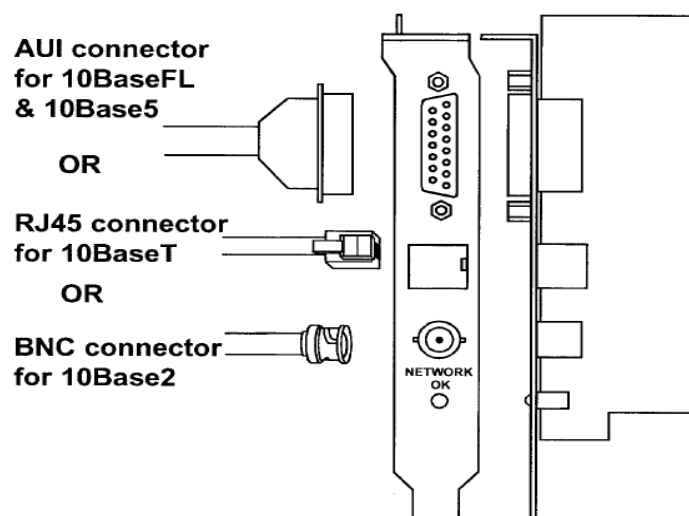
Le routeur contient une base de données appelée « **Routing Table** » qui détient des chemins d'accès aux différents réseaux.

Les routeurs sont en général utilisés au niveau réseau de l'Entreprise, pour relier différentes unités ou différents sites. Ils sont parfois associés à des fonctions de sécurité de type pare-feu « (**Firewall**) » pour filtrer les accès distants.

Un routeur doit être configuré pour pouvoir connaître où router les messages. Les mécanismes de routage sont basés sur l'adresse IP. Les stations sont regroupées sur un même sous-réseau selon leurs adresses IP et leur masque de sous-réseau.

Chaque message adressé à un réseau distant sera transmis au routeur qui assurera le routage vers la bonne destination.

5.5. Carte Réseau



TCP/IP

6. TCP/IP

TCP/IP est un **protocole**, c'est à dire des **règles de communication**.

- **TCP** signifie **Transmission Control Protocol** : littéralement *Protocole de Contrôle de Transmission (couche)*
- **IP** signifie **Internet Protocol** : littéralement "le protocole d'Internet". C'est le principal protocole utilisé sur Internet (couche 3). *{que nous verrons sur l'explication du Modèle O.S.I.}*

6.1. IP

Internet signifie **Inter-networks**, c'est à dire "entre réseaux". Internet est l'*interconnexion des réseaux* de la planète.

Le protocole **IP** permet **aux ordinateurs reliés à ces réseaux de dialoguer entre eux**.

Faisons un parallèle avec la poste.

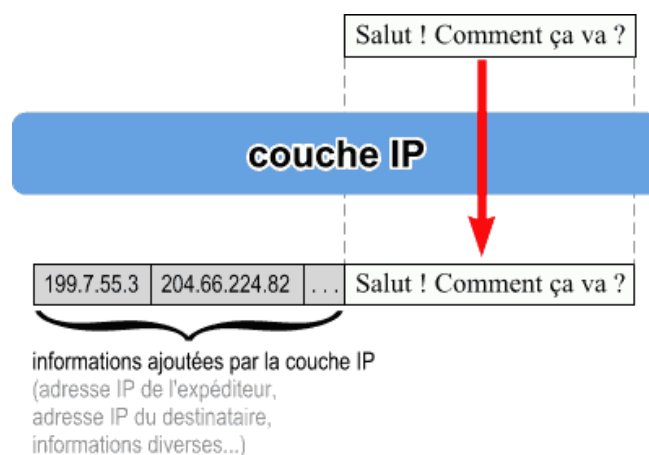
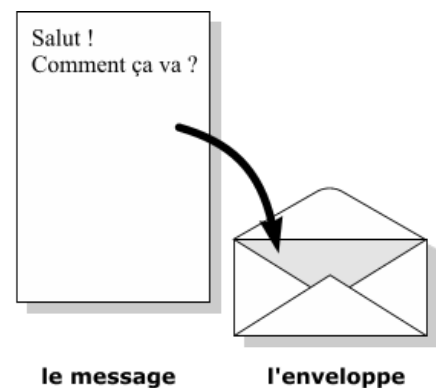
Quand vous voulez envoyer une lettre par la poste:

- vous placez votre lettre dans une **enveloppe**,
- sur le recto vous inscrivez l'**adresse du destinataire**,
- au dos, vous écrivez l'**adresse de l'expéditeur** (la votre).

Ce sont des règles utilisées par tout le monde. C'est un **protocole**.

Sur Internet, c'est à peu près la même chose: chaque message (chaque petit paquet de données) est enveloppé par IP qui y ajoute différentes informations:

- l'adresse de l'expéditeur (votre adresse IP),
- l'adresse IP du destinataire,
- différentes données supplémentaires (qui permettent de bien contrôler l'acheminement du message).



6.2. La couche IP comprend plusieurs protocoles :

IP		
ARP	RARP	ICMP

- ARP : « Address Resolution » Protocol
- RARP : « Reverse Address Resolution » Protocol
- ICM : « Internet Control Message » Protocol

Que l'on va voir plus tard sur le Modèle OSI

6.2.1. Scénario typique de l'utilisation d'ARP (couche 3)

- Un ordinateur connecté à un réseau informatique souhaite émettre une trame Ethernet à destination d'un autre ordinateur dont il connaît l'adresse IP.
- Il interroge son cache ARP à la recherche d'une entrée correspondant à l'adresse IP de la machine cible. Deux cas peuvent se présenter :



1. L'adresse IP est présente dans le cache de l'émetteur, il suffit de lire l'adresse MAC correspondante pour envoyer la trame ethernet. L'utilisation d'ARP s'arrête ici dans ce cas ;
2. L'adresse IP est absente du cache de l'émetteur. Dans ce cas, cet ordinateur va placer son émission en attente et effectuer une requête ARP en Broadcast. Cette requête est de type « quelle est l'adresse MAC correspondant à l'adresse IP ? Répondez à adresseMAC ».

- Puisqu'il s'agit d'un Broadcast tous les ordinateurs connectés au support physique vont recevoir la requête.
En observant son contenu, ils pourront déterminer quelle est l'adresse IP sur laquelle porte la recherche. La machine qui possède cette adresse IP, sera la seule (du moins si elle est la seule, ce qui est censé être le cas dans tout réseau, mais...) à répondre en envoyant à la machine émettrice une réponse ARP du type « je suis adresse IP, mon adresse MAC est adresse MAC ». Pour émettre cette réponse au bon ordinateur, il crée une entrée dans son cache ARP à partir des données contenues dans la requête ARP qu'il vient de recevoir.
- La machine à l'origine de la requête ARP reçoit la réponse, met à jour son cache ARP et peut donc envoyer le message qu'elle avait mis en attente jusqu'à l'ordinateur concerné. Il suffit donc d'un Broadcast et d'un Unicast pour créer une entrée dans le cache ARP de deux ordinateurs. Cette entrée est mémorisée 'un certain temps'. Ce temps dépend du système d'exploitation et du paramétrage réalisé.

L'adresse MAC Matériel sera vue en fin de chapitre

6.2.2. RARP (pour Reverse ARP) :

Permet à partir d'une adresse matériel (adresse MAC) de déterminer l'adresse IP d'une machine. En résumé, RARP fait l'inverse de ARP.....

6.2.3. ICMP (Internet Control Message Protocol -couche 3)

- Le protocole ICMP (Internet Control Message Protocol) permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs. Chaque pile IP, que ce soit des routeurs ou des stations de travail, gèrent ICMP par défaut.

Ce protocole est considéré comme faisant partie de l'ensemble des protocoles TCP/IP. Cependant, contrairement à TCP et UDP, il se situe en couche 3 et donc, il est encapsulé dans IP. Le mot "Encapsulation" relate clairement la confusion du placement d'ICMP dans les 7 couches OSI.

Couches OSI Que l'on va voir plus tard !!

Les messages d'erreur ICMP sont transportés sur le réseau sous forme de Datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreurs peuvent eux-mêmes être sujet aux erreurs. Toutefois, en cas d'erreur sur un message ICMP, aucune trame d'erreur n'est délivrée pour éviter un effet "boule de neige".

- rechercher des routeurs ;
- diagnostiquer les problèmes (**ping, tracert,**) ;
- régler le contrôle du flux pour éviter la saturation de la liaison ou du routeur.

L'**adresse IP** est une adresse **unique** attribuée à chaque ordinateur sur Internet (c'est-à-dire qu'il n'existe pas sur Internet deux ordinateurs ayant la même adresse IP).

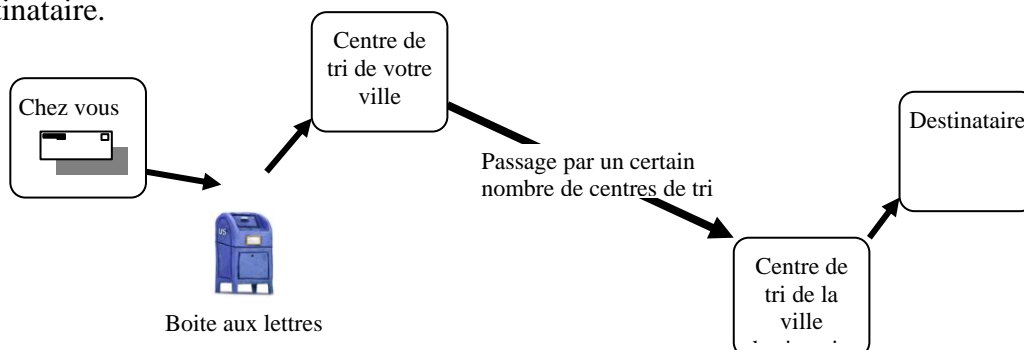
De même, l'adresse postale (nom, prénom, rue, numéro, code postal et ville) permet d'identifier de manière unique un destinataire.

Tout comme avec l'adresse postale, il faut connaître au préalable l'adresse IP de l'ordinateur avec lequel vous voulez communiquer.

L'adresse IP se présente le plus souvent sous forme de 4 nombres (entre 0 et 255) séparés par des points. Par exemple: 204.35.129.3

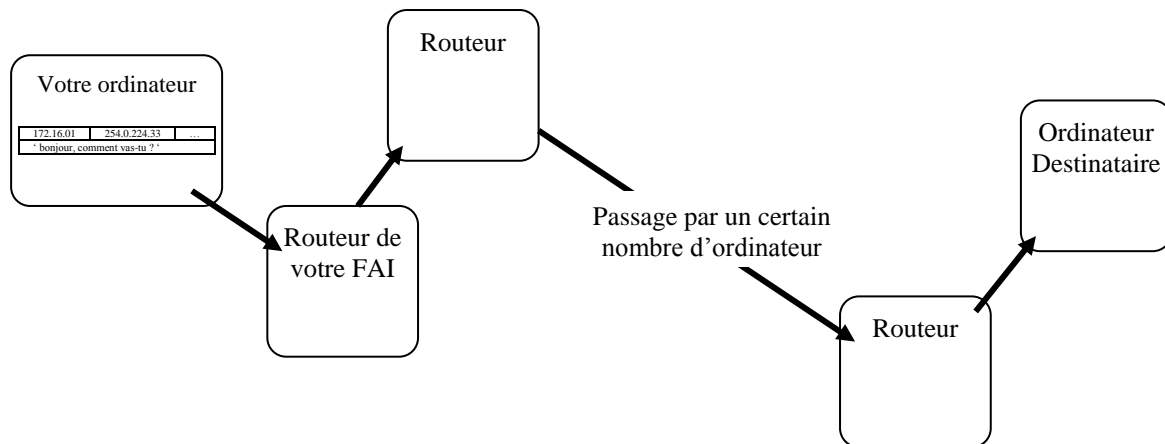
6.2.4. Le routage IP

Pour envoyer votre lettre, vous la postez dans la boîte-aux-lettres la plus proche. Ce courrier est relevé, envoyé au centre de tri de votre ville, puis transmis à d'autres centres de tri jusqu'à atteindre le destinataire.



C'est la même chose sur Internet !

Vous déposez le paquet IP sur l'ordinateur le plus proche (celui de votre fournisseur d'accès en général). Le paquet IP va transiter de routeur en routeur jusqu'à atteindre le destinataire.

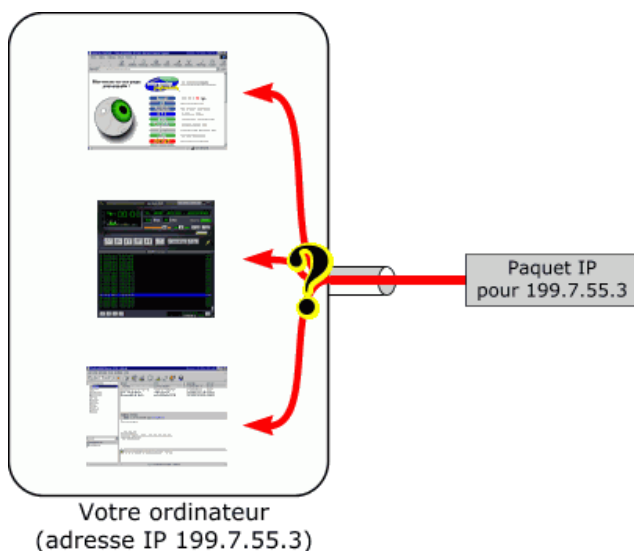


6.2.5. Les ports

Avec IP, nous avons de quoi envoyer et recevoir des paquets de données d'un ordinateur à l'autre.

Imaginons maintenant que nous ayons plusieurs programmes qui fonctionnent en même temps sur le même ordinateur : un navigateur, un logiciel d'email et un logiciel pour écouter la radio sur Internet.

Si l'ordinateur reçoit un paquet IP, comment savoir à quel logiciel donner ce paquet IP ?



Comment savoir à quel logiciel est destiné ce paquet IP ?

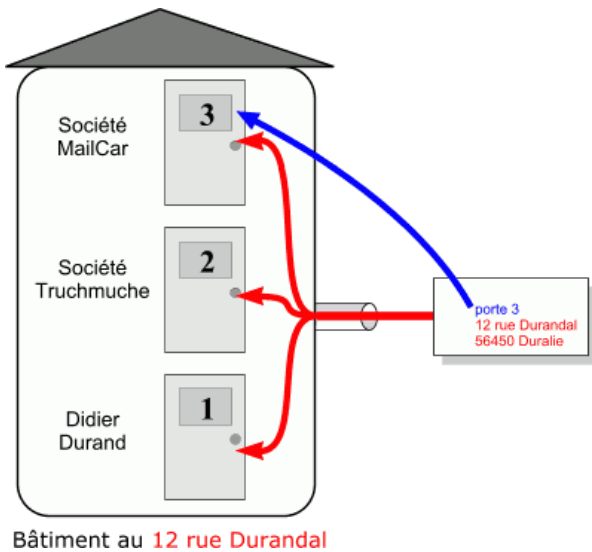
Le navigateur, le logiciel de radio ou le logiciel d'email ?

C'est un problème sérieux !

On pourrait attribuer un **numéro unique** à **chaque logiciel** dans l'ordinateur.

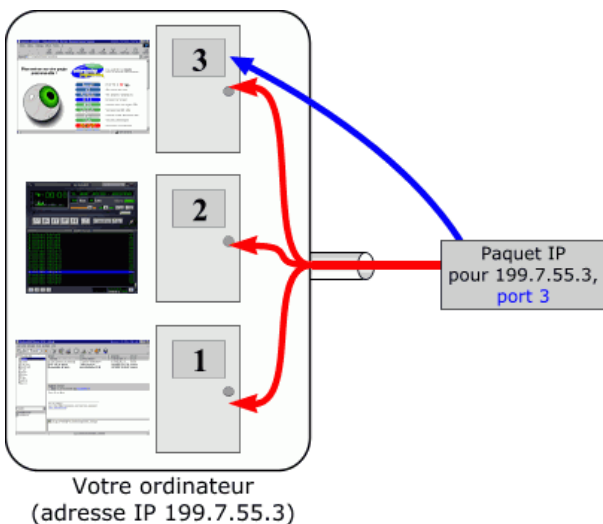
Il suffirait alors de mettre ce numéro dans chaque paquet IP pour pouvoir s'adresser à tel ou tel logiciel.

On appelle ces numéros des **ports** (pensez aux "portes" d'une maison : à une adresse donnée, on va pouvoir déposer les lettres à différentes portes à cette adresse).



Avec la poste, à une même adresse, on peut s'adresser à différentes personnes en indiquant un numéro de porte.

De même, à une même adresse IP, on peut s'adresser à différents logiciels en précisant le numéro de port (ici: 3).



Ainsi, l'adresse **IP** permet de s'adresser à un **ordinateur** donné, et le numéro de **port** permet de s'adresser à un **logiciel** particulier sur cet ordinateur.

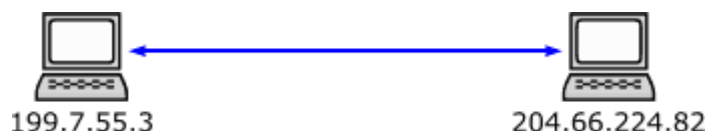
- POP3 : port 110
- HTTP : port 80
- FTP : port 21

- Les ports de type 'Well-known' : ports courants utilisés par les serveurs et gérés par iana.org.
- Les ports de type 'Registered ports' : The Registered Ports are not controlled by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users.

6.3. UDP (User Datagram Protocol)

- **UDP/IP** est un protocole qui permet justement d'utiliser des numéros de **ports** en plus des **adresses IP** (On l'appelle UDP/IP car il fonctionne au dessus d'IP).
- IP s'occupe des adresses IP et UDP s'occupe des ports.

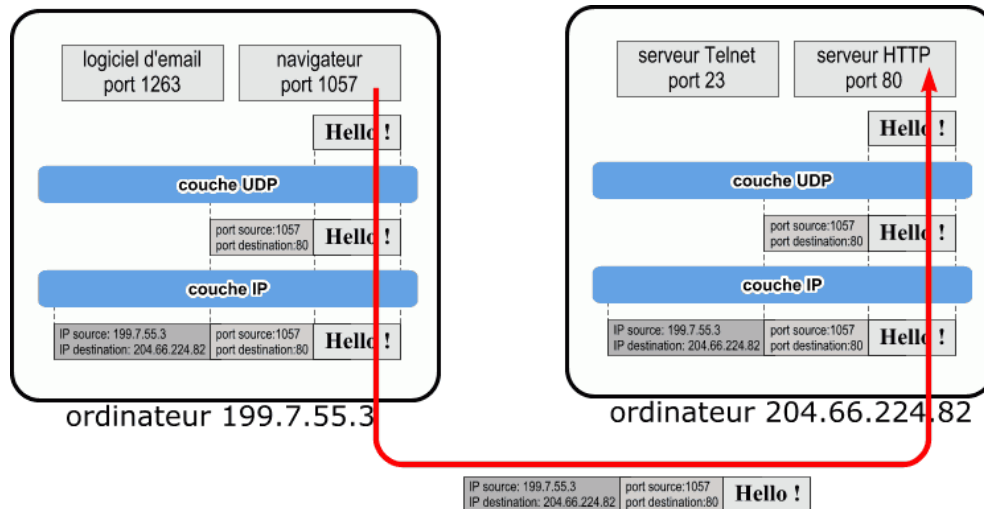
Avec le protocole **IP** on pouvait envoyer des données d'un ordinateur A à un ordinateur B.



Avec **UDP/IP**, on peut être plus précis :

On envoie des données d'une **application x** sur l'**ordinateur A** vers une **application y** sur l'**ordinateur B**.

Par exemple, votre navigateur peut envoyer un message à un serveur HTTP (un serveur Web):



- Chaque couche (UDP et IP) va ajouter ses informations. Les informations de **IP** vont permettre d'acheminer le paquet à destination du bon **ordinateur**. Une fois arrivé à l'ordinateur en question, la couche **UDP** va délivrer le paquet au bon **logiciel** (ici au serveur HTTP), mais il ne garantit pas l'exactitude des informations qu'il remet à la couche application, mais cela permet d'accélérer les échanges.
- L'émetteur ne reçoit aucune confirmation de réception.
- Les deux logiciels se contentent d'émettre et de recevoir des données ("Hello !"). Les couches UDP et IP en dessous s'occupent de tout.

Ce couple (199.7.55.3:1057, 204.66.224.82:80) est appelé un **socket**. Un socket identifie de façon unique une communication entre deux logiciels.

Parmi les usages les plus connus du mode sans connexion (UDP), notons:

- La résolution des noms ou la résolution inverse des adresses (DNS)
- La recherche d'une adresse IP dynamique (DHCP)
- La plupart des jeux en réseau.
- Le streaming (gros volumes d'informations tel que vidéo, chansons) où la perte d'information n'est pas dommageable.

6.4. TCP

Bon... on peut maintenant faire communiquer 2 logiciels situés sur des ordinateurs différents.

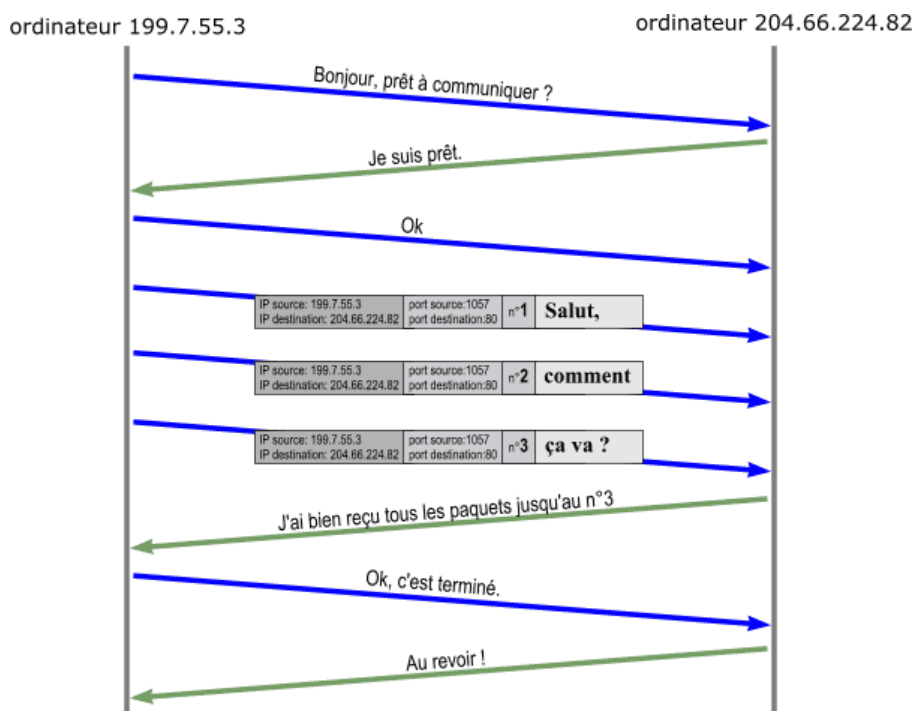
Mais il y a encore de petits problèmes:

- Quand vous envoyez un paquet IP sur Internet, il passe par des dizaines d'ordinateurs. Et il arrive que des paquets IP se **perdent** ou arrivent en **double exemplaire**.
Ça peut être gênant : imaginez un ordre de débit sur votre compte bancaire arrivant deux fois ou un ordre de crédit perdu !
- Même si le paquet arrive à destination, rien ne vous permet de savoir si le paquet est bien arrivé (aucun accusé de réception).
- **La taille des paquets IP est limitée** (environ 1500 octets).
Comment faire pour envoyer le fichier qui fait 62000 octets ? C'est pour cela qu'a été conçu TCP.

TCP est capable:

- de faire tout ce que UDP sait faire (ports).
- de vérifier que le destinataire est prêt à recevoir les données.
- de **découper** les gros paquets de données en paquets plus petits pour que IP les accepte
- de **numéroter** les paquets, et à la réception de **vérifier** qu'ils sont tous bien arrivés, de **redemander** les paquets manquants et de les **réassembler** avant de les donner aux logiciels. Des accusés de réception sont envoyés pour prévenir l'expéditeur que les données sont bien arrivées. Il garantit que toutes les données sont acheminées. Mais les échanges se voient ralentis.

Par exemple, pour envoyer le message "**Salut, comment ça va ?**", voilà ce que fait TCP (Chaque flèche représente 1 paquet IP):



A l'arrivée, sur l'ordinateur 204.66.224.82, la couche TCP reconstitue le message "**Salut, comment ça va ?**" à partir des 3 paquets IP reçus et le donne au logiciel qui est sur le port 80.



6.5. Les adresses TCP/IP :

Dans sa version 4 (codé sur 32 octets), **IP (Internet Protocol)** définit une adresse sur 4 octets. Une partie définit l'adresse, l'autre partie définit l'adresse de l'hôte dans le réseau.

La taille relative de chaque partie varie suivant la classe choisie (IP V6 codé sur 128 octets à venir)

6.5.1. Les classes d'adresses :

Il existe 3 classes d'adresses IP :

Classe A	Octet 4	Octet 3	Octet 2	Octet 1
Classe B	Octet 4	Octet 3	Octet 2	Octet 1
Classe C	Octet 4	Octet 3	Octet 2	Octet 1



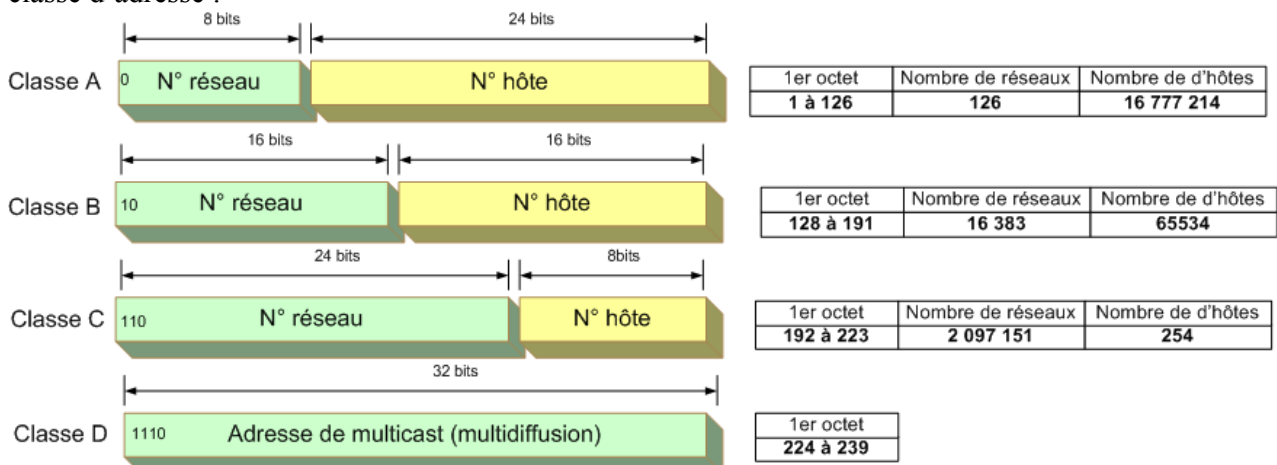
La classe A permet de créer peu de réseaux, mais avec beaucoup d'hôtes dans chaque réseau. La classe C faisant l'inverse.

Classe A	0	Réseau 7 bits		Hôtes 24 bits	
Classe B	1	0	Réseau 14 bits		Hôtes 16 bits
Classe C	1	1	0	Réseau 21 bits	Hôtes 8 bits

6.5.2. Etendue de chaque classe :

Classe	Première adresse	Dernière adresse
A	0.0.0.1	127.255.255.254
B	128.0.0.1	191.255.255.254
C	192.0.0.1	223.255.255.254

Ceci nous amène à faire quelques constatations sur le potentiel d'adresses et de réseaux détenu par chaque classe d'adresse :



Les classes d'adresses IP

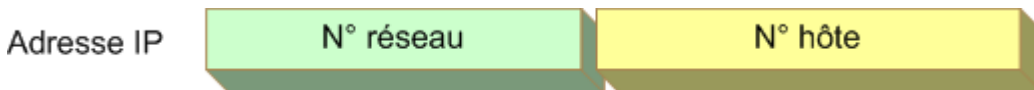
Il y a quelques adresses que l'on ne peut attribuer à un hôte :

- l'adresse d'hôte = 0 (exemple : 192.168.1.0 dans la classe C) est réservée à l'identification du réseau.
- l'adresse d'hôte avec tous ses bits à 1 (exemple : 192.168.1.255) cette adresse comprenant tous les hôtes du réseau 192.168.1.0. Par convention, cette adresse signifie que tous les hôtes du réseau 192.168.1.0 sont concernés (Adresse de broadcast IP).

Constitution d'une adresse IP

Constituée de 4 octets, elle est découpée en 2 parties :

- Le numéro de réseau (**netid**)
- Le numéro de l'hôte sur ce réseau (**hostid**)



Principe d'adressage IP

La taille du *netid* dépend de la **classe d'adresse IP** utilisée. Il existe plusieurs classes d'adresses IP dédiées à des usages différents. Plus le numéro de réseau est grand et plus le nombre d'hôtes sur ce réseau sera petit.

Exemples

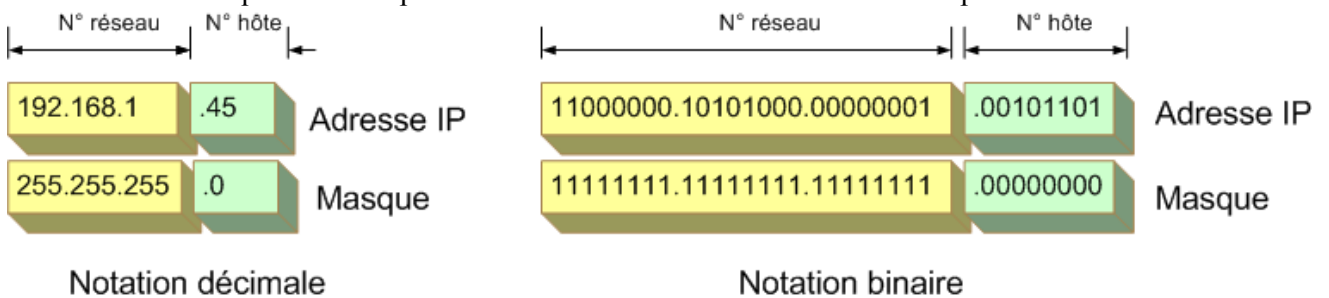
- 83.206.23.134 : Adresse de classe A , netid = 83 , hostid = 206.23.134
- 190.12.24.56 : Adresse de classe B , netid = 190.12 , hostid = 24.56
- 192.168.1.5 : Adresse de classe C, netid=192.168.1 , hostid=5

6.5.3. Le masque de sous réseau :

Le **masque de sous réseau** est un ensemble **de 4 octets destiné à isoler** :.....

- soit **l'adresse de réseau** en effectuant un ET logique bit à bit entre l'adresse IP et le masque
- soit **l'adresse de l'hôte** en effectuant en ET logique bit à bit entre l'adresse IP et le complément du masque.

Tous les bits à 1 du masque permettent de définir chaque bit correspondant de l'adresse IP comme un bit faisant partie du n° de réseau. Par opposition, tous les bits à 0 du masque permettent de définir chaque bit correspondant de l'adresse IP comme un bit faisant partie du n° d'hôte.



Le masque servant à faire la séparation en deux parties sur une adresse IP, il est donc indissociable de celle-ci. Une adresse seule ne **voudra rien dire puisqu'on ne saura pas quelle est la partie réseau et quelle est la partie machine.**

De la même façon, un masque seul n'aura pas de valeur puisqu'on n'aura pas d'adresse sur laquelle l'appliquer. L'adresse IP et le masque sont donc liés l'un à l'autre, même si l'on peut choisir l'un indépendamment de l'autre.

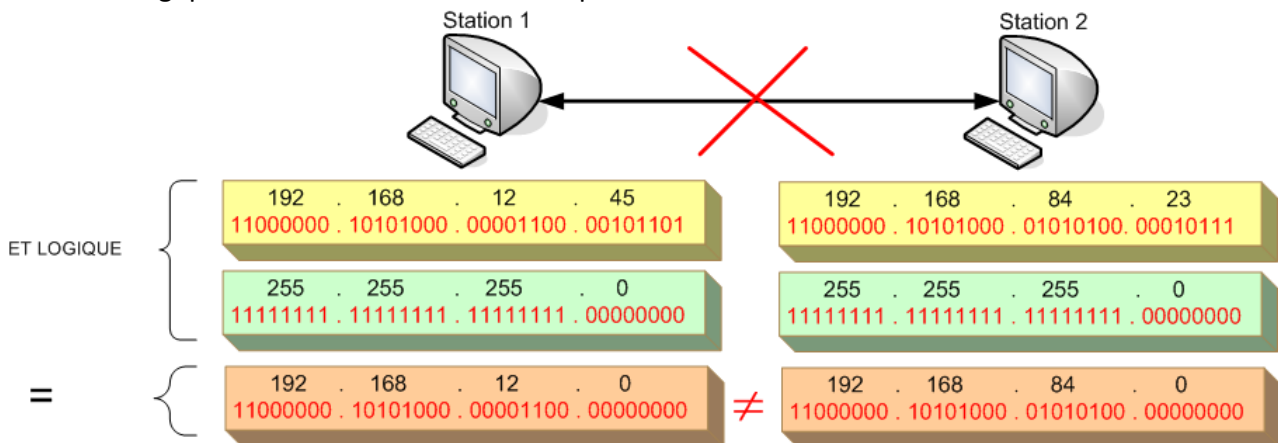
Les masques de sous réseau ont **par défaut** :

Classe	Masque par défaut	Nombre d'octets pour l'hôte
A	255.0.0.0	3
B	255.255.0.0	2
C	255.255.255.0	1

Application du masque

Pour que 2 stations puissent communiquer, la règle est la suivante :

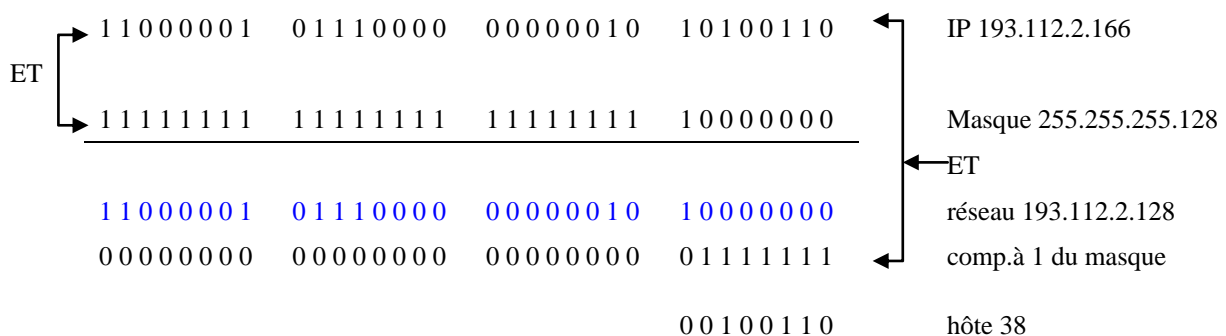
- Un ET logique entre l'adresse IP et le masque de sous réseaux doit donner le même résultat



Exemple d'application du masque

Exemples :

- L'adresse 193.112.2.166 avec le masque 255.255.255.128 désigne la machine numéro 38 du réseau 193.112.2.128 qui s'étend de 193.112.2.128 à 193.112.2.255 (plage de 128 adresses). Les adresses ont été converties en **base 2** :



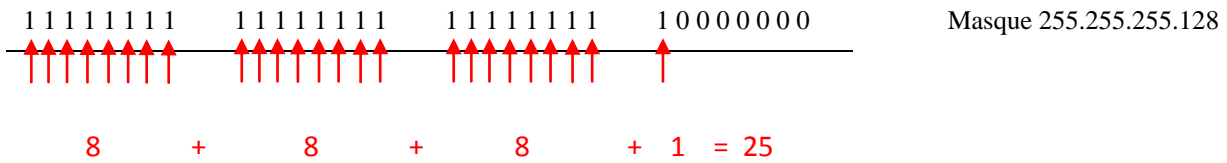
Représentation du masque avec un / (/25)

Il existe une autre manière de noter le masque.

Il s'agit de compter le nombre de bits à 1 du masque et de noter ce chiffre à la fin de l'adresse :

Par exemple, le couple adresse et masque suivant :

■ 193.112.2.166 : avec un masque de → ■ 255.255.255.128



S'écrira dans cette nouvelle notation :

■ 193.112.2.166 / 25

Le chiffre 25 indique que 25 bits du masque sont à 1.

Le modèle O.S.I.

7. Le modèle O.S.I

En 1978 certaines règles sont établies pour donner un standard à TCP/IP pour le développement de systèmes ouverts. La normalisation mise en place par l'ISO (International Standards Organisation) définit un modèle théorique à 7 couches :

le modèle OSI (.....**Open System Interconnection**.....) où chacune des couches est encapsulée dans la couche inférieure.

7.1. La couche physique 1

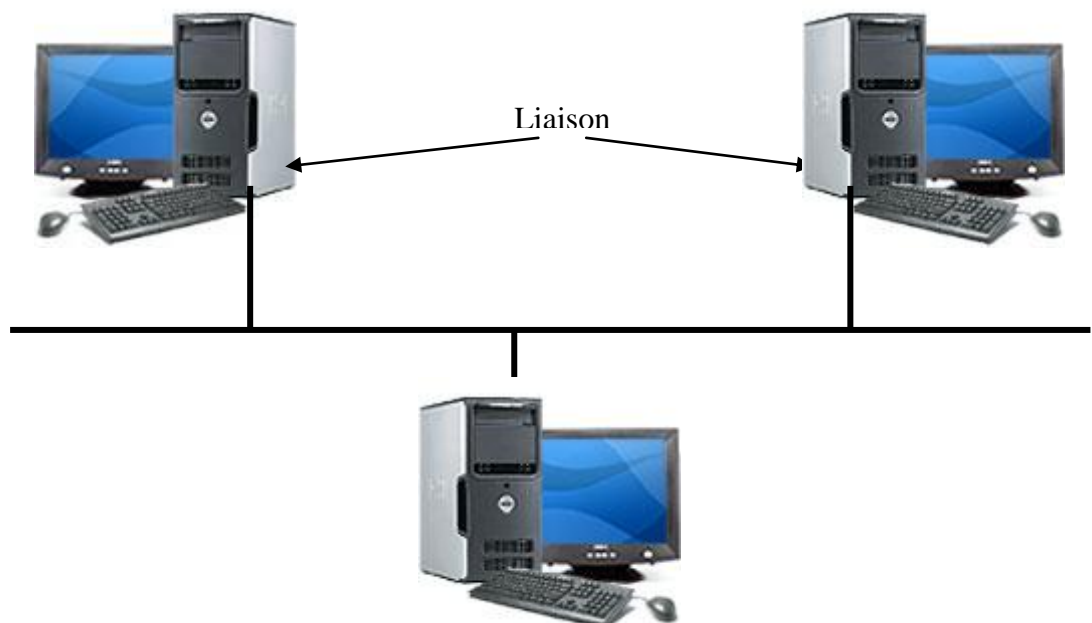
Transmet les bits à travers le canal de communication, elle utilise les interfaces mécaniques et électriques du média physique. La couche physique n'a aucune connaissance des données à émettre ou à recevoir. Elle reçoit des signaux et les convertit en bits de données pour les envoyer à la couche de liaison de données. Elle s'occupe de problème strictement matériel.

Le support physique définit :

- nature du câble.
- les caractéristiques électriques.
- la **vitesse de transmission**.
- le **codage des informations**.
- le connecteur.

7.2. La couche de liaison de données 2

Elle prend les données venant de la couche physique pour les regrouper en trame (voir Ethernet-p21). Elle est chargée de la transmission et de la détection d'erreurs en utilisant un checksum.



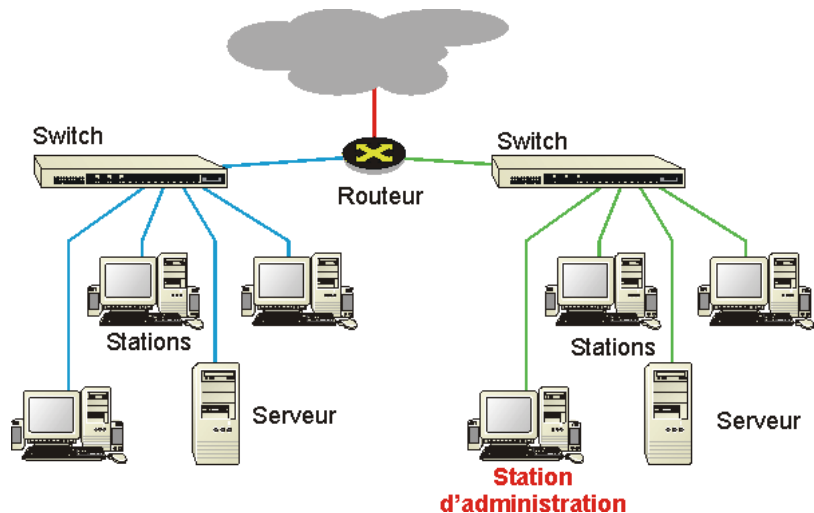
7.3. La couche réseau 3

La couche réseau gère les connexions entre les différents nœuds (appareils) du réseau. Elle sert à acheminer les données (trouver un chemin- routage) entre 2 machines qui ne sont pas sur le même support physique.

Elle sert aussi à réguler le trafic afin d'éviter les congestions de données.

Les couches réseaux les plus connues :

- IP (devenu un standard).....
- IPX (Netware)
- NetBeui (Microsoft)



7.4. La couche transport 4

La couche transport garantit que les données reçues sont celles qui ont été envoyées contrôle de bout en bout du réseau.

Elle permet aussi le multiplexage de plusieurs connexions logiques sur la partie physique.

Il n'est par exemple pas du ressort de la couche réseau de prendre des initiatives si une connexion est interrompue.

C'est la couche Transport qui va décider de réinitialiser la connexion et de reprendre le transfert des données.....

7.5. La couche session 5

La couche session synchronise la communication entre les appareils, elle permet des communications full-duplex ou half-duplex.

Une seule session peut ouvrir et fermer plusieurs connexions, de même que plusieurs sessions peuvent se succéder sur la même connexion. Comme cette explication n'est pas forcément claire pour tout le monde, essayons de prendre quelques exemples :

- Vous avez un message à transmettre par téléphone à un de vos amis, votre épouse doit faire de même avec celle de ce même ami.
Vous appelez votre ami (ouverture d'une connexion), vous discutez avec lui un certain temps (ouverture d'une session), puis vous lui dites que votre épouse voudrait parler à la sienne (fermeture de la session).
- Les épouses discutent un autre certain temps (ouverture d'une seconde session), puis n'ont plus rien à se dire (fermeture de la seconde session) et raccrochent (fin de la connexion). Dans cet exemple, deux sessions ont eu lieu sur la même connexion.

- Vous avez un travail à réaliser avec un collègue, par téléphone. Vous l'appellez (ouverture de la connexion et ouverture de la session). Il vous demande des informations qui nécessitent de votre part une recherche un peu longue, vous raccrochez après lui avoir dit que vous le rappellerez ultérieurement (fermeture de la connexion, mais pas de la session). Votre recherche effectuée, vous rappelez votre collègue (ouverture d'une seconde connexion pour la même session), vous lui transmettez les informations demandées, vous n'avez plus rien à vous dire (fermeture de la session), vous raccrochez (fermeture de la connexion).
 Dans cet exemple une session s'étend sur deux connexions.

7.6. La couche présentation 6

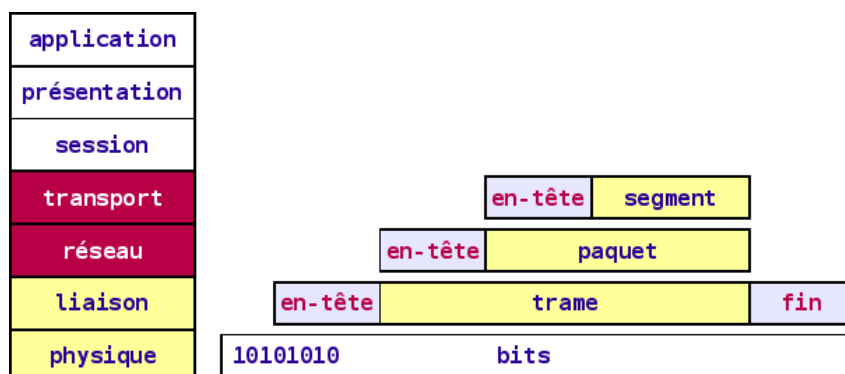
Pour que 2 systèmes se comprennent ils doivent utiliser la même représentation de données, c'est le rôle de cette couche.
 Ex : Codage ASCII

7.7. La couche application 7

Interfaces utilisateurs, nécessaire aux applications qui accomplissent des tâches de communications. Cette couche propose également des services :
 Principalement des services de **transfert de fichiers, (FTP), de messagerie (SMTP) de documentation hypertexte (HTTP) etc**.....
 Ex : logiciel de supervision

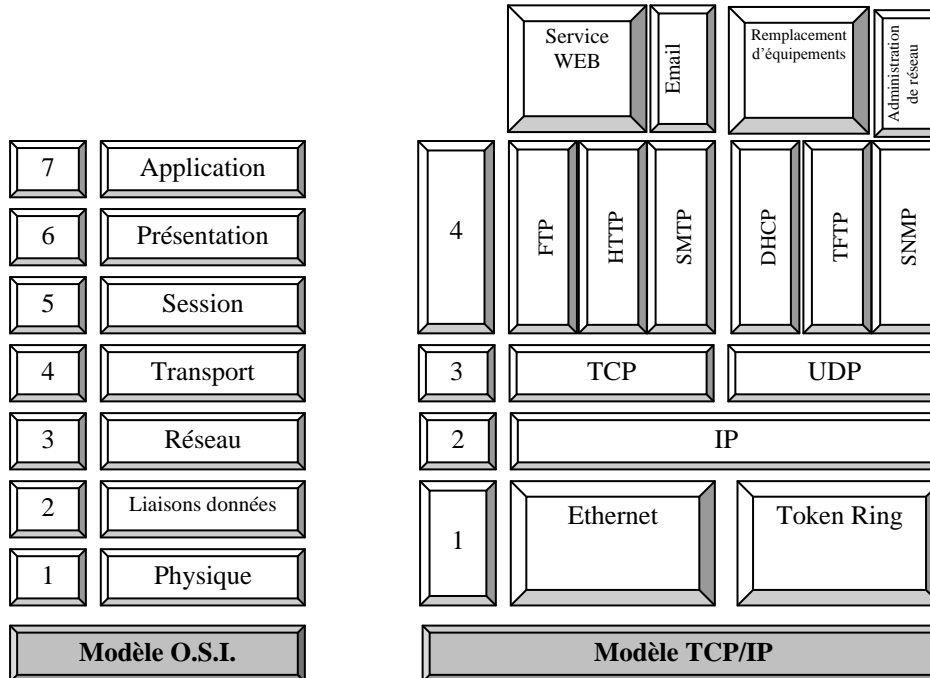
7.8. L'encapsulation

Au passage d'une couche N vers la couche inférieure (N-1), le flot de données est enrichi de champs supplémentaires placés en début et/ou en fin. Dans le premier cas, il s'agit d'un en-tête ou préfixe (*header*) ; dans le second, d'un suffixe (*trailer*). Ces informations apportées renseignent la trame au niveau de la couche qui les a émises (ici N). Ces champs servent donc, lors de la réception par la couche de même niveau (N) de la station destinataire, au traitement que celle-ci doit effectuer. On peut y trouver les adresses source et destination (de niveau N), un contrôle de parité, la longueur concernant le paquet, des bits de priorité, l'identification du protocole de niveau supérieur (N+1) pour le décodage, des numéros d'acquittement, etc.



8. Le modèle OSI et TCP/IP

Bien qu'Ethernet et TCP/IP se conforment au modèle ISO 7 il y a une certaine différence.



Couches 1 à 4 : couches basses chargées d'assurer un transport optimal des données.....

Couche 5 à 7 : couches hautes chargées du traitement des données (représentation, cryptage...)

8.1. En résumé :

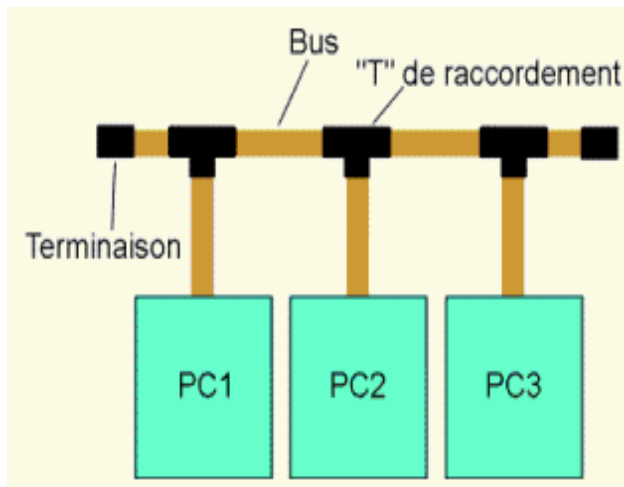
No TCP/IP	Nom TCP/IP	No OSI	Nom	Résumé	Mots clés	PDU	Protocoles,etc.	Equipements et termes associés
4	Application	7	Application	processus réseau vers les applications	Processus réseau aux applications (services de fichiers, d'impression, de messagerie, de base de données et d'application, par exemple). Détermine la disponibilité des ressources entre deux noeuds. (FTP et Telnet, par exemple).	Données	DNS, TFTP, Rlogin, Telnet, FTP (File Transfert Protocol), TFTP (Trivial File Transfer Protocol) SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), HTTP (HyperText Transfer Protocol), BOOTP (Bootstrap Protocol), DHCP (Dynamic Host Configuration Protocol)	Données, logiciels, passerelles
4	Application	6	Présentation	représentation des données	Représentation des données, codage (EBCDIC, ASCII), services de transfert de syntaxe, services de conversion, services de chiffrement, services de cryptage et services de compression.	Données	ASCII, EBCDIC, MIDI, MPEG, PICT, TIFF, JPEG	Codage des données, logiciels, cryptage, compression, logiciels de redirection
4	Application	5	Session	communication interhôte	Communications interhôtes. Etablit, gère et ferme les connexions entre les applications.	Données	Le système NFS (Network File System), Le langage d'interrogation structuré (SQL), L'appel de procédure distant (RPC), Le système X-Window, Le protocole ASP (AppleTalk Session Protocol), Le protocole de contrôle de session DNA (SCP)	Données, logiciels, client-serveur

3	Transport	4	Transport	connexions de bout en bout	Connexions de bout en bout. Segmentation et réassemblage des données dans l'ordre approprié. Etablissement et fermeture de "circuits virtuels" (orientés connexion). Peut assurer la livraison des segments avec la correction d'erreurs, la reprise sur	Segments	TCP ou UDP	Routeur, numéros de port, contrôle de flux, fenêtrage, orienté connexion, non orienté connexion
2	Inter réseau	3	Réseau	adresse et meilleur chemin	Adresses réseau/hôte et sélection du meilleur trajet sur un inter réseau (routage). Encapsule les informations de la couche supérieure sous forme de "paquets".	Paquets, datagrammes	IP, IPX, ICMP, ARP, RARP, Ping, Traceroute	Routeur, commutateur de couche 3, paquet, adressage IP de datagrammes, sous-réseaux, détermination du chemin, protocoles routés (IP, IPX) et protocoles de routage (RIP, IGRP)
1	Réseau	2	Liaison de données	accès au média	Accès au média. Ajoute un en-tête de trame aux informations de la couche supérieure. Cet en-tête contient l'adresse matérielle de l'unité de destination ou de l'unité suivante sur le chemin. La couche liaison de données se divise en deux sous-couches : 1) La sous-couche LLC (Logical Link Control) et 2) la sous-couche MAC (Media Access Control).	Trames	IEEE 802.2, 802.3, 802.5, PPP, HDLC	Ethernet, carte réseau (contrôle de lien logique et adresse MAC), pont, commutateur, trame, protocoles de liaison WAN (HDLC, etc.)
1	Réseau	1	Physique	transmission binaire	Signaux et codage de transmission binaire. Connexions électriques (fil de cuivre), par source de lumière (fibre) et physique, et médias (câblage) entre les unités réseau.	Bits	IEEE 802.3, 802.5	Ethernet, carte réseau (connecteurs physiques - BNC, AUI, RJ-45, etc.), médias (câble coaxial, câble à paires torsadées non blindées, fibre optique), répéteur, concentrateur, ETCD et ETTD, bits, codage

Les topologies Et Architectures

9. Les topologies

9.1. Le BUS



Le principe du "BUS" est extrêmement simple:

- Un conducteur unique représente le réseau.
- Chaque extrémité est bouclée sur un "bouchon" dont l'impédance électrique est égale à l'impédance caractéristique du conducteur, ceci afin d'éviter les réflexions des signaux en bout de câble.
- Chaque poste est "piqué" sur ce bus au moyen d'un "T" de raccordement.

Cette technologie est adaptée aux petits réseaux.

9.1.1. Avantages

Il n'y a qu'un seul avantage à utiliser cette technologie, mais il est de taille :

- Après avoir vu les divers constituants, il devient évident que ce procédé est peu coûteux, facile et rapide à mettre en œuvre.

9.1.3. Conclusions

Malheureusement, ce type de réseau est limité à 10 Mbits/s et ne fait plus partie des offres, bien qu'encore suffisant pour un réseau domestique.

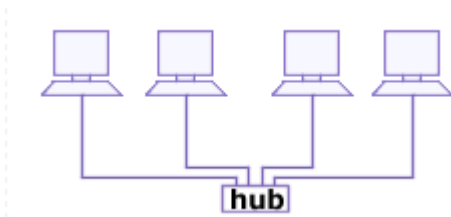
9.1.2. Inconvénients

Ils sont hélas nombreux :

- Si un défaut de connectique apparaît, c'est tout le réseau qui devient inopérant. En effet, tout se passe alors comme si l'on avait deux réseaux, mais chacun d'eux ayant une extrémité non adaptée. Plus rien ne fonctionne et le défaut n'est pas toujours visible. Les investigations sont longues et laborieuses.

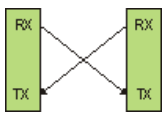
9.2. L'étoile

• Principe

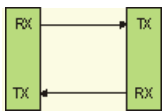


Chaque PC est relié par un câble constitué de 4 paires torsadées (dont deux seulement servent, l'une pour l'émission et l'autre pour la réception) à un concentrateur, encore appelé "HUB" ou à un commutateur encore appelé "SWITCH".

Sur de la paire torsadée, chaque paire est unidirectionnelle.



Deux équipements connectés doivent faire correspondre le TX (Emission) de l'un au RX (Réception) de l'autre. Normalement, il faudrait donc des câbles croisés.



C'est ce qui est nécessaire si l'on souhaite relier directement deux PC entre eux. Mais si l'un des équipements a sa prise déjà croisée, alors, il faut un câble droit.

Les SWITCHES ou les HUBS ont leurs prises croisées, c'est pour cela qu'il y a un X marqué sur ses prises. Il faut donc un câble droit pour connecter un PC à un SWITCH.

Notez que les équipements récents (HUBS et SWITCH) sont capables de détecter automatiquement les signaux d'entrée et de sortie présents sur la prise et réagissent en conséquence. Autrement dit, l'équipement découvrira automatiquement s'il est nécessaire de croiser ou non sa propre prise.

9.2.1. Avantages

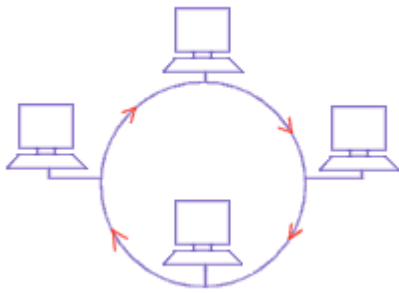
- D'un fonctionnement beaucoup plus sûr que le bus, si un lien vient à se rompre, seul le PC connecté par ce lien est absent du réseau.
- Il est aisé d'ajouter des postes au réseau, même s'ils sont dans une pièce.
- Cette technologie permet de réaliser un réseau 100 Mbits/s.

9.2.2. Inconvénients

- La longueur totale de câble mise en œuvre est importante.
- Au voisinage du SWITCH, on obtient un faisceau de câbles imposant.
- Le coût est tout de même plus élevé que dans une architecture BUS.
- Si le concentrateur tombe en panne, le réseau ne fonctionne plus.

La méthode d'accès au support s'appelle Ethernet, voir Chapitre Ethernet.

9.3. Les réseaux en anneau



Les réseaux en anneau sont constitués d'un seul câble qui forme une boucle logique.

Les réseaux en anneau sont des réseaux déterministes. Le droit de parler sur le réseau est matérialisé par un jeton qui passe de poste en poste. Chaque poste reçoit le jeton chacun son tour, et chaque station ne peut conserver le jeton qu'un certain temps, ainsi le temps de communication est équilibré entre toutes les stations. Le trafic est ainsi très réglementé, il n'y a pas de collisions de « paquets ».

Pour simplifier : le signal électrique circule seul sur le câble, depuis la station émettrice jusqu'à la station réceptrice, et cette dernière renvoie un accusé de réception.

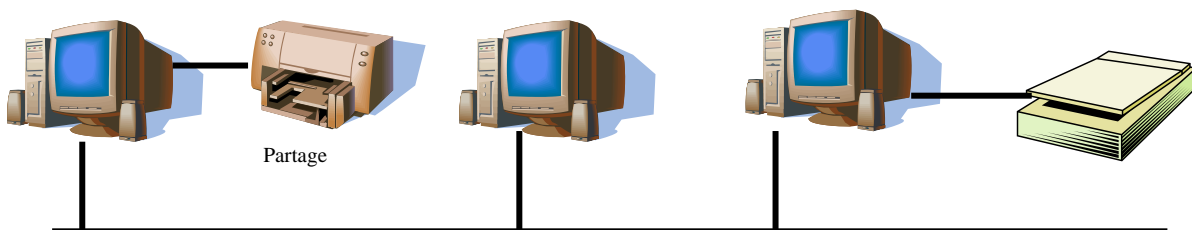
La méthode d'accès au réseau s'appelle le passage du jeton. La topologie en anneau est dite « topologie active » parce que le signal électrique est intercepté et régénéré par chaque machine. Il existe un mécanisme qui permet de contourner une station qui est tombée en panne, c'est le « by-pass ». Quand une station n'a pas reçu le jeton au bout d'un certain temps, une procédure permet d'en créer un autre.

10. Architecture des réseaux

10.1. Poste à poste

Une solution "simple" consiste à exploiter les fonctions de réseau poste à poste intégrées aux systèmes d'exploitation les plus courants (par exemple Window....). Dans ce type d'architecture, il n'y a pas de serveur dédié. Tout poste qui fournit un service à un autre devient serveur.

Exemple : Sur le disque dur de chaque machine est créé un ou plusieurs "dossiers partagés" accessibles à tout moment par les autres.



10.2. Client serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des **machines clientes** (des machines faisant partie du réseau) contactent un **serveur**, une machine parfois très puissante en termes de capacités d'entrée-sortie, qui leur fournit des **services**. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion vers internet, ...

Les services sont exploités par des programmes, appelés **programmes clients**, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client de messagerie, ..., lorsque l'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).

10.2.1. Avantages de l'architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont:

- **des ressources centralisées:** étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.
- **une meilleure sécurité:** car le nombre de points d'entrée permettant l'accès aux données est moins important.
- **une administration au niveau serveur:** les postes clients ayant techniquement peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.
- **un réseau évolutif:** grâce à cette architecture il est possible de supprimer ou rajouter des postes clients ou des postes serveurs sans perturber le fonctionnement du réseau et sans modifications majeures.

10.2.2. Inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques inconvénients parmi lesquelles :

- **un coût un peu plus élevé** dû à la technicité du serveur
- **un maillon faible:** le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui. Sur des réseaux évolués on trouve des routeurs, des serveurs, des Switches en redondance afin d'assurer la continuité de service. Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID : permet d'assurer la sauvegarde d'informations sur différents disques physiques).

11. Les systèmes serveurs

Il est possible de distinguer 4 systèmes serveurs parmi les plus utilisés :

- UNIX
- NETWARE (Novell)
- WINDOWS server
- LINUX

11.1. Basés sur trois protocoles :

- **NetBEUI**

Développé par Microsoft et IBM à l'époque des premiers réseaux de PC, ce protocole simplissime fonctionne très bien sur de petits réseaux. Malheureusement, son efficacité décroît avec le nombre de postes. De plus, il n'est pas "routable", ce qui fait que l'on ne peut interconnecter des réseaux NetBEUI autrement que par des ponts.

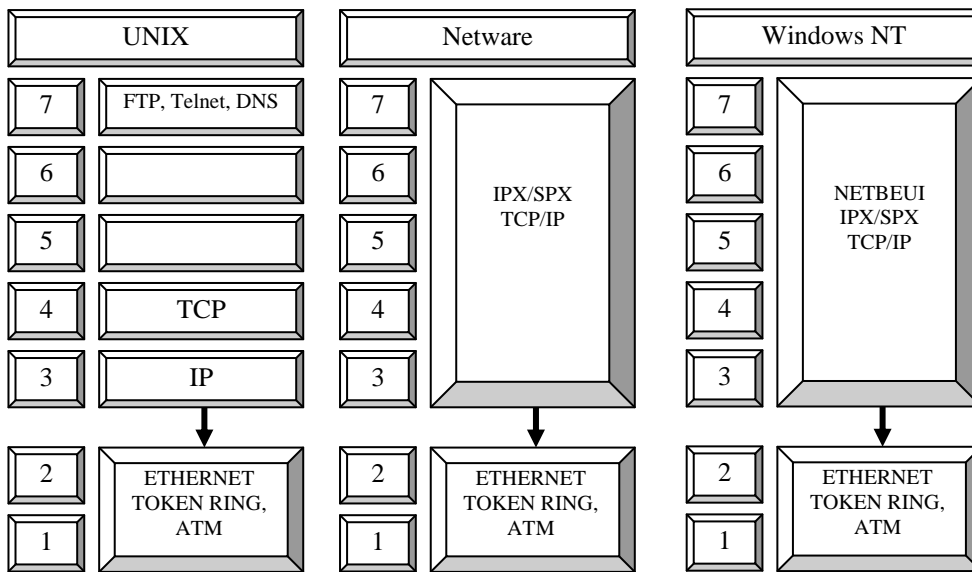
• **IPX/SPX**

Développé par la société NOVELL, qui s'est octroyée la part du lion dans les premiers réseaux de PC avant que Microsoft ne développe Windows NT. Plus efficace que NetBEUI pour les gros réseaux, ce protocole est de plus routable ce qui augmente les possibilités d'interconnexions. Avec un inconvénient : la bande passante est diminuée à cause des nombreux 'Broadcaste'.

• **TCP/IP**

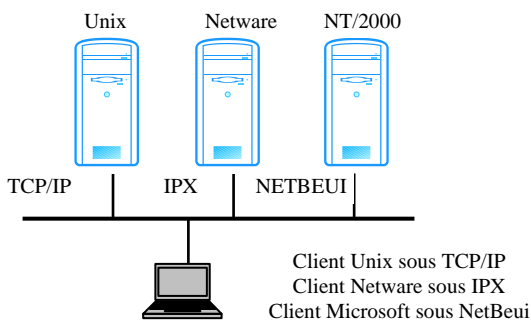
Développé dans le monde UNIX, ce protocole est de très loin le plus compliqué. Cependant, il a été conçu au départ pour l'interconnexion de réseaux (IP=Internet Protocol).

C'est le protocole le meilleur pour les gros réseaux et il est incontournable pour l'usage d'Internet. C'est LE standard actuel.



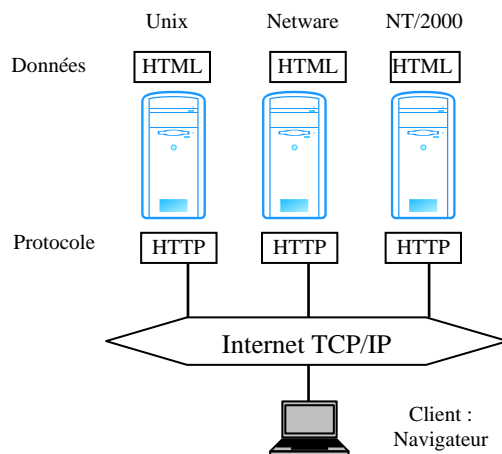
Les couches 1 et 2 sont réalisées par la carte réseau et le driver.

11.2. Communication client / serveur



11.3. Exemple de Communication Internet

Consultation de page WEB



Ethernet

12. ETHERNET

12.1. Historique

Technologie développée par Xéros pour interconnecter des machines bureautiques (1970) :

- Débit 3Mb/s avec câble coaxial
- Protocole d'accès proche du CSMA/CD actuel

Début des années 80 : DEC, Intel, Xéros mettent place Ethernet V2.0
Comité IEEE établit la norme IEEE 802.3

- 1985 : IEEE 802.3 → Ethernet 10 base 5 ('thick').
- 1988 : IEEE 802.3a → Ethernet 10 base 2 ('thin').
- 1990 : IEEE 802.3i → Ethernet 10 base T ('arrivée du Hub').
- 1994 : IEEE 802.3u → Ethernet 100 base T
 - ✓ 100 base TX (2 paires UTO 5, arrivée du Switch)
 - ✓ 100 base T4 (4 paires UTP 3/4/5)
- 1996 : IEEE 802.3z → Gigabit Ethernet
- 2001 : IEEE 802.3ae → 10 Gb/s

Remarque : Ethernet ne gère que les couches 1 (physique) et 2 (liaison) du modèle O.S.I.

12.2. Le support physique

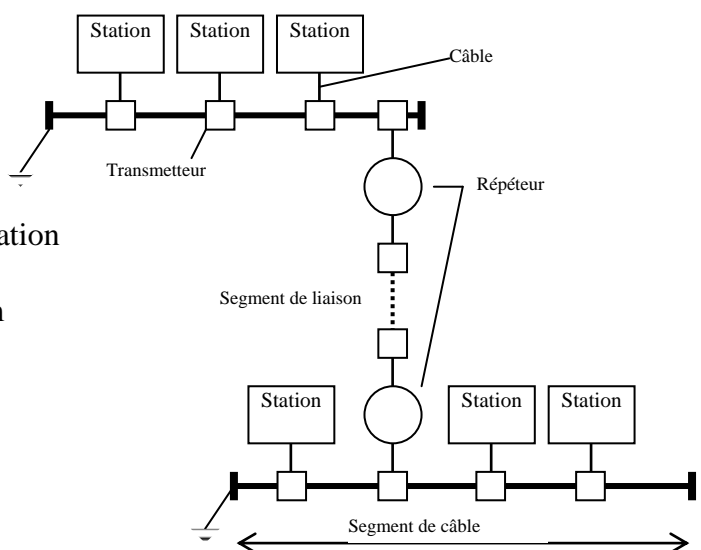
12.2.1. Ethernet 10 base 5

Topologie en Bus.

- Segment de câble
 - 500 m maximum adapté aux deux bouts (3 maxi)
- Nombre de connexion sur un segment
 - 100
 - 2.5 m entre deux connexions
- Segment de liaison (2 maxi)
 - 500 m maxi
- Câble coaxial
 - 50 m entre le transmetteur et la station
- Transmetteur
 - placé sur les repères tous les 2.5m

Chemin maximum entre deux stations

- 3 segment de câble : $500 \times 3 = 1500$ m
- 2 segment de liaison : $500 \times 2 = 1000$ m
- 4 répéteurs
- 2 transmetteurs et 2 câbles (AUI)
- longueur d'un réseau standard : 2.5 km.



12.2.2. Ethernet 10 base 2

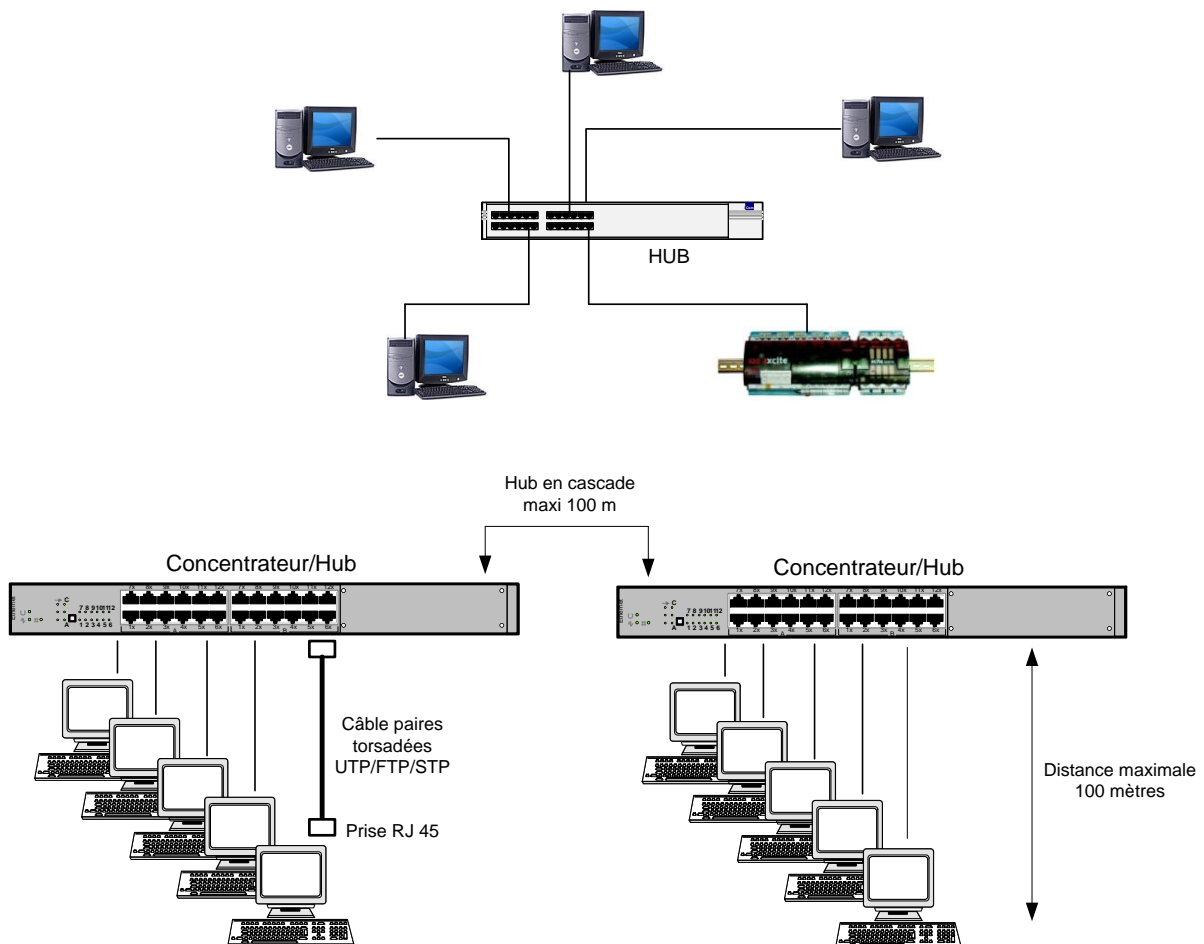
Câble avec BNC (mâle et femelle) et Topologie en Bus.

- 3 segment de câble : $185 \times 3 = 555$ m
- 2 segment de liaison : $185 \times 2 = 370$ m
- 4 répéteurs
- longueur d'un réseau standard : 925m.
- 30 stations par segment
- 0.5 m entre station.

12.2.3. Réseau 10 Base T :

Utilise une topologie en *Etoile*

En 1990, le comité IEEE a publié la spécification 802.3 relative à la mise en œuvre d'Ethernet avec des câbles à paires torsadées, le *10 Base T* (10Mb/s sur paire torsadée).



Longueur maximale d'un câble de liaison : 100m

Longueur minimale d'un câble de liaison : 50cm à 1m

Distance maximale entre 2 stations (nœuds) : 500m

Paires torsadées : voir dossier sur le câblage.

13. Méthode d'accès au support

13.1. Deux problèmes à résoudre

C'est le procédé le plus employé dans les réseaux actuels. Il s'agit du système ETHERNET (à ne pas confondre avec INTERNET). Ici, un poste qui doit émettre commence par écouter le réseau. Si personne n'est en train de parler, il émet une trame de données. Comme chaque poste s'assure qu'il y a le silence avant de prendre la parole, les choses se passent en général bien.

Cependant, lorsqu'il y a beaucoup de postes, il peut se faire que deux postes décident d'émettre en même temps; il y a alors une collision entre les deux trames émises et les données deviennent inutilisables. ETHERNET utilise donc un système de détection de collision, chaque poste écoute également ce qu'il émet. Dans un tel cas, chaque poste attendra un temps aléatoire et refera une tentative.

C'est bien de disposer d'un ensemble de postes connectés entre eux, encore faut-il établir des protocoles pour transmettre les données avec quelques espoirs d'efficacité. Des protocoles, nous allons en voir quelques uns et à tous les étages. Mais commençons par le niveau le plus bas, sur le câble lui-même.

13.2. Parler et se faire entendre...

Contrairement à la téléphonie qui met en œuvre une liaison "point à point", il n'y a en général que deux interlocuteurs en ligne, un réseau informatique met toutes les machines connectées sur la même ligne. Il faut donc trouver un moyen pour que celui qui parle soit entendu. Il y a plusieurs méthodes pour organiser une telle assemblée, nous allons en voir trois :

13.3. La liberté dans l'auto discipline (Ethernet)

13.3.1. Avantages

Lorsqu'il y a peu de trafic sur le réseau, il n'y a pas de perte de temps et les communications sont très rapides.

Les médias mis en œuvre sont simples (paires torsadées ou coaxial) **et peu onéreux, de même que la connectique.**

13.3.2. Inconvénients

Lorsque le taux de collision devient important, le réseau perd beaucoup de temps à transporter des informations inutilisables et le rendement diminue, la bande passante étant alors consommée par les collisions.

Une autre caractéristique peut devenir un inconvénient:

Il est impossible de déterminer le temps qu'il faudra pour être sûr qu'un poste a pu parler à un autre, ce temps pouvant **être très court s'il y a peu de trafic ou beaucoup plus long s'il y a beaucoup de collisions**

13.4. L'organisation déterminée (Token Ring)

C'est le protocole "Token Ring" (Anneau à jeton).

Pour parler, il faut avoir le jeton. Le réseau est constitué comme un anneau sur lequel un contrôleur passe un jeton à chaque hôte connecté, à tour de rôle. Ne peut émettre que celui qui dispose du jeton. C'est Protocole de type multi maître. C'est-à-dire que plusieurs équipements raccordés sur le réseau peuvent simultanément lire / écrire dans les autres équipements.

13.4.1. Avantages

Dans un tel système, il ne peut pas y avoir de collisions, c'est l'ordre parfait.

Il est parfaitement possible, si l'on connaît le nombre de postes sur le réseau, de connaître le temps maximum qu'il faudra pour qu'un poste puisse parler à un autre. (intéressant dans la gestion d'événements "en temps réel").

13.4.2. Inconvénients

Il est difficile de construire une vraie boucle! En fait, le retour se fait dans le même câble. La connectique est donc plus complexe et onéreuse.

13.5. Enfin, une solution chère mais efficace (ATM)

Le réseau ATM, mis au point par les opérateurs de télécommunications, est un procédé complexe et coûteux, mais qui garantit un fonctionnement fluide et une bande passante déterminée pour chaque poste du réseau; conditions indispensables pour effectuer de la téléphonie ou de la télévision, phénomènes en temps réel s'il en est !

Ces réseaux fonctionnent comme des réseaux commutés. Un chemin virtuel est établi entre les deux postes qui veulent échanger des données.

13.6. Accès aléatoire Ethernet

13.6.1. Protocole d'accès au média CSMA/CD

Carrier Sense	→	Ecoute de porteuse
Multiple Access	→	Accès multiple, pas de priorité
Collision Détection	→	Détection Collision

13.6.2. Principe du CSMA/CD

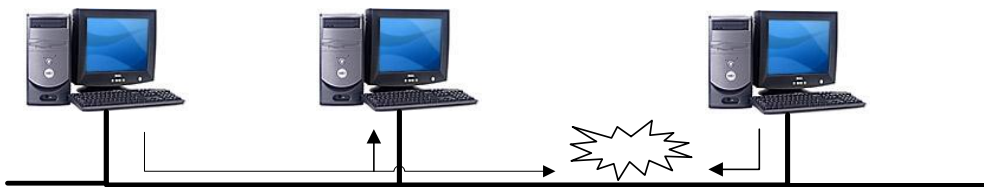
Principe d'émission d'une trame par une station :

1 – Ecoute du média

Si détection de porteuse (une autre station émet)
Alors attente d'un temps aléatoire avant reprise d'écoute.
Sinon émission d'une trame.

2 – Pendant l'émission

Ecoute du média pour vérifier qu'aucune autre station n'émet.
Si tel est le cas → collision



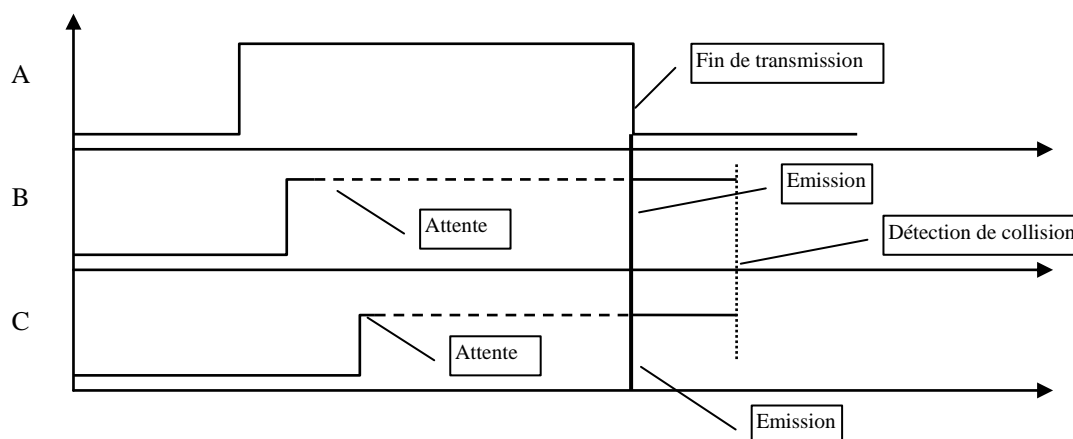
3 – Après l'émission

Attente de $9.6 \mu s$ avant la trame suivante. Ce délai est appelé Interframe Gap.

- **Les collisions**

Si une collision est détectée
Alors les stations émettrices génèrent un signal de brouillage (jam signal) suffisamment long pour prévenir toutes les stations de la collision.

Chaque station attend alors un temps pseudo aléatoire avant de réémettre sa trame.



13.6.3. Vitesse de propagation, temps d'aller-retour

La vitesse de propagation du signal électrique est de l'ordre de 0,77 C (C = vitesse de la lumière dans le vide) $0,77 \times 3 \times 10^8$ m/s 230 000 km/s

A 10Mbits/s un bit occupe le signal électrique pendant $1/(10 \times 10^6)$ s soit 0,1 μ s c'est ce qu'on appelle la durée d'un bit (Bit Time) ou BT.

Comme le signal se déplace à 230 000 km/s, un bit occupe donc $2,3 \times 10^8 \times 10^{-7} = 23$ m sur le câble.

Sur un câble de 500m on peut "mettre" $500/23 = 22$ bits, à un instant donné, qui occuperont le câble pendant $22/(10 \times 10^6) = 2,2$ us.

La norme Ethernet fixe le temps d'aller retour (round trip delay) entre deux émetteurs récepteurs les plus éloignés à 46,4us (464 BT), ce qui permet au signal un aller retour: $230 \times 10^6 \times 46,4 \times 10^{-6} = 10672$ m, soit un réseau de 5336 m sur un seul câble coaxial. Pour des raisons d'atténuation le signal doit être régénéré tous les 500 m, en effet la détection de collisions nécessite la différenciation d'un signal de la superposition de 2 signaux (la superposition de 2 signaux affaiblis pourrait avoir la même énergie qu'un signal non affaibli). Pour régénérer le signal on utilise des répéteurs qui induisent un retard, compte tenu de cela (et des performances des circuits électronique en 1980) la taille maximale d'un réseau Ethernet a été fixée à 2800 m au lieu de 5336 m.

Elle fixe également la durée du signal de brouillage (JAM) à une valeur comprise entre 3,2 et 4,8 us (32 à 48 BT)

La norme Ethernet fixe le slot time (tranche canal) à 51,2 μ s (46,4 + 4,8)

La taille maximum d'un paquet est fixée à 1518 caractères pour ne pas pénaliser les temps d'accès et limiter les mémoires tampons des émetteurs-récepteurs.

Pour être sûr de détecter les collisions il faut que les messages émis à 10 Mbits/s aient au moins une longueur de 10×10^6 bit/s $\times 51,2 \times 10^{-6}$ s = 512 bits soit 64 octets (préambule exclu)

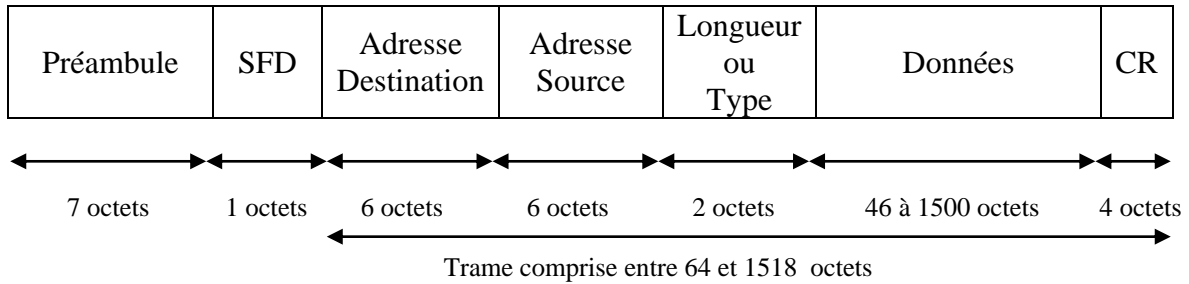
Suivant le débit utilisé il faut tenir compte du domaine de collision régi par les lois de la physique et notamment le déplacement électronique dans un câble de cuivre. Si l'on ne respecte pas ces distances maximales entre machines le protocole CSMA/CD n'a pas lieu d'exister.

Débit	Fenêtre de collision	Diamètre du réseau
10 Mbit/s	51,2 μ s	2500 m
100 Mbit/s	5,12 μ s	250 m
1000 Mbit/s	0,512 μ s	25 m

13.6.4. Performances

- Méthode d'accès non déterministe
- Dégradation des temps de réponses si la charge du réseau dépasse 30% de la charge.
- Le réseau passe sont temps à gérer les collisions.

14. Trame Ethernet



14.1. Le préambule

Le préambule est une suite de 0 et de 1 alternés. Il permet à l'horloge du récepteur de se synchroniser sur celle de l'émetteur. Comme la transmission est asynchrone, il est possible qu'une partie du préambule soit perdue.

14.2. Start Frame Delimiteur

Indique le début de la trame

14.3. Adresse destination et adresse source (MAC)

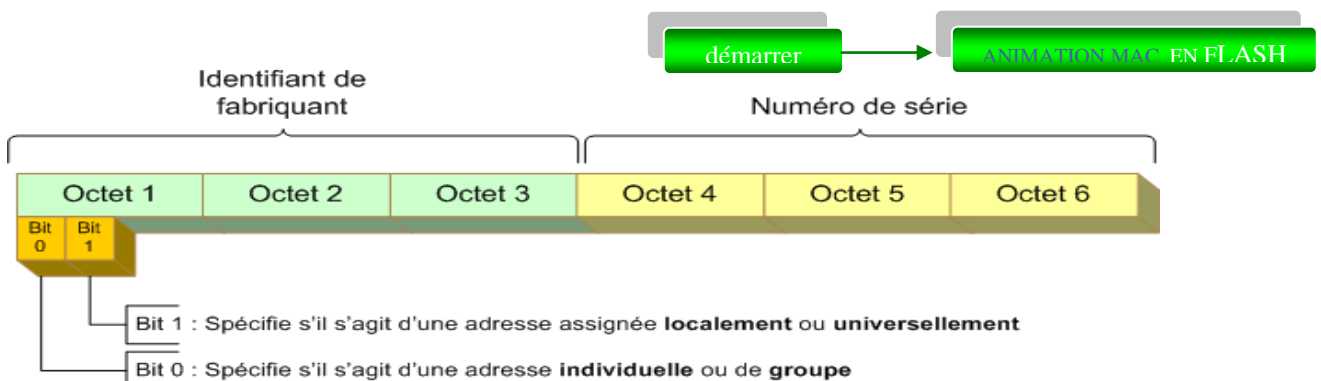
Les adresses MAC (*...Medium Access Control.....*) identifient le ou les destinataire(s) de la trame puis l'émetteur. Elles sont constituées de **6 octets** (théoriquement unique) :

- Les 3 premiers octets font référence au constructeur de l'interface. Ils sont uniques et sont attribués par l'IEEE.
- Les 3 octets suivants donnent le numéro d'interface chez ce constructeur.

L'adresse source (adresse physique de la station émettrice) est toujours celle d'une interface unique (*.....unicast.....*).

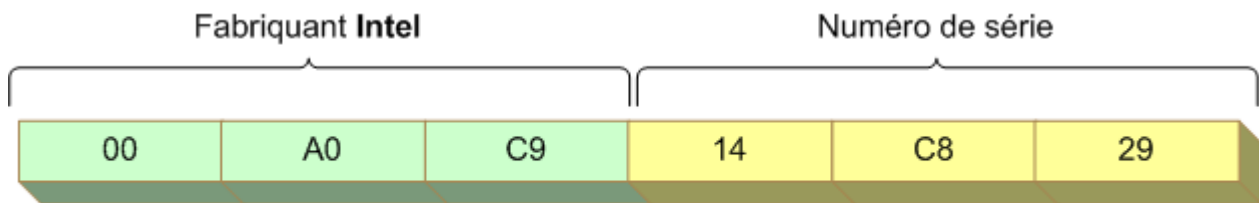
La destination peut être une adresse unique, de groupe (multicast) ou de diffusion générale (broadcast = FF-FF-FF-FF-FF-FF). Dans une adresse de groupe, le premier bit transmis est à 1. Si les autres bits ne changent pas, l'adresse de groupe correspond à toutes les cartes d'un même constructeur.

La sous-couche MAC est implémentée **au niveau 2 du modèle OSI** à l'intérieur de la couche liaison.



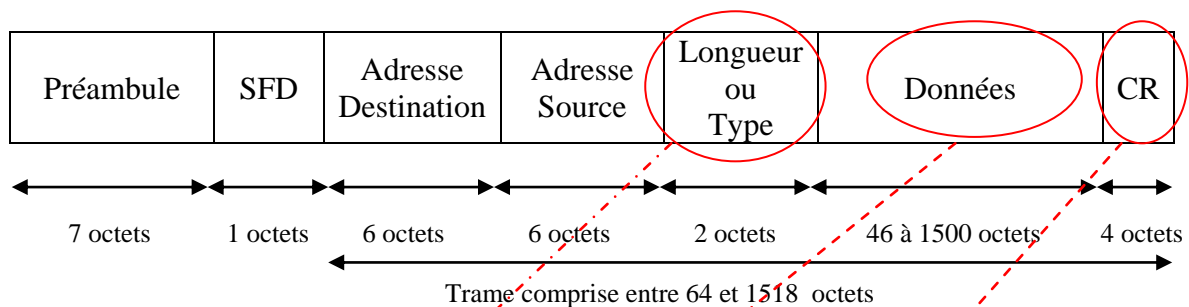
Chaque octet est représenté par un nombre hexadécimal variant de **00 à FF**.

Voici un exemple d'adresse MAC :



Représentation de l'adresse MAC : 00-A0-C9-14-C8-29

Exemple : SCHNEIDER : 00 80 F4 00-30-DE : WAGO 00-05-5D : D-Link
<http://standards.ieee.org/regauth/oui/index.htm>



14.1. Le champ longueur / type

Ce champ de 2 octets a été défini dans le standard Ethernet II pour indiquer le type de protocole de niveau 3 employés pour transporter le message.

14.2. Les données

Au niveau MAC ce champ est vu comme une suite de 46 à 1500 octets que l'on n'interprète pas. Si le nombre de données n'atteint pas 46 octets, le champ est complété par *padding* (*bourrage*).

14.3. Le champ de contrôle

Le FCS : *Frame Check Sequence* est un champ de 4 octets qui permet de valider l'intégrité de la trame à 1 bit près. Il utilise un CRC (*Cyclic Redundancy Check*) qui englobe tous les champs de la trame. Ainsi, la station réceptrice peut décider si la trame est correcte et doit être transmise à la couche supérieure.

14.4. Le temps inter-trame

Le temps inter-trame est appelé indifféremment *Inter Frame Space* ou *Inter Frame Gap*. Une machine ne peut émettre toutes les trames qu'elle a à transmettre les unes à la suite des autres. Le délai inter-trame normalisé est de 96 bits soit 9,6 microsecondes à 10Mbps.

Attention, cette définition a été revue pour le Gigabit-Ethernet. Il correspond au temps minimum de retour au repos du média et permet aux autres stations de prendre la main.

15. Ressource et références :

Pour la réalisation de ce document j'ai puisé dans des documents et sur Internet dans les sites suivants.

- Philippe RIGAUD : prof. Electro-technique lycée P.Neruda
- Michel CARTO : formateur indépendant
- Trend Novar France
- <http://www.linux-france.org>
- <http://sebsauvage.net/comprendre/tcpip/index.html>
- <http://christian.caleca.free.fr/>
- <http://www.frameip.com/>
- <http://www.themanualpage.org/reseau/index.php>
- <http://www.renater.fr/>

De nombreux autres sites traitent de ces sujets.