INTRODUCTION aux RESEAUX LOCAUX
Théorie et Normes

Michel Cabaré
Octobre 2001 ver 3.1

TABLE DES MATIÈRES

NOTIONS GENERALES

Point à point / Multipoint

On peut distinguer fondamentalement deux types de transmission de données :

- La transmission point à point, dans laquelle d'abord on établit la liaison puis on communique, c'est le cas par exemple de la liaison téléphonique classique.
- La transmission multipoint dans laquelle l'émetteur envoi ce qu'il a à transmettre, tout le monde reçoit l'information, même s'il n'est pas le destinataire final (dans ce cas bien sûr l'information n'est pas exploitée), c'est le cas par exemple de la liaison en réseau local classique.

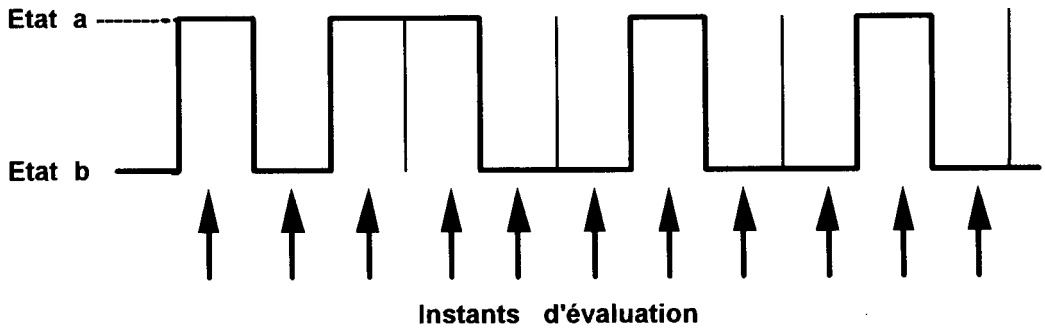
Nature de l'information (binaire):

L'information minimum est toujours supportée par un système à deux états :

allumé	/	éteint	(voyants lumineux)
enfoncé	/	relâché	(boutons poussoirs)

L'unité élémentaire d'information s'appelle le **bit (binary digits)**.On représente graphiquement dans un signal binaire, une succession de bits par une série de créneaux symbolisés par le chiffre 0 et 1, permettant simplement de distinguer un état de l'autre.

Voilà la représentation graphique de la valeur binaire 10110010010 :



Une combinaison de 2 bits peut prendre au maximum (2x2) quatre états différents. L'octet est une combinaison de 8 bits, qui peut donc prendre 2x2x2x2x2x2x2x2 = 256 états différents, ce qui est suffisant pour mémoriser l'ensemble des caractères : les lettres de l'alphabet, majuscules et minuscules, les chiffres et les signes de ponctuation, ainsi que divers signes spéciaux. On fera donc l'analogie octet = caractère ce qui est bien commode dans la pratique.

En conséquence, un support d'information d'une capacité d'un octet est capable de mémoriser une lettre ou un chiffre quelconque. C'est évidemment très peu. On emploi donc le plus souvent des multiples de l'octet :

Le kilo-octet (en abrégé K ou Ko) vaut 1024 octets. Un page dactylographiée a une capacité de 2 K environ.

Pourquoi 1024 et pas 1000 ? Vous savez que l'une des bases de la conception des ordinateurs est le système à deux états. Faites le calcul 2 puissance 10 et on obtient 1024.

Le méga-octet (en abrégé M ou Mo) vaut 1024 K soit plus d'un million de caractères. (exactement 1048576). Pour donner un ordre de grandeur , cela correspond au nombre de caractères d'un journal comme "le monde".

Communication Parallèle - Série :

parallèle:

tous les bits du même mot sont envoyés simultanément dans les fils. Ce système n'est pas employé en général pour les réseaux mais par exemple entre un ordinateur et une imprimante.

ex : caractère à envoyer :A donc la séquence de 8 bits le composant, soit :

- 0 - 1 - 0 - 0 - 0 - 0 - 0 - 1 -

donc utilisation de 8 fils transportant chacun un bit :

_____(fil n° 1)_____ 0
_____(fil n° 2)_____ 1
_____(fil n° 3)_____ 0
_____(fil n° 4)_____ 0
_____(fil n° 5)_____ 0
_____(fil n° 6)_____ 0
_____(fil n° 7)_____ 0
_____(fil n° 8)_____ 1

série:

tous les bits du même mot sont envoyés les uns à la suite des autres sur un même fil. C'est le système employé dans les réseaux en général.

ex : caractère à envoyer :A donc la séquence de 8 bits le composant, soit :

- 0 - 1 - 0 - 0 - 0 - 0 - 0 - 1 -

donc utilisation de 1 fils transportant successivement les 8 bits :

_____(1 fil)_____ 0 1 0 0 0 0 0 1

Communication Série Asynchrone - Synchrone :

Série Asynchrone :

Ce mode est utilisé quand l'émission est lente et irrégulière, comme celle en provenance d'un clavier.

Les « bits utiles » c'est à dire ceux correspondant aux informations à envoyer sont précédés par des bits annonçant le début de l'émission (START BIT) et suivis de bit annonçant la fin de l'émission (STOP BIT).

Le débit est faible (300,600,1200 et2400 b/s) et le rendement moyen (60%).

Série Synchrone :

En général on peut émettre les bits à une cadence constante, conforme à la fois aux capacités du support de transmission et aux capacités de récupération du récepteur. Les bits utiles sont envoyés les uns derrière les autres sans bits de séparations, et le récepteur doit évaluer ces bits à la même cadence et aux même instants (au décalage de transmission près) que l'émetteur.

Le débit est plus important (1200,2400,4800, 9600, 14400, 28800 et 33600 b/s).

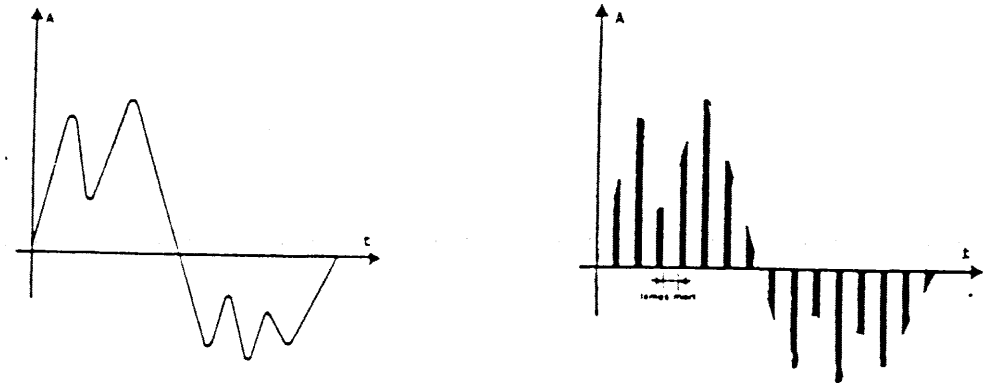
On échange dons non plus des octets mais des blocs d'information appelées TRAMES. Ces trames peuvent avoir l'aspect suivant :

délimiteur de début	@ source	@ destinat	données ...	contrôle cheksum	délimiteur de fin

La typologie de ces trames est fondamentale et débouche sur des normalisations internationales rigoureuses . (exemple AETHERNET 802.3)

Analogique - Numérique:

Un signal analogique peut prendre n'importe quelle valeur entre 2 points, alors que un signal numérique ne peut prendre qu'un nombre fini de valeurs entre deux points.



On appelle échantillonnage le nombre de bande que l'on peut découper pendant la durée d'une seconde.

On appelle quantification le nombre de valeurs différentes que ces bandes peuvent prendre. Plus le nombre de « bandes » est important (échantillonnage), et plus leur hauteur peut être finement réglée (nombre de valeurs possibles admises), plus précise sera la restitution sonore.

Communication Simplex - Half Duplex - Full Duplex:

Simplex :

La transmission est unidirectionelle, c'est à dire que les informations sont toujours véhiculées dans le même sens. Sans jamais d'exceptions, par exemple, entre un PC et une imprimante. (hors câbles bidirectionnel iEEE…)

Half Duplex :

La transmission est bi-directionelle, c'est à dire que les informations ne sont pas toujours véhiculées dans le même sens, mais que tour à tour, l 'émetteur peut devenir récepteur, et vice-versa. . Cependant, à un instant donné, on ne peut pas émettre et recevoir en même temps. par exemple, la communication entre deux « talkie-walkie », dans laquelle soit on parle, soit on écoute.

Full Duplex :

La transmission est bi-directionelle également, mais en plus l 'émetteur peut être récepteur au même instant, et vice-versa. . Par exemple, la communication téléphonique classique, dans laquelle soit on parle, soit on écoute, mais dans laquelle on peut « couper la parole de l'autre ... ».

Bande de Base - Bande Large (Multiplex):

En **Bande de base**, un signal occupe la totalité de la capacité de transport du support. Si le câble est trop long, on peut prendre des précautions en utilisant des répéteurs. Un répéteur reçoit un signal et le retransmet avec l'amplitude et la forme originale, afin d'accroître la longueur exploitable du câble.

En **bande large**, la largeur de bande du support est suffisamment large pour permettre un multiplexage en fréquence de chaque communication, de façon à ce que chacune d'elle n'occupe qu'une partie de la bande

Ainsi pour une communication téléphonique on demande une bande passante de 300-3400 hz, que l'on loge dans une tranche de 4000hz.

En multiplexant on peut à l'intérieur d'un support ayant une bande passante de 48 Khz à 64 Khz faire transiter simultanément 4 communications.

48 Khz

4000 hz	(de 48 à 52)	1 communication
4000 hz	(de 52 à 56)	1 communication
4000 hz	(de 56 à 60)	1 communication
4000 hz	(de 60 à 64)	1 communication

64 Khz

Débits Bit/s - bauds:

Les débits en bits correspondant à des données à transporter se calculent classiquement :

Pour un son de type téléphonique, de 300 à 3300 hz, on échantillonne à 8 Khz (deux fois la fréquence la plus élevées que l'on a à reproduire) soit 8000 bandes par seconde, en s'autorisant un nombre de valeurs possibles égal à 256, soit 8 bits.

Ce qui donne pour 1 seconde de conversation 1 x 8000 x 8 = 64.000 bit/s.

Actuellement les liaisons téléphoniques de France Télécom , utilisent des liaisons à 2048 Kbit/s ce qui autorise 32 canaux à 64 Kbit/s. (30 pour les communications et 2 pour la gestion).

64 Kbit/s c'est le débit d'ailleurs du réseaux NUMERIS ou RNIS.

Pour une qualité de type CD on échantillonne au minimum à 44.1 Khz (deux fois la fréquence la plus élevées que l'on a à reproduire) soit 44100 bandes par seconde, en s'autorisant un nombre de valeurs possibles égal à 65536, soit 16 bits.

Ce qui nous donne pour 1 seconde musique 2 x 44100 x 8 = 705.600 bit/s.

Pour de l'image 640x480 en 256 couleurs à 25 images /s

Ce qui nous donne pour 1 seconde d'image 640 x 480 x 8 x 25 c.a.d. 61.4 mega bit/s.

Pour de l'image 600x800 en 65000 couleurs à 25 images /s

Ce qui nous donne pour 1 seconde d'image 600 x 800 x 16 x 25 c.a.d. 192 mega bit/s.

Les débits nécessaires deviennent impressionnant, heureusement que les techniques de compression existent !

Contrôle de parité :

Dès lors qu'on envoie des données d'un endroit à un autre, on aime vérifier que ce qu'on a envoyé est identique à ce qu'on a reçu. Pour cela, on peut utiliser le **contrôle de parité**.

Pour vérifier les données, on calcule la **parité**. C'est à dire qu'on compte le nombre de 1 de l'octet. **Si ce nombre est pair, on envoie 0, si ce nombre est impair, on envoie 1.**

Par exemple, pour "01100111" on envoie 1 (5 uns donc impair) comme bit de parité.

Celui qui envoie l'octet envoie aussi le bit de parité qu'il a calculé.

Celui qui reçoit l'octet fait **le même calcul** et regarde si il a le même résultat.

Si le résultat n'est pas le même, il demande simplement à l'expéditeur de recommencer à envoyer l'octet parce qu'il y a eu une erreur. Cette solution ne couvre pas toutes les erreurs, mais en détecte une majorité... Il est rare d'avoir 2 bits mauvais dans un seul transfert d'octet, et c'est la condition pour que le contrôle de parité ne fonctionne pas.

Mode connecté (circuit virtuel) - Mode datagramme (non connecté) :

Selon le mode d'acheminement des paquets on distingue deux types de routage.

Mode datagramme (non connecté)

Les paquets sont acheminés indépendamment les uns des autres : deux paquets successifs destinés à la même station peuvent emprunter des chemins différents. Il n'y a pas de contrôle d'erreur. Les paquets peuvent être altérés, perdus, dupliqués ou déséquencés.

L'absence de contrôle d'erreur permet d'augmenter le débit. Donc, on choisit le mode datagramme chaque fois que la rapidité de transmission est plus importante que la fiabilité (vidéo, prélèvements répétitifs de mesures,...). Toutefois, il convient de noter que le mode datagramme peut permettre la transmission des paquets, même en cas de rupture d'un lien.

Dans un réseau local, on est en mode non connecté, on envois tout et ensuite la gestion se fait plus haut.

Mode circuit virtuel (connecté).

Il est généralement associé au mode connecté. A l'ouverture de la connexion, un chemin, appelé circuit virtuel, est choisi entre émetteur et destinataire. Durant la connexion, tous les paquets émis emprunteront ce circuit virtuel. Donc, chaque routeur intermédiaire doit conserver dans ses tables de routage, durant toute la durée de la connexion, les informations concernant le circuit virtuel.

Le mode circuit virtuel est bien adapté à l'établissement de garanties de qualité de service (QoS), telles que débit, rattrapage d'erreur, etc,...

THEORIE DES COUCHES RESEAU

Les couches du modèle OSI de réseau

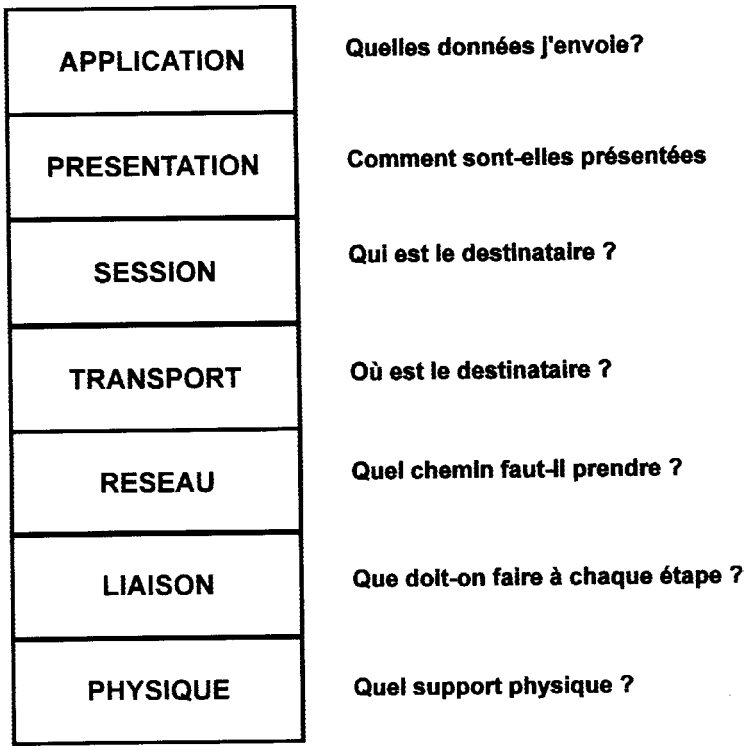
Un réseau se compose d'au moins deux ordinateurs interconnectés par des câbles et exploitant des logiciels leur permettant de communiquer.

Si on « trouve » un jour un câble réseau et qu'on le suive, on pourrait remonter le chemin jusqu'à l'écran de l'ordinateur en passant par une carte, des protocoles et des système d'exploitation.

Câble ➔ Carte ➔ Protocoles ➔ Système d'Exploitation

On peut affiner et remarquer qu'au cours des premières années de la gestion des communications, plusieurs grandes sociétés (IBM, HONEYWELL, DEC) avaient chacune leurs propres normes d'interconnexion d'ordinateurs décrivant les mécanismes nécessaires au transfert des données d'un ordinateur à l'autre. . Evidemment ces normes n'étaient pas compatibles entre elles.

Des organisations de normalisation comme l'ISO (Internationnal Standard Organization) et l'IEEE (Institute of Electrical Standard Organization) ont développé des modèles qui sont peu à peu devenus les normes de conception de tout réseau informatique en décrivant la gestion d'un réseau en terme de couches fonctionnelles.



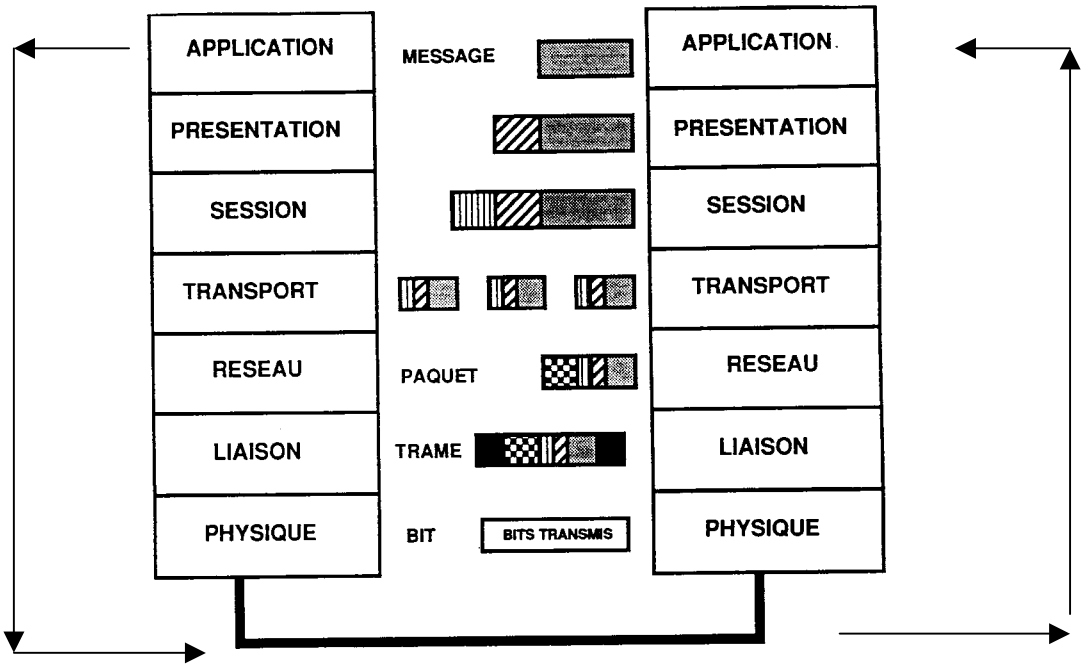
Les Données à travers les couches OSI :

Deux couches de même niveau ne se parlent jamais directement, seules les couches basses de deux ordinateurs, c'est à dire les couches physiques dialoguent « directement » entre elles.

A chaque couches, les données de la couche précédente sont « encapsulées » par des informations spécifiques sous forme d'en-têtes et de queues. Chaque en-tête et queue de **couche N** n'étant exploitable que par la **couche de niveau N semblable** sur l'ordinateur avec lequel on communique.

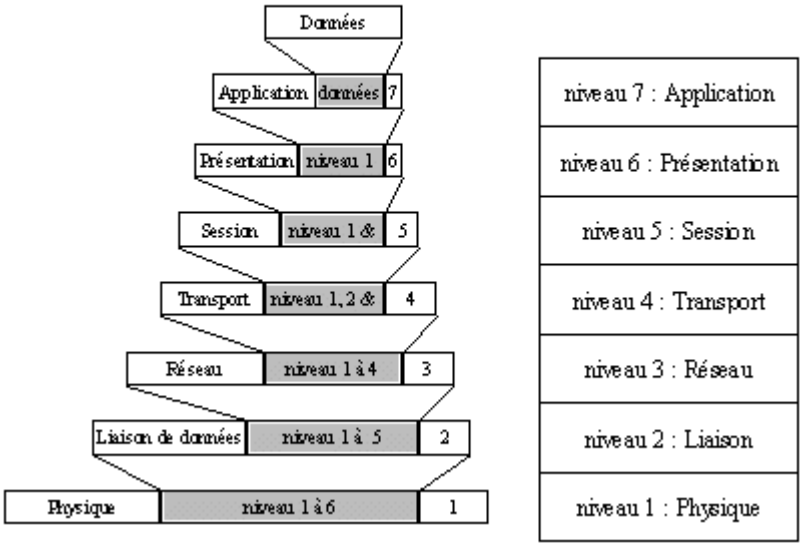
Ce qui pourrait donner schématiquement l'enchaînement suivant :

LE MODELE OSI DE L'ISO



Ce qui pourrait également se présenter de la manière suivante si on voulait mieux symboliser le mécanisme "d'encapsulation"

Le modèle OSI



LES COUCHES RESEAU

Suivons le raisonnement logique de quelqu'un qui trouve un câble par terre, remonte jusqu'à une machine, et qui essaye de comprendre comment les couches réseau s'inscrivent dans ce schéma.

Couche Physique :

C'est elle qui envois les bits dans le câble physique. Elle définit comment le câble est connecté (broches, prises), quelle est sa nature (paires torsadées ou fibres optiques, coaxial voir liaison radio ou infrarouge) et se préoccupe donc de définir comment coder un bit (nature et caractéristiques de l'impulsion électrique, *codage Manchester ou autre*).

Elle est responsable de la transmission des bits d'un ordinateur à un autre même si à ce niveau les bits n'ont pas une réelle signification logique. son rôle est d'assurer de bout en bout le transport bit par bit de l'information, et ce quel que soit la nature du support physique ...

Le support physique peut se prêter soit à une transmission analogique soit à une transmission numérique.

N.B: on parlera du cablâge dans un chapitre spécifique (page 52)

Transmission Analogique :

c'est transmission Analogique des réseaux téléphonique commuté (RTC) reste une des meilleures façons de se connecter à distance via un MODEM. Les débits maximum autorisés étant de 28800 bit/s et 33400 (normalisé), voire le chapitre sur les liaisons disponibles via les réseaux France télécom… (page 30)

en effet avec une bande passante de 3100 hz et une valence de 2 (nombre d'états différents que peut prendre le signal pendant une durée de temps) on obtient une rapidité de modulation maximale de 6200 bit/s. Avec un signal bruit d'environ 40 dB, un mathématicien nommé SHANNON à démontré que le débit maximum théorique du réseau RTC est de 31000 bits/s. (à rapprocher de la dernière normalisation à 28800 bit/s)

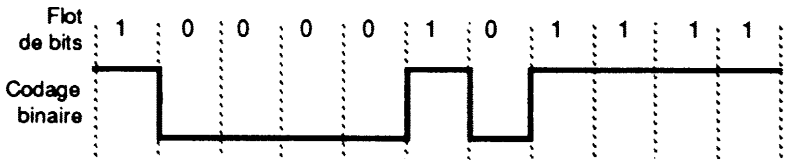
Il existe des liaisons spécialisées analogiques (LSA) dites normales (2 fils) ou supérieures (4 fils) mais qui offrent un débit identique au ligne commutées classiques ce qui est inutile et plus cher que les liaisons numériques, de nos jours.

Transmission Numérique ou "Bande de base":

La transmission numérique dite en bande de base existe sur le réseau télephonique en France ... (voir page 30) mais existe aussi et s'applique particulièrement bien aux réseaux locaux vie la technologie des paires torsadées qui ont une bande passante très large même si présentant un affaiblissement certain avec la fréquence.

Cependant un codage simple du type tout ou rien, correspondant au signal binaire original entraîne des disfonctionnements car les cartes acceptent mal le passage en continu de valeur à 0 (à cause de parasites possibles)

Pour éviter ces problèmes on code les signaux



Il faut donc s'assurer que les séries de bits à transmettre ne se traduisent pas par un courant continu. La méthode la plus simple consiste à effectuer une transition systématique en milieu de temps bit.

- "**code NRZ**" utilisé dans les liaisons **série**

  Ainsi pour les liaisons série de type RS232C (ou dite v24-v28) on ne code pas 0 ou 1 mais +12v et - 12v, ce qui évite d'avoir à interpréter la valeur 0 v !

- "**code Manchester**" utilisé dans les réseaux **Ethernet**

  un 1 est représenté par une transition positive en milieu de temps bit

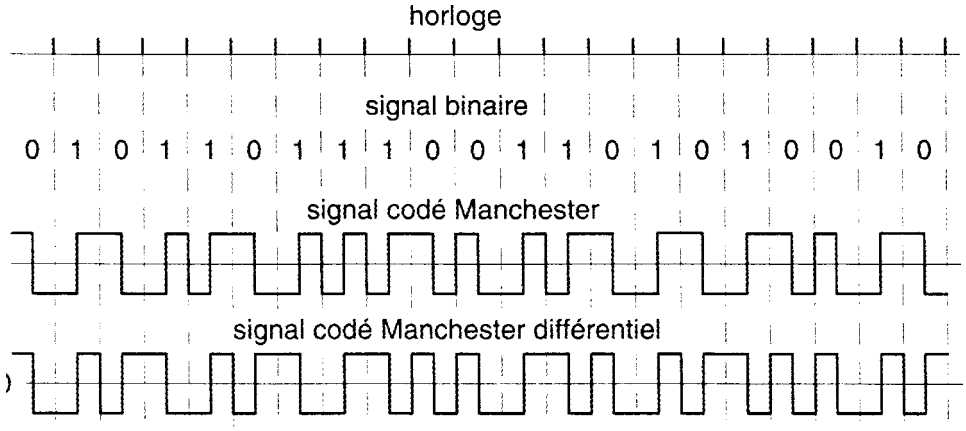
  un 0 "" "" négative "" ""

- "**code Manchester Différentiel**" utilisé dans les réseaux **Token Ring**.

  Un 0 amènera une transition en début de temps bit

  Un 1 n'amènera pas de transition en début de temps bit

  Dans les deux cas on a un transition en milieu de temps bit et donc le signal pour un bit dépends toujours du signal émis pour le bit précédant !



On voit donc clairement que la nature des signaux électrique est différentes selon la norme que l'on emplois, et que deux normes différentes ne peuvent être raccordées physiquement directement l'une à l'autre

Couche Liaison :

Le rôle de la couche liaison est de régler les problèmes non résolus par la couche physique en gérant les erreur de transmission et les conflits d'accès via des méthodes d'accès

Cette couche rassemble les bits de la couche physique pour en faire une structure de données, c'est à dire un paquet logique dans lequel peuvent être placées des données, ce que l'on appelle une trame. Cette couche construit donc des trames afin de pouvoir y incorporer un système de détection d'erreur et instaure un protocole pour les échanger et pouvoir donc éventuellement demander la réemission d'un trame détectée comme erronée.

délimiteur de début	@ source	@ destinat	type de trame	données ...	contrôle cheksum	délimiteur de fin

C'est pourquoi la couche Liaison est décomposée en deux sous - couches :

- la sous-couche **MAC** : Medium Acces Control (méthode d'accès)
- la sous-couche **LLC** : Logical Link Control (protocole d'échange)

ss couche MAC Méthode d'accès (IEEE 802.5 Token Ring, 802.3 Ethernet):

Dans la sous couche MAC, Il s'agit de définir comment on prends la parole sur le réseau.

Jeton (IEEE 802.5...) Token Ring:

privilégiée dans les réseaux en anneau où un jeton est représenté par une trame unique qui circule de noeud en noeud et pouvant prendre deux états: libre ou occupé . Pour émettre un noeud doit attendre que le jeton soit dans l'état libre. Le message à émettre est chargé dans la trame et le jeton est positionné occupé. Tous les postes voient passer le jeton occupé, ne peuvent par conséquent pas émettre et regardent simplement s'ils ne sont pas destinataires du message. Seul le noeud destinataire prends connaissance du message, et place un acquittement dans la trame. Le Jeton ne retrouve sa position libre qu'une fois que le noeud émetteur ait bien vérifié que son message a bien été lu .

En un tour, il y a émission, réception et acquittement.

Un mécanisme de priorité existe permettant de fixer un niveau de priorité (de 0 à 8) différent selon les stations. Une station de priorité supérieure à la station qui émet peut ainsi demander la parole et la station de priorité inférieure libérera immédiatement le jeton, même si elle à d'autres informations à transmettre.

Cette méthode est utilisée par IBM dans les réseaux **Token Ring**.

CSMA (IEEE 802.3...) Ethernet

Carrier Sense Multiple Access : Méthode d'accès aléatoire.

Privilégiée dans les réseaux en Bus ou diverses variantes existent, la plus répandue étant CSMA/CD c'est à dire avec Collision Detection, (détection de collision)

Tous les postes partageant le même support de transmission, un noeud peut émettre à condition qu'aucun autre noeud ne soit en cours de transmission. Pour cela le Noeud écoute avant de transmettre en détectant ou non la présence d'une porteuse (Carrier Sense). Si la ligne est libre, il émet.

Le problème vient que deux noeuds peuvent émettre en même temps. Pour éviter ce phénomène les noeuds écoute la ligne pendant la transmission, et par évaluation du signal électrique détectent une éventuelle collision. La transmission est alors interrompue pour être reprise après un délai aléatoire.

Cette méthode est normalisée par le CCITT et est utilisée dans les réseaux de type **Ethernet**.

ss couche LLC Protocoles d'Echange (HDLC x25 transpac-Rnis):

Dans la sous couche LLC Il s'agit de définir maintenant comment deux stations vont échanger leurs informations a travers un protocole d'échange.

Plusieurs procédures existent comme la SDLC d'Ibm ou le HDLC normalisée par le CCITT, ou les LLC1, LLC2 et LLC3 utilisées dans les réseaux locaux.

HDLC :

Ce protocole HIGH LEVEL DATA LINK CONTROL permet l'échange de trames de données entre deux stations de façon ordonnée. Ce protocole incorpore une gestion de détection et correction d'erreur , (récupération des erreurs de la couche précédente). Pour donner une idée si on a une erreur tous les milliards (dons une erreur de transmis tous les milliards transmis) sur un réseau 10 Base 100 on aurait un « plantage » toutes les 10 secondes, et sur un réseau 10 Base T on aurait un « plantage » toutes les 100 secondes.

Ainsi quand la couche Liaison envois une donnée, elle attend un acquittement de la part du destinataire, et elle peut si besoin rééditer la trame mal reçue...

C'est le protocole utilisée dans les réseaux publics tels que TRANSPAC ou NUMERIS. A quelques variantes près.

Versions du protocole de liaison HDLC.

LAP-A	Asynchronous
LAP-B	Balanced (Réseaux X25-Transpac)
LAP-D	Canal D (Réseaux RNIS)
LAP-M	Modem
LAP-N	Normal
LAP-X	half - duplex

C'est le plus complet, avec toutes une série de trames de nature différentes et de longueur variable permettant un dialogue sophistiqué entre les stations.(Demande d'émission, acquittement, demande de reémission, trame de donnée, fin d'émission ...)

Réseaux Locaux :

Dans un réseau local, on est en mode non connecté, on envois tout et ensuite la gestion se fait plus haut.

En général on envois un seul type de trame d'une longueur toujours identique.

Couche Réseau :

Détermine le chemin à parcourir pour aller d'un ordinateur à un autre, (en cas de chemins multiples, en fonction des conditions du réseau, des priorités, des problèmes d'encombrement) et assure la conversion des adresses logiques en adresses physiques.

On dit que cette couche gère la transmission dans le réseau. Elle est responsable de l'acheminement des paquets qui peuvent traverser plusieurs noeuds intermédiaires.

A l'émission, elle peut réunir entre elles des données différentes entre elles mais trop petites pour êtres émises toutes seules sur le réseau, ou au contraire fractionner en petits morceaux des données trop volumineuses pour êtres envoyées sur le réseau.

A la réception, elle reconstitue les paquets de données pour leur redonner leur taille originelle.

Deux grand type de protocoles existent, le **datagramme**, dans lequel les paquets constituant les données ne suivent pas tous obligatoirement la même route, et le **circuit virtuel** dans lequel tous les paquets suivent la même route.

On peut citer IP et IPX (Novell) mais aussi X.25 pour les réseaux public.

protocole IP :

Ce principe connu sous le nom de "**datagramme en mode non connecté**" est celui utilisé dans les réseaux privés. Internet protocol c'est une façon d'acheminer les informations d'un endroit à un autre.

Chaque paquet se débrouille pour trouver son chemin, les premiers partis peuvent très bien arriver les derniers, et il n'y à pas de raison particulière pour que tous les paquets emprunte toujours le même chemin (au contraire).

Si pendant un échange, un noeud est détruit (coupé), la communication n'est pas pour autant interrompue.

N.B: Un chapitre complet sera consacré à TCP/IP

protocole IPX (novel):

protocole d'inspiration IP mais propriétaire de NOVELL NETWARE.

protocole X25 (transpac):

Ce principe connu sous le nom de "**circuit virtuel en mode connecté**" est celui utilisé dans les réseaux public de France Télecom.

On établit un réseau virtuel à partir du moment où le premier paquet est arrivé avec un acquittement de la part du destinataire. Cela amène un mode connecté qui réserve un chemin unique pendant toute la durée de l'échange.

Si pendant un échange, un noeud est détruit (coupé), la communication est interrompue !

Couche Transport :

Cette couche s'occupe de la détection et de la correction des erreurs., c'est à dire doit s'assurer que les paquets transmis ont bien étés reçus . Cette couche est responsable de la bonne transmission des messages de la couche application, et pour ce faire elle subdivise les messages long en plusieurs paquets et regroupe les messages courts en un seul pour permettre une transmission plus efficace sur le réseau. (un peu comme la couche réseau pour les trames)

On peut citer TCP comme protocole représentatif de cette couche.

Les protocoles de transports sont complémentaires de ceux de la couche réseau. si on regarde essentiellement IP on trouve alors

protocole TCP :

complément logique de IP, il fait apparaître à ce niveau une notion de Port.

Si l'adressage de niveau réseau, comme IP permet de désigner de manière unique une machine située n'importe ou sur le réseau, quand la machine est atteinte il faut pouvoir savoir quelle est l'application qui doit traiter les données.

En effet un ordinateur à fréquemment besoin de plus d'un accès sur le réseau : on peut avoir besoin de télécharger des fichier FTP tout en récupérant son courrier via un serveur POP3…

Les ports proposent 65535 point d'accès à un ordinateur à partir d'une seule adresse physique. L'ensemble composé des adresses physiques des ordinateurs essayant de communiquer et des numéro de ports utilisés crée ce que l'on appelle un "SOCKET"

Il a été ainsi arbitrairement décidé d'un N° de Port pour chaque usage.

Par exemple :

Port n° 21	: File Trandfer Protocol
Port n° 22	: SSH connexion à distance sécurisée
Port n° 23	: Telnet
Port n° 25	: SMTP réception de courrier
Port n° 53	: DNS Domain Name Server
Port n° 80	: HTTP pages web
Port n° 88	: Kerberos authentification
Port n° 110	: POP3 lecture de courrier
Port n° 113 à 139	: NetBios
Port n° 546	: DHCP

Couches "hautes" Session - Présentation - Application :

S'il n'est déjà pas très facile de distinguer clairement les couches basses, cela peut devenir très difficile de distinguer une scission claire entre les couches hautes.

On pourra noter cependant

couche Session :

Il s'agit de permettre à des applications fonctionnant sur différents ordinateurs d'établir et d'utiliser une connexion appelée session. Cette couche assure également la gestion de la connexion, de la déconnexion et du processus de communication (qui transmet, quand, combien de temps, que faire en cas d'interruption...)

Couche Présentation :

C'est la normalisation des matériels présent dialoguant dans un réseau (normes d'écran, de compression, d'encryptage ...) pour une interprétation correcte.

A l'émission, la couche présentation convertit les données envoyées par la couche application en un format exploitable par les couches plus basses.

A la réception, elle convertit le format reçut des couches plus basses en un format exploitable par la couche application de l'ordinateur.

Aujourd'hui le seul fédérateur de fait c'est le phénomène INTERNET.

Couche Application

C'est la couche qui va faire le lien entre les programmes voulant accéder au réseau un et le réseau. Elle représente le lien avec les applications de

l'utilisateur, comme les logiciels de transfert de fichier, d'accès aux base de données ou le courrier électronique.

A l'arrivée au noeud destinataire, le processus en couches est inversé,

- La couche physique reconstitue les bits du message
- La couche de liaison recalcule la somme de contrôle, confirme la reception et enregistre les paquets
- La couche réseau recompte les paquets
- La couche transport recalcule la somme de contrôle et réassemble les segments du message
- La couche session conserve les différentes parties du message jusqu'à réception complète
- La couche présentation décompresse et décrypte le message
- La couche application convertit les bits en caractères et les transmets à l'application

TOPOLOGIE DE RESEAUX

Un réseau se compose d'au moins deux ordinateurs interconnectés par des câbles et exploitant des logiciels leur permettant de communiquer.

Cependant on peut distinguer différentes topologies de connexion, relativement indépendante (pas toujours) des types de protocoles que l'on va faire passer dedans.

On peut distinguer essentiellement deux topologies au niveau du câblage physique et deux topologie au niveau de la méthode d'accès :

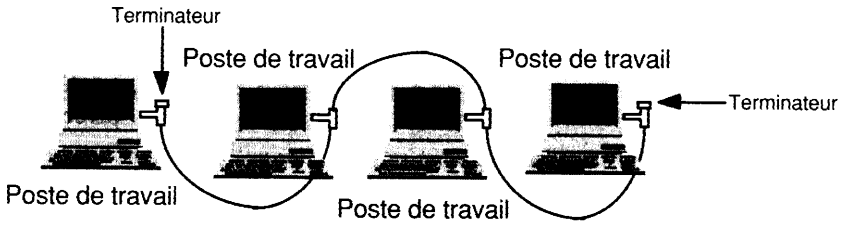
Topologies de Câblage :

deux Topologie principales de câblage existent:

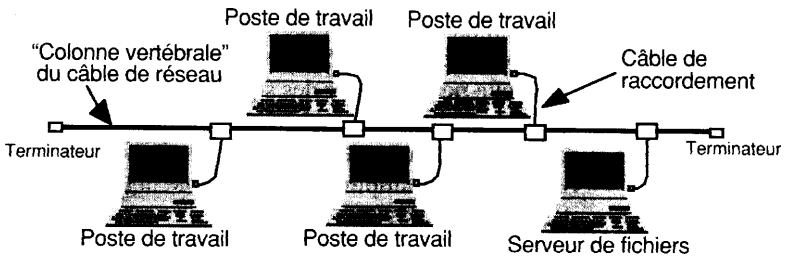
- **Réseaux en BUS**
- **Réseaux en ETOILE**

Réseau en BUS

Dans une topologie en BUS tous les ordinateurs sont connectés au même câble dont chaque extrémité se termine par une résistance appelée bouchon ou terminateur.



Dans un petit LAN le câble de réseau est directement connecté à chaque ordinateur au moyen de connecteurs en "T".



Dans un LAN plus important on emploie des câbles de raccordement

pour connecter chaque ordinateur au câble du réseau appelé "Backbone"

Avantages - Inconvénients :

Avantages	Inconvénients
• La panne d'un poste n'affecte que le poste • Connexions de câble simples, flexibles • Câbles et connecteurs bon marché • ajout / suppression d'un noeud très simple	• La coupure d'un câble peut affecter de nombreux utilisateurs • Longueur et nombre de postes limités (noeuds passifs) • Localisation difficile des défauts de cablâge • Dégradation des performances sensible

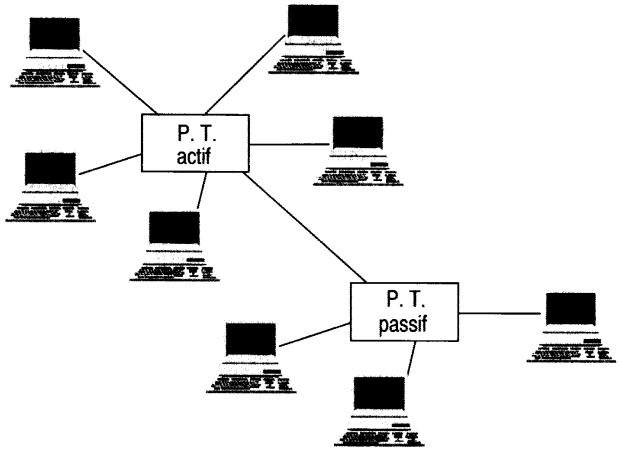
Utilisation dans les réseaux:

Cette topologie est utilisée dans les réseaux **Ethernet 10 Base 2** et **10 Base 5**.

Réseau en Etoile

Dans une topologie en ETOILE tous les ordinateurs sont connectés à un périphérique spécial appelé Hub. Plusieurs Hub peuvent être connectés entre eux, et on peut avoir des hubs passifs ou actifs, augmentant considérablement la distance et le nombre de noeuds connectés.

Des étoiles peuvent se raccorder entre elles par une de leurs branches dans les limites techniques de la norme que l'on décide d'appliquer



Avantages - Inconvénients :

Avantages	Inconvénients
• La panne d'un câble n'affecte qu'un poste • Ajout d'un nouveau poste facile • Gestion centralisée du réseaux	• une panne de Hub bloque tous les postes reliés. • Les débits dépendent du nombre de nœud

Utilisation dans les réseaux:

Cette topologie est utilisée dans les réseaux Ethernet **10 Base T** et **100 Base T**

Topologies de Méthode d'Accès :

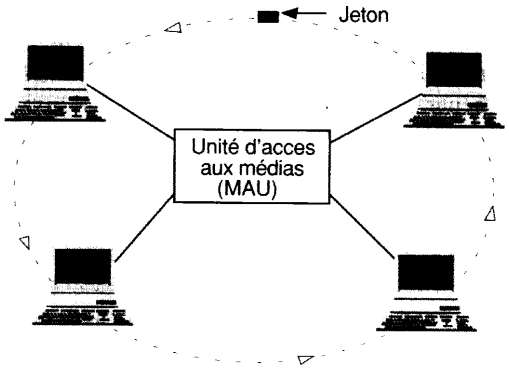
deux Topologie principales de méthode d'accès existent:

- **Par Anneau à Jeton**
- **Par Détection de Collision**

Par Anneau à jeton

Dans une topologie en ANNEAU A JETON tous les ordinateurs sont connectés au même câble formant une boucle fermée au niveau logique, sur laquelle un "jeton" passe d'un poste de travail au suivant. Du point de vue câblage, il s'agit en fait d'une étoile

Un ordinateur communique en s'emparant du jeton et en le faisant circuler sur un anneau électrique logique



Principes de fonctionnement :

Un Jeton, constitué d'un seul message court, circule continuellement le long de la boucle et est lu par la carte réseau de chaque poste lors de son passage.

- Un noeud désirant émettre saisit le jeton lors de son passage, modifie son contenu pour indiqué qu'il est occupé et y attache son message avec l'adresse du noeud destinataire et le code de correction d'erreur.
- Chaque noeud comporte un répeteur qui régénère le message entier en maintient l'intégrité des données
- Chaque noeud inspecte le jeton à son passage et pour voir s'il contient sa propre adresse. Si c'est le cas il prends une copie du message
- Lorsque le message revient au noeud émetteur, celui-ci en retire la partie donnée et restaure l'état initial du jeton (c'est à dire libre).

Avantages - Inconvénients :

Avantages	Inconvénients
• Dégradation faible des performances en cas d'agrandissement • Absence de collision complète	• l'ajout d'un noeud nécessite l'arrêt dur réseau • cablâge et connexions couteûses faible rendement à "bas régime" (on attends son tour)

Utilisation dans les réseaux:

Cette topologie est notamment utilisée dans les réseaux IBM **Token Ring**

par Détection de Collision

Dans une topologie par detection de collision tous les ordinateurs sont connectés au même câble formant un bus ou des étoiles ou un mélange des deux. Du point de vue câblage, il s'agit en fait d'un ensemble de machines devant se connecter entre elles et formant ce que l'on appelle un "domaine de collision"

Principes de fonctionnement :

Un signal va et vient le long du câble entre les deux bouchons et passe devant chaque poste de travail. Tous les postes ou noeud possèdent une adresse unique.

- La carte réseau installée dans un noeud (Ordinateur, Serveur de fichier, Serveur d'impression) écoute le réseau pour s'assurer qu'aucun autre message n'est transmis. Elle envoie alors un message en direction d'un autre noeud en lui incorporant l'adresse du noeud émetteur et du noeud de destination.
- Le message se diffuse sur le câble, et au passage chaque noeud examine la zone adresse du message. Ceux qui ne sont pas destinataires ignorent le contenu, mais si un noeud détecte sa propre adresse, il lit les données, les vérifient et envoie un accusé de réception à l'émetteur.
- Si deux noeuds cherchent à émettre simultanément un message, il y a collision, et l'interférence créée est suffisament caracéristique pour être reconnue comme telle par les autres noeuds.
- Dès qu'un noeud détecte une collision il envoie un signal spécial qui brouille le réseaux de façon à ce que tous les noeuds sachent qu'il y a problème. Chaque noeud attends alors un temps aléatoire avant de tenter la réemission de son message. La méthode se répète jusqu'à ce qu'un noeud réussisse à émettre sans collision.

Avantages - Inconvénients :

Avantages	Inconvénients
• La panne d'un câble n'affecte qu'un poste • Ajout d'un nouveau poste facile • Gestion centralisée du réseaux en divers domaines de collision "indépendant" possible	• une panne de Hub bloque tous les postes reliés. • Une panne de Serveur bloque tout • Les débits dépendent du nombre de noeud

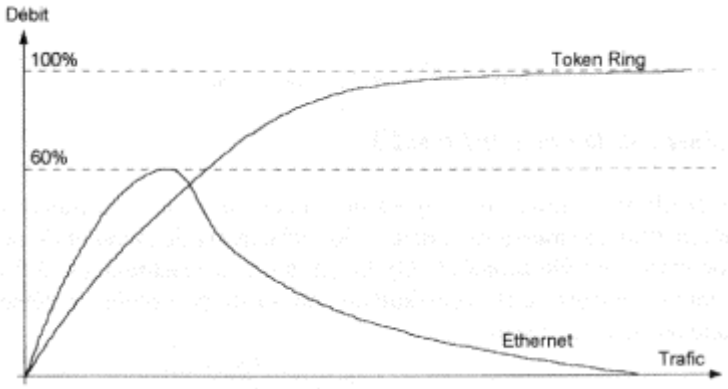
Utilisation dans les réseaux:

Cette topologie est notamment utilisée dans les réseaux **Ethernet**

Anneau à jeton ou Détection de Collision ?:

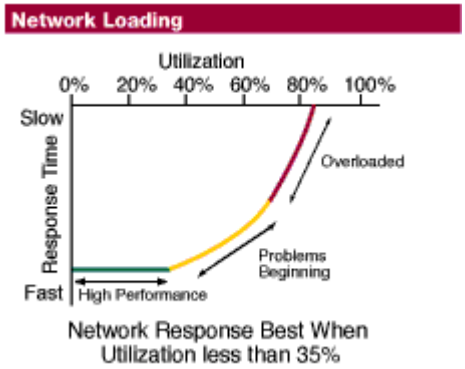
Comparer ces deux méthodes, revient en fait à comparer concrètement deux normes, une TOKEN RING, poussée par IBM et l'autre ETHERNET, ayant fait l'objet d'une normalisation

Pour comparer deux normes, il faut comparer non seulement les débit physiques annoncés des media, mais aussi les débits en charge du réseau, c'est à dire le débit "utile"



A faible charge les réseaux Ethernet présentent une meilleure efficacité car des qu'une station veut émettre, elle peut le faire. mais lorsque la charge monte, les collisions augmentent et le débit "utile" s'effondre.

On a même coutume de dire qu'en sur un réseau Ethernet la bonne utilisation consiste **à ne pas utiliser plus de 35% du débit nominal du média**, et que de toute façon le protocole est tel **qu'on ne peut jamais dépasser 65% du débit nominal du média**



Par contre a faible charge les réseaux Token Ring présentent une mauvaise efficacité car lorsqu'une station veut émettre, elle ne peut le faire que lorsque le jeton passe à sa portée.

Mais lorsque la charge monte, les collisions restent nulles et même si le débit moyen de chaque station diminue, le débit "utile" peut rejoindre **100% du débit nominal du média**

PRESENTATION DES RESEAUX TELECOM

Désormais il n'y a pas uniquement France Telecom, même si pour l'instant les concurrents sont fort timides. A partir de 01/01/2001 le monopole sur la boucle locale disparaît…(c'est à dire la partie finale desservant le téléphone, appelée communément aussi la paire cuivrée…)

Réseau Commuté – Réseau Spécialisé :

Lorsque l'on présente les réseaux télécom on peut traditionnellement découper la présentation en deux parties distinctes :

Les **Réseaux Commutés** caractérisés par :

1. Un abonnement
2. Paiement selon consommation
3. On peut atteindre n'importe quel autre appareil raccordé

On y trouvera notamment :

- R.T.C. : le Réseau Téléphonique Commuté
- Numeris - RNIS : le Réseau Numérique à Intégration de Service
- Transpac : Transport de paquet via le protocole X25
- ADSL : Asymetrical Digital Subscriber Line
- BLR : la Boucle Locale Radio

Les **Liaisons Spécialisées** caractérisées par :

1. Une location via un forfait
2. On relie toujours un point à un autre fixe

On y trouvera notamment :

- Les L.S.A. ou L.L.A.: Liaisons Spécialisées (Louées) Analogiques à ne plus utiliser de nos jours
- Les technologies Numeris – X25 – Frame Relay – ATM à travers des appellations commerciales comme Transpac ou Transfix …

Un peu à part, on peut classer le Câble, et la Liaison Satellite (essentiellement en vue d'une connexion Internet)

Réseaux Télécom et Tarification :

Il faut distinguer deux catégories de tarification, selon que l'on se trouve en réseau commuté ou en réseau spécialisé

La tarification des réseaux commutés est caractérisée on l'a dit par :

1. Un abonnement (des frais de raccordement peu onéreux)
2. Paiement selon consommation

R.T.C.	Abonnement fixe	Consommation = durée + distance + plage horaire
Numeris	Abonnement fixe	Consommation = durée + distance + plage horaire (N.B: idem facturation R.T.C.)
Transpac	Abonnement fixe	Consommation = quantitée (volume) et pas la distance ! (N.B : minitel, transaction bancaires, mais si http alors la facture sera énorme)
ADSL	Abonnement fixe	Consommation forfaitaire incluse (liaison 24h/j mais pas 24h/24h, en effet une déconnexion est faite toutes les 24h !) Consommation téléphonique séparée et classique

La tarification des Liaisons Spécialisées est caractérisée on l'a dit par :

1. Des frais de raccordement très onéreux
2. Paiement forfaitaire selon débit/distance souhaités

LLA-LSA.	Frais de raccordement	Forfait selon distance - débit
Transfix	Frais de raccordement	Forfait selon distance - débit
Transfix HD	Abonnement fixe	Forfait selon distance – débit et durée de l'abonnement
Transfix 2	Abonnement fixe	Forfait selon distance - débit

Réseaux Télécom et Débits :

Le plus difficile, pour savoir de quelle liaison on a besoin, c'est de savoir de quels débits on a besoin…(voir chap sur numérisation du son, d'une image, de la vidéo…)

Il existe des paliers, et depuis une connexion à 9.6Kbs jusqu'à 620 Mbs il y a en effet de la marge…

Les Débits des réseaux commutés sont caractérisés on l'a dit par la technologie employée bien sur:

R.T.C.	2.4 Kbs à 33.6 Kbs	Normes « Modem Analogiques »
Numeris	64 Kbs à 128 Kbs	1 ou 2 canaux groupés
Transpac	9.6 Kbs à 256 Kbs voire 2 Mbs	Selon forfait
ADSL	128 Kbs < 512 Kbs 256 Kbs < 1 Mbs	Selon forfait Débit montant < Débit descendant

N.B : Plus de détails sont donnés pour chaque technologie décrite plus loin dans un chapitre « technologie des réseaux commutés »

Les Débits des liaisons spécialisées sont caractérisés on l'a dit par la technologie employée bien sur.

Mais ici on ne sait jamais quelle technologie est réellement employées, dans le sens ou ne prends pas une liaisons X25 ou ATM (même si on peut s'en douter) mais plutôt une liaison via Transfix, par exemple…

En fait on choisit un « débit », et une « offre commerciale », et pas une technologie !

Numeris	64 Kbs à 128 Kbs	Transfix Oleane
X25	9.6 Kbs à 256 Kbs	Transfix et Transpac Oleane
Frame Relay	34 Mbs	Transfix HD Oleane
ATM	155 Mbs à 620 Mbs	Transfix HD Oleane

N.B : Plus de détails sont donnés pour chaque technologie décrite plus loin dans un chapitre « technologie des liaisons spécialisées »

TECHNOLOGIE DES RESEAUX COMMUTES

Les réseaux commutés sont à la disposition des utilisateurs pour échanger des données informatiques. Ne serait-ce que pour permettre à deux réseaux locaux d'échanger leurs données entre eux .

L'avantage du réseau commuté est la facilité des points d'accès au réseau, au niveau mondial même. Ses inconvénients sont le bruit et le parasitage éventuel de ses équipements.

La scission ici entre réseaux commutés et liaisons spécialisées ne sert qu'à présenter plus commodément les différentes notions, en effet Numeris est souvent utilisées comme première technologie sur les liaisons spécialisées à faible débit, voir comme solution de replis temporaire en cas de défaillance d'un liaison à plus fort débit…

Transpac, est une liaison qui ferait plus partie des liaisons commutées que spécialisées, du fait de la possibilité d'atteindre plusieurs destinataires raccordés au réseau, et du fait de sa tarification dépendant du volume, et donc non forfaitaire comme celle des autres liaisons spécialisées

---

Réseau RTC :

Il s'agit du téléphone classique. Avec un Modem on atteint 28 Kbit/s voir avec compression 50 Kilobit/s bien sûr ces vitesses sont normées

Tarification :

La tarification dépends de la durée / distance / plage horaire.

Local

- **0,024 € HT** (0,16 F) **la minute** au tarif jour, **0,015 € HT** (0,10 F) au tarif nuit, au-delà du crédit-temps.
- Crédit-temps de 1 minute : **0,076 € HT** *(0,50 F)*

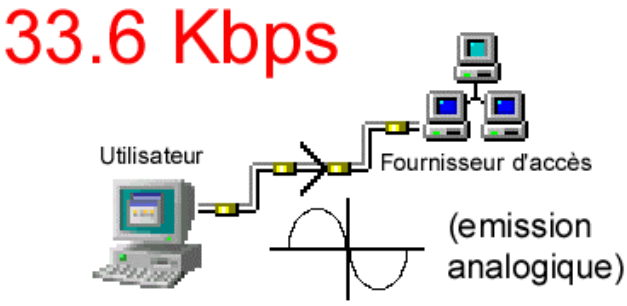
National

- **0,061 € HT** (0,40 F) **la minute** au tarif jour, **0,046 € HT** (0,30 F) au tarif nuit, au-delà du crédit-temps.
- Crédit-temps de 20 secondes : **0,076 € HT** (0,50 F).

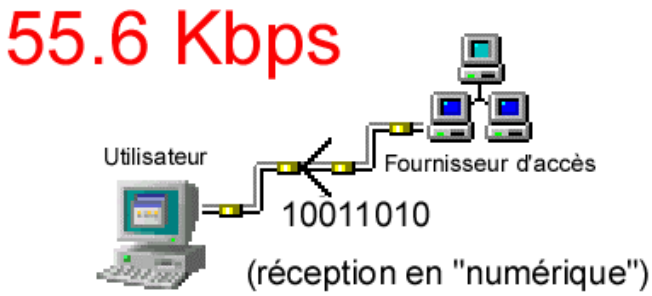
La vitesse du modem

La plus grande vitesse possible actuellement est de 33600 bps (bits par seconde). Certains constructeurs vous proposent des modems à 56 000 bps, cette vitesse n'est absolument pas garantie, de plus elle n'est possible que sous certaines conditions et en mode réception uniquement.

Emission : en 33.6 kbps, modulation analogique



Reception : en 55.6 kbps, pseudo-numérique



Normes principales de transmission concernant les modems

Norme	Description
V23	réception 1200 émission 75 (minitel)
V32	Transmission jusqu'à 9600 bps
V32bis	Transmission jusqu'à 14400 bps
V34	Transmission jusqu'à 28800 bps
V34+	Transmission jusqu'à 33600 bps
V90	Transmission jusqu'à 56000 bps Il existe présentement trois technologies 56 kbit/s, dont deux -- x2 et k56flex -- qui se disputent le marché pour devenir la nouvelle norme de l'industrie. En février 1998 une nouvelle norme v90est apparue

L'avantage du réseau commuté est la facilité des points d'accès au réseau, au niveau mondial même. Ses inconvénients sont le bruit et le parasitage des équipements.

Le RTC sera réservé à des transmission de donnée relativement faibles quand les délais ne sont pas impératifs et le trafic relativement peut important.

Il est important de choisir son type d'abonnement dans la "panoplie" proposée car les variations de tarifications sont importantes. d'autres normes

Avis	Débits principal et repli (bits/s)	Mode de transmission	Support		
			Réseau commut.	LS	
				2 fils	4 fils
V 21	300	A	FD	FD	
V 23	1 200/600 1 200/75	A/S A	HD FD	HD FD	A
V 22	1 200/600	A/S	FD	FD	
V 22 bis	2 400	A/S	FD	FD	
V 26	2400	S			FD
V 26 bis	2 400/1 200	S	HD		
V 26 ter	2 400/1 200	S/A	FD	FD	
V 27	4 800	S	HD	FD	
V 27 bis	4 800/2 400	S	HD	FD	
V 27 ter	4 800/2 400	S	HD		
V 29	9 600/7 200/4 800	S			FD
V 32	9 600/4 800	S	FD	FD	
V 33	14 400/12 000	S			FD

Légende. **A** : transmission asynchrone, **S** : transmission synchrone, **FD** : liaison exploitée en duplex, **HD** : liaison exploitée en semi-duplex, **LS** : ligne spécialisée.

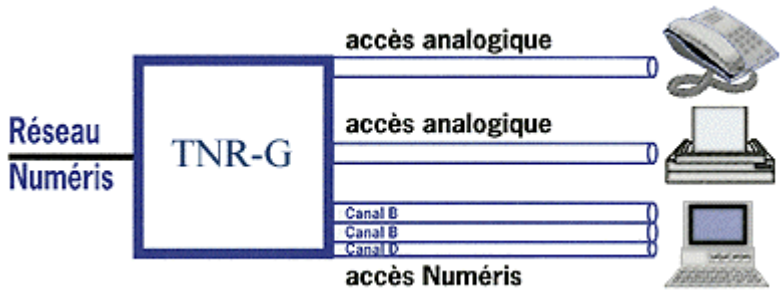
Numeris :

C'est le nom commercial en France d'une normalisation internationale spécifiée par le CCITT d'ailleurs appelée **RNIS** (Réseau Numérique à Intégration de Service) ou **ISDN** (Integrated Service Digital network)

Ce type de liaison peut convenir pour du transport de données, de voie et pour des images fixes.

Elle est véhiculée dans le réseau téléphonique standard car désormais la couverture nationale est numérique, ce qui fait que ce type de liaison est accessible partout.

Un accès Numéris divise une ligne téléphonique en 3 canaux numériques : 2 canaux "B" et un canal "D", pouvant être utilisés ensemble



Les canaux "B" sont utilisés pour transmettre la voix ou des données, à des vitesses de 64 kbits/seconde. Le canal "D" est chargé du travail administratif, comme l'établissement et la conclusion de l'appel entre terminaux.

Pour information, le protocole utilisé par le RNIS est le LAP D, très similaire au HDLC LAP B.

Tarification :

Depuis Novembre 1995 France Télécom a aligné la tarification Numéris sur celle des communications téléphoniques RTC classiques.

La tarification dépends de la durée / distance / plage horaire, et non du type d'abonnement !

Exemple en local

- **0,024 € HT** (0,16 F) **la minute** au tarif jour, **0,015 € HT** (0,10 F) au tarif nuit, au-delà du crédit-temps.
- Crédit-temps de 1 minute : **0,076 € HT** *(0,50 F)*

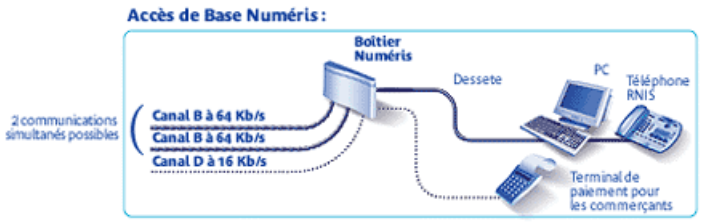
Abonnement:

Il existe plusieurs types d'accès :

- l'Accès de Base Isolé
- Numéris Duo
- l'Accès Primaire groupé.

Accès de Base isolé :

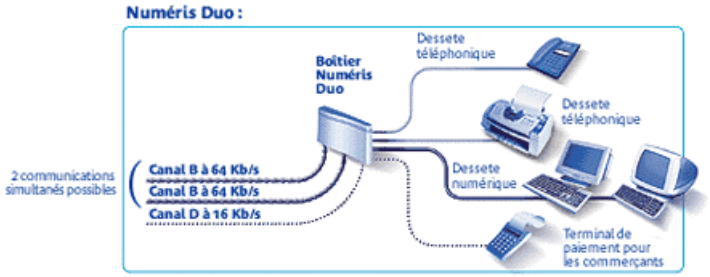
L'accès de base isolé : permet de disposer de deux canaux "B" et d'un canal "D". avec agrégation possible pour arriver à un débit max de 128 Kilobit/s .



Il permet de raccorder via une prise Numéris jusqu'à 5 terminaux numériques (micro-ordinateurs, téléphones Numéris) ou analogiques (téléphones, fax, Minitel, répondeurs)

Duo :

Numéris Duo : Il vous permet de combiner, sur le même accès, les performances de l'accès de base Numéris pour vos applications téléinformatiques et 1 ou 2 accès analogiques (RTC)°de votre installation téléphonique existante.

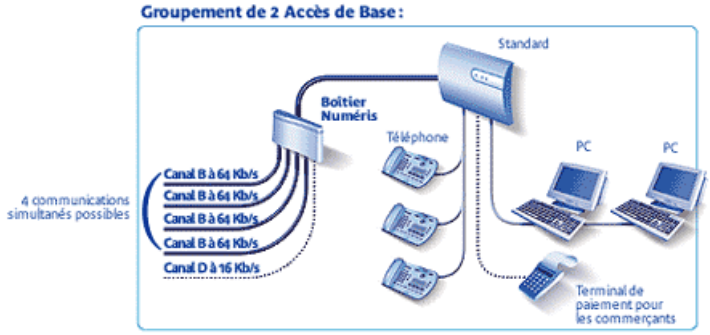


C'est à dire :

- soit 2 soitcanaux à 64 Kilobit/s + 1 canal 16 kilobit/s (utilisé pour la gestion du trafic) soit 128 kilobit/s plus une liaison RTC
- soit une liaison à 64 Kilobit/s et deux liaisons analogiques RTC.

Primaire:

Comprend 30 canaux B (agrégables par 15-20-25 ou 30) et un canal D à 64 Kilobit/s. Il correspond à un multiplexage de type MIC et il s'agit donc d'une liaison MIC complète à 2048 Kilobit/s. permet des groupement jusqu'à six accès de bases. (ici exemple avec 2 accès groupés)



Installation:

Toute entreprise ou particulier peut demander la pose d'une prise dans ses locaux par France Télécom. La plupart des entreprises possédant un autocommutateur (PABX) sont d'ailleurs déjà raccordées par Numéris.

Le service Numéris de France Télécom s'arrête au point dit de terminaison du réseau en général juste à l'intérieur du bâtiment par une T.N.R. (T.N.R. pour l'accès de base isolé, T.N.R.G pour l'accès Duo)

Le rôle de la T.N.R. (Terminaison Numérique de Réseau) est d'assurer l'interface entre la câble (paire téléphonique) de votre installation ou "bus S0" sur lequel viennent se raccorder vos terminaux et le réseau Numéris.

ADSL :

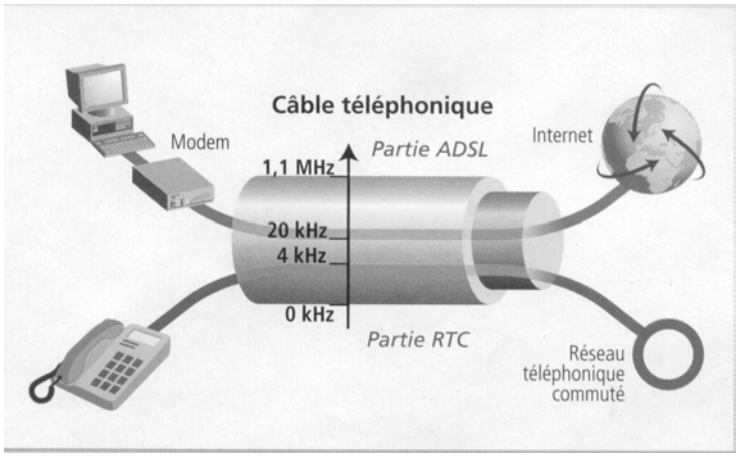
Elle fait partie des liaisons commutées malgré sa tarification « forfaitaire » du fait que on peut accéder à n'importe quel point du réseau ADSL (n'importe quelle autre machine servant une connexion ADSL) et du fait que la liaison n'est pas vraiment permanente. En effet pour éviter les postes qui resteraient en ligne 24/24 France télecom procède aujourd'hui à une déconnexion systématique et « sauvage » toutes les 24h !

Technologie :

Dans la chaîne de communication qui relie le modem au reste du monde , le point faible se situe sur la partie reliant le modem du particulier au central téléphonique.

Cette liaison est constituée de fils de cuivre qui , croit-on , ne peuvent supporter des vitesses de communication que de quelques dizaines de Kbps. En fait , les possibilités des fils de cuivre ne sont pas utilisées a l'optimum car le réseau téléphonique a d'abord été conçu pour transporter de la voix dans cette optique, la bande passante utilisée par les équipements de communication classiques est **bridée à 3.3 Khz** .

Or , les caractéristiques physiques des lignes d'abonnés permettent en réalité de supporter la transmission de signaux à des fréquences de l'ordre de **1 Mhz** .



En modifiant le filtre qui bride la bande passante au **niveau du central téléphonique** et **chez l'utilisateur**, la ligne ainsi optimisée supporte la transmission de données à hauts débits.

Techniquement cette modification nécessite **l'ajout d'un modem particulier à la sortie de votre prise de téléphone murale** et également **à l'intérieur des autocommutateurs de l'opérateur** (actuellement France Télécom).

Mais un autre facteur rentre en jeu la **distance** qui sépare l'utilisateur du central téléphonique de l'opérateur. En effet plus la distance est importante, moins le taux de transfert est élevé. En pratique, pour que l'ADSL fonctionne, la **boucle locale** ne doit pas dépasser six kilomètres, ce qui est le cas pour **80 % des usagers** du téléphone en France.

Mais si dans l'absolu, à 5,5 km le débit tourne autour de 1,5 Mbits/s, à 1 km autour de 6 Mbits/s et à 300m au dessus de 50 Mbits/s, les débits moyens constatés sont actuellement de **2 Mbits/s en réception** et **de 600 Kbits/s en émission**.

Cette asymétrie, qui réserve pour le flux central/abonné une bande passante supérieure au flux abonné/central, est tout à fait adaptée à la consultation de documents multimédia de type vidéo ou son en direct.

Néanmoins Il est facile d'imaginer les possibilités offertes par de tels débits en les comparant à ce qui est aujourd'hui disponible avec un modem V.34...

Un petit comparatif permet de visualiser l'écart important

norme	**Emission**	**réception**
v90	33.6 Kbits/s	56 Kbits/s
RNIS	64 (voir 128) Kbits/s	64 Kbits/s (voir 128 Kbits/s)
ADSL	16 à 640 Kbits/s	1,5 à 9 Mbits/s
HDSL/SDSL	1.544 Mbits/s	1.544 Mbits/s
VDSL	1.5 à 2.3 Mbits/s	13 à 52 Mbits/s

Les technologies qui permettent cette prouesse sont appelées "xDSL" et sont toutes dérivées de la technologie DSL utilisée dans le cadre de liaisons numériques RNIS (le type de codage utilisé pour les transmissions xDSL est le même que pour le RNIS).

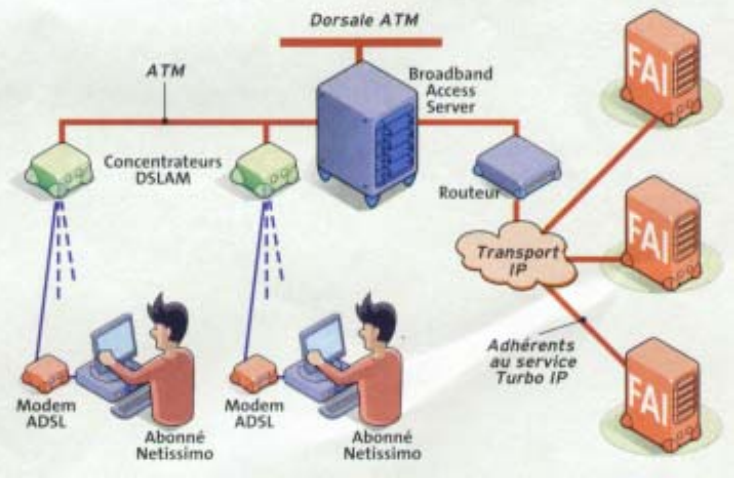
Le terme xDSL se décline en quatre sous-groupes : HDSL , SDSL , ADSL et VDSL

A chacun de ces sous-groupes correspondent une utilisation et des caractéristiques particulières . en fait , le choix d'une technologie est soumise à plusieurs paramètres : les services proposés , la distance , séparant le central de l'abonné , le débit voulu et le caractère symétrique ou non de la liaison.

Technique DSL	Nombre de paires	Débit	Portée max. en km
VDSL	2	De 2 Mbit/s à 53 Mbit/s	2
HDSL (code en ligne 2B1Q)	2	784 kbit/s par paire	3,5
HDSL (code en ligne 2B1Q)	2	1 Mbit/s par paire	3
HDSL (code en ligne CAP)	1	2 Mbit/s par paire	3
SDSL	1	De 192 kbit/s à 2 Mbit/s	3
ADSL (code en ligne : CAP)	1	2 Mbit/s, réception 16 kbit/s, émission	6
ADSL (code en ligne : DMT)	1	8 Mbit/s, réception 640 kbit/s, émission	6

ADSL repose sur des liaisons ATM au eau des liaisons entre ses concentrateurs DSLAM…), le traffic ATM entre plusieurs DSLAM étant géré par un BAS…

Pour offrir un accès ADSL Netissimo, France Télécom doit tout d'abord installer chez l'abonné un filtre et un modem ainsi qu'une unité DSLAM (Digital Subscriber Line Access Multiplexer) au sein du central téléphonique dont dépend la ligne. Chaque DSLAM couvre *n* lignes ADSL et chaque serveur BAS (Broadband Access Server) supervise le trafic ATM d'une dizaine de DSLAM. Enfin, les paquets IP sont livrés à travers un routeur aux FAI adhérant au service turbo IP.



Abonnement :

Il existe des abonnements auprès de France télécom, mais d'autres fournisseurs désormais proposent leur formule…(même si parfois ceux-xi peuvent être génés par la structure ATM de France télécom…)

Dans ce contexte, de nouvelles offres paraissent régulièrement…

Parfois l'offre ADSL est une offre complète comprenant l'accès à la technologie ADSL et le FAI ADSL (voir les offres de Yahoo et Altavista). France Telecom fut la première société à créer un opérateur ADSL : Netissimo. Maintenant Mangoosta est également sur les rangs mais leur offre est moins étendue sur le territoire français que l'offre de Netissimo.

Désormais, les fournisseurs d'accès à Internet ADSL proposent de nouvelles offres appelées packs. Les packs comprennent l'achat d'un modem et un abonnement mensuel (souscrit pour un an minimum) suffisant pour surfer avec l'adsl

Le choix d'un fournisseur est délicat, voici un extrait de comparatif, et une adresse

	Modem		prix	filtres	adresses	Espace
	type	prix	mensuel	fournis	mails	web
Club-Internet	**USB**	**990**	**295**	**3**	**N/C**	**N/C**
Infonie	**USB**	**990**	**299**	**2**	**5**	**50**
Liberty Surf	**USB et Eth**	**995**	**295**	**3**	**illimité**	**100**
Mangoosta	**USB ou Eth**	**990/1250**	**290**	**N/C**	**N/C**	**N/C**
Wanadoo	**USB ou Eth**	**990**	**298**	**3**	**5**	**15**

http://www.adsl-offres.net

France télécom - Netissimo 1

est adapté à des usages monoposte, notamment pour les particuliers gros consommateurs d'Internet.

Interface : Ethernet. Débit des connexions de 500 kbit/s IP crête dans le sens descendant et 128 kbit/s dans le sens remontant.

Son prix est de 265 F TTC/mois + 45 F TTC/mois de location d'un modem (abonnement à votre service Internet non compris).

France télécom - Netissimo 2

peut être utilisé sur plusieurs postes et convient aux PME et petits sites d'entreprises.

Interface Ethernet ou ATM Forum avec 1 Mbit/s IP crête dans le sens descendant et 256 kbit/s dans le sens remontant.

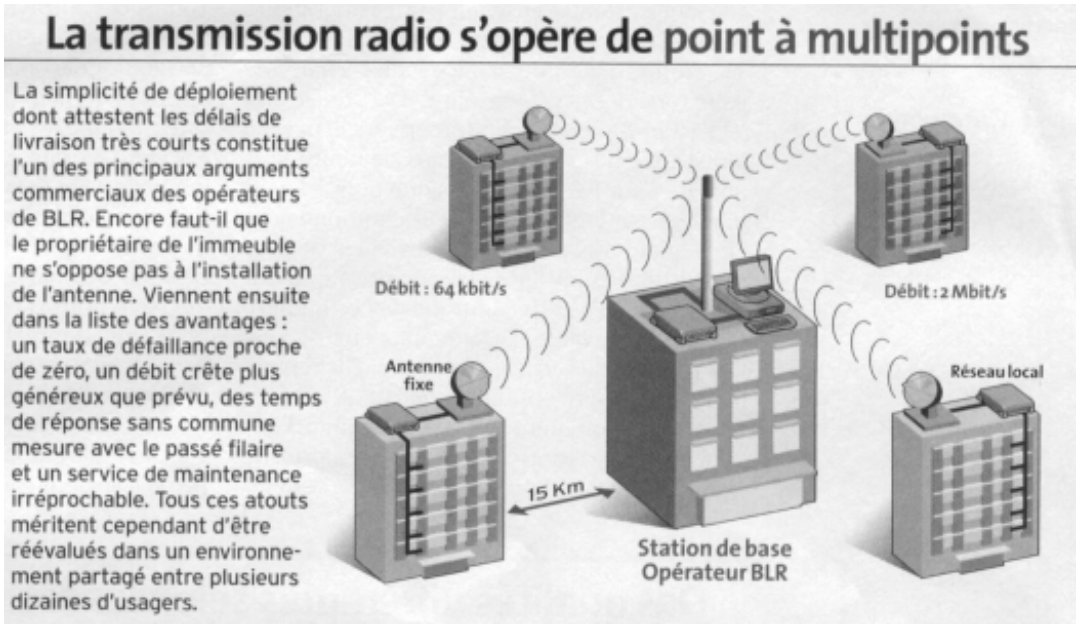
Son prix est de 700 F HT/mois modem inclus (abonnement à votre service Internet non compris).

BLR La Boucle Locale Radio :

La boucle locale radio WLL (Wireless Local Loop) en anglais est un moyen pour un opérateur de télécommunication de relier directement l'abonné à ses équipements en passant par une liaison radio (faisceau hertzien) au lieu d'utiliser les fils de cuivre

La B.L.R. est une technologie de connexion sans fil, fixe et bidirectionnelle:

- ✓ sans fil: utilisation des ondes radio comme moyen de transmission,
- ✓ fixe: le récepteur doit être fixe, il ne peut être mobile comme dans le cas du GSM,
- ✓ bidirectionnelle: la liaison se fait dans les deux sens opérateur client et client opérateur.



Voici, pour la bande des 3,5 Ghz, les distances entre la station de base et l'antenne du client:

zone d'habitation	distance
urbaine (ville)	3,4 Km
suburbaine (banlieue)	5,1 Km
rurale (campagne)	8,9 Km

La portée varie de 5 à 15 km en fonction de la fréquence et du terrain (les antennes doivent être à vue directe)

Avec la gamme de fréquence 3.5GHz les ondes réussissent à traverser les bosquets d'arbres.

Il n'existe pas de norme ouverte point-multipoints. Américains, Japonais et Européens souhaitent imposer leur norme.

Aucun norme ne peut répondre à toutes les demandes (types d'application, zones géographiques).

DECT

Norme européenne. faible portée, approprié aux zones les plus denses

CDMA

Mis au point par Motorola

PHS

Standard Japonais. Utilisé comme téléphone mobile de ville.

CT2

Normalisé en interface radio

GSM

Norme de la téléphonie mobile

DCS 1800

Portée plus faible que le GSM, mais trafic plus élevé; Norme pour les centres urbains denses à fort trafic.

avantages pour les utilisateurs ?

- 40 fois plus rapide qu'un modem classique : débit maxi 2Mbits/s
- Débit constant : chaque internaute dispose de son propre canal de communication
- connexion permanente
- abonnement 20 à 40% moins cher que l'ADSL
- Couverture nationale
- Raccordement provisoires et possibles (expositions , catastrophes,...)

inconvénients pour les utilisateurs ?

- Sensibilité aux conditions météorologiques : chute de débit de 30%
- Nécessité de vue directe entre les antennes (20-40% des habitations situées dans des zones d'ombres ne seraient pas couvertes). Les signaux ne peuvent pas traverser les obstacles entre les antennes émettrice et réceptrices.
- Les opérateurs sont obligés de suivre un plan de mise en place jusqu'en 2004, mais après ils n'ont plus d'obligation d'extension. Les zones à forte densité de population seront équipées avant les zones faiblement peuplées. Fin 2001, 52 % de la population dans les villes de plus de 50 000 habitants en Ile-de-France pourront bénéficier d'un accès à la BLR, contre seulement 5 % des habitants de la Franche-Comté. Le bon exemple est l'abandon des licences régionales pour la corse et l'auvergne.

Rythme de couverture

En France c'est l'ART (Autorité de Régulation des Télécommunications) qui gère l'attribution et l'exploitation des licences de la boucle locale radio.

L'ART à ouvert le dossier en 1996 en observant les expérience anglaises et allemandes.

Il existe 2 types de licences: les licences nationales et les licences régionales.

Les licences nationales : couvrant le territoire national, au nombre de 2 dans les bandes 3,5 Ghz (plus adaptée au densité de population faible débit de 512kbits/s à 1 Mbits/s) et 26 GHz. (dans les agglomérations débits jusqu'à 2Mbits/s)

- Firstmark Communication France
- Fortel

Les licences régionales : Dans chacune des des 22 régions du territoire métropolitain, 2 licences dans la bande des 26 GHz.

Dans chaque départements d'outre mer (Guadeloupe, Martinique, Guyane, Réunion), 2 licences dans la bande des 3,5 GHz.

Cela signifie théoriquement qu'en tout point du territoire métropolitain 4 opérateurs proposeront une connexion en BLR

- Belgacom
- Broadnet France
- Landtel : proposera une offre groupée téléphone + internet à 64 kbits/s pour 206F / mois
- BLR Services

Les régions Corse et Auvergne ont été désertées par les opérateurs désignés un nouvel appel d'offre à du être lancé !

TECHNOLOGIE DES LIAISONS SPECIALISEES

Si les réseaux publics sont à la disposition des utilisateurs pour échanger des données informatiques, on peut "louer" carrément une ligne

Cela peut être des lignes louées qui permettent la transmission de données à moyens ou à hauts débits (2,4 Kbits/s à 140 Mbits/s) en liaisons point à point ou multipoints (c'est ce que l'on appelle le service Transfix).

Les 3 ls les plus répandues sont les T1 (1.5Mbits/sec), les T2 (6Mbits/sec), et les T3 (45Mbits/sec), mais le prix élevé de 10 000 F à l'installation puis 10 000F/mois, peut être dissuasif…

Il existe également des ls qui vont nettement plus vite. C'est le cas des E1 (2Mbits/sec), E2 (8Mbits/sec), E3 (34Mbits/sec), et E4 (140 Mbits/sec).

On l'a déjà dit, mais il faut le répéter. On ne sait jamais exactement quelle technologie est réellement employées, dans le sens ou ne prends pas une liaisons X25 ou ATM (même si on peut s'en douter) mais plutôt une liaison via Transfix, ou Oléane, par exemple… De part le prix que couterait un « raccordement » sur un réseau en Frame Relay ou ATM, seule des entreprises comme ST électronique, Merlin, Schneider etc opèrent cette démarche. De manière générale on prends une **LS** et on ne se préoccupe pas de la technologie !

En fait on choisit un « débit », avec une « offre commerciale », et non pas une technologie !

De chaque coté de la liaison, il faut un routeur avec 2 cartes , au milieu, le réseau France télécom avec ses technologies…

• 1 carte **Ethernet** + **tcp/ip** vers le réseau local • 1 carte de la technologie à utiliser : **Atm** / **X25** / **Frame Relay** / **ADSL**	Réseau France télécom ?	• 1 carte **Ethernet** + **tcp/ip** vers le réseau local • 1 carte de la technologie à utiliser : **Atm** / **X25** / **Frame Relay** / **ADSL**

vont de 155 Mbs à 620 Mbs pour ATM ?

Liaisons analogiques :

Il existe des liaisons spécialisées analogiques (LSA) dites normales (2 fils) ou supérieures (4 fils) mais qui offrent un débit maximal de 64 Kbs ce qui est inutile et plus cher de toute manière que les liaisons numériques (Numeris), de nos jours.

Il NE FAUT PLUS LES UTILISER.

X25 (transpac):

Il faut dire que maintenant, Transpac s 'appuit sur X25, mais aussi sur Frame Relay et ATM, (tout comme on l'a vu ADSL repose sur ATM au niveau des liaisons entre ses concentrateurs DSLAM…)

France télécom à tous ses commutateurs en X25, et a fait longtemps de la « résistance » par rapport au technologies Frame Relay, ou ATM.

Caractéristiques :

La technique étant celle de la commutation par paquets, les données issues du terminal d'un abonné sont découpées en paquets auxquels sont ajoutés des données de service permettant l'acheminement vers le destinataire.

Il existe 2 types de paquets, des paquets de données, et des paquets de service (connexion, de connexion…).

Le paquet de connexion établit un circuit virtuel (c'est à dire un chemin qui persiste pendant toute la durée de la connection). Une fois le chemin virtuel crée, les paquets de données ne possèdent plus l'adresse du destinataire, mais indiquent simplement un numéro de chemin. Ce numéro reste constant pendant toute la communication, même si le coup d'après, il sera différent.

En X25, on fait un vérification au niveau de la couche liaison et couche réseau, ainsi que de la couche physique . C'est plus rapide car on vérifie pas la couche transport (puisque le chemin est unique pendant la session)!

N'empêche que on continue à faire un certain nombre de vérifications, car cette technologie date da la paire cuivrée, et qu'il y avait avec cette technologie pas mal d'erreurs de transmissions….

X25 utilise la technique du circuit virtuel soit commuté soit permanent, selon le type de liaison que l'on a choisit lors de l'abonnement.

Différents protocoles ont étés définis, le mode de transmission pouvant être synchrone ou asynchrone, ce sont les **PAD** Packet Assembly Disassembly qui ont pour rôle d'assembler les caractère émis par le terminal et de les désassembler à la réception.

Pourquoi les débits varient de 64 Kbs à 2 Mbs pour X25

Relai de trame (Frame relay) :

Le relais de trame est une évolution simplificatrice de la commutation par paquet X25

Caractéristiques :

C'est un service fondé sur l'établissement, pour chaque besoin d'interconnexion, d'une Connexion Virtuelle Permanente (CVP) entre deux sites client.

Le routage se fait de façon identique, mais sans s'assurer de l'intégrité des données

A partir du moment ou la technologie est à base de fibre optique, on constate beaucoup moins de perte de données, donc en fait on fait des vérifications en moins. Au point que en Frame Relay, des que l'on a établit le réseau (circuit virtuel) on ne s'occupe plus du tout du contrôle, on transmet juste des paquet avec un numéro de chemin virtuel.

La trame est par conséquent beaucoup plus simple q'une trame X25

Frame Relay est essentiellement utilisé sur des liaisons spécialisées.

Le débit s'établis autour de 34 Mbs pour Frame Relay

ATM (Asynchronous Transfer Mode):

Autre variante de commutation par paquet, ses paquets sont courts et de taille fixe, appelé cellules. Au moment de la définition du standard, les européens pronaient une longueur de paquet fixée à 32 octets, et les américains souhaitaient 64 octets. On a fixé un compromis à 48 octets !

Seul l'en tête est analysé pour permettre les acheminements dans les routeurs, aucun contrôle de flux ou de d'erreur n'est effectué, tout est laissé à la charge des couches supérieures.

Les routeurs ATM sont plutôt appelés Commutateurs ATM, car de fait ils n'effectuent aucun contrôle d'erreur, et ne s'occupent que de transmettre le plus rapidement des paquets de taille fixe sur le bon numéro de chemin. Leur logique peut être câblée !

Sur les Micro ordinateurs, ATM en carte réseau n'a jamais véritablement vu le jour, en effet les constructeurs ont proposé des cartes avec des débits non compatibles entre eux , variant de 16, à 32 ou 50 Megabit, et parallèlement le standard Ethernet 100 Megabit est sorti à un pris défiant toute concurrence…

Résumé :

En X25 :

la trame contient 32-64-128-256 octets, on échange des paquets de taille connue. Des corrections importantes sont effectuées car cette technologie date de la paire cuivrée, relativement peu fiable. On effectue des vérifications au niveau de la couche physique, liaison et réseau.

Débits classiques de 64 kilo à 2 Mega

En Frame Relay :

la trame peut contenir des milliers d'octets, on échange des trames de longueur variable. Cette technologie datant de la fibre optique, beaucoup plus fiable, peu de corrections sont effectuées. On effectue des vérifications au niveau d'une couche spécifique dite noyau en plus de la couche physique.

Débits classiques de 34 Megabits (8 Megabits en France)

En ATM :

La trame est composée de paquets de longueur identiques, fixée à 48 octets, que l'on appelle des cellules. Tous les paquets faisant la même taille, le traitement se fait de manière automatique. Les corrections d'erreur n'étant pas prises en charge, on peut faire de la logique câblée de manière à accélérer au maximum la vitesse de transmission, on parle de commutateur ATM.

Débits classiques de 155 Mega à 620 mega

Par comparaison, en IP on est en mode non connecté, et tous les paquets ont le numéro de machine de destination… deux paquets qui se suivent n'empruntent pas forcément le même chemin. La taille du paquet est de 65000 octets !

En IP, on fait un vérification au niveau de la couche transport, de la couche liaison et couche réseau, ainsi que de la couche physique . C'est moins rapide car on vérifie pratiquement toutes les couches !

L'ASPECT « COMMERCIAL » DES LS

Transfix - Transfix2 - Transfix HD :

Transfix est une offre de liaisons louées numériques point à point, permanentes et réservées à votre usage exclusif, qui vous permettent de communiquer entre deux sites

Particulièrement adapté aux échanges longs et fréquents, Transfix est destiné aussi bien au transfert des données informatiques et d'images - animées ou non -, qu'aux communications téléphoniques. En effet l'abonnement étant forfaitaire. Vous pouvez communiquer aussi longtemps que vous le souhaitez sans incidence sur le coût

Le contrat Transfix inclut la fourniture, l'installation et la maintenance de tous les équipements liés au service.

Transfix est l'offre la plus large du marché, de 2,4 kbit/s à 155 Mbit/s. Vous pouvez choisir les débits suivants :

Sous l'appellation **Transfix** avec un débit à :
2,4 ; 4,8 ; 9,6; 19,2 ; 64 ; 128 ; 256 ; 1.920 ; 1.984 ; 2.048 kbit/s

Sous l'appellation **Transfix HD** avec un débit à :
34 et 155 Mbit/s.

Transfix 2.0 est le nouveau standard d'exigence au sens France Telecom, mais repose fondamentalement sur Transfix. Il ne s'agit que d'une variation sur la livraison rapide, la garantie de réparation en moins de 4 heures et autres "services".

Abonnement :

Contrat à durée indéterminée

Le contrat est signé pour une durée indéterminée. Il est souscrit pour une durée minimale d'un an.

Contrat longue durée de 3 ans ou 5 ans

Le contrat longue durée permet de bénéficier de 10% ou de 15% de réduction sur l'abonnement mensuel si vous vous engagez pour une durée de 3 ou 5 ans, respectivement.

Contrat Réseau Longue Durée (CRLD) de 3 ou 5 ans

Le CRLD permet de bénéficier d'avantages tarifaires lorsque vous vous engagez à garder un parc d'au moins 10 liaisons (contrats à durée indéterminée) pendant 3 ou 5 ans.

Tarification :

Le principe de tarification Transfix est de type forfaitaire, Les frais d'établissement dépendent du débit de la liaison. L'abonnement mensuel dépend du débit et de la distance à vol d'oiseau entre les sites à relier.

La durée des communications et la quantité des données échangées n'ont donc aucune incidence sur le coût.

Transfix

Prix HT en Euros au 1/1/2000 hors remises

Frais d'établissement par extrémité

Débits	2,4 - 4,8 9,6 - 19,2 64 - 128 kbit/s	256 kbit/s	1920 1984 2048 kbit/s
Montant (H.T.)	609,80	1 067,14	3 048,98

Abonnement mensuel pour une durée minimale d'abonnement de 12 mois
Par liaison louée, en fonction du débit et la distance "d" en kilomètres indivisibles.

Débits / Distance	1 à 10 km	11 à 50 km	51 à 300 km	Plus de 300 km
2,4 - 4,8 - 9,6 kbit/s	134,31 + 16,16 d	237,97 + 5,79 d	481,89 + 0,91 d	619,10 + 0,46 d
19,2 kbit/s	245,60 + 12,96 d	337,06 + 3,81 d	481,89 + 0,91 d	619,10 + 0,46 d
64 kbit/s	208,86 + 10,82 d	285,08 + 3,20 d	409,33 + 0,72 d	500,80 + 0,41 d
128 kbit/s	282,03 + 14,64 d	385,24 + 4,31 d	552,17 + 0,98 d	643,64 + 0,67 d
256 kbit/s	520,92 + 27,90 d	714,07 + 8,58 d	1 056,29 + 1,74 d	1 170,81 + 1,36 d
1920 - 1984 kbit/s	605,22 + 50,00 d	895,64 + 20,96 d	1 494,00 + 8,99 d	2 792,87 + 4,66 d
2048 kbit/s	634,19 + 52,44 d	929,94 + 22,87 d	1 554,98 + 10,37 d	3 109,96 + 5,18 d

Transfix HD

Prix HT en Euros au 1/1/2000 hors remises

Frais d'établissement par extrémité

34 Mbit/s 155 Mbit/s	site déjà raccordé en optique	site sans raccordement optique
de 1 à 5 km	3 048,98	4 573,47
plus de 5 km	12 195,92	15 244,90

Abonnement mensuel pour une durée minimale d'abonnement de 12 mois
Par liaison louée, en fonction du débit et la distance "d" en kilomètres indivisibles.

34 Mbit/s	1 à 10 km	11 à 30 km	31 à + 300 km	> 300 km
zone A - zone A	3 048,98 + 670,78 d	6 707,76 + 304,90 d	14 482,66 + 45,73 d	14 482,66 + 45,73 d
zone A - zone B	3 048,98 + 670,78 d	6 707,76 + 304,90 d	13 339,29 + 83,85 d	24 772,97 + 45,73 d
zone B - zone B	3 048,98 + 670,78 d	6 707,76 + 304,90 d	12 607,53 + 108,24 d	31 358,76 + 45,73 d

155 Mbit/s	1 à 10 km	11 à 30 km	31 à + 300 km	> 300 km
zone A - zone A	9 299,39 + 1 143,37 d	19 361,03 + 137,20 d	20 687,33 + 92,99 d	20 687,33 + 92,99 d
zone A - zone B	9 299,39 + 1 143,37 d	19 361,03 + 137,20 d	17 988,98 + 182,94 d	44 972,46 + 92,99 d
zone B - zone B	9 299,39 + 1 143,37 d	19 361,03 + 137,20 d	15 244,90 + 274,41 d	69 669,20 + 92,99 d
	3 430,10	si les deux sites extrémités sont sur le même nœud de raccordement		

Agglomérations appartenant à la zone A:
L'Ile de France dans sa globalité et Amiens, Annecy, Bayonne, Besançon, Bordeaux, Caen, Clermont-Ferrand, Dijon, Grenoble, Le Mans, Lille, Lyon, Marseille, Montpellier, Nancy, Nantes, Nice, Orléans, Poitiers, Reims, Rennes, Rouen, Toulon, Tours, Toulouse et Strasbourg.
Le reste du territoire métropolitain constitue la zone B.

Transpac (X25) :

Transpac est le nom commercial donné par France Télecom pour un réseau utilisant une technique de transport d'information par paquet connue sous l'appellation X25.

Accès direct

Les accès directs X.25 sont adaptés aux applications nécessitant des échanges de données sûrs, fiables, sans erreur et en toute sécurité. Ils assurent une connectivité universelle, permettant d'établir des communications avec tout abonné de France Télécom ou de Global One ainsi que tout utilisateur d'un réseau public X.25 relié au Noeud de Transit International.

Les accès directs par liaison louée couvrent la gamme de débits de 14.400 bit/s jusqu'à 256 Kbit/s et plus.

Les accès via le canal D de Numéris à travers une liaison logique permanente à 9,6 Kbit/s constituent un deuxième type d'accès direct qui est parfaitement adapté aux applications à faible trafic

Accès indirect

L'accès au réseau France Télécom s'effectue via le Réseau Téléphonique Commuté (RTC) ou le RNIS - Numéris en France -, en utilisant des numéros nationaux.

Les accès indirects permettent des communications en mode Asynchrone, couvrant la plage de débit de 300 à 28.800 bit/s, ou des communications en mode Synchrone de 2.400 à 14.400 bit/s par le RTC, ou 64 Kbit/s par le canal B RNIS.

Pour accéder de façon simple et transparente aux serveurs d'entreprise sans se soucier de la localisation géographique de ces serveurs, le service de liaisons groupées généralisées de France Télécom apporte une solution sûre et compétitive.

La sécurisation des sites centraux peut être renforcée par le service de transfert d'appel généralisé, permettant un basculement automatique sur des sites de secours en cas de dérangement.

Des facilités d'adressage, par allocation de numéro court, de numéro garanti ou de tranches d'adresses réservées, apportent une grande souplesse dans la définition et la gestion du plan d'adressage du réseau d'entreprise. De plus, des mécanismes de contrôle d'accès ou de reroutage viennent renforcer la sécurité du réseau.

Les services de réseau intelligent proposés par France Télécom contribuent à améliorer la gestion quotidienne et la sécurisation des réseaux d'entreprise

Services de secours

Une large gamme de services pour satisfaire la diversité des besoins des réseaux d'entreprise et garantir une disponibilité permanente de l'accès au système d'information, tel est l'objectif des services de secours proposés par France Télécom :

- Secourir un accès direct par basculement automatique de la liaison physique sur le RTC ou RNIS
- Secourir un accès à un concentrateur X25 ou un routeur par un Accès Personnalisé Synchrone via un canal B RNIS
- Secourir un site central par reroutage automatique des communications sur un autre site central en cas de dérangement
- Permettre l'établissement des communications via un autre commutateur
- Mettre en oeuvre une procédure multiliaison sur un faisceau de lignes.

Tarification (extraits):

L'abonnement à TRANSPAC dépends de si on prends un accès direct via LL ou via numéris

1. ACCÈS DIRECTS X25

Principe tarifaire : Le prix total du service est composé du prix de l'accès, des éventuels services complémentaires et du prix des communications sur le réseau.

1.1. ACCÈS DIRECT PAR LIAISON LOUÉE (LL).

1.1.1. Abonnement mensuel France

L'abonnement mensuel comprend la liaison d'accès au réseau.

Débit d'accès	Prix mensuel	Caractéristiques de commercialisation
≤ 14 400 bit/s	1 630 F	(accès 14,4 K recommandé)
19 200 bit/s	2 200 F	
48 Kbit/s	2 700 F	(sur étude, accès 64 K recommandé)
64 Kbit/s	2 400 F	
128 Kbit/s	4 700 F	(-)
256 Kbit/s	9 200 F	(-)

Durée initiale d'abonnement : 6 mois.

Pour les débits supérieurs, de 512 Kbit/s à 2 Mbit/s, consulter votre Agence Commerciale.

Nota : Le prix est indépendant de la distance pour les débits inférieurs ou égaux à 64 Kbit/s. Pour les débits supérieurs à 64 Kbit/s, si la distance est supérieure à 15 km, consulter votre Agence Commerciale.

1.1.2. Frais de mise en service et de modification pour accès direct France

Frais de mise en service :

Débit d'accès	mise en service
≤ 128 Kbit/s	10 500 F
256 Kbit/s	16 000 F

Ces frais sont également applicables lorsqu'il y a modification de débit.

Via LL ou numéris

1.2. ACCÈS DIRECT PAR CANAL D NUMÉRIS EN FRANCE

Le prix de l'accès est composé d'un abonnement au service et du trafic émis ou reçu de l'équipement.

1.2.1. Service d'accès direct par canal D

- Abonnement au service :
  par Liaison Logique Permanente (LLP) : 380 F/mois
- Mise en service de l'accès direct ou modification de l'accès avec reconstruction de LLP :
  par Liaison Logique Permanente (LLP) : 2 000 F
- Modification de l'accès sans reconstruction de LLP : 300 F

1.2.2. Trafic émis ou reçu de l'équipement

- Transit du trafic émis ou reçu par l'équipement : 0,052 F/Koctet

NB : Le prix du transfert d'information sur le réseau Transpac est facturé séparement suivant le tarif du § 1.4.

1.2.3. Adaptateur X25/canal D Numéris (ATD)

- Location maintenance de l'adaptateur ATD : 200 F/mois
- Mise en service de l'adaptateur : 1500 F

1.3. SERVICES COMPLÉMENTAIRES POUR ACCÈS DIRECTS

1.3.1. Voies logiques (VL), accès multivoies.

- Par voie logique, à compter de la 2ème et suivantes : 28 F/mois

1.3.2. Groupe Fermé d'abonné (GFA),

- Par abonné, et par GFA souscrit, y compris le groupe commun : 28 F/mois
- Création du GFA : 560 F

Si l'abonné n'a que le groupe commun, celui-ci n'est pas facturé.

L'abonnement à TRANSPAC dépends si on prends un accès indirect

2. ACCÈS INDIRECTS X25

Principe tarifaire : le prix total du service est composé du coût des réseaux d'accès, au tarif de l'opérateur local, et du prix du service facturé par Transpac.

2.1. COÛT DES RÉSEAUX D'ACCÈS FRANCE

Les abonnements aux réseaux Telex, Téléphonique ou Numéris sont facturés par France Télécom. Les communications sur ces réseaux sont facturées en entrée par France Télécom et, en sortie, par Transpac.

- Telex (-) :

En entrée depuis la Métropole :

- Sur le numéro national : tarif Télex de la zone locale,
- Sur les numéros de secours : tarif Télex normal.
- En entrée depuis l'étranger ou les DOM : tarif Télex du réseau appelant vers la Métropole.
- En sortie : tarif de la zone locale vers la Métropole, ou tarif Télex International ou DOM ou TOM depuis la Métropole.

- Teletel :

- Télétel 0 : accès gratuit (numéro vert de France Télécom)
- Télétel 1 : une Unité Télécom toutes les 6 mn pour T1, une Unité Télécom toutes les 3 mn pour T3.

- Téléphone et Numéris canal B (-)

- Pour les Entrées Banalisées sur les numéros d'appel nationaux, les Sorties Banalisées ou les Accès Personnalisés : tarification à la seconde d'utilisation, avec la modulation horaire selon les tarifs de France Télécom.

Le minimum facturé de 0,615 F par appel, donne droit à 111 secondes de communication. Au-delà de cette durée forfaitaire, la communication est facturée 0,332 F/mn.

2.2. ACCÈS TÉLEX ET TÉLÉTEL EN FRANCE

Le prix du service est composé du prix de la porte d'accès au réseau et du prix des communications selon § 2.3.4.

Le prix de la porte est facturé pour le compte de France Télécom et selon ses tarifs.

Prix de la porte pour les Entrées et Sorties Banalisées de Transpac :

		F/mn	Entrées	Sorties
Télex (-)		0,55	EBTX (1)	SBTX
Télétel 0	- 3605 (1), (2), (3)	0,29	T0	
Télétel 1	- 3613 (1)	0,17	T1	
	- 3613 (1)	0,07	T3	

(1) Facturé à l'appelé.
(2) Minimum de facturation : 0,60 F par communication établie.
(3) Abattement de 0,0725 F/mn de connexion au-delà de 10 000 heures par mois.

La tarification pour TRANSPAC ne dépends pas de la distance mais du volume et de la durée.

On transmet des paquets, et cela revient environ à 0.04 centime le Kilo Octet soit 4 Francs le Mega Octet. Cela laisse à penser que si cela peut être satisfaisant pour du texte, c'est prohibitif pour de la vidéo !

1.4. COMMUNICATIONS EN FRANCE POUR ACCÈS DIRECTS

Les communications sont facturées selon le mode Circuit Virtuel Commuté (CVC).

1.4.1. Circuit virtuel Commuté (CVC)

1.4.1.1. Tarification du CVC

Le mode CVC est facturé selon le volume, dont l'unité est le Koctet (ou Ko ; un Koctet = 1 024 octets).

- Le volume minimum facturé par communication est de 3 200 octets. Pour la facturation, les volumes sont arrondis, par tranche horaire, au Koctet supérieur.
- Pour les TOM, le CVC est facturé selon deux composantes : le volume, et la durée qui est facturée à la minute.

	Trafic local (a)	Trafic DOM (b)	Trafic TOM (c)
Volume	0,048 F/Koctet	0,093 F/Koctet	0,46 F/Koctet
Durée	gratuite	gratuite	0,55 F/mn

(a) Le tarif local s'applique aux communications échangées à l'intérieur de la Métropole, d'un TOM ou d'un DOM et aux communications échangées entre la Guadeloupe et la Martinique.
(b) Le tarif DOM s'applique aux communications échangées entre les DOM, sauf exception ci-dessus, ou entre les DOM et la Métropole.
(c) Le tarif TOM s'applique aux communications échangées entre les réseaux Transpac Polynésie ou Transpac Nouvelle-Calédonie et le réseau Transpac Métropole et DOM, et facturées en Métropole ou dans les DOM.

1.4.1.2. Dégressivité du prix du volume sur une même facture bimestrielle

Le trafic LVU (§ 1.4.2) n'est pas compris dans le volume total pour le calcul de la dégressivité. Par contre, le volume lié aux accès indirects est cumulé avec celui des accès directs (§ 2.3.4 et § 2.4.4).

Frame Relay :

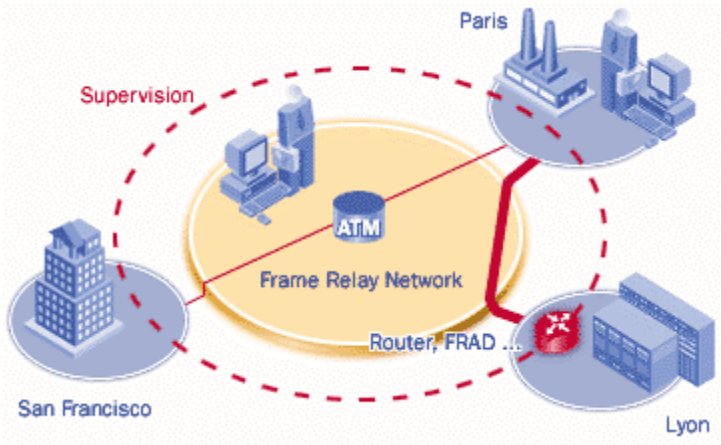
Le service Frame Relay s'appuie sur le réseau partagé de France Télécom dont le backbone est constitué de commutateurs ATM partageant des artères de débit allant jusqu'à 2,5 Gbit/s et se prolonge à l'international via le service Global Frame Relay de Global One.

En France, tout d'abord, le service Frame Relay bénéficie d'une couverture très dense : plus de 150 points de présence, répartis de manière homogène sur le territoire. Au delà, grâce au service Global Frame Relay de Global One, France Télécom offre un service Frame Relay mondial basé sur environ 900 points d'accès dans plus de 50 pays.

Cette infrastructure permet d'offrir un service aux performances particulièrement élevées, avec des garanties concrètes de qualité de service.

- · Les débits d'accès du service Frame Relay peuvent atteindre 8 Mbit/s
- · Le débit minimum garanti (CIR) est choisi entre 4 et 1.024 Kbit/s en fonction des débits d'accès choisis · La disponibilité du réseau est de 99,99%
- · Le temps de transit moyen entre points d'accès en France est inférieur à 40ms

La tarification du service est forfaitaire et indépendante des volumes échangés.



ATM :

Global ATM est une solution de réseau Haut Débit, de 512 kbit/s à 155 Mbit/s, fédérant l'ensemble de vos communications - voix, donnée et multimédia - au national comme à l'international.

Bénéficiant de la technologie ATM et s'appuyant sur le réseau dorsal ATM de France Télécom

Fine granularité des connexions de 512 kbit/s à 155 Mbit/s

Création d'une nouvelle connexion, changement de son débit sur un raccordement existant dans un délai maximum de 7 jours

Accessible partout en France et déjà présent dans 40 pays les interfaces proposées vont de ATM natif à l'adaptation de service (ATM natif, émulation de circuit, Frame Relay, Ethernet...)

La tarification Global ATM se compose :

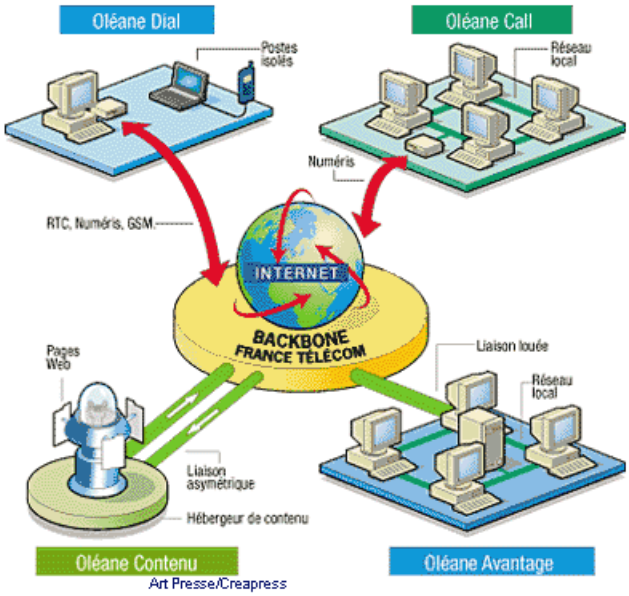
de frais d'accès au service, payables une seul fois et d'un abonnement mensuel forfaitaire qui s'appliquent individuellement à chaque site, raccordement au réseau ATM, et à chaque connexion.

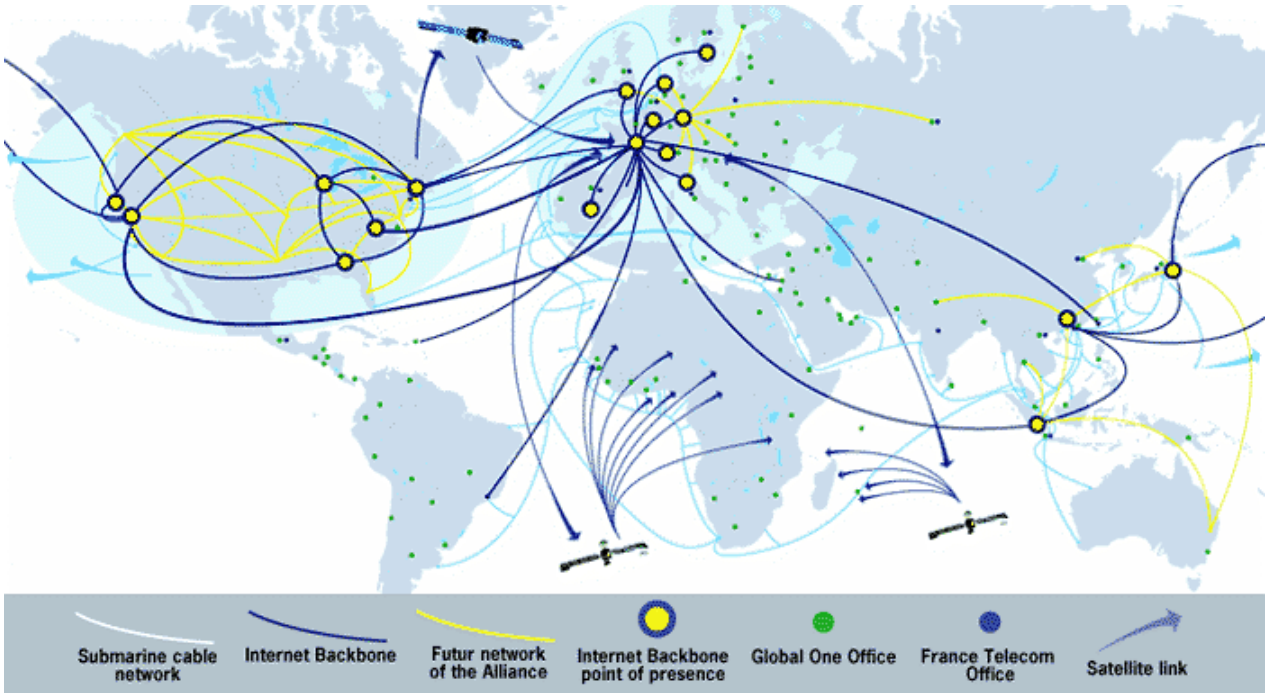
Vous bénéficiez de tarifs dégressifs en fonction des débits et de la durée des contrats. Le débit de vos connexions est ajusté au plus près de vos besoins grâce à une très fine granularité.

Oléane Dial – Call – Contenu - Avantage :

Oléane est l'opérateur professionnel de France télécom pour les communications réseau

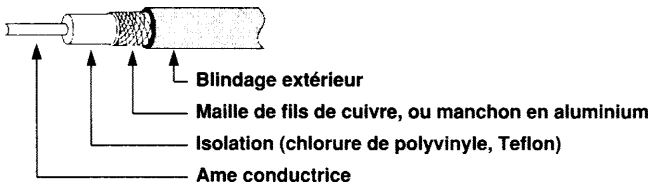
Selon le type de contrat débits – prestations, diverses formules existent…





CABLAGE ETHERNET

Cable Coaxial :



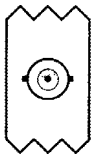
Les câbles coaxiaux les plus courant sont

- **RG11** ou **Ethernet épais** ou **Thicknet** : Il sert généralement d'épine dorsale d'un réseau en Ethernet et réponds au standard 802.3 10Base5.
  Epais, encombrant, il manque de souplesse et coûte cher par rapport aux paires torsadées.
  Offre un débit de 10 Mégabit/s sur une distance de 500 m avec une impédance de 50 ohms.

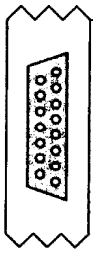
- **RG58** ou **Ethernet fin** ou **Thinnet** : utilisé aux normes 802.3 10Base2.
  Offre un débit de 10 Mégabit/s sur une distance de 185 m avec une impédance de 50 ohms.

N.B: Le câble large bande des réseaux de télévision NE REPONDS PAS AUX NORMES RESEAUX (notamment par son impédance de 75 ohms)

Les prises associées sont :



BNC pour le Thinnet



AUI pour le Thicknet

Un **té de raccordement** placé sur la carte réseau de chaque station ou du serveur sert de point d'arrivée et de départ du **câble coaxial** pour d'autres stations. Chaque station située en fin de réseau est munie d'un **bouchon terminal** nécessaire à une bonne transmission des signaux informatiques

Câble Paires torsadées :

Les paires sont assemblées en câbles multi-paires comportant 2-4-6-8-14-25-56-112-224 paires.

Ils sont conçut ainsi afin de minimiser les interférences avec l'extérieur et les effets de diaphonie.

Câbles STP ou UTP :

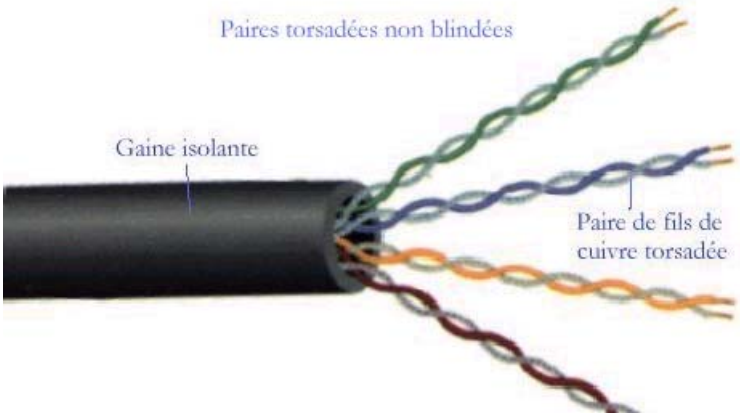
Les câbles à paires torsadées les plus courants sont

- **Paires Torsadées Blindées** ou **STP** ou Shielded Twisted pairs.

Que l'on peut avoir de différentes qualité selon leur bande passante (type 3 ou 5) le type 5 étant la meilleur qualité. Le blindage nécessitant une mise à la masse parfaite entraînant sinon plus de problèmes que d'avantages !

- **Paires Torsadées Non Blindées** ou **UTP** ou Unshielded Twisted pairs.

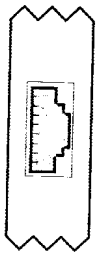
Que l'on peut avoir de différentes qualité selon leur bande passante (type 3 ou 5) le type 5 étant la meilleur qualité.



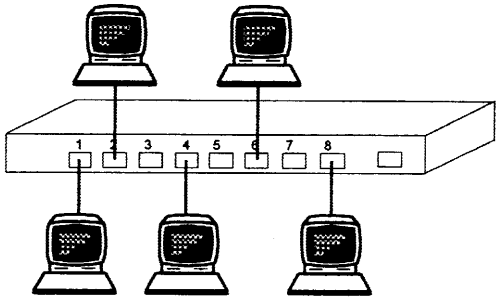
Léger, facile à poser, économique ils n'autorisent pas cependant de très haut débits mais peuvent atteindre 100 Mégabit/s. Sur de longues distances 1Km, ils chuteront sur un débit de 1Megabits/s Extrêmement utilisés sur les réseaux en Etoile avec des Hub.

Les prises associées sont :

Prise **RJ45** pour UTP ou STP (identique visuellement à la RJ11 Téléphonique)



N.B: En Câblage avec des paires torsadées, un réseau même minime doit avoir un Hub.



En effet deux ordinateurs ne peuvent être reliés directement entre eux par une liaison UTP. (il faudrait croiser les paires autrement que dans la configuration classique)

Catégories de câble :

Les différentes qualité de câble paire torsadée sont données par des caractéristiques fort complexes (diaphonie, paradiaphonie, banda passante maximale…

Nous essayerons juste de donner quelques caractéristiques principales, ainsi que leur utilisation standard :

Cordon "Catégorie 3" :

conçus pour du transport de voix/données avec un débit maximal nominal jusqu'à 10 Mhz

A ne plus utiliser aujourd'hui

Cordon "Catégorie 5" :

conçus pour du transport de voix/données avec un débit maximal nominal jusqu'à 100 Mhz

pratiquement toutles les applications peuvent être câblées en UTP cat 3 : modems, RS232, Appletalk, RNIS, T1, E1, Token Ring 4 et 16 Mbs, Ethernet 10BaseT et 100baseT

Cordon "Catégorie 5 améliorée" :

conçus pour du transport de voix/données avec un débit maximal nominal Supérieur à 100 Mhz (dépendant du câble et des applcations)

Cordon "Catégorie 7" :

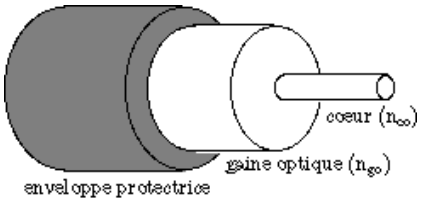
conçus pour du transport de voix/données avec un débit maximal nominal minimal 200 Mhz et supportant le Giga Ethernet sur une distance minimale de 100m.

Fibre Optique :

Chère, difficile à poser elles autorisent cependant des débits de l'ordre de 1 Gigabit/s et un parasitages quasi inexistant, de même qu'une sécurité à toute épreuve !.

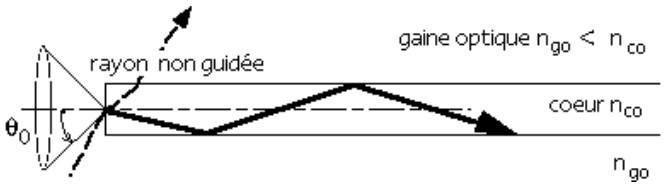
Comment une fibre optique est elle composée ?

En tout premier lieu, une fibre optique est un câble cylindrique qui est fait d'oxyde de silicium (SiO2). Au centre du cylindre, on retrouve le coeur entouré d'une gaine. Le coeur est légèrement dopé pour avoir un indice de réfraction plus élevé que la gaine. Ensuite, la fibre optique est recouverte d'une membrane de plastique pour la rendre plus solide.



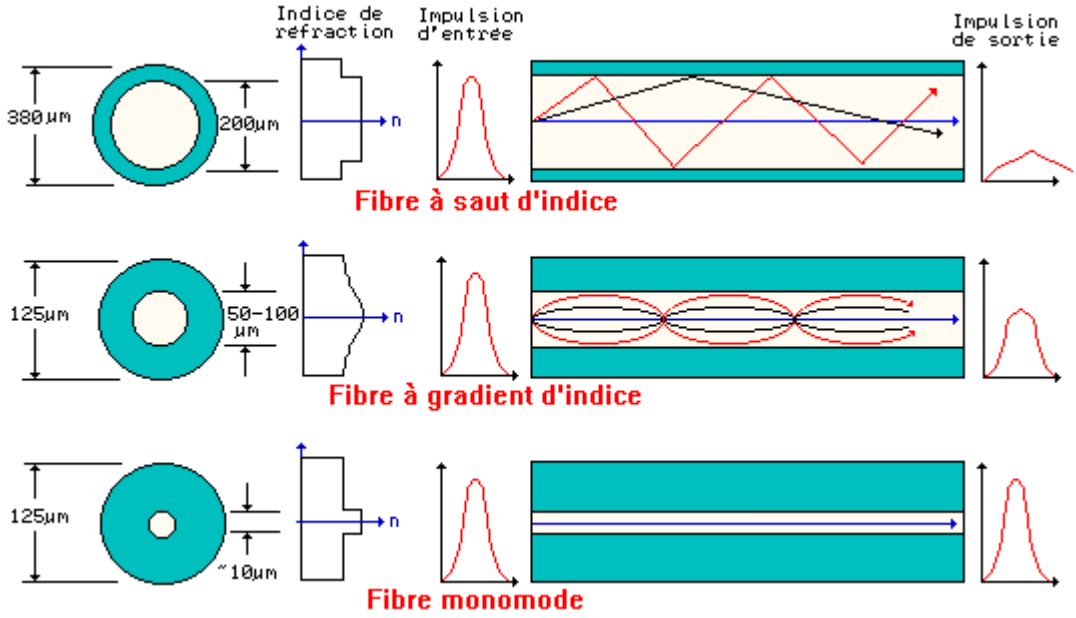
Comment la lumière se propage-t-elle dans la fibre optique ?

Lorsque le faisceau est émit vers la fibre, il doit pénétrer avec un angle supérieur à l'angle critique oo La propagation de la lumière (laser) dans la fibre optique se fait grâce à la réflection totale de la lumière sur les parois de la gaine. En fait, la fibre optique joue le rôle d'un guide d'ondes qui retient prisonnière la lumière dans la coeur. Il y a donc plusieurs modes de propagations pour une même fibre. Comme on considère la lumière comme une onde, elle respecte les lois de Maxwell de l'électromagnétisme.



On peut distinguer différents types de fibre optique:

- **fibres multimodes à saut d'indice**
  Elle est efficace sur de courtes distances parce qu'elle déforme le signal par le principe de dispersion, ce qui manifestement ne convient pas à toutes les applications. Elle est donc limitée dans sa bande passante
  diamètre du cœur 50 µm, affaiblissement 3 Db au km, 50 Mhz sur 10 Km
- **fibre multimodes à gradient d'indice**
  Elle est la plus utilisée pour les moyennes distances. Un des avantages est que la dispersion nodale est diminuée avec cette fibre. Il y a donc une meilleure réception du signal.
  diamètre du cœur 62.5 µm, affaiblissement 1 Db au km, 1 Gigahz sur 30 Km
- **fibre monomode**
  Dans une fibre optique monomode, le coeur est très fin ce qui permet une propagation du faisceau laser presqu'en ligne droite. De cette façon, elle offre peu de dispersion du signal et celle-ci peut être considérée comme nulle. Aussi, la bande passante approche l'infini c'est-à-dire plus de 10GHz. , diamètre du cœur 8 µm, affaiblissement 0.3 Db au km, 100 Gigahz sur 100 Km

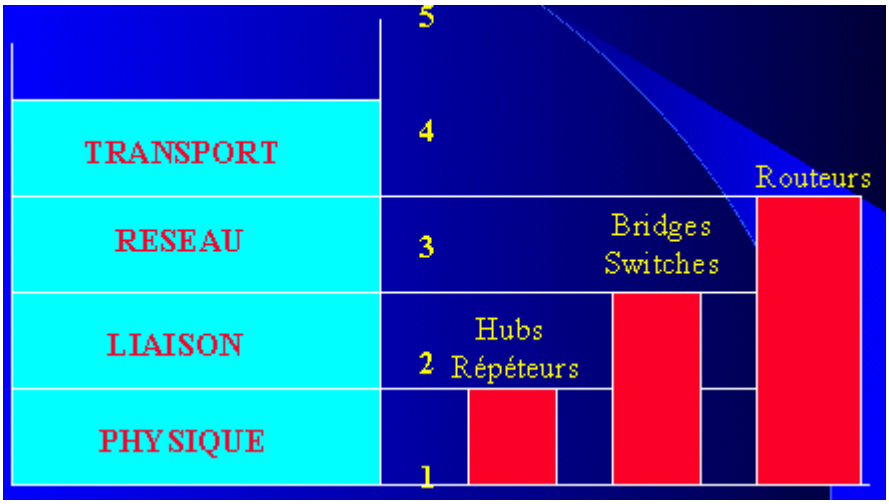

Indice de réfraction
Impulsion d'entrée
Impulsion de sortie
380µm
200µm
n
Fibre à saut d'indice
125µm
50-100 µm
n
Fibre à gradient d'indice
125µm
~10µm
n
Fibre monomode

HUB-SWITCH-ROUTEUR...

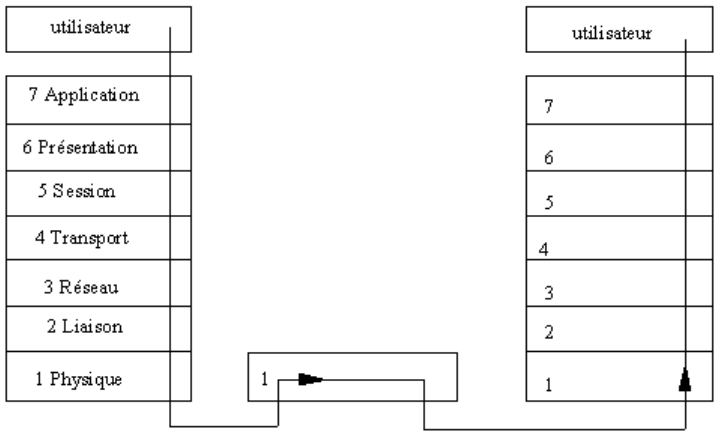
Présentation générale :

Il existe fondamentalement trois types de « machines » utilisées pour acheminer les données : les **hubs** (« répéteurs » en français, mais personne n'utilise ce mot), les **switchs** (commutateurs en français, même remarque) et les **routeurs**.

Les différents appareils que l'on peut lister comme intervenant dans le câblage d'un réseau se caractérisent par leur niveau d'intervention au niveau des couches réseau



Le Hub / Répéteur



Un **Hub** est un amplificateur de signaux qui a au minimum deux connexions réseau. Il travaille sur la **couche 1** du modèle ISO.

Dès qu'il reçoit sur l'une de ses entrées les premiers bits d'une trame, il la retransmet instantanément sur toutes ses sorties. Un répéteur n'opère aucune modification des données. Les hubs sont souvent utilisés quand il s'agit de relier quelques ordinateurs ensemble pour un petit réseau local. Le principe est simple, dès que quelque chose arrive sur une des prises, il est

automatiquement répéter sur toutes les autres prises. C'est pour cela qu'en français, on appelle ça un répéteur...

Sur un hub partagé, toutes les lignes d'entrée (ou au moins toutes les lignes arrivant sur une même carte d'E/S du hub) sont logiquement interconnectées entre elles, constituant ainsi un domaine de collision qui lui est propre. Les règles classiques de la norme 802.3 s'appliquent sur ce hub, y compris l'algorithme de tirage de temps aléatoire ; une seule station à la fois peut transmettre une trame à un instant donné.

Ainsi, dès qu'un ordinateur dit quelque chose, tout le monde l'entend et l'ordinateur concerné traite l'information... C'est pour cette raison que ce système ne peut être utilisé que lorsqu'il n'y a que peu d'ordinateurs, car s'il y a 100 ordinateurs qui parlent en même temps et que tout le monde entend tout ce que tout le monde dit, ça devient vite la … cacophonie !

Deux méthodes existent pour connecter un hub supplémentaire:

- hub "**stand alone**" : Interconnecter des hub au moyen d'un câble

  Dans ce cas, chaque hub à la valeur d'un répéteur selon la règle des répéteurs. (c'est à dire 5 hubs maxi) L'avantage de cette solution réside dans le fait que les répéteurs ne doivent pas se trouver en un voisinage immédiat.

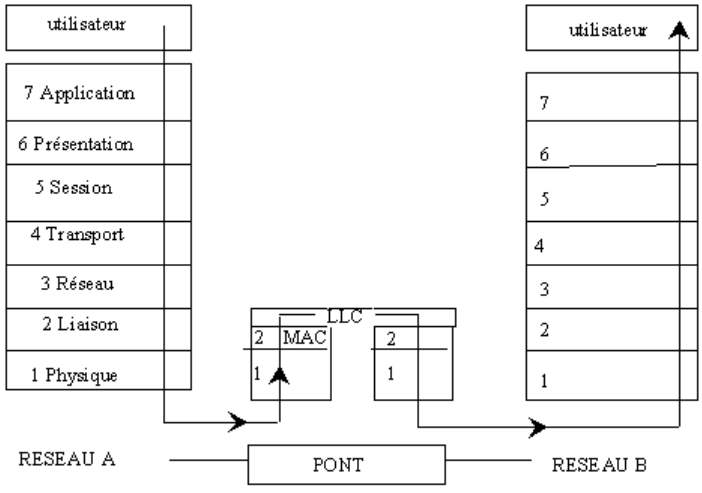
- hub "**empilables**" : Interconnecter les hub à l'aide de ports bus spéciaux et sur des câbles bus très courts.

  L'avantage de cette solution réside dans le fait que tous les répéteurs connectés valent pour un seul hub. on parle alors de hubs empilables

Certains hubs peuvent être aussi équipés d'un module de management. Dans ce cas, on peut piloter ces hubs à distance et effectuer des mesures de trafic et d'erreurs.

Le Switch / Commutateur

Les **switchs** sont un peu plus intelligents. C'est déjà un peu plus gros qu'un hub parce qu'on commence à mettre des choses dedans... Il travaille sur la **couche 2** du modèle ISO.



Il y a toujours ce principe de prises où sont connectés les différents ordinateurs (mais on peut aussi mettre d'autres switchs, ou des hubs, ou ce que l'on veut...). La différence avec le hub, c'est que le switch sait quels sont les ordinateurs qui sont autour de lui. Ainsi, si il reçoit une trame pour l'ordinateur X, il ne l'envoie qu'à l'ordinateur X et pas aux autres. Il commute (il branche) l'entrée des données vers la sortie où est

l'ordinateur concerné. C'est pour cela qu'on appelle ça un commutateur en français...

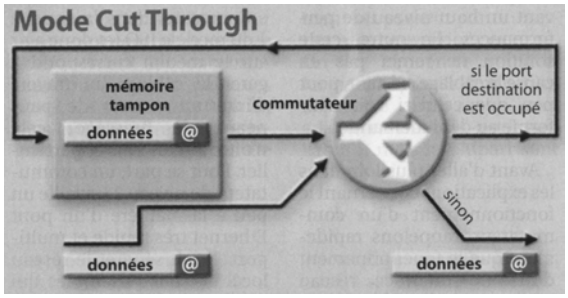
Dans le cas d'un switch, chaque trame arrivant sur une ligne en entrée est mémorisée dans une mémoire tampon interne à la carte d'E/S. Bien que cette façon de faire rende le switch coûteux, elle signifie également que toutes les stations peuvent transmettre et recevoir des trames simultanément. Cela améliore de façon importante les performances globales du système, d'au moins un ordre de grandeur, voire plus. Les trames mémorisées sont ensuite acheminées sur un bus à très haut débit interne au hub, de la carte d'E/S de la station source vers la carte d'E/S de la station destination. Le bus à très haut débit interne au hub n'est pas un produit standardisé, il est le plus souvent spécifique au fabricant de hub.

Lorsque l'on désire augmenter le nombre de noeuds d'un réseau partagé 100Mbits/s et prévenir efficacement les risques de saturation, les switchs sont des équipements incontournables.

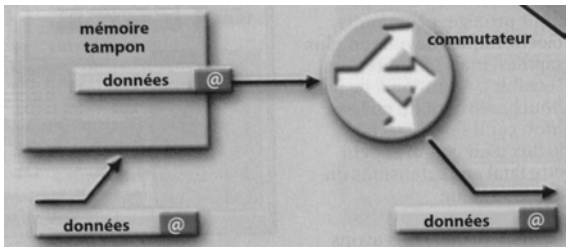
Comment fonctionne un switch ?

Le switch fonctionne en fait comme un pont local multiports. Il permet de scinder un réseau en autant de sous-réseaux qu'il y a de ports. Un switch est nettement plus rapide qu'un pont. Il a deux grands principes généraux de fonctionnement :

1. ***"On the fly" dit aussi "Cut Throuhg" :*** récupère la trame, analyse les adresses MAC et renvoie si nécessaire sur le port concerné du switch. L'opération est très rapide mais peu sûre (aucun traitement n'est effectué).

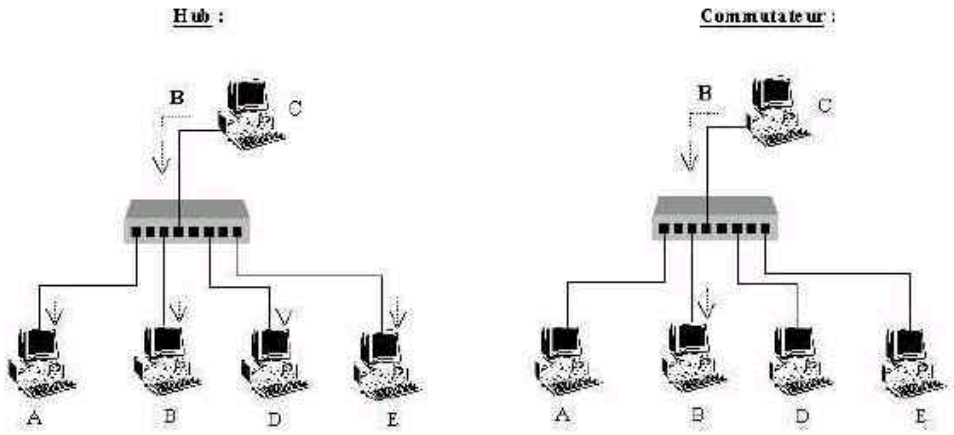


2. ***"Store-and-forward" :*** stocke la trame en mémoire flash, analyse les adresses MAC et vérifie l'intégrité des données, et renvoie si nécessaire sur le port concerné du switch. C'est une méthode plus lente mais extrêmement sûre concernant la qualité des besoins.



Chaque port d'un switch fait partie d'un seul domaine de collision. Chaque port du switch apprend dynamiquement les adresses MAC (Ethernet) des équipements qui lui sont connectés. Le switch est capable d'apprendre 1024 ou 2048 adresses par port. (minimum)

Le switch possède un **buffer** circulaire interne travaillant entre 1 ou 2 Gbits/s qui distribue les paquets entrants aux ports de destination s'il y a concordance avec l'adresse apprise dynamiquement par celui-ci.



Routeur :

C'est ce que l'on fait de mieux pour acheminer les données. Le routeur est quasiment un ordinateur à part entière. Il est capable de décoder les trames jusqu'à retrouver l'adresse IP et de diriger l'information dans la bonne direction. On peut aussi définir dans les trames le chemin où doit passer la trame, le routeur peut comprendre tout cela... Le fait de définir ou de diriger une trame s'appelle « router » une trame.

Pont :

Un pont offre la possibilité d'étendre un réseau 802.3-Ethernet-LAN au delà des limites autorisées (nombre de noeuds, longueur maximale, etc...). Les ponts sont de plus en plus utilisés pour contrôler le trafic et la stabilité d'un réseau. Ils travaillent au niveau 2 (couche liaison) du modèle ISO et servent à relier deux réseaux. Cela signifie que les ponts ne doivent pas analyser les paquets (par exemple X25) ou les datagrammes (par exemple IP ou IPX) de la couche réseau, ils doivent simplement se contenter de les insérer dans des trames et de les acheminer. Ils traitent tous les paquets quelque soit leur adresse destination (**Promiscuous Mode**).

Le **taux de défaillance** est réduit, puisque les interférences se produisant d'un côté du pont ne peuvent accéder de l'autre côté. De même, il accroît la **confidentialité**, puisque certaines informations échangées entre des noeuds d'un côté du pont, ne peuvent être "écoutées" de l'autre côté (par exemple les mots de passe échangés entre un serveur et un ordinateur). Enfin, il optimise le **débit**, puisque des segments séparés par des ponts ont un trafic local qui n'encombre pas le réseau entier.

Les ponts peuvent également relier des segments Ethernet par une ligne synchrone spécialisée, des liaisons satellites, des réseaux commutés et des réseaux en fibre optique (FDDI). En règle générale, ces ponts sont toujours mis en place par paire. Les ponts sont des ordinateurs complets et relativement performants, munis d'une mémoire et d'au moins deux raccords réseau. Ils sont neutres par rapport aux logiciels réseau et peuvent donc fonctionner simultanément avec, par exemple, TCP/IP, IPX, etc...

Résumé :

- Les **hubs** ne regardent pas ce qu'il y a dans les trames, ils se contentent de répéter l'information. Il n'y a aucune analyse du contenu de l'information, Ils travaillent au niveau 1 (physique) du modèle OSI.
- Les **switchs** sont capables d'analyser un peu l'information contenue dans la trame, de repérer l'adresse MAC de la destination et d'envoyer la trame vers le bon ordinateur. On dit que les switchs travaillent au niveau 2 du modèle OSI.
- Les **ponts** sont de plus en plus utilisés pour contrôler le trafic et la stabilité d'un réseau. Ils travaillent au niveau 2 (couche liaison) du modèle ISO et servent à relier deux réseaux
- Pour les **routeurs**, retenez simplement qu'ils sont assez puissants et qu'ils travaillent jusqu'au niveau 3 du modèle OSI. Ils sont capable d'analyser le contenu des trames.
- Si les hubs font partie d'un même **domaine de collision**, les switchs, ponts et routeurs permettent de créer des **domaines de collisions séparés**

LA NORME ETHERNET

Présentation générale :

La Norme Ethernet à été développée par XEROX dans les années 1970 et fit l'objet de spécifications normalisée sous la poussée d'un consortium de 3 entreprises dans les années 1980 DEC - INTEL - XEROX .

En 1985, l' IEEE (Institute of Electrical and Electronic Engineers) publia la norme définitive sous l'apellation IEEE 802.3 CSMS/CD.

Pour comprendre le principe de fonctionnement de la norme Ethernet voir le principe de Détection de collision page 25 (topologie d'accès)

Depuis la norme à constament évolué pour tenir compte des nouveau type de media disponibles et débit possibles.

A ce titre on distingue principalement deux catégories, selon le débit nominal du média, à 10Mbps ou à 100Mbps . et une évolution à 1000Mbps…

à **10 Mbps** (ETHERNET) on distinguera :

la norme **10 BASE 5** :	**Thick Coax**
	Coaxial épais
la norme **10 BASE 2** :	**Thin Coax**
	Coaxial fin
la norme **10 BASE T** :	**Twisted Pair**
	Paires torsadées
la norme **10 BASE F** :	**Fiber Optic**
	Fibre optique

à **100 Mbps** (FAST ETHERNET) on distinguera :

la norme **100 BASE TX** :	**Twisted Pair**
	Paire torsadée
la norme **100 BASE T4** :	**4 Twisted Pair**
	4 Paires torsadées
la norme **100 BASE FX** :	**Fiber**
	Fibre optique

d'autres évolutions à **100 Mbps** (100 VG ANYLAN) et à **1000 Mbps** (GIGABIT ETHERNET) existent

Trâme Ethernet :

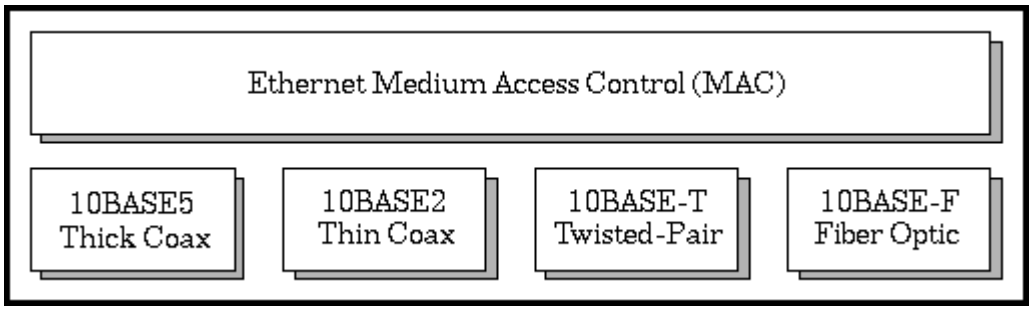
La Norme Ethernet à été développée par XEROX dans les années 1970 et fit l'objet de spécifications normalisée sous la poussée d'un consortium de 3 entreprises dans les années 1980 DEC - INTEL - XEROX .

Préambule 7 octets	SFD 1 octet	@dest 6 octets	@source 6 octets	EtherType 2 octets	Données 46 - 1500 octets	FCS 4 octets

Voir support T1 chap 4 p12

ETHERNET: 10 BASE ...

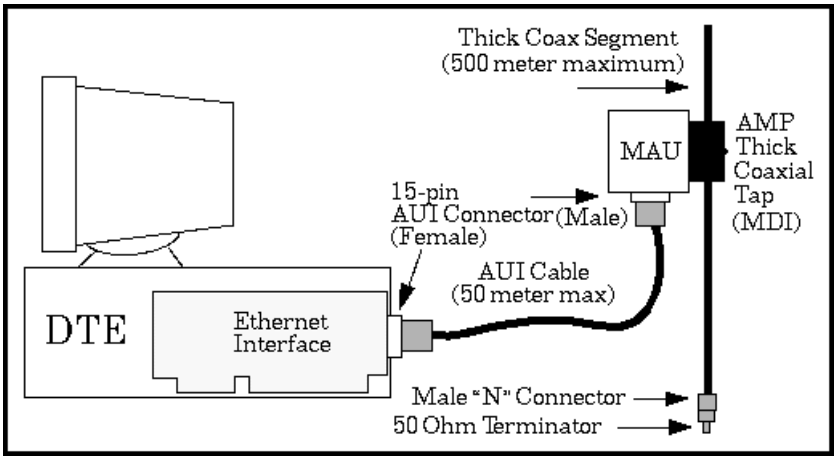
Présentation générale :



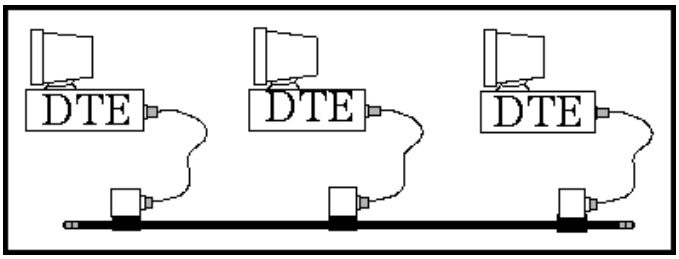
Norme IEEE 802.3

10 BASE 5 "Thick Coax" :

Le principe de raccordement est le suivant :



sur une topologie de câblage dite en BUS.



Avec les valeurs maximales admissibles suivantes :

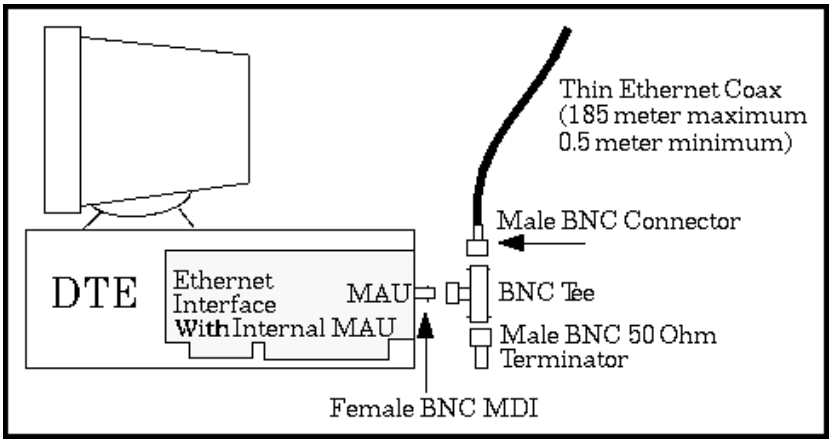
Nombre maxi de segment :	5
Longueur maxi Segment :	500 m
Distance maxi station/segment :	50 m
Distance mini entre deux prises segment :	2.5 m
Nombre maxi de prises par segment :	100

Soit maxi 500 (5 x 100) postes sur une distance de 2.5Km (5 x 500m)

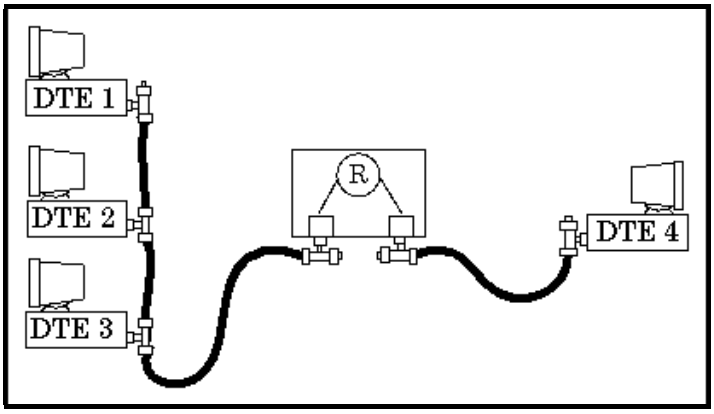
---

10 BASE 2 "Thin Coax" :

Le principe de raccordement est le suivant :



sur une topologie de câblage dite en BUS.



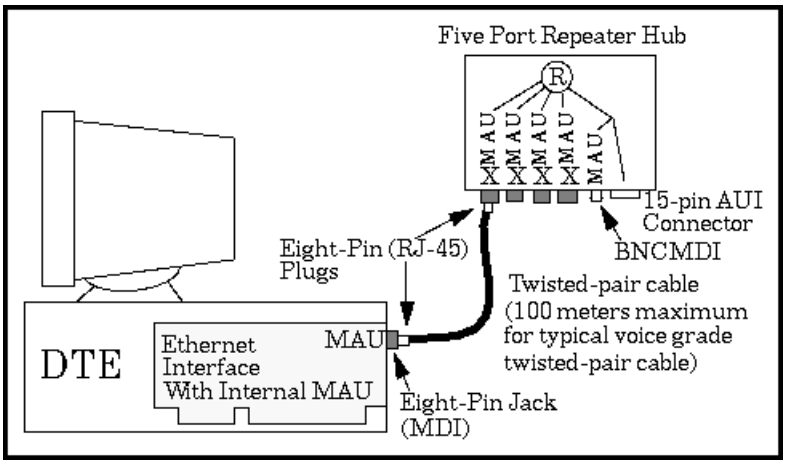
Avec les valeurs maximales admissibles suivantes :

Nombre maxi de segment :	5
Longueur maxi Segment :	185 m
Distance maxi station/segment :	connecteur
Distance mini entre deux connecteurs :	0.5 m
Nombre maxi de prises par segment :	30

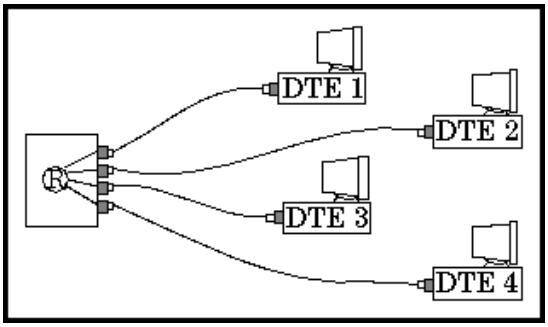
Soit maxi 150 (5 x 30) postes sur une distance de 925m (5 x 185m)

10 BASE T "Twisted pair" :

Le principe de raccordement est le suivant :



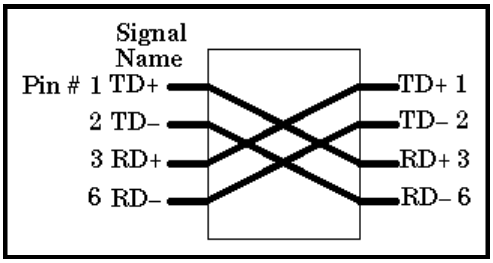
sur une topologie de câblage dite en Etoile avec un schéma suivant :



et un schéma de câblage suivant:

10BASE-T eight-pin connector signals

Pin Number	Signal
1	TD+
2	TD–
3	RD+
4	Unused
5	Unused
6	RD–
7	Unused
8	Unused



Avec les valeurs maximales admissibles suivantes :

Nombre maxi de segment :	5
Longueur maxi Segment :	100 m
Nombre maxi Hub :	4

Soit un maximum non prévu de postes sur une distance de 500m (5 x 100m). Dans un même domaine de collision, le circuit entre 2 stations ne doit **pas comporter plus de 5 segment et 4 hub**

Ce qui est évident dans le schéma ci-dessous

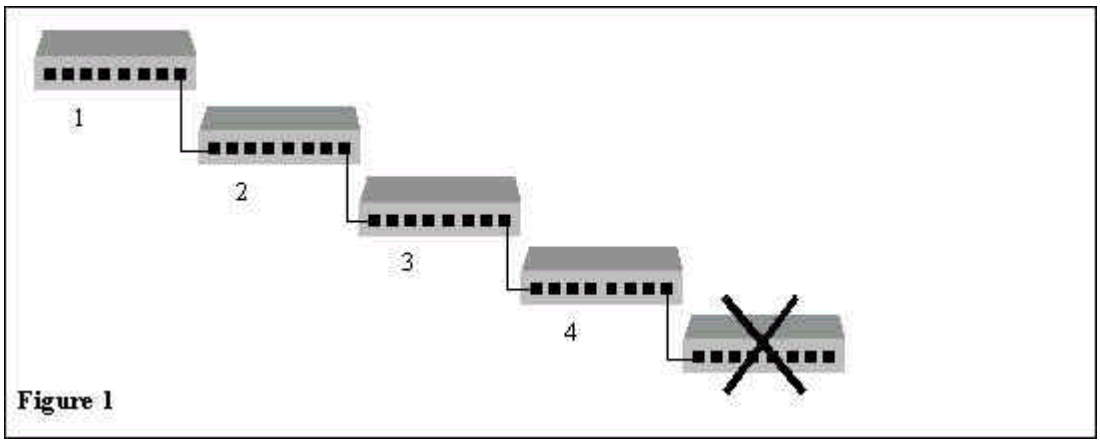


Figure 1

mais ce qui est aussi évident dans le schéma ci-dessous

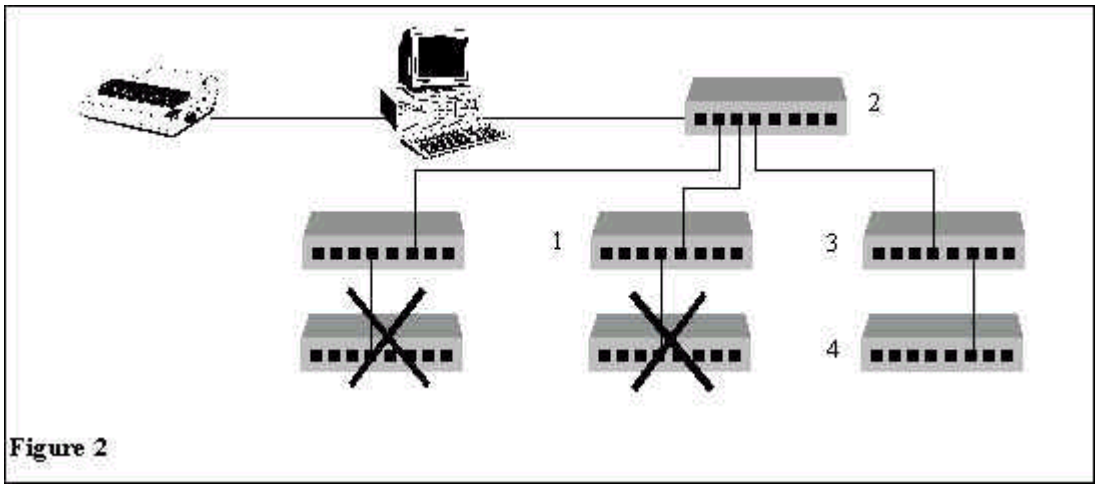
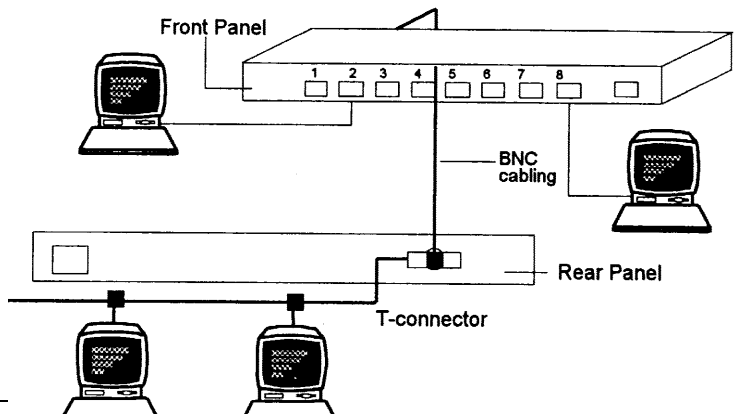


Figure 2

Dans un hub tous les paquets émis sur un segment ou appareil connecté à l'un des ports sera répercuté sur tous les autres ports qui font partie alors de ce que l'on appelle le même "domaine de collision"

Un hub fonctionne au niveau 1 du modèle ISO, et peut faire office de convertisseur de média entre tous les segments ou appareils attachés

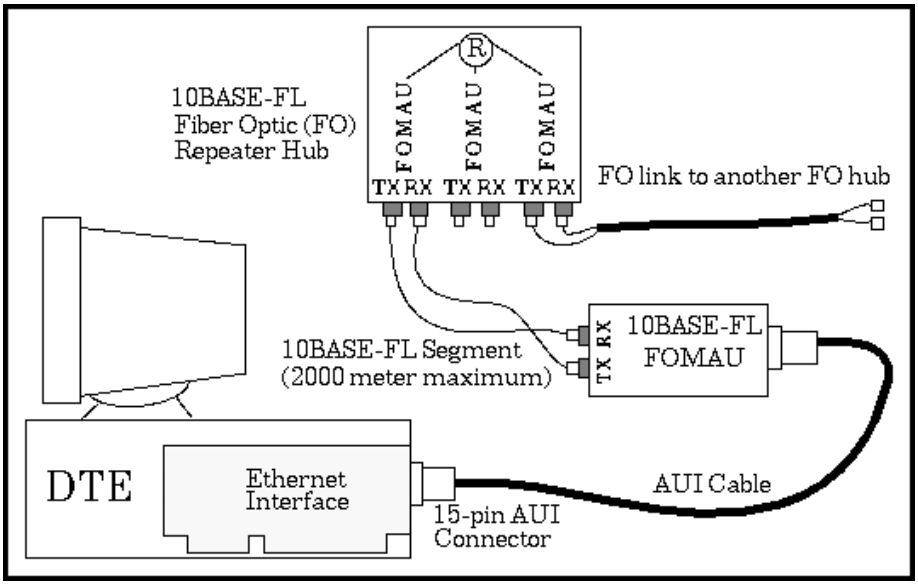
Dans un réseau 10BaseT, plusieurs segments Ethernet - Ethernet Fin, Gros ou d'autres types de câbles - peuvent être interconnectés grâce à des hub. Cela permet de contourner la limite de distance max pour un



segment (par exemple).

10 BASE F "Fiber Optic" :

Le principe de raccordement est le suivant :

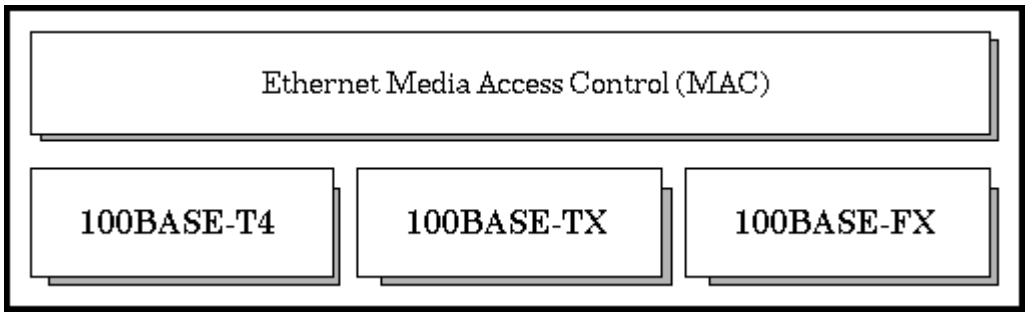


Avec les valeurs maximales admissibles suivantes :

Nombre maxi de segment :	2
Longueur maxi Segment :	2000 m

FAST ETHERNET: 100 BASE ...

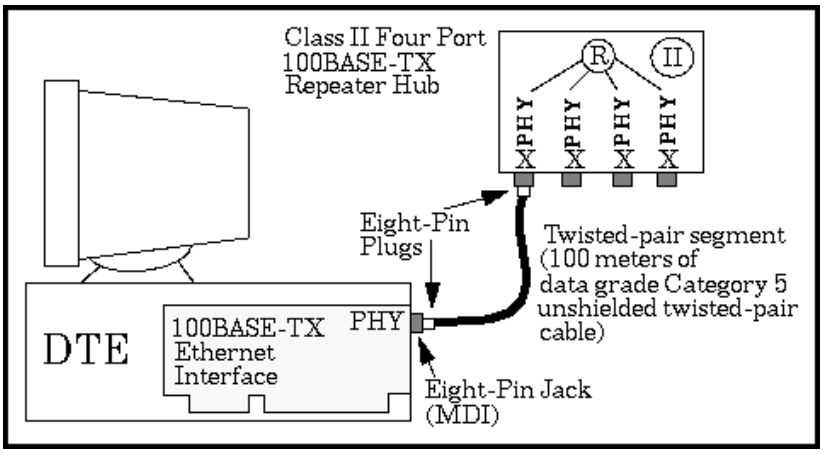
Présentation générale :



C'est une évolution de la norme Ethernet 10Base dénommée IEEE 802.3u

100 Base TX :

Le principe de raccordement est le suivant :



sur une topologie de câblage en Etoile classique (idem 10baseT):

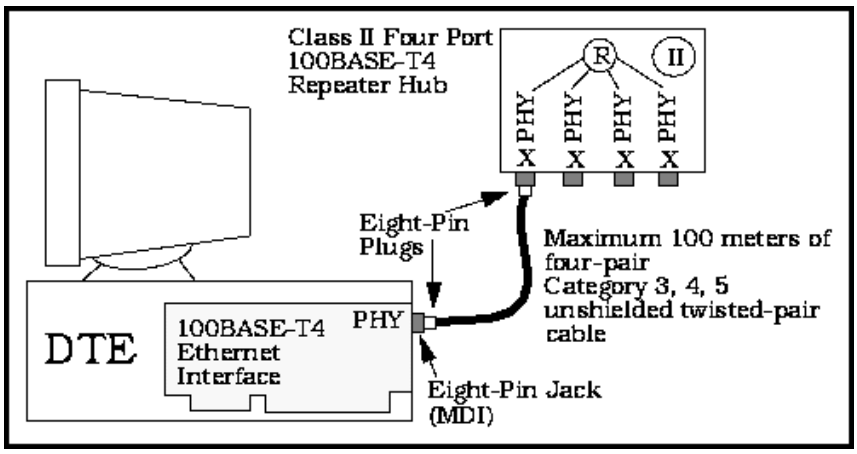
et un schéma de câblage identique au 10 Base T mais nécessitant du **UTP5**

Avec les valeurs maximales admissibles suivantes :

Nombre maxi de segment :	2 / 3 (cf hub classe p 72)
Longueur maxi Segment :	100 m
Nombre maxi Hub :	1 / 2 (cf hub classe p 72)

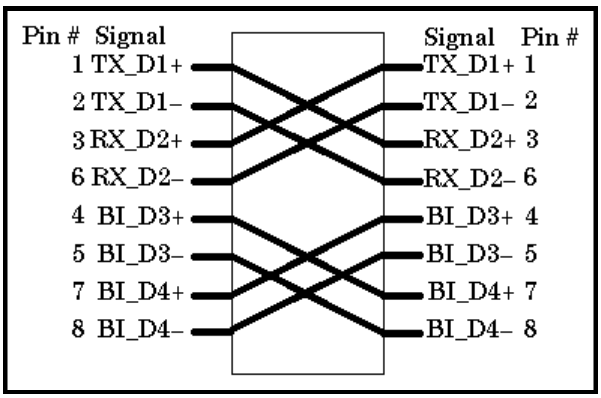
100 Base T4 :

Le principe de raccordement est le suivant :



sur une topologie de câblage en Etoile classique (idem 10baseT):

et un schéma de câblage identique au 10 Base T mais nécessitant 4 paires dans du **UTP5** par conséquent donnant

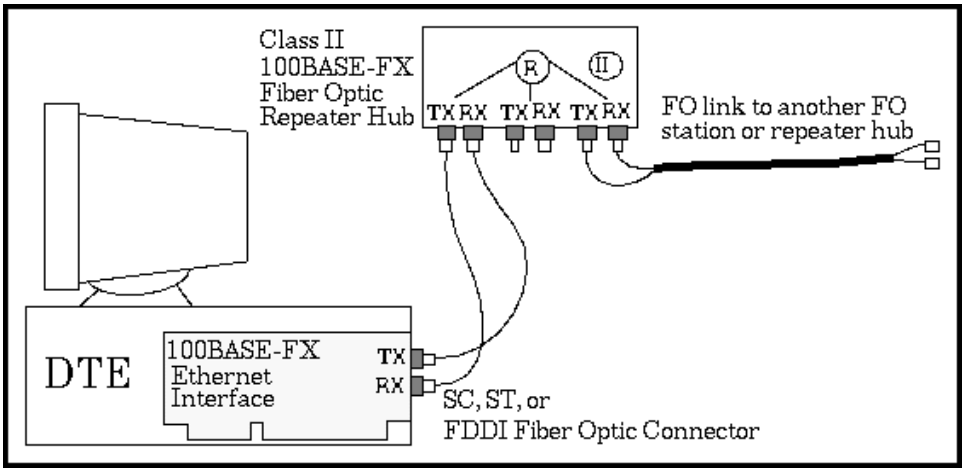


Avec les valeurs maximales admissibles suivantes :

Nombre maxi de segment :	2 / 3 (cf hub classe p 72)
Longueur maxi Segment :	100 m
Nombre maxi Hub :	1 / 2 (cf hub classe p 72)

100 Base FX :

Le principe de raccordement est le suivant :



Avec les valeurs maximales admissibles suivantes :

Nombre maxi de segment :	1
Longueur maxi Segment :	412 m
Nombre maxi Hub :	1

Classe de hub :

Les hub Fast Ethernet 100Mbits/s travaillent comme les Hub10Mbits/s à une vitesse de transfert de données est plus élevée. On fait la différence entre deux classes de répéteurs :

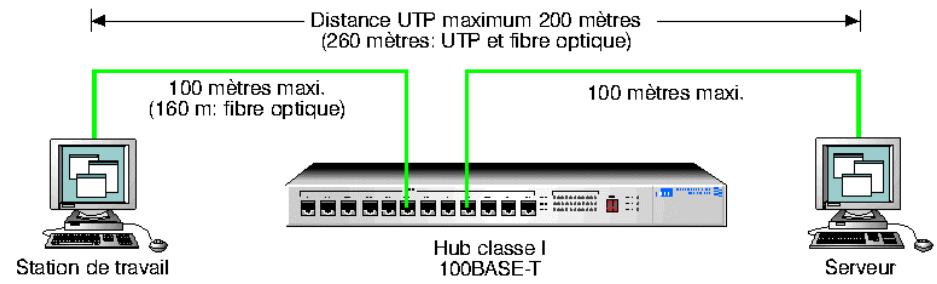
Il existe deux classes de Hub différentes, selon que les signaux soient simplement répétés ou bien régénérés avant d'être retransmis.

Hub de classe I :

le Hub de "classe I " régénère le signal et le diffuse sur les autres ports en l'adaptant au type de port.

Par conséquent on peut connecter à un Hub de classe I des typologies 100Base Tx et/ou des typologies 100Base T4 simultanément

On ne peut pas cascader deux Hub de classe I, par conséquent on ne peut trouver deux hub de classe I entre deux postes

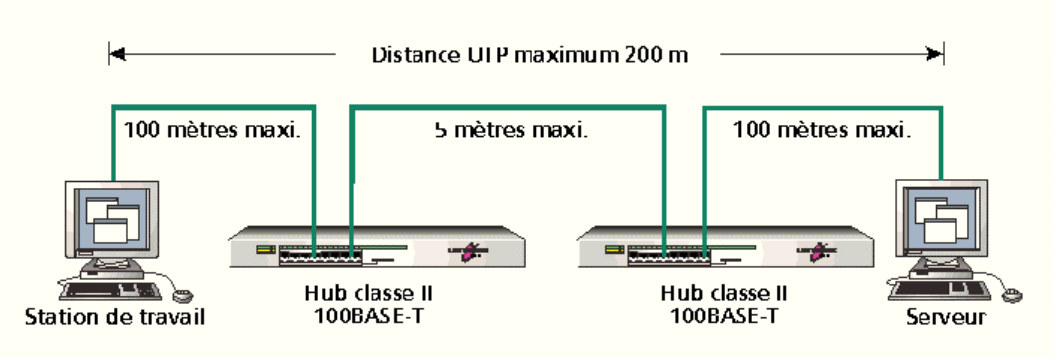


Hub de classe II :

le Hub de "classe II " répète immédiatement le signal

Par conséquent on ne peut connecter à un Hub de classe II que des typologies identiques 100Base Tx ou 100Base T4 sans les mélanger

On peut par contre cascader deux Hub de classe II mais avec une distance inter Hub extrêmement faible : **5 m** maximum



Mélange UTP et fibre optique:

Dans ce cas le calcul de distances maximales possibles se complique.

Le tableau suivant indique les longueurs maximales valables en utilisant un câblage mixte paire torsadée / fibre optique et selon le nombre de Hub :

Type de Connexion	**Mono-type Paire torsadée**	**Mono-type Fibre optique**	**Paire torsadée (T4) + Fibre optique**	**Paire torsadée(TX) + Fibre optique**
Direct Poste à hub	100 m.	412 m.	/	/
1 hub de classe I	200 m. (100 + 100)	272 m. (136 + 136)	231 m. (100t4 + 131fo)	260 m. (100tx + 160fo)
1 hub de classe II	200 m. (100 + 100)	320 m.	/	308 m. (100tx + 208fo)
2 hub de classe II	205 m. (100 + 5 + 100)	228 m. (111fo + 5 + 111fo)	/	216 m. (100tx+ 5 + 111fo) 2200 m. (100tx+2kfo+100tx)

Distances Admissible entre un Routeur et un Hub:

Classe I : 161 m. en Fibre optique

Classe II : 209 m. en Fibre optique

A priori, les restrictions semblent présenter un inconvénient pour la configuration de réseaux Fast Ethernet. Mais Certains composants propriétaires permettent d'augmenter la portée…

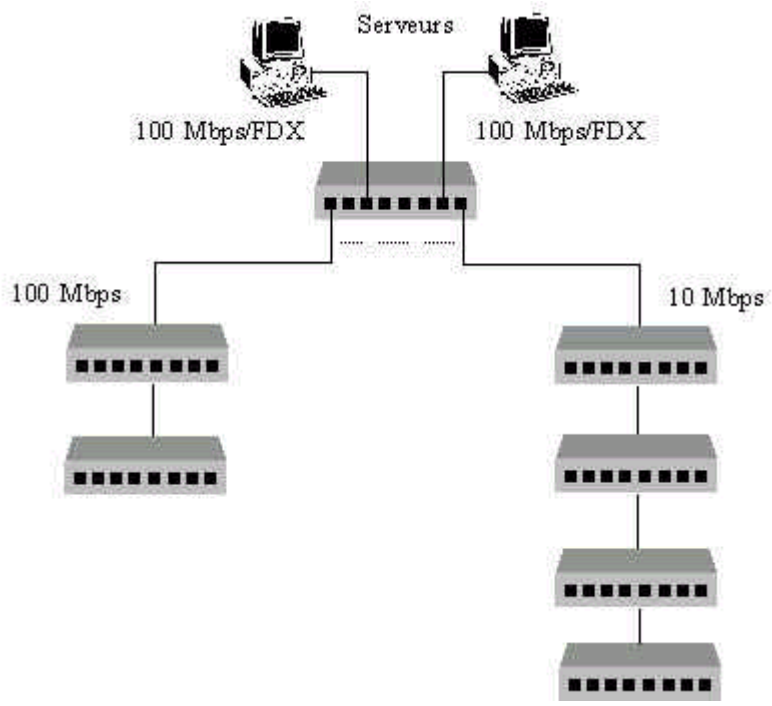
méler 10BaseT, 100BaseT:

Certains modèles de switchs sont **auto-sensing**, ce qui veut dire qu'ils adaptent la vitesse de leurs ports (10/100 Mbits/s) à celle de l'appareil qui lui est connecté.

Autonégociation :

TABLE 0.1 Auto-Negotiation priority resolution table

A:	100BASE-TX Full Duplex
B:	100BASE-T4
C:	100BASE-TX
D:	10BASE-T Full Duplex
E:	10BASE-T



EVOLUTIONS ETHERNET

Ethernet 100VG Any Lan :

En évolution existe encore sous l'appellation 100VG Any LAN, normalement référencée sous la norme IEE 802.12

la typologie est la même que celle sous 10BaseT, mais avec un débit de 100Mbps, avec 4 paire torsadées de qualite vocale (Voice Grade) et compatible Ethernet / Token Ring

Gigabit Ethernet :

Le Gigabit Ethernet est une évolution naturelle qui se veut une technique d'attente plutôt qu'une réelle évolution de la norme

C'est une évolution de la norme Ethernet 10Base dénommée IEEE 802.3z et IEEE 802.3ak

Le Gigabit Ethernet fonctionne en Full-Duplex dans le mode Switch-Switch et en half Duplex pour les stations directement raccordées sur un Hub

En général cependant il n'est pas utilisé pour raccorder directement des stations, mais plutôt pour constituer une ossature (backbone) sur un réseau local. A ce titre il est souvent implémenté avec un technologie un peu propriétaire…

On pourrait distinguer

la norme **1000 BASE CX** : **Coax**

2 paires de Coaxial (25m de long max)

la norme **1000 BASE T** : **Twisted Pair**

paires torsadée (100m de long max)

la norme **1000 BASE SX** : **Fiber**

Fibre optique multimode (300/550m lg max)

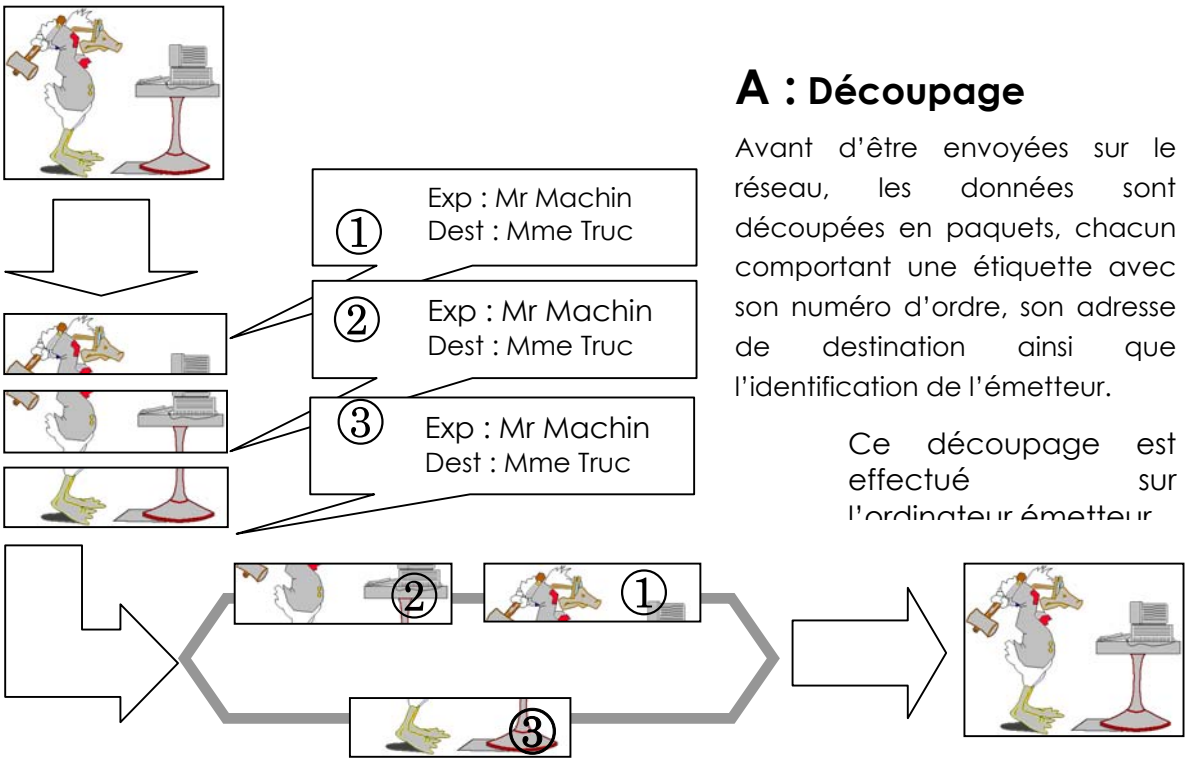
la norme **1000 BASE LX** : **Fiber**

Fibre optique monomode (3 Km long max)

LE PROTOCOLE TCP/IP

TCP/IP

C'est le protocole le plus répandu, notamment à cause de la circulation des informations sur Internet. Il défini des règles précises, appliquées sur tous les équipements chargés de transmette les données. Ces règles sont regroupées sous le terme TCP/IP. Le Transmission Control Protocol (TCP) se charge de découper les données en sections plus petites, **les paquets**, qui peuvent circuler indépendamment les unes des autres, tandis que l'Internet Protocol (IP) assure l'envoi vers la bonne destination.



A : Découpage

Avant d'être envoyées sur le réseau, les données sont découpées en paquets, chacun comportant une étiquette avec son numéro d'ordre, son adresse de destination ainsi que l'identification de l'émetteur.

Ce découpage est effectué sur l'ordinateur émetteur

B : Aiguillage

Au cours du voyage, il peut arriver que les paquets n'empruntent pas tous la même route pour arriver à destination, notamment parce qu'un routeur (équipement de télécommunication) s'est rendu compte qu'un chemin est brusquement devenu saturé et qu'il valait mieux aiguiller quelques paquets sur une autre route.

C : Regroupement

Sur le site destinataire, les paquets n'arrivent pas forcément dans le bon ordre. Ils sont remis en séquence à mesure de leur arrivée grâce à leur numéro d'ordre.

Adresse TCP/IP :

Ce protocole désormais quasi universel repose en partie sur la notion d'adresse IP (Internet Protocol) décernée de façon unique pour chaque élément matériel faisant partie d'une réseau

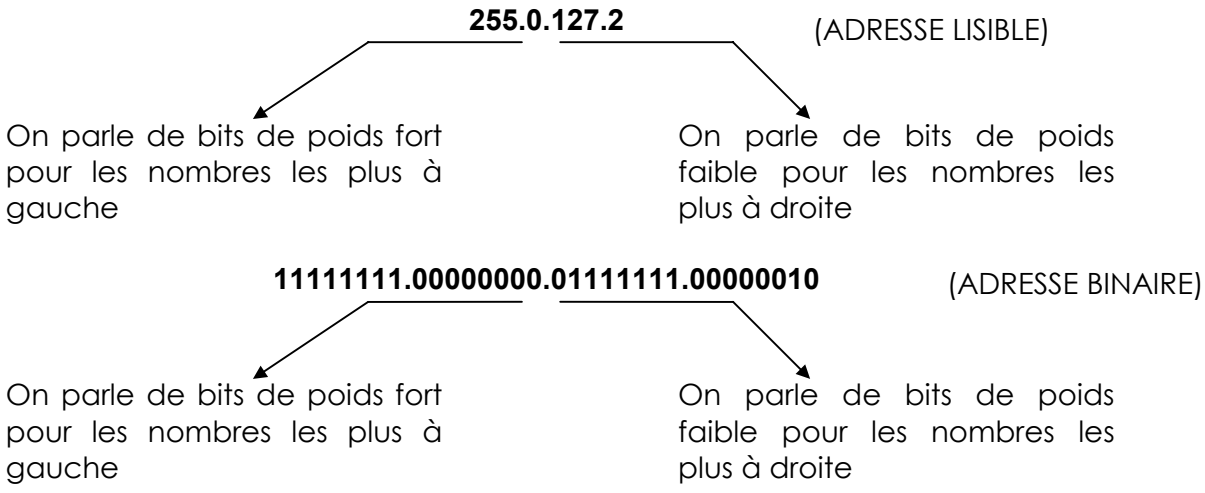
Hôtes et réseaux

L'adressage IP est basée sur le concept d'hôtes et de réseaux. Un **hôte** est tout ce qui peut envoyer ou recevoir des trames IP sur le réseau, comme une station de travail ou un routeur. Il ne faut pas confondre avec un serveur : clients et serveurs sont tous des hôtes IP.

Les hôtes sont connectés entre eux par un ou plusieurs **réseaux**. L'adresse IP de n'importe quel hôte est le rassemblement de deux choses : l'adresse du réseau où il se trouve et son adresse personnelle sur ce réseau.

La taille de la partie adresse de réseau et de la partie adresse de l'hôte dépend du type de réseau où l'on est.

Ces adresses sont codées sur 32 bits, est sont représentées sous la forme de 4 nombre compris entre 0 et 255 (valeur d'un octet) et séparés par un point, soit (par exemple)



On pourrait ainsi dire que les adresses IP varient de la plus petite 0.0.0.0 à la plus grande255.255.255.255. Une adresse valide est dans la plage allant de 0.0.0.0 à 255.255.255.255, soit un total de 4.3 milliards d'adresses

En fait toutes les combinaisons ne sont pas disponibles, et elles reflètent une certaine logique

Classes d'Adresse :

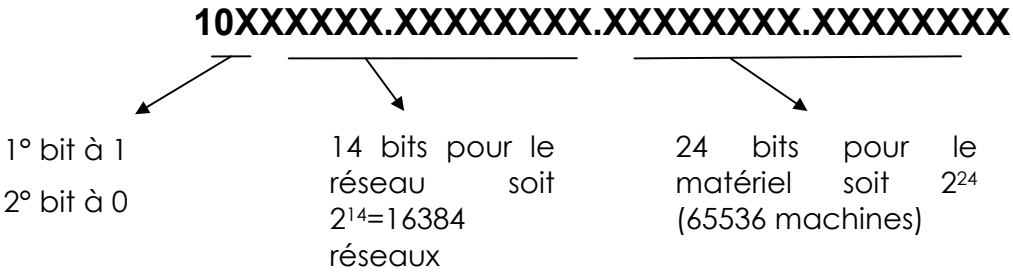
Les bits de poids fort, définissent l'adresse du réseau et les bits de poids faible l'adresse d'un équipement dans le réseau. Mais comme la limite entre poids fort et poids faible n'est pas toujours la même, il semble évident que

- plus les poids fort sont petits, et plus le nombre de machines connectable dans un même réseau sera important, même si on aura peut de réseau de ce type
- plus les poids fort sont nombreux, on aura alors peut de machines connectable pour chacun de ces réseau, même s'il sont plus nombreux

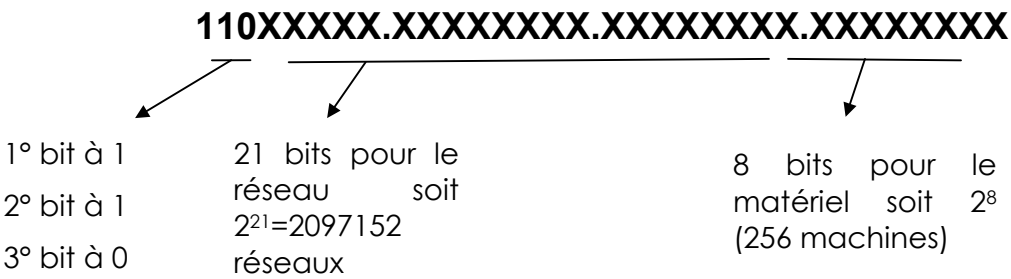
C'est la notion de "classe de réseau"

Réseau de **Classe A** : (commence par 1 à 127)

Réseau de **Classe B** : (commence par 128 à 191)



Réseau de **Classe C** : (commence par 192 à 223)



En résumé, une adresse IP fait 32 bits de long et est composée de deux parties: le **numéro de réseau**, et le **numéro d'hôte**. Par convention, exprimée en quatre nombres décimaux séparés par des points, les premiers bits indiquent la classe à laquelle appartient l'adresse :

Classe	Préfixe	Numéro de réseau	Numéro d'hôte
A	0	bits 1-7	bits 8-31
B	10	bits 2-15	bits 16-31
C	110	bits 3-24	bits 25-31
D	1110	Multicast	Multicast
E	1111	Réservé	Réservé

Les plages d'adresses pour les différentes classes peuvent être déduites :

Classe	Plage de numéros de réseau	Plage de numéros d'hôte
A	0 à 126	0.0.1 à 255.255.254
B	128.0 à 191.255	0.1 à 255.254
C	192.0.0 à 223.255.255	1 à 254

N'importe quelle adresse commençant par 127 est une adresse de particulière et ne devrait jamais être utilisée par autre chose que le serveur central. Un numéro d'hôte composé uniquement de 1 (en binaire) indique une émission à l'attention de l'ensemble des machines du réseau (broadcast). Par exemple, 200.1.2.255 indiquerait une émission pour toutes les machines du réseau 200.1.2. Si le numéro d'hôte est 0 (en binaire), il indique "le réseau même". Tous les bits réservés et adresses réservées réduisent sévèrement les adresses IP disponibles (4,3 milliards). La plupart des utilisateurs reliés à l'Internet se verront assignés des adresses de classe C, puisque l'espace devient très limité. C'est la raison principale du développement d'IPv6, qui aura 128 bits d'espace adresse.

Masque de sous-réseau :

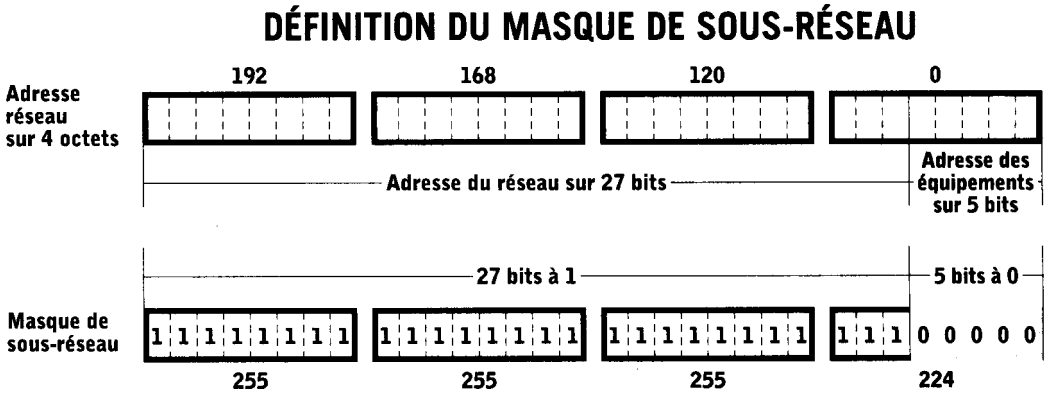
Le masque de sous-réseaux permet de définir le découpage entre les bits de l'adresse qui servent à définir l'adresse de réseau, et ceux servant à définir l'adresse de la machine

Il est construit en mettant à 1 les bits qui servent à définir l'adresse de réseau et à 0 les bits définissant les adresses des machines

Ainsi dans des masques standards, si on à un réseau de

classe A	le masque vaudra	255.0.0.0
classe B	le masque vaudra	255.255.0.0
classe C	le masque vaudra	255.255.255.0

Néanmoins on peut affiner, par exemple avec une classe C de référence on peut en gardant les 5 bits de poids faibles comme bits d'adresse matériel avoir 2^3=8 mini réseaux de 2^5=32 machines maximum ayant comme masque de sous-réseaux 255.255.255.224



Nous avons vu qu'une adresse IP était constitué d'un numéro de réseau et d'un numéro d'hôte. Cela dit, les masques de sous-réseaux permettent de diviser les réseaux de classe A, B ou C en sous-réseaux. En effet, en admettant que tous les hôtes d'un réseau de classe A soit sur le même sous-réseau, le réseau serait très rapidement saturé, ne serait-ce que par les broadcast qui sont destiné à tous les hôtes du même réseau.

Les réseaux sont donc diviser en sous-réseaux et le masque permet de les déterminer. Par exemple, pour un réseau de classe C, on a coutume d'utiliser 255.255.255.0 comme masque de sous-réseau. Cela signifie que dans l'adresse IP, la partie numéro de réseau sera les trois premier nombre et que la partie numéro d'hôte sera le quatrième.

En fait, pour savoir dans une adresse IP quelle est la partie numéro de réseau et numéro d'hôte, il suffit d'écrire l'adresse IP en binaire et d'écrire dessous le masque de sous-réseau, également en binaire. Soit l'adresse IP 192.168.2.53 et le masque 255.255.255.0…On obtient, en binaire :

11000000.10101000.00000010.00110101
11111111.11111111.11111111.00000000

La partie correspondante aux 1 du masque de sous-réseau correspond au numéro de réseau et la partie correspondante au 0 correspond au numéro d'hôte.

Ainsi, dans ce cas, avec un masque de 255.255.255.0, on peut avoir 254 hôtes différents sur le sous-réseau 192.168.2.0…

Essayons maintenant avec un masque de sous-réseau 255.255.255.224, on obtient :

11000000.10101000.00000010.00110101
11111111.11111111.11111111.11100000
La partie numéro de réseau devient donc 192.168.2.32 et le numéro d'hôte est 21. Ainsi, avec le masque 255.255.255.224, on peut diviser le réseau 192.168.2.0 en 8 sous-réseaux différents. Les numéros d'hôte dans ce cas ne peuvent aller que de 1 à 31, la machine d'adresse IP 192.168.2.65 ne fera donc pas partie du même réseau.

Adresses IP Privées :

Avec la prolifération de la technologie TCP/IP à travers le monde, même en dehors de l'Internet lui même, un nombre croissant d'entreprises non connectées utilisent cette technologie et ses capacités d'adressage pour des besoins de communication uniquement intra-entreprise, sans jamais l'intention de se connecter à d'autres entreprises ni à l'Internet lui-même.

Il est normal d'assigner des adresses globalement uniques à toutes les machines qui utilisent TCP/IP. Pour pouvoir étendre la durée de vie de l'adressage IPv4, les organismes d'enregistrement demandent beaucoup plus de justifications qu'auparavant, rendant la tâche plus difficile à des organisations pour acquérir un espace d'adressage supplémentaire [RFC1466].

Les machines de l'entreprise qui utilisent TCP/IP peuvent être divisées en 3 catégories:

- **Catégorie 1 :** les machines qui n'ont pas besoin d'accéder à des machines d'autres entreprises ou à l'Internet dans son ensemble. Les machines de cette catégorie peuvent utiliser des adresses IP qui sont uniques dans l'entreprise, mais qui peuvent être ambigues entre différentes entreprises.
- **Catégorie 2 :** les machines qui ont besoin d'accéder à un nombre limité de services extérieurs (ex: E-Mail, WWW, FTP) qui peuvent êtres servis par des passerelles applicatives. Pour beaucoup de machines dans cette catégorie, un accès non restreint (fourni par la connectivité IP) n'est pas forcément nécessaire et même quelque fois non désiré pour des raisons de sécurité. Pour les mêmes raisons que pour les machines de la première catégorie, de telles machines peuvent utiliser des adresses IP uniques dans l'entreprise, mais qui peuvent être ambigues entre différentes entreprises.
- **Catégorie 3 :** les machines qui ont besoin d'un accès réseau à l'extérieur de l'entreprise (fourni par la connectivité IP). Les machines de cette dernière catégorie ont besoin d'une adresse unique sur tout l'Internet.

On parle pour les machines des catégories 1 et 2 comme de machines "privées", et pour les machines de la 3eme catégorie comme des machines "publiques".

L'Autorité d'Affectation de Numéros sur Internet) a réservé les 3 bloc suivant dans l'espace d'adressage pour des réseaux internes :

10.0.0.0 - 10.255.255.255 (10/8 prefix)

le premier bloc n'est rien d'autre qu'une classe A

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

le second, un ensemble de 16 classes B contiguës

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

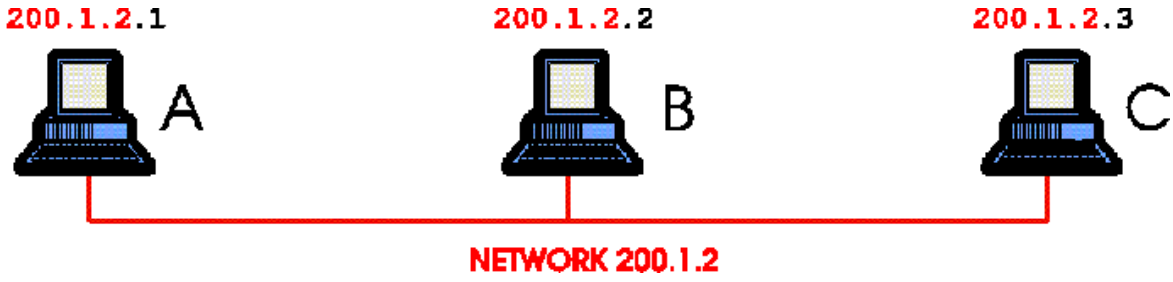
et le troisième, un ensemble de 256 classes C contiguës.

Les **machines privées** peuvent communiquer avec toutes les autres machines de l'entreprise, à la fois publiques et privées. Néanmoins, elles ne peuvent avoir de connectivité IP avec une machine à l'extérieur de l'entreprise. Même si elles n'ont pas de connectivité IP vers l'extérieur, les machines privées peuvent toutefois avoir accès à des services extérieurs grâce à des passerelles (ex passerelles applicatives).

Les **machines publiques** peuvent communiquer avec d'autres machines privées ou publiques à l'intérieur de l'entreprise et possèdent une connectivité IP avec les machines publiques extérieures à l'entreprise. Les machines publiques n'ont pas de connectivité avec des machines privées d'autres entreprises.

Routage IP de base

Soit un réseau interne TCP/IP comprenant un segment Ethernet et trois machines. Le numéro de réseau IP de ce segment est 200.1.2. Les numéro d'hôte pour A, B et C sont 1, 2 et 3 respectivement. Ce sont des adresses de classe C, ce qui permet d'avoir 254 machines sur ce segment.

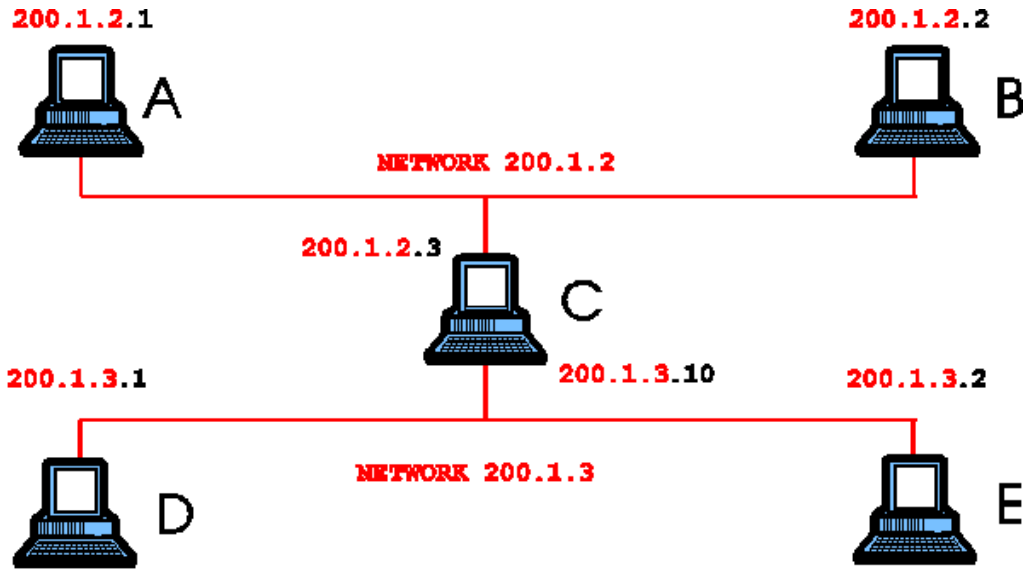


Supposons que A veuille envoyer un paquet à C pour la première fois, et qu'il connait l'adresse IP de C. Pour envoyer ce paquet sur ce brin Ethernet, A aura besoin de connaître l'adresse MAC (ou adresse Ethernet) de C. Le protocole **ARP** (Address Resolution Protocol) est utilisé pour trouver dinamyquement cette adresse.

ARP garde une table interne d'adresses IP et d'adresses MAC correspondantes. Quand A essaye d'envoyer un paquet IP à C, le module d'ARP consulte sa table d'adresses IP et ne découvrira aucune entrée pour C. ARP envoie alors un paquet spécial reçu par tous (broadcast), demandant l'adresse MAC correspondant à l'adresse IP qu'il connait. S'il n'y a pas de "time-out", cela signifie que la machine C a répondu en incluant son adresse MAC dans sa réponse, et le tour est joué. A met à jour sa table d'adresse (ou table d'hôte) et peut envoyer son paquet.

Considérons maintenant 2 réseaux Ethernet séparés et reliés par la machine C, fonctionnant comme un routeur.

La machine C agit comme un routeur entre ces deux réseaux. Un routeur est un élément qui choisit différentes directions pour les paquets en fonction de



l'adresse IP. Comme il y a deux segments Ethernet séparés, chaque réseau a

son propre numéro de réseau de classe C. Ceci est indispensable car le routeur ne connaît à des interfaces qui sont associés à un numéro de réseau.

Si A veut envoyer un paquet à E, il doit d'abord l'envoyer à C qui peut faire suivre le paquet à E. Ceci est possible car A utilise l'adresse MAC de C et l'adresse IP de E. C va donc recevoir le paquet destiné à E et va le faire suivre en utilisant l'adresse MAC de E, soit parce qu'il la connaît, soit en faisant une requête ARP comme décrit précédemment.

Si E reçoit le même numéro de réseau que A, soit "200.1.2", A essayera d'atteindre E de la même façon qui atteint C, par exemple, en envoyant une requête ARP et en attendant la réponse. Quoiqu'il en soit, comme E est physiquement sur un fil différent, il ne verra jamais la requête ARP et le paquet ne pourra pas être délivré. En spécifiant que E est sur un réseau différent, le module IP de A saura que E ne peut être atteint sans avoir été fait suivre par un nœud (élément reliant deux réseaux différents comme un routeur) de son réseau.

Comment faire son plan d'adressage :

Il s'agit normalement d'un travail de véritable spécialistes, mais il est possible de donner des indications.

Compter le nombre de sous réseaux de votre réseau.

Un sous réseau est formé par toutes les machines connectées de manière à pouvoir s'échanger des paquets IP sans faire intervenir de routeur.

Compter le nombre de machines sur chaque sous réseau.

Le but est de prévoir le nombre d'adresses nécesaires sur ce sous réseau. Il faut compter toutes les interfaces branchées sur ce sous réseau, en incluant les routeurs, serveurs de terminaux, imprimantes, etc.

Calculer le nombre de bits nécessaires pour le numéro de hôte sur chaque sous réseau.

En fonction du nombre de machines actuelles et dans deux ans, et en prévoyant un peu plus large, il faut arrondir ce nombre à la puissance de deux strictement supérieure. Le nombre de bits est la puissance de deux correspondante.

Organiser l'adressage des sous réseaux.

Il est préférable que tous les sous réseaux d'un réseau aient le même masque, car un grand nombre de routeurs ne savent pas encore faire du *variable length subnet mask* (VLSM). Il faut alors compter le nombre de groupes de sous-réseaux que l'on peut former.

Calculer alors la taille de l'espace nécessaire.

En sachant que les sous-réseaux 0 et *max* sont réservés, il faut calculer la taille de l'espace d'adressage nécessaire, et en déduire le nombre équivalent de classes C.

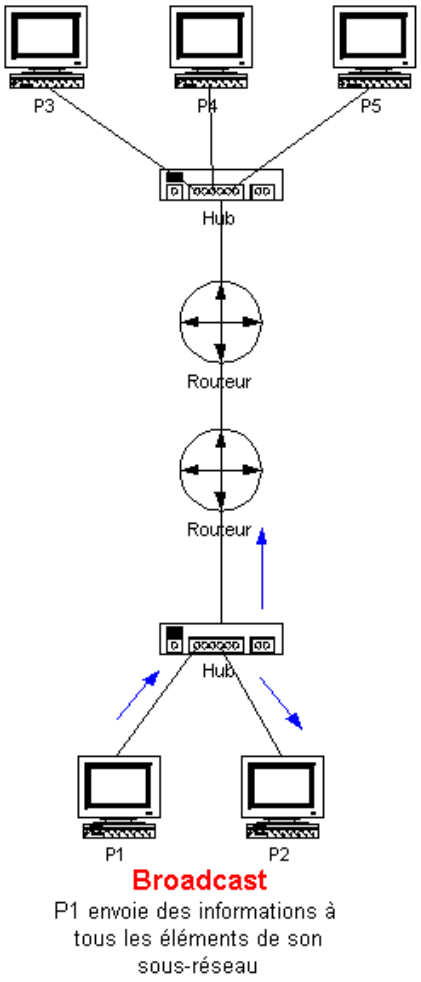
TYPES DE TRAMES TCP/IP

Broadcast :

Le principe du broadcast est d'envoyer une information à tous les ordinateurs du réseau où l'on est. Au lieu d'envoyer en unicast vers l'adresse IP de la chaque machine (ex. 193.169.1.37 avec un masque 255.255.255.0),

on envoie la trame à tous les ordinateurs du sous-réseau en utilisant l'adresse de broadcast (ici, 193.169.1.255). Cette adresse est réservée à cet usage. Chacun des ordinateurs du sous-réseau regarde et traite la trame comme si elle leur était personnellement adressée.

Les trames de broadcast ont une caractéristique particulière : c'est de ne pas pouvoir passer les routeurs puisqu'il s'adresse uniquement à tous les ordinateurs d'un même sous-réseau.



Unicast :

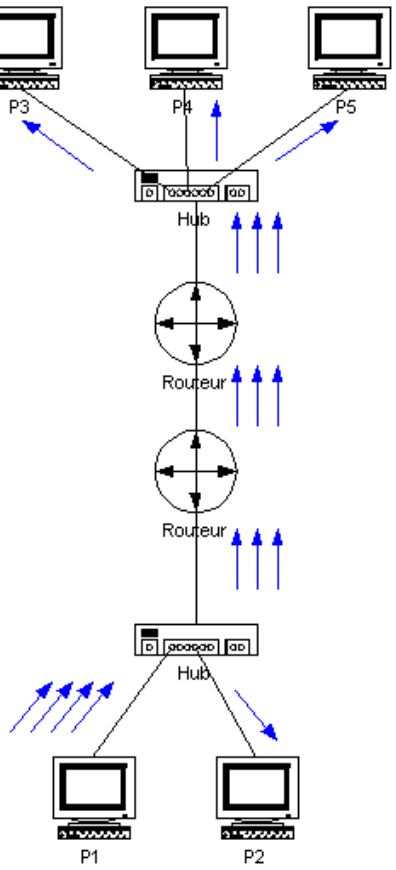
C'est le principe le plus utilisé et le plus simple. Les ordinateurs possédant chacun une adresse IP, on peut envoyer les trames en spécifiant l'adresse IP de l'ordinateur à qui on veut envoyer les informations. Les éléments actifs et passifs du réseau (commutateurs, répéteurs, routeurs, ...) dirigent l'information dans la bonne direction pour que les trames arrivent au bon endroit. Seule la machine ayant l'adresse contenue dans la trame regarde et traite l'information.

Il existe 3 classes d'adresses unicast :

La classe A : Adresses comprises entre 1.0.0.x et 127.255.255.x

La classe B : Adresses comprises entre 128.0.0.x et 191.255.255.x

La classe C : Adresses comprises entre 192.0.0.x et 223.255.255.x



Unicast

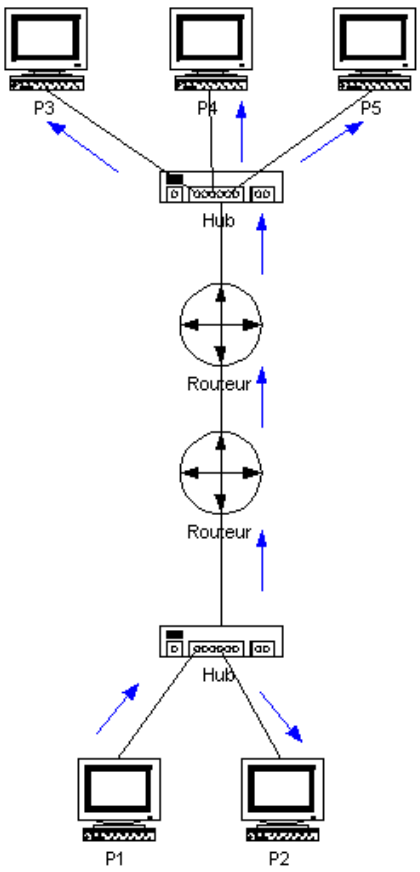
P1 envoie des informations à P2, P3, P4 et P5

Multicast :

Plutôt que d'envoyer les fichiers du serveur vers chacune des machines clientes (unicast) on peut n'envoyer l'information qu'une seule fois et chaque ordinateur client la récupère. En effet, dans un réseau Ethernet par exemple, toutes les trames qui circulent passent par tous les ordinateurs. C'est le principe du multicast : on envoie l'information à une adresse et tous les clients écoutent cette adresse. (utilisé par exemple pour la diffusion de la vidéo….)

Chaque client multicast s'enregistre avec une adresse IP multicast de classe D (entre 224.0.0.0 et 239.255.255.255 sauf 224.0.0.0 non utilisée et 224.0.0.1 qui correspond au "broadcast du multicast"). C'est sur cette adresse que les informations vont être envoyées.

Les clients écoutent ce qui arrive sur cette adresse et suivent la procédure décrite par le protocole multicast implémenté.

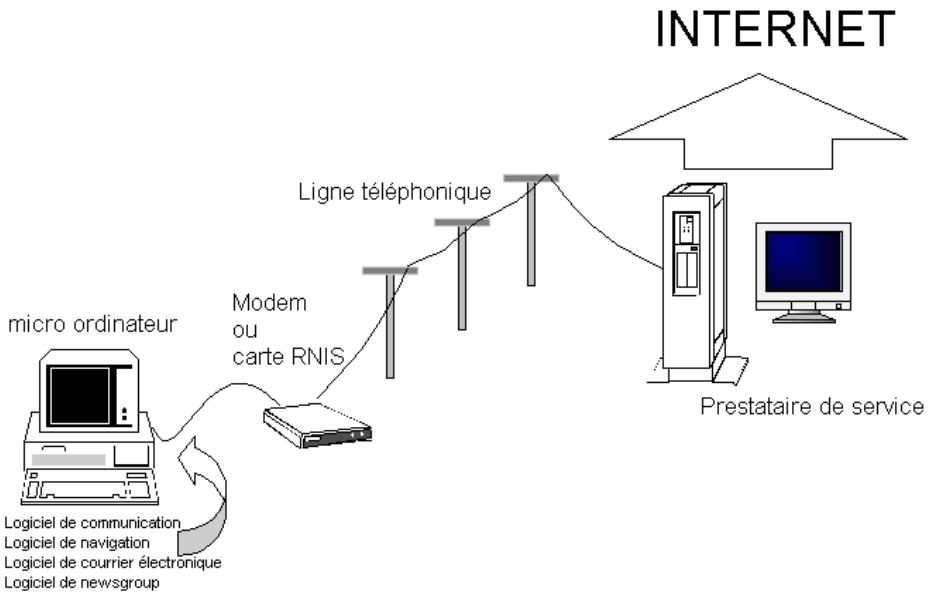


Multicast
P1 envoie des informations à P2, P3, P4 et P5

INTERNET

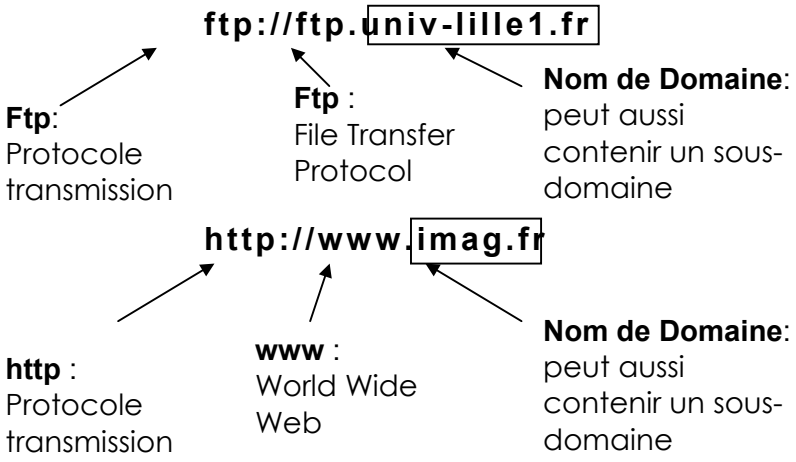
Pour accéder à l'Internet

1. Un ordinateur
2. Un logiciel de communication pour établir la connexion TCP/IP avec le fournisseur :
3. Un ensemble de logiciels permettant
    - La navigation sur Internet (ou browser ou butineur)
    - L'accès aux forums de discussion (newsgroup)
    - L'accès au courrier électronique
4. Une prise de téléphone à laquelle est raccordée votre ordinateur via
    - Un modem (réseau téléphonique analogique) solution usuelle
      ou
    - Une carte RNIS (réseau numérique)
5. Un abonnement chez un fournisseur d'accès à l'Internet ou provider ou prestataire de service.



L'adresse URL :

Uniform Resource Locator (Localisateur Universel de Ressources). Ce type d'adresse fait appel à l'alphabet pour rendre la mémorisation plus facile. A la différence d'une adresse IP, une URL se lit de droite à gauche



Un nom de domaine (imag.fr) se décompose en

- Un Top Level Domain (exemple : fr)
- Un nom d'organisation (appelé aussi nom de domaine) (ex : imag)

Les Top Level Domain les plus courants sont:

Clé	Contenu
.com	Entreprise commerciale
.edu	éducation
.gov	organismes gouvernementaux
.mil	organisations militaires
.net	intervenant d'internet
.org	instance gouvernementale ou institution administrative

Cependant si ces domaines sont a priori internationaux, ils sont à forte dominante américaine. De plus chaque pays possède son nom de domaine (à l'exception des USA qui utilisent les 6 domaines précédents).

Clé	Contenu
.au	Australie
.ca	Canada
.de	Allemagne
.fr	France
.uk	United Kingdom

L'internic se chargeant de l'attribution des adresses dans les domaines internationaux, c'est le NIC France qui se charge des attributions des noms de domaine en .fr

http://www.nic.fr

Domaines et sous domaines

Nom de domaine propre

www.nom.fr

Nom de sous domaine principal

www.nom.fournisseur.fr

Nom de sous domaine partagé

www.fournisseur.fr/nom

Evolution :

Le succès d'Internet rend chaque jour le travail des organisations chargées d'attribuer une adresse de site de plus en plus difficile.

A la suite d'une réunion tenue à GENEVE fin Avril 97, le monde a été divisé en 7 régions, qui accueilleront chacune 4 organisations pour distribuer les adresses de sites, et on pourra faire jouer la concurrence entre elles (à terme ces organisations devraient se multiplier, même si on ne sait pas encore comment réellement ces organisations seront choisies). Du même coup, les « org » « .net » « .fr »ou « .com » vont être épaulés par 7 nouvelles clés dont le détail suit:

Clé	Contenu
.firm	Site à vocation d'affaires et de relations inter-entreprises
.store	Site à vocation de commerce électronique
.web	Site d'organisations se contentant d'activités ayant trait au WEB
.arts	Site à vocation culturelle
.rec	Site spécialisé dans le divertissement
.nom	Site personnel
.info	Site spécialisé dans l'information « ON LINE »

Dans les prochains mois, les nouvelles extensions de noms de domaines tel que .PRO, .INFO, .BIZ, .NAME, .MUSEUM, .AREO, et .COOP seront disponibles!

Il est maintenant possible, depuis le 26 février 2001, de réserver sur Internet des noms de domaines en français, c'est à dire comportant des mots avec des accents. Auparavant exclus des adresses de sites Internet, les mots français composés de caractères accentués pourront bientôt figurer en tête de nos sites Web.

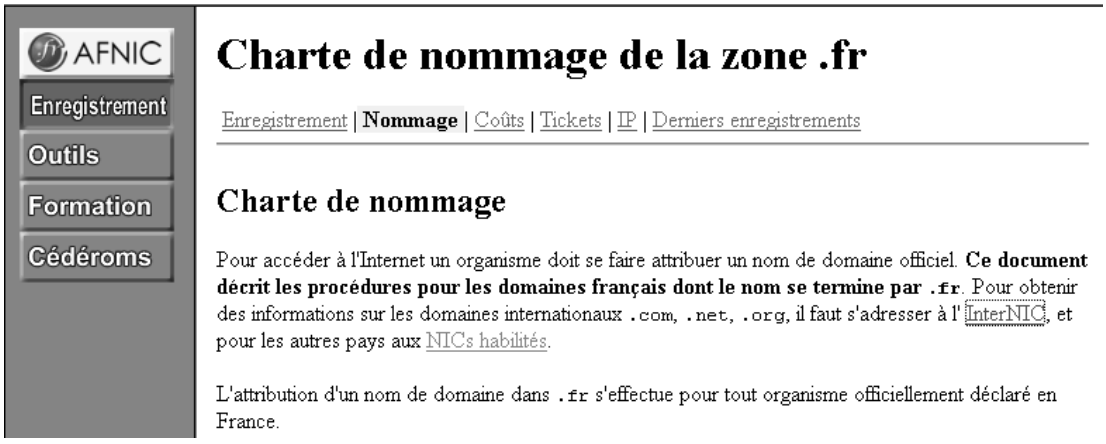
Cette alternative est très intéressante pour les internautes d'expression française : « Cette récente possibilité permettra éventuellement d'éviter certaines confusions aux internautes débutants et pourra accroître la présence du français sur Internet ».

Cette nouvelle survient suite à l'annonce faite par le « Verising Global Registry » qui signalait, au mois de janvier 2001, l'expansion de l'environnement d'enregistrement multilingue à vingt-huit langages européens.

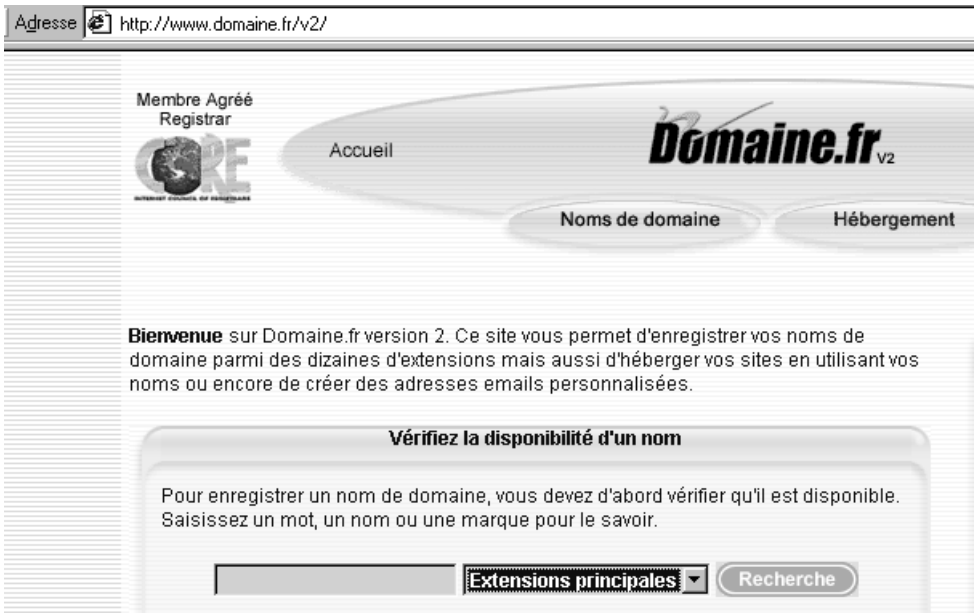
Il est important de noter que les noms de domaines avec accents ne peuvent pas être utilisés sur Internet avant la fin des tests du « Verisign Global Registry ». Par contre, les noms de domaines doivent être réservés le plus rapidement possible afin d'assurer leur disponibilité au moment de les rendre actifs sur Internet. Le « Verisign Global Registry » prévoit offrir cette opportunité sous peu.

Si l'on veut on peut se donner un nom en suivant une charte de nommage, dont la consultation ou le téléchargement peuvent se faire à

http://www.nic.fr/enregistrement/nommage.html



La réservation ou la vérification de possibilité réservation peuvent se faire à de multiples endroits, comme par exemple à l'adresse suivante :



La tarification d'un dépôt de nom de domaine est relativement peu coûteuse

L'adresse E-Mail :

Ou adresse de courrier électronique, utilisée pour la messagerie, identifie un utilisateur sur internet, de la forme :

nom@Organisation.Domaine

le **@** se lit "at"

On parle aussi de FQDN, c'est à dire FULLY QUALIFIED DOMAIN NAME

A partir du moment ou le nom du service postal est varié, il est quasiment impossible de trouver une adresse Mail dans un annuaire…

Les accents dans le Courrier Electronique

Les accents posent souvent problème lors de leur envois via le courrier électronique, à tel point que généralement il est de bon ton de ne …pas en mettre pour peu que le destinataire réside hors de France. A l'origine l'E-mail est nord américain, où les caractères accentués ne sont pas légion, et dans la conception du Mail, ceux-ci ont été un peu délaissé.

Lorsque l'on envoi un Mail, les caractères sont transmis sous forme binaire, plus exactement grâce au code ASCII sur 7 bits, or ce codage ne prévoit pas les accents, qui sont relégués dans les codes dits "nationaux", c'est à dire interprétés différemment par chaque pays, justement pour pouvoir permettre les particularités nationales… Ces caractères nationaux sont codés grâce à un 8° bit, mais le problème tient dans le fait que le courrier électronique repose sur un système à 7 bits !

Alors en emplois une ruse, "pour transmettre des codes de 8 bits avec un système à 7 bits, on aligne tous les codes à 8 bits bout à bout, formant un gigantesque code, et on redécoupe le tout en morceau de 7 bits. Evidamment il faut que à la reception on fasse l'opération inverse pour retrouver le message originel (on doit former un morceau unique avec tous les mots de 7 bits, puis redécouper le tout en morceau de 8 bits…Cet encodage prends le nom d'encodage 8 bits MIME

Limites aux accents

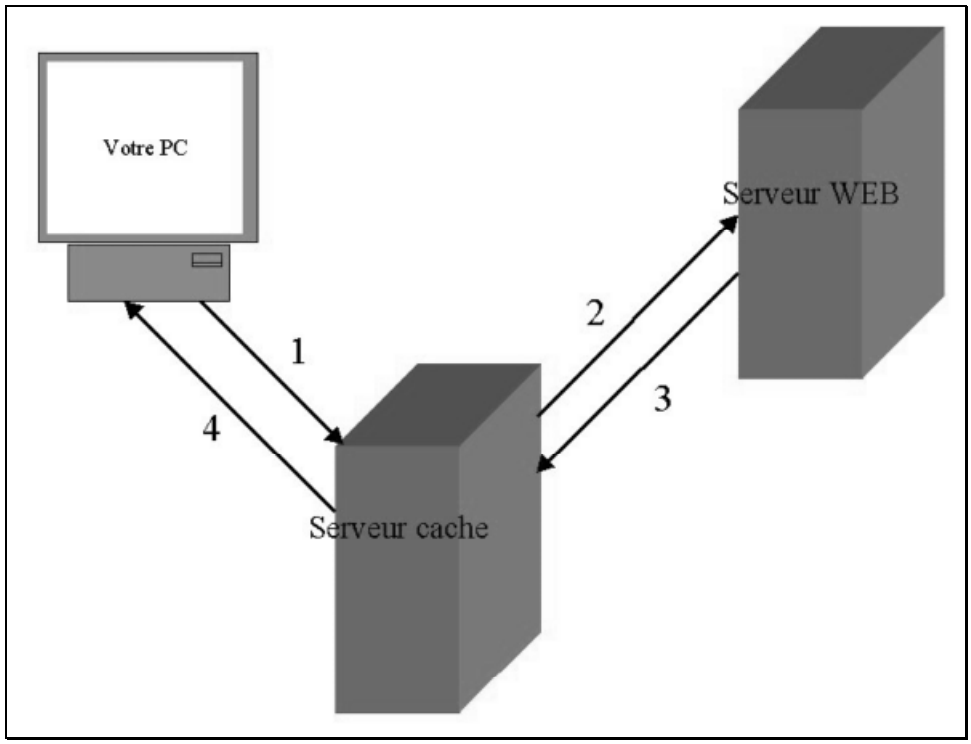
pour que donc vos accents voyages sans problème, il faut

- que votre logiciel de courrier gère ce type d'encodage
- que le logiciel de courrier de votre correspondant le gère également
- que tous les routeurs (ordinateurs par lesquelles passe votre courrier) "passent" l'encodage 8 bit MIME

Au fur et à mesure les accents passent de plus en plus….

Le proxy

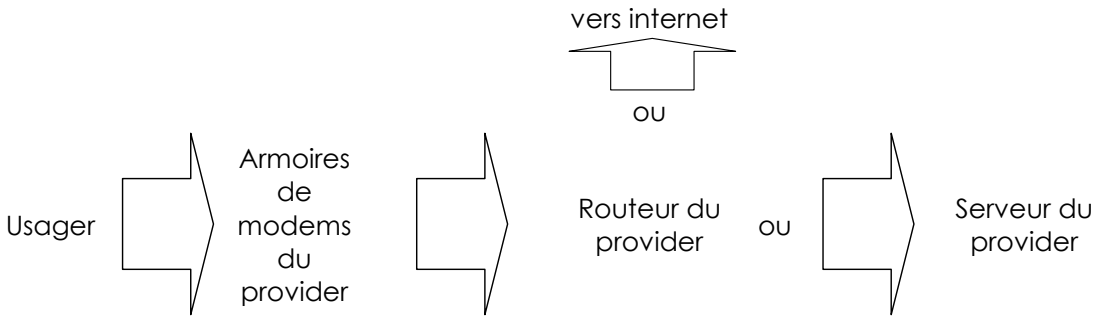
Le processus de consultation des pages Web peut être optimisé. Imaginons que Microsoft fasse une annonce très importante : beaucoup d'usagés veulent consulter son site. Pour des raisons évidentes d'engorgement, il n'est pas possible de transmettre chaque demande au site de Microsoft. Un mécanisme très astucieux, fonctionnant selon le principe de la mémoire cache, permet pourtant de satisfaire tout le monde. Voici comment les choses se passent. La première fois la page Web est transmise à l'usager, mais elle est également stockée sur un disque dur, chez le fournisseur. S'il se présente une requête identique (provenant d'un autre usager), il suffit de consulter le disque dur (du fournisseur), de constater que la page Web s'y trouve déjà, et de la renvoyer . Sur Internet on ne parle pas de mémoire cache mais de « proxy ». Chaque fournisseur stocke ainsi quotidiennement plusieurs gigaoctets de données. Quand l'espace alloué au proxy est plein, les premières pages entrées sont les premières effacées. Le choix des pages à effacer tient aussi compte de la durée de vie des pages, indiquée par le créateur du site.



1. Vous essayez d'accéder à un serveur WEB. Votre outil de navigation envoie la requête au serveur cache
2. Celui-ci vérifie que la page demandée n'est pas déjà stockée sur son disque dur. Si c'est le cas, il la renvoie directement à votre ordinateur. Sinon, il demande la page au serveur WEB distant.
3. Le serveur WEB renvoie la page demandée. Le serveur cache en fait une copie, qu'il garde pour de futures demandes
4. Le serveur cache renvoie la page à votre ordinateur

Anatomie d'un fournisseur d'accès

Le fournisseur d'accès est un point de passage obligé entre un particulier et le réseau Internet. Il dispose d'une configuration matérielle lourde, car il doit assurer le meilleur service possible à ces clients pour réduire les temps d'attente. Pour d'évidentes raisons économiques, son équipement ne permet pas de connecter tous les abonnés en même temps, mais il est optimisé en conséquence, en fonction de statistiques de connexions(répartition dans le temps et durée).



Armoire de modems	Routeur	Serveur
Chaque prestataires de service dispose de centaines de modems, chacun prenant en charge un seul usager à la fois pendant tout le temps de la connexion. Habituellement, les modems fonctionnent jusqu'à la vitesse de 33,6kbps, mais des techniques particulières leur permettent de travailler jusqu'à 56kbps (en émission seulement)	Cet équipement de télécommunication analyse les paquets transmis par les modems et décide, au fur vu de leur adresse IP (la destination), s'il faut les envoyer sur Internet ou si les informations demandées sont disponibles sur l'ordinateur du fournisseur d'accès (serveur Proxy). Il reçoit aussi les données d'Internet et décide s'il faut les transmettre à l'utilisateur ou à l'ordinateur.	L'ordinateur gère différents services indépendants : Le Web Le Proxy La messagerie électronique Les groupes de discussion

Serveur Web et Pages HTML :

Les sites Internet ne répartissent en deux catégories majeures :

- Statiques : Toutes les informations fournies aux internautes sont stockées sous la forme de fichiers figés sur le disque dur du serveur Web, notamment des pages HTML.
- Dynamiques : Avant d'envoyer les informations demandées, le serveur est capable de leur appliquer divers traitements en temps réel. Ces informations sont souvent stockées dans des bases de données dont le contenu est extrait par des requêtes, manipulé, puis mis en forme.

Il existe toute une gamme de technologies serveur permettant la mise en place de solutions dynamiques. Nous traiterons les principales dans ce chapitre.

De nombreuses solutions de ce type utilisent des langages de script (VBScript, Perl, PHP, etc.) ou de requête (SQL et variantes propriétaires) ; elles sont alors désignées sous l'appellation "server scripting".

Serveurs statiques

Les premiers serveurs disponibles sur le Web étaient seulement capables de présenter des informations sous forme de pages HTML fixes stockées sur disque.

On les appelle "serveurs statiques", dans la mesure où ils n'adaptent pas le contenu des informations fournies en fonction de critères choisis par l'utilisateur.

Les serveurs de ce type restent adaptés à de nombreux domaines (présentation d'informations figées), et se révèlent à la fois rapides et très peu onéreux.

Serveurs dynamiques

L'émergence de technologies permettant de prendre en compte les choix de l'utilisateur, et le besoin toujours croissant d'interactivité, ont conduit à la création de "serveurs dynamiques", qui sont capables de générer le contenu qu'ils présentent en fonction des choix de l'utilisateur.

Pour la réalisation des serveurs dynamiques, comme souvent sur le Web, deux tendances s'opposent. La première repose sur les normes définies (HTTP, CGI).

L'autre, poussée par les éditeurs de logiciels, consiste à proposer des extensions (API) aux serveurs HTTP pour permettre d'inclure des ordres particuliers dans les pages HTML.

HTTP (Hyper Text Transfer Protocol) : est un protocole d'échange de document entre un client et un serveur. Il s'appuie sur une procédure simple:

- le client établit une connexion,
- le client envoie une requête au serveur en précisant le document qu'il veut consulter,
- le serveur renvoie une réponse contenant un code de statut et le texte du document s'il est disponible,
- le serveur ferme la connexion.

Les requêtes sont complètement indépendantes les unes des autres. On dit que HTTP fonctionne en mode non connecté, c'est à dire qu'il ne garde pas d'information sur une connexion d'une requête à une autre. Ce mécanisme est transparent pour l'utilisateur pour qui le chargement d'une page HTML est uniforme.

HTML (Hyper Text Markup Language) : est un langage de description de page, il contient à la fois le texte à afficher et les balises permettant de le mettre en forme dans la fenêtre du navigateur Web. Il permet également d'enrichir un page Web d'éléments multimédias (image, séquence sonore ou vidéo) et de la rendre interactive grâce à l'insertion de liens hypertexte.

XML (eXtensible Markup Langage) : est un métalangage qui décrit un document. Il traite de manière séparée la structure, la présentation et le contenu. Il est ainsi possible de générer différents formats de présentation du document selon les besoins (HTML, RTF etc. ...). Le document est traité de manière indépendante du support. Il est donc possible d'envisager des traitements documentaires, comme la personnalisation des contenus adaptés aux différents services de l'entreprise.

Il a été conçu pour dépasser le simple aspect de présentation de HTML, en permettant des traitements et interactions plus élaborées.

Il ouvre la perspective d'un langage pivot, standard à toutes applications. Microsoft d'ailleurs le présente comme le format de base des documents dans les futurs versions de Windows. (Ce qui n'est pas à négliger quand on sait le poids des applications bureautiques dans les entreprises).

CGI (Common Gateway Interface) : est une norme qui permet d'écrire des programmes qui peuvent communiquer avec divers types de serveurs Web. Elle définit une interface par laquelle le serveur peut passer l'information au programme et inversement. Cet outil est utile pour l'interaction sur le Web, en effet, c'est un mécanisme efficace pour l'interrogation de bases de données. CGI est donc un mécanisme simple, compatible avec tous les clients et le serveurs, et bien adapté à des interrogations independantes les unes des autres. Mais, il est consommateur de ressources sur le serveur, mal adapté à l'établissement d'un vrai dialogue entre le poste client et le poste serveur, et difficile à administrer sur le serveur pour garantir la sécurité.

Java : est utilisé pour sa portabilité, sa technologie orientée objets, il est propice au développement d'applications réseaux. Il est également possible de télécharger un programme Java et l'exécuter dans le navigateur

(applet). Les applets sont téléchargées dans le navigateur comme n'importe quel document HTML. Ce document devient vivant et intelligent une fois chargé dans le navigateur : une applet Java peut être aussi riche qu'une application bureautique que client-serveur. Cependant, pour des raisons de sécurité, une applet ne peut ni modifier ni lire le contenu du disque dur. L'applet Java peut établir une connexion permanente avec le serveur depuis lequel elle a été téléchargée, n'échangeant que les informations strictement nécessaires, exécuter une partie des traitements sur le poste client.

JavaScript et VBScript : ce sont des langages scripts, ils sont téléchargés sous forme de texte et interprétés par le navigateur.

JavaScript : permet de rendre les pages HTMLplus interactives, de préparer les paramètres envoyés au serveur par l'intermédiaire des requêtes CGI, de mettre en forme le résultat et d'appeler les applets Java et d'accéder à leur variable. Il ne permet pas de réaliser de connexion avec un serveur distant comme le fait Java.

VBScript : est un langage proposé par Microsoft, directement concurrent de JavaScript. Il permet de réaliser des interfaces réactives et d'effectuer des contrôles locaux et ainsi minimiser les échanges entre le client et le serveur. Ce sont deux langages similaires mais non compatibles avec les même navigateurs.

ActiveX : est associé à DCOM comme Java est associé à RMI. ActiveX va permettre de télécharger des morceaux de programmes. Ceux-ci utilisent alors l'architecture DCOM pour communiquer directement avec un objet située sur le serveur. Comme dans le modèle Java/RMI, l'intranet sert à télécharger l'application cliente, mais ensuite l'interrogation à distance de la base de données s'effectue avec un middleware qui sort du domaine classique de l'Intranet.

DCOM (Disributed Component Object Model) : permet à des composants distants de coopérer comme s'ils étaient sur la même machine. Ce modèle fondé au départ sur la communication entre composants applicatifs au sein d'un même système, s'est étenduaux architectures distribuées en s'enrichissant de fonctions de nommage et d'appels à distance via les RPC.

NAT :

Le NAT, dont la traduction française peut donner "translation d'adresse" est le plus simple des deux mécanismes permettant d'accéder à internet. Voici son principe de fonctionnement :

Soit un routeur gérant le NAT avec 2 interfaces :

- Coté LAN : Réseau d'entreprise avec un adressage interne type 10.0.0.0.
- Coté WAN : Réseau connecté à l'internet. Ce réseau dispose d'une classe 'C' dont une seule adresse est actuellement utilisée par l'interface elle-même.

1. Une personne connectée sur ce réseau d'entreprise (qui a pour adresse 10.0.0.2 par exemple) lance son navigateur et essaye de se connecter à Internet.
2. Le premier paquet IP destiné à l'Internet est envoyé au routeur.
   Ce dernier se dit : " Je ne peux pas envoyer un paquet qui a une adresse source en 10.0.0.2 car personne ne sera capable de renvoyer une réponse. Prenons une adresse disponible parmi la classe 'C' et remplaçons l'adresse privée 10.0.0.2 par cette adresse valide. Je notes dans un coin que 10.0.0.2 a été traduit en "x.x.x.x".
3. Le paquet ainsi modifié peut partir vers l'Internet. Lorsque le destinataire veut faire une réponse, il l'adresse à "x.x.x.x" qui est une adresse valide dans la classe 'C'. Le paquet est routé jusqu'à notre routeur.
   Ce dernier se dit : "*Le paquet a pour destination* "x.x.x.x". *Selon ma table, cette adresse est la traduction de 10.0.0.2. Je remplace donc l'adresse de destination par 10.0.0.2 et je fais suivre le paquet*".
4. Si une autre personne (disons 10.0.0.3) essaye de se connecter à Internet, le routeur va chercher une adresse disponible dans la classe 'C' et faire la même chose. Tant qu'il y a des adresses disponibles dans la classe 'C', chacun peut utiliser Internet. Un simple mécanisme de "timeout" permet de récupérer les adresses IP de la classe 'C' lorsque elles ne sont plus utilisées pendant un certain temps.

Sécurité :

Ce système NAT permet une légère sécurité :

- le seul moyen de rentrer sur le réseau interne est d'utiliser une adresse IP valide parmi celles de la classe 'C'. Si le serveur qui a pour adresse ip réelle 10.0.0.100 n'accède jamais à Internet, son adresse n'apparaîtra jamais dans la table du routeur. Il sera ainsi impossible de contacter directement cet ordinateur depuis l'extérieur.

SUA :

Le SUA, dont la traduction française peut donner "Adresse unique d'Utilisateur" est le plus compliqué des deux mécanismes permettant d'accéder à internet. Voici son principe de fonctionnement :

Soit un routeur gérant le SUA avec 2 interfaces :

- Coté LAN : Réseau d'entreprise avec un adressage interne type 10.0.0.0.
- Coté WAN : Réseau connecté à l'internet. Ce réseau dispose d'une classe 'C' dont une seule adresse est actuellement utilisée par l'interface elle-même.

Il y a bien un système NAT intégré, mais avec une limitation : une seule adresse IP (disons "y.y.y.y") - celle de l'interface elle-même - est disponible pour faire tout le travail. Or si nous ne faisons que remplacer les adresses internes par celle de l'interface, il devient impossible de trier les réponses lorsque elles reviennent. Il est alors nécessaire de trouver un moyen de reconnaître les réponses afin de pouvoir les faire suivre aux destinataires du réseau interne. Cela se fera par un mécanisme de réaffféctation aléatoire de n° de port

1. Un utilisateur du réseau interne veut accéder au service Telnet sur Internet. Le paquet IP émis comportera l'entête suivante :

Source IP	= 10.0.0.2	
Source Port	= 40077	
Destination IP=	123.45.67.89	(host désirée)
Destination Port=	23	(le port telnet)

2. le routeur modifie le paquet qui ressemble ressemble à :

Source IP =	y.y.y.y	(l'adresse IP de l'interface WAN du routeur)
Source Port=	9000	(un port quelconque choisi par le routeur)
Destination IP=	123.45.67.89	
Destination Port=	23	

3. Le paquet ainsi modifié peut partir vers l'Internet. Lorsque le destinataire veut faire une réponse, il l'adresse à "y.y.y.y" qui est l'adresse de notre routeur port 9000. Le paquet est routé jusqu'à notre routeur.
   Ce dernier se dit : "*Le paquet a pour destination le port 9000. Selon ma table, ceprt est la traduction de 10.0.0.2 port 40077. Je remplace donc l'adresse de destination par 10.0.0.2 port 40077 et je fais suivre le paquet*".
4. Si d'autre requête doivent être effectuer, le routeur procédera de la même manière en utilisant les port suivant disponible (9001, 9002, ...) Étant donné qu'il y a plus de 64000 ports disponibles, les seules limitations sont la taille mémoire, la vitesse du processeur ou la vitesse de la liaison.

Sécurité :

Le système SUA garantie une sécurité un peu supérieur au simple NAT puisque

- le pirate doit alors deviner le numéro de port et qu'il n'a aucun moyen de contrôler l'assignation de ces ports.
- Quand bien même le pirate trouverai un port, il ne peut pas savoir quel service est utilisé derrière car les ports sont alloués " aléatoirement " en fonction des services demandés.

Un problème se pose lorsque le réseau interne comporte des application fonctionnant en mode serveur de la liaison: Lorsque le client se trouve à l'extérieur, il y a un gros problème. Imaginons qu'un personne sur Internet veuille accéder au service telnet sur un serveur du réseau interne. Il essayera alors d'atteindre la machine y.y.y.y sur le port 23 (celui du telnet). Malheureusement, le SUA va être bien embarrassé par ce paquet, car aucune correspondance existe pour le port 23. Ce port n'a jamais été utilisé " en sortie " et donc le routeur ne peut faire aucune correspondance.

Une solution existe. Elle consiste à convertir tous les paquets " sans correspondance " vers une adresse IP par défaut sans changer quoi que ce soit sur le numéro de port. Cette solution permet de résoudre le problème, mais un seul serveur pourra être atteint de cette manière. Ceci permet par exemple de faire fonctionner un et un seul serveur Web.

INTERNET ET SECURITE

Introduction :

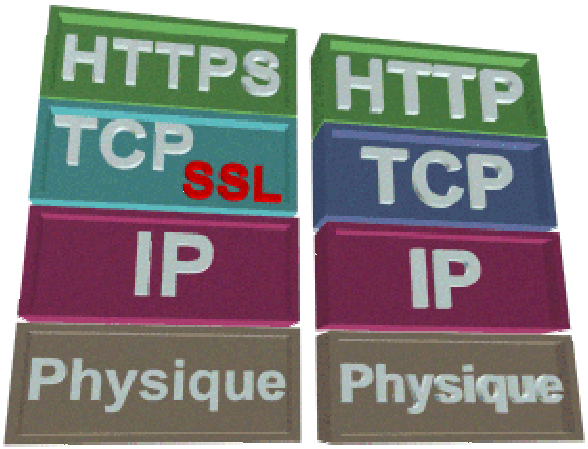
Un mode de paiement sécurisé est aujourd'hui devenu nécessaire car le **commerce électronique** sur Internet prend une grande ampleur surtout aux USA. En france ce type de commerce est encore a ses début (CA de 300Millions de Francs contre 7Milliards de Francs sur Minitel en 1999) . Pour que cela marche, Il faut être en mesure d'éliminer tous risques d'interception des informations lors des transactions. C'est là que le **cryptage** intervient. En effet comme il est impossible de prévenir d'une interception frauduleuse des données il faut donc rendre ces informations illisibles par son intercepteur. Pour cela **RSA** a développé en 1977 un système de cryptage dit "**a clé publique**" qui répond parfaitement à ce besoin. Un standard de communication Web basé sur cet algorithme de cryptage a donc été mis en place . C'est le protocole **HTTPS .** Bien sur le paiement électronique n'est pas la seule application de ce protocole, le but premier étant de pouvoir établir une communication sûre entre un client et un serveur localisés de partout dans le monde. Dans cet exposé seront donc présentés le mécanisme de fonctionnement d'un tel protocole ainsi que son application pour le commerce électronique (paiement direct ou off-line et paiement indirect ou on-line).

Comme nous avons vu le paiement sur Internet est en pleine expansion , en France plusieurs banque proposent des contrats de télécommerce notamment le **Credit Agricole** et la **BNP** . Aujourd'hui les clients ont encore du mal a accepter un tel commerce, les habitudes sont longues à changer. Ceci dit, il y a peu de risque de fraudes sur Internet sécurisée, vous pouvez donc commander sans soucis. Il faut quand même s'assurer que votre navigateur supporte des clés dites fortes (128 bits au moins) . Attention par défaut votre navigateur ne sait pas travailler avec ce type de clê. Il faut installer un patch (utilitaire qui modifiera l'exécutable du navigateur)

Un nouveau mode de paiement est aujourd'hui en train de faire son apparition. Un lecteur de carte personnel (voir photo) connecter au réseau téléphonique France Telecom vous permettra de régler vos achats. c'est le projet **C-Set** (Cybercom) : le Crédit Agricole, le Crédit Mutuel, les Banques Populaires, La Poste, France Telecom et Bull sont des partenaires de ce projet.

HTTPS :

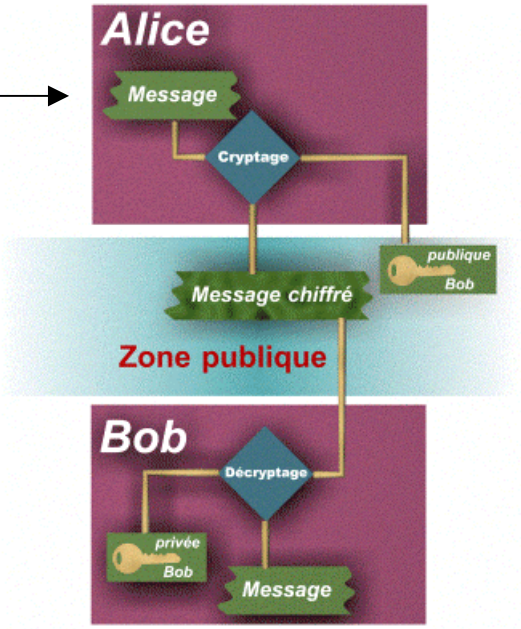
Le protocole HTTPS n'est rien d'autre que le protocole HTTP au dessus d'une implémentation de TCP utilisant SSL (Secure Socket Layer). Dans votre navigateur il suffit de taper **https://www.somewhere.com** pour être connecter a un serveur via SSL . SSL est un protocole de transport sécurisé développé par la société Netscape (fonctionnant également sur Microsoft IE4.X) basé sur l'algorithme de cryptage RSA . SSL n'est d'ailleurs pas spécifique à HTTPS et peut servir a tous les protocole de sessions (HTTP, FTP, TELNET...) mais nous rentrerons dans les détails de SSL dans la page qui lui est consacrée. Il existe aussi une autre différence entre HTTP et HTTPS, lors de la connexion, un mécanisme d'authentification s'opère vous garantissant que vous êtes bien connecté au serveur désiré . Ce mécanisme est décrit dans la page consacrée au Certificat.



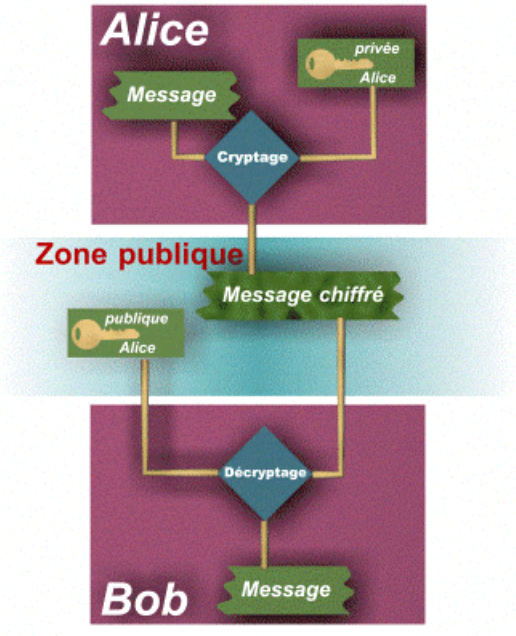
SSL :

SSL est une extension de TCP qui permet de garantir un transport sécurisé entre un client et un serveur localisés dans le monde. Ce protocole a été mis en place par la société **Netscape**. La sécurité est assurée par un système de **cryptage a clé publique** inventé par la société **RSA** en 1977. Il est important de bien comprendre le fonctionnement d'un tel algorithme de cryptage : Cet algorithme fonctionne a l'aide de 2 clés une publique et une privée, tout phrase cryptée par la clé publique ne peut être décryptée que par la clé privée et vice-versa.

Grâce a ce principe, nous pouvons établir une transmission sécurisée (voir **schéma 1**) de Alice a Bob. Bob diffuse sa clé publique, Alice crypte le message qu'elle désire envoyer à Bob avec cette clé. Elle est alors sûre que seulement Bob pourra décrypter ce message. Bien sur il faut s'assurer que la clé présente dans la zone publique est bien celle de Bob pour cela il existe un mécanisme de **certificat** décris plus loin.



Transmission de Alice a Bob sécurisée



Signature électronique d'Alice

Il est aussi possible grâce a ce principe de signer électroniquement (voir **schéma 2**) .
En effet si Alice crypte un message avec sa clé privée seulement sa clé publique pourra le décrypter, Bob est donc sûr que c'est Alice qui a signé ce message.

Certificats :

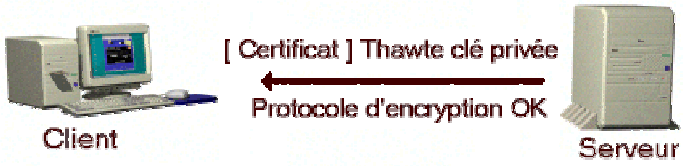
Comme nous avons vu , il n'est pas possible de garantir qu'une clé présente dans la zone publique appartient bien à la personne que vous désirez contacter de manière sécurisée. Pour cela nous avons besoin d'un **tiers de confiance** qui va lui assurer l'appartenance des clés publiques . Aujourd'hui nous trouvons plusieurs organismes qui s'occupent d'un tel travail, en France **Thawte** est certainement le livreur de certificat le plus important. Donc pour pouvoir mettre en place un serveur HTTPS, il vous faut impérativement un certificat. Le format des certificats est défini par la norme **X509**. (Voir en Annexe un exemple de certificat.)

Procédé de certification:

Le procédé de certification est assez simple : vous contacter un tiers certificateur, vous lui transmettez vos coordonnées et après s'être assuré de la validité de ces informations, il vous donne une chaîne de caractère qui est en fait le certificat crypté par la clé privée ce ce même tiers (signature électronique du tiers). Les clés des certificateurs sont souvent des clés dites fortes (au moins aujourd'hui) de **1024 voire 2048 Bits** . Le navigateur du client (Netscape , IE , Opera ...) a déjà la connaissance d'un certain nombre des ces sociétés (de leurs clés publiques) , il va donc pouvoir s'assurer de la validité d'une adresse HTTPS .

Description de la connexion HTTPS:

Etape 1 : Le client envoie une chaine aléatoire au serveur plus le protocole d'encryption qu'il souhaite utiliser (Longeur des clés , sur-encryption , ...)



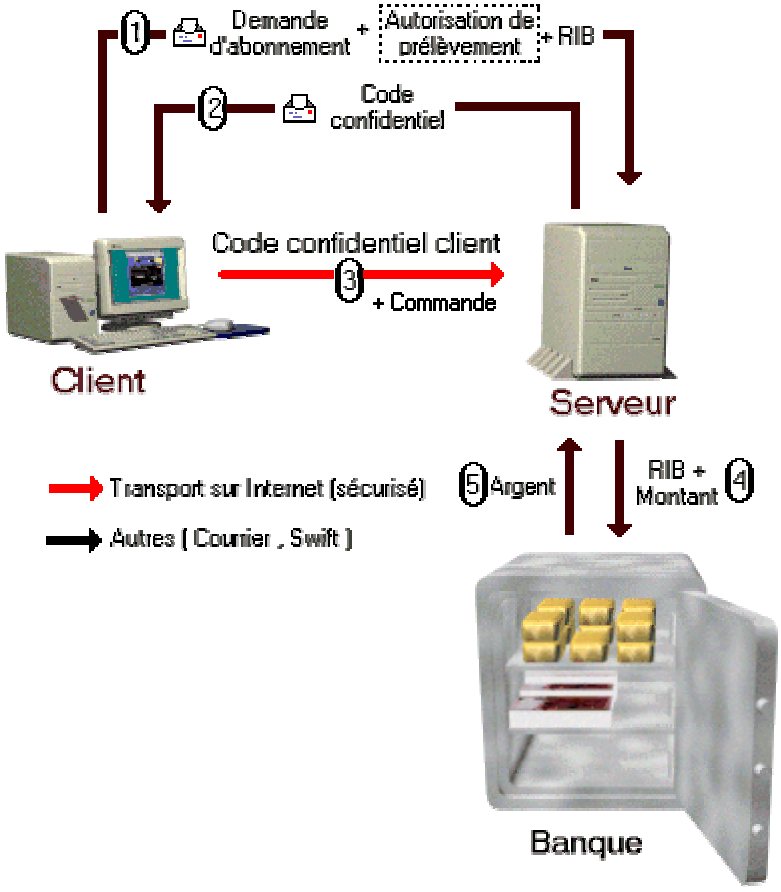
Etape 2: Le serveur répond par son certificat et précise quel protocole d'encryption il supporte . Le client décrypte le certificat , en extrait la clé publique du serveur grâce aux clés de certificateurs intégrées.

Etape 3:. Le client génère ensuite un germe aléatoire qui va servir a produire 2 clés (aujourd'hui de **40 à 128Bits**) : une clé d'écriture et une clé de lecture, puis il transmet ce germe au serveur qui va lui aussi générer ces 2 clés de la même façon. Il faut noter que le fait que le client choisisse lui même son germe aléatoire, lui donne plus de sécurité.

Etape 4: Le serveur, ayant généré ses 2 clés, crypte la chaine aléatoire du début avec la clé d'écriture. Le client pourra donc vérifier le bon fonctionnement en décryptant cette chaine par sa clé de lecture (puisque ces clés sont symétriquement égales) . A ce niveau nous avons donc établie une communication sécurisée d'un client a un serveur.

Il faut noter que des sur-encryptions sont largement utilisées de façon a garantir une sécurité encore plus grande. On trouve souvent du **MD5, RC2 , RC4**. Il faut également noter qu'a partir de l'étape 3 nous pourrions utiliser n'importe quel système de cryptage y compris des systèmes à clé privée (**DES**) . Aussi, Les clients demandent régulièrement un changement de clé (génératiion d'un nouveau germe) au serveur lors d'une transmission.

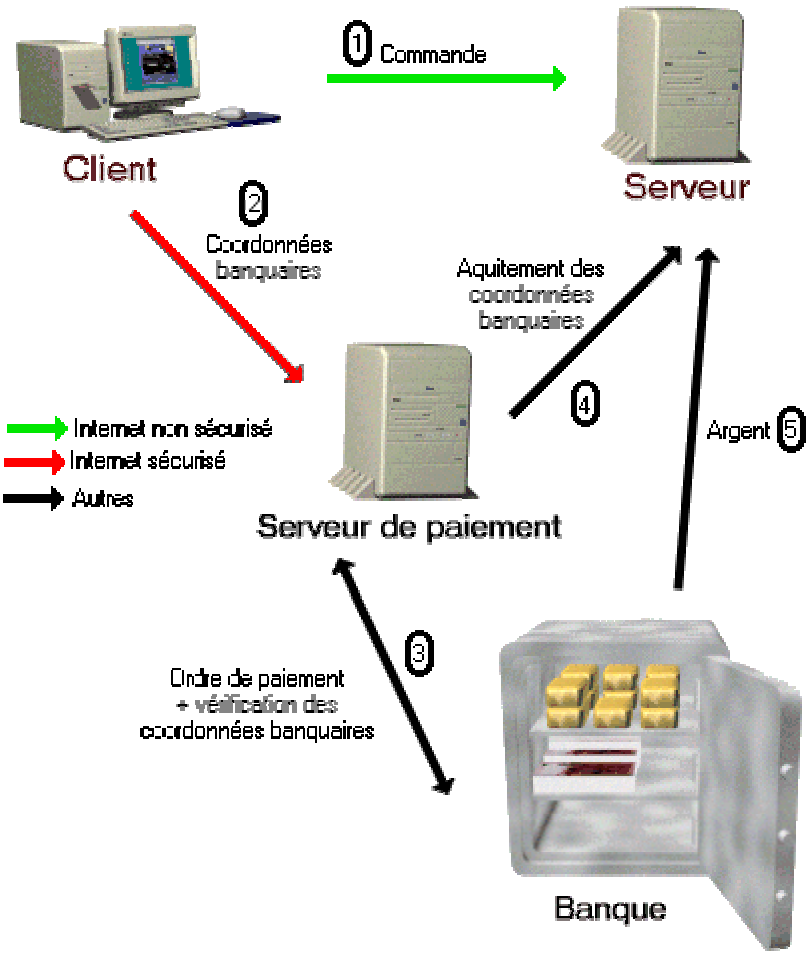
Paiement sécurisé direct (off-line) :



Il s'agit d'un mode de paiement d'un client vers un serveur qui ne fait pas appel a une société externe spécialisée dans le paiement électronique. Ce qui veux dire que ce serveur doit lui-même assurer l'authentification des ses clients et passer un accord avec une banque qui accepte de payer sur simple présentation d'un RIB d'un client (l'autorisation de prélèvement n'étant pas forcement obligatoire). Bien sûr en France, une banque accordera ce privilège uniquement à un organisme auquel elle a entière confiance (Fonction publique ,Société renommée).

Bien que RSA semble aujourd'hui un très bon procédé de cryptage, ce système a l'énorme avantage de ne faire transiter **aucune coordonnées bancaires confidentielles sur l'Internet**. En revanche chaque client est obligé de satisfaire un certain nombre de formalités administratives avant de pouvoir acheter, ce qui diminuera fortement la clientèle (notamment la clientèle étrangère). On peut aussi imaginer que le client alimente un **compte chez son fournisseur** par un mode de paiement extérieur a Internet et qu'il puisse en suite commander en toute tranquillité sans que le commerçant n'ait à obtenir des accords bancaires diverses. Pour information **Swift** est le réseau international sur lequel circule toute les informations inter-bancaires (The Society for Worldwide Interbank Financial Telecommunication) .

Paiement sécurisé indirect (on-line) :



Ce mode de fonctionnement est certainement le plus répandu. Il a l'avantage d'être très simple à mettre en oeuvre. Le commerçant fait simplement appel à une **société de paiement** il n'a plus à gérer aucune transaction financière. Le client n'ayant **pas besoin de s'inscrire** , n'importe qui pourra donc devenir client facilement y compris a travers les frontières . On remarque cependant qu'ici les coordonnées bancaires du client véhicule sur l'Internet. En France on dénombre **quelques centaines de site commerciaux** utilisant ce procédé. Vous pouvez par exemple commander des CD,Video,.. à la FNAC . Il y a aussi un inconvénient : Lorsque q'un client entre ses coordonnées de carte de paiement (Visa, Mastercard, Cirus...) , il n'y a **pas de vérification de code** ce qui veux dire que vous pouvez entrer le numéro de carte de quelqu'un d'autre et cela marchera . Déjà plusieurs plaintes ont été déposées, en effet certains ont pu observer des débits pirates sur le compte. Ceci pose un problème pour la législation : théoriquement lorsqu'une société accepte d'être payée par une carte de paiement sans authentifier le client (en lui faisant saisir son code) elle accepte en cas de réclamation de rembourser sans discuter. C'est par exemple le cas des sociétés auto-routières. En France , le paiement on-line sur Internet a du mal à prendre car **les français ont peur** de se faire pirater leur numéro de carte. En fait c'est une peur injustifiée puisque quand vous payez avec votre carte de paiement, toute ces coordonnées sont inscrites sur votre ticket (une copie allant au commerçant) , il y a donc plus de risques que l'employé qui va enregistrer votre paiement conserve la copie de votre ticket pour piratage plutôt qu'un as

LIAISONS SLIP ET PPP

Objectifs :

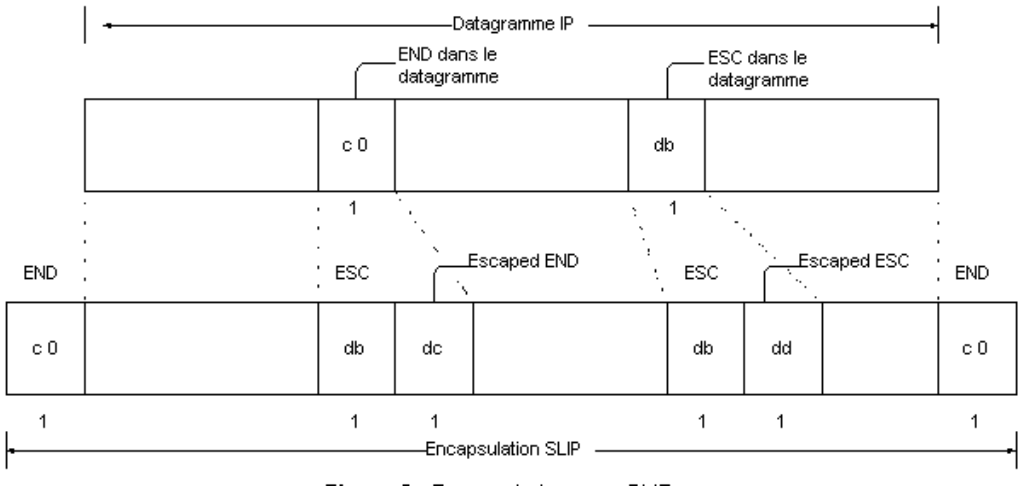
Dans le monde TCP/IP , les liaisons séries sont utilisées pour créer des WAN (Réseaux longue distance). Malheureusement, un protocole standard au niveau de la couche physique pour les lignes séries n'a pas toujours existé concernant cette famille de protocoles TCP/IP. En raison de cette carence, beaucoup de responsables informatiques ont choisi une même marque de routeurs pour leur WAN afin d'assurer la communication au niveau de la couche physique.

La croissance des réseaux longue distance avec TCP/IP a ensuite suscité un vif intérêt pour la standardisation des communications sur liaisons séries afin d'être indépendant de tout fournisseur. De même, l'arrivée de petits systèmes abordables fonctionnant avec TCP/IP ainsi que des modems à haute vitesse ont appuyé cette demande.

Le besoin d'une standardisation pour les communications dans les WAN et celui d'accès TCP/IP par le RTC , ont abouti à la création de deux protocoles de transmission sur ligne série : Serial Line IP (SLIP) et Point-to-Point Protocol (PPP).

SLIP :

SLIP signifie **Serial Line IP** (IP sur liaison série). Il s'agit d'une forme simple d'encapsulation des datagrammes IP sur des liaisons séries, qui est spécifiée dans la RFC 1055 (A Non Standard for Transmission of IP Datagrams Over Serial Lines). SLIP définit une séquence de caractères qui encapsulent des paquets IP sur une ligne série, et rien d'autre. Il ne fournit pas d'adressage, d'identification de paquets, de détection et de correction d'erreurs ou un mécanisme de correction.



Comme le protocole fonctionne de manière simple, il est très facile de le mettre en place. SLIP est devenu populaire grâce à la connexion de systèmes domestiques à Internet , au travers du port série RS232 rencontré sur la plupart des ordinateurs et des modems à grande vitesse.

SLIP puise ses origines au début des années 80 dans l'implémentation de 3COM UNET TCP/IP .

Aux alentours de 1984, Rick Adams mis en œuvre SLIP pour 4.2 Berkeley Unix et les stations de travail Sun Microsystems. Bien qu'ayant été décrit comme non standard, il devint de plus en plus populaire pour finalement être considéré comme la voie la plus simple pour connecter des serveurs TCP/IP et du RTC

Puisque les lignes SLIP sont souvent lentes (19200 bits/sec ou moins), et fréquemment utilisées pour du trafic interactif (comme Telnet et Rlogin, les deux utilisant TCP), elles tendent à être composées de petits paquets TCP échangés à travers une ligne SLIP. La transmission d'un octet de données nécessite un en-tête IP de 20 octets et un en-tête TCP de 20 octets, soit un overhead de 40 octets.

Pour résoudre ce problème de performance, une nouvelle version de SLIP , appelée CSLIP (pour Compressed SLIP), a été spécifiée dans la RFC 1144 (Van Jacobson 1990).

PPP :

Bien plus qu'un standard d'encapsulation de datagramme(comme slip), les liaisons PPP résolvent certains problèmes des protocoles réseaux, tel qu'assigner et gérer des adresses (IP, X.25 et autres..) qui est particulièrement difficile à travers un réseau commuté.

Parallèlement, PPP permet l'encapsulation de trames asynchrone et synchrone orienté bit, de configurer la liaison série, de tester la qualité de la liaison, de multiplexer les différentes couches réseau, détecter les erreurs, et de '' négocier '' les options avec le site distant, tel que la compression de donnée, la vitesse de transfert...

PPP résout tout cela à travers un protocole de contrôle de liaison (LCP) et une famille de protocoles de contrôle de réseaux pour ''négocier'' les paramètres optionnels de la configuration.

PPP est recommandé pour l'utilisation simultanée de plusieurs protocoles de couche réseau. En effet, sa structure permet de multiplexer simultanément différents protocoles de couche réseau.

Choisir :

PPP s'avère un protocole nettement plus puissant que SLIP. Les options de configurations étant nombreuses, sa mise en œuvre est plus délicate ; Il est moins souvent utilisé. Cependant les avantages résultant de l'utilisation de PPP en font le protocole de ligne série de l'avenir et le choix probable des distributeurs de routeurs à la recherche d'un mécanisme standard de transmission sur des lignes série.

PPP constitue le choix approprié comme protocole non-propriétaire pour assurer la connexion des routeurs sur les lignes série. Etant donné que SLIP a été le premier protocole série IP largement répandu, il est par conséquent disponible pour un plus grand nombre de types de matériel que PPP.

L'accès commuté constitue l'une des applications les plus utilisées pour IP sur les lignes série. Le protocole SLIP est plus souvent utilisé à cette fin que le protocole PPP, puisque nombre de système qui proposent l'accès commuté supportent uniquement SLIP. SLIP est disponible pour la plupart des serveurs et dans majorité des mises en œuvre PC de TCP/IP.

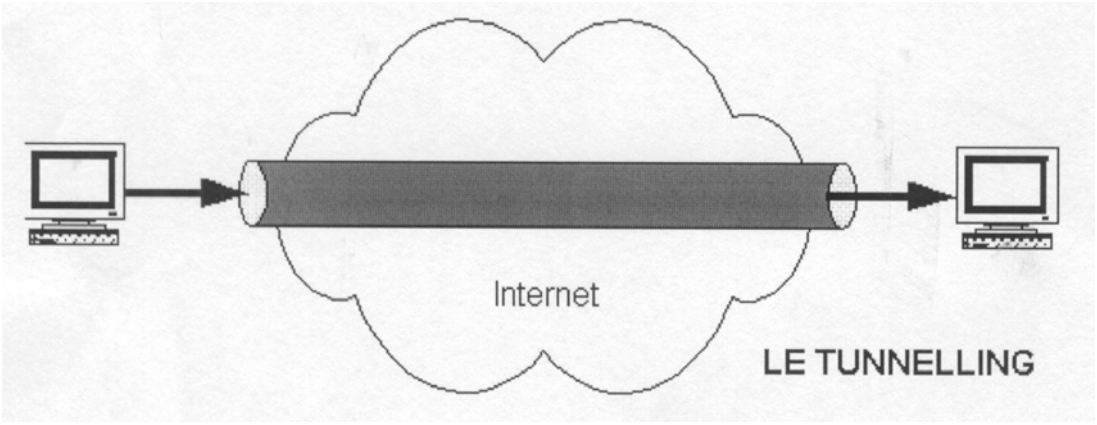
SLIP et PPP ne peuvent échanger des informations, il s'agit de protocole complètement différent. Dés lors, si vos serveurs utilisent uniquement SLIP, les hôtes à distance, interconnectés au travers de ces serveurs doivent aussi utiliser SLIP. Etant donné le nombre de protocoles SLIP, celui-ci sera encore présent de nombreuses années.

VPN

Le Réseau privés virtuel :

Les réseaux privés virtuels (VPN : Virtual Private Network) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Il faut par contre tenir compte de la spécificité d'internet, dans le sens où aucune qualité de service n'est garantie.



Auparavant pour interconnecter deux LANs distants, il n'y avait que deux solutions, soit les deux sites distants étaient reliés par une ligne spécialisée permettant de réaliser un WAN entre les deux sites soient les deux réseaux communiquaient par le RTC.

Une des première application des VPN est de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il utilise la connexion avec son fournisseur d'accès pour se connecter à Internet et grâce aux VPN, il crée un réseau privé virtuel entre l'appelant et le serveur de VPN de l'entreprise.

Cette solution est particulièrement intéressantes pour des commerciaux sillonnant la France : ils peuvent se connecter de façon sécurisée et d'où ils veulent aux ressources de l'entreprise. Cela dit, les VPN peuvent également être utilisé à l'intérieur même de l'entreprise, sur l'intranet, pour l'échange de données confidentielles

Il existe sur le marché trois principaux protocoles :

- PPTP (Point to Point Tunnelling Protocol) de Microsoft
- L2F (Layer Two Forwarding) de Cisco
- L2TP (Layer Two Tunnelling Protocol) de l'IETF

PPTP - Point to Point Tunnelling Protocol - microsoft:

C'est un protocole qui encapsule des trames PPP dans des datagrammes IP afin de les transférer sur un réseau IP. PPTP permet le cryptage des données PPP encapsulées mais aussi leur compression.

Le schéma suivant montre comment un paquet PPTP est assemblé avant d'être transmis par un client distant vers un réseau cible.

L'intérêt de PPTP est de ne nécessiter aucun matériel supplémentaire car les deux logiciels d'extrémité (le client et le serveur) sont intégrés dans NT4 et bien sûr dans 2000

L2F - Layer Two Forwarding - cisco :

L2F est un protocole qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Ce serveur L2F désencapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2PT , L2F n'a pas besoin de client.

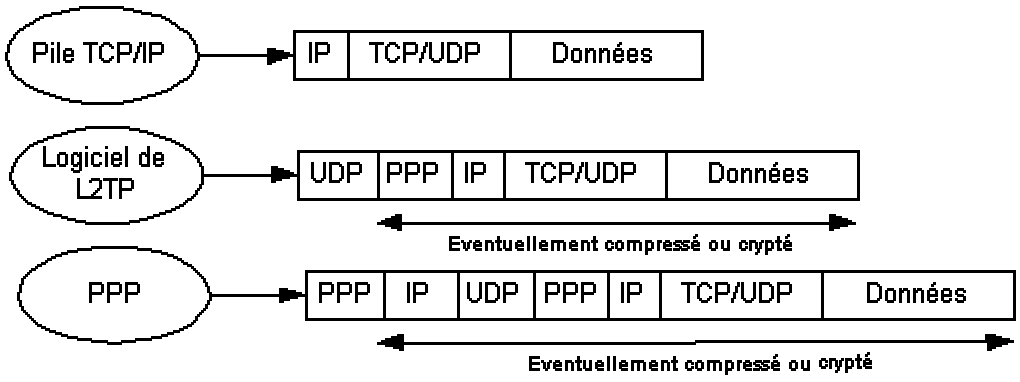
Ce protocole est progressivement remplacé par L2TP qui est plus souple.

L2TP - Layer Two Tunnelling Protocol :

Microsoft et Cisco, reconnaissant les mérites des deux protocoles L2F et PPTP, se sont associés pour créer le protocoles L2TP. Ce protocole réunit les avantages de PPTP et L2F.

L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. Mais L2TP peut aussi être directement mis en œuvre sur des supports WAN (relais de trames) sans utiliser la couche de transport IP.

On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP.



ANNEXE :TYPES DE TRAMES

La trame TCP :

TCP est un protocole sécurisé orienté connexion conçu pour s'implanter dans un ensemble de protocoles multicouches, supportant le fonctionnement de réseaux hétérogènes. TCP fournit un moyen d'établir une communication fiable entre deux tâches exécutées sur deux ordinateurs autonomes raccordés à un réseau de données. Le protocole TCP s'affranchit le plus possible de la fiabilité intrinsèques des couches inférieures de communication sur lesquelles il s'appuie. TCP suppose donc uniquement que les couches de communication qui lui sont inférieures lui procurent un service de transmission de paquet simple, dont la qualité n'est pas garantie.

En principe, TCP doit pouvoir supporter la transmission de données sur une large gamme d'implémentations de réseaux, depuis les liaisons filaires câblées, jusqu'aux réseaux commutés, ou asynchrones.

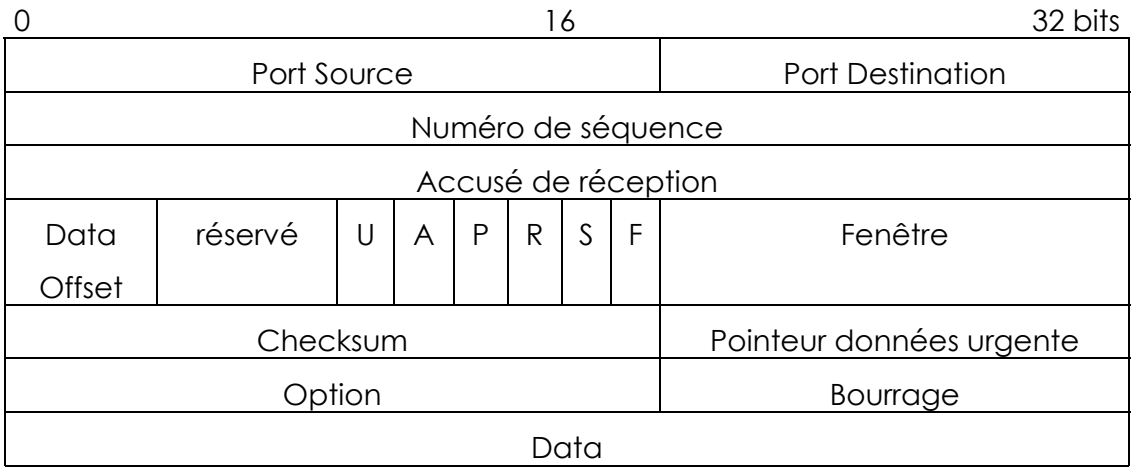
TCP s'intègre dans une architecture multicouche des protocoles, juste au-dessus du protocole Internet IP. Ce dernier permet à TCP l'envoi et la réception de segments de longueur variable, encapsulés dans un paquet Internet appelé aussi "datagramme". Le datagramme Internet dispose des mécanismes permettant l'adressage d'un service TCP source et un destinataire, quelles que soient leur position dans le réseau. Le protocole IP s'occupe aussi de la fragmentation et du réassemblage des paquets TCP lors de la traversée de réseaux de plus faibles caractéristiques. Le protocole IP transporte aussi les informations de priorité, compartimentation et classification en termes de sécurité relatives aux segments TCP. Ces informations se retrouvent alors transmises de bout en bout de la communication.

De grandes parties de ce document sont écrites dans un contexte où les implémentations TCP sont concomitantes à d'autres protocoles de haut niveau dans la même machine. Certains systèmes informatiques seront raccordés au réseau via un frontal qui accueillera les fonctions TCP et IP, ainsi que les protocoles réseau de bas niveau. La spécification TCP décrit une interface à destination des applications de niveau supérieur, y compris dans le cas d'une architecture avec un frontal, pour autant que les protocoles "poste vers frontal" soient implémentés.

TCP prétend fournir un service de communication de processus à processus, dans un environnement réseau complexe. TCP est défini comme un

protocole de communication "host to host", c'est à dire de maître à maître (par opposition à "central à terminal").

En tête TCP



Port source: 16 bits Le numéro de port de la source.

Port Destinataire : 16 bits Le numéro de port du destinataire.

Numéro de séquence : 32 bits Le numéro du premier octet de données par rapport au début de la transmission (sauf si SYN est marqué). Si SYN est marqué, le numéro de séquence est le numéro de séquence initial (ISN) et le premier octet à pour numéro ISN+1.

Accusé de réception : 32 bits Si ACK est marqué ce champ contient le numéro de séquence du prochain octet que le récepteur s'attend à recevoir. Une fois la connexion établie, ce champ est toujours renseigné.

Data Offset : 4 bits La taille de l'en-tête TCP en nombre de mots de 32 bits. Il indique là ou commence les données. L'en-tête TCP, dans tous les cas à une taille correspondant à un nombre entier de mots de 32 bits.

Réservé : 6 bits Réservés pour usage futur. Doivent nécessairement être à 0.

Bits de contrôle : 6 bits (de gauche à droite): URG: Pointeur de données urgentes significatif ACK: Accusé de réception significatif PSH: Fonction Push RST: Réinitialisation de la connexion SYN: Synchronisation des numéros de séquence FIN: Fin de transmission

Fenêtre : 16 bits Le nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.

Checksum : 16 bits Le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de l'en-tête et des données pris deux par deux (mots de 16 bits). Si le message entier contient un nombre impair d'octets, un 0 est ajouté à la fin du message pour terminer le calcul du Checksum. Cet octet supplémentaire n'est pas transmis. Lors du calcul du Checksum, les positions des bits attribués à celui-ci sont marqués à 0. Le Checksum couvre de plus une pseudo en-tête de 96 bits préfixée à l'en-tête TCP. Cette pseudo en-tête comporte les adresses Internet source et destinataires, le type de protocole et la longueur du message TCP. Ceci protège TCP contre les erreurs de routage. Cette information sera véhiculée par IP, et est donnée comme argument par l'interface TCP/Réseau lors des appels d'IP par TCP.

Adresse Source		
Adresse destinataire		
zéro	PTCL	Longueur TCP

0 32 bits

La longueur TCP compte le nombre d'octets de l'en-tête TCP et des données du message, en excluant les 12 octets de la pseudo en-tête.

Pointeur de données urgentes : 16 bits Communique la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence. Le pointeur doit pointer sur l'octet suivant la donnée urgente. Ce champs n'est interprété que lorsque URG est marqué.

Options : variable Les champs d'option peuvent occuper un espace de taille variable à la fin de l'en-tête TCP. Ils formeront toujours un multiple de 8 bits. Toutes les options sont prises en compte par le Checksum. Un paramètre d'option commence toujours sur un nouvel octet. Il est défini deux formats types pour les options: Cas 1: Option mono-octet. Cas 2: Octet de type d'option, octet de longueur d'option, octets de valeurs d'option. La longueur d'option prend en compte l'octet de type, l'octet de longueur lui-même et tous les octets de valeur et est exprimée en octets. Notez que la liste d'option peut être plus courte que ce que l'offset de données pourrait le faire supposer. Un octet de remplissage (padding) devra être dans ce cas rajouté après le code de fin d'options. Cet octet est nécessairement à 0. TCP doit implémenter toutes les options.

Donnée d'option : Taille maximale de segment: 16 bits Si cette option est présente, elle communique à l'émetteur la taille maximale des segments qu'il pourra envoyer. Ce champ doit être envoyé dans la requête de connexion initiale (avec SYN marqué). Si cette option est absente, le segment pourra être pris de n'importe quelle taille.

Bourrage (padding): variable Les octets de bourrage terminent l'en-tête TCP: de sorte que le nombre d'octet de celle-ci soit toujours multiple de 4 (32 bits) de sorte que l'offset de données marqué dans l'en-tête corresponde bien au début des données applicatives.

La trame IP :

La fonction ou rôle du Protocole Internet est d'acheminer les datagrammes à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destination. Les modules Internet sont des programmes exécutés dans des hôtes et des routeurs du réseau Internet. Les datagrammes sont transférés d'un module Internet à l'autre sur un segment particulier de réseau selon l'interprétation d'une adresse Internet. De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet.

Lors de l'acheminement d'un datagramme d'un module Internet vers un autre, les datagrammes peuvent avoir éventuellement à traverser une section de réseau qui admet une taille maximale de paquet inférieure à

celle du datagramme. Pour surmonter ce problème, un mécanisme de fragmentation est géré par le protocole Internet.

Un résumé du contenu de l'en-tête Internet suit :

En tête IP

0		16	32 bits
Ver.	**LET**	**Type de service**	**Longueur totale**
Identification			**Flags** / **Fragment Offset**
Durée de vie		**Protocole**	
Adresse source			
Adresse de destination			
Option + Bourrage			
Data			

Version : 4 bits

Le champ Version renseigne sur le format de l'en-tête Internet. Ce document décrit le format de la version 4 du protocole.

Longueur d'En-Tête : 4 bits

Le champ Longueur d'En-Tête (LET) code la longueur de l'en-tête Internet, l'unité étant le mots de 32 bits, et de ce fait, marque le début des données. Notez que ce champ ne peut prendre une valeur en dessous de 5 pour être valide.

Type de Service : 8 bits

Le Type de Service donne une indication sur la qualité de service souhaitée, qui reste cependant un paramètre "abstrait". Ce paramètre est utilisé pour "guider" le choix des paramètres des services actuels lorsqu'un datagramme transite dans un réseau particulier. Certains réseaux offrent un mécanisme de priorité, traitant préférentiellement un tel trafic par rapport à un trafic moins prioritaire (en général en acceptant seulement de véhiculer des paquets d'un niveau de priorité au dessus d'un certain seuil lors d'une surcharge momentanée). Principalement, le choix offert est une négociation entre les trois contraintes suivantes : faible retard, faible taux d'erreur, et haut débit.

Bits 0-2 : Priorité.

Bit 3 : 0 = Retard standard, 1 = Retard faible.

Bits 4 : 0 = Débit standard, 1 = Haut débit.

Bits 5 : 0 = Taux d'erreur standard 1 = Taux d'erreur faible.

Bit 6-7 : Réservé.

Priorité	D	T	R	0	0

0 8 bits

111 - Network Control

110 - Internetwork Control

101 - CRITIC/ECP

100 - Flash Override

011 - Flash

010 - Immediate

001 - Priority

000 - Routine

L'utilisation des indications en termes de retard, débit, et qualité de transmission peut augmenter le "coût" (d'un certain point de vue) du service. Dans la plupart des réseaux, de meilleures performances pour l'un de ces paramètres s'obtient au prix d'une dégradation des performances pour un autre. A moins d'une situation exceptionnelle, il sera préférable de ne pas activer plus de deux optimisations sur les trois.

Le "Type de Service" sert à préciser le traitement effectué sur le datagramme pendant sa transmission à travers Internet. Des exemples d'association de ce code aux améliorations de service proposées par des réseaux existants comme AUTODIN II, ARPANET, SATNET, et PRNET sont données dans la RFC 795 "Service Mappings" [8].

La priorité dite "Network Control" est stipulée comme étant une priorité à l'intérieur d'un seul réseau. Le fait d'utiliser cette option instaure une priorité pour chaque section traversée. La priorité "Internetwork Control" n'est gérée que par les routeurs. Si l'utilisation de ces priorités ont une signification particulière ou supplémentaire pour l'un des réseaux, il est de la responsabilité de ce dernier de lire et d'interpréter les présentes informations.

Longueur Totale : 16 bits

Le champ "Longueur Totale" est la longueur du datagramme entier y compris en-tête et données, mesurée en octets. Ce champ ne permet de coder qu'une longueur de datagramme d'au plus 65,535 octets. Une telle longueur rendrait de toutes façon les datagrammes impossible à gérer pour la plus grande partie des réseaux. Les hôtes devront au moins pouvoir accepter des datagrammes d'une longueur jusqu'à 576 octets (qu'il s'agisse d'un datagramme unique ou d'un fragment). Il est de même recommandé que des hôtes ne décident d'envoyer des datagrammes de plus de 576 octets que dans la mesure où ils sont sûrs que la destination est capable de les accepter.

Le nombre 576 a été choisi pour permettre à un bloc de données de taille raisonnable d'être transmis dans un datagramme, tenant compte des données à ajouter pour constituer les en-têtes de protocole. Par exemple, cette taille permet la transmission d'un bloc de 512 octets, plus 64 octets d'en-tête dans un datagramme unique. (NdT : je rappelle ici que la taille de 512 octets correspond à un secteur sur la plupart des supports de stockage) La taille maximale d'un en-tête Internet étant de 60 octets, et sa taille typique étant de 20 octets, ce nombre permet de conserver une bonne marge pour les données protocolaires de plus haut niveau.

Identification : 16 bits

Une valeur d'identification assignée par l'émetteur pour identifier les fragments d'un même datagramme.

Flags : 3 bits

Divers commutateurs de contrôle.

Bit 0 : réservé, doit être laissé à zéro

Bit 1: (AF) 0 = Fragmentation possible, 1 = Non fractionnable.

Bit 2: (DF) 0 = Dernier fragment, 1 = Fragment intermédiaire.

0	AF	DF

Fragment Offset : 13 bits

Ce champ indique le décalage du premier octet du fragment par rapport au datagramme complet. Cette position relative est mesurée en blocs de 8 octets (64 bits). Le décalage du premier fragment vaut zéro.

Durée de vie : 8 bits

Ce champ permet de limiter le temps pendant lequel un datagramme reste dans le réseau. Si ce champ prend la valeur zéro, le datagramme doit être détruit. Ce champ est modifié pendant le traitement de l'en-tête Internet. La durée de vie est mesurée en secondes. Chaque module Internet doit retirer au moins une unité de temps à ce champ, même si le traitement complet du datagramme par le module est effectué en moins d'une seconde. De ce fait, cette durée de vie doit être interprétée comme la limite absolue maximale de temps pendant lequel un datagramme peut exister. Ce mécanisme est motivé par la nécessité de détruire les datagrammes qui n'ont pu être acheminés, en limitant la durée de vie même du datagramme.

Protocole : 8 bits

Ce champ indique quel protocole de niveau supérieur est utilisé dans la section données du datagramme Internet. Les différentes valeurs admises pour divers protocoles sont listée dans la RFC "Assigned Numbers" [rfc1060].

Checksum d'en-tête : 16 bits

Un Checksum calculé sur l'en-tête uniquement. Comme certains champs de l'en-tête sont modifiés (ex., durée de vie) pendant leur transit à travers le réseau, ce Checksum doit être recalculé et vérifié en chaque point du réseau où l'en-tête est réinterprétée.

L'algorithme utilisé pour le Checksum est le suivant :

On calcule le complément à un sur 16 bits de la somme des compléments à un de tous les octets de l'en-tête pris par paires (mots de 16 bits). Lorsque l'on calcule le Checksum, on considère une en-tête dont le champ réservé pour ce même Checksum vaut zéro.

L'algorithme de Checksum peut paraître élémentaire mais l'expérimentation a montré que cette technique était suffisante. Il se peut que cet algorithme soit plus tard remplacé par un calcul de type CRC, suivant la nécessité future.

Adresse source : 32 bits

L'adresse Internet de la source.

Adresse destination : 32 bits

L'adresse Internet du destinataire.

Options : variable

Les datagrammes peuvent contenir des options. Celles-ci doivent être implémentées par tous les modules IP (hôtes et routeurs). Le caractère "optionnel" concerne leur transmission, et non leur implémentation.

Dans certains environnements, l'option de sécurité peut être obligatoire dans tous les datagrammes.

Le champ d'option est de longueur variable. Un datagramme peut comporter zéro ou plus options. Voici les deux formats possibles d'option :

Cas 1: Une option codée sur un seul octet.

Cas 2: Un octet codant le type d'option, un octet donnant la taille de l'option, les octets de données d'option.

La taille de l'option compte tous les octets de l'option y compris le type, son propre octet et tous les octets de donnée d'option.

L'octet de type d'option est composé de trois champs de bits :

1 bit	indicateur de recopie
2 bits	classe d'option
5 bits	numéro d'option.

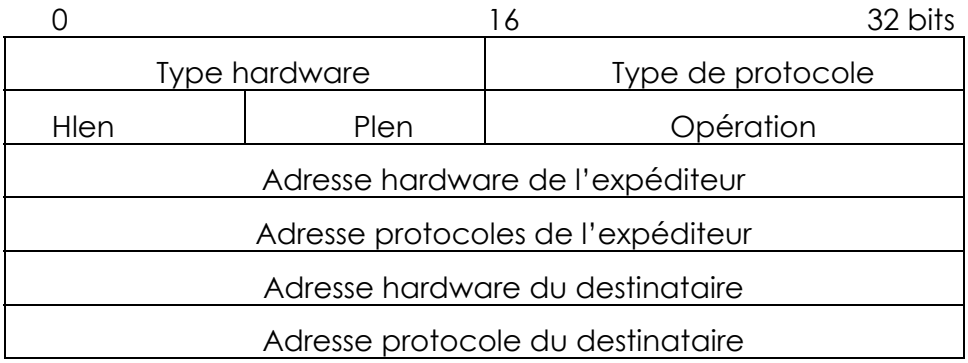
La trame ARP

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines. Pour envoyer un datagramme dans l'internet, le logiciel réseau doit convertir l'adresse IP en une adresse physique qui est utilisée pour transmettre la trame. Si l'adresse physique est un entier court, elle peut être facilement modifiée pour lui faire correspondre l'adresse machine IP. Sinon, la traduction doit être effectuée dynamiquement.

C'est le protocole ARP qui effectue cette traduction en s'appuyant sur le réseau physique. ARP permet aux machines de résoudre les adresses sans utiliser de table statique. Une machine utilise ARP pour déterminer l'adresse physique destinataire en diffusant (broadcast), sur le sous réseau, une requête ARP qui contient l'adresse IP à traduire. La machine possédant

l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode broadcast.

La structure d'une trame ARP est définie ci-dessous :



Type Hardware : spécifie le type de l'interface hardware

Type de protocole : spécifie le type du protocole de haut niveau émis par l'expéditeur

Hlen : longueur de l'adresse hardware

Plen : longueur de l'adresse de haut niveau

Opération : type de l'opération effectuée :

1 Requête ARP

2 Réponse ARP

3 Requête RARP

4 Réponse RARP

5 Requête RARP dynamique

6 Réponse RARP dynamique

7 Erreur RARP dynamique

8 Requête InARP

9 Réponse InARP

Adresse hardware de l'expéditeur : explicite

Adresse protocole de l'expéditeur : explicite

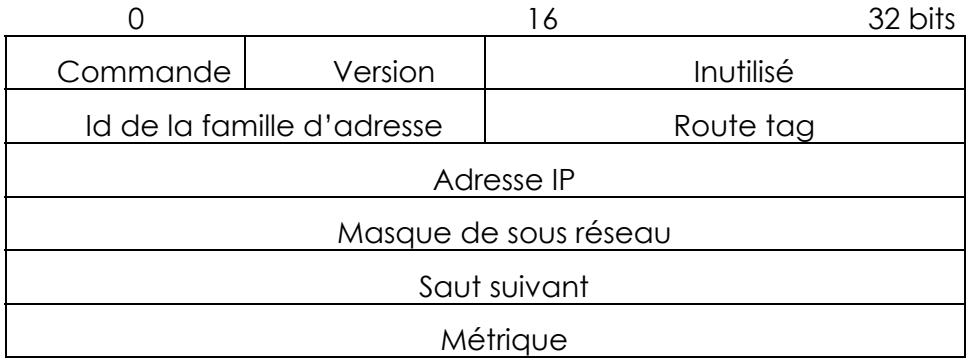
Adresse hardware du destinataire : explicite

Adresse protocole du destinataire : explicite

La trame RIP2

RIP2 est utilisé pour échanger des informations de routage. Il dérive d'un premier protocole développé par Xerox (RIP). Chaque machine qui utilise un protocole RIP2 a un processus qui envoie et reçoit des datagrammes transportés par de l'UDP port numéro 520.

La structure des trames RIP2 est décrite ci-dessous :



Commande : utilisé pour définir le sujet du datagramme

1 Requête

2 Réponse

3 Réservé (Utilisé par Sun microsystems)

Version : numéro de la version RIP.

Identifiant de la famille d'adresses : indique quel type d'adresse est utilisé cela car RIP2 peut transporter d'autres informations de routage.

Route tag : (utilisé par RIP2 ; 0 pour RIP) attribue une route qui doit être préservée par une route. Ce champ permet de séparer les routes RIP internes des routes externes qui ont pu être importée d'un EGP ou d'un autre IGP.

Adresse IP : adresse IP de la destination.

Masque de sous-réseau : (utilisé par RIP2; 0 pour RIP) masque du sous réseau destination.

Saut suivant : adresse IP à laquelle les paquets devront être envoyé au prochain saut.

Métrique : représente le coût total de la source à la destination (en nombre de sauts).

La trame X25

La structure du paquet de données X25 est la suivante:

8	7	6	5	4	3	2	1
Q	D	0	1	Numéro de groupe de voie logique			
Numéro de voie logique							
P (R)			M	P (S)			O
Données							

GFI: Identifiant de format général. Q indique un paquet X25 (0) ou X29 (1). D indique un acquittement local (0 : ETCD) ou distant (1 : ETTD). Les bits 01 indiquent que les numéros de trames vont de 0 à 7. Le format de trame où ils indiquent 10 montre que l'on numérote les trames de 0 à 127 (10). Cela permet d'envoyer beaucoup de trame avant d'acquitter ce qui est intéressant pour les réseaux lents tels que les réseaux satellites.

P(R) : Nombre des paquets reçus.

P(S) : Nombre de paquets envoyés.

M : Seulement dans les paquets de données. Ce champ indique, lorsqu'il est à 1, que le paquet fait partie d'un ensemble de paquets à traiter comme un tout.

Les paquets peuvent être de différents types:

CALL ACC : Appel accepté.

CALL REQ : Demande d'appel.

CLR CNF : Confirmation d'effacement.

CLR REQ : Demande d'effacement.

DATA : Paquet de données

DIAG : Diagnostique.

INF CNF : Confirmation d'interruption.

INT REQ : Demande d'interruption.

REJ : Rejet.

RES CNF : Confirmation de remise à zéro.

RES REQ : Demande de remise à zéro.

RNR : Non prêt à recevoir.

RR : Prêt à recevoir.

RSTR CNF : Confirmation pour recommencer.

RSTR REQ : Demande qu'on recommence.

REG REQ : Demande de registration.

REG CNF : Confirmation de registration.

PETIT LEXIQUE

le vocabulaire du monde des réseaux

Bien sur des lexiques existent en ligne, vous pouvez essayer par exemple

http://www.culture.fr/culture/dglf/ressources/lexiques/abc.htm

et celui-ci (plus technique et en anglais)

http://www.matisse.net/files/glossary.html

ou encore

http://www.csrstds.com/acro-a-d.html

Mais en voici également un "papier"

Adresse :----------	Référence sur le WEB sous forme www.NomEntreprise.NomDomaine
Adresse Electronique: ----------	Voir Mail
ADSL :----------	Asymetrical Digital Subscriber Line nouvelle technologie de transmission permettant des transferts de l'ordre de 1Mbps par la ligne téléphonique classique
Alias : ----------	Autre nom plus facile à utiliser ou permettant de cacher le nom réel. Possible pour une adresse de courrier électronique, par exemple michel.cabare alias cabare (évite au correspondant de connaître nom et prenom...)
ANSI : ----------	American National Standard Institute Organisme de normalisation
Archie : ----------	nom du service internet permettant de localiser des fichier téléchargeable par une liaison ftp anonyme. tends à disparaître
Arpanet :----------	Réseau développé en 1960-1970 "ancêtre" d'Internet
Ascii : ----------	American Standard Code for Information Interchange. Code pour la représentation des caractères de A à Z, de a à z, les chiffres, les signes de ponctuation et les caractères accentués.

Attaché :---------- Fichier inclus dans un message au niveau du mail, cela peut être un type quelconque de fichier

ATM :---------- Asynchronous Transfer Mode Technique de transfert pour les réseaux hauts débits utilisant la commutation de paquet

AUI : ---------- Attachment Unit interface Connecteur dans la terminologie Ethernet

Avis : ---------- "Normalisation" édictée par le CCITT (maintenant l'ITU)

Balise :---------- cf. Tag

Backbone :---------- Ligne à haute vitesse ou ensemble de lignes à haute vitesse constituant un point de passage important du réseau.

Bande de Base :---------- Système employé pour transmettre su un câble des signaux. utilise une seule fréquence (par opposition à Bande Large)

Bande Passante : ---------- Quantité d'information pouvant circuler pendant une durée définie entre deux ordinateurs, mesurée en bps (bits par seconde), kbps (kilobits par seconde) ou mbps (megabits par seconde)

Baud : ---------- Unité de mesure de la vitesse d'un Modem, valant environ 1 bps

BBS :---------- Bulletin Board System. Serveurs qui permettent des échanges d'informations et de fîchiers, essentiellement via réseau RTC / Modem . tendent à disparaître au profit de sites web ou ftp

Bit : ---------- Binary digIT. Quantité élémentaire d'information de valeur 0 ou 1

Blindage :---------- Enveloppe en métal tressée entourant certain type de câble pour absorber les signaux parasitaires

BNC : ---------- British Naval Connector Connecteur particulier dans la terminologie Ethernet

Bookmark : ---------- Voir Signet

Bouchon :---------- Dans une topologie en Bus c'est un connecteur spécial qui se met à chaque extrémité du câble pour éviter les "rebonds".

Browser :---------- Voir Navigateurs

BUS :---------- Se dit d'un réseau dans lequel tous les ordinateurs sont reliés sur le même câble

Butineurs :---------- Voir Navigateurs

CCITT :---------- Comité Consultatif International pour le Télégraphe et le Téléphone. Remplacé

maintenant par 1'ITU. Organisation Internationale qui établit des normes (recommandations ou avis) de télécommunications

CGI : ---------- Common Gateway interface
Langage de programmation pour automatiser sur les serveurs WEB certains traitement sur les pages HTML (comme les formulaires)

Circuit Virtuel :---------- Type de protocole dans lequel tous les paquets suivent la même route, une fois qu'elle à été établie (A opposer à Datagramme)

Client : ---------- Dans un échange sur réseau c'est l'ordinateur effectuant des demandes sur un autre ordinateur

Cookies : ---------- Morceau de logiciel envoyé depuis un site Web sur le poste dur navigateur pour mémoriser certaines informations

Concentrateur : ---------- Voir Hub

CRC : ---------- Code de Redondance Cyclique utilisé pour la détection d'erreurs lors de l'échange de trames

CSMA/CA : ---------- Carrier Sense Multiple Access with Collision Avoidance
Méthode d'accès aléatoire avec prévention des collisions (utilisé dans la couche Liaison)

CSMA/CD : ---------- Carrier Sense Multiple Access with Collision Detection
Méthode d'accès aléatoire avec détection de collisions (utilisé dans la couche Liaison)

Datagramme (IP): ---------- Groupe d'octets (de l'ordre de quelques centaines) qui circule sur le réseau Internet, provenant d'une station et à destination d'une autre station. Type de protocole dans lequel tous les paquets constituant les données ne suivent pas obligatoirement la même route (à opposer à circuit virtuel)

DEFAULT Route : ---------- Route par défaut. Dans une table de routage IP, entrée qui indique la route que doivent suivre les datagrammes pour lesquels il n'y a pas d'autre route explicite dans la table.

DIAL-UP :---------- Nom donné à une connexion sur Internet via une ligne téléphonique et un Modem

DNS : ---------- Domain Name Server
Serveur qui à partir du nom d'une machine sous la forme nom.domaine.organisation sait

indiquer son adresse IP.(C'est un Système d'annuaire distribué)

Domaine : ---------- Un domaine indique un réseau connécté sur Internet, ou un regroupement de plusieurs adresse Internet au sein d'un unité d'Administration logique

Domaine Public :---------- Qualificatif des logiciels que l'on peut librement utiliser gratuitement.

Email : ---------- Voir Mail

Ethernet :---------- Définition d'un type de réseau (couches basses donc cartes, câbles et connecteurs) très utilisé. Différentes variantes existent permettant des débits de 10 Mbits/s à 100 Mbits/s sur différents supports. Très similaire à IEEE 802.3.

FAQ :---------- Frequently Asked Questions
Document texte contenant généralement un jeux de questions-réponses les plus souvent posées sur un thème donné

Firewall : ---------- Méthode utilisée pour restreindre l'accès à un réseau par l'extérieur. En général un ordinateur que l'on met entre un réseau local et un autre réseau (tel Internet), et qui fait office de filtre pour assurer la sécurité des informations à l'intérieur du réseau local.

Forum :---------- cf News

Fournisseur d'accès :---------- Nom donné à l'entreprise auprès de laquelle on souscrit un abonnement pour pouvoir se connecter sur internet

Forward : ---------- Action consistant à faire passer un courrier électronique à un autre utilisateur

Frames :---------- Nom donné au faite qu'une nouvelle fenêtre peut être ouverte automatiquement à l'écran, indépendamment de la fenêtre principale de navigateur

FreeWare :---------- Nom Donné au logiciels dont l'utilisation est gratuite et libre

Frame relay :---------- Relais de trame
Technique de commutation utilisée dans les réseaux longue distance.

Freeware : ---------- Voir Domaine Public

FTP : ---------- File Transfer Protocol
Protocole de transfert et d'échange de fichiers entre sites informatiques sur Internet

FTP Anonyme : ---------- Service FTP sur lequel l'utilisateur peut se connecter sans posséder un compte utilisateur, avec le nom "anonymous" et en

utilisant son adresse courrier (E-Mail) comme mot de passe.

GIF : ---------- Format de fichier graphique utilisable sur le WEB

Graticiel :---------- cf Freeware

Groupe de Discussion : ---------- cf News

HDSL :---------- High Digital Rate Subscriber Line
nouvelle technologie de transmission permettant des transferts de l'ordre de 1.5Mbps par la ligne téléphonique classique

Helper Application :---------- Programme permettant de lire un fichier donné, (souvent multimédia)

Home Page : ---------- Soit la page Web en cours d'édition soit la page d'accueil sur un site

Host :---------- Ordinateur depuis lequel on se connecte

Hostname : ---------- Nom de Serveur déclaré sur le WEB

HTML : ---------- Hyper Text Mark-up Language
type de langage permettant de constituer des pages affichables sur le Web et lisibles via des navigateurs

HTTP :---------- Hyper Text Transfer Protocol
Méthode de transfert d'information entre deux ordinateurs pour des données de type Hyper Texte

Hub : ---------- Dispositif permettant de relier entre eux différents ordinateurs, notamment pour construire des réseaux en étoile

Hypertexte : ---------- se dit d'un système d'écran dans lequel un certain nombre de mots, d'images sont le point d'accès à d'autres pages d'écran, et ce généralement via un simple clic de souris

IEEE : ---------- Institute of Electrical and Electronics Engineers
Organisme de normalisation internationale qui a normalisé en particulier les couches basses des réseaux locaux: normes IEEE 802

IETF :---------- Internet Engineering Task Force.
Ensemble de groupes de travail qui, en particulier, définissent les évolutions techniques (nouveaux standards) de l'Internet

Internet :---------- Interconnection Network
L'ensemble des réseaux d'ordinateur communiquant entre eux et créant le WWW (milliers de réseaux et millions d'ordinateurs)

Intranet :---------- Idem que Internet mais réservé à une catégorie d'utilisateur, par exemple les employés d'une même entreprise

IP (adresse): ---------- Adresse Electronique composée de 4 chiffre allant de 0 à 255 utilisée par les réseaux utilisant le protocole TCP/IP par exemple pour le CUEFA 195.220.28.61, 195.220.28.62 ... etc

IPX/NETX : ---------- Protocole propriétaire Novell sur les réseaux locaux (tends à disparaître au profit de TCP/IP)

ISDN : ---------- Integrated Services Digital Network. Appellation internationale de RNIS

ITU : ---------- International Telecommunications Union. Nouvel organisme qui remplace le CCITT.

JAVAscript : ---------- Langage de programmation inclus en HTML

LAN : ---------- Local Area Network
Réseau local à l'échelle d'une enreprise

Link :---------- Pointeur sur une adresse de document HTML, local ou non

Liste de diffusion : ---------- Système permettant de transmettre les messages de l'abonné au courrier électronique à l'ensemble des abonnés d'un liste de diffusion

Login : ---------- Nom demandé parfois lors d'une connexion pour identifier l'utilisateur

LSA :---------- Liasion Spécialisé Analogique fournie par France telecom…

MAC (adresse): ---------- Par référence à la sous couche de la couche Liaison définissant les protocoles d'échange N° en Héxadécimal unique permettant de repérer une carte réseau

Mail :---------- Courrier Electronique dont les adresses des boîtes au lettre ont la forme nom@entreprise.domaine

Mail List :---------- Voir Liste de diffusion

Map : ---------- Zone composée d'une image et faisant référence selon ses parties pointées à différents liens. Par exemple un plan d'un musée chaque pièce étant cliquable et amenant sur une page précise la décrivant

Masque de sous réseau :---------- masque permettant de savoir si une adresse IP fait partie du même réseaux local ou non pour savoir si on doit aller sur le routeur par défaut ou non

MIME : ---------- Multi Purpose Internet Extension format d'@mail permettant d'envoyer du son et autre formats de document

Modem : ---------- Modulateur / Demodulateur
Appareil permettant de faire dialoguer deux

ordinateurs entre eux via le réseau téléphonique standard

NAT : ---------- Network Adress Translation
mécanisme opéré par un routeur lors d'une demande d'accès à internet par un poste ayant une adresse TCP/IP interne : celle-ci est changée "à la volée"

Navigateurs : ---------- Logiciel permettant le déplacement et la lecture des pages Web notamment grâce aux liens hypertexte. Se décline en général sous le même aspect pour différents systèmes d'exploitation (MAC, WINDOWS, UNIX...)

Netbeui : ---------- protocole propriétaire microsoft pour les petits réseaux en poste à poste essentiellement (tends à disparaître au profit de TCP/IP)

Netiquette : ---------- C'est le nom donné aux règles de "savoir vivre" pour les utilisateurs du WEB

News : ---------- Ensemble de messages sur le réseaux à une adresse particulière traitant d'un même sujet, pouvant être public ou privé (restreint à certains utilisateurs)

NewsGroup :---------- cf News

NIC :---------- Network Information Center
Organisme international gérant l'attribution des adresses IP. En France délègue a l'INRIA.

Numeris : ---------- Appellation commerciale par France télécom d'une liaison téléphonique numérique nécessitant un abonnement et des appareils spécifiques permettant un débit de 64000 bit/s à 128000 bit/s

ON-Line : ---------- Se dit lorsque l'on est connecté

OFF-Line :---------- Se dit lorsque l'on n'est pas connecté

Page HTML :---------- Nom donné à une quantité de code HTML qui sera chargée en une fois par le navigateur et constituera une unité d'affichage. Rien de commun avec des formats papiers classiques

Partagiciel : ---------- cf Shareware

Passerelle :----------

PAT :---------- Port Address Translation
technique permettant d'utiliser à plusieurs postes une seule adresse IP fournie par un Fournisseur d'accès à Internet

PGP :---------- Pretty Good Privacy.
Logiciel d'encodage de données pour E-

Mail, afin d'assurer la confidentialité des messages

Plug-in : ---------- Nom donné à des logiciels étendant la capacité des navigateurs (cf helpers)

Pointeur : ---------- nom donné parfois à une référence URL

POP Server : ---------- Post Office Server
Serveur utilisé pour le courrier électronique

POP 3 : ---------- version plus récente de POP Server

Port (numéro de) : ---------- Numéro attribué à chaque application standard utilisé sur Intemet et basé sur TCP/IP. Exemple : Telnet a pour numéro de port 23, http à 80.

Protocole :---------- Règles de dialogue entre 2 couches de même niveau dans 2 systèmes communicants.

Protocole deRoutage : ---------- Protocole entre les routeurs (et/ou les stations) pour mettre à jour dynamiquement leur table de routage.

Provider : ---------- cf fournisseur d'accès

Proxy Server : ---------- Serveur permettant de se connecter vers l'extérieur depuis un site protéger par un Firewall et servant de cache accélérateur

Queue :---------- File d'attente

RFC : ---------- Request For Comments
Succession d'articles classés au sujet d'Internet et des réseaux et qui définissent généralement un standard de communication ou une application. Ce sont les RFC qui explicitent la norme Internet

RLE : ---------- Réseau Local d'Entreprise Voir LAN

RNIS :---------- Réseau Numérique Intégration Service
Voir Numeris

RTC : ---------- Réseau Téléphonique Commuté correspondant à la liaison téléphonique classique

RTF : ---------- Rich Text Format
Format de fichier texte amélioré reconnus par beaucoup de logiciels et permettant des conversions

Routage : ---------- Processus qui, dans les routeurs en particulier, permet de déterminer ou envoyer des paquets ou datagrammes.

Routeur :---------- Equipement réseau qui interconnecte différentes liaisons et retransmet les datagrammes vers la bonne destination.

SDSL : ---------- Single Line Digital Subscriber Line
nouvelle technologie de transmission

permettant des transferts de l'ordre de 1.5Mbps par la ligne téléphonique classique

Segment : Sur un réseau longueur de câble comprise entre deux dispositifs

Serveur : machine mettant à disposition d'autres machines des données, des services…

Serveur de Nom : Logiciel serveur qui fait partie du DNS et qui répond à des requêtes, par exemple, l'adresse IP d'une station en fournissant le nom domainisé de cette station

Shareware : Nom Donné au logiciels dont l'utilisation est soumise au paiement d'une licence, souvent minime

Signet : Façon de repérer une page WEB par son URL de façon à pouvoir y revenir très facilement

Site : Nom donné à un réseau particulier reconnu

Site Miroir : Site WEB copiant régulièrement une partie ou la totalité d'un autre site plus connu (avec son accord), permettant ainsi des accès moins engorgés que ceux du site copié

Smiley : Convention de signes textes permettant d'envoyer rapidement des annotations par le mail, réservé aux initiés
Ex : ":-)" signifie "je plaisante"

SMTP Server : Simple Mail Transfer Protocol
Serveur permettant d'envoyer du courrier électronique

SNMP : Simple Network Management Protocol
Protocole de gestion des réseaux IP sur les composant permettant "d'interroger" les carrefours utilisés et même de les administrer dynamiquement .

Station : Equipement informatique (micro-ordinateur, station de travail, ...) connecté à un réseau.

SUA : Single User Accountdit aussi PAT
autre appellation de Port Address Translation

Table de Routage : Table utilisée par les routeurs et les stations pour décider vers quelle direction envoyer les datagrammes, suivant l'adresse IP de la station destinataire.

TCP/IP : Transmission Control Protocol / Internet Protocol.
Protocole de communication utilisés dans les réseaux et en particulier dans Internet.

Translation d'adresse : Voir NAT

STP : Shielded Twisted Pair
Paires torsadées blindées

Switch : ---------- ou "Hub intelligent", concentrateur améliorer pour diminuer l'encombrement sur le réseaux et accélérer les transmissions de données

Tag :---------- Nom de commandes utilisées dans le langage HTML et notées entre <..>

Telnet : ---------- Protocole et application utilisés sur les réseaux IP pour se connecter à distance à une station en mode terminal

Terminateur :---------- Voir Bouchon

Thicknet :---------- Câble coaxial Ethernet standard norme RG11 (épais).

Thinnet : ---------- Câble coaxial Ethernet fin

TNR :---------- Terminaison Numérique de Service Boîtier installé par France Télecom pour pouvoir via le RTC accéder a des liaisons numériques à 64 ou 128 Kilobit/s dans une liaison Numeris.

Transfix :---------- Service France Télécom de liaisons spécialisées numériques.

Transpac :---------- Service français de réseau à commutation de paquets.

Trame :---------- élément de protocole du niveau liaison

URL :---------- Uniform Locator Ressource
C'est une référence vers laquelle une liaison de type hypertexte pointe, en général une page HTML Sur le WEB chaque page HTML se trouve à une adresse unique :

UserID :---------- N° d'identité sur un serveur (cf login)

UTP :---------- Unshielded Twisted Pair
Paires torsadées non blindées

VDSL :---------- Very High Data Rate Subscriber Line
nouvelle technologie de transmission permettant des transferts de l'ordre de 13 à 52 Mbps par la ligne téléphonique classique

WEB :---------- Abréviation de WWW

WWW : ---------- cf.World Wide Web

World Wide Web :---------- Littéralement toile d'araignée mondiale, constituée par l'ensemble des ordinateurs interconnectés entre eux et constituant le réseau Internet, et visualisable via une interface unifiée de type graphique, quel que soit le type d'ordinateur utilisé (PC, MAC, Terminal X...)

WYSIWYG : What You See Is What You Get
S'applique à tout éditeur visualisant en direct les effets de style demandés

SOURCES - BIBLIOGRAPHIE

Internet :

le guide Ungi : **http://www.ungi.com**

Réseaux : **http://www.guill.net**
(info et explications très pédagogiques sur des sujets… délicats)

Ethernet : **http://wwwhost.ots.utexas.edu/ethernet**
(normes)

Ethernet : **http://www.lantronix.com/technology/tutorials**
(cours sur switches, divers)

Numeris : **http://www.francetelecom.com/vfrance/boutique/**
(site France telecom)

Reseau : **http://www.nexen.net/networking/**

Bibliographie :

Les Réseaux — par Guy Pujolle
Eyrolles

Divers :

Revue PC EXPERT — Groupe Ziff DAVIS

Certains point ont été inspirés par les cours de
André Plisson — Ingénieur responsable filière au CUEFA grenoble 1996-1996