Les Réseaux Informatiques

Introduction

Ce support de cours est plus qu'un simple support et pas tout à fait un livre sur les réseaux. Il est bien évident que pour chaque chapitre abordé, résumé en 2 à 3 pages, il existe des livres complets. L'important est de dégager une philosophie claire du réseau (si, si, ce n'est pas si ténébreux) et surtout de ne pas se noyer dans les détails.
Il manque certains développements comme Xwindow.
Ce support est une deuxième version appelée à évoluer.
La relecture ayant été rapide, des fautes de français ainsi que des erreurs sur les protocoles peuvent traîner ici et là. Merci de me les signaler (lalot@univ-aix.fr).

Les choix : Parler des protocoles TCP/IP et non des protocoles OSI qui ne sont que très peu utilisés, n'en déplaise aux puristes. Parler aussi de Netbios dans l'environnement IP.
Il y aurait tellement de choses à dire qu'il y a une sélection arbitraire. On ne parle pas de AppleTalk par exemple.
De temps en temps des mots anglais apparaissent. J'ai préféré ne pas traduire des termes qui sont l'espéranto des ingénieurs réseau. Il faut savoir que tous les protocoles INTERNET sont documentés en anglais et que c'est la langue d'échange dans les réseaux. Autant s'y faire. Cela ne nous empêche pas de s'exprimer en Français, comme dans ce livre.
On peut accéder aux informations concernant les protocoles Internet par le lien **http ://www.ietf.org**

Références

Titre	Auteurs	Editeur
Télématique	MACCHI-GUILBERT	Dunod
Switched Fast ETHERNET	Robert Breyer	Ziff Davis
TCP/IP Illustré ***	R.Stevens	Addison Wesley
TCP/IP Protocoles **	D. Comer	Inter Edition
TCP/IP and Unix	Carl Mitchell J.Quaterman	Addison Wesley
Windows NT Server 4.0	Mark Minasi	Sybex
Les Réseaux	Guy Pujolle	Eyrolles
Les RFC	Http ://www.ietf.org	
Le système Linux	Linus Torvald le système Alan Cox pour TCP/IP Beaucoup d'autres..	l'INTERNET

Le système Linux est un système Unix développé par des bénévoles. Ce système est très stable et performant. Ses sources sont disponibles, notamment les sources TCP/IP d'Alan Cox.

Auteur: Dominique LALOT
Ingénieur réseau de l'Université de la Méditerranée.
Faculté des Sciences Economiques Aix en Provence.
Commentaires , suggestions, fautes d'orthographe..
Email : **lalot@univ-aix.fr**

Ce document peut être récupéré grâce à l'URL : http://ciscam.univ-aix.fr/doctech/reseaux.pdf

TABLE DES MATIERES

Introduction 2
HISTORIQUE 4
Le Modèle OSI. de l'ISO 7
La Couche Physique 8
  Les modems 12
  La Détection et la Correction d'Erreur 13
LES RESEAUX LOCAUX 15
  Les types de réseaux locaux 15
  ETHERNET 16
  TOKEN RING 20
  FDDI 22
  VLANS 23
TELEPHONIE NUMERIQUE 24
PROTOCOLES DE LIAISONS POINT A POINT 26
  SDLC et HDLC 26
  SLIP ET PPP 27
PROTOCOLES DE RESEAU 28
  X25 28
  FRAME RELAY 30
  ATM 31
LES TECHNOLOGIES IP 34
  Historique 34
  L'ADRESSAGE IP 35
  BROADCASTING et MULTICASTING 38
  ARP ou Address Resolution Protocol Résolution d'adresses 40
  Le DATAGRAMME IP Réseau 42
Le Routage des Datagrammes IP 44
  Les Routages Dynamiques 46
  Les protocoles de passerelles extérieures (EGP,BGP) 48
  Les Messages ICMP 49
LE TRANSPORT IP 51
  UDP ou User Datagram Protocol 51
  TCP (TRANSPORT CONTROL PROTOCOL) 54
APPLICATIONS 57
  LES SERVEURS DE NOM 57
  SNMP RFC1155/1157 61
  BOOTP / DHCP 65
  TFTP 67
  FTP 68
  SMTP 70
  TELNET et RLOGIN 73
  NFS et les RPC 74
  Les NEWS et LISTSERV 75
  WEB (World Wide Web) 77
LA PROGRAMMATION DES SOCKETS 78
ANALYSE DE PROBLEMES 81
LES RESEAUX LOCAUX DE PC 85
LA SECURITE 89
GERER LA PENURIE D'ADRESSE 93
NAT TRANSLATION D'ADRESSE 93
REFERENCES HTML 99

HISTORIQUE

Quelques dates des évolutions techniques.

Le langage parlé	?	-4 Millions ?
L'écriture	Assyriens	-3500
Les pigeons voyageurs	?	?
Les signaux de fumées	Les amérindiens	?
Les dialectes sifflés	?	?
Les postes	?	< 0
Télégraphe à bras mobiles	Chappe	1792
Télégraphe	Code de Morse	1843
Téléphone	Bell et Gray	1875
Radio	Marconi	1895
Transistor	Bell Labs	1948
Ordinateur ENIAC		1946
ETHERNET	Xerox Intel Dec	1976
Apple2	S.Jobs et Wozniack	1979 ?
IBM PC	IBM	1981 ?

La communication entre ordinateurs ne peut pas être distinguée de celle des hommes. Si au départ, l'ordinateur n'est qu'un gros jouet aux mains de scientifiques, celui-ci a créé une véritable révolution technologique qui devient le support de base de la communication entre les humains. L'informatique est entrée partout, dans le téléphone, dans les disques compacts, la voiture, l'avion. Partout l'ordinateur a remplacé la machine à écrire.

L'évolution des capacités de communication des ordinateurs
L'ordinateur au début n'a que des capacités de calcul. Communiquer avec lui est l'affaire de spécialistes très pointus. Puis, petit à petit, la technique s'améliore. On utilise des bandes perforées puis des cartes perforées. Les sorties sont faites sur des imprimantes.

Les Télétypes sont utilisés pour communiquer avec l'ordinateur. Ce sont des terminaux qui font de la saisie sur un clavier et de l'affichage sur du papier.

Les terminaux vidéo se généralisent ensuite. L'affichage se fait sur écran. Ces écrans deviennent de plus en plus sophistiqués , avec de la couleur, du graphisme. Un terminal est assez « bête », il ne fait que de la saisie et de l'affichage, il envoie les caractères tapés au clavier et reçoit des ordres d'affichage.

Le prix des processeurs diminuant, la technologie devenant à la portée de plus petites équipes, le micro-ordinateur arrive à la fin des années 70 (**INTEL**). Depuis la façon de concevoir les réseaux et les applications a considérablement changé.

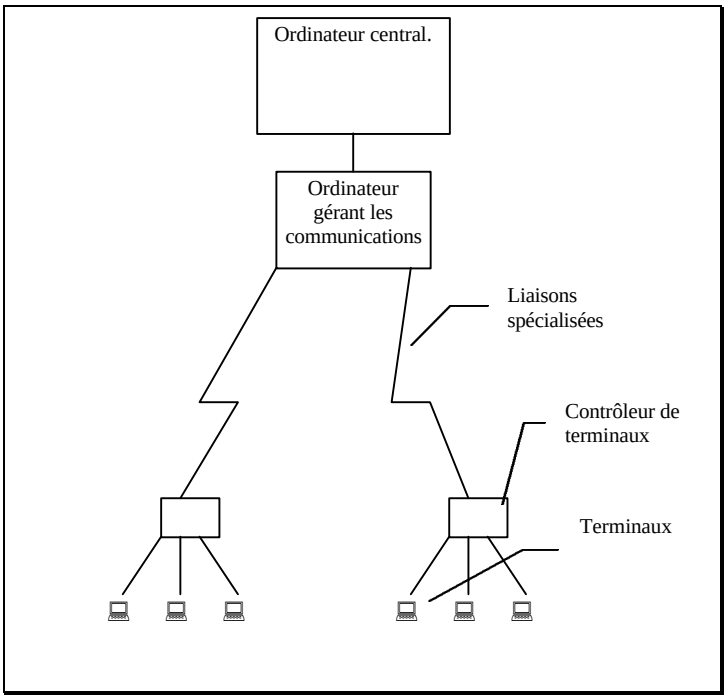
Quelques chiffres qui expliquent bien des bouleversements

Microprocesseur	Date	Prix	Opérations / sec
Intel 4004	1971	?	60000 sur 4 bits
Pentium Pro	1996	<>1000 $	100 Millions / 32 bits

Super Calculateur

Cray 1	1985	10 Millions $	100 Millions / 32 bits

Schéma d'un réseau type des années 70-80 Avant les réseaux locaux



On voit dans cette architecture un système très centralisé, conforme aux prix du marché. L'ordinateur est très cher, les terminaux assez bon marché.

Chaque constructeur durant les années 60-90 a développé son propre réseau informatique avec son langage propriétaire. Ceci permet de garder une clientèle captive, l'utilisateur n'ayant que peu de possibilités d'aller voir un autre constructeur. Certes à cet époque IBM ® se fait copier ses machines par deux ou trois constructeurs mais c'est très limité. La société **IBM** à la fin des années 70 détenait 80 à 90% des ventes d'ordinateurs.

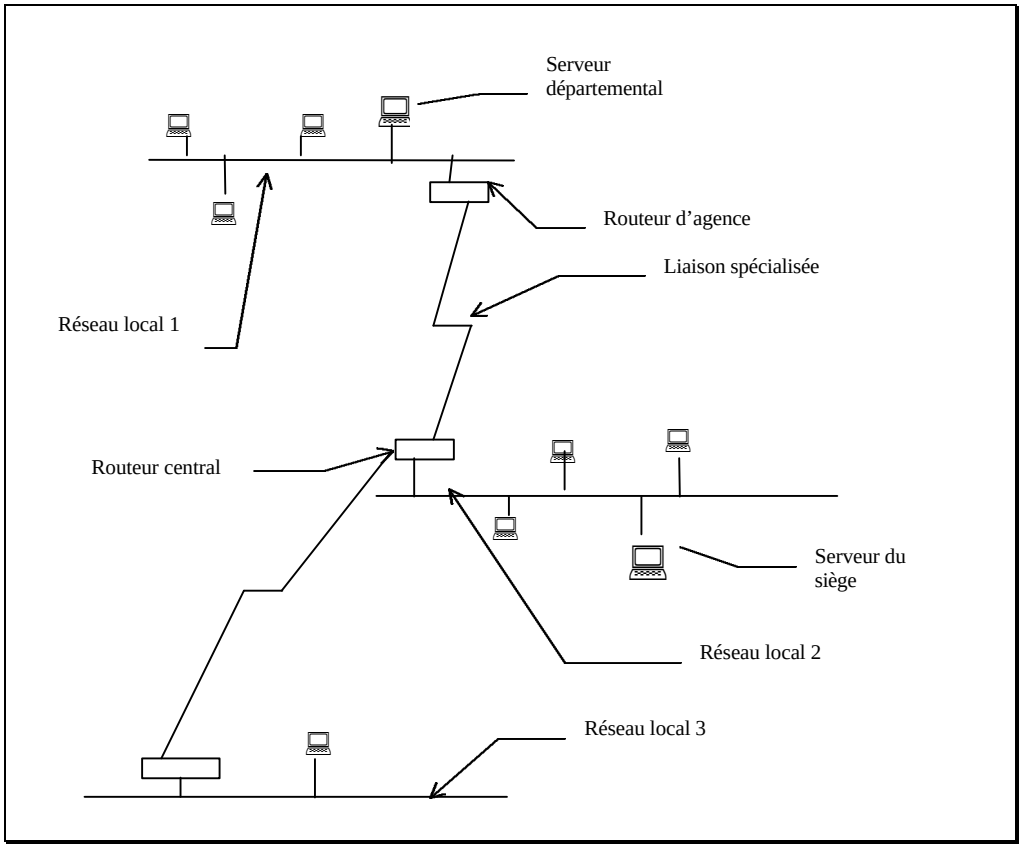
Cependant les clients évoluent, ils rachètent d'autres entreprises qui n'ont pas forcément les mêmes ordinateurs. Comment faire pour communiquer entre deux systèmes complètement différents ?. On voit alors apparaître des machines de réseau qui sont des traducteurs, d'un coté, il vont parler le SNA d'IBM, de l'autre le DSA de BULL. On voit ainsi que pour connecter n constructeurs, il faut créer, à condition que les traducteurs soient réversibles, n (n+1)/2 traducteurs. Travail gigantesque et difficile à mettre à jour car les langages réseaux évoluent très vite.

Il a donc fallu se réunir entre constructeurs pour définir un langage commun qui permette d'interconnecter les systèmes. Il en est résulté le protocole **OSI** (Open System Interconnection) de l'**ISO** (International Standards Organization). Ce langage devait résoudre le problème des communications hétérogènes.

En fait ces développements n'ont jamais été publics (pas de sources), le marché restreint. Peu de constructeurs se sont dit : « J'abandonne mon langage pour l'OSI ». Du coup un petit langage né du Département de la Défense Américain (**DOD**) et promu par des Universités (Berkeley) est devenu ce langage d'interconnexion. Il s'appelle **INTERNET PROTOCOLE** (IP)

Pour donner un ordre d'idée : pour une petite machine IBM des années 1988. OSI valait 100 KF et TCP/IP 5 KF . De plus avec TCP/IP on pouvait se relier à un vaste réseau existant. Le choix est vite fait !.

Schéma typique de l'informatique avec l'arrivée des réseaux locaux



On voit que cette informatique est plus décentralisée. Le serveur central n'est plus sollicité que pour la noble tache.

Le Modèle OSI. de l'ISO

OPEN SYSTEM INTERCONNECTION

Dans les années 1980, des commissions de normalisation , ont défini comment écrire un nouveau réseau, propre à interconnecter les machines de différents constructeurs. Il en est resté un succès qui s'appelle X25 pour la troisième couche, mais le réseau mondial OSI n'existe toujours pas. Cependant ce modèle a clarifié les choses en matière de réseau.

Ce modèle a aboutit à une représentation en couches qui reste une référence pour tout le monde , même si les réalisations différent quelque peu.

Application
Présentation
Session
Transport
Réseau
Liaison
Physique

Niveau 1 Couche Physique

Les signaux électriques, lumineux, le format des connecteurs

Niveau 2 Couche Liaison

On échange des trames de bits entre deux émetteurs en liaison directe

Niveau 3 Couche Réseau

On fait du routage dans les machines du réseau et du démultiplexage dans les extrémités .

Niveau 4 Couche Transport.

On distingue plusieurs classes de transport suivant la qualité des couches précédentes. Plus les couches inférieures sont complètes, moins la couche transport travaille et réciproquement. On s'occupe du contrôle de flux, de la reprise sur erreur, de la remise dans l'ordre des paquets. Nous étudierons TCP (Le transport INTERNET) qui est un exemple bien que développé indépendamment de la normalisation ISO.

Niveau 5 Couche Session

On verra avec TCP/IP que seul 5 couches sont vues a la place des 7 du modèle. Dans Session, on négocie l'établissement de la liaison avec le site distant, on ouvre et on ferme les sessions avec les sites distants. On pose des points de resynchronisation (pour redémarrer en cas de problème sur un point précis).

Niveau 6 Couche présentation

Un langage système pour harmoniser les différents services. En quelque sorte les points d'entrées du système d'exploitation. (les sockets de tcp/ip en plus élaboré)

Niveau 7 Couche application

Toutes les applications réseau, messageries, transfert de fichier, etc ...

Les équipements de routage n'implémentent que les trois premières couches. Seuls les ordinateurs source et destination implémentent les 7 couches.

L'ISO n'est pas le seul organisme de normalisation, on trouve aussi **IEEE** et l'**IAB** (Pour TCP/IP). De nombreuses références sont faites du type ISO8802.3 ou IEEE802.3 ou RFCXXX. Ces références proviennent de ces organismes.

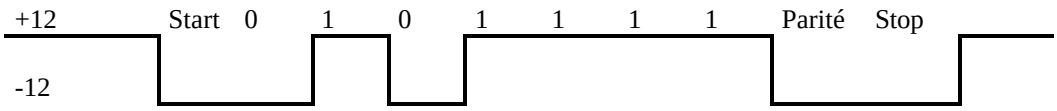
La Couche Physique

Les Codages de caractères
7 bits 8 bits ASCII.. ISO 8809-1. Voir l'utilitaire charmap de windows pour voir une table de codes

La transmission , 2 modes :
- Transmission parallèle : C'est une transmission simultanée des bits d'un même caractère. Ce type de transmission pose des problèmes de synchronisation et reste cantonnée à des courtes distances, du style Bus d'un ordinateur ou câble d'une imprimante. Le câble est le plus souvent plat.
- Transmission en série . On envoie les bits les uns après les autres : 2 types de codages sont utilisés, le codage dit asynchrone et le codage synchrone.

Les supports de transmission
- Les fils (Cuivre, Or..)
- La Fibre Optique
- Les signaux Hertziens (paraboles <10km)
- Les lasers (sans fibre) (<5 km)

Le mode de transmission asynchrone :
schéma temporel :
Il faut distinguer le zéro d'une tension nulle. Un bit 0 n'est pas le rien du tout. L'interface V24 utilise des tensions +- 12Volts



Ce type de transmission est utilisée sur tous les ordinateurs du marché. Chacun possède un port , dit port série, appelé sur les PCs COM1 .. COM4 . Ces ports sont utilisés pour piloter une souris ou un modem[1].
Remarques :
Pour transmettre un caractère, on utilise 2 bits inutiles, donc le débit est diminué. Souvent on utilise en plus une parité, dite paire ou impaire pour faire du contrôle d'erreur . Cette parité est peu efficace et reste à l'état de statistique. Dans le cas d'une liaison INTERNET , le protocole PPP utilise une transmission sur 8 bits sans parité. PPP sera abordé plus loin, c'est une couche de liaison.

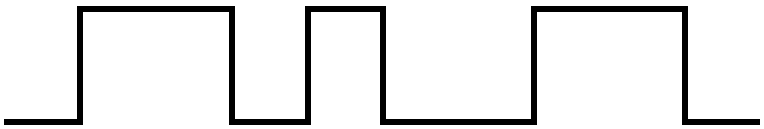
Le mode Synchrone
Emetteur et Récepteur se mettent d'accord sur un moyen de se synchroniser. Le problème vient de ce que les vitesses de transmission ne sont jamais exactes. Les modes synchrones émettent des chaînes de bits au lieu de caractères, ce sont des **trames**. Ces modes sont utilisés pour les forts débits.

Transmission en Bande de Base
Pour éviter de se désynchroniser, il faut éviter la monotonie.. Surtout faire varier le signal. Voici un exemple de codage du bit zéro et un sur le réseau ETHERNET, le codage Manchester . Si l'on transmet 500 bits à un, il ne faut pas se désynchroniser, chaque bit introduit donc une variation du signal.

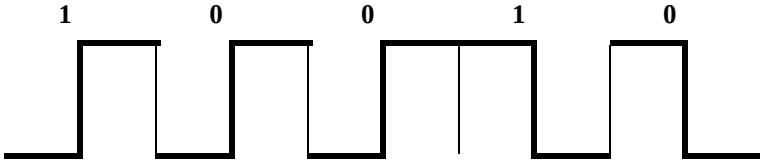
Codage Manchester :
Ceci représente l'évolution du potentiel électrique dans le temps

1 0 0 1 0

[1] modem (Modulateur / Démodulateur) permet de communiquer sur de longues distances via le réseau téléphonique ou des liaisons spécialisées.



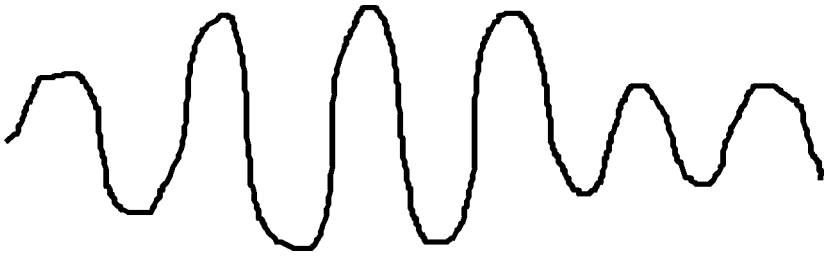
Le Manchester Différentiel
Il tient compte du bit précédent . Le bit zéro est un changement de polarité, le bit un non . Ce codage ne dépend pas de la polarité. Il est utilisé comme niveau physique du réseau Local ETHERNET



Problème de la transmission bande de base : Ces signaux se déforment vite. Le carré s'arrondit, le signal s'aplatit . Ils sont généralement utilisés pour de courtes distances. Pour aller plus loin, on utilise des signaux sinusoï daux. En fait la sortie d'un ordinateur, reste bande de base, plus loin, on utilise un appareil dit modem qui va faire un recodage des signaux. Si la technologie s'améliore on change le modem et non l'ordinateur.

Les Modulations
Sur des transports longue distance on va utiliser un modem qui va transformer le signal bande de base en signal sinusoï dal.. On trouve différents types de modulations qui vont coder l'information.

Modulation d'amplitude.



Modulation de phase

Modulation de fréquence :

Modulation de phase à quatre moments

00 01 10 11 10 00 00

Les Sens de transmission.

On trouve différents types de liaisons.

Simplex	Emetteur	➔	Récepteur
Alternat ou Half-Duplex	Emetteur	➔	Récepteur
	↑		↓
	Récepteur	←	Emetteur
bidirectionnel ou Full Duplex	Emetteur	➔	Récepteur
	Récepteur	←	Emetteur

Contrairement à ce que l'on pourrait croire ETHERNET dans sa version d'origine est un protocole Half-Duplex. On peut soit émettre, soit recevoir.

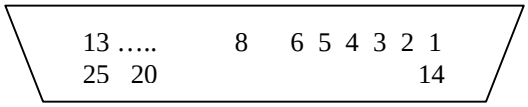
Les jonctions, interfaces ou connectique

Exemple la jonction V24 (ou RS232C).

Ceci décrit l'interface du port série d'un PC, pour communiquer avec un appareil externe. En fait, il existe deux types d'appareils, les DTE (Data Terminal Equipment) ou les DCE (Data Communication Equipement). Le DTE est un terminal ou ordinateur, alors que le DCE est généralement un modem.

La norme V24 hélas n'a jamais décrit le connecteur physique et pendant de nombreuses années , les connecteurs étaient non normalisés. Il fallait créer des câbles spécifiques pour connecter des appareils de constructeurs variés . Depuis l'arrivée des micro-ordinateurs, une interface de type Canon ® DB25 ou DB9 est devenue un standard. C'est celle que l'on voit à l'arrière de l'ordinateur. Cette sortie est trapézoï dale.

Vue de face de la sortie V24 / DB25:



Ces connecteurs vont recevoir ou transmettre des signaux. Comme cette interface doit recevoir beaucoup d'appareils , celle-ci dispose de beaucoup de broches. En fait on utilise principalement ceux-ci :

(Plutôt que de parler DTE /DCE, voici un schéma de connexion PC/modem) . Certains de ces signaux sont obsolètes comme ceux utilisés pour composer des numéros. De nos jours on utilise le protocole Hayes.

Les flèches indiquent qui émet le signal vers qui.

Les numéros 103 , 104 sont les références de la norme que les gens ont transformés en étiquettes plus lisibles comme CD à la place de 109. Cependant, sur certains modems on voit encore ce genre d'indications.

Câblage V24 d'ordinateur à modem

Ordinateur (DTE) DTE = Data Terminal Equipment		Modem (DCE) DCE = Data Communication Equipment
20 (DTR) Terminal prêt	➔	
2 (TD) Transmission de données (103)	➔	
3	←	(RD) Réception de données (104)

4[2] (RTS) Request to Send	→	
5	←	(CTS) Clear to Send
6 (DSR) Modem Prêt	←	Modem Prêt
8 (CD) Carrier detect	←	Détection de porteuse on voit aussi 109 sur les modems

Ces signaux sont juste de type On/Off (+_12V) sauf pour TD/RD qui véhiculent les données. Pour connecter un modem sur un PC, il faut un câble spécial qui est vendu avec les modems. Si l'on veut faire un transfert d'ordinateur à ordinateur, il faudra un câble dit croisé. Voici un schéma type .

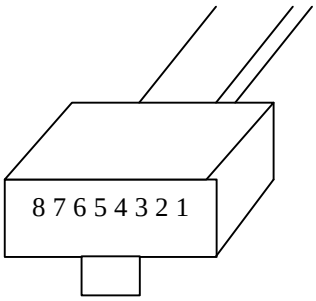
Câblage V24 d'ordinateur à ordinateur. Lien série PC <-> PC

PC		PC
2	→	3
3	←	2
4	→	6
↓ (Soudure)		
5		4
		↓ (Soudure)
6	←	5

4 fils vont donc suffire, mais pour faire des transferts il faudra des programmes spécialisés tels laplink ou le transfert sur câble direct de MICROSOFT.

Il existe bien des jonctions, ETHERNET utilise la RJ45, le téléphone la RJ11

La RJ45 ETHERNET :
Beaucoup plus simple, juste une paire de fils en émission , une paire en réception , avec une particularité !.
Le câblage utilise 8 fils groupés en 4 paires torsadées. Le connecteur mâle suivant rentre dans une prise femmelle murale ou dans un Hub ou dans une carte réseau.



1 et 2 émission 3 et 6 ! réception.
On prend 2 paires de fils suivant un code de couleur précis, pour prendre des automatises. Chaque paire est constituée de torsades, pour la paire réception, un des fils va sur la sortie 3 , l'autre vers le 6.
Les paires sont torsadées (Twisted Pair) on parle aussi de câblage UTP ou STP (Shielded ou Unshielded) suivant que les câbles sont dans un blindage

X21 / V35
Ces interfaces sont utilisées dés que la vitesse sur la ligne spécialisée dépasse 64Kb/s ou que le protocole X25 est utilisé. Celles ci sont réservées au mode synchrone alors que la V24 peut faire de l'asynchrone ou du synchrone.

[2] Ces signaux sont très importants car ils servent au contrôle de flux. Voir le protocole V42bis de compression de données.

Les modems

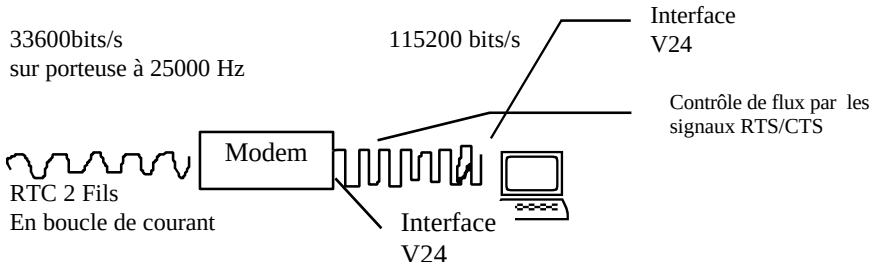
Avis CCITT	Débit en bits/s	Type de modulation	Vitesse de modulation	Exploitation
V 34	28800	Phase+Amplitude	3200 Hz	Full Duplex
V32	9600	Phase+Amplitude	2400 Hz	Full Duplex
V32 bis	14400	« «	3200	« «

Les modems dits asynchrones du marché qui sont utilisés comme Fax ou comme moyen de transmission sur INTERNET ou sur les services kiosque 36xx, sont couramment des modems V34bis (33600 bits/s). Ces modems présentent un certain nombre de possibilités. Ceux-ci sont dits compatibles Hayes, supportant les protocoles V42bis de compression et correction d'erreurs.

Hayes [3] : un jeu de commandes qui permet de paramètrer le modem . Avec une émulation de terminal, ou un terminal, on peut envoyer des commandes à celui-ci[4]. Lorsque le modem est en attente d'une connexion on tape ce genre de commandes. Celles ci démarrent toujours par deux caractères : **at** suivi de la commande
at&v
Le modem affiche sa configuration
atd0442276892
on appelle ce numéro
ats0=2
Mise en réponse automatique.

De nos jours, des systèmes comme Windows95 masquent ce genre de commandes via des drivers. On peut cependant utiliser en direct les commandes pour analyser les erreurs. Dans ce cas on sélectionne le port série dans Hyperterminal de Windows95 ou NT au lieu du pilote de modem.

La compression : On dit en ce moment que l'on transfère à 115kb/s alors que le modem lui va à 33600 Bit/sec. En fait , à travers le port série qui émet à 115Kb/s, on va agir comme dans un entonnoir. Le modem va essayer de comprimer les caractères envoyés. Si la ligne ne va pas assez vite, il va désactiver le signal CTS pour dire qu'il ne veut plus de données. On fait du contrôle de flux avec RTS/CTS (Voir interface V24)



On trouve de nombreux types de modems qui sont utilisés sur des liaisons spécialisés, ceux-ci ne sont parfois même pas normalisés. Il faut alors acheter une paire de modems au même fabricant. France Télécom fournit ses liaisons spécialisées synchrones avec deux modems d'extrémités. Il faut lors de la commande spécifier quel type d'interface on veut pour la liaison spécialisée (V24, V35, X21..) . Cette interface doit être la même que celle de l'équipement que l'on doit raccorder (Un ordinateur ou un routeur).
X2 / K56Flex : Ces modems récents permettent de dépasser les 33.6 Kbs si l'une des extrémités est de type RNIS (Numéris). Ils sont dissymétriques (56 kbs /16kbs) et sont utilisés pour se connecter aux fournisseurs INTERNET.

[3] Hayes est une société qui fabrique des modems. On utilise sa façon de faire
[4] Sous Windows95 on prend Hyperterminal en utilisant directement le port du modem (com1 ..)

La Détection et la Correction d'Erreur

Les données sont transmises mais la ligne peut avoir des parasites, elle est bruitée. Il va donc falloir détecter et corriger ces erreurs.. Les codes correcteurs s'appliquent dans le cas de liaisons longues distances, par exemple les sondes spatiales, ou les délais de propagation de signaux dépassent plusieurs minutes. Il est hors de question de retransmettre. Il s'accumule un train de données énorme entre la sonde et la terre.
Le volume de données entre les deux systèmes peut être de 10 000 000 bit/s[5] * 10 min * 60 sec = 600 Mo (un petit disque dur)..

Les codes correcteurs
Il est donc impératif de corriger les erreurs plutôt que de les retransmettre. Pour ce faire, on va rendre l'information plus complexe en modifiant le codage habituel. Supposons que l'on ait un codage réduit de 4 valeurs : par ex

00,01,10,11, un erreur sur ce genre de codage conduit à une valeur correcte !. On va donc changer le codage et en proposer un autre.

00= 0 0 0 0 0
01= 0 1 1 1 1
10= 1 0 1 1 0
11= 1 1 0 0 1

Une erreur sur un code ne donne plus un code existant, on peut alors faire un calcul de distance sur la combinaison la plus proche. C'est ce genre de technique qui est utilisé. Bien évidemment, celle-ci est très coûteuse en bande passante, puisqu'il faut rajouter de l'information et presque la doubler.. Les protocoles de transport ordinaires ne l'utilisent pas et ne mettent en place qu'un simple mécanisme de détection d'erreur.

Détection d'erreur.
La parité : Tous les sept ou 8 bits , on rajoute un bit dit de parité. Ce genre de protection est peu performante car deux erreurs passent inaperçues .
Les méthodes standard, utilisent une division de polynômes . Les deux extrémités, se mettent d'accord sur un polynôme de degré 16, dit polynôme générateur par exemple $1 + x^7 + x^{16}$. Ensuite, à partir des B éléments de la trame, on va calculer un autre polynôme de degré B-1. Ce polynôme s'écrit , ai étant le iéme élément de la trame,

$$P(x) = a_0 + a_1x + .. + a_{b-1}x^{b-1}$$

On calcule ensuite la division de ce polynôme par le polynôme dit générateur. Le reste est un polynôme de degré 15 qui s'écrit : $R(x)=r_0 + r_1x + ... + r_{15}x^{15}$
Les valeurs r0 à r15 sont ensuite stockées dans la zone de détection d'erreur. Lors de la réception, le récepteur fait le même calcul et compare son résultat avec celui de l'émetteur. Si ça coï ncide , pas d'erreur, sinon erreur.
Limites de la méthode : on peut avoir une erreur sur la zone de contrôle, alors que les données sont valides. Pour diminuer cet effet, il faut éviter que la zone de contrôle soit grande par rapport à la taille de la trame.

Cette zone est appelée dans la littérature **CRC** (Cyclic Redundancy Code) ou **FCS** (Frame Check Sequence).

A cause des erreurs de transmission, l'information est transmise par petites bouffées (**trames**) pour rester en dessous du taux moyen d'erreur (10^{-4} pour le téléphone). Un bit sur 10000 est faux. Les bouffées ou trames devront être de taille inférieure à ce chiffre.

[5] Si la vitesse de modulation du signal est de 10 Mbit/s

LES RESEAUX LOCAUX

LES RESEAUX LOCAUX

Les types de réseaux locaux

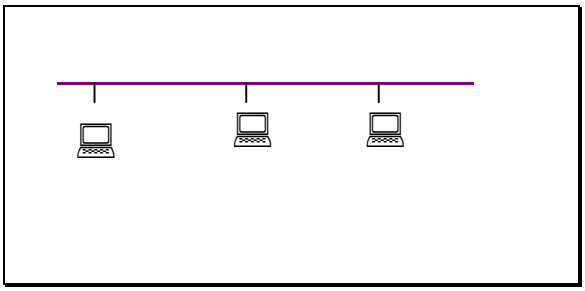
Le But :

Raccorder sur un même support physique des ordinateurs, et permettre de communiquer avec un ensemble d'ordinateurs sur ce support. Un seul message sur le support peut être lu par plusieurs ordinateurs. Les modems sont remplacés par des cartes réseaux que l'on installe dans les ordinateurs. Ces réseaux sont de taille limitée. Cette limite est due au protocole lui-même.

On trouve schématiquement deux types de réseaux, les **BUS** et les **Anneaux**

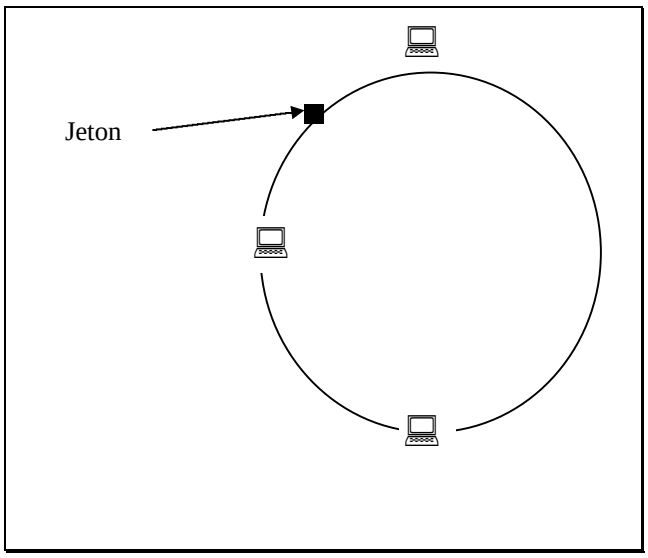
Dans le cas des BUS, tout le monde parle sur un même fil. Pour gérer les collisions inévitables, on s'empare du fil en émettant suffisamment longtemps (le temps de la propagation aller/retour du signal sur le support), pour s'assurer que le message a été correctement lu.

ETHERNET est de type BUS



Dans le cas des Anneaux, une trame vide circule en permanence sur le fil qui relie l'ensemble des machines. Cette trame s'appelle le jeton. La machine qui a le jeton peut y insérer des données. Le jeton peut être perdu. Le temps de réaction à cette perte encadre la dimension du réseau et le nombre des machines qui peuvent s'y connecter. Les anneaux se comportent mieux sous forte charge.

Token Ring est de type Anneau à Jeton



ETHERNET

Le support Physique ETHERNET ou IEEE802.3

ETHERNET ou le début du réseau Local (RFC 894 et 1042)

ETHERNET a été développé par Xerox Corporation au Palo Alto Center (PARC) vers le milieu des années 70. Il fait suite au développement d'un projet de réseau (ALOA) de l'Université de Hawaii. A cette époque, le concept de réseau local n'existe pas, le micro-ordinateur non plus. Bref un peu de paléontologie.. ETHERNET est novateur car la vitesse d'échange entre ordinateurs n'excèdait guère 64 Kilo bits par seconde. Le principe est donc de mettre un support physique en commun, et de faire du très haut débit sur des distances moyennes (>100m).
La spécification de ETHERNET a été faite conjointement par DEC, Xerox et Intel.

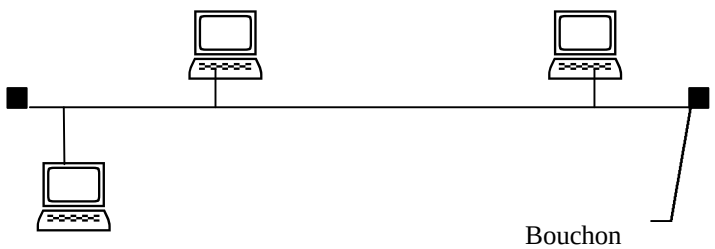
On utilise un câble commun pour relier des dizaines voire des centaines de machines. Ce câble commun va véhiculer les informations à destination de l'ensemble des stations, la méthode utilisée est le CSMA/CD (Carrier Sense Multiple Access / Colision Detection).
Le Câble forme un BUS dans le jargon réseau, reliant les stations. La vitesse est fixée par la norme : 10 Mbs. (10 Millions de bits par seconde). Un bit est une valeur binaire : 0 ou 1.
Des prix : début 80 une carte ETHERNET vaut 10000Fr, maintenant 150Fr ! ! !

La notation IEEE802.3 :
10Base5 10=10Mbs Base=Bande de Base 5 = 5*100mètres ex :

Nom	**10 Base 5**	**10 base2**	**1 Base5**	**10BaseT (1985)**	**10Broad 36**
Vitesse Mbps	**10**	**10**	**1**	**10**	**10**
Signal	**Baseband**	**Baseband**	**Baseband**	**Baseband**	**Broadband**
Longueur Max	**500**	**185**	**250**	**100**	**1800**
Media	**50 Ohm coax (thick)**	**50 Ohm coax (thin)**	**Unshielded Twisted Pair**	**UTP**	**75 ohm coax**
Topologie	**Bus**	**Bus**	**Bus**	**Etoile**	**Bus**

Un certain nombre de réseaux cités sont très rares (10Broad36 ou 1Base5).

Topologie de Bus



Exemple de réseau ETHERNET. Les bouchons sont là pour éviter les réflexions parasites.

Problème : Comment parler sans que ce soit le désordre ?. ETHERNET a dû répondre à ce problème.
Ce protocole est aléatoire, chacun parle quand il a envie, mais suivant des règles strictes. Si deux machines émettent en simultané, il se produit une **collision**. Celle-ci n'est détectée que pendant l'émission d'une trame.

1. Avant de parler on écoute le câble. Si silence étape 2.
2. On émet une trame de 64 octets minimum et au plus 1518 octets. La collision doit être détectée pendant l'émission de la plus petite trame. Celle-ci comprend 64 octets, soit 512 bits transmis en 51,2 µs (à 10 Mbit/s). On écoute pendant l'émission, il faut avoir le retour d'information comme quoi une collision vient d'arriver. Pour cela la longueur maximum du réseau correspond à une durée de 25,6µs. Si l'on utilise une fibre optique, la longueur maximum en km sera de $3*10^5 *25.6*10^{-6} =$ 7km. En fait ce cas est rare car la vitesse est plus faible dans les câbles, de plus le signal s'affaiblit et il faut le régénérer par des répéteurs qui ont des temps de traversée. C'est souvent plus proche de 500m.
3. Le signal se propage comme une onde qui va parcourir le câble. Or, des stations ont pu croire que la câble était libre et se mettent à parler. Il se produit dans le jargon ETHERNET, une collision. On détecte une trame brouillée (Jam).
4. Si collision, on émet une trame de brouillage, on calcule un nombre aléatoire et on attend avant de réémettre[6]. Toutes les stations font le même calcul. Passé ce délai, on réémet la trame. Et ainsi de suite jusqu'à 16 fois, avant de remonter une anomalie à la couche supérieure.

Le support d'origine était un câble coaxial qui ne comporte qu'un fil central et un blindage. Ce type de support ne permet pas une transmission bidirectionnelle mais juste unidirectionnelle. On dit que la transmission est half-duplex. (on émet ou on reçoit). Ceci a changé avec l'apparition de 10 Base T qui comprend 2 paires de fils, une pour émettre et une pour recevoir. Ceci dit, à part dans les commutateurs ETHERNET modernes le protocole reste **half-duplex**.

Au delà de la limite de distance du support , on peut étendre le réseau à l'aide de répéteurs qui vont réamplifier le signal vers un autre segment ETHERNET. On ne peut pas traverser plus de 2 à 3 **répéteurs**. Au-delà on utilise des **ponts .** Le pont lit les trames et les réémet, de plus il apprend les adresses ETHERNET et fait office de filtre. Le répéteurs eux amplifient tout, même les bruits. Le pont travaille au niveau logique, fait du contrôle d'adresses et d'erreurs.
Les ponts peuvent boucler le réseau à condition d'utiliser l'algorithme Spanning Tree. L'expérience montre que loin de faire une redondance entre ponts, la détection des problèmes s'avère fort délicate. Il vaut mieux éviter de boucler un réseau ETHERNET.

Le Format des trames.
On trouve plusieurs formats : IEEE802.3, IEEE802.2, ETHERNET2, ETHERNET SNAP. Pour simplifier, on ne présente que ETHERNET2. TCP/IP utilise la plupart du temps le format ETHERNET2. Pour IEEE802.3 le champ type devient un champ longueur. On ajoute parfois un en-tête dans la partie donnée qui s'appelle le LLC suivi éventuellement du SNAP. Ces en-têtes supplémentaires provoquent une perte de données utiles que TCP/IP évite en prenant le format originel de ETHERNET (II).

Les chiffres indiquent le nombre d'octets (8 bits)

7	1	6	6	2	46-1500	4
Préambule	SOF	Adresse de Destination	Adresse Source	Type	Données	FCS

Préambule :
Attention, une trame arrive, synchronisez vous (Toutes les horloges ont des dérives 10Mb/s +-)
SOF (Start of Frame)
Fanion de début de trame (séquence caractéristique).
Source :
Chaque carte a une adresse unique générée par le constructeur de la carte.
Destination :
Soit l'adresse d'une carte, soit une adresse de diffusion de groupe ou de réseau (Broadcast)
Type :
Quel service réseau va lire la trame. Par exemple IP ou NOVELL ou LAN Manager . Ces types sont normalisés. Le type indique à quel logiciel (couche) on va renvoyer les données.

FCS (CRC Cyclic Redundancy Check)

[6] Il existe de toute façon un temps inter trame égal à 12 octets soit 9.6 µsec

Un code est rajouté pour voire si une erreur a endommagé la trame. Si c'est le cas elle est mise à la poubelle au niveau de la carte réseau.
Polynôme Détecteur d'erreur calculé par un circuit sur la carte :
$g(x) = x^{32} + x^{26} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1$

Chaque carte vendue dans le commerce possède une adresse source qui est unique. Les 3 premiers octets réprésentent un code du constructeur, la suite le numéro de série de la carte. Les machines utilisent leurs adressent matérielles pour communiquer. De temps en temps, elles utilisent l'adresse de diffusion ou broadcast. Celle-ci est constituée par 48 bits à un. Les adresses sont souvent représentées par des valeurs hexadécimales, séparées par le symbole « : » . L'adresse de broadcast s'écrit donc ainsi : FF :FF :FF :FF :FF :FF.

Les JONCTIONS et la connectique
L'Interface AUI
Une interface DB15 (15broches) qui permet de mettre un transceiver externe qui peut s'adapter à tout type de support (Coax fin, 10 BaseT, 10 BaseF) F pour fibre optique. Les cartes ont très souvent ce connecteur supplémentaire. Seul inconvénient, il n'est pas Full-Duplex.

10Base2
Un câble coaxial fin avec des connecteurs en **T**. Facile a mettre en place. Par contre les connecteurs affaiblissent le signal , du coup on ne peut mettre que 30 stations sur le câble. Tend à être remplacé par 10BaseT. Un problème sur le câble et 30 stations en panne contrairement à 10BaseT.

10 Base T :
Le support est constitué de 2 paires de fils torsadés (twisted pairs), prolongés par des connecteurs d 'extrémité appelés **RJ45**. Ces câbles vont dans des appareils appelés HUB qui connectent les machines. Il existe des HUB 8 ports 12 /16/24 ports. On ne doit pas connecter par des câbles, plus de 3 Hubs. Les câbles de connections qui les relient sont des câbles croisés. Voir schéma du cours. En 85, la porte sur le Hub valait 2000Fr , maintenant 300 à 400 Fr. Les Hub peuvent être cascadés en local avec des câbles propriétaires. Ils ne forment alors qu'un seul ensemble. Dés qu'ils sont éloignés , il faut des câbles croisés. Les machines ne doivent pas être à plus de 100 mètres du Hub. Idem pour les Hubs entre eux.

Les évolutions :
La technologie aidant, le prix des processeurs chutant, on voit apparaître des HUB intelligents appelés switch (commutateurs) . Ces commutateurs sont capables de lire une trame et de la diriger sur l'un des ports en fonction de l'adresse de destination. Par rapport au Bus classique, on ne reçoit que les trames pour soi, et donc on améliore nettement la capacité du réseau. C'est un peu comme si l'on mettait un pont entre chaque porte du Hub.
Ces switchs ont deux modes, le Store and Forward et le Cut Through. Le premier lit la trame et si elle est valide l'envoie, le deuxième lit l'adresse destination et dès que celle-ci est lue, envoie le reste vers la bonne destination sans attendre, ceci propage hélas aussi les erreurs (mauvais CRC). Store and forward est de plus en plus utilisé.
Une autre technique est d'attendre la longueur minimale d'une trame (64 octets) avant de la transmettre.

100 Base T
En fait , en gardant le principe de ETHERNET, on transmet à 100 Mbs. Ceci ne peut marcher que sur un réseau qui ne fait que du 100BaseT. Ce sont donc des Hubs particuliers qui utilisent les câbles habituels du 10BaseT, toutefois les connecteurs d'extrémité sont blindés.
Pour avoir à la fois du 100Mbs et du 10Mbs sur le même réseau, il faut interconnecter avec des switchs.
Un switch vaut au moins 1000Fr la porte (200Fr pour un Hub), par contre la carte ETHERNET 100Mbs est à peine plus chère que son ancêtre.
GIGA Bit Ethernet
Le concurrent de l'ATM pour les hauts débits. Même principe mais la vitesse est de 1Gigabit/sec. Le prix des cartes et des liens 1Gbs étant assez bon marché, le Gbs risque de faire une sérieuse concurrence à l'ATM.
Le Gigabit Ethernet utilise en 1999 uniquement les fibres optiques. Cependant, une normalisation sur paire métalliques va avoir lieu. Le cablage recommandé devra suivre les spécification 5E. Il faudra faire très

attention à avoir les mêmes types de cable (impédance). Curieusement, le Gigabit sur cuivre sera un protocole de transport parallèle qui utilise les 8 fils, 4 en émission et 4 en réception. Les émissions étant à 250 Mbs sur chaque fil.

Vers le Full Duplex

On a tendance en fait à réserver 100BaseT pour des serveurs qui sont très sollicités et de laisser 10BaseT pour les stations. Mais ça changera assez vite , surtout pour les installations nouvelles.

On parle aussi de plus en plus du Full Duplex pour le 10BaseT et le 100BaseT. En fait comme on a une paire émission et réception, autant en profiter. Du coup le Hub devenu switch fait disparaître les problèmes de collisions. Une conséquence importante en devient l'agrandissement des distances. Il ne faut pas oublier que plus la vitesse d'émission augmente, plus la dimension du réseau ETHERNET diminue. La dimension minimale de la trame n'a pas évoluée et du coup 64 octets prendront moins de temps à être émis.

Les différentes variations de la trame ETHERNET (pour les initiés)

ETHERNET II (TCP/IP)

Source	Destination	Type	46 à 1500 octets	FCS

ETHERNET 802.3 (NOVELL uniquement)

Source	Destination	Longueur	46 à 1500 octets	FCS

ETHERNET 802.2

Source	Destination	Longueur	LLC 3 octets	46 à 1500 octets	FCS

ETHERNET SNAP (Apple / IBM)

Source	Destination	Longueur	LLC (3)	SNAP (2)	46 à 1500	FCS

Si le champ Type/longueur est supérieur à 05DC, c'est une trame ETHERNET II
La trame 802.3 « brute » est une erreur de NOVELL. Elle disparaît peu à peu.

Les câblages de bâtiments

On utilise le terme de capillaire pour les désigner les câbles qui irriguent chacun des bureaux, et celui de BackBone ou épine dorsale pour les connexions centrales. Généralement le capillaire est fait par de câbles dits de catégorie 5 (100Mbs), en cuivre (paire métalliques torsadées) et se raccordent à des armoires de communication sur des panneaux de répartition. Chaque bureau reçoit au bout de ce câble une prise murale avec une prise RJ45 femelle. Un câble souple permet de connecter l'ordinateur à la prise murale. La distance HUB Ordinateur doit être inférieure à 100 mètres.

Sur le panneau de répartition un autre câble souple relie la prise à un équipement actif . Un HUB ETHERNET ou TOKEN-RING ou un commutateur ATM. Les armoires sont souvent connectées par des fibres optiques permettant de faire passer des débits plus importants sur des distances plus longues.

Remarque : pour connecter des bâtiments différents, la fibre optique est obligatoire pour des raisons de terres électriques.

TOKEN RING
ou IEEE802.5 ou Anneau à Jeton

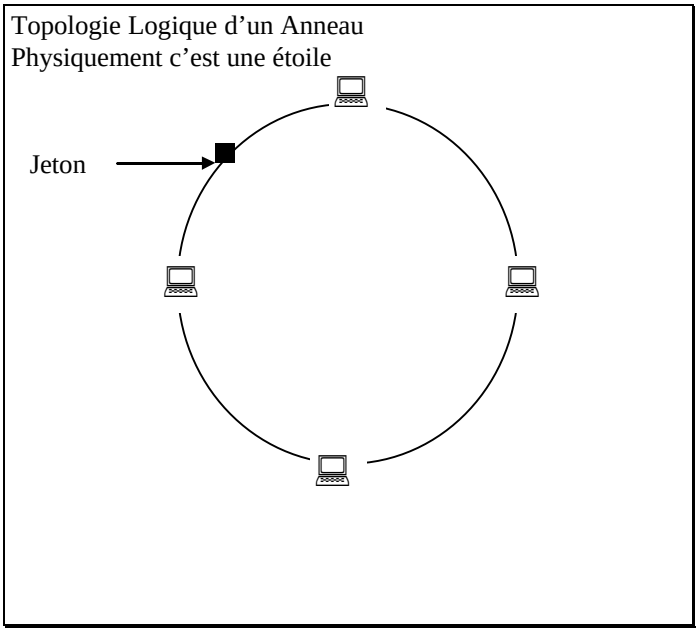
Token Ring est le protocole promu par IBM pour se démarquer de ETHERNET. Stratégie industrielle ?, ou vision différente du réseau et de la société. On a vu avec ETHERNET que l'organisation est très anarchiste. Tout le monde cause quand il veut. Bref IBM n'a pas dû aimer et a inventé l'anneau à jeton[7]. Un jeton tourne, va de station en station. Le jeton est une trame qui circule de station en station. Si vous l'avez et qu'il est vide, vous pouvez y ajouter vos données. Quand on émet, le récepteur prend l'information , indique dans l'en-tête qu'il a lu les données , le récepteur vérifie cette lecture et rend le jeton vide. Cette norme a évolué en vitesse. Au départ , c'était 4Mb/s, maintenant c'est 16 Mbs. La vérification de la lecture à 16Mb/s n'est pas faite.

Ce protocole était assez novateur pour le câblage, car il utilise du matériel actif équivalent au Hub ETHERNET, ceci bien avant 10BaseT. Avantage aussi, sous forte charge, le réseau ne s'écroule pas, tout le monde a le même temps de parole. Par contre sous faible charge il est plus lent. Les trames sont plus longues. On peut insérer des stations ou des MAU (MAU= medium access unit) à chaud. Les MAU sont alimentées par les stations. Donc le matériel est très fiable. Un anneau peut compter 256 stations.
La vitesse d'émission était de 4Mbs à l'origine, puis 16Mbs ensuite.
Le concept de l'anneau reste d'actualité dans les hauts débits (FDDI)

Format de la trame :

1	**1**	**1**	**6**	**6**	**>=0**	**4**	**1**
Start Delimter	**Access Control**	**Frame control**	**Adresse Destination**	**Adresse Source**	**Données**	**FCS**	**End Delimiter**

Le token = StartDelimter+AccessControl+EndDelimiter



Une station est le moniteur actif (la première connectée) et contrôle le réseau. Si une station est en panne, une trame peut ne pas s'arrêter .

[7] IBM n'a pas réussi à imposer TokenRing. Technologie trop chère, ouverture trop tardive ?. Du coup ETHERNET domine le marché et la commutation a enlevé les problèmes d'écroulement sous forte charge.

Rôle du moniteur
Gérer la perte du jeton
Se signaler aux autres par une trame spéciale régulièrement

La méthode d'accès est finalement beaucoup plus complexe et se prête moins bien à l'utilisation des commutateurs. Il faut sans arrêt émettre des jetons sur toutes les portes du commutateur. Par ce principe, la transmission ne peut être Full-Duplex. C'est une limitation de taille.

FDDI
ou Fiber Distributed Data Interface

Né au milieu des années 80 :

Principe : 100 Mbps, double anneau à jeton utilisant un support fibre optique. Les fibres peuvent être Multimode ou monomode. La différence entre les deux vient du fait que l'une est à gradient d'indice alors que l'autre a un cœur d'un autre indice dont le diamètre est égal à la longueur d'onde de la lumière transportée, celle-ci se propage alors en ligne droite sans dispersion. La monomode est réservée pour des cas particuliers (distance) et ses connecteurs sont chers. On utilise le plus souvent de la multimode dite 62.5/125 µm. Des lasers à diodes semi-conductrices sont utilisés pour émettre, de la même façon que pour la lecture d'un CD-ROM.
La technologie FFDI connaît une nouvelle jeunesse avec l'arrivée des commutateurs FDDI. Ceci dit, elle est très concurrencée par l'arrivée de l'ETHERNET à 100 Mbs et de la commutation ETHERNET à 100Mbs. On ne lui prédit plus un très grand avenir. Elle existe cependant de nombreux sites qui ont eu des besoins de gros débits avant l'apparition de 100 Base T.

Caractéristiques principales

- Distance entre deux nœuds 2kms
- 2 anneaux contrarotatifs
- 100 km à plat ou 35 km de diamètre
- 500 à 1000 stations possibles
- Trame maximum de 45000 octets
- Tolérance de panne en cas de coupure des anneaux

Pour émettre, il faut avoir le jeton et avoir été accepté par la station de management.

3 compteurs gérés par la station
LE TRTT (temps max de rotation du jeton)
Le TRT (par rapport au TRTT, combien de temps peut on parler). Si jeton en retard, on n'émet que les informations synchrones (voix, vidéo..)
Le THT temps maximal d'émission synchrone (temps réel)

VLANS
ou Virtual Lan (Réseau Virtuel)

Ce n'est pas une nouvelle norme de réseau local mais une méthode pour gérer les réseaux locaux. Il s'agit plus de supervision de réseau.

Les VLAN constituent une étape importante dans la gestion d'un grand réseau. En effet beaucoup de temps est passé pour séparer physiquement les réseaux dans des panneaux de brassage.
En général un grand réseau n'est pas un réseau tout à plat mais une série de réseaux cloisonnées physiquement et interconnectés par des routeurs.

Lorsqu'un utilisateur se déplace ou un bureau change d'affectation , il faut se déplacer pour modifier le panneau de brassage de manière à mettre ce bureau sur un autre HUB.

En fait avec les VLAN, qui prennent tout leur poids avec les commutateurs et leur généralisation, il est possible à partir d'une station de supervision de grouper les utilisateurs entre eux sans se déplacer. Le résultat est identique à une séparation physique. On ne pourra pas faire de partage d'information bricolé avec le collègue d'un autre service.

Les choix de séparation se font soit sur :
- les numéros de carte ETHERNET.
- les adresses TCP/IP.
- Le plus souvent l'interface physique d'un commutateur. On groupe les ports entre eux, ou qu'ils soient dans le bâtiment.

Problèmes : Jusque récemment, les HUB/Commutateurs communiquent entre eux suivant un protocole propriétaire. Une norme récente **ISO8021Q** devrait résoudre le problème de la coopération d'équipement variés entre eux.[8]

Pour que ces réseaux devenu physiquement séparés communiquent entre eux, il faut soit des routeurs, soit un VLAN commun dans lequel seront mis les serveurs communs. Ce VLAN commun va recevoir tous les broadcast de tous les VLANS.

Les VLANS posent aussi un problème de numérotage du réseau en TCP/IP car les requêtes ARP (broadcast) ne peuvent être satisfaites. En principe, il faudrait mettre chaque VLAN sur un réseau TCP/IP différent ce qui nécessite l'achat d'un gros routeur avec beaucoup d'interfaces, et complique singulièrement le réseau TCP/IP.

Une solution pour éviter ce problème est de forcer le partage d'information en passant par les serveurs centraux. On interdit de fait le partage d'informations de poste à poste.

[8] Cependant, les constructeurs ont tendance à dire qu'une norme est trop restrictive et diminue les possibilités. Le langage entendu chez un constructeur : si vous voulez le maximum de fonctionnalités, achetez tout chez nous.. Ce discours doit être soigneusement évité. La résistance se pratique au quotidien !.

TELEPHONIE NUMERIQUE

ISDN ou RNIS[9] : un exemple le produit Numéris de France Télécom .

HISTORIQUE

Depuis le début du siècle, les techniques de base du téléphone n'avaient que très peu évolué. Depuis le début, les techniques de la téléphonie sont purement analogiques. Un signal de microphone fait varier l'intensité d'une boucle de courant. Ce signal est envoyé à distance via des amplificateurs. De plus l'appareil de l'abonné est alimenté par le réseau via la boucle de courant.
Bref au temps de l'informatique, de l'électricité partout, et vu la chute du cours des microprocesseurs, tout ceci est bien archaï que. Qualité sonore médiocre, informations du réseau inexistntes. Transmissions informatiques rendues très délicates par la très faible bande passante. Celle ci est de 3000Hz et donc nécessite des appareils spéciaux appelés modems (Modulateurs / Démodulateurs) qui vont s'adapter a la ligne et transporter plus d'informations que 3000 bits/sec.

Ces appareils utilisent des codages en variation de phase sur une porteuse (Onde sinusoï dale) émise vers 2500Hz . Ceci permet d'aller beaucoup plus vite , ces modems suivent des normes, on parle de V23 V32 V34 V27 V29 ..Ce sont les avis du CCITT qui normalisent ces modems afin de permettre les interconnexions entre différents fournisseurs.

Cependant on devrait atteindre une limite liée au rapport Signal/Bruit et plus connue sous la forme de théorème de Shanon. Cette limite serait de 33600Bit/sec, limite actuelle. Des techniques mixtes utilisant en partie le réseau Numéris (coté fournisseur) vont permettre d'atteindre le 57.6 Kbits/sec. Il s'agit des modems X2 ou K56Flex qui sont commercialisés en ce moment. X2 est développé par USR (3Com®) et K56Flex par Rockwell ®. La future norme devrait être K56Flex.

Pour lever toutes ces contraintes, les membres du CCITT ont normalisé le **RNIS**. Le téléphone devient alors numérique. Une certaine contrainte apparaît que n'ont pas les protocoles informatiques, ce sont les contraintes de temps. On va alors parler de multiplexage temporel. C'est à dire que chaque communication qui a ouvert un canal de communication aura un égalité de parole dans le temps (ETHERNET ne joue pas ce rôle). Ceci permet d'éviter que la voie de son interlocuteur soit déformée. Elle doit arriver de manière stable dans le temps. Pour numériser la voie suivant les techniques traditionnelles, il faut 64 Kilo bits par secondes.

Le téléphone devient un mini ordinateur qui envoie des informations numérisées. Numéris est au téléphone ce que le Compact Disc Audio est au vinyle . Sur un seul câble, l'abonné dispose de 3 canaux logiques , deux à 64Kbit/sec dits canaux B plus un qui sert aux informations du réseau à 16 kbit/sec (le Canal D). La connectique est de type Bus , dit BUS S. Sur une seule liaison d'abonné, on peut recevoir 2 communications et connecter sur le même Bus jusqu'à 8 appareils[10]. On peut recevoir une télécopie pendant que l'on téléphone.

On reçoit, au niveau du poste téléphonique numérique, une information sur les numéros appelants. La composition du numéro et l'accès est immédiat (<1sec). On transférer entre deux ordinateurs à 64kbit/s voire 2*64kbs. (Téledisquette)

RNIS n'utilise que 2 paires de fils pour l'émission et la réception. On fait du multiplexage temporel sur 3 canaux logiques, 2 canaux B et un canal D. Les appels se font via le Canal D qui est partagé, celui ci doit gérer les collisions. En fait chaque fois que l'on émet dans le canal D, la régie renvoie l'écho de ce qu'elle reçoit. En comparant émission et réception, on s'aperçoit du brouillage.
Le canal D est aussi utilisé pour faire des accès X25 sur Transpac à petite vitesse..

[9] RNIS Réseau Numérique à intégration de service (ISDN est la contraction anglaise). Numéris le nom du produit RNIS de France Télécom.
[10] A condition d'avoir toutefois un autocommutateur. Voir sinon Numéris DUO pour le particulier.

Chacun des canaux B est la propriété d'un seul équipement. Cette technique est un multiplexage temporel à **commutation de circuit**. Un circuit logique est créé entre l'appelant et l'appelé et la gestion de la Bande passante est assez peu optimisée. En effet , on ne peut en aucun cas aller plus vite que le découpage à 64K, alors que la deuxième liaison est inutilisée ou que celle ci est peu bavarde.
RNIS est un produit qui commence à s'imposer sur une technologie déjà dépassée. RNIS date de 1985 époque ou les circuits étaient moins rapides, 10 Base T commuté n'existait pas.. Cependant, cette solution est normalisée et permet d'avoir une garantie de bande passante entre deux abonnés. 64 Kb/s jusqu'au Japon par exemple. Le seul frein est le paiement à la distance pour lequel INTERNET n'a aucun concurrent.

Groupage de canaux : On peut grouper au niveau RNIS ou PPP deux canaux 64 Kbs pour en constituer un seul .

LE RNIS RESTE DU TELEPHONE : Chaque canal B ouvert est tarifé à la durée et à la distance. On peut avoir des liaisons numériques de très longue distance.
VIDEO CONFERENCE : Numéris est parfait pour la vidéo conférence, dans le sens où la bande passante est GARANTIE. (Pas sur INTERNET). De plus les tarifs longues distances chutant, le fait de faire de la vidéo conférence sur INTERNET peut se révéler assez peu intéressant d'ici quelques années (du moins dans la France). (Rapport coût / qualité)
La vidéo conférence sur Numéris utilise 3 canaux. Un pour le son et deux pour l'image.

Produits Numéris et facturation :
Numéris est facturé depuis quelques années comme le téléphone. Par contre le coût d'abonnement est plus cher. Pour l'abonné de base, le produit à retenir est Numéris DUO. Celui-ci fournit une TNR (Terminaison Numérique de Réseau) sur laquelle on peut brancher 2 appareils analogiques (Prise T) et plusieurs appareils numériques (Téléphones, carte RNIS pour PC), via une sortie RJ45. On peut recevoir 2 appels en simultané. On a deux numéros de téléphone.
L'abonnement DUO est 30% plus cher que 2 lignes téléphoniques. Mais quand on transfère souvent des fichiers , la durée de la connexion diminue (et le prix aussi !). Bien sur , si le fichier traîne aux US sur INTERNET, votre abonnement Numéris ne servira à rien.

Les lignes primaires (E1)
De nombreuses entreprises ont des besoins de lignes groupées pour recevoir des appels simultanés. Du point de vue raccordement et cablage, il est plus simple de demander une ligne Numéris primaire. Il s'agit en fait d'une ligne constitué de 2 paires de fils cuivre faisant passer une liaison à 2Mbs. On peut faire circuler jusqu'à 30 Canaux B et un canal D de 64Kbs. On doit commander un nombre minimal de canaux, ensuite aucun déplacement n'est nécessaire pour ajouter des canaux. Tout nouvel ajout, se fait depuis le site central.
Le câblage est donc très simple.

Les protocoles de liaison.
Sur le canal B on utilise HDLC LAP-B (Link Access Protocol Balanced). Le B a donné son nom au canal
Sur le canal D , on utilise HDLC LAP-D.
(voir pages suivantes)

Numéris et INTERNET
Pour le raccordement à INTERNET, on utilise principalement le réseau téléphonique et des modems 33.6Kbs voire 57.6Kbs lorsque le fournisseur est sur Numéris. Numéris permet un gain de vitesse certain, cependant sur INTERNET, l'information peut trainer au loin. Il faut conseiller Numéris lorsque l'on transfère beaucoup de documents via la messagerie. En connexion locale INTERNET, RNIS (Numéris) entre en concurrence avec les modems XDSL (http://www.adsl.org) et le câble.

PROTOCOLES DE LIAISONS POINT A POINT

SDLC et HDLC

Historique

IBM créa le protocole Synchronous Data Link Control (SDLC) au milieu des années 70 pour l'utiliser dans son Architecture de réseau SNA (Systems Network Architecture). SDLC a été le premier protocole de liaison synchrone, orienté chaîne de bit. On retrouve dans SDLC une vision très hiérarchisée de l'information, conforme à ce qui se faisait a l'époque. Il faut voir que les terminaux de type écran n'existaient point et que l'on gérait des machines à écrire, des imprimantes, des machines a cartes , des bandes perforées.. Un ordinateur valait plusieurs millions de francs.

Technologie
Il peut être utilisé sur des liaisons en point à point ou en multipoint. Pour réaliser une multipoint, on installe ce que l'on appelle un éclateur de jonction qui va dupliquer le signal de la ligne vers plusieurs extrémités. Pour gérer la cacophonie, SDLC utilise le polling , un peu comme le Token Ring. Chacun parle suivant l'interrogation d'un primaire. Les communications peuvent être half duplex ou full duplex.

SDLC identifie 2 types de noeuds réseau.

- Le Primaire. Contrôle les opérations des autres stations appelées secondaires. Le primaire interroge le secondaire dans un ordre déterminé. Les secondaires transmettent lorsqu'elles ont des données a émettre. Le primaire a la charge d'établir le lien et de le suspendre.
- Secondaire. Sont contrôlés par des primaires. Il agissent sur les ordres des primaires. On trouve par exemple des contrôleurs de terminaux synchrones qui vont gérer les saisies des utilisateurs.

Format de la Trame. Un peu toujours la même cuisine ! !

1	**1 ou 2**	**1 ou 2**	**Variable**	**2**	**1**
Flag	**Adresse**	**Contrôle**	**Donnée**	**FCS**	**Flag**

Protocoles dérivés : HDLC

HDLC partage le format des trames SDLC. HDLC a une option pour rajouter un CRC sur 32 bits. Il est différent de SDLC qui ne supporte qu'un seul mode de transfert (par polling[11]).

- Normal response Mode (NRM). Ca c'est SDLC.
- Asynchronous response mode (ARM). Les secondaires peuvent initialiser la communication.
- Asynchronous balanced mode (ABM) ABM introduit un mode combiné. Le primaire et le secondaire dépend de la situation.

LAPB
IL est connu pour sa présence dans le protocole X25 et le RNIS. En fait , il s'agit ni plus ni moins que de HDLC réduit au mode ABM. La liaison LAPB est établie par soit le DCE (Data Control Equipment) soit par le DCE (Data Terminal Equipment) (Voir schéma en cours). La station qui initie l'appel est le primaire.

[11] Polling veut dire que l'on va interroger successivement , un peu comme un tour de table dans une réunion

Historique

Au milieu des années 80, un besoin se fait sentir pour l'INTERNET d'un protocole de liaison Point à point pour la famille de protocoles TCP/IP. La plupart des sites alors utilisaient des réseaux locaux (LAN) et des réseaux de paquets tels que X25 pour les liaisons longues distances
Bref on inventa SLIP (Serial Line IP Protocole) que l'on abandonna rapidement pour PPP, car ce protocole était incapable de sélectionner de manière facile les adresses IP des extrémités.

PPP devait résoudre
- l'affectation des adresses IP de chaque coté
- marcher sur une liaison de type synchrone (chaîne de bits) ou asynchrone (Orienté caractère avec stop bit et start bit) .
- Etre Multi-protocole
- Capable de tester la qualité de la ligne, détecter les erreurs (un CRC est ajouté)
- Gérer des options de négociations et de compression (Van Jacobson)

Deux familles de protocoles ont étés crées, Link Control Protocol et Network Control Protocol. PPP est maintenant livré sur tout PC ou Mac comme couche de liaison vers un fournisseur INTERNET en utilisant des modems sur le port série.

1	1	1	2	> 1500 octets	2	1
Flag 7E	addr FF	Control 03	Protocole	Information	CRC	Flag 7E

0021	Datagramme IP
C021	Données de contrôle de liaison
8021	Contrôle de réseau

Bien que surveillant les erreurs, les trames invalides sont mises au rebut, juste une statistique de la liaison est mise à jour. C'est donc à la couche du dessus de réémettre. On a pu constater que PPP avait du mal à fonctionner lorsque les protocoles de correction d'erreurs V42bis[12] des modems asynchrones n'étaient pas actifs..
Pour peu que le MTU (voir IP) soit grand, les trames on alors du mal à passer. Sinon avec les contrôles d'erreurs actifs, un MTU de 1500 est tout à fait correct avec les modems V34.

PAP et CHAP ARAP
Ces noms « barbares » sont des méthodes d'identification négociées à l'intérieur du protocole PPP. On envoie comme renseignement un nom utilisateur et un mot de passe.
PAP laisse passer le mot de passe en clair.
CHAP crypte le mot de passe avant de le passer sur le réseau.
ARAP fait la même chose, mais pour le réseau AppleTalk.

PAP et CHAP sont utilisés classiquement pour les accès distants sur Internet pour valider les autorisations.

[12] C'est au niveau du paramétrage des modems, cette option est en principe l'option par défaut

PROTOCOLES DE RESEAU

X25

Réseaux de transmission par paquets

Les secrets du Minitel.
Nous voici là au niveau 3 des couches OSI. X25 est un protocole de transport de l'information complet qui gère le transport de l'information de bout en bout sur de très longues distances avec un plan de numérotation International. On parle de WAN (Wide Area Network), Public Data Network (PDN) ou réseau public de données.
On parle aussi de réseau de **transport par paquet en mode connecté**. **TRANSPAC** est une société de transport de l 'information basée sur X25. X25 a été formalisé complètement sur papier par des autorités internationales (CCITT) et a débouché sur des applications concrètes (ce n'est pas toujours le cas !.cf OSI).
C'est un projet global de téléphonie informatique avec plan de numérotage, opérateurs internationaux, etc.
Pendant les années 80 X25 a été beaucoup utilisé , mais sa complexité le rend mal adapté aux hauts débits, au transport sur fibre optique et il souffre de la concurrence de ATM et de Frame Relay.
Des réseaux nationaux utilisent X25 pour le transport des données informatiques. TRANSPAC en France est l'opérateur national. Celui-ci facture le service comme pour le téléphone et l'on est facturé à la durée de la connexion et aussi au nombres de paquets X25 transportés (mais pas à la distance sauf international).
Les services 3613,14,15,16,17,21 sont des points d'entrées de ce réseau.

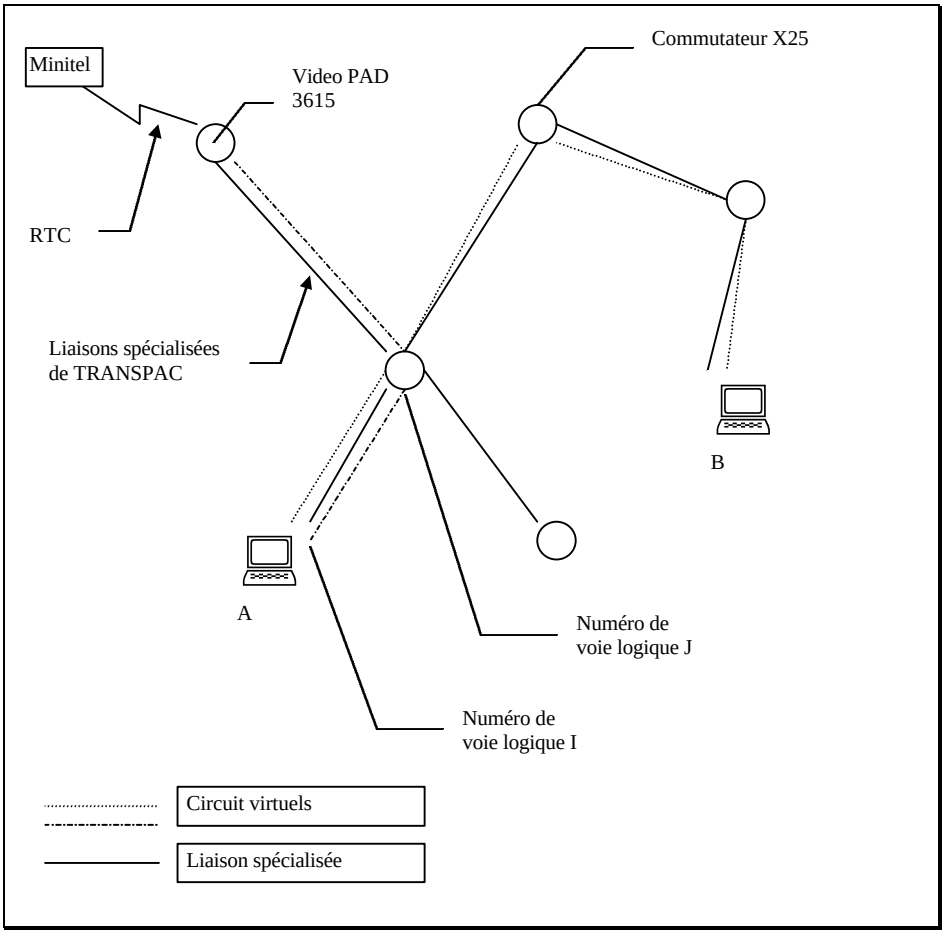
Technologie
X25 défini donc un réseau téléphonique pour ordinateur. L'ordinateur compose un numéro qui va appeler un autre ordinateur. L'appelé peut refuser la communication , accepter du PCV reconnaître l'adresse de l'appelant, lire des données complémentaires du paquet d'appel. De manière classique, on défini deux types de machines, les DTE et les DCE. Le DTE est un terminal ou un ordinateur, alors que le DCE est un modem, un commutateur X25.
Bref, Dans X25 le DTE initie un appel via un numéro (175xxxxx pour paris..). Le réseau route ce paquet d'appel et crée ce que l'on appelle un Circuit Virtuel. Ce protocole est orienté connexion, c'est à dire que tout les équipements le long de la ligne vont garder la mémoire de ce chemin et réserver des ressources (mémoire sous forme de buffers et de files d'attente). Ce système permet une connexion avec un temps de réponse garanti, un contrôle d'erreur au niveau de chaque liaison.
Autre avantage, les paquets ne transmettent pas l'adresse du destinataire une fois le CV effectué. Seuls des numéros de voies logiques sont transmis entre le point d'appel et le premier commutateur.
Par contre dès qu'une ligne a un incident, le CV est coupé, les sessions sont perdues. Il faut se reconnecter. Ce n'est pas le cas pour TCP/IP.

Chaque liaison entre commutateurs X25 est basée sur les trames de niveau 2 HDLC/LAPB. Chaque commutateur ne peut supporter qu'un nombre restreint de CVs (Circuit Virtuels) et ceci même si les liaisons ne véhiculent pas de données.
Grâce à un plan de numérotage de type téléphonique, et donc prédictif, les commutateurs n'ont pas besoin de protocoles de routage complexe. Si c'est du 134, on va sur le commutateur du département de l'Hérault.
Les paquets ont une longueur de 256 octets

1= une machine interne
0= international
3 =kiosque minitel.. En fait avec quelques centaines d'adresses, le commutateur peut travailler de manière autonome.

Le DTE type terminal inintelligent (Minitel) est connecté au réseau public par l'intermédiaire d'un PAD (Assembleur, Désassembleur de paquets). Le PAD qui gère l'accès kiosque va générer un numéro TRANSPAC à la place d'un mnémonique (METEO= un numéro du type 175..) Ce PAD établit le CV qui va joindre la machine de destination et la connexion s'établit ensuite. Le minitel lui n'a aucune notion ni de X25, ni du protocole de liaison, il établit une liaison asynchrone à l'aide d'un modem interne 1200/75 Bits/secs (V23) sur l'une des entrées du PAD ou du VidéoPAD . Celui ci agit comme un concentrateur de terminaux asynchrones qui gère en sortie le protocole X25.

L'affichage du Minitel est géré par l'ordinateur distant. Le VidéoPAD gère lui la saisie de l'appel. Par exemple, il va transformer la saisie de METEO par le numéro TRANSPAC du serveur de la METEO.
Chaque fois que les touches SUITE ENVOI ANNULATION GUIDE SOMMAIRE sont tapées, le VidéoPAD envoie la ligne tapée vers le serveur. Celui-ci en retour envoie des ordres semi-graphiques pour redessiner l'écran.



X25 est complexe car il mélange à la fois des problèmes de réseau (router l'information) et des problèmes de transport. Par rapport aux couches TCP/IP, on pourrait dire que X25, c'est IP+TCP+OSPF+ICMP
Bref c'est du niveau 3++.
Avec ATM ce sera pire, car ATM se préoccupe d'être universel et veut aussi gérer les réseaux locaux, la téléphonie, la vidéo. X25 n'a jamais eu cette prétention pour la bonne raison qu'à cette époque, les réseaux locaux n'existaient pas . X25 a été normalisé entre 1981 et 1984.

Transpac services et évolutions
offre des liaisons CV à 64 kb/s puis des liaisons virtuelles réservées à 256 Kb/s (91) puis 2Mb/s (93).
Le service LVR sert à interconnecter des réseaux locaux.
La taille du paquet X25 va évoluer vers 1024 puis 2048 octets
Un service de type Frame Relay est proposé.

FRAME RELAY
ou Relais de Trame.

Ce protocole connaît un certain succès aux US , et semble proposé comme une alternative au tout nouveau protocole ATM (Asynchronous Transfer Method). En fait il est de la famille des modes de transport par paquets avec Circuit virtuel.

Même famille que X25. Mais comme on peut le voir, Frame Relay est beaucoup plus proche des trames niveau 2. En fait les architectes du projet en 1984 ont trouvé X25 trop lourd, pas assez performant, passant son temps a contrôler les erreurs et les corriger, et à gérer du contrôle de flux . Pour Frame Relay, les lignes étant de moins en moins bruitées, la technologie aidant, on peut se passer de certains contrôles qui de toute façon vont être refaits par les ordinateurs. Un simple contrôle d'erreur est fait par un CRC et la trame qui n'est pas valide est mise à la poubelle. Elle n'est pas retransmise en interne comme dans le cas de X25.

En cas de congestion, le noeud du réseau renvoie à la source une notification de congestion.

Le réseau français TRANSPAC utilise Frame Relay comme protocole de base pour son service INTERNET.

ATM
Asynchronous Transfer Method

Cette technologie est présentée depuis quelques années comme la technologie du futur. Ce sera au marché de juger.. Pour l'instant cette technique risque de se trouver reléguée à la fourniture des gros opérateurs.
Car le 100 BaseT commuté ainsi que le GigaBit ETHERNET risquent de satisfaire bon nombre de clients informatiques qui n'ont que faire du transport de la voix ou de la vidéo. Le marché en terme de ventes risque de s'en ressentir. ETHERNET a encore de beaux jours devant lui.
Il est vrai que les deux ne peuvent se comparer car ETHERNET c'est du niveau 1 et 2 alors que ATM c'est presque tous les niveaux à lui tout seul.

Historique.

- On a vu que Numéris (ISDN) est une impasse technologique (bande passante fixe et déjà faible..).
- ETHERNET ne garantit pas la bande passante et reste spécialisé à un réseau local

Ou se situe ATM ?. C'est une technologie de compromis cherchant à satisfaire à la fois les besoins en vidéo ,en son et en données informatiques. La base de ATM, c'est le soucis de la voix.
Comme on a vu avec Numéris, il faut échantillonner la voix. Si on laisse passer les sons de 0 à 4000 Hz, on doit échantillonner au double, c'est à dire 8000 Hz, on a donc l'obligation d'émettre un octet d'échantillonnage toutes les 125 µsec (1 sec / 8000). On peut se permettre une certaine mise en mémoire des informations, celle-ci ne partent pas tout de suite, on attend de remplir une cellule ATM.
La taille de la cellule ATM est un compromis entre Américains et Européens. Les uns voulant 64 octets de donées les autres 32 octets. Du coup la trame ATM que l'on appelle cellule (vu la petite taille) a une longueur de 48 octets + 5 octets d'en-tête soit **53** octets
Pour remplir ces 48 octets, il faut 48 * 1/8 ms = 6msec.
Pour les remettre dans le combiné distant, il faut aussi 6 msec.

Le délai de propagation (indépendant de la vitesse d'émission) doit rester inférieur à 28msec pour des problèmes d'échos ,.. Il reste donc 28-12= 16msec soit à 200 000 kms/sec 3200 kms. Cette distance pouvant être adaptée si on met des équipements intermédiaires[13] . C'est pour éviter ces équipements que les européens voulaient 32 octets au lieu de 64 pour les américains.
Voilà pour la base historique et le pourquoi de la taille de cellule. ATM est un mode connecté avec circuit virtuel, sans reprise sur erreur, un peu comme Frame Relay.
Il est évident que sur 5 octets, on ne va pas transporter des adresses à la mode IP sur 4 octets et bientôt 16 octets !. Le CV est donc un impératif et le découpage des trames en cellule inévitable.

Les vitesses de transmission normalisées
25 Mbs
155 Mbs
650 Mbs

Pourquoi asynchrone ?.
Contrairement à Numéris (ISDN) ou le canal B2 suit le canal B1, les cellules se suivent dans le désordre.

Synchrone Numéris. Déterministe, donc pas besoin d'en-tête

Canal D	CanalB1	Canal B2	Canal D	Canal B1	Canal B2

Asynchrone ATM

H	CV1	H	CV1	H	CV2	H	CV2	H	CV2	H	CV3

H est un en-tete, le mode synchrone n'en a pas besoin car on sait temporellement quelle information va arriver. L'asynchrone malgré ce tribut à l'en-tête offre plus de souplesse.

[13] Le tout fibre changerait pas mal de choses. 1/3 plus rapide, pas de bruit.

La trame ATM

5	48[14]
En-tête	Données

En-tête UNI (Client vers réseau)

4	8	4	12	3	1	8
GFC	VPI	VPI/VCI	VCI	PT	CLP	HEC

En-tête NNI (Réseau vers réseau 2 noeuds du réseau)

12	16	3	1	8
VPI	VCI	PT	CLP	HEC

GFC = Generic Flow Control
VCI = Virtual Channel Identifier = Numéro de circuit virtuel
VPI = Virtual Path Identifier = Numéro de chemin virtuel (par ex Paris / Toronto)
PT = PayLoad Type utilisé pour la gestion du réseau
CLP = Cell Loss Priority (Donnée en surnombre, peut être perdue)
HEC = CRC basé sur $x^8 + x^2 + x + 1$. Décodé dans la silice des cartes.
Le long du réseau on ne connaît que des VP, les VC ne sont connus que sur les extrémités

Le contrôle de Flux

Sur ATM ce n'est pas rien car il va falloir desservir à la fois des flux à bande passante garantie et des flux non garantis. Le commutateur devra scruter certains CV de manière fixe et garantie et les autres s'il lui reste du temps pour cela. Les octets envoyés sans garantie de bande passante pourront être détruit ailleurs dans le réseau (bit CLP), si besoin s'en fait sentir. La notion de réservation de bande passante, ce n'est pas de la tarte dés que l'on travaille en coopération. IP n'en fait pas (tout du moins en V4). Tout le monde est égal et bien souvent, tout le monde attend, en tout cas pour l'administrateur c'est plus simple ! !. [15]
Dans la littérature, on parle de constant bit rate (CBR) ou variable bit rate (VBR).

Le format des données.
ATM forum a normalisé 5 couches (ATM Adaptation Layer)
certaines sont devenues obsolètes. On retient principalement
AAL1 transmission de vidéo et son On ajoute dans les données un numéro de séquence sur 4 bit et une détection d'erreur sur la séquence de 4bits
AAL5 permet le transport de blocs d'informations jusqu'à 64Ko. Les huit derniers octets de la dernière cellule comprennent un indicateur de longueur sur 16 bits et un code correcteur sur 32 bits.
Ces couches permettent la fragmentation et le réassemblage des trames de plus haut niveau comme IP. Heureusement pour IP le MTU sur ATM n'est pas de 48 octets. Le MTU est défini plus loin.

L'adaptation aux réseaux locaux
Le problème se pose car le broadcast ne marche pas avec ATM . ATM étant un protocole de point à point. Or la plupart des protocoles de réseaux locaux (LAN) utilisent le broadcast. ATM Forum a normalisé une méthode qui s'appelle LAN Emulation.
Des serveurs permettent de se raccorder à un réseau virtuel (on s'enregistre dans le VLAN). Ce sont des LAN Emulation Servers. Ils permettent la résolution des adresses. (arp)
D'autres les BUS assurent les fonctions de gestion des broadcasts .
Tout ça est assez neuf et va évoluer rapidement. Les solutions risquent de changer aussi rapidement

[14] Pour les données informatiques, 2 octets en en-tete plus deux en fin (44 utiles donc)
[15] Dis , j'ai un cours, tu peux pas me donner 2mbs de bande passante pendant une heure ?.

LES

TECHNOLOGIES IP

INTERNET PROTOCOL

LES TECHNOLOGIES IP

Historique

A la fin des années 60 fut créé le réseau ARPANET par l'agence des projets de recherche avancés du département de la défense (l'ARPA) aux Etats Unix , qui interconnectait quelques ordinateurs de centres de recherche et d'universités. Dans les années 1980, le réseau fut divisé en deux parties: Milnet pour le trafic réservé au gouvernement et à l'armée, et NSFNet (National Science Foundation) pour le trafic entre universités qui grandit progressivement au cours des années 80.
Aujourd'hui la croissance est explosive, l'essentiel de l'armature du réseau est toujours assuré par la NSFNet. La coordination internationale est assuré par l'IAB (INTERNET Association Board) et ses deux bureaux l'IETF (INTERNET Engeneering Task Force) et l'IRTF (INTERNET Research Task Force)

Le langage réseau de l'INTERNET
Le langage adopté dans l'INTERNET pour communiquer entre machines est le langage réseau **TCP-IP**. C'est un protocole très novateur dans le sens ou il est faiblement hiérarchisé. Tous les ordinateurs sont égaux dans leur possibilités. Le langage TCP-IP est très répandu dans le monde des systèmes Unix et il est très facile de trouver des sources pour réaliser un support TCP-IP sur n'importe quel système. TCP-IP est de fait le premier véritable langage réseau indépendant de tout constructeur d'informatique, ce qui en fait son succès.
Cependant, Il faut distinguer les protocoles c'est à dire les 'langages de réseau' et les entités administratives. En effet si un réseau parle 'TCP-IP', il n'est pas forcément connecté à l'INTERNET. Ce n'est pas parce que je parle français que je suis français..
Le réseau INTERNET est en fait une fédération de réseaux qui mettent en place une organisation commune. Cette organisation est très fédérale. Parmi les entités de l'INTERNET on va trouver une multitude de sous réseau sous les appellations suivantes:
NSF
NASA
RENATER
FNET
EBONE
R3T2
....
Chaque réseau a des règles de raccordement et des tarifs qui lui sont propres. Les différents adhérents suivent des règles propres à leur réseau. Pour donner un exemple, prenons le cas de RENATER et de R3T2.

RENATER
C'est un GIP (Groupement d'intérêt Public) qui regroupe différents bailleurs de fonds et essentiellement des organismes liés à la recherche. On y trouve le MEN[16], le CNRS, le CEA, EDF,INRIA,IFREMER...
Les fonds apportés permettent de payer les salaires de permanents mais principalement, le coût des liaisons spécialisées. Avant RENATER le MEN payait un certain nombre de liaisons spécialisées souvent dupliquées pour faire passer des protocoles différents (Le SNA d'IBM ou le DecNet...). La volonté a été de ne plus payer que pour des Liaisons rapides supportant le protocole TCP-IP.
RENATER finance donc les interconnexions de plaques régionales et internationales et ne fait passer sur son réseau que les 'gens' habilités c'est à dire ceux qui participent au GIP.

R3T2
C'est le réseau régional PACA et un certain nombre de sites (dont le nôtre) ont été équipés de prises R3T2. On peut imaginer que certains sites soient équipés de prises R3T2 mais n'aient pas l'agrément RENATER. Par cela, il ne pourront pas sortir de la région via RENATER. (http://www.RENATER.fr)
L'Agent Opérateur de ces 2 réseaux est France Télécom. C'est lui qui connecte les sites gère les tables de routage et les incidents. La situation est variable selon les réseaux. Certains sont gérés directement par les utilisateurs.

[16] Ministère de l'Education Nationale

L'ADRESSAGE IP

Le principe de base d'un réseau IP

IP est un réseau de transport de paquets en mode non fiable et non connecté. C'est à dire que le paquet peut être perdu dans le réseau, arriver dans le désordre voire en double. La fiabilité n'est assurée que par les couches de transport qui sont dans les ordinateurs d'extrémité. Les éléments intermédiaires du réseau sont des routeurs IP qui vont servir d'aiguillage. Un routeur peut être arrêté sans que les liaisons passant par ce routeur en soit perturbées. Le réseau se reconfigure et les paquets seront acheminés par d'autres chemins.
Rien ne garantit non plus que les paquets vont prendre le même chemin . On pourrait comparer cela au réseau postal. Deux enveloppes ne passeront pas forcément par le même centre de tri, et n'arriveront pas forcément en même temps.
On appelle datagramme le paquet élémentaire. Celui-ci comme une enveloppe de courrier comprend une adresse de destination et une adresse de départ. Derrière les routeurs, on trouve des réseaux locaux, des liaisons spécialisées.

L'ADRESSE IP
L'adresse IP est constituée de 32 bits , soit 4 octets notés de façon décimale de 0 à 255, par ex 193.50.125.2. Une adresse est affectée non pas à une machine mais à une interface d'une machine. Celle-ci peut donc avoir plusieurs adresses. L'adresse se décompose en 2 parties, une partie réseau et une partie machine. Cet adressage n'est pas hiérarchisé dans le sens que 193.50.126.0 pourrait être un réseau japonais, alors que 193.50.125.0 serait un réseau français. C'est la très grosse faiblesse de cet adressage. Le successeur (IP V6) prévoit des hiérarchies d'adresses à la manière du téléphone.
Chaque machine a une ou plusieurs adresses. Elle a obligatoirement une adresse IP par carte réseau. Elle peut aussi avoir plusieurs adresses sur une seule carte (IP ALIASING). C'est le cas des machines hébergeant plusieurs sites WEB.

LES DIFFERENTES CLASSES D'ADRESSES INTERNET
Pour des raisons administratives et de routage, on regroupe ces adresses sous forme de classes. On pourra ensuite utiliser ces adresses à sa guise pour gérer son réseau. Ces adresses sont demandées auprès du NIC[17] (Network Information Center). Le NIC France (l'INRIA[18]) délègue la fourniture des adresses aux grands fournisseurs d'accès au réseau. Dans le cas de nos universités, toute nouvelle adresse doit être demandée à RENATER, organisme qui s'occupe du réseau de la recherche.
RENATER a plusieurs réseaux de classe B et des blocs d'adresses de classe C, qu'il va morceler en sous réseaux pour ses utilisateurs. RENATER sera donc responsable du routage de l'ensemble des classes B et classes C qui lui ont été attribués. Le détail de ce qui sera fait dans la classe B sera invisible de l'extérieur.

En principe l'adressage comprend donc 256**4 adresses c-a-d : 4294967296 adresses (4 Milliards). En fait, on va voir qu'il y a beaucoup de pertes et que cet adressage est au bord de la saturation.
Les adresses sont regroupées en différentes classes pour des raisons d'administration et de routage. La partie machine est réservée à l'usage du gestionnaire du réseau qui peut redécouper cette partie, c'est à dire « subnetter ».

- Le réseau de classe **A**. Il peut contenir beaucoup de machines car l'adresse est sur 7 bits L'adresse du réseau est donc sur un octet dont la valeur la plus grande est un zéro par conséquent le premier chiffre sera inférieur à 128. Le classe A démarre à 0 jusqu'à 127

0	Réseau	Machine	Machine	Machine

- Le Classe **B**: adresse sur 14 bits: commence à 128

[17] NIC http://www.nic.fr ou le fournisseur d'accès.
[18] INRIA, Institut National pour la Recherche en Informatique et Automatismes. (Un pionnier français du réseau INTERNET et des systèmes Unix).

10	Réseau	Réseau	Machine	

- Le Classe **C** , le plus utilisé en ce moment, dû à la disparition des classes B devenues indisponibles par suite de manque d'adresses. Démarre donc à l'adresse 192

110	Réseau	Réseau	Réseau	Machine

- Le Classe **D** est utilisé pour des groupes de multicast Commence à 224

1110	Réseau	Réseau	Réseau	Machine

- Le Classe **E** réservé pour usage futur, commence à 240

1111	Réseau	Réseau	Réseau	Machine

Le Sous adressage ou subnetting ,exemple du classe B .
Classe B normal

01	Réseau	Réseau	Machine	Machine

Classe B après sous adressage : Ce classe B est décomposé en sous réseaux de 256 machines.

01	Réseau	Réseau	Réseau	Machine

Pour le Classe A 34.0.0.0 , on peut décomposer des réseaux de différentes manières, en précisant une information que l'on appelle masque de sous réseau ou Subnet Mask

Si 34.0.0.0 veut décomposer en beaucoup de sous réseaux, de 256 machines, il va prendre un subnet mask de 255.255.255.0 . Pour décomposer en réseau de 256*256 machines , on va alors avoir un masque de 255.255.0.0.

Cette information concerne, les routeurs et les machines du réseau. Elle définit ainsi la famille de la machine. Le subnet, veut dire que la machine appartenant a un réseau de type 255.255.0.0 pourra adresser directement 256*256 machines sans passer par un routeur.

Evidemment des réseaux aussi larges sont rares car 256*256 machines sur le même réseau physique, ca fait beaucoup de bruit. Cette information est utile pour les mécanismes de diffusion, lorsque l'on veut faire un broadcast IP, on va mettre à un les bits machines pour indiquer que cette information concerne toutes les machines de ce réseau.

Pour conclure, un réseau ou subnet au sens IP constitue un groupe de machines et une information de routage et de diffusion (broadcast)
Il faut noter qu'il n'y a rien d'incompatible à avoir sur le même support physique (ETHERNET) deux réseaux IP. Les machines pour communiquer devront soit avoir deux interfaces, soit passer par un routeur bien qu'étant sur le même câble.[19]

Le réseau **127.0.0.0**
Celui ci est particulier, il est réservé pour l'usage local de la machine. On appelle ça, la loopback adresse ou adresse de bouclage. 127.0.0.1 est l'adresse locale de la machine et ne doit jamais sortir sur le réseau. Ceci permet de faire des tests en local sans sortir sur le réseau, ou d'appeler des services en mode TCP/IP alors qu'ils sont dans la même machine. On accède alors aucun réseau physique.

Les faiblesses de l'adressage IP
On voit de tout ceci que bien qu'étant très simple à la base, le laxisme de la définition initiale de IP entraîne un vrai casse-tête pour les administrateurs, au niveau des réseaux internes et au niveau des routeurs.
Il faut changer les adresses lorsque l'on déplace une machine. C'est compliqué et délicat pour un utilisateur non averti.[20]

[19] C'est un peu tordu, mais en matière de réseau, on voit de tout. Ca ne peut avoir de sens que si l'ETHERNET est commuté (avis personnel).
[20] BOOTP et DHCP simplifient ce genre de choses. Ils distribuent l'adresse en dynamique.

En effet si on a un classe C, on est limité à 256 adresses, moins adresse 255 moins adresse du routeur. Si le réseau dépasse 254 machines, il faut donc faire du routage, séparer les réseaux physiques, compliquer les déclarations de routage. Comment router appletalk, novell etc..

Exemple de sous adressage d'un réseau de classe C.
On veut découper un réseau de classe C en sous réseaux de 32 machines. De 0 à 31 nous avons 32 possibilités. 31 s'écrit en binaire : 11111 (5 bits).
Si l'on admet, cas courant que l'adresse du réseau est dans les 3 bits restants à gauche (les trois de poids fort), nous avons huit sous réseaux. Le masque représente la partie réseau, soit les bits 6,7,8. Le 6ème vaut 32, le 7ème 64, le 8ème 128. Le masque s'écrit avec tout ces bits à un, soit : 32+64+128=224.
Le masque du sous réseau sera donc 255.255.255.224. Cette précieuse information sera à fournir au routeur et dans la configuration des machines du réseau.

```
193.50.126.97      11000001.00110010.01111110.01100001
Masque             11111111.11111111.11111111.11100000
```

Les 8 réseaux possibles seront donc:
000 = **0** 001=**32** 010=**64** 011=**96** 100=**128** 101=**160** 110=**192** 111=**224**

Pour un routeur la machine d'adresse 100 appartiendra au réseau X.X.X.96 masque 255.255.255.224
Ce routeur aura des routes du style

interface ETHERNET 0
route X.X.X.96 255.255.255.224
interface ETHERNET 1
route X.X.X.32 255.255.255.224

Pour la machine 100, son masque sera 255.255.255.224 et son routeur aura comme adresse, une adresse comprise entre 96 et 126 (pas 127 car 127 sera l'adresse de broadcast de ce sous réseau). Un masque pour un réseau de classe C ne pourra pas être 255.255.0.0 , inférieur à la partie réseau officielle (255.255.255.0)

LES ROUTAGES
Au niveau des routeurs de l'interconnexion INTERNET, chaque réseau entraîne une consommation mémoire dans les routeurs et des temps de transferts pour les mises à jour des tables de routage. Si toutes les adresses sont distribuées, on consomme dans les routeurs 128 adresses de classe A, 64 * 256 adresses de classe B et 32 * 256 * 256 de classes C soit plus de 2 millions d'entrées.
Un entrée dans le routeur, c'est au minimum deux adresses IP, un coût, une date de mise à jour et donc au minimum 12 octets. En tout et au minimum , il faudra compter 24 Mo de mémoire dans le routeur, sans compter le temps de rafraîchissement des informations qui vont contribuer à diminuer la bande passante.

CIDR
Pour ces raisons l'INTERNET s'oriente vers un routage **CIDR** (ClassLess InterDomain Routing) . c'est à dire sans classes de numéros mais en utilisant une **agrégation** de numéros de réseaux lié à un système autonome . On verra cela plus tard dans les routages extérieurs. On préfère dire de 193.20 à 194.12 envoyez ces réseaux vers RENATER .

IPV6
Dans les prochaines années IPV4 deviendra IPV6 et on passera à des adresses de 128 bits.
Beaucoup de choses vont évoluer en même temps que l'adressage.
Voir pour cela la page de l'UREC[21] http://www.urec.fr/IPng/

A retenir :
Le masque sert à reconnaître pour quelles adresses on doit passer par un routeur pour communiquer.
Les adresses ne sont pas isolées mais regroupées par classes (comme le téléphone)

[21] Unité de Réseau du CNRS. Une foule de renseignements sur les réseaux

BROADCASTING et MULTICASTING

Il existe dans les réseaux trois types d'adresses, les adresses locales, les adresses de broadcast, les adresses multicast.

Pour résumer
1. Je parle directement à quelqu'un (unicast)
2. Je parle à tout le monde (broadcast)
3. Je parle à un groupe restreint (multicast)

TCP/IP gère ainsi que ETHERNET ces différent types d'adresses. On verra que ARP est un broadcast ETHERNET, RIP est un broadcast IP/UDP qui sera convertit en broadcast ETHERNET, si ETHERNET est la couche de liaison.

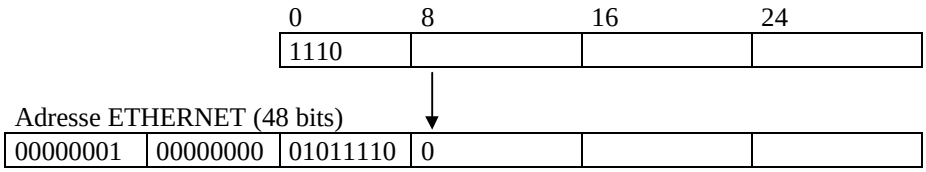
Pour TCP/IP l'adresse de broadcast consiste à mettre les bits de l'adresse machine à un. Si 193.50.125.0 est mon réseau, 193.50.125.255 sera l'adresse de broadcast IP. Suivant comment est décomposé le réseau, la partie finale ne sera pas forcément 255. Par contre pour un réseau de classe C non subnetté, ce sera toujours le cas.
Heureusement ping 255.255.255.255 ne génère pas un broadcast à l'ensemble de l'INTERNET.
Un routeur ne laisse jamais passer les broadcasts de niveau 2. Par contre il peut laisser passer les broadcastde niveau 3 (adressage IP). A priori, il n'y a aucune raison de le faire. Ce genre de chose se voit par malveillance ou mauvaise installation (par ex NT4.0 propose des masques de classe B par défaut..). Il faut filtrer ces broadcast IP au niveau des routeurs.

Typiquement le multicast est utilisé pour transmettre des conférences sur l'INTERNET.
Pour IP les adresses de multicast vont de 224.0.0.0 à 239.0.0.0
Le RFC Assigned Numbers a déjà alloué certaines adresses
- 224.0.0.1 signifie tous les systèmes de ce sous réseau
- 224.0.0.2 tous les routeurs de ce sous réseau
- 224.0.1.1 est réservée à NTP Network Time Protocol
- 224.0.0.9 RIP-2

Adresse de broadcast sur ETHERNET
FF :FF :FF :FF :FF :FF

adresses de multicast sur ETHERNET
le premier octet de l'adresse contient la valeur 01 et les adresses du multicast IP vont de
01 :00 :5E :00 :00 :00 et 01 :00 :5E :7F :FF :FF
Transformation d'une adresse de multicast IP en adresse ETHERNET

Adresse IP de classe D



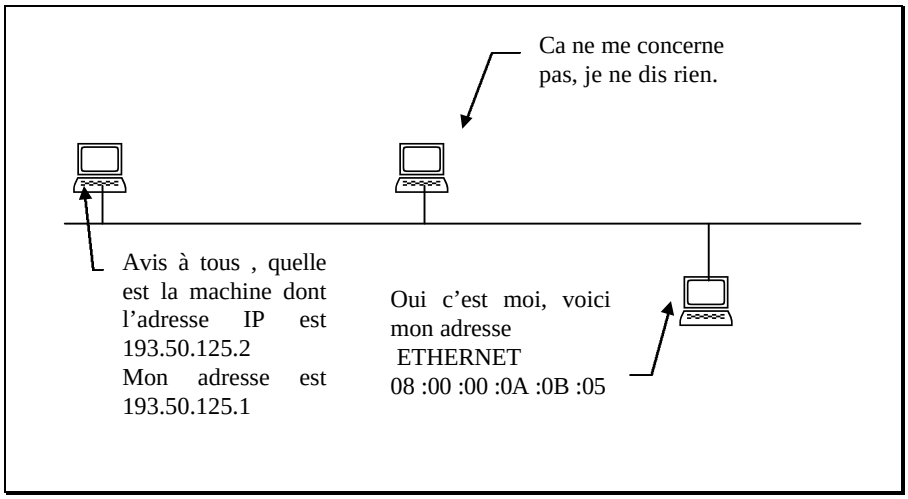
On prend les 23 derniers bits de l'adresse. La transformation étant non bijective, la couche IP devra filtrer une partie de ce qui lui arrive.

Comment ca marche ?.
Lorsqu'une application utilise une adresse multicast, IP va générer l'adresse ETHERNET en remplissant les 23 derniers bits de l'adresse IP
Le Multicast est utilisé pour des applications comme les conférences sur INTERNET (MBONE). Le routeur local devient routeur de multicast IGMP. Les stations s'abonnent à un réseau multicast IP particulier auprès

du routeur. Ce routeur aura été ajouté dans les membres de la conférence. Chaque machine connectée pourra alors recevoir les informations.

ARP ou Address Resolution Protocol *Résolution d'adresses* et RARP Reverse Address Resolution Protocol

Au niveau ISO, ce serait la couche 2.99 , en fait la jonction entre la couche liaison et la couche réseau. Dans un cas très classique, comment faire le lien entre les adresses ETHERNET et les adresses IP ?. C'est le rôle de ARP.



Pour parvenir à avertir tout le monde, au niveau ETHERNET, on utilise comme adresse de destination, une adresse de diffusion. Comme cela, toutes les machines lisent la trame, et celle qui a la bonne adresse répond. Evidemment, si la machine est arrêtée, aucune réponse n'arrivera.

Il se peut aussi qu'une autre machine ait pris cette adresse. A ce moment là, c'est la plus rapide qui sera enregistrée. Ceci peut arriver, si les deux ordinateurs ont été configurés par une copie de disquette.
Ou si quelqu'un essaye de pirater le réseau en se faisant passer pour un autre !. Il existe une commande qui s'appelle arp et qui donne la correspondance numéro IP , numéro ETHERNET

arp -a

Cette commande existe sous Unix , Windows95 et NT.

ARP correspond a un numéro de service bien particulier (**806**) dans la trame ETHERNET. Cette technique ne s'applique pas que pour IP. Dans la trame ARP, est indiqué le type du protocole.
On pourrait se dire aussi, pourquoi ne pas diffuser les données. Ceci est beaucoup trop coûteux. En effet toutes les machines seront interrompues pour lire la trame, les ponts et les commutateurs devront tout laisser passer..

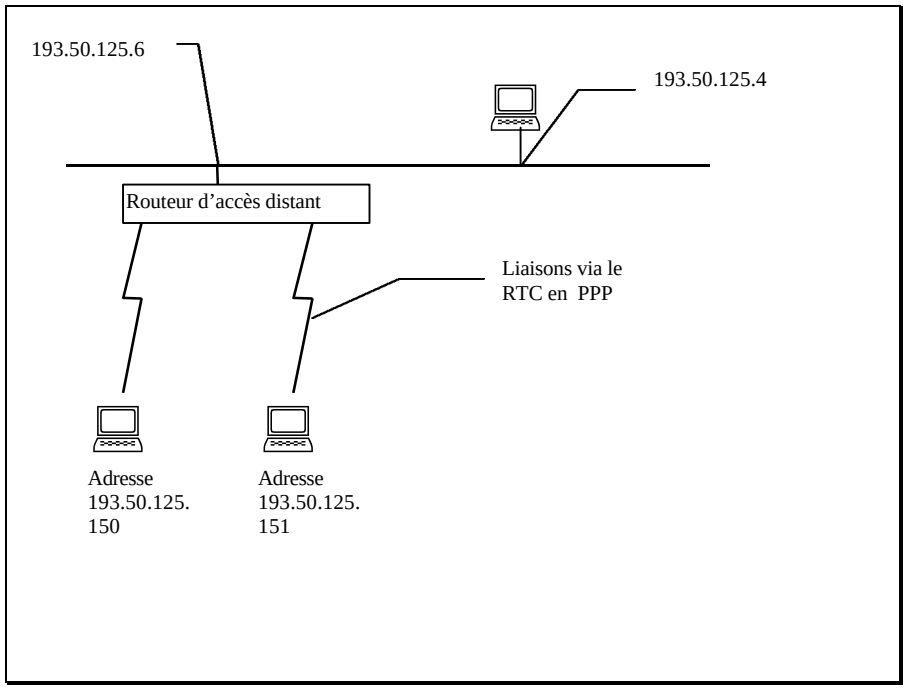
Cache et Timeout
Une fois cette résolution obtenue, l'adresse est mise dans un cache en mémoire, celui ci peut être effacé par la commande ***arp -d*** . (Cas où un serveur du réseau vient d'avoir sa carte changée).
Ce cache doit être rafraîchi périodiquement, une machine inactive (pas de paquets reçus depuis un certain temps) est retirée de ce cache, ceci arrive entre 10 et 20 minutes selon les systèmes. Il est possible de rentrer de manière statique l'adresse d'une machine, a des fins de sécurité, par exemple entre un routeur et des serveurs du réseau (***arp -s***) .
Les machines ayant fait la résolution vont transmettre les paquets avec l'adresse ETHERNET (MAC) de la machine a contacter. Dans le champ service de la trame ETHERNET, nous aurons la valeur **800** qui correspond aux trames de service IP.

Le ARP gratuit
Certains systèmes d'exploitation ont un comportement des plus curieux. En fait , ils font une requête ARP en demandant leur propre adresse IP.
En fait ceci permet de détecter si une autre machine n'aurait pas la même adresse, ce qui nuirait au fonctionnement normal de la machine. On est averti de suite qu'une machine a la même adresse.

RARP
C'est arp à l'envers, la machine diffuse (broadcast) une trame ETHERNET pour demander sa propre adresse IP. Un serveur va lui renvoyer son adresse dans une trame ETHERNET parfaitement définie (service **8035**). C'est utilisé pour des machines n'ayant pas de disque dur, serveurs de terminaux... Cependant, comme nous le verrons, l'adresse IP est insuffisante pour travailler sur un vaste réseau où nous devons définir l'adresse de la passerelle, des serveurs de noms, etc. RARP est donc abandonné au profit de BOOTP et dernièrement de DHCP qui assument ce genre de fonction de manière beaucoup plus évoluée.

Proxy ARP
Une machine peut utiliser ARP pour faire du routage transparent. Cette machine fera la correspondance entre l'adresse reçue et l'interface sur laquelle elle achemine l'information.
C'est le cas par exemple pour un routeur d'accès distant.

Proxy arp



On peut se demander qu'elle est la différence entre le routage et proxy arp. En fait la machine qui appelle (193.50.125.4) a l'impression que 150 et 151 sont sur son réseau. En quelque sorte proxy arp , c'est du routage transparent. On voit parfois les termes de IP forwarding qui correspondent à cette technique. Derrière le routeur, on peut avoir un réseau non vu de l'extérieur dont seul le routeur a connaissance. On réalise d'une certaine façon un déport d'adresse.

Le DATAGRAMME[22] IP *Réseau*

Un service de remise de paquets en mode non connecté

L'INTERNET s'appuie sur un protocole (IP ou INTERNET PROTOCOL) qui est un service de remise de paquets non fiable. La remise du paquet s'effectue sans garantie de remise mais un message ICMP « doit » signaler la suppression du paquet[23], ces paquets peuvent suivre des routes différentes, être dupliqués, arriver dans le désordre[24].

Structure des datagrammes :

0	4	8	16	24	32
VERS	LGMAT	Type Service	Longueur Totale		
Identification			Drap	Déplacement Fragment	
Durée de Vie (TTL)		Protocole	Total de Contrôle en-tête		
ADRESSE IP SOURCE					
ADRESSE IP DESTINATION					
Options IP Eventuelles				Bourrage	
Données					

Signification :
VERS= numéro de version. En ce moment IPV4 bientôt IPV6
LGMAT= longueur d'en-tête en mots de 32 bits. Généralement, 20 octets = 160 bits=5*32bits
LGMAT vaut 5 la plupart du temps
Type de service codé sur 8 bits

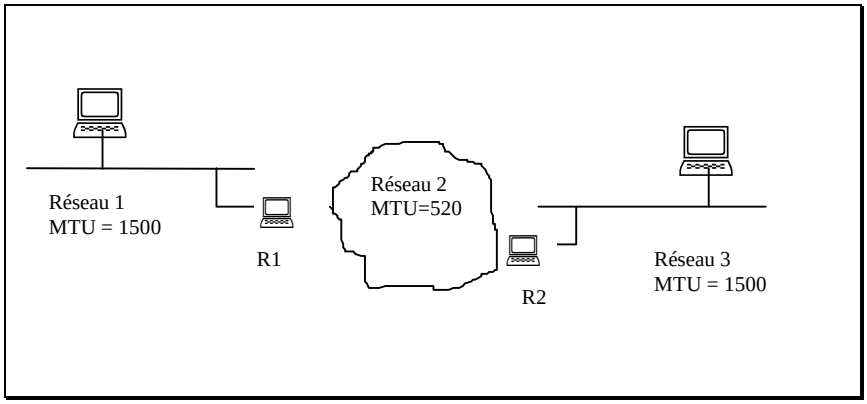
0	3	4	5	6 7
Priorité	D	T	R	Inutilisé

Priorité 0 (cas normal), 7 supervision réseau
DTR, représente le type d'acheminement :
D requiert un délai court (style éviter un satellite)
T débit élevé
R grande fiabilité
Longueur Totale = longueur en octets du datagramme, en-tête plus données
Déplacement fragment, voir plus loin
Durée de vie : compteur que l'on décrémente a chaque passage de passerelle, si il atteint zéro, le message est détruit, et un ICMP est envoyé à la source.
Protocole : Comme pour ETHERNET ou IP vaut 800, ici on indique le type de données , à ce niveau, il s'agit de ICMP, UDP, TCP, EGP. L'explication de ces valeurs viendra plus tard.
Total de contrôle : C'est une valeur permettant de vérifier l'intégrité de l'en-tête
Options , souvent utilisées pour la supervision du réseau : pour résumer, on trouve :
Enregistrement de route
Routage défini par la source. (avec retour des temps de passage)
Horodatage
DO NOT FRAGMENT

A retenir : sont particulièrement importants :
Adresse Source | Adresse Destination | Type de Service | TTL

[22] Dans la terminologie IP , on parle de datagramme qui n'est ni plus ni moins qu'un paquet. Au niveau liaison on parle de trame. Tout ceci est tout de même équivalent. En X25, on ne parle que de paquet.
[23] Sauf s'il est dans un routeur qui vient de s'arrêter, comme on n'est pas dans un mode connecté, aucune information ne sera remontée !. TCP niveau 4 devra réémettre
[24] IP c'est du désordre très bien organisé

Taille du datagramme, MTU (Maximum transmit Unit) et fragmentation.
Chaque datagramme pour être transféré devra s'appuyer sur une trame du protocole de liaison. Or la taille de la trame de liaison peut être très différente. Par exemple, dans le cas de ETHERNET, c'est 1500, TokenRing (16Mbs) 16K. Le MTU est un paramètre local de l'ordinateur ou du routeur et dépend de la couche de liaison. IP a prévu un mécanisme de fragmentation lorsque le datagramme est supérieur au MTU, c'est à dire que le datagramme est découpé en fragments. Le datagramme peut faire jusqu'à 64Ko, il va être découpé si besoin dès le départ en multiples de MTU.



R1 va fragmenter les datagrammes du réseau 1 vers Réseau3, et va donc générer 3 trames de 520 pour une trame de 1500. Les déplacements indiquent l'index dans les données du paquet non fragmenté du départ.

De temps en temps le MTU local peut être paramètré en local. Il faut faire quelques tests de transferts pour juger de la bonne taille. Cependant, la plupart des machines étant d'abord reliées à un réseau ETHERNET local, utilisent un MTU de 1500 pour avoir de grosses trames ETHERNET

Tous les fragments dans le schéma vont arriver sur la destination qui va les réassembler. Ce n'est pas la tache des routeurs car il leur faudrait mémoriser les fragments pour les réassembler.

La fragmentation est tout de même ennuyeuse car au moindre fragment perdu, c'est tout le datagramme IP qu'il faut réémettre. **IL FAUT EVITER LA FRAGMENTATION**

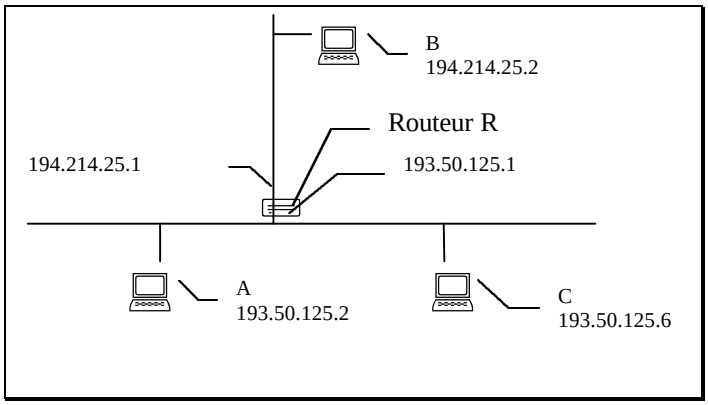
A cause de cela la couche UDP limite le datagramme à 512 octets
La couche TCP prend le maximum si la destination est locale (1496 en ETHERNET) et limite à 1024 octets dès que la destination sort du réseau local.

Attention, ceci peut dépendre du fournisseur de la couche de transport IP. Certaines couches TCP utilisent l'algorithme **PATH MTU DISCOVERY** (découverte du MTU de chemin) afin d'optimiser la taille du datagramme. TCP met alors dans chaque datagramme IP, l'option DO NOT FRAGMENT. Si le datagramme est refusé par un routeur, celui-ci envoie un message ICMP de refus. TCP diminue alors la taille du MTU lié à la session jusqu'à ce que le datagramme passe.

Le Routage des Datagrammes IP

Le routage est l'opération d'acheminer les paquets à bonne destination. Les machines effectuant cette opération sont appelées **routeurs** ou **passerelles**. Dans la terminologie Anglo-saxonne, on parle de « router » ou « gateway »[25]. Un routeur est souvent une machine spécialisée et sans disque dur (fiabilité). Cependant une station Unix ou un Windows NT peuvent faire le travail.

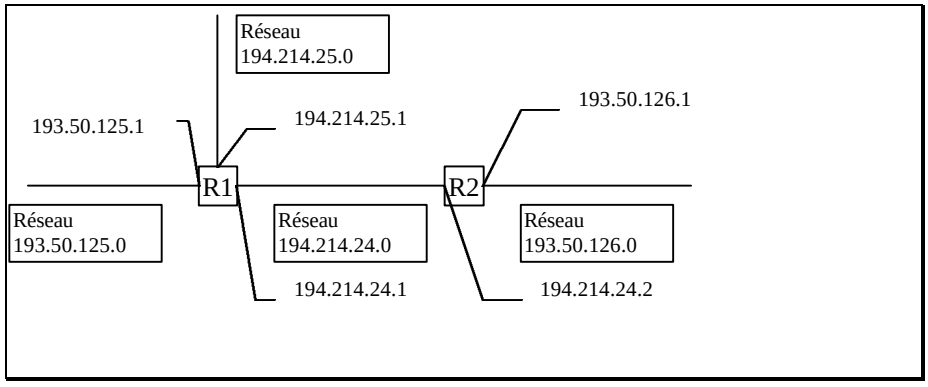
Transfert direct ou indirect.
Si les 2 machines sont sur le même réseau physique, la remise est directe, on s'appuie sur la couche de liaison pour envoyer les informations. Pour déterminer l'adresse physique, on utilise arp. Dans le cas ou les machines ne sont plus sur le même réseau, on va passer par un routeur.



Pour atteindre C , A effectue une remise directe. Pour atteindre B, ce sera indirect en passant par le routeur. Le routeur a deux adresses car l'adressage IP ne concerne que les interfaces sur le réseau et non la machine elle même. A ce propos , si le routeur est connu par l'adresse 193.50.125.1 et que la carte est en panne, on ne pourra l'atteindre alors que ce serait possible via 194.214.25.1 en supposant que les 2 réseaux aient des accès indépendants vers l'extérieur.

Pour que le routage marche, A pour atteindre B et connaissant l'adresse IP du routeur R, va faire un broadcast ARP, extraire l'adresse physique de D et ensuite générer le paquet avec une adresse Destination qui n'est pas celle du routeur. Celui ci s'en servira pour acheminer plus loin ce datagramme.

Routage IP via des tables statiques
Cette table va indiquer les routes a prendre en fonction du réseau, un peu comme une carte routière.



[25] Il est vrai que gateway s'applique plus souvent à une machine qui va faire une traduction de protocole, ce qui n'est pas le cas ici. Cependant dans beaucoup de références gateway est utilisé à la place de router.

Les tables seraient les suivantes :
pour R1

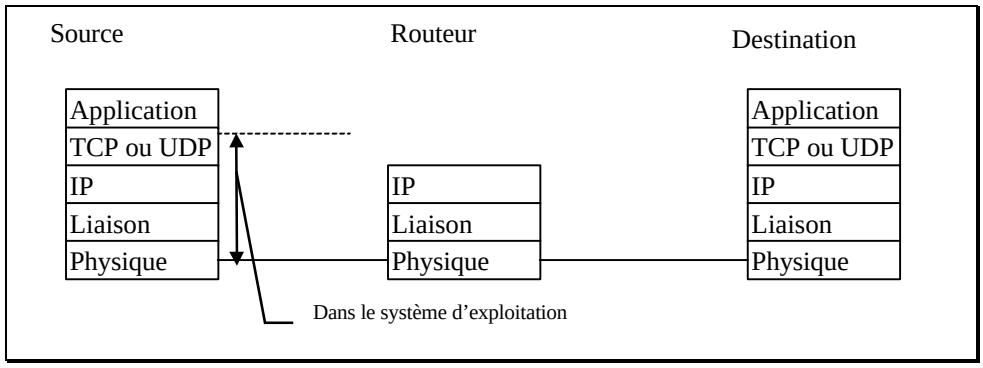
193.50.125.0	Direct
194.214.25.0	Direct
194.214.24.0	Direct
193.50.126.0	194.214.24.2

Pour R2

193.50.125.0	194.214.24.1
194.214.25.0	194.214.24.1
194.214.24.0	194.214.24.1
193.50.126.0	Direct

Pour conserver de petites tables (Il y a des millions de réseaux), on invente le panneau Autres Directions. Ce panneau s'appelle la **ROUTE PAR DÉFAUT**.
Si R1 est le routeur externe, R2 peut avoir à la place des 3 réseaux cités : 0.0.0.0 194.214.24.1
ce qui veut dire tous réseaux non cités : passer par R1
Ces tables sont définies statiquement par l'administrateur du réseau. Nous verrons plus loin qu'il existe des protocoles de routage qui permettent la mise à jour automatique des tables de routage.
On parle de RIP, EGP, BGP, OSPF , etc ..

Les couches traversées dans le réseau . Le routeur ne lit que l'en-tête IP et travaille avec la couche physique. Il ignore (à priori) tout du contenu du paquet.



Certains routeurs dits filtrants examinent les adresses Sources, Destination et aussi le type de l'application, de manière à éviter des entrées illicites sur le réseau Interne. C'est le principe des pare-feux ou firewall.

A retenir
La route par défaut.
Un ordinateur simple (PC / MAC) , station de travail, ne connaît que la route par défaut. (Une seule passerelle). En effet la boite de dialogue standard ne permet pas autre chose. Cependant, la commande **route** permet d'ajouter manuellement une route statique. Les ordinateurs ajoutent aussi des routes par réponse à des messages ICMP REDIRECT.

Les Routages Dynamiques

On a vu que le routage statique est difficile à gérer pour des réseaux importants. Nous abordons ici les routages dynamiques, les routeurs s'échangent des informations sur leurs tables de routage, décident du meilleur chemin, inactivent la route. Dés le départ, on obtient un message route barrée, au lieu que les paquets aillent se perdre en silence. On obtient alors le message explicite Host unreachable
On considère deux types de routage, les routages Intérieurs et les routages Extérieurs.
L'intérieur est un routage local qui concerne des réseaux gérés par la même structure administrative, les routages extérieurs concernent les problèmes d'interconnexion de vastes réseaux.
Système Autonome : un système qui a établi sa propre politique de routage. RENATER est un système autonome, le campus de Jussieu, celui de Luminy sont des systèmes autonomes.

Protocoles de routages intérieur (RIP, OSPF, HELLO)

RIP et un peu obsolète, mais il est toujours utilisé, notamment par MICROSOFT sous NT 3.51/4.0 mais aussi sous NOVELL 3.12. Il faut donc parler de son principe dans le cas ou l'on utilise ces systèmes pour interconnecter des réseaux. Sous Unix on trouve des versions plus évoluées . Les deux démons[26] standards s'appellent GATED et ROUTED . ROUTED ne gère que RIP V1 et devrait donc être écarté. GATED V3 gère RIP V2 ainsi que OSPF V2 et BGP V2,V3.

Les principes de RIP (RFC 1058)
RIP est multi-protocoles et est utilisé ailleurs que dans IP (NOVELL/ Appletalk)
RIP s'appuie sur une notion de métrique (Hop count) qui est un compteur de saut. C'est un algorithme de routage à vecteur de distance.

« Pour aller sur ce réseau, il faut passer par machin et c'est 2 sauts plus loin ».

RIP considère que si le saut est supérieur à 15, c'est une route désactivée. RIP n'est utilisable que sur des petits réseaux. De plus une liaison directe a un coût de 1 et non 0.
Au démarrage, le routeur envoie des broadcast sur les interfaces actives. Ce sont des broadcast IP UDP dont le numéro de port est 520 . Cette requête constitue à demander à tous les voisins gérant RIP leurs tables de routage. Un datagramme UDP est limité à 512 octets, par conséquent, un datagramme ne peut transporter que 25 routes (Il faut 20 octets par route). Cependant plusieurs datagrammes peuvent être émis.

Mises à jour. Toutes les 30 secondes, la table est émise sur le réseau sous forme de broadcast !.
Mises à jour volontaires. Lorsqu'une métrique change, seules les entrées concernées sont envoyées.
Si on trouve une route avec un plus petit hop count, c'est celle ci qui remplace l'ancienne. Si un routeur ne donne plus signe de vie, au bout de 90 secondes, la route passe en état invalide, puis au bout de 270 secondes la route passe en flush et est détruite 60 secondes après (2 broadcast minimum).
On voit que la suppression d'une route est un processus lent et que RIP converge très lentement.

Les bonnes nouvelles voyagent vite, les mauvaises lentement

Table RIP typique

Destination	Next Hop	Distance	Timers	Flags
Réseau A	Routeur 1	3	t1, t2 , t3	x,y
Réseau B	Routeur 2	5	t1, t2 , t3	x,y
Réseau C	Routeur 1	2	t1, t2 , t3	x,y
.	.	.	.	.

Pour éviter des problèmes de bouclage de route, on attend suffisamment longtemps quand une route tombe, de plus on évite de renvoyer des informations de routage sur une route qu'un voisin déclare comme plus proche.

[26] on appelle démons des programmes qui tournent en tache de fond dans le système d'exploitation. Ce sont des programmes fantômes, d'ou le nom de démon (démon dans la littérature)

Inconvénients

- RIP manque aussi une information essentielle qui est le masque de sous réseau. Dans certains cas de réseaux, il peut y avoir confusion sur la signification des bits machine si l'adresse réseau n'est pas en multiple d'octets. Si les deux derniers octets de l'adresse sont ainsi :
  1111 0000 . 0000 0000 , la partie machine peut être sur 8 bits ou 12 bits, il est impossible de le déterminer !.
- Aucun calcul du temps de réponse ou de charge du réseau n'est fait. Il est aberrant de considérer de la même façon un réseau ETHERNET à 10 Mbs avec une liaison PPP à 38400 bps.
- Un utilisateur malveillant peut détourner le trafic ou écrouler le réseau !.
- RIP émet des tonnes de broadcast (tous les routeurs, toutes les 30 secondes..)

RIP V2 (1993)

- Ajout du subnet mask.
- Retour d'information vers un protocole de routage extérieur.
- Support de Multicast pour diminuer les broadcast.
- Signature des tables.

OSPF (Open Short Path First) RFC 1247

C'est un protocole à état de liens (link-state). Chaque routeur teste l'état du lien avec ses voisins et leur envoie ses informations. Chaque routeur se constitue une arborescence du réseau en déterminant le chemin le plus court. (RIP s'arrête à ses proches voisins)
OSPF utilise la couche IP et non UDP. Il a un champ service spécial (pas un numéro de port).

- OSPF peut gérer des routes différentes en fonction du champ qualité de service IP (3 bits et 8 possibilités) delay, throughput, reliability.
- A chaque interface est associé un coût qui peut dépendre du débit, du temps d'aller-retour.
- On peut diviser un système autonome en Area, et avoir des tables par area et qualité de service.
- A égalité de coût OSPF établit une répartition de charge
- Supporte les sous réseaux via les masques
- Les liaisons Point à points entre routeurs ne demandent pas d'adresse IP
- Utilise le multicast
- Authentification par mot de passe des tables
- Passerelle désignée : une passerelle va concentrer les messages sur elle pour les diffuser sur d'autres, on limite ainsi le nombre des diffusions linéaire en n au lieu de n2 si n est le nombre de passerelles.
- Remonte des informations de passerelles intérieures vers les extérieures.
- Peut gérer des routes de machine à machine

1	1	2	4	4	2	2	8	Variable
Version	Type	Longueur	Routeur Id	Area Id	FCS	Type d'authentification	Authentification	Données

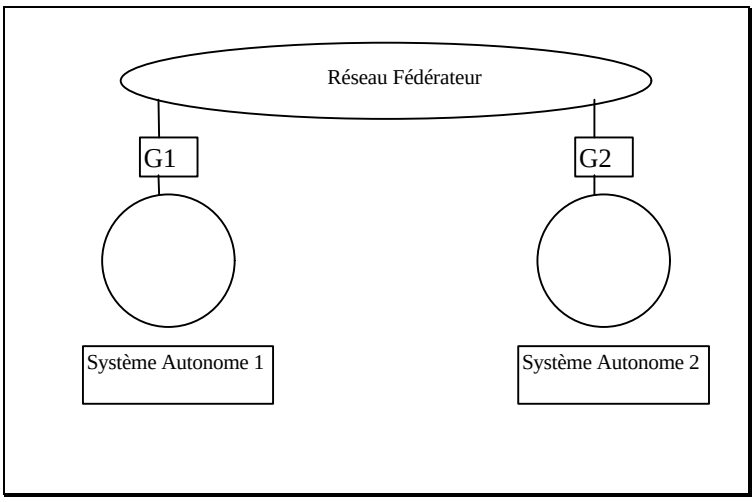
5 types de datagrammes OSPF

- Hello : généré entre voisins pour maintenir les relations
- Database description. Décrit le contenu d'une base topologique adjacente. Celle-ci est échangée au démarrage d'un voisin
- Link State Request Demande d'une partie de base topologique
- Link State Update Réponse à la question précédente. Transmet les LSA (Link State Advertising)
- Link State Acknowledgement. Une sécurité essentielle !.

Les LSA ont 4 types :
Router links advertising (RLA) UN routeur l'envoie à toute l'aire à laquelle il appartient.
Network Links Advertissements (NLA) défini les routeurs multi-aires
Summary Links Advertissements (SLA) Générés par les routeurs frontaliers
AS external links advertissements. Décrit une route externe au système autonome

A retenir : deux types de routage dynamique et compte de distance ou vecteur de chemin

Les protocoles de passerelles extérieures (EGP,BGP)[27]



Un mécanisme est nécessaire pour permettre aux passerelles périphériques d'informer le système central de l'existence de nouveaux réseaux ou des incidents de ses réseaux internes en les marquant non joignables.
Ces protocoles sont des protocoles de passerelles extérieures. G1 et G2 vont causer EGP avec le réseau fédérateur. Celui-ci en interne va mixer les informations de son routage interne avec les informations EGP. En utilisant EGP, c'est comme si l'on mettait sur la porte d'entrée du système autonome des panneaux indicateurs. « *Je possède tel et tel réseau* »

EGP (Exterior Gateway Protocol) RFC904 Avril 1984
Un réseau EGP est constitué de voisins (neighbor) qui se testent régulièrement. Ils transportent des informations sous forme de métriques un peu comme RIP. Cependant ces métriques calculées par rapport à la sortie du réseau ne sont pas interprétées comme élément de routage. Seul le fait de mettre la valeur 255 dans la distance va mettre la route comme invalide.

- Sépare les informations de routage de celles d'accessibilité dans un but d 'économiser la bande passante.
- Propage des informations d'accessibilité et limite la topologie de l'interconnexion à un arbre dont la racine est le système central. EGP est un protocole de frontière.
- Propage qu'un chemin vers un réseau donné.
- Entre deux réseaux fédérateurs, EGP n'est pas optimal, il faut créer des routes manuellement pour optimiser le trafic.
- Oblige une passerelle à ne propager que des informations concernant des réseaux accessibles à l'intérieur du système autonome. Ouf, sinon les routeurs de campus auraient toutes les routes de l'INTERNET !..

BGP (Border Gateway Protocol) RFC 1267
BGP définit trois types de systèmes autonomes.

1. Le stub (en fait une feuille du réseau)
2. Un multi-interfaces : plusieurs connexions sur les système central
3. Un transit . Ce système autonome peut router à la fois du trafic local et du trafic de transit.

BGP s'appuie sur TCP et utilise un protocole à vecteur de distance. Les décisions de routage sont entrées par des fichiers de configuration. Comme EGP les décisions de routage ne font pas partie du protocole. Les mises à jour successives sont transmises via TCP lorsque les tables évoluent. Pas question de broadcast et de liaisons non sécurisées..

[27] C'est difficile de comprendre ces termes. En fait, c'est à la limite du routage. C'est plutôt une déclaration de possession de réseaux.

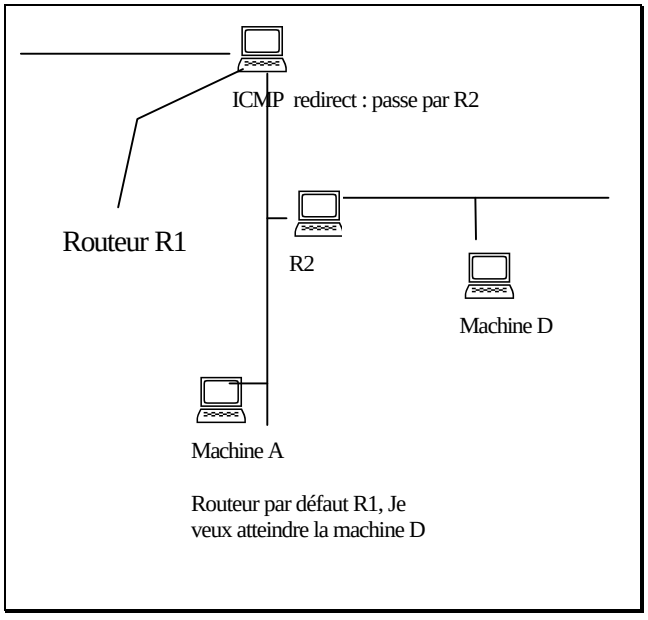
Les Messages ICMP
INTERNET CONTROL AND ERROR MESSAGE PROTOCOL

Le réseau TCP/IP sur lequel s'appuie INTERNET est un réseau de type Datagramme. Le réseau n'a aucune mémoire de ce qui se passe, les datagrammes n'ont que deux renseignements, une adresse source et une adresse destination. A aucun moment, on ne sait par quel routeur le datagramme est passé. Or, il faut bien informer la source des problèmes du réseau.
Pour cela, on utilise les messages ICMP, voici différentes valeur du champ type de ICMP :

Type de Champ	
0	Réponse d'écho (la commande ping)
3	Destination inaccessible
4	Limitation de source (source quench)
5	Redirection
8	Demande d'écho (la commande ping)
11	Expiration de délai
12	Problème de paramètre pour un datagramme
13	Demande estampille de temps
14	Réponse estampille de temps
15	Obsolète
16	Obsolète
17	Demande de masque
18	Réponse de masque

Ces messages sont traités prioritairement.
Le contrôle de flux est assuré par des ICMP de type 4. Le routeur demande à la source de limiter son débit. C'est ce que fait la source tant que ce genre de message est envoyé. Celle ci augmente ensuite régulièrement le débit tant qu'un message de limitation n'arrive pas. Ce message est envoyé par un routeur , dans les ordinateurs, TCP utilise la taille de fenêtre.

Redirection: le routeur vous indique de suivre une autre route. Ce message n'a de sens que si le routeur et l'émetteur sont sur le même support physique, car l'émetteur n'a aucun moyen de changer de route sur INTERNET. Ceci s'active dès que l'on a plusieurs routeurs sur le même réseau ETHERNET . Les machines n'ont qu'une adresse de routeur, si celui ci connaît une route plus courte, il l'indique



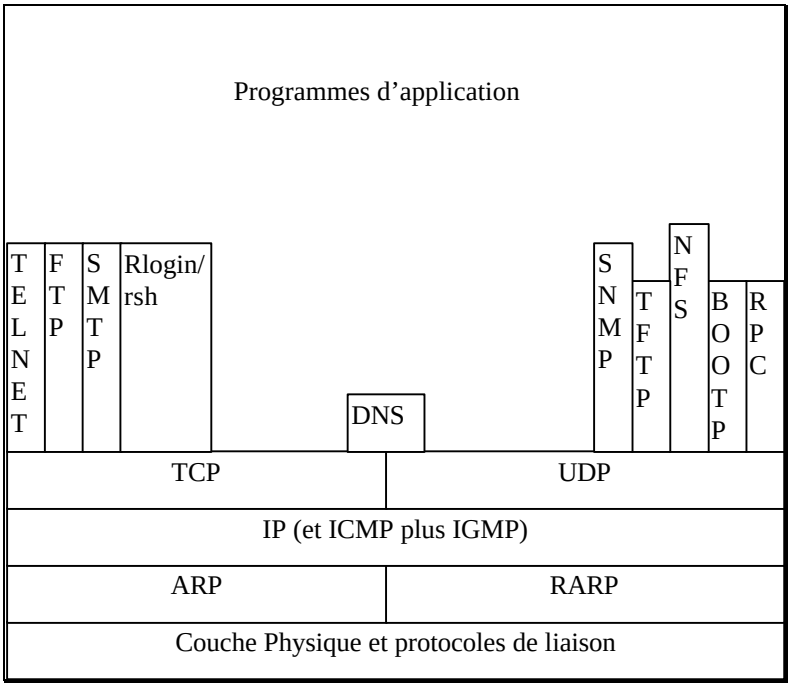
Détection des boucles de routage :
Chaque datagramme IP a une indication précieuse, c'est son HOP COUNT ou TIME TO LIVE, chaque fois qu'une trame traverse un routeur, on décrémente de un cette valeur jusqu'à atteindre zéro, le routeur émet alors un ICMP de type 11 (à condition que l'on puisse encore le recevoir..). Une trame IP part généralement avec un TTL de 32. La commande traceroute utilise le TTL en l'augmentant progessivement et reçoit du réseau les informations venant de tous les routeurs parcourus. Pour 20 routeurs traversés, il envoie 20 * 3 datagrammes, car traceroute fait des statistiques de temps de réponse.

A retenir
- Les ICMP sont les messages d'incident de réseaux.
- Il avertissent les machines émettrices des incidents du réseau.
- Un routeur ne peut avertir un autre routeur par ICMP.
- Les commandes PING et TRACEROUTE s'appuient sur les ICMP.

LE TRANSPORT IP

UDP ou User Datagram Protocol

Architecture IP :



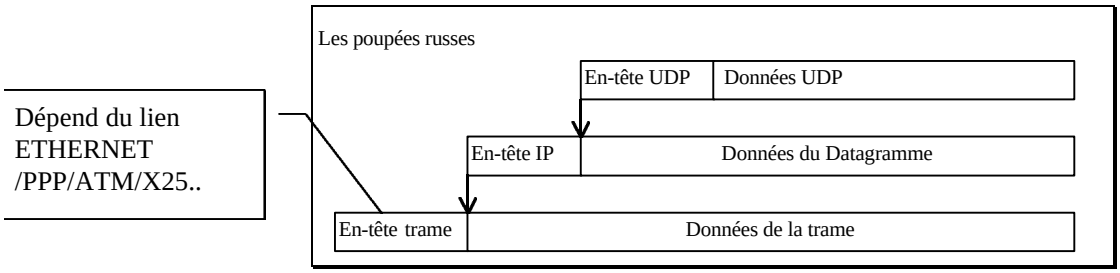
La couche IP dans la machine source ou destination agit comme une couche de multiplexage. C'est un peu comme une gare de triage. S'appuyant sur le champ protocole de l'en-tête IP, elle va traiter différemment ces paquets et les remonter si besoin aux couches supérieures.
UDP s'inscrit dans la couche 4. Il s'agit d'un transport en mode non connecté. UDP envoie des datagrammes et utilise une information complémentaire, le numéro de **PORT**. La trame UDP est constituée d'un numéro de port source et d'un numéro de port destination. Ce transport est en fait une succession de messages sans liens. L'application devra surveiller l'ordonnancement des messages et les problèmes de contrôle de flux que UDP ne gère pas. A part NFS (Network File System), UDP est utilisé par des applications qui ne transfèrent que des petits messages, TCP étant trop coûteux pour ce genre d'opérations. BOOTP et SNMP sont des applications typiques de UDP. Chaque écriture d'une application provoque l'envoi d'un datagramme UDP. Il n'y a aucune temporisation.

0 8	16 31
Port UDP source	Port UDP destination[28]
Longueur message UDP	Total de contrôle
Données	

Le port source est facultatif et vaut zéro généralement, sinon il contient le numéro du port ou renvoyer les réponses.
Longueur message UDP : longueur totale du datagramme, en-tête UDP compris. (<64Ko)[29]
Total de contrôle : Un code de détection d'erreur qui est facultatif (dépend de l'application). On décompose en mots de 16 bits, on fait la somme en complément à un, puis on garde le complément à un du résultat. Ce code concerne tout le datagramme UDP (données + en-tête). Ce calcul utilise un peu en violation du

[28] 16 bits = 65536 ports, donc sessions simultanées sur une même machine, valeur agrandie dans IPV6
[29] La plupart des implémentations limitent la longueur à 512 octets de données pour éviter la fragmentation

principe des couches, une partie de l'en-tête IP pour faire un contrôle plus serré. Ceci permet de contrôler que l'on a bien un datagramme pour cette adresse IP et que c'est bien UDP qui est concerné.
La méthode de calcul des erreurs est moins performante que celle d'ETHERNET. En particulier une inversion de 2 octets peut passer inaperçue. Le fait de faire deux fois le calcul sur deux parties indépendantes assure une sécurité supplémentaire.



Certains ports UDP sont prédéfinis , mais les programmeurs sont libres d'en utiliser d'autres. Voici un exemple de ports réservés :
On peut voir cela sous le système Unix avec le fichier /etc/services
Ou sous c:\windows\services

Décimal	Mot Clé	Mot Clé Unix	Description
0			Réservé
7	ECHO	echo	Echo
9	DISCARD	discard	détruire
11	USERS	sysstat	Utilisateurs actifs
53	DOMAIN	nameserver	Serveur de noms de domaine
67	BOOTPS	bootps	Serveur de protocole d'amorce
68	BOOTPC	bootpc	Client de protocole d'amorce
69	TFTP	tftp	Transfert de fichiers simple

Finalement UDP se réduit une à une petite couche , gare d'aiguillage entre différentes applications. Ces applications auront du travail, si elles transfèrent de grosses informations sur des grands réseaux car les paquets vont arriver déséquencés[30]. Pour éviter cela et éviter que chaque application se préoccupe du transport (chacun dans son coin, avec les problèmes de reprise, le contrôle de flux, etc..), TCP a été créé. C'est disons, un sous programme commun à certaines applications qui tourne dans le système d'exploitation de la machine.

La commande netstat
C'est le principe des couples adresses port. En fait netstat n'affiche en standard que les connexions TCP
Il faut taper ***netstat –a –u inet*** (linux) ou ***netstat –a –p udp*** (commande windows)

```
Active INTERNET connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp    65412      0 *:syslog                *:*
udp        0      0 *:tftp                  *:*
udp        0      0 localhost:domain        *:*
udp        0      0 romarin.univ-aix:domain *:*
udp        0      0 *:1026                  *:*
udp        0      0 *:ntp                   *:*
udp        0      0 localhost:ntp           *:*
udp        0      0 romarin.univ-aix.fr:ntp *:*
udp        0      0 *:49                    *:*
```

Choix des couples adresses, port

[30] A ce niveau là, l'application la plus énigmatique est celle de Sun NFS qui s'appuie sur UDP alors qu'il s'agit de transferts de fichiers. Ca pose d'ailleurs des problèmes de performance et de sécurité.

Une session TCP ou UDP, s'identifie par un couple de valeurs, adresseIPlocale.port, adresseIPdistante.port
On peut avoir plusieurs adresses locales (plusieurs sorties sur différents réseaux). Lors d'un appel, on utilise deux ports. L'un est un « well-known » port (une application bien précise ex : TELNET=23), l'autre est un port local libre généralement > 1023.
Un serveur ou démon UDP peut préciser lors du démarrage du service, en s'attachant un « well-known » port, sur quelles adresses IP locale ou distante, il veut que la couche UDP lui envoie les données dans une file d'attente. Il est possible de lancer plusieurs applications sur le même port local mais qui traiteront des adresses différentes.

Type de sélection des couples adresses port que l'on va recevoir
Il est vrai qu'en local on peut avoir plusieurs cartes réseau donc plusieurs adresses et faire une sélection à ce niveau. Voir l'interface de programmation des sockets (**bind**)

Local IP.port	foreign IP. Port
*.port	foreign IP.*
*.port	*.*

A retenir
- Les ports
- Des clients faciles à écrire
- Des serveurs difficiles à écrire
- Sécurité faible, car pas d'état.
- Des petits messages comme SNMP et DNS

TCP (TRANSPORT CONTROL PROTOCOL)

TCP est un protocole de transport qui pourrait être indépendant de IP et même s'appuyer directement sur des réseaux physiques comme ETHERNET. Cependant on le trouve toujours en relation avec IP d'ou le terme **TCP/IP**.

- TCP est un protocole connecté. C'est à dire qu'il existe une phase de création d'une connexion où les deux machines négocient leurs options et réservent des ressources. TCP informe les applications du succès ou de l'échec et ensuite contrôle le lien. Si celui-ci tombe, les applications en sont prévenues. Même si IP n'est pas un réseau connecté, TCP réalise cela au niveau des machines source et destination.
- Transferts bufferisé, sauf ordre on attend de remplir un segment, ou la fermeture de session.
- TCP va soit découper, soit rassembler dans un paquet suffisamment d'informations pour minimiser les transferts réseaux. Les unités de transfert sont appelés **SEGMENTS** dans le jargon TCP.
- Connexions Bidirectionnelles :
- Fiabilité des transferts et acquittements.

En-tête d'un « segment »TCP :

20 octets	20 octets	
En-tête IP	En-tête TCP	données TCP

Détail de l'en-tête en mots de 32 bits

<table>
<tr><td colspan="3">Port source (16 bits)</td><td colspan="3">Port destination (16 bits)</td></tr>
<tr><td colspan="6">Numéro de séquence sur 32 bits</td></tr>
<tr><td colspan="6">Numéro d'acquittement sur 32 bits</td></tr>
<tr><td>Longueur en-tête (4 bits)</td><td>réservé (6)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">taille de fenêtre sur 16 bits</td></tr>
<tr><td colspan="3">Somme de contrôle TCP</td><td colspan="3">Pointeur urgent sur 16 bits</td></tr>
<tr><td colspan="6">Options éventuelles</td></tr>
<tr><td colspan="6">Données</td></tr>
</table>

Signification des bits
URG le pointeur de données urgentes est valide
ACK est à un lorsque le segment contient un accusé de réception
PSH Ce segment requiert un push (on n'attend pas le remplissage ex : TELNET)
RST abandon violent de la connexion
SYN échange initial des numéros de séquence
FIN Séquence de fin de connexion

De la même façon que UDP, les couples (adresses, ports) identifient les connexions. Cette combinaison s'appelle socket[31] du même nom que l'interface de programmation de Berkeley.
Le numéro de séquence représente le rang du premier octet de données dans le paquet depuis le début de la connexion. Ce numéro de séquence ne démarre pas à un mais à une valeur propre au système d'exploitation appelé ou appelant et qui s'incrémente régulièrement. On peut remarquer que ce ne sont pas les segments qui sont numérotés mais les octets envoyés pendant la connexion. La valeur initiale du numéro de séquence a pour but d'éviter qu'une connexion se ferme, puis s'ouvre et que pendant ce temps des paquets retardataires de l'ancienne connexion ne soient pris pour valables.

Détail d'une ouverture de session
Le client envoie un segment TCP avec le bit SYN positionné à un. Il envoie son numéro de séquence ainsi que la taille de sa fenêtre (**WIN**) et la taille maximum de son segment (**MSS**). Il effectue ce que l'on appelle une ouverture active.

[31] Socket veut dire prise, comme une prise de courant

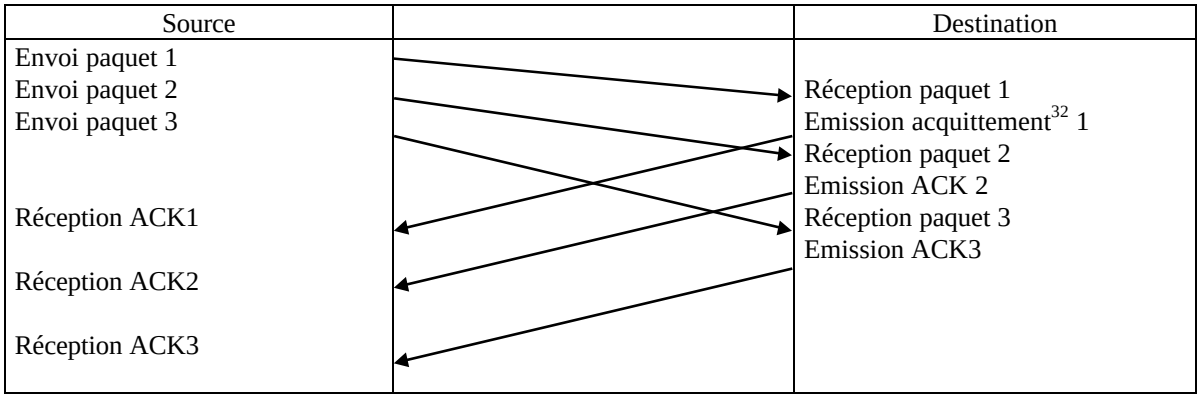
Le serveur va acquitter cette ouverture avec le bit SYN et fournit ses mêmes renseignements au client (MSS et WIN), il fait une ouverture passive. Le client acquitte ce segment en retour, la connexion est alors créée. On l'appelle l'ouverture à trois poignées de main !. Généralement, pour éviter la fragmentation, TCP prend comme taille de MSS 1460 caractères lorsque les trames sont sur une liaison ETHERNET.
Ceci est transmis dans le champ options éventuelles lors de l'initialisation SYN. En cas de problème de réponse, la demande est retransmise au bout de 9 sec, puis 24 sec puis 75 sec avant de signaler un échec.

Principe des fenêtres

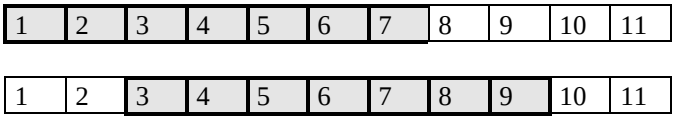
Pour chaque paquet envoyé, le récepteur envoie une confirmation de bonne réception. Afin de ne pas attendre cette réception , on s'autorise à émettre un certain nombre de paquets avant de s'arrêter faute d'un acquittement. Tout segment doit être acquitté. Si on émet 5 segments et que le premier se perd, le récepteur ne va acquitter que la séquence antérieure au premier, or il a reçu les 4 autres. L'émetteur part en time-out sur cet acquittement, remet le 1er ainsi que les 4 autres que le récepteur va confirmer de suite.

Ce mécanisme est un mécanisme d'acquittement cumulatif, il indique l'endroit jusqu'où tout va bien. On aurait pu faire différemment. Cependant, lorsque le paquet en panne arrivera , on enverra un seul acquittement qui validera tous les segments de la fenêtre.
La fenêtre évolue en taille de manière dynamique, celle-ci s'exprime en nombre d'octets (taille de fenêtre **win**). C'est à dire que elle peut augmenter ou diminuer en fonction de la rapidité du réseau et des machines. Si l'application arrête de lire des données, la couche TCP du récepteur va très vite envoyer une fenêtre de taille nulle.

Voici le diagramme dans le temps



En fait, on peut perdre l'ACK2, si l'on reçoit l'ACK3, c'est que 2 a été bien transmis
Concept de fenêtre glissante :



A gauche de la fenêtre se trouvent les paquets transmis, au milieu les paquets en cours, à droite ceux qui restent. Dès que l'acquittement du 1 arrive, la fenêtre glisse. La taille est de 7 pour dire que l'on peut émettre 7 segments avant d'attendre l'acquittement. En fait la taille de fenêtre[33] s'exprime en octets et on a tout intérêt à prendre un multiple entier de la taille du segment.

Temporisations et retransmissions.
TCP gère de manière dynamique les temporisations. IL essaye pour cela de déterminer Round Trip Time (RTT) ou temps de bouclage moyen. Il regarde le temps qui s'écoule entre l'émission d'un segment et la

[32] On note l'acquittement ACK (acknowledge)
[33] On aurait pu compter en nombre de segments et compter les fenêtres sur un seul octet. WIN peut préciser : je ne veux que 10 caractères.

réception d'un ACK sur un segment non retransmis. Il utilise une moyenne de ce temps pour calculer sa temporisation avant réemission.

Gestion des congestions ou le contrôle de flux
Le réseau ou la machine distante peut être engorgé. Pour chaque perte, TCP diminue sa fenêtre de moitié et il double la valeur de sa temporisation (et ainsi de suite), c'est le repli exponentiel[34]. Ceci permet de désengorger les routeurs du réseau. Le redémarrage s'effectue à l'inverse lentement , on augmente de un segment à chaque ACK. Lorsque l'on a atteint une fois et demie la taille de la fenêtre initiale, on n'augmente plus que de un segment lorsque tous les segments de la fenêtre ont été acquittés.
Lorsque le récepteur envoie une taille de fenêtre nulle, TCP passe en timer persistant et envoie toutes les 60 secondes un segment de sonde de fenêtre (on peut avoir raté le segment d'ouverture de la fenêtre..).

Gestion des erreurs ICMP
Si on reçoit source quench, la taille de la fenêtre passe à un segment.
On ne traite pas host unreachable !.. Les concepteurs pensent que c'est un problème de réseau transitoire et que ce problème sera résolu ou que la gestion des temporisations fera échouer la connexion par un « connection timed out ».

Timer keep alive.
C'est une fonction de TCP qui permet de détecter les absences. En effet si aucune donnée ne circule, la liaison TCP est silencieuse. Il existe deux solutions, soit l'application s'en occupe elle-même, soit elle demande à TCP un timer keep alive. C'est le cas de TELNET et RLOGIN. En effet si un client éteint sa machine, la session va rester ouverte et consommer des ressources machines.
On émet un paquet sonde toutes les 2 heures, si échec, 9 sondes toutes les 75 secondes, si erreur toujours, on fait un RST sur la connexion.

Vitesses constatées d'échange TCP :

ETHERNET	8 600 000 bits/sec
FDDI	80 à 98 Mbit/sec

Remarque
On ne peut pas aller plus vite que la taille de la fenêtre divisée par le temps d'aller retour entre les deux machines.

A retenir
- TCP est une méthode de transport qui tourne dans le système d'exploitation des serveurs et des clients (pas les routeurs).
- TCP assure la remise en ordre des datagrammes, la retransmission et le groupage des informations avant envoi (MSS), le segment est rempli
- TCP est la base de la plupart des services de l'INTERNET
- Pour voir qui est connecté en TCP au niveau réseau ***netstat –t***

[34] C'est tellement exponentiel qu'il faut attendre 9 minutes pour faire tomber la connexion !. TCP c'est de la glue.

APPLICATIONS

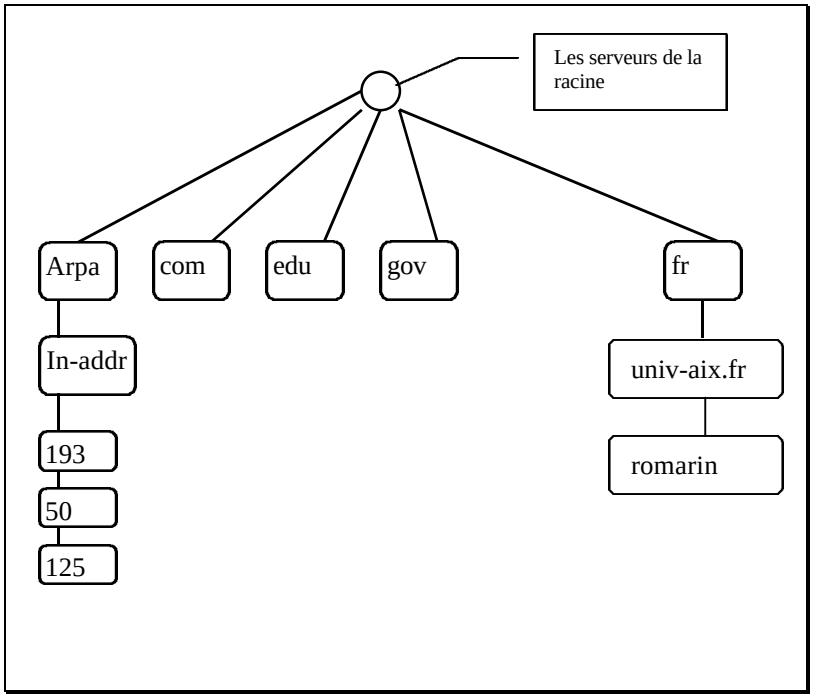
LES SERVEURS DE NOM

DOMAINE NAME SERVER (DNS)

L'adresse IP numérique étant difficile à manipuler, une représentation hiérarchique de nom de machines a été mise en place pour faciliter l'utilisation du réseau. Cependant dans les couches basses du réseau, seule la valeur numérique est utilisée. Le DNS n'est qu'une application non une couche du réseau[35].

Les noms sont composés par une suite de caractères alphanumériques encadrés par des points[36]. Par ex romarin.univ-aix.fr correspond à l'adresse 193.50.125.2 et le mécanisme qui associe le nom au numéro s'appelle la résolution de noms. Cette représentation est hiérarchique.

Les serveurs qui traitent la conversion nom = adresse ou adresse = nom sont des serveurs de nom ou **DNS**



Les domaines de la racine sont des domaines génériques ou des domaines géographiques.

Domaine	Description
com	Organisations commerciales (hp.com)
edu	Institutions éducatives (américaines)
gov	Organisations gouvernementales US
int	Organisations internationales
mil	Militaires Us
net	Réseau
org	Organisation à but non lucratif
de	Allemagne
uk	Angleterre
fr	La France

[35] Et pourtant, le DNS c'est la base de l'INTERNET.

[36] On peut mettre un point dans un nom, sans créer un sous domaine.

Les domaines géographiques sont sous forme de 2 caractères (ISO 3166).

Comment ça marche ?.

Une organisation : le NIC (Network Information Center) a en charge la bonne marche des DNS et délègue son autorité sur des sous domaines. En France, l'autorité responsable est l'INRIA qui gère le domaine fr. Quelques une des machines de l'INRIA sont les serveurs du domaine fr. (http://www.nic.fr)
Quant une application (TELNET, web..) a besoin de résoudre une adresse symbolique, elle va utiliser un renseignement de la configuration de la machine. Sous Unix, il s'agit du fichier /etc/resolv.conf.
Dans ce fichier, on va trouver l'adresse de un ou 2 serveurs de noms. On envoie une requête UDP sur le port 53 du serveur de noms en demandant la résolution.
Celui-ci va alors appeler un série de serveurs[37] (ses collègues) pour la résolution. Tout d'abord, celui-ci va faire appel aux serveurs de la racine. Il s'agit de 8 serveurs dont les adresses sont figées dans la configuration du serveur [38]. Dans la cas ou on cherche www.linux.org, on va appeler la racine pour demander qui gère le domaine com. On va récupérer une série d'adresses de serveurs.
Ensuite on interroge l'un de ses serveurs pour déterminer les adresses des machines qui gèrent le sous domaine linux.

Enfin, la dernière machine, va délivrer la bonne information, et la réponse va être envoyée à la machine demandeuse. Le serveur va garder cette information au maximum jusqu'à son expiration (indiquée par le propriétaire du domaine, champ refresh) . Au delà, le serveur de nom devra redemander l'adresse. Lors de changement importants (un serveur de nom par exemple), il est conseillé de changer les valeurs REFRESH une bonne semaine avant, afin que les noms soient gardés le moins longtemps possible dans les caches de l'INTERNET. En effet, le changement peut mettre jusqu'à deux jours pour se propager partout !.

Les machines serveurs ne sont jamais seules à gérer un domaine. Il faut veiller aux pannes !. Il existe donc des serveurs primaires et des serveurs secondaires. Les secondaires appellent les primaires au bout d'un temps défini par le primaire (généralement 2 jours, champ MINIMUM) pour mettre à jour les informations. Pour faire cette copie elles utilisent TCP avec le port 53.
Ces machines répondront ensuite de manière cyclique aux requêtes extérieures du réseau. Ces machines sont déclarées auprès du NIC.
Les machines clientes du DN S ne font aucun cache. Elles appellent sans arrêt le serveur de noms.

Configuration d'un serveur de nom :

Le fichier **/etc/named.boot** contient les déclarations initiales. En gros de qui suis je le primaire ou le secondaire.
Cas du domaine univ-aix.fr

```
primary         univ-aix.fr             named.data
primary         puget.univ-aix.fr       puget.named.data
primary         iae.univ-aix.fr         iae.named.data
primary         lpl.univ-aix.fr         lpl.named.data
secondary       iut.univ-aix.fr 194.199.116.10 iut.named.data
;les zones pour le mapping inverse :
primary         125.50.193.in-addr.arpa 193.50.125.db
```

le fichier **named.data** contient les infos suivantes :
Le premier est un champ de type SOA (Start of authority) . On y défini l'adresse électronique du responsable de la zone , la fréquence de mise à jour de la zone.

```
@       IN      SOA     romarin.univ-aix.fr.        postmaster.romarin.univ-aix.fr.
(
                        1996121301              ; Serial ANMMJJNum
                        28800   ;refresh[39]          : 8 heures
                        7200    ;retry[40]            : 2 heures
                        3600000 ;expire[41]           : 41 jours
                        86400 ) ;minimum[42]          : 2 jour
```

[37] à moins qu'il n'ait déjà cette information dans son cache
[38] on trouve cette information sur le serveur www.nic.fr
[39] refresh concerne la relecture des informations par les serveurs secondaires
[40] retry les secondaires en cas d'échec réessayent toutes les 2 heures
[41] expire : au bout de 40 jours sans nouvelles du primaire, la zone ou sous domaine est détruire

Si le serial est modifié, les secondaires vont recopier la zone au bout du délai refresh. Expire sert lorsque les secondaires n'arrivent plus à contacter le primaire. Minimum indique que l'enregistrement par défaut aura une durée de vie de 2 jours.

Extrait des déclarations du domaine univ-aix.fr
Les serveurs des sous domaines de univ-aix.fr

```
iut.univ-aix.fr.        IN      NS      romarin.univ-aix.fr.
iut.univ-aix.fr.        IN      NS      alpha.iut.univ-aix.fr.
iae.univ-aix.fr.        IN      NS      romarin.univ-aix.fr.
iae.univ-aix.fr.        IN      NS      aixup.univ-aix.fr.
```

Des enregistrements de messagerie (MX records) utilisés par SMTP

; Le relais de messagerie pour le domaine (attention au "." en fin de nom absolu)

```
univ-aix.fr. IN       MX      100     romarin.univ-aix.fr.
```

Des déclarations de machines , il faut bien dire qui est romarin !

```
romarin         IN      A       193.50.125.2
www             IN      CNAME   romarin
w3              IN      CNAME   romarin
```

romarin a des alias www ou w3. Donc www.univ-aix.fr = romarin.univ-aix.fr
Signification des différents champs

CNAME	alias
NS	Serveur de nom
PTR	Adresse inverse (Pointeur dans la littérature)
A	Adresse de machine
SOA	Start of Authority
MX	Redirection du courrier

Les résolutions inverses

on cherche parfois à savoir qui est la machine dont le numéro est 193.50.125.2. En fait on va générer une requête en cherchant quelle est la machine 125.50.193.in-addr.arpa. On va interroger ainsi le pseudo-domaine arpa (les serveurs de la racine) puis les serveurs in-addr puis 193 puis 50 jusqu'à parvenir sur le serveur du domaine qui va renvoyer l'info suivante :
193.50.125.2 = romarin.univ-aix.fr

le fichier **193.50.125.db** contient les reverses de la zone :

```
$ORIGIN 125.50.193.in-addr.arpa.
@       IN      SOA    romarin.univ-aix.fr.        postmaster.romarin.univ-aix.fr. (
                        1996110801                              ; Serial
                        28800   ;refresh          : 8 heures
                        7200    ;retry            : 2 heures
                        3600000 ;expire           : 41 jours
                        86400 ) ;minimum          : 2 jour
; ------------------------------------------------------
;
@       IN      NS      romarin.univ-aix.fr.
@       IN      NS      irisa.irisa.fr.
@       IN      NS      cnudns.cnusc.fr.
;
2       IN PTR  romarin.univ-aix.fr.
```

Ceci est utilisé pour filtrer des accès à certains services comme les serveurs ftp ou news. On veut savoir si la machine appartient au réseau fr ou univ-aix.fr ou univ-mrs.fr de manière à créer des services différents ou rejeter des appels. Il est aussi plus facile de lire des rapports ou l'adresse FQDN (Full Qualified Domain Name) est indiquée.
Toute machine du réseau auquel on attribue une adresse IP **devrait** avoir sa reverse adresse de définie !. De plus en plus les machines ne suivant pas cette règle sont rejetées par les serveurs.

Tout ces mécanismes sont accessibles via des API bien documentées, il s'agit des fonctions *gethostbyaddr()* et *gethostbyname()*

[42] minimum : La valeur la plus importante car stockée avec les valeurs des résolutions dans tous les serveurs de noms de l'INTERNET. Combien de temps cette information est valide.

Les commandes utilisateur Unix :[43]

host romarin ou
host 193.50.125.2
host -t mx mediterranee.univ-mrs.fr

nslookup
Cette commande permet d'interroger un serveur de nom de manière interactive , de demander à lister le domaine (toutes les machines du domaine par ex)
dig
whois

NB : Un nom peut correspondre à plusieurs adresses (www.microsoft.com).

```
host www.microsoft.com
www.microsoft.com has address 207.68.137.59
www.microsoft.com has address 207.68.137.62
www.microsoft.com has address 207.68.137.65
www.microsoft.com has address 207.68.143.193
www.microsoft.com has address 207.68.156.16
www.microsoft.com has address 207.68.156.49
www.microsoft.com has address 207.68.156.52
www.microsoft.com has address 207.68.156.53
www.microsoft.com has address 207.68.156.54
www.microsoft.com has address 207.68.156.58
www.microsoft.com has address 207.68.156.61
www.microsoft.com has address 207.46.130.16
www.microsoft.com has address 207.46.130.138
www.microsoft.com has address 207.46.130.139
www.microsoft.com has address 207.46.130.149
www.microsoft.com has address 207.46.130.150
www.microsoft.com has address 207.46.130.151
www.microsoft.com has address 207.46.131.15
www.microsoft.com has address 207.46.131.141
www.microsoft.com has address 207.68.137.53
www.microsoft.com has address 207.68.137.56
www.microsoft.com mail is handled (pri=10) by mail1.microsoft.com
```

Attention, par expérience, il est assez facile de mettre en place un domaine. Par contre, il existe des gros pièges qui pénalisent le bon fonctionnement :

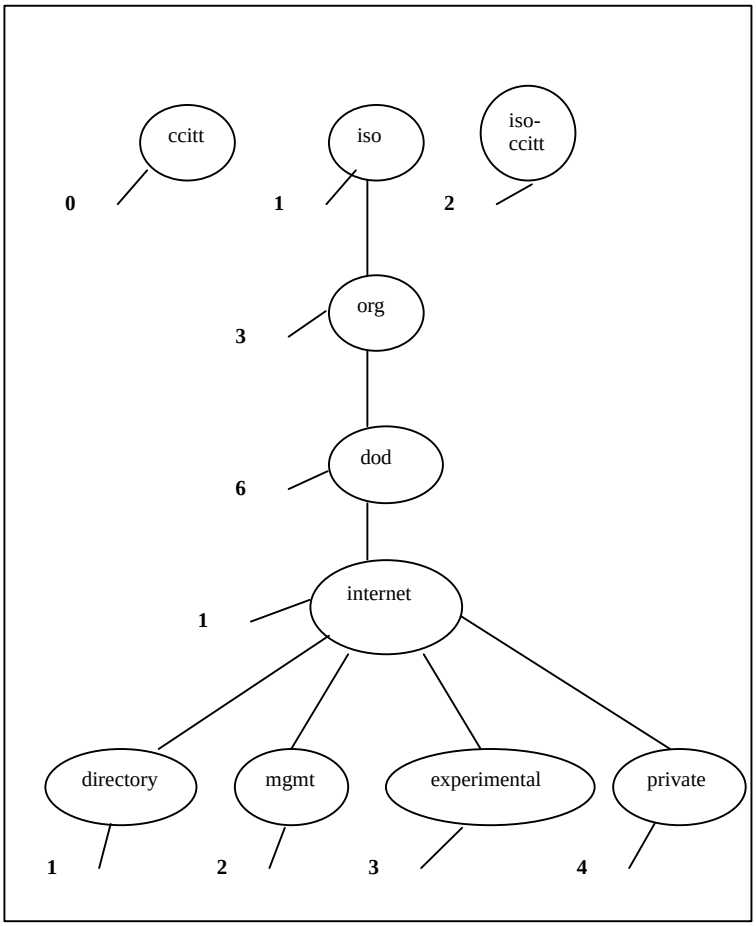
- Sur vos postes clients, vous vous trompez et mettez dans les DNS à contacter un routeur. En fait, si celui-ci est le premier contacté, vous allez perdre un temps important 30 sec à une minute avant d'appeler le deuxième. Il faut mettre l'adresse de 2 « vrais » DNS dans les configurations.
- Par rapport à votre domaine père vous déclarez trop de serveurs de noms qui gèrent votre zone. Ces serveurs ne sont pas chez vous mais chez des collègues. Etes vous bien sur qu'il sont actifs et bien configurés ?. Sinon ce sera les clients qui viendront chez vous qui devront attendre de tomber sur le bon serveur ! !. Ne mettez donc pas trop de serveurs de noms « officiels » sur votre zone (3 maximum).

[43] Sous Win95, c'est le désert : aucune commande livrée en standard !

Ce protocole sert à la gestion des équipements de réseau. Il s'appuie sur UDP (161/162) pour transporter des petites informations vers des logiciels de gestion de réseau .
Par une simple commande, il est possible de connaître le nombre de paquets émis par secondes sur l'interface d'un routeur ou la carte ETHERNET d'un simple Ordinateur.
Les commandes utilisent des mots de passes codés en clair. SNMPV2 est sensé régler ce problème mais est déjà mort né !.
Les commandes interrogent ou modifient des « variables ».
L'équipement peut aussi envoyer des « traps », c'est à dire des événements comme la mise sous tension d'une station sur un Hub. Le logiciel d'administration recoit la trap et modifie alors la représentation de l'élément en présentant par exemple une lumière verte, comme si l'on voyait l'équipement.
Les opérations de base:

get-request	récupère une valeur
get-next-request	récupère une valeur dans une table
get-response	réponse à un get-request
get-bulk	
set-request	modifie une valeur
trap	message évenementiel non sollicité

Les variables des équipement sont disposées dans une arborescence de données :



Ici sous mgmt, on trouve encore mib (1), puis sous mib :
système (1) interfaces(2) arp (3) ip (4) icmp(5) tcp(6) udp(7) egp(8)

Pour appeler une variable comme system.sysuptime, le client SNMP enverra une chaine de valeur numériques comme 1.3.6.1.2.1.3. On pourra aussi bien demander la valeur system.sysuptime ou 1.3.6.1.2.1.3.

Comment configurer SNMP ?.

En fait les équipements récents sont tous administrables SNMP. Certains fabricants de HUB, fournissent même leur logiciel de supervision. Pour programmer l'équipement (HUB, routeur), on doit initialiser la configuration, généralement via un port « Console », en fait un port asynchrone que l'on peut relier à un simple PC et une émulation de terminal (minicom Linux ou Hyperterminal Windows). Parfois l'équipement fait du BOOTP et on peut le configurer ou le « pirater ! » via un simple telnet[44]. Ensuite on donne une adresse IP à cette équipement et un mot de passe. Le reste de la configuration (gestion des traps) peut se faire en mode ligne, ou via un logiciel à distance.

Les MIB (Management Information Base)

Une représentation commune des éléments essentiels de la MIB a été normalisé. Les noms des variables sont communs à tous les équipements. Les variables interrogées sont représentées suivant une représentation hiérarchique. On peut interroger la variable system.SysUpTime et bien d'autres encore. Les constructeurs ajoutent une partie privée à la MIB. Le problème est ensuite de savoir à quoi correspondent les variables listées. Les outils comme snmpget utilisent une MIB /usr/lib/mib.txt. Ce fichier suit une syntaxe normalisée appelée ASN.1. Il faut modifier ce texte pour voir apparaître les noms des variables proriétaires.

Exemple de syntaxe ASN.1

```
sysUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time (in hundredths of a second) since the network
            management portion of the system was last re-initialized."
    ::= { system 3 }
```

Si l'on a des dizaines de constructeurs différents, ajouter ces informations n'est pas chose facile. En fait les administrateurs travaillent directement sur les valeurs numériques. Dans le cas du constructeur Cisco, sa « MIB » privée est sous 1.3.6.1.4.1.9

Par exemple pour voir la consommation CPU d'un Cisco, on fait un :

snmpget routeur-cisco motdepasse .1.3.6.1.4.1.9.2.1.57.0

enterprises.9.2.1.57.0 = 5

Il faut lire 5% de CPU sur la dernière minute

Dans la Mib Cisco, la variable s'appelle AvgBusy1

Exemples de commandes SNMP, classiques sous Unix

Ces commandes sont installées dans la plupart des distributions Linux. Win95 ou NT ne donnent rien en standard.

snmpget cisco motdepasse system.sysuptime

```
system.sysUpTime.0 = Timeticks: (528409207) 61 days, 3:48:12
```

snmpwalk cisco motdepasse system

```
system.sysDescr.0 = "Cisco Internetwork Operating System Software ..IOS (tm) 450
0 Software (C4500-I-M), Version 11.0(5), RELEASE SOFTWARE (fc1)..Copyright (c) 1
986-1996 by cisco Systems, Inc...Compiled Mon 05-Feb-96 22:35 by hochan"
system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (528409207) 61 days, 3:48:12
system.sysContact.0 = ""
system.sysName.0 = "cisco-cdc1.univ-aix.fr.univ-aix.fr"
system.sysLocation.0 = ""
system.sysServices.0 = 6
```

snmpwalk cisco password icmp

```
icmp.icmpInMsgs.0 = 9749
icmp.icmpInErrors.0 = 0
icmp.icmpInDestUnreachs.0 = 5027
icmp.icmpInTimeExcds.0 = 7
icmp.icmpInParmProbs.0 = 0
icmp.icmpInSrcQuenchs.0 = 0
icmp.icmpInRedirects.0 = 0
icmp.icmpInEchos.0 = 4602
```

[44] Sur un switch 3Com, la doc donne le mot de passe standard..Il suffit d'une config bootp..sécurité ! !

```
        icmp.icmpInEchoReps.0 = 113
        icmp.icmpInTimestamps.0 = 0
        icmp.icmpInTimestampReps.0 = 0
        icmp.icmpInAddrMasks.0 = 0
        icmp.icmpInAddrMaskReps.0 = 0
        icmp.icmpOutMsgs.0 = 657872
        icmp.icmpOutErrors.0 = 0
        icmp.icmpOutDestUnreachs.0 = 44609
        icmp.icmpOutTimeExcds.0 = 3460
        icmp.icmpOutParmProbs.0 = 0
        icmp.icmpOutSrcQuenchs.0 = 15365
        icmp.icmpOutRedirects.0 = 589700
        icmp.icmpOutEchos.0 = 140
        icmp.icmpOutEchoReps.0 = 4601
        icmp.icmpOutTimestamps.0 = 0
        icmp.icmpOutTimestampReps.0 = 0
        icmp.icmpOutAddrMasks.0 = 0
        icmp.icmpOutAddrMaskReps.0 = 0
```

snmpnetstat -i cisco motdepasse

```
        Name        Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs
        Ethernet0   1500  none        none           290662643     0 261303643    27 0
        Ethernet1   1500  none        none           329321626   148 361966900     0 0
        Ethernet2   1500  none        none            66088017     0 59743572     0 0
        Ethernet3   1500  none        none             1055965     0  1657673     1 0
        Ethernet4*  1500  none        none                   0     0        2     1 0
        Ethernet5*  1500  none        none                   0     0        2     1 0
        Serial0     1500  none        none           46281099 901907 46332851     0 0
        Serial1     1500  none        none            2463035  2760  2364075     0  0
```

snmpnetstat -r cisco motdepasse

```
        Routing tables
        Destination      Gateway            Flags   Interface
        default          193.50.124.2       UG      if0
        192.168.1        192.168.1.1        U       Ethernet2
        193.48.48        193.50.124.2       UG      Ethernet1
        193.50.124       193.50.124.1       U       Ethernet1
        193.50.125       cisco-cdc1         U       Ethernet0
        193.50.126.32    slip15-cdc         UG      if0
        193.50.126.64    slip14-cdc         UG      if0
        193.50.126.96    slip13-cdc         UG      if0
        193.50.126.128   this-network       U       Serial1
        193.50.126.192   193.50.126.193     U       Ethernet3
        193.50.127       192.168.1.2        UG      if0
        193.50.173       slip16-cdc         UG      if0
        193.50.174       this-network       U       Serial0
        193.50.175       this-network       U       Serial0
        194.57.187       192.168.1.2        UG      if0
        194.57.195       192.168.1.2        UG      if0
        194.199.116      this-network       U       Serial0
```

snmpnetstat -s cisco motdepasse

```
        ip:
                729278605 total datagrams received
                3464 datagrams with header errors
                3 datagrams with an invalid destination address
                727238565 datagrams forwarded
                0 datagrams with unknown protocol
                0 datagrams discarded
                1816006 datagrams delivered
                1412295 output datagram requests
                112823 output datagrams discarded
                95870 datagrams with no route
                0 fragments received
                0 datagrams reassembled
                0 reassembly failures
                5 datagrams fragmented
                0 fragmentation failures
                0 fragments created
        icmp:
                9751 total messages received
                0 messages dropped due to errors
                657956 ouput message requests
                0 output messages discarded
                Output Histogram:
                        Destination unreachable: 44615
                        Time Exceeded: 3460
                        Source Quench: 15365
                        Redirect: 589776
                        Echo Request: 140
                        Echo Reply: 4603
                Input Histogram:
```

```
                    Destination unreachable: 5027
                      Time Exceeded: 7
                    Echo Request: 4604
                    Echo Reply: 113
    tcp:
            2 active opens
            27 passive opens
            0 failed attempts
            7 resets of established connections
            0 current established connections
            7929 segments received
            5588 segments sent
            4 segments retransmitted
    udp:
            1498219 total datagrams received
            946971 datagrams to invalid port
            0 datagrams dropped due to errors
            513925 output datagram requests
```

La commande netstat sous Linux, quoique ce ne soit pas du SNMP, mais une commande directe du système. Souvent **netstat –s** donne ce genre d'information. Que ce soit pour les systèmes Unix ou Windows

MRTG
Un très bel outil qui interroge des routeurs et présente des statistiques sous forme Gif/HTML.
http://ee-staff.ethz.ch/~oeticker/webtools/mrtg/mrtg.html

Les logiciels de supervision de réseaux.
Quelques noms : HP OpenView, IBM Netview, Sun NetManager. Une caractéristique commune, ces logiciels nécessitent un temps d'apprentissage important. Un long moment à faire les dessins de son réseau, avant de jouer avec le sapin de Noël. Autre problème, ces logiciels ne représentent que les variables standard. Dés lors, pour optimiser, il faut ajouter deux ou trois logiciels propriétaires pour chaque type de routeur par exemple. L'administraion clique bouton n'est pas tout à fait pour tout de suite..

Encore que.. De plus en plus, les constructeurs ajoutent des agents HTML. Via le WEB, on peut alors facilement consulter les variables et voir directement visualiser de beaux graphiques. Des agents Java seront vraisemblablement intégrés dans les éléments et rendront plus facile la construction d'un outil adapté aux besoins de tout le monde. Quelque part on peut dire que le développement de SNMP n'ira pas plus loin. Il est suffisant pour l'essentiel.

CMIP est l'équivalent de SNMP pour les protocoles ISO.

BOOTP / DHCP

Le Protocole d'amorce (RFC 951 et 1532)

Comme nous avons vu précédemment RARP est un protocole qui permet de demander son adresse IP. RARP passe par des protocoles de niveau 1, non routables. De plus seule l'adresse IP est récupérée.
BOOTP marche au niveau IP/UDP et permet des choses plus intéressantes.
BOOTP utilise deux ports UDP : le port serveur 67 et le port client 68.
On n'utilise pas de port éphémère car la réponse peut être broadcastée (en principe ceci est évité).
BOOTP peut servir à démarrer un serveur, un terminal X en renvoyant le nom du fichier de démarrage qui sera récupéré par TFTP.
BOOTP n'accepte et ne traite que la première réponse.

Le format de la trame BOOTP sur 300 octets

0	8	16	24
Code Opération (1 requête , 2 réponse)	Type de matériel 1=ETHERNET	Longueur adresse matérielle 6 si ETHERNET	compteur de saut (0 en général sauf routeur)
Identificateur de transaction (tiré au hasard , envoyé et renvoyé tel que)			
Nombre de secondes		Non utilisé	
adresse IP du client (souvent 0.0.0.0)			
votre adresse IP (renvoyée par serveur)			
Adresse IP du serveur (rare)			
adresse IP du routeur (si un routeur route la demande)			
adresse matérielle du client (16 octets) (émise et retournée)			
nom de machine du serveur (64 octets) si boot			
nom du fichier de démarrage (128 octets) si boot			
information spécifique (64 octets) (retour des infos)			

Certains champs sont remplis quand la machine a une notion de ce qu'elle veut. Elle peut avoir déjà une adresse IP et demander des renseignements complémentaires et même avoir le nom ou l'adresse du serveur qui doit la servir.

Pour démarrer , le client fait un broadcast ETHERNET avec dans cette trame, comme adresses IP 0.0.0.0 , destination 255.255.255.255 et remplit l'adresse matérielle, port 67.
Le serveur renvoie sans broadcast la réponse sur la machine. Elle évite de faire un ARP pour renvoyer la réponse car le client ne connaît pas encore son adresse. Le serveur ajoute « à la main » l'entrée dans la cache.

Passage par un routeur
si le routeur est configuré[45] pour router les trames vers un serveur BOOTP particulier, celui ci ajoute 1 dans le hop count , met l'adresse IP de l'interface qui a reçu l'appel dans le champ adresse IP du routeur et transmet la demande au serveur . Le serveur a ainsi une correspondance entre l'adresse matérielle et le réseau sur lequel se trouve la machine.

Configuration des serveurs.
Ceux ci ont des fichiers de configuration constituées de centaines de lignes du style :
adresse ETHERNET = adresse IP

Pour chaque réseau, ils ont des informations spécifiques, comme l'adresse du routeur, le masque, les serveurs de nom, les serveurs de temps..
Les informations sont renvoyées dans le champ spécifique du vendeur.

Les évolutions de BOOTP : DHCP

[45] C'est la commande ip helper dans les routeurs cisco

Pour rendre la distribution d'adresse IP encore plus facile, un nouveau protocole DHCP (Dynamic Host Configuration Protocol) a été ajouté vers 1995. Celui ci permet de distribuer dynamiquement des adresses par des plages de numéros. Ces adresses peuvent être distribuées pour des temps plus ou moins long (notion de bail). L'adresse peut être réattribuée à la demande suivante.
DHCP utilise un mécanisme d'acquittement pour dire au serveur qui a envoyé la réponse que l'adresse envoyée a été validée par la machine cliente. Le serveur n'attribuera plus cette adresse pour la durée du bail. De plus le client vérifie par une requête ARP qu'aucune machine n'a déjà cette adresse. Ce n'est pas le cas de BOOTP !.

Ceci dit la couche du dessus peut envoyer un ARP gratuit et se rendre compte du problème. Cependant la machine n'aura aucun moyen de négocier une autre adresse via BOOTP. Seul DHCP peut permettre cela.

Hormis les machines fixes (serveurs) du réseau, toute machine cliente devrait utiliser DHCP pour son adresse. Ca évite bien des problèmes de copies de configurations avec la même adresse.
DHCP est standard sous Windows95 et WindowsNT[46]
DHCP utilise le format de BOOTP et s'appuie sur les passerelles pour faire parvenir les requêtes au serveur. Le champ non utilisé contient des options DHCP et la trame dépasse 300 octets.

Remarque :
BOOTP/ DHCP offrent une grande souplesse, il est facile de reconfigurer le réseau. Par contre il est très difficile de reconnaître facilement une machine du réseau par son adresse. Hors ceci est bien utile lors de l'analyse d'un problème. Préfère-t-on voir un piratage ou problème depuis la machine pc-bureau205 ou depuis pc-dhcpxxx ?. Lequel des deux systèmes est le plus parlant ?

Ceci dit , il est très important de se faire un fichier de toutes les cartes ETHERNET et « d'essayer de le tenir à jour !».

[46] On peut reprocher à MICROSOFT de ne pas avoir mis en option BOOTP, mais c'était probablement à l'époque pour vendre des serveurs NT pour gérer le service DHCP ! !

TFTP

Trivial File Transfer Protocol (RFC 1350)

Ce protocole permet le transfert de fichiers pendant des séquences de démarrage ou pour sauvegarder des configurations de routeurs. Il doit donc être très petit pour tenir dans un mémoire morte[47].
Donc pas de TCP, mais UDP (port 69) comme couche de transport.
Il n'y a pas de fenêtre de transmission mais une attente à chaque transmission de l'acquittement du paquet. Si celui-ci n'est pas acquitté, on retransmet.

Le protocole en 4 lignes :

20 octets	8 octets	2	N octets	1	N octets	1
En-tête IP	En-tête UDP	Code	nom du fichier	0	mode	0

	2 octets	0 à 512 octets
3=data	No de bloc	Données

	2 octets
4=ack	No de bloc

erreur	2 octets		
5=Err	No d'erreur	message d'erreur	0

Si le code vaut 1 , c'est une lecture, s'il vaut 2 une écriture
mode = netASCII ou byte
Le dernier paquet fait moins de 512 octets.
Pour ne pas bloquer le port 69 qui ne fait qu'écouter les appels (1 et 2) pour le reste du service, TFTP serveur récupère un port éphémère et finit le transfert avec ce numéro de port
Ce protocole est très simple (trivial) et ne sert pas à transférer des gros fichiers sur de longues distances. Pour cela on utilise FTP.
Aucun mot de passe n'est utilisé, le serveur restreint l'accès à un répertoire particulier généralement /tftpboot avec des droits de propriétés de fichiers très limitatifs.

Sécurité : Sous Unix, utilisez TCP/ WRAPPER qui fait le contrôle des adresses appelantes.

Cependant, quelqu'un peut par des programmes appropriés, modifier l'adresse source, et se faire passer pour vous. Il peut par ce biais non pas lire mais écrire dans des fichiers. Attention donc aux bugs de sécurité de ce genre de serveurs !.

On l'emploie souvent pour sauvegarder la configuration d'un routeur, ou les démarrer

[47] En 1998 les mémoires mortes ne sont plus si petites, et FTP est plus sur que TFTP..

FTP
File Transfer Protocol RFC959

Le protocole de transfert de fichier utilise deux connexions TCP. L'une pour les ordres (le port 21) l'autre pour les données (20).
La connexion pour les données est crée à chaque fois qu'un fichier est transféré mais aussi pour lister un répertoire. Cette connexion de données s'établit du serveur vers le client en sens inverse de la première connexion de contrôle. Une simple émulation de terminal suffit à donner les ordres car ceux-ci sont composés de caractères courants et non de chaînes de bits.
Les commandes courantes sont les suivantes :

ABOR
LIST
PASS
PORT n1,n2,n3,n4,n5,n6
QUIT
RETR nom de fichier
GET nom de fichier

Pour transférer les données qui peuvent être des fichiers ou des commandes du style DIR (listage d'un répertoire), le serveur va faire une ouverture TCP active. Le client fait une ouverture passive sur un port éphémère TCP. Dans la connexion de données, celui-ci indique au serveur qu'il attend les données sur le port qu'il vient d'ouvrir. C'est la commande PORT (qui se termine le plus souvent par port successfull)
Les serveur utilise son port ftp-data (20) pour appeler et fait le transfert (cas du get) et ferme la connexion à la fin. S'il s'agit d'un transfert du client vers le serveur, c'est le client qui envoie les données et ferme la connexion.
En fait c'est assez simple à écrire, on peut juste regretter que pour la commande dir, il faille créer une session TCP supplémentaire pour cela.
Principalement, FTP a deux modes de transfert , le mode binary et le mode ASCII. Dans le cas du mode ASCII, on suppose que le fichier distant est du texte et qu'il faut le convertir. Le plus souvent, les gens transfèrent des informations pour leur système d'exploitation et n'ont pas (même si c'est du texte) à faire de conversion. Ca sert surtout pour voire un fichier README écrit sous Unix où les lignes ne sont pas finies par CRLF comme sous DOS. L'option ASCII fera la conversion des fins de ligne

Commandes
Client Port 1025 ➔ Serveur Port 21

Données
Client Port 1026 ➔ Serveur Port 20

Il existe deux types de fonctionnement dans les serveurs FTP, le mode anonyme et le mode utilisateur. Au tout départ, on indique son identité , si on donne comme nom anonymous, on donne par respect vis à vis de l'administrateur du site son adresse électronique comme mot de passe. Dans le cas de l'anonymous, on a des accès restreints à une partie du système et généralement, accès en lecture seulement. Les accès nominatifs sont généralement liés à des comptes utilisateurs sous Unix.
Il faut noter que ces transferts ne changent en rien les données (pas comme sous mail-SMTP) mais nécessitent des comptes et des mots de passe.
Dans les défauts de FTP, les attributs de fichier, propriétaires, types (records bloqués, variables..) ne sont pas transmis. C'est pour cela et des besoins de compression que les fichiers sont généralement dans des archives et donc stockés compressés avec des attributs de fichiers dans l'archive.
On trouve ces fichiers stockés sous la forme
.gz (Unix)
.tar.Z (Unix)
.zip (Dos)
.gzip (Unix)
.hqx (Mac)

L’utilitaire winzip sous Windows95 reconnaît la plupart de ces formats.

Session FTP type:

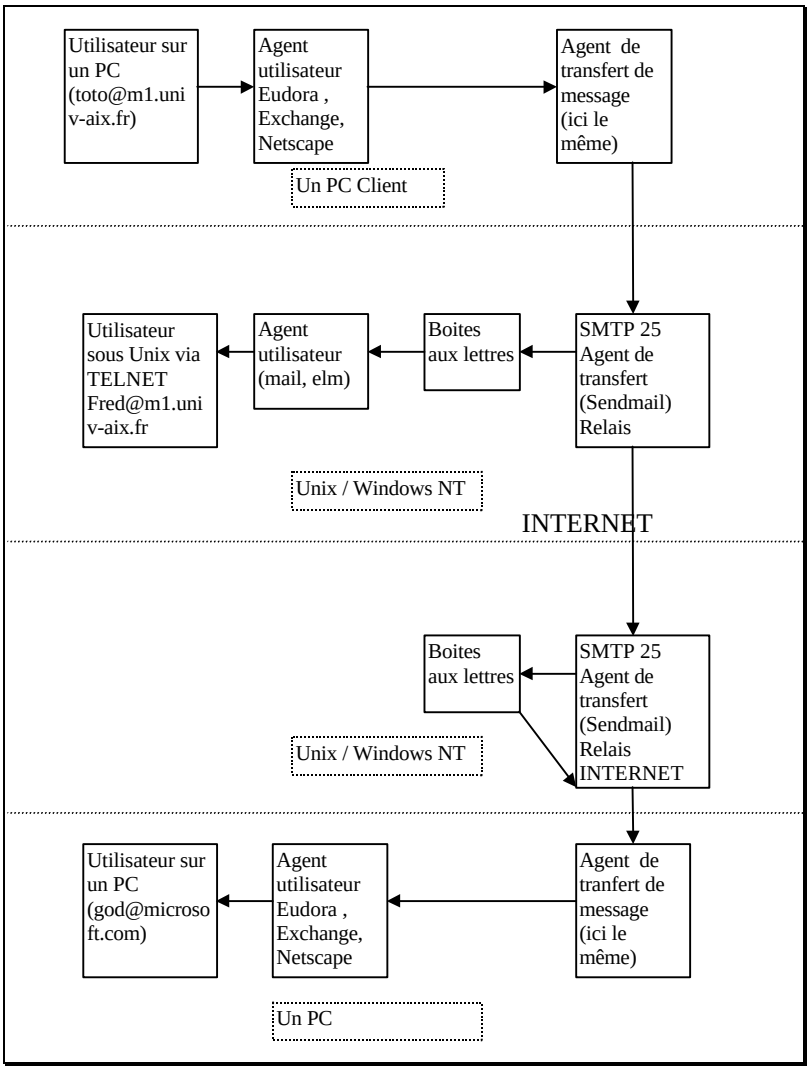
```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /pub/linux
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 4
drwxr-xr-x   3 root     root         1024 Jan  7 16:11 .
drwxrwxr-x   5 root     wheel        2048 Oct 17 10:02 ..
drwxr-xr-x   7 lalot    root         1024 Jan 23 03:10 kernel
lrwxrwxrwx   1 root     root           24 Sep 21 07:44 redhat ->
../../pub1/linux2/redhat
lrwxrwxrwx   1 root     root           32 Nov 19 11:46 redhat-contrib ->
../../pub1/linux2/redhat-contrib
lrwxrwxrwx   1 root     root           27 Jan  7 16:11 slackware ->
../../pub1/linux2/slackware
226 Transfer complete.

ftp> get README
200 PORT command successful.
150 Opening BINARY mode data connection for README (1099 bytes).
226 Transfer complete.
1099 bytes received in 0.0136 secs (79 Kbytes/sec)
```

SMTP
Simple Mail Transfer Protocol RFC 821 822

Un peu comme FTP et beaucoup d'applications INTERNET, on peut communiquer avec un machine parlant SMTP par le port TCP 25 à l'aide d'un simple TELNET. Les réponses sont sous la forme texte : 3 valeurs numériques ASCII suivies d'un texte compréhensible par un humain.
Cette façon de faire est très pratique car elle permet de débugger à la main les serveurs et de comprendre ce qui se passe.

Schéma d'un échange de courrier



Dans la littérature on distingue deux types de programmes, le Mail User Agent (**MUA**)et le Mail Transfert Agent (**MTA**). Certains programmes sont les deux à la fois comme ceux qui tournent sur les PCs sous Windows. Ceux-ci ont cependant des fonctions de transfert réduites. Il ne savent pas faire du relais, avoir plusieurs comptes utilisateurs locaux, etc. Principalement, ils ne reçoivent pas les demandes de connexions SMTP.
La frontière est donc un peu délicate à déterminer. Dans le protocole SMTP tout le monde est égal, un serveur devient client et réciproquement.
Habituellement, seuls deux relais sont utilisés, ils sont appelés aussi Bureaux de postes. Ces machines sont connectées 24h/24 et gèrent des centaines de comptes utilisateurs. Le micro ordinateur vient récupérer ses courriers par l'intermédiaire d'un second protocole (**POP** ou Post Office Protocol).

Alors que SMTP ne demande aucun mot de passe, POP demande le mot de passe du compte utilisateur pour pouvoir récupérer les messages. POP s'appuie sur les ports TCP 109 et 110 suivant la version.

Comme nous allons le voir SMTP est vraiment SIMPLE MAIL TRANSFER PROTOCOL. Il n'existe aucune identification certaine de l'expéditeur, pas d'accusé de réception et pourtant c'est lui qui est utilisé par tout le monde (ou presque). Il n'est pas cher et facile à comprendre. La messagerie X400 qui est une norme OSI a bien du mal à décoller..

SMTP ne transfère que les caractères codés sous 7 bits donc pas de caractères accentués. Une extension (ESMTP) permet cela. Cependant de nombreux MTA ne la supportent pas encore.

Sous Unix, on peut utiliser un MUA (mail) pour voir ce qui se passe lors du transfert du message. Celui ci renvoie sur le terminal toute la discussion avec le MTA (sendmail)
Généralement, on voit ceci :

Client	HELO romarin.univ-aix.fr
Serveur	220 whitehouse.gov Hello romarin.univ-aix.fr, pleased to meet you
Client	MAIL From :<toto@romarin.univ-aix.fr>[48]
Serveur	250 <toto@romarin.univ-aix.fr>... Sender ok
Client	RCPT To : <clinton@whitehouse.gov>
Serveur	250 <clinton@whithehouse.gov>... Recipient ok
	Eventuellement plusieurs RCPT
Client	DATA
Serveur	Enter mail, end with « . » on a line by itself
Client	Salut Bill !
Client	.
Serveur	250 Mail accepted
Client	quit
Serveur	221 whitehouse.gov delivering mail

Dans le cas de ESMTP au lieu de faire un HELO, le client envoie EHLO, le serveur envoie soit une erreur, soit un complément d'information.
Les lignes de DATA ne doivent pas dépasser 1000 caractères

Les commandes VRFY ou EXPN permettent de tester si un utilisateur existe (c'est l'outil de l'administrateur).

Retransmissions
Parfois le transfert ne peut se faire de suite. Dans ce cas le message est mis dans une file d'attente (/var/spool/mqueue) , puis toutes les 30 minutes et pendant 3 jours, le sendmail (MTA) va essayer de transférer jusqu'à ce que ça marche sinon sendmail retourne le message au destinataire.
Le message est à l'arrivée stocké dans un répertoire (/var/spool/mail) dans la boite aux lettres de l'utilisateur (un fichier portant son nom).

Le courrier est composé de trois parties
1. L'enveloppe : les champs From et To
2. Les en-têtes
3. Ils sont utilisés par les MTA et MUA. On voit le nom du MUA (Eudora sa version..), le nom des différents MTA ..X-Mailer, Subject, Message-id, Date, Reply-to, Received

Le corps du message

Les MX records
Certaines machines ne sont que des pseudos de messagerie, les MTA demandent les MX records au DNS pour déterminer ou envoyer le courrier. S'il n'existe pas de MX records, on transfère directement sur la machine.

[48] Aucune vérification n'est faite sur l'origine. On peut se faire passer pour n'importe qui !.

S'il existe plusieurs MX sur la même machine, on prend celui de plus petit rang. Si celle ci est en panne, on appelle la machine de rang au dessus. [49]

MIME Multipurpose INTERNET Mail Extension (RFC 1521)
5 nouveaux champs d'en-tête
Mime-Version :
Content-Type : TEXT/PLAIN ; charset=US-ASCII ou iso-8859-X
Content-Transfer-Encoding : 7bit ou quoted-printable ou base64 ou 8 bit ou binary
Content-ID :
Content-Description :

Ces en-têtes permettent entre autre de définir le type du corps message, son codage etc. Si ESMTP est utilisé on devrait avoir comme encoding 8 bits. Sinon le message est transféré en quoted printable ou é devient =E9. Le MUA va convertir cela automatiquement car il comprend mime la plupart du temps.

Le transfert de fichier via SMTP
Beaucoup de gens l'utilisent car aucun mot de passe n'est demandé. Cependant contrairement à FTP, il y a des contraintes , longueur de la ligne, ligne contenant un point unique. Du coup pour transférer des fichiers , on est obligé de coder les données suivant différentes méthodes (Base64, Mime, uuencode). C'est une suite de lignes lisibles qui constitue le fichier. Le MUA décodera suivant les déclarations d'en-tête.
On voit tout de suite que ces codages grossissent les fichiers à transmettre et il faut éviter de faire circuler des courriers trop gros. De nombreux administrateurs limitent la taille des messages pour ne pas recevoir des fichiers de plusieurs dizaines de Méga-octets qui bloqueraient le spool (la zone de réception des courriers).

Le cryptage et la signature
Certains courriers peuvent être cryptés et signés électroniquement. C'est une application externe qui fait cela. En France, c'est interdit. La prochaine loi permettra de signer électroniquement librement, et de crypter en déposant sa clé dans un organisme agréé.
Les signatures électroniques sont particulières, elles englobent le contenu du courrier . Si celui-ci change, la signature n'est plus valable. C'est mieux qu'une signature manuelle !.
On a deux clés, une clé privée et une publique. La clé publique sert à vérifier la signature du message mais ne peut pas permettre d'en créer un. La clé privée gardée secrète par l'émetteur lui permet de fabriquer la signature. Toute modification du texte produit une falsification de la signature.
Un des produits employé sur INTERNET s'appelle PGP (Pretty Good Privacy).

IMAP
Une version de POP qui gère la boite aux lettres utilisateur sur un serveur. Les messages restent stockés et organisés sur les serveur et non pas rapatriés en local. C'est encore peu utilisé.

SPAM
Les administrateurs protègent de plus en plus les serveurs SMTP contre l'envoi de messages anonymes. Des gens peu scrupuleux inondent des millions d'utilisateurs de leurs messages personnels. Des listes noires ont été mises en place pour les bannir. De plus les serveurs refusent de relayer du courrier pour des machines en dehors de leur domaine.

A retenir
La messagerie dans l'INTERNET est peu sécurisée et est très sommaire (pas d'accusés de réception). Mais ça marche !.

[49] La machine qui prend le relais n'a pas besoin d'avoir les mêmes comptes utilisateurs. Celle-ci ne gère qu'une file d'attente et enverra le courrier au vrai serveur lorsque celui-ci aura redémarré.

TELNET et RLOGIN
L'émulation de terminal

RLOGIN est une émulation de terminal disponible sous Unix, elle est très sommaire et transmet peu de variables de l'environnement utilisateur. **TELNET** est moins spécialisé Unix, il évolue régulièrement et possède toute une phase de négociation d'options ce qui lui permet de coopérer avec des systèmes différents et des versions moins évoluées.
Le principe général est que tout caractère frappé au clavier est transmis au site distant qui va décider de l'afficher ou bon lui semble sur l'écran. La souris n'existe pas. Celle-ci est gérée par les terminaux graphiques comme XWINDOW. On utilise le bit PSH de TCP pour envoyer le caractère.

Les commandes
Elles sont transmises dans le flot de données par l'intermédiaire du caractère 0xFF (255). Pour envoyer FF, on l'envoie deux fois. L'octet suivant est une commande. Parmi celles-ci :

EOF	236	Fin de fichier
SE	240	Fin de sous option
BRK	243	Break (suite à CtrlC)
SB	250	Début de sous Option
WILL	251	
WONT	252	
DO	253	
DONT	254	
IAC	255	Interpret as Command

Les négociations d'options sont transmises par IAC suivi de WILL,DO,WONT,DONT puis de l'identificateur d'option.

1	Echo
3	suppress go ahead
24	Terminal type
31	window size
34	linemode
36	Variables d'environnement

Les modes de fonctionnement
1 Semi Duplex (abandonné)
2 Un caractère à la fois (comme RLOGIN)
3 Une ligne à la fois
4 Mode Ligne (1990)

TELNET utilise très peu le mode Urgent TCP, contrairement à RLOGIN. Le CtrlC est transmis par un <IAC><IP>

Voici les couches traversées par un pauvre petit caractère..

Utilisateur ➔ Terminal Driver ➔ Client TELNET ➔ Session TCP/IP port 23 ➔ Serveur TELNET ➔ Terminal Driver ➔ Application
Idem pour le sens du retour.

Grâce à TELNET, on peut exécuter des commandes à distance. On peut sélectionner un numéro de port TCP pour faire des test. C'est un outil irremplaçable, qui manque beaucoup sous WindowsNT/95.

NFS et les RPC

NFS et RPC sont des développements de la société SUN qui ont été repris amplement par la suite. Tout système Unix supporte ces protocoles. NT supporte aussi RPC (mais pas NFS). DCE (Environnement Informatique Distribué) est un équivalent en mieux des RPC, mais est moins « distribué » au sens propre. Il faut l'acheter , il n'est pas en standard dans le système la plupart du temps.

L'avantage des RPC

- Le programmeur écrit juste un programme client et des procédures serveur appelées par le client
- Si UDP est utilisé, les TimeOut et retransmissions sont gérées par les RPC
- Les RPC permettent une traduction des différentes façon de coder l'information.

Bien évidemment la façon de programmer en RPC est très différente de la programmation habituelle des sockets

En appel

En-tête IP	20
En-tête UDP	8
Identificateur Transaction XID	4
appel (0) / Réponse (1)	4
Version RPC (2)	4
Numéro de programme	4
Numéro de version	4
Numéro de procédure	4
crédits	...
vérificateur	...
Paramètres de procédure	Dépend de la procédure

En réponse

En-tête IP	20
En-tête UDP	8
Identificateur Transaction XID	4
Réponse (1)	4
statut (0) accepté	4
Vérificateur	>400 octets
statut	4
Résultat de la procédure	....

Les RPC utilisent une technique pour enregistrer les ports associés aux procédures. Sous UNIX, il s'agit du démon Portmapper (Port 111) . Les programmes serveur RPC s'enregistrent auprès du **portmapper**, ils enregistrent le numéro du programme , le numéro de version ainsi que le numéro de port sur lequel ces procédures attendent le client. Sous Unix, la commande ***rcpcinfo -p*** indique les procédures enregistrées.
NFS est un protocole qui permet le partage des fichiers entre deux ordinateurs, on trouve NFS plutôt sur les sytèmes Unix.

Habituellement, on trouve 3 serveurs :

- mountd qui sert aux demandes de montage de fichiers (autorisations) port 702 (habituel). Mountd va répondre à une commande du style ***mount news :/pub/pub/linux/redhat /mnt*** .Celle ci va monter le système de fichier de la machine news sous le répertoire /mnt. Sous Unix cette commande est une commande privilégiée. Il faut avoir les droits de root (on est multi utilisateur..). Mountd transmet au système client un handle de système de fichier. Celui ci sera utilisé lors des échanges suivants.
- lockmgr verrous sur les fichiers NFS
- nfs démon qui va servir les fichiers (port 2049 souvent)

commandes ***mount*** et ***showmount***
NFS a une quinzaine de procédures qui sont parmi d'autres LOOKUP, READ, WRITE..
Par mesure de sécurité, les accès NFS (lorsque celui-ci est utilisé) doivent être filtrés sur les routeurs.

Les NEWS permettent aux utilisateurs de l'INTERNET de participer à des discussions (sous forme écrite), on parle d'articles comme élément d'échange. L'organisation qui gère les NEWS s'appelle USENET.

Les NEWS ne transitent pas par les messageries des utilisateurs (heureusement). Ces NEWS sont alimentés par des clients connectés sur des serveurs de NEWS. Ces serveurs vont véhiculer l'information de proche en proche. Chaque serveur ayant un ou plusieurs collègues.
L'organisation entre serveurs n'est pas hiérarchisée, un article peut arriver plusieurs fois. Chaque article a un numéro de série lié au serveur initial qui l'a reçu.
Le serveur reçoit l'article et garde une base de donnée indiquant qu'il a bien reçu cet article. Si l'article apparaît une nouvelle fois, celui-ci est ignoré.
Les **articles sont purgés** régulièrement suivant la place disque disponible. Chaque jour, notre serveur reçoit plus de ½Go d'articles.
Ces articles sont organisés en conférences elle mêmes organisées en hiérarchies.
Par ex
fr.comp.os.linux veut dire France / ordinateur / système / linux
fr.rec.cuisine France / divers / Cuisine

Ces conférences sont crées par des votes, chaque hiérarchie étant sous la dépendance d'un administrateur qui va générer des messages pour créer des nouvelles conférences.
Ceci ressemble un peu à l'organisation des DNS

comp ordinateurs
sci science
rec divers
..
fr
de
uk
etc..

alt est une hiérarchie particulière car la création des groupes est libre. Ce qui favorise bien des groupes nazis, pédophiles.. etc. C'est une des raisons pour laquelle le réseau des Universités ne véhicule plus alt.

Les NEWS utilisent le port TCP 119.
Les machines qui se connectent au serveur sont filtrées en fonction de leur adresse IP.
Comme logiciel client, Netscape Navigator ou INTERNET Explorer font très bien l'affaire

LES IRC
INTERNET Relay Chat
Bavardage (ou drague) INTERNET.
Les IRC permettent les discussions en direct à plusieurs. Les gens se connectent à un serveur sur une réunion particulière. Tout message tapé sera reçu immédiatement par l'ensemble des utilisateurs de ce groupe. Ca n'a que peu d'intérêt professionnel, mais ça a un gros succès auprès de ceux qui ont du temps à perdre.

Les listes LISTSERV / TULP / MAJORDOMO[50]
Ces listes existaient sur le réseau BITNET qui a disparu depuis peu. LISTERV est une application intéressante qui a été reprise.
C'est un moyen de créer des conférences qui passent par la messagerie. C'est un bon moyen pour un petit groupe d'individus de se transmettre des informations.

[50] LISTSERV était utilisé sur le réseau IBM BITNET. TULP et MAJORDOMO sont d'autres « produits » issus de LISTSERV

Un logiciel spécial va traiter des courriers qui arrivent à des utilisateurs fictifs. LISTSERV (ou MAJORDOMO ou SYMPA[51]) est l'utilisateur auquel on envoie des commandes.

Mail **listserv@machine.domaine**
Tout message envoyé à listserv sera considéré comme une commande
type de commandes tapée dans le corps du message

help	aide
sub liste dupont frederic	on s'abonne
rev liste	qui est abonné à la liste
ind liste	Liste des fichiers associés à la liste
ind	liste des listes
get liste fichier	retrouve un fichier
signoff liste dupont frederic	on se désabonne

Listserv va utiliser le champ From du message pour expédier les messages de la liste aux membres. Il faut donc se méfier et utiliser son vrai compte de messagerie. Certaines listes sont privées, l'administrateur ajoute à la main les utilisateurs et parfois les messages[52] .
Pour envoyer un message dans la liste.

mail liste@machine.domaine

ATTENTION, NE PAS LE FAIRE QUAND ON EST PAS ABONNE, par respect envers les membres de la liste.

Une liste des listes francophones :
http://www.cru.fr/listes

[51] Hélas pas de normes de ce coté là. Gérer des milliers de comptes avec des gens qui s'abonnent partout et sans retenue est un véritable casse tête pour les administrateurs !.
[52] On appelle ça un modérateur . Dans le système des NEWS, ça existe aussi

WEB (World Wide Web)
HTTP (Hyper Text Transfer Protocol)

Le WEB, c'est l'application qui a « vendu » le réseau INTERNET qui jusque là n'était prisé que de quelques initiés. Pourtant ce développement récent, est dû au CERN, Centre Européen de la Recherche Nucléaire.
Le principe est de transmettre par le réseau des documents hypertexte, contenant des images, des liens, etc, un peu comme le help de windows ou hypercard de Apple.

Une normalisation d'adressage des différents services de TCP/IP a été crée de manière à banaliser l'accès aux services au travers d'un browser ou butineur (terme proposé en français).
Parmi ceux-ci on peut citer Netscape, INTERNET Explorer, Mosaic (l'ancêtre).
Format du lien HTML
Service : // adresse INTERNET FQDN / nom du fichier ou de l'objet

ftp ://ftp.news.univ-aix.fr/pub/pc/win95	Donne accès en anonyme au serveur ftp dans le répertoire win95
news ://news.univ-aix.fr/fr.comp.os.linux	Accès à la conférence fr.comp.os.linux
http ://www.microsoft.com/support	Accès à la page support de MICROSOFT
http :///c/mapage.html	idem sur le disque C local

HTTP est Hyper Text Transport Protocol , HTML le langage des pages Hyper Text Markup Language
Pour http, le langage des documents s'appelle le HTML, il existe un certains nombre d'outils pour créer ces pages
Hot Dog pro, NetScape, Adobe PageMil, MICROSOFT FrontPage.
..
Ce sont des fichiers texte lisibles, et un bon spécialiste peut écrire directement en HTML. Bref ce qui vend le mieux le réseau est peut être une des applications les plus triviales.

Chaque page est transmise par une session TCP port 80 qui est fermée à la fin de la réception. Le clic sur une information hypertexte est purement local et va directement au serveur concerné, on ne repasse pas par le même serveur.
L'information trouvée est mise en cache localement. De plus en plus , on utilise des serveurs intermédiaires pour faire des caches au niveau d'un très grand nombre d'utilisateurs. En cliquant sur une information située aux Japon, on a de bonne chance de l'avoir dans un cache régional ou national. Ces caches sont activés de manière transparente (fonction **HTTP PROXY**). L'adresse URL est passée en texte au serveur PROXY qui résoudra la requête. On atteint parfois 25% de succès. Une fois sur 4 la page est déjà dans le cache.

Les suites de HTTP/HTML
Le business étant rentré dans les protocoles INTERNET , les choses avancent très vite mais de façon plus désordonnée. Auparavant beaucoup de développements étaient dus à des organismes de recherche sans soucis de rentabilité ou de compétition.
Le WEB permet aussi de passer des données à un serveur qui va construire une page HTML constituant la réponse (cgi-bin). Ceci est un peu limité car on ne peut pas faire exécuter un programme au client. Plusieurs développements ont eu lieu ces derniers temps.
SUN , société qui vend et fabrique des stations de travail sous Unix a crée un nouveau langage et concept de réseau : **JAVA** Ce langage est de type C++ et le programme est envoyé au client qui l'exécute ensuite. Il existe des compilateurs qui vont créer un pseudo-code JAVA qui sera interprété dans la machine distante.
MICROSOFT met en avant **ActiveX** qui est du même style mais très dépendant de Windows et de la plate forme Intel. D'ou problème pour faire tourner l'application sur un Mac ou une station Unix.
NETSCAPE fournit aussi **JavaScript** qui n'a rien avoir avec Java et permet de développer dans un langage interprété assez simple.
La plupart des browsers sont plus ou moins compatibles avec ces langages.
De toute façon le choix sera fait par les développeurs, mais MICROSOFT risque d'avoir une longueur d'avance car INTERNET Explorer est inclus dans les dernières versions de Windows.

LA PROGRAMMATION DES SOCKETS

Ceci est un résumé sur les principes généraux. Il existe des livres que sur cette programmation, mais comme souvent le détail masque la limpidité de la philosophie.
L'Université de Berkeley a défini il y a quelques années , un standard de communication entre programmes, celui-ci devant être indépendant du système et fonctionner en réseau. Cette interface de programmation a eu un grand succès et est utilisée sur de nombreux systèmes en dehors du monde Unix. Les micro-ordinateurs ont aussi cette interface de programmation. Chez MICROSOFT, on parle de winsock (les sockets de Windows)
Les sockets utilisent un concept de tube nommé et constitue un généralisation de la méthode d'accès aux fichiers sous Unix. Une socket (ou prise traduit littéralement) défini une extrémité de la connexion.

Créer une prise (socket) :

descripteur = socket (af , type , protocole)

af défini une famille de protocoles et peut avoir les valeurs suivantes :

AF_INET	TCP/IP
AF_PUP	Famille de protocoles Xerox
AF_APPLETALK	Apple
AF_UNIX	Unix

....

Le Type peut être

SOCK_STREAM	Type de transport connecté (TCP)
SOCK_DGRAM	Type Datagramme
SOCK_RAW	Permet d'accéder aux couches basses. Cas d'un analyseur de trames

Héritage et terminaison des sockets

Un programme Unix peut créer une tache fille par deux mécanismes, soit fork, soit exec. Dans les deux cas la tache fille hérite des sockets et fichiers ouverts par le père. Généralement dans le cas d'un serveur, le père referme la socket qu'il vient de transmettre au fils (elle reste ouverte pour le fils) et en ouvre une autre pour écouter les nouvelles connexions. Pour Windows95 ou WindowsNT, voir la programmation des threads.
Pour fermer

close (descripteur)

Pour plus de clarté on appellera le descripteur socket. Lorsque tous les processus ont fermé cette socket, la connexion est alors coupée.

Spécification des adresses locales

bind (socket , adresse-locale , longueur adresse)

cette commande permet de choisir l'interface et le port sur lequel on va recevoir les informations. Par défaut, on reçoit sur toutes les interfaces.

Connexion des sockets avec l'adresse de destination

connect (socket , adresse de destination , longueur adresse)

Emission des informations

write (socket , message , longueur) cf le write standard d'Unix

send (socket , message , longueur , drapeaux)

Cette commande permet entre autre d'envoyer des données urgentes (TCP)
Ces fonctions permettent l'émission de données sans connexion préalable.

sendto (socket , message , longueur , drapeaux , adresse destination , longueur adresse)

sendmsg (socket , structure de message , drapeaux)

Réception des informations

read (socket , réception , longueur) longueur ici évite de faire déborder la zone de réception.

recvfrom (socket , réception , longueur , drapeaux , adresse source , longueur adresse)

Cette primitive permet de connaître l'origine du message qui est renvoyée dans le champ adresse source

Renseignements sur la source

Les processus fils, n'ont pas vu la phase d'établissement de la connexion. Ils ont des primitives pour demander au système comment s'appelle leur interlocuteur ou à travers quelle interface, ils sont connectés.

getpeername (socket , adresse de destination , longueur adresse)
Ceci n'a de sens qu'avec TCP
getsockname (socket , adresse locale , longueur adresse)

Demander et définir des options de socket

Ceci permet de définir des options TCP ou IP par ex les options d'en-tête

getsockopt (socket , niveau , Nom de l'option , valeur de l'option , longueur)
setsockopt (socket , niveau , Nom de l'option , valeur de l'option , longueur)
niveau = opération sur socket ou couche de protocole

Mise en attente de connexions entrantes d'un serveur TCP

Listen permet de dire au système que l'application est prête a recevoir des appels et demande de réserver une certaine taille de file d'attente pour ses informations. C'est juste une préparation, cet appel n'est pas bloquant. La primitive accept va réaliser la dernière partie.

listen (socket , longueur file d'attente)
newsock = accept (socket, adresse , longueur adresse)

Le serveur se met en attente avec la commande accept. Le système (TCP) libère le serveur lorsqu'un appel entrant arrive et fournit une nouvelle socket. Celui ci crée un processus fils, ferme newsock qui sera possédé par le fils et retourne en état bloqué sur la fonction accept.

Accès au serveur de domaine.

Pour utiliser les primitives de base (bind , sendto , connect), il faut utiliser les numéros IP. Il existe donc des primitives pour convertir une adresse symbolique en adresse IP.

ptr = gethostbyname (nom de domaine)
obtenir le numéro IP
ptr = gethostbyaddr (adresse , longueur , type)
retourne le nom symbolique d'une adresse IP (reverse adresse)

Des informations sur la programmation des sockets sous windows :
tout sur winsock.dll
ftp://sunsite.unc.edu/pub/micro/pc-stuff/ms-windows/winsock/

Exemple de programmation par sockets tiré du livre (TCP/IP illustré Volume 1) de R Stevens
Programme pour installer un serveur sur un port (partie du programme sock) développé par Richard Stevens
source : *ftp://ftp.uu.net/published/books/stevens.tcpipiv1.tar.Z*

```
/*
 * Copyright (c) 1993 W. Richard Stevens.  All rights reserved.
 * Permission to use or modify this software and its documentation only for
 * educational purposes and without fee is hereby granted, provided that
 * the above copyright notice appear in all copies.  The author makes no
 * representations about the suitability of this software for any purpose.
 * It is provided "as is" without express or implied warranty.
 */

#include        "sock.h"

int
servopen(char *host, char *port)
{
        int                                     fd, newfd, i, on, pid;
        char                            *protocol;
        unsigned long           inaddr;
        struct sockaddr_in      cli_addr, serv_addr;
        struct servent          *sp;

        protocol = udp ? "udp" : "tcp";

                /* Initialize the socket address structure */
        bzero((char *) &serv_addr, sizeof(serv_addr));
        serv_addr.sin_family      = AF_INET;

                /* Caller normally wildcards the local INTERNET address, meaning
                   a connection will be accepted on any connected interface.
                   We only allow an IP address for the "host", not a name. */
        if (host == NULL)
                serv_addr.sin_addr.s_addr = htonl(INADDR_ANY);          /* wildcard *
        else {
                if ( (inaddr = inet_addr(host)) == INADDR_NONE)
```

```
                        err_quit("invalid host name for server: %s", host);
                serv_addr.sin_addr.s_addr = inaddr;
        }
/* See if "port" is a service name or number */
        if ( (i = atoi(port)) == 0) {
                if ( (sp = getservbyname(port, protocol)) == NULL)
                        err_ret("getservbyname() error for: %s/%s", port, protocol);

                serv_addr.sin_port = sp->s_port;
        } else
                serv_addr.sin_port = htons(i);

        if ( (fd = socket(AF_INET, udp ? SOCK_DGRAM : SOCK_STREAM, 0)) < 0)
                err_sys("socket() error");

        if (reuseaddr) {
                on = 1;
                if (setsockopt(fd, SOL_SOCKET, SO_REUSEADDR,
                                                                                (char  err_sys("setsockopt
of SO_REUSEADDR error");
        }

                /* Bind our well-known port so the client can connect to us. */
        if (bind(fd, (struct sockaddr *) &serv_addr, sizeof(serv_addr)) < 0)
                err_sys("can't bind local address");

        if (udp) {
                buffers(fd);

                if (foreignip[0] != 0) {        /* connect to foreignip/port# */
                        bzero((char *) &cli_addr, sizeof(cli_addr));
                        cli_addr.sin_family      = AF_INET;
                        cli_addr.sin_addr.s_addr = inet_addr(foreignip);
                        cli_addr.sin_port        = htons(foreignport);
                                /* connect() for datagram socket doesn't appear to al
                                   wildcarding of either IP address or port number */

                        if (connect(fd, (struct sockaddr *) &cli_addr, sizeof(cli_addr))

                                err_sys("connect() error");

                }

                sockopts(fd, 1);

                return(fd);             /* nothing else to do */
        }
        buffers(fd);            /* may set receive buffer size; must do here to get
                                        correct window advertised on SYN */
        sockopts(fd, 0);        /* only set some socket options for fd */
        listen(fd, listenq);
        if (pauselisten)
                sleep(pauselisten);             /* lets connection queue build up */
        if (dofork)
                TELL_WAIT();                    /* initialize synchronization primitives */
        for ( ; ; ) {
                i = sizeof(cli_addr);
                if ( (newfd = accept(fd, (struct sockaddr *) &cli_addr, &i)) < 0)
                        err_sys("accept() error");
                if (dofork) {
                        if ( (pid = fork()) < 0)
                                err_sys("fork error");
                        if (pid > 0) {
                                close(newfd);   /* parent closes connected socket */
                                WAIT_CHILD();   /* wait for child to output to terminal */
                                continue;               /* and back to for(;;) for another accept() */
                         } else {
                                close(fd);              /* child closes listening socket */
                 }
         }
                        /* child (or iterative server) continues here */
                if (verbose) {
                                /* Call getsockname() to find local address bound to socket:
                                   local INTERNET address is now determined (if multihomed). */
                        i = sizeof(serv_addr);
                        if (getsockname(newfd, (struct sockaddr *) &serv_addr, &i) < 0)
                                err_sys("getsockname() error");

                                        /* Can't do one fprintf() since inet_ntoa() stores
                                           the result in a static location. */
                        fprintf(stderr, "connection on %s.%d ",
                                        INET_NTOA(serv_addr.sin_addr), ntohs(serv_addr.sin_port));
                        fprintf(stderr, "from %s.%d\n",
                                        INET_NTOA(cli_addr.sin_addr), ntohs(cli_addr.sin_port));
                }
               buffers(newfd);         /* setsockopt() again, in case it didn't propagate
                                                from listening socket to connected socket */
                sockopts(newfd, 1);     /* can set all socket options for this socket */
                if (dofork)
                        TELL_PARENT(getppid()); /* tell parent we're done with terminal */
                return(newfd);
        }
```

ANALYSE DE PROBLEMES

UNIX

Les commandes suivantes sont souvent en standard sous Unix

arp –a	Correspondance adresse IP/ adresse MAC (Ethernet / TokenRing / FFDI..)
ping	teste si une machine répond aux icmp echo
host	teste la conversion adresse IP adresse symbolique FQDN
netstat	état des connexions TCP (avec -a les connexions TCP/UDP en état listen)
	-s = statistiques
rpcinfo -p	Serveurs causant Remote Procedure Call
nslookup / dig	outils DNS
showmount	clients nfs
ifconfig	Montre la configuration des interfaces
tcpdump	outil d'analyse de trames, nécessite le compte privilégié root
	tcpdump dst host and tcp port xxx
	tcpdump broadcast
	tcpdump arp
route	crée les routes , syntaxe variable suivant OS

Non standard sous Unix mais utiles.

ttcp permet de tester les performances de transfert réseau (TCP ou UDP)

bing permet de tester les vitesses de ligne entre deux machines (basé sur ICMP)

echoping teste les temps de réponse sur les ports ECHO (TCP/UDP) ou HTTP

perl Ce langage de programmation est le grand dada des adminstrateurs systèmes car il est puissant , permet de lancer des commandes, récupérer facilement les sorties, utiliser des sockets.. des librairies puissantes autour. Il est tellement bien qu'il a été porté même sous NT et W95. Un must !. On fait en 5 lignes l'équivalent de plusieurs pages de C.

DOS

Pas grand chose en standard, il faut ajouter des commandes à la couche winsock Trumpet. Il existe un très très bon shareware : **ethld200.zip**. Faire un ftpsearch (http://ftpsearch.ntnu.no). Ce produit montre à la fois des statistiques et permet de voir des détails sur chaque protocole. Il est non spécialisé IP. Il suffit d'avoir un packet driver ou le niveau ODI ou NDIS de chargé.

W95

arp -a	
ping	
netstat	
nbtstat	netbios statistiques sur IP
winipcfg	configuration IP
route	
net / ?	commandes netbios

NT

idem sauf que

winipcfg devient ipconfig Il existe donc deux équipes en concurrence acharnée chez MICROSOFT ! ! !

EXEMPLES

exemple de netstat -s sur la machine romarin.univ-aix.fr

on peut remarquer que IBM a traduit les messages de son système AIX ce qui rend la sortie particulièrement lisible.

netstat -s

```
ip:
        16606935 paquets reçus au total
        0 en-têtes de totaux de contrôle incorrects
        25 paquets avec une taille inférieure au minimum
        0 paquets avec taille de données inf. à longueur des données
        0 paquets avec la longueur d'en-tête inf. à longueur des données
```

```
        0 paquets avec la longueur des données inf. à la longueur d'en-tête
        74 fragments reçus
        0 fragments abandonnés pour double emploi ou manque de place
        0 fragments abandonnés après le délai d'attente
        0 paquets renvoyés
        10510 paquets impossibles à renvoyer
        0 redirects envoyés
icmp:
        5049 appels à icmp_error
        0 erreurs non générées parce que l'ancien message était icmp
        Histogramme en sortie:
                réponse d'écho: 2887
                destination impossible à atteindre: 2040
        29436 messages avec des zones code incorrectes
        0 messages inférieurs à la longueur minimale
        0 totaux de contrôle incorrects
        0 messages de longueur incorrecte
        Histogramme en entrée:
                réponse d'écho: 106
                destination impossible à atteindre: 67785
                source quench: 3314
                routage redirigé: 17009
                écho: 2904
                dépassement de délai: 12680
        2887 réponses à des messages générées
tcp:
        13781754 paquets envoyés
                9031491 paquets de données (-1959641964 octets)
                345648 paquets de données (128069197 octets) retransmis
                2494766 paquets d'URG uniquement
                0 paquets d'URG uniquement
                281375 paquets d'investigation (probe) de fenêtre
                700810 paquets de mise à jour de fenêtre
                927664 paquets de control
        11614359 paquets reçus
                6051908 ACK (pour -1970016459 octets)
                460169 ACK dupliqués
                34 ACK pour des données non envoyées
                5107411 paquets (1353166444 octets) reçus en séquence
                251900 paquets dupliqués (57456432 octets)
                1296 paquets avec des données dupliquées (180514 octets en double)
                429080 paquets hors séquence (115471206 octets)
                116 paquets (2051 octets) de données après la fenêtre
                7 investigateurs (probe) de fenêtre
                179286 paquets de mise à jour de fenêtre
                1930 paquets reçus après close
                totaux de contrôle incorrects: 10974 mis au rebut
                zones de décalage de l'en-tête incorr.: 3 mis au rebut
                paquet trop court: 14 mis au rebut
        177645 demandes de connexion
        416593 acceptations de connexion
        476097 connexions établies (acceptations comprises)
        637903 connexions terminées (dont 195175 connexions rejetées)
        134851 connexions à l'état embryonnaire rejetées
        4564158 segments rtt mis à jour (4907399 tentatives)
        610406 timeouts de retransmission
                4653 connexions coupées par timeout de retransmission
        282373 timeouts persistants
        23069 timeouts keepalive
                875 keepalive probes envoyés
                13850 connexions coupées par keepalive
udp:
        0 en-têtes inachevés
        3 zones de longueur de données incorrectes
        51 totaux de contrôle incorrects
        14247 socket buffer overflows

news:~# ping ftp.ibp.fr
PING pascal.ibp.fr (132.227.60.2): 56 data bytes
64 bytes from 132.227.60.2: icmp_seq=0 ttl=51 time=47.0 ms
64 bytes from 132.227.60.2: icmp_seq=1 ttl=51 time=49.8 ms
64 bytes from 132.227.60.2: icmp_seq=2 ttl=51 time=103.4 ms
64 bytes from 132.227.60.2: icmp_seq=3 ttl=51 time=44.9 ms

--- pascal.ibp.fr ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 44.9/61.2/103.4 ms



news:~# traceroute ftp.ibp.fr
```

```
traceroute to pascal.ibp.fr (132.227.60.2), 30 hops max, 40 byte packets
 1  cisco-cdc1.univ-aix.fr (193.50.125.1)  1.127 ms  1.141 ms  0.995 ms
 2  193.50.124.2 (193.50.124.2)  1.992 ms  2.561 ms  2 ms
 3  aix.r3t2.ft.net (193.48.48.49)  4.211 ms  4.206 ms  4.162 ms
 4  marseille2.r3t2.ft.net (193.48.48.37)  7.147 ms  6.911 ms  6.872 ms
 5  marseille1.r3t2.ft.net (193.48.48.81)  89.561 ms  48.06 ms  124.761 ms
 6  marseille.RENATER.ft.net (193.48.48.249)  17.267 ms  11.785 ms  8.554 ms
 7  stamand1.RENATER.ft.net (195.220.180.89)  22.765 ms  20.461 ms  22.064 ms
 8  stamand3.RENATER.ft.net (195.220.180.41)  34.804 ms  24.147 ms  49.075 ms
 9  stlambert.rerif.ft.net (195.220.180.10)  20.431 ms  23.835 ms  21.171 ms
10  danton1.rerif.ft.net (193.48.53.50)  20.547 ms  28.044 ms  23.968 ms
11  u-jussieu-paris.rerif.ft.net (193.48.58.122)  32.367 ms  22.945 ms  24.1 ms
12  r-jusren.reseau.jussieu.fr (192.44.54.126)  22.256 ms  31.718 ms  47.724 ms
13  r-ibp.reseau.jussieu.fr (134.157.254.250)  33.582 ms  29.909 ms  57.689 ms
14  pascal.ibp.fr (132.227.60.2)  54.88 ms  73.052 ms  52.783 ms
```

On traverse donc 13 routeurs pour aller sur la machine ftp.ibp.fr

netstat sous windows95

L'option -a de netstat indique les ports en attente de connexions

```
C:\WINDOWS>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    pc-lalot:1025          news:nbsession         ESTABLISHED
Connexion en mode client de serveur de fichiers microsoft/netbios sur news
  TCP    pc-lalot:6000          news:1641              ESTABLISHED
  TCP    pc-lalot:6000          news:1174              ESTABLISHED
  TCP    pc-lalot:6000          news:1184              ESTABLISHED
  TCP    pc-lalot:6000          news:1531              ESTABLISHED
Connexions XWindow
  TCP    pc-lalot:1210          inet1.tek.com:80       CLOSE_WAIT
  TCP    pc-lalot:1211          inet1.tek.com:80       CLOSE_WAIT
Connexions Web
  UDP    pc-lalot:talk          *:*
  UDP    pc-lalot:ntalk         *:*
  UDP    pc-lalot:177           *:*
  UDP    pc-lalot:nbname        *:*
  UDP    pc-lalot:nbdatagram    *:*
Ports UDP en écoute
```

Statistiques netbios

nbtstat -s

```
NetBIOS Connection Table

Local Name             State    In/Out  Remote Host           Input   Output
-------------------------------------------------------------------------------
LALOT          <00>  Connected  Out   NEWS           <20>   894B     792B
LALOT          <03>  Listening
```

dig ftp.cica.indiana.edu

```
; <<>> DiG 2.1 <<>> ftp.cica.indiana.edu
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; Ques: 1, Ans: 2, Auth: 3, Addit: 3
;; QUESTIONS:
;;      ftp.cica.indiana.edu, type = A, class = IN

;; ANSWERS:
ftp.cica.indiana.edu.   50400   CNAME   cica.cica.indiana.edu.
cica.cica.indiana.edu.  50400   A       129.79.20.27

;; AUTHORITY RECORDS:
cica.indiana.edu.       50400   NS      ns.indiana.edu.
cica.indiana.edu.       50400   NS      ns2.indiana.edu.
cica.indiana.edu.       50400   NS      argus.cso.uiuc.edu.

;; ADDITIONAL RECORDS:
ns.indiana.edu. 50400   A       198.88.18.1
ns2.indiana.edu.        50400   A       198.88.19.1
argus.cso.uiuc.edu.     86400   A       128.174.5.58

;; Total query time: 4203 msec
;; FROM: news to SERVER: default -- 193.50.125.2
```

```
;; WHEN: Tue Jan 21 12:05:11 1997
;; MSG SIZE  sent: 38  rcvd: 201
```

rpcinfo -p

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp    779  mountd
    100005    1   tcp    781  mountd
    100003    2   udp   2049  nfs
    100003    2   tcp   2049  nfs
```

showmount -e ftp.univ-aix.fr

```
Export list for news.univ-aix.fr:
/pub/pub (everyone)
```

LES RESEAUX LOCAUX DE PC

Apple a vers le milieu des années 1980 été le premier à concevoir et à developper son réseau. Il a utilisé une technique, le CSMA-CA qui est un peu ressemblant à ETHERNET sur des paires métalliques normales (localtalk). Le débit de ce réseau est de 250 Kb/s. Le connecteur était très peu cher (400Fr). Le réseau permettait le partage des imprimantes à une époque où une imprimante Laser valait très cher. Ce service ainsi que la simplicité du système a fait le succès d'Apple.
Depuis, Apple a adopté ETHERNET (ethertalk) ,TokenRing (tokentalk). Pour les protocoles de plus haut niveau, Apple a développé le strict minimum concernant INTERNET, n'a pas cherché à développer un support natif Netbios. Apple a pris beaucoup de retard ces derniers temps dans le domaine des réseaux.

Les PC sont restés assez longtemps sans réseau. Il a fallu attendre la fin des années 80 pour voir une société (NOVELL) proposer enfin des serveurs de fichiers et d'impression (Netware) et des couches réseau sur les PC en MS/DOS. Quelques temps après MICROSOFT et IBM ont suivi le pas et ont proposé leurs solutions (Netbios et Lan Manager). Le serveur tournait sous OS/2.
Cette époque a été l'objet de tâtonnements et au bout de quelques temps les principaux acteurs ont défini des couches de protocoles de liaison réseau pour les machines clientes sous MS/DOS. Le but étant de donner une interface homogène au dessus de la carte réseau et de permettre de gérer du **Multiprotocole**. Par exemple sur la même machine pouvoir utiliser SNA (IBM), LANMAN, NOVELL, TCP/IP en même temps.

Pour NOVELL cette interface s'appelle **ODI** (OPEN DATA LINK INTERFACE)
MICROSOFT a proposé avec 3Com **NDIS** (Network Driver Interface Specification)
Les cartes réseau du marché sont donc vendues avec des drivers compatibles avec ces normes

Les packets drivers
L'université de Clarkson a normalisé une interface et a développé, une série d'outils pour faire de l'INTERNET (FTP et TELNET ping..). Ces drivers ont encore de temps en temps sur des machines MS/DOS leur utilité. Cependant plutôt que d'utiliser le packet driver spécifique de la carte, on peut utiliser le packet driver qui s'appuie sur les couches ODI et NDIS . odipkt.com ou ndispkt.com. Ceci s'est fait avant les normes NDIS et ODI.

Les types de réseau locaux de PC

On trouve deux types : le réseau poste à poste et le réseau Serveur Client.

- **Les SERVEURS**

Un serveur est une machine du réseau sur laquelle on enregistre des noms d'utilisateurs avec des mots de passe. C'est le cas de NT Server et de Netware. Les utilisateurs à partir de leur PC vont se connecter sur le serveur en tapant leur nom et leur mot de passe. Le serveur exécute un script qui va lancer des commandes, attacher des lecteurs réseau au poste local. L'utilisateur pourra alors accéder les données du serveur en fonction des droits donnés par l'administrateur. Généralement ces serveurs ont des groupes d'utilisateurs. L'appartenance à ces groupes donnent des droits sur les fichiers et les imprimantes.

- **Les DOMAINES**

Les choses se compliquent lorsque l'on installe plusieurs serveurs. En effet pour avoir accès à plusieurs ressources du réseau, il va falloir se connecter plusieurs fois, avec des mots de passe différents.. Pour résoudre ces problèmes, on a inventé une couche supérieure. NOVELL appelle cela **Netware Directory Services** alors que MICROSOFT parle de **domaines**. En fait tout ceci existait sous Unix , c'est une fonctionnalité que l'on appelait les **pages jaunes**, devenues depuis NIS.
Le principe est simple. Un serveur central est maître de l'annuaire des utilisateurs. Celui ci communique avec les machines clients de son domaine pour indiquer que la station X correspond à l'utilisateur Y. Ainsi par une seule connexion, l'utilisateur aura accès à toutes les ressources (machines imprimantes..) du domaine

- **Le POSTE à POSTE**

Un serveur, ça coûte cher. Beaucoup de petits sites n'ont pas les moyens ni parfois les compétences pour installer un serveur . Depuis Windows pour Workgroups, MICROSOFT fournit en standard ses logiciels clients avec la possibilité de faire du poste à poste. Chaque poste peut ainsi mettre en partage son

imprimante ou ses fichiers. Ce partage se fait par mot de passe sur chaque poste. Il est bien évident que dès que le nombre de postes augmente, le nombre de mots de passes à retenir devient énorme (2 à 3 par poste).
Afin de faciliter l'utilisation du réseau dans ces cas là, MICROSOFT a mis en place une technique très discutable qui consiste à conserver sur le poste les mots de passe servant à l'utilisation du réseau. C'est pour cela que dès que l'on installe le support du réseau, W95 et WfW demandent un nom utilisateur.
Ce nom va servir a stocker les mots de passe dans un fichier **nom.pwl**. Ainsi l'utilisateur utilisant le même nom et le même mot de passe n'aura plus à taper tous les mots de passe. Les connexions seront automatiques.
On peut simplement noter que cette technique est très mauvaise sur le plan de la sécurité . Un programme permet de décrypter instantanément le mot de passe !.
Le poste à poste amélioré : Si on possède un serveur, on peut partager son disque ou son imprimante non plus avec un mot de passe mais par rapport à un utilisateur ou groupe d'utilisateurs du domaine.

Les protocoles de liaison classiques
Trames encapsulées dans ETHERNET ou TOKEN-RING
On va trouver

NetBEUI.	Ce sont des trames utilisables pour le protocole NetBios (en voie de disparition).
TCP/IP	Netbios et les applications INTERNET. Nomé DoD TCP/IP[53]
DLC	utilisé par SNA.
IPX/SPX	Utilisé par NOVELL mais aussi par Netbios.

On voit que Netbios passe partout. Netbios est une API de transport développée par MICROSOFT et IBM, un peu comme les sockets

Les couches NOVELL sur un PC client

Couches NOVELL	Définition
LSL	Link Support layer
Driver de carte ODI	ODI
IPXODI	Couche IPX sur ODI
VLM ou NETX	Virtual Loadable Module

Le réseau MICROSOFT
L'histoire de MICROSOFT est lié à **netbios**, les serveurs de MICROSOFT ont évolué en passant de OS2 à WindowsNT pour des raisons stratégiques. Mais le protocole reste le même. Cependant, MICROSOFT a fait un effort en direction de TCP/IP ce qui permet d'utiliser facilement les protocoles au travers d'une interconnexion INTERNET.

Les noms de fichier UNC NETBIOS
Pour un réseau, les noms de fichiers MSDOS sont peu pratiques, car un fichier est désigné par ce genre de syntaxe : **lecteur:\répertoire\fichier**
Or une machine ne peut avoir que 26 lecteurs (de A à Z), c'est donc plutôt limité
Les noms UNC sont fabriqués ainsi : **\\serveur\partage\repetoire\fichier**
à noter que pour NOVELL , c'est : /serveur :volume\repertoire\fichier
Ceci évidemment n'a rien à voir avec le WEB ! ! ! (mais ça aurait pu)
Le nom du serveur en netbios est limité à 15 caractères.

Ceci permet d'appeler un fichier sur n'importe quel serveur sans lui donner une lettre de lecteur et donc de connecter un lecteur (à partir du moment ou l'on a les droits)
NB : certaines commandes ne connaissent que netbios d'autres que TCP/IP. Par conséquent si TOTO est le nom netbios de la machine titi.domaine.fr
ping titi.domaine.fr marche mais ping TOTO ne marche pas car ping utilise l'API Winsock
idem à l'envers pour la commande net

Les noms de machines, les groupes de machines

[53] DoD Department of Defense. Le bailleur de fond du projet TCP/IP. Lorsque l'on installe les couches TCP/IP sous W95 ou NT, il faut chercher Microsoft TCP/IP (le propriétaire a du changer ?).

Si je désire partager des informations avec d'autres utilisateurs, il faut que ceux-ci puissent découvrir ma machine. La plupart du temps, les serveurs de réseaux locaux utilisent la diffusion d'informations périodiques par l'intermédiaire de broadcasts. Au début, tous les serveurs faisaient des broadcasts et la situation allait en empirant car tout PC a maintenant la possibilité de faire du partage en poste à poste et non plus en client et serveur central. 1000 machines faisant des broadcasts, c'est mille personnes qui crient sur le réseau. En gros, on passe son temps à frapper à votre porte.

Il a donc fallu créer des groupes de machines. Chaque machine fait partie d'un groupe. La première qui crée un groupe va répondre aux demandes d'enregistrements dans le groupe. Ainsi au début la machine diffuse sa demande, le gestionnaire du groupe l'enregistre en vérifiant l'unicité du nom de machine. Après , c'est le gestionnaire qui diffusera et lui seul régulièrement l'information sur le groupe. En cas d'arrêt, un mécanisme d'élection redéfini l'enregistreur. Ceci dit tout ça ne marche qu'a condition de ne pas avoir de machines sur des réseaux différents où les routeurs vont bloquer l'information. Ils filtrent les broadcasts.

Pour passer cette barrière , il faut utiliser **WINS** (Windows Name Server). WINS est un service qui tourne sur un serveur NT. Dans la configuration TCP/IP des clients Windows, on indique l'adresse IP du serveur WINS. Ainsi pour le parcours du réseau, la découverte des serveurs passera par une demande au serveur WINS. Lors du démarrage de la machine client, celle-ci fournit a WINS son nom et son groupe. WINS l'enregistre dans sa base automatiquement.

Certains Types de noms de machines (codes affichés par nbtstat)

00	Station
03	Service de message
20	Serveur
BE	Moniteur réseau
1B	Maître explorateur de domaine
1D	Maître Explorateur

Types de groupes

00	membre d'un domaine ou groupe de travail
1C	Contrôleur de domaine
1^E	Accepte d'être explorateur

La résolution des noms.
Le résolveur IP des machines windows peut utiliser Netbios et WINS pour la résolution de noms, d'habitude sur les autres systèmes, seul le DNS est contacté.
Sur l'ordinateur, il existe des commandes orientées netbios et d'autres winsock. Leurs comportement différent sur les noms de machines. Netbios limite le nom à 15 caractères et celui ci n'est pas hiérarchisé comme pour winsock et le DNS.

Voici comment les applications utilisent les noms

Etapes traversées pour la résolution Winsock

Fichier hosts ?
DNS ?
<15 Caractères
WINS ?
Diffuser 3 fois la demande
Fichier LMHOSTS ?
échec ?

Pour NetBios attention les comportements de W95 et NT ne sont pas identiques

WINS ?
3 Diffusions
LMHOSTS ?
DNS ?
HOSTS ?
échec ?

Les commandes (DOS) de réseaux locaux de PC

NOVELL

NOVELL avait conquis une grosse partie du marché des serveurs. Cependant MICROSOFT a repris celui-ci. L'avantage majeur de NOVELL Netware est surtout qu'un simple PC sous DOS permet d'administrer les serveur. De plus on peut avoir accès à la console du serveur à distance. Seul inconvénient, le serveur est un système propriétaire sur lequel le jeu de commande est limité.
C'est exactement l'inverse pour MICROSOFT.

LOGIN SERVEUR/NOM	Connexion au serveur
MAP k :=serveur/volume	Attacher un lecteur au poste
SLIST	Liste des serveurs
USERS	Liste des utilisateurs sur le serveur
SYSCON	Gestion des utilisateurs
FCONSOLE	
NDIR, NCOPY	Commandes DOS modifiées pour afficher les droits
GRANT	Donne des droits sur les repertoires
REVOKE	Enlève les droits

MICROSOFT

Une seule commande, la commande NET (voir aussi NBTSTAT)

NET USE * \\serveur\partage	Idem commande MAP
NET VIEW	Parcours du réseau
NET LOGON ou LOGOFF	
NET CONFIG	Visualise la configuration utilisateur

LA SECURITE

Vaste sujet que la sécurité sur INTERNET. Celle-ci va être abordée de façon succincte. En effet un livre complet pourrait ne pas y suffire. Concernant la sécurité toute entreprise un peu importante devrait avoir un expert en sécurité ou faire appel à des sociétés pratiquant un **AUDIT.** Bien entendu cette inspection doit être faite avec les pleins pouvoirs et la participation active de la direction. Dans nos campus universitaires, c'est bien là le problème. Le Monsieur Sécurité doit être un très bon spécialiste pas quelqu'un que l'on met à ce poste pour l'occuper.
Les pirates eux ne comptent pas leurs heures, ni leurs nuits et week-ends. Une bonne source d'information http://www.cert.org, site officiel de sécurité mais aussi http://www.rootshell.com et bien d'autres sites de hackers http://www.hackers.com. Pour les news : news://comp.os.security.announce. Il faut rappeler qu'au terme de nombreuses lois, le fait de pénétrer un système est passible de prison. Et sur un système bien administré, on laisse toujours des traces.

Le type des attaques.

- **Vol d'adresse IP au niveau ARP** Un serveur est arrêté et un pirate monte un cheval de Troie. Est ce j'envoie mon mot de passe à la bonne machine ?.
- **IP SPOOFING**. Changer l'adresse source d'une trame IP. Par exemple y mettre la même que la destination. Ceci ne marche que pour les applications marchant sur UDP (TFTP, DNS, NFS). Rejeté par un firewall ou routeur filtrant
- **DNS SPOOFING**. Faire croire à un DNS que l'adresse 202.15.20.5 appartient à www.maboite.com. Comme certaines sécurités se basent sur la résolution de noms.. Avoir la bonne version du démon named (appelé aussi BIND).
- **BUFFER OVERFLOW**. La meilleure de toute sur les systèmes Unix. Sur Unix, ceci conduit parfois à une prise de main de la machine. Sous NT peut faire « geler » le serveur. En fait chaque application attend du réseau des réponses probables. Exemple : un nom c'est moins de 20 caractères. Les pirates envoient des noms spéciaux qui vont bien au delà. Ils provoquent un écrasement des données et des retours de procédures pas si au hasard que cela. Par exemple forcer le lancement d'un terminal xterm. Actuellement c'est très en vogue car de nombreux programmes ne font pas de vérifications suffisantes. Le langage C qui est le langage des développeurs est très laxiste sur les chaînes de caractères, le débordement y est facile.
- **SYN/FLOOD** Saturer un serveur d'appels d'ouverture TCP incomplets.
- **PING OF DEATH**. Un ping avec plus de 60000 caractères. Provoque le plantage de plein de systèmes Mise à jour vers un système récent, ou filtre ICMP sur un firewall (réponse rapide).
- **Et bien d'autres**…

Se Protéger localement (60% des attaques sont internes...)

- Les réseaux locaux sont sensibles au piratage. Des outils sous Dos/Unix permettent facilement de lire les trames du réseau. IL faut donc impérativement remplacer les HUBS par des Commutateurs ou séparer les réseaux entre eux. Des HUBS différents pour des utilisateurs différents. Il faut noter que la seule bonne solution est le commutateur, car qui vérifiera que dans tel bureau un petit malin a mis en route un sniffer (nom donné aux programmes qui lisent les trames).[54]

Les systèmes

- **Les serveurs Unix.**

Avantages d'un serveur Unix .
20 ans de métier dans l'INTERNET, Système puissant rapide . Possibilité de tout faire à distance par un simple TELNET (ça peut être un inconvénient). Très riche jeu de commande. **On peut tout automatiser.**
Dans le cas du système **Linux**, c'est la façon la moins onéreuse et la plus performante de monter des serveurs TCP/IP. Ce système développé par des bénévoles dame le pion de bien des systèmes payants. Comme on dit : « On peut avoir moins bien, mais c'est plus cher !. »

Inconvénients d'un serveur Unix.

[54] Recherchez pour l'analyse des trames, l'excellent produit shareware sous DOS ethload (ethld200.zip)

Les privilèges dans la machine sont le superuser (root) et l'utilisateur lambda.. Hélas beaucoup de programmes pour fonctionner ont besoin un faible instant de privilèges root. Lorsque ces programmes sont mal écrits, un utilisateur du système par un simple TELNET peut devenir root. L'accès à TELNET et au langage de commande ne doit être donné qu'a des gens de confiance. Il n'est pas utile de faire du TELNET pour faire de la messagerie, du FTP ou du SQL (Base de donnée).
L'interface utilisateur n'est pas très bonne. C'est un système pour spécialiste
Faiblesse de la table des mots de passe :

Celle-ci est accessible par n'importe quel utilisateur TELNET/FTP. En principe le mot de passe doit être dans un fichier séparé possédé par root. (Shadow password). Sinon n'importe quel accès FTP utilisateur permet de récupérer la table, puis un utilitaire (Crack) permet de trouver les mots de passe simples. D'ou le conseil, celui-ci doit être long et ne pas être dans un dictionnaire.
Attention : si quelqu'un de l'INTERNET pirate le serveur, donc devient root, il pourra ensuite installer un sniffer et par conséquent lire ce qui se passe sur le réseau. On devra donc particulièrement surveiller une installation de serveur Unix.

Avez vous un bon ingénieur système Unix ?. A-t-il le temps de penser sécurité ?. Sur ce genre de serveur se trouve installé au départ un certain nombre de services INTERNET. Par exemple en standard se trouvent installé des services FTP, Sendmail, TELNET, Finger, NFS. IL est bon de regarder ce qui est utile, et de désinstaller ce qui ne sert pas. Concernant ce qui est utile, doit on ouvrir tel ou tel service à tous l'INTERNET ou juste à quelques adresses. Pour cela généralement, il est bon de regarder certains fichiers :

/etc/inetd.conf Quels services lancer (se borner à POP FTP TELNET)
/etc/hosts.allow Fichiers de configuration de TCP/Wrapper
/etc/hosts.deny
Ces fichiers indiquent quelles adresses de l'INTERNET sont autorisées à accéder à quel service. Regarder les annonces de news://comp.os.security.announce. Surveiller les logs (/var/log/secure ou/var/log/messages sous Linux)

- **Les serveurs NT**

Avantages.
Ils sont conviviaux, assez robustes (moins que Unix). On trouve beaucoup de logiciels. La prise en main est très rapide. Les configurations standard sont faciles à faire.
Inconvénients.
Lourd, gourmand en mémoire, pas facile d'automatiser des tâches car MICROSOFT n'a plus développé de commandes lignes depuis plusieurs années. Les boites de dialogue sont parfois moins compréhensibles qu'un fichier de configuration en texte clair de Unix. Le système est binaire. Tout est stocké dans des registries (mais sans commentaires..). Sortir des boites de dialogue et automatiser une installation est un problème compliqué. C'est le syndrome du clickodrome !. De plus il faut souvent redémarrer. Sous Unix, on peut changer l'adresse IP de la carte sans redémarrer.
En ce moment, il faut aussi avoir une bonne paire de basket. Car en dehors de créer un utilisateur et de manipuler le disque, il faut se déplacer pour exécuter un jeu de commandes et faire certaines manipulations.

Sécurité.
Pas d'accès de prise de contrôle distante donc moins de problèmes (mais c'est contraignant). Des attaques sur le compte de l'administrateur ont eu lieu. Les serveurs comme Samba sous Unix et dont les sources sont publics ouvrent la porte de la connaissance et celle des attaques. Suite à de nombreuses bugs de sécurité, il a fallu mettre en place des filtres pour se protéger de l'extérieur. Il faut à ce jour installer 3 services packs (par serveur NT) pour dormir tranquille.

Les Gardes barrières.

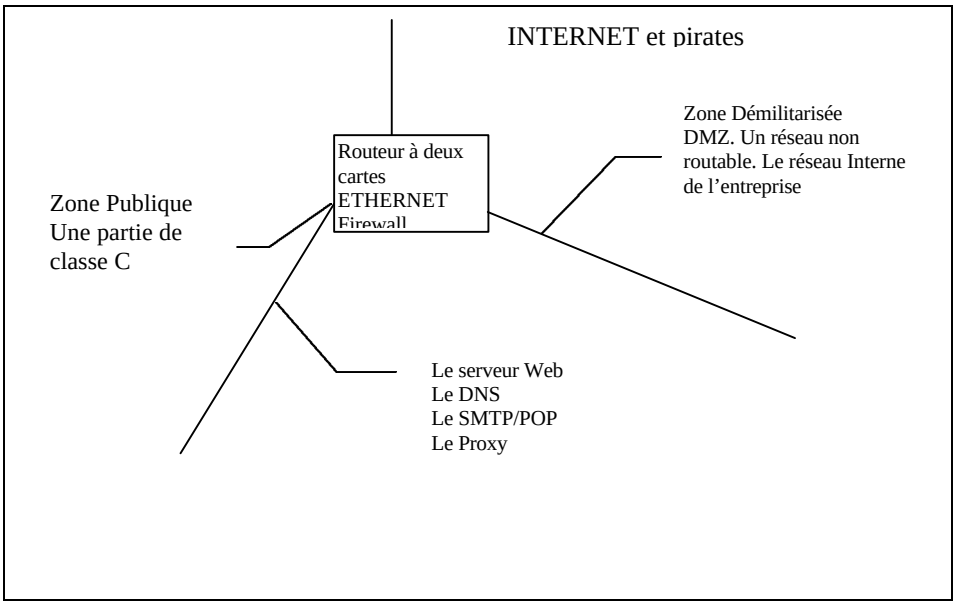
- **Les routeurs / Firewall** (ou garde barrières)
  Heureusement, ils sont là et permettent de centraliser la sécurité. On voit bien que chaque machine peut avoir ses faiblesses. En cas de problèmes, il faut pouvoir intervenir rapidement et le seul endroit ou passe toute l'information est le routeur. Ceux-ci ont maintenant des possibilités de filtrage basés sur les adresses sources et destination IP ainsi que sur les numéros de port. Il est alors possible de dire que le TELNET extérieur ne pourra pas passer : Sur un routeur CISCO par ex :
  access-list 102 deny any any eq TELNET

Ces commandes ont un sens d'application, on dit que l'access list s'applique en entrée ou sortie de l'interface. Ceci permet surtout de contrôler totalement le réseau. En effet en Interne tout le monde peut bricoler un serveur mal configuré. Grâce à la politique des Firewall, ce serveur « non déclaré » ne pourra être visible.

Les Topologies possibles de réseau

- **Bien protéger son réseau par une zone démilitarisée.**
  On ne laisse que 2 ou 3 serveurs en accès extérieurs, le reste du réseau étant dans une zone non accessible. Dans cette zone, on y met le serveur de mail, le serveur de nom, le serveur WEB, ainsi que le serveur Proxy WEB/FTP. Dans cette solution, personne ne peut en interne mettre un donnée sur l'INTERNET, accessible sur son poste . Il devra demander à l'Administrateur de la machine extérieure La zone interne, peut avoir une classe de numéro IP non accessible de l'extérieur (ex 10.0.0.0) ou (192.168.0.0) ou 172.16.0.0

  On peut même pousser le vice à supprimer la passerelle dans la configuration d'un poste et ne plus mettre qu'une route manuelle.[55]



Dans ce cas de figure, une machine du réseau DMZ ne pourra faire un ping sur l'INTERNET. Elle passera par les serveurs PROXY du réseau Public, pour faire des requêtes WEB .

De quels services faut il se méfier sous Unix.

1. Enlever tout ce qui sert à rien, surtout les démons lancés par root. Même le démon talk a eu des bugs de sécurité.
2. Eviter les rcommandes (rlogin , rsh..) basées sur la confiance en une adresse IP ou pire en un nom FQDN. Regarder les fichiers .rhosts et les enlever.
3. Enlever le shell aux utilisateurs (remplacer /bin/bash par /bin/true) dans /etc/passwd
4. Avoir un mot de passe de root long > 8 caractères et alpha numérique
5. Xwindow. Ne pas faire de commandes au hasard (xhost + par exemple). Filtrer les accés Xwindow sur le firewall (Port 6000). En effet souvent une bug de sécurité permet de lancer la commande xterm –DISPLAY=adresse IP du pirate. Et un joli shell apparaît sur le terminal X du pirate.

[55] On peut le faire avec la commande route. On le met par exemple dans autoexec.bat

6. Si par paresse « normale », vous voulez des rcommandes, fixez par la commande arp –s la correspondance adresse IP, adresse ETHERNET. Et ensuite n'autorisez que ces adresses là dans le fichier rhosts.
7. Utilisez TCP Wrapper (man tcpd ou hosts.allow hosts.deny). ce programme ajoute une vérification sur les adresses IP de tous les services.
8. Sendmail : Ce programme qui gère 80% des serveurs de courrier sur INTERNET tourne avec les autorisations root et a de nombreuses bugs de sécurité. On peut installer qmail en remplacement.
9. Pour tous les services réseaux qui sont actifs, consultez fréquemment news://comp.os.security.announce

Programmation d'un Firewall

Cisco propose une solution PIX pour faire un firewall, déchargeant ainsi le routeur. Cette solution ne s'impose que sur les gros réseaux.

Basersa sécurité sur un système étranger dont on n'a pas les sources. Est ce une bonne soultion ?. J'ai tendance à penser que les solutions freeware, Linux, FreeBSD etc.., sont plus sures. Qui peut dire s'il n'existe pas dans les routeurs Cisco ou dans les OS Microsoft des clés permettant l'espionnage. Dans ces temps de « guerre économique » mieux vaut être méfiant.

Exemple d'access lists CISCO pour filtrer des trames à l'arrivée du réseau. Cette liste simple refuse de recevoir des paquets de l'extérieur dont l'adresse source vient de chez nous. Impossible sauf si piratage extérieur. On peut voir les refus dans les valeurs matches. Pour plus d'informations : http://www.cru.fr/securite/Filtres

```
Extended IP access list 101
    deny   ip 193.50.125.0 0.0.0.255 any log (267 matches)
    deny   ip 193.50.126.0 0.0.0.255 any log
    deny   ip 193.50.127.0 0.0.0.255 any log
    deny   ip 193.50.173.0 0.0.0.255 any log
    deny   ip 194.57.187.0 0.0.0.255 any log
    deny   ip 194.57.195.0 0.0.0.255 any log
    deny   ip 193.50.174.0 0.0.0.255 any log
    deny   ip 193.50.175.0 0.0.0.255 any log
    deny   ip 194.199.116.0 0.0.0.255 any log (437 matches)
    deny   ip 127.0.0.0 0.255.255.255 any log (57 matches)
    permit ip any any (120074001 matches)
```

GERER LA PENURIE D'ADRESSE

NAT TRANSLATION D'ADRESSE

Comme on a vu précédemment, l'adressage INTERNET a de grosses limites en terme de numérotation. En fait récemment de bonnes idées ont résolu en partie ce problème. Le routeur fait de la translation d'adresse. Comment ça marche ?.
En fait on peut avoir dans les numéros IP 3 réseaux spéciaux :

Le Classe A 10.0.0.0	16 millions d'adresses
Le Classe B 172.16.0.0	65000 adresses
Les Classe C 192.168.0.0	65000 adresses

Ces adresses ne seront jamais attribuées officiellement à un réseau global de l'INTERNET. On peut sans crainte les utiliser pour construire un réseau et faire des tests ou connecter ce réseau plus tard à l'INTERNET en faisant de la translation d'adresse. On est sur que jamais www.machin.com n'aura une de ces adresses et qu'il n'y aura jamais de confusion.

Pour résoudre le problème de ces adresses non « routables », le routeur va faire la « sale besogne ». C'est-à-dire violer le principe de l'indépendance des couches. Que fait un routeur : modifier les adresses de niveau 2 et de choisir un type d'enveloppe (l'encapsulation), il ne s'occupe que des adresses niveau 2 et 3 . En fait avec NAT , le routeur travaille avec la couche 4 voire le niveau application. Tout ceci n'est possible qu'avec l'amélioration des performances hardware des routeurs. Cependant les routeurs centraux des grands carrefours ne feront probablement jamais du NAT.

Le routeur a une petite série d'adresse (Un pool d'adresses) vue de l'extérieur[56], mais comme on va le voir, une classe C suffit amplement à connecter plusieurs milliers de machines.

On distingue 3 types de configurations en fonction des services :
1. Le mappage statique pour les serveurs (DNS Web News Proxy Sendmail). C'est à dire 193.50.125.2 = 10.0.0.1. Le routeur va interchanger les adresses de niveau3

2. Le mappage dynamique
Le routeur choisit dynamiquement comme DHCP des adresses pour les machines qui veulent discuter avec l'extérieur. Le routeur surveille la fin des sessions TCP, et gère un timer pour les «sessions» UDP. Comme les machines ne sont pas toutes en discussion au même moment, on peut ainsi avec peu d'adresses faire passer beaucoup de machines. De plus si le réseau possède un serveur proxy, un DNS, un serveur de messagerie, les postes clients ne feront que peu de sessions extérieures. En ce moment, on s'aperçoit que la pénurie d'adresse est là à cause des postes clients, non des serveurs. Si on traite les postes clients avec du NAT, il existe encore pas mal de temps pour IPV4[57].

3. Le mappage des sessions TCP[58] pour le reste (lorsqu'il y a pénurie).
Le routeur va faire croire au poste interne que celui-ci est en discussion avec le réseau externe. En fait les sessions TCP seront faites à trois : Une du poste interne vers ce qu'il croit être la machine externe, en fait le routeur, puis une session du routeur vers la machine externe. Hors chaque adresse IP peut établir 64000 connexions TCP (numéros de ports). On voit que la saturation est facilement levée par ceci. Cependant certaines applications qui s'échangent des numéros de port pour communiquer dans les parties données posent problème. C'est le cas de FTP, on a vu que la commande PORT renvoie un numéro de PORT ou aller transférer le fichier. Ce port n'est donc pas négocié par une demande d'ouverture classique. Ainsi NAT impose au routeur d'aller non seulement s'occuper des états des sessions TCP , mais aussi de regarder une partie des données.

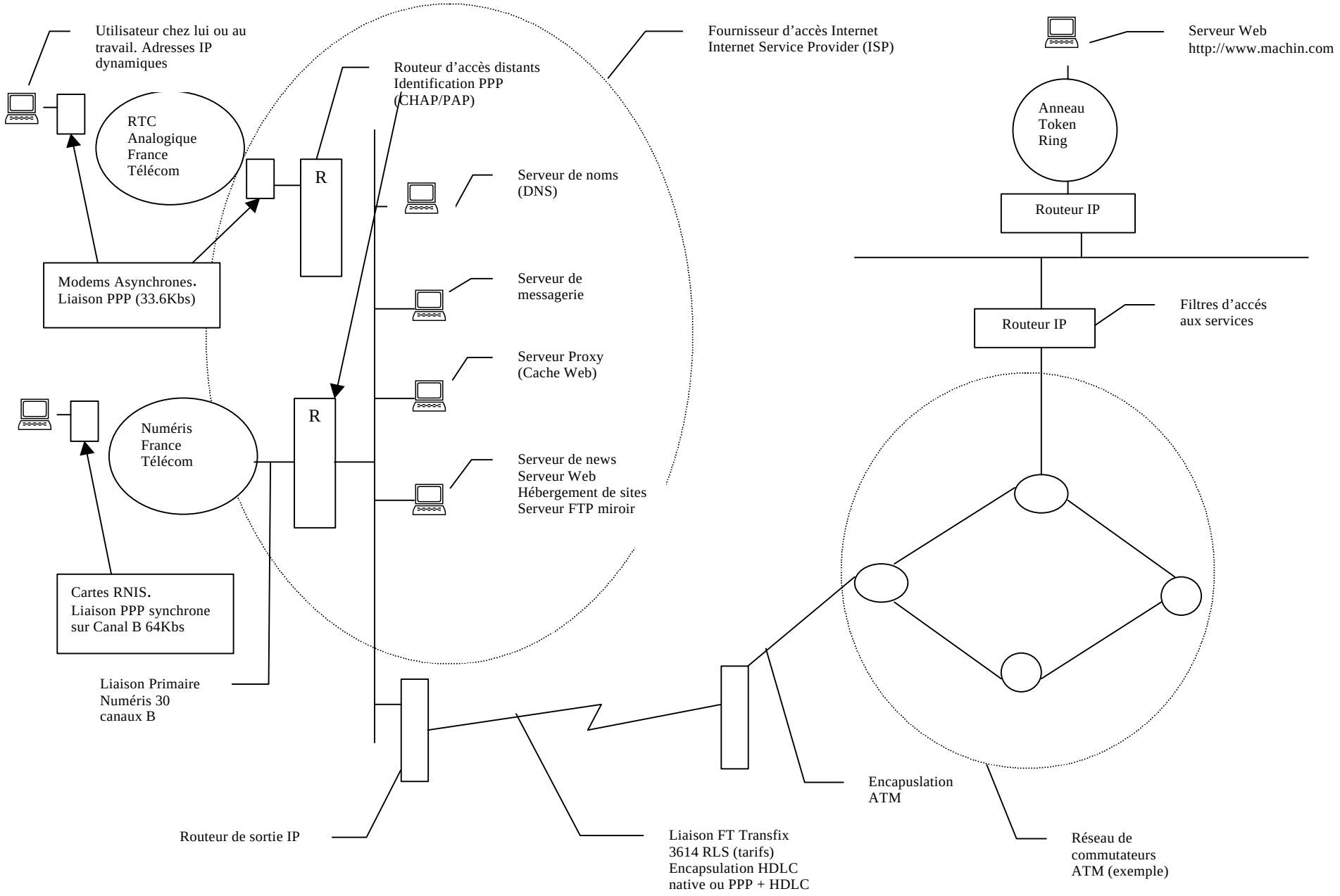
[56] Un réseau officiel, par exemple un subnet de classe C
[57] IPV6 c'est pour quand ?. Il semble s'éloigner de plus en plus !.
[58] On parle aussi de IP masquerade

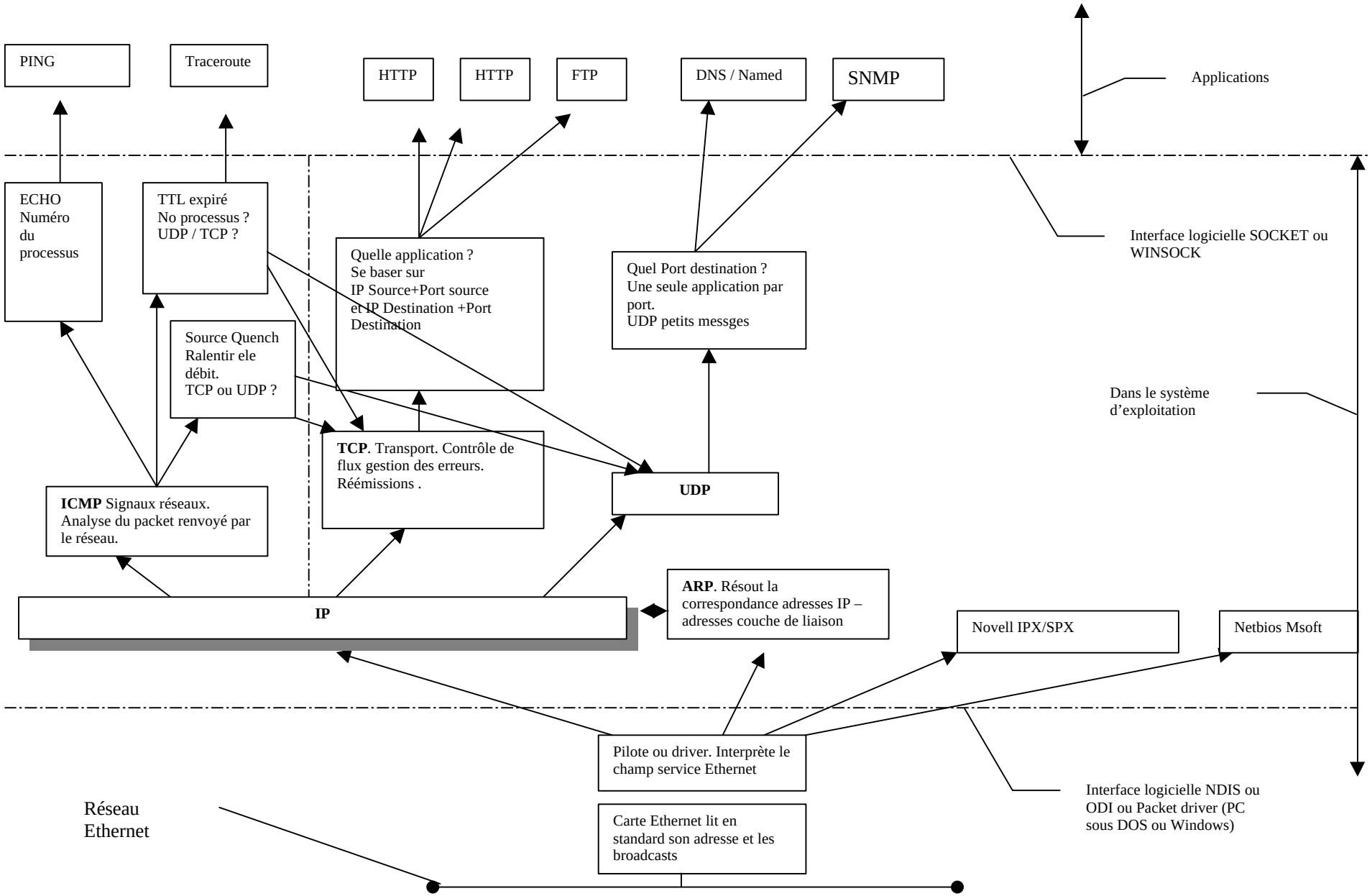
	Machine Interne	Routeur	Machine externe
Adresse IP	10.0.0.2	10.0.0.1 pool 193.50.194. (1à 15)	193.50.125.2
Socket vue en local	Machine Interne 10.0.0.2 Port 1025 193.50.125.2 port 21	Routeur 10.0.0.2 port 1025 devient 193.50.194.2 port 35200	Machine externe 193.50.125.2 port 21 193.50.194.2 port 35200

La machine externe ne sait pas qu'elle discute avec 10.0.0.2. Elle croit discuter avec 193.50.194.2. Lorsque la session se sera fermée la prochaine sera peut être avec une autre adresse IP. Imaginons une bug de sécurité sur un poste client, le pirate aura bien du mal à retrouver une deuxième fois cette machine. Cette technique (IP masquerade) est employée pour « router » un réseau local avec une seule adresse IP. Ce qui est le cas des gens utilisant des accès via le RTC.

Problèmes : Et oui ça serait trop beau.. D'une part certaines applications (peu importantes ne marchent pas). Il faut plus de mémoire sur les routeurs, mais ça c'est bon pour les fabricants.
Si le routeur a une panne électrique, ou que celui ci est « rechargé » pour maintenance, toutes les correspondances des sessions en cours sont perdues. Il faudrait une modification des routeurs pour garder la mémoire des sessions sur un support style mémoire flash. Pour l'instant, un pépin et toutes les sessions en cours sont perdues.
L'avantage des routeurs jusque là était d'être quasi sans mémoire (hormis les routes qui sont rechargées automatiquement). Un routeur arrêté et relancé ne provoque généralement qu'un délai d'attente.

Une bonne référence sur comment programmer un routeur Cisco ™ avec NAT.
Documentation : Didier Benza de l'Université de Toulon.
http://www.univ-tln.fr/~benza/nat.html


Utilisateur chez lui ou au travail. Adresses IP dynamiques
RTC Analogique France Télécom
Modems Asynchrones. Liaison PPP (33.6Kbs)
Numéris France Télécom
Cartes RNIS. Liaison PPP synchrone sur Canal B 64Kbs
Liaison Primaire Numéris 30 canaux B
Routeur d'accès distants Identification PPP (CHAP/PAP)
R
R
Fournisseur d'accès Internet Internet Service Provider (ISP)
Serveur de noms (DNS)
Serveur de messagerie
Serveur Proxy (Cache Web)
Serveur de news Serveur Web Hébergement de sites Serveur FTP miroir
Routeur de sortie IP
Liaison FT Transfix 3614 RLS (tarifs) Encapsulation HDLC native ou PPP + HDLC
Encapuslation ATM
Serveur Web http://www.machin.com
Anneau Token Ring
Routeur IP
Routeur IP
Filtres d'accés aux services
Réseau de commutateurs ATM (exemple)


PING
Traceroute
HTTP
HTTP
FTP
DNS / Named
SNMP
Applications
ECHO
Numéro
du
processus
TTL expiré
No processus ?
UDP / TCP ?
Quelle application ?
Se baser sur
IP Source+Port source
et IP Destination +Port
Destination
Quel Port destination ?
Une seule application par
port.
UDP petits messges
Interface logicielle SOCKET ou
WINSOCK
Source Quench
Ralentir ele
débit.
TCP ou UDP ?
Dans le système
d'exploitation
TCP. Transport. Contrôle de
flux gestion des erreurs.
Réémissions .
UDP
ICMP Signaux réseaux.
Analyse du packet renvoyé par
le réseau.
ARP. Résout la
correspondance adresses IP –
adresses couche de liaison
IP
Novell IPX/SPX
Netbios Msoft
Pilote ou driver. Interprète le
champ service Ethernet
Interface logicielle NDIS ou
ODI ou Packet driver (PC
sous DOS ou Windows)
Réseau
Ethernet
Carte Ethernet lit en
standard son adresse et les
broadcasts

REFERENCES HTML

Unité réseau du CNRS ou le CRU (Comité Réseau des Universités) excellent pointeur sur des infos réseau
http://www.urec.fr ou http://www.urec.fr

Richard Stevens Home Page (Auteur de TCP/IP Illustré)
http://www.noao.edu/~rstevens

RFC en France
ftp://ftp.inria.fr/inet/INTERNET-drafts

La librairie virtuelle
http://www.w3.org/vl

La librairie des télécommunications
http://www.analysys.co.uk/commslib.htm

Les Organismes de Normalisation

IETF INTERNET Engeneering Task Force (RFC)
http://www.ietf.org/1id-abstracts.html
IEEE
http://www.ieee.org
CCITT / ITT / ITU
http://www.itu.ch
ISO
http://www.iso.ch
ANSI
http://www.ansi.gov

IRTF INTERNET Research Task Force
http://www.irtf.org/irtf
IAB INTERNET Association Board
http://www.iab.org

INTERNET Society
http://www.isoc.gov

La programmation des sockets de windows
ftp://sunsite.unc.edu/pub/micro/pc-stuff/ms-windows/winsock

INTERNET Software Consortium
http://www.isc.org

Les groupes de news à regarder sur les réseaux
fr.network.*
comp.dcom.*
comp.protocols.*
comp.os.linux.networking
comp.os.ms-windows.networking.*

Atm Forum
http://www.atmforum.com

Les FAQs indexées à l'Institut Pasteur
http://www.pasteur.fr/computer/other