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.
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.

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. Malgré l'indépendance des couches réseaux, au 21ème siècle, il faut bien constater la dominante ETHERNET TCP/IP.

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.

Dominique LALOT est ingénieur réseaux et systèmes au pôle réseau de l'université de la Méditerranée. Il a mis en place le réseau IPV6, et gère un certain nombre de services parmi

Table des matières

HISTORIQUE

Quelques dates des évolutions techniques.

L'humanité	Afrique?	-4 Ma
Le langage parlé	?	-200000? (controverses)
L'écriture	Mésopotamie (IRAK)	-3500
Les pigeons voyageurs	?	?
Les signaux de fumées	Les amérindiens	?
Les dialectes sifflés	Iles Canaries	
Les postes	Romains	< 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 Collossus	UK	1943
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.

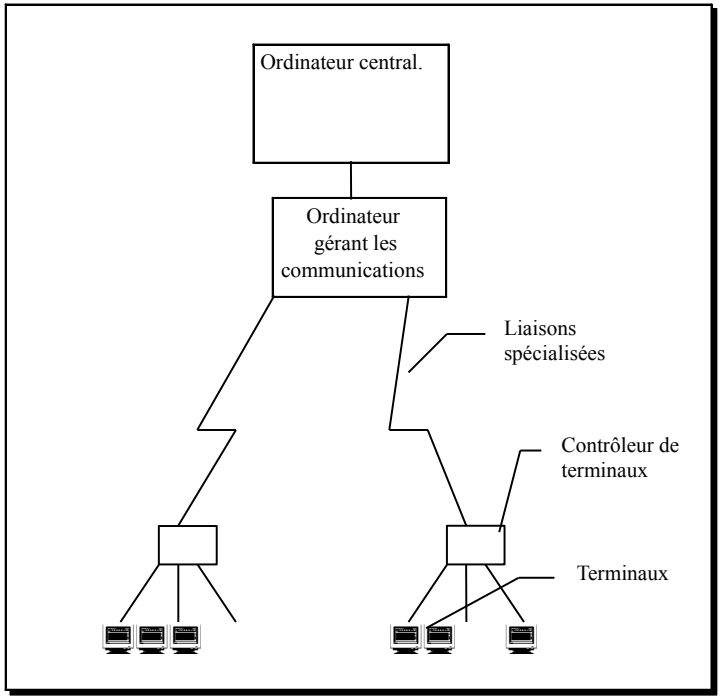
L'évolution des capacités de communication des ordinateurs
L'ordinateur au début n'a que des capacités de calcul. Communiquer avec lui est l'affaire de spécialistes très pointus. Puis, petit à petit, la technique s'améliore. On utilise des bandes perforées puis des cartes perforées. Les sorties sont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

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



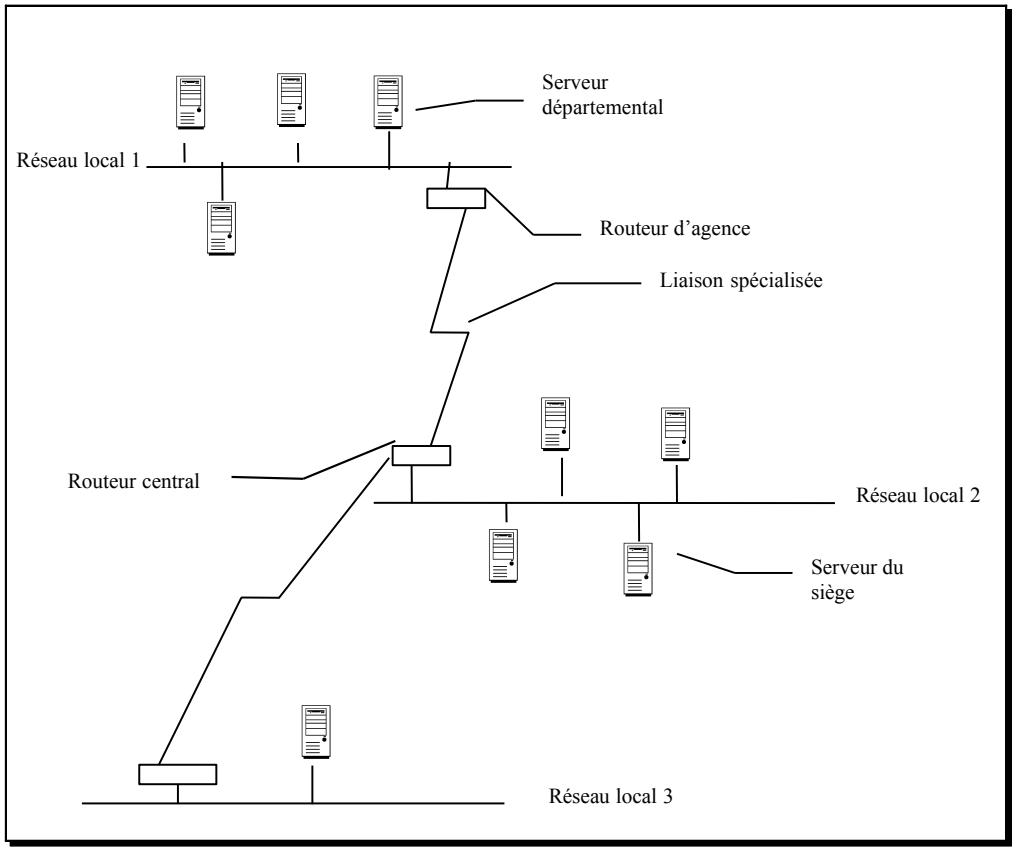
On voit dans cette architecture un système très centralisé, conforme aux prix du marché.
L'ordinateur est très cher, les terminaux assez bon marché.

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'inter-connecter les systèmes. Il en est né le protocole **OSI** (Open System Interconnection) de l'**ISO**

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.

7 application
6 présentation
5 session
4 transport
3 réseau
2 liaison
1 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)

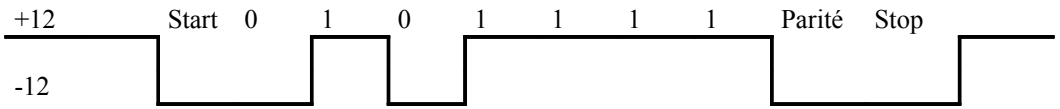
La Couche Physique , couche 1 de l'OSI

Les Codages de caractères
7 bits 8 bits ASCII.. ISO 8859-1. Voir l'utilitaire charmap de windows pour voir une table de codes
Le codage UFT8 de longueur variable est en train de devenir le standard. ASCII 7bits consomme un octet. Les caractères accentués 2 octets.

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 quelques dizaines de km)
- ✔ Les lasers (sans fibre) (<5 km)

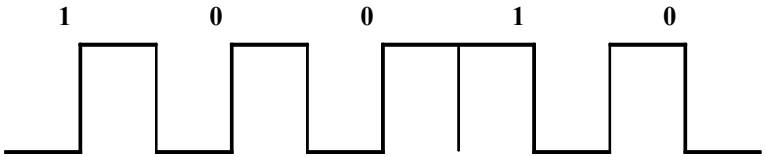
Le mode de transmission asynchrone :
schéma temporel :
Il faut distinguer le zéro d'une tension nulle. Un bit 0 n'est pas le rien du tout. L'interface V24 utilise des tensions +- 12Volts



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
Émetteur et Récepteur se mettent d'accord sur un moyen de se synchroniser. Le problème vient de

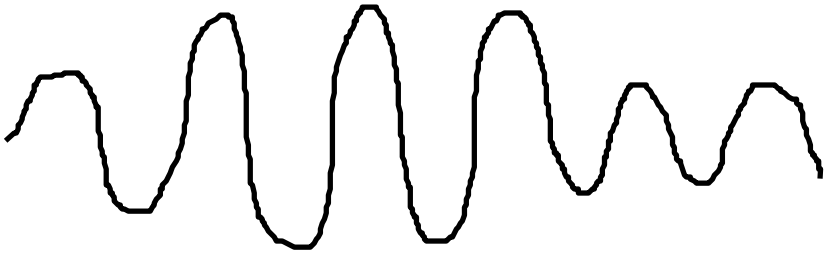
Le Manchester Différentiel
Il tient compte du bit précédent. Le bit zéro est un changement de polarité, le bit un non . Ce codage ne dépend pas de la polarité. Il est utilisé comme niveau physique du réseau Local ETHERNET



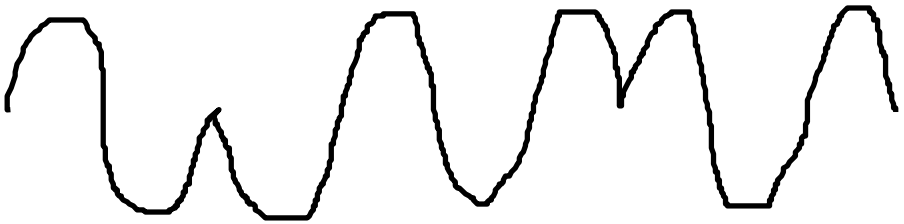
Problème de la transmission bande de base : Ces signaux se déforment vite. Le carré s'arrondit, le signal s'aplatit . Ils sont généralement utilisés pour de courtes distances. Pour aller plus loin, on utilise des signaux sinusoïdaux. En fait la sortie d'un ordinateur, reste bande de base, plus loin, 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 sinusoïdal.. On trouve différents types de modulations qui vont coder l'information.

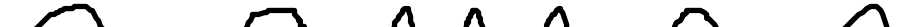
Modulation d'amplitude.



Modulation de phase



Modulation de fréquence :

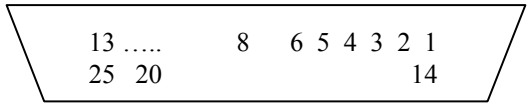


Les Sens de transmission.
On trouve différents types de liaisons.

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 trapézoïdale.
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

6 (DSR) Modem Prêt ← Modem Prêt
8 (CD) Carrier detect ← Détection de porteuse on voit aussi 109 sur les modems

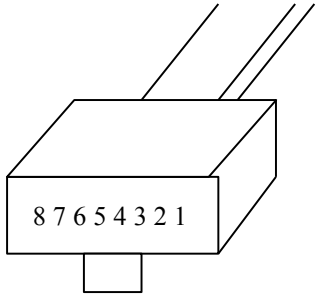
Ces signaux sont juste de type On/Off (+_12V) sauf pour TD/RD qui véhiculent les données. Pour connecter un modem sur un PC, il faut un câble spécial qui est vendu avec les modems. Si l'on veut faire un transfert d'ordinateur à ordinateur, il faudra un câble dit croisé. Voici un schéma type .

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 femelle murale ou dans un HUB ou dans une carte réseau.



1 et 2 émission et 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

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	« «

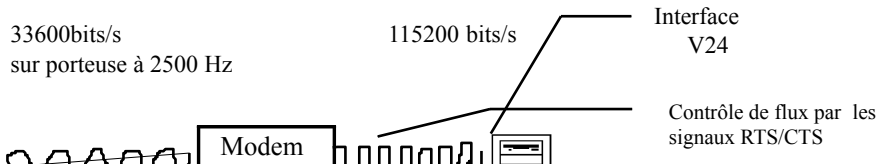
Les modems dits asynchrones du marché qui sont utilisés comme Fax ou comme moyen de transmission sur INTERNET ou sur les services kiosque 36xx, sont couramment des modems V34bis (33600 bits/s). Ces modems présentent un certain nombre de possibilités. Ceux-ci sont dits compatibles Hayes, supportant les 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 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 un émulateur de terminal au lieu du pilote de modem.

La compression: On dit que l'on transfère à 115kb/s alors que le modem ne va qu'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)



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.

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 CDROM)..

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,

$$P(x) = a_0 + a_1 x + .. + a_{b-1} x^{b-1}$$

On calcule ensuite la division de ce polynôme par le polynôme dit générateur. Le reste est un polynôme de degré 15 qui s'écrit : $R(x)=r_0 + r_1 x + ... + r_{15} x^{15}$
Les valeurs r0 à r15 sont ensuite stockées dans la zone de détection d'erreur. Lors de la réception, le

Les équipements au niveau liaison ou réseau, vont mettre la trame à la poubelle. Ils ne la transmettent plus. La couche transport devra se préoccuper de la perte et demander une retransmission

LES RESEAUX LOCAUX

LES RESEAUX LOCAUX

Les types de réseaux locaux

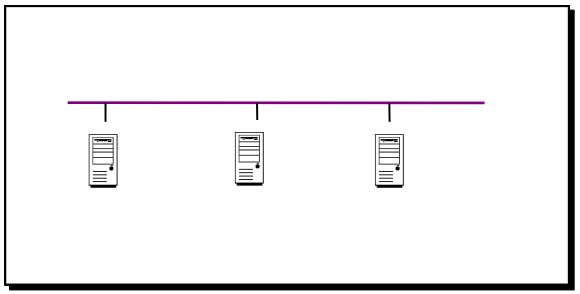
Le But :

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 (IEEE802.3 ou ISO8802.3)

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'excédait 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 1500€, maintenant 15€.

La notation IEEE 802.3:
10Base5 10=10Mbs Base=Bande de Base 5 = 5*100mètres ex:

Nom	10 Base 5	10 base2	10BaseT (1985)
Vitesse Mbps	10	10	10
Signal	Baseband	Baseband	Baseband
Longueur Max	500	185	100
Media	50 Ohm coax (thick)	50 Ohm coax (thin)	UTP
Topologie	Bus	Bus	Etoile

Un certain nombre de réseaux cités sont très rares (10base2 et 10Base5 sont obsolètes et 10BaseT remplacé par 100BaseT).

Topologie de Bus

Exemple de réseau ETHERNET.
Les bouchons sont là

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). La longueur maximum du réseau correspond à une durée de propagation de 51,2µs. Si l'on utilise une fibre optique, la longueur maximum en km sera de $3*10^5 *51.2*10^{6-} = 15$km. 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 ré-émettre ^{6}. Toutes les stations font le même calcul. Passé ce délai, on ré-émet 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 ré-amplifier 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 ré-émet. 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 le format ETHERNET2.

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

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)
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 représentent 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. Cette interface est historique et n'est plus utilisée

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.
Ce type de réseau a pratiquement disparu.

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 1985, la porte sur le Hub valait 300€ , en 1997 45 €. 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.

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 inter-connecter avec des switchs.

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 a fait une sérieuse concurrence à l'ATM.
Le Gigabit Ethernet utilise en 1999 uniquement les fibres optiques. Depuis la norme 1000BastT permet l'utilisation normalisé sur le cablage traditionnel. Le câblage recommandé est la spécification 5E. Curieusement, le 1000BaseT est 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. La transmission se fait à 100Mhz par codage des informations.

Vers le Full Duplex
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.

802.3af
On voit plusieurs dénominations: ETHERTRUNK ETHERCHANNEL. On peut interconnecter deux équipements en vis à vis via une agrégation de liens. On peut soit émettre sur tous les liens, soit les mettre en backup.

802.3ae ou POE (Power over Ethernet)
Norme d'alimentation électrique pour des équipements auto-alimenté à travers des switchs. On utilise les deux paires inutilisées 4/5 et 7/8. On alimente ainsi des téléphones IP ou des Point d'accès WIFI.

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

ETHERNET II (TCP/IP) Le format de trame ETHERNET le plus utilisé

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.

l'UTP ou du FTP. On trouve maintenant du 5E dont la certification se fait à plus haute fréquence que la catégorie 5. Cependant le 5 est souvent aussi bon mais qualifié pour des fréquences plus basses. Le 6 est certifié pour 250MHz.

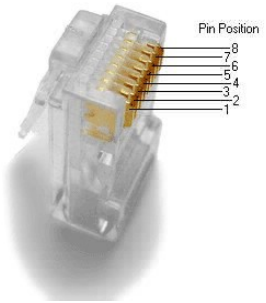
Remarque :

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

http://fr.wikipedia.org/wiki/RJ45

http://fr.wikipedia.org/wiki/Paire_torsad%C3%A9e

http://www.ertyu.org/steven_nikkel/ethernetcables.html



RJ45

RJ-45 cable droit (TIA/EIA-568-B T568A)

Pin	Pair	Color	tel	10BASE-T	100BASE-TX	1000BASE-T	PoE mode A	PoE mode B
1	3	white/green	-	TX+	z	bidi	48V out	-
2	3	green	-	TX-	z	bidi	48V out	-
3	2	white/orange	-	RX+	z	bidi	48V return	-
4	1	blue	ring	-	-	bidi	-	48V out
5	1	white/blue	tip	-	-	bidi	-	48V out
6	2	orange	-	RX-	z	bidi	48V return	-
7	4	white/brown	-	-	-	bidi	-	48V return
8	4	brown	-	-	-	bidi	-	48V return

WIFI ou IEEE802.11

Le WIFI (Wireless Fidelity) est une appelation commerciale pour recouvrir les normes de réseau locaux sans fils 802.11. 802.11 a été normalisé en 1999.

802.11 a	5Ghz	54Mbs
802.11 b	2,4 Ghz	11Mbs
802.11 g	2,4 Ghz	54 Mbs

802.11a est peu utilisé en Europe, car à puissance égale 5Ghz porte moins loin.
Ces normes utilisent une technologie proche des réseaux locaux Ethernet 802.3, mais avec une petite variante, le CSMA/CA à la place de CSMA/CD. Il y a une demande d'émission et donc une certaine notion de maître esclave. Les trames au niveau liaison sont des trames ETHERNET classiques.

Un peu de terminologie:
Mode infrastructure: les clients se connectent à des bornes dites points d'accès ou AP. (Access Point in english)
Mode ad-hoc: les clients sont aussi point d'accès, c'est une notion de peer-to-peer. Attention en terme de sécurité. Il faut éviter de mettre les machines en mode ad-hoc.
SSID: Le nom du réseau est broadcasté à intervalle régulier (BEACON). Ceci est la configuration par défaut, mais on peut l'interdire. Le client voit dans son interface, la liste des réseaux disponibles. Une borne évoluée peut diffuser plusieurs SSID sur plusieurs canaux.
Canaux: Autour de la fréquence de base, il existe 14 fréquences séparées par quelques dizaines de Mhz qui permettent autant de réseaux différents. Ceci permet d'éviter les interférences. Il est recommandé d'utiliser 4 canaux d'écart entre deux bornes proches. La canal 14 n'est autorisé qu'au Japon.
Puissance: 100mw, donc beaucoup moins qu'un téléphone GSM
Fréquence: de l'ordre des micro-ondes (métrique). Par conséquent très bien absorbée par les corps, réfléchi par les métaux, le béton.
Portée:
Il n'y a pas de limites de portée. Avec de grandes oreilles et un grand micro, on peut capter de très loin. Les communications GSM sont écoutées sur des satellites du réseau ECHELON alors qu'on a parfois du mal à avoir le réseau! Par contre avec le matériel grand public, 50 m est assez classique.
Débit:
Les débits sont variables. Plus on est loin de la borne (AP), plus le débit est faible, jusqu'à 2Mbs. Les clients à faible débit vont monopoliser la transmission.
Commutation:
Il n'y en a pas. On partage une bande de fréquence et un débit. La qualité est plus proche de la téléphonie mobile que de la téléphonie fixe.
Fiabilité:

partagée ou via un serveur RADIUS ou Active Directory et les extensions EAP http://fr.wikipedia.org/wiki/Extensible_Authentication_Protocol

Une dernière amélioration est le **WPA2** qui remplace TKIP par CCMP plus sûr et qui utilise un cryptage AES au lieu de RC4. Il n'est disponible que depuis 2005, mais en standard dans les OS que depuis peu.

Petite dernière:
Le **802.11n** avec la technologie MIMO permet un plus grand débit avec une meilleure gestion des signaux parasites. Attendons de voir.

Remarques:
La diffusion des Clefs Partagées reste un problème dès que le réseau est de taille importante.
Mettre en place une structure cryptée n'est pas simple. Les machines peuvent être anciennes, et ne supporter qu'un jeu réduit de mode de fonctionnement. Aussi pour une très large population est il plus simple, de ne pas crypter, de mettre le système WIFI dans un VLAN séparé, et de mettre en place un **portail captif**.
Un portail captif est un routeur et parefeu un peu spécial. Quand il ne connaît pas une machine (son adresse matérielle), il détourne les requêtes web vers une page web https et demande un couple login/mot de passe. La machine est ensuite autorisée à sortir. Bien entendu, comme la connexion n'est pas cryptée par la suite, tout protocole non crypté susceptible d'échanger un mot de passe est filtré. Il en est ainsi de POP, IMAP etc.
Il est ensuite assez facile de monter une solution de VPN (tunnel crypté en IPSEC ou PPTP) et de faire que la connexion sera cryptée et même beaucoup plus loin que jusqu'à l'AP. A l'intérieur du VPN, on pourra faire passer du POP ou de l'IMAP.

Enfin, pour enfoncer le clou, les systèmes sans fils sont vraiment inquiétants dans la mesure où, dès la sortie les prix se sont avérés bas, tournés vers le grand public. Ainsi a-t-on vu fleurir dans les entreprises ou les labos, des AP posées par des néophytes ouvrant une brèche redoutable au niveau de la sécurité.
Nous déployons du WIFI plus pour combler un vide avant qu'il ne soit comblé par d'autres.
Déployer un vaste réseau sans fil nécessite des moyens financiers importants. Dans notre université, nous avons choisi la solution du constructeur ARUBA qui fournit une solution complète de transport d'un réseau de niveau 2 sur un réseau IP et centralise la gestion des bornes.

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.

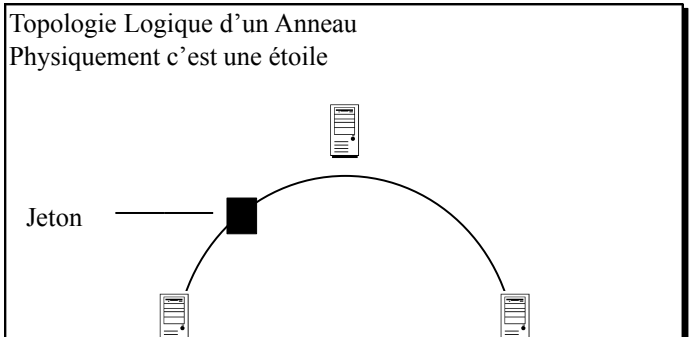
Ce protocole était assez novateur pour le câblage, car il utilise du matériel actif équivalent au Hub ETHERNET, ceci bien avant 10BaseT. Avantage aussi, sous forte charge, le réseau ne s'écroule pas, tout le monde a le même temps de parole. Par contre sous faible charge il est plus lent. Les trames sont 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

Topologie Logique d'un Anneau
Physiquement c'est une étoile



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.

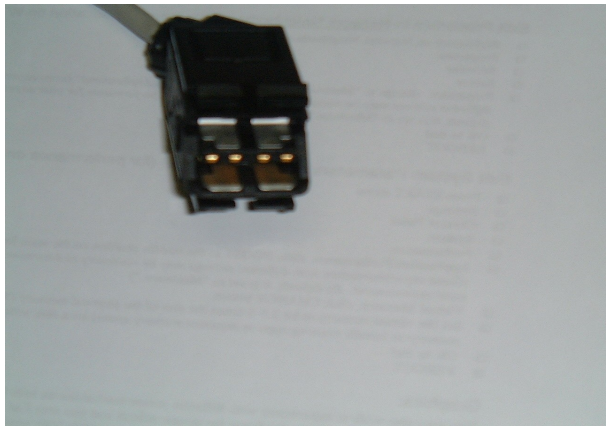


Illustration 1: Prises hermaphrodite

VLANS

ou Virtual Lan (Réseau Virtuel) IEEE 802.1Q

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. De plus en séparant physiquement, on augmente le nombre d'équipements actifs à acheter.

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 groupe les ports physiques entre eux dans le même VLAN, où qu'ils soient dans le bâtiment.

Pour que ces réseaux devenu physiquement séparés communiquent entre eux, il faut utiliser des routeurs. C'est la couche 3 réseau qui permettra la communication.

Les liens entre Commutateurs véhiculent des trames "taggées", qui ne sont pas compréhensibles par une station "normale". Le No du VLAN est indiqué dans l'en-tête Ethernet. Ces liens doivent être déclarées taggés dans les équipements, de part et d'autre. Le réseau devient donc moins transparent et facile à administrer, mais plus robuste.
On peut ainsi partager un équipement actif pour plusieurs usages.
Il est possible de mettre des serveurs dans plusieurs VLAN en le mettant sur un lien taggé 802.1Q.
Ceci est souvent lié à une mauvaise gestion du réseau. Par exemple WINS et les serveurs de domaines Active Directory permettent de se passer des broadcast pour les résolutions de nom de machine ou de domaines. Les serveurs UNIX s'appuient sur les mécanismes de nomage DNS étudiés plus loin.
On doit en fait mettre les machines dans différents VLAN:

- ✔ serveurs intranet seulement(pas d'accès depuis Internet)
- ✔ serveurs publics (accessibles depuis Internet)
- ✔ les réseaux clients (étudiants, administration, recherche,..)

Sur chaque commutateur, il n'est pas obligatoire de créer tous les VLANS. Ils doivent juste avoir le même numéro. Et ces VLANS doivent donc être envoyés sur le/les liens taggés qui arrivent sur le commutateur.

Il existe aussi un double 'tagging' appelé QinQ qui permet de transporter des VLAN dans des VLAN, ce qui est pratique pour les opérateurs.

TELEPHONIE NUMERIQUE

ISDN ou RNIS[8] : 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 archaïque. 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 sinusoïdale) 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 [9]. On peut recevoir une télécopie pendant que l'on téléphone.

On reçoit, au niveau du poste téléphonique numérique, une information sur les numéros appelants.

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)

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 [10]).

- ✔ Normal response Mode (NRM). Ca c'est SDLC.

SLIP ET PPP

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 ré-émettre. On a pu constater que PPP avait du mal à fonctionner lorsque les protocoles de correction d'erreurs V42bis [11] 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

PROTOCOLES DE RESEAU Couche 3 de l'OSI

Qu'est ce qui va distinguer les protocoles réseaux de la couche liaison? On peut se poser la question. En effet, un commutateur ETHERNET d'une certaine manière va commuter des trames et donc aussi faire à sa façon du routage. Pourrait on concevoir un réseau ETHERNET mondial? En fait, tel que se joue la commutation ETHERNET, le niveau de détail est beaucoup trop important. On indique pour chaque MacAdress un port physique. Si nus étions sur le même VLAN, il faudrait gérer des milliards d'adresses et des broadcast en pagaille!
Donc il nous faut autre chose de mieux organisé qui sera la couche réseau avec des adresses globales, une stratégie de distribution de ces adresses, voir une organisation hiérarchisée de la numérotation.

Il faut distinguer deux types de réseaux de niveau 3, les réseaux à commutation de circuits et ceux à commutation de paquets.

Commutation de circuit (mode connecté)
Ils sont de type téléphonique. Un peu comme dans les temps anciens du téléphone, on appelle une opératrice qui va appeler une collègue derrière un panneau de brassage et va vous mettre en relation avec votre interlocuteur. Pendant ce temps là, vous attendez que la ligne se construise. Bien entendu, les choses vont plus vite! Ces réseaux sont bien adaptés à la voix car l'information emprunte le même chemin, une fois le chemin initial tracé, il n'est plus besoin de garder l'adresse de destination. Les commutateurs font juste une correspondance, port x, voie logique 3 vers port z voie logique 2.
On va trouver dans cette famille:
le téléphone, RNIS, X25, Frame Relay, ATM

Commutation de paquet (mode non connecté)
Comme le réseau postal, pour chaque information (paquet,lettre), l'adresse destination est complète et consomme pas mal de place. Mais à chaque instant sur le réseau, on sait comment acheminer l'information. Ceci permet d'alléger la tache des routeurs qui ne gardent pas d'états. On peut ainsi redémarrer un équipement sans perdre les milliers de connexions passant par ce noeud. Et dans le cadre de la guerre froide, c'est très probablement ce qui a poussé au design initial de TCP/IP.
TCP/IP ne définit pas de couche de liaison, ce qui n'est pas le cas d'ATM ou d'X25. Il est un bon exemple de l'indépendance des couches. Il a été conçu indépendamment d'ETHERNET (quoique à la même époque) et pourtant, il peut l'utiliser.
MPLS est une technologie IP qui permet de retrouver la commutation de circuits (labels) et de mixer le meilleurs des deux modes.

Les réseaux d'aujourd'hui
On peut dire que les solutions les plus utilisées sont:
Ethernet + TCP/IP + MPLS (opérateurs)

X25

Réseaux de transmission par paquets

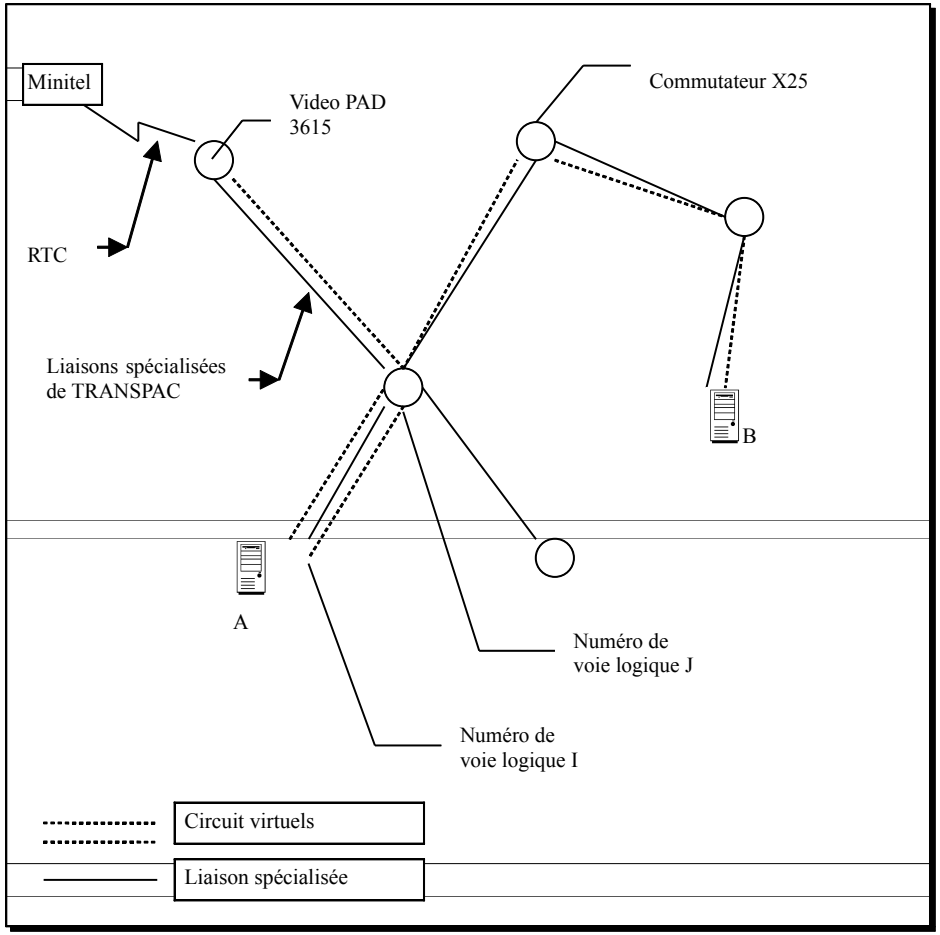
Les secrets du Minitel.
Nous voici là au niveau 3 des couches OSI. X25 est un protocole de transport de l'information complet qui gère le transport de l'information de bout en bout sur de très longues distances avec un plan de numérotation International. On parle de WAN (Wide Area Network), Public Data 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.

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 re-dessiner 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.

FRAME RELAY

ou Relais de Trame.

Ce protocole connaît un certain succès aux US , et semblait 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. En 2007, il doit rester très peu de réseaux de ce style.

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. (En 2007, le marché est largement dominé par Ethernet + IP + MPLS)
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 [12] . 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

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.

La trame ATM

5	48[13]
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 dès 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 ! !. [14]
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.

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
RENATER
GEANT
ORANGE
....

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 [15], 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

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. 128 bits dont le préfixe est le réseau de l'opérateur de collecte
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 des serveurs virtuels. L'adresse IP est liée à une localisation fixe comme un numéro de téléphone fixe et fait partie d'une suite d'adresses contiguës qui forment le réseau local. Cette information est donnée par le masque ou longueur du préfixe en notation CIDR.

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 des opérateurs d'accès. Ceux ci obtiennent leurs adresses auprès des RIR. Www.ripe.net en Europe. 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. On parle toujours de classes alors que celles-ci sont historiques. Depuis les années 1993, on parle d'agrégation, de préfixes et de notation CIDR, mais certaine habitudes

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

MASQUE
La partie réseau est définie en mettant tous les bits réseau à un.
Classe A masque 255.0.0.0
Classe B masque 255.255.0.0
Classe C masque 255.255.255.0
Le masque sert à définir une route vers un réseau. Dans le cas du réseau local c'est la route directe de l'interface réseau. Ce masque servira plus loin à comparer les parties réseaux de deux adresses: une adresse destination et un réseau dans la table de routage.

CIDR
Devant la multitude de réseaux de classe C non continus, l'IETF a préconisé la redistributions des classes ainsi que le re-numérotation de certains réseaux, afin de diminuer la taille des tables de routage.
Pour ces raisons INTERNET vers 1993 s'est orienté vers un routage **CIDR** (ClassLess InterDomain Routing), c'est à dire sans classes d'adresses, mais en utilisant une **agrégation** d'adresses 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 routez ces réseaux vers RENATER . Au niveau routage, chaque réseau doit donc être complété par son masque.
En notation CIDR, on ne parle plus de masque mais de longueur de préfixe, mais hélas, ceci n'est pas généralisé. Suivant les constructeurs la saisie du masque peut se faire en CIDR mais l'affichage avec les masques ou le contraire!
Classe A /8
Classe B /16
Classe C /24

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 passer par un routeur bien qu'étant sur

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 réseaux privés RFC1918:

Ceux ci ne sont pas distribués sur internet et sont « privés ». Il servent en interne pour inter-connecter des équipements où pour numéroter des réseaux qui feront appel à NAT (remplacement d'adresses IP à la volée).

10.0.0.0/8
172.16.0.0/16
192.168.0.0/16

Réseau privé Lien local: 169.254.0.0/8 RFC3927

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. [17]

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. (ou /24)

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). Les trois premiers octets de l'adresse sont connus, mais comment écrire le dernier?

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**

Le masque sera 193.50.126.224

193.50.126.0/27 Broadcast 193.50.126.31
193.50.126.32/27 Broadcast 193.50.126.63
..
193.50.126.224/27 Bcast 193.50.126.255

Pour un routeur la machine d'adresse 100 appartiendra au réseau 193.50.126.96 masque 255.255.255.224

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.

IPV6
Passage des adresses à 128 bits. Voir le chapitre IPV6

A retenir :
Le masque sert à reconnaître un ensemble d'adresses accessibles sur un même lien local ou sur une même route..
Les adresses ne sont pas isolées mais regroupées par réseaux (un peu comme le téléphone)

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)

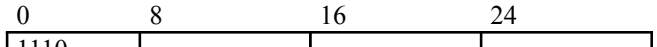
TCP/IP gère ainsi que ETHERNET ces différent types d'adresses. On verra que ARP est un broadcast ETHERNET, RIP est un broadcast IP/UDP qui sera convertit en broadcast ETHERNET, si ETHERNET est la couche de liaison.

Pour TCP/IP l'adresse de broadcast consiste à mettre les bits de l'adresse machine à un. Si 193.50.125.0/24 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, XP proposent des masques de classe B par défaut..). Il faut filtrer ces broadcast IP au niveau des routeurs, mais c'est devenu la règle par défaut (no ip directed broadcast chez CISCO)

Typiquement le multicast est utilisé pour transmettre des visio-conférences sur INTERNET. Les opérateurs l'utilisent pour retransmettre la télévision.
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

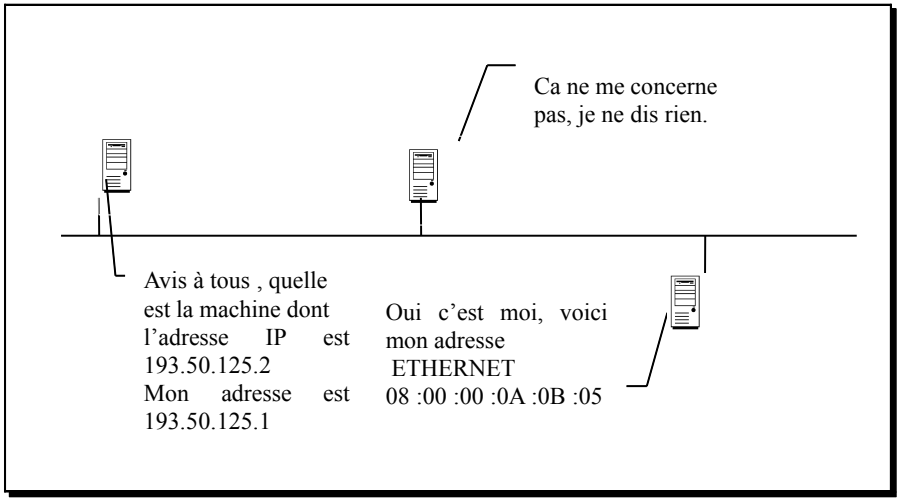
Adresse de broadcast sur ETHERNET
FF:FF:FF:FF:FF:FF

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 n'émet qu'une seule trame qui sera dupliquée ensuite par les routeurs en fonction des abonnements IGMP. Les switch niveau 2 doivent implémenter IGMP snooping pour éviter de transformer du multicast en broadcast.

ARP ou Address Resolution Protocol Résolution d'adresses



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. Évidemment, 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 , Windows.
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..
exemples d'analyse de trames:

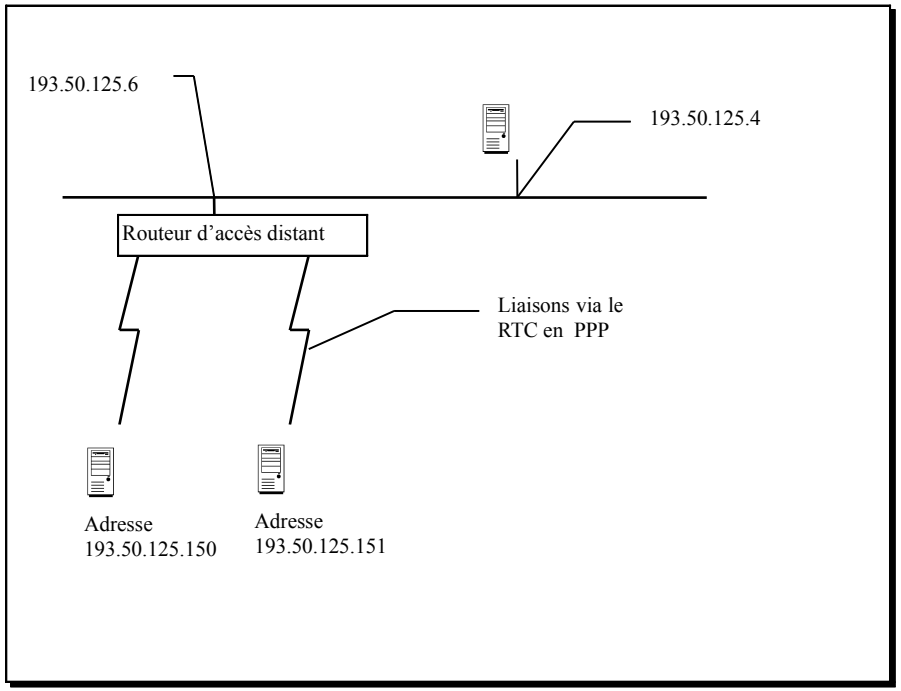
```
tcpdump -e arp (en premier les adresses ethernet)
0:6:5b:3e:4e:a6 0:13:72:77:35:86 arp 42: arp who-has dhcp138.univ-aix.fr tell romarin.univ-aix.fr
```

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 (Obsolete)
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 a donc été abandonné au profit de BOOTP puis 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



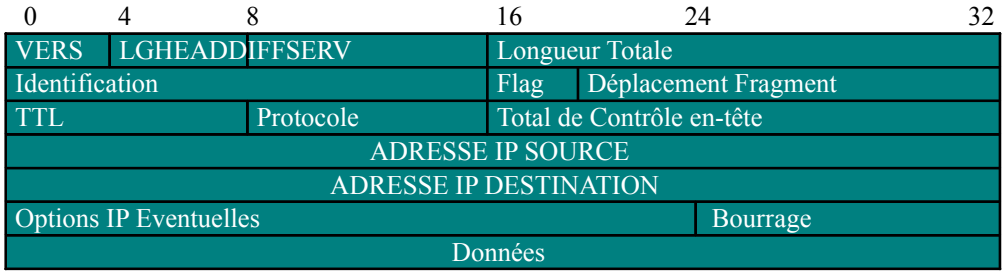
On peut se demander qu'elle est la différence entre le routage et proxy arp. En fait la machine qui appelle (193.50.125.4) a l'impression que 150 et 151 sont sur son réseau. En quelque sorte proxy arp

Le DATAGRAMME [18] IP

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 [19], ces paquets peuvent suivre des routes différentes, être dupliqués, arriver dans le désordre [20].

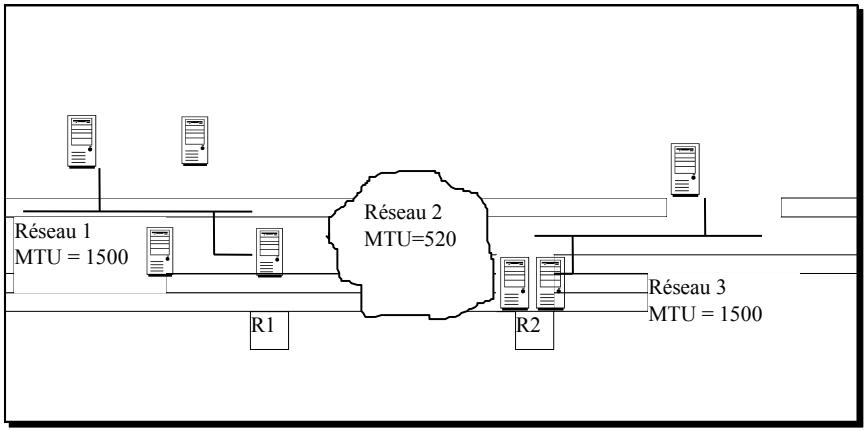
Structure des datagrammes :



Signification:

- VERS= numéro de version. En ce moment vaut 4 (IPV4) mais 6 pour IPV6
- LGHEAD= longueur d'en-tête en mots de 32 bits. Généralement, 20 octets = 160 bits=5*32bits
- LGHEAD vaut 5 la plupart du temps, soit 20 octets
- DIFFSERV (Differentiated Services): utilisé pour la qualité de service. Il s'agit d'un marquage de priorité qui est effectué par des routeurs d'extrémités et dont la priorité va être suivie par les routeurs du domaine DiffServ, en général le réseau d'un opérateur. La transmission de ce champ entre opérateur reste un problème. On parle de QOS ou qualité de service. Ce champ peut être marqué au regard des applications transportées ou via le marquage d'un champ COS 802.1Q.
- Longueur Totale = longueur en octets du datagramme, en-tête plus données jusqu'à 64Ko, mais de fait rarement supérieure à un MTU Ethernet de 1500 octets
- Identification: concerne la fragmentation (quasi obsolète, supprimé en IPV6)
- Flag: MF (More fragments trame fragmentée) DF (Don't Fragment souvent positionné)
- Déplacement fragment, voir plus loin (idem)
- TTL: Time to live ou 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. Il est appelé HopCount en IPV6
- 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, abondonné en IPV6. Ce contrôle doit être recalculée à chaque changement du TTL.

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 octets, TokenRing (16Mbs) 16Ko. 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 2 trames de 520 et une de 460 pour une trame de 1500. Les déplacements indiquent l'index dans les données du paquet non fragmenté du départ.

Le MTU minimum recommandé par l'IETF est de 1500 octet soit le contenu d'une trame ETHERNET. On peut cependant dans les réseaux locaux ETHERNET augmenter cette valeur et utiliser par exemple des jumbo frames (9Ko).

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

La fragmentation est tout de même ennuyeuse car au moindre fragment perdu, c'est tout le datagramme IP qu'il faut ré-émettre. **IL FAUT EVITER LA FRAGMENTATION.** En IPV6, celle-ci disparaît.

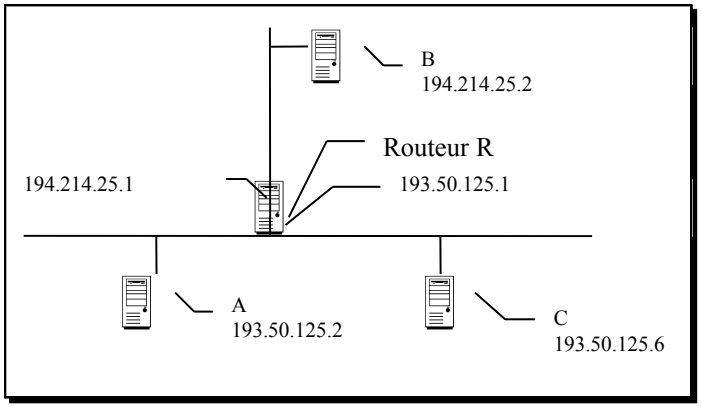
TCP utilise l'algorithme **PATH MTU DISCOVERY** (découverte du MTU de chemin) afin d'optimiser la taille du datagramme. TCP met alors dans chaque datagramme IP, l'option DO NOT FRAGMENT. Si le datagramme est refusé par un routeur, celui-ci envoie un message ICMP de refus avec la taille du MTU. TCP diminue alors la taille du MTU lié à la session afin que le datagramme passe.

Note: si les messages ICMP sont filtrés, les machines peuvent être bloquées. Malheureusement, pour bloquer les ping, beaucoup d'administrateurs bloquent ICMP en totalité ce qui induit pas mal d'effet de bord.

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 » [21]. 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.

pour R1

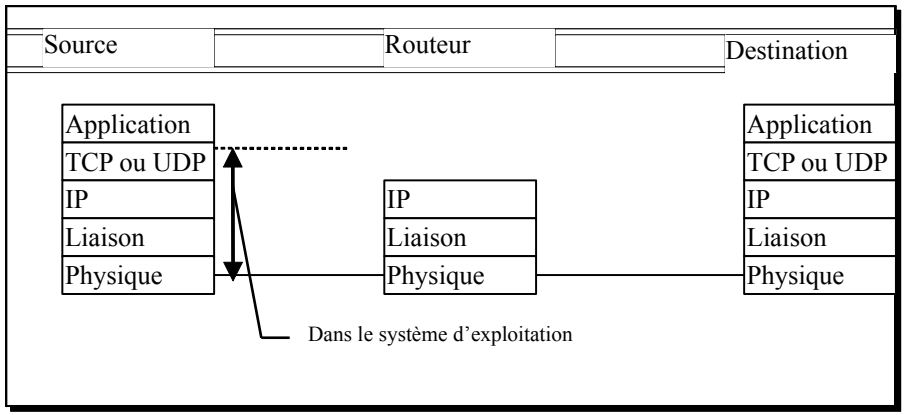
193.50.125.0	Direct
194.214.25.0	Direct
194.214.24.0	Direct
193.50.126.0	194.214.24.2

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.

Plusieurs routes pour une même destination.
On privilégie d'abord les routes les plus précises, donc le préfixe le plus long. Ensuite, on regarde les types. Une route directe (sur le lien local donc) sera privilégiée. Ensuite une route statique, enfin les routes dynamiques. Le routeur indique en cas d'égalité laquelle est prioritaire.

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 ou Interior Gateway Protocol IGP (RIP, OSPF,IS-IS)
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

- ✔ 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 est bavard en broadcast (tous les routeurs, toutes les 30 secondes..)

RIP V2 (1993)

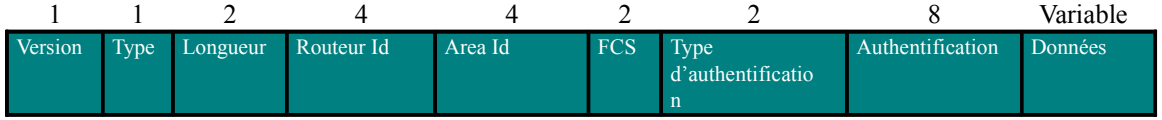
- ✔ Ajout du subnet mask.
- ✔ Retour d'information vers un protocole de routage extérieur.
- ✔ Support de Multicast pour diminuer les broadcast.
- ✔ Signature des tables.

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 a ainsi toujours l'ensemble des routes à sa disposition. Dès que le nombre de routeurs et important, on peut segmenter en AREA pour éviter de passer trop de temps à calculer le meilleur chemin.

OSPF utilise la couche IP et non UDP. Il a un champ service spécial (pas un numéro de port).

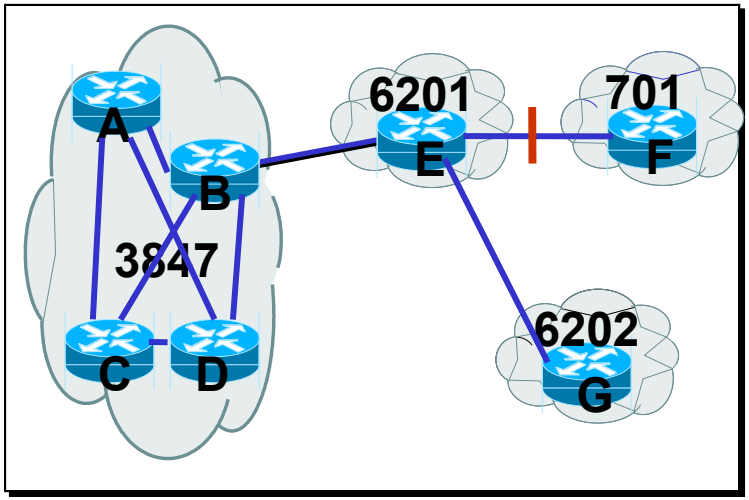
- ✔ OSPF peut gérer des routes différentes en fonction du champ qualité de service IP (3 bits et 8 possibilités) delay, throughput, reliability.
- ✔ A chaque interface est associé un coût qui peut dépendre du débit, du temps d'aller-retour.
- ✔ On peut diviser un système autonome en Area, et avoir des 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



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)

Les protocoles de passerelles extérieures (BGP4) RFC 1771



On parle aussi de routage inter-domaine.
Le problèmes des IGP est qu'ils ne s'intéressent pas aux aspects administratifs des réseaux. Il est donc apparu rapidement nécessaire de rajouter des informations à celles de base que sont le réseau, le préfixe, la métrique, et le next hop (passerelle).
On ne peut pas non plus se contenter des routes par défaut, car les réseaux sont maillés et donc redondants.
On vient donc ajouter des éléments tels que l'AS (Autonomous system), la communauté, la local pref.
Comme son nom l'indique, BGP veut dire Border Gateway Protocol. Il prend assez naturellement sa place à la frontière (Border) entre deux entités administratives, comme RENATER et FREE. Bien sur il est important de filtrer ce que l'on reçoit ou se que l'on émet, voir de changer les paramètres d'origine.

Un Autonomous System (Système Autonome) est défini par un numéro (16 bits). Il existe deux types, les publics qui vont être visibles dans le coeur de l'internet et les privés qui seront gardés en interne (64512 à 65535). Les numéros d'AS publics sont distribués aux opérateurs. Comme les adresses IP, il faut les demander aux RIR (ex: www.ripe.net)

Les routes sont annoncées soient manuellement soit par un report automatique de routes apprises par l'IGP ou par BGP.
Lorsque BGP apprend des routes, il peut les donner à l'IGP (par ex OSPF). En général, on évite de donner toutes les routes à un site feuille.

On distingue deux modes: eBGP et iBGP. EBGP signifie une session avec un AS extérieur alors que iBGP signifie une session avec un routeur BGP du même AS
Au sein d'un même AS, il peut y avoir plusieurs point de contact avec plusieurs autres AS. Tous les routeur de l'AS (dans le 3847 cf schéma) sont en session iBGP entre eux et communiquent leurs routes.
Dans le cas de gros opérateurs, le nombre de combinaisons étant trop important, on monte un route reflector. En fait c'est un routeur spécialisé avec lequel tous les routeurs de bordure (edge) communiquent.
Les sessions BGP s'échangent les réseaux puis les mises à jour. Le protocole est assez peu bavard. Les routeurs s'interrogent régulièrement cependant. Pour annoncer une route, il faut que celle-ci soit accessible via l'IGP.

Aggregation de réseaux
Les réseaux qui se suivent sont agrégés dans un préfixe plus court. On diminue ainsi le nombre de réseaux à transmettre.

Dampening RFC 2439
Lorsqu'une route disparaît puis réapparaît, celle-ci subit une pénalité, on évite ainsi de propager les instabilités d'un opérateur dans les autres réseaux. Il faut donc faire attention lorsqu'on doit faire des changement de configuration à ne pas faire tomber le peering BGP. Cisco a une commande « clear bgp soft » qui permet de repartir à zéro sans faire tomber le peering BGP.

exemple sur matériel extreme network:

```
U2SceEcoAix:3 # sh bgp neighbor
     Peer             AS    Weight State        InMsgs  OutMsgs(InQ)  Up/Down
-------------------------------------------------------------------------------
Ee--- 193.55.248.17   2457  1      ESTABLISHED   11727  11586 (0    ) 8:0:55:28
Ee--- 193.55.248.193  2457  1      ESTABLISHED   11122  11270 (0    ) 7:17:14:57

I-internal peer, E-external peer, e-enabled, d-disabled
r-route reflector client, c-send communities, m-EBGP multihop
BGP Peer Statistics
  Total Peers   : 2
  EBGP Peers    : 2
  IBGP Peers    : 0
  RR Client     : 0
  EBGP Multihop : 0
  Enabled       : 2
  Disabled      : 0

U2SceEcoAix:4 # sh bgp neighbor 193.55.248.17 received-routes all
Feasible Routes
---------------
  Destination        Peer            Next-Hop        LPref Weight  MED AS-Path
 i0.0.0.0        /0  193.55.248.17   193.55.248.17                  40 2457 65200 2457
*i139.124.243.0  /24 193.55.248.17   193.55.248.17                     2457 65206
*i139.124.242.0  /24 193.55.248.17   193.55.248.19                     2457 65251

U2SceEcoAix:5 # sh bgp neighbor 193.55.248.17 transmitted-routes all
Advertised Routes
---------------
 Destination        Next-Hop        LPref MED   AS-Path
```

NAT - PAT Network (Port) Address Translation

Comme on a vu précédemment, l'adressage INTERNET a de grosses limites en terme de disponibilité d'adresses. Dans la fin des années 1997, il est devenu évident que l'on allait vers la saturation. Une technique a été alors mise au point pour pallier à la pénurie, le nouveau protocole IPV6 n'étant pas encore assez mûr. Dix ans après, cette technique est abondamment employée, mais IPV6 commence à arriver. Le routeur fait de la translation d'adresse. Comment ça marche ?.
En fait on peut dispose de plusieurs réseaux privés dits RFC1918:

Le Classe A	10.0.0.0/8	16 millions d'adresses
Le Classe B	172.16.0.0/16	65536 adresses
Les Classe C	192.168.0.0/16	65536 adresses

Ces adresses ne seront jamais attribuées officiellement à un réseau public 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 la résolution d'adresse publique www.machin.com ne donnera une de ces adresses et qu'il n'y aura jamais de confusion. Il existe de milliers/millions de réseaux en 10.0.0.0/8

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 matérielles des routeurs. Cependant les routeurs centraux des grands réseaux ne font jamais du NAT. Celui-ci est fait en périphérie, à la sortie d'un réseau privé.

Le routeur a une petite série d'adresse (Un pool d'adresses) vue de l'extérieur [22], mais comme on va le voir, une classe C suffit amplement à connecter plusieurs milliers de machines. Par exemple, une consultation web consiste à afficher une page, la machine cliente ne reste pas connectée au sens TCP sur le serveur.

Plusieurs techniques sous ce vocable:
NAT
On change juste l'adresse IP source privée, le traitement est rapide.
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 échanger 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 gère un timer et fait tomber la correspondance si celle-ci est inactive trop longtemps. Comme les machines ne sont pas toutes en discussion au même moment, on peut ainsi avec peu d'adresses faire passer beaucoup de machines. Si on traite les postes clients avec du NAT, il existe encore pas mal de temps pour IPV4 [23]

Cependant certaines applications s'échangent des numéros de port pour communiquer. 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 PAT impose au routeur d'aller non seulement s'occuper des états des sessions TCP , mais aussi de regarder une partie des données.
Table de correspondance entre une machine 10.0.0.2 voulant discuter avec 193.50.125.2

	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 un bug de sécurité sur un poste client, le pirate aura plus de mal à retrouver une deuxième fois cette machine. Le routeur ne gère pas la session TCP, il remplace juste le numéro de port.

Problèmes : Et oui ça serait trop beau.. D'une part certaines applications 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.
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.
Suivant votre fournisseur d'accès et votre technique de translation, certains protocoles ne passent pas, car il faut activer des modules pour les VPN par exemple qui n'utilisent pas UDP/TCP (ex GRE et PPTP). IPSEC subit un traitement spécial appelé Nat-traversal.
Un NAT très complet impose d'aller voir dans les données, ce qui consomme de la performance dans les équipements.

Remarque: Avec un serveur proxy http, des serveurs SMTP ou de fichiers accessibles en intranet, un client peut ne pas avoir besoin d'être naté, car jamais il ne sortira sur internet. Seul le proxy http ira chercher l'information publique extérieure pour la lui fournir ensuite.
Les routeurs internes de l'entreprise, savent router les réseaux privés, et une machine en 10.0.0.0/8 est capable de joindre une adresse publique ou privée de l'entreprise.

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 :
ICMP est le protocole 1 (champ protocole sur 8 bits de la trame IP)

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.

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 progressivement 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. C'est un bon outil pour analyser les problèmes réseau.
IPV6 fait un appel plus important à ICMP. Il s'appuie sur des trames de multicast. Un des problèmes actuels (2007) est le manque de matériel de niveau 2 capable de gérer LMD (Listener

IPV6 rfc2460

C'est la nouvelle version du protocole IP. Elle est en gestation depuis 1994. Il se met vraiment en place depuis 2004. Parlons en un peu. Celle-ci ne touche pas TCP et peu UDP.
La configuration des adresses est automatique. On dispose au minimum d'adresses liens locaux.
Les adresses sont sur 128bits, notées en hexadécimal, et préfixées par l'opérateur. Ainsi nos adresses globales et officielles s'écrivent ainsi en notation CIDR (fini les masques..ouf)
L'internet IPV6 unicast officiel utilise le préfixe **2001::/16**.
RENATER s'est vu attribuer par son RIR (www.RIPE.net) le préfixe 0660.
2001:660:5402::/48 c'est notre préfixe vu du coté opérateur
:: veut dire tout à zéro. On ne peut l'employer qu'une seule fois dans l'écriture de l'adresse.
Nous allons pouvoir déployer 65536 réseaux physiques avec ce préfixe. Nous avons donné à notre réseau de serveur le 800 donc notre réseau s'écrit **2001:660:5402:800::/64**

L'adresse lien local.
L'adresse lien local commence par **FE80** et finit par l'adresse matérielle. Elle permet l'utilisation du réseau local sans configurer un équipement de routage, ce qui est bien pratique!
En IPV6 il est courant d'avoir plusieurs adresses sur la même interface.

Dans la partie droite des 64 bits suivants, on va trouver sauf configuration manuelle l'adresse matérielle complétée à 64 bits.. Les 64 bits sont nécessaires pour Firewire ou IEEE1394. Le but de tout cela est la configuration automatique des équipements. Le préfixe du réseau est diffusé en multicast ICMPv6 par le routeur.

Exemple d'une machine IPV4 et IPV6

```
eth0      Lien encap:Ethernet  HWaddr 00:14:22:0C:90:2A
          inet adr:139.124.132.145  Bcast:139.124.132.255  Masque:255.255.255.0
          adr inet6: 2001:660:5402:800:214:22ff:fe0c:902a/64 Scope:Global
          adr inet6: fe80::214:22ff:fe0c:902a/64 Scope:Lien
```

L'adresse de loopback
::1/128 Tout à zéro avec le dernier bit à un. Même usage que IPV4 127.0.0.1

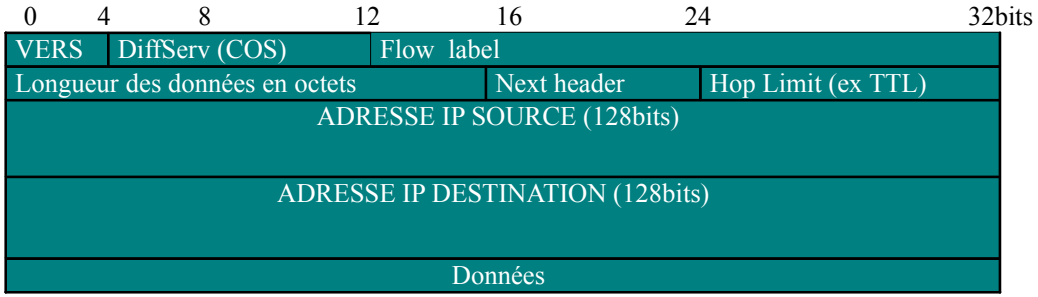
Le multicast
FF00::/8

Les adresse 6to4
2002::/16 On trouve l'adresse IP dans les 4 derniers octets écrits de façon décimale. Il s'agit d'une encapsulation de données. On 'appelle 6to4tunnel. Un en-tête IPV4 avec une encapsulation spécifique (protocole IPV6) et dont les données sont une trame IPV6. Les routeurs vont encapsuler ou decapsuler selon que la trame passe du monde IPV4 au monde IPV6

le broadcast devient multicast
C'est la fin des broadcast, si toutefois votre matériel de niveau 2 sait gérer LMD Listener Multicast

en 1, on émet un multicast IPV6 ICMP6 qui se transforme en mulicast ethernet sur l'adresse 33:33:ff:00:01:20
en 2, la réponse
en 3,4 des échanges de ping IPV6

Datagramme IPV6
Une simplification notable de l'en-tête malgré le rallongement des adresses.
L'en-tête (header) passe de 20 à 40 octets malgré les adresses multipliées par 4. La fragmentation n'est plus gérée par les routeurs, c'est l'affaire des extrémités qui doivent appliquer PMTU (Path MTU discovery)



Next Header est le champ service ou protocole en IPV4, par exemple TCP ou UDP (upper-layer header), mais il peut être autre chose comme la gestion de la fragmentation. Dans ce cas, il existe un en-tête qui suit (fragment header). On peut cumuler ainsi toute une suite d'options (routing, fragment, authentication, encapsulating, destinations option..)

IPV6 Header (40 Octets) Next Header = routing	Routing Header Next Header = Fragment	Frament Header Next Header = TCP	Fragment of TCP header and data

Flow label est une valeur aléatoire et unique générée par la source. Par exemple, tous les paquets d'une session TCP auront une même valeur. Ceci permet ainsi de faciliter la tache des routeurs.
Une fois résolue la route, il suffit de lire le label et la source.

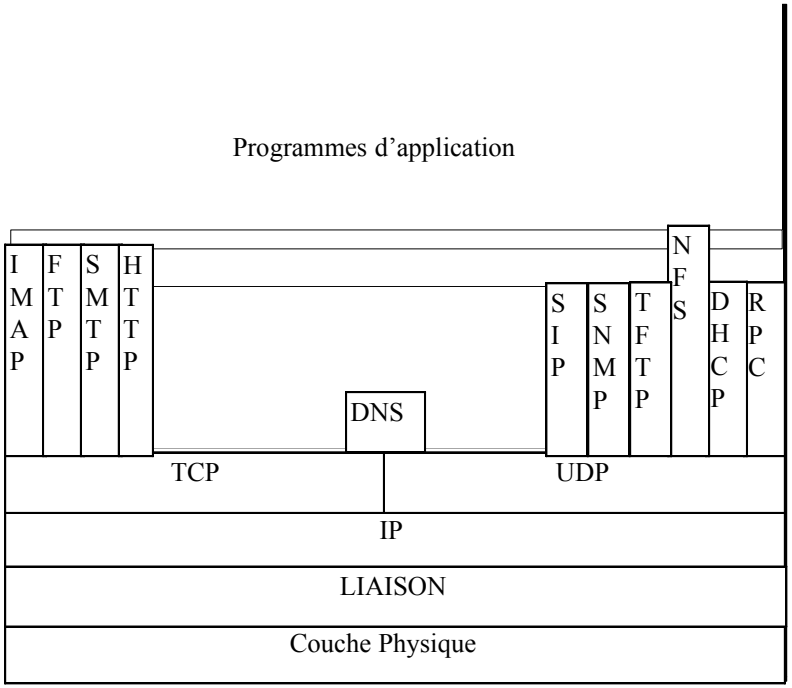
Le checksum de l'en-tête a disparu: c'est du ressort de la couche 2. De toute façon, le Hop count (ex TTL) étant touché (décrémenté), il faut à chaque routeur IPV4 recalculer le checksum!

Transition
Il existe plusieurs solutions: la double pile IPV4 et IPV6, et les tunnels. Tout dépend de savoir si on est dans un mode IPV4 seul, ou IPV6 seul, ou les deux à la fois. Le fait d'utiliser IPV6 résulte en fait d'une résolution DNS. On a rajouté des RR dit « quada » (AAAA) qui donne l'adresse IPV6. Si ce RR est disponible, alors la machine qui a une pile IPV6 va essayer de contacter en IPV6. Si la route est invalide, elle va essayer en IPV4.
On peut aussi mettre des serveurs proxy http pour les machines purement IPV6. Le but du jeu est

LE TRANSPORT IP

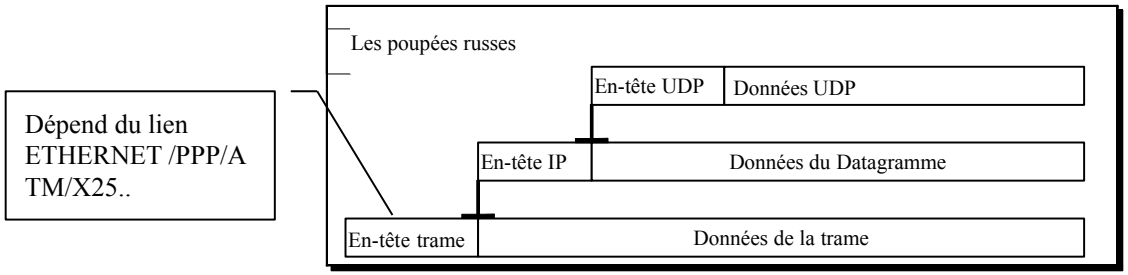
UDP ou User Datagram Protocol

Architecture IP :



UDP est le protocole IP 17.
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.

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 (wellknown ports):
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 [28]. 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

Choix des couples adresses, port

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
- ✔ la vidéo, le son en direct pour lequel, on ne peut gérer des erreurs à la façon TCP
- ✔ le multicast UDP toujours. TCP est de type unicast, entre deux machines. UDP permet de recevoir un flux avec un dialogue minimal du client.

TCP (TRANSMISSION 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 le protocole IP 6

- ✔ 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, en tout 20 octets

Port source (16 bits)										Port destination (16 bits)
Numéro de séquence sur 32 bits										
Numéro d'acquittement sur 32 bits										
Longueur en-tête (4 bits)	réservé (4)	CWR	ECN	URG	ACK	PSH	RST	SYN	FIN	taille de fenêtre sur 16 bits
Somme de contrôle TCP										Pointeur urgent sur 16 bits
Options éventuelles										
Données										

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

Détail d'une ouverture de session

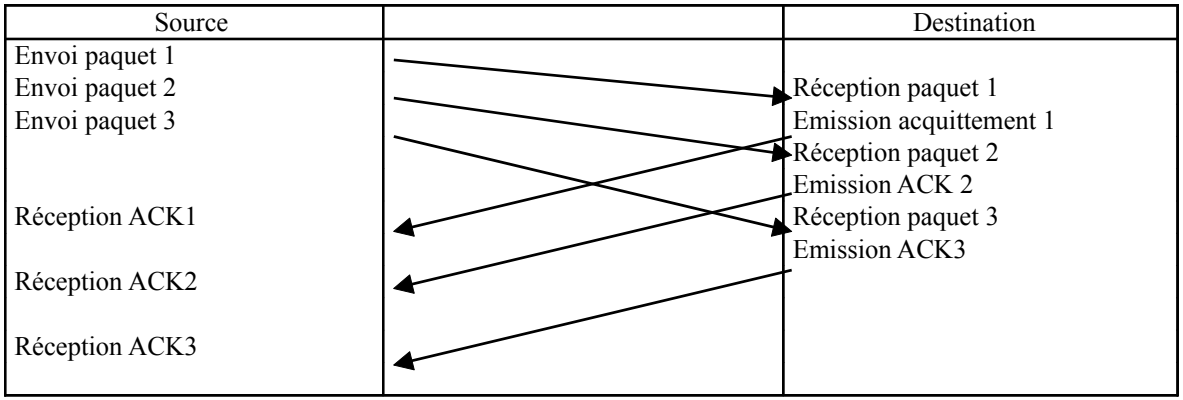
Le client envoie un segment TCP avec le bit SYN positionné à un. Il envoie son numéro de séquence ainsi que la taille de sa fenêtre (**WIN**) et la taille maximum de son segment (**MSS**). Il effectue ce que l'on appelle une ouverture active.
Le serveur va acquitter cette ouverture avec le bit SYN et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



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 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, 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 [31]. 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.

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.

Les états de la liaison qui n'existe que pour TCP (voir netstat)

LISTEN	en écoute
SYN-SENT	début
SYN-RECEIVED	début
ESTABLISHED	connexion établie
FIN-WAIT-1	fin
FIN-WAIT-2	fin
CLOSE-WAIT	fin
CLOSING	fin

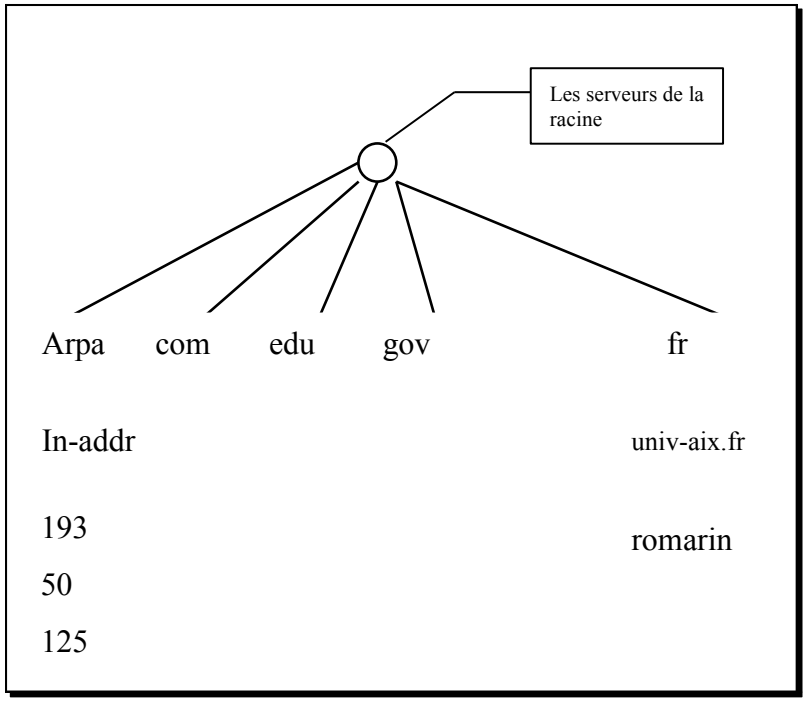
APPLICATIONS

DNS 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 [32].

Les noms sont composés par une suite de caractères alphanumériques encadrés par des points [33].
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)

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 [34] (ses collègues) pour la résolution. Tout d'abord, il va faire appel aux serveurs de la racine. Il s'agit de 13 serveurs dont les adresses sont figées dans la configuration du serveur [35]. Dans la cas ou l'on cherche www.linux.org, on va appeler la racine pour demander qui gère le domaine org. 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 (TTL de la zone ou de l'enregistrement) . 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 TTL quelques jours avant, afin que les noms soient gardés le moins longtemps possible dans les caches de résolution. 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 DNS ne faisaient aucun cache. Microsoft a initié une autre politique, les machines clientes windows gardent en cache les résolutions pour la valeur du TTL donné en réponse qui est d'une journée la plupart du temps. La commande ipconfig /displaydns permet de voir le cache. Coté Unix, on commence aussi à voir apparaître ce fonctionnement.

Configuration d'un serveur de nom :

Le fichier **/etc/named.conf** 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
```

```
                                7200    ;retry[37]              : 2 heures
                                3600000 ;expire[38]             : 41 jours
                                86400 ) ;minimum[39]            : 1 jour
```

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 ou TTL indique la durée de validité de chaque enregistrement.

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     86400    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 IPV4
SOA	Start of Authority
MX	Redirection du courrier
AAAA	Adresse IPV6

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'information 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.
```

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

Les commandes utilisateur Unix : [40]

host romarin ou
host 193.50.125.2
host -t mx univmed.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

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. Êtes vous bien sur qu'il sont actifs et bien configurés? Sinon ce seront 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).

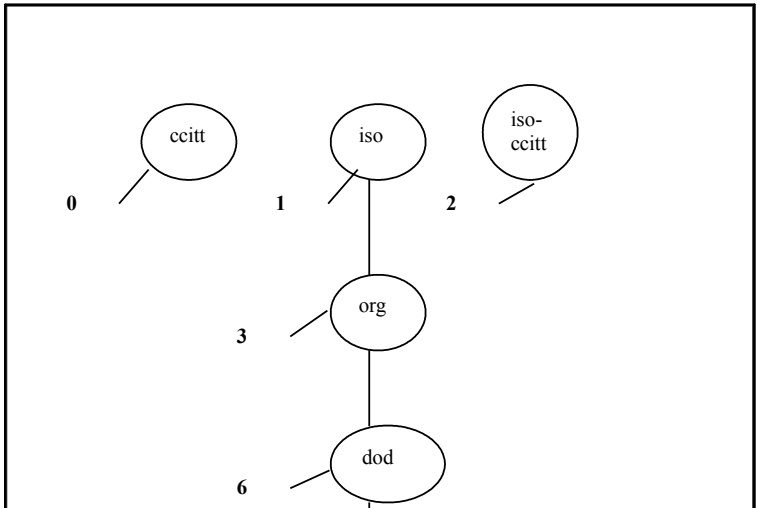
SNMP

Simple Network Management Protocol **RFC1155/1157**

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[41]. 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

```
        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
        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
```

```
        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 de graphiques Gif ou PNG. Une évolution ("RRDTOOL") permet de nouvelles possibilités.
http://www.mrtg.org

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'administration clique bouton n'est pas tout à fait pour tout de suite..

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 [42] pour router les trames vers un serveur BOOTP particulier, celui ci

Les évolutions de BOOTP : DHCP

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. Si la machine reboote et que le bail n'est pas dépassé, aucune demande n'est envoyée à un serveur.
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.
DHCP client 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 et 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 !». On peut associer aussi une adresse matérielle ethernet à une adresse IP

Attention aux problèmes de sécurité: Ne réserver DHCP qu'a des machines quelconques ou des portables. Il est très facile à un virus de singer un serveur DHCP et de rendre votre réseau inopérant!.

Internet Software Consortium (ISC) soutient plusieurs logiciels importants: BIND (DNS) et DHCP. Il existe donc une implémentation libre et riche permettant de retrouver des fonctions de BOOTP dans 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 [43].
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 !.

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

Il existe deux modes:

- Le mode active historique
- Le mode passive

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)
Le 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.
Dans le cas de passive, c'est le serveur qui ouvre un port et indique au client de s'y connecter. Le mode passive est devenu le mode par défaut car il permet de passer à travers les parefeux. Dans le cas de active, c'est un serveur FTP qui se connecte sur une machine. Les parefeux, le plus souvent interdisent ce fonctionnement sauf s'il sont à état (statefull).

En fait un serveur FTP 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. Ça sert surtout pour voire un fichier README écrit sous

Les serveurs FTP anonymes ont tendance à être remplacés par des serveurs HTTP, bien plus souples.
Dans les défauts de FTP, les attributs de fichier, propriétaires, types (records bloqués, variables..) ne sont pas transmis. C'est pour cela et aussi pour des besoins de compression que les fichiers sont de temps en temps regroupés dans des archives et donc stockés compressés avec des attributs de fichiers dans l'archive.
On trouve ces fichiers stockés sous les formats:

.gz (Unix)
.tar.Z (Unix)
.zip (Windows/Unix)
.gzip (Unix)
.hqx (Mac)

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)
```

FTP est resté le standard pour mettre à jour les sites web des internautes et il existe des versions clientes très intuitives et performantes. La transmission du mot de passe n'est pas cryptée. FTP est l'un des plus anciens protocoles avec TELNET.

Dans les transferts en entreprise, on pourra préférer SSH avec sa contrepartie de transfert: scp ou sftp ainsi que rsync

A retenir:

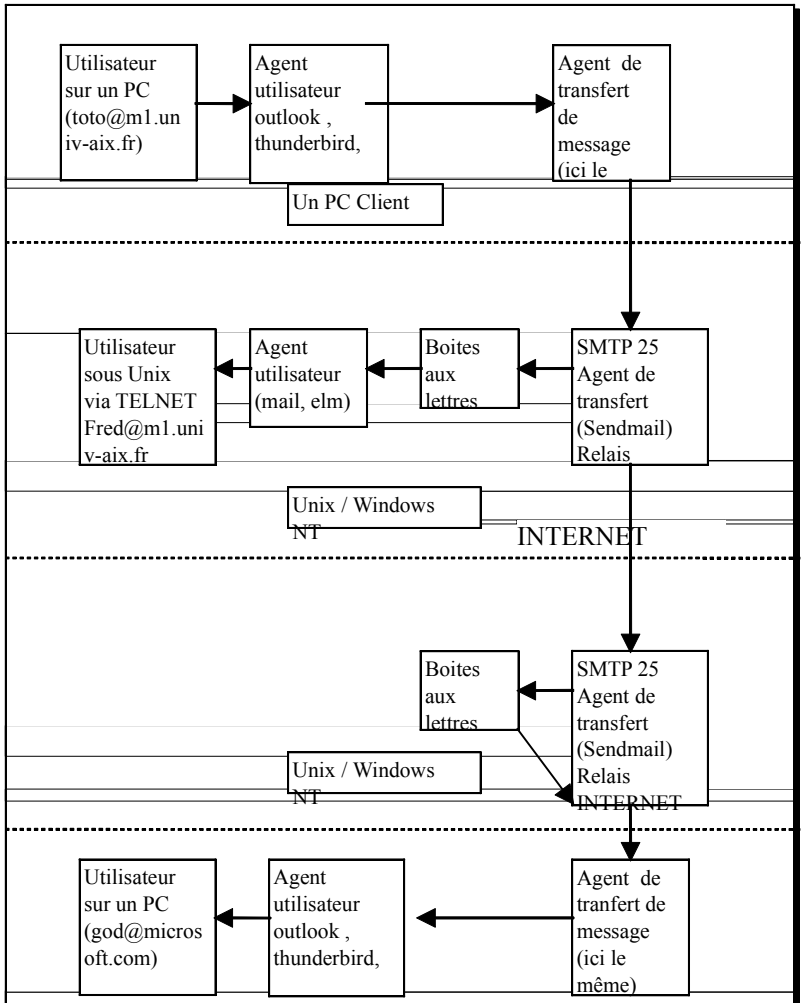
- ✔ le port de commande et le port de données
- ✔ un protocole un peu complexe pour passer la translation d'adresse.
- ✔ Des mots de passes non cryptés

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 chiffres suivis 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



POP

Le micro ordinateur vient récupérer ses courriers par l'intermédiaire d'un second protocole **POP** (Post Office Protocol) ou IMAP. 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. Le mot de passe est transmis en clair, sauf si l'on utilise la version cryptée POPS. Les courriers récupérés sont ensuite détruits du serveur. IMAP les laisse et ne récupère localement que les en-têtes.

Comme nous allons le voir SMTP est vraiment SIMPLE MAIL TRANSFER PROTOCOL. Il n'existe aucune identification certaine de l'expéditeur. Il n'est pas cher et facile à comprendre. La messagerie X400 qui est une norme OSI a bien du mal à décoller, et n'a toujours pas décollée 10 ans après cette remarque...

SMTP ne transfère que les caractères codés sous 7 bits donc pas de caractères accentués, mais l'extension (MIME) permet cela.

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.
Généralement, on voit ceci :

Client	EHLO 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> [44]
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 (récipient ou destinataire)
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

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.
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. [45]

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. Ceci est possible via les extensions SMIME.
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.

IMAP

Une version de POP qui gère la boite aux lettres utilisateur sur un serveur. Les messages restent

A retenir

La messagerie sur INTERNET est peu sécurisée et sommaire (pas d'accusés de réception fiables).
Mais ça marche!

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)

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

- ✔ 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 , les Listes

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 ½ Go 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

Un logiciel spécial va traiter des courriers qui arrivent à des utilisateurs fictifs. LISTSERV (ou MAJORDOMO ou SYMPA [47]) 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 [48].
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
http://www.sympa.org Sympa est un excellent logiciel développé par le Comité Réseau des Universités

HTTP HyperText Transfer Protocol (World Wide Web)

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, a été fait au CERN, Centre Européen de la Recherche Nucléaire par Tim Berners Lee.
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 d'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 navigateur.
Parmi ceux-ci on peut citer Netscape, INTERNET Explorer, Mosaic (l'ancêtre), FireFox, Opera, Konqueror, Safari.
Format du lien HTML ou URL
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.
On peut comparer HTTP à FTP, en plus simple. Il ne s'occupe que de transférer des documents. Les commandes sont simples: GET ou POST.
Dans le cas de GET, les paramètres sont transmis dans l'URL.
Dans le cas de POST, les paramètre sont transmis dans les paramètres HTTP et sont invisibles dans l'URL.
Les commandes et réponses HTTP sont du texte simple. On va donc trouver:
Coté client:
la demande via une connexion TCP:80 sur la machine www.monsite.fr, suivi des commandes ou renseignements suivants:

GET http://linuxfr.org/pub/ HTTP/1.1

```
uri: http://www.monsite.fr/index.html
Host: linuxfr.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.8.1.9)
Gecko/20071025 Firefox/2.0.0.9
Accept: text/xml,application/xml,application/xhtml
+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

```
Cache-Control: no-store, no-cache, must-
revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=5, max=1023
Connection: Keep-Alive
Content-Type: text/html;
charset=iso-8859-15
Content-Encoding: gzip
Content-Length: 17768
```

le contenu suit cette ligne vide pour 17768 octects. Le client peut demander d'autres documents (option keepalive des serveurs) et fermer la connexion. Les commandes et transferts ont lieu dans la même connexion TCP. HTTP est bien plus simple que FTP. HTTP permet de passer tout type de documents, texte, images, html dont le type est indiqué par la phrase content-type. Le serveur peut aussi répondre par un « location: », indiquant un déplacement du document demandé, ou renvoyer un code d'erreur 404 indiquant un « document not found »
Le navigateur va ensuite interpréter le document reçu et l'afficher en fonction du type. S'il reçoit une page HTML, il va interpréter les TAGS et mettre les enrichissements.

Une page HTML minimaliste s'écrit ainsi:

<HTML>
<HEAD>
</HEAD>
<BODY>
</BODY>
<P>Ceci est un mot en <B>police grasse</B></P>
</HTML>
Voir le site http://www.w3c.org pour plus d'explications sur les TAGS et le HTML. Ceci n'est plus à proprement parler un cours de réseau, mais un cours sur la technologie web.

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) définit une extrémité de la connexion. On trouve ces fonctions dans la plupart des langages mais ont été initialement écrites pour le langage C sous Unix.

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 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. Cette primitive est utilisée par un service pour se mettre à l'écoute du réseau sur un port précis. Voir listen plus bas.

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

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 / digoutils 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 (historique)

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.

Windows

ipconfig

arp -a

ping

netstat

nbtstat netbios statistiques sur IP

winipcfg configuration IP

route

```
        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
```

```
 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
```

```
    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 (historique..)
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 spécifications 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

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. C'est ce vers quoi il faut aller dans les entreprises.

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.
DLC	utilisé par SNA.
IPX/SPX	Utilisé par NOVELL mais aussi par NETBIOS avant windows98

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

Le réseau MICROSOFT
Le réseau de MICROSOFT est lié à une origine IBM **netbios.** Cependant, MICROSOFT a fait un effort en direction de TCP/IP ce qui permet d'utiliser facilement les protocoles au travers d'une interconnexion IP.

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\répertoire\fichier**
à noter que pour NOVELL , c'est : /serveur :volume\répertoire\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.

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 windws ou Unix (SAMBA). 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

Les commandes ligne de réseaux locaux de PC

MICROSOFT

Une seule commande, la commande NET, mais beaucoup de paramètres (voir aussi NBTSTAT)

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

Active Directory

Depuis WINDOWS 2000, Microsoft exploite complètement TCP/IP. Ils ont donc levé les limitations liées à netbios et au réseau local. La résolution s'appuie sur les zones DNS et des enregistrements spéciaux. Trouver un serveur de domaine passe en dernier par une résolution de type broadcast.
Une fois connecté à un domaine, avoir la liste des machines actives et des partages est facile.
Avec l'Active Directory, on bénéficie d'une administration centralisée d'un parc de machines. On peut donner des droits sur des logiciels, paramétrer les logiciels à distance, télécharger les dernières versions automatiquement.
La gestion des utilisateurs et des machines se fait dans un annuaire de type LDAP et s'appuie sur le protocole KERBEROS
Une partie de ces possibilités est émulée par le logiciel SAMBA qui tourne sur des systèmes Unix.

LA SECURITE

Vaste sujet que la sécurité informatique. 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-end. 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** Un serveur est arrêté et un pirate monte un cheval de Troie. Est ce j'envoie mon mot de passe à la bonne machine?
- ✔ **ARP SPOOFING** Une machine se fait passer pour un routeur en jouant sur les annonces ARP et détourne le trafic.
- ✔ **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 bien configuré.
- ✔ **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). On peut aussi empoisonner les caches de résolution des machines locales.
- ✔ **BUFFER OVERFLOW**. La meilleure de toute sur les systèmes Unix et windows. Ceci conduit parfois à une prise de contrôle à distance de la machine. 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 réseau et systèmes 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. A provoqué 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**…

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.
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 IP sont autorisées à accéder à quel service. Surveillez les logs (/var/log/secure ou/var/log/messages sous Linux)
Les couches parefeu des systèmes Unix sont bien pensées et efficaces (iptables netfilter..)

✔ **Les serveurs windows**
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.
Lourds, gourmands 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

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

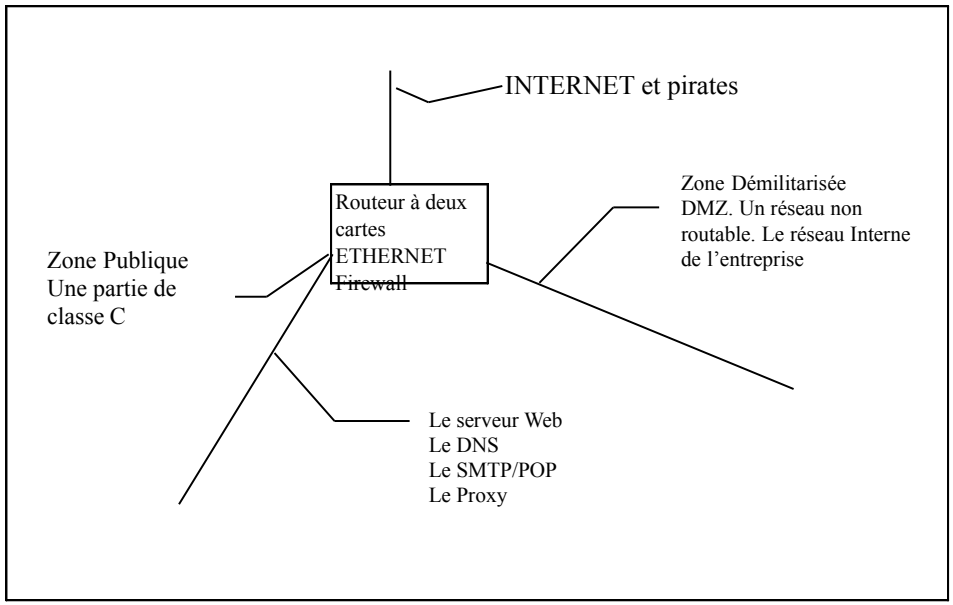
Ces commandes ont un sens d'application, on dit que l'access list s'applique en entrée ou sortie de l'interface. Ceci permet surtout de contrôler totalement le réseau. En effet en Interne tout le monde peut bricoler un serveur mal configuré. Grâce à la politique des Firewall, ce serveur « non déclaré » 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. [50]



commande xterm –DISPLAY=adresse IP du pirate. Et un joli shell apparaît sur le terminal X du pirate.

6. Si par paresse « normale », vous voulez des rcommandes, privilégiez ssh qui est un bijou.
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. Pour tous les services réseaux qui sont actifs, consultez fréquemment news://comp.os.security.announce

Programmation d'un Firewall central.

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

Baser sa sécurité sur un système étranger dont on n'a pas les sources. Est ce une bonne solution ?. 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)
```

Parefeu à état:

La couche parefeu peut être à état. C'est la solution que je préconise sur les serveurs. La couche parefeu va surveiller l'état des sessions TCP et mettre au rebut tout ce qui n'est pas conforme. Faire tourner le même système en central nécessite des machines spécialisées et chères. Je préfère des routeurs parefeu sans état et des serveurs avec parefeu à état.

Automatisation des mises à jour de sécurité

Quelque soit l'OS, c'est la régle numéro un. Coté windows, il faut bien trop souvent redémarrer le serveur, ce qui n'est pratiquement pas le cas sous Unix (juste les services).

Remarques :

- ✔ Une sécurité forte peut être brisée par une simple ligne téléphonique, une clef USB, une installation WIFI mal maitrisée.
- ✔ Un logiciel de tunneling peut permettre de contourner de simples ACL basées sur des adresses

CRYPTAGE

Les bases:
Le cryptage moderne utilise des techniques mathématiques de très haut niveau. Le but de ce document n'est pas de rentrer dans ces détails, mais d'essayer d'expliquer celui-ci de manière simple.
Pour chiffrer un message, on utilise les techniques suivantes:

- ✔ Blocs chaînés et chiffrés de taille fixe 64 à 128 bits -> ne pas reconnaître la structure de départ et ne pas faire de codage basé sur le caractère (le E apparaît souvent en français..). On utilise des permutations circulaires, des substitutions, on hashe.
- ✔ Utilisation de clés de chiffrements de longueurs 56,128,256,512,1024 bits. Plus la clé est longue, plus le décryptage est long.
- ✔ Les méthodes de cryptage symétriques ont pour nom DES (Data Encryption Standard) la plus vieille et la moins sûre, 3DES,RC4,BlowFish,AES (la plus récente, rapide et sûre).

On appelle cryptage symétrique lorsque la clef est la même des deux cotés.

Cryptographie à clef publique/privée:

Ceci fut une révolution. En effet, pour crypter, il faut se communiquer un secret partagé. Par téléphone, email (dangereux), poste…
L'algorithme, clé publique/clé privée permet de crypter des communications de manière automatique avec des millions de personnes. Il se trouve principalement sous deux formes: Diffie Hellman et RSA.

1. Diffie/Hellman:
Soit 2 personnes, Alice et Bernard:
Soit **G** un nombre public, Alice utilise un secret **X** et calcule $\mathbf{G}^{\mathbf{X}}$. Elle envoie cette valeur à Bernard. Bernard de son coté utilise son secret **Y** et calcule $\mathbf{G}^{\mathbf{Y}}$, et l'envoie à Alice. Alice et Bernard peuvent alors calculer $\mathbf{G}^{\mathbf{XY}}$.
Cependant si quelqu'un espionne la transmission, le système ne marche pas. On utilise alors l'opération modulo avec un nombre public **P**. Alice transmet alors $\mathbf{G}^{\mathbf{X}}$ **modulo P**. De même Bernard lui envoie $\mathbf{G}^{\mathbf{Y}}$ **modulo P**. Par ce système, Alice et Bernard ont chacun deux clés, une secrète (X ou Y), une publique $\mathbf{G}^{\mathbf{XouY}}$ **modulo P.**
Bernard va utiliser la clé publique de Alice pour envoyer son message à Alice. Celle-ci sera la seule à pouvoir décrypter le message avec sa clé secrète. L'opération modulo étant irréversible (c'est juste le reste d'une division), il est impossible de remonter sur X ou Y. Sauf grande découverte mathématique, qui mettrait à mal la Net Économie!.

RSA:
Fondé sur la factorisation des nombres. Il est très facile de multiplier deux grands nombres premiers, très difficile de les décomposer en facteur premiers le produit obtenu. Sauf si une méthode révolutionnaire arrivait à factoriser rapidement!. RSA a fait l'objet d'un brevet limitant son utilisation en dehors de États Unis. Ce brevet est tombé dans le domaine publique en 2000.

En fait, ces algorithmes à clés publique/privée demandent une grosse puissance de calcul (les

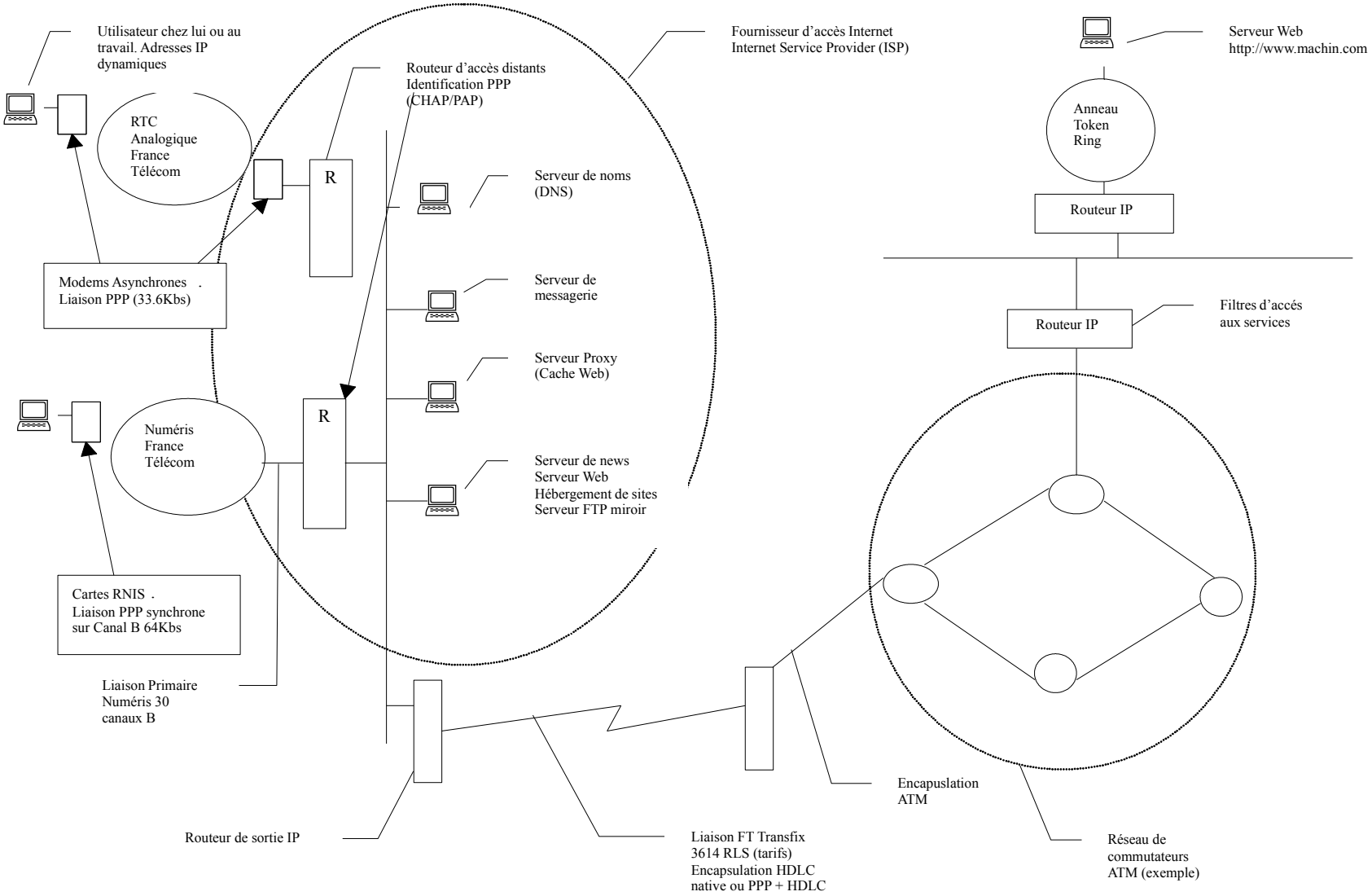
Pour décrypter un message sur 128bits, il faut tester en gros 3*10 [38] combinaisons, ce qui prend un temps littéralement astronomique.

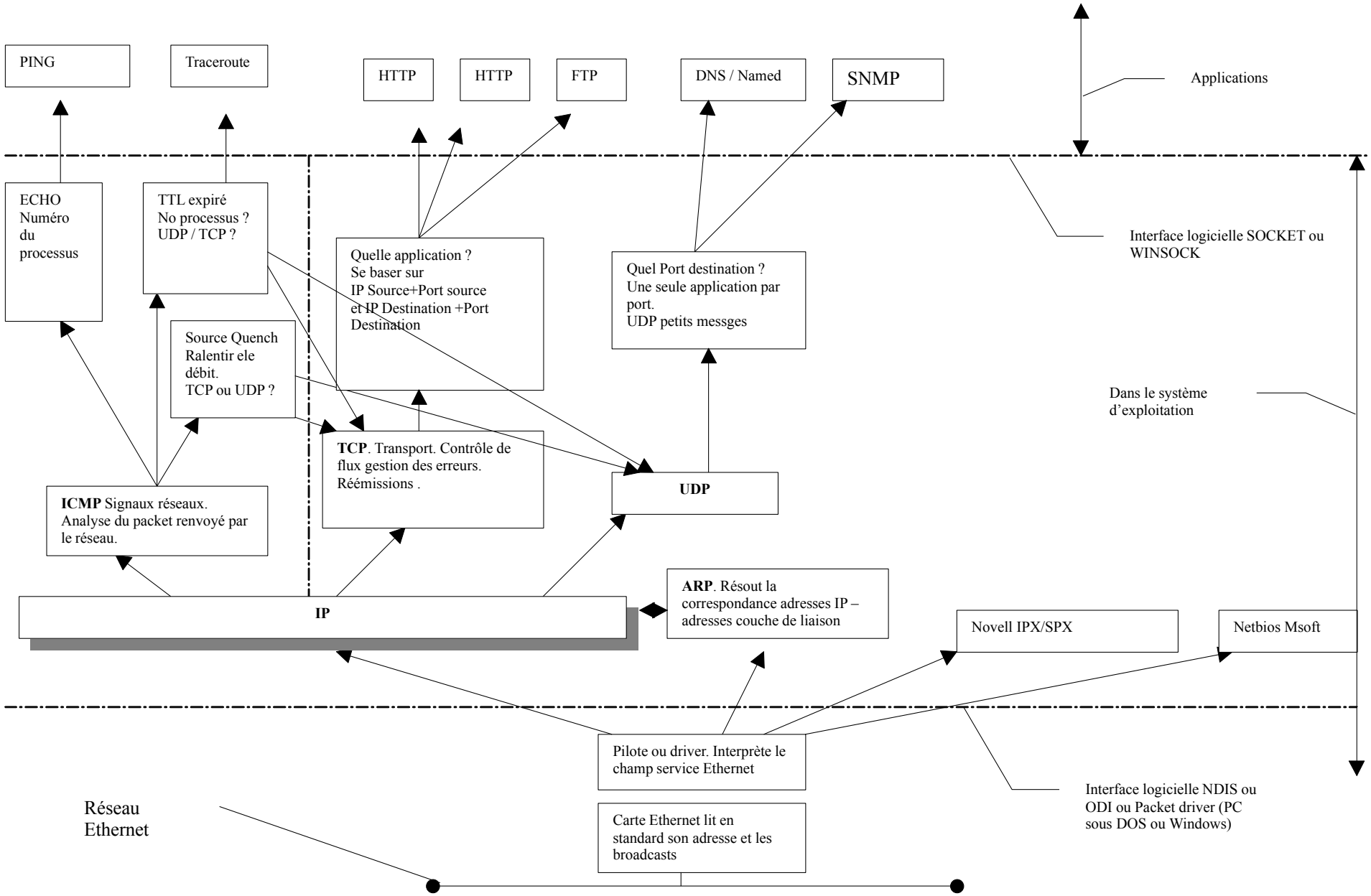
Décret français du 19 Mars 1999.
Il est possible d'utiliser en France tout logiciel dont la clé est inférieure à 128 bits. Au delà, il faut déposer sa clé. C'est une grande victoire pour la protection de nos systèmes d'information. Avec 128bits, au mieux, il faut des années pour décrypter.
Utilisation du cryptage dans les systèmes informatiques:
Un des premiers outils à avoir "démocratisé" le cryptage, fut PGP (Pretty Good Privacy). Le cryptage n'existait auparavant que pour crypter les mots de passe. Ce style de cryptage est à sens unique, on ne peut décrypter que par force brute et vérifier que par comparaison. PGP en mettant en œuvre les cryptages à clés publiques a permis de chiffrer des fichiers, de signer des emails..
On peut en effet transmettre en clair un email signé par PGP. La vérification de la signature montrera que le texte n'a pas été altéré. C'est un progrès énorme par rapport à une signature classique. La norme SMIME est venue généraliser la signature des emails basée sur des certificats clients. Le certificat délivré par une autorité de confiance contient l'email de la personne. Avec PGP, il faut télécharger les clefs des utilisateurs.
Netscape a créé **SSL** (Secure Socket Layer) pour crypter les accès au Web. Cette librairie de cryptage est depuis largement utilisée dans de nombreuses applications.

Il existe à ce sujet plusieurs façons d'opérer le cryptage:

- ✔ Les applications qui ont été "sécurisées", elles sont modifiées (c'est assez peu de travail car la librairie fait tout) afin d'intégrer la sécurité. On peu citer: HTTPS, IMAPS, POPS, SSH, SMTPS qui sont les formes cryptées des applications. SSL utilise les algorithmes à clés publiques/privées pour transmettre des clés secrètes qui serviront ensuite à crypter les échanges. On peut aussi utiliser un wrapper qui va rajouter la fonction de cryptage. Ces applications sécurisées ont des ports spéciaux réservés, différents du mode non sécurisé. La librairie [51] la plus connue dans le monde des logiciels libres et OPENSSL.
- ✔ L'utilisation de VPN (Virtual Private Network) qui vont crypter les transmissions en clair ou pas. On parle de IPSEC, PPTP, VPNSSL. Les VPN peuvent crypter des clients isolés ou des réseaux entre deux routeurs.
- ✔ Le cryptage de la couche de liaison. WIFI et WPA par exemple.

Sécurité et confidentialité:
Comme dirait Wietse Wenema auteur de Postfix, logiciel opensource réputé de transfert de courrier. Faire dépendre une application d'une librairie de cryptage, veut dire être dépendant de milliers de lignes de code complexes. Les erreurs dans ces libraires peuvent aboutir à une faille de sécurité. La dernière faille sur OPENSSL nous a imposé de revoir la plupart de nos services.
Le crytage est donc de la confidentialité, et si celle-ci protège la transmission d'un mot de passe, c'est aussi de la sécurité, mais la fiabilité de votre système peut en prendre un coup. Ne cryptez que l'essentiel.


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
Réseau de commutateurs ATM (exemple)
Serveur Web http://www.machin.com
Anneau Token Ring
Routeur IP
Routeur IP
Filtres d'accés aux services


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 Bibliographiques

Wikipedia: une très bonne source non disponible pour la première version.
http://fr.wikipedia.org
http://en.wikipedia.org

Comment ça marche: Du bon et du moins bon
http://www.commentcamarche.net

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

Richard Stevens Home Page (Auteur de TCP/IP Illustré)
http://en.wikipedia.org/wiki/W._Richard_Stevens. Cet auteur a marqué les esprits par sa clarté.

Le style décapant d'un grand gourou français.
http://www.bortzmeyer.org/index.html

Les RFC en français
http://abcdrfc.free.fr/

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

IETF INTERNET Engeneering Task Force
http://www.ietf.org/
IAB INTERNET Architecture Board
http://www.iab.org

Titres	Auteurs	Editeur
Télématique	MACCHI-GUILBERT	Dunod