Support de Formation en ligne

Cours réseaux

Support de cours réalisé pour la formation effectuée
du 29 Octobre au 9 Novembre 2001 à Bobo−Dioulasso au Burkina Faso

par Africa Computing en partenariat
avec l'Association Innovations et Développements.

Auteur : Marc Dovero

Support d'origine :
Ce cours est en principale partie
un résumé du support « Les réseaux informatiques »
de Dominique Lalot de la faculté d'Aix en provence.

Infos : service−formation@africacomputing.org

Africa Computing est un organisme de formation professionnelle
Déclaration DDTEFP n°93 13 10226 13.

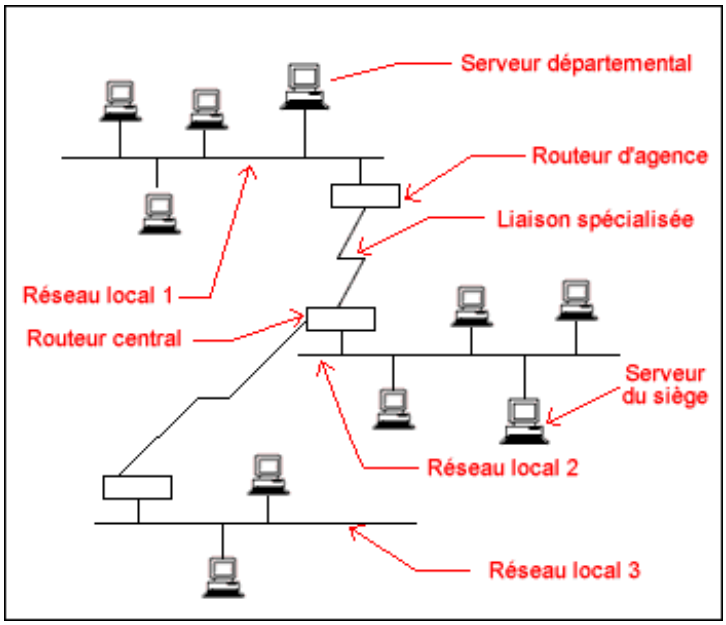
PLAN DE LA FORMATION

1. INTRODUCTION

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.

Un réseau informatique est composé d'ordinateurs, de routeurs, de liaisons et de réseaux locaux.



Les réseaux locaux permettent aux ordinateurs de communiquer entre eux sur un site (un bâtiment, une agence, un bureau). On utilise pour ces communications des technologies permettant aux ordinateurs de communiquer rapidement mais sur de courtes distances (100 mètres par exemple).

Ces réseaux locaux sont connectés entre eux par des liaisons spécialisées ou d'autres liaisons (Numéris par exemple) permettant de transporter l'information sur de longues distances (plusieurs kilomètres). Pour gérer ces liaisons et pour interconnecter des réseaux on utilise des ordinateurs spécialisés : des routeurs.

Note : ce cours est en principale partie un résumé du support "Les réseaux informatiques" de Dominique Lalot de la faculté d'Aix en Provence.

2. LE MODÈLE OSI (OPEN SYSTEMS INTERCONNECTION)

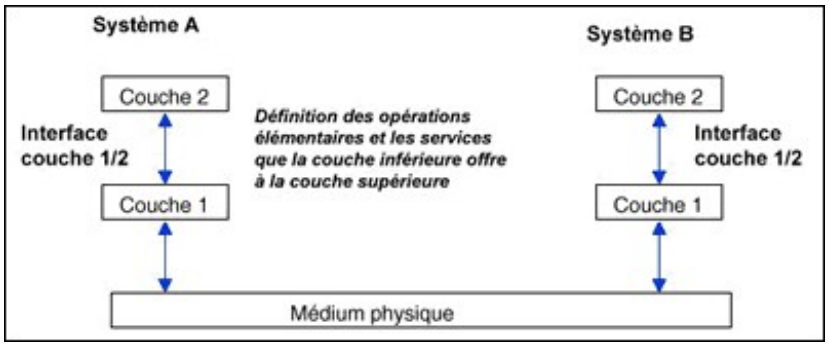
2.1. PRINCIPE

Modèle fondé sur un principe énoncé par Jules César : Diviser pour mieux régner.

Le principe de base est la description des réseaux sous forme d'un ensemble de couches superposées les unes aux autres.

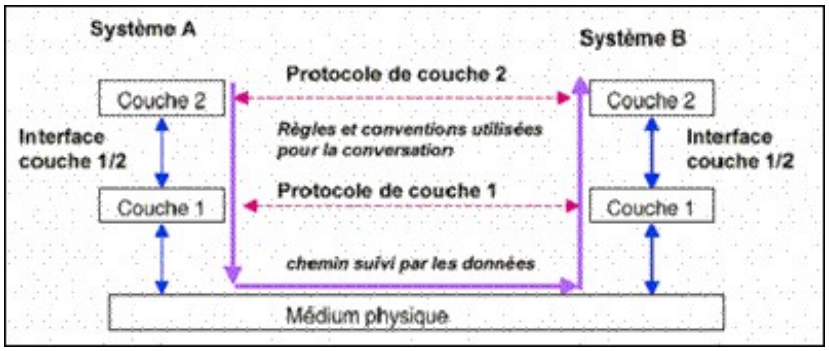
L'étude du tout est réduite à celle de ses parties, l'ensemble devient plus facile à manipuler.

Le nombre de couche, leurs noms et leurs fonctions varient selon les réseaux. L'objet de chaque couche est d'offrir certains services aux couches plus autres.



2.2. TRANSMETTRE DES INFORMATIONS

Les données émises d'un système A à un autre et encapsulé par le système A. Quand le système B veut comprendre les données émises par le système A, il "décapsule" les couches successives.



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.

2.3. ISO ET TCP/IP

TCP/IP ne suit pas scrupuleusement les préconisations de l'ISO. Les différentes couches de TCP/IP sont les suivants :

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. Par exemple : ethernet, fast ethernet.

Niveau 3 : Couche Réseau
On fait du routage dans les machines du réseau et du démultiplexage dans les extrémités. Par exemple : IP (Internet Protocole).

Niveau 4 : Couche Transport
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 bon exemple bien que développé indépendamment de la normalisation ISO.

Niveau 7 : Couche application
Toutes les applications réseau, messageries, transfert de fichier, etc. Les équipements de routage n'implémentent que les trois premières couches. Seuls les ordinateurs source et destination implémentent les 7 couches. L'utilisateur ne se sert que de cette couche là.

Il existe dans le modèle OSI deux autres couches, qui ne sont pas originellement présentes dans l'architecture TCP/IP.

Niveau 5 : Couche Session
Cette couche gère l'organisation du dialogue entre processus : l'initialisation, la synchronisation et la terminaison du dialogue. En n'étant pas très précis, on peut dire que la couche Netbios se situe au niveau 5 du modèle.

Niveau 6 : Couche Présentation
Elle prend en charge la représentation des informations que les entités d'application s'échangent.

3. LA COUCHE PHYSIQUE (NIVEAU 1)

3.1. LA TRANSMISSION

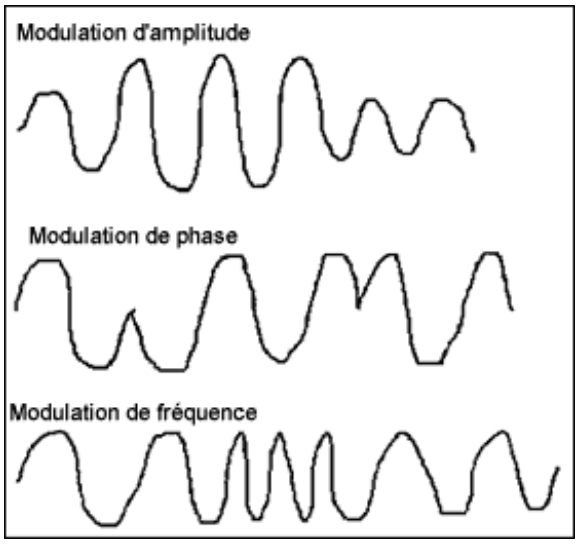
3.1.1. Transmission parralèle et transmission en série

La transmission posséde 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.

Il y a plusieurs types de modulations possibles pour coder les bits sur une liaison série :



3.1.2. Les supports de transmission

- Les fils (cuivre, or..),

- La fibre optique,

- Les signaux Hertziens (paraboles

- Les lasers (sans fibre) (

3.2. LES PRINCIPAUX MODES DE CONNEXION

3.2.1. Modem

Un modem est un appareil passif qui est connecté a un ordinateur, il est de fait géré par le système d'exploitation de l'ordinateur.

Le modem est connecté à une ligne téléphonique analogique. Quand on utilise le modem, on paye le prix d'une communication téléphonique.

Il constitue le moyen ideal de communication d'un poste de travail isolé.

A l'heure actuelle tout ordinateur est vendu avec un modem.

Un modem peut se connecter à un autre ordinateur possédant aussi un modem. On peut aussi se connecter à un réseau comme Internet grâce à des routeurs acceptants des appels de modems.

La vitesse de transmission et d'émission d'un modem varie de 14 à 56 Kbits/s selon les modèles.

3.2.2. Réseau numérique à intégration de services

Le réseau Rnis est basé sur le même modèle économique que les communications modems. La vitesse de communication est plus importante : elle est de 64 Kbits/s.

Il est aussi possible avec une ligne numéris d'avoir une communication a 128 Kbits/s, mais dans ce cas−là on paye le prix de deux communications téléphoniques.

RNIS 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 Kbits/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. On peut par exemple recevoir une télécopie pendant que l'on téléphone.

4. LA COUCHE LIAISON (NIVEAU 2)

4.1. 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.

4.2. NOTION DE TRAMES

Les informations binaires sont découpées en trames.
Une trame est un "paquet" d'informations regroupées entres elles.

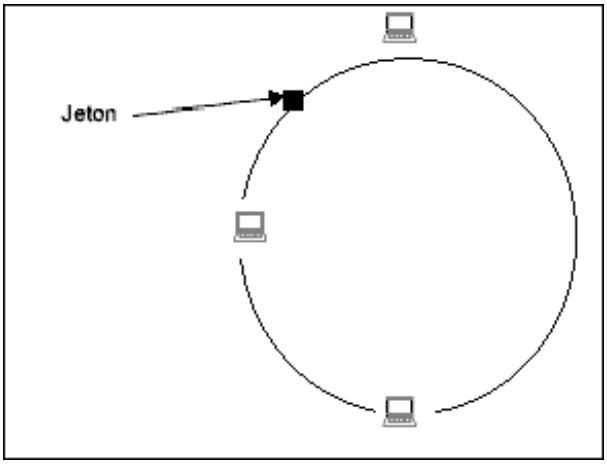
Sur un réseau local :

- A un instant donné, une seule trame circule sur le câble.
- Une trame émise par un équipement est reçue par tous les équipements.
- Une trame contient l'adresse de l'émetteur et l'adresse du destinataire.

4.3. TOKEN RING : ANNEAUX À JETON

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.

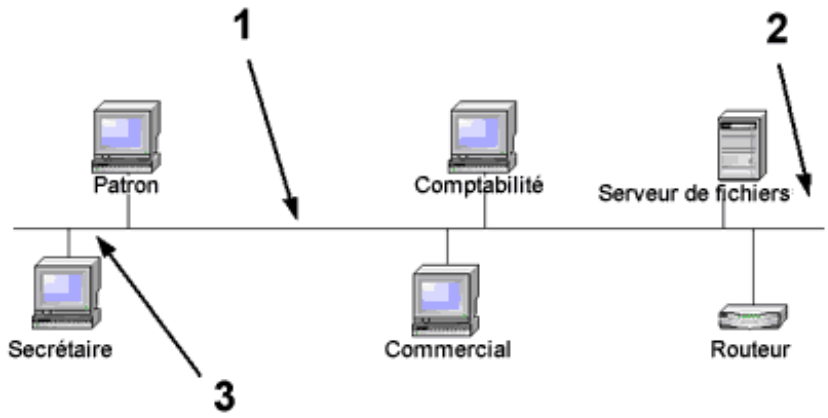


4.4. ETHERNET

Histoire : Le principal protocole de liaison utilisé sur les réseaux locaux est l'Ethernet, c'est un protocole normalisé (nombre IEEE802.3). ETHERNET a été développé par Xerox Corporation au Palo Alto Center (PARC) vers le milieu des années 70.

Des prix : début 80 une carte ETHERNET vaut 10.000 FF, maintenant 150 FF ! ! !

Le Bus Ethernet :



1 : Le câblage est réalisé avec du câble coaxial, qui ressemble à du câble d'antenne de télévision. La bande passante s'élève à 19 Mbps mais est mutualisée.

2 : Aux deux extrémités se trouve une résistance de terminaison. Par abus de language on appelle cette terminaison un bouchon.

3 : Chaque poste de travail est connecté au câble coaxial grâce à un T. Si une personne coupe le bus sur le T de son ordinateur, plus personne ne peut communiquer.

4.5. LE RÉSEAU ETHERNET EN BUS

Le principe est de mettre un support physique en commun, et de faire du très haut débit sur des distances moyennes (>100m).

On utilise dans la technologie Ethernet, 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 Mbps (10 Millions de bits par seconde). Un bit est une valeur binaire : 0 ou 1.

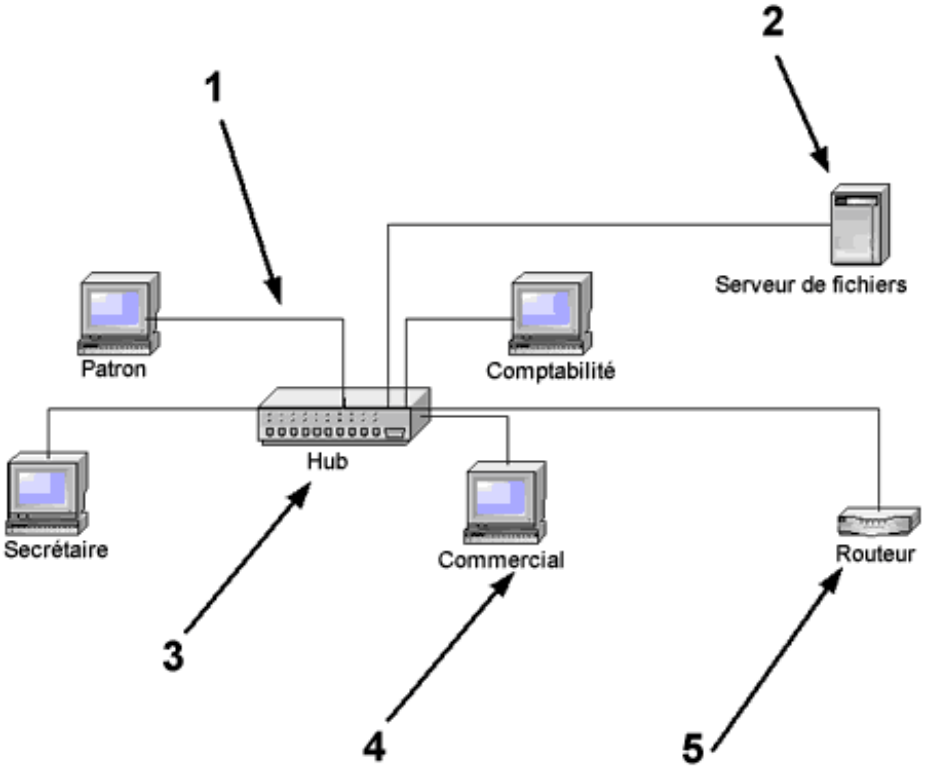
Cette technologie est appelée 10Base2.

Le câble coaxial fin est facile à mettre en place. Par contre les connecteurs affaiblissent le signal, du coup on ne peut pas mettre beaucoup de stations sur le câble. Cette technologie tend à être remplacé par 10BaseT aussi appelé « réseau ethernet en étoile ». De plus un problème sur le câble et toutes les stations se retrouvent privées de réseau.

4.6. LE RÉSEAU ETHERNET EN ÉTOILE

4.6.1. L'Ethernet 10baseT

Ethernet 10baseT



1 : Pour un réseau Ethernet, on utilise du câble réseau spécifique appelé paire torsadée (Twisted pai). En fonction de la bande passante nécessaire et des conditions d'environnement, on utilise du câble catégorie 5, 6 ou 7.

2 : Dans les entreprises, on trouve généralement un "serveur". Le serveur centralise la gestion des fichiers, fédère une base de données ou un service de messagerie.

3 : Le hub centralise les connexions de chaque micro−ordinateur et leur permet de communiquer entre eux.

4 : Chaque poste est relié au câble réseau grâce à une carte réseau insérée dans l'ordinateur.

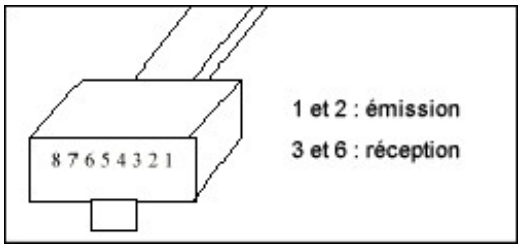
Ici le support est constitué de 2 paires de fils torsadés (twisted pairs), prolongés par des connecteurs d'extrémité appelés RJ45. Ces câbles vont dans des appareils appelés HUB qui connectent les machines.

Il existe des HUB 8 ports 12 /16/24 ports. En 85, la porte sur le Hub valait 2.000 FF, maintenant 300 à 400 FF. Les Hub peuvent être cascadés en local avec des câbles propriétaires. Ils ne forment alors qu'un seul ensemble. Les machines ne doivent pas être à plus de 100 mètres du Hub.

Sur ce type de réseau si un câble est endommagé une seule machine est privée de réseau (et non pas la totalité des machines comme sur les réseaux Bus).

4.6.2. Câblage d'une RJ45 sur réseau Ethernet 10BaseT

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.

4.6.3. Fast Ethernet ou 100BaseT

L'Ethernet en étoile a aussi une vitesse de 10Mbits/s. Il existe maintenant une technologie similaire mais plus rapide : le Fast Ethernet.

Pour faire fonctionner un réseau en technologie fast−ethernet il faut que le Hub et les cartes réseaux soient compatibles. De plus il faut que le câblage soit certifié Catégorie 5.

La mode de fonctionnement est exactement le même mais la vitesse de transfert est de 100 Mbits/s.

Il existe enfin une technologie mixte appelée 10/100 : cette technologie permet de connecter des ordinateurs à 100Mbits (si leur carte réseau le permet) mais aussi des ordinateurs à 10 Mbits pour les ordinateurs qui n'ont qu'une carte réseau 10Mbits.

4.6.4. Switch Ethernet

La technologie aidant, le prix des processeurs chutant, on voit apparaître des HUB intelligents appelé switch (commutateurs).

Un Hub classique émet la trame émise par un ordinateur à TOUTES les machines du réseau. Ce fonctionnement est historique : on reconstitue ainsi le mode de fonctionnement du bus (rappel sur le principe du bus : une machine émet des données qui sont émises a toutes les autres machines).

Les commutateurs sont capables de lire une trame et de la diriger sur l'un de ses ports en fonction de l'adresse de destination. Ainsi il n'y a qu'une machine qui reçoit la trame. Ainsi le réseau est fluidifié et est plus rapide.

5. LA COUCHE RÉSEAU (NIVEAU 3)

5.1. IP

5.1.1. 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 assurée par l'IAB (INTERNET Association Board) et ses deux bureaux l'IETF (INTERNET Engeneering Task Force) et l'IRTF (INTERNET Research Task Force).

5.1.2. Principes de base

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 leurs 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.

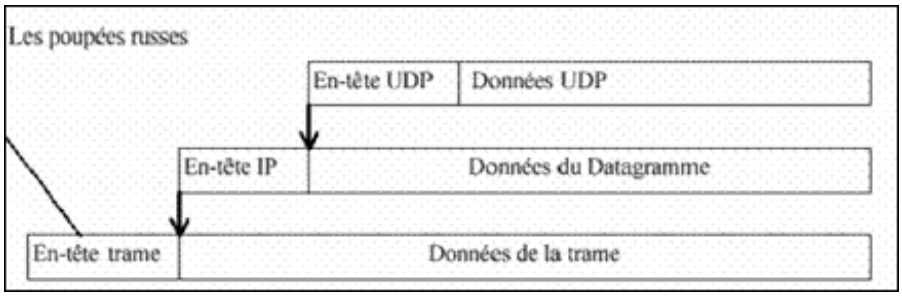
Cependant, Il faut distinguer les protocoles c'est à dire les "langages de réseau" et les entités administratives. En effet si un réseau parle "TCP−IP", il n'est pas forcément connecté à l'INTERNET. Ce n'est pas parce que je parle français que je suis français.

5.1.3. Mode de fonctionnement

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 orcément en même temps.

On appelle datagramme le paquet élémentaire. Celui−ci,comme une enveloppe de courrier, omprend une adresse de destination et une adresse de départ. Derrière les routeurs, on trouve des réseaux locaux, des liaisons spécialisées.

5.1.4. ISO appliqué à TCP/IP



L'entête Ethernet sur un réseau Ethernet c'est la première encapsulation : couche 2.

L'entête IP est présente dans la trame ethernet. Elle permet de diriger le paquet IP au travers du réseau IP. Le paquet IP contient un paquet UDP ou TCP qui permet de certifier la bonne arrivée des paquets. Les données du paquet UDP ou TCP dépendent de l'application utilisée.

5.1.5. Adressage IP

L'adresse IP est constituée de 32 bits, soit 4 octets notés de façon décimale de 0 à 255 (par exemple 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.

5.1.6. Les classes

Pour des raisons administratives et de routage, on regroupe ces adresses sous forme de classes. On pourra ensuite utiliser ces adresses à sa guise pour gérer son réseau. Ces adresses sont demandées auprès du NIC (Network Information Center). Le NIC France (l'INRIA) délègue la fourniture des adresses aux grands fournisseurs d'accès au réseau. Dans le cas de nos universités, toute nouvelle adresse doit être demandée à RENATER, organisme qui s'occupe du réseau de la recherche.

En principe l'adressage comprend donc 256**4 adresses c'est à dire 4.294.967.296 adresses (plus de 4 milliards !). En fait, on va voir qu'il y a beaucoup de pertes et que cet adressage est au bord de la saturation. Les adresses sont regroupées en différentes classes pour des raisons d'administration et de routage. La partie machine est réservée à l'usage du gestionnaire du réseau qui peut re−découper cette partie, c'est à dire "subnetter".

Classe A :

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

0	Réseau	Machine	Machine	Machine

Classe B :

- adresse sur 14 bits,
- commence à 128.

10	Réseau	Réseau	Machine	

Classe C :

La classe C, la plus utilisé en ce moment, du fait de la disparition des classes B devenues indisponibles par suite de manque d'adresses. Démarre donc à l'adresse 192.

110	Réseau	Réseau	Réseau	Machine

Classe D :

La classe D est utilisée pour des groupes de multicast. Commence à 224.

1110	Réseau	Réseau	Réseau	Machine

Classe E :

La classe E, réservée pour un usage futur, commence à 240.

1111	Réseau	Réseau	Réseau	Machine

5.1.7. Le réseau 127.0.0.0

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

5.1.8. Adresses spéciales

Il existe dans les réseaux trois types d'adresses, les adresses locales, les adresses de broadcast, et 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 sur ces différents types d'adresses. On verra que ARP est un broadcast ETHERNET, RIP est un broadcast IP/UDP qui sera convertit en broadcast ETHERNET, si ETHERNET est la couche de liaison.

Pour TCP/IP l'adresse de broadcast consiste à mettre les bits de l'adresse machine à un. Si 193.50.125.0 est mon réseau, 193.50.125.255 sera l'adresse de broadcast IP. Suivant comment est décomposé le réseau, la partie finale ne sera pas forcément 255. Par contre pour un réseau de classe C non subnetté, ce sera toujours le cas.

5.1.9. SubNets

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

Si on veut décomposer 34.0.0.0 en beaucoup de sous réseaux, de 256 machines, il faut prendre un subnet mask de 255.255.255.0. Pour décomposer en réseau de 256*256 machines, on faut prendre un masque de 255.255.0.0. Cette information concerne, les routeurs et les machines du réseau. Elle définit ainsi la famille de la machine. Le subnet, veut dire que la machine appartenant à un réseau de type 255.255.0.0 pourra adresser directement 256*256 machines sans passer par un routeur.

5.1.10. Exemple de Subnet

Exemple de sous adressage d'un réseau de classe C :

On veut découper un réseau de classe C en sous réseaux de 32 machines. De 0 à 31, nous avons 32 possibilités. 31 s'écrit en binaire : 11111 (5 bits). Si l'on admet, cas courant que l'adresse du réseau est dans les 3 bits restants à gauche (les trois bits de poids fort), nous avons huit sous réseaux. Le masque représente la partie réseau, soit les bits 6,7,8. Le 6 ième vaut 32, le 7 ème 64, le 8 ème 128. Le masque s'écrit avec tous ses 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.

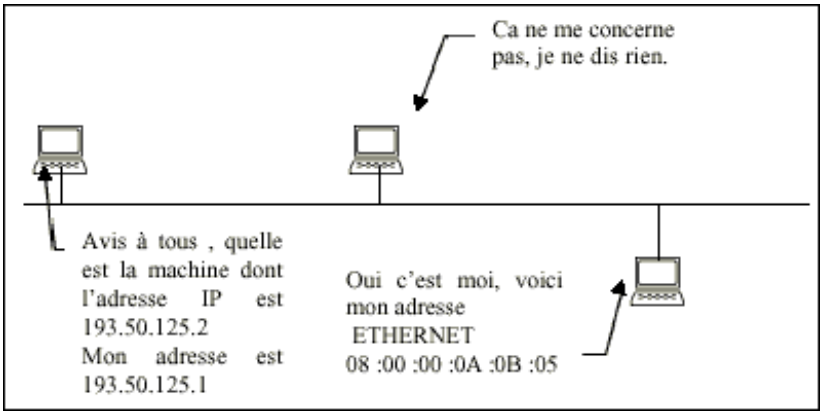
193.50.126.97 11000001.00110010.01111110.01100001 Masque 11111111.11111111.11111111.11100000

Les 8 réseaux possibles seront donc :

000=**0** 001=**32** 010=**64** 011=**96** 100=**128** 101=**160** 110=**192** 111=**224**

5.2. ARP

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



Pour parvenir à avertir tout le monde, au niveau ETHERNET, on utilise comme adresse de destination, une adresse de diffusion. Comme cela, toutes les machines lisent la trame, et celle qui a la bonne adresse répond. Evidemment, si la machine est arrêtée, aucune réponse n'arrivera. Il se peut aussi qu'une autre machine ait pris cette adresse. A ce moment là, c'est la plus rapide qui sera enregistrée. Ceci peut arriver, si les deux ordinateurs ont été configurés par une copie de disquette. Ou si quelqu'un essaye de pirater le réseau en se faisant passer pour un autre ! Il existe une commande qui s'appelle arp et qui donne la correspondance entre numéro IP et numéro ETHERNET.

```
arp −a
```

Cette commande existe sous Unix, Windows95 et NT.

ARP correspond à 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 seraient interrompues pour lire la trame, les ponts et les commutateurs devraient tout laisser passer.

5.2.1. Cache et Timeout

Une fois cette résolution obtenue, l'adresse est mise dans un cache en mémoire, celui ci peut être effacé par la commande `arp -d` (cas où un serveur du réseau vient d'avoir sa carte changée). Ce cache doit être rafraîchi périodiquement, une machine inactive (pas de paquets reçus depuis un certain temps) est retirée de ce cache, ceci arrive entre 10 et 20 minutes selon les systèmes. Il est possible de rentrer de manière statique l'adresse d'une machine, a des fins de sécurité, par exemple entre un routeur et des serveurs du réseau (`arp -s`) .

Les machines ayant fait la résolution vont transmettre les paquets avec l'adresse ETHERNET (MAC) de la machine à contacter. Dans le champ service de la trame ETHERNET, nous aurons la valeur **800** qui correspond aux trames de service IP.

5.2.2. L'ARP gratuit

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

6. LA COUCHE TRANSPORT (NIVEAU 4)

6.1. PROTOCOLES DE LIAISONS POINT À POINT (PPP)

6.1.1. Historique

Au milieu des années 80, le besoin se fait sentir pour l'INTERNET d'un protocole de liaison Point à Point pour la famille des protocoles TCP/IP. La plupart des sites utilisaient alors 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 ;
- fonctionner sur une liaison de type synchrone (chaîne de bits) ou asynchrone (orienté caractère avec stop bit et start bit) ;
- être 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.

6.1.2. PAP &CHAP

Ces noms "barbares" sont des méthodes d'identification négociées à l'intérieur du protocole PPP. On envoie comme renseignement un nom utilisateur et un mot de passe.

PAP laisse passer le mot de passe en clair.

CHAP crypte le mot de passe avant de le passer sur le réseau.

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

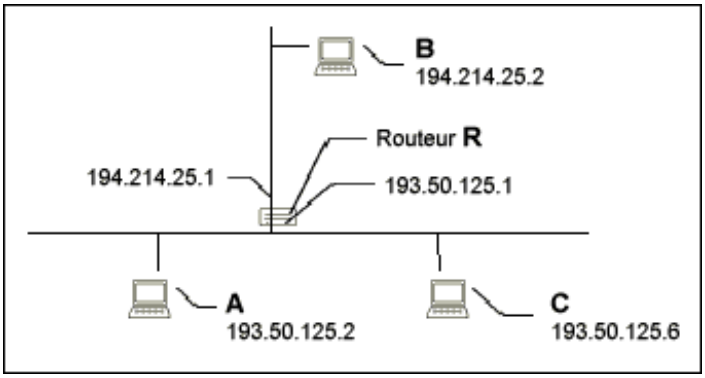
6.2. LE ROUTAGE DES DATAGRAMMES IP

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**. Un routeur est souvent une machine spécialisée et sans disque dur (fiabilité). Cependant une station Unix ou un Windows NT peuvent faire le travail.

6.2.1. 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.

6.2.2. Exemple de transfert



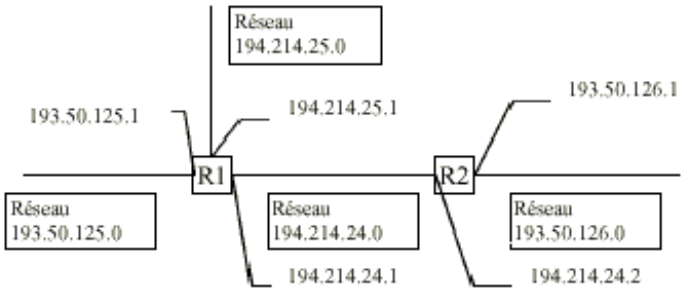
Pour atteindre C, A effectue une remise directe. Pour atteindre B, ce sera indirect en passant par le routeur. Le routeur a deux adresses car l'adressage IP ne concerne que les interfaces sur le réseau et non la machine elle même. A ce propos , si le routeur est connu par l'adresse 193.50.125.1 et que 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 de destination qui n'est pas celle du routeur. Celui ci s'en servira pour acheminer plus loin ce datagramme.

6.2.3. Routage IP via des tables statiques

Cette table va indiquer les routes à prendre en fonction du réseau, un peu comme une carte routière.

Exemple de routage IP via des tables statiques :



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

6.2.4. Default gateway ou passerelle

Pour conserver de petites tables (il y a des millions de réseaux), on a inventé le panneau "Autres Directions". Ce panneau s'appelle la **ROUTE PAR DEFAUT**.

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.

6.2.5. Mise à jour des tables

Ces tables sont définies statiquement par l'administrateur du réseau. 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..

6.3. 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.

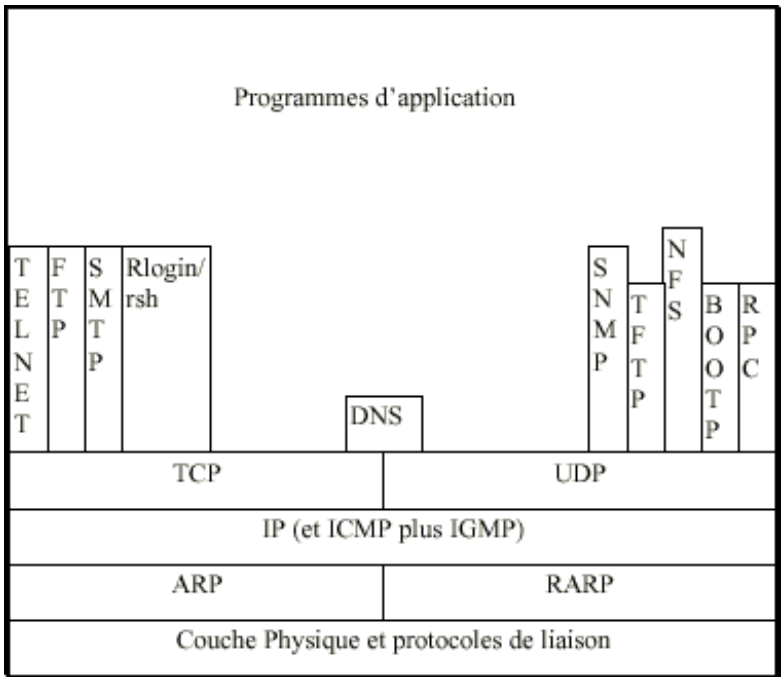
Pour cela, on utilise les messages ICMP, voici les différentes valeurs du champ type de ICMP :

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

A retenir :

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

6.4. UDP &TCP



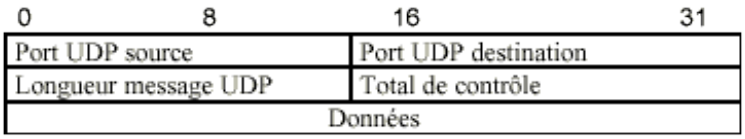
La couche IP dans la machine source ou destination agit comme une couche de multiplexage. C'est un peu comme une gare de triage.

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.

6.5. UDP

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.



Le port source est facultatif et vaut zéro généralement, sinon il contient le numéro du port ou renvoyer les réponses.

Longueur message UDP : longueur totale du datagramme, en−tête UDP compris(< 64 Ko).

Total de contrôle : Un code de détection d'erreur qui est facultatif (dépend de l'application).

6.6. TCP (TRANSPORT CONTROL PROTOCOL)

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

- TCP est un protocole connecté. C'est à dire qu'il existe une phase de création d'une connexion où les deux machines négocient leurs options et réservent des ressources. TCP informe les applications du succès ou de l'échec et ensuite contrôle le lien. Si celui−ci tombe, les applications en sont prévenues.
  Même si IP n'est pas un réseau connecté, TCP réalise cela au niveau des machines source et destination.

- Transferts bufférisé, 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 appelées **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

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 (6)	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

De la même façon que UDP, les couples (adresses, ports) identifient les connexions. Cette combinaison s'appelle socket du même nom que l'interface de programmation de Berkeley.

Le numéro de séquence représente le rang du premier octet de données dans le paquet depuis le début de la connexion. Ce numéro de séquence ne démarre pas à un mais à une valeur propre au système d'exploitation.

6.7. LA COMMANDE NETSTAT

C'est le principe des couples adresses port. En fait netstat n'affiche en standard que les connexions TCP

Il faut taper `netstat −a`

```
Active INTERNET connections (including servers)
Proto Recv−Q Send−Q Local Address Foreign Address State
```

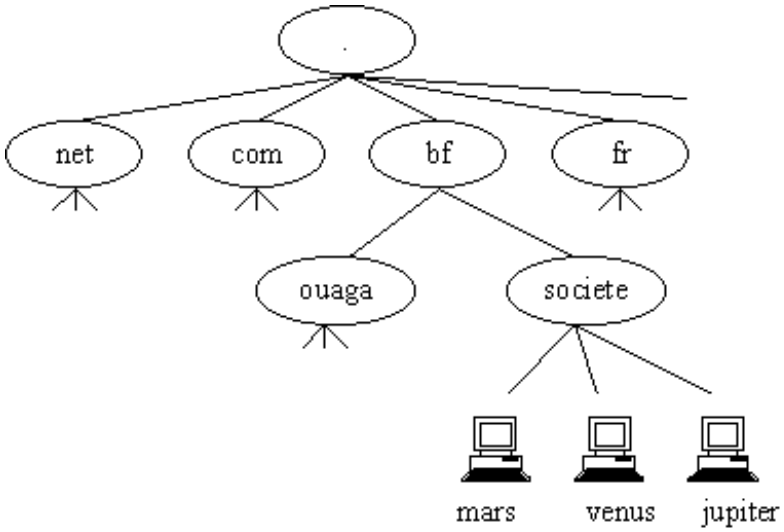
```
udp 65412 0 *:syslog *:*
udp 0 0 *:tftp *:*
udp 0 0 localhost:domain *:*
udp 0 0 romarin.univ−aix:domain *:*
udp 0 0 *:1026 *:*
udp 0 0 *:ntp *:*
udp 0 0 localhost:ntp *:*
udp 0 0 romarin.univ−aix.fr:ntp *:*
udp 0 0 *:49 *:*
```

7. LA COUCHE APPLICATION (NIVEAU 7)

7.1. LES SERVEURS DE NOM (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 est non pas une couche du réseau, mais une application. Les noms sont composés par une suite de caractères alphanumériques encadrés par des points. Par exemple 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.

com : Organisations commerciales (hp.com par exemple)
edu : Institutions éducatives (américaines)
gov : Organisations gouvernementales US
int : Organisations internationales
mil : Militaires Us
net : Réseau
org : Organisation à but non lucratif

bf : Burkina Faso
de : Allemagne
uk : Angleterre
fr : France

7.2. 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 exemple).

- Sur vos postes clients, vous vous trompez et mettez dans les DNS à contacter un routeur. En fait, si celui−ci est le premier contacté, vous allez perdre un temps important 30 sec à une minute avant d'appeler le

deuxième. Il faut mettre l'adresse de 2 "vrais" DNS dans les configurations.

- Par rapport à votre domaine père vous déclarez trop de serveurs de noms qui gèrent votre zone. Ces serveurs ne sont pas chez vous mais chez des collègues. Etes vous bien sur qu'il sont actifs et bien configurés ? Sinon ce sera les clients qui viendront chez vous qui devront attendre de tomber sur le bon serveur ! Ne mettez donc pas trop de serveurs de noms "officiels" sur votre zone (3 maximums).

7.3. LE FTP (FILE TRANSFERT PROTOCOL)

File Transfer Protocol RFC959 :

Le protocole de transfert de fichier utilise deux connexions TCP : l'une pour les ordres (le port 21) et 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.

Exemple :

```
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)
```

7.4. LE 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, est dû au CERN, Centre Européen de la Recherche Nucléaire.

Le principe est de transmettre par le réseau des documents hypertextes, contenant des images, des liens, etc.., un peu comme le help de windows ou hypercard de Apple.

Une normalisation d'adressage des différents services de TCP/IP a été crée de manière à banaliser l'accès aux services au travers d'un browser ou butineur (terme proposé en français).

Parmi ceux−ci on peut citer Netscape, INTERNET Explorer, Mosaic (l'ancêtre).

7.4.1. Format du lien HTML

Syntaxe :

Service : // adresse INTERNET FQDN / nom du fichier ou de l'objet

Exemples :

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

HTTP est Hyper Text Transport Protocol , HTML le langage des pages Hyper Text Markup Language. Pour http, le langage des documents s'appelle le HTML, il existe un certain nombre d'outils pour créer ces pages (Hot Dog pro, NetScape, Adobe PageMil, Dreamweaver, Microsoft FrontPage, etc..).

Ce sont des fichiers texte lisibles, et un bon spécialiste peut écrire directement en HTML. Bref ce qui vend le mieux le réseau est peut être une des applications les plus triviales.

Chaque page est transmise par une session TCP port 80 qui est fermée à la fin de la réception. Le clic sur une information hypertexte est purement local et va directement au serveur concerné, on ne repasse pas par le même serveur.

7.4.2. Proxy

L'information trouvée est mise en cache localement. De plus en plus, on utilise des serveurs intermédiaires pour faire des caches au niveau d'un très grand nombre d'utilisateurs. En cliquant sur une information située aux Japon, on a de bonne chance de l'avoir dans un cache régional ou national. Ces caches sont activés de manière transparente (fonction **HTTP PROXY**). L'adresse URL est passée en texte au serveur PROXY qui résoudra la requête. On atteint parfois 25% de succès. Une fois sur 4 la page est déjà dans le cache.

7.4.3. Les suites de HTTP/HTML

Le business étant rentré dans les protocoles INTERNET, les choses avancent très vite mais de façon plus désordonné. Auparavant, beaucoup de développements étaient dus à des organismes de recherche sans soucis de rentabilité ou de compétition.

Le WEB permet aussi de passer des données à un serveur qui va construire une page HTML constituant la réponse (cgi−bin par exemple). Ceci est un peu limité car on ne peut pas faire exécuter un programme au client. Plusieurs développements ont eu lieu ces derniers temps.
SUN, société qui vend et fabrique des stations de travail sous Unix a crée un nouveau langage et concept de réseau : le JAVA. Ce langage est de type C++ et le programme est envoyé au client qui l'exécute ensuite. Il existe des compilateurs qui vont créer un pseudo code **JAVA** qui sera interprété dans la machine distante.

MICROSOFT met en avant **ActiveX** qui est du même style mais très dépendant de Windows et de la plate forme Intel. D'ou problème pour faire tourner l'application sur un Mac ou une station Unix. NETSCAPE fournit aussi

JavaScript qui n'a rien avoir avec Java et permet de développer dans un langage interprété assez simple.

La plupart des browsers sont plus ou moins compatibles avec ces langages.
De toute façon le choix sera fait par les développeurs, mais MICROSOFT risque d'avoir une longueur d'avance car INTERNET Explorer est inclus dans les dernières versions de Windows.