LES RESEAUX INFORMATIQUES

SOMMAIRE

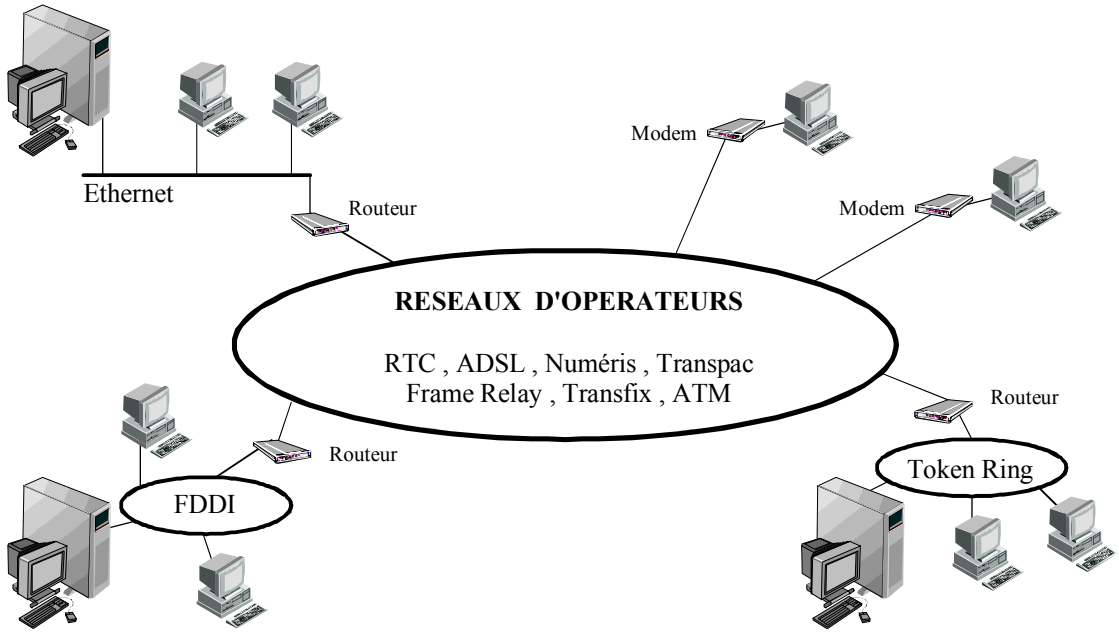
PARTIE A : CONCEPTS DE BASE DES RESEAUX

A.1) PRESENTATION

Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages, partage de ressources, transfert de fichiers, consultation de bases de données, gestion de transaction, télécopie ...

Un réseau de transmission de données peut être défini comme l'ensemble des ressources liées à la transmission et permettant l'échange des données entre les différents systèmes éloignés.

On distingue deux familles de réseaux :
- les réseaux informatiques dont font partie les réseaux locaux. Les lignes de transmission et les équipements de raccordement sont le plus souvent la propriété de l'utilisateur.
- les réseaux de télécommunication pour des liaisons longues distances. Ils sont la propriété d'opérateurs (France Télécom, ATT ...) qui louent leur utilisation et des services aux clients.



A.2) LES DIFFERENTS TYPES DE RESEAUX INFORMATIQUES

- Les réseaux locaux ou *LAN (Local Area Network)* qui correspondent par leur taille aux réseaux intra-entreprises.
- Les réseaux métropolitains ou *MAN (Metropolitan Area Network)* qui permettent l'interconnexion de plusieurs sites (ou de LAN) à l'échelle d'une ville.
- Les réseaux longues distances ou *WAN (Wide Area Network)*, généralement réseaux d'opérateurs, et qui assurent la transmission des données sur des distances à l'échelle d'un pays.
- Les réseaux locaux industriels avec principalement les réseaux *CAN (Controller Area Network)* et *VAN (Vehicule Area Network)* développés pour les véhicules automobiles.

PARTIE B : LES RESEAUX LOCAUX

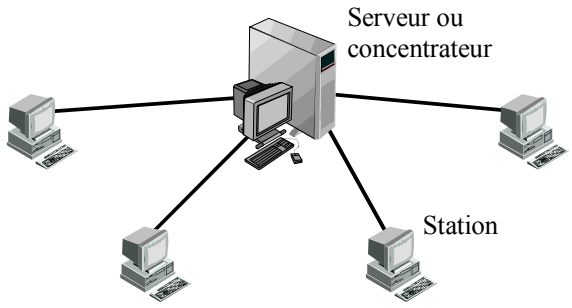
Un réseau local peut être défini comme l'ensemble des ressources téléinformatiques permettant l'échange à haut débit de données entre équipements au sein d'une entreprise, d'une société ou de tout autre établissement.
Le type et le volume des informations à transmettre, ainsi que le nombre d'utilisateurs simultanés, constituent la charge du réseau et vont déterminer le débit minimum nécessaire, et donc les types de supports possibles.

B.1) TOPOLOGIE

La topologie représente la manière dont les équipements sont reliés entre eux par le support physique.

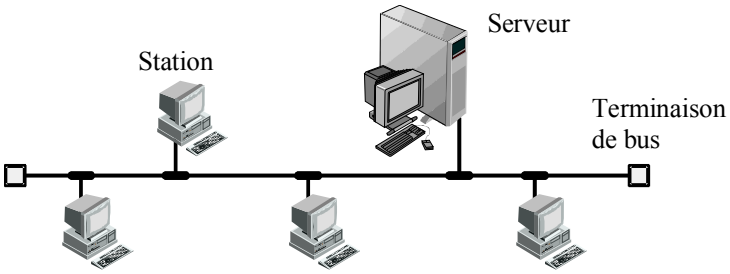
B.1.1) Etoile

Cette topologie permet d'ajouter aisément des équipements. La gestion du réseau se trouve facilitée par le fait que les équipements sont directement interrogeables par le serveur. En revanche, elle peut entraîner des longueurs importantes de câbles.



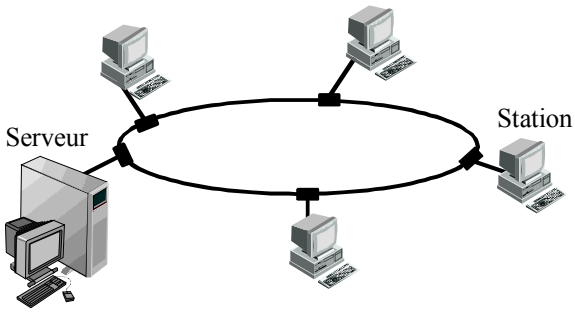
B.1.2) Bus

Cette topologie est économique en câblage et permet facilement l'extension du réseau par ajout d'équipement. En cas de rupture du câble commun, tous les équipements en aval par rapport au serveur sont bloqués.



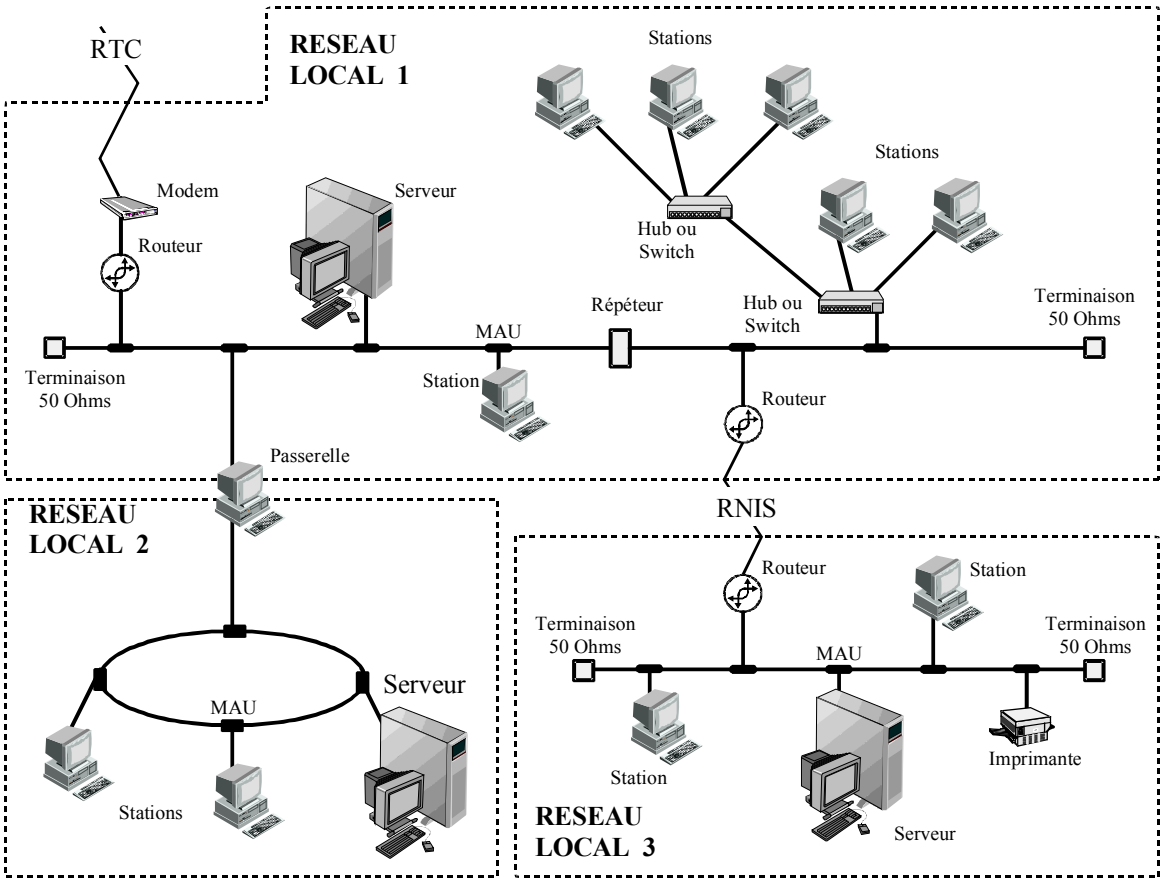
B.1.3) Anneau

Dans cette topologie, les informations transitent d'équipement en équipement jusqu'à destination. Un double anneau permet d'éviter une panne en cas de rupture de l'un des câbles.



La topologie en bus est celle adoptée par les réseaux Ethernet, Appletalk et la plupart des réseaux locaux industriels. Le réseau ATM utilise une topologie double bus à transmission unidirectionnelle. Les réseaux Token Ring et les réseaux en fibres optiques FDDI *(Fiber Distributed Data Interface)* utilisent respectivement les topologies en anneau et double anneau.

B.2) ELEMENTS D'UN RESEAU LOCAL



B.2.1) Equipements terminaux

La fonction principale d'un équipement terminal est de permettre à l'utilisateur d'accéder aux ressources du réseau. La famille de terminaux comprend les terminaux, les imprimantes, les ordinateurs (souvent appelées stations) et les serveurs.

B.2.2) Contrôleurs de communication

Les contrôleurs de communication gèrent l'accès d'un équipement terminal à la ligne de transmission. La famille comprend les cartes d'interface série (asynchrones ou synchrones), les cartes d'interface réseau et les contrôleurs pour le raccordement aux réseau public (ex: modem).

Les cartes d'interface réseau ou NIC (Network Interface Card) sont spécifiques au réseau utilisé et au type d'ordinateur. Elles possède une adresse unique appelée adresse MAC codée sur 6 octets.

B.2.3) Equipements d'interconnexion

Le répéteur reçoit et restitue l'information sans modification. Il peut adapter des types de supports différents tes que coaxial / paire torsadée ou coaxial / fibre optique.

Le MAU (Medium Access Unit) est une unité ou interface de raccordement au support.

Le hub a pour rôle d'assurer la communication entre les stations comme si elles étaient reliées à un bus bien que physiquement la topologie soit de type étoile.

Le pont reproduit, adapte et filtre la trame en fonction de l'adresse du destinataire.

Le switch possède les mêmes fonctionnalités que le hub et permet en plus de regrouper dans un même segment les stations liées par des trafics importants.

Le routeur assure la correspondance d'adresses. Il permet la connexion de 2 réseaux locaux par deux contrôleurs.

La passerelle assure la translation complète des protocoles.

B.3) L'ARCHITECTURE ETHERNET

Mise au point dans les année 80 par Xerox, Intel et Dec, l'architecture Ethernet permet l'interconnexion de matériel divers avec de grandes facilités d'extension.

B.3.1) Caractéristiques principales

- topologie en bus;
- support de type câble coaxial, paires torsadées ou fibre optique;
- débit de 10 Mbit/s à 1 Gbit/s;
- transmission en bande de base, codage Manchester;
- méthode d'accès suivant la norme IEEE 802.3

B.3.2) Supports de transmission

Le choix du support est fonction de critères interdépendants parmi lesquels :
la distance maximum entre stations, les débits minimum et maximum, le type de transmission (numérique ou analogique), la nature des informations échangées (donnée, voix, vidéo ...), la connectique, la fiabilité, le coût ...

Types	***Caractéristiques***
Paire torsadée	Débits pouvant atteindre 100 Mbit/s. Affaiblissement important. Sensible aux parasites d'origine électromagnétique.
Câble coaxial	Bande passante pouvant atteindre 300 à 400 MHz. Peu sensible aux inductions.
Fibre optique	Bande passante supérieure au GHz. Affaiblissement très faible. Insensible aux parasites d'origine électromagnétique.

Exemple du Fast Ethernet

Norme IEEE	Débit	Support	Longueur d'un segment
802.3u 100Base TX	100 Mbit/s	2 paires torsadées classe D , catégorie 5	100 m
802.3u 100Base T4	100 Mbit/s	4 paires torsadées classe D , catégorie 3,4 ou 5	100 m
802.3u 100Base FX	100 Mbit/s	2 fibres optiques	2 km
802.12 100Base VG	100 Mbit/s	paires torsadées fibre optique	200 m 2 km

B.3.3) L'accès aléatoire : CSMA/CD (Carrier Sens Multiple Access / Collision Detection)

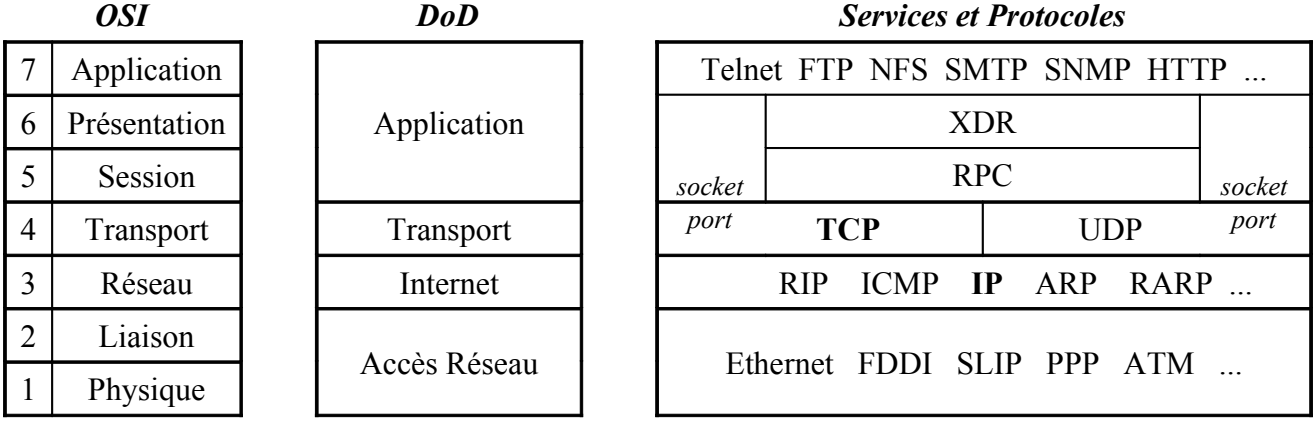
Une station avant de parler, écoute le canal. S'il est libre, elle émet sa trame mais en continuant d'écouter le canal. Si 2 stations éloignées écoutent le silence en même temps et émettent simultanément leurs trames, une 3ème station détecte la collision et envoie un signal de purge du réseau. Les 2 stations se taisent un moment, puis après un temps déterminé mais différent pour les deux stations, elles renouvellent leur tentative d'émission de leurs trames avec une probabilité de collision moindre. Sur la base de ce principe, la probabilité d'avoir l'accès au réseau par une station est fonction décroissante de la charge du réseau.

PARTIE C : TCP/IP
(*Transmission Control Protocol / Internet Protocol*)

C.1) PRESENTATION

Défini par l'ARPA *(Advanced Reserch Project Agency)*, sous l'égide du DoD *(Department of Defense)* aux Etats-Unis, les protocoles TCP/IP visent l'interconnexion des systèmes (machines) et réseaux hétérogènes. Présents dans toutes les implantations du système d'exploitation UNIX et largement utilisés dans le cadre d'Internet, ils se sont imposés comme standards d'interconnexion.

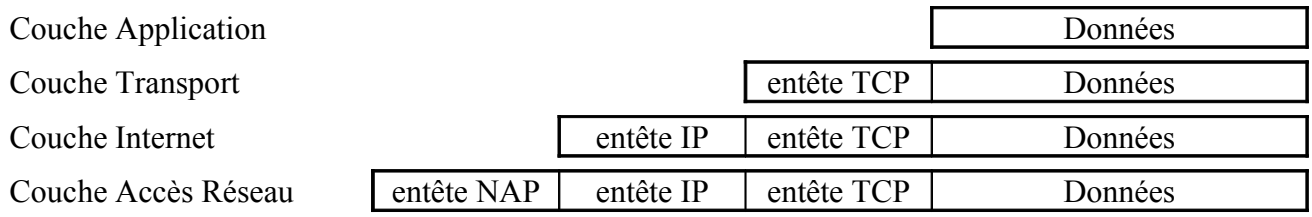
C.1.1) Comparaison du modèle DoD (ou TCP/IP) au modèle OSI



Les protocoles TCP et IP servent de base à une famille de protocoles de niveaux supérieurs définis dans des RFC (*Requests For Comments*, demande de commentaires).

C.1.2) Encapsulation des données

Tout comme dans le modèle OSI, les données sont transférées verticalement d'une couche à une autre en y rajoutant une entête *(header)*. Cette entête permet de rajouter des informations identifiant le type de données, le service demandé, le destinataire, l'adresse source etc...



Le ***datagramme*** est l'unité de base du transfert de données avec le protocole IP.

Le routage

Le routage d'un paquet consiste à trouver le chemin de la station destinatrice à partir de son adresse. Si le paquet émis par une machine ne trouve pas sa destination dans le réseau local, il doit être dirigé vers un routeur qui rapproche le paquet de son objectif.

C.1.3) Adaptation inter-réseau

Les réseaux physiques empruntés ne véhiculent pas forcément des messages de tailles identiques. Des opérations de fragmentation et groupage en émission ainsi que leur inverse en réception peuvent être réalisées soit au niveau de TCP, d'IP ou de la couche accès réseau.

C.2) LA COUCHE ACCES RESEAU

Sur cette couche se trouve le protocole lié à l'architecture physique du réseau. Il a pour fonction l'encapsulation des datagrammes provenant de la couche IP et la traduction des adresses en adresses physiques (adresse MAC) utilisées sur le réseau.

C.3) LE PROTOCOLE IP

C.3.1) Fonctionnalités

Ses principales fonctions sont :

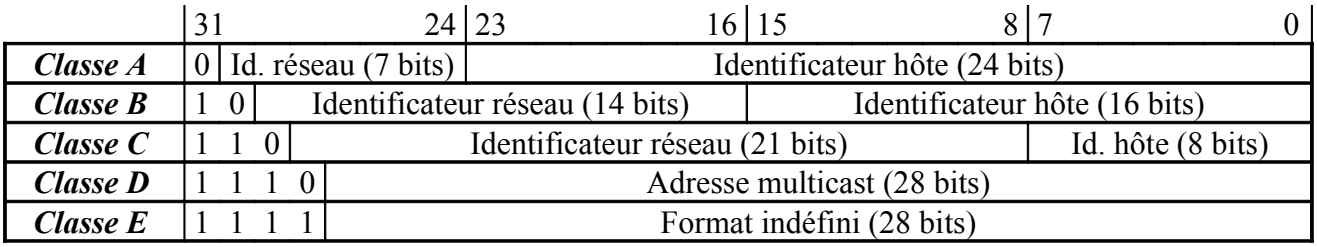
- Définir le format des données (datagramme).
- Assurer l'adressage et le routage des datagrammes jusqu'à leur adresse de destination (routage).
- Fragmenter et réassembler les datagrammes si nécessaire.

IP est un protocole qui n'est pas connecté, donc il n'y a pas d'établissement de connexion et de vérification de la validité des datagrammes.

C.3.2) Adressage IP

Sur un réseau TCP/IP, chaque machine se voit attribuer une adresse IP en principe unique. Les adresses sont codées sur 32 bits soit 4 octets représentés en décimal et séparés par des points. Ces adresses comportent 2 parties : l'adresse du réseau *(net)* et l'adresse de l'hôte *(host)* désignant une machine donnée. Suivant l'importance du réseau, plusieurs classes sont possibles :

- la classe A : pour les réseaux de grande envergure (ministère de la défense, IBM, AT&T ...)
- la classe B : pour les réseaux moyens (universités, centres de recherches ...)
- la classe C : pour les petits réseaux comprenant moins de 254 machines (PME/PMI)
- la classe D : les adresses ne désignent pas une machine particulière sur le réseau, mais un ensemble de machines voulant partager la même adresse *(multicast)*.
- la classe E : classe expérimentale, exploitée de façon exceptionnelle.



	Classe A	*Classe B*	*Classe C*
Premier réseau	1.x.x.x	128.1.x.x	192.0.1.x
Dernier réseau	126.x.x.x	191.254.x.x	223.255.254.x
Nombre de réseaux	126	16 382	2 097 150
Réseaux réservés à un usage privé	10.x.x.x	172.16.x.x à 172.31.x.x	192.168.0.x à 192.168.255.x
Adresse du réseau	x.0.0.0	x.x.0.0	x.x.x.0
Adresse de diffusion du réseau	x.255.255.255	x.x.255.255	x.x.x.255
Première machine	x.0.0.1	x.x.0.1	x.x.x.1
Dernière machine	x.255.255.254	x.x.255.254	x.x.x.254
Nombre de machines	16 777 214	65534	254
Masque de sous-réseau par défaut	255.0.0.0	255.255.0.0	255.255.255.0

Adresses particulières ou réservées

- L'adresse dont la partie basse (adresse machine) est constituée de bits à 0 est l'adresse du réseau.
- L'adresse dont la partie basse (adresse machine) est constituée de bits à 1 est l'adresse de diffusion *(broadcast)* et permet d'envoyer un message à l'ensemble des machines sur le réseau.
- L'adresse 127.0.0.1 est une adresse de bouclage *(localhost, loopback)* et permet l'utilisation interne de TCP/IP sans aucune interface matérielle.
- L'adresse 0.0.0.0 est une adresse non encore connue, utilisée par les machines ne connaissant pas leur adresse IP au démarrage.

Masque de sous réseau

Parfois, il convient de subdiviser un réseau en sous-réseaux afin de mieux s'adapter à l'organisation du travail et du personnel. Cette subdivision est faite localement en appliquant un masque *(subnet mas*k) sur la partie hôte de l'adresse IP. Exemple de masquage :

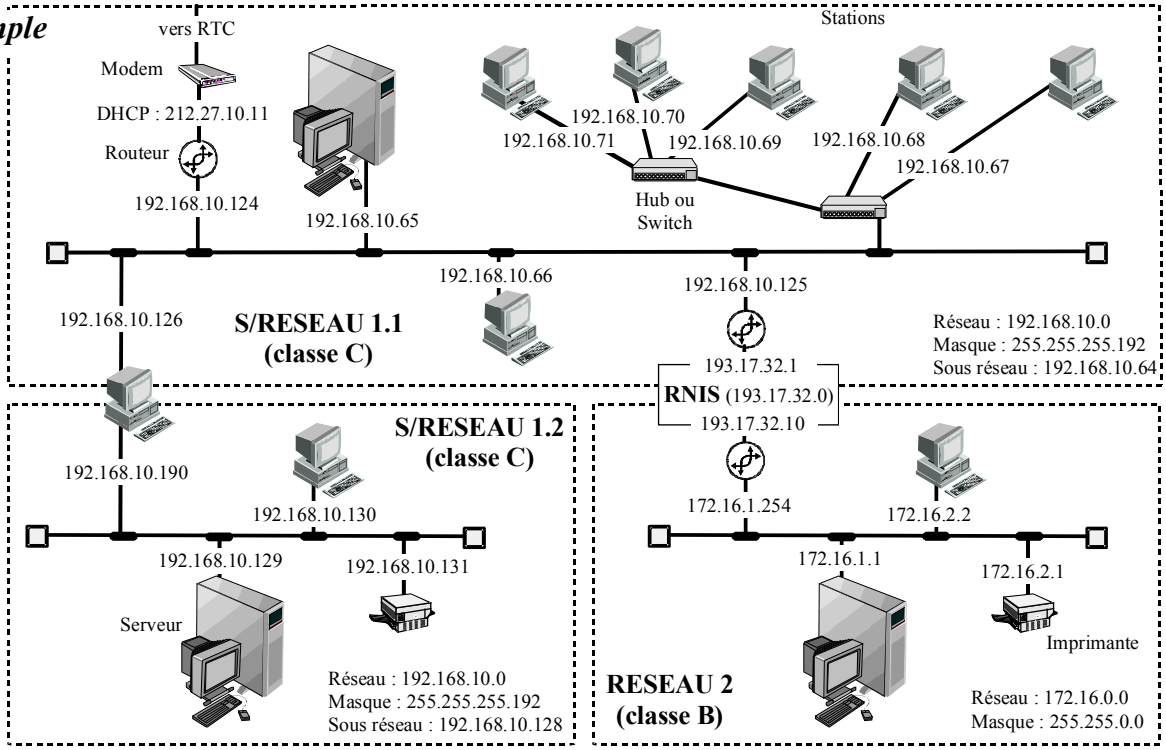
Réseau de classe B
Masque 255.255.255.0

Réseau			Hôte		
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1		1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	
Id. Réseau			Id. Sous-réseau	Id. Hôte	

Protocole DHCP

Le DHCP *(Dynamic Host Configuration Protocol)* est un protocole de configuration dynamique de l'hôte qui permet d'allouer à la demande des adresses IP aux machines se connectant au réseau. Il présente les avantages d'une gestion centralisée des adresses IP et permet d'obtenir un nombre d'adresses IP disponibles différent du nombre de machines du réseau.

Exemple



C.3.3) Evolution

La croissance fulgurante des connexions Internet et la quasi-saturation du plan d'adressage de IP version 4 (IPv4) actuelle qui s'en suit, rend nécessaire à très court terme le passage à IP version 6 (IPv6). Parallèlement à un champ d'adresse qui passe de 32 à 128 bits (soit 8 mots de 16 bits), d'autres fonctions améliorent le confort d'utilisation.

C.4) LE PROTOCOLE TCP

C.4.1) Fonctionnalités

Comme TCP fonctionne en mode connecté, il établit une connexion logique, bout à bout, entre les deux intervenants. Au départ, avant tout transfert de données, TCP demande l'ouverture d'une connexion à la machine cible qui renvoie un acquittement signifiant son accord. De même, lorsque l'ensemble des données ont été échangées, TCP demande la fermeture de la connexion et un acquittement de fermeture est alors envoyé sur le réseau. Lors du transfert, à chaque datagramme, un acquittement de bonne réception est émis par le destinataire. En effet, après vérification du Checksum, s'il s'avère que la donnée est endommagée, le récepteur n'envoie pas d'acquittement de bonne réception. Ainsi, après un certain temps, l'émetteur ré-émet le datagramme sur le réseau.
Le protocole assure aussi la segmentation et le ré-assemblage des données, le multiplexage des données issues de plusieurs processus hôtes, le contrôle de flux, la gestion des priorités des données et la sécurité de la communication.

C.4.2) Port

Le protocole TCP identifie les processus utilisant des ressources réseaux grâce à leur numéro de port qui est unique. Les valeurs supérieures à 1000 correspondent à des ports clients et sont affectées à la demande par la machine qui effectue une connexion TCP.

Numéros de port usuels

Process	Echo	FTP	SSH	Telnet	SMTP	Time	HTTP	POP3	SNMP
n° de port	7	21	22	23	25	37	80	110	161

C.5) LE PROTOCOLE UDP

Le protocole UDP fonctionne en mode non connecté et donc ne possède pas de moyen de détecter si un datagramme est bien parvenu à son destinataire. Le choix d'utiliser UDP comme protocole de la couche transport peut-être justifié par plusieurs raisons :
- le fait d'utiliser une entête de taille très réduite procure un gain de place assez considérable,
- on évite l'ensemble des opérations de connexion, détection d'erreur et déconnexion, et dans ce cas le gain de temps peut être très appréciable, surtout pour de petits transferts.

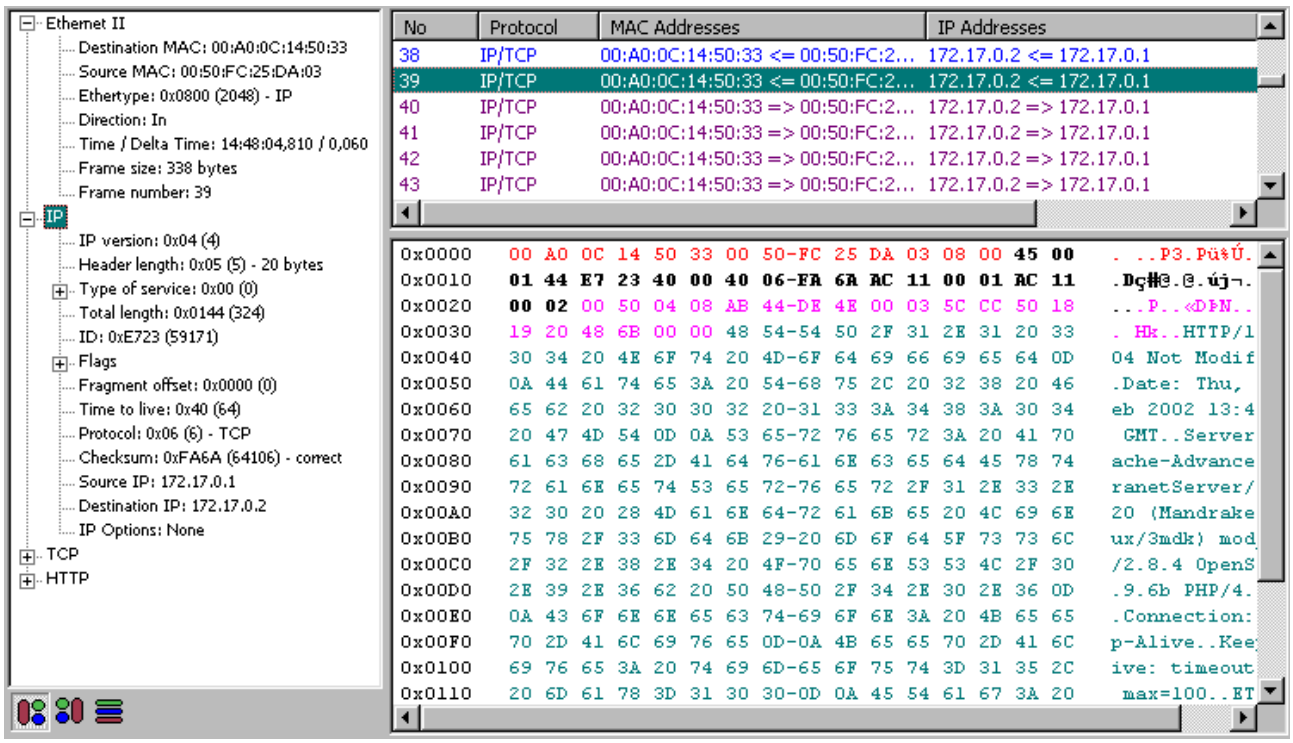
C.6) LA COUCHE APPLICATION

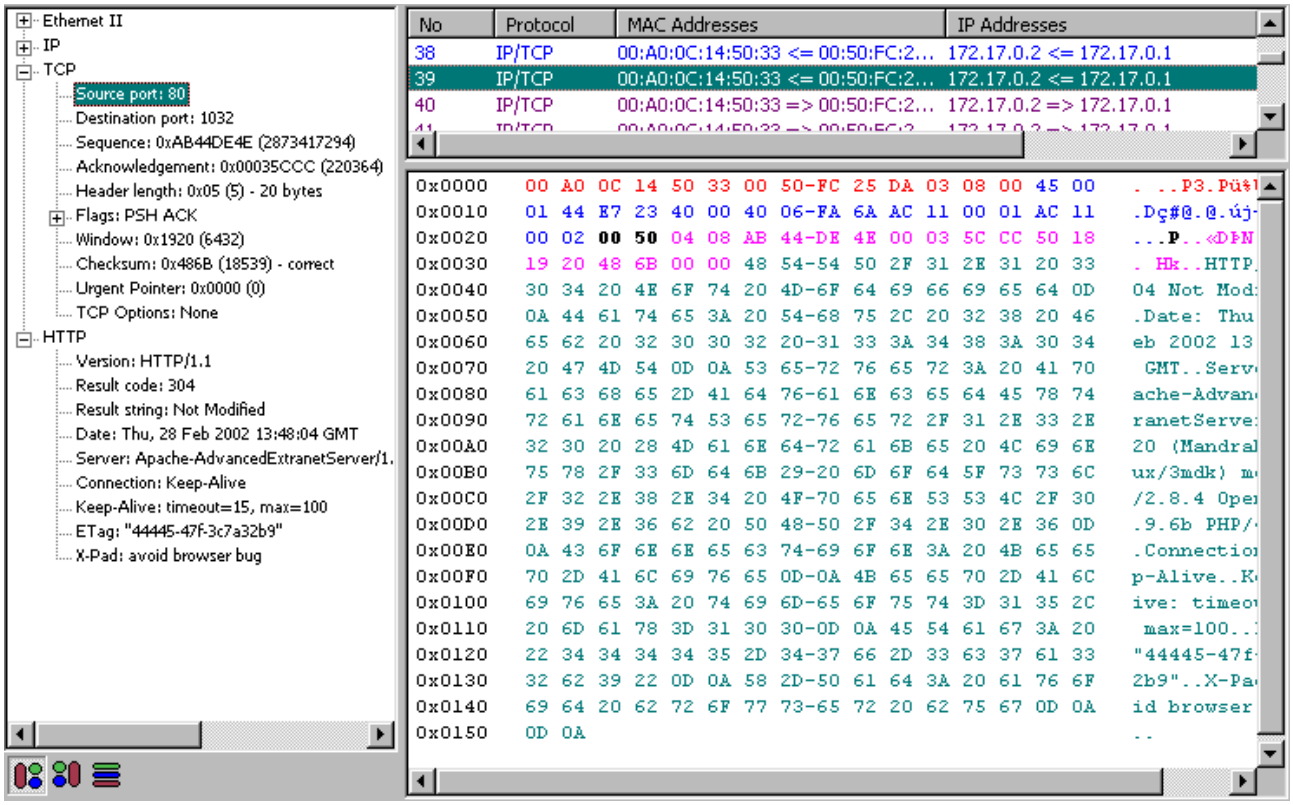
Cette couche rassemble l'ensemble des applications qui utilisent TCP/IP pour échanger des données. On dénombre de plus en plus de services différents, les derniers comme WWW étant de plus en plus performants et souples d'utilisation.

C.6.1) Socket

Des bibliothèques de fonctions d'interface avec TCP et UDP *(library socket)* inclues en standard dans les systèmes UNIX et Windows permettent aux développeurs d'écrire simplement des applications réseaux.
Le terme socket est aussi défini par la combinaison de l'adresse IP et du numéro de port.

C.7) EXEMPLE DE TRAME





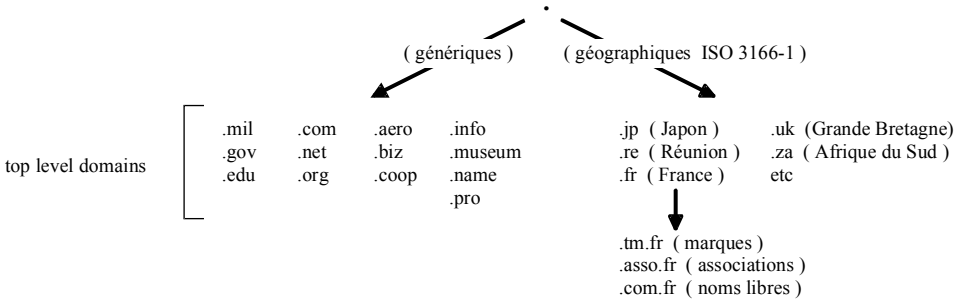
PARTIE D : INTERNET

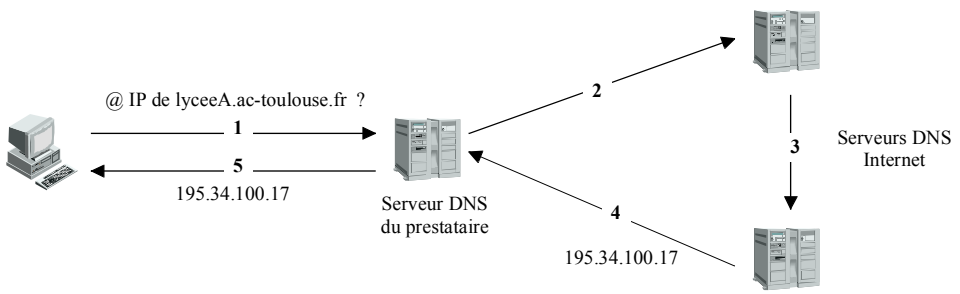
D.1) HISTORIQUE

C'est en 1969 que l'agence américaine *DARPA (Defense's Advenced Research Projects Agency)* sous l'égide du DoD *(Department of Defense)* a commencé à développer un grand réseau informatique expérimental baptisé ARPAnet, connectant les principaux organismes de recherche des Etats-Unis. Devenu opérationnel en 1975 après avoir prouvé son utilité ARPAnet adopte en 1983 comme standard la nouvelle suite de protocoles TCP/IP. L'UNIX BSD, de l'Université de Californie à Berkeley, intégrant TCP/IP permit de communiquer à travers ARPAnet à un faible coût. L'ARPAnet initial devint alors l'épine dorsale d'une fédération de réseaux locaux et régionaux appelée ***Internet***. En 1988 le DARPA décide d'arrêter l'expérience. Un nouveau réseau est alors fondé par la NSF *(National Science Foundation)* appelé NSFNET qui remplace ARPAnet dans le rôle d'épine dorsale de l'Internet. En 1995 l'épine dorsale gérée par l'organisme public NSFNET est remplacée par un ensemble d'épines dorsales commerciales exploitées par des opérateurs de télécommunication.

D.2) DOMAINES

L'utilisateur final préfère adresser les machines destinataires par un nom, plutôt que par leur adresse IP. Le service DNS *(Domain Name Service)* s'occupe de dresser la table de correspondance entre les noms et les adresses IP. Le nombre de noms connus dans l'Internet interdit une gestion par une machine unique. Le monde a donc été découpé en TLDs *(Top Level Domains)* gérés par IANA *(Internet Assigned Numbers Autority)*. AFNIC (Association Française pour le Nommage Internet en Coopération) est chargée de l'attribution des noms de domaine en france. Il y a généralement un "top level domains" par pays. Les Etats-Unis qui sont à l'origine de ce nommage en ont plusieurs. Chaque pays peut ensuite créer des sous-domaines de son "top level domains", puis les entreprises ou universités du pays vont créer des sous-domaines de chaque sous-domaine ...





D.3) OPERATEURS ET PRESTATAIRES DE SERVICES

D.3.1) Opérateurs

Ils disposent de leur réseau pour assurer le transport des informations d'un point à un autre. Ils fournissent les points de connexions sur leur réseau aux entreprises et aux prestataires qui ont obtenu des adresses IP d'un organisme agréé tel que l'InterNIC ou l'AFNIC.

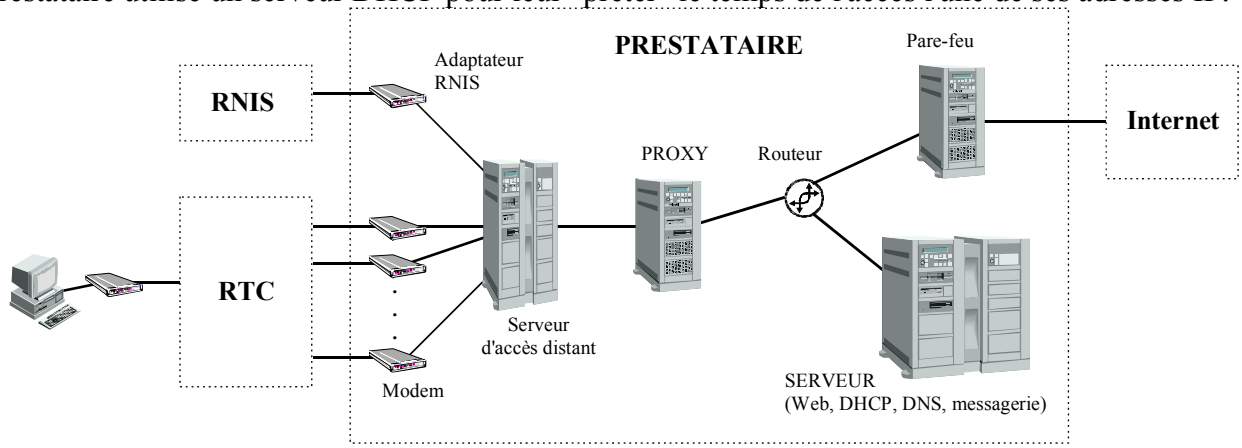
D.3.2) Prestataire de service

Le prestataire de service ou fournisseur d'accès aux services *(Internet Services Provider)* fournit :

- des service de connexion utilisant les réseaux d'opérateurs de télécommunication,
- les adresses IP aux particuliers ou aux entreprises qui ne peuvent obtenir une adresse (256 au minimum) auprès de l'InterNIC ou de l'AFNIC,
- des services tels que la messagerie, la connexion aux serveurs Web ou l'hébergement de pages Web.

Type de connexion

- Les entreprises souhaitant se connecter et être accessibles directement à tout moment par Internet choisissent la solution *full Internet*. Le prestataire attribue au client l'une de ses adresses IP.
- Les particuliers qui veulent se connecter temporairement à Internet choisissent la solution *dual-up*. Le prestataire utilise un serveur DHCP pour leur "prêter" le temps de l'accès l'une de ses adresses IP.



PROXY

L'expérience montre qu'un nombre important de clients Internet consultent les mêmes pages sur les mêmes sites (page d'accueils en particulier). Un serveur PROXY garde dans ses mémoires les dernières pages consultées puis les distribue à tous les clients qui demandent ces pages. Il en résulte un temps d'accès beaucoup plus rapide à ces pages et un moindre trafic à travers l'Internet mondial. Par contre, le PROXY allonge le temps d'accès pour les pages rarement consultées.

D.4) SERVICES ET PROTOCOLES ASSOCIES

D.4.1) Messagerie

Plus connu sous le nom de e-mail *(electronic mail ou courrier électronique)*, ce service permet d'échanger des messages et des fichiers. Le ou les messages sont stockés par le serveur de messagerie dans la boîte à lettre du client, en attendant que ce dernier vienne les consulter.

MIME (Multipurpose Internet Mail Extensions) est le protocole le plus utilisé pour la mise en forme des messages. ***SMTP (Simple Mail Transport Protocol***) est le protocole courant de gestion du courrier électronique sur Internet. Dans la mesure où SMTP a été conçu pour des système reliés en permanence, un utilisateur connecté de façon intermittente utilise SMTP pour expédier son courrier (courrier sortant)

et ***POP3 (Post Office Protocol version 3)*** pour lire les courriers qui l'attendent sur le serveur (courrier entrant). ***IMAP (Interactive Mail Access Protocol)***, plus récent que POP3, permet d'accéder aux message sans les télécharger et d'effectuer des recherches de courrier selon des critères.
IRC (Internet Relay Chat) est un protocole qui permet à des utilisateurs de communiquer en direct.

D.4.2) Transfert de fichier

Il permet à un client de récupérer des fichiers auprès d'un serveur de fichier. Le mode *anonymous* permet au serveur de servir des clients ne disposant pas de compte.
FTP (File Transfer Protocol) est le protocole utilisé entre le client et le serveur pour le transfert.

D.4.3) Web (WWW)

Le service World Wide Web (WWW) a vu le jour en 1989 au CERN (Centre Européen pour la Recherche Nucléaire). Il permet à un client d'accéder à des documents au format HTML *(HyperText Markup Language)*, image, son ou vidéo.
HTTP (HyperText Transfer Protocol) est le protocole de communication entre le navigateur du client et le serveur Web, basé sur le principe des liens hypertextes. Il suffit de cliquer sur un des liens d'un document pour accéder à un autre document localisé sur le même serveur ou n'importe où sur le réseau Internet.

D.5) URL *(Uniform Resource Locators)*

URL permet identifier l'accès aux documents disponibles sur Internet.

[service ou protocole] :// [adresse de la machine] / [ressource dans la machine]

exemples :	http://www.apache.org	ftp://192.100.200.8/doc
	http://serveur/machine1	file:///c:/Mes Documents/fichier.txt