Introduction générale

Environ d'une page

Chapitre 01

Généralités sur les réseaux informatique

I- Généralités sur les réseaux informatique_

1- Que signifie réseau

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations.
Le terme réseau en fonction de son contexte peut désigner plusieurs choses. Il peut désigner l'ensemble des machines, ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui 'est le cas lorsque l'on parle de Internet.
Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées. C'est le cas lorsque l'on dit que les machines d'un site (sur un réseau local) sont sur un réseau Ethernet, Token Ring, réseau en étoile, réseau en bus,...
Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent. On peut parler de réseau TCP/IP, NetBeui (protocole Microsoft) DecNet(protocole DEC),IPX/SPX,...
Lorsque l'on parle de réseau, il faut bien comprendre le sens du mot.

2- Pourquoi des réseaux

Les réseaux sont nés d'un besoin d'échanger des informations de manière simple et rapide entre des machines. Lorsque l'on travaillait sur une même machine, toutes les informations nécessaires au travail étaient centralisées sur la même machine. Presque tous les utilisateurs et les programmes avaient accès à ces informations. Pour des raisons de coûts ou de performances, on est venu à multiplier le nombre de machines. Les informations devaient alors être dupliquées sur les différentes machines du même site. Cette duplication était plus ou moins facile et ne permettait pas toujours d'avoir des informations cohérentes sur les machines. On est donc arrivé à relier d'abord ces machines entre elles; ce fût l'apparition des réseaux locaux. Ces réseaux étaient souvent des réseaux "maisons" ou propriétaires. Plus tard on a éprouvé le besoin d'échanger des informations entre des sites distants. Les réseaux moyenne et longue distance commencèrent à voir le jour. Ces réseaux étaient souvent propriétaires. Aujourd'hui, les réseaux se retrouvent à l'échelle planétaire. Le besoin d'échange de l'information est en pleine évolution. Pour se rendre compte de ce problème il suffit de regarder comment fonctionnent des grandes sociétés. Comment pourrait-on réserver une place de train dans n'importe quelle gare? Sans échange informatique, ceci serait très difficile.

3- Classification des réseaux (définition +schéma)

Un **réseau informatique** est un ensemble d'équipements reliés entre eux pour échanger des informations. Par analogie avec un filet (un réseau est un « petit rets », c'est-à-dire un petit filet), on appelle nœud *(node)* l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions (un ordinateur, un routeur, un concentrateur, un commutateur).

Il existe de trois type de réseaux : MAN .LAN . WAN

a- LAN :

(Local Area Network) réseau local . Un LAN est un réseau situé généralement dans la même entité géographique (entreprise, campus,...). Des LAN peuvent être interconnectés pour former des réseaux plus grands (WAN, MAN,...). On dit alors que le LAN est un sous-réseau du réseau auquel il est connecté.

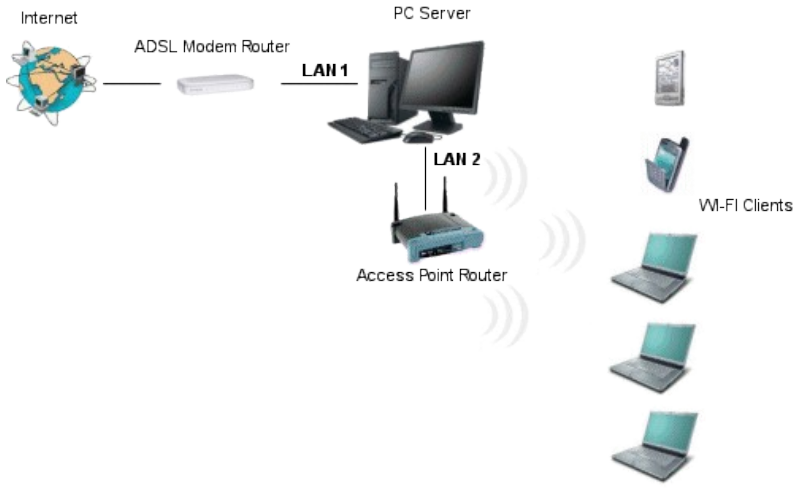


Figure 01

b- MAN

(Metropolitan Area Network) Ce type de réseaux est récent et garde les avantages des LAN sur de plus longues distances de l'ordre de la ville.

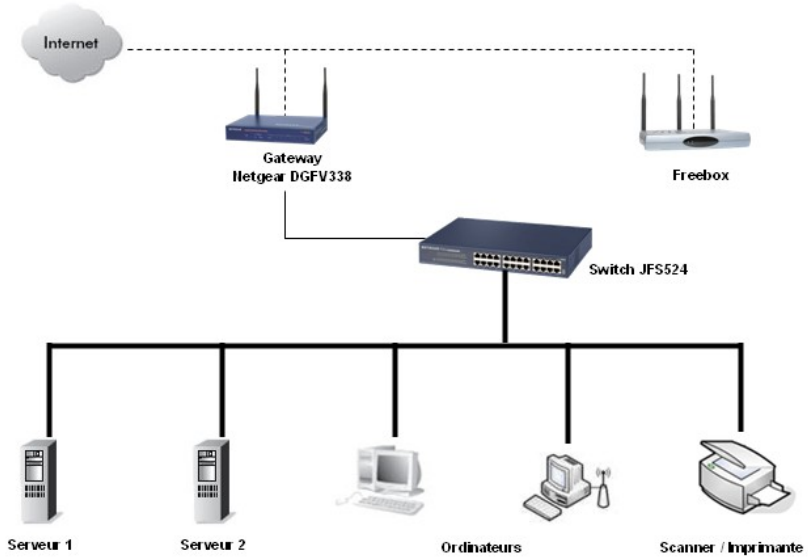


Figure 02

c- WAN :

Wide Area Network) réseau grande distance. Un WAN est un réseau qui se mesure sur une grande échelle géographique. Certaines sociétés, généralement internationales (IBM, UNISYS, AT&T, AIR France, ...) disposent souvent de tels réseaux à l'échelle planétaire. Internet est un réseau de type WAN

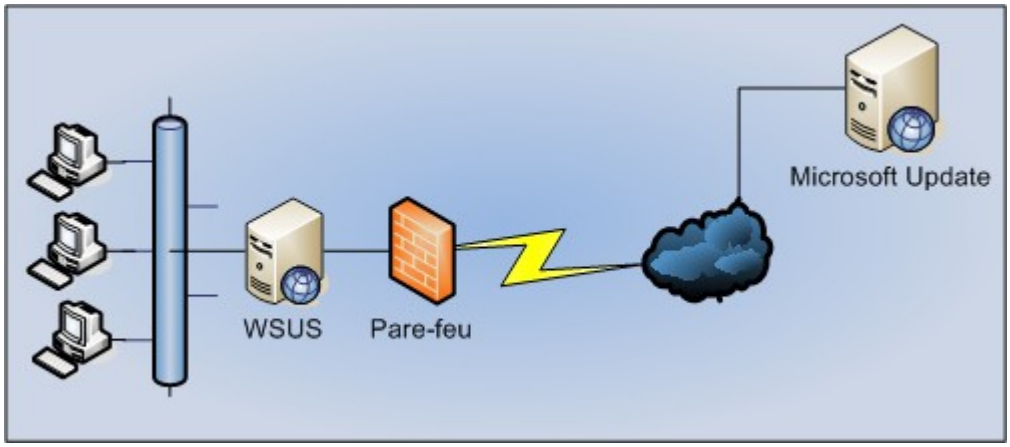


Figure 03

II- EQUIPEMENTS ET TOPOLOGIE DES RESEAUX LOCAUX

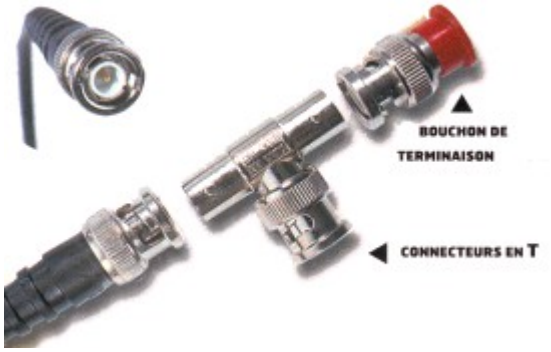
LES COMPOSANTES PHYSIQUES DU RESEAU LOCAL

1- Le Média

Il correspond au moyen de transporter l'information, en général il s'agit du câblage ou support
3 types de câblage sont utilisés en réseau local :

a- le câble coaxial

Il est composé de deux conducteurs cylindriques séparés par une matière isolante (comme dans du câble d'antenne)
Il est utilisable sur 185 m (câble 10 B 2) ou 500 m (câble 10 B 5) Le débit est toutefois limité à 10Mbps (cordon BNC)
Connecteurs BNC et bouchons d'impédance
Le câble coaxial s'utilise dans les réseaux en bus.



b- la paire torsadée :

Il correspond à une version améliorée du câble téléphonique, le coût est faible mais les performances s'amenuisent avec la distance. Il subit les interférences électriques (câble RJ45), il s'utilise avec un hub. Le débit peut atteindre 100 Mbps (câble 100 BT) ou 1000 Mbps (câble 1000 BT). La distance **est limitée** à 100 m (au delà le risque de perte de données est important).

Connecteur RJ45

Figure 05

Figure 04

c- La fibre optique :

Elle est constituée en fibre de verre, l'information circule sous forme lumineuse.

Avantages :

- très grande fiabilité,
- débit élevé,
- utilisation sur de grandes distances (jusqu'à 50 km)

Inconvénient : coût élevé.

Fibre optique

Figure 06

d- La carte réseau (carte LAN – Carte Ethernet)

Elle est installée sur **chaque ordinateur** (y compris sur le serveur) du réseau et sur les imprimantes réseau. Elle permet de faire communiquer les ordinateurs entre eux (en gérant la couche liaison de données du modèle OSI). Elle prend en charge la détection des collisions sur un réseau Ethernet : une collision se produit lorsque 2 ordinateurs envoient simultanément des informations. Les cartes réseaux ont une adresse physique unique attribuée par le constructeur. Cette adresse, appelée adresse MAC (Media Access Control) est essentielle car elle permet à une machine d'être reconnue par les autres machines du réseau.

La carte réseau se présente sous la forme d'une carte d'extension connectée à un bus (généralement PCI) et comportant un connecteur RJ45 ou BNC ou fibre. Certaines cartes réseaux (voir photo) sont polyvalentes (combo), elles comportent alors un connecteur BNC permettant de relier le poste à un réseau en bus et un connecteur RJ45 permettant de relier le poste à un réseau en étoile.

Carte réseaux

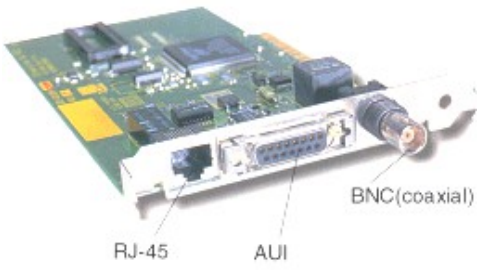
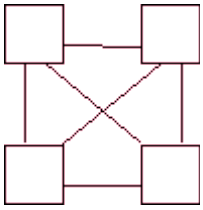


Figure 07

II/ La topologie des réseaux locaux

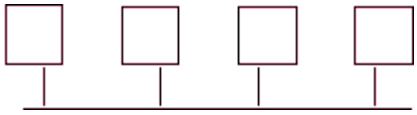
a- Câblage en maille

Chaque machine est reliée à toutes les autres par un câble.



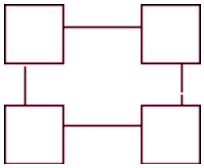
b- Câblage en bus

Chaque machine est reliée à un câble appelé bus.



c- Câblage en anneau

Chaque machine est reliée à une autre de façon à former un anneau



1- Principes de fonctionnement

a- Maille:

Ce type de câblage n'est plus utilisé car il nécessite beaucoup de câbles.
Avec n machines il faut : n (n -1) /2 cables.

b- Bus:

Sur un câble de type bus, on utilise souvent un système CSMA/CD (Carriere Sense Multiple Acces / Collision Detection) Accès multiple avec détection de porteuse et détection des collisions.

- **Exemple : câblage Ethernet.**

Lorsqu'une machine veut émettre un message sur le bus à destination d'une autre, la première commence par "écouter" le câble (CS). Si une porteuse est détectée, c'est que le bus est déjà utilisé. La machine attend donc la fin de la communication avant d'émettre ses données. Si le câble est libre, alors la machine émet ses données. Durant l'émission la machine reste à l'écoute du câble pour détecter une collision (CD). Si une collision est détectée, chaque machine qui émettait suspend immédiatement son émission et attend un délai aléatoire tiré entre 0 et une valeur N. Au bout du temps N le cycle recommence. Si une seconde détection est repérée le délai est tiré entre 0 et 2 * N. Ainsi de suite jusqu'à 16 * N. Après on recommence à N.
Chaque machine reçoit donc toutes les données qui circulent sur le bus. C'est au niveau de la couche 2 que l'on décide de garder les données ou de les jeter.

c- Anneau:

Les informations circulent toujours dans le même sens. Chaque machine qui reçoit un message, le recopie immédiatement sur le second câble. En même temps, l'information est remontée en couche 2 pour savoir si elle est doit être conservée par la machine ou détruite. L'information finira par revenir à la source. Cette dernière ne réemmettra pas l'information. Elle pourra comparer les

données envoyées et les données reçus pour une éventuelle détection d'erreurs.
Sur un câble de type anneau on utilise souvent un système de jeton. Le jeton est un message particulier que les machines se font passer les une aux autres. Une machine n'a alors le droit d'émettre que lorsqu'elle dispose du jeton. Si la machine qui dispose du jeton n'a rien à émettre, alors elle fait passer le jeton à la machine suivante. Il existe des algorithmes pour régénérer un jeton lorsque ce dernier est perdu suite à un incident.

d- Etoile:

Sur un réseau en étoile toutes les communications passent par la machine qui est au centre de l'étoile. C'est cette dernière qui redirige l'information vers le destinataire.

2- Avantages et inconvénients

Le câblage en maile n'est plus utilisé car trop coûteux en câble.
De part son architecture, le câblage en bus avec des protocoles CSMA/CD convient très mal dans un environnement temps réel. Sur un réseau en bus, deux machines peuvent monopoliser le câble.
L'architecture en anneau avec un protocole à base de jeton, peut servir dans un environnement temps réel car le délai maximum pour transmettre une information entre 2 machines peut être calculé. Le câblage en anneau nécessite plus de câble puisqu'il faut reboucler la dernière machine sur la première. Le câblage en anneau peut être perturbé par la panne d'une seule machine.
Dans une étoile, le point faible est le centre de l'étoile, si cet élément tombe en panne, alors tout le réseau est paralysé.

III/ Concentrateur (hub) ou commutateur (Switch)

Le **concentrateur** ou **hub** a pour principal inconvénient de diviser la bande passante entre tous les ports connectés, soit entre chaque poste. Ainsi, si un poste envoie un message sur le réseau, il sera renvoyé sur tous les ports du hub et diffusé à l'ensemble des postes qui le recevront, quitte à le rejeter s'ils n'en sont pas destinataires (ceci est totalement transparent pour l'utilisateur qui ne se rend compte de rien). Par exemple, si sur un réseau à 100 Mbps sont connectés 10 ordinateurs à un hub et un 2ème hub regroupant 15 autres postes (soit au total 25 postes) la bande passante théorique sera alors de 100/25 = 4Mbps pour chaque poste.

Le **commutateur** ou **switch** permet de « **segmenter** » le trafic sur le réseau en ne réduisant pas la **bande passante :** la bande passante reste la même sur chaque port. Ainsi un message envoyé par un poste sera transmis directement sur le port relié au poste destinataire (grâce à une gestion de la liste des adresses MAC des postes dans le switch) ; le message ne sera pas envoyé à l'ensemble des postes.
Seul problème : un switch coûte beaucoup plus che qu'un h

Chapitre 02

La normalisation des réseaux informatique

I- La normalisation des réseaux informatique

1- Pourquoi une normalisation

Si chacune des personnes (physiques ou morales) ne devait échanger des informations qu'avec des gens de sa communauté, alors il n'y aurait pas besoin de normalisation, chaque entité pourrait échanger ces informations avec des membres de la même entité. Il suffirait que chacune des personnes utilise le même "langage" (protocole) pour échanger ces informations.
Malheureusement (?), de plus en plus d'entité on besoin d'échanger des informations entre elles (SNCF, agence de voyage, organisme de recherche, école, militaires, ...). Si chacune de ces entités utilise son réseau (au sens protocole) pour que ces entités puissent communiquer ensemble il faudrait chaque fois réinventer des moyens pour échanger l'information. C'est ce qui se faisait au début. Des gens ont eu l'idée de réfléchir à ce problème et ont essaye de recenser les différents problèmes que l'on trouvait lorsque que l'on veut mettre des machines en réseau. De cette réflexion est sortie le modèle OSI de l'ISO.

2- Le modèle OSI de l'ISO

Pour faire circuler l'information sur un réseau on peut utiliser principalement deux stratégies.
L'information est envoyée de façon complète.
L'information est fragmentée en petits morceaux (paquets), chaque paquet est envoyé séparément sur le réseau, les paquets sont ensuite réassemblés sur la machine destinataire.
Dans la seconde stratégie on parle réseau à commutations de paquets.
La première stratégie n'est pas utilisée car les risques d'erreurs et les problèmes sous-jacents sont trop complexes à résoudre.
Le modèle OSI est un modèle à 7 couches qui décrit le fonctionnement d'un réseau à commutations de paquets. Chacune des couches de ce modèle représente une catégorie de problème que l'on rencontre dans un réseau. Découper les problèmes en couche présente des avantages. Lorsque l'on met en place un réseau, il suffit de trouver une solution pour chacune des couches.
L'utilisation de couches permet également de changer de solution technique pour une couche sans pour autant être obligé de tout repenser.
Chaque couche garantit à la couche qui lui est supérieur que le travail qui lui a été confié a été réalisé sans erreur.

Tab : 01

Couche	Fonctionnalité
7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Matériel

a- La couche 1 Matériel

Dans cette couche, on va s'occuper des problèmes strictement matériels. (Support physique pour le réseau). Pour le support, on doit également préciser toutes ces caractéristiques.

Pour du câble :

- Type (coaxial, paires torsadées,...)
- si un blindage est nécessaire
- le type du signal électrique envoyé (tension, intensité,...)
- nature des signaux (carrés, sinusoïdaux,...)
- limitations (longueur, nombre de stations,...)
- ...

Pour des communications hertziennes

- Fréquences
- Type de modulation (Phase, Amplitude,...)
- ...

Fibre optique

- Couleur du laser
- Section du câble
- Nombre de brins

- **La couche 2 Liaison**
  Dans cette couche on cherche à savoir comment deux stations sur le même support physique (cf. couche 1) vont être identifiées. Pour ce faire, on peut par exemple assigner à chaque station une adresse (cas des réseaux Ethernet,....).
- **La couche 3 Réseau**
  Le rôle de cette couche est de trouver un chemin pour acheminer un paquet entre 2 machines qui ne sont pas sur le même support physique.
- **La couche 4 Transport**
  La couche transport doit normalement permettre à la machine source de communiquer directement avec la machine destinatrice. On parle de communication de bout en bout (end to end).
- **La couche 5 Session**
  Cette couche a pour rôle de transmettre cette fois les informations de programmes à programmes.
- **La couche 6 Présentation**
  A ce niveau on doit se préoccuper de la manière dont les données sont échangées entre les applications.
- **La couche 7 Application**
  Dans la couche 7 on trouve normalement les applications qui communiquent ensemble. (Courrier électronique, transfert de fichiers,...)

b- Les protocoles applicatifs (couche application)

La couche application représente les déférents services fournis aux utilisateurs

Pour administration des réseaux, cette opération regroupe un ensemble de tâches garantissant le bon fonctionnement du réseau, c'est à dire permettre aux utilisateurs d'accéder aux ressources disponibles en toute transparence et selon des niveaux de sécurité bien définis.

Ces tâches comprennent :

- la gestion des utilisateurs et des ordinateurs du réseau,
- l'affectation des dossiers aux utilisateurs
- la gestion des sauvegardes
- la mise à jour des logiciels (applications bureautiques, professionnelles, antivirus,…)

Les outils d'administration sont regroupés dans le panneau de configuration de Windows 2003 Server sous l'icône :  Outils d'administration.

Les outils les plus importants sont les suivants :

Services	Donne accès à l'ensemble des services qui sont exécutés sur le serveur. Lorsqu'un service est défaillant, l'outil services permet de redémarrer le service
DHCP	DHCP (Dynamic Host Control Protocol) permet d'attribuer automatiquement une adresse IP à chaque poste du réseau
DNS	DNS (Domain Name Server) permet de convertir, une adresse d'ordinateur du type www.monserveur.fr en adresse IP.
Gestionnaire de licences	Permet un suivi du nombre de licences en cours d'utilisation sur le réseau. Lorsque la limite est atteinte, l'utilisation du logiciel devient alors impossible. Intérêt : éviter l'emploi de logiciels sans licences
Gestionnaire des services Internet	Permet de configurer le serveur en tant que serveur web pour l'intranet ou l'Internet si l'entreprise dispose d'une connexion permanente à Internet
Utilisateurs et ordinateurs Active Directory	Permet de gérer les utilisateurs ainsi que les ordinateurs appartenant au domaine voir I

Tab 02 : Les outils les plus importants

Tab 02 : Les outils les plus importants

Chapitre 03

Le protocole TCP/IP

I- Le protocole TCP/IP, adressage IP et routage

TCP/IP est actuellement le protocole de communication le plus utilisé dans les réseaux locaux. C'est aussi le protocole de transport utilisé par le réseau Internet

1- L'adresse IP

a- Qu'est ce qu'une adresse IP

Chaque machine d'un réseau TCP/IP possède une adresse IP (Internet Protocol).
Une adresse IP est constituée d'un groupe de 4 octets soit 4 fois 8 bits, les octets les plus à gauche déterminent l'adresse du réseau et le ou les octets de droite déterminent l'adresse de la machine.
Exemple : 192.168.1.5
192.168.1.0 correspond à l'adresse réseau alors que 5 représente l'adresse de l'ordinateur dans le réseau. Le nombre de machines maximum pouvant être connectés sur ce type de réseau est de 254 (i1 comporte 256 possibilités de 0 à 255 mais les octets 0 et 255 sont réservés).

b- Les classes d'adresse

Les adresses IP sont regroupées en 3 classes principales. Ce sont les bits de poids forts (bits à gauche de l'adresse IP) qui déterminent la classe d'adresse :

Classe	1er octet	Etendue	Etendue en nombre décimal	Nbre de machines possibles
A	**0**	De 00000001 à **0**1111110	De 1 à 126	256^3-2=**16 777 214**
B	**10**	De **10**000000 A **10**111111	De 128 à 191	256^2-2=**65 534**
C	**110**	De **110**00000 à **110**11111	De 192 à 223	256-2=**254**
D	**1110**	De **1110**0000 à **1110**1111	De 224 à 239	Réservé (multicast)
E	**1111**	De **1111**0000 à **1111**1110	De 240 à 254	Réservé à un usage futur

Tab 03 : Les classes d'adresse

Conclusion : pour connaître la classe d'un réseau, il suffit de lire le premier octet.
Exemple : 192.168.1.5 est l'adresse IP d'une machine appartenant à un réseau de classe C (192 appartient à la classe C)

Remarque : l'adresse 127.0.0.1 est une adresse de « bouclage ». Cette adresse correspond à l'adresse interne de tout ordinateur et est destinée à effectuer des tests. Exemple : pour tester un serveur web depuis la machine où ce service « tourne » il suffit de saisir l'adresse http://127.0.0.1

c- Le masque de sous-réseau

Le masque de sous-réseau permet de différencier l'adresse IP du réseau de l'adresse IP de la machine.
Comme l'adresse IP, le masque de sous-réseau se compose d'un groupe de 4 octets. Chaque classe d'adresse comporte un masque par défaut (qui peut être personnalisé pour créer des sous-réseaux mais c'est une affaire de spécialiste).

Masques de sous-réseau par défaut :

Classes	Masque de sous-réseau par défaut	Nombre de machines maximum
A	255. 0. 0. 0	256^3-2=**16 777 214**
B	255.255. 0. 0	256^2-2=**65 534**
C	255.255.255.0	256-2=**254**

Tab 04 : Masques de sous-réseau par défaut

Les octets ayant la valeur 0 déterminent la plage d'adresses utilisable pour les machines

Exemple :
Adresse IP : 172. 16.12.21
Masque de sous-réseau : 255.255. 0. 0

On en déduit :

- que cette machine est dans un réseau de classe B (172 est compris entre 127 et 191)
- que l'adresse du réseau est : **172.16**.0.0 (l'adresse de réseau est codée sur les 2 premiers octets car les deux premiers octets du masque de réseau sont égaux à 255)
- les deux derniers octets servent à identifier de manière unique chaque machine du réseau 172.16.0.0 (car les deux derniers octets du masque de réseau sont égaux à 0)
- que l'adresse IP de la machine est : 172.16.**12.21.**

En fait, sur le réseau 172.16.0.0 on peut avoir potentiellement 65534 machines connectées.
Si on ajoute d'autres machines sur ce réseau, leur adresse IP commencera alors par **172.16** et les deux derniers octets seront librement choisis de 172.16.**0.1** à 172.16.**255.254**

d- Le choix d'une adresse IP

Le choix de l'adresse IP n'est pas libre :

1) En cas d'ajout d'un nouvel ordinateur à un réseau local, il faut tenir compte de l'adresse réseau et vérifier que l'adresse IP n'est pas déjà prise par un autre ordinateur
2) La majorité des adresses IP sont réservées pour l'Internet et pour en bénéficier il faut les acquérir auprès de l'Internic. En effet Internet utilise l'adressage IP pour identifier de manière unique les postes qui lui sont reliés.

Cependant, l'Internic a réservé trois plages d'adresses IP utilisables dans le cadre d'un réseau local et inaccessibles depuis l'internet. Ces plages d'adresses réservées dites « **publiques** » ou adresses **non routables** ne seront jamais visibles depuis Internet. Ceci permet notamment de limiter les risques d'attaques extérieures en évitant que toutes les machines du réseau soient visibles depuis Internet.
Ces plages d'adresses sont :

Classe A : 10.0.0.0
Classe B : de 172.16.0.0 à 172.31.0.0
Classe C : de 192.168.0.0 à 192.168.255.0

Remarque : en raison de la saturation du nombre d'adresses IP sur Internet, une nouvelle norme d'adresses IP (norme IPv6) a été définie et est utilisée pour les routeurs de l'Internet

e- Adressage IP statique – adressage IP dynamique

L'adressage IP statique consiste à attribuer à chaque ordinateur (serveur, station,…) une adresse IP fixe.

Sous Windows 2003, effectuez un clic droit sur l'icône **Favoris réseau** puis cliquez sur **Propriétés**

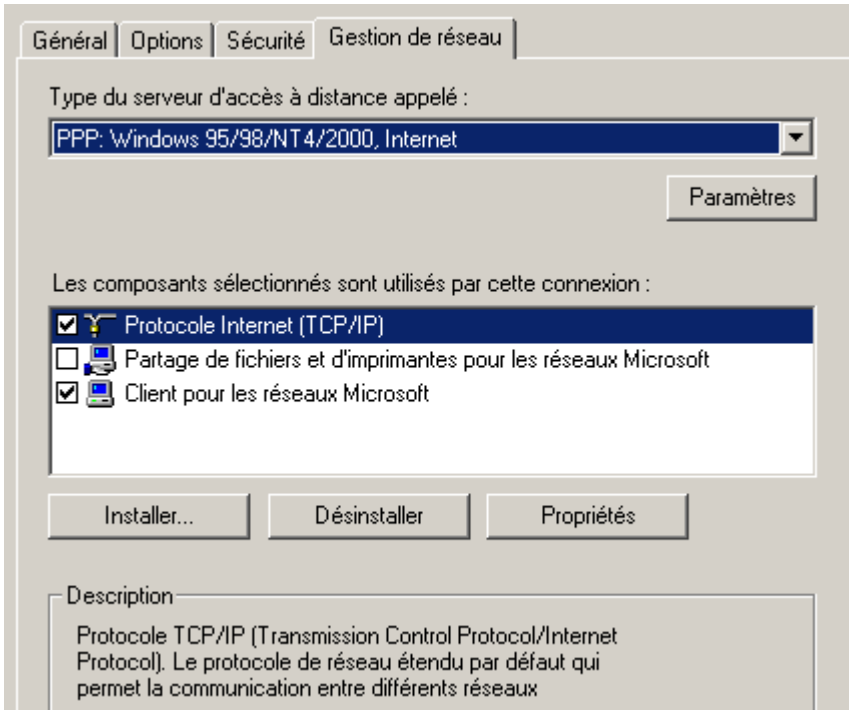


Fig : 08

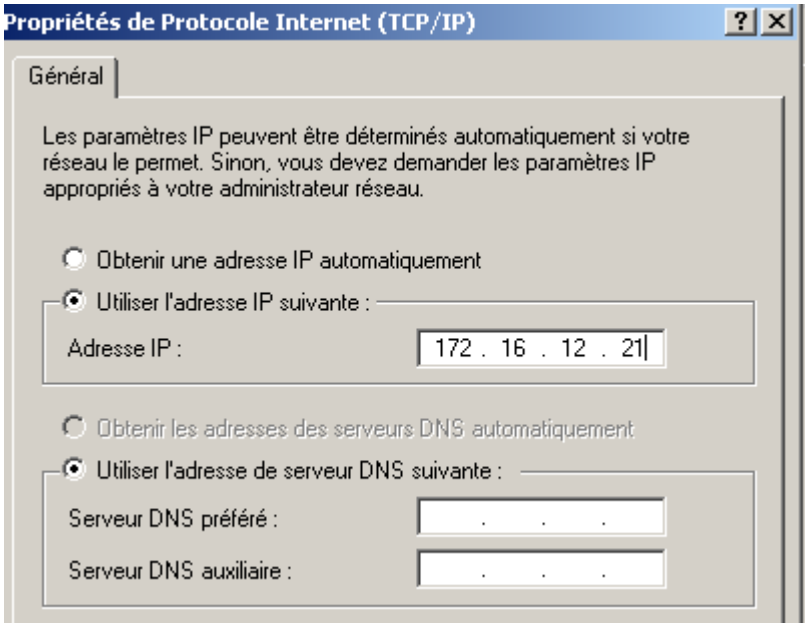


Fig : 09

L'adressage dynamique consiste à obtenir une adresse IP automatiquement : au moment de la connexion au réseau, la station (client) effectue une requête auprès d'un serveur DHCP (DHCP= Dynamic Host Control Protocol) pour obtenir une adresse IP.

2- Le routage

Le routage permet l'échange de données entre deux ordinateurs qui ne sont pas situés sur le même réseau. Le routage fait appel à un dispositif physique : le routeur.

Fig :10

Routage

a- Le routage, comment ça marche ?

Insérer schéma page 5 doc

Sur ce schéma, il y a trois réseaux. Supposons que l'ordinateur P2 souhaite contacter l'ordinateur P6.

- P1 envoie donc un message qui sera réceptionné par tous les postes de son réseau (message de diffusion)

Si **P6 était dans le même réseau que P1**, P6 aurait reçu directement le message (on parle de remise directe)

- Le routeur R4 reçoit le message, il consulte sa table de routage et constate qu'il n'est pas concerné
- Le routeur R1 reçoit également le message, et consulte sa table de routage : P6 (@ip 192.168.1.3 est bien une machine faisant partie du réseau 192.168.1.0), il peut alors relayer le message et l'adresser à P6.

Le routeur agit comme une **passerelle** entre deux réseaux. Lorsqu'un message émis par une machine d'un réseau concerne un autre réseau, le routeur redirige alors le message vers le ou les routeurs voisins
Pour chaque routeur, on peut alors construire une table de routage :

Table de routage de R1

Réseau	Nom routeur	Adresse IP du routeur
172.24.0.0	R6	172.16.10.1
192.168.1.0	R2	10.0.0.2

Tab 05

Table de routage de R2

Réseau	Nom routeur	Adresse IP du routeur
172.16.0.0	R1	10.0.0.1
172.28.0.0	R3	192.168.1.60

Tab 06

Table de routage de R3

Réseau	Nom routeur	Adresse IP du routeur
172.28.0.0	R4	221.12.10.1
172.28.0.0	R2	172.16.0.0

Tab 07

Table de routage de R4

Réseau	Nom routeur	Adresse IP du routeur
192.168.1.0	R3	221.12.10.2

Tab 08

Table de routage de R5

Réseau	Nom routeur	Adresse IP du routeur
172.16.0.0	R6	172.31.20.1

Tab 09

Table de routage de R6

Réseau	Nom routeur	Adresse IP du routeur
172.24.0.0	R5	172.31.10.1
192.168.1.0	R1	172.16.0.1

Tab 10

Donc on peut dire que

Toute machine d'un réseau local utilisant TCP/IP est identifiée par une adresse IP composée de 4 octets. Un masque de sous-réseau composé également de 4 octets permet de déterminer d'une part l'adresse de réseau (ou de sous-réseau) et l'adresse de la machine d'autre part.

Les adresses IP se répartissent principalement en 3 classes d'adresses, chaque classe comportant un masque de sous-réseau par défaut :

Classes	Adresse IP commençant par	Masque de sous-réseau par défaut
A	De 1 à 126	255. 0. 0. 0
B	De 128 à 191	255.255. 0. 0
C	De 192 à 223	255.255.255.0

Tab 11

Le routeur comporte trois fonctions principales
1) Permettre la communication entre des machines n'appartenant pas au même réseau
2) Offrir un accès internet à des utilisateurs d'ordinateur en réseau local
3) Il comporte généralement un système de filtrage des paquets IP qui bloque les accès non autorisés à un réseau, ce système s'appelle un pare-feu (firewall)

De plus, bien que les tables de routage puissent être configurées manuellement (dans les petits réseaux), des protocoles spécifiques (ex : RIP = Routing Information Protocol) permettent aux routeurs de communiquer entre eux pour échanger dynamiquement (de manière automatique) des informations de routage.

Bibliographie :

- « TCP/IP pour les nuls » - éditions Sybex
- http://www.ac-nancy-metz.fr/pres-etab/chopin/cours/reseaux/ Cours en ligne destiné à des étudiants de BTS IG et réalisés par Thierry Jeandel du lycée Chopin

3- Passage des adresses IP aux adresses physiques.

Dans un réseau TCP/IP, nous avons dit que chaque machine était identifiée par une adresse IP. Cette adresse est logique, elle ne dépend pas du matériel utilisé pour relier les machines ensemble. Ces adresses IP peuvent être modifiées relativement rapidement par les administrateurs pour diverses raisons. Nous avons vu jusqu'à présent (couche 2 du modèle OSI) que chaque machine disposait d'une adresse physique différente. Cette adresse physique dépend du matériel réseau utilisé. Il faut trouver un système qui permette de convertir l'adresse logique IP en une adresse physique de la machine. Pour ce faire plusieurs méthodes sont utilisables

a- La table

On peut imaginer que sur chaque machine travaillant avec TCP/IP on dispose d'une table qui fait la conversion entre une adresse logique IP et une adresse matérielle type Pronet, Ethernet, ou ... . Cette méthode, quoi que très efficace, devient lourde à gérer. A chaque ajout, suppression ou modification d'une adresse IP pour une machine, il faut remettre à jour la table de correspondance sur toutes les machines.

b- La conversion directe

Avec des réseaux physiques dont les adresses doivent être paramétrées par l'administrateur, on peut supposer que ce dernier peut faire coïncider tout ou partie de l'adresse physique à l'adresse IP. Cette technique est très facile à mettre en œuvre sur un réseau Pronet, on peut par exemple décider que le dernier octet de l'adresse IP sera égal à l'adresse physique. Cette méthode ne peut cependant pas toujours être mise en œuvre (c'est le cas avec Ethernet).

c- La conversion dynamique (ARP)

Cette méthode de résolution d'adresses physiques est basée sur le principe suivant : chaque machine connaît son adresse IP et son adresse physique. Il faut donc trouver le moyen de demander à une machine dont on ne connaît que l'adresse IP de bien vouloir nous donner son adresse physique pour que l'on puisse lui envoyer les informations.

A première vue nous retombons sur le même problème : obtenir une adresse physique pour demander cette adresse physique.
Pour résoudre ce problème il faut que le réseau (couche 2) supporte la diffusion c'est à dire qu'il existe une "adresse physique" qui corresponde à toutes les machines.
Pour obtenir l'information, la machine qui veut émettre une information sur une machine distante va regarder si elle connaît l'adresse physique du destinataire. Si oui elle va directement lui envoyer cette information.
Sinon, elle va émettre en diffusion sur le réseau une demande de résolution d'adresse. Toutes les stations du réseau vont donc recevoir cette information. Dans cette demande, on trouve l'adresse IP dont on veut connaître l'adresse physique. La machine qui a l'adresse IP correspondante pourra envoyer une réponse contenant son adresse physique.
La correspondance Adresse physique / adresse IP sera gardée par la machine émettrice pendant un certain temps, de façon à ne pas reposer la question trop souvent. Cette information doit expirer au bout d'un moment, car la carte d'interface réseau du destinataire peut être changée donc probablement son adresse physique (c'est le cas avec Ethernet). Ce mécanisme est connu sous le nom d'ARP (Adresse Resolution Protocol). ARP peut être utilisé avec tous types de réseaux supportant la diffusion. Il peut également être utilisé par n'importe quelles familles de protocoles en particulier avec TCP/IP.

4- La résolution inverse (RARP)

Connaître l'adresse physique d'une machine connaissant son adresse IP, permet de communiquer. Il y a cependant des cas où la machine ne connaît que sa propre adresse physique et souhaite obtenir son adresse IP.
Prenons le cas d'une machine qui démarre. Si cette machine démarre sur un disque, elle peut aller lire des fichiers de configurations et donc trouver son adresse IP. Dans ce cas, cette machine n'a pas de problème. Si cette machine va chercher son OS sur le réseau, au démarrage elle ne connaît que son adresse physique. Pour obtenir un fichier image de son boot, elle doit utiliser des protocoles de transfert de fichiers qui sont souvent basés sur TCP/IP. Cette machine doit donc travailler avec TCP/IP et par conséquent connaître son adresse IP. Pour connaître son adresse IP en ne connaissant que son adresse physique, la machine peut utiliser RARP(Reverse Addresse Resolution Protocol).
Le principe est le suivant:
Sur le réseau, on doit avoir une ou plusieurs machines (serveur RARP) contenant des tables (mises à jour à la main) associant des adresses physiques à des adresses IP. La machine qui veut connaître son adresse IP envoie en diffusion sur le réseau une demande RARP. Les machines serveurs RARP vont donc recevoir cette demande et pouvoir donner l'adresse à la machine.
Cette dernière peut ainsi demander une image de son OS qui pourra être transférée avec des protocoles de hauts niveaux (tftp, bootp,...).

Chapitre 04

Les réseaux locaux

I- Introduction

Pour répondre à leurs besoins propres en informatique distribuée, les entreprises ont commencé à mettre en œuvre, au sein de leurs établissements des *réseaux locaux d'entreprise,* les RLE ou LAN (*Local Area Network*). Ces réseaux utilisent des protocoles assez simples. Les distances couvertes sont courtes, de quelques centaines de mètres à quelques kilomètres, et les débits peuvent être importants, jusqu'à plusieurs dizaines de Mbit/s.
Ces réseaux se sont prolongés par la suite, surtout aux États-Unis, par des réseaux plus étendus, entre établissements d'une même ville, ou MAN (*Metropolitan Area Network*), ou interurbains, les WAN (*Wide Area Network*).
Les réseaux locaux informatiques ont été introduits pour répondre aux besoins de communication entre ordinateurs au sein d'une entreprise. Dans une structure commerciale, le réseau local est utilisé pour des applications de gestion.
Dans un environnement bureautique, il sert à la création de documents, à la gestion d'agenda, à l'analyse de données, etc. Il s'agit de relier un ensemble de ressources devant communiquer entre elles et d'en assurer le partage à haut débit : stations de travail, imprimantes, disques de stockage, ordinateurs, équipements vidéo. L'accès aux réseaux publics de données est recherché dans un stade ultérieur.

1- Les topologies d'un LAN

Trois topologies sont utilisées essentiellement:

Dans la topologie Bus, uniquement la station destinatrice prélève le message:

Dans la topologie Anneau, le nœud agit comme un répéteur et seule la station destinatrice prélève le message:

Dans la topologie en étoile, chaque station est reliée à un nœud central qui peut être soit un hub soit un nœud:

2- Adressage

Pour différencier les stations reliées sur un même réseau local, il est nécessaire de les repérer par une adresse. Celle-ci est gérée au niveau MAC et possède un format défini par l'IEEE sur 16 bits ou sur 48 bits. Ce dernier format permet un adressage universel des équipements : il correspond à un numéro de série avec un champ donnant le constructeur qui est attribué par l'IEEE, et le numéro de la carte librement choisi par le constructeur. De cette façon, toute carte réseau d'un ordinateur possède une adresse unique dans le monde.
L'administrateur du réseau peut cependant choisir de définir lui-même ses adresses — on parle d'adresse locale — et de les coder sur 16 ou 48 bits. Le format universel sur 48 bits est le plus utilisé. Il est possible de définir des adresses de groupe qui englobent plusieurs utilisateurs. Lorsque tous les bits sont positionnés à 1 (sur 16 bits ou sur 48 bits), il s'agit d'une adresse de diffusion correspondant à l'ensemble des stations d'un réseau local.

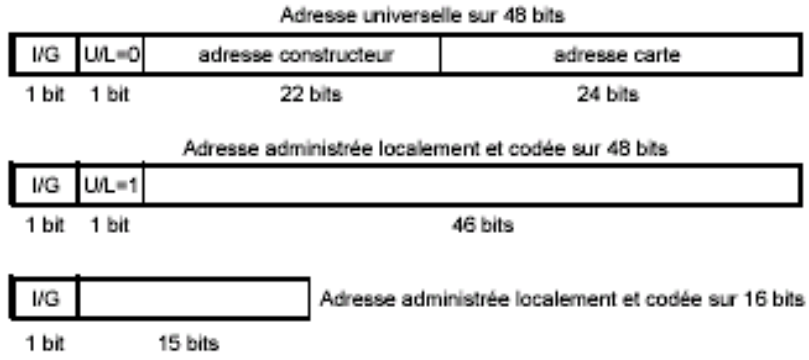


Fig 11 : adressages dans les réseaux locaux

Il existe plusieurs réseaux locaux, dans notre cas nous avons choisis le réseau Ethernet

3- Réseau Ethernet

Les couches 1 et 2 du modèle OSI sont souvent englobées dans l'adaptateur réseau.
Nous allons baser cette étude sur la technologie Ethernet et la technologie Pronet-10. La première est une topologie de type bus et la seconde une topologie de type anneau.
L'étude de ces 2 technologies du marché nous permettra de présenter 2 solutions aux problèmes des couches 1 et 2. Cette étude permettra de voir l'interaction entre les différentes couches et de fixer la notion d'adresses physiques.

Les réseaux Ethernet sont toujours très utilisés malgré l'âge de ce dernier. A l'origine seul le câblage en 10B5 existait. Aujourd'hui, on trouve de réseaux Ethernet en 10B2, 10BT ,100B2ou xxBF.
Un nom de la forme xBy ce lit de la façon suivante: B : modulation de base; x bande passante du réseau (en méga bits par seconde)y définie le type du câble utilisé:

- 5 : câble coaxial de 1,7 cm de diamètre (gros Ethernet)
- 2 : câble coaxial de 0,5 cm de diamètre (Ethernet fin, cheapernet)

- T: paires torsadées.

- F: Fibre optique.

- Câblage en 10B5

Ethernet est le nom que Xerox a donné à cette technologie, au cours des années 1970. Bien que "vieux" par rapport à l'évolution des systèmes informatiques, les réseaux locaux Ethernet sont toujours présents. Aujourd'hui encore, lorsqu'on envisage la création d'un réseau local, on pense souvent Ethernet. La version présentée ici est une version qui a été normalisée par les sociétés Intel, Xerox et DEC.
A l'origine un réseau Ethernet était matérialisé par un câble coaxial de couleur jaune d'environ 1,7 cm de diamètre. Sur ce câble, les machines ne peuvent être connectées que tous les multiples de 2,5m. Pour

facilité les mesures, sur le câble normalisé de couleur jaune, on trouve une bague noire tous les 2,5m. La connexion d'une nouvelle machine (souvent appelée station) se fait via l'intermédiaire d'une prise "vampire". La pose de cette dernière ne nécessite pas de rupture du câble donc d'interruption du réseau. La prise est constituée d'une partie connectique, qui dérive une partie du signal électrique vers un dispositif électronique (appelé Transceiver). Le rôle du transceiver, est de détecter l'utilisation du câble et de transformer les signaux analogiques véhiculer sur le câble en signaux numérique compréhensible par l'ordinateur. Chaque station est connectée à son transceiver par un câble 15 fils (appelé Drop Câble).

Voici quelques propriétés d'un câblage en 10B5:

- Chaque extrémité du câble est terminée par (un "bouchon") une résistance de 50 W entre l'âme et la tresse de blindage.
- La tresse de blindage doit être reliée à la terre à ces extrémités.
- La longueur maximale d'un segment est de 1500m.
- La longueur maximale du drop câble est de 100m
- Pour une courbure, l'angle maximal est de 120° sur un rayon minimum de 20 cm.

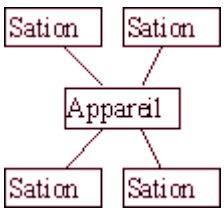
Câblage en 10B2

Le câblage en 10B2 plus connu sous les noms d'Ethernet fin", "thin Ethernet", "cheapernet " est une évolution récente du 10B5. Cette évolution due aux progrès de l'électronique permet de diminuer les coûts de câblage.
Les transceivers sont directement intégrés à la carte réseau. Sur chaque carte réseau on vient fixer un T disposant de connecteur BNC (2 femelles et un mâle que l'on branche sur la carte). Les stations sont reliées les unes aux autres par des cordons munis de connecteur BNC mâles que l'on connecte sur les T. Lorsque l'on veut insérer une station sur le bus, on est obligé de pratiquer une coupure sur le câble et de mettre des connecteurs BNC.
Voici quelques propriétés d'un câblage en 10B2:

- Chaque extrémité du câble est terminée par (un "bouchon") une résistance de 50 W entre l'âme et la tresse de blindage.
- La longueur maximale d'un segment est de 185m.
- La distance minimale entre 2 stations et de 50 cm.
- Le nombre de stations sur un segment est limité à 30

Câblage en 10BT ou 100BT

Cette technique de câblage a été prévue pour pouvoir utiliser les paires non utilisées par les gens des télécom dans les bâtiments. Il ne s'agit physiquement plus d'un câblage de type bus mais d'un câblage de type étoile. Toutes les stations sont connectées par des paires torsadées sur un élément actif (hub, switch,.)



Ce câblage de type étoile respecte également le principe CSMA/CD d'Ethernet puisque l'appareil (passif) réémet l'information vers toutes les stations.

Il existe différents types d'appareils que nous allons détailler plus tard. Pour l'instant, nous allons supposer qu'à chaque fois qu'une station émet une information, l'appareil réemet cette information vers toutes les autres. Ainsi, on retrouve le principe de diffusion sur un bus.
Les limitations varient en fonction de la bande passante (10Mb ou 100Mb)que l'on souhaite obtenir.
Pour obtenir une bande passante de 100 Mb il faut que le câblage soit de catégorie 5. Ce qui implique des contraintes énormes sur la qualité du câble et sur la pose de ce dernier.
Pour obtenir une bande passante de 10 Mb il faut que le câblage soit de catégorie 3.
La catégorie 3 correspond en général au câblage utilisé par les téléphonistes.
La catégorie 5 nécessite une pose, et un câble, spécifiques.

a- Amélioration en nombre de stations

Sur un réseau Ethernet, en fonction du câblage utilisé, il existe des limitations soit en nombre de machines et/ou en longueur de câble. Sur un réseau local, on peut cependant dépasser ces limitations grâce à du matériel. L'ajout de ce matériel (actif ou passif) ne modifie pas les principes généraux. En particulier, lorsque l'on parlera d'interconnexion de réseaux, ce matériel sera complètement transparent.

b- Eléments passifs

Ce type de matériel intervient directement au niveau de la couche 1. Il prend le signal et l'amplifie.
On trouve des répéteurs pour les câblages en 10B5 et 10B2. On ne peut mettre que 2 répéteurs au maximum sur un réseau de type Ethernet.
Sur un câblage 10BT ou 100BT les appareils au centre de l'étoile peuvent être de type passif ou actif .

c- Eléments actifs

Ce type de matériel est dit actif, car il doit connaître le type des trames envoyées. Ces appareils sont considérés comme une station sur le bus, ils reçoivent des trames et les réémettent sur le second câble si ces dernières sont valides. On peut trouver des ponts (bridge), multiports, ... en 10B5 et 10B2.
En 10 BT, ce matériel n'existe pas, car il suffit d'interconnecter les hubs les uns aux autres.

d- Amélioration des performances

Le problème d'un réseau Ethernet est qu'à un instant donné, seulement 2 machines (sauf en diffusion) peuvent communiquer ensemble.
Il existe des appareils actifs qui vont permettre de segmenter le réseau physique en petit morceau pour du 10Bx. On trouve des variantes de ponts et de multiports qui sont dits filtrant. Ils agissent au niveau de la couche 2. En regardant l'adresse de l'émetteur et celle du destinataire (contenues dans la trame) l'appareil peut savoir s'il doit recopier ou non l'information sur les autres câbles.
Le principe en 10BT est différent, car les machines sont sur des câbles différents. L'idée consiste à "ne relier" à un moment donner (durant le passage de la trame) que les câbles des machines concernées. Si plusieurs couples de machines communiquent, l'appareil (un switch) établie plusieurs canaux de communication.

Chapitre 04

Administration d’un réseau local sous Windows server

.

Travail demandé

1) Lire bien les chapitres
2) Ajouter une introduction générale (aperçue sur le réseau+nécessité des réseaux au sein de l'entreprise +notre travail)

3) Vous devez numéroter (les pages, les figures, les tableaux, et les schémas)
Exemple : ***figure I.1*** **:** nom de la figure
Tableau I.2 : titre de tableau

4) Ajouter les définitions des réseaux MAN, LAN, WAN +schéma
5) Conclusion pour chaque chapitre+conclusion générale

N'oublier pas la bibliographie (site +livre)

6) ***Chapitre 04***

Deuxième étape (la pratique)

- Présentation de windows server 2003
- Mise en ouvre d'un réseau locale sous Windows server 2003
  1) Matériels nécessaires
  2) Les étapes de la configuration
  3) Maintenance et vérification

7) **Mise en forme du chapitre**
Titre : Time New Roman, 16, gras souligné
Sous titre : Time New Roman, 13.5, gras
Texte : Time New Roman, 12, normal

Entête de chapitre exemple : [chapitre 01 généralité sur les réseaux informatique]
Remarque : Entête en gras souligné