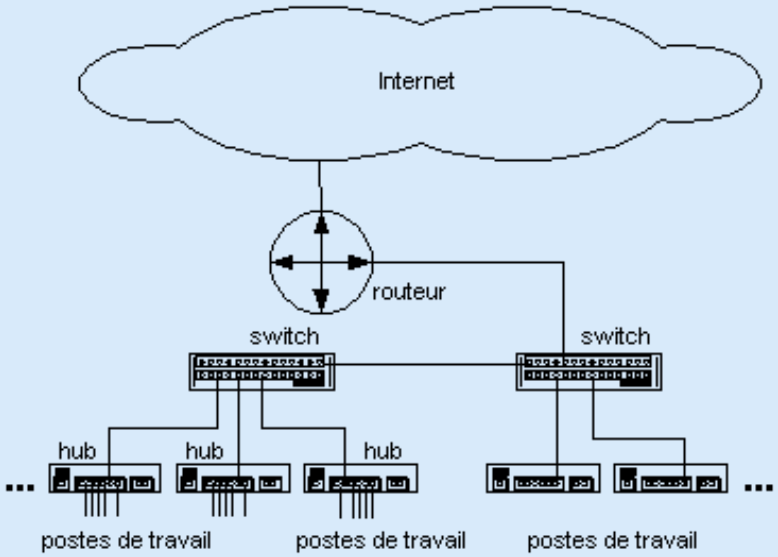
5. Hub, switch, routeur réseaux

5.1 Introduction

Jusqu'ici, nous avons utilisé le terme "concentrateur réseau" pour désigner les "nœuds" des réseaux en T Base 10, T base 100, gigahertz, ... (à l'exclusion des réseaux de type câble coaxial de topologie en bus). Ceci est très simpliste. Les concentrateurs Ethernet rassemble les hub, les switch, routeurs, ... Au niveau installation, la technique des câblages est quasiment la même. Le choix du type de concentrateur varie suivant l'importance du réseau, l'emplacement du concentrateur et l'importance (inter-connexion) de réseaux.



5.2. Hub (répétiteur)

Les Hub sont utilisés en Ethernet base 10 et base 100. L'Hub est le concentrateur le plus simple. Ce n'est pratiquement qu'un répétiteur (c'est son nom en Français). Il amplifie le signal pour pouvoir le renvoyer vers tous PC connectés. Toutes les informations arrivant sur l'appareil sont donc renvoyées sur toutes les lignes. Dans le cas de réseaux locaux importants par le nombre de PC connectés ou par l'importance du flux d'informations transférées, on ne peut utiliser des HUB. En effet, dès qu'un PC dit quelque chose, tout le monde l'entend et quand chacun commence à transmettre, les vitesses diminuent directement. Les HUB sont caractérisés par un nombre de connexion: 4, 5, 8, 10, 16, 24, ...

Suivant la version et le modèle, ils intègrent quelques particularités de connexion spécifiques à l'appareil.

Hubs base 10: nombre de connexion suivant le modèle, port inverseur (celui-ci permet de connecter deux Hubs entre-eux, évitant l'utilisation d'un câble RJ45 croisé), une connexion coaxial. Par connexion, on retrouve une led signalant la connexion à une carte et une led de collision par canal ou pour l'ensemble. Cette dernière signale l'état de l'ensemble des connexions.

Hubs base 100: nombre de connexion suivant le modèle, port inverseur (celui-ci permet de connecter deux Hubs entre-eux), jamais de connexion coaxial. Par connexion, on retrouve une LED signalant la connexion à une carte et une led de collision par canal ou pour l'ensemble. Cette dernière signale l'état de l'ensemble des connexions. De plus, pour les versions 10/100, on retrouve deux LED pour chaque canal (base 10 et base 100)

Une dernière remarque, selon la norme, le **nombre maximum de HUB en cascade** (raccordés port à port, par de types empilables) est limité à 4 entre 2 stations pour le 10 base T et à 2 pour le 100 base T. Ceci est lié au temps de propagation maximum d'un signal ETHERNET avant sa disparition et au temps de détection des collisions sur le câble. Il se pourrait que la collision ne soit pas détectée à temps et que la deuxième station émettrice envoie le message en pensant que la voie est libre. Ceci n'existe pas pour les switch "store and forward" qui enregistrent les trames avant de les envoyer et segmentent le réseau suivant les connexions, évitant ces collisions.

5.3. Switch (commutateur).

5.3.1. Introduction

D'aspect extérieur, il est équivalent à un HUB.

Le défaut des HUB's est que toutes les données transitent vers tous les PC. En recevant une information, un switch décode l'entête pour connaître le destinataire et ne l'envoie que vers celui-ci dans le cas d'une liaison PC vers PC. Ceci réduit le trafic sur le câblage réseau. A la différence, les informations circulent toutes sur tout le câblage avec les hub's et donc vers toutes les stations connectées. Ils travaillent donc sur le niveau 1, 2 et 3 du modèle OSI, pour seulement les couches 1 et 2 dans le cas du HUB'S. Le niveau 3 du modèle OSI détermine les routes de transport. Les switch remplacent de plus en plus les HUB'S. Les prix deviennent pratiquement équivalents.

La majorité des switch peuvent utiliser le **mode Full duplex.** La communication est alors bi-directionnelle, doublant le taux de transfert maximum. Cette fonction n'est jamais implantée dans les HUB. Le Switch vérifie automatiquement si le périphérique connecté est compatible full ou half duplex. Cette fonction est souvent reprise sous la dénomination "**Auto Negociation**".

Les modèles de switch actuels sont souvent **Auto MDI/MDIX**. Ceci signifie que le port va détecter automatiquement le croisement des câbles pour la connexion Ethernet. Dans le cas des HUB, un port muni d'un bouton poussoir, reprend la fonction manuellement. Vous pouvez néanmoins utiliser des câbles croisés pour relier des concentrateurs entre eux.

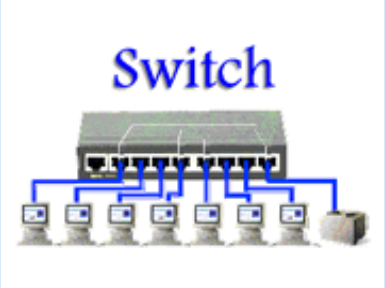
L'utilisation des switch permet de réduire les collisions sur le câblage réseau. Pour rappel, lorsqu'un périphérique souhaite communiquer, il envoie un message sur le câblage. Si un autre périphérique communique déjà, deux messages se retrouvent en même temps sur le réseau. Le premier reprend son message au début et le deuxième attend pour réessayer quelques millisecondes plus tard.

Il n'y a (en théorie) pas de limitations du nombre de switch en cascade sur un réseau.

5.3.2. Fonctionnement d'un switch.

Au démarrage, un switch va construire une table de correspondance adresse MAC - numéro de port de connexion. Cette table est une mémoire interne du switch. Par exemple pour un D-link DSS-16+ (16 ports), elle est de 8000 entrées (stations). Par contre, pour un modèle de gamme inférieure (D-Link DES -1024D de 24 ports) elle est également de 8000 entrées, pour la majorité des switchs 5 ports, elle varie de 512 à 1000 entrées. Ceci ne pose pas de problèmes pour un petit réseau mais bien pour de gros réseaux. De toute façon, le nombre de PC maximum connectés est limité par la classe d'adresse IP utilisée. Lorsqu'une nouvelle carte va se connecter sur un de ses ports, il va adapter sa table. Les performances du switch sont donc tributaire de l'importance de cette table.

Voyons maintenant ce qui se passe lorsqu'un PC (PC1) communique vers un autre PC (PC2) connecté sur le même switch. Le message de départ incluant l'adresse de destination, le switch va retrouver directement dans sa table l'adresse du PC2 et va rediriger le message sur le port adéquat. Seul le câblage des 2 ports (PC1 et PC2) vont être utiliser. D'autres PC pourront communiquer en même temps sur les autres ports.



Voyons maintenant le cas ou le réseau utilise 2 switch. Le PC1 envoie le message avec l'adresse de destination sur le switch1 sur lequel il est raccordé. Le switch va vérifier dans sa table si l'adresse de destination est physiquement raccordé sur un de ses ports dans sa table. Dans notre cas ce n'est pas le cas. Le switch va donc envoyer un message spécial (une adresse MAC FF.FF.FF.FF.FF.FF, appelée broadcast) sur tous ses ports pour déterminer sur quel port se trouve le périphérique de destination. Ce broadcast passe généralement sur tout le réseau. En recevant le broadcast, le switch 2 va vérifier dans sa table si l'adresse de destination est dans sa table. Dans notre cas, elle est présente. Il va donc renvoyer un message au switch 1 signifiant que le message est pour lui. Le switch 1 va donc diriger le message vers le port connecté au switch 2. Le switch 1 va mémoriser dans sa table l'adresse du PC2 et le port associé (dans notre cas celui du switch 2). Ceci ne pose pas trop de problèmes tant que la capacité de la table du switch 1 est suffisante.

Voyons maintenant quelques cas plus complexes. Lorsqu'une adresse MAC non connectée en direct est placée dans la table, le switch va la garder pendant un certains temps. Si une nouvelle demande vers cette adresse est reçue, le port de destination est retrouvé dans la table. Par contre, si le délai entre les demandes est trop long (généralement 300 secondes), l'entrée de la table est effacée et le processus de broadcast est de nouveau activé. Forcément, si la table est trop petite (cas des Switch avec un faible nombre de ports sur un réseau très important), l'entrée MAC dans la table peut-être effacée prématurément.

Ces particularités de tables réduites dans les switch de bas de gamme pose de gros problèmes dans les réseaux. De plus, moins le switch comporte d'entrée, plus la table est petite. Ceci implique que pour l'utilisation de petits switchs (4-8 ports), le nombre de switch relié entre-eux pour une connexion entre 2 PC est limitée. J'ai déjà eut le problème dans un réseau de 30 PC. Dès que l'usine démarrait, les communications réseaux s'effondraient. Le remplacement de switch par des HUB pour les stations les plus éloignées a résolu le problème mais on aurait pu utiliser des switch de meilleure qualité.

Tous les switch ne sont pas équivalents. Pour des réseaux d'une dizaine de stations, le problème ne se pose pas. Par contre, pour les réseaux importants, les switch de milieu et haute gamme corrigent mieux les atténuations des signaux reçus avant transmission.

5.3.3. Types de switch

La technologie d'un switch est étroitement liée au type de donnée, à la topologie du réseau et aux performances désirées.

Le premier procédé de fonctionnement et le plus courant, appelé **Store and Forward**, stocke toutes les trames avant de les envoyer sur le port adéquat. Avant de stocker l'information, le switch exécute diverses opérations, allant de la détection d'erreur (RUNT) ou construction de la table d'adresses jusqu'aux fonctions applicables au niveau 3 du modèle OSI, tel que le filtrage au sein d'un protocole. Ce mode convient bien au mode client/serveur car il ne propage pas d'erreur et accepte le mélange de diverses médias de liaison. Ceci explique qu'on les utilise dans les environnements mixtes cuivre / fibre ou encore dans le mélange de débits. La capacité de la mémoire tampon varie de 256 KB à plus de 8 MB pour les plus gros modèles. Les petits switch de ce type partagent souvent la capacité de mémoire par groupes de ports (par exemple par 8 ports). Par contre, les modèles de haute gamme utilisent une mémoire dédiée par port d'entrée. Le temps d'attente entre la réception et l'envoi d'un message dépend de la taille des données. Ceci ralentit le transfert des gros fichiers.

Le mode **Cut Through** analyse uniquement l'adresse Mac de destination (placée en en-tête de chaque trame, codée sur 48 bits et spécifique à chaque carte réseau) puis redirige le flot de données sans aucune vérification. Ce type de switch ne fait aucune

vérification sur le message proprement dit. Dans le principe, l'adresse de destination doit être préalablement stockée dans la table, sinon on retrouve un mécanisme de broadcast. Ces switch sont uniquement utilisées dans des environnements composés de liaisons point à point (clients - serveur). On exclus toutes applications mixtes de type peer to peer.

Le mode **Cut Through Runt Free** est dérivé du Cut Through. Lorsqu'une collision se produit sur le réseau, une trame incomplète (moins de 64 octets) appelée Runt est réceptionnée par le switch. Dans ce mode, le switch analyse les 64 premiers bits de trames avant de les envoyer au destinataire. Si la trame est assez longue, elle est envoyée. Dans le cas contraire, elle est ignorée.

Le mode **Early Cut Through** (également appelé **Fragment Free** chez CISCO) est également dérivé du Cut Through. Ce type de switch transmet directement les trames dont l'adresse de destination est détectée et présente dans la table d'adresse du switch. Pour cela, la table doit être parfaitement à jour, ce qui est difficile dans le cas de gros réseaux. Par contre, il n'enverra pas les trames dont l'adresse de destination n'est pas clairement identifiée. Il ne tient pas compte non plus de l'adresse d'origine. Les temps d'attente sont très bas.

Le mode **Adaptive Cut Through** se distingue surtout au niveau de la correction des erreurs. Ces commutateurs gardent la trace des trames comportant des erreurs. Lorsque le nombre d'erreur dépasse un certain seuil, le commutateur passe automatiquement en mode Store and Forward. Ce mécanisme évite la propagation des erreurs sur le réseau en isolant certains segments du réseau. Lorsque le taux d'erreur redevient normal, le commutateur revient au mode Cut Through.

5.3.4. Particularités supplémentaires

Un Switch peut être **stackable** (empilable). Dans ce cas, un connecteur spécial permet de relier plusieurs switch de même marque entre-eux. Le nombre de switch empilés (du même modèle) est limité. L'ensemble du groupe de switch est vu comme un seul switch. Ceci permet d'augmenter le nombre de ports et de reprendre une table commune plus importante. Les HUB ne sont pas véritablement stackables puisque ceci reviendrait exactement au même que de les interconnecter avec des câbles croisés).

Certains switch sont **manageables**. Par une interface de type WEB reliée à l'adresse IP du switch ou par RS232 et l'utilisation de Telnet, vous pouvez bloquer certains lignes, empêchant par exemple, un partie de PC de se connecter vers un autre bloc de PC ou de déterminer physiquement quel PC a accès à quel serveur. Ceci permet également de déterminer des plages d'adresses sur des ports (cas où plusieurs switch - Hub sont chaînés) et ainsi d'augmenter la vitesse. Une petite remarque néanmoins, le management se fait généralement en fonction des adresses MAC (unique et déterminée à la fabrication de la carte réseau ou du périphérique). L'utilisation de ces caractéristiques doit être envisagée avec précaution puisque si vous changez une carte réseau, le switch devra être reconfiguré. Certains modèles permettent néanmoins de créer des groupes d'utilisateurs en utilisant le protocole IGMP. Ils sont dits de niveau 2 (layer 2 du modèle OSI) s'ils permettent de déterminer les adresses et de niveau 3 (layer 3 du modèle OSI) s'ils permettent en plus de bloquer par ports (TCP ou UDP).

Via l'interface IP ou Telnet, un **switch manageable** permet également de vérifier à distance les connexions sur le switch (affichage de la face avant), sauvegarder ou restaurer la configuration, mise à jour du firmware, paramétrer la durée de vie des adresses MAC dans la table, ...

Certains switch de type Cut Through intègrent des fonctions supplémentaires comme le **Meshing** qui permet de créer une table sur plusieurs switch (et de ne plus envoyer les informations sur tous les ports quand l'appareil de destination n'est pas directement connecté) sur le switch. Le **Port Trunking** permet de réserver un certain nombre de ports pour des liaisons entre 2 commutateurs.

5.4. Routeurs.

Les hub et switch permettent de connecter des appareils faisant partie d'une même classe d'adresse en IP ou d'un même sous-réseau (autres protocoles). Pour rappel, une adresse IP d'un appareil connecté à un réseau est unique. Il est de type X.X.X.X, par exemple 212.52.36.98. Les valeurs X peuvent varier de 0 à 255. L'adresse IP est constituée de 32 bits et d'un masque également codé sur 32 bits.

On a déterminé des hiérarchies dans les adresses, appelées classes d'adresse.

Classe A	Réseau	Machine	Machine	Machine
Adresses de 1.0.0.0 à 126.255.255.255. La plage 10.0.0.0. à 10.255.255.255 est privée. 128 domaines (réseau) et 16.777.216 machines de classe A par domaine 1.X.X.X.X, 2.X.X.X.X, ...				
Classe B	Réseau	Réseau	Machine	Machine
127.0.0.0 à 191.255.255.255. La plage 172.16.0.0. à 172.31.255.255 est privée 16.000 domaines et 65.536 Machines de classe B par domaine 127.0.X.X., 127.1.X.X., ...				
Classe C	Réseau	Réseau	Réseau	Machine
192.0.0.0 à 223.255.255.255. La plage 192.168.0.0. à 192.168.255.255 est privée 2.000.000 domaines et 254 machines de classe C par domaine 192.0.0.X, 192.0.1.X, 192.0.2.X, ...				
Classe D	Multicast			
Classe E	Expérimentale			

Les adresses terminant par 0 ou 255 ne sont pas utilisables directement.

2 Stations dans un même réseau ou même sous-réseau peuvent communiquer directement ou avec de simple équipement de niveau 2 (hub ou switch).

2 stations dans 2 sous réseaux différents doivent communiquer via un routeur.

Par exemple:

.un équipement avec l'adresse 12.0.0.0 (classe A) peut directement communiquer avec un équipement d'adresse TCP/IP 16.23.25.98.

. un équipement avec l'adresse 127.55.63.23. (classe B) peut directement communiquer avec un appareil situé à l'adresse 191.255.255.255 (classe B).

. un PC dans un réseau interne avec l'adresse 192.168.1.23 peut communiquer avec l'adresse 192.168.1.63 (classe C identique).

Par contre, la connexion d'un PC avec l'adresse 192.168.1.23 (classe C) devra passer par un routeur pour communiquer avec une installation situé en 15.63.23.96 (classe A). Ceci est le cas pour un PC qui se connecte à un site Internet (utilisant des adresses de classes A ou B). De même, dans un réseau interne, la connexion de deux stations dans des réseaux de classes C différentes (par exemple **192.168.2**.23 et **192.168.3.**32) doivent passer par un routeur. Un réseau sans routeur est donc limité à 254 stations (0 et 255 ne sont pas utilisées).

De même; comme les adresses des sites INTERNET peuvent être pratiquement dans toutes les plages d'adresses A et de classe B, le **raccordement d'un réseau interne à INTERNET** passe obligatoirement par un **routeur**.

Rien n'oblige à utiliser les adresses de classes C pour un réseau interne, mais c'est préférable.

Remarque, la classe d'adresse **169.254.XXX.XXX** n'est pas utilisable dans un réseau interne pour un partage Internet, cette plage d'adresse particulière ne l'accepte pas même si elle est souvent donnée par défaut par DHCP de Windows.

Le routeur est pratiquement un ordinateur à lui tout seul. Celui-ci décode les trames et reconnaît des parties s'informations des

entêtes et peuvent ainsi transmettre les informations sur d'autres routeurs qui reconduisent les informations vers les destinataires.

Un routeur réunit des réseaux au niveau de la couche réseau (couche 3), il permet de relier 2 réseaux avec une "barrière" entre les deux. En effet, il filtre les informations pour n'envoyer que ce qui est effectivement destiner au réseau suivant. L'utilisation la plus courante est la connexion de multiples stations vers INTERNET. Les données transitant sur le réseau local (non destinées à Internet) ne sont pas transmises à l'extérieur. De plus, les routeurs permettent en partie de cacher le réseau. En effet, dans une connexion Internet par exemple, le fournisseur d'accès donne une adresse TCP/IP qui est affectée au routeur. Celui-ci, par le biais d'une technologie NAT / PAT (Network adress translation / port adress translation) va rerouter les données vers l'adresse privée qui est affectée au PC.

Les routeurs sont paramétrables et permettent notamment de bloquer certaines connexions. Néanmoins, il n'assurent pas de sécurité au niveau des ports TCP ou UDP. Ils sont utilisés pour interfacer différents groupes de PC (par exemple les départements) en assurant un semblant de sécurité. Certains switch de manageables peuvent en partie être utiliser pour cette fonction tant que le réseau reste dans la même classe d'adresses. La principale utilisation en PME est le partage d'une connexion Internet, mais d'autres existent comme réseau sous Win98 et suivant ou appareils spécifiques. Pour renseignements complémentaires pour le partage Internet, référez-vous aux différents chapitres sur le cours INTERNET

Les routeurs ne servent pas qu'à connecter des réseaux à Internet, ils permettent également de servir de pont (Bridge en anglais) pour se connecter à un réseau d'entreprise. Les connections futures pour ce genre d'application sécurisées vont plutôt pour les VPN via INTERNET. Nous verrons ceci dans le chapitre 10: Connexions distantes

Il n'est pas possible de relier directement 2 réseaux en branchant 2 cartes réseaux dans un PC central, sauf en utilisant un logiciel de liaison proxy (passerelle) de type Wingate.

Un serveur **DHCP** (Dynamic Host Configuration Protocol) peut être implanté de manière software (Windows 2000 par exemple) ou dans un routeur. Cette possibilité permet d'attribuer automatiquement les adresses IP à chaque station dans une plage d'adresse déterminée (dans la même classe d'adresse).

5.5. Répéteurs

Le répéteur est un équipement qui permet d'outrepasser la longueur maximale imposée par la norme d'un réseau. Pour se faire il amplifie et régénère le signal électrique. Il est également capable d'isoler un tronçon défaillant (Câble ouvert par exemple) et d'adapter deux médias Ethernet différents. (Par exemple 10base2 vers 10baseT). Cette dernière utilisation qui est la principale actuellement.

Pour les liaisons 1000Base LX mono-mode, il existe des appareil permettant des liaisons de plus de 100 kilomètres.

5.6. Différence entre un HUB et un Switch

HUB	SWITCH
Les informations envoyées d'un PC vers un autre (ou une imprimante) sont envoyés à tous les PC qui décodent les informations pour savoir si elles sont destinées.	Les informations envoyées d'un équipement réseau vers un autre ne transitent que vers le destinataire. Si un autre PC envoie des informations vers l'imprimante, les deux communications peuvent donc se faire simultanément.
	

La bande passante totale est limitée à la vitesse du hub. Un hub 100 base-T offre 100Mbps de bande passante partagée entre tous les PC, quelque soit le nombre de ports	La bande passante totale est déterminée par le nombre de ports sur le Switch. i.e. Un Switch 100 Mbps 8 ports peut gérer jusqu'à 800Mbps de bande passante.
Ne supporte que les transferts en "half-duplex" ce qui limite les connections a la vitesse du port. Un port 10Mbps offre une connexion a 10Mbps.	Les Switchs qui gèrent les transferts en mode "full-duplex"offrent la possibilité de doubler la vitesse de chaque lien, de 100Mbps à 200Mbps par exemple.
Moins onéreux par port.	Le rapport performances/prix accru, vaut le supplément de prix.

5.7. Passage des adresses IP aux adresses MAC

Nous savons déjà que les communications se font par les adresses MAC et pas directement par les adresses IP.

Pour une communication, le PC émetteur vérifie si le PC est dans la même classe d'adresse IP. Si c'est le cas, il va envoyer un ARP pour déterminer l'adresse MAC de destination et envoie directement le packet de données et les en-têtes sur le réseau. Les HUBS laissent le packet tel quel puisqu'ils sont de simples amplificateurs. Par contre, si le réseau est relié par des switchs, chaque switch va vérifier l'adresse MAC dans sa table, éventuellement envoyer un broadcast.

Par contre, si le PC de destination n'est pas dans la même classe d'adresse, il envoie le packet au routeur (dont l'adresse MAC est connue) avec l'adresse IP de destination. Le routeur va vérifier s'il est connecté au sous-réseau (classe IP) de destination. S'il est directement connecté, il envoie les informations au destinataire via un ARP. Dans le cas contraire, il va envoyer le packet au routeur suivant, et ainsi de suite.

5.8. Connexion d'un réseau Ethernet.

Par la partie connexion Ethernet, nous savons déjà que:

1. Pour relier 2 hubs (switch) entre-eux, nous devons utiliser un câble croisé. Néanmoins, un petit interrupteur à poussoir est souvent présent sur un des ports qui permet d'utiliser un câble normal. Les nouveaux modèles détectent également automatiquement le croisement.

2. En Ethernet 10, 4 Hubs présentent un blocage au niveau des vitesses de connexion.

3. En Ethernet 100, 2 HUBS en série commencent à provoquer des "bouchons" dans les flux de données.

4. Les distances maximales doivent être respectées (100 mètres maximum pour le câble).

5. Les règles de câblages doivent être strictes: connecteurs, proximités des câbles électriques, réseaux.

Passons maintenant à un réel réseau Ethernet.

A. Les départements (ou bureaux, ou étages) peuvent être connectés par un HUB ou un switch. Si toutes les connexions se font des PC vers un seul serveur, un Hub peut être suffisant. Par contre, en cas d'utilisation d'autres périphériques (imprimantes réseau par exemple), un switch est nettement préférable. L'HUB ou le SWITCH doit avoir un nombre suffisant de ports. Dans le cas d'une petite application unique clients - 1 serveur, comme toutes les communications vont vers un seul PC (le serveur), l'utilisation de switch ou Hub est pratiquement équivalente, sauf si que l'utilisation d'un switch va réduire le nombre de collisions. Le switch peut également être Full duplex (communication bidirectionnelle)

B. Les départements entre-eux peuvent être reliés par des HUB's ou des switchs, mais la préférence doit aller à des switch, si possible manageables qui permettent de bloquer certaines connexions. Toutes connexions extérieures (Internet et liaison inter-réseau) nécessite un routeur. Le cas de partages INTERNET directement sur un PC raccordé à INTERNET doit être proscrit pour les entreprises (partage par Windows), principalement en cas de réseaux lourds de type Win NT ou Netware. En effet, les routeurs incluent la fonction NAT qui permet masquer les différentes adresses du réseau interne et incluent de plus en plus des bases de sécurité intrusions de type firewall hardware.

Lorsque nous terminerons la partie Réseau, nous verrons des cas concrets de connexion réseau.

La suite du cours Hardware 2 -> Chapitre 6: liaisons haute vitesse

Révision: 02/11/2005

Le cours "Hardware 1": PC et périphériques, le cours "Hardware 2": Réseau, serveurs et communication.

Pour l'ensemble de la formation hardware.

Le site YBET informatique à Pin - Chiny