

# **Formation Réseau**

Cette formation est centrée sur la maintenance et l'installation du matériel réseau.

**L'approche de ce cours réseau n'est pas logicielle, mais matérielle:** que le système d'exploitation du serveur réseau soit Windows, Linux ou Novell n'intervient pas directement dans le cours. Nous analyserons ici l'installation et le choix des appareils de connexions. Même si des solutions logicielles sont abordées pour comparaison, la finalité restera la solution hardware. Notre travail dans ce cours se limite (ce n'est déjà pas si mal) au choix, à l'installation, à la maintenance, au dépannage et au paramétrage d'une installation réseau au niveau matériel.

<b>1. INTRODUCTION AUX RESEAUX INFORMATIQUES.....</b>	<b>5</b>
1.1. GENERALITES .....	5
1.2. LE MODELE OSI.....	5
1.3. LE MODELE TCP/IP .....	7
1.3.1. Couche application.....	7
1.3.2. Couche transport.....	7
1.3.3. Couche INTERNET .....	8
1.3.4. Couche Accès réseau.....	8
1.4. LES TYPES D'ORDINATEURS CONNECTES, TYPES DE RESEAUX .....	9
1.5. LES APPLICATIONS RESEAUX.....	9
1.6. LES TYPES DE SERVEURS.....	10
1.7. CARACTERISTIQUES D'UN RESEAU.....	11
1.8. SECURITE ET ADMINISTRATION.....	11
<b>2. BASE DE TRANSMISSION RESEAU.....</b>	<b>13</b>
2.1. INTRODUCTION .....	13
2.2. LE CABLAGE ETHERNET.....	14
2.2.1. La paire torsadée téléphonique.....	14
2.2.2. Le câble coaxial.....	15
2.2.3. La fibre optique .....	15
2.3. LES TOPOLOGIES RESEAU .....	16
2.4. TOPOLOGIE RESEAU EN BUS .....	16
2.5. TOPOLOGIE EN ANNEAU .....	16
2.6. TOPOLOGIE EN ETOILE.....	17
2.7. TOPOLOGIE MIXTE.....	17
2.8. TOPOLOGIE MAILLEE.....	17
2.9. METHODE D'ACCES .....	18
<b>3. RESEAUX ETHERNET.....</b>	<b>19</b>
3.1. INTRODUCTION .....	19
3.2. ETHERNET, IEEE 802.3 10 BASE 5 ET IEEE 802.3 10 BASE 2.....	19
3.3. RESEAU ETHERNET, IEEE 802.3 10 BASE T .....	20
3.4. ETHERNET 100 BASE TX ET 100 BASE T4, FAST ETHERNET.....	23
3.5. GIGABIT ETHERNET.....	25
3.6. CARTE RESEAU ETHERNET.....	25
3.7. HALF DUPLEX ET FULL DUPLEX.....	26
3.8. CABLAGE RJ45 ETHERNET, REGLES, PROBLEMES DE LIAISONS ET APPAREILS DE TESTS .....	27
3.9. ADRESSE MAC.....	29
<b>4. HUB, SWITCH, ROUTEUR RESEAUX.....</b>	<b>31</b>
4.1. INTRODUCTION .....	31
4.2. HUB (REPETITEUR).....	31
4.3. SWITCH (COMMUTATEUR).....	32
4.3.1. Introduction.....	32
4.3.2. Fonctionnement d'un switch.....	32
4.3.3. Types de switches.....	33
4.3.4. Particularités supplémentaires.....	34
4.4. DIFFERENCES ENTRE UN HUB ET UN SWITCH.....	35
4.5. ROUTEUR.....	35

4.6.	REPETEURS .....	37
4.7.	PASSAGE DES ADRESSES IP AUX ADRESSES MAC .....	38
4.8.	CONNEXION D'UN RESEAU ETHERNET .....	38
<b>5.</b>	<b>LIAISONS A HAUTE VITESSE, HAUT DEBIT, ADSL, ATM .....</b>	<b>39</b>
5.1.	INTRODUCTION .....	39
5.2.	LES TECHNOLOGIES DSL .....	39
5.3.	SOLUTIONS SYMETRIQUES .....	39
5.3.1.	HDSL : .....	39
5.3.2.	SDSL (Symetric Digital Subscriber Line): .....	40
5.3.3.	SHDSL .....	40
5.4.	SOLUTIONS ASYMETRIQUES: ADSL, RADSL ET VDSL .....	41
5.4.1.	ADSL (Asymetric Digital Subscriber Line): .....	41
5.4.2.	RADSL .....	42
5.4.3.	VDSL .....	42
5.4.4.	Tableau récapitulatif des technologies DSL .....	44
5.5.	LIGNE LOUEE .....	45
5.6.	CONNEXION INTERNET PAR SATELLITE .....	45
5.7.	CABLE TV .....	46
5.8.	LIAISON ATM .....	46
<b>6.</b>	<b>RESEAU SANS FILS .....</b>	<b>47</b>
6.1.	INTRODUCTION .....	47
6.2.	BLUETOOTH .....	47
6.3.	IEEE 802.11 .....	48
6.4.	IEEE 802.11A .....	48
6.5.	IEEE 802.11B - WIFI - IEEE 802.11 HR .....	48
6.6.	RESEAU SANS FIL IEEE 802.11B+ .....	49
6.7.	RESEAU SANS FIL 802.11 G .....	49
6.8.	CONNEXION SANS FIL 802.11G+ .....	49
6.9.	IEEE 802.11N .....	50
6.10.	CONNEXION INFRA-ROUGE .....	50
6.11.	PARAMETRAGE ROUTEUR D-LINK DI-624 .....	50
6.11.1.	Paramétrage de base du routeur ADSL .....	50
6.11.2.	Paramétrage avancé du routeur D-Link DI-624 .....	53
6.12.	SECURITE DES RESEAUX SANS FILS .....	55
6.12.1.	Introduction .....	55
6.12.2.	Paramétrage d'un point d'accès 802.11G+ D-Link DWL2100AP .....	56
6.12.3.	Configuration d'une station .....	59
6.12.4.	En conclusion .....	61
<b>7.</b>	<b>MONTER UN PETIT RESEAU .....</b>	<b>63</b>
7.1.	INTRODUCTION .....	63
7.2.	LA LIAISON PHYSIQUE .....	63
7.3.	LE LANGAGE DE COMMUNICATION .....	64
7.4.	L'INSTALLATION DES LOGICIELS .....	64
7.5.	LE PARTAGE DE MODEM POUR INTERNET .....	66
7.6.	ET QUAND CELA NE MARCHE PAS? .....	66
7.7.	ET EN RESEAUX LOURDS .....	66
<b>8.</b>	<b>DEPANNAGE RESEAU .....</b>	<b>67</b>
8.1.	RAPPEL .....	67
8.2.	DEPANNAGE .....	67
8.3.	QUELQUES COMMANDES DOS RESEAU .....	69
8.4.	PARTAGE DE CONNEXION INTERNET .....	69
<b>9.</b>	<b>EXERCICE: ARCHITECTURE D'UN RESEAU D'ENTREPRISE .....</b>	<b>72</b>
9.1.	L'EXERCICE .....	72
9.2.	L'ARCHITECTURE GLOBALE .....	73
9.3.	CONNEXION DEPARTEMENT ADMINISTRATIF ET COMMERCIAL .....	75
9.4.	CONNEXION BATIMENT FABRICATION - COMMANDE .....	76
9.4.1.	Cas 1: utilisation de 2 classes d'adresses différentes .....	76
9.4.2.	Cas 2: utilisation d'une même classe d'adresse avec switch manageable .....	77

9.5.	CONNEXIONS GLOBALES DU RESEAU .....	77
9.6.	UN AUTRE POINT DE VUE DE CETTE CONNEXION: MELANGE DE PROTOCOLES. ....	78
9.7.	QUELQUES ERREURS CLASSIQUES .....	79
<b>10.</b>	<b>TECHNOLOGIES ALTERNATIVES RESEAU .....</b>	<b>80</b>
10.1.	INTRODUCTION. ....	80
10.2.	TECHNOLOGIE IPP .....	80
10.3.	CONNEXION ETHERNET PAR RESEAU ELECTRIQUE .....	80
10.3.1.	<i>Introduction.</i> .....	80
10.3.2.	<i>Connexion Internet.</i> .....	81
10.3.3.	<i>Ethernet via réseau électrique.</i> .....	81
10.4.	VOIP, VOICE OVER IP .....	82

# 1. Introduction aux réseaux informatiques

## 1.1. Généralités

Avant de nous attaquer aux infrastructures réseaux, reprenons quelques notions de base sur les réseaux informatiques en général.

Un **réseau** permet de partager des ressources entre plusieurs ordinateurs: données ou périphériques (imprimante, sauvegarde sur bandes, modem, scanner, ...). La première partie de ce cours reprend toutes les informations permettant de connecter ces ordinateurs entre eux. Comme cette formation informatique est **typiquement hardware**, je m'intéresse principalement à l'aspect matériel. Les autres parties d'un réseau sont repris dans les autres cours, notamment "Bases réseaux", "Initiation aux systèmes LINUX & UNIX", "Logiciels réseaux", ...

La transmission d'information entre 2 programmes informatiques sur 2 machines différentes passe par deux modèles: le modèle OSI ou le modèle TCP/IP. Ces deux normes permettent à chaque partie de la communication de dialoguer. Chaque modèle inclut plusieurs couches et chaque couche doit envoyer (et recevoir pour l'autre ordinateur) un message compréhensible par les deux parties. Le chapitre suivant (base de transmission réseau) traitera de la communication dans ses détails.

## 1.2. Le modèle OSI

Le modèle OSI (Open System Interconnection Model) défini en 1977 régit la communication entre 2 systèmes informatiques selon 7 couches. A chaque couche, les 2 systèmes doivent communiquer "compatibles". En hardware (le but de ce cours), nous n'utilisons que les couches inférieures, jusqu'au niveau 3. L'utilisation de Novell Netware, Microsoft Windows NT, Windows 2000, Linux ou tout autre gestionnaire de réseaux n'intervient pas de manière significative sur l'hardware, à part pour les pilotes.

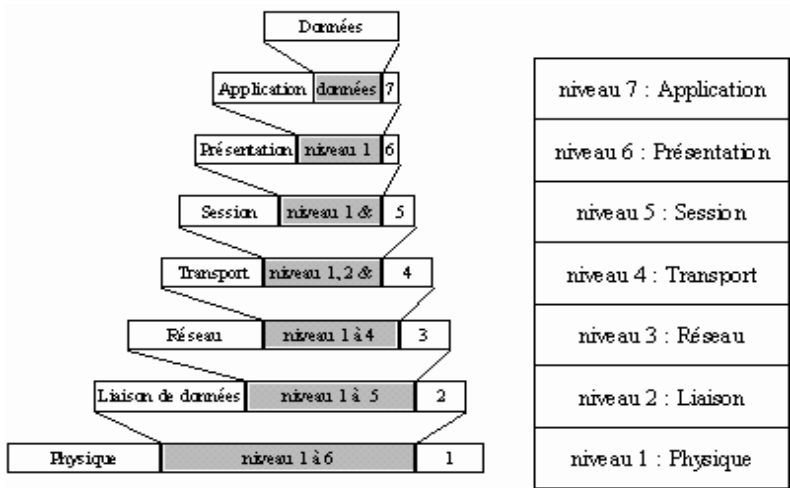
L'OSI est un modèle de base qui a été défini par l'International Standard Organisation (ISO). Ce modèle OSI définit 7 niveaux différents pour le transport de données. Ces niveaux sont également appelés couches.

Application	⇓	<b>Couche Application</b>	7	<b>Couche Application</b>	↑	
	⇓	<b>Couche Présentation</b>	6	<b>Couche Présentation</b>	↑	
	⇓	<b>Couche Session</b>	5	<b>Couche Session</b>	↑	
Transport des données	⇓	<b>Couche Transport</b>	4	<b>Couche Transport</b>	↑	
	⇓	<b>Couche Réseau (Network)</b>	3	<b>Couche Réseau (Network)</b>	↑	Paquet
	⇓	<b>Couche liaison de données (Data Link)</b>	2	<b>Couche liaison de données (Data Link)</b>	↑	Trame
	⇒	<b>Couche Physique (Physical)</b>	1	<b>Couche Physique (Physical)</b>	⇒	BIT

	<b>Support de communication</b>	
--	---------------------------------	--

- **Niveau 7**: couche application, gère le transfert des informations entre programmes.
- **Niveau 6**: couche présentation, s'occupe de la mise en forme des données, éventuellement de l'encryptage et de la compression des données, par exemple mise en forme des textes, images et vidéo.
- **Niveau 5**: la couche session, s'occupe de l'établissement, de la gestion et coordination des communications
- **Niveau 4**: la couche transport, gère la remise correcte des informations (gestion des erreurs), utilise notamment l'UDP et le TCP/IP
- **Niveau 3**: la couche réseau, détermine les routes de transport et s'occupe du traitement et du transfert de messages: gère IP et ICMP
- **Niveau 2**: la couche liaison de données, définit l'interface avec la carte réseau: hubs, switch, ...
- **Niveau 1**: la couche physique, gère les connexions matérielles, définit la façon dont les données sont converties en signaux numériques

A chacun de ces niveaux du modèle OSI, on encapsule un en-tête et une fin de trame (message) qui comporte les informations nécessaires en suivant les règles définies par le protocole utilisé. Ce protocole est le langage de communication pour le transfert des données (TCP/IP, NetBui, IPX sont les principaux) sur le réseau informatique. Sur le schéma ci-dessous, la partie qui est rajoutée à chaque niveau est la partie sur fond blanc. La partie sur fond grisé est celle obtenue après encapsulation du niveau précédent. La dernière trame, celle qu'on obtient après avoir encapsulé la couche physique, est celle qui sera envoyée sur le réseau.



**Le modèle OSI**

En hardware, nous ne nous intéressons qu'aux trois premiers niveaux du modèle OSI (jusqu'aux routeurs et switches de haut de gamme), éventuellement au niveau 4 pour les firewalls.

## 1.3. Le modèle TCP/IP

Le modèle TCP/IP est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre:

Protocoles utilisés	Modèle TCP/IP	Modèle OSI
	Couche application	Couche application
		Couche Présentation
		Couche session
TCP / UDP	Couche Transport	Couche transport
IP / ARP /ICMP / RARP / IGMP	Couche Internet (IP)	Couche réseau
	Couche Accès réseau	Couche Liaison de donnée
		Couche Physique

A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches:

Le paquet de données est appelé **message** au niveau de la couche application

Le message est ensuite encapsulé sous forme de **segment** dans la couche transport. Le message est donc découpé en morceau avant envoi.

Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme**

Enfin, on parle de **trame** au niveau de la couche accès réseau

Les **couches TCP/IP** sont plus générales que dans le modèle OSI

### 1.3.1. Couche application

La **Couche Application** englobe les applications standards du réseau:

**SMTP**: "Simple Mail Transport Protocol", gestion des mails

**TELNET**: protocole permettant de se connecter sur une machine distante (serveur) en tant qu'utilisateur

**FTP**: "File Transfert Protocol", protocole permettant d'échanger des fichiers via Internet et d'autres moins courants.

### 1.3.2. Couche transport

La **Couche transport** assure l'acheminement des données et les mécanismes permettant de connaître l'état de la transmission

Les protocoles des couches suivantes permettent d'envoyer des informations d'une machine à une autre. La couche transport permet d'identifier les applications qui communiquent. Pour faciliter la communication, on a défini non pas des noms d'applications, mais des **ports** de

communication (numéro variant de 0 à 65535,  $2^{16}$ ) spécifiques à chaque application.

La couche transport gère 2 protocoles de livraison des informations, indépendamment du type de réseau emprunté:

**TCP** assure le contrôle des données, orienté connexion (vérifie les envois de données par des signaux d'accusés de réception -acknowledge - du destinataire), il assure ainsi le contrôle des données

**UDP**, archaïque et non orienté connexion, n'assure aucun contrôle de transmission des données.

Ces 2 types (orienté connexion ou non) sont une notion utilisée pour les firewall. En effet, lorsque vous fermez un port en TCP, l'envoi d'un message ne renvoie pas de signal de retour (acknowledge), faisant croire que l'adresse IP n'est pas utilisée. Par contre, en UDP, le port fermé ne renvoyant pas d'informations fait croire que l'adresse IP est utilisée. En effet, l'UDP renvoie un message uniquement si le port est en erreur (ne répond pas)

### 1.3.3. Couche INTERNET

La **couche INTERNET** est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition / recombinaison des segments.

La couche Internet contient 5 protocoles (les 3 premiers sont les plus importants):

1. Le **protocole IP**: gère les destinations des messages, adresse du destinataire
2. Le **protocole ARP** (Adresse Resolution Protocol): gère les adresses des cartes réseaux. Chaque carte a sa propre adresse d'identification codée sur 48 bits.
3. Le **protocole ICMP** (Internet Control Message Protocol) gère les informations relatives aux erreurs de transmission. ICMP ne corrige pas les erreurs, mais signale aux autres couches que le message contient des erreurs.
4. Le **protocole RARP** (Reverse Address Resolution Protocol) gère l'adresse IP pour les équipements qui ne peuvent s'en procurer une par lecture d'information dans un fichier de configuration. En effet, lorsqu'un PC démarre, la configuration réseau lit l'adresse IP qu'elle va utiliser. Ceci n'est pas possible dans certains équipements qui ne possèdent pas de disques durs (terminaux essentiellement)
5. Le **protocole IGMP** (Internet Group Management Protocol) permet d'envoyer le même message à des machines faisant partie d'un groupe. Ce protocole permet également à ces machines de s'abonner ou de se désabonner d'un groupe. Ceci est utilisé par exemple dans la vidéo conférence à plusieurs machines, envoi de vidéos, ... La principale application HARDWARE de l'IGMP se retrouve dans les SWITCH managés. Ce protocole permet de regrouper des stations.

### 1.3.4. Couche Accès réseau

La **couche Accès réseau** spécifie la forme sous laquelle les données doivent être acheminées, quel que soit le type de réseau utilisé.

Elle prend en charge les notions suivantes:

- Acheminement des données sur la liaison
- Coordination de la transmission de données (synchronisation)
- Format des données



- Conversion des signaux (analogique/numérique) pour les modems RTC
- Contrôle des erreurs à l'arrivée

## 1.4. Les types d'ordinateurs connectés, types de réseaux

Un réseau permet de relier des ordinateurs quel que soit le type: PC, Mac, Main Frames (ordinateur central), ... entre eux pour partager des ressources.

On détermine deux types d'ordinateurs connectés sur le réseau: les **serveurs** et les **clients**. Les serveurs réseaux partagent leurs ressources (fichiers, périphériques de stockage, périphériques d'impression, ...). Les clients utilisent ces ressources partagées.

On distingue trois types de réseaux:

1 - Les réseaux "**Peer to Peer**" ou **point à point**. Dans ces petits réseaux, les ordinateurs connectés sont à la fois clients et serveurs. Un réseau Peer to Peer courant est constitué de PC sous Windows 95 /98 mis en réseaux. Ce terme est également utilisé par extension pour le partage de musiques et fichiers divers entre PC connectés sur INTERNET, un cauchemar pour les administrateurs réseaux et une excellente faille de sécurité pour les hackers.

2 - Les réseaux **dits lourds** utilisent un ordinateur central (appelé serveur) qui partage ses ressources. Dans ce cas, les niveaux d'accès des utilisateurs permettent de sécuriser les données. Les différents périphériques connectés sur ce serveur augmentent encore cette sécurité (backup, UPS, ...). La gestion se fait par un système d'exploitation spécifique de type "Serveur" comme par exemple Linux, Windows NT serveur, Windows 2000 - 2003 server ou Novell Netware.

3 - Les réseaux **Wan** (World Area Network) sont des réseaux internationaux permettant d'interconnecter des réseaux de type lourds. Internet est un réseau de ce type. Un réseau Wan n'est pas lié à la distance, mais bien au type d'interconnexion entre deux réseaux.

Les applications, les coûts et les difficultés de mise en oeuvre et gestion sont proportionnels. La sécurité est forcément proportionnelle.

Nous ne nous intéresserons pas trop à ces concepts. En effet, à part pour les connexions, les considérations Peer To Peer, serveurs ou Wan sont plus déterminés par le système d'exploitation et l'utilisation que par les machines.

. Win 95/98/me/ XP home/ XP Pro pour les Peer To Peer

. Win NT, 2000 (toutes versions), Windows 2003 serveur, linux ou Netware pour les réseaux lourds

. système Unix ou propriétaires (spécifique au fabricant) pour les autres, même si un Wan est de plus en plus configuré à l'aide de rassemblement de réseaux lourds. Internet ne fait pas exception à la règle.

## 1.5. Les applications réseaux.

Connecter des ordinateurs en réseau ne sert pas à grand chose sans des applications. L'utilisation d'un réseau permet:

- **Partage de fichier.** Selon le niveau de sécurité et d'administration centralisée souhaité, on peut opter soit pour un réseau Peer To Peer, soit pour un réseau lourd. Dans un réseau Peer To Peer, la sécurité et l'administration sont quasiment nulles mais l'installation est relativement facile et souple. De plus, il est plus facile d'effectuer une sauvegarde d'un seul ordinateur (le serveur) que sur tous les PC connectés. Les Peer to Peer ne sont donc utilisés que pour un nombre restreint d'ordinateurs.

- **Application centrale.** Dans des applications de gestion au sens large, on fait appel à un programme gérant une (ou plusieurs) bases de données. Ces logiciels nécessitent généralement un serveur lourd avec un système d'exploitation dédié. Ceci permet à plusieurs PC de travailler sur la même base de donnée simultanément à partir de PC différents (comptabilité, gestion de fabrication, facturation et gestion de stock,...). La sécurité se fait à deux niveaux: accès aux dossiers et limitations des droits d'accès dans le programme lui-même.

- **Partage de connexion Internet.** Il permet de connecter plusieurs ordinateurs simultanément sur Internet via une seule connexion. Le partage utilise les fonctionnalités de Windows (Win98se et supérieur), l'utilisation d'un routeur ou d'un logiciel spécifique pour des utilisations plus professionnelles.

- **Partage de périphériques.** Utiliser une imprimante par PC permet une souplesse d'utilisation mais l'utilisation simultanée d'une seule imprimante de grosse capacité s'avère rentable (plus rapide, prix de revient de l'impression inférieur).

Cette liste n'est pas exhaustive.

## 1.6. Les types de serveurs.

Dans le chapitre précédent, nous avons parlé de serveurs au sens large. Dans l'informatique, on distingue trois types de serveurs:

- Un **serveur de fichier** stocke et distribue les fichiers de programmes ou les données partageables par les utilisateurs du réseau local. Il résulte d'une combinaison de matériels et de logiciels qui peut être spécifique.
- Un **serveur d'application** permet d'exploiter une application (un programme) sur un serveur à partir de tous les clients. Ceci est typique aux applications basées sur des bases de données (gestion de fabrication, gestion commerciale, comptabilité, stock, ...). Elle permet par exemple de facturer, gérer les stocks,... à partir de plusieurs PC en même temps dans une gestion commerciale. Ces applications doivent être dédiées à ce mécanisme de partage. La configuration de ces serveurs est généralement nettement plus musclée (multiprocesseurs par exemple). Le programme doit être conçu comme application centralisée. En effet, un fichier (texte, tableau,...) ne peut être utilisé que par un programme (1 PC client dans notre cas) à la fois. Ceci pose des problèmes pour les sauvegardes lorsque le serveur travaille. Pour éviter les risques d'erreurs (modification du même enregistrement par 2 utilisateurs à la fois et corruption des données), le logiciel dédié va bloquer chaque enregistrement utilisé par une station. Pour rappel, dans les bases de données, l'enregistrement d'une modification se fait sans besoin d'utiliser la commande enregistrer du menu fichier. Par contre, si la base de donnée est utilisée, il est impossible de la

sauvegarder. La sécurité (contrôle d'accès, sauvegardes,...) est cependant facilitée car centralisée.

- Un **serveur d'imprimante** permet de partager des imprimantes connectées sur un seul PC. Certaines imprimantes réseaux peuvent être directement connectées sur le réseau sans passer par un PC, des boîtiers spécifiques peuvent également être utilisés.

Dans la pratique, un serveur rassemble souvent les trois applications. Les configurations (puissances) sont différentes pour chaque application, les serveurs d'applications sont les plus performants.

## 1.7. Caractéristiques d'un réseau.

Les réseaux locaux sont des infrastructures complexes et pas seulement des câbles entre stations de travail. Si l'on énumère la liste des composants d'un réseau local, on sera surpris d'en trouver une quantité plus grande que prévue:

- Le **câblage** constitue l'infrastructure physique, avec le choix entre paire téléphonique, câble coaxial et fibre optique. Ce choix détermine le type de concentrateurs (switch, HUB) du réseau. Ceux-ci constituent les nœuds internes dans le cas de réseaux en étoile. Dans ce cours, les liaisons hertziennes (sans fils) sont vues comme un câblage particulier.
- La **méthode d'accès** décrit la façon dont le réseau arbitre les communications des différentes stations sur le câble : ordre, temps de parole, organisation des messages. Elle dépend étroitement de la topologie et donc de l'organisation spatiale des stations les unes par rapport aux autres. La méthode d'accès est essentiellement matérialisée dans les cartes d'interfaces, qui connectent les stations au câble.
- Les **protocoles** de réseaux sont des logiciels qui "tournent" à la fois sur les différentes stations et leurs cartes d'interfaces réseaux. C'est le langage de communication. Pour que deux structures soient connectées sur le réseau, elles doivent "parler" le même protocole.
- Le **système d'exploitation** du serveur réseau (ou NOS pour Network Operating System), souvent nommé gestionnaire du réseau, est installé sur le ou les serveurs. Il gère les partages, droits d'accès,... Pour Microsoft, on retrouve Windows NT serveur, Windows 2000 serveur, Windows 2003 (.NET). Ce sont des versions spécifiques. Linux est utilisé sous différentes versions serveurs. Novell Netware est un système dédié principalement efficace comme serveur de fichiers.
- Le **système de sauvegarde** est un élément indispensable qui fonctionne de diverses manières soit en recopiant systématiquement tous les fichiers du ou des serveurs, soit en faisant des sauvegardes régulières, éventuellement automatisées.
- Un **pont**, un **routeur** ou **passerelle** constituent les moyens de communication qui permettent à un de ses utilisateurs de "sortir" du réseau local pour atteindre d'autres réseaux locaux ou des serveurs distants.
- Le **système de gestion et d'administration** du réseau envoie les alarmes en cas d'incidents, comptabilise le trafic, mémorise l'activité du réseau et aide le superviseur à prévoir l'évolution de son réseau. Cette partie est typiquement software.

## 1.8. Sécurité et administration.

Un des aspects importants d'un réseau informatique local est la centralisation de l'administration des données. Ceci permet de sauvegarder et sécuriser les données sur une seule machine, réduisant les pertes de temps liées à cet aspect rébarbatif mais obligatoire de l'informatique.

La sécurité rassemble un ensemble de mesures: intrusion et droits d'accès, virus, sauvegardes des données, continuité de l'application (pas d'arrêts),...

Il n'y a pas de solutions idéales pour la sécurité des réseaux (et pour la sécurité informatique en général). Trois solutions sont envisageables : les solutions matérielles que nous verrons, des solutions basées sur Linux et des solutions basées sur Windows ou des programmes rajoutés sur ces stations Windows. Le mélange de plusieurs solutions est possible dans certains cas. Certaines solutions sont d'ailleurs complémentaires. Sur un gros réseau "sensible", mettre un VPN hardware n'est pas suffisant. Une sécurité logicielle complémentaire incluant des contrôles d'accès au niveau administration serveur (serveur, dossier, droits d'accès) et logiciels de sécurité vérifiant le trafic sur le réseau interne n'est pas superflue.

- Les **routeurs** peuvent être remplacés par le logiciel WinGate ou par des applications spécifiques en Linux sur un PC dédié par exemple
- Les **serveurs proxy** sont parfois intégrés dans les routeurs (mais généralement sous Windows ou Linux)
- Les **firewall anti-intrusion** sont intégrés dans certains routeurs mais des logiciels assurent (presque) des fonctions équivalentes (ex.:Symantec, Zonealarm)
- Les **réseaux privés intégrés (VPN)** permettant un accès à un réseau lourd par Internet sont inclus dans certains systèmes d'exploitation ou logiciels.
- Les **anti-virus** sont généralement logiciels, mais parfois inclus dans les routeurs qui possèdent leur propre logiciel anti-virus. Ces appareils renvoient directement tous messages contenant un virus à son expéditeur.

Selon l'application, le concepteur - administrateur du réseau utilisera l'un ou l'autre ou une combinaison des deux. D'autres programmes de gestion réseaux (logiciels) permettent de gérer les trafics, les utilisateurs,... En clair, par hardware, vous pouvez bloquer l'accès complet à un serveur, par software, autoriser seulement une partie des ressources d'un serveur.

## 2. Base de transmission réseau

### 2.1. Introduction

Pour communiquer des informations entre ordinateurs et périphériques informatiques dans un réseau local, différents concepts sont nécessaires. Avant d'attaquer les liaisons réseaux, commençons pour le plaisir par une communication courante entre un ordinateur et une ... imprimante.

Dans une liaison parallèle, chacun des bits constituant un octet (byte) sont transférés en même temps. Cette liaison est constituée de 8 fils de données et de différents fils de masse, plus des signaux de communications. Intéressons-nous aux fils de données. Pour faire passer un octet de l'ordinateur vers l'imprimante, nous envoyons sur ces 8 fils une tension ou non suivant le message binaire à envoyer. Pour savoir si un message est envoyé, l'imprimante ne fait que regarder sur les 8 fils de données si une tension est présente ou non. Ceci ne nécessite pas en théorie de signaux de contrôle.

Quoique intéressantes, les liaisons parallèles sont supplantées par les liaisons séries. Ce remplacement est lié au prix des connexions physiques et à l'encombrement des fils. Si le cuivre n'est pas trop cher, l'installation par un électricien est nettement plus onéreuse et l'encombrement des fils des liaisons parallèles deviendrait rapidement ingérable.

Dans une liaison série, on ne retrouve au départ qu'un fil de communication (deux pour le bidirectionnel) et un fil de masse. En pratique, d'autres fils sont utilisés pour le contrôle des communications. Le principe est le même que ci-dessus, sauf que les 8 bits de données vont passer sur une seule ligne à tour de rôle. L'ordinateur envoie sur un fil spécialisé un signal électrique (tension) qui signale au récepteur un envoi de donnée et celui-ci se prépare à regarder ce qui se passe sur le câble. Si une tension est présente, le signal reçu est le 1, si aucun signal n'est présent, le signal reçu est 0. Les différents signaux sont envoyés à la suite de l'autre, ce qui explique que la liaison série est réputée lente.

Dès que l'on envoie un signal d'un endroit à un autre, les données doivent être contrôlées. Une solution serait de demander au récepteur de renvoyer les données reçues pour vérification. L'importance des vitesses de transfert rend ce principe impossible. Dans la pratique, on effectue un **contrôle de parité**. Pour calculer la parité, on compte le nombre de 1. Si ce nombre est pair, la parité est 0, s'il est impair, la parité est 1. Dans le cas d'une parité paire, EVEN (l'inverse dans une parité impaire, ODD). On envoie comme neuvième bit ce nombre paritaire. Cette vérification des données n'est pas totalement fiable. Si deux bits sont mauvais, la parité est juste, alors que le signal reçu est faux. Pour améliorer la sécurité de transmission, on augmente le nombre de bits de parités (liaisons spatiales). Ce système de parité est utilisé dans les modems, mais plus dans les systèmes réseaux.

Dans notre liaison parallèle ou série classique, seulement deux installations sont connectées entre elles. Cette connexion n'est pas très réaliste pour un réseau constitué d'ordinateurs. La connexion physique (les fils) doivent relier tous les ordinateurs entre eux. Chacun doit également prendre la parole à son tour pour éviter que plusieurs signaux soient présents en même temps. Ceci est régi par le type de réseau local.

Comment des ordinateurs de types différents peuvent-ils se comprendre lors de la transmission de données en réseau? Ce qu'on envoie comme suite de 0 et de 1 constituant le message s'appelle une trame. Elle est constituée des données et des entêtes et fin de messages ajoutées par les couches du modèle OSI ou Internet. Ces **trames** sont organisées de manières spécifiques selon un **protocole**.

Un **protocole** est la manière dont les informations sont envoyées vers le destinataire. Comme dans le **langage** humain, l'expéditeur doit utiliser le même langage (protocole) que le destinataire pour que l'échange d'information soit correct. Les protocoles réseaux les plus courants sont TCP/IP, IPX, NetBeui, ... Malgré cette courte description, les protocoles n'interviennent pas dans la partie hardware des réseaux (à part pour le routage). En effet, dans le **modèle OSI** du chapitre 1, nous nous limitons aux 3 premiers niveaux, alors que le protocole est lié au niveau 4: transport.

## 2.2. Le câblage Ethernet

Le câblage des réseaux locaux tend aujourd'hui à se banaliser, et à ne pas se distinguer du câblage informatique et téléphonique général de l'entreprise. Trois médias sont aujourd'hui utilisés dans les réseaux locaux.

### 2.2.1. La paire torsadée téléphonique

Peu chère, assez facile à poser, elle est aujourd'hui le support le plus répandu pour les réseaux locaux. Elle est souvent reprise sous le terme réseau Ethernet ou réseau RJ45

Le type de câble utilisé détermine la vitesse maximale de transmission des données, ainsi que le standard de connexion des réseaux. Dans le cas de la paire torsadée, on utilise du câble téléphonique. Néanmoins, ces câbles sont repris suivant leurs caractéristiques physiques (diamètre, isolant, longueur des torsades) dans différentes catégories ci-dessous:

Type de câble	Vitesse supportée	Type de réseau
Catégorie 1	Téléphonie	Téléphone
Catégorie 2	1 Mbps	Token-ring et téléphone
Catégorie 3	16 Mbps	Token-Ring et 10 base T
Catégorie 4	20 Mbps	10 Base T
Catégorie 5	100 Mbps	10BaseT et 100 Base TX
Catégorie 5e (catégorie 6)	1 Gbps	Giga Ethernet

Il existe 2 familles de câbles de paires torsadées.

Les câbles blindés (**STP**: Shilded Twisted Pair) sont entourés d'une feuille d'aluminium pour faire écran électrostatique.

Les câbles **UTP** (Unshielded twisted Pair) n'en possèdent pas. Les plus courants sont les UTP.

### 2.2.2. Le câble coaxial

Nettement plus cher, est en perte de vitesse après avoir été le support par excellence des premiers réseaux locaux qui fonctionnaient en mode large bande (bande passante découpée en plages de fréquence, chacune étant attribuée à un canal). Aujourd'hui, la plupart des réseaux locaux fonctionnant en bande de base (toutes les stations émettent sur un même canal occupant la totalité de la bande passante), le câble coaxial est presque uniquement utilisé pour l'interconnexion de différents réseaux locaux ou dans des environnements perturbés par des parasites électromagnétiques (moteurs électriques par exemple).



- La gaine permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (parfois en Chlorure de polyvinyle (PVC), éventuellement en téflon)
- Le blindage (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support des parasites (autrement appelé bruit) pouvant causer une distorsion des données.
- L'isolant entourant la partie centrale est constitué d'un matériau diélectrique permettant d'éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit).

L'âme, accomplissant la tâche de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.

### 2.2.3. La fibre optique

Encore plus chère, parce qu'elle permet des débits élevés et est insensible aux parasites, commence à faire une percée dans les réseaux locaux à gros besoins de bande passante (calcul technique, CAO), mais sert surtout pour interconnecter plusieurs réseaux locaux. La fibre optique est chère, fragile et fastidieuse à installer. Elle casse facilement sous l'effet de la torsion.

La fibre optique possède néanmoins de nombreux avantages :

- Légèreté
- Immunité au bruit
- Faible atténuation
- Tolère des débits de l'ordre de 100Mbps
- Largeur de bande de quelques dizaines de mégahertz à plusieurs gigahertz (fibre monomode)

Le **câblage optique** est particulièrement adapté à la liaison entre répartiteurs (liaison centrale entre plusieurs bâtiments, appelé backbone) car elle permet des connexions sur des longues distances (de quelques kilomètres à 60 km dans le cas de fibre monomode) sans nécessiter de mise à la masse. De plus ce type de câble est très sûr car il est difficile de mettre un tel câble sur écoute.

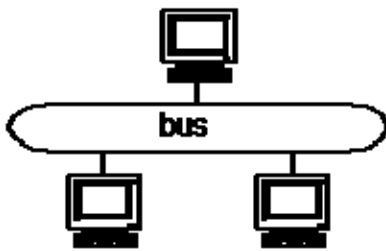


## 2.3. Les topologies réseau

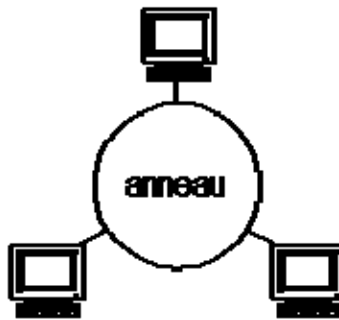
Dans le cas de notre liaison série ou parallèle standard, la communication se fait seulement entre 2 périphériques. Dans une connexion réseau, il ne suffit plus de connecter 2 appareils, mais bien plusieurs dans le sens large. Dans un réseau local, les appareils à relier sont connectés entre eux par un câble (nous verrons également plus tard des liaisons infrarouges ou hertziennes). Avant d'étudier les différentes formes de liaisons, voyons les type de raccordements, appelés topologie.

Il y a trois types de topologies principales:

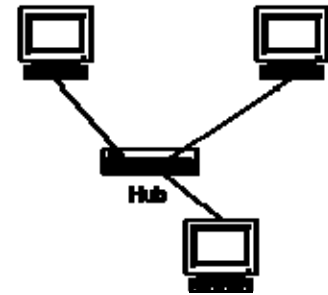
### Topologie en bus



### Topologie en anneau



### Topologie en étoile



## 2.4. Topologie réseau en bus

Le bus, un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinataire peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

L'avantage du bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est, de plus, très facile à mettre en place. Par contre, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles. Cette topologie est utilisée dans les réseaux Ethernet 10 Base 2 et 10 Base 5.

## 2.5. Topologie en anneau

Développée par IBM, cette architecture est principalement utilisée par les réseaux Token Ring. Token Ring utilise la technique d'accès par "jeton". Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite...

Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénéré par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable. L'interconnexion de plusieurs anneaux n'est pas facile à mettre en œuvre. Enfin, cette architecture étant la propriété d'IBM, les prix sont élevés et la concurrence quasiment inexistante. Cette topologie est utilisée par les réseaux Token Ring et FDDI.

Remarque: depuis 2000, IBM ne développe plus de circuits intégrés pour ce type de bus.



## 2.6. Topologie en étoile.

C'est la topologie réseau la plus courante, notamment avec les réseaux Ethernet RJ45. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le **concentrateur**, celui-ci envoie les données à toutes les autres machines (**hub**) ou uniquement au destinataire (**switch**).

Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies.

Cette topologie est utilisée par les réseaux Ethernet 10, 100 Base T et suivants.

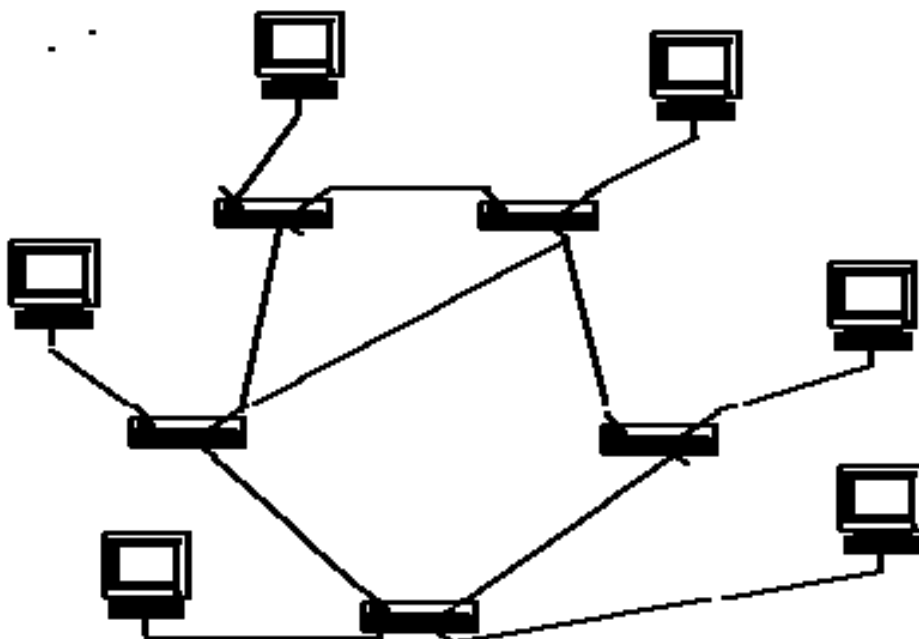
## 2.7. Topologie mixte.

Une topologie comme ci-dessus est malheureusement trop simpliste dans le cas de réseaux importants. Si une topologie en étoile est parfaite dans le cas d'un réseau limité géographiquement, un réseau mondial ne peut utiliser une liaison de ce type. La méthode utilisée est donc de relier des réseaux en étoile (par bâtiments par exemple) via des liaisons en bus (téléphoniques par exemple).

Dans la suite du cours, en nous intéressant aux connexions inter réseaux, nous reverrons ce type de réseau mixte, en sachant que chaque partie du réseau est généralement en étoile.

## 2.8. Topologie maillée.

Les réseaux maillés (ici représentés par des ordinateurs) sont reliés par des routeurs qui choisissent la meilleure voie suivant plusieurs possibles. INTERNET est une topologie maillée, ceci garantit le mieux la stabilité en cas de panne d'un noeud mais est difficile à mettre en oeuvre, principalement au niveau du choix des routes à suivre pour transférer l'information. Ceci nécessite l'utilisation de **routeurs** intelligents.



Cette topologie ne peut pas être utilisée dans les réseaux internes Ethernet.

## 2.9. Méthode d'accès

Pour "mettre de l'ordre" dans un réseau local, où tous les ordinateurs peuvent prendre l'initiative des envois de messages, il faut une règle respectée par tout le monde. C'est la méthode d'accès. On distingue deux méthodes principales, la contention et le jeton. Elles distinguent les deux principales famille de réseaux locaux : Ethernet, qui utilise la contention, et l'anneau à jeton (Token-Ring d'IBM), méthode "déterministe" (non aléatoire).

Les deux méthodes sont normalisées par l'**IEEE** (comité 802), normalisation reprise dans le cadre de l'ISO. Si l'on se réfère au modèle OSI, ce qui distingue les méthodes d'accès se situe bien entendu dans la couche 1 (couche Physique) du modèle OSI, puisque les câblages et les topologies sont différents, mais surtout dans une sous-couche inférieure de la couche 2 du modèle OSI (Liaison de données) appelée Mac (Medium Access Control). La méthode Ethernet **CSMA/CD** (Carrier Sense Multiple Access With collision Detection) est normalisée sous l'appellation 802.3 et l'anneau à jeton sous 802.5.

Dans la méthode Ethernet, utilisant la contention, chaque ordinateur envoie son message sans trop s'occuper de ce qui se passe sur le câble. Si une station émet pendant qu'une autre est en train d'émettre, ceci provoque ainsi une collision. La deuxième station émettrice stoppe la transmission pour recommencer plus tard. Dans le cas du Giga Ethernet, les stations n'envoient plus le message, mais un signal de départ pour vérifier si la voie est libre. Le CSMA/CD (Carrier Sense Multiple Acces with Collision Detection) se charge de la détection des collisions.

Dans la méthode à jeton, chaque station peut communiquer à son tour. Si 3 stations sont connectées en anneau, la station 1 prend la parole, ensuite la 2, puis la 3. La station 1 peut de nouveau prendre la parole, et ainsi de suite.

## 3. Réseaux Ethernet.

### 3.1. Introduction

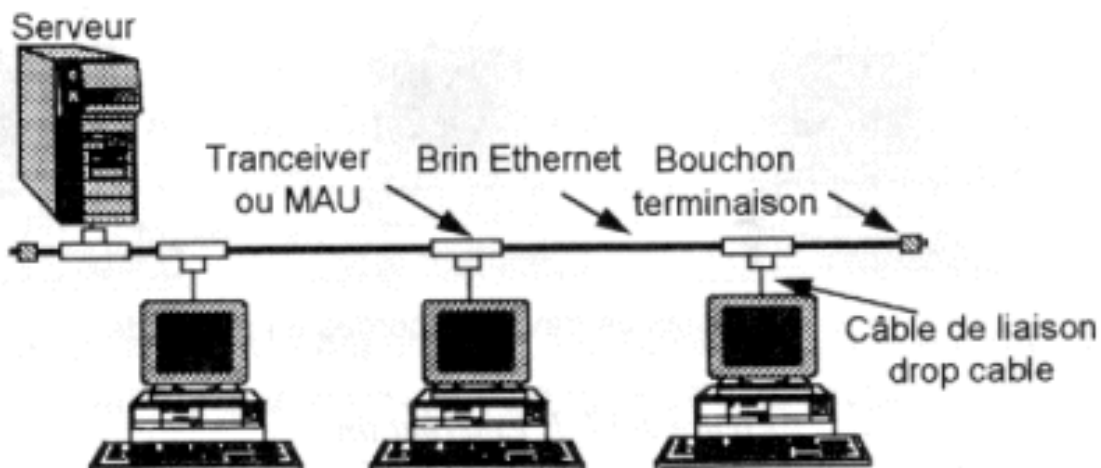
La connexion entre ordinateurs nécessite une carte réseau implantée dans chaque PC (aussi appelées **NIC, Network Interface Card**). Les cartes réseau local les plus courantes sont de type Ethernet. Ce chapitre rassemble tous les types de connexion Ethernet et le câblage (fabrication, précaution,...) des fils de raccordement

Le réseau local Ethernet est apparu à la fin des années 70 aux Etats-Unis. Il est né des expériences complémentaires de DEC, Intel et Xerox, bien avant les avancées de la normalisation. Ceci implique que l'essentiel des couches supérieures du **modèle OSI** n'est pas spécifié.

Tous les PC peuvent communiquer sur le câble réseau informatique en même temps. Il faut donc une règle dans le cas où deux stations se mettraient à communiquer au même moment. La méthode utilisée est la **contention**. La principale méthode de contention en réseaux locaux est le **CSMA/CD** (Carrier Sense Multiple Access), avec détection de collision (CD). C'est celle des réseaux Ethernet. Elle consiste pour une station, au moment où elle émet, à écouter si une autre station n'est pas aussi en train d'émettre. Si c'est le cas, la station cesse d'émettre et réémet son message au bout d'un délai fixe. Cette méthode est **aléatoire**, en ce sens qu'on ne peut prévoir le temps nécessaire à un message pour être émis, transmis et reçu. Voyons l'évolution des réseaux Ethernet.

### 3.2. Ethernet, IEEE 802.3 10 Base 5 et IEEE 802.3 10 Base 2

La version 10 Base 5 (10Mbps en bande de base sur câble coaxial d'une longueur maximale par segment de 500 mètres) est la version d'origine d'Ethernet, elle est représentée ci-dessous :

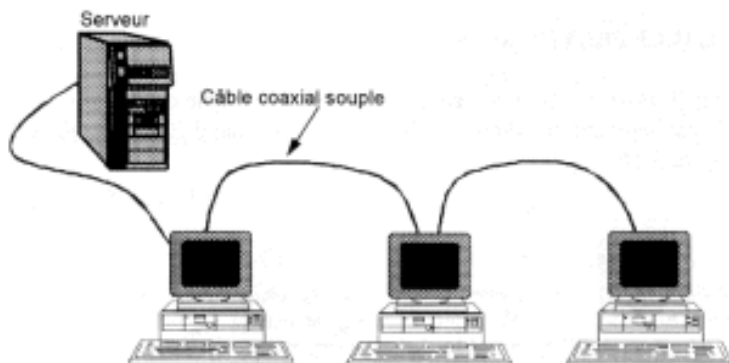


Chaque station est équipée d'une interface réseau " Ethernet " qui assure l'adaptation physique et gère l'algorithme **CSMA/CD**. Comme dans toutes les connexions coaxiales, les 2 extrémités du câble sont raccordées à un bouchon (résistance de terminaison), une résistance spécifique qui atténue les réverbérations du signal sur le câble. Le drop câble est constitué de paires torsadées, longueur maximale de 50 mètres. Le câble coaxial est un câble épais de couleur jaune

d'un demi-pouce de diamètre de type BELDEN 9580. La longueur totale du réseau peut atteindre 2,5 kilomètres avec 100 points de connexion.

Le 10 base 5 n'est pratiquement plus utilisée que dans les environnements perturbés (rayonnement électromagnétique) ou pour garantir la confidentialité des échanges (pas de rayonnement du câble coaxial).

Une version économique (IEEE 802.3 10 base 2) utilise du câble coaxial fin (Thin Ethernet).

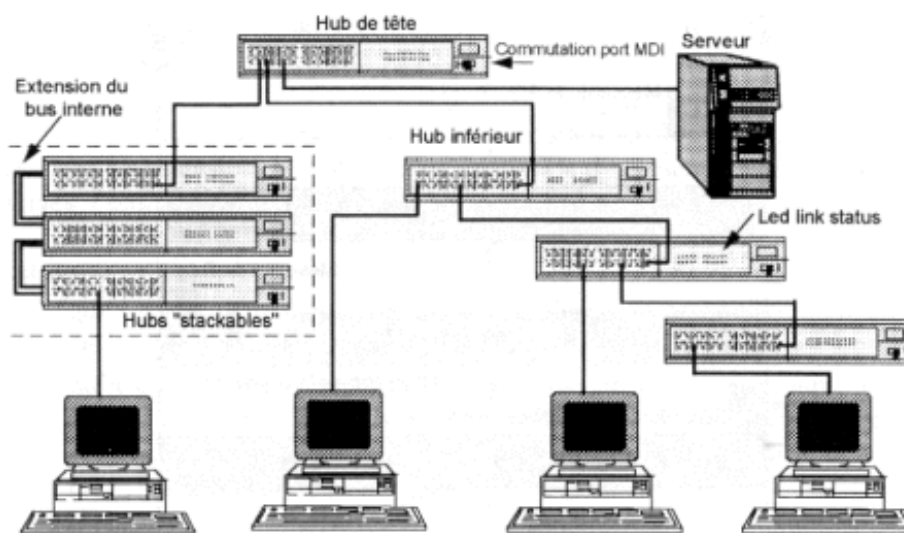


Cette architecture physique de réseau peut être utilisée pour des petits réseaux 2 ou 3 PC. Chaque carte est reliée au câble via un connecteur en T de type BNC. Les 2 extrémités du réseau sont fermées par une résistance de terminaison (**bouchon**) de 50 ohms. Cette terminaison n'est pas obligatoire, mais la vitesse de transmission est nettement réduite puisque cette résistance élimine les "réverbérations sur le câble": le signal transmis revient sur le câble et les stations croyant à un signal véritable attendent que la ligne soit libre.

La longueur maximum du réseau est de 185 mètres, avec un maximum de 30 équipements connectés. La distance minimale entre 2 connexions est de 50 centimètres. Ce câblage est souvent utilisé pour connecter "la petite station en fond d'usine".

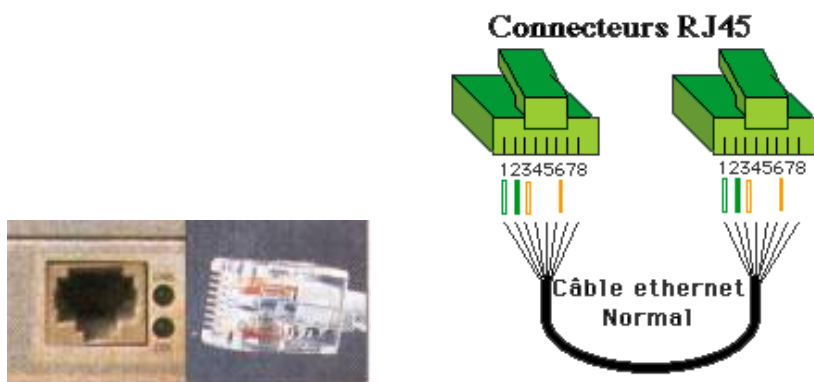
### 3.3. Réseau Ethernet, IEEE 802.3 10 Base T

AT&T a imaginé de réutiliser le **câblage téléphonique** préexistant dans les immeubles de bureaux pour la réalisation du réseau. Cela imposait deux contraintes : l'une de débit, l'autre de distance. Ce réseau Ethernet fonctionnait à 1Mbps, stations connectées sur des concentrateurs en étoile via des répéteurs (**hub**) et la distance entre le hub et une station était limitée à 250 mètres. Cette architecture (802.3 1 base 5 ou Starlan) complètement obsolète a évolué vers une version 10Mbps (**802.3 10 base T**). La figure suivante présente le réseau 10 base T.



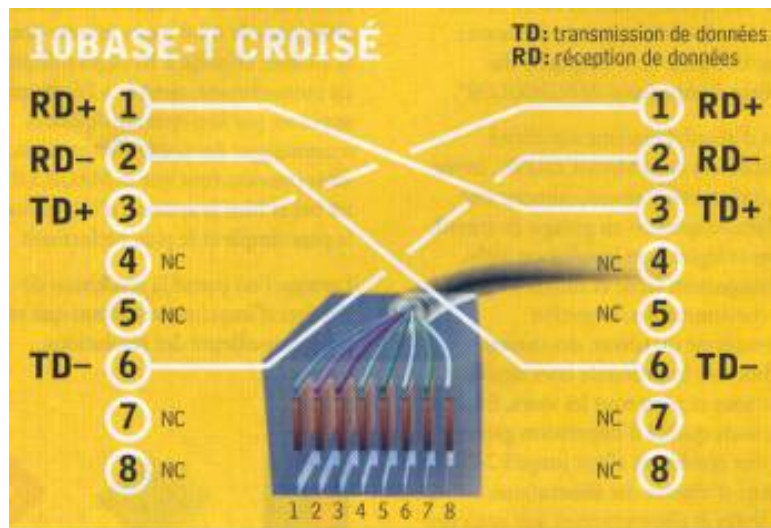
L'Ethernet 10 base T utilise un câblage par paire téléphonique (2 paires soit 4 fils). Sa vitesse maximum est de 10 Mbps (méga bit par seconde). Le câblage est de type étoile. Les noeuds sont constitués de concentrateurs (**hub, switch, routeur**). Cette solution est actuellement la plus répandue, mais si la norme a évolué en vitesse.

Le câblage sous RJ45 en 10Base-T nécessite 4 fils (pour 8 accessibles dans le connecteur). Les fils sont vendus tout fait dans le commerce, mais on peut facilement fabriquer les câbles RJ45. Généralement, on insère les 8 fils mais ce n'est pas obligatoire, notamment si vous souhaitez utiliser un câble pour 2 stations.



Connecteur et prise carte réseau Câble RJ45 droit en 10 Base T et 100 base T  
(pas en full duplex)

Si on n'utilise pas de concentrateur (connexion de 2 stations) ou pour connecter 2 concentrateurs entre eux, les fils doivent être de type câble croisé comme ci-dessous. Vous devez respecter les polarités et les paires doivent être appariées.

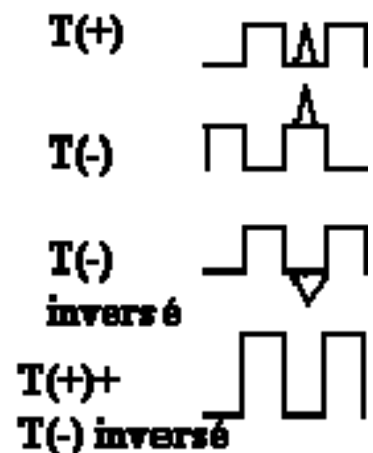


### Pourquoi respecter le câblage par paires.

Le signal au départ de la carte réseau est envoyé sur la forme T+ et sur la forme T- (signal inversé).

Supposons un parasite qui apparaît sur le câble pendant la transmission du signal. Il est de même sens sur les 2 fils. Comme une paire est torsadée, les perturbations électriques liées à des courants induits seront généralement différentes d'une paire à l'autre. Pour rappel, le passage d'un courant électrique dans un fil produit un champ électromagnétique dans son entourage et de ce fait induit un courant dans les fils électriques proches.

Invertissons T(-). Le signal et le parasite sont inversés. En additionnant T(+) et T(-) inversé, le signal double mais le parasite est supprimé.

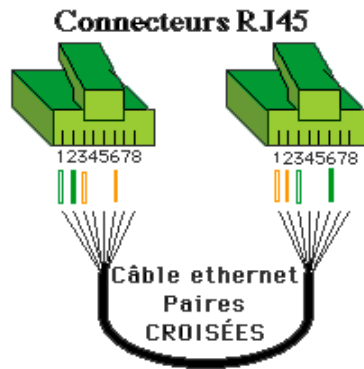


### Matériel nécessaire pour un câblage RJ45:

- Du câble 4 paires torsadées catégorie 5
- Des connecteurs RJ45 à sertir catégorie 5
- Des manchons caoutchouc, pour éviter de sectionner le câble.
- Une pince à sertir et si la pince ne l'inclut pas: une pince coupante et une pince à dénuder.
- 

### Procédure à suivre :

- Enfiler le manchon sur le câble.
- Dénuder la gaine extérieure sur environ 15 mm.
- Pour le cordon croisé, trier les fils selon le schéma ci-dessous.



### Câble RJ45 croisé (10 base T et 100 base T)

- Maintenir les fils en place en respectant les paires et bien les couper en ligne. Il doit rester environ 13mm, l'extrémité ne doit pas former un arc de cercle.
- Placer les fils dans le connecteur en appuyant sur l'ensemble du fil pour que les paires rentrent jusqu'au fond du connecteur.
- Sertir le connecteur.
- Enficher le manchon.

Vérifiez, par transparence, le bon état de votre montage, si les fils arrivent bien en bout de connecteur.

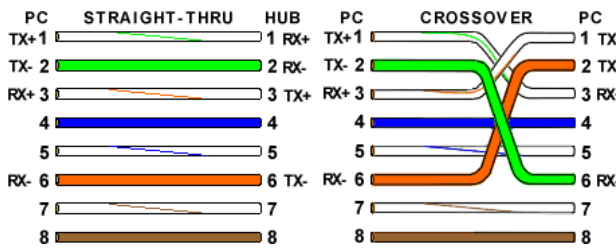
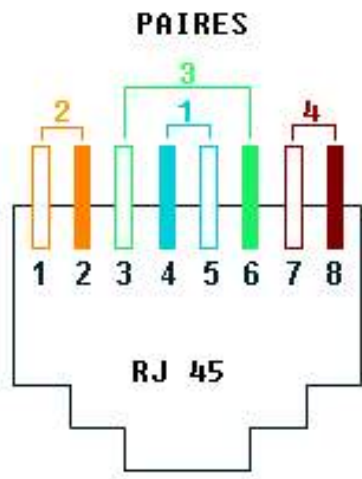
### 3.4. Ethernet 100 Base TX et 100 Base T4, Fast Ethernet

Sorti en 1992, la norme 100 base T a un débit théorique est de 100 Mbps. Le fast ethernet oblige également à utiliser des concentrateurs de type hub ou switch.

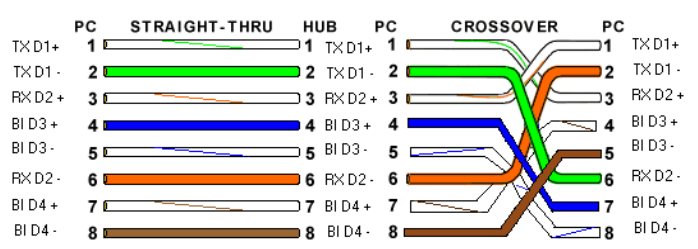
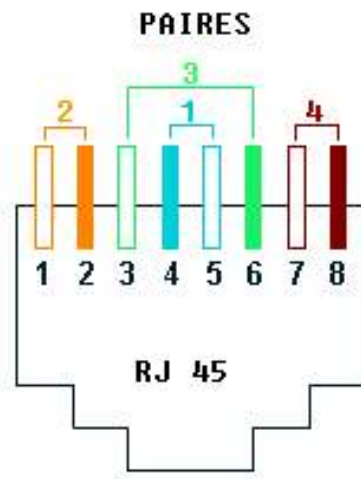
On retrouve 2 catégorie de 100 Base T: le **100 Base T4** et le **100 Base TX**. Le 100 Base TX (le plus répandu) utilise les mêmes 2 paires que le 10 Base T. Par contre, le 100 Base T4 utilise les 4 paires. Néanmoins, le 100 base T4 (quasiment plus utilisé) utilise 3 paires simultanément pour l'émission et la réception. Ce mode ne peut donc pas utiliser le **Full Duplex** (communication bidirectionnelle simultanée).

En 100 base TX, le câblage est le même que en Ethernet base 10, seul le câble doit être de meilleure qualité (catégorie 5) et les 4 fils doivent être connectés suivant les couleurs ci-dessous, même si chaque "câbleur" utilise souvent son propre code de couleurs. Les câbles croisés utilisent les deux mêmes croisements qu'en 10 base T.

## Câble normal et croisé 100 Base TX



## Câble normal et croisé 100 Base T4





### 3.5. Gigabit Ethernet.

Si au départ, le gigabit utilisait une connexion en fibre optique, elle est remplacée par une connexion de type RJ45 de classe 5e (avec une limitation de distance limitée à 100 mètres). Le gigabit utilise le même format de trames de données que le 10 Base –T et le 100 Base TX et le même protocole anticollision, le **CSMA-CD**. Cette norme permet à chaque ordinateur de signaler qu'il va transmettre un message avant d'émettre les données sur le réseau (ce qui évite les collisions).

**Tableau comparatif des vitesses. Le 1000 base T est le plus courant**

Nomenclature	Speed	Distance	Media
10BASE-T	10 Mbps	100m	Cuivre
100BASE-TX	100 Mbps	100m	Cuivre
100BASE-FX	100 Mbps	412 m 2 Km	half Duplex Multi-mode Fibre optique Full Duplex multi-mode Fibre optique
<b>1000 Base LX</b>	1000 Mbps 1000 Mbps	3 Km 550m	Single-mode Fibre optique (SMF) Multi-mode Fibre optique (MMF)
<b>1000 Base SX</b>	1000 Mbps 1000 Mbps	550m 275m	Multi-mode Fibre optique (50u) Multi-mode Fibre optique (62.5 u)
<b>1000 Base C</b> (pas supportée par les applications industrielles standards)	1000 Mbps	25m	Cuivre, 4 paires UTP5
<b>1000 Base T - 1000 Base TX IEEE 802.3 ab</b> ratifié le 26 juin 1999,	1000 Mbps	100m	Cuivre, câble catégorie 5, transmission sur 4 paires (250 Mbits/paire)
1000 BASE LH	1000 Mbps	70 km	Fibre optique

Le câblage sur paires torsadées des 1000 C et 1000 TX est identique à celui du 100 Base T4, y compris pour les câbles Ethernet RJ45 croisés.

### 3.6. Carte réseau Ethernet

On retrouve dans les PC trois types de cartes réseaux: 10, 100 et Giga Ethernet. Les premières cartes base 10 de 3Com utilisaient uniquement les connecteurs coaxial et un connecteur spécifique. Les anciennes cartes 10 MB se connectent en coaxial et en RJ45. Par contre, les cartes base 100 n'utilisent plus que le RJ45.

Dès lors, l'utilisation d'un réseau en coaxial oblige l'utilisation d'une carte base 10. Comme l'utilisation d'un câble RJ45 nécessite l'utilisation d'un concentrateur, celui-ci et les cartes reliées doivent utiliser les mêmes paramètres soit du 10 MBb/s. Les concentrateurs 10 incluent généralement (mais pas chaque fois) un connecteur coaxial et le nombre spécifique au concentrateur de câblage RJ45. Les concentrateurs 100 permettent les liaisons à 100 Mb, ils détectent également des cartes 10 Mb.

Les cartes réseaux sont également caractérisées par le bus interne utilisé: ISA et PCI. Il y a des parfois incompatibilités entre les cartes PCI 3.3V et carte mère en 5V (anciens Pentium). Comme toutes cartes PC, elles sont caractérisées par une adresse et une interruption pour qu'elles soient reconnues par le PC. Certaines cartes incluent un socket permettant d'insérer une Eprom pour démarrer le PC via le réseau (sans disque dur), solution peu utilisée.

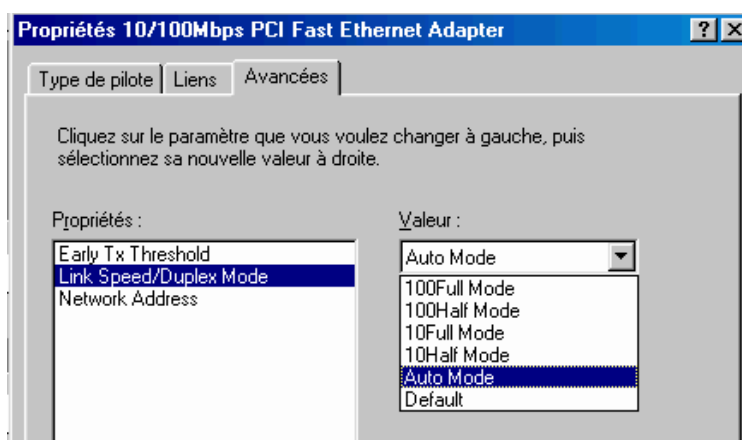
Chaque carte réseau Ethernet en RJ45 inclut 2 LED. La première, généralement verte, signale que la carte est reliée sur un concentrateur via un câble. La deuxième, orange ou verte, signale la transmission / réception de données. Les cartes réseau actuelles commutent automatiquement sur chaque vitesse Ethernet (10 ou 100).

A de très rares exceptions (hub et switch de bas de gamme), **avec une carte en connectée en RJ45 sur un concentrateur, la (les) LED doit s'allumer sur la carte et sur le HUB, Switch, Routeur. Sinon**, cela signifie que **l'accès réseau est mal paramétré**, c'est du ressort des administrateurs réseaux, sauf si la vitesse de connexion est faible.

### 3.7. Half Duplex et Full Duplex.

Une carte réseau Ethernet peut être de type Half Duplex et Full duplex. Les cartes Half Duplex (normales) ne peuvent émettre et recevoir en même temps. Par contre, les cartes Full Duplex (et les switch associés) peuvent émettre et recevoir en même temps sur des canaux (câbles) différents. Cette solution permet de doubler le taux de transfert sur le réseau Ethernet. Par exemple, une carte 100 base TX (le 100 base T4 n'autorise pas le Full duplex) va autoriser un taux de transfert de 200 Mbps pour 100 dans le cas half duplex.

S'il est nécessaire de ralentir le réseau (passer en 100 Half mode ou même en cas de perturbations réseau d'obliger la carte 100 Base TX à travailler en 10 base T). Le paramétrage se fait dans les paramètres réseaux en utilisant les propriétés de la carte réseau. Voici par exemple le cas d'une carte à base du circuit Realtec RTL8139D (10base T et 100 base TX automatique).



### 3.8. Câblage RJ45 Ethernet, règles, problèmes de liaisons et appareils de tests

Les câbles RJ45 peuvent être achetés tout fait. Néanmoins, dans des câblages professionnels, ils sont intégrés dans des goulottes, passent à travers des murs,... La solution consiste à acheter une pince, les connecteurs (avec les protections), le câble et de respecter strictement les couleurs de câblage RJ45 ci-dessus.

Connecter deux structures entre elles par des câbles amène toujours différents types de problèmes.

La première reste les conditions maximales d'exploitation. Il est tentant de mettre un fil plus long que celui prévu par la norme entre un **Hub** (ou un **switch**) et un PC (100 mètres pour un T base 10 ou 100). **Première erreur.**

Si le câble est acheté tout fait, la connexion est généralement bonne. Ceci est valable pour les petits réseaux internes mais c'est rarement le cas pour les réseaux industriels. Comme un testeur de câblage réseau vaut facilement le prix d'une petite voiture sportive, mieux vaut câbler correctement **d'avance.**

Chaque connexion est limitée par le nombre de HUBS en cascade. Pour une connexion 10 base T, le nombre maximum entre 2 stations est de 4. Par contre, elle est de 2 en 100 base T

En dernier, le câble RJ45 doit être correctement posé. Parmi les problèmes rencontrés, on trouve:

- câble réseau coupé ou égratigné ou plié.
- plus sournois: le câble passe à coté de câbles électriques qui perturbent le signal, à côté de tubes fluorescents ou néon (minimum 50 cm). Proximité de moteurs électriques de fortes puissances. Le tableau ci-dessous reprend les distances minimum entre les câbles réseaux et les câbles électriques en fonction de la distance.

**Ecartement entre les câbles courant fort (réseau électrique, néon) et courant faible (réseau ethernet)**

Ecartement en cm									
30 cm									
20 cm									
10 cm									
5 cm									
		10 m		20 m		30 m			80 m
	<b>Cheminement parallèle en mètres</b>								

Pour un câble RJ45 de faible longueur, on pourrait mettre les câbles électriques et réseaux dans les mêmes goulottes. Ceci serait oublier les normes de sécurité électriques qui interdisent d'insérer des câbles électriques et téléphoniques (basse tension) dans les mêmes goulottes, même si c'est courant dans les faux-plafonds en industries.

On trouve sur le marché différents types d'**appareils de tests** des câbles réseaux.

Le **premier type** d'appareil de test fonctionne comme un ohmmètre sur 8 lignes. Il est important que l'appareil puisse se scinder en deux parties (une partie de contrôle et un boîtier de terminaison) pour permettre le tests de câbles posés. Ces appareils permettent généralement de détecter les câbles droits et les câbles croisés ainsi que d'autres connecteurs (RJ11, RJ45, USB,...). Ces appareils ne sont fiables que jusqu'à un certain point. Ils vérifient uniquement si la connexion est correcte, pas si la liaison est correcte. Si l'appareil détecte une erreur de câblage, le fils est à recommencer. S'il ne détecte pas d'erreur, cela ne signifie pas forcément que le câble est bon. Un mauvais contact sera souvent considéré comme bon par le testeur, mais pas de connexion réseau.



Ici, un test de câble croisé. La partie gauche reprend le module de commande, la partie droite, la terminaison détachable. Les 8 Led au-dessus indique si les fils individuellement sont corrects. La partie gauche donne des indications sur les connexions.

SHORT (câble coupé ou mauvaise connexion sur au moins un fil).

CONNECTED que le câble est droit.

NON-PARALLEL que le câble est croisé.

NO CONNECTION que le câble n'est pas inséré.

Le prix varie de 100 à 150 €.

Le **deuxième type** fonctionne à la manière d'une carte réseau. Ces appareils testent la ligne (et pas uniquement les fils. l'appareil se connecte au bout d'un câble et teste la liaison sur un HUB ou un switch. Dans ce sens, ils sont plus efficaces. Ils sont un peu plus onéreux.

Le **troisième type** de testeur réseau ressemble à un mini-ordinateur. Le prix revient facilement à 10.000 €, pas à la portée de tout le monde. La méthode de test est identique à celle des premiers appareils. Ils offrent les mêmes possibilités que les appareils du premier groupe mais permettent en plus:

1. les tests effectifs des faux contacts ou des coupures sur chaque câble.
2. la longueur du câble
3. en cas de coupure d'un fils (ou de plusieurs), la distance à laquelle il est coupé.
4. différentes perturbations qui transitent sur le câble (perturbations électriques).

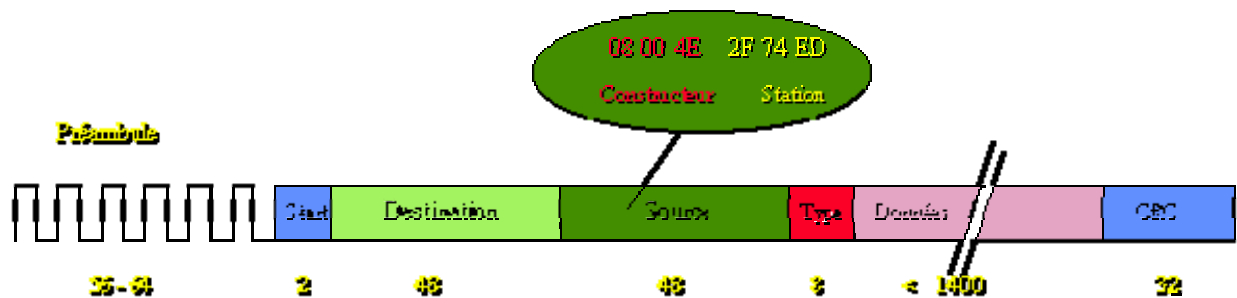
### 3.9. Adresse MAC

Chaque carte réseau se distingue par une adresse MAC. Cette adresse est unique pour toutes les cartes réseaux dans le monde. Elle est constituée de 6 octets de type XX.XX.XX.XX.XX.XX ou chaque XX varie de 0 à 255. L'adresse est souvent donnée sous forme hexadécimale. Par exemple 4D.FF.56.D2.AF.26.

Dans Démarre -> exécuter, tapez la commande **WINIPCFG** (présent dans le répertoire windows sous windows 98) ou **ipconfig / all** dans une fenêtre DOS (Windows 2000 et XP) pour la déterminer suivant votre carte réseau.

L'adresse Mac FF.FF.FF.FF.FF.FF est particulière, les données sont envoyées à l'ensemble du réseau. C'est l'adresse de **Broadcast**.

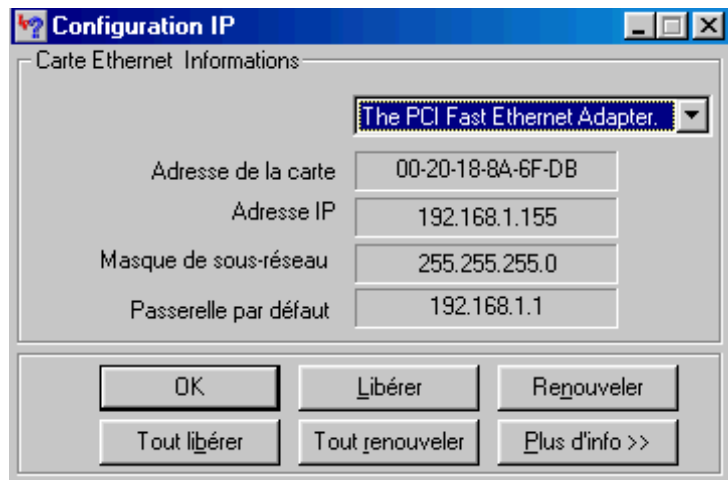
Le protocole Ethernet utilise cette adresse MAC pour faire communiquer des équipements entre eux via un réseau. Quand une machine veut parler à une autre, elle envoie un paquet sur le réseau, contenant l'adresse MAC destination, l'adresse MAC source, la longueur du paquet, les données et le CRC (Cyclic Redundancy Checking), un contrôle d'erreur,...



- Chaque trame Ethernet débute par un *Préambule* qui a pour but de synchroniser les récepteurs des appareils connectés et d'effectuer le test de collision
- La fin du préambule est identifiée par deux bits à "1" appelé *Start*
- Suivent les adresses de *Destination* et de *Source* codées sur 48 bits et attribuées par licence de Xerox. On obtient ainsi une adresse unique au monde (48 bits = plus de 140 trillion d'adresses!). L'adresse contient le code du constructeur de l'adaptateur Ethernet, qui est écrit dans une ROM
- Après la *Source*, le *Type* qui donne sur 8 bits le protocole utilisé dans les données (802.3)
- Les *Données* contiennent en plus l'adresse propre au protocole choisis (Ex: Adresse IP)
- Le CRC Circle Redundant Check qui est le OU exclusif des tranches de 32 bits calculé de l'adresse de destination à la fin des données. Ce même calcul sera effectué par la carte réseau du récepteur pour valider le paquet

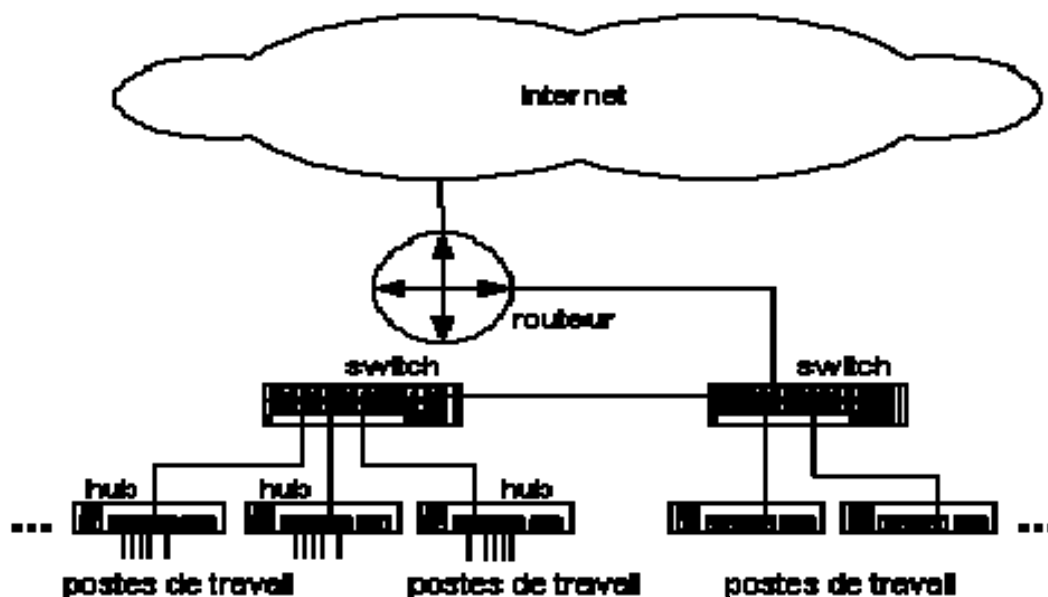
Le temps entre deux paquets *Interframe Spacing* ne doit pas être inférieur à 9.6 µS

L'adresse MAC est prioritaire sur l'adresse IP. Lorsqu'une communication réseau a été établie sous Ethernet, la commande DOS *arp -a* permet de retrouver l'adresse MAC des autres PC du réseau.



## 4. Hub, switch, routeur réseaux

### 4.1. Introduction



Le chapitre précédent nous a permis d'étudier les types de réseaux Ethernet. 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). Les concentrateurs Ethernet rassemblent les hubs, les switches, 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'interconnexion de réseaux.

### 4.2. Hub (répétiteur)

Les **Hubs** sont utilisés en Ethernet **base 10** et **base 100**. Le Hub est le concentrateur le plus simple. Ce n'est pratiquement qu'un répéteur (c'est son nom en Français). Il amplifie le signal réseau pour pouvoir le renvoyer vers tous les 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 pas utiliser des HUB: dès qu'un PC communique, tous les ordinateurs l'entendent et quand chacun commence à transmettre, les vitesses de transmissions chutent. 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 coaxiale. Par connexion, on retrouve une led signalant la connexion à une carte et une led de collision par canal ou pour tous les ports.

**Hubs base 100:** nombre de connexion suivant le modèle, port inverseur, pas de connexion coaxiale. 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)

Selon la norme, le **nombre maximum de HUB en cascade** (raccordés port à port, 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 switches qui enregistrent les trames avant de les envoyer.

## 4.3. Switch (commutateur)

### 4.3.1. Introduction

En recevant une information, un switch décode l'entête pour connaître le destinataire et ne l'envoie uniquement que vers le port Ethernet associé. Ceci réduit le trafic sur le câblage réseau par rapport à un HUB. A la différence, les informations circulent toutes sur tout le câblage avec les hubs et donc vers toutes les stations connectées. Les switches travaillent sur le niveau 1, 2 et 3 du **modèle OSI**, pour seulement les couches 1 et 2 dans le cas du HUB. Le niveau 3 du modèle OSI détermine les routes de transport. Les switches remplacent de plus en plus les Hubs. Les prix deviennent pratiquement équivalents.

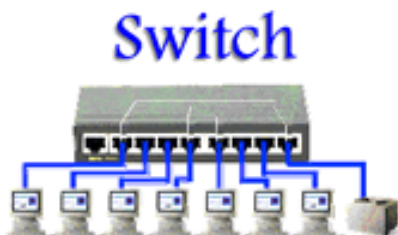
La majorité des switches peuvent utiliser le **mode Full duplex**. La communication est alors bidirectionnelle, doublant le taux de transfert maximum. Cette fonction n'est jamais implantée dans les Hubs. Le Switch vérifie automatiquement si le périphérique connecté est compatible full ou half duplex. Cette fonction est souvent reprise sous le terme "**Auto Negotiation**".

Les modèles 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 Hubs, 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 switches 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 switches en cascade sur un réseau.

### 4.3.2. Fonctionnement d'un switch.



Au démarrage, un switch va construire une table de correspondance adresse MAC - numéro de port de connexion. Cette table est enregistrée dans une mémoire interne des switches. 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 switches 5 ports, elle varie de 512 à 1000 entrées. Ceci ne pose pas de problèmes pour un petit réseau interne 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 réseau est connectée sur un de ses ports, il va adapter sa 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) va être utilisé. D'autres PC pourront communiquer en même temps sur les autres ports.

Dans le cas où le réseau utilise 2 switches. Le PC1 envoie le message avec l'adresse de destination sur le switch1 sur lequel il est raccordé. Celui-ci va vérifier dans sa table si l'adresse de destination est physiquement raccordée sur un de ses ports. 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 l'ordinateur 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 Ethernet associé. 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 certain 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 Switchs 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 switches de bas de gamme avec 1 faible nombre de ports pose de gros problèmes dans les réseaux. Ceci implique que pour l'utilisation de petits switches (4-8 ports), le nombre de switches reliés entre eux pour une connexion entre 2 PC est limité. J'ai déjà eu 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 réduire le nombre de concentrateurs pour les remplacer par 1 ou 2 switches de plus grosse capacité.

### 4.3.3. Types de switches

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

**Store and Forward** ; plus courant, 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 divers médias de liaison (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 switches 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 pour chaque port réseau. 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 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 switches sont uniquement utilisés dans des environnements composés de liaisons point à point (clients - serveur). On exclut toute application mixte 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'envoiera 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.

#### 4.3.4. Particularités supplémentaires

Un Switch peut être **stackable** (empilable): un connecteur spécial permet de relier plusieurs switch de même marque entre eux. Le nombre de switches 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 hubs ne sont pas véritablement stackables puisque ceci reviendrait exactement au même que de les interconnecter avec des câbles croisés).

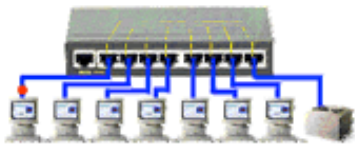
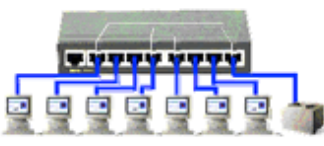
Certains switch sont **manageables**. Par une interface de type WEB reliée à l'adresse IP ou par RS232 et l'utilisation de Telnet, vous pouvez bloquer certaines lignes, empêchant par exemple, une partie de PC de se connecter vers un autre bloc de PC ou de déterminer physiquement quel PC a accès à quel 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. 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). L'utilisation d'un routeur - firewall hardware est néanmoins préférable si c'est pour bloquer les accès.

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.

#### 4.4. Différences entre un HUB et un Switch

HUB	SWITCH
Les informations envoyées d'un PC vers un autre (ou une imprimante) sont envoyées 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.
 <p style="text-align: center;"><b>Hub</b></p>	 <p style="text-align: center;"><b>Switch</b></p>
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, quel que 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 " <b>half-duplex</b> " ce qui limite les connexions à la vitesse du port. Un port 10Mbps offre une connexion à 10Mbps.	Les Switchs qui gèrent les transferts en mode " <b>full-duplex</b> " offrent la possibilité de doubler la vitesse de chaque lien, de 100Mbps à 200Mbps par exemple.
Le prix par port réseau est quasiment équivalent.	

#### 4.5. Routeur.

Les hubs et switchs 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.

<b>Classe A</b>	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, ...				
<b>Classe B</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., ...				
<b>Classe C</b>	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, ...				
<b>Classe D</b>	Multicast			
<b>Classe E</b>	Expérimentale			

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

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).

Comme les adresses des sites INTERNET sont dans des classes différentes de votre ordinateur en réseau local, 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.

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 d'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 destiné 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 address translation / port address 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, ils n'assurent pas de sécurité au niveau des ports TCP ou UDP. Ils sont utilisés pour interfacier différents groupes de PC (par exemple les départements) en assurant un semblant de sécurité. Certains switch manageables peuvent en partie être utilisés 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.

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 connexions futures pour ce genre d'application sécurisée vont plutôt pour les VPN via INTERNET.

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).

## 4.6. Répéteurs

Le répéteur est un équipement qui permet d'outrepasser la longueur maximale imposée par la norme d'un réseau. Pour ce 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 appareils permettant des liaisons de plus de 100 kilomètres.

## 4.7. 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'adresses IP. Si c'est le cas, il va envoyer un **ARP** pour déterminer l'adresse MAC de destination et envoie directement le paquet de données et les en-têtes sur le réseau. Les HUBS laissent le paquet tel quel puisqu'ils sont de simples amplificateurs. Par contre, si le réseau est relié par des switches, 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 paquet 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 paquet au routeur suivant, et ainsi de suite.

## 4.8. Connexion d'un réseau Ethernet.

Par la partie connexion Ethernet, nous savons déjà que:

- 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 switch détectent automatiquement le croisement.
- En Ethernet 10, 4 Hubs présentent un blocage au niveau des vitesses de connexion.
- En Ethernet 100, 2 HUBS en série commencent à provoquer des "bouchons" dans les flux de données.
- Les distances maximales doivent être respectées (100 mètres maximum pour le câble).
- Les règles de câblages doivent être strictes: connecteurs, proximités des câbles électriques, réseaux.
- Les hubs disparaissent, le prix d'un switch étant équivalent. Quels choix pour un réseau local ethernet?

A. Les ordinateurs d'un département (ou bureau, ou étage) 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 mais le switch sont Full duplex (communication bidirectionnelle).

B. Les départements entre eux doivent être reliés par des switches, si possible managables qui permettent de bloquer certaines connexions. Toutes connexions extérieures (Internet et liaison inter-réseau) nécessitent 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 de masquer les différentes adresses du réseau interne et incluent de plus en plus des bases de sécurité intrusions de type firewall hardware.

## 5. Liaisons à haute vitesse, haut débit, ADSL, ATM.

### 5.1. Introduction

Ce chapitre du cours hardware réseaux et communications traite des liaisons à haut débit pour la connexion des sites INTERNET et la connexion haute vitesse entre l'utilisateur et INTERNET: connexion xDSL, ATM, lignes louées, câble de télédistribution, liaison satellite,... Toutes ces solutions nécessitent un abonnement spécial chez un fournisseur d'accès.

### 5.2. Les technologies DSL

Le DSL regroupe tout ce qui permet de faire passer des flots de données à haute vitesse sur de simples lignes téléphoniques torsadées. Il existe différentes variantes :

- **HDSL** : High bit rate DSL
- **SDSL** : Single pair, ou symmetric DSL
- **ADSL** : Asymmetric DSL
- **RADSL** : Rate adaptative DSL
- **VDSL** : Very high DSL

Les différences essentielles entre ces technologies sont affaires de :

- vitesse de transmission
- distance maximale de transmission
- variation de débit entre le flux montant (utilisateur/réseau) et flux descendant (réseau/utilisateur)

Les technologies xDSL sont divisées en deux grandes familles, celles utilisant une **transmission symétrique** et celle utilisant une **connexion asymétrique**.

### 5.3. Solutions symétriques

Une solution xDSL symétrique a la même vitesse de transfert en download (Internet vers utilisateur) qu'en upload (utilisateur vers Internet), contrairement aux liaisons asymétriques (Adsl par exemple). Ceci est primordial pour l'hébergement d'un site au sein de l'entreprise. Les solutions symétriques sont surtout utilisées pour remplacer les lignes louées trop chères.

#### 5.3.1. HDSL :

La première technique issue de la technologie DSL a vu le jour au début des années 1990, c'est l'HDSL. Cette technique haut débit divise le tronc numérique du réseau de lignes louées (T1 aux États-Unis et E1 en Europe) sur plusieurs paires de fils ( 2 au lieu de 24 pour T1 et 3 au lieu de 32 pour E1). Ceci a été réalisé grâce à l'évolution de la théorie du signal permettant d'augmenter le nombre de bits par symbole transmis.

Avec cette technique, il est possible d'atteindre un débit de 2Mbps sur trois paires torsadées et 1,5Mbps sur deux paires. Tout ceci en possédant une longueur de boucle locale de 4,5km et sans adjonction supplémentaire de répéteurs. Le principal argument du HDSL est d'ordre économique.

L'HDSL est particulièrement bien adapté pour:

- le remplacement de lignes T1 et E1 (réseaux d'accès des opérateurs télécoms)
- les réseaux locaux LAN
- les systèmes intégrant des PABX (Autocommutateur d'entreprise) et la Voix sur IP

En résumé, l'HDSL permet :

- d'écouler le trafic de façon symétrique mais nécessite deux ou trois paires de cuivre. Il alloue la même largeur de bande dans le sens montant que dans le sens descendant.
- d'avoir un débit de 2Mbps, ce dernier pouvant tomber à 384 kbps en fonction de la qualité de la ligne et de la distance (limitée à 4,5 km).

En Europe, les opérateurs commencent juste à déployer massivement ces technologies et les prix tardent à baisser faute de concurrence. L'innovation devrait provenir de HDSL2. Cette technologie, dérivée du HDSL, offre les mêmes performances mais sur une seule paire torsadée. Elle est actuellement testée aux États-Unis à 1,5Mbps. Le problème actuel de cette technologie est une standardisation encore imparfaite.

### **5.3.2. SDSL (Symmetric Digital Subscriber Line):**

Le précurseur de la technologie HDSL2 est le SDSL. Comme HDSL, SDSL supporte les transmissions symétriques sur T1 et E1, cependant, elle diffère d'HDSL par trois points importants :

1. la transmission se fait sur une paire torsadée
2. la longueur de la boucle locale est limitée à 3,6km (soit 1,8 km du concentrateur)
3. le débit est limité à 2 Mb/s en download et en upload.

Tout comme le HDSL, cette solution symétrique est réservée au remplacement des lignes louées T1 et E1. L'utilisation de la ligne avec un appel téléphonique est impossible.

Il est possible de coupler 2 lignes pour atteindre 4 Mb/s. La distance du répartiteur est en théorie de 1,5 Km, mais des tests montent jusqu'à 2 km

### **5.3.3. SHDSL**

La dernière solution symétrique SHDSL (Single-pair High-speed DSL) date de 2002. Elle rassemble les technologies HDSL et HDSL2 et SDSL. Les taux de transfert (en charge utile) sont identiques dans les deux directions et peuvent varier de 192 Kb/s à 2,3 Mb/s en mode deux fils (une paire) à 384 Kb/s to 4.6 Mb/s en mode quatre fils (deux paires).

Cette solution utilise toute la bande passante de la ligne téléphonique. Il n'est donc plus possible d'utiliser la ligne téléphonique en même temps. L'utilisation de filtres n'est donc pas nécessaire. Ces lignes permettent également le passage de signaux téléphoniques "numérisés" de type normal ou ISDN via des appareils spécifiques (PABX par exemple).

Le débit d'une ligne SHDSL est configurée pour un débit fixe (jusque 2,3 Mb/s). Dans le cas où le modem ne peut pas atteindre cette vitesse, il n'y a pas de connexion. Néanmoins, quelques fabricants autorisent une auto détection de la vitesse par le modem des vitesses inférieures. La distance maximum est de 5 Km sur une simple paire de cuivre.



## 5.4. Solutions asymétriques: ADSL, RADSL et VDSL

Par différents tests, on s'est aperçu qu'il était possible de transmettre les données plus rapidement depuis le central du réseau public vers l'utilisateur. Comme la concentration des câbles est plus importante lorsqu'on se rapproche du central, ces derniers génèrent donc plus de diaphonie à proximité du commutateur. Les signaux provenant de l'utilisateur, plus atténués, sont plus sensibles au bruit causé par ces perturbations électromagnétiques. Il est donc préférable de transmettre en basse fréquence (ou sur une bande de fréquence moins large) les données issues de l'utilisateur.

L'idée est l'utilisation d'une connexion asymétrique, en imposant un débit plus faible de l'abonné vers le central. Les systèmes utilisant cette technique ont été nommés ADSL. Il en existe au moins deux variantes: le RADSL et le VDSL

Ces solutions asymétriques sont caduques pour l'hébergement de site Internet importants, la vitesse de transfert serveur Internet vers Internet (vers l'utilisateur) est nettement inférieure à la vitesse de transfert utilisateur vers serveur. Par contre, ceci peut tout à fait fonctionner pour l'hébergement d'un petit site d'amateur ou de PME à condition d'utiliser une adresse TCP fixe ou d'utiliser un programme de redirection d'adresse TCP.

### 5.4.1. ADSL (Asymmetric Digital Subscriber Line):

La plus importante caractéristique de l'ADSL est sa capacité d'offrir des services numériques rapides sur le réseau téléphonique cuivré existant, en superposition et sans interférence avec le service téléphonique. Un circuit ADSL relie un central du réseau public au modem ADSL de l'utilisateur, créant ainsi trois canaux d'information:

1. un canal descendant haut débit
2. un canal duplex moyen débit
3. un canal de téléphonie (voix normales)

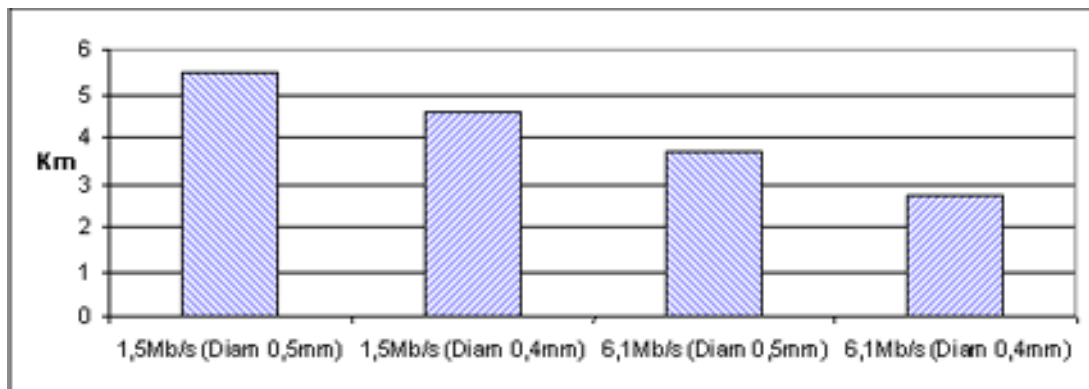
Pour créer des canaux multiples, les modems ADSL divisent la largeur de bande disponible d'une ligne téléphonique suivant l'un des deux types: le multiplexage à division de fréquence (FDM) et l'annulation d'écho. □ Avec l'une ou l'autre de ces techniques, les transmissions ADSL laissent la région autour des 4kHz libre afin de laisser passer les communications téléphoniques. L'installation de l'ADSL nécessite, en plus du modem ADSL, un séparateur de ligne (splitter qui filtre les signaux téléphoniques voie - signal digital), comme expliqué dans la partie **installation du filtre ADSL**.

L'ADSL permet, pour une longueur de boucle maximale de 5,6km, de fournir des débits de :

- au minimum de 1,5 à 2Mbps dans le sens commutateur vers utilisateur (maximum 8Mbps)
- au minimum de 16 kbps dans le sens utilisateur vers commutateur (maximum 640kbps)

Les abonnements en France fournissent des vitesses de 256 Kb/s, 512 kb/s,... Vous pouvez parfois augmenter le débit en changeant d'abonnement chez votre fournisseur d'accès (nettement plus chères).

Ces débits maximum dépendent également d'un certain nombre de facteurs comprenant, la longueur de la boucle, sa section et les interférences. L'atténuation de ligne augmente avec sa longueur, la fréquence du signal émis ainsi que l'étrouitesse du câble.



**Distances maximales de transmission**

Ces vitesses de transfert transforment le réseau public téléphonique existant (limité à la voix, au texte et aux graphismes basse résolution) en un système puissant capable de supporter le multimédia, y compris la vidéo temps réel. En transmettant des films, des programmes de télévision, des données de réseaux locaux d'entreprises, et surtout en introduisant l'Internet dans les maisons, ADSL rend les marchés viables et rentables pour les compagnies de téléphone et les fournisseurs d'applications.

En décembre 1998, une importante étape a été franchie par l'UIT (Union Internationale des Télécommunications) en ce qui concerne la normalisation des systèmes DSL. Le standard le plus attendu était l'ADSL-Lite, qui cache une version allégée de l'ADSL. Il est destiné aux accès rapides à Internet et fonctionne à des débits inférieurs à ceux de son aîné (mais largement supérieurs à ceux des modems V.92 en 55.600 kb/s maximum). Il est moins complexe à mettre en œuvre et ne requiert pas de filtre ADSL (splitter).

### 5.4.2. RADSL

Avec RADSL (Rate Adaptive DSL), la vitesse de la transmission est fixée de manière automatique et dynamique, selon la qualité de la ligne de communication. Aussi longtemps qu'il fut question de transfert de données vidéo, il fut hors de question de faire varier le débit. Dans ce cas précis, il est nécessaire de faire un traitement synchrone. Cependant, depuis l'échec du VDT (Video Dial Tone), qui a subi la concurrence de la TV câblée et par satellite, d'autres applications sont apparues :

1. les architectures client/serveur
2. l'accès aux réseaux à distance
3. l'Internet et le multimédia

Ces applications possèdent deux avantages, la synchronisation n'est plus obligatoire, et l'architecture asymétrique devient évidente (dans la mesure où l'on transmet plus d'informations dans le sens serveur/client que dans l'autre). Le RADSL adapte donc sa vitesse aux conditions locales.

RADSL permettrait des débits constants (ascendants de 128kbps à 1Mbps et descendant de 600kbps à 7Mbps), pour une longueur maximale de boucle locale de 5,4km (comme l'ADSL). RADSL est en cours de normalisation par l'ANSI. L'organisme considère les technologies QAM, CAP et DMT comme modulations RADSL.

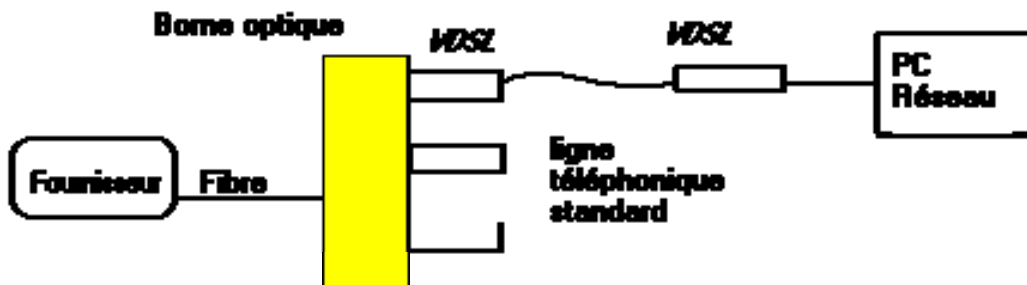
### 5.4.3. VDSL

VDSL est la plus rapide des technologies xDSL. Elle est capable de supporter, sur une simple

paire torsadée, des débits :

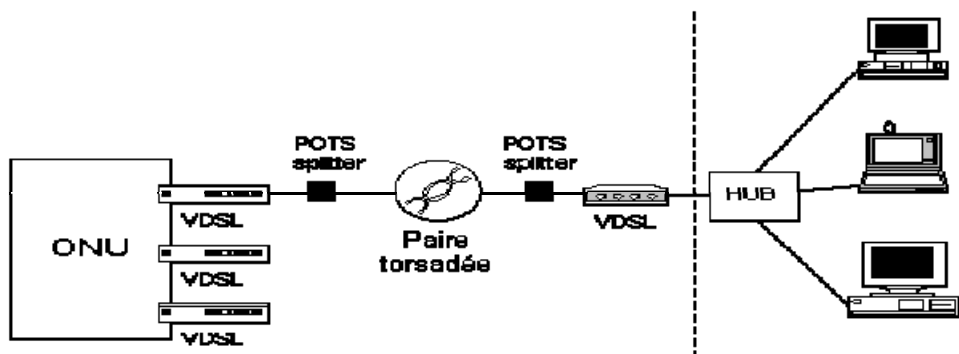
- descendants de 13 à 52 Mbps
- ascendants de 1,5 à 2,3 Mbps

En revanche, la longueur maximale de la boucle est seulement de 1,5km. Cette distance est très faible mais elle peut être augmentée en utilisant de la fibre optique, du fournisseur jusqu'à une borne optique spéciale proche de l'utilisateur. A partir de cette borne ce dernier peut être connecté en VDSL (voir figure ci-dessous).

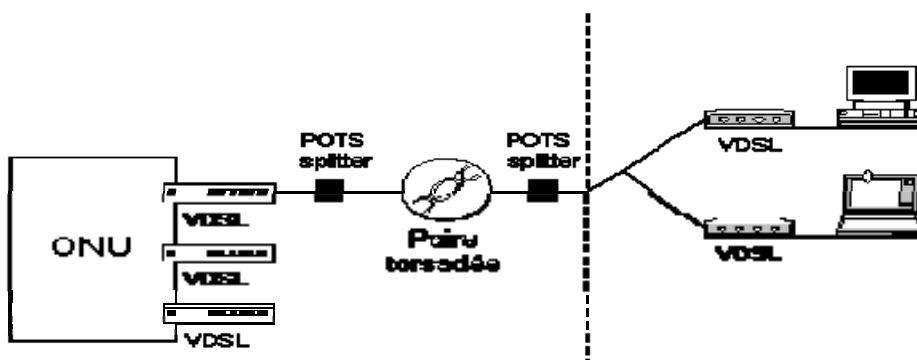


En ce qui concerne la modulation, les deux canaux de données sont séparés des bandes utilisées pour la téléphonie d'une part, et de celles utilisées pour le RNIS d'autre part. Ceci permettrait aux fournisseurs de services de superposer VDSL aux services déjà existants. Pour l'heure il est envisagé que les deux canaux (ascendants et descendant) soient aussi séparés en fréquence.

Les données descendantes pourront être transmises à chaque équipement terminal (terminaison passive de réseau) ou à un pivot qui distribue les données aux équipements terminaux (terminaison active de réseau).



**Terminaison active de réseau**



**Terminaison passive de réseau**

Pour les données ascendantes, le multiplexage est plus difficile. Dans une configuration

passive, chaque équipement terminal doit partager un câble commun. Un système de détection de collisions pourrait être utilisé, cependant, deux autres solutions peuvent être envisagées.

Une première solution consisterait à ce que la borne optique envoie des trames à tous les équipements terminaux. Ces trames autoriseraient un seul équipement à communiquer et pendant une certaine période (TDMA Time Division Multiplexing Access). Cet équipement se reconnaîtrait, grâce à la trame, et transmettrait pendant cette période. Cependant, cette méthode est lourde dans la mesure où elle implique d'insérer un certain temps d'attente entre deux autorisations et où elle nécessite beaucoup d'octets pour son seul protocole de fonctionnement (ce qui réduit le débit utile).

La seconde méthode consisterait à diviser le canal ascendant en différentes bandes de fréquences et associer chaque bande à un équipement terminal (FDMA Frequency Division Multiplexing Access). Cette méthode possède l'avantage de s'affranchir de tout protocole de dialogue. Cependant, elle limiterait à une valeur fixe le débit disponible de chaque équipement terminal.

En conclusion, nous avons vu que l'augmentation de la bande passante du VDSL permet au fournisseur d'accès d'offrir des services de télévision haute définition et de vidéo de qualité numérique, de l'Internet multimédia et des services LAN aux consommateurs.

#### 5.4.4. Tableau récapitulatif des technologies DSL

Les technologies DSL						
Technologie	Définition	Mode de transmission	Débit Internet -> PC (Download)	Débit PC -> Internet (Upload)	Distance maximale	Nombre de paires
HDSL	High data rate DSL	Symétrique	1.544 Mbps □ 2.048 Mbps	1.544 Mbps 2.048 Mbps	3.6 km	2 ou 3 suivant le débit souhaité
HDSL 2	High data rate DSL 2	Symétrique	1.544 Mbps	1.544 Mbps	3.6 km	1
SDSL	Single line DSL	Symétrique	768 Kbps	768 Kbps	3.6 km	1
SHDSL	Single-Pair High-Speed DSL	Symétrique	- 192 Kb/s à 2,3 Mb/s (une paire), - 384 Kb/s to 4.6 Mb/s (deux paires)	- 192 Kb/s à 2,3 Mb/s (une paire), - 384 Kb/s to 4.6 Mb/s (deux paires)	5 km	1 ou 2 suivant le débit souhaité
ADSL	Asymmetric DSL	Asymétrique	128 Kbps à 9 Mbps	16-640 Kbps	5.4 km	1
RADSL	Rate Adaptive DSL	Asymétrique	0.6- 7 Mbps	128 kb/s-1 Mb/s	5.4 km	1

VDSL	Very high data DSL	Asymétrique	15-53 Mbps	1.544-2.3 Mbps	1.3 km	1
------	--------------------	-------------	------------	----------------	--------	---

## 5.5. Ligne louée

Une autre méthode de connexion à Internet ou à un réseau d'entreprise (interconnexion) utilise des lignes louées. Elles présentent actuellement le débit le plus élevé mais le nombre de paires est nettement plus élevée (24 paires pour T1 et 32 paires pour E1 par exemple). Cette solution est forcément nettement plus chère que les solutions standards. C'est actuellement la connexion la plus sûre puisqu'elle relie directement 2 points sans passer par des intermédiaires. Malheureusement, la sécurité a un prix. Par compression, ces lignes permettent d'utiliser la ligne autant en communication INTERNET, qu'en communication de type ISDN ou RTC via PABX.

Dans le cas des fournisseurs d'accès européens, les types actuels sont E1 (2Mb/s, 50 km maximum), E2 (8Mb/s), E3 (34 Mb/s) et E4 (140 Mb/s)

Dans le cas des fournisseurs américains, T1 (1,544 Mb/s), T2=4X T1 (6,312 Mb/s) et T3=7\*T2 (44,736 Mb/s)

Pour le Japon: T1 (1,544 Mbps), T2=4\*T1 (6,312 Mbps), T3=5\*T2 (32,064 Mbps) et T4=3\*T3 (97,728 Mbps).

## 5.6. Connexion INTERNET par satellite

La connexion INTERNET par satellite a quelques avantages, notamment de ne pas dépendre d'installations terrestres existantes: câbles de télédistribution, réseau téléphoniques avec bornes DSL proches,...

Les premières connexions par satellite utilisaient un système hybride: réception par liaison hertzienne, émission par modem RTC classique. Cette solution peu avantageuse permet d'utiliser une antenne parabole standard.

Les nouvelles paraboles permettent l'émission et la réception. La vitesse en upload (envoi vers INTERNET) varie de 128 k à 1024k et de 512kbps à 2 Mbps en download (Internet vers utilisateur) pour les applications commerciales. La limite théorique de cette connexion avoisine les 155 Mbps (un record). Ceci ne tient pas compte des temps de latence (près de 700 millisecondes) entre le signal émis et le signal reçu de l'autre côté de la liaison. Comme les satellites sont géostationnaires, la distance entre le satellite et la terre est de 36.000 km (multipliez par 2, soit 72.000 km, pour la distance à parcourir). Le temps de propagation entre le message envoyé et le début d'envoi de l'information est un peu plus important que dans les autres connexions haute vitesse (c'est le même problème avec les connexions par GSM satellite). De ce fait, la vitesse de ping est très faible. Ceci ne devrait néanmoins perturber que quelques applications critiques ou les joueurs via Internet; dans une moindre mesure le VoIP.

Cette solution a quelques défauts supplémentaires puisque le prix de l'installation est cher (comptez début 2004 à partir de 1000 € pour l'antenne de moins d'1 mètres de diamètre, terminal de transmission / réception), sans compter la pose de l'antenne par un technicien spécialisé qui va diriger l'antenne sur un satellite précis. De plus les abonnements restent également nettement supérieurs à ceux de l'ADSL. Cette solution n'est à préconiser que pour les zones non desservies par les technologies DSL.

## 5.7. Câble TV.

Cette solution utilise le réseau de télé-distribution. Les fréquences de transfert sur ces câbles s'étalent de 10 à 860 Mhz mais certaines zones sont bloquées pour ne pas interférer avec les radio FM, communications militaires,... Sur ce large spectre, les chaînes de télé numériques sont regroupées par paquets de 8. Chacun de ces paquets occupe une largeur de bande de 8 Mhz. Par contre, les chaînes de télévision analogiques ne peuvent être rassemblées et occupent 8 Mhz également.

Deux zones de fréquences sont réservées pour INTERNET, une pour le flanc montant, l'autre pour le flanc descendant. Le débit de la partie montante, large de 30 Mhz, atteint 128 kbs/s. Dans le sens descendant, le débit varie suivant les offres commerciales entre 512 et 768 kb/s mais peut aller jusqu'à 1,500 Mbps. Contrairement à l'ADSL, cette largeur de bande est partagée entre tous les utilisateurs d'un même tronçon, typiquement plusieurs immeubles.

## 5.8. Liaison ATM.

L'ATM (Asynchronous Transfer Mode) fut choisi comme standard vers la fin des années 80. Il est l'héritier direct de Frame Relay dont il diffère par l'emploi de paquets de petite taille et fixe (appelées cellule). Le protocole ATM est orienté connexion.

L'ATM transporte un flux continu de cellules (trames) de **taille fixe** comportant 5 octets (byte) d'en-tête et 48 octets (byte) de données. La bande passante est optimale. Les liaisons ATM utilisent un mécanisme de priorité des données, appelé QOS (Quality Of Service). Ceci signifie que les messages haute priorité sont envoyés directement. Lorsque ATM trouve des blancs (pas d'émission de données prioritaire), il va envoyer des données moins prioritaires pour boucher ces blancs. Cette possibilité permet de transférer via des liaisons ATM toutes sortes d'informations (données, voix et autres). La transmission est supposée sans erreur. Ceci signifie que le message n'est jamais rémis. Ceci nécessite un réseau (câblage) avec de faibles pertes.

En pratique, les fonctions de routage de cellule sont directement implantées en hardware, contrairement à la plupart des routeurs IP. Pour les liaisons ATM, le terme utilisé pour les routeurs est Switch. ATM rajoute aux technologies qui l'ont précédé la possibilité de garantir capacité et qualité du service. On peut ainsi établir une connexion ATM entre 2 systèmes et spécifier par exemple que l'on souhaite un débit garanti de 3 Mb/s, un délai maximum de 100 ms, une variation de délai inférieure à 5 ms et un taux de perte inférieur à  $10^{-10}$ . De telles garanties sont nécessaires pour pouvoir transporter sur ATM les circuits numériques (à 64 Kb/s, 2 Mb/s, 34 Mb/s, ...à 622 Mb/s actuellement). C'est cette qualité de service qui le rend indispensable par rapport aux réseaux Ethernet. En plus, certaines liaisons ATM peuvent atteindre 10 Gb/s sur quasiment n'importe quelle distance.

Les liaisons ATM sont indépendantes du type de support réseau. La technologie ATM peut donc être implantée sur du câble réseau torsadé, coaxial ou fibre optique avec des limitations pour les grandes vitesses. Elle n'est pas forcément indépendante de la technologie IP, mais complémentaire. La technologie ATM n'a pas dans sa structure des adresses de destinations et d'émissions. Elle régit uniquement les couches basses du modèle OSI chargées du transport.

## 6. Réseau sans fils

### 6.1. Introduction

Les connexions sans fils permettent de connecter différents appareils ... sans câble. La liaison peut être soit de type hertzienne, soit par lumière infrarouge. Pour les liaisons infrarouges, l'émetteur et le récepteur doivent être face à face. Ces connexions étaient utilisées (sans grand succès) pour les claviers et les souris mais sont implantés dans certaines imprimantes.

Les liaisons sans fils ont pris une toute autre direction, la connexion simultanée de plusieurs appareils entre eux. Il peut s'agir d'imprimantes, GSM et périphériques divers ou même de réseaux (appelés Wlan - Wireless Lan). La difficulté de mise en œuvre tient de la zone de réception, liée à la puissance de l'émetteur, à la détection du récepteur (d'où un protocole définissant clairement celui-ci) et de la sécurité des données transmises. Cette sécurité doit tenir compte de la vérification des données mais également du cryptage des informations. Rien ne sert de sécuriser un réseau si un simple récepteur hertzien peut pomper toutes les données circulant sur le réseau.

Actuellement, plusieurs types de réseaux "sans fils" sont sur le marché pour des distributions courantes.

Les solutions hertziennes posent des problèmes d'environnement que peu de constructeurs signalent. Il n'y a qu'à se promener dans un bâtiment industriel (en tôle) pour se rendre compte que l'environnement pose quels problèmes de liaisons GSM par exemple. Les distances maximales fournies par les constructeurs parlent de terrains découverts, ce qui est rarement le cas dans les habitations ou entreprises, même s'il est possible d'installer des antennes externes dans de nombreux cas. Les environnements perturbés par des champs électromagnétiques (machines électriques de fortes puissances) posent les mêmes problèmes que dans les câblages réseaux classiques. Souvent, il faudra mélanger des solutions avec câblage réseau et liaison hertzienne.

### 6.2. Bluetooth

Ce type de liaison sans fil permet de relier deux appareils via une liaison hertzienne. Ces appareils peuvent être des appareils photo numériques, des PDA, imprimantes, .. Bluetooth exploite la gamme de fréquence des 2,45 Ghz **ISM** (Industrial, Scientific & Medical) qui est normalement libre de droit pour la majorité des pays. Le nombre de fréquences distinctes utilisées est de 79. Vous pourriez donc utiliser 79 réseaux différents dans la même pièce. Le débit de la connexion est de maximum 1 Mb/s pour des périphériques distants de maximum 4 mètres et 75 kb/s pour des distances supérieures. La distance maximum est de 10 mètres, mais peut atteindre dans certains cas 100 mètres. En effet, la technologie Bluetooth définit 2 catégories de puissance radiofréquence pour les réseaux personnels, la plage courte (0 dBm) qui autorise des distances jusqu'à 10 mètres et la plage moyenne (+ 20 dBm) qui porte jusqu'à 100 mètres. La liaison radio soutient à la fois la transmission de données et vocale avec une vitesse maximum de données de 72 kb/s, ce qui est en pratique le taux maximum.

Sécurisée, cette connexion est transparente uniquement si les deux appareils se connaissent. Chaque périphérique reçoit un code à la fabrication sur six octets: les trois premiers désignant le constructeur et les trois autres la machine. En effet, chaque appareil bluetooth peut être désactivé pour une connexion automatique ou activé pour seulement certains appareils. Les périphériques utilisent donc des systèmes de protection évitant le transfert de données non autorisées. Néanmoins, la sécurité est souvent désactivée par défaut et le piratage est donc possible pour récupérer par exemple les données du carnet d'adresse d'un GSM ou d'un PDA à partir d'un autre appareil ou



utiliser le GSM du voisin pour une connexion INTERNET.

Au sein d'un réseau bluetooth, un appareil sert de maître et jusqu'à 7 périphériques esclaves se partagent la bande passante. Il est possible en théorie de faire communiquer jusqu'à 10 groupes d'appareils, soit 80 appareils.

Au contraire des liaisons IEEE 802.11, ce type de connexion n'est pas dédié pour les liaisons réseaux (même si c'est possible). Il permet par exemple de connecter un PDA directement à un Notebook ou à un GSM.

### **6.3. IEEE 802.11**

Liaison hertzienne utilisant également la bande de fréquence des 2,45 Ghz (ISM). Le débit maximal est de 2 Mb/s sur une distance maximum de 100 mètres. Les spécificités un peu vieillottes de ce standard de réseaux sans fils datent de 1997. Elle n'est plus utilisée actuellement.

### **6.4. IEEE 802.11a**

Cette norme opère dans la bande de fréquence 5-6 Ghz. Le schéma de modulation utilisé est le "orthogonal frequency-division multiplexing" (OFDM). Dans ce type de modulation, le signal est découpé et envoyé sur plusieurs de fréquences différentes. Ceci limite les interférences et rend possible des vitesses de transmission de données allant jusqu'à 54 Mb/s (soit environ 10 MB/s), mais plus généralement les communications se passent à 6 Mb/s, 12 Mb/s ou 24 Mb/s.

La distance maximale entre le point central (qui fonctionne comme un Hub) et les stations est de 366 m à 6 Mbps en extérieur et de 91 m à 6 Mbps en intérieur. Pour de faibles distances, il est plus rapide que le 802.11B Wifi.

Cette norme est parfois appelée Wifi5. Elle est peu utilisée en Europe mais très implantée aux Etats-Unis.

### **6.5. IEEE 802.11b - Wifi - IEEE 802.11 HR**

Dérivé du IEEE 802.11 (1999), cette liaison hertzienne utilise également la bande de fréquence des 2,4 Ghz. Elle est utilisée comme connexion réseau via des cartes réseaux spécifiques et un appareil central appelé point d'accès (Access Point) fonctionnant comme un hub (la bande passante totale est donc partagée entre les différents PC. Cette connexion permet un débit maximum de 11 Mb/s sur un rayon d'une centaine de mètres mais la portée dépend fortement de l'environnement (murs ou cloisons, ...). Le nombre de périphérique est limité à 10 par stations.

Cette solution est adaptée actuellement pour les réseaux sans fils. La connexion utilise les 2 couches basses du modèle OSI qui servent au transport. Chaque PC, portable et périphérique inclus une carte réseau de type WIFI avec une antenne. Un concentrateur (HUB, switch ou même routeur) sert de point central pour le partage ou éventuellement pour une connexion vers un concentrateur classique.

La méthode de prise de ligne est de type CSMA/CA, identique aux réseaux Ethernet. Une grosse différence tout de même. Lorsqu'une station émet sur une liaison filaire Ethernet, elle est à l'écoute de toutes les stations sur le câble, ce qui pourrait ne pas être le cas dans une liaison hertzienne. En effet, le fait que 2 stations puissent se raccorder sur le nœud central n'inclut pas que les stations puissent communiquer directement entre elles si la distance est trop importante. Pour



cela, on utilise le mécanisme de "Virtual Carrier Sense". Une station voulant émettre transmet un petit paquet appelé **RTS** (Request To Send), qui indique la source, la destination et la durée de la transmission. La station répond, si elle est libre, par un paquet de contrôle appelé **CTS** (Clear To Send) qui inclue les mêmes informations de durée. Toutes les stations qui reçoivent un RTS ou un CTS déclenchent un indicateur de Virtual Carrier Sense (appelé NAV - Network Allocation Vector) pour une certaine durée.

Pratiquement tous les fabricants de composants réseaux incluent de tels appareils dans leur catalogue.

La distance maximale est de 503 m à 1 Mbps en extérieur et de 152 m en 1 Mbps en intérieur.

Un routeur WIFI peut servir de routeur ou de pont. Il utilise généralement 2 antennes directionnelles. Les cartes réseaux sont spécifiques, avec une antenne extérieure. Ci-dessous la photo d'un routeur Wifi de D-Link.



## 6.6. Réseau sans fil IEEE 802.11B+

Le 802.11 B+ est dérivé du 802.11 B. Il utilise la même gamme de fréquence mais avec des particularités d'en cryptage spécifiques puisque celui-ci se fait sur 64, 128 ou même 256 bits. Pour rappel, les versions actuelles d'Internet Explorer ne cryptent que sur 128 bits. Ce système permet des débits de 22 Mbps, soit le double de 802.11b.

Il est tout à fait compatible descendant avec le 802.11B standard. Un périphérique 802.11B+ acceptera donc la connexion avec les périphériques 802.11B. Par contre, ce standard n'est pas normalisé. Il est donc possible que des appareils 802.11B+ de fabricants différents **ne soient pas compatibles**.

## 6.7. Réseau sans fil 802.11 G

Même si la normalisation date de mai 2003, quelques appareils sont sortis avant. Les premiers appareils réellement à la norme sont sortis début juillet 2003. Cette norme wireless permet des liaisons à 54 Mbps en utilisant la gamme de fréquence des 2,4 Ghz (idem que le 802.11 b). Cette utilisation de la même zone de fréquence devrait permettre de mélanger des points d'accès 802.11 B et 802.11 B+ (dans la même marque). Le point central adapte sa vitesse en fonction du périphérique connecté, permettant à des clients 802.11 B de se connecter.

Voir le paramétrage d'un routeur D-Link DI-624 (6.11.)

## 6.8. Connexion sans fil 802.11G+

Cette amélioration du 802.11G est sortie début 2004 et double la vitesse de connexion des 802.11G pour atteindre 108 Mb/s. Voir un exemple de configuration d'un pont D-link DWL-2100AP dans « Sécurité des réseaux sans fil » (6.12.)

## 6.9. IEEE 802.11N

En cours d'élaboration en 2006, cette norme n'est pas encore réellement sortie, même si quels appareils sont déjà sur le marché avec des incompatibilités avec les normes existantes, quand ce n'est pas directement des interférences.

## 6.10. Connexion infra-rouge.

Ce type de connexion va disparaître et être remplacé par les connexions hertziennes vues plus haut. Le premier problème de ce type de connexion vient de son mode de fonctionnement, la lumière. Les appareils connectés doivent être parfaitement en face l'un de l'autre, ce qui n'est pas toujours aisé. De plus, de nombreuses solutions ont été proposées. Même si la liaison IrDA (installé dans les imprimantes HP990CXi par exemple) a pris plus d'ampleur que les autres liaisons, cette multitude de système a fortement réduit le champ d'activité.

La liaison infrarouge IrDA permet une connexion de 1 mètre pour une vitesse maximum de 16 Mb/s

## 6.11. Paramétrage routeur D-Link DI-624

### 6.11.1. Paramétrage de base du routeur ADSL

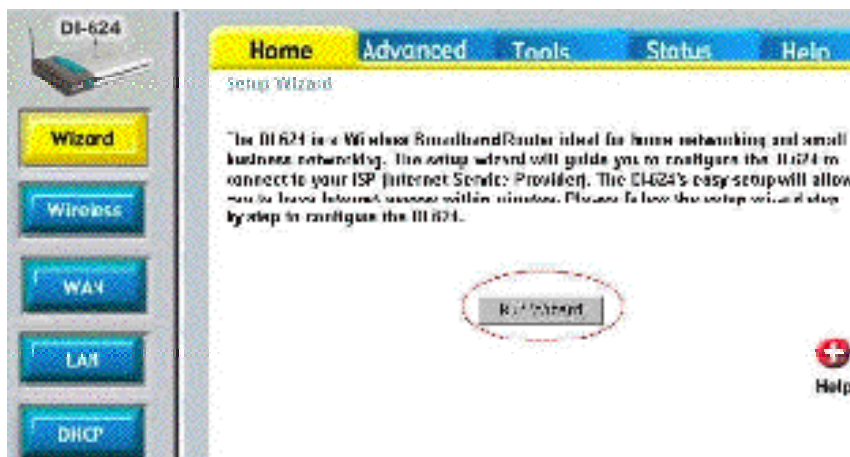
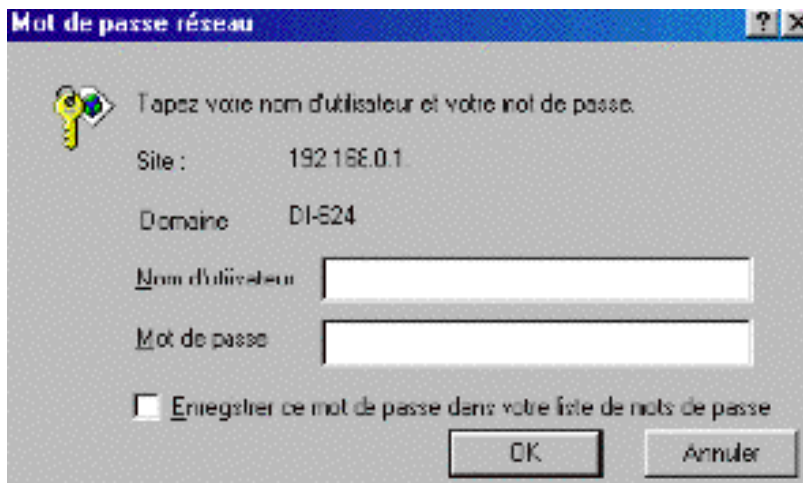
Le routeur D-Link DI 624 ressemble au modèle 802.11 B. Il est constitué de 4 ports Ethernet 10/100 pour les liaisons "câbles", une liaison Wan pour le modem ADSL (RJ45) et d'une connexion 802.11G pour les connexions sans fils. L'appareil est muni de 2 antennes directionnelles.



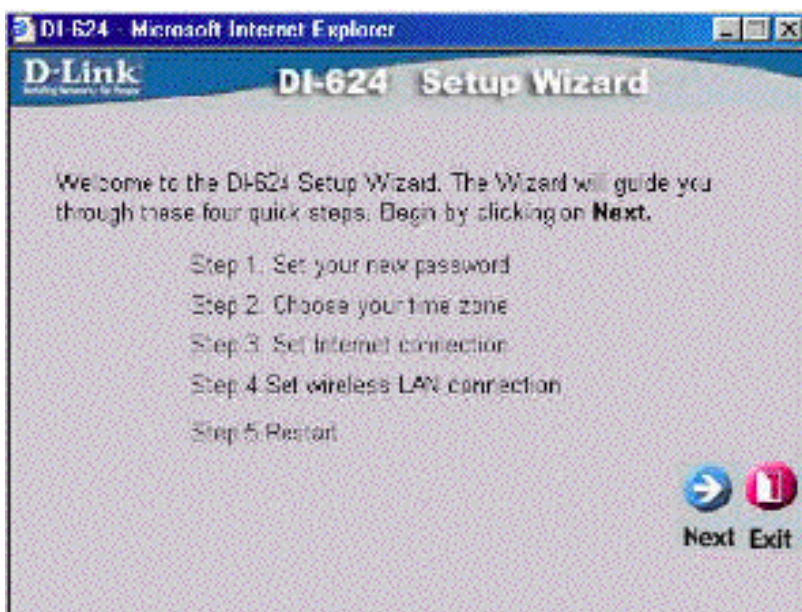
Commençons par connecter le routeur sur l'alimentation, un PC via une carte réseau Ethernet 10/100, un modem ADSL RJ45 (préalablement configuré en mode pont).

Une fois connecté sur un PC via une carte réseau, le PC doit être redémarré. En effet, l'adresse de base de l'appareil est 192.168.0.1. Le routeur D-Link inclut un serveur **DHCP** qui va automatiquement attribuer une adresse à chaque PC connecté dans la même classe d'adresses 192.168.0.X. Cette fonction pourrait perturber le fonctionnement de réseaux existants. Il est donc conseillé de connecter l'appareil sur un ordinateur seul et pas sur un réseau Ethernet interne existant.

Le paramétrage de l'appareil se fait par Internet Explorer en tapant l'adresse de l'appareil (192.168.0.1.) dans la barre d'adresses. La fenêtre suivante demande le login et le mot de passe de la connexion. Par défaut, le mot de passe est admin, sans mot de passe.



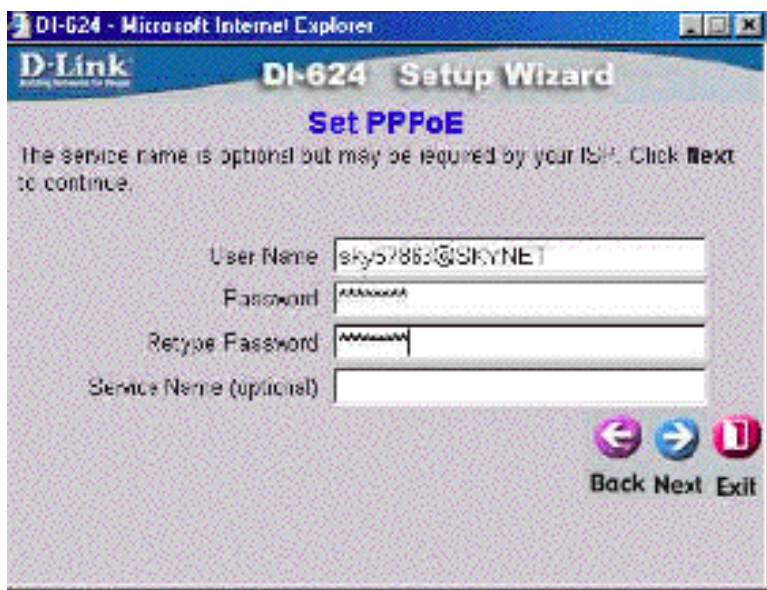
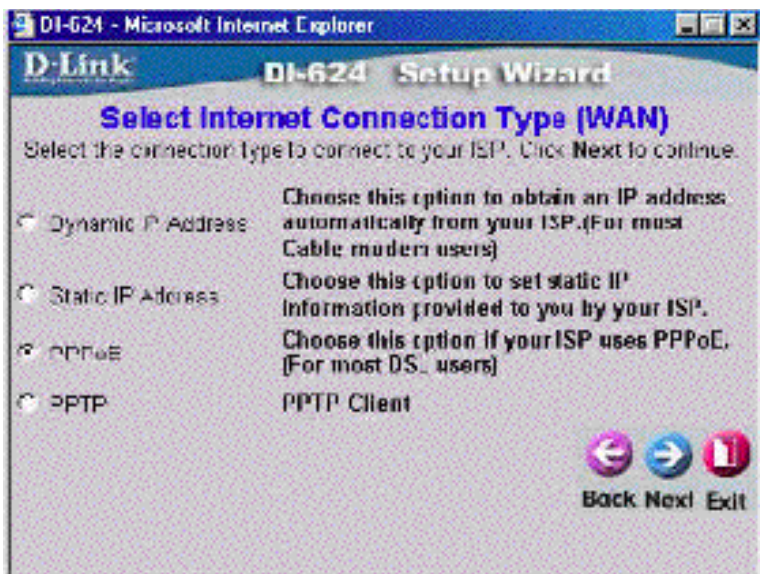
Une configuration de base du routeur est relativement facile puisqu'il suffit de cliquer sur le bouton "**Run Wizard**" pour débuter la configuration.



La première chose va être de donner **un mot de passe à l'appareil**. La zone GMT correspond à GMT +1 (Bruxelles - Paris).

Le point suivant va détecter le modem ADSL programmé en mode pont, un Tornado Webjet

810 dans notre cas. Il est immédiatement détecté en mode PPPoE (ce qui est le paramétrage de la majorité des connexions de type ADSL), il ne reste plus qu'à faire le setup de la connexion: login et mot de passe. Ceci est valable avec une adresse fournie par le fournisseur d'accès variable, suivant les types de connexion Internet.



L'étape suivante va nous permettre de configurer le réseau sans fil.



Le point suivant va paramétrer le réseau sans fil.

Sélectionnons le canal 6 par exemple. Ce point pourra être modifié ultérieurement pour s'implanter dans un réseau existant.

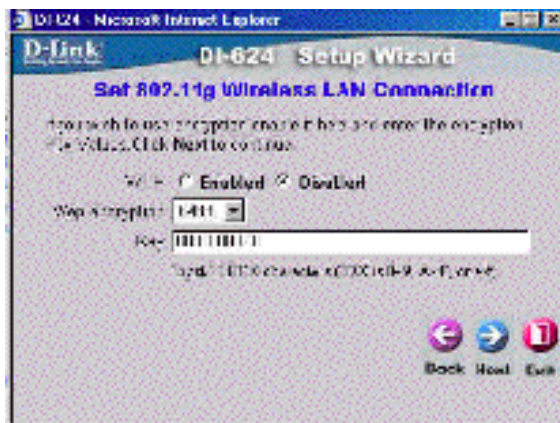


Nous allons maintenant sécuriser le réseau et crypter le signal sur le réseau sans fil. Par défaut, il n'est pas activé (disabled).

Le niveau de cryptage peut être 64 ou 128 bits. Il faudra rentrer une clé identique pour les cartes réseau sans fil constituée de 10 chiffres en Hexadécimal (variant de 0 à F).

Par exemple:

FAC916D556



La configuration étant complétée, il ne reste plus qu'à redémarrer le routeur sans fil. Dans certains cas, il faudra programmer pour chaque station: le **DNS**, une adresse IP automatique. La configuration ci-dessus m'a pris à peine 1 minutes (mais le modem était déjà paramétré).

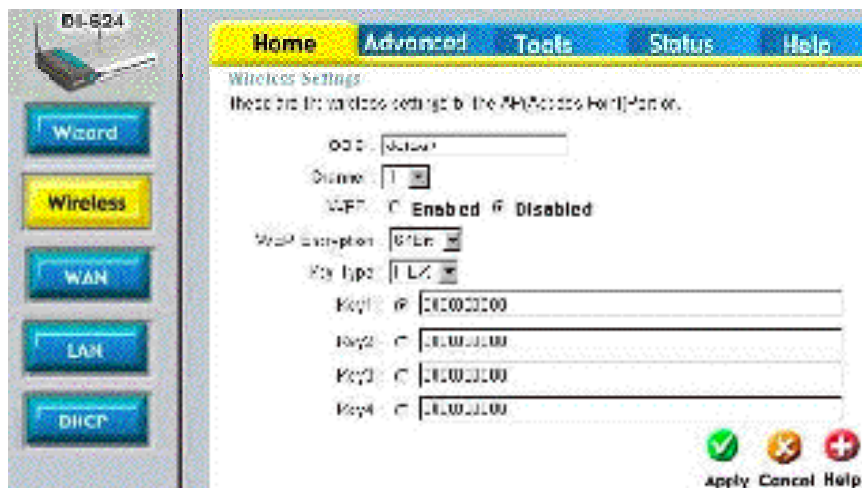
### 6.11.2. Paramétrage avancé du routeur D-Link DI-624

Bref aperçu des fonctions "sans fil" de l'appareil. Les boutons au-dessus rassemblent les catégories. Pour chaque catégorie, les différentes parties sont subdivisées par les boutons à gauche.

#### 1. Le menu Home

La fonction **Wizard** permet le paramétrage automatique.

La fonction **Wireless** permet de modifier le canal utilisé et l'encryptage des données (ici désactivé) suivant une clé à choisir parmi 4 (10 chiffres en hexadécimal). Ceci avait déjà été parcouru dans le paramétrage automatique.



La fonction **Wan** permet de modifier le type de connexion (PPPoE), les adresses DNS fournies par votre provider (même si elles peuvent être paramétrées individuellement pour chaque station). C'est également ici que vous devez paramétrer les adresses IP provider fixes.

La fonction **LAN** permet de modifier l'adresse interne du routeur. Dans ce cas, il faudra également modifier les paramètres DHCP pour rester dans la même classe d'adresses IP.

La fonction **DHCP** (très efficace) permet d'attribuer les plages d'adresses (obligatoirement dans la même classe) du réseau. On voit ici qu'actuellement 2 PC sont connectés.



## 2. Le menu Advanced

Ce menu reprend les fonctions de Firewall hardware du routeur. Une fonction permet la connexion d'Internet vers le réseau interne (fonction VPN).

## 3. Le menu TOOLS

C'est par ici que vous pouvez modifier les mots de passe, l'heure interne du routeur, accepter ou non certaines commandes (ping externe), changer le mot de passe, ...

## 4. Le menu STATUS

Ce menu permet d'afficher les statistiques (octets envoyés et émis) par le routeur Wifi, les temps de connexion....

## 6.12. Sécurité des réseaux sans fils

### 6.12.1. Introduction.

Installer un réseau sans fil (Wlan) implique la sécurisation du réseau pour éviter son utilisation de l'extérieur par des personnes "non-admises": utilisation de votre connexion Internet ou même piratage complet de votre système par une personne mal intentionnée. Rien ne sert de protéger l'accès à votre réseau interne des intrusions via Internet si le voisin (ou un autre) peut rentrer directement.

Une connexion sans fil utilise différents niveaux :

- le type de connexion
- le canal utilisé
- la divulgation du SSID, le nom du groupe raccordé sans fils
- l'autorisation uniquement de cartes avec des [adresses MAC](#) définies.
- La clé de cryptage

Nous allons utiliser pour cette procédure un pont (répéteur). Le pont va uniquement servir à connecter des PC munis de cartes réseaux sans fil à un réseau local Ethernet standard. La connexion Internet utilisera un routeur Ethernet standard en plus.

#### A) Les types de réseaux sans fils Wifi

	Fréquence liaison hertzienne	Débit maximum	Distance maximum	Remarque
<b>802.11</b>	2,45 Mhz	2 Mb/s	100 mètres	Premier réseau sans fils
<b>802.11A Wifi5</b>	5 à 6 Ghz	54 Mb/s maximum	Jusque 366 mètres à l'extérieur, 91 m à l'intérieur.	Incompatible avec les autres liaisons
<b>802.11B Wifi</b>	2,4 Ghz	11 Mb/s	100 mètres	Liaison sans fils la plus courante en Europe
<b>802.11B+</b>	2,4 Ghz	22 Mb/s	100 mètres	Amélioration du 802.11B et compatible Cryptage sur 64, 128 et 256 bits.
<b>802.11G</b>	2,4 Ghz	54 Mb/s	100 mètres	Compatible 802.11, 802.11B et 802.11B+
<b>802.11G+</b>	2,4 Ghs	108 Mb/s	100 mètres	Version améliorée du 802.11G

Le 802.11A ne travaille pas dans la même zone de fréquence que les autres normes. Un appareil 802.11A ne pourra donc pas se connecter sur un autre type de réseau sans fil.

Pour les autres liaisons, il y a une compatibilité ascendante. Un appareil de connexion en 802.11G+ adaptera sa vitesse si une carte réseau en 802.11 tente de se connecter par exemple, et

ainsi de suite.

## B) Les canaux de communications.

Une connexion sans fil peut utiliser un canal parmi 13 (de 1 à 13). Pour une communication entre 2 appareils sans fils, les canaux doivent correspondre. Certains appareils détectent automatiquement le canal.

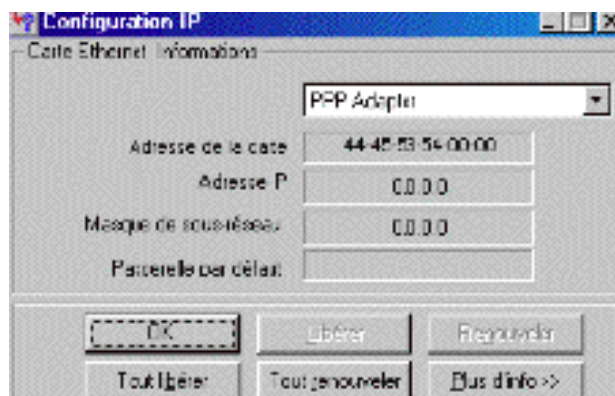
## C) Le SSID

Le SSID est un genre de nom de groupe de la connexion sans fil, le groupe de travail. Un appareil sans fil ne peut se connecter que s'il est du même groupe que l'équipement à raccorder. Néanmoins, un pont wifi communique par défaut son nom de groupe. De ce fait, tout appareil se baladant dans la zone de couverture détectera ce nom de groupe. Il est néanmoins possible sur de nombreux appareils de ne pas envoyer le SSID. Les appareils déjà configurés avec ce SSID pourront néanmoins se connecter.

## D) L'adresse MAC.

Chaque carte, routeur possède une adresse spécifique et unique que l'on appelle l'adresse MAC. Elle est implantée dans la carte à la fabrication et ne peut donc pas être modifiée. Certains appareils permettent d'accepter des connexions uniquement par des installations dont l'adresse MAC est consignée dans une liste interne. C'est le meilleur niveau de sécurité mais le plus difficile à mettre en œuvre.

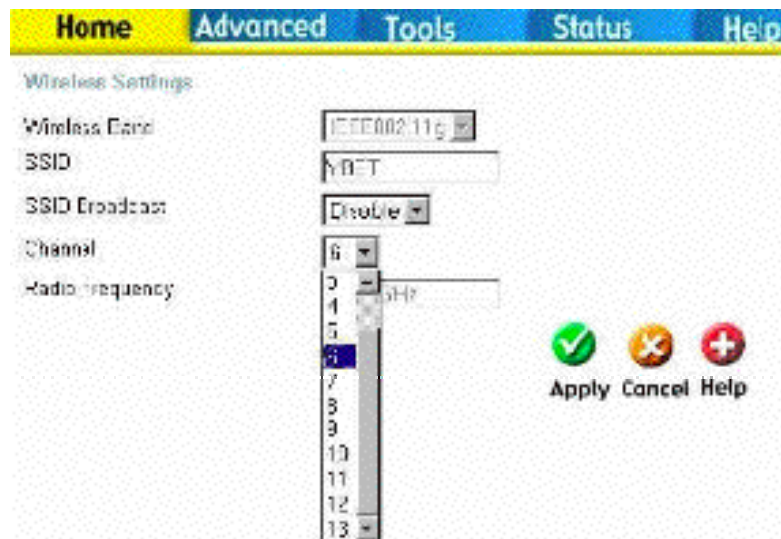
En Win98, l'adresse MAC est donnée par la commande **winipcfg.exe** (Démarrer -> exécuter)



### 6.12.2. Paramétrage d'un point d'accès 802.11G+ D-Link DWL2100AP

Je ne reprends pas ici la configuration complète de l'appareil. Voyons comment sécuriser la connexion sans fil. Je vous passe également les mots de passe,... pour rentrer dans l'administration de l'appareil. Les systèmes sont équivalents dans la majorité des appareils.

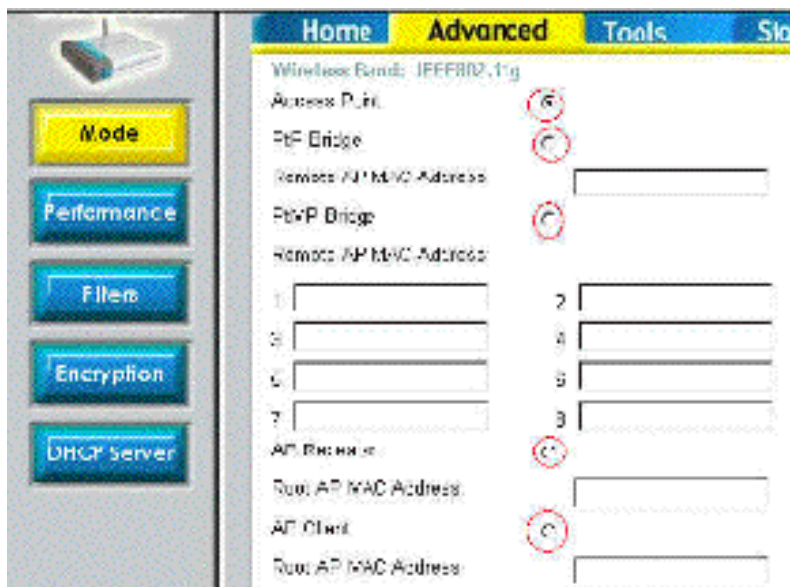




Première fenêtre de configuration, l'accès sans fil. La zone Wireless Band ne peut être modifiée et signale que l'appareil travaille en 802.11G. En effet, le G+ n'est pas (encore) normalisé.

Le **SSID** (ici YBET) est le groupe d'utilisateurs autorisés à se connecter. Par défaut, le **SSID Broadcast** est autorisé (ENABLE). Le pont envoie donc à l'extérieur son groupe via les liaisons hertziennes. Ceci signifie qu'un PC dans le rayon de l'appareil détectera le réseau par son nom de groupe. Il est ici interdit (DISABLE). L'appareil ne communique pas son nom de groupe à l'extérieur. Par contre, un PC programmé avec ce groupe pourra se connecter. Il y a néanmoins un décalage de quelques secondes entre la mise en route de la liaison sans fil et la connexion effective. DISABLE est donc nettement préférable pour la sécurisation du réseau qui sera inconnu de l'extérieur.

Le Channel (canal) est celui utilisé par la communication. Normalement, les appareils doivent obligatoirement être dans le même canal. Néanmoins, certains équipements font un scannage de tous les canaux disponibles (DWL-610 par exemple). Ce n'est donc pas en elle-même une sécurité suffisante.



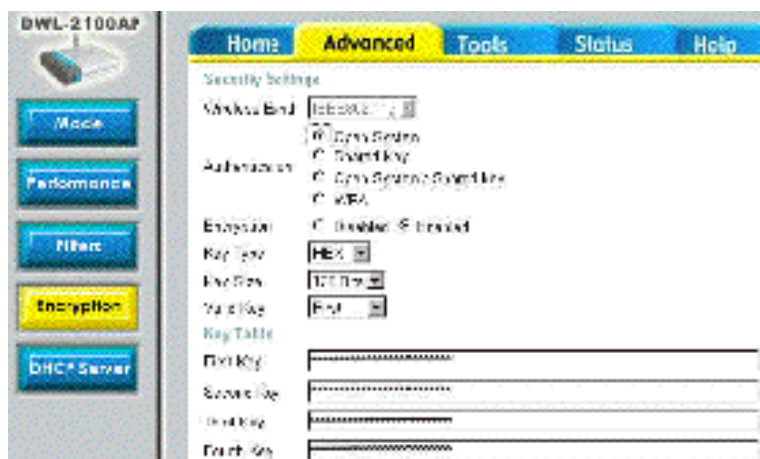
La page suivante reprend des configurations particulières:

Access Point	PtP Bridge	PtMP Bridge	AP repeater	AP Client
Mode par défaut, permet la connexion de PC au réseau sans fil	Connexion de 2 points d'accès entre eux. Par exemple, 2 bâtiments.	Connexion de plusieurs points d'accès sans fils.	Cette configuration permet au DWL-2100 AP de fonctionner comme un répéteur et d'augmenter la distance de transmission	Configuration comme client sans fils. Dans ce mode, le DWL est vu comme un simple appareil sans fil.
	L'adresse MAC de l'autre équipement doit être indiquée. La connexion est donc uniquement entre 2 appareils, à l'exclusion de PC.	Les adresses MAC des autres points d'accès (à l'exclusion des PC) ne sont pas obligatoires mais fortement conseillées.	Dans ce mode, l'adresse MAC de l'appareil de connexion sans fils qui est connecté doit être rentrée. Ceci n'est pas lié à la sécurité mais pour éviter des interférences.	L'adresse MAC du point d'accès (un autre appareil connecté en access Point) doit être rentrée.

Nous ne nous intéressons qu'au mode "Access Point", le plus courant.



La fonction Filtrage (Filters) va permettre d'autoriser uniquement des cartes d'adresse MAC prédéfinies. C'est pour rappel, le niveau de sécurité le plus élevé.



Dernière commande de sécurité, l'encryptage. Un réseau utilisant cette protection utilise une clé de chiffres hexadécimaux ou ASCII. Pour rappel, l'hexadécimal utilise une base 16, tandis que les codes ascii (utilisés pour les lettres) une base 8.

**Open System:** Dans ce cas toutes les stations peuvent se connecter (sauf filtrages plus haut) mais doivent utiliser la même clé que l'appareil si l'option est Enabled comme ci-dessus.

**Shared Key:** Ceci nécessite l'implantation d'un protocole spécial, le PAE. C'est l'ordinateur serveur qui va accepter la connexion de l'utilisateur et renvoyer la clé de cryptage au client. Le serveur doit être renseigné au point d'accès.

**WPA (Wi-fi Protect Access):** Le WPA est une norme de sécurité non standardisée. Elle est remplacée depuis juin 2003 par la norme **IEEE 802.11i** et permet de changer automatiquement la clé de chiffrement. La norme suivante (802.11X) permettra encore une meilleure sécurisation des connexions par certification utilisateurs.

**Le chiffrement:** La première sécurité est d'activer (enabled) cet encryptage. Le choix peut être dans cet appareil en hexadécimal ou en ASCII. Généralement, dans les cartes réseaux, seul l'hexadécimal est utilisable.

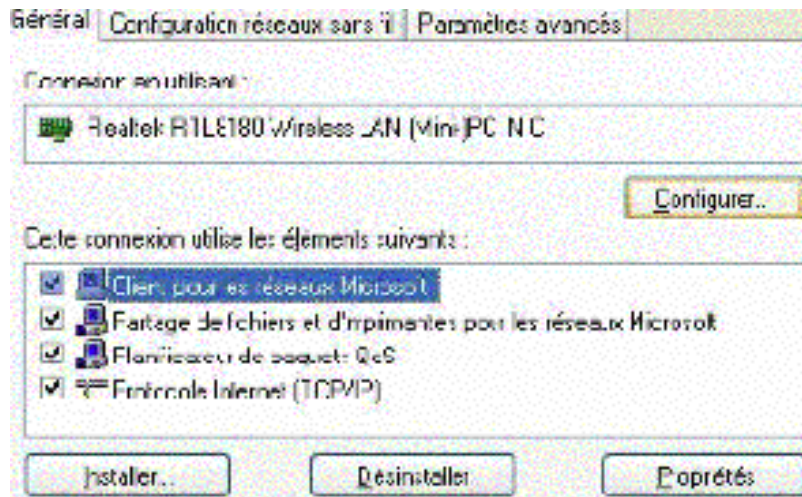


Le cryptage peut être avec une clé de 64, 128 ou 256 bits (la dernière est la plus souvent implantée dans les cartes réseaux actuelles). Plus la longueur de la clé est grande, plus la "découverte" de la clé est difficile et donc meilleure est la sécurité.

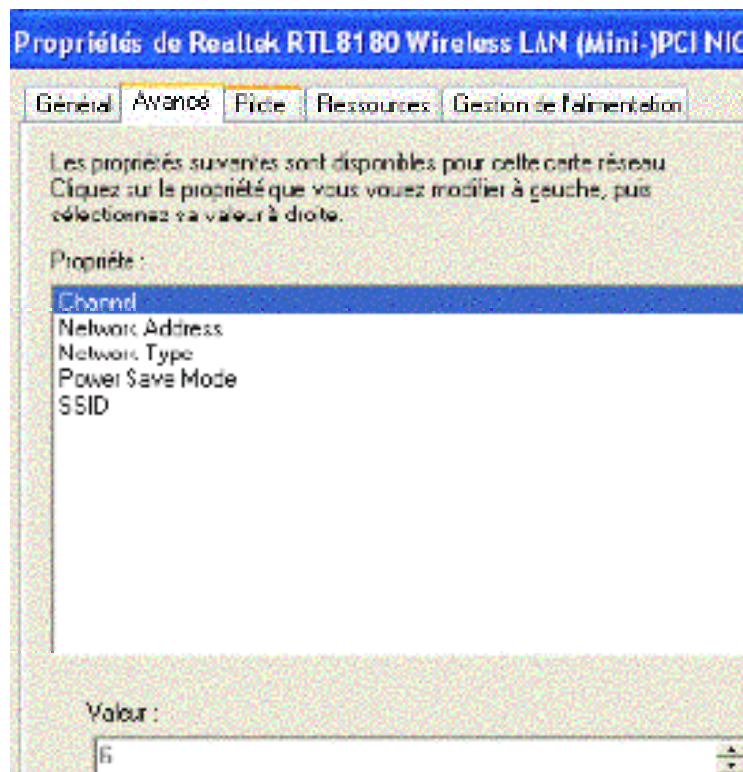
L'option suivante permet d'utiliser 4 clés de sécurité. Néanmoins, l'option VALID Key ne permet de n'en utiliser qu'une à la fois. **L'utilisation de 4 clés est donc nettement optionnelle.**

### 6.12.3. Configuration d'une station

Voyons maintenant la connexion d'une station, ici un portable avec carte réseau intégrée sous Windows XP home.



Nous utiliserons directement les fonctions fournies par Windows XP. Comme les propriétés du réseau ne sont pas différentes d'un réseau Ethernet normal, nous ne nous intéressons qu'à la configuration de la carte (Configurer).

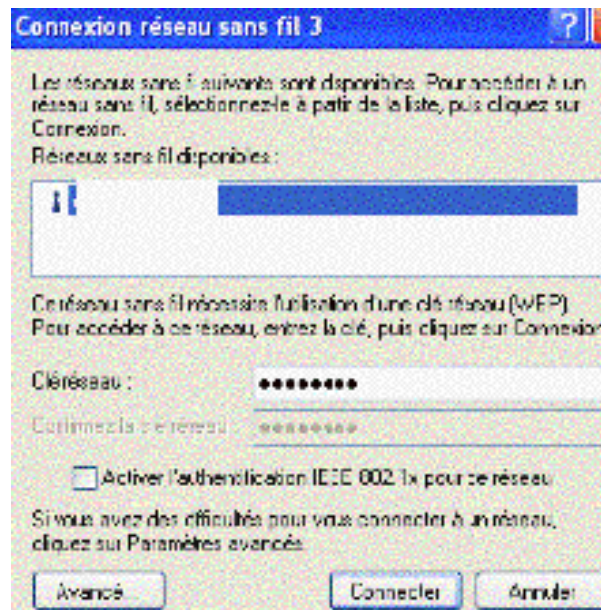


La configuration est assez réduite. Néanmoins, on retrouve:

**Channel**, le canal de communication identique à celui du point, ici 6. **Network Type** est de type infrastructure pour une connexion sur un point d'accès. Le **SSID** est repris ici et permet de déterminer le groupe de connexion.

Ce n'est pas tout. Dans les connexions réseaux, utilisons la touche contextuelle pour sélectionner la fonction "Afficher les réseaux disponibles"





Cette fonction permet d'afficher tous les réseaux sans fil disponibles (qui transmettent leur SSID). Ici, le SSID est donné à la carte réseau puisque nous avons sélectionné **NE PAS TRANSMETTRE LE nom du réseau** par le pont Wifi. La clé réseau doit être identique à la clé sélectionnée dans le pont.

L'authentification par 802.11X ne doit être cochée que si vous utilisez sur le pont le mode Shared Key, les clés sont automatiquement fournies par le serveur et nécessitent l'implantation du PAE.

#### 6.12.4. En conclusion.

La **configuration** d'un réseau sans fil passe par:

- Choix du canal
- Choix du SSID

La **sécurisation** du réseau sans fil demande

- Pas de transmission par le pont du SSID
- Clé réseau, si possible 128 bits
- Filtrage des adresses MAC autorisées à se connecter

Ceci n'est qu'à **la limite du suffisant**. En effet, des logiciels permettent d'analyser les **trames** (les messages) et ainsi de détecter les informations dans les messages (login, mots de passe,...). Parmi ces logiciels, on retrouve Wi-Fi Scanner et Airport sous Linux, Net Stumbler (Windows) et même Mini Stumbler pour les PocketPc. Bref, les possibilités sont nombreuses et seule l'utilisation des adresses MAC autorisées permet réellement de sécuriser un réseau sans fil. La solution de sécurité de cryptage (clé réseau) utilise le WEP (Wired Equivalent Privacy). Selon des études récentes, **ce n'est pas une réelle sécurité**. Le chiffrement est facilement déterminable par des professionnels

Pour les réseaux hautement sensibles, l'utilisation d'un VPN est également une source supplémentaire de sécurité. Le VPN se branche alors entre la borne de réception sans fil (ici le DWL-2100AP) et le switch de connexion au réseau Ethernet. Pour rappel, le VPN encapsule des paquets IP chiffrés (en-têtes et données) dans d'autres paquets qui transitent entre 2 stations.

Pour une réelle sécurité, il faudra attendre l'arrivée de la norme informatique de sécurité **802.11X** qui permettra l'authentification des utilisateurs avec le protocole **EAP** (Extensible Authentication Protocole), en plus du cryptage des informations. Dans ce cas, l'accès n'est autorisé que si l'utilisateur est enregistré sur un serveur RADIUS (Remote Authentication Dial-In User Service) tel que le logiciel libre Free Radius. Ce logiciel fonctionne sous Windows 2000 serveur et Win2003 serveur. L'échange préalable du login - mot de passe peut passer par certificat (éventuellement intégré dans une carte à puce) ou plus simplement par l'algorithme MD5 avec une sécurité moindre.

Dans tous les cas de données sensibles, il est préférable de connecter l'installation sans fil comme liaison extérieure du firewall, par exemple entre le firewall et la connexion ADSL. Ceci implique forcément l'utilisation d'un VPN.

## 7. Monter un petit réseau

### 7.1. Introduction

Avant de rentrer dans **des détails techniques**, commençons par voir les types, possibilités et avantages des réseaux. Les réseaux permettent de connecter des ordinateurs entre eux. Le cas le plus courant actuellement est Internet. Vous vous connectez à l'aide d'un modem sur un réseau formé d'une multitude d'ordinateurs reliés par des lignes téléphoniques à grande vitesse. Ce n'est pas le cas qui nous intéresse ici. Voyons les réseaux plus généraux qui permettent de partager des ressources.

Sur un réseau, on distingue les serveurs qui partagent leurs ressources et les clients qui utilisent les ressources des serveurs. Par ressources, on entend: dossier ou disque dur complet, imprimantes, modem, scanner, bandes de sauvegarde, ... Ceci est le cas général. Dans le cas d'appareils courants, les périphériques effectivement partagés sont les disques, imprimantes et dans quelques cas modem. Les autres nécessitent des appareils spéciaux (dédiés pour le partage) ou des gestionnaires de réseau (système d'exploitation de type lourd: Windows NT ou 2000 serveurs et Netware). Nous n'en parlerons pas pour nous concentrer sur les réseaux de type Win95/95/me et éventuellement Windows 2000 clients.

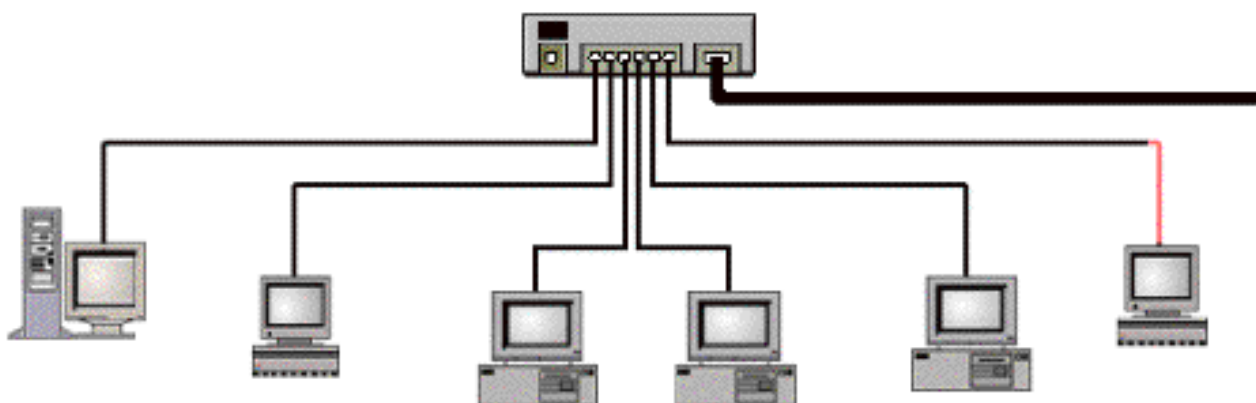
### 7.2. La liaison physique

Pour connecter des PC, nous devons insérer dans chaque ordinateur une carte réseau. Cette carte réseau peut être Ethernet 10 ou Ethernet 100. La différence est au point de vue vitesse, vous l'avez compris: 10 Mb/s pour Ethernet 10 et 100 Mb/s pour Ethernet 100. Divisez par 10 pour obtenir la vitesse de transfert effective. Certaines cartes Ethernet 100 acceptent de travailler en 10. Après le choix des cartes réseaux, reste le câblage.

En Ethernet 10, nous avons 2 possibilités:

**soit en câblage coaxial.** Le câble est presque identique à un câble de télévision et est muni à chaque extrémité d'un connecteur BNC. On relie le câble à la carte réseau via un connecteur en "T". Chaque PC est relié à la suite de l'autre. Au deux extrémités de la ligne, on place une terminaison. La vitesse maximum est de 10 MB/s, la distance maximum entre 2 PC est de 100 mètres. Ceci est théorique, mais quelques installations dans la région utilisent des distances supérieures.

**Soit en RJ45.** L'installation nécessite l'utilisation d'un appareil spécial appelé HUB. Ceci est un câblage en étoile.



La distance est également au maximum de 100 mètres entre une station (ou un serveur) et l'UPS, mais les problèmes commencent à 50 mètres. Dans une entreprise de la région, un technicien d'une autre firme a fait des tests avec un appareil spécial et les surprises ont commencé quant à la qualité des liaisons. Remarquez que certains UPS 10 Mb acceptent les RJ45 et une liaison coaxiale, ce qui permet de mixer les connexions.

En Ethernet 100, le **câblage est également de type RJ45** et par souci de performances, la distance diminue. L'UPS est ici de type Ethernet 100 mais la majorité des UPS acceptent la connexion de carte Ethernet 10 avec une vitesse réduite pour la connexion forcément.

Pour les câbles RJ45, il est conseillé de les acheter tout fait. J'utilise ci-dessus des UPS, mais on utilise également des switch. Ils sont similaires en apparence mais le fonctionnement est un peu différent. Dans le cas d'un UPS, tous les PC reçoivent les informations et seul le destinataire les décode. Dans le cas d'un switch, celui-ci décode le destinataire et envoie les informations uniquement à celui-ci. Le trafic sur le câble est donc réduit. Des concentrateurs permettent d'augmenter la distance entre stations.

Un dernier type de réseau fait son apparition, le réseau sans fils Bluetooth. Ce réseau sans fils de type hertzien permet d'éliminer le câblage avec une vitesse maximum de 11 Mb/s. Forcément, la technique coûte plus chère.

### 7.3. Le langage de communication

Une fois le câblage déterminé et terminé, il reste la liaison entre les PC. Pour communiquer, les PC doivent utiliser le même langage de communication. En réseau, on appelle cela un **protocole**. Un PC peut utiliser plusieurs protocoles en même temps. Dans des réseaux normaux amateurs, ceci n'apporte aucun intérêt mais augmente le trafic de données sur le câble et donc ralentit la communication. Par contre, sur un réseau d'entreprise, ceci permet de bloquer complètement certains accès ou est même nécessaire. Les protocoles réseaux les plus employés sont:

- TCP/IP: il est obligatoire pour toutes les communications INTERNET mais est également utilisé dans des réseaux internes depuis Win98 par défaut.
- NetBUI: ancien protocole, utilisé par certains programmes.
- IPS/SPX: protocole utilisé principalement par les réseaux lourds Netware de NOVELL

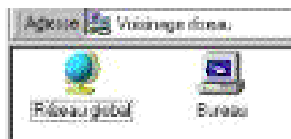
Le protocole le plus utilisé est TCP/IP. Comme TCP/IP est utilisé par Internet, un extérieur pourrait communiquer avec l'intérieur du réseau. Utiliser un autre protocole à l'intérieur diminue les chances de hacking (intrusion). D'autres raisons imposent parfois le multi-protocole. Dans une installation "modem partagé" qui permet via le réseau d'utiliser un seul modem pour accès à l'INTERNET, utiliser un protocole différent (par exemple IPX) sur tous les PC et TCP/IP en plus sur les PC pouvant se connecter sur INTERNET réduit les accès.

### 7.4. L'installation des logiciels.

Commençons par installer les cartes réseaux dans chaque PC et raccordons les câbles. Au démarrage du PC, Win95/98/Me/2000 détecte un nouveau matériel et demande les pilotes spécifiques à la carte (quand il ne les inclut pas directement). Généralement, le système d'exploitation demande également le CD de Windows, quelle que soit la version. Mais que va-t-il installer? Windows installe les parties nécessaires à la connexion. Dans Paramètres, choisissons Réseau (après installation). Les 4 composants d'un réseau sont:



- la carte réseau, mais dans le cas d'Internet également l'accès réseau à distance.
- le client: permet la communication avec d'autres ordinateurs (client pour les réseaux Microsoft et client pour les réseaux Netware).
- le protocole, nous savons déjà que c'est le langage qu'utilise les PC pour communiquer
- le service, comme le partage des disques durs et imprimantes. Ceci est une option.



Sous Windows 95, le protocole est par défaut IPX, il faudra donc si nous voulons utiliser INTERNET cliquer sur le bouton AJOUTER dans paramètres réseaux, sélectionner protocole et dans la catégorie Microsoft sélectionner TCP/IP, éventuellement supprimer IPX. Pour les autres Windows (98/Millennium et 2000), il est sélectionné par défaut.

Comme client, nous sélectionnerons "Client pour les réseaux Microsoft", qui est mis par défaut.

Windows rajoute alors une icône sur le bureau de



type

Si nous cliquons sur celui-ci, la liste des ordinateurs connectés apparaît. Nous verrons plus bas ce qu'il faut vérifier si cela ne fonctionne pas.

Pour ajouter le service "partage des imprimantes et disques (y compris CD-ROM, disquette et zip), il suffit de cliquer sur Partage de fichiers et imprimantes et de cocher les partages que nous souhaitons sur l'ordinateur.

Windows demande de redémarrer, et nous pouvons maintenant paramétrer les partages de disques ou de dossiers. Sélectionnons par exemple un dossier que nous souhaitons partager avec d'autres PC connectés au réseau. Avec la touche droite de la souris faisons apparaître le menu contextuel et sélectionnons partage.

Par défaut, il est non partagé. Nous pouvons le partager en lecture seule (et l'utilisateur pourra copier les fichiers, les lire, mais ne pourra pas directement les modifier sur l'autre PC). Nous pouvons lui donner un accès complet et les autres PC pourront supprimer le fichier, le modifier, ... ou selon un mot de passe pour la lecture ou pour l'accès complet.

Pour avoir l'accès via un autre ordinateur aux dossiers partagés, nous pouvons passer par Voisinage réseau en cliquant sur l'ordinateur souhaité, soit par l'explorateur Windows en sélectionnant également Voisinage réseau.

Le partage des imprimantes est tout aussi facile. Sur le PC où est connectée l'imprimante, sélectionnez-la avec la touche droite de la souris et en sélectionnant partage, cocher la case "Imprimante partagée en tant que". Sur les autres PC, toujours dans Paramètres imprimantes, sélectionnez "Ajout d'imprimante"

Sélectionnez Imprimante réseau (suivant), puis Cliquez sur le bouton "Parcourir pour désigner l'emplacement de l'imprimante (sur quel PC elle est raccordée). Installez les pilotes adéquats.

## **7.5. Le partage de modem pour INTERNET.**

Cette fonction n'est accessible que sous Win98 seconde édition et sous Win Millenium. N'utilisez pas le paramétrage automatique de Millenium. Connectez un modem sur un PC, installez-le et dans "Ajout / suppression" de programmes, sélectionnez "Installation Windows" et le groupe "Outils Internet". Cochez la case: Partage de connexion INTERNET

La connexion INTERNET sur ce PC se fait de manière identique à un PC seul. Voyons les autres. Dans "Options INTERNET", sélectionnez l'option "Connexion".

Cliquez sur le bouton "Installer" et cochez la case "Je veux configurer ma connexion manuellement ...".

en utilisant un réseau:

Il suffit alors de suivre les indications par défaut pour reconfigurer les mails, ... Le tour est joué. Un petit problème néanmoins, Vous pouvez démarrer la connexion depuis n'importe que PC, mais la déconnexion doit se faire obligatoirement sur le PC sur lequel le modem est connecté.

## **7.6. Et quand cela ne marche pas?**

Pour qu'un PC soit détecté dans Voisinage réseau, il faut qu'un dossier (ou un disque) ou une imprimante soit partagée la majorité du temps. Deuxièmement, en RJ45, la carte et le HUB sont équipés d'une petite LED verte. Les deux sont allumées en cas de connexion. Les protocoles doivent être les mêmes pour tous les PC qui doivent se reconnaître.

Sous Windows Millenium, n'utilisez pas les paramètres automatiques avec disquettes. Ils ne fonctionnent pas vraiment (c'est un euphémisme), mais faites-le suivant la procédure ci-dessus. En cas de problème, dans la configuration réseau, supprimez tout, redémarrez le PC et refaites un paramétrage manuel.

Pour le partage de modem, le système d'exploitation doit être Win98 SE ou Millenium. Si un PC au moins est sous Windows Millenium, c'est lui qui doit partager le modem.

## **7.7. Et en réseaux lourds.**

Si vous souhaitez vous connecter sur des réseaux lourds (Windows NT, Windows 2000 server ou Netware), vous devez obligatoirement donner un nom et un mot de passe au démarrage. Ceux-ci doivent correspondre à ceux fournis sur le serveur.

Les réseaux lourds permettent avec des versions de logiciels spécifiques d'accéder aux mêmes données via plusieurs PC en même temps. Le PC connecté au magasin peut gérer les factures, stocks, ... en même temps que les autres PC connectés sur le réseau, mais ceci dépasse le cadre de cet article.

## 8. Dépannage réseau

### 8.1. Rappel.

Un réseau local permet de connecter plusieurs PC entre eux pour partager les ressources (imprimante, modem, données et répertoires du disque dur,...) ou partager une connexion INTERNET. La connexion entre 2 ordinateurs nécessite la comptabilité entre:

- le support de communication (câble, liaison sans fil)
- les cartes réseaux (spécifique selon le câblage) mais généralement Ethernet
- le programme de gestion (système d'exploitation)
- le protocole. Le protocole est le langage utilisé par le programme de gestion pour communiquer entre les ordinateurs. Le langage le plus utilisé actuellement est le TCP/IP. D'autres existent mais ne peuvent être utilisés sur INTERNET: NetBui, IPX (réseaux Novell avant Netware 4.1).

Si vous avez installé un firewall, avant de tester l'ensemble de l'installation, commencez par vérifier les configurations du firewall, ou du moins désactivez-le pour les tests. Ceci est surtout valable pour Windows XP qui inclut ce genre de programme en standard.

Un dépannage réseau complet serait trop complexe mais voici déjà quelques pistes pour des réseaux TCP/IP

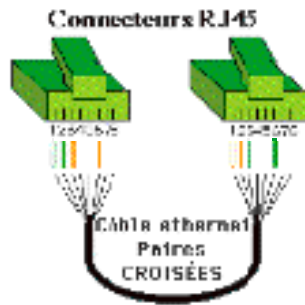
### 8.2. Dépannage

#### A. Dans "Voisinage réseau", le PC ne se reconnaît pas lui-même.

- Vérifiez si le partage disque dur / imprimante est activé pour cet ordinateur.
- Carte réseau et connexion OK: en RJ45, vérifiez les LED sur le HUB (switch) **et** sur la carte réseau. A de très rares exceptions prêt (faux contact dans les connecteurs RJ45, inversion de câble avec des switches de très bas de gamme) ceci signifie que la connexion réseau est bonne.
- Vérifiez si le pilote de la carte réseau est le bon (notamment lors d'une détection automatique de Windows). Généralement, un pilote non adapté spécifique à la carte fonctionne mais les connexions sont ralenties.
- Attention aux nombreux problèmes de câblage (paires respectées, éloignement des fils du réseau électrique,...)

#### B. Dans "Voisinage réseau", le PC se reconnaît lui-même. Dans ce cas, le pilote de la carte réseau est correct.

- Dans le cas d'un branchement direct réseau entre 2 ordinateurs (sans switch), le câble doit être croisé. Ce même câble doit être utilisé pour relier 2 concentrateurs (hub, switch, routeur) entre eux. Dans le cas d'un PC branché sur un concentrateur, le câble doit être droit.



Commencez par déterminer l'adresse IP sur chaque PC. Utilisez pour cela la commande DOS "IPCONFIG".

```

C:\WINDOWS>IPCONFIG
Configuration IP de Windows 98
E - Carte Ethernet :
    Adresse IP. . . . . : 0.0.0.0
    Masque de sous-réseau . . . : 0.0.0.0
    Passerelle par défaut . . . :
I - Carte Ethernet :
    Adresse IP. . . . . : 192.168.1.152
    Masque de sous-réseau . . . : 255.255.255.0
  
```

Faites ensuite un ping XXX.XXX.XXX.XXX ou les X sont l'adresse de chaque PC à partir des autres (ping est un programme DOS). Dans l'exemple ci-dessus, tapez à partir des autres PC **ping 192.168.1.152** . Ceci permet de déterminer si les PC sont en communication et donc si la connexion (câble, switch ou hub,...) est correcte. Dans le cas de 2 PC connectés en direct, le câble doit être croisé. Pour rappel, pour que 2 stations puissent communiquer entre elles sans passer par un routeur, les stations doivent être dans la **même classe d'adresse**.

Dans Paramètres / réseau, vérifiez si le groupe de travail est le même pour les 2 ordinateurs.

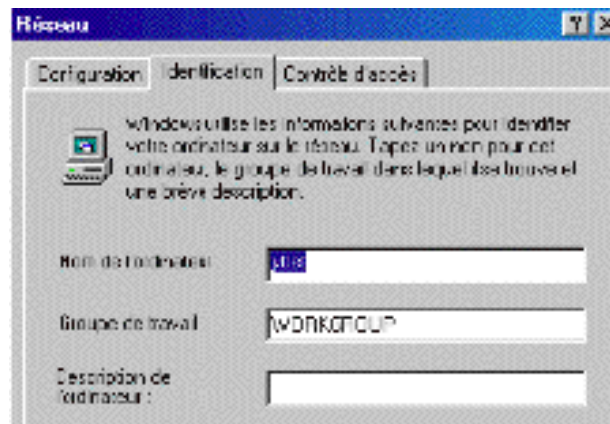
Message mot de passe non valide: "vérifiez votre login / mot de passe", en correspondance sur le serveur. Sur serveur WinNT ou 2000, utilisez déconnexion dans le menu Démarrer pour ouvrir une autre session (avec mot de passe).

Dans les paramètres réseaux, vérifiez les protocoles sur chaque machine (TCP/IP le plus courant, mais pour certains programmes ou configuration: NetBui, IPX).

Si vous avez attribué des adresses IP fixes, elles doivent être dans la même **classe d'adresse** mais différentes (sinon, message conflit d'adresse). Par exemple: 192.168.1.5 et 192.168.1.20. Essayez la commande DOS ipconfig.exe pour déterminer les paramètres TCP/IP. Vous pouvez également utiliser la commande DOS Ping (TCP/IP) pour vérifier si le PC est bien connecté. Par exemple Ping 192.168.1.5

En mélange Win95/98/Me, n'utilisez pas les paramétrages automatiques par disquette proposés par Windows! Ils ne fonctionnent qu'avec le même système d'exploitation

**Aucun autre PC détecté:** vérifier le groupe de travail dans les propriétés réseaux.



**Firewall logiciel installé.** Vérifiez s'il ne bloque pas ces connexions. Pour rappel, Windows XP inclut d'office un firewall (même si ses performances sont ...)

### C. Problèmes de communication.

Sont rassemblés ici quelques problèmes liés à l'expérience dans des problèmes de communication aléatoires.

La connexion réseau fonctionne mais est lente. Ce problème peut venir d'une quantité de raisons: pilote carte réseau, câblage,...

. Le **pilote de la carte réseau** doit être celui fourni par la carte. Ce problème survient notamment avec les cartes utilisant un circuit Railtek. Même si le circuit électronique est le même, utiliser un pilote "équivalent" provoque souvent des ralentissements aléatoires.

. Les **règles de câblage** doivent être respectées: respect des paires, longueur inférieure à 100 mètres, pas de passage près des fils électriques et Néons.

## 8.3. Quelques commandes DOS réseau

L'ensemble des X est remplacé par l'adresse de destination IP ou par le nom du site

**PING** XXX.XXXX.XXX.XXX (sous DOS) pour vérifier la communication. Si les PC ne sont pas dans la même classe d'adresses, le ping fonctionne mais pas la connexion.

Connaître l'adresse IP d'une station **IPconfig** (sous DOS)

Quels sont les PC connectés **NET View** (sous DOS)

D'où vient la connexion et par quel chemin: **Tracert** XXX.XXX.XXX.XXX (sous DOS)

**Winipcfg** (par exécuter, commande Windows), affiche l'adresse MAC et l'adresse IP.

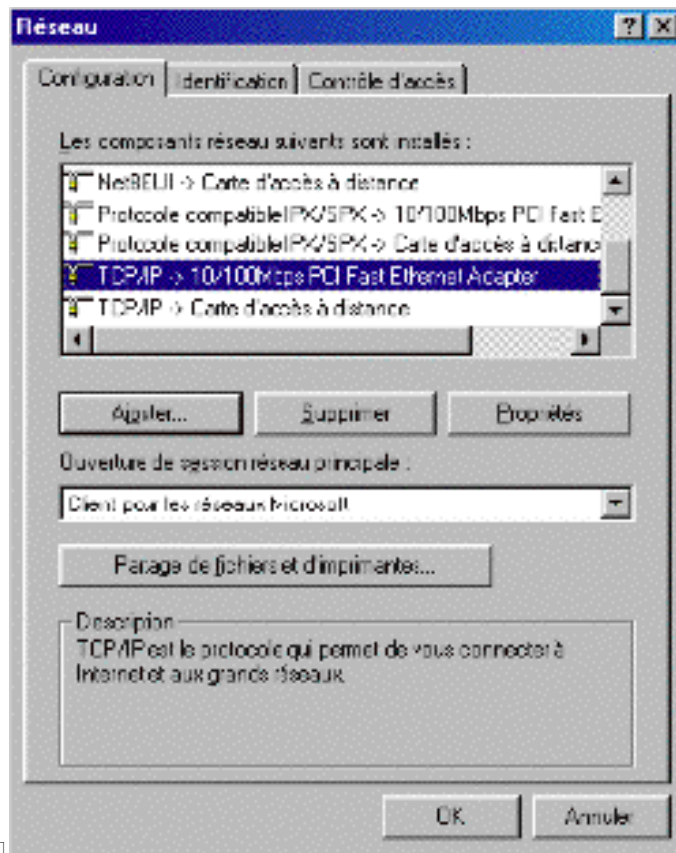
## 8.4. Partage de connexion INTERNET.

Avant de vérifier le partage, les PC connectés entre eux pour le partage doivent se reconnaître.

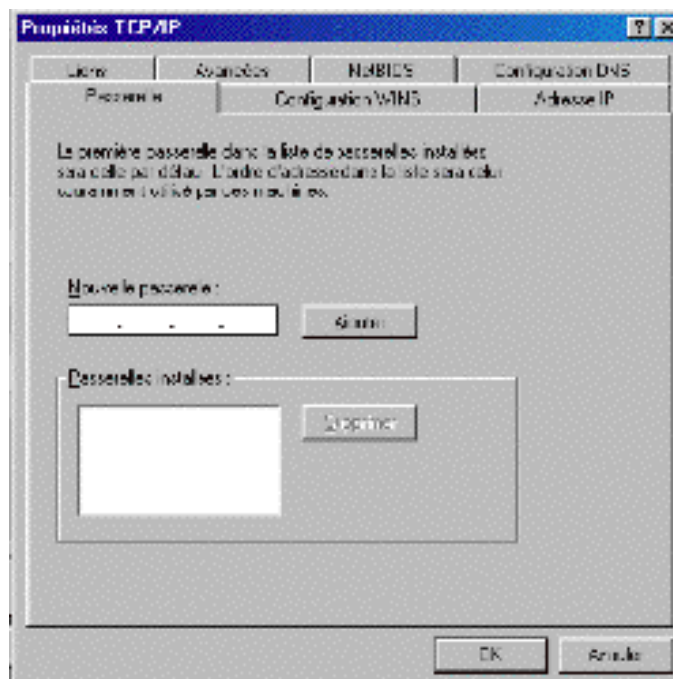
- PC dans la même classe d'adresse (y compris adresse interne du routeur). Si ce n'est pas

le cas, le réseau ne fonctionne pas.

- Protocole IP utilisé pour tous les PC. Ce protocole est utilisé par défaut pour tous les systèmes d'exploitation Microsoft sauf Windows 95 (à rajouter par Démarrer -> Paramètre -> Panneau de configuration -> Réseau).

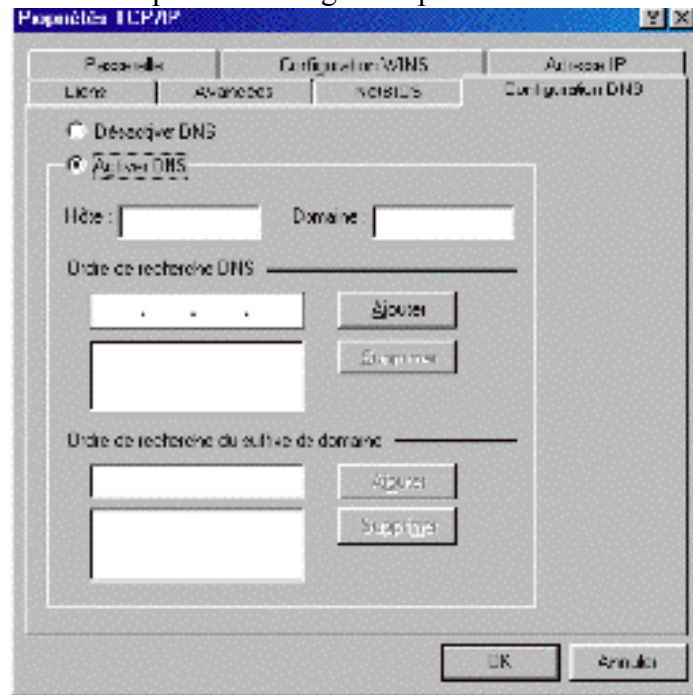


Dans les propriétés de TCP/IP -> carte réseau: La passerelle doit souvent être renseignée. L'adresse de la passerelle est celle du PC qui partage la connexion (partage par Windows) ou celle du routeur. Parfois cela fonctionne sans, parfois non. Généralement je la mets.



De même les paramètres DNS primaire et secondaire doivent souvent être activés sur les PC.

Ils sont fournis par le fournisseur d'accès. La fenêtre ci-dessous provient d'un Win98. Hôte et domaine peuvent être inventés dans notre cas. Par contre, en Win 2000 et XP, si le réseau interne est important, le nom de domaine peut être obligatoire pour le réseau interne.





## 9. Exercice: architecture d'un réseau d'entreprise

### 9.1. L'exercice

Voyons un cas concret de l'architecture d'une installation réseau (appareils à mettre en oeuvre) dans une entreprise.

2 bâtiments à connecter distants de 80 mètres (pas de chance, une route au milieu). Chaque bâtiment dispose de deux étages avec 2 départements différents (soit 4 départements). Je veux absolument des niveaux de sécurité (hardware) pour que chaque PC d'un département ne puisse (sauf autorisation par station de travail) se connecter sur un autre département. Cette solution de protection sera en pratique couplée avec des protections logicielles.

Les départements sont :

1. **Bâtiment 1**: 80 PC de fabrication (pas d'accès INTERNET) et 1 serveur avec un logiciel dédié. Distance maximum avec le serveur 100 mètres que nous appellerons **Fabrication**. Ce département rassemble la fabrication, les stocks, gestion des transports,... C'est le département à protéger. Un arrêt d'usine de 1 heure coûte nettement plus chère à l'entreprise qu'un arrêt de 2 jours de la comptabilité.

2. **Bâtiment 1**: 10 ordinateurs de gestion de commandes et 1 serveur dédié. Certains d'entre eux peuvent avoir accès au service du serveur de la fabrication sur un rayon de 30 mètres. Pas d'accès INTERNET, ni vers le bâtiment 2. Nous appellerons ce département **Commande**

3. **Bâtiment 2**: 10 PC administratifs: direction, comptabilité, ... sur un rayon de 30 mètres. Nous appellerons ce département **Administration**

4. **Bâtiment 2**: 10 commerciaux. et services divers sur un rayon de 30 mètres. Nous appellerons ce département **Commercial**.

Le bâtiment 2 abrite un petit serveur de fichier (documents Word, Excell,...) et un serveur d'application (comptabilité), appelé **serveur administratif**. Certains PC peuvent avoir accès au serveur "gestion de commande". Le bâtiment 2 (administration et commercial) doit avoir un accès sécurisé sur INTERNET via une ligne ADSL. Il doit être possible pour les commerciaux de se connecter au serveur de l'entreprise à distance via INTERNET.

Je ne parle pas de sécurité via mots de passe, mais bien par des paramétrages TCP/IP ou des matériels informatiques. C'est nettement plus sûr, même si les mots de passe utilisateurs sont loin d'être facultatifs.

Donnez le schéma de l'installation reprenant les serveurs, concentrateurs utilisés (hub, switch, routeur, nombre de ports), types de liaisons, câbles droits ou croisés, ... Dans le cas où vous utilisez un HUB ou un switch, expliquez. Je ne demande pas explicitement la marque et l'appareil de chaque concentrateur. Attention : un switch de 80 ports, ce n'est pas courant, manageable?

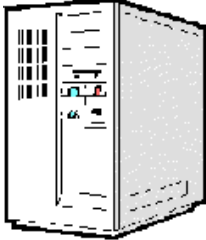






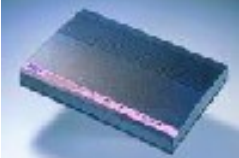



L'installation du réseau doit être complète, pensez aux sécurités à installer (protections électriques, sauvegarde) et aux types de serveurs utilisés. Comme le matériel informatique réseau peut tomber en panne, le matériel doit être standardisé (par exemple les switches) pour que l'on puisse utiliser un minimum de matériel de réserve: maximum de concentrateurs de même type et capacité pour l'ensemble du réseau pour n'utiliser qu'un appareil de remplacement pour toute l'entreprise. Je ne demande pas les paramétrages des appareils, juste la structure du réseau ethernet.



Ne vous occupez pas trop du budget, mais choisissez les caractéristiques en gestionnaire informatique responsable (pas la peine d'utiliser de l'Ethernet Gigabit sur fibre optique pour connecter les stations).



## 9.2. L'architecture globale.

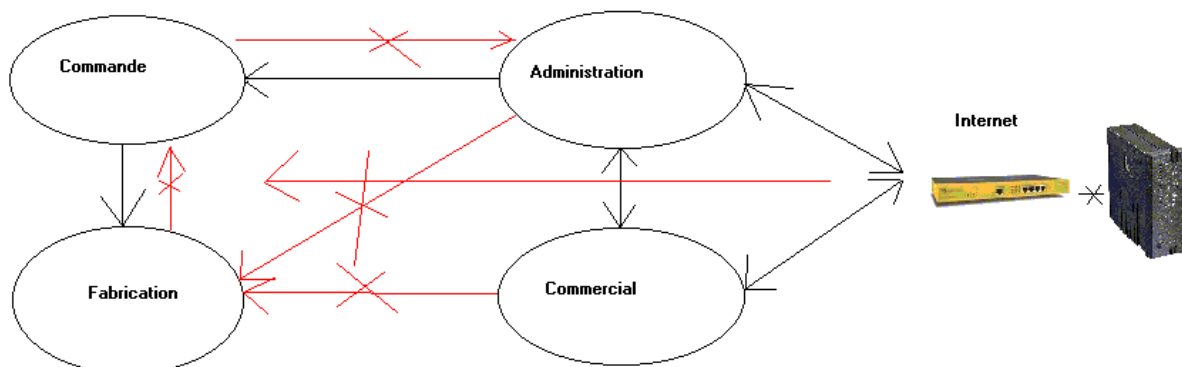
Pour faciliter la mise en place de l'architecture de notre réseau, examinons les appareils à mettre en oeuvre. Nous utiliserons les dessins suivants pour faciliter l'analyse du schéma global du réseau.

			
<p>Serveur</p>	<p><a href="#">Switch</a> ou <a href="#">Hub</a> Ethernet (ici un des1024d de Dlink 24 ports 10/100)</p>	<p>Switch manageable: autoriser (ou bloquer) certaines connexion de PC vers PC (ou plutôt de groupes de PC), en plus des mots de passe sessions utilisateurs gérés par le système d'exploitation</p> <p>Ici un DGS 3224, 20 ports 10/100 et 2 ports Gigabits en base T (cuivre) de Dlink</p>	
			
<p>Routeur sans fils Wifi, utilisable comme routeur et comme pont. Nous pourrions utiliser un simple switch sans fils dans notre cas.</p>	<p>Un câble RJ 45 croisé</p>	<p>modem routeur ADSL, ici un tornado Copperjet 812. Il peut être utilisé comme simple modem en mode pont</p>	<p>Un firewall - VPN (ici une série 100 de symantec) permet le partage de la connexion Internet et l'accès de l'extérieur au réseau de l'entreprise</p>
			
<p>Routeur firewall intégré permet de sécurisé les</p>	<p>un simple routeur</p>	<p>NAS (ici un série 300 low cost de</p>	<p>Un département avec les PC associés</p>

connexions en bloquant certains ports et / ou certaines plages d'adresses.		IOMEGA)	
			
UPS (ici APC 420W, un peu faible pour un serveur): protection électrique	Sauvegarde sur bande <a href="#">SDLT</a> (ici modèle Quantum)		

Analysons le problème en fonction des différentes parties et des sens de communication autorisées. Ceci va scinder le problème et envisager en gros les appareils à utiliser au niveau connexion, routage et sécurité.

Les départements administration et commerciaux ne sont pas très différents. Ils utilisent tous deux: INTERNET (ce sont les seuls), les mêmes serveurs (un serveur de fichier et un petit serveur d'application). Par contre, un ordinateur de l'administration doit pouvoir se connecter sur le département commande (mais pas sur le département fabrication), le département commercial ne peut en aucun cas se connecter sur les départements commande et fabrication. L'accès à INTERNET vers les serveurs du bâtiment 2 (administration et commercial) nous oblige à utiliser un firewall VPN pour la connexion INTERNET (ici un série 100 de symantec) et un modem ADSL (ici un tornado 812 utilisé en pont. Avec les 20 PC repris dans le bâtiment 2, il n'y a pas besoin d'un appareil très puissant, mais suffisamment sécurisé. Comme l'accès de l'extérieur est possible, la connexion doit être de type IP fixe. Ceci nous donne une bonne marche de manoeuvre pour les connexions.



En noir les communications autorisées (même avec des blocages), en rouge celles qu'il faut bloquer. Ça donne une bonne idée de la structure globale de l'installation. La route entre les deux bâtiments va nous bloquer avec une liaison sur cuivre ou fibre optique. Nous devons déjà utiliser une liaison sans fils, de type WIFI 802.11B à 11 Mb/s (éventuellement 802.11B+ à 22 Mb/s).

Comme les vitesses de communications ne sont pas trop importantes, l'utilisation de 100 base T (éventuellement 1000 Base T pour les serveurs) est suffisante pour l'ensemble du réseau.

### 9.3. Connexion département administratif et commercial

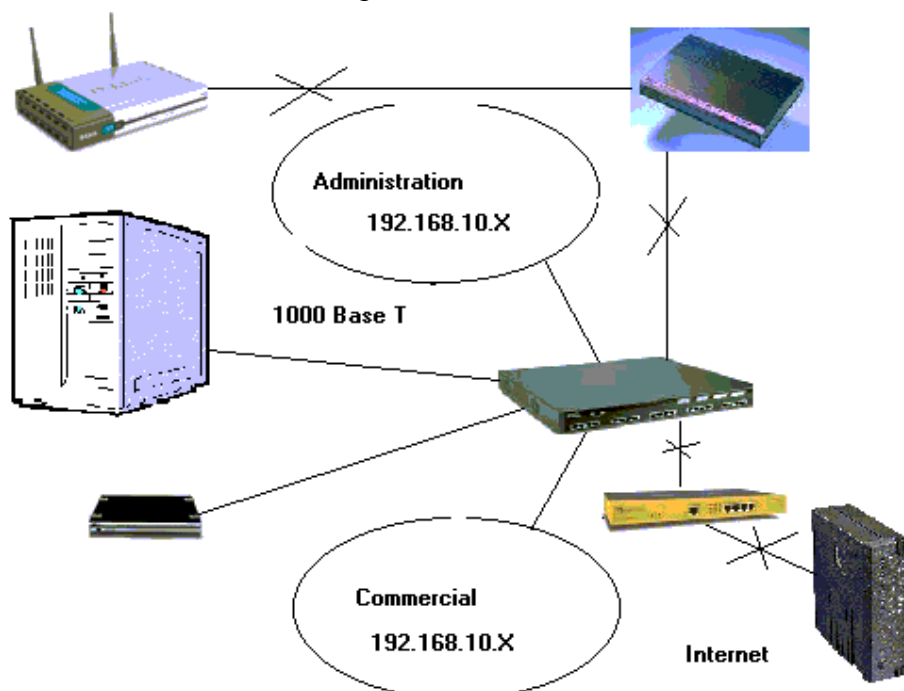
La connexion entre administration et commercial doit laisser passer certaines communications (mais pas toutes). En plus, ils utilisent les mêmes serveurs. Nous pouvons utiliser soit deux classes d'adresses différentes (d'où l'emploi de routeurs pour relier les 2 départements), soit un switch manageable (et donc bloquer ou autoriser certaines connexions) en utilisant la même classe d'adresses IP. Utiliser 2 routeurs pour les communications alourdit directement le paramétrage. Choisissons la solution même classe d'adresse (par exemple 192.168.10.X) pour l'ensemble des deux départements et bloquons les accès au niveau d'un switch manageable.

Les départements utilisent un serveur d'application et un petit serveur de fichier. Comme serveur de fichier, pour réduire les coûts, utilisons un NAS. Comme nous devons connecter 20 PC + 1 serveur + 1 NAS + 1 connexion bâtiment 1, l'appareil représenté (20 ports + 2 Giga) serait insuffisant mais nous pourrions utiliser un switch 8 ports additionnels. Les NAS sont rarement en 1000 Base T.

Pour la connexion vers le deuxième bâtiment nous devons utiliser une connexion sans fils. Comme le bâtiment 2 peut avoir la connexion vers le département commande (pas vers la fabrication) nous allons utiliser des classes d'adresses différentes pour le bâtiment 1. Ceci nécessite l'emploi d'un routeur. Comme la connexion doit être sécurisée (bloquée à partir du bâtiment 1 vers 2) plus l'interdiction de connexion INTERNET vers le bâtiment 2, utilisons un routeur firewall et un routeur 802.11B en pont. Dans ce cas, le firewall ne va pas être utilisé pour bloquer des ports: dans un réseau interne, les ports dynamiques (1024 - 65535) sont utilisés de manière aléatoire pour les communications réseaux internes, nous ne pouvons pas les bloquer. Nous allons uniquement bloquer les communications sur les plages d'adresses. Par exemple bloquer les communications de l'adresse IP du VPN vers le bâtiment 2.

Une autre solution pour bloquer l'accès "Fabrication" - "administratif" serait de sécuriser le réseau sans fils en fonction des adresses mac des PC du département administration

Voici notre schéma matériel réseau pour le bâtiment 2.

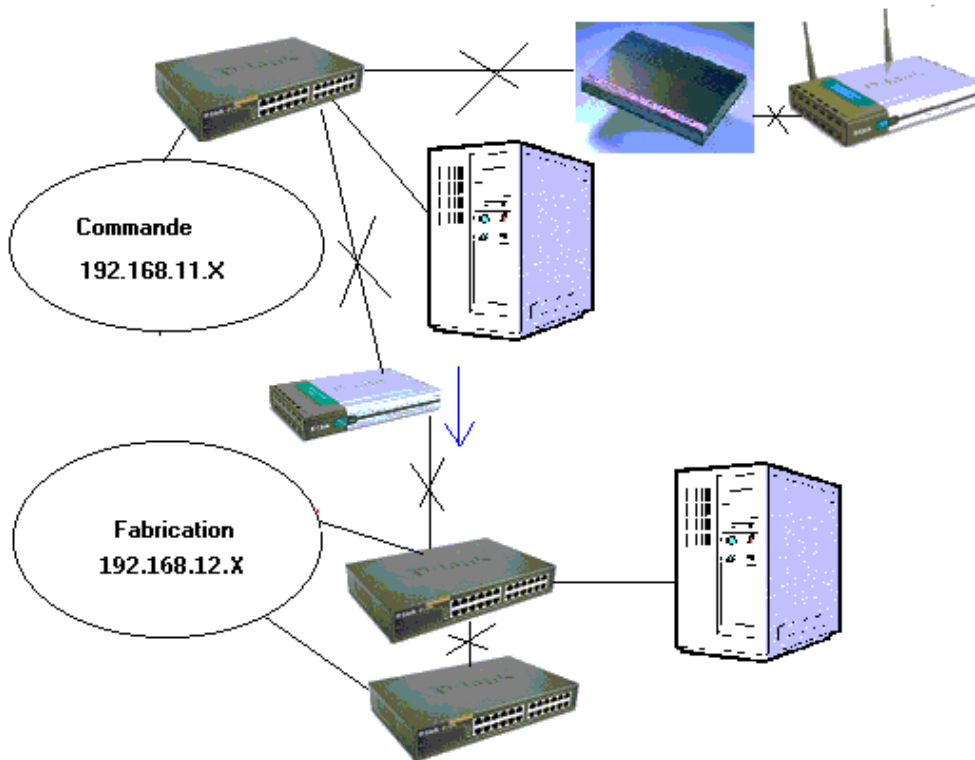


## 9.4. Connexion Bâtiment fabrication - commande

Les communications usine vers commande sont interdites. Seules les communications commande vers usine sont autorisées (sous certaines réserves). Nous avons de nouveau 2 possibilités d'utilisation des classes d'adresses IP. Soit deux classes différentes avec l'emploi de routeur, soit la même classe d'adresse avec un switch manageable (au choix).

### 9.4.1. Cas 1: utilisation de 2 classes d'adresses différentes.

L'utilisation d'un routeur (et donc de 2 classes d'adresses) va augmenter la sécurité. L'utilisation d'un routeur avec firewall n'est pas obligatoire puisque la communication bidirectionnelle nécessite deux routeurs alors que nous utilisons la communication uniquement de commande vers fabrication. Ceci empêche déjà l'usine de se connecter vers le département commande. La sécurité à partir d'Internet est déjà assurée pour rappel avec le VPN et le firewall placé à la sortie du bâtiment administratif vers le routeur WIFI. De même, pour les communications du bâtiment 1 vers le bâtiment 2, nous pouvons soit utiliser un routeur WIFI en mode pont et un firewall (cas ci-dessous), soit un routeur WIFI sans firewall. La sécurité est de toute façon assurée par le firewall de l'autre côté de la liaison sans fils.



Le nombre de switch 24 ports pour la partie fabrication a volontairement été réduit pour la clarté du schéma. Il nous en faudrait minimum 4, voire 5 pour avoir des lignes de réserves. L'utilisation d'un seul switch de 96 ports pourrait poser des problèmes de longueur de câbles et en cas de panne de ce seul appareil, toute la fabrication serait bloquée. L'utilisation de multiples switch 24 ports permet d'en avoir 1 de réserve pour l'ensemble du bâtiment.

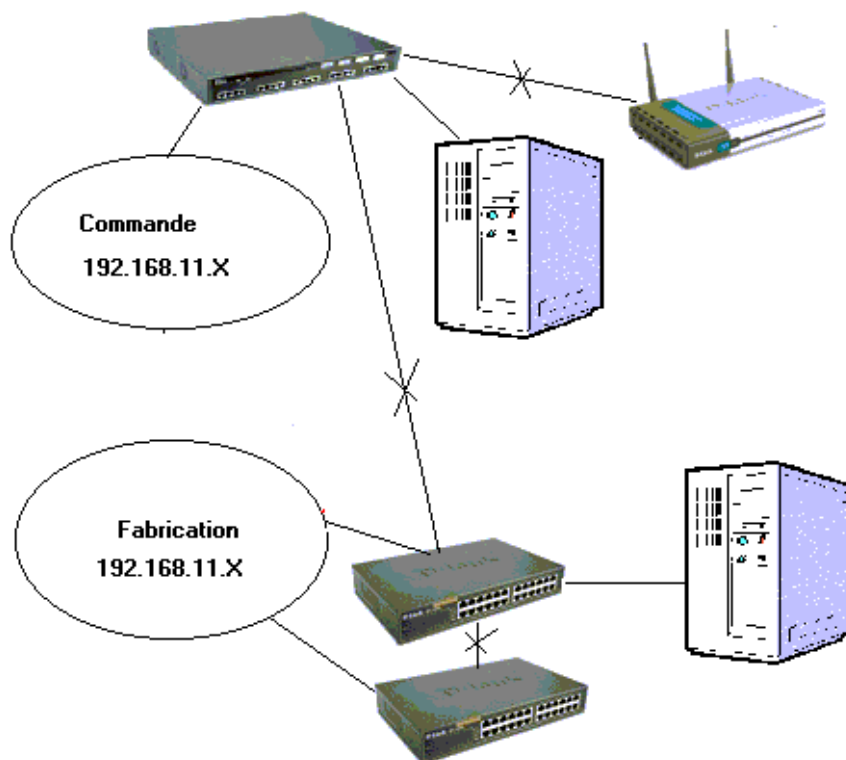
Pour rappel, le nombre de HUBS (moins de contrainte pour les switch) est limité à maximum 2 entre 2 PC en 100 base T (même si plus souvent utilisé), le serveur fabrication **doit être raccordé sur le premier switch** de la fabrication

L'utilisation d'un routeur firewall entre le switch et la connexion WIFI 802.11B n'est pas nécessaire si un firewall est installé de l'autre côté. Ils feraient double emploi (ce qui n'est pas trop

grave) mais obligerait une configuration plus complexe de l'infrastructure.

### 9.4.2. Cas 2: utilisation d'une même classe d'adresse avec switch manageable.

Dans ce cas, tous les PC sont dans la même classe d'adresse, l'utilisation d'un routeur (ou routeur - firewall) n'est plus nécessaire entre les deux départements. , c'est le switch manageable qui va accepter ou bloquer les communications. Dans ce cas (et contrairement à la solution précédente), on peut bloquer les communications de manière hardware entre les PC des commandes et les PC de fabrication).



Cette solution est nettement plus chère (mais plus sécurisée). Elle permet néanmoins de raccorder les serveurs en 1000 base T sur le switch manageable. Les distances entre chaque PC, serveurs et concentrateurs sont respectées puisque qu'en 100 base T en 1000 base T, la distance maximum est de 100 mètres. Pour rappel, **les switch manageables travaillent généralement avec les adresses MAC**. En cas de panne d'un PC avec échange standard (ce qui se fait en pratique pour minimiser l'arrêt), on risque de devoir reprogrammer le switch. Ce n'est pas forcément du niveau de tous les techniciens de maintenance d'usine (sans compter les mots de passe administrateurs pour paramétrer le switch). Par contre, certains modèles acceptent le regroupement de station suivant le protocole IGMP. ("Internet Group Management Protocol", protocole permettant d'envoyer le même message à des machine faisant partie d'un groupe).

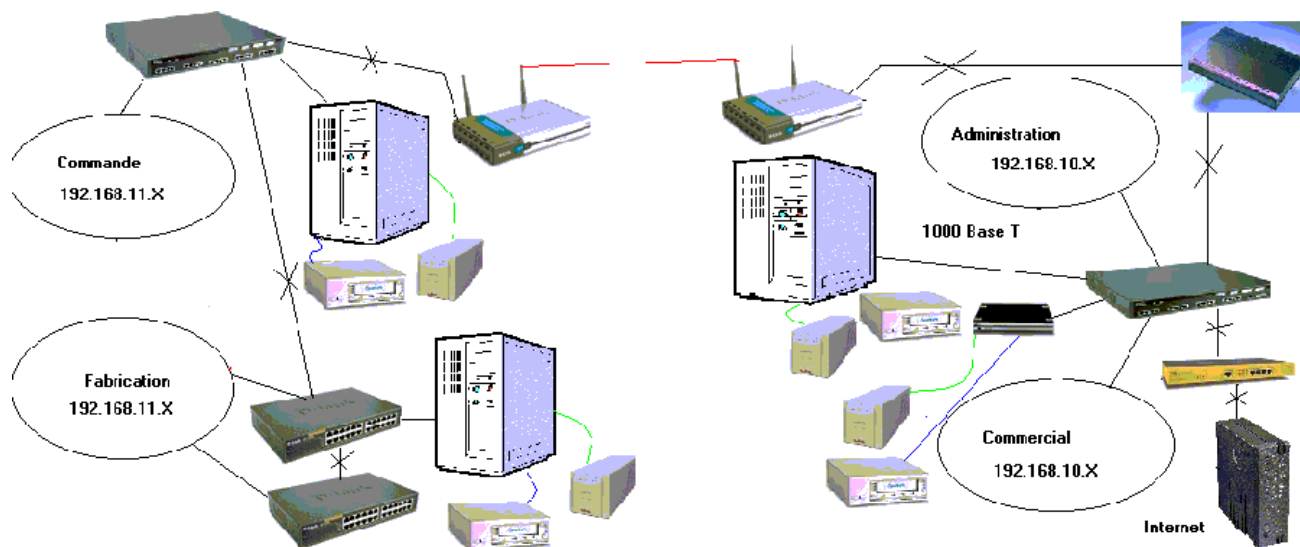
## 9.5. Connexions globales du réseau

Il ne reste plus qu'à relier les 2 réseaux de l'entreprise et positionner nos sécurités (UPS et sauvegarde) et choisir les serveurs.

Les serveurs utilisés pour le bâtiment 2 et les commandes sont en fait de petits serveurs. Par contre, le serveur utilisé en fabrication est un serveur d'application musclé (avec logiciel dédié) de

type bi-processeur. Pour des raisons de sécurité des données, nous utilisons des serveurs SCSI RAID 1 ou mieux RAID 5. Plus le processeur est gros plus il consomme. L'UPS (de type On-Line de préférence) devra être en rapport. Pour rappel, la puissance de l'UPS = puissance consommée par le serveur X 1,6. Pour un serveur consommant 800 W (écran compris), la puissance de l'UPS est donc de  $800 \times 1,6 = 1280$  W.

Pour la sauvegarde des données, nous utiliserons des bandes de type DAT ou Super DLT pour les capacités de ces technologies, mais également au niveau vitesse de sauvegarde.

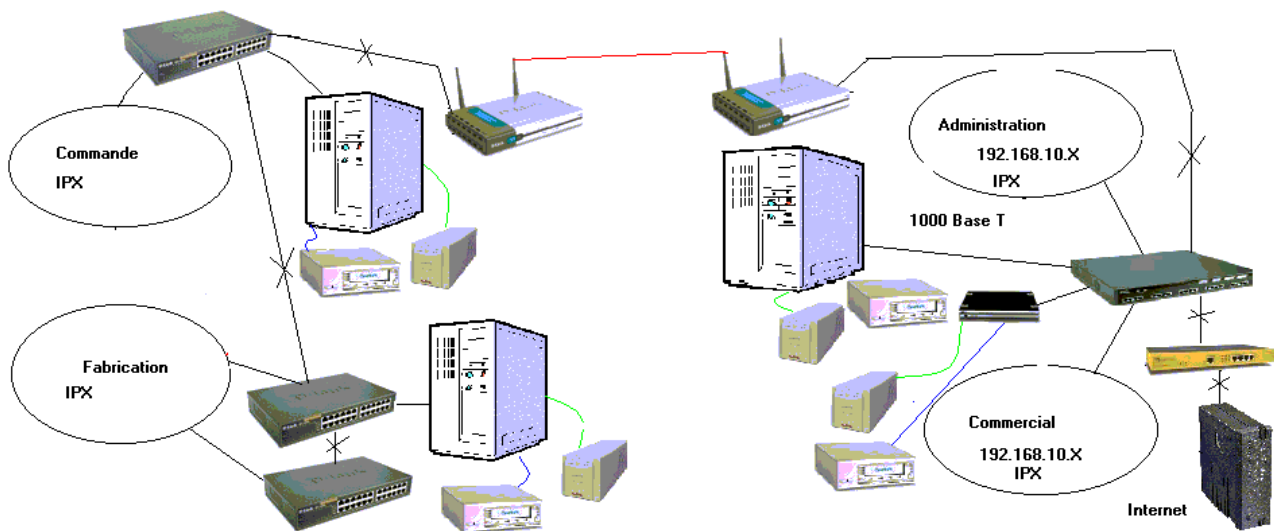


Nous pourrions encore ajouter sur le schéma des petits UPS pour certaines stations ou concentrateurs, selon les desiderata de l'entreprise.

## 9.6. Un autre point de vue de cette connexion: mélange de protocoles.

Dans les montages ci-dessus, nous avons utilisé exclusivement le protocole TCP/IP. Il en existe 2 autres: l'IPX et le NetBeui. Le NetBeui n'est pas routable, l'IPX (utilisé principalement par les réseaux NOVELL), oui. Le schéma suivant va mélanger des protocoles. Pour accéder à un serveur, le PC doit utiliser le même protocole (mais il peut en utiliser plusieurs en même temps).

Dans le cas du bâtiment 2 administratif, comme on utilise Internet, TCP/IP est obligatoire. Par contre, dans le bâtiment 1 (commande et fabrication), INTERNET est interdit en sortie comme en entrée (intrusion). Nous allons nettement réduire le nombre d'appareils en utilisant dans le bâtiment 1 uniquement IPX et pour le bâtiment 2, les PC qui doivent se connecter sur la partie commande utiliserons IPX et TCP/IP. Cette façon de procéder bloquera toutes les tentatives d'intrusion directes d'Internet vers le bâtiment 1. Par contre, la connexion du département commande vers Fabrication (et vis versa) sera uniquement bloqué par les droits de sessions et les communications pourront également passer du bâtiment 1 vers les PC IPX du bâtiment 2. Il suffit de bloquer les partages dans le bâtiment 2 en IPX.



Dans ce cas, nous remplaçons un switch manageable par un simple switch (avec d'autres du même type utilisés sur l'ensemble du réseau) et plus aucun firewall dans l'ensemble du réseau (à part le VPN pour INTERNET). Cette solution n'est pas à envisager pour une usine de 500 PC, mais bien pour des moyennes structures. Les utilisateurs de réseaux NOVELL privilégieront probablement cette solution.

## 9.7. Quelques erreurs classiques

- Réseau bâtiment 2: 2 classes d'adresses IP différentes pour administratif et commerciaux reliés tous deux sur les ports d'entrée du VPN (connexion INTERNET correcte) mais pas de routeur entre les deux. Dans ce fait, pas d'interconnexion entre les 2 groupes de PC mais plus grave, 1 seul département sur les 2 aura accès au serveur et au NAS. Bref, **l'infrastructure réseau du bâtiment 2 ne fonctionne pas.**
- 2 classes d'adresses différentes pour commande et fabrication. Les PC commande branchés sur un routeur 16 ports (suis pas sûr que cela existe) et branché sur un HUB 8 port qui est relié sur 5 hub 24 ports pour la fabrication. Comme le serveur Fabrication est une application dédiée, on présume que les PC ne se connecteront pas entre eux mais tous vers le serveur à leur tour avec quelques problèmes de collisions (le serveur répondra à chacun à son tour, ce qui peut être correct). Par contre, l'utilisation d'un Hub comme tête de pont entre le routeur commande et les différents HUB fabrication va directement ralentir l'ensemble du réseau Ethernet.
- Utilisation de **2 firewall** (1 de chaque côté du pont **WIFI sans fils**), configuration de l'architecture du réseau plus complexe.



## 10. Technologies alternatives réseau

### 10.1. Introduction.

Sont rassemblées ici un ensemble de technologies hardware qui sont plus ou moins en cours de conceptions et d'autres technologies difficilement classables dans les autres chapitres.

### 10.2. Technologie IPP

Cette technologie permettra d'imprimer via Internet. Elle est développée depuis 1996 conjointement entre différents fournisseurs d'imprimantes (HP, Novell, Microsoft, Xerox, Lexmark). Elle utilisera selon les derniers développements le port NetBios 631 au lieu du port tcp 80 utilisé par HTTP.

Les développements actuels penchent également sur une adresse imprimante de type "ipp://..." au lieu de http://www.... cette technologie permettra non seulement d'imprimer à distance via Internet, mais également d'assurer certaines tâches administratives sur ces imprimantes ou même d'imprimer à distance un site Web.

### 10.3. Connexion Ethernet par réseau électrique.

#### 10.3.1. Introduction.

Le réseau le plus courant est le réseau électrique en 230 V. Plusieurs tentatives ont ou sont en cours de développement pour faire passer les informations digitales (réseau informatique) via ce réseau électrique, notamment les connexions INTERNET avec plus ou moins de succès. Par contre, différents fabricants proposent depuis début 2003 des solutions de réseau interne via le réseau électrique (en concurrence avec les réseaux sans fils).

Avant d'étudier quelques possibilités, voyons quelques contraintes du réseau de distribution électrique.

Quelques rappels:

Le réseau domestique dans une habitation est en 230 V monophasé. Par contre, le réseau électrique extérieur est en triphasé (3 phases ou 3 phases + neutre). En prenant 2 fils, on obtient le réseau monophasé. Pour que le signal soit propagé d'un point à l'autre, il faut que les 2 points soient sur la même phase. Il se pourrait très bien que vous puissiez communiquer avec une maison à plus de 100 mètres et ne pas pouvoir atteindre la maison à côté. C'est le même problème avec les appareils pour surveiller les enfants en bas âge de type "baby phone".

Pour transporter le courant électrique sur de longue distance, la tension électrique est augmentée pour réduire les pertes d'énergie. C'est ce qu'on appelle les lignes haute tension qui dépassent les 5000 V. Pour passer de la tension 230 V à la haute tension, et vis et versa, on utilise un transformateur. Ces transformateurs réduisent (ou augmentent) les signaux parasites et les signaux digitaux en même temps que la tension du réseau. En plus, de par l'effet de self d'un transfo, la forme des signaux est modifiée. Ceci explique les problèmes des liaisons Internet par réseau électrique rencontrés actuellement en développement chez EDF en France.

Avec le chapitre sur les protections réseaux électriques, nous savons également que celui-ci est parcouru par de nombreux parasites. Dans les milieux "usine", cette solution risque de poser de

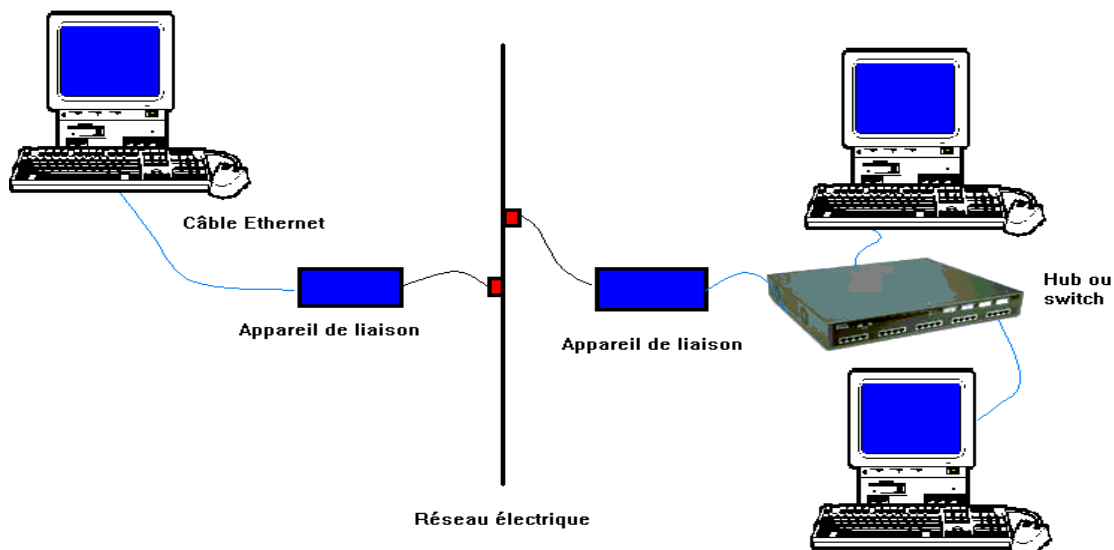
sérieux problèmes.

### 10.3.2. Connexion Internet.

EDF en France notamment développe un accès large bande INTERNET via le réseau électrique. Le problème majeur qu'ils tentent de résoudre vient de la modification (perte) du signal lors du passage à travers les transformateurs dans les cabines "haute tension". Cette solution est limitée pour un village ou un immeuble.

### 10.3.3. Ethernet via réseau électrique.

Cette solution existe déjà en Belgique depuis 2003. De la même manière que la modulation des modems, le signal est modulé sur la fréquence du réseau électrique. Les contraintes liées aux transformateurs sont également de mise. Le problème des phases du réseau est le deuxième problème.



La liaison Ethernet à travers le réseau électrique (Ethernet Over Power Line) utilise des appareils spécifiques que se chargent du transfert des signaux via la ligne électrique. De l'autre côté, l'appareil est muni d'une liaison Ethernet classique 10/100 qui se connecte sur les carte réseaux des PC, Hubs, switch, ...

Le débit maximum de ce type d'installation est de maximum 14 Mbps, soit un peu plus que le Wifi 802.11B à 10 Mps. La distance maximale est actuellement limitée à 200 mètres. Mais les caractéristiques devraient évoluer dans les prochains mois (mi-2003).

La méthode de communication utilise une modulation de type OFDM (Orthogonal Frequency Division Multiplexing) déjà utilisée dans la norme 802.11a. Cette technologie intègre de nombreuses fonctions, comme la gestion de la QoS (classes de priorité, contrôle de la latence, et adaptation des taux de transmission au temps de propagation d'un paquet).

Cette solution permet via d'autres appareils de relier directement via le port USB des PC en transitant par le réseau électrique. La vitesse est ici limitée par celle du port USB 1.1 qui est de 12 Mb/S, un peu plus lent. Dans ce cas, chaque PC à connecter reçoit une interface.

## 10.4. VoIP, Voice Over IP

Au début des réseaux, les liaisons ont utilisé les fils téléphoniques. Juste retour des choses, les liaisons réseaux vont accepter les liaisons téléphoniques et, en général, la voie sur des réseaux TCP/IP.

Une distinction avant de commencer. Il faut impérativement dissocier le VoIP et ToIP. Dans le premier cas, le réseau Ethernet permet de faire transiter la parole. Dans le deuxième cas, des logiciels permettent de "téléphoner" via le réseau INTERNET. Le ToIP est donc plus lié aux logiciels qu'à l'infrastructure réseau.

L'avantage est surtout lié aux communications à grande distance (via Internet). Néanmoins, cette solution fonctionne également sur le câble réseau interne de l'entreprise avec une communication vers des opérateurs utilisant un central téléphonique particulier sur le site de l'entreprise (permettant de connecter des téléphones au sein de l'entreprise), faisant transiter le signal TCP/IP voice sur le réseau internet pour le réinjecter sur soit une autre connexion Voice / Over IP, soit comme une communication téléphonique normale. Le VOiP utilise des téléphones (et des centraux téléphoniques) particuliers.

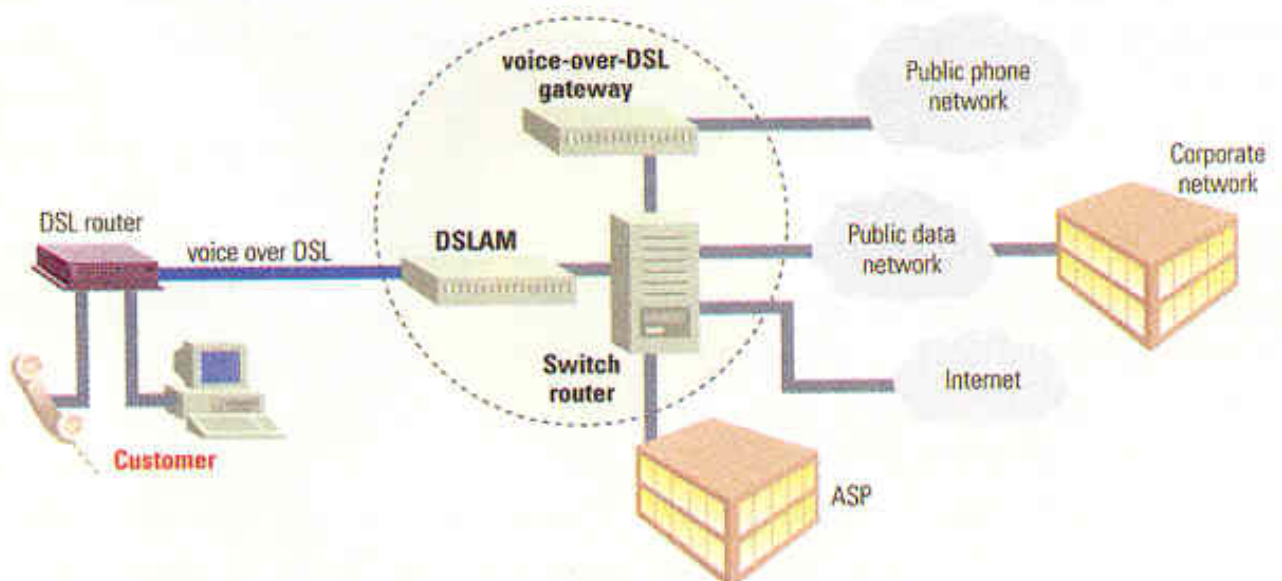
La technologie évolue actuellement avec des corrections, notamment au niveau des pertes de paquets, problèmes d'écho, temps de transfert de la voix ou même des variations de délais entre les différentes parties du signal sonore, ce qui rendait parfois le message incompréhensible.

Plusieurs protocoles sont actuellement utilisés:

. **H 323**: le standard actuellement le plus répandu mais ne garanti pas une qualité du service. Cette technologie (hardware et software) est notamment utilisée par Netmeeting de Microsoft.

. **SIP** (session Initiation Protocol): nouveau standard plus proche du monde informatique que de la téléphonie, les messages sont de format similaire à une application texte (comme la navigation HTTP). Ceci garantit une meilleure qualité de réception du signal. Ce protocole permet également une meilleure implantation dans les programmes.

SIP est constitué de 8 routines: Invite, Register, Bye, ack, cancel, options, subscribe et notify. Couplé à XML, il mène à un sous-protocole IPTML (IP Terminal Markup Language). L'ensemble des 2 devrait permettre de rassembler des textes, sons, vidéos dans un même transfert de données.



Le lecteur ne doit donc pas trop penser en terme de communication Internet, mais bien en terme de connexion téléphonique transitant sur Internet.