La théorie des réseaux locaux et étendus

par Patrick Hautrive

Date de publication : 07/10/2006

Dernière mise à jour : 07/10/2006

Ce cours vous expose les principes fondamentaux des réseaux.

I - Introduction

I-1 - Téléchargements

Format	Liens	
Tutoriel en PDF	FTP	HTTP

I-2 - Introduction

Ce tutoriel a pour but de vous exposer les principes fondamentaux des réseaux. Ces principes sont valables lors de la rédaction de ce tutoriel. Le document original est écrit par Patrick Hautrive (hautrive arobase free.fr) et est disponible sur son site

II - Les avantages des réseaux

II-1 - La chaîne numérique

L'avantage d'un réseau sur un ensemble d'ordinateurs indépendants, est que le réseau permet de ne pas interrompre la chaîne numérique, d'automatiser, de standardiser, et de centraliser certaines tâches.

A l'époque de la création du réseau Ethernet, les utilisateurs du nouveau réseau pouvaient ironiser sur leur collègue qui ne disposait pas de cette nouvelle technologie : le partage de fichiers sans réseau était appelé, le « Sneakernet » (le réseau basket, du nom d'une paire de chaussures). Cette antique technique de l'huile de genoux (qui remonte aux marathoniens) ne pouvait prémunir les utilisateurs de travailler sur des versions différentes d'un même fichier. D'autre part, tous les ordinateurs devaient être équipés des logiciels adéquats pour lire chaque type de fichier.

Les réseaux permettent de travailler autrement. Par exemple, la messagerie électronique permet de communiquer avec plusieurs personnes en même temps, indépendamment de la disponibilité de chacun. Cette technologie apporte une valeur ajoutée qui n'existait pas sans les réseaux, c'est pourquoi, elle peut être paradoxalement appelée « une application dévoreuse de ressources », dans le sens qu'une fois adoptée par les utilisateurs, ceux-ci ne peuvent plus travailler comme avant, au contraire, ils en redemandent, contaminent leurs collègues, leurs familles et leurs connaissances, et expriment sans cesse leur besoin de disposer de ressources informatiques supplémentaires.

L'avantage fondamental d'un réseau est qu'il créé des synergies. Le tout est potentiellement supérieur à la somme de ses parties.

II-2 - La communication numérique

II-3 - La centralisation de l'administration

II-4 - Les outils de centralisation de l'administration

Les outils de centralisation de l'administration permettent de collecter à travers le réseau des informations sur les configurations des ordinateurs distants, et d'effectuer une reconfiguration à distance, voire d'uniformiser les configurations de tous les postes.

Les avantages de l'administration centralisée sont appréciables :

- Le gain de temps
- Le gain d'argent
- La bienveillance des utilisateurs qui n'ont plus de problème de configuration
- La crédibilité de l'administrateur réseau

Les outils de centralisation de l'administration d'un réseau sont nombreux :

- SMS (System Management Server) de Microsoft pour les réseaux WINDOWS NT
- Saber LAN Manager de Network Associates
- TME10 de Tivoli
- Norton Administrator for Networks de Symantec

III - La classification des réseaux

Il y a autant d'architectures réseau, au sens large, que de configurations d'ordinateur, de visages ou de façons de s'habiller. C'est la jungle et pour s'y retrouver, il n'y a rien de mieux que d'**identifier leurs caractéristiques afin de déterminer une unité de mesure pour les comparer.**

III-1 - Les critères de classification d'un réseau

Les réseaux peuvent être classifiés en fonction de différents critères :

III-2 - Les protocoles routables

Les protocoles routables permettent de franchir la barrière des routeurs pour communiquer avec d'autres sous-réseaux.

Protocoles routables	Protocoles non routables
TCP/IP	NETBEUI
IPX/SPX	LAT de DEC
OSI	
XNS	
DDP (AppleTalk)	

IV - La topologie des réseaux

IV-1 - La représentation d'un réseau

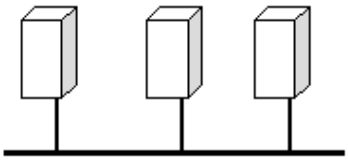
La topologie est une représentation d'un réseau. Cette représentation peut être considérée du point de vue de l'emplacement des matériels (câbles, postes, dispositifs de connectivité,...), alors on parle de « topologie physique », ou du point de vue du parcours de l'information entre les différents matériels, alors on parle de « topologie logique ». La topologie logique détermine la manière dont les stations se partagent le support et dépend de la méthode d'accès au réseau. Par exemple, un réseau peut être considéré comme appartenant à une topologie en étoile, du point de vue physique, alors qu'en réalité il appartient à une topologie en anneau, du point de vue logique.

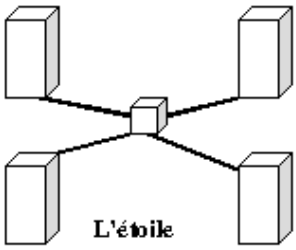
En général, la topologie représente la disposition physique de l'ensemble des composants d'un réseau. La topologie d'un réseau est aussi appelée le schéma de base, l'architecture ou le plan

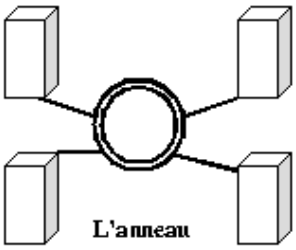
La topologie d'un réseau se représente souvent par un dessin qui réuni l'ensemble des postes, des périphériques, du câblage, des routeurs, des systèmes d'exploitation réseaux, des protocoles, etc...

La topologie d'un réseau peut avoir une extrême importance sur l'évolution du réseau, sur son administration, et sur les compétences des personnels qui seront amenés à s'en servir.

Les différentes topologies de réseaux sont les suivantes :







Physiquement, les réseaux en bus, en étoile et en anneau peuvent se ressembler beaucoup parce qu'ils peuvent être tous organisés autour d'un boîtier. Selon la topologie, le boîtier contient un bus, un concentrateur ou un anneau.

D'une manière plus générale, la représentation d'un réseau peut s'établir en fonction de la circulation de l'information. D'un point de vue Client Serveur, les rôles sont bien définis et bien séparés. Ainsi, un réseau peut être "centralisé", "réparti" ou "distribué" bien que ces notions soient relatives et souples.

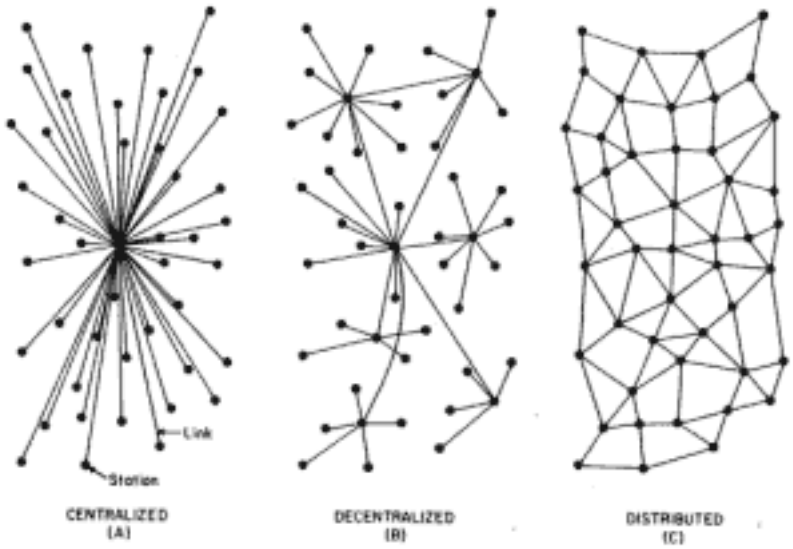


FIG. 1 — Centralized, Decentralized and Distributed Networks

IV-2 - Les réseaux en bus

Les réseaux en bus sont aussi appelés réseaux en bus linéaire, épine dorsale ou backbone. Les différents postes ou périphériques du réseau sont reliés à un seul et même câble (tronçon (trunk), segment). A toutes les extrémités du câble est fixé un bouchon, un terminator. La topologie en bus est dite « topologie passive » parce que le signal électrique qui circule le long du câble n'est pas régénéré quand il passe devant une station.

Les réseaux en bus sont simples, peu coûteux, faciles à mettre en place et à maintenir. Si une machine tombe en panne sur un réseau en bus, alors le réseau fonctionne toujours, mais si le câble est défectueux alors le réseau tout entier ne fonctionne plus. Le bus constitue un seul segment que les stations doivent se partager pour communiquer entres elles.

IV-3 - Les réseaux en étoile

Dans un réseau en étoile chaque poste est relié au réseau par l'intermédiaire de son propre câble à un concentrateur (un hub). Les concentrateurs s'appellent différemment selon la topologie à laquelle ils appartiennent (les switchs, les commutateurs, les MAU ne concernent que les réseaux en anneau de type Token Ring), et les termes employés par les spécialistes peuvent également être utilisés indifféremment (ou confusionnellement).

Les concentrateurs sont dénommés différemment selon leurs fonctionnalités :

- Les HUB sont de simples concentrateurs qui régénèrent le signal et le transmettent à tous les ports (ceux sont des répéteurs).
- Les SWITCH sont des HUB améliorés qui peuvent transmettre des données simultanément entre plusieurs couples de stations (des répéteurs plus efficaces).
- Les commutateurs segmentent le réseau et filtrent les paquets.

Quand un des ports d'un concentrateur est inoccupé, alors le concentrateur le court-circuite automatiquement afin que le réseau ne soit pas coupé (à contrario d'un réseau en bus qui ne fonctionne plus si une station est déconnectée). Il existe des "HUB administrables" qui permettent de segmenter le réseau.

Les concentrateurs sont essentiellement un segment à l'intérieur d'une boîte. Il existe de vieux concentrateurs à « média partagé » qui sont « mono segment » (le réseau est constitué d'un seul segment logique), et les nouveaux concentrateurs (on parle plus facilement de commutateurs) qui segmentent le trafic (le réseau est constitué de plusieurs segments logiques). Le concentrateur centralise tous les échanges (le trafic), et toutes les communications passent au travers du concentrateur. Le concentrateur régénère le signal électrique (comme un répéteur multiport). Un concentrateur peut posséder 8 ou 10 ports, les ports peuvent être de différents types (concentrateurs hybrides).

Les commutateurs permettent de créer des segments logiques pour chacune des stations qui est reliée à l'un de ses ports, et indépendamment des autres segments des autres stations. Le trafic est ainsi segmenté, et chacune des stations peut émettre n'importe quand, c'est alors au commutateur de répartir les communications qui lui parviennent. Il existe des commutateurs qui disposent d'une fonction d'auto découverte (autodiscovery en anglais) et qui en 10 minutes enregistrent les adresses MAC des noeuds du réseau.

Un commutateur peut être relié à plusieurs concentrateurs, en cascade (à l'aide d'un câble UPLINK, le port juste à coté ne fonctionne plus), ce qui permet d'étendre un réseau en longueur et en nombre de stations. L'utilisation du commutateur permet de compartimenter le trafic de tout le réseau, les concentrateurs sont tous reliés au commutateur, les stations reliées à un même concentrateur (HUB) constituent un segment logique, et il y a autant de segments logiques qu'il y a de HUB. L'incorporation d'un commutateur au milieu de concentrateurs permet d'augmenter la bande passante relative des stations appartenant au même segment logique. 3 HUB de 4 ports chacun en cascade équivalent à un seul HUB de 10 ports.

Les réseaux en étoile sont plus faciles à administrer et à planifier. Si une machine ou un câble tombe en panne, alors le réseau fonctionne toujours pour les autres machines ; mais si le concentrateur tombe en panne, alors c'est tout le réseau qui ne fonctionne plus. Les réseaux en étoile sont plus faciles à gérer car très faciles à déplacer.

IV-4 - Les réseaux en anneau

Les réseaux en anneau sont constitués d'un seul câble qui forme une boucle logique.

Les réseaux en anneau sont des réseaux qui gèrent particulièrement le trafic. Le droit de parler sur le réseau est matérialisé par un jeton qui passe de poste en poste. Chaque poste reçoit le jeton chacun son tour, et chaque station ne peut conserver le jeton qu'un certain temps, ainsi le temps de communication est équilibré entre toutes les stations. Le trafic est ainsi très réglementé, il n'y a pas de collisions de « paquets », le signal électrique circule seul sur le câble, depuis la station émettrice jusqu'à la station réceptrice, et cette dernière renvoi un accusé de réception.

La méthode d'accès au réseau s'appelle le passage du jeton. La topologie en anneau est dite « topologie active » parce que le signal électrique est intercepté et régénéré par chaque machine. Il existe un mécanisme qui permet de contourner une station qui est tombée en panne, c'est le « by-pass ». Quand une station n'a pas reçu le jeton au bout d'un certain temps, une procédure permet d'en créer un autre.

En général, l'anneau se trouve à l'intérieur d'un boîtier qui s'appelle un MAU (Multistation Access Unit). Toutes les stations sont reliées au MAU. Il existe des anneaux doubles, où chaque station est reliée à deux anneaux différents. Cette redondance permet d'assurer une certaine sécurité. C'est généralement le cas de figure des réseaux étendus de type FDDI.

IV-5 - Les réseaux mixtes

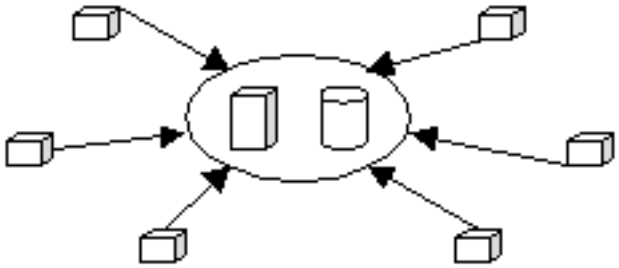
Les réseaux mixtes sont des réseaux qui mélangent deux topologies :

- Les bus en étoile
- Les réseaux 100VG-AnyLAN (ETHERNET à 100 Mb/s) de la spécification IEEE 802.12 qui fonctionnent avec la méthode d'accès de la priorité de la demande
- Les anneaux en étoile

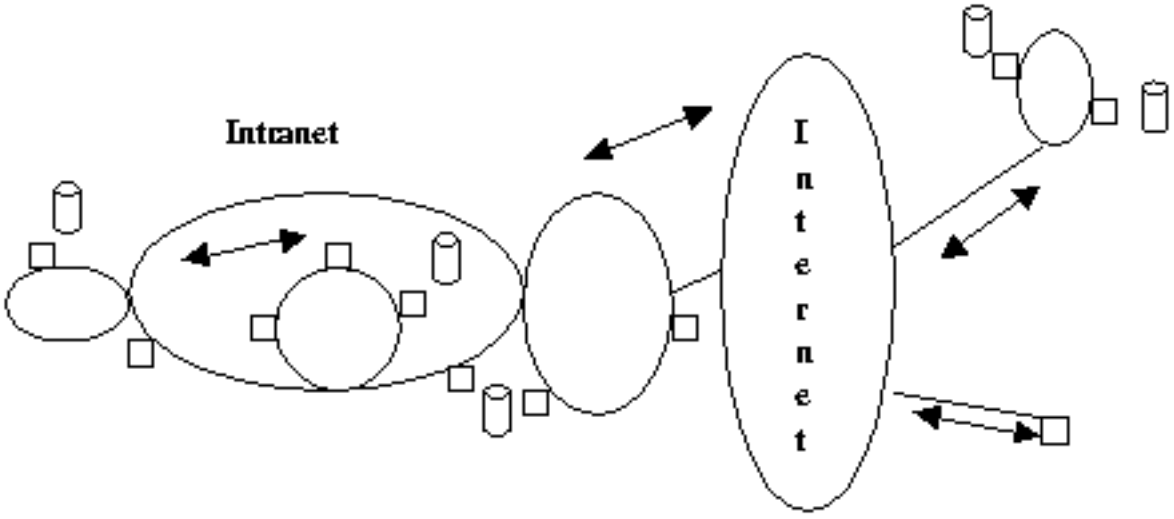
V - Les types d'organisation des réseau

V-1 - L'informatique centralisée

Les premiers réseaux étaient propriétaires et centralisés, ils étaient conçus, fabriqués et mis en oeuvre par une seule société (c'était le temps du monopole d'IBM). De tels réseaux étaient constitués de matériels et de logiciels issus d'une seule société qui cumulait les rôles de constructeur, d'architecte et d'éditeur. Ces réseaux étaient vendus clefs en main, mais ils ne fonctionnaient pas avec d'autres réseaux, ils étaient compatibles avec eux même et c'était déjà beaucoup. L'architecture d'un réseau propriétaire était centralisée autour d'un gros ordinateur très puissant, pour l'époque, et de terminaux « passif » qui interrogeaient le super calculateur central (il y a une dissymétrie entre les clients et le serveur).



Désormais, la conception d'une machine et l'organisation d'un réseau se sont largement ouvertes aux autres. On parle de réseaux décentralisés, répartis ou distribués. Les petites machines sont devenues bien plus puissantes avec les progrès de la technologie. C'est l'ère de la compatibilité, de la normalisation, de l'interopérabilité et des environnements hétérogènes (plusieurs types de machines peuvent cohabiter sur un réseau, plusieurs systèmes d'exploitation doivent coopérer ensembles, l'organisation interne et externe des réseaux est bien plus ordonnée et contrôlée). Les réseaux se sont interconnectés entre eux pour former une vaste « toile », et les perspectives sont si florissantes que les décideurs politiques parlent des « autoroutes de l'information ». Les ordinateurs font souvent partie d'un réseau, et les réseaux font partie d'un immense « maillage interplanétaire ». Les communications s'effectuent dans tous les sens et il n'y pas de dissymétrie entre les clients et les serveurs.



Les réseaux sont dits soit « de postes à postes », soit de type « client/serveur ». En fait, dans la majorité des cas, un réseau est de type « mixte », c'est à dire que coexistent les deux types. Les réseaux client-serveur ou Postes à Postes peuvent fonctionner sur toutes les topologies (en bus ou en étoile,...) et toutes les architectures (Ethernet,

FDDI,...).

V-2 - Les réseaux postes à postes (peer to peer)

Les réseaux « postes à postes » sont également appelés des réseaux « Peer to Peer » en anglais, ou « point à point » ou « d'égal à égal ». Les réseaux postes à postes ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.

Dans un réseau peer to peer, chaque poste est à la fois client et serveur. Toutes les stations ont le même rôle, et il n'y a pas de statut privilégié pour l'une des stations (comme c'est le cas avec le Contrôleur Principal de Domaine (le CPD) dans un réseau client-serveur Windows NT).

Chaque utilisateur décide lui-même des partages sur son disque dur et des permissions qu'il octroie aux autres utilisateurs. Mais une ressource partagée l'est pour tous les autres utilisateurs, c'est le concept de « partage arbitraire » développé par Microsoft. Une ressource partagée sur un ordinateur apparaît sur les autres ordinateurs qui s'y sont connectés sous la forme d'une lettre de lecteur qui vient s'ajouter aux différentes partitions déjà présentes sur la machine, c'est ce que l'on appelle monter un lecteur distant.

Les réseaux Postes à Postes permettent de travailler en équipe, ou en « groupe de travail », et il peut coexister plusieurs groupes de travail au sein d'un même réseau (ce qui permet de constituer une segmentation logique des machines du réseau).

Les petits réseaux, comme les réseaux d'égal à égal, n'ont pas vraiment besoin d'utiliser la lourde pile de protocole TCP/IP, et peuvent se contenter de NetBEUI qui est plus rapide (il faut simplement identifier les machines par des noms différents, puisque ce sont ces noms de machines qui permettent d'adresser les paquets). NetBEUI est un protocole non routable, il ne fonctionne qu'à l'intérieur d'un seul segment de câble, il ne peut servir pour Internet, qui requière TCP/IP, ni pour étendre le réseau local avec des routeurs. NetBEUI est livré avec tous les systèmes d'exploitation de Microsoft.

Les systèmes d'exploitation Microsoft qui gèrent un réseau de postes à postes :

- WINDOWS for WORKGROUPS, au début des années 1990, était un système d'exploitation qui consommait trop de mémoire vive pour faire fonctionner le réseau, et il n'en restait guère pour les applications. Par ailleurs, l'interface pour la configuration des paramètres réseaux n'était pas très intuitive. Enfin, le seul protocole fourni était NetBEUI.
- WINDOWS 95 et 98, sortis en 1995 et en 1998, était le premier système d'exploitation multi tâches 32 bits (la configuration minimale : 8 Mo de RAM, processeur 386 DX). Le système était compatible avec un réseau NetWare (SPX/IPX) et était fourni avec la pile de protocole TCP/IP.
- WINDOWS NT 3.1 en 1993 était le système d'exploitation destiné aux entreprises (la configuration minimale : 16 Mo de RAM, processeur 80486/33 et RISC). Le système était particulièrement lent et lourd, et n'exécutait pas très bien les applications 16 bits qui représentaient la majorité des applications de l'époque. La version WINDOWS NT 3.5 était une refonte complète du système, qui fut séparé en deux systèmes, WINDOWS NT WORKSTATION et WINDOWS NT SERVER, qui pouvait gérer un réseau centralisé autour de la notion de DOMAINE, et qui devenait plus robustes parce que les applications chargées en mémoire s'exécutent désormais dans des espaces mémoire séparés. La version WINDOWS NT 4.0 propose la même interface graphique que le populaire WINDOWS 95.
- Etc...

Dans une organisation Postes à Postes, les clients « voient » toutes les autres stations clientes ou serveurs (dans l'icône « Voisinage Réseau » des interfaces Windows).

Les réseaux Postes à Postes sont faciles et peu coûteux à installer au départ mais deviennent très difficiles à gérer avec le temps. Ils conviennent pour les petites structures (moins de quinze postes) avec des utilisateurs compétents pour administrer eux-mêmes leur propre machine, et où la sécurité des données n'est pas un enjeu déterminant. En fait, de nos jours quelle société pourrait revendiquer satisfaire à tous ces critères sans se dévaloriser elle-même ?

V-3 - Les réseaux Client/Serveur

Les réseaux Client/Serveur comportent en général plus de dix postes. La plupart des stations sont des « postes clients », c'est à dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs. Les « postes serveurs » sont en général de puissantes machines, elles fonctionnent à plein régime et sans discontinuité.

Les serveurs peuvent être réservés ou dédiés à une certaine tâche :

- Les serveurs de fichiers et d'impression
- Les serveurs d'applications (applications bureautiques, applications de base de données)
- Les serveurs de messagerie
- Les serveurs de télécopies
- Les serveurs PROXY pour accéder aux services de l'Internet
- Les serveurs web pour publier le site Internet et servir les internautes
- Les serveurs RAS pour les accès à distance
- etc...

Dans une organisation client-serveur, les clients ne « voient » que le serveur. Le système d'exploitation du serveur peut être différent de celui des stations clientes. En tout cas, le système d'exploitation du serveur doit être véritablement multitâches afin de pouvoir servir un grand nombre de requêtes en même temps et de façon équitable, c'est à dire en octroyant le même temps processeur à chaque client.

Les systèmes d'exploitation réseaux qui gèrent les réseaux client-serveur :

- WINDOWS NT SERVER de Microsoft
- NetWare de Novell
- OS/2 d'IBM
- MACINTOSH d'Apple
- UNIX
- LINUX

V-4 - L'avantage des réseaux Client/Serveur

L'avantage des réseaux Client/Serveur est de réunir deux avantages complémentaires, l'indépendance et la centralisation :

Dans un réseau client-serveur, avec des serveurs d'applications et de fichiers, et une configuration standardisée pour les stations clientes, il est très facile de changer une machine en panne. C'est « l'interchangeabilité » qui limite la durée d'une panne pour l'utilisateur (malheureusement l'environnement de l'utilisateur et sans doute les procédures de son activité sont relativement uniformisés). Toutefois, une organisation en client-serveur requiert des machines dédiées et très performantes. Les serveurs deviennent les points faibles du réseau et doivent être protégés rigoureusement, avec un système RAID par exemple.

V-5 - La configuration minimum de WINDOWS NT 4 SERVER

Le système d'exploitation réseau WINDOWS NT 4 SERVER est un système qui peut fonctionner dans les deux modes :

- Le mode autonome PEER to PEER
- Le mode CLIENT SERVEUR

Le système d'exploitation réseau WINDOWS NT 4 SERVER ne fonctionne pas sur n'importe quelle machine, WINDOWS NT 4 SERVER a été conçu pour fonctionner avec au minimum une certaine configuration matérielle. La configuration matérielle minimum pour faire tourner WINDOWS NT 4 SERVER est la suivante (données du constructeur) :

- Un processeur INTEL 80486/33 ou supérieur
- 16 Mo de mémoire RAM ou plus
- 125 Mo d'espace ROM sur le disque dur

VI - Les réseaux client-serveur

VI-1 - L'apparition du modèle client-serveur

Le modèle client-serveur s'oppose aux vieux systèmes informatiques centralisés autour d'un gros ordinateur, basés sur une architecture propriétaire. Le système central traite la requête d'un terminal, puis lui envoie la réponse. Le modèle client-serveur s'oppose également au mode autonome de travail des réseaux PEER to PEER.

Dans une organisation de type égal à égal (ou poste à poste), les fichiers sont répartis sur les disques durs de tous les ordinateurs (c'est la pagaille décentralisée) et tous les utilisateurs « voient » les autres ordinateurs qui sont connectés en même temps, c'est ainsi qu'ils peuvent savoir si une ressource localisée sur telle machine est accessible ou non.

Par contre, dans une organisation de type client-serveur, les fichiers sont généralement centralisés sur un serveur, et les utilisateurs « voient » le serveur mais ne « voient » pas les autres machines utilisateur, tout passe par l'intermédiaire du serveur. Dans un réseau de type client-serveur, les ordinateurs ne devront jamais avoir besoin des ressources d'une autre station, parce qu'ils ne pourront simplement pas y accéder. La totalité de l'architecture du réseau repose sur un ou plusieurs serveurs dédiés.

Dans certains réseaux client-serveur plus complexes, certaines stations peuvent faire office de clients et de serveurs (comme par exemple un réseau client-serveur basé sur un serveur NetWare et des clients Windows 95 en mode égal à égal). Le réseau est dit « bi-protocoles » (IPX et NetBEUI) ou « dual stack ». C'est souvent le cas quand le serveur NetWare sert de serveur d'impression.

Le modèle client-serveur est apparu grâce aux progrès technologiques qui ont permis de transformer les terminaux dépourvus d'intelligence, en de véritables ordinateurs avec une véritable capacité de traitement, de stockage, de présentation et de communication... Pour autant, quand un client fait appel à un serveur de base de données, par exemple, le serveur ne transmet pas toute la base de données au client (même si cela est envisageable, cette solution encombrerait beaucoup le réseau). En réalité, la situation la plus courante est que le client et le serveur se partagent le travail.

Les serveurs peuvent être dédiés à plusieurs tâches spécialisées :

- Les serveurs d'authentification
- Les serveurs de fichiers
- Les serveurs d'applications
- Les serveurs d'impression
- Les serveurs de messagerie
- Les serveurs Internet
- Les serveurs proxy
- Les serveurs RAS pour les connexions des utilisateurs à distance
- Les serveurs de sauvegarde

VI-2 - Les avantages du modèle client-serveur

Les avantages du modèle client-serveur :

VI-3 - Le processus d'une requête SQL en client-serveur

L'application la plus utilisée en mode client-serveur est la base de données. Les bases de données permettent

d'organiser fonctionnellement un très grand nombre d'informations, et de les trier au fur et à mesure des besoins. Le modèle client-serveur permet de centraliser les informations de la base de données et de répondre à un grand nombre de requêtes simultanées de la part des clients. Le langage pour exprimer une requête auprès de la plupart des bases de données est le SQL (Structured Query Language). Le langage SQL est un « langage d'interrogation structuré » qui a été conçu par la société IBM. SQL est devenu une norme, un standard dans le monde des bases de données. Le processus d'une requête SQL en client-serveur :

- L'utilisateur émet une demande
- La commande est traduite en SQL
- Le redirecteur intercepte la requête SQL et l'envoie à la carte réseau qui la transmet au support de communication
- La requête circule sur le réseau jusqu'au serveur de base de données
- Le serveur de base de données accepte la requête, la traite (recherche, extrait et trie les informations contenues dans les tables de la base de données) et envoie une réponse (un enregistrement SQL)
- La réponse circule sur le réseau
- Le client reçoit la réponse du serveur
- L'utilisateur visualise la réponse

L'application de base de données MICROSOFT ACCESS possède son propre langage SQL, mais son interface utilisateur permet d'interroger la plupart des autres bases de données.

VI-4 - Le Client et le Serveur

Les composants d'un modèle client-serveur sont le client (aussi appelé le frontal, le FRONT END) et le serveur (aussi appelé le dorsal ou le BACK END). Les tâches sont réparties entre le client et le serveur (le client affiche, tandis que le serveur calcule).

L'outil VISUAL BASIC permet de programmer des frontaux et de personnaliser les accès et les requêtes auprès d'une base de données.

L'application MICROSOFT SQL SERVER permet à d'autres clients que ceux de MICROSOFT d'accéder à une base de données, sans avoir besoin d'installer un client supplémentaire.

VI-5 - Le client

L'ordinateur client exécute une application cliente (le frontal) localement qui lui présente des fenêtres et s'occupe de la traduction des demandes en SQL :

- Une interface graphique utilisateur
- Des formulaires de demande (des clés de recherche)
- L'application formate les demandes de l'utilisateur en requêtes SQL
- L'application convertie et affiche les résultats (les enregistrements) renvoyés par le serveur

VI-6 - Le serveur

Le serveur exécute l'application de base de données (le dorsal) localement, mais n'exécute pas d'application pour gérer l'interface utilisateur. Le serveur supporte la charge des requêtes des utilisateurs, et généralement stocke les informations de toute la base de données. Les données de la base peuvent être éventuellement stockées sur un

ou plusieurs autres ordinateurs.

Le serveur de base de données s'occupe également de l'enregistrement des modifications (ajouts, suppressions, ...) des données, mais aussi de la conservation et de la consolidation de la base.

Quand il y a plusieurs serveurs sur le réseau pour la même base de données, la synchronisation des bases doit s'effectuer régulièrement. Quand les données de la base sont stockées sur plusieurs ordinateurs, il est possible de centraliser la base sur un DATA WAREHOUSE qui contient toute la base tandis que les autres ordinateurs n'en contient qu'une partie (généralement les données les plus fréquemment demandées).

Les procédures stockées (Stored Procedures) sont de petites routines préprogrammées qui permettent de simplifier les traitements les plus courants et d'obtenir plus rapidement les réponses. Une procédure peut être appelée par plusieurs clients en même temps.

VI-7 - Les spécifications techniques pour un serveur

En général, les ordinateurs hébergeant un serveur dédié sont très puissants. Il faut que l'accès aux données stockées sur le serveur depuis le réseau soit acceptable pour toutes les stations clientes (qui peuvent émettre des requêtes en même temps). C'est pourquoi, les spécifications techniques d'un serveur sont hors du commun :

- Le bus de la carte mère rapide (nombre de bits transférés en parallèle d'un composant vers un autre, et la fréquence à laquelle ces bits sont transférés)
- Un ou plusieurs processeurs rapides
- Une quantité de mémoire vive importante
- Un ou plusieurs disques durs rapides et volumineux. Le temps d'accès aux disques (en lecture et en écriture) appelé le débit entrée / sortie (« throughput » en anglais) doit être très rapide, parce que c'est ce qui ralentit l'accès aux données pour le client.
- Une ou plusieurs cartes réseaux rapides
- Un câblage à haut débit

VII - Les organismes de normalisation

VII-1 - L'influence des normes

Les normes établies par les organismes internationaux (et particulièrement américains) de normalisation ont contribué à l'ouverture des architectures propriétaires, à la convergence des efforts des petites sociétés, et à l'expansion de la micro-informatique dans le monde... D'une certaine façon, les organismes de normalisation sont à l'origine de la compatibilité, de l'interopérabilité et de la démocratisation des outils informatiques. Par exemple, les réseaux de l'architecture SNA d'IBM, ne pouvaient communiquer avec les réseaux DNA de DIGITAL...

Les besoins croissants des entreprises en matière d'interactivité , de partage de données, et de portage des applications dans différents environnements ont accéléré le développement des normes pour les réseaux.

En général, les normes sont des spécifications techniques qui imposent certaines contraintes de fabrication aux constructeurs. Les fabricants adhèrent volontairement à ces directives, à ces recommandations, parce qu'elles leur assurent une large part de marché. Aujourd'hui, la conformité aux normes est presque un impératif.

Les normes concernent tous les aspects de l'informatique : les matériels, les logiciels, et même les personnels avec les certifications. Tout doit rentrer dans l'ordre !

Les normes correspondent à la publication d'une certaine technologie par des organismes, tandis que les standards correspondent à la reconnaissance des utilisateurs pour une certaine technologie.

Les principaux organismes de normalisation sont soutenus par les grandes entreprises de l'industrie informatique.

VII-2 - Les principaux organismes de normalisation

Les organismes de normalisation peuvent être constitués de différentes manières :

- Les services d'un état
- Des instituts universitaires
- Des organismes de recherche
- Des consortiums d'entreprises privées
- Un "melting pot"

Les principaux organismes de normalisation sont les suivants :

VIII - Le modèle OSI

VIII-1 - La normalisation des communications des réseaux hétérogènes

Le modèle OSI (Open Systems Interconnection) d'interconnexion des systèmes ouverts décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Le modèle OSI est organisé en 7 couches successives.

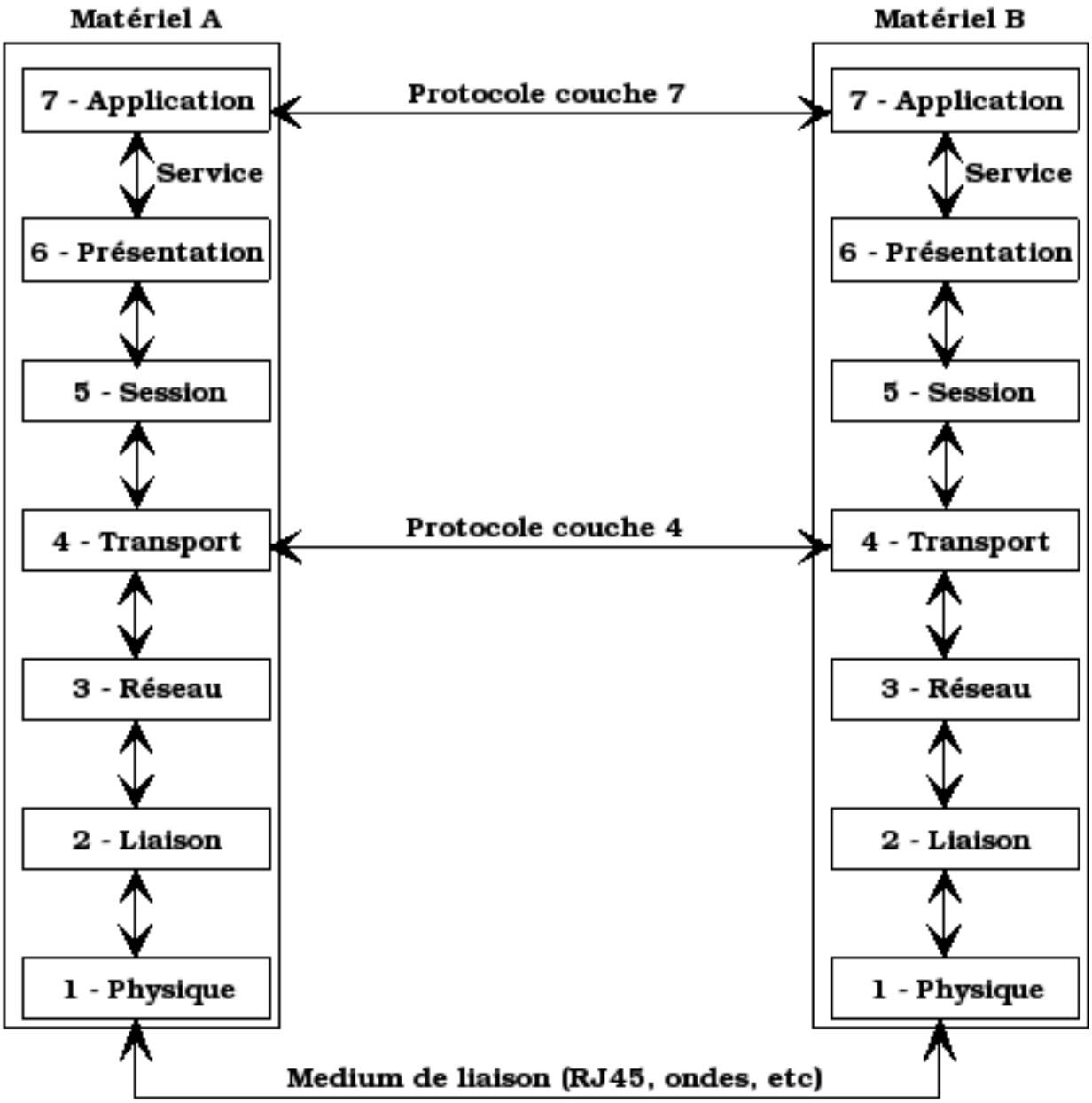
Le modèle OSI a été publié en 1978 par un organisme de normalisation, l'ISO (International Standard Organization). En 1984, l'ISO publia une mise à jour du modèle OSI qui dès lors devint une norme internationale. Le modèle IEEE 802 (de février 1980) est une version améliorée du modèle OSI.

Le modèle OSI est le modèle le plus connu et le plus utilisé pour décrire et expliquer un environnement réseau. Les fabricants d'équipements réseaux suivent les spécifications du modèle OSI, mais aucun protocole ne s'y conforme à la lettre.

VIII-2 - L'activité d'un réseau

L'activité d'un réseau consiste à envoyer et à recevoir des données d'un ordinateur vers un autre. « L'ordinateur émetteur » prépare les données (qui seront transmises sur le support de communication du réseau) afin que celles-ci s'acheminent correctement vers « l'ordinateur récepteur ».

L'activité d'un réseau ressemble à l'activité de la belle Cendrillon. Cendrillon suit des règles très précises de séduction auxquelles elle ne déroge jamais. Cendrillon s'habille d'abord, puis la princesse monte dans son carrosse, pour aller danser au bal, enfin Cendrillon se déshabille. Effectivement, Cendrillon se comporte de la même façon que les données qui sont transmises sur un réseau. Dans un premier temps, les données sont revêtues des habits adéquats par « l'ordinateur émetteur », dans un deuxième temps, les trames défilent et dansent sur le support de communication (un câble par exemple), dans un troisième temps, les données sont déshabillées par « l'ordinateur récepteur ».



VIII-3 - La préparation des données

La préparation des données, du coté de « l'ordinateur émetteur », est en réalité une transformation. Plusieurs tâches sont réalisées lors de ce processus de transformation, et à chacune de ces tâches correspond une fonction bien précise :

- La reconnaissance des données
- La segmentation des données en « paquets »
- L'adjonction d'informations à chaque paquet :
- L'adresse de l'expéditeur
- L'adresse du destinataire
- Les bits de synchronisation

- Les bits de contrôle d'erreurs
- L'expédition des trames sur le support de communication

Le système d'exploitation réseau effectue chacune de ces tâches en suivant strictement un ensemble de procédures appelées « protocoles ». Ces procédures ont été normalisées par l'ISO qui les a rassemblées dans le modèle OSI en 7 couches.

VIII-4 - L'architecture en 7 couches du modèle OSI

Le modèle OSI est constitué de 7 couches successives. Chacune de ces 7 couches est spécialisée dans une tâche bien précise. Les données de « l'ordinateur émetteur » traversent chacune des ces 7 couches (de haut en bas) avant d'être transmises (sous la forme de trames) au support de communication, puis, arrivées à destination, les trames traversent chacune des ces 7 couches (de bas en haut) avant d'être communiquées à « l'ordinateur récepteur ».

L'architecture du modèle OSI		
Numéro	Nom	Fonction
7	Application	Une interface pour l'accès au réseau
6	Présentation	Le format des données
5	Session	La gestion d'une connexion
4	Transport	La gestion des paquets
3	Réseau	La gestion de l'adressage
2	Liaison	La gestion des trames
1	Physique	La gestion des signaux sur le câble
Le support physique		

Chaque couche est spécialisée dans une tâche bien précise. On dit que chaque couche propose une fonctionnalité ou un « service ». A chaque niveau, un traitement est réalisé, et des informations sont codées ou décodées (ajoutées ou en levées du paquet).

Chaque couche de « l'ordinateur émetteur » ajoute des informations supplémentaires dans le paquet qui lui a été transmis par la couche supérieure, et transmet celui-ci à la couche inférieure (ou au support). Les informations de chaque couche sont destinées à « la couche homologue » de « l'ordinateur récepteur ». Les couches de « l'ordinateur récepteur » décodent et enlèvent une partie des informations contenues dans le paquet qui lui a été transmis par la couche inférieure (ou par le support), et transmet celui-ci à la couche supérieure.

L'activité de chaque couche est codifiée selon un certain protocole. La fonctionnalité d'une couche peut être réalisée par un logiciel, un équipement et un protocole différents de ceux des autres couches.

Chaque couche prépare les données pour la couche suivante. On dit que les couches « communiquent » entre elles, et la frontière qui les sépare est appelée une « interface ».

Les couches 7 à 3 sont appelées les couches hautes et leur travail est plus complexe que celui des couches basses. Les couches 1 et 2 sont appelées les couches basses, leur fonction est d'envoyer des flux de bits sur le réseau.

Les « couches homologues » sont les deux couches d'un même niveau, l'une située dans « l'ordinateur émetteur » et l'autre dans « l'ordinateur récepteur ». Les « couches homologues » ont la même fonction, l'une fait ce que l'autre défait. L'activité de chacune des couches est codifiée selon un protocole très précis, de façon que chacune des couches sache exactement comment travail son homologue (les couches ont besoin de savoir exactement comment ont été transformées les données afin de pouvoir les restituer à l'identique).

Les données provenant de « l'ordinateur émetteur » sont découpées en « paquets ». Les paquets passent de couche en couche. A chaque couche, des informations de formatage et d'adressage sont ajoutées au paquet. Les paquets sont transformés en trames, et ce sont les trames qui circulent sur le réseau. Arrivées à destination les trames sont transformées en paquets par les couches de « l'ordinateur récepteur ». Les informations de formatage et d'adressage sont vérifiées puis supprimées à chaque niveau, de telle sorte que les données émises soient exactement les données reçues.

Il n'y a que la couche la plus basse qui puisse « communiquer » directement avec son homologue sans que « le message » ne transite par toutes les autres couches. Toutes les autres couches ne « communiquent » pas avec leur homologue, les informations qu'elles ajoutent à chaque paquet sont transmises à la couche suivante et ainsi de suite. S'il peut paraître qu'il y ait une forme de « communication virtuelle » entre chaque couche et son homologue, c'est seulement parce que chaque couche a été définie de la même façon que son homologue (fondue dans le même moule, comme les clones sont issus des même gênes) et que chacune effectue le travail symétrique de l'autre.

VIII-5 - La couche APPLICATION

La couche APPLICATION (APPLICATION LAYER) joue le rôle d'une interface d'accès des applications au réseau. La couche APPLICATION concerne les applications réseaux qui tournent sur un poste (TELNET, FTP,...), et correspond à l'interface de l'utilisateur.

Les fonctions de la couche APPLICATION :

- La gestion des applications réseaux
- Utilitaires de transfert de fichiers
- Logiciels d'accès aux bases de données
- Messagerie électronique
- L'accès au réseau
- Le contrôle du flux et la correction des erreurs

VIII-6 - La couche PRESENTATION

La couche PRESENTATION (PRESENTATION LAYER) détermine le format utilisé pour l'échange des données entre ordinateurs du réseau.

Les fonctions de la couche PRESENTATION :

- La conversion du format issu de la couche APPLICATION en un format standard
- La conversion des protocoles
- La traduction et l'encodage des données
- La conversion du jeu de caractères

- L'exécution des commandes graphiques
- La compression ou la décompression des données

Un utilitaire appelé « redirecteur » (REDIRECTOR) opère sur la couche PRESENTATION et permet de rediriger les opérations d'Entrée/Sortie vers les ressources d'un serveur.

La couche PRESENTATION permet par exemple d'afficher des données UNIX sur un écran MS-DOS.

VIII-7 - La couche SESSION

La couche SESSION (SESSION LAYER) gère la connexion entre deux ordinateurs du réseau.

Les fonctions de la couche SESSION :

- L'ouverture et la fermeture d'une connexion (d'une session)
- La reconnaissance des noms
- La synchronisation des tâches utilisateur à l'aide de points de contrôle
- Le contrôle du dialogue entre les processus communicants (qui transmet, à qui, à quel moment, pour combien de temps, ...)

VIII-8 - La couche TRANSPORT

La couche TRANSPORT (TRANSPORT LAYER) s'assure que les paquets ont été reçus dans l'ordre, sans erreurs, sans pertes, ni duplication. La couche TRANSPORT gère l'empaquetage et le réassemblage des paquets ainsi que le contrôle et la correction des erreurs.

Les fonctions de la couche TRANSPORT :

- La division des messages longs en plusieurs paquets
- Le contrôle de la taille des paquets
- Le regroupement des messages courts en un seul paquet
- Le rassemblement des paquets en un seul message
- L'extraction et la reconstitution du message d'origine
- L'envoi et la réception d'un accusé de réception
- Le contrôle du flux et la correction des erreurs dans la reconstitution des paquets

VIII-9 - La couche RESEAU

La couche RESEAU (NETWORK LAYER) se charge de l'adressage des messages. La couche RESEAU fournit un schéma d'adressage. La couche RESEAU traduit les adresses logiques (les adresses IP) en adresses physiques (les adresses MAC des cartes réseaux).

Les fonctions de la couche RESEAU :

- La traduction des adresses et des noms logiques en adresses physiques

- Le routage des messages en fonction de leur priorité et de l'état du réseau
- La gestion du trafic sur le réseau :
- La commutation de paquets
- Le contrôle de l'encombrement des messages sur le réseau
- Le découpage ou le réassemblage des messages en fonction de la capacité de la carte réseau (et de celle de son correspondant)

VIII-10 - La couche LIAISON

La couche LIAISON (DATA LINK LAYER) gère le transfert des trames. Une trame (souvent synonyme de paquet) est une structure logique et organisée dans laquelle sont placées les données.

La structure d'une trame (d'un paquet) est toujours la même. La trame est constituée de plusieurs éléments et dans un ordre précis :

Les fonctions de la couche LIAISON :

- La préparation des trames pour la couche PHYSIQUE :
- La fabrication des trames en fonction de la méthode d'accès au réseau.
- La division des messages en trames de bits bruts ou leur regroupement.
- Le contrôle CRC des erreurs dans la transmission d'un paquet.
- L'envoi et la réception d'un accusé de réception pour chaque trame, sinon la trame est réexpédiée.

VIII-11 - La couche PHYSIQUE

La couche PHYSIQUE (PHYSICAL LAYER) transmet des flux de bits bruts sur le support de communication. La couche PHYSIQUE est en relation directe avec la carte réseau.

Les fonctions de la couche PHYSIQUE :

- La gestion du branchement au support :
- Le branchement du câble à la carte réseau
- La définition du nombre de broches du connecteur
- La fonction de chacune des broches du connecteur
- La gestion des signaux, électriques, optiques, mécaniques :
- L'encodage et la synchronisation du flux de bits
- La durée de chaque bit, les caractéristiques de l'impulsion électrique ou optique
- La méthode d'accès des bits sur le support de communication :
- L'envoi des trames sur le réseau

VIII-12 - Le modèle IEEE-802

Le modèle IEEE 802 fait référence au mois et à l'année où il sortit (février 1980). Le modèle IEEE 802 a été mis au point par l'IEEE (Institute of Electrical and Electronics Engineers) pour définir des normes pour les réseaux locaux.

Le modèle IEEE 802 est sorti juste un peu avant le modèle OSI ; les deux modèles se ressemblent beaucoup et sont compatibles entre eux.

Le modèle IEEE 802 définit :

- La façon dont les données accèdent et sont transmises sur le réseau
- Les normes des composants physiques d'un réseau :
- La carte réseau
- Le câblage en coaxial ou en paires torsadées
- Les spécifications correspondant aux couches LIAISON et PHYSIQUE du modèle OSI

VIII-13 - Les douze catégories du modèle IEEE 802

La norme 802 a été présentée en douze catégories :

Les normes IEEE 802 pour les réseaux locaux	
Numéro	Caractéristiques
802.1	Le fonctionnement inter réseaux (INTERNETWORKING)
802.2	Le contrôle des liaisons logiques LLC (Logical Link Control)
802.3	Les réseaux locaux en bus logique (ETHERNET LAN) à 10 Mb/s, avec la méthode d'accès CSMA/CD
802.4	Les réseaux locaux en bus à jeton (Token Bus LAN)
802.5	Le réseau local en anneau logique (Token Ring LAN) à 4 ou 16 Mb/s, avec la méthode d'accès du passage du jeton. L'anneau logique ressemble à une étoile, mais l'anneau physique se trouve à l'intérieur de concentrateur...
802.6	Les réseaux métropolitains MAN (Metropolitan Area Network)
802.7	La transmission en large bande (Broadband Technical Advisory Group)
802.8	La fibre optique (Fiber-Optic Technical Advisory Group)
802.9	Les réseaux intégrant la voix et les données (Integrated Voice/Data Networks)
802.10	La sécurité des réseaux (Network Security)
802.11	Les réseaux sans fil (Wireless Networks)
802.12	La méthode d'accès priorité de la demande (Demand Priority Access LAN) pour les réseaux 100VG-AnyLAN à 100 Mb/s

VIII-14 - Les sous-couches LLC et MAC du modèle IEEE 802

Les deux couches basses du modèle OSI (LIAISON et PHYSIQUE) définissent la façon dont plusieurs ordinateurs peuvent utiliser simultanément le réseau sans interférer les uns avec les autres. Le comité de normalisation 802 a voulu définir plus en détail ces deux couches.

La couche LIAISON a été divisée en deux sous couches :

Certaines normes de la spécification 802 concernent les sous-couches LLC ou MAC.

<table>
<tr><th colspan="3">Les couches basses et la norme 802</th></tr>
<tr><th>Les sous-couches</th><th>Les normes spécifiques</th><th>La norme générale</th></tr>
<tr><td rowspan="2">LLC</td><td>802.1 La gestion des réseaux</td><td rowspan="6">802.1
La gestion des réseaux</td></tr>
<tr><td>802.2 LLC</td></tr>
<tr><td rowspan="4">MAC</td><td>802.3 CSMA/CD</td></tr>
<tr><td>802.4 Bus à jeton</td></tr>
<tr><td>802.5 Anneau à jeton</td></tr>
<tr><td>802.12 Priorité de la demande</td></tr>
</table>

VIII-15 - La segmentation des données en paquets

Un réseau ne fonctionne pas de manière optimale si les fichiers qui sont transmis sur le réseau ne sont pas segmentés. La « taille des chaînes de données d'origine » est souvent importante et peut pénaliser le réseau :

- Le transfert de gros fichiers en un seul bloc monopolise le support de communication pendant une période importante, pendant laquelle les autres ordinateurs ne peuvent pas accéder au réseau. Un seul ordinateur peut saturer le réseau avec un seul fichier, et la notion d'interactivité est exclue du réseau.
- Une erreur de transmission sur un gros fichier implique de retransmettre l'intégralité du fichier. Quand les données sont segmentées et qu'une erreur survient, seul la petite partie concernée est retransmise.

Les données sont segmentées afin d'apporter de la fluidité et de la convivialité au réseau. Les données sont segmentées en petites parties appelées « paquets » (les paquets sont aussi, par abus de langage, appelées des « trames ». Les trames sont construites avec une en-tête et une queue, tandis que les paquets n'ont qu'une en-tête. On utilisera les deux termes comme des synonymes!).

Les paquets sont « l'unité de base des communications réseaux ». La division des données en paquets accélère la transmission globale des données de tous les utilisateurs. Les données sont segmentées chez l'émetteur puis réassemblées chez le récepteur.

VIII-16 - La structure d'un paquet

La segmentation des données d'origine en paquets commence dès la première couche (la couche 7 : APPLICATION) du modèle OSI. Chaque couche du modèle OSI ajoute sa propre entête au paquet, avec des informations spécifiques à la couche en question, ce qui permet aux « couches homologues » de « l'ordinateur récepteur » de pouvoir traduire correctement le paquet. La couche TRANSPORT détermine la taille d'un paquet en fonction du protocole utilisé, mais aussi des capacités respectives de la carte réseau de l'expéditeur et de celle du destinataire.

Un paquet est toujours constitué de la même manière :

Lors de la segmentation des données en paquets, certaines informations sont ajoutées aux paquets. Toutes les couches du modèle OSI contribuent à la constitution du paquet, chacune des six couches ajoutent des informations au paquet. Ce sont les « couches basses » qui procèdent à « l'encapsulation finale » du paquet (la couche LIAISON ajoute la queue et la couche PHYSIQUE ajoute le début de l'entête) :

```
Paquet = En-tête + Données + Queue
```

Certaines de ces informations sont ajoutées systématiquement à tous les paquets, tandis que d'autres ne sont ajoutées que s'il est nécessaire de le faire :

Les informations ajoutées systématiquement à chaque paquet :

Les informations ajoutées selon les besoins :

- Les commandes de contrôle (comme par exemple une requête de service)
- Les codes de contrôle de session (comme par exemple pour demander une retransmission après une erreur)
- Les accusés de réception

VIII-17 - L'adressage d'un paquet

Généralement un paquet n'est adressé qu'à un seul destinataire avec une adresse bien précise.

Les paquets circulent le long d'un segment de câble et passent devant chacune des cartes réseaux (un noeud qui peut être une station, un routeur, une imprimante,...) qui est connectée au même segment de câble. Quand le paquet lui est destiné, la carte réseau l'intercepte et le traite ; quand le paquet ne lui est pas destiné, la carte réseau le laisse défiler sans intervenir. Les cartes réseaux « écoutent » le câble à la recherche d'un signal d'alerte indiquant qu'un paquet est en cours de transmission. Quand un paquet passe à leur hauteur, la carte réseau vérifie si l'adresse du destinataire lui correspond. Si le paquet lui correspond, soit la carte réseau envoie une requête d'interruption à l'ordinateur et celui-ci enregistre le paquet dans sa mémoire vive (mémoire RAM), soit la carte réseau enregistre directement le paquet (dans la mémoire vive de l'ordinateur, si elle a un accès direct à la mémoire (DMA) ou dans sa propre mémoire vive si elle en dispose). Aucune ressource de l'ordinateur n'est engagée tant que la carte réseau n'a pas identifié un paquet comme lui étant adressé.

Il existe des « adresses de diffusion générale » (BROADCAST). Les paquets avec une telle adresse sont adressés à toutes les stations d'un segment de câble, voire à toutes les stations d'un réseau.

Le processus de transfert d'un paquet peut être condensé en quelques étapes :

Le processus de transmission d'un paquet	
L'ordinateur émetteur	L'ordinateur récepteur
Transmission des données vers le logiciel réseau	
Établissement d'une connexion	
Négociation des paramètres de transmission	
	Établissement d'une connexion
	Écoute du réseau
Segmentation des données en paquets	
Écoute de la disponibilité du réseau	
Transmission des paquets sur le réseau	
Circulation des paquets sur le support de communication du réseau	
	Lecture de l'adresse du destinataire des paquets
	Vérification de l'adresse de destination des paquets
	Enregistrement des paquets concordants
	Reconstitution des données originales
	Transmission des données à l'ordinateur
	Transmission des données à l'application réseau

VIII-18 - Le routage d'un paquet

Dans un contexte de « réseaux étendus », c'est à dire dépassant le cadre d'un LAN (Local Area Network), les dispositifs de connexion et les équipements de commutation du réseau utilisent les informations d'adressage des paquets afin de déterminer la route la plus appropriée. L'adresse cible d'un paquet et d'une manière plus générale les informations d'en-tête d'un paquet peuvent être utilisées, soit pour rediriger le paquet, soit pour le filtrer.

VIII-19 - Les types de trame avec le protocole IPX

La plupart des protocoles déterminent eux-mêmes quel est le type de paquet à utiliser. Il est quand même important de bien vérifier si toutes les stations du réseau communiquent avec le même protocole, c'est un minimum...

Il peut toutefois survenir des problèmes de trames, particulièrement avec le protocole IPX. Le protocole IPX de la

pile SPX/IPX de NOVELL, comme la couche TRANSPORT du protocole NWLink de MICROSOFT, n'est pas associé à un seul type de trames. Le protocole IPX peut employer plusieurs types de trames différentes :

IX - Les réseaux APPLETALK

IX-1 - L'architecture des réseaux APPLETALK

La société APPLE COMPUTER a introduit APPLETALK en 1983. Les réseaux APPLETALK fonctionnent avec un petit ensemble d'ordinateurs MACINTOSH. La taille des réseaux APPLETALK étant limitée, c'est une architecture qui a été supplantée par l'avènement des réseaux ETHERNET. L'architecture APPLETALK est une architecture propriétaire. L'architecture APPLETALK est intégrée au système d'exploitation MAC OS. Tous les ordinateurs MACINTOSH sont équipés des fonctionnalités réseaux APPLETALK, ce qui rend plus facile la mise en place d'un tel réseau. L'architecture APPLETALK PHASE II incorpore des protocoles réseaux qui correspondent au modèle OSI. Les réseaux APPLETALK sont communément appelés des réseaux LOCALTALK.

De nombreux ordinateurs provenant d'autres constructeurs peuvent fonctionner sous APPLETALK :

- Les ordinateurs IBM compatibles PC
- Les gros systèmes IBM
- Les ordinateurs VAX de chez DIGITAL EQUIPMENT CORPORATION
- Certains ordinateurs UNIX

APPLE est ouvert aux produits développés par des sociétés indépendantes...

IX-2 - Les caractéristiques des réseaux APPLETALK

Les caractéristiques des réseaux APPLETALK sont les suivantes :

- La topologie en bus ou en arbre.
- La méthode d'accès au réseau CSMA/CA (avec prévention des collisions).
- Le câblage en paires torsadées non blindées (UTP) ou blindées (STP), la fibre optique.
- APPLETALK est bon marché et facile à installer parce qu'il est intégré au système d'exploitation.
- APPLETALK convient pour de petits réseaux.
- Les ZONES constituent des sous-réseaux APPLETALK. Les ZONES permettent d'accroître la dimension d'un réseau trop petit ou à l'inverse de segmenter un réseau trop surchargé. Les ZONES permettent de connecter d'autres réseaux utilisant d'autres architectures, par exemple de raccorder un réseau TOKEN RING à un réseau APPLETALK.
- ETHERTALK permet aux protocoles APPLETALK de fonctionner sur un câble coaxial (câble ETHERNET).

IX-3 - Les composants matériels d'un réseau APPLETALK

Les composants matériels d'un réseau APPLETALK sont les suivants :

- Des câbles LOCALTALK
- Les câbles d'APPLE
- Un maximum 32 ordinateurs
- Les câbles de FARALLON PHONENET
- Un maximum de 254 machines
- Les câbles et les connecteurs téléphoniques acceptent les topologies en bus ou en étoile avec un concentrateur central
- Des modules de connexion
- Des prises 8 broches pour relier les câbles au module de connexion

IX-4 - L'identification d'une machine sur un réseau APPLETALK

L'identification d'une machine sur un réseau APPLETALK s'effectue en trois étapes :

- La machine s'attribue une adresse au hasard dans une plage d'adresse autorisée.
- La machine diffuse sur le réseau son adresse.
- Si aucune autre machine n'utilise son adresse, elle la garde et l'enregistre.

X - Les réseaux ARCNET

X-1 - L'architecture ARCNET

L'architecture ARCNET (Attached Ressource Computer Network) a été mise au point la société DATAPOINT CORPORATION en 1977. Les premières cartes réseaux ARCNET ont été commercialisées en 1983. La technologie ARCNET précède les normes IEEE 802, mais elle correspond à peu près à la norme 802.4 qui réglemente les réseaux en bus avec le passage du jeton comme méthode d'accès. Les réseaux ARCNET sont bon marché et conviennent pour de petits réseaux.

X-2 - Les caractéristiques des réseaux ARCNET

Les caractéristiques des réseaux ARCNET sont les suivantes :

- Une topologie en bus ou en bus en étoile
- La méthode d'accès au réseau le passage du jeton, le jeton se déplace sur le réseau en suivant l'ordre numérique attribué à chaque machine, sans tenir compte de leur localisation.
- Un débit de 2,5 Mb/s, et de 20 Mb/s pour ARCNET PLUS

X-3 - Le format de la trame ARCNET

La trame ARCNET est relativement sobre en informations :

X-4 - Les composants matériels d'un réseau ARCNET

Les réseaux ARCNET fonctionnent autour d'un concentrateur, et ne gèrent pas plusieurs segments.

XI - Le réseau ARPANET

XI-1 - Un programme de recherche américain

Le réseau ARPANET est le premier réseau au monde et est à l'origine du réseau Internet. Le réseau ARPANET provient d'un programme de recherche gouvernemental américain, ARPA (Advance Research Products Agency) dont le but était de faire interagir des ordinateurs entre eux. Le programme de recherche fut la responsabilité d'une entreprise informatique du Massachusetts, le BBN (Bolt, Beranek and Newman).

Les données transmises d'un ordinateur à un autre étaient découpées en « datagrammes » (en paquets), puis transférées sur le réseau téléphonique grâce à la « commutation de paquets » (Paquets Switching).

XI-2 - L'origine de la commutation de paquets

La commutation de paquet fut une révolution dans la transmission de données, parce qu'elle présente plusieurs avantages :

- Plusieurs flots de données peuvent parcourir le support en même temps
- Plusieurs ordinateurs peuvent transmettre des données en même temps
- Les paquets peuvent emprunter plusieurs chemins différents, les paquets sont routés
- La correction des erreurs garantit la transmission des données
- Une somme de contrôle et des numéros de séquences permettent de réassembler les paquets dans le bon ordre
- Les entêtes composés de l'adresse source et de l'adresse de destination assurent que les données sont expédiées au bon endroit

XII - Les réseaux ETHERNET

XII-1 - Historique des réseaux ETHERNET

L'université de Hawaï développa à la fin des années 1960 un réseau étendu. Les bâtiments de son campus étaient très éloignés les uns des autres et il fallait réunir les ordinateurs disséminés en un seul réseau. La méthode d'accès CSMA/CD fut développée à cette occasion. Ce premier réseau a constitué la base des réseaux ETHERNET futurs.

Robert Metcalfe (Bob qui fonda la société 3COM) et David Boggs du PARC (Palo Alto Research Center) inventèrent un système de câbles et de signalisation en 1972. Puis en 1975, ils présentèrent le premier réseau ETHERNET :

- Débit de 2,94 Mb/s
- Connexion de plus de 100 stations
- Distance maximale entre deux ordinateurs de 1 Kilomètre

Le réseau ETHERNET de la société XEROX rencontra un tel succès, en 1976, que XEROX s'associa avec INTEL CORPORATION et DIGITAL EQUIPEMENT CORPORATION pour élaborer une norme à 10 Mb/s.

L'architecture ETHERNET est aujourd'hui l'architecture la plus répandue dans le monde.

XII-2 - La norme IEEE 802.3

Les caractéristiques des premiers réseaux EHERNET ont servi de base pour l'élaboration de la norme IEEE 802.3. La norme IEEE 802.3 décrit la méthode d'accès au réseau CSMA/CD et concerne les sous-couches LLC et MAC, lesquelles font parties des couches LIAISON et PHYSIQUE du modèle OSI. Maintenant, tous les réseaux ETHERNET satisfassent à la norme IEEE 802.3. La norme IEEE 802.3 a été publiée en 1990 par le comité IEEE, et concerne les réseaux ETHERNET câblés.

XII-3 - Les caractéristiques générales d'un réseau ETHERNET

Les caractéristiques générales d'un réseau ETHERNET sont les suivantes :

- La norme IEEE 802.3
- La topologie en bus linéaire ou en bus en étoile
- La transmission des signaux en bande de base
- La méthode d'accès au réseau CSMA/CD, méthode à contention
- Un débit de 10 à 100 Mb/s
- Le support est « passif » (c'est l'alimentation des ordinateurs allumés qui fournit l'énergie au support) ou « actif » (des concentrateurs régénèrent le signal)
- Le câblage en coaxial, en paires torsadées et en fibres optiques
- Les connecteurs BNC, RJ45, AUI et/ou les connecteurs pour la fibre optique
- Des trames de 64 à 1518 Octets

Les réseaux ETHERNET peuvent utiliser plusieurs protocoles, dont TCP/IP sous UNIX, ce qui explique pourquoi c'est un environnement qui a été plébiscité par la communauté scientifique et universitaire. Les performances d'un réseau ETHERNET peuvent être améliorées grâce à la segmentation du câble. En remplaçant un segment saturé par deux segments reliés par un pont ou un routeur. La segmentation réduit le trafic et le temps d'accès au réseau.

XII-4 - Le format de la trame ETHERNET

Pendant le processus de transmission des données, celles-ci sont découpées en paquets ou trames. Les trames d'un même réseau ETHERNET se ressemblent toutes, mais elles sont différentes des trames qui appartiennent à d'autres types de réseaux.

Par exemple les trames ETHERNET II pour TCP/IP ont toutes la même structure :

La longueur d'une trame ETHERNET est comprise entre 64 et 1518 Octets. Les informations d'en-tête et de queue requièrent 18 Octets, il reste donc un espace de 46 à 1500 Octets pour les données.

XII-5 - Les normes du réseau ETHERNET

Les normes Ethernet s'expriment toutes de la même façon (« x » modulation « y ») :

Les normes IEEE définissent les spécifications relatives à la mise en oeuvre de plusieurs types de réseaux ETHERNET.

Il arrive fréquemment que de grands réseaux combinent plusieurs normes en même temps...

Les normes IEEE à 10Mb/s ne furent pas assez rapides pour supporter des applications gourmandes en bande passante (CAO, FAO, la vidéo, la GED, ...). Aussi, les comités IEEE développèrent de nouvelles normes pour des réseaux à 100 Mb/s comme 100VG-AnyLAN et 100BaseX. Ces nouvelles normes sont compatibles avec le 10BaseT, et leur implantation n'est pas synonyme de restructuration...

XII-6 - Les systèmes d'exploitation sur un réseau ETHERNET

De nombreux systèmes d'exploitation réseaux fonctionnent sur un réseau ETHERNET :

XII-7 - Le tableau récapitulatif des réseaux ETHERNET à 10 Mb/S

Tableau récapitulatif des réseaux ETHERNET à 10 Mb/s				
	10BaseT	10Base2	10Base5	10BaseFL
Nom	Ethernet	Thinnet	Ethernet Standard	
Norme	IEEE 802.3	IEEE 802.3	IEEE 802.3	IEEE 802.8
Débit	10 Mb/s	10 Mb/s	10 Mb/s	10 Mb/s
La transmission des signaux	bande de base	bande de base	bande de base	bande de base
L'accès au réseau	CSMA/CD	CSMA/CD	CSMA/CD	CSMA/CD
Topologies	En étoile, en bus en étoiles	En bus	En bus, une dorsale et des bus	En bus
Règle		Règle des 5-4-3	Règle des 5-4-3	
Dorsale	Concentrateurs		Transceivers	
Câbles	Paire torsadées	Coaxial fin	Coaxial épais	Fibre optique
Catégorie câble	UTP 3, 4 et 5	RG-58		
Plusieurs câbles	UTP ou STP (Une		Coaxial épais	La fibre optique pour

Tableau récapitulatif des réseaux ETHERNET à 10 Mb/s				
	dorsale en coaxial ou en fibre optique)		(principale) et coaxial fin (secondaires)	relier entre des répéteurs
Impédance câble		50 Ohms		
Prises vampires	(Si dorsale)	NON	OUI	
Transceiver	(Si dorsale en coaxial épais)	OUI	Reliés à un répéteur	
Câbles de transceiver	Si dorsale	OUI	OUI, 50 mètres	
Concentrateurs	Répéteurs multiports			
Connecteurs	RJ45 et/ou AUI (si dorsale)	BNC et AUI s'il y a un transceiver	AUI ou DIX	
Résistance des connecteurs		50 Ohms	50 Ohms	
Bouchons et prolongateurs		BNC	Série N	
Cartes réseaux	RJ45; AUI (si dorsale)	Compatible BNC	Compatible AUI (ou DIX)	
Segment	100 mètres	185 mètres	500 mètres	2000 mètres
Répéteurs	OUI	OUI	OUI	OUI, en fibre
Réseau		925 mètres	2500 mètres	
Câble de descente		inférieur à 50 mètres	inférieur à 50 mètres	
Écart entre deux ordinateurs	2,5 mètres	0,5 mètre	2,5 mètres (hors câble de descente)	
Noeuds par segment		30 noeuds	100 noeuds	
Noeuds par réseaux	1024 transceivers	86 stations	296 stations	
Utilisation			Un immeuble	Entre bâtiments

XII-8 - Le 10BaseT

90% des nouvelles installations utilisent un réseau Ethernet 10BaseT avec un câblage UTP de catégorie 5, parce que ce type de câble permet ensuite de passer à un débit de 100 Mb/s.

Les réseaux ETHERNET en 10BaseT utilisent en général des câbles en paires torsadées non blindées (UTP), mais ils fonctionnent tout aussi bien avec des câbles en paires torsadées blindées (STP).

La topologie des réseaux ETHERNET en 10BaseT ressemble généralement à une étoile avec un concentrateur (HUB), mais le concentrateur central contient en réalité un bus interne. Le concentrateur sert de répéteur multiports et se trouve souvent dans une armoire de câblage. Des répéteurs peuvent être utilisés pour allonger la longueur du câble qui est limité à 100 mètres.

Un réseau ETHERNET en 10BaseT offre les avantages d'une topologie en étoile, il est aisé de déplacer une station vers un autre endroit, sans pour cela interrompre le réseau. Il suffit pour cela de changer le cordon du tableau de connexion qui se trouve dans l'armoire de câblage...

Plusieurs concentrateurs peuvent être reliés ensemble par une dorsale en câble coaxial ou en fibre optique. Selon la spécification IEEE 802.3, 1024 ordinateurs peuvent appartenir au même réseau ETHERNET 10BaseT, sans composants de connectivité...

Les caractéristiques de L'ETHERNET en 10BaseT :

- « 10 » pour 10 Mb/s
- « Base » pour la transmission des signaux en bande de base
- « T » pour les câbles à paire torsadées :
- Câbles à paires torsadées non blindées (UTP catégorie 3, 4 et 5)
- Câbles à paires torsadées blindées (STP)
- La méthode d'accès au réseau CSMA/CD
- Des connecteurs RJ45
- Des cartes réseaux compatibles RJ45
- Avec un transceiver intégré
- Avec un transceiver externe
- La longueur maximale d'un segment est de 100 mètres (c'est la distance entre le concentrateur et le transceiver de l'ordinateur)
- L'écart minimal entre deux ordinateurs est de 2,5 mètres
- Le nombre maximal d'ordinateurs est de 1024 transceivers
- Un ou des concentrateurs (répéteur multiports)
- Un seul concentrateur pour une topologie en étoile
- Plusieurs concentrateurs reliés ensemble par une dorsale (en câble coaxial ou une fibre optique) pour une topologie en bus en étoile
- Des répéteurs pour allonger la longueur d'un segment

XII-9 - Le 10Base2

Le 10Base2 est aussi appelé ETHERNET fin (THINNET). Les réseaux ETHERNET en 10Base2 utilisent des câbles coaxiaux fins. Les spécifications IEEE 802.3 n'autorisent pas de transceiver entre le connecteur BNC en « T » du câble et la carte réseau de l'ordinateur ; le câble se branche directement sur un connecteur BNC de la carte réseau. Un réseau ETHERNET FIN peut combiner jusqu'à 5 segments de câbles reliés par 4 répéteurs, mais 3 seulement de ces segments pourront accueillir des stations, c'est la règle des 5-4-3. Deux segments doivent rester inexploités, ils servent de liaisons inter répéteurs et permettent d'augmenter la longueur total du réseau. La spécification IEEE 802.3 recommande un maximum de 30 noeuds (ordinateurs, répéteurs,...) par segment, et un maximum de 1024 ordinateurs pour la totalité d'un réseau.

Les réseaux ETHERNET FIN sont de bonnes solutions pour les petits réseaux, bon marché, simple à installer et facile à configurer...

Les caractéristiques de L'ETHERNET en 10Base2 :

- « 10 » pour 10 Mb/s
- « Base » pour la transmission des signaux en bande de base
- « 2 » parce que le câble coaxial fin (RG-58 avec une impédance de 50 Ohm) peut transporter un signal sur une distance d'à peu près 2x100 mètres, en fait 185 mètres
- La méthode d'accès au réseau CSMA/CD
- Des connecteurs, des prolongateurs et des bouchons de terminaisons BNC (résistance de 50 Ohm)
- Des cartes réseaux compatibles BNC
- La longueur maximale d'un segment est de 185 mètres
- L'écart minimum entre deux stations est de 0,5 mètre
- La longueur maximum pour le câble de descente (le « drop cable » en anglais) est de 50 mètres.
- Un nombre maximal de 30 noeuds (ordinateurs, répéteurs,...) par segment
- La longueur maximale pour la totalité du réseau est de 925 mètres (185x5)
- Le nombre maximal d'ordinateur sur le réseau est de 86 stations (29+1+28+1+1+1+29)

- Une topologie en bus
- Des répéteurs pour allonger la longueur du réseau

XII-10 - Le 10Base5

Les réseau ETHERNET en 10Base5 sont aussi appelés ETHERNET STANDARD (STANDARD ETHERNET). Les réseaux ETHERNET en 10Base5 utilisent des câbles coaxiaux épais (ETHERNET EPAIS ou THICK ETHERNET).

Le câble principal est appelé une dorsale (BACKBONE). Des prises vampires percent la dorsale, et des transceivers se branchent sur les prises vampires. Les transceivers ont des connecteurs AUI ou DIX à 15 broches d'où partent les câbles de transceiver ou autrement dit les câbles de descente. Le câble de descente se branche au connecteur AUI ou DIX de la carte réseau. Le transceiver assure les communications entre l'ordinateur et le câble principal. Les connecteurs AUI ou DIX sont situés à chaque extrémité du câble de transceiver.

La même règle des 5-4-3 s'applique aux réseaux ETHERNET STANDARD (5 segments, 4 répéteurs, 3 segments seulement peuvent accueillir des stations).

La combinaison des câbles en coaxial fin et en coaxial épais permet de construire un réseau vaste et fiable. Des câbles ETHERNET EPAIS sont utilisés pour le câble principal (une dorsale en coaxial épais), et des câbles ETHERNET FIN sont utilisés pour les câbles secondaires (en coaxial fin). Le transceiver du câble principal est relié à un répéteur, et le répéteur est relié au câble secondaire qui accueille les stations.

Les distances et les tolérances du câble ETHERNET EPAIS sont plus importantes que celles du câble EHERNET FIN, c'est pourquoi il est souvent utilisé pour desservir tout un immeuble...

Les caractéristiques de L'ETHERNET en 10Base5 :

- « 10 » pour 10 Mb/s
- « Base » pour la transmission des signaux en bande de base
- « 5 » parce que le câble coaxial épais (peut transporter un signal sur une distance de 5x100 mètres, donc de 500 mètres
- La méthode d'accès au réseau CSMA/CD
- Des câbles de transceiver (ou câbles de descentes de 3/8 pouces) qui relient la carte réseau d'un ordinateur au transceiver de la dorsale
- Des connecteurs AUI ou DIX pour le branchement aux cartes réseaux et aux transceivers de la dorsale
- Des prolongateurs et des bouchons de terminaisons de série N (résistance de 50 Ohm)
- Des cartes réseaux compatibles AUI ou DIX
- La longueur maximale d'un segment est de 500 mètres
- L'écart minimum entre deux stations est de 2,5 mètres. Cette distance ne comprend pas la longueur du câble de descente, mais mesure la distance entre deux transceiver sur le câble principal.
- La longueur maximale du câble de transceiver est de 50 mètres. C'est la distance entre l'ordinateur et le transceiver du câble principal.
- Un nombre maximal de 100 noeuds (ordinateurs, répéteurs,...) par segment
- La longueur maximale pour la totalité du réseau est de 2500 mètres (500x5)
- Le nombre maximal d'ordinateur sur le réseau est de 296 stations (99+1+98+1+1+1+99)
- Une topologie en bus ou en bus avec une dorsale (BACKBONE)

- Des répéteurs pour allonger la longueur du réseau

XII-11 - Le 10BaseFL

La norme IEEE 802.8 concerne les réseaux ETHERNET en 10BaseFL qui utilisent des câbles en fibre optique.

Les câbles en fibre optique permettent d'installer de très long câbles entre des répéteurs. Les répéteurs spéciaux pour la fibre optique sont nécessaires pour convertir le signal lumineux en un signal électrique. L'ETHERNET en 10BaseFL permet de relier deux bâtiments.

Les caractéristiques de l'ETHERNET en 10BaseFL :

- « 10 » pour 10 Mb/s
- « Base » pour la transmission des signaux en bande de base
- « FL » pour Fiber Link, c'est à dire pour désigner les câbles en fibre optique
- La méthode d'accès au réseau CSMA/CD
- La longueur maximale d'un segment est de 2000 mètres
- Des répéteurs pour la fibre optique

XII-12 - Le 100VG-AnyLAN

L'architecture des réseaux 100VG-AnyLAN a été développée par la société HEWLETT-PACKARD. La norme IEEE 802.12 définie les spécifications des réseaux 100VG-AnyLAN.

Les réseaux 100VG-AnyLAN combinent les caractéristiques des réseaux ETHERNET (norme IEEE 802.3) et des réseaux TOKEN RING (norme IEEE 802.5). Les réseaux 100VG-AnyLAN s'appellent indifféremment 100BaseVG, VG, AnyLAN

Les réseaux 100VG-AnyLAN fonctionnent avec la méthode d'accès de la priorité de la demande qui autorise deux niveaux de priorité (haute et basse).

Les réseaux 100VG-AnyLAN offre la possibilité de filtrer les trames au niveau d'un concentrateur, ce qui permet d'accroître la confidentialité des données. Les réseaux 100VG-AnyLAN permettent de transmettre les trames de type ETHERNET et les trames de type TOKEN RING.

Les réseaux 100VG-AnyLAN s'appuient sur une topologie en étoile autour d'un concentrateur. La topologie en étoile en cascade s'appuie autour d'un concentrateur principal appelé « parent » auquel sont reliés des concentrateurs secondaires appelés « enfants ». Les concentrateurs des réseaux 100VG-AnyLAN sont spécifiques à cette norme. Les câbles des réseaux 100VG-AnyLAN sont plus courts que ceux des réseaux 10BaseT, c'est pourquoi ils sont souvent équipés de plus de boîtier...

Les caractéristiques de l'ETHERNET en 100BaseVG :

- « 100 » pour 100 Mb/s
- « Base » pour la transmission des signaux en bande de base
- « VG » pour Voice Grade
- Des câbles en paires torsadées de catégorie 3, 4 et 5, ou avec de la fibre optique
- La méthode d'accès au réseau priorité de la demande
- La longueur de câble est limitée à 250 mètres
- Topologie en étoile ou en étoile en cascade

XII-13 - Le 100BaseX

Le 100BaseX est aussi appelé le FAST ETHERNET. Le 100BaseX est issu d'une extension de la norme ETHERNET.

Le 100BaseX englobe trois normes différentes :

- Le 100BaseT4 pour la paire torsadée à quatre paires de fils
- Le 100BaseTX pour la paire torsadée à deux paires de fils
- Le 100BaseFX pour la fibre optique

Les caractéristiques de l'ETHERNET en 100BaseX :

- « 100 » pour 100 Mb/s
- « Base » pour la transmission des signaux en bande de base
- « X » pour « T4 », « TX » ou « FX » selon le câblage
- La méthode d'accès CSMA/CD
- Les câbles :
- Pour la norme 100BaseT4, des câbles de type téléphonique à paires torsadées non blindées (UTP quatre paires de la catégorie 3, 4 et 5) avec quatre paires de fils (TELEPHONE GRADE)
- Pour la norme 100BaseTX, des câbles de type transmission de données (DATA GRADE) à paires torsadées non blindées ou blindées (UTP ou STP à deux paires de fils de la catégorie 5)
- Pour la norme 100BaseFX, des câbles en fibre optique
- Des concentrateurs
- Topologie en bus en étoile

XIII - Les réseaux TOKEN RING

XIII-1 - La version IBM des réseaux TOKEN RING

La version IBM des réseaux TOKEN RING est sortie en 1984, et a la particularité de fonctionner avec toutes les dimensions de sa gamme d'ordinateurs :

- Les ordinateurs personnels IBM PC compatibles
- Les mini-ordinateurs
- Les gros systèmes évoluant dans un environnement réseau SNA (System Network architecture)

En 1985, le réseau TOKEN RING d'IBM devient une norme ANSI/IEEE. Les réseaux TOKEN RING se conforment à la norme IEEE 802.5.

XIII-2 - L'architecture des réseaux TOKEN RING

Les réseaux TOKEN RING se différencient des autres réseaux plus par la méthode d'accès au réseau (le passage du jeton), que par la composition (la paire torsadée) ou la disposition (en anneau) du câblage.

L'architecture des réseaux TOKEN RING se présente sous la forme d'un « anneau physique ». L'architecture de la version IBM des réseaux TOKEN RING est un anneau en étoile, les ordinateurs sont tous connectés à un concentrateur central (une étoile) dans lequel se trouve l'anneau physique ; on parle « d'anneau logique » pour expliciter le fait que l'aspect du réseau soit en étoile, mais que la circulation des trames est en anneau.

Il y a deux sortes de Token Ring :

- Le Token Ring en anneau, c'est le Token Ring « normal ».
- Le Token Bus, c'est le Token Ring sur un support en bus.

XIII-3 - Les caractéristiques des réseaux TOKEN RING

Les caractéristiques des réseaux TOKEN RING sont les suivantes :

- La spécification IEEE 802.5
- Une topologie en anneau en étoile
- La méthode d'accès au réseau le passage du jeton
- Le mode de transmission des signaux en bande de base
- Le câblage en paires torsadées non blindées (UTP) ou blindées (STP), rarement de la fibre optique.
- Les types 1, 2 et 3 des câbles IBM
- Un débit de 4 ou 16 Mb/s

XIII-4 - Le format de la trame TOKEN RING

La trame est constituée de la manière suivante :

XIII-5 - Les conditions de fonctionnement d'un réseau TOKEN RING

La méthode d'accès au réseau le passage du jeton implique certaines conditions :

- Il ne peut avoir qu'un seul jeton sur le réseau à un moment donné.
- Le jeton ne circule que dans un seul sens, la circulation des données est unidirectionnelle. Ce qui permet de n'utiliser qu'un seul brin de fibre optique par exemple...
- Il ne peut avoir qu'un seul ordinateur émetteur en même temps. Seul l'ordinateur qui s'empare du jeton peut transmettre sur le réseau. Il ne peut avoir ni contention ni de collision. Le passage du jeton est déterministe, c'est à dire qu'un ordinateur ne peut pas forcer l'accès au réseau.
- Tous les ordinateurs du réseau régénèrent les trames qui passent et les renvoient sur le réseau. Les ordinateurs font office de répéteur unidirectionnel.
- Le premier ordinateur allumé sur le réseau crée un jeton et assure la surveillance du réseau. Il se désigne comme le contrôleur du réseau s'assure que le réseau fonctionne normalement, et il vérifie si les trames sont correctement émises.
- Un réseau TOKEN RING ne fonctionne qu'à une seule vitesse de transmission de 4 Mb/s ou de 16 Mb/s selon les cartes réseaux.
- Un réseau TOKEN RING transmet en continu (DATA STREAMING).

XIII-6 - Le contrôleur du réseau TOKEN RING

Le contrôleur du réseau est souvent la première machine allumée sur le réseau. Le contrôleur du réseau est responsable du bon fonctionnement du système TOKEN RING, et ses tâches sont multiples :

- Le contrôleur du réseau s'assure qu'il n'y a qu'un seul jeton qui circule.
- Le contrôleur du réseau détecte si des trames ont fait plus d'une fois le tour de l'anneau.
- Le contrôleur du réseau s'assure qu'il n'y a pas d'adresse en double. L'adresse de chaque machine sur le réseau est unique.
- Le contrôleur du réseau prévient les autres ordinateurs de l'arrivée d'une nouvelle station sur le réseau.

XIII-7 - La circulation du jeton dans un réseau TOKEN RING

L'initialisation d'un réseau TOKEN RING suit une procédure stricte et systématique :

- Un ordinateur émet un jeton sur le réseau (le premier ordinateur du réseau qui s'allume).
- Le jeton circule autour de l'anneau dans le sens des aiguilles d'une montre. Les ordinateurs allumés du réseau qui veulent émettre vérifient si la trame qui circule est un jeton.
- Un ordinateur s'empare du jeton quand il veut transmettre sur le réseau, seul l'ordinateur qui détient le jeton peut transmettre des informations sur le réseau. L'ordinateur en possession du jeton émet ses trames sur le réseau.
- La trame circule sur le réseau et passe devant tous les ordinateurs.
- Les ordinateurs du réseau vérifient si la trame leur est destinée
- L'ordinateur récepteur recopie la trame qui lui est destinée dans sa mémoire tampon. L'ordinateur récepteur modifie le champ d'état de la trame pour indiquer que celle-ci a été recopiée par son destinataire. L'ordinateur récepteur renvoie la trame sur le réseau.
- La trame circule de nouveau sur le réseau
- L'ordinateur émetteur réceptionne la trame, vérifie qu'elle a bien atteint sa cible, en accuse réception, et la détruit. L'ordinateur continue d'émettre jusqu'à la fin de sa transmission. Le jeton est replacé sur le réseau quand l'ordinateur a terminé sa transmission.
- Le jeton circule sur le réseau.

XIII-8 - Les composants matériels d'un réseau TOKEN RING

Le réseau TOKEN RING fonctionne en général autour d'un concentrateur passif dans lequel se situe l'anneau physique du réseau. Cependant, un réseau TOKEN RING peut être composé au maximum de 33 concentrateurs (l'empilement des concentrateurs ne forment qu'un seul anneau logique). Plus le réseau TOKEN RING comporte de concentrateurs et plus il est à même de gérer un nombre important d'ordinateurs. Les concentrateurs sont reliés entre eux par les points de connexion (en entrée et en sortie) qui permettent de ne constituer qu'un seul anneau. Les concentrateurs sont reliés par un câblage en paire torsadées.

Dans un « réseau à jeton pur », si une station tombe en panne, alors c'est tout le réseau qui ne fonctionne plus puisque la course du jeton est interrompue. Certaines MSAU peuvent détecter l'arrêt d'une carte réseau et automatiquement désactiver le port correspondant, ainsi l'anneau logique n'est pas « coupé ».

Le concentrateur MSAU de chez IBM a 10 ports de connexion et peut relier 8 ordinateurs. Le câblage est le plus souvent de l'UTP, mais le STP et la fibre optique sont aussi employés.

Les composants matériels d'un réseau TOKEN RING sont les suivants :

XIII-9 - Le Token Bus

Le Token Bus est une architecture qui correspond à une topologie logique en anneau sur un support physique en bus. Chaque station connaît l'adresse de la station précédente, et celle de la station suivante (dans un anneau virtuel) à l'aide d'une table de correspondance, qui est mise à jour à chaque fois qu'une station est installée. Les communications se passent comme si c'était un anneau, les paquets circulent de station en station, les stations attendent d'avoir le jeton pour communiquer, et les bouchons de terminaison absorbent les paquet en bout de câble...

XIV - Les réseaux étendus

XIV-1 - L'accès à distance

L'accès à distance est une fonction importante des réseaux parce qu'il permet d'accéder aux ressources d'un réseau loin du lieu physique où il se trouve. L'accès à distance caractérise les réseaux étendus.

L'accès à distance peut s'effectuer de deux façons différentes :

XIV-1-1 - L'accès à Internet par un Fournisseur d'Accès à Internet

L'accès à Internet s'effectue en général par l'intermédiaire d'un Fournisseur d'Accès à Internet (FAI) aussi appelé un Provider (ISP pour Internet Service Provider en anglais), dans le cadre d'un abonnement forfaitaire à une ligne analogique via un modem par exemple.

Le plus souvent la connexion au Fournisseur d'accès à Internet s'effectue avec le protocole PPP et une adresse IP dynamique est allouée par le Provider. Les adresses IP dynamiques ne permettent pas de router soi-même le courrier électronique, ni d'avoir son propre serveur WEB, sauf utilisation de services spéciaux de DNS (dyndns, no-ip). Les messages électroniques sont récupérés et envoyés au serveur de messagerie du Provider en utilisant le protocole POP 3 ou IMAP 4, et ils sont routés sur le réseau Internet avec le protocole SMTP.

Il est possible de recevoir une adresse IP fixe de la part du Provider, cela coûte plus cher qu'une adresse IP dynamique, mais moins cher qu'une liaison numérique dédiée.

XIV-1-2 - L'accès à Internet par un opérateur téléphonique

L'accès à Internet peut également s'effectuer par l'intermédiaire d'un opérateur téléphonique, dans le cadre d'un abonnement permanent à une ligne numérique dédiée via un routeur et un dispositif de connectivité spécialisé par exemple.

Les paquets du réseau interne destinés à Internet sont filtrés et routés par le routeur (en utilisant le protocole EGP par exemple), puis les paquets sont transmis à Internet par le dispositif de connectivité spécialisé. C'est le dispositif de connectivité spécialisé qui assure la liaison avec le réseau Internet. Le plus souvent la connexion à une ligne numérique dédiée permet d'avoir une adresse IP fixe. Une adresse IP fixe permet d'avoir son propre serveur WEB et son propre serveur de messagerie pour router les messages électroniques directement avec SMTP.

XIV-1-3 - Les ressources d'Internet

L'accès à Internet permet de se connecter aux ressources du réseau des réseau :

- Consulter ou créer un site WEB
- Communiquer par e-mail
- Télécharger des fichiers par FTP
- Dialoguer dans les salons CHAT avec IRC

- Échanger des Informations avec USENET (les newsgroups, les listes, les forums de discussion)
- Rechercher des informations avec GOPHER et ARCHIE
- Contrôler un hôte distant avec TELNET

XIV-1-4 - Les qualifications d'une connexion à Internet

Les connexions à Internet peuvent être qualifiées en fonction de plusieurs critères qui ne sont pas exclusifs les uns des autres, et qui peuvent au contraire se combiner :

- Les adresse IP dynamiques pour simplement avoir accès aux ressources d'Internet de temps en temps et pour des durées variables mais plutôt courtes.
- Les adresses IP fixes pour assurer une présence constante sur Internet.
- Les connexions mono utilisateur pour les particuliers.
- Les connexions multi utilisateurs pour les entreprises, la bande passante est alors divisée par le nombre de connexion simultanées.
- Les « connexions à la demande » passent par un serveur Internet installé sur l'Intranet d'une entreprise, lequel se connecte automatiquement au fournisseur d'accès quand l'un des utilisateurs émet une requête sur Internet.
- Les matériels réseaux de Danya
- Le programme Steelhead de Microsoft pour Windows NT
- La connexion de trois lignes simultanément via Multilink PPP permet d'augmenter la bande passante.
- Les « connexions manuelles » sont effectuées par les utilisateurs qui se déplacent sur le serveur Internet de l'Intranet de l'entreprise.
- Les « connexions permanentes » s'effectuent à l'aide d'une adresse IP fixe via une ligne analogique (et par l'intermédiaire d'un ordinateur qui fait office de passerelle par défaut), ou mieux mais plus chère, via une ligne numérique dédiée (et par l'intermédiaire d'un routeur qui filtre et route les paquets vers Internet, le routeur est alors la passerelle par défaut du réseau, c'est à dire la passerelle par laquelle transitent tous les paquets qui ne sont pas destinés au réseau interne). Les connexions permanentes doivent être protégées des intrusions malveillantes de l'extérieur. Cette protection est mis en place par un parefeu (un firewall en anglais).
- Les « connexions à distance » permettent à un utilisateur itinérant de se connecter au réseau Intranet de son entreprise. La connexion à distance s'effectue généralement avec un ordinateur portable, un modem et un abonnement à un fournisseur d'Accès à Internet via une ligne analogique et un numéro de serveur national. Le réseau Intranet de l'entreprise doit être en mesure d'attendre l'appel de l'utilisateur distant, c'est le rôle du serveur RAS qui est connecté à Internet en permanence.
- Les connexions analogiques utilisent des lignes analogiques et passent généralement par un fournisseur d'accès qui lui-même loue des lignes à l'opérateur téléphonique pour se connecter au réseau Internet. Les connexions analogiques s'effectuent avec le protocole PPP.
- Les connexions numériques utilisent les lignes numériques, soit en passant par l'intermédiaire d'un Provider, soit directement par l'opérateur téléphonique. Les connexions numériques s'effectuent avec un modem Bande de Base et le protocole BGP ou EGP.

XIV-1-5 - La retransmission des adresses IP

La retransmission d'adresses IP (IP Forwarding) est un mécanisme (installé sur un serveur Internet du réseau Intranet d'une entreprise) qui permet de rediriger les paquets Internet vers les ordinateurs de l'Intranet et vice versa. Le serveur Internet reçoit les demandes internes qui peuvent provenir de plusieurs ordinateurs en même temps, et les redirige sur Internet en utilisant l'adresse IP allouée par le Provider ; ensuite, le serveur Internet reçoit les réponses (qui sont toutes envoyées à la même adresse IP, celle qui est allouée par le Provider) et les redirige vers chaque poste en interne qui en a fait la demande. Le serveur Internet doit mémoriser qui demande quoi, quelle est l'adresse interne qui communique avec telle ou telle adresse externe. Toutes les communications vers l'extérieur passent par le serveur Internet et utilisent la même adresse IP. La retransmission d'adresse IP fonctionne avec une adresse IP dynamique ou fixe.

XIV-1-6 - Les adresses IP internationales

Le réseau Internet utilise la pile de protocole TCP/IP, et pour pouvoir y accéder, il faut une adresse IP internationale, parmi celles qui sont attribuée par Internic. Les adresses IP allouées par le Fournisseur d'Accès à Internet sont des adresses qui ont été achetées à Internic, elles constituent un pool d'adresses que le Provider distribue à ses clients.

Le protocole TCP/IP peut être également utilisé dans un réseau Intranet, les ordinateurs du réseau interne disposent d'une adresse IP (mais ces adresses IP n'ont rien avoir avec celles qui sont utilisées sur Internet). Quand le réseau Intranet est connecté à Internet, et que les deux réseaux utilisent le protocole TCP/IP, il ne faut pas faire la confusion entre les adresses IP internes et les adresses IP externes. Souvent, les ordinateurs de l'Intranet s'adressent à la passerelle par défaut pour communiquer avec Internet, alors seule la passerelle par défaut dispose d'une adresse IP internationale.

Toutefois, il peut arriver que tous les ordinateurs de l'Intranet est besoin d'une adresse IP internationale, dans ce cas, l'entreprise achète une classe d'adresse à Internic, et l'entreprise dispose d'une plage d'adresse IP internationale qu'elle peut répartir à tous ou une partie de ces ordinateurs. Les plages d'adresses IP, qu'elles soient internationales ou internes peuvent être fixes ou dynamiques à l'intérieur du réseau Intranet. Quand les adresses IP sont dynamiques, elles sont allouées par un serveur DHCP (Dynamic Host Configuration Protocol) pour une durée déterminée à chaque ordinateur qui en fait la demande.

Les réseaux Intranet qui utilisent un autre protocole que TCP/IP, par exemple SPX/IPX, peuvent avoir recours à une passerelle de traduction de protocole pour pouvoir accéder à Internet. Par contre, un réseau Intranet qui comporte un serveur Web ouvert sur Internet devra obligatoirement utiliser le protocole TCP/IP pour pouvoir communiquer avec les internautes qui se connectent au serveur web de l'entreprise.

XIV-1-7 - La protection contre les intrusions d'Internet

Les connexions permanentes doivent être protégées des intrusions malveillantes de l'extérieur. Cette protection est mise en place par un parefeu (un firewall en anglais). Un firewall est un ordinateur qui s'intercale entre le réseau Intranet et le réseau Internet, et qui vérifie et authentifie toutes les connexions qui proviennent de l'extérieur.

Le firewall peut être installé sur un tout petit réseau (appelé réseau DMZ pour zone démilitarisée). Le réseau DMZ joue le rôle d'un sas, c'est à dire d'un lieu où transitent les paquets sortants et les paquets entrants. Il y a donc trois principaux réseaux en présence :

Le firewall est alors intercalé entre le concentrateur du réseau Intranet et le routeur qui est lui-même connecté au dispositif de connectivité pour l'Internet ; le firewall dispose ainsi de deux cartes réseaux.

Le réseau DMZ peut également inclure un serveur proxy qui permet de cacher les adresses IP internes au réseau Intranet. Les ordinateurs du réseau Intranet s'adressent toujours au serveur proxy pour lancer une requête vers l'Internet. Le serveur proxy fait la demande en son propre nom, c'est à dire qu'il recherche sur Internet les informations demandées par les stations locales avec sa propre adresse IP. Quand le serveur proxy reçoit la réponse, il la dispatche à la station du réseau Intranet.

XIV-1-8 - Le réseau DMZ

Un réseau DMZ est généralement constitué de plusieurs dispositifs :

- Le dispositif de connectivité relié à Internet (un commutateur DSUACSU (pour une liaison numérique par exemple) qui établit la liaison avec le serveur du fournisseur d'Accès à Internet).
- Le routeur qui filtre et route les paquets provenant de l'Intranet vers Internet.
- Le concentrateur du réseau DMZ
- Le serveur proxy qui filtre les requêtes internes pour Internet.
- Le firewall qui filtre les connexions externes. Le firewall a deux cartes réseaux, l'une dirigée vers le réseau DMZ et l'autre vers le concentrateur du réseau Intranet.

XIV-1-9 - L'envergure des réseaux étendus

Les réseaux étendus sont les réseaux qui dépassent l'envergure d'un réseau local. Les réseaux étendus sont généralement la réunion de plusieurs réseaux, ou du moins l'ensemble des moyens de communication qui permettent de réunir plusieurs réseaux :

- Les réseaux MAN (Metropolitan Area Network) sont à l'échelle d'une ville
- Les réseaux WAN (Wide Area Network) sont à l'échelle des continents

Un WAN est souvent constitué de deux LAN reliés entre eux par une ligne téléphonique numérique dédiée à haut débit. Les WAN conviennent aux multinationales qui souhaitent établir une présence significative dans le monde entier...

Un réseau MAN ou WAN peut être entièrement constitué de composants privés ou loués selon que les dispositifs de connectivité et les lignes sont privées ou louées. Un MAN ou un WAN peut faire partie ou non du réseau Internet, selon que ces données transitent ou non par le réseau Internet.

Selon le nombre de personnes qui se connecte en même temps à un réseau à distance, il peut être intéressant de construire un pool de modem sur un serveur.

Les principaux systèmes d'exploitation réseau propose des solutions de connexion distante simultanée :

- RAS (Remote Access Service) de Windows NT de Microsoft
- Netware Connect de Novell
- LAN Distance d'OS/2 d'IBM
- Les multiples Daemon du système UNIX

Outre ces solutions « internes » au réseau préexistant, il existe des solutions dédiées, propriétaires et indépendantes qui peuvent s'interfacer avec le système d'exploitation réseau qui a été mis en place :

- Les serveurs de communication LANrover de Shiva
- CUBIX
- MultiTech

XIV-1-10 - Les débits des réseaux étendus

Les débits (ou la bande passante) des réseaux étendus (et le coût) diffèrent selon les technologies employées :

- RNIS à 128 Kb/s pour 2 canaux B
- Frame Relay à 56 Kb/s
- FDDI à 100 Mb/s
- T1 à 1,544 Mb/s
- T3 à 45 Mb/s
- L'ATM qui est la technologie émergeante, et qui peut atteindre 155 Mb/s voire 622 Mb/s)

Les lignes numériques des réseaux longue distance WAN ne sont pas aussi rapides que les supports de communication des réseaux LAN :

- 10 Mb/s au minimum avec du coaxial
- 100 Mb/s pour de l'UTP catégorie 5
- 622 Mb/s voire 1 Gb/s pour la fibre optique

Ainsi, les liaisons distantes entre deux réseaux locaux sont toujours un facteur de ralentissement.

XIV-2 - Les caractéristiques des réseaux étendus

Les réseaux étendus permettent à des utilisateurs distants (de différents endroits) d'accéder en temps réel à une base de données (un système transactionnel qui rassemble des données communes à plusieurs sites par exemple).

L'établissement d'un réseau étendu devra prendre en considération plusieurs facteurs :

Les moyens nécessaires pour installer et maintenir des liaisons distantes sont tellement importants que les entreprises louent les services de fournisseurs internationaux.

Il peut arriver qu'un réseau utilise plusieurs types de supports de communication, plusieurs vitesses de transmission, plusieurs modes de transmission, plusieurs protocoles réseaux, plusieurs technologies ou architectures réseaux et plusieurs interconnections à plusieurs réseaux...

On peut dire aujourd'hui que « l'ordinateur, c'est le réseau ».

XIV-2-1 - La gestion des coûts des réseaux étendus

La gestion des coûts des réseaux étendus est une notion fondamentale et déterminante, que ce soit du point de vue de la décision de la mise en place d'une telle infrastructure, que du point de vue de la conservation d'un tel système. Les réseaux étendus coûtent très chers en achat, en location et en services.

Les réseaux étendus sont très coûteux :

- Le prix de la ligne numérique
- Le prix de l'installation
- Le prix des équipements spéciaux
- Le prix de la maintenance et de l'assistance (dans les différents sites)

Les coûts d'assistance et de maintenance sont souvent « cachés », mais ils représentent une part non négligeable du coût total de fonctionnement (le TCO pour Total Cost of Ownership). Ainsi, le retour sur investissement (RSI) d'une telle infrastructure est, quand on peut le calculer, un critère déterminant pour les « décisionnels ».

Les lignes des opérateurs téléphoniques sont assez chères pour pouvoir exiger la garantie d'une certaine qualité et pérennité de service :

- L'engagement de disponibilité (SLA pour Service Level Agreement) permet de se prémunir des ruptures « accidentelles » des lignes ou du moins d'en être dédommagées.
- Les contrats de qualité de service (QOS pour Quality Of Service) permettent de garantir un certain niveau de bande passante pendant toute la durée de l'abonnement.

Un moyen de réduire le coût d'un WAN est de l'externaliser. L'externalisation d'un WAN peut être réaliser auprès de plusieurs types d'entreprises :

- Les intégrateurs de systèmes réseaux, les entreprises de type SSII qui jouent le rôle du maître d'ouvrage
- Les grands groupes de consultants
- Les fournisseurs d'accès à Internet qui vendent plutôt des services de connexion (leur infrastructure réseaux est déjà en place) que des services d'expertise. Il « suffit » de paramétrer les routeurs pour réexpédier les paquets de l'entreprise, ou d'installer un Réseau Privé Virtuel (ou VPN pour Virtual Private Network en anglais) qui utilise le réseau Internet. Les solutions via Internet ne sont pas très sécurisées, et les nombreuses possibilités de capture ou d'interception des données doivent être prises en compte.

XIV-2-2 - Les modes de transmission des réseaux étendus

Les modes de transmission des réseaux étendus peuvent se différencier soit par le type de signal (analogique ou numérique), soit par le chemin emprunté par les données (un chemin unique ou plusieurs chemins possibles). Les lignes peuvent être commutées (plusieurs chemins possibles) ou dédiées (un seul chemin) :

- La transmission analogique
- Les lignes commutées du réseau RTC (plusieurs chemins)
- Les lignes louées (un seul chemin)
- La transmission numérique (les données transitent sur un circuit dédié, sauf pour le 56 commuté)
- La commutation de paquets (les paquets peuvent utiliser plusieurs chemins possibles)

Les Réseaux Privés Virtuels (RPV ou VPN) ne sont pas limités aux lignes téléphoniques spécialisées des liaisons numériques, mais ils peuvent aussi être mis en place via une ligne analogique et à travers le réseau Internet.

XIV-2-3 - Les protocoles d'accès à distance des réseaux étendus

Les protocoles d'accès à distance des réseaux étendus font généralement partie de la pile de protocole TCP/IP (comme SLIP et PPP). Les protocoles SLIP et PPP permettent de transporter les paquets de données sur des lignes téléphoniques analogiques, et éventuellement d'effectuer des contrôles d'erreurs de transmission (pour PPP). Les protocoles SLIP et PPP sont les protocoles utilisés pour une liaison « série », c'est à dire qu'ils ont été développés pour les ordinateurs ne disposant pas de carte réseau, mais seulement d'un port série. Le modem de l'ordinateur (interne ou externe) est connecté à l'un des ports série de l'ordinateur (COM1, COM2, voire COM3 ou COM4). Le modem est relié à la prise téléphonique dans le cas d'une liaison analogique, ou à un adaptateur de terminal ISDN (RNIS ou NUMERIS en France) dans le cas d'une liaison numérique.

Le protocole SLIP est remplacé par le protocole PPP qui est plus performant (plus rapide et plus efficace). Le protocole PPP dispose de plus fonctionnalités (notamment dans le contrôle d'erreurs). Le protocole d'accès à distance PPP peut supporter plusieurs protocoles réseaux simultanément (TCP/IP, NetBEUI, SPX/IPX). Par ailleurs, le protocole PPP gère plusieurs méthodes d'authentification (y compris le système KERBEROS dans lequel les mots de passe ne circulent jamais sur le réseau).

Un modem en attente d'un appel est une tentation pour un « hacker », surtout que généralement le processus d'identification lors d'une connexion distante n'est pas sécurisé. Les logins et les mots de passe circulent « en clair » et l'écoute d'une connexion réussie permet de capturer le login et le mot de passe d'un utilisateur autorisé, et de s'en servir pour une autre connexion.

Il est possible d'améliorer la sécurité des connexions distantes :

Pour les systèmes d'exploitation réseau de Microsoft (Windows 95 et Windows NT,...), la configuration de SLIP ou de PPP s'effectue par l'intermédiaire de l'Accès Réseau à Distance.

Le protocole PPP a besoin de plusieurs paramètres pour établir une connexion distante :

- Le numéro de téléphone du serveur distant (du fournisseur d'accès à Internet par exemple).
- L'adresse DNS du serveur de noms de domaine.
- Une adresse IP statique ou dynamique attribuée par un serveur DHCP.
- L'adresse IP de la passerelle par défaut (éventuellement). C'est l'adresse IP de l'ordinateur qui fait office de passerelle pour pouvoir accéder à Internet.

XIV-2-4 - Le mode de transmission analogique

La transmission analogique s'effectue par l'intermédiaire des câbles des réseaux téléphoniques (une paire de fils en cuivre) :

- Le Réseau Téléphonique Commuté (RTC) en France
- Le PSTN (Public Switched Telephone Network) en « anglais »

Les liaisons analogiques conviennent pour les connexions intermittentes de courte durée, elles ne sont pas aussi fiables que les autres modes de transmission, elles sont lentes et deviennent rapidement coûteuses. Les lignes analogiques ne proposent pas une qualité uniforme et régulière. Les lignes analogiques sont parfois perturbées par un bruit de fond qui induit un brouillage du signal. Les paquets de données doivent être retransmis et une partie de la bande passante non négligeable est utilisée pour la correction des erreurs.

La transmission analogique requière des modems de part et d'autre de la liaison. Les modems effectuent une conversion du signal, ce qui peut ralentir la communication. Les modems ont été inventés pour réduire le besoin des lignes numériques trop onéreuses. Les premiers modems transmettaient les données à 300 bits par secondes. Aujourd'hui, les modems transmettent à 56 Kb/s (en fait, la transmission est asymétrique, 53 Kb/s en download (réception) et seulement 33 Kb/s en upload (émission)). Une très grande partie des informations qui sont transmises par les modems serve au contrôle et à la correction des erreurs de transmission. Les modems se connectent au port série de l'ordinateur.

Les modems utilisent les ports série des ordinateurs, et en général il n'y a que deux ports (COM1 et COM2) sur les ordinateurs INTEL. Toutefois, il existe des « cartes série multiports » qui se branche sur la carte mère, et qui permettent de connecter plus de 16 modems différents sur la même carte série. Ainsi, il est possible de constituer ainsi un pool de modem qui augmente la bande passante disponible pour les utilisateurs d'un réseau LAN qui veulent se connecter simultanément à Internet par exemple.

L'établissement d'une connexion avec un modem est un processus d'une trentaine de secondes.

Les fournisseurs de lignes téléphoniques proposent différents types de lignes :

- Les lignes commutées du réseau RTC sont les lignes téléphoniques standards. Les liaisons sur des lignes commutées sont temporaires avec plusieurs chemins possibles, elles sont ouvertes puis refermées, car la communication téléphonique longue distance reste très chère. Les lignes commutées sont classées et numérotées de 1 à 10 en fonction de leur qualité. Les lignes de type 1 transmettent simplement la voix, tandis que les lignes de type 9 transmettent la voix et la vidéo par exemple.
- Les lignes louées sont des lignes téléphoniques spéciales ou spécialisées. Les lignes louées sont des liaisons permanentes et dédiées (un seul chemin). Les lignes louées sont plus rapides et plus fiables que les lignes commutées (plusieurs chemins).

Les fournisseurs de lignes proposent également des services ou des conditionnements qui accompagnent la ligne proprement dite. Les conditionnements sont classés par des lettres (C ou D) et des chiffres (C1 à C8). Par exemple, une ligne 5/C3 est une ligne de type 5 avec un conditionnement C3.

Le choix entre une ligne commutée ou une ligne louée dépend de plusieurs critères :

- La durée et la fréquence des communications
- Le coût
- Les débits
- La fiabilité
- Les types d'information véhiculés

XIV-2-5 - Le mode de transmission numérique

Le mode de transmission numérique est utilisé quand le mode de transmission analogique n'est pas à la hauteur des exigences du réseau (durée, débit). Les lignes numériques sont plus rapides et plus fiables que les lignes analogiques. Les lignes numériques sont utilisées pour transmettre n'importe quelles données (la voix, les données, les images, la vidéo).

Le mode de transmission numérique n'a pas besoin de convertir les signaux avec des modems, puisque le signal reste numérique (dans l'ordinateur et sur le support de communication) ; pourtant, les transmissions numériques requièrent du matériel spécialisé.

Le réseau est connecté à un pont ou un routeur, lequel est branché sur un CSU/DSU (Channel Service Unit / Data Service Unit), qui est lui-même relié à un répéteur, auquel est raccordée la ligne numérique. Le même dispositif se retrouve de l'autre coté de la liaison. Le CSU/DSU convertit le signal numérique de l'ordinateur en un signal numérique bipolaire appartenant à l'univers des communications synchrones.

```
RESEAU + PONT + CSU/DSU + REPETEUR + LIGNE + REPETEUR + CSU/DSU + PONT + RESEAU
```

Les lignes numériques proposent des communications synchrones point à point. Les circuits "point à point" sont des circuits dédiés qui offrent une liaison permanente avec la garantie d'une bande passante bidirectionnel simultanée (Full Duplex).

Il existe plusieurs modes de transmission pour les lignes numériques :

- La commutation de paquets
- Le Frame Relay (ou Relais de trames)
- Les Réseaux Privés Virtuels (VPN) qui utilisent le réseau Internet. Il est virtuel parce qu'il n'utilise pas de ligne spécialisée mais les supports de données d'Internet. Il est Privé parce que les données sont cryptées en utilisant un protocole de « tunneling ». Les VPN sont souvent basés sur des lignes numériques RNIS, mais ils peuvent également emprunter le réseau téléphonique analogique.

XIV-2-6 - Les lignes analogiques

Les lignes analogiques du réseau téléphonique commuté (le RTC) permettent de communiquer à distance. Les lignes RTC ont l'avantage d'exister partout ou presque dans le monde, mais elles n'offrent pas la même qualité de service que les lignes numériques. Les communications distantes via une ligne analogique doivent passer par un modem pour transformer le signal digital des ordinateurs en une fréquence.

Les modems transmettent à des vitesses de 56 Kb/s et conviennent pour des liaisons de courte durée (avec un volume de données peu important comportant essentiellement du texte par exemple) et des liaisons peu fréquentes.

Les lignes DSL (Digital Subscriber Line) correspondent à une nouvelle technologie qui utilise les lignes analogiques (la paire torsadée en cuivre que l'on a tous chez soi), mais qui ne véhicule pas les données sous la forme de modulations de fréquences. L'inconvénient d'une ligne DSL est qu'elle est limitée à une longueur maximale de 6 kilomètres, c'est à dire que la distance entre la prise de téléphone et le central téléphonique ne doit pas excéder 6 kilomètres.

Il existe plusieurs technologies DSL :

- L'ADSL (Asymetric Digital Subscriber Line) convient pour l'accès à Internet parce que le flot de données entrantes (download) est plus rapide que le flot sortant (upload).
- L'HDSL (High-speed Digital Subscriber Line) transmet les données de façon symétrique (les vitesses sont les même dans les deux sens) mais sur une distance de 5 Kilomètres seulement. Les débits de l'HDSL sont voisins de ceux d'une ligne T1 (1,544 Mb/s).
- Le RADSL (Rate Adaptive Digital Subscriber Line) peut adapter la vitesse de transfert en fonction du support physique, mais reste limité à une distance maximale de 6 Kilomètres.
- Le VDSL (Very high bit-rate Digital Subscriber Line) ne dépassent 3 kilomètres pour une vitesse comparable à celle des LAN (10 Mb/s).

XIV-2-7 - Les lignes numériques

Les lignes numériques sont souvent appelées des lignes dédiées ou des lignes spécialisées. Elles sont obtenues auprès d'un opérateur téléphonique, et constituent généralement une liaison « point à point », c'est à dire un circuit

réservé pour l'entreprise.

Il existe plusieurs types de lignes numériques :

XIV-2-8 - Le mode de transmission par commutation de paquets

Le mode de transmission par commutation de paquets est utilisé pour transmettre des données sur de très longues distances. La commutation de paquets est fiable, rapide et commode.

Les réseaux à commutation de paquets (Packets-switching Networks) permettent de transférer des données en utilisant plusieurs chemins possibles (il n'y a pas de circuits dédiés). Les données sont fractionnées en petits paquets et chaque paquet est orienté sur la route optimale à un moment donné. Chaque paquet est commuté séparément. Les paquets qui arrivent à destination dans le désordre sont reconstitués. Le désassemblage et l'assemblage des paquets exigent un certain niveau d'intelligence.

Les réseaux à commutation de paquets sont constitués d'un maillage de plusieurs « échangeurs » qui lisent les paquets et les commutent. Afin d'optimiser le temps des « commutateurs » et de réduire la quantité des données retransmises (en cas d'erreur), la taille des paquets est limitée. Les réseaux à commutation de paquets sont appelés des « connexions any-to-any ».

De nombreux réseaux à commutation de paquets utilisent des circuits virtuels (Virtual Circuits). Les circuits virtuels sont composés d'une série de connexions logiques (il ne s'agit pas d'une liaison physique dédiée entre les deux stations mais d'une bande passante allouée à la demande). Les réseaux virtuels à commutation de paquets sont appelés des « connexions point-to-many-point » :

- Les Circuits Virtuels Commutés (CVC ou SVC pour Switched Virtual Circuits) utilisent les ressources d'un réseau commuté pour établir une liaison dédiée, avec un seul chemin.
- Les Circuits Virtuels Permanents (CVP ou PVC pour Permanent Virtual Circuits) utilisent les ressources d'un réseau commuté pour établir une liaison dédiée et permanente qui ressemble à une ligne louée sauf que le client ne paye que la durée d'utilisation.

XIV-3 - Les technologies des réseaux étendus

Les réseaux étendus se présentent concrètement sous des dénominations qui englobent toutes les technologies qui permettent de réaliser une communication distante :

- Relais de trames
- X.25
- ATM
- RNIS
- FDDI
- SONET
- SMDS

Les dispositifs de connectivité de chacune de ces technologie différent les uns des autres. Par exemple, un modem RNIS d'une ligne numérique « à la demande » n'est pas le même équipement qu'un commutateur CSU/DSU d'une ligne numérique « dédiée ».

XIV-3-1 - Les caractéristiques des réseaux étendus Relais de trames

Les caractéristiques des réseaux étendus Relais de trames (Frame Relay) :

- Un réseau numérique à commutation de paquets sur de la fibre optique (fiable, rapide, sécurisé, et qui peut garantir une bande passante...) qui dérive des réseaux X.25 en France.
- Des fonctionnalités de contrôle des erreurs moins strictes que le X.25
- Des Circuits Virtuels Permanents (PVC) pour des « connexions point à point »
- Des trames de longueur variable
- Des commutateurs de données (Data Switch)
- Des ponts et des routeurs compatibles

Les réseaux étendus fonctionnant en Relais de Trames sont moins efficaces que les réseaux étendus fonctionnant sur des lignes numériques spécialisées. Il existe deux raisons qui expliquent ce phénomène :

- La vitesse de validation des information (le CIR pour Committed Information Rate) qui mesure la vitesse la moins bonne possible, c'est à dire la vitesse garantie. Le CIR est en général égal à la moitié de la bande passante annoncée.
- Le routeur chargé de transmettre les données doit empaqueter (ou encapsuler) les paquets du réseau local en un autre format, la « trame » qui est véhiculée sur le réseau étendu. Empaqueter les paquets et les dépaqueter prend du temps, ce qui affecte les performance des réseaux étendus en Relais de Trame.

L'alternative à cette inefficacité consiste à utiliser une « signalisation en bande de base » (CCS pour Clear Channel Signaling ou Common Channel Signaling). Avec le CCS, les données de signalisation utilisent un autre canal que les données proprement dites, et l'opérateur téléphonique n'a plus besoin d'empaqueter les données.

XIV-3-2 - Les caractéristiques des réseaux étendus X.25

Le réseau X.25 est le réseau à Relais de Trames en France. Le protocole X.25 permet à des réseaux différents de pouvoir communiquer par l'intermédiaire de passerelles.

Les caractéristiques des réseaux étendus X.25 :

- Un réseau analogique à commutation de paquets. Le maillage est représenté sous la forme de nuages.
- Des fonctionnalités de contrôle des erreurs très élaborées mais qui consomment de la bande passante.
- Une suite de protocoles X.25 qui définit l'interface entre les hôtes et les lignes louées (interface ETTD/ETCD) :
- Un hôte disposant d'une interface X.25
- Un PAD (Packet Assembler Disassembler)
- Une passerelle X.25
- Des noeuds de commutation

XIV-3-3 - Les caractéristiques des réseaux étendus ATM

Les caractéristiques des réseaux étendus ATM (Asynchronous Transfert Mode) :

- Des réseaux analogiques (Large de Bande) ou numérique (Bande de Base) à commutation de paquets.
- Les réseaux ATM ont été définies en 1988 par le CCITT dans le cadre d'un réseau BISDN (Broadcast Integrated Services Digital Network) ou d'un réseau RNIS à large bande passante.
- Une technologie puissante et polyvalente (véhicule la voix et les données) pour des vitesses très élevées (de 155 Mb/s à 622 Mb/s)

- Des trames (cellules) de longueur fixe (53 Octets dont 5 Octets pour l'entête ATM). La taille uniforme des cellules optimise l'utilisation des tampons des commutateurs et la planification de la bande passante.
- La panoplie des identificateurs qui accompagne les cellules permet, par exemple, d'instaurer une « qualité de service » (QOS pour Quality Of Service qui sera intégré à la nouvelle version de TCP/IP, Ipv6), c'est à dire d'appliquer une priorité à certains paquets. Ainsi, les courriers électroniques pourront avoir une priorité inférieure à celle des données en temps réel comme la vidéo.
- Une vitesse théorique de 1, 2 Giga Bytes par seconde (Gb/s)
- Des équipements ATM spécifiques, dont des commutateurs ATM
- Tous les supports de communication en cuivre, mais la fibre optique est plus appropriée...
- Utilisé pour les dorsales longue distance des opérateurs téléphoniques.
- Les sociétés FORE SYSTEMS et IBM ont beaucoup investi dans la technologie ATM...

XIV-3-4 - Les caractéristiques des réseaux étendus RNIS

Les réseaux étendus RNIS (Réseau Numérique à Intégration de Services) sont l'équivalent des réseaux ISDN (Integrated Services digital Network) aux Etats-Unis.

L'ISDN est apparue aux Etats-Unis dans les années 1980 et n'a pas rencontré un très grand succès auprès des petites entreprises qui voulaient s'équiper d'une ligne numérique commutée bon marché, parce qu'il était difficile de configurer le SPID (Service Provider ID) des terminaux ISDN.

Les caractéristiques des réseaux étendus RNIS :

- Un réseau numérique à commutation de paquet. Le réseau RNIS est la version numérique du réseau RTC.
- Un réseau RNIS (2B+D) à accès de base (Basic Access ISDN) permet de diviser la bande passante en trois canaux :
- Deux canaux à 64 Kb/s appelés canaux B qui peuvent être utilisés simultanément pour assurer un débit de 128 Kb/s.
- Un canal à 16 Kb/s appelé canal D pour la gestion des données et de la ligne
- Un réseau RNIS à accès primaire (Primary Access RNIS) utilise toute la bande passante d'une liaison T1 qu'elle peut diviser en 23 canaux B à 64 Kb/s et un canal D à 16 Kb/s.
- RNIS est une solution peu chère et adaptée pour les petites entreprises.
- Les adaptateurs de terminaux IDSN sont reliés à l'ordinateur par l'intermédiaire d'un câble croisé (qui évite l'utilisation d'un concentrateur entre la carte réseau et l'adaptateur de terminal IDSN) qui se connecte au connecteur réseau (BNC, RJ 45, AUI,...) de la carte réseau Ethernet de l'ordinateur. C'est l'adaptateur de terminal IDSN qui compose le numéro de téléphone du réseau ISDN quand il reçoit des paquets de la part de l'ordinateur. Les adaptateurs de terminal IDSN conviennent pour le travail à domicile.
- Le modem RNIS est souvent un modem Bande de Base branché au port série d'un ordinateur. Les modem RNIS utilisent le protocole PPP pour établir la connexion.
- L'établissement d'une connexion RNIS est un processus de 2 ou 3 secondes.

XIV-3-4 - Les caractéristiques des réseaux étendus FDDI

Les caractéristiques des réseaux étendus FDDI (Fiber Distributed Data Interface) :

- Un réseau en fibre optique définie en 1986 par le comité ANSI X3T9.5 afin d'accroître les débits des architectures Token Ring.
- Un réseau à grande vitesse (100 Mb/s)
- Une topologie à anneau double qui permet à plusieurs stations d'émettre en même temps (réseau partagé). L'anneau primaire qui tombe en panne est remplacé immédiatement par l'anneau secondaire. Les ordinateurs

connectés aux deux anneaux s'appellent des stations de classe A, et ceux qui ne sont connectés qu'à un seul anneau, des stations de classe B. Les anneaux peuvent être disposées dans une topologie en anneau en étoile.
- Un système de détection et de localisation des défaillances (Beaconing) avec un jeton spécial appelé le BEACON (une balise).
- Un support limité à 100 Km qui peut accueillir 500 stations, avec des répéteurs tous les 2 Km.
- Un environnement haut de gamme comme les réseaux scientifiques ou CAO, FAO qui requièrent une très large bande passante.
- Un réseau fédérateur (Backbone) permettant de réunir plusieurs autres réseaux.
- Les réseaux FDDI peuvent être mis en oeuvre sur des câbles en cuivre, c'est alors du CDDI (Copper Distributed Data Interface).
- Lorsqu'un serveur est connecté à deux anneaux par l'intermédiaire de deux concentrateurs MAU (Multistation Access Unit), on parle d'un système « biconnecté » (Dual Homed).

XIV-3-5 - Les caractéristiques des réseaux étendus SONET

Les caractéristiques des réseaux étendus SONET (Synchronous Optical Network) :

- Un réseau en fibre optique défini par l'association ESCA (Exchange Carriers Standards Association) pour l'ANSI.

XIV-3-6 - Les caractéristiques des réseaux étendus SMDS

Les caractéristiques des réseaux étendus SMDS (Switched Multimegabit Data Service) :

- Un réseau de commutation de paquets compatible avec la norme IEEE 802.6 pour les réseau MAN et RNIS à large bande (avec en plus un service de facturation et d'administration).
- Une transmission sans contrôle d'erreurs ni contrôle de flux.
- Un débit de 1 à 34 Mb/s.
- Une connectivité de type « many-to-many ».
- Une méthode d'accès au réseau DQDB (Distributed Queue Dual Bus).
- Une topologie à bus double qui forme un anneau ouvert.
- Les relais de cellules fixes d'ATM

XV - Les réseaux hétérogènes

Les réseaux hétérogènes sont des réseaux multi fournisseurs, c'est à dire que les composants matériels ou logiciels proviennent de fournisseurs différents. Le défi des environnements réseaux hétérogènes est l'interopérabilité...

De nos jours, la majorité des réseaux sont des réseaux hétérogènes :

- La technologie a évolué
- Les fournisseurs recherchent la plus grande compatibilité de leurs produits
- Les administrateurs réseaux sont devenus « multi compétents » pour mettre en oeuvre une telle complexité
- Les réseaux se construisent petit à petit, par petits bouts
- Les utilisateurs ont leurs préférences (le MAC pour les graphistes, UNIX pour les adeptes de la ligne de commande, les PC pour la part de marché, ...), certains ordinateurs « avaient » un avantage comparé sur d'autres

XV-1 - Les environnements réseaux hétérogènes

L'hétérogénéité des réseaux provient de la cohabitation plus ou moins heureuse de plusieurs fournisseurs, de plusieurs normes :

- Les éditeurs de système d'exploitation réseau
- Les constructeurs de machines
- Les fondeurs de processeurs
- Les normes de protocoles réseaux
- Les matériels, les câbles, les topologies, les méthodes d'accès...

La plupart des réseaux hétérogènes combinent les processeurs, les machines, les systèmes d'exploitation réseaux, les protocoles réseaux

Les réseaux hétérogènes				
Les processeurs	CISC			RISC
Les machines	Les PC IBM compatibles			Macintosh
Éditeurs	Microsoft	Novell	30 ans de travail	Apple
Les systèmes d'exploitation	MS-DOS, Windows 95, Windows NT	Netware	Unix, BSD, Linux	Mac OS
Les protocoles réseaux	TCP/IP, NWLink, NetBEUI	SPX/IPX	TCP/IP	AppleTalk

XV-2 - Les conditions de fonctionnement d'un réseau hétérogène

Pour qu'un réseau hétérogène fonctionne, il faut réunir plusieurs conditions :

- Les machines parlent le même langage, le même protocole réseau est installé sur toutes les machines qui communiquent entre elles. La communication doit être assurer par un protocole réseau commun.
- Les machines comprennent le langage des autres machines :
- Les postes clients sont équipés des redirecteurs adéquats pour s'adresser aux serveurs d'un autre système d'exploitation
- Les postes serveur sont équipés des services adéquats pour recevoir les requêtes des clients d'un autre système d'exploitation

- Les postes serveur sont équipés des passerelles adéquates pour accepter les requêtes des clients d'un autre système d'exploitation vers un serveur d'un autre système d'exploitation

Les redirecteurs sont appelés des requêteurs dans un réseau Netware, et des interpréteurs de commandes (ou SHELL) chez les clients MS-DOS.

XV-3 - La solution WINDOWS NT pour les réseaux hétérogènes

Le système d'exploitation réseau WINDOWS NT propose une palette complète d'outils pour assurer l'interopérabilité de son système dans un environnement multi fournisseurs, et pour s'assurer la croissance de ses parts de marché...

L'interopérabilité est assurée au niveau du client ou de celui du serveur.

WINDOWS NT permet aux clients NT de s'adresser à des serveurs NT. WINDOWS NT permet aux clients NT de s'adresser à un serveur Netware et aux clients Netware de s'adresser à un serveur NT (concurrence oblige...), enfin WINDOWS NT permet aux clients Apple de s'adresser à un serveur NT :

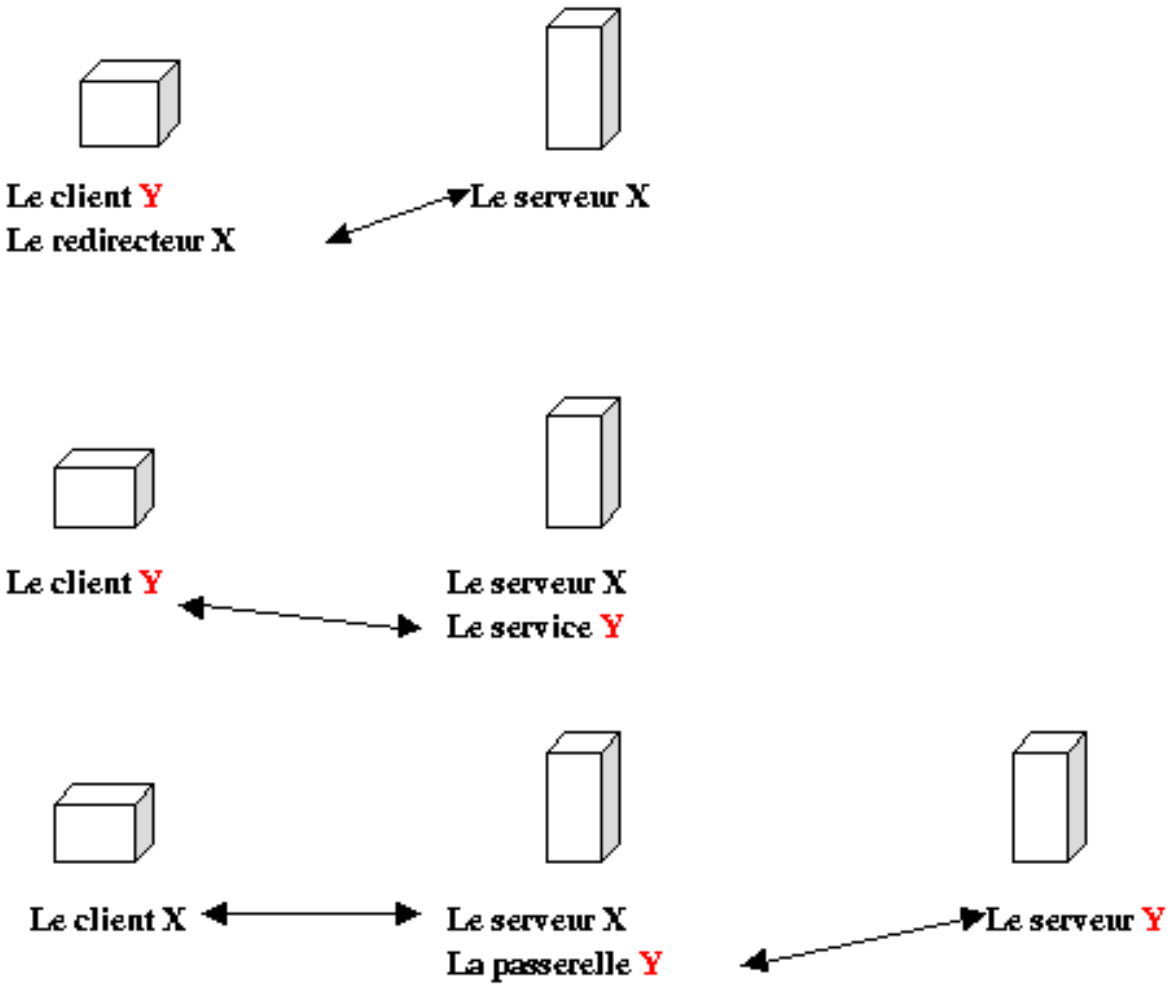
- Avec un redirecteur (CSNW) installé sur chaque client NT
- Par l'intermédiaire d'une passerelle (GSNW) installée sur un serveur NT
- Grâce à un service (service pour Macintosh) installé sur le serveur NT

La solution WINDOWS NT pour les réseaux hétérogènes		
Système d'exploitation	Client NT	Serveur NT
Netware de Novell	CSNW, NDS	Passerelle GSNW
Mac OS d'Apple		Service pour Macintosh

Le redirecteur Microsoft est installé sur tous ses systèmes d'exploitation réseaux (WINDOWS for WORKGROUP, WINDOWS 95 et 98, WINDOWS NT). Le redirecteur permet aux clients WINDOWS, non seulement d'accéder aux ressources d'un réseau WINDOWS, mais aussi de partager ses propres ressources sur un réseau WINDOWS (mais il faut installer le redirecteur).

Novell propose également une certaine compatibilité, avec des requêteurs pour certains systèmes d'exploitation (MS-DOS, WINDOWS NT, OS/2).

Le redirecteur d'Apple est intégré au système d'exploitation Apple. Les ordinateurs Macintosh sont directement équipés pour se connecter à un réseau AppleTalk, ils sont tout de suite en mesure de partager des fichiers, d'accéder à un serveur d'impression,...



XV-4 - Le dépannage des réseaux hétérogènes

Le dépannage des réseaux hétérogènes consiste la plupart du temps à vérifier la concordance des matériels et des logiciels avec les systèmes d'exploitation. Les problèmes peuvent provenir des matériels, des logiciels, des réseaux ou des utilisateurs :

XVI - Les protocoles réseaux

XVI-1 - Les protocoles de communication

Un protocole réseau est un ensemble de règles et de procédures de communication utilisées de part et d'autre par toutes les stations qui échangent des données sur le réseau.

Il existe de nombreux protocoles réseaux (NETWORK PROTOCOLS), mais ils n'ont pas tous, ni le même rôle, ni la même façon de procéder. Certains protocoles réseaux fonctionnent au niveau de plusieurs couches du modèle OSI, d'autres peuvent être spécialisés dans la réalisation d'une tâche correspondant à une seule couche du modèle OSI. Un paquet transmis sur le réseau est constitué de plusieurs couches d'informations correspondant aux différents traitement de chacun des protocole de la pile.

Différentes piles de protocoles peuvent coexister sur une même station, selon les besoins de communication vers des environnements différents. Les piles sont alors ordonnées entres elles afin que le processus de transmission essaye d'abord l'une puis l'autre.

Un réseau qui comporte plusieurs segments doit en général utiliser un protocole routable.

XVI-2 - Le modèle OSI et la pile de protocoles

Une pile de protocoles est une combinaison de plusieurs protocoles. Plusieurs protocoles peuvent collaborer ou coopérer au sein d'une suite ou d'une « pile de protocoles » (PROTOCOL STACK). Dans une pile de protocole, les différents protocoles sont organisés, ordonnés, hiérarchisés, les uns à la suite des autres, afin d'accomplir un ensemble de tâches correspondant à tout ou partie du modèle OSI. Le fonctionnement des différents protocoles de la pile doit être coordonné afin de prévenir les conflits et les opérations inachevées.

L'architecture en couche du modèle OSI se retrouve dans la pile de protocoles et assure la coordination de chacune des opérations du processus de transmission des données. En général, on parle de pile de protocole pour désigner l'ensemble du processus de transmission des données sur le réseau, et donc l'ensemble des couches du modèle OSI. Toutefois, le seul empilement de deux protocoles peut être également désigné par le terme de pile de protocoles.

Selon le modèle OSI, le processus de transmission des données sur un réseau est décomposé en plusieurs étapes, dans un ordre bien déterminé. Le modèle OSI distingue 7 étapes fondamentales, et décompose le processus de transmission des données en 7 couches. Chaque couche a une fonction bien précise dans le processus de transmission des données. A chacune de ces couches correspond la réalisation d'une ou de plusieurs tâches, et plusieurs cas de figure sont envisageables :

- Une tâche est réalisée par un seul protocole.
- Toutes les tâches d'une couche OSI sont réalisées par un seul protocole.
- Plusieurs tâches appartenant à différentes couches OSI sont réalisées par un seul protocole.
- Toutes les tâches de plusieurs couches OSI sont réalisées par un seul protocole.

Ainsi, les spécifications du modèle OSI sont respectées, mais la délimitation de chaque couche ne l'est pas forcément. Dans le processus de transmission, les données « traversent » la pile de protocoles, mais le nombre de protocoles constituant la pile n'est pas obligatoirement égale au nombre de couches du modèle OSI. La théorie ne correspond pas exactement à la réalité... Les couches du modèle OSI correspondent plus ou moins aux couches d'une pile de protocoles.

Les couches basses spécifient la manière dont les matériels sont connectés, tandis que les couches hautes énoncent les règles de communication. Les opérations des couches hautes sont plus complexes que celles des couches basses.

Le modèle OSI	
Les couches	Les fonctions
APPLICATION	Initie ou accepte une requête réseau
PRESENTATION	Ajoute des informations de formatage, d'affichage, de cryptage
SESSION	Ajoute des informations de flux pour indiquer le départ d'un paquet
TRANSPORT	Ajoute des informations pour le traitement des erreurs des paquets
RESEAU	Ajoute un numéro d'ordre et des informations d'adressage au paquet
LIAISON	Ajoute des informations de contrôle d'erreurs d'un paquet (CRC)
PHYSIQUE	Émet les paquets sur le réseau sous la forme d'un flot de bits bruts

XVI-3 - Les liaisons de protocoles

Dans une pile de protocoles, il y a au moins un protocole correspondant à chacune des couches du modèle OSI. Dans un tel cas, le processus de transmission des données est unique et traverse successivement tous les protocoles de la pile jusqu'à l'émission des trames sur le réseau. Il n'y a pas de liaison parce qu'il n'y a pas de choix à faire entre plusieurs protocoles de la même couche (en fait, les liaisons sont évidentes et sous-entendues, mais on dit qu'il n'y a pas de liaison parce qu'il n'y a pas de bifurcations).

Le plus souvent, la pile de protocole est constituée, pour chacune des couches du modèle OSI, de plusieurs protocoles différents. Une pile qui comporte à chaque niveau plusieurs protocoles est capable de communiquer dans plusieurs environnements (ce sont les avantages de l'ouverture, de la compatibilité et de la diversité). Le processus de transmission des données doit obligatoirement passer par l'un des protocoles de chaque couche (sinon la fonction de la couche correspondante ne serait pas réalisée), mais selon les besoins, il peut passer par n'importe lesquels d'entre eux. Le processus de transmission des données est guidé par des liaisons (BINDINGS) qui indiquent à chaque niveau le protocole à choisir et le protocole suivant. Les liaisons des protocoles de la pile indiquent les différents chemins possibles pour le processus de transmission des données. Chacun des chemins peut être (par un raccourci conceptuel et linguistique) considéré et appelé une pile.

Quand il existe plusieurs protocoles pour une même couche, il existe en général des liaisons en amont et en aval. Chacun des protocoles d'un même niveau est relié à l'un des protocoles précédents par une liaison, et à l'un des protocoles suivant par une autre liaison. Le processus de transmission des données doit faire un choix à chaque niveau où il y a une liaison.

Les liaisons sont hiérarchisées entre elles par un ordre de priorité. L'ordre des liaisons de la pile de protocole détermine l'ordre dans lequel le système d'exploitation réseau exécute les protocoles. Ainsi, selon le type de données à transmettre, le type de correspondant, ou le type de réseau, l'un ou l'autre des protocoles sera sélectionné ; par défaut, le protocole le plus prioritaire sera exécuté en premier, s'il n'aboutit pas, le protocole suivant sera exécuté, et ainsi de suite... Par exemple, dans un ordinateur NT, plusieurs protocoles de connexion ou d'acheminement des paquets (par exemple TCP/IP et NWLink) peuvent cohabiter à l'intérieur d'une même pile de protocole. Le protocole prioritaire de la pile (par exemple TCP/IP) sera d'abord utilisé pour établir la connexion avec l'ordinateur auquel les données doivent être transmises, si la connexion ne peut s'établir, alors le deuxième protocole (par exemple NWLink) effectuera à son tour une tentative de connexion...

En général, les liaisons de protocoles sont créées pendant l'installation du système d'exploitation réseau ou pendant l'installation des protocoles.

XVI-4 - Les avantages des liaisons de protocoles

L'utilisation de plusieurs protocoles procure des avantages :

- La communication dans des environnements hétérogènes :
- La réunion d'ordinateurs différents sur le même réseau
- La coopération de systèmes d'exploitation différents sur le même réseau
- La jonction de réseaux utilisant des protocoles différents :
- L'utilisation conjointe d'un protocole routable et d'un protocole non routable

Les liaisons de protocoles permettent de combiner plusieurs protocoles réseaux sur un même ordinateur. Les liaisons de protocoles sont très utiles dans un réseau hétérogène parce qu'elles permettent de faire communiquer des ordinateurs qui fonctionnent sur différents systèmes d'exploitation (par exemple MICROSOFT et NOVELL) et des réseaux qui fonctionnent avec différents protocoles (par exemple TCP/IP et SPX/IPX). Plusieurs protocoles (par exemple TCP/IP et SPX/IPX) peuvent être « liés » à la même carte réseau, et le processus de transmission des données utilise soit l'un, soit l'autre.

Les liaisons de protocoles permettent de combiner plusieurs cartes réseaux. Plusieurs cartes réseaux peuvent être installées sur le même ordinateur, et à chacune peut correspondre une pile de protocoles différents.

XVI-5 - Les piles standards

Certaines piles de protocoles sont reconnues par l'industrie informatique comme des standards ; ce sont soit des protocoles propriétaires, soit des protocoles issus d'organismes de normalisation (la plupart du temps ces organismes sont américains) qui ont initié une réflexion volontaire et concertée :

- Le modèle OSI
- L'architecture SNA (Systems Network Architecture) de la société IBM
- L'architecture DECnet de la société DIGITAL EQUIPMENT COMPUTER pour mettre en oeuvre l'architecture DNA (Digital Network Architecture) dans le cadre des réseaux locaux ETHERNET ou des réseaux étendus MAN. La version actuelle s'appelle DECnet phase V.
- L'architecture NetWare de la société NOVELL
- L'architecture AppleTalk de la société APPLE COMPUTER
- La pile Internet TCP/IP

Les organismes de normalisation comme l'ISO, l'IEEE, l'ANSI (American National Standard Organisation), le

CCITT devenue le l'ITU (International Telecommunication Union) et bien d'autres ont développé des protocoles correspondant aux spécifications du modèle OSI (avec ses 7 couches) et du modèle IEEE 802 (avec les deux sous-couches LLC et MAC).

Tableau comparatif des piles de protocoles										
Le modèle OSI	Windows NT				La pile internet					
APPLICATION	Redirecteurs		Serveurs		NFS XDR	SNMP	FTP	Telnet	SMTP	
PRESENTATION	TDI									
SESSION	TCP/IP	NWLink	NBT	DLC	TCP					
TRANSPORT	NDIS 4.0				IP					
RESEAU	Wrapper NDIS dont les pilotes des cartes réseaux NDIS				Pilotes LAN					
LIAISON					La sous-couche MAC					
PHYSIQUE	La couche Physique				La couche Physique					

Tableau comparatif des piles de protocoles							
Le modèle OSI	NetWare		APPLE				
APPLICATION	NCP		AppleShare				
PRESENTATION			NCP				
SESSION	Tubes nommés	NetBIOS	ASP	ADSP	ZIP	PAP	
TRANSPORT	SPX		ATP	NBP	AEP	RTMP	
	IPX		DDP				
RESEAU	Pilotes LAN		Pilotes LAN				
LIAISON	ODI	NDIS	Local Talk		TokenRing	EtherTalk	
PHYSIQUE	La couche physique		La couche physique				

XVI-6 - Les protocoles en trois catégories

Les protocoles peuvent être classés par simplification en trois catégories et non plus en sept couches comme le recommande le modèle OSI. En effet, dans la réalité, les protocoles ne suivent pas strictement les frontières établies par l'organisme de normalisation ISO. Le modèle OSI est réduit à trois couches.

Le tableau de substitution des sept couches en trois catégories	
Les sept couches du modèle OSI	**Les trois catégories de protocoles**
APPLICATION	APPLICATION
PRESENTATION	
SESSION	
TRANSPORT	TRANSPORT
RESEAU	RESEAU
LIAISON	
PHYSIQUE	

XVI-7 - Les protocoles de la catégorie APPLICATION

Les protocoles de la catégorie APPLICATION garantissent l'interaction et l'échange des données :

- APPC (Advanced Program to Program Communication) est le protocole SNA poste à poste d'IBM essentiellement utilisé sur les ordinateurs AS/400.
- FTAM (File Transfer Access and Management) est un protocole OSI d'accès aux fichiers.
- X.400 est un protocole CCITT (Comité Consultatif International de Télégraphie et de Téléphonie) permettant la transmission internationale de messagerie électronique.
- X.500 est un protocole CCITT offrant des services de fichiers et de répertoires répartis sur plusieurs systèmes.
- SMTP (Simple Mail Transfer Protocol) est un protocole Internet pour le transfert de messagerie électronique.
- FTP (File Transfer Protocol) est un protocole Internet pour le transfert de fichiers.
- SNMP (Simple Network Management Protocol) est un protocole Internet permettant la surveillance des réseaux et de leurs composants.
- TELNET est un protocole Internet pour la connexion à des hôtes distants et le traitement local de données.
- SMB (Server Message Blocks) est le redirecteur client (shell) de MICROSOFT.
- NCP (Novell Netware Core Protocol) est le redirecteur client (shell) de NOVELL.
- APPLETALK et APPLESHARE est la suite de protocole d'APPLE.
- AFP (AppleTalk Filing Protocol) est un protocole APPLE (pour les ordinateurs MACINTOSH) destiné à l'accès distant à des fichiers.
- DAP (Data Access Protocol) est un protocole DECnet pour l'accès aux fichiers.

XVI-8 - Les protocoles de la catégorie TRANSPORT

Les protocoles de la catégorie TRANSPORT assurent les connexions et le contrôle des transferts de données :

- TCP (Transmission Control Protocol) est une partie du protocole Internet TCP/IP qui garantit la remise des données en séquence.
- SPX (Sequential Paquet Exchange) est une partie du protocole SPX/IPX de NOVELL qui garantit la remise des données en séquence. C'est un protocole réduit, rapide et routable. SPX/IPX est un produit dérivé du protocole XNS (Xerox Network System) qui a été développé par la société XEROX pour les réseaux locaux ETHERNET. La pile XNS est un protocole qui a largement été diffusé dans les années 1980, mais qui a été progressivement remplacé par la pile TCP/IP. La pile XNS générait de nombreux messages de diffusion général (BROADCAST), ce qui le rendait lent en plus d'être volumineux.
- NWLink est la version MICROSOFT du protocole SPX/IPX de NOVELL.
- NetBEUI (NetBIOS Extended User Interface) est un protocole qui crée des sessions NetBIOS (Network Basic

Input Output System) et fournit des services de transport de données (NetBEUI). NetBEUI est basé sur le protocole de transfert SMB.
- ATP (AppleTalk Transaction Protocol) et NBP (Name Binding Protocol) sont des protocoles APPLE pour les ordinateurs MACINTOSH.
- X.25 est un ensemble de protocoles pour les réseaux à commutation de paquets utilisés pour connecter des terminaux distants à de gros systèmes hôtes (MAINFRAME).

XVI-9 - Les protocoles de la catégorie RESEAU

Les protocoles de la catégorie RESEAU fournissent les services de liaisons (adressage, routage, contrôle d'erreurs et requête de retransmission) et définissent les règles de communication des réseaux ETHERNET, TOKEN RING,... :

- IP (Internet Protocol) est la partie du protocole Internet TCP/IP qui achemine et route les paquets
- IPX (Internetworking Packet Exchange) est la partie du protocole SPX/IPX de NOVELL qui achemine et route les paquets
- NWLink est la version MICROSOFT du protocole SPX/IPX de NOVELL
- NetBEUI est le protocole qui fournit les services de transport aux applications et sessions NetBIOS
- DDP (Datagram Delivery Protocol) est un protocole APPLETALK pour le transport des données (pour les ordinateurs MACINTOSH)

XVI-10 - Les protocoles routables

Jusque vers le milieu des années 80, les réseaux locaux n'étaient constitués que d'un seul segment de câble, et pour la plupart étaient des réseaux isolés. L'évolution de la technologie et des besoins a conduit à une ouverture et un raccordement des réseaux. Les réseaux locaux devaient devenir des sous-ensembles de réseaux plus vastes, faisant partie intégrante d'un « réseau étendu ».

La complexité du maillage des réseaux s'est avec le temps de plus en plus accrue. Les chemins possibles pour qu'un paquet atteigne sa cible croissaient en fonction du nombre de noeuds du réseau. Il fallait non seulement garantir que le paquet arrive à destination, mais aussi qu'il le fasse dans un délai raisonnable. Certains protocoles permettent au paquet d'emprunter plusieurs chemins, on dit alors que ce sont des « protocoles routables ». Les protocoles routables permettent au paquet d'atteindre sa cible le plus rapidement possible :

- En utilisant le chemin le plus court
- En utilisant le chemin le moins encombré, en fonction du trafic du réseau

Les protocoles routables permettent aux paquets de « traverser » les routeurs.

XVI-11 - Le protocole SPX/IPX

Le protocole SPX/IPX a été développé au début des années 1980 par la société Novell parce que le protocole TCP/IP était encore très compliqué. Longtemps, les systèmes NetWare étaient incompatibles avec Internet qui utilise le protocole TCP/IP.

Avec la version « IntranetWare 4.11 », Novell permet aux utilisateurs de son système d'accéder à l'Internet. Toutefois, l'intégration de TCP/IP n'est pas « native », c'est une traduction de SPX/IPX en TCP/IP, ce qui prend un certain temps et ralentit quelque peu l'accès à Internet. En fait, SPX/IPX convient si les postes client n'ont pas

besoin d'une adresse IP en interne pour pouvoir y accéder depuis l'extérieur du réseau NetWare.

Le protocole SPX/IPX est auto configurable, c'est à dire que Netware construit automatiquement une adresse réseau sous la forme d'un nombre hexadécimal à partir d'une plage d'adresses choisies par l'administrateur et de l'adresse MAC de l'ordinateur. Ainsi, l'adresse réseau IPX est unique et disponible immédiatement sans l'intervention de l'administrateur.

XVI-12 - Le protocole TCP/IP

Le protocole TCP/IP (Transmission Control Protocol / Internet Protocol) est le plus connu des protocole parce que c'est celui qui est employé sur le réseau des réseaux, c'est à dire Internet. Historiquement, TCP/IP présentait deux inconvénients majeurs, sa taille et sa lenteur. Le protocole TCP/IP fait partie du système d'exploitation UNIX depuis le milieu des années 1970 (auparavant, c'est le protocole UUCP (UNIX to UNIX Copy Program) qui était employé pour copier des fichiers et des messages électroniques entre deux machines).

Le protocole TCP/IP est une norme ouverte, c'est à dire que les protocoles qui constituent la pile de protocoles TCP/IP ont été développés par des éditeurs différents sans concertation. Le groupe de travail IETF (Internet Engineering Task Force) a rassemblé les différents protocoles de la pile TCP/IP pour en faire une norme. Le travail de l'IETF est régulièrement soumis à l'ensemble de la « communauté Internet » dans des documents appelés RFC (Request For Comments). Les RFC sont considérées comme des brouillons parce que les spécifications qu'elles contiennent peuvent à tout moment être réexaminées et remplacées. L'IETF essaye de statuer en ce moment sur une norme (Internet Calendar, Simple Scheduling Transfert Protocol) concernant le transport des données des agendas et des plannings.

TCP/IP est une pile de protocoles relativement volumineuse, ce qui peut causer des problèmes avec un client comme MS-DOS. Toutefois, les systèmes d'exploitation réseaux avec une interface graphique comme WINDOWS 95 ou WINDOWS NT n'ont pas de contrainte de mémoire pour charger la pile TCP/IP. Quant à la vitesse d'exécution et de transmission des paquets, celle de TCP/IP équivaut à SPX/IPX.

Les protocoles de la pile TCP/IP	
Nom	Fonction
FTP	FTP (File Transfer Protocol) s'occupe des transferts de fichiers.
TELNET	TELNET permet d'établir une connexion à un hôte distant et de gérer les données locales.
TCP	TCP (Transmission Control Protocole) s'assure que les connexions entre deux ordinateurs sont établies et maintenues.
IP	IP (Internet Protocol) gère les adresses logiques des noeuds (stations,...).
ARP	ARP (Adress Resolution Control) fait correspondre les adresses logiques (IP) avec les adresses physiques (MAC).
RIP	RIP (Routing Information Protocol) trouve la route la plus rapide entre deux ordinateurs.
OSPF	OSPF (Open Shortest Path First) est une amélioration de RIP, plus rapide et plus fiable.
ICMP	ICMP (Internet Control Message Protocol) gère les erreurs et envoie des messages d'erreurs.

Les protocoles de la pile TCP/IP	
BGP/EGP	BGP/EGP (Border Gateway Protocol / Exterior Gateway Protocol) gère la transmission des données entre les réseaux.
SNMP	SNMP (Simple Network Management Protocol) permet aux administrateurs réseaux de gérer les équipements de leur réseau.
PPP	PPP (Point to Point Protocol) permet d'établir une connexion distante par téléphone. PPP (après SLIP) est utilisé par les fournisseurs d'accès à Internet.
SMTP	SMTP (Simple Mail Transport Protocol) permet d'envoyer des courriers électroniques.
POP 3 et IMAP 4	POP 3 (Post Office Protocol version 3) et IMAP 4 (Internet Message Advertising Protocol version 4) permettent de se connecter à un serveur de messagerie et de récupérer son courrier électronique.

Le protocole TCP/IP est devenu la référence à partir de laquelle sont évalués les autres protocoles. La pile de protocole TCP/IP est la plus riche fonctionnellement.

Le protocole IP dispose de fonctions standardisées, les « API sockets » qui se comportent de la même façon sur tous les types de matériels.

TCP/IP est très répandu et très fonctionnel, mais assez compliqué et assez volumineux. En fait, l'inconvénient majeur provient de son succès, et de la diminution du nombre des adresse IP disponibles (en attendant la version IPV6 appelé aussi IPNG).

XVI-13 - Les caractéristiques du protocole TCP/IP

- Une norme industrielle
- Relativement volumineux et relativement rapide
- Tous les réseaux reconnaissent TCP/IP :
- Une interopérabilité entre ordinateurs hétérogènes
- Un standard pour la communication inter-réseaux et particulièrement entre des réseaux hétérogènes
- Un protocole routable
- D'autres protocoles ont été développés spécialement pour TCP/IP :
- SMTP pour la messagerie électronique
- FTP pour l'échange de fichiers
- SNMP pour la surveillance des réseaux

XVI-14 - Le protocole NetBEUI

A l'origine les protocoles NetBIOS et NetBEUI constituaient une seule et même pile. Certains fournisseurs séparèrent le protocole de la couche SESSION (NetBIOS) afin de pouvoir l'utiliser avec des protocoles routables de la couche TRANSPORT (le protocole de transport NetBEUI n'est pas routable).

NetBIOS est une interface pour les réseaux locaux développée par IBM. NetBIOS est relativement populaire parce que de nombreuses applications ont été programmées pour fonctionner avec cette interface.

Le protocole NetBEUI est un protocole de la couche TRANSPORT, mais n'est pas routable. Le protocole NetBEUI convient pour les réseaux « mono segment », il est très rapide si le nombre d'utilisateurs n'est pas trop grand. Pour accéder à Internet, les paquets NetBEUI doivent être « encapsulés » dans une couche TCP/IP, c'est ce qui s'appelle NBT.

Le protocole NetBEUI utilise des noms alphanumériques (les noms NetBIOS, ou les noms d'ordinateur) pour reconnaître les différentes machines du réseau. Les paquets ne sont pas adressés avec des adresses numériques, les noms de machine ne sont pas traduit en numéros. Il est donc plus facile pour les utilisateurs de reconnaître les autres machines, et d'installer le protocole. Les noms NetBIOS doivent être résolus en adresses IP quand d'autres ordinateurs utilisent TCP/IP.

L'inconvénient du protocole NetBEUI est qu'il n'est pas routable, les communications sont toujours transmises en « broadcast », et les machines connectées au réseau doivent continuellement se faire connaître aux autres machines, ce qui utilise de la bande passante.

Le protocole NetBEUI convient pour les petits réseaux qui utilisent les produits de Microsoft.

XVI-15 - Les caractéristiques de NetBEUI

- Petit, rapide et efficace
- Tous les produits MICROSOFT en sont équipés, comme OS/2 Warp et LanStatic de la société Artisoft
- Existe depuis le milieu des années 1980
- A été fourni avec MS NET, le premier produit réseau de MICROSOFT
- Fonctionne très bien avec les clients MS-DOS
- Mais c'est protocole qui n'est pas routable, et qui reste donc limité à de petits réseaux sur un seul segment de câble...

XVI-16 - L'installation des protocoles

L'installation des protocoles s'effectue le plus souvent en même temps que l'installation du système d'exploitation réseau. Par exemple, WINDOWS NT installe TCP/IP et le considère comme le protocole par défaut du système. Le module RESEAU du PANNEAU de CONFIGURATION de WINDOWS NT SERVER permet d'installer ou de supprimer des protocoles, et permet de modifier l'ordre des liaisons entre les différents protocoles qui sont installés.

Un réseau découpé en plusieurs segments doit utiliser un protocole routable, si les stations d'un segment sont censées communiquer avec les stations d'un autre segment. Par contre, l'utilisation d'un protocole non routable garanti que les données du segment ne seront pas détournées vers un autre segment...

XVII - Les adresses IP

XVII-1 - L'espace d'adressage

L'espace d'adressage est défini en fonction du nombre de bits nécessaires pour exprimer une adresse IP. Plus le nombre de bits est important, et plus le nombre de possibilités est important.

Il existe deux espaces d'adressage pour les adresses IP :

- L'espace d'adressage de 32 bits qui correspond au système d'adresses IP actuelles (Ipv4).
- L'espace d'adressage de 128 bits qui correspond au prochain système d'adresses IP qui est en train d'être élaboré (Ipv6 pour IP version 6 ou IPNG pour IP New Generation).

XVII-2 - L'espace d'adressage 32 bits

L'espace d'adressage 32 bits est constitué de 4 octets de 8 bits chacun (4x8 = 32). Chaque octet est constitué de huit bits, et chaque bit peut prendre la valeur binaire 1 ou 0. Ainsi, la valeur décimale de chaque octet peut être comprise en 0 et 255 (256 possibilités = 2 à la puissance 8), et l'espace d'adressage est compris entre 1 et 4 294 967 296 (2 à la puissance 32 moins 1).

Les adresses IP sont généralement exprimées dans la « notation décimale pointée » (c'est à dire que chaque octet est séparé par un point).

L'espace d'adressage IP		
	IPV4	IPV6
Espace d'adressage	Une adresse sur 32 bits	Une adresse sur 128 bits
Structure de l'adresse	4 mots (x.x.x.x)	8 mots (x.x.x.x.x.x.x.x)
Notation	Décimale pointée	Hexadécimale pointée
Définition d'un mot	Un mot = 1 octet= 8 bits	Un mot = 4 hexadécimales = 16 bits
Dimension pour un mot	0 à 255 (en base 10)	0000 à FFFF (en base 16)
Possibilité par mot	2 puissance 8 = 256	16 puissance 4 = 65 536 2 puissance 16 = 65 536
Possibilité d'adresse	256 puissance 4 = 2^32 = 4 294 967 296	65 536 puissance 8 = 2^128 2^128 = un nombre très grand

XVII-3 - Le masque de sous réseau

Une adresse IP permet d'identifier une station sur le réseau Internet. Les stations présentent sur Internet possèdent au moins une adresse IP unique afin de pouvoir être reconnue par les autres stations.

Le réseau Internet est le réseau des réseaux, c'est à dire qu'il est constitué d'un ensemble de réseaux qui sont connectés entre eux, et à l'intérieur desquels se trouvent les stations qui ont accès à Internet. Afin de pouvoir contacter une autre station sur Internet, il faut connaître le réseau auquel elle appartient (c'est la partie réseau de l'adresse IP) et son identification personnelle à l'intérieur de ce réseau (c'est la partie station de l'adresse IP).

Une adresse IP est constituée de 4 octets, c'est à dire de 32 bits. Sur les 32 bits, une partie (plus ou moins grande) sera utilisée pour identifier le réseau et une autre partie (le complément) sera utilisée pour identifier la station à l'intérieur de ce réseau.

L'adresse IP est composée de deux parties :

- La partie réseau
- La partie station

Le masque de sous réseau permet de savoir qu'elle est la partie des 32 bits qui est utilisé pour identifier le réseau. Les bits du masque de sous-réseau sont à 1 pour indiquer « la partie réseau » et sont à 0 pour indiquer « la partie station ». Les bits de « la partie station » n'utilisent jamais les valeurs extrêmes, 0 et 255 pour ne pas être confondus avec « la partie réseau ».

Pour identifier une station sur le réseau Internet, il faut connaître deux adresse IP :

- Le masque de sous réseau
- L'adresse IP

Par exemple:

L'adresse IP : 198.64.32.1

Le masque de sous réseau : 255.255.0.0

La partie réseau : 198.64.0.0

La partie station : 0.0.32.1

L'adresse du réseau dans Internet est 198.64.0.0 et l'adresse de la première station à l'intérieur de ce réseau est 198.64.32.1.

C'est un organisme international, l'IEEE au Etats-Unis et l'INRIA en France qui se charge d'octroyer les adresses de réseau, afin d'en assurer l'unicité sur Internet. Les adresses internes des stations sont gérées par l'administrateur réseau.

XVII-4 - Le sous adressage

Le sous adressage consiste à utiliser une partie de « la partie station » pour l'incorporer à « la partie réseau » et ainsi agrandir celle-ci. Le nombre de sous-réseau sera plus important, mais le nombre de station par sous réseau le sera moins.

XVII-5 - Les classes d'adresse IP

La partie réseau de l'espace d'adressage 32 bits est divisé en classes.

- Les adresses de classe A
- Les adresses de classe B
- Les adresses de classe C
- Les adresses de classe D
- Les adresses de classe E

A chaque classe correspond un nombre maximum de réseaux pouvant appartenir à cette classe, et à chaque réseau d'une certaine classe, correspond un nombre maximum d'adresses, c'est à dire un nombre maximum de stations pouvant bénéficier d'une adresse fixe à l'intérieur de ce réseau.

Les classes des adresses IP					
	Classe A	Classe B	Classe C	Classe D	Classe E
Fonction	Multinationales	Grandes entreprises	Petites entreprises	Multicasting	Recherche expérimentale
Réseau	Sur 1 octet	Sur 2 octets	Sur 3 octets		
Station	Sur 3 octets	Sur 2 octets	Sur 1 octet		
Structure de la partie réseau	1.0.0.0 à 126.0.0.0	128.1.0.0 à 191.254.0.0	192.0.1.0 à 223.254.254.0		
Valeur du 1er octet en binaire	00000001 à 01111110	10000000 à 10111111	11000000 à 11011111		
Nombre de machines par réseau	16 millions	65 536	256		

XVII-6 - Les adresses IP conventionnelles

Certaine adresses sont réservées pour une utilisation conventionnelle :

- 0.0.0.0 est utilisée par les machines pendant la procédure de démarrage de l'ordinateur (le BOOT).
- 127.0.0.0 est utilisée pour tester une adresse IP.
- 192.168.0.0 n'existe pas sur internet, afin d'être réservée pour les réseaux locaux sous TCP/IP
- 255.255.255.255 est utilisée comme adresse de broadcast générale.

XVII-7 - Le routage inter domaine sans classe

Le routage inter domaine sans classe (Classeless Inter-Domain Routing ou CIDR) est une méthode permettant de contourner la limitation de l'allocation des adresses IP par classe, et de pallier la pénurie des adresses IP version 4 des classes B et C. Le CIDR est décrit dans la RFC 1519 (Request For Comment). Les entreprises disposant d'une classe B alors qu'elles n'ont qu'un petit nombre de stations « gaspillent » des adresses IP potentielles. Par ailleurs, le saut d'une classe à une autre est très important, à la fois en terme de coût et en terme de nombre d'adresse.

Le CIDR permet essentiellement de combiner deux adresses de réseaux de classe C pour ne former qu'un seul réseau.

Par exemple, une entreprise a besoin de 300 adresses IP pour son réseau. Cette entreprise choisit de ne pas

utiliser d'adresses de réseau de classe B (avec 65 536 adresses IP possibles), soit parce qu'elle ne peut se l'offrir, soit parce qu'il n'existe plus d'adresses de réseau de classe B disponibles. L'entreprise décide alors d'acheter deux adresses de réseau de classe C (avec 256 adresses IP pour chaque adresse de réseau, soit un total de 512, ce qui est largement suffisant).

Le CIDR permet de gérer plus efficacement un pool d'adresse IP, sans perte ni gaspillage. Le CIDR représente une couche de complexité supplémentaire pour les tables de routage. Avant d'acheter un routeur, il convient de déterminer si celui-ci doit posséder les fonctionnalités de CIDR.

En attendant la nouvelle version d'Ipv6 (avec un adressage sur 128 bits), le système CIDR prend une place de plus en plus importante dans les réseaux IP.

XVII-8 - L'adresse de broadcast d'un réseau local

L'adresse de broadcast d'un réseau local est l'adresse de diffusion générale à toutes les stations du réseau. L'adresse de broadcast est en général la dernière adresse du réseau.

L'adresse IP se compose de « la partie réseau » qui identifie le réseau, et de « la partie machine » qui identifie une station à l'intérieur de ce réseau. Par exemple, 192.155.87.0 pour la partie réseau, et 192.155.87.x avec x allant de 1 à 255 pour la partie machine. Ainsi, l'adresse de broadcast d'un tel réseau serait 192.155.87.255.

XVII-9 - Ipv6

Ipv6 (pour IP version 6 ou IPNG pour IP New Generation), sera fondée sur un espace d'adressage de 128 bits.

Ipv6 disposera de fonctionnalités natives d'authentification et de cryptage.

XVII-10 - Un exemple d'adressage réseau

Voici le schéma d'un petit réseau comprenant 4 sous réseaux locaux reliés par 3 routeurs, et avec une ouverture vers Internet.

L'organisme d'attribution des classes réseaux octroie les coordonnées de classe B suivantes :

- Le masque principal de réseau : 255.255.0.0
- L'adresse IP du réseau : 152.80.0.0 (ou la valeur x.y.0.0)

Les deux premiers octets (16 bits) du masque principal de réseau sont à 1. Pour constituer 4 sous réseaux à l'intérieur de celui-ci, il faut un masque de sous réseau qui comporte plus de bits à 1, mais pas trop car sinon, chaque sous réseau ne pourra disposer de suffisamment d'adresses pour les stations. Le choix du nombre de bits supplémentaires à 1 constituant le masque de sous réseau doit tenir compte des besoins futurs, de l'évolution du réseau, en terme de nombre de sous réseaux et de nombre de stations pour chacun des sous réseaux.

Il reste 2 octets (16 bits) pour constituer le masque de sous réseau. Si le réseau ne devait pas comporter de sous réseaux, il y aurait 2 à la puissance 16 = 65 536 stations ou adresses IP différentes sur ce réseau. Si le masque de

sous réseau avait tous les 64 bits à 1, il y aurait autant de sous réseaux que de stations, chaque station aurait son propre sous réseau, et chaque sous réseau n'aurait qu'une seule station. Mais combien y aurait-ils de sous réseaux ?

Un masque de sous réseau de 1 bit à 1 supplémentaires (10000000 = 128 en décimale) se présente ainsi : 255.255.128.0 mais n'offre que 2 sous réseaux (2 à la puissance 1 = 2) :

00000000 = 0 en décimal pour le 3ième octet :

Les adresses IP des stations de ce premier sous réseau ont des valeurs allant de x.y.0.1 jusqu'à x.y.127.255(en enlevant l'adresse réseau 152.80.0.0).

10000000 = 128 en décimale pour le 3ième octet :

Les adresses IP des stations de ce deuxième sous réseau ont des valeurs allant de x.y.128.0 jusqu'à x.y.255.255

Toutefois, chacun de ces sous réseaux peut contenir un très grand nombre de stations. Il reste en effet 15 bits pour identifier les stations de chaque sous réseau (2 à la puissance 15 = 32768 stations ou adresses IP différentes)

Un masque de sous réseau de 2 bits à 1 supplémentaires (11000000 = 192 en décimal) se présente ainsi : 255.255.192.0 mais n'offre que 4 sous réseaux. Le calcul est le suivant : 2 à la puissance {2 bits} = 4 sous réseaux :

00000000 = 0 en décimal pour le 3ième octet

Les adresses IP des stations de ce premier sous réseau ont des valeurs allant de x.y.0.1 jusqu'à x.y.63.255 (en enlevant la première adresse réseau x.y.0.0).

01000000 = 64 en décimal

Les adresses IP des stations de ce deuxième sous réseau ont des valeurs allant de x.y.64.0 jusqu'à x.y.127.255

10000000 = 128 en décimal

Les adresses IP des stations de ce troisième sous réseau ont des valeurs allant de x.y.128.0 jusqu'à x.y.191.255

11000000 = 192 en décimal

Les adresses IP des stations de ce quatrième sous réseau ont des valeurs allant de x.y.192.0 jusqu'à x.y.255.255

Chacun de ces sous réseaux peut contenir 2 à la puissance 14 = 16384 stations. Ainsi, ce masque de sous réseau (255.255.192.0) conviendrait pour constituer 4 sous réseaux , avec un pas de 64 entre chaque sous réseau. Mais ne serait-il pas prudent de pouvoir disposer de sous réseaux supplémentaires dans l'avenir ?

Un masque de sous réseau de 3 bits à 1 supplémentaire (11100000 = 224 en décimale) se présente ainsi : 255.255.224.0 et offre 8 sous réseaux (2 à la puissance 3 = 8 sous réseaux) :

00000000 = 0 en décimal pour le 3ième octet

Les adresses IP des stations de ce premier sous réseau ont des valeurs allant de x.y.0.1 jusqu'à x.y.31.255 (en enlevant la première adresse réseau x.y.0.0).

00100000 = 32 en décimal

Les adresses IP des stations de ce deuxième sous réseau ont des valeurs allant de x.y.32.0 jusqu'à x.y.63.255

01000000 = 64 en décimal

Les adresses IP des stations de ce troisième sous réseau ont des valeurs allant de x.y.64.0 jusqu'à x.y.95.255

01100000 = 96 en décimal

Les adresses IP des stations de ce quatrième sous réseau ont des valeurs allant de x.y.96.0 jusqu'à x.y.127.255

10000000 = 128 en décimal

Les adresses IP des stations de ce cinquième sous réseau ont des valeurs allant de x.y.128.0 jusqu'à x.y.159.255

10100000 = 160 en décimal

Les adresses IP des stations de ce sixième sous réseau ont des valeurs allant de x.y.160.0 jusqu'à x.y.191.255

11000000 = 192 en décimal

Les adresses IP des stations de ce septième sous réseau ont des valeurs allant de x.y.192.0 jusqu'à x.y.223.255

11100000 = 224 en décimal

Les adresses IP des stations de ce huitième sous réseau ont des valeurs allant de x.y.224.0 jusqu'à x.y.255.255

Chacun de ces sous réseaux peut contenir 2 à la puissance 13 = 8192 stations ou adresse IP différentes. Il y a un pas de 32 entre chaque sous réseau.

Un masque de sous réseau de 4 bits à 1 supplémentaire (11110000 = 240 en décimale) se présente ainsi : 255.255.240.0 et offre 16 sous réseaux (2 à la puissance 4 = 16 sous réseaux). Chacun de ces sous réseaux peut contenir 2 à la puissance 12 = 4096 stations ou adresse IP différentes. Il y a un pas de 16 entre chaque sous réseau.

00000000 = 0 en décimal

00010000 = 16 en décimal

00100000 = 32 en décimal

00110000 = 48 en décimal

01000000 = 64 en décimal

01010000 = 80 en décimal

01100000 = 96 en décimal

01110000 = 112 en décimal

10000000 = 128 en décimal

10010000 = 144 en décimal

10100000 = 160 en décimal

10110000 = 176 en décimal

11000000 = 192 en décimal

11010000 = 208 en décimal

11100000 = 224 en décimal

11110000 = 240 en décimal

Un masque de sous réseau de 5 bits à 1 supplémentaire (11111000 = 248 en décimale) se présente ainsi : 255.255.248.0 et offre 32 sous réseaux (2 à la puissance 5 = 32 sous réseaux). Chacun de ces sous réseaux peut contenir 2 à la puissance 11 = 2048 stations ou adresse IP différentes. Avec un pas de 8 entre chaque sous réseaux.

Un masque de sous réseau de 6 bits à 1 supplémentaire (11111100 = 252 en décimale) se présente ainsi : 255.255.252.0 et offre 64 sous réseaux (2 à la puissance 6 = 64 sous réseaux). Chacun de ces sous réseaux peut contenir 2 à la puissance 10 = 1024 stations ou adresse IP différentes. Avec un pas de 4 entre chaque sous réseaux.

Un masque de sous réseau de 8 bits à 1 supplémentaire reviendrait à utiliser le troisième octet pour différencier les sous réseaux. Le masque de sous réseau (11111111 = 255 en décimale) se présente ainsi : 255.255.255.0 et offre 256 sous réseaux (2 à la puissance 8 = 256 sous réseaux). Chacun de ces sous réseaux peut contenir 2 à la puissance 8 = 256 stations ou adresse IP différentes. Les adresses IP seraient toutes entièrement définies par le 4ième octet.

Un masque de sous réseau de15 bits à 1 supplémentaire (11111111 = 255 pour le 3ième octet et 11111110 = 254 en décimale pour le 4ième octet) se présente ainsi : 255.255.255.254 et offre 32768 sous réseaux (2 à la puissance 15 = 32768 sous réseaux). Chacun de ces sous réseaux peut contenir 2 à la puissance 1 = 2 stations ou adresse IP différentes. Avec un pas de 2 entre chaque sous réseaux.

Un masque de sous réseau de16 bits à 1 supplémentaire (11111111 = 255 pour le 3ième octet et 11111110 = 255 en décimale pour le 4ième octet) se présente ainsi : 255.255.255.255. Un tel masque ne serait pas utiliser dans la pratique puisqu'il correspond par convention à l'adresse de broadcast générale. Toutefois, en en écartant cette convention, et en utilisant les valeurs extrêmes, il y aurait une valeur théorique de 65536 sous réseaux (2 à la puissance 16 = 65 536 sous réseaux). Chacun de ces sous réseaux pourrait contenir une seule station par sous réseau (2 à la puissance 0 = 1)!

On constate qu'à chaque bits supplémentaire à 1 pour le masque de sous réseau, il y a deux fois plus de sous réseaux, mais deux fois moins de stations dans chaque sous réseau. Il y a bien un arbitrage à faire entre le nombre de sous réseau et le nombre d'adresse IP disponibles dans chaque sous réseau...

XVIII - Les applications réseaux

XVIII-1 - L'avantage du travail en réseau

L'avantage du travail en réseau ne consiste pas seulement à échanger des messages ou des fichiers. Le travail en réseau permet de travailler en équipe, mais aussi de travailler à plusieurs, dynamiquement, sur le même projet.

De plus en plus d'applications sont conçues pour le travail dynamique en réseau. La plupart des applications ont généralement été conçues pour être exécutées sur des ordinateurs en mode autonome. De plus en plus, les éditeurs développent des versions multi-utilisateurs pour un environnement réseau de leurs applications.

Les applications réseaux changent les méthodes de travail :

XVIII-2 - Les applications réseaux

L'expression « applications réseaux » peut désigner plusieurs choses :

- Les « applications » qui sont mises à la disposition des utilisateurs sur un serveur d'application.
- Les gestionnaires de données personnels (PIM pour Personal Information Manager)
- Les « applications réseaux » (Applications GROUPWARE) qui ont été conçues pour fonctionner en réseau et en mode multi utilisateurs.
- Les « systèmes d'application réseaux » (systèmes GROUPWARE) qui permettent le travail en groupe sur un réseau.

Les applications réseaux sont généralement spécialisées dans un champ d'activité :

XVIII-3 - La messagerie électronique

La messagerie électronique permet d'échanger des messages et des documents annexés au message en « pièces jointes ». Les correspondants d'une messagerie électronique doivent tous avoir une adresse électronique, une adresse de messagerie qui les identifie sur le réseau. Les applications de messagerie électronique stimulent la croissance des réseaux.

La messagerie électronique est souvent la première pierre des applications de groupware. La messagerie électronique permet de transporter des données d'un ordinateur vers un autre. En utilisant un « serveur de liste », il est possible d'effectuer des envois groupés aux personnes qui se sont abonnées à la liste (subscribe en anglais).

XVIII-4 - Les agendas de groupe

Les agendas permettent de planifier une réunion et de gérer les plannings :

- Les plannings individuels
- Les plannings de groupes

Les agendas de groupe permettent d'organiser et d'harmoniser les emplois du temps de plusieurs utilisateurs :

- L'avertissement automatique d'un prochain rendez-vous.
- L'organisation de réunions :
- La vérification sur les agendas personnels de la disponibilité de toutes les personnes conviées à une réunion (pour une certaine plage horaire).
- L'incorporation de la réunion (dans une plage horaire qui convient à tous) dans tous les agendas individuels des personnes concernées.

L'unité de temps des plannings peut varier :

- Journalier
- Hebdomadaire
- Mensuel
- Semestriel
- Annuel

Il existe différents produits d'agenda de groupe, mais ils ne sont pas standardisés (par l'IETF) et ne sont pas compatibles entre eux :

- ICAL (Internet Calendaring Standard) pour organiser des réunions via Internet
- ICAP (Internet Calendar Access Protocol)
- SSTP (Simple Scheduling Transport Protocol)

XVIII-5 - La gestion des contacts

Les logiciels de gestion des contacts permettent de constituer une base de données commune et accessible par différents utilisateurs. La base de données peut rassembler et structurer les informations (concernant les clients, les fournisseurs, les employés,...) et effectuer des recherches en fonction de différents critères (le nom, l'adresse, les rendez-vous, les appels téléphoniques, les lettres, le chiffre d'affaire, le salaire,...).

Les logiciels de gestion des contacts ne sont pas encore normalisés par l'IETF :

- ACT ! de Symantec
- Commence de Commence Corporation
- Gold Mine

XVIII-6 - Les logiciels de productivité de groupe (GROUPWARE)

Le terme GROUPWARE peut désigner les logiciels de travail en groupe proprement dit, que les moyens informatiques mis à la disposition des groupes de travail. Le principe du GROUPWARE est de fournir certaines fonctionnalités pour les équipes, les documents et les projets du groupe de travail :

Voici des exemples d'applications de GROUPWARE (logiciels de productivité de groupe) :

- Les BBS (Bulletin Board Systems) sont des systèmes de tableau d'affichage sur lequel plusieurs utilisateurs peuvent simultanément dessiner...
- Les conférences interactives (la visioconférence)
- L'agenda de groupe MICROSOFT SCHEDULE+
- La messagerie électronique de MICROSOFT EXCHANGE
- Les applications multimédia de groupware
- La famille d'application de lotus notes

- Le service de messagerie INTELLIGENT BANYAN
- TEAMLINK de DIGITAL EQUIPMENT
- NOVELL GROUPWISE

Il faut quand même faire la part des choses et essayer de distinguer les applications de GROUPWARE (qui peuvent être utilisées dans le cadre d'un groupe de travail en réseau, mais qui ont une fonction bien précise, comme l'échange de messages par exemple), et les systèmes de GROUPWARE (qui sont des applications spécifiques, et dont le seul but est d'organiser et de coordonner les activités des groupes de travail en réseau).

Les meilleurs systèmes de GROUPWARE sont capables de fonctionner dans un environnement hétérogène...

XVIII-7 - LOTUS NOTES

LOTUS NOTES est un système de GROUPWARE complet et cohérent.

LOTUS NOTES se décline en trois versions différentes :

- LOTUS NOTES
- LOTUS NOTES DESKTOP
- LOTUS NOTES EXPRESS

LOTUS NOTES apporte des fonctionnalités spécifiques au travail en groupe :

- L'administration
- La connexion
- Les services d'annuaire
- La gestion des documents
- La réplication
- La sécurité

LOTUS NOTES est compatible avec pratiquement tous les environnements...

XVIII-8 - Le journal de bord de l'administrateur réseau

L'administrateur réseau se doit d'être prévoyant, pour le prouver, il devrait tenir un journal de bord contenant toues les informations relatives aux applications partagées sur son réseau !

Les informations du journal de bord :

- Les besoins en ressources de l'application :
- La quantité d'espace libre sur le disque dur pour accueillir l'application.
- La capacité du serveur à répondre aux sollicitations des utilisateurs pour la nouvelles application.
- Les périphériques associés à la nouvelle application (un traitement de texte va de pair avec une imprimante...)
- L'identification de l'application :
- Le nom
- La date d'installation

- La procédure d'installation
- Le numéro de version de l'application ou de la mise à jour
- La configuration de l'application :
- Les fichiers batch (éventuellement) pour configurer l'application
- Les choix de configuration de l'application
- L'administration des utilisateurs et des groupes :
- Les droits, les permissions, les niveaux d'accès,...
- La formation
- La sauvegarde
- La sauvegarde des documents générés par la nouvelle application
- La copie de sauvegarde de l'application sur un CDROM

XIX - L'impression en réseau

Le travail d'impression initialisé par un utilisateur passe par plusieurs étapes avant d'être reçu par le périphérique d'impression, communément appelé « l'imprimante ». Le terme « d'imprimante » peut également être employé pour désigner le fichier qui stocke tous les travaux d'impression avant qu'ils soient chacun leur tour envoyés au périphérique d'impression.

Le périphérique d'impression peut être relié au réseau de deux façons différentes :

- Le périphérique d'impression peut être relié au réseau par l'intermédiaire d'un serveur d'impression
- Le périphérique d'impression peut être directement relié au câble du réseau, il s'agit alors d'une véritable « imprimante réseau » avec une carte réseau, un processeur et de la mémoire RAM, ...)

XIX-1 - Le processus d'impression en réseau

Le processus d'impression en réseau s'effectue en plusieurs étapes :

- L'utilisateur déclenche un travail d'impression (une requête d'impression) depuis une application exécutée localement sur son ordinateur
- La commande d'impression est interceptée par le redirecteur, le travail d'impression n'est pas envoyé vers le port parallèle (LPT1 ou LPT2), mais vers la carte réseau qui le place sur le câble du réseau
- Le travail d'impression circule sur le réseau
- Le logiciel réseau (celui du serveur d'impression ou celui du périphérique d'impression réseau) réceptionne le travail d'impression, et l'envoie dans la file d'attente (qui stocke éventuellement d'autres travaux d'impression)
- Le travail d'impression se place dans la file d'attente en fonction de sa priorité
- Le périphérique d'impression imprime le travail d'impression
- L'utilisateur va chercher son document imprimé...

XIX-2 - La file d'attente du périphérique d'impression

Sur un réseau très chargé, de nombreux travaux d'impression sont envoyés en même temps. Les travaux d'impressions sont stockés et attendent dans la file d'attente du périphérique d'impression.

La file d'attente du périphérique d'impression est aussi dénommée un « spool » (Simultaneous Peripheral Operations On Line). Le spool est une mémoire tampon appartenant à la mémoire RAM du serveur d'impression (ou à la mémoire RAM de l'imprimante réseau). Tous les travaux d'impression sont stockés dans le SPOOL, puis selon leur degré de priorité, ils sont chacun leur tour imprimés. Quand le SPOOL est saturé, les requêtes d'impression sont alors stockées sur le disque dur du serveur d'impression, mais alors le transfert du travail d'impression entre le SPOOL et le périphérique d'impression est moins rapide...

XIX-3 - Le partage du périphérique d'impression réseau

Pour être accessible depuis un ordinateur distant, le périphérique d'impression réseau doit avoir une identification réseau et doit être partagé. Le périphérique d'impression réseau qui est partagé sera « visible » depuis chaque ordinateur.

La procédure de partage d'un périphérique réseau dépend du système d'exploitation, mais comporte en général certaines actions indispensables :

- L'installation du périphérique d'impression sur le serveur d'impression
- Le chargement du pilote du périphérique d'impression sur le serveur d'impression
- La création d'un nom de partage compréhensible par les utilisateurs
- La configuration du redirecteur de tous les ordinateurs, afin de lui indiquer la direction de la sortie pour les travaux d'impression...
- Le paramétrage du format des travaux d'impression afin que ceux-ci soient conformes à ce que peut « comprendre » le périphérique d'impression.

Sous WINDOWS NT SERVER, le partage d'imprimante s'effectue avec l'aide d'un assistant, d'un utilitaire qui guide l'administrateur dans les différentes étapes de la configuration du périphérique d'impression (Panneau de Configuration + Module Imprimantes + Ajout d'une Imprimante).

XIX-4 - La connexion à un périphérique d'impression

Un utilisateur qui souhaite se connecter à un périphérique d'impression partagé doit connaître deux choses :

- Le nom du serveur d'impression auquel est relié le périphérique d'impression
- Le nom du périphérique d'impression pour lequel l'utilisateur possède les droit d'impression. Plusieurs périphériques d'impression peuvent dépendre du même serveur d'impression...

Sous WINDOWS NT, la connexion à un périphérique d'impression s'effectue à l'aide d'une interface graphique qui guide l'utilisateur d'impression (Panneau de Configuration + Module Imprimantes + Ajout d'une Imprimante).

XIX-5 - L'administration du périphérique d'impression

L'administration du périphérique d'impression est souvent conférée à une autre personne que l'administrateur du réseau (il y a tellement à faire...). Il est préférable en tout cas que « l'administrateur de l'imprimante » (l'opérateur d'impression) soit le seul responsable de l'imprimante afin qu'il n'y ait pas de rassemblement de mauvaise humeur lors de la survenue d'un incident, et que son lieu de travail soit tout près du périphérique, afin de pouvoir résoudre le plus rapidement possible les problèmes les plus fréquents :

L'administration d'une imprimante réseau WINDOWS NT peut s'effectuer localement sur le serveur d'impression, ou à distance à partir de n'importe quel poste. Sous WINDOWS NT un utilitaire facilite l'administration de l'imprimante et la gestion des utilisateurs (Panneau de Configuration + Module Imprimantes + Icône de l'imprimante partagée).

XIX-6 - Les droits et les permissions d'imprimer pour les utilisateurs

Les utilisateurs doivent avoir le droit d'imprimer.

XIX-7 - Les droits et les permissions de l'administrateur de l'imprimante

L'administrateur de l'imprimante doit avoir les droits et les permissions correspondant à ses responsabilités :

- La gestion des utilisateurs
- L'octroie du droit d'imprimer
- La suppression du droit d'imprimer

- La création d'un nouvel administrateur de l'imprimante pour le suppléer ou le remplacer
- La gestion des travaux d'impression dans le SPOOL de l'imprimante
- La modification des priorités
- La suspension en cas de saturation
- La suppression

Sous WINDOWS NT un utilitaire facilite l'administration de l'imprimante et la gestion des utilisateurs (Panneau de Configuration + Module Imprimantes + Icône de l'imprimante partagée + Onglet Sécurité).

XIX-8 - Le langage de description de page

Les langage de description de page (PDL pour Page Description Languages) permet au périphérique d'impression de savoir comment imprimer un travail d'impression. Le langage de description de page constitue en code qui est interprété, converti par l'imprimante afin d'aboutir à une réalisation graphique sur le papier.

Le langage de description de page accompagne le travaille d'impression et renseigne l'imprimante sur les valeurs de la ou des polices de caractères utilisées dans le document :

- La ou les polices de caractères
- Les paramètres de la police de caractères :
- La taille
- La couleur
- L'épaisseur
- Le soulignement

Les polices de caractères peuvent être de deux types :

- Les polices bit-map qui ont été conçues avec certaines tailles, et sont définie à l'intérieur d'une matrice
- Les polices vectorielles qui sont « extensibles » à volonté puisqu'elles sont définies par une formule mathématique :
- La police TRUETYPE de la société APPLE
- La police POSTSCRIPT de la société Adobe

Les polices de caractères de type vectoriel sont plus souples, elles permettent plus de créativité dans la conception et la mise en page de documents, et elles offrent un rendu graphique plus lissé...

XX - La messagerie électronique

XX-1 - L'échange de messages électroniques

Le courrier électronique, la messagerie électronique, le mail, sont différentes dénominations pour désigner l'outil de communication le plus connu et le coutumier des réseaux. Le courrier électronique permet de rester dans le monde du numérique, il n'y a plus de « hard copy », les documents transitent d'ordinateurs à ordinateurs sans passer par l'étape de l'impression papier, c'est l'ère du « zéro papier ».

La messagerie électronique permet d'échanger des messages et des documents annexés au message en « pièces jointes ». Les correspondants d'une messagerie électronique doivent tous avoir une adresse électronique, une adresse de messagerie qui les identifie sur le réseau.

Le courrier électronique peut être restreint à une zone ou élargie au monde entier :

- La messagerie interne (en Intranet). Installée à l'intérieur d'une entreprise et exclusivement réservée aux employés de l'entreprise, le service de messagerie est géré par le service informatique de l'entreprise.
- La messagerie externe (avec Internet). Permettant la communication avec l'extérieur de l'entreprise (avec d'autres entreprises, ou des particuliers), le service de messagerie (souvent constitué d'une passerelle qui convertit les protocoles) est géré par un fournisseur extérieur.

Selon les envergures des zones, les populations et les fournisseurs de la messagerie électronique, les protocoles de communication, les formats ne sont pas forcément les même, et il faudra installer des passerelles de messagerie pour convertir les messages d'une messagerie à l'autre, d'une plate-forme de communication à une autre...

MICROSOFT EXCHANGE est une application de courrier électronique groupware pour les réseaux Intranet. Son successeur OUTLOOK est un produit « intégré » qui gère dans une seule interface plusieurs fonctionnalités, dont la réception des mails (les boites aux lettres), l'expédition des mails (serveur de messagerie), l'agenda de groupe, et la gestion des contacts. OUTLOOK 98 est compatible avec le protocole IMAP 4.

XX-2 - Les fonctionnalités de la messagerie électronique

Les fonctionnalités de la messagerie électronique ou du courrier électronique sont nombreuses et s'apparentent aux différents services que propose la Poste :

- La boîte aux lettres pour chaque utilisateur
- La notification personnalisée interpelle en temps réel le destinataire qu'un courrier vient de lui parvenir
- L'accusé de réception informe l'expéditeur que son message est bien arrivé
- La réponse à un courrier peut inclure le message d'origine
- Les pièces jointes annexées au message peuvent être de tous les formats possibles (textes, photos, sons, vidéos, graphiques, feuilles de calcul, tables d'une base de données,...)
- L'envoi en copie du même message à un autre destinataire (avec le champ CC pour Carbon Copy)
- L'expédition groupé d'un même message à plusieurs destinataires
- L'annuaire (Directory en anglais) répertorie tous les abonnées aux service de messagerie
- La récupération des message effacés par erreurs
- L'absence de bureau (OOF pour Out of Office en anglais) permet d'indiquer au correspondants que le

destinataire de leur courrier n'est pas là et qu'il reviendra bientôt...

XX-3 - L'administration d'une messagerie électronique

L'administrateur du réseau peut désigner un « administrateur de messagerie ».

Le tâches de l'administrateur de messagerie sont nombreuses et répétitives :

- La gestion des utilisateurs
- Les boîtes aux lettres
- Les comptes des utilisateurs et des groupes
- Les droits et des permissions des utilisateurs
- L'annuaire
- La formation des utilisateurs à cette nouvelle technologie
- La gestion des messages
- Le stockage des messages sur le serveur de messagerie
- La définition du bureau de poste
- La gestion du réseau :
- Le contrôle des utilisateurs distants
- Les autres services de messagerie
- La mise en place de passerelles pour convertir les courriers des messageries externes à l'entreprise

XX-4 - Les normes de messagerie électronique

La norme ISO localise la gestion du courrier électronique au niveau de la couche APPLICATION, la couche 7. Ainsi, des réseaux utilisant des systèmes d'exploitation différents peuvent s'échanger des messages...

Il existe différentes normes pour le courrier électronique correspondant à des systèmes de messagerie différents :

- X.400 élaboré par le CITT (Comité Consultatif International de télégraphie et de téléphonie) pour gérer les messages indépendamment des matériels et des logiciels.
- L'agent utilisateur (User Agent)
- Le système de transfert de messages (Message Transfert System)
- L'agent de transfert des messages (Message Transfert Agent)
- X.500 échafaudé par le CITT, pour gérer les services d'annuaire des réseaux distribués, et permettre de retrouver facilement l'adresse d'un utilisateur appartenant à un autre réseau.
- Une structure hiérarchique d'annuaires
- Des agents pour retrouver l'information
- SMTP (Simple Mail Transfert Protocole) a été conçu pour l'échange de messages entre deux ordinateurs distants. C'est le protocole de messagerie utilisé sur les systèmes UNIX et sur Internet, il fait partie de la pile de protocole TCP/IP.
- MHS (Message Handling Service) a été popularisé par la société NOVELL et ressemble à X.400. Les serveur MHS servent de passerelles et convertissent les messages provenant de systèmes de messagerie différents.

XX-5 - Les passerelles entre systèmes de messagerie

Les systèmes de messageries utilisant des normes différentes (par exemple entre différents opérateurs téléphoniques ou entre différents fournisseur d'accès à Internet) doivent passer par des passerelles pour échanger des courriers avec les autres systèmes. Les passerelles sont souvent situées sur des ordinateurs dédiés. Les passerelles convertissent les protocoles des différentes messageries.

Certaines messageries incorporent les services d'une passerelle :

- MICROSOFT EXCHANGE
- MICROSOFT MAIL
- CC:MAIL

XX-6 - L'origine de la messagerie électronique

L'email est dès l'origine une fonction de base des systèmes UNIX. Il s'agissait d'un automate de copie de fichier d'un disque dur vers un disque dur d'un ordinateur distant. Il existait différentes versions de cet automate. Afin d'harmoniser les outils, Eric Altman écrivit un programme appelé « sendmail ».

Au départ, les e-mails étaient simplement du texte. L'IETF considéra qu'il fallait rendre plus attractive l'apparence des e-mails, et créa la norme MIME (Multipurpose Internet Mail Extensions). La norme MIME permet également d'associer à un message un fichier, et cela quelque soit son format.

XX-7 - Les applications de messagerie propriétaires

Il existe des applications de messagerie « propriétaire » développées par des sociétés informatiques :

- CC :MAIL de Lotus
- Microsoft Mail de Microsoft
- MHS (Mail Handling System) de Novell

Les différents produits de ces différentes sociétés sont généralement plus faciles à mettre en oeuvre que « sendmail », mais sont généralement incompatibles entre eux. Fort heureusement, cette situation provoqua le besoin de communiquer et échanger des e-mails entre ces différents systèmes de messagerie ; ces sociétés informatiques développèrent alors de nouveaux produits pour répondre à la demande, les passerelles de messagerie.

Ces systèmes de messagerie « propriétaires » sont dits « serveur centrique », c'est à dire qu'ils fonctionnent dans un réseau local. Pour s'ouvrir à Internet et échanger des messages à travers le monde entier, ils ont besoin non seulement une connexion à Internet, mais surtout, d'une autre passerelle, celle qui convertie les e-mail au format SMTP, standard de la pile de protocole TCP/IP d'Internet. Ces différentes conversion consomme des ressources et prennent du temps, c'est pourquoi, il est préférable dès le départ d'utiliser un standard ouvert.

XX-8 - Les standard ouverts d'Internet

Les standards ouverts pour la messagerie électronique d'Internet ont été définies par l'IETF :

- SMTP pour la partie serveur, c'est la partie qui stocke les e-mails entrants des utilisateurs et qui le transmet au serveur du destinataire. Le protocole SMTP (Simple Mail Transfert Protocol) route le courrier entre les différents serveurs de messagerie de l'Internet. SMTP est plus simple que UUCP (Unix to Unix copy Program) qui nécessitait que l'utilisateur connaisse et saisisse le chemin complet entre l'expéditeur et le destinataire (y compris tous les noeuds intermédiaires). SMTP requière de la part de l'utilisateur, seulement un nom d'utilisateur et un nom de domaine, le reste, il s'en charge...
- POP 3 et IMAP 4 pour la partie cliente, c'est la partie qui envoie les e-mails sur le serveur de messagerie de l'expéditeur. Avec POP 3, le client le plus ancien, l'utilisateur doit se connecter au serveur de messagerie

pour télécharger ses messages, une fois fait, ceux-ci sont effacés du serveur, tandis que IMAP 4 peut éventuellement en garder une copie. Le protocole IMAP 4 est recommandé pour les réseaux dont les utilisateurs se déplacent.

XXI - Le travail de télécopie en réseau

Le travail de télécopie en réseau ressemble au travail d'impression en réseau. Un serveur de télécopie peut être installé sur le réseau comme il y a des serveurs d'impression. Le serveur de télécopie est relié à un « modem partagé », lequel est relié au réseau téléphonique RTC.

XXI-1 - Les avantages du travail de télécopie en réseau

Dans un réseau, un serveur de télécopie peut être installé afin de faciliter la gestion des télécopies de tous les utilisateurs de réseau :

- La centralisation des télécopies sur un serveur de télécopie :
- La gestion des télécopies
- Le filtrage des télécopies publicitaires
- La surveillance des télécopies entrantes et sortantes
- L'association du numéro de télécopie d'un utilisateur à son adresse électronique sur l'intranet permet de dispatcher automatiquement (router) les télécopies entrantes
- La gestion des utilisateurs ayant le droit de télécopier
- Le gain de temps pour les utilisateurs :
- Les utilisateurs n'ont plus besoin de se déplacer vers le fax
- Les utilisateurs n'ont plus la contrainte d'attendre à coté du fax

XXI-2 - Le routage des télécopies

Les télécopies entrantes sont adressées à un numéro de télécopie, la télécopie mentionne généralement le nom du destinataire, mais il peut arriver qu'il n'y figure pas. Par ailleurs, les télécopies provenant de l'extérieur (leurs expéditeurs) ne peuvent pas savoir si le site de destination est organisé autour d'un intranet, les télécopies entrantes ne sont donc pas associées à une adresse électronique. Il faut router les télécopies entrantes vers leur destinataire final, quand elles arrivent sur le serveur de télécopie.

Le routage des télécopies entrantes peut s'effectuer de différentes manières :

- Le routage manuel, une personne se consacre régulièrement à transférer les télécopies vers leur destinataire, mais ce n'est pas une solution très opérationnelle, ni très confidentiel...
- L'utilisation d'un logiciel de reconnaissance optique de caractères (OCR pour Optical Character Recognition) permet de convertir le texte de la page de garde. Il faut ensuite automatiser les tâches de recherche et de lecture du champ « destinataire » de la télécopie afin d'identifier le nom du destinataire, et enfin associer le nom du destinataire avec son adresse électronique sur le réseau.
- L'utilisation d'un logiciel de reconnaissance intelligente de caractères (ICR pour Intelligent Character Recognition) permet de convertir le texte de la page de garde et recherche le nom du destinataire.
- Le sous-adressage T.30 est un protocole de télécopie qui a été modifié afin d'intégrer un champ supplémentaire (un numéro complémentaire) pour le routage interne de la télécopie.
- La technologie NEST (Novell Embedded Systems Technologie) est semblable au sous-adressage T.30
- Le routage par code barre sur la télécopie
- Le routage TSI (Transmission Station Identification) qui utilise le numéro de télécopieur de l'expéditeur pour router la télécopie vers son destinataire.
- Le routage RFL (Received Fax Line) qui utilise plusieurs modem et plusieurs numéro de téléphone. Les télécopies adressées à un certain numéro sont routées vers un groupe d'utilisateurs.
- La technique SDA (Sélection Directe à l'arrivée) qui utilise une ligne téléphonique spéciale (Trunk) associée à plusieurs numéro de téléphone. Toutes les télécopies entrantes sont envoyées à un seul numéro de

téléphone, mais quand une télécopie arrive, l'opérateur téléphonique émet un signal particulier afin de spécifier le routage de la télécopie entrante.

XXI-3 - Le logiciel FACSys 4.0 pour WINDOWS NT

Le logiciel FACSys 4.0 conçu par la société OPTUS SOFTWARE fournie une passerelle télécopie pour WINDOWS NT :

- Les applications des utilisateurs (comme un traitement de texte, un tableur, une base de données, une messagerie électronique, etc...) peuvent servir de « frontal » au serveur de télécopie, c'est à dire que les utilisateurs peuvent émettre des télécopies depuis leurs applications. Le frontal envoie la requête de télécopie au serveur de télécopie qui la transmet au réseau téléphonique.
- Le logiciel FACSys 4.0 procure une interface WINDOWS ou MS-DOS aux ordinateurs clients.
- Le logiciel FACSys 4.0 reconnaît différents langage de description de page :
- Le langage HP PCL (Hewlett Packard Printer Control Language)
- Le langage PCL5
- Le langage POSTSCRIPT
- Le logiciel FACSys 4.0 route automatiquement les télécopies entrantes.
- Le logiciel FACSys 4.0 est compatible avec plusieurs type de cartes fax modem :
- GAMMAFAX
- INTEL SATISFAXTION
- HAYES
- JTFAX
- Le logiciel FACSys 4.0 fournit un utilitaire de diagnostique et des fonctionnalités d'administration très utiles...

XXII - Les performances des réseaux

Augmenter les performances d'un réseau signifie accélérer la transmission des données (le débit) ou augmenter la quantité de donnée qu'il est possible de transmettre (la bande passante).

Les performances d'un réseau peuvent être mesurées par le débit, c'est à dire la quantité de Méga Octets transmis sur le câble par secondes. Plus le nombre de Méga Octets par seconde est élevé et plus le réseau est performant. On dit que le réseau « s'effondre » quand plus aucune machine ne peut transmettre de message.

Les performances d'un réseau dépendent de nombreux facteurs :

- Le nombre de machines connectées au même câble
- Le débit théorique maximal du câblage
- Le tuning
- Les cartes réseaux

XXII-1 - Les performances de la carte réseau

La carte réseau est un élément crucial de la performance d'un réseau. Si la carte réseau est lente, alors les données seront transmises lentement sur le réseau. Dans un réseau en bus par exemple, personne ne peut utiliser le réseau tant que le réseau n'est pas libre, et une carte lente augmente les délais d'attente pour les autres utilisateurs.

Les stations qui produisent un volume important de données sur le réseau sont généralement les serveurs. La carte réseau des serveurs doit être équipée en priorité des modèles les plus performants.

La carte réseau d'une station de travail n'a généralement pas besoin d'être performante, bien sûr tout dépend de la nature de l'activité de la station. Une station qui n'exécute que des applications bureautiques ne génère pas beaucoup de trafic, mais une station qui travaille sur une application réseau comme une base de données ou une application d'ingénierie génère rapidement beaucoup de trafic.

Une carte réseau produite par un fabricant connu depuis longtemps aura une meilleure pérennité, fiabilité, et les pilotes auront plus de chance d'être mis à jour par la suite.

XXII-2 - Les facteurs d'amélioration d'une carte réseau

Les facteurs d'amélioration des performances sont de deux ordres, soit la carte réseau accède directement aux ressources de l'ordinateur, soit elle dispose de ses propres ressources. Quoiqu'il en soit, il faut une quantité de mémoire vive suffisante et un processeur rapide :

- Un accès direct à la mémoire (DMA) de l'ordinateur. La carte réseau transfère directement les données depuis la mémoire tampon de la carte réseau vers la mémoire de l'ordinateur (RAM), sans passer par le microprocesseur.
- Le contrôle du bus (bus mastering) de l'ordinateur. La carte réseau prend le contrôle du bus de l'ordinateur,

les données sont transmises directement à la mémoire vive (RAM) de l'ordinateur sans passer par le microprocesseur de l'ordinateur qui peut s'occuper d'autres traitements. Ces cartes réseaux sont onéreuses, mais elles peuvent améliorer les performances du réseau de 20 à 70 %. Les cartes réseaux EISA et MCA permettent de prendre le contrôle du bus de l'ordinateur.

- La mémoire partagée de la carte réseau. La carte réseau possède de la mémoire vive (RAM) qu'elle partage avec l'ordinateur. L'ordinateur considère cette mémoire comme la sienne et les données sont directement adressées à la mémoire vive de la carte réseau.
- La RAM tampon de la carte réseau. La carte réseau possède de la mémoire vive (RAM) qui lui sert de mémoire tampon. Les données circulent généralement beaucoup plus vite sur le réseau que ne peut les traiter la carte réseau ; afin d'absorber le flux trop important de données provenant du réseau, la carte réseau les stocke dans la mémoire tampon. La mémoire tampon permet d'éviter les goulets d'étranglement.
- Un microprocesseur intégré à la carte réseau. La carte réseau possède son propre processeur qui traite les données sans passer par le processeur de l'ordinateur.
- La mémoire système partagée. La carte réseau possède un processeur et utilise une partie de la mémoire vive (RAM) de l'ordinateur pour traiter les données du réseau.

Une carte réseau avec son propre processeur et sa propre mémoire vive (RAM) sera plus rapide que n'importe quels autres cartes réseaux. Une carte réseau avec de la mémoire partagée sera plus rapide qu'une carte réseau avec un accès directe à la mémoire de l'ordinateur (DMA) et à fortiori bien plus rapide qu'une carte réseau avec des E/S normales.

XXIII - La planification et la maintenance d'un réseau

XXIII-1 - Le processus de décision

Avant de prendre une décision importante, il faut procéder en trois étapes :

- La collecte d'informations
- Les études de marché
- La documentation
- Les interviews des clients, des utilisateurs et des dirigeants
- La rencontre avec les experts, les consultants, les intégrateurs, les constructeurs, les éditeurs, les fournisseurs et les distributeurs
- L'analyse des informations
- Le choix d'une solution
- La diffusion de la décision aux personnes concernées

Il faut savoir aussi remettre en question ses propres décisions : « Le changement est la seule constante ». La loi de Moore, le cofondateur de la société Intel, indique que la puissance des processeurs double tous les 18 mois. Il se trouve que le besoin en mémoire vive des applications grossit de version en version.

Les technologies de l'informatique évoluent très rapidement, le cycle de renouvellement du matériel est très court, aussi est-il rentables d'anticiper les besoins futurs. Le choix de la configuration la plus performante du moment pour un serveur (processeur, mémoire vive, espace de stockage,...) permet parfois d'allonger la durée de vie d'un matériel. Les équipements qui disposent de fonctionnalités avancées deviennent moins rapidement obsolètes que les autres.

Bien sûr, une décision a un coût, et même si l'installation d'un réseau est une aventure intellectuelle, la plus part du temps celle-ci est engagée en attendant un retour sur investissement (RSI). Le Gartner Group estime le coût annuel d'un PC à 60 000,00 Francs. En général, l'installation d'un réseau est facteur de réduction des coûts à moyen terme et d'augmentation de la productivité.

Un réseau en bon état de marche ne sert à rien s'il n'y a des utilisateurs qui se servent d'applications pour créer des documents et les transmettre à d'autres utilisateurs. La planification du réseau devrait prendre en compte les types et le nombre de logiciels dont ont besoins les utilisateurs dans leur travail. En général, quand plus de 20 utilisateurs emploient la même application, il est rentable d'acquérir une licence de cette application pour le site. Il va sans dire qu'il faut acheter les logiciels d'une part pour ne pas spolier les auteurs de leurs droits, mais aussi pour rester dans la légalité et recourir au support technique et aux mises à jour de l'éditeur.

La rédaction d'une « spécification » précise et détaillée permettra de limiter les risques de dérive du projet, comme l'ajout de fonctionnalités supplémentaires. De surcroît, le document rassemblant les spécifications du réseau est non seulement une source d'information pour la maintenance et le dépannage quotidien, mais aussi, peut être un point de départ pour l'extension et le développement du réseau.

XXIII-2 - Les critères fondamentaux

La planification et la maintenance dépendent d'un grand nombre de facteurs dont il faut avoir conscience et qu'il

faut savoir estimer dans la mesure du possible.

Certains critères sont fondamentaux :

Par exemple, un réseau de plus de 20 ordinateurs doit s'organiser autour d'une architecture client-serveur, et requièrent une centralisation de l'administration sous la responsabilité d'au moins 2 personnes. L'organisation en client-serveur permet la centralisation des fichiers, facilite les sauvegardes, et accroît le contrôle des utilisateurs.

Les serveurs ont généralement besoin de plus de puissance, de plus de mémoire et de plus de capacité de stockage.

Dans une topologie en étoile organisée autour d'un commutateur qui segmente le réseau, il est intéressant de réserver l'un des segments pour le serveur, ainsi l'accès et le transfert des données sera optimisé. Il existe des commutateurs qui permettent de restreindre la « visibilité » des ports et par conséquent des segments entre eux. Par exemple, le port 2 peut être configuré de telle sorte qu'il ne puisse « voir » que le port 6 et vice versa, ainsi, non seulement les deux segments sont « segmentés », c'est à dire que les paquets sont filtrés et routés, mais aussi, les deux segments forme un petit LAN indépendamment des autres segments du réseau (cette technologie s'appelle un VLAN ou Virtual LAN).

L'administration centralisée d'un réseau s'effectue par l'intermédiaire des protocoles SNMP (Simple Network Management Protocol) et RMON (Remote Monitor), aussi dans l'éventualité future d'une administration centralisée du réseau, il est précautionneux de n'acheter que du matériel qui est compatible avec ses deux protocoles.

Souvent un dessin vaut mieux qu'un long discours, aussi est-il judicieux d'élaborer un diagramme logique du réseau, c'est à dire un dessein organisationnel, fonctionnel et relationnel qui répertorie et classe tous les ordinateurs du réseau, logiquement et physiquement. Il faut vérifier la ventilation ou la climatisation de la pièce.

Quand plusieurs appareils partagent le même local, il est prudent de vérifier si l'alimentation électrique existante sera suffisante pour alimenter tous les appareils de la pièce. La somme des consommations électriques (des intensités) de chaque appareil (généralement en milliampères) ne doit pas dépasser l'ampérage de la prise.

Avant la mise en place concrète du réseau, il faut s'assurer que tous les composants ont bien été livrés, et que ceux-ci correspondent aux spécifications qui ont été commandées. Par exemple, il faut vérifier le type, le nombre et la longueur du support de communication (câbles coaxial, en paires torsadées, en fibre optique,...), le type et le nombre de connecteurs (ou l'armoire de brassage), le nombre et la longueur des cordons de brassage, les types et le nombre des dispositifs de connectivité (répéteur, pont, routeur, passerelle, commutateur, modem,...), etc...

D'une façon générale, il faut consigner dans un cahier tout ce qui se passe, afin de garder une trace des innombrables événements qui jalonnent l'implémentation d'un réseau, et de pouvoir entamer un recours en cas de litige. Enfin, il faut tester tout de suite l'installation.

Certaines sociétés proposent des questionnaires qui permettent d'orienter le choix entre la multitude des technologies. D'autres sociétés, proposent des configurations génériques.

Parfois, il faut tenir compte des caractéristiques d'un réseau préexistant...

XXIII-3 - Les diagrammes réseaux

Les ordinateurs du réseau sont classées par types en fonction de leur utilisation, du service auquel ils appartiennent, ou de la catégorie de leurs utilisateurs. Chaque type d'ordinateur partage avec les autres types un certain nombre d'informations :

Il est aussi instructif de dessiner le diagramme physique du réseau qui montrera la topologie les dispositifs de connectivité (avec le nombre et le type de ports), les câbles, la segmentation et les machines réparties dans les différentes pièces ou locaux du site.

Il existe plusieurs logiciels de création des diagrammes réseaux :

- Visio Pro
- ClickNet
- NetDraw

XXIII-4 - Un exemple d'un petit réseau standard

Un petit réseau pour une petite société (50 postes, localisés dans le même immeuble, véhiculant des données importantes mais pas stratégiques) est un type de réseau très courant et facile à mettre en oeuvre :

- Bus en étoile
- Câble en paire torsadée non blindée (UTP catégorie 5)
- Cartes réseaux Ethernet 10BaseT
- Organisation mixte peer to peer et C/S
- Des serveurs dédiés pour les fichiers et la messagerie Intranet
- Imprimante réseau avec un SPOOLER
- Un serveur pour l'accès à Internet

XXIII-5 - Le questionnaire

XXIII-6 - La vie du réseau

La maintenance d'un réseau commence dès le début de la planification et se poursuit tout au long de la vie du réseau :

La stratégie, la théorie, l'élaboration du projet, la planification :

La tactique, la pratique, l'installation ou l'implémentation :

- L'installation (COMMENT) scrupuleuse et attentive des câbles, des matériels et des logiciels.
  L'implémentation par une société externe.
- La segmentation du réseau pour limiter, circonscrire ou répartir le trafic

- La répartition des responsabilités (comme la diversification des actifs d'un portefeuille financier). Il ne faut pas que tout le réseau dépende d'un seul matériel ou alors il faut surprotéger ce matériel. Si le budget est limité, il vaut mieux souvent répartir la charge entre plusieurs petits serveur, plutôt que d'investir dans un seul et ultra puissant ordinateur qui n'est pas exempt d'une panne.
- La redondance va de pair avec la dépendance. Il faut prévoir la redondance du matériel et des données, c'est à dire anticiper les pannes afin que le système et les informations soient toujours accessibles.
- La configuration précise et consciente des multiples paramètres. L'attribution de noms explicites à chacune des ressources du réseau.
- La sécurisation physique (il suffit de redémarrer un système avec une disquette de BOOT pour accéder à toutes les informations qu'il contient) et logique (à l'aide d'une stratégie de mots de passe qui peut résister assez longtemps à une attaque en force (Brute force cracking) qui essaye toutes les combinaisons possibles).
- L'optimisation, le tunning de la configuration (après un temps d'adaptation...), c'est à dire l'adaptation personnalisée de la configuration en fonction des activités particulières des utilisateurs du réseau.
- La standardisation des applications et de l'environnement des utilisateurs.

L'administration du réseau, les méthodes, les références et les outils :

L'information, la formation, la documentation et l'assistance externe :

L'administration, la maintenance et le dépannage sont des tâches complémentaires qui doivent être réservées à un nombre restreint de collaborateurs compétents et honnêtes. Les responsables du réseau doivent participer à toutes les étapes de la vie du réseau afin d'en connaître tous les aspects. Le monde informatique est tellement compliqué et changeant, les informaticiens sont tellement spécialisés et occupés, que seuls des années d'expérience et d'expérimentation peuvent apporter la compétence...

Les responsabilités de l'administrateur sont très importantes et se placent dans la durée et dans le risque. La tâche de l'administrateur et de ses collaborateurs évolue en fonction de son environnement :

- L'évolution des besoins, des contraintes et des risques
- L'évolution de la taille du réseau, du nombre de ses noeuds et de la bande passante
- L'évolution des technologies, des produits et des fonctionnalités
- La réflexion stratégique et organisationnelle

XXIII-7 - Le dépannage à chaud

Le dépannage à chaud survient à n'importe quel moment :

- Un utilisateur appelle l'administrateur
- Une alerte prévient l'utilisateur
- Un bruit de crash offusque soudainement les tympans...

Une approche structurée (méthodologique) est en moyenne bien plus efficace qu'une approche aléatoire :

La dégradation des performances peut provenir d'une mauvaise configuration d'un protocole, en effet, les protocoles sont programmés pour essayer de résoudre eux même un problème de transmission, ce qui engendre plus de trafic que d'habitude... Un jeu en réseau peut être l'origine d'une dégradation des performances du réseau...

Comme un train peut en cacher un autre, un problème peut avoir différentes causes...

Avant tout, il faut savoir distinguer l'origine de la panne. Les câbles sont la première chose que vérifient les spécialistes (d'où l'utilité d'un réflectomètre).

XXIII-8 - Les sources de pannes

Les pannes peuvent provenir de différentes sources :

XXIII-9 - La stratégie de sauvegarde

La stratégie de sauvegarde doit être adaptée :

- Au réseau
- Aux utilisateurs
- Aux données
- Jamais à l'administrateur...

La stratégie de sauvegarde du « grand-père, du père et du fils » n'est pas un dogme mais une façon de faire comme une autre, et qui peut éventuellement en inspirer d'autres.

Le principe est d'organiser la rotation des bandes après avoir effectuer au moins une sauvegarde complète en début de cycle :

La restauration du système ne requière que deux bandes, la dernière sauvegarde complète du dernier vendredi, et la dernière sauvegarde différentielle de la veille.

Il faut systématiquement stocker les bandes d'archivage, les bandes « grands-pères » dans un autre lieu en inscrivant dessus toutes les informations utiles pour leur restauration éventuelles :

- La date
- Le support
- Le logiciel de sauvegarde
- L'opérateur
- La procédure de restauration

XXIV - Les systèmes d'exploitation réseaux

XXIV-1 - Les systèmes d'exploitation

Les systèmes d'exploitation se classent en deux catégories :

- Soit ils sont conçus pour fonctionner sur une machine isolée (comme par exemple, une station cliente), et alors ils sont construit pour offrir les meilleures performances pour l'application qui tourne en premier plan (l'application en cours).
- Soit ils sont conçus pour fonctionner en réseau (comme par exemple un serveur), et alors ils sont construit pour satisfaire toutes les demandes de service qui leur sont adressée en même temps par des clients différents. Leur capacité doit être répartie équitablement selon le nombre d'utilisateurs connectés.

XXIV-2 - Le système d'exploitation et le logiciel réseau

Il y a encore quelque temps, il fallait ajouter un logiciel réseau au système d'exploitation d'un ordinateur afin que celui-ci puisse être connecté à un réseau. Le logiciel réseau et le système d'exploitation devait être compatible, et il y avait en quelque sorte deux systèmes d'exploitation qui fonctionnaient en même temps sur la même machine, l'un pour gérer les ressources internes de l'ordinateur (en mode autonome) et l'autre pour accéder aux ressources externes (en mode réseau).

Unix est le premier né des systèmes d'exploitation réseaux, il a été conçu à la fin des années 1960, sous le nom de Multix (pour multi utilisateurs), dans les laboratoires de la société américaine Bell AT et T. NetWare de Novell (son fondateur Ray Noorda) est le premier système d'exploitation réseau « grand public » (1980). Par exemple, MICROSOFT LAN MANAGER ajoutait des fonctionnalités réseaux à des systèmes d'exploitation comme MS-DOS, UNIX, OS/2. Depuis 1995, les systèmes d'exploitation modernes de Microsoft intègrent les fonctionnalités réseaux.

XXIV-3 - Le rôle du système d'exploitation

Le système d'exploitation est le chef d'orchestre de l'ordinateur. Le système d'exploitation gère l'allocation et l'utilisation de toutes les ressources de l'ordinateur, et coordonne les interactions entre l'utilisateur et les programmes qui sont exécutés sur l'ordinateur :

XXIV-4 - Le système d'exploitation multitâche

Un système d'exploitation multitâche (Multitasking) est un système qui permet d'effectuer plusieurs tâches en même temps. Les tâches sont divisées en petits morceaux (des instructions), et le processeur exécute un petit morceau de chacune des tâches les uns après les autres : un petit morceau d'une certaine tâche, puis un petit morceau d'une autre tâche et ainsi de suite jusqu'à l'exécution de tous les petits morceaux de toutes les tâches.

En fait, un véritable système d'exploitation multitâche peut exécuter simultanément autant de tâches qu'il y a de processeur. Un véritable système d'exploitation multitâche travail en général avec plusieurs processeurs. Mais, quand le nombre de processeur est inférieur au nombre de tâches à exécuter en même temps, alors le système d'exploitation multitâche répartie le temps du ou des processeurs. Les tâches sont traitées à tour de rôle, pendant une durée déterminée par le système d'exploitation. Le traitement multitâche d'un seul processeur donne l'impression que toutes les tâches sont exécutées simultanément, alors qu'elles le sont à tour de rôle (plus le processeur est cadencé à une grande vitesse et plus il donne l'impression d'être « l'homme orchestre » qui joue de

plusieurs instrument en même temps...

XXIV-5 - Les deux modes de fonctionnement multitâche

Il existe deux modes de fonctionnement multitâche :

- Le mode préemptif
- Le mode coopératif (le mode non préemptif)

Avec le multitâche préemptif, le système d'exploitation contrôle « le temps processeur » alloué à chacune des tâches, sans avoir besoin de la coopération de la tâche.

Avec le multitâche coopératif, le système d'exploitation donne à une tâche le contrôle du processeur. C'est la tâche qui décide du moment où elle libère le processeur pour l'exécution d'une autre tâche. Les programmes qui sont conçus pour des systèmes d'exploitation coopératifs doivent contenir des instructions permettant de libérer le processeur, sinon, le programme monopolisera le processeur jusqu'à la fin de la réalisation d'une tâche, et les autres tâches des autres programmes devront attendre que le « squatter » rende la main.

Un système d'exploitation multitâche préemptif permet de suspendre un traitement local et d'allouer le processeur à une tâche réseau.

XXIV-6 - Le rôle du système d'exploitation réseau

Le système d'exploitation réseau est le chef de gare du réseau. Le rôle du système d'exploitation réseau est multiple :

XXIV-7 - Les composants d'un système d'exploitation réseau

Un réseau est composé d'au moins deux ordinateurs, un serveur et un client (dans une organisation de type Client/Serveur). Les deux ordinateurs peuvent être à la fois client et serveur (dans une organisation de type postes à postes). Quoi qu'il en soit, des fonctionnalités réseaux doivent être installées à la fois sur les postes clients et sur les postes serveurs. Le système d'exploitation réseau peut être en quelque sorte divisé en deux parties, la partie pour le client, et la partie pour le serveur. Le « logiciel client » est appelé le « redirecteur » (REDIRECTOR) et permet à un ordinateur d'accéder au réseau. Le « logiciel serveur » est appelé un « service » et permet à un serveur d'accepter les demandes (ou les requêtes) des clients :

Les composants d'un système d'exploitation réseau		
	Le client	Le serveur
Partie du système d'exploitation	Le logiciel client	Le logiciel serveur
Fonctionnalités	L'accès au réseau	Accepte les requêtes des clients
Nom	Le redirecteur	Le service

Le système d'exploitation réseau WINDOWS NT WORKSTATION intègre à la fois le logiciel client et le logiciel serveur. Les ordinateurs qui en sont équipés bénéficient des fonctionnalités réseaux des clients et des serveurs.

XXIV-8 - Le processus d'une requête d'un client vers un serveur

Le processus d'une requête d'un client vers un serveur se décompose en plusieurs étapes :

- L'utilisateur travail en mode autonome sur son ordinateur et exécute une commande pour demander à l'ordinateur d'effectuer une tâche réseau.
- La commande est interceptée par le redirecteur avant d'emprunter le bus local de l'ordinateur pour aller vers le processeur. Le redirecteur interprète cette commande comme une requête réseau et la redirige vers le réseau.
- La requête circule sur le réseau jusqu'au serveur.
- Le service réseau du serveur accepte la requête du client, la traite et renvoi la réponse sur le réseau.
- La réponse du serveur circule sur le réseau jusqu'au client.
- L'ordinateur client reçoit la réponse et la transmet au bus local pour l'afficher sur le moniteur.
- L'utilisateur médite la réponse du serveur...

XXIV-9 - Le redirecteur

Le redirecteur (REDIRECTOR) redirige les requêtes réseaux vers le réseau. Selon le système d'exploitation réseau, le redirecteur est appelé par d'autres noms :

- L'interpréteur de commande (SHELL)
- Le requêteur (REQUESTER)

Le redirecteur intercepte les commandes effectuées par l'utilisateur et détermine si elles sont locales ou réseau. Quand une commande est une requête réseau, le redirecteur la redirige vers le réseau.

Le redirecteur doit connaître les désignations associées aux ressources du réseau. Par exemple, avec WINDOWS NT, un répertoire partagé sur un serveur est identifié chez le client par une lettre de l'alphabet. La lettre est attribuée par le gestionnaire de fichier quand le client y accède pour la première fois, et la lettre figure dans l'arborescence du client jusqu'à ce que celui-ci décide d'interrompre l'association entre ce disque virtuel et la ressource partagée. Lors de l'ouverture d'une session réseau, le gestionnaire de fichier vérifie les associations réseaux qui sont en cours.

Le redirecteur peut envoyer une requête à un périphérique réseau. Par exemple, si le port LPT1 est associé à une imprimante réseau, alors, le redirecteur intercepte les commandes d'impression et les redirige vers le périphérique d'impression réseau.

Ainsi, le redirecteur permet aux utilisateurs de ne pas s'occuper de l'emplacement des ressources du réseau (que se soient un fichier, un répertoire ou un périphérique).

XXIV-10 - Les systèmes d'exploitation réseaux pour les machines INTEL

Il existe plusieurs types de processeurs. Chaque type de processeur caractérise la carte mère sur lequel il est ou ils sont installés, et par voie de conséquence caractérise l'unité centrale (la machine ou l'ordinateur) construite autour de cette carte mère. On dit qu'il existe plusieurs types de plates-formes...

Les machines INTEL sont équipées de processeur INTEL et de nombreux systèmes d'exploitation sont compatibles avec leur architecture parce qu'elle représente la partie la plus importante du marché de l'ordinateur

dans le monde.

XXIV-11 - Les systèmes d'exploitation réseaux

Il existe plusieurs éditeurs de systèmes d'exploitation réseaux (NOS pour Network Operating system en anglais) :

En général, les systèmes d'exploitation réseaux peuvent fonctionner dans les deux types d'organisation, le réseau égal à égal (Peer To Peer), et/ou le réseau client-serveur.

XXIV-11.1 - Le système d'exploitation réseau UNIX

Unix est le premier né des systèmes d'exploitation réseaux, il a été conçu à la fin des années 1960, sous le nom de Multix (pour multi utilisateurs), dans les laboratoires de la société américaine Bell AT et T. Multix était lent, lourd et aussi technocratique que le cahier des charges dont il était issu, aussi les programmeurs de Bell AT et T entreprirent de construire un autre système d'exploitation, rapide, léger et extensible (les utilisateurs étaient encouragés à modifier le système en fonction de leurs besoins), qu'ils nommèrent UNIX par dérision. L'avantage d'UNIX était qu'il pouvait fonctionner sur des petits ordinateurs (moins puissants et moins coûteux que les VM d'IBM et les VMS de DIGITAL), c'est pourquoi il fut adopté par les universités (Bell AT et T diffusa des copies très bon marché d'UNIX aux universités).

Au début des années 1970, UNIX fut entièrement réécrit en langage C qui est un langage de programmation « portable » sur différentes machines. Le langage C a été élaboré dans les laboratoires de Bell AT et T par Brian kernighan et Denis Ritchie. Les distributions d'UNIX incluaient le code source du système d'exploitation, lequel pouvait être recompilé en fonction de la machine sur lequel il était installé. La compilation du code source consiste à traduire le code source (le programme écrit en langage C), en langage machine. Il existe des compilateurs C pour les PC Intel, pour les Macintosh, etc...

Au milieu des années 1970, Ken Thompson et Bill Joy de l'université de Berkeley en Californie écrivirent un éditeur de programme ou éditeur de texte appelé « vi », et ils créèrent le premier système d'exploitation UNIX en 1978 qui n'était issu des laboratoires de Bell AT et T. Ils baptisèrent leur nouvel UNIX de l'acronyme BSD (Berkeley Software Distribution). Aujourd'hui, toutes les versions d'UNIX et de LINUX proviennent d'une de ces deux sources, l'UNIX de Bell AT et T ou l'UNIX BSD. Avec le temps, les distributions provenant de ces deux sources se différencièrent de plus en plus (au niveau de la syntaxe), puis se rapprochèrent, tant et si bien qu'il est difficile, de nos jours, de les distinguer.

Toutefois, les versions d'UNIX vendues par des éditeurs privés différents ne sont pas forcément « compatibles binairement » entre elles (c'est à dire que les applications qui tournent sur une des versions d'UNIX peut ne pas tourner correctement sur une autre version du système d'exploitation). L'arrivée de Windows NT contribua à diminuer les revenus des différents éditeurs UNIX, et provoqua une standardisation des différentes versions d'UNIX.

Au début des années 1990, la société Bell AT et T décida de ne plus participer au commerce des logiciels UNIX, et vendit la marque déposée et les droits de licence à la société Novell. Le président de Novell, Ray Noorda, acheta d'autres logiciels, comme WordPerfect et Quattro Pro à la société Bordland, mais il fut remercié. Son successeur à la tête de Novell, Robert Frankenberg, revendit les applications bureautiques à la société Corel, et UNIX à la société Santa Cruz Operation (SCO). En 1997, Microsoft a vendu plus de Windows NT dans le monde, qu'il n'existe d'UNIX...

UNIX existe depuis plus de 30 ans (1970) et possède des qualités de stabilité, de robustesse et une richesse fonctionnelle unique au monde. UNIX est un logiciel qui a évolué et qui a été testé par des générations d'informaticiens. UNIX est un système d'exploitation « autosuffisant », c'est à dire qu'il n'a pas besoin de logiciels extérieurs (produits dits de tierce partie) pour l'administrer. UNIX est un système performant, extensible, mais relativement complexe. Unix est un logiciel ouvert.

UNIX n'est plus uniquement disponible avec la ligne de commande et dispose d'une interface graphique appelée « X Window » et de gestionnaire de fenêtres (comme MOTIF, Open Look, CDE,... qui gèrent les fenêtres comme le fait les environnements de Microsoft ou d'Apple).

Plusieurs éditeurs en commercialisent des versions plus ou moins différentes :

- SOLARIS de la société Sun Microsystems.
- UNIX SCO puis UNIXWARE de la société Santa Cruz Operation
- AIX de la société IBM
- ULTRIX de la société DEC
- HP-UX de la société Hewlett Packard

Ainsi, les applications UNIX d'un éditeur ne sont pas forcément compatibles avec celle d'un autre éditeur. La « comptabilité binaire » n'est pas systématique, c'est à dire que la compilation d'une application ne fonctionne pas sous toutes les versions des différents éditeurs. Il n'existe pas de véritable standard d'UNIX, et le meilleur système d'exploitation au monde reste accessible uniquement sous des versions propriétaires, d'ailleurs, les éditeurs d'UNIX sont également des constructeurs, ils vendent leurs systèmes avec leurs machines (équipées de leurs processeurs). Cette absence d'unité, de standard et de compatibilité contribue à donner une image d'un système abscons réservé aux professionnels (ce qui est en définitive le cas...). LINUX à contrario est un logiciel libre et donne une image plus démocratique du système d'exploitation.

En fait, UNIX est "Multi". Le système d'exploitation UNIX est constitué d'un ensemble de modules (chaque module est un programme spécialisé, indépendant des autres, mais compatibles avec les autres). Les différents modules qui sont sélectionnés par l'administrateur lors de l'installation du système d'exploitation sont compilés pour former le noyau du système. Ainsi chaque noyau est différent d'un autre, et chaque système UNIX peut être spécialisé et optimisé pour la réalisation d'une tâche très précise.

UNIX est système d'exploitation multi tâches préemptif, c'est à dire qu'il est capable de traiter les processus de différents programmes en même temps (dans un espace mémoire réservé qui protège chaque programme de ces congénères).

UNIX est système d'exploitation multi fonctions, c'est à dire qu'il peut servir à réaliser presque toutes les tâches dévolues au monde binaire. Il peut fonctionner aussi bien en tant que serveur (c'est généralement pourquoi il est adopté) qu'en tant que client, et peut être implémenter à n'importe quel niveau de l'entreprise. Les serveurs UNIX peuvent traiter les requêtes de nombreux « terminaux passifs » (comme les « terminaux VT100 » de Digital qui sont reliés au serveur central par l'intermédiaire d'un port série, ou comme les « terminaux X » qui utilisent l'interface graphique de X Window et qui sont connectés au serveur central par l'intermédiaire d'une connexion réseau), à l'aide de petits programmes (dont les dernières lettres sont « tty » pour Terminal Type) qui affiche les résultats sur l'écran du terminal. UNIX peut prendre en charge, aussi bien les « systèmes transactionnels », que les « architectures distribuées ».

UNIX est un système d'exploitation multi plate formes, c'est à dire qu'il est disponible pratiquement sur toutes les plates formes matérielles.

UNIX est un système d'exploitation multi processeurs, c'est à dire qu'il peut fonctionner avec plusieurs processeurs en même temps, lesquels se répartissent en temps réel la charge de travail.

UNIX est un système d'exploitation multi protocoles, c'est à dire qu'il peut véhiculer les communications réseaux avec de nombreux protocoles différents. UNI supporte le protocole SPX/IPX pour interagir avec les réseaux NetWare, ou le protocole SMB pour interagir avec les réseaux Windows NT. Toutefois, le protocole TCP/IP, qui permet d'interagir avec Internet, a été créé en même temps qu'UNIX et pour UNIX. TCP/IP est le protocole naturel d'UNIX, TCP/IP est intégré « nativement » à UNIX.

UNIX est un système d'exploitation multi utilisateurs, c'est à dire que de nombreux utilisateurs peuvent se connecter simultanément à un serveur UNIX.

UNIX est compatible avec plusieurs systèmes de fichiers distants :

- NFS (Network File System) de SUN qui permet de « monter » des disques UNIX sur un ordinateur distant de type PC.
- AFS (Andrew File system)
- DFS (Distributed File System)
- SAMBA est un programme freeware qui permet à un système UNIX de partager ses ressources comme le ferait un système Windows avec SMB.

Les langages de script permettent de réaliser des tâches très complexes, grâce à un commutateur (« | ») appelé « pipe » en anglais ou « tube » en français qui transmet des données d'un programme à un autre. Les « scripts shell » d'UNIX correspondent aux fichiers « batch » du DOS de Microsoft.

Unix dispose d'une panoplie de langages de scripts :

- PERL (Pratical Extraction and Reporting Language) qui permet de récupérer les données saisies dans une page Web.
- TCL/TK
- Les scripts SHELL

UNIX organise ses ressources hiérarchiquement (avec le slash (« / ») penché à droite, et non pas avec l'anti-slash (« \ ») qui est utilisé sur les systèmes de Microsoft). Chaque répertoire peut avoir des restrictions d'accès particulières. UNIX supporte les espaces disques très volumineux (en Tera Octets), les noms longs de fichiers jusqu'à 32 caractères et garantie l'unicité des noms de fichier. UNIX est sensible à la casse, c'est à dire qu'il fait la différence entre les caractères minuscules et les caractères majuscules.

La hiérarchie des ressources d'un système UNIX :

- / est la racine, le départ ou le sommet de la hiérarchie qui n'est accessible que par l'utilisateur « root » (l'administrateur, le super utilisateur).

- /dev est le répertoire réservé aux matériels (device en anglais) :
- /dev/fd0 pour le lecteur de disquettes
- /dev/modem pour le modem
- /dev/tty0 et dev/tty1 pour les ports séries
- /bin est le répertoire réservé aux exécutables binaires (binary en anglais) :
- /bin/sh pour les variables d'environnement des utilisateurs.
- /etc est le répertoire des fichiers de configuration :
- /etc/password pour les mots de passe cryptés
- /pub est le répertoire public

Les stations graphiques hauts de gamme de Silicon Graphics (machine INDY) qui produisent les effets spéciaux de l'industrie cinématographique tournent sous UNIX.

XXIV-11.2 - Le système d'exploitation réseau NetWare

NetWare de Novell (son fondateur Ray Noorda) est le premier système d'exploitation réseau « grand public » (1980). NetWare a été optimisé pour l'accès aux fichiers et à l'imprimante. Netware est plus rapide que Windows NT, mais il est plus difficile à installer et à maintenir. NetWare est un système rapide, fiable, efficace et stable.

NetWare utilise un système de fichiers propriétaire NWFS (NetWare Files system) et un protocole routable propriétaire SPX/IPX (les versions récentes peuvent traduire le protocole IPX en IP ou encapsuler les paquets IPX dans une couche IP). NetWare peut inter opérer avec la plus part des autres systèmes d'exploitation. NetWare est capable de transmettre au câble différentes sortes de trames, le trames Ethernet 802.2 et Ethernet 802.3. NetWare est un système multi sites avec son service d'annuaire NDS (NetWare Directory Services).

NetWare 3 était simple et performant, mais chaque serveur devait être administré séparément.

NetWare 4 est un produit complexe, aride et difficile (sa console est en mode texte), mais qui n'a pas été conçu pour s'ouvrir sur Internet (Le protocole SPX/IPX était propriétaire et incompatible avec TCP/IP parce qu'à l'époque le protocole d'Internet était immature et complexe à paramétrer). NetWare est un système multi tâches en mode protégé. NetWare 4 introduit le service d'annuaire NDS qui permet de conserver la trace de toutes les ressources du réseau. NetWare 4 permet de dupliquer les données en temps réel.

NetWare s'appelle de nos jours « IntranetWare ». Les outils Netadmin pour le DOS et Nwadmin pour Windows permettent une administration avec une interface graphique.

Le système d'exploitation a souffert de sa précocité en développant son propre protocole réseau et NetWare ne s'est adapté à l'Internet que très tardivement ; il a souffert de la concurrence marketing de Microsoft et de son produit Windows NT ; enfin, Netware a souffert de sa politique d'assistance basée sur des ingénieurs certifiés Novell (les fameux CNE pour Certified Novell Engineers) très compétent mais trop cher pour les petites entreprises. D'autre part, NetWare est vendu avec toutes les licences utilisateurs, ce qui revient cher au départ, mais avantageux quand on rajoute des poste au réseau puisqu'il n'y a plus besoin d'acheter de nouvelles licences pour les nouveaux utilisateurs. A la différence de Windows NT Server qui est moins cher (pour l'achat du système d'exploitation pour le serveur), mais avec lequel il faut acheter des licences pour chaque poste client supplémentaires (ou acheter directement une licence pour le site de l'entreprise).

Les nouvelles versions de NetWare peuvent traduire SPX/IPX en TCP/IP pour se connecter à Internet.

Cependant, Netware 4 présente les meilleurs performances pour certains services :

- Les serveurs de fichiers et d'imprimante
- Le partage de fichier et d'imprimante
- Les services de répertoire d'annuaire (NDS) qui permettent l'administration d'un nombre important d'utilisateur et de ressources sur différents sites. Cette fonctionnalité propre à NetWare ne le sera plus avec la version Windows 2000 (Windows NT 5.0) et ACTIVE DIRECTORY.

NetWare supporte les grandes partitions, les noms long de fichiers avec de nombreux attributs de fichier. NetWare conserve en mémoire une liste de tous les fichiers stockés sur le disque afin d'y accéder plus rapidement.

XXIV-11.3 - Le système d'exploitation réseau Windows NT

Windows NT de Microsoft est certainement le système d'exploitation le plus répandu. Dès le début, la connectivité de Windows NT a été conçue de manière très large pour s'intégrer avec la plus part des autres systèmes (Netware, MACINTOSH, les mini ordinateurs AS/400 d'IBM, les Main Frame...) et pour s'ouvrir sur Internet avec TCP/IP comme protocole par défaut. De plus, Windows NT avait l'avantage de s'administrer dans une interface graphique (plus conviviale qu'une ligne de commande) et de partager le même environnement que les autres systèmes d'exploitation grand public de Microsoft.

Le système d'exploitation Windows NT était moins rapide et moins stable que ses concurrents (UNIX, NetWare, OS/2,...), mais plus facile à installer et à administrer !

Les fonctions réseaux de Windows NT reposent sur les RPC (Remote Procedure Call) qui permettent à plusieurs ordinateurs de fonctionner ensemble.

La première version date des années 1980 avec Windows NT 3.11 qui était le même produit pour les serveur et pour les stations. Le produit s'appelait NTAS (NT Advanced Server) et fut rebaptisé Windows NT Server.

Longtemps après, la nouvelle version en 1993, Windows NT 3.5 présentait deux versions différentes, l'une pour les serveurs et l'autre pour les stations. Seul, la version Windows NT Server possédait les utilitaires réseaux indispensables pour son administration. Sinon, certaines personnes disaient volontiers que la seule différence entre les deux versions étaient deux clefs de la base de registre. Windows NT Workstation a une limite légale de 10 connexions simultanées. Windows NT Server ne fonctionne pas en mode égal à égal, mais seulement dans le cadre d'une organisation centralisée du type Clients Serveurs pour laquelle il est conçu (« works as designed », cela fonctionne pour ce pourquoi c'est conçu, et pas pour autre chose, touchez avec les yeux et passez à la caisse en sortant merci...).

Windows NT 4.0 est un véritable système d'exploitation multi tâches et multi threads qui présente la même interface graphique que le populaire Windows 95.

Windows 2000 (Windows NT 5.0) inclus « Active Directory » qui est service d'annuaire qui manquait (et qui faisait l'avantage comparé de NetWare).

Windows NT Server fut construit à partir d'une feuille blanche. Le système dispose ainsi de beaucoup d'option, comme par exemple trois systèmes de fichier compatibles :

- FAT (File Allocation Table) ou FAT 16 est l'héritage de MS-DOS et impose la règle de nomage des 8.3
- HPFS (High Performance File System) est le système de fichier d'OS/2 d'IBM, présent dans la version Windows NT 3.5, il a été retiré dans la version Windows NT 4.0.
- NTFS (NT File system) est le système de fichier propre à Windows NT, et supporte les noms long de fichiers (jusqu'à 254 caractères).

Tous les systèmes d'exploitation de Microsoft fonctionnent (étonnant non ?) avec SMB (Server Message Block) qui est un protocole permettant d'utiliser des ressources distantes. SMB fait partie de la structure de NetBEUI le dernier-né des protocoles NetBIOS. SMB est le protocole fondamental de Windows NT au même titre que NCP (NetWare Core Protocole) est le coeur de NetWare.

Windows NT Server fonctionne (toujours d'accord ?) autour de la notion de « domaine » (à ne pas confondre avec les domaines DNS d'Internet, comme les sept Top Level Domain (TLD)que sont « .com », « .mil », « .gov », etc...), c'est à dire un groupe d'ordinateur qui appartiennent à la même entité logique (cela dépend du point de vue non ?). Dans un domaine, un ordinateur central, appelé Contrôleur Principal de Domaine (CPD) authentifie toutes les connexions au domaine (au réseau). Un réseau peut être constitué de plusieurs domaines qui peuvent, deux à deux, éventuellement entretenir des relations d'approbation (qui ne sont pas transitives et qui ne sont pas implicites). L'organisation des domaines peut suivre plusieurs structures :

- Le domaine unique
- Le domaine maître
- Le domaine à maître multiples
- Les domaines à relation d'approbation multiples

Le modèle d'approbation de domaine n'est pas aussi extensible que les autre modèles du marché. C'est pourquoi, Windows 2000 apporte cette fonctionnalité avec Active Directory :

- Le modèle d'annuaire NDS de NetWare. Le standard ouvert LDPA (Lightweight Directory Access Protocol) qui fait partie de la pile de protocole TCP/IP.
- NFS (Network File System) de SUN MICROSYSTEM. NFS est le standard pour monter des disques distants.

Les ordinateurs clients à l'intérieur d'un domaine (qui sont en théorie limités à 40 000) peuvent provenir de plusieurs éditeurs :

- Windows for Workgroups
- Windows 95 et 98
- Windows NT Station
- Les clients NetWare
- Les clients Macintosh
- Les clients UNIX

Les comptes utilisateurs peuvent être placés dans des groupes locaux ou globaux. Les permissions d'accès à une ressource sont gérées plus finement avec Windows NT Server (au niveau du fichier avec NTFS, et non pas seulement au niveau du répertoire comme avec les autres systèmes Windows en FAT 16 et FAT 32). Les

permissions sont aussi plus nombreuses :

- Aucun accès
- Lire
- Modifier
- Contrôle total
- Accès selon le mot de passe

Seul l'administrateur réseau peut enlever la permission « aucun accès ». Le partage d'une ressource peut éventuellement spécifier le nombre maximal d'accès simultanés.

Windows NT Server dispose d'un ensemble d'outils livrés d'office :

- Les outils TCP/IP pour l'administration réseau.
- Le serveur DNS pour les noms de domaine.
- Le serveur DHCP pour les adresse IP dynamiques.
- Le serveur RAS pour les connexion distantes avec le protocole PPP.

Windows NT Server peut être accompagné de la suite de logiciels, appelée « Back Office », qu'a développé Microsoft :

- Exchange Server qui gère la messagerie internes.
- SQL Server qui gère les base de données.
- SMS qui rassemble plusieurs logiciels et qui permet de centraliser l'administration du réseau.
- SNA Server qui gère les connexions à des mini ordinateurs ou à des main frames IBM.
- IIS qui peut servir de serveur Internet pour les services web, Gopher, FTP,...

XXIV-11.4 - Le système d'exploitation réseau OS/2

A la fin des années 1980, le système d'exploitation réseau OS/2 a été développé en partenariat par IBM et Microsoft. Puisqu'il s'agissait du deuxième système d'exploitation d'IBM, il a été appelé OS/2 (Operation System 2). Au début des années 1990, Microsoft s'est séparé d'IBM pour créer son propre système d'exploitation multi tâches 32 bits, qui est devenu Windows NT. IBM a continué seul le développement d'OS/2 avec une version réseau appelée OS/2 WARP Connect, et dont le successeur s'appela MERLIN (OS/2 4.0).

Le système d'exploitation réseau MERLIN dispose de fonctionnalités qui n'existe pas chez les autres systèmes d'exploitation :

- Les connexions différenciées ou l'utilisation de plusieurs logins en même temps, c'est à dire qu'il est possible d'ouvrir plusieurs session complètement séparées les unes des autres sur le même ordinateur.

OS/2 est un système intéressant qui peut interagir avec bon nombre d'autres systèmes d'exploitation, mais il souffre d'un manque d'applications. Les éditeurs ont préféré se concentrer sur le leader du marché des systèmes d'exploitation (Windows) pour développer des logiciels compatibles avec cette plate forme.

XXV - La stratégie de sécurité

XXV-1 - Les sept règles d'or de la sécurité

- Leurrer
- Séparer
- Copier
- Cacher
- Blinder
- Surveiller
- Filtrer

XXV-2 - L'objectif de la stratégie de sécurité

La stratégie de sécurité d'un réseau dépend de la « sensibilité » des données qui circulent sur le réseau et qui sont transformées par les utilisateurs.

La stratégie de sécurité d'un réseau doit se situer à trois niveaux :

- L'intégrité des données
- La conformité des opérations effectuées sur le réseau
- La régularité du fonctionnement des équipements

Les réseaux centralisés autour de serveurs offrent une bien meilleure sécurité que les réseaux postes à postes. Les données sensibles sont plus protégées quand elles sont stockées sur un seul serveur de fichiers.

XXV-3 - L'environnement de la stratégie de sécurité

La stratégie de sécurité d'un réseau doit prendre en compte l'environnement du réseau dans son ensemble :

La sécurité d'un réseau est bien mieux assurée si le réseau est organisé en Clients Serveurs avec une authentification et une administration centralisée.

XXV-4 - Les failles potentielles d'un réseau

Les failles potentielles d'un réseau sont nombreuses :

XXV-5 - La stratégie de sécurité

Il peut être plus coûteux pour une entreprise de faire face à un problème de sécurité que de se prémunir, tant faire ce peut, des facteurs susceptibles de déclencher un tel problème. Les moyens mis à la disposition d'un administrateur réseau pour protéger son environnement informatique sont de trois ordres :

La répression... (après)

Nous ne parlerons pas de « l'ordre répressif », mais les différentes méthodes de sécurisation d'un réseau ne sont pas exclusives les unes des autres, bien au contraire. La sauvegarde est considérée comme la première ligne de défense ; le contrôle des utilisateurs (la stratégie des mots de passe et des permissions) est considéré comme l'étape suivante...

La stratégie de sécurité préventive concerne toutes les actions ou toutes les méthodes qui essayent d'anticiper la survenue d'un problème. La stratégie de sécurité préventive, bien qu'elle puisse évoluer dans le temps, est mise en place à un certain moment. A un moment donné, la solution à un problème éventuel est apportée ou pas !

La stratégie de sécurité préventive implique la définition de procédures strictes et contrôlées. Les différentes solutions d'une stratégie de sécurité préventive s'appliquent aux utilisateurs, aux données et aux matériels. Le contrôle des données permet de préserver les données sensibles, d'assurer la continuité du fonctionnement du réseau, et de consolider la confidentialité des données.

XXV-6 - Le contrôle des utilisateurs

Le contrôle des utilisateurs permet de filtrer les connexions et de réglementer l'activité et l'environnement des utilisateurs :

Outre le contrôle des connexions et des permissions, il existe des logiciels de configuration qui permettent de gérer à partir d'une console centrale la configuration logicielle et l'interface utilisateur d'un ensemble d'ordinateurs.

XXV-6.1 - Le contrôle des utilisateurs : les deux modèles de sécurité

Il existe deux modèles de sécurité différents, selon l'attribution du mot de passe :

- L'accès à une ressource partagées. Les utilisateurs connectés au réseau doivent fournir un certain mot de passe quand il essayent d'accéder à une ressource. Ce modèle de sécurité s'appèle « le partage protégés par mot de passe ». C'est la sécurité au niveau partage.
- L'accès de l'utilisateur au réseau. Les utilisateurs s'authentifient auprès d'une base de données des comptes utilisateurs quand il essayent de rentrer dans le réseau (lors de l'ouverture d'une session réseau). Pendant l'établissement de la connexion d'un utilisateur, le système contrôle ses droits, ses permissions et ses appartenances à des groupes. Ce modèle de sécurité s'appèle « les permissions d'accès » ; C'est la sécurité au niveau utilisateur.

Les utilisateurs communiquent facilement le mot de passe associé à une ressource, mais en général ont plus de réticence à divulguer leur propre mot de passe (qui les identifie sur le réseau). C'est pourquoi, le modèle de sécurité au niveau des utilisateurs est plus fiable. Par ailleurs, le modèle de sécurité au niveau des utilisateurs reconnaît plus de niveaux différents de permissions, ce qui en fait un modèle plus sophistiqué.

Toutefois, la plupart des réseaux sont à même d'employer les deux modèles de sécurité en même temps.

XXV-6.2 - Le contrôle des utilisateurs : le modèle de sécurité au niveau des ressources

Dans le modèle du partage protégé par le mot de passe, une ressource peut être partagée de différentes façon :

- La ressource est partagée en « lecture seule ». L'utilisateur qui possède le mot de passe de la ressource peut accéder à la ressource, Il peut télécharger le fichier sur son poste, mais il ne peut pas modifier le fichier original.
- La ressource est partagée en « accès complet ». L'utilisateur qui possède le mot de passe de la ressource a le contrôle total sur celle-ci, il peut lire, modifier ou supprimer le fichier original.
- La ressource est partagée plusieurs fois à des niveaux différents. Certain utilisateur possède le mot de passe de la ressource associé à une lecture seule, tandis que d'autres utilisateurs possède le mot de passe de la ressource (différent du précédent bien sûr) associé à un contrôle total.

XXV-6.3 - Le contrôle des utilisateurs : le modèle de sécurité au niveau des utilisateurs

Lors de la connexion d'un utilisateur au réseau, une procédure d'authentification vérifie le nom de l'utilisateur (le login) et son mot de passe (password) ; soit le contrôleur de domaine valide la connexion, et alors l'utilisateur peut accéder à toutes les ressources dont il possède les permissions (directement ou par l'intermédiaire de l'appartenance à un groupe), soit la connexion est refusée, et l'utilisateur est rejeté du réseau. Le nom de l'utilisateur et son mot de passe sont enregistrés dans « une base de données de sécurité » dans laquelle se trouve associés ses droits, ses permissions, et ses appartenances à des groupes. La base de données de sécurité contient également la liste des ressources qui sont partagées sur le réseau. A chaque fois que l'utilisateur souhaite accéder à une ressource, le serveur sur lequel se situe la ressource demande à un contrôleur de domaine de vérifier dans la base de données de sécurité s'il possède les permissions adéquates. Si l'utilisateur possède la permission, alors le serveur valide l'accès à la ressource.

Les niveaux de partages sont plus sophistiqués dans le modèle de sécurité au niveau des utilisateurs :

- Aucun accès
- Lire (Read)
- Exécuter (eXecute)
- Modifier (Write)
- Supprimer
- Contrôle total (RXW)

Les différentes permissions d'accès à une ressource peuvent être associées à un compte utilisateur ou à un groupe. Les utilisateurs qui appartiennent au groupe possède par transitivité les permissions du groupe.

Dans WINDOWS NT SERVER l'octroie d'une permission à une ressource s'effectue en deux temps :

XXV-6.4 - Le contrôle des utilisateurs : les logiciels de configuration

Les logiciels de gestion des configurations sont des logiciels qui permettent de gérer à partir d'une console centrale la configuration logicielle et l'interface utilisateur des ordinateurs. Les logiciels de gestion de configuration requièrent l'installation sur chacun des ordinateurs d'un « agent de configuration » qui interagit avec la base de données de la console centrale.

Les logiciels de configuration peuvent inventorier un réseau très rapidement, installer ou mettre à jour une application simultanément sur un ensemble de station de travail. Ils peuvent mettre en place des alarmes qui enregistrent les actions non autorisées sur telle ou telle station (comme le changement de matériel ou l'installation illicite de logiciel,...).

XXV-7 - Le contrôle des données

XXV-7.1 - Le contrôle des données : les sauvegardes sur bandes

Les sauvegardes sur bandes permettent de préserver les données sensibles.

Les sauvegardes sur bandes (ou tout autre support de stockage à grande capacité...) est le moyen le moins onéreux, mais il implique une astreinte rigoureuse, un calendrier stricte et un lieu sûr pour le stockage des bandes, et surtout des tests de restauration et d'utilisation des données après une sauvegarde.

L'administrateur doit tenir compte de plusieurs facteurs avant de choisir un système de sauvegarde :

Il existe différents types d'unité de bandes :

- Les bandes numériques audio de 4 mm ou DAT (Digital Tape Audio) qui peuvent stocker plus de 8 Giga Octets
- Les bandes numériques linéaires ou DLT (Digital Linear Tape) qui peuvent stocker entre 20 Go et 40 Go
- Les bandes intelligentes ou AIT (advanced intelligent Tape) qui peuvent stocker plus de 50 Go.

La plupart des unités de bandes ne gèrent qu'une seule bande à la fois ; c'est pourquoi, il existe des « changeurs de bandes » qui peuvent gérer des bibliothèques de plusieurs milliers de bandes.

XXV-7.2 - Le contrôle des données : les systèmes à tolérance de pannes

Les systèmes de tolérances de panne (Fault tolerance) permettent d'assurer la continuité du fonctionnement du réseau. Si l'entreprise ne peut pas se permettre d'arrêter le réseau, ni le travail de ses employés, alors un système RAID compensera cette faiblesse. Les systèmes RAID ne remplacent pas une sauvegarde, mais apporte un complément à la stratégie de sécurité.

Les systèmes RAID fonctionnent avec un contrôleur RAID (un contrôleur SCSI spécial sur la carte mère ou sur une carte d'extension), et avec des disques SCSI. De nombreux contrôleur RAID fonctionne « en mode temps réel », c'est à dire qu'il est possible d'extraire et de remplacer l'un des disques pendant leur exploitation ; cette fonctionnalité s'appèle « l'échange à chaud » (le hot swapping), le contrôleur RAID recopie automatiquement les données sur le nouveau disque. Les serveurs RAID sont généralement installés dans de grosses tours, avec des portes verrouillées pour les baies des disques RAID. Le matériel RAID coûte cher et il est préférable de faire appèle à des constructeurs haut de gamme (Digital, HP, Compaq, IBM, Dell,...) afin de pouvoir éventuellement bénéficier de leur expérience en cas de problème.

Les données sont enregistrées en temps réel sur plusieurs emplacements (plusieurs partitions ou plusieurs disques physiques). Un agrégat par bandes est constitué de plusieurs partitions qui peuvent être situées sur plusieurs disques différents. L'agrégat par bande rassemble plusieurs portions non formatées de disque en une seule et grande unité logique. Quand il y a plusieurs disques physiques, et s'il y a plusieurs contrôleurs de disque, les enregistrements sont plus rapides qu'avec un seul contrôleur.

La copie des données sur un autre disque ou la répartition des données sur plusieurs disques avec un contrôle de parité aboutit à une redondance des données. Les données sont tout de suite accessibles ou peuvent être reconstituées très rapidement. En raison de cette « redondance », les données sont toujours accessibles, même après la défaillance d'un des supports de stockage (mais que faire si plusieurs disques tombent en panne simultanément ?). La redondance est souvent implémentée en ajoutant un deuxième matériel (un deuxième disque, une deuxième carte réseau, un deuxième serveur qui reste en « stand-by » près pour le remplacement, parfois une deuxième carte mère...). Toutefois, la redondance matérielle exige un certain temps pour basculer d'un appareil à l'autre.

Le contrôle de la parité correspond à l'ajout d'un bit dans les données. Le bit de parité est calculé en fonction de la somme des valeurs (pair ou impair, 1 ou 0) d'un groupe de bits. La valeur du bit de parité est déterminée de telle façon que la somme des bits soit toujours égale à un nombre pair ou impair (au choix). Le contrôle de la parité permet de reconstituer les données, comme le code de correction d'erreur (ECC), c'est donc un facteur de tolérance de panne.

La tolérance de panne ne doit pas remplacer la sauvegarde régulière !

XXV-7.3 - Le tableau des caractéristiques RAID

Le système RAID (Redundant Array of Inexpensive Disk) classe les agrégats en différentes catégories, mais toutes les catégories n'offre pas la tolérance de panne :

- RAID 0 : L'agrégat par bandes sans parité (Disk Stripping). Les données sont découpées en block de 64 Kilo Octets, et réparties sur tous les disques constituant l'agrégat. Cette méthode permet d'accroître le débit (en lecture et en écriture) et d'optimiser l'espace disponible sur plusieurs disques. Mais, il n'y a pas de tolérance de panne, si un disque tombe en panne, certaines données seront inexorablement perdues.
- RAID 1 : Le miroir de disque (Disk Mirroring). Les données sont dupliquées sur un autre disque physique. Les disques SCSI doivent être de même taille et connectés au même contrôleur RAID. C'est le contrôleur RAID qui gère la duplication des données sur les deux disques. Le miroitage ressemble à une sauvegarde en continue, c'est pourquoi, c'est un système de tolérance de panne assez lent.
- La duplication de disque (Duplexing) est un miroitage de disque où le deuxième disque dispose de son propre contrôleur RAID.
- RAID 2 : L'agrégat par bandes avec code de correction d'erreurs. Les données sont réparties (entrelacées) sur tous les disques de l'agrégat. Le code ECC prend plus d'espace que le contrôle de parité, ce qui en fait une méthode moins efficace que le RAID 5.
- RAID 3 : L'agrégat par bandes avec contrôle de parité. Les données proprement dites utilisent 85% de l'espace de l'agrégat.
- RAID 4 : L'agrégat par bandes avec grands blocs (Agrégat de volume). Les données ne sont plus répartie au fur sur tous les disques de l'agrégat. Il n'y a pas d'entrelacement des données. L'écriture des block de données s'effectue en séquence sur la totalité du premier disque, puis sur le deuxième et ainsi de suite ; les données de parité sont écrites sur un disque séparé.
- RAID 5 : L'agrégat par bande avec parité. C'est la méthode la plus utilisée et la plus rapide. Les données et les données de parité sont réparties sur tous les disques de l'agrégat (stripping), mais les données proprement dîtes et les données de parité associés ne se trouvent jamais sur le même disque. Il y a un bloc de données de parité pour chaque bande de l'agrégat. Il y a tolérance de panne puisque si l'un des disques (mais un seul) tombe en panne, alors, les informations peuvent être reconstituées. La vitesse d'accès aux données est plus rapide puisque les données sont lues sur trois disques en même temps.
- RAID 10 : L'agrégat en miroir. Il y a deux agrégats identiques de type RAID 0. C'est un miroir d'agrégat.

Les caractéristiques des systèmes RAID							
RAID	0	1	2	3	4	5	10

Les caractéristiques des systèmes RAID							
Nombre de disques	0 à 32	1	1 à 32	1 à 32	1 à 32	3 à 32	0 à 32
Tolérance de panne	NON	OUI	OUI	OUI	OUI	OUI	OUI
Entrelacement	OUI	NON	OUI	OUI	NON	OUI	NON
Calcul de parité	NON	NON	ECC	OUI	OUI	OUI	
Parité répartie					NON	OUI	

XXV-7.4 - La tolérance de panne avec WINDOWS NT SERVER

Les solutions RAID de WINDOWS NT SERVER sont des solutions logiciels.

Seuls les RAID 0, 1 et 5 sont compatibles avec WINDOWS NT SERVER.

Sous WINDOWS NT SERVER, un agrégat par bande exige au moins deux disques physiques, et peut aller jusqu'à 32 disques. Les disques constituant un agrégat peuvent être de types différents, des disques IDE, ESDI, ou SCSI,...

WINDOWS NT SERVER propose une autre fonctionnalité, la neutralisation des secteurs défectueux des disques (Sector Sparing) ou le dépannage à chaud (Hot Fixing). C'est le pilote de tolérance de panne qui lors de l'opération Entrée/Sortie déplace les bloc de données vers des secteurs en parfait état. Les périphérique SCSI peuvent neutraliser les secteur défectueux, mais pas les disques IDE ou ESDI.

Le Microsoft Clustering est une technique de tolérance de panne qui permet de rassembler plusieurs serveurs. Le logiciel de clustering gère les serveurs qui tombent en panne, l'accès aux ressources du serveur est toujours possible, et la charge de travail est répartie sur les autres serveurs.

La tolérance de panne avec WINDOWS NT SERVER s'effectue avec l'administrateur de disques. L'administrateur de disques gère aussi le partitionnement et le formatage des disques.

XXV-7.5 - Le contrôle des données : le cryptage

Le cryptage permet de consolider la confidentialité des données qui circulent sur le réseau ou qui sont stockées sur les supports de stockage (les ordinateurs ou les bandes de sauvegarde...). Le cryptage est fortement conseillé quand la divulgation des données de l'entreprise peut lui être très préjudiciable, quand les données peuvent être utilisées contre l'entreprise :

XXV-7.6 - Le contrôle des données : la protection contre les virus

La protection contre les virus doit être permanente parce que la protection est assurée par une identification du virus, et que l'identité des virus (et des pirates) est en perpétuelle évolution. C'est pourquoi, il ne suffit pas d'avoir un logiciel de lutte contre les virus installé sur les ordinateurs, mais il faut continuellement tenir à jour sa base de

données des virus connus...

XXV-8 - Le contrôle des matériels

XXV-8.1 - Le contrôle du matériel : l'UPS

L'alimentation électrique de secours, l'UPS (Uninterruptible Power Supply) permet d'alimenter un ou plusieurs ordinateurs, en cas de panne du secteur. L'UPS peut fonctionner avec une batterie, un moteur rotatif, ou un groupe électrogène (la durée et le coût ne sont pas les même...). L'UPS est situé entre la prise électrique et un ordinateur.

Selon la sophistication de l'UPS, celui-ci permet de faire plusieurs choses avant l'interruption totale du réseau :

- Alimenter plusieurs machines
- Gérer les surtensions ou les baisses de tension du courant électrique
- Informer les utilisateurs et l'administrateur de la panne de courant, via le serveur
- Inviter les utilisateurs a arrêter leur travail
- Enregistrer le travail en cours
- Empêcher les nouveaux accès des utilisateurs aux serveurs
- Fermer proprement les serveurs
- Avertir les utilisateurs, le cas échéant, que le courant est revenu
- Recharger automatiquement les batteries quand le courant est rétablit

Le meilleur système d'UPS est celui qui permet au réseau de fonctionner en continu, quelles que soient les perturbations de l'alimentation électrique...

XXV-8.2 - Le contrôle du matériel : la protection physique des équipements

La protection physique des équipements consiste à rendre inaccessible les équipements :

- L'enfermement des serveurs dans des chambres fortes
- Les ordinateurs sans lecteurs ni disques qui démarrent avec une puce d'amorçage sur la carte réseau
- Le choix d'un type de câbles :
- Le blindage des câbles limite les interférences magnétiques qui se propagent autour du câble
- L'enterrement des câbles (à l'intérieur des structures du bâtiment) limite la possibilité de se brancher directement dessus
- La fibre optique ne produit pas d'interférence

XXV-8.3 - La surveillance des performances : les outils d'administration

La surveillance des performances des machines est un travail de tous les jours qui requière des compétences techniques importantes. La surveillance s'effectue à l'aide des outils d'administration de WINDOWS NT SERVER :

- L'analyseur de performance pour suivre l'activité des composants du réseau
- Le Moniteur Réseau pour suivre les trames qui circulent sur le réseau
- Les agents du protocole SNMP pour suivre l'activité des composants du réseau
- Le logiciel SMS de Microsoft pour administrer le réseau depuis un poste centralisé

La surveillance des performances permet non seulement de suivre le niveau d'utilisation des ressources du réseau en temps réel et le comparer avec un niveau de référence, mais aussi de détecter les goulets d'étranglement...

XXV-8.4 - La surveillance de l'activité des utilisateurs : l'audit

La surveillance de l'activité des utilisateurs est une tâche qui doit s'effectuer régulièrement. L'audit pour suivre l'activité des utilisateurs :