Le Networking

Mémoire sur la pratique du shell Bash sous Gnu Linux

Par Patrick Hautrive
http://hautrive.free.fr

La table des matières

INTERNET

Le réseau internet

Le réseau internet est le réseau des réseaux. Le réseau internet relie entre eux les réseaux du monde entier (**Interconnected Network**) pour former un seul et immense réseau international (**International Network**). Le réseau internet est un réseau qui permet de relier entre eux tous les autres réseaux de la planète, qu'ils soient privés, public, personnel ou professionnel. Les intranets ou les réseaux **LAN** (Local Area Network) s'interconnectent avec internet ou les réseaux **WAN** (World Area Network).

Le réseau internet est un réseau de **commutation de paquets** qui utilise la pile de protocole **TCPIP** (Transport Control Protocol Internet Protocol). C'est-à-dire que les messages sont découpés en petits morceaux (**packets**), transportés sur le réseau par des routes en fonction du trafic, puis reconstitués chez le destinataire. Le protocole Tcp-ip est un protocole dît **connecté**, c'est-à-dire que l'expéditeur reçoit un accusé de réception qui lui garantit que le destinataire à bien reçut le message.

Ces particularités, du **maillage** du réseau, de la **diversité** des serveurs, et de la **sécurité** des échanges, font du réseau internet un outil **puissant** et **fiable** au service de la **communication** moderne et de l'avènement de la **civilisation** de l'information. Le “réseau est l'ordinateur” affirmait un dirigeant américain de la société Sun Micro Systems (**“The network is the computer”**).

Le protocole d'internet

Le protocole Tcp est un protocole avec connexion (**Ack** et **Sync**) qui assure que les messages sont transmis au destinataire. La **pile** de protocole Tcp-ip comporte de nombreux **protocoles** d'échange et de communication qui sont véhiculés par la couche du transport **TCP** (Transport Control Protocol) et adressés par la couche du réseau **IP** (Internet Protocol).

Les messages sont découpés en petits morceaux (**packets**) et empruntent des chemins indéterminés et différents selon le trafic sur le réseau (**route**). Arrivés à destination, les messages sont reconstitués, vérifiés (**control**) et un accusé de réception est envoyé à l'expéditeur.

L'histoire d'internet

Historiquement, c'est le **DOD** (Department Of Defense) de l'armée américaine qui en 1960 (période de la guerre froide entre les U.S.A et l'U.R.S.S) finance le développement d'un réseau **universel** et **autonome** capable de résister à une attaque nucléaire. L'objectif était de concevoir et de construire un réseau qui puisse toujours fonctionner, même si des parties étaient détruites. Le projet démarre au sein de l'agence **DARPA** (Defense Advanced Research Projects Agency). Les premiers tests sont réalisés avec quelques machines gouvernementales et universitaires.

En 1969, le réseau **Arpanet** comprend plusieurs universités de l'ouest américain (UCLA, Santa Barbara, Stanford, Utah) et les sockets du protocole **Tcp-ip** sont mises au point par l'université de Berkeley et intégrés au système d'exploitation multi tâches **"Bsd 4.2"**. En 1980, les protocoles **DNS** (Domain Name Service) et **NFSNET** (Network File System) sont implémentés dans Tcp-ip et le réseau **Ansnet** accueille les sociétés **IBM** (International Business Machines) et **AOL** (America On Line) qui fournit un accès à internet (**provider**) et des boites mail (**mail address**) à ses clients.

En 1989, le chercheur Tim Berners-Lee du **CERN** (Centre Européen de Recherche Nucléaire) invente le protocole **HTML** (Hyper Text Markup Language) et le principe de la navigation **WWW** (World Wide Web). En 1990, le réseau s'étend à d'autre pays avec **Europanet** (Ebone) pour devenir une hyper base de données dynamiques et multimédia mondiale (**data base**). Les utilisateurs peuvent désormais échanger des **mails**, naviguer sur la **toile**, créer leur site et communiquer via des **serveurs** (IRC, NEWS, FTP, GOPHER, BBS, HTTP), et les entreprises peuvent créer leur **site** et proposer leurs **services** commerciaux

Le projet **Xanadu** du sociologue Ted Nelson en 1965 fut le point de départ de la conception d'internet. Paul Baran eut l'idée de créer un réseau sous la forme d'une grande toile aux innombrables fils interconnectés.

La navigation internet

La navigation internet consiste à utiliser un **navigateur** pour consulter les pages de **sites** internet. Le navigateur est un logiciel qui met en **page** les données HTML livrées par des **serveurs**. Les **internautes** butinent (**browse**) comme des abeilles, en sautant d'un lien vers un autre, et parcourent ainsi la toile au gré du hasard et de leurs centres d'intérêts. Les navigateurs ont été nombreux à rechercher la prédominance du marché et les préférences des utilisateurs. Finalement, le Logiciel Libre **Firefox** de la fondation **Mozilla** occupe une place importante et innovante (onglet, popup, historique, bookmarks, complétion). D'autres navigateurs moins performants permettent de visionner les pages internet (Mosaic, Opera, Netscape, Internet Explorer, Konqueror, Emacs, Lynx).

La navigation internet est devenue de plus en plus sophistiquée, et des concepts comme le Web 2.0 jalonnent les conversations des **"salarymen"** et les discours des dirigeants des multinationales sur l'avenir imprévisible, inquiétant mais prometteur, du réseau des réseaux. Les **technologies** dynamiques et propriétaires s'emparent du monde virtuel de l'internet et en modifient le paysage visuel (Shockwave, Gif Animés, Flash, Plugins, Cookies, Scripts Cgi-bin, Java, Applets, ActiveX, Xml, Type Mime, Bluetooth, Wifi, Voip, Google Earth, Sms, Msn, Jpeg, Mp3, flux RSS, Certificats, Cloud Computing, etc).

En même temps, des sites **communautaires** investissent l'espace numérique pour proposer des services utiles et gratuits, comme des sites d'expression, de mise en relation, de collaboration ou de **partage** de

contenus (Spip, Blog, Alert Mail, Mailing List, Irc Freenode, Chat Jabber, Linux Lug, Mud, Peer2peer, Google Calendar, Youtube, Facebook, Couchsurfing, Woofing, Linked, Tiers de confiance).

L'usage d'internet

L'usage d'internet est **multiple** et diversifié, comme le sont les utilisateurs à travers le monde. L'activité d'internet ne s'arrête pas aux **frontières** (sauf pour certain pays qui pratique encore la censure comme en Chine par exemple) et fonctionne en **permanence** (jours et nuits, 24 heures sur 24, 7 jours sur 7 et 365 jours par an). Il se produit comme une **migration** des activités humaines qui passent de la sphère matérielle à l'univers virtuel (**virtual**). C'est une des raisons qui expliquent l'importance stratégique des Logiciels Libres (**free software**).

Il y a bien sûr la **navigation** sur internet (Url, Http, Web, Html, Site, Link), la recherche des **informations** (Faq, Howto, RFC, Wikipédia,) avec des **moteurs** de recherche (google), les échanges de **messages** électroniques (Mailbox, Mailing list, Spam), les échanges de **fichiers** (Ftp, Download, Peer to peer, Images Iso, Binaires, Photographies, Vidéos, Musiques, Journaux, Magasines, Télévisions, TNT), les échanges d'**opinions** (Chat, Irc, Webcam, Forums, News Groupes), les **jeux** en réseaux et en groupes (Counter Strike, Mud, Mush, Worldcraft, Second Life), la **sécurisation** des réseaux, l'intégrité et la confidentialité des comminications (VPN, SSH, Routers, Firewall, Antivirus, Spyware, Cryptographie, Public Keys, ACL, PGP).

La netiquette

Le bon usage d'internet s'appèle la Nétiquette. D'une manière générale, il est appréciable de faire preuve de courtoisie et de respect de la dignité humaine. Par exemple, il est recommandé de respecter **l'opinion** et **l'anonymat** des autres utilisateurs, de demander l'autorisation pour copier un fichier ou une adresse de courrier électronique (**e-mail**), de ne pas saturer la boite mail de quelqu'un avec des messages non sollicités ou des pièces jointes trop lourdes (un lien suffit pour mettre à disposition un fichier), et de ne jamais écrire en **majuscule**, ce qui est considéré comme une marque d'insulte et de véhémence.

Certains serveurs disposent de modérateurs (**moderators**) ou d'administrateur (**operators**) qui surveillent les conversations et imposent la discipline. Ce sont le plus souvent des bénévoles qui invitent les autres internautes à respecter la **charte** d'utilisation du site. Dans les forums, il est recommandé d'écrire ses **réponses** à la suite d'une conversation, de ne conserver que les **paragraphes** contextuels, et de limiter sa **signature** à quelques lignes.

La **mesure** et la retenue sont de bonnes qualités à suivre sur internet afin d'éviter les **malentendus** et l'engrenage de la violence qui sont faciles et fréquent sur internet (trolls, flames, virus, robots, cross posting, racism, social spying). Le mélange de la distance et de la familiarité favorisent la confusion et le laxisme des mœurs. Comme dans la vie réelle (**real life**), l'internaute n'a pas intérêt à accorder sa

confiance à des inconnus trop rapidement, ni dévoiler sa vie privée au tout venant. Avant d'appeler à l'aide, il est recommandé de lire le **manuel** d'instruction, de chercher soi même, si une solution n'est pas déjà disponible sur internet, et d'indiquer avec précision sa configuration et sa situation.

Le contrôle parental

Des logiciels de contrôle parental (**parental control**) permettent de restreindre l'accès à certains sites et d'empêcher les propositions irrévérencieuses. Toutefois, rien ne vaut l'assistance et l'accompagnement bienveillant des parents eux même ou des proches. Les gens mal intentionnés trouvent toujours les moyens de contourner les gardes fous qui freinent leur cupidité, et démontrent avec une inquiétante constance leur avidité à exploiter les failles ou les trous juridiques.

Quoi qu'il en soit, internet est un nouvel **outil** de communication incontournable, et il appartient à chacun, d'apprendre à s'en servir, et de savoir ce que l'on est en droit d'en attendre. Il est important de se souvenir que l'on ne sait jamais qui se trouve ou qui se cache à l'autre bout d'un câble. La généralisation des **cybercafés** et la démocratisation des techniques de **piratage** ne doit pas éluder le devoir de chacun de se protéger et de rester informer.

Les **robots** sont de moins en moins discernables des êtres humains, et la réciproque est également de plus en plus une réalité. Et si les autorités d'un pays règlementent la **traçabilité** des connexions, il est bien souvent trop tard quand elles n'interviennent. Enfin, c'est un droit légitime que de pouvoir surfer dans l'anonymat et de préserver sa vie privée. C'est donc un **apprentissage** de tous les jours que de suivre les changements du monde, et de prendre quotidiennement les précautions indispensables pour se prémunir des risques que l'on encoure.

Un outil de communication

Le réseau internet est un **outil** de communication instantanée qui rapproche les gens, et c'est naturellement que les gens entrent en relation les uns avec les autres, et proposent éventuellement leur aide et leur conseil. Mais, il n'y a en la matière, ni de **règles**, ni d'obligation, ni de panacée, ni de certitudes. Les informations que l'on glane sur internet ne sont pas forcément les plus authentiques, ni les plus actuelles. Toutefois, dans certains cas, c'est le contraire qui est indéniable.

Ainsi, les internautes et les usagers des réseaux doivent toujours garder intact leur esprit **critique**, conserver leur calme et leur modestie, et **relativiser** devant la complexité de l'outil. Ce ne sont jamais que des **bits** qui circulent, et qui n'ont pour valeurs que celles que nous voulons bien leur attribuer. La censure n'a jamais éradiquée l'éblouissante clarté des idées, et les bonnes intentions n'ont jamais été les garantes d'une véritable justice.

Chacun est invité à se familiariser avec l'outil, et à prendre le temps de connaitre les enjeux des **NTIC** (Nouvelles Techniques de l'Information et de la Communication). La **connaissance** est le moyen de rester libre et la condition pour s'en servir à bon escient et pour essayer d'en tirer le meilleur parti. Par

exemple, c'est un bon **réflexe** que de prendre le temps d'effectuer des **sauvegardes** régulières de son travail, et c'est une bonne **attitude** que de savoir se passer d'un écran pour vivre et communiquer autrement.

Les standards ouverts

Le réseau internet ne pourrait être ce qu'il est sans ouverture. Ainsi, il est également recommandé d'utiliser des **formats** de fichier aux standards ouverts, afin de ne pas pénaliser les utilisateurs qui ne disposent pas des mêmes applications, ni des mêmes moyens.

Il est aussi recommandé d'utiliser les **Logiciels Libres**. Les Logiciels Libres (**free software**) garantissent la **transparence** et la **pérennité** de l'accès au code source des programmes (**open source**), et ils protègent les intérêts des utilisateurs avec la licence **Gnu GPL**.

La documentation sur une Debian Gnu Linux peut être trouvée sur le système ou sur Internet.

file:///usr/share/doc/debian/FAQ/index.html#contents
File://usr/share/doc/debian/debian-manifesto
file://usr/share/doc/debian/constitution.txt
http://debian.org

Les abréviations sur internet

Comme dans tout nouvel espace, les populations se l'approprient en créant de nouvelles **habitudes** et de nouveaux codes de **reconnaissance** qui sont pour ainsi dire des signes distinctifs et d'appartenance. Les abréviations sont un particularisme linguistique et sociologique très américains.

Les abréviations sur internet	
BTW	(By The Way)
IMHO	(In My Humble Opinion)
RSN	(Real Soon Now)
RTFM	(Read The fucking Manual)
TIA	(Thanks In Advance)
TLA	(Thee Letter Acronyme)
MDR	(Mort De Rire)
MUD	(Multi User dungons)
MUSH	(Multi User Shared Hallucination)
ASAP	(As Soon As Possible)

Les adresses URL

Les adresses internet **URL** (Uniform Ressource Locator) sont généralement formulées en indiquant dans l'ordre, le nom du protocole réseau, le nom du serveur, le nom de domaine, le nom du **TLD**, puis le numéro de port optionnel, et enfin le chemin absolu vers le fichier dans l'arborescence du serveur. Une adresse internet écrite en extension est conforme au **FQDN** (Full Qualified Domain Name).

Les numéros de port (**port**) sont utilisés pour indiquer au destinataire (**target**) le type de service (**daemon**) recherché sur le serveur (**server**). Les services emploient généralement toujours les mêmes numéros de port. Par exemple, le port 22 est le port du service de connexion à distance sécurisée (**ssh**) et le port 80 est généralement celui du serveur internet (**apache**). La correspondance entre les noms des services et les numéros de port peut être paramétrée. La liste des services se trouve dans un système Gnu Linux dans le fichier **"/etc/services"**.

La formulation des adresses des serveurs internet		
URL (Uniform Ressource Locator)	**protocol://name.host.server.domain.tld:port//path/to/file**	
FQDN (Full Qualified Domain Name)	http://	Le protocole hypertexte des pages web
	https://	Le protocole hypertexte sécurisé
	ftp://	Le protocole de transfert de fichiers
	gopher://	Le protocole gopher
	news://	Le protocole de Usenet
	telnet://	Le protocole de connexion non sécurisé
	file:///	Le protocole pour l'arborescence locale
	mailto:	Le protocole pour indiquer une adresse mail

La hiérarchie des noms de domaines TLD

Les **TLD** (Top Level Domain) sont les **noms de domaine** qui forment la cime de la **hiérarchie** sur **internet**. Les TLD indiquent soit la nature de **l'activité** de l'organisation, soit le **pays** où se trouve la dite organisation.

La hiérarchie internet des noms de domaine TLD (Top Level Domain)			
.org	Les organisations	.fr	L'extension de la France (France)
.gouv	Les gouvernements	.be	L'extension de la Belgique (Belgium)
.com	Les sociétés commerciales	.uk	L'extension du royaume uni (United Kingdom)
.edu	Les universités	.de	L'extension de l'Allemagne (Deutchland)
.mil	Les administrations militaires	.it	L'extension de l'Italie(Italy)
.asso	Les associations	.us	L'extension des U.S.A (United State of America)
.net	Les sociétés internet	.sp	L'extension de l'espagne (Spain)
.int	Les administrations internationales	.pt	L'extension du Portugal (Portugal)
		.ch	L'extension de la Suisse (Schweiz)
		.ir	L'extension de l'Irlande (Ireland)
		.in	L'extension de l'Inde (India)
		.ru	L'extension de la Russie (Russia)
		.au	L'extension de l'Australie (Australia)
		.sw	L'extension de la Suède (Sweden)
		.nz	L'extension de la Nouvelle Zélande (New Zealand)

Les organismes de régulation d'internet

Les organismes d'internet ont pour objectifs d'organiser et de réguler le réseau internet.

Les organismes de régulation et de normalisation d'internet	
ISO	(International Standards Organization)
ANSI	(American National Standards Institute)
IEEE	(Institute of Electrical and Electronics Engineers)
IETF	(Internet Engineering Task Force)
IANA	(Internet Assigned Numbers Authority)
EIA	(Electronics Industries Association)
NSA	(National Security Agency)
IAB	(Internet Architecture Board)
NIST	(National Institute of Standards and Technology)
COSE	(Common Open Software Environnement)
OMG	(Object Management Group)
OSF	(Open Software foundation)
SAG	(SQL Access Group)
ITTCC	(International Telegraph and Telephone Consultative Committee)
CCITT	(Comité Consultatif International de Télégraphie et de Téléphonie)
ITU	(International Telecommunication Union)
AFNOR	(Association Française de Normalisation)
INRIA	(Institut National de Recherche en Informatique et Automatique)
CNIL	(Commission Nationale Informatique et Libertés)
INTERNIC	(Internet National Information Center)

Les forums internet

Les forums internet permettent une communication asynchrone en mode texte. Les serveurs de news (**usenet**) propagent les articles (**threads**) qui sont classés par sujets et postés par des particuliers. Ainsi, les internautes peuvent se tenir informés sur des sujets très spécialisés. Certains forums proposent un envoi hebdomadaire avec un résumé (**digest**) ou l'envoi des entêtes seulement (**headers**).

Les forums sont regroupés par thèmes au sein d'un arbre hiérarchique qui comprend de multiples branches. La branche “alt” (**alternatives**) proposent des sujets libres, la branche “fr” (**french**) est en langue française, la branche “comp” (**computer**) est dédiée aux ordinateurs et la branche “misc” (**miscellanous**) recueille les thèmes qui n'ont pas d'autres lieux pour s'exprimer.

Les **forums** (news groups) utilisent des serveurs de news qui transmettent les **conversations**. Ces serveurs constituent entre eux des réseaux qui acceptent plus ou moins toutes les **branches** de la hiérarchie. Les serveurs dupliquent entre eux leurs données afin de pouvoir les distribuer plus rapidement. Les **FAI** (Fournisseur d'Accès à Internet) filtrent parfois le contenu des forums qu'ils mettent à la disposition de leurs abonnées, et leur portail ressemble plus à une barrière qu'à une porte d'entrée. Les **protocoles** utilisés par les serveurs de news sont **UUCP** (Unix to Unix Copy Protocol) et **NNTP** (Network News Transport Protocol).

Les Forums ou News groups								
Networks			**Hierarchy**				**News Readers**	
Usenet	comp	computer	news	news	talk	conversation	pine	nn
Bitnet	fr	french	rec	recreation	bit	binaries	emacs	slrn
Arpa	misc	miscellanous	soc	social	gnu	free	mozilla	trn
	alt	alternatives	sci	science	software			

Les infrastructures téléphoniques

Les équipements (**routers**) et les infrastructures des réseaux hertziens (**satellites**) ou téléphoniques (**cable**) déterminent les types de service que peuvent proposer les Fournisseurs d'Accès à Internet (**provider**). Les liaisons réseaux passent en général par des lignes téléphoniques (**lines**) qui peuvent être publiques ou privées. Les lignes privées sont généralement des lignes spécialisées et dédiées de type “T1” qui sont directement reliées aux réseaux hauts débits nationaux (**backbones**).

Les réseaux téléphoniques ont progressivement évolués de la technologie **RTC** (Réseau Téléphonique Commuté), à **l'ADSL** (Asymetric Digital Subscriber Line), et maintenant la fibre optique (**fiber chanel**). Les équipements des ordinateurs ont suivis les progrès de la technologie et les types de connexion ont évoluées du **modem** (Port Serie, RJ11), à la **carte réseau** (Ethernet, RJ45) et maintenant au **routeur** (Adsl). Les types de connexion influencent la qualité du **signal**, et le débit montant

(**upload**) et descendant (**download**). Les protocoles de connexion ont également évolués (SLIP, CSLIP, PPP, ADSL).

La bande passante

La bande passante représente la **quantité** théorique maximale d'information qui peut transiter sur une ligne en une seconde et exprime la **vitesse** d'une connexion. La bande passante norme les **débits** effectifs qui sont mesurés en Bits par seconde (**Bits per seconde**) ou en Octets par seconde (**bytes per seconde**).

Selon les **technologies** (cable, connexion, protocols), le débit est plus ou moins conséquent. Ainsi, le niveau de la bande passante est prépondérante quant aux types de données qui peuvent être véhiculées par le réseau, et réceptionnées chez les utilisateurs. Par exemple, les connexions **RTC** permettaient de naviguer sur internet (**web**) et d'échanger des mails (**text**), tandis que **l'ADSL** (Asymetric Digital Subscriber Line) ouvre des perspectives bien plus large, avec la téléphonie sur internet ou **VIOP** (Voice Over Internet Protocol) et la réception de chaines de télévision (**television**). Les autoroutes de l'information (**information highways**) ne seront une réalité qu'avec la généralisation de la fibre optique.

L'évolution de la bande passante (Band Width)	
Lignes RTC (Réseau Téléphonique Commuté)	28,8 à 56 Ko/s
Lignes spécialisées T1	1,5 Mo/s
Lignes spécialisées T3	45 Mo/s
Lignes ADSL (Asymetric Digital Subscriber Line)	64 Mo/s à 8 Go/s
La fibre optique	

Les connexions RTC

Les connexions à internet par la ligne de téléphone **RTC** (Réseau Téléphonique Commuté) peuvent être, soient **analogiques** avec un modem **HAYES** et le protocole **PPP** (Point to Point Protocol), soient **numériques** avec un modem **ADSL** (Asymetric Digital Subscriber Line) et les protocoles **PPOE** et **PPOA**.

Les connexions analogiques par modem ont longtemps été le type de connexion le plus répandu avant l'arrivée de l'ADSL. Les connexions analogiques utilisent les lignes téléphoniques courantes, et les communications transitent par un appareil qui transforme le signal numérique de l'ordinateur en signal analogique pour la ligne de téléphone. Ces appareils sont appelés des **modems** (mot valise qui provient de la contraction de modulation et de démodulation) et ils se branchent sur les connecteurs des ports séries (**serial**) de l'ordinateur. Les connexions analogiques s'appuient sur le standard HAYES pour les communications en modulation de fréquence et le protocole PPP.

Les connexions numériques ADSL requièrent que le standard téléphonique soit situé à moins de 5 kilomètres, et qu'il soit équipé d'un appareil de **dégroupage** numérique (DSLAM). Les connexions numériques passent par un modem ADSL, et sont désormais configurées avec les protocoles PPOE et PPOA.

NETWORK

Les réseaux

Les réseaux sont des ensembles qui réunissent des unités qui partagent le même moyen de communication. Les ordinateurs d'un réseau sont reliés entre eux, le plus souvent par un câble, et disposent du même protocole de communication pour échanger des données. Les réseaux sont devenus indispensables pour les organisations humaines. Il existe différents types de réseaux.

Les avantages des réseaux

Les deux avantages principaux des réseaux sont la communication numérique et la continuité de la **chaîne numérique**. Ensuite, les utilisateurs profitent du partage des ressources, du travail en groupe, et de la centralisation de l'administration. La communication numérique crée des **synergies**.

La chaine numérique

La mise en réseau d'un ensemble d'ordinateurs permet de ne pas interrompre la chaine numérique. Le réseau permet de standardiser, d'automatiser, de mutualiser et de centraliser certaines tâches d'administration. Le partage de fichier d'avant le réseau était appelé le «réseau disquette», ou le **«Sneakernet»** (réseau basket) du nom d'une marque de paire de chaussure américaine.

Le réseau permet également de maintenir la cohérence des différentes **versions** d'un même 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.

La communication numérique

La communication numérique permet de profiter de la vitesse de transfert des électrons, et de conserver les fichiers dans un **format** digital qui peut se stocker longtemps et dans peu de place. Le partage des **ressources** en réseau permet de mettre en commun, les fichiers, les applications et les périphériques comme les imprimantes, les scanners, ou les routeurs. Il est même possible de partager l'écran d'une interface graphique avec un correspondant à distance, et de déporter l'affichage avec le serveur graphique. Les **moyens** de la communication numérique sont la messagerie interne ou externe, l'accès à internet, l'accès à distance aux ressources du réseau.

Le travail en groupe permet la **synchronisation** des agendas et des notes de service, le suivie des différentes versions d'un même projet et le travail interactif et collaboratif entre les membres d'une même équipe.

La centralisation de l'administration

La centralisation de l'administration est un avantage prépondérant pour l'administrateur du réseau et les responsables d'équipes. Les réseaux permettent une meilleure **efficacité** des tâches répétitives. Les **procédures** sont plus **sophistiquées** et peuvent être appliquées machinalement et sans délais. Ainsi, les réseaux permettent une meilleure **sécurisation** et **confidentialité** des données. **L'authentification** des utilisateurs et le contrôle de l'accès aux ressources sont facilités par la mise en place de procédures **systématiques**. La gestion centralisée des droits et des permissions pour les comptes et pour les groupes permet une certaine **uniformisation** de la politique de contrôle des identités.

Les réseaux rendent possible une organisation **globale** et **hiérarchique** des documents éparpillés sur tous les postes. Ainsi, la **sélection** des documents sensibles et une stratégie **d'automatisation** des **sauvegardes** et des **installations** peuvent être mises en place. La **protection** de tous les documents numériques (lettres, tableaux, photographies, vidéos, exécutables) est assurée, et une politique de **normalisation** des postes des utilisateurs peut être appliquée. La **standardisation** des applications pour un grand nombre de poste permet de suivre plus facilement les mises à jours, les besoins de formation et de **maintenance**.

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 configuration à distance, voire d'uniformiser les configurations de tous les postes. Les avantages de l'administration centralisée sont appréciables en terme de **temps**, **d'argent** et **d'opinion**. Les outils de centralisation de l'administration d'un réseau sont nombreux.

La classification des réseaux

Les réseaux peuvent être classifiés en fonction de différents critères. Ces critères peuvent être **l'envergure** géographique (LAN, MAN ou WAN), le degré **d'ouverture** (Intranet, Extranet ou Internet), la **densité** des nœuds (dizaine, centaines ou milliers), le **protocole** de communication (TCP ou ATM), le **support** physique (câbles, ondes, microwave), la **hiérarchie** de l'organisation (Main Frame ou Client Serveur), la **topologie** architecturale (Bus, Étoile ou Anneau) ou la **méthode** d'accès au réseau (Collision, Jeton ou Priorité).

En 1970, les réseaux fonctionnaient principalement avec le protocole **X.25** (Tymnet, Sprintnet, Transpac). En 1980, les réseaux employaient la technologie **Frame Relay**. En 1990, les réseaux étendus sont équipés majoritairement par la technologie **ATM** (Asynchronous Transfert Mode).

La classification des réseaux			
L'envergure géographique	TAN	Tiny Area Network	House
	CAN	Campus Area Network	Property
	LAN	Local Area Network	Building
	MAN	Metropolitan Area Network	City
	WAN	Wide Area Network	Country
	RLE	Réseau Local d'Entreprise	Society
Le degré d'ouverture	Intranet	Réseaux privés internes d'une entreprise	Private
	Extranet	Réseaux privés ouverts vers l'extérieur	Private
	Internet	Réseaux publiques nationaux ou internationaux	Public
La densité des postes	Le nombre de postes, de nœuds, ou de cartes réseaux (nodes)		Nodes
Le protocole de communication	OSI	Modèle de protocoles en sept couches	Routing
	TCP/IP	Standard libre pour internet et réseaux locaux	Routing
	IPX/SPX	Réseaux Novell	Routing
	XNS	Xerox Network System	Routing
	X.25	Commutation qui devint le Frame Relay (fiber)	Routing
	ATM	Asynchronous Transfert Mode	Routing
	DDP	Réseaux Apple Talk de Macintosh™	Routing
	NetBEUI	Réseaux non routable de Microsoft	Subnet
Le support physique	Le câble coaxial (blindé ou non)		Cable
	Le câble en paires torsadées (blindée ou non)		Cable
	Les lignes téléphones (Réseau Téléphonique Commuté)		Cable
	La fibre optique (fiber)		Cable
	Les ondes radios (antennes)		Air
	Les micro ondes (Wifi)		Air
	Les ondes infrarouges (Bluetooth)		Air
	Les satellites (paraboles)		Air
La hiérarchie de l'organisation	Terminal	Réseaux passifs et centralisés (Main Frame)	Central
	Poste	Réseaux décentralisés ou répartis (peer to peer)	Poste
	Serveur	Réseaux distribués en clients et en serveurs	Server
La topologie architecturale	Bus	Réseaux linéaires (le long d'un câble)	Line
	Étoile	Réseaux centralisés (autour d'un switch)	Star
	Anneau	Réseaux circulaires (circuit en ronde)	Ring
La méthode d'accès au réseau	Collision	Réseaux Ethernet (CSMA/CD et CSMA/CA)	First
	Jeton	Réseaux en anneaux (Token Ring et FDDI)	Next
	Priorité	Réseaux 100VG-AnyLAN (Ethernet 100 Mb/s)	Priority

Les protocoles routables

Les protocoles routables (**routing**) permettent de franchir la barrière des routeurs (**routers**) pour communiquer avec d'autres sous-réseaux. Les protocoles non routables ne permettent la communication qu'avec les postes appartenants au même sous réseau (**subnet**), tandis que les protocoles routables redirigent les communications, qui ne sont pas destinées au même sous réseau, vers une passerelle par défaut (**gateway**). La segmentation des sous réseaux permet de séparer les espaces et de circonscrire le trafic, mais il est aussi important que les stations puissent communiquer avec une station d'un autre sous réseau. Le routage permet ces communications entre sous réseaux, et avec internet. La segmentation en sous réseau permet également le filtrage des paquets avec un pare feu (**firewall**).

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.** Pour qu'un réseau hétérogène fonctionne, il faut réunir plusieurs conditions. Les machines doivent parler le même langage. Un **protocole** réseau en commun doit être installé sur toutes les machines qui communiquent entre elles. La communication doit être assurée par un protocole **routable** quand il y a plusieurs segments de réseaux et un accès à internet. L'interopérabilité, la **portabilité** et la **liberté** de l'accès au code source sont les principes d'administration d'un système d'information dans un environnement multi fournisseurs.

De nos jours, la majorité des réseaux sont des réseaux **hétérogènes** et de nombreuses raisons contribuent à qu'il en soit ainsi. Les **technologies** évoluent. Les fournisseurs recherchent la plus grande **compatibilité** de leurs produits. Les administrateurs réseaux deviennent multi compétents pour mettre en œuvre une telle complexité. Les réseaux se construisent petit à petit, la **planification** se déroule en phase et les **évolutions** se généralisent par petits bouts, en fonction des budgets ou de la concurrence. Les utilisateurs ont leurs **préférences**, le Macintosh™ pour les graphistes, Unix™ pour les administrateurs de serveurs adeptes de la ligne de commande, les compatibles PC pour les inconditionnels des tendances et de la part de marché, les Clusters ou le Main Frame pour les administrateurs de bases de données et de centre de calcul. Certaines **architectures** présentent à un moment donné, un avantage comparé sur d'autres.

Les environnements réseaux hétérogènes

L'hétérogénéité des réseaux provient de la cohabitation plus ou moins heureuse des nombreux fournisseurs qui se battent ou s'entendent pour conquérir des parts de marchés et imposer leurs normes.
Les éditeurs de système d'exploitation réseau développe des **API** (Application Program Interface) qui leur sont propres, les constructeurs de machines conçoivent des architectures **propriétaires**, les fondeurs de processeurs mettent au point des **instructions** processeurs particulières, les organismes de

régulation s'apparentent parfois à des **consortiums** de multinationales et de services spéciaux des états qui revendiquent le contrôle de l'univers numérique et le **monopole** des nouvelles technologies.

Les **normes** des protocoles réseaux ne sont pas toujours suivies, les **technologies** suivent des processus de création et de validation qui sont privés, le **cycle** de vie des produits est court et incertain, les constructeurs de matériels essayent de favoriser leurs produits et utilisent les techniques de **commercialisation** et de fidélisation “moderne”, basé sur la dépendance, l'influence des lobbies, les progrès de la sociologie de groupe et les neurosciences. La plus part des réseaux hétérogènes combinent les architectures, les technologies, les protocoles, les systèmes et les logiciels.

Les réseaux hétérogènes	
Computers	Mini Main Frame Terminal IBM PC Blade Macintosh™
Processors	CELLS CISC RISC
Constructors	IBM HP Sun Intel Dell Motorola Xerox Nokia Sony Asus 3com
Cryptography	Cesar Vigenere RSA DES MD5 CHA PGP Asymetric
Langages	Assembler Delphi C C++ Java Sql Php Shell Ruby Python
Normes	ANSI IEEE 802 EIA 568 IPV4 IPV6 RFC ITU OSI
Editors	Microsoft Novell Oracle Unices Community Apple
Systems	Windows Netware OS/2 Bsd Unix™ Gnu Linux Mac OS
Protocols	NetBEUI UDP XNS SPX/IPX TCP/IP Apple Talk
Servers	Nfs Ftp Ssh Apache Postfix Smtp Pop Bind Mysql
Topology	Bus Star Ring Ethernet LAN MAN WAN Internet
Networks	Peer to Peer Intranet DMZ Extranet Client Server Private Public
Lines	RTC ADSL RNIS X.25 ATM FDDI VPN
Transmission	Analogical Broadband Digital Baseband A/Synchronous Commutation
Supports	Coaxial UTP/STP Fiber Radio Spectral Microwave Satellite Laser
Connectors	BNC AUI DIX RJ11 RJ45 USB Serie Wifi LPT FIRE
Slots	ISA EISA MCA PCI PCX AGP RAM VGA DVI
Methods	Collision Prevention Jeton Priority Canals Modem Sneakernet
Concentrators	Hub Switch MAU CSUDSU Bridge Router Firewall Gateway

Le dépannage des réseaux hétérogènes

Le dépannage des réseaux hétérogènes consiste la plus part du temps à vérifier la concordance et la conformité des matériels et des logiciels avec les systèmes d'exploitation. Les problèmes peuvent provenir des matériels, des logiciels, des réseaux ou des utilisateurs. La première chose a vérifier dans un réseau, c'est si le **câble** est branché, si **l'alimentation** est opérationnelle, et si les **dispositifs** sont allumés. Ensuite, il faut vérifier si les matériels sont compatibles et reconnus, si les bons **pilotes** sont bien installés, si les spécifications pour la **configuration** matérielle minimale sont scrupuleusement respectées. Enfin, il faut contrôler si les **protocoles** sont bien installés, si la configuration des **cartes** réseaux est correcte, et si les **applications** clientes et les applications serveurs idoines sont de part et d'autres biens installées et bien démarrées. Pour les imprimantes réseaux, il faut s'assurer que les **fichiers** du périphérique (**spool**) ne sont pas saturés.

La surveillance du réseau peut consister, à vérifier les **trames** qui circulent sur le support de communication, à mesurer le **trafic** réseau, à tester les **boîtiers** qui segmentent et qui filtrent le réseau, et à superviser la configuration des **passerelles**. La surveillance des utilisateurs peut consister, à partager les **ressources** nécessaires, à octroyer les **permissions** indispensables et à soutenir les demandes légitimes de **formation** des usagers.

Les performances d'un réseau

Augmenter les performances d'un réseau signifie, soit accélérer la transmission des données (**speed**), soit augmenter la quantité de donnée qu'il est possible de transmettre, c'est-à-dire la bande passante (**broadband**). Les performances réelles d'un réseau peuvent être mesurées par le débit, c'est à dire la quantité d'Octets transmis sur le câble par secondes. Plus le nombre d'Octets par seconde est élevé et plus le réseau est performant. La bande passante est une limite maximale théorique qui est fonction du type de câble (**cable**) et du mode de transmission. On dit que le réseau «s'effondre» quand plus aucune machine ne peut transmettre de message (**down**). La surveillance des performances réseaux permet d'intervenir avant d'atteindre le seuil de non retour (**alarm**).

Les performances d'un réseau dépendent de nombreux facteurs, dont le nombre de machines connectées au même câble (**hosts**), le débit théorique maximal du câblage (**broadband**), les ajustements de configuration effectués par l'administrateur (**tuning**) et les capacités des cartes réseaux (**interface**).

Les performances des cartes réseaux

La carte réseau est un élément crucial de la performance d'un réseau, parce qu'elle représente un carrefour obligé pour toutes les données. Si la carte réseau est lente, alors les données seront transmises lentement sur le réseau. Par exemple, dans un réseau en bus Ethernet, 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. Les cartes réseau des **serveurs** doivent être équipées en priorité avec les modèles les plus performants. La carte réseau d'une station de travail n'a généralement pas besoin d'être aussi performante. Bien sûr, tout dépend de la nature de **l'activité** de l'utilisateur de la station. Une station qui n'exécute que des applications bureautiques ne génère pas beaucoup de trafic. A contrario, une station qui fait tourner une application réseau, comme une base de données, ou une application d'ingénierie, génère rapidement beaucoup de trafic. Les cartes réseaux produites par des **fabricants** reconnus offrent en moyenne de meilleurs rendements, une durée de vie plus longue et des pilotes plus souvent mis à jours.

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 est toujours préférable de disposer d'une quantité de mémoire vive suffisante, d'un processeur et d'un bus bien cadencés. Ac l'accès direct à la mémoire ou **DMA** (Direct Access Memory) de l'ordinateur, la carte réseau transfère directement les données depuis sa mémoire tampon vers la mémoire de l'ordinateur, sans passer par le microprocesseur. Les données sont ainsi plus rapidement traitées par le système. Avec 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 de l'ordinateur sans passer par le microprocesseur de l'ordinateur. 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.

Avec la **mémoire partagée** de la carte réseau, la carte réseau partage avec le système une partie de sa propre mémoire. Le système considère cette mémoire comme la sienne et les données traitées par le système sont directement adressées à la mémoire partagée de la carte réseau. Avec la **mémoire tampon** de la carte réseau, la carte réseau accumule directement les trames du réseau dans sa mémoire tampon et les redirige au fur et à mesure. Les trames 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.

Avec un microprocesseur intégré à la carte réseau, la carte réseau dispose de son propre processeur qui lui permet de traiter elle même les données sans passer par le processeur de l'ordinateur. Avec la mémoire système partagée, la carte réseau dispose de son propre processeur mais elle utilise une partie de la mémoire vive de l'ordinateur pour traiter les données du réseau. Une carte réseau avec son propre processeur et sa propre mémoire vive sera toujours plus rapide qu'une autre. Une carte réseau avec de la mémoire partagée sera plus rapide qu'une carte réseau avec un accès direct à la mémoire de l'ordinateur (DMA) et à fortiori bien plus rapide qu'une carte réseau avec des E/S normales.

GROUPWARE

Le 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. Le travail en réseau peut être asynchrone ou synchrone, et faire gagner beaucoup de **temps**. Le premier utilisateur a bénéficier des avantages du réseau est l'administrateur réseau.

De plus en plus d'applications sont conçues pour le travail dynamique en réseau de plusieurs utilisateurs. Les avantages sont nombreux, par exemple, une application réseau multi utilisateurs représente la même **interface** pour tous les utilisateurs, et les efforts d'apprentissages n'en sont que plus réduit. De même, la maintenance de l'application est également facilitée pour l'administrateur qui n'a qu'un seul applicatif à gérer, et éventuellement qu'une seule **licence** d'utilisation à financer. Enfin l'uniformisation des interfaces va de pair avec la standardisation des **formats** de fichiers qui facilitent la conservation des données ainsi que les **sauvegardes**.

Avec les outils réseaux, les communications peuvent s'effectuer en discontinue, à contrario du téléphone qui requière que les deux correspondants soient disponibles à un même moment. Entre l'envoi d'un mail par l'expéditeur et la lecture du mail par le destinataire, il peut se passer du temps puisque les communications sont enregistrées. Comme avec une lettre, la **trace** des communications permet de mieux organiser le travail futur, et de mieux retrouver l'enchainement des évènement passés.

Les applications réseaux

L'expression «application réseau» peut désigner plusieurs choses.

Les applications réseaux
Les **applications** centralisées et téléchargées par les utilisateurs sur un serveur d'application
Les serveurs qui proposent des **services** (authentification, fichiers, impression, base de données)
Les pare feux qui filtrent les communications et protègent les ressources (**firewall**)
Les plateformes de travail collaboratif (**groupware**) en réseau et en mode multi utilisateurs
Le courrier électronique pour échanger messages et documents avec les intervenants extérieurs
La **messagerie** Intranet pour communiquer avec les collaborateurs à l'intérieur de l'organisation
Les **agendas** de groupe pour organiser des réunions en fonction de l'emploi du temps de chacun
Les gestionnaires de données personnelles **PIM** (Personal Information Manager)
Les applications de gestion des contacts

Le courrier électronique

La messagerie électronique permet d'échanger des messages (**mail**) et des documents annexés (**attached**) au message en «pièces jointes». Les correspondants d'une messagerie électronique doivent tous avoir une adresse électronique (**mail address**), 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 (**mailing list**), il est possible d'effectuer des envois groupés aux personnes qui se sont abonnées à la liste (**subscribe**).

Les agendas de groupe

Les agendas permettent de planifier une réunion et de gérer les plannings individuels et 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 permet de libérer son esprit sur des questions de fond plutôt que de formes. L'organisation de réunions, la vérification de la **disponibilité** des personnes, et l'incorporation automatique de la réunion dans tous les agendas individuels.

Il existe différents produits d'agenda de groupe, mais ils ne sont pas encore standardisés par **l'IETF** (Internet Engineering Task Force). Les produits **ICAL** (Internet Calendaring Standard), **ICAP** (Internet Calendar Access Protocol) et **SSTP** (Simple Scheduling Transport Protocol) permettent d'organiser des réunions via internet.

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 ou les employés. La consolidation des informations en base de données permet de faire des **recherches** en fonction de différents critères (nom, adresse, rendez-vous, appels téléphoniques, lettres, Chiffre d'Affaire, salaire, compétences, hobbies).

Les logiciels de gestion des contacts ne sont pas encore normalisés par l'IETF (ACT! de Symantec, Commence de Commence Corporation ou Gold Mine).

Les logiciels de groupware

Les logiciels de productivité (**groupware**) sont des outils de travail collaboratif. Par exemple, les **BBS** (Bulletin Board Systems) sont des systèmes de tableau d'affichage sur lequel plusieurs utilisateurs

peuvent simultanément dessiner. Les conférences interactives (**visioconference**) permettent de se voir et de s'entendre à distance.

Les applications Lotus Notes permettent d'organiser globalement les communications et les échanges entre tous les collaborateurs d'une même organisation. Les meilleurs systèmes de groupware sont capables de fonctionner dans un **environnement hétérogène**.

Les outils de travail collaboratif (groupeware)	
Communication	Envoyer des messages Planifier des conférences de groupe Échanger des documents
Coordination	La centralisation en temps réel des documents de travail du groupe L'accès simultané à un document pour les membres d'un groupe de travail La composition de documents «liés» à plusieurs sources
Organisation	La gestion de projet Le suivi des procédures et des tâches La gestion des relations clients, fournisseurs, partenaires, associés, employés La constitution des membres d'un groupe de travail

Les applications Lotus Notes

Les applications Lotus Notes représentent un système de groupware complet et cohérent. Les applications Lotus Notes apportent des fonctionnalités spécifiques au travail en groupe, comme l'administration, la connexion, les services d'annuaire, la gestion des documents, la réplication, la sécurité. Les applications Lotus Notes sont compatibles avec pratiquement tous les environnements.

Le journal de bord de l'administrateur

L'administrateur réseau se doit d'être prévoyant, et pour le prouver, il devrait tenir un journal de bord contenant toues les informations relatives aux matériels et aux logiciels sur son réseau! Le journal de bord permet de garder une trace papier de l'évolution de l'infrastructure et des différentes interventions.

Le journal de bord peut être une aide précieuse en situations critiques et charnières.

PRINTER

Les imprimantes réseaux

Les travaux d'impression initialisé par un utilisateur passe par plusieurs étapes avant d'être reçu par le périphérique d'impression (**device**), communément appelé «l'imprimante». Le terme «d'imprimante» peut également être employé pour désigner le fichier (**spool**) 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 par l'intermédiaire d'un serveur d'impression ou directement relié au câble du réseau, il s'agit alors d'une véritable «imprimante réseau» avec une carte réseau (**interface**), un processeur (**processor**) et de la mémoire vive (**memory**).

Le processus d'impression en réseau

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

Le processus d'impression en réseau
L'utilisateur utilise une application exécutée localement sur son ordinateur
L'utilisateur déclenche un travail d'impression (une **requête** d'impression)
La commande d'impression est interceptée par le **système** d'exploitation
Le travail d'impression est envoyé vers la carte **réseau** qui le place sur le câble du réseau
Le travail d'impression circule sur le réseau
Le serveur ou le **périphérique** d'impression réseau réceptionne le travail d'impression
Le travail d'impression est stocké dans une file d'attente ou **spooler**
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

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 peut être une mémoire tampon appartenant à la mémoire vive du serveur d'impression 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.

Le partage de l'imprimante 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. Plusieurs **périphériques** d'impression peuvent dépendre du même serveur d'impression.

La procédure de partage d'un périphérique réseau dépend du **système** d'exploitation, mais comporte en général certaines actions indispensables. En premier lieu, l'administrateur des imprimantes procède à l'installation **matérielle** du périphérique d'impression, puis à l'installation **logicielle** qui consiste à copier le **pilote** du périphérique d'impression. Ensuite il désigne le périphérique avec un **nom de partage** compréhensible et intuitif pour les utilisateurs, et un fichier de **spool** pour stocker les travaux d'impression. Enfin, il installe le **pilote** ou le client sur les **stations** des utilisateurs, et configure le paramétrage du **format** des travaux d'impression afin que ceux-ci soient conformes à ce que peut «comprendre» le périphérique d'impression.

L'administration de l'imprimante

L'administration du périphérique d'impression est souvent conférée à une autre personne que l'administrateur du réseau. Dans tous les cas, il est préférable l'administrateur de l'imprimante ou l'opérateur d'impression soit une personne disponible, responsable et que son lieu de travail soit tout près du périphérique, afin de pouvoir résoudre le plus rapidement possible les incidents.

Les incidents fréquents sur une imprimante sont l'alimentation électrique, l'alimentation en encre (cartouches pour les imprimantes à jet d'encre et toners pour les imprimantes lasers), l'alimentation en papier (il faut assez de place à coté de l'imprimante pour stocker les cartons de papier), le débourrage de papier, la récupération des imprimés dans le bac de sortie (il faut placer l'imprimante près des utilisateurs pour ne pas "perdre" son temps à aller chercher sa copie).

La surveillance des performances de l'imprimante réseau et la collaboration avec l'administrateur du réseau pour résoudre les autres problèmes et faire remonter la satisfaction des utilisateurs, sont des tâches quotidiennes qui incombent à l'administrateur de l'imprimante. Il ne faut pas oublier que les utilisateurs doivent avoir le droit d'imprimer, et que l'administrateur de l'imprimante doit avoir les droits et les permissions correspondant à ses responsabilités.

Les langages de description de page

Les langages de description de page ou **PDL** (Page Description Languages) permettent au périphérique d'impression de suivre les instructions qui figurent dans tout travail d'impression. L'impression d'un document dans un format texte est appelé brute (**raw**). Le langage de description de page constitue un 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. Le langage **PCL5**.

Les polices de caractères peuvent être, soient des **"polices bit-map"** qui ont été conçues avec certaines tailles, et qui sont définies à l'intérieur d'une matrice, soient des **"polices vectorielles"** qui sont «extensibles» à volonté puisqu'elles sont définies par une formule mathématique.

La police **TrueType** de la société Apple et la police **Postscript** de la société Adobe sont des polices de caractères vectoriels. 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.

La 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 (**fax**) est relié à un «modem partagé», lequel est relié au réseau téléphonique **RTC** (Réseau Téléphonique Commuté).

Le serveur de télécopie

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 permet de limiter les appareils et de filtrer les télécopies **publicitaires**. Les télécopies sont des documents qui ont une valeur juridique, aussi est-il important de surveiller les télécopies entrantes et sortantes. Certains serveurs de télécopie permettent d'associer le **numéro** de téléphone d'un utilisateur à son **adresse** électronique sur l'intranet, ainsi les télécopies sont dispatchées, ou routées automatiquement vers l'utilisateur final.

Le serveur de télécopie peut être une source de gain de **temps** pour les utilisateurs qui travaillent beaucoup avec ce moyen de communication. Les utilisateurs n'ont plus besoin de se déplacer vers le fax, ni la contrainte d'attendre à coté du fax.

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 expéditeurs des télécopies provenant de l'extérieur ne peuvent pas savoir si le site de destination est organisé autour d'un intranet, aussi 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 est **manuel** quand une personne se consacre régulièrement à transférer les télécopies vers leur destinataire, mais ce n'est pas une solution très opérationnelle, ni très confidentiel. Le routage est informatisé quand c'est une procédure automatique qui fait le routage. Il existe différentes solutions, comme la lecture de la télécopie (OCR, ICR), le pré routage (T.30, NEST, TSI) ou le pré adressage (RFL, SDA).

L'utilisation d'un logiciel de reconnaissance optique de caractères ou **OCR** (Optical Character Recognition) permet de convertir l'image de la page de garde en document numérique textuel. Ensuite, il faut automatiser les tâches de recherche et de lecture du champ «destinataire» de la télécopie dans le document numérisé. Quand le nom du destinataire est identifié et associé à son adresse électronique sur le réseau, alors, la télécopie peut être convoyé vers la bonne personne. L'utilisation d'un logiciel de reconnaissance intelligente de caractères ou **ICR** (Intelligent Character Recognition) permet de convertir le texte de la page de garde et d'effectuer directement la recherche sur 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, comme le routage **TSI** (Transmission Station Identification) permet d'utiliser le numéro du télécopieur de l'expéditeur pour router la télécopie vers son destinataire.

Le routage **RFL** (Received Fax Line) utilise plusieurs modems et plusieurs numéros de téléphone. Les télécopies adressées à un certain numéro sont routées vers un groupe d'utilisateurs. La technique **SDA** (Sélection Directe à l'arrivée) utilise une ligne téléphonique spéciale (**trunk**) associée à plusieurs numéros 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.

Le logiciel FACSys 4.0 conçu par la société OPTUS SOFTWARE fournie une passerelle de télécopie qui route les entrées et qui sert de serveur pour les sorties. Les applications des utilisateurs, comme un traitement de texte, un tableur, une base de données ou une messagerie électronique intègrent la passerelle et peuvent dès lors servir de «**frontal**» pour le 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 reconnaît différents langages de description de page, comme **HP PCL** (Hewlett Packard Printer Control Language) ou le très répandu langage Postscript.

MAIL

La messagerie électronique

Le courrier électronique, la messagerie électronique, le mail, sont différentes dénominations pour désigner l'outil de communication le plus connu et le plus coutumier des utilisateurs 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 facile, pratique et écologique. L'ère du «**zéro papier**» est indispensable pour arrêter la pollution de la planète (**ecology**).

Le courrier électronique peut être restreint à une zone ou élargie au monde entier. La messagerie interne (**intranet**) est installée à l'intérieur d'une entreprise et exclusivement réservée aux employés de l'entreprise. Le service de messagerie interne est géré par le service informatique de l'entreprise. La messagerie externe (**internet**) permet la communication avec les personnes à l'extérieur de l'entreprise. Le service de messagerie externe est géré par un fournisseur extérieur (Hotmail, Google Mail).

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 faut parfois installer des **passerelles** de messagerie pour convertir les messages d'une messagerie à l'autre, d'une plate-forme de communication à une autre. L'administrateur du réseau peut désigner un «administrateur de messagerie».

L'adresse 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 (**mail address**), une adresse de messagerie qui les identifie individuellement sur le réseau. Pour avoir une adresse électronique, il faut disposer d'un compte (**login**) et d'un mot de passe (**password**) sur un serveur de messagerie.

L'origine de la messagerie électronique

L'e-mail (**electronical mail**) est dès l'origine une fonction de base des systèmes Unix™. Il s'agissait d'un automate de copie (**copy**) de fichier d'un disque dur vers un autre disque dur sur un ordinateur distant (**remote**). Il existait différentes versions de cet automate. Afin d'harmoniser les outils, Eric Altman écrivit un programme de messagerie appelé «**sendmail**».

Au départ, les e-mails étaient simplement du texte. **L'IETF** (Internet Engineering Task Force)

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.

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 **notification** personnalisée prévient en temps réel le destinataire qu'un courrier vient de lui parvenir. 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 d'une copie du même message peut être envoyé automatiquement vers un autre destinataire en remplissant le champ **CC** (Carbon Copy). L'absence de bureau ou **OOF** (Out of Office) permet d'indiquer aux correspondants que le destinataire de leur courrier n'est pas là et qu'il reviendra bientôt pour consulter sa messagerie.

Les fonctionnalités de la messagerie électronique
La notification personnalisée des messages entrants (**notification**)
L'accusé de réception informe l'expéditeur que son message est bien arrivé (**ack**)
La réponse à un courrier peut inclure le message d'origine (**conversation**)
Les pièces jointes annexées au message peuvent être de tous les formats (**mime**)
L'envoi de copie vers un autre destinataire (**carbon copy**)
L'expédition groupé d'un même message à plusieurs destinataires (**mailing list**)
L'annuaire répertorie tous les abonnées au service de messagerie (**directory**)
La récupération des messages effacés par erreurs (**recovery**)
L'envoi de réponses automatiques (**out of office**)

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'exploitations différents peuvent s'échanger des messages, s'ils respectent les recommandations de l'OSI. Il existe différentes normes pour le courrier électronique correspondant à des systèmes de messageries différents. Les systèmes de messagerie utilisant des normes différentes (par exemple entre différents **opérateurs** téléphoniques ou entre différents **fournisseurs** 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.

Les normes de messagerie électronique
X.400 élaboré par le **CCITT** (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 CCITT, 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 Unices 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 serveurs MHS servent de passerelles et convertissent les messages provenant de systèmes de messageries différents.

Les messageries propriétaires

Il existe des applications de messagerie «propriétaire» développées par des sociétés informatiques (CC:MAIL de Lotus, Microsoft Mail de Microsoft et **MHS** (Mail Handling System) de Novell). Les différents produits de ces différentes sociétés sont généralement plus faciles à mettre en œuvre que «**sendmail**» qui est un logiciel libre parmi d'autres (**Postfix**, **Majordomo**). Les messageries propriétaires sont généralement incompatibles entre elles. Fort heureusement, le besoin de communiquer et d'échanger des e-mails entre ces différents systèmes de messagerie suscita le désir chez ces sociétés informatiques propriétaires de développer 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-mails au format SMTP qui est le standard libre de la pile de protocole TCP/IP. Ces différentes conversions consomment des ressources et du temps, c'est pourquoi, il est préférable dès le départ d'utiliser un standard ouvert.

La messagerie libre

Les standards ouverts pour la messagerie électronique sur internet ont été définies par **l'IETF** (Internet Engineering Task Force).

Le protocole SMTP pour la partie serveur et les protocoles POP3 et IMAP4 pour les clients sont des

protocoles qui font partie de la pile de protocoles de TCP/IP.

Le protocole SMTP correspond à la partie serveur du service de messagerie, celle qui stocke les e-mails sortants des utilisateurs. Le protocole **SMTP** (Simple Mail Transfert Protocol) route le courrier entre les différents serveurs de messagerie sur 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 nœuds intermédiaires. SMTP est simple d'utilisation pour les utilisateurs qui n'ont qu'à fournir le nom du destinataire et le nom de domaine. Le nom du destinataire est rattaché au nom de domaine (login@domaine.tld) par un A commercial (**arrobase**).

Les protocoles POP 3 et IMAP 4 correspondent à la partie cliente du service de messagerie, celle qui reçoit les e-mails entrants. Avec POP3, 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.

TOPOLOGY

La topologie des réseaux

La topologie **physique** des réseaux considère les réseaux du point de vue de l'emplacement des matériels (câbles, postes, dispositifs de connectivité). La topologie **logique** des réseaux considère les réseaux du point de vue du parcours du signal électrique entre les différents matériels. La topologie logique détermine la manière dont les stations se partagent le support, c'est-à-dire la méthode d'accès au réseau. Par exemple, un réseau peut être considéré comme appartenant à une topologie en étoile, du point de vue de la disposition physique visible des câbles, alors qu'en réalité il appartient à une topologie en anneau, du point de vue logique.

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 réunit l'ensemble des postes, des serveurs, des périphériques, du câblage, des routeurs, des systèmes d'exploitations réseaux, des protocoles, et des adresses. 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 réseaux en bus, les réseaux en étoile, les réseaux en anneaux ou les réseaux mixtes (en bus étoile ou en anneau étoile). Physiquement, les réseaux en bus, en étoile et en anneau peuvent se ressembler beaucoup parce qu'ils peuvent être tous organisés autour d'un **boitier**. Selon la topologie logique, le boitier contient un bus, un concentrateur ou un anneau.

Les réseaux en bus

Les réseaux en bus sont aussi appelés réseaux en bus **linéaire**, en épine dorsale (**backbone**). Les différents postes ou périphériques du réseau sont reliés à un seul et même câble qui constitue un tronçon (**trunk**) ou un segment. A toutes les extrémités du câble est fixé un bouchon (**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 couteux, facile à mettre en place et à maintenir. Si une machine tombe en panne sur un réseau en bus, alors le reste du 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.

Les réseaux en étoile

Dans un réseau en étoile, les postes disposent de leur propre câble et tous les câbles sont reliés à un même boitier. Le **boitier** fait office de concentrateur (**hub**) pour un seul sous réseau ou de commutateur (**router**) pour plusieurs sous réseaux.

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 stations des réseaux en étoile peuvent être facilement enlevées ou déplacées.

Les concentrateurs

Le **concentrateur** centralise tous les échanges (**hub**), et toutes les communications passent au travers du concentrateur. Les concentrateurs sont des **répéteurs**. Ils régénèrent le signal électrique, et le retransmettent simultanément à tous les ports (comme un répéteur multiport). Un concentrateur peut posséder 8 ou 10 ports, et les ports peuvent être de différents types (concentrateurs hybrides). Les concentrateurs améliorés (**switch**) sélectionnent les stations auxquelles ils retransmettent des données.

Les commutateurs

Les **commutateurs** segmentent le réseau en sous réseaux et filtrent les paquets. Les commutateurs (**router**) permettent de créer des sous réseaux indépendants les uns des autres. 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**) et qui en 10 minutes enregistrent les adresses MAC des nœuds du réseau.

Un commutateur peut être relié à plusieurs concentrateurs, en **cascade** (à l'aide de câbles **UPLINK**), 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 réseaux en anneau

Les réseaux en anneau sont constitués d'un **boitier** à l'intérieur duquel se trouve un circuit qui forme une **boucle** logique. Les boitiers pour les réseaux en anneau de type **Token Ring** sont appelés des **MAU** (Multistation Access Unit). En général, l'anneau se trouve à l'intérieur du boitier MAU et 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** (Fiber Distributed Data Interface).

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 règlemente, 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 renvoie un accusé de réception.

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

L'organisation des réseaux

D'une manière plus générale, la **représentation** d'un réseau peut s'établir en fonction de la **circulation** de l'information. Ainsi, un réseau peut être **centralisé** (avec un point central qui détient toutes les données), **réparti** (avec plusieurs centres qui se partagent les données) ou **distribués** (sans centre, mais avec un maillage dense qui relie tous les postes, lesquels peuvent ou non partager leurs données). L'organisation d'un réseau peut être qualifiée d'autonome ou de hiérarchique.

Toutefois, ces notions didactiques et conceptuelles d'organisation doivent être comprises avec relativité et souplesse, parce qu'elles sont sujettes à l'évolution des capacités technologiques et des conceptions humaines du **partage** de l'information. Dans les réseaux centralisés, les rôles sont bien définies et bien séparés, il y a un gros ordinateur central et des **terminaux** passifs. Dans les réseaux distribués, les rôles peuvent être moins évidents, parce que les postes sont à la fois des **clients** et des **serveurs**.

Dans les premiers temps de l'informatique, uniquement le **mode** centralisé fut privilégié avec de gros ordinateurs centraux (**Main Frame**). Aujourd'hui, c'est plutôt le mode Clients Serveurs qui emporte la faveur des **architectes**.

L'informatique centralisée

Les premiers réseaux étaient **propriétaires** et centralisés. Ils étaient conçus, fabriqués et mis en œuvre par une seule société qui bénéficiait d'une situation de **monopole** (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, avec des contrats de maintenance et de fidélité sur plusieurs dizaines d'années. Ces réseaux fonctionnaient bien seuls, mais ils ne fonctionnaient pas avec d'autres réseaux.

L'architecture d'un réseau centralisé était conçu autour d'un ordinateur très puissant (pour l'époque) et de **terminaux** passifs qui n'avaient pour seule fonction que de transmettre les requêtes à un super calculateur central. Il existait donc une **dissymétrie** de taille entre les clients et le serveur, et une **dépendance** quant au sens de la circulation de l'information.

L'informatique distribuée

Désormais, la conception d'une machine et de sa place dans le réseau doit tenir compte de l'environnement et s'ouvrir aux autres technologies. L'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**.

Les environnements hétérogènes sont des environnements où cohabitent plusieurs types de machines, plusieurs systèmes d'exploitation, et plusieurs types de protocoles qui doivent coopérer et communiquer 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 y a moins de dissymétrie et de dépendance entre les clients et les serveurs.

Les réseaux postes à postes

Les réseaux postes à postes (**peer to peer**) sont également appelés des réseaux "point à point" ou "d'égal à égal". Dans les réseaux postes à postes chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de hiérarchie entre les postes ou 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. Chaque utilisateur décide lui-même des services sur son système et des partages sur son disque dur, ainsi que des permissions qu'il octroie aux autres utilisateurs.

Les réseaux client serveur

Les réseaux client serveur permettent de spécialiser les rôles. La plupart des machines sont des postes clients et quelques machines sont dédiées à une tâche qu'elle proposent à toutes les autres. Les machines dont se servent les utilisateurs sont appelées des **stations**, tandis que les autres machines sont appelées des **serveurs**. Les serveurs sont en général des machines plus puissantes et plus fiables parce qu'elles fonctionnent à plein régime et sans discontinuité.

Les échanges de données et les communications fonctionnent en mode **"clients serveurs"**, c'est-à-dire qu'il y a un logiciel client qui communique avec un logiciel serveur. Les logiciels clients sont installés sur les stations, et les logiciels serveurs sont installés sur les serveurs. Une machine peut être qualifiée de serveur quand un logiciel serveur y tourne.

Le **système** d'exploitation du serveur peut être différent de celui des stations clientes. Il suffit que les stations soient équipées d'un logiciel client compatible. Le système d'exploitation du serveur doit être

véritablement multitâches et stable 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 serveurs sont en général **dédiés** à une certaine tâche. Il existe des serveurs de fichiers, des serveurs d'impression, des serveurs d'applications, des serveurs de base de données, des serveurs de messagerie, des serveurs de télécopies, des serveurs internet, des serveurs d'authentification qui gèrent la base des comptes des utilisateurs.

Les systèmes d'exploitations réseaux multi tâches et clients serveurs
Les systèmes Windows™ NT Server et Windows™ 2000 de Microsoft
Le système NetWare de Novell
Le système OS/2 d'IBM
Les systèmes Mac OS X d'Apple
Les systèmes Unix™ propriétaires (Solaris, HP-UX, Ultrix, AIX)
Les systèmes libres FreeBSD, Open BSD et Net BSD
Le système libre Gnu Linux sous licence Gnu GPL (General Public Licence)

Les avantages des réseaux clients serveurs

L'avantage des réseaux clients serveurs est de réunir deux avantages complémentaires, l'indépendance des utilisateurs et la centralisation de l'administration. **L'indépendance** des utilisateurs est assurée parce qu'ils peuvent ouvrir des sessions localement sur des stations qui travaillent en mode autonome, et parce que toutes les communications se passent directement de clients à serveurs.

La **centralisation** de l'administration est réalisée parce qu'un administrateur compétent peut configurer les serveurs comme il l'entend, répartir la charge des requêtes, automatiser les mises à jour des applications et les sauvegardes des données, uniformiser la configuration pour un grand nombre de postes, planifier l'évolution du réseau, et décider de la stratégie de sécurité adaptée.

Les avantages du modèle client serveur
L'architecture réseau la plus répandue
Les matériels les plus compatibles
Le cout relativement bon marché de la plate-forme
La capacité de traitement comparable aux grands systèmes
La réduction du trafic réseau
La répartition des tâches entre les clients et les serveurs
La personnalisation des configurations
L'installation d'applications partagées
L'indépendance des utilisateurs
La centralisation de l'administration, de la stratégie de sécurité, de la maintenance, des sauvegardes
La centralisation des fichiers
La souplesse et la puissance des infrastructures

Le modèle client serveur

Le modèle client serveur met en jeu deux ordinateurs qui communiquent ensemble. L'un des ordinateurs joue le rôle du client, avec un logiciel client (**client**), et l'autre joue le rôle du serveur, avec un logiciel serveur (**server**). Le modèle client serveur est apparu grâce aux progrès technologiques qui a permis de transformer les terminaux dépourvus d'intelligence, en de véritables ordinateurs avec une véritable capacité de traitement (**processor**), de stockage (**data**), de présentation (**graphic**) et de communication (**network**). Le modèle client serveur est le **compromis** entre l'informatique centralisée et hiérarchique des architectures propriétaires, et l'informatique décentralisée et anarchique des réseaux poste à poste. Le modèle client serveur est plus souple tout en restant contrôlé.

Dans une organisation de type client serveur classique, les fichiers sont généralement centralisés sur un serveur, et la totalité de l'architecture du réseau repose sur un ou plusieurs serveurs **dédiés**. Dans une organisation moins conventionnelle, certaines stations peuvent faire office de clients et de serveurs en même temps. Les machines peuvent être configurées selon les besoins et disposer de logiciels clients hétérogènes et de plusieurs protocoles (**dual stack**).

Pour autant, quand un client fait appèle 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 **partage** le travail. Les serveurs peuvent être dédiés à une ou plusieurs tâches spécialisées.

La spécialisation des serveurs
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 des connexions à distance
Les serveurs de sauvegarde
Les serveurs de base de données

Les spécifications d'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 et que les administrateurs de base de données recherchent toujours plus de puissance et plus d'espace de stockage. Les composants les plus rapides, les plus chers et les plus

résistants seront toujours préférés. Les sauvegardes et la redondance des données seront également étroitement surveillée.

Les spécifications techniques d'un serveur de base de données
La largeur et la fréquence du bus de la carte mère (**mother board front side bus**)
Le nombre et la fréquence des processeurs (**processor frequency**)
La quantité et la fréquence de la mémoire vive (**working memory**)
Le nombre et la capacité des disques durs (**hard disk capacity**)
Le temps d'accès aux disques appelé le débit entrée / sortie (**throughput**)
Le nombre et la fréquence des cartes réseaux (**network interface**)
Le débit du câblage (**network bandwidth**)

Un exemple de requête SQL

L'application la plus utilisée en mode Clients Serveurs 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 plus part des bases de données est le langage **SQL** (Structured Query Language). Le langage SQL est un langage d'interrogation structuré qui a été conçu par la société IBM. Le langage SQL est devenu une norme et un standard dans le monde des bases de données.

Les composants du modèle Client Serveur sont le client, aussi appelé le **frontal** (Front End) et le serveur, aussi appelé le **dorsal** (Back End). Les tâches sont réparties entre le client et le serveur (le client affiche, tandis que le serveur calcule). Un outil de **programmation** permet de programmer des frontaux et de personnaliser les accès et les requêtes auprès d'une base de données.

Le serveur exécute l'application de base de données localement, mais n'exécute pas d'application pour gérer l'interface utilisateur. Le serveur supporte la **charge** et le traitement des requêtes des utilisateurs. Généralement, c'est aussi le serveur qui stocke les informations de toute la base de données, mais il peut arriver qu'elles soient stockées sur une ou plusieurs autres machines. Le serveur de la base de données s'occupe également de l'enregistrement des modifications des données (ajouts, suppressions) 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, les données sont centralisées dans un seul endroit (**Data Warehouse**) qui contient toute la base, tandis que les autres ordinateurs n'en contiennent 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.

Un exemple de requête SQL en mode client serveur
L'utilisateur souhaite faire une **demande** à la base de données
L'utilisateur ouvre le **logiciel client** ou **l'interface** client correspondant à la base de données
L'utilisateur rédige sa demande avec des **clefs** de recherche dans un **formulaire**
Le **logiciel client** traduit la demande en **requête SQL**
Le **logiciel client** envoie la requête SQL au système de la machine cliente avec l'adresse du serveur
Le **système** de la machine cliente formate la requête SQL en paquets TCP-IP pour le protocole réseau
La **machine** cliente envoie les paquets TCP-IP à la machine serveur sur le réseau TCP-IP
Le **réseau** TCP-IP transporte les paquets TCP-IP vers la machine serveur qui exécute la base
La **machine** serveur accepte les paquets TCP-IP provenant de la machine cliente
Le **système** de la machine serveur formate les paquets TCP-IP en requête SQL pour le logiciel serveur
Le **système** de la machine serveur transmet la requête SQL au logiciel serveur de la base
Le logiciel serveur de la base de données reçoit la requête SQL
Le **moteur** de la base de donnée traite la **requête SQL**
Le **moteur** de la base de donnée extrait et trie **les enregistrements des tables de la base de données**
Le **moteur** de la base de donnée sélectionne la **réponse SQL**
Le logiciel serveur de la base de données envoi au système la réponse SQL avec l'adresse du client
Le **système** de la machine serveur reçoit la requête SQL du logiciel serveur de la base
Le **système** de la machine serveur formate la réponse SQL en paquets TCP-IP pour le protocole réseau
La **machine** serveur envoie les paquets TCP-IP à la machine client sur le réseau TCP-IP
Le **réseau** TCP-IP transporte les paquets TCP-IP jusqu'à la machine cliente qui en a fait la demande
La **machine** cliente accepte les paquets TCP-IP provenant de la machine serveur
Le **système** de la machine cliente formate les paquets TCP-IP en réponse SQL pour le logiciel client
Le **logiciel client** reçoit **la réponse SQL** provenant du système de la machine cliente
Le **logiciel client** converti la réponse SQL et la présente à l'utilisateur
L'utilisateur visualise la réponse SQL
L'utilisateur ferme le client de la base de données
L'utilisateur s'interroge sur la signification du résultat, en déduit des solutions, et lance des initiatives

L'influence des normes

Les normes établies par les organismes internationaux, et particulièrement les organismes américains de normalisation, ont contribué à favoriser l'ouverture des architectures propriétaires, la convergence des pratiques, et 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 pouvait 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 accélérés le développement des normes pour les réseaux. Les normes concernent tous les aspects de l'informatique. Les matériels doivent être assemblés. Les logiciels qui doivent fonctionner ensembles. Et même les personnels doivent travailler selon des **certifications**.

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 (**market shares**). Aujourd'hui, la conformité aux normes est presque un impératif. Les **normes** correspondent à la publication d'une certaine technologie par des organismes officiels, tandis que les **standards** correspondent à une reconnaissance de l'industrie ou à une adoption par les utilisateurs d'une certaine technologie.

Les organismes de normalisation

Les principaux organismes de normalisation sont soutenus par les grandes entreprises de **l'industrie** informatique. Les organismes de normalisation peuvent être constitués de différentes manières (administrateurs des services de l'état, professeurs des universités, chercheurs des instituts de recherche, directeurs ou représentant des **consortiums** d'entreprises privées).

OSI

Le modèle OSI

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

Le modèle **OSI** (Open Systems Interconnection) est un modèle **théorique** qui présente une méthode générale pour l'interconnexion des systèmes ouverts. Le modèle ISO décrit un ensemble de spécifications et de procédures pour une architecture réseau permettant la connexion d'équipements hétérogènes et la communication des applications clients serveurs. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer une communication réseau. Le modèle OSI est organisé en **7 couches** successives.

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.

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 afin que celles-ci s'acheminent correctement vers l'ordinateur **récepteur**. Les données sont transmises sur le **support** de communication du réseau.

L'activité de communication des réseaux								
Émetteur	**Message**	**Code**	**Support**	**Signal**	**Support**	**Decode**	**Message**	**Récepteur**

La parabole de Cendrillon

L'activité d'un réseau ressemble à l'activité de la belle Cendrillon. La belle Cendrillon suit des **règles** très précises de séduction auxquelles elle ne déroge jamais. D'abord, Cendrillon choisit ses vêtements, puis s'habille et se maquille. Ensuite, la belle demoiselle monte dans son beau carrosse conduit par de magnifiques chevaux blancs qui arpentent les vallées giboyeuses du royaume. Arrivée au palais du prince, la belle Cendrillon descend de son carrosse et entre dans la salle de bal, où elle danse toute la soirée (la valse, la polka ou le rock & roll). Enfin, quand la belle Cendrillon s'est bien fait remarquée par son prince, elle s'éclipse avant le douzième coup de minuit, laisse l'un de ses escarpins en souvenir, et rentre chez elle pour se déshabiller, et s'endormir plein de rêves de princesse (nous resterons discret sur les activités nocturnes qu'elle pût avoir par la suite avec son prince charmant).

Effectivement, Cendrillon se comporte de la même façon que les données qui sont transmises sur un réseau (et nous resterons tout aussi discret sur la nature des messages et les intentions des utilisateurs qui les réceptionnent). Dans un premier temps, les **données** sont transformées en **paquets** par l'ordinateur expéditeur. Dans un deuxième temps, les **trames** défilent sur le support de communication et parcourent le chemin jusqu'au destinataire. Dans un troisième temps, l'ordinateur récepteur récupèrent les trames, et retransforment les paquets pour qu'ils redeviennent des données présentables. Et la même séquence se produit pour effectuer le chemin du retour(quand c'est la princesse qui invite au bal).

Les couches du modèle OSI

Le modèle OSI est un modèle théorique de communication réseau entre deux machines. Les couches du modèle OSI se retrouvent donc chez les deux machines. Chez l'expéditeur, les données à transmettre par l'application réseau émettrice, descendent les sept couches, pour être transformées, et envoyées sur le réseau sous forme de trames. Chez le destinataire, les trames sont reçues, et remontent les sept couches, pour être transformées, et présentées en données compréhensibles pour l'application réseau réceptrice.

La transformation des données et de leur cheminement sur le réseau avec le modèle OSI			
Ordinateur émetteur (source)		**Ordinateur récepteur** (target)	
APPLICATION	Données (**data**)	Données (**data**)	**APPLICATION**
PRESENTATION	Format (**format**)	Format (**format**)	**PRESENTATION**
SESSION	Processus (**process**)	Processus (**process**)	**SESSION**
TRANSPORT	Paquet (**segment**)	Paquet (**segment**)	**TRANSPORT**
NETWORK	Datagramme (**header**)	Datagramme (**header**)	**NETWORK**
LIAISON	Trame (**trailer**)	Trame (**trailer**)	**LIAISON**
PHYSICAL	Signal (**flux**)	Signal (**flux**)	**PHYSICAL**
Support de communication			

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. 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 théorique **OSI** en 7 couches. Les

spécifications de la norme **IEEE 802** en définit les particularités pratiques et techniques.

L'application réseau (**client**) fait appel aux fonctions réseaux du système. Le système d'exploitation réseau identifie les données à transmettre (**data**) et les passe au protocole réseau (**tcp-ip**) qui se charge de les préparer en suivant les recommandations du modèle OSI. Le protocole (**protocol**) segmente les données en paquets (**packets**), y adjoint des informations réseaux, comme l'adresse de l'expéditeur (**source**) et l'adresse du destinataire (**target**) et des informations pour leur bon acheminement, comme les bits de synchronisation (**sync**), de contrôle (**control**), et de réception (**ack**). Quand les trames sont prêtes, la carte réseau (**interface**) les expédie sur le réseau (**network**), et celles-ci cheminent (**route**) sur le support de communication (**cable**) jusqu'à la carte réseau de l'ordinateur destinataire (**server**).

L'architecture 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 logicielles de l'ordinateur émetteur traversent chacune des ces 7 couches (**de haut en bas**) pour être transformées en paquets avant d'être transmises sous la forme de trames au support de communication. Arrivées à destination, les trames traversent chacune des ces 7 couches (**de bas en haut**) pour que les paquets soient transformés et présentées au logiciel de l'ordinateur récepteur.

L'architecture du modèle OSI		
Numéro	**Nom**	**Fonction**
7	**APPLICATION**	Une **interface** pour l'accès au réseau (ftp, mysql, postfix,ssh)
6	**PRESENTATION**	Le **format** des données (ascii, compression, LF, CR)
5	**SESSION**	La gestion des processus d'une **connexion** (control)
4	**TRANSPORT**	L'assemblage des **paquets** (size, order, Ack, ECC)
3	**RESEAU**	L'adressage et le **routage** (@ip, @mac, MTU, hops, trafic)
2	**LIAISON**	La gestion des **trames** (Ack, CRC)
1	**PHYSIQUE**	La gestion des **signaux** sur le câble (interface, length, sync)
Le support physique		

La succession des couches

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 enlevées du paquet). Chaque couche s'occupe de l'habillage pour une

transmission et du déshabillage pour une réception.

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 différent de ceux des autres couches. Chaque couche prépare les données pour la couche suivante. On dit que les couches **homologues** communiquent entre elles. Les couches **adjacentes** (supérieure et inférieure) communiquent également entre elles. Les couches adjacentes forment une frontière qui les sépare les unes des autres et qui 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 & 2 sont appelées les couches **basses**, et leur fonction est d'envoyer des flux de bits sur le réseau.

Les couches homologues

Les couches **homologues** sont les deux couches d'un même niveau, l'une située sur l'ordinateur émetteur et l'autre sur 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 travaille son homologue.

Les couches ont besoin de savoir exactement comment ont été transformé les données afin de pouvoir les restituer à l'identique et les communiquer à la couche adjacente. Même entre **protocoles** différents, les communications entre couches homologues sont règlementées afin d'assurer la **compatibilité** et la fonction que la couche est sensée réaliser.

Les couches adjacentes

Les couches adjacentes d'une couche sont les couches du niveau supérieur et inférieur. Par exemple, la couche TRANSPORT communique avec les couches adjacentes SESSION et RESEAU. Pour une **transmission**, les couches reçoivent les données de la couche supérieure et les transmettent à la couche inférieure. L'on dit que les couches rendent des **services** aux couches adjacentes, et qu'elles présente une interface pour recevoir les informations de la couche précédente..

Pour une **réception**, les couches reçoivent les données de la couche inférieure et les transmettent à la

couche supérieure. Entre chaque couche adjacente, se situe **l'interface** entre les deux couches. Cette interface obéit très précisément aux **règles** qui régissent le mode de transmission des données d'une couche à l'autre. La **pile de protocole** définit ses règles et l'agencement des différentes couches.

La symétrie des couches

Dans les processus de transformation des couches OSI, les données de l'ordinateur émetteur sont découpées en paquets. Les paquets passent de couches en couches. A chaque couche, des informations de **formatage** et d'**adressage** sont ajoutées au paquet. Enfin, 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 les trames ne transite par toutes les autres couches. Toutes les autres couches communiquent avec leur homologue par l'intermédiaire des couches qui les précèdent. Les informations sont pour ainsi dire filtrer à chaque **niveau** et transmises à la couche suivante, et ainsi de suite. S'il peut paraitre 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, et que chacune effectue le travail symétrique de l'autre.

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, Mysql, Mail, Postfix, Ssh), et correspond à l'affichage des informations dans l'interface de l'utilisateur.

Les fonctions de la couche APPLICATION	
La gestion des applications réseaux (l'interface de l'utilisateur)	
Les utilitaires de transfert de fichiers	(ftp)
Les logiciels d'accès aux bases de données	(mysql)
Les serveurs de messagerie électronique	(postfix)
Les serveurs de connexion distante	(ssh)
Le contrôle du flux et la correction des erreurs	

La couche PRESENTATION

La couche PRESENTATION (PRESENTATION LAYER) détermine le format des données à afficher (**format**). Le format utilisé pour l'échange des données entre les deux ordinateurs du réseau peut être

un format de compression (**compress**), un format de cryptage (**crypt**) ou tout autre format spécifique. Par exemple, la couche PRESENTATION est sensée afficher et convertir (**conversion**) convenablement les données d'un texte Unix™ dans un terminal MS-DOS™.

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 (ascii)
L'exécution des commandes graphiques
La compression ou la décompression des données

La couche SESSION

La couche SESSION (SESSION LAYER) gère la **connexion** entre deux ordinateurs du réseau. Deux processus distants communiquent par le réseau, l'un se trouve sur la station émettrice et l'autre sur la station réceptrice. En réalité, même si c'est bien l'une des stations qui, au départ, a initié la communication, les deux stations qui communiquent, échangent, envoient et reçoivent des données.

Les fonctions de la couche SESSION
L'ouverture et la fermeture d'une connexion (d'une session)
La reconnaissance des noms d'hôtes et des noms de domaine
La synchronisation des tâches accomplies par utilisateur à l'aide de points de contrôle
Le contrôle du dialogue entre les processus communicants (qui, à qui, quand, quoi, timing)

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 ré-assemblage des paquets ainsi que le contrôle et la correction des erreurs. La couche TRANSPORT correspond au protocole TCP (Transport Control Protocol).

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 accusée de réception
Le contrôle du flux et la correction des erreurs dans la reconstitution des paquets

La couche RESEAU

La couche RESEAU (NETWORK LAYER) se charge de **l'adressage** des messages. La couche RESEAU fourni un schéma d'adressage et de **routage**. La couche RESEAU traduit les adresses logiques (**@ip**) en adresses physiques des cartes réseaux (**@mac**). La couche RESEAU négocie la taille maximale des messages ou **MTU** (Maximum Transfert Unit), et s'occupe éventuellement du découpage ou du ré-assemblage des paquets. La taille des messages est décidée en fonction de la capacité maximale comparée de la carte réseau de l'émetteur et de celle de son correspondant. La couche RESEAU correspond au protocole **IP** (Internet Protocol).

Les fonctions de la couche RESEAU
La traduction des noms logiques et des adresses (@ip) en adresses physiques (@mac)
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 (TTL)
Le découpage ou le ré-assemblage des paquets en taille compatible (MTU)
messages en fonction de la capacité de la carte réseau (et de celle de son correspondant)

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 qui seront transmises sur le réseau. Une trame est composée d'une entête (**header**), d'un corps (**data**) et d'une queue (**trailer**). C'est au niveau de la couche LIAISON que la finalisation des paquets a lieue. L'enveloppe d'expédition est en quelque sorte fermée, et la queue (**trailer**) est rajoutée.

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'une trame
L'envoie et la réception d'un accusé de réception pour chaque trame, sinon la trame est réexpédiée

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 la carte réseau au support du câble
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'envoie des trames sur le réseau

La constitution d'une trame

La structure d'une trame est toujours la même (**headers**, **body**, **trailer**). Les **paquets** n'ont qu'une en-tête. Tandis que les **trames** sont construites avec une en-tête et une queue qui est rajoutée par la couche LIAISON. Toutes les couches du modèle OSI ajoutent leurs propres entêtes, la première entête d'une trame étant celle qui est rajoutée par la dernière couche, la couche PHYSIQUE.

La trame est constituée de plusieurs éléments et dans un ordre précis (au bit près). L'entête contient les informations d'adressage, de routage, de priorité et de segmentation. Le corps contient les données à transmettre (**encapsulation**). La queue contient les informations de contrôle des erreurs **CRC** (Cyclical Redundancy Check) pour la correction et la vérification des erreurs dans la transmission.

La constitution d'une trame		
L'entête (**headers**)	Informations de transmission (**talking**)	Alert
	Informations de synchronisation (**sync**)	Horloge
	Informations d'adressage (**addressing**)	Adresse du destinataire (@ip, @mac) Adresse de l'expéditeur (@ip, @mac)
	Informations de routage (**routing**)	Détection du type de trame Routage et priorité Segmentation des données
	Informations des couches (**heading**)	Encapsulation des couches OSI (**headers**)
Le corps (**body**)	Les données (**data**)	Encapsulation de données (**crypt**)
La queue (**trailer**)	Informations d'intégrité (**check**)	CRC (Cyclical Redundancy Check)
	Informations de contrôle (**control**)	Synchronisation des sessions (**timing**)

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 sortie 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, dont la carte réseau et le câblage en coaxial ou en paire torsadées. La norme 802 a été présentée en douze catégories correspondant chacune à un type de réseaux. Le modèle IEEE 802 précise les caractéristiques techniques des couches LIAISON et PHYSIQUE. La couche LIAISON est divisée en deux sous couches, la sous couche **LLC** (Logical Link Control) et la sous couche **MAC** (Media Access control).

Les catégories du modèle IEEE 802

Les normes IEEE 802 pour les réseaux	
Norme	**Caractéristiques** (types de réseaux et couches)
802.1	Le fonctionnement inter réseaux en général (Internet Working)
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 intégrants 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

Les sous-couches LLC et MAC

Les deux couches basses du modèle OSI sont les couches LIAISON et PHYSIQUE qui définissent la façon dont plusieurs ordinateurs peuvent utiliser simultanément le réseau sans interférer les uns avec les autres. C'est la **méthode d'accès au réseau**. Le comité de normalisation 802 a voulu définir en détail

ces deux couches et en préciser les caractéristiques pour chaque **type de réseaux**.

La couche LIAISON a été divisée en **deux sous couches**. La sous-couche Contrôle des Liaisons Logiques ou **LLC** (Logical Link Control), et la sous couche Contrôle d'Accès au Support ou **MAC** (Media Access control).

Les sous-couches LLC et MAC
La sous-couche Contrôle des Liaisons Logiques ou **LLC** (Logical Link Control) Charger de contrôler le flux des données Responsable de l'interface Points d'Accès aux Services ou **SAP** (Services Access Point)
La sous-couche Contrôle d'Accès au Support ou **MAC** (Media Access control) Charger de mettre en forme les trames en fonction de la méthode d'accès au réseau Charger de contrôler l'accès au réseau et les erreurs de transmission des paquets Responsable du transfert sans erreurs des données entre deux ordinateurs Communique directement avec la carte réseau

Les couches basses de la norme 802

Certaines normes de la spécification 802 qui caractérisent les spécificités des types de réseau s'implémentent à l'intérieur des sous-couches LLC ou MAC.

Les couches basses de la norme 802		
Les sous-couches	**Les normes spécifiques**	**La norme générale**
LLC	802.1 La gestion des réseaux	802.1 La gestion des réseaux
	802.2 LLC	
MAC	802.3 CSMA/CD	
	802.4 Bus à jeton	
	802.5 Anneau à jeton	
	802.12 Priorité de la demande	

La segmentation 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 **chaines** des données d'origine est souvent trop importante et peut pénaliser **l'efficacité** des transmissions sur 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 de **partage** et d'interactivité n'est plus fonctionnelle.

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 qui sont appelées des paquets (**packets**) ou des segments (**segments**).

Les appellations des paquets

Les termes de paquet, de segment, de datagramme, de cellule, de frame, de trame sont confusionellement employés pour désigner les données ou les messages qui sont envoyés sur le réseau. En réalité, chacun de ses termes correspond à une réalité bien précise, et l'usage qui en est fait, est surtout un abus de langage.

Le terme de **paquet** peut convenir, en général, pour qualifier les données ou les messages dans le processus de transmission réseau. Les paquets n'ont qu'une entête et l'usage devrait réservé strictement l'expression pour la transformation des données dans le cadre des couches TRANSPORT et NETWORK du modèle OSI.

Le terme de **segment** est plus approprié pour désigner un paquet qui est découpé dans une taille uniforme, et ordonné lors du processus de segmentation des données de la couche TRANSPORT. Le terme de **datagramme** est plutôt qualifié pour mentionner la structure d'un paquet, avec son entête et ses drapeaux qui paramètrent sa circulation sur le réseau, et ses entêtes qui sont ajoutées lors du processus d'encapsulation des différentes couches du modèle OSI. Le terme de **cellule** peut être considéré comme un synonyme de datagramme, parce qu'il met en exergue la structure identique de tous les paquets, et leur dimension commune, mais c'est une expression surtout employée pour les réseaux ATM.

Enfin, le terme de **trame** explicite la finalisation d'un paquet avec la dernière enveloppe. Les **paquets** n'ont qu'une en-tête. Tandis que les **trames** sont construites avec une en-tête et une queue lors du processus de finalisation de la couche LIAISON du modèle OSI. Les trames sont généralement formalisées par le pilote (**driver**) de la carte réseau. Les analyseurs de trames (**sniffer**) sont des outils qui écoutent la circulation des trames brutes sur le réseau. Le teme de **frame** peut être considéré comme un synonyme de trames, dans le sens où il correspond à ce qui peut être écouté sur un support de communication, mais c'est une expression qui est plutôt employée dans les réseaux à Relais de Trames (Frame Relay).

La transmission des trames

Les trames sont en quelque sorte l'unité de base des communications réseaux. La division des données en paquets puis en trames accélère la transmission globale des données de tous les utilisateurs. Les données sont segmentées chez l'émetteur puis rassemblées chez le récepteur. Les paquets sont ordonnés

(**order**), vérifiés (**check**) et réceptionnés (**ack**). Les paquets n'arrivent pas toujours chez le destinataire dans le bon ordre, mais l'ordre est reconstitué chez le destinataire pour chaque message.

L'intégrité de chaque paquet est vérifié par un calcul de **CRC** (Cyclical Redundancy Check). Quand un paquet est réceptionné, un **accusé de réception** est envoyé à l'expéditeur pour l'enjoindre à continuer la transmission avec les autres paquets.

L'encapsulation des couches

La segmentation des données en paquets commence dès la première couche (la couche 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. Toutes les couches du modèle OSI contribuent à la constitution du paquet.

Chacune des sept 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**. Toutefois, c'est la couche TRANSPORT qui segmente en paquets et qui détermine la taille d'un paquet. La taille des paquets est décidées en fonction du protocole utilisé, mais aussi des capacités respectives de la carte réseau de l'expéditeur et de celle du destinataire. L'on dit que c'est une **négociation**, mais en réalité, c'est la taille commune la plus élevée qui l'emporte. La taille des paquets est définie dans par la **MTU** (Maximum Transfert Unit). La taille des paquets peut être fixée entre 100 et 2000 Octets. En général, la bonne taille pour les communications RTC est de 500 Octets, et de 1536 pour les réseaux Ethernet.

La structure d'un paquet

Un paquet (**packet**) est toujours constitué de la même manière. Lors de la segmentation des données en paquets (**segment**), et lors de l'adressage de paquets (**datagramme**), certaines informations sont ajoutées aux paquets. 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 sont les entêtes (**headers**), le corps (**data**) et la queue (**trailer**).

L'important est de se souvenir que plusieurs types d'information sont transmises dans un paquet. Les informations transmises concernent la transmission (**alert**), la synchronisation (**horloge**), l'adressage (**@ip**, **@mac**, **source**, **target**), le routage (**priority**), la reconnaissance des entêtes des couches (**heading**), les données proprement dîtes (**data**), l'intégrité (**check**) et les options de contrôle (**control**) et les accusés de réception (**ack**).

La structure d'un paquet (segment, datagramme, trame)	
HEADER	Des informations de **transmission** (couche PHYSIQUE) Un signal d'alerte indiquant qu'un paquet est en cours de transmission Des informations d'horloge pour la **synchronisation** de la transmission Des informations de **routage** et **d'adressage** (couche RESEAU) L'adresse source de l'expéditeur L'adresse cible du destinataire Les **entêtes** de chacune des couches du modèle OSI Des informations d'interface (couche APPLICATION) Des informations de formatage (couche PRESENTATION) Des informations de connexion (couche SESSION) Des informations de séquence pour le ré-assemblage (couche TRANSPORT)
DATA	Les données (DATA) ou une partie des données d'origines La taille des données à l'intérieur d'un paquet varie en fonction des réseaux, mais cette section est généralement comprise entre 512 octets et 4 Ko.
TRAILER	La queue dépend du protocole utilisé Des informations **d'intégrité** (couche LIAISON) Le **CRC** (Cyclical Redundancy Check) est le résultat d'un calcul mathématique effectué chez l'émetteur et vérifié chez le destinataire. Quand le CRC n'est pas conforme, une demande de retransmission est envoyée à l'expéditeur (ou l'accusé de réception n'est pas envoyé, ce qui déclenche une retransmission du paquet).
OPTIONS	Les informations ajoutées selon les besoins Les informations de **contrôle** (par exemple une requête de service) Les codes de contrôle de SESSION (par exemple une demande de retransmission) Les accusés de réception (Acknowledgment)

L'adresse MAC

L'adresse MAC est l'identifiant unique d'une carte réseau. L'adresse MAC est un numéro de **48 bits** qui reprend le numéro d'identification du **constructeur** de la carte réseau et qui est suivi d'un numéro séquentiel. L'adresse MAC d'une carte réseau est unique, et ne peut être que difficilement changé. Les communication Tcp-ip utilisent l'adresse MAC pour envoyer les paquets, et les cartes réseaux reconnaissent leur propre numéro pour récupérer un paquet sur le réseau.

La circulation des paquets

Généralement, un paquet n'est adressé qu'à un seul destinataire avec une adresse bien précise. Toutefois, les communications vers toutes les adresses du sous réseau sont possibles (**broadcasting**).

Quand une station envoie un paquet sur le réseau, celui-ci circule le long du **segment** de câble et passe devant chacune des cartes réseaux. Toutes les cartes réseaux représentent un nœud. Les cartes réseaux

peuvent correspondre à différents types de matériels, cela peut être une station, un routeur, un serveur, une imprimante ou un sniffer. Toutes les cartes réseaux qui sont connectées sur le segment de câble sont susceptibles d'interceptées les communications.

Le passage des paquets

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 filer 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.

Quand 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 identifiée un paquet comme lui étant adressée.

Quand un paquet est reconnue par la carte réseau, celui-ci peut correspondre à une demande de **connexion** ou à une connexion qui est déjà établie. La nouvelle connexion démarre avec la négociation (**handshaking**) des paramètres communs pour la communication, et l'établissement d'un numéro d'identification (**identification**) pour cette communication.

Les adresses de broadcast

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 routage des paquets

Les réseaux étendus ou **WAN** (Wide Area Network) sont constitués de plusieurs sous réseaux (**subnet**). Les réseaux locaux ou **LAN** (Local Area Network) peuvent être connectés à un réseau étendu. Le routage consiste à transmettre les paquets d'un sous réseau à l'autre, en passant éventuellement par le réseau des réseaux (**internet**). Les paquets ne peuvent sortir d'un sous réseau que s'il existe des matériels spécifiques qui permettent le routage des paquets (**routers**).

Le routage d'un paquet consiste à le transmettre à un autre sous réseau. La redirection du paquet s'effectue par l'intermédiaire d'une passerelle (**gateway**). La passerelle peut être une passerelle par défaut (**default gateway**), ou être un routeur (**router**) spécifique pour une route bien déterminée. Tous les sous réseaux qui communiquent avec d'autres sous réseaux doivent avoir au moins une route par défaut, afin de pouvoir rediriger les paquets qui n'y sont pas destinés vers l'extérieur.

Le routage est réalisé par le système, puis par les routeurs. Le système d'exploitation (**system**) conserve

en mémoire une table de routage qu'il consulte pour diriger les paquets qu'il doit transmettre. Les routeurs disposent également d'une mémoire qui contient leur table de routage (**routing table**). La table de routage d'un routeur contient les informations des sous réseaux à proximité. Les protocoles de routage imposent aux routeurs de s'échanger régulièrement leurs tables de routage respectives. Ainsi, chaque routeurs connait un peu la carte des routeur qui lui sont proches et l'état du trafic. Les routeurs appliques des règles qui peuvent varier.

Les paquets considérés comme complet ou **FQNF** (Fully Qualified Name First) sont redirigés en priorité. Le routage prioritaire (**priority**) est un enjeu sur internet, parce qu'il permettrait d'améliorer considérablement la transmission des paquets et particulièrement les paquets contenants des images vidéo en streaming ou des chaines de télévision en directe. Le protocole **IPV6** prévoie des indicateurs de priorité.

Le routage peut être statique (**Networking Bridging**), et l'allocation d'adresse IP peut être dynamique avec le protocole **DHCP** (Dynamic Host Configuration Protocol).

Les sauts des paquets

La rencontre d'un routeur pour un paquet représente un saut (**hops**), et les paquets sont configurés pour ne franchir qu'un certain nombre de sauts pour arriver à destination. Le nombre de saut possible est stipulé dans la variable **TTL** (Time To Live) qui est décrémentée à chaque rencontre avec un routeur. Quand la variable a épuisé son crédit initial, le paquet (**packet**) est considéré comme perdus, et le routeur le lâche (**drop**). Les paquets perdus seront automatiquement retransmis par l'expéditeur, passé un délais d'attente d'un accusé de réception (**ack**).

Le filtrage des paquets

Les dispositifs de connexion et les équipements de commutation (**routers**) du réseau utilisent les informations d'adressage des paquets afin de déterminer la route la plus appropriée. L'adresse cible (**target**) identifiant le destinataire d'un paquet, et d'une manière plus générale, toutes les informations des entêtes (**headers**) d'un paquet peuvent être utilisées, soit pour **rediriger** le paquet, soit pour le **filtrer**. Les pare feux (**firewall**) sont des routeurs sophistiqués qui analysent ces informations d'entête pour déterminer le sort d'un paquet qui leur parvient.

ARPANET

Le réseau Arpanet

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** (Advanced Research Products Agency) dont **l**e 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). Le réseau Arpanet effectuait une commutation numérique de paquets en mode différé (**store and forward**).

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. Tout d'abord, plusieurs flots de données peuvent parcourir le support en même temps. Ensuite, plusieurs ordinateurs peuvent transmettre des données en même temps. En plus, les paquets peuvent emprunter plusieurs chemins différents, les paquets sont routés. Enfin, la correction des erreurs garantie la transmission des données. Une somme de contrôle et des numéros de séquences permettent de ré assembler 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.

ETHERNET

L'invention 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 au réseau **CSMA/CD** fut développée à cette occasion. Ce premier réseau a constitué la base des futurs réseaux Ethernet.

Robert Metcalfe, 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. Le réseau Ethernet de la société Xerox rencontra un tel succès, en 1976, que Xerox s'associa avec Intel Corporation et Digital Equipment Corporation pour élaborer une norme à 10 Mb/s.

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

Le premier réseau Ethernet
Débit de 2,94 Mb/s Connexion de plus de 100 stations Distance maximale entre deux ordinateurs de 1 Kilomètre

La norme IEEE 802.3

Les caractéristiques des premiers réseaux Ethernet 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.

Les réseaux Ethernet

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.

Les spécifications d'un réseau Ethernet
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)
Le support est **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**

La trame Ethernet

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

La trame Ethernet	
L'en-tête	Le préambule La destination La source Le type de protocole de la couche RESEAU (IP ou IPX par exemple)
Le corps	Les données
La queue	Le contrôle cyclique de redondance (CRC)

Les normes Ethernet

Les normes Ethernet s'expriment toutes selon la même formule («x»Mb/s Base «y»). Avec «x» qui exprime la vitesse en Mb/s, le mot Base qui indique que le mode de transmission est la **modulation** en Bande de Base, et «y» qui décrit le support de communication, et qui peut être la lettre «T» pour les câbles en paires torsadées, un chiffre pour le câble coaxial («2» pour le coaxial fin ou «5» pour le coaxial épais) ou les lettres «FL» ou «FO» pour la fibre optique.

La norme I**EEE 802** définie les spécifications relatives à la mise en œuvre 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 rapide pour supporter des applications gourmandes en bande passante comme la **CAO** (Conception Assitée par Ordinateur), la **FAO** (Fabrication Assistée par Ordinateur), la **VOD** (Video On Demand) et la **GED** (Gestion Electronique des Données). 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.

Les normes Ethernet IEEE 802	
IEEE 802.3 (cable)	Le 10BaseT pour les câbles en paires torsadées non blindées et blindées Le 10Base2 pour les câbles en coaxial fin Le 10Base5 (Ethernet STANDARD) pour les câbles en coaxial épais Le 100BaseX (FAST Ethernet) Le 100BaseT4 pour la paire torsadées à quatre paires de fils (UTP) Le 100BaseT5 pour la paire torsadées de catégorie 5 Le 100BaseTX pour la paire torsadées blindée (STP) Le 100BaseFX pour la fibre optique
IEEE 802.8 (fiber)	Le 10BaseFL pour la fibre optique
IEEE 802.12 (fast)	Le 100VG-AnyLAN

Le tableau Ethernet à 10 Mb/S

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	Fiber Link
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
Transmission du signal	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	Star, Star Bus	Bus	Dorsale et Bus	Bus
Règle		Règle des 5-4-3	Règle des 5-4-3	
Dorsale	Concentrateurs		Transceivers	
Câbles	**Paire torsadées**	**Coaxial fin**	**Coaxial épais**	**Fibre optique**
Mixité des câbles	UTP 3, 4, 5 STP	RG-58	Coaxial épais et fin	La fibre optique
Prises vampires	(Si dorsale)	NON	OUI	
Transceiver	(Si coaxial épais)	OUI	Avec un répéteur	
Câbles de transceiver	(Si dorsale)	OUI	OUI, 50 mètres	
Connecteurs	RJ45 et/ou AUI	BNC et AUI	AUI ou DIX	
Résistance Impédance		50 Ohm	50 Ohm	
Bouchons		BNC	Série N	
Cartes réseaux	RJ45 ou AUI	BNC	AUI (ou DIX)	
Segment	100 mètres	185 mètres	500 mètres	2000 mètres
Répéteur Concentrateur	OUI multiport	OUI	OUI	OUI, en fibre
Réseau		925 mètres	2500 mètres	
Câble de descente		<50 mètres	<50 mètres	
Écart ordinateurs	2,5 m	0,5 m	2,5 m	
Nœuds par segment		30 nœuds	100 nœuds	
Nœuds par réseaux	1024 transceivers	86 stations	296 stations	
Utilisation	évolutif 100Mb/s	peu couteux	Un immeuble	Entre bâtiments

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 blindée (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 relié 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 spécifications du 10BaseT
Débit de 10 Mb/s
Transmission des signaux en bande de base
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 (entre le concentrateur et le transceiver)
L'écart minimal entre deux ordinateurs est de 2,5 mètres
Le nombre maximal d'ordinateurs est de 1024 transceivers
Un ou des concentrateurs (répéteurs multiports)
Un seul concentrateur pour une topologie en étoile
Des concentrateurs sur une dorsale (coaxial ou fibre optique) pour une topologie en bus en étoile
Des répéteurs pour allonger la longueur d'un segment

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'autorise 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 totale du réseau. La spécification IEEE 802.3 recommande un maximum de **30 nœuds** (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 spécifications du 10Base2
Débit de **10 Mb/s**
Transmission des signaux en **bande de base**
Câble **coaxial fin** (RG-58 avec une impédance de **50 Ohm**)
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 nœuds** (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

Le 10Base5

Les réseaux Ethernet en 10Base5 sont aussi appelés Ethernet Standard (Standard Ethernet). Les réseaux Ethernet en 10Base5 utilisent des câbles **coaxiaux épais** (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** (de 3/8 pouces). 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 (5segments, 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 épais 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 épais sont plus importantes que celles du câble Ethernet fin, c'est pourquoi il est souvent utilisé pour desservir tout un immeuble.

Les spécifications du 10Base5
Débit de **10 Mb/s**
Transmission des signaux en **bande de base**
Câble **coaxial épais** (peut transporter un signal sur une distance de 5x100 mètres)
La méthode d'accès au réseau **CSMA/CD**
Des câbles de transceiver (câbles de descentes) de la carte réseau au transceiver de la dorsale
Des connecteurs **AUI ou DIX** pour les cartes réseaux et les 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** (hors câble de descente)
La longueur maximale du câble de transceiver est de **50 mètres**
Un nombre maximal de **100 nœuds** (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

Le 10BaseFL

La norme **IEEE 802.8** concerne les réseaux Ethernet en 10BaseFL qui utilisent des câbles en **fibres optiques**. Les câbles en fibres optiques permettent d'installer de très longs 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 spécifications du 10BaseFL
Débit de **10 Mb/s**
Transmission des signaux en **bande de base**
Câble FL (Fiber Link), c'est à dire pour désigner les câbles en **fibres optiques**
La méthode d'accès au réseau **CSMA/CD**
La longueur maximale d'un segment est de **2000 mètres**
Des répéteurs pour la fibre optique

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'appèlent indifféremment 100BaseVG, VG, ou 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'accroitre 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 étoiles 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 boitier.

Les spécifications du 100VG-AnyLAN
Débit de **100 Mb/s**
Transmission des signaux en **bande de base**
Câble VG (**Voice Grade**)
Des câbles en **paire 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 étoiles en cascade**

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 (100BaseT4 pour la paire torsadées à quatre

paires de fils, 100BaseTX pour la paire torsadées à deux paires de fils, 100BaseFX pour la fibre optique). Pour la norme 100BaseT4, les câbles sont 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, les câbles sont 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).

Les spécifications du 100BaseX
Débit de **100 Mb/s**
Transmission des signaux en **bande de base**
Câbles indéterminés «X» pour «T4», «TX» ou «FX» selon le câblage
La méthode d'accès **CSMA/CD**
Pour la norme 100BaseFX, des câbles en **fibre optique**
Des concentrateurs
Topologie **en bus en étoile**

APPLETALK

Les réseaux Apple Talk

La société Apple Computer a introduit l'architecture Apple Talk en 1983. Les réseaux Apple Talk fonctionnent avec un petit ensemble d'ordinateurs Macintosh™. La taille des réseaux Apple Talk étant limitée, c'est une architecture qui a été supplantée par l'avènement des réseaux Ethernet. L'architecture Apple Talk est une architecture propriétaire. L'architecture Apple Talk est intégrée au système d'exploitation Mac OS. Tous les ordinateurs Macintosh™ sont équipés des fonctionnalités réseaux Apple Talk, ce qui rend plus facile la mise en place d'un tel réseau. L'architecture Apple Talk Phase II incorpore des protocoles réseaux qui correspondent au modèle OSI. Les réseaux Apple Talk sont communément appelés des réseaux Local Talk.

De nombreux ordinateurs provenant d'autres constructeurs peuvent fonctionner sous Apple Talk, comme par exemple, 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.

Les caractéristiques des réseaux Apple Talk

Les Zones permettent d'accroitre 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 Apple Talk. Ether Talk permet aux protocoles Apple Talk de fonctionner sur un câble coaxial (câble Ethernet).

Les caractéristiques des réseaux Apple Talk
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) et la fibre optique
Apple Talk est bon marché et facile à installer parce qu'il est intégré au système d'exploitation
Apple Talk convient pour de petits réseaux
Les Zones constituent des sous-réseaux Apple Talk
Ether Talk permet aux protocoles Apple Talk de fonctionner sur un câble coaxial (câble Ethernet)

Les composants matériels d'un réseau Apple Talk

Les composants matériels d'un réseau Apple Talk
Un maximum 32 ordinateurs avec les câbles Local Talk d'Apple
Un maximum de 254 machines avec les câbles de Farallon Phonenet
Les câbles et les connecteurs sont compatibles avec les réseaux en bus ou en étoile
Des prises 8 broches pour relier les câbles au module de connexion
Les cartes réseaux Ether Talk NB pour Macintosh™ II sur un réseau Ethernet (IEEE 802.3)
Logiciel Ether Talk est compatible avec Apple Talk Phase II
Les cartes réseaux Token Talk pour Macintosh™ II sur un réseau Token Ring (IEEE 802.5)
Le logiciel Token Talk qui est compatible avec Apple Talk Phase II

L'identification Apple Talk

L'identification d'une machine sur un réseau Apple Talk s'effectue en trois étapes. La machine s'attribue une adresse au hasard dans une plage d'adresses autorisées, puis la machine diffuse sur le réseau son adresse, enfin, si aucune autre machine n'utilise son adresse, elle la garde et l'enregistre.

ARCNET

Les réseaux 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.

Les caractéristiques des réseaux Arcnet

Le jeton se déplace sur le réseau en suivant l'ordre numérique attribué à chaque machine, sans tenir compte de leur localisation. Les réseaux Arcnet fonctionnent autour d'un concentrateur, et ne gèrent pas plusieurs segments.

Les caractéristiques des réseaux Arcnet
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
Un débit de 2,5 Mb/s, et de 20 Mb/s pour Arcnet Plus

Le format de la trame Arcnet

La trame Arcnet est relativement sobre en informations. La trame Arcnet est constituée de l'entête avec l'adresse de destination, du corps et d'une queue contenant l'adresse source. La trame est de 508 Octets pour Arcnet et de 4096 Octets pour Arcnet Plus.

Les composants matériels d'un réseau Arcnet

Les composants matériels des réseaux Arcnet
Les concentrateurs «passifs» relayent simplement les trames
Les concentrateurs «actifs» régénèrent les trames avant de les réexpédier
Les concentrateurs «intelligents» (Smart Hub) régénèrent le signal et font des diagnostics
Les câbles coaxial RG-62 A/U et RG-59 avec une résistance respective de 93 Ohm et 75 Ohm
La topologie en bus avec un concentrateur actif distant au maximum de 305 mètres
La topologie en bus en étoile avec un concentrateur actif distant au maximum de 610 mètres
Les câbles en paire torsadée non blindée pour des bus ou des bus en étoile distant de 244 mètres
La fibre optique

TOKENRING

Les réseaux Token Ring

La version IBM des réseaux Token Ring est sortie en 1984, avec la particularité de pouvoir fonctionner avec toutes les dimensions de sa gamme d'ordinateurs, les ordinateurs personnels IBM PC compatibles, les mini-ordinateurs et 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**.

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 qui est le Token Ring «normal», et le Token Bus, c'est le Token Ring sur un support en **bus**.

Les caractéristiques des réseaux Token Ring

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

Le format de la trame Token Ring

Le format de la trame Token Ring	
Un en-tête	Un délimiteur de début de trame Un contrôle d'accès pour indiquer la priorité de la trame (jeton ou données) Un contrôle de trame L'adresse récepteur du destinataire L'adresse émetteur de l'expéditeur
Le corps	Les données
La queue	Une séquence de contrôle de trame, le CRC Un délimiteur de fin de trame Un indicateur de l'état de la trame, reconnue, recopiée, ou si adresse indisponible

Le 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 exister, 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 (**supervisor**) et 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).**

Le contrôleur du réseau Token Ring

Le contrôleur du réseau (**supervisor**) 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 et que **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.

La circulation du jeton

L'initialisation d'un réseau Token Ring suit une procédure stricte et systématique.

La circulation du jeton
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 (recopiée) par son destinataire.
L'ordinateur **récepteur renvoi** 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
L'ordinateur émetteur **accuse réception** que sa trame a été recopiée et la détruit
L'ordinateur continu 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.

Les composants 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** (MultiStation Access Unit) 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	
Concentrateurs	MAU (Multistation Access Unit) MSAU (MultiStation Access Unit) MSAU de chez IBM SMAU (Smart Multistation Access Unit) Un nombre maximal de 33 segments reliés par 33 concentrateurs
Câblage	Les paires torsadées non blindées (UTP) porte 72 ordinateurs par segment Les paires torsadées non blindées (UTP) d'impédance de 100 à 120 Ohm Les paires torsadées blindées (STP) porte 260 ordinateurs par segment Les paires torsadées blindées (STP) d'une impédance de 150 Ohm Les câbles IBM de catégories 1 ont une longueur de 101 mètres (STP) Les câbles IBM de catégories 2 ont une longueur de 100 mètres (STP) Les câbles IBM de catégories 3 ont une longueur de 45 mètres (UTP) D'autres constructeurs proposent une longueur maximale de 150 mètres Les câbles de connexion (Patch Cables) de type 6 ont une longueur de 45 mètres La fibre optique augmente considérablement la portée d'un réseau Token Ring
Connecteurs	MIC (Media Interface Connector) pour connecter les câbles de type 1 et 2 RJ45 et RJ11pour les câbles de type 3
Filtres	Les filtres de support des cartes réseaux Token Ring pou les prises RJ45 ou RJ11
Répéteurs	Les répéteurs allongent la longueur d'un câble Les répéteurs régénèrent et synchronisent le signal Deux répéteurs à 730 mètres entre les deux MSAU (câble de type 1 ou 2) Deux répéteurs à 365 mètres entre les deux MSAU (câble de type 3)
Cartes réseaux	Les cartes réseaux de 4 Mb/s Les cartes réseaux de 16 Mb/s sont compatibles avec un réseau à 4 Mb/s Le mode 16 Mb/s bascule en mode 4 Mb/s (mais évidemment pas l'inverse) Les cartes réseaux 16 Mb/s utilisent une trame plus longue L'écart minimal entre deux ordinateurs est de 2,5 mètres

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 connait l'adresse de la station précédente, et celle de la station suivante (**virtual ring**) 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 paquets en bout de câble.

WAN

Les réseaux étendus

Les réseaux étendus sont des réseaux à l'échelle planétaire ou **WAN** (Wide Area Network). Les réseaux étendus peuvent être spécifiques à une seule organisation. En général, l'on parle de réseaux étendus pour parler des réseaux planétaires qui rassemblent et interconnectent d'autres réseaux, lesquels peuvent disposer de caractéristiques techniques différentes. Des passerelles (**gateway**) permettent de traduire les communications et d'assurer la compatibilité entre les différents protocoles (**protocol**). Le réseau internet est le principal réseau étendu mondial de la planète Terre. Le réseau internet est aussi appelé la toile ou **WWW** (World Wide Web).

Le réseau internet utilise le protocole Tcp-ip pour le transport et l'adressage. La version courante de l'adressage est **IPV4**, mais la plus part des infrastructures sont déjà prêtes pour IPV6 (**ipv6ready**). Les connexions au réseau internet sont proposées par les opérateurs téléphoniques nationaux ou par des sociétés spécialisées dans les réseaux étendus. Ces sociétés spécialisées dans les transmissions et les tuyaux sont appelées des **FAI** (Fournisseur d'Accès à Internet) ou **ISP** (Internet Service Provider). L'accès à internet nécessite de disposer d'une adresse IP. Cette adresse IP peut être louée, dans le cadre d'un abonnement chez le provider ou achetée auprès de l'organisation de régulation qui gère l'adressage sur internet (IANA ou Internic).

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, en prenant le **contrôle** d'une machine à distance, ou en établissant une **connexion** à distance avec un serveur.

Le contrôle à distance

Le contrôle à distance consiste à prendre le contrôle d'un ordinateur distant à partir d'un **terminal** ou d'un autre ordinateur. Bien avant l'essor d'internet, c'était pratiquement le seul moyen pour accéder à des ressources à distance. Les ordinateurs portables de l'époque n'étaient pas assez puissant pour être en mesure de charger les applications d'un serveur distant, et leur capacité de stockage ne leur permettait pas de stocker des données sur une station itinérante. Le rôle du terminal consistait seulement à afficher l'interface de l'ordinateur distant et à envoyer des commandes.

Cette technique nécessite l'installation d'un logiciel sur l'hôte et sur l'invité. De plus, il faut rester connecter pour pouvoir travailler. Enfin, il faut placer l'ordinateur hôte en situation d'attente pour qu'il puisse recevoir l'appel de l'utilisateur distant. Aujourd'hui, les logiciels de prise de contrôle à distance

sont surtout utilisés pour les applications qui exigent beaucoup de ressources, comme les bases de données, et pour les dépannages et les configurations à distance. Il existe plusieurs logiciels permettant la prise de contrôle d'un autre ordinateur à distance (X forwarding, VNC, PC Anyware de Symantec, Reach Out de Stac et Laplink de Traveling Software). Avec le contrôle à distance, l'interface de la machine distante est **déportée** vers le client qui peut agir localement comme s'il était à distance.

La connexion à distance

La connexion à distance (ou le nœud à distance) est une technique plus récente qui a vu le jour avec l'essor de l'internet et des capacités des ordinateurs. Le **nœud** représente une station qui s'intègre au réseau comme tout autre nœud, sauf la distance. L'ordinateur distant se connecte au réseau comme tout autre client du réseau, comme s'il était connecté sur place. L'ordinateur distant utilise un **protocole** de communication comme PPP de la pile TCP/IP pour établir une connexion jusqu'au réseau. Le nœud à distance est un ordinateur comme tous les autres du réseau, il peut accéder à toutes les ressources qui sont partagées sur le réseau (à condition d'en avoir la permission) et peut effectuer toutes les opérations systèmes sur le réseau (à condition d'en avoir les droits et les privilèges).

De plus, le nœud à distance peut télécharger les fichiers dont il a besoin, travailler **hors connexion** avec les applications installées sur le portable (ou sur un ordinateur de bureau), et enregistrer les fichiers en local. Le nœud à distance s'est largement répandu avec internet, et beaucoup d'internautes emploient cette technique sans le savoir. De nombreuses entreprises profitent de cette technique, avec des liaisons spécialisées, pour rapprocher leurs collaborateurs dans le monde entier, et pour améliorer la gestion des différentes versions des documents sur lesquels ils travaillent en même temps ou à des moments différents. La connexion à distance permet d'accroitre la **productivité** des groupes de travail en se libérant des **contraintes** d'horaire et de l'éloignement géographique. C'est une technique qui devient spontanée avec la **mondialisation** des échanges et la **globalisation** des décisions.

La connexion à un réseau à distance peut s'effectuer de différentes manières, soir par l'intermédiaire d'un Fournisseur d'Accès à internet (**provider**), soir par l'intermédiaire de liaisons spécialisées fournies par les opérateurs téléphoniques. Le provider peut s'occuper des formalités de réservation d'une ligne dédiée (une liaison de type T1 ou 56 K).

Le provider

L'accès à internet s'effectue en général par l'intermédiaire d'un **FAI** (Fournisseur d'Accès à Internet) ou d'un **ISP** (Internet Service Provider), dans le cadre d'un **abonnement** forfaitaire. L'abonnement peut concerner une ligne analogique chez les particuliers, ou une ligne numérique dédiée chez les professionnels. L'abonnement peut être souscrit pour l'obtention d'une adresse IP dynamique qui est renouvelée à chaque connexion, ou pour l'obtention d'une adresse IP fixe, ou d'une plage d'adresse fixe.

La connexion au Fournisseur d'Accès à Internet s'effectue avec le protocole PPP pour les lignes analogiques, et avec une adresse IP **dynamique** qui est allouée par le provider. Dans le cadre d'un

abonnement classique pour les particuliers, les messages électroniques (**mail**) sont récupérés depuis le serveur de messagerie du provider en utilisant le protocole POP3 ou IMAP4, et ils sont envoyés au serveur de messagerie du provider en utilisant le protocole SMTP.

Les adresses IP dynamiques ne permettent pas de router soi-même le courrier électronique, ni d'avoir son propre serveur Web, puisque l'adresse IP change en fonction des plages disponibles chez le provider. Il est possible de recevoir une adresse IP **fixe** de la part du provider. L'abonnement chez un provider avec une adresse IP fixe coute plus cher qu'une adresse IP dynamique, parce que l'adresse IP est réservée, même quand la connexion n'est pas utilisée. Mais cela coûte moins cher qu'une liaison numérique dédiée.

L'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. Les paquets du réseau interne destinés à internet sont filtrés et routés par le **routeur**, 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.

De la même façon qu'avec un provider, la connexion, chez un opérateur téléphonique, 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**.

Les ports de connexion

Les ports de connexion ou la connectique pour se connecter à internet sont nombreux en théorie, mais dans la pratique, c'est le plus rapide qui est toujours privilégié. La connectique de connexion peut utiliser tous les ports d'un ordinateur, le port série (**serial**), le port parallèle (**parallel**), le port de périphérique rapide (**firewire**), le port USB (**usb**). Avec la généralisation d'internet, les ports réseaux sont de plus en plus démocratisé, comme le port RJ45 (**Ethernet**) et le port de micro onde (**wifi**).

Les connexions par ondes courtes (**wifi**) sont susceptibles, comme les téléphones portables (**cellular**) ou les micro ondes des cuisines de provoquer des dysfonctionnements hormonaux ou cérébraux, particulièrement envers les personnes dites ultra sensibles.

Les informations de connexion

Certaines informations de connexion sont indispensables pour configurer une connexion à internet. Certaines de ces informations doivent être fournies avant la connexion, et d'autres sont fournies pendant, comme l'adresse IP dynamique (**dynamic**) qui est octroyée par le serveur **DHCP** (Dynamic Host Configuration Protocol) pour un bail d'une durée aléatoire. Le renouvellement de l'adresse IP

dynamique s'effectue automatiquement (**release**).

Les informations de connexion à internet
Le numéro de téléphone (**telephone**) du serveur du fournisseur (**provider**)
Le nom de connexion (**login**)
Le mot de passe associé (**password**)
L'adresse IP dynamique (**dynamic**) du serveur **DHCP** (Dynamic Host Configuration Protocol)
Le nom de domaine du fournisseur (**domain**)
Le masque de réseau (**netmask**)
L'adresse de broadcast (**broadcast**)
L'adresse de la passerelle (**gateway**)
L'adresse des serveurs DNS (Domain Name Service) pour résoudre les noms de domaine (**name**)
L'adresse de boucle interne (**loopback**)
L'adresse du serveur de messagerie entrant (**pop**)
L'adresse du serveur de messagerie sortant (**smtp**)
L'adresse du serveur de news (**nntp**)
L'adresse Mail (**mail**)

La connexion à internet

L'accès à internet permet de se connecter aux ressources du réseau des réseaux, d'utiliser sur un moteur de recherche (**google**), de consulter des annuaires (**gopher**) ou des sites (**firefox**), d'échanger des messages (**mail**), de télécharger des fichiers (**ftp**), de dialoguer sur des chats ou dans des salons (**irc**), de participer aux conversations des forums (**news**), de se connecter à un serveur distant privé (**ssh**), et de constituer des communications cryptées sur des réseaux privés virtuels ou **VPN** (Virtual Private Network). Le déport de l'affichage d'une station vers une autre station (**XForwarding**) s'effectue avec une application client serveur appelée **VNC** (Virtual Network Computing).

Les types de connexion

Les types de connexions à internet sont nombreuses et peuvent éventuellement se mélanger ou se combiner. Les types de connexion se différencient principalement par la permanence ou non de la connexion, par l'obtention d'une adresse IP dynamique ou statique, par la nature analogique ou numérique de la transmission, et par la situation locale ou à distance. Les connexions peuvent être directe ou indirecte en passant par un serveur de connexion ou un serveur cache (**proxy**). Plusieurs configurations peuvent être envisagées pour les utilisateurs itinérants.

Les connexions peuvent être réalisées via une ligne **analogique** ou via une ligne **numérique** dédiée. 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.

Les adresses IP dynamiques (**dynamic**) permettent d'avoir accès aux ressources d'internet de temps en temps et pour des durées variables, mais plutôt courtes. Les adresses IP fixes (**static**) permettent d'assurer une présence constante sur internet. Les connexions **permanentes** s'effectuent à l'aide d'une adresse IP fixe. Les connexions peuvent être **mono** utilisateur pour un seul poste, ou **multi** utilisateurs, afin de partager la bande passante qui est alors divisée par le nombre de connexions simultanées.

Les connexions à la **demande** peuvent passées par un serveur de connexion 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. La mutualisation des connexions sur trois lignes **simultanément** permet d'augmenter la bande passante (avec par exemple Multilink PPP). Les connexions **manuelles** sont effectuées par les utilisateurs qui adaptent la configuration de la connexion en fonction de l'endroit où ils se trouvent.

Quand la ligne est **dédiée**, les connexions passent 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 une porte coupe feu (**firewall**).

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 des serveurs de connexion à distance qui sont connectés en permanence à internet.

La traduction des adresses IP

La retransmission d'adresses IP (**IP Forwarding**) est un mécanisme qui peut être installé sur un serveur de connexion internet du réseau Intranet d'une entreprise. La retransmission d'adresse consiste à **rediriger** les paquets internet vers les ordinateurs de l'Intranet et vice versa. Le serveur de connexion internet reçoit les demandes internes, qui peuvent provenir de plusieurs ordinateurs en même temps, et les redirige sur internet en utilisant sa propre adresse IP, qui peut être une adresse IP fixe ou une adresse IP dynamique, allouée par le provider. Ensuite, le serveur de connexion internet reçoit toutes les réponses depuis internet, lesquelles sont toutes envoyées à la même adresse IP, la sienne.

Le serveur de connexion internet redirige chacune des réponses vers le poste en interne qui en a fait la demande. Le serveur de connexion internet doit mémoriser qui demande quoi, et quelle est l'adresse interne qui communique avec telle ou telles adresses externes. Toutes les communications vers

l'extérieur passent par le serveur de connexion internet et utilisent la même adresse IP. La retransmission d'adresse IP fonctionne avec une adresse IP dynamique ou fixe. Ainsi, la retransmission d'adresses IP permet de masquer les adresses IP en interne.

Les adresses intranet

Le protocole TCP/IP peut être également utilisé dans un réseau **Intranet**, les ordinateurs du réseau interne disposent d'une adresse IP. Les adresses IP internes sont choisies parmi des plages d'adresses réservées pour un usage privé. Les adresses IP privées ont le même format qu'une adresse IP internationale ou publique. 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.

Les ordinateurs de l'Intranet utilisent les adresses IP privées pour les communications internes, et s'adressent à la passerelle par défaut (**default gateway**) pour communiquer avec internet. La passerelle par défaut doit disposer d'une adresse IP internationale.

Les adresses internet

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** en France ou par **l'IANA** aux États Unis d'Amériques. Les adresses IP allouées par le Fournisseur d'Accès à Internet sont des adresses qui ont été achetées à Internic, elles constituent un groupe d'adresses (**pool**) que le provider distribue à ses clients.

Le réseau Intranet d'une entreprise peut avoir besoin d'adresse IP internationale. Par exemple, des serveurs de pages internet (**apache**) requiert une adresse IP internationale pour livrer les pages demandés par les visiteurs du site. Dans ce cas, l'entreprise peut acheter le privilège d'utiliser une adresse IP internationale. Cette réservation s'effectue auprès d'une organisation de régulation comme Internic. L'adresse IP internationale fera partie d'une classe d'adresse (**classe**), et permettra de disposer, selon la classe, d'un adressage plus ou moins important.

Les adresses IP internationales, dont dispose l'entreprise, peuvent être réparties selon les besoins et les stratégies de l'entreprise. 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.

Le firewall

Les connexions permanentes doivent être protégées des intrusions malveillantes de l'extérieur. Cette protection est mis en place par une porte coupe feu (**firewall**). Un firewall est un dispositif qui peut être un ordinateur dédié ou un routeur spécialisé, et qui s'intercale entre le réseau Intranet et le réseau internet. Le firewall vérifie et authentifie toutes les connexions qui proviennent de l'extérieur.

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 toujours d'au moins deux cartes réseaux.

La DMZ

Le firewall peut être installé à l'entrée d'un tout petit réseau et constituer ainsi une zone séparée. Cette zone protégée par un firewall est appelée une zone démilitarisée ou un réseau **DMZ** (Demilitarized Zone). Le firewall d'un réseau DMZ joue le rôle d'un sas, c'est à dire d'un filtre où transitent tous les paquets sortants et tous les paquets entrants.

Une organisation classique se compose du réseau **internet**, d'un réseau **DMZ** abritant les serveurs Web ouverts sur l'extérieur, et d'un réseau privée et fermé qui constitue **l'Intranet**.

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.

Les réseaux privés

Les réseaux étendus sont les réseaux qui dépassent **l'envergure** d'un réseau local. Hormis internet, le réseau des réseaux, les réseaux étendus privés sont généralement la réunion de plusieurs réseaux locaux privés. Les réseaux privés **MAN** (Metropolitan Area Network) sont à l'échelle d'une ville, tandis que les réseaux privés **WAN** (Wide Area Network) sont à l'échelle des continents. Un WAN peut être constitué de deux **LAN** (Local Area Network) 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.

Les réseaux privés peuvent être entièrement constitués de composants privés ou loués. Les infrastructures peuvent être louées (les serveurs, les dispositifs de connectivité, les lignes), mais le réseau sera tout de même un réseau privé. Un réseau privé peut faire partie, ou non, du réseau internet, selon que ces données transitent, ou non, par le réseau internet, et que ses utilisateurs ont accès, ou non, au réseau internet.

Selon le nombre de personnes qui se connecte en même temps à un réseau à distance, il peut être intéressant d'envisager une ligne numérique dédiée ou de construire un **pool de modem** sur un serveur.

Les débits des réseaux étendus

Les débits (ou la bande passante) des réseaux étendus (et le coût) diffèrent selon les technologies employées. Les lignes numériques des réseaux **étendus** longues distances ne sont pas aussi rapides que les supports de communication des réseaux locaux. Ainsi, les liaisons distantes entre deux réseaux **locaux** sont toujours un facteur de ralentissement.

Les réseaux étendus permettent à des utilisateurs distants d'accéder, en même temps à un serveur, et en temps réel à une base de données. L'intégrité des données d'une **base de données** est primordiale, et quand des changements sont effectuées sur les données, celles-ci doivent être intégrées à la base aussi rapidement que possible. Une base de données est un système **transactionnel** qui peut rassembler des données communes à plusieurs sites. La vitesse de communication et d'échange des données est dès lors très importante quand les sites sont éloignés les uns des autres.

Les débits effectifs dépendent du support de connexion et de sa vitesse de transmission maximale (**fiber**), du mode de transmission, des protocoles réseaux (**ip**), des protocoles de transport (**tcp**), de l'architecture réseau et des dispositifs de connectivité. Le mode de transmission peut être la commutation de paquets des réseaux publics (**any-to-any**) ou les circuits dédiés des lignes spécialisées (**point-to-point**).

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 types de réseaux.

Les débits des réseaux étendus	
Les lignes téléphoniques analogiques (RTC)	
Modem RTC (Réseau Téléphonique Commuté)	56 Kb/s
Modem ADSL (Asymetric Digital Subscriber Line)	
ATM (Asynchronous Transfert Mode)en Large de Bande	155 Mb/s
X25 en France	
Les lignes téléphoniques numériques	
IDSN (Numeris ou RNIS en France)	128 Kb/s pour 2 canaux B
Frame Relay	56 Kb/s
Lignes T1	1,544 Mb/s (aux U.S.A)
Lignes E1	2,048 Mb/s (en Europe)
LignesT3	45 Mb/s (aux États-Unis)
FDDI (Fiber Distributed Data Interface)	100 Mb/s
ATM en Bande de Base (technologie émergente)	622 Mb/s
Les débits des réseaux locaux	
Local Ethernet 10Base5	10 Mb/s au minimum avec du coaxial
Local Ethernet 100BaseT	100 Mb/s pour de l'UTP catégorie 5
Local Fiber (fibre optique)	622 Mb/s ou 1 Gb/s

Le cout des réseaux

La gestion des couts des réseaux est une notion fondamentale et déterminante, que ce soit du point de vue de la conception et de la mise en place d'une telle **infrastructure**, que du point de vue de la conservation et de l'administration d'un tel système. Les réseaux coutent très chers à l'achat, à la location, en maintenance et en services.

Les couts de gestion d'un réseau étendu doit prendre en compte le prix de la **ligne** numérique, le prix de **l'installation**, le prix des **équipements** spéciaux et le prix de la **maintenance** et de **l'assistance** (dans les différents sites). Outre les couts d'installation et de maintenance, il faut également prendre en compte les couts de **conception**, **d'évolution** et de **décision**, ainsi que les risques éventuels liés à **l'intégrité**, la **confidentialité** et la **sécurité** des données.

La qualité des réseaux

Les coûts d'assistance et de maintenance sont souvent des coûts cachés (**hiden cost**), mais ils représentent une part non négligeable du coût total de fonctionnement ou **TCO** (Total Cost of Ownership). Ainsi, le retour sur investissement d'une telle infrastructure est, quand on peut le calculer,

un critère déterminant pour les personnels 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 ou **SLA** (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 ou **QOS** (Quality Of Service) permettent de contractualiser un certain niveau de bande passante pendant toute la durée de l'abonnement.

L'externalisation des réseaux

Un moyen de réduire le cout d'un réseau est de l'externaliser. Une société qui fait appel à une autre va jouer le rôle de **maitre d'œuvre** (MOE), c'est-à-dire qu'elle devient le client d'un **fournisseur**, qu'elle définit un cahier des charges, finance et provisionne le projet, assume les décisions et les responsabilités, contrôle la qualité, la conformité et l'achèvement des réalisations, supervise les recettes et les tests, prévoie des pénalités de dépassement de budget ou de calendrier, et qu'elle paye son prestataire.

La solution de l'externalisation peut être réalisée auprès de plusieurs types d'entreprises. Les **intégrateurs** de systèmes réseaux et les entreprises de type **SSII** (Société de Services en Ingénierie Informatique) jouent le rôle du maitre d'ouvrage (MOE), tandis que les grands groupes de **consultants** jouent le rôle de médiateurs. Les fournisseurs d'accès à internet (**provider**) vendent plutôt des services de connexion (leur infrastructure réseau est déjà en place) que des services d'expertise.

L'expertise des réseaux

L'expertise des réseaux est un long apprentissage qui requiert de connaitre la théorie et d'expérimenter la pratique. Les technologies évoluent très rapidement et un expert peut devenir très vite obsolète. Il est trop simple et trop facile de penser que les solutions existent et qu'il suffit de les mettre en œuvre. La compréhension des enjeux et des techniques est un lourd investissement intellectuel.

Il est faux de croire qu'il suffit de paramétrer les routeurs pour réexpédier les paquets de l'entreprise, ou de louer une bande passante chez un fournisseur pour y installer un réseau privé virtuel ou **VPN** (Virtual Private Network) qui utilise le réseau internet. La conception, les configurations, les choix stratégiques, la planification, les mises au point (**tuning**) et les tests (**benchmarking**) prennent beaucoup plus de temps en réflexion qu'à la mise en œuvre. Les solutions qui utilisent internet doivent être sécurisées par des moyens de cryptologie. La complexité des techniques et la multitude des intervenants sur le réseau internet font que des nombreuses possibilités de capture ou probabilités d'interception sont à envisager.

Les modes de transmission

Les modes de transmission des réseaux étendus se différencient par le type de **signal** (analogique ou

numérique), selon le **rythme** des émissions et des réceptions (synchrone ou asynchrone) ou par la spécialisation du **chemin** emprunté par les données (commutation ou spécialisation).

Les transmissions analogiques sont appelées des transmissions en **"large de bande"** parce qu'elles peuvent scinder la largeur de la bande de fréquence du support en plusieurs canaux (fréquence continue unidirectionnelle) et les transmissions numériques sont appelées des transmissions en **"bande de base"** parce qu'elles occupent toute la bande de fréquence pour un seul canal (fréquence discrète bidirectionnelle).

Les communications sur des lignes publiques commutées empruntent plusieurs chemins possibles, tandis que les communications sur des lignes dédiées n'emprunte qu'un seul chemin, mais ne permettent pas d'en changer. Les réseaux privés virtuels ou **VPN** (Virtual Private Network) ne sont pas limités aux lignes spécialisées des liaisons numériques des opérateurs téléphoniques, mais peuvent très bien fonctionner avec une ligne analogique sur le réseau internet. La création d'un tunnel crypté (**tunneling**) de communication permet d'assurer un certain niveau de sécurité.

Les transmissions analogiques

Les transmissions analogiques utilisent en général les réseaux téléphoniques câblés publics.

La transmission analogique en large de bande (BROADBAND)
Les signaux **analogiques** sont transportés sur une plage de fréquence
Les signaux analogiques sont transmis en **continus** sans interruption
La **hauteur** de la fréquence qui varie et correspond à un bit plein (one) ou vide (zero)
Les signaux analogiques peuvent être des **ondes** électromagnétiques ou optiques
Le câble transporte éventuellement plusieurs communications simultanément (**échantillonnage**)
La bande passante peut être divisée en plusieurs **canaux** de transmission
Les signaux analogiques ne sont transportés que dans un seul sens (**flux unidirectionnel**)
Les lignes téléphoniques disposent d'un câble montant (**speak**) et d'un câble descendant (**listen**)

Les transmissions numériques

Certains équipements d'un réseau en bande de base transmettent les signaux numériques dans les deux sens simultanément. Par exemple, les transmissions numériques sont utilisées sur les réseaux Ethernet.

La transmission numérique en bande de base (BASEBAND)
Les signaux numériques sont transportés sur une **fréquence unique**
Les signaux prennent la forme d'impulsions **discrètes** (interruptions entre chaque impulsion)
Les signaux peuvent être électriques ou lumineux
La transmission en bande de base occupe toute la bande passante (un seul signal à la fois)
Le câble constitue un **canal unique**
La transmission des signaux peut s'effectuer dans les deux sens(**bidirectionnelle**)

L'affaiblissement du signal

A mesure qu'il parcourt un câble, le signal électrique diminue progressivement en **intensité** et peut être l'objet de **distorsion**. Un signal trop faible ou déformé risque de ne pas être reconnu ou d'être mal interprété par son destinataire; c'est pourquoi des **répéteurs** sont installés sur des câbles trop longs afin de rétablir la force et la **définition** du signal d'origine.

La transmission téléphonique

La transmission téléphonique est une transmission **analogique** qui s'effectue par l'intermédiaire des câbles des réseaux téléphoniques et d'un **modem** qui opère la modulation et la démodulation du signal. Le fil du **téléphone** est un **câble** qui dispose de plusieurs fils de cuivre (la paire torsadées et les connecteurs RJ45), chacun matérialisés par un **code couleur**. Deux seulement sont connectés à la prise de téléphone, et ils peuvent être utilisés pour la transmission analogique, l'un pour entendre et l'autre pour recevoir. Le réseau téléphonique public s'appèle en France le **RTC** (Réseau Téléphonique Commuté) et le **PSTN** (Public Switched Telephone Network) dans les pays anglo-saxons.

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 couteuses. 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 nomenclature des lignes de téléphone

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 cher. 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). Le choix entre une ligne commutée ou une ligne louée dépend de plusieurs critères, dont la durée, la fréquence des communications, le budget, le cout, les débits souhaités, la fiabilité attendue, les types d'information véhiculés.

Les fournisseurs de lignes proposent également des services ou des conditionnements qui accompagne 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.

Les lignes analogiques

Les lignes analogiques du réseau **RTC** (Réseau Téléphonique Commuté) 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 analogique. 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

Les lignes **DSL** (Digital Subscriber Line) correspondent à une nouvelle technologie qui utilise les lignes téléphoniques pour des transmissions numériques (digital). Les lignes DSL utilisent la paire torsadée en cuivre que l'on a tous chez soi, mais ne véhiculent 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**.

Les lignes analogiques RTC et DSL
Ligne RTC (Réseau Téléphonique Commuté) **Ligne 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). **Ligne 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). **Ligne 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. **Ligne VDSL** (Very high bit-rate Digital Subscriber Line) ne dépassent 3 kilomètres pour une vitesse comparable à celle des LAN (10 Mb/s).

La 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, sécurité). 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 et la location d'une ligne numérique spécialisée auprès d'un opérateur téléphonique est en général utilisés pour relier deux sites géographiques appartenant à une même entreprise.

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.

La transmission des lignes spécialisées numériques								
Réseau	Pont	**CSU/DSU**	Répéteur	**Ligne**	Répéteur	**CSU/DSU**	Pont	Réseau

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**).

Les modes de transmission numérique
La **commutation** de paquets ATM Le **Frame Relay** (ou Relais de trames) Les réseaux privés virtuels ou **VPN** (Virtual Private Network) qui utilisent le réseau internet. Il est virtuel parce qu'il n'utilise pas de ligne spécialisée mais les supports de communication 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

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.

Les lignes numériques sont les lignes **DDS** (Digital Data Service), les lignes T1 qui n'existent qu'aux États-Unis, les lignes E1 qui correspondent aux lignes T1 mais en dehors des États-Unis, les lignes T3 offrent les meilleures performances et les lignes 56 commutées (Switched 56) sont la version commutée des lignes DDS. Les lignes 56 commutées (Switched 56) sont la version commutée des lignes DDS. Les lignes 56 commutées peuvent être utilisées à la demande.

Les lignes **T1** offrent un débit de 1,544 Mb/s qui est la norme DS1. Les lignes T1 sont appelées des lignes **interurbaines** parce qu'elles relient les grandes villes américaines depuis les années 1960. Les lignes T1 peuvent être constituées de différents supports comme le coaxial, la fibre optique, les faisceaux hertziens.

Les lignes T1 utilisent le multiplexage (**multiplexing**) inventé par Bell Labs. Les réseaux téléphoniques commençaient à être saturés, une méthode, appelée «réseau T-Carrier», a permis de transmettre plusieurs appels en même temps sur le même câble. Les signaux provenant de différentes sources convergent vers un **multiplexeur** qui les transmet au fur et à mesure. Les signaux sont ensuite dé multiplexés et dispatchés.

Les lignes T1 sont très utilisées, mais très chers, aussi est-il possible de s'abonner à une ligne T1 **partielle**, c'est à dire à un ou plusieurs canaux de 64 Kb/s qui est la norme DS0. La bande passante d'une ligne T1 à 1,544 Mb/s est divisée en 24 **canaux** différents (Fractionnal T-1), chacun échantillonné 8000 fois par seconde. Il est possible, selon ses besoins de s'abonner à un seul canal d'une ligne T1 ou éventuellement à plusieurs canaux, c'est **l'agrégation** de canaux, qui permet d'augmenter la vitesse d'une ligne numérique par incréments de 64 Kb/s. Les lignes E1 correspondent aux lignes T1 en dehors des États-Unis, et offrent une vitesse de 2,048 Mb/s.

Les lignes T3 offrent les meilleures performances avec un débit de 45 Mb/s qui correspond à la norme DS3 avec un débit exact de 44 736 Mb/s. Les lignes T3 requièrent un support à hautes fréquences comme la **fibre optique** ou les **micro ondes**. Les lignes T3 sont utilisées par les très grandes entreprises et les fournisseurs d'accès à internet. Les lignes T3 peuvent être utilisée dans leur totalité ou partiellement.

Les débits des lignes numériques		
Lignes numériques	**Débits**	**Norme**
Les lignes DDS (Digital Data Service)	2 Kb/s	
Les lignes 56 commutées (Switched 56)	56 Kb/s	
Les lignes T1 (aux États-Unis)	1,544 Mb/s qui est la norme	DS1
Les lignes Fractionnal T1 (États-Unis)	24 canaux de 64 Kb/s	DS0
Les lignes E1	2,048 Mb/s	
Les lignes T3	45 Mb/s	DS3

La 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 représentent un moyen de confectionner des lignes spécialisées sur un réseau à commutation de paquets. Les circuits virtuels sont constitués d'une série de connexions logiques qui compose un itinéraire pour une communication sur internet. 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 **CVC** (Circuits Virtuels Commutés) ou **SVC** (Switched Virtual Circuits) utilisent les ressources d'un réseau commuté pour établir une liaison dédiées, avec un seul chemin. Les **CVP** (Circuits Virtuels Permanents) ou **PVC** (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.

Les types de réseaux étendus

Les réseaux étendus se présentent concrètement sous des dénominations qui englobent toutes les technologies qui permettent de réaliser une communication distante. Les dispositifs de connectivité de chacune de ces technologies diffèrent les uns des autres. Par exemple, un modem **RNIS** (Réseau Numérique à Intégration de Services) d'une ligne numérique «à la demande» n'est pas le même équipement qu'un commutateur CSU/DSU d'une ligne numérique «dédiée».

Les types de réseaux étendus (WAN)
X.25 analogique à commutation
Relais de trames (Frame Relay) numérique à commutation sur de la fibre
ATM (Asynchronous Transfert Mode) analogique et numérique à commutation sur cuivre et fibre
RNIS (Réseau Numérique à Intégration de Services) numérique à commutation de paquet sur T1
FDDI (Fiber Distributed Data Interface) réseaux numériques en anneaux sur cuivre et fibre
SONET (Synchronous Optical Network) numérique à commutation sur de la fibre
SMDS (Switched Multimegabit Data Service) analogique à commutation en bus double (open ring)

Les réseaux X.25

Le réseau X.25 est le réseau à Relais de Trames en France. Le réseau X25 est un réseau **analogique** à **commutation** de paquets. Le **maillage** est représenté sous la forme de nuages. Le réseau X25 propose 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) permet à des réseaux différents de pouvoir communiquer par l'intermédiaire de **passerelles**.

Les réseaux X25
Un réseau analogique à commutation de paquets
Des fonctionnalités de contrôle des erreurs élaborées, mais qui consomment de la bande passante
Une suite de protocoles X.25 (interface ETTD/ETCD)
Un hôte disposant d'une interface X.25
Un PAD (Packet Assembler Disassembler)
Une passerelle X.25
Des nœuds de commutation

Les réseaux Frame Relay

Le Relay de Trames (Frame Relay) est un réseau **numérique** à **commutation** de paquets sur de la **fibre** optique. C'est un réseau fiable, rapide, et sécurisé qui peut garantir une bande passante, et qui dérive des réseaux X.25 en France.

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 informations ou **CIR** (Committed Information Rate) 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 dans un autre format pour constituer la «**trame**» qui est véhiculée sur le réseau étendu. Le processus d'empaquetage des paquets et de dés-empaquetage prend du temps, ce qui affecte les performances des réseaux étendus en Relais de Trame.

L'alternative a cette inefficacité consiste à utiliser une «signalisation en bande de base» ou **CCS** (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.

Les réseaux Frame Relay
Les lignes numériques en fibre optique
Un réseau numérique à commutation de paquets
Une garantie de bande passante
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 longueurs variables
Des commutateurs de données (Data Switch)
Des ponts et des routeurs compatibles

Les réseaux ATM

Les réseaux **ATM** (Asynchronous Transfert Mode) sont 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. Les réseaux ATM proposent une technologie puissante et polyvalente, permettant de véhiculer la voix et les données, et pour des vitesses très élevées, allant de 155 Mb/s à 622 Mb/s, alors que la vitesse théorique maximale est de 1,2 Giga Bytes par seconde (Gb/s). Les réseaux ATM sont compatibles avec tous les supports de communication en cuivre, mais la fibre optique est plus appropriée. Les lignes en fibres optiques sont utilisées pour les dorsales longues distances des opérateurs téléphoniques.

Les trames sont appelées des **cellules** et ont une 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» ou **QOS** (Quality Of Service) qui sera intégré à la nouvelle version de TCP/IP (**ipv6**). Les identificateurs permettent 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. Les sociétés Fore Systems et IBM ont beaucoup investi dans la technologie ATM.

Les réseaux ATM (Asynchronous Transfert Mode)
Des réseaux analogiques (Large de Bande) ou numérique (Bande de Base) La transmission par commutation de paquets Des débits allant de 155 Mb/s à 622 Mb/s Une longueur de trames (cellules) de 53 Octets dont 5 Octets pour l'entête ATM Des identificateurs qui accompagnent les cellules pour une **QOS** (Quality Of Service) Une vitesse théorique de 1,2 Giga Bytes par seconde (Gb/s) Des équipements ATM spécifiques, dont des commutateurs ATM Les lignes en cuivre Les lignes en fibre optique

Les réseaux RNIS

Les réseaux étendus **RNIS** (Réseau Numérique à Intégration de Services) sont l'équivalent des réseaux **ISDN** (Integrated Services digital Network) aux États-Unis. L'ISDN est apparue aux États-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** à **commutation** de paquets bon marché, parce qu'il était difficile de configurer le **SPID** (Service Provider ID) des terminaux ISDN. Les réseaux RNIS représentent une solution peu chère et adaptée pour les petites entreprises.

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, et 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.

Les adaptateurs de terminaux IDSN sont relié 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. L'adaptateur ISDN se connecte au connecteur réseau (BNC, RJ45, 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 modems RNIS utilisent le protocole PPP pour établir la connexion. L'établissement d'une connexion RNIS est un processus de 2 ou 3 secondes.

Les réseaux RNIS ou ISDN
Un réseau numérique à commutation de paquet Trois canaux RNIS (2B+D) à accès de base (Basic Access ISDN) Deux canaux à 64 Kb/s appelés canaux B qui peuvent être utilisés simultanément Un canal à 16 Kb/s appelé canal D pour la gestion des données et de la ligne Vingt trois canaux B à 64 Kb/s et un canal D à 16 Kb/s RNIS (Primary Access RNIS) ligne T1 Les adaptateurs de terminaux IDSN sur des câbles croisés Les adaptateurs de terminal IDSN se branche à la carte réseau Ethernet (BNC, RJ45, AUI) Le modem RNIS en Bande de Base branché au port série de l'ordinateur

Les réseaux FDDI

Les réseaux **FDDI** (Fiber Distributed Data Interface) sont des réseaux en **anneaux** utilisant la **fibre** optique. Les réseaux FDDI ont été définies en 1986 par le comité **ANSI X3T9.5** afin d'accroitre les débits des architectures **Token Ring**. Les réseaux FDDI proposent une grande vitesse de transmission allant jusqu'à 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'appèlent 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**) utilise un jeton spécial appelé une balise (**beacon**).

Le support est limitée à 100 Km mais peut accueillir jusqu'à 500 stations, avec des répéteurs tous les 2 Km. Les réseaux FDDI constituent un environnement haut de gamme destiné aux 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 œuvre 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), l'on parle d'un système «biconnecté» (**Dual Homed**).

Les réseaux FDDI (Fiber Distributed Data Interface)
Un réseau en **fibre** optique Définition en date de 1986 par le comité ANSI X3T9.5 Architectures en **anneau** Token Ring. Un débit de 100 Mb/s Une topologie à anneau double Les ordinateurs connectés aux deux anneaux s'appèlent des stations de classe A Les ordinateurs connectés à un seul anneau s'appèlent des stations de classe B Topologie en anneau en étoile Un système de détection et de localisation des défaillances (Beaconing) 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 Câbles en **cuivre** pour les réseaux CDDI (Copper Distributed Data Interface) Concentrateurs MAU (Multistation Access Unit)

Les réseaux SONET

Les réseaux étendus **SONET** (Synchronous Optical Network) sont des réseaux en **fibre** optique définis par l'association **ESCA** (Exchange Carriers Standards Association) pour l'ANSI.

Les réseaux SMDS

Les réseaux SMDS (Switched Multimegabit Data Service)
Un réseau de **commutation** de paquets compatible avec la norme IEEE 802.6 La transmission **analogique** à large bande 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

PROTOCOL

Les protocoles réseaux

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 traitements de chacun des protocoles de la pile réseau.

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**.

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 générale, 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.

L'architecture OSI

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 envisageable. Soit, une tâche est

réalisée par un seul protocole, soit, toutes les tâches d'une couche OSI sont réalisées par un seul protocole, soit, plusieurs tâches appartenant à différentes couches OSI sont réalisées par un seul protocole, soit, 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** (1 & 2) spécifient la manière dont les matériels sont connectés, tandis que les couches **hautes** (7 à 3) énoncent les règles de communication. Les opérations des couches hautes sont plus complexes que celles des couches basses.

Le modèle OSI	
Layers	**Fonctions**
APPLICATION	Informations pour initier ou accepter une **requête** réseau (affichage)
PRESENTATION	Informations de **formatage**, de conversion, de cryptage (structure)
SESSION	Informations de **connexion** de départ d'un paquet (synchronisation)
TRANSPORT	Informations de segmentation, ordre, réception des **paquets** (fragmentation)
RESEAU	Informations **d'adressage** au paquet (routage)
LIAISON	Informations de **contrôle** d'erreurs d'un paquet (CRC) et queue (empaquetage)
PHYSIQUE	Missions des **trames** sur le réseau en forme de flux de bits bruts (impulsion)

Les liaisons de protocoles

Dans une pile de protocoles, toutes les couches du modèle OSI sont représentées au moins une fois. Quand la pile est limité au minimum, les requêtes réseaux traversent la pile sans qu'il y ait de choix. Le processus de transmission des données traverse successivement les protocoles de la pile jusqu'à l'émission des trames sur le réseau. Il n'y a pas de liaisons 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 liaisons 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, plusieurs protocoles de connexion ou d'acheminement des paquets (TCP/IP et NWLink) peuvent cohabiter à l'intérieur d'une même pile de protocole. Le protocole prioritaire de la pile 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 effectuera à son tour une tentative de connexion.

En générale, les liaisons de protocoles sont créées pendant l'installation du système d'exploitation réseau ou pendant l'installation des protocoles. L'utilisation de plusieurs protocoles permet de d'échanger des données dans un environnement hétérogène.

Les architectures réseaux

Certaines piles de protocoles sont reconnues par **l'industrie** informatique comme des **standards**. Les piles standards peuvent être, soit des protocoles **propriétaires**, développés par des sociétés privées commerciales, soit des protocoles issus d'organismes de **normalisation** qui ont initiés une réflexion volontaire et concertée.

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 en 7 couches et du modèle IEEE 802 (avec les deux sous-couches LLC et MAC).

Les architectures réseaux de l'industrie de l'informatique
L'architecture du modèle OSI en 7 couches L'architecture SNA (Systems Network Architecture) de la société IBM L'architecture DECnet de la société Digital Equipment Computer (DECnet phase V) L'architecture DNA (Digital Network Architecture) des réseaux locaux Ethernet ou MAN L'architecture NetWare de la société Novell L'architecture Apple Talk de la société Apple Computer L'architecture libre de la pile internet TCP/IP

La comparaison des piles de protocoles

La comparaison des piles de protocoles permet de se faire une vue d'ensemble de l'architecture réseau des différents protagonistes. Les recommandations du modèle OSI et les sept couches ne sont pas toujours respectées. Toutefois, le **modèle** OSI reste le canevas théorique qui peut servir d'exemple et d'échelle de comparaison. La pile de protocole Tcp-ip est universellement reconnue par les différentes **architectures**, parce que c'est une **implémentation** libre et éprouvée, et parce que c'est l'architecture du réseau internet.

<table>
<tr><th colspan="5">La comparaison des piles de protocoles</th></tr>
<tr><th>Modèle OSI</th><th>TCP-IP</th><th>Windows™ NT</th><th>Apple</th><th>NetWare</th></tr>
<tr><td>Application</td><td>NFS FTP SNMP</td><td>Redirecteur Serveur</td><td>AppleShare</td><td rowspan="2">NCP</td></tr>
<tr><td>Presentation</td><td>XDR SMTP RIP</td><td colspan="2">TDI</td><td>AFP</td></tr>
<tr><td>Session</td><td>ARP POP3 OSPF
PPP IMAT ICMP</td><td>NWLink NBT DLC</td><td>ASP ADSP ZIP PAP</td><td>Tube NetBIOS</td></tr>
<tr><td>Transport</td><td colspan="2">TCP</td><td>ATP NBP AEP RTMP
DDP</td><td>SPX
IPX</td></tr>
<tr><td>Network</td><td colspan="2">IP</td><td>Pilotes LAN</td><td>Pilotes LAN</td></tr>
<tr><td>Liaison</td><td colspan="2">Pilotes LAN
Couche MAC</td><td>Local Talk Token Ring Ether Talk</td><td>ODI NDIS</td></tr>
<tr><td>Physique</td><td colspan="4">La carte réseau</td></tr>
</table>

La simplification du modèle OSI

Les protocoles peuvent être classés par simplification en trois catégories, et non plus en sept couches qui sont la **recommandation** du 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 peut être réduit à trois couches, les couches APPLICATION, TRANSPORT et RESEAU.

Le simplification du modèle OSI en 3 couches	
Les sept couches du modèle OSI	**Les trois catégories générales**
APPLICATION	
PRESENTATION	APPLICATION
SESSION	
TRANSPORT	TRANSPORT
RESEAU	
LIAISON	RESEAU
PHYSIQUE	

Les protocoles APPLICATION

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

Les protocoles APPLICATION
APPC (Advanced Program to Program Communication) est le protocole SNA d'IBM AS/400
FTAM (File Transfer Access and Management) est un protocole OSI d'accès aux fichiers
X.400 est un protocole CCITT pour la transmission internationale de messagerie électronique
X.500 est un protocole CCITT offrant des services de fichiers et de répertoires répartis
SMTP (Simple Mail Transfer Protocol) pour le transfert de messagerie électronique
NFS (Network File System) pour l'échange et le partage de fichiers sous Unix™ et Gnu Linux
FTP (File Transfer Protocol) pour le transfert de fichiers
SNMP (Simple Network Management Protocol) pour la surveillance des matériels réseaux
TELNET est un protocole non sécurisé pour la connexion à des hôtes distants
SMB (Server Message Blocks) pour l'échange et le partage de fichier sous Windows™
NCP (Netware Core Protocol) pour la redirection des clients Windows™ vers un serveur Novell
Apple Talk et APPLESHARE est la suite de protocole d'Apple pour Macintosh™
AFP (Apple Talk Filing Protocol) pour l'accès à distance depuis des ordinateurs Macintosh™
DAP (Data Access Protocol) est un protocole DECnet pour l'accès aux fichiers

Les protocoles TRANSPORT

Les protocoles de la catégorie TRANSPORT assurent les connexions et le contrôle des transferts de données. Le protocole **X.25** est un ensemble de protocoles anciens pour les réseaux à commutation de paquets et qui était utilisé pour connecter des terminaux distants à de gros systèmes hôtes (**main frame**).

Le protocole **XNS** (Xerox Network System) 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, et qui a été le modèle de la pile SPX/IPX de Novell, mais qui a été progressivement remplacé par la pile TCP/IP. La pile XNS générait de nombreux messages de diffusion générale (**broadcast**), ce qui le rendait lent en plus d'être volumineux. Le protocole **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. Le protocole NetBEUI n'est pas routable, et est en partie basé sur le protocole de transfert SMB.

Les protocoles TRANSPORT
X.25 est un ensemble de protocoles anciens pour les réseaux analogiques à commutation de paquets
XNS (Xerox Network System) pour l'acheminement des paquets sur les réseaux Xerox
SPX (Sequential Paquet Exchange) pour l'acheminement des paquets sur les réseaux Novell
NWLink est la version de la société Microsoft du protocole SPX/IPX de Novell
NetBEUI (NetBIOS Extended User Interface) pour les réseaux locaux Windows™
ATP (Apple Talk Transaction Protocol) est un protocole Apple pour les ordinateurs Macintosh™
NBP (Name Binding Protocol) est un protocole Apple pour les ordinateurs Macintosh™
TCP (Transport Control Protocol) pour l'acheminement des paquets sur les réseaux TCP/IP

Les protocoles 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 et Token Ring.

Les protocoles RESEAU
IPX (Internetworking Packet Exchange) pour le routage des paquets sur les réseaux SPX/IPX
NWLink est la version de la société Microsoft du protocole SPX/IPX de Novell
NetBEUI est le protocole non routable des réseaux Windows™ et des sessions NetBIOS
DDP (Datagram Delivery Protocol) pour le transport Apple Talk des données Macintosh™
IP (Internet Protocol) pour l'adressage et le routage des paquets sur les réseaux TCP/IP

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 accrue très rapidement. Les chemins possibles pour qu'un paquet atteigne sa cible croissaient en fonction du nombre de nœud 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 en moyenne plus rapidement, parce qu'ils utilisent les routes les moins fréquentées ou les plus directes. Les protocoles routables sont conçus pour «traverser» les routeurs et prendre la route qui leur est indiquée.

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 développés par **IBM**. NetBIOS est relativement populaire parce que de nombreuses applications ont été programmées pour fonctionner avec cette interface. Le protocole NetBIOS est rapide, mais **non sécurisé**. Le protocole NetBIOS existe depuis le milieu des années 1980. Il a été fourni avec MSNET, le premier produit réseau de la société Microsoft. 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'utilisateur 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'appèle NBT.

Le protocole NetBEUI utilise des noms alphanumériques pour identifier les machines sur le réseau. Les **noms NetBIOS**, autrement dit, les noms d'hôte des ordinateurs, servent à 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 connaitre aux autres machines, ce qui utilise de la bande passante. Le protocole NetBEUI convient pour les petits réseaux qui utilisent les produits de la société Microsoft et les jeux en réseau LAN.

Les protocoles NetBIOS et NetBEUI
Petit, rapide, efficace pour de petit réseau isolé et non sécurisé
Protocole non routable
Réseau avec un seul segment
Adressage par les noms NetBIOS
Communications en broadcast
Fonctionne très bien avec les clients MS-DOS

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 permis aux utilisateurs de son système d'accéder au réseau internet. Toutefois, l'intégration de TCP/IP n'est pas «native». La traduction de SPX/IPX en TCP/IP prend un certain temps et ralentit quelque peu l'accès à internet.

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 IPS est unique et disponible immédiatement sans l'intervention de l'administrateur.

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, le système **Windows™ NT** installe TCP/IP et le considère comme le protocole par défaut du système. Le module Réseau du Panneau de Configuration du système 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. Dans un système **Gnu Linux**, la pile de protocole Tcp-ip est intégrée à la compilation du noyau (**kernel**). L'on dit que la pile de protocole Tcp-ip est "**native**" dans le système Gnu Linux, et il n'y a pas besoin de l'installer puisqu'elle s'y trouve déjà depuis plus de trente années. La pile de protocole Tcp-ip est indispensable pour communiquer avec le réseau **internet**.

Un réseau découpé en plusieurs segments doit utiliser un protocole **routable**, si les stations d'un segment sont sensées 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.

L'histoire de TCP/IP

Le protocole TCP/IP (Transport Control Protocol / Internet Protocol) est le plus connu des protocoles 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 intégrante du système d'exploitation BSD 4.2 et des systèmes Unix™ depuis le milieu des années 1970. Auparavant, c'était 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.

La pile TCP-IP

La pile TCP/IP est une pile de protocoles relativement volumineuse et sa vitesse d'exécution et de transmission des paquets est comparable à SPX/IPX. 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. La pile TCP-IP est relativement **volumineux**, mais **rapide**. Le protocole TCP/IP est un protocole en mode datagramme (**commutation** de paquets) avec connexion (**ack+sync**) et perte (**TTL**).

Le protocole IP dispose de fonctions standardisées, les «**API sockets**» qui se comportent de la même façon sur tous les types de matériels. Les sockets sont des mécanismes qui permettent la **communication inter processus distant**. C'est-à-dire que les sockets assurent l'échange de données entre différents processus appartenant à des systèmes différents reliés par le réseau. Le mécanisme des socket existe depuis 1969 avec Unix™ BSD 4.2 de l'université de Berkeley. La pile TCP/IP est très **répandue** et très **fonctionnelle**, mais assez compliqué et assez volumineux. En fait, l'inconvénient majeur provient de son **succès**, et de la diminution du nombre des adresses IP disponibles, en attendant la version **IPV6** appelé aussi IPNG.

La pile TCP-IP est une **norme** industrielle. Tous les réseaux reconnaissent les protocoles TCP/IP et correspond à un **standard** pour la communication inter réseau et particulièrement entre des réseaux hétérogènes. La pile TCP-IP assure **l'interopérabilité** entre les systèmes hétérogènes. Le protocole TCP-IP est un protocole **routable**.

De nombreux protocoles ont été développés pour la pile TCP-IP, que ce soit pour la gestion des adresses physiques du réseau (**arp**), le routage (**rip** et **ospf**), la réception des mails (**pop3** et **imap4**), l'envoie de mail à un serveur de messagerie (**smtp**), le transfert de fichier (**ftp**), ou la surveillance des réseaux (**snmp**). Le protocole **ARP** (Address Resolution Protocol) permet de retrouver l'association entre l'adresse IP (**@ip**) et l'adresse MAC d'une machine (**@mac**). Le protocole **RARP** (Reverse Address Resoltion Protocol) permet de faire l'inverse, c'est-à-dire retrouver à partir de l'adresse MAC (**@mac**) l'adresse IP (**@ip**) d'une station.

Les protocoles de la pile TCP/IP	
Nom	**Fonction**
SSH	**SSH** (Secure Shell) pour se connecter en mode sécurisé à un serveur ssh
UDP	**UDP** (User Datagram Protocol) protocole non connecté sans contrôle de flux (**no ack**)
HTTP	**HTTP** (Hyper Text Transport Protocol) affiche les pages HTML
FTP	**FTP** (File Transfer Protocol) s'occupe des transferts de fichiers
TELNET	**TELNET** permet d'établir une connexion non sécurisé à un hôte distant
TCP	**TCP** (Transport Control Protocol) assure la segmentation et la transmission des paquets
IP	**IP** (Internet Protocol) gère les adresses logiques des nœuds (**address**)
ARP	**ARP** (Address Resolution Control) associe les adresses IP et physiques MAC (**@mac**)
RARP	**RARP** (Reverse Address Resolution Control) associe les adresses MAC et IP (**@ip**)
RIP	**RIP** (Routing Internet Protocol) trouve la route la plus rapide (**route**)
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 les réponses (**ping**)
BGP/EGP	**BGP/EGP** (Border Gateway Protocol / Exterior Gateway Protocol) sécurise les réseaux
SNMP	**SNMP** (Simple Network Management Protocol) permet de gérer les matériels réseaux
PPP	**PPP** (Point to Point Protocol) permet d'établir une connexion distante par téléphone
NFS	**NFS** (Network File System) pour partager des fichiers sur le réseau
DNS	**DNS** (Domain Name Service) pour la résolution des noms de domaine
NIS	**NIS** (Network Information Service) centralise les informations d'un réseau (**nis domain**)
NNTP	**NNTP** (Network News Transport Protocol)
SMTP	**SMTP** (Simple Mail Transport Protocol) permet d'envoyer des courriers électroniques
POP3	**POP3** (Post Office Protocol version 3) permet de récupérer son courrier électronique
IMAP4	**IMAP4** (Internet Message Advertising Protocol version 4) pour la messagerie

TCP-IP

Le protocole Tcp-ip

Le protocole Tcp-ip est le protocole d'échange de données sur **internet** et sur la plupart des réseaux **intranet**. Le protocole Tcp-ip se compose de deux protocoles distincts, le protocole TCP et le protocole IP. Le protocole **TCP** (Transport Control Protocol) assure le transport des messages sur le réseau et correspond à la couche TRANSPORT du **modèle OSI**. Le protocole **IP** (Internet Protocol) assure l'adressage des messages et correspond à la couche RESEAU du modèle OSI.

Le protocole TCP est un protocole de **commutation** de paquets routés dans le maillage des routeurs du réseau internet. Les paquets (**packets**) sont découpés (**segments**), encapsulés (**datagrammes**) et véhiculés (**trames**) selon l'état du trafic (**trafic**), et empruntent le chemin (**route**) le plus directe ou le plus rapide. En théorie, un paquet peut très bien traverser l'atlantique pour arriver chez votre voisin.

Le protocole Tcp-ip est un protocole de **connexion**, c'est-à-dire que les messages ne sont pas simplement envoyés. L'émetteur entame toute une procédure de connexion avec le destinataire. Les échanges sont systématiquement vérifiés (**check**) et réceptionnés (**ack**), et parfois, ils sont même synchronisés (**sync**) et contrôlés (**control**). Autrement dit, l'expéditeur d'un paquet attend un retour de la part du destinataire.

La commande **"man tcp"** présente la mise en œuvre du protocole de connexion TCP.
La commande **"man udp"** présente la mise en œuvre du protocole non connecté UDP
La commande **"man ip"** présente la mise en œuvre du protocole d'adressage IP.

Les primitives réseaux

Le noyau (**kernel**) d'un système Gnu Linux intègre des **fonctions** ou des primitives réseaux qui sont des appels systèmes pour gérer les communications réseaux et la pile TCP/IP.

Les primitives réseaux du noyau Gnu Linux
listen ()
connect ()
send ()
receive ()
disconnect ()

Les RFC

Les **RFC** (Request For Comments) sont des documents techniques qui décrivent les mécanismes des technologies utilisés sur internet et dans les réseaux en général. Ce sont des documents qui explicitent en détail le fonctionnement d'un protocole ou d'une norme et qui font référence pour les constructeurs de matériels, les opérateurs, les administrateurs et les professionnels des réseaux et de l'industrie informatique. Les RFC sont numérotés dans leur ordre historique d'apparition, de la plus anciennes à la plus récentes. Des **sites** spécialisés proposent la consultation en ligne de ces documents.

Les RFC (Request For Comments)
RFC 768 UDP
RFC 791 DARPA
RFC 792 ICMP
RFC 793 TCP
RFC 821 SMTP
RFC 822 MAIL
RFC 950 SUBNET
RFC 977 NNTP
RFC 1058 ROUTING IP
RFC 1178 DOMAIN NAME
RFC 1180 TEACHING TCPIP
RFC 1208 GLOSSARY
RFC 1219 ADDRESSING
RFC 1234 ROUTING IPX
RFC 2196 SECURITY
RFC 1597 PRIVATE NETWORK

La communication client serveur

La communication client serveur est un **échange** entre deux ordinateurs, l'un joue le rôle du client et l'autre joue le rôle du serveur. Parfois les rôles s'intervertissent.

La communication client serveur				
Client	**Network**			**Server**
connect	1	---->	2	listen
receive (ack)	4	<----	3	send (ack)
send (request)	5	---->	6	receive (request)
receive (response)	8	<----	7	send (response)
disconnect	9	---->	10	close connexion

L'entête TCP

L'entête TCP permet le transport des paquets. L'entête TCP est de 40 Octets. Certaines informations des entêtes sont importantes comme les drapeaux (**flags**) qui permettent de configurer la communication. Par exemple, **TTL** (Time To Live) indique le nombre maximal de saut de routeurs, **MSS** (Maximum Segment Size) indique la taille maximale des segments, ou **IRTT** (Initial Round Trip Time). Les initiales ont une signification: U (up), H (host), G (gateway), D (dynamic) et M (modified).

L'entête TCP (40 Octets)
Le contrôle des erreurs avec réexpédition (**check**)
Le contrôle des séquences avec ré-assemblage (**order**)
Le contrôle de flux avec des “fenêtres de tir” (**timing**)
L'accusé de réception (**ack**)
Le port de la source émettrice (**sport**)
Le port de destination (**dport**)
Le numéro de séquence des données (**sequence**)
Le numéro de l'accusé de réception (**ack number**)
La taille de l'entête TCP (**data offset**)
Le drapeau de contrôle (**control**)
La fenêtre de tir (**window**)
Le total de contrôle de l'entête TCP (**tcp checksum**)
Le pointeur d'urgence (**urgent**)
Les options éventuelles comme la taille maximale (**options**)

L'entête IP

L'entête IP permet l'adressage et le routage des paquets ou des trames sur le réseau TCP/IP. L'entête IP est de 20 Octets.

L'entête IP (20 Octets)
La version du protocole IPV4 ou IPV6 (**ipv4**)
La longueur de l'entête IP (**length**)
Le type de service prioritaire ou non (**service**)
La longueur totale du paquet (**total**)
L'identification du paquet ou le numéro de séquence des données (**sequence**)
Les informations de défragmentation (**defrag**)
Le nombre de sauts de routeurs encore possible (**TTL**)
Le nom du protocole de transport (**tcp**)
Le calcul de la parité de contrôle de l'entête IP (**ip checksum**)
L'adresse IP de l'ordinateur émetteur (**@source**)
L'adresse IP de l'ordinateur de destination (**@target**)
Les options éventuelles (**options**)

ADDRESS

L'adressage Tcp-ip

Le protocole Tcp-ip utilisent les adresses IP pour identifier et communiquer avec les autres nœuds d'un réseau. Les adresses IP internationales sont utilisées pour **internet** et les adresses IP privées sont utilisées pour les réseaux **privés** sous Tcp-ip. L'adressage Tcp-ip est utilisé sur internet dans sa version IPV4 (32 bits) et prochainement dans sa version IPV6 (128 bits).

Ce sont des organismes internationaux de régulation du réseau internet qui se chargent d'octroyer les adresses internationales du réseau Tcp-ip mondial, afin d'en assurer l'unicité sur internet. Ces organismes sont l'IANA aux États-Unis et l'Internic en France. Les adresses internes des stations sont gérées à la convenance de l'administrateur réseau.

Liens vers internet

Internet Links				
ietf.net	icann.org	network-solutions.com	internic.net	inria.fr
	archie.au	http://www.cybertheque.fr	nic.fr	enst.fr
		http://metalab.unc.edu	nic.switch.ch	wuarchives.wnstl.edu
		http://archie.emnet.co.uk	ftp.iecc.com	liszt.com
http://www.cotse.com/networkcalculator.html		nic-nfs.net	sri.com	infoseek.com

L'espace d'adressage

L'espace d'adressage est définie en fonction du nombre de bit nécessaire pour exprimer une adresse IP. Plus le nombre de bit est important, et plus le nombre de possibilité est importante.

Il existe deux espaces d'adressage pour les adresses IP. L'espace d'adressage de 32 bits correspond au système actuel d'adresses IP (Ipv4). L'espace d'adressage de 128 bits correspond au prochain système d'adresses IP qui est en train d'être élaboré (Ipv6). Le protocole IPV6 est la version 6 d'IP ou **IPNG** (IP New Generation).

L'adressage unique

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 forment une hiérarchie. Les réseaux (**network**) sont connectés entre eux par l'intermédiaire de

dispositifs de connexion (**routers**). A l'intérieur de ces réseaux se trouvent les stations qui ont accès à internet. Les adresses réseaux (**address**) comportent une partie réseau (**net**) qui permet aux paquets (**packets**) de circuler dans la hiérarchie, et une partie station (**host**) qui permet d'identifier la station à l'intérieur du réseau.

Pour contacter une autre station sur internet, la station émettrice (**source**) et le protocole de communication (**protocol**) ont besoin de connaître l'adresse IP du destinataire (**target**), et d'identifier le réseau (c'est la partie réseau de l'adresse IP) et d'identifier la station 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. La séparation entre les deux parties s'effectue avec le masque de réseau (**netmask**).

Le masque de sous réseau

L'adresse IP est composée de deux parties, la partie réseau (**net**) et la partie station (**host**). Le masque de sous réseau permet de savoir qu'elle est la partie des 32 bits qui est utilisé pour identifier le réseau, et donc par déduction quelle est la partie qui permet d'identifier la station.

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 qui sont réservées pour identifier, respectivement, le réseau (**zero**), et les messages de diffusion générale (**broadcast**).

Pour identifier une station sur le réseau internet, il faut connaitre deux séries de 32 bits. La première série correspond à l'adresse IP (**address**) et la seconde correspond au masque de réseau (**netmask**). Les deux séries permettent de déduire le réseau (**net**) et la station (**host**).

Le protocole TCP/IP accepte les masques de "sous réseaux" et les masques de "sur réseaux".

Un exemple d'adressage

Un exemple d'adressage internet et intranet					
Internet	Public Address	55.55.55.55	**Router**	Private Address	198.168.32.1
	Public Net Mask	255.255.255.0		Private Net Mask	255.255.0.0
	Public Network	55.55.55.0		Private Network	198.168.0.0
	Public Host	0.0.0.55		Private Host	0.0.32.1

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. La valeur décimale de chaque octet peut être comprise en 0 et 255 (256 possibilités = 2 à la puissance 8 = 2^8), et l'espace d'adressage est compris entre 1 et 4 294 967 296 (2 à la puissance 32 moins 1). Il faut retirer l'adresse de broadcast qui a tous ses bits à un et qui s'exprime sous la forme 255.255.255.255.

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 = 2^8	16 puissance 4 = 65 536 = 16^4 2 puissance 16 = 65 536 = 2^16
Possibilité d'adresse	256 puissance 4 = 2^32 2^32 = 4 294 967 296	65 536 puissance 8 = 2^128 2^128 = un nombre très grand

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 réseaux sera plus important, mais le nombre de station par sous réseau le sera moins.

Les classes d'adresse

La partie réseau de l'espace d'adressage 32 bits est divisé en cinq classes. Les classes sont identifiées par des lettres (A, B, C, D, E). Chacune des classes est spécialisée pour correspondre à un type d'organisation ou d'usage. Par exemple, une adresse IP de la classe A pourra être attribuée à une multinationale qui dispose d'un grand réseau et de nombreux postes. Une adresse de classe C pourra être attribuée à une petite entreprise. Les adresses IP de la classe A sont rares et chères.

A chaque classe correspond un nombre maximum de réseau 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 adresses de classe A
Les adresses de classe B
Les adresses de classe C
Les adresses de classe D
Les adresses de classe E

Les classes des adresses IP (IPV4)					
Class	**A**	**B**	**C**	**D**	**E**
Role	Internationales	Nationales	Régionales	Multicasting	Research
Form	N.H.H.H	N.N.H.H	N.N.N.H	N.N.N.H	N.N.N.H
Mask	255.0.0.0	255.255.0.0	255.255.255.0	255.255.255.0	255.255.255.0
Net	x.H.H.H	x.x.H.H	x.x.x.H	x.x.x.H	x.x.x.H
Host	N.y.y.y	N.N.y.y	N.N.N.y	N.N.N.y	N.N.N.y
Pool	1.0.0.0 126.0.0.0	128.1.0.0 191.254.0.0	192.0.1.0 223.254.254.0	224.254.254.0 239.254.254.0	240.254.254.0 254.254.254.0
Out	0.0.0.0 (boot)	127.0.0.0 (loopback)	127.0.0.1 (localhost)	255.255.255.255 (internet broadcast)	
Local	10.0.0.0/8	172.16.0.0/16 172.31.0.0/16	192.168.0.0/24		
Real	55.0.0.1	177.22.0.1	199.33.44.1		
Zero	First	Second	Third	Fourth	Fith
Bytes	00000001.H.H.H 01111110.H.H.H	10000000.N.H.H 10111110.N.H.H	11000000.N.N.H 11011110.N.N.H	11100000.N.N.H 11101110.N.N.H	11110000.N.N.H 11110110.N.N.H
Nets	126-1 =125	(192-128)x(254-1) =16192	(223-192)x(254)x(254-1) =1992122		
Hosts	16777216= (256^3)= (2^24)	65 536= (256^2)= (2^16)	256= (2^8)		

Les adresses conventionnelles

Certaines adresses sont réservées pour une utilisation conventionnelle (**special**), et ne peuvent être attribuées, ni pour internet, ni pour un usage privé. D'autres sont réservées pour adresser les réseaux privés sous le protocole Tcp-ip.

Les adresses conventionnelles		
Class	**Range**	**Fonction**
www	0.0.0.0	Adresse pour la procédure de démarrage de l'ordinateur (**current node**)
	255.255.255.255	Adresse de diffusion générale pour le réseau internet (**internet broadcast**)
Local	127.0.0.0	Adresse de boucle (**loopback**)
	127.0.0.1	Adresse pour désigner l'ordinateur localement (**localhost**)
A	10.0.0.0	**Réseau** privé de classe A (**private A network**)
	10.0.0.1	Adresse d'un nœud privé de classe A (**First A node**)
	255.0.0.0	Masque de réseau privé de classe A (**private A mask**)
	10.255.255.255	Broadcast privé de classe A (**private A broadcast**)
B	176.16.0.0	**Réseau** privé de classe B (**private B network**)
	176.16.0.1	Adresse d'un nœud privé de classe B (**First B node**)
	255.255.0.0	Masque de réseau privé de classe B (**private B mask**)
	176.0.255.255	Broadcast privé de classe B (**private B broadcast**)
C	192.168.0.0	**Réseau** privé de classe C (**private C network**)
	192.168.0.1	Adresse d'un nœud privé de classe C (C **node**)
	255.255.0.0	Masque de réseau privé de classe C (**private C mask**)
	192.168.255.255	Broadcast privé de classe C (**private C broadcast**)

Le routage inter domaine sans classe

Le routage inter domaine sans classe ou **CIDR** (Classeless Inter-Domain Routing) 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'adresse de réseau de classes B (avec 65 536 adresses IP possibles), soit parce qu'elle ne peut se l'offrir, soit parce qu'il n'existe plus d'adresse 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.

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, la partie réseau est 192.155.87.0 (**net**), et 192.155.87.x avec x allant de 1 à 254 pour la partie machine. Ainsi, l'adresse de broadcast d'un tel réseau serait 192.155.87.255. Le **masque** de réseau (255.255.255.0) et l'adresse de **broadcast** (192.155.87.255) doivent se compléter pour mettre tous les bits à un (255.255.255.255).

Le masque réseau et l'adresse de broadcast				
255.255.255.0	+	N.N.N.255	"="	255.255.255.255

L'adressage Ipv6

L'adressage **IPV6** (IP Version 6) ou **IPNG** (IP New Generation), sera fondé sur un espace d'adressage de 128 bits. L'adressage IPV6 disposera de fonctionnalités natives, de priorité, d'authentification et de cryptage.

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 octroit les coordonnées de classe B (152.80.0.0).

Une adresse de classe B présente toujours un masque avec les deux premiers octets à "un", ce qui donne toujours la possibilité d'avoir 65 536 stations sur le réseau avec chacune une adresse internet internationale valide. En achetant une classe B, l'administrateur réseau achète en réalité la capacité de mettre 65 536 adresses internet. Les deux premiers bits d'une classe B sont toujours égaux à "10".

Les deux premiers octets (16 bits) du masque principal de réseau sont à 1. Pour constituer 4 sous réseau 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.

Un exemple de sous réseaux de classe B								
	1000 0000	0100 0000	0010 0000	0001 0000	0000 1000	0000 0100	0000 0010	0000 0001
	128	64	32	16	8	4	2	1
Mask	255.255.0.0		1111 1111 .	1111 1111 .	0000 0000 .	0000 0000		
Net	152.80.0.0		1001 1000 .	0101 0000 .	0000 0000 .	0000 0000	2^0 = 1 net 2^16 = 65 536 nodes	
Submask	255.255.128.0		1111 1111 .	1111 1111 .	1000 0000 .	0000 0000	2^1 = 2 Subnets 2^15 = 32 768 stations	
Submask	255.255.192.0		1111 1111 .	1111 1111 .	1100 0000 .	0000 0000	2^2 = 4 Subnets 2^14 = 16 384 stations	
Submask	255.255.224.0		1111 1111 .	1111 1111 .	1110 0000 .	0000 0000	2^3 = 8 Subnets 2^13 = 8 192 stations	
Submask	255.255.240.0		1111 1111 .	1111 1111 .	1111 0000 .	0000 0000	2^4 = 16 Subnets 2^12 = 4 096 stations	
Submask	255.255.248.0		1111 1111 .	1111 1111 .	1111 1000 .	0000 0000	2^5 = 32 Subnets 2^11 = 2 048 stations	
Submask	255.255.252.0		1111 1111 .	1111 1111 .	1111 1100 .	0000 0000	2^6 = 64 Subnets 2^10 = 1 024 stations	
Submask	255.255.252.0		1111 1111 .	1111 1111 .	1111 1110 .	0000 0000	2^7 = 128 Subnets 2^9 = 512 stations	
Submask	255.255.255.0		1111 1111 .	1111 1111 .	1111 1111 .	0000 0000	2^8 = 256 Subnets 2^8 = 256 stations	

Un masque de sous réseau de 2 bits à 1 supplémentaires (11000000 = 192 en décimale) se présente ainsi: le **masque de sous réseau 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**. 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 ?

N.N.0000 0000.H donne un premier sous réseau = 158.80.0.0
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).

N.N.0100 0000.H donne un deuxième sous réseau = 158.80.64.0
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

N.N.1000 0000.H donne un troisième sous réseau = 158.80.128.0

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

N.N.1100 0000.H donne un quatrième sous réseau = 158.80.192.0
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

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

N.N.0000 0000.H donne un premier sous réseau = 158.80.0.0
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).
N.N.0010 0000.H donne un deuxième sous réseau = 158.80.32.0
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
N.N.0100 0000.H donne un troisième sous réseau = 158.80.64.0
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
N.N.0110 0000.H donne un quatrième sous réseau = 158.80.96.0
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
N.N.1000 0000.H donne un cinquième sous réseau = 158.80.128.0
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
N.N.1010 0000.H donne un sixième sous réseau = 158.80.160.0
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
N.N.1100 0000.H donne un septième sous réseau = 158.80.192.0
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
N.N.1110 0000.H donne un huitième sous réseau = 158.80.224.0
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

Un masque de sous réseau de 4 bits à 1 supplémentaire (11110000 = 240 en décimale) se présente ainsi: le **masque de sous réseau 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 décimale
00010000 = 16 en décimale
00100000 = 32 en décimale
00110000 = 48 en décimale
01000000 = 64 en décimale
01010000 = 80 en décimale
01100000 = 96 en décimale
01110000 = 112 en décimale
10000000 = 128 en décimale
10010000 = 144 en décimale
10100000 = 160 en décimale
10110000 = 176 en décimale
11000000 = 192 en décimale
11010000 = 208 en décimale
11100000 = 224 en décimale
11110000 = 240 en décimale

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 adresses 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 adresses 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 adresses IP différentes. Les adresses IP seraient toutes entièrement définies par le 4^{ième} octet.

Un masque de sous réseau de15 bits à 1 supplémentaire (11111111 = 255 pour le 3^{ième} octet et 11111110 = 254 en décimale pour le 4^{ième} 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 adresses 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 3^{ième} octet et 11111110 = 255 en décimale pour le 4^{ième} octet) se présente ainsi: 255.255.255.255. Un tel masque ne serait pas utilisé dans la pratique puisqu'il correspond par convention à l'adresse de broadcast générale.

Toutefois, 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 bit 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.

SIGNAL

Les signaux électriques

Les ordinateurs utilisent un langage binaire (**binary digit**). Le langage binaire constitue la chaîne numérique (**digital**) et virtuelle (**virtual**). Le langage binaire permet de calculer (**process**), de stocker (**data**), de présenter les données (**show**) et de les communiquer (**share**). Les machines communiquent entres elles par l'intermédiaire de signaux électriques codés qui circulent sur le câble. Le signal électrique court sur le câble à la vitesse de la lumière (en réalité un peu moins vite à cause de la résistance du support).

Les types de signaux

Les signaux peuvent être électriques (**electrical**), lumineux (**light**) ou mécaniques (**wave**). La **propagation** du signal dépend de la conductivité du support sur lequel il est véhiculé. Le signal peut prendre différentes formes et sa transmission s'effectue sur un support de communication bien précis.

Les types de signaux et leurs supports	
Signal	**Support**
Les impulsions électriques	Le cuivre pour les câbles coaxiaux et en paires torsadées Les métaux comme l'or sont de très bons conducteurs
Les impulsions lumineuses	Le verre des câbles en fibre optique
Les vibrations mécaniques	L'eau pour les dauphins Le cuir de la peau de bête pour les tambours L'aluminium ou la fonte pour les casseroles de la ménagère
Les ondes aériennes	L'air ou l'espace pour les ondes radio et les ondes des satellites

La fréquence du signal

La fréquence d'un signal électrique peut être analogique ou numérique. La fréquence analogique ressemble aux ondulations (**waves**) d'un serpent dans un tunnel. La fréquence analogique utilise une plage de fréquence d'une certaine largeur. Il y a de nombreuses possibilités entre le haut et le bas, c'est pourquoi, elle est utilisée dans le monde des télécommunications pour transmettre la voix par le téléphone.

La fréquence numérique ressemble aux créneaux (**square**) d'un château fort. La fréquence numérique n'utilise qu'une seule fréquence. Il n'y a que deux possibilités, ça passe ou ça ne passe pas, comme dans le monde binaire de l'informatique.

Le bruit

Les câbles en cuivre véhiculent des impulsions électriques qui dégagent des **ondes** électromagnétiques tout autour. C'est ce qu'on appèle les **interférences** qui peuvent se produire entre plusieurs câbles, et perturber la qualité du signal. De plus, ce **rayonnement** est susceptible d'être écouté par **induction**. L'induction consiste à installer une boucle magnétique qui entoure le câble, et qui est capable de détecter et de capturer les signaux.

Les câbles en fibre **optique** sont de ce point de vue beaucoup plus sécurisés parce qu'ils véhiculent les données avec les impulsions lumineuses générées par un laser. Les signaux lumineux ne produisent pas de bruit, mais dégagent une **aura** de lumière. Les données ne peuvent pas être interceptées par la méthode de l'induction. Par contre, il ne faut jamais regarder à l'œil nu l'extrémité d'un câble en fibre optique, car le **faisceau** lumineux peut bruler la rétine.

Le domaine de collision

Les machines qui sont placées sur le même segment sont susceptibles d'émettre simultanément. Cela se produit, quand la méthode d'accès au réseau le permet, c'est à dire, quand il y a un accès multiple comme pour la méthode d'accès CSMA/CD. Le segment sur lequel les machines sont placées en concurrence, s'appèle «**le domaine de collision**». Plus le nombre de machines est important dans le domaine de collision, et plus grande est la probabilité qu'une collision survienne. C'est d'ailleurs pour cette raison que les concepteurs d'Ethernet ont limité le nombre de machines sur un seul segment.

Quand deux machines émettent un signal électrique en même temps, il y a **collision**. En cas de collision, aucun des messages ne sera transmis, parce que le message est alors brouillé. Les deux machines devront s'entendre pour que chacune émette chacun son tour. Ce procédé d'accès et de partage du **support** est communément appelé la **méthode** de transmission. Pour qu'il n'y ait pas de confusion, une seule machine à la fois peut envoyer des signaux électriques sur le support de connexion.

Le rebond du signal

Dans un réseau en bus, le signal électrique parcourt toute la longueur du câble. Arrivé à la fin du câble, se produit le phénomène de rebond du signal. Le rebond du signal est un phénomène de **réflectrométrie**. Quand celui-ci n'est pas absorbé en bout de câble, le signal rebondit alors en parcourant le câble dans le sens opposé. C'est pourquoi les câbles des réseaux en bus sont toujours terminés par des bouchons de terminaison (**terminator**) installés en bout de câble. Les bouchons de terminaison absorbent le signal et libèrent le câble de toute interférence.

Le signal électrique d'un réseau en bus peut rebondir pour plusieurs raisons. La raison principale est souvent que le bouchon de terminaison manque, qu'il est mal installé ou qu'il est défectueux. Parfois, le

câble est sectionné. Si le signal rebondit de part et d'autre, alors celui-ci n'est jamais absorbé, ni d'un coté, ni de l'autre, et le rebond **monopolise** le câble, alors, aucune machine ne peut émettre et le réseau est saturé.

L'intensité du signal

L'atténuation du signal électrique correspond à une diminution de **l'intensité** du signal quand il se déplace le long d'un fil de cuivre. Plus le câble est long et plus l'atténuation du signal est importante. C'est pourquoi certaines spécifications réseaux imposent une longueur maximal de **segment**. En général, la distance affaiblie le signal.

Dans le cas de l'informatique, le contrôle des erreurs et la régénération du signal ralentissent également l'acheminement des données. A mesure qu'il parcourt un câble, le signal électrique diminue progressivement en intensité, et peut être l'objet de distorsion. Un signal trop faible ou déformé risque de ne pas être reconnu ou d'être mal interprété par son destinataire. Ainsi, des répéteurs (**repeater**) sont installés sur des câbles trop longs afin de rétablir la force et la **définition** du signal d'origine.

La prolongation du câble

Un prolongateur ou BNC en «T» (**barrel connector**) permet de relier deux câbles ensembles afin de constituer un segment plus grand. Toutefois, les prolongateurs ont une limite, ils affaiblissent le signal électrique. C'est pourquoi, il est préférable, soit d'acheter dès le départ un câble plus long, soit d'interposer un répéteur (**repeater**). Le répéteur, non seulement connecte les deux câbles pour n'en former qu'un seul, mais aussi, amplifie et régénère le signal avant de le réexpédier.

L'impédance

L'impédance correspond à la **résistance** opposée par un fil conducteur au courant électrique alternatif qui le traverse. L'impédance est mesurée en **OHM**. Quand elle existe, l'impédance d'un câble montre qu'il y a un courant électrique qui le traverse. L'impédance d'un câble doit être d'une certaine valeur afin que le courant électrique circule convenablement. La résistance d'un câble coaxial fin est plus importante que pour un câble coaxial épais; plus le diamètre du câble est important et plus le courant le traverse facilement. La **vitesse** de transmission est plus grande avec un câble coaxial épais.

Les mesures de l'impédance s'effectuent à l'aide d'un appareil qui s'appèle un **ohmmètre**. Les mesures sont prises sur le câble, les connecteurs et/ou les bouchons de terminaison. Les mesures qui restituent les valeurs de 50 Ohm ou de 75 Ohm, selon le type de câble, montrent que le courant passe bien, que le média fonctionne correctement, et qu'il n'y a pas de problèmes sur le support de communication. La mesure zéro (**zero**) implique qu'il n'y a pas de circulation d'électron et qu'il y a un court circuit quelque part. La mesure infinie (**infinite**) indique qu'il n'y a pas de bouchon de terminaison, ou que l'un d'entre eux est défectueux, ou que le câble est coupé quelque part.

La bande passante

La bande passante d'un câble est définie par la différence entre la fréquence (**frequency**) minimale et la fréquence maximale. On parle de largeur de la bande passante (**bandwidth**). Plus la largeur de la bande passante est importante, et plus grand est le nombre de canaux possibles. Le mode de transmission en large de bande (**broadband**) des réseaux analogiques permet l'utilisation de plusieurs bandes de fréquences sur le même câble. Par extension, l'expression "bande passante" est utilisée pour désigner la quantité maximale théorique de bits par seconde qui peut être véhiculée, c'est-à-dire le **débit**.

Les protections antistatiques

En général, les cartes d'extension ou les cartes réseaux sont vendues neuves à l'intérieur d'un sachet plastique en **mylar** argenté. Toutes les manipulations des composants internes de l'unité centrale d'un ordinateur doivent être effectuées avec la plus grande précaution afin de ne pas endommager les composants électroniques très fragiles.

Par exemple, l'utilisation d'un **bracelet** antistatique raccordé à une **masse**, ou le **réflexe** de toucher des mains régulièrement un objet métallique relié au sol, permettent d'équilibrer l'énergie **statique** qui s'accumule dans le corps.

BAND

Les types de communication

Les communications peuvent être classées en fonction du destinataire, de la direction des signaux ou des chemins qu'elles peuvent empruntés.

La direction des signaux des communications peut être unidirectionnelle (**simplex**), bidirectionnelle (**full duplex**), bidirectionnelle alternée (**half duplex**). Le destinataire peut être unique (**unicast**), multiple (**multicast**) ou la diffusion peut être générale (**broadcast**). La communication peut être décrite comme une relation privilégiée (**point to point**) ou de masse (**one to many**). Les chemins empruntés par les communications peuvent être dédiés (**specialisation**) ou indéterminés et variables selon le trafic (**commutation**).

La transmission des signaux

Il existe principalement deux techniques ou modes de transmission des signaux qui sont utilisés en informatique. La transmission en large de bande (**broadband**) est une transmission **analogique**. La transmission en bande de base (**baseband**) est une transmission **numérique**. La transmission d'un signal peut également se différencier selon que l'émetteur et le récepteur fonctionne (**synchrone**) ou pas (**asynchrone**) au même rythme.

La transmission **asynchrone** transfère des unités de données les une après les autres. Par exemple, une unité de donnée peut être un octet et valoir un caractère alphanumérique. Chaque unité est encadrée par un bit de début (**bit start**) et un bit de fin (**bit stop**). La transmission **synchrone** transfère les données par groupe de données rassemblées dans un paquet. Les données sont rassemblées, encadrées et expédiées en groupe. Par exemple, un paquet peut contenir 1500 octets de données. Les paquets sont constitués d'une entête, d'un corps et d'une queue.

Certains matériels peuvent servir de passerelle (**gateway**) entre les circuits asynchrones et synchrones. Par exemple, un **PAD** (Packet Assembler Disassembler) est utilisé sur les réseaux numériques français **Transpac** pour transformer les messages de l'asynchrone vers le synchrone et vice versa. Un PAD peut être intégré à une carte réseau et peut être programmé pour définir le nombre maximum d'octet d'un paquet.

Les modes de transmission des signaux
Analogique en large de bande (**broadband**) est continue, unidirectionnelle, en plages à deux câbles **Numérique** en base de bande (**baseband**) est discrète, bidirectionnelle, en canal unique à impulsion **Synchrone** opère par blocs de données en trames (entête, corps et queue) **Asynchrone** opère par unités de données encadrées (bits start et bit stop)

La transmission analogique

La transmission analogique est un mode de transmission en large de bande (**broadband**). La transmission analogique permet de diviser la bande de fréquence en plusieurs canaux de communication. La répartition de la bande de fréquence est l'une des spécificités de la transmission en large de bande. Ainsi, plusieurs communications peuvent se dérouler simultanément sur le même support.

Par exemple, la **télévision** par câble utilise ce mode de transmission. La bande passante est divisée en **plage**, et chaque plage constitue un canal de communication indépendant. Dans un réseau informatique, les ordinateurs qui communiquent sur une certaine fréquence doivent être configurés pour n'utiliser que la plage qui leur a été attribuée.

Les systèmes de communication analogique en large de bande ont recourts à des **amplificateurs** pour régénérer le signal analogique.

La transmission analogique en large de bande (broadband)
Les signaux analogiques circulent sur une **plage** de fréquence
Les signaux sont **continus**, sans interruption, c'est seulement la hauteur de la fréquence qui varie
Les signaux peuvent être des ondes électromagnétiques ou optiques
Le câble peut servir pour plusieurs **canaux** de transmission
Le câble peut véhiculer plusieurs signaux simultanément
Les signaux circulent toujours dans un seul sens
La transmission est toujours **unidirectionnel**

La transmission en basebande

La transmission numérique en base de bande (**basebande**) est le mode privilégié des communications informatiques parce que la chaine numérique n'est pas interrompue, et qu'un seul câble ou une seule ligne permet d'émettre et de recevoir.

La transmission numérique en base de bande (Base Bande)
Les signaux numériques circulent sur une **unique** fréquence
Les signaux ont la forme d'impulsions **discrètes** avec une interruption entre chaque **impulsion**
Les signaux sont électriques ou lumineux
La transmission occupe toute la bande passante et transporte un seul signal à la fois
Le câble constitue un **canal** unique
Les signaux peuvent circuler dans les deux sens
La transmission est **bidirectionnelle**
La transmission est bidirectionnelle simultanée avec des équipements spécialisés

La division de la bande

Le système de transmission **analogique** en large de bande (**broadband**) est **unidirectionnel**, il doit donc posséder deux **câbles** afin de véhiculer les signaux dans les deux sens. Deux câbles sont nécessaires pour que les ordinateurs d'un réseau soient en mesure d'émettre et de recevoir. Toutefois, à l'intérieur d'un même câble, la **bande** de fréquence peut être divisées en deux canaux. Les deux canaux d'un même câble peuvent transmettre deux communications différentes, mais dans la même direction.

Pour la communication dans les deux sens, les transmissions analogiques en large de bande (**broadband**) doivent disposer de deux câbles distincts, l'un pour recevoir et l'autre pour émettre. La division de la bande de fréquence analogique (**broadband**) en deux canaux consiste en une subdivision **médiane**. La bande passante est divisée en deux, horizontalement, avec un canal supérieur et un canal inférieur.

Pour les transmissions numériques **bidirectionnelles** (**baseband**), une partie de la bande passante sert pour recevoir et l'autre partie pour émettre.

METHOD

Les méthodes d'accès au support

La méthode d'accès à un réseau définit comment la carte réseau accède au câble réseau, c'est-à-dire comment les données sont déposées sur le **support** de communication et comment elles sont récupérées. La méthode d'accès permet de contrôler le trafic sur un réseau (qui parle, quand, et pour combien de temps). La méthode d'accès au réseau est aussi appelée «méthode de transmission».

Les méthodes d'accès au réseau permettent de différencier et de classer les réseaux en plusieurs catégories. Il existe trois méthodes différentes, la méthode de **collisions** (CSMA/CD et CSMA/CA), la méthode du **jeton** pour les réseaux en anneaux (Token Ring et FDDI) et la méthode de la **priorité** de la demande pour les réseaux Ethernet rapides (100VG-AnyLAN).

Les méthodes CSMA/CD et CSMA/CA concernent les réseaux Ethernet en bus et en étoile. La méthode du passage du jeton est particulière aux réseaux en anneau (Token Ring et FDDI). La méthode de la priorité de la demande est spécifique aux réseaux Ethernet 100VG-AnyLAN à 100 Mb/s.

Les méthodes d'accès au support
L'accès multiple, écoute de la porteuse (collisions acceptées, détectées, délais de retransmission)
Avec détection des collisions (CSMA/CD)
L'accès réservé (délais d'attente de transmission et le risque de collision est proscrit)
Avec prévention des collisions (CSMA/CA)
Le passage du jeton (Token Ring et FDDI)
L'accès au réseau est centralisée (des concentrateurs segmentent le réseau en bus anneau)
La priorité de la demande (DPMA) des réseaux Ethernet 100VG-AnyLAN à 100 Mb/s

Le choix de la méthode d'accès

Le choix de la méthode d'accès au réseau est déterminé par la carte réseau (**interface**). Certaines cartes réseaux ne peuvent fonctionner qu'avec telle ou telle méthode d'accès. Avant d'acheter une carte réseau pour intégrer une nouvelle station sur un réseau préexistant, il faut s'assurer qu'elle est compatible avec la méthode d'accès déjà utilisée sur le réseau. Sur un réseau (**network**), il ne peut avoir qu'une seule méthode d'accès (**method**) qui régente l'accès au support. Si ce n'était pas le cas, les règles de communication ne seraient pas harmonisées entre elles, et ce serait la cacophonie, le chaos, le tintamarre dodécaphonique, le brouhaha infernal des embouteillages kafkaïens.

Sur un réseau, toutes les cartes réseaux doivent être du même type et **partager** la même méthode d'accès au réseau. Ainsi, il est plus efficace d'avoir sur un même réseau des composants qui ont les mêmes caractéristiques. Par exemple, les communications sont plus efficaces avec des cartes réseaux qui transmettent à la même vitesse. En général, les cartes réseaux de même type, mais provenant de

fabricants différents, sont compatibles.

La puissance et la liberté

La référence aux mêmes **codes** et aux mêmes **procédures** est un indice d'appartenance à un même groupe, parce qu'ainsi, les communications sont règlementées, fiables et efficaces. L'uniformisation et l'homogénéisation est un facteur d'efficacité de toutes les **organisations**, qu'elles soient humaines ou matérielles.

Toutefois, la diversité, la pluralité et la mixité sont des facteurs d'adaptation et permettent d'aller à l'encontre de l'entropie universelle. C'est en quelque sorte le principe du **droit** commun républicain qui s'appliquent aux réseaux informatiques, mais qui ne saurait rien valoir sans la **liberté** et la démocratie. La puissance n'est pas en contradiction avec l'indépendance. La même loi pour tous, partout et tout le temps, mais avec la liberté de s'exprimer, de circuler et d'évoluer.

Les collisions de paquets

Les cartes réseaux écoutent le câble du réseau. Elles écoutent si une fréquence circule, si une **porteuse** passe, si un signal défile. Elles attendent pour émettre que le câble soit libre, c'est-à-dire qu'il n'y ait pas ou plus de porteuse. L'émission simultanée **brouille** le message et les trames ne sont pas exploitables. La collision de paquet ralentit les communications, parce que les trames doivent être réexpédiées.

Quand deux ordinateurs émettent exactement en même temps, leurs trames respectives vont se rencontrer et le signal de chacune sera complètement brouillé. Les trames qui sont entrées en collision ne sont plus exploitables, et leurs émetteurs doivent les réexpédier, si possible en évitant une nouvelle collision. Les collisions proviennent le plus souvent de l'émission **simultanée** de plusieurs ordinateurs. Le rôle de la méthode d'accès consiste, soit à réduire les inconvénients d'une telle **concomitance**, soit de l'empêcher.

Le rôle de la méthode d'accès

La méthode d'accès doit permettre, soit de limiter le risque d'occurrence des collisions et imposer une règle de retransmission fiable, soit de proscrire les conditions de survenue des collisions en interdisant l'accès multiple. Il s'agit donc de deux tactiques différentes pour faire face aux collisions. Il y a un choix à faire entre le délai d'attente ou le **délai** de retransmission quand le risque de collision est accepté. La méthode d'accès doit permettre à toutes les stations d'émettre. Le passage du jeton, qui interdit les collisions, permet également de répartir uniformément le temps de transmission entre toutes les stations, l'on parle alors de méthode d'accès **isofonctionnelle**.

La détection des collisions

La méthode d'accès **CSMA/CD** (Carrier-Sense Multiple Access / Collision Detection) impose à toutes les stations d'un réseau d'écouter continuellement le support de communication, pour détecter les porteuses et les collisions. C'est le **transceiver** (le mot valise «transmeter et receiver») qui écoute le câble, et qui lit les entêtes (**headers**) des paquets qui sont de 64 octets à 1500 octets au maximum. La méthode d'accès CSMA/CD est relativement fiable et rapide pour les réseaux composés d'un nombre restreint de stations.

Plus le nombre de station est important, plus le risque de collision s'accroît, et plus le nombre de collisions augmente, et plus les délais d'attente sont importants. Le nombre de collision peut exploser rapidement, et le réseau saturer, si le nombre de station est excessif. En parcourant le **support**, le signal s'atténue, les cartes réseaux doivent être en mesure de détecter une collision en bout de câble, or elles n'entendent plus rien au-delà d'une certaine distance (ni collisions, ni porteuses).

La méthode d'accès CSMA/CD est une méthode à **contention**, c'est-à-dire que les ordinateurs qui veulent émettre doivent rivaliser entre eux pour accéder au support. Les rivaux sont départagés par la durée aléatoire du délai d'attente en cas de collision. C'est une méthode fiable, rapide, mais limité à un nombre de stations **restreint**.

La méthode d'accès CSMA/CD (Collision Detection)
L'accès multiple au réseau permet à plusieurs ordinateurs d'émettre en même temps
Le risque de collision est accepté
Il n'y a pas de priorité, ni besoin d'une autorisation pour émettre
Écoute du câble et détection de la porteuse
Écoute du câble et détection des collisions
Interdiction à toutes les stations d'un réseau d'émettre si le support n'est pas libre
En cas de collision, les stations concernées cessent de transmettre pendant une durée aléatoire
Les stations émettent de nouveau si le câble est libre après ces délais
La distance maximale entre deux stations est de 2500 mètres
Une méthode à contention où les ordinateurs rivalisent entre eux pour accéder au support
Les rivaux sont départagés par la durée aléatoire du délai d'attente en cas de collision
Une méthode fiable, rapide, mais limité à un nombre de stations restreint

La prévention des collisions

La méthode d'accès **CSMA/CA** (Carrier-Sense Multiple Access / Collision Avoidance) n'est pas une méthode très répandue. Les collisions sont proscrites, chaque station avant d'émettre doit signaler son intention. Les demandes de transmission augmentent le trafic et ralentissent le réseau. La méthode d'accès CSMA/CA est plus lente que CSMA/CD.

Le passage du jeton

La méthode du passage du jeton est une méthode propre aux réseaux en **anneau**. Les collisions sont

proscrites, les stations ne peuvent pas émettre simultanément. Les stations doivent attendre le jeton qui donne la **permission** de «parler», il y a des **délais** d'attente pour obtenir le jeton, mais il n'y a pas de collisions, donc pas de délais de retransmission. Le jeton est un paquet spécial qui passe de station en station, et qui autorise celle qui le détient à émettre.

Les stations sont ordonnées les unes par rapport aux autres, et la plus haute dans la **hiérarchie** a la responsabilité de surveiller le bon fonctionnement du jeton (la durée des trames pour parcourir l'anneau, le temps moyen de rotation, la suppression des trames qui sont revenues à leur expéditeur, l'avertissement des autres stations qu'il est toujours le **superviseur**), et éventuellement d'en créer un nouveau. Le superviseur d'un réseau Token Ring est d'abord la première station allumée sur le réseau, puis si celle-ci se déconnecte, il y a une **élection** du nouveau superviseur. Après une élection, c'est la station qui possède l'adresse MAC la plus grande qui est élue superviseur.

La priorité de la demande

La méthode d'accès de la priorité de la demande ou **DPMA** (Demand Priority Access Method), est une méthode d'accès récente qui a été mise au point pour les réseaux mixtes en bus en étoile. Les réseaux Ethernet **100VG-AnyLAN** à 100 Mb/s répondent à la norme **IEEE 802.12** définie pour les réseaux en bus en étoile. Les réseaux 100VG-AnyLAN sont constitués de plusieurs concentrateurs (**hub**), ou de répéteurs (**repeater**).

Les concentrateurs sont reliés ensembles et forment une architecture «double», une architecture à deux niveaux, les concentrateurs forment entre eux un bus, comme une épine dorsale, et chaque concentrateur contient un anneau auquel sont reliées les stations. Ainsi, des données peuvent être transmises simultanément, mais à l'intérieur de sous-ensembles différents. D'autre part le câblage d'un réseau 100VB-AnyLAN est constitué de **quatre paires de fil** ce qui permet quatre transmissions simultanées.

Les concentrateurs gèrent l'accès au réseau. Le réseau est composé du même nombre de sous-ensembles qu'il y a de **concentrateurs**. Chaque concentrateur s'occupe de son sous-ensemble. Le réseau est en quelque sorte segmenté en plusieurs parties. Les messages ne sont pas diffusés sur tout le réseau, mais seulement sur la partie concernée. La gestion de l'accès au réseau est **centralisée** (il y a autant de pôles centralisateurs que de concentrateurs). Les concentrateurs agissent comme des routeurs.

Les concentrateurs interrogent tous les «nœuds terminaux» de la partie du réseau dont ils ont la charge, c'est à dire toutes les stations branchées sur leur anneau, et tous les concentrateurs auxquels ils sont reliés. L'interrogation des nœuds s'effectue à tour de rôle (méthode «**round-robin**»), et permet à chaque concentrateur de connaitre les **informations** d'adressage et de routage de chacun des nœuds. Les informations de routage sont, l'adresse des nœuds terminaux d'un même anneau, les plages d'adresses gérées par les concentrateurs proches, l'état de fonctionnement de chacun des nœuds.

Par exemple, un concentrateur reçoit une demande de transmission de la part d'un ordinateur. La

demande de transmission contient l'adresse du destinataire. Le concentrateur recherche si la route pour acheminer les données jusqu'au destinataire est libre, puis le cas échéant, il autorise la station à émettre. Le concentrateur reçoit alors les données et les transmet, soit directement à la station (si l'ordinateur récepteur est situé sur son propre anneau), soit au concentrateur à travers lequel devront passer les données (le deuxième concentrateur examine à son tour la partie du réseau qui lui incombe et procède de la même façon). Une **demande** de transmission peut provenir directement d'une station ou indirectement d'un concentrateur.

Un nœud terminal est un équipement qui est susceptible d'émettre ou de recevoir (un ordinateur, une station, un serveur, un dispositif de connectivité (pont, routeur, commutateur)).

La méthode d'accès de la priorité de la demande est une méthode d'accès à **contention**. La méthode d'accès de la priorité de la demande implique que deux ordinateurs peuvent se retrouver en situation de «rivaliser» pour obtenir le droit de «parler», mais cette méthode d'accès a l'avantage de permettre une configuration où certains types de données, définis à l'avance, ont la **priorité** sur d'autres. La priorité de certains types de données permet de résoudre les conflits. Quand deux demandes d'accès ont la même priorité, alors les deux demandes sont traités en alternance.

Les communications sont découpées en plusieurs parties, la communication entre un ordinateur **émetteur** et un dispositif de connectivité, la communication entre deux dispositifs de **connectivité**, la communication entre le dispositif de connectivité et l'ordinateur **récepteur**.

Le tableau des méthodes d'accès

Les différentes méthodes d'accès peuvent être rassemblées dans un tableau comparatif.

La comparaison des méthodes d'accès au support				
	CSMA/CD	**CSMA/CA**	**Passage du jeton**	**Priorité de la demande**
Diffusion	Tout le réseau	Tout le réseau	Tout le réseau	Une partie du réseau
Routage	NON	NON	NON	OUI (concentrateurs)
Rivalité	Contention	Contention	Pas de contention	Contention
Réseaux	Ethernet	Local Talk	Token Ring & FDDI	100VG-AnyLAN
Topologie	Bus	Bus	Anneau	Bus en anneau
Accès	Multiple direct	Multiple direct	Unique direct	Simultané indirecte
Collision	OUI	NON	NON	NON
Gestion	Décentralisée	Décentralisée	Centralisée (superviseur)	Centralisée multi pôles

CABLE

Les câbles réseaux

Un câble est un support de connexion. Les signaux électriques sont véhiculés sur câble. L'on dit que l'on «**tire un câble**» le long d'une plainte, d'une gouttière ou dans un sous plafond. Dans un espace exigu, il est parfois difficile de tirer un câble rigide, aussi est-il prévoyant de déterminer à l'avance, la longueur nécessaire, et si un câble flexible s'impose. Un réseau peut être équipé de plusieurs sortes de câble.

Il existe différents types de câbles, le câble **coaxial**, fin ou épais, la paire **torsadée**, non blindée (UTP) ou blindée (STP) et la **fibre** optique. Les réseaux certifiés de catégorie 5 n'utilisent que des câbles en paires torsadées de la catégorie 5.

La paire torsadée

Les fabricants de câbles ont mis au point une nomenclature de leurs différents produits.

Les types de câble en paire torsadées (UTP STP RJ45)	
Normes	**Caractéristiques**
RG 58 /U	Un seul toron de cuivre
RG 58 A/U	Torsade de plusieurs brins de cuivre
RG 58 C/U	Version militaire du RG 58 A/U
RG 59	Transmission à large bande
RG 6	Fréquence plus élevée que le RG 59
RG 62	Réseaux Arcnet

Le câblage IBM

En 1984, La société américaine IBM a développé son propre système de câblage. Par exemple, les connecteurs IBM hermaphrodites se connectent les uns sur les autres.

Le système AWG

Le système **AWG** (American Wire Gauge) est un système de mesure de l'épaisseur d'un câble. Plus le code AWG est petit et plus le câble est épais. Par exemple, le fil téléphonique et le STP ont une valeur de 22 AWG.

Le choix d'un câble

Le choix d'un câble dépend de plusieurs facteurs, dont le **budget** octroyé, le volume et la régularité du **trafic** sur le réseau, la grandeur du **site** et le nombre de machines, la **sensibilité** des informations et la sécurité des transmissions, les **interférences** du site. La vitesse, la pureté et la sécurité entrainent des couts supplémentaires. Les câblages blindés et la fibre optique remplissent les critères de hautes performances.

Quand les câbles sont longs, les signaux électriques se détériorent progressivement. Même si un système de détection des **erreurs** est mis en place, celui-ci demande une **retransmission** du message quand il détecte une erreur, ce qui ralenti la transmission du message. Les retransmissions augmentent le trafic sur le réseau. Quand le trafic sur le réseau est important, les messages sont transmis plus lentement, et la qualité s'en ressent très rapidement. Avec les progrès de la technologie, les câbles ont une «**longueur utile**» de plus en plus grandes et un «**débit théorique**» de plus en plus grands.

Tableau comparatif des spécificités des câbles					
	Le câble coaxial		**La paire torsadée**		**La fibre optique**
	Coaxial fin	**Coaxial épais**	**Non blindée (UTP)**	**Blindée (STP)**	
Norme	10 base 2	10 base 5	10 base T	10 base T	
Réseau	Ethernet fin	Ethernet épais			
Longueur	185 mètres	500 mètres	100 mètres	100 mètres	2 kilomètres
Connecteur	BNC	BNC, AUI	RJ45	RJ45	
Débit	10 Mb/s	10 Mb/s	10 à 100 Mb/s	10 à 100 Mb/s	0,1 à 1 Gb/s
Blindage	Oui	Oui	Non	Oui	Non
Installation	Simple	Simple	Simple	Simple	Compliquée
Flexible	Assez flexible	Peu flexible	Très flexible	Assez flexible	Pas flexible
Atténuation	Oui	Oui	Oui	Oui	Non
Interférences	Peu sensible	Peu sensible	Très sensible	Sensible	Pas sensible
Sécurité	Faible	Faible	Très faible	Assez Faible	Importante
Site	Moyen	Backbone	Petit	Token Ring	Excellence
Coût	Peu cher	Assez cher	Le moins cher	Pas cher	Le plus cher

Les répartiteurs de brassage

Les réseaux en étoile concentrent souvent les câbles dans un répartiteur de brassage ou un panneau de brassage constitué de connecteurs RJ45. Les répartiteurs de brassage ne sont pas indispensables, mais ils facilitent la gestion des **câbles** et accroissent la **sécurité** dans la mesure où ils sont enfermés dans une armoire fermée à clefs où se trouvent également les **commutateurs** et les **concentrateurs**. Le répartiteur de brassage est un bon endroit pour espionner les communications puisqu'il concentre tous les câbles et toutes les transmissions.

En fait, les câbles en paires torsadées courent à l'intérieur des murs, depuis une prise murale jusqu'à la salle ou se situe le répartiteur de brassage. Tous les câbles convergent vers le répartiteur de brassage. Les commutateurs et les concentrateurs sont reliés au répartiteur de brassage par des cordons de brassage, de la même façon, la carte réseau des ordinateurs est reliée au connecteur RJ45 de la prise murale par un **cordon** de brassage.

De nombreuses solutions existent pour centraliser et organiser les câbles et les connexions d'un réseau, avec, par exemple, des coupleurs de prises ou des prises murales. Il est possible de rassembler les câbles dans des armoires et des étagères de distribution, ou dans des tableaux de connexions extensibles jusqu'à 96 port RJ45 et jusqu'à 100 Mb/s. D'autre part, il est possible de faciliter la maintenance grâce à des codes couleurs.

Le câble coaxial

Il existe deux types de câbles coaxiaux, le câble coaxial fin et le câble coaxial épais. Les réseaux basés sur un câble coaxial sont souvent appelés Ethernet ou "**Ethernet fin**" pour un câble coaxial fin, et "**Ethernet épais**" pour un câble coaxial épais.

Le câble coaxial est constitué de plusieurs éléments, dont une **gaine** isolante extérieure généralement en PVC ou toute autre matière plastique, un **blindage** tressé en cuivre ou en aluminium qui sert de conducteur extérieur, une **enveloppe** isolante en PVC ou en TEFLON et un **brin** central conducteur en cuivre: l'âme du câble où circulent les signaux électriques.

Le blindage

Le blindage absorbe les **interférences** extérieures (les signaux parasitaires, le bruit,…) qui peuvent provenir d'autres câbles à proximité. Le blindage joue le rôle de masse et ne doit jamais être en contact avec le brin central (sinon, il y a un court circuit).

Les normes des gaines

Il existe deux normes pour les câbles coaxiaux, le chlorure de poly vinyle (PVC) et le plénum. Le

chlorure de poly vinyle (PVC) est une matière plastique dont est composé la gaine et l'enveloppe isolante. Le PVC est flexible, peu cher, mais il dégage des gaz **toxiques** lors d'un incendie. Le **plénum** est constitué d'une matière qui résiste au feu, il est plus cher que le PVC et moins flexible. Le plénum est le nom que l'on donne aux faux plafonds qui servent dans les bureaux pour l'aération et l'alimentation électrique. Le plénum est le seul type de câble à pouvoir être installé dans un faux plafond.

Les qualités du câble coaxial

Le «**coax**» est très employé et réuni beaucoup de qualité. Il est léger, **flexible**, facile à utilisé, peu cher, et il permet de véhiculer un volume important de données (comme les images, le son, etc…) sur de longues distances. Le coaxial est en outre plus **résistant** aux interférences et à l'atténuation du signal électrique que la paire torsadée. Le câble coaxial permet, avec un équipement peu sophistiqué et d'un faible cout, d'avoir des débits importants sur de longues distances. Mais le coaxial est relativement **fragile**, instable et vulnérable aux interférences et aux écoutes.

Les réseaux en coaxial sont constitués d'une succession de petits câbles reliant un ordinateur à un autre et dont le nombre est égal au nombre de nœuds moins un. Les réseaux en coaxial sont essentiellement des réseaux à la topologie de **bus**, avec un seul **segment** logique. Sauf pour les réseaux avec une épine dorsale en coaxial épais auquel sont branchés des transceivers à partir desquels partent des câbles en coaxial fin en cascade.

Le câble coaxial fin

Le câble coaxial fin est utilisé pour la télévision par exemple.

Le câble coaxial fin (Thinnet)
Un diamètre de 6 millimètres Un fil flexible Un débit de 10 Mb/s Une longueur maximum de 185 mètres Une impédance de 50 Ohm 10 base 2

Le câble coaxial épais

Le câble coaxial épais permet de transmettre des données sur de plus longues distances, parce que le fil de cuivre est plus épais, et qu'il est plus résistant aux interférences.

Le câble coaxial épais (Thicknet ou Ethernet Standard)
Un diamètre de 12 millimètres Un fil rigide Un débit de 10 Mb/s Une longueur maximum de 500 mètres Une impédance de 75 Ohm 10 bases 5

Les transceivers

Les transceivers peuvent se présenter sous différentes formes, les transceivers **internes** à la carte réseau, et les transceivers externes qui ont l'avantage de disposer de 4 prises AUI, ce qui permet de relier 4 stations avec un seul transceiver. Les transceivers externes d'un réseau câblé avec du coaxial **fin** sont connectés au câble par l'intermédiaire d'un connecteur **BNC**. Les transceivers externes d'un réseau câblé avec du coaxial **épais** sont connectés au câble par l'intermédiaire d'une «prise vampire» (**vampire tap**). Une fois le câble transpercé, il n'est plus possible d'enlever la prise vampire, et celle-ci ne sert qu'une seule fois.

Le câble coaxial épais est parfois utilisé comme le câble principal d'une épine dorsale (**backbone**) d'un réseau en bus auquel se rattachent des câbles secondaires en coaxial fin. Sur le câble principal des prises vampires percent la gaine (**vampire tap**), le blindage et l'enveloppe isolante jusqu'à établir le contact avec le brin central. Sur ces prises vampires sont branchés les transceivers externes (**transceiver**). A partir du connecteur AUI ou DIX de chaque transceiver (**connector**) part un câble de transceiver. Le câble de transceiver est aussi appelé câble de descente (**drop cable**). Le câble de descente conduit, soit à un répéteur (**repeater**) d'où part un câble coaxial fin (**cable**), dans le cas d'une dorsale avec des câbles secondaires, ou conduit à un connecteur AUI ou DIX d'une carte réseau (**interface**) d'un ordinateur (**computer**).

Les connecteurs des «câbles de transceivers»

Les connecteurs des «câbles de transceivers» (**drop cable**) peuvent être de trois différentes sortes. Ce sont, soit des connecteurs **AUI** (Attachement Unit Interface), soit des connecteurs **DIX** (Digital Intel Xerox), soit des connecteurs **15 broches DB-15**.

Les connecteurs BNC

Le câble coaxial fin et le câble coaxial épais utilisent les mêmes connecteurs **BNC** (British Naval Connector). Le connecteur BNC est serti ou soudé à une extrémité du câble. Le connecteur BNC en «**T**» permet de relier la carte réseau d'un ordinateur aux connecteurs BNC du câble. Le **prolongateur** BNC permet de relier deux segments de câble coaxial pour n'en former qu'un seul mais plus long. Le **bouchon** de terminaison BNC est situé en bout de câble, il permet d'absorber les signaux électriques

qui ont déjà parcouru toute la longueur du segment. Le bouchon de terminaison BNC peut être relié à la masse.

Les câbles à paires torsadées

Le câble à paire torsadée (Twisted Pair Cable) est composé de plusieurs éléments, dont les **brins** de cuivre entrelacés (torsadés) et **l'enveloppe** isolante. Le câble à paire torsadée a été largement diffusé parce qu'il est à l'origine utilisé pour les **lignes** téléphoniques, et qu'il était jusqu'en 1983 systématiquement pré installé dans tous les nouveaux bâtiments américains. Le câble à paire torsadée est le support (**média**) le plus utilisé à l'intérieur d'un bâtiment.

L'entrelacement des brins de cuivre permet de limiter les **interférences** extérieures (moteur, relais, transformateur), toutefois la protection d'un blindage est bien plus efficace pour diminuer les risques d'interférences. Il existe deux types de câbles à paires torsadées, le câble à paire torsadée **non blindée** ou **UTP** (Unshielded Twisted Pair) et le câble à paire torsadée **blindée** ou **STP** (Shielded Twisted Pair).

La paires torsadées non blindées

La paires torsadées non blindées (UTP)
Deux ou quatre brins de cuivre entrelacés (torsadés) et une enveloppe isolante A l'origine pour les lignes téléphoniques Spécifications de la norme «10 base T» des réseaux Ethernet Très utilisé pour les petits réseaux locaux intérieurs Une longueur maximale de 100 mètres

La norme EIA/TIA

La norme «Commercial Building Wiring Standard 568» de l'**EIA/TIA** (Electronic Industries Association / Telecommunication Industries Association) a été mise au point aux États Unis pour garantir la qualité et les conditions d'utilisation des câbles de l'industrie américaine. Cette norme classe les câbles **UTP** en 5 catégories, définie la **vitesse** maximale de transfert des données numériques qui est mesurée en Méga Bit par seconde (Mb/s), et détermine le nombre de **torsions** par «pied» (33 centimètres) que peut subir un câble UTP.

La catégorie N°1 correspond au câble téléphonique traditionnel et véhicule la voix analogique, mais pas les données numériques. La catégorie N°5 des câbles en paires torsadées est celle qui doit être recommandée dans la majorité des situations, d'une part parce qu'elle permet d'évoluer à terme vers un réseau à 100 Mb/s, et d'autre part parce qu'elle est de meilleure qualité et qu'elle est définie plus précisément. Par exemple, les spécifications des câbles de catégorie N°5 stipule que les **torsades** des fils doivent être maintenues de bout en bout du câble et que l'extrémité servant au **raccordement** (et qui est «dé-torsadé») ne doit pas dépasser un centimètre. De plus, ce n'est pas le câble qui coute cher,

mais plutôt son installation par des techniciens qualifiés.

Les réseaux «**certifiés de catégorie 5**» n'utilisent que des câbles de la catégorie 5. Toutefois, un réseau peut être équipé de plusieurs sortes de câble.

La norme EIA/TIA des câbles en paires torsadées UTP				
Catégorie	**Fonction**	**Vitesse**	**Nombres de brins**	**Torsions par «pied»**
1	La voix analogique (téléphone)		2	
2	Les données numériques	4 Mb/s	4	
3	Les données numériques	10 Mb/s	4	3
4	Les données numériques	16 Mb/s	4	
5	Les données numériques	100 Mb/s	4	

La norme de câblage pour les paires torsadées est EIA 568B est très stricte et définie l'ordre dans lequel les fils sont raccordés aux 8 broches du connecteur RJ 45. Les câbles à paires torsadées respectant la norme EIA/TIA 568 sont utilisés indifféremment pour les réseaux Ethernet ou Token Ring.

L'ordre de raccordement de la norme EIA 568 pour les câbles en paires torsadées	
N° de la broche du connecteur RJ 45	**Couleur du fil**
1	Blanc et orange
2	Orange
3	Blanc et vert
4	Bleue
5	Blanc et bleue
6	Vert
7	Blanc et marron
8	Marron

La paires torsadées blindées

Les composants d'un câble à paire torsadée blindée ou **STP** (Shielded Twisted Pair) sont les **quatre brins** de cuivre entrelacés deux par deux, deux **blindages** autour de chaque couple de brins et une **enveloppe** isolante. Le blindage permet de réduire les interférences ou les mélanges des signaux

électriques de plusieurs lignes. Le blindage (STP) permet des transferts de données à des débits plus important et sur des distances plus grandes que l'UTP.

Les connecteurs RJ45

Les connecteurs sont les même pour les câbles à paires torsadées non blindées (UTP) ou blindées (STP). Le connecteur RJ45 comporte **8 broches** ou 8 conducteurs. Le connecteur RJ45 ressemble au connecteur **RJ11** du téléphone, mais celui-ci est plus petit et ne comporte que 4 broches. Certaines topologies réseaux propriétaires (le pré10 base T) utilisent la paire torsadée avec des connecteurs RJ11, mais ces architectures sont relativement rare.

Les qualités de la paire torsadée

Les qualités de la paire torsadée
La paire torsadée répond aux spécifications de la norme «10 base T»
Très utilisé pour les réseaux locaux
Une longueur maximale de 100 mètres
Un débit de 10 à100 Mb/s
Un câblage peu couteux, c'est le moins cher
Une installation et des connexions simples
La plus grande flexibilité du câble
La plus grande vulnérabilité aux interférences
Un choix fiable qui ne garanti, ni l'intégrité, ni débits élevés

FIBER

La fibre optique

La fibre optique permet de transférer les données numériques sous la forme d'impulsions lumineuses modulées. La fibre optique (Fiber Optic Cable) est le meilleur support de connexion pour la **rapidité**, la qualité, la **fiabilité** et la **sécurité** des transmissions numériques. La fibre optique est plus cher que les autres types de câble (coaxial, UTP, STP), mais les spécifications techniques sont nettement plus **compétitives**. L'installation et la maintenance des réseaux en fibre optique requièrent les compétences de techniciens spécialement qualifiés et expérimentés. Le câblage en fibre optique est en **verre** et reste toujours très fragile. La connexion de deux fibres optiques requière un polissage délicat et un parallélisme parfait.

En contre partie de ces inconvénients, la fibre optique propose le mode de transmission le plus fiable et le plus sécurisé du marché et de l'état de l'art. La fibre optique permet la transmission de gros volumes de données à **haut débit** de 100 Mb/s à 622 Mb/s, et jusqu'à plus de 1 Gb/s (Giga Bit par seconde). Le signal lumineux reste **pur** le long de la fibre optique et ne s'affaiblit pas. Il n'y a pas d'atténuation du signal comme avec le cuivre. Il est impossible «d'écouter» ou d'intercepter les signaux lumineux qui circulent à l'intérieur d'une fibre optique, ce qui en fait un support naturellement **sécurisé**. Il n'y a pas d'interférences, ni de rayonnement.

Les caractéristiques de la fibre optique (Fiber Optical)	
Inconveniences	La fibre optique est plus cher que les autres types de câble (coaxial, UTP, STP) L'installation et la maintenance s'effectuent par des techniciens qualifiés Le verre de la fibre optique est fragile et la connexion délicate
Avantages	Le mode de transmission le plus fiable et le plus sécurisé du marché Les débits allant de 100 Mb/s à 622 Mb/s et jusqu'à plus de 1 Gb/s Le signal lumineux reste pur le long de la fibre optique et ne s'affaiblit pas Le support est naturellement sécurisé, sans interférences, ni rayonnements

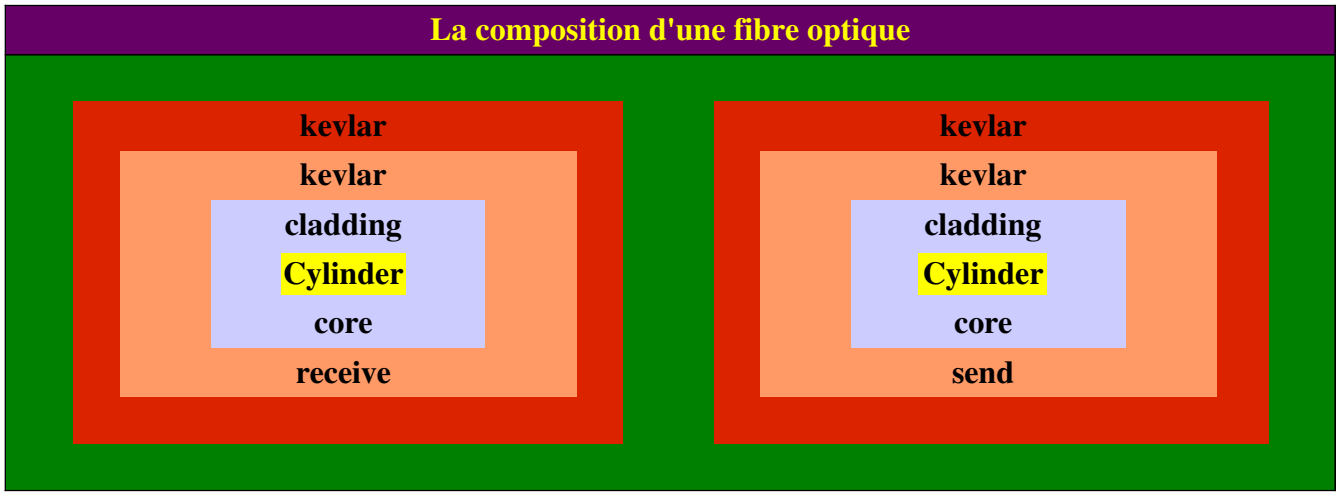
La composition de la fibre optique

Le signal lumineux ne circule que dans un seul sens, aussi la fibre optique contient toujours deux fibres, l'une pour recevoir les données et l'autre pour les envoyer.

Un câble en fibre optique (**fiber**) se compose de deux cylindres (**cylinders**) extrêmement fins, soit en verre ou en silice, soit en plastique. Les cylindres sont spécialisés dans un sens, l'un permet de recevoir les données (**receive**), tandis que l'autre permet de les envoyer (**send**). Ces deux cylindres forment le cœur (**core**) de la fibre optique. Chaque cylindre du cœur est recouvert d'une gaine optique en verre concentrique (**cladding**), une pour chaque cylindre. Les gaines sont constituées de deux couches de

fibre, une première couche appelée le petit isolant (**kevlar**), et une deuxième couche appelée le grand isolant (**kevlar**).

Le cœur peut être fabriqué en plastique, mais alors le signal lumineux ne porte pas aussi loin qu'avec du verre. Toutefois, les cœurs en plastique ont l'avantage d'être plus facile à installer. L'extrémité de la fibre optique doit être polie et doit s'insérer très précisément dans son réceptacle, que ce soit le connecteur de la carte réseau ou celui d'un concentrateur.



L'utilisation de la fibre optique

Originellement, et principalement du fait de son coût élevé, la fibre optique était réservée pour les **dorsales** à haut débit entre concentrateurs, et pour les applications spécialisées très consommatrices de bande passante. La fibre optique est compatible avec différentes **architectures** (Ethernet ou Token Ring), différentes topologies (en bus ou en anneau) et différentes technologies (100Base-FX, FDDI, ATM). La fibre optique reste cher à acheter, à installer et à maintenir, mais elle est devenue une **infrastructure** indispensable aux autoroutes de la **société** de l'information.

La fibre optique fut longtemps le privilège de centres de **ressources** hautement stratégiques comme les applications **militaires** ou **scientifiques**, et les communications **intercontinentales**. La fibre optique était impérativement recommandée, quand le budget n'était pas un enjeu, et que la **sécurité** était une contrainte forte, pour protéger les données sensibles. Aujourd'hui, la fibre optique se démocratise, parce que les besoins en vitesse de transmission se généralisent. Les applications hauts débits, comme les **bases de données**, ou la **virtualisation** requièrent de plus en plus, une bande passante large et fiable, et les applications **graphiques** en trois dimensions, ou **ludiques** comme les jeux en réseaux sur internet y trouvent un espace de création et de divertissement.

WIRELESS

La communication sans fil

La communication sans fil utilise un autre support que la communication que les câbles. En réalité, les réseaux sans fil se connectent la plupart du temps à des réseaux câblés et constituent ainsi des réseaux mixtes ou **hybrides**. La communication sans fil convient principalement dans deux cas de figures, les réseaux ou les stations **mobiles** et les connexions **temporaires.**

La communication sans fil a besoin d'émetteurs et de récepteurs. Quand ces dispositifs de transmission appartiennent à une entreprise privée, l'on parle «réseaux locaux étendus» parce qu'ils permettent de relier deux sites distants. Quand ils appartiennent à un service public de télécommunication (comme les sociétés AT&T, MCI ou SPRINT aux États Unis), l'on parle «d'informatique mobile».

Pour établir une connexion sans fil à un réseau câblé, il faut qu'un des ordinateurs du réseau câblé serve de **point d'accès** pour les stations sans fil. L'ordinateur qui sert de point d'accès et les ordinateurs mobiles doivent être équipés d'une **carte réseau sans fil** et d'un transceiver.

Les caractéristiques du sans fil

Les avantages d'un réseau sans fil sont nombreux mais les occasions d'en profiter sont rares. Les réseaux sans fil sont propice aux connexions **temporaires**, aux matériels de **secours**, aux matériels **mobiles**. Les réseaux sans fil permettent d'accroitre l'étendue d'un réseau et la **distance** entre des postes. Enfin, ils offrent la possibilité de s'abstraire de la **contrainte** filaire et de pouvoir déplacer une machine aussi facilement qu'un livre dans une bibliothèque. Toutefois, les réseaux sans fil utilisent les micro ondes pour les transmissions, et créent dès lors un environnement **magnétique** qui peut être néfaste pour la santé de certaines personnes ultra sensibles.

Les techniques de transmission sans fil

Les techniques de transmission sans fil sont **l'infrarouge**, le **laser**, la **radio** à bande étroite (fréquence unique), la radio à **spectre étalé**, les transmission par **satellites** et les transmissions par **micro ondes**.

Les techniques de transmission sans fil (Wireless)	
Signal	**Technologies**
L'infrarouge	Les réseaux infrarouges à visibilité directe (Bluetooth) Les réseaux infrarouges à diffusion Les réseaux infrarouges à réflecteurs Les réseaux infrarouges à liaison optique à large bande
Le laser	
La radio	La radio à ondes courtes et à fréquence unique La radio à spectre étalé sur plusieurs fréquences La radio longue portée
Les satellites	Les connexions privées sur une parabole La radio communication publique par paquets
Les micro ondes	Les réseaux des téléphones cellulaires Les réseaux wifi

L'infrarouge

L'infrarouge est un faisceau de lumière. Les transmissions en infrarouge doivent être très **intenses** afin qu'il n'y ait pas de confusion avec les nombreuses sources de lumière qui existent dans une pièce (fenêtres, néons, télévision, ampoules). Un réseau infrarouge est commode, rapide, mais sensible aux interférences lumineuses. Le faisceau ne doit jamais être coupé sinon la transmission est interrompue. La lumière infrarouge possède une large bande passante, les débits sont relativement importants, mais la portée est faible.

Il existe quatre types de réseaux infrarouges. Les réseaux à **visibilité directe** (les émetteurs et les récepteurs doivent être proches les uns des autres). Les réseaux **infrarouges à diffusion** (les signaux infrarouges se réfléchissent sur les murs et les plafonds sur une distance de 30 mètres, mais le débit est lent en raison des rebonds du signal). Les réseaux **réflecteurs** (les transceivers des ordinateurs transmettent les signaux vers le même point lequel fait office de routeur en les redirigeant vers l'ordinateur destinataire). Les réseaux à **liaison optique à large bande** (les performances sont comparables à un réseau câblé et permettent de transmettre des fichiers multimédias).

L'infrarouge
Le débit de 20 Mb/s La portée de 30 mètres Les interférences des autres sources lumineuses Les réseaux à visibilité directe Les réseaux infrarouges à diffusion Les réseaux réflecteurs Les réseaux à liaison optique à large bande

e

Le laser

Le laser est une technologie semblable à l'infrarouge en ce sens qu'elle nécessite une visibilité directe. Le laser est aussi appelé «**la lumière cohérente**».

La radio à ondes courtes

La radio à ondes courtes (bande étroite à fréquence unique) fonctionne comme une radio, il faut régler l'émetteur et le récepteur sur la même fréquence. La radio à ondes courtes ne nécessite pas de visibilité directe, la porté de diffusion est importante de l'ordre de 1650 mètres, mais la vitesse de transmission est faible, environ 4,8 Mb/s. La transmission par les ondes radio requière une licence ou une **autorisation** de la part des autorités locales, comme la **FCC** (Federal Communications Commission) aux États Unis ou le ministère de l'intérieur en France.

La radio à ondes courtes
La fréquence est unique La portée de 1650 mètres Le débit de 4,8 Mb/s

La radio à spectre étalé

La technique de transmission par radio à spectre étalé diffuse des signaux sur une certaine **plage** de fréquence. La bande passante est divisée en plusieurs **canaux** de communication. Les cartes réseaux pour «spectre étalé» sont réglées pour une durée prédéterminée sur un des canaux, puis passe sur un autre canal, c'est ce que l'on appèle des **sauts de fréquence**. Tous les ordinateurs sont synchronisés pour «sauter» en même temps. Pour intercepter de tels signaux, il faut connaitre **l'algorithme** de changement de canal.

La vitesse de transmission est faible (25 Kb/s à 4 Mb/s) mais la portée importante (250 mètres à l'intérieur et 3000 mètres à l'extérieur). La technique de transmission par radio à spectre étalé permet de créer un véritable réseau sans fil. L'équipement est relativement courant et requiert, des cartes réseaux radio (Xircom Credit Card Netware Adapter) sur chaque ordinateur et un point d'accès (Netware Access Point) sur l'un des ordinateurs du réseau câblé.

La radio point à point

La technique de transmission point à point n'est pas une véritable technique de transmission réseau. Cette technique permet de transmettre en **série** des signaux uniquement **entre deux ordinateurs**. Les ondes radio point à point traversent les murs, les planchers et les plafonds. La technique de transmission point à point utilise une liaison **radio** point à point. La transmission des signaux s'effectue

en série, pour un **débit** de 1,2 Kb/s à 38,4 Kb/s et une **portée** de 70 mètres à l'intérieur et de 500 mètres en visibilité directe à l'extérieur. La technique de transmission point à point requière des composants spécifiques comme un transceiver isolé et un transceiver hôte.

La radio longue portée

La transmission sur les réseaux locaux étendus consiste à transmettre des signaux sur de longues distances, mais requière un équipement particulier. Les ponts sans fil (**Wireless Bridge**) pour les réseaux locaux sans fil permettent de joindre deux réseaux distants de 5000 mètres. Deux bâtiments peuvent être ainsi connectés sans avoir recourt à des câbles.

Le pont sans fil à longue portée (Air Lan / Bridge Plus) qui utilise la technique de transmission **radio à spectre étalé** permet de créer une liaison principale sans fil ou une dorsale (**backbone**) et de relier ainsi plusieurs sites éloignés. Ce type d'équipement est relativement couteux mais permet d'économiser, entre autres, les frais de terrassement ou la location de lignes spécialisées. Les ponts sans fil à longue portée permettent de relier des sites distants de 40 Kilomètres sans avoir recourt aux lignes numériques T1 américaines (1,544 Mb/s) ni à des connexions micro-ondes.

L'informatique mobile

L'informatique mobile passe par l'intermédiaire d'entreprise de télécommunication ou de service public. L'informatique mobile est très utile pour les personnes qui sont souvent en déplacement et qui ont besoin d'échanger du courrier électronique ou de transmettre des fichiers. L'informatique mobile fonctionne avec différents types de matériels, comme les ordinateurs portables ou les **PDA** (Personnal Digital Assistant). Les vitesses de transmission sont lentes, et peuvent être encore plus ralenties si elles intègrent la correction d'erreurs (débits de 8 Kb/s à 19 Kb/s).

Les techniques de transmission mobile

Les différentes techniques de transmissions sans fil des signaux de l'informatique mobile sont, les réseaux des téléphones **cellulaires**, les réseaux **micro ondes** comme le Wifi, les connexions privées par **satellites** et les radios communications publiques par transmission de **paquets** par satellites.

Les réseaux cellulaires

Le réseau cellulaire doit se connecter à un réseau câblé par l'intermédiaire d'un équipement spécialisé. Par exemple, la société canadienne Nortel fabrique un équipement **UIE** (Unité d'Interface Ethernet), qui permet de relier un réseau cellulaire à un réseau câblé. Le système **CDPD** (Cellular Digital Packet Data) des téléphones cellulaires permet de transmettre des données informatiques sur les réseaux vocaux analogiques.

Les micro-ondes

La technique de transmission des micro-ondes, comme le **Wifi**, permet d'interconnecter des bâtiments répartis sur des zones relativement peu étendues, mais exige une visibilité directe. Les micro-ondes sont très utilisés aux États Unis, dans les campus universitaires, dans les zones industrielles, entre un satellite et une installation terrestre ou entre deux bâtiments (sur l'eau ou dans un désert). Une installation micro-ondes est composée de plusieurs éléments, dont deux transceivers radio, l'un pour recevoir, l'autre pour émettre et deux antennes directionnelles orientées vers les transceivers et installées le plus haut possible.

Les connexions privées par satellites

Les connexions privées par satellites passent par l'intermédiaire d'une **parabole** qui reçoit les ondes radios envoyées par un satellite qui tourne autour de la planète «terre». L'accès à Internet (**download**) peut être véhiculé par satellite pour les personnes isolées qui n'ont pas de relais téléphoniques proches.

La radio communication par paquets

La radio communication publique par paquets est une technique de transmission qui divise un message en paquets. Un paquet est toujours composé d'un **entête** (l'adresse source, l'adresse de destination et les informations nécessaires pour la correction d'erreurs) et d'un **corps** qui contient le message. Les paquets sont envoyés à un **satellite** qui les retransmet à l'ordinateur destinataire.

ROUTER

La connectivité

Les dispositifs de connectivité sont des matériels ou des logiciels qui permettent de prolonger, de segmenter ou de raccorder des réseaux entre eux. Par exemple, les dispositifs de connectivité permettent d'étendre un réseau local, de se connecter à internet ou de filtrer le trafic.

Les dispositifs de connexion

Les dispositifs de connexion permettent de relier et de séparer les segments de réseau. Les dispositifs de connexion sont branchés par un câble à un port. Les dispositifs peuvent être plus ou moins sophistiqués.

Les amplificateurs et les répéteurs (**repeater**) régénère le signal. Les ponts (**bridge**) prolongent les segments de câble. Les concentrateurs simples (**hub**) diffusent les paquets sur tout le segment du sous réseau. Les concentrateurs redirecteurs (**switch**) distribuent les paquets à la station du sous réseau. Les commutateurs (**router**) dispatchent et orientent les paquets. Les appareils de modulation démodulation (**modem**) transforment les signaux analogiques et numériques.

Les passerelles (**gateway**) traduisent les paquets pour les convertir dans un autre protocole. Les pare feux (**firewall**) filtrent et sécurisent les sous réseaux (**subnet**). Les cartes réseaux (**interface**) écoutent les trames du segment de réseau et recopient celles qui les concerne. Les appareils et logiciels de capture de trames (**sniffer**) écoutent et analysent les communications qui circulent sur le réseau, en fonction des ports (**service**), des protocoles (**protocol**) et des informations contenues dans les corps des trames (**data**).

Les dispositifs de connexion réseau
INTERFACE PORT CABLE ROUTER CABLE PORT INTERFACE
Les amplificateurs et les répéteurs (**repeater**) régénère le signal
Les ponts (**bridge**) prolongent les segments de câble
Les concentrateurs simples (**hub**) diffusent les paquets sur tout le segment du sous réseau
Les concentrateurs redirecteur (**switch**) distribuent les paquets à la station du sous réseau
Les commutateurs (**router**) dispatchent et orientent les paquets sur un autre sous réseau
Les appareils de modulation (**modem**) transforment les signaux analogiques et numériques
Les passerelles (**gateway**) traduisent les paquets pour les convertir dans un autre protocole
Les pare feux (**firewall**) filtrent et sécurisent les sous réseaux (**subnet**)
Les cartes réseaux (**interface**) écoutent les trames du segment de réseau et recopient les leurs
Les appareils et logiciels de capture de trames (**sniffer**) écoutent et analysent les communications

Les caractéristiques des dispositifs de connectivité

Les caractéristiques des dispositifs de connectivité					
Fonction	**Répéteur**	**Pont**	**Routeur**	**Pont-routeur**	**Passerelles**
Régénération	OUI	OUI	OUI	OUI	OUI
Prolongation	OUI	OUI	OUI	OUI	OUI
Les nœuds	OUI	OUI	OUI	OUI	OUI
Les supports	Multi câbles	Multi câbles	Multi câbles	Multi câbles	Multi câbles
Multi ports	Concentrateur	OUI	OUI	OUI	OUI
Broadcast	OUI	OUI	NON	OUI et NON	NON
Segmenter	NON	OUI	OUI	OUI	OUI
Filtrer	NON	OUI	OUI	OUI	OUI
Router	NON	NON	OUI	NON et OUI	OUI
Traduire	NON	NON	OUI	OUI	OUI
Couche OSI	1.Physique	2.LIAISON	3.RESEAU	2. et 3.	1. à 7.
Chemins	Un seul	Un seul	Plusieurs	Plusieurs	Plusieurs
Adresses		@ physique (mac)	@ réseau (ip)		
Méthode	La même	La même	CSMA/CD Jeton		Plusieurs
Protocoles	Un seul	Un seul	Routables		Plusieurs
Architecture	La même	La même	Ethernet Token Ring		Spécifiques
Topologie	Bus	Dorsale	Maillage	Maillage	Maillage
Utilisation	Rallonger	Regrouper	Optimiser	Simplifier	Traduire
Dispositif	Matériel	Logiciel aussi	Logiciel aussi	Logiciel aussi	Logiciel aussi

L'extension d'un réseau local

L'avantage principal, c'est la nécessité. Les **besoins** ont augmenté, le **trafic** explose et met en danger la pérennité du réseau existant. Un réseau local est une structure évolutive, qui change en fonction des besoins et du degré de son utilisation. Tous les réseaux locaux sont amenés à devenir insuffisant au fur

et à mesure que les utilisateurs l'apprivoise et que les activitées humaines s'y déploient.

Chaque architecture réseau a ses propres **limites** et ses propres **contraintes**. Parfois, il ne suffit pas de rajouter des postes sur le réseau existant, et le réseau doit évoluer. Les capacités de transmission du câble peuvent se révéler insuffisantes. Les délais d'attente peuvent devenir intolérables. Les activités réseaux peuvent se développer et de nouveaux besoins peuvent apparaitre. Par exemple, le partage de nouvelles ressources, l'augmentation du nombre de collaborateurs, l'extension de la messagerie Intranet, le succès des applications réseaux et des bases de données, les nouveaux modes d'organisation du travail en réseaux (**groupware**) sont des motivations pour étendre le réseau et accroitre ses capacités.

Les répéteurs

Les répéteurs régénèrent le signal électrique qui se dégrade à mesure qu'il parcourt le câble. Cet affaiblissement du signal s'appèle l'atténuation du signal. Selon le type de câble, la distance maximum de conservation du signal est différente. Le répéteur permet au signal de parcourir une distance plus grande (dans les deux sens). Ainsi, le répéteur permet d'étendre un réseau au-delà de ses limites, il permet d'accroitre la longueur du câble et le nombre de nœuds. Certains répéteurs peuvent passer les paquets d'un support à un autre, comme par exemple d'un brin de coaxial fin vers de la fibre optique. Le répéteur peut être multi câble.

Le répéteur agit au niveau de la couche PHYSIQUE du modèle OSI, c'est à dire qu'il réceptionne chaque paquet qui lui arrive, le régénère et le réexpédie de l'autre coté du câble. Les paquets ne sont pas filtrés, ni routés, ni traduit dans un autre protocole. De part et d'autre du répéteur, la méthode d'accès au réseau et le protocole doivent être strictement les même. Un répéteur ne segmente pas un réseau et ne diminue jamais le trafic. Au contraire, les problèmes de saturation du trafic, les tempêtes de diffusions générales (**Broadcast Storm**), se communiquent sur tout le réseau.

Un répéteur se situe toujours entre deux et seulement deux segments. Toutefois, quand le répéteur dispose de plusieurs ports, c'est un répéteur **multi ports** et il fait office de concentrateur.

Les répéteurs sont les dispositifs les moins chers. Il ne faut pas utiliser de répéteur dans certaines conditions. Par exemple, quand le trafic réseau est très important, l'engorgement demeurera même si un répéteur est installé. Quand les segments du réseau utilisent des méthodes d'accès différentes ou des protocoles réseaux sont différents, alors le répéteurs ne sont pas appropriés. Enfin, quand les paquets doivent être filtrés et/ou routés, alors les répéteurs ne sont pas compétents.

Les ponts

Les ponts (**bridges**) permettent de prolonger et de segmenter un réseau, d'augmenter le nombre de postes (**lnodes**), de réduire les goulets d'étranglement, de router les paquets, de relier des supports différents. Les ponts permettent de relier ou de segmenter deux réseaux qui utilisent le même protocole. La segmentation permet d'isoler le trafic sur chaque segment, et parfois cela facilite la localisation d'un

problème. Les ponts sont souvent utilisés pour des protocoles réseaux qui ne peuvent pas être routés.

Les ponts agissent au niveau de la couche LIAISON du modèle OSI. Les ponts n'accèdent pas aux couches supérieures, ils ne font pas la différence entre des protocoles différents, et donc, tous les protocoles traversent les ponts. La couche LIAISON peut être divisée en deux sous-couches, la sous-couche LLC et la sous-couche MAC. Les ponts travaillent au niveau de la sous-couche MAC qui reconnait les adresses MAC des cartes réseaux. L'adresse Mac de chaque carte réseau, de chaque nœud du réseau, est une adresse unique dans le monde entier. Les ponts sont parfois appelés des «ponts de couche MAC».

Les ponts possèdent une mémoire dans la quelle ils stockent les informations de la table de routage. Au démarrage, la table de routage d'un pont est vide. Les ponts construisent une table de routage en examinant les adresses sources des paquets qui lui parviennent. Ainsi, au fur et à mesure du trafic, les ponts accumulent les informations sur les stations émettrices (l'adresse MAC et le segment).

Quand un paquet arrive sur un pont, celui-ci vérifie si l'adresse source de l'expéditeur figure dans sa table de routage, si ce n'est pas le cas, le pont l'y inscrit. Ensuite, le pont vérifie si l'adresse cible du destinataire figure dans sa **table de routage**, si c'est le cas, alors il achemine le paquet vers le segment auquel appartient le destinataire (sauf, si c'est le même segment que l'expéditeur), si ce n'est pas le cas, le pont transfert le paquet vers tous les autres segments, vers tous ses ports (le pont devra attendre que le destinataire émette à son tour…).

Les paquets sont **filtrés** (si le destinataire appartient au même segment, le paquet n'est pas retransmis une seconde fois, le paquet est rejeté, le trafic est réduit et les autres segments sont isolés). Les paquets sont **routés** (seul le segment du destinataire reçoit le paquet).

Les «**ponts distants**» sont utilisés pour réunir des réseaux très éloignés les uns des autres. Il faut deux ponts distants de part et d'autre, deux modems synchrones et une ligne téléphonique louée par exemple. Il peut arriver que plusieurs réseaux locaux soient réunis par des ponts distants, et qu'il existe plusieurs chemins pour acheminer un paquet. Le Network Management Committee de la norme **802.1** de l'IEEE a mis au point un **algorithme** afin de déterminer le meilleur chemin. L'algorithme **STA** (Spanning Tree Algorithm) permet de déterminer le chemin le plus efficace, de désactiver les autres chemins possibles ou de les réactiver si le chemin principal devient inaccessible.

Les ponts permettent de regrouper plusieurs petits réseaux pour n'en former qu'un seul. Les ponts sont relativement faciles à installer et à configurer, de plus ils sont peu chers et transparents pour les utilisateurs. Mais, les ponts ne conviennent pas dans certaines conditions. Par exemple, les liaisons distantes avec un débit supérieur à 56 Kb/s, et le routage par commutation de paquets qui utilise plusieurs chemins simultanément ne conviennent pas pour les ponts.

Les ponts peuvent se présenter sous plusieurs formes différentes. Les ponts peuvent être des dispositifs de connectivité externe, comme un matériel qui a l'aspect d'un petit boîtier, ou des dispositifs de

connectivité interne, comme un logiciel installé sur un serveur.

Les routeurs

Les routeurs (**routers**) sont aussi appelées des passerelles (**gateway**). Les routeurs permettent de prolonger et de segmenter un réseau, d'augmenter le nombre de postes (**nodes**), de réduire les goulets d'étranglement, de router les paquets, de relier des supports différents, de relier des segments qui utilisent des méthodes d'accès au réseau différentes, ou des protocoles routables différents. Les routeurs sont souvent utilisés pour interconnecter plusieurs réseaux entre eux. Les interconnections des réseaux proposent plusieurs **chemins** possibles pour que deux stations communiquent. Les routeurs permettent de «router» les paquets d'un réseau vers un autre, tout en considérant le chemin le plus court ou le plus rapide.

Les routeurs travaillent au niveau de la couche RESEAU du modèle OSI. Lorsqu'un paquet est transmis à un autre routeur, les **adresses** réseaux de la source et de la cible sont recréées, et éventuellement traduites, c'est ce qui permet à un routeur de transmettre les paquets d'un segment Ethernet vers un segment Token Ring par exemple.

La table de routage

La **table de routage** d'un routeur conserve les informations de routage qui le concerne directement, c'est à dire les informations des matériels adjacents (ordinateurs ou routeurs) qui sont installés sur les segments auxquels il est lui-même raccordé. Un routeur ne communique pas avec les ordinateurs qui sont situés au-delà d'un autre routeur. Les routeurs partagent leurs **informations** de routage avec les autres routeurs du réseau. Les informations de routage permettent aux routeurs de déterminer la route optimale.

Les informations de routage des routeurs
Les adresses réseaux des ordinateurs placés sur les segments adjacents
Les masques de sous-réseaux des autres segments
Les plages d'adresse qui sont gérées par les routeurs adjacents
Les chemins possibles pour acheminer un paquet vers un des routeurs du réseau
Le nombre de sauts de routeurs pour arriver à tel ou tel segment

Le routage des paquets

Les routeurs ne laissent pas passer les messages de diffusion générale (**broadcast**), ils ne laissent passer que les **protocoles routables**. Les routeurs ne laissent passer que les paquets dont les adresses sont connues. Les routeurs peuvent servir de **barrière** de sécurité entre les segments d'un réseau. Les routeurs permettent de prévenir les saturations de diffusion.

Les routeurs peuvent commuter et acheminer les paquets vers plusieurs réseaux, ils optimisent le trafic

en dirigeant les paquets vers le meilleur chemin, c'est pourquoi ils sont utilisés dans les réseaux complexes. Le meilleur chemin est calculé en fonction du nombre de routeurs que le paquet devra traverser, c'est le nombre de saut, de bonds (**hops**). Quand il existe plusieurs chemins possibles (**routes**), et si l'un des routeurs tombe en panne, alors un autre chemin peut être utilisé pour acheminer les paquets.

Des **algorithmes** de routage permettent de calculer le meilleur chemin, au moindre cout. Ces algorithmes sont incorporés dans des «protocoles de routage», c'est à dire des protocoles qui permettent de router les paquets d'un endroit vers un autre en choisissant le meilleur chemin possible.

Les protocoles routables

Les protocoles routables	
Les protocoles routables	DECnet IP IPX OSI XNS DDP (Apple Talk)
Les protocoles non routables	LAT (Local Area Transport) de DEC NetBEUI de la société Microsoft

Les protocoles de routage

Les protocoles de routage sont généralement appelés des **protocoles de passerelles** et font partie de la pile de protocole de TCP/IP. Les protocoles de **routage interne**, comme RIP et OSPF, sont utilisé pour des réseaux privés, qui des lors constituent un «système autonome» ou **AS** (Autonome System), c'est à dire un ensemble de routeurs interdépendant qui utilisent le même protocole de routage (l'un des deux). Les protocoles de **routage externe**, comme EGP et BGP, sont utilisés pour router les paquets vers internet, et vers d'autres systèmes autonomes, ou vers un «extranet».

Les protocoles de routage interne

Les protocoles de routage interne s'emploient à l'intérieur d'un réseau local (**lan**). Les protocoles de routage interne sont **RIP** (Routing Information Protocol), **OSPF** (Open Shortest Path First) et **NLSP** (NetWare Link Services Protocol).

Le protocole RIP s'appuie sur un algorithme à vecteur de distance (Distance Vector). RIP est un protocole de routage interne **statique**, c'est-à-dire que la configuration des paramètres est manuelle, et ceux-ci sont figés. RIP est le plus ancien des protocoles de routage interne, et son algorithme à vecteur de distance est moins efficace que l'algorithme basé sur l'état des liaisons. RIP autorise un maximum

de 16 **sauts** entre la source et la cible avant que le paquet ne soit rejeté. Les paquets rejetés sont considérés comme non délivrables, et ils doivent être réexpédiés. Cette restriction concernant le nombre de saut fait que RIP n'est pas le bon choix pour un grand réseau comme Internet parce que le nombre de saut y est souvent supérieur à 20.

Le protocole de routage interne **OSPF** (Open Shortest Path First) est un protocole **dynamique** dont la stratégie de routage évolue en fonction de l'état du réseau à un moment donné. OSPF n'est pas restreint par un nombre de saut limité, et convient bien pour les grands réseaux. OSPF est basé sur l'algorithme **Dijkstra** qui examine l'état des liaisons (Links State), et qui prend en considération, le nombre de bonds, la vitesse de la ligne, le trafic.

Les protocoles de routage externe

Les protocoles de routage externe s'emploie pour le routage à l'extérieur d'un réseau local et sont appropriés pour les réseaux étendus (**wan**). Les protocoles de routage externe sont **EGP** (External Gateway Protocol) et **BGP** (Border Gateway Protocol) qui est une nouvelle version d'EGP.

BGP se repose sur TCP pour s'assurer que les paquets ont bien été livrés. BGP dispose d'une table de routage optimisée, ce qui signifie qu'il ne gaspillera pas de bande passante. BGP détecte les routes défaillantes à un moment donné. BGP peut être utilisé sur un réseau privé, un «système autonome», mais, il est indispensable qu'il y est un des routeurs qui fonctionne avec RIP ou OSPF afin de fournir une porte de sortie aux paquets routés par BGP. Sinon, les routeurs BGP se renverraient les paquets indéfiniment sans trouver le réseau interne vers lequel ils sont sensés router les paquets.

Les protocoles de routage	
Interne	**RIP** (Routing Information Protocol) est statique sur l'algorithme Distance Vector à 16 sauts **OSPF** (Open Shortest Path First) est dynamique sur l'algorithme Dijkstra et l'état des liaisons **NLSP** (NetWare Link Services Protocol)
Externe	**EGP** (External Gateway Protocol) repose sur TCP **BGP** (Border Gateway Protocol) table de routage optimisée et un routeur RIP ou OSPF

Les types de routeurs

Il existe deux types de routeurs, les routeurs statiques et les routeurs dynamiques. Les routeurs **statiques** sont des routeurs pour lesquels les tables de routage doivent être créées manuellement par l'administrateur. Les routes sont définies une bonne fois pour toute, et les paquets empruntent toujours le même chemin, celui désigné par l'administrateur. Les routeurs **dynamiques** sont des routeurs qui détectent automatiquement toutes les routes d'un réseau et qui adapte le routage.

Les routeurs effectuent des tâches complexes sur les paquets qui les traversent, aussi sont-ils plus lent que les ponts. Les routeurs disposent de **mémoire** pour stocker les informations de la table de routage.

En général, les routeurs sont d'autan plus rapide que leur **table de routage** est petite. L'accroissement de la taille des tables de routage des routeurs d'internet explique en partie le ralentissement des communications.

Les types de routeurs	
Statique	Les tables de routage et les routes sont fixées par manuellement par l'administrateur
Dynamique	Les tables de routage évoluent automatiquement et les routes s'adaptent

Les fonctionnalités des routeurs

Les fonctionnalités des routeurs se diversifient, de plus en plus les routeurs **sophistiqués** proposent des fonctionnalités de filtrage, d'authentification et de cryptage. Bien que ces nouveaux types de routeurs ne remplacent pas un véritable pare feu (**firewall**), ils accroissent d'autan la sécurisation d'un réseau.

La fonctionnalité **d'authentification** de l'émetteur permet de s'assurer de la provenance des données en vérifiant l'adresse source d'un paquet. Le **cryptage** des données permet de modifier l'apparence des données afin de réduire leur lisibilité. Une clef de cryptage est nécessaire pour déchiffrer un message crypté. Le niveau de sécurité d'une **clef** de cryptage dépend de sa longueur et donc du nombre de bit utiliser pour la décrire. Une clef de 40 bits est relativement facilement cassée avec la puissance des systèmes informatiques d'aujourd'hui, et représente un niveau de cryptage «faible». Par contre une clef de 128 bits est plus difficile à casser, et représente un «fort» niveau de cryptage.

Les échanges de données avec **l'algorithme** de cryptage **Diffie-Hellman** utilisent deux clefs de cryptage qui permettent de créer une troisième clef de cryptage appelé «clef de session». La **cryptographie** à clef publique est basé sur la génération de grands nombres premiers. La clef publique et la clef privée sont construites en même temps à l'aide de la factorisation de deux nombres premiers. La clef publique est diffusée à tous, tandis que la clef privée est réservée à une seule personne qui s'en servira pour décoder les messages qui ont été cryptés avec sa clef publique.

Avant d'installer un routeur, il faut s'assurer que le réseau fonctionne avec un ou des protocoles routables. Avant d'acheter un routeur, il convient de déterminer si celui-ci doit posséder les fonctionnalités de **CIDR** (routage des adresses IP sans classe).

Les ponts-routeurs

Les ponts-routeurs ou B Router (**Bridge Router**) sont une combinaison des fonctionnalités d'un pont et d'un routeur. Les ponts-routeurs routent les protocoles routables et servent uniquement de pont pour les protocoles non routables. Les ponts-routeurs facilitent la gestion du trafic d'un réseau quand celui-ci est composé à la fois de ponts et de routeurs.

Les passerelles

Les passerelles (**gateway**) permettent la communication entre réseaux d'architecture différente. Les passerelles interconnectent les réseaux **hétérogènes** multi fournisseurs. Par exemple, les passerelles peuvent être utilisées pour relier un réseau d'ordinateurs personnels à un réseau de mini ordinateurs ou à un réseau de grands systèmes. Ainsi, les utilisateurs ont la possibilité d'accéder aux ressources d'un grand système par exemple.

Une passerelle est toujours spécifique à deux architectures. Une passerelle peut agir sur toutes les couches du modèle OSI et fait office de **traduction** de protocoles. La passerelle re-formate les paquets, les données entrantes sont «dépouillées» de leur pile de protocole (dés-encapsulées) et «rhabillées» (ré-encapsulées) avec l'autre pile de protocole. La passerelle remplace une pile de protocole par une autre. Les passerelles sont des traducteurs de protocoles. Les passerelles sont souvent utilisées pour les réseaux qui ne disposent pas de TCP/IP (par exemple, les réseaux NetWare qui fonctionnent sous SPX/IPX et qui veulent avoir un accès à Internet).

En général, la passerelle est un logiciel installé sur un serveur **dédié**, parce que le travail de traduction des protocoles exige beaucoup de bande passante, et beaucoup de traitement. Les passerelles sont lentes et couteuses.

INTERFACE

L'interface

L'interface est une **expression** largement utilisée dans le domaine de l'informatique pour indiquer une **frontière** et un **passage** entre plusieurs technologies. Par exemple, l'on parle d'interface graphique pour distinguer le traitement de l'affichage, d'interface utilisateur pour séparer la zone système de la zone d'utilisation. L'expression d'interface réseau est employée pour parler de passerelle (**gateway**) entre deux réseaux (**network**) utilisant des protocoles différents (**protocol**), ou pour parler des cartes réseaux (**interface**) qui permettent la connexion entre un dispositif (**router**) ou un ordinateur (**computer**) et le support de communication (**cable**). Tous les dispositifs et toutes les machines qui communiquent, échangent, partagent, filtrent ou transmettent sur un réseau doivent être équipés d'une ou de plusieurs cartes réseaux.

La carte réseau

La carte réseau (Network Adapter Card) ou ou **NIC** (Network Interface Card) joue le rôle d'une **interface** physique entre l'ordinateur et le câble réseau. La carte réseau permet de préparer, d'envoyer et de contrôler les données circulant sur le réseau.

En général, un ordinateur échange des données avec un autre ordinateur, les signaux transmis par la carte réseau de l'un s'adresse précisément à la carte réseau de l'autre. Les données sont transmises à une et une seule **adresse** du réseau. Parfois toutefois, certains messages doivent être envoyés à toutes les stations du réseau, et plutôt que d'envoyer le même message à chacune des stations du réseau, il est bien plus efficace d'envoyer à tous un seul message, on parle alors de **broadcasting**.

Le contrôle de flux

La carte réseau convertit le **flux** de données parallèles de l'ordinateur (de 8, 16, 32 ou 64 bits selon le bus de la carte mère) en un flux série pour les données sortantes qui sont mises sur le câble. La **conversion** inverse est également effectuée par la carte réseau pour les données entrantes. Il existe des cartes réseaux asynchrones et synchrones. La carte réseau effectue le contrôle de flux qui permet de détecter les erreurs éventuelles de transmission. C'est la carte réseau qui gère **l'adressage** des communications vers le bon destinataire. Sur un réseau, tous les postes et tous les périphériques réseaux doivent être munis d'une carte réseau.

Le firmware

Les cartes réseaux contiennent un micro programme propre au constructeur (**firmware**) qui est stocké dans une mémoire morte sur la carte réseau. C'est ce micro programme qui met en œuvre les sous

couches **LLC** (Logical Link Control) et **MAC** (Media Access Control) de la couche LIAISON du modèle **OSI** (Open System Interconnection). Le pilote de la carte réseau (**driver**) doit être compatible avec cette puce électronique (**chipset**) et le système d'exploitation (**system**).

Les fonctions réseaux

Les fonctions d'une carte réseau sont simples, une carte réseau doit émettre et recevoir des données, mais les opérations intermédiaires sont nombreuses et complexes.

Les fonctions de communication de la carte réseau	
Émettre	**Recevoir** les données émises par l'ordinateur sur lequel elle est installée
	Stocker les données dans une **mémoire tampon**
	Restructurer les données d'un **flux parallèle en un flux série**
	Préparer les données à transmettre sur le réseau en fonction du **protocole**
	Engager un **dialogue** afin d'établir des paramètres communs pour la transmission
	Transférer les données
	Contrôler le flux de données transmis sur le réseau
	Terminer la transmission
Recevoir	**Écouter le réseau** et filtrer les trames en fonction des entêtes et de l'adressage
	Engager un **dialogue** pour s'entendre sur les paramètres communs de la transmission
	Réceptionner les données émises par un autre ordinateur du réseau
	Contrôler le flux de données reçues depuis le réseau
	Stocker ces données dans une mémoire **tampon**
	Préparer les données, dés-encapsuler les **protocoles**
	Restructurer les données d'un **flux série en un flux parallèle**
	Transmettre à l'ordinateur les données reçues

La transformation des données

A l'intérieur d'un ordinateur les données circulent sur les bus de la carte mère. Les données se déplacent côte à côte et en même temps sur les bus **parallèles**. Les bus peuvent avoir des largeurs différentes (8 bits pour les anciens ordinateurs, 16 bits à partir du PC/AT d'IBM, 32 bits pour les PC d'aujourd'hui, bientôt 64 bits). Sur le câble du réseau, les données se déplacent en **série**, les bits circulent les uns derrières les autres. C'est la carte réseau qui se charge de transformer les données en sortant et en entrant. Cette conversion consiste en une restructuration du flux parallèle en un flux série, et vice versa. La conversion du signal analogique en signal numérique, et vice versa, est effectuée par un modem.

L'unicité de l'adresse MAC

L'adresse MAC d'une carte réseau est unique au monde. L'organisme **IEEE** (Institute of Electrical and Electronics Engineers) est un organisme américain qui attribue des plages d'adresses à tous les **fabricants** de cartes réseaux dans le monde. Les fabricants de cartes réseaux inscrivent sur la puce de chacun de leur produit une adresse unique. Ce numéro unique représente l'adresse physique ou l'adresse MAC de la carte réseau. L'adresse MAC est une série de chiffre et de lettres sur 48 bits. L'adresse MAC est composé de 6 octets convertis en hexadécimal de 12 quartets.

Les trois premiers octets sont réservés pour identifier le constructeur de la carte réseau, tandis que les trois derniers octets sont gérés par le constructeur. Les trois premiers octets des adresses MAC sont décernés par l'IEEE et sont réservés pour identifier les constructeurs. Par exemple, la société 3 COM (08 00 03), la société HP (08 00 09), la société IBM (08 00 5A), la société DEC (AA 00 00). Le système **LAA** (Localy Administrated Address) permet de choisir l'adresse MAC de la carte réseau, mais, c'est un système qui n'est valable que pour un réseau privé et fermé.

L'adresse MAC d'une carte réseau					
Constructor			**Interface**		
00 à FF	00 à FF	00 à FF	00 à FF	00 à FF	00 à FF

L'achat d'une carte réseau

Avant d'acquérir des cartes réseaux, il faut s'assurer qu'elles soient compatibles non seulement avec l'architecture des ordinateurs (**driver**) sur lesquels elles seront installées, mais aussi avec l'architecture du réseau (**network**) et la nature du câblage (**connector**). Par exemple, une carte réseau pour un ordinateur Macintosh™ ne fonctionne pas sur un ordinateur PC. Un réseau en anneau requière des cartes réseaux spéciales. Le protocole Apple Talk est un protocole propriétaire (**protocol**). La connectique des cartes réseaux doivent être compatibles avec les connecteurs du câblage et les dispositifs de routage (**router**).

Avant d'installer un réseau, il faut déterminer les besoins, le type de câble, le type de connecteur, et enfin le type de cartes réseaux. Avant d'acheter une carte réseau, il faut s'assurer qu'il existe bien un pilote compatible avec le système d'exploitation réseau. La liste du matériel compatible ou **HCL** (Hardware Compatibility List) peut être consultée sur le site du constructeur de cartes réseaux.

Les types de cartes réseaux

En premier lieu, la carte réseau doit être compatible avec l'architecture du réseau et plus précisément avec le type de support de communication (**connector**). En second lieu, la carte réseau doit être compatible avec l'architecture de l'ordinateur, l'architecture interne de la carte mère et plus précisément l'architecture du bus de communication (**bus**). La carte réseau qui s'insère dans un des connecteurs d'extension (**slot**) de la carte mère doit être compatible avec l'architecture de bus local,

dont les fréquences compatibles et la largeur. Les cartes réseaux **PCMCIA** ou PC CARD s'insèrent dans un compartiment spécial dont l'ordinateur doit être pourvu. Les branchements PCMCIA des ordinateurs portables permettent d'insérer des cartes réseaux qui ont également la fonction de modem, de fax ou de répondeur.

Les cartes réseaux peuvent être équipées de leur propre mémoire de travail qui est une mémoire vive qui sert de mémoire tampon pour stocker les flux de données, et aussi d'un processeurs indépendant pour accélérer leur travail. Certaines cartes réseaux ont une mémoire **PROM** (Programmable Read Only memory) qui permet à l'ordinateur de démarrer par le réseau. Une telle station, comme un terminal passif, est dispensée de l'équipement «normal» de tout ordinateur (un processeur, un disque dur, un lecteur de disquette ou de CDROM).

Les types de cartes réseaux (port)	
Connectors Interface	**BNC** pour le câble coaxial fin des réseaux Ethernet **AUI** (DB-15) à 15 broches pour le câble coaxial épais des réseaux Ethernet **RJ45** pour la paire torsadée **Fiber** pour fibre optique **Ring** pour les réseaux en anneau (Token Ring) **Antenne** pour les réseaux Wifi sans fils (wireless)
Slots Mother Board	**ISA** (Industry Standard Architecture) 8 et 16 bits **EISA** (Extended Industry Standard Architecture) 32 bits **MCA** (Micro Chanel Architecture) 16 bits ou 32 bits **PCI** (Peripheral Component Interconnect) 32 bits **PCX** (Peripheral Component Extended)

L'architecture ISA

L'architecture ISA (Industry Standard Architecture) équipe historiquement les ordinateurs personnels compatibles IBM PC de type XT et AT. L'architecture ISA propose un bus de **8 bits** puis de **16 bits** en 1984 quand IBM sort le PC/AT. Les cartes réseaux 8 bits peuvent s'insérer dans un connecteur 1- bits, mais l'inverse n'est pas possible. L'architecture ISA a été la norme des ordinateurs personnels jusqu'à ce que la société Compaq et d'autres constructeurs développent l'architecture EISA.

L'architecture EISA

L'architecture **EISA** (Extended Industry Standard Architecture) est une norme de bus qui a été introduite sur le marché en 1988 par un consortium de neuf sociétés (Ast Research, Compaq, Epson, Hewlett-Packard, Nec, Olivetti, Tandy, Wyse Technology et Zenith). Les spécificités de l'architecture EISA sont le bus **32 bits** compatible avec l'architecture ISA (les cartes ISA peuvent s'insérer dans les connecteurs EISA). L'architecture EISA propose les mêmes fonctionnalités que l'architecture MCA.

L’architecture MCA

L’architecture **MCA** (Micro Chanel Architecture) est une norme introduite par IBM en 1988. Les spécificités de l’architecture MCA sont le bus de **16 bits** ou de **32 bits**, mais incompatibles avec l’architecture ISA. L'architecture MCA est sortie en même temps que la nouvelle gamme des ordinateurs PS/2 d’IBM. Plusieurs contrôleurs de bus peuvent le gérer indépendamment.

L’architecture PCI

L’architecture **PCI** (Peripheral Component Interconnect) est une norme et pratiquement un standard. Les spécificités de l’architecture PCI sont la compatibilité avec les ordinateurs Intel Pentium et les processeurs Motorola pour Power Macintosh™ de la société Apple. L'architecture PCI propose un bus de **32 bits**, Plug & Play, c'est-à-dire que la carte PCI est automatiquement reconnue dès le premier branchement. La technologie Plug & Play est une philosophie de conception et un ensemble de spécifications concernant l’architecture des ordinateurs personnels. L'architecture **PCX** (Peripheral Component Extended) vient remplacer progressivement les bus et les cartes PCI, et propose des débits plus rapides.

Les ports réseaux

Les cartes réseaux possèdent au moins un port auquel est branché un connecteur du câble réseau. Certaines cartes réseaux, appelées des cartes combo possèdent plusieurs ports afin d’être compatibles avec plusieurs types de câbles et de connecteurs. La connectique ou les ports (connector) des cartes réseaux peuvent être, de type **BNC** pour les réseaux Ethernet en coaxial fin, de type **AUI** (DB-15) à 15 broches pour les réseaux Ethernet en coaxial épais, ou de type **RJ45** pour les réseaux Ethernet en paire torsadées.

Il ne faut pas confondre les ports matériels d'une carte réseau, ou d'un ordinateur qui sont des portes d'entrées physiques (**connector**), des ports utilisés par les services réseaux (**daemon**) et les serveurs (**server**) qui sont des portes d'entrées logiques et conventionnelles (**“/etc/services”**).

La carte réseau sans fil

La carte réseau sans fil est généralement fournie avec plusieurs éléments (une antenne omnidirectionnelle d’intérieur, un câble d’antenne, un logiciel réseau, un logiciel de diagnostic, un logiciel d’installation).

L’accès direct à la mémoire

Certaines cartes réseaux ont un accès direct à la mémoire de l’ordinateur, on dit qu’elles sont compatibles **DMA** (Direct Access Memory). Le système d’exploitation réseau peut affecter à ce type de carte réseau une partie de la mémoire vive de l’ordinateur (**memory**). Les cartes réseaux compatibles

DMA utilisent cette mémoire RAM comme mémoire tampon.

Les données circulent plus vite à l'intérieur de l'ordinateur qu'à travers une carte réseau. La carte réseau a besoin de stocker le flux de données parallèles provenant de l'ordinateur. Les données parallèles de l'ordinateur sont stockées dans la mémoire tampon avant d'être restructurées en donnée série pour le réseau.

L'adresse du destinataire

Le signal électrique contient l'adresse du destinataire (**target**) qui est l'adresse d'une autre machine (**host**) sur le réseau (**network**). L'adresse des machines sur le réseau sont uniques (**uniq**) afin d'identifier précisément chaque ordinateur. Si plusieurs machines ont la même adresse, c'est alors une erreur qui provoquera des dysfonctionnements. L'adresse d'une machine doit être connue des ordinateurs qui souhaitent entrer en communication avec elles.

Des serveurs de noms **DNS** (Domain Name Service) permettent de faire la correspondance entre le nom alphabétique d'une machine (**hostname**) et son adresse IP (**address**). Quand il n'y a pas de serveur de nom, il est possible de renseigner chaque machine individuellement dans son fichier **"/etc/hosts"**. Un paquet qui circule sans adresse de destinataire valide arrivera sans doute jusqu'au sous réseau, mais là il sera perdu (**lost**) parce qu'aucune station ne le reconnaîtra. Le service **NIS** (Network Information Service) propose une centralisation des informations d'un réseau (**nis domain**). La configuration d'un serveur DNS local permet d'accélérer la résolution des noms de domaines.

L'identification d'une machine peut être, soit l'adresse MAC de sa carte réseau (**@mac**) qui est un numéro unique au monde et inscrit sur la carte réseau, soit l'adresse IP (**@ip**) correspondant au protocole TCP/IP du réseau, soit le nom de la machine sur le réseau (**hostname**). Si l'expéditeur ne connait que le nom de la machine, alors la pile de protocole réseau doit procéder à une **résolution** de nom. La résolution de nom consiste à rechercher dans une table de correspondance interne, ou à faire une demande auprès d'un serveur de noms sur le segment de réseau. La résolution de nom d'hôte (**resolver**) permet également de compléter le nom d'un hôte avec son domaine (host.domain.tld)

Quand une interface réseau (**interface**) est active (**up**), celle-ci écoutent toujours le câble réseau (**cable**) sur lequel elle est branchée. La carte réseau détecte si le support est libre (**free**), et si elle peut émettre (**send**). La carte réseau capte (**listen**) et enregistre (**receive**) les paquets qui lui sont adressés. Cette écoute est basé sur les signaux électriques (**signal**) des trames (**trames**) qui correspondent à leur adresse (**target**).

Le contrôle de la communication

Le contrôle des données est fondamental dans une transmission. Six étapes sont nécessaires pour que

chaque partie soit sûr qu'un message ait été correctement transmis et reçus.

Le contrôle de la communication		
Source	**Network**	**Target**
Envoi d'un message (**send msg**)	1 --> 2	Réception du message (**receive msg**)
Réception de l'accusé (**receive ack**)	4 <-- 3	Envoi d'un accusé de réception (**send ack**)
Envoi d'une confirmation (**send ack ok**)	5 --> 6	Réception de la confirmation (**receive ack ok**)

La négociation des cartes réseaux

Avant d'émettre une carte réseau entame un dialogue avec la carte réseau du destinataire. Les deux cartes réseaux doivent s'entendre sur un certain nombre de paramètres afin que la communication s'effectue dans de bonnes conditions. On dit que les cartes réseaux «négocient». Les paramètres faisant l'objet de la négociation sont des quantités, des durées et une vitesse de transfert. Une fois la mise au point des paramètres de connexion terminée, la transmission des données peut commencer.

Les paramètres de négociation des cartes réseaux
La taille maximale des paquets de données
Le volume maximal de données qu'une carte peut envoyer avant de recevoir une confirmation
L'intervalle de temps entre les transmissions partielles de données
Le délai d'attente pour une confirmation
La quantité maximale de données que peut traiter chaque carte réseau avant un débordement
La vitesse de transmission des données (la vitesse maximale commune aux deux cartes réseaux)

Le pilote réseau

Le pilote est un logiciel qui indique au système d'exploitation comment reconnaitre le périphérique et comment utiliser toutes ses fonctionnalités. Les fabricants de périphériques (**constructors**) fournissent en principe leurs pilotes aux éditeurs de logiciels (**editors**). Le pilote d'un périphérique (**driver**) est toujours spécifique au matériel (**hardware**) et au système d'exploitation (**system**). Idéalement, il faudrait que tous les pilotes, de tous les matériels, et de tous les fabricants puissent être incorporés, systématiquement et automatiquement dans toutes les procédures d'installation des systèmes d'exploitation. En réalité, il peut arriver que l'administrateur installe le pilote d'un périphérique après l'installation du système. Les pilotes sont en général téléchargeables depuis le site du constructeur du matériel.

Le pilote d'une carte réseau permet la communication entre la carte réseau et le système d'exploitation réseau. Quand une requête réseau est transmise au système d'exploitation, celui-ci la transmet au pilote de la carte réseau qui la traite et la redirige ensuite vers la carte réseau qui l'expédie. Dans le sens

contraire, c'est la carte réseau qui transmet les trames au pilote de la carte réseau, qui les traite et les redirige vers le système d'exploitation, qui l'envoie à l'application cible. Le pilote d'une carte réseau permet la communication entre la carte réseau et le système d'exploitation de l'ordinateur, c'est pourquoi il se situe au niveau de la couche LIAISON du modèle OSI.

L'installation du pilote réseau

Une fois installée, la carte réseau (**interface**) a besoin de son pilote (**driver**) pour pouvoir fonctionner. Le pilote est en général installé, supprimé ou mis à jour, soit par le chargement d'un module (**modules**), soit par un programme d'installation (**setup**) qui peut proposer une jolie interface graphique interactive. Un pilote obsolète doit être supprimé parce qu'il peut éventuellement rentrer en conflit avec un autre périphérique.

Le fichier du pilote qui doit être copié sur le disque dur de l'ordinateur peut provenir de plusieurs sources. Le pilote peut être sur une **disquette** vendue avec le matériel. Le pilote peut être sur le **site** internet du constructeur. Les **versions** de pilotes évoluent très rapidement, et il est parfois crucial d'installer la dernière version compatible. Quand cela est possible, il est préférable de privilégier l'achat de la carte réseau chez des **fabricants** de matériels reconnus, qui ont une longue expérience, et qui sont bien implantés. D'autre part, il est conseillé de choisir les matériels qui ont été testés par l'éditeur du système d'exploitation. Les matériels opérationnels figurent sur la liste des matériels compatibles ou **HCL** (Hardware Compatibility List). Les problèmes de pilotes sont fréquents et récurrents (vétusté, port de connexion, compatibilité avec le système d'exploitation). Lors de l'acquisition d'un nouveau matériel, il faut se préoccuper de savoir si un pilote existe pour le système d'exploitation en place.

Lors d'une mise à jour du système d'exploitation, il peut arriver que les **anciens** pilotes, qui fonctionnaient correctement avec l'ancien système, ne remplissent plus leur rôle. D'autre part, les pilotes fournis avec le nouveau système ne sont par forcément compatibles avec les vieux périphériques. Dans de tels cas, il faudra mettre à jour les pilotes de chaque périphérique, ce qui est plus facile que de racheter du matériel neuf. C'est pourquoi, il est judicieux de rechercher si des pilotes ont été développés pour les anciens matériels et le nouveau système.

Les pilotes de l'imprimante réseaux

Les pilotes de l'imprimante réseaux peuvent être à l'origine de nombreux déboires. Par exemple, la moitié seulement de la page est imprimée, ou les pages ne s'impriment pas avec la bonne police de caractères, ou les pages imprimées sont remplies de code d'impression illisibles, ou chaque page imprimée ne contient qu'un seul caractère. Dans de telles situations, il faut bien sur mettre à jour le pilote de l'imprimante ou le réinstallé s'il a été corrompu.

Le transceiver

Le transceiver (Transmitter Receiver) peut être un transceiver **externe** qui est relié à la carte réseau par

un câble de transceiver ou un transceiver **interne** qui est intégré à la carte réseau. Certaines cartes réseaux disposent d'un transceiver et d'un port pour transceiver, et il faut alors déterminer à l'aide de cavaliers lequel sera employé.

L'amorçage à distance

Certains environnements réseaux sont très sensibles à la **sécurité** des données et les stations de travail ne sont pas équipé de **disques**, ni de lecteur. Les données sont chargées depuis le réseau et restent à l'intérieur du réseau. Uniquement les serveurs sont équipés de disques durs, et les utilisateurs ne peuvent «exporter» aucunes informations numériques vers l'extérieur. Comme les ordinateurs ont besoin d'une séquence d'amorçage pour démarrer, celle-ci est stockée sur une mémoire **PROM** (Programmable Read Only memory) de la carte réseau. Cette puce est appelée «PROM d'amorçage à distance» et contient le microcode nécessaire pour démarrer et connecter l'ordinateur au réseau.

La configuration de la carte réseau

La configuration d'une carte réseau peut s'effectuer de deux façons, soit de façon automatique, soit de façon manuelle. La carte réseau doit être reconnu par la **détection** du nouveau matériel. La configuration automatique s'effectue avec l'aide d'un logiciel, il faut que la carte réseau et le système d'exploitation soit **Plug & Play**. Les cartes réseaux récentes sont généralement configurables via un utilitaire. Les paramètres et les options de configuration sont les même que pour une installation manuelle, soit, le numéro d'interruption système ou **IRQs** (Interrupt ReQuest), l'adresse de base en mémoire du port d'**Entrée/Sortie** (E/S) ou I/O (Input/Output), **l'adresse de base** de la mémoire pour le stockage des requêtes en mémoire tampon, le support DMA (Direct Memory Access), le type de support de communication, et le type de connecteurs.

La configuration manuelle s'effectue en déplaçant des cavaliers (**jumpers**), des commutateurs **DIP** (Dual Inline Package) qui indique à la carte réseau quel circuit électronique suivre. Les positions des cavaliers sont normalement détaillées dans la documentation du constructeur. Les jumpers contiennent une languette en métal conducteur permettant de relier deux broches. Les jumpers sont dits «fermés» lorsque qu'ils relient les deux broches, assurant ainsi la continuité du circuit. Ils sont dits «ouverts» dans le cas contraire. Les jumpers sont utilisés pour paramétrer les adresses des Entrées Sorties (I/O) utilisées par la carte pour dialoguer avec le système d'exploitation, et pour configurer les IRQ. Les Entrées Sorties sont souvent situées entre 200 hexadécimal et 380 hexadécimal.

L'adresse de base en mémoire

L'adresse de base en mémoire désigne un emplacement de la mémoire vive (**memory**) de l'ordinateur. La carte réseau utilise cet emplacement comme une mémoire **tampon** pour stocker les données qui la traversent. L'adresse de base en mémoire est parfois appelée «**adresse de début**» (Ram Start Address). L'adresse de base en mémoire ne doit pas être accessible, ni utilisée par un autre périphérique (**device**). L'adresse de base en mémoire doit être réservée et protégée. L'adresse de base en mémoire s'exprime

en hexadécimale, par exemple D80000 (D80000 peut être réduit en D8000 avec un zéro en moins).

Certaines cartes réseaux n'ont pas d'adresse de base en mémoire parce qu'elles n'utilisent pas les ressources de la mémoire vive de l'ordinateur. D'autres cartes réseaux disposent d'un paramètre permettant de spécifier la **quantité** de mémoire réservée pour le réseau (par exemple 16 Ko ou 32 Ko). Évidemment, plus la quantité de mémoire allouée à la carte réseau est élevée, et meilleures seront les performances du réseau.

L'adresse de base du port E/S

L'adresse de base du port E/S (Entrées Sorties) ou I/O (Input Output) spécifie un **canal** par l'intermédiaire duquel circulent les informations entre le périphérique (**device**) et le système d'exploitation (**system**) de l'unité centrale (**computer**). Pour le système, le port apparait comme une adresse mémoire (**memory**). L'adresse de base du port E/S permet au système de reconnaitre l'origine des données qui lui sont transmises. Chaque périphérique utilise une adresse de base du port E/S différente. Les numéros de port s'expriment en notation **hexadécimale**.

Les adresses mémoires d'Entrées Sorties de communication avec le système (I/O)

Périphérique (device)	**Adresse mémoire**
COM 1	03E8
COM 2	02E8
LPT 1	0378
Contrôleur de disques IDE	170 ou 1F0
Carte son	220 ou 330

Les IRQs

Les IRQs (Interrupt ReQuest) sont des **requêtes** d'interruption attribuées à tous les périphériques (clavier, souris, lecteurs, ports E/S, cartes réseaux, …) qui sont installés sur un ordinateur. Les IRQs permettent aux périphériques de communiquer avec l'unité centrale et d'effectuer une demande de services au **microprocesseur** de l'ordinateur. Les IRQs sont numérotés (de 0 à 15) et à chaque numéro correspond une **priorité**. Plus le numéro de l'IRQ est petit, plus la priorité est grande. Une IRQs permet d'interrompre le travail du microprocesseur au profit du périphérique qui en fait la demande. Quand plusieurs IRQs font en même temps une demande, c'est celle qui a la priorité la plus grande qui passe avant l'autre. Le choix d'une IRQ pour un périphérique s'effectue pendant l'installation ou la configuration du matériel. Une même IRQ peut être attribuée à plusieurs périphériques. Les périphériques peuvent **partager** la même IRQ, mais ils ne doivent jamais fonctionner en même temps, car sinon il y aurait risque de conflit. Comme le téléphone rouge, une IRQ emprunte un circuit dédié

qui mène directement au microprocesseur. L'impulsion électrique de l'IRQ utilise une ligne spéciale intégrée au matériel que l'on appèle une **ligne** de requête d'interruption. Chaque périphérique utilise une ligne de requête d'interruption qui lui est propre et qui est distincte de celle des autres périphériques. L'IRQ de la carte réseau peut être choisie parmi toutes celles qui sont disponibles. Généralement, c'est l'IRQ3 ou l'IRQ5 qui est sélectionnée. Néanmoins, L'IRQ5 est conseillé parce que c'est celle qui est le paramètre par défaut de beaucoup de carte réseau. Les IRQ 2 et 9 sont dites «**cascadées**», c'est à dire qu'elles contrôlent les IRQ de 9 à 15 qui ne sont donc pas des IRQ dédiés à une seule tâche, il vaut mieux éviter d'utiliser ces IRQ qui sont susceptibles de provoquer des conflits. Des utilitaires (**tools**) permettent de connaitre la distribution des IRQs.

La distribution des IRQs

Les IRQs pour un processeur Intel 80286	
IRQ	**Périphérique généralement associé** (device)
0	Réservé au système (timer system)
1	Contrôleur clavier
2 (9)	La carte graphique EGA/VGA (Enhanced Graphics Adapter / Video Graphics Adapter)
3	Deuxième port série COM 2 et COM 4, ou souris série
4	COM 1 et COM 3, modem
5	Deuxième port parallèle LPT2 ou carte son
6	Contrôleur de lecteur de disquette
7	Port parallèle LPT1 ou l'imprimante
8	Horloge système CMOS temps réel
9	
10	
11	
12	Souris PS/2 de type bus (contrairement aux souris de type série)
13	Coprocesseur arithmétique ou mathématique
14	Contrôleur primaire des disques IDE
15	Contrôleur secondaire des disques IDE

MODEM

Les modems

Les communications avec des modems utilisent les lignes de **téléphone** comme support de communication.

La transmission **analogique** requière des modems de part et d'autre de la liaison. Les modems (modulateur démodulateur) 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 réception (**download**) et seulement 33 Kb/s en émission (**upload**). 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. En général, il n'y a que deux ports (COM1 et COM2) sur les ordinateurs. Toutefois, il existe des «**cartes série multiport**» 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 connexions séries

Les connexions séries sont des connexions établies sur le port série d'un ordinateur (**serial**). Les connexions séries permettent de brancher un modem à la prise du téléphone et d'obtenir une connexion analogique avec un opérateur de téléphone ou un fournisseur d'accès à internet (**provider**). Le modem de l'ordinateur (interne ou externe) est connecté à l'un des ports séries de l'ordinateur (COM1, COM2, 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.

Les connexions analogiques sur le port série utilisent les protocoles DIP, SLIP, CSLIP ou PPP de la pile de protocole TCP/IP. 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 des protocoles d'accès à distance aux réseaux étendus.

Une connexion série peut être établie directement entre deux ordinateurs à l'aide d'un câble **Null Modem**.

Les lignes du réseau téléphonique

La communication par modems peut s'effectuer sur deux sortes de support de communication, les lignes RTC et les lignes louées. Les lignes ordinaires du réseau téléphonique public ou **RTC** (Réseau Téléphonique Commuté) qui conviennent pour des communications **analogiques** de courte durée, et peu fréquentes. Les lignes RTC ont été conçues pour transmettre la voix et non pour échanger des données.

Les lignes louées auprès d'un opérateur téléphonique, sont des lignes **numériques** spécialisées, dédiées. Les lignes louées sont plus efficaces et conviennent pour les communications permanentes, avec de gros transfert de fichiers. Les débits d'une ligne louée peuvent atteindre 45 Mb/s. Les opérateurs téléphoniques proposent leurs propres lignes spécialisées et louent les lignes d'autres opérateurs. Ainsi, des lignes spécialisées peuvent être établies sur plusieurs réseaux de téléphone public. Ces lignes spécialisées sont des lignes dédiées, c'est à dire que le support de communication et la bande passante sont réservés. Ces lignes spécialisées permettent de réaliser des réseaux privés virtuels ou **VPN** (Virtual Private Network).

Les avantages des modems

Les modems font partis des équipements qui permettent d'établir une liaison distante avec un réseau lointain et étendu ou **WAN** (Wide Area Network). Les modems permettent de se connecter, via le **RTC** (Réseau Téléphonique Commuté), à internet, ou à tout autre réseau branché sur le réseau téléphonique. Les modems permettent d'agrandir un réseau local, «sans tirer de câbles», puisque le réseau téléphonique existe déjà à travers le monde entier, ou presque.

Les critères pour choisir le type de liaison

La mise en place d'un système de communication par modem requière de confronter et d'arbitrer plusieurs critères.

La **fréquence** des communications (occasionnelle ou permanente), le **volume** ou la quantité des données à transférer (petits fichiers ou grosses bases de données), la **vitesse** de transfert ou le débit, le **mode** de transfert (synchrones ou asynchrone), le **cout** des communications téléphoniques (locales ou internationales), le cout de matériels, le cout de l'installation et de la maintenance, la **qualité** de la ligne (analogique, RTC, louée ou numérique) et la **sécurité** des échanges.

Les fonctionnalités d'un modem

Un modem permet de "MODuler" et de "DEModuler". Les signaux numériques de l'ordinateur sont transformés (modulés) en signaux analogiques (une courbe continue) pour être transportés sur les câbles en cuivre du réseau de téléphone **RTC** (Réseau Téléphonique Commuté).

Une fois arrivée à destination, les signaux analogiques sont transformés (démodulés) en signaux numériques pour être traités par la machine. Les signaux numériques sont des impulsions binaires (il y a un haut et un bas), tandis que les signaux analogiques sont **modulations de fréquences**, des courbes continues (il y a tous les niveaux possibles entre le minimum et le maximum).

La vitesse de transmission

La vitesse de transmission des données s'exprime de deux façons, en Bauds par seconde (B/s) et en bits par seconde (b/s).

Les **Bauds** par seconde (B/s) ont été inventés par l'ingénieur français Emile Baudot, officier des services de transmission de l'armée française. Le «baud» désigne la **vitesse de modulation de l'onde** analogique qui transporte une unité d'information sur le câble de la ligne téléphonique. A l'époque, une unité d'information correspondait à un bit.

Le nombre de **bits** par seconde (b/s) exprime le nombre de bits numériques qui sont transmis depuis l'ordinateur. Aujourd'hui, les techniques de **compression** et d'encodage des données permettent d'accélérer les transmissions en réduisant la taille des fichiers. Le nombre d'unité d'information analogique à transférer sur le câble du réseau téléphonique est donc inférieur au nombre de bits d'origine. Chaque modulation d'onde transporte toujours une unité d'information, mais à cette unité d'information peut correspondre plusieurs bits. Le nombre de bits par secondes est donc toujours supérieur ou égal au nombre de Bauds par secondes. Désormais, les vitesses de transmission s'expriment en bits par seconde, et tiennent compte des technologies de compression.

La vitesse de transmission des données doit tenir compte des capacités respectives des modems qui se trouvent de part et d'autre. C'est la vitesse commune la plus rapide qui est utilisée par les deux modems. Il peut exister des **pools** de modems, c'est à dire le rassemblement de plusieurs modems qui permettent de mutualiser les capacités de transmission.

La compression des données

La compression des données permet d'accélérer globalement la transmission des données. Les données ont été «épurées» des éléments **redondants** et des espaces vides. Les données doivent au préalable être encodées ou compressées, ce qui prend un certain temps, puis les données compressées sont envoyées sur le câble ou le canal de communication. Sur le support de communication, les données compressées sont transportées à la vitesse que supporte le canal ou **vitesse de signalisation** ou débit.

La compression des données permet plus ou moins de doubler la quantité d'information transmis, et donne l'impression que les données sont transmises deux fois plus vite. Les unités d'information transitent toujours à la même vitesse (en fonction du type de câble), mais les unités d'information véhiculent virtuellement un nombre de bits plus important, d'où l'idée d'affirmer que le débit est plus

important. Ce n'est pas la vitesse qui augmente, c'est la quantité qui diminue!

Le protocole **MNP** de classe 5 est une norme de compression des données pour les communications asynchrones. Il faut que les deux extrémités d'une communication utilisent la norme MNP 5 pour que la transmission s'effectue deux fois plus vite.

Les méthodes de transmission des modems

Les méthodes de transmission des modems sont classées en deux catégories. Les communications asynchrones (**Asynchronous**) et les communications synchrones (**Synchronous**) qui requiert respectivement des modems asynchrones et des modems synchrones.

Les communications asynchrones

Les communications asynchrones (Asynchronous) sont les plus répandues parce qu'elles utilisent une ligne de **téléphone** ordinaire. La transmission asynchrone expédie les données sous la forme d'un flux **discontinu**. Les données sont découpées en petits paquets (un octet par exemple, donc une série de huit bits), à chaque paquet est rajouté un bit de début et un bit d'arrêt. Lors de l'établissement de la connexion, les deux modems asynchrones (celui de l'émetteur et celui du récepteur) se mettent d'accord sur le nombre de bits constituant une série.

L'envoi des bits n'est pas synchronisé. Le contrôle et la coordination des données représentent 25 % du trafic d'une transmission asynchrone. Les modems asynchrones sont moins chers que les modems synchrones (qui prennent en charge la synchronisation de la transmission des données, et qui sont dotés pour cela de circuits électroniques spécifiques).

Le contrôle des erreurs des communications asynchrones

Les communications asynchrones peuvent incorporer un bit de parité (**Parity Check**) qui permet de détecter et de corriger les erreurs de transmission. Le nombre de bit d'une série doit toujours être pair. Ainsi, le bit de parité sera présent ou non, en fonction du nombre de bits à un dans la série. C'est la société Microcom qui inventa pour la norme V.32, une technique de contrôle des erreurs ou **MNP** (Microcom Network Protocol). Cette technologie fût adoptée par les autres fabricants, puis développée en différentes classes (les protocoles MNP de classe 2, 3 ou 4…).

En 1986, le **CCITT** publia une norme de contrôle d'erreurs, la norme V.42 qui incorpore deux protocoles de contrôle d'erreurs, le protocole LAPM (Link Access Procedure for Modems) pour les modems compatibles V.42 et le protocole MNP de classe 4 (Microcom Network Protocol) pour toutes les normes de modems. La vitesse de transmission d'une communication asynchrone peut atteindre 28 800 b/s, et 115 200 b/s avec des méthodes de compression très performantes.

Les caractéristiques des modems asynchrones

Les modems asynchrones se présentent de deux façons. Les modems **externes** sont des boîtiers qui se branchent à un des ports de l'ordinateur (port série, port USB). Les modems **internes** sont des cartes qui s'insèrent sur un des connecteurs de la carte mère (ISA, EISA, PCI).

Les modems sont des **ETCD** (Equipements Terminaux de Circuits de Données). L'interface de communication avec l'ordinateur est une interface **série** (RS-232) ou une interface USB. L'interface série est le type de connectique le plus répandu qui se trouve en bout du câble série et à l'arrière de l'ordinateur. L'interface pour la ligne téléphonique est de type RJ11, c'est la connectique qui se branche sur la prise murale du téléphone, et qui permet de relier le modem au réseau téléphonique.

Les normes des modems asynchrones

Il existe deux normes pour les modems asynchrones, la norme HAYES et les normes V de l'UIT. La norme **HAYES** est issue de la société Hayes Microcomputer Products qui au début des années 1980 inventa le «Hayes Smartmodem». Ce modem était considéré comme intelligent (**smart**) parce qu'il pouvait composer automatiquement le numéro de téléphone, sans qu'il faille décrocher le combiné du téléphone. Cette technologie devint rapidement un standard, et l'on parle toujours de modems compatibles Hayes.

Les normes V de **l'UIT** (Union Internationale des Télécommunications) sont, la norme V.22bis qui permettait en 1984 un transfert de 2 400 b/s, la norme V.42 qui propose en 1995 un transfert de 57 600 b/s et la norme V.42bis/MNP5 qui transporte des données compressées à 76 800 b/s.

Aujourd'hui, les modems peuvent combiner plusieurs normes différentes afin d'optimiser les performances. Par exemple, pour une liaison asynchrone par circuits analogiques entre réseaux locaux, la norme V.32bis est utilisée pour la signalisation, la norme V.42 est utilisée pour le contrôle des erreurs et la norme V.42bis est utilisée pour la compression des données.

Les communications synchrones

Les communications synchrones (**synchronous**) sont moins répandues, mais plus difficile à mettre en œuvre. Les communications synchrones sont plus chères, mais plus efficaces. Les communications synchrones sont surtout utilisées pour les liaisons **numériques** avec des lignes numériques, et ne sont pas destinées au marché grand public.

Dans les communications synchrones, il n'y a plus de bits de début, ni de bits d'arrêt, mais des bits de synchronisation qui encapsulent les données. Les données sont rassemblées en paquets qui comportent plus de bits qu'une série en mode asynchrone. L'on parle plutôt de **trames** en mode synchrone, et il y a plusieurs octets par trames.

Les **protocoles** des communications synchrones effectuent, comme tout autre protocole, plusieurs

tâches, dont le formatage des données et l'ajout de bits pour le contrôle des erreurs.

Les protocoles synchrones
Le protocole **SDLC** (Synchronous Data Link Control)
Le protocole **HDLC** (High-level Data Link Control)
Le protocole **BSC** (Binary Synchronous Communication)

Le protocole PPP

Les protocoles SLIP et PPP sont les protocoles utilisés pour une **liaison «série**». La liaison série permet de brancher un modem à la prise téléphonique et de configurer une connexion **analogique**. Les liaisons séries ont été développés pour les ordinateurs ne disposant pas de carte réseau, mais seulement d'un port série. Le protocole SLIP est remplacé par le protocole **PPP** (Point to Point Protocol) 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 constitue un trou de sécurité, surtout que généralement le processus d'identification lors d'une connexion distante n'est pas sécurisé. Les noms de compte (login) 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, en gardant une trace dans un **journal** de tous les appels entrants et de toutes les tentatives de connexion, en limitant le nombre des **tentatives** de connexion pendant une certaine durée pour le même login, en utilisant des **jetons** d'accès (ce sont des numéros qui sont générés par des calculettes, et qui changent constamment) en plus du login et du mot de passe, en modifiant les paramètres de PPP et en utilisant une connexion **cryptée**, en utilisant des protocoles d'accès à distance plus sécurisés, comme les protocoles **CHAP** (Challenge Handshake Authentication Protocol) et **PAP** (Password Authentication Protocol).

Les paramètres d'une connexion PPP (Point to Point Protocol)
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)
L'adresse IP de l'ordinateur peut faire office de passerelle pour pouvoir accéder à internet
Le protocole de sécurisation **CHAP** (Challenge Handshake Authentication Protocol)
Le protocole de sécurisation **PAP** (Password Authentication Protocol)

PROJECT

Le processus de décision

Avant de prendre une décision importante, il faut procéder en quatre étapes. La **collecte** d'informations (**gathering**) est un processus long, vaste et hétéroclite qui va dépendre des enjeux (**goals**) et du temps (**time**) que l'on est prêt a y consacré. La planification d'un projet requiert de savoir ce qui est **possible** et de déterminer ce qui est **souhaitable**. En réalisant des études de marché (**market**), en s'imprégnant des technologies (**technology**), en lisant la documentation, en interviewant les clients, les futurs utilisateurs, les collaborateurs et les dirigeants, en rencontrant les experts, les consultants, en inspectant les méthodes des intégrateurs, en inventoriant les produits des constructeurs, en comparant les stratégies et les algorithmes des éditeurs, en prenant contact avec les fournisseurs et les distributeurs (**people**), l'on évalue la situation plus ou moins objectivement, et l'on se crée une carte mentale des **contraintes**, des fantasmes, des **intervenants** et de leurs attitudes.

L'analyse de toutes ces informations (**analysis**) doit être méticuleuse et il faut savoir perdre son temps pour les laisser décanter, mûrir, prendre place et s'harmoniser avec les idées directrices et fondatrices du projet. Le choix d'une solution, ou le choix de ne pas pousser plus loin le projet, est une décision qui doit un jour ou l'autre être prise. Ce choix (**choice**) dépend bien évidemment des informations qui ont été collectées et de la valeur qui leur ont été assignées. La non décision est une décision aussi importante et aussi lourde de conséquences que le choix d'une solution. La diffusion (**spreading**) de la décision aux personnes concernées est importante et constitue le premier pas concret en avant vers la réalisation du projet, ou le premier vers un autre projet. Faire comprendre aux autres ce que l'on fait (**why**), ce que l'on veut (**what**), ce que l'on peut (**how**), ce que l'on a décidé (**who**) et le temps que l'on se donne pour l'accomplir (**when**) est cruciale pour le rassemblement des motivations et le positionnement de toutes les personnes qui prendront part au projet.

Le cycle de vie

Il faut savoir entendre les critiques, savoir relativiser les situations, et savoir aussi remettre en question ses propres décisions afin de pouvoir les adapter. Le changement est la seule constante. La **Loi de Moore**, le co fondateur de la société Intel, indique que la puissance des processeurs doubles tous les 18 mois. Il se trouve que le besoin en mémoire vive des applications grossit de version en version. Ainsi, les progrès de la puissance de calcul sont absorbés par les besoins qui s'adaptent aux capacités, et les traitements s'appliquent à des objets de plus en plus complexe.

Les technologies de l'informatique évoluent très rapidement, le **cycle** de renouvèlement du matériel est très court, aussi est-il rentable d'anticiper les besoins futurs et d'adopter les technologies qui vont rester. Le choix de la configuration la plus performante du moment pour un serveur (processeur, mémoire vive, espace de stockage, carte graphique) permet parfois d'allonger la durée de vie d'un matériel, mais

ce n'est pas toujours une nécessite que de courir après les **innovations**.

Le cout de possession

Le **cout** des dernières technologies est toujours moins important, passé le délai d'annonce et la campagne de promotion. Les équipements qui disposent de fonctionnalités avancées deviennent moins rapidement obsolètes que les autres. Bien sûr, une décision a un cout, 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 cout annuel d'utilisation d'un PC à 60 000,00 Francs (**ownership cost**). En générale, l'installation d'un réseau est un facteur de réduction des couts à moyen terme et un levier d'augmentation de la productivité.

Un réseau en bon état de marche ne sert à rien s'il n'y a pas d'utilisateurs qui se servent du système, des applications et des fonctions pour créer de la **valeur ajoutée** et activer des niches de rentabilité. L'utilisation d'un système d'information consiste principalement à organiser l'information et à la transmettre à d'autres personnes. 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 ont besoin de la même fonction ou qu'ils emploient la même application, c'est qu'il est rentable d'envisager une solution mutualisé et une automatisation.

Les couts d'acquisition des **licences** des produits propriétaires sont très importants. Il va sans dire qu'un utilisateur se doit d'acheter le droit d'utilisation du logiciel dont il se sert, d'une part pour ne pas spolier les auteurs de leurs revenus, mais aussi pour rester dans la légalité, et pouvoir recourir au support technique et aux mises à jour que la clientèle est en droit d'attendre. Toutefois, l'utilisation des **Logiciels Libres** est un choix avantageux financièrement, parque qu'il n'y a pas de licence à payer, mais c'est surtout un choix technique et stratégique pour l'avenir, en même temps qu'un choix éthique et communautaire.

Le cahier des charges

La rédaction d'un **cahier des charges** rassemblant les spécifications précises et détaillées du projet permet de limiter les risques de dérive et de perdition. Il faut savoir arrêter la conception et valider l'avancement d'un projet par la mise en valeur d'étapes structurantes et motivantes. Par exemple, il n'est pas judicieux de changer de direction en cours de projet ou de procéder à l'ajout de fonctionnalités supplémentaires.

De surcroit, le document rassemblant les spécifications du réseau constitue 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.

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 en amont, dans la mesure du possible.

Les critères d'évaluation d'un système d'information	
Fonction	Le partage des ressources, le travail en groupe et l'accès à internet (**share**) La méthodologie, la centralisation et l'automatisation de l'administration (**digital**) Les délais, les marges, les budgets, les contraintes, les risques, les études (**planning**)
Strategy	L'anticipation des évolutions futures et la rétro compatibilité avec l'existant (**generation**) Les degrés d'ouverture, de compatibilité, d'hétérogénéité et d'interopérabilité (**open**) L'adoption des standards et la conformité aux normes et aux lois (**conformation**) La portabilité vers d'autres architectures (**portable**)
Service	Les serveurs de fichiers, d'impression et de sauvegarde (**data**) Les serveurs d'applications bureautiques et de (**groupware**) Les serveurs réseaux de messagerie, de routage (**servers**) Les dispositifs de sécurité et les serveurs d'authentification (**firewall**)
Size	Le nombre de nœuds pour les stations, les serveurs et les routeurs (**nodes**) Le nombre de sites, de liaisons et de sous réseaux (**segmentation**) La localisation des sites, la mobilité des utilisateurs et l'accès à distance (**remote**)
Data	Le format et la nature des données publiques, privées ou sensibles (**privacy**) Le contrôle de l'intégrité et de la confidentialité des données (**integrity**) La redondance, les équipements, les volumes et le calendrier des sauvegardes (**backup**) La rédaction d'un cahier des charges, d'un journal de bord et de diagrammes (**paper**)
Network	Le débit moyen attendu et futur, le routage des communications (**broadband**) Le type de câblage et la nature des signaux et le benchmarking (**cables**) Le type d'architecture du réseau et le mode de transmission (**architecture**) Le choix des protocoles et des logiciels libres (**free software**)
Product	La dépendance vis à vis d'un constructeur, d'un éditeur ou d'un distributeur (**freedom**) Le service après vente des produits par leurs fournisseurs (**support**)
People	Le nombre des utilisateurs, leurs compétences et leurs formations informatiques (**users**) L'administration, les tests, les alertes, la veille technologique et concurrentielle (**root**) La conception, la planification, l'installation, la configuration, l'optimisation (**tuning**) Les intervenants, l'assistance, les services et l'expertise extérieure (**outsiders**)
Security	L'évaluation du niveau de sécurité attendu, les certifications, les labels (**clearance**) La mise en œuvre de procédures et de sanctions strictes et généralisées (**monitoring**) Les outils de surveillance et de protection contre les virus et les intrusions (**firewall**) La conservation du sang froid, du bon sens et de la bonne humeur (**spirit**)

Des exemples d'organisation

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 clients et serveurs permet la **centralisation** des fichiers, facilite les sauvegardes, et accroit le contrôle des utilisateurs. Les serveurs ont généralement besoin de plus de puissance, de plus de mémoire et de plus de **capacité** de stockage que les stations.

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 optimisés. 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 séparés, c'est à dire que les paquets sont filtrés et routés, mais aussi, les deux segments forment un sous réseau indépendamment des autres **zones** du réseau. Cette technique s'appèle un **VLAN** (Virtual LAN).

L'administration centralisée d'un réseau peut être plus ou moins poussée. Les outils d'administration réseaux reposent sur les **protocoles** standard, comme TCP/IP, **SNMP** (Simple Network Management Protocol) et **RMON** (Remote Monitor). Il ne faut pas que tout le réseau dépende d'une seule personne, ni d'un seul matériel ou alors il faut surprotéger cette personne et ce matériel. Si le budget est limité, il vaut mieux souvent répartir la charge entre plusieurs petits serveurs, plutôt que d'investir dans un seul et ultra puissant ordinateur qui n'est pas exempt d'une panne.

Souvent, un dessein vaut mieux qu'un long discours, aussi est-il judicieux d'élaborer un **diagramme** du réseau, c'est à dire un dessein organisationnel, fonctionnel et relationnel qui répertorie et classe tous les ordinateurs et tous les dispositifs du réseau, logiquement et physiquement. Il est important de ne pas négliger les conditions d'utilisation et de fonctionnement, comme la ventilation ou la **climatisation** des pièces. Quand plusieurs appareils partagent le même local, il est prudent de vérifier si **l'alimentation** électrique existante sera suffisante pour alimenter tous les appareils. 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 nombre et le type des matériels (**device**), la longueur des supports de communication et des cordons de brassage (**cable**), la correspondance entre les connecteurs (**connector**), les concentrateur (**hub**), les dispositifs de connectivité (**router**) et les cartes réseaux (**interface**), la surface utile de l'armoire de brassage (**room**), et le temps pour mettre tout cela en place dans les délais (**timing**).

D'une façon générale, il faut consigner dans un cahier tout ce qui se passe (**booking**), afin de garder une trace des innombrables évènements qui jalonnent l'implémentation et l'administration d'un réseau,

et de pouvoir entamer un recours en cas de litige. Enfin, il faut tester tout de suite l'installation (**testing**). Certaines sociétés proposent des questionnaires qui permettent d'orienter le choix entre la multitude des technologies. D'autres sociétés, proposent des configurations génériques ou un simple accord de confiance.

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 sécurisation physique des matériels est une prise de conscience importante. Il suffi de redémarrer un système avec une disquette (**boot**) pour accéder à toutes les informations qu'il contient. La sécurisation logique des données est également un point de départ à leur pérennisation et leur confidentialité. Une stratégie de mot de passe peut résister plus ou moins longtemps à une attaque en force (**brute force cracking**) qui essaye toutes les combinaisons possibles. L'optimisation (**tuning**) et la personnalisation de la configuration dépend de la connaissance des exigences du site et des activités particulières des utilisateurs du réseau.

Les ressources internet

De nombreuses ressources sont disponibles sur internet, mais celles-ci sont à prendre avec précaution.

La navigation sur la toile ou **WWW** (World Wide Web) permet de rechercher des informations et de trouver des pages en **HTML** (Hyper Text Markup Language). Les serveurs **FTP** (File Transfert Protocol) permettent de télécharger des documents ou des programmes. Le protocole **ARCHIE** permet de retrouver les sites FTP, tandis que les **BBS** (Bulletin Board Services) permettent de s'abonner à des discussions thématiques. La messagerie électronique permet d'échanger des messages électroniques (**mail**) et de recourir à une aide en direct dans des salons de chat (**irc**) ou de façon asynchrone sur des forums avec le protocole **NNTP** (Network News Transfer Protocol). Les forums permettent d'échanger des nouvelles, et de participer à des conversions ou à des conférences. Les serveurs **Gopher** indexent et classent les fichiers, et qui permettent avec l'aide d'un moteur de recherche de retrouver des informations sans en connaitre l'emplacement sur la toile.

Les diagrammes réseaux

Les ordinateurs d'un réseau peuvent être classés selon leur fonction, leur emplacement ou la catégorie de leurs utilisateurs. Il est instructif de dessiner le diagramme complet du réseau qui montrera la topologie les dispositifs de connectivité, avec le nombre et le type de ports, les câbles, la segmentation et la répartition des machines dans les sous réseaux et dans le différentes pièces ou locaux du site.

Il existe plusieurs logiciels de création des diagrammes réseaux (Visio Pro, ClickNet, NetDraw).

Un exemple de 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, assez facile à mettre en œuvre et d'un cout raisonnable.

Un exemple de petit réseau standard
Une architecture Ethernet en bus en étoile
Un câblage en paire torsadée non blindée (UTP catégorie 5)
Des cartes réseaux Ethernet avec des connecteurs RJ45
Une segmentation en sous réseau avec des routeurs et une passerelle ADSL vers internet
Une organisation en client serveur avec des serveurs de fichiers et une imprimante réseau
Une stratégie de sauvegarde sur un disque dur dédié et sur CD-ROM
L'utilisation de Logiciels Libres et de protocoles ouverts

INTERVIEW

Un exemple de questionnaire

Les sites de production
Le nombre maximal de sites:
La distance maximale entre les sites:
L'emplacement des câbles internes :
L'emplacement des liaisons externes:
Les types de liaison entre les sites
La communication entre deux sites (liaison point à point):
La communication entre plusieurs sites et un site central (liaison point à multi point):
La communication entre de nombreux sites (liaison multi point à multi point):
La redondances des chemins entre sites (commutation):
La correspondance des architectures des sites (homogénéité):
La sécurisation des communications
Les fournisseurs de télécommunication dans la région:
La protection du câblage contre les interférences et les écoutes:
La chambre forte pour le serveur principal:
Le lieu de stockage externe pour les sauvegardes:
L'accès à internet:
L'externalisation de la gestion du site internet:
Les types et la quantité de matériels
La distance maximale entre les postes:
La distance maximale entre les postes et le concentrateur:
Les types d'ordinateurs:
Le nombre d'ordinateurs:
La puissance des ordinateurs:
La capacité multimédia des ordinateurs:
La capacité de connexion des ordinateurs à internet :
Le nombre d'imprimantes:
Le nombre de feuilles imprimées par jour:
L'alimentation électrique:
La climatisation:
Les logiciels
Les types de systèmes d'exploitation réseau:
Les applications les plus utilisées:
Le nombre de personnes utilisant chacune de ces applications:
L'application de messagerie (interne ou externe):
L'application de base de données:
Les applications de travail collaboratif (groupeware):

La réactivité des mises à jour des applications et des pilotes:

Les données

La sensibilité des données:
Les types de fichiers les plus utilisés :
Le cryptage des données:
La protection contre les virus:
La régularité des sauvegardes:
La mise en place d'une redondance des données (tolérance de panne, système RAID):
La régulation de l'alimentation électrique avec un ondulateur (UPS):
La copie des logiciels et des pilotes dans un lieu sûr:
La documentation:

L'administration

La centralisation de la sécurité:
La centralisation de l'administration:
La centralisation des applications sur des serveurs dédiés:
La centralisation des données sur des serveurs dédiés :
Les répertoires personnels de chaque utilisateur (privé, partagé, public) :
La standardisation de l'interface pour tous les utilisateurs:
Le délai moyen pour accéder à une ressource partagée sur le réseau:
La durée maximale d'interruption du réseau:
Le délai minimal pour restaurer un système défaillant:
Les ressources partagées:
Les ressources protégées:
La stratégie des mots de passe au niveau des ressources:
La stratégie des mots de passe au niveau des utilisateurs:
La détermination de valeurs de références:
La veille technologique et l'analyse des tendances:

Le trafic du réseau

Le suivi du trafic réseau:
La détection des goulets d'étranglement:
La segmentation du trafic:
Le routage du trafic:
La redondance des chemins:
La surveillance des activités des utilisateurs:
L'audit des ressources:
La possibilité de «sortir» des informations du réseau:

Les personnels internes

Le responsable du projet:
Le responsable qualité:
L'administrateur réseau:
Le nombre maximum d'utilisateurs:
Les permissions (accès, lecture, écriture) de chaque utilisateur:
La délégation des responsabilités:

Le nombre de groupes d'utilisateurs:
Les périodes de formation pour les utilisateurs:
Le type de formation:
La certification:
Les kits de ressources techniques:
Les personnels externes
Les consultants:
Les experts:
Les fournisseurs:
Les constructeurs:
Les éditeurs:
Les intégrateurs et société de services:
L'assistance technique extérieure:
Les services de diagnostic à distance :
Les risques et les contraintes
La protection des données de l'ancien système:
L'incorporation et la conversion des données de l'ancien système au nouveau système :
La période de transition entre l'ancien système et le nouveau:
Les tests de validation du nouveau système:
La date butoir pour le nouveau réseau:
La personne qui prononce le discours d'inauguration:
Le budget maximal

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 planification et la maintenance des réseaux sont étroitement liées.

La conception et la planification du réseau (AVANT)

La rédaction d'un cahier des charges (POURQUOI) réaliste et conforme aux besoins :
Les études d'opportunités, de faisabilités et de marchés
Les utilisateurs, les «process», les services concernés par l'informatisation
La mise par écrit des fonctions, des spécifications détaillées, des garanties
La normalisation des composants (interopérabilité) et des applications (compatibilité)
La sélection des intervenants (QUI) reconnus et fiable dans le temps :
La mise en concurrence des fournisseurs, des consultants et des experts
Le choix du maitre d'œuvre et du maitre d'ouvrage, leurs responsabilités respectives
L'administrateur, le technicien réseau, les interviews de satisfaction des utilisateurs
Le service d'assistance sur site ou par téléphone (la hot ligne, l'administration à distance)
L'établissement d'un planning (QUAND) précis et souple :
Les délais

Les marges
La date de livraison
La période du service après vente

L'élaboration d'un budget (COMBIEN) strict et prévoyant :

L'amortissement
La facturation
Les pénalités en cas de dépassement des délais
La majoration des imprévues
La négociation des développements futurs

La planification (OU) d'une architecture cohérente et évolutive :

L'envergure géographique du réseau (Intranet, LAN, MAN, WAN)
La taille du réseau en nombre de nœuds (10, 100, 1000)
La sensibilité des données (entre utilisateurs, partenaires ou concurrents)
La protection des données (interférences, blindage, écoutes, piratages, virus, défaillances, pannes)
Le débit, la bande passante (dans le présent et le futur)
L'ouverture vers l'extérieur (internet, les liaisons distantes, les réseaux étendus)
Les lignes analogiques commutées du réseau téléphonique (RTC)
Les lignes numériques louées, dédiées, spécialisées
La location d'une bande passante garantie
La commutation de paquets des liaisons distantes
Les lignes privées ou les réseaux virtuels sécurisés (VPN)
L'implémentation d'une seule plate-forme ou l'harmonisation de l'hétérogénéité

La sélection des technologies (QUOI) :

L'architecture (Ethernet, Token Ring, ATM, FFDI)
La topologie (en bus, en étoile, en anneau, le maillage)
Le câblage (en cuivre, en fibre optique, les ondes radios, les satellites, les liaisons spécialisées)
Les connecteurs (BNC, RJ45, fibres)
Les types de fichiers (voix, vidéo, applications partagées, bases de données, messagerie, cryptages)
Le type de signal (la modulation de fréquence électrique, la lumière, les ondes)
Le mode de transmission des signaux (le large de bande analogique, la bande de base numérique)
Les dispositifs de connectivité (concentrateurs, répéteurs, ponts, routeurs, passerelles, modems)
L'architecture interne de la carte mère (les ports d'extension, le bus interne, le nombre de processeur)
Les cartes réseaux (les ports BNC, RJ45, AUI, le débit, la mémoire tampon, le processeur dédié)
La méthode d'accès au câble (CSMA/CD, CSMA/CA, le jeton, la priorité de la demande)
Les protocoles réseaux (routables ou non)
Le type d'organisation (peer to peer, clients serveurs, centralisée, distribuée, partagée, relationnelle)
Les systèmes d'exploitation réseaux multi tâches (Unix, Gnu Linux, Windows, Novell, Mac OS, OS/2)
Les outils d'administration

<u>L'installation et l'administration du réseau (PENDANT)</u>

L'installation et l'implémentation (COMMENT) scrupuleuse et attentive :

L’implémentation des câbles, des matériels et des logiciels en interne ou par une société externe
La segmentation du réseau pour limiter, circonscrire ou répartir le trafic
La répartition des responsabilités
La configuration précise et consciente des multiples paramètres
L’attribution de noms explicites à chacune des ressources du réseau
La standardisation des applications et de l’environnement des utilisateurs
L’administration du réseau (QUOI) méthodique et officiels :
L’administration des utilisateurs et des groupes
Le partage des ressources
Au niveau des ressources
Au niveau des utilisateurs
La stratégie de mot de passe
L’établissement d’une convention de nommage des noms de compte (login) des utilisateurs
La longueur, les caractères autorisés, la durée de validité, l’historique des anciens mots de passe
Les conditions de verrouillage des comptes
Les permissions d’accès aux groupes
Les droits d’effectuer des tâches systèmes à quelques personnes
La désactivation du compte invité
L’utilisation restreinte du compte administrateur
La prévention (QUAND) prudente et soignée des multiples causes de dysfonctionnement :
Les sauvegardes régulières et systématiques
Le type de sauvegarde, complète, incrémentielles, différentielles
La fréquence des sauvegardes
Le média utilisé pour les sauvegardes (bandes, disques amovibles, CDROM ré-inscriptibles)
La localisation des bandes à l’extérieur du site
Le calendrier des sauvegardes
Le journal de sauvegarde
Le segment séparé pour le serveur de sauvegarde
L’alimentation de secours (UPS)
La redondance des matériels
La redondance de la carte mère
La redondance des disques vierges ou avec une copie miroir
La redondance des serveurs avec un système de cluster
La redondance des données, la tolérance de panne et les systèmes RAID
Les programmes de clonage qui créent une image d’un disque dur comme (Ghost)
La prévoyance de l'évolution du réseau et des besoins futurs
Les mises à jour des logiciels en dehors des heures de travail
Les tests des mises à jours sur une machine indépendante et pendant une période significative
L’installation régulière des «patchs» et des correctifs des éditeurs
La mise en place d’une procédure de récupération ou de désinstallation.
Les tests des nouvelles configurations et des procédures de restauration
La veille technologique et concurrentielle
L’état de l’art des techniques et des métiers

L'apprentissage et l'acquisition d'information (librairies, livres, thèses, journaux, magazines, clubs).
La surveillance de l'évolution des méthodes d'espionnage

La surveillance (QUI) des composants, du trafic et des utilisateurs:

L'enregistrement de valeurs de référence (sur une longue période) du trafic et du taux d'utilisation
Le suivi des connexions et des activités des utilisateurs
La journalisation des accès, des copies et des modifications de fichiers
Le suivi du trafic, des paquets non valides ou altérés, des broadcasts, des émissions répétées
La définition des seuils d'alertes
L'observation des tendances
La détection des goulets d'étranglement
L'écoute de la satisfaction des utilisateurs
Le monitoring, le benchmarking et les analyseurs de performance des composants
Les voltmètres numériques mesurent la continuité de la tension (ohm) dans une résistance
Le réflectomètres temporels qui envoient des impulsions comme un sonar
Les oscilloscopes qui repèrent l'atténuation du signal
Les contrôleurs de câble analysent les trames et détectent les collisions
La mesure de la vitesse de propagation du signal et la longueur du câble
Les moniteurs réseaux
Les analyseurs de protocoles qui capturent et décodent les paquets

L'optimisation de l'accès (OU) aux ressources matérielles, logicielles et personnelles :

La défragmentation régulière des disques durs
La désinstallation des anciennes applications qui ne servent plus
La vérification des disques durs
La puissance et la rapidité de traitement des serveurs
Les serveurs de fichier rassemblent les données sensibles
Les serveurs d'impression regroupent les équipes
Les serveurs d'applications réseaux augmentent la productivité des personnels
La disponibilité et la compétence de l'administrateur, de son équipe (en interne et en externe)

La définition (POURQUOI) de la stratégie de sécurité et de l'intégrité des données :

La définition des règles et leur incorporation dans les contrats de travail
La définition des comportements
La définition des permissions, des droits, des privilèges, des autorisations et des habilitations
La définition des procédures de gestion, de sauvegarde, d'audit, de surveillance et d'expertise
La définition des sanctions, la faute, le licenciement, les poursuites judiciaires
La formation de tous les utilisateurs (administrateurs, techniciens, utilisateurs)
Les centres de formation et de certification agrées
Les centres de formations indépendants
Les kits d'auto formation
La formation sur le tas
L'assistance quotidienne de l'administrateur
Les services d'assistance extérieure
La documentation
Le cahier des charges rassemblant les spécifications techniques du réseau

Les plans des locaux, les schémas des câblages et des matériels, les diagrammes physiques du réseau
Les diagrammes logiques du réseau
L'emplacement des branchements (armoire de câblage, tableau de connexion)
L'emplacement des nœuds (serveurs, stations, périphériques, dispositifs de connectivité)
Les contrats, les factures, les licences d'exploitation
Le journal de bord du réseau, écrit sur papier
Le journal de bord consignant l'historique des problèmes, des symptômes et des solutions
Les consignes, les procédures, les «check-lists»
Les journaux des évènements, les statistiques des performances «normales» du réseau
Les ressources des éditeurs
Les bases de connaissance
Les ressources d'internet
Les disquettes de tous les pilotes
Les CD-ROM de tous les logiciels et une copie de sauvegarde
L'identification des personnes responsables ou compétentes
La liste et le numéro de téléphone des personnes pouvant aider l'administrateur
La liste des collaborateurs, des services d'assistance, des consultants
La liste des distributeurs, des fournisseurs, des constructeurs, des éditeurs

MAINTAIN

Le rôle de l'administrateur

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 connaitre 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 une réelle compétence. Les **responsabilités** de l'administrateur sont très importantes et se placent dans la durée et dans le risque. Les tâches de l'administrateur et de ses collaborateurs évoluent en fonction de son environnement. Et l'environnement évolue très rapidement et dans le sens de la **complexité**, que ce soit l'évolution des besoins, des contraintes et des risques, ou que ce soit l'évolution de la taille des réseaux, du nombre de ses nœuds, du temps de connexion et de la bande passante, ou que ce soit l'évolution des technologies, des produits et des fonctionnalités.

Le rôle de l'administrateur réseau s'inscrit dans une réflexion stratégique et organisationnelle.

Le dépannage à chaud

Le dépannage à chaud peut survenir à n'importe quel moment, d'où les **astreintes** des personnels d'administration. Un utilisateur appèle l'administrateur, une **alerte** se déclenche brusquement, un bruit de **crash** offusque soudainement les tympans, les conditions sont multiples et ne peuvent pas être connues à l'avance.

Une approche structurée (**méthodologique**) est en moyenne bien plus efficace qu'une approche aléatoire. En gardant à l'esprit la priorité ou l'objectif principal du système d'information, il faut être capable d'évaluer **l'impact**, **l'urgence**, les **risques** et la **durée** de la panne.

Ici aussi, la collecte d'informations est cruciale et va déterminer la suite des évènements. L'interview de l'utilisateur, avec des **questions simples**, appelant des **réponses claires** (oui ou non) permettent d'évaluer objectivement la situation.

Il faut essayer d'identifier la **cause**, les **symptômes**, les **effets** de la panne. Il faut déterminer s'il y a eu des **changements** dernièrement ou un évènement **déclencheur**, si une manipulation malencontreuse s'est produite, si quelqu'un a déjà essayé de réparer le problème, s'il est possible de circonscrire la panne à un petit segment ou s'il existe un risque de généralisation, si la panne est du coté **système** ou du coté **réseau**, si le trafic du réseau est normal ou s'il est saturé, si les serveurs fonctionnent après une coupure de courant, si une machine à café (ou un générateur électromagnétique) a été récemment installée près du réseau, si les **dates** des fichiers systèmes ont changées et si une **activité** intrusive est à craindre.

Il faut établir la liste des causes possibles de la plus probable à la moins plausible, et tester chacune d'entre elle. Les **tests** consistent à remplacer les composants ou les matériels avec d'autres composants dont on est sûr qu'ils fonctionnent correctement. Il faut savoir **segmenter** le réseau pour circonscrire les dysfonctionnements, mettre en place une solution et vérifier si la **solution** résout le problème, pourquoi et comment. Il ne faut pas hésiter à demander de l'aide extérieure tout en restant le plus **discret** possible et éviter les **fuites**, la **panique** et les **rumeurs**.

La dégradation des performances peut provenir d'une mauvaise configuration d'un protocole. Par exemple, certains 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 et s'assurer qu'il n'y en ait pas d'autres. Les câbles et les **branchements** sont les deux premières choses que vérifient les spécialistes (d'où l'utilité d'un réflectomètre).

La stratégie de sauvegarde

La sauvegarde est l'ultime ressource d'un système d'information. La stratégie de sauvegarde doit être adaptée au réseau, aux utilisateurs, aux données, mais 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 effectué au moins une sauvegarde complète en début de cycle.

Les bandes de **roulement** sont les 4 bandes pour les 4 jours normaux de la semaine (lundi, mardi, mercredi et jeudi). Ces bandes sont utilisées pour effectuer une sauvegarde **différentielle**, tous les jours, en fin de journée par exemple. Ce sont les bandes «**fils**». Les bandes **complètes** sont les 4 bandes pour les 4 derniers jours de la fin de semaine (vendredi) de chaque mois. Elles sont dénommées vendredi 1, vendredi 2, vendredi 3 et vendredi 4. Ces bandes sont utilisées pour effectuer une sauvegarde complète en fin de semaine. Ce sont les bandes «**pères**». Les bandes **d'archivage** sont les 12 bandes pour les 12 mois de l'année. La bande du dernier vendredi du mois est stockée et prend le nom du mois. Ce sont les bandes «**grands-pères**». 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 éventuelle, c'est-à-dire, la date, le type de support, le logiciel de sauvegarde, le nom de l'opérateur et le nom de la procédure de restauration.

Les sources de pannes

Les sources des pannes	
Cable	L'alimentation électrique (**power**)
	Les supports de communication (**lines**)
	Les connecteurs (**connector**)
Network	Les dispositifs de connectivité (**router**)
	Les cartes réseaux (**interface**)
	Les protocoles (**protocols**)
Computer	La mémoire (**memory**)
	Le disque (**disk**)
	La carte graphique (**video**)
System	Les pilotes (**driver**)
	Les services (**daemon**)
	Les mises à jour de sécurité (**patch**)
Software	Les applications clientes (**client**)
	Les applications serveurs (**server**)
People	Les utilisateurs (**user**)
	Les administrateurs (**root**)
	Les fournisseurs (**contractor**)
	Les organismes (**regulation**)
	Les experts (**hackers**)
	Les pirates (**crackers**)

SYSTEM

Les systèmes d'exploitation

Le système d'exploitation est un logiciel qui fait **l'interface** entre l'utilisateur et l'ordinateur. C'est le système qui gère les applications, les calculs du processeur, l'enregistrement des données et leur affichage sur un écran. Il existe des systèmes qui ne fonctionnent que sur un certain type de **matériel** et d'autres qui sont conçus pour fonctionner en réseau, en échangeant des **données** et en communiquant avec d'autres ordinateurs.

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. La gestion des ressources comprend la gestion de la mémoire vive de l'ordinateur, le chargement et l'exécution des applications, l'allocation du temps processeur ou **CPU** (Central Processing Unit) aux différents processus, la gestion des lectures et des écritures sur l'espace de stockage du disque (la mémoire de masse non volatile), la gestion des périphériques, des ports, ou des interruptions systèmes ou **IRQ** (Interruption Request).

Les systèmes d'exploitation réseaux

Les systèmes d'exploitation réseaux sont conçus pour fonctionner et **interagir** avec d'autres ordinateurs en réseau. Par exemple, une station **cliente** peut faire appèle aux services d'une station **serveur**. Les deux stations sont équipées toutes les deux d'un système d'exploitation réseau. Le système d'exploitation réseau peut être le même, pour le client et pour le serveur, ou peut être différent. L'important est que les deux stations puissent communiquer ensemble, et pour cela, elles ont toutes les deux besoins d'avoir le même **protocole** de communication.

Les machines **serveurs** disposent d'un système d'exploitation réseau et d'applications qui permettent de satisfaire les demandes de service qui leur sont adressées par d'autres machines du réseau. Ces autres machines disposent également d'un système d'exploitation réseau, mais leurs applications sont les **clientes** des applications des serveurs.

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. Les **requêtes** réseaux étaient redirigées vers le logiciels réseau. Le logiciel réseau et le système d'exploitation devaient être bien sûr compatibles. Le système s'occupait de gérer les ressources internes de l'ordinateur (en mode autonome) et le logiciel réseau s'occupait de l'accès aux ressources externes de l'ordinateur (en mode réseau).

Le système Unix™ est le premier véritable système d'exploitation réseaux **multi tâches**. Il a été conçu à la fin des années 1960, sous le nom de **Multix**, pour dans les laboratoires de la société américaine

Bell AT&T. Le système d'exploitation **NetWare** de la société Novell, dirigé par son fondateur Ray Noorda, est le premier système d'exploitation réseau «grand public» et fut disponible dès les années 1980.

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 (**instructions**), et le processeur exécute ces petits morceaux les uns après les autres, en répartissant sont temps de manière équitable entre toutes les tâches qui lui sont demandées.

En fait, un véritable système d'exploitation multitâche peut exécuter simultanément autant de tâches qu'il y a de processeur, en parallèle. 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 simultanément, alors le système d'exploitation multitâche répartie le temps du ou des processeurs. Les tâches sont traitées à tour de rôle, pendant une durée, ou plus exactement, pendant un certain nombre de **cycle** d'horloge, déterminé 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 fréquence élevée, et plus il donne l'impression d'être «une machine orchestre» qui joue de plusieurs instruments à la fois.

Les modes de fonctionnement multitâche

Il existe deux modes de fonctionnement multitâche, le mode préemptif et 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. Le système Gnu Linux est un véritable système multi tâches, multi utilisateurs et multi processeurs, avec une pile de protocole TCP/IP intégrée dans le noyau.

Le modèle client serveur

Un réseau est composé d'au moins deux ordinateurs, avec un serveur et un client, dans une organisation de type client serveur. Les deux ordinateurs peuvent être à la fois, et chacun leur tour, un client et un

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.

Les architectures processeurs

Il existe plusieurs types de processeurs. Chaque type de processeur caractérise la carte mère sur laquelle il est installé. L'on dit qu'il existe plusieurs types de **plates-formes** ou d'architecture. Un système d'exploitation est conçu pour fonctionner avec un certain type de processeur. Les systèmes Gnu Linux proposent des **noyaux compilés** pour tel ou tel type d'architecture, tandis que les systèmes propriétaires, comme Windows™ et Macintosh™ ont été conçus historiquement pour ne fonctionner qu'avec un seul type d'architecture.

Les machines Intel sont équipées de processeur Intel et la plus part des systèmes d'exploitation sont compatibles avec leur architecture parce qu'elle représente la part de marché la plus importante dans le monde.

Les systèmes réseaux

Il existe plusieurs systèmes d'exploitation réseaux ou **NOS** (Network Operating System). L'on distingue, les systèmes propriétaires et les systèmes libres. Les systèmes propriétaires sont développés par des sociétés commerciales dont le but est de faire du profit, et les systèmes libres sont développés par les communautés de Logiciels Libres sur internet.

Parmi les systèmes **propriétaires** se retrouvent les systèmes qui dérivent d'Unix™ d'AT&T, comme Solaris de Sun, et les autres systèmes d'exploitation propriétaires des sociétés IBM (OS/2), Novell (NetWare™), Microsoft (Windows™) ou Apple (Macintosh™).

Parmi les systèmes **libres** se retrouvent les systèmes **BSD** (Berkeley Software Development) et les systèmes Gnu Linux qui sont des systèmes réseaux, sécurisés, libres, ouverts, universels et gratuits.

Le système Unix™ AT&T

Le système Unix™ est le premier des systèmes d'exploitation réseaux multi tâches. Il a été conçu à la fin des années 1960, sous le nom de **Multix**, dans les laboratoires de la société américaine Bell AT&T. Multix était lent, lourd et technocratique comme le cahier des charges dont il était issu. Aussi, les programmeurs de Bell AT&T entreprirent de construire volontairement un autre système d'exploitation, rapide, léger et extensible, et les utilisateurs étaient encouragés à modifier le système en fonction de leurs besoins. Le nouveau système fut développé librement en parallèle, et les utilisateurs le nommèrent **Unix**™ par dérision. L'avantage du système Unix™ était qu'il pouvait fonctionner sur de petits ordinateurs, moins puissants et moins couteux que les VM d'IBM et les VMS de Digital, c'est pourquoi il fut adopté par les universités. La société Bell AT&T diffusa auprès des universités des copies très bon marché de son système Unix™.

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&T par Brian kernighan et Denis Ritchie. Les distributions d'Unix™ AT&T incluaient le code **source** du système d'exploitation, lequel pouvait être re compilé 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 exécutable par le processeur. Il existe des compilateurs C pour tous les types d'architecture processeurs, comme les PC Intel.

Les systèmes BSD

Au milieu des années 1970, Ken Thompson et Bill Joy de l'université de Berkeley en Californie écrivirent un éditeur appelé «vi» (**visual**) qu'ils proposèrent d'inclure librement avec le système d'exploitation Unix™ modifié et adapté par les étudiants de l'université. Ils baptisèrent leur système Unix™ BSD en adjoignant au nom original, l'acronyme **BSD** (Berkeley Software Distribution). Aujourd'hui, toutes les versions propriétaires d'Unix™ et toutes les versions libres des systèmes BSD proviennent de ces deux sources, l'Unix™ Système V de la société AT&T et l'Unix™ BSD 4.2 de l'université de Berkeley. Avec le temps, les distributions provenant de ces deux sources se différencièrent de plus en plus, jusqu'à devenir incompatibles entre elles.

Les versions d'Unix™ vendu 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 propriétaires d'Unix™ ne tournent pas 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™.

Les systèmes Unices

Au début des années 1990, la société **AT&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 du fait de ces endettements 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 **SCO** (Santa Cruz Operation) qui était la propriété de Microsoft. 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 «**auto suffisant**», 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™ n'est plus uniquement

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

Plusieurs éditeurs en commercialisent des versions plus ou moins différentes. Le système **Solaris** appartient à la société Sun Microsystems qui a libéré son code source pour les architectures Intel. Le système Unix™ SCO puis Unix™ Ware de la société Santa Cruz Operation n'a jamais vraiment été exploité commercialement. Le système **AIX** est maintenu par la société IBM. Le système **ULTRIX** était le système vendu avec les machines de la société DEC. Le système **HP-UX** est le système commercialisé par la société Hewlett Packard.

L'incompatibilité binaire des Unices

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, et l'administration d'un système propriétaire est un monde en soi, les applications et les utilitaires ne sont pas portables. Il n'existe pas de véritable standard d'Unix™, et le meilleur système d'exploitation au monde reste accessible uniquement sous des versions **propriétaires**. Les éditeurs des Unix™ propriétaires 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 à des professionnels très spécialisés de l'industrie informatique.

Le système Gnu Linux

Le système Gnu Linux, initié en 1990 par le finlandais Linus Torvald, est à contrario est un système portable, modulaire et très performant. C'est de plus un logiciel libre qui est construit bénévolement par les meilleurs professionnels mondiaux de l'industrie informatique. Le système Gnu Linux donne une image plus **démocratique** du système d'exploitation, et défend la stratégie de la transparence en permettant d'étudier et d'adapter le code source. Le système Gnu Linux est distribué sous la licence Gnu **GPL** (General Public Licence) qui garantie l'accès au code source et protège les intérêts des utilisateurs.

L'architecture des systèmes Unices

En fait, il n'existe pas de système Unix™ mais plutôt de nombreux systèmes Unices propriétaires ou libres. En réalité, les systèmes "Unices" sont des systèmes "Multices". L'on parle de systèmes Unices en général pour désigner l'architecture multi tâches des systèmes Unix™ propriétaires et des systèmes libres, comme FreeBSD, NetBSD, OpenBSD et Gnu Linux.

Les systèmes d'exploitation Unices sont constitués d'un ensemble de modules. Chaque **module** est un programme spécialisé, indépendant des autres, mais compatibles avec les autres modules. Les différents modules sont sélectionnés par l'administrateur lors de la compilation du système d'exploitation et sont

intégrés pour former le noyau du système. Ainsi chaque noyau est différent d'un autre, et chaque système Unice peut être spécialisé et optimisé pour la réalisation d'une tâche très précise. Il existe des noyaux très petits dits **embarqués** (embedded).

Les systèmes Unices sont des systèmes d'exploitation multi tâches **préemptif**, c'est à dire qu'ils sont capables de traiter les processus de différents programmes en même temps, dans un espace mémoire réservé qui protège chaque programme de ces congénères. Les systèmes Unices sont également des systèmes d'exploitation multi fonctions, c'est à dire qu'ils peuvent servir à réaliser presque toutes les tâches dévolues au monde binaire. Ils peuvent fonctionner aussi bien en tant que serveur, qu'en tant que client, et peuvent être implémentés à n'importe quel niveau de l'entreprise. Les serveurs Unices **centralisés** peuvent traiter les requêtes de nombreux **terminaux**. Par exemple, les terminaux VT100 de Digital sont reliés au serveur central par l'intermédiaire d'un port série, et ils permettent d'envoyer des commandes au serveur et d'afficher les résultats sur l'écran. Les systèmes Unices peuvent prendre en charge, aussi bien les systèmes **transactionnels**, que les architectures **distribuées**.

Les systèmes Unices sont des systèmes d'exploitation **multi plate formes**, c'est à dire qu'ils sont disponibles pratiquement sur toutes les plates formes matérielles, particulièrement en ce qui concerne le système NetBSD. Les systèmes Unices sont des systèmes d'exploitation **multi processeurs**, c'est à dire qu'ils peuvent fonctionner avec plusieurs processeurs en même temps, lesquels se répartissent en temps réel la charge de travail. Les systèmes Unices sont des systèmes d'exploitation **multi protocoles**, c'est à dire qu'ils peuvent véhiculer les communications réseaux avec de nombreux protocoles différents. Les systèmes Unices supportent le protocole SPX/IPX pour interagir avec les réseaux NetWare, ou le protocole SMB pour interagir avec les réseaux Windows™. Le protocole TCP/IP, qui permet d'interagir avec internet, est le protocole naturel des systèmes Unices. TCP/IP est intégré «nativement» aux systèmes Unices. Les systèmes Unices sont des systèmes d'exploitation **multi utilisateurs**, c'est à dire que de nombreux utilisateurs peuvent se connecter simultanément au même serveur.

Les systèmes Unices sont compatibles avec la plus part des systèmes de fichiers locaux ou distants, comme **NFS** (Network File System) de Sun qui permet de «monter» des disques sur un ordinateur distant, comme **AFS** (Andrew File system) ou **DFS** (Distributed File System) ou encore **SMB** (Server Message Block) qui permet de partager les ressources d'un ordinateur Windows™.

Les langages de script permettent de réaliser des tâches très complexes. Le commutateur de redirection appelé «**pipe**» en anglais ou «**tube**» en français («|») permet de transmettre des données d'un programme à un autre. Les «**scripts shell**» correspondent aux fichiers «**batch**» de Microsoft.

Les systèmes Unices disposent d'une panoplie de langages de scripts, dont les scripts **PERL** (Pratical Extraction and Reporting Language) qui permet de récupérer les données saisies dans une page Web, ou **TCL/TK** ou **PHP**.

Les systèmes Unices organisent les fichiers **hiérarchiquement** avec comme séparateur de répertoire le slash («/») penché à droite, et non pas l'anti-slash («\») qui est utilisé sur les systèmes de Microsoft.

Chaque répertoire peut avoir des **restrictions** d'accès particulières. Le système de fichier des systèmes Unices supporte les espaces disques très volumineux (Tera Octets), les **noms** de fichiers allant de 14 à 32 ou à 255 caractères selon les versions, garantie l'unicité des noms de fichier, et 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 Unice dépend des distributions, mais en général l'on retrouve la **racine** ("/") qui représente le départ ou le sommet de la **hiérarchie** et qui n'est accessible que par l'utilisateur «**root**» qui est l'administrateur ou le super utilisateur, et l'on retrouve le répertoire ("/dev") pour l'identification des matériels (**device**), le répertoire ("/bin") réservé aux exécutables binaires (**binary**), le répertoire (/etc) qui contient les fichiers de configuration (**text**), le répertoire ("/var") pour les fichiers à taille aléatoire (**variable**) et le répertoire ("/pub") qui est ouvert à tous (**public**).

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

Le système d'exploitation réseau NetWare

Le système 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 propriétaires **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, les trames Ethernet 802.2 et les trames 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 d'organiser et de conserver la trace de toutes les ressources du réseau. NetWare 4 permet de dupliquer les données en temps réel. NetWare s'appèle de nos jours «IntranetWare».

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. Netware 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 ou **CNE** (Certified Novell Engineers) très compétents, 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 postes 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, à l'achat du système d'exploitation pour le serveur, mais auquel il faut ajouter le prix de toutes les licences pour chaque poste client supplémentaire, ou le prix d'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 meilleures performances pour certains services, comme les serveurs de fichiers et d'imprimante, le partage de fichier et d'imprimante, ou les services de répertoire d'annuaire (NDS) qui permettent l'administration d'un nombre important d'utilisateurs 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 la gestion de l'Active Directory™. NetWare supporte les grandes partitions, les noms longs de fichiers avec de nombreux attributs. NetWare conserve en mémoire une liste de tous les fichiers stockés sur le disque afin d'y accéder plus rapidement.

Le système Windows™ NT

Le système 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 de 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. Le système 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 client serveur pour laquelle il est conçu. La conception de la société Microsoft de ses utilisateurs est une conception **paternaliste**, la phrase "works as designed", qui signifie, cela fonctionne pour ce pourquoi c'est conçu, montre la **culpabilité** qui est projetée inconsciemment sur les utilisateurs qui rencontrent une difficulté de configuration. La société Microsoft a multiplié les versions pour faire croitre son chiffre d'affaire et provoquer indirectement des

incompatibilités internes qui poussaient les administrateurs à acheter les nouvelles versions.

Le système 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. Le système Windows™ 2000 (Windows™ NT 5.0) inclus «**Active Directory**» qui est le service d'annuaire qui manquait, comparé au système de Netware™. Windows™ NT Server fut construit, dit on, à partir d'une feuille blanche. Le système dispose ainsi de beaucoup d'option, comme par exemple trois systèmes de fichiers compatibles.

Le système de fichier **FAT** (File Allocation Table) ou FAT 16 est l'héritage de MS-DOS et impose la règle de nommage des 8.3. Le système de fichiers **HPFS** (High Performance File System) est le système de fichier d'OS/2 d'IBM, qui est présent dans la version Windows™ NT 3.5, il a été retiré dans la version Windows™ NT 4.0. Le système de fichiers **NTFS** (NT File system) est le système de fichier propre à Windows™ NT, et supporte les noms longs de fichiers (jusqu'à 254 caractères). Tous les systèmes d'exploitation de Microsoft fonctionnent 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 cœur de NetWare™.

Windows™ NT Server fonctionne autour de la notion de «**domaine**», à ne pas confondre avec les domaines DNS d'internet, comme les septs Top Level Domain (TLD) que sont «.com», «.mil», «.gov». Un domaine est un groupe d'ordinateur qui appartiennent à la même entité logique. Dans un domaine, un ordinateur central, appelé **CPD** (Contrôleur Principal de Domaine) authentifie toutes les connexions au domaine. Un réseau peut être constitué de plusieurs domaines qui peuvent, deux à deux, éventuellement entretenir des relations d'approbation, lesquelles ne sont pas transitives et ne sont pas implicites. L'organisation des domaines peut suivre plusieurs structures (le domaine unique, le domaine maitre, le domaine à maitres multiples, les domaines à relation d'approbation multiple).

Le modèle d'approbation de domaine n'est pas aussi extensible que les autres modèles du marché. C'est pourquoi, Windows™ 2000 apporte cette fonctionnalité avec Active Directory. Le modèle d'annuaire NDS de Netware™ ou le standard ouvert **LDPA** (Lightweight Directory Access Protocol) qui fait partie de la pile de protocole TCP/IP sont des modèles d'annuaire qui inventorient toutes les ressources du système d'information et qui constituent une base de données hiérarchique.

Les ordinateurs clients à l'intérieur d'un domaine sont en théorie limités à 40 000. Les clients d'un domaine Windows™ peuvent être des clients Windows™ for Workgroups, Windows™ 95&98, Windows™ NT Station, ou des clients Netware™ ou des clients Macintosh™, ou des clients Unix™. Les comptes utilisateurs peuvent être placés dans des groupes locaux ou globaux. Les permissions d'accès à une ressource sont gérées avec Windows™ NT Server au niveau du fichier sous NTFS, et non plus 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 Protégé avec un 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 adresses IP dynamiques, le serveur RAS pour les connexions distantes avec le protocole PPP). Windows™ NT Server peut être accompagné de la suite de logiciels, appelée «Back Office», qu'a développé Microsoft et qui contient les produits Exchange Server qui gère la messagerie interne, SQL Server qui gère les bases de données, SMS qui rassemble plusieurs logiciels qui permet de centraliser l'administration du réseau, SNA Server qui gère les connexions à des mini ordinateurs ou à des main frames IBM et IIS qui peut servir de serveur internet pour les services web, Gopher, FTP.

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, la société Microsoft a rompu son partenariat avec la société 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. Par exemple, les connexions différenciées ou l'utilisation de plusieurs logon en même temps, c'est à dire qu'il est possible d'ouvrir plusieurs sessions complètement séparées les unes des autres sur le même ordinateur.

Le système 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 préférés se concentrer sur le leader du marché des systèmes d'exploitation (Windows™) pour développer des logiciels compatibles avec cette plate forme.

SECURITY

La sécurité

La sécurité ne doit pas être une obsession. Le niveau de sécurité optimal doit dépendre de la taille du réseau et de la sensibilité des activités. La meilleure sécurité, c'est de n'avoir rien à cacher, rien à voler et de rester poli s'il vous plait ;-).

Pourtant, certaines mesures de sécurité sont parfois indispensables pour assurer de bonnes conditions d'utilisation des **ressources**. La sécurisation est une question de politesse et de **discipline**. La sécurité est bien souvent un prétexte pour limiter les droits des utilisateurs. Les principes de la sécurité reposent sur des stratégies guerrières ou des **stratagèmes** militaires (leurrer, séparer, copier, cacher, renforcer, surveiller, filtrer, prévoir, attendre, dissuader, négocier, espérer). Il n'y a pas de **règles** d'or en matière de sécurité de la sécurité.

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. Toutes les données peuvent être manipulées, orientées, instrumentalisées. La stratégie de sécurité d'un réseau doit se situer à trois niveaux. L'intégrité des **données** permet de conserver intacte les données (fichier ou binaire). La conformité des **opérations** effectuées sur le réseau permet de s'assurer du type d'activité pratiquées par les utilisateurs autorisés. La régularité du fonctionnement des **équipements** permet de vérifier si les matériels sont en état opérationnel et sous contrôle.

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

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. L'environnement peut être scindé en deux parties distinctes, l'environnement intérieur et l'environnement extérieur. L'environnement **intérieur** est constitué des matériels, des logiciels, des systèmes et des utilisateurs. L'environnement **extérieur** est constitué des partenaires, des concurrents, des malveillants et des services des états nationaux.

Les failles potentielles

Les failles potentielles d'un réseau sont nombreuses. Tout peut être suspecté, en général, c'est ce qui n'a

pas été prévu qui se révèle être une faille. L'accès aux **données** peut être crucial pour une entreprise, la panne du matériel, le dysfonctionnement d'un logiciel, la saturation du réseau, le vol des données peuvent être préjudiciables aux intérêts de l'entreprise. L'écoute du support de communication, l'accès non autorisé, la découverte d'un mot de passe, la **connexion** au réseau, l'accès aux ressources du réseau, le téléchargement d'information (depuis l'intérieur de l'entreprise ou depuis l'extérieur), la destruction des données (accidentelle ou intentionnelle) peuvent ne paralyser que temporairement une entreprise qui possède un jeu de sauvegarde valide, ou remettre en cause sa pérennité, quand elle ne peut reconstituer la matière première, l'information, de ses activités.

Il faut prendre en considération le **temps** nécessaire pour rétablir le réseau dans son état antérieur. Les dommages physiques, la perte d'un jeu de sauvegarde, le crash d'un disque dur, l'incendie, la **catastrophe** naturelle, l'arrêt ou la dégradation (surtension) de l'alimentation électrique peuvent provoquer la perte des données en cours, celle qui sont stockées en mémoire vive.

Les dommages **intentionnels**, l'attaque d'un virus, la falsification des données, la vengeance d'un employé remercié, l'attaque concurrentielle, l'attaque idéologique, l'attaque de représailles sont autant de failles potentielles qui dépendent du **comportement** de l'entreprise et des **relations** qu'elle entretient avec son environnement.

La stratégie de sécurité

Il peut être plus couteux 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 misent à la disposition d'un administrateur réseau pour protéger son environnement informatique sont de trois ordres. L'administrateur peut envisager la prévention (**avant**), la surveillance (**pendant**) et la dissuasion (**après**). La sécurité peut être envisagé selon son objet qui peut être matériel (**hardware**), logiciel (**software**), relationnel (**middleware**) ou personnel (**peopleware**).

Nous ne parlerons pas de «l'ordre répressif», ni des méthodes de **pressions** psychologiques ou de harcèlement qui poussent à l'auto censure, à la soumission, au silence, et à l'acceptation de contraintes et de privation des libertés fondamentales. La sécurité est un **ensemble** de différentes méthodes qui 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, et la stratégie des mots de passe et des **permissions** est considéré comme l'étape suivante. Ensuite viennent les contrôles des **trames**.

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, en **concertation**, et correspond à une volonté déterminée. 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.

La stratégie de sécurité	
Prevention	Le contrôle des utilisateurs (**user**) Le partage protégé par le mot de passe au niveau des ressources (**share**) Les permissions d'accès au niveau des utilisateurs (**password**) L'intégrité des données (**data**) La disponibilité du réseau (**broadband**) Les sauvegardes sur bande (**backup**) Les systèmes de tolérances de panne (**raid**) La confidentialité et le cryptage des données (**crypt**) La protection contre les logiciels malveillants ou d'espionnage et (**virus**) Le contrôle des matériels (**hardware**) L'alimentation électrique de secours, les batteries et les onduleurs (**power**) La protection physique des équipements sous clefs (**room**)
Alert	La surveillance des performances (**monitoring**) La surveillance des activités réseaux (**filtering**) L'audit externe et la veille technologique (**benchmarking**)
Dissuasion	Les clauses contractuelles de non divulgation et de discrétion (**clearance**) L'enregistrement des preuves (**logging**) Les contres mesures et défenses juridiques (**prodedures**)

Le contrôle des utilisateurs

Le contrôle des utilisateurs permet de filtrer les connexions et de règlementer l'activité et l'environnement des utilisateurs. **L'authentification** des utilisateurs par des mots de passe permet de vérifier l'identité d'un utilisateur. Les profils utilisateurs, le chargement d'une configuration réduite, la personnalisation des ouvertures de **session**, la limitation des logiciels installés localement et la formation des utilisateurs permet de réduire les risques potentiels.

Les firewalls permettent de filtrer les connexions extérieures tout en permettant l'accès des utilisateurs nomades. Les routeurs permettent de canaliser les **communications** à certains segments de sous réseaux.

L'authentification des utilisateurs

Lors de la connexion d'un utilisateur au réseau, une procédure d'authentification vérifie le nom de l'utilisateur (**login**) et son mot de passe (**password**). Quand l'authentification réussie, c'est qu'il y a concordance entre le compte et le mot de passe. L'utilisateur peut alors accéder à toutes les ressources dont il possède les permissions (directement ou par l'intermédiaire de l'appartenance à un groupe).

Les différentes permissions d'accès à une ressource sont la consultation (**read**), la transformation

(**write**) et l'exécution (**execute**). Les permissions peuvent être associées à un compte utilisateur ou à un groupe. Les utilisateurs qui appartiennent au groupe possède par **transitivité** les permissions du groupe.

La configuration des utilisateurs

Les logiciels de gestion des configurations sont des logiciels qui permettent de gérer à partir d'une interface **centrale** la configuration logicielle et l'interface 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 l'interface 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.

Le contrôle des données

Le contrôle des données concerne la gestion automatique des **sauvegardes**, l'installation de systèmes de **tolérances** de panne qui assurent que les données sont toujours accessibles malgré une défaillance d'un disque dur, comme les systèmes RAID, le **cryptage** des données stockées ou des données transmises sur le réseau et la protection contre les **virus**.

Les données sont généralement considérées comme perdues quand elles ne sont plus accessibles. Toutefois, un fichier effacé, ne signifie pas qu'il n'existe plus de trace sur le disque dur. Souvent, c'est simplement le numéro d'inode du fichier qui a été libéré dans le système de fichiers (**inode**). Des programmes sophistiqués permettent la récupération des données (**recovery**), et parfois même de lire les cellules d'un disque dur après une réécriture. D'autres programmes permettent de s'assurer qu'un fichier est bien effacé, en écrivant plusieurs fois des bits aléatoires sur les cellules du disque (**shred**).

Les sauvegardes

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, comme les **délais** pour reconstituer les données, la **fréquence** des sauvegardes (plusieurs fois par jour, quotidienne, hebdomadaire, mensuel), le **volume** de données a sauvegarder (un disque dur entier ou seulement les fichiers vitaux), la **vitesse** de transfert des données des supports de stockage et des supports de communication (le trafic réseau explose pendant une sauvegarde).

Si le lecteur de bande est branché sur un serveur de fichier, alors les données ne transitent pas par le réseau et l'opération de sauvegarde est plus rapide. Si les serveurs de fichiers possèdent deux cartes réseaux, l'une pour la partie «utilisateurs», et l'autre pour la partie «sauvegarde», alors le **trafic** généré par l'ordinateur de sauvegarde situé sur le segment «sauvegarde» n'encombre pas le segment «utilisateur» puisqu'il est séparé.

Le travail de sauvegarde est plus rapide quand le réseau n'est pas utilisé par les utilisateurs, la nuit ou en fin de journée par exemple. Plusieurs copies de même sauvegarde permet d'en garder une qui reste sur place et une autre qui est rangé dans une **armoire** ignifugée dans un autre bâtiment par exemple. Le travail de sauvegarde et de restauration sont plus faciles, plus surs et plus rapides quand toutes les données à sauvegarder sont regroupées sur un même **serveur** de fichier. Selon le nombre et la capacité des bandes disponibles, le **cycle** de sauvegarde peut s'étaler sur une **période** plus ou moins longue. Il est parfois prudent de disposer de plusieurs **jeux** de sauvegarde à un moment donné, celui d'hier et celui de la semaine précédente par exemple.

Les types de sauvegarde

Il faut distinguer la copie simple de la véritable sauvegarde qui permet de marquer les fichiers sauvegardés (à l'aide d'un **attribut**) afin de pouvoir ultérieurement déterminer (lors d'une nouvelle sauvegarde) s'ils ont été modifiés (par rapport à la précédente sauvegarde). Ainsi, les sauvegardes peuvent être **complètes** (en enregistrant l'intégralité des données d'un support), **incrémentielles** (en marquant les fichiers modifiés depuis la précédente sauvegarde) et **différentielles** (en ne sauvegardant que les fichiers qui ont été modifiés depuis la précédente sauvegarde). La régularité des tests de restauration constitue le seul moyen d'être sûr que les jeux de sauvegarde sont fiables.

Le journal des sauvegardes

La tenue d'un **journal** de sauvegarde sur papier permet de savoir tout de suite le contenu d'une sauvegarde. Les informations à mettre en évidence sont la date, l'auteur, le lieu de stockage des bandes, les numéros des bandes, le type de sauvegarde, et le descriptif des serveurs, des répertoires et des fichiers sauvegardés.

Les types de bandes

Il existe différents types d'unité de **bandes**. Les bandes numériques audio de 4 mm ou **DAT** (Digital Tape Audio) 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 plus parts 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.

La tolérance de panne

Les systèmes de tolérance 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 peuvent être logiciels ou matériels.

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» (**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 choisir 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. Toutefois, seule la sauvegarde permet de récupérer des données quand 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 ou **ECC** (Error Code Correction), c'est donc un facteur de tolérance de panne.

Les disques constituant un agrégat peuvent être de types différents, des disques IDE, ESDI, ou SCSI. La neutralisation des secteurs défectueux des disques (**Sector Sparing**) ou le dépannage à chaud (**Hot**

Fixing) sont des fonctionnalités des systèmes RAID. C'est le pilote de tolérance de panne qui lors de l'opération Entrée/Sortie déplace les blocs de données vers des secteurs en parfait état. Les périphériques 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 ne doit pas remplacer la sauvegarde régulière!

Les agrégats par bandes

Le système **RAID** (Redundant Array of Inexpensive Disk) classe les agrégats en différentes catégories, mais toutes les catégories n'offrent pas la tolérance de panne.

Le RAID 0 est un 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.

Le RAID 1 est un miroitage 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, mais fiable. La duplication de disque (**Duplexing**) est un miroitage de disque où le deuxième disque dispose de son propre contrôleur RAID.

Le RAID 2 est un 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.

Le RAID 3 est un agrégat par bandes avec contrôle de **parité**. Les données proprement dites utilisent 85% de l'espace de l'agrégat.

Le RAID 4 est un agrégat par bandes avec grands **blocs** (Agrégat de Volume). Les données sont réparties au fur et à mesure sur tous les disques de l'agrégat. Il n'y a pas d'entrelacement des données. L'écriture des blocs 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.

Le RAID 5 est un 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 associées 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.

Le RAID 10 est un agrégat en miroir. Il y a deux agrégats identiques de type RAID 0. C'est un miroitage d'agrégat.

Les caractéristiques des systèmes RAID							
RAID	**0**	**1**	**2**	**3**	**4**	**5**	**10**
Nombre de disques	1 à 32	2	1 à 32	1 à 32	1 à 32	3 à 32	6 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	

Le cryptage des données

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, c'est à dire quand les données peuvent être utilisées contre les intérêts de l'entreprise.

Le cryptages s'effectue à l'aide d'algorithmes de cryptage qui rendent incompréhensible les données sans une clef pour décoder les documents cryptés. Certains algorithmes de cryptage peuvent être classés «**secret défense**». Les systèmes de cryptage peuvent être logiciels ou matériels. Les systèmes de cryptage matériel sont onéreux.

Les systèmes de cryptage sont soit **symétriques**, soit asymétriques. Les systèmes de cryptage symétrique sont basés sur une clef unique, et il requiert un échange de clés confidentielles. L'on dit qu'ils sont symétriques parce que c'est la même clef qui effectue le cryptage et le décryptage. La norme **DES** (Data Encryption Standard) et la norme **CCEP** (Commercial COMSEC Endorsement Program) sont des normes américaines introduites par la **NSA** (National Security Agency) pour autoriser les entreprises privées à utiliser le cryptage de leurs données.

Les systèmes de cryptage **asymétriques** sont basés sur deux clefs, l'une est appelée la clef publique, elle est distribuée à tout le monde, et elle permet le cryptage, et l'autre est appelée la clef privée, elle est

gardée confidentiellement par une personne, et elle permet le décryptage des données cryptées avec la clef publique. Les deux clefs sont générées en même temps, par la factorisation de deux nombres premiers. La clef publique est ainsi liée à la clef privée, et la clef privée ne peut décrypter que les messages qui ont été cryptés avec la clef publique associée.

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 ou la **signature** d'un virus est en perpétuelle évolution. C'est pourquoi, il ne suffit pas d'avoir un logiciel **antivirus** installé sur les ordinateurs.

Il faut continuellement tenir à jour sa base de données des virus connus.

L'alimentation électrique

L'alimentation électrique de secours ou **UPS** (Uninterruptible Power Supply) permet d'alimenter un ou plusieurs ordinateurs, en cas de panne du secteur, et de réguler la tension électrique (**ondulator**). L'UPS peut fonctionner avec une batterie, un moteur rotatif, ou un groupe électrogène. Les durées d'autonomie et les couts 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, inviter les utilisateurs a arrêter leur travail, enregistrer le travail en cours, empêcher les nouveaux accès des utilisateurs aux serveurs, interrompre 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.

La protection physique des équipements

La protection physique des équipements consiste à rendre inaccessible les équipements, hormis à ceux qui en ont l'autorisation. Les disques durs peuvent être protégés par des cadenas. L'enfermement des serveurs dans des **chambres fortes** permet d'isoler le matériel. Les ordinateurs sans lecteurs, ni disques, mais qui démarrent avec une **puce d'amorçage** sur la puce PROM de la carte réseau permettent de contrôler les données qui sont stockées sur un serveur. 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 et offre naturellement une protection physique.

Les outils d’administration

Les outils d'administration dépendent du système d'exploitation qui est installés et des protocoles qui sont utilisés. La surveillance des performances des machines est un travail de tous les jours qui requiert des compétences techniques importantes. La surveillance s’effectue à l’aide d'outils d’administration ou d'audit. 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, et les tentatives d'intrusion.

L’audit

Les audits externes permet de mettre à l'épreuve les infrastructures et les procédures de sécurité...