LES NOTIONS FONDAMENTALES

Introduction

Un réseau est un ensemble d'éléments reliés entre eux et réglés de manière qu'ils puissent communiquer. C'est aussi simple que ça. Et les réseaux informatiques n'échappent pas à cette règle. Afin de pouvoir communiquer, les êtres humains ont été dotés d'un langage auditif et/ou visuel. Dans le cas où notre interlocuteur ne comprend pas notre langue, alors nous nous dotons tout simplement d'interprètes.

En transposant cette définition globale des réseaux, nous pouvons conclure qu'un réseau informatique est un ensemble d'équipements informatiques reliés – disons plutôt interconnectés – entre eux et paramétrés de manière qu'ils puissent communiquer.

Il est de bon ton de souligner ici l'adage informatique qui dit que le réseau c'est l'ordinateur, c'est-à-dire que sans le réseau l'ordinateur est sous-exploité.

Voici quelques exemples de la réseautique.

- La mise en place d'un réseau informatique permet de faciliter et de sécuriser le stockage de l'information.
- Elle permet la standardisation des applications et le partage des données entre les postes de travail de manière efficace.
- La mise en réseau bien conçue facilite les opérations de gestion et de maintenance des applications et des équipements informatiques.
- La mise en réseau permet de réduire considérablement les coûts d'infrastructure. Grâce au réseau, les ressources matérielles et logicielles sont partagées entre plusieurs utilisateurs. Par exemple, au lieu d'acheter plusieurs imprimantes pour chaque service, une imprimante peut être partagée par tous les services. Il en est de même pour les applications distribuées.

Les différents types de réseaux

Il existe différentes sortes de réseaux, en fonction de la taille, du débit des informations, des types de protocoles de communication, etc. La technologie des réseaux a été abordée dans les chapitres précédents. Dans ce qui suit, nous nous concentrerons sur des concepts complémentaires en rapport avec l'architecture des réseaux en vue d'élargir nos compétences. Nous serons ainsi en mesure de réaliser un projet de conception d'un réseau d'entreprise avec une vision globale de la mise en réseau.

Dans un premier temps, nous allons définir brièvement les modèles conceptuels des réseaux, les différents types de réseaux locaux (*LAN*), les réseaux locaux virtuels (*VLAN*), les réseaux métropolitains (*MAN*), les réseaux étendus (*WAN*), les réseaux privés (*VPN*) et les réseaux sans fil (*wireless*). Nous verrons, dans les sections à venir, le modèle OSI qui constitue le cadre de référence qui nous permet de comprendre comment les informations circulent dans un réseau ainsi que l'architecture d'un réseau distribué; nous approfondirons les notions de réseaux locaux virtuels, pour terminer sur le stockage des données centralisées.

L’architecture des réseaux locaux

On distingue plusieurs types de réseaux qui se différencient entre eux en fonction de la distance entre les systèmes informatiques, ou encore en fonction de la technologie qui permet de les mettre en œuvre.

*Les réseaux locaux (*LAN*)*

Ce sont des réseaux de taille plus ou moins modeste, complexes, qui permettent l'échange de données informatiques et le partage de ressources (données, disques durs, périphériques divers, etc.). L’étendue géographique des réseaux locaux ne dépasse pas 10 km (ex. : pour un immeuble ou un campus). Le débit, ou la vitesse de communication, varie de quelques Mbps à 100 Mbps. Le nombre de stations ne dépasse généralement pas 1 000. Une variante du *LAN* est le *LAN* fédérateur ou réseau de base (*backbone*) qui est la voie principale empruntée par le trafic.

*Les réseaux locaux virtuels (*VLAN*)*

Un réseau local virtuel est un groupe logique d'unités ou d'utilisateurs qui peuvent être regroupés par fonction, service ou application peu importe l'emplacement de leur segment physique. La configuration d'un réseau local virtuel est effectuée dans le commutateur par un logiciel. Les réseaux locaux virtuels ne sont pas uniformisés et nécessitent l'utilisation d'un logiciel propriétaire vendu par le fournisseur de commutateurs. Ce type de réseau est vu plus en détails à la section suivante.

*Les réseaux locaux sans fils (*wireless, LAN *ou* WLAN*)*

Ce sont des réseaux sans connexions physiques visibles. Ces réseaux utilisent les ondes (radio, infrarouges, etc.) comme support de communication. Les ordinateurs mobiles ou les assistants personnels (*Palm Pilot*, etc.) constituent le secteur informatique en plus forte progression. Beaucoup de possesseurs de ce type d'ordinateurs ont également un ordinateur relié à des *LAN* ou des *WAN*, chez eux ou au bureau, auxquels ils sont reliés à tout instant.

- ***Les réseaux métropolitains (MAN)***

Les réseaux métropolitains permettent l'interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une zone urbaine dont l’étendue géographique n’excède pas 200 km. Ces réseaux peuvent être privés ou publics. Ils se distinguent aussi par leurs taux d’erreurs de communication. Le taux d’erreurs pour les réseaux *MAN* reste faible bien que plus élevé que pour les réseaux locaux : de 1 bit erroné sur 10^8 à 1 bit sur 10^{15}. Le débit est élevé car supérieur à 100 Mbps (sur liens de fibre optique).

- ***Les réseaux étendus (WAN)***

Les *WAN* (*Wide Area Network*) appelés aussi réseaux longue distance se situent à l’échelle nationale et internationale. Ce sont généralement des réseaux de télécommunications gérés par des opérateurs, qui assurent la transmission des données entre les villes et les pays à l’échelle de la planète. Leurs supports de transmission sont variés (ligne téléphonique, ondes hertziennes, fibre optique, satellite, etc.). La plupart de ces types de réseaux sont publics. Le taux d’erreurs de communication est plus élevé que celui des *MAN* : de 1 bit erroné sur 10^6 à un bit erroné sur 10^{12}. Les débits généralement plus faibles que dans les réseaux locaux dépendent du support de

transmission : ils varient de 56 kbps à plus de 625 Mbps pour les réseaux *ATM* (*Asynchronous Transfer Mode*) que nous verrons plus loin.

- ***Les réseaux privés virtuels (VPN)***

Les réseaux privés virtuels consistent en l'interconnexion de *LAN* à l'échelle nationale ou internationale. Ces réseaux restent privés et sont transparents pour l'utilisateur. Ils permettent en fait, par exemple pour une entreprise, de s'affranchir de certaines contraintes, telles que la localisation géographique. Ils rendent possible une transmission plus sécuritaire des données sur un réseau publique, en particulier sur Internet.

Le modèle *OSI*

Le modèle *OSI* constitue un cadre de référence qui nous permet de comprendre comment les informations circulent dans un réseau. C'est aussi un modèle conceptuel d'architecture de réseau qui facilite la compréhension théorique du fonctionnement des réseaux. Il est constitué de sept couches, chacune définissant des fonctions particulières du réseau.

Dans les sections suivantes, nous examinerons :

- Les bases théoriques sur lesquelles les réseaux et leurs protocoles reposent, autrement dit le modèle d'interconnexion des systèmes ouverts (*Open Systems Interconnection – OSI*) élaboré par l'Organisation internationale de normalisation (ISO);
- Les sept couches du modèle *OSI*.

La première version du modèle *OSI* repose sur une série de normes publiées par l'Organisation internationale de normalisation en 1978. Une seconde version apparaît en 1984. Cette dernière s'est à son tour établie en tant que standard reconnu au niveau international puisqu'elle intègre la quasi-totalité des cartes réseau et des protocoles.

Toute personne dont l'activité a un rapport avec les réseaux doit connaître les principes de base de ce modèle, car c'est sur eux que repose l'appellation des composants. Ainsi, dans le jargon des professionnels des réseaux, un commutateur de couche 3 (*switch layer 3*) est un commutateur fonctionnant au niveau 3 du modèle *OSI*.

Le modèle *OSI* se subdivise en **sept couches** (*layers*), ou niveaux. Chaque couche traite une tâche, un **protocole**[1] ou un composant matériel, repose sur les couches sous-jacentes, et communique avec les autres couches.

Cette communication entre les couches s'effectue au travers d'interfaces définies. En principe, seules deux couches adjacentes peuvent communiquer, dans la mesure où la famille de protocoles utilisée les exploite. Il n'est pas possible de « sauter » une couche.

La couche la plus élevée (couche application) est la plus proche de l'utilisateur; la couche inférieure (couche physique) est la plus proche des médias de transmission.

[1] **Protocole**
Description formelle d'un ensemble de règles et de conventions qui réglementent la façon dont les équipements sur un réseau échangent des informations. Source : Le lexique des réseaux.
Ensemble des spécifications décrivant les conventions et les règles à suivre dans un échange de données. Source : Le Grand Dictionnaire terminologique.

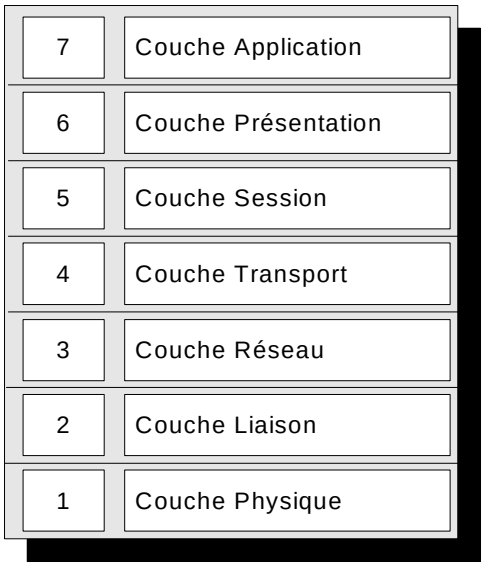

Figure 1 : Les sept couches du modèle *OSI*

1. La couche physique

La couche physique (*physical layer*) assure, comme son nom l'indique, le transport physique de données. Il s'agit de la transmission de signaux électriques, optiques ou de radiofréquences à travers des médias appropriés. Un média est un support physique par lequel passe le signal transmis. Dans le domaine des réseaux, on parle de câbles de cuivre, de fibre de verre, de l'atmosphère ou même du vide (dans l'espace).

La totalité des paramètres de cette transmission y sont définis, selon les spécifications propres au type de la transmission. Ces spécifications portent tant sur la méthode de codage des données que sur les caractéristiques des composants tels les câbles, les connecteurs et leur brochage.

Le codage des données spécifie la représentation physique de bits (0 ou 1) par des tensions électriques, des ondes radio ou des flux optiques, ainsi que la coordination de la suite de signaux et la synchronisation des systèmes émetteurs et récepteurs. Le but est évidemment qu'un bit de valeur 1 transmis soit effectivement reconnu comme tel.

Le média de la couche physique est généralement caractérisé par :

- La **distance maximale** parcourue sans répéteur, par exemple 100 mètres pour le câble à paire torsadée *UTP* catégorie 5. Nous verrons dans les sections qui suivent les différents types de câbles. Disons dès à présent qu'un répéteur est un dispositif qui régénère et propage les signaux électriques entre deux segments (tronçons) du réseau.
- La **bande passante** qui représente la mesure de la quantité de données pouvant circuler d'un endroit à un autre en une période de temps donnée, par exemple 100 Mbps pour le câble à paire torsadée *UTP* catégorie 5.

Il ne faut pas confondre la bande passante et le **débit**. Le débit correspond à la bande passante réelle, mesurée à un instant précis entre l'émetteur et le récepteur, par

exemple lors du transfert d'un fichier particulier. Le débit est généralement inférieur à la bande passante du média utilisé.

2. La couche liaison de données

La couche liaison de données (*data link layer*) assure la fiabilité de la transmission en élaborant les datagrammes[2] appelés trames (*frames*) à partir des paquets (blocs de données) de la couche réseau, à destination de la couche physique. Cela signifie que les données seront structurées en trames (trains de bits) que la couche 1 se chargera de transmettre. Le type des trames dépendra du type du réseau. Ainsi, une trame *Ethernet* n'est pas structurée de la même manière qu'une trame *token ring*. *Ethernet* et *token ring* sont des normes de base en réseau dont nous parlerons dans la suite de ce document.

Le but principal de la couche liaison est de garantir aux couches de niveau supérieur une transmission fiable par le réseau. Cette couche doit donc recevoir un accusé de réception des données expédiées. Si elle ne le reçoit pas, elle renouvelle la transmission. Le type de l'accusé de réception dépend également du type de réseau.

Un examen plus approfondi permet de subdiviser cette couche en deux sous-couches. Ces deux couches sont appelées procédure *LLC* (*Logical Link Control – LLC*) et commande d'accès au support (*Medium Access Control – MAC*). Le *LLC* est la partie assurant la fiabilité des transmissions et il répond aux caractéristiques précédemment évoquées. Les mécanismes de la sous-couche *LLC* permettent d'associer plusieurs protocoles à une même carte réseau ou un protocole à plusieurs cartes réseau dans le même ordinateur. La sous-couche *MAC* traite la méthodologie d'accès au support de transmission (comment l'information parvient au médium de transmission) et transfère vers la couche physique les données reçues du *LLC*. Il est également responsable de l'adressage des cartes réseau qui possèdent toutes un numéro d'identification unique. Ce numéro, identificateur *MAC* ou adresse physique, permet d'identifier une carte parmi toutes celles qui existent au monde.

La couche 2 traite les modes d'accès à des réseaux tels *CSMA/CD* (*Carrier Sense Multiple Access/Collision Detection*) ou *Token-Passing* dont nous parlerons plus loin.

3. La couche réseau

La couche réseau contient les protocoles de transport tels *IP* (utilisé dans Internet) ou *IPX* (des réseaux *Novell Netware*). L'adressage des messages, la définition de la route d'acheminement sont définis par un routeur ou un commutateur de niveau 3. Cette couche traitera également les problèmes d'acheminement tels que l'indisponibilité d'un segment de réseau, et la subdivision des données en petits blocs appelés paquets, dans la mesure où leur taille à la réception des couches supérieures dépasse celle admise par le protocole de niveau 3.

4. La couche transport

---

[2] **Datagramme**
Terme générique pour désigner un bloc de données. En fonction de la couche, le datagramme prend un nom spécifique. De la couche 7 à la couche 5, c'est un message, ou tout simplement une donnée. À la couche 4, c'est un segment (le message est découpé en plusieurs morceaux dont la taille est compatible avec le protocole utilisé à cette couche). À la couche 3, c'est un paquet. À la couche 2, c'est une trame, et à la couche 1, ce sont des bits.

La couche transport assure le transfert sans erreur des paquets. Elle subdivise en petits blocs les messages longs. Les paquets trop petits sont assemblés en grands paquets. Les paquets ainsi créés sont numérotés à la couche 3. Symétriquement, les données sont extraites des paquets reçus par le destinataire, mises en ordre et un accusé de réception est éventuellement envoyé.

Les contrôles de flux et d'erreurs sont également assurés par la couche transport. Elle traite les erreurs de constitution des paquets et de transmission de données ainsi que la réception par la station cible. Lorsque deux systèmes communicants ouvrent une session ou créent une liaison, cela se déroule au niveau 4 du modèle *OSI*.

Cette couche contient les protocoles de transport tels *TCP* (*Transmission Control Protocol*) ou *UDP* (*User Datagram Protocol*).

5. La couche session

La couche 5 du modèle *OSI* correspond à la couche session, également qualifiée de « couche de contrôle des communications ». Le niveau session assure l'établissement correct, le maintien et l'arrêt d'une communication sécurisée de deux applications de plusieurs ordinateurs. Elle gère les noms de ressource et prend en compte l'aspect sécurité de l'application. Dès qu'une application tente de communiquer avec une application d'un autre ordinateur, la couche session se procure l'adresse de l'ordinateur cible et demande à la couche transport d'établir une connexion. Aux applications sont alors proposés des services pour contrôler cette liaison. Ces services, tels que prescrits par l'*ISO*, sont articulés selon la classe *Basic Combined* pour les fonctions générales, la classe *Basic Synchronized* pour les méthodes de synchronisation de la liaison, et la classe *Basic Activity* pour gérer les activités réseau entre les stations.

6. La couche présentation

La couche présentation définit un format des données par lequel les informations circuleront dans le réseau. Les données de la couche présentation sont adaptées à un format uniforme pour que tous les ordinateurs concernés puissent les traiter.

Cela est nécessaire car les plates-formes PC, Macintosh ou les différents UNIX représentent les données de manière différente. Il convient donc d'adopter une représentation unique si nous souhaitons que ces plates-formes puissent communiquer. Les données sont alors traduites en un format intermédiaire, et transmises en ce format. Le destinataire retranscrira les données reçues en fonction des impératifs de la plate-forme. Cette couche traite également d'éléments tels la compression, le changement de jeux de caractères ou le codage des données. Dans le cas des ordinateurs qui, dans un Intranet[3], sont exploités en tant que serveurs ou stations de travail, nous trouverons également les utilitaires qui assurent des entrées/sorties à travers le réseau. Nous pensons ici aux lecteurs ou aux imprimantes en réseau.

7. La couche application

La couche application est la couche supérieure du modèle *OSI* et donne accès aux services réseau de l'ordinateur. Elle comprend des programmes tels que le navigateur qui permet à l'utilisateur de lire des pages Web, le client *FTP* (*File Transfer Protocol)*

[3] **Intranet**
Réseau informatique privé qui utilise les protocoles de communication et les technologies du réseau Internet. Source : Le grand dictionnaire terminologique.

pour le téléchargement de fichiers, le programme de messagerie, les applications de bases de données et de nombreux autres logiciels qui nécessitent un accès réseau.

- ***Principe de fonctionnement des couches OSI***

Chaque couche possède des fonctions, qu'elle met à la disposition des couches supérieures. L'utilisateur ne voit en principe que la couche application du niveau supérieur, alors que le spécialiste du réseau se préoccupera également des autres couches.

Lorsque deux ordinateurs entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes. Cela signifie que les couches se comportent comme si elles étaient en contact direct et non à travers des couches inférieures. Nous avons représenté à la figure 2 une telle communication à travers des couches session de deux ordinateurs. Le fonctionnement du transfert des données y est clairement expliqué.

La couche session de la station 1 signale à la couche transport qu'elle souhaiterait faire parvenir un message à son homologue de la station 2 et le lui transmet. La couche transport découpe le message en segments de taille définie, ajoute des informations sur l'adressage et le format et les transmet à la couche suivante. Celle-ci procède de même. Et ainsi de suite jusqu'à ce que les données soient expédiées vers la station 2.

Parvenus au poste destinataire, les paquets de données sont débarrassés des éléments devenus inutiles, intégrés par l'expéditeur dans leur en-tête, et transmis aux couches de niveau supérieur, jusqu'à atteindre leur destination. Cette dernière couche extraira les informations utiles.

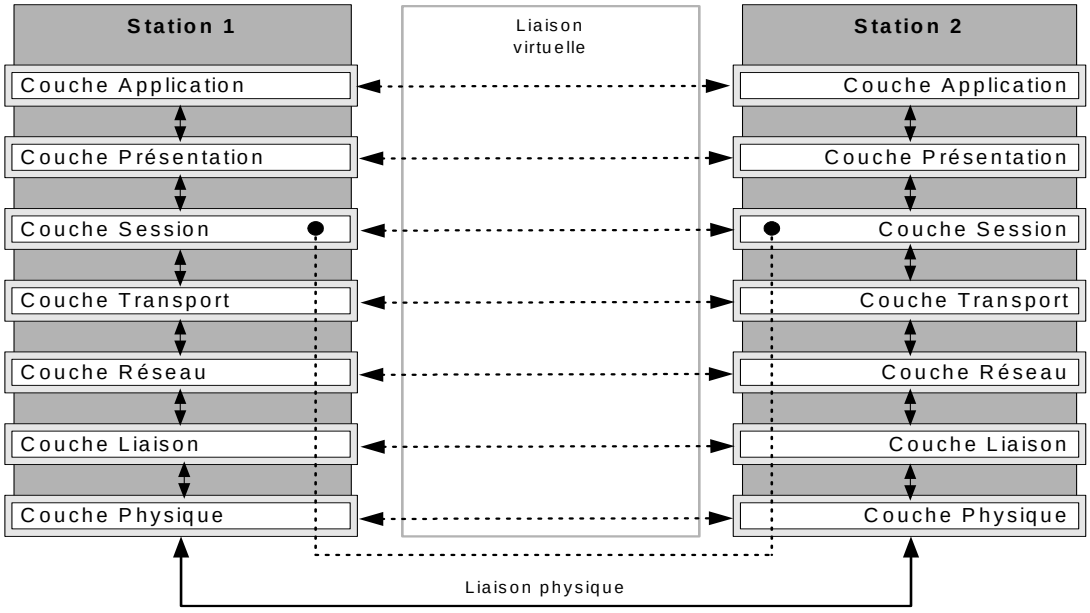

Figure 2 : La communication entre deux couches à travers une liaison virtuelle

Le processus qui consiste à prendre l'unité de données qui provient d'un niveau supérieur et à bâtir une nouvelle unité en y ajoutant des informations de contrôle propre à ce niveau est connu sous le nom *d'encapsulation*. L'opération inverse porte le nom de *décapsulation* et correspond au processus de retrait des en-têtes ajoutés par une couche supérieure pour accéder aux données.

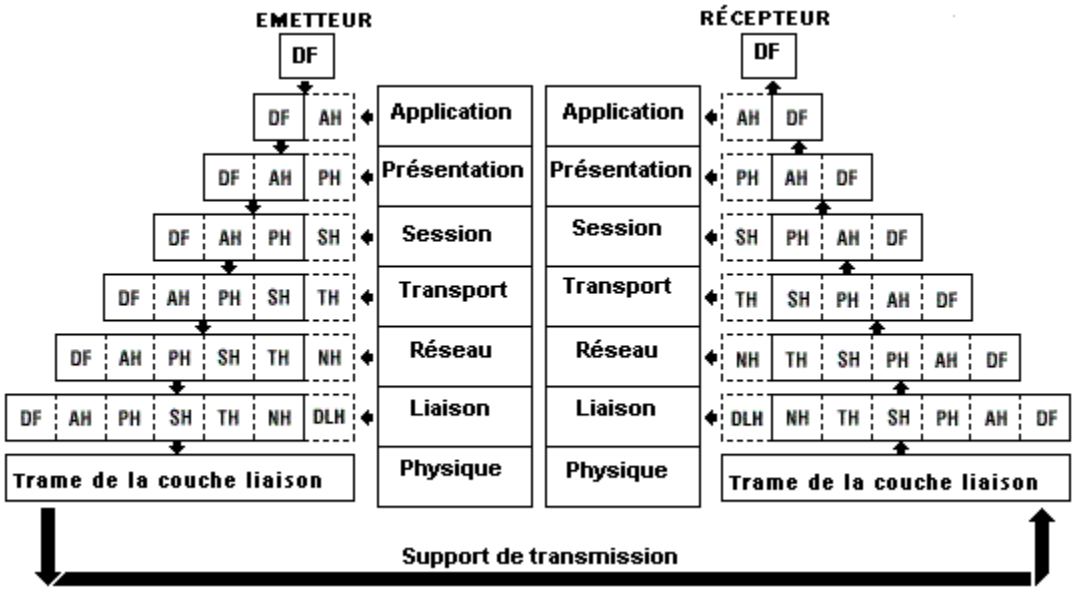

Figure 3 : Empaquetage d'un paquet émanant de la couche application

- ***Les services et interfaces OSI***

Information

Une couche *OSI* communique avec une autre couche adjacente en se servant des services fournis par celle-ci. Une interface délimite les services offerts par deux couches adjacentes. En somme, ces services permettent à une couche spécifique *OSI* de communiquer avec la couche *OSI* correspondante (couche homologue – *peer layer*) d'un autre ordinateur. Un service est composé de trois éléments : l'utilisateur du service, le fournisseur du service et le point d'accès au service (*Service Access Point – SAP*).

Dans ce contexte, l'utilisateur de services est la couche *OSI* qui fait une demande de services à la couche adjacente. Le fournisseur de services est la couche *OSI* qui fournit les services aux utilisateurs. Le *SAP* est un portail conceptuel à travers lequel une couche *OSI* peut faire une requête de services auprès d'une autre couche.

La figure suivante démontre l'interaction de ces trois éléments dans le cas d'une couche supérieure (N + 1) et de sa couche inférieure adjacente (N).

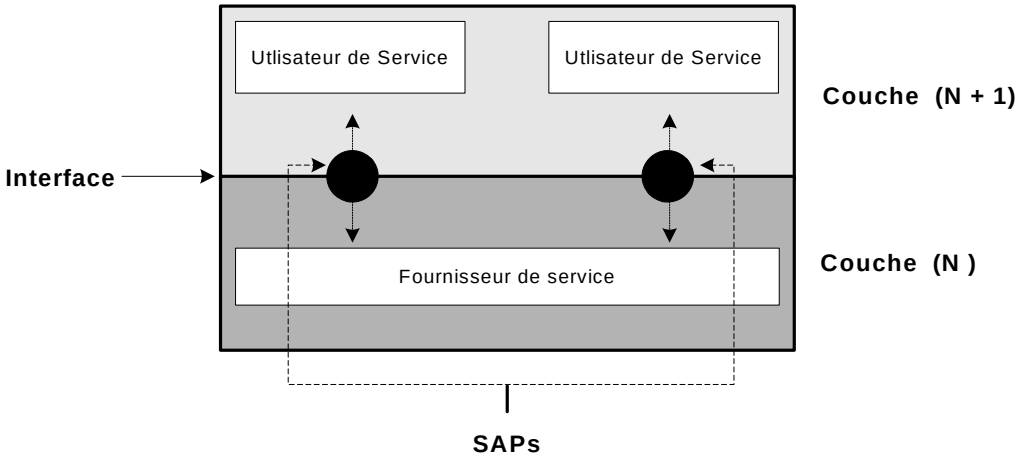

Figure 4 : Interaction entre une couche supérieure (N + 1) et sa couche inférieure adjacente (N)

- ***Règles et exceptions***

Le modèle en couches *ISO*/*OSI* est un cadre compatible avec les protocoles et les types de réseau les plus courants. De nombreux éléments ne se retrouvent toutefois pas dans une couche unique bien définie. Par exemple, dans le cas de réseaux basés sur les normes *Ethernet*, *token ring* ou *FDDI* (qui seront définies plus tard), il n'est pas possible de séparer les couches impliquées. Une partie des spécifications (type des câbles et connecteurs ou caractéristiques électriques) figureront dans la couche 1, la couche physique, alors que les méthodes d'accès se retrouveront dans les couches supérieures.

Dans le cas des protocoles ainsi que des applications, certaines fonctions ne se limitent pas à une seule couche. Presque tout applicatif déborde de la couche application et s'étend, en raison de la conversion des codages ou des compressions de données internes au programme, dans la couche de présentation des données. Il est courant de parler de pile de protocoles (*protocol stack*) qui, outre les protocoles de liaison et de transport, contient également d'autres sous-protocoles de niveau supérieur. Ces niveaux supérieurs peuvent aussi s'intégrer dans des applicatifs.

Il est en outre courant de ne pas traiter certaines couches et de se reposer sur d'autres. Cela ne constitue toutefois que l'exception, lorsqu'il s'agit d'obtenir de hautes performances de transfert. De tels manquements aux règles ne se produisent que dans des réseaux de production et dans le pilotage d'installations.

Les organismes de standardisation et de normalisation

Les normes sont des ensembles de règles ou de procédures établies par un organisme officiel et qui servent de standard ou de modèle pour concevoir un produit ou proposer un service. Les normes internationales permettent en général d'assurer la compatibilité et l'interopérabilité entre les différentes technologies de réseau développées par de nombreuses entreprises dans le monde entier. Elles contribuent à nous simplifier la vie et à accroître la fiabilité et l'efficacité des biens et services que nous utilisons.

Les organismes les plus importants émettant des normes dans le domaine du réseautage sont :

- *ISO* : L'organisation internationale de normalisation est une fédération mondiale d'organismes nationaux de normalisation de quelque 140 pays, à raison d'un organisme par pays.
- *IEEE* : L'Institute of Electrical and Electronics Engineers est un organisme professionnel américain basé à Washington, dont les activités incluent le développement de normes relatives aux communications et aux réseaux.
- *EIA/TIA* : Electrical Industries Association/Telecommunications Industry Association. Organismes américains qui développent des normes relatives aux technologies de télécommunications. Ensemble, la TIA et l'EIA ont établi des normes formelles comme EIA/TIA-568 A et B sur les caractéristiques du câblage horizontal en télécommunications dans les bâtiments.
- UIT : Union internationale des télécommunications. C'est une agence des Nations unies basée à Genève, spécialisée dans les questions de télécommunications. Les questions techniques et l'élaboration de normes volontaires (appelées recommandations ou avis) sont traitées par deux comités de l'UIT, l'UIT-R (anciennement Comité consultatif international des radiocommunications – CCIR) et l'UIT-T (autrefois Comité consultatif international télégraphique et téléphonique – CCITT).
- ACNOR : Au Canada, l'Association canadienne de normalisation (*CSA – Canadian Standard Association*).
- AFNOR : Association française de normalisation en France.
- *DIN* : Institut allemand pour la normalisation en Allemagne.
- *BSI* : British Standard Institution au Royaume-Uni.
- *IEEE-SA* : IEEE Standard Association de l'organisation professionnelle IEEE

Topologie des réseaux

- **Topologie physique**. Le terme topologie physique désigne l'organisation ou la disposition physique des nœuds du réseau. Un nœud de réseau représente un ordinateur, une imprimante, un équipement d'interconnexion. La topologie physique détermine non seulement le type de câble utilisé, mais également la façon dont le câblage doit être effectué. Il existe trois topologies principales que nous allons voir plus loin : en bus, en étoile et en réseau.

- **Topologie logique.** La topologie logique correspond à la disposition logique du réseau. Elle fait référence en général à la façon dont l'information circule à l'intérieur du réseau au niveau de la couche liaison de données (couche 2).

Les méthodes d'accès des réseaux

Token ring (réseau en anneau à jeton)

Cette technologie fut introduite par IBM en 1984. Elle répond à la spécification IEEE 802.5 et n'est plus employée dans les nouvelles installations. Mais la technologie sur laquelle repose le réseau en anneau à jeton est exploitée dans d'autres domaines, si bien que nous l'examinerons ici.

Le principe

Le but était de relier une série d'ordinateurs par un câblage simple. Le support retenu fut la paire torsadée (*twisted pair*), déjà employée en téléphonie. Le câble peut être du type 1, 2 ou 3.

Figure 5 : La paire torsadée

Information
Les types de câbles IBM 1, 2 et 3
Voici les caractéristiques des câbles de type 1, 2 et 3, définies par IBM.
Type 1 : câble de données en paire torsadée blindée.
Type 2 : câble de données et de signal audio en paire torsadée blindée par tresse.
Type 3 : câble de signal audio en 4 paires torsadées fortement blindées.

La topologie d'un réseau *token ring* est un anneau logique qui se concrétise physiquement par une étoile. Cela signifie qu'un concentrateur (*Medium Attachment Unit – MAU* ou *hub*) relie la ligne d'émission d'une station à la ligne de réception de la station suivante, ce qui, logiquement, crée un anneau. Le concentrateur est un appareil, un dispositif, qui permet de relier plusieurs ordinateurs dans un réseau en étoile. Physiquement, les cordons qui contiennent chacun tant la ligne d'émission que la ligne de réception seront disposés en étoile par rapport au concentrateur.

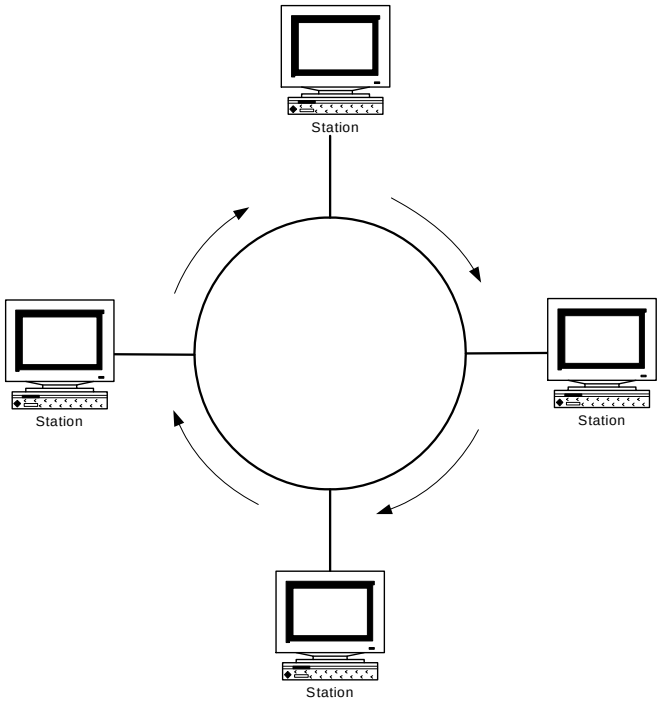

Figure 6 : La topologie logique du réseau en anneau à jeton

Les données envoyées par une station sont transférées vers les stations suivantes par l'anneau que forme le concentrateur. Si, en lisant l'adresse du paquet, cette station détermine qu'elle en est le destinataire, elle le prend. Sinon, elle le transmet à la station suivante. Le paquet parcourt ainsi la boucle jusqu'à ce qu'il parvienne à son destinataire ou qu'il revienne à son expéditeur, auquel cas il est effacé. La méthode d'accès utilisée dans ce cas s'appelle passage de jeton (*token passing*), d'où le nom anneau à jeton (*token ring*).

Ce jeton se compose d'un petit paquet de données qui parcourt en permanence l'anneau. Il est créé par le premier ordinateur qui s'identifie auprès du réseau. Lorsqu'une station désire émettre des données, elle attend de recevoir le jeton. Elle l'extrait alors du circuit et le remplace par le paquet de données à transmettre. Le processus ne durant qu'une fraction de seconde, la transmission par les stations semble instantanée.

Les données parviennent à la station réceptrice. Celle-ci copie le paquet également appelé trame. Les données sont ensuite transmises aux couches supérieures du réseau. Simultanément, la station dépose une trame d'acquittement dans l'anneau. Cette trame est transmise à la station émettrice, qui la prend et la remplace par le jeton.

Inscription dans l'anneau

Lorsqu'une station s'active, elle s'inscrit dans l'anneau. Elle reçoit une adresse unique et les autres ordinateurs sont informés de sa présence.

Moniteur d'anneau (ring monitor)

L'un des ordinateurs occupe le poste de moniteur d'anneau. Il s'agit généralement du premier ordinateur s'inscrivant dans le réseau. Sa tâche est de gérer correctement le transfert des paquets de données. Il s'assure, entre autres, qu'un paquet ne parcourt pas plusieurs fois l'anneau et qu'un seul jeton circule dans le réseau.

Les concentrateurs de l'anneau

L'anneau, comme nous l'avons évoqué, se ferme au niveau du concentrateur. Il peut en fait y avoir plusieurs concentrateurs, reliés par leur entrée et leur sortie d'anneau. Il faut veiller à ce que leur raccordement crée un nouvel anneau.

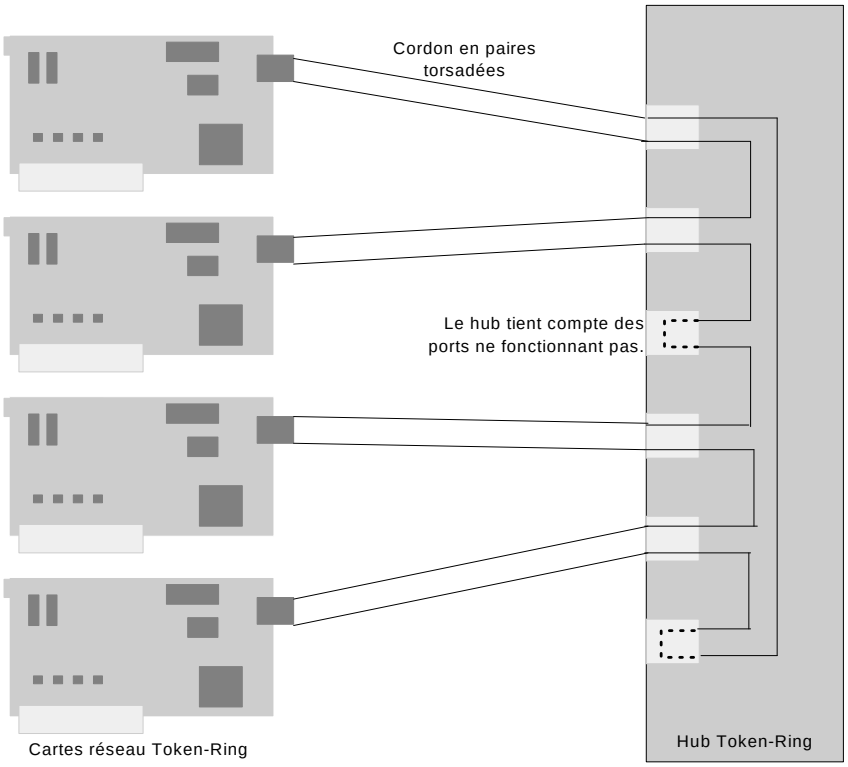

Figure 7: Un concentrateur de réseau en anneau à jeton

Le concentrateur d'un réseau en anneau à jeton détecte si une station qui lui est raccordée fonctionne ou non. Cela est nécessaire pour éviter que la mise hors tension d'un ordinateur n'ouvre la boucle et bloque le réseau. Il détecte également les raccordements non utilisés ou défectueux.

Les variantes de token ring

Token ring existe en version 4 Mbps et 16 Mbps. À l'opposé de la version 4 Mbps, la version 16 Mbps exploite la technologie dite de la libération anticipée du jeton (*early token release*). L'émetteur ne conserve alors pas le jeton jusqu'au moment de l'accusé de réception, mais le réintroduit dans le circuit dès que l'émission des données est terminée. L'avantage est de ne pas limiter la transmission à une section du réseau et d'autoriser la communication simultanée de plusieurs stations. Les trames de la version 16 Mbps sont également plus grandes que celles de la version 4 Mbps.
Un réseau peut donc fonctionner selon l'un des deux principes. Les cartes de type 16 Mbps seront certes utilisées, mais elles passeront en mode 4 Mbps puisqu'un seul mode peut s'employer dans un réseau.

	Token ring
Topologie	Anneau en étoile
Méthode d'accès	Passage de jeton
Type de câble	*UTP* ou *STP*
Connecteur	*MIC* pour type 1 et 2

Vitesse	4 ou 16 Mbps
Impédance	100-120 pour *UTP* 150 pour *STP*
Distance minimum	2,5 m entre 2 PC
Longueur maximum d'un segment	45 m pour *UTP* 100 m pour *STP* 101 m pour type 1
Nombre maximum de segments	33 MSAU
Longueur maximum du réseau	Distance max. entre MSAU de 150 m; avec 2 répéteurs et type 3 : 365 m; type 1 ou 2: 730 m
Nombre maximum de PC par segment	*UTP* : 72 PC par concentrateur *STP* : 260 PC

Information
Que signifie Mbps?
Mbps est l'abréviation de mégabit par seconde et désigne la vitesse du flux de données réseau.

Ethernet

Après les réseaux en anneau à jeton, nous allons étudier la technologie Ethernet. *Ethernet* est la norme la plus employée dans les réseaux locaux actuels. La première version fut développée en 1972 par David Boggs et Robert Metcalfe au Paolo Alto Research Center (PARC) de la société Xerox. Les premiers produits *Ethernet* furent commercialisés en 1975. L'*Ethernet* d'origine pouvait relier 100 ordinateurs par un cordon d'une longueur de 1 000 mètres et fonctionner à une vitesse de 2,96 Mbps.
Ce succès fit que Xerox, Digital Equipment Corporation et Intel s'unirent pour créer une nouvelle norme qui portait la vitesse de transmission à 10 Mbps. Cette norme est aujourd'hui connue sous le nom de 10Base5 ou *yellow cable*. Ce « câble jaune » vient du type de câble employé à l'époque, de couleur jaune, et qui s'appelle *thick Ethernet* (gros câble *Ethernet* jaune). Ethernet est assujetti à la norme IEEE 802.3. *Fast Ethernet* (100 Mbps) et *Gigabit Ethernet* (1 000 Mbps).

La technologie sous-jacente

Un réseau *Ethernet* est de type topologie logique en bus. Cela signifie que toutes les stations reliées à un segment *Ethernet* accèdent à un même support partagé (*shared*

medium).

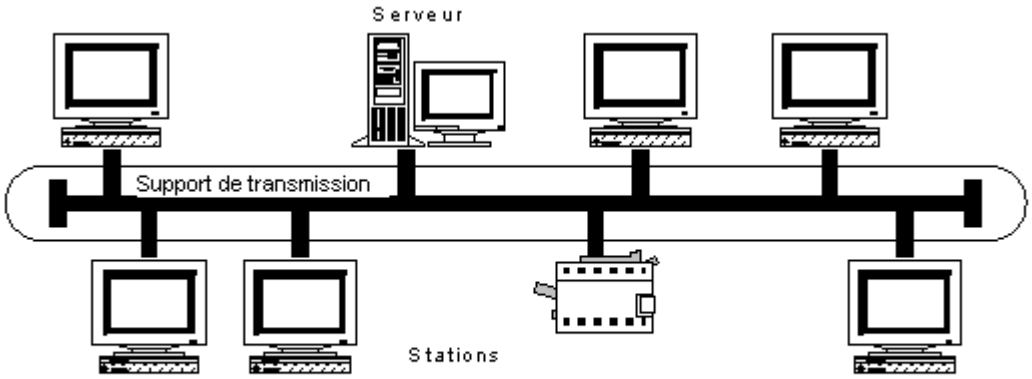

Figure 8 : La topologie en bus

La méthode d'accès répond au principe *CSMA/CD*. Exprimé en langage de tous les jours, le principe revient à « parler tout en écoutant s'il se passe quelque chose ». Avant d'émettre un message, le nœud de réseau « écoute » sur la liaison commune pour déterminer si le chemin est libre (*carrier sense*, détection de porteuse). Si le chemin est libre, elle envoie le message. Mais si, à ce moment précis, une station démarre une émission (*multiple access*, multiaccès), les deux signaux se perturbent et il est question alors de collision.
Les cartes *Ethernet* vérifient si une collision s'est produite (*collision detection*, détection de collision). Ce contrôle repose sur la vérification de la tension présente sur la ligne. Une transmission normale se traduit par un signal de 1 volt. En cas de collision, la tension des signaux augmente. Si, sur le média partagé, la carte mesure une tension supérieure à 1 volt, elle en conclut qu'une collision s'est produite. Dans ce cas, un générateur de nombres aléatoires fixera une durée s'exprimant en dixièmes de seconde. Cette durée écoulée, le système fait une deuxième tentative d'émission. Cette dernière peut également se traduire par une collision et la durée de transmission s'allonge d'autant. Lorsque le segment est fortement chargé, cela conduit à un ralentissement du trafic pouvant aller jusqu'au blocage du réseau.
Les données sont transmises au sein de trames. Une trame est un paquet d'informations transmis sur la connexion commune. Sa taille varie entre 64 et 1 518 octets, 18 octets étant utilisés pour la structure de la trame.

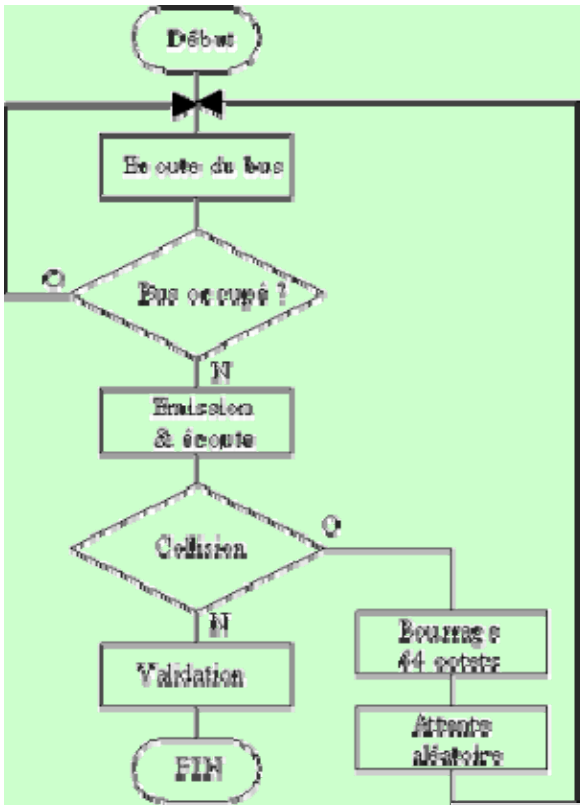

Figure 9 : Méthode d'accès à un support partagé

Information
Qu'est-ce qu'un octet?
Un octet est tout simplement une séquence de 8 bits.
Exemple : 11010100

Il existe essentiellement deux types de trame *Ethernet* :
Ethernet-II et IEEE 802.3.

La structure d'une trame de type Ethernet-II est décrite dans le tableau.

Tableau 1 Structure d'une trame de type Ethernet-II

Champ	Longueur	Explication
Préambule	8 octets	Identifie le début de la trame des données
Adresse cible	6 octets	Adresse *MAC* de l'ordinateur cible
Adresse source	6 octets	Adresse *MAC* de l'ordinateur source
Type	2 octets	Type de protocole de transport
Données	46-1 500 octets	Données utiles
CRC	4 octets	Contrôle de redondance cyclique

Tableau 1 : Structure d'une trame de type Ethernet

1

La spécification IEEE 802.3 d'*Ethernet* se distingue en ce que le champ Type est remplacé par un champ Longueur. Cette longueur est celle des données utiles transmises dans le paquet. La détection de la norme *Ethernet* utilisée s'effectue d'après ce champ. Si la valeur qui y figure est supérieure à 1 500, alors il s'agit d'une trame Ethernet II et le champ identifie le type de protocole de transport. Si la valeur est inférieure, alors il s'agit d'un champ IEEE 802.3 indiquant la longueur des données utiles. L'adressage des paquets *Ethernet* s'effectue au travers des adresses *MAC*, qui signifie *Medium Access Control* (description de l'accès au support réseau). L'adresse de 6 octets (48 bits) est généralement inscrite de manière définitive dans la carte et l'identifie parfaitement. Les 3 premiers octets de l'adresse sont définis en fonction du fabricant de la carte et sont attribués par un comité gérant les identificateurs des fabricants. Les 3 octets suivants sont une numérotation définie par le fabricant. La combinaison des deux valeurs assure l'identification univoque du matériel, comme l'exige *Ethernet*.

Les différentes normes reliées à Ethernet

10Base5 appelée également *yellow cable* ou *thick Ethernet* ou gros câble jaune.

- **10** pour 10 mégabits par seconde
- **Base** pour envoi du signal en bande de base (le signal occupe toute la bande passante du média de transmission)
- **5** pour 5 fois 100 mètres soit 500 mètres.

10Base5 utilise un câble coaxial de l'épaisseur d'un doigt comme média de transmission. Dans les anciens réseaux, ce câble représentait la dorsale (*backbone* ou câble fédérateur) du réseau. Un segment *Ethernet* 10Base5 peut atteindre une longueur de 500 m. Des répéteurs (*repeaters*) peuvent assembler jusqu'à 5 segments, ce qui permet d'atteindre une longueur totale de 2 500 mètres. Vous devez veiller à respecter la règle 5-4-3. Si vous ne la connaissez pas, elle est expliquée dans le prochain encadré.

Information
La règle 5-4-3.
Les segments 10Base5 et 10Base2 peuvent s'assembler en de grands réseaux. Nous devons toutefois veiller à ce qu'un tel réseau se compose au plus de 5 segments, chacun régénéré par un répéteur. Un répéteur assure l'amplification et la remise en forme des signaux.
La longueur maximale de ligne ne doit pas non plus être dépassée.

La norme 802.3 pour Ethernet 10 Mbps limite à 2 le nombre de répéteurs entre 2 stations.

On peut atteindre le nombre de 4 répéteurs à condition que 2 segments traversés soient en point à point, c'est-à-dire sans aucune station connectée. Soit 5 segments reliés par 4 répéteurs avec seulement 3 segments recevant des

stations.

Un concentrateur (*hub*) est un répéteur multiport; il constitue une solution économique pour l'extension d'un réseau *Ethernet*.

Aujourd'hui, l'avenir d'Ethernet est une question très préoccupante car 10 Mbps n'est plus considéré comme une vitesse élevée. Néanmoins, il existe des variantes de ce protocole qui permettent d'atteindre une plus grande vitesse. En outre, le fait qu'un réseau de type Ethernet soit peu coûteux et facile à administrer est de nature à garantir l'usage de ce protocole.

L’architecture du modèle distribué

Les débuts

C’est bien beau de vouloir simplifier la vie aux utilisateurs des réseaux… mais c’est un véritable casse-tête pour les maîtres d’œuvre! En réfléchissant un peu sur la question, on peut aisément comprendre combien les approches traditionnelles pour exécuter des instructions à travers un réseau vers d'autres ordinateurs étaient sujettes à des erreurs de transmission ainsi qu’à des problèmes de compatibilité matériel et logiciel.

Après cogitation, un consortium de constructeurs, qui s’est donné le nom de code de *OSF*, s’est réuni et a conclu que la meilleure manière de poser ce problème était la suivante : il s’agit de considérer un objet présent sur une autre machine, de lui envoyer un message et d’obtenir un résultat comme si l'objet se trouvait sur notre propre appareil, à cet instant précis. C’est ce qui se passe avec le web. L’*OSF* a donné naissance à l’architecture du modèle distribué.

OSF est l’abréviation de *Open Software Foundation*. Il s’agissait d’une organisation de fabricants d'ordinateurs dont l'objectif était de promouvoir les systèmes ouverts, par exemple en mettant sur pied une norme valide de système d’exploitation. L’*OSF* a vu le jour en mai 1988. Elle a regroupé différents constructeurs et fournisseurs de logiciels (dont 9 fondateurs : IBM, Bull, HP, DEC, Apollo, Hitachi, Nixdorf, Philips, Siemens) œuvrant à la détermination d'un environnement applicatif commun complètement standardisé. L’*OSF* fournissait des produits, retenait des logiciels déjà disponibles parmi ses membres (au moyen de *RFT – Request For Technology*), puis éventuellement confiait les développements complémentaires à des organismes choisis. *OSF* et *Unix International* poursuivaient les mêmes buts et étaient donc concurrents. Les principaux produits *OSF* étaient :

- *MOTIF*, environnement graphique;
- *OSF/1*, noyau *Unix* fondé sur la technologie micro noyau *MACH* de *Carnegie Mellon*;
- *DCE*, environnement de distribution permettant l'accès quasi transparent à des services quels que soient leur localisation;
- *ANDF*, format de distribution universel;
- *DME*, environnement de gestion de systèmes et de réseaux.

En 1996, *OSF* et *X/OPEN* créent un consortium commun : *Open Group*, qui reprend les objectifs de chacun. Pour la petite histoire, ces fabricants étaient tellement en désaccord avec les autres consortiums visant le même objectif qu'ils ont eu beaucoup de mal à aboutir à quelque chose de cohérent!

L’évolution des systèmes informatiques

Ceci étant, le système informatique a tout de même énormément évolué ces vingt dernières années. Il est en effet passé du système centralisé pour aboutir de nos jours au système distribué.

Le système centralisé (années 70) est un système dans lequel l’ensemble des composants est localisé sur un seul site. C’est un système dont les données et les

traitements sont centralisés. Il gère des terminaux passifs au sein de réseaux propriétaires.

Un système décentralisé (années 80) est un système dans lequel les composants sont localisés sur plusieurs sites et n'ont peu ou pas de coordination entre eux.

Enfin, le système distribué (années 90) est un système dans lequel les composants, localisés sur des sites différents, sont capables de coopérer et de coordonner leurs opérations à travers un réseau. Le système distribué est :

- une collection d'équipements faiblement couplés (pas de mémoire commune) et
- reliés par des réseaux pouvant être indépendants et hétérogènes
- interconnectés au moyen de réseaux de communication
- coopérant par réseau de messages pour former une machine virtuelle (ordinateur unique).

On distingue deux principaux types de systèmes distribués :

- le système client/serveur,
- le système à objets distribués.

Le modèle client/serveur est la description conceptuelle de la communication entre un client qui émet une requête vers un serveur qui traite la requête émise. Il est également l'implémentation physique et logicielle du modèle client/serveur. Une application client/serveur est une application développée au sein d'un système du même nom et qui permet une gestion plus simple de la cohérence et de l'intégrité des données. Ce système ne résout cependant pas les problèmes de portabilité et d'interopérabilité d'applications, c'est-à-dire qu'il n'y a pas de transparence de localisation.

Le système à objets distribués est la description conceptuelle du modèle de communication permettant à des objets distribués d'interopérer à travers un réseau hétérogène. Un système à objets distribués est l'implémentation physique et logicielle du modèle à objets distribués. Un système client/serveur est une restriction d'un système à objets distribués.

Les différents types de réseaux locaux virtuels (*VLAN*)

Le terme réseau local, autrefois défini comme un réseau d'ordinateurs situé dans une même enceinte, désigne actuellement un ensemble de machines connectées entre elles dans un même domaine de diffusion. Une information envoyée par un ordinateur en diffusion vers son réseau est ainsi reçue par tous les postes de ce réseau. Les domaines de diffusion, séparés par des routeurs, dépendent des architectures physiques du matériel de connexion.

Dans les réseaux locaux, les commutateurs posent un problème. En effet, le fait qu'un commutateur ne parvienne pas à assurer un bon filtrage des accès des informations contenues en en-têtes des trames des couches réseau, transport ou application

(adresse *IP*[4], port *TCP*[5], etc.) a poussé les constructeurs à réfléchir à une solution qui puisse assurer la confidentialité des données. C'est la raison qui a fait que la meilleure solution était de remplacer dans cette architecture le commutateur par un routeur. Ce dernier est capable non seulement d'appliquer un filtrage évolué, mais aussi de découper le « domaine de diffusion » en sous-domaines. Malheureusement, l'utilisation d'un routeur pour interconnecter des sous-réseaux présente lui aussi quelques inconvénients. En voici quelques-uns :

- Une augmentation de la lenteur des communications entre les sous-réseaux : là où le commutateur se contentait d'aiguiller la trame, le routeur doit traiter l'en-tête du paquet contenu dans la trame.

- Une gestion plus compliquée des adresses *IP*, à cause du découpage en plusieurs domaines *DHCP*, chacun ayant son propre serveur *DHCP*. Il faut remarquer que certains routeurs peuvent assurer eux-mêmes la fonction de serveur *DHCP*. *DHCP* est le sigle de *Dynamic Host Configuration Protocol* qui est un service mis en œuvre dans un réseau pour fournir automatiquement des adresses IP à un dispositif qui s'y connecte.

- Une flexibilité réduite : une machine qui se déplace entre deux sous-réseaux ne peut pas, en général, garder son adresse réseau *IP*, *IPX*, etc. Aussi, la connexion des machines à un concentrateur – et, par conséquent, le découpage en sous-réseaux – se fait en général sur un critère de proximité physique, qui ne correspond pas toujours aux découpages organisationnels et donc aux besoins de filtrage d'accès.

Il fallait donc qu'une nouvelle technologie soit développée pour pallier ces insuffisances. C'est ainsi qu'ont vu le jour les réseaux locaux virtuels ou *VLAN*. Les *VLAN* ont apporté des solutions, parfois partielles, à ces problèmes plutôt complexes. En effet, grâce aux *VLAN*, il est maintenant possible de déconnecter la structure logique des groupes de travail de la structure physique des supports réseau. Au départ, ce type de réseau était basé sur des solutions propriétaires, mais le développement de normes IEEE 802.1Q a permis de garantir de nos jours une certaine interopérabilité. Le but de la norme 802.1Q impose aux *VLAN* d'être compatibles avec les protocoles *MAC* de tous les standards *LAN* de la série 802 (*Ethernet*, *token ring*, *FDDI*, *fast Ethernet*, *Gigabit*, etc.).

Un *VLAN* fait donc appel à des commutateurs de nouvelle génération, du même type qu'*Ethernet*, ou de technologie hétérogène, et qui sont interconnectés par un réseau fédérateur à haut débit (*fast Ethernet*, *gigabit Ethernet*, *FDDI*, *ATM*). Un aspect très important des *VLAN* est qu'ils peuvent se limiter à un seul commutateur ou relier des machines distantes, connectées à des commutateurs différents. Ainsi, les « domaines de diffusion » correspondent aux *VLAN* individuels. Même si la connexion d'une machine à un commutateur se fait sur un critère de proximité physique, cela n'empêche pas cette machine de faire partie d'un même *VLAN* que des machines connectées à un autre commutateur. En plus des commutateurs qui permettent aux *VLAN* de fonctionner (*VLAN aware*), des équipements d'interconnexion, qui fonctionnent indépendamment

---

4 Une adresse IP (*Internet Protocol*) est un mécanisme permettant l'identification d'une machine sur un réseau.

5 Un port TCP (*Transmission Control Protocol*) est un port d'accès de service de la couche transport à la couche application.

des *VLAN* (*VLAN unaware*), peuvent continuer « d'exister » dans le réseau, à condition de les dédier à des *VLAN* individuels.

Ainsi, lorsqu'un commutateur *VLAN aware* reçoit une trame en provenance d'une station, il lui ajoute une étiquette (*tag*) de format fixe. L'étiquette peut dépendre du numéro de port sur lequel la trame est arrivée, de l'adresse physique l'émetteur, ainsi que d'autres informations contenues dans les en-têtes à différents niveaux. Le commutateur est capable de gérer des informations contenues dans les en-têtes des couches de niveau supérieur à 2, ce qui fait que le commutateur n'est donc plus vraiment un équipement de niveau 2. La vitesse de la commutation peut malheureusement en être affectée. L'étiquette permet à un *VLAN* d'en identifier l'émetteur afin de lui attribuer éventuellement un niveau de priorité pour la communication. La trame étiquetée est ensuite transmise au commutateur *VLAN aware* suivant, qui prend en compte les informations contenues dans l'étiquette afin que le traitement approprié lui soit appliqué. Selon que le nœud suivant est *VLAN aware* ou *VLAN unaware*, l'étiquette reste associée ou est enlevée à la trame par le commutateur.

Tous les commutateurs qui participent à l'implémentation des *VLAN* sur un réseau de niveau support partagent des tables de filtrage (*filtering database*) qui indiquent l'appartenance des différentes machines aux *VLAN* et la localisation physique des machines. Ces tables sont en partie définies par l'administrateur du réseau et en partie actualisées dynamiquement au cours du fonctionnement comme pour certains *VLAN*, en cas de déplacement d'une machine.

Les types de fonctionnement des VLAN

Pour ce qui concerne le fonctionnement, nous pouvons distinguer différents types de *VLAN*.

- *Les VLAN de niveau 1 basés sur les numéros des ports*. Dans ce cas, l'appartenance d'une machine à un *VLAN* dépend du numéro du port par lequel elle est connectée au commutateur. Cette technique n'est pas souple, dans la mesure où, à chaque fois qu'il faut déplacer une machine, il faut redéfinir son appartenance au *VLAN*. De plus, dans certaines configurations, il est difficile d'assurer une séparation stricte entre les *VLAN* : une machine peut éventuellement recevoir des trames qui ne sont pas destinées au *VLAN* auquel elle appartient.

- *Les VLAN de niveau 2 basés sur l'adresse MAC IEEE 802* (ou adresse « physique »). Dans ce cas, l'appartenance d'une machine à un *VLAN* dépend de l'adresse *MAC* (*Ethernet*, etc.) de la machine. Un très bon niveau de sécurité peut être assuré car l'adresse *MAC* est intrinsèque à la carte réseau de la machine, et ne peut donc pas être modifiée par un utilisateur malveillant. De plus, si la machine est déplacée, les tables de filtrage peuvent être mises à jour de façon automatique, donc l'administration du *VLAN* en est simplifiée. En revanche, définir au départ des *VLAN* à partir des adresses *MAC* est extrêmement fastidieux, car les adresses *MAC* ne sont pas structurées et il faut donc les entrer une par une.

- *Les* VLAN *de niveau 2 basés sur l'identité du protocole de niveau supérieur indiquée dans l'en-tête IEEE 802.2*. Cette technique peut être appliquée à condition d'avoir une hétérogénéité au niveau des protocoles de niveau 3. Elle présente un intérêt dans la mesure où elle permet de restreindre les « domaines de diffusion » aux machines dont les protocoles réseau font un usage fréquent de la diffusion (*IPX*, *Appletalk*, etc.), diminuant ainsi l'impact négatif de celui-ci sur les autres machines du réseau.

- *Les* VLAN *de niveau 3 basés sur l'adresse de niveau 3 (*IP*, numéro réseau* IPX*, etc.)*. Toute l'adresse de niveau 3 ou une partie seulement, le numéro de sous-réseau, peut être employée pour définir l'appartenance d'une machine à un *VLAN*. Même si la machine est déplacée, elle garde son adresse de niveau 3 et donc son appartenance à un *VLAN*. Dans la mesure où l'adresse de niveau 3 peut être modifiée par un utilisateur malveillant (pour changer de *VLAN*), cette technique peut poser des problèmes de sécurité. De plus, l'obligation pour un commutateur de regarder l'adresse dans l'en-tête de niveau 3 augmente sa latence. En général, les commutateurs utilisés n'assurent aucune fonction de routage et font appel à l'adresse de niveau 3 uniquement pour déterminer le *VLAN* auquel appartient la machine. La définition d'un *VLAN* à partir des adresses de niveau 3 est simplifiée grâce à la structure logique hiérarchique de ces adresses (numéro de réseau, numéro de sous-réseau, …, numéro de machine).

- *Les VLAN de niveau supérieur, basés sur différentes informations présentes dans les en-têtes successifs de niveau 3, 4, ou plus*. La nécessité de rechercher des informations dans des en-têtes successifs, parfois de format variable, augmente de façon sensible le temps de réponse des commutateurs.

Nous voyons ainsi que la définition des *VLAN* permet de séparer des groupes de machines du point de vue des accès physiques. Par ailleurs, l'accès à des machines depuis plusieurs *VLAN* (serveurs, postes d'administration) existe aussi, bien que en général source de problèmes pour des *VLAN* de type 1.

Nous remarquerons que l'étiquetage peut être implicite; rien n'est ajouté à la trame, quand un seul commutateur intervient dans la communication, ou quand le fonctionnement du *VLAN* est de type 2, 3, 4 ou 5. Toute l'information est déjà présente dans la trame. Afin de diminuer le temps de réponse, il peut être intéressant d'utiliser des étiquettes explicites même pour ces *VLAN* : l'appartenance à un *VLAN* est déterminée à l'entrée de la trame dans le premier commutateur (temps de réponse élevé), les autres commutateurs ne regardent plus que l'étiquette (temps de réponse minimal).

Le marché des VLAN

Le choix d'un type de fonctionnement et d'un mode de définition des *VLAN* doit être fait après une étude approfondie de l'utilisation du réseau. Une solution qui allie performance, flexibilité, sécurité et facilité d'administration est celle qui assure un fonctionnement de type 2 (basé sur l'adresse *MAC*), tout en permettant une définition des *VLAN* à partir des adresses réseau, plus faciles à gérer que les adresses *MAC*.

L'offre commerciale est arrivée à maturité et le choix est vaste; les solutions non propriétaires peuvent être privilégiées dans un milieu en évolution rapide, où l'interopérabilité est une contrainte forte. Il n'en demeure pas moins que les *VLAN* restent encore des solutions propriétaires.

Les constructeurs qui proposent des solutions *VLAN* sont les acteurs majeurs du marché des commutateurs, à savoir Cisco, 3Com, Bay Networks, IBM, etc. Ils ont tous voté en faveur de la proposition 802.1Q. Malgré tout, en raison de la variété des types de *VLAN*, il n'est pas surprenant que chaque constructeur ait développé sa propre solution *VLAN* propriétaire. Ainsi, les commutateurs d'un constructeur ne pourront interopérer complètement avec les *VLAN* d'un autre. Il y a cependant une exception : c'est le cas où les *VLAN* sont implémentés en conjonction avec un réseau fédérateur *ATM* et l'émulation *LAN*.

Parmi les avantages offerts par les *VLAN* dans la mise en place des réseaux, on peut ainsi distinguer :

- la réduction de la charge des trafics en minimisant les domaines de diffusion dans un réseau;
- la formation de groupes virtuels;
- l'augmentation de la sécurité;
- la simplification de l'administration;
- la réduction des coûts.

Le stockage des données centralisé (*Storage Area Network – SAN*)

Les administrateurs de réseaux doivent avoir en permanence une vision claire et précise de l'ensemble des infrastructures composant leur réseau. Or, la multiplication des serveurs et des stations de travail rend l'obtention d'informations cohérentes et facilement exploitables très difficile à gérer. Afin de pallier cet inconvénient, on peut songer à une technologie qui rapatrie toutes les informations indispensables à la compréhension du fonctionnement des réseaux (*LAN* et *WAN*), et les stocker dans une base de données centrale. Le stockage des données centralisé doit ainsi permettre aux administrateurs des réseaux d'avoir une vision globale des ordinateurs, des groupes locaux de partage, des configurations réseau, des utilisateurs des différents services installés, des configurations *TCP/IP*, des groupes globaux, des fichiers de marquage dynamique des blocs défectueux d'un disque dur communément appelés *hotfixes*, (des BIOS …Ce sont là les défis que veulent relever les *SAN – Storage Area Network*.

Le stockage des données est devenu une affaire de réseau. Ainsi, d'après la société Auspex, en 1999, 92 % des données stockées dans le monde étaient encore directement rattachées aux serveurs et aux postes clients. Mais, croissance exponentielle des volumes oblige, les réseaux de stockage (*SAN*) se taillent désormais la part du lion dans les nouvelles applications. Corollaires de cette montée en puissance du stockage détaché des serveurs, les légitimes inquiétudes des utilisateurs : le transit des données par le réseau ne nuit-il pas à la fiabilité? Et la confidentialité? Comment contrôler l'accès aux données quand les ressources de stockage sont mutualisées? Sur tous ces problèmes liés à la sécurité, les directions informatiques peuvent s'en remettre aux architectures de stockage dernier cri, sous réserve cependant de quelques précautions.

De l'avis des constructeurs

Une architecture redondante

Le *SAN* est « la » solution de stockage sécurisée par excellence. La fibre optique alors utilisée permet de délocaliser un centre de sauvegarde, qui peut se trouver jusqu'à soixante kilomètres du site. Alors qu'avec une interface *SCSI*, la distance est limitée à quelques dizaines de mètres. Grâce au *SAN*, on peut entreposer les données vitales pour l'entreprise dans de véritables bunkers, dont la localisation est peut être gardée secrète. En outre, le réseau de stockage offre un excellent niveau de fiabilité.

La fibre optique utilisée pour les liaisons est un moyen de transmission en série, réputé plus fiable que les moyens de transmission parallèles, utilisés par exemple pour le *SCSI*. Le protocole *Fibre Channel* a été spécialement conçu pour le stockage, avec le souci que les données soient transportées avec fiabilité et dans l'ordre. C'est un protocole déterministe, par opposition à *Ethernet*, par exemple. Autrement dit, le temps de transmission des données est prévisible. De plus, à la différence d'*Ethernet*, *Fibre Channel* présente l'avantage de ne pas être ouvert sur Internet, ce qui limite les risques d'intrusion et d'accès inopportun aux données de l'entreprise.

Compartimenter les baies de stockage

La connectique du *SAN* est également très fiable en raison de l'architecture généralement redondante des réseaux de stockage, à tous les niveaux.

Chaque serveur est relié par deux liens à deux commutateurs. Il existe néanmoins un risque pour la sûreté des données inhérent au *SAN*, qui n'existe pas lorsque le stockage est directement attaché aux serveurs. Comment s'assurer en effet que le serveur A n'accède pas aux données du serveur B quand ils partagent tous deux une baie de stockage? En fait, un serveur sous Windows NT ne peut lire les données d'un grand système. Mais il existe quand même un risque qu'il ait accès à l'espace physique où sont stockées les données, par exemple qu'il reformate la zone attribuée aux données du grand système. Il faut donc cloisonner la baie : c'est ce qu'on appelle le *zoning*.

Les outils d'administration réalisant cette fonction peuvent être situés sur les serveurs (par exemple, les logiciels *Sanergy*), les commutateurs (par exemple, les solutions de *Brocade*), ou encore les baies de stockage (par exemple, les applications *EMC*). Enfin, les risques liés à l'utilisation d'un réseau de stockage sont analogues à ceux des réseaux classiques. Le réseau centralisé de stockage est comme le miroir du réseau local. De même que dans le second, plusieurs clients sont reliés à un serveur, dans le premier, ce sont plusieurs serveurs qui partagent une baie de stockage. Alors que dans un réseau local, on doit définir des règles de protection des interactions entre les portes clients, dans un réseau centralisé de stockage, c'est entre les serveurs que ça se passe. Dans les deux cas, on a besoin d'outils d'administration pour réaliser ces fonctions.

Du point de vue des gestionnaires

Des solutions réseau *SAN* spécifiques aux stockages sont proposées visant les moyens de stockage et les serveurs. Est-ce que ces nouvelles technologies « réseaux » apportent quelque chose aux systèmes d'information des entreprises?

Au sujet des connexions des systèmes de stockage, deux architectures sont possibles :

- les baies de stockage directement connectées au réseau en utilisant des cartes *Ethernet*;

- les baies de stockage derrière des serveurs maîtres, en utilisant soit des interfaces *SCSI* ou *Fibre Channel*. Dans ce dernier cas, les baies pourraient constituer un réseau de stockage *SAN*, formé de commutateurs et de concentrateurs spécifiques.

Les figures suivantes comparent ces types de réseaux.

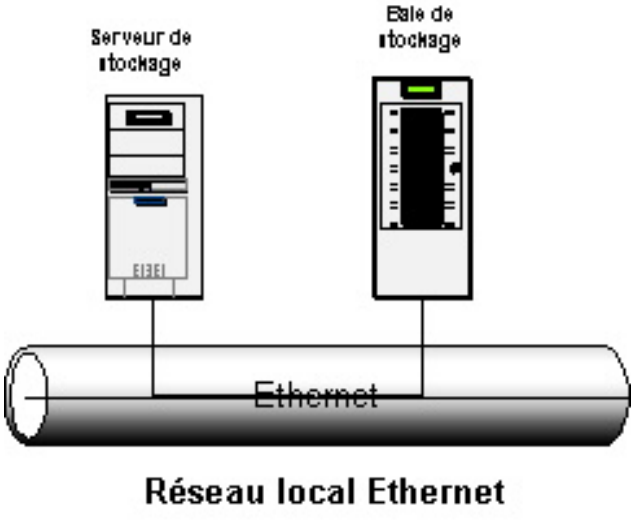

Figure 10 : Architecture en réseau *Ethernet*

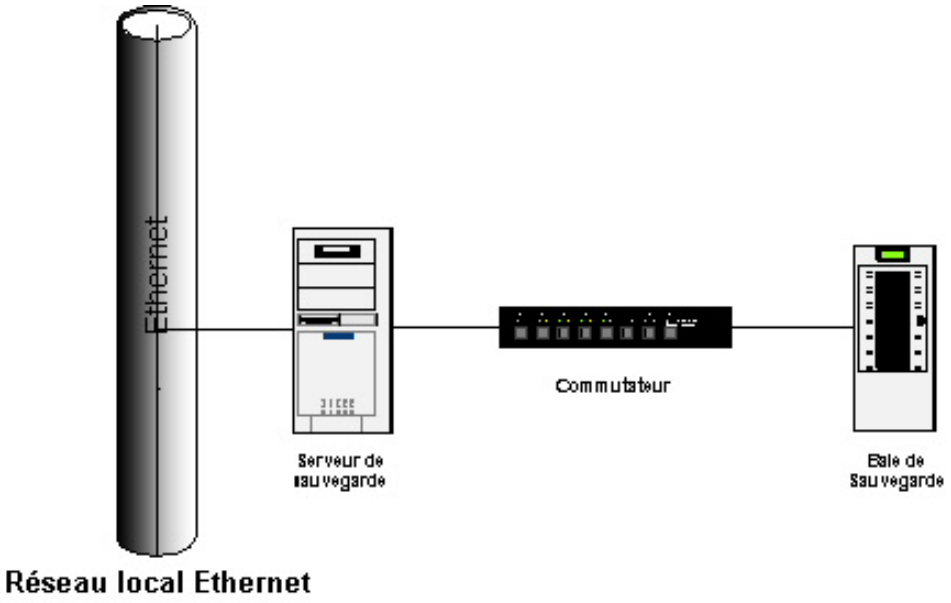

Figure 11 : Architecture en réseau *SAN*

Quelques critères d'évaluation de la technologie *SAN* :

Équipements	Les équipements *SAN*, interface, commutateur, etc., sont 5 à 10 fois plus chers que les équipements réseau *Ethernet* (voire plus). Dans beaucoup de cas, les investissements ne sont pas toujours nécessaires. Dans le cas de l'architecture réseau *Ethernet*, le serveur de stockage est déjà connecté sur le réseau, il y a une disponibilité des ports sur *Ethernet*, le câblage existant est utilisable, etc.
Débit	Les réseaux *Ethernet* à haut débit et les réseaux *SAN* ont des débits comparables (de 100 Mbps à Gbps).
Disponibilité	La disponibilité est améliorée en dédoublant (redondance) les équipements. Dans le cas du réseau *SAN*, il faut dédoubler non seulement les cartes *FC*, mais aussi les cartes réseau *Ethernet* du serveur. On se retrouve ainsi avec quatre cartes (deux connexions *Ethernet* et deux connexions *SAN*).
Gestion de réseau	Non seulement faut-il mettre en place une gestion du réseau *Ethernet* (et *IP*) avec un des outils classiques du marché *SNMP*, mais il faut aussi mettre en place une gestion technique plus spécifique au réseau *SAN*.
Compétences/Maintenance	Il faut développer et maintenir des compétences internes pour gérer le réseau *SAN* et les contrats de maintenance particulière à ce réseau.

Conclusion

Tout au long de ce chapitre, nous avons expliqué les réseaux informatiques à partir de leurs composantes et de leurs fonctions ainsi que des règles, normes et standards qui les régissent. Il ressort de cette étude que la principale entité de standardisation est l'ISO. En effet, l'ISO renferme un groupe de normes pour les protocoles qui ont été normalisés dans une structure logique afin d'exécuter des processus réseaux. Cependant, le modèle OSI est souvent considéré comme un modèle conceptuel. Cela signifie qu'il n'est pas absolument respecté dans le fonds. De nombreux protocoles peuvent être associés à plus d'une couche (ex. : le protocole NCP se retrouve dans les couches Présentation et Session). Ainsi, le fait que les chercheurs aient opté, tout en s'inspirant du modèle OSI, d'un modèle *TCP/IP* ne doit pas tellement surprendre.

Nous avons aussi étudié, sommairement, le stockage centralisé des données. C'est une architecture complexe. Le stockage est accessible à travers un réseau qui lui est spécialement dédié. Sa principale fonction est de fournir aux serveurs un stockage consolidé basé sur un canal spécial dénommé le « *Fibre Channel* ». Le stockage centralisé des données est idéal pour les bases de données et le traitement des transactions en ligne. Des composants matériels et logiciels redondants donnent au système une haute disponibilité.