



EXPOSE RESEAUX : SAN ET NAS

Exposé Réseaux : SAN et NAS – 3^{ème} année - Ingénieurs 2000

JASON – LESZKO – FOREL

INTRODUCTION

La maîtrise de l'information est un défi permanent pour chaque entreprise informatisées. Le volume de données stockées subit une croissance exponentielle qui peut atteindre 100% par an. Les applications de messageries et de bases de données sont de plus en plus volumineuses ce qui offrent des performances de plus en plus dégradées. Les opérations de sauvegarde doivent être effectuées dans un temps de plus en plus réduits. L'interopérabilité des données sur des plates-formes hétérogènes doit être assurées. C'est autant de problèmes qui montrent les limites des architectures actuelles.

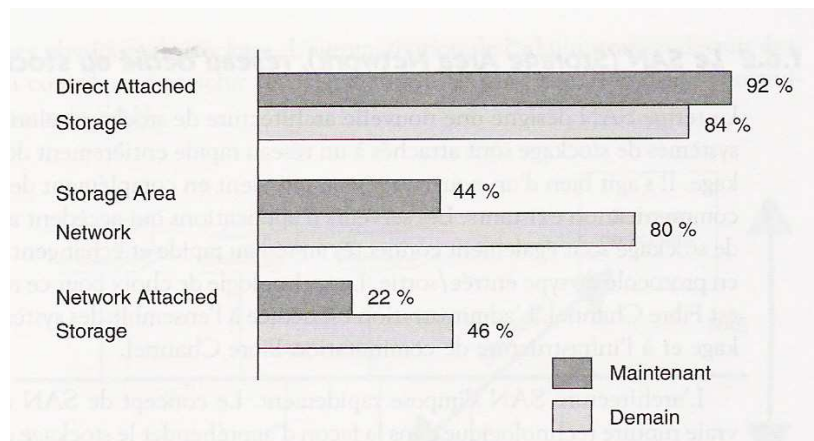
Il faut savoir que les hommes ont produit plus d'informations durant ces 30 dernières années que pendant les cinq mille ans qui les ont précédés. Cette évolution exponentielle double tous les 12 à 18 mois. Par exemple, un simple message électronique, de renvois en renvois, peut aboutir à la création de l'équivalent d'un téraoctet de données.

Pour supporter l'évolution de cette masse de données, il a fallu agir sur plusieurs critères:

- ◆ Augmenter les capacités des supports de stockage
- ◆ Eviter les pertes de productivités dû au ralentissement de l'outil informatique
- ◆ Avoir une meilleur administration des systèmes de stockage
- ◆ Sauvegarder les données de plus en plus vite
- ◆ Administrer efficacement des ressources hétérogènes
- ◆ Protéger l'information contre les sinistres

Pour ce faire, plusieurs architectures de stockage et de sauvegarde des données ont vu le jour. Deux conceptions sont en tête des solutions de stockage en réseau : le NAS (Network Attached Storage) et le SAN (Storage Area Network). La figure suivante nous montre la montée en puissance de ces 2 conceptions. Elle est tirée d'un questionnaire proposé aux 50% des 3500 plus grande entreprises américaines en 2003/2004.





Evolution des systèmes de stockage

Les NAS sont des systèmes de stockage qui viennent se connecter sur les réseaux d'entreprise existant tels qu'Ethernet. Ils se comportent alors comme serveur de fichiers. Le mode de communication s'appuie alors sur les protocoles réseaux comme TCP/IP. L'administration du stockage se fait à travers des agents implantés dans les serveurs.

Les SAN est une nouvelle architecture de stockage selon laquelle les systèmes de stockage sont attachés à un réseau rapide entièrement dédié au stockage. C'est un nouveau réseau qui vient en complément d'un réseau existant. Le Fibre Channel est la technologie de choix pour ce réseau. Grâce à ce type d'architecture apparaît le terme de virtualisation qui rend l'espace logique des données indépendant des systèmes physiques de stockage. L'automatisation de l'administration enrichit considérablement les solutions de stockage construites autour du SAN.

	NAS	SAN
Réseau	Réseau existant (Ethernet, FDDI,...)	Réseau dédié (Fibre Channel)
Fonction	Serveur de fichiers Gestion multi protocoles	Serveur de ressources de stockage Aide à la protection, au partage et au mouvement des données
Protocole	Type message (TCP/IP)	Type E/S (SCSI,...)
Bande passante	Ethernet haut débit, FDDI, ATM	Fibre Channel (10Gbits/s) Dépend aussi de l'architecture (Fabric, FC-AL)
Administration	Via le serveur	Directe, dans l'infrastructure réseau

Différences SAN et NAS

TABLE DES MATIERES

INTRODUCTION	2
TABLE DES MATIERES	4
1 NAS	6
1.1 PRINCIPE.....	6
1.2 CRITERES DE CHOIX	7
1.3 PORTRAIT-ROBOT	8
2 SAN	10
2.1 PRINCIPE.....	10
2.1.1 <i>Un réseau dédié</i>	10
2.1.2 <i>Du SCSI au FC-AL</i>	11
2.1.3 <i>Des concentrateurs aux commutateurs</i>	11
2.2 DIFFÉRENTES TOPOLOGIES	12
2.2.1 <i>Architecture point à point</i>	13
2.2.2 <i>Architecture de type boucle arbitrée (Fibre Channel Arbitrated Loop)</i>	13
2.2.3 <i>Les commutateurs</i>	15
2.2.4 <i>SAN : de nombreux avantages</i>	16
3 FIBRE CHANNEL	17
3.1 COUCHE FC-0.....	19
3.2 COUCHE FC-1.....	20
3.2.1 <i>Architecture</i>	20
3.2.2 <i>Conversion des caractères FC-1</i>	20
3.2.3 <i>Les règles de codage</i>	20
3.3 COUCHE FC-2.....	21
3.3.1 <i>Le jeu de commandes</i>	21
3.3.2 <i>Les trames</i>	22
3.3.3 <i>La séquence</i>	23
3.3.4 <i>Les échanges</i>	23
3.3.5 <i>Protocole</i>	24
3.4 COUCHE FC-3.....	25
3.5 COUCHE FC-4.....	25



4	VIRTUALISATION.....	26
4.1	DÉFINITION	26
4.2	RAID.....	26
4.3	SAN IN A BOX	28
4.4	SERVEURS DE DOMAINES VIRTUELS.....	29
4.5	METASERVEURS.....	31
5	INTERNET FIBRE CHANNEL PROTOCOL (IFCP).....	33
5.1	POURQUOI LE PROTOCOLE IFCP ?.....	33
5.2	LE MODELE DE RESEAU IFCP.....	34
5.3	ARCHITECTURE D'UNE PASSERELLE.....	35
6	SCSI OVER IP (ISCSI).....	36
6.1	LE MODELE DU PROTOCOLE ISCSI.....	37
	CONCLUSION.....	38

1 NAS

1.1 Principe

Un système de type NAS ressemble à un ensemble de disques durs installés dans une plateforme matérielle directement connectée au réseau local de l'entreprise. Elle dispose de sa propre adresse réseau. Les utilisateurs accèdent directement aux fichiers qui y sont enregistrés ou passent par le serveur d'application. Ce dernier se charge de la redirection des requêtes. Les plates-formes fonctionnent sur le même principe qu'un serveur de réseau traditionnel. Elles offrent l'avantage d'une réelle autonomie fonctionnelle, par opposition au stockage habituel qui réside physiquement à l'intérieur du serveur de réseau. Une plate-forme NAS est vue comme un poste client parmi d'autres. La possible différence est qu'elle nécessite une IP fixe.

Les NAS offrent également la possibilité de multiplier simplement la capacité de stockage en lui ajoutant des disques durs, voire d'ajouter une seconde baie de disques à la première. Elle sera alors considérée comme faisant partie intégrante de la première. Si jamais cela ne suffit pas, il est possible d'y ajouter un autre système de fichiers indépendant.



Exemple de NAS

Un autre avantage du SAN est la rapidité. En rendant l'accès aux données et son administration autonomes par rapport au serveur du réseau, les applications et les fichiers peuvent être disponibles aux utilisateurs plus rapidement, car ils ne disputent pas les ressources processeur du serveur.

Une solution NAS regroupe plusieurs éléments. Outre la batterie de disques durs et une architecture matérielle généralement comparable à un serveur renforcé, elle inclut son propre système de gestion de fichiers, un logiciel spécifiquement conçu pour le stockage distribué (déploiement, gestion, administration) et, le plus souvent, un sous-système RAID pour la sécurisation en temps réel.

Si la mise en place d'un NAS est relativement simple, le déploiement d'une solution de ce type nécessite souvent la mise à jour des réseaux locaux afin d'éviter qu'ils se révèlent être un goulot d'étranglement.

1.2 Critères de choix

◆ Interventions à chaud

Il existe de nombreuses raisons d'intervenir sur un système NAS: remplacement d'un composant défaillant, maintenance préventive, augmentation de la capacité d'un sous-système RAID... Il faut veiller à ce que le système permette de faire tout cela sans bloquer tous les utilisateurs du réseau.

◆ Reconstruction d'un disque de secours

Les constructeurs ont largement optés pour le RAID 5. Le spare-disk permet de maintenir l'accessibilité des données temporairement à partir d'un serveur ou d'un second système NAS si le premier doit être arrêté. La reconstruction est entièrement automatisée afin d'éviter les erreurs de manipulation et les oublis.

◆ Systèmes d'alerte

Il en existe de plusieurs sortes, à commencer par les alarmes de type SNMP. Ces dernières sont consolidées dans des logiciels d'administration, soit livrés avec les serveurs de fichiers, soit commercialisés par des éditeurs tiers. D'autres systèmes d'alertes existent: Appel d'un numéro de téléphone, e-mail, pager...).

◆ Fonctions d'administration

La surveillance des grappes (groupes de disques durs), des volumes (espace de stockage alloués à certaines données particulières), des dossiers partagés et du niveau de performance est indispensable. Toutes les informations livrées en standard dans l'outil d'administration doivent être présentes. Il est judicieux de se doter d'un logiciel d'administration de réseau et système pour recouper les informations du NAS.



- ◆ Gestion des groupes d'utilisateurs

Un système NAS efficace doit permettre d'allouer des espaces de stockage différenciés et dotés de droits d'accès différents en fonction des utilisateurs et de leur appartenance à certains groupes.

- ◆ Configuration à distance

Indispensable pour un système réseau.

- ◆ Sécurité hiérarchisée

Une hiérarchie des mots de passe permet de sécuriser le système. Des droits différenciés selon les utilisateurs et les opérations à effectuer évite les dégâts malencontreux ou intentionnels.

- ◆ Accès directe au système de fichiers

En cas de panne, il est indispensable d'avoir accès direct aux systèmes de fichiers pour récupérer rapidement des données critiques et économiser beaucoup de temps.

- ◆ Simplicité de déploiement

Certaines sociétés veulent faire croire que le système est compliqué à installer pour mieux vendre leur expertise. Il est possible de rencontrer des difficultés d'installation mais cela tient d'avantage à la nécessité de modifier les paramètres des serveurs et des postes clients que l'installation physique.

- ◆ Compatibilité avec les protocoles réseau

Les protocoles NetBEUI, NFS, CIFS doivent pouvoir être gérés. Cela permet d'éviter la réplication de données qui sont partagées entre les différents environnements.

- ◆ Compatibilité avec les systèmes d'exploitation

1.3 Portrait-Robot

- ◆ Performance

Un niveau de 30Mo/s constitue une bonne moyenne. Mais cette rapidité ne doit pas trop chuter si le nombre d'utilisateurs augmente. Un chiffre supérieur à 100 transactions par minute pour 50 utilisateurs simultanés peut être considéré comme très satisfaisant.

- ◆ Evolutivité

Certains systèmes NAS sont chaînables. Les meilleurs offrent plusieurs baies pouvant recevoir jusqu'à une trentaine de disques durs. Les modèles haut de



gamme acceptent 150 disques en tout. Mais cette capacité d'évolution interne s'obtient souvent au détriment de l'encombrement.

- ◆ Disques durs

Aujourd'hui, les disques Ultra 160 SCSI obtiennent de très bonnes performances.

- ◆ Mémoire vive

Attention aux systèmes NAS provenant de serveurs de réseau recyclés. La mémoire vive servira principalement de mémoire cache, divisant l'accès aux données.

- ◆ Connexions

L'idéal est un modèle équipés de connecteurs Gigabit pour les liaisons inter commutateurs, commutateurs serveurs et Fast Ethernet pour les liaisons avec les postes clients.

- ◆ Sous-systèmes RAID

Il faut prévoir au minimum 2,5 fois la capacité totale de tous les disques durs de tous les postes de votre réseau.

- ◆ Equipements redondants

Les systèmes NAS sont soumis à de fortes contraintes physiques: dégagements de chaleur des disques rapides, pics d'alimentation électrique exigeant une stabilisation... Le système doit posséder une alimentation et des ventilateurs redondants.

2 SAN

Il est apparu, dans les années quatre-vingt, que le moyen le plus efficace pour acheminer la puissance informatique aux utilisateurs passait par la mise en œuvre de réseaux dédiés, en lieu et place des connexions point à point entre les utilisateurs et les serveurs.

À l'origine, les réseaux de stockage (SAN ou Storage. Area Network) ont été conçus pour soulager les réseaux locaux (LAN) face à l'explosion de la masse des données produite par l'ère numérique.

À la fin des années quatre-vingt-dix, les taux de croissance des informations à stocker étaient de l'ordre de 100 % tous les douze à dix-huit mois. Et encore, pour les entreprises gravitant autour d'Internet, le volume doublait tous les trois à six mois. Ces besoins commencent à dépasser les capacités des infrastructures LAN les plus perfectionnées. Les sauvegardes sur bandes représentent, dans certains cas, jusqu'à 65% du trafic du réseau local. À cela s'ajoutent les fenêtres de sauvegarde qui ne cessent de s'accroître et pouvant durer, dans certaines entreprises, plus de vingt-quatre heures. Dans ce cas, les administrateurs ne peuvent plus assurer la sauvegarde exhaustive des données avec les risques que cela comprend. C'est pourquoi, en dehors des environnements grands systèmes, la percée s'est opérée autour du Fibre Channel. Ce n'est donc que récemment (1998) que la mise en oeuvre de réseaux de stockage a pu vraiment débiter.

2.1 Principe

2.1.1 Un réseau dédié

Les SAN sont des réseaux dédiés qui affranchissent les réseaux locaux d'entreprises des charges que représentent le stockage et la sauvegarde des données. Les LAN retrouvent donc leur but premier, à savoir assurer la circulation rapide d'informations d'un équipement à un autre. De leur côté, les SAN possèdent maintenant leur propre intelligence et assurent un rôle primordial dans la continuité opérationnelle. En effet, ils assurent une disponibilité permanente des données, vingt-quatre heures sur vingt-quatre, sept jours sur sept. Ainsi, les SAN libèrent les réseaux locaux qui retrouvent 100 % de leurs capacités pour les utilisateurs et les applications.



2.1.2 Du SCSI au FC-AL

Pendant près de vingt ans, la majorité des systèmes distribués ont exploité l'interface de stockage parallèle SCSI (Small Computer Systems Interface). Ce dernier n'a une portée que de quelques dizaines de centimètres et ne permet donc de connecter qu'un nombre limité d'équipements. De plus, la connexion directe a également pour conséquence de dégrader fortement les performances lors des transferts de données.

L'interface SCSI s'est donc révélé être, à l'usage, inadaptée aux besoins dévolution, de performance et de distance des grandes infrastructures de stockage.

Toutefois à partir de 1985, tout a changé avec l'avènement du câblage fibre optique. Cette solution fut commercialisée pour la première fois sous le nom de Escon. Cette dernière, peut être considérée comme étant un prototype du SAN, sachant qu'à l'époque, la notion de stockage en réseau n'existait pas. Par la suite, le Fibre Channel Arbitrated Loop (FC-AL), basé sur cette nouvelle technologie s'est rapidement imposée comme étant le standard de fait du SAN. Proposant des débits atteignant plusieurs centaines de mégaoctets par seconde, elle permet de relier sans problème des milliers d'équipements sur des distances atteignant 100 km.

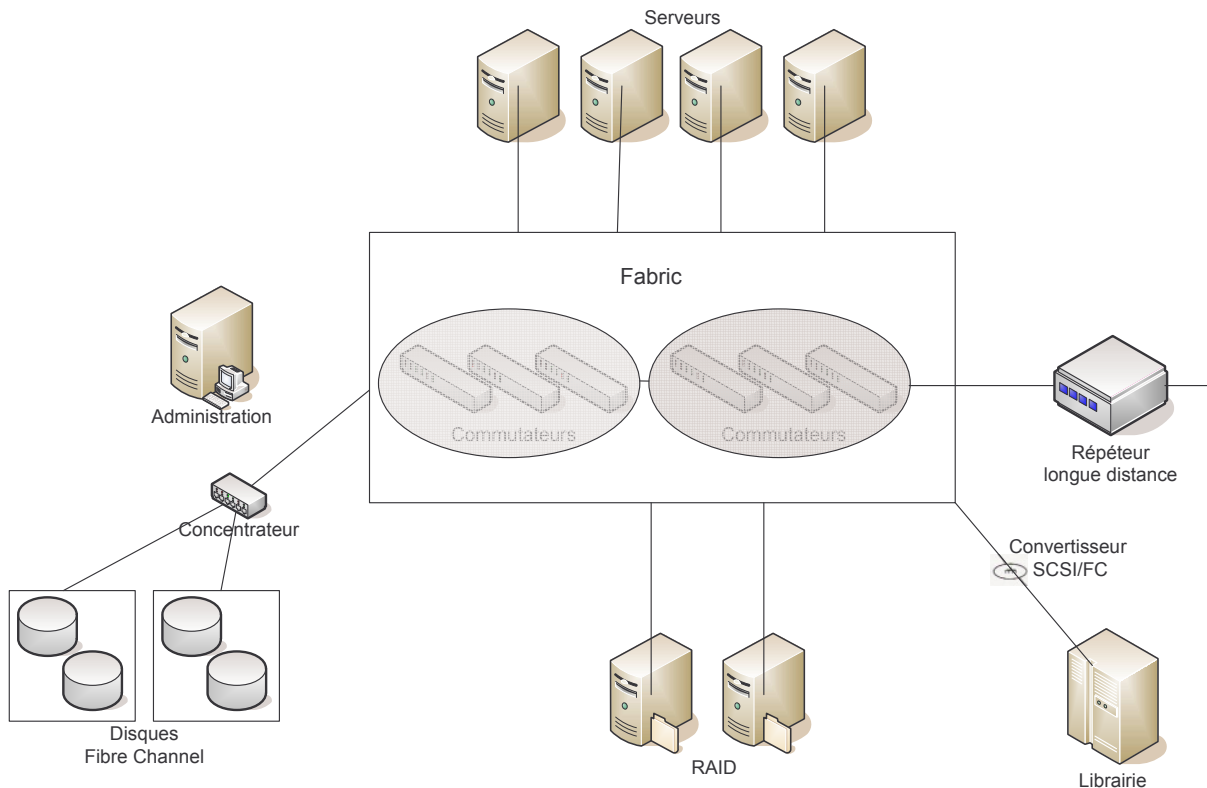
Les SAN dotés de la technologie Fibre Channel et de ses différentes moutures (comme FC-AL) permettent de déporter aisément et en toute sécurité les données sur des sites éloignés.

C'est pourquoi les grands industriels, opérateurs de télécommunications ou les sociétés internationales ont recours aux technologies SAN pour bâtir leur plan de reprise après sinistre et de continuité opérationnelle.

2.1.3 Des concentrateurs aux commutateurs

Les premiers SAN étaient bâtis avec des concentrateurs (hub) Fibre Channel. Les commutateurs Fibre Channel se sont très rapidement imposés, repoussant les concentrateurs sur les étagères des entrepôts. En effet, les réseaux commutés permettent de supporter sans problème les fortes montées en charge et les sollicitations intensives.

Aujourd'hui un réseau SAN basé sur des commutateurs pourrait se présenter de la manière suivante :



2.2 DIFFÉRENTES TOPOLOGIES

Comme toutes les technologies de communication, Fibre Channel n'a cessé d'évoluer au fil du temps. Ces évolutions ont eu un impact fort au niveau des topologies du réseau SAN. Ils proposent maintenant sans sourciller des bandes passantes de 2 Gbits/s pour les liaisons classiques. Certains montent à 10 Gbits/s. Cette vitesse est surtout utilisée pour relier deux sites entre eux ou pour bâtir un backbone (épine dorsale) réseau. Seulement, ce grand bond en avant entre les connexions point à point et les réseaux commutés a nécessité une étape. La boucle arbitrée Fibre Channel constitue ce passage obligé. Nous verrons donc les trois architectures des réseaux SAN.

2.2.1 Architecture point à point

Cette architecture est la plus simple de toutes les topologies SAN existantes. Elle consiste à relier deux N_Ports entre eux afin d'y établir une connexion. La bande passante est donc entièrement dédiée aux deux équipements qui souhaitent communiquer entre eux. Ils disposent de 1 Gbit/s dans les deux directions. Cette architecture a été la première à être mise en oeuvre. Elle se retrouve encore dans le monde des systèmes mainframes. Son principal défaut réside dans son manque de souplesse pour suivre l'évolution des besoins. En effet, à chaque ajout d'un équipement, il faut tirer des liaisons entre ce dernier et les équipements avec lesquels il doit dialoguer. Cela devient très vite ingérable. Autant dire que cette architecture réseau n'a presque plus cours aujourd'hui, à l'exception de quelques milieux spécifiques.



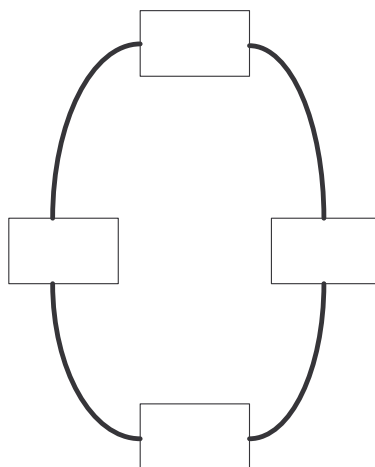
2.2.2 Architecture de type boucle arbitrée (Fibre Channel Arbitrated Loop)

Ainsi, après les connexions point à point, solution insuffisamment souple pour faire évoluer l'architecture et peu économique, les constructeurs ont concentré leur effort sur une architecture qui résolvait ces deux inconvénients majeurs. Celle-ci s'appelle boucle arbitrée Fibre Channel- Cette solution est économique et assure la mise en relation de plusieurs équipements entre eux. Pour cela, elle partage la bande passante, de 1 Gbit/s, entre tous les équipements reliés sur la boucle. Elle est toutefois limitée à 127 points de connexion. Cette architecture ressemble fort à la topologie appelée « partagée » dans les LAN et bâtie autour de concentrateurs.

L'équipement qui initie une demande sait qu'il a obtenu le contrôle de la boucle lorsqu'il reçoit sa propre adresse en écho à sa demande; c'est pour cette raison que cette architecture est dite « boucle arbitrée ». En cas de conflit de demandes, l'attribution de la boucle revient à l'équipement disposant de l'adresse la plus faible. L'équipement peut alors initier un échange bidirectionnel. Ce dernier s'opère uniquement entre deux N_Ports de la boucle.

Les équipements de stockage sont installés, de manière logique, en série sur la boucle, même si physiquement cela n'est pas évident. les boucles sont construites autour de concentrateurs (hubs) qui centralisent les attachements des divers appareils et rétablissent la continuité de la boucle en cas de détection des pannes.

La boucle Fibre Channel convient très bien aux périphériques de stockage qui intègrent les fonctions d'un FL_Port {Port Fibre Channel Arbitrated Loop) comme les disques par exemple. En effet, ces derniers équipements sont dotés de deux FL_Ports. Ces derniers peuvent à la fois recevoir ou émettre des données à la vitesse maximale de la bande passante, à savoir le Gbit/s. Toutefois, ils ne peuvent pas être opérationnels simultanément. Il est cependant possible d'installer des architectures doubles boucles. Dans ce cas, deux boucles sont déployées en parallèle, reliant les mêmes équipements. Ainsi, les deux FL_Ports peuvent être opérationnels simultanément. Avec ce type d'architecture, la bande passante passe de 100 Mo/s à 200 Mo/s, de quoi répondre à un large spectre de besoins. Seulement, la mise en place d'une telle solution s'avère onéreuse. En outre, les boucles restent toujours limitées à 127 points de connexion.



2.2.3 Les commutateurs

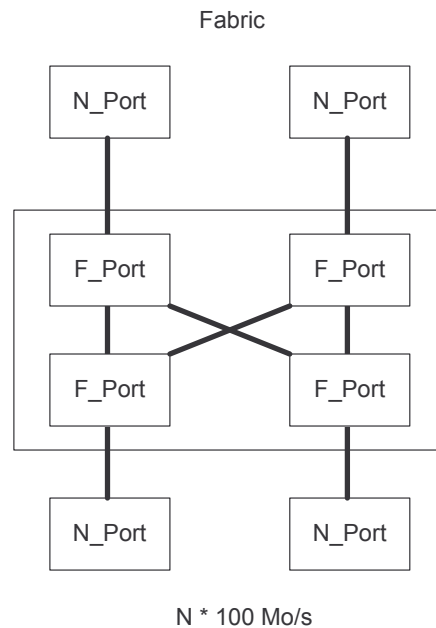
Ces équipements apportent les mêmes avantages aux SAN qu'aux réseaux locaux. La bande passante entre deux points de connexion est maintenant dédiée. Ils permettent donc d'exploiter au mieux la bande passante. De plus, les fonctions avancées assurent une plus grande sécurité. Il est possible de mettre en place des liaisons redondantes, qui assurent l'acheminement des données, même en cas de rupture d'une liaison. Dans les équipements de haute disponibilité, les parties vitales (alimentations, ventilateurs, etc.) sont redondantes, garantissant ainsi une parfaite continuité de service.

Les commutateurs offrent au Fibre Channel et aux réseaux SAN de sortir de leur confinement imposé par les connexions point à point et les boucles arbitrées. Les commutateurs étaient initialement utilisés pour interconnecter des boucles entre elles. La dimension d'un réseau SAN commuté est uniquement limitée par le nombre de points de connexion supportés par le système d'adresse. Ce dernier est codé sur 224 bits, ce qui représente potentiellement une palette de seize millions d'adresses.

La fonction première d'un commutateur consiste à aiguiller les trames reçues par un émetteur vers le bon destinataire. Pour cela, le commutateur analyse l'adresse de destination contenue dans la trame reçue puis lance une recherche dans sa matrice de commutation afin de trouver le bon chemin. De son côté, l'émetteur se contente de créer une liaison point à point avec le commutateur. Ce dernier assure ensuite la création d'une connexion point à point avec le destinataire. Toutefois, si ce dernier est occupé lors de la requête, le commutateur envoie un message « busy » à l'émetteur afin de le prévenir. Celui-ci reformulera sa demande après un délai d'attente.

Les commutateurs disposent aussi de mécanismes de gestion de classes de service qui correspondent aux cinq classes définies dans Fibre Channel.





2.2.4 SAN : de nombreux avantages

Après avoir utilisé les réseaux SAN comme des réseaux de stockage assurant la décongestion des réseaux locaux (LAN) et résolvant le casse-tête des fenêtres des sauvegardes, les entreprises découvrent de nouvelles vertus au SAN : la capacité d'évolution du réseau et de l'espace de stockage, les performances qui ne cessent de s'améliorer (le Fibre Channel 10 Gbits) et enfin la continuité opérationnelle.

3 FIBRE CHANNEL

L'objectif du Fibre Channel consiste à développer une approche pratique, apportant une bande passante suffisante, pour transférer des données entre les serveurs d'application, les mainframes, les mini, etc. Fibre Channel représente le nom générique pour une série de standards développés par l'American National Standards Institute (ANSI).

Il existe deux types de communications logiques pour les données : le type canal d'entrée/sortie (très souvent utilisé dans le monde du stockage avant l'arrivée du Fibre Channel - le protocole SCSI appartient à cette catégorie) et le type réseau (la pile TCP/IP appartient à cette famille). Une communication de type canal fournit une connexion directe ou commutée entre les différents équipements qui échangent des informations. À l'inverse, les réseaux de communication s'apparentent à une agrégation de nœuds (station de travail, serveurs de fichiers, périphériques, etc.) avec un ou plusieurs protocoles de communication qui établit un dialogue entre eux.

Le projet Fibre Channel est ambitieux puisque les protocoles le composant ont pour objectif de reprendre le meilleur des deux mondes dans une interface d'entrée/ sortie qui réponde à la fois aux besoins des utilisateurs de communication de type canal et à ceux des réseaux.

Bien qu'elle soit appelée Fibre Channel, cette architecture ne s'apparente en aucun cas à celle de type canal d'entrée/sortie ni à celle d'un réseau pur. Elle tient compte d'un système d'interconnexion intelligent, appelé Fabric (qui prend le plus souvent la forme de commutateur Fibre Channel), pour relier les équipements entre eux. Les N_Ports Fibre Channel se contentent de gérer la communication point à point entre le Fabric et eux-mêmes.

Remarque : Par convention, les points de connexion (ou node en anglais) sont appelés N_Port. Les serveurs ou les baies de stockage disposent donc de N_Port. Ce dernier se transforme en NL_Port dans les architectures de type boucle arbitrée Fibre Channel (Fibre Channel Arbitrated Loop), Tous les ports de communication (N_Port et NL_Port) possèdent un circuit pour l'émission et un autre pour la réception.



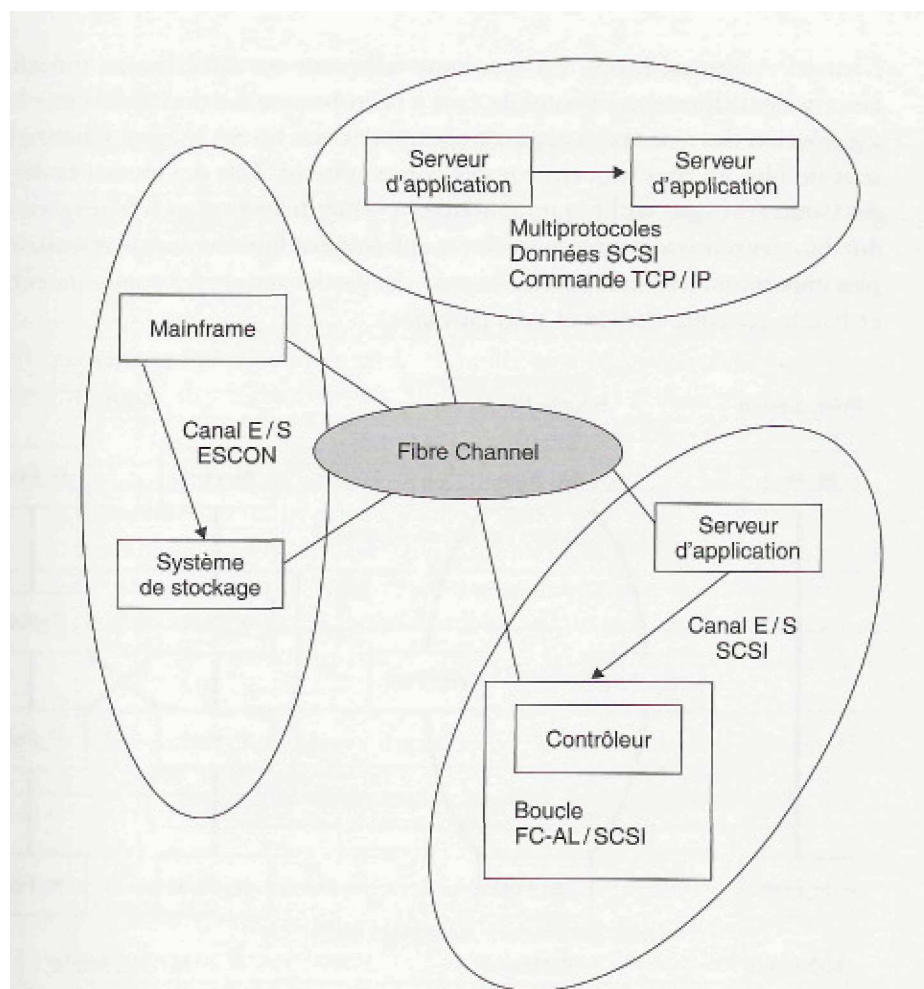
Fibre Channel s'apparente à une liaison série haute performance disposant de son propre protocole de communication. Cette liaison est aussi compatible avec des protocoles de niveau plus élevé, comme le SCSI, HIPPI ou encore IPL.

Fibre Channel est avant tout destiné au transfert rapide d'une quantité très importante de données.

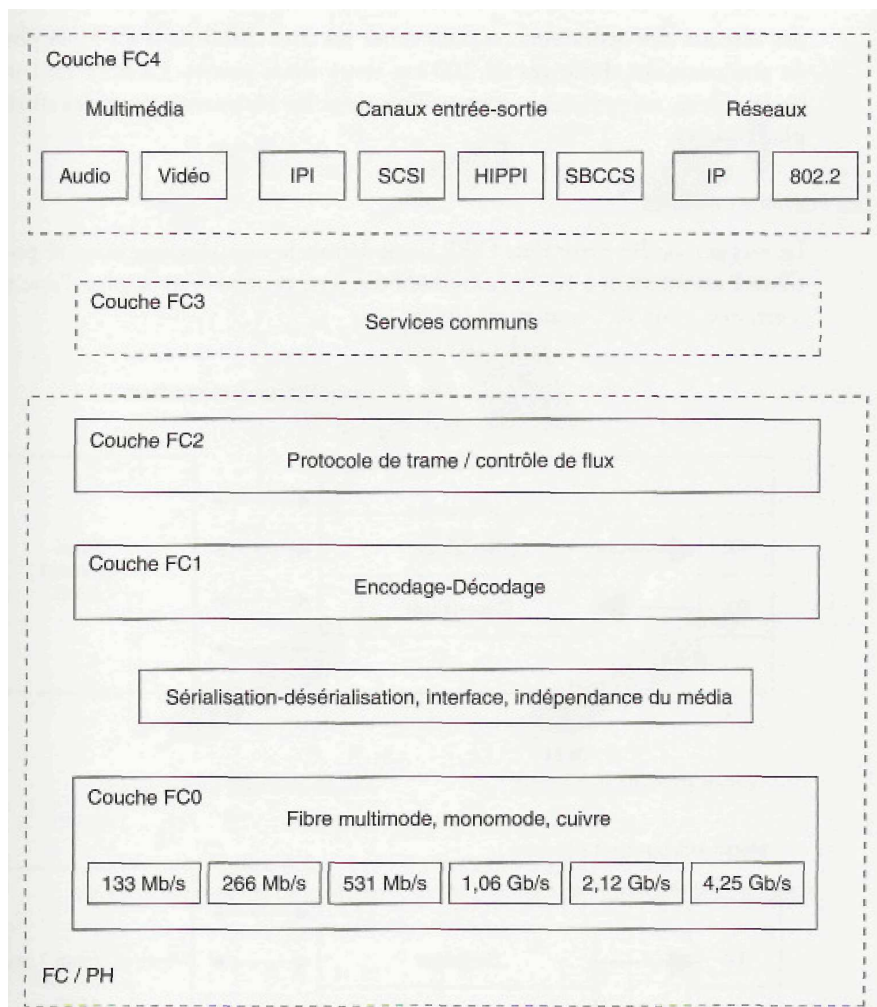
C'est pourquoi il fonctionne à différentes vitesses (133 Mbits/s, 266 Mbits/s, 530 Mbits/s, 1 Gbits/s, 2 Gbits/s et 10 Gbits/s) et sur trois médias optique ou électrique. La distance de transmission varie en fonction de la vitesse et du média retenu.

Un réseau Fibre Channel peut très bien communiquer avec les réseaux locaux d'entreprises. Pour cela, il suffit d'ajouter un convertisseur IP/Fibre Channel. Cependant cette solution est peu utilisée à cause des contraintes introduites par les convertisseurs (latence, gestion des mémoires tampon, etc.).

Les réseaux Fibre Channel assurent la cohabitation des canaux d'entrée/ sortie et des réseaux comme le montre l'image ci-dessous.



Enfin, Fibre Channel se compose de 5 couches, numérotées de 0 à 4, ayant toutes une utilité particulière. Fibre Channel est structuré comme un panel de fonction hiérarchisée. Les trois premières forment le standard FC-PH qui a été adopté en 1994. L'architecture Fibre Channel est représentée dans le schéma ci-après :



Afin de mieux comprendre le fonctionnement de Fibre Channel nous présenterons les différentes couches qui le composent.

3.1 Couche FC-0

La couche basse, baptisée FC-0 Layer, définit la liaison physique du système, incluant la fibre optique et le cuivre, les connecteurs, les paramètres optiques ou électriques pour les taux de transfert des données. Cette couche définit également les caractéristiques de longueur et de vitesse de transfert. Ces deux informations sont directement liées au support physique utilisé : soit de la fibre monomode pour relier

des sites distants de plusieurs kilomètres, soit de la fibre multi mode ou cuivre pour des distances courtes.

Enfin, la couche basse du Fibre Channel définit un système de sécurité, intitulé Open

Fibre Control System, pour les liaisons utilisant les lasers, afin de se prémunir contre les dépassements de puissance des lasers.

3.2 Couche FC-1

La couche FC-1 du Fibre Channel définit le protocole de transmission, incluant ainsi l'encodage série et les opérations de décodage associées, les caractères spéciaux, le contrôle d'erreur ainsi que la reconstitution de l'horloge de transmission et la synchronisation des octets. Les informations transmises au-dessus d'une fibre sont encodées sur 8 bits, contenus dans le caractère de transmission (*Transmission Character*) comprenant 10 bits. On parle alors de code 8B/10B.

3.2.1 Architecture

Le code 8B/10B évite les trop longues séquences de 1 et de 0, qui ont une tendance à désynchroniser l'horloge reconstruite à partir du signal de données. Ce code engendre une redondance de 25 % ce qui a pour avantage d'améliorer de manière logique la vitesse de transmission.

3.2.2 Conversion des caractères FC-1

Un bit d'information non codé est composé de 8 informations et de 1 bit de contrôle variable. Cette information est ensuite encodée par la couche Fibre Channel 1 sur 10 bits. Le variable de contrôle a soit la valeur D (D-Type) pour le caractère D et la valeur K (K-Type) pour les caractères spéciaux.

3.2.3 Les règles de codage

Chaque bit de données ou caractère spécial dispose de deux codes de transmission. Ils sont codés en fonction du *Running Disparity* (RD) initial. Ce RD est un paramètre binaire, qui est calculé en fonction des valeurs des sous blocs (les six premiers bits et les quatre derniers) du caractère de transmission.

3.3 Couche FC-2

La couche FC-2 correspond au protocole de signalisation et sert de mécanisme de transport indépendant des couches supérieures pour le Fibre Channel. Les règles des structures des trames de données qui sont transmises entre deux ports, les différents mécanismes dédiés au contrôle des trois classes de services et les moyens de gestion de séquence des transferts de données sont définis par cette couche FC-2. Pour aider dans le transport des données, les blocs suivants sont définis :

- ◆ le jeu de commandes;
- ◆ les trames;
- ◆ la séquence;
- ◆ les échanges (*Exchange*) ;
- ◆ le protocole.

3.3.1 Le jeu de commandes

Le jeu de commandes est avant tout destiné à organiser les échanges : initialisation des circuits, séparation des trames et signification de la fin d'une communication. Ce jeu de commande est codé sur 4 bits. Il existe trois paramètres définis au sein du protocole de signalisation :

- ◆ les délimiteurs de trame *Start-of-Frame* (SOF) et *End-of-Frame* (EOF) précèdent et suivent le contenu d'une trame Fibre Channel.
- ◆ Les deux primitives de signal : *Idle* (attente) et *Receiver Ready* (R_RDY, réception prête). Elles définissent un état du port. *Idle* est envoyé pour indiquer que le port peut à la fois recevoir ou émettre des données. Le *Receiver Ready* indique que la mémoire tampon du « receveur » est parée à recevoir des données.
- ◆ La primitive de séquence : lorsqu'une telle primitive est reçue et décodée, soit une autre primitive de séquence est envoyée soit une primitive de signal *Idle* est expédiée. Les primitives de séquence prises en charge par le standard Fibre Channel sont le *Offline* (OLS), la *Not Opération* (NOS), *Link Reset* (LR) et la *Link Reset Response* (LRR).

3.3.2 Les trames

La Fibre Channel communique en ayant recours à des trames. Ces dernières contiennent un champ appelé *payload* (ou champ de charge utile), l'adresse du port de la source et de la destination ainsi que les éléments nécessaires au contrôle de la liaison. Cette géométrie variable a de nombreux avantages. En effet, il est possible de transporter, sans le sectionner, un datagramme Ethernet (1512 octets) directement dans le champ *payload*.

Les trames peuvent être :

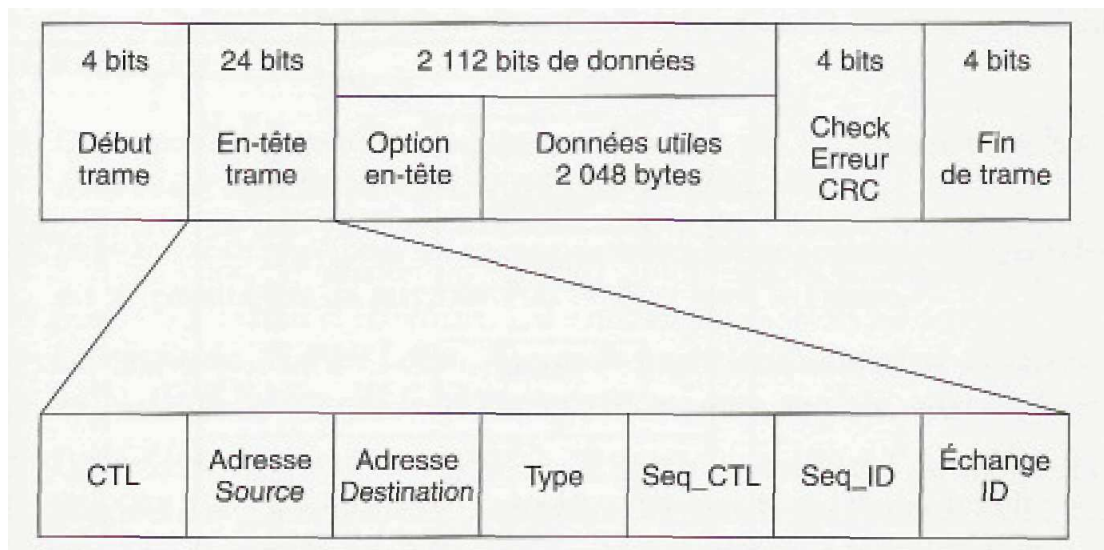
- ◆ soit des trames de données
- ◆ soit des trames de contrôle

Les trames de contrôle, sont classifiées comme étant des trames d'acquiescement (*acknowledgement*) et des trames de réponse sur l'état du lien (occupé et rejeté).

Toutes les trames Fibre Channel disposent du même modèle d'architecture. Elles se composent des éléments suivants :

- ◆ un champ de début de trame, intitulé SOF (*Start of Frame*). Ces 4 octets sont affectés au jeu de commande ;
- ◆ un en-tête (aussi appelé *header*), codé sur 24 bits. Il contient notamment les données nécessaires à l'identification de l'émetteur, le destinataire, le protocole et le type de données échangées (données ou commandes) ;
- ◆ un champ de données utiles variable (de 0 octet à 2 112 octets) ;
- ◆ un champ CRC pour la détection et la correction des erreurs ;
- ◆ un champ de fin de trame, codé sur 4 octets et associé au jeu de commandes.

Le schéma ci-dessous montre les différents qui composent une trame :



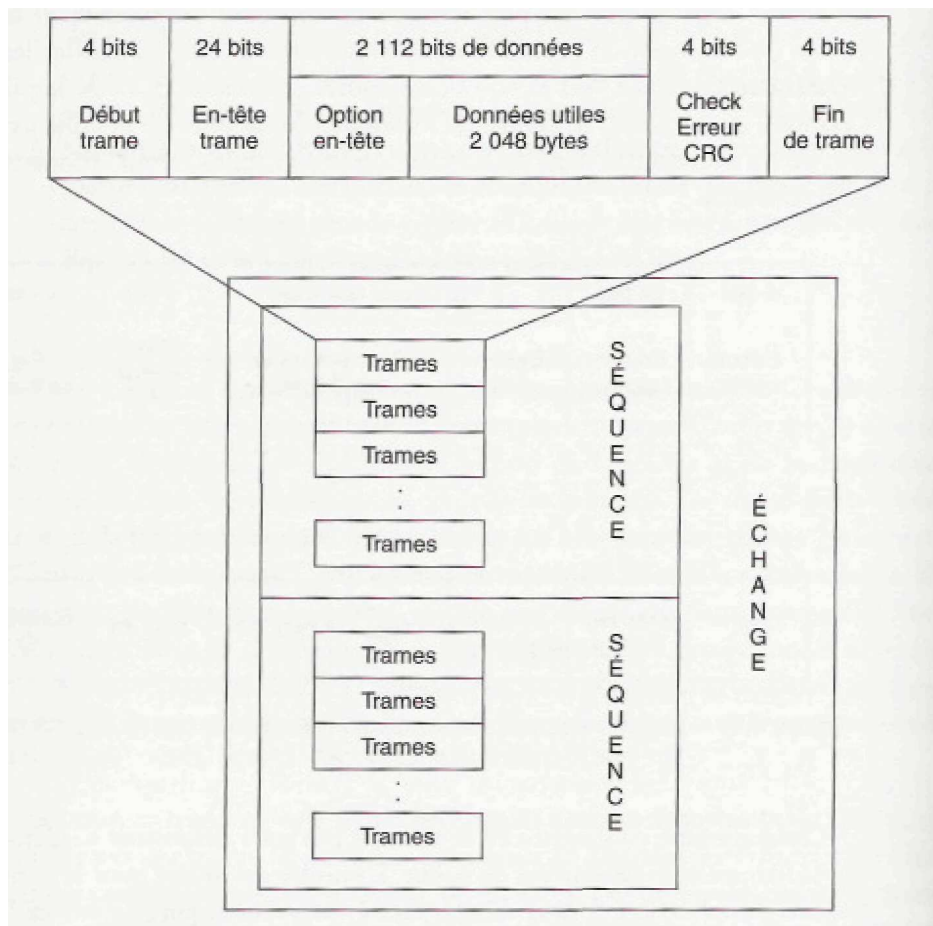
3.3.3 La séquence

Une séquence est composée par une série d'une ou plusieurs trames qui sont transmises entre un point A et un point B. Chaque trame appartenant à la même séquence est numérotée de manière exclusive par un compteur spécial. Chaque trame est donc unique. L'utilisation de séquence permet donc de décharger les applications de la gestion de la longueur des trames, cette opération étant directement à la charge de la couche Fibre Channel FC-2. Enfin lorsqu'une erreur survient, la reprise intervient directement au niveau de la séquence et non au niveau de la trame incriminée.

3.3.4 Les échanges

Un échange se compose d'une ou de plusieurs séquences non concurrentes associées pour une opération simple. Les échanges peuvent être unidirectionnels ou bidirectionnels entre deux N_Ports. Lors d'un échange, seulement une séquence peut être active en même temps, mais les séquences des différents échanges peuvent être actives simultanément.

Le schéma ci-dessous récapitule l'organisation des blocs cités précédemment au sein de la couche Fibre Channel FC-2 :



3.3.5 Protocole

Les protocoles sont relatifs aux services offerts par le Fibre Channel. Ils peuvent être spécifiques pour les services associés aux couches de haut niveau. Fibre Channel fournit ses propres paramètres de protocole afin de gérer les environnements opérationnels pour les transferts de données. Les protocoles suivants sont définis par les standards :

- ◆ Le protocole de « *primitive séquence* ». Il repose sur les séquences de primitives et est spécifié pour les erreurs sur les liens.
- ◆ Le protocole de *Login* pour les environnements Fabric (commutés). Les échanges de paramètres de services d'un N_Port avec le Fabric.
- ◆ Les protocoles *N_Port Login*. Avant de procéder au transfert de données, les N_Ports échangent leurs paramètres services avec un autre N_Port-
- ◆ Le protocole de *transfert de données*. Il décrit les méthodes de transfert des données des protocoles de couche haute (*Upper Layer Protocol- ULP*) utilisant la gestion du contrôle de flux de Fibre Channel.

- ◆ *Le protocole N_Port Logout.* Ce protocole est activé lorsqu'une requête de révocation est émise par un autre N_Port. Il est utilisé pour libérer les ressources connectées à un N_Port.

Enfin le contrôle de flux est un processus de contrôle FC-2 pour s'assurer du bon acheminement du flux des trames entre deux N_Ports *via* un Fabric (commutateur).

3.4 Couche FC-3

Le niveau Fibre Channel 3 vise à fournir des services communs entre agents pour les fonctions avancées comme :

- ◆ agréger plusieurs liaisons en parallèle afin d'augmenter la bande passante pour une connexion spécifique;
- ◆ la possibilité pour plusieurs ports de répondre à une seule et même adresse;
- ◆ le *multicast* pour délivrer une information à de multiples ports.
- ◆ Cette couche n'est pas encore totalement standardisée.

3.5 Couche FC-4

La couche de niveau 4 du Fibre Channel définit l'interface permettant de connecter des applications au-dessus de Fibre Channel. Elle spécifie les règles de mapping (mise en correspondance) des protocoles de plus haut niveau s'adossant à Fibre Channel.

Les protocoles de type réseau et de type canal suivants sont compatibles ou en passe de l'être avec la couche 4 de Fibre Channel :

- ◆ Small Computer System Interface (SCSI);
- ◆ Intelligent Peripheral Interface (IPI) ;
- ◆ High Performance Parallel Interface (HIPPI) Framing Protocol;
- ◆ Internet Protocol (IP);
- ◆ ATM Adaptation Layer for Computer Data (AAL5) ;
- ◆ Link Encapsulation (FC-LE);
- ◆ Single Byte Command Code Set Mapping (SBCCS);
- ◆ IEEE 802.2.

IPI constitue un ensemble de commande, souvent utilisé avec HIPPI.

HIPPI est un protocole bidirectionnel sans jeu de commandes. Il opère sur des liaisons parallèles à 100 Mo/s. Au départ, Fibre Channel cherchait à sérialiser HIPPI.

4 Virtualisation

4.1 Définition

Mais que se cache-t-il donc derrière cet anglicisme ? La virtualisation définit un concept simple à comprendre : elle décorrèle les ressources physiques des ressources logiques. En clair, les serveurs d'applications connaissent l'adresse logique de stockage des données, qui ne correspond pas à l'adresse physique. Par exemple, l'application A entrepose ses données sur l'espace A qui lui est réservé. Seulement, cet espace peut très bien être réparti physiquement sur les disques durs des baies de stockage 1, 2 et 3. L'application, elle, visualise un espace de stockage unique, comme s'il s'agissait d'un seul disque dur.

Cette notion n'a vraiment rien d'une nouveauté. Pourtant, actuellement, tous les éditeurs et constructeurs du secteur de stockage ne parlent que de virtualisation. Sans les avantages du concept de la virtualisation, le SAN risque de se contenter d'être un simple réseau de stockage, certes rapide, mais très difficilement administrable, surtout face à la croissance des données à stocker. De plus, sans virtualisation, le SAN a toutes les chances de rester cantonné à quelques îlots au sein de l'entreprise. La virtualisation répond donc à cette double problématique : gérer à moindre coût un réseau hétérogène de données, le volume de ces dernières ne cessant de croître.

La virtualisation peut donc être considérée comme une couche d'abstraction. Cependant, pour fonctionner, ce concept nécessite l'existence de mécanismes capables d'assurer la correspondance logique - physique. C'est à ce niveau que les divergences apparaissent entre les différentes solutions de virtualisation. Actuellement la mise en œuvre de la virtualisation a donné naissance à cinq approches, nous allons étudier par la suite de ce chapitre les 4 principales approches : le RAID, le SAN *in a box*, les serveurs de domaines virtuels, les métaserveurs.

4.2 RAID

La virtualisation du stockage a commencé avec les unités de stockage. Les technologies RAID constituent les premières formes d'espace virtuel.



RAID est l'acronyme de Redundant Array of Independent/Inexpensive Disks, défini en 1987 à l'université de Berkeley (Californie). Cette technique consiste à empiler dans une baie de stockage plusieurs disques afin d'obtenir des performances, une fiabilité et un volume de stockage élevés. Les applications voient ces différentes unités de stockage comme un seul et même espace. Il existe donc une couche d'abstraction logique, implémentée soit dans le contrôleur disque, soit de manière logicielle au niveau des outils d'exploitation du serveur.

RAID est composé de nombreux niveaux, qui combinés entre eux, en génèrent de nouveaux. Il faut retenir les cinq principaux.

- RAID 0 : *striping* (segmentation des données sans adjonction de parité)
Cette approche est souvent utilisée pour améliorer les performances d'accès.

- RAID 1 : miroir
C'est une des techniques RAID les plus répandues, déjà utilisée avant la définition des niveaux de RAID. Toutes les données sont dupliquées, mais les performances d'entrées/sorties ne sont pas améliorées.

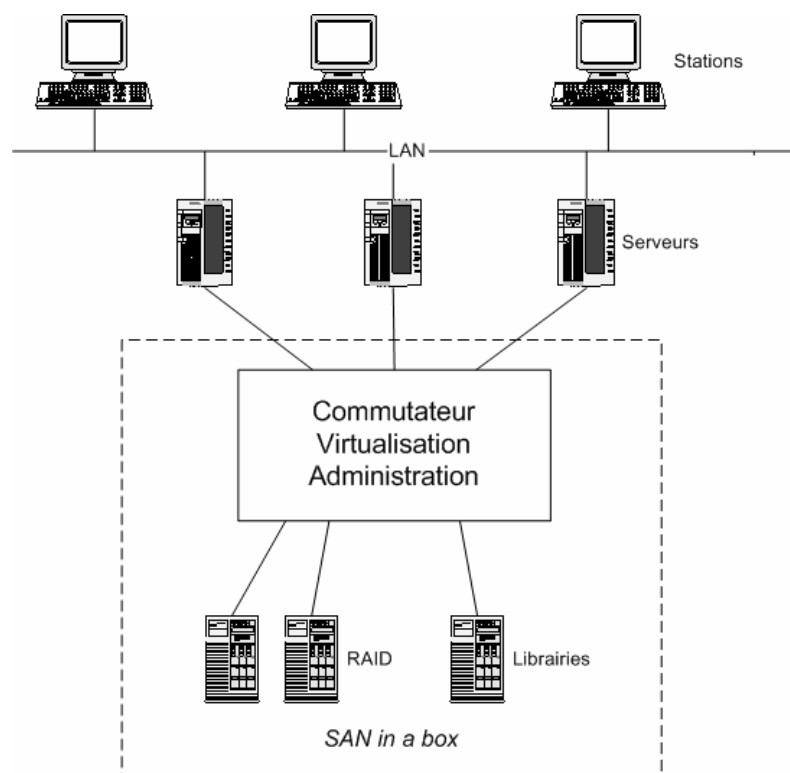
- RAID 0+1 : *striping* et miroir
Ce niveau combine les performances du RAID 0 (*striping*) et la sécurité du RAID 1 (Miroir). Il apporte donc une plus grande sécurité tout en améliorant les performances.

- RAID 3: *striping* avec parité
Un disque par groupe est dédié à la parité. Il a la charge de fiabiliser l'ensemble. Ce niveau est surtout utilisé pour les supercalculateurs et les ordinateurs graphiques. Il convient parfaitement aux environnements dans lesquels l'importance de la bande passante prime sur les performances d'entrées/sorties.

- RAID 5: *striping* avec parité distribuée
La parité et les données sont distribuées de manière séquentielle sur tous les disques composant la grappe. Ce niveau assure une excellente protection contre une panne survenant sur une des unités de stockage. Ce niveau de RAID se retrouve fréquemment dans les environnements transactionnels. En outre, il est adapté pour délivrer de bonnes performances lors d'accès séquentiels.

4.3 SAN in a box

Cette approche de la virtualisation repose sur un équipement de type *appliance*. Ces équipements sont apparus initialement dans... l'électroménager. Ils définissent une catégorie précise ; celle des produits qui sont dédiés à une seule tâche, comme les aspirateur par exemple. Cette dénomination est très largement sortie de ce cadre restreint. Elle s'étend aussi au secteur informatique (au sens large) et définit des équipements ayant une fonction unique. Dans le cas du *SAN in a box*, le produit embarque toutes les composantes d'un réseau de stockage SAN.



A savoir : le système de commutation, le système disques, les outils d'administration et de gestion de l'espace virtuel ainsi que les fonctions de supervision.

Cet équipement présente de multiples avantages. En premier lieu, il est totalement transparent et non intrusif pour le réseau déployé. Il s'insère dans des environnements hétérogènes. Ces facultés le font ressembler à un caméléon de la virtualisation. De plus, l'*appliance* est aisée à installer, reste économiquement intéressante et, bien souvent, plus performante qu'une solution éclatée ou distribuée. Il

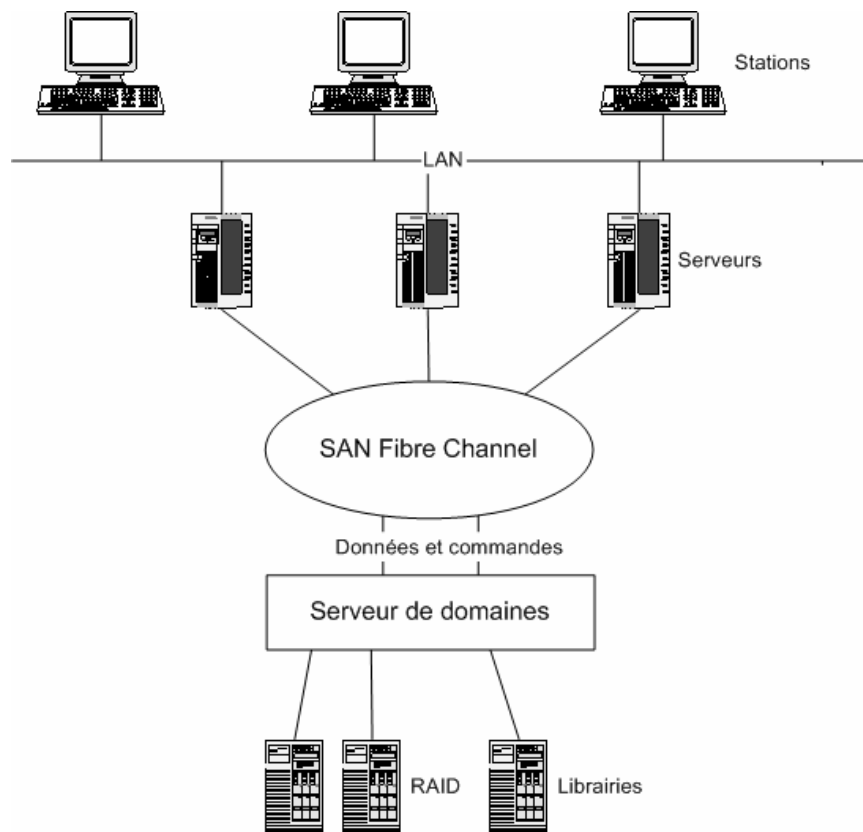
est évident que l'appliance étant uniquement dédié à la virtualisation, il est nettement plus facile d'optimiser le système de commutation, la fonction de cache ainsi que le pilotage des disques.

Seulement, cette appliance a aussi les défauts de ses qualités. En effet, cet équipement non seulement fédère toutes les ressources nécessaires à la virtualisation mais tous les flux doivent transiter via cette appliance. Il apparaît alors très vite que les performances du SAN *in a box*, aussi bonnes soient-elles, risquent de ne plus être suffisantes lors de la montée en puissance du réseau. Dans ce cas, il faut positionner plusieurs *appliances* en parallèle et les consolider. Lorsque le réseau s'accroît, il peut être nécessaire de paralléliser les appliances consolidées.

Cette solution n'est donc que peu adaptée à des réseaux promis à une montée en puissance rapide. De plus, son caractère propriétaire limite également sa capacité d'évolution à intégrer les nouvelles technologies de virtualisation.

4.4 Serveurs de domaines virtuels

Avec cette solution, la virtualisation des blocs est confiée à un serveur de domaines de stockage implanté sur une plate-forme standard. Généralement, le serveur de domaines s'intercale entre les réseaux SAN et les unités de stockage. Il gère les translations logique/physique pour les serveurs hôtes. Mais le serveur de domaines virtuels peut aussi très bien être implanté dans les commutateurs et les routeurs Fibre Channel.



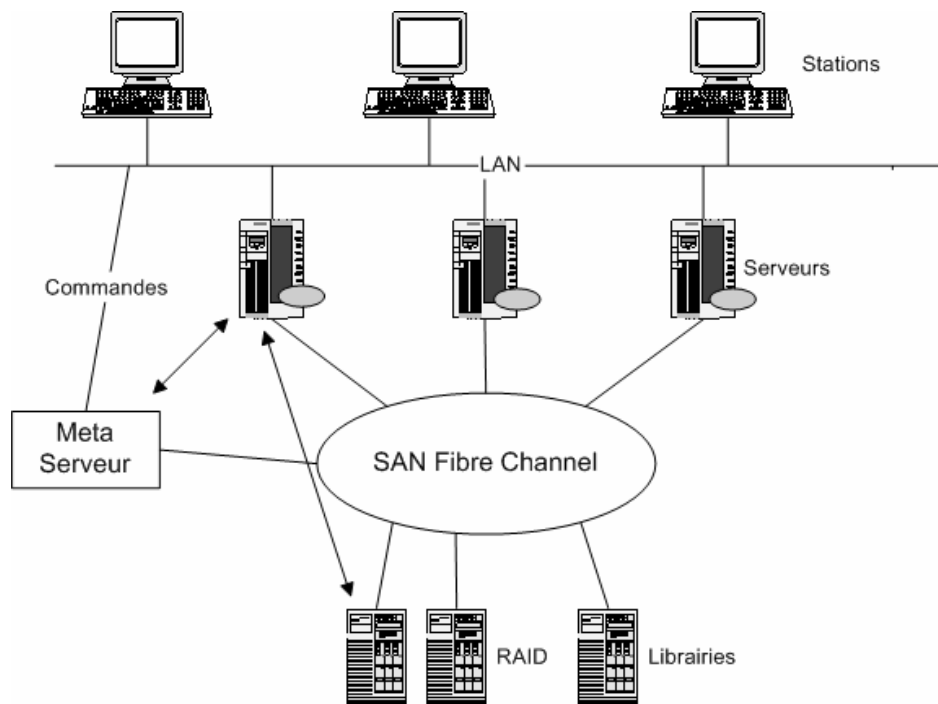
Le serveur de domaines constitue le cœur de la solution. Toutes les informations, qu'elles soient du type données ou commandes, transitent obligatoirement par le serveur de virtualisation. Cette solution a le mérite de simplifier l'administration de la virtualisation. En effet, il n'y a qu'un seul point d'entrée et elle ne nécessite pas l'implantation d'agent côté hôte puisque les données et les commandes transitent par le même chemin. Une telle architecture est dite symétrique. Le serveur de domaines s'appuie sur une variété de technologies de stockage.

En revanche, l'écoulement des flux de données devient alors critique. De même, l'efficacité des caches et des files d'attente doit, être considérée comme un point clé de l'architecture. Comme pour les solutions SAN *in a box*, cette solution peut très vite s'avérer coûteuse et avoir des difficultés pour répondre aux exigences de haute disponibilité et de croissance des grands SAN.

Néanmoins, cette technologie de virtualisation dispose d'un atout non négligeable : elle prend en compte d'anciennes technologies qui, sans elle, seraient restées sur le bord de la route du SAN, obligeant ainsi les entreprises à réinvestir dans de nouveaux équipements pour mettre en place leurs réseaux de stockage.

4.5 Metaserveurs

Cette approche marque une rupture avec les deux précédentes. En effet, les chemins empruntés par les données et celui emprunté par les commandes sont différents. On parle alors d'architecture asymétrique.



Le metaserveur de virtualisation est toujours connecté au réseau commuté Fibre Channel seulement, comme cet équipement ne constitue plus le point de passage obligé de tous les flux, l'installation d'un metaserveur nécessite en outre le déploiement d'agents sur les serveurs d'application. Ces agents sont installés afin de donner des informations indispensables aux serveurs d'application, comme l'espace disque disponible par exemple. En revanche, les transferts s'effectuent directement entre les serveurs d'applications et les espaces de stockage.

Les metaserveurs peuvent aussi bien être implémentés sur des plates-formes standard que sur des commutateurs et des routeurs.

Cette architecture, contrairement au modèle symétrique, offre une manipulation des volumes virtuels très souple. L'administrateur a la possibilité de les partager entre plusieurs serveurs, de les dupliquer ou encore de les échanger. De même, les problèmes de zoning sont grandement simplifiés. En effet, le serveur n'accède qu'au

volume qui lui a été attribué par le metaserveur. Enfin, les opérations de restauration sont plus simples puisque les serveurs d'applications gèrent leur volume comme si la virtualisation n'était pas présente.

En revanche, l'installation d'agents côté serveur d'applications est une nécessité. Il faut donc disposer de tels composants pour chaque serveur d'application, quel qu'il soit. L'éditeur ou le constructeur qui propose une telle solution doit obligatoirement tenir sa base à jour. De son côté, le client se doit de faire suivre sa base d'agents parallèlement aux versions des serveurs d'application. Si tel n'est pas le cas, des décalages peuvent très vite survenir entre ces deux solutions logicielles. En outre, cette mise à niveau peut, sur une longue période, se révéler coûteuse.



5 Internet Fibre Channel Protocol (iFCP)

Les spécifications Internet Fibre Channel Protocol définissent un protocole de passerelle à passerelle pour l'implémentation de Fabric Fibre Channel (réseau Fibre Channel commuté) dans lequel les éléments de routage et de commutation IP remplacent les équipements Fibre Channel. Ce protocole permet l'attachement de produits de stockage Fibre Channel déjà déployés à des réseaux IP tout en prenant en charge les services de commutation de chacun des deux environnements.

iFCP s'appuie sur le protocole Fibre Channel, le standard série de l'ANSI utilisé pour l'acheminement des commandes SCSI, des données et des messages de statut sur une liaison série, comme un réseau Fibre Channel. Seulement, iFCP remplace la couche transport de Fibre Channel par un réseau IP. Il conserve toutefois les caractéristiques des couches supérieures. Cette opération s'effectue via un *mapping* de la couche transport du protocole Fibre Channel sur la pile TCP/IP.

Cette caractéristique constitue justement une des grandes forces de ce protocole. En effet, il est désormais possible de relier des réseaux SAN en mode point à point ou non sans pour autant avoir recours aux équipements purement SAN. Le iFCP permet donc de s'affranchir des contraintes de distances liées au Fibre Channel tout en pérennisant les lourds investissements consentis par les entreprises dans leur SAN. La mise en relation de différents îlots SAN s'effectue donc sans aucune modification préalable.

5.1 Pourquoi le protocole iFCP ?

iFCP est conçu avant tout pour les utilisateurs qui ont un large panel d'équipements Fibre Channel et qui désirent les relier facilement entre eux. Pour cela, iFCP assure l'interconnexion de réseaux distants tout en utilisant le couple TCP/IP. Ce protocole permet également aux entreprises d'exploiter les réseaux TCP/IP en place pour bâtir des réseaux de stockage Fibre Channel. L'investissement initial est nettement moins important que pour un SAN Fibre Channel pur. En implémentant le protocole iFCP comme un protocole de passerelle à passerelle, les utilisateurs conservent les bénéfices de leur infrastructure Fibre Channel tout en utilisant le réseau IP de l'entreprise comme vecteur pour acheminer les données. Ils tirent alors parti de l'infrastructure IP en ce qui concerne l'exploitation. Les administrateurs réseau maîtrisent parfaitement

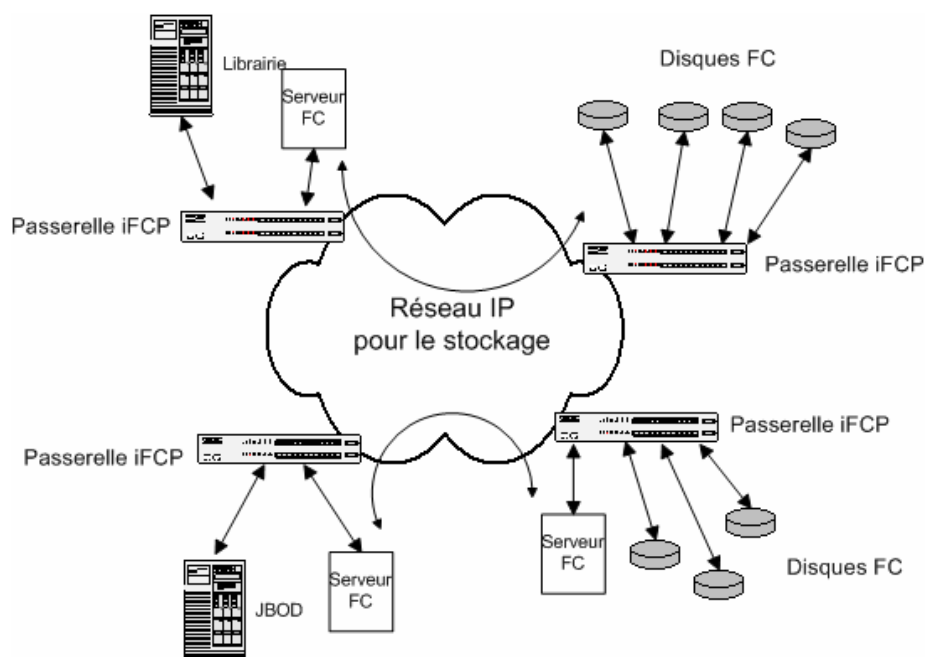


la pile TCP/IP, les outils d'exploitation ainsi que les équipements de communication. De plus, le coût de mise en œuvre est moindre.

iFCP permet donc à des équipements Fibre Channel de communiquer entre eux en empruntant des réseaux IP étendus ou locaux. Cette communication s'effectue à un coût nettement moindre que ceux proposés actuellement par les technologies SAN et Fibre Channel.

5.2 Le modèle de réseau iFCP

Le protocole iFCP assure la mise en correspondance des services de transport Fibre Channel sur un réseau IP. La figure suivante représente très bien le modèle iFCP, mettant en œuvre à la fois des îlots SAN et des réseaux IP.



Dans cette implémentation, des passerelles sont utilisées pour connecter les réseaux Fibre Channel existants aux infrastructures IP. Elles sont dotées d'interfaces physiques IP et Fibre Channel.

iFCP correspond au couple de protocoles TCP/IP qui transporte, en les encapsulant dans un datagramme IP, des trames FC-4 entre deux passerelles.

5.3 Architecture d'une passerelle

L'architecture d'une passerelle iFCP appartient à la fois à un domaine réseau Fibre Channel et à un domaine réseau IP. Les équipements Fibre Channel sont directement connectés à des ports du Fabric et sont considérés comme faisant partie intégrante de la passerelle. Chaque équipement connecté à un des ports est perçu comme ayant un attachement direct. Ces mêmes ports sont présentés, du côté IP comme étant des interfaces iFCP directement rattachées au réseau local. Les translations d'adresses entre les deux environnements sont automatiques.

Lorsque les paquets sont reçus du réseau IP, ils sont aussitôt convertis en des Fibre Channel puis transmis au destinataire en utilisant les couches Fibre Channel. Cette opération est bidirectionnelle. Les trames Fibre Channel entraînées dans la passerelle se voient attribuer une adresse de port puis sont encapsulée dans un datagramme disposant de sa propre adresse IP.



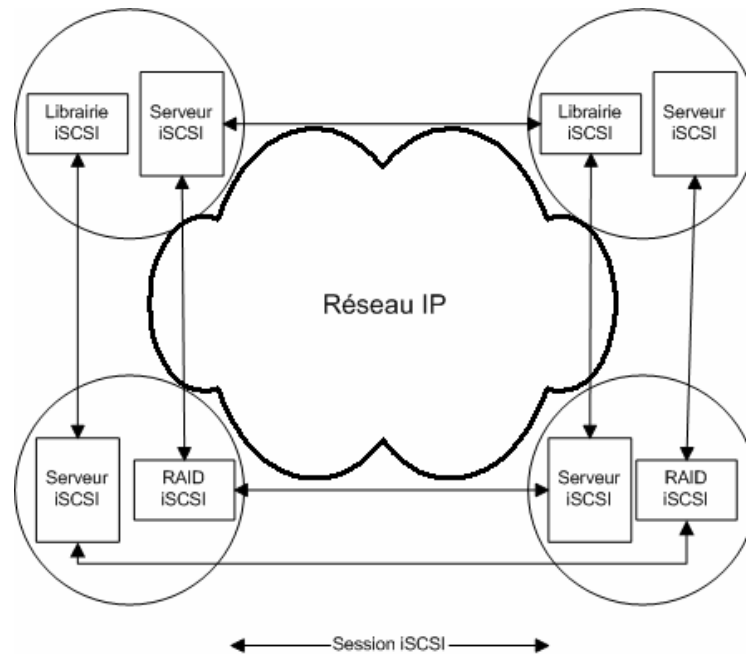
6 SCSI over IP (iSCSI)

Les architectures SCSI reposent sur le modèle client - serveur. Le client est typiquement un système hôte, comme un serveur de fichiers sur lequel s'effectuent de nombreuses opérations de lecture/écriture. Le serveur est une ressource au même titre qu'une baie de disques et répond aux requêtes des clients. Un serveur dispose d'une ou de plusieurs unités logiques qui sont susceptibles de recevoir des commandes. Les unités logiques possèdent une identification particulière ou un numéro d'unité logique (LUN, Logical Unit Number). Les commandes sont contenues dans un bloc de description de commande (CDB, Command Descriptor Block) délivré par le système hôte. Un CDB envoie à une unité logique spécifique, par exemple, une commande afin de lire un bloc de données précis. L'unité logique cible commencera le transfert vers l'expéditeur de la requête, qui se terminera avec un message de statut indiquant que la requête s'est bien passée.

Le protocole de communication iSCSI est un *mapping* du modèle de procédure d'invocation à distance du SCSI sur le protocole TCP, d'où son appellation, qui n'est autre que l'abréviation de SCSI *over* IP traduit par SCSI sur IP. Les commandes SCSI sont transportées dans les requêtes.

Pour des raisons de performance, ce protocole autorise une « *phase-collapse* ». Une commande, ainsi que les données associées, peuvent être envoyées ensemble par l'expéditeur vers le destinataire. La réponse et les informations qui la composent peuvent également être envoyées ensemble.

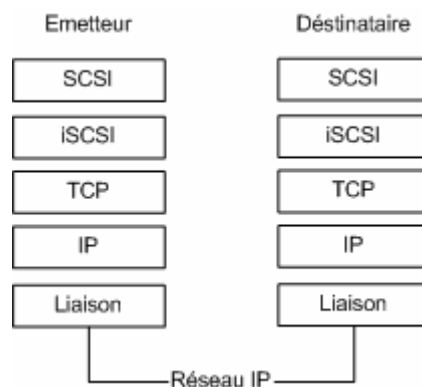
La mission première du protocole iSCSI consiste à encapsuler et fiabiliser les transactions CDB entre le destinataire et l'expéditeur en empruntant un réseau TCP/IP.



6.1 Le modèle du protocole iSCSI

Le protocole de communication iSCSI s'appuie sur TCP pour assurer la transmission des données de manière fiable. La couche iSCSI comprend l'encapsulation des commandes SCSI, les données et les informations relatives au statut de la session. Lorsque, par exemple, un système d'exploitation ou une application demandent une opération d'écriture, le SCSI CDB doit être encapsulé avant d'emprunter une liaison et d'être délivré au destinataire.

Le protocole iSCSI surveille les transferts de données (en mode bloc) et valide les opérations de lecture/écriture. Ces opérations s'effectuent au travers d'une ou plusieurs connexions TCP entre la cible et l'émetteur. En pratique, l'émetteur peut disposer de plusieurs cibles et donc multiplier les connexions TCP.



CONCLUSION

Aussi bien SAN que NAS tentent de répondre aux besoins croissants en matière de consolidation et de mise en communs des espaces de stockage de données. En effet plus le volume et les sources des données à conserver sont importants, plus il devient matériellement impossible de n'avoir qu'un unique point de stockage. Une différence radicale sépare cependant les deux technologies : le NAS utilise le réseau déjà présent de l'entreprise, alors que le SAN constitue en lui-même un réseau dédié au stockage. Les possibilités offertes par le second sont donc nettement supérieures à celles du NAS, mais le coût induit est en conséquence bien plus élevé. Pour simplifier, on pourrait dire que le SAN répond aux exigences des grandes entreprises, alors que le NAS correspond en général aux besoins moins contraignants des petites et moyennes entreprises.

iFCP et iSCSI sont les deux principaux protocoles qui tentent de répondre au problème du stockage via IP. Chacun d'entre eux possède cependant des sphères d'applications bien spécifiques.

iSCSI permet le transfert de données sur des réseaux Ethernet par IP. On peut le considérer comme une alternative à Fibre Channel.

Le iSCSI a besoin d'un réseau Ethernet très performant, rapide et résistant à la charge. Mais le coût est sans comparaison avec un réseau Fibre Channel spécifique. Son coût modéré le destine principalement aux petites et moyennes entreprises qui ne souhaitent pas investir dans un SAN Fibre Channel.

Il fonctionne localement mais également à distance, au travers du réseau Internet, ce qui est une façon simple d'accéder à des données éloignées.

Protocole plus récent et, peut-être, plus sophistiqué, iFCP apparaît comme une pile de couches normalisées, à l'instar de TCP/IP.

Il peut être utilisé pour connecter à travers un réseau IP des périphériques de stockage Fibre Channel déjà déployés à un réseau SAN IP ou établir des passerelles entre SANs distincts. L'investissement initial est donc largement inférieur à un SAN Fibre Channel pur. L'administration est plus aisée puisque la plupart des administrateurs maîtrisent les outils d'exploitation et d'administration des réseaux IP.