HOÀNG DƯƠNG THỊNH CÔNG NGHỆ THÔNG TIN 2004- 2006

Hà Nội
2006

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

LUẬN VĂN THẠC SĨ KHOA HỌC

NGHÀNH : CÔNG NGHỆ THÔNG TIN

NGHIÊN CỨU VỀ MẠNG LƯU TRỮ VÀ ĐỀ XUẤT PHƯƠNG ÁN MẠNG LƯU TRỮ ỨNG DỤNG CHO TỔNG CÔNG TY BẢO HIỂM VIỆT NAM

HOÀNG DƯƠNG THỊNH

HÀ NỘI 2006

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

LUẬN VĂN THẠC SỸ KHOA HỌC

NGHIÊN CỨU VỀ MẠNG LƯU TRỮ VÀ ĐỀ XUẤT PHƯƠNG ÁN MẠNG LƯU TRỮ ỨNG DỤNG CHO TỔNG CÔNG TY BẢO HIỂM VIỆT NAM

NGÀNH : CÔNG NGHỆ THÔNG TIN

MÃ SỐ :

HOÀNG DƯƠNG THỊNH

*Người hướng dẫn khoa học : TS .***TRỊNH VĂN LOAN**

HÀ NỘI 2006

LỜI CẢM ƠN

Trong lời đầu tiên của luận văn Thạc sĩ khoa học này, em muốn gửi những lời cảm ơn và biết ơn chân thành của mình tới tất cả những người hỗ trợ, giúp đỡ em về chuyên môn, vật chất và tinh thần trong quá trình thực hiện Luận văn.

Trước hết, em xin chân thành cảm ơn thầy giáo Tiến sĩ Trịnh Văn Loan người đã trực tiếp hướng dẫn, nhận xét, giúp đỡ em trong suốt quá trình thực hiện luận văn.

Em xin chân thành cảm ơn các thầy, cô giáo trong khoa Công nghệ Thông tin, Bộ môn Kỹ thuật Máy tính,Trung tâm đào tạo và bồi dưỡng sau đại học và các thầy cô trong Trường Đại học Bách Khoa Hà Nội, những người đã dạy dỗ, chỉ bảo em trong suốt những năm học tập tại trường.

Cuối cùng, em xin bày tỏ lòng biết ơn tới gia đình, những người bạn thân và các bạn đồng nghiệp đã giúp đỡ, động viên em trong suốt quá trình học tập và làm luận văn tốt nghiệp.

Do thời gian thực hiện có hạn, kiến thức chuyên môn còn nhiều hạn chế nên luận văn em thực hiện chắc chắn không tránh khỏi những thiếu sót nhất định. Em rất mong nhận được ý kiến đóng góp của thầy cô giáo và các bạn.

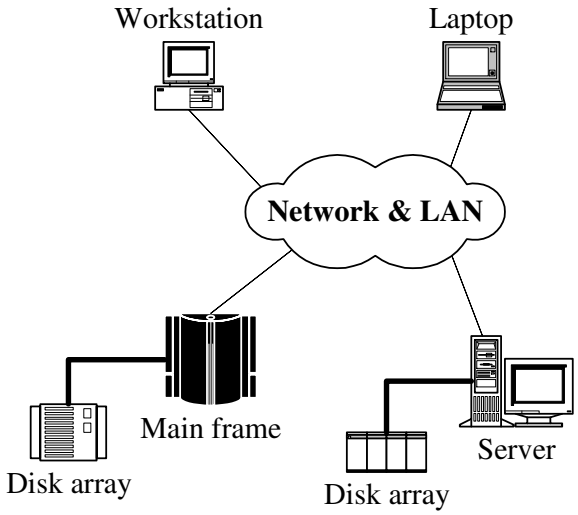
Em xin chân thành cảm ơn!

Hà Nội,ngày 15 tháng 11 năm 2006
Học viên

Hoàng Dương Thịnh

MỞ ĐẦU

Trước đây hệ thống máy tính lớn thường được sử dụng để quản lý tập trung các dịch vụ dữ liệu. Ở những hệ thống này thiết bị lưu trữ được gắn trực tiếp vào các kênh vào/ra của máy chủ. Máy chủ độc quyền truy xuất và quản lý tất cả thiết bị lưu trữ gắn trực tiếp vào chúng. Khi đó, các ứng dụng hoặc các máy trạm chỉ có thể truy xuất dữ liệu một cách gián tiếp thông qua mạng.



Hình 1 - Mô hình thiết bị lưu trữ gắn trực tiếp

Mô hình "thiết bị lưu trữ gắn trực tiếp" hoạt động hiệu quả trong một thời gian dài, đặc biệt trong môi trường xí nghiệp vừa và nhỏ. Tuy nhiên khi áp dụng mô hình này cho các doanh nghiệp lớn (doanh nghiệp đang sử dụng các ứng dụng có lượng dữ liệu luân chuyển lớn và có nhiều yêu cầu đặc biệt) thì mô hình trên bộc lộ nhiều điểm hạn chế:

Khả năng mở rộng: Số thiết bị gắn trực tiếp vào kênh vào ra của máy chủ thường bị giới hạn bởi một số cố định. Ví dụ như kênh SCSI giới hạn 16 thiết bị trên một kênh kể cả thiết bị điều hợp. Khi đó, dung lượng dữ liệu lưu trữ cũng bị giới hạn theo.

Hiệu năng thực thi: Các thiết bị lưu trữ chia sẻ băng thông trên kênh vào ra

mà chúng gắn vào. Do vậy, khi gắn thêm thiết bị lưu trữ vào một kênh sẽ làm giảm hiệu năng thực thi.

Giới hạn về mặt khoảng cách: Không gian đặt thiết bị lưu trữ bị ràng buộc nhất định về khoảng cách, đặc biệt trong các kênh giao tiếp song song. Nhằm đảm bảo hiệu năng thực thi và kỹ thuật tín hiệu điện, các kênh vào ra có độ dài tối đa thường chỉ vài mét.

Khả năng sẵn sàng: Người quản trị phải tắt hoạt động của toàn bộ chuỗi thiết bị trên một kênh khi muốn bổ sung, loại bỏ hay cấu hình lại hệ thống lưu trữ. Điều này ảnh hưởng đến sự hoạt động liên tục của hệ thống.

Bảo vệ dữ liệu: Khi có nhiều máy chủ, chi phí cho thiết bị sao lưu dữ liệu tăng nhanh đồng thời việc quản trị càng phức tạp do phải sao lưu dữ liệu trên từng máy chủ riêng biệt. Ngoài ra, việc sao lưu thông qua mạng cục bộ sẽ ảnh hưởng đến hoạt động của mạng doanh nghiệp trong một thời gian dài.

Hiệu quả: Khó phân phối lại không gian lưu trữ do mỗi máy chủ quản lý hoạt động của các thiết bị một cách riêng biệt. Điều này dẫn tới hầu hết các công ty phải mua bổ sung thiết bị cho máy chủ này trong khi máy chủ khác còn nhiều không gian lưu trữ chưa dùng đến.

Những hạn chế của mô hình "thiết bị lưu trữ kết nối trực tiếp" cũng chính là những lý do thúc đẩy công nghệ lưu trữ đi sang một thế hệ mới, thế hệ "mạng lưu trữ". Mạng lưu trữ có tiềm năng được ứng dụng rộng rãi bởi những ưu điểm sau:

- Mạng lưu trữ đưa ra khả năng mở rộng, cho phép kết nối hàng ngàn thiết bị lưu trữ phân tán trong phạm vi rộng lớn.
- Mạng lưu trữ cho phép lưu chuyển dữ liệu giữa các thiết bị lưu trữ mà không chiếm dụng băng thông của mạng cục bộ và không phải trung chuyển qua những máy chủ.
- Mạng lưu trữ cho phép cấu hình lại hoặc bảo trì hệ thống lưu trữ mà không yêu cầu dừng hoạt động của cả hệ thống.

- Mạng lưu trữ cung cấp một giải pháp quản lý tập trung năng lực lưu trữ.

Mấy năm gần đây, thị trường SAN đạt mức tăng trưởng cao nhờ sự hỗ trợ và đa dạng hóa các giải pháp kết nối. Theo thống kê của của tổ chức Gartner Group's Dataquest, chỉ riêng thị trường Nhật bản đã đạt doanh thu 7.2 tỷ đô la mỹ và đạt mức tăng trưởng 17.5% trong năm 2005. Công nghệ SAN đã được áp dụng ở nhiều nước trên thế giới. Ở Việt Nam, công nghệ SAN mới gây được sự quan tâm trong thời gian gần đây và mới bước đầu được ứng dụng.

Luận văn tập trung nghiên cứu công nghệ SAN, tình hình phát triển SAN trên thế giới và khả năng ứng dụng công nghệ SAN tại Việt Nam, qua đó xây dựng giải pháp thích hợp lưu trữ khối lượng dữ liệu lớn tại một doanh nghiệp cụ thể. Cấu trúc luận văn bao gồm:

Phần: "Mở đầu" giới thiệu về sự hình thành công nghệ lưu trữ SAN, những tiềm năng của SAN.

Chương 1: "Mạng lưu trữ - SAN". Tổng quan hệ thống mạng lưu trữ: các khái niệm cơ bản, các thành phần chính, các ứng dụng trong mạng SAN, việc quản lý và khai thác mạng SAN.

Chương 2: "IP SAN". Phân tích chi tiết hai giao thức iFCP và iSCSI. Các giao thức này sẽ được sử dụng làm cơ sở phát triển công nghệ SAN dựa trên nền tảng IP.

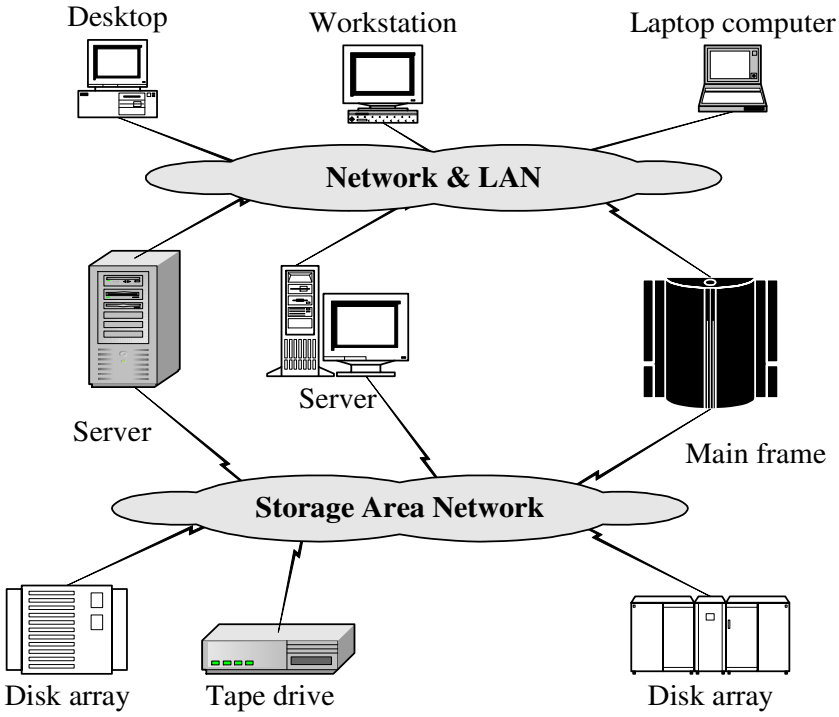
Chương 3: "Ứng dụng SAN giải quyết bài toán thực tiễn", thiết kế mạng lưu trữ giải quyết bài toán lưu trữ khối lượng dữ liệu lớn của Tổng Công ty Bảo Hiểm Việt Nam (Bảo Việt).

Cuối cùng, phần: "Kết luận" tổng hợp lại những nghiên cứu chính của luận văn, giới thiệu một số hướng phát triển và những khắc phục một số những hạn chế hiện tại của SAN.

CHƯƠNG 1: MẠNG LƯU TRỮ - SAN

1.1. Mạng lưu trữ là gì?

Mạng lưu trữ SAN (*Storage Area Network*) được định nghĩa là một mạng dành riêng liên kết giữa các máy chủ và thiết bị lưu trữ [6]. Nó có cấu trúc tương tự mạng cục bộ (*LAN*) nhưng tách biệt khỏi mạng cục bộ. Máy chủ và các thiết bị lưu trữ gọi là các nút (*node*) trong mạng lưu trữ. Sơ đồ mạng lưu trữ được thể hiện qua hình 2



Hình 2 - Sơ đồ mạng lưu trữ

Mạng lưu trữ là giải pháp mới kết nối các thiết bị lưu trữ với máy chủ. SAN sử dụng những tiến bộ trong công nghệ mạng nhằm nâng cao băng thông, hiệu năng thực thi và độ sẵn sàng cao cho hệ thống lưu trữ [6]. Mạng lưu trữ được sử dụng để kết nối: các mạng đĩa được chia sẻ (*Shared Storage Array*), các cụm máy chủ (*Cluster Server*), các đĩa hay ổ băng từ của máy tính lớn (*MainFrame Disk or Tape*) với các máy chủ hoặc máy trạm. Đơn giản, mạng lưu trữ là một mạng thông thường

được tạo nên từ giao diện các thiết bị lưu trữ.

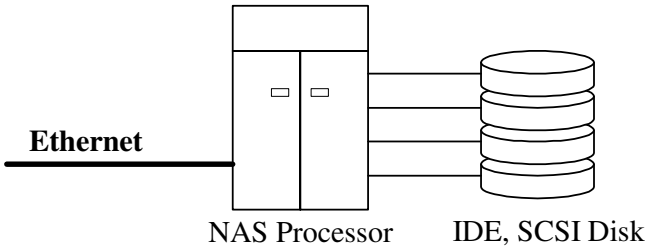
Do mạng lưu trữ tách biệt với hệ thống mạng thông thường nên khi hoạt động sẽ không chiếm băng thông của hệ thống mạng. Mạng lưu trữ thể hiện một hướng chia sẻ không gian lưu trữ mới, cho phép nhiều máy chủ cùng chia sẻ một không gian lưu trữ. Mạng lưu trữ hỗ trợ ba kiểu trao đổi dữ liệu:

- Máy chủ tới thiết bị lưu trữ: là kiểu kết nối truyền thống, mạng lưu trữ có ưu điểm lớn là cho phép nhiều máy chủ truy xuất tuần tự hoặc cùng lúc tới một thiết bị lưu trữ.
- Máy chủ tới máy chủ: sử dụng mạng lưu trữ làm đường truyền thông giữa các máy chủ.
- Thiết bị lưu trữ tới thiết bị lưu trữ: cho phép truyền tải dữ liệu giữa các thiết bị lưu trữ mà không có sự can thiệp của máy chủ. Điều này giúp cho dữ liệu được truyền tải nhanh hơn đồng thời không tốn thời gian xử lý của CPU.

Tuy cấu trúc giống mạng thông thường, mạng lưu trữ SAN có một số khác biệt do được tạo dựng từ giao diện các thiết bị lưu trữ. Nếu như trong mạng thông thường giao diện kết nối có dạng tuần tự thì trong mạng lưu trữ giao diện kết nối có thể là các chuẩn kết nối song song.

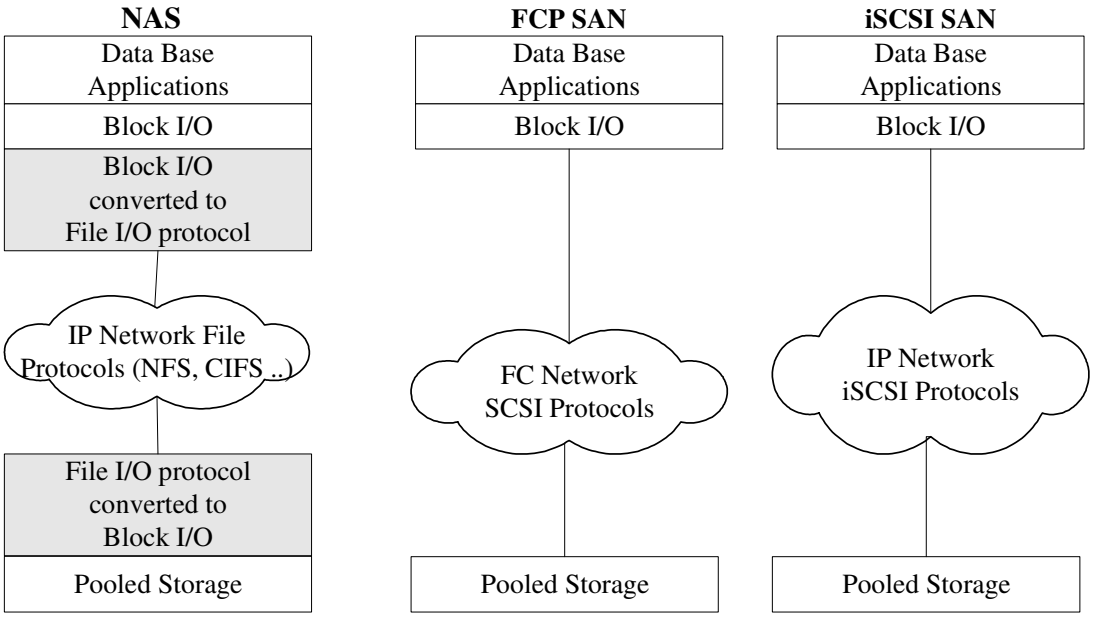
1.2. Thiết bị lưu trữ gắn mạng (NAS - Network Attached Storage)

Thiết bị lưu trữ gắn mạng (NAS - Network Attached Storage) là dãy các đĩa gắn trực tiếp với mạng LAN thông qua giao diện kết nối như Ethernet [6]. Với chức năng là một máy chủ trong mô hình *Client/Server*, NAS có bộ vi xử lý riêng, hệ điều hành riêng và đối tượng xử lý là các file. Đại diện tiêu biểu nhất cho mô hình thiết bị lưu trữ gắn mạng là *Server Message Block* và *Network File System*.



Hình 3 - Kiến trúc NAS

Phân biệt NAS với SAN: dựa trên phương thức trao đổi dữ liệu theo file hay khối (*block*). NAS truyền tải các file qua các giao thức hướng file như *NFS (Network File System)* hay *CIFS (Common Internet File System)* trong khi SAN truyền tải các khối bằng giao thức hướng khối như *SCSI-3*.



Hình 4 - So sánh NAS và SAN

1.3. Các thành phần của mạng lưu trữ - SAN Components

1.3.1. Máy chủ SAN

Máy chủ SAN là những phần tử tính toán được gắn trực tiếp vào mạng SAN [3]. Máy chủ SAN có nhiệm vụ quản lý tôpô mạng và trừu tượng hóa thiết bị lưu trữ. Máy chủ SAN có thể hoạt động trên nhiều hệ điều hành khác nhau như

Windows NT, UNIX, OS/390. Một mạng SAN có thể có nhiều máy chủ SAN hoạt động trong một môi trường hỗn hợp.

1.3.2. Giao diện kết nối SAN

SCSI, FC-AL, SSA, ESCON, Bus-and-Tag, và *HIPPI* là những giao diện kết nối thường được sử dụng trong SAN. Những giao diện này cho phép thiết bị lưu trữ được mở rộng phạm vi khỏi máy chủ và có thể chia sẻ dữ liệu. Chúng ta có thể sử dụng nhiều kênh kết nối để tăng hiệu năng thực thi cũng như tạo kênh dư thừa (dự phòng). Tuy SCSI là giao diện truyền dữ liệu song song, người quản trị vẫn có thể mở rộng, trộn kênh, chuyển mạch, hay kết nối với cổng mạng giống như với giao diện nối tiếp.

1.3.3. Kết nối SAN

Giống như mạng LAN, SAN thường sử dụng một số thiết bị như *Extenders, Mux, Hubs, Routers, Switchs, Directors* để kết nối giữa các thành phần SAN. Trong giải pháp mạng SAN cụ thể, người ta có thể sử dụng nhiều loại thiết bị và kiến trúc kết nối khác nhau để đạt được hiệu quả tốt nhất.

1.3.3.1 Các thiết bị kết nối SAN

- **Thiết bị điều hợp (Host Bus Adapter)**: HBA là thiết bị kết nối giữa thiết bị chủ quản (thiết bị lưu trữ hay máy chủ) với mạng SAN và chức năng của nó là biến đổi những tín hiệu song song từ bus của thiết bị lưu trữ hay của máy chủ sang dạng tín hiệu tuần tự để gửi vào mạng SAN.

  Một HBA có thể có nhiều cổng giao tiếp cùng hay khác loại nhằm cung cấp thêm kết nối với mạng SAN. Cũng tương tự, một thiết bị chủ quản có thể được gắn một hoặc nhiều thiết bị điều hợp cùng hay khác loại.
- **Thiết bị kéo dài (Extenders)**: Thiết bị kéo dài được sử dụng để kéo dài khoảng cách cho phép giữa các nút trong mạng SAN. Về mặt vật lý, thiết kéo dài là một bộ khuyếch đại lại tín hiệu.
- **Bộ trộn (multiplexors)**: bộ trộn được sử dụng để tận dụng hiệu quả của

đường kết nối băng thông rộng bằng cách trộn dữ liệu luân phiên từ nhiều nguồn khác nhau vào một kết nối duy nhất. Bộ trộn còn có nhiều ưu điểm khác: cho phép nén dữ liệu, sửa lỗi, nâng cao tốc độ truyền và khả năng ngắt nhiều kết nối một lúc.

- **Bộ tập trung (hubs):** bộ tập trung cung cấp kết nối giữa các nút với nhau. Tất cả các nút này cùng chia sẻ băng thông nên hiệu quả đạt được không cao như bộ chuyển mạch.
- **Bộ định tuyến (routers)**: bộ định tuyến cho thiết bị lưu trữ khác với bộ định tuyến ở mạng thông thường. Dữ liệu được định tuyến sử dụng các giao thức định tuyến cho thiết bị lưu trữ như FCP hay SCSI trong khi mạng thông thường sử dụng các giao thức thông điệp như TCP/IP. Đường truyền dữ liệu trong các thiết bị lưu trữ giống đường truyền thông điệp trong mạng thông thường nhưng nội dung truyền sẽ chứa những thông tin riêng của giao thức.
- **Cầu (Brigdes)**: cầu thường được sử dụng để kết nối những đoạn mạng LAN/SAN hoặc những mạng có giao thức khác nhau.
- **Cổng mạng (Gateways)**: cổng mạng dùng để kết nối hai hoặc nhiều mạng có giao thức không giống nhau. Thiết bị này thường được dùng để kết nối giữa LAN và WAN. SAN sử dụng cổng mạng để mở rộng mạng thông qua mạng WAN.
- **Bộ chuyển mạch(switchs)**: bộ chuyển mạch là một trong những thiết bị được sử dụng nhiều nhất. Bộ chuyển mạch có nhiều ưu điểm như: cung cấp khả năng kết nối đến một lượng lớn thiết bị, băng thông lớn, giảm thiểu tắc nghẽn, dễ mở rộng. Vì bộ chuyển mạch hỗ trợ kiểu kết nối tới một điểm bất kỳ nên phần mềm quản lý bộ chuyển mạch có thể đặt tuỳ chọn kết nối riêng cho từng cổng. Một số công ty lớn sử dụng dư thừa bộ chuyển mạch hoặc cấu hình nhiều bộ chuyển mạch song song nhằm tăng băng thông và khả

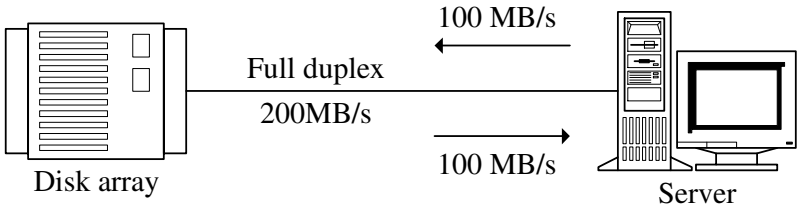
năng chịu lỗi [3].

- **Bộ định hướng (Directors)**: như bộ chuyển mạch nhưng được sử dụng với giao diện kết nối ESCON.

1.3.3.2 Các kiến trúc kết nối SAN

Việc lựa chọn kiến trúc kết nối SAN có ảnh hưởng nhiều đến hiệu năng của toàn bộ hệ thống cũng như quyết định trang thiết bị kết nối. Kênh truyền vật lý trong kiến trúc kết nối mà luận văn đề cập là kênh quang học (*Fibre channel*). Các kiến trúc kết nối trong mạng SAN.

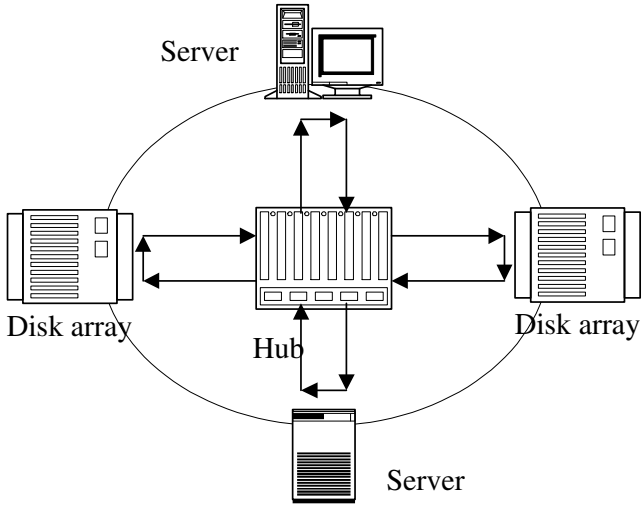
- **Kết nối trực tiếp điểm - điểm (point to point topology):** đây là phương thức kết nối dễ thực hiện và dễ quản trị nhất. Một kênh kết nối cao tốc được được thiết lập giữa hai nút như ở hình 5.



Hình 5 - Kiến trúc kết nối điểm tới điểm

Kiến trúc kết nối có hiệu quả khi kết nối các máy chủ cung cấp dịch vụ file (*File server*) tới chuỗi các đĩa (*Disk array*). Kiến trúc không sử dụng thiết bị kết nối sẽ giảm chi phí cho hệ thống nhưng không thể áp dụng cho những mạng SAN lớn.

- **Kết nối vòng (loop) với thiết bị tập trung (Hubs):** kiểu kiến trúc này cho phép ta xây dựng được kết nối có băng thông rộng và chi phí thấp. Một nút muốn truyền dữ liệu sẽ phải đợi nhận được thẻ điều khiển kênh (giống như thẻ bài trong mạng *Token Ring*). Khi đó, nút có thẻ điều khiển kênh sẽ thiết lập một kết nối kiểu điểm - điểm (kết nối ảo) tới một nút khác trên vòng. Dữ liệu được trao đổi giữa hai nút đó. Khi quá trình trao đổi hoàn thành, các nút khác trong vòng sẽ nhận được thẻ điều khiển kênh.

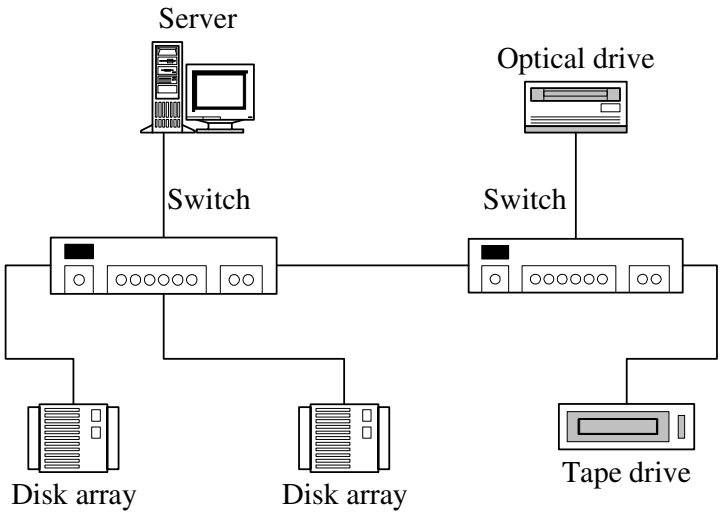


Hình 6 - Kiến trúc kết nối vòng

Kiến trúc kết nối vòng có một số đặc điểm sau:

- Hạn chế số thiết bị kết nối trong một vòng: 126 thiết bị.
- Một nút trong vòng bị hỏng không ảnh hưởng đến hoạt động của vòng.
- Tự dò tìm (quá trình này xác định được toàn bộ các nút trên vòng và thông báo cho mọi nút khác).
- Cho phép thiết lập kết nối ảo (giữa hai thiết bị trong vòng).
- Một vòng có thể kết nối với thiết bị chuyển mạch *(Switch)* để mở rộng vòng.

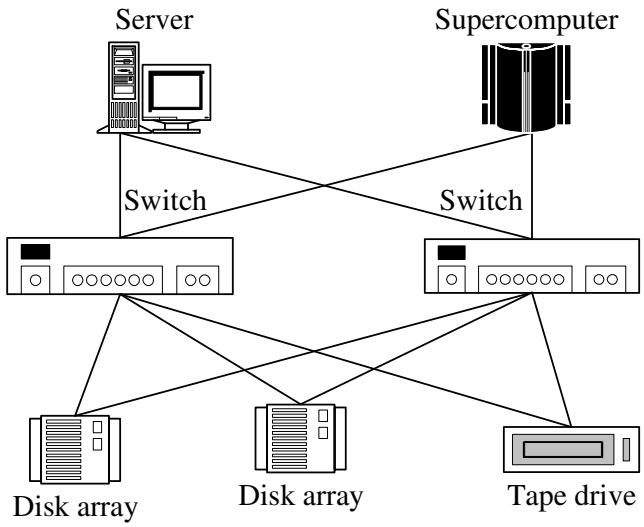
- **Kiến trúc chuyển mạch (Switches)**: Kiến trúc này hay được sử dụng trong thực tế với nhiều ưu điểm như: băng thông rộng, số lượng thiết bị kết nối lớn, có khả năng mở rộng tốc độ thực thi, cho phép sự dư thừa đường kết nối.



Hình 7 - Kiến trúc chuyển mạch

Qua việc tìm hiểu các kiến trúc kết nối mạng SAN trên, chúng tôi nhận thấy có thể xây dựng cấu trúc mạng SAN từ nhiều bộ chuyển mạch cho phép kết nối nhiều thiết bị với nhau. Khi các bộ chuyển mạch được kết nối với nhau, thông tin cấu hình của từng bộ chuyển mạch sẽ được sao chép cho các bộ chuyển mạch khác. Hiện nay có hai dạng kiến trúc chuyển mạch: chuyển mạch không phân tầng và chuyển mạch phân tầng [3].

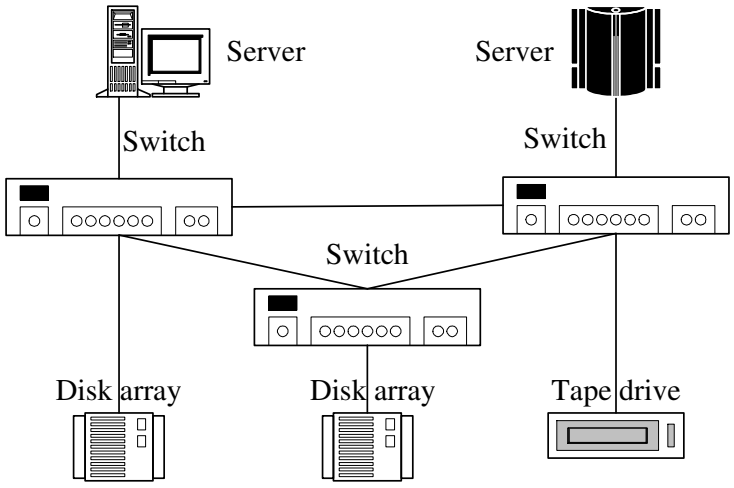
Chuyển mạch không phân tầng (without cascading): chuyển mạch không phân tầng được ứng dụng trong những hệ thống lớn có hiệu năng cao. Hệ thống không kết nối trực tiếp các bộ chuyển mạch với nhau mà thiết lập cấu hình đảm bảo bất kỳ hệ thống con nào đều có thể truy cập được tới mọi bộ chuyển mạch. Với cấu hình này, hệ thống vẫn hoạt động liên tục khi một bộ chuyển mạch bị hỏng, tuy hiệu năng của hệ thống sẽ bị giảm đi so với lúc ban đầu.



Hình 8 - Kiến trúc chuyển mạch không phân tầng

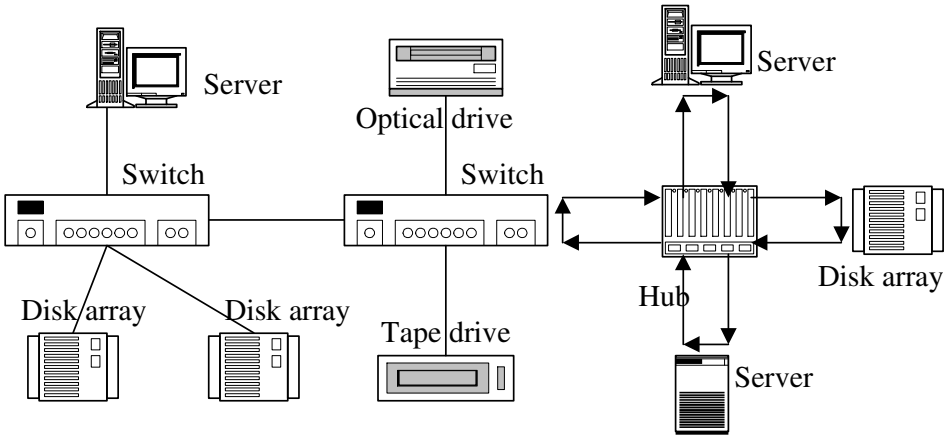
Chuyển mạch có phân tầng (Cascade Switching): Kiến trúc này liên kết các bộ chuyển mạch với nhau tạo thành bộ chuyển mạch logic có các cổng là tập cổng của các bộ chuyển mạch riêng lẻ. Mọi cổng trong kiến trúc chuyển mạch phân tầng đều liên thông với các cổng còn lại.

Với mô hình này công việc quản lý phức tạp hơn. Người quản trị cần phát hiện kịp thời đường liên kết hỏng giữa các bộ định tuyến để đảm bảo tính liên thông và kiểm soát việc lưu thông giữa các khối dữ liệu trong mạng



Hình 9 - Kiến trúc chuyển mạch phân tầng

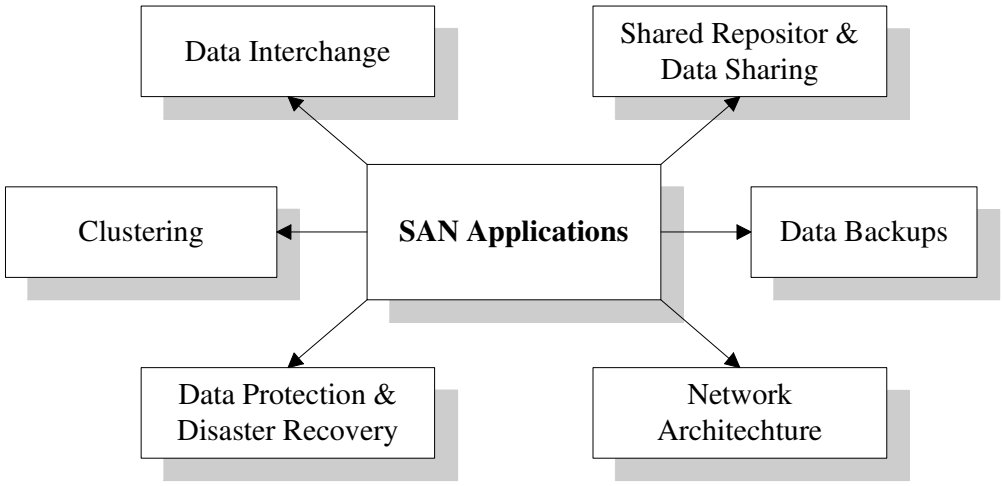
Kết hợp kiến trúc chuyển mạch và Kiến trúc vòng (Mixed topology): Để kết hợp kiến trúc chuyển mạch và kiến trúc vòng, bộ chuyển mạch phải có cổng lặp để gắn kết vào vòng. Quá trình phát hiện thiết bị và phần mềm quản lý SAN sẽ trở nên phức tạp hơn khi hệ thống áp dụng kiến trúc này.



Hình 10 - Kiến trúc chuyển mạch hỗn hợp

1.3.4. Ứng dụng SAN

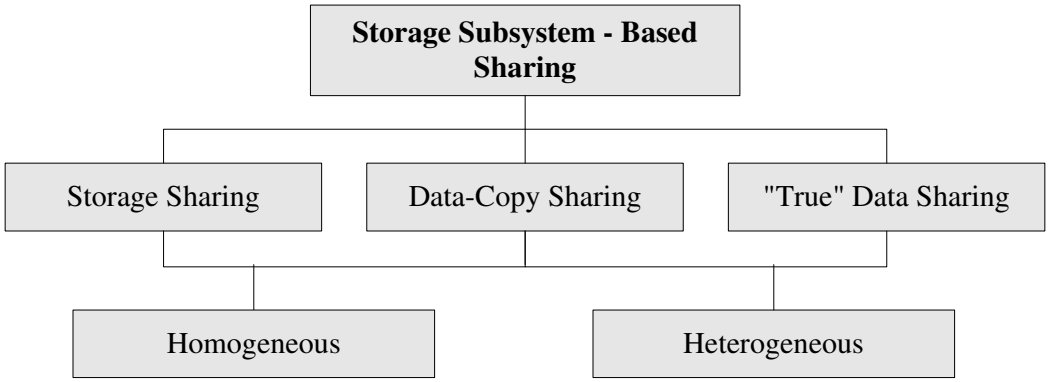
Mạng lưu trữ cung cấp cho các ứng dụng: khả năng quản lý, khả năng mở rộng và tốc độ thực thi. Một số ứng dụng đặc trưng trong mạng SAN [3]:



Hình 11 - Các ứng dụng SAN

- ***Chia sẻ không gian lưu trữ và chia sẻ dữ liệu***: SAN hỗ trợ mở rộng không gian lưu trữ và tập trung hóa dữ liệu. Khi đó, dữ liệu được chia sẻ giữa

nhiều máy chủ mà không ảnh hưởng đến hiệu năng hệ thống. Khái niệm "chia sẻ dữ liệu" mô tả khả năng truy cập dữ liệu chung bởi nhiều máy chủ. Các máy chủ lưu trữ dữ liệu chia sẻ có thể được cài đặt trên nhiều hệ điều hành khác nhau.



Hình 12 - Chia sẻ không gian lưu trữ và chia sẻ dữ liệu

+ Chia sẻ không gian lưu trữ (*Storage Sharing*): Cho phép một hoặc nhiều máy chủ chia sẻ cùng một không gian lưu trữ con. Không gian lưu trữ con cũng có thể được chia làm nhiều phân vùng (partition) và mỗi phân vùng được sở hữu bởi một hoặc nhiều máy chủ.

+ Chia sẻ bản sao dữ liệu (*Data Copy Sharing*): Bằng cách gửi những bản sao dữ liệu, các máy chủ chạy trên nhiều nền hệ điều hành khác nhau có thể truy xuất cùng một dữ liệu được chia sẻ. Có hai hướng tiếp cận chia sẻ bản sao dữ liệu giữa hai máy chủ: truyền file phẳng (*Flat file*) và dùng ống chuyển đổi (Piping).

+ Chia sẻ dữ liệu thực (*True Data Sharing*): dữ liệu chia sẻ có thể được truy xuất bởi nhiều máy chủ chạy trên các nền hệ điều hành khác nhau. Hiện các ứng dụng kiểu này chỉ sử dụng được trên các máy chủ có nền tảng đồng nhất như Oracle Parallel Server hay OS/390 Parallel Sysplex. Có ba cơ chế chính thực hiện việc chia sẻ dữ liệu thực:

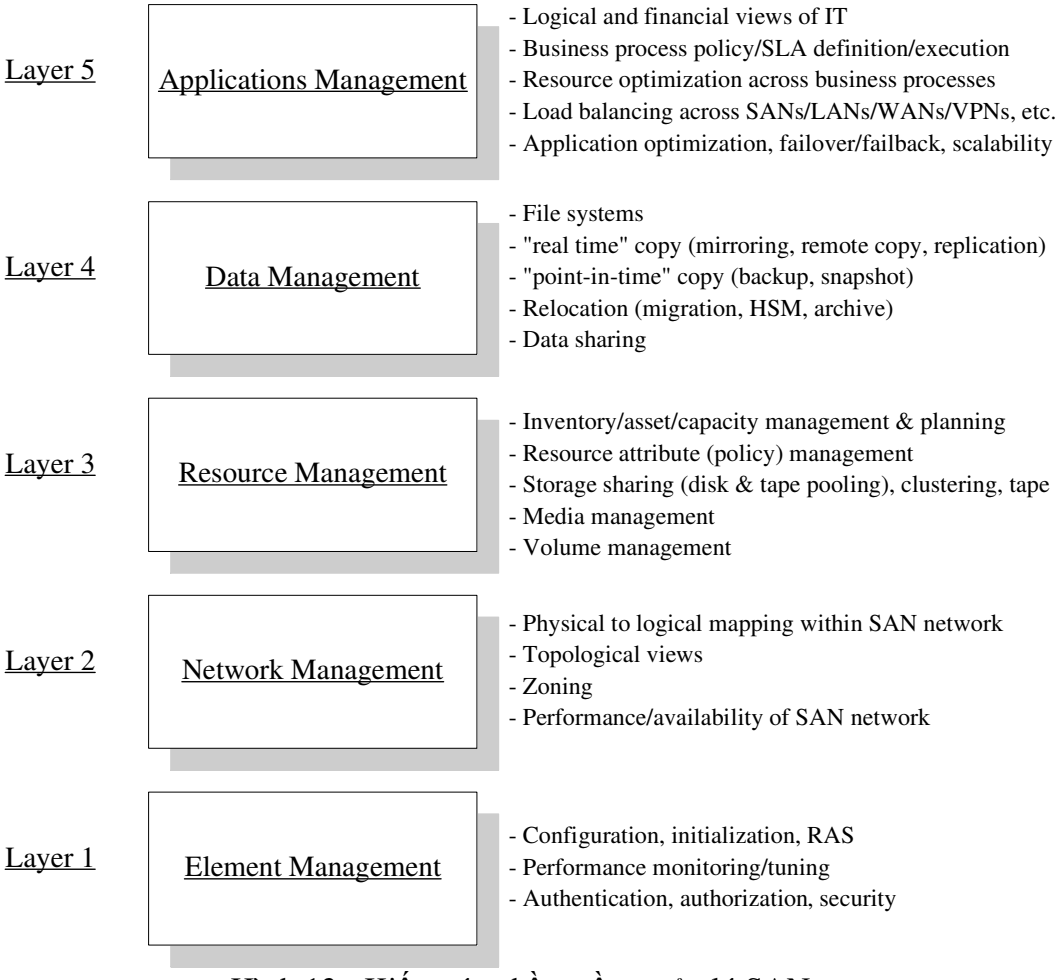
- Tuần tự, tại từng thời điểm chỉ có một máy chủ có thể truy xuất dữ liệu.

- Nhiều máy chủ đồng thời đọc dữ liệu và chỉ có một máy chủ được phép cập nhật dữ liệu.
- Nhiều máy chủ đồng thời đọc và ghi dữ liệu.

- **Kiến trúc mạng**: Trong hệ thống, mạng thông điệp như Ethernet thường được xác định là mạng chính, SAN được coi là mạng thứ hai (còn gọi là mạng sau máy chủ - *The Network behind the Server*). Kiến trúc mạng này cho phép tập trung hóa không gian lưu trữ bằng cách sử dụng kết nối như mạng LAN, WAN với các thiết bị như *router, hub, switch, gateway.* Khi đó, SAN được hiểu như mạng cục bộ hay từ xa, chia sẻ hoặc dành riêng. Chính vì lý do trên, mạng SAN được đánh giá có khả năng sẵn sàng, tốc độ thực thi và khả năng mở rộng trong không gian lưu trữ.
- **Sao lưu dữ liệu (Data backup)**: SAN cho phép truyền thông giữa các thiết bị lưu trữ nên dữ liệu có thể chuyển trực tiếp từ đĩa đến ổ băng từ. Dữ liệu từ các đĩa khác nhau được sao lưu trên những ổ băng từ dùng chung. Thao tác sao lưu dữ liệu được lập lịch và quản lý tập trung, không gây ảnh hưởng tới mạng LAN cũng như giải phóng máy chủ khỏi công việc sao lưu số liệu.
- **Tính toán cụm (Clustering)**: Nhờ nhiều máy chủ hoạt động đồng thời trên một tập dữ liệu, tính toán cụm cung cấp tốc độ thực thi và khả năng chịu lỗi cao hơn cho ứng dụng. SAN cung cấp môi trường tính toán cụm hiệu quả bởi chúng cho phép nhiều máy chủ truy xuất dữ liệu dùng chung với băng thông rộng.
- **Bảo vệ dữ liệu và khôi phục dữ liệu**: Kỹ thuật nhân bản dữ liệu (*replication/mirror*) được áp dụng để đảm bảo cho ứng dụng vẫn tiếp tục hoạt động ngay cả khi một bản dữ liệu bị hỏng. SAN tạo và liên kết các bản sao để bảo vệ và khôi phục dữ liệu bằng phương pháp dư thừa dữ liệu nhằm đáp ứng các ứng dụng có yêu cầu sẵn sàng cao.

1.3.5. Quản lý SAN

Lựa chọn phần mềm quản lý SAN là một trong những điểm mấu chốt trong các giải pháp SAN. Để tận dụng được các điểm mạnh của SAN nhất thiết phải có phần mềm quản lý SAN hiệu quả và phần mềm này có thể được cài đặt trên các máy chủ SAN.



Hình 13 - Kiến trúc phần mềm quản lý SAN

Nhằm tạo tiền đề cho các nhà phát triển, tổ chức SNIA đã đưa ra một chuẩn mở mô tả kiến trúc phần mềm quản lý SAN. Mô hình kiến trúc được tổ chức theo phân cấp lớp, mỗi lớp đảm nhiệm cung cấp những chức năng khác nhau và cung cấp dịch vụ cho lớp bên trên hoặc bên dưới.

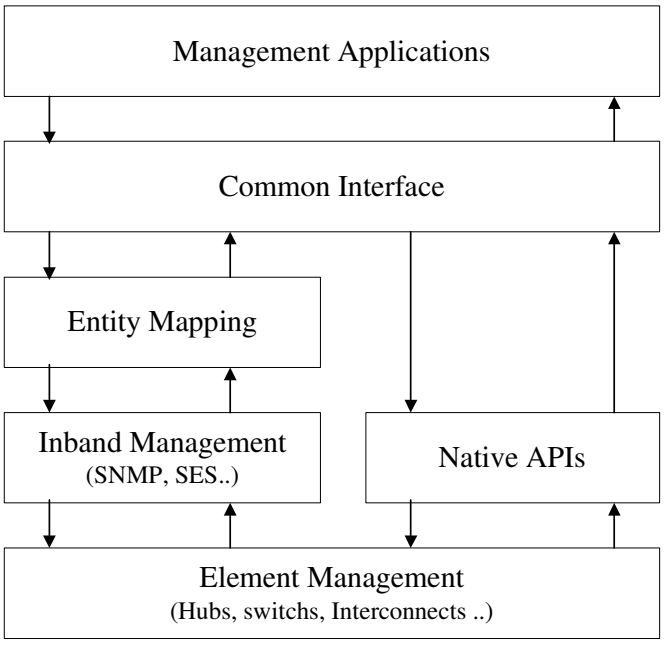
*** Lớp quản lý ứng dụng- Applications Management:**

Đây là lớp quản lý cao nhất trong mô hình, có nhiệm vụ cung cấp một khung nhìn trong suốt và toàn diện về toàn bộ tài nguyên hệ thống. Các thông tin như cấu hình, trạng thái, hiệu năng, dung lượng hữu dụng... đều được chuyển từ những tầng bên dưới lên cho lớp ứng dụng quản lý.

Các chức năng của lớp ứng dụng quản lý bao gồm:

- Cung cấp cái nhìn chi tiết và logic về hệ thống SAN.
- Thiết lập và thực thi chính sách giao dịch, bảo mật.
- Tối ưu hóa tài nguyên theo mô hình nghiệp vụ.
- Cân bằng tải trong SAN, LAN, WAN, VPNs …
- Tối ưu hóa ứng dụng, ngăn ngừa lỗi, khắc phục lỗi.

Hai tổ chức SNIA và SNMWG đưa ra mô hình giao tiếp chung (*Common Interface Model*) làm chuẩn giao tiếp của lớp ứng dụng với lớp dưới. Đây là cơ sở cho các nhà phát triển viết ứng dụng SAN hoạt động được trên môi trường hỗn hợp.



Hình 14 - Mô hình giao diện chung cho phần mềm quản lý SAN

*** Lớp quản lý dữ liệu - Data Management**:

Lớp này chịu trách nhiệm kiểm soát về chất lượng dịch vụ dữ liệu:

- Đảm bảo tính sẵn sàng dữ liệu và cung cấp khả năng truy cập dữ liệu cho các ứng dụng.
- Đảm bảo về mặt hiệu năng dữ liệu cho các ứng dụng.
- Đảm bảo khả năng khôi phục dữ liệu.

Và lớp còn cung cấp các dịch vụ dữ liệu cơ sở:

- Dịch vụ file.
- Các dịch vụ sao chép thời gian thực: tạo ảnh (*mirroring*), nhân bản (*replication*).
- Các dịch vụ sao chép tại một thời điểm: sao lưu, bản chụp nhanh.
- Các dịch vụ di chuyển dữ liệu
- Chia sẻ dữ liệu.

*** Lớp quản lý tài nguyên - Resource Management:**

Lớp quản lý tài nguyên liên quan tới hiệu quả sử dụng, tính thống nhất, tự động hóa quản lý tài nguyên lưu trữ và kiến trúc lưu trữ. Nó còn cung cấp khả năng tự động sửa lỗi khi cần. Lớp này cung cấp các chức năng:

- Tạo quỹ đĩa.
- Quản lý không gian lưu trữ.
- Tạo quỹ và chia sẻ thiết bị lưu trữ có thể tháo lắp.
- Tăng cường cho tính năng lưu trữ tức thời.

Yêu cầu của lớp này là phải cung cấp một khung nhìn đơn nhất về hệ thống và từ một điểm có khả năng quản lý được tất cả các nguồn tài nguyên lưu trữ phân tán.

*** Lớp quản lý mạng - Network Management**:

Lớp quản lý mạng thực hiện việc quản lý các kết nối giữa các thực thể của SAN, các thực thể này có thể là thực thể logic hay vật lý. Toàn bộ kiến trúc kết nối và kết nối vật lý của các thành phần của SAN đều được lớp này quản lý. Đồng thời nó còn quản lý các mối quan hệ giữa các thực thể vật lý bằng cách tạo ra các thực thể logic như vùng (*zone*). Lớp này cung cấp các chức năng:

- Ánh xạ logic và vật lý trong mạng lưu trữ.

- Cấu trúc liên kết mạng (*topology*).
- Phân vùng (*zoning*).
- Độ sẵn sàng và hiệu năng mạng của mạng lưu trữ.
- Quản lý lỗi kết nối.

*** Lớp quản lý thành phần - Element Management:**

Lớp này làm việc với các thiết bị phần cứng xây dựng lên SAN. Các thiết bị này có thể là các hệ đĩa thông minh, các thiết bị lưu trữ có thể tháo rời, các bộ chuyển mạch, ..vv. Thông thường các nhà cung cấp thiết bị sẽ cung cấp kèm theo những chương trình cơ sở (*firmware*) để quản lý thiết bị.

Các chức năng cụ thể được lớp này cung cấp bao gồm:

- Cấu hình, khởi tạo, thiết lập kết nối từ xa (RAS) cho các thành phần.
- Theo dõi và điều chỉnh hiệu năng.
- Xác thực, cấp phép và bảo mật.

CHƯƠNG 2: IP SAN

Sau một thời gian dài phát triển và ứng dụng trong thực tế, giao thức TCP/IP trở thành chuẩn chính thức và được ứng dụng trong hầu hết các hệ thống mạng của các doanh nghiệp trên thế giới. Việc ứng dụng SAN dựa trên nền tảng giao thức TCP/IP có những ưu điểm sau:

- SAN được xây dựng từ những thiết bị trong hệ thống mạng LAN nhằm giúp doanh nghiệp tận dụng thiết bị đã được trang bị trước đó, giảm được chi phí đào tạo và chi phí điều hành.
- Có thể sử dụng mạng internet như là công cụ để truyền và lưu trữ dữ liệu khi luồng dữ liệu vượt qua những giới hạn của LAN.

Tuy nhiên, giao thức TCP/IP ban đầu không được thiết kế riêng biệt cho những ứng dụng như SAN nên khi sử dụng SAN trên nền IP tồn tại một số nhược điểm sau:

- TCP sử dụng cơ chế điều khiển luồng và kiểm soát lỗi phức tạp. Điều này sẽ làm giảm hiệu suất truyền tải dữ liệu.
- Quá trình định tuyến (*routing*) và chuyển tiếp gói tin (*forwarding*) đòi hỏi phải có thời gian xử lý thông tin tiêu đề gói tin (*header*), sẽ làm giảm hiệu suất truyền tải dữ liệu.

Những hạn chế trên có thể được khắc phục khi ta sử dụng những thiết bị mạng có hỗ trợ cơ chế đảm bảo chất lượng dịch vụ (*QoS*) hay bộ điều hợp mạng (*Adaptor*) được thiết kế nhằm tăng tốc cho một số tác vụ được sử dụng trong giao thức TCP.

Trong chương này chúng tôi phân tích chi tiết hai giao thức: iSCSI và iFCP - những giao thức được ứng dụng cho SAN dựa trên nền tảng IP.

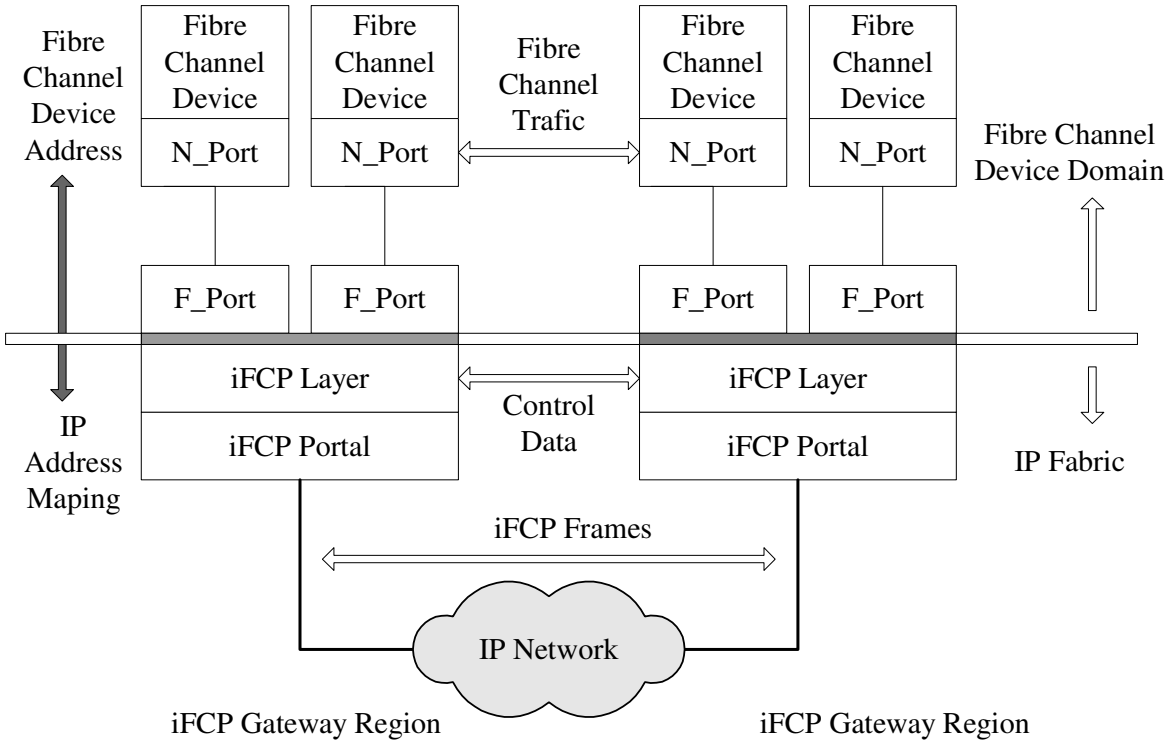
2.1. Giao thức iFCP (Internet Fibre Channel Protocol)

iFCP là giao thức từ cổng mạng tới cổng mạng (*gateway to gateway*), kết nối

các thiết bị kênh quang học đã có bằng cách sử dụng mạng IP nhằm cung cấp dịch vụ kênh quang học (*Fibre Channel Services*) cho các thiết bị cuối có cổng là kênh quang học dựa trên mạng TCP/IP [1]. iFCP sử dụng TCP làm công cụ điều khiển luồng và kiểm soát lỗi.

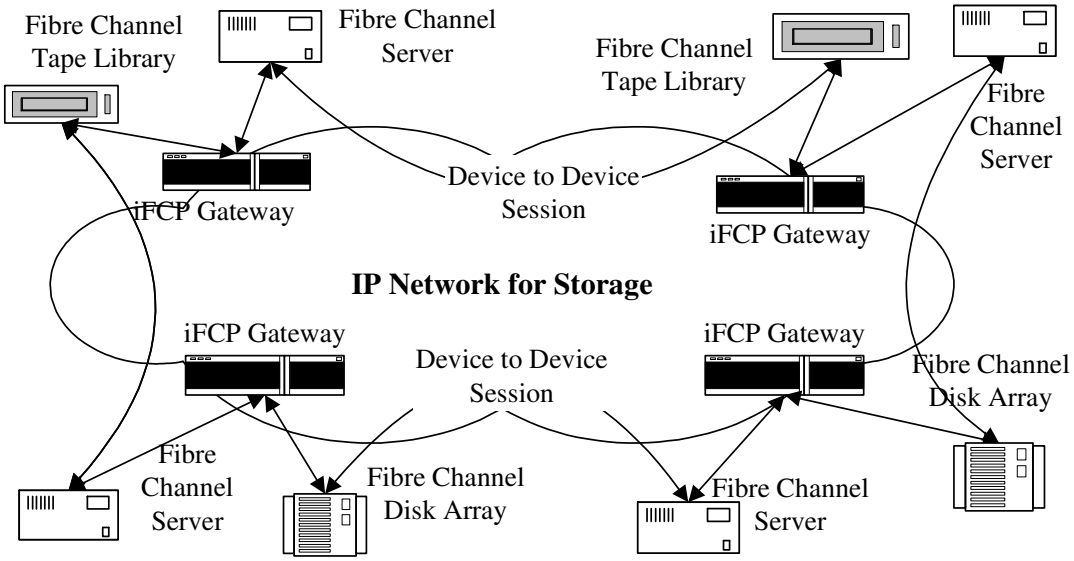
2.1.1. Kiến trúc mạng iFCP

iFCP thích nghi với các thiết bị cuối trên kênh quang học bằng cách giả lập giao diện cổng kết nối quang học (*F_Port*). Khi đó, iFCP có chức năng như một thiết bị chuyển mạch quang học (*Fibre Channel Switch*) như hình 15 dưới đây.



Hình 15 - Kiến trúc iFCP

Tại tầng iFCP, địa chỉ (*24 bit*) của một thiết bị kênh quang học được ánh xạ với một địa chỉ IP duy nhất và cung cấp địa chỉ IP cho thiết bị nguồn và thiết bị đích (thiết bị kênh quang). Tương ứng với tầng vận tải của kênh quang (*FC-2*) được iFCP thay thế bằng giao thức TCP/IP để truyền tải dữ liệu qua mạng IP.



Hình 16 - sử dụng iFCP kết nối các thiết bị thông qua mạng IP

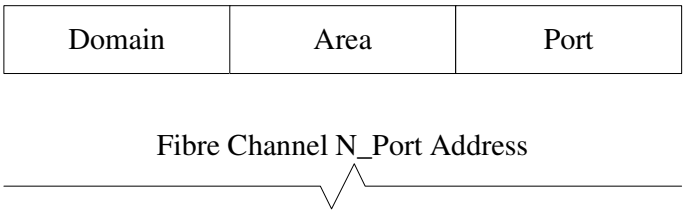
Việc kết nối tới các thiết bị kênh quang được cung cấp thông qua cổng FL_Port (kiến trúc kết nối vòng) hay qua cổng E_Port (kiến trúc kết nối chuyển mạch) giữa một cổng của iFCP (iFCP gateway) và một bộ chuyển mạch quang. Đặc tính này cho phép những SAN kênh quang riêng lẻ có thể được sử dụng trong kiến trúc IP. Lúc này các thiết bị kênh quang được gắn vào thiết bị chuyển mạch quang đó sẽ được gán cho một địa chỉ IP ánh xạ. Như vậy iFCP cung cấp phương thức kết nối mềm dẻo kết nối các thiết bị kênh quang với nhau nên nó có thể được dùng để thay thế các bộ chuyển mạch quang.

3.1.2. Địa chỉ iFCP

Đặc tả iFCP xác định hai chế độ địa chỉ của các thiết bị kênh quang là: chế độ trong suốt (*transparent mode*) và chế độ chuyển đổi (*translation mode*).

Ở chế độ trong suốt, các thiết bị kênh quang được xác định bởi địa chỉ duy nhất có độ dài 24 bit, là địa chỉ theo cách đánh của chuẩn kênh quang. Theo chuẩn này, các bộ chuyển mạch quang chịu trách nhiệm cấp phát một địa chỉ duy nhất cho các thiết bị kênh quang khi các thiết bị này thực hiện quá trình đăng nhập (*login*). Hình 17 thể hiện định dạng địa chỉ của các thiết bị cuối kênh quang, còn được gọi là

địa chỉ N_Port. Địa chỉ N_Port có độ dài 24 bit và chia làm 3 phần, mỗi phần có độ dài 8 bit (1 byte): byte thứ nhất chứa thông tin nhận dạng miền (*Domain ID*), byte thứ hai chứa thông tin nhận dạng vùng (*Area ID*) và byte cuối cùng chứa thông tin nhận dạng cổng (*Port ID*).



Hình 17 - Định dạng địa chỉ N_port của thiết bị kênh quang

Theo chuẩn kênh quang, mỗi bộ chuyển mạch được gán tương ứng với một định danh miền. Như vậy trong một mạng quang thì số miền tối đa là 239 miền và mỗi miền có khả năng cấp phát được 65000 địa chỉ khác nhau cho các thiết bị cuối. Khi biết được địa chỉ của một thiết bị cuối kênh quang, chúng ta có thể xác định được vị trí của thiết bị đó. Định danh miền giúp ta xác định được bộ chuyển mạch mà thiết bị được gắn vào, cặp định danh vùng/cổng (*Area/Port*) giúp ta xác định được cổng mà thiết bị được gắn vào.

Địa chỉ N_Port phụ thuộc vào vị trí của thiết bị trong mạng quang nên khi ta chuyển kết nối của thiết bị từ cổng này sang cổng khác của bộ chuyển mạch hay từ bộ chuyển mạch này sang bộ chuyển mạch khác thì địa chỉ N_Port cũng thay đổi theo. Sự thay đổi địa chỉ N_Port buộc quá trình định tuyến dữ liệu thay đổi. Tuy nhiên thiết bị kênh quang sẽ vẫn được xác định duy nhất nhờ địa chỉ cứng WWN. Địa chỉ WWN là duy nhất trên toàn cầu và có độ dài 64 bit. Địa chỉ WWN không được dùng để định tuyến vì độ dài của nó khá lớn và không có cấu trúc phù hợp với việc định tuyến như địa chỉ N_Port.

Trong khung dữ liệu của kênh quang, có hai trường chứa địa chỉ N_Port: trường D_ID (*Destination ID*) chứa địa chỉ N_Port bên đích đến và trường S_ID (*Source ID*) chứa địa chỉ N_Port bên nguồn. Địa chỉ D_ID và S_ID được sử dụng

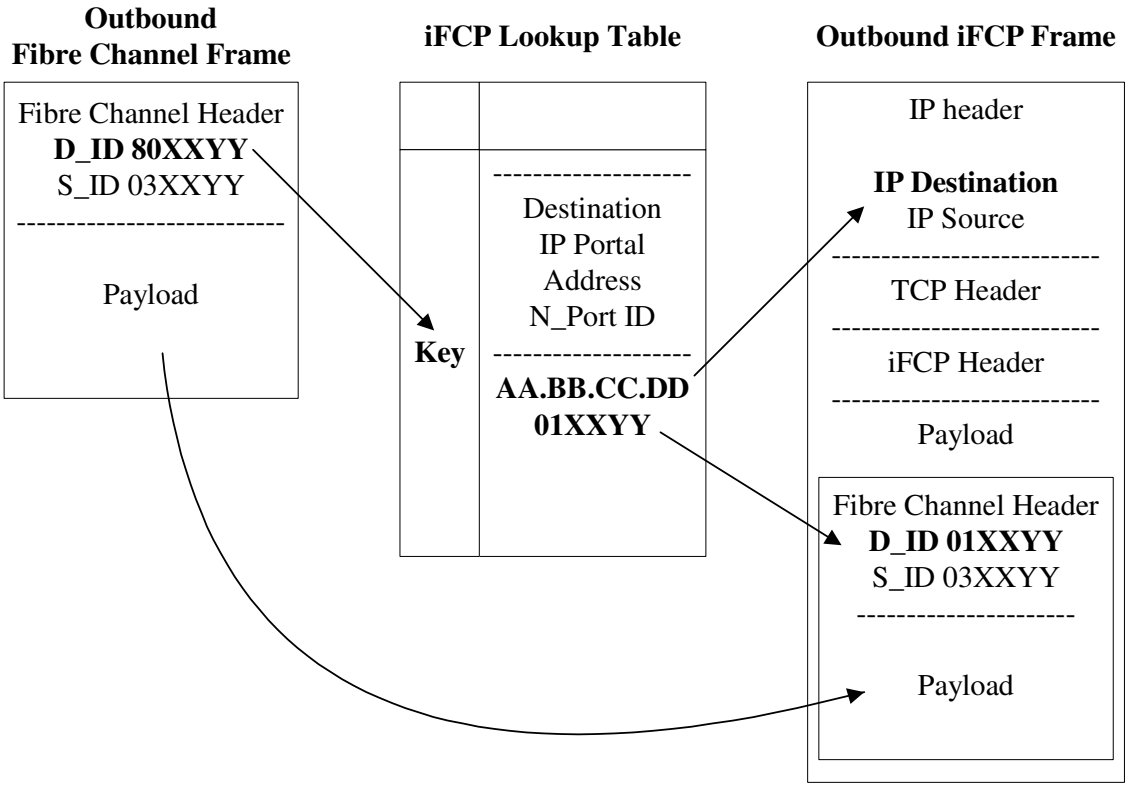
suốt quá trình trao đổi dữ liệu. Kết thúc quá trình giao dịch, trong khung dữ liệu sẽ chứa địa chỉ WWN. Thông tin này rất cần thiết để đảm bảo tính toàn vẹn của giao dịch vì địa chỉ nguồn hoặc đích có thể bị một thiết bị khác chiếm dụng khi thiết bị này được cắm vào chỗ thiết bị nguồn hoặc đích cắm.

iFCP có một số hạn chế do sử dụng lược đồ đánh địa chỉ của mạng quang. Mỗi iFCP gateway đều được coi như một khối gồm 65000 địa chỉ ngay cả khi chỉ có một vài địa chỉ được sử dụng cho vài thiết bị đang hoạt động. Hơn nữa, khi một bộ chuyển mạch được gắn vào, mạng quang sẽ thực hiện quá trình gán định danh miền mới và yêu cầu toàn bộ thiết bị gắn vào nó thực hiện quá trình đăng nhập để cấp phát lại địa chỉ N_Port mới. Một mạng quang có qui mô lớn với nhiều bộ chuyển mạch và thiết bị sẽ mất nhiều thời gian để ổn định lại toàn bộ mạng quang.

Để đảm bảo SAN dựa trên nền tảng IP mở rộng hơn những giới hạn của mạng quang, iFCP còn sử dụng chế độ địa chỉ chuyển đổi. Trong chế độ địa chỉ chuyển đổi, iFCP gateway vẫn gán những địa chỉ N_Port 24 bit cho những thiết bị gắn vào nó. Về mặt chức năng, những giao dịch nội bộ trong cùng một iFCP gateway cũng giống như một bộ chuyển mạch quang. Nhưng không giống với bộ chuyển mạch quang, iFCP gateway còn gán địa chỉ N_Port cho những thiết bị từ xa (không cùng trên một iFCP gateway) và coi chúng như những thiết bị cục bộ. Địa chỉ được gán cho các thiết bị từ xa này còn được gọi là địa chỉ N_Port ủy nhiệm (*proxy address)* và chúng chỉ có thể được sử dụng trong phạm vi cục bộ iFCP gateway, không được quảng bá khắp IP SAN. iFCP gateway thực hiện chuyển đổi địa chỉ N_Port ủy nhiệm với địa chỉ N_Port thực sự. Nó sẽ thay thế trường D_ID của địa chỉ ủy nhiệm bằng địa chỉ thực sự trong khung dữ liệu khi giao dịch. Quá trình này làm tăng thêm thời gian xử lý tại iFCP gateway nhưng nó tránh được những vấn đề phát sinh trong sơ đồ đánh địa chỉ của mạng quang.

iFCP thực hiện ánh xạ địa chỉ IP, địa chỉ này được lưu trong phần thông tin tiêu đề IP (*IP header*) của khung số liệu iFCP. Trong hình 18, iFCP gateway duy trì một bảng tra cứu (*lookup table*) để ánh xạ địa chỉ N_Port với địa chỉ IP. Trong chế

độ chuyển đổi địa chỉ, bảng tra cứu này bao gồm cả địa chỉ N_Port ủy nhiệm và địa chỉ N_Port thực.



Hình 18 - Chế độ chuyển đổi địa chỉ iFCP và địa chỉ IP

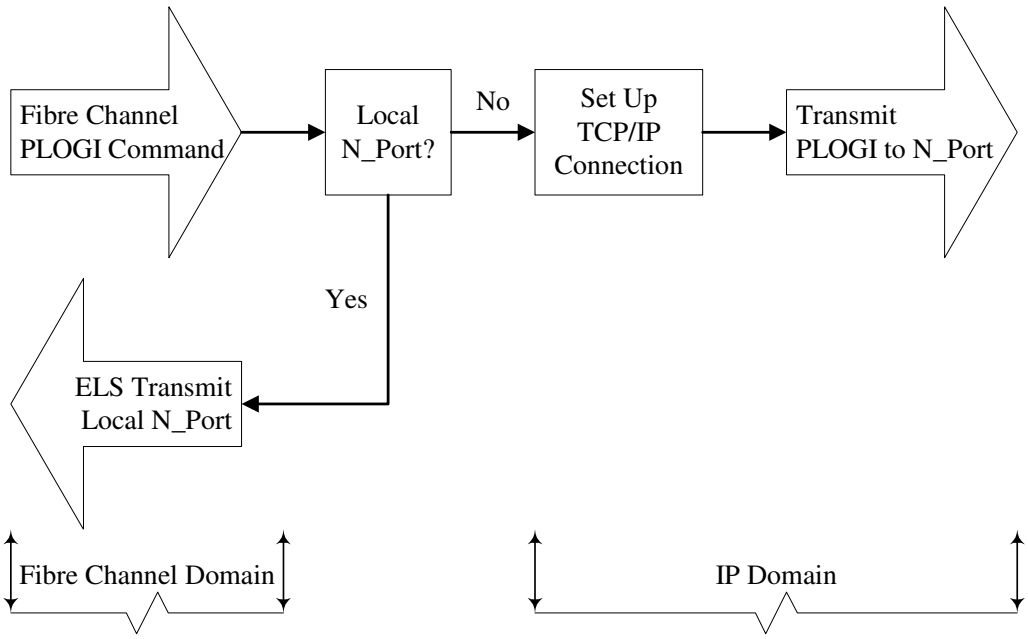
Trong sơ đồ trên, "80" là giá trị định danh miền của địa chỉ D_ID trong mạng quang. địa chỉ N_Port ủy nhiệm trong khung số liệu này thông báo với iFCP rằng: khung số liệu này cần được chuyển đến một thiết bị từ xa nào đấy. iFCP gateway thực hiện thao tác tìm địa chỉ trong bảng tìm kiếm, kết quả trả về là địa chỉ IP và N_Port thực tương ứng. Trong quá trình xây dựng khung dữ liệu iFCP, địa chỉ N_Port thực sự được gắn vào phần thông tin tiêu đề kênh quang, địa chỉ IP đích được điền vào phần thông tin tiêu đề IP của khung số liệu iFCP.

Quá trình ánh xạ và chuyển đổi địa chỉ làm tăng thời gian trễ xử lý. Tuy nhiên trong thực nghiệm, iFCP vẫn có thể đạt được tốc độ gigabit.

2.1.3. Giả lập dịch vụ kênh quang học của iFCP

Giao thức iFCP được thiết kế hỗ trợ thiết bị cuối quang học cũng như thiết bị thuần

iFCP. Do một cổng mạng iFCP có thể thay thế trực tiếp một bộ chuyển mạch kênh quang và cho phép kết nối N_Port, nó phải giả lập những dịch vụ kênh quang chuẩn như đăng nhập, đăng ký SNS và ELS. Hơn nữa iFCP gateway chặn các yêu cầu của kênh quang như đăng nhập cổng (*PLOGI*) và phải thiết lập kết nối TCP/IP với iFCP gateway đích.

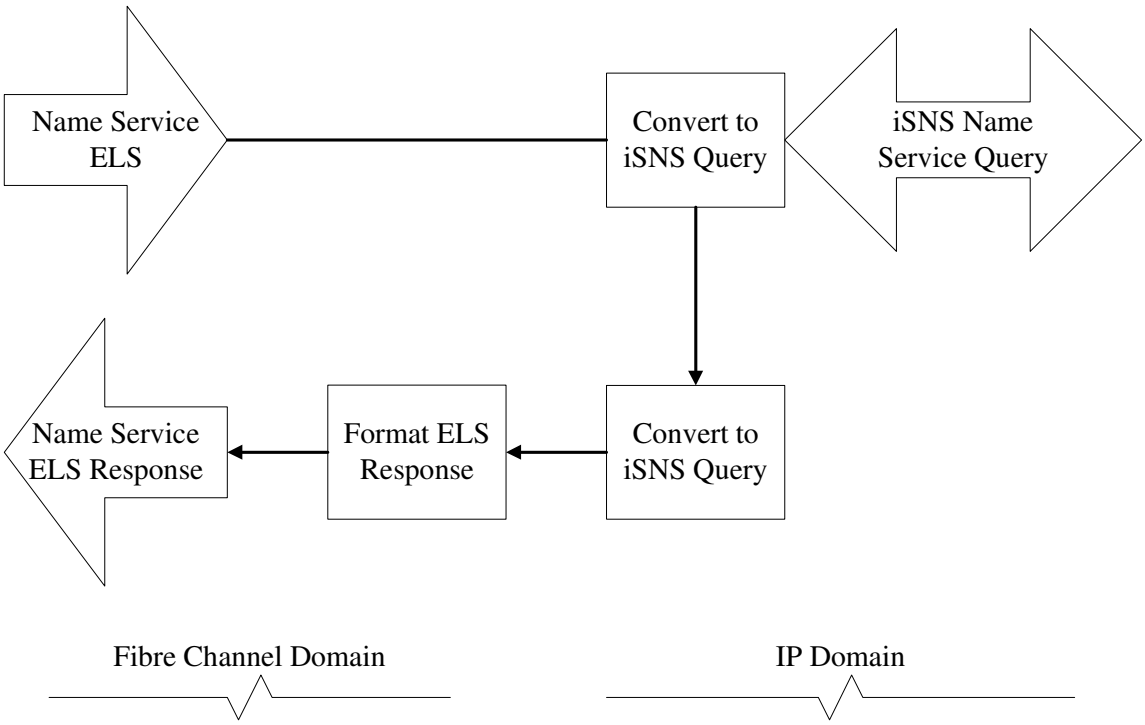


Hình 19 - iFCP gateway xử lý PROGI

Hình 19 minh họa quá trình một thiết bị kênh quang cục bộ gửi yêu cầu PLOGI tới đích. Đầu tiên, iFCP phải xác định đích là cục bộ hay ở xa. Nếu PLOGI được gửi đến địa chỉ đích là một thiết bị cục bộ, iFCP chuyển tiếp tới cổng tương ứng. Ngược lại, cổng mạng iFCP thiết lập kết nối TCP/IP đến đúng iFCP gateway có gắn thiết bị đó và gửi yêu cầu PLOGI thông qua khung dữ liệu iFCP. Bước tiếp theo là quá trình đàm phán về kích cỡ tối đa của khung số liệu giữa hai thiết bị kênh quang, kết quả đàm phán được cập nhật vào trường qui định kích cỡ tối đa cho khung số liệu. Nói chung, cổng mạng iFCP khi đàm phán sẽ đề nghị kích cỡ gói dữ liệu tối đa là 1.5KB để đảm bảo khung số liệu kênh quang được đóng gói trong mạng Ethernet mà không làm phân mảnh gói tin

Trong mạng kênh quang, bên nguồn gửi truy vấn SNS tới bộ chuyển mạch, kết

quả nhận được là danh sách địa chỉ kênh quang của bên đích. iFCP gateway cũng giả lập dịch vụ này, nhưng lại chuyển đổi truy vấn SNS thành truy vấn iSNS. Khi nhận được phản hồi từ máy chủ iSNS, iFCP gateway ghi lại địa chỉ kênh quang và địa chỉ IP tương ứng vào trong bảng chuyển đổi địa chỉ (*Translation Table Address*) và định dạng thành hồi đáp SNS để gửi cho bên nguồn. Hình 20 thể hiện một quá trình xử lý yêu cầu SNS, trong quá trình này việc cập nhật lại bảng chuyển đổi địa chỉ để tạo thuận lợi cho quá trình truyền thông sau này giữa bên nguồn và bên đích.



Hình 20 - Quá trình iFCP gateway xử lý một yêu cầu SNS

Nhằm hỗ trợ các thiết bị kênh quang gửi và nhận yêu cầu một cách thuận tiện, iFCP sử dụng những địa chỉ đã được chuẩn hóa trong kênh quang. Ví dụ dịch vụ SNS có địa chỉ "FF FF FC" ở cả bộ chuyển mạch và iFCP.

2.1.4. Điều khiển kết nối TCP và iFCP

iFCP gatewway có hai loại giao tiếp: F_Port giao tiếp với thiết bị cuối kênh quang và FCP Portal giao tiếp với mạng TCP/IP. iFCP gateway không sử dụng dịch vụ truyền của kênh quang (dựa trên giao thức định tuyến FSPF - *Fabric Shortest*

Path First) mà thiết lập kết nối TCP/IP tới iFCP gateway khác và sử dụng giao thức định tuyến như OSPF (*Open Shortest Path First*) để truyền.

Khi các thiết bị đã phát hiện ra nhau thông qua iSNS, iFCP gateway có thể thiết lập nhiều kết nối TCP/IP giữa chúng. Kết nối TCP được quản lý nhờ hình thức trao đổi thông điệp kết nối giữa các iFCP gateway. Kết nối TCP gọi là có ràng buộc khi cổng N_Port đang lưu thông dữ liệu sử dụng kết nối này. Kết nối TCP gọi là không ràng buộc khi kết nối tồn tại nhưng không có sự lưu thông dữ liệu. Khi thiết bị kênh quang gửi yêu cầu PLOGI tới một thiết bị kênh quang khác không gắn cùng iFCP gateway, iFCP gateway chọn một kết nối TCP không ràng buộc nếu có hoặc thiết lập kết nối TCP mới cho phiên đăng nhập đó. Một kết nối TCP không ràng buộc sẽ trở thành kết nối TCP ràng buộc nếu iFCP đưa ra lệnh ràng buộc kết nối tới iFCP gateway của thiết bị đích.

Trong quá trình đăng nhập, thiết bị kênh quang được ràng buộc với một kết nối TCP, nó sẽ sử dụng kết nối này trong suốt thời gian giao dịch. Khi phiên giao dịch kết thúc, kết nối TCP sẽ chuyển sang trạng thái không bị ràng buộc và sẵn sàng cho một quá trình đăng nhập mới. iFCP gateway lại khác, nó có thể có nhiều kết nối TCP tới nhiều iFCP khác và các các kết nối này có thể được áp dụng những chính sách chất lượng dịch vụ khác nhau.

2.1.5. Kiểm soát lỗi của iFCP

iFCP có trách nhiệm phát hiện lỗi trên cả kênh quang học và TCP. iFCP luôn phải theo dõi giá trị giới hạn thời gian xử lý (*timeout*) của kênh quang như E_D_TOV và R_A_TOV cũng như các lỗi của TCP. Nếu một kết nối TCP hoặc một thiết bị kênh quang phát sinh lỗi không thể khắc phục được, cổng mạng iFCP sẽ ngắt kết nối TCP đó và hủy bỏ các khung dữ liệu chưa được xử lý xong. Tiếp đó iFCP yêu cầu thiết bị cuối kênh quang bên nguồn thực hiện một phiên đăng nhập mới tới bên đích. Khi cổng mạng iFCP phát hiện ra lỗi nghiêm trọng như bộ định tuyến hoặc bộ chuyển mạch gắn với nó bị lỗi thì iFCP sẽ kết thúc toàn bộ các kết nối TCP và thiết lập lại kết nối tới mạng IP đích. Trong trường hợp có một trong

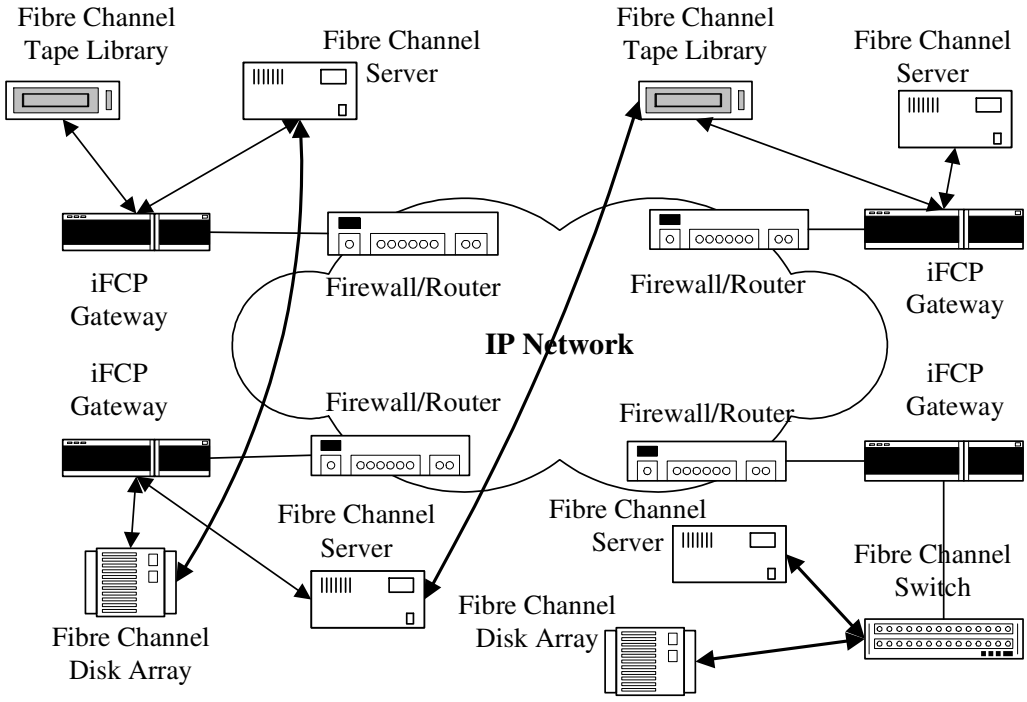
nhiều kết nối bị hỏng, iFCP chỉ xử lý kết nối hỏng đó và duy trì những kết nối còn lại.

2.1.6. An ninh iFCP

Bảo mật các giao dịch iFCP được thực hiện theo một số cách khác nhau. Hình thức đầu tiên là bảo mật giao dịch ngay từ mức vật lý. bản thân mạng quang kênh quang đã có sự bảo mật về mặt vật lý, iFCP gateway được sử dụng để thay thế các bộ chuyển mạch kênh quang. Ngoài ra, các iFCP gateway được kết nối với nhau thông qua mạng IP SAN tách biệt với mạng IP LAN thông thường nhằm đảm bảo tính bảo mật cho dữ liệu lưu trữ.

Ngay trong trung tâm lưu trữ, dữ liệu có thể bị chia tách thành nhiều vùng cho các ứng dụng hoặc đối tượng sử dụng khác nhau. Hệ thống cần bảo mật sao cho đối tượng không có quyền truy nhập các vùng sẽ không truy xuất được dữ liệu. Trong mạng quang, việc phân tách không gian lưu trữ dữ liệu được gọi là phân chia vùng. Trong iFCP, chức năng tương tự được thực hiện thông qua dịch vụ khám phá miền (*Discovery domains*), dịch vụ này cho phép bên nguồn (đã được cấp phép) có thể phát hiện và thiết lập phiên làm việc với thiết bị đích. Các giao dịch bên nguồn và bên đích được bảo mật nhờ sử dụng phương thức xác thực với khóa công khai hoặc khóa riêng. Máy chủ iSNS và iFCP gateway quản lý quá trình xác thực này.

iFCP tăng cường khả năng bảo mật trong mạng IP bằng cách sử dụng giao thức IPSec để xác thực và mã hóa dữ liệu nhằm hạn chế IP SAN bị tấn công. Khả năng bảo mật sẽ cao hơn nếu các thiết bị trong IP SAN (như bộ định tuyến hay bộ chuyển mạch) áp dụng chính sách bảo mật sử dụng danh sách điều khiển truy nhập (*Access Control List*). Khi đó để thiết lập được kết nối thì cả bên nguồn và bên đích đích đều phải có trong danh sách điều khiển truy cập. Hơn nữa, iFCP gateway có thể sử dụng thiết bị tường lửa lọc gói tin (*firewall*) đứng trước bảo vệ. Thiết bị *Firewall* ngăn chặn sự tấn công từ bên ngoài và cung cấp mạng riêng ảo cho việc lưu thông dữ liệu lưu trữ.



Hình 21 - Sử dụng Firewall để bảo mật trong môi trường iFCP

Hình 21 minh họa việc sử dụng các thiết bị *Firewall* nhằm bảo mật kết nối giữa các cổng mạng iFCP. Mạng SAN sử dụng iFCP có nhiều lựa chọn và linh hoạt hơn trong vấn đề bảo mật so với những mạng SAN chỉ sử dụng kênh quang.

2.1.7. Các vấn đề của iFCP

Trong giao thức chuẩn dành cho mạng SAN dựa trên giao thức IP, chỉ có giao thức iFCP được thiết kế để hỗ trợ cả thiết bị mạng quang và thiết bị trên nền IP (trong đó thiết bị trên nền IP phải sử dụng chồng giao thức iFCP). Các đặc tả của giao thức iFCP không hỗ trợ cho thiết bị iSCSI. Nhà cung cấp cần có những bổ sung thích hợp để thiết bị iSCSI, thiết bị kênh quang và thiết bị iFCP có thể kết nối làm việc cùng nhau và tạo nên một mạng IP SAN đa giao thức liên kết.

Đảm bảo hoạt động của các thiết bị kênh quang trên môi trường IP SAN đòi hỏi iFCP tìm cách thích ứng những dịch vụ mà mạng kênh quang truyền thống cung cấp. Chức năng Điều khiển tắc nghẽn trong trong kênh quang được iFCP thích ứng bằng các sử dụng cơ điều khiển luồng của giao thức TCP. FCP dựa vào WWNs để

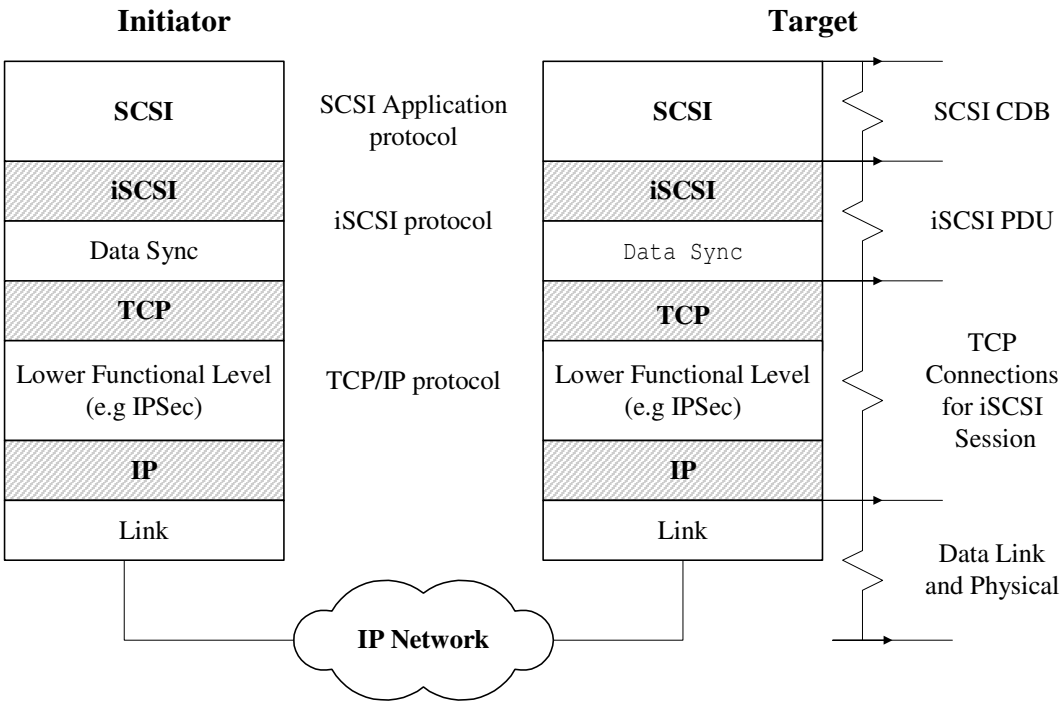
xác nhận duy nhất thiết bị và sử dụng địa chỉ 24 bit trong định tuyến. iFCP thích ứng bằng cách sử dụng ánh xạ địa chỉ IP (IP Mapping) và cơ chế chuyển đổi địa chỉ (Address translation). Tóm lại, iFCP luôn phải điều chỉnh để tương thích với các vấn đề phát sinh trong môi trường kênh quang nguyên thủy [1].

2.2. Giao thức iSCSI (Internet SCSI Protocol)

Giao thức iSCSI (*Internet SCSI Protocol*) cho phép những khối dữ liệu SCSI (lệnh hoặc dữ liệu) chuyển qua hệ thống mạng dựa trên nền tảng TCP/IP. Giao thức iSCSI được đánh giá như một công nghệ then chốt để phát triển thị trường SAN [1]. Do tính phổ biến của mạng nên iSCSI dễ dàng được chấp nhận và được ứng dụng rộng rãi.

2.2.1. Mô hình lớp của giao thức iSCSI

Mô hình lớp trong giao thức iSCSI được thể hiện thông qua hình 21:



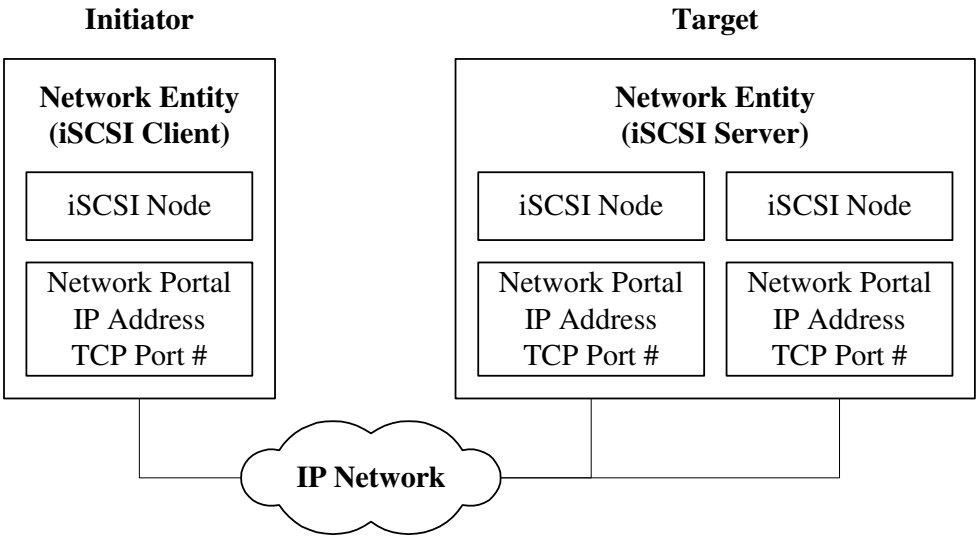
Hình 22 - Mô hình giao thức iSCSI

Đặc tả iSCSI bổ sung thêm vào giữa tầng giao vận TCP/IP một lớp chức năng nhằm cung cấp thêm một số dịch vụ như dịch vụ mã hóa dữ liệu IPSec. Lớp *Data*

Sync phục vụ cơ chế định hướng và đồng bộ dữ liệu. Lớp *Data Sync* đảm bảo đúng thứ tự lệnh, dữ liệu và làm phù hợp dữ liệu khi ghi trực tiếp vào vùng bộ nhớ của ứng dụng. Nếu không có lớp *Data Sync*, thiết bị iSCSI đòi hỏi lượng bộ nhớ đệm lớn hơn và phải thực hiện một số tác vụ sao chép để lưu trữ cũng như sắp xếp lại dữ liệu trước khi chuyển chúng lên lớp trên.

Việc thiết lập một phiên giao dịch iSCSI giữa *Initiator* và *Target* cần dùng một hoặc nhiều kết nối TCP để vận chuyển các lệnh, trạng thái và dữ liệu SCSI bên trong các các gói dữ liệu iSCSI (là đơn vị dữ liệu của giao thức - PDU). PDU chứa khối mô tả lệnh SCSI chuẩn theo cấu trúc thông điệp báo cho bên nhận biết đó là gói dữ liệu hay lệnh điều khiển.

2.2.2. Địa chỉ iSCSI và qui ước đặt tên



Hình 23 - Sử dụng tên và địa chỉ để liên kết giữa nguồn và đích

Giống như SCSI, iSCSI thực hiện theo mô hình *Client/Server* trong đó *Target* làm chức năng cung cấp dữ liệu theo yêu cầu của *Initiator*. iSCSI hoạt động trên toàn mạng nên cả *Target* và *Initiator* đều phải có định danh mạng, mỗi thực thể được gán một hoặc vài địa chỉ IP. Hình 23 minh họa việc sử dụng tên và địa chỉ để liên kết giữa bên nguồn và đích thông qua mạng IP.

Một nút iSCSI được định nghĩa như một thiết bị SCSI đặc biệt bên trong một thực thể mạng, có thể truy cập được thông qua *Network Portal*. Một thực thể mạng có nhiều nút iSCSI thể hiện đầu vào của nhiều *Intiator* và *Target*. Mỗi nút iSCSI được nhận diện thông qua một tên iSCSI duy nhất, có độ dài tối đa 255 ký tự và được thiết lập bởi người quản trị.

Việc tách biệt tên iSCSI và địa chỉ iSCSI đảm bảo: mỗi thiết bị lưu trữ chỉ có một định danh duy nhất trong mạng. Tên iSCSI được gán mềm và độc lập với thiết bị phần cứng. Địa chỉ iSCSI giúp ta phát hiện ra thiết bị ngay cả khi ta thay đổi vị trí của thiết bị trong mạng. Ví dụ khi người quản trị chuyển thiết bị sang một phân đoạn mạng khác, địa chỉ IP và số hiệu cổng TCP có thể bị thay đổi nhưng tên iSCSI vẫn được giữ nguyên. Vì lý do độ dài (cho phép tối đa 255 ký tự), tên iSCSI không được sử dụng cho mục đích định tuyến. Khi đó nút iSCSI sử dụng địa chỉ IP và số hiệu cổng TCP (người quản trị gán cho) để thực hiện giao dịch.

Tuy không bắt buộc (chỉ cần đảm bảo tính duy nhất), việc đặt tên iSCSI nên tuân theo những qui định chuẩn về đặt tên tài nguyên được mô tả trong RFC 1737. Giao thức iSCSI còn cho phép khai báo thêm tên bí danh (alias), mặc dù tên bí danh không thay thế được cho tên iSCSI. Tên bí danh cũng có độ dài tối đa là 255 ký tự và được trao đổi trong quá trình đăng nhập. Tên bí danh được sử dụng như công cụ để người quản trị phân biệt thiết bị lưu trữ một cách nhanh chóng.

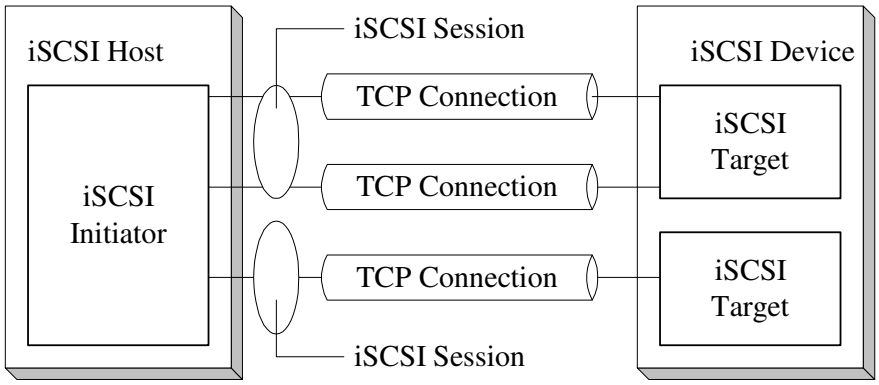
2.2.3 Quản lý phiên giao dịch iSCSI

Trước khi thực hiện một phiên giao dịch giữa bên nguồn và đích, hệ thống phải thực hiện một tiến trình đăng nhập còn được gọi là pha đăng nhập iSCSI. Quá trình này thực hiện việc trao đổi các tham số và trong một số trường hợp, nó bao gồm cả việc xác thực hai bên. Nếu thành công, bên đích phát đi thông báo chấp nhận việc đăng nhập cho bên nguồn. Ngược lại việc đăng nhập bị loại bỏ và kết nối cũng bị ngắt.

Tiến trình đăng nhập sử dụng các trường text để trao đổi những tham số biến

được phép. Những trường này bao gồm các từ khoá và giá trị của chúng. Ví dụ trường: số kết nối tối đa (MaxConnections) dùng để thiết lập số kết nối TCP tối đa cho một phiên giao dịch iSCSI. Nếu số kết nối tối đa được qui định ở bên nguồn và đích khác nhau thì giá trị được chọn là giá trị nhỏ nhất. Trường text cũng được sử dụng để trao đổi tên và tên bí danh cũng như các tham số khác như giao thức an ninh, giá trị timeout…

Trong thực tế, việc thiết lập phiên khá phức tạp vì một thiết bị iSCSI có thể có nhiều cổng mạng (gồm địa chỉ IP + số hiệu cổng TCP) và có thể đại diện cho nhiều iSCSI *Target* (ví dụ dãy các đĩa). Khi bên nguồn thiết lập phiên làm việc SCSI với bên đích, các số nhận diện phiên làm việc được sinh ra để xác định duy nhất từng giao tiếp giữa nút iSCSI cụ thể với những thực thể mạng tương ứng. Bên nguồn đăng nhập và gửi đi: tên iSCSI và số nhận diện phiên làm việc của nó cho bên đích (ISID). Bên đích tạo ra số nhận diện phiên duy nhất (TSID) đáp ứng yêu cầu đăng nhập của bên nguồn. Kết quả của quá trình "bắt tay" tạo ra một cặp giá trị ISID/TSID với nhiều kết nối TCP giữa chúng (trong đó cặp tên iSCSI/ISID đối với bên nguồn và bên đích là duy nhất trong thực thể mạng).

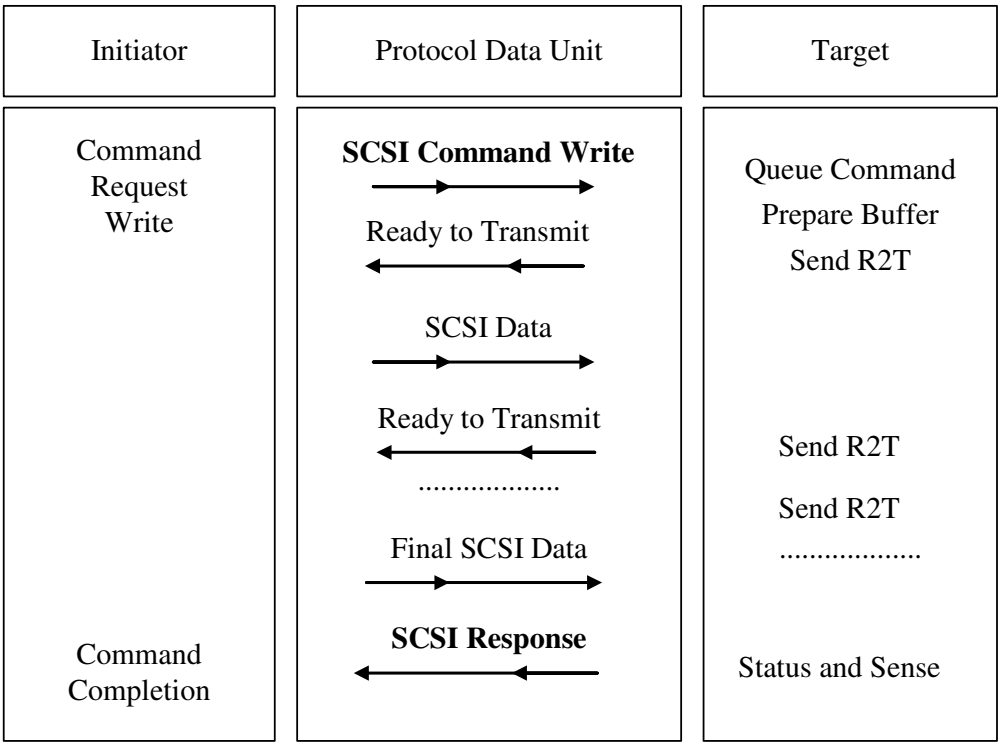


Hình 24 - Kết nối TCP trong các phiên giao dịch

Khi quá trình đăng nhập hoàn thành, phiên iSCSI cho phép thực hiện những giao dịch bình thường. Trường hợp phiên có nhiều kết nối thì từng cặp ra lệnh/đáp ứng đều phải thực hiện đúng qua kết nối tương ứng. Điều này đảm bảo các lệnh đọc và ghi dữ liệu được hoàn thành mà không phải kiểm tra từng kết nối. Một lệnh đọc

hoặc ghi dữ liệu được thực hiện thông qua một kết nối đơn cho đến khi tất cả dữ liệu được truyền xong. Một giao dịch khác có thể diễn ra đồng thời dựa trên những kết nối của chúng trong cùng một phiên giao dịch.

Trong hình 25, R2T (iSCSI PDUs báo trạng thái sẵn sàng nhận) được sử dụng để gửi lệnh, trạng thái, dữ liệu và thực hiện vai trò điều khiển luồng SCSI giữa nguồn và đích. Đối với thao tác ghi, R2T được hiểu là trạng thái thông báo bộ đệm của thiết bị đích đã sẵn sàng tiếp nhận thêm dữ liệu. Khi quá trình ghi hoàn thành, bên đích sẽ gửi thông báo trạng thái R2T xác nhận giao dịch đã thành công.



Hình 25 - Ví dụ về quá trình ghi trong một phiên giao dịch

Dữ liệu vận chuyển trong quá trình đọc hoặc ghi được theo dõi thông qua trạng thái, số tuần tự của gói dữ liệu và cặp thông số: con trỏ của bộ nhớ đệm và trường độ dài dữ liệu truyền trong gói số liệu iSCSI. Bên đích điều khiển tốc độ nhận dữ liệu bằng cách điều chỉnh giá trị độ dài dữ liệu truyền. Bên đích có thể yêu cầu truyền các khối dữ liệu theo một thứ tự nhất định bằng cách thiết lập địa chỉ con trỏ bộ nhớ đệm khi bắt đầu giao dịch.

Khi bên nguồn không nhận được hồi đáp yêu cầu từ bên đích, nó sẽ gửi một thông báo giống như lệnh *ping* (lệnh kiểm tra kết nối), kèm theo dữ liệu để kiểm tra trạng thái bên đích. Nếu bên đích không hồi đáp hoặc hồi đáp với dữ liệu lỗi thì bên nguồn sẽ ngắt kết nối và thiết lập lại một kết nối mới.

Phiên iSCSI và kết nối của chúng được giữ nguyên ở trạng thái mở và chờ lệnh SCSI từ tầng ứng dụng bên trên gửi xuống. Bên nguồn thường gắn kết tài nguyên đĩa trong mạng lưu trữ và hiếm khi ngắt các kết nối trừ khi phải thực hiện quá trình khởi động lại. Trong môi trường iSCSI, bên nguồn có thể yêu cầu nhiều kết nối TCP cho một giao dịch. Do đó, nếu một vài kết nối trong phiên làm việc bị ngắt thì cũng không làm gián đoạn phiên làm việc đó. Điều này rất hữu ích trong một số trường hợp, ví dụ như trường hợp cần ngắt kết nối để bảo trì mạng, thiết bị. Lệnh thoát khỏi phiên làm việc iSCSI (*logout*) được sử dụng để kết thúc phiên hoặc ngắt các kết nối trong một phiên bằng (nếu có tham số: số nhận diện kết nối) . Trường hợp lỗi kết nối, lệnh *logout* đưa ra một kết nối thay thế hoặc thiết lập một kết nối mới.

2.2.4. Kiểm soát lỗi iSCSI

Kiến trúc SCSI được thiết kế với giả thuyết môi trường không lỗi, Thiết bị SCSI được gắn vào kênh dành riêng song song, không xảy ra hiện tượng gián đoạn kênh. iSCSI được triển khai trên mạng IP tốc độ cao, kiến trúc truyền thông không tin cậy. Nhưng tầng TCP lại cung cấp tính tin cậy cần thiết cho iSCSI. iSCSI cung cấp thêm các cơ chế kiểm tra kết nối TCP và phát hiện lỗi trong các gói số liệu (tại tầng này). iSCSI sử dụng tham số *timeout* và thiết lập phạm vi tìm lại dữ liệu. Khi gói số liệu trong một dãy gói tin liên tiếp nhau bị lỗi, thì bên đích phải phát lại các gói số liệu đó. Trong mạng Gigabit, việc phát lại cả dãy gói số liệu không gây ảnh hưởng quá nhiều đến tốc độ hiệu dụng.

Phương pháp kiểm soát lỗi iSCSI yêu cầu cả bên nguồn và bên đích phải có khả năng lưu lệnh và những hồi đáp trong bộ đệm cho đến khi chúng được xác

nhận. Ví dụ với lệnh ghi SCSI, bên nguồn phải giữ lại trong bộ đệm dữ liệu đã chuyển đi cho đến khi bên nguồn nhận được thông báo R2T từ bên đích (R2T thông báo dữ liệu chuyển đi trước đó đã được nhận và bên đích đang sẵn sàng nhận dữ liệu mới). Tối thiểu thiết bị iSCSI phải có khả năng tạo dựng lại những gói dữ liệu bị mất hoặc bị hỏng trong quá trình truyền để thực hiện truyền lại.

Trong quá trình truyền, Lỗi có thể xuất hiện ở phần thông tin mào đầu (*iSCSI PDUs header*) hay ở phần dữ liệu (*content*) của đơn vị dữ liệu iSCSI (iSCSI PDUs). Lỗi xuất hiện có thể chia ra hai loại:

- Lỗi khuôn dạng (*format error*): lỗi này xảy ra khi một trường trong phần thông tin mào đầu bị mất hoặc các trường chứa đựng những thông tin trái ngược nhau.
- Lỗi nội dung (*Digest Content Error*): lỗi này xuất hiện khi nội dung của phần thông tin tiêu đề hoặc nôi dung dữ liệu mang theo (*payload*) trong PDUs bị hỏng.

Trong trường hợp lỗi định dạng, bên đích sẽ gửi hồi đáp có chứa con trỏ (offset indicator) trỏ tới byte đầu tiên bị lỗi trong phần thông tin mào đầu. Ngược lại, bên đích sẽ loại bỏ gói tin lỗi và yêu cầu gửi lại bằng cách sửa đổi giá trị trường offset trong R2T PDU.

iSCSI phát hiện sự thất lạc dữ liệu bằng cách theo dõi số tuần tự của gói tin (SNACK - Sequence Number Acknowledgment). Trong giao dịch, một hoặc một vài PDUs trong một dãy PDUs có thể bị thất lạc. Chỉ những PDUs bị thất lạc này mới được truyền lại theo lệnh SNACK của bên đích sẽ đảm bảo hiệu quả kênh truyền.

Phát hiện và khắc phục lỗi iSCSI có thể xảy ra ở nhiều cấp độ. Nó có thể thực hiện tại tầng SCSI mà cũng có thể là tầng bên dưới, tầng TCP. Kết nối TCP được sử dụng để chuyển tải dữ liệu có thể bị lỗi và trong trường hợp này iSCSI sẽ cố khắc phục thông qua lệnh khởi tạo lại. Một phiên giao dịch iSCSI lại có thể gồm nhiều kết nối TCP nên có thể không phải chỉ một kết nối phải khởi tạo lại. Trong trường

hợp xấu nhất, khi phiên giao dịch bị lỗi không thể khắc phục được, nó sẽ đóng tất cả các kết nối TCP, tạm ngừng tất cả các công việc, các lệnh trong hàng đợi và thực hiện tạo lại giao dịch mới thông qua quá trình đăng nhập.

2.2.5 An ninh iSCSI

Do iSCSI được thiết kế để có thể triển khai trên mạng diện rộng như Internet nên các giải pháp về an ninh cho iSCSI là hết sức quan trọng. Các giải pháp về an ninh cho iSCSI SAN bao gồm [1]:

* *Discovery Domains (DDSs)*: phương pháp này dựa một phần vào dịch vụ iSNS. iSNS cung cấp những tiện nghi để đăng ký, phát hiện, quản lý thiết bị lưu trữ (IP Storage) và quản lý những thay đổi về trạng thái. DDSs tạo ra miền và cho phép những thiết bị (được xác nhận bởi iSNS) trong cùng một miền có thể thiết lập được phiên giao dịch. DDSs được sử dụng trong IP SAN tương đương với dịch vụ Zoning của kênh FC SAN.

* *LUN Masking*: phương pháp này dựa trên việc ẩn giấu các LUNs. Bình thường khi bên nguồn thiết lập một phiên làm việc với bên đích, bên nguồn sẽ gửi đến bên đích lệnh truy vấn về số hiệu LUNs của những đĩa nó định đọc hoặc ghi số liệu. Bên đích sẽ đáp lại bằng cách gửi danh sách số hiệu các LUNs mà nó có bằng lệnh "Report LUNs" cho bên nguồn. Như vậy giới hạn danh sách các LUNs của bên đích trả về cho bên nguồn cũng là một phương thức an ninh. Tính năng "LUN Masking" không bắt buộc phải có trong các thiết bị lưu trữ iSCSI. Nó chỉ là một lựa chọn trong các phương thức an ninh của IP SAN.

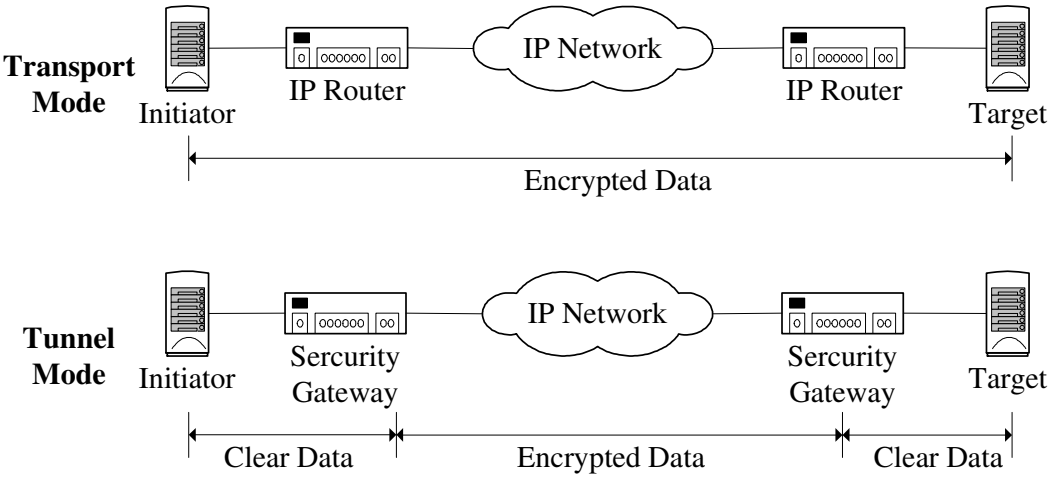
* *Danh sách điều khiển quyền truy cập (Access Control Lists -ACL)*: Những thiết bị mạng như bộ định tuyến hay bộ chuyển mạch có thể cung cấp chính sách bảo mật đơn giản thông qua ACLs. ACL đơn giản được hiểu như một bảng có chứa danh sách địa chỉ nào (với tầng 2 là địa chỉ MAC và tầng 3 là địa chỉ IP) thì được quyền truy cập, địa chỉ nào thì không. ACL cũng có thể sử

dụng loại dịch vụ vận chuyển (TCP hay UDP) hay số hiệu cổng TCP để giới hạn quyền truy cập.

* *Mạng ảo (VLAN):* VLAN có thể được áp dụng để phân tách và thiết lập quyền ưu tiên cho các luồng dữ liệu luân chuyển qua thiết bị mạng. Ứng dụng vào IP SAN, VLAN là một giải pháp để bảo mật cũng như để phân vùng (zoning).

* *IPSec*: IPSec gồm hai cơ chế chính: mào đầu xác thực (AH) và đóng gói an toàn dữ liệu (ESP). IPSec cung cấp các dịch vụ mã hoá, xác thực cho dữ liệu truyền tải trên mạng IP.

IPSec cung cấp hai chế độ kết nối là chế độ vận tải (Transport Mode) và chế độ đường hầm (Tunnel Mode). Chế độ vận tải bắt buộc áp dụng cơ chế an ninh ở tất cả các điểm thuộc kết nối còn chế độ đường hầm chỉ yêu cầu cơ chế an ninh từ điểm đầu đến điểm cuối của đường hầm.



Hình 26 - Hai chế độ kết nối của IPSec

IPSec có thể được áp dụng hết sức linh hoạt trong IP SAN, Nó có thể được áp dụng trên toàn mạng SAN hay chỉ trên những đoạn mạng có khả năng rủi ro cao. Nếu sử dụng IPSec thì SAN bị giảm hiệu năng do phải vận chuyển thêm thông tin của khóa khi trao đổi dữ liệu và làm tăng thời gian trễ khi xác nhận, mã hóa hoặc giải mã. Để khắc phục điều này, các thiết bị mạng và thiết bị lưu

trữ cần tích hợp sẵn IPSec.

Việc thoả thuận kiểu bảo mật giữa hai thiết bị iSCSI được thực hiện trong quá trình đăng nhập. Nếu thành công, các gói dữ liệu trao đổi giữa các thiết bị iSCSI sẽ được định dạng cho phù hợp với những yêu cầu của tiến trình an ninh. Tiến trình này có thể được thực hiện với sự trợ giúp của máy chủ iSNS.

2.3. So sánh FCP SAN và IP SAN

Các giao thức nền tảng được sử dụng trong SAN bao gồm: FCP (Fibre Channel Protocol), FCIP (Fibre Channel over IP), iFCP (Internet Fibre Channel Protocol), iSCSI (Internet SCSI)..vv. Mỗi giao thức đều có những điểm thuận lợi và những hạn chế riêng. Trong luận văn này, chúng tôi chỉ xem xét, đánh giá hai giao thức được sử dụng phổ biến nhất trong thực tế là FCP và iSCSI.

Khái niệm SAN thường gắn với mạng quang, dành riêng phục vụ kết nối giữa các thiết bị lưu trữ hoặc giữa thiết bị lưu trữ và máy chủ. Giao thức dùng để vận chuyển các khối dữ liệu cũng là giao thức kênh quang (Fibre Channel). Trong thời gian gần đây, iSCSI được coi là giao thức đầy tiềm năng trong việc phát triển thị trường SAN. Những ưu điểm và nhược điểm của giao thức iSCSI dựa trên cơ sở giao thức vận tải dữ liệu mà nó sử dụng (TCP/IP). Chính vì vậy, ta có thể coi việc so sánh giữa hai giao thức của SAN là FCP và iSCSI chính là so sánh giữa hai giao thức vận tải dữ liệu kênh quang (FC) và TCP/IP.

So sánh các chỉ tiêu:

***Khoảng cách kết nối*:**

FCP cho phép thực hiện các kết nối có khoảng cách xa lên tới 10 km. Tuy vậy, việc triển khai những kết nối như vậy là không thực tiễn đối với các doanh nghiệp. Trong thực tế, những mạng SAN có sử dụng kết nối kênh quang cho trung tâm dữ liệu ở trong một hay nhiều tòa nhà gần nhau.

iSCSI không chỉ cung cấp giải pháp xây dựng SAN cho những trung tâm dữ liệu tập trung, nó còn thực hiện tốt việc kết nối giữa những khoảng cách cực

lớn nhờ mạng internet toàn cầu. Sự phát triển hệ thống mạng internet băng thông rộng sẽ là một thuận lợi cho việc phát triển thị trường iSCSI [5].

***Khả năng tương tác*:**

Các nhà phát triển thiết bị lưu trữ kênh quang vẫn phát triển và cải tiến sản phẩm phần cứng và phần mềm một cách riêng rẽ. Điều này dẫn đến khả năng tương thích không cao của các thiết bị. Để giảm bớt những lỗi phát sinh, người sử dụng thường phải giảm thiểu việc sử dụng các tính năng mới của các thiết bị kênh quang. iSCSI sử dụng nền giao thức TCP/IP là chuẩn thống nhất nên không phát sinh những lỗi liên tác giữa các thiết bị.

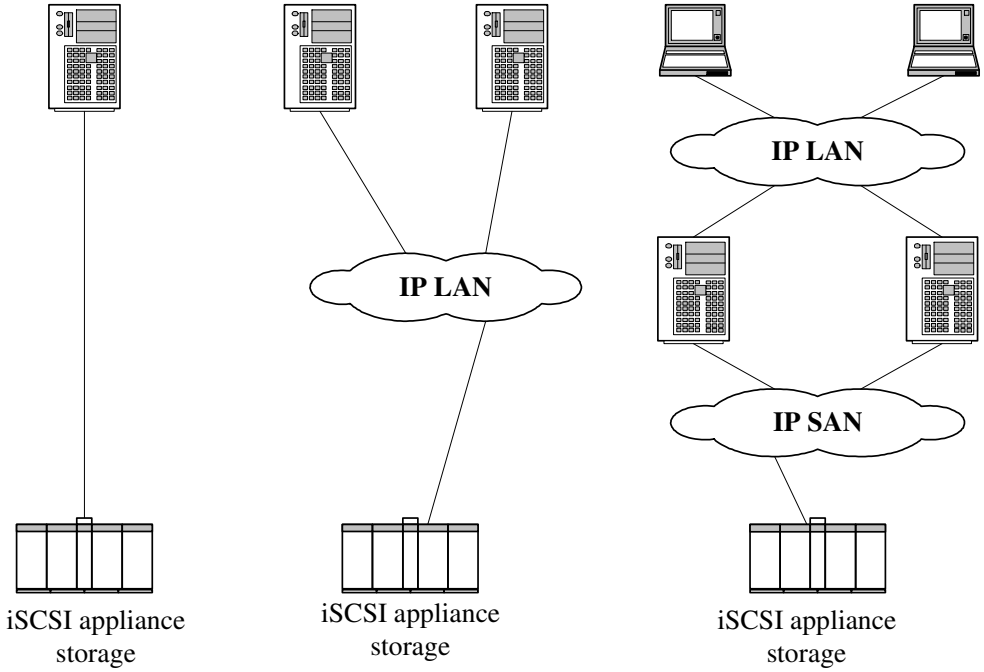
***Chi phí*:**

Trong thực tế cho thấy chi phí cho SAN dựa trên iSCSI thường thấp hơn. Các yếu tố làm giảm chi phí cho iSCSI SAN bao gồm:

- Giá các thiết bị thành phần SAN dựa trên giao thức iSCSI thấp hơn do tính phổ dụng, số lượng nhà cung cấp và qui mô sản xuất của các thiết bị xây lên SAN như bộ điều hợp, bộ chuyển mạch, bộ dẫn đường,..vv.
- Thời gian đào tạo, chi phí đào tạo và duy trì iSCSI SAN thấp hơn nhiều so với FCP SAN. TCP/IP gần như là kỹ năng cơ bản của các kỹ thuật viên công nghệ thông tin và việc đào tạo cũng như duy trì hệ thống SAN không đòi hỏi các chuyên gia thuộc các lĩnh vực công nghệ thông tin khác nhau [2].

***Kết nối*:**

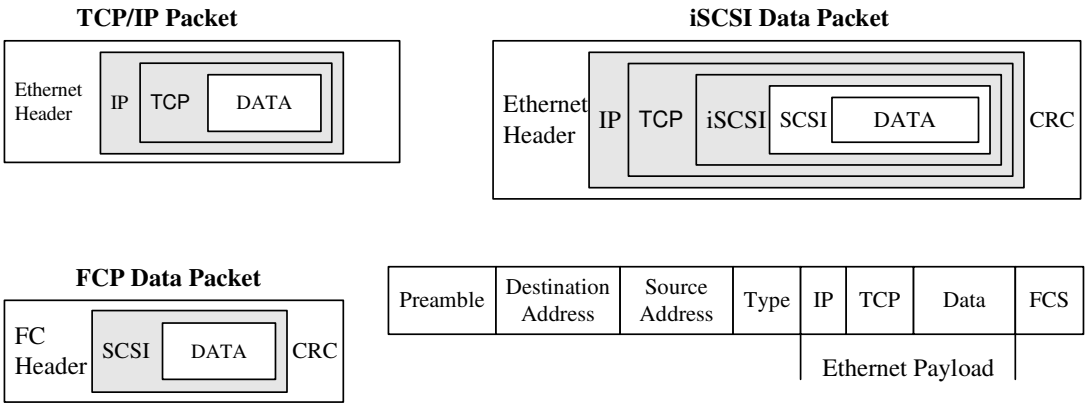
Với iSCSI, kết nối của thiết bị lưu trữ với máy chủ rất đa dạng thông qua IP SAN, qua IP LAN hay thậm chí nối thẳng vào máy chủ và được sử dụng như là một thiết bị lưu trữ gắn thẳng (DAS - Direct Attacked Storage) [5]:



Hình 27 - Các dạng kết nối iSCSI

Hiệu năng, thông lượng truyền tải:

TCP/IP không phải là một giao thức đạt hiệu quả cao trong việc tận dụng băng thông. Lý do là nó phải thực hiện đóng/giải gói tiêu đề (pack/unpack header) ở cả hai tầng TCP và IP. Hơn nữa cơ chế để kiểm soát lỗi, điều khiển lưu lượng, điều khiển tắc nghẽn của TCP phức tạp làm tăng thời gian trễ xử lý [5].



Hình 28 - So sánh FCP SAN và iSCSI SAN

Hiệu năng giữa FCP và iSCSI sẽ càng khác biệt nếu iSCSI sử dụng kết nối

theo chuẩn Ethernet. Kích cỡ đầu gói số liệu (over head) của FCP chỉ là 36 byte trong khi kích cỡ gói số liệu tiêu đề theo tiêu chuẩn Ethernet là 66 byte (một byte bắt đầu và một byte báo hiệu kết thúc gói số liệu). Các số liệu sau thể hiện rõ hơn sự khác biệt trong việc chuyển tải 256 MB dữ liệu [2]:

* FCP:

$$256MB * \frac{1}{2112B} * \frac{36B}{1} = 4.36\ MB$$

Trong đó:

- 2112B là kích cỡ dữ liệu tối đa có thể mang trong gói số liệu FCP.
- 4.36 MB là tổng kích cỡ tiêu đề.

* Ethernet:

$$256MB * \frac{1}{1460B} * \frac{66B}{1} = 11.57\ MB$$

$$256MB * \frac{1}{454B} * \frac{66B}{1} = 37.22\ MB$$

Trong đó:

- 1460B là kích cỡ dữ liệu tối đa có thể mang trong gói số liệu Ethernet.
- 454B là kích cỡ dữ liệu tối thiểu có thể mang trong gói số liệu Ethernet.
- 11.57 MB và 37.22 là tổng kích cỡ tiêu đề tương ứng với từng trường hợp.

Sử dụng những công nghệ hỗ trợ như TOEs hay iSCSI Accerleter sẽ khắc phục được nhược điểm của iSCSI (thông lượng truyền tải). Do đó iSCSI SAN là giải pháp khá hoàn thiện. Bảo việt sẽ sử dụng giải pháp iSCSI SAN làm giải pháp lưu trữ trong hệ thống thông tin của mình.

CHƯƠNG 3: ỨNG DỤNG SAN GIẢI QUYẾT BÀI TOÁN THỰC TIỄN

3.1 Giới thiệu bài toán

Bảo việt bắt đầu hoạt động kinh doanh bảo hiểm từ 15/01/1965, có phạm vi hoạt động trên tất cả các tỉnh, thành phố trong cả nước và là một trong 25 doanh nghiệp nhà nước lớn nhất của Việt Nam. Kể từ ngày 30/06/2004, Bảo việt sẽ được tổ chức theo mô hình tập đoàn tài chính bảo hiểm với hai tổng công ty trực thuộc hạch toán độc lập kinh doanh ở hai mảng nghiệp vụ nhân thọ và phi nhân thọ.

Với mục tiêu "trở thành tập đoàn tài chính hàng đầu Việt Nam" trong lĩnh vực bảo hiểm nhân thọ, bảo hiểm phi nhân thọ, đầu tư tài chính và đầu tư chứng khoán, Bảo việt phải luôn thực hiện việc nâng cao trình độ quản lý, chất lượng phục vụ khách hàng trong bất kỳ lĩnh vực kinh doanh nào của tập đoàn, từ việc nghiên cứu phát triển các sản phẩm, dịch vụ tới việc tư vấn cho khách hàng các giải pháp tối ưu hoặc xây dựng các mối quan hệ hợp tác chắt chẽ, cùng phát triển với khách hàng và các đối tác. Việc ứng dụng công nghệ thông tin vào trong các hoạt động giao dịch trở thành một yếu tố quan trọng giúp mục tiêu đề ra sớm trở thành hiện thực.

Năm 1995, Bảo Việt xây dựng hệ thống hạ tầng công nghệ thông tin và các ứng dụng cho hầu hết nghiệp vụ kinh doanh trong Bảo Việt. Hệ thống thông tin Bảo Việt hiện được tổ chức theo mô hình phân tán và phân cấp. Tại mỗi đơn vị thành viên ở các tỉnh thành, Bảo Việt đã xây dựng cơ sở hạ tầng thông tin và triển khai những ứng dụng quản lý nghiệp vụ thống nhất trong toàn ngành.

Không gian lưu trữ hiện là một trong những vấn đề được quan tâm trong định hướng xây dựng và phát triển cơ sở hạ tầng thông tin. Những con số thống kê: hơn 30 triệu lượt khách hàng mỗi năm, hơn 2 vạn cán bộ nhân viên các đại lý cần quản lý và hơn 6 ngàn tỷ đồng doanh thu cần được tập hợp, quản lý và phân bổ trong năm phần nào nói lên lượng dữ liệu phát sinh trong hoạt động của doanh nghiệp. Vấn đề

không gian lưu trữ càng trở lên thiết yếu khi Bảo Việt có định hướng xây dựng những ứng dụng trực tuyến, xây dựng kho dữ liệu *(Dataware house)*, hay triển khai những dịch vụ tích hợp như thư thoại hay *Call center*.

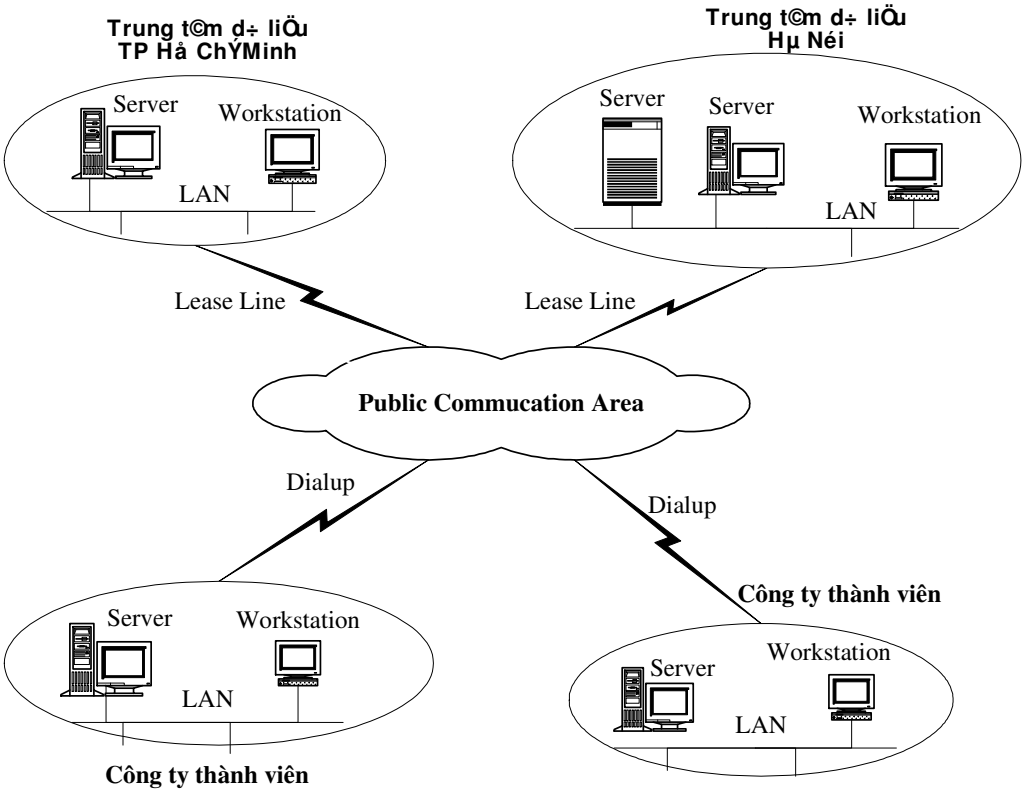
3.2. Hiện trạng hệ thống thông tin

3.2.1. Các thành phần và kiến trúc kết nối của hệ thống thông tin Bảo việt

Tổ chức thông tin của hệ thống thông tin Bảo việt bao gồm:

- Trung tâm dữ liệu đặt tại Hà nội.
- Trung tâm dữ liệu đặt tại thành phố Hồ Chí Minh
- Hệ thống thông tin của các đơn vị thành viên
- Hệ thống thông tin tại các văn phòng đại diện trực thuộc đơn vị thành viên.

Kiến trúc kết nối Bảo việt:



Hình 29: Sơ đồ tổ chức mạng truyền thông Bảo Việt.

Trong đó:

- Hai trung tâm dữ liệu được trang bị kết nối thuê bao riêng (lease line). Chúng thực hiện cập nhật số liệu trực tuyến với nhau thông qua đường truyền thông này.
- Các đơn vị trao đổi số liệu cũng như lấy nâng cấp chương trình thông qua đường kết nối quay số (dialup). Trong tương lai gần có thể các kết nối này sẽ được nâng cấp lên lease line và sử dụng VPN để trao đổi số liệu với các trung tâm dữ liệu thông qua mạng Internet.

3.2.2. Hệ thống thông tin thành phần

3.2.2.1. Hệ thống thông tin của trung tâm dữ liệu đặt tại Hà nội

Đặt tại 94 bà triệu, Trung tâm thông tin là nơi tập trung, xử lý, đồng bộ dữ liệu nghiệp vụ của toàn Bảo việt.

Máy chủ: Trung tâm được trang bị các máy chủ chạy trên các nền tảng phần cứng và phần mềm khác nhau. Các máy chủ cung cấp các loại hình dịch vụ khác nhau như: cơ sở dữ liệu trên nền tảng Oracle, dịch vụ web dựa trên Oracle Portal, Dịch vụ FTP, dịch vụ làm việc nhóm như mail, dịch vụ fax, quản lý công văn ..

Thiết bị	CPU/ Hệ Điều hành	Dung lượng Lưu trữ	Dịch vụ / Ứng dụng
HP Proliant 530	Intel/Windows 2000	120 GB	Quản lý công văn, Lotus Notes
HP Proliant 530	Intel/Windows 2000	120 GB	Kế toán, Tổ chức cán bộ.
HP LH6000	Intel/Windows 2000	60 GB	Bảo hiểm phương tiện, bảo hiểm con người - học sinh, bảo hiểm cháy - xây lắp, bảo hiểm tàu - hàng hóa.
HP 9000	HP/ Unix	160	Bảo hiểm nhân thọ
HP 9000	HP/ Unix	160	Bảo hiểm nhân thọ

HP Proliant 530	Intel/Windows 2000	120 GB	Lưu số liệu nghiệp vụ kế toán của các công ty thành viên truyền về.
HP Proliant 530	Intel/Windows 2000	120 GB	Lưu số liệu nghiệp vụ bảo hiểm nhân thọ của các công ty thành viên truyền về.
HP Proliant 530	Intel/Windows 2000	120 GB	Lưu số liệu nghiệp vụ bảo hiểm phi nhân thọ của các công ty thành viên truyền về.

Thiết bị mạng: Các thiết bị mạng được trang bị cho trung tâm đều hoạt động dựa trên nền tảng IP.

Thiết bị	Mục đích sử dụng
Cisco 3600 – RAS	Cung cấp kết nối từ xa cho các đơn vị thành viên, số kết nối hiện đang sử dụng là 16 đường.
Cisco 6500 – Switch	Cung cấp kết nối trong toàn bộ trung tâm bằng cách gắn kết giữa các bộ chuyển mạch kênh quang và các chuyển mạch Ethernet khác. Nói cách khác nó cung cấp trục xương sống cho các phân đoạn mạng con.
Cisco Pix 525 - Firewall	Đảm nhận việc cung cấp kết nối với mạng Internet và bảo vệ mạng LAN khỏi sự thâm nhập từ bên ngoài.
Cisco 7800	Hoạt động như một tổng đài, cung cấp dịch vụ thoại trên nền tảng IP.
Cisco Switch 3550	Được trang bị cho các tầng, cung cấp kết nối 100 Mb cho các máy trạm với nhau và 1Gb với đường trục.

3.2.2.2. Hệ thống thông tin tại các đơn vị thành viên

Do số lượng ứng dụng triển khai tại các đơn vị thành viên thành viên ít hơn nên thiết bị trang bị cho đơn vị có cấu hình thấp. Các ứng dụng chính bao gồm: cơ

sở dữ liệu trên nền Oracle, dịch vụ làm việc nhóm như thư và quản lý công văn trên nền Lotus Notes. Dữ liệu các giao dịch phát sinh trong địa bàn được tích lũy tại đây và sẽ được truyền về trung tâm dữ liệu hàng tháng.

Máy chủ: Do làm việc với lượng dữ liệu nhỏ hơn nên các đơn vị thành viên được trang bị các máy chủ có công suất nhỏ và dung lượng lưu trữ ít hơn.

Thiết bị	CPU/ Hệ điều hành	Dung lượng Lưu trữ	Dịch vụ/ Ứng dụng
HP Proliant 370	Intel Xeon 2GHz /Windows 2000	60 GB	Lotus Notes và các nghiệp vụ được xây dựng trên nền tảng File Server
HP A500	HP/Unix	40 GB	Bvlife (cơ sở dữ liệu Oracle)

Thiết bị Mạng: Các đơn vị thành viên được trang bị những thiết bị sau:

Thiết bị	Mục đích sử dụng
Cisco 3600 – RAS	Cung cấp kết nối từ xa cho các văn phòng đại diện đặt tại các huyện.
HP Switch	Cung cấp đường kết nối 10/100 Mb cho các máy trạm trong văn phòng công ty.
Modem 33.6 Kb	Là phương tiện kết nối giữa văn phòng đại diện với đơn vị và đơn vị với trung tâm thông tin.

Hệ thống thông tin tại các văn phòng đại diện trực thuộc đơn vị thành viên: bao gồm hệ thống kết nối mạng ngang hàng sử dụng giao thức TCP/IP. Ở cấp độ này, hệ thống thông tin không được trang bị máy chủ và các ứng dụng tại đây đều dựa trên nền tảng chia sẻ tập tin. Dữ liệu các giao dịch trong ngày sẽ được truyền và trao đổi thông qua kết nối dial-up với đơn vị thành viên trực tiếp quản lý.

3.2.3. Các ứng dụng hiện đang sử dụng tại Bảo việt:

Chiếm đa số là các ứng dụng cơ sở dữ liệu lớn, mỗi ứng dụng có thể phục vụ công tác quản lý cho từng nhóm nghiệp vụ bảo hiểm. Các ứng dụng đều có giao diện tiếng việt và đều sử dụng font TCVN3. Trong thời gian tới, khi các dữ liệu chuyển sang định dạng unicode thì lượng không gian lưu trữ đòi hỏi sẽ phải tăng đáng kể.

Những ứng dụng chính có số lượng số liệu lớn hiện đang được sử dụng tại Bảo Việt bao gồm:

- **BVLife - Bảo hiểm nhân thọ: (phần mềm nền: Oracle)**

  Nhiệm vụ:

  - Quản lý giấy yêu cầu bảo hiểm cho tất cả các nghiệp vụ.
  - Quản lý cấp phát hợp đồng bảo hiểm.
  - Quản lý cập nhật, thay đổi cho các hợp hợp đồng bảo hiểm.
  - Lập kế hoạch và in hóa đơn thu phí (hóa đơn in sẵn - quản lý mã vạch).
  - Lập và quản lý quỹ dự phòng.
  - Lập chương trình chăm sóc khách hàng.
  - Quản lý lãi chia hợp đồng bảo hiểm.
  - Quản lý hợp đồng đáo hạn.

  Lượng số liệu: số liệu qui chuẩn là khoảng 140 GB nhưng không gian chiếm thực tế là gần 500 GB. Lượng dữ liệu phát sinh do:

  - Quản lý gần 3 triệu hợp đồng.
  - Quản lý gần 20 triệu giao dịch trong một năm.
  - Quản lý hoa hồng cho hơn 2 vạn đại lý.
  - Quản lý lãi chia hàng năm cho hơn một triệu khách hàng.
  - Số liệu được lũy kế từ năm này sang năm khác (hợp đồng có thể kéo dai tối đa là 17 năm).

- **Kế toán: (phần mềm nền: Foxpro)**

  Nhiệm vụ:

- Quản lý hoạt động thu chi hội sở.
- Quản lý hoạt động thu chi nghiệp vụ.
- Quản lý lương thưởng các cán bộ trong doanh nghiệp.
- Quản lý chi hoa hồng đại lý.
- Quản lý tài sản doanh nghiệp.
- Quản lý kế hoạch chi tiêu trong doanh nghiệp.
- Lập báo cáo tài chính doanh nghiệp.
- Lập báo cáo tài chính riêng báo các bộ Tài chính.

Lượng số liệu: số liệu qui chuẩn chiếm khoảng 12 GB hàng năm phát sinh chủ yếu do:

- Quản lý khoảng 60 triệu giao dịch trong một năm.

- **Tổ chức cán bộ: (phần mềm nền: Foxpro)**

  Nhiệm vụ:

  - Quản lý nhân sự của doanh nghiệp.
  - Quản lý đại lý bảo hiểm.
  - Quản lý chi nhánh và văn phòng đại diện.
  - Quản lý cơ cấu phòng ban trong các đơn vị thành viên.

  Lượng số liệu: số liệu qui chuẩn chiếm khoảng 100 MB phát sinh do:

  - Quản lý hồ sơ của hơn hai vạn cán bộ và đại lý.
  - Gần hai nghìn chi nhánh trong cả nước.

- **DocMan - Quản lý công văn: (phần mềm nền: Lotus Notes)**

  Nhiệm vụ:

  - Quản lý công văn đến, đi của doanh nghiệp.
  - Quản lý các văn bản ISO của doanh nghiệp.
  - Quản lý thông tin thị trường.
  - Quản lý nhiệm vụ của cán bộ trong doanh nghiệp.
  - Quản lý tờ trình và trao đổi nghiệp vụ giữa các phòng ban.
  - Tích hợp với hệ thống thư điện tử intranet và internet của doanh nghiệp.

- Lập lịch làm việc của cá nhân.

Lượng số liệu: Chiếm gần 60 GB được sinh ra chủ yếu từ việc lưu trữ fax và thư điện tử từ năm 1999 đến nay.

- **Bảo hiểm phương tiện: (phần mềm nền: Foxpro)**

  Nhiệm vụ:

  - Quản lý nghiệp vụ bảo hiểm xe cơ giới bao gồm: quản lý cấp đơn, quản lý đơn, quản lý hoa hồng, quản lý hồ sơ bồi thường.
  - Quản lý ấn chỉ xe in sẵn.
  - Chăm sóc khách hàng, tái tụng hợp đồng bảo hiểm.
  - Báo cáo thống kê, xây dựng biểu phí bảo hiểm xe

  Lượng số liệu: hàng năm chiếm hơn 3 GB và được phát sinh ra để quản lý:

  - Hơn hai triệu xe cơ giới.
  - Gần hai triệu khách hàng.

- **Bảo hiểm con người, học sinh: (phần mềm nền: Foxpro)**

  Nhiệm vụ:

  - Quản lý nghiệp vụ bảo hiểm con người, học sinh bao gồm: quản lý cấp đơn, quản lý đơn, quản lý hoa hồng, quản lý hồ sơ bồi thường.
  - Quản lý ấn chỉ in sẵn.
  - Chăm sóc khách hàng, tái tụng hợp đồng bảo hiểm.
  - Báo cáo thống kê, xây dựng biểu phí bảo hiểm con người

  Lượng số liệu: hàng năm chiếm gần 5 GB và được phát sinh để quản lý:

  - Gần bốn triệu học sinh các cấp.

- **Bảo hiểm cháy, xây lắp: (phần mềm nền: Foxpro)**

  Nhiệm vụ:

  - Quản lý nghiệp vụ bảo hiểm cháy, xây lắp bao gồm: quản lý cấp đơn, quản lý đơn, quản lý hoa hồng, quản lý hồ sơ bồi thường.
  - Quản lý ấn chỉ in sẵn.
  - Chăm sóc khách hàng, tái tụng hợp đồng bảo hiểm.
  - Báo cáo thống kê.

Lượng số liệu: Chiếm hơn 1GB để phục vụ quản lý hơn 100 000 đối tượng bảo hiểm khác nhau

- **Bảo hiểm hàng hóa: (phần mềm nền: Foxpro)**

  Nhiệm vụ:

  - Quản lý nghiệp vụ bảo hiểm hàng hóa: quản lý cấp đơn, quản lý đơn, quản lý hoa hồng, quản lý hồ sơ bồi thường, tái bảo hiểm.
  - Quản lý ấn chỉ in sẵn.
  - Chăm sóc khách hàng, tái tụng hợp đồng bảo hiểm.
  - Báo cáo thống kê.

  Lượng số liệu: Chiếm hơn 2GB để phục vụ quản lý gần 300 000 lượt chuyên chở hàng hóa trong năm.

Với lượng dữ liệu lớn như vậy, Việc giải quyết bài toán lưu trữ là rất cần thiết. Nó là cở sở để duy trì hoạt động của các ứng dụng hiện tại và xây dựng những ứng dụng mới phục vụ hoạt động kinh doanh của Bảo việt.

3.2.4. Hệ thống lưu trữ

Dữ liệu nghiệp vụ của toàn Bảo việt đều tập trung về trung tâm dữ liệu. Do độ lớn của dữ liệu lớn nên việc lưu trữ phải phân tán ra nhiều máy chủ. Trung tâm dữ liệu bảo việt hiện tổ chức lưu trữ như sau:

Lưu trữ dữ liệu của các đơn vị thành viên:

- Sử dụng một máy chủ "HP Proliant 530" để lưu trữ số liệu do các công ty thành viên truyền về cho các nghiệp vụ sau: hàng hóa, bảo hiểm học sinh, bảo hiểm con người, bảo hiểm xe cơ giới, bảo hiểm cháy.
- Sử dụng một máy chủ "HP Proliant 530" để lưu trữ số liệu do các công ty thành viên truyền về cho nghiệp vụ kế toán.
- Sử dụng một máy chủ "HP Proliant 530" để lưu trữ số liệu do các công ty thành viên truyền về cho nghiệp vụ bảo hiểm nhân thọ.

Lưu trữ dữ liệu tác nghiệp:

- Máy chủ ứng dụng được sử dụng để lưu trữ dữ liệu cho nghiệp vụ tương

ứng.

Sao lưu bảo vệ số liệu:

- Các máy chủ ứng dụng sử dụng thiết bị sao lưu đi kèm để sao lưu số liệu nghiệp vụ tương ứng.
- Các máy chủ lưu trữ dữ liệu của các đơn vị thành viên cũng sử dung tape đi kèm để sao lưu số liệu.

Giải pháp lưu trữ trên đã và đang bộc lộ nhiều nhược điểm trong quá trình vận hành. Thời gian sắp tới, Bảo việt sẽ phải thay đổi giải pháp lưu trữ để đáp ứng nhu cầu lưu trữ dữ liệu phát sinh trong hoạt động kinh doanh.

3.3. Xây dựng giải pháp lưu trữ cho Bảo việt

3.3.1. Tiêu chí xây dựng giải pháp

Xây dựng hệ thống từ nhỏ đến lớn, thiết kế vừa đủ cho nhu cầu trong thời gian gần nhưng có thể mở rộng mà không làm gián đoạn hoạt động hệ thống.

Việc thiết kế, xây dựng hệ thống lưu trữ thông tin Bảo việt phải đảm bảo đáp ứng được các yêu cầu sau:

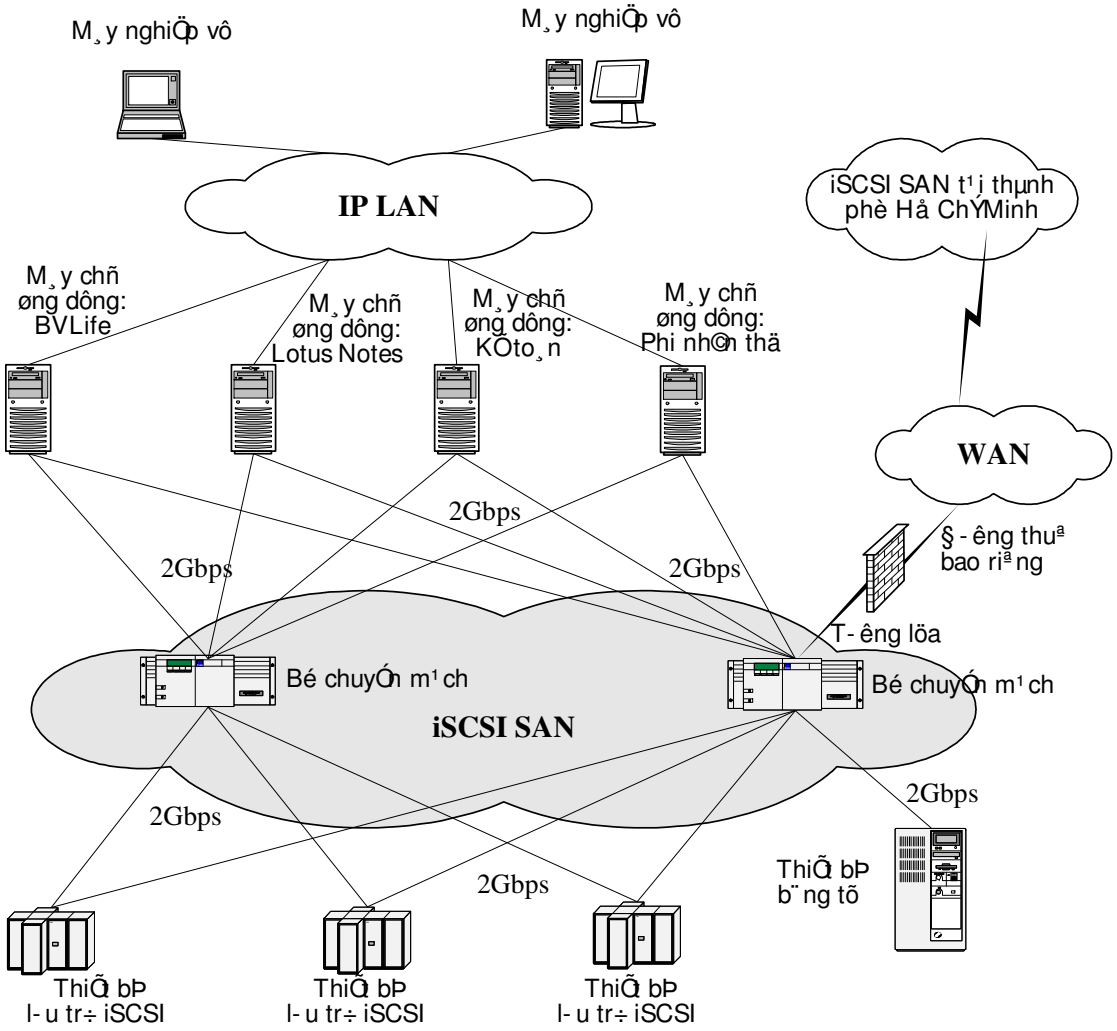
- Thiết kế các hệ lưu trữ phù hợp với điều kiện kinh tế, qui mô tổ chức, qui mô dữ liệu cho từng cấp độ khác nhau.
- Có khả năng mở rộng hệ thống khi có phát sinh nhu cầu.
- Có khả năng tận dụng những thiết bị có sẵn.
- Đáp ứng được các tiêu chí về tốc độ truy xuất dữ liệu, độ sẵn sàng cao, ổn định.
- An ninh dữ liệu phải được đảm bảo sao cho: các máy chủ úng dụng chỉ có thể truy xuất được vùng lưu trữ dữ liệu của nó.
- Vấn đề an toàn thông tin phải được tự động hóa (sao lưu và phục hồi dữ liệu).

3.3.2. Phương án cho trung tâm số liệu

3.3.2.1. Kiến trúc SAN

Dựa trên phương pháp xây dựng hệ thống SAN từ lớn đến nhỏ, từ đơn giản

đến phức tạp. Đồng thời phải cân bằng các yếu tố: độ sẵn sàng, tốc độ, số lượng thiết bị phải trang bị. Kiến trúc SAN của trung tâm thông tin Bảo việt được dự kiến như hình 30.



Hình 30 - Kiến trúc iSCSI SAN của Bảo việt

3.3.2.2. Lựa chọn thiết bị mạng

Hệ thống mạng Bảo việt được xây dựng chủ yếu từ những thiết bị của hãng Cisco cung cấp và được vận hành bởi một kỹ sư công nghệ thông tin. Việc sử dụng thiết bị của một hãng khác sẽ làm cho hệ thống mạng phải đối mặt với những vấn đề về tính tương thích, và kèm theo đó là phải đào tạo thêm cho người vận hành. Hiện

nay, Cisco là hãng cung cấp thiết bị mạng uy tín lớn nhất trên thế giới, do đó, việc tiếp tục sử dụng sản phẩm của Cisco là phù hợp.

Để phục vụ cho việc thiết lập mạng SAN, Cisco đã đưa ra sản phẩm "Cisco catalyst 6509 switch" với nhiều tính năng ưu việt. Sản phẩm này được thiết kế cho môi trường doanh nghiệp với nhiều tính năng mạnh và mới của công nghệ mạng LAN truyền thống. Những thông số kỹ thuật của thiết bị có lợi trong việc ứng dụng vào SAN bao gồm:

Băng thông:

Một điểm bất lợi của SAN dựa trên nền tảng TCP/IP là tỷ số "băng thông hữu ích" trên "băng thông cho phép" không cao nên việc tăng cường tối đa băng thông ở tầng mạng sẽ ngăn ngừa sự xuất hiện nút chai tại tầng TCP/IP trong SAN.

- Backplane: 32Gbps shared bus
- Port max speed: 10 Gbps

Khả năng mở rộng:

Các trung tâm dữ liệu thường trang bị một số lượng lớn thiết bị lưu trữ, máy chủ và mỗi thiết bị trên lại có thể thiết lập nhiều kết nối (multi path) đến nhau nhằm nâng cao băng thông hay tăng cường độ chịu lỗi của hệ thống. Số lượng cổng kết nối phản ánh khả năng mở rộng của SAN và là một yếu tố cần được cân nhắc để đảm bảo khả năng mở rộng theo nhu cầu nảy sinh trong hoạt động kinh doanh.

- 10/100/1000 Ethernet : 576 ports, all support Inline Power
- 10/100 Fast Ethernet : 1152 ports, all support Inline Power
- 100 Base FX : 288 ports
- Gigabit Ethernet : 194 ports (2 ports provided on supervisor engine)
- 10 Gigabit Ethernet : 32 ports

Hỗ trợ kết nối WAN:

Tính năng này là cần thiết cho việc trao đổi dữ liệu giữa hai trung tâm của Bảo Việt đặt tại Hà nội và thành phố Hồ Chí Minh thông qua kênh thuê bao riêng. Nó giúp cho việc cấu hình như một SAN từ xa (remote SAN) cho trung tâm dữ liệu tại thành phố Hồ Chí Minh được thuận lợi.

- OC-3 POS ports : 192
- OC-12 POS ports : 48
- OC-12 POS ports : 24
- OC-48 POS/DPT ports : 24
- Digital T1/E1 Trunk ports : 216
- FXS Interfaces : 864

Tích hợp bảo mật:

Việc tách rời SAN khỏi LAN cũng là một hình thức bảo mật không cho người dùng thực hiện biến đổi dữ liệu một các trái phép. Tuy nhiên trong nhiều trung tâm dữ liệu còn yêu cầu việc bảo mật phải chặt chẽ hơn. Ví dụ như nhưng trung tâm có nhiều người quản trị, mỗi quản trị viên lại quản trị một nhóm máy chủ ứng dụng riêng rẽ. Vì các máy chủ này đề được gắn vào IP SAN nên việc đòi hỏi phân vùng dữ liệu cho các máy chủ ứng dụng và đảm bảo cho phân vùng dữ liệu này không bị truy xuất bởi các máy chủ ở phân vùng dữ liệu khác. Các tính năng hỗ trợ bảo mật của "Cisco catalyst 6509 switch" bao gồm:

- Gigabit firewall.
- High-performance SSL.
- Gigabit VPN and standards-based IP Security (IPSec)
- VPN layer 2.

Độ sẵn sàng cao:

Cho phép kết nối nhiều đường (*multi path*) nhằm đảm bảo tính sẵn sàng và tăng băng thông cho SAN. Trong mạng LAN thông thường, không đơn giản là chỉ tạo nhiều kết nối song song là thực hiện được kết nối nhiều đường vì hiện tượng gói tin đi vòng có thể xảy ra. "Cisco catalyst 6509 switch" hỗ trợ thêm

một số giao thức đặc biệt làm cho việc kết nối nhiều đường trở nên dễ dàng. Các giao thức đó bao gồm:

- Gateway Load Balancing Protocol.
- Hot Standby Router Protocol.
- Multimodule EtherChannel.
- Rapid Spanning Tree.
- Multiple Spanning Tree.
- Per VLAN Rapid Spanning Tree.
- Rapid Convergence L3 Protocols.

3.3.2.3. Lựa chọn thiết bị lưu trữ

Do giao thức nền tảng được chọn lựa là iSCSI nên thiết bị lưu trữ cũng sẽ phải tương thích với giao thức này. IBM là nhà sản xuất tiên phong trong việc xây dựng và phát triển chuẩn iSCSI và hiện nay hãng đã có một số dòng sản phẩm lưu trữ iSCSI. "IBM IP Storage 200i model 210" là một sản phẩm có cấu hình mạnh nhất của hãng hiện nay, được thiết kế để làm việc trên môi trường hỗn hợp (WinNT, Windows 2000, Linux) và có giá thành hợp lý nên phù hợp với môi trường phần mềm và qui mô của Bảo Việt. Các thông số về thiết bị lưu trữ được thể hiện qua bảng:

Giao tiếp mạng và kết nối: được trang bị sẵn giao tiếp mạng 10/100/1000 Mbps hoặc giao tiếp quang (mạng quang hoạt động theo cơ chế LAN). Giao tiếp mạng sẽ được bổ sung thêm khi cần nhờ các khe cắm còn trống.

- Network	10/100/1000 or Gigabit Fibre
- PCI slots	5 (4x64-bit and 1x32-bit)

Không gian lưu trữ: phạm vi dao động của không gian lưu trữ khá rộng từ mức 192GB đến mức tối đa là 3.5 TB. Điều này cho phép giảm thiểu chi phí trang bị ban đầu và bổ sung không gian lưu trữ khi cần.

- Disk type/ capacity/ speed	Ultra160 SCSI / 36.4 GB / 10 000 rpm Ultra160 SCSI / 73.4 GB / 10 000 rpm (option)
- Number of disks/ capacity (min.)	3 / 109.2 GB
- Number of disks/ capacity (max.)	6/440.4 GB (internal) 48/3.52 TB (with three 4125 Expanded)

Khả năng xử lý: hệ thống được trang bị tối đa 1 GB bộ nhớ trong và 2 bộ vi xử lý hoạt động theo cơ chế đa xử lý đối xứng. Điều này là rất cần thiết bởi giao thức TCP/IP chiếm tài nguyên CPU ở cả bên nguồn, bên đích hay cả ở những thiết bị định tuyến.

- Processor	Two 1.13-GHz Pentium III with 133-MHz front-side bus
- Level 2 cache per processor	512 KB
- Memory	ECC SDRAM memory 1 GB

Khả năng chịu lỗi: để đảm bảo khả năng hoạt động liên tục, hệ thống được trang bị những công nghệ phòng ngừa lỗi dựa trên phương pháp dư thừa. Các thành phần dư thừa của hệ thống bao gồm nguồn và phần đĩa cứng.

- RAID accelerator	ServeRAID 4H - four-channel
- Power supply	Three 250-W (hot swap, auto-restart and redundant)

Phần mềm: "IBM IP Storage 200i model 210" được trang bị sẵn một ổ cứng 20GB để chứa các phần mềm đi kèm và các phần mềm được bổ sung sau này.

- Internal disk	20-GB IDE 20-GB IDE
- Operating system	Linux
- Network management	SNMP
- Remote administration	Web-based GUI Web-based GUI
- Configuration	IBM ServeRAID Manager RAID Configuration and Monitoring. IBM Appliance Configuration Utility.

3.3.2.4. Lựa chọn thiết bị sao lưu

Vì khối lượng dữ liệu của Bảo Việt phải sao lưu là rất lớn, nên việc chỉ sử dụng một băng từ là không khả thi. Chúng tôi lựa chọn cho giải pháp sao lưu là "IBM TotalStorage™ Ultrium Scalable Tape Library 3583". Giải pháp này cho phép sử dụng nhiều băng từ trong quá trình sao lưu và tự động hoá công việc sao lưu. Các thông số kỹ thuật chính của thiết bị bao gồm:

Dung lượng: Thiết bị cho phép sao lưu lượng dữ liệu khá lớn, ngay cả khi sử dụng chế độ sao lưu toàn phần (Full Backup) thì nó vẫn đảm bảo đủ không gian chứa dữ liệu Bảo việt hơn một tháng.

- Media type : IBM TotalStorage LTO Ultrium 200GB Data Cartridge
- Capacity per cartridge : Up to 400 GB per cartridge compressed
- Number of tape cartridges : 72
- Total Capacity per library : Up to 28.8TB compressed; 14.4TB native

Tốc độ sao lưu: tốc độ của thiết bị này cho phép sao lưu toàn bộ dữ liệu của Bảo Việt chỉ mất khoảng một giờ. Việc giảm thiểu thời gian sao lưu là yếu tố quan trọng để nâng cao tính an toàn của dữ liệu, thời gian sao lưu càng dài thì khả năng mất dữ liệu do sự cố trong quá trình sao lưu càng cao.

- Number of drives : Up to 6
- Sustained data transfer rate : Up to 70 MB/sec compressed
- Aggregate sustained data rate : Up to 1482 GB/hour with six drives (compressed)

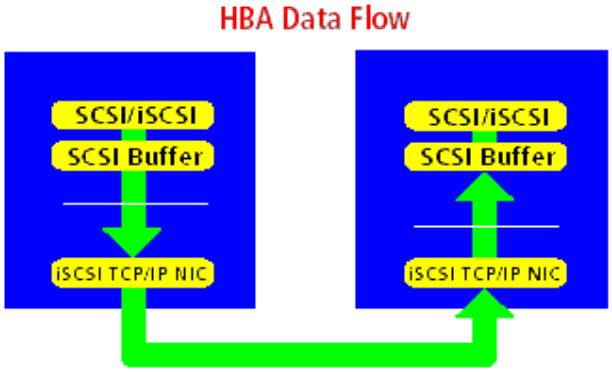
Giao tiếp: Thiết bị cung cấp hai giao tiếp để sử dụng sao lưu số liệu trong môi trường SAN lẫn môi trường DAS (gắn trực tiếp vào máy chủ)

- Native switched fabric 2Gb Fibre Channel.
- LVD Ultra2/Wide or Ultra 160 SCSI.

3.3.2.5. Lựa chọn thiết bị bổ sung

Danh sách thiết bị bổ sung thêm cho giải pháp SAN của bảo việt bao gồm:

- *Cisco SN5420 Storage Router*: Sử dụng để cung cấp kết nối đến các thiết bị SCSI có giao tiếp kênh quang thông qua mạng TCP/IP. Nói cách khác thiết bị này hoạt động như một bộ định tuyến SCSI (SCSI Routing) dựa trên giao thức iSCSI. "Cisco SN5420 Storage Router" rất hiệu quả trong những SAN sử dụng cả thiết bị kênh quang lẫn TCP/IP. Giao tiếp của thiết bị bao gồm:
  - Gigabit Ethernet Port.
  - Fibre Channel Port.
- *Alacritech SES1001T iSCSI Accelerator*: là một giải pháp nhằm cải thiện tốc độ luân chuyển dữ liệu trong IP SAN là sử dụng công nghệ TCP Offload Engine. Công nghệ này thay thế công việc xử lý gói tin TCP/IP của phần mềm bằng cách sử dụng phần cứng chuyên biệt. Nhờ đó, Nó giảm thiểu sự chiếm dụng năng lực CPU của máy chủ và giảm thời gian trễ xử lý. "Alacritech SES1001T iSCSI Accelerator" cũng áp dụng phương thức như vậy, tuy nhiên nó cứng hoá đến lớp iSCSI.

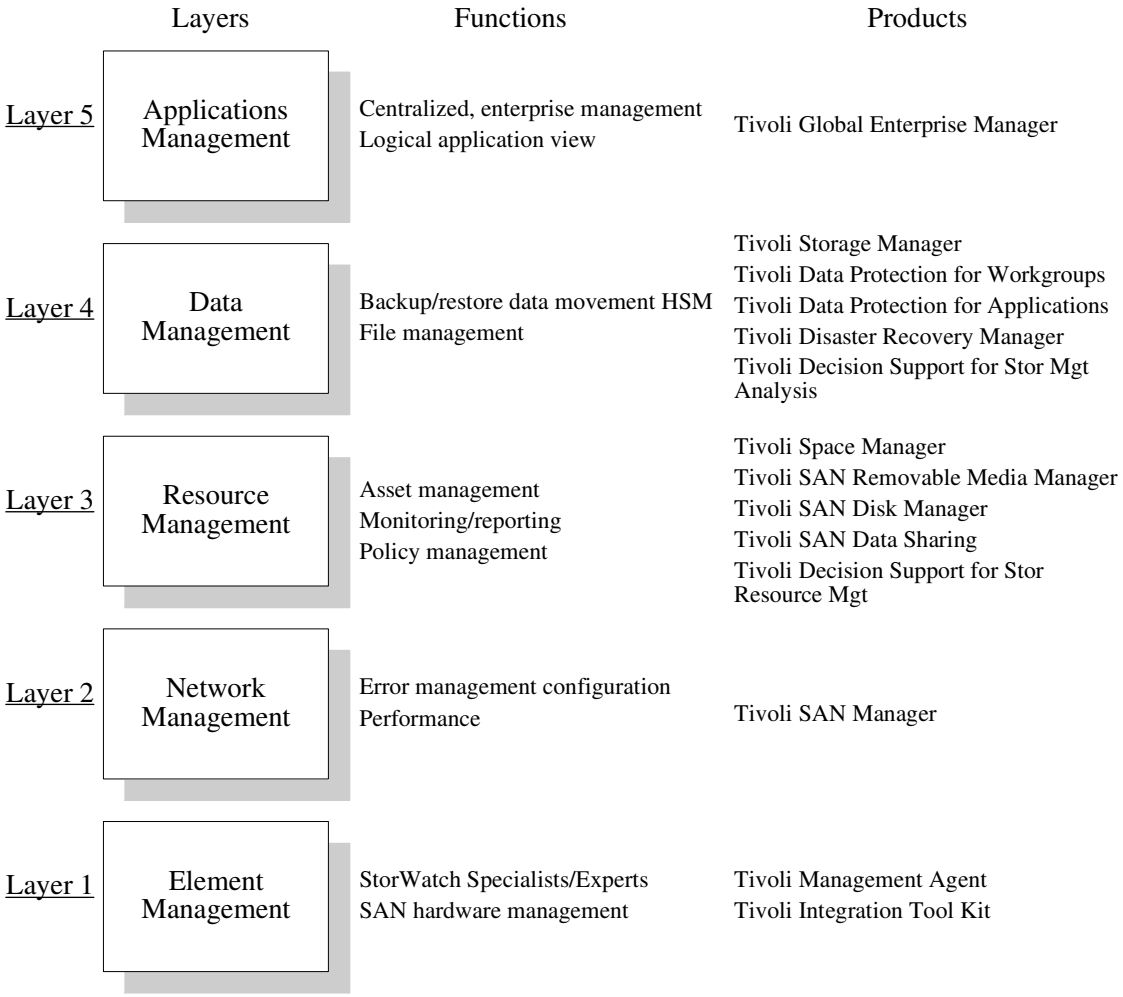


Hình 31 - Luồng dữ liệu thông qua thiết bị "iSCSI Accelerater"

3.3.2.6. Lựa chọn phần mềm quản lý

IBM là một tập đoàn sản xuất thiết bị công nghệ thông tin lớn nhất thế giới. IBM không chỉ cung cấp thiết bị phần cứng mà còn cung cấp các giải pháp chọn gói

gồm nhiều thành phần: máy chủ, máy trạm, thiết bị mạng, thiết bị lưu trữ, hệ điều hành, hệ quản trị cơ sở dữ liệu, hệ phần mềm hỗ trợ nhóm ..vv. Những hiểu biết chuyên sâu về các lĩnh vực công nghệ thông tin là một thuận lợi cho việc thiết kế và xây dựng phần mềm quản lý SAN tốt. "IBM Tivoli Storage Manager" là một trong những phần mềm quản lý SAN được thiết kế theo kiến trúc mở để đảm bảo khả năng hoạt động trên môi trường hỗn hợp.



Hình 32 - Kiến trúc phần mềm Tivoli

"IBM Tivoli Storage Manager" không là một gói phần mềm mà là một tập hợp các mô đun phần mềm. Trong đó mỗi lớp trong mô hình chuẩn mở tương ứng với một hoặc nhiều mô đun phần mềm. Việc chia nhỏ thành các mô đun đảm bảo tính

linh hoạt trong việc phát triển phần mềm quản lý. Hơn nữa khách hàng có thể không phải mua toàn bộ mà chỉ mua những thành phần cần thiết cho nhu cầu hiện tại. Điều này rất phù hợp với Bảo Việt nói riêng và các đơn vị của Việt nam nói chung do nguồn lực về tài chính rất hạn hẹp.

Những mô đun phần mềm Tivoli dự kiến trang bị cho giải pháp SAN của Bảo việt bao gồm:

**** Tivoli Global Enterprise Manager (Tivoli GEM)***: Thuộc lớp quản lý ứng dụng, Tivoli GEM cung cấp cái nhìn trong suốt, tổng thể về hệ thống lưu trữ. Nó giúp quản trị viên tối ưu hóa tài nguyên theo ứng dụng và theo dõi tình trạng hoạt động của SAN.

**** Tivoli Storage Manager (TSM)***: Không thể thiếu mô đun này trong giải pháp, nó cung cấp nền tảng để quản lý dữ liệu. Thuộc lớp quản lý dữ liệu, TSM được cài đặt như là một lớp bên trên của lớp quản lý cơ sở dữ liệu (*Database Manager*). TSM sẽ tối ưu hóa các truy xuất dữ liệu của ứng dụng đối với cơ sở dữ liệu. TSM còn cung cấp thêm các chức năng:

- Chia sẻ ổ tape (Tape Resoure Sharing).
- Sao lưu dữ liệu từ máy trạm mà không sử dụng băng thông của LAN (*LAN-free backup/client transfer*).
- Truyền tải dữ liệu không thông qua máy chủ (*Server-free data transfer*).

**** Tivoli SAN Disk Manager (Tivoli SDM)***: sử dụng Tivoli SDM, quản trị hệ thống có thể: tạo quỹ đĩa ảo từ các thiết bị lưu trữ gắn vào SAN, bớt hoặc phân bổ thêm không gian lưu trữ ảo đó, bảo mật, thiết lập kết nối logic giữa thiết bị chủ quản với các LUNs (*Logical Units*) trong SAN. Nằm trong lớp quản lý tài nguyên, Tivoli SDM bao gồm các thành phần:

- *Common Discovery Agents:* Tích hợp các Agent để phục vụ chức năng quản lý cho các mô đun thuộc lớp bên trên.
- *Host to LUN mapping:* cho phép tạo kết nối logic và bảo mật theo các kịch bản:

- Một số LUN với một thiết bị chủ quản.
- Một số LUN với nhiều thiết bị chủ quản (hay sử dụng với clustering).
- Kết hợp cả hai kịch bản trên.

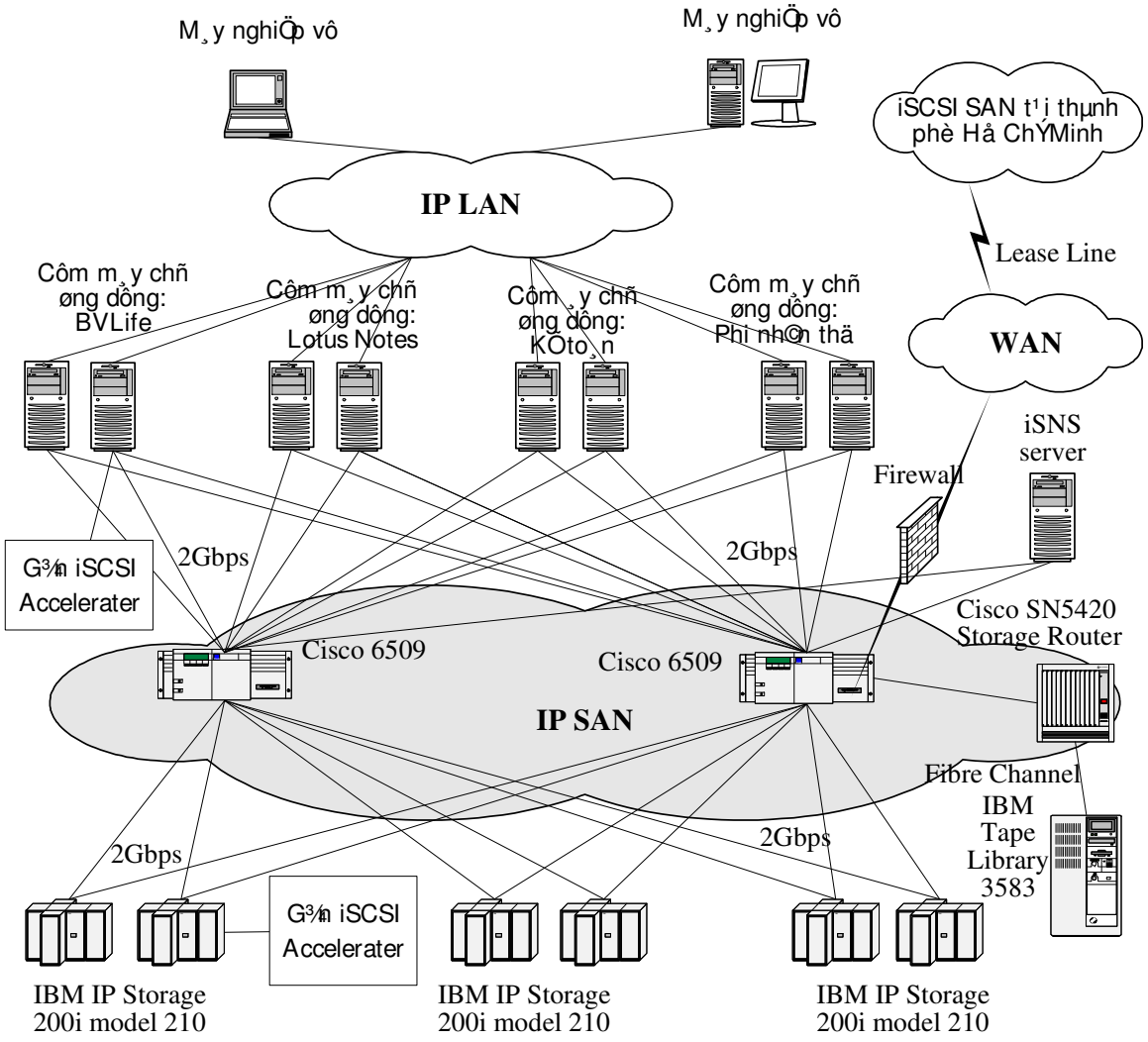
- *Hỗ trợ quyết định trong quản lý tài nguyên lưu trữ*: bằng việc đưa ra các số liệu thống kê về tài nguyên lưu trữ:
  - Số liệu về thiết bị: thông tin về toàn bộ các thiết bị phần cứng trong SAN.
  - Số liệu về không gian lưu trữ: thông tin về không gian lưu trữ thực dụng, không gian lưu trữ thực tế, dung lượng còn trống …
- *Tự động cấp phát không gian lưu trữ*: cho phép ngăn ngừa lỗi xảy ra khi ứng dụng sử dụng hết không gian đĩa được cấp phát. Khi tỷ lệ phần trăm dữ liệu lưu trữ/ không gian lưu trữ của một phân vùng logic lớn hơn ngưỡng do người quản trị thiết lập. Hệ thống sẽ tự động phân bổ không gian lưu trữ dự phòng cho phân vùng đó. Chi tiết sự phân bổ dựa theo các thông tin do người quản trị cung cấp như: cấp phát thêm bao nhiêu dung lượng, lấy từ nguồn dự phòng nào.

**** Tivoli SAN Manager (Tivoli SM)***: Mô đun này cung cấp thông tin quản lý ở mức mạng cho các mô đun phần mềm thuộc lớp trên. Nó sử dụng "Common Discovery Agents" để phát hiện và theo dõi các thiết bị gắn vào SAN. Mọi thông tin thu thập được là cơ sở để nó đưa ra mô hình kiến trúc vật lý của SAN. Người quản trị thực hiện phân vùng hoặc ánh xạ các kết nối từ thiết bị chủ quản đến thiết bị lưu trữ hay và kết nối từ thiết bị lưu trữ đến thiết bị chủ quản dựa trên mô hình kiến trúc vật lý đó. Tivoli SM luôn theo dõi trạng thái hoạt động của các thiết bị. Khi xảy ra lỗi, một mặt nó thông báo với người quản trị, mặt khác nó sẽ cố gắng cô lập lỗi.

**** Tivoli Management Agent (Tivoli MA)***: Thuộc lớp quản lý thành phần, Tivoli MA quản lý các thiết bị phần cứng từ các nhà sản xuất khác nhau bằng cách tự cập nhật, bổ sung các trình điều khiển thiết bị đi kèm vào phần mềm. Nhờ sử dụng đúng phần mềm điều khiển thiết bị cho từng thiết bị, Tivoli MA loại trừ được

sự hoạt động không ổn định của các thiết bị thành phần.

3.3.2.5. Thể hiện chi tiết và đánh giá



Hình 33 - Thiết kế SAN của trung tâm dữ liệu tại Hà nội

Tính sẵn sàng cao: Hệ thống được thiết kế để đảm bảo tính sẵn sàng cao ở tất cả các mức:

- Máy chủ được tổ chức thành các Cluster (cụm).
- Hệ thống mạng backbone cũng bao gồm một cặp hai bộ chuyển mạch Cisco Catalyst 6509.
- Các kết nối giữa thiết bị lưu trữ với nhau và với máy chủ đều sử dụng kết

nối nhiều đường (2 đường). Mô hình kết nối ở đây là mô hình kết nối đầy đủ.

- Các thiết bị lưu trữ sẽ được áp dụng công nghệ RAID nhiều tầng để bảo vệ dữ liệu. Bản thân thiết bị lưu trữ sẽ được cấu hình RAID 5 bảo vệ dữ liệu trong từng hệ thống lưu trữ con (IBM IP Storage 200i). Tiếp đến là sử dụng phần mềm Tivoli để cấu hình RAID 10 cho từng cụm hai "IBM IP Storage 200i series 210".

Với thiết kế trên, độ sẵn sàng của hệ thống đạt được khá cao. Khả năng duy trì hoạt động được tính (theo mô hình khả năng Markov) như sau:

- Gọi P_0: là khả năng thái hoạt động bình thường của hệ thống.
- Gọi P_1: là khả năng một thiết bị bị hỏng nhưng hệ thống vẫn hoạt động được.
- Gọi P_2: là khả năng hệ thống bị hỏng (cả hai thiết bị cùng hỏng).
- $P_0 + P_1 + P_2 = 1$.
- Gọi λ: là tần suất xuất hiện lỗi (tính theo đơn vị lỗi/giờ)
- Gọi μ: là thời gian khắc phục lỗi (tính theo giờ).

Khi đó, quan hệ giữa P_0, P_1, P_2 được thể hiện qua hệ phương trình:

$6\lambda P_0 = \mu (P_1+P_2)$.

$P_1 (3\lambda + \mu) = 6\lambda P_0$.

$\mu P_2 = 3\lambda P_1$.

Ước tính theo số liệu của hãng Cisco cung cấp (μ =0.5 giờ, $\lambda = 1.39 \times 10^{-6}$), Độ sẵn sàng của hệ thống đạt khoảng 99.999999%.

Không gian lưu trữ: Theo thiết kế này, không gian lưu trữ tối đa của SAN có thể được tính như sau:

73.4GB*54*(2/3)*(6/2) = 7927.2GB (xấp xỉ 8 TB)

Trong đó:

- 73.4 GB là dung lượng một ổ cứng trong một thiết bị "IBM IP Storage 200i model 210".

- 54 (48 external + 6 internal) là số ổ cứng tối đa trong một thiết bị "IBM IP Storage 200i model 210".
- 2/3 là tỷ số dung lượng lưu trữ thực khi thiết bị "IBM IP Storage 200i model 210" được cấu hình RAID 5.
- 6/2 là tỷ số dung lượng lưu trữ thực khi 6 thiết bị "IBM IP Storage 200i model 210" thiết bị cấu hình RAID 10.

Không gian lưu trữ sẽ được phân bổ cho các máy chủ ứng dụng tùy theo nhu cầu dữ liệu. Máy chủ trong trung tâm số liệu được tổ chức thành các cụm, mỗi cụm sẽ chạy một nhóm các ứng dụng riêng biệt. Chi tiết tổ chức dịch vụ của các cụm máy chủ bao gồm:

- Cụm máy chủ ứng dụng BV Life sử dụng phần mềm quản trị cơ sở dữ liệu Oracle. Hệ quản trị Oracle sẽ được cấu hình để thực hiện các thao tác vào ra dựa trên các khối dữ liệu logic (I/O Block) mà phần mềm quản lý SAN (mô đun *Tivoli Storage Manager*) cung cấp, nhằm đạt hiệu năng cao trong việc truy xuất và cập nhật cơ sở dư liệu. Phần mềm Oracle 9i sẽ được cài đặt trên nền hệ điều hành Unix và trên phần nền phần cứng HP Class 9000.
- Cụm máy chủ ứng dụng kế toán, quản lý nhân sự sử dụng dịch vụ file do mô đun *Tivoli Storage Manager* cung cấp. Nền tảng phần cứng được sử dụng ở đây sẽ là Intel và hệ điều hành Windows 2000.
- Giống như cụm máy chủ ứng dụng BVLife, cụm máy chủ ứng dụng phần mềm nhóm (thư, quản lý công văn) cũng sử dụng dịch vụ vào ra dựa trên khối do "IBM Tivoli" cung cấp. Phần mềm Lotus Domino sẽ trực tiếp sử dụng khối trong các thao tác đọc ghi dữ liệu của mình. Hệ điều hành được sử dụng trong Cluster này là hệ điều hành mã nguồn mở Linux trên nền Intel (HP Proliant 530).
- Cụm máy chủ ứng dụng bảo hiểm phi nhân thọ được sử dụng cho các nghiệp vụ: xe cơ giới, bảo hiểm con người và học sinh, bảo hiểm cháy, xây lắp, bảo hiểm hàng hóa. Vì các ứng dụng dựa trên cơ sở là chia sẻ file (file

sharing) nên mô đun *Tivoli Storage Manager* sẽ cung cấp dịch vụ file cho những ứng dụng này.

Toàn bộ không gian lưu trữ của SAN sẽ được nhóm thành bốn vùng logic (*logic Zone*) nhờ sự hỗ trợ của máy chủ iSNS để chứa dữ liệu cho các ứng dụng thông qua "Tivoli Resource Management". Dữ liệu luân chuyển trong từng phân vùng thực chất sẽ sử dụng chung các kết nối phần cứng nhưng lại hoạt động trong bốn VSAN(Virtual SAN) khác. Các VSAN được tạo ra nhờ sử dụng tính năng VSAN mà "Cisco Catalyst 6509 switch" cung cấp.

Trong mỗi vùng logic ta có thể phân bổ tiếp thành các ổ logic khác nhau. Ví dụ phân vùng 4 sẽ chứa dữ liệu phục vụ cho cụm máy chủ ứng dụng phi nhân thọ. Máy chủ này cung cấp dịch vụ chia sẻ file cho 4 ứng dụng bảo hiểm phi nhân thọ khác nhau nên ta có thể tạo ra bốn ổ logic để chia sẻ cho bốn nhóm đối tượng khai thác dữ liệu khác nhau.

Sao lưu bảo vệ dữ liệu (backup): Quá trình sao lưu sẽ được tự động hóa, các máy chủ được cài đặt phần mềm Tivoli Storage Manager sẽ cho phép các máy trạm lập lịch công việc sao lưu và ra lệnh phục hồi dữ liệu. Nhờ thiết kế tách biệt SAN và LAN nên dữ liệu sao lưu sẽ chỉ luân chuyển trong SAN và không chiếm dụng băng thông của LAN.

Băng từ sẽ được tổ chức thành các bộ (Media Set), mỗi bộ sẽ gồm 12 băng từ. Cách thức sao lưu được thực hiện như sau:

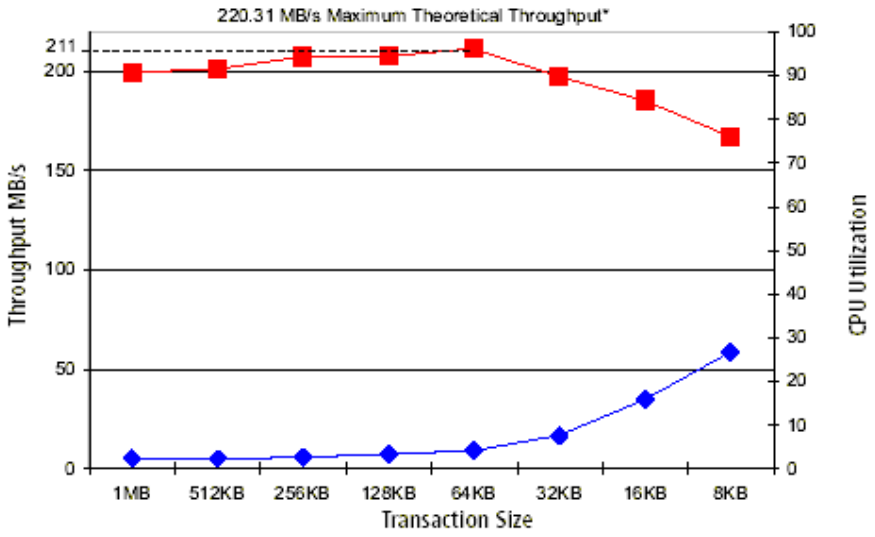
- Bộ thứ nhất sẽ sao lưu theo chế độ sao lưu toàn phần (Full Backup) vào ngày cuối tuần (Chủ nhật)
- Bộ thứ hai sẽ sao lưu theo chế độ tăng cường (Incremental) theo ngày chẵn.
- Bộ thứ ba sẽ sao lưu theo chế độ tăng cường theo ngày lẻ.

Phương thức tổ chức sao lưu như vậy để dung hòa được hiệu quả sao lưu và thời gian khôi phục dữ liệu. Công việc thay đổi các bộ băng mỗi ngày cũng sẽ được tự động hóa bởi "IBM TotalStorage™ Ultrium Scalable Tape Library 3583".

Hiệu năng: SAN được kết cấu từ nhiều thành phần, hiệu năng của SAN không chỉ phụ thuộc vào cấu hình phần cứng các thiết bị thành phần. Nó còn phụ thuộc vào kiến trúc kết nối, cấu hình cụ thể và cả phần mềm khai thác nữa.

Hệ thống mạng SAN sẽ được tách rời với mạng LAN để tránh gây tắc nghẽn và đảm bảo an ninh dữ liệu. Toàn bộ mạng SAN thống nhất sử dụng kết nối Ethernet Full Duplex có tốc độ 2 gigabit. Toàn bộ các máy chủ và các thiết bị lưu trữ "IBM IP Storage 200i model 210" đều được gắn card tăng tốc "Alacritech SES1001T iSCSI Accelerator" để tăng cường hiệu quả sử dụng băng thông mạng và giảm thiểu chiếm dụng CPU của máy chủ.

Hãng Alacritech đã thử nghiệm thiết bị "Alacritech SES1001T iSCSI Accelerator" trên thực tế để kiểm tra tốc độ truyền tải dữ liệu thông qua một kết nối Ethernet 2 Gigabit (Full Duplex). Kết quả được thể hiện qua biểu đồ:



Hình 34 - Biểu đồ chiếm dụng CPU và thông lượng truyền tải

Kết quả đo thể hiện tốc độ luân chuyển dữ liệu dao động từ khoảng 160 MBps cho đến 210 MBps và tỷ lệ chiếm dụng CPU dao động từ 5% đến gần 30%. Thiết bị lưu trữ "IBM IP Storage 200i model 210" chỉ gắn các ổ cứng có tốc độ truyền dữ liệu là 160 MBps. Mô hình SAN của Bảo việt có sử dụng nhiều đường kết nối và dữ liệu thực tiễn cũng được phân mảnh trên các thiết bị lưu trữ khác nhau nên tốc độ trao

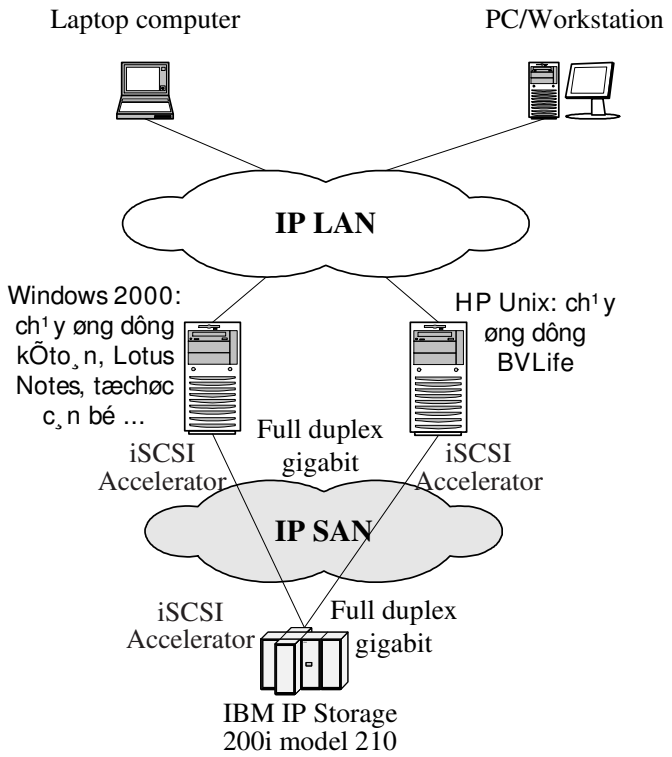
đổi dữ liệu của một ứng dụng có thể vượt qua ngưỡng 210 MBps. Các chỉ số tốc độ sẽ sát hơn khi áp dụng những phần mềm đo đạc trong hệ thống SAN thực tiễn.

3.3.3. Phương án cho các đơn vị thành viên

Mô hình SAN được triển khai tại các đơn vị thành viên sẽ hết sức đơn giản, các thành phần của nó bao gồm:

- Giao thức cơ sở: iSCSI.
- Thiết bị lưu trữ: IBM IP Storage 200i model 210.
- Thiết bị kết nối: Alacritech SES1001T iSCSI Accelerator.
- Thiết bị sao lưu: Sử dụng thiết bị sẵn có.
- Phần mềm quản lý: IBM Tivoli Storage Manager.

Tại các đơn vị thành viên, hai mạng SAN và LAN vẫn được tách rời. Tuy nhiên mô hình kết nối SAN là kết nối thẳng, không thông qua các thiết bị kết nối như bộ chuyển mạch.



Hình 35 - Mô hình SAN ở các đơn vị thành viên

3.3.4. Phương án cho văn phòng đại diện

Không có sự thay đổi trong các văn phòng đại diện, nhu cầu lưu trữ sẽ được được giải quyết bằng cách trang bị thêm thiết bị lưu trữ tháo lắp ngoài hay nâng cấp ổ cứng. Điều đó có nghĩa là những ứng dụng được triển khai tại văn phòng đại diện vẫn sẽ hoạt động trên ổ cứng của máy trạm.

KẾT LUẬN

Xuất phát từ sự cần thiết nhu cầu tìm kiếm của tác giả về giải pháp lưu trữ có thể ứng dụng tốt cho những đòi hỏi công việc hiện tại đề ra và có thể mở rộng trong tương lai, Luận văn này nghiên cứu về giải pháp SAN nói chung và giải pháp IP SAN nói riêng và vận dụng những hiểu biết trong quá trình nghiên cứu để ứng dụng trong thực tế.

Qua quá trình tìm hiểu chúng tôi nhận thấy rằng:

- FC SAN là giải pháp khá hoàn thiện. Nó không chỉ có tốc độ luân chuyển dữ liệu lớn mà còn đáp ứng được các tiêu chí như sự ổn định, bảo mật và đảm bảo chất lượng dịch vụ. Tuy nhiên, triển khai nó không phải là một nhiệm vụ dễ dàng nhất là trong điều kiện nước ta hiện nay.
- IP SAN nổi lên như là một đối thủ tiềm tàng nhất của FC SAN nhờ tính phổ dụng và sự phát triển cả về chiều rộng lẫn chiều sâu của mạng Internet. Triển khai IP SAN khá dễ dàng khi các sản phẩm phần cứng phần mềm hỗ trợ cho giao thức TCP/IP rất phong phú. IP SAN có thể vượt qua những khoảng cách lớn nhờ kết nối thông qua mạng internet mà vẫn đảm bảo an ninh dữ liệu. Một điểm khá bất lợi của IP SAN là hiệu năng không cao do độ trễ gặp phải trong quá trình xử lý gói số liệu TCP/IP. Hạn chế này đã được khắc phục phần nào nhờ công nghệ TOEs (*TCP Offload Engine*) hay iSCSI Accerleter.
- Nằm trong giải pháp IP SAN, giao thức iSCSI như chìa khóa đưa hệ thống lưu trữ SCSI chuyển sang thế hệ lưu trữ mới, vượt qua những giới hạn của kênh SCSI truyền thống. iSCSI SAN vừa có các ưu điểm của IP SAN vừa tiếp thu những thành tựu của công nghệ SCSI sau nhiều năm phát triển. Đặc biệt, chuẩn SCSI-3 sẽ hỗ trợ giao thức iSCSI. Như vậy, iSCSI có thể xuất hiện hầu hết trong các hệ thống thông tin trong một tương lai gần.

Công nghệ SAN được phát triển được nhờ sự tiến bộ của công nghệ kết nối

nên theo dõi sự phát triển của công nghệ kết nối cũng là một cách dự đoán xu hướng phát triển của SAN. Trong thời gian tới, chúng ta có thể bắt gặp những SAN dựa trên cở sở kết nối không dây. "Wireless SAN" là một hướng tiềm năng trong định hướng phát triển SAN.

Sự phong phú các loại hình dịch vụ mà các doanh nghiệp cung cấp làm thay đổi quan niệm về dữ liệu. Khuôn dạng dữ liệu được lưu trữ ngày nay không chỉ là các con số hay text. Âm thanh, hình ảnh thậm chí cả video cũng là những đối tượng để lưu trữ và xử lý. Yêu cầu của những dữ liệu này không chỉ đòi hỏi về băng thông mà còn đòi hỏi về chất lượng dịch vụ. FC SAN có thể đáp ứng được khá tốt về chất lượng dịch vụ. Đảm bảo chất lượng dịch vụ trong IP SAN là một hướng nghiên cứu cần thiết để làm phong phú giải pháp IP SAN.

TÀI LIỆU THAM KHẢO

[1] Tom Clarl (2002), *A Guide to iSCSI, iFCP, and FCIP Protocols for Storage Area Networks*, pp.126 - 149

[2] Kevin Duncan (2001), *Fibre Channel and Gigabit Ethernet: A Look at Technology for Storage Area Networks*, pp.13-14

[3] Ravi Kumar Khattar, *Introduction to Storage Area Network*, pp.52-61

[4] Rowell Hernandez (2002), *Using iSCSI Solutions' Planning and Implementation*, pp.4-14

[5] Jon Tate (2000), *Designing an IBM Storage Area Networks*, pp.36 - 42, 155 – 166

[6] John Vacca (2002), *The Essential Guide to Storage Area Network*, pp.4 - 5

MỤC LỤC