MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CÁC TỪ VIẾT TẮT

CÁC THUẬT NGỮ

DFS Namespace	Là một vùng tên trung tâm giúp người dùng có thể có được cái nhìn thống nhất về một folder chia sẻ có trong DFS.
Namespace Root	Là phần cao nhất trong DFS Namespace, Namespace root và DFS namespace có cùng tên.
DFS Folder	Là một folder hiện diện với client trong DFS namespace, nhưng dưới quyền DFS root.
DFS Tree	Là quy chiếu cho trật tự DFS. Một cây bắt đầu với DFS root, và chứa tất cả các folder DFS đã được xác định trong root.

CÁC TỪ VIẾT TẮT

APR	Address Resolution Protocol	Phân giải địa chỉ MAC
BDC	Backup Domain Controller	Hệ thống chạy dự phòng khi PDC xảy ra lỗi.
CSDL	Cơ sở dữ liệu	

DHCP	Dynamic Host Configuration Protocol	Cấp phát địa chỉ IP động
DPM	Data Protect Manager	Phần mềm sao lưu – phục hồi dữ liệu cho hệ thống Exchange, MS SQL
DFS	Distributed File System	Hệ thống lưu trữ file tập trung
DNS	Domain Name System	Dùng để ánh xạ giữa các tên miền và các địa chỉ IP.
FTP	File Transfer Protocol	Dịch vụ truyền tập tin
GAN	Global Area Network	Mạng kết nối máy tính từ các châu lục khác nhau.
HTTP	Hypertext Transfer Protocol	Giao thức ứng dụng web
ICMP	Internet Control Message Protocol	Giao thức giám sát tình trạng mạng
IGMP	Internet Group Management Protocol	Giao thức ứng dụng multicast
IMAP	Internet Message Access Protocol	Giao thức truy cập thư điện tử
LAN	Local Area Network	Mạng cục bộ
MAC	Medium Access Control	Giao thức điều khiển truy cập
MAN	Metropolitan Area Network	Mạng đô thị

MS SQL	Microsoft Structured Query Language	Ngôn ngữ truy vấn có cấu trúc của hãng Microsoft
NAS	Network Attack Storage	Giải pháp lưu trữ dữ liệu trên mạng máy tính
NIC	Network Interface Controller	Thiết bị giao tiếp mạng
NNTP	Network New Transfer Protocol	Giao thức gửi, chuyển tiếp và tìm kiếm thông điệp
PDC	Primary Domain Controller	Hệ thống quản trị người dùng và tài khoản trong Domain
POP3	Post Office Protocol version 3	Giao thức mail
SAM	Security Account Manager	Hệ thống quản trị tài nguyên
SMTP	Simple Mail Transfer Protocol	Giao thức gửi và nhận e-mail
SNMP	Simple Network Management Protocol	Giao thức quản lý thiết bị
TCP	Tranmission Control Protocol	Giao thức truyền dữ liệu hướng liên kết.
TELNET	Terminal Network	Giao thức kết nối thiết bị đầu cuối ảo.
UDP	User Datagram Protocol	Giao thức truyền dữ liệu phi liên kết.
WAN	Wide Area Network	Mạng diện rộng

DANH MỤC CÁC BẢNG VÀ HÌNH VẼ

CÁC BẢNG

HÌNH VẼ

MỞ ĐẦU

Hiện nay, khoa học kỹ thuật phát triển dẫn đến sự bùng nổ của Internet. Việc ứng dụng ngày càng rộng rãi của thương mại điện tử và các ứng dụng multimedia đã làm cho yêu cầu về lưu trữ thông tin ngày càng tăng. Các nhà phân tích dự tính rằng yêu cầu về lưu trữ đang tăng lên khoảng 100% mỗi năm.

Dữ liệu sẽ phải đối diện với nhiều mối đe dọa khác nhau, trong đó những rủi ro thường xảy ra hư hỏng dữ liệu: do các lỗi vật lý, do virus hay do lỗi của người dùng hoặc do các thảm họa như động đất, hỏa hoạn, khủng bố…

Em đã chọn đề tài *"Xây dựng hệ thống lưu trữ tập trung trên nền tảng Distributed File System Windows Server 2008 "* làm đồ án tốt nghiệp của mình. Với đồ án này em mong muốn tìm hiểu sâu hơn về vấn đề đảm bảo an toàn cho hệ thống dữ liệu.

Được sự chỉ bảo, hướng dẫn tận tình của các thầy, cô trong Khoa, đặc biệt là thầy giáo, Thạc sỹ Bùi Huy Hùng, em đã hoàn thành đồ án với 03 nội dung chính:

Thứ nhất là đưa ra cái nhìn tổng quát về mạng máy tính.

Thứ hai là tìm hiểu các mô hình mạng và một số dịch vụ mạng thường sử dụng trên Windows.

Thứ ba là xây dựng hệ thống lưu trữ dữ liệu tập trung dựa trên nền tảng Distributed File System trên Windows Server.

Em mong rằng đồ án sẽ đưa ra cho mọi người một cái nhìn tổng quát về mạng máy tính. Ngoài ra đồ án giới thiệu giải pháp đảm bảo an toàn cho hệ thống dữ liệu người dùng. Mặc dù nhận được sự chỉ bảo tận tình của các thầy cô, nhưng do trình độ, thời gian có hạn nên đề tài vẫn mắc phải những thiếu sót. Vì vậy em rất mong nhận được sự chỉ bảo, phê bình và góp ý quý báu đến từ thầy cô và các bạn.

Em xin chân thành cảm ơn!

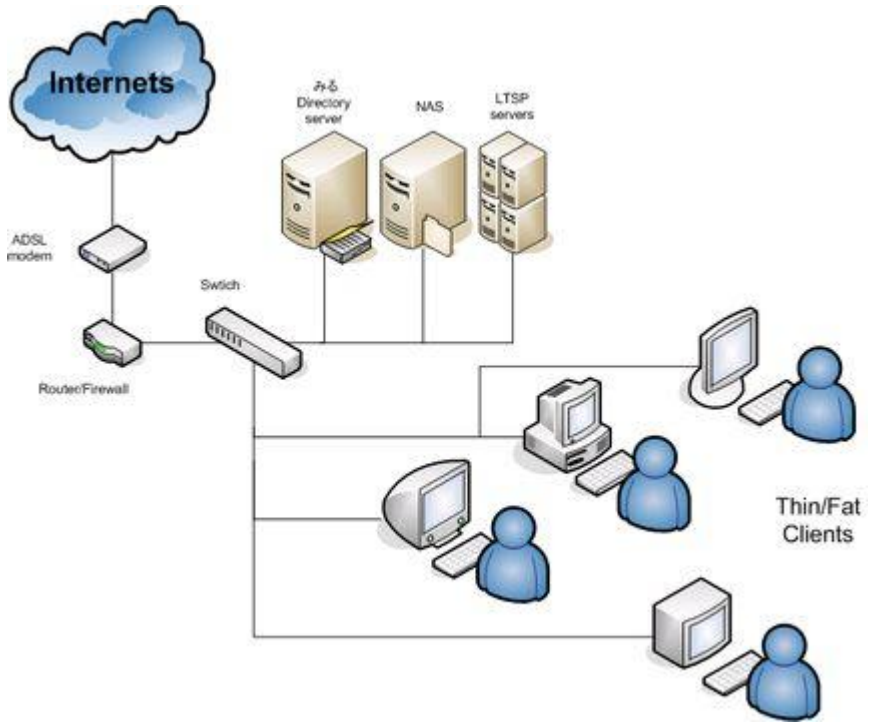
CHƯƠNG 1: TỔNG QUAN VỀ MẠNG MÁY TÍNH

1.1 Mạng máy tính

1.1.1 Khái niệm về mạng máy tính

Mạng máy tính là tập hợp các máy tính được kết nối với nhau bởi các đường truyền theo một cấu trúc nào đó và thông qua đó các máy tính có thể trao đổi thông tin qua lại cho nhau.

Đường truyền là một hệ thống các thiết bị truyền dẫn có dây, không dây dùng để chuyển các tín hiệu điện tử từ máy này sang máy khác. Đường truyền kết nối có thể là: cáp đồng trục, cáp xoắn đôi, cáp quang, các đường truyền tạo nên cấu trúc mạng.



Hình 1.1: Mô hình mạng máy tính.

Lợi ích của mạng máy tính:

- Sử dụng chung một phần mềm tiện ích.
- Chia sẻ kho dữ liệu dùng chung.

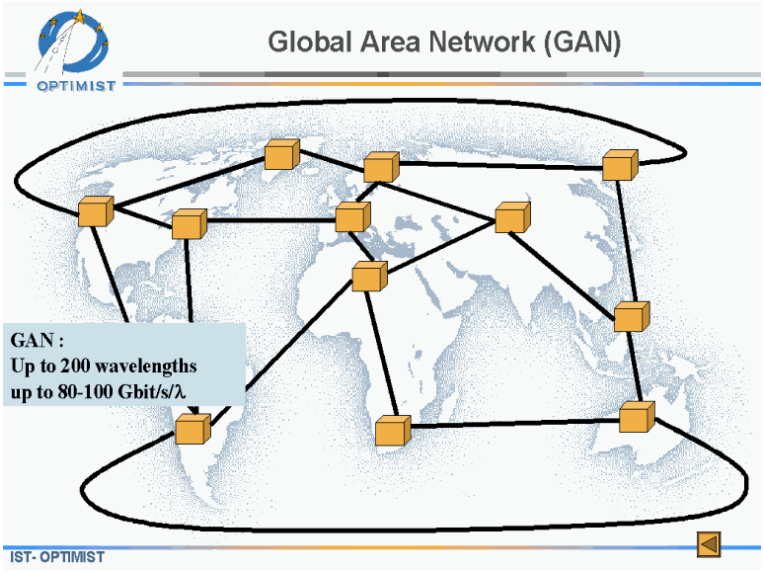
- Trao đổi thông điệp hình ảnh.
- Dùng chung các thiết bị ngoại vi (máy in, máy fax, modem…).
- Giảm thiểu chi phí và thời gian đi lại.
- Tăng độ tin cậy của hệ thống, dễ dàng bảo trì máy móc và lưu trữ (backup) dữ liệu chung khi có sự cố. Đồng thời hệ thống cũng có thể khôi phục nhanh chóng. Các dữ liệu có thể được đồng bộ từ đó nâng cao hiệu quả khai thác.

1.1.2 Phân biệt các loại mạng

Máy tính ngày nay phát triển khắp nơi với những ứng dụng ngày càng đa dạng cho nên để phân biệt được một cách đầy đủ và chi tiết các loại mạng là một việc rất phức tạp.

1.1.2.1 Phân loại mạng theo vùng địa lý

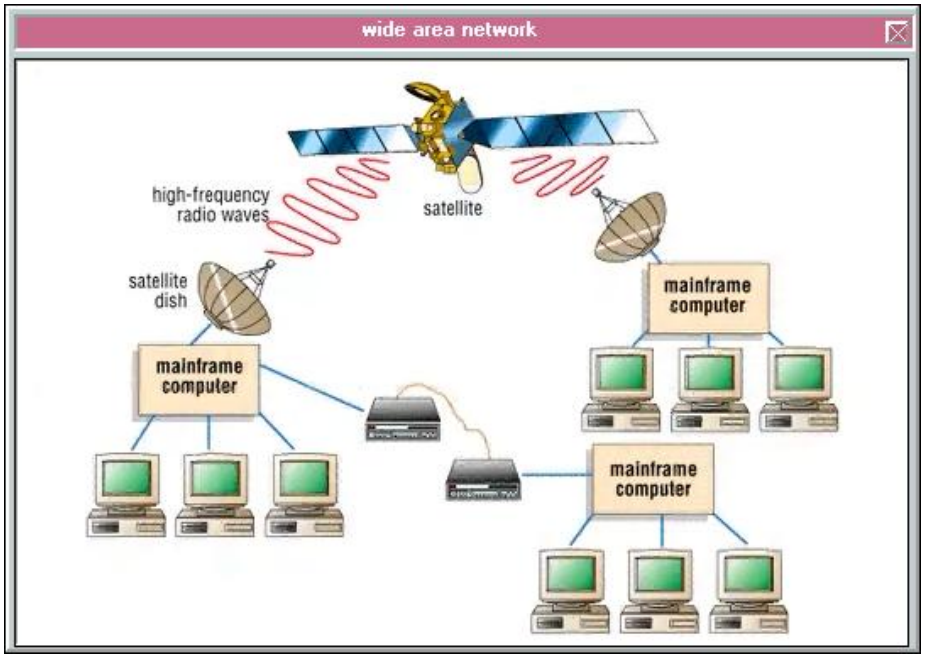
GAN (Global Area Network) là mạng dùng để kết nối máy tính từ các châu lục khác nhau. Thông thường kết nối này được thông qua mạng viễn thông.



Hình 1.2:Mô hình mạng GAN

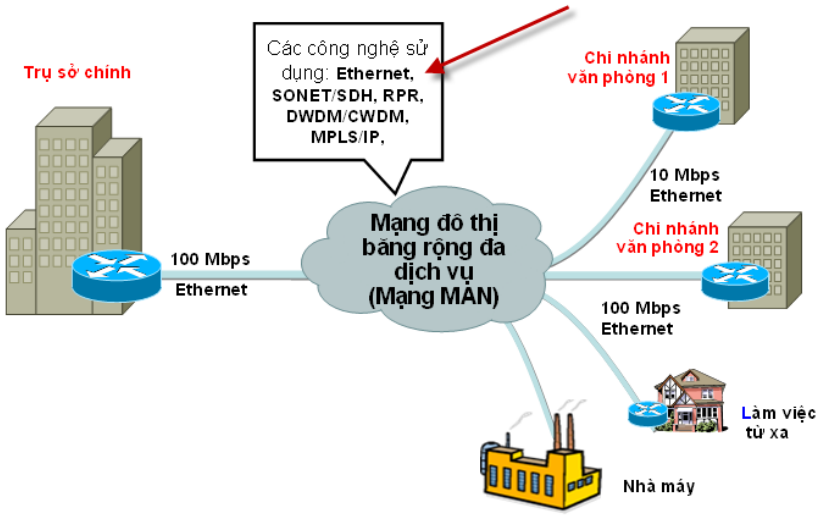
WAN (Wide Area Network) mạng diện rộng: là mạng dùng để kết nối máy tính trong nội bộ các quốc gia hay giữa các quốc gia trong một vụng châu lục.

Thông thường kết nối này thường được thực hiện thông qua mạng viễn thông. Các mạng WAN có thể được kết nối với nhau thành GAN hay tự nó đã là GAN.



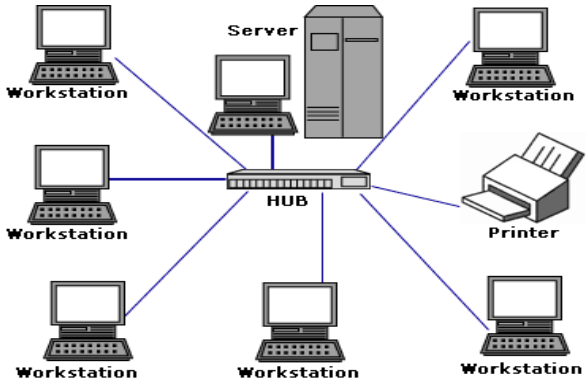
Hình 1.3: Mô hình mạng WAN

MAN (Metropolitan Area Network) là mạng dùng để kết nối các máy tính trong phạm vi một thành phố. Kết nối này được thực hiện thông qua các môi trường truyền thông tốc độ cao (50 – 100 Mbit/s).



Hình 1.4: Mô hình mạng MAN

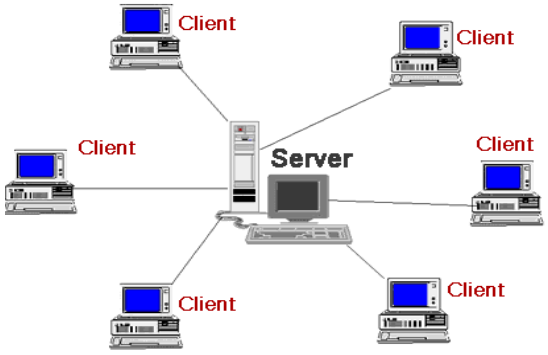
LAN (Local Area Network) mạng cục bộ: là mạng dùng để kết nối các máy tính trong một khu vực bán kính hẹp thông thường khoảng vài trăm mét. Kết nối được thực hiện thông qua các môi trường truyền thông tốc độ cao, ví dụ: cáp đồng trục, cáp xoắn đôi, cáp quang,... LAN thường được sử dụng trong một cơ quan/tổ chức như: trường học, phòng thực hành,… Các mạng LAN có thể được kết nối với nhau qua WAN.



Hình 1.5: Mô hình mạng LAN

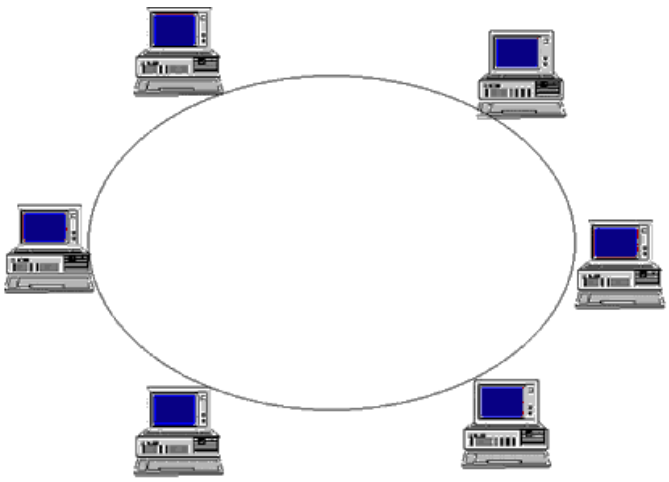
1.1.2.2 Phân loại mạng theo chức năng

Mạng Client – Server: một hay một số máy tính được thiết lập để cung cấp các dịch vụ như: file server, mail server… Các máy tính được thiết lập để cung cấp các dịch vụ được gọi là Server, còn các máy tính truy cập và sử dụng dịch vụ thì được gọi là Client.



Hình 1.6: Mô hình mạng Client – Server.

Mạng ngang hàng (Peer – to – Peer): Các máy tính trong mạng có thể hoạt động vừa như một Client vừa như một Server.



Hình 1.7: Mô hình mạng Peer – to – Peer.

Mạng kết hợp: Các mạng máy tính thường được thiết lập theo cả hai mô hình mạng Client – Server và Peer – to – Peer.

1.1.3 Phân loại mạng theo cấu trúc (Topology)

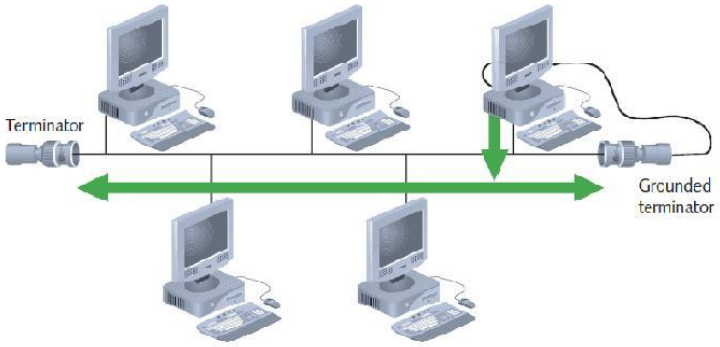
Topology là cấu trúc hình học không gian của mạng, thực chất nó là cách bố trí vật lý các điểm và cách thức kết nối chúng lại với nhau. Điển hình và sử dụng nhiều nhất là các mạng theo cấu trúc: dạng xương sống, dạng vòng, dạng hình sao, cùng với các dạng kết hợp của chúng.

1.1.3.1 Mạng dạng xương sống (Bus Topology)

Thực hiện theo cách bố trí hành lang, các máy tính và các thiết bị khác – các nút, đều được kết nối với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu. Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được bít bởi một thiết bị gọi là Terminator. Các tín hiệu và dữ liệu khi truyền đi trên dây cáp đều mang theo địa chỉ nơi đến.

- **Ưu điểm:** Loại hình này dùng dây cáp ít nhất, dễ lắp đặt giá thành rẻ.

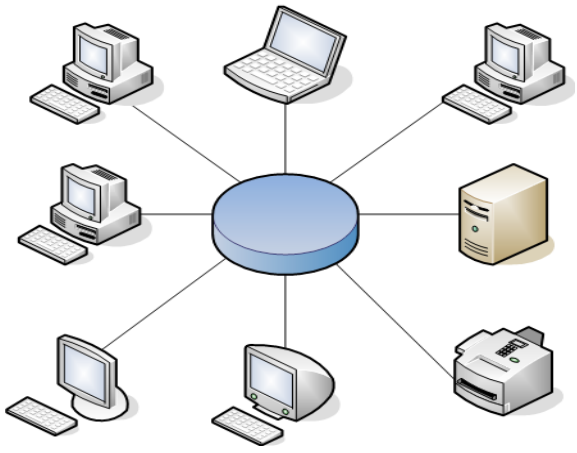
- **Nhược điểm:** Sự tắc nghẽn đường truyền khi di chuyển dữ liệu với lưu lượng lớn. Khi có sự cố ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống. Cấu trúc này ngày nay ít sử dụng.



Hình 1.8: Cấu trúc mạng dạng xương sống (Bus topology)

1.1.3.2 Mạng dạng vòng (Ring Topology)

Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có địa chỉ kèm theo cụ thể của mỗi trạm tiếp nhận.



Hình 1.9: Cấu trúc mạng dạng vòng (Ring Topology)

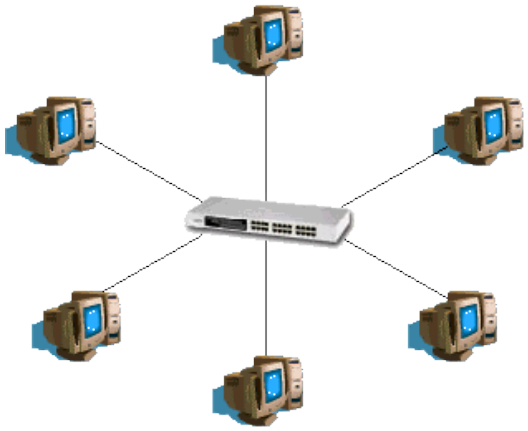
- **Ưu điểm:** Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Mỗi trạm có thể đạt được tốc độ tối đa khi truy nhập.
- **Nhược điểm:** Đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.

1.1.3.3 Mạng dạng sao (Star Topology)

Mạng dạng hình sao bao gồm một bộ kết nối trung tâm và các nút. Các nút này là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Bộ kết nối trung tâm cảu mạng diều phối mọi hoạt động trong mạng.

Mạng hình sao cho phép nối các máy tính vào một bộ tập trung (Hub) bằng cáp, giải pháp này cho phép nối trực tiếp máy tính với Hub không cần thông qua trục BUS, tránh được các yếu tố gây ngưng trệ mạng.

Mô hình kết nối hình sao ngày nay đã trở lên hết sức phổ biến. Với việc sử dụng các bộ tập trung hoặc bộ chuyển mạch, cấu trúc hình sao có thể được mở rộng bằng cách tổ chức nhiều mức phân cấp, do vậy dễ dàng cho việc quản lý và vận hành.



Hình 1.10: Cấu trúc mạng hình sao (Star topology)

- **Ưu điểm:**
  - Hoạt động theo nguyên lý nối song song nên nếu có một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
  - Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
  - Mạng có thể dễ dàng mở rộng hoặc thu hẹp
- **Nhược điểm:**
  - Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm.
  - Khi trung tâm có sự cố xảy ra thì toàn mạng ngừng hoạt động.
  - Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100m).

Để triển khai mô hình mạng này thì người ta thường sử dụng các thiết bị như sau:

* Thiết bị giao tiếp mạng - NIC (Network Interface Controller) là thiết bị để kết nối với mạng LAN, mỗi NIC có một địa chỉ MAC cung cấp định danh duy nhất cho từng thiết bị.
* Bộ tập trung – Hub là thiết bị kết nối các thiết bị một cáp tới một cổng trên Hub. Hub hoạt động như một bộ chuyển tiếp, khi nó chuyển từng thông điệp từ cổng này tới cổng khác và chuyển tới mạng. Hub là một thành phần tương đối đơn giản của một mạng, hoạt động ở tầng vật lý để truyền dữ liệu mà không cần thao tác xử lý nào. Điều này làm cho các hub dễ cài đặt và quản lý, vì chúng không đòi hỏi cấu hình đặc biệt nào.

Hình 1.11: Bộ tập trung Hub

* Switch tương tự như Hub, tuy nhiên thì switch tối ưu băng thông bằng cách tạo ra một kênh ảo.

Hình 1.12. Bộ chuyển mạch (Switch)

* Router: là thiết bị kết nối các mạng LAN, giữa mạng LAN ra WAN và tìm đường tối ưu.

Hình 1.13: Bộ định tuyến (Router)

1.1.3.4 Mạng kết hợp

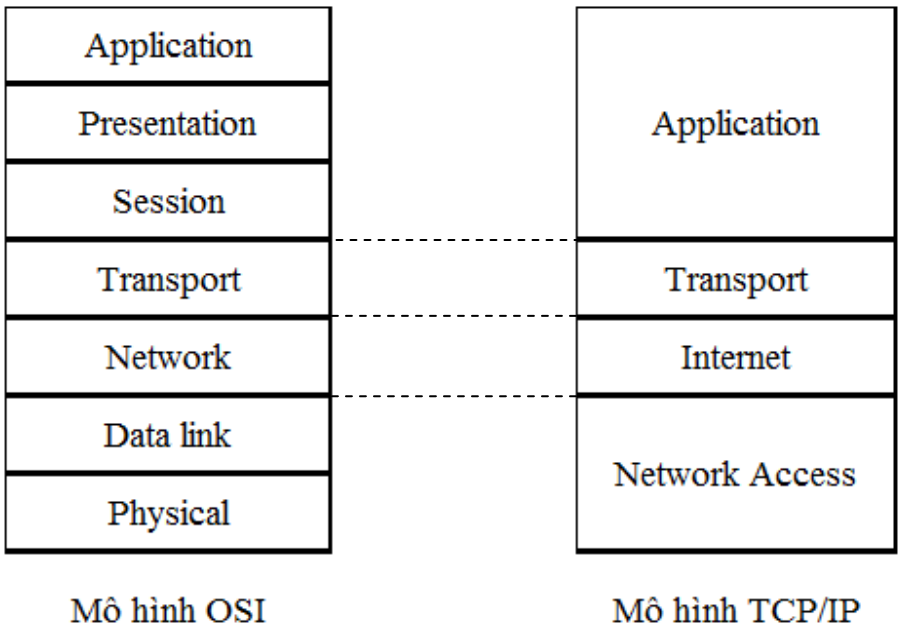
Kết hợp hình sao và hình tuyến: Cấu hình mạng dạng này có bộ phận tách tín hiệu (Spliter) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể

chọn Ring Topology hoặc Linear Bus Topology. Ưu điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở xa cách nhau.

Cấu hình dạng kết hợp Star/Ring Topology có một thẻ bài liên lạc được chuyển vòng quanh một cái Hub trung tâm. Mỗi trạm làm việc được nối với Hub là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

1.2 Mô hình phân tầng

Hiện nay kiến trúc hệ thống mạng được định nghĩa theo hai dạng mô hình là: TCP/IP (4 tầng) và OSI (7 tầng). Nhưng trong thực tế thì mô hình OSI rất khó cài đặt và ứng dụng trong thực tế. Hai mô hình TCP/IP và OSI có sự tương đồng với nhau, nhưng mô hình OSI chia kiến trúc mạng thành 7 tầng logic. Mỗi tầng của mô hình OSI chỉ ra các nhiệm vụ cơ bản của các giao thức mạng phải thực hiện. Một tầng trong mô hình TCP/IP có thể ứng với một hay nhiều tầng trong mô hình OSI như hình 1.14.



Hình 1.14: Kiến trúc của mô hình OSI và TCP/IP

1.2.1 Tầng vật lý (Physical)

Tầng vật lý bao gồm môi trường vật lý như yêu cầu về cáp nối, các thiết bị kết nối, các đặc tả giao tiếp, hub và các repeater,...

1.2.2 Tầng liên kết dữ liệu (Data Link)

Tầng liên kết có nhiệm vụ truyền dữ liệu giữa các thực thể mạng, phát hiện và có thể sửa chữa các lỗi trong tầng vật lý (nếu có).

Các đặc tính: tạo khung (framing), tạo địa chỉ vật lý (MAC), điều khiển lưu lượng, kiểm tra lỗi, điều khiển truy cập.

Địa chỉ MAC là địa chỉ của tầng 2. Các nút trên LAN gửi thông điệp cho nhau bằng cách sử dụng các địa chỉ IP và các địa chỉ này phải được chuyển đổi sang các địa MAC tương ứng.

Giao thức phân giải địa chỉ (ARP: Address Resolution Protocol) chuyển đổi địa chỉ IP thành địa chỉ MAC.Một vùng nhớ cache lưu trữ các địa chỉ MAC tăng tốc độ xử lý này, và có thể kiểm tra bằng tiện ích arp –a

1.2.3 Tầng mạng (Network)

Tầng mạng là tầng nằm ngay phía trên tầng liên kết dữ liệu, nó có chức năng định tuyến qua đó cho phép truyền dữ liệu từ một nguồn tới một đích thông qua một hoặc nhiều mạng

Giao thức được sử dụng là Internet Protocol (IP), nó sử dụng các địa chỉ IP để định danh các nút trên mạng. Các router ở tầng 3 được sử dụng để định đường đi trong mạng.

1.2.4 Tầng giao vận (Transport)

Tầng giao vận có nhiệm vụ chuyển dữ liệu giữa các người dùng tại đầu cuối và kiểm soát độ tin cậy của một kết nối cho trước.

Để phân biệt các ứng dụng trao đổi dựa trên address ports.

Các giao thức được sử dụng là TCP và UDP.

Phương thức truyền dữ liệu:

- **Theo độ tin cậy:**
  - Với độ tin cậy cao: tầng giao vận có nhiệm vụ gửi đi các gói tin xác thực hay các thông điệp truyền lại nếu dữ liệu bị hỏng hay bị thất lạc, hay dữ liệu bị trùng lặp.
  - Với độ tin cậy không cao: tầng giao vận sẽ không kiểm tra xem các gói tin hay các thông điệp đã nhận được, có lỗi xảy ra hay không.
- **Theo sự liên kết:**
  - Hướng liên kết: một kết nối phải được thiết lập trước khi dữ liệu hay các thông điệp được gửi hoặc nhận.
  - Phi liên kết: không cần giai đoạn thiết lập liên kết.

1.2.5 Tầng Phiên (Session)

Tầng phiên có nhiệm vụ thiết lập, quản lý và kết thúc các kết nối giữa trình ứng dụng cục bộ với trình ứng dụng ở xa.

Tầng phiên có những đặc điểm:

- Hỗ trợ các hoạt động song công (duplex), bán song công (half-duplex) hoặc đơn công (single).
- Thiết lập các quy trinh đánh dấu các điểm hoàn thành (checkpointing) – giúp việc phục hồi truyền thông nhanh hơn khi có lỗi xảy ra.
- Ngắt mềm các phiên và kiểm tra phục hồi các phiên.

1.2.6 Tầng trình diễn (Presentation)

Tầng trình diễn làm nhiệm vụ dịch dữ liệu được gửi từ tầng Application sang định dạng (Format) chung.

Các chức năng của tâng trình diễn:

- Dịch các mã ký tự từ bảng mã ASCII sang EBCDIC.
- Chuyển đổi dữ liệu.

- Nén dữ liệu để giảm lượng dữ liệu trên mạng.
- Mã hóa và giải mã dữ liệu để đảm bảo sự bảo mật trên mạng.

1.2.7 Tầng ứng dụng (Application)

Tầng ứng dụng có nhiệm vụ giúp người dùng truy cập các thông tin và dữ liệu trên mạng thông qua các chương trình ứng dụng. Đây là giao diện chính để người dùng tương tác với chương trình ứng dụng, thông qua đó truy cập vào mạng.

Các giao thức hoạt động trong tầng ứng dụng gồm có: Telnet, giao thức truyền tập tin FTP, giao thức truyền thư điện tử SMTP, HTTP,…

1.3 Các giao thức mạng

Mô hình OSI đã chỉ ra một mô hình các tầng giao thức và cách chúng hoạt động cùng với nhau. Trong thực tế thì một dạng cụ thể của mô hình OSI đã được cài đặt là chồng giao thức của bộ giao thức TCP/IP, nó bao gồm 4 tầng: Network Access, Internet, Transport và Application.

Trong đó:

- Tầng liên kết (Network Access) tương ứng tầng vật lý (Physical) và tầng liên kết dữ liệu (Data Link) trong mô hình OSI.
- Tầng mạng (Internet) sử dụng giao thức IP, tương ứng với tầng mạng (Network) trong mô hình OSI.
- Tầng giao vận (Transport) sử dụng giao thức TCP và UDP, tương ứng với tầng giao vận (Transport) trong trong mô hình OSI.
- Tầng ứng dụng (Application) thực hiện nhiệm vụ của các tầng phiên (Session), tầng trình diễn (Presentation) và tầng ứng dụng (Application) trong mô hình OSI.

Để tìm hiểu về chức năng và mục đích của các giao thức của họ giao thức TCP/IP, chúng ta tìm hiểu theo trình tự:

- Các giao thức cơ bản.

- Các giao thức Internet.
- Các giao thức E-mail.
- Các giao thức khác.

1.3.1 Các giao thức mạng cơ bản

Họ giao thức TCP/IP có cấu trúc phân tầng đơn giản hơn nhiều so với mô hình OSI. Trong đó IP, TCP, UDP, ICMP và IGMP là các giao thức chính trong họ giao thức TCP/IP. Hai giao thức ICMP và IGMP là mở rộng tính năng của giao thức IP.

1.3.1.1 Internet Protocol – IP

IP là một giao thức hướng dữ liệu và không liên kết, được sử dụng bởi các máy chủ nguồn và đích để truyền dữ liệu trong một liên mạng chuyển mạch gói. Nó có chức năng định tuyến trong môi trường liên mạng và thiết lập cơ bản về Internet.

Hiện nay trên thế giới tồn tại hai dạng là: IPv4 và IPv6.

Khi gửi một thông điệp (dữ liệu), giao thức IP nhận thông điệp (dữ liệu) từ các giao thức tầng trên như TCP hay UDP và đưa vào trường header chứa thông tin của đích. Một gói tin trong giao thức IP có các thông tin như trong bảng 1.1.

Trường	Độ dài	Mô tả
IP Version (Phiên bản IP)	4 bits	Phiên bản IP. (Phiên bản giao thức hiện nay là IPv4 và IPv6)
IP Header Length (Chiều dài Header)	4 bits	Chiều dài của header.
Type of Service (Kiểu dịch vụ)	1 byte	Kiểu dịch vụ cho phép một thông điệp được đặt ở chế độ thông lượng cao hay bình thường, thời gian trễ là bình thường hay lâu, độ tin cậy bình thường hay cao. Điều này có lợi cho các gói được gửi đi trên mạng. Một số kiểu mạng sử dụng thông tin này để xác định độ ưu tiên
Total Length (Tổng chiều dài)	2 bytes	Hai byte xác định tổng chiều dài của thông điệp – header và dữ liệu. Kích thước tối đa của một gói tin IP là 65535, nhưng điều này là không thực tế đối với các mạng hiện nay. Kích thước lớn nhất được chấp nhận bởi các host là 576 bytes. Các thông điệp lớn có thể phân thành các đoạn – quá trình này được gọi là quá trình phân đoạn
Identification (Định danh)	2 bytes	Nếu thông điệp được phân đoạn, trường định danh trợ giúp cho việc lắp ráp các đoạn thành một thông điệp. Nếu một thông điệp được phân thành nhiều đoạn, tất cả các đoạn của một thông điệp có cùng một số định danh.
Flags	3 bits	Các cờ này chỉ ra rằng thông điệp có được phân đoạn hay không, và liệu gói tin hiện thời có phải là đoạn cuối cùng của thông điệp hay không.
Fragment Offset	13 bits	13 bit này xác định offset của một thông điệp. Các đoạn có thể đến theo một thứ tự khác với khi gửi, vì vậy trường offset là cần thiết để xây dựng lại dữ liệu ban đầu. Đoạn đầu tiên của một thông điệp có offset là 0

Trường	Độ dài	Mô tả
Time to Live	1 byte	Xác định số giây mà một thông điệp tồn tại trước khi nó bị loại bỏ.
Protocol	1 byte	Byte này chỉ ra giao thức được sử dụng ở mức tiếp theo cho thông điệp này. Các số giao thức
Header Checksum	2 bytes	Đây là chỉ là checksum của header. Bởi vì header thay đổi với từng thông điệp mà nó chuyển tới, checksum cũng thay đổi.
Source Address	4 bytes	Cho biết địa chỉ IP 32 bit của phía gửi
Destination Address	4 bytes	Địa chỉ IP 32 bit của phía nhận
Options	variabe	
Padding	variabe	

Bảng 1.1: Cấu trúc gói tin trong giao thức IP

1.3.1.1.1 IPv4 – Internet Protocol version 4

IPv4 là phiên bản chính thức đầu tiên của IP. Mỗi địa chỉ IP có 32 bit, đếm đều từ trái sang phải từ bit 1 đến bit 32 chia thành 4 octet (1octet = 8 bit), các octet cách nhau bởi dấu chấm (.) có dạng: x.x.x.x.

Ví dụ: Địa chỉ 192.168.1.1 biểu diễn dưới dạng 32 bit nhị phân:

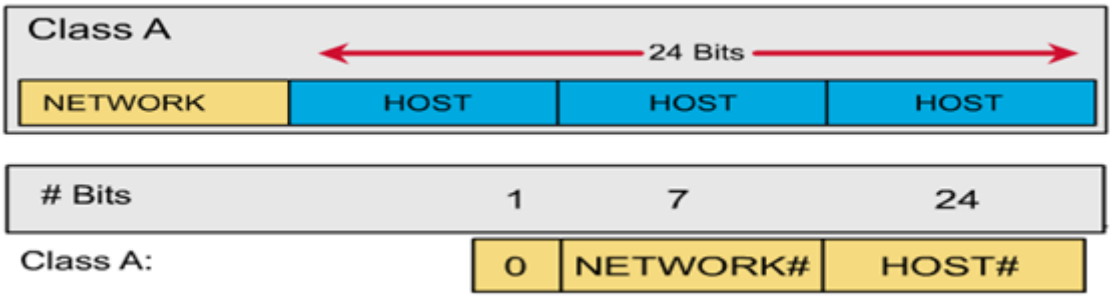
11000000.10101000.00000001.00000001

Một địa chỉ IP gồm hai phần: Phần địa chỉ mạng (NetID) và phần địa chỉ host (Host ID). Tùy thuộc vào từng lớp mạng, phần địa chỉ mạng bao gồm một, hai hay ba octet đầu tiên. Địa chỉ IPv4 được chia thành 5 lớp: A, B, C, D, E, trong đó hiện tại đã dùng hết lớp A, B và gần hết lớp C, còn lớp D và E tổ chức Internet đang để dành cho mục đích khác nên không phân.

Lớp	Octet 1	Octet 2	Octet 3	Octet 4
A	Networks (1-127)	Host (0-255)	Host (0-255)	Host (0-255)
B	Networks (128-191)	Networks (0-255)	Host (0-255)	Host (0-255)
C	Networks (192-223)	Networks (0-255)	Networks (0-255)	Host (0-255)

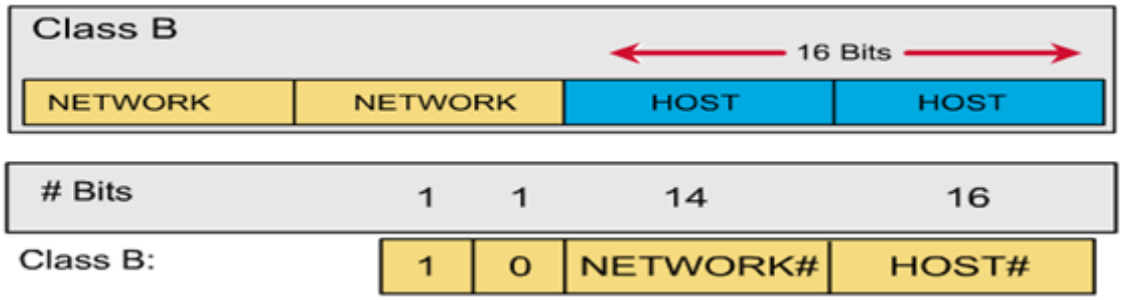
Bảng 1.2: Phân chia địa chỉ mạng và địa chỉ host trong từng lớp mạng.

- Địa chỉ IP của mạng lớp A:
  + Bit đầu tiên của lớp A luôn là 0, dùng octet đầu làm NetID.
  + Dùng 3 octet còn lại cho HostID.
  + Dãy địa chỉ mạng có bắt đầu từ 1.0.0.0 đến 127.0.0.0.
  + Mỗi Network ở lớp A có 16777214 địa chỉ host.
  + Các mạng có địa chỉ mạng là 127 thuộc khoảng địa chỉ dự phòng. Địa chỉ 127.0.0.1 là địa chỉ localhost, địa chỉ 127.0.0.0 là địa chỉ looback.



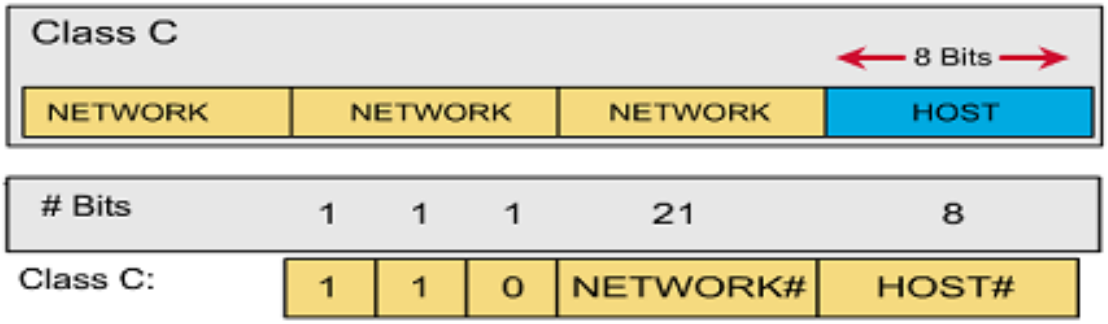
Hình 1.15: Cấu trúc địa chỉ IPv4 lớp A

- Địa chỉ IP mạng của lớp B:
  + Hai bit đầu của lớp B luôn là 10, dùng 2 octet đầu làm NetID.
  + Dãy địa chỉ mạng có thể bắt đầu từ 128.0.0.0 đến 191.255.0.0.
  + Sử dụng 2 octect còn lại làm HostID.
  + Mỗi Network ở lớp B có 65534 địa chỉ host.
  + Default Netmask là 255.255.0.0.



Hình 1.16: Cấu trúc địa chỉ IPv4 lớp B

- Địa chỉ IP của mạng lớp C:
  + Ba bit đầu tiên của lớp B luôn là 110, dùng 3 octet đầu làm NetID.
  + Dãy địa chỉ mạng có thể bắt đầu từ 192.0.0.0 đến 223.255.255.0.
  + Sử dụng 1 octet cuối làm phần HostID.
  + Mỗi Network ở lớp C có 254 địa chỉ host



Hình 1.17: Cấu trúc địa chỉ IPv4 lớp C

- Một số địa chỉ đặc biệt:
  + Địa chỉ mạng: là địa chỉ mà HostID chỉ chứa toàn bit 0.

    Ví dụ: 192.168.1.0
  + Địa chỉ host: là địa chỉ mà phần HostID tồn tài cả bit 0 và 1.

    Ví dụ: 192.168.1.25

+ Địa chỉ netmask (mặt nạ mạng): là địa chỉ mà bit ở phần NetID toàn là bit 1 và bit ở phần HostID toàn là bit 0.

  Ví dụ: 255.255.255.0.

+ Địa chỉ broadcast: là địa chỉ mà phần HostID chứa toàn bit 1.

  Ví dụ: 192.168.1.255.

+ Địa chỉ mạng sử cho mạng riêng (mạng nội bộ, không sử dụng làm địa chỉ internet).
  - Lớp A: 10.0.0.0
  - Lớp B: 172.16.0.0 ÷ 172.31.255.255
  - Lớp C: 192.168.0.0 ÷ 192.168.255.255

+ Mặt nạ mặc định (Default Mask) là giá trị thập phân cao nhất (khi các bit đều bằng 1) trong các octet dành cho địa chỉ mạng – NetID và được đặt trước cho từng lớp địa chỉ A, B, C. Mặt nạ mặc định: Lớp A: 255.0.0.0; Lớp B: 255.255.0.0; Lớp B: 255.255.255.0.

1.3.1.1.2 IPv6 – Internet Protocol version 6

Hiện nay do sự phát triển của mạng và các dịch vụ Internet nhu cầu về số địa chỉ IP tăng cao mà IPv4 không thể đáp ứng đủ. Phiên bản địa chỉ Internet mới IPv6 được thiết kế để thay thế cho phiên bản IPv4.

Địa chỉ IPv6 có chiều dài 128 bit, biểu diễn dưới dạng các cụm số hexa phân cách bởi dấu **::**, ví dụ: 2001**::**0DC8**::**1005**::**2F43**::**0BCD**::**FFFF.

Với 128 bít chiều dài, không gian địa chỉ IPv6 gồm 2^{128} địa chỉ, cung cấp một lượng địa chỉ khổng lồ cho hoạt động Internet.

IPv6 có các đặc điểm sau: Không gian địa chỉ gần như vô hạn, khả năng tự động cấu hình (Plug and Play), khả năng bảo mật kết nối từ thiết bị gửi đến thiết bị nhận, quản lý định tuyến tốt hơn, dễ dàng thực hiện Multicast, hỗ trợ cho quản lý chất lượng mạng.

1.3.1.2 Transmission Control Protocol – TCP

Giao thức TCP giao thức truyền dữ liệu hướng liên kết có thể sử dụng truyền dữ liệu với độ tin cậy cao. Trong đó giao thức tầng giao vận có thể gửi các xác thực rằng đã nhận dữ liệu và yêu cầu truyền lại dữ liệu nếu chưa nhận được dữ liệu hoặc dữ liệu bị hỏng.

Cấu trúc của một TCP header:

Trường	Độ dài	Mô tả
Cổng nguồn (Source port)	2 bytes	Số hiệu cổng của nguồn
Cổng đích (Destination port)	2 bytes	Số hiệu cổng đích
Số thứ tự (Sequence Number)	4 bytes	Số thứ tự được tạo ra bởi nguồn và được sử dụng bởi đích để sắp xếp lại các gói tin để tạo ra thông điệp ban đầu, và gửi xác thực tới nguồn.
Acknowledge Number	4 bytes	
Data offset	4 bits	Các chi tiết về nơi dữ liệu gói tin bắt đầu
Reserved	6 bit	Dự phòng
Control		
Window Size	2 bytes	Trường này chỉ ra kích thước của vùng đệm nhận. Phía nhận có thể thông báo cho phía gửi kích thước dữ liệu tối đa mà có thể được gửi đi bằng cách sử dụng các thông điệp xác thực
Checksum	2 bytes	Checksum cho header và dữ liệu để xác định xem gói tin có bị hỏng không
Urgent Pointer	2 bytes	Trường này thông báo cho phía nhận biết có dữ liệu khẩn
Options		
Padding		

Bảng 1.3: Mô tả chi tiết chức năng của các trường trong TCP header

Giao thức TCP là một giao thức phức tạp và mất thời gian do cơ chế bắt tay, nhưng giao thức này đảm bảo các gói tin đến đúng đích.

Một số giao thức ứng dụng sử dụng TCP như HTTP, FTP, SMTP, và Telnet. TCP yêu cầu một liên kết phải được thiết lập trước khi dữ liệu được gửi đi. Ứng dụng server phải thực hiện một thao tác mở thụ động để tạo một liên kết với một số hiệu cổng cho trước.

1.3.1.3 User Datagram Protocol – UDP

Giao thức UDP là giao thức truyền dữ liệu phi liên kết có thể sử dụng truyền dữ liệu với độ tin cậy thấp. UDP không cần giai đoạn thiết lập liên kết, dữ liệu được gửi đi ngay khi cần. UDP không gửi các thông điệp xác thực, vì vậy dữ liệu có thể nhận được hoặc bị thất lạc.

Cấu trúc của UDP header được thể hiện trong bảng :

Trường thông tin	Độ dài	Mô tả
Source port (Cổng nguồn)	2 byte	Xác định cổng nguồn là một tùy chọn với UDP. Nếu trường này được sử dụng, phía nhận thông điệp có thể gửi một phúc đáp tới cổng này
Destination Port	2 byte	Số hiệu cổng đích
Length	2 byte	Chiều dài của thông điệp bao gồm header và dữ liệu
Checksum	2 byte	Để kiểm tra tính đúng đắn

Bảng 1.4: Cấu trúc của UDP header.

1.3.1.4 Số hiệu cổng (Port number)

Số hiệu cổng (Port number) được các giao thức TCP hay UDP dùng để định danh các ứng dụng. Các số hiệu cổng của TCP và UDP được phân ra thành:

+ Các số hiệu cổng hệ thống (trong khoảng từ 0 đến 1023).
+ Các số hiệu cổng người dùng (trong khoảng từ 1024 đến 49151).
+ Các số hiệu cổng riêng và động (trong khoảng từ 49152 đến 65535).

1.3.1.5 Socket

Socket là một phương pháp để thiết lập kết nối truyền thông giữa một chương trình yêu cầu dịch vụ và một chương trình cung cấp dịch vụ trên mạng LAN, WAN, hay Internet và đôi khi là giữa các tiến trình trong cùng một máy tính. Thông tin của một Socket bao gồm địa chỉ IP và số hiệu cổng.

1.3.1.6 Internet Control Message Protocol – ICMP

ICMP là một giao thức được phát triển từ giao thức IP, các thông tin phản hồi về trạng thái của hệ thống được ICMP phản hồi bởi các thông điệp.

Các lỗi được phát hiện có thể được thông báo bằng các thông điệp ICMP. Các thông điệp ICMP được sử dụng để gửi các thông tin phản hồi về tình trạng của mạng. Ví dụ, một router gửi thông điệp ICMP "destination unreachable" nếu không tìm thấy một điểm vào cho mạng trong bảng định tuyến. Một router cũng có thể gửi thông điệp ICMP "redirect" nếu tìm thấy đường đi tốt hơn.

ICMP không có trên giao thức IP mà được gửi đi trong các IP header.

Trường thông tin	Độ dài	Mô tả
Type	1 byte	Trường này xác định kiểu thông điệp ICMP. Ví dụ: type có giá trị 3 nghĩa là không đến được đích, 11 nghĩa là quá thời gian, và 12 nghĩa là các tham số header không đúng
Code	1 byte	Code cung cấp thông tin về kiểu thông điệp. Nếu kiểu type là 3, "destination unreachable", thì code xác định là mạng (0), host (1), hay protocol (2), hoặc port (3) là không thể đến được
Checksum	2 bytes	Checksum của thông điệp ICMP
	4 bytes	Bốn byte cuối cùng của header ICMP có thể cung cấp thông tin bổ trợ tùy thuộc vào kiểu thông điệp
Header IP thông thường	…	

Bảng 1.5: Cấu trúc của gói tin ICMP

1.3.1.7 Internet Group Management Protocol – IGMP

Tương tự với ICMP, IGMP là sự mở rộng của giao thức IP và phải được cài đặt trong module IP. IGMP được sử dụng bởi các ứng dụng multicast.

Các thông điệp IGMP được gửi bên trong gói tin IP với trường protocol number bằng 2, trong đó trường TTL có giá trị bằng 1. Các gói IGMP chỉ được truyền trong LAN và không được tiếp tục chuyển sang LAN khác do giá trị TTL của nó.

Chức năng của IGMP là:

+ Thông báo cho router multicast rằng có một máy muốn nhận multicast traffic của một nhóm cụ thể.

+ Thông báo cho router rằng một có một máy muốn rời một nhóm multicast (nói cách khác, có một máy không còn quan tâm đến việc nhận multicast traffic nữa). Các router thường dùng IGMP để duy trì thông tin cho từng cổng của router là những nhóm multicast nào router cần phải chuyển và những host nào muốn nhận.

1.3.2 Các giao thức Internet.

1.3.2.1 File Transfer Protocol – FTP

FTP được sử dụng để tải các tập tin lên server, và tải về các tập tin từ server. Nó là một giao thức mức ứng dụng, dựa trên nền tảng của giao thức TCP. Ứng dụng client cung cấp một giao diện người dùng và tạo ra một yêu cầu FTP tương ứng với yêu cầu của người dùng cùng với đặc tả của FTP. Lệnh FTP được gửi tới ứng dụng server thông qua giao thức TCP/IP, trình thông dịch trên FTP phải thông dịch lệnh FTP tương ứng. Tùy thuộc vào lệnh FTP, một danh sách các tập tin hoặc một tập tin từ hệ thống tệp của server được trả về cho client trong đáp ứng của FTP.

Giao thức FTP có các đặc trung sau:

- Truyền dữ liệu với độ tin cậy cao thông qua giao thức TCP.
- Cho phép truy xuất vô danh hoặc xác thực người dùng với username và password.
- Các tệp tin được truyền đi dưới dạng mã ASCII hoặc dữ liệu nhị phân.

1.3.2.2 Hypertext Transfer Protocol – HTTP

HTTP là một giao thức được sử dụng bởi các ứng dụng web. HTTP là một giao thức có độ tin cậy cao, được cài đặt dựa trên nền giao thức TCP. Tương tự như FTP, HTTP cũng được sử dụng để truyền các tệp tin qua mạng, nhưng nó có các đặc trưng như : đệm dữ liệu, định danh các ứng dụng client, hỗ trợ cho các

định dạng kèm theo khác, như MIME,… Những đặc trưng này có trong header HTTP.

1.3.2.3 Hypertext Transfer Protocol Secure – HTTPS

HTTPS là một sự kết hợp giữa giao thức HTTP và giao thức bảo mật SSL (Secure Socket Layer) hay TLS (Transport Layer Security) cho phép trao đổi thông tin một cách bảo mật trên Internet. Giao thức HTTPS thường được dùng trong các giao dịch nhạy cảm cần tính bảo mật cao.

SSL và TLS nằm ở tầng trên của giao thức TCP, chúng có nhiệm vụ mã hóa dữ liệu được truyền trên mạng bằng phương pháp mã hóa công khai, vì vậy có thể bảo mật được dữ liệu truyền trên mạng.

1.3.3 Các giao thức E-mail

Hiện nay các giao thức phổ biến sử dụng cho e-mail như sau:

- SMTP – Simple Mail Transfer Protocol

SMTP là một giao thức để gửi và nhận các e-mail. Nó có thể được sử dụng để gửi e-mail giữa client và server sử dụng cùng giao thức giao vận, hoặc để gửi e-mail giữa các server sử dụng các giao thức giao vận khác nhau. SMTP có khả năng chuyển tiếp các thông điệp thông qua các môi trường dịch vụ giao vận. SMTP không cho phép chúng ta đọc các thông điệp từ một mail server.

- POP3 – Post Office Protocol version 3

POP3 được thiết kế cho các môi trường không được liên kết. Trong các môi trường không duy trì liên kết thường trực với mail server, ví dụ: trong các môi trường trong đó thời gian liên kết lâu.

Với POP3, client có thể truy xuất tới server và tìm kiếm các thông điệp mà server hiện đang nắm giữ. Khi các thông điệp được tìm kiếm từ client, chúng thường bị xóa khỏi server, mặc dù điều này là không cần thiết.

- IMAP – Internet Message Access Protocol

Giống như POP3, IMAP được thiết kế để truy xuất tới các mail trên một mail server. Tương tự như các client POP3, một client IMAP có thể có chế độ offline nhưng các client IMAP có các khả năng lớn hơn trên chế độ online như: tìm kiếm các header, các đoạn mail, tìm kiếm các thông điệp cụ thể trên các server, và thiết lập các cờ như cờ trả lời. Về căn bản, IMAP cho phép các client làm việc trên các hộp thư ở xa như là các hộp thư cục bộ.

- NNTP – Network News Transfer Protocol

NNTP là giao thức tầng ứng dụng để gửi, chuyển tiếp, và tìm kiếm các thông điệp tạo nên một phần của các cuộc thảo luận nhóm tin. Giao thức này cung cấp khả năng truy cập tới một server tin tức để tìm kiếm các thông điệp có chọn lọc và hỗ trợ cho việc truyền thông điệp từ server tới server.

1.3.4 Các giao thức khác

1.3.4.1 SNMP (Simple Network Management Protocol)

SNMP là giao thức cho phép quản lý các thiết bị. Dựa trên mạng dựa vào các biến đếm hiệu năng từ các thiết bị, SNMP quản lý các thiết bị một cách hiệu quả bằng cách sử dụng các chuông báo hiệu được kích hoạt bởi các vấn đề về hiệu năng và lỗi, và cho phép cấu hình các thiết bị.

Một tác tử SNMP được gắn với một thiết bị mạng cụ thể sẽ có một cơ sở dữ liệu MIB (Management Information Base) bao gồm tất cả các thông tin có thể kiểm soát về thiết bị đó theo phương pháp hướng đối tượng. Một client SNMP truy xuất thông tin trong cơ sở dữ liệu bằng cách gửi các yêu cầu GET. Ngược lại, yêu cầu SET được sử dụng để cấu hình cơ sở dữ liệu MIB.

Trong những trường hợp có lỗi hoặc có các vấn đề về hiệu năng, tác tử SNMP gửi các thông điệp tới SNMP client.

1.3.4.2 TELNET (Terminal Network)

TELNET là một giao thức mạng – trên cổng 23, được sử dụng trên mạng Internet hoặc mạng nội bộ để cung cấp một thông tin liên lạc hai chiều, tương tác dòng lệnh theo định hướng cơ sở sử dụng để kết nối thiết bị đầu cuối ảo.

TELNET cho phép hai hệ điều hành khác nhau có thể truy cập đến một chương trình ứng dụng trên máy tính ở xa để truy cập thông tin, thực thi các chương trình và sử dụng một số tài nguyên khác.

1.4 Internet

1.4.1 Intranet và Extranet

Một Intranet có thể sử dụng các công nghệ TCP/IP tương tự như với Internet. Sự khác biệt là intranet là một mạng riêng, trong đó tất cả mọi người đều biết nhau. Intranet không phục vụ cho việc truy xuất chung, và một số dữ liệu cần phải được bảo vệ khỏi những truy xuất từ bên ngoài.

Một Extranet là một mạng riêng giống như Intranet nhưng các Extranet kết nối nhiều Intranet thuộc cùng một công ty hoặc các công ty đối tác thông qua Internet bằng cách sử dụng một tunnel. Việc tạo ra một mạng riêng ảo trên Internet tiết kiệm chi phí nhiều cho công ty so với việc thuê riêng một đường truyền để thiết lập mạng.

1.4.2 Firewall

Có những kẻ phá hoại trên mạng Internet!. Để ngăn chặn chúng, người ta thường thiết lập các điểm truy cập tới một mạng cục bộ và kiểm tra tất cả các luồng truyền tin vào và ra khỏi điểm truy nhập đó. Phần cứng và phần mềm giữa mạng Internet và mạng cục bộ, kiểm tra tất cả dữ liệu vào và ra, được gọi là firewall.

Firewall đơn giản nhất là một bộ lọc gói tin kiểm tra từng gói tin vào và ra khỏi mạng, và sử dụng một tập hợp các quy tắc để kiểm tra xem luồng truyền tin

có được phép vào ra khỏi mạng hay không. Kỹ thuật lọc gói tin thường dựa trên các địa chỉ mạng và các số hiệu cổng.

1.4.3 Proxy

Khái niệm proxy có liên quan đến firewall. Nếu một firewall ngăn chặn các host trên mạng liên kết trực tiếp với thế giới bên ngoài. Một máy bị ngăn kết nối với thế giới bên ngoài bởi một firewall sẽ yêu cầu truy xuất tới một trang web từ một proxy server cục bộ, thay vì yêu cầu một trang web trực tiếp từ web server ở xa. Proxy server sau đó sẽ yêu cầu trang web từ một web server, và sau đó chuyển kết quả trở lại cho bên yêu cầu ban đầu. Các proxies cũng được sử dụng cho FTP và các dịch vụ khác. Một trong những ưu điểm bảo mật của việc sử dụng proxy server là các host bên ngoài chỉ nhìn thấy proxy server. Chúng không biết được các tên và các địa chỉ IP của các máy bên trong, vì vậy khó có thể đột nhập vào các hệ thống bên trong.

Trong khi các firewall hoạt động ở tầng giao vận và tầng internet, các proxy server hoạt động ở tầng ứng dụng. Một proxy server có những hiểu biết chi tiết về một số giao thức mức ứng dụng, như HTTP và FTP. Các gói tin đi qua proxy server có thể được kiểm tra để đảm bảo rằng chúng chứa các dữ liệu thích hợp cho kiểu gói tin. Ví dụ, các gói tin FTP chứa các dữ liệu của dịch vụ telnet sẽ bị loại bỏ.

Vì tất cả các truy nhập tới Internet được chuyển hướng thông qua proxy server, vì thế việc truy xuất có thể được kiểm soát chặt chẽ. Ví dụ, một công ty có thể chọn giải pháp phong tỏa việc truy xuất tới www.playboy.com nhưng cho phép truy xuất tới www.microsoft.com.

CHƯƠNG 2: HÌNH VÀ MỘT SỐ DỊCH VỤ MẠNG THƯỜNG SỬ DỤNG TRÊN WINDOWS

2.1 Giới thiệu

Hầu hết các mạng máy tính hiện nay được thiết kế rất đa dạng và đang thực hiện những ứng dụng trên nhiều lĩnh vực của đời sống xã hội. Điều đó có nghĩa là các thông tin lưu trữ trên mạng và các thông tin truyền giao trên mạng ngày càng mang nhiều giá trị có ý nghĩa sống còn. Do vậy những người quản trị mạng ngày càng phải quan tâm đến việc bảo vệ các tài nguyên của mình.

Việc bảo vệ an toàn là quá trình bảo vệ mạng khỏi bị xâm nhập hoặc mất mát, khi thiết kế các hệ điều hành mạng người ta phải xây dựng một hệ thống quản lý nhiều tầng và linh hoạt giúp cho người quản trị mạng có thể thực hiện những phương án về quản lý từ đơn giản mức độ thấp cho đến phức tạp mức độ cao trong những mạng có nhiều người tham gia. Thông qua những công cụ quản trị đã được xây dựng sẵn người quản trị có thể xây dựng những cơ chế về an toàn phù hợp với cơ quan của mình.

Thông thường hệ thống mạng có những mức quản lý chính sau:

- Mức quản lý việc thâm nhập mạng (Login/Password): có nhiệm vụ xác định những ai và lúc nào có thể vào mạng. Đối với người quản trị và người sử dụng mạng, mức an toàn này dường như khá đơn giản mà theo đó mỗi người sử dụng (người sử dụng) có một tên login và mật khẩu duy nhất.
- Mức quản lý trong việc quản lý sử dụng các tài nguyên của mạng: Kiểm soát những tài nguyên nào mà người sử dụng được phép truy cập, sử dụng và sử dụng như thế nào.

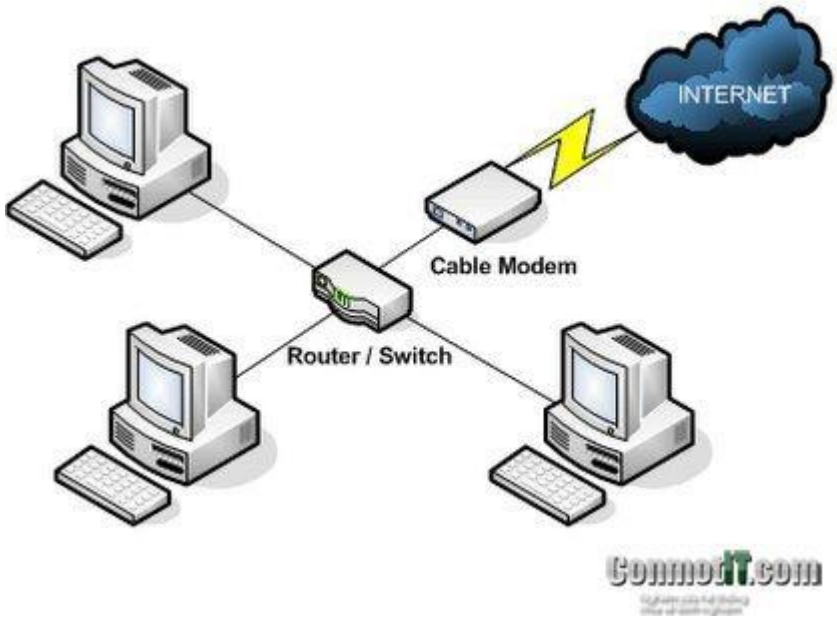
- Mức quản lý với thư mục và file: Mức an toàn của file kiểm soát những file và thư mục nào người sử dụng được dùng trên mạng và được sử dụng ở mức độ nào.
- Mức quản lý việc điều khiển File Server: Mức an toàn trên máy chủ kiểm soát ai có thể được thực hiện các thao tác trên máy chủ như bật, tắt, chạy các chương trình khác… Người ta cần có cơ chế như mật khẩu để bảo vệ.

2.2 Các mô hình mạng trong Windows

Mạng LAN cung cấp các dịch vụ theo hai cách: qua cách chia sẻ tài nguyên theo nguyên tắc ngang hàng và thông qua những máy chủ trung tâm. Dù bất cứ phương pháp nào được sử dụng, vấn đề cần phải giải quyết là là giúp người sử dụng xác định được các tài nguyên có sẵn ở đâu để có thể sử dụng. Trong đó, một số mô hình thường sử dụng trong hệ thống Windows: Workgroup, Domain, mô hình kết hợp.

2.2.1 Mô hình Workgroup

Trong mô hình này, các máy tính làm việc dựa trên nguyên tắc mạng ngang hàng (Peer – to – Peer network), các người sử dụng chia sẻ tài nguyên trên máy tính của mình với những người khác, máy nào cũng vừa là chủ (server) vừa là khách (client). Người sử dụng có thể cho phép các người sử dụng khác sử dụng tập tin, máy in, modem... của mình, và đến lượt mình có thể sử dụng các tài nguyên được các người sử dụng khác chia sẻ trên mạng. Mỗi cá nhân người sử dụng quản lý việc chia sẻ tài nguyên trên máy của mình bằng cách xác định cái gì sẽ được chia sẻ và ai sẽ có quyền truy cập. Mạng này hoạt động đơn giản: sau khi logon vào, người sử dụng có thể duyệt (browse) để tìm các tài nguyên có sẵn trên mạng.



Hình 2.1: Mô hình mạng Workgroup

Workgroup là nhóm logic các máy tính và các tài nguyên của chúng nối với nhau trên mạng mà các máy tính trong cùng một nhóm có thể cung cấp tài nguyên cho nhau. Mỗi máy tính trong một workgroup duy trì chính sách bảo mật và CSDL quản lý tài khoản bảo mật SAM (Security Account Manager) riêng ở mỗi máy. Do đó quản trị workgroup bao gồm việc quản trị CSDL tài khoản bảo mật trên mỗi máy tính một cách riêng lẻ, mang tính cục bộ, phân tán. Điều này rõ ràng rất phiền phức và có thể không thể làm được đối với một mạng rất lớn.

2.2.1.1 Đặc điểm

Mỗi người truy cập vào mạng Windows tổ chức theo mô hình Workgroup cần phải đăng ký: tên vào mạng và mật khẩu vào mạng.

Dựa vào tên và mật khẩu đã cho, Windows cung cấp cho người một số gọi là mã số của người sử dụng (user account). Mã số này được lưu dữ trong cơ sở dữ liệu là hệ thống quản trị tài nguyên (SAM - Security Account Manager database). Hệ thống quản trị tài nguyên dùng để đảm bảo an toàn về tài nguyên trên mạng. Người vào mạng muốn truy nhập vào tài nguyên phải qua sự kiểm

duyệt của hệ thống quản trị tài nguyên. Trong mô hình Workgroup mỗi máy trạm có một nguồn tài nguyên tương ứng với một hệ thống quản trị tài nguyên bảo vệ nó.

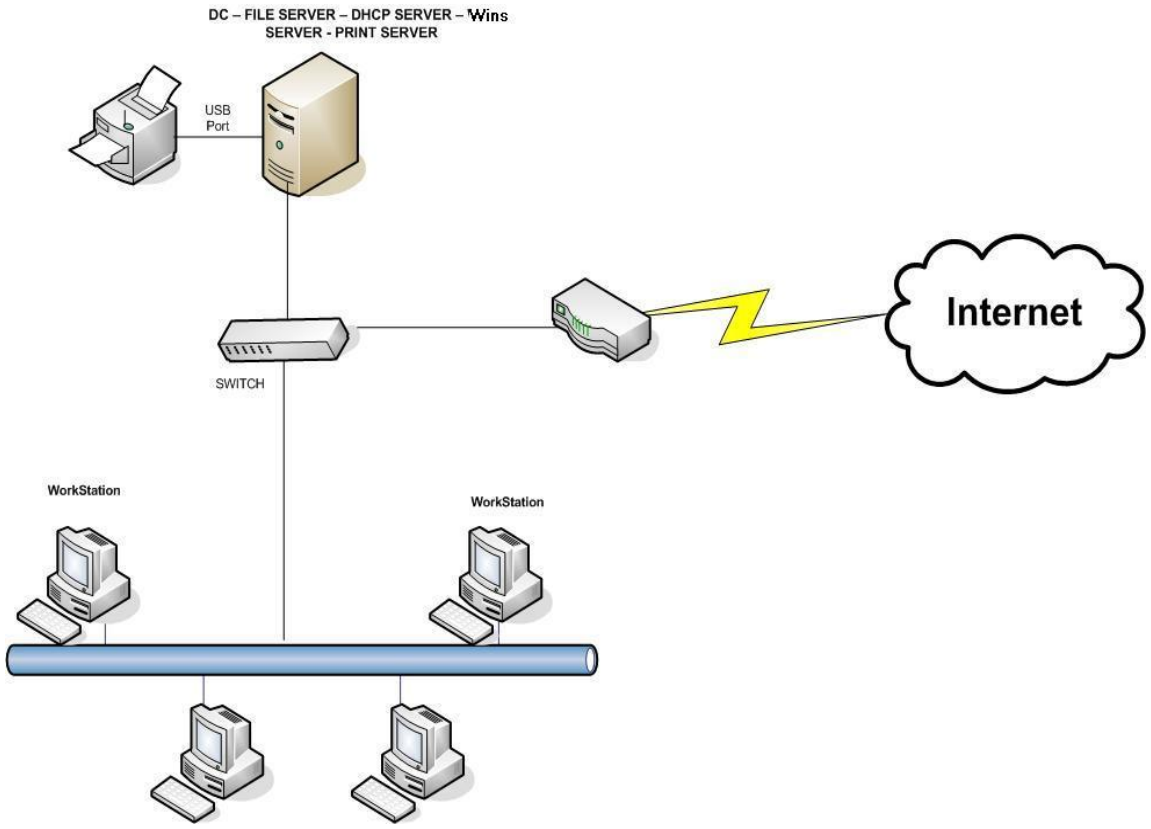
2.2.1.2 Nhận xét

Trong quá trình hoạt động, với nguyên lý hoạt động của mình thì mô hình Workgroup bộc lộ nhiều ưu và nhược điểm:

* Ưu điểm:
  - Đơn giản, tiện lợi, dễ quản lý.
  - Chi phí đầu tư thấp.
  - Chia sẻ tài nguyên hiệu quả.
* Ưu điểm:
  - Bảo mật kém.
  - Đối với mạng lớn, lượng tài nguyên có sẵn trong mạng lớn thì người dùng khó xác định được chúng để khai thác.

2.2.2 Mô hình Domain

Domain được xây dựng dựa trên sự hoạt động của thư mục và nhóm làm việc. Tương tự như workgroup, Domain có thể được quản trị bằng hỗn hợp các biện pháp quản lý tập trung và cục bộ. Domain là một tập hợp các máy tính dùng chung một nguyên tắc bảo mật và CSDL tài khoản người dùng (user account). Những tài khoản người dùng và nguyên tắc an toàn có thể được nhìn thấy khi thuộc vào một CSDL chung và được tập trung.



Hình 2.2: Mô hình mạng hoạt động theo Domain

Tương tự như một thư mục, một Domain tổ chức tài nguyên của một vài máy chủ vào một cơ cấu quản trị. Người sử dụng được cấp quyền logon vào Domain chứ không phải vào từng máy chủ riêng lẻ. Ngoài ra, vì Domain điều khiển tài nguyên của một số máy chủ, nên việc quản lý các tài khoản của người sử dụng được tập trung và do đó trở nên dễ dàng hơn là phải quản lý một mạng với nhiều máy chủ độc lập.

Các máy chủ trong một Domain cung cấp dịch vụ cho các người sử dụng. Một người sử dụng khi logon vào Domain thì có thể truy cập đến tất cả tài nguyên thuộc Domain mà họ được cấp quyền truy cập. Họ có thể dò tìm (browse) các tài nguyên của Domain giống như trong một workgroup, nhưng nó an toàn, bảo mật hơn.

Để xây dựng mạng dựa trên Domain, ta phải có ít nhất một máy Windows Server trên mạng. Một máy tính Windows có thể thuộc vào một workgroup hoặc một Domain, nhưng không thể đồng thời thuộc cả hai. Mô hình Domain được thiết lập cho các mạng lớn với khả năng kết nối các mạng toàn xí nghiệp hay liên kết các kết nối mạng với các mạng khác và những công cụ cần thiết để điều hành.

Việc nhóm những người sử dụng mạng và tài nguyên trên mạng thành Domain có lợi ích sau:

- Quản lý chặt chẽ hơn :
- Khai thác tài nguyên dễ dàng hơn;

2.2.2.1 Đặc điểm

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau: tên Domain, tên người sử dụng và mật khẩu.

Các thông tin này được lưu ở máy chủ dưới dạng một mã số, gọi là tài khoản người sử dụng (user account) và các mã số cũa người sử dụng trong một Domain được tổ chức thành một cơ sở dữ liệu trên máy chủ. Khi người sử dụng muốn truy nhập vào một Domain người đó phải chọn tên Domain trong hộp thoại trên máy trạm. Máy trạm sẽ chuyển các thông tin về hệ thống quản trị tài nguyên (SAM - Security Account Manager database) của Domain để kiểm tra. Khi đó hệ thống quản trị tài nguyên trên máy chủ sẽ kiểm tra các thông tin này, nếu kết quả kiểm tra là đúng, người khai thác mới được quyền truy nhập vào tài nguyên của Domain.

- Máy trạm chỉ có thể cung cấp các mã số được tạo ra trên nó. Nếu máy này bị hư hỏng thì những người khai thác mạng không thể truy nhập bằng mã số của họ. Nếu máy này nằm trong một Domain nào đó thì các mã số này còn được lưu trong SAM của một Domain trên máy chủ.

* Sử dụng máy trạm không tham gia vào Domain, người khai thác mạng không thể truy nhập vào tài nguyên của Domain, mặc dù mã số của của người này có trong SAM của Domain.

Trong một Domain thường có các loại máy thực hiện những công việc sau:

* Primary Domain Controller (PDC), bao giờ cũng phải có để quản trị hệ thống các người sử dụng và các tài khoản trong Domain (hệ thống này gọi là cơ sở dữ liệu SAM - Security Account Manager của Domain). SAM trên máy chủ được thiết kế như hệ thống kiểm soát Domain. Trong một Domain chỉ có duy nhất một PDC.
* Backup Domain Controller (BDC). Trong một Domain có thể có một hoặc nhiều BDC. Các BDC có thể dùng thay thế cho máy PDC trong trường hợp cần thiết, chẳng hạn máy PDC bị hư. Người quản trị Domain chỉ cần tạo tài khoản người sử dụng (user account) chỉ một lần trên máy Primary Domain Controller, thông tin được tự dộng copy đến các máy Backup Domain Controller.

2.2.2.2 Nhận xét

Với những đặc điểm trên thì trong quá trinh hoạt động mô hinh Domain cho thấy nhiều ưu điểm nhưng bên cạnh đó nó cũng tồn tại nhiều nhược điểm chưa khắc phục được.

* Ưu điểm:
  - Quản trị toàn bộ mạng theo cơ chế tập trung.
  - Cung cấp khả năng dự phòng và tự động chuyển đổi dự phòng.
  - Truy cập tài nguyên dễ dàng, bảo mật cao.
  - Quản lý chặt chẽ hệ thống máy trạm.
  - Luôn sẵn sàng cho các dịch vụ mới.

* Nhược điểm:
  - Đòi hỏi phải bổ sung nhân lực trong quản trị hệ thống mạng.
  - Khó cài đặt.
  - Trang thiết bị cần được đầu tư (tối thiểu cần 03 máy chủ, cùng với mỗi phòng máy 01 máy tính được ủy quyền quản lý. Thiết bị lưu trữ tập chung khoảng 03 TB).

2.2.3 Mô hình kết hợp

Mô hình Workgroup và Domain là hai mô hình quan trọng của Windows nhưng trong quá trình triển khai trong thực tế thì việc kết hợp giữa hai mô hình này sẽ áp dụng các đối tượng có nhu cầu bảo mật khác nhau.

Ví dụ như các phòng thực hành thì không cần có chế độ bảo mật cao nên chỉ cần dùng mô hình Workgroup. Còn đối với các phòng ban cần có chế độ bảo mật cao hơn như các phòng làm việc liên quan đến cơ sở dữ liệu, hay thiết kế các dự án thì sử dụng mô hình Domain

2.3 Một số dịch vụ thường sử dụng.

Là hệ điều hành mạng cho phép tổ chức quản lý một cách chủ động theo nhiều mô hình khác nhau: Peer – to – Peer, clien/server. Nó thích hợp với tất cả các kiến trúc mạng hiện nay như: hình sao (star), đường thẳng (bus), vòng (ring) và phức hợp. Nó có một số đặc tính ưu việt bảo đảm thực hiện cùng lúc nhiều chương trình mà không bị lỗi. Bản thân Windows NT đáp ứng được hầu hết các giao thức phổ biến nhất trên mạng và cũng hỗ trợ được rất nhiều những dịch vụ truyền thông trên mạng. Nó vừa đáp ứng được cho mạng cục bộ (LAN) và cho cả mạng diện rộng (WAN).

Windows NT cho phép dùng giao thức TCP/IP, vốn là một giao thức được sử dụng rất phổ biến trên hầu hết các mạng diện rộng và trên Internet. Giao thức TCP/IP dùng tốt cho nhiều dịch vụ mạng trên môi trường Windows NT.

Trong thực tế có một số dịch vụ có thể chạy song song với cùng chức năng trong cả hai mô hình Workgroup va Domain. Các dịch vụ chạy trên cả hai mô hình đó là các dịch vụ quản lý dữ liệu, file, web, mail, DHCP, DNS,…

2.3.1 Quản lý khai thác dữ liệu

Để quản lý và khai thác dữ liệu trong hệ thống mạng, Windows NT cung cấp một cơ chế quản lý và phương thức khai thác. Trước khi được người dùng khai thác thì các tài nguyên phải được khai báo trước, và cung cấp cho người dùng quyền sử dụng phù hợp.

Khi một người sử dụng muốn truy cập một tập tin thì tất cả các thông tin về phương thức phục hồi giao dịch và phục hồi giao dịch khi bị lỗi sẽ được đăng ký bởi Log File Server. Nếu giao dịch thành công, tập tin đó sẽ truy xuất được, ngược lại giao dịch sẽđược phục hồi. Nếu có lỗi trong quá trình giao dịch, tiến trình giao dịch sẽ kết thúc.

Việc truy xuất tập tin (File hoặc thư mục) được quản lý thông qua các quyền truy cập (right), quyền đó sẽ quyết định ai có thể truy xuất và truy xuất đến tập tin đó với mức độ giới hạn nào. Những Quyền đó là Read, Execute, Delete, Write, Set Permission, Take Ownership.

Trong đó:

- **Read** (**R**): Được đọc dữ liệu, các thuộc tính, chủ quyền của tập tin.
- **Execute** (**X**): Được chạy tập tin.
- **Write** (**W**): Được phép ghi hay thay đổi thuộc tính.
- **Delete** (**D**): Được phép xóa tập tin.
- **Set Permission** (**P**): Được phép thay đổi quyền hạn của tập tin.
- **Take Ownership** (**O**): Được đặt quyền chủ sở hữu của tập tin.

Để chia sẻ file trong mạng thì Windows dùng giao thức File Sharing Protocol, Windows sử dụng giao thức chia sẻ file là CIFS, SMB – giao thức mạng mức cao, cung cấp cấu trúc và ngôn ngữ yêu cầu chia sẻ file giữa client và server. Giao thức này cung cấp các lệnh để mở, đọc, ghi và đóng file qua môi trường mạng và cũng có thể cung cấp truy cập vào các dịch vụ Directory.

2.3.2 Dịch vụ quản lý tập tin – File Services 2008

File Services là một dịch vụ trên hệ thống Windows Server, cung cấp cho người quản trị các kỹ thuật quản lý dung lượng lưu trữ (Storage), cơ chế backup dữ liệu bằng thức tạo bản sao của dữ liệu ở các server khác (replication), quản lý tài nguyên, chia sẻ, hỗ trợ các máy tính *NIX truy cập tài nguyên hệ thống Windows.

Sử dụng dịch vụ File Services giúp:

- Làm giảm số lượng File Server và thuận tiện trong quá trình sử dụng.
- Đồng bộ được dữ liệu.
- Triển khai các dịch vụ sao lưu/phục hồi một cách dễ dàng.

2.3.3 Dịch vụ web – Internet Information Server (IIS)

Internet Information Server (IIS) là một ứng dụng chạy trên Windows NT, tích hợp chặt với Windows NT, khi cài đặt IIS, IIS có đưa thêm vào tiện ích màn hình kiểm soát (Performance monitor) một số mục như thống kê số lượng truy cập, số trang truy cập. Việc kiểm tra người dùng truy cập cũng dựa trên cơ chế quản lý người sử dụng của Windows NT. IIS chạy trên giao thức HTTP.

IIS gồm có các dịch vụ:

- World Wide Web (WWW): là một trong những dịch vụ chính trên Internet cho phép người sử dụng xem thông tin một cách dễ dàng, sinh động. Dữ liệu chuyển giữa Web Server và Web Client thông qua giao thức HTTP (Hypertext Transfer Protocol).

- File Transfer Protocol (FTP): sử dụng giao thức TCP để chuyển file giữa 2 máy và cũng hoạt động theo mô hình Client/Server, khi nhận được yêu cầu từ client, đầu tiên FTP Server sẽ kiểm tra tính hợp lệ của người dùng thông qua tên và mật mã. Nếu hợp lệ, FTP Server sẽ kiểm tra quyền người dùng trên tập tin hay thư mục được xác định trên FTP Server. Nếu hợp lệ và hệ thống file là NTFS thì sẽ có thêm kiểm tra ở mức thư mục, tập tin theo NTFS. Sau khi tất cả hợp lệ, người dùng sẽ được quyền tương ứng trên tập tin, thư mục đó.
- Gopher: là một dịch vụ sử dụng giao diện menu để Gopher Client tìm và chuyển bất kỳ thông tin nào mà Gopher Server đã được cấu hình. Gopher cũng sử dụng kết nối theo giao thức TCP/IP.

2.3.4 Dịch vụ mail – Exchange Server

Trong hệ điều hành Windows, có nhiều phần mềm triển khai và quản lý dịch vụ mail, nhưng hiện nay chủ yếu dùng phần mềm Exchange server.

Ngày nay đối với hầu hết các doanh nghiệp, e-mail là công cụ liên lạc vô cùng quan trọng cho công việc. E-mail cho phép nhân viên tạo ra các kết quả tốt nhất. Sự lệ thuộc ngày càng lớn hơn vào e-mail đã làm tăng số lượng tin nhắn gửi và nhận, tạo ra sự phong phú của công việc phải hoàn thành, và thậm chí tăng tốc độ của chính quá trình kinh doanh. Trong bối cảnh thay đổi như vậy, kỳ vọng của nhân viên ngày càng phát triển. Ngày nay, nhân viên mong muốn có được khả năng truy cập phong phú, hiệu quả – tới email, lịch làm việc, tài liệu gửi kèm, thông tin liên hệ và còn nhiều hơn nữa – cho dù họ đang ở đâu hoặc đang sử dụng thiết bị gì.

Dịch vụ mail hoạt động trên các giao thức : SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), IMAP (Internet Message Access Protocol), NNTP (Network News Transfer Protocol).

Exchange Server là phần mềm của Microsoft chạy trên các máy chủ, cho phép gửi và nhận thư điện tử cũng như các dạng khác thông qua mạng máy tính. Được thiết kế chủ yếu để giao tiếp với Microsoft Outlook nhưng cũng có thể giao tiếp tốt với các phần mềm khác như Outlook Express. Exchange Server được thiết kế cho cả các doanh nghiệp lớn và nhỏ với các ưu điểm nổi trội là dễ quản trị, hỗ trợ nhiều tính năng và có độ tin cậy cao.

Những tính năng nổi bật của hệ thống Exchange server:

- Tích hợp tính năng bảo vệ với các chức năng: chống thư rác, mã hóa các thông điệp ra – vào hệ thống,…
- Truy cập mọi lúc mọi nơi.
- Hỗ trợ toàn bộ những tính năng của Outlook.

2.3.5 Dịch vụ DHCP – Dynamic Host Configuration Protocol.

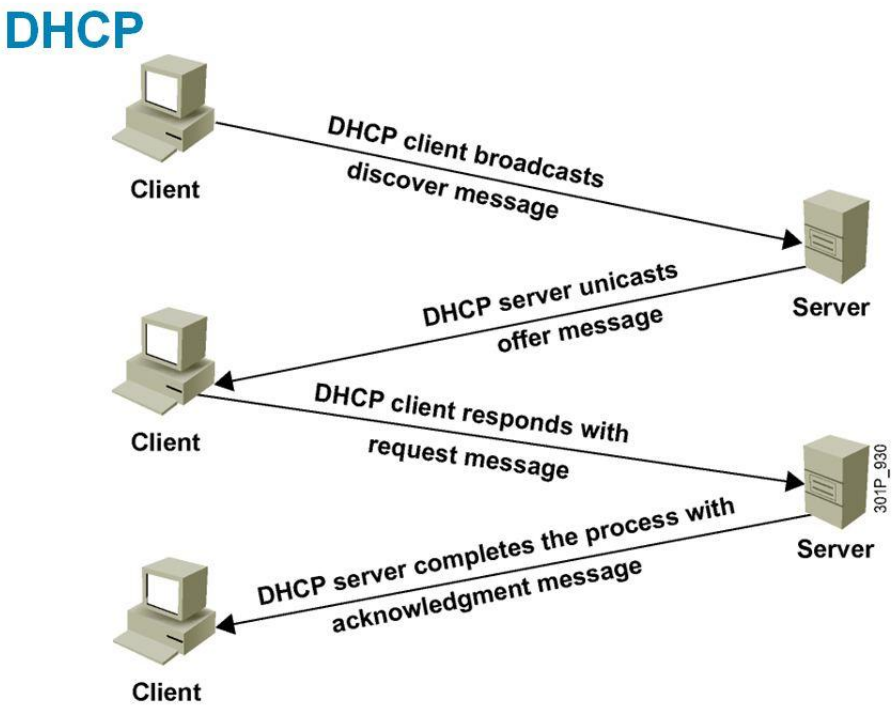
Dynamic Host Configuration Protocol (DHCP) là một giao thức cấu hình tự động địa chỉ IP. Máy tính được cấu hình một cách tự động vì thế sẽ giảm việc can thiệp vào hệ thống mạng. Nó cung cấp một cơ sở dữ liệu (database) trung tâm để theo dõi tất cả các máy tính trong hệ thống mạng. Mục đích quan trọng nhất là tránh trường hợp hai máy tính khác nhau lại có cùng địa chỉ IP.

Trong mạng máy tính NT khi một máy phát ra yêu cầu về các thông tin của TCP/IP thì gọi là DHCP client, còn các máy cung cấp thông tin của TCPIP gọi là DHCP server. Các máy DHCP server bắt buộc phải là Windows NT server.

Cách cấp phát địa chỉ IP trong DHCP: Một user khi logon vào mạng, nó cần xin cấp 1 địa chỉ IP, theo 4 bước sau :

- Gởi thông báo đến tất cả các DHCP server để yêu cầu được cấp địa chỉ.
- Tất cả các DHCP server gởi trả lời địa chỉ sẽ cấp đến cho user đó.

* User chọn 1 địa chỉ trong số các địa chỉ, gửi thông báo đến server có địa chỉ được chọn.
* Server được chọn gởi thông báo khẳng định đến user mà nó cấp địa chỉ.



Hình 2.3: Quá trình cấp phát DHCP

2.3.6 Dịch vụ DNS – Domain Name System.

DNS (Domain Name System) là một hệ cơ sở dữ liệu phân tán dùng để ánh xạ giữa các tên miền và các địa chỉ IP. DNS đưa ra một phương pháp đặc biệt để duy trì và liên kết các ánh xạ này trong một thể thống nhất. Trong phạm vi lớn hơn, các máy tính kết nối với internet sử dụng DNS để tạo địa chỉ liên kết dạng URL (Universal Resource Locators).

Theo phương pháp này, mỗi máy tính sẽ không cần sử dụng địa chỉ IP cho kết nối mà nó sử dụng giao thức UDP, sử dụng cổng 53.

Cấu trúc của DNS gồm các bản ghi sau:

- A (Address): Ánh xạ từ một tên máy (host) sang một địa chỉ IP.
- CNAME: Ánh xạ từ một tên máy (host) sang một tên dịch vụ nào đó.
- MX: Xác định máy trạm chuyển tiếp mail cho một máy (host) nào đó.
- NS (name server): Khai báo máy chủ tên miền cho một tên miền nào đó.
- PTR (Pointer): Ánh xạ từ một tên miền sang một địa chỉ IP và ngược lại.
- SOA (Start of authority): Hiện thị trạng thái thông tin của một tên miền.

CHƯƠNG 3: XÂY DỰNG HỆ THỐNG LƯU TRỮ DỮ LIỆU TẬP TRUNG

3.1 Các giải pháp lưu trữ

Thông tin dưới các dạng như thư điện tử, tài liệu, các bài trình bày, các cơ sở dữ liệu, đồ thị, các tệp dữ liệu ở dạng âm thanh, hình ảnh cũng như các bảng tính là nhân tố quyết định đến sự thành công của phần lớn các công ty. Các ứng dụng để chạy và bảo vệ những dữ liệu của công ty bạn thường đòi hỏi một dung lượng khá lớn "ô nhớ" trong hệ thống các ổ đĩa cứng. Bên cạnh đó, những xu thế và yêu cầu phát triển mới cũng là yếu tố kích thích làm cho các doanh nghiệp luôn cảm thấy " thiếu " dung lượng nhớ cần thiết cho việc lưu trữ dữ liệu của mình và có nhu cầu cấp bách cần phải mở rộng " dung lượng hệ thống lưu trữ dữ liệu".

Hiện nay có rất nhiều phương án lựa chọn phù hợp với các doanh nghiệp cả về phương thức quản lý dữ liệu và địa điểm lưu giữ những dữ liệu đó. Nhưng để lựa chọn được một phương án tốt thì cần phải đánh giá các nhu cầu lưu trữ dữ liệu của mình, các doanh nghiệp cần cần phải xem xét và cân nhắc các khía cạnh như các ứng dụng nào hay sử dụng , các loại hình dữ liệu của mình là gì và cách thức cũng như địa điểm lưu trữ các dữ liệu đó.

Để đánh giá một cách chính xác nhu cầu lưu trữ thì ta cần trả lời các câu hỏi sau:

- Ứng dụng nào sẽ tạo ra các tệp dữ liệu "lớn nhất"?
- Ứng dụng nào chạy trên các hệ thống máy chủ nào?
- Dữ liệu đã có từ bao lâu?
- Dữ liệu 'bị trùng lặp' hoặc đã quá cũ chiếm bao nhiêu?
- Những dữ liệu không liên quan đến hoạt động kinh doanh chiếm bao nhiêu?

- Mức độ "nhanh" hay "chậm" cần phải được đáp ứng khi khai thác dữ liệu?
- Cần khai thác dữ liệu nào và từ đâu?

Sau khi đã nắm được các thông tin liên quan đến nhu cầu lưu trữ của dữ liệu, từ đó có thể lựa chọn các phương án phù hợp. Một số phương pháp lưu trữ có thể áp dụng trong thực tế:

- Các ổ đĩa lưu động.
- Ổ cứng ngoài.
- Lưu trữ trên các hệ thống mạng trực tuyến.
- Lưu trữ trên mạng máy tính.

3.1.1 Lưu trữ trên các ổ đĩa lưu động

Loại ổ đĩa này phù hợp với các chuyên gia thường xuyên phải đi công tác hoặc làm việc ở khá cơ động ở chiều nơi khác nhau, có kích thước nhỏ, vừa đủ để với chuỗi phím và không có các bộ phận động. Có thể kết nối bộ nhớ động này với máy tính thông qua cổng USB để làm việc.

Một số bộ nhớ USB có chức năng mã hóa giúp dữ liệu vẫn bảo mật khi bị mất.

3.1.2 Lưu trữ trên các ổ cứng ngoài

Sử dụng ổ cứng ngoài để kết nối với máy tính. Nhưng việc dùng phương pháp này gặp phải những hạn chế sau:

- Luôn phải sao lưu tất cả các tệp dữ liệu nếu như các tệp dữ liệu trên đĩa mà không được lưu trữ ở nơi khác.
- Khi có hỏa hoạn hay sự cố thiên nhiên xảy ra tại nơi đặt ổ cứng ngoài, thì dữ liệu không không được bảo vệ.

3.1.3 Lưu trữ trên các hệ thống mạng trực tuyến

Khai thác các lợi ích của các dịch vụ cung cấp " dung lượng lưu trữ và sao lưu dữ liệu trên hệ thống Internet". Dữ liệu sẽ được sao lưu và cất giữ các tệp dữ liệu quan trọng của tại một máy chủ ở xa nhưng an toàn.

Trong thực tế thì việc sử dụng giải pháp này có những ưu – nhược điểm sau:

* Ưu điểm:
  - Tránh được rủi ra thảm họa, thiên tai xảy ra tại cục bộ một khu vực.
  - Chia sẻ dễ dàng những tệp dữ liệu lớn với khách hàng, đối tác.
  - Có thể sử dụng trình duyệt Web để truy cập và lấy các tệp dữ liệu ở mọi nơi có mạng internet.
* Nhược điểm:
  - Tốc độ truy cập vào dữ liệu hoàn toàn phụ thuộc vào đường truyền mạng.

3.1.4 Lưu trữ trên mạng máy tính (NAS)

NAS là cách lưu giữ số liệu đơn giản, dễ dàng truy cập với tốc độ cao và đáng tin cậy. Các giải pháp NAS phù hợp với các doanh nghiệp cỡ vừa và nhỏ luôn có nhu cầu phải sử dụng các tệp dữ liệu kinh tế có dung lượng lớn, nhiều người sử dụng cùng lúc và cho phép chia sẻ trong hệ thống mạng máy tính.

Trong đó một giải pháp NAS có thể thuộc một trong các loại sau:

* Các giải pháp NAS có thể chỉ là một ổ cứng đơn lẻ với cổng Ethernet hoặc là kết nối Wi-Fi với một hệ thống lưu trữ với dung lượng 300GB hoặc nhiều hơn. Ở mức độ cao hơn thì các giải pháp NAS có thể cung cấp cả các cổng USB phụ hay các cổng FireWire cho phép kết nối với các ổ cứng ngoài để mở rộng dung lượng lưu trữ. Một giải pháp NAS có

thể cho phép cài đặt và chia sẻ chỉ một máy in cho nhiều người sử dụng khác nhau một cách dễ dàng.

* Các giải pháp NAS cũng có thể gồm cả nhiều ổ cúng trong hệ thống đĩa dự phòng (RAID) ở mức 1. Hệ thống lưu trữ trong hệ thống RAID ở mức 1 có thể bao gồm 1 trong nhiều ổ cứng tương ứng (mỗi ổ đĩa có dung lượng 250GB) được kết nối với nhau tạo thành 1 thiết bị mạng. Dữ liệu được ghi lên đĩa thứ nhất và đồng thời được ghi lên đĩa thứ 2. Phương thức sao lưu dữ liệu dự phòng một cách tự động này để đề phòng trường hợp một đĩa bị hỏng/chết thì vẫn truy cập được vào dữ liệu đã được sao lưu dự phòng ở ổ đĩa kia.

Các giải pháp NAS cũng có thể upload tập tin, dữ liệu từ các máy chủ khác trong hệ thống trong hệ thống mạng, và cho phép thống nhất lưu trữ dữ liệu.

Sử dụng hệ thống NAS có những lợi ích như :

- Nâng cao hiệu quả hoạt động của hệ thống.
- Giảm chi phí.
- Đơn giản quy trình quản trị và sao lưu cũng như khôi phục các tập tin, dữ liệu.
- Hệ thống dễ mở rộng và nâng cấp để có thể đáp ứng được nhu cầu lưu trữ số liệu ngày càng tăng.

3.1.5 Một số giải pháp đảm bảo an toàn cho hệ thống.

Hiện nay, tại các cơ quan hay các tổ chức thì hệ thống mạng thường được tổ chức theo mô hình Domain. Microsoft Windows Server là một trong những hệ điều hành dành cho các hệ thống máy chủ cung cấp các dịch vụ như chia sẻ tập tin, phân luồng,… Microsoft Windows Server 2008 hỗ trợ các dịch vụ có thể đáp ứng được nhu cầu của người dùng trong việc đảm bảo an toàn phù hợp đối với từng loại dữ liệu cho hệ thống của các công ty, cơ quan cụ thể. Cùng với việc tổ

chức lưu trữ thì nhu cầu đảm bảo an toàn cho dữ liệu cũng được ưu tiên hàng đầu. Có nhiều giải pháp lưu trữ khác nhau phù hợp cho nhiều nhóm người dùng với nhu cầu lưu trữ khác nhau. Tuy cách thức tổ chức hệ thống mạng tại các cơ quan, đơn vị cụ thể chúng ta có thể đưa ra các lựa chọn, các giải pháp lưu trữ một cách hợp lý để đảm bảo an toàn dữ liệu.

- Dữ liệu tồn tại dưới dạng cơ sở dữ liệu MS SQL, cơ sở dữ liệu thư điện tử Exchange,… một trong số các giải pháp có thể sử dụng là triển khai phần mềm Data Protection Manager (DPM) để đảm bảo an toàn dữ liệu.
- Dữ liệu tồn tại dưới các tập tin thông thường như: các tệp văn bản, tệp tin ảnh, video,… việc triển khai Distributed File System đáng được quan tâm.

Trong phạm vi của đồ án này, em tiến hành tìm hiểu các giải pháp "*xây dựng hệ thống lưu trữ tập trung trên nền tảng Distributed File System Windows Server 2008*".

3.2 Tổng quan về Distributed File Systems

Với các cơ quan, tổ chức hay các công ty, lượng dữ liệu cần phải lưu trữ sẽ là rất lớn. Với yêu cầu cần phải lưu trữ dữ liệu với dung lượng lớn, đảm bảo tính sẵn sàng của hệ thống dữ liệu cần lưu trữ mọi thời điểm và đáp ứng cao nhất số yêu cầu truy cập trong một thời điểm.

Microsoft Windows Server 2008 cung cấp dịch vụ Distributed File System để giải quyết vấn đề số lượng kết nối lớn tới dữ liệu tại cùng một thời điểm.

Distributed File System được sử dụng để xây dựng cấu trúc đại diện cho nhiều vị trí chia sẻ dữ liệu trên nhiều File Server khác nhau. Distributed File System có nhiệm vụ nhóm tất cả các chia sẻ trong hệ thống server dưới một tên duy nhất giúp người dùng có thể sử dụng một cách dễ dàng.

3.2.1 Các mô hình triển khai dịch vụ Distributed File System:

Trong quá trình triển khai dịch vụ DFS, chúng ta có thể chọn một trong hai kiểu namespace: Domain-based namespace hoặc Stand-alone namespace.

∗ Domain-base namespace: tất cả các server phải là thành viên của hệ thống Active Directory. Môi trường này hỗ trợ việc đồng bộ hóa tự động các DFS target. Namespace root của namespace dựa trên sự kết hợp giữa tên NetBIOS của server và tên root, được liệt kê trong DNS. Một server có thể host nhiều root DFS khác nhau.

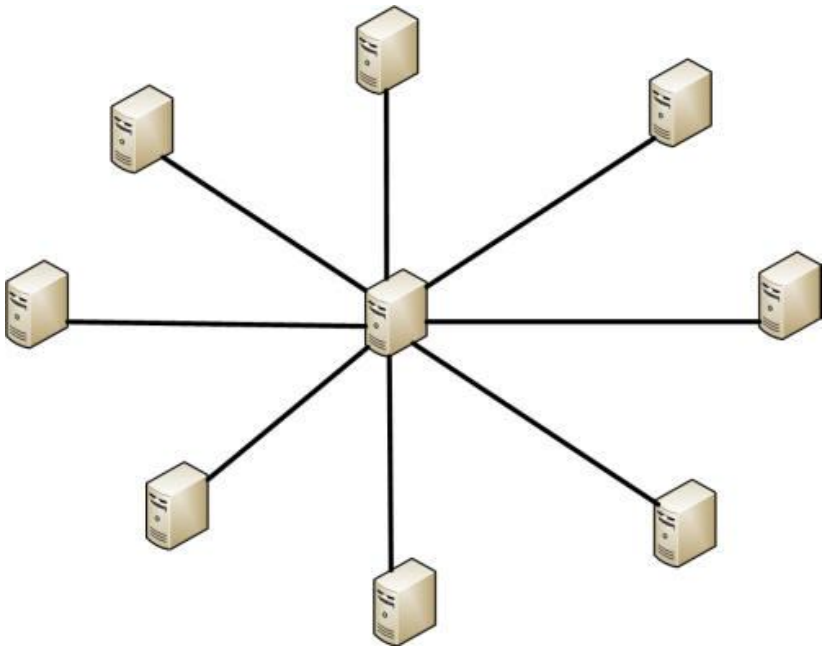
∗ Stand – alone namespace: cho phép một DFS gốc mà chỉ tồn tại trên máy tính địa phương, và do đó không sử dụng Active Directory . Một DFS độc chỉ có thể được truy cập trên máy tính mà nó được tạo ra. Nó không cung cấp bất kỳ khả năng chịu lỗi và không thể được liên kết với bất kỳ DFS khác.

3.2.2 Các cấu trúc liên kết sao lưu

Trong khi triển khai hệ thống DFS tại các tổ chức với số lượng truy cập tới các file dữ liệu lớn thì một vấn đề đặt ra đó là làm sao để giảm tải, tăng khả năng chịu lỗi cho các server và đảm bảo quá trình hoạt động của người dùng diễn ra liên tục. Windows Server 2008 hỗ trợ một vài dạng cấu trúc liên kết nhân bản khác biệt cho các server DFS. Những cấu trúc liên kết này có những điểm tốt và chưa tốt do đó cần phải đưa ra lựa chọn một cách hợp lý.

∗ Cấu trúc Hub và Spoke:

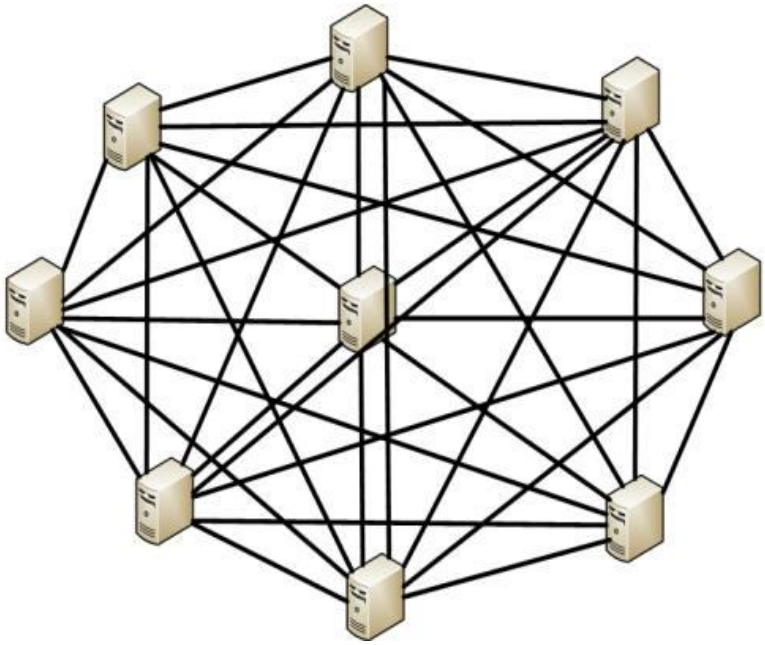
Cấu trúc này đặt initial master vào giữa cấu trúc liên kết. Một bản sao thực hiện hai các sao chép với initial master, nhưng không sao chép thêm bất kỳ bản sao nào khác. Loại cấu trúc này rất hiệu quả nhưng tất các bản sao sẽ ngừng hoạt động khi initial master bị lỗi, và sẽ chỉ hoạt động trở lại khi vị trí initial master được nối trở lại.



Hình 3.1: Cấu trúc liên kết Hub và Spoke.

- **Cấu trúc liên kết Full Mesh:**

Cấu trúc này cho phép mỗi bản sao được sao chép với mỗi bản sao khác. Ưu điểm là mỗi bản sao vẫn tiếp tục chức năng cho dù server có offline. Nhược điểm là nó có thể dẫn đến một lưu lượng quá mức các bản sao.



Hình 3.2: Cấu trúc liên kết Full Mesh

- **Cấu trúc liên kết No Topology:**

Cấu trúc này cho phép người dùng tạo một nhóm bản sao mà không cần xác định cấu trúc liên kết nhân bản, điều này cho phép người dùng tạo ra một nhóm sao chép tùy chỉnh sau.

3.2.3 Cài đặt dịch vụ

a. Giới thiệu

Mô hình sử dụng 1 Domain Controllers (DC) thực hiện công việc chứng thực cho các client đăng nhập vào hệ thống. Đồng thời sử dụng 2 File Server để giảm tải cho nhau và tăng khả năng chịu lỗi khi có một File Server bị lỗi thì vẫn còn một File Server thay thế.

Chuẩn bị: 1 Domain Controllers (DC), 1 Primary File Server, 1 Secondary File Server.

b. Triển khai dịch vụ DFS trên hai File Server

Để triển khai dịch vụ DFS trên hai File Server, chúng ta cần thực hiện các bước sau:

- **Bước 1: Cài đặt dịch vụ.**

Trên hai File Server (server 01 và server 02) thực hiện các công việc sau:

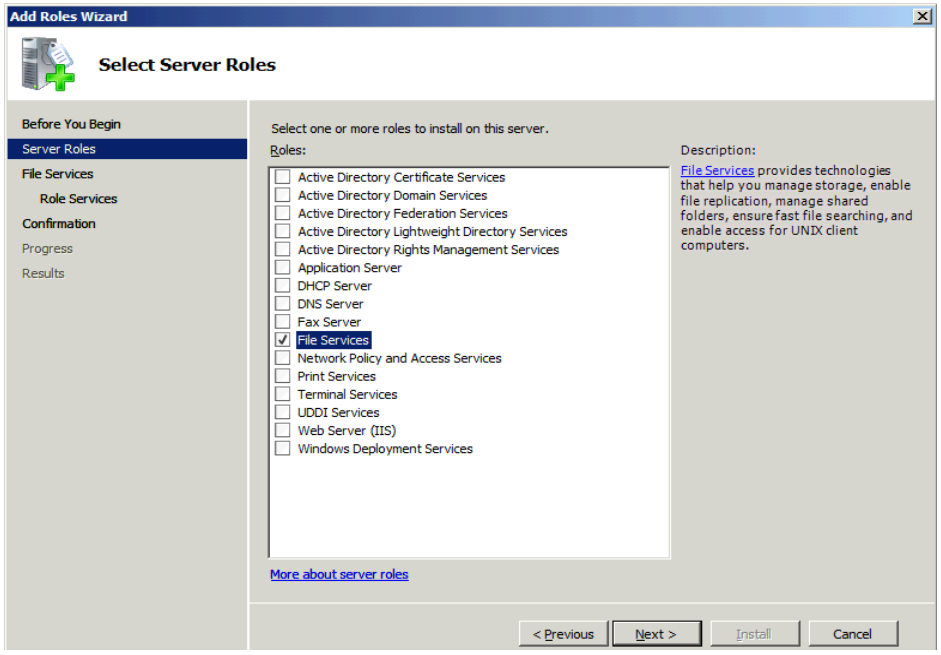
Vào **Server Manager** → chọn **Roles** → chọn **Add roles**

Hộp thoại **Before You Begin** xuất hiện, Chọn **Next** để bỏ qua giới thiệu dịch vụ.

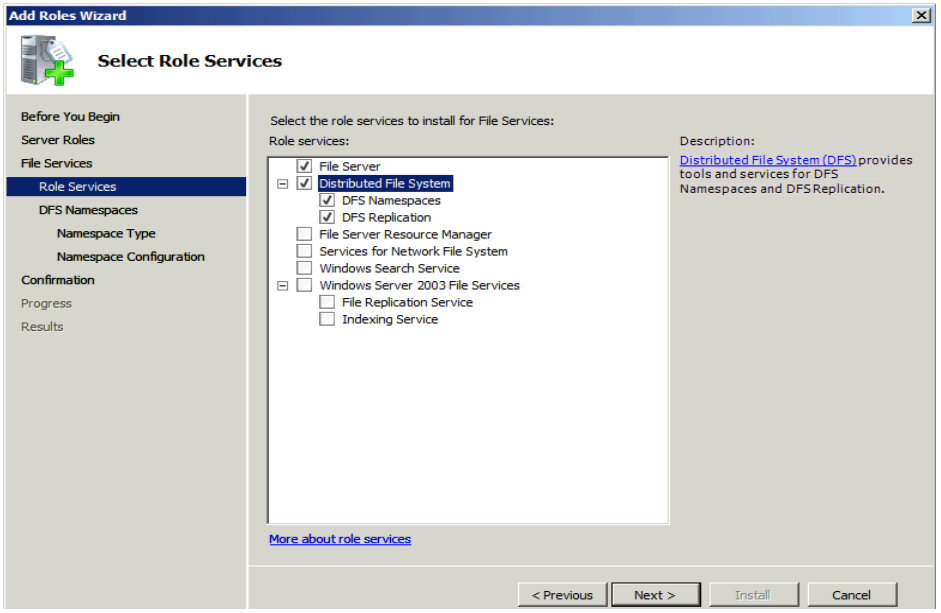
Đánh dấu chọn vào **File Services** như hình 3.3 → chọn **Next**.

Xem phần giới thiệu về dịch vụ **File Services** → chọn **Next**.

Hộp thoại **Select Role Services** xuất hiện, đánh dấu chọn vào mục **DFS Namespaces** và **DFS Replication** như hình 3.4 → chọn **Next**.



Hình 3.3: Giao diện lựa chọn các dịch vụ như File Server



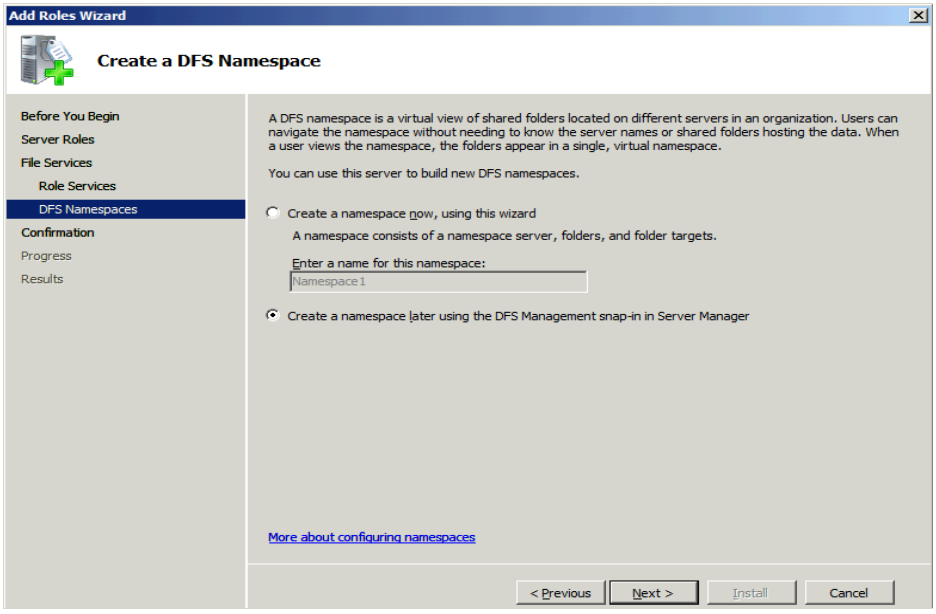
Hình 3.4: Giao diện lựa chọn các dịch vụ của DFS

Hộp thoại **Create a DFS Namespace,** chọn **Create a namespace late using the DFS Management snap-in in Server Manager** như hình 3.5 → chọn **Next**.

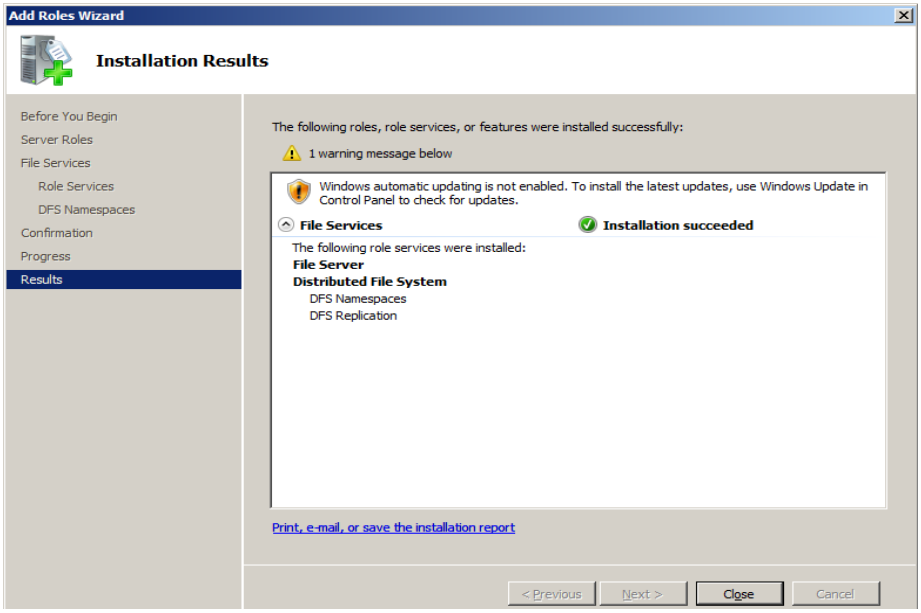
Hộp thoại **Confirm Installation Sellections** xuất hiện, chọn **Install.**

Hộp thoại **Intallation Progress** xuất hiện để hiển thị quá trình cài đặt DFS

Khi quá trình cài đặt kết thúc, hộp thoại **Install Results** xuất hiện như hình 3.6→ chọn **Close** để kết thúc.



Hình 3.5: Giao diện lựa chọn thời điểm cài đặt DFS Namespaces.



Hình 3.6: Kết quả của cài đặt DFS

- **Bước 2: Cấu hình dịch vụ.**

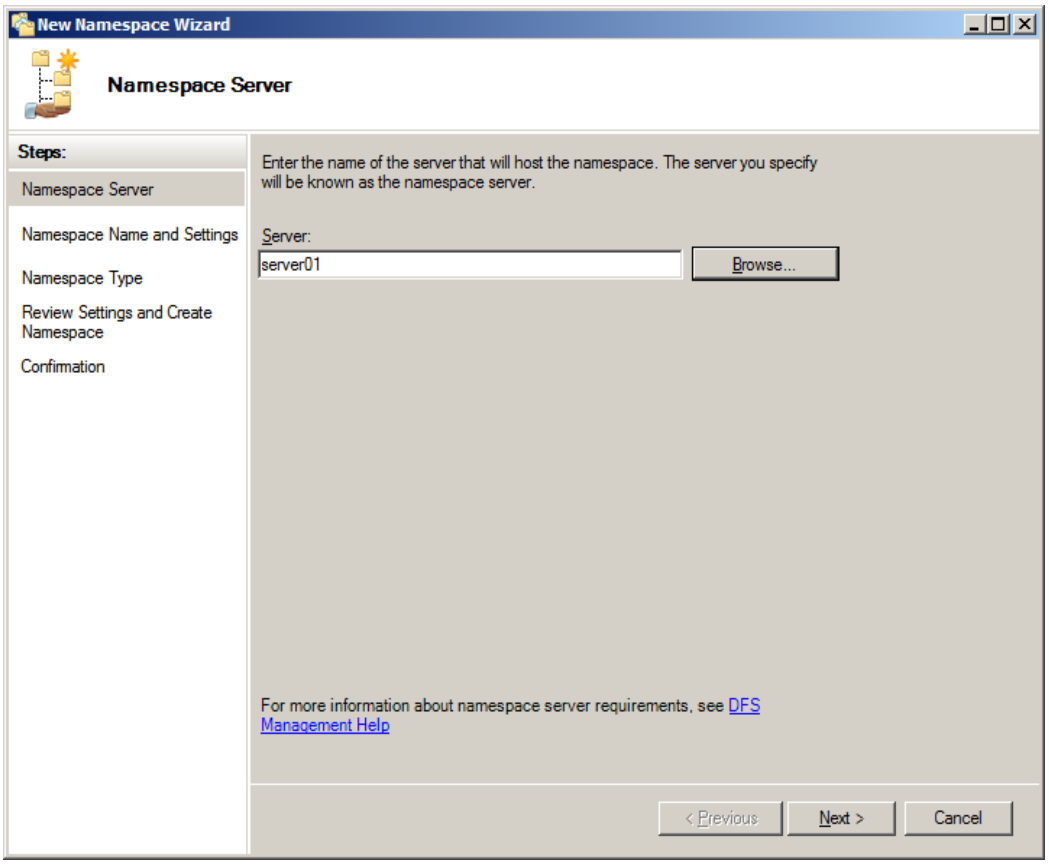
Để cấu hình dịch vụ DFS, trên server01 ta cần thực hiện các công việc sau:

- Tạo Namespace:

Vào **Start → Administrative Tools → DFS Management**.

Hộp thoại **DFS Management** xuất hiện, chọn chuột phải vào mục **Namespaces** → chọn **New Namespaces**.

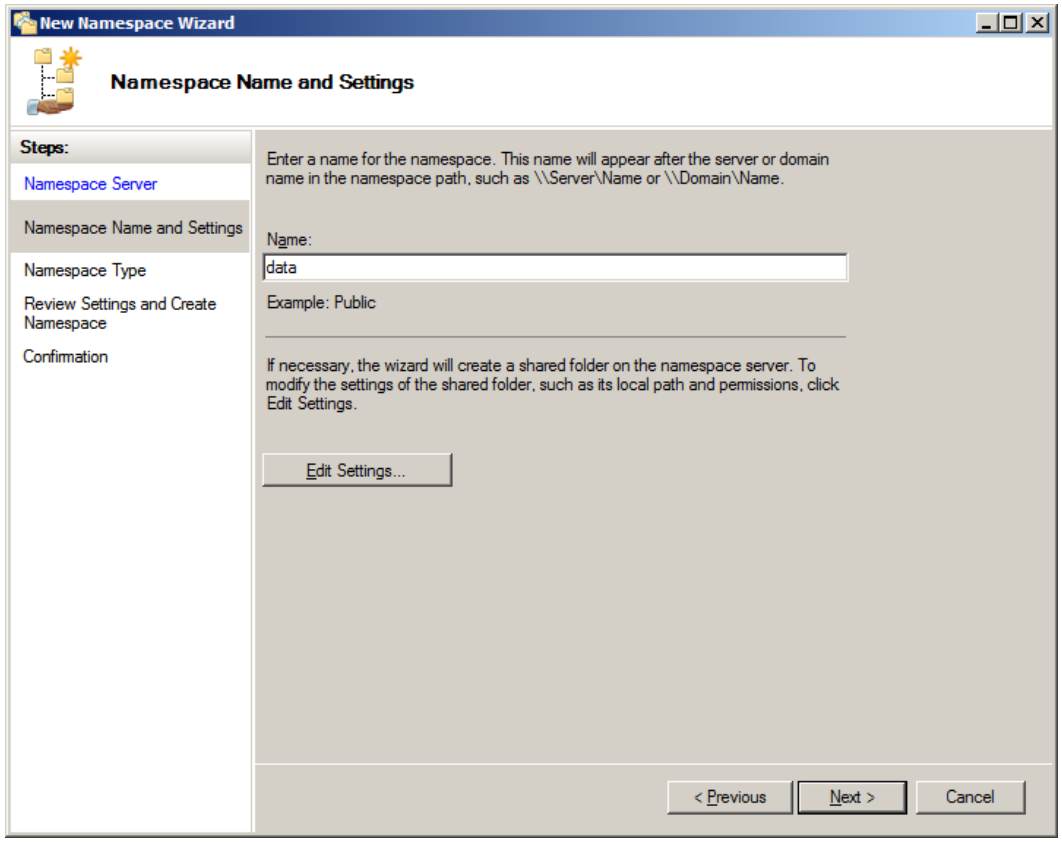
Hộp thoại **Namespace Server** xuất hiện, nhập **server01** như hình 3.7 hoặc chọn **Browse** → hộp thoại **Select** xuất hiện, chọn **SERVER01**→ chọn **Next**.



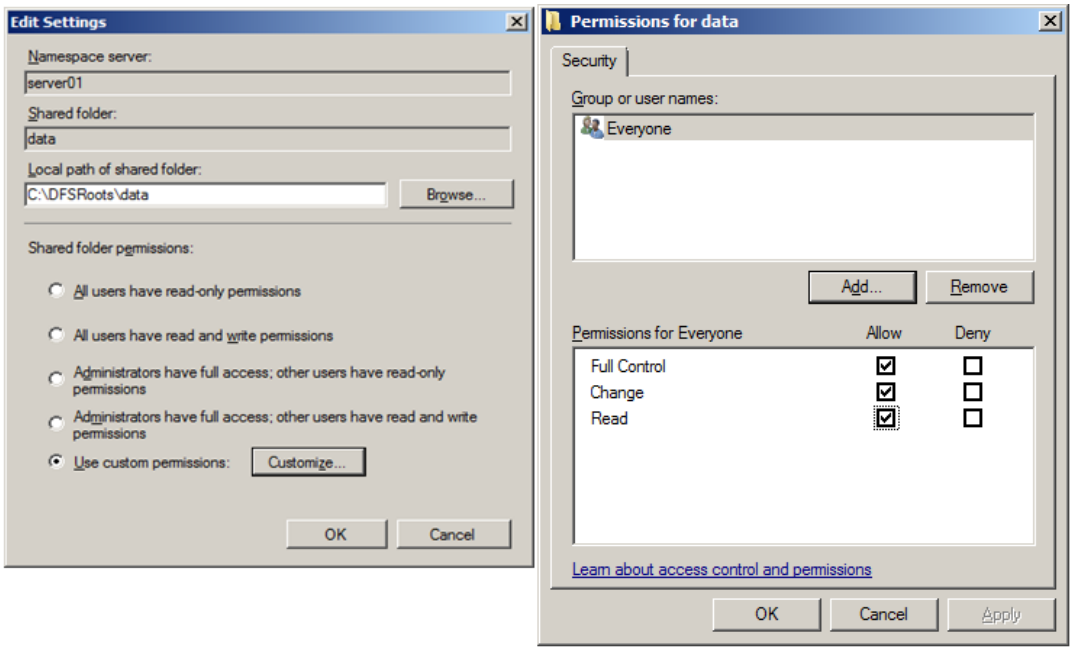
Hình 3.7: Lựa chọn server chạy dịch vụ Namespaces.

Hộp thoại **Namespace Name and Settings** xuất hiện, khai báo tên thư mục (folder) chứa dữ liệu sẽ chia sẻ trong hệ thống cho users truy cập lấy tài nguyên cũng như lưu trữ dữ liệu,…

Trong ô **Name**, nhập tên thư mục như hình 3.8.



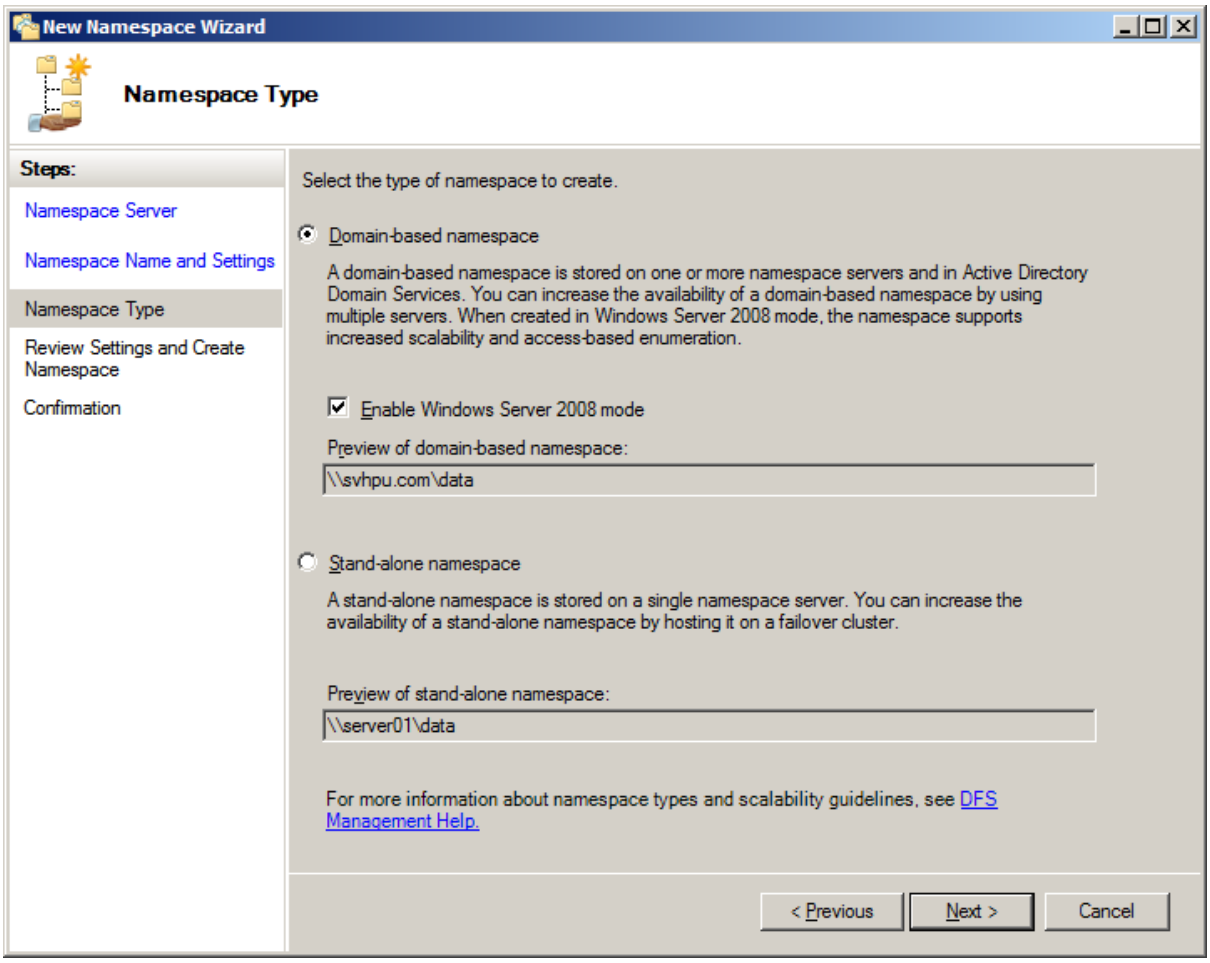
Hình 3.8: Khai báo tên thư mục chia sẻ và phân quyền cho user



Hình 3.9: Hộp thoại phân quyền người dùng

Chọn **Edit Settings** → chọn **Use custom permissions** → chọn **Customize**

Hộp thoại **Permission for data** → chọn **Full Control** ở cột **Allow** như hình 3.9. Chọn **OK**→ chọn **OK** → Hộp thoại **Namespace name and settings**, chọn **Next.**

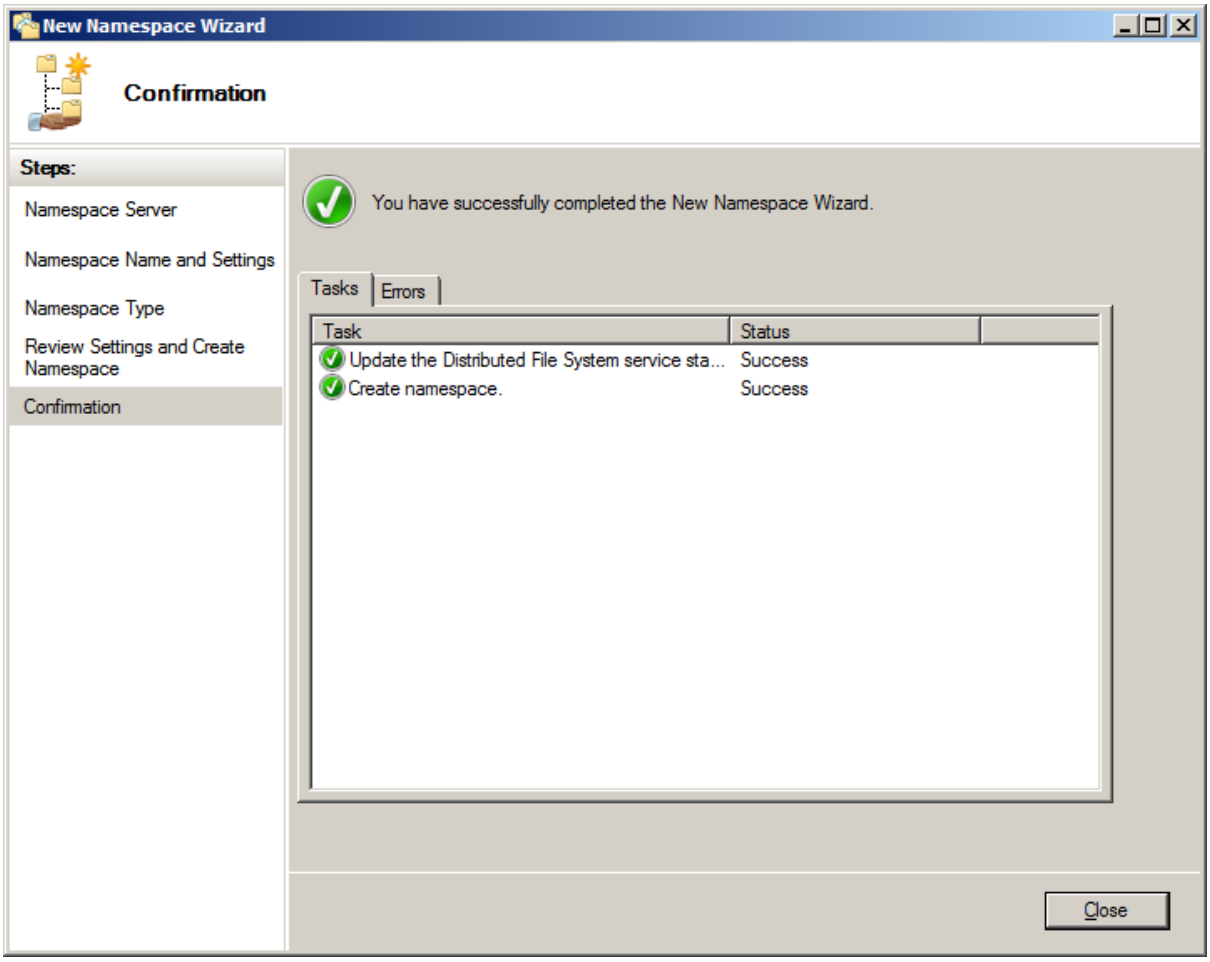


Hình 3.10: Chọn kiểu Namespaces

Hộp thoại **Namespace Type** xuất hiện, đánh dấu chọn và mục **Domain-based namespace** như hình 3.10 → chọn **Next**.

Hộp thoại **Review Settings and Create Namespace** → chọn **Create**.

Hộp thoại **Confirmation** xuất hiện, phải đảm bảo là hệ thống thông báo **Success** như hình 3.11→ chọn **Close**.

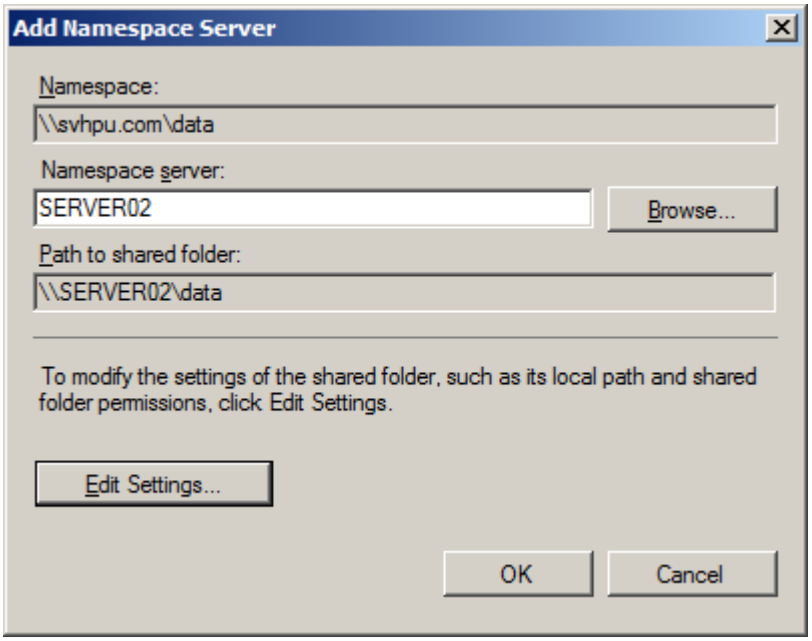


Hình 3.11: Thông báo kết quả cài đặt

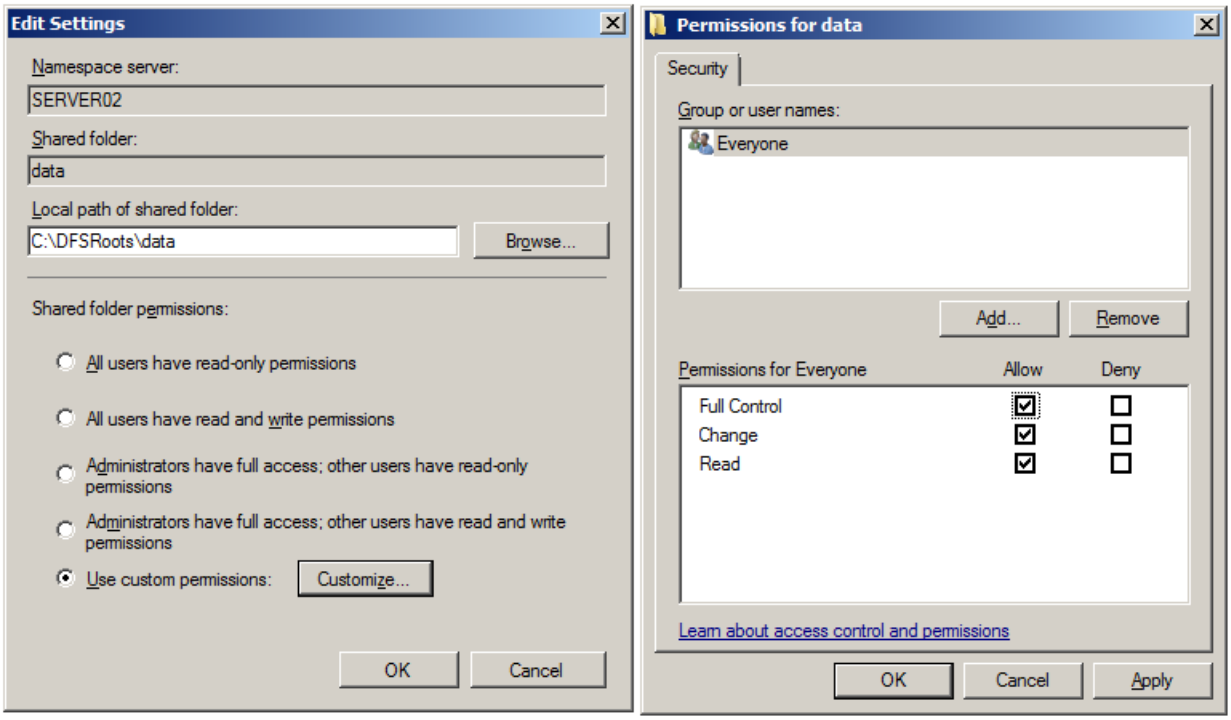
- Chọn server để Replicate dữ liệu:

Trong cửa sổ **DFS Management**, chọn chuột phải lên **Namespace** mới tạo → chọn **Add Namespace Server**. Hộp thoại **Add Namespace Server** xuất hiện, chọn **Browse** → chọn **SERVER02** như hình 3.12

Chọn **Edit Settings**. Trong hộp thoại **Edit Settings** đánh dấu vào mục **Use custom permissions** và chọn **Customize**. Trong hộp thoại **Permissions for data** cho group **Everyone** quyền **Full Control** ở cột **Allow** như hình 3.13 → chọn **OK** → chọn **OK** → chọn **OK**.



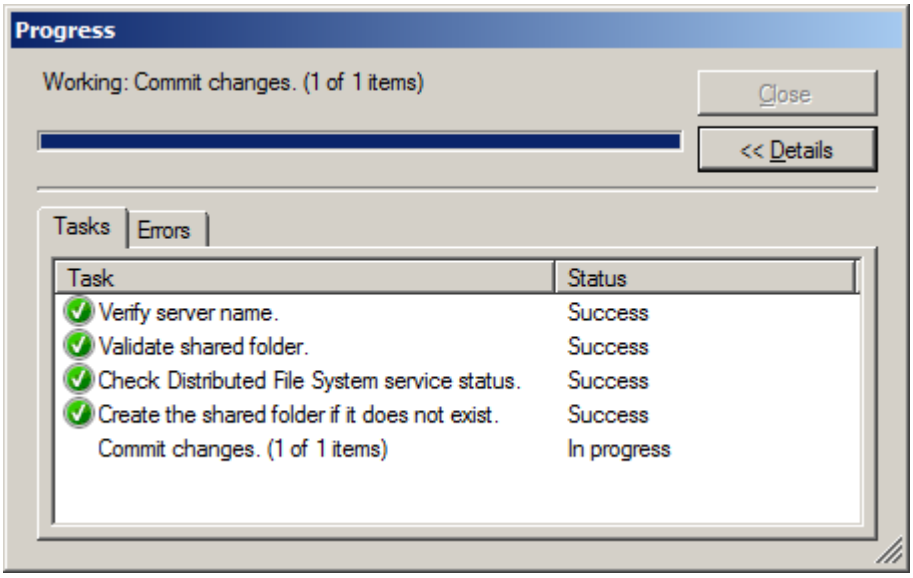
Hình 3.12: Chọn server chạy chức năng replicate dữ liệu



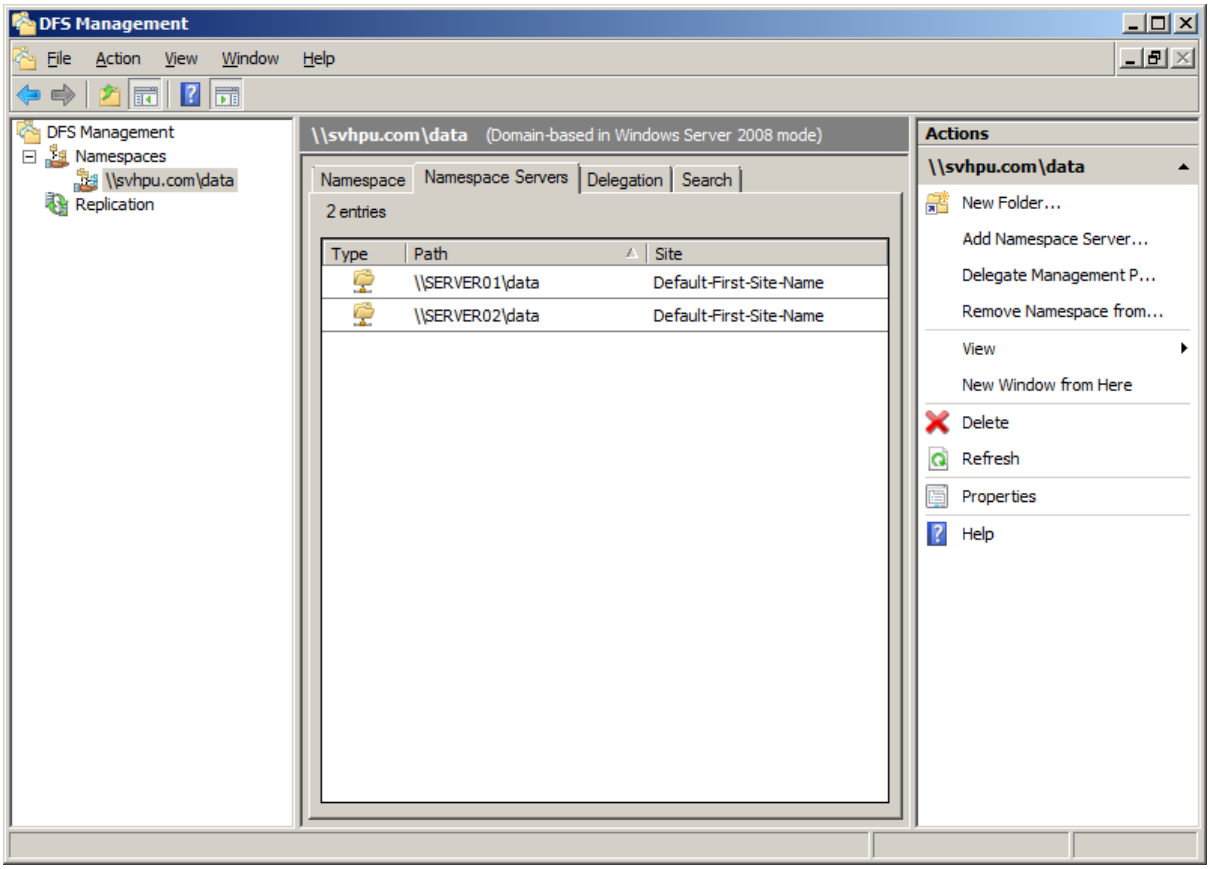
Hình 3.13: Phân quyền sử dụng của người dùng

Hệ thống sẽ thực hiện cài đặt, như hình 3.14.

Khi cài đặt xong, hộp thoại **DFS Management** có giao diện như hình 3.15.



Hình 3.14: Cài đặt để server02 sao chép dữ liệu của server01

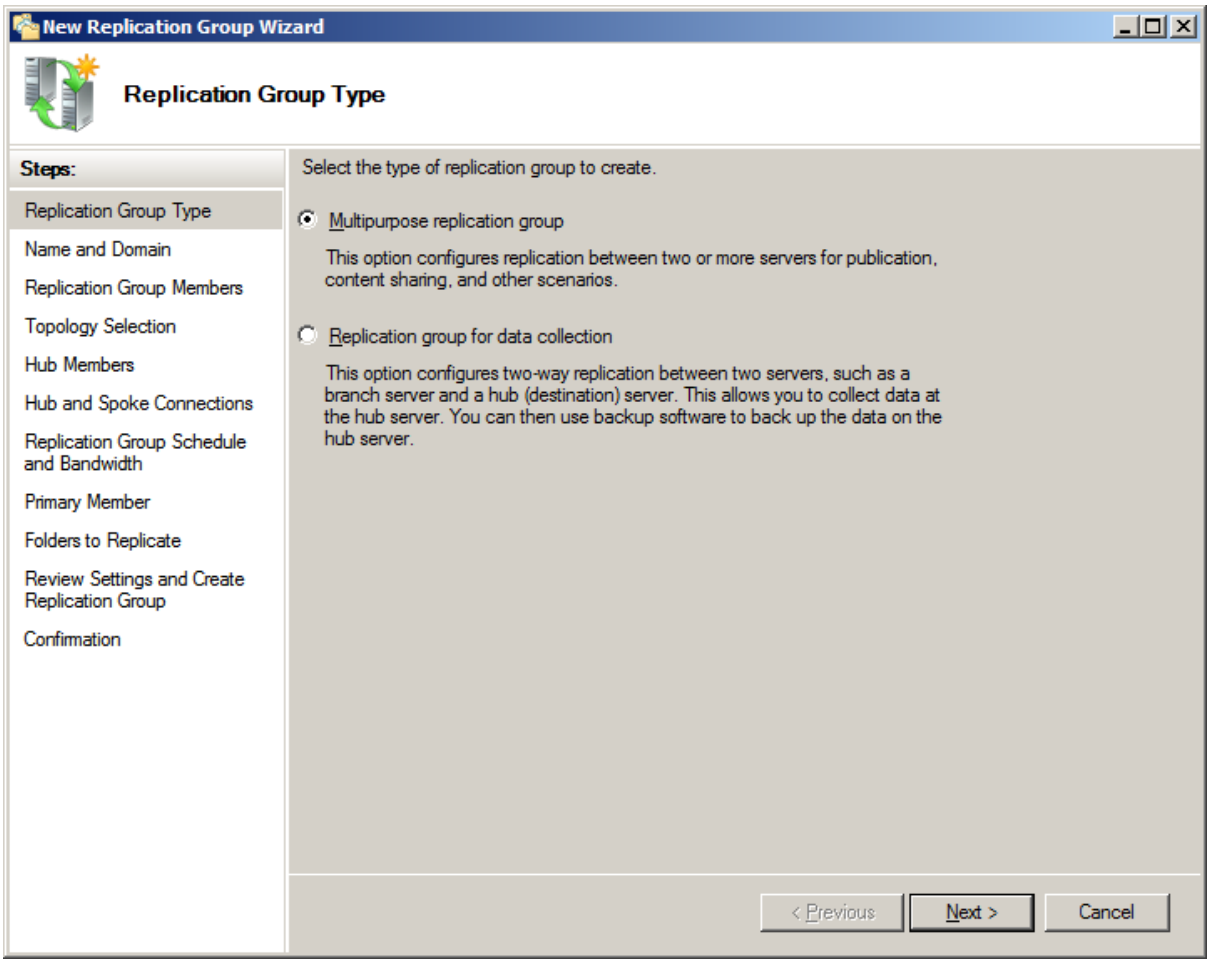


Hình 3.15: Giao diện của DFS Management sau khi cấu hình Namespaces.

- **Bước 3: Cấu hình replication group**

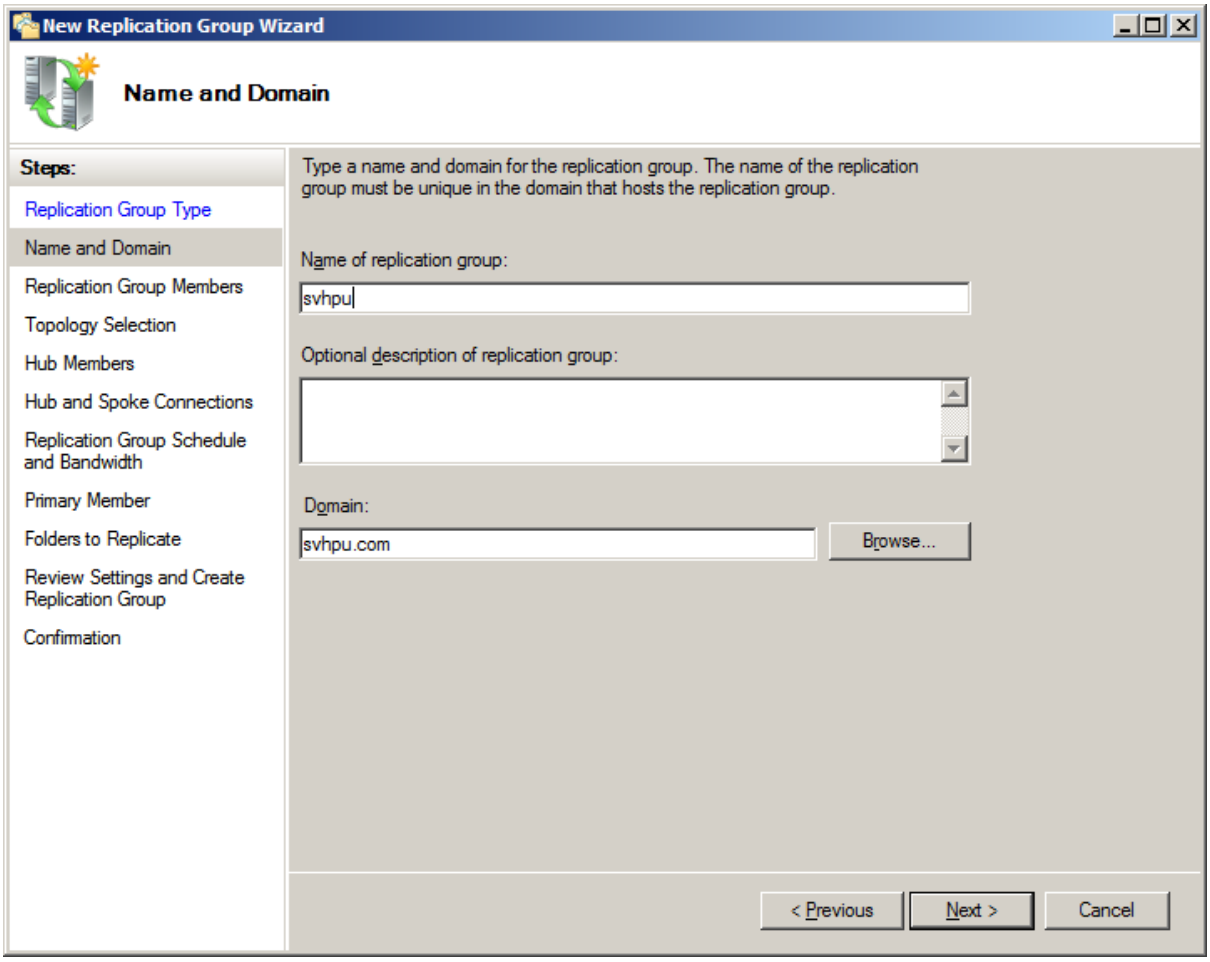
Cửa sổ DFS Management click chuột phải lên mục **Replication** → chọn **New Replication Group**.

Hộp thoại **Replication Group Type**, đánh dấu chọn vào ô **Multipurpose replication group** như hình 3.16 → chọn **Next**.



Hình 3.16: Chọn kiểu sao chép dữ liệu.

Hộp thoại **Name and Domain** xuất hiện, đặt tên cho **replication group** là: svhpu, chọn Domain là: svhpu.com như hình 3.17 → chọn **Next**.

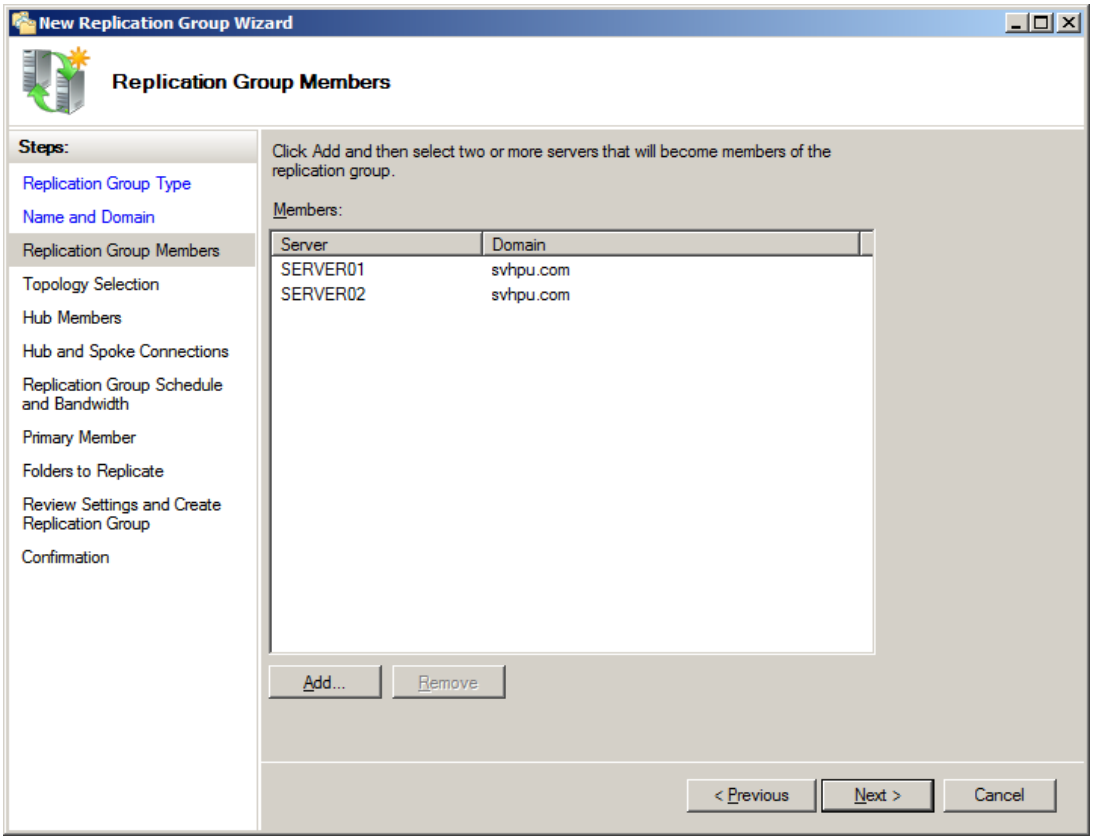


Hình 3.17: Đặt tên và chọn Domain cho replication group.

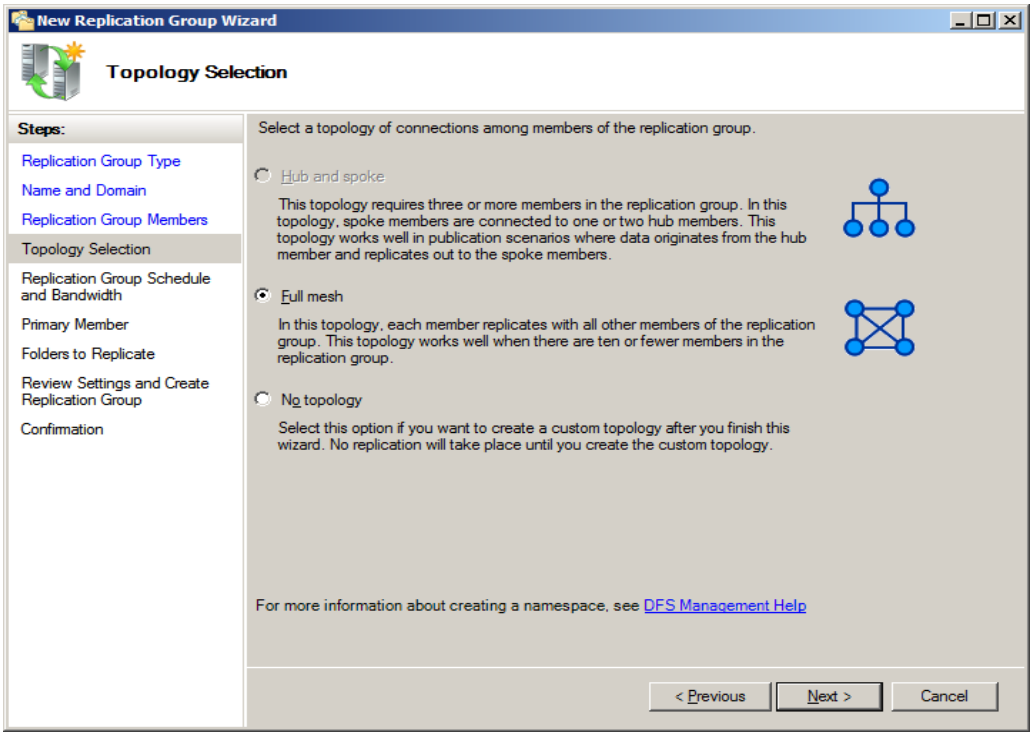
Trong hộp thoại **Replication Group Members**, chọn chuột trái vào **Add**. Hộp thoại **Select Computers** xuất hiện, chọn SERVER01 và SERVER02 (2 File Server) → chọn **OK**, như hình 3.18→ chọn **Next**.

Trong hộp thoại **Topology Selection**, đánh dấu chọn vào mục **Full mesh** như hình 3.19→ chọn **Next**.

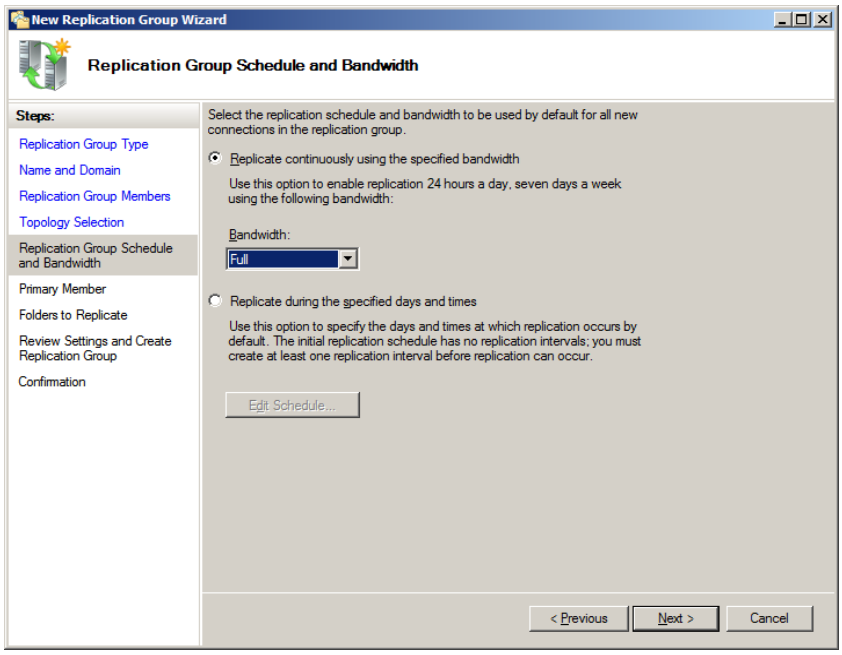
Trong hộp thoại **Replication Group Schedule and Bandwidth**, chọn **Replication continuously using the specified** bandwidth: **Full** như hình 3.20→ chọn **Next**.



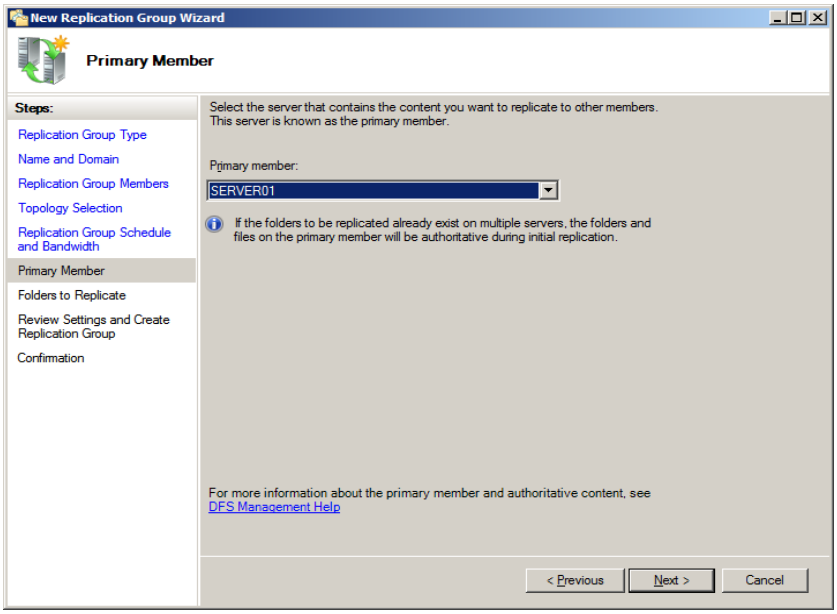
Hình 3.18: Lựa chọn các server trong Replication Group Members.



Hình 3.19: Lựa chọn kiểu liên kết sao chép.



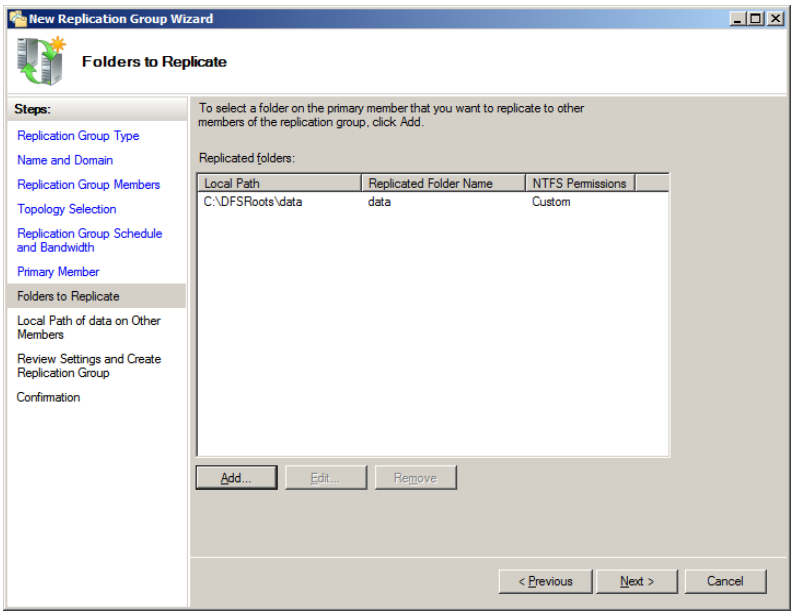
Hình 3.20: Chọn thông tin cho Replication Group Schedule and Bandwidth



Hình 3.21: Lựa chọn máy chủ làm chức năng Primary member.

Trong hộp thoại **Primary Member** chọn **SERVER01** như hình 3.21 → chọn **Next**.

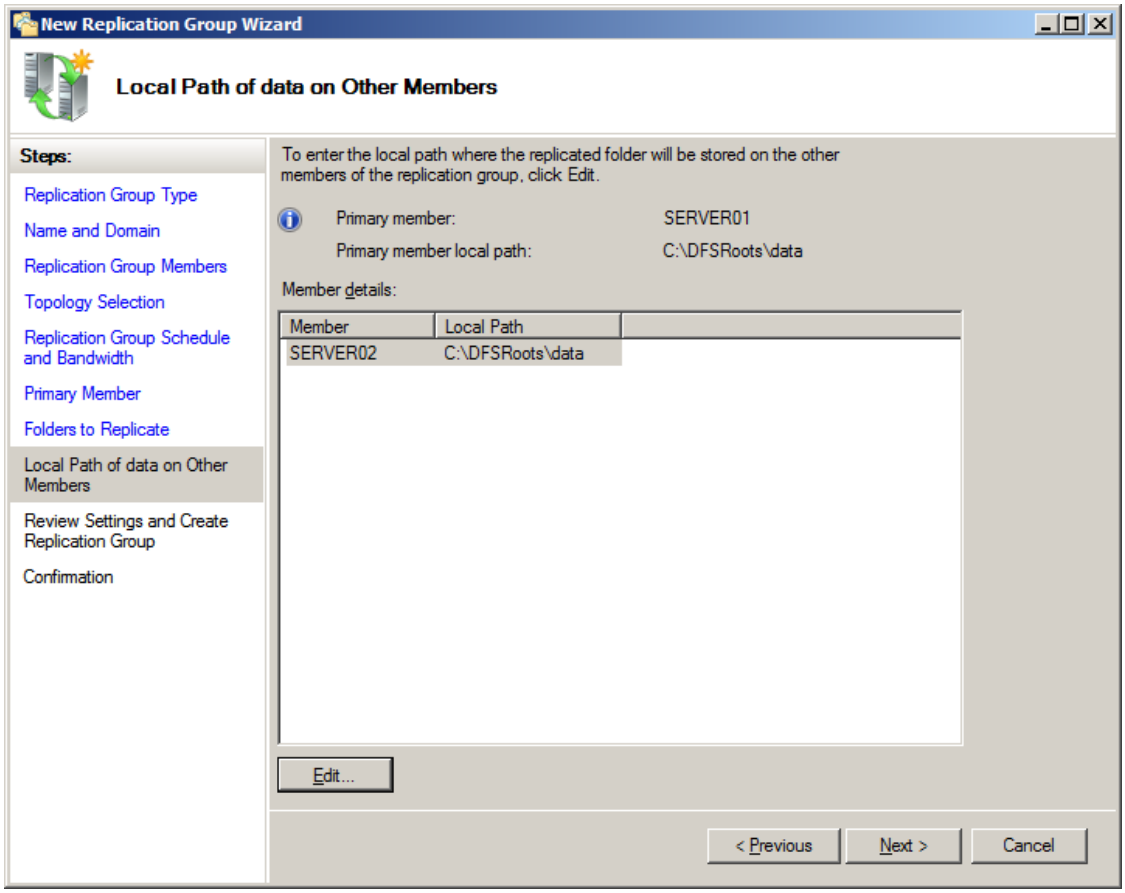
Hộp thoại **Folder to Replicate**, chọn **Add**. Chọn **Browse**, trong hộp thoại **Browse For Folder**, chọn folder theo đường dẫn **C:\DFSRoots\data**. Trong Hộp thoại **Add Folder to Replicate** đảm bảo path là **C:\DFSRoots\data** → chọn **Permissions** → chọn **Custom permissions** → chọn **Edit Permissions** → chọn **OK** → chọn **OK.** Trở lại hộp thoại **Folders to Replicate** như hình 3.22 → chọn **Next**.



Hình 3.22: Lựa chọn thư mục cần sao chép.

Trong hộp thoại **Local Path of data on other Member** chọn SERVER02. Hộp thoại **Edit**, chọn **Enabled** và chọn **Browse** theo đường dẫn **C:\DFSRoots\data** → chọn **OK**.

Trở lại hộp thoại **Local Path of data on Other Members**, đảm bảo có thành viên **SERVER2** và có đường dẫn **là C:\DFSRoots\data** như hình 3.23 → chọn **Next**.

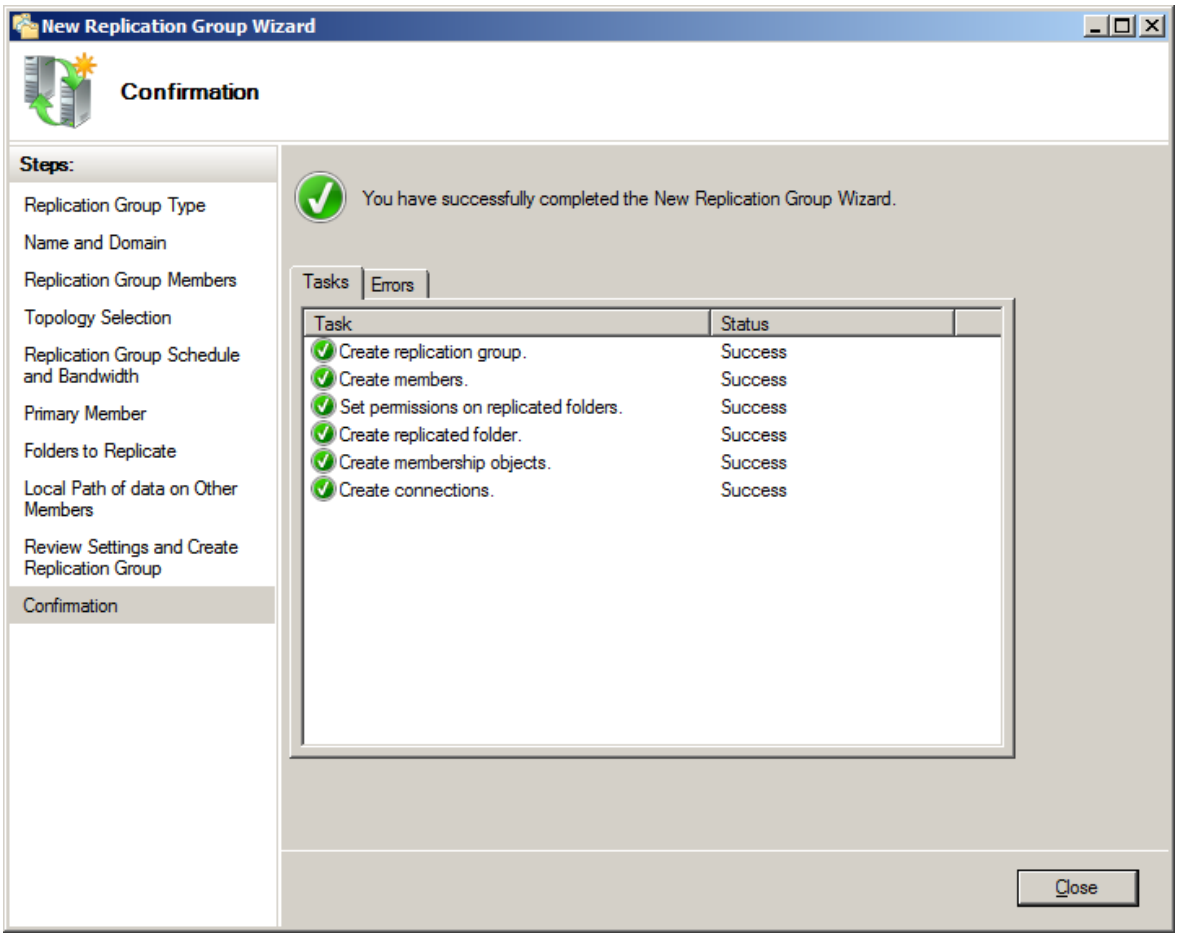


Hình 3.23: Lựa chọn server làm chức năng sao chép dữ liệu cho SERVER01.

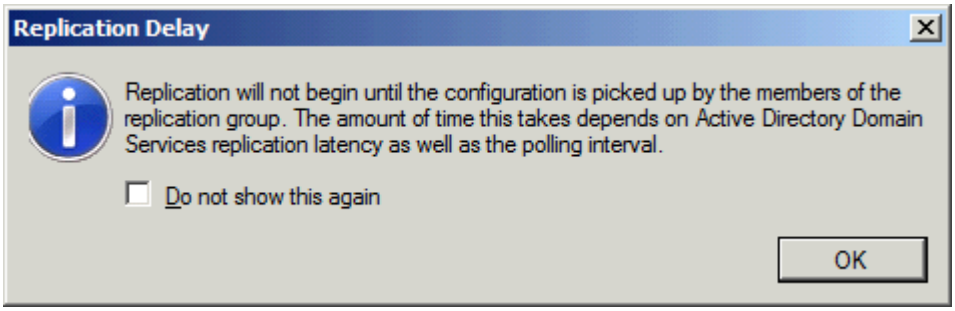
Trong hộp thoại **Review Settings and Create Replication Group** → chọn **Create**.

Hộp thoại **Confirmation** đảm bảo là **Success** như hình 3.24, chọn **Close**.

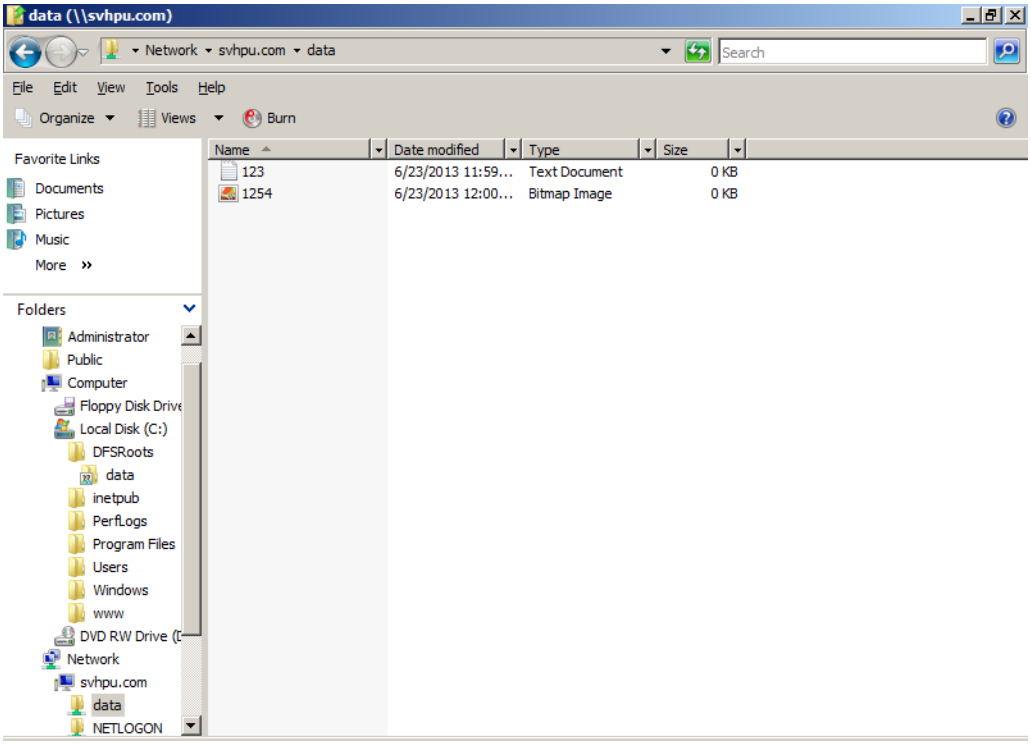
Xuất hiện thông báo của hệ thống như hình 3.25, chọn **OK** để hoàn thành.



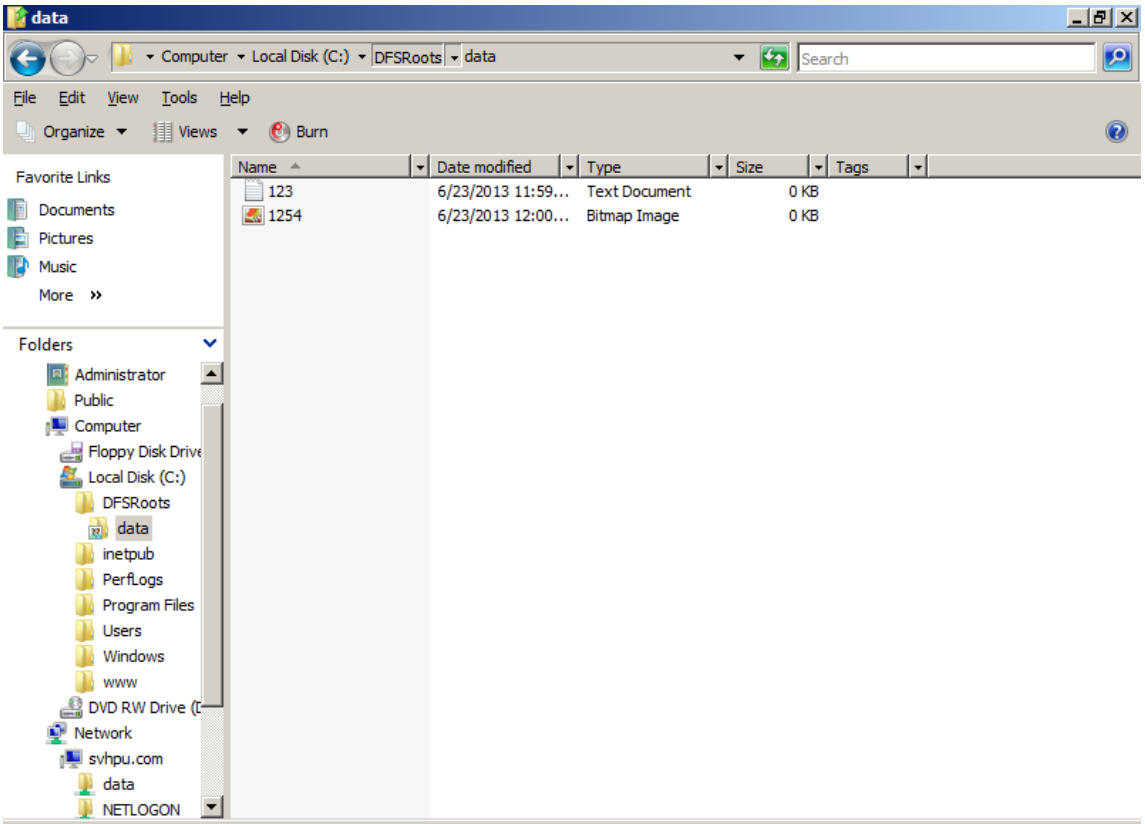
Hình 3.24: Trạng thái của quá trình cài đặt.



Hình 3.25: Thông báo của hệ thống sau khi hoàn tất cài đặt.



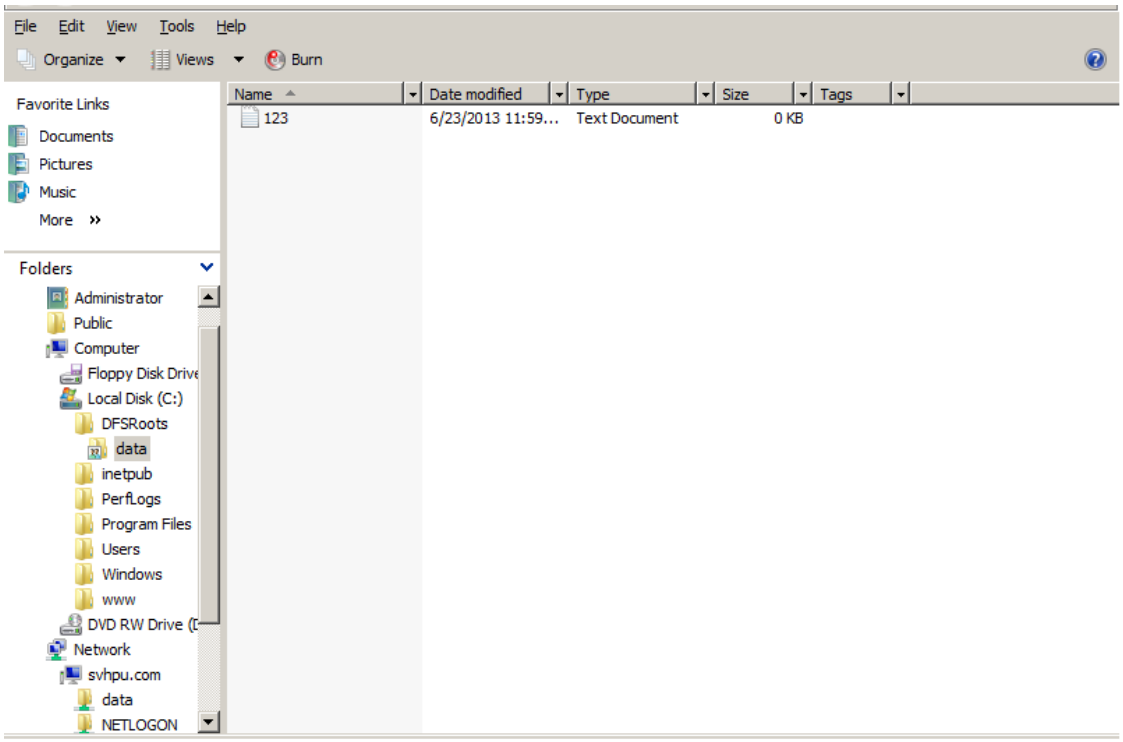
Hình 3.26: Giao diện của khi người dùng truy cập theo đường dẫn \\svhpu.com\data



Hình 3.27: Các file trong thư mục DFSRoots của Replicate server (server02).

Sau khi cài đặt chương trình cài đặt hoàn tất, chúng ta tiến hành thử nghiệm xem DFS có hoạt động có hoạt động hay không. Từ một máy client chúng ta vào **Start** → chọn **run** → gõ **\\svhpu.com\data** → **Enter**, không gian thư mục chia sẻ file có giao diện như hình 3.26 và đồng thời truy cập vào thư mục **data** của server02 theo đường dẫn **\\DFSRoots\data** hiển thị như hình 3.27.

Để thử nghiệm cơ chế nhân bản giữa hai server cho nhau. Tại máy server01, chúng ta vào **Start** → chọn **run**, nhập **\\DFSRoots\data**, sau đó ta xóa một tập tin bất kỳ, ví dụ: xóa file ảnh có tên là **1254** có định dạng như hình 3.27. Sau đó, tại máy server02 chúng ta truy cập vào thư mục theo đường dẫn **\\DFSRoots\data**, các tập tin trên thư mục như hình 3.28.



Hình 3.28: Thư mục DFSRoots\data trên máy server02 khi xóa file trên server 01

Để thử nghiệm khả năng chịu lỗi, chúng ta tắt **server01** và cho client truy cập theo đường dẫn **\\svhpu.com\data** thì vẫn thấy kết nối được với dữ liệu. Điều này chứng tỏ client đã truy cập vào dữ liệu thông qua server02, qua đó thể hiện khả năng chịu lỗi của hệ thống.

3.2.4 Nhận xét

Trong một hệ thống mạng lớn thì việc để một máy File Server gánh tất cả các yêu cầu là không thể. Mà yêu cầu là làm sao để có nhiều File Server hơn và cùng chia sẻ một lượng tài nguyên nào đó. Để giải quyết, Microsoft đã đưa ra một giải pháp là Distributed File System hay còn gọi là hệ thống dữ liệu phân tán. Dữ liệu dùng để chia sẻ cho người dùng sẽ không còn nằm trên 1 File Server nữa mà tùy vào yêu cầu thực tế mà người quản trị sẽ thiết kế 2 hay nhiều File Server cùng thực hiện việc chia sẻ này, tổng hợp tất cả các File Server này được gọi là DFS.

Ta có thể liên kết tất cả các chia sẻ tới Departments root (không cần bận tâm tới vị trí thực sự của các chia sẻ). DFS root giúp giảm một số lượng lớn các bước quản lý chia sẻ và tăng tốc độ truy cập tới tất cả các liên kết thêm vào thông qua DFS root dù tập tin chia sẻ đang trên bất kỳ máy chủ nào.

Việc sử dụng DFS sẽ cho phép các quản trị viên chỉ rõ các các ánh xạ điều khiển mạng tới một vị trí để truy nhập tới tất cả các liên kết chia sẻ. Việc giảm bớt số lượng ánh xạ điều khiển và bảo trì có thể kết hợp với việc quản lý các ánh xạ đó. Với những doanh nghiệp lớn thường có hàng tá hoặc thậm chí hàng trăm File server. Đây chính là vấn đề nan giải khi mà người dùng khó nhớ được server nào lưu trữ tập tin nào đó. DFS cung cấp một vùng không gian duy nhất cho phép người dùng có thể kết nối đến bất cứ thư mục chia sẻ nào trong doanh nghiệp. Với DFS, tất cả mọi thư mục chia sẻ có thể được truy cập.

KẾT LUẬN

Đồ án "*Xây dựng hệ thống lưu trữ tập trung trên nền tảng Distributed File System Windows Server 2008*" đã đạt được một số kết quả như sau:

Về lý thuyết, đồ án đã trình bày và hiểu được:

- Tổng quan về mạng máy tính, cách phân loại mạng máy tính, các thiết bị hoạt động trong mạng máy tính.
- Tìm hiểu một số mô hình và dịch vụ thường sử dụng trong mạng Windows.
- Tìm hiểu về dịch vụ Distributed File System trên Windows Server 2008.

Về thực nghiệm, đồ án đã tiến hành

- Cài đặt thử nghiệm dịch vụ File Server
- Triển khai thử nghiệm hệ thống lưu trữ tập trung Distributed File System.

Tuy nhiên trong quá trình thực hiện, do năng lực còn nhiều hạn chế, cùng những nguyên nhân khách quan khác như: thời gian, cơ sở vật chất, khả năng dịch hiểu tiếng Anh trong quá trình trao đổi trên các diễn đàn công nghệ nên chắc chắn trong đồ án còn nhiều sai sót. Em rất mong nhận được sự đóng góp ý kiến của các Thầy Cô và các bạn để em có thêm kiến thức và kinh nghiệm tiếp tục hoàn thiện nội dung nghiên cứu trong đề tài.

Em xin chân thành Cảm ơn!

TÀI LIỆU THAM KHẢO

Sách tham khảo

[1] Nguyễn Hồng Sơn, "Giáo trình hệ thống mạng máy tính CCNA Semester 1", Nguyễn Hồng Sơn, NXB Lao động xã hội, 2005

[2] Nguyễn Hồng Sơn, "Giáo trình hệ thống mạng máy tính CCNA Semester 2", Nguyễn Hồng Sơn, NXB Lao động xã hội, 2005

[3] Đào Kiến Quốc, "Bài giảng mạng LAN", ĐH Công nghệ, ĐH Quốc Gia HN

[4] Hồ Đắc Phương, Mạng căn bản, NXB Đại Học Quốc Gia HN, 2006

Website

[5] http://tailieu.hpu.edu.vn/

[6] http://tailieu.tv/tai-lieu/de-tai-cac-dich-vu-mang-cua-windows-nt-server-2948/

[7] http://en.wikipedia.org/

[8] http://cameranewvn.mov.mn/bvct/

[9] http://forum.itlab.com.vn/index.php?threads/xay-dung-cau-truc-dfs.1011/

[10] http://www.quantrimang.com.vn/

[11] http://technet.microsoft.com/en-us/ms772425