PHỤ LỤC B: HỆ ĐIỀU HÀNH MẠNG WINDOWS NT VÀ HỆ THỐNG QUẢN LÝ CỦA WINDOWS NT

Nội dung

- Hệ điều hành mạng Windows NT.
- Hệ thống quản lý của Windows NT.

Hướng dẫn học

- Đọc tài liệu, nắm bắt các nội dung chính.
- Làm bài tập và luyện thi trắc nghiệm theo yêu cầu của từng bài.

Mục tiêu

Sau khi học bài này, các bạn có thể:

Trình bày được khái niệm về hệ điều hành Windows NT cũng như hệ thống quản lý của nó.

TÌNH HUỐNG DẪN NHẬP

Tình huống

Các máy tính trong công ty Hoàng Nam được ghép nối với nhau thành một mạng máy tính. Để quản lý tài nguyên trong mạng, xử lý các truy cập một cách thống nhất trong toàn mạng máy tính của công ty cần có hệ thống phần mềm quản lý. Công ty Hoàng Nam lựa chọn hệ điều hành mạng Windows NT để quản lý các tác vụ trên.

Câu hỏi

1. Cấu trúc hệ điều hành mạng Windows NT như thế nào?
2. Hệ điều hành Windows NT hỗ trợ những cách nào để tổ chức các tài nguyên trong mạng?

B.1 Hệ điều hành mạng Windows NT

B.1.1 Thế nào là một hệ điều hành mạng

Với việc ghép nối các máy tính thành mạng thì cần thiết phải có một hệ thống phần mềm có chức năng quản lý tài nguyên, tính toán và xử lý truy cập một cách thống nhất trên mạng, hệ như vậy được gọi là hệ điều hành mạng. Mỗi tài nguyên của mạng như tệp, đĩa, thiết bị ngoại vi được quản lý bởi một tiến trình nhất định và hệ điều hành mạng điều khiển sự tương tác giữa các tiến trình và truy cập tới các tiến trình đó.

Căn cứ vào việc truy cập tài nguyên trên mạng người ta chia các thực thể trong mạng thành hai loại chủ và khách, trong đó máy khách (Client) truy cập được vào tài nguyên của mạng nhưng không chia sẻ tài nguyên của nó với mạng, còn máy chủ (Server) là máy tính nằm trên mạng và chia sẻ tài nguyên của nó với các người dùng mạng.

Hiện nay các hệ điều hành mạng thường được chia làm hai loại là hệ điều hành mạng ngang hàng (Peer-to-peer) và hệ điều hành mạng khách/chủ (client/server).

Với hệ điều hành mạng ngang hàng mỗi máy tính trên mạng có thể vừa đóng vai trò chủ lẫn khách tức là chúng vừa có thể sử dụng tài nguyên của mạng lẫn chia sẻ tài nguyên của nó cho mạng, ví dụ: LANtastic của Artisoft, NetWare lite của Novell, Windows (for WorkGroup, 95, NT Client) của Microsoft.

Với hệ điều hành mạng khách/chủ các máy tính được phân biệt chủ và khách, trong đó máy chủ mạng (Server) giữ vai trò chủ và các máy cho người sử dụng giữ vai trò khách (các trạm). Khi có nhu cầu truy cập tài nguyên trên mạng các trạm tạo ra các yêu cầu và gửi chúng tới máy chủ sau đó máy chủ thực hiện và gửi trả lời. Ví dụ các hệ điều hành mạng phân biệt: Novell Netware, LAN Manager của Microsoft, Windows NT Server của Microsoft, LAN Server của IBM, Vines của Banyan System với server dùng hệ điều hành Unix.

B.1.2 Hệ điều hành mạng Windows NT

Windows NT là hệ điều hành mạng cao cấp của hãng Microsoft. Phiên bản đầu có tên là Windows NT 3.1 phát hành năm 1993, và phiên bản server là Windows NT Advanced Server (trước đó là LAN Manager for NT). Năm 1994 phiên bản Windows

NT Server và Windows NT Workstation version 3.5 được phát hành. Tiếp theo đó ra đời các bản version 3.51. Các phiên bản Workstation có sử dụng để thành lập mạng ngang hàng; còn các bản server dành cho quản lý file tập trung, in ấn và chia sẻ các ứng dụng.

Năm 1995, Windows NT Workstation và Windows NT Server version 4.0 ra đời đã kết hợp shell của người anh em Windows 95 nổi tiếng phát hành trước đó không lâu (trước đây shell của Windows NT giống shell của Windows 3.1) đã kết hợp được giao diện quen thuộc, dễ sử dụng của Windows 95 và sự mạnh mẽ, an toàn, bảo mật cao của Windows NT.

Windows NT có hai bản mà nó đi đôi với hai cách tiếp cận mạng khác nhau. Hai bản này gọi là Windows NT Workstation và Windows NT server. Với hệ điều hành chuẩn của NT ta có thể xây dựng mạng ngang hàng, máy chủ mạng và mọi công cụ quản trị cần thiết cho một máy chủ mạng ngoài ra còn có thể có nhiều giải pháp về xây dựng mạng diện rộng. Cả hai bản Windows NT station và Windows NT server cùng được xây dựng trên cơ sở nhân NT chung và các giao diện và cả hai cùng có những đặc trưng an toàn theo tiêu chuẩn C2. Windows NT Wordstation được sử dụng để kết nối những nhóm người sử dụng nhỏ, thường cùng làm việc trong một văn phòng. Tuy nhiên với Windows NT server ta có được một khả năng chống hỏng hóc cao, những khả năng cung cấp dịch vụ mạng lớn và những lựa chon kết nối khác nhau, Windows NT Server không hạn chế về số người có thể thâm nhập vào mạng.

Với Windows NT ta cũng có những công cụ quản trị từ xa vào mạng mà có thể thực hiện được việc quản trị từ những máy tính ở xa. Nó thích hợp với tất cả các sơ đồ mạng BUS, STAR, RING và hỗn hợp.

Windows NT là hệ điều hành có sức mạnh công nghiệp đầu tiên cho số lượng khổng lồ các máy tính IBM compatible. Windows NT là một hệ điều hành thực sự dành cho người sử dụng, các cơ quan, các công ty xí nghiệp. Windows NT là một hệ điều hành đa nhiệm, đa xử lý với địa chỉ 32 bit bộ nhớ. Nó yểm trợ các ứng dụng DOS, Windows, Win32 GUI và các ứng dụng dựa trên ký tự. Windows NT server là một hệ điều hành mạng hoàn chỉnh, nó nhanh chóng được thừa nhận là một trong những hệ điều hành tốt nhất hiện nay vì:

- Là hệ điều hành mạng đáp ứng tất cả các giao thức truyền thông phổ dụng nhất. Ngoài ra nó vừa cho phép giao lưu giữa các máy trong mạng, vừa cho phép truy cập từ xa, cho phép truyền file v.v... Windows NT là hệ điều hành vừa đáp ứng cho mạng cục bộ (LAN) vừa đáp ứng cho mạng diện rộng (WAN) như Intranet, Internet.
- Windows NT server hơn hẳn các hệ điều hành khác bởi tính mềm dẻo, đa dạng trong quản lý. Nó vừa cho phép quản lý mạng theo mô hình mạng phân biệt (Clien/Server), vừa cho phép quản lý theo mô hình mạng ngang hàng (peer to peer).
- Windows NT server đáp ứng tốt nhất các dịch vụ viễn thông, một dịch vụ được sử dụng rộng rãi trong tương lai.
- Windows NT server cài đặt đơn giản, nhẹ nhàng và điều quan trọng nhất là nó tương thích với hầu như tất cả các hệ mạng, nó không đòi hỏi người ta phải thay đổi những gì đã có.

- Cho phép dùng các dịch vụ truy cập từ xa (Remote access service - RAS), có khả năng phụp vụ đến 64 cổng truy cập từ xa (trong đó Lan manager 16 cổng).
- Đáp ứng cho cả các máy trạm Macintosh nối với Windows NT server.

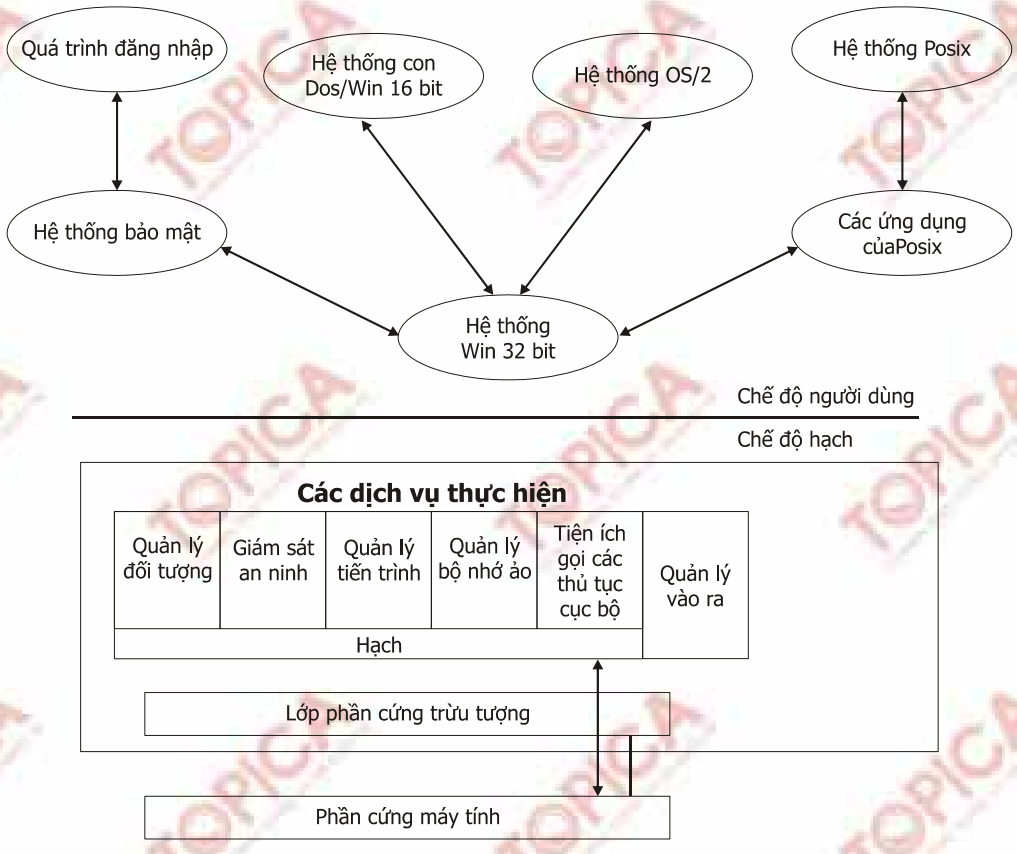
Windows NT yểm trợ mọi nghi thức mạng chuẩn như NetBUEI, IPX/SPX, TCP/IP và các nghi thức khác. Windows NT cũng tương thích với những mạng thông dụng hiên nay như Novell NetWare, Banyan VINES, và Microsoft LAN Manager. Đối với mạng lớn và khả năng thâm nhập từ xa sản phẩm Windows NT Server cũng cũng cấp các chức năng bổ sung nhu khả năng kết nối với máy tính lớn và máy MAC.

B.1.3. Cấu trúc của hê điều hành mạng Windows NT

Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular). Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của Windows NT được trình bày trong hình B1 Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (cốt lõi của hệ điều hành). Khi một thành phần của hệ điều hành chạy dưới cốt lõi của hệ điều hành (Kernel), nó truy cập đầy đủ các chỉ thị máy cho bộ xử lý đó và có thể truy cập tổng quát toàn bộ tài nguyên trên hệ thống máy tính.

Trong Windows NT: Executive Services, Kernel và HAL chạy dưới chế độ cốt lõi của hệ điều hành.

Hệ thống con (Sub system) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ User. Bằng cách đặt các hệ thống con này trong chế độ User, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.



Hình B.1: ***Cấu trúc Windows NT***

Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:

- Lớp phần cứng trừu tượng (Hardware Astraction Layer - HAL): Là phần cứng máy tính mà cốt lõi của hệ điều hành (Kernel) có thể được ghi vào giao diện phần cứng ảo, thay vì vào phần cứng máy tính thực sự. Phần lớn cốt lõi của hệ điều hành sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là cốt lõi của hệ điều hành và tất cả các thành phần khác phụ thuộc vào cốt lõi có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền (Platform) phần cứng khác. Một thành phần nhỏ trong cốt lõi của hệ điều hành, cũng như bộ quản lý Nhập / Xuất truy cập phần cứng máy tính trực tiếp mà không cần bao gồm HAL.
- Lớp Kernel (cốt lõi của hệ điều hành): Cung cấp các chức năng hệ điều hành cơ bản được sử dụng bởi các thành phần thực thi khác. Thành phần Kernel tương đối nhỏ và cung cấp các thành phần cốt yếu cho những chức năng của hệ điều hành. Kernel chủ yếu chịu trách nhiệm quản lý luồng, quản lý phần cứng và đồng bộ đa xử lý.
- Các thành phần Executive: Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như:
  - Quản lý đối tượng (Object Manager).
  - Bảo mật (Security Reference Monitor).
  - Quản lý tiến trình (Process Manager).
  - Quản lý bộ nhớ ảo (Virtual Memory Manager).
  - Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager).

B.1.4. Cơ chế quản lý của hệ điều hành Windows NT

B.1.4.1. Quản lý đối tượng (Object Manager)

Tất cả tài nguyên của hệ điều hành được thực thi như các đối tượng. Một đối tượng là một đại diện trừu tượng của một tài nguyên. Nó mô tả trạng thái bên trong và các tham số của tài nguyên và tập hợp các phương thức (method) có thể được sử dụng để truy cập và điều khiển đối tượng.

Ví dụ một đối tượng tập tin sẽ có một tên tập tin, thông tin trạng thái trên file và danh sách các phương thức, như tạo, mở, đóng và xóa, đối tượng mô tả các thao tác có thể được thực hiện trên đối tượng file.

Bằng cách xử lý toàn bộ tài nguyên như đối tượng Windows NT có thể thực hiện các phương thức giống nhau như: tạo đối tượng, bảo vệ đối tượng, giám sát việc sử dụng đối tượng (Client object) giám sát những tài nguyên được sử dụng bởi một đối tượng.

Việc quản lý đối tượng (Object Manager) cung cấp một hệ thống đặt tên phân cấp cho tất cả các đối tượng trong hệ thống. Do đó, tên đối tượng tồn tại như một phần của không gian tên toàn cục và được sử dụng để theo dõi việc tạo và sử dụng đối tượng.

Sau đây là một số ví dụ của loại đối tượng Windows NT:

- Đối tượng thư mục (Directory).
- Đối tượng tập tin (File).
- Đối tượng kiểu object.
- Đối tượng tiến trình (Process).

- Đối tượng luồng (Thread).
- Đối tượng mô tả bộ nhớ (Section and segment).
- Đối tượng cổng (Port).
- Đối tượng Semaphore và biến cố.
- Đối tượng liên kết ký hiệu (Symbolic).

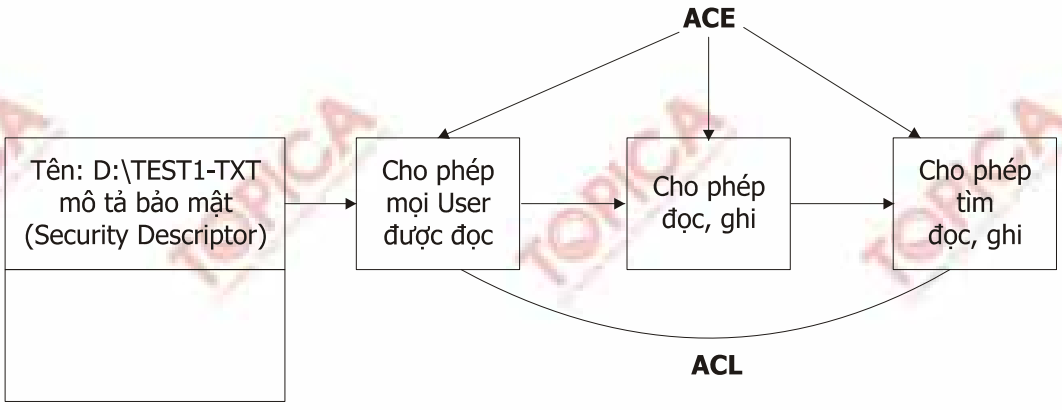
B.1.4.2. Cơ chế bảo mật (SRM – Security Reference Monitor)

Được sử dụng để thực hiện vấn đề an ninh trong hệ thống Windows NT. Các yêu cầu tạo một đối tượng phải được chuyển qua SRM để quyết định việc truy cập tài nguyên được cho phép hay không. SRM làm việc với hệ thống con bảo mật trong chế độ User. Hệ thống con này được sử dụng để xác nhận User login vào hệ thống Windows NT.

Để kiểm soát việc truy cập, mỗi đối tượng Windows NT có một danh sách an toàn (Access Control List - ACL). Danh sách an toàn của mỗi đối tượng gồm những phần tử riêng biệt gọi là Access Control Entry (ACE). Mỗi ACE chứa một SecurityID (SID: số hiệu an toàn) của người sử dụng hoặc nhóm. Một SID là một số bên trong sử dụng với máy tính Windows NT mô tả một người sử dụng hoặc một nhóm duy nhất giữa các máy tính Windows NT.

Ngoài SID, ACE chứa một danh sách các hành động (action) được cho phép hoặc bị từ chối của một User hoặc một nhóm. Khi người sử dụng đăng nhập vào mạng Windows NT, sau khi việc nhận dạng thành công, một Security Access Token (SAT) được tạo cho người dùng đó. SAT chứa SID của người dùng và SID của tất cả các nhóm người dùng thuộc mạng Windows NT. Sau đó SAT hoạt động như một "thẻ chuyển" (passcard) cho phiên làm việc của người dùng đó và được sử dụng để kiểm tra tất cả hoạt động của người dùng.

Khi người dùng tham gia mạng truy cập một đối tượng, Security Reference Monitor kiểm tra bộ mô tả bảo mật của đối tượng xem SID liệt kê trong SAT có phù hợp với giá trị trong ACE không. Nếu phù hợp, các quyền về an ninh được liệt trong ACE áp dụng cho người dùng đó.



Hình B.2: ***Ví dụ về danh sách an toàn (Access Control List).***

B.1.4.3. Quản lý nhập/xuất (I/O Manager)

Chịu trách nhiệm cho toàn bộ các chức năng nhập / xuất trong hệ điều hành Windows NT. I/O Manager liên lạc với trình điều khiển của các thiết bị khác nhau.

B.1.4.4. I/O Manager

Sử dụng một kiến trúc lớp cho các trình điều khiển. Mỗi bộ phận điều khiển trong lớp này thực hiện một chức năng được xác định rõ. Phương pháp tiếp cận này cho phép một thành phần điều khiển được thay thế dễ dàng mà không ảnh hưởng phần còn lại của các bộ phận điều khiển.

Hình B.3: ***Các trình điều khiển thiết bị theo lớp của I / O Manager***

B.1.5. Các cơ chế bảo vệ dữ liệu trong Windows NT

Cơ chế bảo vệ dữ liệu của Windows NT gọi là fault tolerance, nó cho phép hệ thống khả năng tiếp tục làm việc và bảo toàn dữ liệu của hệ thống trong trường hợp một phần của hệ thống có sự cố hỏng hóc sai lệch. Trong Windows NT cơ chế fault tolerance bao gồm các biện pháp sau:

- Chống cúp điện bất thường.
- Cung cấp khả năng bảo vệ hệ thống đĩa (Fault Tolerance Disk Subsystem).
- Cung cấp khả năng sao chép dự phòng (backup) từ băng từ.

Khả năng bảo vệ hệ thống đĩa của Windows NT là RAID (viết tắt của Redundant Array of Inexpensiredisk). Thực chất RAID là một loạt các biện pháp để bảo vệ hệ thống đĩa. Các biện pháp trong RIAD được chia thành 6 mức sau:

- Mức 0: Đây là mức ứng với biện pháp chia nhỏ đĩa (Disk Striping). Thực chất nội dung của biện pháp này là phân chia dữ liệu thành khối và sau đó sắp xếp các khối dữ liệu theo thứ tự trong tất cả các đĩa thành 1 mảng.
- Mức 1: Mức này ứng với biện pháp disk Mirroring, biện pháp này cho phép tạo ra 2 đĩa giống nhau. Nếu trong quá trình vận hành mạng một đĩa có sự cố thì hệ thống sử dụng dữ liệu của đĩa kia.
- Mức 2: Mức này ứng với biện pháp phân chia nhỏ đĩa bằng cách phân chia các file thành các byte và sắp xếp các byte sang nhiều đĩa. Mức này sử dụng mã sửa sai (Error Correcting Code) trong quá trình phân chia đĩa. Nói chung biện pháp dùng ở mức này tốt hơn biện pháp dùng trong mức 1.

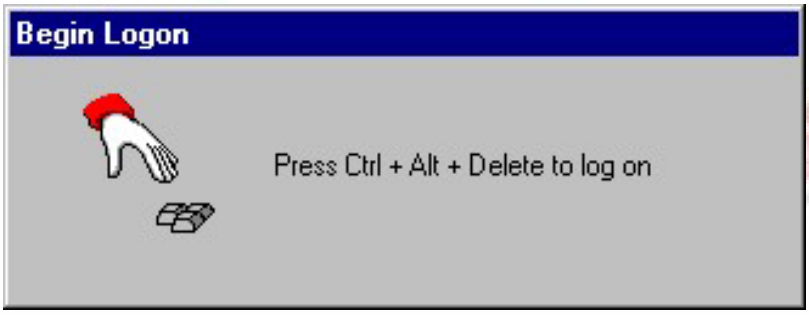
- Mức 3: Mức này sử dụng biện pháp giống mức 2. Tuy nhiên mã sửa sai (Error Correction Code) chỉ sử dụng cho một đĩa. Không áp dụng cho nhiều đĩa như ở mức 2. Người ta thường dùng mức này để truy cập vào một số ít file có dung tích lớn.
- Mức 4: Mức này sử dụng biện pháp giống ở mức 2 và 3 nhưng bằng phương pháp phân chia đĩa thành các khối lớn. Giống như mức 3 tất cả các mã sửa sai (Error Correction Code) được ghi vào một đĩa và tách khỏi khối dữ liệu.
- Mức 5: Trong mức này người ta sử dụng biện pháp phân chia đĩa thành từng phần gọi là Striping with party. Biện pháp sử dụng ở mức này tương tự như mức 4, số liệu được phân nhỏ thành các khối lớn và sau đó ghi vào tất cả các đĩa. Các thông tin (Party Infomation) được coi như các dữ liệu dùng tạm thời (Data Redundancy).

Ngoài ra chúng ta còn có thể áp dụng các biện pháp bảo vệ dữ liệu trong Windows NT:

- Biện pháp Disk mirroring: Disk mirroring là cách sao tạm (Redundant) lại đĩa hoặc partition. Biện pháp này bảo vệ dữ liệu tránh sự cố bằng cách đưa ra chế độ thường xuyên backup đĩa hoặc partition.
- Disk Duplexing: Biện pháp dùng đĩa kép (Disk Duplexing) tương tự như disk mirroring chỉ khác là chúng dùng 2 disk controler. Điều này cho thêm khả năng bảo vệ khi controler của một đĩa có sự cố. Trong khi đó biện pháp Mirror không thể khắc phục được tình huống này.
- Mirror Set: Các partition hoặc đĩa trong chế độ Mirror được tạo ra bằng cách lặp sao lại partition hoặc đĩa trên đĩa khác cùng một tên ổ đĩa được gán cho cả 2 partition. Ta có thể dùng establish Mirror trong bảng chọn Fault tolerance. Nếu đĩa hoặc partition trong chế độ Mirror bị lỗi thì chế độ Mirror cần phải ngắt để thực hiện chế độ sao chép dự phòng vào một đĩa riệng. Sau đó sao backup trở lại.

B.1.6. Giới thiệu về hoạt động của Windows NT Server

Khi chúng ta khởi động Windows NT Server hộp thoại Begin logon sẽ hiện ra, server chờ đợi để chúng ta nhấn Ctrl+Alt +Del để có thể tiếp tục hoạt động. Ở đây có điểm khác với các hệ điều hành DOS, Windows 95 là tổ hợp Ctrl+Alt +Del không phải là khởi động lại máy. Trong trường hợp này Windows NT loại bỏ mọi chương trình Virus hay không có phép đang hoạt động trước khi bước vào làm việc.



Hình B.4: ***Thông báo gia nhập mạng***

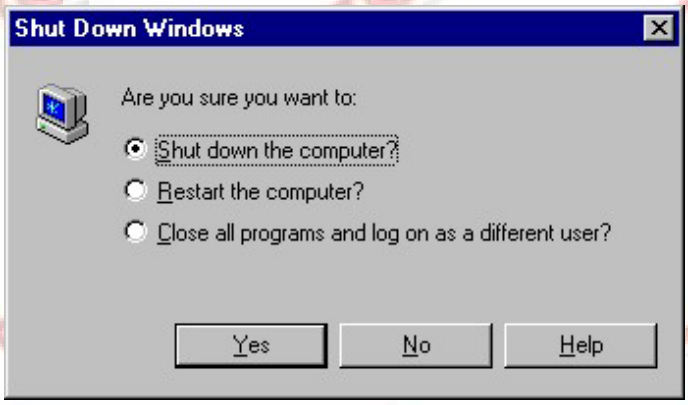
Lúc này chúng ta sẽ thấy hộp thoại Logon Information xuất hiện và yêu cầu chúng ta phải gõ đúng tên và mật khẩu thì mới được đăng nhập vào Server. Nếu là người dùng mới thì phải được người quản trị khai báo tên và mật khẩu trước khi đăng nhập.

Hình B.5: ***Màn hình đăng nhập mạng***

Cũng giống như màn hình nền của hệ điều hành Windows 95 khi muốn thực hiện các trình, gọi các bảng chọn hệ thống chúng ta dùng nút Start ở cuối màn hình

Hình B.6: ***Điểm khởi đầu của Windows***

Trước khi muốn kết thúc chương trình và tắt máy chúng ta phải nháy Start rồi chọn ShutDown, màn hình kết thúc sẽ hiện ra cho chúng ta lựa chon công yêu cầu về tắt hay khởi động lại.



Hình B.7: ***Màn hình thoát khỏi Windows***

B.2. Hệ thống quản lý của Windows NT

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): 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 có một tên login và mật khẩu duy nhất.
- Mức quản lý trong việc 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.

B.2.1. Quản lý các tài nguyên trong mạng

Như chúng ta đã biết, 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 giúp người sử dụng xác định được các tài nguyên có sẵn ở đâu để có thể sử dụng.

Các kỹ thuật sau đây đã được sử dụng để tổ chức tài nguyên mạng máy tính:

- Quản lý đơn lẻ từng máy chủ (Stand-Alone Services).
- Quản lý theo dịch vụ thư mục (Directory Services).
- Quản lý theo nhóm (WorkGroups).
- Quản lý theo Domain (Domains).

B.2.1.1. Quản lý đơn lẻ từng máy chủ (Stand – Alone Services)

Với cách quản lý này trong mạng LAN thường chỉ có một vài máy chủ, mỗi máy chủ sẽ quản lý tài nguyên của mình, mỗi người sử dụng muốn thâm nhập những tài nguyên của máy chủ nào thì phải khai báo và chịu sự quản lý của máy chủ đó. Mô hình trên phù hợp với những mạng nhỏ với ít máy chủ và khi có trục trặc trên một máy chủ thì toàn mạng vẫn hoạt động. Cũng vì trong mạng LAN chỉ có ít máy chủ, do đó người sử dụng không mấy khó khăn để tìm các tập tin, máy in và các tài nguyên khác của mạng (Plotter, CDRom, Modem...).

Việc tổ chức như vậy không cần những dịch vụ quản lý tài nguyên phức tạp. Tuy nhiên khi trong mạng có từ hai máy chủ trở lên vấn đề trở nên phức tạp hơn vì mỗi máy chủ riêng lẻ giữ riêng bảng danh sách các người sử dụng và tài nguyên của mình. Khi đó mỗi người sử dụng phải tạo lập và bảo trì tài khoản của mình ở hai máy chủ khác nhau mới có thể đăng nhập (Logon) và truy xuất đến các máy chủ này. Ngoài ra việc xác định vị trí của các tài nguyên trong mạng cũng rất khó khăn khi mạng có quy mô lớn.

B.2.1.2. Quản lý theo dịch vụ thư mục (Directory Services)

Hệ thống các dịch vụ thư mục cho phép làm việc với mạng như là một hệ thống thống nhất, tài nguyên mạng được nhóm lại một cách lôgic để dễ tìm hơn. Giải pháp này có thể được dùng cho những mạng lớn. Ở đây thay vì phải đăng nhập vào nhiều máy chủ,

người sử dụng chỉ cần đăng nhập vào mạng và được các dịch vụ thư mục cấp quyền truy cập đến tài nguyên mạng, cho dù được cung cấp bởi bất kể máy chủ nào.

Người quản trị mạng chỉ cần thực hiện công việc của mình tại một trạm trên mạng mặc dù các điểm nút của nó có thể nằm trên cả thế giới. Hệ điều hành Netware 4.x cung cấp dịch vụ nổi tiếng và đầy ưu thế cạnh tranh này với tên gọi Netware Directory Services (NDS).

Giải pháp này thích hợp với những mạng lớn. Các thông tin của NDS được đặt trong một hệ thống cơ sở dữ liệu đồng bộ, rộng khắp được gọi là DIB (Data Information Base). Cơ sở dữ liệu trên quản lý các dữ liệu dưới dạng các đối tượng phân biệt trên toàn mạng. Các định nghĩa đối tượng sẽ được đặt trên các tập tin riêng của một số máy chủ đặc biệt, mỗi đối tượng có các tính chất và giá trị của mỗi tính chất. Đối tượng bao hàm tất cả những gì có tên phân biệt như Người sử dụng, File server, Print server, Group. Mỗi loại đối tượng có những tính chất khác nhau ví dụ như đối tượng Người sử dụng có tính chất về nhóm mà người sử dụng đó thuộc, còn nhóm có các tính chất về người sử dụng mà nhóm đó chứa.

Việc thiết lập các dịch vụ như vậy cần được lập kế hoạch, thiết kế rất cẩn thận, liên quan đến tất cả các đơn vị phòng ban có liên quan. Loại mạng này có khuyết điểm là việc thiết kế, thiết lập mạng rất phức tạp, mất nhiều thời gian nên không thích hợp cho các mạng nhỏ.

B.2.1.3. Quản lý theo nhóm (WorkGroup)

Các nhóm làm việc làm việc theo ý tưởng ngược lại với các dịch vụ thư mục. Nhóm 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.

WorkGroup là nhóm lôgic 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.

Nhưng workGroup cũng có điểm là đơn giản, tiện lợi và chia sẻ tài nguyên hiệu quả, do đó thích hợp với các mạng nhỏ, gồm các nhóm người sử dụng tương tự nhau.

Tuy nhiên WorkGroup dựa trên cơ sở mạng ngang hàng (Peer-to-Peer), nên có hai trở ngại đối với các mạng lớn như sau:

- Đối với mạng lớn, có quá nhiều tài nguyên có sẵn trên mạng làm cho các người sử dụng khó xác định chúng để khai thác.

- Người sử dụng muốn chia sẻ tài nguyên thường sử dụng một cách dễ hơn để chia sẻ tài nguyên chỉ với một số hạn chế người sử dụng khác.

Điển hình cho loại mạng này là Windows for WorkGroups, LANtastic, LAN Manager... Window 95, Windows NT Workstation.

B.2.1.4. Quản lý theo vùng (Domain)

Domain mượn ý tưởng từ thư mục và nhóm làm việc. Giống như một workGroup, Domain có thể được quản trị bằng hỗn hợp các biện pháp quản lý tập trung và địa phương. Domain là một tập hợp các máy tính dùng chung một nguyên tắc bảo mật và CSDL tài khoản người dùng (người sử dụng 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.

Giống 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 NT Server trên mạng. Một máy tính Windows NT 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:

- Mã số của người sử dụng được quản lý tập trung ở một nơi trong một cơ sở dữ liệu của máy chủ, do vậy quản lý chặt chẽ hơn.
- Các nguồn tài nguyên cục bộ được nhóm vào trong một Domain nên dễ khai thác hơn.

Quản lý theo WorkGroup và Domain là hai mô hình mà Windows NT lựa chọn. Sự khác nhau căn bản giữa WorkGroup và Domain là trong một Domain phải có ít nhất một máy chủ (máy chủ) và tài nguyên người sử dụng phải được quản lý bởi máy chủ đó.

B.2.2. Hệ thống quản lý trên Hệ điều hành mạng Windows NT Server

Windows NT cung cấp những chức năng tuân theo chuẩn C2 (chuẩn về an toàn quốc tế) trong đó Windows NT đảm bảo tránh được những người không được phép vào trong hệ thống hoặc thâm nhập vào các file và chương trình trên đĩa cứng. Người ta không thể thâm nhập vào được nếu không có mật khẩu đúng và qua đó đã bảo vệ được các file. Windows NT cung cấp công cụ để xây dựng các lớp quyền dành cho nhiều nhiệm vụ khác nhau nhằm xây dựng hệ thống an toàn một cách mềm dẻo.

Nhiều người sử dụng có thể có quyền vào một máy chủ Windows NT. Một tài khoản của người sử dụng trên máy bao gồm tên, mật khẩu và nhiều tính chất được cho bởi người quản trị mạng. Người sử dụng có thể che các thư mục hay file của mình từ những người khác và cài đặt các thông số của File manager, Programe Manager, Control Panel một cách phù hợp.

Khi người dùng thâm nhập vào hệ thống thì tự động khởi động mọi thông số đã được lưu trữ từ trước. Nếu người sử dụng có quyền cao hơn thì họ có thể chia sẻ hoặc ngừng các tài nguyên đang dùng chung trên mạng như máy in hay file hoặc họ có thể thay đổi quyền của những người dùng mạng khác khi thâm nhập vào mạng.

B.2.2.1. Mô hình WorkGroup (nhóm) của mạng Windows NT

Mỗi người truy cập vào mạng Windows NT tổ chức theo mô hình WorkGroup cần phải đăng ký:

- Tên vào mạng.
- Mật khẩu vào mạng.

Dựa vào tên và mật khẩu đã cho, Windows NT 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 cập 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.

Chú ý: Mỗi người khai thác mạng phải nhớ nhiều mã số, vì ứng với mỗi máy trạm có một hệ thống quản trị tài nguyên riêng của nó.

B.2.2.2. Mô hình vùng (Domain)

Domain là một khái niệm rất cơ bản trong Windows NT server, nó là hạt nhân để tổ chức các mạng có quy mô lớn.

Mỗi người tham gia trong Domain cần phải đăng ký thông tin sau:

- Tên Domain.
- Tên người sử dụng.
- 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 cập 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 cập vào tài nguyên của Domain.

Một máy Windows NT mà không tham gia vào một Domain có nhược điểm sau:

- 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 cập 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 Máy chủ.

- Qua máy trạm không tham gia vào Domain, người khai thác mạng không thể truy cập 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.
- Ngoài ra hệ thống còn có một hay nhiều máy làm Backup Domain Controller (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 động copy đến các máy Backup Domain Controller.

B.2.2.3. Mô hình quan hệ giữa các Domain trong mạng Windows NT

Trong một mạng có thể có nhiều Domain nhưng một máy tính Windows NT là thành viên của chỉ một Domain tại mỗi thời điểm. Tuy nhiên, có một vài trường hợp đôi khi chúng ta cần truy cập tài nguyên trong những Domain khác, để là được điều này hệ điều hành Windows NT server cho phép giữa các Domain có thể tồn tại một quan hệ gọi là quan hệ tin cậy (Trust Relationship). Chúng ta có thể sử dụng quan hệ tin cậy giữa các Domain cho phép người dùng trên một Domain truy cập tài nguyên trong Domain khác.

Hai Domain A, B gọi là quan hệ tin cậy (trust relationship) mà trong đó Domain A tin cậy Domain B nếu giữa chúng có một mối liên kết sao cho người khai thác mạng của Domain B có thể truy cập vào Domain A từ một máy trạm trong Domain B.

Từ góc độ của người quản trị mạng mục đích của việc thiết lập quan hệ tin cậy giữa các Domain là làm cho việc quản lý mạng trở lên đơn giản hơn bằng cách kết hợp các Domain vào một đơn vị quản lý. Trong quan hệ tin cậy các Domain được chia ra như sau:

- Domain được tin cậy (Trusted Domain).
- Domain tin cậy (Trusting Domain).

Một Domain là loại này hoặc loại kia thông thường phụ thuộc vào nó chứa mã số của người sử dụng (người sử dụng Account) hay chỉ chứa tài nguyên (Resource):

- Domain tin cậy (Trusting Domain) là Domain chứa tài nguyên.
- Domain được tin cậy (Trusted Domain) là Domain chứa mã số người sử dụng.

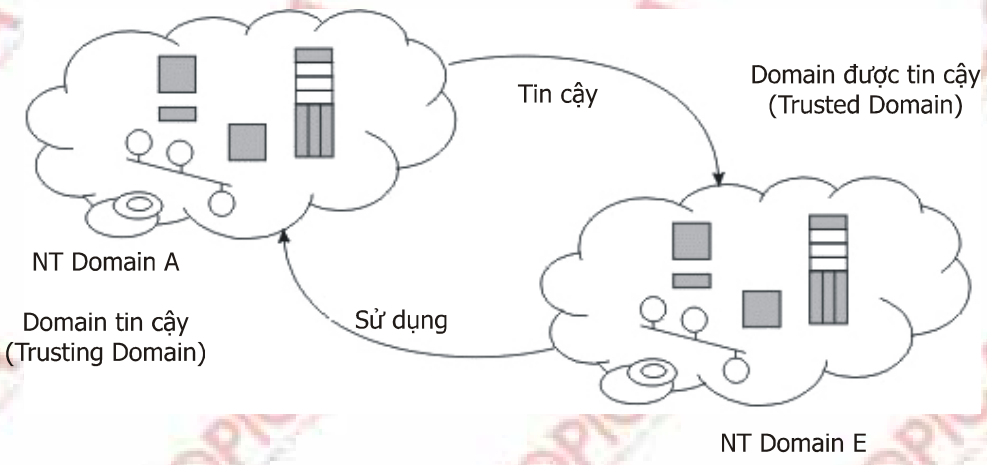
Khi người sử dụng truy cập từ một máy trạm trong Domain tin cậy (Trusting DDomain) vào Domain được tin cậy (Trusted Domain) thì quá trình kiểm soát diễn ra như sau:

- Người sử dụng cho mã số (mã số này ứng với tên, mật khẩu, tên Domain cần truy cập).
- Mã số được chuyển về máy chủ của Domain tin cậy.
- Máy chủ của Domain tin cậy chuyển mã số này sang Domain được tin cậy.

- Kết quả kiểm tra của máy chủ trong Domain được tin cậy diễn ra theo quá trình ngược lại.

Ở đây chúng ta chú ý:

- Việc liên kết giữa các Domain không có tính bắc cầu.
- Thông qua việc thiết lập mối quan hệ tin tưởng, chúng ta có thể sử dụng một tài khoản để truy xuất đến nhiều tài nguyên của nhiều Domain. Có thể quản trị nhiều Domain từ một vị trí tập trung.



Hình B.8: ***Mô hình tin cậy của các Domain trong mạng Windows NT***

B.2.2.4. Nhóm (Group) trong Windows NT

Trong mạng Windows NT khái niệm nhóm (Group) là một trong những khái niệm quan trọng đối với công việc quản lý, điều hành mạng Windows NT. Nhóm làm cho việc khai thác tài nguyên được dễ dàng thuận lợi và đơn giản hóa việc quản trị. Mỗi nhóm được đăng ký bởi một tài khoản (Group Account) và có các thành viên của nó. Các quyền đã được gán cho nhóm sẽ tự động gán cho các người sử dụng là thành viên của nhóm. Các tiện lợi của nhóm như sau:

- Quyền có thể được gán cho, hoặc hủy đi trên mọi thành viên của nhóm.
- Khi một người sử dụng bị loại ra khỏi nhóm, thì tự động bị mất các quyền đã được cấp khi còn trong nhóm.

Trong mạng Windows NT người ta phân biệt phân biệt hai loại nhóm là nhóm toàn cục (Global Group) và nhóm cục bộ (Local Group).

B.2.2.5. Nhóm toàn cục (Global Group)

Nhóm toàn cục còn được gọi là nhóm vùng (Domain Group). Thành viên của nhóm là các người dùng cấp vùng (Domain User). Họ ngược lại với người dùng cục bộ (Local User) là người có phạm vi giới hạn trong máy tính mà họ được xác định. Thành viên của nhóm toàn cục được phép chuyển ra ngoài (Export) một Domain khác. Phạm vi của nhóm toàn cục là toàn bộ vùng trên đó User dược xác định, và thấy được từ bất kỳ máy tính NT nào trong vùng đó. Quyền có thể được gán cho nhóm toàn cục cho các tài nguyên trên một máy NT Server hay NT Workstation trong vùng.

Các tài khoản nhóm toàn cục được lưu ở PDC (Primary DomainController) của Domain, và được sao lưu đến các BDC (Backup Domain Controller) trong Domain đó.

Nhóm toàn cục có những đặc trưng sau:

- Thành viên của nhóm phải là các người sử dụng của Domain (Domain User Account).
- Nhóm toàn cục có thể được gán quyền cho tài nguyên bất kỳ trong vùng mà chúng được xác định.
- Nhóm toàn cục có thể được gán quyền đến các tài nguyên trong vùng khác với vùng chúng được xác định khi quan hệ tin cậy (Trust Relationship) giữa các vùng có hiệu lực.
- Các thành viên của nhóm toàn cục có thể sử dụng nguồn tài nguyên trong vùng bất kỳ mà nhóm toàn cục có quyền.
- Nhóm toàn cục chỉ chứa mã số của người sử dụng trong Domain của nó. Nó không thể chứa các nhóm cục bộ và nhóm toàn cục khác.

B.2.2.6. Nhóm cục bộ (Local Group)

Nhóm cục bộ, trái lại, được gán quyền cho nguồn tài nguyên trên máy NT mà nó được xác định. Nếu máy NT là một phần của vùng, thì để tiện cho việc gán quyền, một nhóm cục bộ có thể chứa các tài khoản người dùng cấp vùng (Domain User Account) và các nhóm toàn cục trong Domain đó, nơi máy tính NT là thành viên, hoặc những người dùng từ Domain được tin cậy. Các người dùng cấp vùng (Domain User) có thể được gán quyền truy cập đến tài nguyên bất kỳ trong Domain đó.

Nếu Windows NT computer không nối với mạng thì các thành viên trong Local Group có thể được gán quyền để truy xuất đến tài nguyên trên máy tính mà trong đó các thành viên được tạo ra còn nếu Windows NT computer nối vào mạng thì để tiện lợi cho việc phân quyền thì người quản trị mạng có thể đưa global Group và Domain User vào trong Local Group.

Có hai loại nhóm cục bộ: nhóm cục bộ trạm làm việc (Workstation Local Group) và nhóm cục bộ vùng (Domain Local Group). Một mạng làm việc theo cơ chế vùng bao gồm cả Windows NT Server và Windows NT Workstation việc hiểu rõ sự khác nhau giữa hai loại nhóm cục bộ là rất quan trọng.

Nhóm cục bộ trạm làm việc (Workstation Local Group)

Nhóm cục bộ trạm làm việc hiện diện trên Windows NT Workstation trên đó chúng được tạo ra. Chúng được chứa trong dữ liệu SAM lưu trữ trên Windows NT Workstation. Một người dùng cục bộ được tạo ra bằng công cụ User Manager của Windows NT Workstation (khác với công cụ User Manager for Domains trên Windows NT Server) có thể có quan hệ thành viên chỉ trong nhóm cục bộ của trạm làm việc đó. Một nhóm cục bộ trong một trạm làm việc chỉ có thể được dùng trên máy tính trên đó nhóm được tạo ra, và không thể làm việc rên bất kỳ máy Windows NT nào khác.

Nhóm cục bộ trạm làm việc có thể chứa:

- Các tài khoản người dùng cục bộ từ trạm làm việc trên đó nó được xác định.
- Các tài khoản người dùng cấp vùng (Domain User Account) và các nhóm toàn cục từ vùng trong đó họ được xác định.
- Các tài khoản người dùng cấp vùng (Domain User Account) và các nhóm toàn cục từ các vùng được ủy quyền.

Nhóm cục bộ vùng (Domain Local Group)

Nhóm cục bộ vùng hoạt động trên Windows NT Server ở mức vùng, và được tạo ra bằng User Manager for Domains (trên Windows NT Server). Các nhóm cục bộ vùng chỉ có thể hiện hữu trên máy Windows NT Server tạo ra nó. Do đó, các nhóm cục bộ vùng có thể dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Server trong vùng đó, mà không dùng để truy cập nguồn tài nguyên trên máy tính Windows NT Workstation trong vùng này. Nhóm cục bộ vùng không thể được gán quyền trên bộ điều khiển không có cấp vùng, thậm chí cả các máy chủ.

B.2.3. Các mô hình Domain trong mạng Windows NT

Windows NT máy chủ cung cấp 4 kiểu tổ chức Domain gọi tắt là các mô hình Domain (Domain Models). Dưới đây là 4 mô hình tổ chức của nó:

- Mô hình Domain đơn (Single Domain).
- Mô hình Domain chính (Master Domain).
- Mô hình Multiple Master Domain.
- Mô hình Complete Truts.

B.2.3.1. Mô hình Domain đơn (Single Domain)

Mô hình Domain đơn là mô hình trong mạng chỉ có một Domain. Mô hình này thích hợp cho mạng ít người khai thác, cần quản lý tập trung. Mô hình đơn nói chung tương tự như mô hình WorkGroup, trong mô hình này người sử dụng có thể xem xét, khai thác tài nguyên theo cả mô hình workGroup và mô hình Domain.

Loại mô hình này không có các quan hệ ủy quyền vì chỉ có một Domain duy nhất, Domain này cũng chứa CSDL SAM cho toàn bộ mạng và việc quản trị mạng có thể thực hiện từ một vị trí trung tâm.

Các tài khoản người dùng trong vùng (Domain User Account) và tài khoản nhóm trong vùng (Domain Group acconunt) có thể được xây dựng và có các quyền truy cập tài nguyên được gán trên các nhóm và người dùng riêng rẽ và có một phạm vi bao gồm tất cả các máy vi tính trong vùng.

Trong mô hình Domain đơn vấn đề an toàn dữ liệu, quản lý hệ thống được xem xét một cách tốt hơn so với WorkGroup.

B.2.3.2. Mô hình Domain chính (Master Domain)

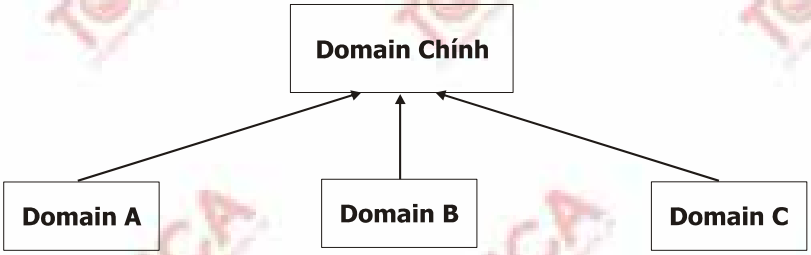
Mô hình Domain chính có thể được sử dụng cho các cơ quan khi họ muốn tổ chức mạng thành nhiều Domain tài nguyên (Resource Domain) nhưng vẫn có những tiện lợi trong việc quản lý tập trung. Bằng cách phân chia tài nguyên mạng vào nhiều Domain, chúng ta sẽ tiện tổ chức và quản lý một lượng tài nguyên lớn. Một Domain chủ (Master Domain) được sử dụng để hỗ trợ việc quản trị tập trung mà trong đó tất cả mã số của người sử dụng và mã số các nhóm toàn cục (Global Group) trên mạng được lưu giữ.

Đặc điểm của mô hình Domain chính:

- Mô hình Master Domain là mô hình có nhiều Domain, trong đó có 1 Domain là Domain chính (Premery Domain). Mô hình này thích hợp cho mạng có số người dùng không quá lớn, nhưng cần phải phân chia thành các đơn vị nhỏ hơn nhưng việc quản lý được tiến hành tập trung.

- Trong mô hình này tất cả mã số của người khai thác mạng và mã số của các nhóm toàn cục (Global Group) đều chứa trên server trên Domain chính.

Trong mô hình này tất cả các khác Domain đều tin cậy với Domain chính.



Hình B.9: ***Mô hình Domain chính***

Trong mô hình này mã số của người sử dụng quản lý tập trung và các nhóm toàn cục chỉ cần xác định một lần trong Domain chính. Tài nguyên được nhóm logic thành các đơn vị nhỏ hơn để có thể quản lý bởi từng Domain.

Mô hình Domain chính là mô hình quản lý tập trung vì vậy chiến lược phát triển mạng cần dựa vào các nhóm cục bộ và các nhóm toàn cục.

Mô hình này không những quản lý tập trung các mã số của người sử dụng mà còn cung cấp các dịch vụ như cài đặt phần mềm, sao chép backup cho tất cả các máy chủ trên mạng.

Tuy nhiên mô hình này có nhược điểm có thể gây ùn tắc nếu có quá nhiều nhóm và nhiều người dùng và các nhóm cục bộ cần phải xác định trong mỗi Domain mà chúng được sử dụng.

B.2.3.3. Mô hình nhiều Domain chính (Muliple Master Domain)

Mô hình nhiều Domain chính (Muliple Master Domain) có thể được sử dụng cho các tổ chức có nhiều khu vực và mỗi khu vực có nhiều bộ phận. Trong nhiều mạng kiểu như vậy, bộ phận điều hành riêng biệt cho mỗi khu vực muốn quản lý tập trung các tài nguyên mạng trong khu vực. Chúng ta xây dựng một Domain chủ (Master Domain) cho mỗi khu vực và chia các tài nguyên trong mỗi khu vực thành nhiều Domain tài nguyên (Resoure Domain) riêng biệt.

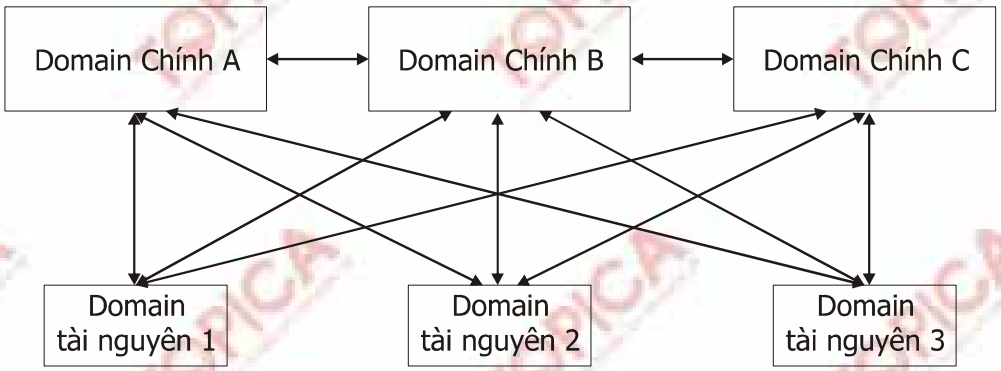
Trên mô hình này tồn tại các quan hệ sau:

- Mỗi Domain chính quan hệ tin cậy hai chiều với các Domain chính khác. Điều này cho phép mỗi Domain chính có thể quản lý các Domain chính khác.
- Các Domain không phải là chính không có mã số của người sử dụng mà chỉ cung cấp tài nguyên trên mạng.
- Các Domain không phải là chính tin cậy đối với tất cả các Domain chính. Nhờ điều này mỗi mã số của người sử dụng sẽ được sử dụng trên tất cả các Domain chính và có được quyền truy cập vào tài nguyên trong các tài nguyên trên các Domain khác của mạng.

Bằng cách phân chia tài nguyên mạng thành nhiều Domain, chúng ta có nhiều thuận lợi trong việc tổ chức quản lý một số lượng lớn các tài nguyên trong các đơn vị phù hợp.

Mô hình nhiều Domain chính có ưu điểm đối với mạng nhiều người dùng trong đó các tài nguyên được nhóm một cách logic theo công việc. Tuy nhiên các nhóm cục bộ và

toàn cục phải xác định nhiều lần và mã số của người sử dụng phải chứa ở nhiều Domain chính.

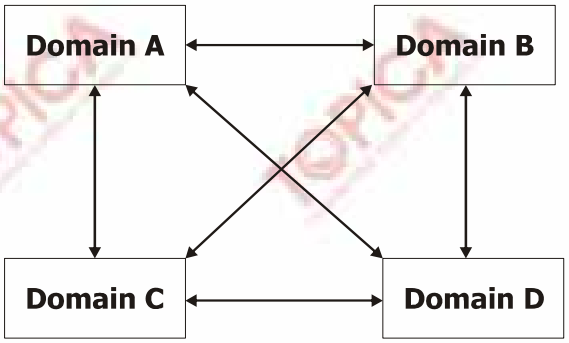


Hình B.10: ***Mô hình nhiều Domain chính***

B.2.3.4. Mô hình tin cậy hoàn toàn (complete trust)

Mô hình tin cậy hoàn toàn là mô hình mà trong đó mỗi Domain là quan hệ tin cậy 2 chiều với các Domain khác. Với mô hình này, người sử dụng có thể truy cập vào bất kỳ Domain nào trên mạng từ một máy trạm nào đó.

Mô hình này có thể áp dụng với qui mô mạng tùy ý và phù hợp cho các cơ quan không có nhóm quản trị tập trung, nó cho phép không hạn chế số người khai thác mạng và số nhóm. Mỗi bộ phận trong đơn vị có thể kiểm soát được mã số của người sử dụng cũng như tài nguyên của bộ phận mình trong đó tài nguyên và mã số người sử dụng được nhóm thành một Domain.



Hình B.11: ***Mô hình nhiều Mô hình tin cậy hoàn toàn***

B.2.4. Các mặt hạn chế của những mô hình Domain

Mô hình vùng có một số kẽ hở về cấu trúc. Những hạn chế về Domain được thảo luận ở đây nhằm mục đích giúp bạn thiết kế mạng chính xác và hoàn hảo:

- Domain NT đơn điệu theo nghĩa là không có cách nào diễn tả quan hệ phân cấp hoặc nhóm tài nguyên trong một vùng đơn. Người dùng có thể sử dụng những quyền được ủy thác thể hiện các quan hệ giữa những vùng, nhưng đây là quan hệ sử dụng và không thích hợp cho việc tổ chức mạng dựa trên phạm vi địa lý, tài nguyên sở hữu, logic hoặc nền tảng sơ đồ tổ chức.
- Mô hình vùng Domain chính duy nhất theo Microsoft thích hợp cho các mạng ít hơn 40.000 người dùng và nhóm. Khi số người dùng và nhóm tăng lên, số quan hệ

ủy quyền và chi phí quản lý quan hệ cũng tăng. Nói cách khác chi phí quản lý mạng có thể tăng bất thình lình khi kích thước mạng tăng.

- Người dùng phải cẩn trọng về kẽ hở của quan hệ ủy quyền - đặc biệt quan hệ ủy quyền hai chiều. Nếu không cẩn thận trong việc gán các quan hệ ủy quyền và không có kế hoạch đúng đắn, người sử dụng có thể kết thúc bằng một mô hình ủy quyền trọn vẹn, với tất cả những hạn chế của mô hình đi kèm.
- Ngoài ra có một nguy cơ thực sự sẽ xảy ra là người cài đặt mạng có thể cài đặt một mạng hoạt động tốt trong thời gian ngắn còn khi mạng hoạt động dài hạn này sẽ nảy sinh vấn đề về mặt chính sách là ai ủy quyền cho ai.