HỆ ĐIỀU HÀNH WINDOWS NT

Bài 1: Tổng quan về hệ điều hành Windows NT

Tài liệu tham khảo

- Quản trị Windows Server 2003 – NXB Hồng đức
- Quản trị mạng Windows NT

I. Thế nào là một hệ điều hành mạng

1. Mạng và HĐH

- Lúc đầu mỗi hệ thống máy tính hoạt động độc lập với nhau và thực hiện những công việc xác định.
  - Khi đó, việc chia xẻ những tài nguyên hệ thống cũng như các thông tin khác diễn ra rất khó khăn.
  - Những tổ chức ở xa nhau rất khó trao đổi thông tin trực tiếp với nhau, đặc biệt là ở những lĩnh vực: thương mại, chính trị quốc phòng…

- Khi xã hội có những sự phát triển → nhu cầu liên lạc và chia xẻ thông tin đã trở nên cực kì cấp thiết.
- Tại thời điểm đó: Network Computer và Network Operating System ra đời đã đánh dấu một bước tiến lớn của con người trong lĩnh vực khoa học máy tính và viễn thông.

Mạng

- **Mạng máy tính gồm tài nguyên:**
  - ✓ Tài nguyên mạng: máy trạm, máy in mạng…
  - ✓ Các thiết bị viễn thông dùng để liên kết các tài nguyên: cầu nối, router, cổng gateway, dây dẫn…

do hệ điều hành mạng.

- Công việc của hệ điều hành mạng bao gồm:
  - ✓ Quản lý tài nguyên nội bộ giống như một hệ điều hành bình thường như: Hệ thống file nội bộ, bộ nhớ trên máy tính, …
  - ✓ Quản lý các tài nguyên mạng như: hệ thống file của các máy trạm, bộ nhớ chia xẻ, thực thi các trình ứng dụng chia xẻ trên mạng, …

- Căn cứ vào việc truy nhập tài nguyên trên mạng người ta chia các thực thể trong mạng thành hai loại chủ và khách:
  - ✓ Máy khách (Client) truy nhập được vào tài nguyên của mạng,
  - ✓ Máy chủ (Server) là máy tính nằm trên mạng và chia sẻ tài nguyên của nó với các người dùng mạng.

- Các hệ điều hành mạng thường được chia làm hai loại:
  - ✓ Hệ điều hành mạng ngang hàng (Peer-to-peer)
  - ✓ Hệ điều hành mạng phân biệt (Client/Server).

2. 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:
  - ✓LAN tastic của Artisoft
  - ✓ NetWare lite của Novell
  - ✓Windows (for Workgroup, 95, NT Client, ...) của Microsoft.

3. Với hệ điều hành mạng phân biệt

- 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 nhập 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.

II. Hệ điều hành mạng Windows NT

1. Lịch sử phát triển

- **Năm 1994 :**
  - ✓ Công nghệ NT (*New Technology*) ra đời
  - ✓ Các phiên bản đầu tiên: Windows NT 3.1/3.5/4.0 thích hợp cho các máy chủ và các trạm làm việc trên mạng.
- **Năm 1995:**
  - ✓ Windows 95 là HĐH 32 bit đâu tiên của dòng Window 9X, chủ yếu dành cho các máy đơn
  - ✓ Windows 9x và Windows NT có các điểm mạnh: hỗ trợ đa người SD, khả năng hỗ trợ mạng mạnh.

- **Năm 2000:**

  Microsoft dựa vào họ Windows 9X và họ Windows NT làm nền tảng cho các phiên bản Windows sau này như :

  - ***Windows Me***
  - ***Windows 2000***
  - ***Windows 2002***
  - ***Windows XP***
  - ***Windows Server 2003***
  - ***Windows Server 2008, …***

Version	Marketing Name	Editions	Release Date
NT 5.0	Windows 2000	Professional, Server, Ad Server, Datacenter Server	February 17, 2000
NT 5.1	Windows XP		
NT 5.2	Windows Server 2003	Standard, Enterprise, Datacenter, Web, Storage, SB Server, Compute Cluster	April 24, 2003
NT 6.0	Windows Server 2008	Standard, Enterprise, Datacenter, Web, Storage, SB Server	February 27, 2008 (expected)

- 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 của NT ta có thể xây dựng mạng ngang hàng, mạng chủ/khách và mọi công cụ quản trị mạng.

- Cả hai bản Windows NT Workstation 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 (Tiêu chuẩn của Trung tâm an toàn điện toán quốc gia và Bộ quốc phòng Mỹ).

2. Một số mục tiêu trong việc thiết kế hệ điều hành mạng Windows NT

a. Khả năng tương thích:

Windows NT có khả năng tạo ra các môi trường cho các trình ứng dụng được viết cho các hệ điều hành khác (như MS DOS, OS/2, Windows 3.x), hỗ trợ một số hệ thống file thông dụng (như FAT, NTFS) và khả năng nối kết với các môi trường mạng khác hiện có.

b.Tính thuận tiện:

Windows NT có thể chạy được với các bộ vi xử lý hỗ trợ CISC (Complex Instruction Set Computer - có bộ chỉ lệnh phức hợp) như Intel® 80386-80486, và RISC (Reduced Instruction Set Computer-dùng tập lệnh rút gọn) như MIPS® R4000, DEC Alpha.

c. Tính đa xử lý:

Windows NT có thể chạy trên máy tính có từ 1 đến 16 bộ vi xử lý, mở rộng lên những hệ máy lớn đáp ứng được những yêu cầu rất cao của môi trường kinh doanh.

d. Tính an toàn

Cung cấp những tính năng an toàn đáng tin cậy bao gồm việc kiểm soát truy cập đến tài nguyên, bảo vệ bộ nhớ, kiểm soát toàn bộ quá trình thâm nhập của người dùng, tính an toàn và khả năng khắc phục sau sự cố…

e. Khả năng xử lý chia sẻ và phân phối

Windows NT có khả năng nối kết với nhiều môi trường mạng khác mà có hỗ trợ nhiều loại giao thức truyền thông khác nhau.

f. Độ tin cậy

Windows NT cung cấp cơ chế đảm bảo các ứng dụng thi hành một cách an toàn, không vi phạm đến hệ thống và các ứng dụng khác.

g. Tính đại chúng

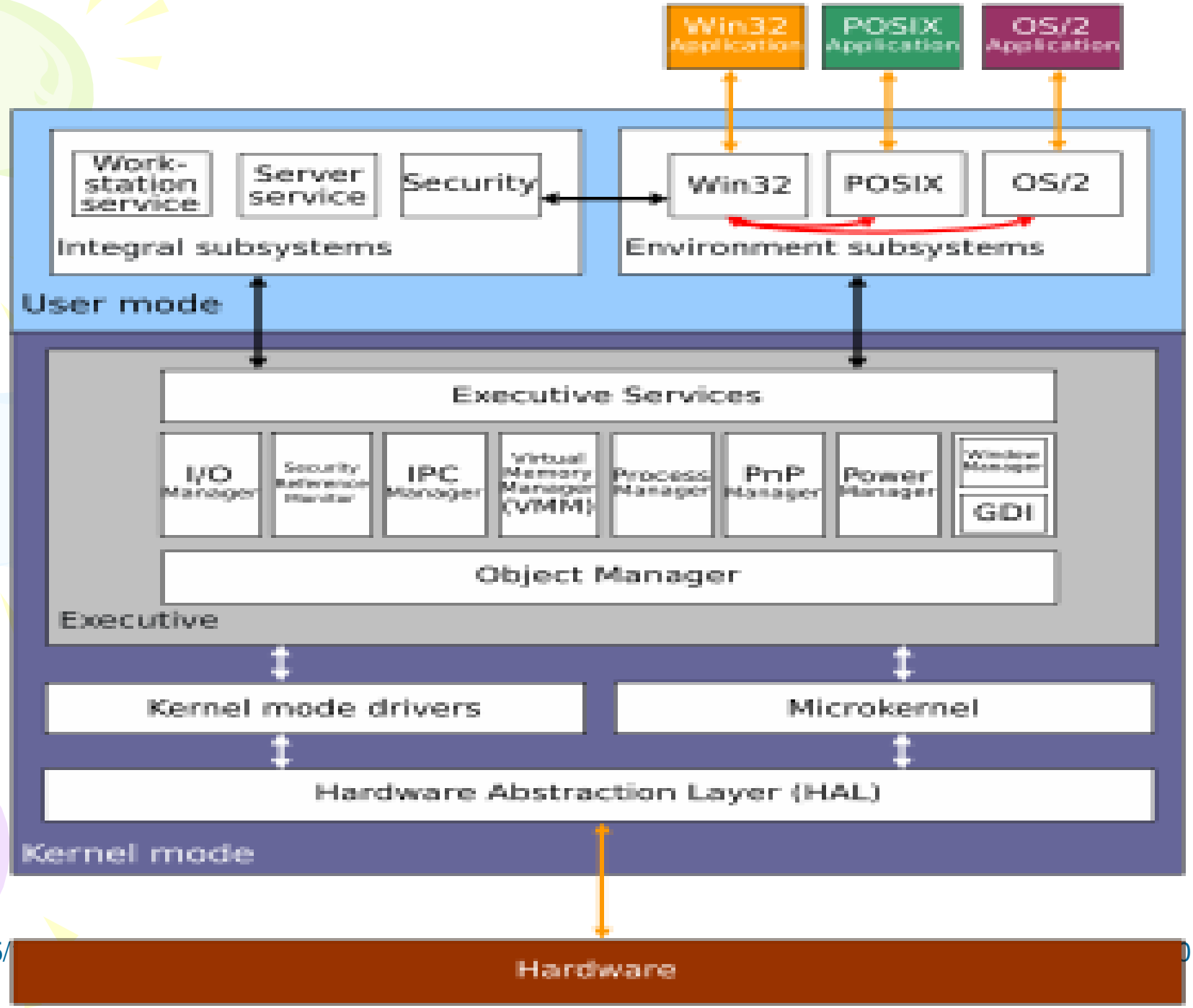
Windows NT đề ra mục tiêu thiết kế để có thể ứng dụng ở nhiều quốc gia, nhiều ngôn ngữ.

h. Dễ nâng cấp, mở rộng

Kiến trúc Windows NT tiếp cận theo cách phân chia thành các đơn thể có nhiệm vụ xác định, cung cấp khả năng nâng cấp, mở rộng trong tương lai.

III. Cấu trúc của HĐH Windows NT

- Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular).
- Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User mode (người sử dụng) và Kernel mode (lõi của hệ điều hành).


Win32 Application
POSIX Application
OS/2 Application
Work-station service
Server service
Security
Integral subsystems
Win32
POSIX
OS/2
Environment subsystems
User mode
Executive Services
I/O Manager
Security Reference Monitor
IPC Manager
Virtual Memory Manager (VMM)
Process Manager
PnP Manager
Power Manager
Window Manager
GDI
Object Manager
Executive
Kernel mode drivers
Microkernel
Hardware Abstraction Layer (HAL)
Kernel mode
Hardware

1. Chế độ Kernel mode

- Các đơn thể có toàn quyền truy cập đến phần cứng ở dưới bao gồm khả năng sử dụng không hạn chế các chỉ thị CPU và các tài nguyên hệ thống…;
- Các đơn thể của Windows NT thi hành ở chế độ này bao gồm Executive Services, Kernel, Hardware Abstraction Layer (HAL).

2. Chế độ User mode

- Ở chế độ này các chương trình không trực tiếp truy cập đến phần cứng mà phải thông qua các đơn thể ở Kernel mode.
- Việc đặt các hệ thống con (Subsystem) ở chế độ User mode giúp cho các nhà thiết kế dễ dàng hơn trong việc thay đổi, bổ sung các thành phần mà không làm ảnh hưởng đến thành phần khác ở Kernel mode.

3. Các lớp chính của hệ điều hành WINDOWS NT SERVER

a. Lớp phần cứng trừu tượng (Hardware Astraction Layer - HAL)

- Là phần cứng máy tính mà 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 lõi của hệ điều hành sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là Kernel và tất cả các thành phần khác phụ thuộc vào lõi có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền (Platform) phần cứng khác.

b. Lớp Kernel

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 sử lý***.

c. Các thành phần Executive

- Quản lý đối tượng (object manager)
- Bộ phận giám sát an toàn (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)

IV.Cơ chế quản lý của Windows NT

1. Quản lý đối tượng (Object Manager)

Trong môi trường Windows NT, các ứng dụng chia sẻ với nhau các tài nguyên hệ thống bao gồm bộ nhớ, những thiết bị nhập xuất, file, bộ xử lí… dưới sự giám sát chặt chẽ của hệ điều hành thông qua một cơ chế an toàn rất đáng tin cậy, đảm bảo các ứng dụng không thể truy cập đến những tài nguyên không được phép.

Về mặt nội bộ, Windows NT xem tất cả các tài nguyên hệ thống, bao gồm cả tập tin (file) là những đối tượng. Việc tạo, đặt tên và hủy đối tượng thông qua một thành phần thực thi thuộc Kernel mode gọi là Object Manager - trình quản lý đối tượng.

Ngoài ra Object Manager còn có nhiệm vụ bảo vệ đối tượng khỏi xự xâm phạm của các đối tượng khác, giám sát ai đang sử dụng đối tượng đó và đối tượng đó đang dùng những tài nguyên gì.

- Như vậy, khi một đối tượng được tạo ra nó được gán tên và kèm theo là những thông tin về an toàn áp đặt trên đối tượng đó, các thông tin này được lưu trữ trong những cấu trúc xác định và được gắn kèm với đối tượng đó.

Bằng cách xử lý toàn bộ tài nguyên như là các đối tượng Windows NT có thể thực hiện các phương thức giống nhau như:

- Tạo đối tượng, quản lý 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.

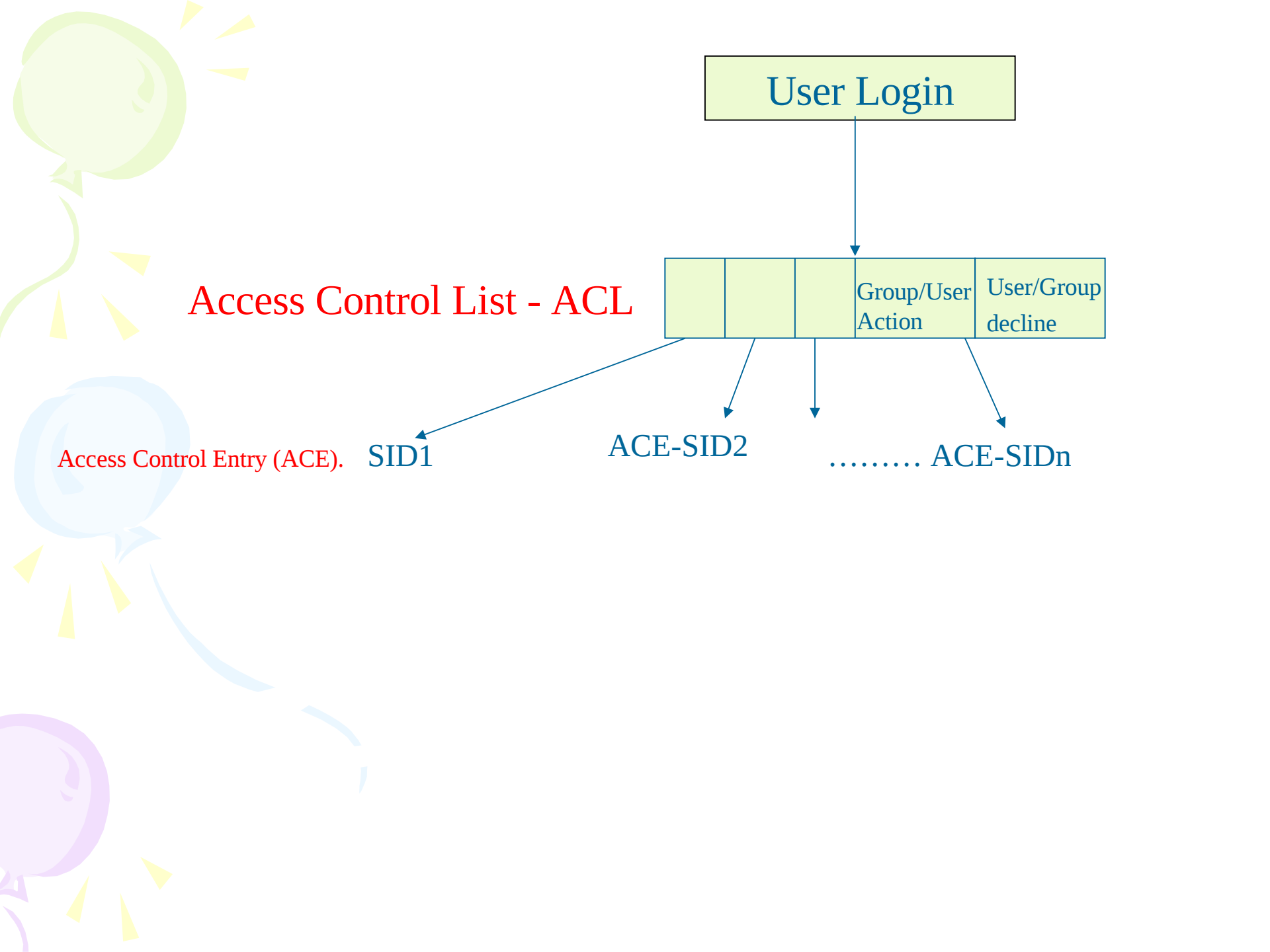
2. *Cơ chế bảo mật* (SRM - Security Reference Monitor)

- 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 truy cập (Access Control List - ACL).
- Danh sách truy cập 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.

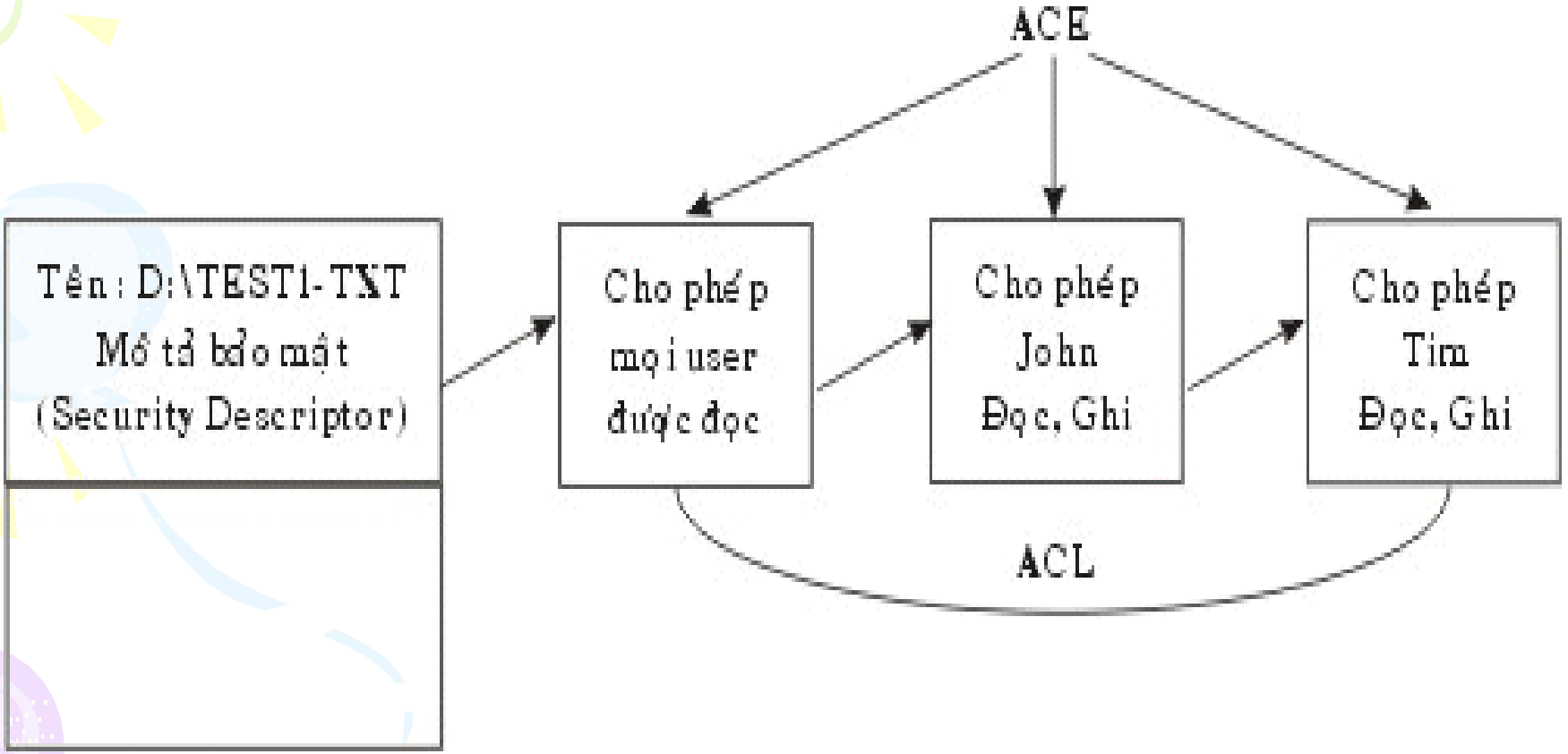
- Ngoài SID, ACE chứa một danh sách các hành động (action) được cho phép hoặc bị từ chối của một user hoặc một nhóm nào đó.

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 "passcard" (thẻ chuyển) cho phiên làm việc của người dùng đó và được sử dụng để kiểm tra tất cả hoạt động của người dùng.


User Login
Access Control List - ACL
Group/User Action
User/Group decline
Access Control Entry (ACE).
SID1
ACE-SID2
…… ACE-SIDn

- 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.

Ví dụ về danh sách truy cập (Access Control List)

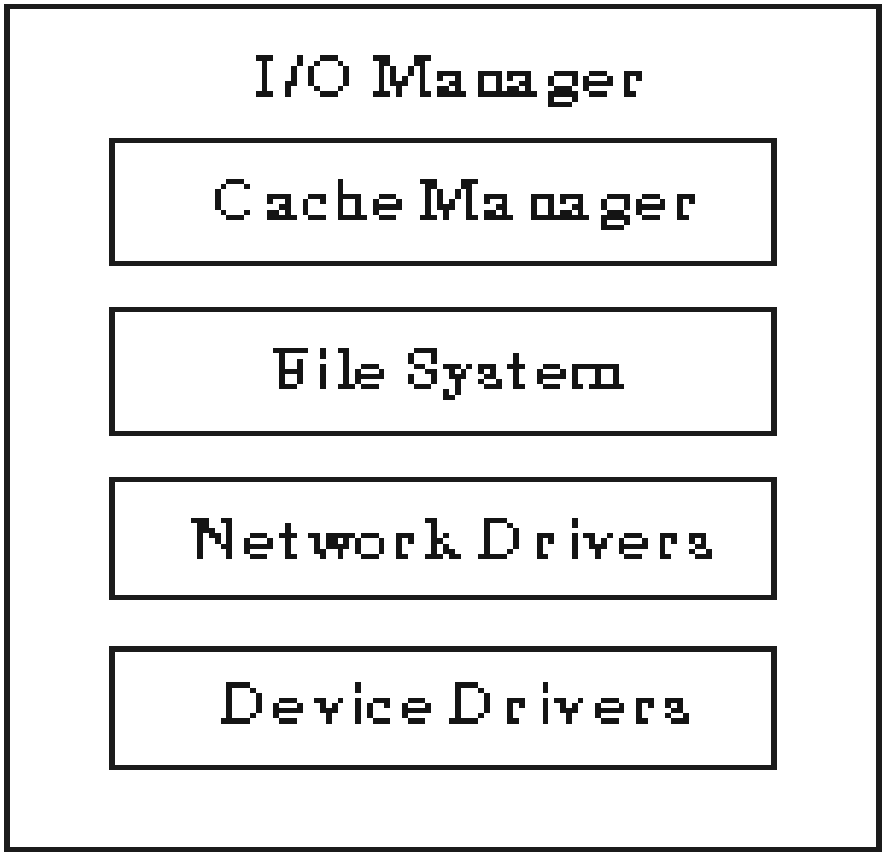


3. Quản lý nhập/xuất (I/O Manager) :

- 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.

Các trình điều khiển thiết bị theo lớp của I / O Manager



V. 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.

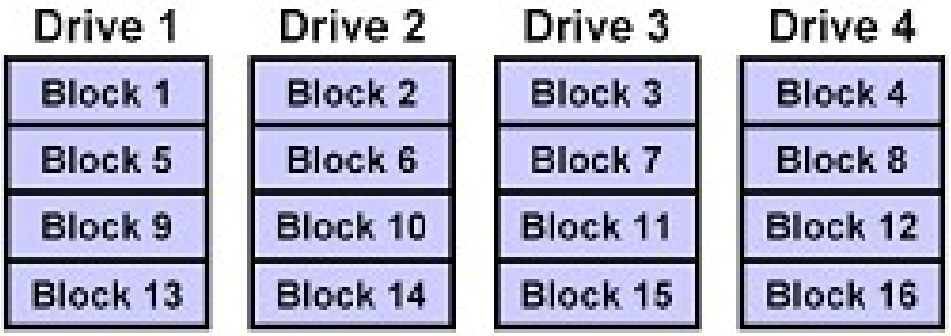
Trong Windows NT cơ chế fault tolerance bao gồm các biện pháp sau

- 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.

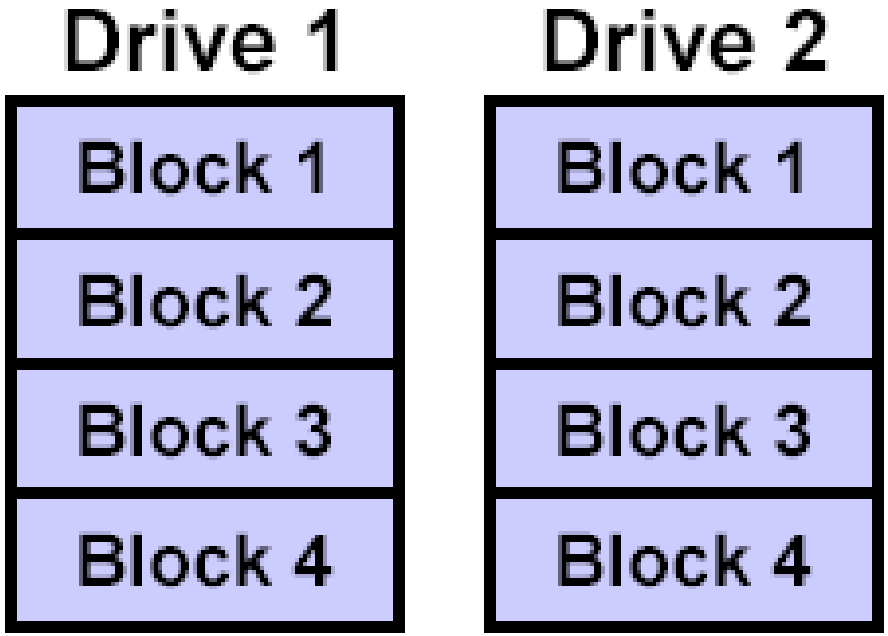
- **Khả năng bảo vệ hệ thống đĩa của Windows NT là RAID (viết tắt của Redundant Array of Inexpensiredisk). Thực chất RAID là một loạt các biện pháp để bảo vệ hệ thống đĩa.**

Các biện pháp trong RAID được chia thành 6 mức.

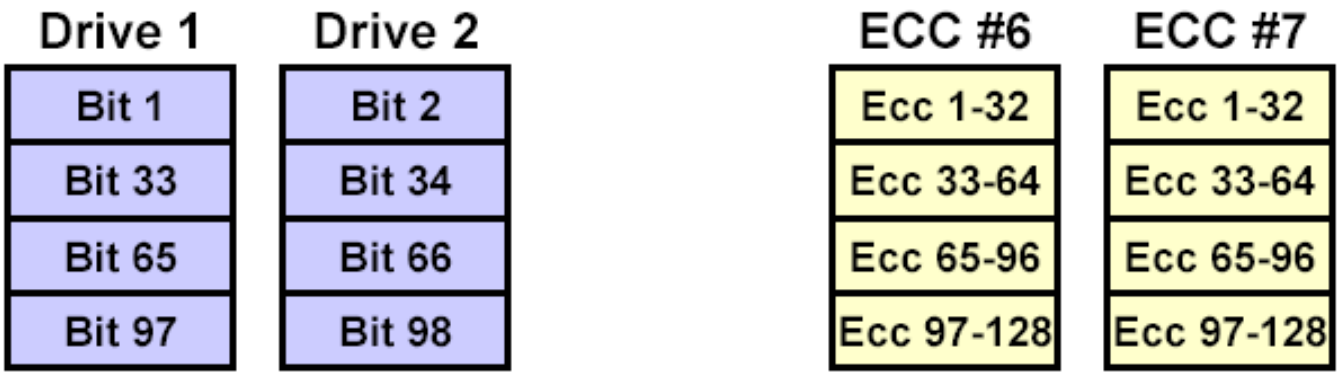
***Mức 0*:** Đây là mức ứng với biện pháp chia nhỏ đĩa (disk striping). Thực chất nội dung của biện pháp này là phân chia dữ liệu thành khối và sau đó sắp xếp các khối dữ liệu theo thứ tự trong tất cả các đĩa thành 1 mảng.



***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.**

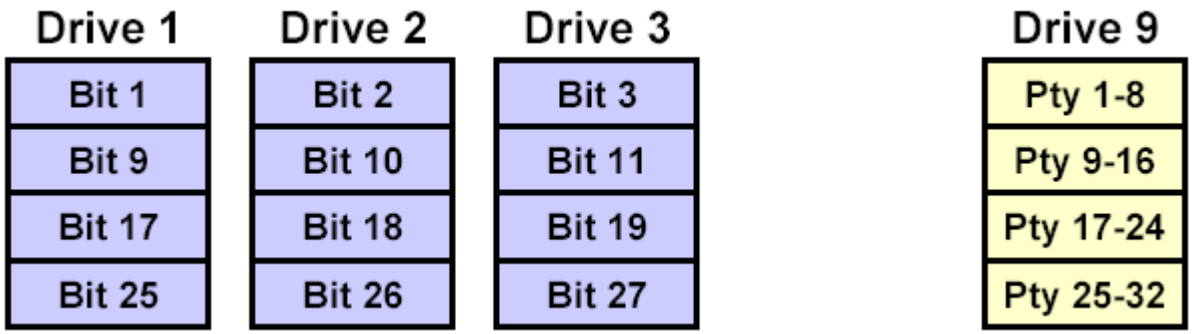


***Mức 2*:** Mức này ứng với biện pháp phân chia nhỏ đĩa bằng cách phân chia các file thành các byte và sắp xếp các byte sang nhiều đĩa. Mức này sử dụng mã sửa sai (error correcting code) trong quá trình phân chia đĩa. Nói chung biện pháp dùng ở mức này tốt hơn biện pháp dùng trong mức 1.



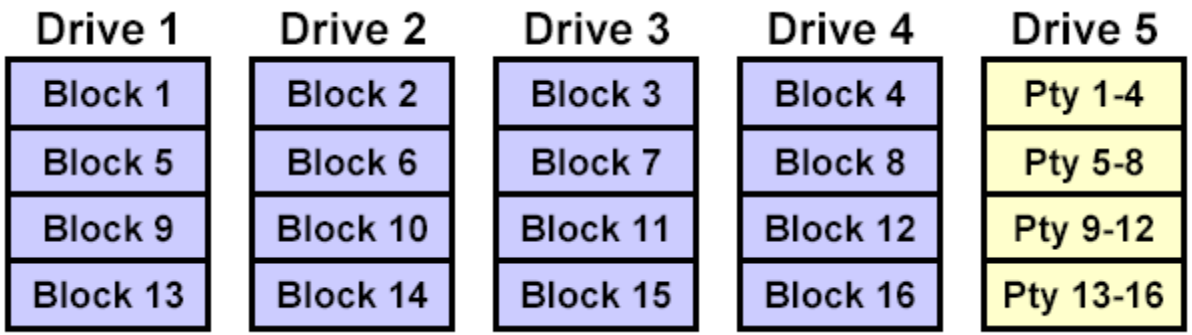
Mức 3:

Lưu trữ dữ liệu lên các dãy (**strip**) bằng nhau trên một hoặc nhiều đĩa vật lý



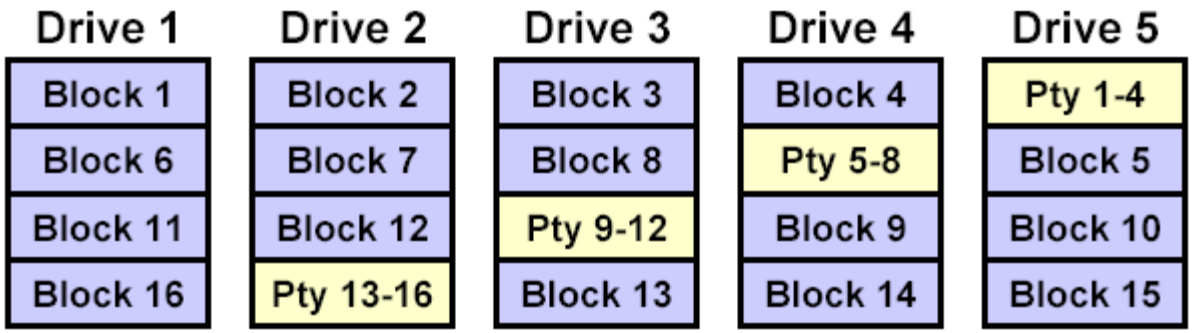
Mức 4:

Là hai bản sao của một **volume** đơn giản. Bạn dùng một ổ đĩa chính và một ổ đĩa phụ.



***Mức 5*:**

Tương tự như **volume striped** nhưng **RAID-5** lại dùng thêm một dãy (**strip**) ghi thông tin kiểm lỗi **parity**.



VI. Giới thiệu về hoạt động của Windows NT Server

Màn hình gia nhập mạng