

## BÀI 7: QUẢN TRỊ WINDOWS



### Nội dung

- Quản trị người dùng.
- Tài khoản người dùng.
- Tài khoản nhóm.
- Chiến lược quản trị.
- Công cụ quản trị.
- Chia sẻ tài nguyên.
- Tài nguyên File, Printer.
- Quyền truy cập trên file.
- Các chế độ chia sẻ file.
- Dịch vụ mạng.
- Giới thiệu mạng máy tính.
- Dịch vụ DHCP.
- Dịch vụ DNS.

### Mục tiêu

- Tổng quan về hệ điều hành Windows.
- Cơ bản nắm được các khái niệm.
- Biết và sử dụng được các công cụ, tính năng được cung cấp bởi Windows.
- Hướng dẫn sử dụng hiệu quả hệ điều hành Windows.
- Các khái niệm quản trị, chia sẻ tài nguyên và các dịch vụ trong Windows.

### Thời lượng học

- 10 tiết.

## TÌNH HUỐNG DẪN NHẬP

### Tình huống

Sau khi cài đặt Microsoft Windows 2003 server, các tác vụ quản trị quan trọng tiếp theo là cấu hình và triển khai các dịch vụ hạ tầng nền tảng.



### Câu hỏi

Vậy làm cách nào để cấu hình các dịch vụ mạng sau trong mạng máy tính:

1. Quản trị tài khoản người dùng và nhóm người dùng.
2. Quản trị tài nguyên file và máy in.
3. Dịch vụ DHCP và DNS.

## 7.1. Quản trị người dùng

Trước khi bất cứ người dùng nào có thể truy nhập vào máy tính chạy Microsoft Windows 2003 thì họ phải được xác thực. Xác thực là quá trình nhận dạng và xác nhận các điều kiện của người dùng. Trong hầu hết các trường hợp, quá trình xác thực yêu cầu người dùng nhập tên tài khoản và mật khẩu để máy chủ kiểm tra. Quản lý tài khoản người dùng và mật khẩu là một trong các tác vụ thông thường của người quản trị.

Tài khoản người dùng (User Account) là một đối tượng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng username. Chuỗi nhận dạng này giúp hệ thống phân biệt người này và người khác trên mạng, từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép.

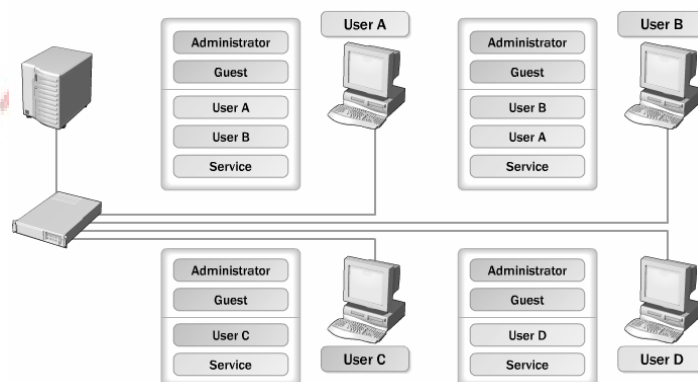
### 7.1.1. Tài khoản người dùng

Mạng Microsoft Windows dựa trên hai mô hình tổ chức thường được biết đến là nhóm (Group) và miền (Domain). Cả hai mô hình này đều yêu cầu người sử dụng có tài khoản để xác thực. Về bản chất, các tài khoản người dùng và các công cụ quản lý chúng đối với hai mô hình có khác nhau. Các điểm khác nhau giữa tài khoản người dùng cục bộ sử dụng cho nhóm và tài khoản người dùng miền được tổng kết trong bảng:

	Local User	Domain User
Công cụ quản lý	Local Users And Groups	Active Directory Users And Computers
Nơi lưu tài khoản	Quản lý các Tài khoản Bảo mật (SAM–Security Accounts Manager) trên từng máy tính cục bộ	Active Directory
Nơi đăng nhập	Máy tính cục bộ	Miền với Active Directory
Truy cập	Tài nguyên trên máy tính cục bộ	Tài nguyên mạng trên miền

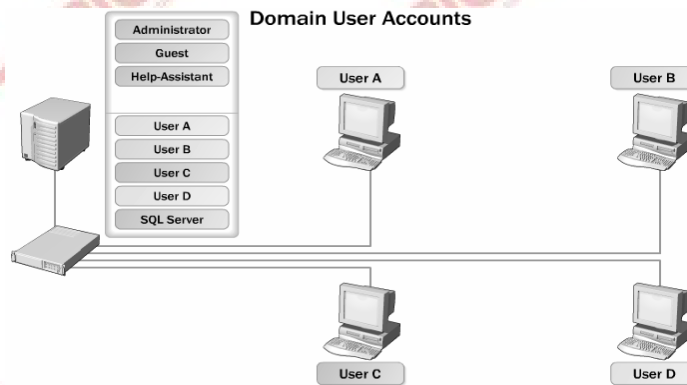
Tài khoản người dùng cục bộ (Local User Account) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy domain controller hoặc máy tính chứa tài nguyên chia sẻ.

Local User Accounts



Tài khoản người dùng miền (Domain User Account) là tài khoản người dùng được định nghĩa trên Active Directory và được phép đăng nhập (logon) vào mạng trên bất

kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng.



### 7.1.2. Tài khoản nhóm

Tài khoản nhóm (Group Account) là một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (Security Group) và nhóm phân phối (Distribution Group).

Nhóm bảo mật là nhóm được dùng để cấp phát các quyền hệ thống (Rights) và quyền truy cập (Permission). Có ba loại nhóm bảo mật chính là: Local, Global và Universal.

**Local group (nhóm cục bộ):** là loại nhóm có trên các máy Stand-Alone Server, Member Server, WinXP,... Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó.

**Domain local group (nhóm cục bộ miền):** là loại nhóm cục bộ đặc biệt vì chúng là local group nhưng nằm trên máy quản trị miền Domain Controller. Các máy Domain Controller có một cơ sở dữ liệu Active Directory chung và được đồng bộ với nhau, do đó một local group trên một Domain Controller này thì cũng sẽ có mặt trên các Domain Controller khác trong miền. Các nhóm tạo sẵn (Built-in) của Active Directory là các domain local.

**Global group (nhóm toàn cục):** là nhóm nằm trong Active Directory và được tạo trên các Domain Controller. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua ranh giới của một miền. Một nhóm global có thể đặt vào trong một nhóm Local của các Server thành viên trong miền. Chú ý khi tạo nhiều nhóm global thì có thể làm tăng tải công việc của Global Catalog.

**Universal group (nhóm tổng quát):** là loại nhóm có chức năng giống như global group nhưng dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm Global Group và Local Group vì chúng dễ dàng lồng các nhóm vào nhau. Nhưng chú ý là loại nhóm này chỉ có thể dùng được khi hệ thống của bạn phải hoạt động ở chế độ Windows 2000 Native Functional Level hoặc Windows Server 2003 Functional level có nghĩa là tất cả các máy Domain Controller trong mạng đều phải là Windows Server 2003 hoặc Windows 2000 Server.

**Quy tắc thành viên nhóm:**

- Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong nhóm Machine Local.

- Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong chính loại nhóm của mình.
- Nhóm Global và Universal có thể đặt vào trong nhóm Domain local.
- Nhóm Global có thể đặt vào trong nhóm Universal.

### 7.1.3. Chiến lược quản trị tài khoản

Trước khi thực sự bắt tay vào việc tạo tài khoản người dùng cục bộ hoặc tài khoản người dùng trên miền, bạn nên cân nhắc chiến lược quản lý, nhất là khi làm việc với một mạng lớn và phức tạp. Mặc dù việc tạo tài khoản người dùng ban đầu dường như là đơn giản.

#### Đặt tên

Khi bạn tạo tài khoản người dùng, cả dạng cục bộ và miền, bạn phải xác định First Name (Tên gọi) và Last Name (Họ) của người dùng, nhưng thông tin thực sự được dùng khi đăng nhập và xác thực là tên tài khoản. Tên của tài khoản người dùng cục bộ và tài khoản người dùng miền có độ dài tối đa cho phép là 20 ký tự, nhưng để thuận lợi cho người dùng nên đặt ngắn hơn. Các tên không phân biệt chữ hoa chữ thường (mặc dù Microsoft Windows 2003 giữ nguyên kiểu chữ bạn nhập vào) và không được chứa các ký tự đặc biệt như \*, +, ?, ...

Định dạng tên tài khoản ở mỗi tổ chức có thể sử dụng một số kiểu kết hợp của First Name hoặc Last Name, hoặc thêm các tiền tố,... Tuy nhiên, dù bạn sử dụng bất cứ dạng nào cho tên tài khoản, điều quan trọng nhất là bạn tạo được tập hợp các quy tắc để tạo ra chúng và trung thành với các quy tắc này. Việc đặt tên tài khoản một cách không thống nhất, sử dụng các biệt danh (Nickname) tối nghĩa hay theo sở thích của người sử dụng sẽ dẫn đến việc nhầm lẫn của các quản trị khác khi xác định tên tài khoản cho một người sử dụng cụ thể nào đó.

#### Mật khẩu

Ngày nay, bảo mật ảnh hưởng mạnh mẽ đến nhiệm vụ của quản trị trên toàn mạng và việc tạo tài khoản người dùng cũng không thuộc ngoại lệ. Khi tạo tài khoản người dùng mới bạn phải xác định mật khẩu và áp dụng chính sách với mật khẩu tùy theo mức độ bảo mật mà tổ chức của bạn muốn.

Mặc định, khi tạo tài khoản người dùng miền trong Microsoft Windows 2003, bạn phải đặt mật khẩu dạng phức tạp, có độ dài tối thiểu 7 ký tự. Những ràng buộc này được ấn định tại chính sách nhóm, được cấu hình mặc định tại Default Domain Policy Group Object – GPO. Tài khoản người dùng cục bộ sẽ không phải tuân theo các ràng buộc này. Bạn có thể điều chỉnh lại các ràng buộc và các quy tắc gán mật khẩu mặc định bằng cách sử dụng bảng điều khiển Group Policy Object Editor để sửa lại các thiết lập chính sách mật khẩu.

### 7.1.4. Quản trị tài khoản cục bộ

#### 7.1.4.1. Công cụ quản lý tài khoản người dùng cục bộ.

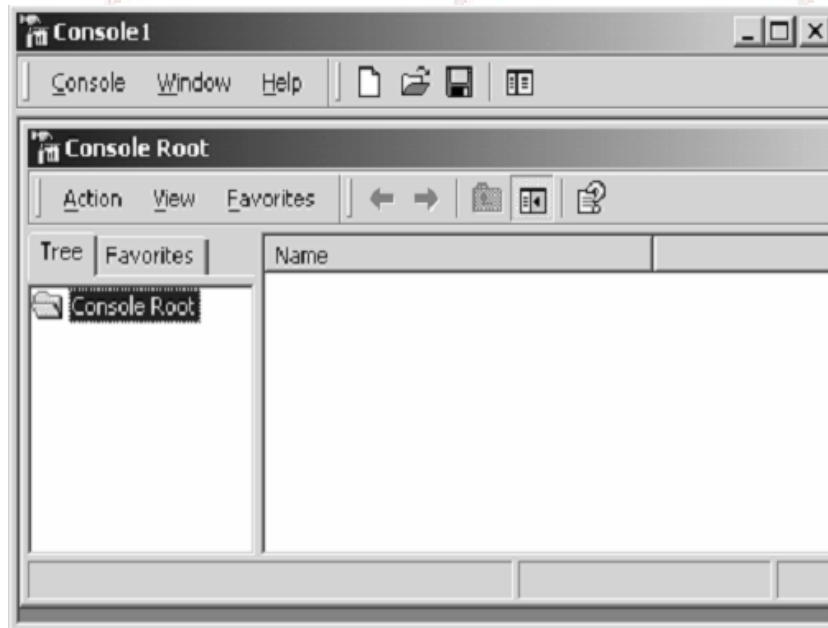
Để tổ chức và quản lý người dùng cục bộ, ta dùng công cụ Local Users and Groups. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã. Có hai cách truy cập đến công cụ Local Users and Groups:



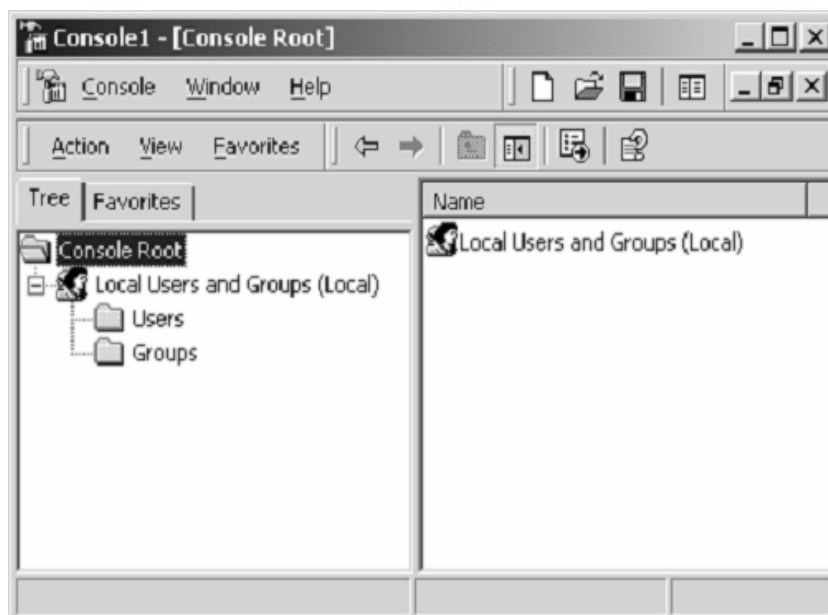
- MMC (Microsoft Management Console) snap-in.
- Computer Management.

Các bước thêm Local Users and Groups snap-in vào trong MMC:

- Chọn Start → Run, nhập **mmc** và nhấn phím Enter để mở cửa sổ MMC.

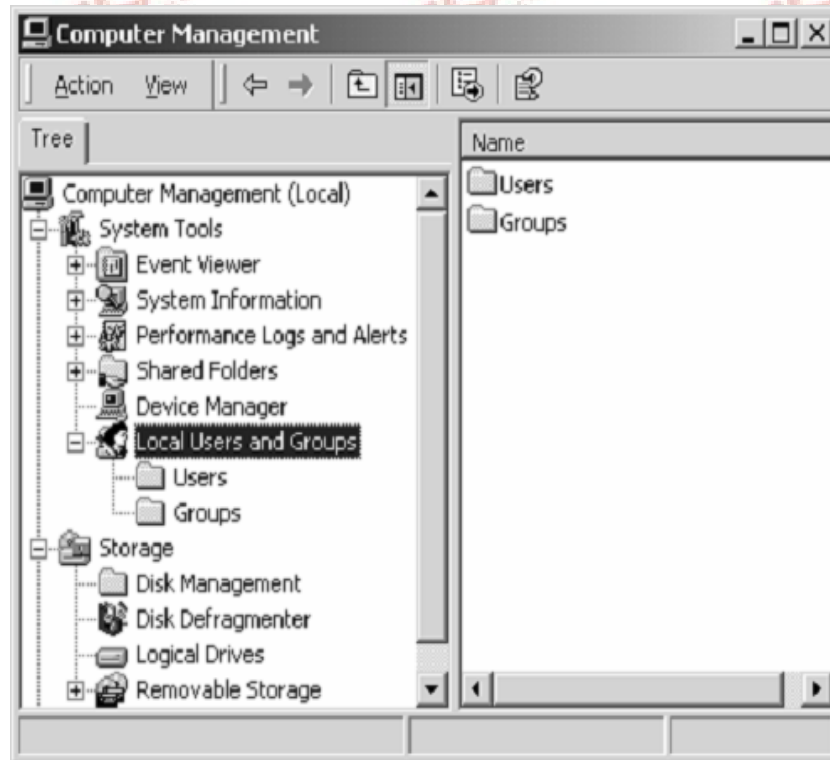


- Chọn Console → Add → Remove Snap-in để mở hộp thoại Add → Remove Snap-in.
- Kích vào nút Add để mở hộp thoại Add Standalone Snap-in.
- Chọn Local Users and Groups và nhấn Add.
- Hộp thoại Choose Target Machine xuất hiện, chọn Local Computer và nhấn vào nút Finish để trở lại hộp thoại Add Standalone Snap-in.
- Nhấn Close để trở lại hộp thoại Add → Remove Snap-in.
- Nhấn OK để xác nhận, ta sẽ thấy Local Users and Groups snap-in được đưa vào MMC.



Lưu lại Console bằng cách chọn Console → Save, sau đó nhập đường dẫn và tên file.

Nếu không dùng MMC thì ta có thể sử dụng công cụ Computer Management. Kích phải chuột vào My Computer và chọn Manage từ pop-up menu. Trong cửa sổ Computer Management, mục System Tools, ta sẽ thấy mục Local Users and Groups.



#### 7.1.4.2. Các tác vụ quản lý tài khoản người dùng cục bộ

##### Tạo tài khoản mới

Từ Local Users and Groups, kích phải chuột vào mục Users và chọn New User, hộp thoại.

New User xuất hiện ta nhập các thông tin, trong đó bắt buộc phải có là:

- User Name: tên tài khoản để đăng nhập.
- Full Name: tên đầy đủ của người dùng.
- Description: diễn giải về người dùng hoặc chức năng của người dùng.
- Password: mật khẩu xác thực, có độ dài tối đa 127 ký tự.
- Confirm Password: nhập lại mật khẩu để chắc chắn bạn đã nhập đúng.
- User Must Change Password At Next Logon: chọn tùy chọn này nếu bạn muốn người dùng phải thay đổi lại mật khẩu khi đăng nhập vào hệ thống lần đầu.
- User Cannot Change Password: người dùng sẽ không thay đổi lại được mật khẩu.
- Password Never Expires: mật khẩu không bao giờ bị hết hạn.
- Account Is Disabled: vô hiệu hóa tài khoản, tài khoản bị khóa và không dùng được.

##### Xóa tài khoản

Bạn chỉ nên xóa tài khoản người dùng nếu chắc chắn rằng tài khoản này không bao giờ cần dùng lại nữa.

Để xóa tài khoản người dùng, trong Local Users and Groups, chọn tài khoản cần xóa, kích phải chuột và chọn Delete (hoặc vào Menu Action → Delete).

### Khóa tài khoản

Khi tài khoản sẽ không được sử dụng trong thời gian dài, ta nên khóa lại vì lý do bảo mật và an toàn hệ thống (Nếu ta xóa tài khoản này đi thì không thể phục hồi lại được, do đó ta chỉ tạm khóa).

Để khóa, trong Local Users and Groups, nhấp đúp chuột vào tài khoản cần khóa, hộp thoại Properties của tài khoản xuất hiện.

Trong Tab General, đánh dấu vào Account is disabled. Nhấn Apply hoặc OK để lưu lại.

### Khởi tạo lại (Reset) mật khẩu

Muốn khởi tạo lại mật khẩu của tài khoản, trong công cụ Local Users and Groups, chọn tài khoản cần thay đổi, kích phải chuột và chọn Reset password. Trong hộp thoại nhập lại mật khẩu mới.

Bạn đọc có thể tự thực hành để quản trị tài khoản nhóm cục bộ.

## 7.1.5. Quản trị tài khoản trên miền

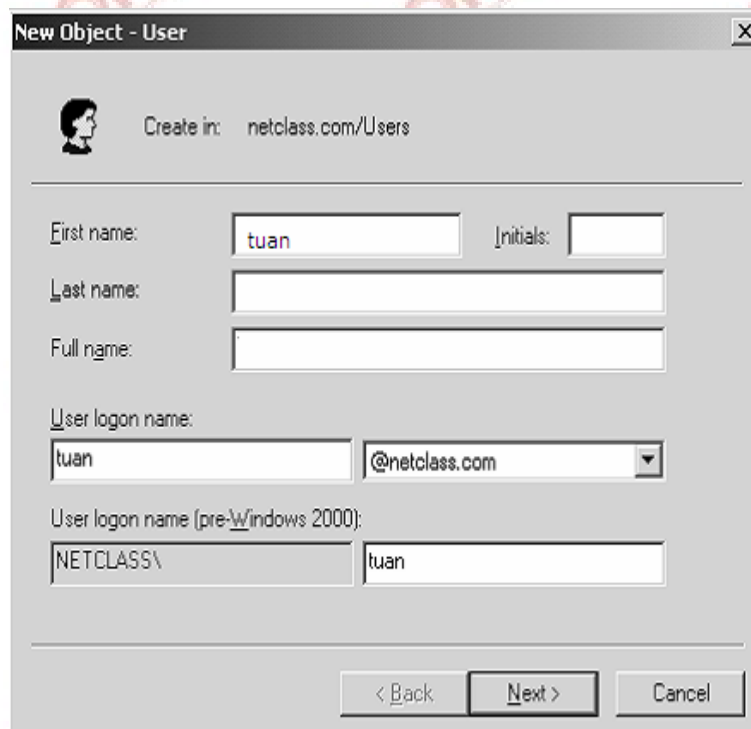
Ta sử dụng công cụ Active Directory User and Computers (trong mục Administrative Tools) trên máy quản trị miền (Domain Controller) để tạo các tài khoản miền.

Để tạo đối tượng người dùng, bạn phải là thành viên của nhóm Enterprise Admins, Domain Admins hoặc Account Operators, hoặc bạn phải được ủy quyền quản trị cần thiết.

### 7.1.5.1. Tạo mới tài khoản người dùng

Chọn Start → Programs → Administrative Tools → Active Directory Users and Computers.

Trong cửa sổ quản trị, chọn mục Users, chọn New → User. Trình trợ giúp (Wizard) tạo tài khoản người dùng xuất hiện:



New Object - User

Create in: netclass.com/Users

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel



Trong bước 1, nhập các thông tin sau:

- First Name: tên gọi của người dùng.
- Last Name: tên họ của người dùng.
- Full name: tên đầy đủ.
- User Logon Name: tên đăng nhập–tên của tài khoản sử dụng để đăng nhập (bắt buộc phải có), tên miền (trùng DNS). Tổ hợp này phải là duy nhất.
- User Logon Name (Pre–Windows 2000): tên tài khoản sử dụng để đăng nhập vào các máy khách trước Windows 2000 (bắt buộc).
- Nhấn Next để tiếp tục.

Trong bước 2, bạn sẽ cần nhập mật khẩu và một số thuộc tính như khóa tài khoản, thay đổi mật khẩu – tương tự tài khoản cục bộ đã trình bày ở mục Tạo Tài khoản cục bộ.

Nhấn Next để tiếp tục. Bước cuối là xác nhận và kết thúc việc tạo tài khoản.

#### 7.1.5.2. Cập nhật thuộc tính tài khoản người dùng

Để cập nhật thông tin tài khoản, nhấp đúp chuột vào tên tài khoản (hoặc chọn tài khoản, nhấp chuột phải và chọn menu Properties).

Cửa sổ thông tin tài khoản xuất hiện với hơn 10 tab thông tin:

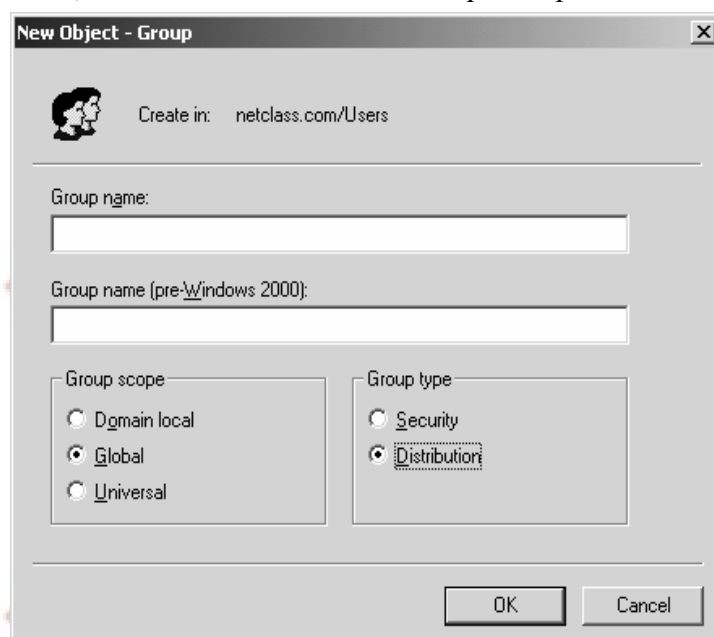
- **Tab Address:** khai báo các thông tin liên quan đến địa chỉ của người dùng như: địa chỉ đường, thành phố, mã vùng, quốc gia...
- **Tab Telephones:** cho phép khai báo các số điện thoại của tài khoản người dùng
- **Tab Organization:** cho phép khai báo các thông tin như: tên công ty, tên phòng ban,...
- **Tab Account:** cho phép khai báo lại username, giờ được đăng nhập (logon) vào mạng của người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản, quy định thời điểm hết hạn của tài khoản...
- **Tab Profile:** cho phép khai báo đường dẫn đến Profile của tài khoản, khai báo tệp tin logon script (tệp được tự động thực thi khi người dùng đăng nhập) hay khai báo home folder. Để ý các tùy chọn trong Tab Profile này chủ yếu phục vụ cho các máy trạm trước Windows 2000, đối với các máy trạm từ Win2K trở về sau (Win2K Pro, WinXP) thì ta có thể cấu hình các lựa chọn này trong Group Policy.
- **Tab Member Of:** cho phép xem và cấu hình tài khoản hiện tại là thành viên của những nhóm nào. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này. Muốn gia nhập vào nhóm nào bạn nhấn chuột vào nút Add.

#### 7.1.6. Tạo tài khoản nhóm

Tài khoản nhóm trên Active Directory được tạo và quản trị thông qua công cụ Active Directory Users and Computers. Trước khi tạo nhóm, ta cần xác định loại nhóm cần tạo, phạm vi hoạt động của nhóm như thế nào.

##### Tạo tài khoản nhóm

- Thực thi Active Directory Users and Computers từ menu Start → Programs → Administrative Tools → Active Directory Users and Computers.
- Nhấn chuột phải vào mục Users, chọn New trên pop-up menu và chọn Group.
- Trong hộp thoại New Object – Group, nhập tên nhóm vào mục Group name, trường tên nhóm cho các hệ điều hành trước Windows 2000 (pre-Windows 2000) tự động được tạo, bạn có thể hiệu chỉnh lại cho phù hợp.



## 7.2. Chia sẻ tài nguyên

### 7.2.1. Tài nguyên File

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, bạn phải logon vào hệ thống với vai trò người quản trị (Administrators) hoặc là thành viên của nhóm Server Operators.

Trong Explorer, kích phải chuột trên thư mục cần chia sẻ và chọn Properties, hộp thoại Properties xuất hiện, chọn Tab Sharing.



- Do not share this folder: thư mục chỉ được phép truy cập cục bộ.
- Share this folder: thư mục được phép truy cập cục bộ và truy cập qua mạng.
- Share name: tên thư mục chia sẻ (tên người dùng mạng nhìn thấy và truy cập).
- Comment: mô tả thêm.
- User Limit: số kết nối tối đa truy xuất vào thư mục tại một thời điểm.
- Permissions: thiết lập danh sách người dùng, nhóm có quyền truy cập qua mạng.
- Offline Settings: cho phép thư mục được lưu trữ tạm tài liệu khi làm việc dưới chế độ Offline.

### 7.2.2. Quyền truy cập trên file

#### 7.2.2.1. Quyền truy cập trên hệ thống file NTFS

Các hệ điều hành Microsoft Windows thường hỗ trợ 2 loại hệ thống file là FAT (bao gồm FAT16 và FAT32) và NTFS (được giới thiệu cùng với Windows NT). Hệ thống file FAT không hỗ trợ bảo mật, còn NTFS thì có hỗ trợ bảo mật. Nếu phân hoạch đĩa định dạng FAT thì mọi người đều có thể thao tác trên các file, thư mục, còn ngược lại là định dạng NTFS thì tùy theo người dùng có quyền truy cập không, nếu người dùng không có quyền thì không thể nào truy cập được dữ liệu trên đĩa. Hệ thống Windows

Server 2003 dùng các ACL (Access Control List) để quản lý các quyền truy cập của đối tượng cục bộ và các đối tượng trên Active Directory. Một ACL có thể chứa nhiều ACE (Access Control Entry) đại diện cho một người dùng hay một nhóm người.

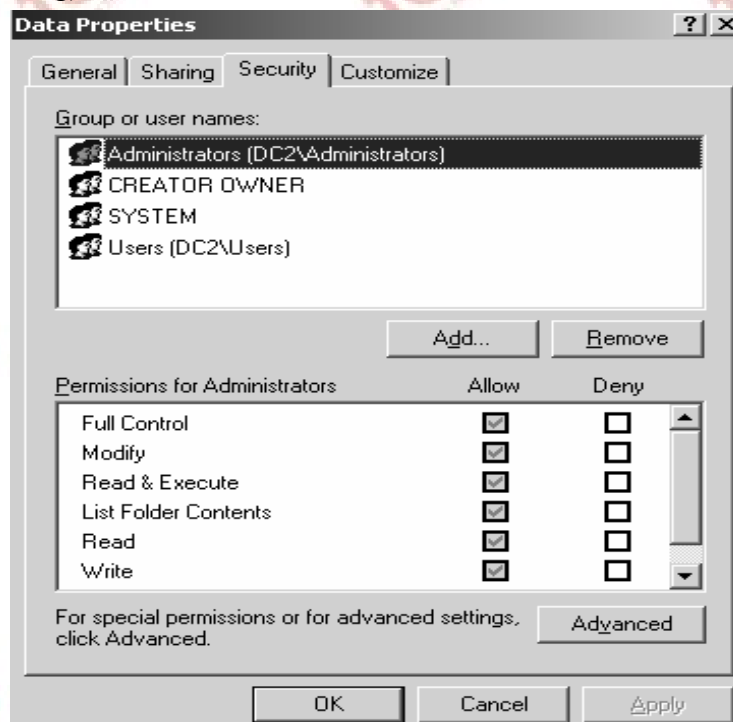
**Danh sách các quyền:**

- Traverse Folder/Execute File: quyền duyệt các thư mục và thi hành các file chương trình.
- List Folder/Read Data: liệt kê nội dung của thư mục và đọc dữ liệu của các tệp tin trong thư mục.
- Read Attributes: đọc các thuộc tính của tệp tin và thư mục.
- Read Extended Attributes: đọc các thuộc tính mở rộng của tệp tin và thư mục.
- Create File/Write Data: tạo các tệp tin mới và ghi dữ liệu lên các tệp tin này.
- Create Folder/Append Data: tạo thư mục mới và chèn thêm dữ liệu vào các tệp tin.
- Write Attributes: thay đổi thuộc tính của các tệp tin và thư mục.
- Write Extended Attributes: thay đổi thuộc tính mở rộng của các tệp tin và thư mục.
- Delete Subfolders and Files: xóa thư mục con và các tệp tin.
- Delete: xóa các tệp tin.
- Read Permissions: đọc các quyền trên các tệp tin và thư mục.
- Change Permissions: thay đổi quyền trên các tệp tin và thư mục.
- Take Ownership: lấy quyền sở hữu của các tệp tin và thư mục.

**7.2.2.2. Gán quyền truy cập NTFS trên thư mục dùng chung**

Để gán quyền trên NTFS, thông qua Windows Explorer bạn nhấp chuột phải vào tệp tin hay thư mục cần cấu hình quyền truy cập rồi chọn *Properties*. Hộp thoại Properties xuất hiện. Chọn *Tab Security* để cấp quyền cho các người dùng.

(Nếu ổ đĩa của bạn định dạng FAT thì sẽ không có tab Security, chỉ có hai Tab là General và Sharing).



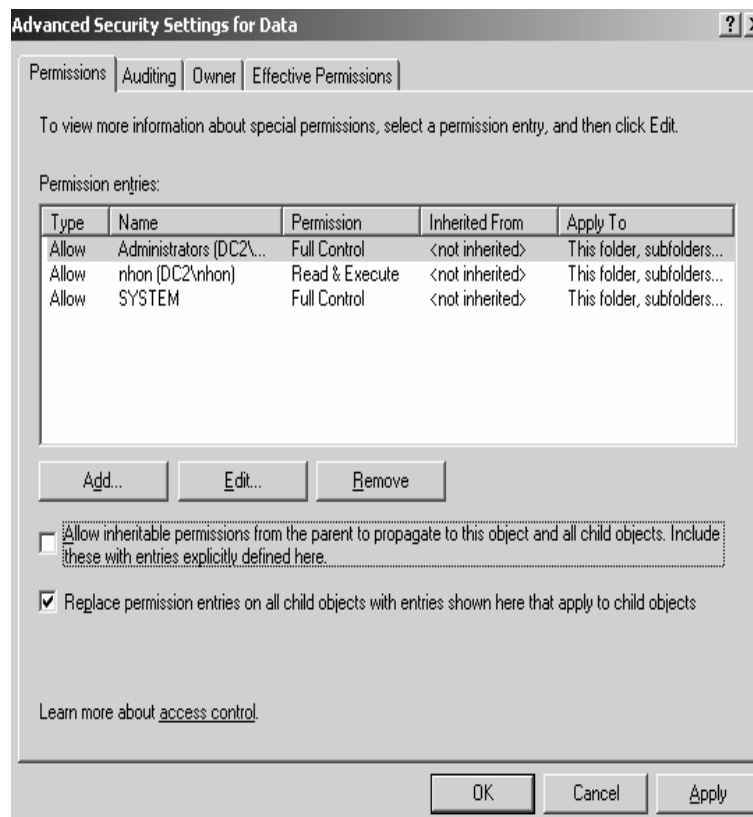
Để cấp quyền truy cập cho người dùng, nhấn Add. Hộp thoại chọn lựa người dùng và nhóm xuất hiện, chọn người dùng và nhóm cần cấp quyền, nhấn chuột vào nút Add để thêm vào danh sách, sau đó nhấn chuột vào nút OK để trở lại hộp thoại chính.

Trong hộp thoại đã hiện sẵn danh sách quyền, bạn muốn cho một người dùng quyền gì thì đánh dấu vào phần Allow, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục Deny.

### 7.2.2.3. Kế thừa và thay thế quyền của đối tượng con

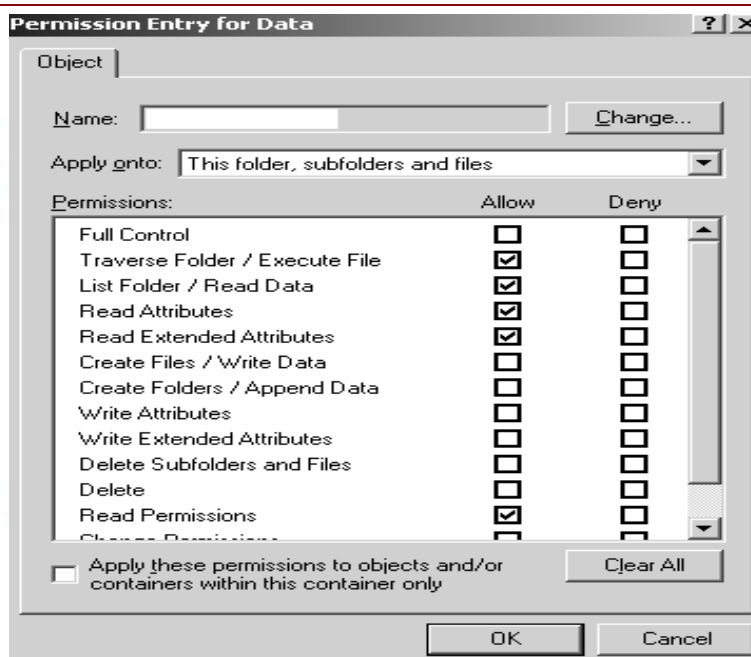
Trong hộp thoại chính trên, ta có thể nhấn chuột vào nút *Advanced* để cấu hình chi tiết hơn cho các quyền truy cập của người dùng.

Khi nhấn chuột vào nút *Advanced*, hộp thoại *Advanced Security Settings* xuất hiện, trong hộp thoại, nếu bạn đánh dấu vào mục *Allow Inheritable Permissions From Parent To Propagate To This Object And Child Objects* thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, bạn muốn xóa những quyền thừa hưởng từ thư mục cha bạn phải bỏ đánh dấu này. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra, nếu bạn đánh dấu vào mục *Replace Permission Entries On All Child Objects With Entries Shown Here That Apply To Child Objects* thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tệp tin và thư mục con có nghĩa là các tệp tin và thư mục con sẽ được thay thế quyền truy cập giống như các quyền đang hiển thị trong hộp thoại.



Cũng trong hộp thoại này, ta có thể kiểm tra và cấu hình lại chi tiết các quyền của người dùng và nhóm, để thực hiện, bạn chọn nhóm hay người dùng cần thao tác, sau đó nhấn chuột vào nút Edit.





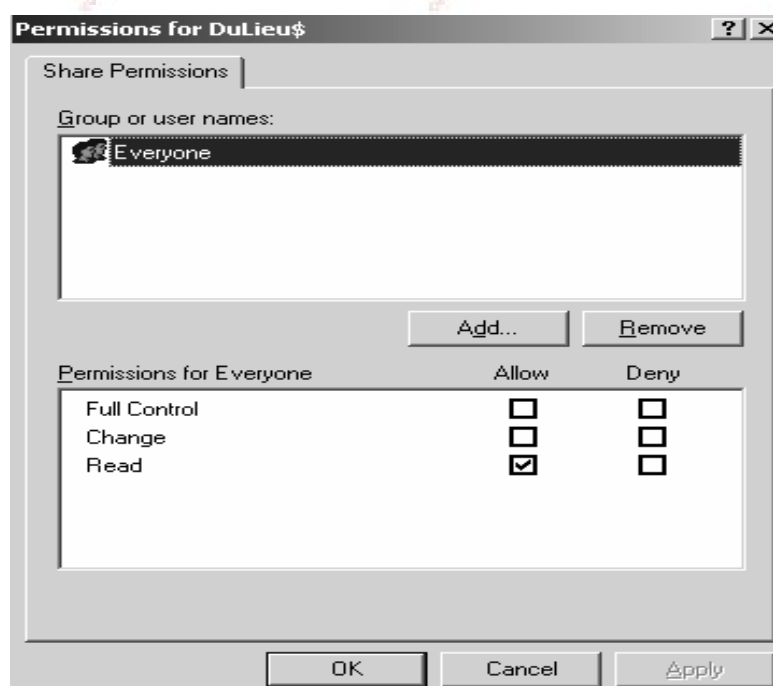
#### 7.2.2.4. Thay đổi quyền khi di chuyển thư mục và tệp tin

Khi ta sao chép (Copy) một tệp tin hay thư mục sang một vị trí mới thì quyền truy cập trên tệp tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha chứa chúng. Ngược lại, nếu ta di chuyển (Move) một tệp tin hay thư mục sang bất kỳ vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.

### 7.2.3. Chia sẻ file

#### 7.2.3.1. Share Permissions.

Nếu bạn muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng Share Permissions. Share Permissions chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với NTFS Permissions là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa.



Trong hộp thoại Share Permissions, chứa danh sách các quyền sau:

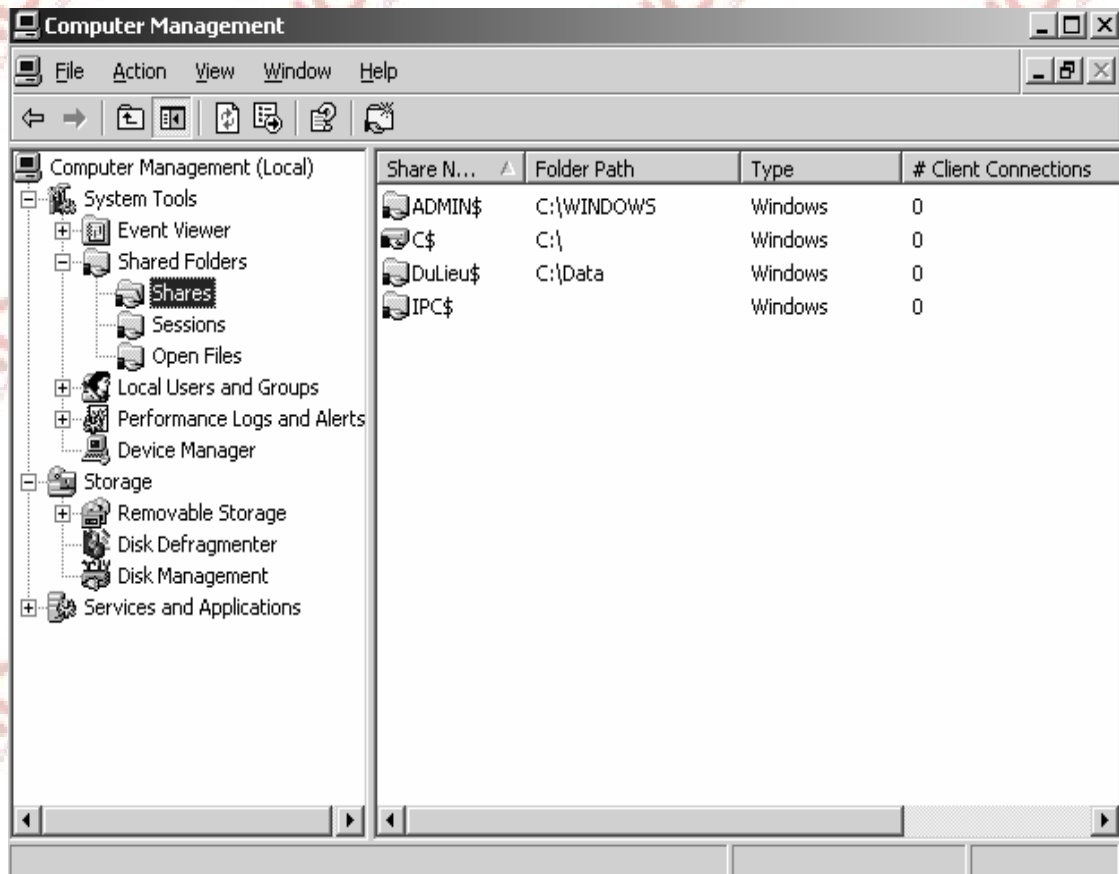
- Full Control: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- Change: cho phép người dùng thay đổi dữ liệu trên tệp tin và xóa tệp tin trong thư mục chia sẻ.
- Read: cho phép người dùng xem và thi hành các tệp tin trong thư mục chia sẻ.

Để lựa chọn người dùng, nhóm được truy cập, nhấn Add.

Trong hộp thoại, muốn cấp quyền cho người dùng, ta đánh dấu vào mục Allow, ngược lại để cấm quyền thì đánh dấu vào mục Deny.

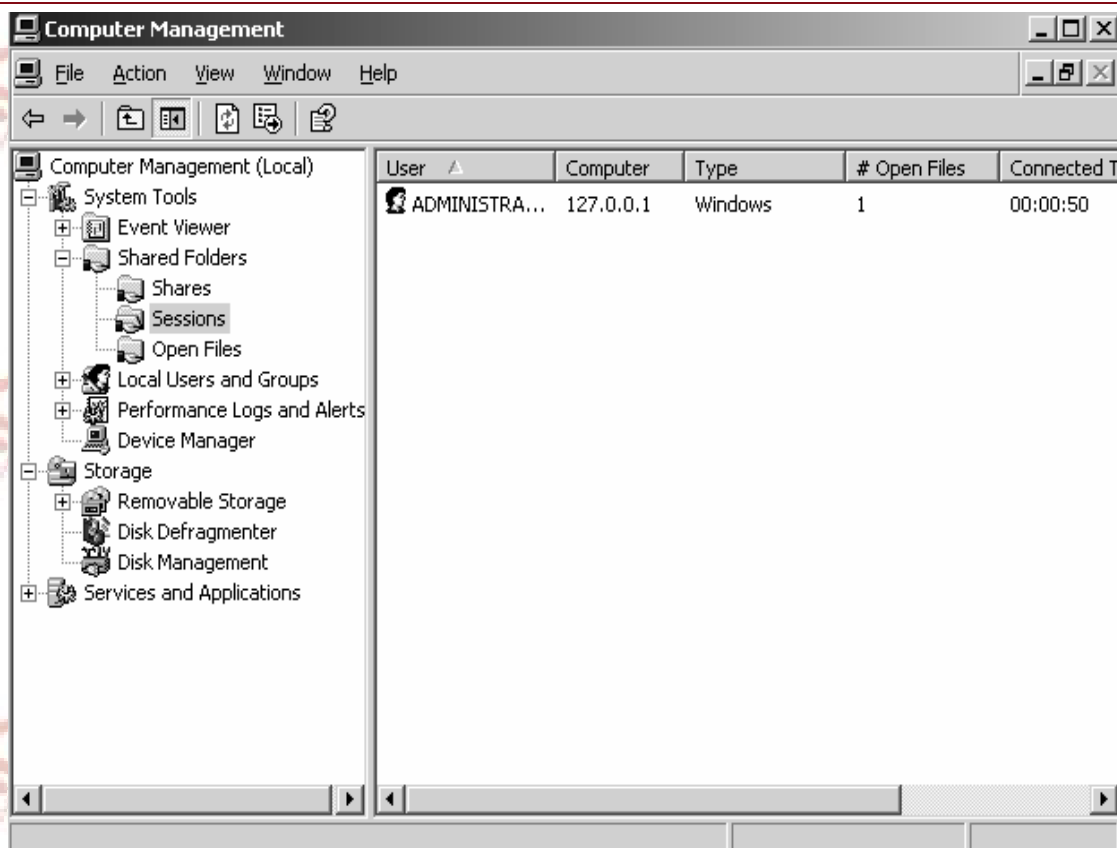
### 7.2.3.2. Xem các thư mục dùng chung

Mục Shared Folders trong công cụ Computer Management cho phép tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục Shares. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (Share Name) là dấu \$ thì tên thư mục dùng chung này được ẩn đi và không tìm thấy khi bạn tìm kiếm thông qua My Network Places hoặc duyệt các tài nguyên mạng. Các chia sẻ với phần đuôi là \$ thường dùng cho các mục đích quản trị.



### 7.2.3.3. Xem các phiên làm việc trên thư mục dùng chung

Muốn xem danh sách các người dùng đang truy cập đến các thư mục dùng chung trên máy tính, ta chọn mục Sessions.



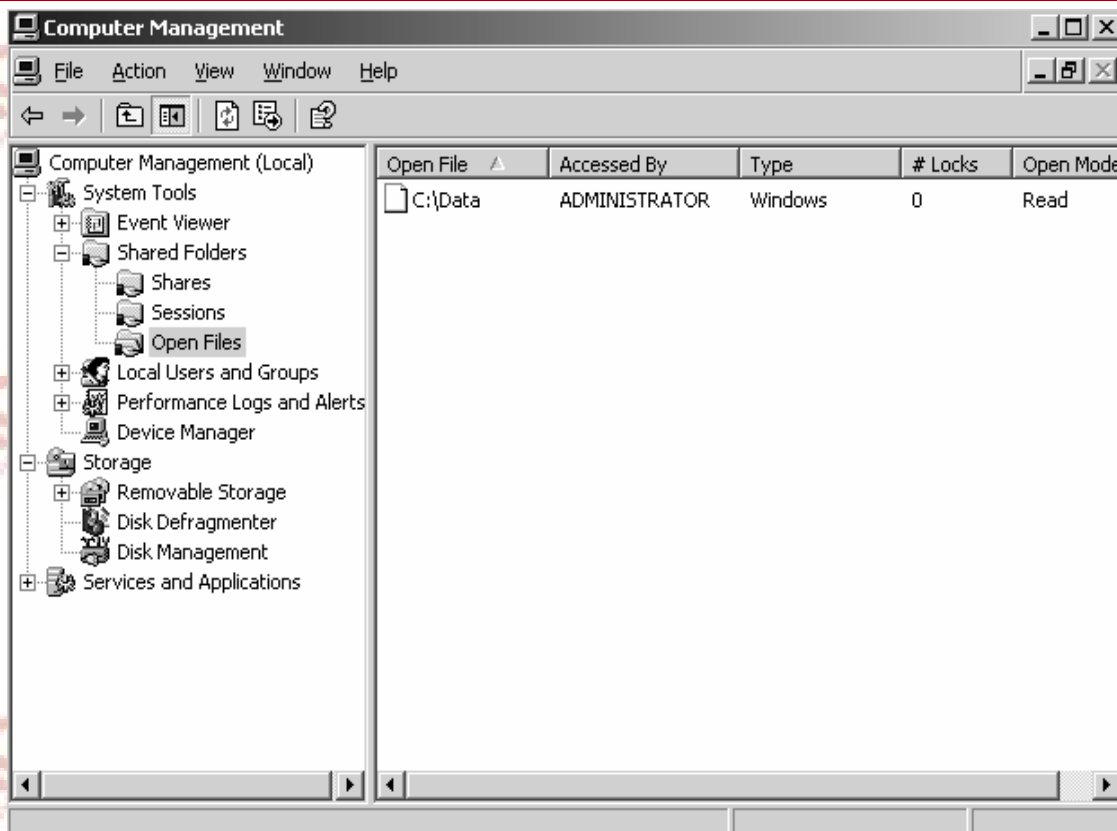
Mục Sessions cung cấp các thông tin sau:

- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tệp tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.
- Truy cập của người dùng Guest hay không?

#### 7.2.3.4. Xem các tệp tin đang mở trong các thư mục dùng chung

Muốn xem các tệp tin đang mở trong các thư mục dùng chung bạn nhấp chuột vào mục Open Files. Mục Open Files cung cấp các thông tin sau:

- Đường dẫn và tệp tin đang được mở.
- Tên tài khoản người dùng đang truy cập tệp tin đó.
- Hệ điều hành mà người dùng sử dụng để truy cập tệp tin.
- Trạng thái tệp tin có đang bị khoá hay không.
- Trạng thái mở sử dụng tệp tin (Read hoặc Write).



#### 7.2.4. Chia sẻ máy in

##### 7.2.4.1. Cài máy in

Trước khi có thể truy xuất vào thiết bị máy in vật lý thông qua hệ điều hành Windows Server 2003 thì bạn phải tạo ra một máy in logic. Nếu máy in của bạn có tính năng Plug and Play thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành Windows Server 2003. Tiện ích Found New Hardware Wizard sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn cho bạn từng bước để cài đặt máy in. Nếu hệ điều hành nhận diện không chính xác thì bạn dùng đĩa CD được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Ngoài ra, bạn cũng có thể tự mình thực hiện tạo ra một máy in logic bằng cách sử dụng tiện ích Add Printer Wizard. Để có thể tạo ra một máy in logic trong Windows Server 2003 thì trước hết bạn phải đăng nhập vào hệ thống với vai trò là một thành viên của nhóm Administrators hay nhóm Power Users (trong trường hợp đây là một Server thành viên) hay nhóm Server Operators (trong trường hợp đây là một Domain Controller).

Bạn có thể tạo ra một máy in logic cục bộ tương ứng với một máy in vật lý được gắn trực tiếp vào máy tính cục bộ của mình hoặc tương ứng với một máy in mạng (máy in mạng được gắn vào một máy tính khác trong mạng hay một thiết bị Print Server).

Thao tác tạo một máy in cục bộ hay một máy in mạng:

- Nháy chuột chọn *Start*, rồi chọn *Printers And Faxes*.
- Nháy vào biểu tượng *Add Printer*, tiện ích *Add Printer Wizard* sẽ được khởi động. Nháy chuột vào nút *Next* để tiếp tục.
- Hộp thoại *Local Or Network Printer* xuất hiện. Bạn nháy vào tùy chọn *Local Printer Attached To This Computer* trong trường hợp bạn có một máy in vật lý gắn trực tiếp vào máy tính của mình. Nếu trường hợp ta đang tạo ra một máy in logic

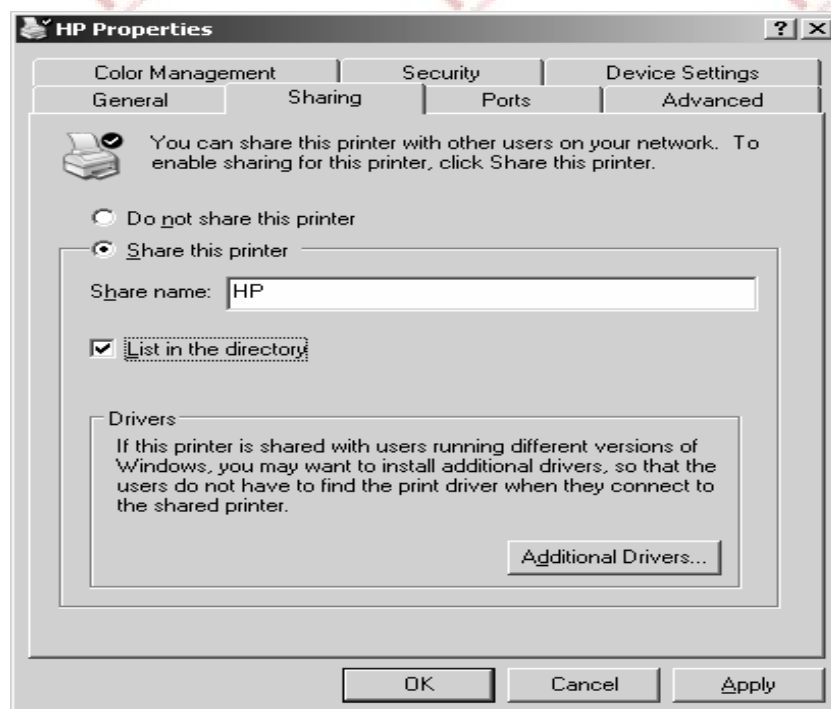
ứng với một máy in mạng thì ta nhấn vào tùy chọn *A Printer Attached To Another Computer*. Nếu máy in được gắn trực tiếp vào máy tính, bạn có thể chọn thêm tính năng *Automatically Detect And Install My Plug And Play Printer*. Tùy chọn này cho phép hệ thống tự động quét máy tính của bạn để phát hiện ra các máy in Plug and Play và tự động cài đặt các máy in đó cho bạn. Khi đã hoàn tất việc chọn lựa, nhấn chuột vào nút Next để sang bước kế tiếp.

- Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích *Found New Hardware Wizard*. Tiện ích này sẽ hướng dẫn bạn tiếp tục cài đặt driver máy in qua từng bước.
- Hộp thoại *Print Test Page* xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính của bạn, bạn nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, nếu máy in là máy in mạng thì bạn nên bỏ qua bước này. Nhấn chuột vào nút Next để sang bước kế tiếp.
- Hộp thoại *Completing The Add Printer Wizard* hiện ra. Hộp thoại để ta xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Nếu bạn phát hiện có thông tin nào không chính xác, hãy nhấn chuột vào nút Back để quay lại sửa chữa thông tin cho đúng. Còn nếu nhận thấy mọi thứ đều ổn cả thì bạn nhấn chuột vào nút Finish.
- Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ *Printer And Faxes*. Theo mặc định, máy in sẽ được chia sẻ.

#### 7.2.4.2. Chia sẻ máy in

Nhấn phải chuột trên biểu tượng máy in cần chia sẻ, chọn *Properties*. Hộp thoại *Properties* xuất hiện, bạn chọn *Tab Sharing*.

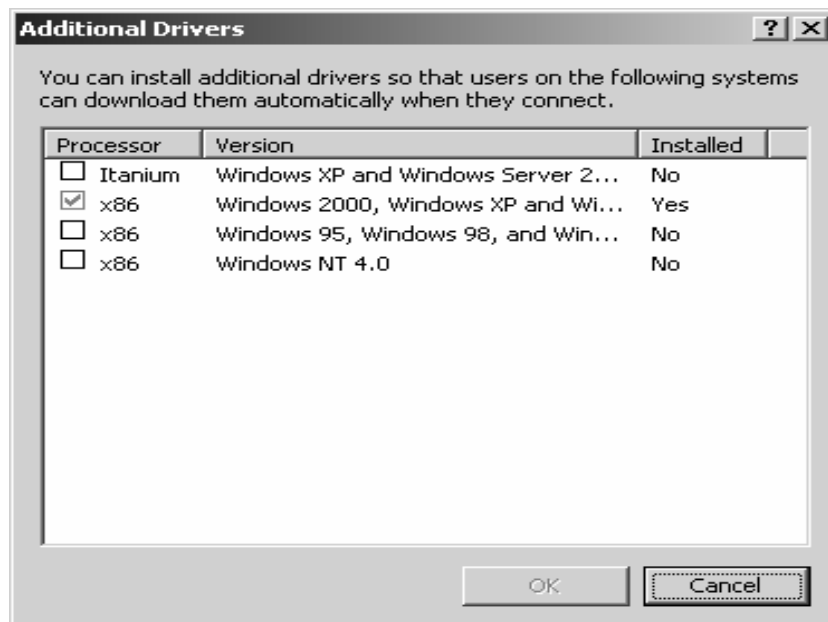
Để chia sẻ máy in này cho nhiều người dùng, bạn nhấn chuột chọn *Share this printer*. Trong mục *Share name*, bạn nhập vào tên chia sẻ của máy in, tên này sẽ được nhìn thấy trên mạng. Bạn cũng có thể chọn mục *List In The Directory* để cho phép người dùng có thể tìm kiếm máy in thông qua *Active Directory* theo một vài thuộc tính đặc trưng nào đó.





Ngoài ra, trong Tab Sharing, ta có thể cấu hình driver hỗ trợ cho các máy trạm sử dụng máy in trong trường hợp máy trạm không phải là Windows Server 2003. Đây là một tính năng cần thiết vì nó cho phép chỉ định các driver hỗ trợ in để các máy trạm có thể tải về một cách tự động. Mặc định, driver duy nhất được nạp vào là driver của hãng Intel cho các máy trạm là Windows 2000, Windows Server 2003 và Windows XP. Để cung cấp thêm các driver cho máy trạm khác, bạn nhấp chuột vào nút *Additional Drivers* nằm phía dưới *Tab Sharing*. Hộp thoại Additional Drivers xuất hiện. Windows Server 2003 hỗ trợ các driver thêm vào cho các Client là một trong những hệ điều hành sau:

- Itanium Windows XP hay Windows Server 2003.
- X86 Windows 2000, Windows XP, hay Windows Server 2003 (mặc định).
- X86 Windows 95, Windows 98, hay Windows Millennium Edition.
- X86 Windows NT 4.



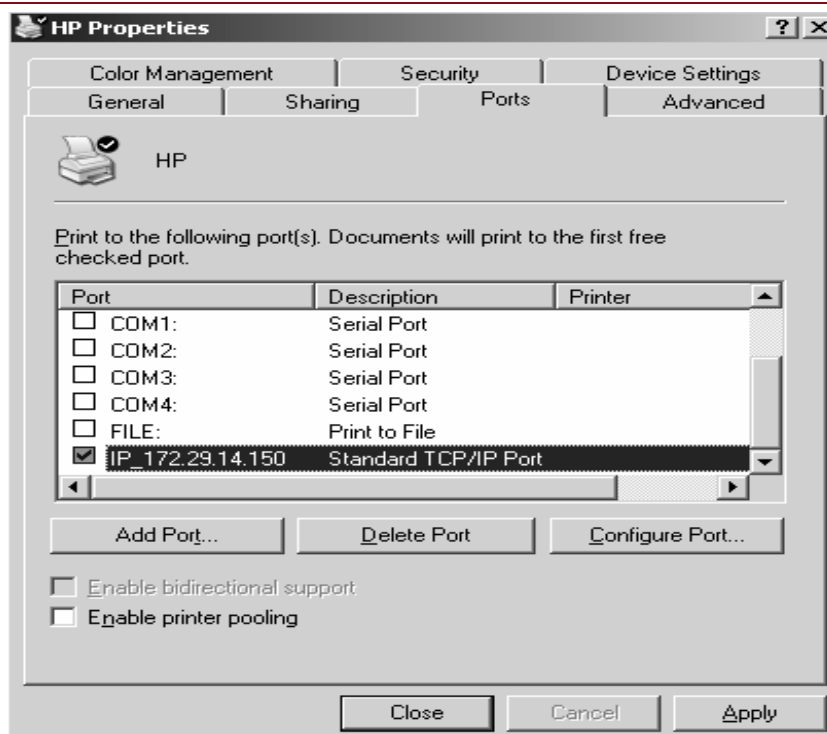
#### 7.2.4.3. Cấu hình cổng (Port)

Cấu hình các thông số trong Tab Port.

Trong hộp thoại Properties, bạn chọn Tab Port để cấu hình tất cả các Port đã được định nghĩa cho máy in sử dụng. Một Port được định nghĩa như một interface cho phép máy tính giao tiếp với thiết bị máy in. Windows Server 2003 hỗ trợ các Port vật lý (Local Port) và các Port TCP/IP (Port Logic).

Port vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính. Trong trường hợp Windows Server 2003 đang được triển khai trong một nhóm làm việc nhỏ, hầu như bạn sẽ gắn máy in vào Port LPT1.

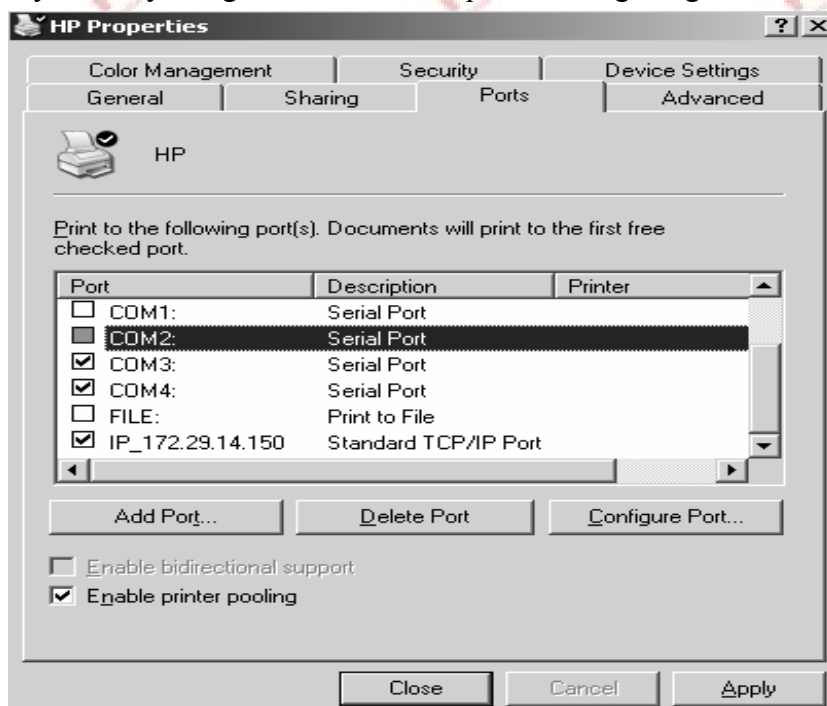
Port TCP/IP được sử dụng khi máy in có thể kết nối trực tiếp vào mạng (trên máy in có hỗ trợ Port RJ45) và máy in này có một địa chỉ IP để nhận dạng. Ưu điểm của máy in mạng là máy in có thể đặt bất kì nơi nào trong hệ thống mạng. Khi đó bạn cần chỉ định một Port TCP/IP và khai báo địa chỉ IP của máy in mạng. Cùng với việc xóa và cấu hình lại một Port đã tồn tại, bạn cũng có thể thiết lập Printer Pooling và điều hướng các công việc in ấn đến một máy in khác.



#### 7.2.4.4. Printer Pooling

Printer Pool được sử dụng nhằm phối hợp nhiều máy in vật lý với một máy in logic. Lợi ích của việc sử dụng Printer Pool là máy in rảnh đầu tiên sẽ thực hiện thao tác in ấn cho bạn. Tính năng này rất hữu dụng trong trường hợp ta có một nhóm các máy in vật lý được chia sẻ cho một nhóm người dùng.

Để cấu hình một Printer Pool, bạn nhấp chuột vào tùy chọn Enable Printer Pooling nằm ở phía dưới Tab Port trong hộp thoại Properties. Sau đó, kiểm tra lại tất cả các Port mà ta dự định gắn các máy in vật lý trong Printer Pool vào. Nếu ta không chọn tùy chọn Enable Printer Pooling thì ta chỉ có một Port duy nhất cho mỗi máy in. Chú ý tất cả các máy in vật lý trong một Printer Pool phải sử dụng cùng một driver máy in.



### 7.3. Dịch vụ mạng

#### 7.3.1. Mạng máy tính

##### 7.3.1.1. Khái niệm

Mạng máy tính là một nhóm các máy tính, thiết bị ngoại vi được nối kết với nhau thông qua các phương tiện truyền dẫn như cáp, sóng điện từ, ... giúp cho các thiết bị này có thể trao đổi dữ liệu với nhau một cách dễ dàng.

Các thành phần cơ bản cấu thành nên mạng máy tính:

- Các loại máy tính: Palm, Laptop, PC, MainFrame...
- Các thiết bị giao tiếp: Card mạng (NIC hay Adapter), Hub, Switch, Router...
- Môi trường truyền dẫn: cáp, sóng điện từ, sóng vi ba, tia hồng ngoại...
- Các protocol: TCP/IP, NetBeui, Apple Talk, IPX/SPX...
- Các hệ điều hành mạng: WinNT, Win2000, Win2003, Novell Netware, Unix...
- Các tài nguyên: file, thư mục.
- Các ứng dụng mạng: phần mềm quản lý kho bãi, phần mềm bán vé tàu...

**Server:** là máy tính được cài đặt các phần mềm chuyên dụng làm chức năng cung cấp các dịch vụ cho các máy tính khác. Tùy theo dịch vụ mà các máy này cung cấp, người ta chia thành các loại server khác nhau, chẳng hạn: File server (cung cấp các dịch vụ về file và thư mục), Print server (cung cấp các dịch vụ về in ấn). Do làm chức năng phục vụ cho các máy tính khác nên cấu hình máy server phải mạnh.

**Client (máy trạm):** là máy tính sử dụng các dịch vụ mà các máy server cung cấp. Do xử lý số công việc không lớn nên thông thường các máy này không yêu cầu có cấu hình mạnh.

##### 7.3.1.2. Các loại hình mạng

###### Mạng cục bộ LAN (Local Area Network)

Mạng LAN là một nhóm máy tính và các thiết bị truyền thông mạng được nối kết với nhau trong một khu vực nhỏ như một toà nhà cao ốc, khuôn viên trường đại học, khu giải trí ...

Mạng LAN thường có đặc điểm sau:

- Băng thông lớn, có khả năng chạy các ứng dụng trực tuyến như xem phim, hội thảo qua mạng.
- Nhảy thước mạng bị giới hạn bởi các thiết bị.
- Chi phí các thiết bị mạng LAN tương đối rẻ.
- Quản trị đơn giản.

###### Mạng đô thị MAN (Metropolitan Area Network)

Mạng MAN gần giống như mạng LAN nhưng giới hạn của nó là một thành phố hay một quốc gia. Mạng MAN nối kết các mạng LAN lại với nhau thông qua các phương tiện truyền dẫn khác nhau (cáp quang, cáp đồng, sóng...) và các phương thức truyền thông khác nhau.

Đặc điểm của mạng MAN:

- Băng thông mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng...

- Do MAN nối kết nhiều LAN với nhau nên độ phức tạp cũng tăng đồng thời công tác quản trị sẽ khó khăn hơn.
- Chi phí các thiết bị mạng MAN tương đối đắt tiền.

### **Mạng diện rộng WAN (Wide Area Network)**

Mạng WAN bao phủ vùng địa lý rộng lớn có thể là một quốc gia, một lục địa hay toàn cầu. Mạng WAN thường là mạng của các công ty đa quốc gia hay toàn cầu, điển hình là mạng Internet. Do phạm vi rộng lớn của mạng WAN nên thông thường mạng WAN là tập hợp các mạng LAN, MAN nối lại với nhau bằng các phương tiện như: vệ tinh (Satellites), sóng viba (Microwave), cáp quang, cáp điện thoại...

Đặc điểm của mạng WAN:

- Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng offline như e-mail, web, ftp...
- Phạm vi hoạt động rộng lớn không giới hạn.
- Do kết nối của nhiều LAN, MAN lại với nhau nên mạng rất phức tạp và có tính toàn cầu nên thường là có tổ chức quốc tế đứng ra quản trị.
- Chi phí cho các thiết bị và các công nghệ mạng WAN rất đắt tiền.

### **7.3.1.3. Mô hình OSI**

#### **Giao thức (Protocol)**

Là quy tắc giao tiếp (tiêu chuẩn giao tiếp) giữa hai hệ thống giúp chúng hiểu và trao đổi dữ liệu được với nhau.

Ví dụ: Transmission Control Protocol/ Internetnetwork Protocol (TCP/IP), NetBIOS, ...

#### **Các tổ chức chuẩn**

- ITU (International Telecommunication Union): Hiệp hội Viễn thông quốc tế.
- IEEE (Institute of Electrical and Electronic Engineers): Viện các kỹ sư điện và điện tử.
- ISO (International Standardization Organization): Tổ chức Tiêu chuẩn quốc tế, trụ sở tại Geneve, Thụy Sĩ.

#### **Mô hình OSI**

Mô hình OSI (Open System Interconnection): là mô hình được tổ chức ISO đề xuất từ 1977 và công bố lần đầu vào 1984. Để các máy tính và các thiết bị mạng có thể truyền thông với nhau phải có những quy tắc giao tiếp được các bên chấp nhận.

Mô hình OSI là một khuôn mẫu giúp chúng ta hiểu dữ liệu truyền qua mạng như thế nào đồng thời cũng giúp chúng ta hiểu được các chức năng mạng của mỗi lớp.

Trong mô hình OSI có bảy lớp, mỗi lớp mô tả một phần chức năng độc lập. Sự tách lớp của mô hình này mang lại những lợi ích sau:

- Chia hoạt động thông tin mạng thành những phần nhỏ hơn, đơn giản hơn giúp chúng ta dễ khảo sát và tìm hiểu hơn.
- Chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà cung cấp sản phẩm.
- Ngăn chặn được tình trạng sự thay đổi của một lớp làm ảnh hưởng đến các lớp khác, như vậy giúp mỗi lớp có thể phát triển độc lập và nhanh chóng hơn.

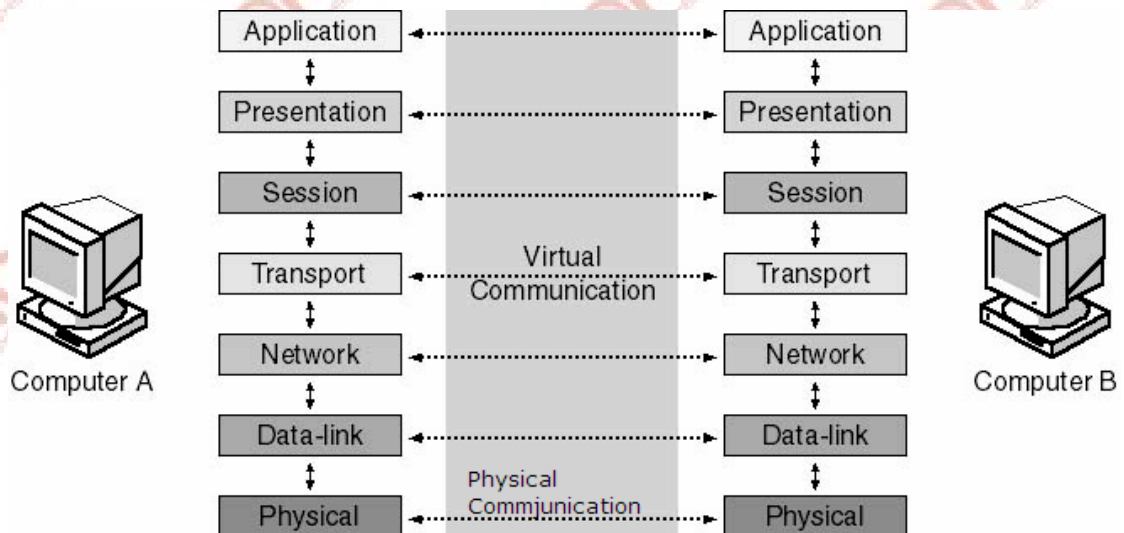


Mô hình tham chiếu OSI định nghĩa các quy tắc cho các nội dung sau:

- Cách thức các thiết bị giao tiếp và truyền thông được với nhau.
- Các phương pháp để các thiết bị trên mạng khi nào thì được truyền dữ liệu, khi nào thì không được.
- Các phương pháp để đảm bảo truyền đúng dữ liệu và đúng bên nhận.
- Cách thức vận tải, truyền, sắp xếp và kết nối với nhau.
- Cách thức đảm bảo các thiết bị mạng duy trì tốc độ truyền dữ liệu thích hợp.
- Cách biểu diễn một bit thiết bị truyền dẫn.

Mô hình tham chiếu OSI được chia thành bảy lớp với các chức năng sau:

- Application Layer (lớp ứng dụng): giao diện giữa ứng dụng và mạng.
- Presentation Layer (lớp trình bày): thỏa thuận khuôn dạng trao đổi dữ liệu.
- Session Layer (lớp phiên): cho phép người dùng thiết lập các kết nối.
- TransPort Layer (lớp vận chuyển): đảm bảo truyền thông giữa hai hệ thống.
- Network Layer (lớp mạng): định hướng dữ liệu truyền trong môi trường liên mạng.
- Data link Layer (lớp liên kết dữ liệu): xác định việc truy xuất đến các thiết bị.
- Physical Layer (lớp vật lý): chuyển đổi dữ liệu thành các bit và truyền đi.



#### 7.3.1.4. Chức năng của các lớp trong mô hình tham chiếu OSI

**Tầng ứng dụng (Application Layer):** là giao diện giữa các chương trình ứng dụng của người dùng và mạng. Lớp Application xử lý truy nhập mạng, kiểm soát luồng và phục hồi lỗi. Lớp này không cung cấp các dịch vụ cho lớp nào mà nó cung cấp dịch vụ cho các ứng dụng như: truyền file, E-mail, HTTP, FTP, SMTP...

**Tầng trình diễn (Presentation Layer):** chịu trách nhiệm thương lượng và xác lập định dạng dữ liệu được trao đổi. Nó đảm bảo thông tin mà lớp ứng dụng của một hệ thống đầu cuối gửi đi, lớp ứng dụng của hệ thống khác có thể đọc được. Lớp trình bày chuyển đổi giữa nhiều dạng dữ liệu khác nhau thông qua một dạng chung, đồng thời nó cũng có thể nén và giải nén dữ liệu. Thứ tự byte, bit bên gửi và bên nhận quy ước quy tắc gửi nhận một chuỗi byte, bit từ trái qua phải hay từ phải qua trái. Nếu hai bên không thống nhất thì sẽ có sự chuyển đổi thứ tự các byte bit vào trước hoặc sau khi



truyền. Lớp presentation cũng quản lý các cấp độ nén dữ liệu nhằm giảm số bit cần truyền. Ví dụ: JPEG, ASCII, EBCDIC....

**Tầng phiên (Session Layer):** chức năng thiết lập, quản lý và kết thúc các phiên trao đổi thông tin giữa hai thiết bị đầu cuối. Lớp phiên cung cấp các dịch vụ cho lớp trình bày. Lớp phiên cung cấp sự đồng bộ hóa giữa các tác vụ người dùng bằng cách đặt những điểm kiểm tra vào luồng dữ liệu. Bằng cách này, nếu mạng không hoạt động thì chỉ có dữ liệu truyền sau điểm kiểm tra cuối cùng mới phải truyền lại. Lớp này cũng thi hành kiểm soát hội thoại giữa các quá trình giao tiếp, điều chỉnh bên nào truyền, khi nào, trong bao lâu. Ví dụ như: RPC, NFS,... Lớp này kết nối theo ba cách: Half-duplex, Simplex, Full-duplex.

**Tầng vận chuyển (TransPort Layer):** lớp vận chuyển phân đoạn dữ liệu từ hệ thống máy truyền và tái thiết lập dữ liệu vào một luồng dữ liệu tại hệ thống máy nhận đảm bảo rằng việc bàn giao các thông điệp giữa các thiết bị đáng tin cậy. Dữ liệu tại lớp này gọi là segment. Lớp này thiết lập, duy trì và kết thúc các mạch ảo đảm bảo cung cấp các dịch vụ chính sau:

- Xếp thứ tự các phân đoạn: khi một thông điệp lớn được tách thành nhiều phân đoạn nhỏ để bàn giao, lớp vận chuyển sẽ sắp xếp thứ tự các phân đoạn trước khi ráp nối các phân đoạn thành thông điệp ban đầu.
- Kiểm soát lỗi: khi có phân đoạn bị thất bại, sai hoặc trùng lặp, lớp vận chuyển sẽ yêu cầu truyền lại.
- Kiểm soát luồng: lớp vận chuyển dùng các tín hiệu báo nhận để xác nhận. Bên gửi sẽ không truyền đi phân đoạn dữ liệu kế tiếp nếu bên nhận chưa gửi tín hiệu xác nhận rằng đã nhận được phân đoạn dữ liệu trước đó đầy đủ.

**Tầng mạng (Network Layer):** lớp mạng chịu trách nhiệm đánh địa chỉ các thông điệp, diễn dịch địa chỉ và tên logic thành địa chỉ vật lý đồng thời nó cũng chịu trách nhiệm gửi packet từ mạng nguồn đến mạng đích. Lớp này quyết định đường đi (định tuyến) từ máy tính nguồn đến máy tính đích. Nó quyết định dữ liệu sẽ truyền trên đường nào dựa vào tình trạng, ưu tiên dịch vụ và các yếu tố khác. Nó cũng quản lý lưu lượng trên mạng chẳng hạn như chuyển đổi gói, định tuyến và kiểm soát sự tắc nghẽn dữ liệu. Nếu bộ thích ứng mạng trên bộ định tuyến (Router) không thể truyền đủ đoạn dữ liệu mà máy tính nguồn gửi đi, lớp Network trên bộ định tuyến sẽ chia dữ liệu thành những đơn vị nhỏ hơn, nói cách khác, nếu máy tính nguồn gửi đi các gói tin có kích thước là 20Kb, trong Router chỉ cho phép các gói tin có kích thước là 10Kb đi qua, thì lúc đó lớp Network của Router sẽ chia gói tin ra làm 2, mỗi gói tin có kích thước là 10Kb. Ở đầu nhận, lớp Network ráp nối lại dữ liệu. Ví dụ: một số giao thức lớp này: IP, IPX,... Dữ liệu ở lớp này được gọi là packet hoặc datagram.

**Tầng liên kết dữ liệu (Data link Layer):** cung cấp khả năng chuyển dữ liệu tin cậy xuyên qua một liên kết vật lý. Tầng này liên quan đến:

- Địa chỉ vật lý.
- Mô hình mạng.
- Cơ chế truy cập đường truyền.
- Thông báo lỗi.
- Thứ tự phân phối frame.

Tại lớp data link, các bit đến từ lớp vật lý được chuyển thành các frame dữ liệu bằng cách dùng một số giao thức tại lớp này. Lớp data link được chia thành hai lớp con:

- LLC (Logical Link Control).
- MAC (Media Access Control).

Tầng con LLC là phần trên so với các giao thức truy cập đường truyền khác, nó cung cấp sự mềm dẻo về giao tiếp. Bởi vì lớp con LLC hoạt động độc lập với các giao thức truy cập đường truyền, cho nên các giao thức lớp trên hơn (ví dụ như IP ở lớp mạng) có thể hoạt động mà không phụ thuộc vào loại phương tiện LAN. Lớp con LLC có thể lệ thuộc vào các lớp thấp hơn trong việc cung cấp truy cập đường truyền.

Tầng con MAC cung cấp tính tự truy cập vào môi trường LAN. Khi nhiều trạm cùng truy cập chia sẻ môi trường truyền, để định danh mỗi trạm, lớp cho MAC định nghĩa một trường địa chỉ phần cứng, gọi là địa chỉ MAC address. Địa chỉ MAC là một con số đơn nhất đối với mỗi giao tiếp LAN (card mạng).

**Tầng vật lý (Physical Layer):** định nghĩa các quy cách về điện, cơ, thủ tục và các đặc tả chức năng để kích hoạt, duy trì và dùng một liên kết vật lý giữa các hệ thống đầu cuối. Một số các đặc điểm trong lớp vật lý này bao gồm:

- Mức điện thế.
- Khoảng thời gian thay đổi điện thế.
- Tốc độ dữ liệu vật lý.
- Khoảng đường truyền tối đa.
- Các đầu nối vật lý.

### 7.3.1.5. Mô hình TCP/IP

Sự hình thành kỹ thuật Internet là kết quả nghiên cứu dưới sự tài trợ của Defense/Advanced Research Projects Agency (ARPA/DARPA), bao gồm một tập hợp của các chuẩn mạng, đặc tả chi tiết cách thức mà các máy tính thông tin liên lạc với nhau, cũng như các quy ước cho các mạng interconnecting và định tuyến giao thông. Tên chính thức của bộ giao thức là TCP/IP Internet Protocol Suite và thường được gọi là TCP/IP, có thể dùng để thông tin liên lạc qua tập hợp bất kỳ các mạng interconnected. Nó có thể dùng để liên kết mạng trong một công ty, không nhất thiết phải nối kết với các mạng khác bên ngoài.

#### Các lớp của mô hình tham chiếu TCP/IP

- Lớp Application: quản lý các giao thức, như hỗ trợ việc trình bày, mã hóa, và quản lý cuộc gọi. Lớp Application cũng hỗ trợ nhiều ứng dụng, như: FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), TFTP (Trivial File Transfer Protocol).
- Lớp TransPort: đảm nhiệm việc vận chuyển từ nguồn đến đích. Tầng TransPort đảm nhiệm việc truyền dữ liệu thông qua hai giao thức: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol).
- Lớp Internet: đảm nhiệm việc chọn lựa đường đi tốt nhất cho các gói tin. Giao thức được sử dụng chính ở tầng này là giao thức IP (Internet Protocol).

Application
Transport
Internet
Network Interface

- Lớp Network Interface: có tính chất tương tự như hai lớp Data Link và Physical trong kiến trúc OSI.

**Địa chỉ IP**

Ở đây ta đề cập đến địa chỉ IP phiên bản 4.

Là địa chỉ có cấu trúc, được chia làm hai phần: network\_id và host\_id.

Là một số có kích thước 32 bit. Khi trình bày, người ta chia thành bốn phần, mỗi phần có kích thước 8 bit, gọi là octet hoặc byte. Có các cách trình bày sau:

- Ký pháp thập phân có dấu chấm. Ví dụ: 172.16.30.56.
- Ký pháp nhị phân. Ví dụ: 10101100 00010000 00011110 00111000.

Không gian địa chỉ IP (gồm  $2^{32}$  địa chỉ) được chia thành nhiều lớp (class) để dễ quản lý. Đó là các lớp: A, B, C, D và E; trong đó các lớp A, B và C được triển khai để đặt cho các host trên mạng Internet; lớp D dùng cho các nhóm multicast; còn lớp E phục vụ cho mục đích nghiên cứu.

Địa chỉ IP còn được gọi là địa chỉ logical, trong khi địa chỉ MAC còn gọi là địa chỉ vật lý.

**Các lớp địa chỉ****Lớp A:**

Dành 01 byte cho phần network\_id và 03 byte cho phần host\_id.

Để nhận diện lớp A, bit đầu tiên của byte đầu tiên phải là bit 0. Dưới dạng nhị phân, byte này có dạng 0xxxxxxx. Vì vậy, những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 (00000000) đến 127 (01111111) sẽ thuộc lớp A. Ví dụ địa chỉ 50.14.32.8 là một địa chỉ lớp A ( $50 < 127$ ).

Byte đầu tiên này cũng chính là network\_id, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại bảy bit để đánh thứ tự các mạng, ta được 128 ( $2^7$ ) mạng lớp A khác nhau. Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 ( $2^7 - 2$ ) địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.

Phần host\_id chiếm 24 bit, tức có thể đặt địa chỉ cho 16.777.216 ( $2^{24}$ ) host khác nhau trong mỗi mạng. Bỏ đi một địa chỉ mạng (phần host\_id chứa toàn các bit 0) và một địa chỉ broadcast (phần host\_id chứa toàn các bit 1) như vậy có tất cả 16.777.214 host khác nhau trong mỗi mạng lớp A. Ví dụ, đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.

**Lớp B:**

Dành hai byte cho mỗi phần network\_id và host\_id. Dấu hiệu để nhận dạng địa chỉ lớp B là byte đầu tiên luôn bắt đầu bằng hai bit 10. Dưới dạng nhị phân, là octet có dạng 10xxxxxx. Vì vậy những địa chỉ nằm trong khoảng từ 128 (10000000) đến 191 (10111111) sẽ thuộc về lớp B. Ví dụ 172.29.10.1 là một địa chỉ lớp B ( $128 < 172 < 191$ ).

Phần network\_id chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16.384 ( $2^{14}$ ) mạng khác nhau (128.0.0.0 đến 191.255.0.0).

Phần host\_id dài 16 bit hay có 65536 ( $2^{16}$ ) giá trị khác nhau. Trừ 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B. Ví dụ, đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.

**Lớp C:**

Ba byte cho phần network\_id và một byte cho phần host\_id.

Byte đầu tiên luôn bắt đầu bằng ba bit 110 và dạng nhị phân của octet này là 110xxxxx. Như vậy những địa chỉ nằm trong khoảng từ 192 (11000000) đến 223 (11011111) sẽ thuộc về lớp C. Ví dụ một địa chỉ lớp C là 203.162.41.235 ( $192 < 203 < 223$ ).

Phần network\_id dùng ba byte hay 24 bit, trừ đi 3 bit làm ID của lớp, còn lại 21 bit hay  $2.097.152$  ( $2^{21}$ ) địa chỉ mạng (từ 192.0.0.0 đến 223.255.255.0).

Phần host\_id dài một byte cho 256 ( $2^8$ ) giá trị khác nhau. Trừ đi hai trường hợp đặc biệt ta còn 254 host khác nhau trong một mạng lớp C. Ví dụ, đối với mạng 203.162.41.0, các địa chỉ host hợp lệ là từ 203.162.41.1 đến 203.162.41.254.

### Lớp D và E:

Các địa chỉ có byte đầu tiên nằm trong khoảng 224 đến 255 là các địa chỉ thuộc lớp D hoặc E.

## 7.3.2. Dịch vụ DHCP

### 7.3.2.1. DHCP

Mỗi thiết bị trên mạng có dùng bộ giao thức TCP/IP đều phải có một địa chỉ IP hợp lệ, phân biệt. Để hỗ trợ cho vấn đề theo dõi và cấp phát các địa chỉ IP được chính xác, tổ chức IETF (Internet Engineering Task Force) đã phát triển ra giao thức DHCP (Dynamic Host Configuration Protocol).

Dịch vụ DHCP này cho phép cấp phát động các thông số cấu hình mạng cho các máy (DHCP client). Các hệ điều hành của Microsoft và các hệ điều hành khác như Unix hoặc Macintosh đều hỗ trợ cơ chế nhận các thông số động. Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:

- Khắc phục được tình trạng đụng địa chỉ IP và giảm chi phí quản trị cho hệ thống mạng.
- Giúp cho các nhà cung cấp dịch vụ (ISP) tiết kiệm được số lượng địa chỉ IP thật (Public IP).
- Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.
- Kết hợp với hệ thống mạng không dây (Wireless) cung cấp các điểm Hotspot như: nhà ga, sân bay, trường học...

### 7.3.2.2. Giao thức DHCP

Giao thức DHCP làm việc theo mô hình client/server. Theo đó, quá trình tương tác giữa DHCP client và server diễn ra theo các bước cơ bản sau:

- Khi client khởi động, nó gửi gói tin broadcast DHCPDISCOVER, yêu cầu một server DHCP phục vụ mình. Gói tin này cũng chứa địa chỉ MAC của máy client.
- Các máy DHCP Server trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy Client gói tin DHCPOFFER, đề nghị cấp địa chỉ IP trong một khoản thời gian nhất định, kèm theo các thông tin mạng khác (Subnet Mask, địa chỉ của DHCP Server)
- Máy Client sẽ lựa chọn một trong những đề nghị (DHCPOFFER) và gửi broadcast lại gói tin DHCPREQUEST chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được dùng sẽ được các Server rút lại và dùng để cấp phát cho Client khác.

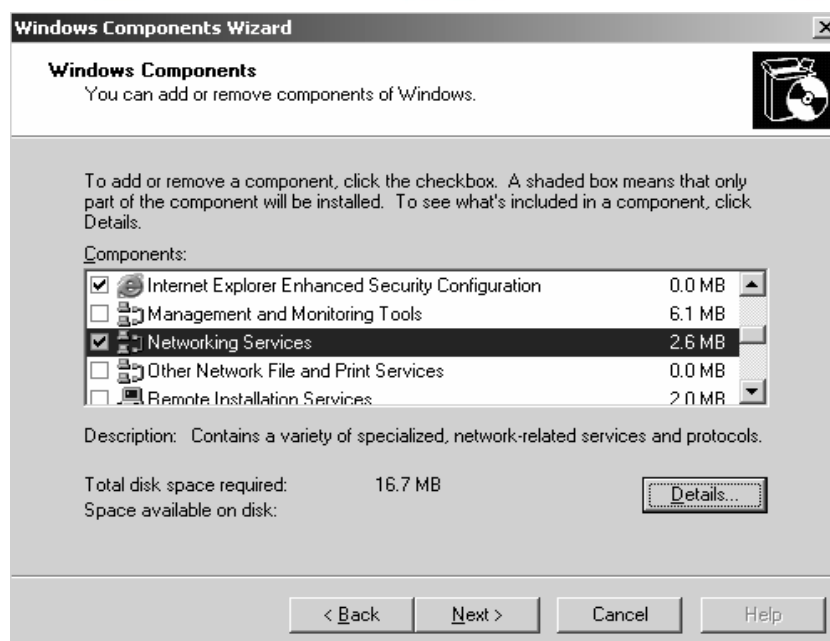


- Máy Server được Client chấp nhận sẽ gửi ngược lại một gói tin DHCPACK như là một lời xác nhận, cho biết là địa chỉ IP và thời hạn cho sử dụng sẽ chính thức được áp dụng. Ngoài ra Server còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ của gateway mặc định, địa chỉ DNS Server, ...

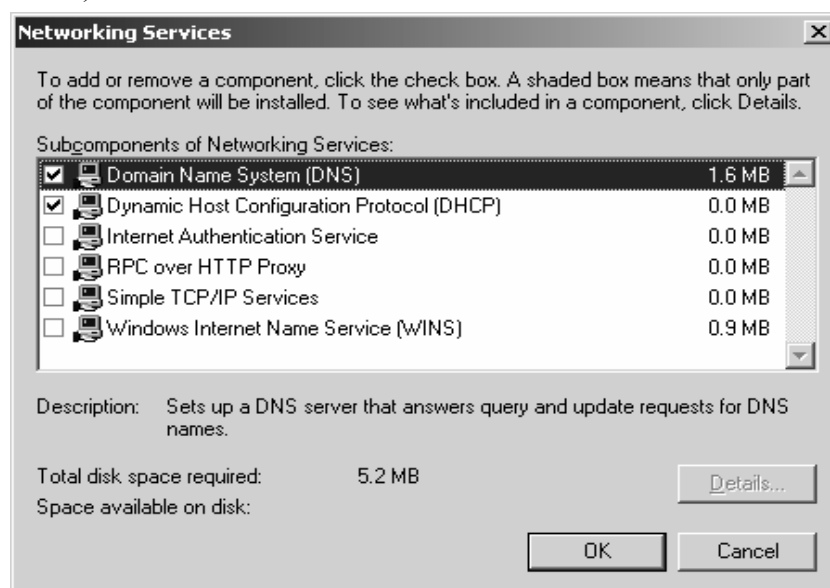
### 7.3.2.3. Cài đặt dịch vụ DHCP

Thực hiện theo các bước sau:

- Chọn menu Start → Settings → Control Panel.
- Trong cửa sổ Control Panel, nhấp chuột vào mục Add → Remove Programs.
- Trong hộp thoại Add → Remove Programs, chọn mục Add → Remove Windows Components.
- Trong hộp thoại Windows Components Wizard, chọn Networking Services và nhấn Details.



Trong hộp thoại Networking Services, chọn mục Dynamic Host Configuration Protocol (DHCP) và nhấn nút OK.





Trở lại hộp thoại Windows Components Wizard, chọn Next. Windows sẽ cài đặt cấu hình các thành phần được lựa chọn (dịch vụ DHCP).

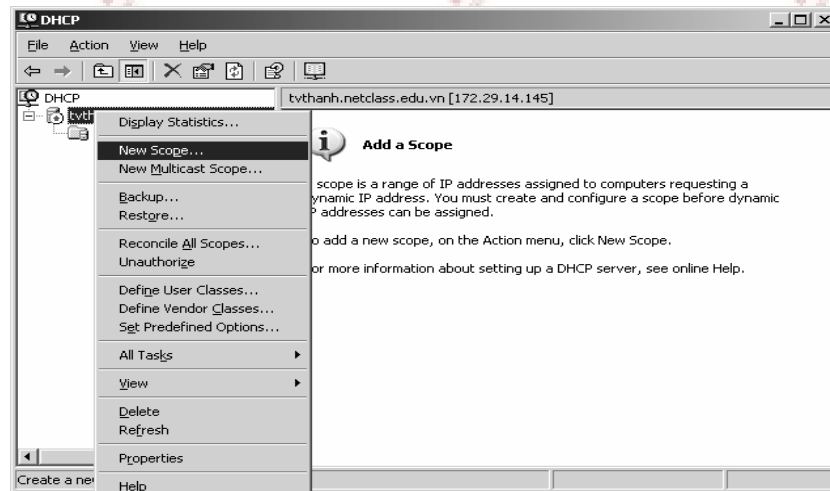
Cuối cùng, trong hộp thoại Completing the Windows Components Wizard, nhấn nút Finish để kết thúc.

#### 7.3.2.4. Cấu hình DHCP

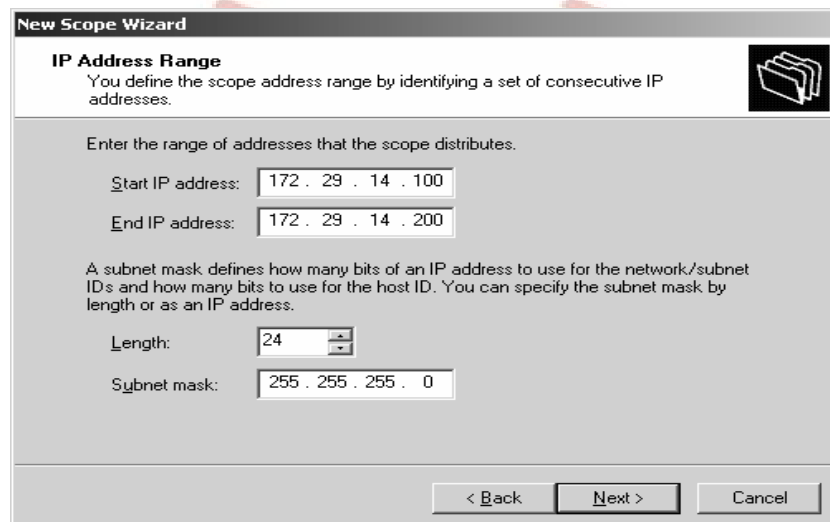
Sau khi cài đặt, dịch vụ DHCP sẽ được thực thi, trong menu Administrative Tools sẽ có biểu tượng DHCP. Để cấp phát địa chỉ, ta cần tạo các kho địa chỉ để cấp phát (Scope).

Để tạo một scope cấp phát địa chỉ:

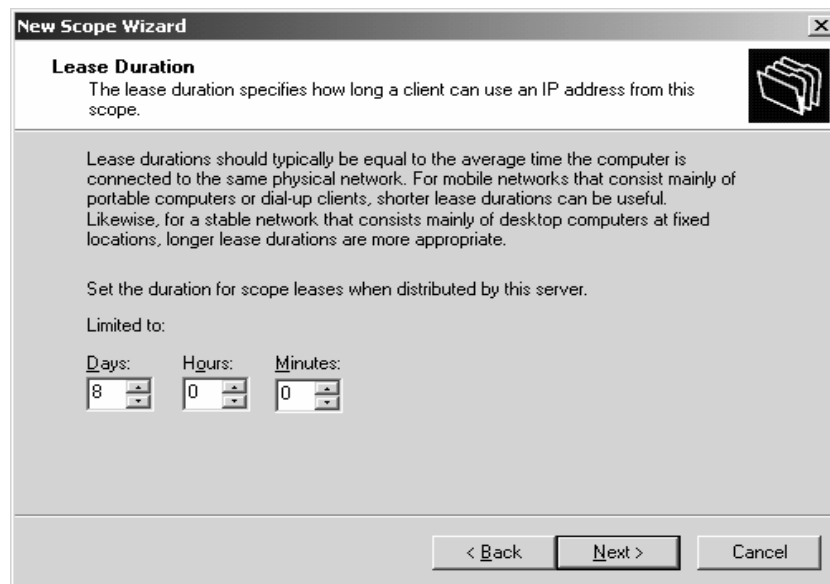
- Chọn menu Start → Programs → Administrative Tools → DHCP.
- Trong cửa sổ quản trị DHCP, nhấp chuột phải lên biểu tượng Server của bạn và chọn mục New Scope trong Popup Menu.



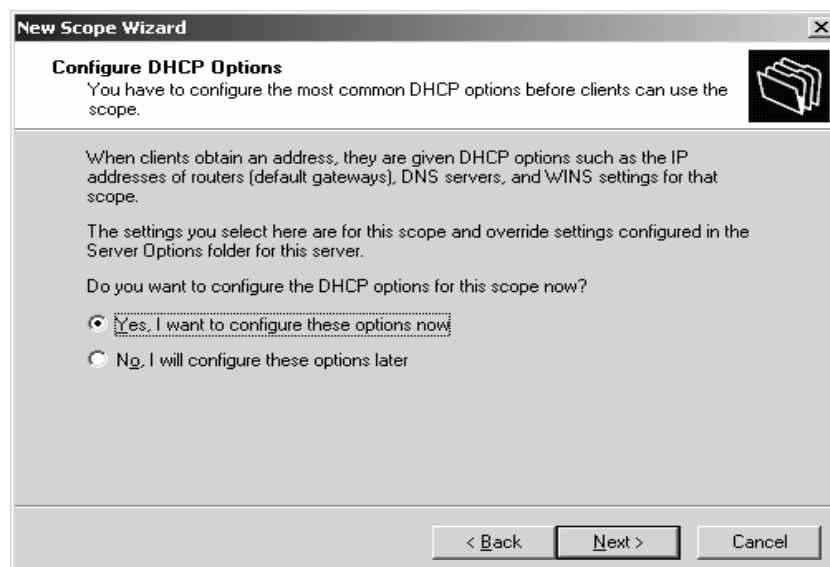
- Hộp thoại New Scope Wizard xuất hiện. Nhấn Next.
- Trong hộp thoại Scope Name, nhập vào tên và chú thích, giúp cho việc nhận diện ra scope này.
- Sau đó nhấn Next.
- Hộp thoại IP Address Range xuất hiện, nhập vào địa chỉ bắt đầu và kết thúc của dải địa chỉ cấp phát.
- Sau đó bạn chỉ định subnet mask bằng cách cho biết số bit 1 hoặc nhập vào chuỗi số. Nhấn Next.



- Trong hộp thoại Add Exclusions, ta thiết lập các địa chỉ sẽ được loại trừ ra khỏi nhóm địa chỉ đã chỉ định ở trên. Thường các địa chỉ loại trừ này được dùng để đặt cho các máy tính dùng địa chỉ tĩnh. Để loại trừ một địa chỉ duy nhất, bạn chỉ cần nhập địa chỉ trong ô Start IP Address và nhấn Add. Để loại trừ một nhóm các địa chỉ, bạn nhập địa chỉ bắt đầu và kết thúc của nhóm đó trong Start IP Address và End IP Address, sau đó nhấn Add. Nhấn Remove để huỷ một hoặc một nhóm các địa chỉ ra khỏi danh sách trên.
- Sau khi đã cấu hình xong, bạn nhấn nút Next để tiếp tục.
- Trong hộp thoại Lease Duration tiếp theo, ta nhập thời gian các máy trạm có thể sử dụng địa chỉ này. Theo mặc định, một máy Client sẽ cố làm mới lại địa chỉ khi đã sử dụng được phân nửa thời gian cho phép. Thời gian cho phép mặc định là 8 ngày. Bạn có thể chỉ định lượng thời gian khác tùy theo nhu cầu.
- Sau khi đã cấu hình xong, nhấn Next để tiếp tục.



- Hộp thoại Configure DHCP Options xuất hiện. Bạn có thể đồng ý để cấu hình các tùy chọn phổ biến (chọn Yes, I want to configure these options now) hoặc không đồng ý, để việc thiết lập này thực hiện sau (chọn No, I will configure these options later).

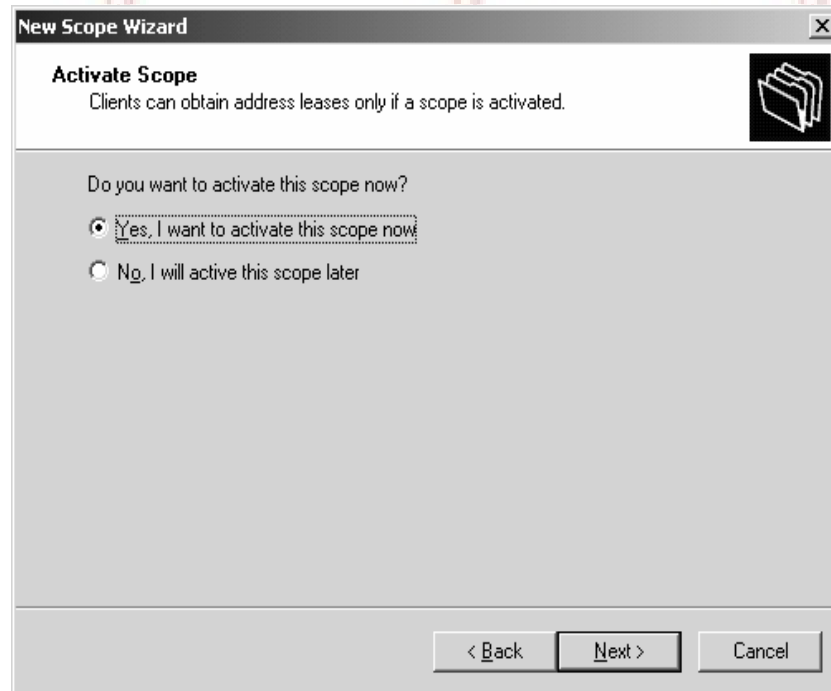


- Trong hộp thoại Router (Default Gateway), nhập địa chỉ IP của default gateway mà các máy DHCP Client sẽ sử dụng và nhấn Add. Sau đó nhấn Next.

- Trong hộp thoại Domain Name and DNS Server, nhập tên domain mà các máy DHCP client sẽ sử dụng, địa chỉ IP của DNS Server dùng phân giải tên.
- Sau khi đã cấu hình xong, nhấn Next để tiếp tục.

- Trong hộp thoại WINS SERVER tiếp theo, nhập địa chỉ của của WINS Server chính và phụ dùng phân giải các tên NetBIOS thành địa chỉ IP. Sau đó nhấn chọn Next. (dịch vụ WINS ít được sử dụng, do đó bạn có thể bỏ qua bước này, không nhập thông tin gì hết.)

- Trong hộp thoại Activate Scope, hỏi có kích hoạt scope này hay không. Scope chỉ có thể cấp địa chỉ cho các máy Client khi được kích hoạt. Nếu bạn định cấu hình thêm các thông tin tùy chọn cho scope thì chưa nên kích hoạt bây giờ. Sau khi đã lựa chọn xong, nhấn chọn Next.



- Nhấn Finish để kết thúc.

### 7.3.3. Dịch vụ DNS

Mỗi máy tính trong mạng muốn liên lạc hay trao đổi thông tin cần phải biết rõ địa chỉ IP của nhau. Tuy nhiên, với con người, việc nhớ tên dễ dàng hơn vì chúng có tính trực quan và gọi nhớ hơn địa chỉ IP là một số. Vì thế các máy tính được gán tên (hostname) và người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính.

Với quy mô mạng nhỏ, chỉ cần một tệp tin HOSTS.TXT lưu thông tin về ánh xạ tên máy thành địa chỉ IP. Trong đó tên máy chỉ là 1 chuỗi không phân cấp (flat name). Tệp tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tệp tin HOSTS.TXT có các nhược điểm như sau:

- Dễ bị xung đột tên: không được phép có 2 máy tính có cùng tên trong tệp tin HOSTS.TXT. Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tệp tin nên có nguy cơ bị xung đột tên.
- Không đảm bảo sự toàn vẹn: việc duy trì 1 tệp tin trên mạng lớn rất khó khăn. Ví dụ như khi tệp tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

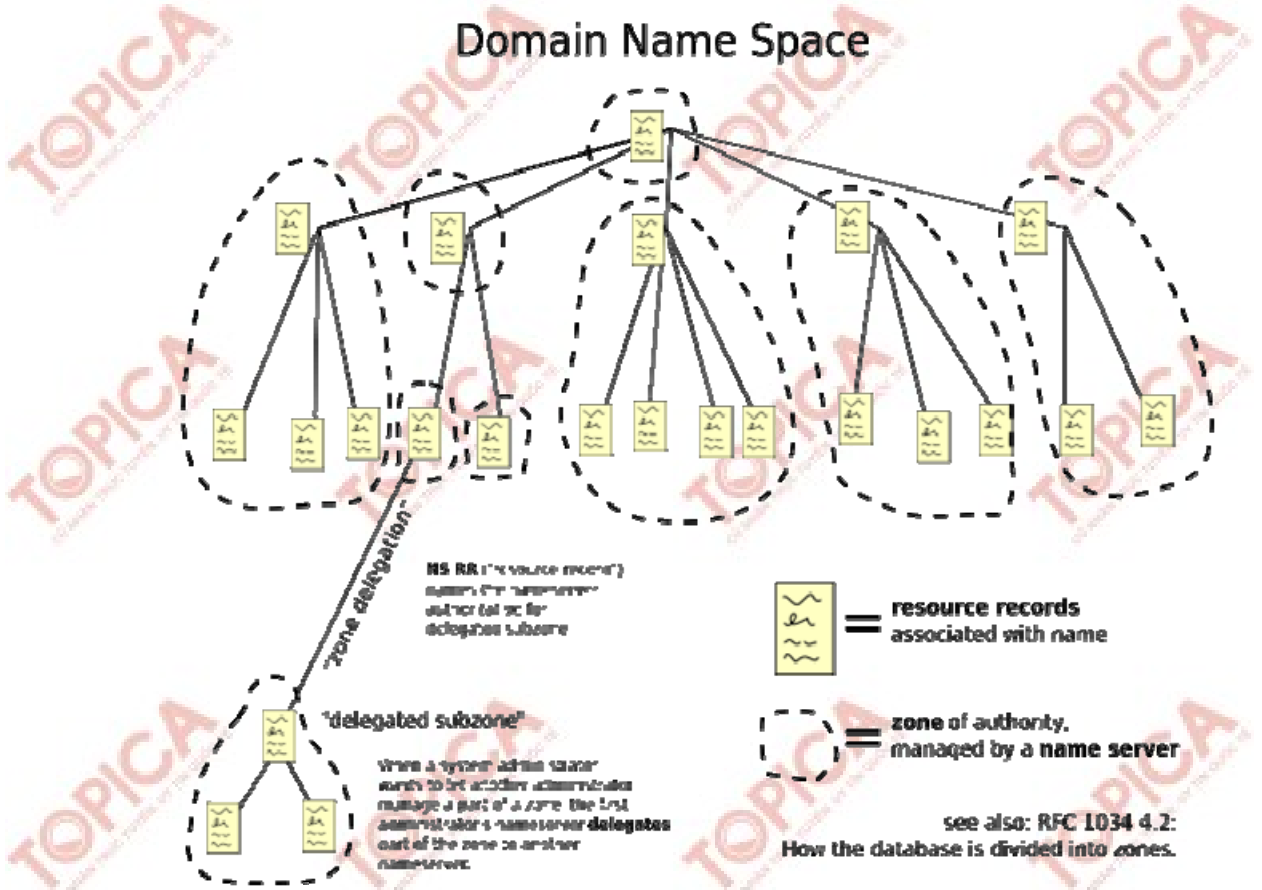
Việc dùng tệp tin HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Dịch vụ DNS ra đời nhằm khắc phục các nhược điểm này. Người thiết kế cấu trúc của dịch vụ DNS là Paul Mockapetris – USC's Information Sciences Institute,

và các khuyến nghị RFC của DNS là RFC 882 và 883, sau đó là RFC 1034 và 1035 cùng với 1 số RFC bổ sung như bảo mật trên hệ thống DNS, cập nhật động các bản ghi DNS ...

Hiện tại trên các máy chủ nói chung vẫn hỗ trợ sử dụng tệp tin hosts.txt để phân giải tên máy tính thành địa chỉ IP (Với Windows, tệp này nằm trong thư mục WINDOWS\system32\drivers\etc).

Dịch vụ DNS hoạt động theo mô hình Client-Server: server gọi là máy chủ phục vụ tên hay còn gọi là Name Server, Client là chương trình cần phân giải tên. DNS được thi hành như một giao thức tầng Application trong mạng TCP/IP.

DNS là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình Client-Server. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (Replication) và lưu tạm (Caching). Một hostname trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm (.).



Cơ sở dữ liệu(CSDL) của DNS là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL DNS gọi là 1 miền (Domain). Mỗi Domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (Subdomain).

Mỗi Domain có 1 tên (Domain Name). Tên domain chỉ ra vị trí của nó trong CSDL DNS. Trong DNS tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút



gốc của cây và phân cách nhau bởi dấu chấm. Tên nằm bên phải trong mỗi Domain Name được gọi là Top-Level Domain.

Các Top Domain chính:

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Bên cạnh đó, mỗi nước cũng có một top-level domain. Ví dụ top-level domain của Việt Nam là .vn.

Tên miền quốc gia	Mô tả
.vn	Việt Nam
.ru	LB Nga
.uk	Anh
.sg	Singapore

## TÓM LƯỢC CUỐI BÀI

Nội dung bài học bạn đọc lưu ý các vấn đề sau đây:

- Quản trị người dùng.
- Các chiến lược quản trị và các công cụ quản trị.
- Tài nguyên, chia sẻ tài nguyên.
- Các quyền truy cập và các chế độ chia sẻ.
- Dịch vụ mạng:
  - Dịch vụ DHCP.
  - Dịch vụ DNS.

**CÂU HỎI TỰ LUẬN**

**Câu 1.** Tài khoản người dùng cục bộ và tài khoản người dùng miền là như thế nào? Nêu sự khác nhau giữa chúng?

**Câu 2.** Nhóm cục bộ, nhóm cục bộ miền, nhóm toàn cục có gì khác nhau?

**Câu 3.** Nêu các khái niệm sau:

- a. Mạng máy tính?
- b. Server (máy chủ)?
- c. Client (máy trạm)?

**Câu 4.** Nêu khái niệm và đặc điểm của mạng WAN?

**Câu 5.** Vì sao phải có dịch vụ DHCP? Cách thức thực hiện?

**BÀI TẬP TRẮC NGHIỆM**

**1.** Tài khoản nhóm được sử dụng để làm gì?

- a) Đăng nhập vào mạng.
- b) Quản lý người sử dụng.
- c) Đại diện cho một nhóm người sử dụng.
- d) Cả a, b, c đều đúng.

**2.** Có mấy loại tài khoản nhóm?

- a) 1 loại: nhóm người dùng.
- b) 2 loại: nhóm bảo mật và nhóm phân phối.
- c) 3 loại: nhóm cục bộ, nhóm bảo mật và nhóm phân phối.
- d) Có tất cả 4 loại.

**3.** Tác vụ thông thường của người quản trị là gì?

- a) Quản lý tài khoản và mật khẩu người sử dụng.
- b) Quản lý tài nguyên mạng.
- c) Quản lý, kiểm soát các dịch vụ mạng.
- d) Quản trị windows.

**4.** Mạng Microsoft Windows được tổ chức dựa trên mô hình nào?

- a) Nhóm (Group).
- b) Miền (Domain).
- c) Khu vực (Region).
- d) Nhóm và Miền.

**5.** Hệ thống quản lý tệp tin nào sau đây hỗ trợ bảo mật?

- a) FAT16.
- b) FAT32.
- c) NTFS.
- d) FAT32 và NTFS.

**6.** Quyền truy cập thư mục và tệp tin thay đổi thế nào nếu ta di chuyển chúng?

- a) Thừa hưởng toàn bộ quyền sẵn có của thư mục cha, nơi chúng chuyển đến.
- b) Giữ nguyên quyền hạn của chúng, tức không thay đổi bằng việc di chuyển.
- c) Các quyền hạn của chúng được thiết lập lại về trạng thái ban đầu.
- d) Thay đổi một cách ngẫu nhiên.

**7.** Kích thước địa chỉ IP (phiên bản 4)?

- a) 8 bit.
- b) 16 bit.
- c) 32 bit.
- d) 128 bit.