ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG CAO ĐẲNG KỸ THUẬT LÝ TỰ TRỌNG

GIÁO TRÌNH
MẠNG MÁY TÍNH VÀ QUẢN TRỊ MẠNG

NGÀNH: Công nghệ thông tin

BẬC: Cao đẳng kỹ thuật

CHỦ BIÊN: GV Nguyễn Văn Đôn

Tài liệu lưu hành nội bộ

TP.HCM – Tháng 07 /2011

MỞ ĐẦU

Giáo trình *"Mạng máy tính và quản trị mạng"* cung cấp các kiến thức nền tảng của hệ thống mạng máy tính. Giáo trình hướng dẫn chi tiết các bước thực hành để tạo kỹ năng, kỹ xảo cho người mới bắt đầu thiết lập và quản trị một hệ thống mạng. Giáo trình gồm 2 phần chính.

Phần 1 - Mạng máy tính

Phần này chủ yếu là lý thuyết. Trình bày những khái niệm cơ bản nhất về mạng máy tính. Phân tích các mô hình OSI và TCP/IP để biết hệ thống mạng được thiết kế và hoạt động như thế nào. Trình bày các thiết bị mạng, kiến trúc mạng và các chuẩn mạng hiện nay trên thế giới. Quan trọng nhất là kiến thức về IP và chia mạng con trong hệ thống mạng TCP/IP.

Phần 2 - Quản trị mạng

Phần này chủ yếu là thực hành. Trình bày cách thiết lập và bảo mật trong hai hệ thống quản lý mạng hiện nay là Workgoup (mạng ngang hàng) và Domain (Client/Server). Đi từ cơ bản nhất từ cài đặt hệ điều hành đến quản lý và bảo mật user, tài nguyên mạng. Trình bày chi tiết quá trình thiết lập một dịch vụ mạng DHCP (cấp IP động).

Giáo trình được biên soạn theo sát đề cương chi tiết của môn "Mạng máy tính và quản trị mạng" Trường CĐ KT Lý Tự Trọng TP.HCM. Giáo trình được lưu hành nội bộ và sử dụng cho sinh viên hệ cao đẳng Trường CĐ KT Lý Tự Trọng TP.HCM.

Giáo trình này được đúc kết từ kinh nghiệm giảng dạy tại Trường CĐ KT Lý Tự Trọng TP.HCM. Kết hợp nhiều phương pháp, tài liệu tham khảo lấy ý kiến của các chuyên gia và đồng nhiệp. Giáo trình này dành cho sinh viên hệ cao đẳng của khoa Công nghệ thông tin Trường CĐ KT Lý Tự Trọng TP.HCM học tập, tham khảo và nghiên cứu.

Nội dung giáo trình được trình bày từ cơ bản nhất. Sinh viên nên đọc từ đầu đến cuối để nắm bắt các vấn đề rõ ràng. Trên các hình vẽ mô tả thứ tự các thao tác và chức năng, khi đọc nên khảo sát hình vẽ một cách kỹ lưỡng.

Giáo trình được viết lần đầu tiên nên không thể tránh khỏi những thiếu sót, rất mong sự đóng góp từ các bạn sinh viên và bạn đọc để có thể hoàn thiện nội dung giáo trình tốt hơn.

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

STT	Viết tắt	Tiếng Anh	Tiếng Việt
1	ACL	Access Control List	Danh sách điều khiển truy cập
2	AD	Active Directory	Cơ sở dữ liệu trong mô hình domain
3	ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
4	ARPA	Advanced Research Projects Agence	Kỹ thuật truyền thông trên Internet
5	ARPANET	Advanced Research Projects Agence Network	Mạng máy tính của Bộ quốc phòng Mỹ
6	BOOTP	Bootstrap Protocol	Giao thức cấu hình IP động cho client
7	Bps	Bits per second	Bit trên giây
8	COM	Common Object Model	Cổng giao tiếp ngoại vi nối tiếp
9	CSMA/CD	Carrier Sense Multiple Access with Collision Domain	Cảm sóng đa truy chấp nhận đụng độ
10	DC	Domain Controler	Máy chủ quản lý miền
11	DHCP	Dynamic Host Configuration Protocol	Giao thức cấp địa chỉ IP động
12	DSAP	Destination Service Access Point	Điểm truy cập đích
13	DTE	Data Terminal Equipment	Thiết bị đầu cuối dữ liệu
14	DTP	Data Transfer Process	Truyền dữ liệu trong FTP
15	EMI	Electromagnetic interference	Nhiễu điện từ
16	FAT	File Allocation Table	Bảng phân phối file
17	FDDI	Fiber Distributed Data Interface	Mạng cáp quang 2 vòng ngược nhau
18	FTP	File Transfer Protocol	Giao thức truyền file
19	Gbps	Gigabits per second	Giga bít trên giây

20	GPO	Group Policy Object	Chính sách nhóm trong Active Directory
21	GUI	Graphical User Interface	Giao diện người dùng đồ họa
22	HTTP	Hypertext Transfer Protocol	Giao thức truyền Web
23	IANA	Internet Assigned Numbers Authority	Tổ chức cấp phát số hiệu Internet
24	IE	Internet Explorer	Trình duyệt web của Microsoft
25	IEEE	Electrical and Electronics Engineers	Viện các kỹ sư điện và điện tử
26	IETF	Internet Engineering Task Force	Tổ chức quản lý kỹ thuật Internet
27	IGRP	Interior Gateway Routing Protocol	Giao thức định tuyến dựa vào cổng biên
28	IP	Internet Protocol	Giao thức mạng Internet
29	ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hóa quốc tế
30	ISPs	Internet Service Providers	Nhà cung cấp dịch vụ Internet
31	ITU	International Telecommunication Union	Liên minh viễn thông quốc tế
32	Kbps	Kilobits per second	Kilobit trên giây
33	LAN	Local Area Network	Mạng cục bộ
34	LLC	Logical Link Control	Lớp điều khiển liên kết luận lý
35	MAC	Media Access Control	Lớp điều khiển truy cập đường truyền
36	MAN	Metropolitan Area Network	Mạng đô thị
37	Mbps	Megabits per second	Megabit trên giây
38	NAS	Network-attached Storage	Dịch vụ lưu trữ dữ liệu tập trung qua mạng
39	NAT	Network Address Translation	Kỹ thuật chuyển đổi địa chỉ
40	NIC	Network Interface Card	Card giao tiếp mạng
41	NTFS	NT File System	Định dạng hệ thống file của

			Microsoft
42	OS	Operation System	Hệ điều hành
43	OSI	Open Systems Interconnection	Mô hình hệ thống kết nối mở
44	OU	Organization Unit	Đơn vị tổ chức trong Active Directory
45	PC	Personal Computer	Máy tính cá nhân
46	PCI	Peripheral Component Interconnect	Khe giao tiếp thiết bị ngoại vi
47	PDU	Protocol Data Unit	Đơn vị dữ liệu giao tiếp
48	PI	Protocol Interperter	Biên dịch lệnh trong FTP
49	POP	Post Office Protocol	Giao thức truyền mail
50	RFCs	Request for Comments	Những công bố mô tả các khái niệm
51	RIP	Router Information Protocol	Giao thức định tuyến động
52	SAM	Security Accounts Manager	File lưu trữ thông tin account trong Workgroup
53	SID	Security Identifyer	Chỉ danh bảo mật (cho mỗi đối tượng)
54	SMTP	Simple Mail Transfer Protocol	Giao thức truyền mail giữa các server
55	SSAP	Source Service Access Point	Điểm truy cập nguồn
56	SSID	Service Set Identifier	Tên của một điểm kết nối không dây
57	Tbps	Terabits per second	Tetrabit trên giây
58	TCP	Transmission Control Protocol	Giao thức truyền tin cậy
59	TTL	Time to live	Thời gian sống của gói tin
60	UDP	User Datagram Protocol	Giao thức truyền không tin cậy
61	UNC	Universal Naming	Đường dẫn truy cập tài nguyên

		Convention	mạng LAN
62	URL	Uniform Resource Locator	Đường dẫn truy cập tài nguyên trên Internet
63	VLAN	Virtual Local Area Network	Mạng riêng ảo
64	VNPT	VNPT	Tập đoàn bưu chính viễn thông Việt Nam
65	WAN	Wide Area Network	Mạng diện rộng
66	Win2K	Windows Server 2000	Hệ điều hành Windows Server 2000
67	Win2K3	Windows Server 2003	Hệ điều hành Windows Server 2003
68	Win2K8	Windows Server 2008	Hệ điều hành Windows Server 2008
69	Win7	Windows 7	Hệ điều hành Windows 7
70	WinXP SP2	Windows XP Service Pack 2	Hệ điều hành Windows XP bản vá lỗi 2

PHẦN 1 - MẠNG MÁY TÍNH CĂN BẢN

CHƯƠNG 1 - TỔNG QUAN VỀ MẠNG MÁY TÍNH

∗ Tóm tắt nội dung chương 1

- Những khái niệm cơ bản về mạng máy tính.
- Các mô hình mạng, mô hình xử lý, mô hình quản lý và mô hình ứng dụng mạng.
- Các dịch vụ mạng căn bản.
- Kết nối trực tiếp hai máy tính bằng cáp xoắn đôi.

∗ Mục tiêu chương 1

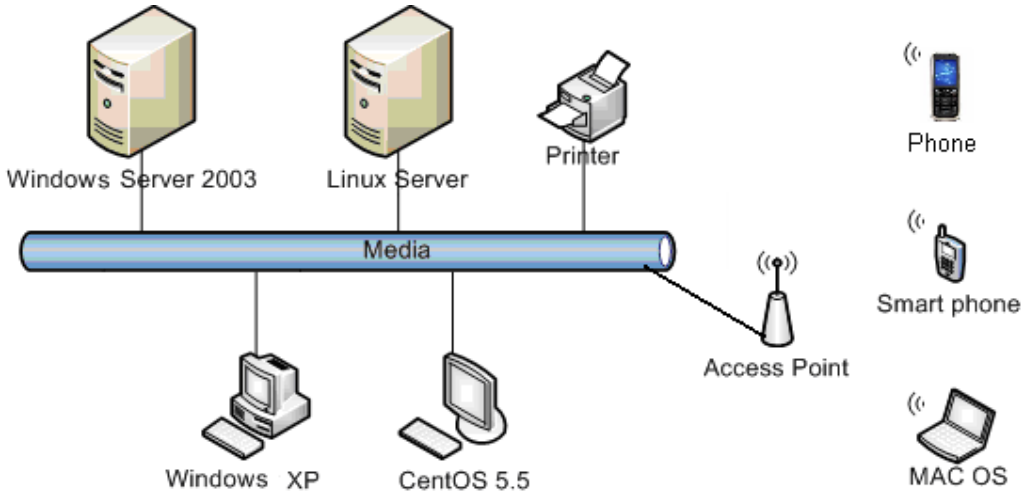
Sau khi học xong sinh viên có khả năng:

- Trình bày các khái niệm cơ bản về mạng máy tính và các dịch vụ mạng.
- Phân biệt các loại mô hình và cho ví dụ ứng dụng trong thực tế.
- Kết nối và truy cập máy tính khác bằng cáp xoắn đôi.

1.1. Các khái niệm cơ bản

1.1.1. Mạng máy tính

Mạng máy tính là một hệ thống các máy tính hoặc thiết bị ngoại vi được kết nối với nhau thông qua các phương tiện truyền dẫn, giúp cho các thiết bị này có thể truyền thông và trao đổi dữ liệu một cách dễ dàng và nhanh chóng.



Hình 1. 1 - Mô hình mạng có server, client, printer, phone, smart phone kết nối qua dây và sóng wireless

1.1.2. Các thành phần cơ bản trong mạng máy tính

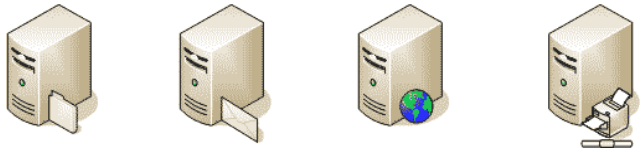
- Máy tính: PC, laptop, phone, smart phone, server, host...
- Thiết bị ngoại vi: printer, scaner, modem, fax...
- Tài nguyên mạng: file, folder, web, mail...
- Thiết bị giao tiếp mạng: NIC, repeater, hub, bridge, switch, router, gateway...
- Môi trường truyền dẫn: cáp, hồng ngoại, bluetooth, wireless, WWan...

- Hệ điều hành mạng: Win NT, Win 2K3, Win 2K8, Linux, Unix...
- Giao thức mạng: Net Beui, TCP, UDP, IP, FTP, HTTP, POP, SMTP...
- Ứng dụng mạng: phần mềm bán vé máy bay, quản lý bán hàng, quản lý doanh nghiệp...

1.1.3. Một số thuật ngữ cơ bản

Server (máy chủ): là máy tính chuyên cung cấp các dịch vụ cho các máy khác, được gọi tên ứng với dịch vụ mà nó cung cấp:

- File server: cung cấp các dịch vụ file và thư mục (vd: megaupload.com).
- Mail server: cung cấp các dịch vụ mail (vd: mail.yahoo.com).
- Web server: cung cấp các các dịch vụ web (vd: vnexpress.net).
- Print server: cung cấp các dịch vụ in ấn.



Hình 1. 2 - Các ký hiệu chuẩn file server, mail server, web server và print server

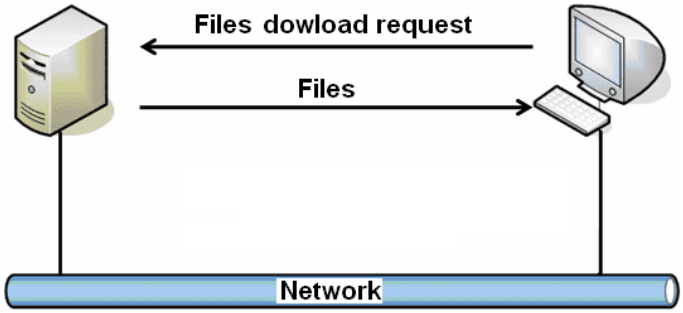
Máy server phục vụ một cách liên tục, nhanh chóng và bảo mật nên thường là:

- Các máy chuyên dụng của các hãng: IBM, DELL, HP...
- Cài hệ điều hành server chuyên dụng: Win2K3, Win2K8, Redhat server...
- Cài các phần mềm cung cấp dịch vụ và bảo mật chuyên dụng.

Hình 1. 3 - Một server chuyên dụng của hãng HP

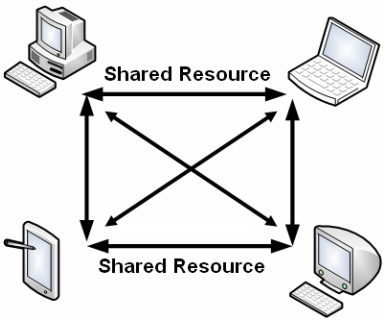
Client (máy khách): là máy sử dụng dịch vụ do máy server cung cấp:

- Client không cần cấu hình mạnh.
- Cài đặt các hệ điều hành dùng cho client: Windows XP, Windows 7...
- Cài đặt các ứng dụng dành cho người dùng.



Hình 1. 4 - Client sử dụng dịch vụ file do file server cung cấp

Peer (máy ngang hàng): là máy vừa cung cấp dịch vụ cho các máy khác và vừa sử dụng dịch vụ của máy khác cung cấp. Máy này không cần sử dụng các hệ điều hành chuyên dụng và thường hoạt động trong Peer-to-Peer (mạng ngang hàng).



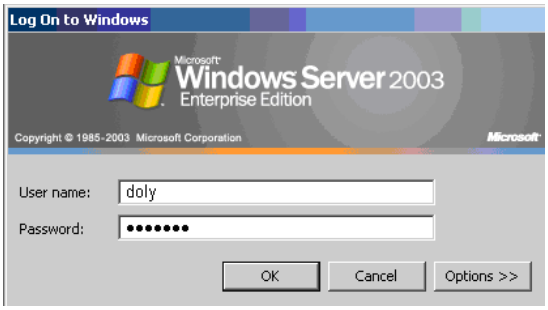
Hình 1. 5 - Các máy peer chia sẻ tài nguyên và sử dụng tài nguyên trên mạng Peer-to-Peer

Media (phương tiện truyền dẫn): là cách thức và vật liệu kết nối mạng (cáp đồng trục, cáp xoắn đôi, wireless, bluetooth...)

Shared data (dữ liệu dùng chung): các tập tin, thư mục, dữ liệu mà các máy tính chia sẻ trên mạng cho các máy khác sử dụng.

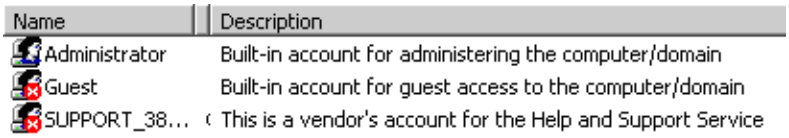
Resource (tài nguyên): file, thư mục, printer, fax, băng thông, dung lượng... tất cả những gì trên mạng mà người dùng có thể sử dụng được gọi là tài nguyên mạng.

User (người dùng): mỗi người muốn sử dụng tài nguyên mạng đều được quản trị viên cung cấp một account (tài khoản) để đăng nhập vào hệ thống và sử dụng các tài nguyên được phép sử dụng.



Hình 1. 6 - Đăng nhập vào hệ thống bằng một account

Administrator (quản trị viên): là người có quyền hạn cao nhất trong hệ thống, thường là người đầu tiên thiết lập hệ thống. Administrator quản trị, ủy quyền, phân quyền... cho tất các người dùng theo chính sách của tổ chức, công ty...



Hình 1. 7 - Win2K3 vừa cài đặt chỉ cho phép Administrator

1.2. Các loại mạng máy tính

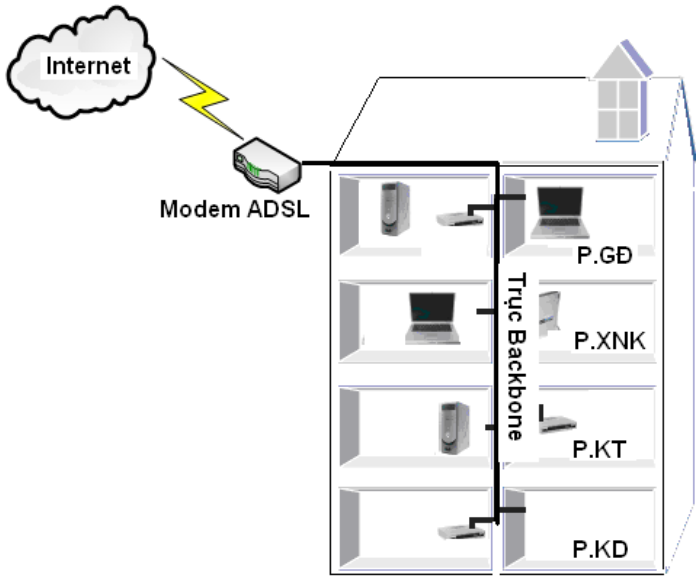
Tùy theo tầm vực hệ thống mạng được chia ra các loại mạng máy tính sau đây.

1.2.1. LAN (mạng cục bộ)

LAN (Local Area Network) có phạm vi giới hạn trong một tòa nhà, công ty, trường học, bệnh viện...

Đặc điểm:

- Kích thước nhỏ, bán kính khoảng vài Km.
- Các thiết bị đơn giản, rẻ tiền.
- Băng thông lớn, sử dụng các ứng dụng online như quản lý doanh nghiệp, hội thảo qua mạng...
- Quản trị đơn giản.



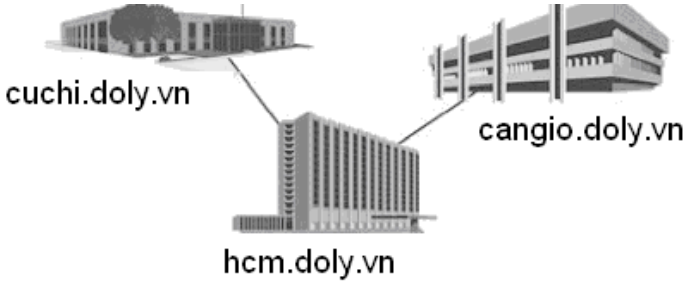
Hình 1. 8 - Mô hình mạng cục bộ của một công ty

1.2.2. MAN (mạng đô thị)

MAN (Metropolitan Area Network) là các LAN được kết nối với nhau có phạm vi trong một thành phố hoặc một quốc gia.

Đặc điểm:

- Băng thông trung bình, phục vụ cho các ứng dụng: chính phủ điện tử, thương mại điện tử, ngân hàng, du lịch...
- Thiết bị phức tạp, đắt tiền.
- Độ phức tạp cao. quản trị khó khăn hơn LAN.



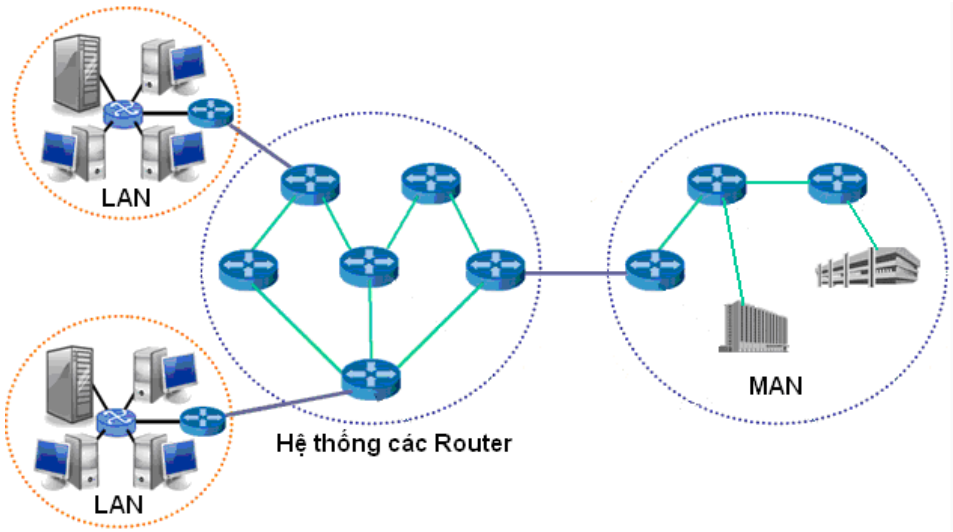
Hình 1. 9 – một MAN nối 3 LAN

1.2.3. WAN (mạng diện rộng)

WAN (Wide Area Network) là kết nối của các LAN và MAN lại với nhau có phạm vi rộng lớn vượt qua giới hạn quốc gia có thể là toàn cầu. Một điển hình của WAN là mạng Internet.

Đặc điểm:

- Băng thông thấp, thường đáp ứng các ứng dụng offline như file, web, mail... phục vụ cho các công ty đa quốc gia.
- Thiết bị phức tạp, rất đắt tiền.
- Không giới hạn vị trí địa lý, độ phức tạp rất cao nên phải có các tổ chức thế giới đứng ra quản trị: IEEF, IETF, ITU, IANA, Whois...



Hình 1. 10 - Một mô hình WAN kết nối thông qua các router

1.2.4. Mạng Internet

Là một trường hợp đặc biệt của WAN, xuất phát từ mạng ARPANET của bộ quốc phòng Mỹ. Cung cấp các dịch vụ mang tính toàn cầu: web, chat, game, void, file, mail,

truy cập từ xa... có thể được kết nối thông qua các ISPs (Internet Service Providers – nhà cung cấp dịch vụ Internet).

Đặc điểm:

- Mang tính toàn cầu.
- Miễn phí hoàn toàn (người dùng chỉ trả phí duy trì kết nối cho ISPs).

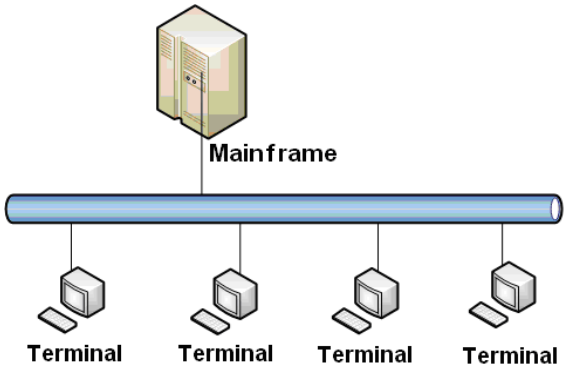
1.3. Các mô hình xử lý mạng

1.3.1. Mô hình xử lý mạng tập trung

Tất cả dữ liệu lưu trữ và tiến trình xử lý do Mainframe (máy tính trung tâm) đảm nhiệm, còn lại là các Terminal (thiết bị đầu cuối) hoạt động như các thiết bị nhập xuất dữ liệu tương tác với người dùng. Thường ứng dụng trong: siêu thị, sân bay, quán cà phê...

Ưu điểm: chi phí thấp, dễ quản trị, an toàn.

Khuyết điểm: tốc độ truy xuất chậm, thường chỉ đáp ứng một ứng dụng nào đó như quản lý nhân viên, quản lý bán hàng...



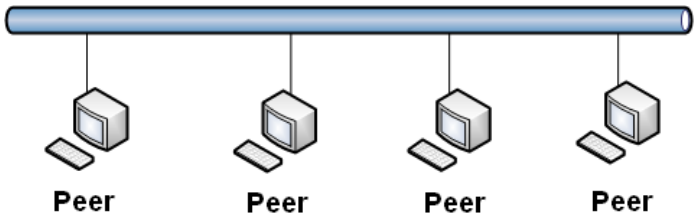
Hình 1. 11 - Mô hình xử lý mạng tập trung

1.3.2. Mô hình xử lý mạng phân phối

Các máy tính hoạt động độc lập, các công việc được chia cho nhiều máy xử lý. Dữ liệu được lưu trữ tại các máy và được chia sẻ để dùng chung trên mạng.

Ưu điểm: tốc độ cao, không hạn chế các ứng dụng.

Khuyết điểm: dữ liệu rời rạc, khó backup, khó bảo mật, dễ nhiễm virus.



Hình 1. 12 - Mô hình xử lý mạng phân phối

1.3.3. Mô hình xử lý mạng cộng tác

Nhiều máy tính hợp tác để xử lý một công việc lớn. Các máy tính có thể mượn năng lực xử lý của các máy tính khác trong mạng.

Ưu điểm: rất nhanh và mạnh, chạy các ứng dụng lớn và các phép toán lớn.

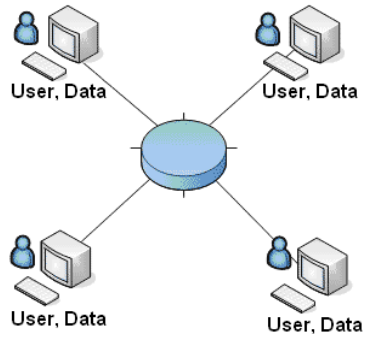
Khuyết điểm: dữ liệu rời rạc khó đồng bộ và backup, khả năng nhiễm virus rất cao.

Hình 1. 13 - Siêu máy tính Deep Blue II đánh thắng vua cờ Kasparov

1.4. Các mô hình quản lý mạng

1.4.1. Workgroup

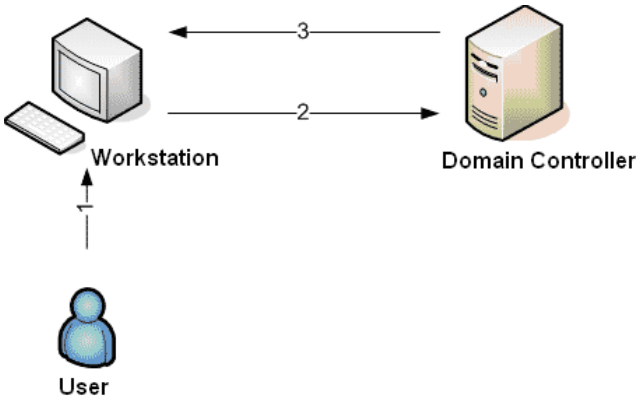
Các máy tính trong mạng có quyền hạn ngang nhau, tự bảo mật và quản lý tài nguyên của mình. User cục bộ của máy tính nào chỉ có quyền đăng nhập vào cục bộ máy tính đó.



Hình 1. 14 - Mô hình quản lý mạng Workgroup

1.4.2. Domain

Quản lý và chứng thực phải thông qua DC (Domain Controler - máy chủ điều khiển miền). Tất cả user và tài nguyên mạng được máy DC quản lý và phân quyền.



Hình 1. 15 - Chứng thực của user trong mô hình quản lý Domain

Ở hình 1.15, khi User dùng Workstation (máy trạm) muốn đăng nhập vào hệ thống (Domain) (1). Workstation sẽ chuyển quyền chứng thực lên DC (2). DC sẽ kiểm tra xem User này có quyền đăng nhập vào hệ thống hay không, sau đó hồi đáp cho Workstation (có quyền hay không có quyền) (3). Khi User đã được phép đăng nhập vào hệ thống thông qua Workstation, User này chịu toàn bộ sự quản lý của DC. Muốn sử dụng tài nguyên, thực thi các chương trình... đều phải thông qua các chính sách do DC quản lý (các chính sách này do tổ chức, công ty đưa ra để quản lý người dùng).

1.5. Các mô hình ứng dụng mạng

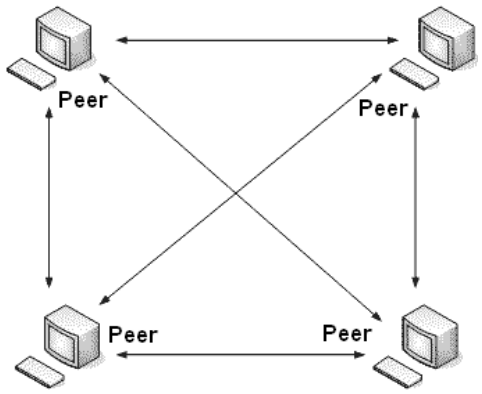
1.5.1. Peer to Peer (mạng ngang hàng)

Như đã biết máy Peer là máy ngang hàng, vừa cung cấp và vừa sử dụng dịch vụ. Vậy mạng ngang hàng không có máy đóng vai trò là máy chủ phục vụ. Các user tự quản lý và chia sẻ tài nguyên của máy mình.

Quản lý theo mô hình Workgroup chỉ đáp ứng cho các tổ chức nhỏ (công ty nhỏ, dịch vụ Internet...). Microsoft khuyến cáo dùng mô hình này đối với các công ty có cỡ 10 máy tính trở xuống, nếu công ty có hơn 10 máy tính việc quản trị sẽ gặp khó khăn trong đồng bộ, backup dữ liệu và bảo mật...

Ưu điểm: đơn giản, rẻ tiền và dễ quản trị.

Khuyết điểm: dữ liệu rời rạc, khó backup, kém bảo mật, khó định vị tài nguyên trên mạng.



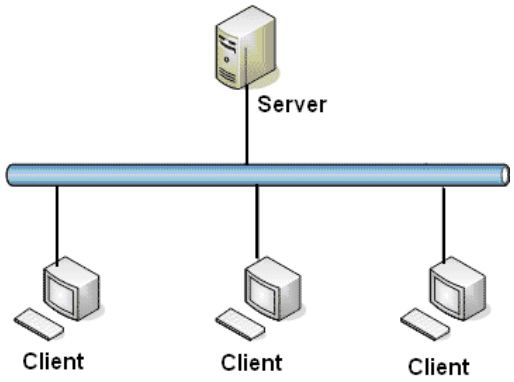
Hình 1. 16 - Mô hình ứng dụng mạng ngang hàng

1.5.2. Client/Server (mạng khách chủ)

Các server sẽ cung cấp tài nguyên và dịch vụ cho các client sử dụng. Trong mô hình này có những máy chuyên cung cấp tài nguyên và dịch vụ, có những máy chuyên sử dụng tài nguyên và dịch vụ do các máy khác cung cấp.

Ưu điểm: dữ liệu tập trung nên dễ đồng bộ, backup và bảo mật. Tài nguyên được quản lý nên hoạt động hiệu quả, đúng mục đích cho nhiều người dùng chung trên mạng.

Khuyết điểm: tốn rất nhiều chi phí cho việc mua server, thuê quản trị viên, mua các hệ điều hành mạng và các phần mềm bảo mật chuyên dụng...



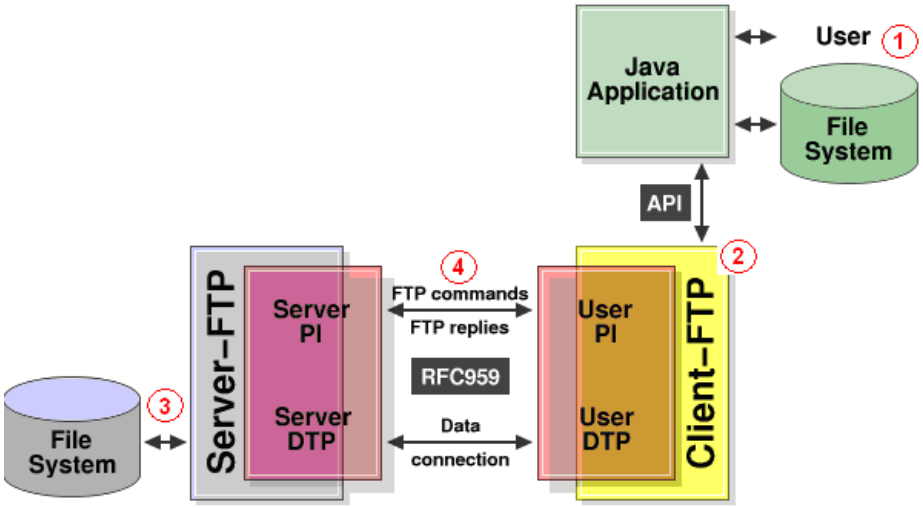
Hình 1. 17 - Mô hình ứng dụng mạng Client/Server

1.6. Các dịch vụ mạng

1.6.1. File services (dịch vụ tập tin)

Dịch vụ file lưu trữ, truyền và tìm kiếm file thông qua mạng, hoạt động theo cơ chế Client/Server. Một dịch vụ file phổ biến là FTP (File Transfer Protocol) được mô tả trong RFC959 http://www.w3.org/Protocols/rfc959/

Dịch vụ này cho phép client yêu cầu server upload (tải lên) hoặc download (chép về) các tập tin, cho phép người dùng tương tác giữa hệ thống này với hệ thống khác mà không quan tâm đến hệ điều hành tại đó.

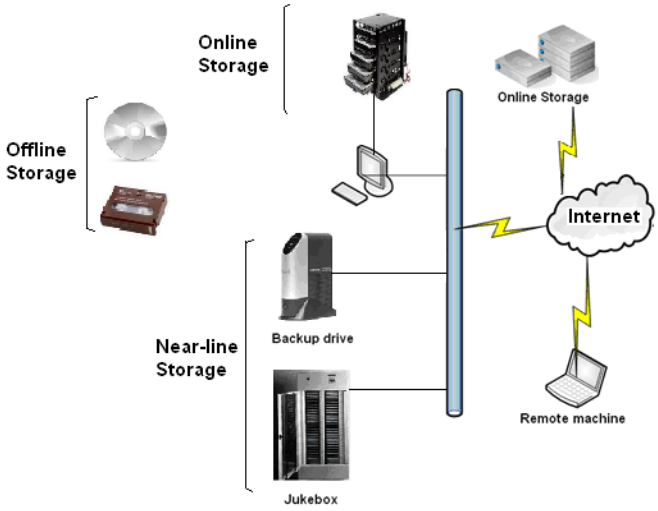


Hình 1. 18 - Mô tả hoạt động của FTP services

Ở hình 1.18, quá trình download file diễn ra như thế nào? User đang sử dụng ứng dụng Java (có hệ thống file riêng của mình), ứng dụng Java cần download một file từ server (1). Ứng dụng Java này không thể lấy file trực tiếp từ server mà phải thông qua trình khách Client-FTP (2). Trình khách này yêu cầu download file từ hệ thống file của server thông qua trình chủ Server-FTP (3). Client-FTP và Server-FTP tương tác nhau thông qua các lệnh FTP (lệnh download file là get) và nhờ một giao thức PI để biên dịch các lệnh này. Tiếp theo là quá trình download file diễn ra thông qua một kết nối các cổng giữa client và server do giao thức DTP đảm nhiệm (4).

Một số khái niệm về lưu trữ và xử lý dữ liệu:

- Online storage (lưu trữ trực tuyến): lưu trữ ngay trên ổ cứng hoặc thông qua mạng nên truy xuất dễ dàng và bất cứ lúc nào. Nhưng với cách lưu trữ này tốn rất nhiều dung lượng (có giới hạn) của ổ cứng trên máy tính hoặc mua của ISP, khó di dời và chi phí cao.
- Offline storage (lưu trữ ngoại tuyến): lưu trữ trên các thiết bị bên ngoài như USB drive, đĩa quang, đĩa từ... với chi phí thấp, an toàn, dễ di dời. Nhưng với cách lưu trữ này không thể sử dụng tức thời mà phải kết nối thiết bị lưu trữ với máy tính thường áp dụng để bakup dữ liệu.
- Near-line storage (lưu trữ cận tuyến): lưu trữ trên các thiết bị chuyên dụng như jukebox (thiết bị quản lý các băng từ và đĩa quang), USB backup drive... khắc phục được các khuyết điểm của hai cách lưu trữ online và offline. Nhưng các thiết bị lưu trữ này khá đắt và cần phải có quản trị viên.

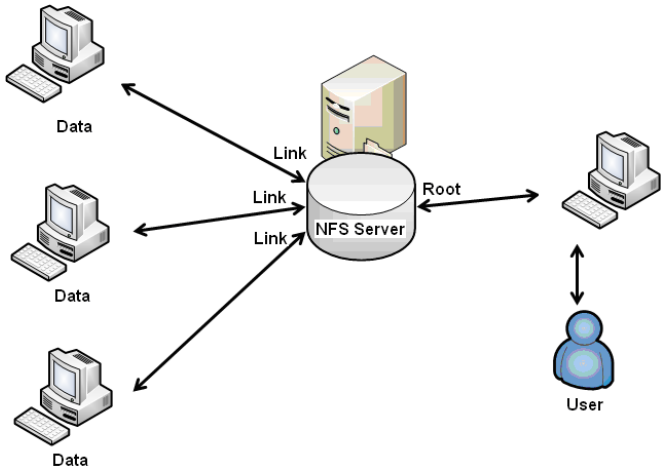


Hình 1. 19 - Lưu trữ dữ liệu

- Data migration (di trú dữ liệu): là quá trình chuyển dữ liệu từ cách lưu trữ này sang cách lưu trữ khác, thường dùng trong auto backup để tự động chuyển dữ liệu từ online sang offline hoặc near-line.
- Sync (đồng bộ hóa): khi nhiều user sử dụng một file, để bảo đảm tính nhất quán của dữ liệu phải có sự đồng bộ dữ liệu. Nhiều đại lý cùng bán vé cho một chuyến bay thì làm sao các đại lý phải có bản sao mới nhất danh sách các vé đã bán.
- Sao lưu dự phòng (backup - restore): tạo ra các bản sao dữ liệu (backup) khi có rủi ro người dùng dễ dàng phục hồi (restore) lại dữ liệu đã mất.

1.6.2. Directory services (dịch vụ thư mục)

Thiết lập một thư mục dùng chung thông qua đó user sử dụng nhanh chóng, hiệu quả mà không cần quan tâm dữ liệu đó được lưu trữ ở đâu. Dịch vụ hay sử dụng là NFS (Network File System), dịch vụ này tạo các đường liên kết đến các nơi chứa dữ liệu, user chỉ cần truy xuất đến NFS server và xem như tất cả dữ liệu nằm ở đây.



Hình 1. 20 - Mô hình dịch vụ thư mục NFS

1.6.3. Web services (dịch vụ truyền siêu văn bản)

Tích hợp nhiều dạng thông tin (văn bản, hình ảnh, âm thanh...) trên một trang hypertext (siêu văn bản) để cung cấp một cách nhanh chóng, sinh động và hiệu quả cho người dùng. Dịch vụ thông dụng là HTTP (Hypertext Transfer Protocol), phục vụ cho tất cả các ngành nghề trong xã hội như thương mại điện tử, chính phủ điện tử, báo điện tử, web cá nhân... thông qua các trình duyệt web như Internet Explorer, Opera, Firefox... người dùng tải về các trang web cung cấp thông tin trên toàn thế giới phục vụ giải trí, học tập, việc làm, công việc, nghiên cứu...

1.6.4. Message services (dịch vụ thông điệp)

Cung cấp các dịch vụ news (dịch vụ tin nhắn), mail (dịch vụ thư điện tử)... phục vụ cho công việc nhanh chóng hiệu quả và tiết kiệm chi phí. Dịch vụ này mang tính pháp lý (chống từ chối) giúp các công ty tiết kiệm chi phí đi lại, thời gian và tiền bạc. Các hệ thống mail hay sử dụng là POP3 (Post Office Protocol version 3), Exchange, MDeamon, Yahoo mail, Gmail...

1.6.5. Database services (dịch vụ cơ sở dữ liệu)

Dịch vụ này cung cấp cho người dùng truy vấn dữ liệu một cách nhanh chóng, chính xác với một khối lượng dữ liệu khổng lồ và cung cấp cho nhiều người dùng cùng lúc. Đồng thời tối ưu, bảo mật dữ liệu và phân phối dữ liệu qua nhiều hệ thống khác nhau mà vẫn bảo đảm tính toàn vẹn và nhất quán của dữ liệu. Cơ sở dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu, thường hay gặp là MySQL, Access, SQL, Oracle...

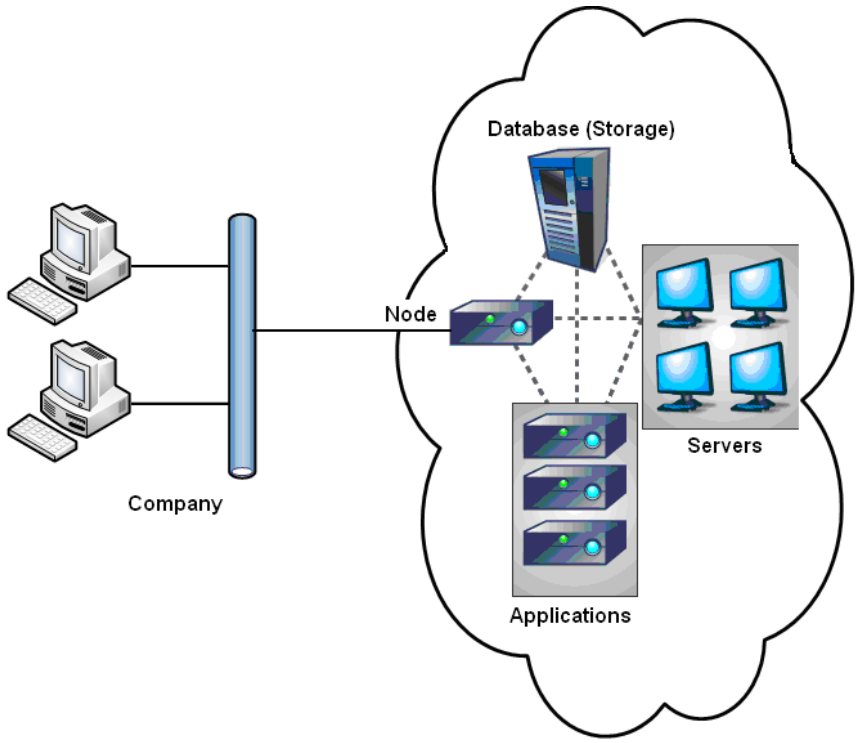
1.6.6. Print services (dịch vụ in ấn)

Máy in là một thiết bị đa dạng (Laser, màu, khổ lớn, vẽ...) và thường rất đắt. Dịch vụ in ấn giúp người dùng chia sẻ để dùng chung các thiết bị này, đồng thời lập lịch, cấp quyền hạn, thiết lập độ ưu tiên để phục vụ công việc một cách chính xác, nhanh chóng và tiết kiệm chi phí văn phòng. Người dùng có thể thiết lập mềm thông qua hệ điều hành, trình quản lý thiết bị hoặc có thể quản lý thông qua các thiết bị phần cứng như print server để triển khai dịch vụ này.

1.6.7. Application services (dịch vụ ứng dụng)

Dịch vụ này cho phép chia sẻ các ứng dụng đắt tiền hoặc sử dụng năng lực xử lý của máy khác.

Ví dụ: có một máy cấu hình thấp không chạy nổi một ứng dụng nào đó. Để sử dụng được ứng dụng đó trên máy này người dùng chạy ứng dụng đó trên một máy cấu hình mạnh và lấy kết quả về. Hiện nay các ứng dụng được xây dựng trên nền tảng công nghệ Portal (một cổng) và Cloud computing (công nghệ điện toán đám mây). Công nghệ Portal được xây dựng bởi các tập đoàn lớn như Yahoo, Google, AOL... Người dùng chỉ cần nhớ một cổng duy nhất yahoo.com ở đó cung cấp tất cả các dịch vụ cần thiết. Việc mua bản quyền, triển khai và quản lý các phần mềm là một công việc đau đầu và tốn kém cho các nhà quản lý. Nhờ vào công nghệ điện toán đám mây mà ở đó người dùng không cần quan tâm đến việc mua ở đâu, bảo trì thế nào, lưu trữ dữ liệu ra sao...



Hình 1. 21 - Công nghệ điện toán đám mây

1.7. Lợi ích của mạng máy tính

Tiết kiệm tài nguyên phần cứng: chia sẻ CDRom, folder, printer, fax... ví dụ: một công ty có rất nhiều máy tính nhưng các máy tính đó không cần gắn ổ CDRom, ổ cứng mà sử dụng thông qua mạng. Tất cả các máy tính truy cập Internet thông qua một đường truyền duy nhất nhờ dịch vụ chia sẻ Internet...

Trao đổi, đồng bộ dữ liệu một cách dễ dàng, nhanh chóng. Dữ liệu tập trung dễ quản lý, backup và bảo đảm tính toàn vẹn và nhất quán của dữ liệu.

Chia sẻ ứng dụng hiệu quả và tiết kiệm, ứng dụng bán hàng qua mạng, chính phủ điện tử...

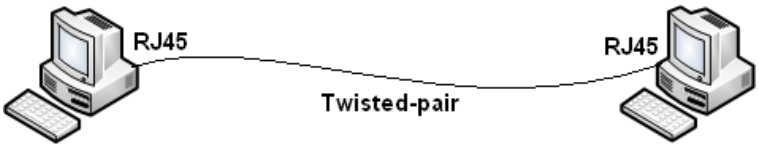
Sử dụng các dịch vụ thông qua Internet: web, chat, mail, game, VoIP...

Giúp cho các tổ chức quản lý hiệu quả và tiết kiệm.

Chia sẻ và tìm kiếm thông tin một cách dễ dàng.

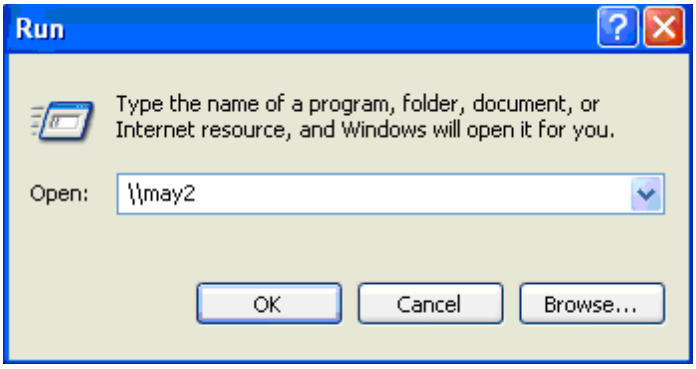
1.8. Kết nối trực tiếp hai máy tính bằng cáp xoắn đôi

Với cáp xoắn đôi được bấm chéo hai đầu RJ45 có thể kết nối trực tiếp hai máy tính lại với nhau. Đoạn dây này phải dài tối thiểu 0,5 mét, được bấm chéo hai đầu RJ45, cắm trực tiếp vào cổng RJ45 của card mạng, khai báo địa chỉ IP cùng lớp mạng. Sau khi kết nối thành công, các máy tính có thể chia sẻ tài nguyên cho nhau.



Hình 1. 22 - Kết nối trực tiếp hai máy tính bằng cáp xoắn đôi

Truy cập vào máy tính trên mạng, vào ***Start*** → ***Run*** sau đó gõ vào Open: ***\\tên máy tính cần truy cập***, sau khi chứng thực được quyền truy cập người dùng sẽ sử dụng được các tài nguyên máy đó đã chia sẻ.



Hình 1. 23 - Truy cập vào may2

1.9. Giới thiệu các hệ điều hành và phần mềm hỗ trợ mạng

Hệ điều hành dành cho server: Windows Server 2003, Windows Server 2008, Redhat, CentOS, Fedora...

Hệ điều hành dành cho client: Windows Xp, Windows Vista, Windows 7, Ubuntu, Fedora...

Phần mềm Total commander: hỗ trợ kết nối các máy tính trên mạng và kết nối FTP server.

Phần mềm VMware Workstation: xây dựng hệ thống mạng ảo trên máy tính.

Phần mềm Netop School: hỗ trợ giảng dạy qua mạng.

Phần mềm Bootrom: hỗ trợ chia sẻ ổ cứng qua mạng.

Phần mềm Microsoft Visio: hỗ trợ thiết kế mạng.

Phần mềm Packet Tracert: giả lập hạ tầng mạng.

1.10. Câu hỏi và bài tập

1. Vẽ một mô hình mạng đơn giản kết nối các thiết bị sau: file server, print server, web server, mail server, client?

2. Trình bày, vẽ hình và cho ví dụ thực tế của các mô hình xử lý mạng, mô hình quản lý mạng và mô hình ứng dụng mạng?

3. Trình bày và cho ví dụ thực tế các lợi ích thực tiễn của mạng máy tính?

4. Kể tên một số hãng sản xuất server và thiết bị mạng mà bạn biết?

5. So sánh mạng máy tính và mạng điện thoại di động?

6. Kể tên một số nhà cung cấp dịch vụ mạng và các dịch vụ mà họ cung cấp?

7. So sánh, phân tích ứng dụng của hai mô hình Workgroup và Domain?

8. Trình bày khái niệm Công nghệ Portal và Cloud Computing là?

9. Viết dòng lệnh truy cập vào một máy tính trên mạng?

10. Nối hai máy tính sử dụng cáp xoắn đôi bấm chéo (có sẵn), sau đó chia sẻ tài nguyên và truy cập lẫn nhau.

CHƯƠNG 2 - MÔ HÌNH OSI VÀ TCP/IP

∗ Tóm tắt nội dung chương 2

- Mô hình OSI, quá trình đóng gói của gói tin khi đi qua 7 lớp của mô hình.
- Khảo sát chi tiết lớp Data link, quá trình tìm địa chỉ vật lý MAC, cơ chế CSMA/CD, phân biệt collision domain và broadcast domain.
- Khảo sát chi tiết lớp Network, quá trình tìm đường đi của gói tin.
- Khảo sát chi tiết lớp Transport, phân biệt cơ chế truyền tin cậy (TCP) và truyền không tin cậy (UDP).
- Mô hình TCP/IP, quá trình đóng gói gói tin khi đi qua 4 lớp TCP/IP.

∗ Mục tiêu chương 2

Sau khi học xong sinh viên có khả năng:

- Trình bày chức năng và quá trình đóng gói các các gói tin trong mô hình OSI và TCP/IP.
- Mô tả quá trình tìm địa chỉ MAC của lớp 2 và quá trình tìm đường đi của lớp 3.
- Phân biệt broadcast domain và collision domain; TCP và UDP.
- Phân tích cơ chế CSMA/CD.

1.11. Mô hình tham chiếu OSI (Open System Interconnection)

2.1.1. Khái niệm giao thức mạng

Là một tập các tiêu chuẩn để trao đổi thông tin giữa hai hệ thống. Giao thức qui ước cách thức giao tiếp để hai máy tính, thiết bị mạng có thể trao đổi thông tin. ví dụ: truyền file theo giao thức FTP, mở IE gõ vào ftp://freeftp.com kết nối vào FTP server theo giao thức FTP và server yêu cầu chứng thực để đăng nhập.

Hình 2. 1 - Kết nối vào FTP server dùng giao thức FTP

Tương tự truy cập web site dùng giao thức HTTP http://vnexpress.net, lập tức trang web tải về cho người dùng. HTTP là cách thức mà web server giao tiếp với web client. Danh sách các giao thức mạng được trình bày tại WIKIPEDIA có URL là: http://en.wikipedia.org/wiki/List_of_network_protocols

2.1.2. Các tổ chức định chuẩn

Trên thế giới có rất nhiều cơ quan được giao trách nhiệm đưa ra các quy chuẩn. Các quy chuẩn này thường được mô tả và công bố qua các RFCs. Một số tổ chức định chuẩn trên thế giới:

- ITU: liên minh viễn thông quốc tế.
- IEEE: viện các kỹ sư điện và điện tử quốc tế.
- ISO: tổ chức tiêu chuẩn hóa quốc tế...

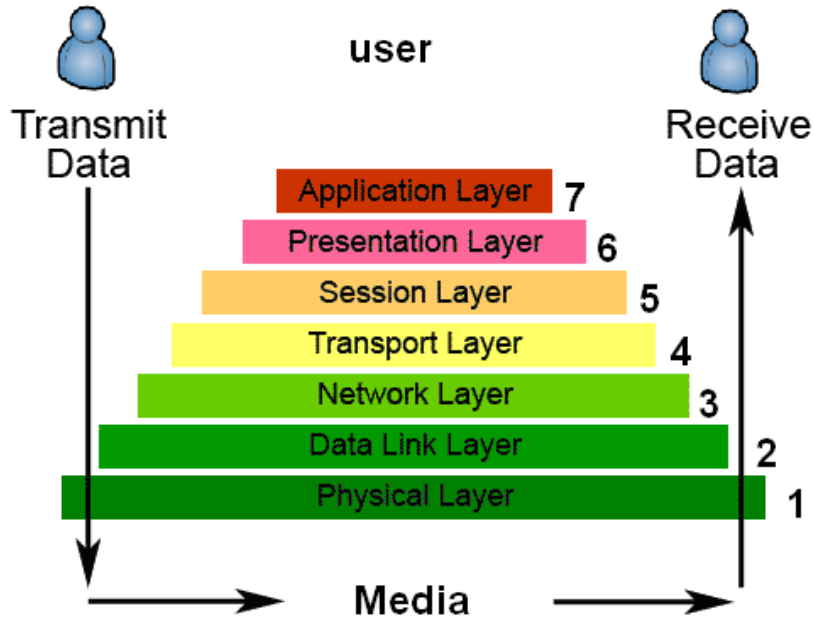
2.1.3. Bảy lớp trong mô hình OSI

Vào năm 1984, tổ chức chuẩn hóa quốc tế ISO chính thức đưa ra mô hình hệ thống kết nối mở OSI. Nhằm mục đích chuẩn hóa quá trình kết nối mạng máy tính. Chia quá trình truyền gói tin trên mạng ra 7 lớp, có nhiệm vụ và chức năng độc lập. Việc chia như thế có rất nhiều lợi ích.

- Chia quá trình truyền thông trên mạng thành các giai đoạn nhỏ giúp dễ nghiên cứu, khảo sát và quản lý hơn.
- Các lớp có các giao thức và phần cứng riêng biệt và không liên quan đến nhau nên khi có sự thay đổi ở một lớp thì không ảnh hưởng đến lớp khác.
- Các nhà sản xuất phần mềm và phần cứng thiết kế tuân thủ theo quy chuẩn này sẽ tương thích với các phần mềm và phần cứng của các hãng khác.

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

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



Hình 2. 2 - Bảy lớp trong mô hình OSI

2.1.3.1. Application Layer (lớp ứng dụng)

Là giao diện giữa ứng dụng của người dùng và mạng, người dùng giao tiếp với mạng thường phải thông qua một ứng dụng nào đó. Lớp Application cung cấp các giao thức FTP, HTTP, POP3, IMAP4... cho các ứng dụng. Nó không cung cấp dịch vụ cho các lớp khác.

2.1.3.2. Presentation Layer (lớp trình bày)

Lớp Presentation chịu trách nhiệm thương lượng và xác lập dạng thức dữ liệu được trao đổi. Cung cấp dịch vụ cho lớp Application, bảo đảm dữ liệu mà lớp Application gửi đi và chuyển cho lớp Application các dữ liệu mà lớp Application đọc được. Nó đảm nhiệm các nhiệm vụ:

- Chuyển đổi nhiều dạng dữ liệu khác nhau từ lớp Application thành một dạng dữ liệu chung để truyền đi và ngược lại. Có thể dạng dữ liệu nguồn và dạng dữ liệu đích khác nhau do hai hệ thống mạng khác nhau (ví dụ nguồn là máy tính hệ Intel, đích là điện thoại di động Nokia).
- Nén dữ liệu để giảm số bit truyền trên mạng và giải nén.
- Mã hóa dữ liệu để bảo mật trên mạng và giải mã.

2.1.3.3. Session Layer (lớp phiên)

Lớp Session thực hiện chức năng thiết lập, quản lý và kết thúc các phiên giao dịch giữa các thiết bị truyền nhận. Trước khi dữ liệu được truyền đi một session phải được thiết lập. Lớp Session cung cấp dịch vụ cho lớp Presentation, đảm nhiệm các nhiệm vụ sau:

- Cung cấp sự đồng bộ hóa dữ liệu bằng cách đặt những điểm kiểm tra luồng dữ liệu. Bằng cách này chỉ có các dữ liệu sau điểm kiểm tra cuối cùng mới được truyền lại.
- Cung cấp cơ chế nắm quyền trong trao đổi dữ liệu, bên nào truyền và truyền trong bao lâu.
- Áp đặt các quy tắc kết nối: Simplex (đơn công), Half-duplex (bán song công), Full-duplex (song công).

2.1.3.4. Transport Layer (lớp vận chuyển)

Lớp Transport chia dữ liệu ra thành các phân đoạn dữ liệu (segment) ở máy gửi, truyền các segment từ hệ thống này sang hệ thống khác và tái thiết lập dữ liệu từ các segment tại máy nhận. Lớp Transport thiết lập, duy trì và kết thúc các mạch ảo để đảm bảo các dịch vụ sau:

- Xếp thứ tự các segment: khi chia dữ liệu thành các segment, lớp này sẽ đánh thứ tự các segment, sắp xếp thứ tự các segment để tái thiết lập lại thành dữ liệu ban đầu.
- Kiểm soát lỗi: khi có một segment bị lỗi, lớp vận chuyển sẽ yêu cầu truyền lại.
- Kiểm soát luồng: dùng các tín hiệu báo nhận thành công một segment, để đảm bảo quá trình truyền các segment theo thứ tự.

Một số giao thức hoạt động ở lớp này là TCP (truyền tin cậy), UDP (truyền không tin cậy).

2.1.3.5. Network Layer (lớp mạng)

Lớp Network chia các segment nhận được từ lớp vận chuyển thành các gói tin (packet hay datagram), đánh địa chỉ đích cho gói tin và tìm đường đi tối ưu cho gói tin này. Lớp Network phải đáp ứng được nhiều loại mạng khác nhau và thực hiện hai chức năng chính là tìm đường (routing) và chuyển tiếp (relaying). Lớp Network thực hiện các chức năng sau:

- Kiểm soát sự nghẽn dữ liệu: chia gói tin thành các gói tin nhỏ hơn để tương thích với thiết bị truyền, ráp nối các gói tin ở đầu nhận.
- Đánh địa chỉ cho gói tin: mỗi lần gói tin đi đến thiết bị định tuyến, lớp Network sẽ đánh lại địa chỉ đích của gói tin để gói tin này đi đến mạng kế tiếp hoặc đến thiết bị nhận.
- Tìm đường đi tối ưu cho gói tin: dựa vào bảng định tuyến, thiết bị định tuyến sẽ xác định đường đi ngắn nhất cho gói tin để gói tin đi xuyên qua các mạng khác nhau đến mạng đích.

Lớp Network làm việc với địa chỉ logic (luận lý), một số giao thức hoạt động ở lớp này là IP (giao thức Internet) và IPX (IP Exchange).

2.1.3.6. Data Link Layer (lớp liên kết dữ liệu)

Lớp Data Link chia các gói tin thành các khung dữ liệu (frame) và truyền xuyên qua các liên kết vật lý. Lớp này chia làm hai lớp con:

- LLC (Logical Link Control): là lớp điều khiển liên kết với lớp luận lý phía trên (lớp Network), nó cung cấp các dịch vụ chuyển đổi để một mạng logic phía trên có thể truyền dữ liệu với các hạ tầng mạng khác nhau bên dưới.
- MAC (Media Access Control): là lớp điều khiển truy cập đường truyền vật lý, quy định thứ tự truy cập đường truyền. Lớp này làm việc với địa chỉ vật lý MAC và hiểu được các thông tin của lớp LLC.

Như vậy để liên kết một mạng luận lý (logic) với một mạng vật lý (physical), lớp Data Link như một lớp thông dịch để liên kết dữ liệu. Lớp này còn có chức năng thông báo lỗi, đánh số thứ tự các frame, điều khiển dòng, xác định cơ chế truy cập đường truyền...

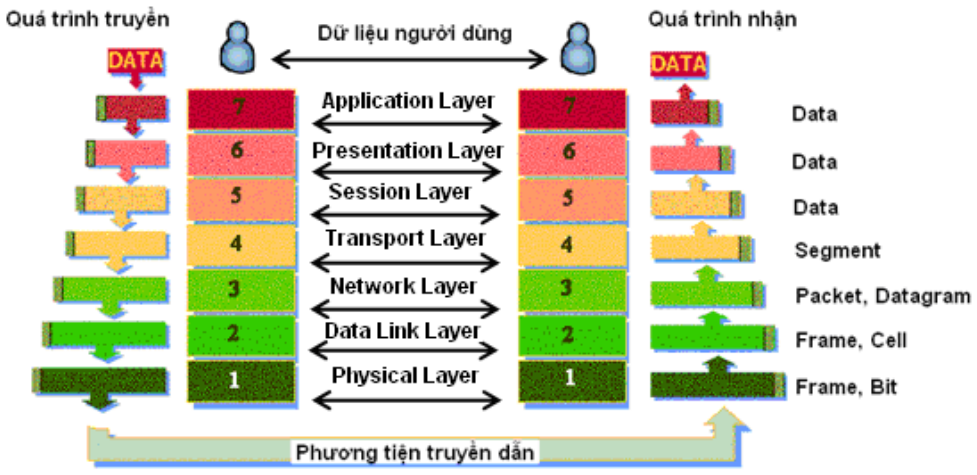
2.1.3.7. Physical Layer (lớp vật lý)

Nhận các frame dữ liệu từ lớp Data Link và truyền chúng trên các phương tiện truyền dẫn theo các tín hiệu điện 0, 1. Một số đặc điểm của lớp này là các chuẩn kết nối, tần số hoạt động, khoảng cách tối đa, tốc độ truyền dữ liệu, băng thông cho phép, mức điện thế hoạt động...

2.1.4. Chức năng của các lớp trong mô hình OSI

∗ Quá trình truyền dữ liệu tại máy gửi

Ở mỗi lớp sẽ có các đơn vị dữ liệu khác nhau, gọi là PDU (Protocol Data Unit - đơn vị dữ liệu giao tiếp). Dữ liệu truyền qua mỗi lớp sẽ được đóng gói thành các PDU của lớp đó.



Hình 2. 3 - Quá trình truyền dữ liệu thông qua 7 lớp OSI

Bước 1: ứng dụng của người dùng tạo ra các dữ liệu (DATA) cần gửi đi trên mạng, các dữ liệu này sẽ được lớp Application đóng gói và gắn thêm vào đầu dữ liệu các thông tin về dữ liệu này (header). Header xác định dữ liệu này của ứng dụng nào (ví dụ: FTP, HTTP...), các thông tin để phục hồi lỗi... và chuyển DATA cho lớp Presentation.

Bước 2: lớp Presentation sẽ thể hiện lại DATA thành dạng dữ liệu chung, nén và mã hóa DATA. Sau đó thêm header chứa thông tin để bên nhận có thể giải nén, giải mã... và chuyển DATA cho lớp Session.

Bước 3: lớp Session thêm header chứa các thông tin kết nối, phục hồi lỗi và chuyển DATA cho lớp Transport.

Bước 4: lớp Transport chia DATA ra thành các segment, sau đó thêm header về số thứ tự segment, các thông tin kiểm soát lỗi và luồng. Các segment được chuyển cho lớp Network.

Bước 5: lớp Network chia các segment thành các packet, đánh địa chỉ và thêm header chứa các thông tin về định tuyến. Tiếp theo packet được chuyển xuống lớp Data Link.

Bước 6: lớp Data Link chia nhỏ các gói tin thành các frame, thêm header chứa các thông tin kiểm soát lỗi, luồng... và chuyển các frame cho lớp Physical.

Bước 7: lớp Physical chuyển các frame thành các bit và truyền trên các phương tiện truyền dẫn sang máy nhận.

∗ Quá trình nhận dữ liệu tại máy nhận

Ngược lại bảy bước trong quá trình truyền dữ liệu. Ở mỗi lớp, các thông tin header PDU của lớp đó được lấy ra. Dựa vào các thông tin đó dữ liệu phục hồi lại để gửi lên lớp trên đồng thời xóa các header của lớp đó đi. Như vậy trong mô hình OSI bên nhận và gửi thì lớp nào chỉ liên lạc với lớp đó mà thôi.

2.1.5. Quá trình tìm đường đi của gói tin

Quá trình gửi gói tin trong mạng máy tính được thực hiện trong các thiết bị mạng như sau:

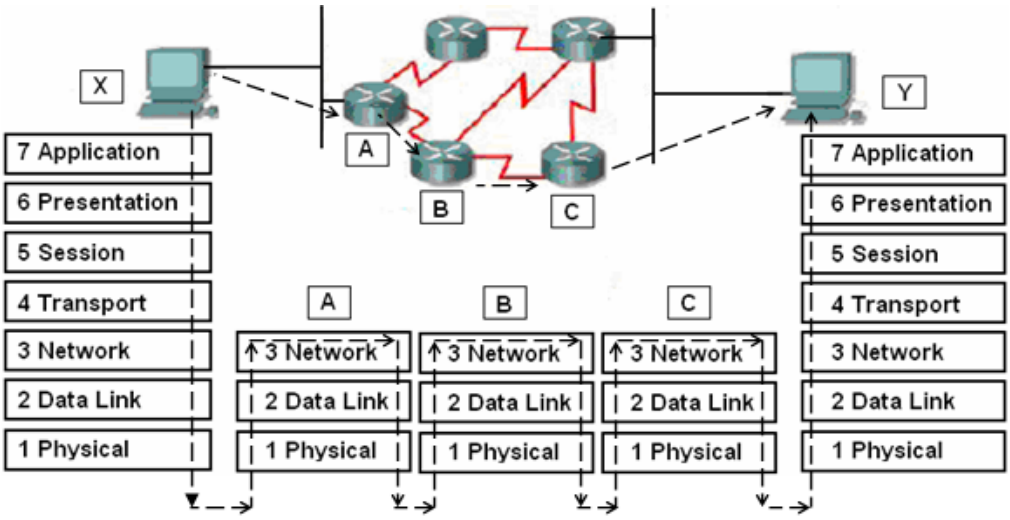
Thiết bị nhận được gói tin luôn có địa chỉ IP nguồn và IP đích, nó sẽ so sánh địa chỉ IP đích với địa chỉ IP của nó.

- Nếu IP của nó và IP đích của gói tin cùng mạng, nó kiểm tra trong ARP table (hoặc MAC table) của nó để tìm địa chỉ MAC đích.
- Nếu đã có, nó truyền gói tin đi.
- Nếu chưa có, nó sẽ tìm địa chỉ MAC đích bằng cách dùng giao thức ARP (sẽ trình bày sau). Cùng mạng nên chắc chắn nó sẽ tìm được MAC đích và truyền gói tin đi đồng thời cập nhật địa chỉ MAC vào ARP table (hoặc MAC table).
- Nếu khác mạng.
- Nếu là bộ định tuyến nó tìm đường đi cho gói tin trong routing table (bảng định tuyến) để gửi gói tin đi. Nếu không có thông tin định tuyến nó gửi qua default gateway (cổng mặc định) nếu có khai báo default gateway.

• Nếu không khai báo default gateway nó sẽ hủy gói tin và thông báo lỗi ***"Destination host unreachable".***

> Lưu ý: trong Windows dùng lệnh.
> ***arp –a*** để xem ARP table.
> ***route print*** để xem bảng định tuyến.
> ***ping*** để kiểm tra một host có tồn tại trên mạng.
> ***tracert*** để xem đường đi của một gói tin.

Quá trình tuyền dữ liệu



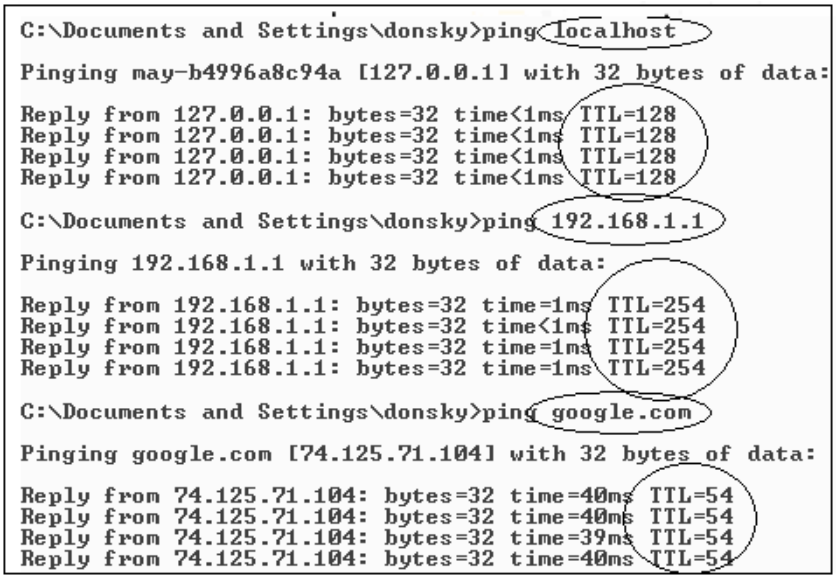
Hình 2. 4 - Quá trình truyền dữ liệu thông qua các lớp OSI

Ở hình 2.4, dữ liệu được truyền từ máy X đến máy Y thông qua hệ thống các router.

• Bước 1: trình ứng dụng tạo ra dữ liệu thông qua quá trình đóng gói dữ liệu, thêm vào header và trailer. Đánh địa chỉ IP nguồn – IP đích (X-Y) cho các gói tin và chuyển cho lớp Physical để truyền lên mạng. X, Y chắc chắn khác mạng nên máy tính X sẽ truyền các gói tin cho router A (theo khai báo default gateway) thông qua lớp Physical bằng các bit.

• Bước 2: lớp Physical của router A nhận được các bit sẽ phục hồi lại gói tin và chuyển lên lớp Network. Địa chỉ A, Y chắc chắn khác mạng nên router A dựa vào routing table để xác định đường đi tiếp theo cho gói tin. Router A xác định rằng, để đi qua mạng Y thì phải đi qua router B. Router A truyền các gói tin cho router B.

Ở router A gói tin được phục hồi và bị giết (kill) đi thành các bit để truyền đi. Như vậy mỗi lần qua một router gói tin bị kill một lần.



Hình 2. 5 - Thời gian sống (TTL) của gói tin trên mạng

Ở hình 2.5, khi ping localhost TTL (Time To Live) = 128. Vậy trong windows, gói tin khi phát sinh sẽ có thời gian sống là 128. Khi ping google.com TTL=54 (128 – 54 = 74), như vậy xác định được từ máy mình đến máy google.com đi qua 74 thiết bị router. Nhưng khi ping vào một thiết bị router (192.168.1.1) thì TTL=254. Khi TTL của gói tin bằng 0 nó sẽ bị hủy (tránh tạo vòng lặp trong mạng).

- Bước 3: router B dựa vào routing table của mình xác định rằng, để đi đến mạng Y thì phải đi qua router C. Các gói tin sẽ được truyền cho router C.
- Bước 4: router C xác định C, Y cùng mạng, dựa vào ARP table của mình nó truyền gói tin cho máy Y. Thông qua 7 lớp, dữ liệu sẽ tái tạo lại và chuyển cho ứng dụng người dùng tại máy Y.

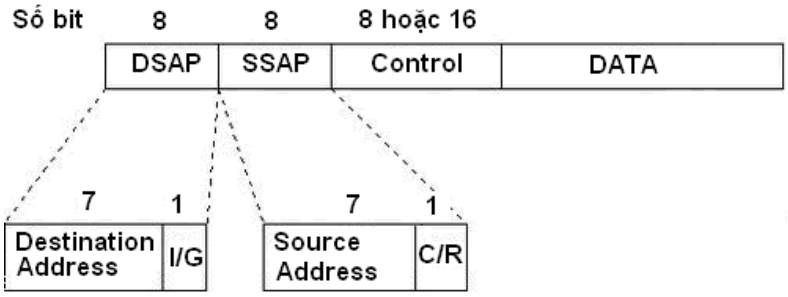
2.2. Khảo sát chi tiết lớp 2 (Data Link)

Lớp Network và lớp Physical không thể hiểu nhau vì một bên là mạng logic làm việc với địa chỉ IP một bên là mạng vật lý làm việc với địa chỉ MAC. Vậy lớp Data Link phải hiểu được cả hai lớp Network và Physical nên nó chia làm 2 lớp con LLC và MAC.

2.2.1. Lớp con LLC và MAC

∗ LLC (Logical Link Control)

Lớp LCC đóng gói dữ liệu từ lớp Network chuyển xuống thành các khối, thêm các thông tin vào để truyền các gói IP đến đích. Được mô tả trong RFC1483, ở mỗi lớp đều có một đơn vị dữ liệu để giao tiếp gọi là PDU (Protocol Data Unit).



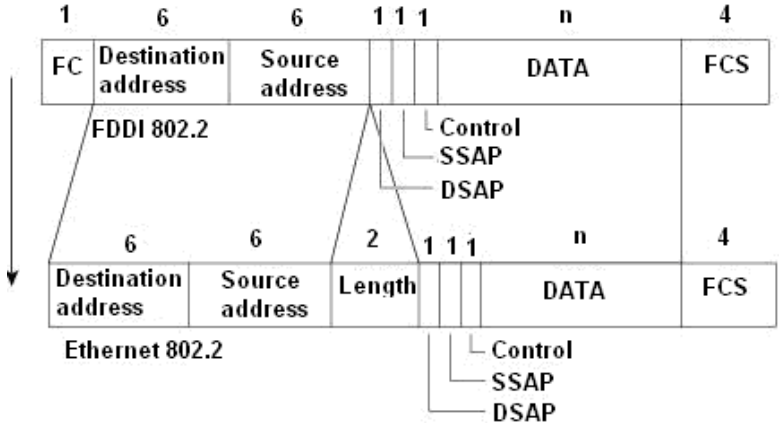
Hình 2. 6 - PDU của LCC

Ở hình 2.6, PDU của LCC đóng gói dữ liệu và thêm 2 thành phần điểm truy cập nguồn (SSAP) và điểm truy cập đích (DSAP) của đặc tả 802.2. Sau đó đóng gói trở lại dạng IP và chuyển cho lớp MAC.

∗ MAC (Media Access Control)

Lớp MAC nhận các gói tin từ lớp LCC, gán địa chỉ định danh cho các gói tin. Địa chỉ này là địa chỉ vật lý (MAC). Địa chỉ MAC không phân cấp như địa chỉ IP, nó ngang hàng nhau trên mạng và là địa chỉ duy nhất. Lớp MAC phải làm sao có địa chỉ này để truyền gói tin đến đích, vì thực chất để truyền gói tin đến đúng thiết bị mạng là truyền đến địa chỉ MAC của thiết bị mạng đó.

Lớp MAC chia dữ liệu thành các frame dữ liệu, đánh số các frame, thêm các thành phần kiểm soát lỗi.



Hình 2. 7 - Cấu trúc frame của FDDI 802.2 và Ethernet 802.2

2.2.2. Quá trình phân giải địa chỉ MAC

Gói tin TCP/IP khi truyền trên mạng nó phải đúng cả hai địa chỉ IP và địa chỉ MAC nên hầu hết các thiết bị mạng đều có một ARP table để lưu lại IP và MAC của các thiết bị nối với mình. Khi một gói tin truyền đến, thiết bị mạng sẽ so sánh trong ARP table để tìm ra MAC của thiết bị nhận. Nếu trường hợp không có trong ARP table tức chưa biết được địa chỉ MAC của thiết bị nhận, quá trình phân giải MAC được thực hiện thông qua giao thức ARP. Có 2 cách tìm MAC:

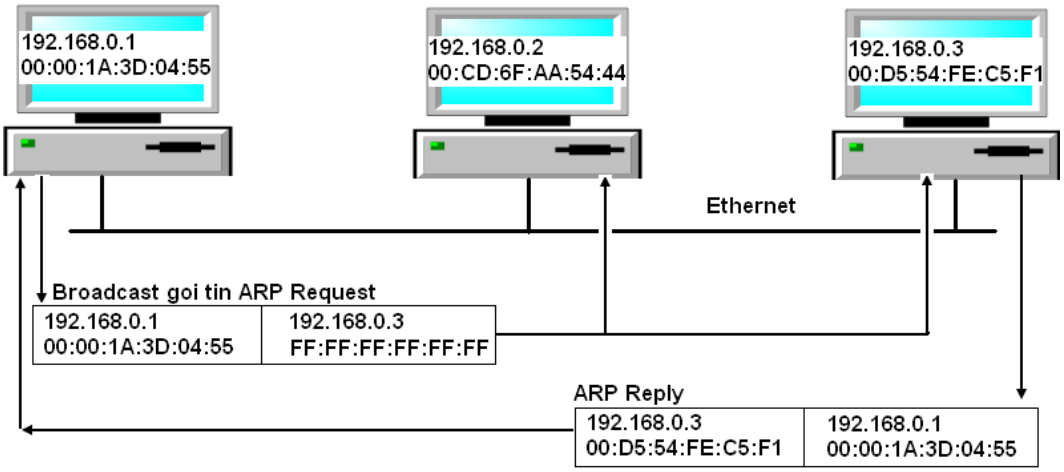
Tự học: khi nhận được một gói tin trong đó luôn có địa chỉ IP, MAC nguồn. Thiết bị nhận sẽ kiểm tra IP và MAC có trong ARP table chưa, nếu chưa có sẽ cập nhật vào ARP table.

Đi hỏi: thiết bị sẽ broadcast một gói tin ARP request chứa địa chỉ IP cần xin MAC. Các thiết bị trên mạng đều nhận được và phân tích gói tin này. Có hai trường hợp xảy ra:

Địa chỉ IP cần xin MAC cùng mạng, thiết bị nào nhận được thấy đó là IP của mình thì trả lời bằng gói tin ARP reply. Nếu không có thiết bị nào có IP đó thì không có ARP reply nào cả.

Địa chỉ IP cần xin MAC khác mạng, lúc này việc xin MAC thực hiện qua thiết bị định tuyến router.

- Nếu router có bật tính năng proxy ARP, khi nhận được gói tin ARP request nó kiểm tra xem địa chỉ IP xin MAC có khác mạng không. Nếu khác nó trả lời gói tin ARP response chứa địa chỉ MAC của cổng (port trên thiết bị router) mà nó nhận được gói tin ARP request.
- Nếu thiết bị gửi có khai báo default gateway trỏ về router thì gói tin sẽ có MAC đúng của router và gói tin được truyền cho router xử lý.
- Trường hợp không khai báo default gateway hay tính năng proxy ARP của router không bật thì gói tin sẽ bị hủy.



Hình 2. 8 - Cập nhật Địa chỉ MAC

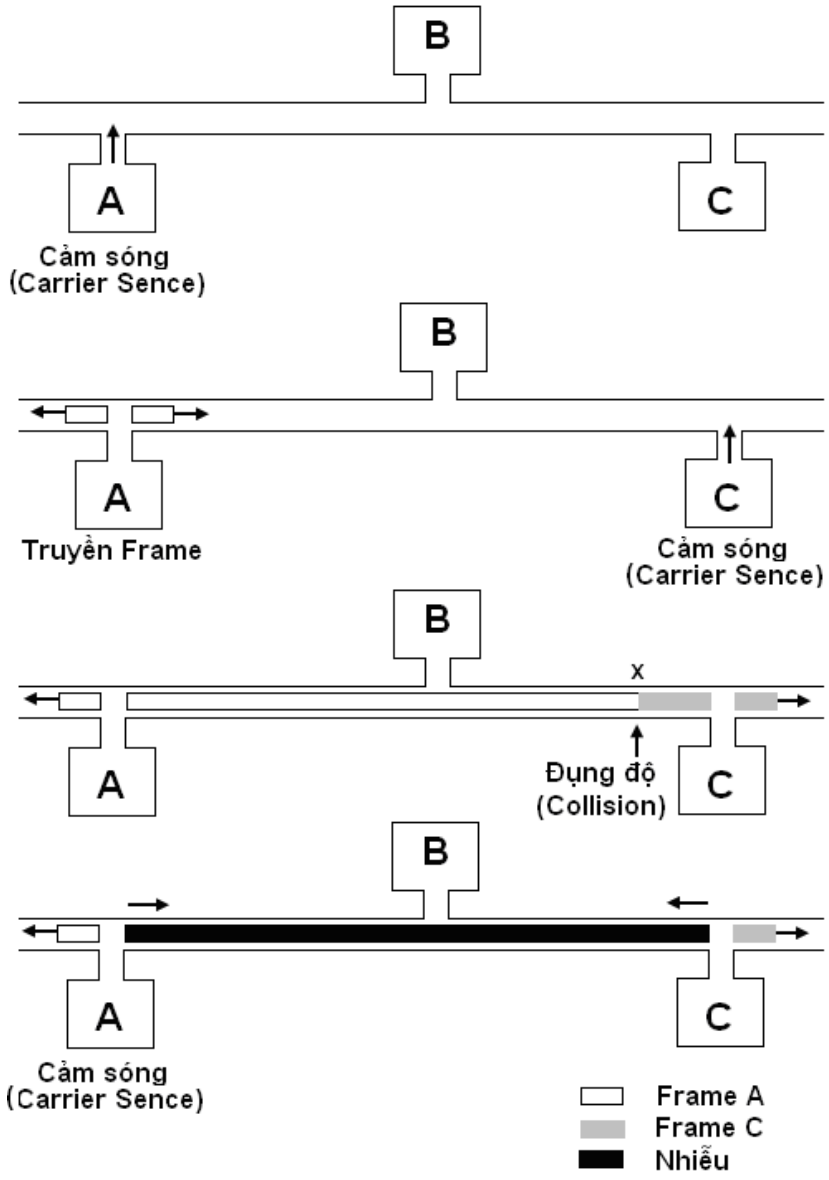
2.3. Các phương pháp truy cập đường truyền

2.3.1. Cảm sóng đa truy chấp nhận đụng độ (CSMA/CD)

Trong mạng LAN có dây, chuẩn Ethernet IEEE802.3, các máy cùng nhau chia sẻ đường truyền và cơ hội truy cập đường truyền là như nhau (multiple access). Để biết có máy nào đang truy cập đường truyền hay không, máy tính kiểm tra sóng mang (carrier) trên mạng. Nếu có sóng mang, tức có máy đang truyền dữ liệu nó sẽ chờ một khoảng thời gian sau đó cảm sóng lại (carrier sense). Với việc mỗi máy lắng nghe đường truyền và cùng truy cập chung một đường truyền được gọi là cảm sóng đa truy.

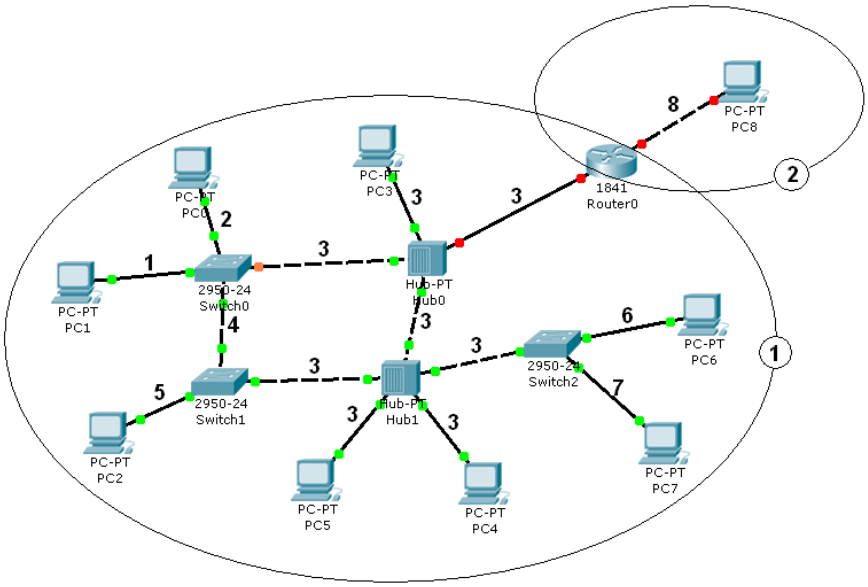
Với kiểu truy cập này đụng độ có thể xảy ra. Khi hai máy cùng cảm sóng tại một thời điểm, phát hiện đường truyền rảnh, 2 máy cùng truyền dữ liệu. Việc đụng độ (collision) chắc chắn xảy ra và với kỹ thuật này, hay chấp nhận sự đụng độ này. Khi phát hiện đụng độ, hai máy sẽ hủy sự truyền trong một khoảng thời gian ngẫu nhiên sau đó cảm sóng và truyền lại.

Các máy có thể đụng độ với nhau trong mạng tạo thành một miền gọi là miền đụng độ (collision domain). Khi số lượng máy trong mạng càng lớn thì miền đụng độ này càng lớn, việc này làm giảm băng thông mạng.



Hình 2. 9 - CSMA/CD cảm sóng đa truy chấp nhận đụng độ

2.3.2. Phân biệt broadcast domain (miền quảng bá) và collision domain (miền đụng độ)



Hình 2. 10 - Broadcast domain và collision domain

Ở hình 2.10, có 2 broadcast domain và 8 collision domain. Khi PC1 broadcast một gói tin. Switch0 sẽ truyền gói tin đến tất cả các port trừ port nhận vậy PC0, Switch1, Hub0 nhận được gói tin này. Khi switch1 nhận được nó gửi cho PC2, Hub1. Hub0 nhận được nó cũng truyền cho tất cả các port của nó trừ port nhận nên PC3, Router0, Hub1 nhận được. Hub 1 nhận được thì PC5, PC4, Switch2 nhận được. Switch2 nhận được thì PC6, PC7 nhận được. Router0 không cho phép gói tin broadcast đi qua.

Vậy tất cả thiết bị trong vòng tròn 1 đều nhận được gói tin broadcast này hay nó là một broadcast domain.

Tương tự Router0 và PC8 là một broadcast domain.

Khi hub nhận được một gói tin nó sẽ truyền gói tin đến tất cả các port còn lại trừ port nhận. Vậy tất cả các port của hub có khả năng đụng độ với nhau hay là một collision domain

Còn switch thì ngược lại, nhờ có MAC table nên có tính năng truyền gói tin đến chính xác port nhận nên tránh được đụng độ. Vậy mỗi port của switch là một collision domain.

Theo đó ở hình trên có 8 miền đụng độ.

Lưu ý: trong một broadcast domain có thể có nhiều collision domain.

2.3.3. Chuyển thẻ bài (Token-passing)

Trong mạng IEEE 802.5 các máy nối thành vòng tròn, thường sử dụng một thẻ bài truyền tuần tự cho các máy trên mạng. Thẻ bài là một đơn vị dữ liệu đặc biệt khác với dữ liệu thông thường. Khi một máy nhận được thẻ bài, nó giữ lại thẻ bài và truyền một frame dữ liệu trong hàng đợi của nó sau đó truyền thẻ bài cho máy kế tiếp. Nếu một máy nhận

được thẻ bài mà không có frame dữ liệu nào cần truyền nó lập tức truyền thẻ bài cho máy kế tiếp.

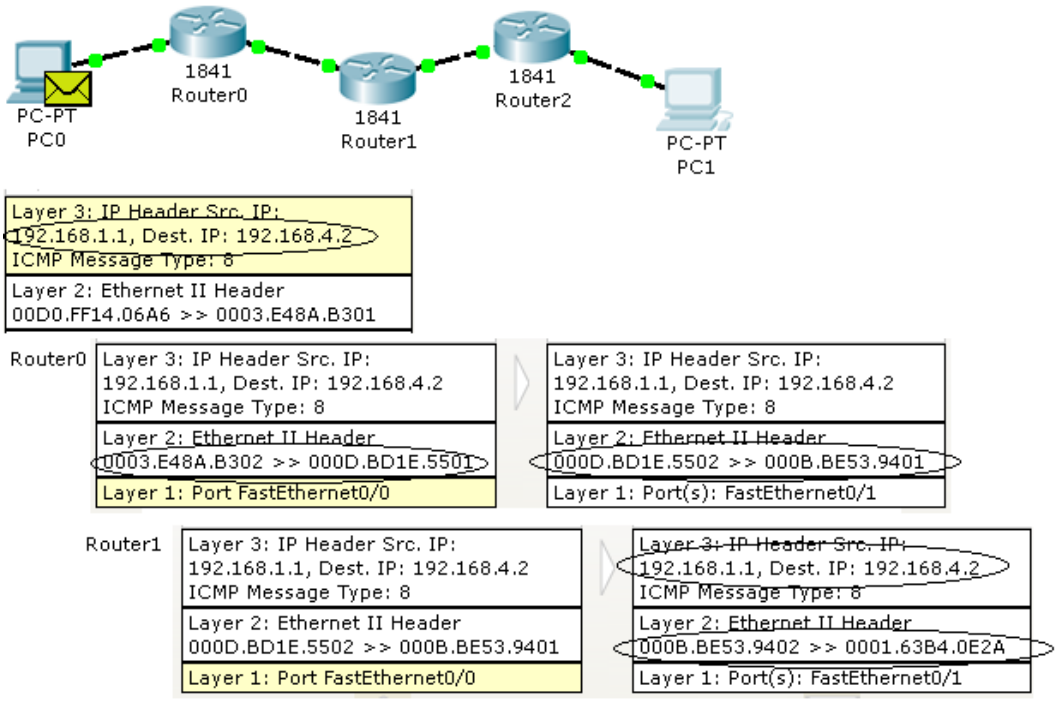
Với kỹ thuật này sẽ không có đụng độ xảy ra và các máy sử dụng đường truyền một cách công bằng (không phụ thuộc vào tốc độ máy). Nó đáp ứng cho các mạng lớn, khi số lượng máy tăng lên ít bị ảnh hưởng băng thông mạng. Nhưng nó sẽ mất kết nối toàn mạng nếu một máy làm mất thẻ bài hoặc một máy bị mất kết nối.

Kỹ thuật này thích hợp trong mạng FDDI, là công nghệ mạng tốc độ cao thường dùng cho sợi quang (có thể dùng sợi đồng). Với khoảng cách lên đến 100Km, ứng dụng trong MAN. FDDI có 2 vòng ngược nhau dùng để backup. Kỹ thuật này sẽ trình bày chi tiết ở cuối bài.

Hình 2. 11 - FDDI

2.4. Khảo sát chi tiết lớp 3 (Network)

Chức năng quan trọng nhất của lớp Network là định tuyến (routing) cho gói tin. Công việc này có 2 phần là chuyển mạch (switching) và tìm đường (path determination).

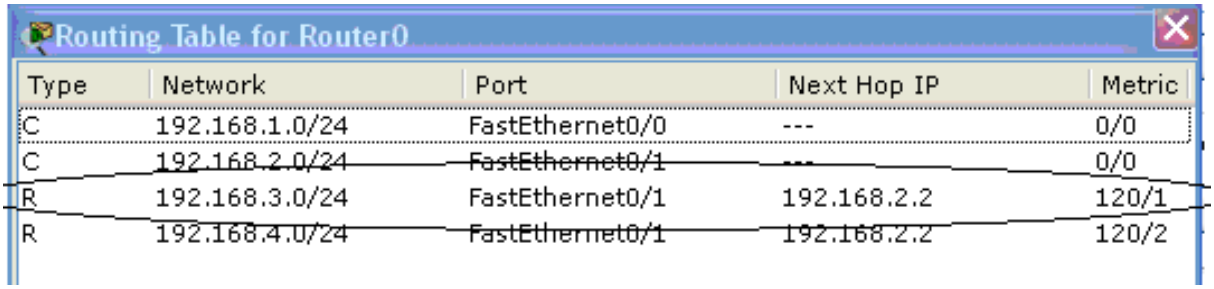


Hình 2. 12 - Sự thay đổi địa chỉ MAC khi qua các router

Switching: gói tin từ máy gửi mang địa chỉ IP nguồn, MAC nguồn, IP đích, MAC của Router đầu tiên (hay default gateway). Router đầu tiên sẽ phân tích gói tin và tìm MAC của IP đích, nếu nó không biết truyền đi đâu mà nó không khai báo default gateway thì nó hủy gói tin. Ngược lại nó sẽ đổi địa chỉ MAC nguồn là MAC cổng nó truyền đi, MAC đích là MAC của cổng trên router kế tiếp và nó truyền gói tin đến router tiếp theo (next hop). Vậy khi gói tin qua mỗi hop địa chỉ MAC nguồn và MAC đích thay đổi liên tục, nhưng IP nguồn và IP đích không đổi. Xem hình 2.12.

Path determination: dựa vào bảng định tuyến (routing table) và các giải thuật tìm đường đi ngắn nhất (routing algorithm, ví dụ: Dijkstra, Bellman-Ford...) mà router xác định được đường đi ngắn nhất đến mạng đích.

Có thể định tuyến tĩnh (static) bằng cách cập nhật vào routing table. Router có thể tự cập nhật routing table bằng cách broadcast một phần hoặc toàn bộ thông tin của routing table cho các router láng giềng, được gọi là định tuyến động (RIP, IGRP...).



Hình 2. 13 - Bảng định tuyến của Router0 cập nhật bằng giao thức RIP

Ở hình 2.13 dòng 3, cột Type là R có nghĩa entry này được cập nhật động bằng giao thức RIP. Các cột tiếp theo thể hiện, để đi qua mạng 192.168.3.0/24 thì đi qua cổng FastEthernet0/1 của nó và cổng biên là 192.168.2.2 (gateway nằm trên router kế tiếp - Cisco gọi là next hop), độ ưu tiên của RIP là 120 (càng nhỏ càng ưu tiên) hay còn gọi là trọng lượng (Weighting).

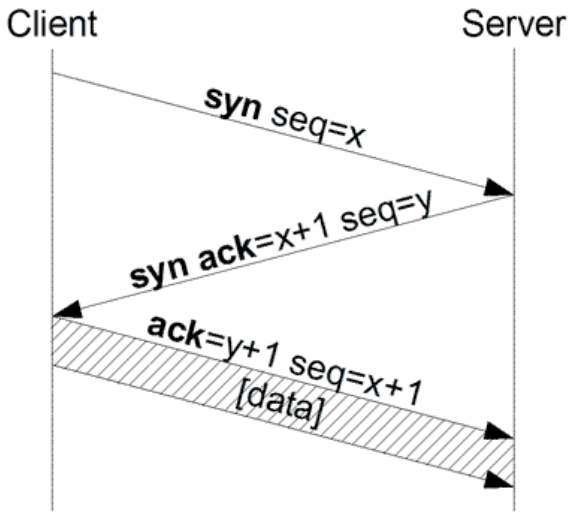
2.5. Khảo sát chi tiết lớp 4 (Transport)

Nhiệm vụ chính của lớp 4 là xác định phương thức truyền dữ liệu. Truyền tin cậy (TCP) đáp ứng các dịch vụ offline, truyền không tin cậy (UDP) đáp ứng các dịch vụ online.

2.5.1. TCP

Giao thức TCP thiết lập kết nối tin cậy và có thứ tự, kiểm soát lỗi và truyền lại. TCP đòi hỏi phải kết nối trước khi truyền dữ liệu và trải qua 3 bước: thiết lập kết nối, truyền dữ liệu và kết thúc kết nối.

Giao thức TCP thiết lập kết nối bằng phương pháp bắt tay 3 lần (three-way handshake), trước khi client muốn kết nối với server thì server phải đăng ký mở một cổng dịch vụ (mở thụ động) thông qua cổng này client kết nối với server (mở chủ động).



Hình 2. 14 - Tạo kết nối TCP, bắt tay 3 lần

∗ Quá trình bắt tay 3 lần:

Client yêu cầu mở cổng dịch vụ bằng cách gửi gói tin SYN (gói tin TCP, xem hình 2.14) trong gói tin này sequence number được gán bằng con số ngẫu nhiên x.

Server hồi đáp lại bằng gói tin syn-ack, trong gói tin này giá trị acknowlidgement number có giá trị là x+1 và sequence number được gán bằng con số ngẫu nhiên y.

Hoàn tất quá trình, client gửi cho server gói tin ACK, trong đó sequence number có giá trị x+1 và acknowledgement number có giá trị là y+1. Lúc này cả client và server đều được xác nhận một kết nối đã được thiết lập và việc truyền dữ liệu bắt đầu.

+	Bit 0 - 3	4 - 9	10 - 15	16 - 31
0	Source Port			Destination Port
32	Sequence Number			
64	Acknowledgement Number			
96	Data Offset	Reserved	Flags	Window
128	Checksum			Urgent Pointer
160	Options (optional)			
160/192+	Data			

Hình 2. 15 - Cấu trúc gói tin TCP

2.5.2. UDP

Ngược lại với TCP, UDP truyền dữ liệu không cần kết nối. Các gói dữ liệu đến không cần đúng thứ tự và không truyền lại khi lỗi. UDP đáp ứng cho các ứng dụng đáp ứng thời gian thực (ví dụ: DNS, VoIP, Webcam...). Khung dữ liệu của UDP rất đơn giản và không cần trả ACK về nên băng thông cao đáp ứng ứng dụng có số người dùng lớn.

+	Bits 0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Hình 2. 16 - Cấu trúc gói tin UDP

2.5.3. Khái niệm Port

Khi truyền thông trên mạng, mỗi ứng dụng được quy định một port để truyền dữ liệu. ví dụ: HTTP 80, FTP 21, DNS 53... Có tổng cộng 65535 port . Xem ở URL:

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

TCP và UDP sử dụng các port hoặc socket để truyền dữ liệu cho các ứng dụng. Các port từ 0-1023 là các port chuẩn (đã được định nghĩa sẵn và bất khả xâm phạm) gọi là Well-known port. Các port từ 1024 trở đi gọi là high port, người dùng có thể đăng ký để sử dụng. IANA là tổ chức quản lý việc cấp phát các port này.

Vậy khi truyền dữ liệu trong mạng, ngoài IP phải xác định thêm port cho dữ liệu truyền thuộc ứng dụng nào. ví dụ: cần kết nối vào một FTP server 192.168.1.100:21, IP của FTP server là 192.168.1.100, port của FTP là 21. Đây là khái niệm ***Socket = IP + Port***, được viết theo cú pháp ***IP:Port***.

Lưu ý: dùng lệnh ***netstat*** để kiểm tra các port đang mở trong hệ thống Windows.

```
C:\Documents and Settings\donsky>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    may-b4996a8c94a:2168   localhost:2628         ESTABLISHED
  TCP    may-b4996a8c94a:2628   localhost:2168         ESTABLISHED
  TCP    may-b4996a8c94a:2628   localhost:4777         ESTABLISHED
```

Hình 2. 17 - Lệnh netstat kiểm tra các port đang mở

2.6. Mô hình tham chiếu TCP/IP

Mô hình TCP/IP xuất phát từ mạng ARPANET của bộ quốc phòng Mỹ và phát triển để dùng truyền thông trên Internet. Kỹ thuật ARPA bao gồm tập hợp các chuẩn mạng, đặc tả các giao thức truyền thông trên Internet. Ngày nay nó đã phát triển và dùng cho LAN, MAN, WAN và Internet.

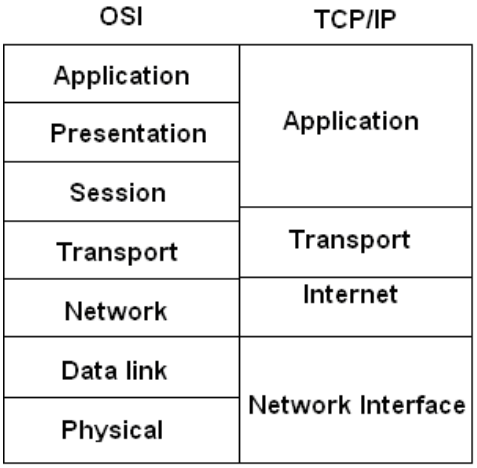
2.6.1. Bốn lớp của mô hình TCP/IP

Application: quản lý các giao thức của các ứng dụng: HTTP, FTP, DNS, POP, SMTP... Được gộp 3 lớp đầu trong mô hình OSI: Application, Presentation, Session.

Transport: bảo đảm truyền thông, thông qua 2 giao thức TCP (truyền tin cậy) và UDP (truyền không tin cậy).

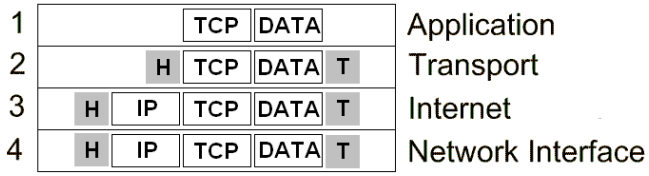
Internet: tìm đường đi tối ưu cho gói tin, dùng giao thức IP.

Network Interface: truyền thông tin trên thiết bị truyền dẫn thông qua các giao tiếp mạng. Được gộp hai lớp cuối trong mô hình OSI là Data Link và Physical.



Hình 2. 18 - Tương quan giữa hai mô hình OSI và TCP/IP

2.6.2. Các bước đóng gói dữ liệu



Hình 2. 19 - Đóng gói dữ liệu trong TCP/IP

Bước 1: dữ liệu được lớp Application nén, mã hóa... Gắn thêm header chuyển cho lớp Transport.

Bước 2: lớp Transport gắn thêm header để xác định dữ liệu được truyền theo phương thức nào và chuyển cho lớp Internet.

Bước 3: lớp Internet thêm địa chỉ IP và các thông tin về đường đi sau đó chuyển cho lớp Network Interface.

Bước 4: lớp Network Interface thêm địa chỉ MAC và các thông tin kiểm soát lỗi.

2.6.3. So sánh mô hình OSI và TCP/IP

∗ Giống nhau

- Đều có cấu trúc phân lớp (lớp này không ảnh hưởng lớp kia).
- Đều có các lớp Application, Transport, Network (đáp ứng nhiều ứng dụng, nhiều phương thức truyền và tìm đường đi tối ưu).
- Đều dùng kỹ thuật chuyển gói (packet switched).
- Quản trị viên phải nắm rõ hai mô hình này.
- Khác nhau

OSI	TCP/IP
Chi tiết, dùng để nguyên cứu và giảng dạy. Chia thành 7 lớp riêng biệt. Lớp Application, Presentation, Session Lớp Network Lớp Data link và Physical	Đơn giản, ứng dụng hiệu quả trong thực tế. Chia thành 4 lớp riêng biệt. Gộp lại thành lớp Application Đổi thành lớp Internet Gộp lại thành lớp Network Interface

2.7. Câu hỏi và bài tập

1. Trình bày ngắn gọn các chức năng chính của các lớp trong mô hình OSI và TCP/IP?

2. Trình bày quá trình phân giải địa chỉ MAC đích cho gói tin của lớp Data Link?

3. Trình bày quá trình tìm đường đi cho gói tin của lớp Network?

4. So sánh hai giao thức TCP và UDP, ứng dụng thực tế của nó trong các dịch vụ mạng như thế nào?

5. Nêu lý do tại sao phải dùng cơ chế CSMA/CD chấp nhận đụng độ mà không dùng cơ chế tránh đụng độ.

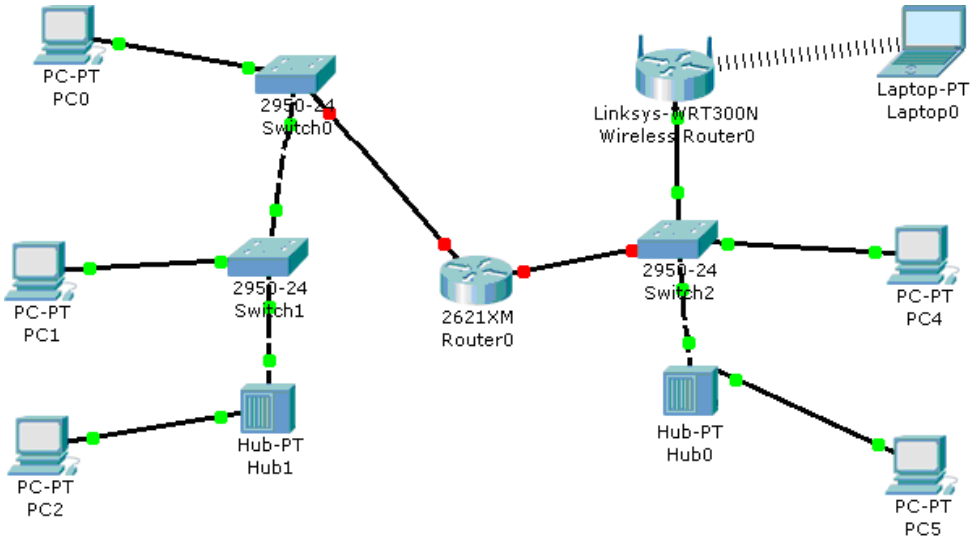
6. Lập bảng so sánh hai mô hình OSI và TCP/IP.

7. Nếu một gói tin đến router, trong bảng định tuyến của router không cho biết đường đi đến mạng đích. router sẽ làm gì?

8. Dịch vụ online thường dùng cơ chế truyền nào, tại sao?

9. Trình bày cơ chế bắt tay 3 lần trong TCP, tại sao phải bắt tay 3 lần?

10. Hình vẽ bên dưới có bao nhiêu collision domain và bao nhiêu broadcast domain?


PC-PT
PC0
2950-24
Switch0
Linksys-WRT300N
Wireless Router0
Laptop-PT
Laptop0
PC-PT
PC1
2950-24
Switch1
2621XM
Router0
2950-24
Switch2
PC-PT
PC4
Hub-PT
Hub1
Hub-PT
Hub0
PC-PT
PC2
PC-PT
PC5

CHƯƠNG 3 - PHƯƠNG TIỆN TRUYỀN DẪN VÀ THIẾT BỊ MẠNG

∗ Tóm tắt nội dung chương 3

- Các khái niệm, đặc tính, cấu tạo, cách lắp đặt và ưu khuyết điểm của các phương tiện truyền dẫn và thiết bị mạng.

∗ Mục tiêu chương 3

Sau khi học xong sinh viên có khả năng:

- Trình bày được các khái niệm, đặc tính, cấu tạo, cách lắp đặt, ưu khuyết điểm của các phương tiện truyền dẫn và thiết bị mạng.
- Đọc và hiểu được các thông số của nhà sản xuất ghi trên các phương tiện truyền dẫn và thiết bị mạng.

3.1. Giới thiệu về phương tiện truyền dẫn

3.1.1. Khái niệm

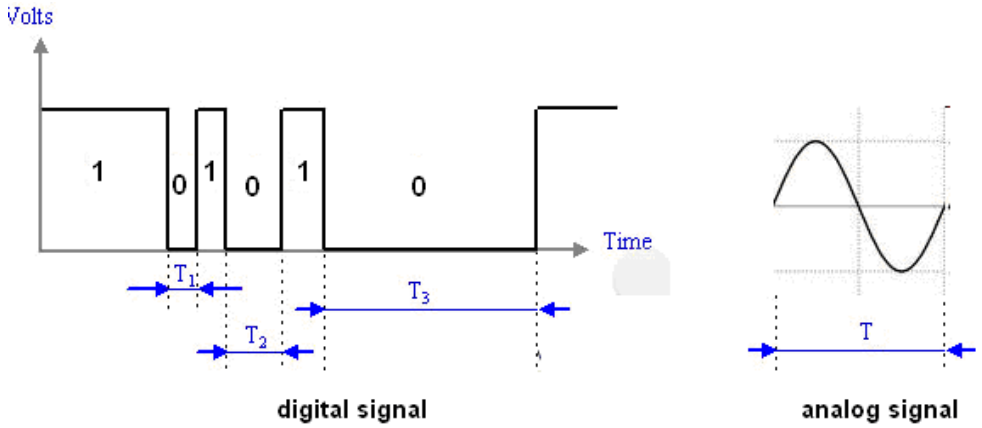
Phương tiện truyền dẫn (transmission media) là phương tiện vật lý cho phép truyền tải tín hiệu giữa hai thiết bị trên mạng.

Có hai loại tín hiệu:

- Tín hiệu tương tự (analog).
- Tín hiệu số (digital).

Có hai loại phương tiện truyền dẫn chủ yếu:

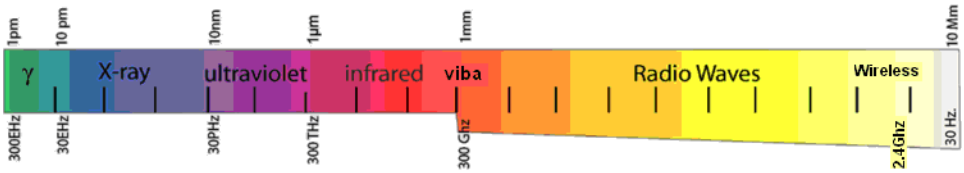
- Hữu tuyến (bounded media).
- Vô tuyến (boundless media).



Hình 3. 1 - Hai loại tín hiệu truyền trên phương tiện truyền dẫn

3.1.2. Tần số truyền thông

Tín hiệu truyền trên môi trường truyền dẫn dù là analog hay digital, truyền hữu tuyến hay vô tuyến đều có một tần số nhất định. Tùy theo thiết kế mà tín hiệu sẽ được truyền trên dải tần số nào. Sau đây là một số dải tần số quy định.



Hình 3. 2 - Dải tần số

Tín hiệu truyền trong mạng LAN dùng dải tần từ sóng Radio đến hồng ngoại (infrared) thông qua cáp đồng trục, cáp xoắn đôi hay phủ sóng radio. Sóng viba dùng kết nối vệ tinh-mặt đất và mặt đất-mặt đất. Sóng Wireless, bluetooth dùng dải tần số tự do không cần đăng ký. Sóng hồng ngoại dùng với khoản cách ngắn và các tần số cao dùng trong cáp quang.

3.1.3. Các đặc tính của phương tiện truyền dẫn

Băng thông (bandwidth): tổng dung lượng thông tin có thể truyền tại một thời điểm nhất định. Nó phụ thuộc vào nhiều yếu tố như phương tiện truyền, kỹ thuật truyền, thiết bị truyền. Băng thông thường là thông số đánh giá trong truyền dẫn và nó giúp quản lý việc truyền tải trên mạng.

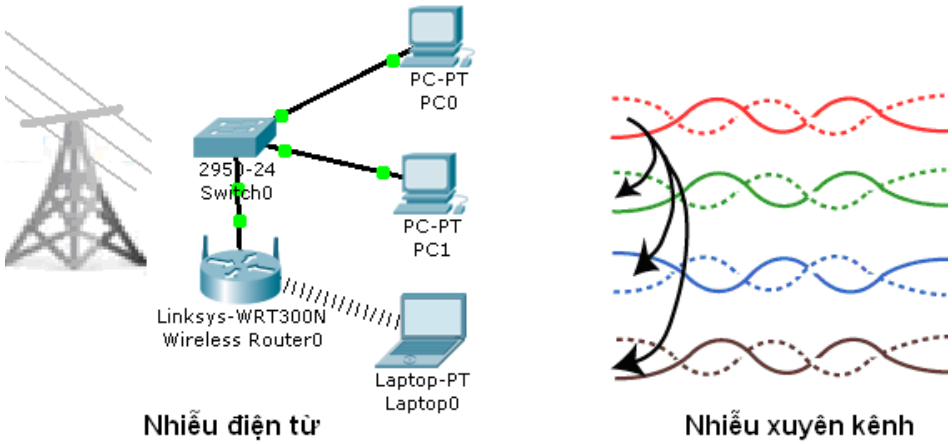
Đơn vị cơ bản của băng thông là Bps (bit trên giây), Kbps = 1000 Bps, Mbps = 1000 Kbps, Gbps = 1000 Mbps, Tbps = 1000 Gbps...

Thông lượng (throughput): tổng dung lượng thông tin thực sự truyền tại một thời điểm nhất định.

Băng tần cơ sở (baseband): dành toàn bộ băng thông cho một kênh truyền.

Băng tần mở rộng (boardband): chia sẻ băng thông cho nhiều kênh truyền, cho phép nhiều kênh truyền trên một phương tiện truyền dẫn.

Độ suy giảm (attenuation): tín hiệu đi xa sẽ bị suy giảm biên độ và mất hẳn tùy vào phương tiện truyền dẫn và khoảng cách khác nhau. Như vậy ứng với mỗi phương tiện truyền dẫn sẽ có các thông số kỹ thuật cho từng môi trường, thiết bị mạng và người dùng phải tuân thủ các thông số kỹ thuật này khi thiết kế hoặc triển khai.



Hình 3. 3 - Nhiễu điện từ và nhiễu xuyên kênh

Nhiễu điện từ (EMI): khi phương tiện truyền dẫn đi trong môi trường có điện từ, điện từ này sẽ tác động làm sai lệch tín hiệu trong phương tiện truyền dẫn. Vì vậy khi thiết kế phải chú ý đến môi trường xung quanh và chống nhiễu điện từ cho phương tiện truyền dẫn và thiết bị. Thường các dây dẫn dùng lưới kim loại tạo ra lồng Fraday để chống nhiễu điện từ.

Nhiễu xuyên kênh (crosstalk): khi có nhiều kênh truyền trên một phương tiện truyền dẫn, từ trường do chúng sinh ra gây nhiễu lẫn nhau. Thường từng cặp cáp được xoắn đôi để từ trường khử lẫn nhau không gây nhiễu ra bên ngoài.

3.1.4. Các loại truyền dẫn

Đơn công (simplex): Trong loại truyền này, một thiết bị chỉ có tính năng phát tín hiệu và một thiết bị chỉ có tính năng thu tín hiệu. Ứng dụng trong truyền thanh, truyền hình...

Bán song công (half duplex): thiết bị tại một thời điểm chỉ có thể thu hoặc phát tín hiệu. Ứng dụng trong bộ đàm, có nút bật để chuyển sang chế độ phát hoặc thu.

Song công (full duplex): trong cùng một thời điểm thiết bị vừa thu vừa phát tín hiệu. Ứng dụng trong điện thoại.

3.2. Các loại cáp

3.2.1. Cáp đồng trục

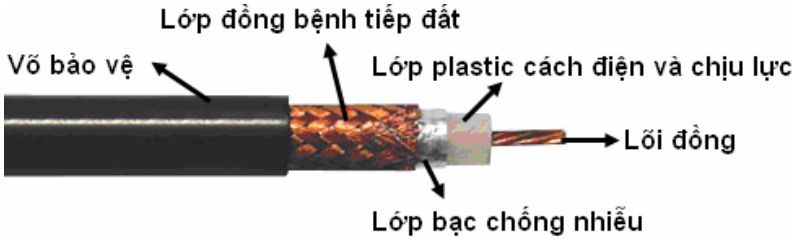
∗ Cấu tạo

Chính giữa là một dây dẫn trung tâm, thường làm bằng đồng hoặc đồng bện.

Tiếp theo là một lớp cách điện, thường làm bằng plastic vừa chống nhiễu vừa chịu lực khi kéo dây với khoảng cách dài.

Tiếp theo là lưới đồng bện, dùng làm dây tiếp đất và tạo lòng Faraday chống nhiễu điện từ.

Bên ngoài là võ plastic bảo vệ.



Hình 3. 4 - Cấu tạo chung của cáp đồng trục

∗ Các loại cáp đồng trục

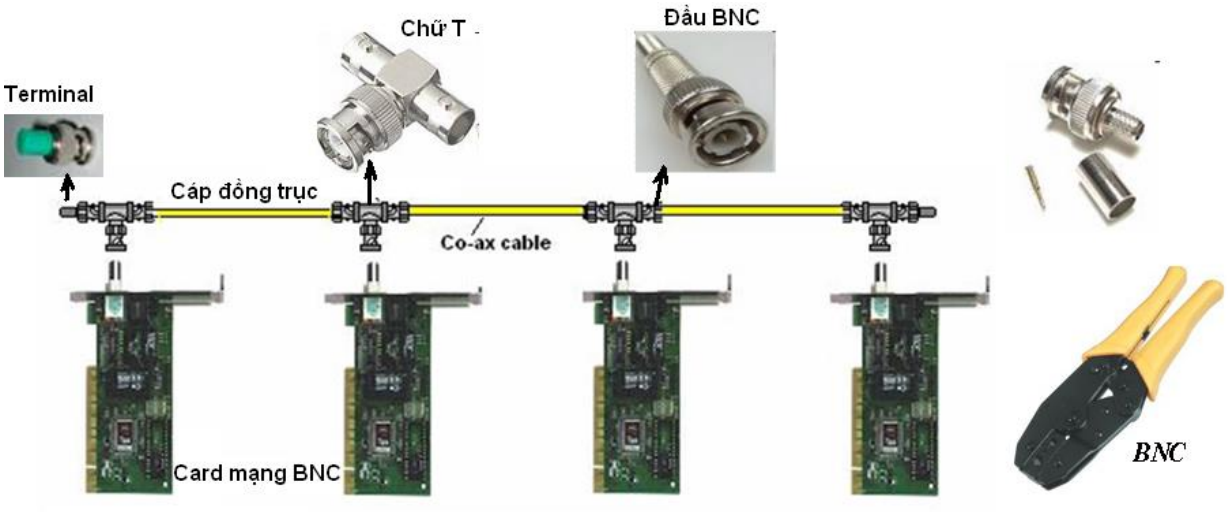
Cáp mỏng (thinnet): đường kính 0,25 inch, tốc độ tối đa dùng trong ethernet là 10 Mbps, khoảng cách tối đa là 200 m. Ngoài thị trường gọi là cáp 3C.

- Cáp RG-58, trở kháng 50 Ω dùng cho ethernet, camera.

- Cáp RG-59, trở kháng 75 Ω dùng cho truyền hình cáp.

Cáp dày (thicknet): đường kính 0,5 inch, tốc độ tối đa dùng trong ethernet là 10 Mbps, khoảng cách tối đa là 500 m, Ngoài thị trường gọi là cáp 5C.

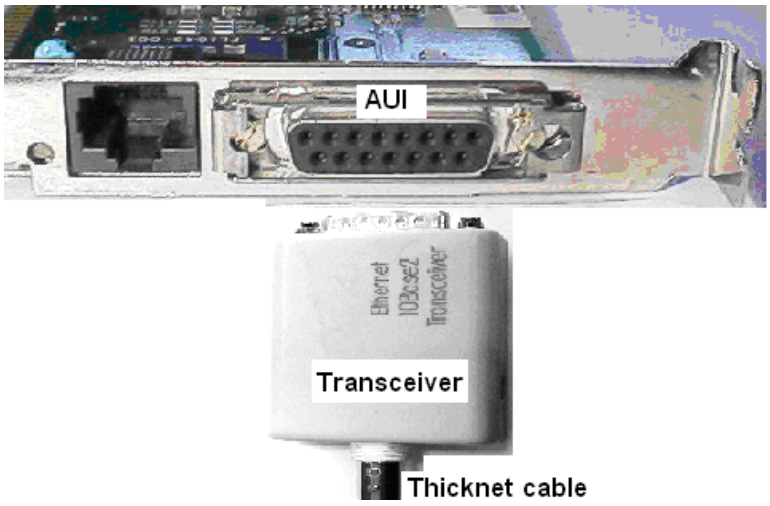
Cách lắp đặt



Hình 3. 5 - Cách lắp đặt hệ thống mạng bằng cáp đồng trục

Ở hình 3.5, mô tả cách lắp đặt một mạng gồm 4 máy tính bằng cáp đồng trục. Mỗi máy tính phải có một card mạng BNC hoạt động tốt. Chữ T dùng để nối card mạng với dây dẫn, vậy cần 4 chữ T. Ba đoạn dây cáp đồng trục mỏng (quy định chống nhiễu chiều dài tối thiểu 0,5m) đã được bấm hai đầu (gọi là đầu BNC) bằng kiềm bấm chuyên dụng, vậy cần 6 đầu BNC. Khi một máy phát tín hiệu, tín hiệu này sẽ lan truyền từ máy đó về hai phía của hệ thống mạng. Khi tín hiệu đến máy cuối cùng thì nó sẽ bị dội ngược trở lại và chắc chắn sẽ gây nhiễu cho toàn mạng. Để triệt tiêu tín hiệu này, ở hai đầu được gắn 2 điện trở (thường là 8 Ω) gọi là terminal, vậy cần 2 terminal.

Muốn kết nối bằng cáp đồng trục dày phải dùng đầu chuyển transceiver thông qua cổng AUI của card mạng.



Hình 3. 6 - Kết nối mạng bằng cáp đồng trục dày

∗ Ưu, khuyết điểm

Ưu điểm: dễ lắp đặt, giá thành rẻ, dễ đi dây.

Khuyết điểm: dễ mất kết nối, không bảo mật, tốc độ không cao.

3.2.2. Cáp xoắn đôi

Cấu tạo

Gồm nhiều cặp dây đồng, mỗi cặp được xoắn lại với nhau nhằm triệt tiêu từ trường của nhau chống nhiễu xuyên kênh. Cáp dùng để kết nối mạng là UTP gồm 4 cặp xoắn đôi có màu như sau:

- Cặp 1: xanh dương - trắng xanh dương.
- Cặp 2: nâu - trắng nâu.
- Cặp 3: xanh lá - trắng xanh lá.
- Cặp 4: cam - trắng cam.

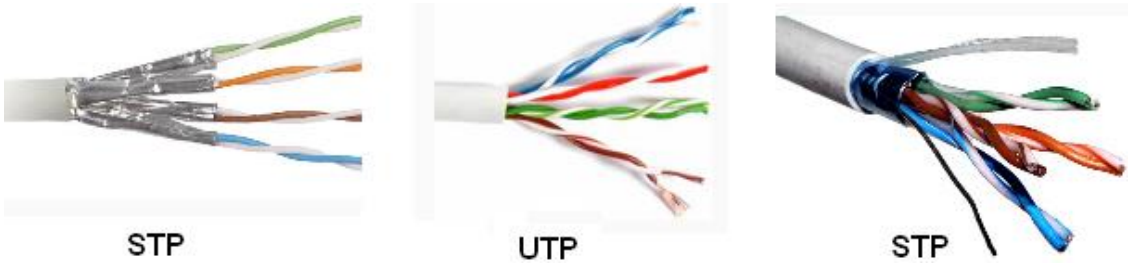
Hình 3. 7 - Cáp xoắn đôi

∗ Các loại cáp xoắn đôi

Cáp STP (có vỏ bọc chống nhiễu): tốc độ tối đa 500 Mbps, khoảng cách 100m.

Cáp UTP (không có vỏ bọc chống nhiễu): tốc độ tối đa 100 Mbps, khoảng cách 100 m.

Cáp FTP: lai tạo giữa STP và UTP: tốc độ tối đa 200 Mbps, khoảng cách 100m.



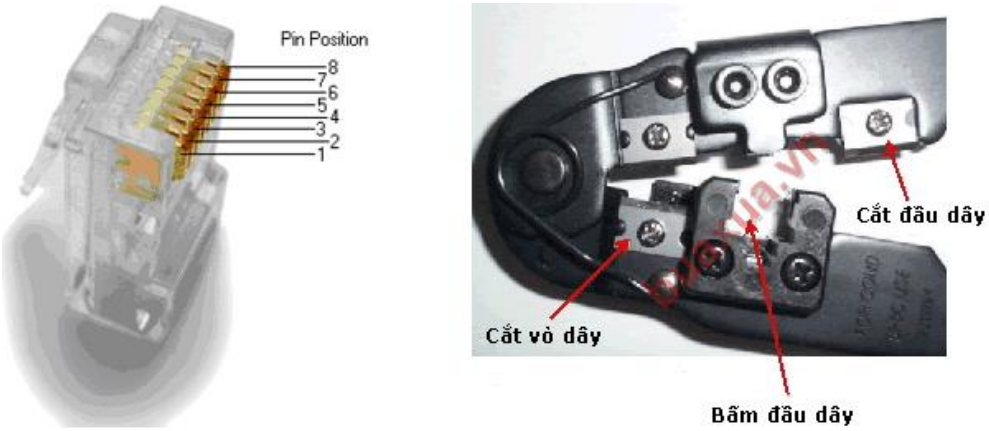
Hình 3. 8 - Các loại cáp xoắn đôi

Tùy theo độ dày của ruột, cáp được phân ra nhiều loại cáp (category): CAT3, CAT4, CAT5, CAT5e, CAT6, CAT6e. CAT5 sử dụng cho tốc độ 10/100 Mbps (100Base), CAT6 cho tốc độ 1000 Mbps (1000Base).

Ngoài ra còn một số loại cáp có hơn 4 cặp cáp dùng để đi âm tường.

∗ Kỹ thuật bấm cáp xoắn đôi

- Đầu bấm RJ45: gồm 8 pin được đánh số 1 đến 8 từ trái qua.



Hình 3. 9 - Đầu bấm và kiềm bấm RJ45

- Đối với chuẩn 100Base: chỉ dùng 2 cặp dây, tốc độ 100 Mbps.
  – Pin 1 (Tx+) và pin 2 (Tx-) dùng để truyền tín hiệu (transmit).
  – Pin 3 (Rx+) và pin 6 (Rx-) dùng để nhận tín hiệu (receive).
- Đối với chuẩn 1000Base: dùng cả 4 cặp dây, tốc độ 1000 Mbps.
  – Pin 1, 2, 4, 5 dùng để nhận tín hiệu (receive).
  – Pin 3, 6, 7, 8 dùng để truyền dữ liệu (transmit).
- Chuẩn 100Base, có 2 chuẩn bấm cáp là T568A và T568B được quy định như sau:
  – T568A: cặp xanh lá dùng để truyền tín hiệu, trắng xanh lá (Tx+) pin 1, xanh lá (Tx-) pin 2. Cặp cam dùng để nhận tín hiệu, trắng cam (Rx+) pin 3, cam (Rx-) pin 6.
  – T568B: ngược lại cặp cam dùng để truyền tín hiệu và cặp xanh lá dùng để nhận tín hiệu. Trắng cam (Tx+), cam (Tx-), trắng xanh lá (Rx+), xanh lá (Rx-).

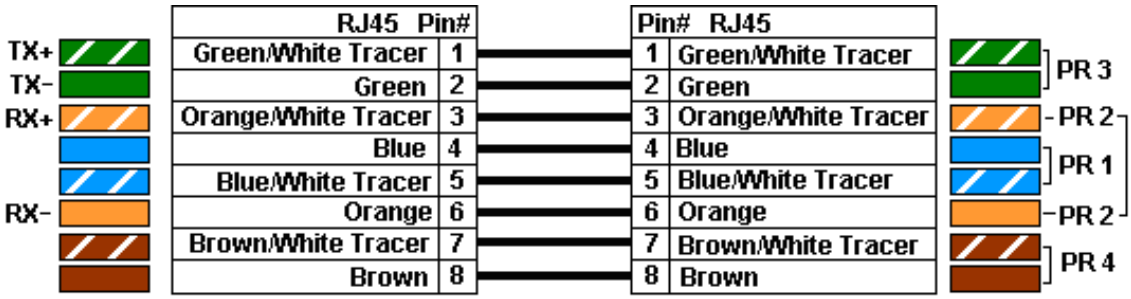
Pin	T568A Color	
1	white/green stripe	Truyền (Tx+)
2	green solid	Truyền (Tx-)
3	white/orange stripe	Nhận (Rx+)
4	blue solid	Không sử dụng
5	white/blue stripe	Không sử dụng
6	orange solid	Nhận (Rx-)
7	white/brown stripe	Không sử dụng
8	brown solid	Không sử dụng

Pin	T568B Color	
1	white/orange stripe	Nhận (Rx+)
2	orange solid	Nhận (Rx-)
3	white/green stripe	Truyền (Tx+)
4	blue solid	Không sử dụng
5	white/blue stripe	Không sử dụng
6	green solid	Truyền (Tx-)
7	white/brown stripe	Không sử dụng
8	brown solid	Không sử dụng

Hình 3. 10 - Cách bấm chuẩn T568A và T568B

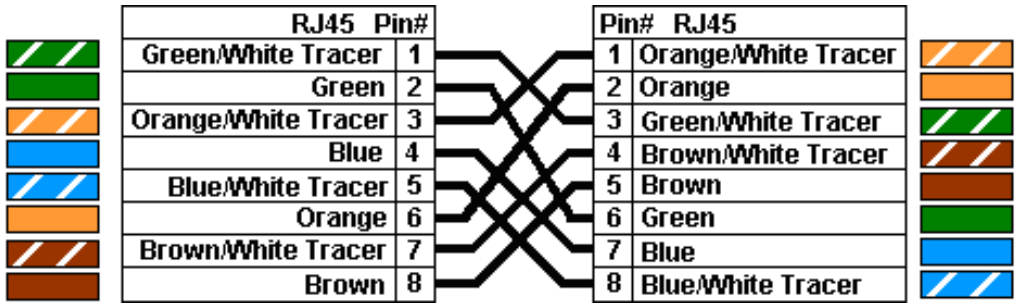
Lưu ý: thuộc lòng nguyên tắc: *một hai ba sáu*.

• Cáp thẳng (Straight-thru cable): là cáp có 2 đầu bấm cùng chuẩn, nếu đầu này là T568A thì đầu kia phải là T568A.



Hình 3. 11 - Cáp RJ45 thẳng

• Cáp chéo (Crossover cable): là cáp có 2 đầu được bấm khác chuẩn, nếu đầu này là T568A thì đầu kia phải là T568B.



Hình 3. 12 - Cáp RJ45 chéo

• Cách dùng cáp: được chia thiết bị mạng làm 3 nhóm:

– Nhóm 1: máy tính và router.

– Nhóm 2: hub và switch.

– Nhóm 3: modem ADSL.

Đối với nhóm 1 và 2, khi nối 2 thiết bị cùng nhóm thì dùng cáp chéo, khi nối 2 thiết bị khác nhóm thì dùng cáp thẳng. ví dụ: nối hai máy tính với nhau dùng cáp chéo, nối máy tính với switch dùng cáp thẳng.

Đối với nhóm 3, dùng cáp thẳng hoặc chéo đều được.

• Cáp Console: dùng để kết nối máy tính với các thiết bị mạng (switch, router...) để cấu hình cho thiết bị đó. Vì đoạn dây này ngắn nên nhiễu không nhiều nên không cần chọn cặp dây xoắn đôi mà quy định cho dễ nhớ: bấm theo màu, ở đầu này 1 đến 8 thì đầu kia ngược lại 8 đến 1.

∗ Ưu khuyết điểm

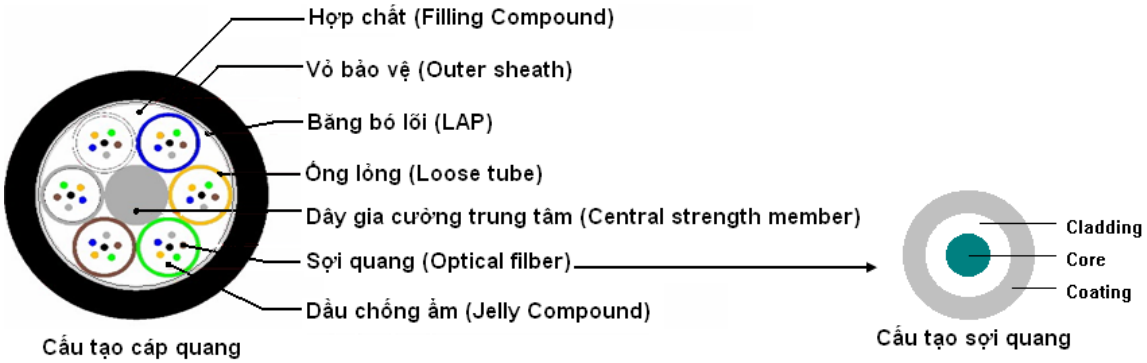
Ưu điểm: rẻ tiền, thông dụng.

Khuyết điểm: thường dùng với mạng hình sao nên rất nhiều dây dẫn gây khó khăn trong việc thiết kế và lắp đặt.

3.2.3. Cáp quang (fiber-optic cable)

∗ Cấu tạo

– Dây dẫn trung tâm là sợi thủy tinh hoặc plastic được tráng bạc để phản xạ ánh sáng vào trong.



Hình 3. 13 - Cấu tạo cáp quang và sợi quang

– Core: trung tâm phản chiếu nơi tín hiệu ánh sáng được truyền đi, có đường kính bằng sợi tóc.

– Cladding: vật chất bao bên ngoài Core để phản xạ ánh sáng vào trong.

– Buffer coating: lớp phủ bảo vệ bên ngoài.

– Jacket: lớp bao bọc nhiều sợi quang thành một bó được gọi là cáp quang.

Các loại cáp quang

– Loại lõi 8.3 micron, lớp lót 125 micron, chế độ đơn.

– Loại lõi 62.5 micron, lớp lót 125 micron, đa chế độ.

– Loại lõi 50 micron, lớp lót 124 micron, đa chế độ.

– Loại lõi 100 micron, lớp lót 140 micron, đa chế độ.

Lắp đặt cáp quang

– bộ chuyển đổi (converter): giữa chuẩn Base-T (cáp xoắn đôi) và Base-FX (cáp quang).

– Đầu nối cáp quang (connector): có rất nhiều loại đầu nối, trên thị trường thường gặp: FT, ST, SC, FC...

Hình 3. 14 - Một số đầu nối cáp quang và converter

– Tủ quang: có thể treo tường hoặc gắn vào tủ rack.

– Dây nhảy quang (patch cord): dùng để nối các thiết bị có cổng quang lại với nhau, ví dụ: máy tính với loa, máy tính với modem ADSL...

– Măng xông quang: dùng để cố định các điểm nối quang tránh sự tác động bên ngoài gây mất kết nối.

Hình 3. 15 - Một số thiết bị dùng để kết nối quang

∗ Ưu khuyết điểm

Ưu điểm: Vì tín hiệu được truyền đi bằng ánh sáng nên băng thông rất lớn lên đến 10 Gbps, không bị nhiễu điện từ và rất khó nghe lén. Do độ suy giảm tín hiệu nhỏ nên khoảng cách rất xa vài Km.

Khuyết điểm: Thiết bị kết nối quang rất đắt tiền, khó lắp đặt.

3.3. Đường truyền vô tuyến

3.3.1. Giới thiệu

Khi thiết kế mạng có những nguyên nhân không nên đi dây hoặc không thể đi dây, giải pháp vô tuyến sẽ giải quyết các bài toán:

- Đối với các mạng tạm thời (hội họp, làm sự kiện...).
- Những nơi công cộng, người dùng di chuyển liên tục (nhà ga, sân bay...).
- Những địa hình không thể đi dây hoặc khoảng cách vượt quá giới hạn dây dẫn.

Nhưng mạng không dây có các khuyết điểm của nó.

- Dễ nhiễu, dễ suy yếu tín hiệu.
- Băng thông không cao.
- Tính bảo mật thấp.

3.3.2. Sóng vô tuyến (Radio)

Sóng Radio nằm trong phạm vi từ 30 Hz đến 300 Ghz, ở dải tần số này có các băng tần được đăng ký sử dụng cho các dịch vụ: FM dùng cho truyền thanh, UHF/VHF dùng cho truyền hình, GMS/CDMA dùng cho điện thoại di động...

Nhưng có một dải tần tự do sử dụng không cần đăng ký, hệ thống mạng thường sử dụng dải tần này để truyền tín hiệu: Bluetooth, Wireless dùng dải tần 2,4 Ghz.

3.3.3. Sóng vi ba

Là sóng có bước sóng siêu ngắn, tần số từ 30 Khz đến 300 Ghz nên có thể truyền đi xa được. Ứng dụng trong việc truyền tín hiệu giữa mặt đất-mặt đất , mặt đất-vệ tinh. Tín hiệu suy yếu do vật cản, thời tiết. Rất dễ nghe lén nên thông tin thường được mã hóa. Ứng dụng trong truyền hình kỹ thật số...

3.3.4. Sóng hồng ngoại

Nằm trong dải tần từ 100 Ghz đến 1000 Ghz có khả năng truyền với tốc độ rất cao từ 1 đến 10 Mbps. Khoảng cách và độ xuyên tường kém.

3.4. Thiết bị mạng

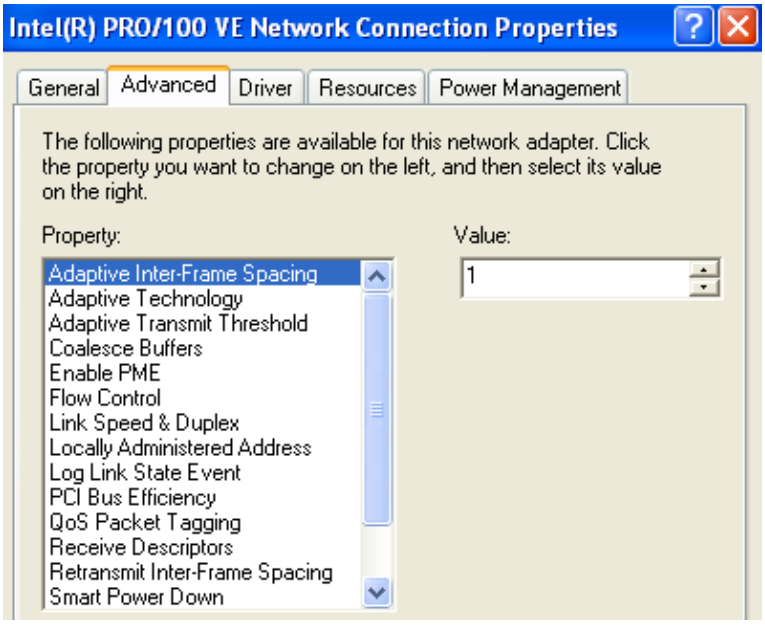
3.4.1. NIC (card mạng)

Là thiết bị giao tiếp giữa máy tính và cáp mạng có thể tích hợp sẵn trên motherboard hay thông qua các khe giao tiếp PCI, PCMCIA... NIC giao tiếp với cáp mạng thông qua các cổng: AUI, BNC, RJ45...

Hình 3. 16 - Một số chuẩn giao tiếp card mạng

∗ Các chức năng chính của NIC.

- Chuyển đổi các Frame dữ liệu thành các bit và truyền trên dây dẫn với tín hiệu điện.
- Kiểm soát luồng, lỗi trong quá trình truyền.
- Kiểm soát lưu lượng, tốc độ và cách thức truyền dữ liệu.

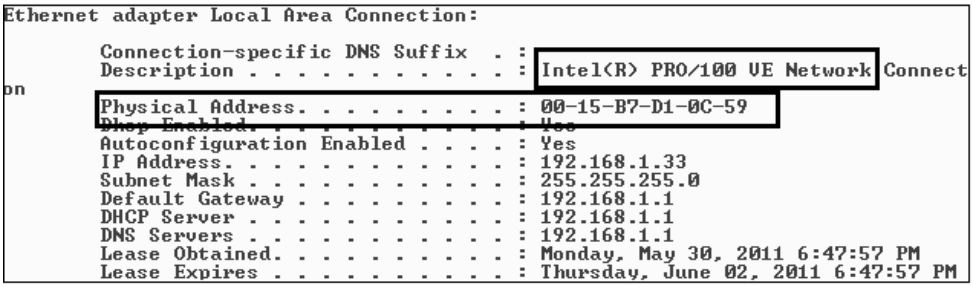


Hình 3. 17 - Các thuộc tính của NIC

Địa chỉ vật lý (MAC) của NIC: để có thể truyền thông tin đến chính xác một máy nào đó, chính là phải truyền thông tin đến một NIC nào đó trên mạng. Như vậy một NIC phải có một địa chỉ và địa chỉ này phải là duy nhất để truy cập mạng gọi là địa chỉ MAC

(địa chỉ vật lý của card mạng). Địa chỉ MAC do IEEE quản lý và cấp cho các nhà sản xuất card mạng.

MAC là một con số gồm 6 byte, được ghi theo ký số thập lục phân. 3 byte đầu là mã nhà sản xuất, 3 byte sau là số serial của nhà sản xuất đánh cho card mạng của mình. Theo nguyên tắc thì địa chỉ này không thay đổi được. Dùng lệnh ***ipconfig /all*** để xem địa chỉ này.



Hình 3. 18 - địa chỉ MAC của card mạng do Intel sản xuất

∗ Giới thiệu một số NIC của hãng Intel.

Capabilities:

Capabilities	Fiber Media	Connector	Full-Height	Low-Profile	1000	100	10	32-bit	64-bit	33	66	100	133	x1 lane slot	x4 lane slot	x8 lane slot	x16 lane slot	
Adapter Model	**Cabling**		**Bracket**		**Speeds**			**Slots**		**PCI / PCI-X**				**PCI Express**				**Controller**
Desktop Adapters																		
Gigabit CT Desktop		RJ-45	X	X	X	X	X							X	X	X	X	82574L
PRO/1000 PT Desktop		RJ-45	X		X	X	X							X	X	X	X	82572GI
PRO/1000 PT Desktop (with low-profile bracket)		RJ-45		X	X	X	X							X	X	X	X	82572GI
PRO/1000 GT Desktop		RJ-45	X		X	X	X	X		X	X							82541PI
PRO/1000 MT Desktop		RJ-45	X		X	X	X	X		X	X							82540EM
PRO/1000 MT Desktop C39226-xxx		RJ-45	X		X	X	X	X		X	X							82541GI
PRO/1000 GTL Desktop		RJ-45		X	X	X	X	X		X	X							82541PI
PRO/1000 MTL Desktop		RJ-45		X	X	X	X	X		X	X							82540EM
PRO/1000 MTL Desktop C36064-xxx		RJ-45		X	X	X	X	X		X	X							82541GI
PRO/1000 T Desktop		RJ-45	X		X	X	X	X		X	X							82544GC
Server Adapters																		
Gigabit EF Dual Port	SX	LC	X	X	X										X	X	X	82576GB
Gigabit ET Dual Port		RJ-45	X	X	X	X	X								X	X	X	82576GB
Gigabit ET Quad Port		RJ-45	X	X	X	X	X								X	X	X	82576GB
Gigabit ET2 Quad Port		RJ-45	X	X	X	X	X								X	X	X	82576GB
I340-F4	SX	LC	X	X	X										X	X	X	82580
I340-T4		RJ-45	X	X	X	X	X								X	X	X	82580
PRO/1000 PF Server	SX	LC	X	X	X										X	X	X	82572GI
PRO/1000 PF Dual Port	SX	LC	X	X	X										X	X	X	82571GB
PRO/1000 PT Server		RJ-45	X	X	X	X	X							X	X	X	X	82572GI
PRO/1000 PT Dual Port		RJ-45	X	X	X	X	X								X	X	X	82571GB
PRO/1000 PT Quad Port		RJ-45	X		X	X	X								X	X	X	82571GB

Hình 3. 19 - Một số thông số của NIC của hãng Intel

Ở hình 3.19, xét các thông số của NIC PRO/1000 GT Desktop. Không có cổng quang, một cổng RJ45, dùng cho case đứng, tốc độ 10/100/1000 Mbps, cắm vào khe 32 bit chuẩn PCI (bus 33 hoặc 66), sử dụng chip 82541PI.

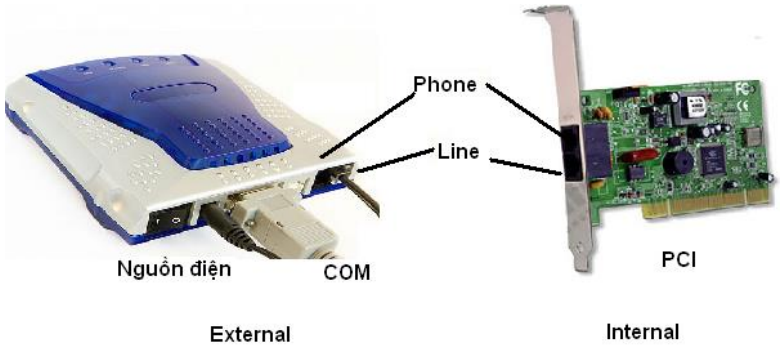
Tương tự NIC dành cho Server, xét PRO/1000 PF Server. Có một cổng quang SX (IEEE 802.3z, multimode), đầu nối quang LC, dùng cho cả case đứng và case nằm, tốc độ 1000 Mbps, gắn vào khe PCI Express x4, x8, x16, sử dụng chip 82572GI.

Hình 3. 20 - Một số NIC của Intel

3.4.2. Modem (Modulation and Demodulation)

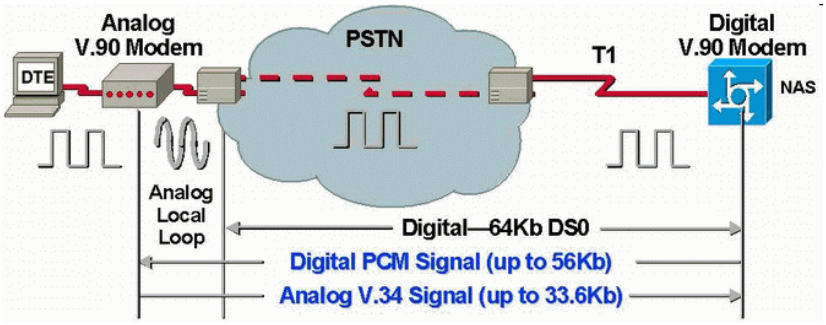
Là thiết bị cho phép kết nối mạng thông qua đường dây điện thoại quay số (dial-up). Thường có 3 cổng:

- Line nối vào đường dây điện thoại bằng đầu nối RJ11
- Phone nối ra điện thoại khi đang kết nối mạng thì không gọi điện thoại được.
- Cổng thứ 3 giao tiếp với máy tính, gắn trong (internal) thường giao tiếp qua khe PCI, gắn ngoài (external) thường giao tiếp qua cổng COM.



Hình 3. 21 - Modem gắn ngoài và modem gắn trong

Modem điều chế (modulation) chuyển tín hiện số (digital) thành tín hiệu tương tự (analog) để truyền đi trên đường dây điện thoại, đó là chiều đi ra. Đối với chiều đi vào modem giải điều chế (demodulation) chuyển tín hiệu analog trên đường dây điện thoại thành tín hiệu digital đưa vào thiết bị mạng.



Hình 3. 22 - DTE sử dụng NAS từ xa thông qua kết nối bằng modem

Ở hình 3.22, một thiết bị đầu cuối DTE kết nối với một hệ thống lưu trữ dữ liệu tập trung qua mạng NAS thông qua đường truyền điện thoại của PSTN và sử dụng 2 modem.

Modem analog V.34 có chuẩn V90 (thường modem có 2 chuẩn V90 và V92). Kết nối DTE với PSTN thông qua đường dây điện thoại thông thường.

Modem digital PCM, chuẩn V90 kết nối NAS với PSTN thông qua một kênh thuê riêng (leased line) T1. Tốc độ của T1 là 1,5 Gbps.

- Chuẩn V90: là sự kết hợp của hai công nghệ K56Flex (công ty Lucent Technologies kế hợp với Rockwell Semiconductor Systems đưa ra) với x2 (của 3COM coporation/US Robotics đưa ra). Sự kết hợp này nâng cao tốc độ truyền và tạo sự tương thích trên toàn thế giới.
- Chuẩn V92: vào năm 2000 ITU đưa ra chuẩn V92 có thêm 3 tính năng vượt trội so với chuẩn V90. Kết nối nhanh gấp đôi, tốc độ upload có thể lên đến 48 Kbps, nhớ số điện thoại và duy trì tham số đường truyền nên không cần kết nối lại khi bị nhiễu.

Với tính năng như vậy, có thể dùng modem kết nối một máy tính ở xa vào mạng nội bộ hoặc nối hai mạng nội bộ ở xa lại với nhau bằng các chương trình hỗ trợ kết nối từ xa. Ví dụ: sử dụng RRAS trong Win2K3.

Ở Việt Nam VNPT tuyên bố "ở đâu có điện thoại, ở đó có Internet". VNPT cung cấp 3 tổng đài kết nối dùng cho 3 dạng khách hàng:

- vnn1260: dùng cho các công ty, có băng thông rộng và phải đăng ký thuê bao. Các công ty sử dụng dịch vụ này để chia sẻ Internet cho toàn công ty. Thường công ty sẽ dành riêng một line điện thoại cho việc kết nối Internet.
- vnn1268: dùng cho cá nhân, có băng thông trung bình và đăng ký sử dụng trả theo dung lượng. Các gia đình sử dụng gói cước này để truy cập mạng thông qua line điện thoại có sẵn.
- vnn 1269: sử dụng rộng rãi, băng thông tùy vào từng thời điểm. Không cần đăng ký, ở đâu có line điện thoại, ở đó có thể kết nối Internet.

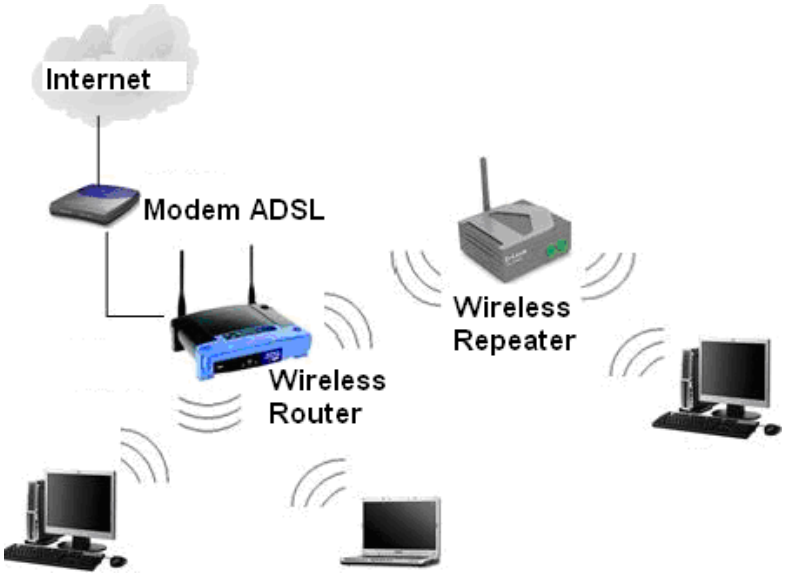
Muốn các máy trong mạng nội bộ có thể truy cập Internet. Máy đang truy cập Internet dùng một chương trình chia sẻ Internet như Wingate để chia sẻ cho tất cả các

máy trong công ty sử dụng. Rất tiện lợi và hiệu quả, nhưng kết nối thông qua đường dây điện thoại thông thường có các khuyết điểm sau:

- Đường dây điện thoại giới hạn tốc độ truyền.
- Khi truy cập Internet (tạo kết nối) thì không thể dùng điện thoại được, vì khi đó cuộc gọi tới VNPT với các số điện thoại 1260, 1269, 1268 đang được kết nối.
- Phải trả tiền thuê bao Internet và cước gọi nội hạt.

3.4.3. Repeater

Là thiết bị làm tươi tín hiệu để có thể truyền đi xa. Nó chỉ làm việc với tín hiệu điện nên khi khuếch đại tín hiệu có thể bị sai và không thể sửa được, vì thế khi thiết kế phải tuân thủ các nguyên tắc kỹ thuật được đưa ra để tránh nhiễu. Hoạt động ở lớp physical trong mô hình OSI cùng với NIC. Nó giúp mở rộng phạm vi của mạng, thường thấy ứng dụng trong các hệ thống WIFI (hotspot) tầm phủ sóng rộng.



Hình 3. 23 - Một hệ thống WIFI sử dụng Repeater

3.4.4. Hub

Là một repeater có nhiều port (cổng). Khi một port nhận tín hiệu, nó làm tươi tín hiệu và truyền đến tất cả các port còn lại. Các port được đánh số thứ tự từ 1 trở đi và có một đèn led để theo dõi kết nối.

Hình 3. 24 - Thiết bị Hub

Thông thường Hub hoạt động ở lớp vật lý trong mô hình OSI, có 3 loại Hub thường gặp:

- Passive Hub: chỉ thuần túy là thiết bị nối cáp, không có nguồn điện nên không xử lý gì cả.
- Active Hub: khuếch đại tín hiệu.
- Intelligent Hub: khuếch đại tín hiệu và chuyển tín hiệu đó đến port cần nhận, không gửi tới các port còn lại. Việc này làm tăng băng thông của mạng và bảo mật.

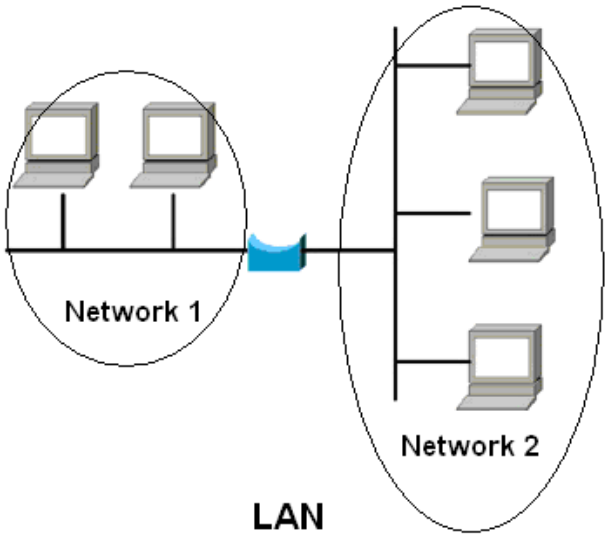
Hub thường hoạt động ở 10 Mbps và bị chia sẻ băng thông khi số lượng port tham gia tăng lên. Hiện nay, kết nối mạng dùng switch thay thế Hub vì tốc độ cao và có nhiều tính năng vượt trội.

3.4.5. Bridge

Là thiết bị dùng để nối 2 nhánh mạng lại với nhau. Khác biệt ở đây là nó hoạt động ở lớp Data Link trong mô hình OSI, nên nó không hiểu được địa chỉ IP và làm việc được với các gói tin. Bridge có một MAC table để lưu lại tất cả các địa chỉ MAC của các máy trên mạng nhờ đó nó chuyển gói tin chính xác đến máy nhận. Các gói tin không mang địa chỉ hợp lệ sẽ bị hủy.

Để cập nhật MAC table, bridge có thể tự học hoặc có thể cài đặt bằng tay. Brigde được sử dụng để tách một nhánh mạng lớn thành nhiều nhánh mạng nhỏ hơn để tăng băng thông của mạng.

Bridge có thể kết nối hai nhánh mạng có kiến trúc khác nhau lại với nhau.



Hình 3. 25 - Bridge nối hai nhánh mạng lại với nhau thành 1 mạng

3.4.6. Switch

Là bridge có nhiều port và nhiều tính năng mở rộng, hoạt động của switch như sau:

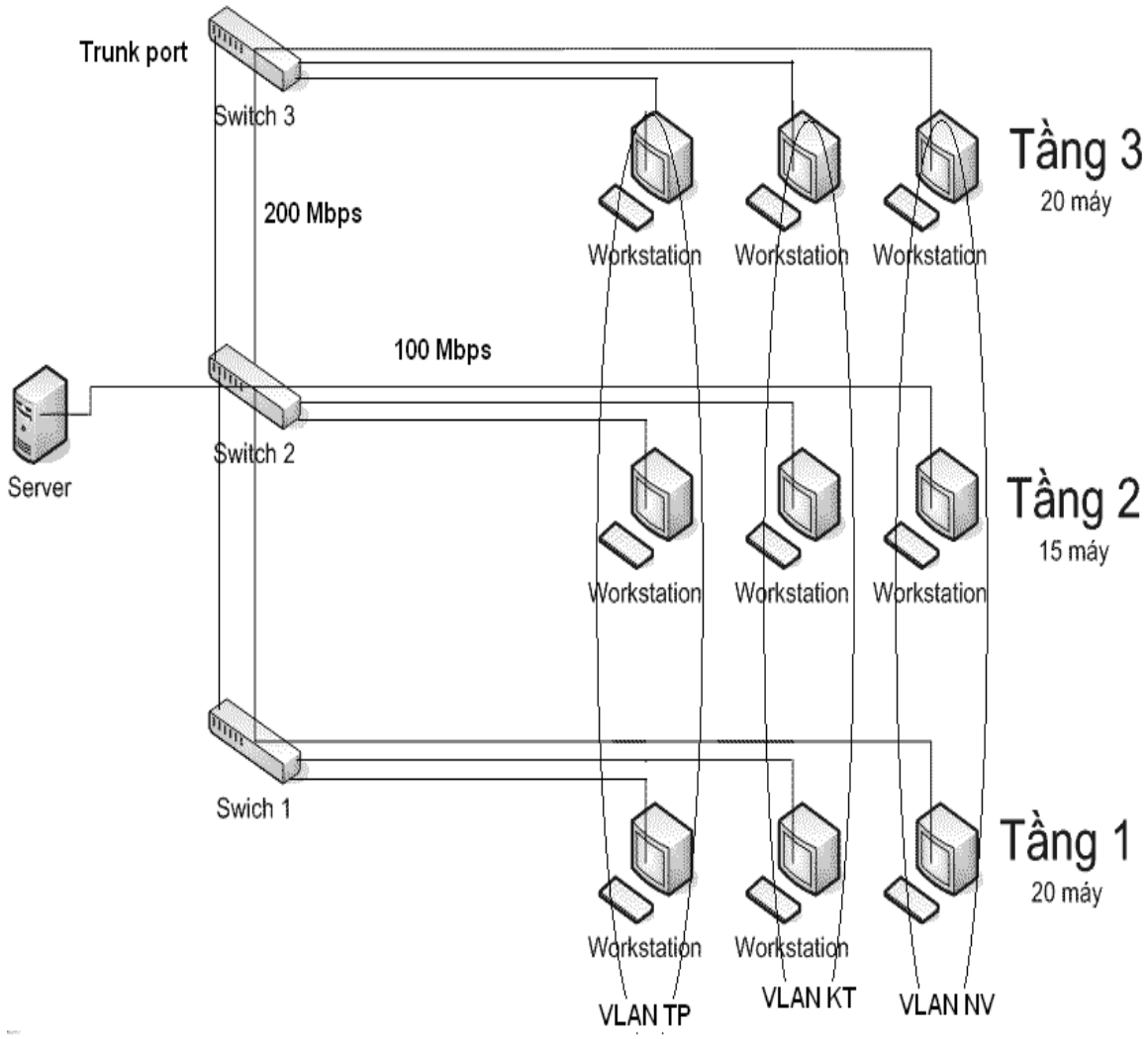
Khi một gói tin đến một port (port nguồn), switch sẽ kiểm tra địa chỉ MAC nguồn của gói tin đó. Nếu địa chỉ này không có trong MAC table của nó, nó sẽ cập nhật địa chỉ này vào MAC table. Đây là cơ chế tự học địa chỉ MAC của switch.

Sau đó nó kiểm tra địa chỉ MAC đích của gói tin. Nếu không có trong bảng MAC của nó, nó sẽ gửi tới tất cả các port còn lại (trừ port nhận). Nếu có trong bảng MAC của nó:

- Hủy gói tin nếu địa chỉ MAC nguồn trùng địa chỉ MAC đích.
- Gửi chính xác đến port đích nếu không trùng.

∗ Các tính năng mở rộng của switch:

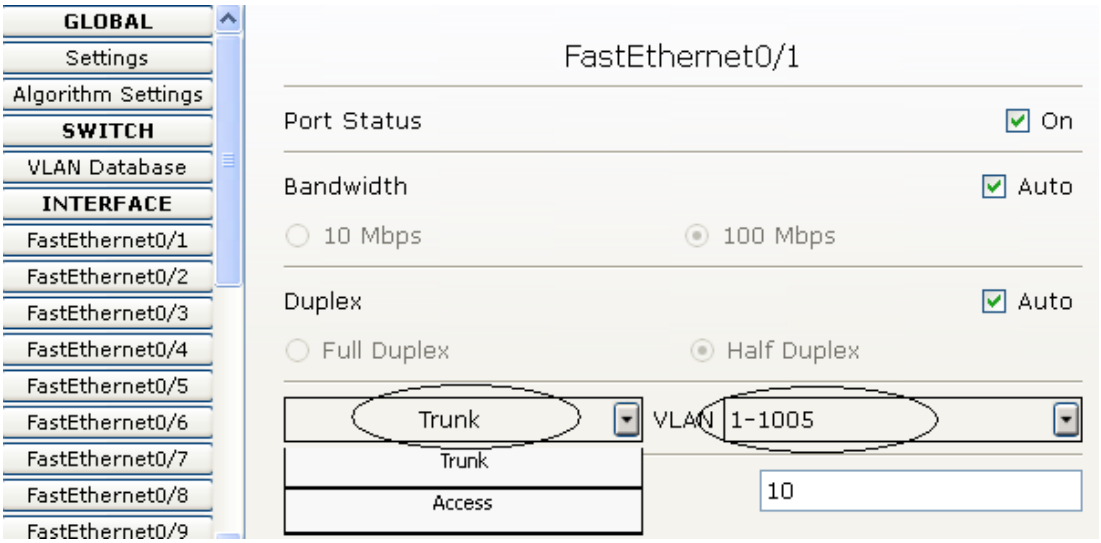
- Stored and Forward: lưu trữ dữ liệu trong bộ đệm trước khi truyền đến port đích. Điều này làm tăng băng thông của mạng và tránh được đụng độ. Với kỹ thuật này switch sẽ nhận đủ gói tin, xử lý nó rồi mới truyền đi. Vậy sự truyền luôn có một độ trễ tùy thuộc và kích thước của frame dữ liệu.
- Cut Through: truyền gói tin ngay tức khắc khi biết địa chỉ đích. Độ trễ ít và là con số chính xác không phụ thuộc vào kích thước frame.
- Trunking: khi một port ở chế độ trunk thì nó cho phép mở rộng băng thông mạng và backup, thông thường sử dụng cho các trục xương sống của mạng (backbone). Đồng thời nó cũng cho phép nhiều mạng ảo dùng chung một đường truyền thật ứng dụng tạo ra các mạng ảo để giảm đụng độ và bảo mật.



Hình 3. 26 - Switch có port trunking

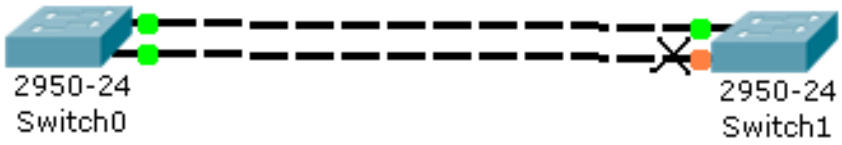
Ở hình 3.26, dùng port trunk để tăng băng thông và backup cho backbone của công ty. Công ty này có 3 tầng lầu vậy phải thiết kế một backbone, các port của switch hoạt động ở 100 Mbps. Khi số lượng máy tăng lên mạng sẽ hoạt động chậm lại, muốn tăng băng thông các port được chuyển sang chế độ trunk và nối song song với nhau. Lúc này 2 dây dẫn là một (point to point) nhưng băng thông tăng lên 200 Mbps.

Vấn đề tiếp theo đặt ra là mỗi phòng ban có một trưởng phòng, phải tạo ra một mạng riêng biệt VLAN TP cho nhóm trưởng phòng để bảo mật. Với hạ tầng có sẵn như vậy, không cần đi dây lại và không cần mua thêm thiết bị nào nữa. Xác định các máy trưởng phòng gắn vào port nào của switch nào (mặc nhiên tất cả đều thuộc VLAN 0) sau đó chuyển các port này về cùng một VLAN. Trong hình có 3 VLAN, vậy các port nối các switch lại với nhau là đường đi chung của cả 3 mạng này nên phải đổi chế độ của các port đó về trunk.



Hình 3. 27 - Cấu hình trunk cho port FastEthernet0/1 trong switch Cisco

Spanning tree: tạo ra một cây bao trùm cho tất cả các đường đi giữa các switch trong mạng nhằm truyền thông tin một cách hiệu quả và tránh việc tạo vòng lặp vô hạn trong khi truyền.



Hình 3. 28 - Spanning tree tạo cây bao trùm.

Ở hình 3.28, nếu nối hai switch như vậy có thể sẽ tạo vòng lặp vô hạn. Nhờ giải thuật Spanning tree sẽ không cho một số port trên switch hoạt động tránh tạo vòng lặp.

Hình 3. 29 - Switch SLM224G4PS của Linksys

Switch LSM224G4PS của Linksys với những tính năng:

- Hỗ trợ cài đặt và cấu hình thiết bị qua giao diện web nhanh chóng.
- Phát triển mạng với những lựa chọn: Stacking, Link Aggregation, Sppaning tree.
- Xác thực qua cổng 802.1x và lọc địa chỉ MAC mang đến sự bảo mật cho tất cả các cổng.
- Hỗ trợ chuẩn IEEE 802.3af cấp nguồn qua PoE tới IP phone, camera giám sát và AP. Cấp nguồn cho 12 cổng (cổng 1 đến 6 và cổng 13 đến 18 qua PoE lên tới 100W).

Switch thông thường sử dụng để tách miền đụng độ trong mạng (mỗi port của nó là một collision domain). Làm giảm miền đụng độ trên mạng, tăng băng thông mạng. Thông thường hoạt động ở lớp Data Link trong mô hình OSI, hiện nay có các switch cao cấp hoạt động ở lớp Network trong mô hình OSI. Hoạt động 10/100/1000 Mbps.

3.4.7. Access point

Là thiết bị kết nối mạng không dây dùng sóng wireless, hoạt động ở băng tần tự do 2.4 Ghz. Có các chuẩn IEEE 802.11A/B/G/N... hiện nay hay sử dụng chuẩn B (tốc độ 54 Mbps) và chuẩn N (tốc độ 150 Mbps). Có 3 dạng kết nối:

- Adhoc: máy tính với máy tính.
- Infrastructure I: máy tính với access point.
- Infrastructure II: access point với access point.

∗ Access point còn có thêm một số tính năng:

- Bảo mật mã hóa WEP, WPA...
- Bảo mật che dấu SSID của mình.

Hình 3. 30 - Access point WAP610N

Access point WAP610N với những tính năng:

- Ăng ten được thiết kế nằm trong.
- Thiết bị không giây chuẩn N.
- Có thể hoạt động ở 2 dải tần làm tăng khả năng mở rộng hệ thống mạng.
- Được thiết kế để giảm thiểu sự ngắt quãng khi xem video qua mạng không giây.

3.4.8. Router

Dùng để định tuyến cho một gói tin chạy trên mạng, nó xác định đường đi tối ưu cho các gói tin từ mạng này sang mạng khác. Mỗi port của router là một mạng riêng biệt. Trong router có một bảng định tuyến mà ở đó có đường đi đến các mạng khác nhau, có một cổng mặc định (default gateway) khi không biết đường đi đến một mạng ở xa router gửi gói tin qua cổng này.

Bảng định tuyến được cập nhật động (dynamic) bằng cách học từ các router láng giềng hoặc được cài đặt tĩnh (static). Router hoạt động ở lớp Network trong mô hình OSI.

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.33      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.33    192.168.1.33      20
     192.168.1.33  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.1.255  255.255.255.255    192.168.1.33    192.168.1.33      20
      192.168.3.0    255.255.255.0    192.168.3.1     192.168.3.1       20
      192.168.3.1  255.255.255.255      127.0.0.1       127.0.0.1       20
    192.168.3.255  255.255.255.255    192.168.3.1     192.168.3.1       20
    192.168.121.0    255.255.255.0  192.168.121.1   192.168.121.1       20
    192.168.121.1  255.255.255.255      127.0.0.1       127.0.0.1       20
  192.168.121.255  255.255.255.255  192.168.121.1   192.168.121.1       20
        224.0.0.0        240.0.0.0    192.168.1.33    192.168.1.33      20
        224.0.0.0        240.0.0.0    192.168.3.1     192.168.3.1       20
        224.0.0.0        240.0.0.0  192.168.121.1   192.168.121.1       20
  255.255.255.255  255.255.255.255    192.168.1.33    192.168.1.33      1
  255.255.255.255  255.255.255.255    192.168.1.33                4     1
  255.255.255.255  255.255.255.255    192.168.3.1     192.168.3.1       1
  255.255.255.255  255.255.255.255  192.168.121.1   192.168.121.1       1
Default Gateway:       192.168.1.1
```

Hình 3. 31 - Dùng lệnh route print trong Windows để xem bảng định tuyến

Lưu ý: dùng lệnh *rout print* để xem bảng định tuyến và default gateway trong Windows

Ở hình 3.31 dòng số 3, nếu muốn đi đến mạng 192.168.1.0/24 thì đi qua cổng 192.168.1.33 với độ ưu tiên là 20 (càng nhỏ càng ưu tiên). Cổng mặc định là 192.168.1.1.

Hình 3. 32 - Router 2800 của Cisco

3.4.9. Gateway (Proxy)

Là thiết bị có khả năng nối hai mạng hoạt động ở hai giao thức khác nhau. Nó nối mạng máy tính bên trong (dùng giao thức IP) với các mạng bên ngoài như mạng điện thoại, mạng vệ tinh... Thiết bị VoiIP dùng để gọi điện thoại với một thuê bao quay số thông qua mạng IP. Đồng thời nó có thêm một số chức năng quản lý các luồng dữ liệu, chia sẻ truy cập Internet, bảo mật mạng...

VoIP gateway Draytek V3300V

- Cân bằng tải & Security Broadband Router
- Thiết Bị Voip - 8 cổng FXS nội điện thoại bàn voi hoặc BPX
- 4 cổng WAN kết nối với router ADSL 4, cân bằng tải & liên kết dự phòng.
- 4 cổng LAN 10/100Mbps với VLAN
- VPN sever với 200 VPN / IPsec đường hầm,
- 1 cổng điều khiển nối tiếp RS232. Riêng LAN-side & DMZ Port (10/100BaseT)
- Quản lý băng thông và QoS Chức năng. Dynamic DNS, multi-NAT, ..
- Tường lửa bảo mật với NAT, DoS & DDoS, DMZ, Packet Filtering, nhiều mạng con, Hạn chế truy cập, ...

Secure quản lý từ xa, SNMP Agent với MIB-II

Hình 3. 33 - Gateway VoIP V3300V của Draytek

3.5. Câu hỏi và bài tập

1. Vẽ hình và mô tả cách bấm cáp mạng RJ45 tốc độ 1000 Mbps theo hai chuẩn T568A và T568B?
2. Hãy cho biết dải tần số của sóng viba, sóng hồng ngoại, sóng wireless và sóng bluetooth?
3. Trình bày địa chỉ vật lý MAC của card mạng, trong Windows dùng lệnh gì để xem địa chỉ MAC?
4. So sánh nguyên lý hoạt động của Hub và switch?
5. Trình bày chức năng của kỹ thuật trunking và spanning tree, kỹ thuật này được sử dụng trong thiết bị nào?
6. Trình bày ý nghĩa các cột trong bảng định tuyến, trong Windows dùng lệnh gì để xem bảng định tuyến?
7. Hãy kể tên một số thiết bị mạng, hãng sản xuất, chức năng của nó?
8. Hãy cho biết ý nghĩa thông số kỹ thuật của hai card mạng trong bảng sau?

Capabilities	Fiber Media	Connector	Full-Height	Low-Profile	1000	100	10	32-bit	64-bit	33	66	100	133	x1 lane slot	x4 lane slot	x8 lane slot	x16 lane slot	
Adapter Model	**Cabling**		**Bracket**		**Speeds**			**Slots**		**PCI / PCI-X**				**PCI Express**				**Controller**
PRO/1000 MT Desktop C39226-xxx		RJ-45	X		X	X	X	X		X	X							82541GI
I340-T4		RJ-45	X	X	X	X	X								X	X	X	82580

9. Khi số lượng máy trong công ty gia tăng, mạng hoạt động chậm lại. Hãy đưa ra một số giải pháp đã học để cải thiện băng thông mạng.

CHƯƠNG 4 - CÁC KIẾN TRÚC VÀ CHUẨN MẠNG

∗ Tóm tắt nội dung chương 4

- Các khái niệm, đặc tính, cấu tạo, và ưu khuyết điểm của các kiến trúc mạng và chuẩn mạng.

∗ Mục tiêu chương 4

Sau khi học xong sinh viên có khả năng:

- Trình bày được các khái niệm, đặc tính, cấu tạo, ưu khuyết điểm của các kiến trúc mạng và các chuẩn mạng.
- Nêu ra các thông số cho từng loại chuẩn mạng.

3.6. Khái niệm

Kiến trúc mạng (network topology) là sơ đồ vật lý của các thiết bị mạng và phương tiện truyền dẫn. Có hai kiểu kiến trúc mạng chính.

- Kiến trúc vật lý: sự sắp xếp hình học của các nút mạng và các dây dẫn.
- Kiến trúc logic: mô tả đường đi thật sự của dữ liệu qua các nút mạng.

3.7. Các kiến trúc mạng chính

3.7.1. Mạng Bus (tuyến)

Các thiết bị mạng nối với nhau thành một hàng thông qua một dây dẫn. Trước đây cách nối này rất thông dụng, nhưng do các khuyết điểm của nó nên hiện nay ít sử dụng. Khi một máy truyền dữ liệu, tín hiệu lan truyền về hai đầu đoạn cáp nên tất cả các máy đều nhận được. Máy nào thấy dữ liệu của mình thì nhận.

Khi tín hiệu truyền đến 2 đầu của đoạn cáp, tín hiệu sẽ bị triệt tiêu bằng một terminal (thường là điện trở 8 Ω) để tránh trường hợp tín hiệu dội ngược lại gây nhiễu.

Hình 4. 1- Kiến trúc mạng Bus

Ưu điểm:

- Rất ít dây, dễ lắp đặt, rẻ tiền.
- Dễ dàng thêm máy và mở rộng mạng bằng repeater.

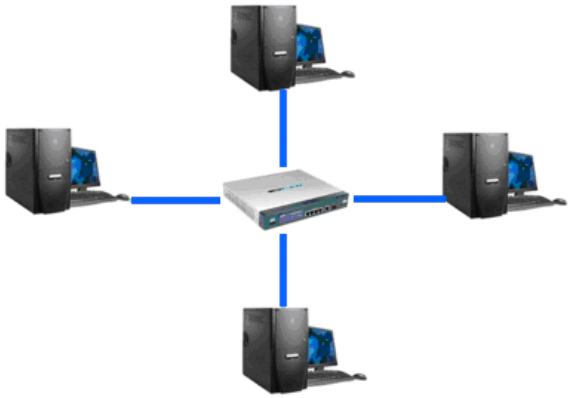
Khuyết điểm:

- Dễ mất kết nối (một máy làm mất kết nối gây ảnh hưởng toàn mạng), dễ bị nhiễu.

- Sử dụng chung đường truyền nên băng thông giảm đáng kể khi số lượng máy tăng lên.

3.7.2. Mạng Star (sao)

Tất cả các thiết bị mạng được nối với thiết bị trung tâm (Hub hoặc switch). Khi một máy truyền tín hiệu đến, thiết bị trung tâm sẽ khuyết đại tín hiệu và truyền đi.



Hình 4. 2 - Kiến trúc mạng Star

Ưu điểm:

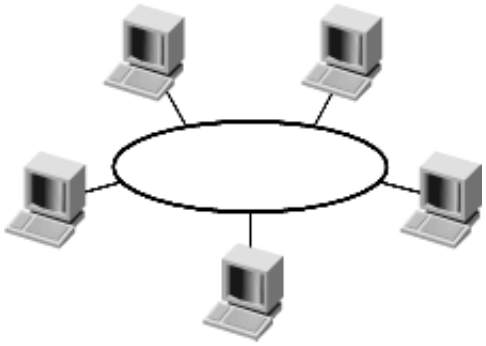
- Các máy độc lập không gây ảnh hưởng lẫn nhau. Cấu trúc này cho phép mở rộng và thu hẹp mạng một cách dễ dàng.

Khuyết điểm:

- Mỗi máy cần một cặp dây nối với thiết bị trung tâm nên phải tính toán nơi đặt thiết bị trung tâm, dây rất nhiều.
- Khi thiết bị trung tâm ngưng hoạt động, toàn mạng cũng ngưng hoạt động.

3.7.3. Mạng Ring (vòng)

Các thiết bị mạng được nối với nhau thành một vòng khép kín. Các máy tính truyền tính hiệu theo một chiều nhất định dựa vào một thẻ bài (Token-ring). Thẻ bài truyền đi lần lượt trên mạng, thiết bị nào giữ thẻ bài thì được truyền dữ liệu, không có dữ liệu truyền hoặc truyền xong thì chuyển thẻ bài cho thiết bị kế tiếp. Mạng này thường được sử dụng cáp quang.



Hình 4. 3 - Kiến trúc mạng Ring

Ưu điểm:

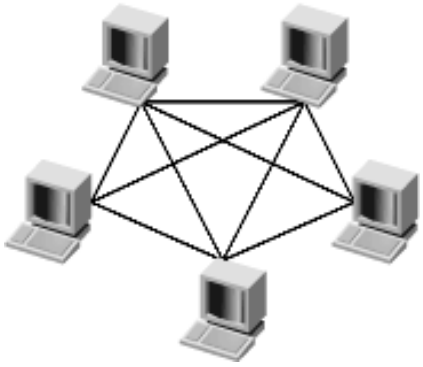
- Mỗi lúc chỉ có một máy truyền nên không đụng độ, quyền ưu tiên truyền trên mạng giống nhau không phụ thuộc vào tốc độ máy.
- Ít bị giảm băng thông khi số lượng máy tăng lên. Mỗi trạm đạt tốc độ truy cập tối đa.

Khuyết điểm:

- Khi một trạm bị ngưng toàn bộ hệ thống bị ngưng, thông thường dùng hai vòng chạy ngược nhau để cân bằng tải và backup.

3.7.4. Mạng Mesh (lưới)

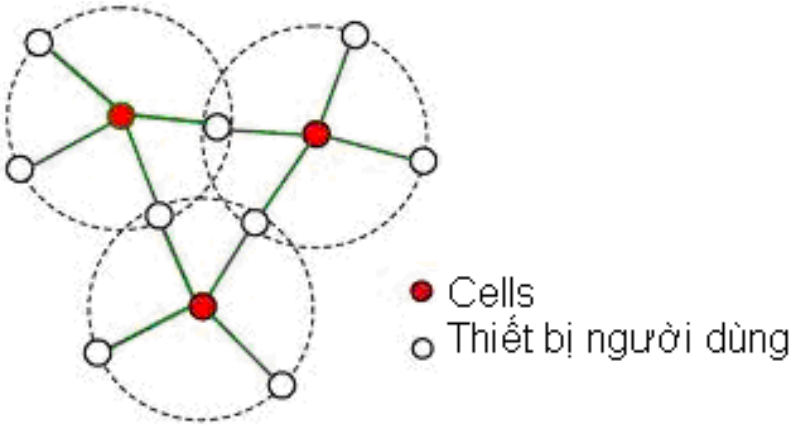
Các thiết bị kết nối với nhau, khi số lượng thiết bị gia tăng thì số lượng kết nối cũng gia tăng. Thường thì mạng này xuất hiện khi các máy tự kết nối với nhau vào mạng chứ ít khi sử dụng kiến trúc mạng này.



Hình 4. 4 - Kiến trúc mạng Mesh

3.7.5. Mạng Cellular (tế bào)

Các thiết bị mạng nằm trong khu vực địa lý của cell (trung tâm kết nối mạng) nào thì kết nối với cell đó. Các cell được nối với nhau thành một mạng. Kết nối này thường dùng sóng radio để kết nối, thường dùng trong mạng điện thoại hoặc trạm phát WIFI.

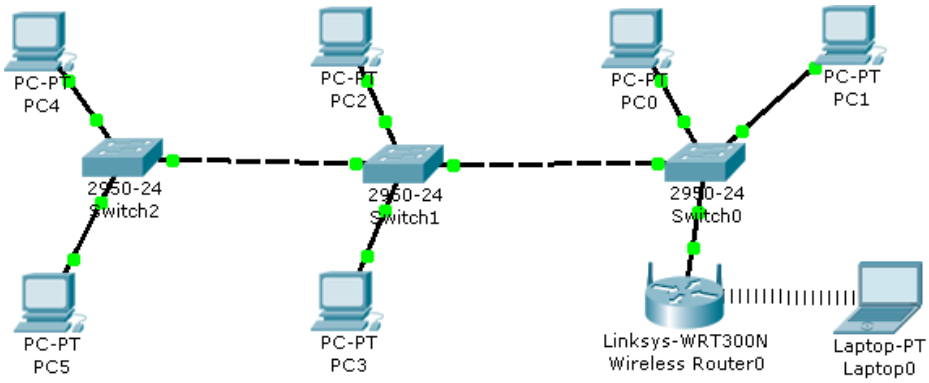


Hình 4. 5 - Kiến trúc mạng Cellular

3.8. Các kiến trúc mạng kết hợp

3.8.1. Mạng Star bus

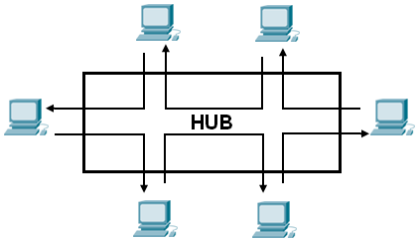
Các mạng Star được nối với nhau qua một mạng Bus. Kiến trúc này hay gặp khi đi mạng trong một tòa nhà nhiều tầng. Ở mỗi tầng là một mạng Star, nối các tầng lại với nhau bằng một backbone (trục xương sống). Cũng có thể gặp khi nối các tòa nhà lại với nhau.



Hình 4. 6 - Kiến trúc mạng Star bus

3.8.2. Mạng Star ring

Các máy trong mạng nối vòng với nhau thông qua một thiết bị trung tâm. Điều này khắc phục được các nhược điểm của hai mạng Star và Ring.



Hình 4. 7 - Kiến trúc mạng Star ring

3.9. Các chuẩn mạng Ethernet

3.9.1. Ethernet

Vào năm 1973 Robert Metcalfe thuộc trung tâm nghiên cứu Palto Alto của hãng Xerox đưa ra ý tưởng cho phép các máy tính và máy in trao đổi dữ liệu không thông qua máy chủ (Mainframe). Đến năm 1980 chuẩn DIX Ethernet ra đời (do DEC, Intel và Xerox sản xuất) với tốc độ 10Mbps. Ủy ban 802.3 của IEEE lấy chuẩn này để nghiên cứu, tuy đến nay không sử dụng nhưng IEEE802.3 được xem là chuẩn của Ethernet.

Các đặc điểm của Ethernet:

Hoạt động ở lớp Data Link trong mô hình OSI, làm việc với các khung dữ liệu.

Preamble 7 bytes	SFD 1 byte	DA 6 bytes	SA 6 bytes	Length 2 bytes	LLC 3 bytes	Data+pad 43—1497 bytes	FCS 4 bytes

Hình 4. 8 - Cấu trúc khung Ethernet

- Preamble: trường này đánh dấu sự xuất hiện khung bit, nó luôn mang giá trị 10101010. Từ nhóm bit này, phía nhận tạo ra xung nhịp 10Mhz.
- SFD (Start Frame Delimiter): trường này thực sự xác định sự bắt đầu của một khung, nó luôn mang giá trị 10101011
- DA (Destination Address): địa chỉ trạm đích.
- SA (Source Address): địa chỉ trạm nguồn.
- Length: độ dài dữ liệu mà khung mang theo.
- FCS, CRC (Cyclic Redundancy Checksum): dùng để tính toán kiểm tra, nếu FCS khác CRC thì khung dữ liệu bị lỗi. Có thể dùng các bit kiểm tra để phục hồi lỗi hoặc truyền lại.

Dùng địa chỉ MAC, gồm 6 byte (hệ thập lục). 00-15-B7-D1-0C-59 (một MAC của Intel). Là địa chỉ duy nhất được ghi chết trong ROM của NIC (không thay đổi được).

- 3 byte đầu là mã nhà sản xuất card giao tiếp Ethernet (do IEEE cấp).
- 3 byte sau là serinumber của sản phẩm.

Có 3 loại khung Ethernet:

- Khung Unicast: truyền đến một trạm duy nhất. Khung được tạo ra với một địa chỉ MAC nguồn và một địa chỉ MAC đích. Khung này gởi lên toàn mạng nhưng chỉ có trạm có MAC trùng với MAC đích của khung mới xử lý khung này, các trạm còn lại bỏ qua.
- Khung Broadcast: truyền cho tất cả các máy trên mạng. Địa chỉ MAC đích của khung là FF-FF-FF-FF-FF-FF, khi các trạm nhận được khung này bắt buộc phải xử lý nó.
- Khung Multicast: truyền đến một số trạm xác định trong nhóm Multicast. Địa chỉ MAC đích là một địa chỉ đặc biệt, chỉ có các máy cùng nhóm mới chấp nhận khung dữ liệu này.

Dùng cơ chế CSMA/CD để truy cập đường truyền.

- Khi một máy muốn truyền, nó cảm sóng mang xem đường truyền có rảnh không, nếu rảnh nó chờ một khoản thời gian IFG và bắt đầu truyền. Nếu truyền nhiều khung thì khoảng cách hai khung là IFG.
- Nếu đường truyền bận thì tiếp tục lắng nghe.
- Nếu 2 trạm cùng truyền đồng thời sẽ xảy ra đụng độ, trạm tiếp tục truyền hết 32 bit. Khi truyền xong 32 bit trạm sẽ chờ một khoảng thời gian ngẫu nhiên và truyền lại. Nếu vẫn bị đụng độ, trạm sẽ chờ trong khoảng thời gian dài hơn. Nếu trạm truyền hết 512 bit, lúc này xem như trạm đã chiếm đường truyền (thời gian này này gọi là SlotTime). SlotTime là thời gian mà chắc chắn rằng các máy xa nhất trên mạng nhận được tín hiệu và phát hiện đường truyền đang bận.

• IFG (Interfame gap) gọi là khoảng trống liên khung bằng 96 lần thời gian của một bit:

– Ethernet 10Mbps: IFG = 9,6 µs
– Ethernet 100Mbps: IFG = 960 ns
– Ethernet 1000Mbps: IFG = 96 ns

Dùng kiến trúc Bus hoặc Star.

Tốc độ tuyền 10/100/1000 Mbps.

Sử dụng cáp thinnet, thicknet, UTP.

3.9.1.1. Các chuẩn Ethernet tốc độ 10 Mbps

3.9.2. 10Base5

• Là tiêu chuẩn Ethernet đầu tiên.

• Khoảng cách tối đa 500 m, tối thiểu 2,5 m, toàn bộ chiều dài mạng không vượt quá 2500 m.

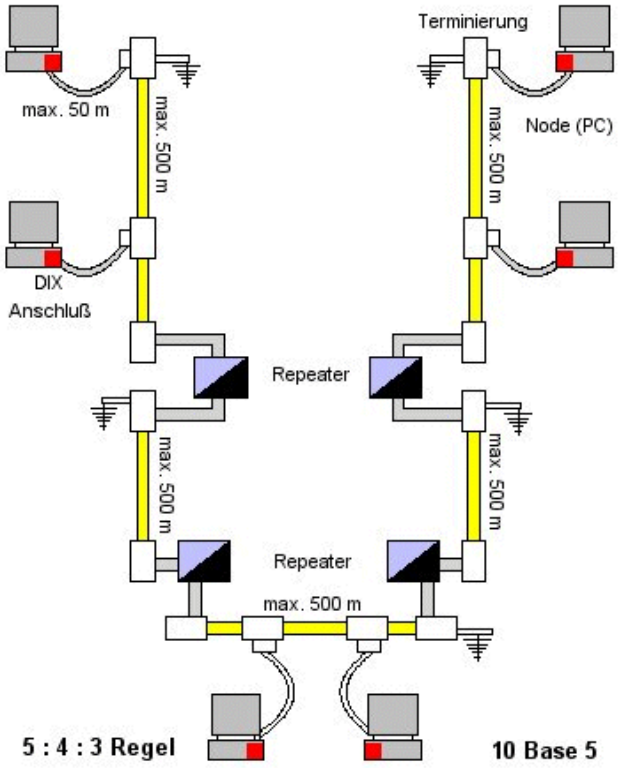
• Dùng cáp thicknet, tốc độ 10 Mbps, dùng băng tầng cơ sở.

• Cáp thu phát (tranceiver cable), nối từ máy tính đến trạm thu phát, có chiều dài tối đa 50 m.

• Số nút tối đa cho 1 phân đoạn mạng là 100 (kể cả máy tính và repeater).

• Thiết bị đầu cuối (terminator) phải nối đất.

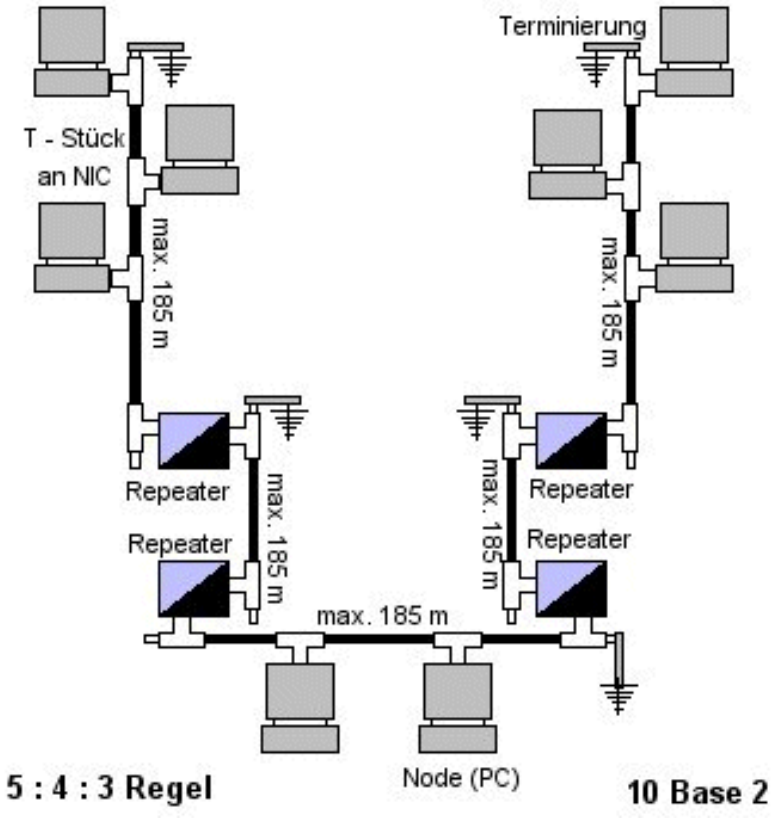
• Tuân theo quy tắc 5-4-3: 5 đoạn cáp, 4 bộ chuyển tiếp, chỉ có 3 đoạn được nối máy trạm.



Hình 4. 9 - Ethernet 10Base5

3.9.3. 10Base2

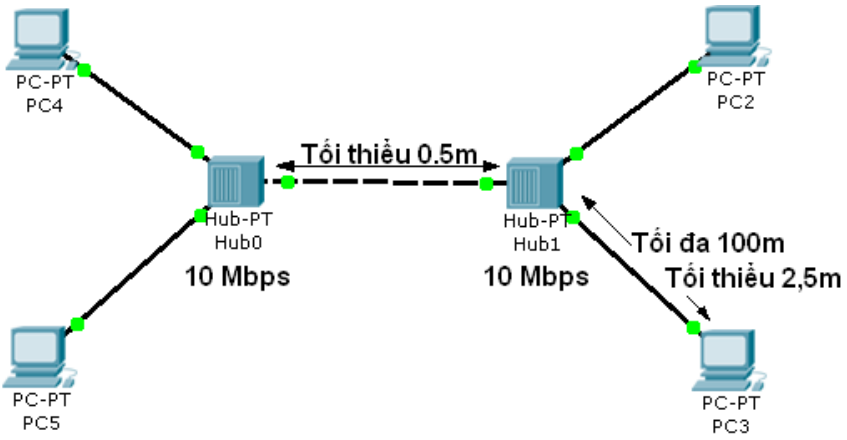
- Khoảng cách tối đa 1 phân đoạn mạng là 185 m (IEEE làm tròn thành 200 m), tối thiểu 0,5 m, toàn bộ chiều dài mạng không vượt quá 925 m.
- Dùng cáp thinnet, đầu nối chữ T, tốc độ 10 Mbps, dùng băng tần cơ sở.
- Số nút tối đa cho một phân đoạn mạng là 30.
- Trở kháng 50 Ω và được nối đất.
- Tuân theo nguyên tắc 5-4-3.



Hình 4. 10 - Ethernet 10Base2

3.9.4. 10BaseT

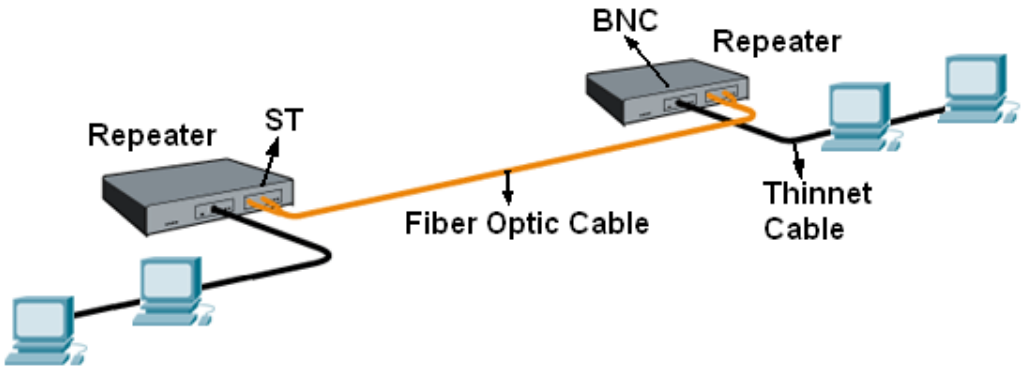
- T là viết tắt của twisted-pair (cáp xoắn đôi).
- Khoảng cách tối đa 100 m, tối thiểu 2,5 m.
- Dùng cáp UTP 3,4,5 hoặc STP, đầu nối RJ45, tốc độ 10 Mbps, dùng băng tần cơ sở.
- Số nút tối đa 512, số lượng máy tối đa 1024.
- Dùng kỹ thuật IEEE802.3, kiến trúc mạng Star có thể nối các phân đoạn mạng 10BaseT bằng cáp đồng trục hay cáp quang.
- Dùng thiết bị trung tâm Hub, khoảng cách tối thiểu các Hub là 0,5 m.



Hình 4. 11 - Ethernet 10BaseT

3.9.5. 10BaseFL

- F là viết tắt của Fiber-Optic (sợi quang), ra đời năm 1993.
- Khoảng cách tối đa 2 Km.
- Dùng cáp quang, tốc độ 10 Mbps, dùng băng tần cơ sở.
- Số nút tối đa lớn hơn nhiều so với 10Base2, 10Base5.

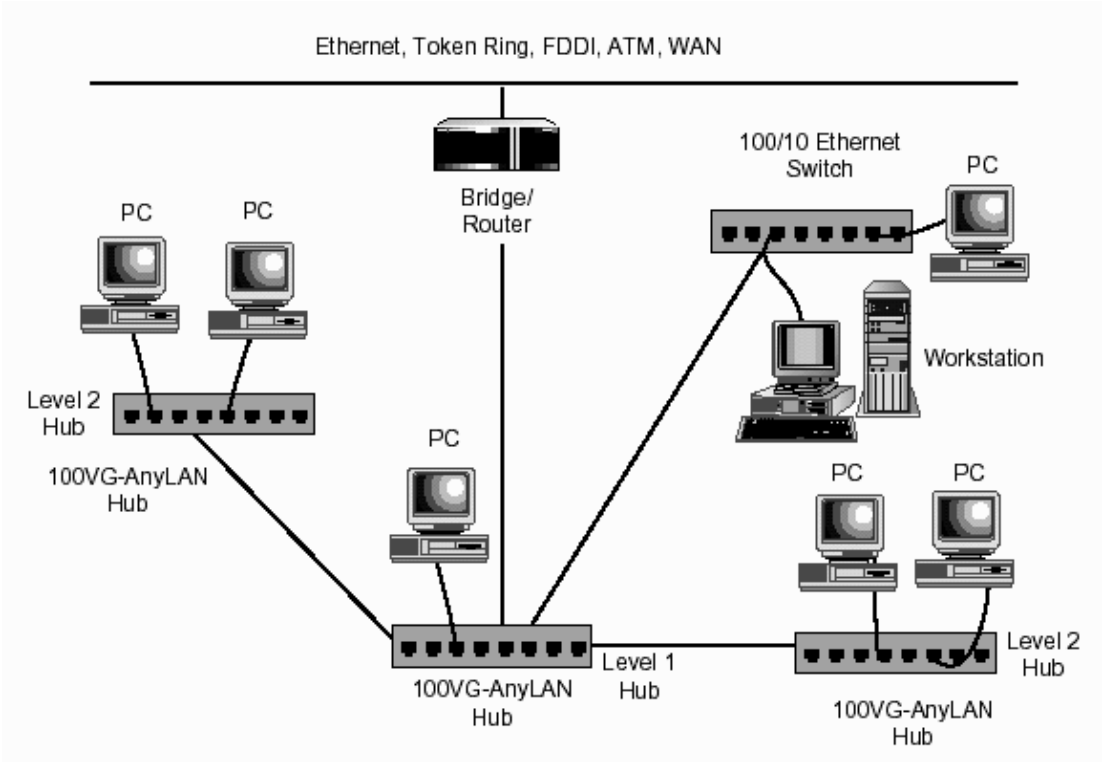


Hình 4. 12 - Ethernet 10Base-FL

3.9.5.1. Các chuẩn Ethernet tốc độ 100 Mbps

3.9.6. 100VG-anyLAN

- Là sự kết hợp Ethernet và Token Ring.
- Dùng cáp UTP (3,4,5), STP hoặc cáp quang. Tốc độ tối thiểu 100 Mbps.
- Dùng kỹ thuật IEEE802.12, chấp nhận cả khung Ethernet và gói Token-Ring.
- Sử dụng Hub, có thể mở rộng mạng bằng cách nối thêm Hub con, khoảng cách tối đa giữa hai Hub là 250 m.



Hình 4. 13 - Ethernet 100BaseVG-anyLAN

3.9.7. 100BaseX

Là mở rộng của Ethernet còn gọi là Fast Ethernet, chữ X nói đến đặc tính mã hóa đường truyền (phương pháp mã hóa 4B, 5B). Tốc độ 100 Mbps, bao gồm 3 chuẩn:

- 100BaseT4: dùng cáp UTP (3,4,5), 4 cặp xoắn đôi.
- 100Base TX: dùng cáp UTP (3,4,5) , STP hai cặp xoắn đôi.
- 100Base FX: dùng cáp quang gồm 2 sợi (lõi).
- 100BaseT
- Sử dụng cáp xoắn đôi lẫn cáp quang, tốc độ 100 Mbps.

Chuẩn	Loại cáp	Chiều dài tối đa	Đầu nối
10Base2	Thinnet	185m	BNC
10Base5	Thicknet	500m	AUI
10Base-T	UTP cat 3-4-5, 2 cặp dây	100m	RJ45
100Base-TX	UTP cat 5, 2 cặp dây	100m	RJ45
100Base-FX	Cáp quang Multimo lõi 62.5 hoặc 125 µm	400m	MIC, ST, SC
1000Base-CX	STP	25m	RJ45
1000Base-T	UTP cat 5, 4 cặp dây	100m	RJ45
1000Base-SX	Cáp quang Multimode lõi 62.5 hoặc 50 µm	62.5µm → 275m 50 µm → 550m	SC
1000Base-LX	Cáp quang Multimode, lõi 62.5 hoặc 50µm Cáp quang Singlemode, lõi 9 micro	62.5 micro → 440m 50 micro → 550m 9 micro → 3-10Km	SC

Hình 4. 14 - Tổng hợp chuẩn Ethernet

3.9.7.1. Các chuẩn Ethernet tốc độ 1000 Mbps

3.9.8. 1000BaseX

Mã hóa bằng phương pháp 8B/10B, dùng hệ thống kết nối tốc độ cao fiber channel, được phát triển bởi ANSI. Gồm có 3 loại:

- 1000Base-SX: tốc độ 1000 Mbps, sử dụng sợi quang, sóng ngắn.
- 1000Base-LX: tốc độ 1000 Mbps, sử dụng sợi quang, sóng dài.
- 1000Base-CX: tốc độ 1000 Mbps, sử dụng cáp đồng.

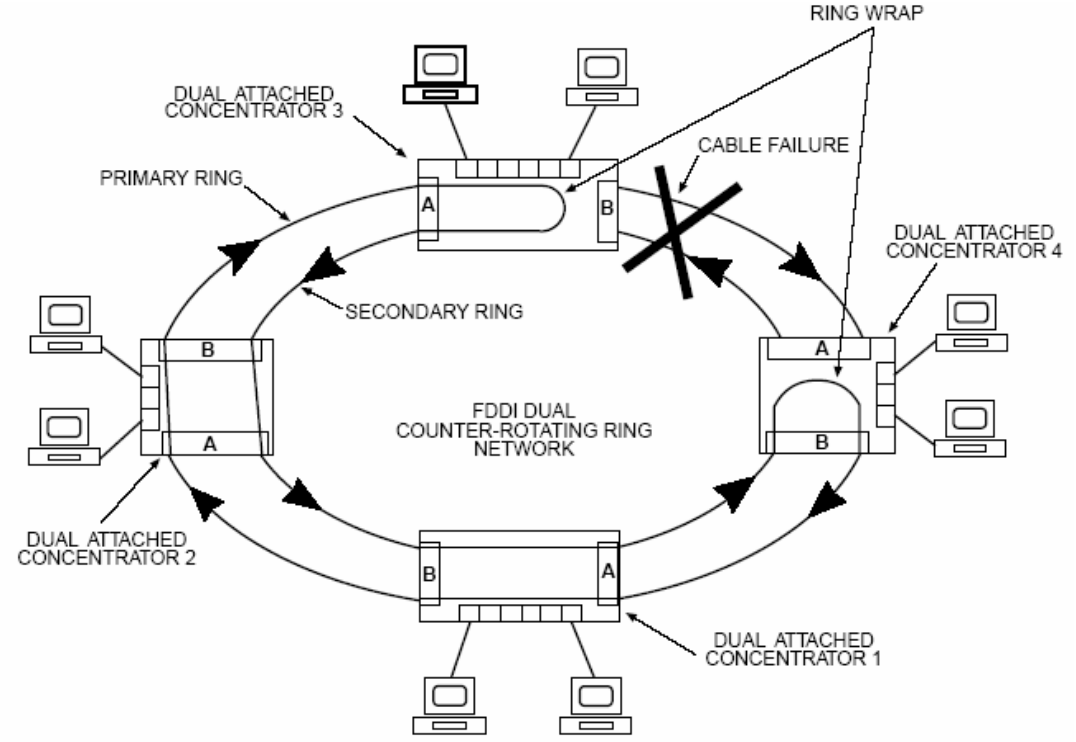
3.9.9. 1000BaseT

Tốc độ 1000 Mbps, sử dụng cáp xoắn đôi Cat 5, 5e, 6, 6e.

3.9.9.1. FDDI (Fiber Distributed Data Interconnection)

Sử dụng 2 vòng sợi quang ngược chiều để backup, truyền thẻ bài, tốc độ cao (gấp 10 lần Ethernet).

- Chiều dài tối đa 200 Km cho 2 vòng và 100 Km cho 1 vòng.
- Hổ trợ 500 máy trong một mạng.
- Mã hóa, chống nghe lén khi đứt cáp, không bị nhiễu điện từ.



Hình 4. 15 - FDDI

Ở hình 4.15, khi một trong 2 vòng bị đứt thì vòng còn lại truyền dữ liệu. Khi cả hai vòng bị đứt (thường thì 2 vòng đi chung vỏ bọc, nên khi đứt thì đứt cả hai) một vòng được hình thành từ hai vòng ngược chiều.

3.10. Câu hỏi và bài tập

1. Trình bày và vẽ hình minh họa hai kiến trúc mạng Star bus và Star ring, tại sao phải kết hợp các kiến trúc mạng lại với nhau?
2. Nêu các đặc tính kỹ thuật của các chuẩn mạng: 100BaseT, 1000BaseT và FDDI?
3. Trình bày nguyên tắc của luật 5-4-3, nguyên tắc này được áp dụng ở đâu?
4. Vẽ bảng tổng hợp các chuẩn mạng Ethernet?
5. Trình bày các kiến trúc mạng hiện nay Việt Nam đang sử dụng?

CHƯƠNG 5 - ĐỊA CHỈ IP

∗ Tóm tắt nội dung chương 5

- IPv4, IPv6 và cách chuyển đổi từ IPv4 sang IPv6.
- Chia mạng con trong IPv4.
- Hai loại địa chỉ private và public, cơ chế chuyển đổi địa chỉ NAT.

∗ Mục tiêu chương 5

Sau khi học xong sinh viên có khả năng:

- Trình bày 3 lớp địa chỉ A, B, C của IPv4.
- Làm các dạng bài tập chia mạng con IPv4.
- Trình bày được cấu trúc và các loại IPv6.
- Chuyển đổi được IPv4 sang IPv6 và cấu hình mạng bằng IPv6.

Số nhị phân 8 bit

Số nhị phân 8 bit được sử dụng mô tả cho địa chỉ IP, nên phải nắm vững các kiến thức về nó.

Máy tính sử dụng hệ nhị phân gồm 2 bit, ***1*** (5V hay đúng), ***0*** (0V hay sai).

Phép toán trên số nhị phân

Bảng 3. 1 - Phép toán AND và OR trên các bit

Phép AND			Phép OR		
A	B	A And B	A	B	A Or B
1	1	1	1	1	1
1	0	0	1	0	1
0	1	0	0	1	1
0	0	0	0	0	0

phép AND và phép OR hai số nhị phân.

```
      10100110          10100110
AND   00110010    OR    00110010
-------------     -------------
      00100010          10110110
```

Đổi số nhị phân sang số thập phân.

$1 = 1.2^0 = 1.1 = 1$

$11 = 1.2^1 + 1.2^0 = 2 + 1 = 3$

$111 = 1.2^2 + 1.2^1 + 1.2^0 = 4 + 2 + 1 = 7$

.....

$11111111 = 1.2^7 + 1.2^6 + 1.2^5 + 1.2^4 + 1.2^3 + 1.2^2 + 1.2^1 + 1.2^0$
$= 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$
$= 255$

$10101010 = 1.2^7 + 0.2^6 + 1.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 1.2^1 + 0.2^0$
$= 128 + 0 + 32 + 0 + 8 + 0 + 2 + 0$
$= 170$

Các bit được ghi từ phải qua trái, các bit 1 được xem như được bật. Có thể đọc như sau: bit 8 (cuối cùng bên trái) bật, bit 7 tắt, bit 6 bật... Các bit này được nhân với hệ số từ 2^0 trở đi.

Đổi số thập phân sang số nhị phân.

Đổi số thập phân 139 ra số nhị phân

139 / 2 = 69 dư 1
69 / 2 = 34 dư 1
34 / 2 = 17 dư 0
17 / 2 = 8 dư 1
8 / 2 = 4 dư 0
4 / 2 = 2 dư 0
2 / 2 = 1 dư 0
1 / 2 = 0 dư 1

Lần lượt lấy kết quả chia cho 2 cho đến hết, lấy số dư ghi từ trái sang phải.

$\Rightarrow$ 139 = 10001011

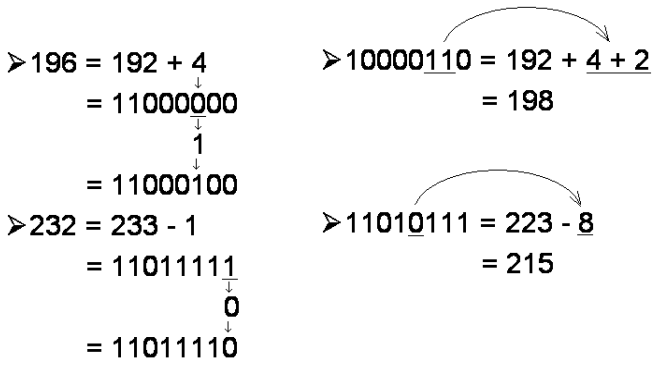
Dãy số 8 bit cần nhớ

Khi làm việc với IP thì chỉ làm việc với số 8 bit. Số 8 bit đổi sang số thập phân chạy từ 0 đến 255 (00000000 → 11111111)

Cần học thuộc dãy số sau để làm việc với IP một cách dễ dàng: ***128, 192, 224, 248, 252, 254, 255***

10000000 = 128	➢01111111 = 127
11000000 = 192	➢10111111 = 191
11100000 = 224	➢11011111 = 223
11110000 = 240	➢11101111 = 239
11111000 = 248	➢11110111 = 247
11111100 = 252	➢11111011 = 251
11111110 = 254	➢11111101 = 253
11111111 = 255	➢11111111 = 255

Đổi số dựa vào dãy số 8 bit



Nhận thấy 196 bằng 192 cộng 4, mà 192 là 10000000, 4 là 2 mũ 2 (tức bật bit 3 lên 1). Tương tự 10000110 bằng 10000000 cộng 110, tức là bằng 192 cộng 4 cộng 2 = 198.

Như vậy việc thuộc dãy số 8 bit giúp việc tính nhẩm nhanh khi đổi các số nhị phân 8 bit sang số thập phân và ngược lại.

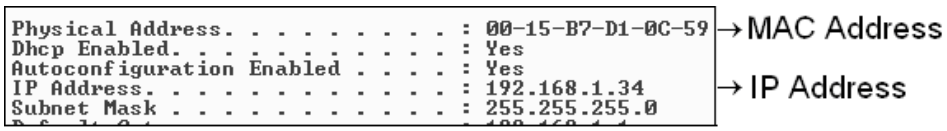
Địa chỉ IPv4 (Internet Protocol Version 4)

Trước đây khi thiết kế địa chỉ IP, số lượng thiết bị kết nối mạng còn ít và không gian địa chỉ IPv4 được xem như là vô tận. Nhưng hiện tại, IANA đã tuyên bố hết IPv4 vào cuối năm 2011. IPv6 sẽ được triển khai và dần thay thế IPv4 trong tương lai. Khi nói địa chỉ IP tức là địa chỉ IPv4, nếu là địa chỉ IPv6 thì ghi rõ là IPv6.

3.11. Cấu trúc địa chỉ IP

Truyền thông trong mạng máy tính là việc gửi các khung dữ liệu đến máy đích. Các khung dữ liệu này chứa các địa chỉ vật lý MAC. MAC là địa chỉ không phân cấp, tất cả các máy trên mạng có cơ hội ngang nhau. MAC là một con số 6 byte và để nhớ con số này thì thật khó khăn (ví dụ: phải nhớ số CMND của một người nào đó).

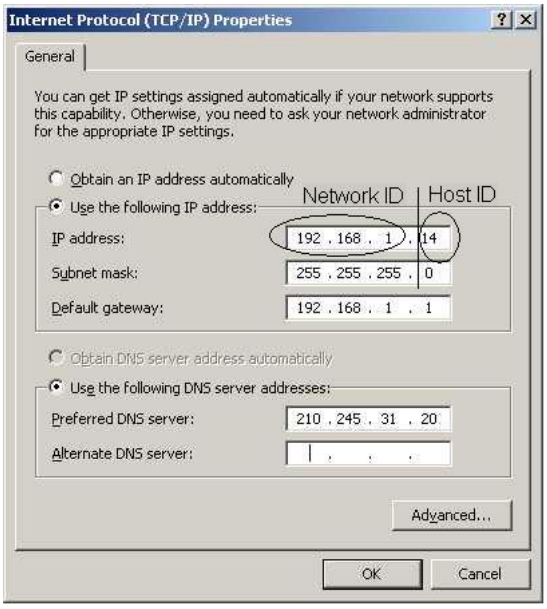
Nhưng khi gửi dữ liệu đi, phải biết địa chỉ của máy đích và nó phải dễ nhớ. Địa chỉ để người dùng làm việc là địa chỉ luận lý (logic) IP và họ không cần quan tâm đến địa chỉ MAC. Trong Windows dùng lệnh ***ipconfig /all*** để xem IP.



Hình 5. 1 - Địa chỉ vật lý MAC và địa chỉ luận lý IP

IP có cấu trúc phân lớp, các ràng buộc cấu trúc như thế nào là một địa chỉ IP hợp lệ. IP được chia làm 2 hoặc 3 phần:

- Network-id . host-id (không chia mạng con).
- Network-id . subnet-id . host-id (có chia mạng con).



Hình 5. 2 - Cấu hình IP cho NIC trong Windows

Ở hình 5.2, dựa vào subnet mask xác định được địa chỉ IP 192.168.1.14 được chia làm 2 phần network-id là 192.168.1 (tức là NIC này thuộc mạng 192.168.1), host-id 14 (tức là chỉ danh máy trong mạng là 14).

IP là một con số có kích thước 32 bit (4 byte), được chia làm 4 phần cách nhau bởi dấu chấm. Mỗi phần có 8 bit (1 byte) được gọi là Octet. IP thường được trình bày bằng ký pháp thập phân có dấu chấm (Dotted-decimo notation). Có thể trình bày bằng dạng nhị phân 10101100.00010000.00011110.00111000 hoặc dạng thập lục phân AC 10 1E 38.

IP được ký hiệu là ***w.x.y.z*** (đọc là octet w, octet x, octet y, octet z).

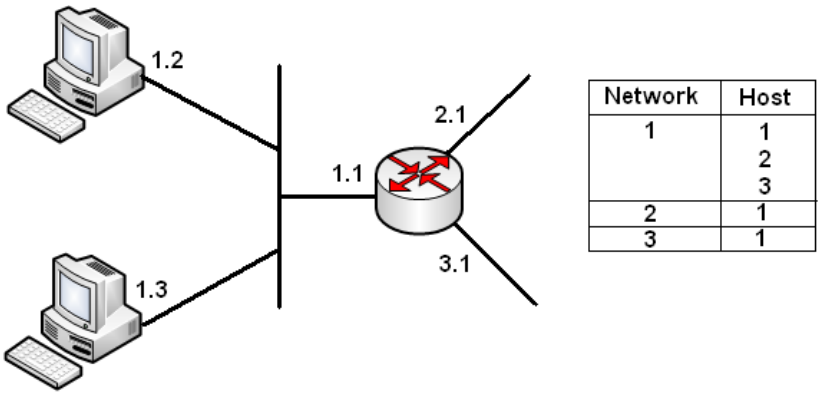
Bảng 3. 2 - Điểm khác giữa địa chỉ IP và địa chỉ có cấu trúc khác như thuê bao điện thoại

Telephone	IP
0 84 0983 797979	210.245.31.20
Phân cấp rõ ràng Không thể tự thay đổi Chỉ cần nhớ	Không phân cấp rõ ràng Có thể tự thay đổi cho phù hợp Phải học cách cấu hình

3.12. Một số khái niệm liên quan đến IP

3.12.1.Network-id

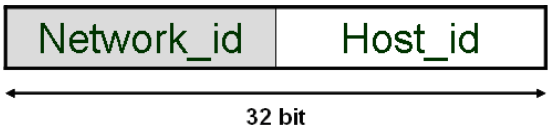
Là giá trị xác định đường mạng, một số bit đầu trong 32 bit được dùng để xác định đường mạng cho một địa chỉ IP. Ở hình 5.3, vì mỗi port của router là một mạng nên có 3 mạng: 1, 2, 3. Network-id của 3 mạng này phải khác nhau, router không cho phép khai báo các IP cho các port của mình cùng mạng nhau.



Hình 5. 3 - Network-id và host-id

3.12.2.Host-id

Là giá trị xác định các host trong một mạng, một số bit cuối của 32 bit xác định host-id. Ở hình 5.3, mạng 1 có 2 host thì giá trị 2 host-id này phải khác nhau. Nếu khai báo 2 host có host-id giống nhau thì xảy ra xung đột IP (conflict IP) và một trong 2 host đó không hoạt động được.



Hình 5. 4 - Network-id và host-id

3.12.3.Địa chỉ host

Là địa chỉ IP được cấu hình cho một interface của một host. Theo hai khái niệm trên thì:

- Hai host cùng network-id thì cùng mạng, lúc này host-id phải khác nhau.
- Hai host khác network-id thì khác mạng, lúc này host-id tùy ý.

IP1: 192.168.1.14 (network-id: 3 octet, host-id: 1 octet)

IP2: 192.168.1.114 (network-id: 3 octet, host-id: 1 octet) cùng mạng với IP1

IP2: 192.168.2.14 (network-id: 3 octet, host-id: 1 octet) khác mạng với IP1

3.12.4.Mạng (network)

Là nhiều host kết nối trực tiếp với nhau, giữa hai host bất kỳ không có thiết bị lớp 3 (Network). Nói cách khác, qua thiết bị lớp 3 là qua mạng khác.

Địa chỉ mạng (network number)

Thường viết tắt là NN. Là địa chỉ IP dùng để đặt cho một mạng, địa chỉ này không dùng để đặt cho interface. ***Địa chỉ NN xác định bằng cách giữ nguyên giá trị của network-id, tắt tất cả các bit phần host-id về 0***

Ví dụ 5.1:

IP1: 192.168.1.14 (network-id: 3 octet, host-id: 1 octet)

Giữ nguyên 3 octet đầu (192.168.1), tất cả các bit của octet z sau cùng tắt về 0 (00000000 = 0).

⇒ NN của IP1 là: 192.168.1.0

Mạng con (subnet)

Subnet là chia một mạng thành các mạng con nhỏ hơn để tiết kiệm IP (thường ISP làm việc này để chia nhỏ các mạng đến một IP trên một mạng để bán cho khách hàng). Chia mạng con có những ưu điểm sau:

- Tránh nhiễm virus.
- Giảm broadcast, tăng băng thông mạng.
- Tiết kiệm tiền mua IP.

Ví dụ 5.2:

IP1: 192.168.1.14 (network-id: 3 octet, host-id: 1 octet)

Octet z có thể chạy từ 0 đến 255. Nhưng 192.168.1.0 là địa chỉ mạng nên không thể đánh cho host, 192.168.1.255 là địa chỉ broadcast cũng không sử dụng. Địa chỉ đánh cho host từ 1 → 254 hay mạng này có thể có 254 host. Nếu mạng chỉ có 20 host thì điều này là phí phạm IP và nên chia nhỏ mạng 192.168.1.0 ra thành nhiều mạng nhỏ hơn để sử dụng hiệu quả không gian địa chỉ IP. Phần này sẽ nói chi tiết hơn trong phần chia mạng con.

Địa chỉ broadcast

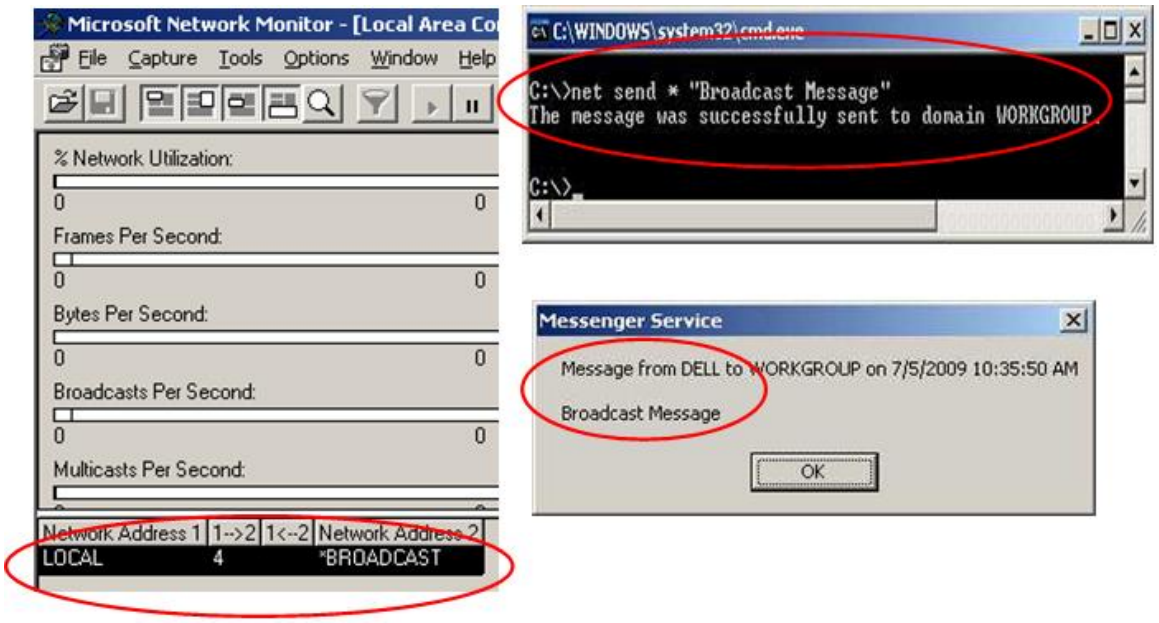
Thường viết tắt là B. Là địa chỉ IP đại diện cho tất cả các host trong mạng, khi một gói tin mang địa chỉ IP đích là địa chỉ này, nó sẽ được gửi cho tất cả các host trong mạng. Địa chỉ này không dùng để đánh địa chỉ cho host. ***Địa chỉ B xác định bằng cách giữ nguyên giá trị phần network-id, bật tất cả các bit phần host-id lên 1.***

Ví dụ 5.3:

IP1: 192.168.1.14 (network-id: 3 octet, host-id: 1 octet)

Giữ nguyên 3 octet đầu (192.168.1), tất cả các bit octet z bật lên 1 (11111111 = 255)

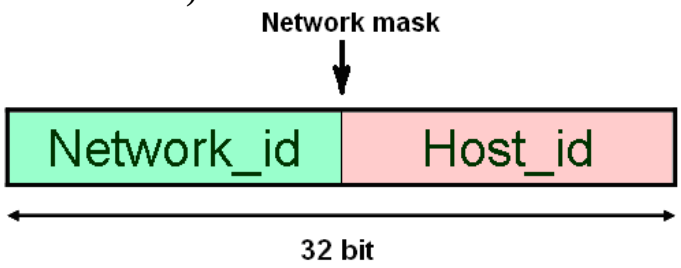
⇒ B của IP1 là 192.168.1.255



Hình 5. 5 - Dùng Network Monitor bắt gói tin broadcast

Ở hình 5.5, dùng công cụ bắt gói tin trong Win2K3 là ***Network Monitor***, sau đó dùng lệnh ***net sent*** để broadcast gói tin lên toàn mạng. Chính máy gởi cũng nhận được gói tin này và Network Monitor bắt được gói tin này.

Mặt nạ mạng (network mask)



Hình 5. 6 - Mặt nạ mạng

Còn gọi là subnet mask viết tắt là SM, dùng để phân biệt network-id + subnet-id với host-id. ***Network mask được xác định bằng cách bật tất cả các bit phần network-id lên 1,tắt tất cả các bit phần host-id về 0***.

Ví dụ 5.4:

IP1: 192.168.1.14 (network-id: 3 octet, host-id: 1 octet)

Tất cả các bit của octet w, x, y bật lên 1 (11111111.11111111.11111111 = 255.255.255), tất cả các bit của octet z tắt về 0 (00000000 = 0). Vậy SM của IP1 là 255.255.255.0

Khi viết địa chỉ IP phải có SM, nếu không có SM thì không xác định IP đó thuộc mạng nào. Ví dụ: IP 192.168.1.79 nếu SM là 255.255.0.0 thì nó thuộc mạng 192.168.0.0, nếu SM là 255.255.255.0 thì nó thuộc mạng 192.168.1.0.

∗ **Cách viết IP như sau: *IP/SM*, ví dụ: 192.168.1.79/255.255.255.0**

∗ **Để đơn giản hơn, khi IP trên có số bit phần network-id là 24 bit. Thì viết gọn lại là *IP/số bit phần network-id + subnet-id*, ví dụ: 192.168.1.79/24**

∗ **Công thức xác định mạng của địa chỉ IP:**

IP and SM = NN

Ví dụ 5.5:

IP →	172.29.14.10	=	10101100.00011101.00001110.00001010
SM →	255.255.0.0	=	11111111.11111111.00000000.00000000
	AND		AND
NN →	172.29.0.0	=	10101100.00011101.00000000.00000000

Các lớp của địa chỉ IP

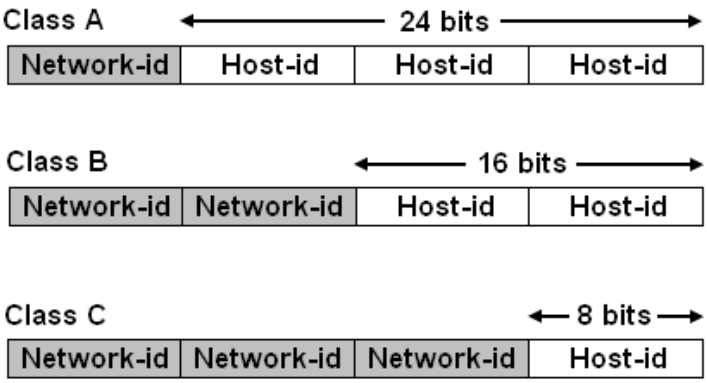
Không gian địa chỉ IP gồm 2^{32} địa chỉ, được chia làm nhiều lớp để dễ quản lý. Năm lớp được chia là A, B, C, D, E. Trong đó:

– Lớp A, B, C dùng để đánh địa chỉ các host trong mạng.

– Lớp D dùng cho nhóm địa chỉ multicast.

– Lớp E dùng cho mục đích nghiên cứu.

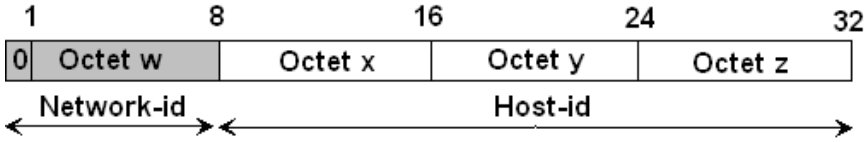
Tài liệu chỉ nghiên cứu 3 lớp A, B, C dùng để đánh địa chỉ IP cho các host trên mạng.



Hình 5. 7 - Ba lớp địa chỉ IP A, B, C

Địa chỉ IP lớp A

∗ **Dành 1 byte cho network-id và 3 byte cho host-id**



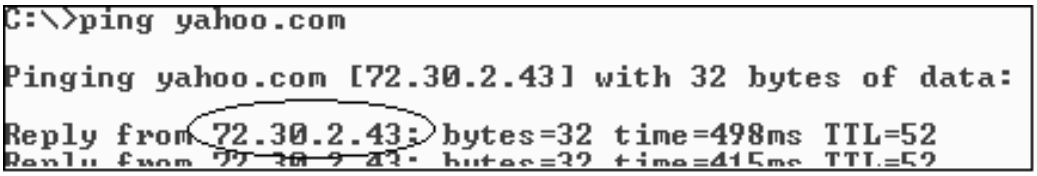
Hình 5. 8 - Địa chỉ IP lớp A

∗ **Nhận diện lớp A: bit đầu tiên luôn là 0.**

∗ **Dạng của octet w là: *0wwwwwww* (w = 0 hoặc 1).**

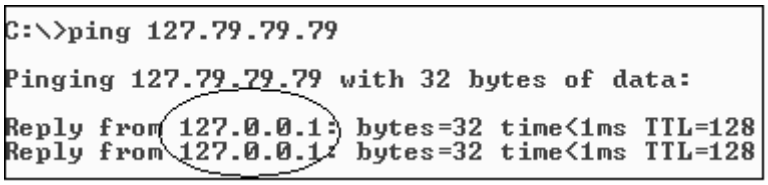
Như vậy octet w chạy từ 00000000 = 0 đến 01111111 = 127

Hay địa chỉ IP nào có octet đầu tiên từ 1 đến 127 là thuộc lớp A



Hình 5. 9 - IP của Yahoo

Ping yahoo.com có địa chỉ 72.30.2.43, octet w = 72, vậy địa chỉ Yahoo.com thuộc lớp A.



Hình 5. 10 - Mạng Loopback.

Ping bất cứ IP nào thuộc mạng 127.0.0.0 đều trả về ***127.0.0.1*** (địa chỉ ***Localhost***). Mạng này gọi là mạng ***Loopback***, không sử dụng đánh địa chỉ cho host. Mạng ***0.0.0.0*** cũng không sử dụng.

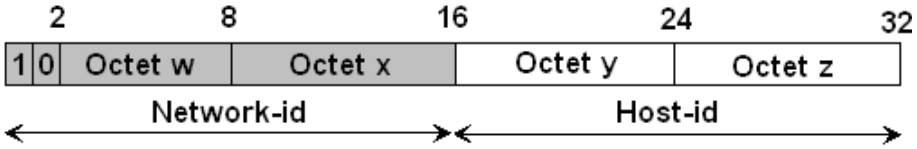
⇒ lớp A có: 126 mạng (từ 1 đến 126)

Host-id có 24 bit, có 2^{24} trạng thái. Bỏ đi một địa chỉ mạng (host-id toàn bit 0), một địa chỉ broadcast (host-id toàn bit 1).

⇒ Mỗi mạng thuộc lớp A có: 2^{24} -2 = 16.777.214 (host)

Địa chỉ IP lớp B

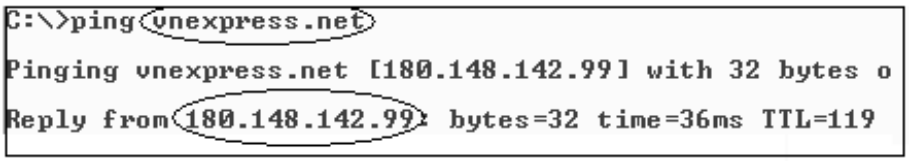
∗ **Dành 2 byte cho network-id và 2 byte cho host-id**



Hình 5. 11 - Địa chỉ IP lớp B

∗ **Nhận diện lớp B: 2 bit đầu của octet w là 10.**

∗ **Dạng của octet w là: *10wwwwww*, chạy từ 10000000 = 128 đến 10111111 = 191.**



Hình 5. 12 - IP của Vnexpress

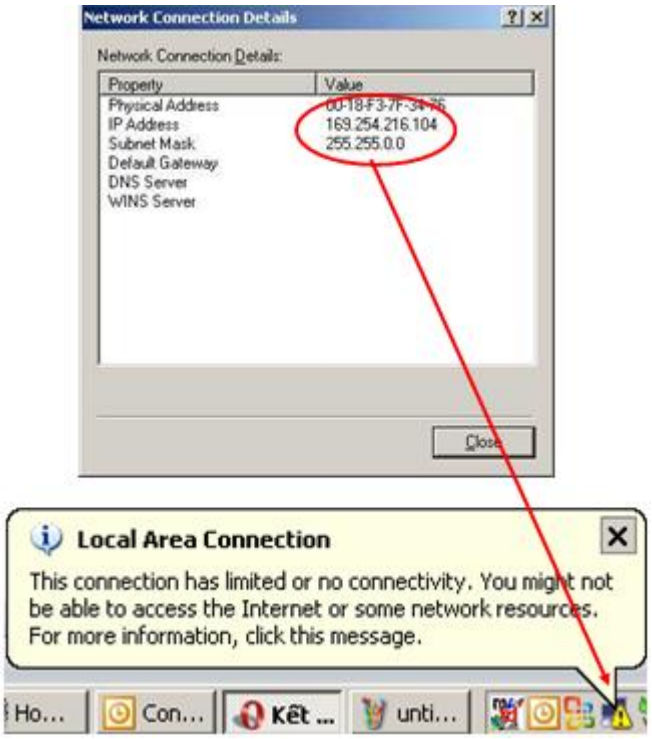
Địa chỉ IP của báo điện tử vnexpress.net thuộc lớp B

Phần network-id có 16 bit, dành 2 bit để nhận dạng lớp còn lại 14 bit

⇒ Lớp B có 2^{14} = 16.384 (mạng).

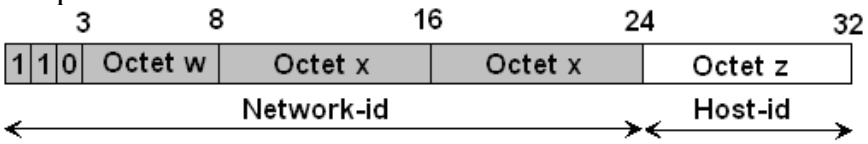
⇒ Số host trong mỗi mạng là 2^{16} – 2 = 65.534 (host)

Lưu ý: khi đánh địa chỉ cho các host, không nên dùng mạng 169.254.0.0. Vì mạng này là mạng Apipa (được tự động cấp phát khi không ai cấp phát IP cho host).



Hình 5. 13 - IP Apipa tự động cấp phát và cảnh báo

Địa chỉ IP lớp C



Hình 5. 14 - Địa chỉ IP lớp C

∗ **Dành 3 byte cho network-id và 1 byte cho host-id.**

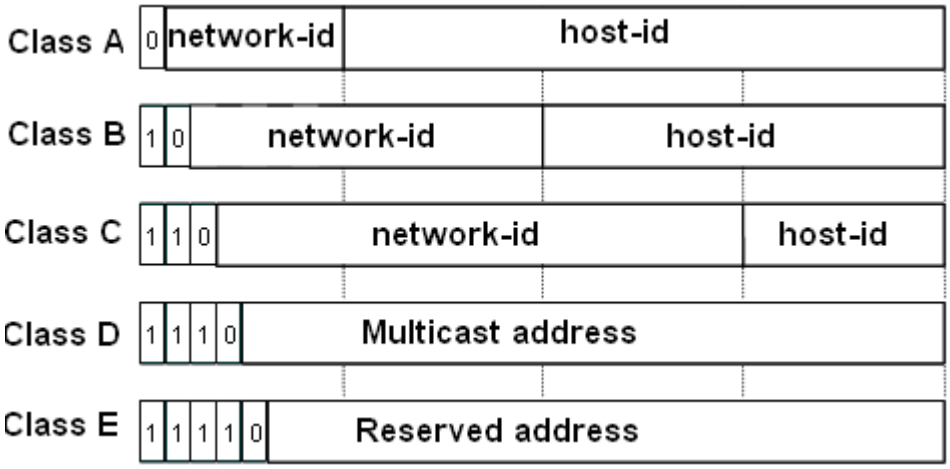
∗ **Nhận dạng lớp C:** ***3 bit đầu của octet w là 110*****, chạy từ 11000000 = 192 đến 11011111 = 223.**

```
C:\>ping 5giay.vn

Pinging 5giay.vn [210.245.123.158] with 32 bytes of data:

Reply from 210.245.123.158: bytes=32 time=14ms TTL=58
Reply from 210.245.123.158: bytes=32 time=13ms TTL=58
```

Hình 5. 15 - IP của trang 5giay

⇒ Địa chỉ IP của 5giay.vn thuộc lớp C.
Phần network-id có 24 bit, bỏ đi 3 bit nhận dạng lớp còn lại 21 bit
⇒ Lớp C có 2^{21} = 2.097.152 (mạng).
⇒ Số host trong mỗi mạng là $2^8 - 2 = 254$ (host).

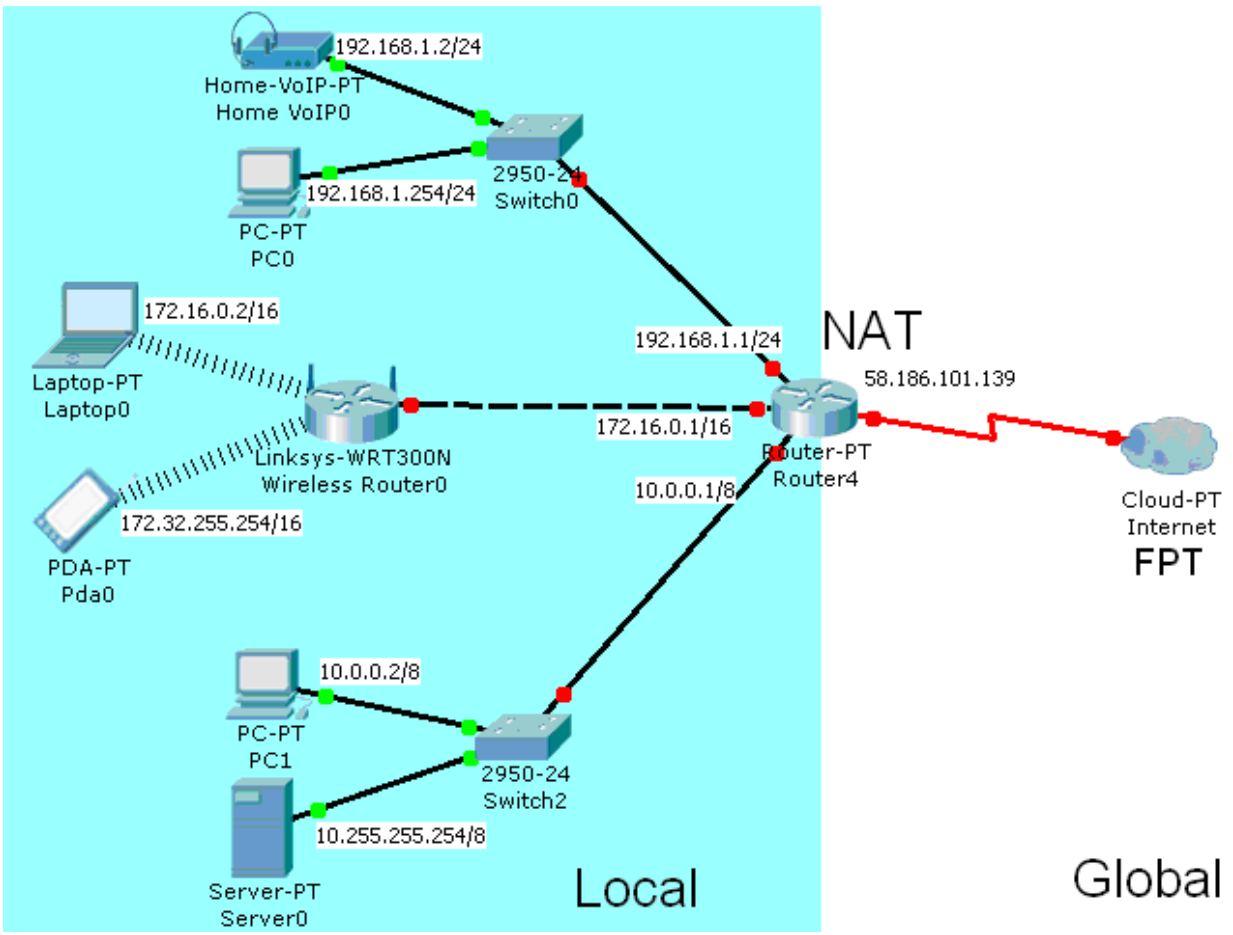
∗ **Các IP còn lại thuộc lớp D và E (không khảo sát)**



Hình 5. 16 - Các lớp trong địa chỉ IPv4

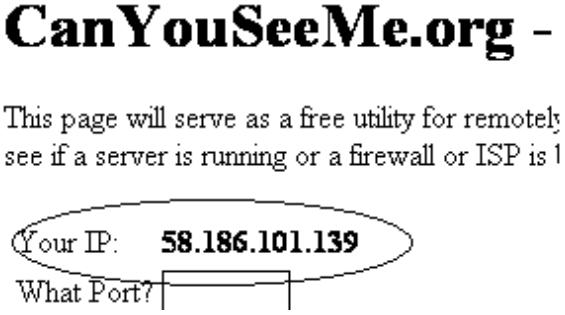
Bảng 5.1 - Tổng kết các lớp địa chỉ IPv4.

	Lớp A	Lớp B	Lớp C
Giá trị của byte đầu tiên	0 – 127	128 – 191	192 – 223
Số byte phần Network_id	1	2	3
Số byte phần Host_id	3	2	1
Network mask	255.0.0.0	255.255.0.0	255.255.255.0
Broadcast	XX.255.255.255	XX.XX.255.255	XX.XX.XX.255
Network Address	XX.0.0.0	XX.XX.0.0	XX.XX.XX.0
Số đường mạng	126	16.384	2.097.152
Số host trên mỗi đường mạng	16.777.214	65.534	254



Hình 5. 17 - Địa chỉ IP private và IP public

Hệ thống bên trong công ty được gọi là local (hay inbound), bên ngoài gọi là global (hay outbound). Trong công ty việc hoạch định cấu hình IP là tùy ý, nhưng khi muốn ra Internet phải có một IP hợp lệ được ISP cấp (có thể xem bằng trang canyouseeme.org.



Hình 5. 18 - Xem IP public của mình đang sử dụng

Ví dụ: Trường CĐ KT Lý Tự Trọng, việc tổ chức bên trong là do trường quyết định. Khi liên hệ bên ngoài thì mọi người chỉ biết đến địa chỉ 390 Hoàng Văn Thụ mà thôi.

IANA cung cấp một số mạng để sử dụng cấu hình IP cho các máy trong local. Các IP này gọi là IP private, IP này không thể ra WAN và gọi là IP không hợp lệ. Khi router nhận được một gói tin mang địa chỉ nguồn là IP private thì:

- Nó chuyển IP private này thành IP public (nếu cơ chế NAT bật) và chuyển gói tin đi.
- Nếu không thể chuyển đổi thành địa chỉ IP public, nó hủy gói tin.

∗ Địa chỉ IP private (miễn phí)

– Lớp A: 10.0.0.0/8 (1 mạng)
– Lớp B: 172.16.0.0/16 đến 172.32.0.0/16 (32 mạng)
– Lớp C: 1892.168.0.0/24 (256 mạng)

Tất cả IP còn lại thuộc lớp A, B, C gọi là IP Public (IP hợp lệ), được phép ra WAN, khi sử dụng phải mua (dùng để nối chi nhánh các công ty...) hoặc do ISP cấp động.

Tất cả các gói tin mang địa chỉ IP private sẽ bị hủy khi ra Internet. Để giúp các máy tính trong local ra global, dùng kỹ thuật chuyển đổi địa chỉ NAT (Network Address Translation).

- NAT Outbound: chuyển IP private thành IP public ra Internet
- NAT Inbound: chuyển IP public thành IP private để các máy bên ngoài global truy cập các máy bên trong local.

Kỹ thuật chia mạng con (subneting)

Mặt nạ mạng (network mask)

Network mask là mặt nạ của địa chỉ IP, còn gọi là subnet mask (SM). SM đánh dấu phân cách các bit xác định đường mạng và các bit host trong 32 bit của IP.

Mặc nhiên khi chưa chia subnet, SM của lớp A là 255.0.0.0 hay 8 bit, lớp B 255.255.0.0 hay 16 bit, lớp C 255.255.255.0 hay 24 bit. Gọi là subnet mask default (SMD)

Nếu một IP có SM = SMD thì chưa chia mạng con, ngược lại SM ≠ SMD thì đã chia mạng con.

Ví dụ 5.6:

Một host được ghi nhận địa chỉ IP: 203.113.188.1/255.255.255.192

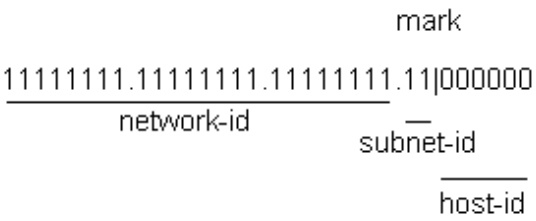
Octet w = 203 ($192 \leq 203 \leq 223$).

⇒ IP thuộc lớp C, SMD=255.255.255.0

SM của IP là 255.255.255.192 ≠ SMD.

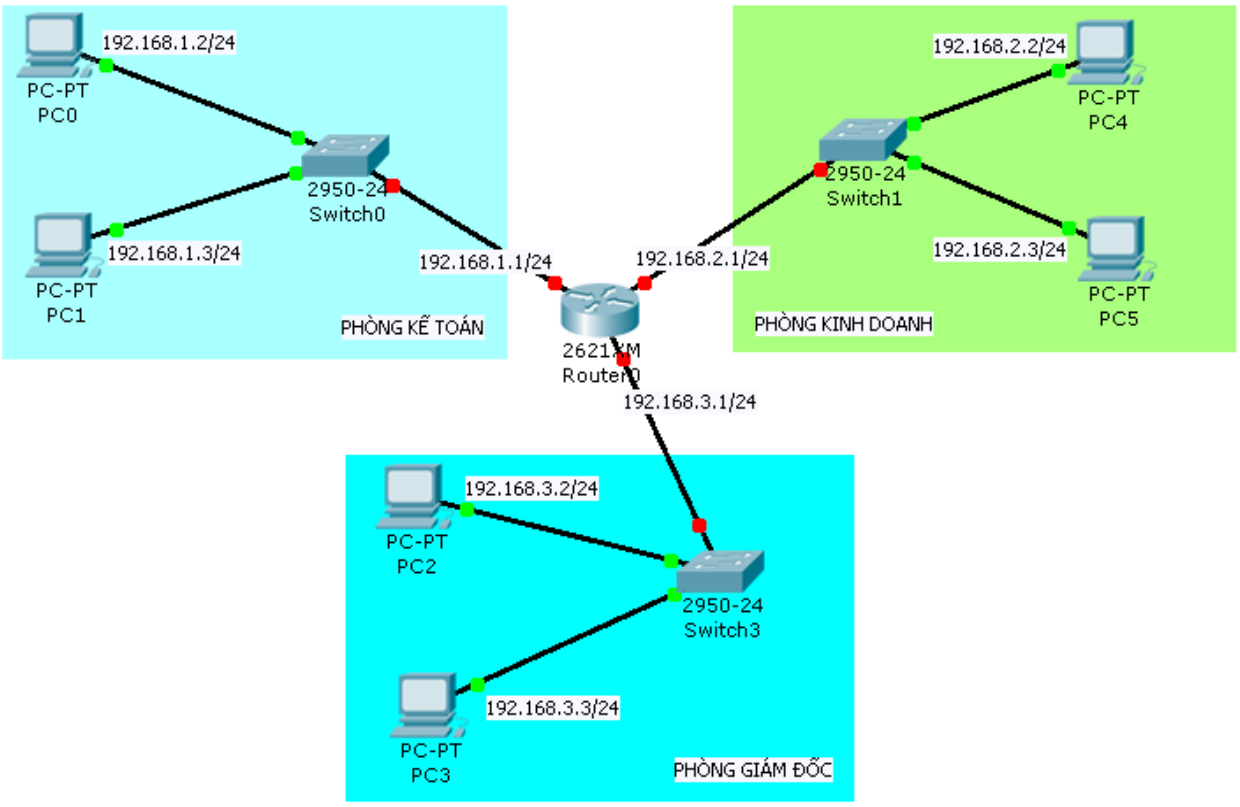
⇒ IP này đã chia mạng con.

Lúc này số 192 gọi là số khó chịu: 192 = 11000000, tức lúc này đã mượn 2 bit của host-id làm subnet-id.



Hình 5. 19 - Subnet-id

Chia mạng con



Hình 5. 20 - Hệ thống IP có 3 đường mạng

Ví dụ 5.7:

Công ty A có 3 phòng, mỗi phòng 2 máy tính. Các phòng này được tách mạng bằng Router0. Vậy cần 3 mạng khác nhau cho 3 phòng 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24.

Khi số lượng phòng ban lớn hơn phải dùng nhiều mạng hơn, ở đây mỗi mạng có 254 máy. Sử dụng IP như thế này rất phí phạm, nhất là IP ra Internet (hiện nay IANA đã tuyên bố hết IPv4 và chuyển sang sử dụng IPv6).

Giải pháp ở đây là chỉ dùng một mạng 192.168.1.0/24 và chia ra thành nhiều mạng con để sử dụng. Về kỹ thuật, chia subnet là mượn một số bit phần host-id dùng làm subnet-id. Octet w thuộc khoảng 192 đến 223 vậy IP này thuộc lớp C, số bit network-id là 24 vậy IP chưa chia mạng con.

Ở đây cần 3 mạng con, nhưng khi chia mạng con thì mạng đầu và mạng cuối không sử dụng được (vì các thiết bị không chạy được 2 mạng này). Nên chính xác, cần 5 mạng (tức là 5 trạng thái). Để có được 5 trạng thái phải có 3 bit ($2^3 = 8$ trạng thái 000, 001, 010, 011, 100, 101, 110, 111), nếu mượn 2 bit chỉ có $2^2 = 4$ trạng thái (còn thiếu), mượn 4 bit có $2^4 = 16$ trạng thái (quá dư).

> Lưu ý: Các thiết bị mạng hiện nay có thể chạy được mạng đầu và mạng cuối, nhưng các thiết bị cũ không thể chạy. Vậy khi thi cử thì tuân thủ bỏ mạng đầu và cuối.

⇒ Số bit mượn = 3
⇒ Số bit host-id = 8 -3 = 5
⇒ Số bit network-id + subnet-id = 24 + 3 = 27

∗ có 6 mạng:

~~Net 0:~~ 192.168.1.000|00000 = 192.168.1.0/27 (không sử dụng)

Net 1: 192.168.1.001|00000 = 192.168.1.32/27

NN = 192.168.1.32

Host = 192.168.1.33 → 192.168.1.62

B = 192.168.1.63

Net 2: 192.168.1.010|00000 = 192.168.1.64/27

NN = 192.168.1.64

Host = 192.168.1.65 → 192.168.1.94

B = 192.168.1.95

Net 3: 192.168.1.011|00000 = 192.168.1.96/27

NN = 192.168.1.96

Host = 192.168.1.97 → 192.168.1.126

B = 192.168.1.127

Net 4: 192.168.1.100|00000 = 192.168.1.128/27

NN = 192.168.1.128

Host = 192.168.1.129 → 192.168.1.158

B = 192.168.1.159

Net 5: 192.168.1.101|00000 = 192.168.1.160/27

NN = 192.168.1.160

Host = 192.168.1.161 → 192.168.1.190

B = 192.168.1.191

Net 6: 192.168.1.110|00000 = 192.168.1.192/27

NN = 192.168.1.192

Host = 192.168.1.193 → 192.168.1.222

B = 192.168.1.223

~~Net 7:~~ 192.168.1.111|00000= 192.168.1.224/27 (không sử dụng)

Ở octet z các mạng cách nhau 32 đơn vị được gọi là bước nhảy, kí hiệu BN.

$$BN = 2^{\text{số bit host-id}}$$

Đối với ví dụ trên

$\Rightarrow BN = 2^5 = 32$

∗ **Xét Net 1: 192.168.1.32/27**

Mạng này có IP chạy từ 192.168.1.32/27 đến 192.168.1.63/27 (vì sang 192.168.1.64/27 thuộc mạng con thứ 2)

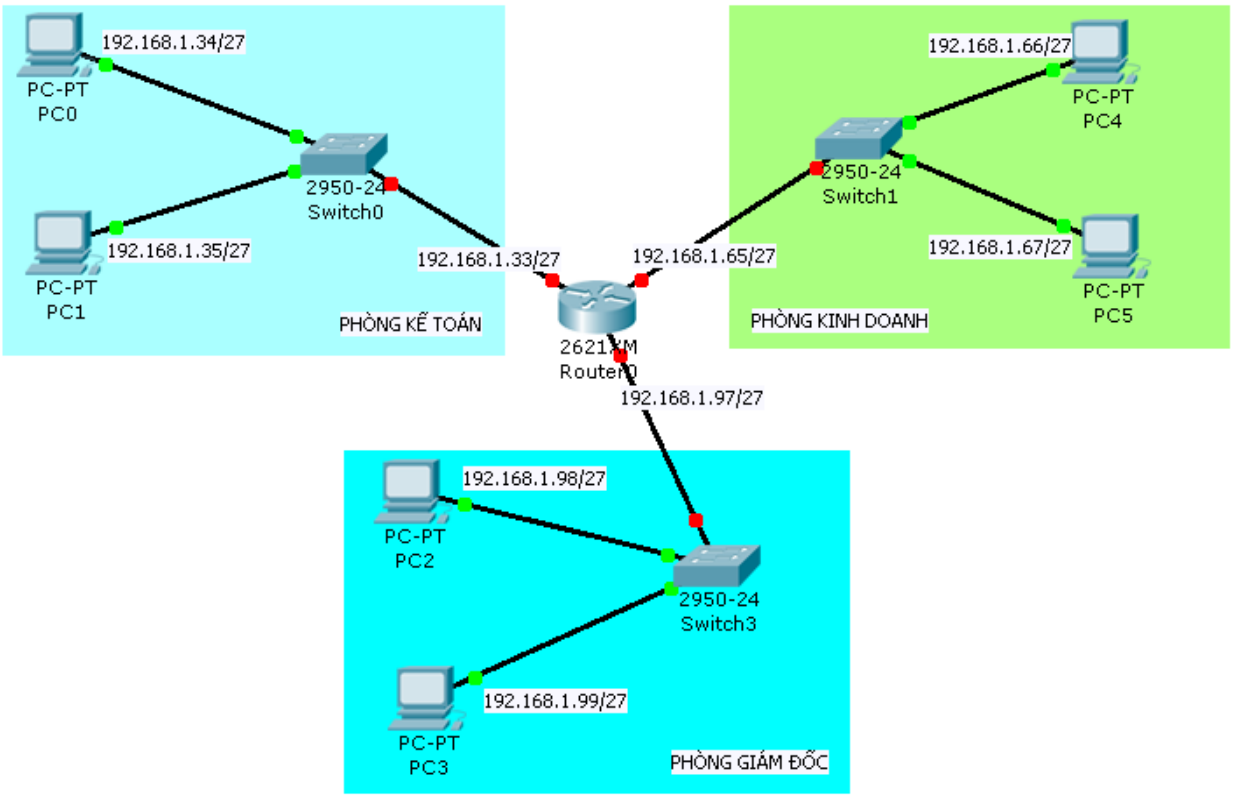
NN của mạng này là: 192.168.1.32

B của mạng này là địa chỉ cuối cùng của mạng: 192.168.1.63

IP của 30 host: từ 192.168.1.33 đến 192.168.1.62

Tương tự cho các mạng con còn lại.

Dùng Net 1, Net 2 , Net 3 để đánh địa chỉ cho công ty A.



Hình 5. 21 - Chia 192.168.1.0/24 thành các subnet

Với giải pháp trên mỗi subnet có 30 host, vẫn còn phí phạm IP. Giải pháp chỉ dùng 1 mạng con Net 1 để đánh địa chỉ cho công ty A. Như vậy tiếp tục chia nhỏ Net 1. Khi chia nhỏ từ lần thứ 2 trở đi, không phải bỏ mạng đầu và mạng cuối nữa.

Cần 3 trạng thái hay số bit mượn = 2 (2^2 =4)

⇒ Số bit host-id = 5 – 2 = 3

⇒ BN = 2^3 = 8

⇒ Số host trong mỗi mạng con = 2^3 – 2 = 6 (trừ NN và B)

⇒ Số bit phần mạng (network-id) = 27 + 2 = 29

* **Có 4 mạng:**

Net 1.0 → NN: 192.168.1.32/29

B: 192.168.1.39/29

Net 1.1 → NN: 192.168.1.40/29

B: 192.168.1.47/29

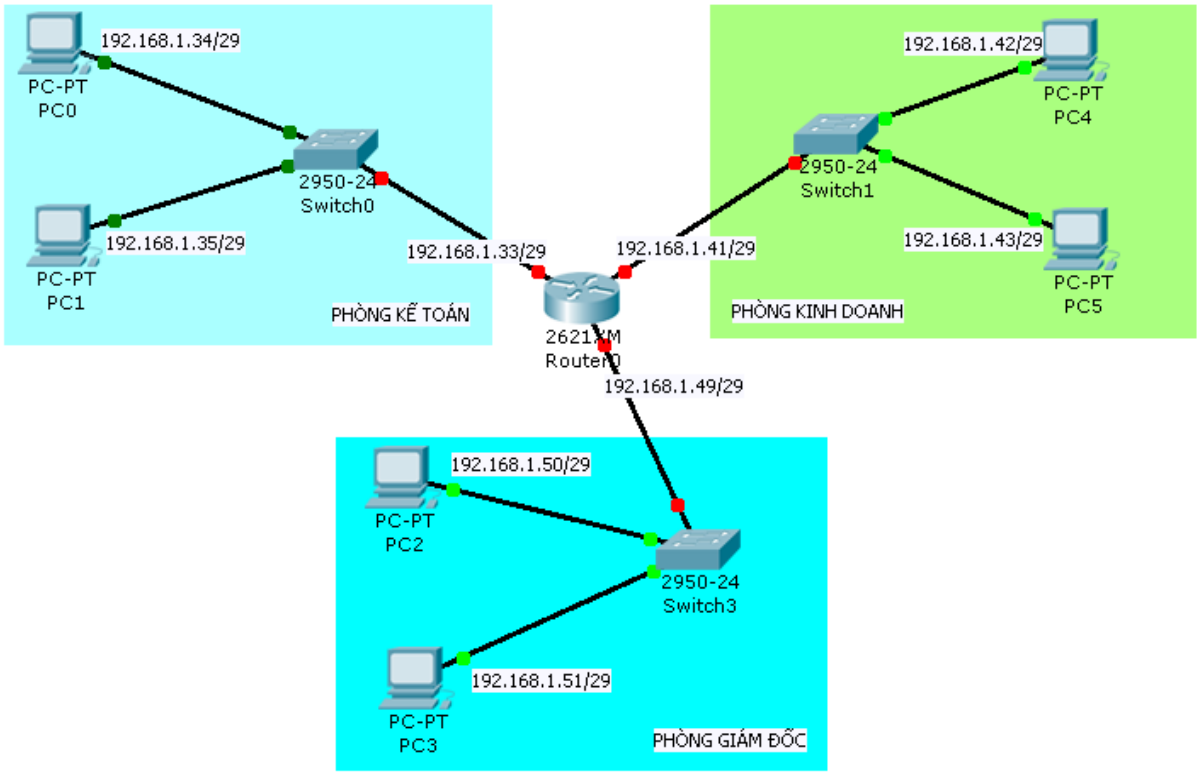
Net 1.2 → NN: 192.168.1.48/29

B: 192.168.1.55/29

Net 1.3 → NN: 192.168.1.56/29

B: 192.168.1.63/29

Dùng Net 1.0, Net 1.1, Net 1.2 đánh địa chỉ cho công ty A.



Hình 5. 22 - Dùng net 1.0, net 1.1, net 1.2 đánh địa chỉ cho công ty A

Đến lúc này đã tối ưu hóa việc tiết kiệm IP, dư rất nhiều IP ở các mạng: Net 1.3, Net 2, Net 3, Net 4, Net 5, Net 6 của mạng 192.168.1.0/24. Thay vì phải sử dụng đến 3 mạng 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 như lúc đầu.

Ví dụ 5.8:

Cần chia IP 172.16.55.71/16 thành: 12 mạng con mỗi mạng 4094 (host), 2 mạng mỗi mạng 1024 (host), 4 mạng 1022 (host). IP: 172.16.229.79/22 thuộc mạng nào?

*** Nhận xét:**

Octet w = 172 ($128 \leq 172 \leq 191$)

$\Rightarrow$ IP trên thuộc lớp B

Số bit network-id = 16

SM = SMD

$\Rightarrow$ Chưa chia mạng con

Để tính được số bit mượn dựa vào số host cần thiết cho mỗi mạng. Số host là 4094 = 2^{12} -2 nên số bit host cho mỗi mạng là 12, nên có thể cho mượn được 16 – 12 = 4 bit, số mạng có thể chia 2^4 =16, đề bài cần 12 + 2 = 14 mạng (bỏ mạng đầu mạng cuối). Vậy thỏa đề bài.

$\Rightarrow$ Số bit mượn = 4 (2^4 = 16)

Lưu ý: chỉ chú ý đến octet có mask (ranh giới subnet-id và host-id).

Mượn 4 bit của octet y, nên chỉ chú ý đến octet y mà thôi.

$\Rightarrow$ Số bit host-id của octet y = 8 – 4 = 4

$\Rightarrow$ BNy = 2^4 = 16

~~Net 0~~ → NN: 172.16.0.0/20
B: 172.16.15.255/20

Net 1 → NN: 172.16.16.0/20
B: 172.16.31.255/20

Net 2 → NN: 172.16.32.0/20
B: 172.16.47.255/20

Net 3 → NN: 172.16.48.0/20
B: 172.16.63.255/20

Net 4 → NN: 172.16.64.0/20
B: 172.16.79.255/20

Net 5 → NN: 172.16.80.0/20
B: 172.16.95.255/20

Net 6 → NN: 172.16.96.0/20
B: 172.16.111.255/20

Net 7 → NN: 172.16.112.0/20
B: 172.16.127.255/20

Net 8 → NN: 172.16.128.0/20
B: 172.16.143.255/20

Net 9 → NN: 172.16.144.0/20
B: 172.16.159.255/20

Net 10 →NN: 172.16.160.0/20
B: 172.16.175.255/20

Net 11 →NN: 172.16.176.0/20
B: 172.16.191.255/20

Net 12 →NN: 172.16.192.0/20
B: 172.16.207.255/20

Net 13 →NN: 172.16.208.0/20
B: 172.16.223.255/20

Net 14 →NN: 172.16.224.0/20
B: 172.16.239.255/20

~~Net 15~~ →NN: 172.16.240.0/20
B: 172.16.255.255/20

Dùng 12 mạng từ Net 1 đến Net 12 cho yêu cầu đề bài.

∗ Tiếp theo cần 2 mạng mỗi mạng 1024 host

1024 = 2^{10}, nếu host-id có 10 bit thì thiếu 2 (vì cần 2^{10} +2), nên số bit host-id phải là 11.

Số bit có thể mượn 32 – 20 – 11 = 1 bit, số mạng có thể chia = 2^1 = 2 (đáp ứng đề bài.

- Chọn Net 13 để chia

  Số bit mượn = 1

  Số bit host-id của octet y = 4-1 = 3

  $\Rightarrow$ BNy = 2^3 = 8

Net 13.0 → NN: 172.16.208.0/21
B: 172.16.215.255/21

Net 13.1 → NN: 172.16.216.0/21
B: 172.16.223.255/21

∗ **Tương tự, cần 4 mạng mỗi mạng 1022 host, chọn net 14 để chia.**

$1022 = 2^{10} - 2$

$\Rightarrow$ Số bit host-id = 10

Số bit có thể cho mượn = 12 – 10 = 2, chia được $2^2 = 4$ mạng

$\Rightarrow$ Số bit mượn = 2

Số bit host-id của octet y = 4 – 2 = 2

$\Rightarrow$ BNy = $2^2 = 4$

Net 14.0 → NN: 172.16.224.0/22

B: 172.16.227.255/22

Net 14.1 → NN: 172.16.228.0/22

B: 172.16.231.255/22

Net 14.2 → NN: 172.16.232.0/22

B: 172.16.235.255/22

Net 14.3 → NN: 172.16.236.0/22

B: 172.16.239.255.22

$\Rightarrow$ IP: 172.16.229.79/22 thuộc mạng: Net 14.1

Một số bài giải mẫu về chia mạng con

Dạng 1

Ví dụ 5.9:

Một host trên mạng được ghi nhận IP: 210.245.31.125/24.

a/ Chia mạng trên thành 6 mạng con?

b/ Cho biết số host trong mỗi mạng con?

c/ IP trên thuộc mạng nào, broadcast và subnet mask của nó?

Giải:

a/ Nhận dạng lớp: $192 \leq 210 \leq 223$

$\Rightarrow$ IP trên thuộc lớp C

Subnet mask default (SMD) có 24 bit 1

SM = SMD

$\Rightarrow$ IP trên chưa chia mạng con

Chia làm 6 mạng con nên mượn 3 bit vì $2^3 - 2 = 6$

> Lưu ý: Chia lần đầu tiên, số mạng chia (NNs) = $2^{\text{số bit mượn}} - 2$ (vì không sử dụng mạng đầu và cuối), chia nhỏ hơn nữa NNs = $2^{\text{số bit mượn}}$.

$\Rightarrow$ Số bit mượn = 3 (bit)

$\Rightarrow$ Số bit host-id = 8 – 3 = 5 (bit)

> Lưu ý: phần host-id chưa chia mạng lớp C có 8 bit mượn 3 bit nên còn 5 bit.

⇒ Bước nhảy Octet z: BNz = 2^5 = 32

∗ **Chia làm 6 net như sau:**

~~Net 0~~	NN:	210.245.31.0/27	Net 4	NN:	210.245.31.128/27
	B:	210.245.31.31/27		B:	210.245.31.159/27
Net 1	NN:	210.245.31.32/27	Net 5	NN:	210.245.31.160/27
	B:	210.245.31.63/27		B:	210.245.31.191/27
Net 2	NN:	210.245.31.64/27	Net 6	NN:	210.245.31.192/27
	B:	210.245.31.95/27		B:	210.245.31.223/27
Net 3	NN:	210.245.31.96/27	~~Net 7~~	NN:	210.245.31.224/27
	B:	210.245.31.127/27		B:	210.245.31.255/27

Net 0 và Net 7 không sử dụng, vậy đã chia làm 6 net từ net 1 đến net 6

Lưu ý: bước nhảy là 32, mạng đầu tiên khi chưa chia bắt đầu từ 0, cộng thêm 31.

b/ Số host trong một mạng (hosts):

Hosts = $2^5 – 2$ = 30 (host)

Lưu ý: Hosts = $2^{\text{số bit host-id}}$ -2 (trừ đi địa chỉ đầu NN và địa chỉ cuối B).

c/ 210.245.31.125

Lưu ý: chỉ quan tâm đến octet có mask, là octet z.

210.245.31.011|11101

Lưu ý: 127 = 01111111, mà 125 kém 127 là 2. Tức là tắt bit 2 về 0 hay 125 = 01111101

⇒ NN = 210.245.31.011|00000 = 210.245.31.96

Lưu ý: NN = tắt tất cả các bit thuộc phần host-id về 0.

$\Rightarrow$ B = 210.245.31.011|11111 = 210.245.31.127

Lưu ý: B = bật tất cả các bit thuộc phần host-id lên 1.

$\Rightarrow$ SM = 255.255.255.111|00000 = 255.255.255.224

Lưu ý: SM = bật tất cả các bit thuộc phần network-id và subnet-id lên 1. Tắt tất cả các bit thuộc phần host-id về 0.

Ví dụ 5.10:

Một host trong mạng được ghi nhận địa chỉ IP như sau: 169.254.87.1 /16

a/ Chia mạng trên thành 2 mạng con?

b/ Cho biết số host trong một mạng?

c/ IP trên thuộc mạng nào, broadcast và subnet mask của nó?

Giải:

a/ Nhận dạng lớp: $128 \le 169 \le 191$

IP trên thuộc lớp B

Subnet mask default (SMD) có 16 bit 1

SM = SMD nên IP trên chưa chia mạng con

Chia làm 2 mạng con nên mượn 2 bit vì $2^2 - 2 = 2$

$\Rightarrow$ Số bit mượn = 2 (bit)

$\Rightarrow$ Số bit phần host-id = 16 – 2 = 14 (bit)

Lưu ý: phải xác định Mask nằm ở octet nào và chỉ làm việc trên octet đó mà thôi.

Số bit phần host-id thuộc octet y = 8 – 2 = 6

Bước nhảy của octet y: BNy = 2^6 = 64

∗ Chia làm 2 net như sau:

~~Net 0~~	NN:	169.254.0.0/18	Net 2	NN:	169.254.128.0/18
	B:	169.254.63.255/18		B:	169.254.191.255/18
Net 1	NN:	169.254.64.0/18	~~Net 3~~	NN:	169.254.192.0/18

B: 169.254.127.255/18 B: 169.254.255.255/18

Net 0 và Net 3 không sử dụng, vậy có 2 net là Net 1và Net 2

b/ Số host trong một mạng (hosts):

Hosts = $2^{14} – 2 = 16382$ (host)

Lưu ý: cách tính $\boldsymbol{2^{10} = 1024}$, $2^{11} = 2048$, $2^{12} = 4096$, $2^{13} = 8192$, $2^{14} = 16384$.

c/ 169.254.87.1

169.254.01|010111.1

NN: 169.254.01|000000.00000000 = 210.245.64.0

B: 169.254.01|111111.11111111 = 210.245.127.255

SM: 255.255.11|000000.00000000 = 255.255.192.0

Dạng 2

Ví dụ 5.11:

Một host trên mạng được ghi nhận địa chỉ IP: 203.113.188.67 / 255.255.255.224

a/ Địa chỉ IP trên có chia mạng con hay không?

b/ Chia bao nhiêu mạng con (NNs)?

c/ Mỗi mạng con có bao nhiêu host (hosts)?

d/ NN, B, và các IP cùng mạng với IP trên?

Giải:

a/ Nhận dạng lớp: $192 \le 203 \le 223$

thuộc lớp C

SMD = 255.255.255.0

SM khác SMD nên có chia mạng con

b/ Số khó chịu 224 = 111|00000

Số bit mượn octet z = 3

NNs = $2^3 – 2 = 6$ (net)

c/ số bit phần host-id = 8 – 3 = 5 (bit)

Hosts = $2^5 -2 = 30$ (host)

d/ 203.113.188.67

203.113.188.010|00011

NN: 203.113.188.010|00000 = 203.113.188.64

B: 203.113.188.010|11111 = 203.113.188.95

Các IP cùng mạng với IP trên: 203.113.188.65 đến 203.113.188.94

Lưu ý: các IP cùng mạng trong khoản dưới NN và trên B.

Dạng 3

Ví dụ 5.12:

Hai host trên mạng được ghi nhận địa chỉ IP như sau:

IP1: 170.204.138.2/255.255.192.0

IP2: 170.204.181.244/255.255.192.0

a/ hai IP1 và IP2 có cùng mạng hay không?

b/ NN, B của mạng có IP1 và IP2?

Giải:

a/ Nhận dạng lớp: $128 \leq 170 \leq 191$

$\Rightarrow$ Lớp B

SMD: 255.255.0.0

SM khác SMD

$\Rightarrow$ Có chia mạng con

Số khó chịu 192 = 11|000000

$\Rightarrow$ Mượn 2 bit của octet y

IP1: 170.204.10|001010.2

IP2: 170.204.10|110101.224

SM: 255.255.11|000000.0

Phần network-id và subnet-id của IP1 và IP2 giống nhau

$\Rightarrow$ IP1 và IP2 cùng mạng con

b/ NN: 170.204.10|000000.0 = 170.204.128.0

B: 170.204.10|111111.255 = 170.204.191.255

Dạng 4

Ví dụ 5.13:

Một host trong mạng được ghi nhận địa chỉ IP: 171.154.86.55 /16

a/ Chia mỗi mạng con có 1024 (host), có bao nhiêu mạng con, số host trong mỗi mạng?

b/ IP trên thuộc mạng con nào NN, B, SM?

Giải:

a/ Nhận dạng lớp: $128 \leq 171 \leq 191$

$\Rightarrow$ Lớp B

SMD: có 16 bit

SMD = SM

$\Rightarrow$ Chưa chia mạng con

$2^{11} - 2 = 2046 >= 1024$

Lưu ý: nếu lấy 10 bit: $2^{10} - 2 = 1022$ không đáp ứng đề bài.

Số bit phần host = 11

Số bit mượn = 16 – 11 = 5

$\Rightarrow$ Số mạng con = $2^5 - 2 = 30$ (mạng)

$\Rightarrow$ Số host trong một mạng = $2^{11} - 2 = 2046$ (host)

b/ 171.154.01010|110.55

NN: 171.154.01010|000.0 = 171.154.80.0

B: 171.154.01010|111.255 = 171.154.87.255

SM : 255.255.11111|000.0 = 255.255.248.0

Dạng 5

Ví dụ 5.14:

Một host trên mạng được ghi nhận địa chỉ IP: 169.150.144.56 / 16

Hãy chia làm 1 mạng có 2^{14} -2 (host) và 2 mạng có $2^{13} - 2$ (host)?

Giải:

Nhận dạng lớp: $128 \leq 169 \leq 191$

$\Rightarrow$ Lớp B

SMD có 16 bit

SMD = SM

⇒ Chưa chia mạng con

Chia một mạng có $2^{14} - 2$ (host)

Số bit phần host-id = 14

⇒ Số bit mượn = 16 – 14 = 2

Mượn 2 bit của octet y

⇒ Số bit phần host-id của octet y = 8 – 2 = 6

⇒ Bước nhảy của octet y: BNy= $2^6 = 64$

∗ **Chia làm 2 net như sau:**

~~Net 0~~	NN:	169.150.0.0/18	Net 2	NN:	169.150.128.0/18
	B:	169.150.63.255/18		B:	169.150.191.255/18
Net 1	NN:	169.150.64.0/18	~~Net 3~~	NN:	169.150.192.0/18
	B:	169.150.127.255/18		B:	169.150.255.255/18

Net 0 và Net 3 không sử dụng, vậy có Net 1 và Net 2

Net 1 có 2^{14} - 2 (host) thỏa đề bài

Chọn Net 2 chia tiếp tục sao cho mỗi host có $2^{13} - 2$ (host)

Số bit phần host-id = 13

⇒ Số bit mượn = 14 – 13 = 1

Mượn 1 bit của octet y

Số bit phần host-id của octet y = 6 – 1 = 5

⇒ BNy = $2^5 = 32$

∗ **Chia làm 2 net như sau:**

Net 2.0	NN:	169.150.128.0/19	Net 2.1	NN:	169.150.160.0/19
	B:	169.150.159.255/19		B:	169.150.191.255/19

⇒ Có 2 net và mỗi net có $2^{13} - 2$ (host)

> Lưu ý: khi chia nhỏ mạng con từ lần thứ 2 trở đi không bỏ mạng đầu và cuối.

Dạng 6

Hãy gom các IP sau thành một mạng

IP1: 10.35.245.31/11

IP2: 10.67.210.30/11

IP3: 10.100.188.113/11

Giải:

Nhận dạng lớp octet w = 10 (nằm trong khoảng 1 đến 126)

⇒ Thuộc lớp A

SM = 11 ≠ SMD = 8

⇒ Có chia mạng con

⇒ Số bit mượn của octet x = 11 – 8 = 3 (bit)

IP1: 10.001|00011.245.31

IP2: 10.010|00011.210.30

IP3: 10.011|00100.188.113

Subnet-id của 3 IP khác nhau nên khác mạng. Nếu muốn 3 IP này cùng mạng thì phần network-id và subnet-id phải giống nhau. phần giống nhau là 10.0 lúc này chỉ còn mượn 1 bit. Khi đó chỉ cần sửa lại SM cho các IP là 255.128.0.0

IP1: 10.35.245.31/9

IP2: 10.67.210.30/9

IP3: 10.100.188.133/9

Cả 3 thuộc mạng 10.0.0.0/9

Lưu ý: Địa chỉ IP của 3 host không đổi, chỉ cần sửa SM lại là 3 host cùng mạng với nhau.

IPv6

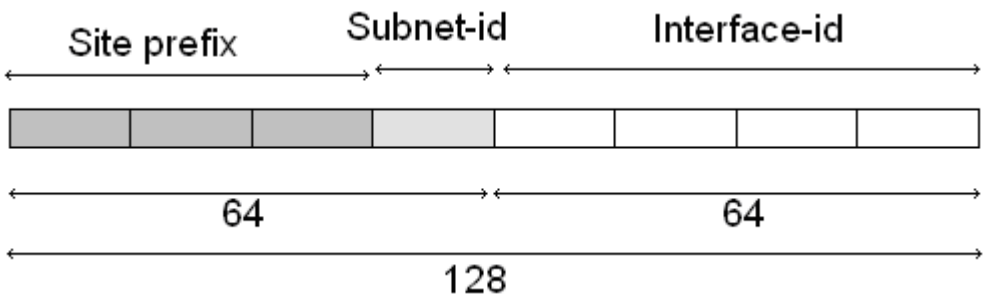
Cấu trúc của IPv6

Tổng cộng 128 bit, 64 bit đầu là phần network, 64 bit sau là phần interface-id

∗ Phần network để xác định các subnet, do ISP hoặc các tổ chức quản lý IANA gán. Được chia là 2 phần:

- Site prefix giống như network-id trong IPv4, được ISP gán cho một site (vị trí). Vậy các máy cùng một site có cùng Site prefix (giống như chưa chia mạng con).
- Subnet-id giống như subnet-id trong IPv4, mô tả các mạng con bên trong.

∗ Interface-id giống địa chỉ host trong IPv4, là địa chỉ ngẫu nhiên dựa vào 48 bit của địa chỉ MAC.



Hình 5. 23 - Cấu trúc của IPv6

∗ Chia là 8 nhóm, mỗi nhóm 2 byte, biểu diễn bằng 4 ký tự thập lục phân (từ 0 đến F). Ký pháp không phân biệt hoa thường, cách nhau bởi dấu hai chấm. Phần cuối chỉ ra độ dài của phần prefix. ví dụ: 2011:0ace:0000:0000:0000:1974:0000:7979/48

∗ Hai nguyên tắc viết rút gọn.

- Trong mỗi nhóm, có thể bỏ các số 0 đứng đầu.
- Được phép thay (một lần duy nhất) một dãy số 0 liên tiếp thành ::
  Với ví dụ trên, có thể viết thành 2011.ace::1974:0:7979.
  – 0ace → ace
  – 0000:0000:0000 → ::
  – 0000 → 0 (không thể thay thành ::, vì đã dùng một lần rồi).

∗ 32 bit cuối của IPv6 là IPv4, đối với các thiết bị tương thích IPv6 thì sẽ chấp nhận các gói tin IPv4.

Để biểu diễn cho IPv4: 192.168.1.100

0000:0000:0000:0000:0000:FFFF:C0A8:0164

C0 = 12 * 16^1 + 0 * 16^0 = 192

A8 = 10 * 16^1 + 8 * 16^0 = 168

01 = 0 * 16^1 + 1 * 16^0 = 1

64 = 6 * 16^1 + 4 * 16^0 = 100

Có thể viết gọn thành

::ffff:c0a8:0164 hoặc ::ffff:192.168.1.100

Một số đặc điểm

∗ Có 128 bit không gian địa chỉ là (340 tỉ tỉ tỉ tỉ)

2^{128} ≈ 340.000.000.000.000.000.000.000.000.000.000.000

∗ Không có khái niệm IP private, không cần cơ thế NAT để ra Internet cũng như không thể che dấu IP bên trong mạng. Điều này hạn chế kỹ thuật fake IP của hacker.

∗ Cấu trúc đơn giản nên hoạt động hiệu quả hơn, tránh được tình trạng tràn ngập gói tin quảng bá (broadcast storm).

∗ Tương thích với IPv4.

∗ Hiện nay IANA tuyên bố hết IPv4, các nước đã tiến hành chuyển các kết nối mạng lớn sang IPv6.

Các loại địa chỉ IPv6

Địa chỉ Unicast

Dùng đánh cho một interface, là một địa chỉ duy nhất trên mạng. Gói tin mang địa chỉ đích là Unicast thông qua router sẽ được chuyển đến một interface duy nhất. Được chia là 4 loại:

∗ Link-local: phạm vi hoạt động trong một nhánh mạng, không được định tuyến qua router. Dùng để giao tiếp các máy tính trong cùng một mạng. 10 bit đầu luôn là 1111.1110.10, 54 bit sau là 0.

Như vậy phần prefix luôn không thay đổi: fe80::/64

```
Physical Address. . . . . . . . . : C0-A8-79-01
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : fe80::5efe:192.168.121.1%2
```

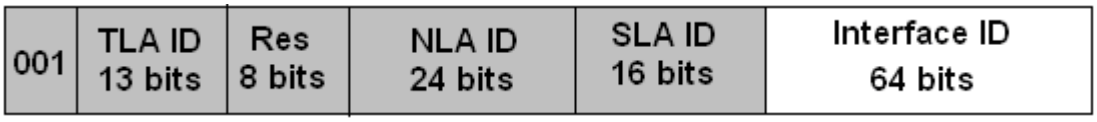
Hình 5. 24 - Unicast Link-local

Ở hình 5.24, dùng lệnh ping xác định được IPv6 link-local.

∗ Site-local: phạm vi hoạt động trong một mạng LAN,. giống địa chỉ private trong IPv4, không được định tuyến qua router. 10 bit đầu luôn là 1111.1110.11 54 bit sau là subnet-id.

Frefix: fec0::/10

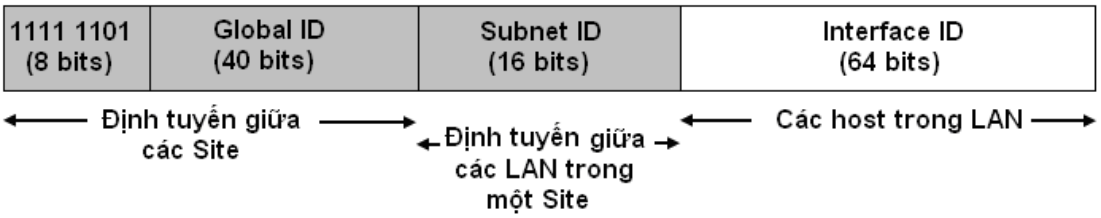
∗ Global: phạm vi hoạt động toàn cầu, giống địa chỉ public trong IPv4. 3 bit đầu luôn là 001.



Hình 5. 25 - Cấu trúc Unicast Global

- TLA ID (Top Level Aggregation): xác định nhà cung cấp dịch vụ cao nhất.
- Res: chưa sử dụng.
- NLA ID (Next Level Aggregation): xác định nhà cung cấp dịch vụ tiếp theo.
- SLA ID (Site Level Aggregation): xác định các site để tạo các subnet.

∗ Unique-local: là địa chỉ định tuyến giữa các subnet trong LAN. 8 bit đầu tiên luôn có giá trị là 1111 11101, FD00::/8. 40 bit sau là địa chỉ site, 16 bit tiếp theo là địa chỉ subnet.



Hình 5. 26 - Cấu trúc địa chỉ Unique-local IPv6

Địa chỉ Anycast

Là địa chỉ được gán cho một nhóm thiết bị, khi gói tin mang địa chỉ đích là anycast nó sẽ được chuyển đi theo cấu trúc định tuyến đến thiết bị gần nhất. Địa chỉ này không được gán cho địa chỉ nguồn. Thường địa chỉ anycast được gán cho các router thuộc một tổ chức nào đó.

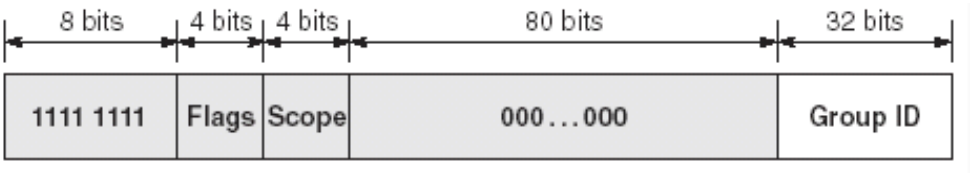
Địa chỉ anycast không có không gian địa chỉ riêng mà khi địa chỉ unicast được gán đồng thời cho nhiều thiết bị, nó trở thành địa chỉ anycast.

ví dụ: ISP cung cấp dịch vụ phân giải tên miền cho khách hàng. Khách hàng chỉ cần nhớ 1 địa chỉ của DNS server và nhờ server này phân giải. Nhưng thực chất ISP có rất nhiều server và gói tin người dùng được định tuyến đến server gần nhất để yêu cầu phân giải tên.

Địa chỉ Multicast

Là địa chỉ để nhận dạng một nhóm các thiết bị, nó thay thế cho địa chỉ multicast và broadcast trong IPv4. 8 bit đầu là 1111 1111, FF00::/8, 4 bit sau là flags, 4 bit tiếp theo là scope.

Có rất nhiều dạng địa chỉ multicast tùy theo phạm vi hoạt động của nó: phạm vi node, phạm vi link (subnet), phạm vi site (LAN)...



Hình 5. 27 - Cấu trúc địa chỉ Multicast IPv6

∗ **Flags:**

0000: Well-Known

0001: Transient

∗ **Scope:**

0001: Node-local

0010: Link-local

0101: Site-local

1000: Organization-local

1111: Global

Các địa chỉ IPv6 tương thích với IPv4

Địa chỉ tương thích được định nghĩa nhằm mục đích chuyển đổi từ IPv4 sang IPv6, được xây dựng từ IPv4.

– IPv4-compatible: 0:0:0:0:0:0:w.x.y.z hay ::w.x.y.z

ví dụ: ::192.168.1.1

– IPv4-Mapped: 0:0:0:0:0:FFFF:w.x.y.z hay ::FFFF:w.x.y.z

ví dụ: ::FFFF:192.168.1.1

– 6to4: IANA cấp phát một prefix 2002::/16 dành riêng trong vùng địa chỉ có 3 bit đầu là 001 (vùng địa chỉ unicast toàn cầu). Địa chỉ này dùng để chuyển đổi giao tiếp IPv4-IPv6 rất tiện dụng có tên gọi là công nghệ tunnel 6to4, sử dụng trong giao tiếp giữa hai node mạng chạy đồng thời cả hai thủ tục IPv4 và IPv6 trên cơ sở hạ tầng định tuyến IPv4.

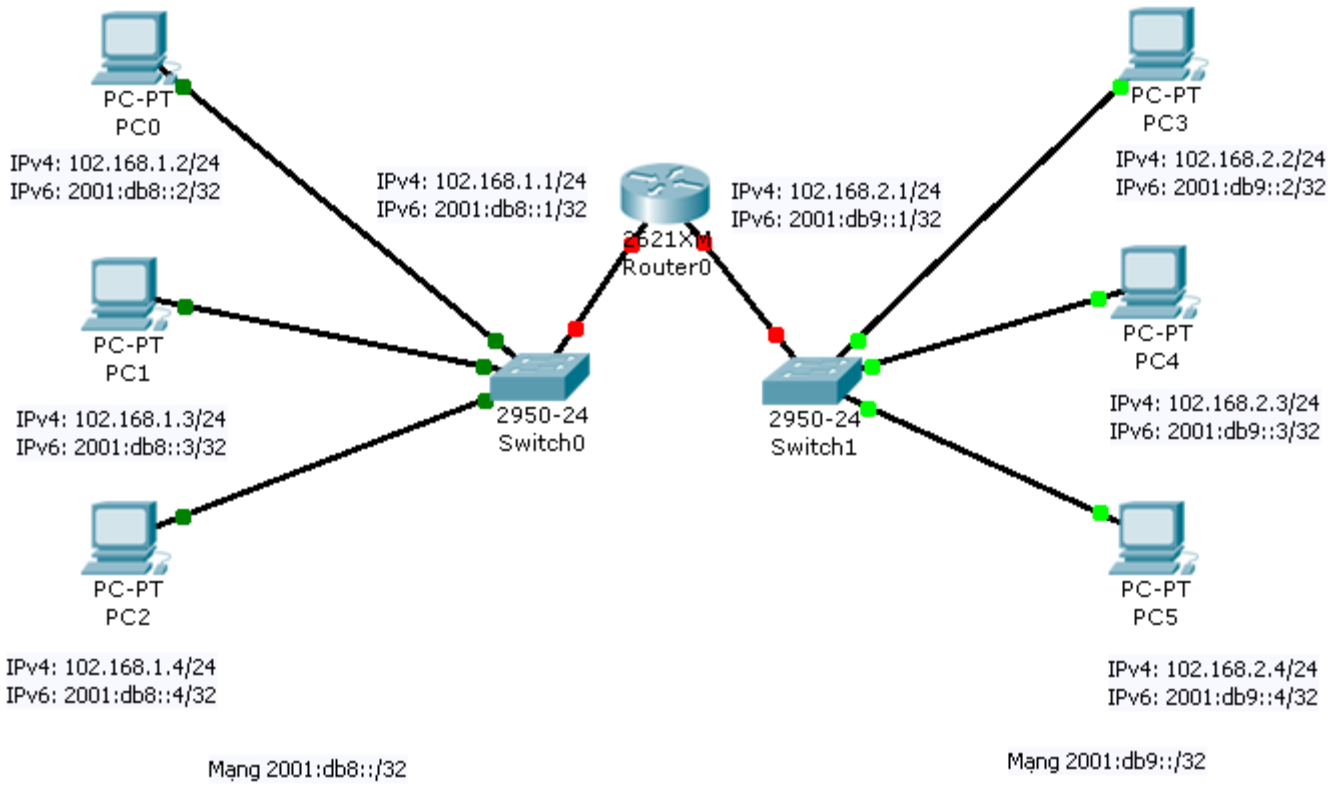
Được hình thành bằng cách gắn prefix 2002::/16 với 32 bit của IPv4 (viết theo dạng hexa) tạo thành prefix /48.

ví dụ: IPv4 là 192.168.1.1 chuyển thành IPv6 là 2002:C0A8:0101::/48

Bảng 5.2 - Tóm tắt IPv6

Địa chỉ	Cấu trúc	Mô tả
Link-local	::/128	Địa chỉ không xác định dùng trong thủ tục kiểm tra trùng lặp địa chỉ link local
Link-local	::1/128	Địa chỉ Loopback
Link-local	Fe80::/10	Địa chỉ chỉ được dùng trong một mạng, tương tự Apipa trong IPv4 (169.254.0.0/16)
Site-local	Fc00::/7	Địa chỉ này có thể dùng trong hệ thống liên mạng
Multicast	Ff00::/8	Prefix của địa chỉ multicast
IPv4	::ffff:w.x.y.z/96	Địa chỉ tương thích IPv4-Mapped
IPv4	2002::/16	Địa chỉ tương thích 6to4
IPv4	::w.x.y.z/96	Địa chỉ tương thích IPv4-Compatible
	2001:db8::/32	Địa chỉ được sử dụng làm ví dụ trong các tài liệu về IPv6
Global	Các địa chỉ IPv6 còn lại	Đùng định tuyến giữa các Site

Ví dụ triển khai IPv6



Hình 5. 28 - Triển khai IPv6 cho 2 mạng

Câu hỏi và bài tập

1. Vẽ bảng tóm tắc 3 lớp IP A, B, C?
2. Hãy nêu các khái niệm: network-id, host-id, subnet-id, subnet mask, subnet mask default, broadcast?
3. Trình bày các địa chỉ IP của 3 lớp A, B, C không được đánh cho host?
4. Vẽ bảng tóm tắt IPv6?
5. Trình bày khái niệm địa chỉ private và public, cơ chế nào cho phép chuyển đổi giữa hai dạng địa chỉ?
6. Vẽ hình và triển khai một mạng với 5 đoạn mạng dùng IPv6.
7. Phân tích câu "Tôi thấy chia IP còn tốn IP hơn", nói vậy đúng hay sai?
8. Một host trên mạng được ghi nhận IP: 10.76.67.125/8
   a. Chia mạng trên thành 6 mạng con hợp lệ?
   b. Cho biết số host trong một mạng?
   c. IP trên thuộc mạng nào, broadcast và subnet mask của nó?
9. Hai host trên mạng được ghi nhận địa chỉ IP như sau

   IP1: 159.104.194.21

   IP2: 159.104.187.22

   SM: 255.255.224.0

   a. Hai IP1 và IP2 có cùng mạng hay không?
   b. NN, B của mạng có IP1, IP2?
10. Một host trên mạng được ghi nhận IP như sau 129.154.130.55/16
    a. Chia mỗi mạng con có tối thiểu 1024 (host), có bao nhiêu mạng con, số host trong mỗi mạng?
    b. IP trên thuộc mạng con nào NN, B, SM?
11. Trả lời các câu hỏi sau:
    a. Địa chỉ IP ở lớp B có subnet mask là 255.255.255.224 Có bao nhiêu mạng con hợp lệ và mỗi mạng có bao nhiêu host?
    b. Cho biết subnet mask thuộc lớp B cho phép số mạng con hợp lệ trên 164 và số host trong mỗi mạng trên 150.
    c. Cho biết địa chỉ IP nào sau đây là địa chỉ IP của lớp C?
       - 1.1.1.1
       - 200.1.1.1
       - 128.128.128.128
       - 224.1.1.1
       - 223.223.223.255

    d. Giá trị của octet đầu tiên của lớp A là đoạn nào?
12. Hãy ghép các IP sau đây, sao cho các host mang các IP này cùng mạng:
    IP1: 178.226.42.44/22
    IP2: 178.266.44.78/22
    IP3: 178.266.35.82/22
    IP4: 178.266.39.69/22

PHẦN 2 - QUẢN TRỊ MẠNG

MÔ HÌNH WORKGROUP

∗ Tóm tắt nội dung chương 6

Quản lý user trong Windows 7.

Quản trị tài nguyên mạng trong môi trường Workgroup (thư mục, ổ đĩa, máy in).

∗ Mục tiêu chương 6

Sau khi học xong sinh viên có khả năng:

Quản lý user trong Windows 7.

Chia sẻ, quản lý và bảo mật cho folder, drive và printer.

Giới thiệu hệ điều hành (OS) dùng cho client

Trong mô hình Workgroup, các máy cài đặt các OS dùng cho cho client hoạt động trong mạng ngang hàng (Peer to Peer). Các máy tính sử dụng loại OS này chỉ có một loại user duy nhất được sử dụng gọi là local user. User của máy nào chỉ có thể đăng nhập vào máy đó mà thôi.

Tài nguyên local muốn trở thành tài nguyên mạng, phải được chia sẻ (share). Việc chia sẻ tài nguyên này do Administrator của từng máy quản lý. Khi một máy khác muốn sử dụng tài nguyên mạng của máy nào đó, thì phải có 2 quyền chính.

Quyền hệ thống (rights): máy đó phải chứng thực bằng một user của máy đang giữ tài nguyên mạng.

Quyền truy cập (permission): sau khi đã chứng thực vào hệ thống bằng một user, thì việc sử dụng tài nguyên phụ thuộc vào quyền của user đó trên hệ thống.

Các OS dùng cho client cung cấp một số dịch vụ cơ bản để phục vụ cho các máy khác trên mạng (như: chia sẻ Internet, truy cập từ xa, dịch vụ web...). Các dịch vụ này cung cấp cho số ít người dùng và ít tính năng hỗ trợ cũng như bảo mật.

∗ Các OS dùng cho client của Microsoft: Windows XP, Windows Vista, Windows 7...

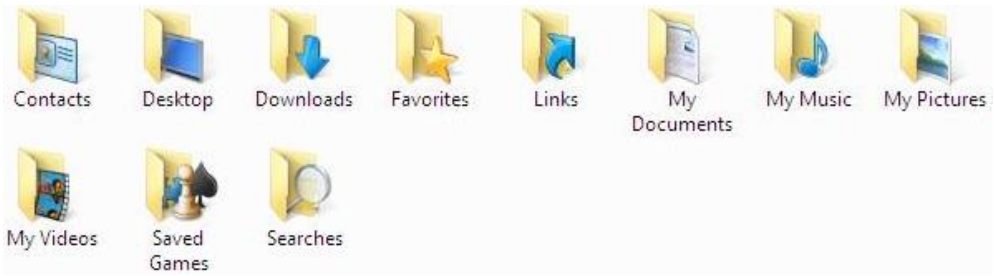
∗ Các OS mã nguồn mở: Ubuntu, Slackware, Caldera Open Linux, Su.S.E Linux, Debian, CentOS, Fedora...

Quản trị user account trên Windows 7

Một máy tính có thể có nhiều người sử dụng. Mỗi người sử dụng sẽ được quản trị viên tạo ra một user account (gọi tắt là user). Một user bao gồm một username và password để chứng thực vào hệ thống. Mỗi user sẽ có một profile (là một folder cùng tên với user) được lưu trong %Systemdrive%\Documents and Settings\%Username% hay %Userprofile% (xem bảng 6.1).

Profile của user là nơi lưu tất cả các cấu hình (Start Menu, Desktop...), lưu dữ liệu của người dùng (UserData, My Document...), đồng thời lưu các thông tin ẩn của người dùng (Internet Explorer, Microsoft Outlook...).

User chỉ có quyền sử dụng profile của mình (hoặc All User), việc này đảm bảo tính cá nhân khi nhiều người sử dụng chung máy tính. Administrator được quyền xem tất cả các profile.



Hình 6. 1 – Profile của u1

Bảng 6.1: Bảng một số biến môi trường hay dùng trong Windows

Biến môi trường	Ý nghĩa	Ví dụ
%Systemdrive%	Ổ đĩa hệ thống	C:
%Systemroot%	Thư mục gốc	C:\WINDOWS
%Systemdirectory%	Thư mục hệ thống	C:\WINDOWS\SYSTEM32
%Username%	Tên user	u1
%Userprofile%	Profile của user	C:\Documents and Settings\u1
%Programfile%	Thư mục chương trình	C:\Program Files

Tạo user

Để tạo user, phải có quyền Administrator.

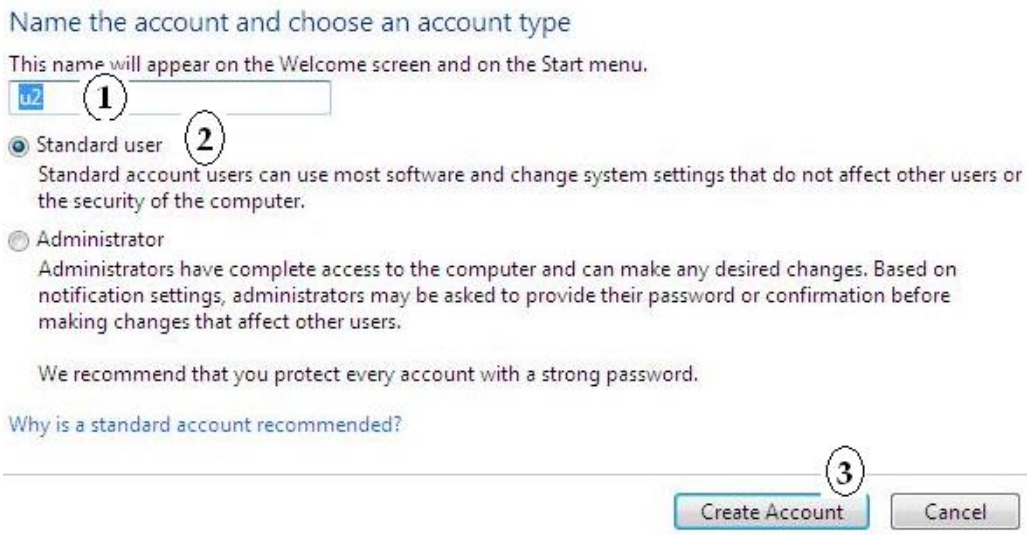
Vào <Start> → Chọn <Control Panel> → chọn <User Accounts> → chọn <Manage another account>.

Hộp thoại ***<User Accounts>***. Mặc nhiên khi cài Win7 xong có 2 account. Account được tạo khi cài đặt <u1> có quyền admin, account <Guest> bị khóa. → Chọn ***<Create a new account>*** → Nhập tên user cần tạo vào <New account name>.

Có 2 loại account.

- Standard user:
  Sử dụng hầu hết các phần mềm và các thay đổi hệ thống, nhưng không thể tác động tới các user khác và hệ thống bảo mật của máy tính.
- Administrator
  Quyền quản trị hệ thống, tác động đến các user khác.

Chọn <***Standard user***> → Nhấn nút <***Create Account***>.



Hình 6. 2 - chọn loại User account

User u2 được tạo ra, logoff và logon vào u2, mở không được profile của u1 vì không có quyền.

Thay đổi một user

Vào ***<Start>*** → Chọn ***<Control Panel>*** → chọn ***<User Accounts>*** → Trong hộp thoại ***<User Acccounts>***, cho phép thay đổi tên, tạo (hoặc thay đổi) password, thay đổi Icon, thay đổi loại account (Administrator hay Standard).

Hình 6. 3 - Thay đổi User account

Xóa user

Để tạo user, phải có quyền Administrator.

Vào ***<Start>*** → chọn ***<Control Panel>*** → chọn ***<User Accounts>*** → chọn ***<Manage another account>*** → chọn account cần xóa → chọn <Delete the account>.

Có hai cách để xóa account.

– Keep Files: Trước khi xóa account, Windows sẽ tự động lưu nội dung Desktop, My Document... vào một folder trên Desktop với tên là tên account. Tuy nhiên,

Windows không lưu các thông số cấu hình (Microsoft Outlook, Internet favorites...).

– Delete Files: Trước khi xóa account, Windows sẽ xóa tất cả các thông tin liên quan đến account.

Bảo mật cho user

Để thiết lập bảo mật phải có quyền admin, thiết lập bảo mật để tránh hacker dò tìm password.

Vào <Start> → Chọn menu <Control Panel> → Chạy <Administrative Tools> → Chạy <Local Security Policy>.

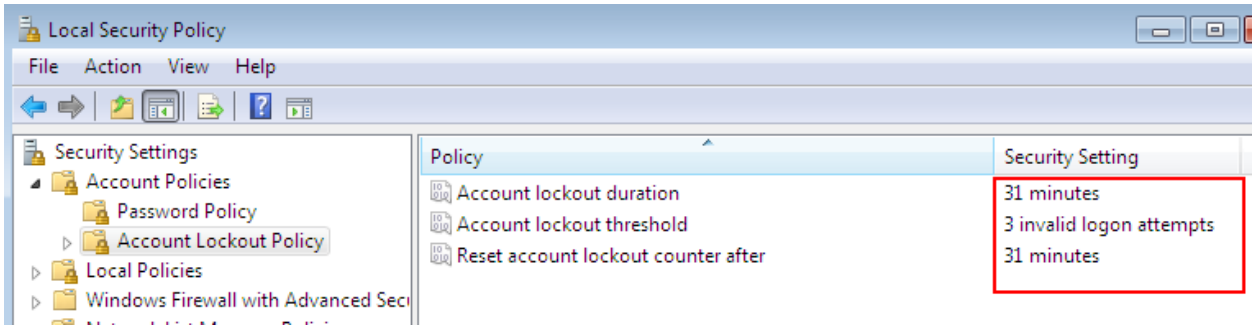
Hộp thoại ***<Local Security Settings>*** → Click vào dấu cộng ***<Account Policies>*** → Chọn ***<Account Lockout Policy>*** → thiết lập các thông số sau.

– Account lockout threshold: số lần đăng nhập sai password, lúc này tài khoản sẽ bị khóa. Mặc nhiên là giá trị 0 (không sử dụng)

– Account lockout duration: thời gian khóa tài khoản.

– Reset account lockout counter after: thời gian reset lại bộ đếm, thời gian này phải nhỏ hơn Account lockout duration.

Trong hình dưới: khóa Account nếu gõ sai password 3 lần, 31 phút sau tài khoản sẽ mở đồng thời với việc reset lại bộ đếm.



Hình 6. 4 - Account policies

Quản trị tài nguyên mạng (ổ đĩa, thư mục, máy in)

Trong mô hình Workgroup các máy trên mạng là máy Peer (tự quản lý tài nguyên của mình), nên user có quyền admin sẽ chia sẻ tài nguyên của mình cho các máy trên mạng sử dụng.

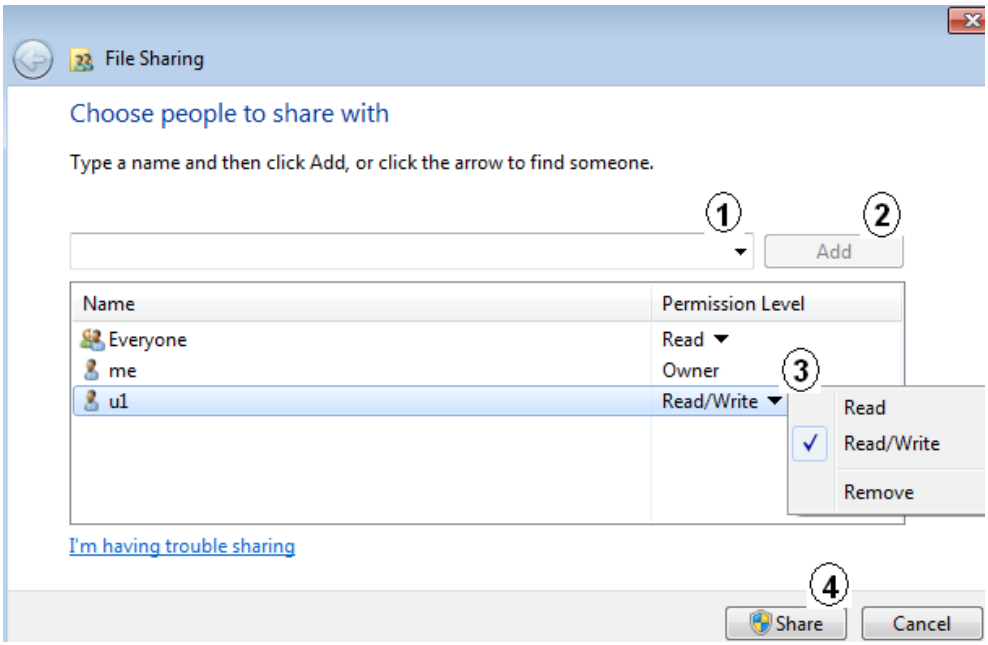
Chú ý: các user sử dụng tài nguyên mạng phải có password và các quyền trên hệ thống và quyền truy cập tài nguyên.

Chia sẻ tài nguyên ổ đĩa và thư mục

Việc chia sẻ tài nguyên ổ đĩa thường gặp là các ổ đĩa quang, ổ đĩa luận lý (partition). Chia sẻ ổ đĩa và folder cách làm giống nhau, các máy khác sử dụng các tài nguyên này như một folder dùng chung trên mạng.

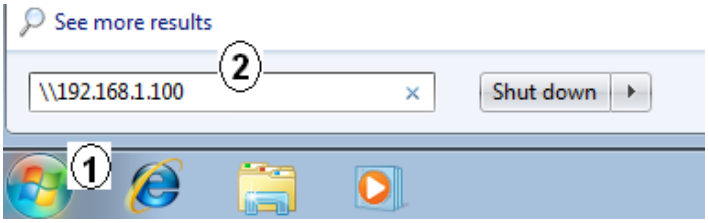
Phải chuột lên ổ đĩa cần chia sẻ → Chọn menu ***<Properties>*** → Chọn tab ***<Sharing>*** → Nhấn vào nút ***<Share>***

Click vào mũi tên xuống ***<Type a name...>*** chọn đối tượng cần chia sẻ (hoặc ghi tên vào) ***<u1>*** → Nhấn nút ***<Add>*** → Cấp quyền cho đối tượng ***<Permission Level>*** → Nhấn nút ***<Share>*** → Nhấn nút ***<Done>*** → Nhấn nút ***<Close>***.



Hình 6. 5 - Chia sẻ thư mục

Các máy cần sử dụng tài nguyên này thì kết nối vào máy chia sẻ. Vào ***<Start>*** → Nhập vào ***\\IP của máy chia sẻ*** (hoặc tên của máy chia sẻ) trong ***<Search...>*** → Nhấn phím <Enter>. Ở đây, phải dùng một user trên máy chia sẻ để kết nối (không dùng user máy mình).



Hình 6. 6 - Truy cập tài nguyên

Lưu ý: đường dẫn ***\\192.168.1.100*** được gọi là đường dẫn ***UNC*** là đường dẫn dùng để truy cập các tài nguyên trong mạng LAN.

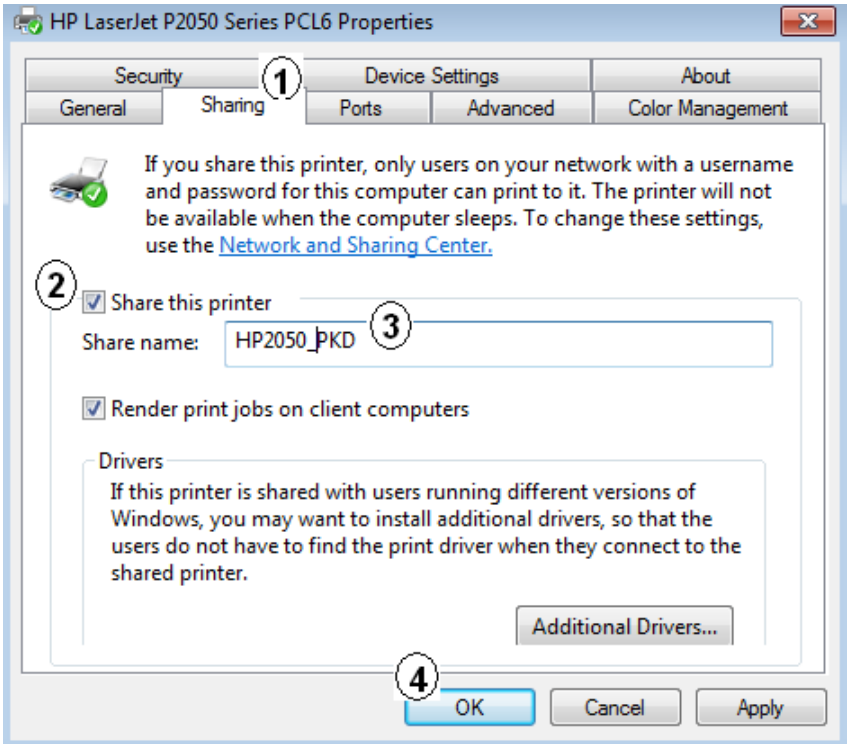
Có thể truy cập thẳng vào tài nguyên mạng khi biết tên chia sẻ của nó, ví dụ: \\192.168.1.34\shared

Dùng lệnh ***net share*** để xem các tài nguyên được chia sẻ trong hệ thống

Chia sẻ tài nguyên máy in

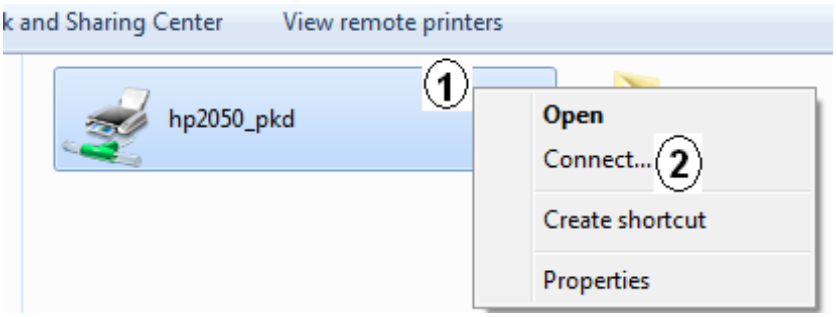
Máy in là thiết bị văn phòng đắt tiền, chiếm không gian và tốn chi phí bảo trì. Để máy in hoạt động hiệu quả, đúng mục đích máy in thường đặt tại một nơi tiện lợi, chia sẻ cho các máy sử dụng chung.

Vào ***<Start>*** → Chọn ***<Devices and Printers>*** → Phải chuột lên máy in cần chia sẻ ***<HP LaserJet P2050 Series PCL6>*** → Chọn menu ***<Printer Properties.>*** → Chọn tab ***<Sharing>*** → Check vào ***<Share this printer>*** → Điền vào tên tài nguyên gợi nhớ trong ***<Share name>*** → Nhấn nút ***<OK>.***



Hình 6. 7 - Chia sẻ máy in

Các máy cần sử dụng máy in mạng, Các máy cần sử dụng tài nguyên này thì kết nối vào máy chia sẻ. Vào ***<Start>*** → Nhập vào ***\\IP của máy chia sẻ*** (hoặc tên của máy chia sẻ) trong ***<Search...>*** → Nhấn phím <Enter***>*** → Phải chuột lên máy in mạng ***<hp2050_pkd>*** → chọn menu ***<Connect...>.***

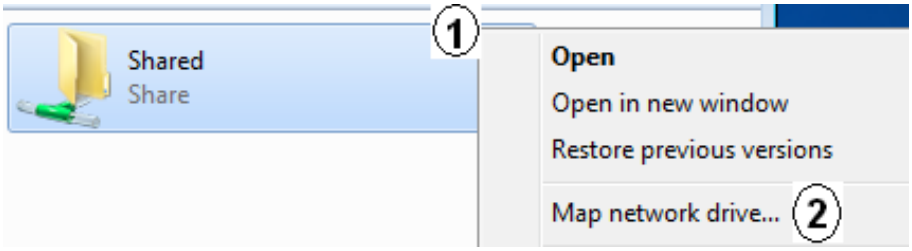


Hình 6. 8 - Sử dụng máy in mạng

Ánh xạ ổ đĩa mạng

Khi thường xuyên sử dụng một folder trên mạng nên ánh xạ chúng thành một ổ đĩa trên máy để sử dụng nhanh chóng và hiệu quả.

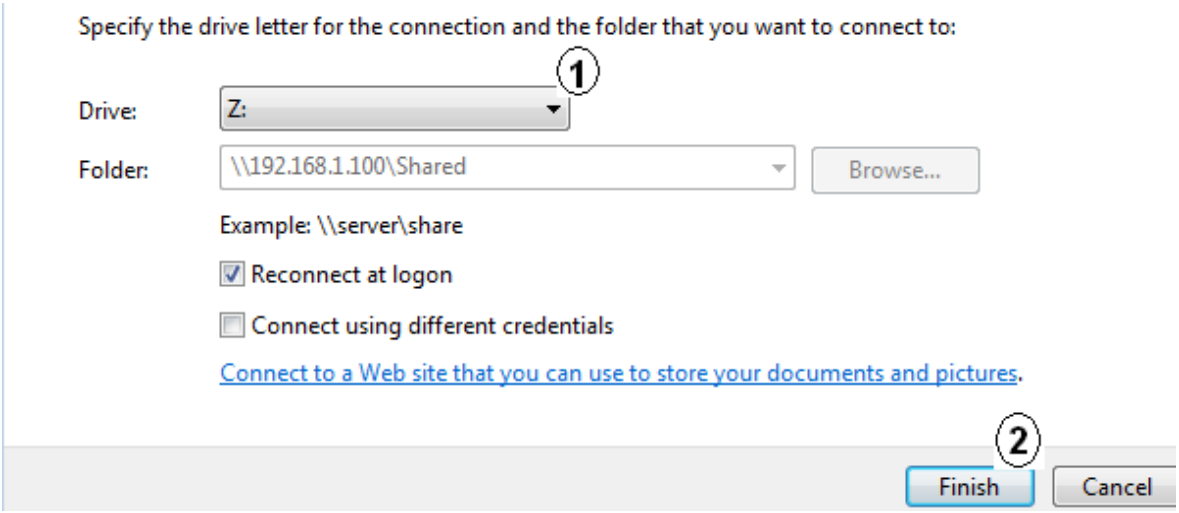
Phải chuột lên folder mạng cần ánh xạ ***<SharedDocs>*** → Chọn menu ***<Map Network Drive...>***.



Hình 6. 10 - Ánh xạ ổ đĩa mạng

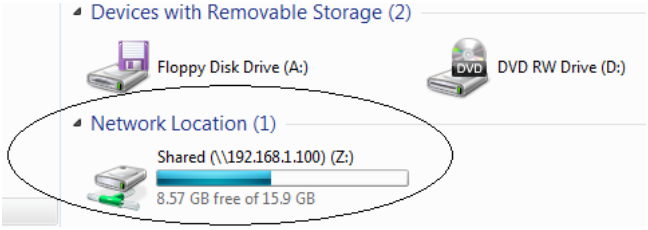
Lưu ý: tài nguyên mạng có biểu tượng nhánh mạng bên dưới.

Chọn nhãn cho ổ đĩa cần tạo trong ***<Drive>*** → nhấn nút ***<Finish>*** để hoàn tất.



Hình 6. 11 - Chọn ổ đĩa ánh xạ

Vào ***<My Computer>*** sẽ thấy ổ đĩa này.



Hình 6. 12 - Truy cập ổ đĩa ánh xạ

Lưu ý: dùng lệnh ***net use Z: \\192.168.1.34\SharedDocs*** để ánh xạ ổ đĩa mạng.

Bảo mật tài nguyên mạng (ổ đĩa, thư mục, máy in)

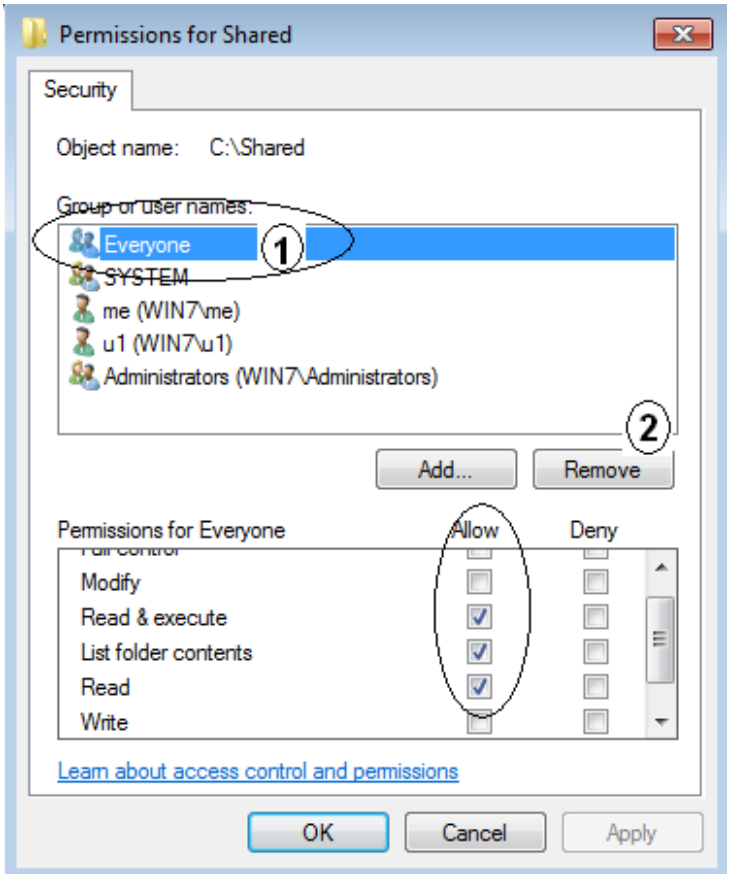
Bảo mật cho ổ đĩa và thư mục

Các tài nguyên mạng được chia sẻ với mục đích dùng chung. Nhưng nó phải sử dụng đúng mục đích. Vậy việc bảo mật trên các tài nguyên rất quan trọng.

– Giới hạn người truy cập (chia sẻ cho ai sử dụng).

– Giới hạn quyền truy cập (ai được quyền đọc, thêm, xóa, sửa...).

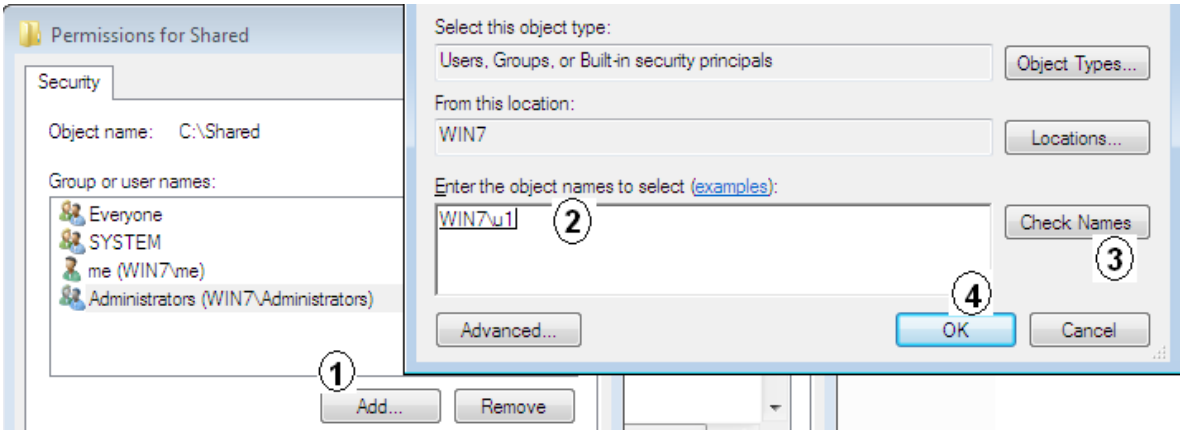
Phải chuột lên tài nguyên cần bảo mật (ví dụ folder Shared) → Chọn menu ***<Properties>*** → Chọn tab ***<Security>*** → Nhấn nút ***<Edit...>*** → Chọn nhóm ***<Everyone>*** trong ***<Groups or users names>,*** nhóm Everyone có quyền đọc và thực thi → Nhấn nút ***<Remove>,*** lúc này nhóm Everyone sẽ không có quyền gì trên tài nguyên này nữa (thử mở Shared ra sẽ được thông báo không có quyền "***You don't currently have permission to access this folder"***).



Hình 6. 13 - Xóa quyền nhóm Everyone

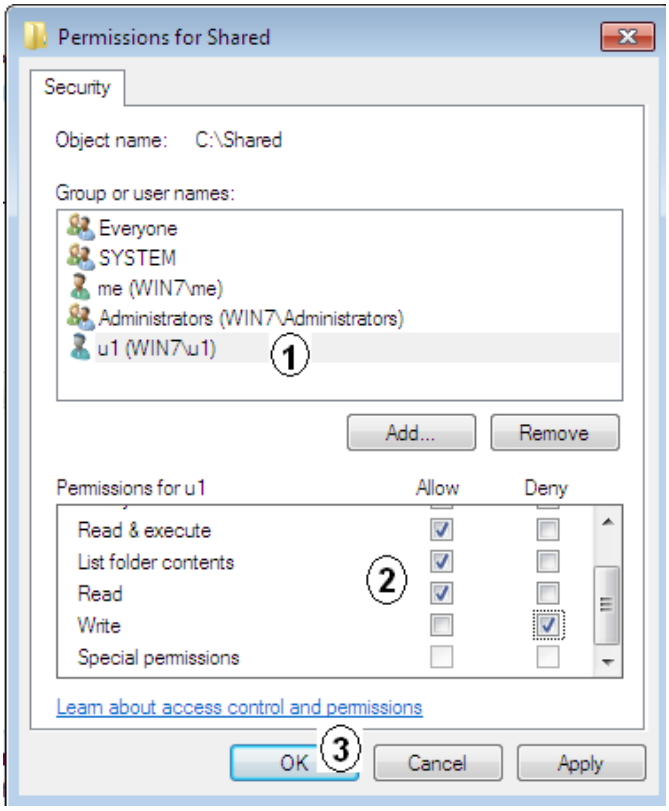
Bây giờ cho phép u1 đọc và thực thi folder này, nhưng cấm ghi lên folder này (nghĩa là cấm tạo thêm folder và file bên trong).

Trong hộp thoại ***<Permission for Shared>*** → Nhấn nút ***<Add...>*** → Hộp thoại ***<Select Users or Groups>*** hiện ra → Nhập vào ***<u1>*** trong ***<Enter the object name to select>*** → Nhấn nút ***<Check Names>,*** nếu u1 tồn tại trong hệ thống thì tên này sẽ có thêm đường dẫn và gạch chân → Nhấn nút ***<OK>.***



Hình 6. 14 - Thêm đối tượng u1 vào ACL

Chọn ***<u1>*** trong ***<Group or user names>*** → Ở cột ***<Allow>*** check vào ***<Read & Execute>*** (lúc này cả 2 check <List Folder Contents> và <Read> được tự động check theo, vì quyền đọc thực thi bao gồm cả quyền mở folder và đọc folder) → Ở cột ***<Deny>*** check vào ***<Write>*** → Nhấn nút ***<OK>***. Dùng máy khác, truy cập vào folder này (Shared). Mở thử folder, sau đó tạo một folder con và một file.

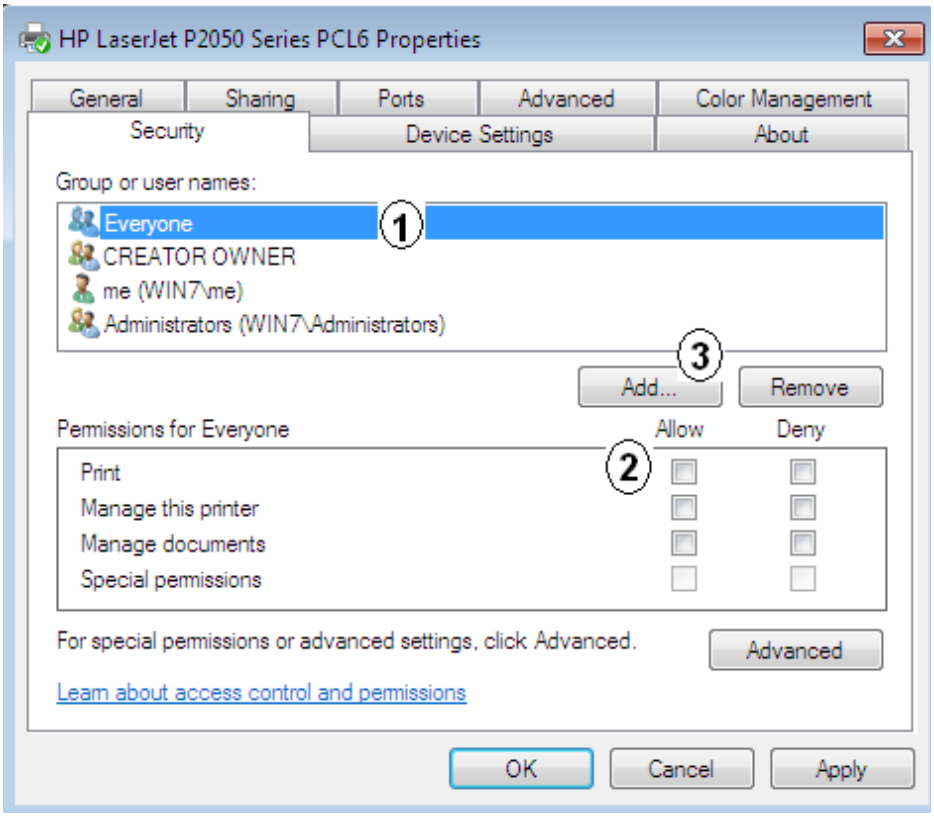


Hình 6. 15 - Cấp quyền cho u1

Bảo mật máy in

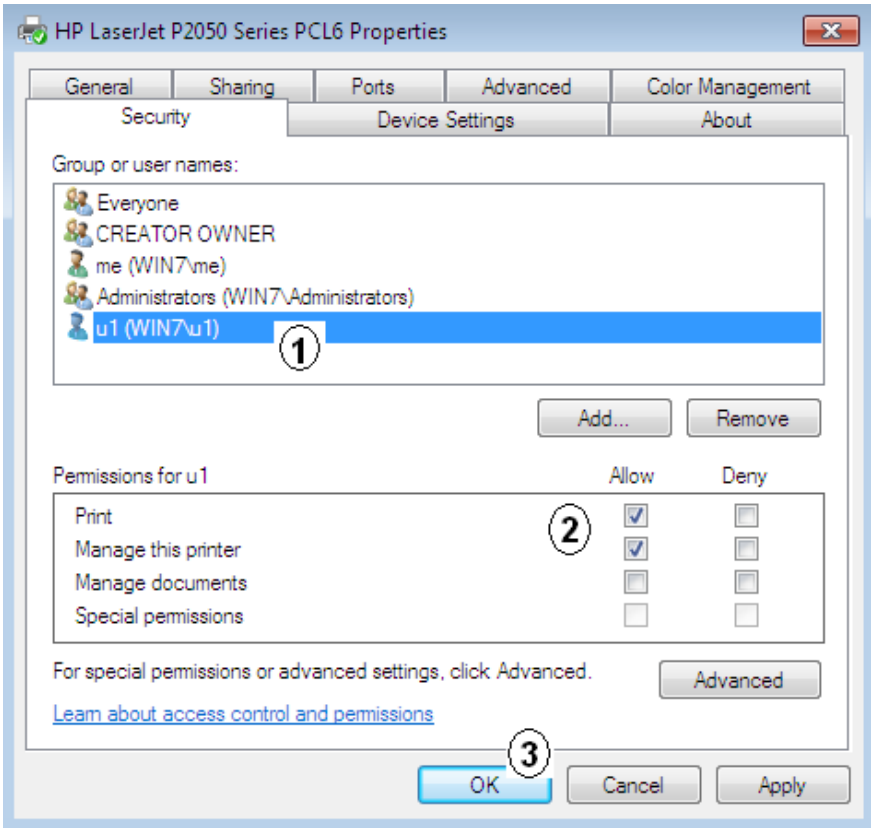
Tương tự như bảo mật ổ đĩa và thư mục. Việc bảo mật máy in nhằm mục đích sử dụng máy in một các hiệu quả, đúng mục đích và tiết kiệm chi phí văn phòng.

Vào ***<Start>*** → Chọn ***<Devices and Printers>*** → Phải chuột lên máy in cần bảo mật ***<HP LaserJet P2050 Series PCL6>*** → Chọn menu ***<Printer Properties>*** → Chọn tab ***<Security>*** → Chọn ***<Everyone>*** trong ***<Group or user names>,*** Mọi người đều có quyền in trên máy in này→ Ở cột ***<Allow>*** bỏ check ***<Print>*** → Nhấn nút ***<Add...>*** → Nhập vào ***<u1>*** trong ***<Enter the object name to select>*** → Nhấn nút ***<Check Names>,*** nếu u1 tồn tại trong hệ thống thì tên này sẽ có thêm đường dẫn và gạch chân → Nhấn nút ***<OK>.***



Hình 6. 16 - Xóa quyền in của Everyone

Chọn ***<u1>*** trong ***<Group or user names>*** → Ở cột ***<Allow>*** check vào ***<Print>*** và ***<Manage this Printer>,*** cho phép u1 in và quản lý máy in → nhấn nút ***<OK>.***



Hình 6. 17 - Cấp quyền in, quản lý máy in cho u1

Câu hỏi và bài tập

- Phân biệt các loại user trong Windows 7?
- Trình bày các biến môi trường hay sử dụng trong Windows?
- Trình bày ý nghĩa của Account lockout threshold, Account lockout duration, Reset account lockout counter after?
- Trình bày chi tiết các bước chia sẻ một folder?
- Trình bày chi tiết các bước chia sẻ một printer?
- Trình bày chi tiết các bước ánh xạ một folder thành một ổ đĩa mạng?
- Làm sao để user u1 chỉ được đọc không được ghi trên thư mục data?
- Viết lệnh truy cập vào tài nguyên mạng trên server S1 với thư mục chia sẻ là Public?
- Nếu Administrator không cài đặt password, người dùng có thể dùng account này để lấy tài nguyên chia sẽ từ một máy khác không, tại sao?
- Hãy tắt chức năng share tài nguyên trong card mạng để bảo mật cho máy tính?
- Hãy tiến hành cài bản vá lỗi mới nhất cho Windows 7?
- Hãy tắt chế độ Autorun để bảo mật khi cắm thiết bị lưu trữ ngoài vào máy?

MÔ HÌNH CLIENT/SERVER

∗ **Tóm tắt nội dung chương 7**

– Hướng dẫn cài đặt Windows Server 2003 SP2 và tạo file trả lời để cài đặt tự động.
– Giới thiệu AD, thăng cấp một server lên DC và join một workstation vào miền.
– Quản trị các object trong AD.
– Share permission và NTFS permission.

∗ **Mục tiêu chương 7**

Sau khi học xong sinh viên khả năng:

– Cài đặt Windows Server 2003, tạo file trả lời tự động.
– Trình bày kiến trúc AD, thuộc tính và chức năng của các object.
– Thăng cấp một server lên DC và join một workstation vào miền.
– Cấp quyền share permission và NTFS permission.

7.1. Hệ điều hành (OS) dùng cho server

Các OS thông dụng có hai loại chính đó là Windows và Linux, hiện nay để giảm chi phí và bảo mật (tránh virus và hacker). Các nhà đầu tư chọn Linux làm OS cho máy chủ của mình, nhưng Windows cũng có thế mạnh rất lớn (nhất là dịch vụ AD).

∗ **Microsoft OS:**

– Họ Windows NT: Windows NT 3.1, Windows NT 3.5, Windows NT 3.51, Windows NT 4.0.
– Họ Windows 2000, có 3 dòng chính tùy vào các tính năng mở rộng: Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server.
– Họ Windows 2003, có 4 phiên bản sử dụng rộng rãi: Standard Edition, Enterprise Edition, Datacenter Edition và Web Edition.
– Họ Windows 2008 cũng có 4 phiên bản thay thế cho 4 phiên bản của Windows 2003, khi nâng cấp phải chọn đúng phiên bản: Standard Edition, Enterprise Edition, Datacenter Edition hay Web Edition.
– Standard Edition: dành cho các chương trình phục vụ nhỏ không cần tụ nhóm (clustering), có 4 bộ xử lý.
– Enterprise Edition: dành cho các chương trình phục vụ lớn hơn, cho phép tụ nhóm , có 8 bộ xử lý.
– Datacenter Edition: dành cho máy chủ mainframe, có 128 bộ xử lý.
– Web Edition cho chủ web cơ bản, có 2 bộ xử lý.

∗ **Linux OS: các phiên bản thường gặp là.**

– RedHat Linux.
– Slackware.
– Caldera Open Linux.
– Su.S.E Linux.
– Debian.
– CentOS.

– Fedora.

7.1.1. Cài đặt hệ điều hành Windows Server 2003

Giới thiệu

Windows Server 2003 (Win2K3) là một OS dành cho máy chủ server của Microsoft, có rất nhiều phiên bản dành cho các máy chủ có chức năng khác nhau. Trong Win2K3 tích hợp hầu hết các dịch vụ mạng, dịch vụ ứng dụng mạng cần thiết.

Cài đặt

Cài đặt Win2K3 có một số điểm khác với cài đặt WinXP. Server sẽ có nhiều client kết nối tới và hệ thống có nhiều server, vậy phải hoạch định cài đặt như thế nào cho phù hợp với quy mô của tổ chức. Các giai đoạn giống với cài WinXP sẽ được trình bày vắn tắt.

∗ **<u>Bước 1</u>: Chuẩn bị cài đặt**

Khi cài đặt phải cung cấp các thông tin cần thiết cho quá trình cài đặt. Để lên kế hoạch cho việc nâng cấp hoặc cài mới, nên tham khảo hướng dẫn từ Microsoft Windows Server 2003 Deployment Kit. Các thông tin cần biết trước khi nâng cấp hay cài đặt.

– Yêu cầu hệ thống: tốc độ tối thiểu Pentium 233 MHz, ram tối thiểu 64 MB, ổ cứng trống tối thiểu 1.5 GB.

– Tính tương thích phần cứng và phần mềm: có thể kiểm tra bằng chương trình trong đĩa CD bằng cách tại dấu nhắc lệnh chạy ***\i386\winnt32 /checkupgradeonly*** hoặc có thể kiểm tra trên trang Catalog.

– Xác định ổ đĩa cài đặt: là primary partition đã active.

– Chọn định dạng đĩa: FAT, FAT32 hay NTFS. Khuyến cáo chọn NTFS.

– Chọn cách quản lý là Workgroup hay Domain. Khuyến cáo chọn Workgroup, nếu là máy quản lý miền thì thăng cấp lên DC sau hoặc nếu là máy con của một miền thì join vào miền sau.

– Chọn chế độ sử dụng giấy phép

– Per Server Licensing: là lựa chọn tốt nhất khi hệ thống có một server phục vụ cho một số lượng client nhất định, lúc này phải xác định số lượng giấy phép lúc cài đặt. Số lượng giấy phép tùy thuộc vào số lượng client kết nối tới server, tuy nhiên trong khi sử dụng có thể thay đổi số lượng kết nối cho phù hợp với thời điểm hiện tại.

– Per Seat Lincensing: là lựa chọn tốt nhất trong trường hợp mạng có nhiều server. Trong chế độ giấy phép này, mỗi client chỉ cần một giấy phép duy nhất để kết nối tới tất cả các server và không hạn chế số lượng kết nối đồng thời tới server.

– Chọn phương án kết nối mạng, ngôn ngữ, múi giờ...

∗ **<u>Bước 2</u>: bắt đầu quá trình cài đặt.**

– Kiểm tra xem hệ thống mình là cài đặt mới, nâng cấp từ phiên bản cũ hay cài song song hai OS.

– Có thể cài đặt từ đĩa CDRom, từ Source đã có sẵn trong máy hay trên mạng (thư mục i386). Dùng lệnh winnt.exe để cài đặt.

– Ở đây, sẽ cài mới Win2K3 từ CDRom.

– Đưa đĩa CDRom vào và thiết lập máy tính boot từ CDRom này.

∗ **Bước 3: giai đoạn Text-based**

– Khởi động máy tính → dòng chữ ***"press any key to boot CD..."*** hiện lên báo nhấn một phím bất kỳ để boot từ CDRom, nhấn phím bất kỳ → OS sẽ kiểm tra phần cứng nếu thích hợp sẽ tiến hành cài đặt.

– Quá trình cài đặt báo: nếu dùng ổ cứng SCSI thì nhấn <F6> để cài đặt driver cho ổ đĩa này.

– Quá trình cài đặt báo: nếu muốn tạo một backup thì nhấn phím <F2>, Windows Server Backup sẽ tạo image backup.

– Quá trình cài đặt tải các file cần thiết trong quá trình cài và các driver.

– Hộp thoại <Welcome to Setup> báo để tiếp tục cài đặt nhấn phím <Enter>, để sửa lỗi nhấn phím <R>, để kết thúc quá trình cài đặt nhấn phím <F3> → Nhấn phím ***<Enter>.***

– Hộp thoại <Windows Licensing Agreement> báo nếu đồng ý thông tin bản quyền nhấn phím <F8>, không đồng ý nhấn phím <ESC>, nhấn phím <Page Down> để đọc trang kế tiếp → Nhấn phím ***<F8>.***

– Hộp thoại <Win2K3, Enterprise Edition Setup> báo nhấn phím <Enter> để tiếp tục cài đặt, để tạo một partition mới từ không gian đĩa trống nhấn phím <C>, để xóa một partition nhấn phím <D> → Chọn ***<partition>*** thích hợp → Nhấn phím ***<Enter>.***

– Trường hợp cài trên một partition mới. Quá trình cài đặt đề nghị xác định dung lượng của partition này. Nhập dung lượng vào ***<Create partition of size (in MB)>*** → Nhấn phím ***<Enter>.***

– Quá trình cài đặt báo: nhấn phím <Enter> để cài đặt lên partition được chọn, để tiếp tục tạo partition khác nhấn phím <C>, để xóa partition nhấn phím <D> → Chọn ***<partition>*** thích hợp → Nhấn phím ***<Enter>.***

– Quá trình cài đặt báo: định dạng partition theo dạng nào, chọn định dạng nhanh NTFS → Chọn ***<Format the partition using the NTFS file system (Quick)>*** → Nhấn phím ***<Enter>.***

– Quá trình định dạng partition thực hiện. Sau khi định dạng xong partition, các file cần thiết trong quá trình cài đặt được chép vào máy. Các file này là các trình điều khiển, cơ sở dữ liệu, giao diện đồ họa...

– Hệ thống yêu cầu khởi động lại, đếm ngược trong vòng 8 giây hoặc có thể nhấn phím <Enter> để khởi động lại ngay.

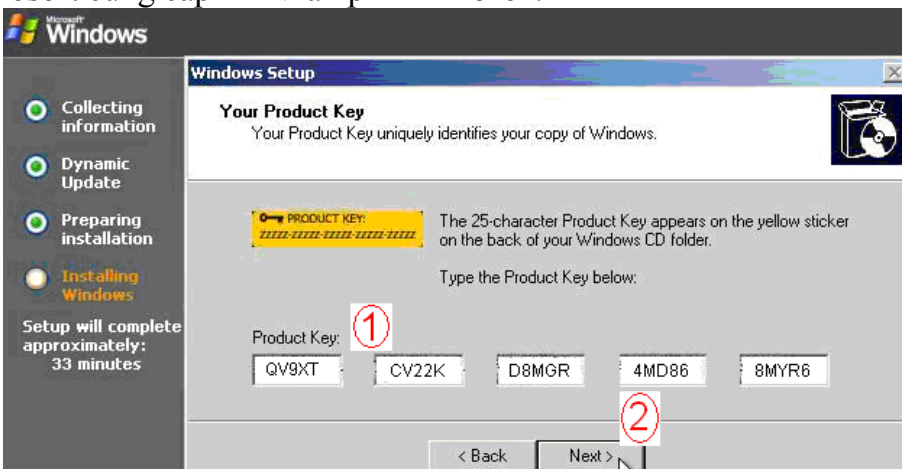
∗ **Bước 4: giai đoạn GUI-based.**

– Khi khởi động lại, quá trình cài đặt chuyển sang giao diện đồ họa → Cài các trình điều khiển thiết bị (driver).

– Hộp thoại ***<Regional and Language Options>***, cho phép nhập vào: ngôn ngữ, đơn vị tiền tệ, ngày tháng năm... → Nhấn nút ***<Next>***.

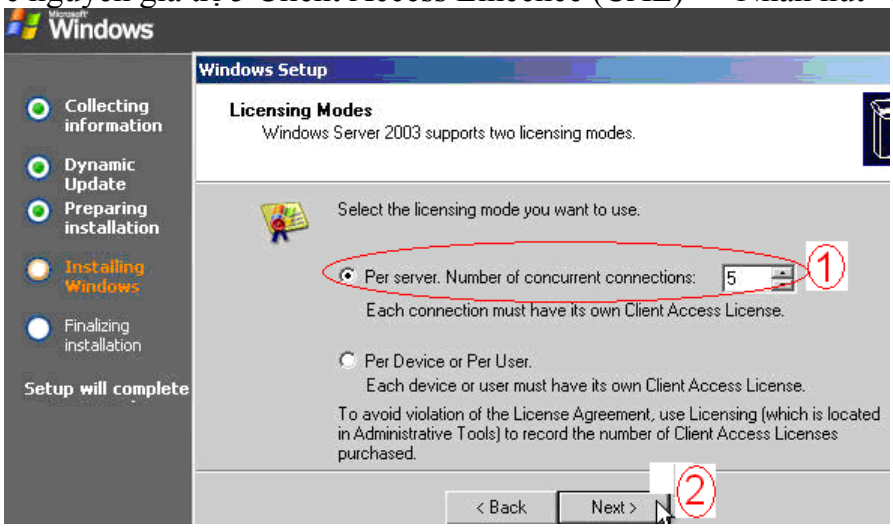
– Hộp thoại ***<Personalize Your Software>*** → Điền tên người sử dụng vào ***<Name>***, tên tổ chức sử dụng và ***<Organization>*** → Nhấn nút ***<Next>***.

– Hộp thoại <***Your Product Key***> → Nhập vào <**Product Key**> 25 chữ số do Microsoft cung cấp → Nhấn phím <***Next***>.



Hình 7. 1 - Nhập vào product key

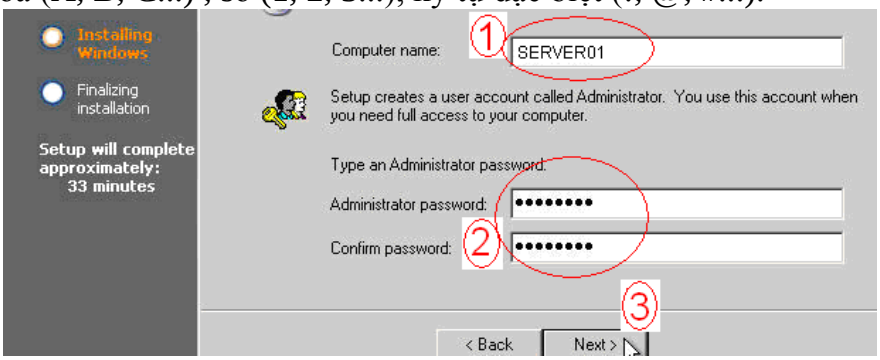
– Hộp thoại <***Licensing Modes***>, có 2 loại bản quyền. <Per server Number of concurrent connection> dùng nhiều trong trường hợp hệ thống có 1 server. Server sẽ đếm số kết nối đồng thời và không cho quá số kết nối đăng ký. Số lượng kết nối cùng một lúc là xác định, số này có thể thay đổi sau. <Per Device or Per User> dùng nhiều trong hệ thống nhiều server, mỗi thiết bị hoặc user có thể kết nối vào nhiều server cùng một lúc. Lúc này không cần quan tâm đến giới hạn số kết nối trên từng server, mà chỉ quan tâm đến thiết bị và user nào kết nối với hệ thống → Chọn option <***Per server. Number of concurrent connections***> → Để nguyên giá trị 5 Client Access Lincence (CAL) → Nhấn nút <***Next***>.



Hình 7. 2 - Chọn chế độ licensing

– Hộp thoại <***Computer Name and administrator Password***> → Nhập tên máy tính vào <***Computer name***> → Nhập password của quản trị hệ thống vào <***Administrator password***> → Xác nhận lại password trong <***Confirm password***> → Nhấn nút <***Next***>.

Win2K3 yêu cầu password phải phức tạp: từ 7 ký tự trở lên, không có từ Administrator hay Admin và chứa 3 loại ký tự trong bốn nhóm ký tự sau: chữ thường (a, b, c...), chữ hoa (A, B, C...) , số (1, 2, 3...), ký tự đặc biệt (!, @, #...).



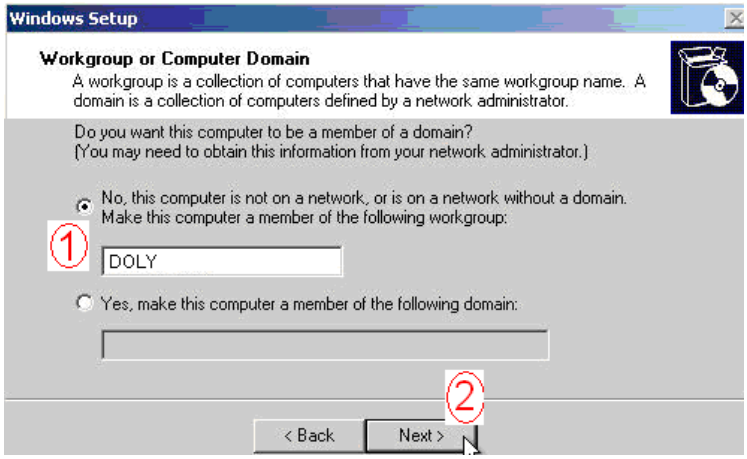
Hình 7. 3 - Nhập tên máy tính và password Administrator

– Hộp thoại <***Date and Time Settings***> → Chỉnh lại ngày giờ hệ thống trong <***Date & Time***> → Chọn múi giờ cho phù hợp trong <***Time Zone***> → Nhấn nút <***Next***>.

Lưu ý: múi giờ của Việt Nam là ***GMT +07***

– Hộp thoại <***Networking Settings***>, cho phép cài đặt NIC thông thường <Typical settings> (gồm có: Client for Microsoft Networks, File and Print Sharing for Microsoft Networks, QoS Packet Scheduler và TCP/IP transport protocol), hay cài đặt tùy chọn <Custom settings> → Chọn option <***Typical settings***> → Nhấn nút <***Next***>.

– Hộp thoại <***Workgroup or Computer Domain***>, có 2 option. <No, this computer is not ...> máy tính này là máy peer hoạt động trong mạng workgroup. <Yes, make this computer a member...> máy tính này là phần tử của một miền → Chọn option <***No, this computer is not on a net work...***> → Đặt tên cho nhóm làm việc <***DOLY***> → Nhấn nút <***Next***>.



Hình 7. 4 - Đặt tên cho nhóm làm việc

– Quá trình cài đặt hoàn tất→ máy tính khởi động lại → nhấn tổ hợp phím <***Ctrl***> + <***Alt***> + <***Del***> hộp thoại logon hiện lên → đăng nhập vào bằng tài khoản Administrator.

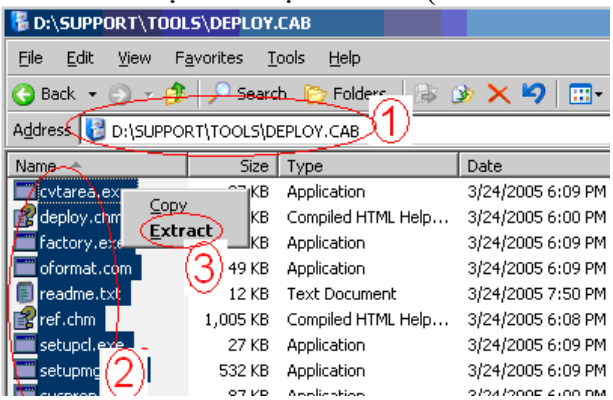
7.1.2. Tự động hóa quá trình cài đặt Win2K3

Việc cài đặt Windows cho nhiều máy với các thông số giống nhau là một việc tốn kém và nhàm chán. Để tự động hóa quá trình này có 2 cách, một là dùng ảnh đĩa hoặc ảnh partition (disk image, partition image), hai là dùng phương pháp cài không cần theo dõi (unattended installation) thông qua một kịch bản (script) hay tập tin trả lời.

Tạo file trả lời tự động

File trả lời tự là một file có cấu trúc, trả lời sẵn các thông số và thông tin khi cài đặt. File trả lời có thể soạn thảo bằng Notepad hoặc dùng công cụ có trong đĩa source Win2K3.

– Mở đĩa source ***CD Windows Server 2003***→ Vào trong thư mục DEPOY.CAB ***SUPPORT\TOOLS\DEPLOY.CAB*** → Chọn hết tất cả các file trong thư mục DEPLOY.CAB → Phải chuột lên vùng bôi đen → Chọn menu <***Extract***> để giải nén DEPLOY.CAB vào một thư mục nào đó (vd: C:\Unattended).



Hình 7. 5 - Giải nén DEPLOY.CAB

– Mở C:\Unattended → chạy file ***setupmgr.exe***.

– Màn hình <***Welcome***> → nhấn <***Next***>.

– Hộp thoại <***New or Existing Answer File***> có 2 option. <Create new> để tạo mới một file kịch bản. <Modify existing> sửa một file kịch bản có sẵn → Chọn option <***Create new***> → Nhấn nút <***Next***>.

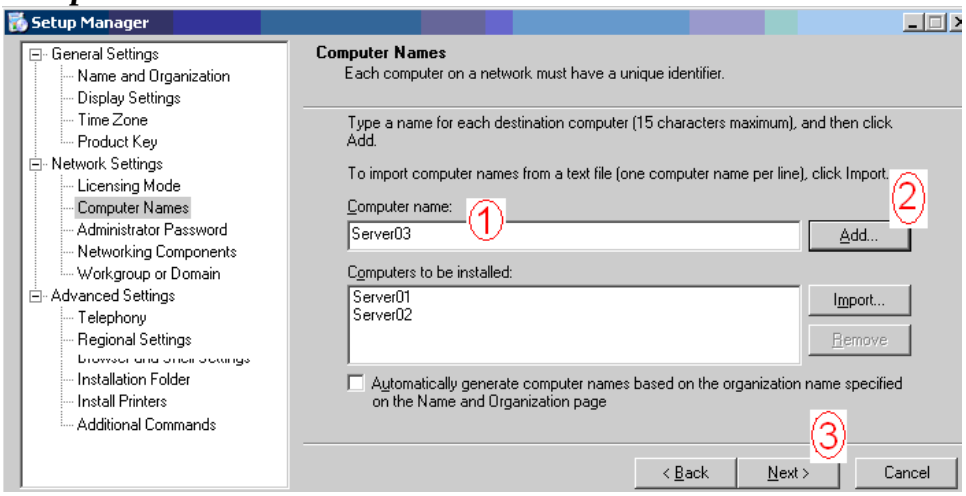
– Hộp thoại <***Type of Setup***> có 3 option. <Unattended setup> tạo file kịch bản Winnt.sif. <Sysprep setup> sẽ tạo ra một Mini-Setup (xóa hết SID nên có thể chạy trên các máy khác). <Remote Installation Services (RIS)> dùng để cài đặt Windows từ xa → Chọn option <***Unattended setup***> → Nhấn nút <***Next***>.

– Hộp thoại <***Product***>, chọn loại hệ điều hành Windows → Chọn option <***Windows Server 2003, Enterprise Edition***> → nhấn nút <***Next***>.

– Hộp thoại <***User Interaction***>, mức độ tương tác khi cài đặt, Chọn <***Fully automated***> → nhấn nút <***Next***>.

– Hộp thoại <***Distribution Share***>, kiểu phân phối file kịch bản → Chọn option <***Setup from a CD***> → nhấn nút <***Next***>.

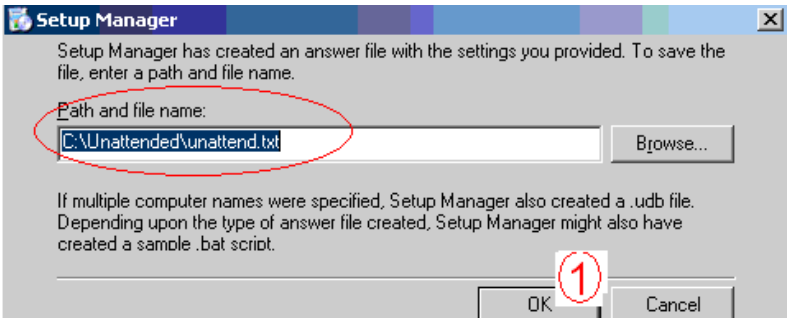
– Hộp thoại <License Agreement>, chấp nhận bản quyền→ Check vào <I accept the terms of the...> → Nhấn nút <Next>.
– Hộp thoại ***<Name and Organization>***, nhập tên người sử dụng và tên tổ chức. Nếu không nhập thì Windows sẽ bắt nhập trong quá trình cài đặt → Nhập tên vào ***<Name>*** → Nhập tên tổ chức vào ***<Organization>*** → nhấn nút ***<Next>***.
– Hộp thoại ***<Display Settings>***, thay đổi cách hiển thị → Để nguyên cách hiển thị mặc nhiên → Nhấn nút ***<Next>***.
– Hộp thoại ***<Time Zone>***, chọn múi giờ → Nhấn mũi tên xuống chọn ***<GMT +07>*** → Nhấn nút ***<Next>.***
– Hộp thoại ***<Product Key>***, mã sản phẩm → Nhập vào 25 số key sản phẩm trong ***<Product Key>*** → Nhấn nút ***<Next>***.
– Hộp thoại ***<Licensing Mode>***, loại bản quyền → Chọn option ***<Per server>*** → Để nguyên giá trị ***5 Client Access Licence*** → Nhấn nút ***<Next>.***
– Hộp thoại ***<Computer Name>***, nhập tên máy tính dự định cài đặt vào ***<Computer name>*** → Nhấn nút ***<Add...>*** → Lần lượt thêm các máy khác vào hộp ***<Computers to be installed>*** → Nhấn nút ***<Next>.***



Hình 7. 6 - Nhập tên các máy tính dự định cài đặt

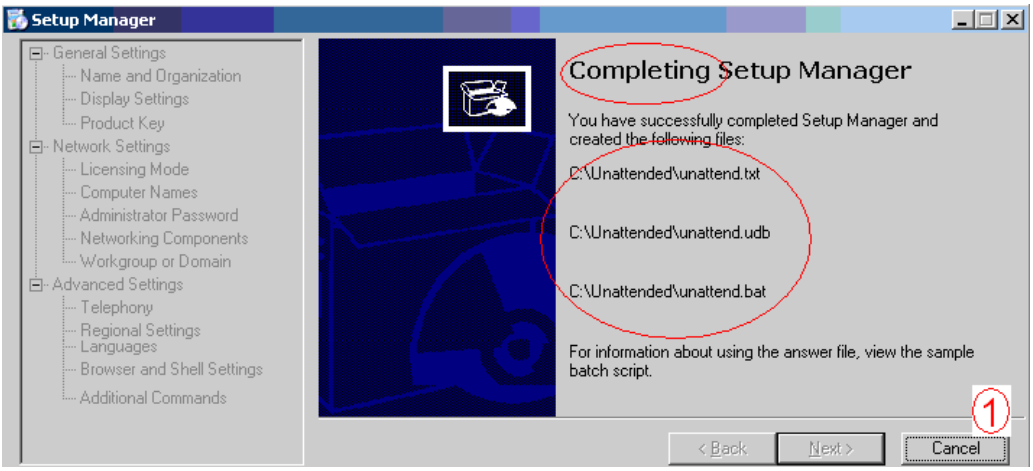
– Hộp thoại ***<Administrator Password>*** → Nhập password của Admin vào ***<Password>*** → Xác nhận lại password trong ***<Confirm password>*** → Check vào <Encrypt the Administrator...> để mã hóa password Admin trong file trả lời → Nhấn nút ***<Next>.***
– Hộp thoại ***<Networking Components>*** có 2 option. <Typical settings> dùng các protocol mạng mặc nhiên. <Custom settings> thêm bớt các protocol mạng → Chọn option ***<Typical settings>*** → Nhấn nút ***<Next>.***
– Hộp thoại ***<Workgroup or Domain>***, máy tính thuộc mô hình quản lý nào → Chọn opiton ***<Workgroup>*** → Nhập tên nhóm làm việc → Nhấn nút ***<Next>***.
– Hộp thoại ***<Telephony>***, cung cấp số điện thoại cho người sử dụng → Nhấn nút ***<Next>.***
– Hộp thoại <Regional Settings>, chỉ định vùng → Chọn option <Specify regional settings in the answer file> → Chọn <Vietnamese> → Nhấn nút <Next>.

– Hộp thoại <***Languages***>, chọn ngôn ngữ → Chọn <***Vietnamese***> → nhấn nút <***Next***>.
– Các hộp thoại tiếp theo có thể dùng mặc định → Nhấn <***Next***> cho đến hộp thoại chỉ định đường dẫn để tạo file kịch bản→ Chỉ đường dẫn đến file <***unattend.txt***> → Nhấn nút <***OK***>.



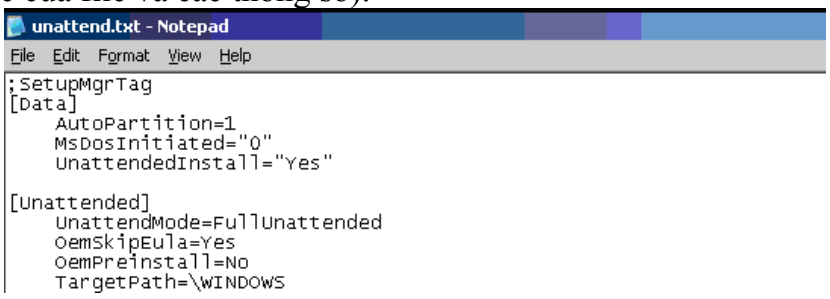
Hình 7. 7 - Vị trí lưu file kịch bản

– Ba file unattend.txt, unattend.udb, unattend.bat được tạo ra, nhấn nút <Cancel> để kết thúc.



Hình 7. 8 - Ba file trả lời được tạo ra

– Sau đây là nội dung của file trả lời tự động, có thể sửa lại cho đúng bằng Notepad. Cách thứ 2 tạo file này là chùng Notepad soạn thảo (lúc này phải biết rõ cấu trúc của file và các thông số).



Hình 7. 9 - Nội dung file trả lời

Sử dụng file kịch bản

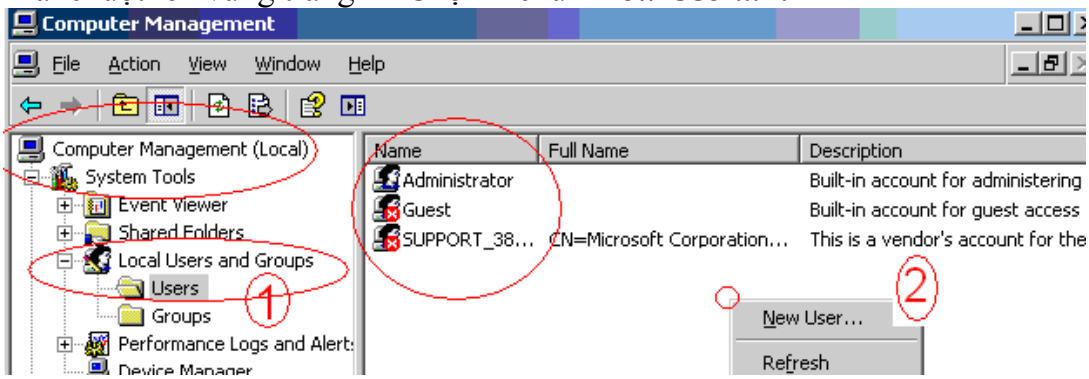
– Đổi tên file ***unattend.txt*** thành ***winnt.sif***
– Chép file winnt.sif vào thư mục i386 của bộ source cài đặt.

7.2. Kỹ năng tạo user, group và gán quyền cục bộ trong môi trường workgroup

7.2.1. Tạo user

Khi vừa cài đặt xong, máy tính trở thành một máy chủ chưa cung cấp dịch vụ gì cả và được gọi là máy stand-alone (máy chủ độc lập). Lúc này hệ thống chỉ có 3 user được tạo ra.

– Administrator: toàn quyền quản trị hệ thống, đang hoạt động (enable), có thể đổi tên để bảo mật, không thể xóa khỏi hệ thống (Built-in).
– Guest: bị giới hạn quyền, chưa hoạt động (disable), có thể đổi tên, không thể xóa được (Built-in).
– SUPPORT: là user bên ngoài dùng cho dịch vụ Help and Support, có thể đổi tên, chưa hoạt động (disable), có thể xóa khỏi hệ thống.
– Trên Desktop, phải chuột lên <***My Computer***> → Chọn menu <***Manage***> → Chọn mục <***Computer Management (Local)***> → Click vào dấu cộng <***System Tools***> → Click vào dấu cộng <***Local Users and Groups***> → Chọn <***User***> → Phải chuột lên vùng trắng → Chọn menu <***New User...***>.



Hình 7. 10 - Tạo mới một user

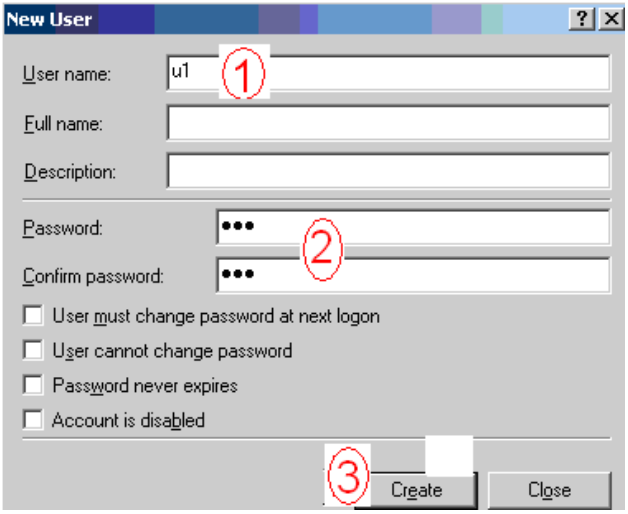
Lưu ý: có thể mở Computer Management bằng lệnh ***compmgmt.msc***

– Hộp thoại <***New User***> → Nhập tên user vào <***User name***> → Nhập tên đầy đủ vào <full name> → Nhập mô tả về user vào <***Description***> → Nhập password vào <***Password***> → Xác nhận lại password trong <***Confirm password***> → Nhấn nút <***Create***> để tạo user → Tạo các user tiếp theo → Nhấn <***Close***>.

Khi tạo user, có 4 chính sách dành cho user:

– User must change password at next logon: khi Admin giao account cho người nào đó sử dụng, để bảo đảm rằng người này không dùng luôn password mặc định (vì mục đích bảo mật). Admin bắt buộc user khi đăng nhập lần đầu tiên phải thay đổi password.
– User cannot change password: nếu user này được dùng chung cho nhiều người sử dụng (vd: máy tính công cộng). Admin không cho phép user này thay đổi password.

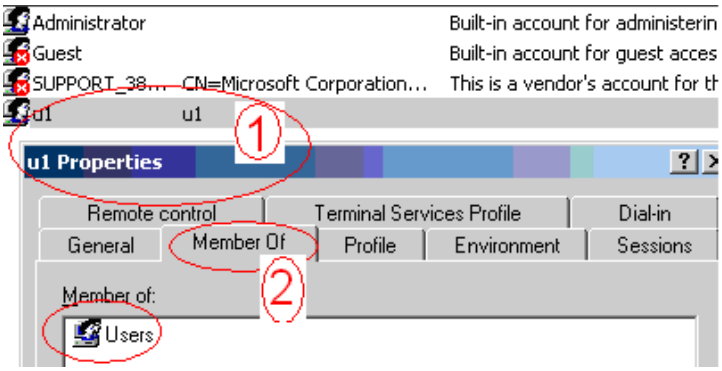
– Password never expires: password này không bao giờ hết hạn, dùng cho các user công cộng không cần bảo mật.
– Account is disabled: user được tạo ra nhưng chưa được sử dụng. Dùng chính sách này để khóa tạm thời account.



Hình 7. 11 - Tạo user

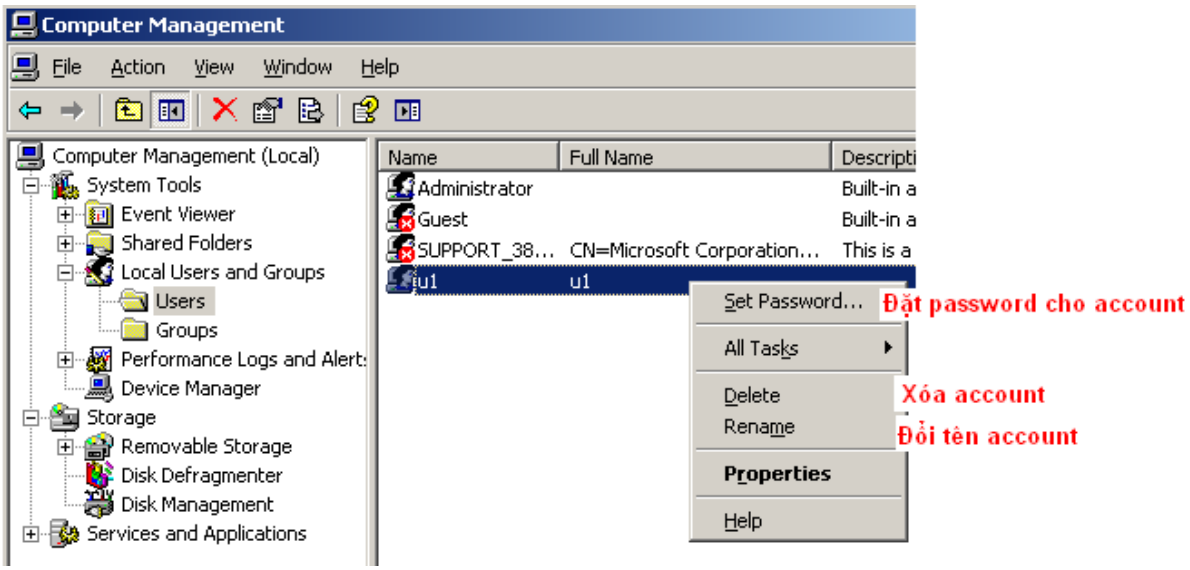
Lưu ý: có thể tạo user u2 password 123 bằng dòng lệnh: ***net user u2 123 /add***

– Trong hộp thoại <***Computer Management***> → Phải chuột lên <***u1***> → Chọn menu <***Properties***> → Chọn tab <***Member Of***> user vừa tạo chỉ thuộc duy nhất một nhóm Users.



Hình 7. 12 - Xem nhóm mà u1 là thành viên

– Trong hộp thoại <***Computer Management***> → Phải chuột lên <***u1***>, có thể đặt lại password cho account, đổi tên account và xóa account khi chắc chắn rằng account này không còn được sử dụng nữa.



Hình 7. 13 - Xóa u1

Lưu ý: có thể xóa account u1 bằng dòng lệnh ***net user u1 /delete***

7.2.2. Tạo group

Việc phân ra nhóm làm việc (group) để hỗ trợ phân quyền trên hệ thống. Thông thường phân quyền trên group, rất ít khi phân quyền trên user. Khi cài đặt Win2K3 xong hệ thống tự có các group sau:

– Administrators: có toàn quyền không giới hạn truy cập vào máy tính và miền.

– Backup Operators: có thể gán các quyền về mục đích sao lưu và phục hồi file.

– Distributed COM users: cho phép khởi tạo và sử dụng các đối tượng COM trong máy tính.

– Guests: bị giới hạn quyền, tương tự nhóm User mặc nhiên (chưa thay đổi).

– Network Configuration Operators: có một vài đặc quyền quản trị để quản lý cấu hình mạng.

– Performance Log Users: có thể truy cập từ xa, quản lý, lập lịch các log file.

– Performance Monitor Users: có thể truy cập từ xa để theo dõi máy tính.

– Power Users: có hầu hết quyền của nhóm Administrator (điều khác là nó chỉ có thể xóa những gì do nó tạo ra).

– Print Operators: có quyền quản trị máy in.

– Remote Desktop Users: có quyền logon từ xa (để quản trị server từ xa).

– Replicator: hỗ trợ đồng bộ file trên domain.

– Users: có quyền với các ứng dụng, nhưng cấm nhiều quyền trên hệ thống (nhằm bảo mật).

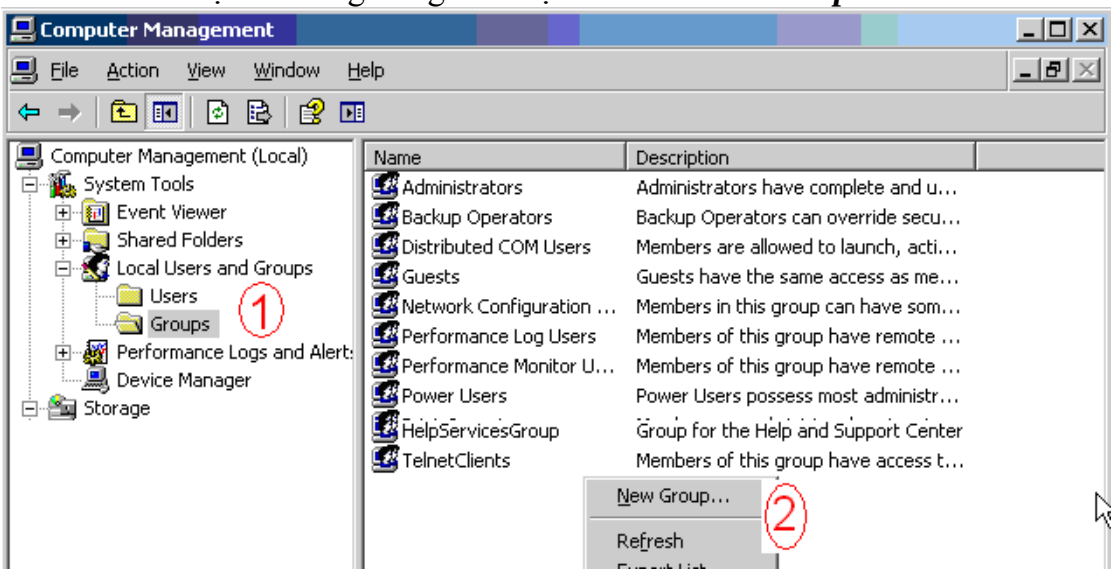
– HelpServicesGroup: dùng cho trung tâm Help and Support.

– TelnetClients: có quyền telnet đến server.

Thường các nhóm có sẵn không đáp ứng đúng yêu cầu của người dùng, nên đối với mỗi nhóm làm việc nên tạo riêng một group để phân quyền.

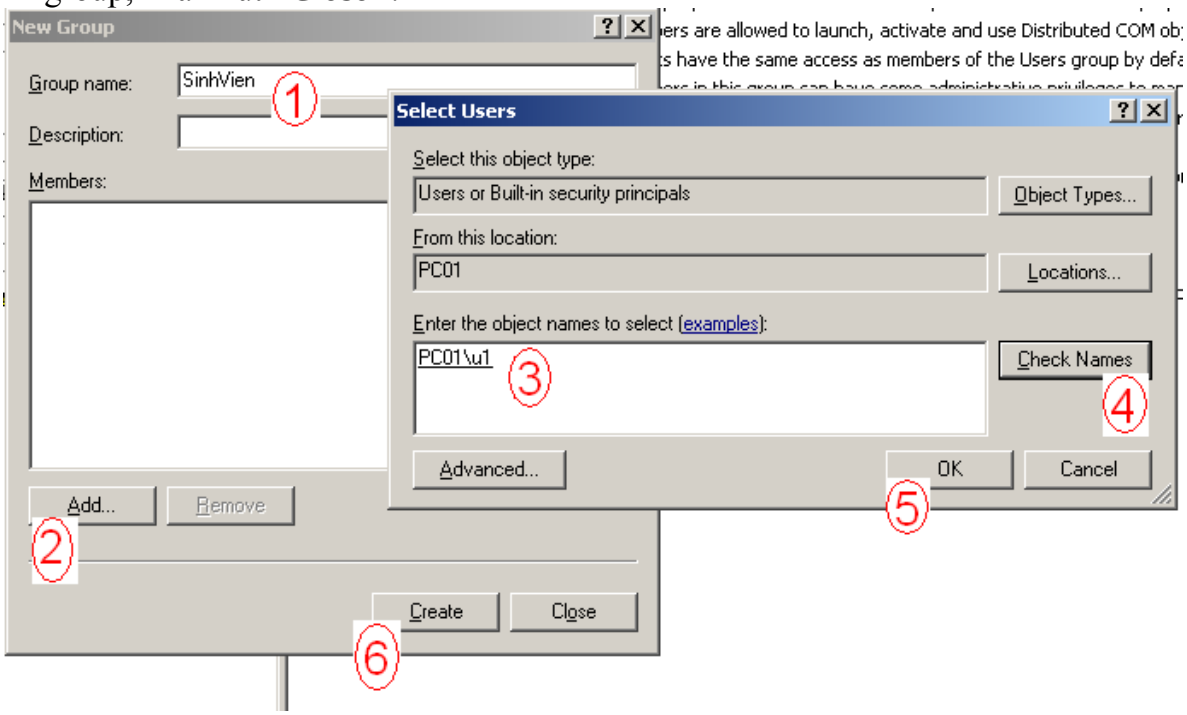
– Trên Desktop, phải chuột lên <***My Computer***> → Chọn menu <***Manage***> → Chọn mục <***Computer Management (Local)***> → Click vào dấu cộng <***System***

Tools> → Click vào dấu cộng <***Local Users and Groups***> → Chọn <**Groups**> → Phải chuột lên vùng trắng → Chọn menu <***New Group...***>.



Hình 7. 14 - Tạo group

– Trong hộp thoại <***New Group***> → Nhập tên group cần tạo vào <***Group name***> → Nhập mô tả cho group vào <***Description***> → Nhấn nút <***Add...***> → Hộp thoại <***Select Users***> hiện ra → Nhập <***u1***> vào <***Enter the object names to select***> → Nhấn nút <***Check Names***> → Nhấn nút <***OK***> → Bây giờ u1 là thành viên của nhóm Sinhvien, nhấn nút <***Create***> để tạo group → Khi tạo xong tất cả các group, nhấn nút <***Close***>.



Hình 7. 15 - Thêm u1 vào group

∗ **Để thêm một hoặc nhiều user có sẵn vào group có sẵn, có 2 cách:**

– Phải chuột lên tên user → Chọn menu <***Properties***> → Chọn tab <***Member Of***> → Nhấn nút <***Add...***> để thêm group vào.

– Phải chuột lên tên group → Chọn menu <***Properties***> → Chọn tab <***Member***> → Nhấn nút <***Add...***> để thêm user vào.

Lưu ý: có thể tạo local group SV bằng dòng lệnh ***net localgourp SV /add***

7.2.3. Gán chính sách cục bộ (local policies)

Sau đây sẽ trình bày một số chính sách thông dụng, để mở cửa sổ thiết lập chính sách, vào <***Start***> → Chọn <***Run...***> → Chạy lệnh ***secpol.msc***

Chính sách về password (password policy)

Nhằm sử dụng password đúng mục đích và bảo mật (khuyến cáo 1 tháng phải đổi password một lần, sử dụng password phức tạp, password không dưới 7 ký tự).

Security Settings/ Account Policies/ Password Policy

– Enforce password history: số lần đổi password không được trùng lại password cũ. (mặc nhiên là 0, không sử dụng).

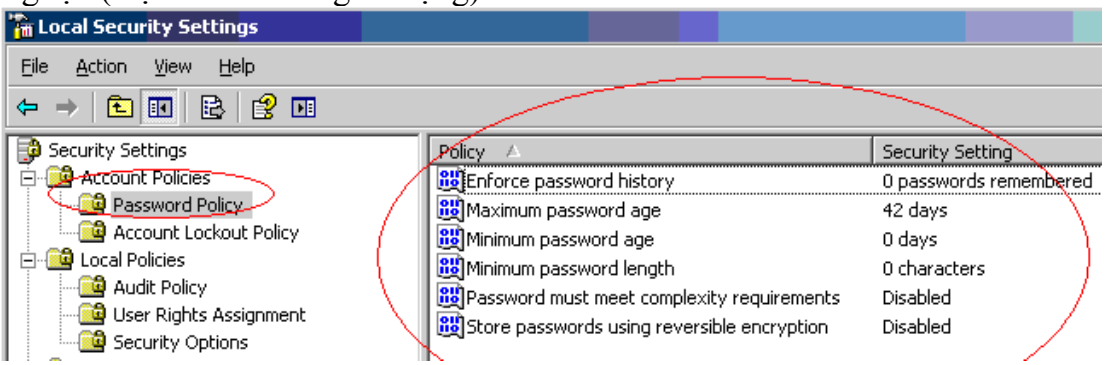
– Maximum password age: thời gian tối đa của một password, sau thời gian này phải thay đổi lại password khác (mặc nhiên là 42 ngày).

– Minimum password age: thời gian tối thiểu cho phép đổi password khác (mặc nhiên là 0 ngày, không sử dụng).

– Minimum password length: số ký tự tối thiểu của password, mặc nhiên là 0 ký tự.

– Password must meet complexity requirements: password phải phức tạp (mặc nhiên không sử dụng). Password phức tạp là không có các từ Administrator hoặc Admin, trong password phải tồn tại 3 loại trong 4 nhóm ký tự (chữ thường, chữ hoa, số, ký tự đặc biệt).

– Store passwords using reverible encryption: lưu trữ password ở dạng mã hóa ngược (mặc nhiên không sử dụng).



Hình 7. 16 - Password policy

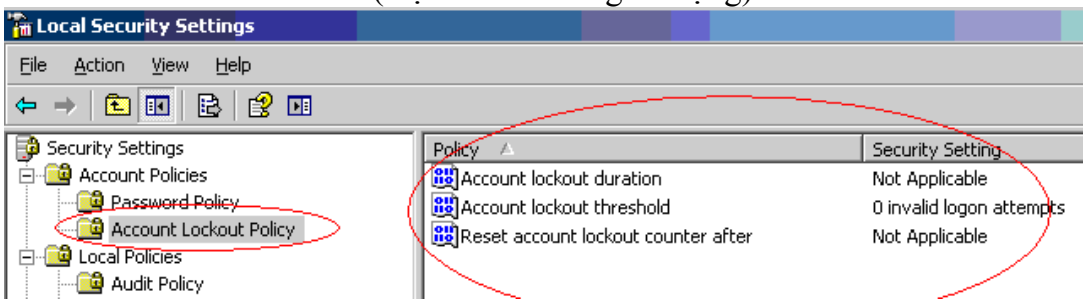
Chính sách về account (Account Lockout Policy)

Nhằm bảo vệ account tránh việc dò password...

Security Settings/ Account Policies/ Account Lockout Policy

– Account lockout duration: thời gian khóa tài khoản tạm thời (mặc nhiên không sử dụng).

– Account lockout threshold: số lần cho phép nhập password sai, quá số lần này tài khoản sẽ bị lock tạm thời (mặc nhiên là 0, không sử dụng).
– Reset account lockout counter after: thời gian reset lại bộ đếm, phải nhỏ hơn Account lockout duration (mặc nhiên không sử dụng).



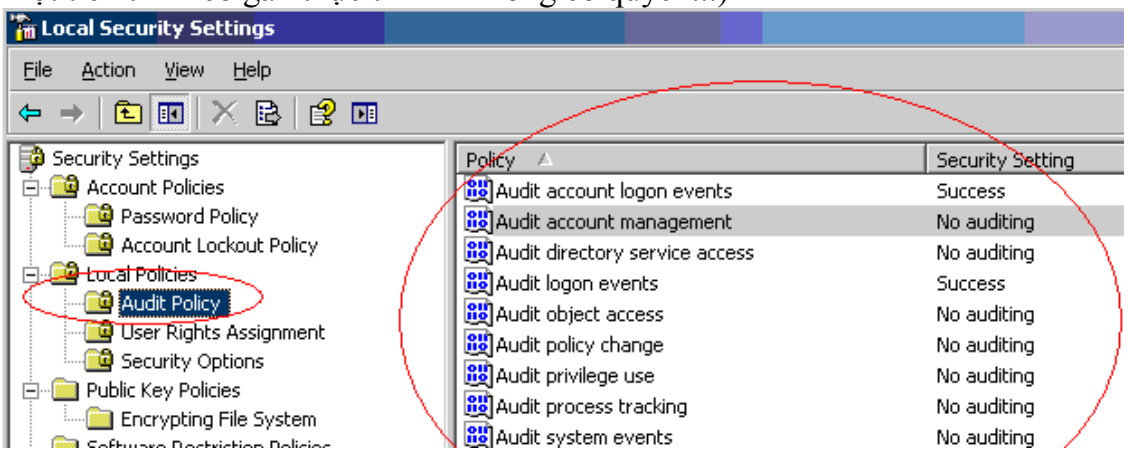
Hình 7. 17 - Account lockout policy

Chính sách về kiểm toán (Audit Policy)

Ghi lại các hoạt động trong hệ thống, dùng cho việc theo dõi bảo mật hệ thống.

Security Settings/ Local Policies/ Audit policy

– Audit account logon events: kiểm toán việc đăng nhập (logon, logoff, kết nối từ một máy tính khác).
– Audit account mangement: kiểm toán việc thay đổi các thông số account (đổi tên, đổi password, enable account, disable account, tạo account, xóa account...).
– Audit directory serviece access: kiểm toán việc truy cập AD.
– Audit logon events: kiểm toán các sự kiện khi logon vào hệ thống (Logon Script, Roaming Profile...).
– Audit object access: kiểm toán việc sử dụng các object (file, folder, printer...).
– Audit policy change: kiểm toán việc thay đổi các chính sách hệ thống.
– Audit Privilege use: kiểm toán một số thực thi đặc quyền (cấp quyền, xóa quyền...).
– Audit process tracking: kiểm toán các tiến trình hoạt động.
– Audit system events: kiểm toán việc tác động đến hệ thống (Shutdown, restart, một tiến trình cố gắn thực thi khi không có quyền...)



Hình 7. 18 - Audit policy

Chính sách hệ thống của user và group (User Rights Assignment)

Đây là các chính sách về hệ thống được gán cho các user và group, thường thì gán chính sách cho group. Ở đây chỉ khảo sát một số chính sách thông dụng.

Security Settings/ Local Policies/ User Rights Assignment

– Access this computer from the network: các user và group có trong chính sách này được phép dùng máy tính khác trên mạng truy cập vào máy này.

– Allow log on locally: được phép logon vào máy tính này.

– Allow log on throuht Terminal Services: được phép logon máy tính từ xa.

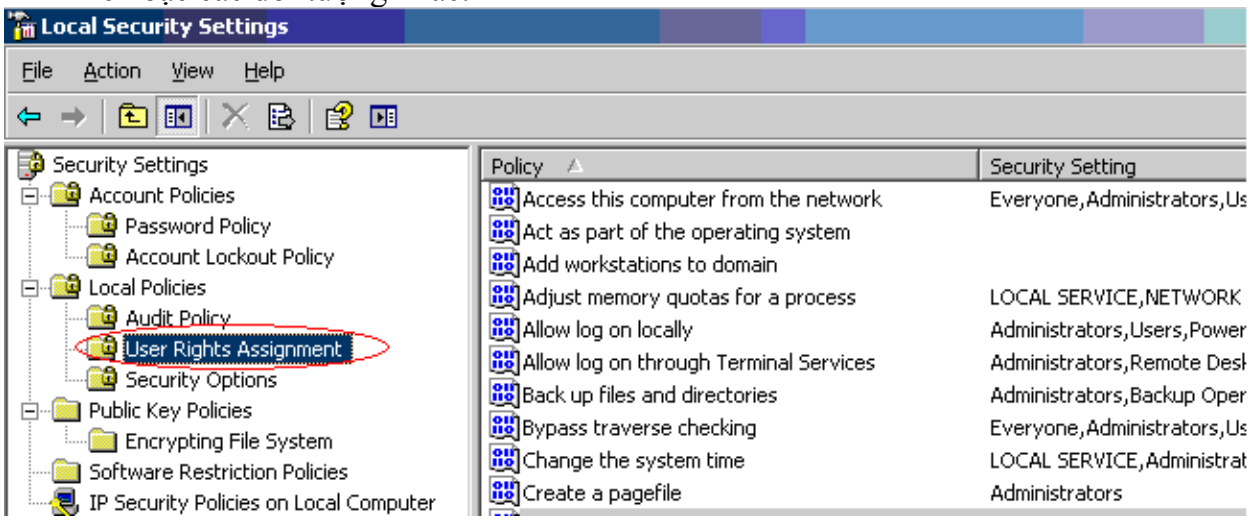
– Backup files and directories: được phép sao lưu file và folder.

– Change the system time: được phép thay đổi ngày giờ hệ thống.

– Restore files and directories: được phép phục hồi file và folder.

– Shut down the system: được phép shutdown máy.

– Take ownership of files or other objects: được phép chiếm quyền sở hữu của file hoặc các đối tượng khác.

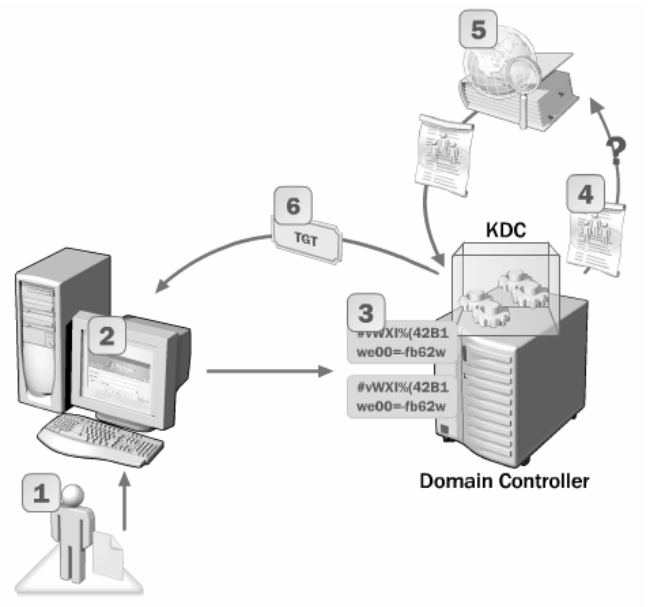


Hình 7. 19 - User rights assignment

7.3. Thăng cấp lên Domain Controller với Active Directory

Trong mô hình workgroup (chương trước), tất cả các thông tin về account đều lưu trong máy tính cục bộ và máy tính cục bộ tự chứng thực người dùng đăng nhập vào hệ thống. Thông tin này được lưu trong file SAM (Security Accounts Manager) và file SAM được mã hóa để bảo mật.

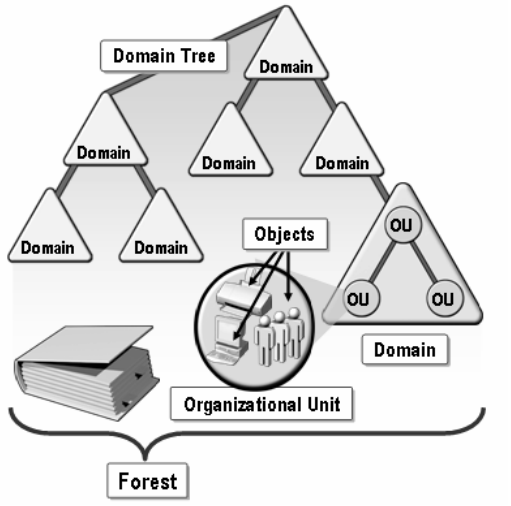
Khác với mô hình workgroup, mô hình domain hoạt động theo cơ chế Client/Server. Có ít nhất một máy điều khiển miền DC (Domain Controler) chứa cơ sở dữ liệu của tất cả tài nguyên thuộc miền. Dịch vụ AD được cài đặt trên DC sẽ quản lý tất cả các tài nguyên thuộc miền và chứng thực cho tất cả các user đăng nhập vào miền. Cơ sở dữ liệu này được lưu trong NTDS.DIT, có thể lưu trữ hàng triệu người dùng (workgroup lưu khoảng 5000 người dùng).



Hình 7. 20 - Chứng thực trong mô hình domain

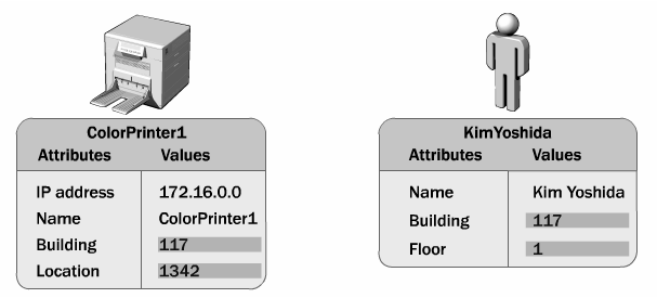
Ở hình 7.1, user (1) muốn đăng nhập vào hệ thống (2) phải thông qua DC chứng thực (3), DC sẽ truy vấn (4) cơ sở dữ liệu AD (5) xem thử user này có quyền đăng nhập vào hệ thống hay không (6).

7.3.1. Kiến trúc của AD



Hình 7. 21 - Kiến trúc của AD

Các đối tượng (Object)

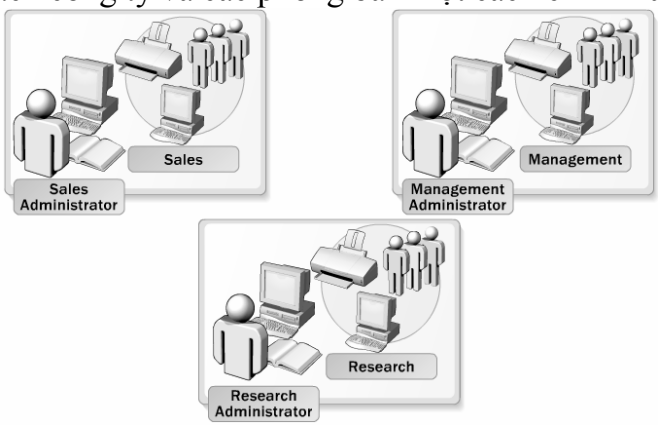


Hình 7. 22 - Object printer và object user

Mỗi đối tượng đều có một thuộc tính (attirbuted) riêng (name, office localtion...) các đối tượng cùng loại thì có các thuộc tính giống nhau tạo thành một lớp đối tượng (object class). Các lớp đối tượng thông dụng là User, Group, Printer, Computer... AD lưu sẵn các lớp đối tượng này, khi tạo một đối tượng thuộc lớp nào thì đối tượng tạo ra thừa hưởng tất cả các thuộc tính của lớp đối tượng đó.

Đơn vị tổ chức (Organization Unit)

Gọi tắt là OU, là đơn vị nhỏ nhất trong AD. OU chứa các object và chứa các OU con. Ở hình 7.4, có một OU cha là công ty. Trong OU công ty tạo ra 3 OU con là Sales (phòng kinh doanh), Management (phòng quản lý), Research (phòng nghiên cứu thị trường) và ủy quyền cho các Sub-administrator (Sales Admin, Management Admin, Research Admin) quản trị 3 OU con này. Việc này giảm bớt gánh nặng cho Admin quản trị toàn hệ thống, tăng hiệu quả quản lý. Đồng thời thiết lập các chính sách nhóm (GPO) để áp đặt các chính sách công ty và các phòng ban một cách chính xác và hiệu quả.

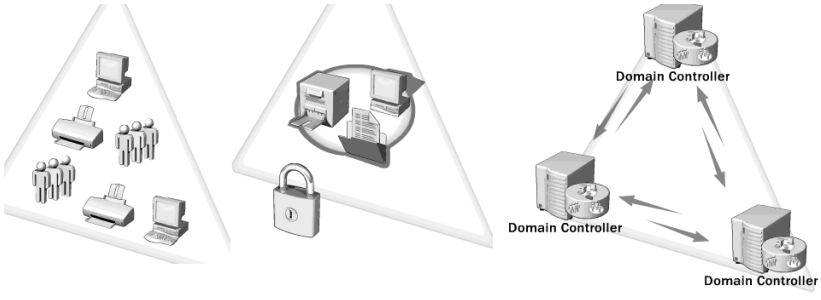


Hình 7. 23 - Đơn vị tổ chức (OU)

Miền (Domain)

Là đơn vị nòng cốt của cấu trúc Logic của AD, ở đó có các chính sách chung giống nhau đóng vai trò như một khu vực quản trị (administrative boundary). Có chung một sơ sở dữ liệu, ủy quyền và đồng bộ dữ liệu giữa các server. Domain chứa OU và các Object.

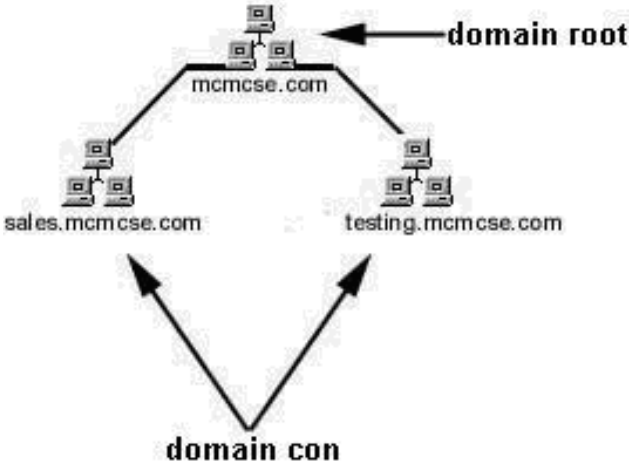
Ví dụ: Trường CĐ KT Lý Tự Trọng là một đơn vị giáo dục có các khoa và các phòng ban chức năng, có miền là lytc.edu.vn. Tạo ra các OU: CNTT, CK, OTO... để trực tiếp quản trị từng đơn vị này.



Hình 7. 24 - Các chức năng của domain

Cây domain (Domain Tree)

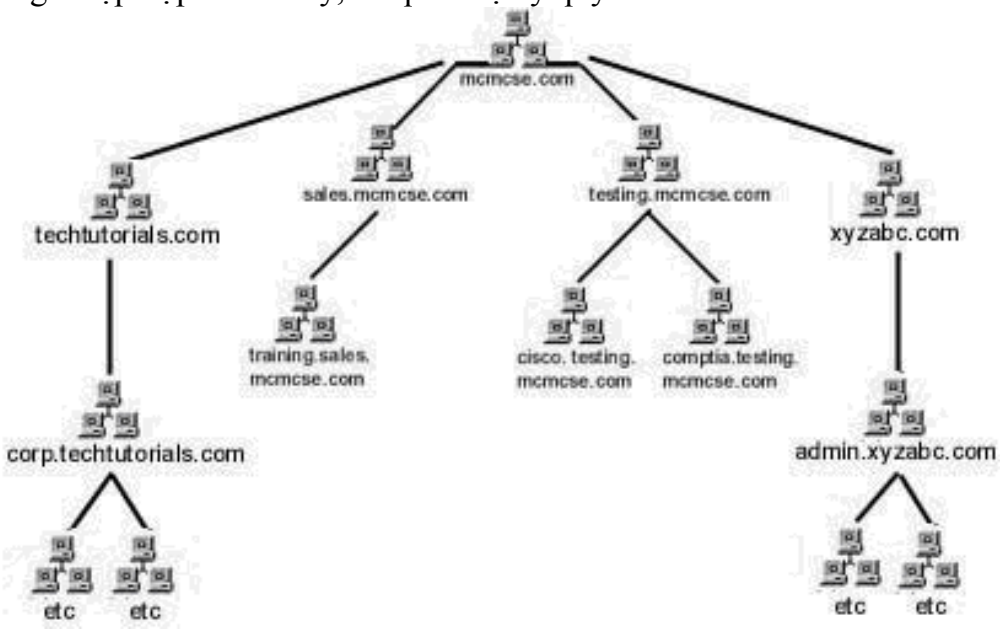
Là một cây đảo ngược các nút là các domain (không được trùng tên), có một gốc gọi là root domain và quan hệ cha (parent domain) con (child domain). Tên domain được viết ngược, miền sales.mcmcse.com là con của miền mcmcse.com.



Hình 7. 25 - Domain tree

Rừng (Forest)

Rừng là tập hợp nhiều cây, có quan hệ ủy quyền lẫn nhau.



Hình 7. 26 - Forest

Thăng cấp Server lên DC

Việc thăng cấp lên DC tương đương với việc cài đặt dịch vụ AD và biến server thành máy quản lý miền.

Trước khi thăng cấp lên DC cần chuẩn bị một miền để DC điều khiển (ví dụ miền doly.vn) và có DNS server để phân giải miền này (vấn đề này sẽ được học sau). Trong phần hướng dẫn này đầu tiên sẽ cài DNS lên server để phân giải miền doly.vn, sau đó mới thăng cấp server này lên DC nhằm mục đích hoàn thiện bài thực hành.

Các điều kiện cần nhớ

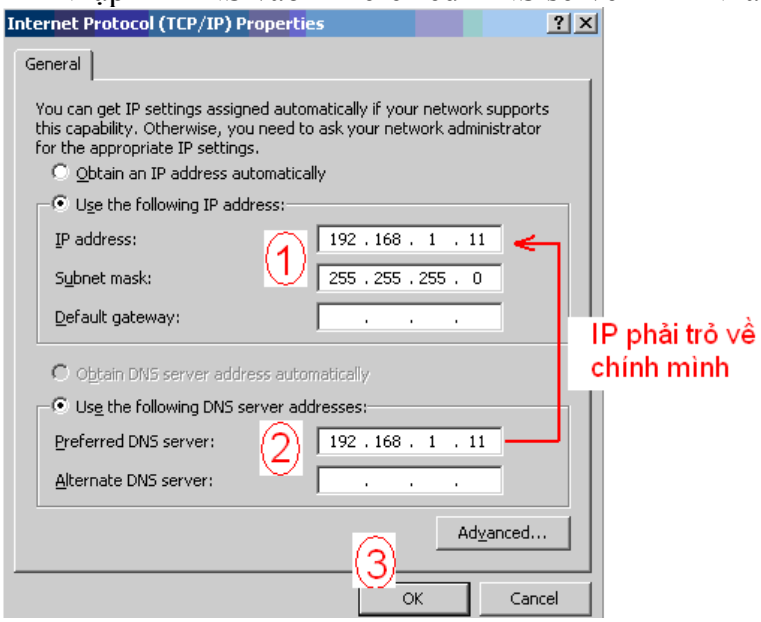
– Server luôn phải có IP tĩnh.
– Preferred DNS Server phải trỏ về chính mình (để phân giải miền doly.vn).

Cài đặt

∗ Bước 1: cấu hình IP tĩnh, DNS trỏ về chính mình, chuẩn bị miền quản lý (Premary DNS Suffix).

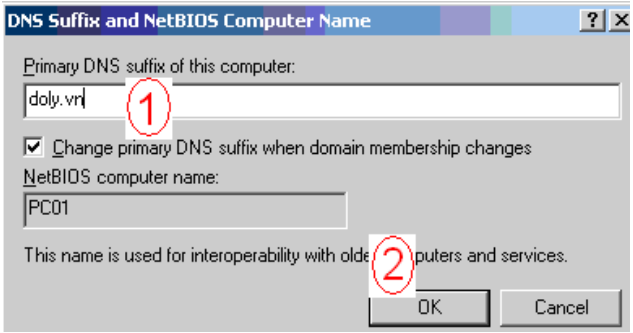
– Trên <Desktop> → Phải chuột lên <My Network Places> → Chọn menu <Properties> → Nhấn đúp chuột lên <Interface> cần cấu hình → Nhấn nút <Properties> → Chọn <Internet Protocol (TCP/IP)> trong <This connection uses the following items> → Nhấn nút <Properties>.

– Hộp thoại <Internet Protocol (TCP/IP) Properties> → Nhập IP vào <IP address> → Nhập IP DNS vào <Preferred DNS server> → Nhấn nút <OK>.



Hình 7. 27 - Trỏ Preferred DNS về chính mình

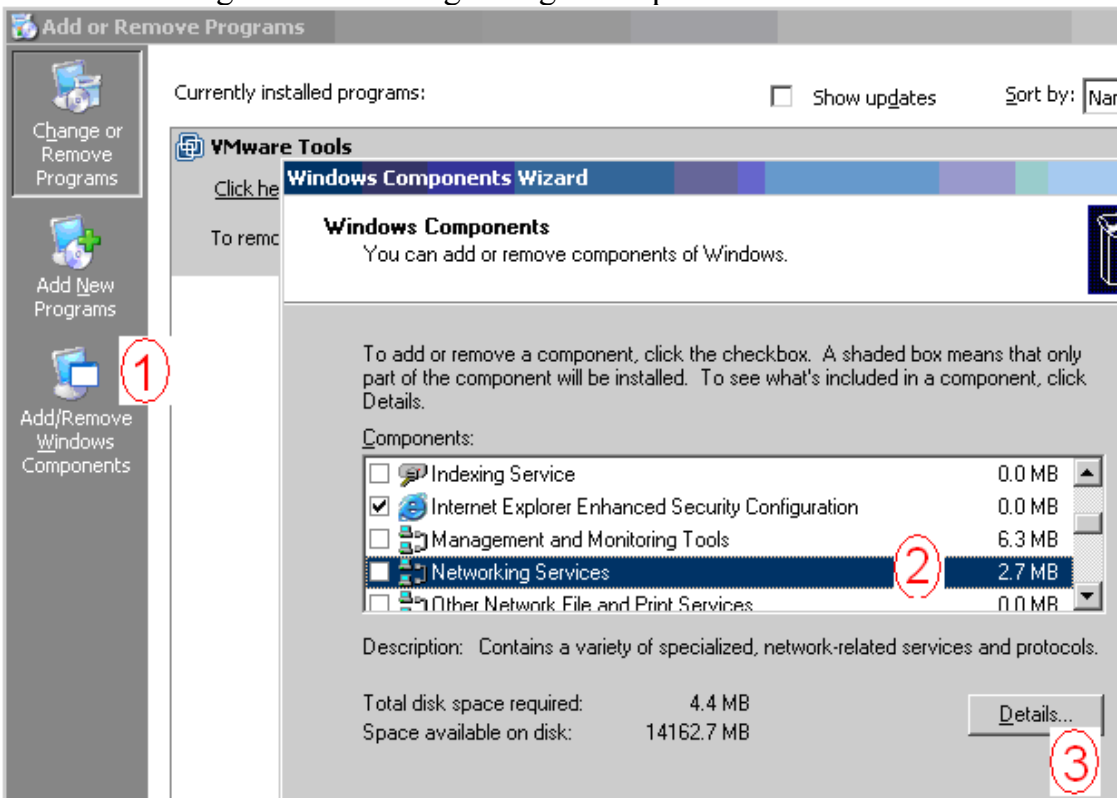
– Trên <***Desktop***> → Phải chuột lên <***My Computer***> → Chọn menu <***Properties***> → Chọn tab <***Computer Name***> → Nhấn nút <***Change...***> → Nhấn nút <***More...***> → nhập vào tên miền <**doly.vn**> trong <***Primary DNS suffix of this computer***> → Nhấn nút <***OK***> → Nhấn nút <***OK***> → Khởi động lại máy tính.



Hình 7. 28 - DNS suffix

∗ Bước 2: cài đặt DNS.

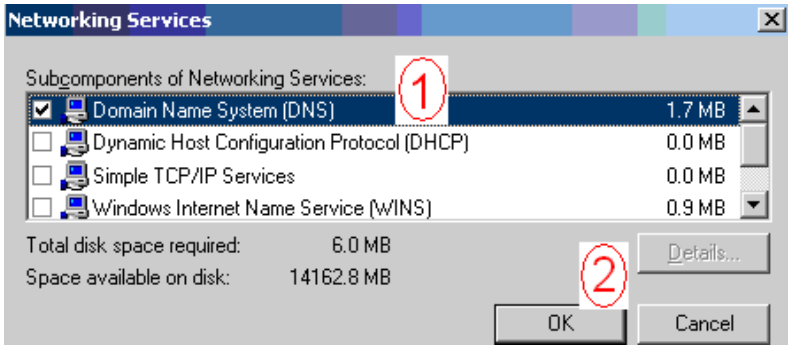
– Vào <Start> → Chọn <All Programs> → Chọn <Control Panel> → Chạy <Add or Remove Programs> → Nhấn nút <Add/Remove Windows Components> → Hộp thoại <Windows Components Wizard> hiện ra → Chọn <Networking Services> trong khung <Components> → Nhấn nút <Details...>.



Hình 7. 29 - Networking services

> Lưu ý: Để mở hộp thoại <Add or Remove Programs> dùng lệnh ***appwiz.cpl***
> Để di chuyển nhanh đến mục <Networking Services> nhấn phím ***N***.
> Không check vào mục <Networking Services> vì các dịch vụ bên trong sẽ chọn hết.

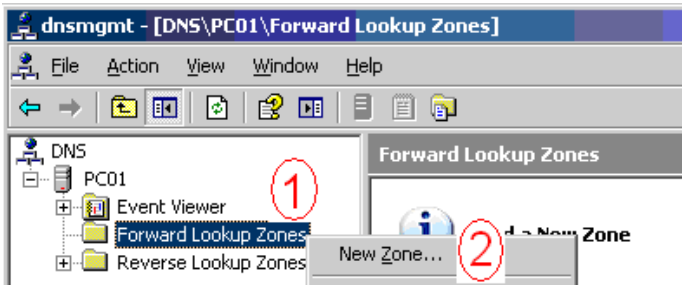
– Hộp thoại ***<Networking Services>*** → Check vào ***<Domain Name System (DNS)>*** → Nhấn nút ***<OK>*** → Nhấn nút ***<Next>***, quá trình cài đặt yêu cầu source i386 của Win2K3 → Nhấn nút ***<Finish>***.



Hình 7. 30 - Cài dịch vụ DNS

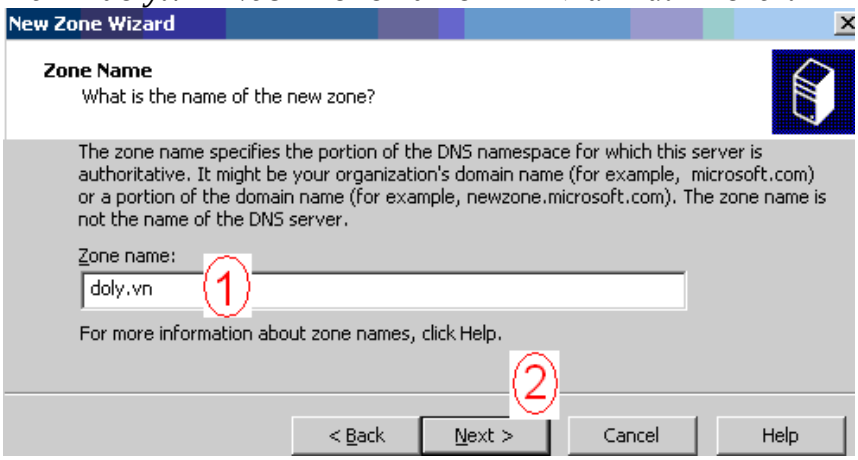
∗ **Bước 3: cấu hình DNS phân giải miền doly.vn.**

– Vào <***Start***> → Chọn <***Administrative Tools***> → Chọn <***DNS***> → Hộp thoại <***dnsmgmt***> mở ra → Click vào dấu cộng tên server → Chọn <***Forward Lookup Zones***> → Phải chuột lên <***Forward Lookup Zones***> → Chọn menu <***New Zone...***>.



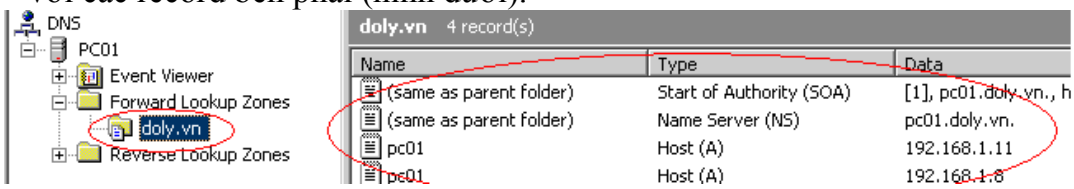
Hình 7. 31 - Tạo Forward lookup zones

– Hộp thoại <***Welcome***> → Nhấn nút <***Next***> → Hộp thoại <***Zone Type***>, chọn option <***Primary zone***> → Nhấn nút <***Next***> → Hộp thoại <***Zone Name***>, nhập tên domain <***doly.vn***> vào <***Zone name***> → Nhấn nút <***Next***>.



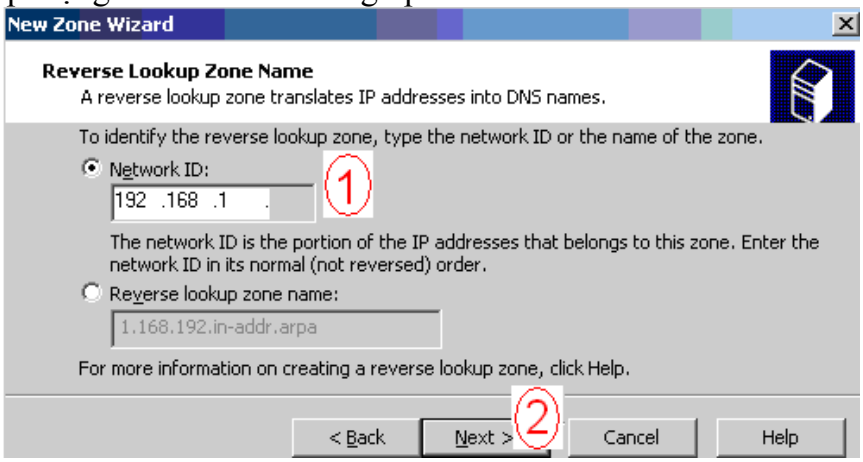
Hình 7. 32 - Nhập tên của zone

– Hộp thoại <***Zone File***>, để mặc nhiên nhấn <***Next***> → Hộp thoại <***Dynamic Update***>, chọn option <***Allow both nonsecure and secure dynamic update***> → Nhấn nút <***Next***> → Nhấn nút <***Finish***> để hoàn tất. Zone doly.vn được tạo ra với các record bên phải (hình dưới).



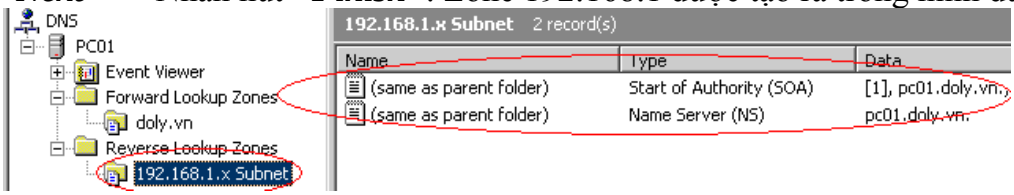
Hình 7. 33 - Các record của Forward lookup zone

– Hộp thoại <dnsmgmt> → Chọn <Reverse Lookup Zones> → Phải chuột lên <Reverse Lookup Zones> → Chọn menu <New Zone...> → Hộp thoại <Welcome>, Nhấn <Next> → Hộp thoại <Zone Type>, chọn option <Primary Zone> → Nhấn nút <Next> → Hộp thoại <Reverse Lookup Zone Name>, nhập vào lớp mạng <192.168.1> trong option <Network ID> → Nhấn nút <Next>.



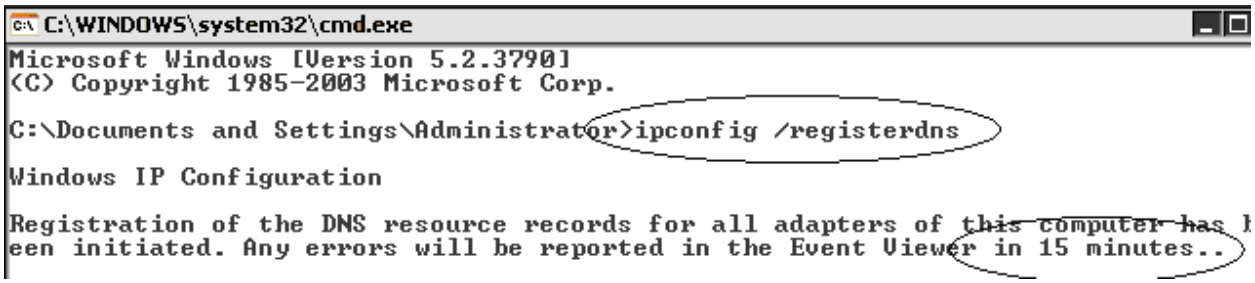
Hình 7. 34 - Tạo Reverse lookup zone

– Hộp thoại <***Zone File***>, nhấn nút <***Next***> → Hộp thoại <***Dynamic Update***>, chọn option <***Allow nonsecure and secure dynamic updates***> → Nhấn nút <***Next***> → Nhấn nút <***Finish***>. Zone 192.168.1 được tạo ra trong hình dưới.



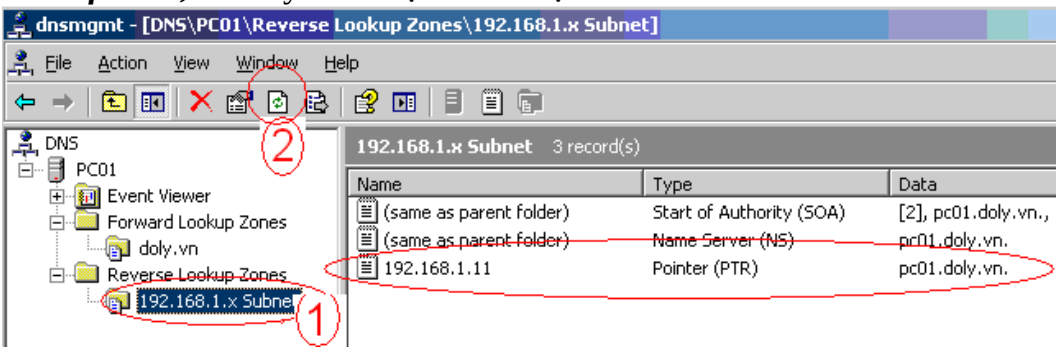
Hình 7. 35 - Các record của Reverse lookup zone

– Zone 192.168.1 còn thiếu một record cần thiết để phân giải tên, tiến hành update bằng dòng lệnh ***ipconfig /registerdns***



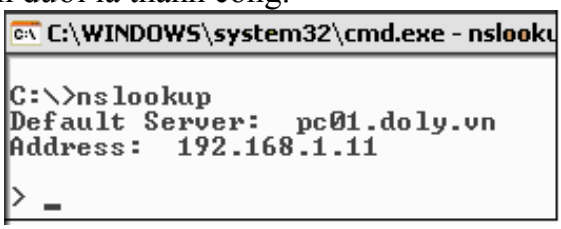
Hình 7. 36 - Cập nhật DNS server

– Quay lại hộp thoại <***dnsmgmt***> → Chọn zone <***192.168.1***> → Nhấn nút <***Prefresh***>, lúc này xuất hiện thêm một record Pointer.



Hình 7. 37 - Record pointer

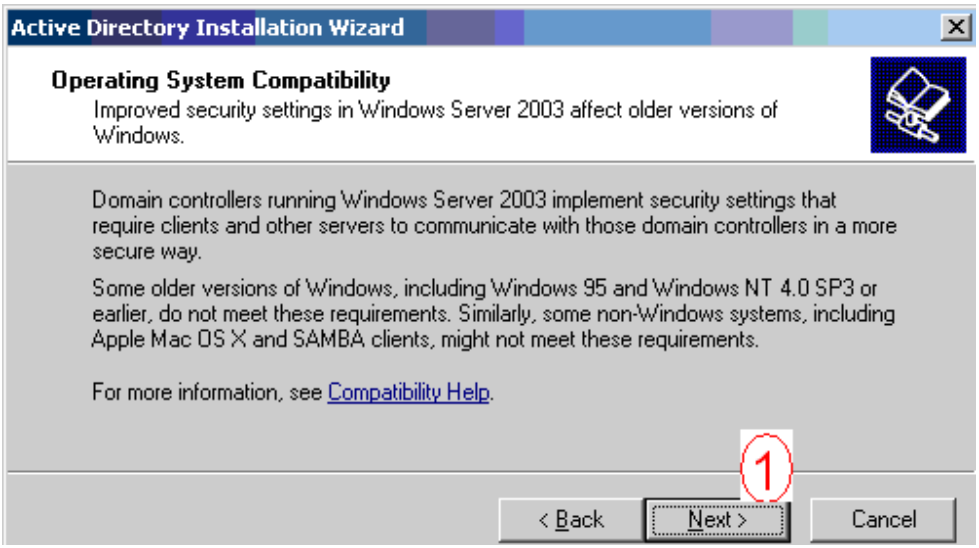
– Để kiểm tra việc phân giải tên có thành công hay không dùng lệnh ***nslookup***, nếu như hình bên dưới là thành công.



Hình 7. 38 - Kiểm tra phân giải tên ra IP

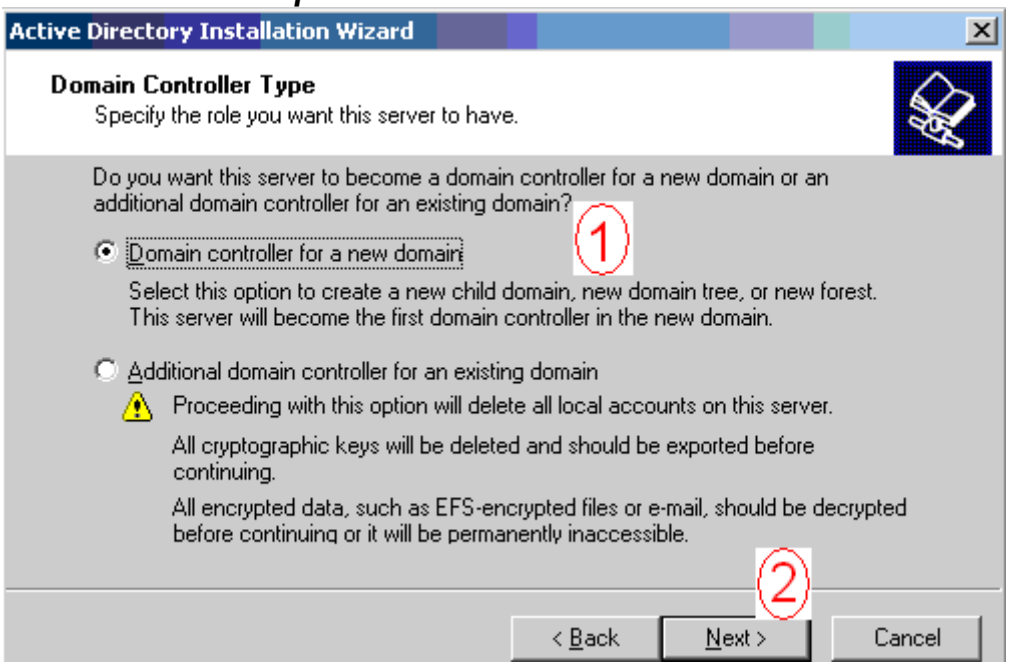
∗ Bước 3: thăng cấp lên DC

– Vào <***Start***> → Chọn <***Run...***> → Chạy lệnh ***dcpromo*** → Hộp thoại <***Welcome***>, nhấn nút <***Next***> → Hộp thoại <***Operating System Compatibility***>, cảnh báo các version cũ (Windows 95, NT 4.0 SP3 và cũ hơn) sẽ bị loại bỏ khỏi miền, nhấn nút <***Next***> .



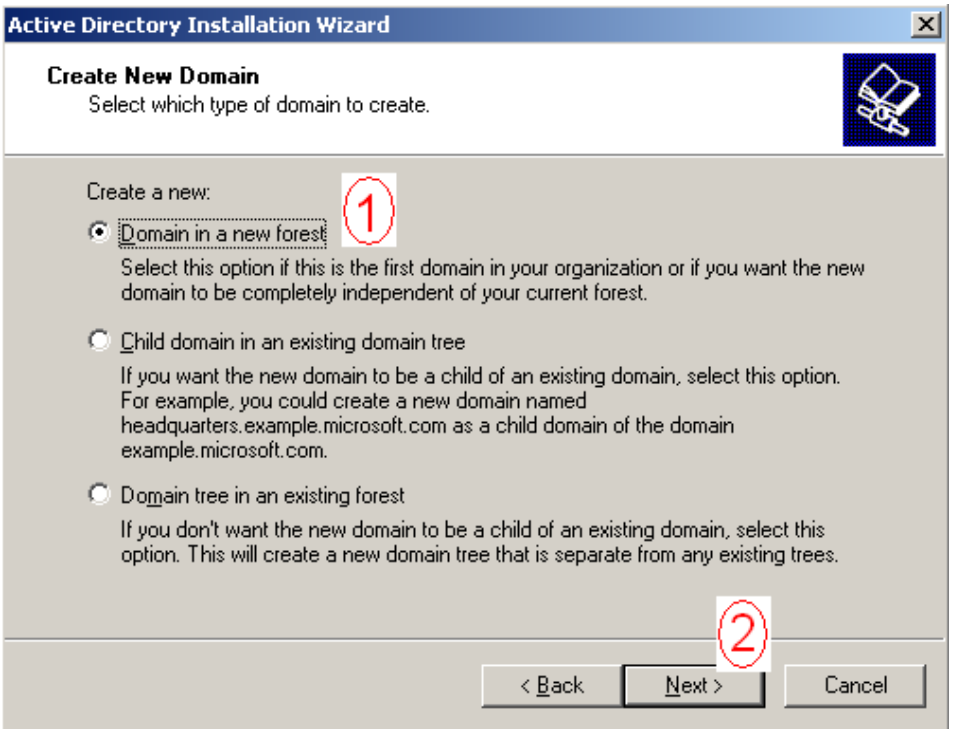
Hình 7. 39 - Cảnh báo tương thích các phiên bản HĐH cũ

– Hộp thoại **<*Domain Controller Type*>** có 2 option. <Domain Controller for a new domain> DC tạo ra quản lý cho miền mới. <Additional domain controller for an existing domain> thêm một DC cho một miền có sẵn → Chọn option **<*Domain Controller for a new domain*>** → Nhấn nút **<*Next*>**.



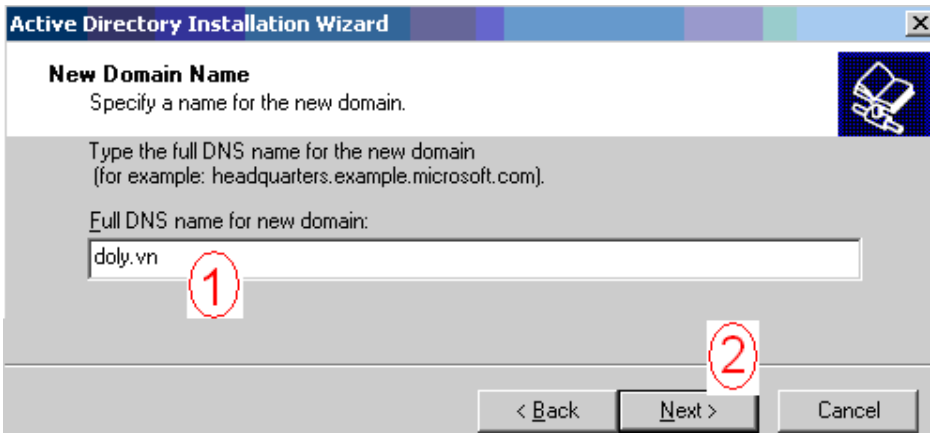
Hình 7. 40 - Dựng DC cho một miền mới

– Hộp thoại **<*Create New Domain*>** có 3 option. <Domain in a new forest> miền này trong một cây hoàn toàn mới. <Child domain in an existing domain tree> miền là con của một cây có sẵn. <Domain tree in an existing forest> một cây trong một rừng có sẵn → Chọn option **<*Domain in a new forest*>** → Nhấn nút **<*Next*>** .



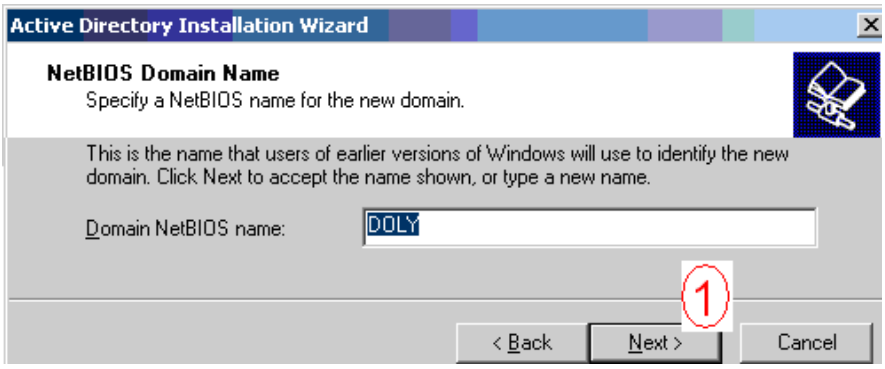
Hình 7. 41 - Dựng DC trong một rừng mới

– Hộp thoại <New Domain Name> → Nhập tên domain đầy đủ doly.vn vào <Full DNS name for new domain> → Nhấn nút <Next>.



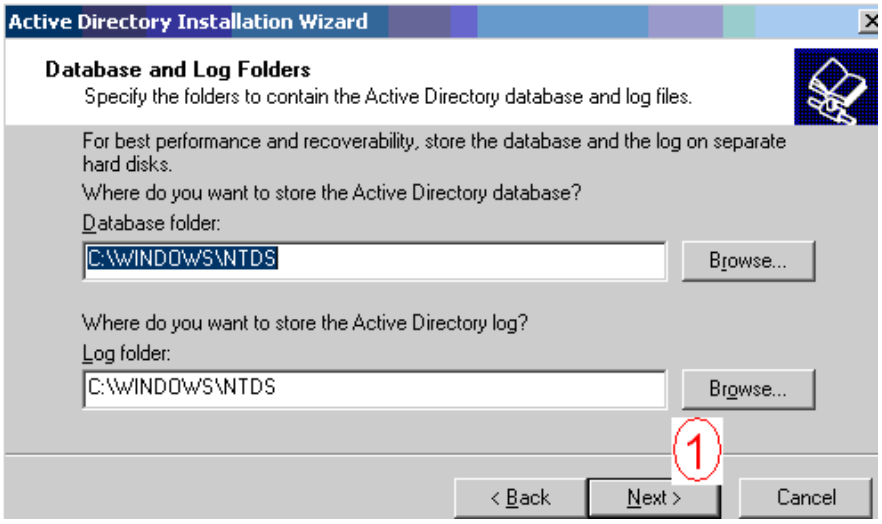
Hình 7. 42 - Nhập tên miền đầy đủ

– Hộp thoại ***<NetBIOS Domain Name>***, tên không phân cấp NetBIOS tương thích cho các version cũ (Windows NT), để nguyên → Nhấn nút ***<Next>*** .



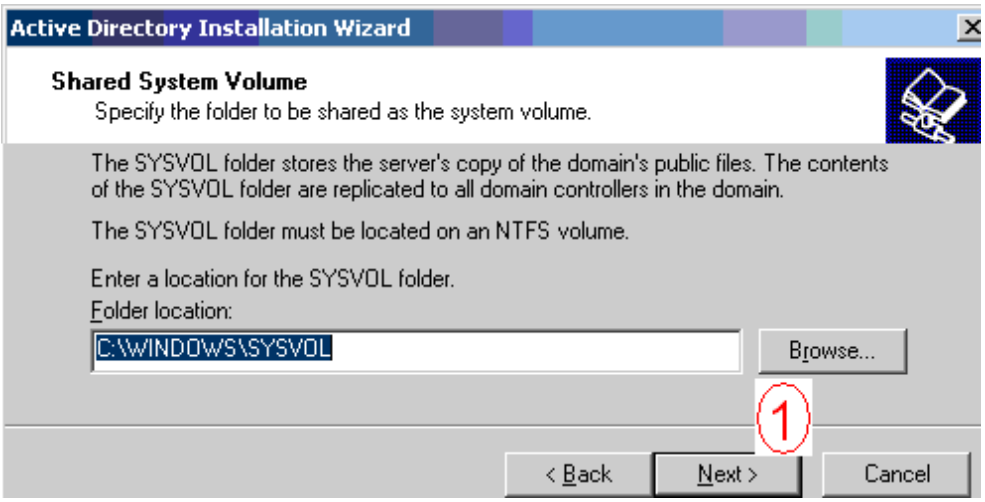
Hình 7. 43 - Nhập tên NetBIOS

– Hộp thoại <***Database and Log Folders***>, đường dẫn lưu database folder và Log folder → Để mặc định ***C:\WINDOWS\NTDS*** → Nhấn nút <***Next***>.



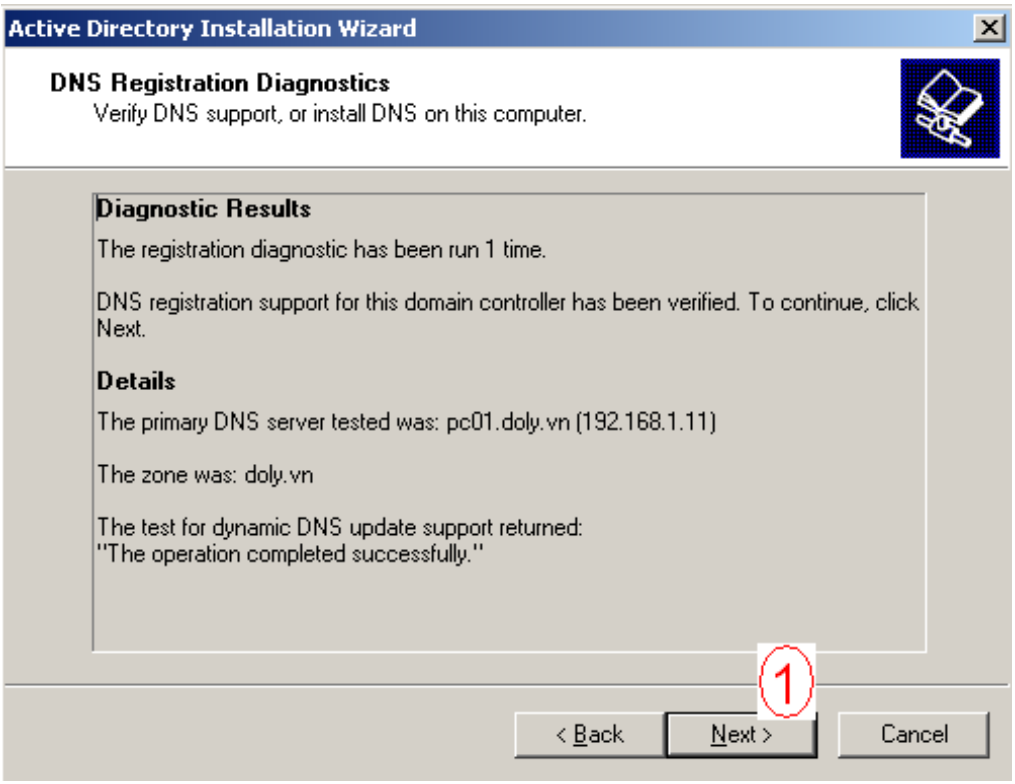
Hình 7. 44 - Vị trí lưu cơ sở dữ liệu AD

– Hộp thoại <***Shared System Volume***>, đường dẫn lưu thư mục SYSVOL. Tất cả dữ liệu trong thư mục SYSVOL sẽ được tự động sao chép sang các DC khác trong miền. Có thể thay đổi nhưng lưu ý thư mục này phải nằm trên một NTFS volume → Để mặc định ***C:\WINDOWS\SYSVOL*** → Nhấn nút <***Next***>.



Hình 7. 45 - Vị trí lưu SYSVOL

– Hộp thoại <***DNS Registration Diagnostics***>, kiểm tra DNS hoạt động chưa (nếu chưa có sẽ hiện hộp thoại cài đặt DNS) → Nhấn nút <***Next***>.



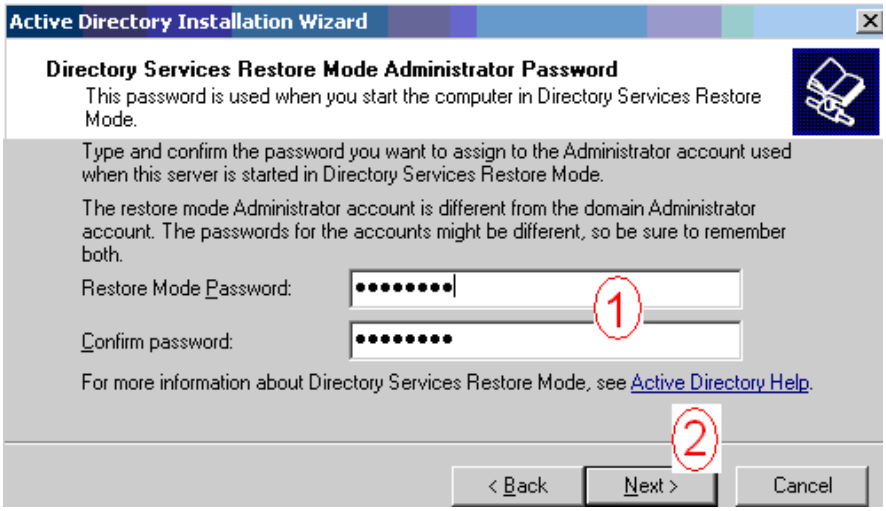
Hình 7. 46 - Kiểm tra DNS server

– Hộp thoại <***Permissions***> có 2 option. <Permission compatible with pre-Windows 2000 server operating systems> sẽ tương thích với các version trước Windows 2000. <Permission compatible only with Windows 2000 or Windows Server 2003 operating systems> khi chắc chắn trong hệ thống mạng chỉ có các version từ Windows 2000 trở lên → Chọn option <***Permission compatible only***

with Windows 2000 or Windows Server 2003 operating systems> → Nhấn nút <***Next***>.

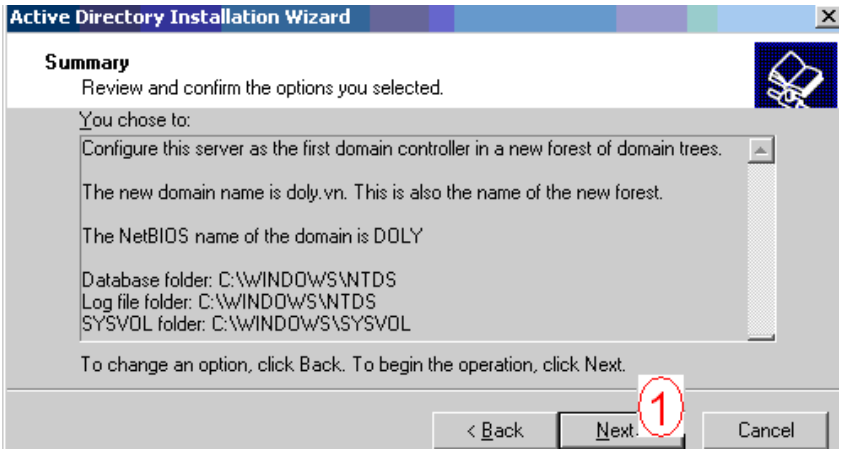
Hình 7. 47 - Loại các server trước Windows 2000

– Hộp thoại <Directory Services Restore Mode Administrator Password> → Nhập vào password cần thiết khi server chạy chế độ <Directory Services Restore Mode> → Nhấn nút <Next>.



Hình 7. 48 - Tạo password cho chế độ restore

– Hộp thoại <***Summary***>, tổng kết lại các thông tin, nếu sai xót nhấn nút <Back> để sửa lại → Nhấn nút <***Next***>.



Hình 7. 49 - Thông tin tổng kết

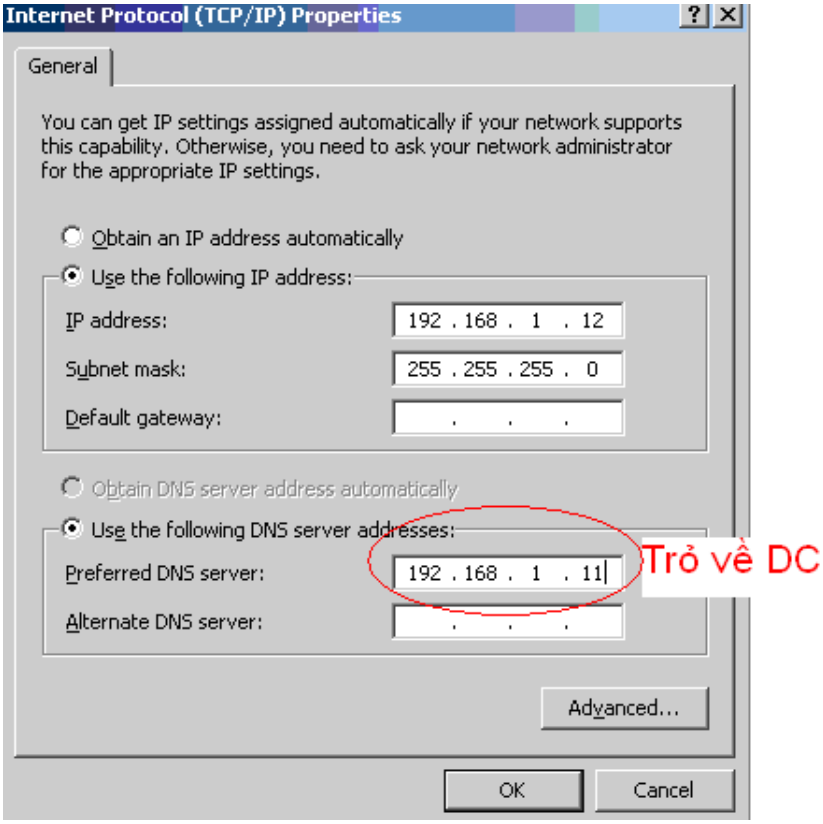
– Quá trình thăng cấp thực hiện → Nhấn <***Finish***> để hoàn tất → Khởi động lại máy tính.

Hình 7. 50 - Quá trình thăng cấp lên DC

7.3.2. Gia nhập máy trạm vào domain (join domain)

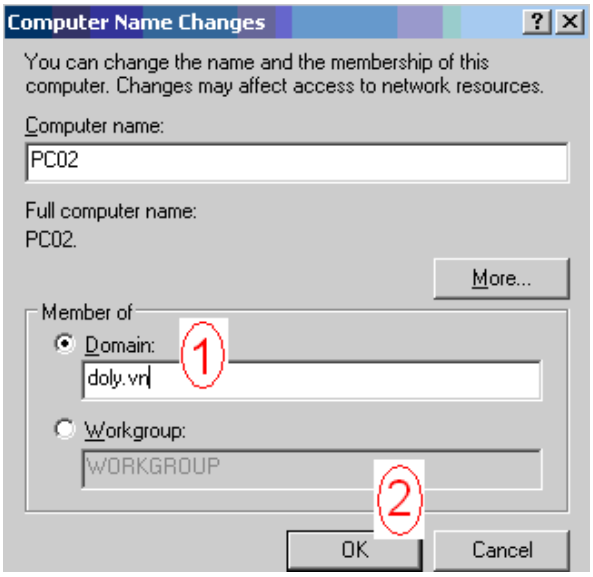
Một máy trạm gia nhập vào một domain là việc thiết lập một mối quan hệ tin cậy (trust relationship) giữa máy trạm đó và DC. Điều kiện gia nhập là máy trạm phải có quyền Administrator trên máy trạm, user trên DC dùng để join phải có quyền Add Workstation to Domain.

– Máy trạm cấu hình IP có Perferred DNS server trỏ về máy DC. Máy trạm phải ping phải thấy máy DC.



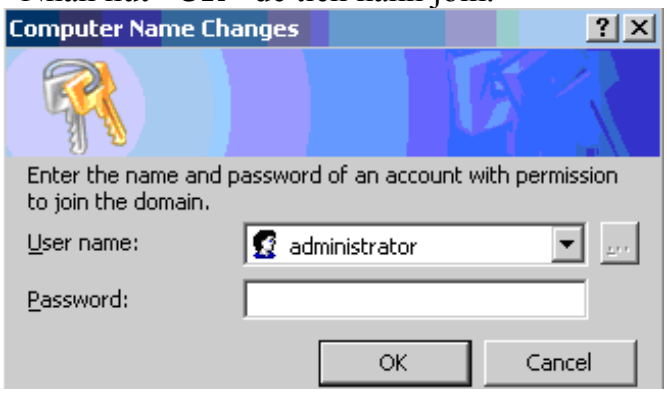
Hình 7. 51 - Trỏ preferred DNS về DC

– Trên <***Desktop***> → Phải chuột lên <***My Computer***> → Chọn menu <***Properties***> → Chọn tab <***Computer Name***> → Nhấn nút <***Change...***> → Trong <***Member of***>, chọn option <***Domain***> → Nhập tên miền <***doly.vn***> vào <***Domain***> → Nhấn nút <***OK***>.



Hình 7. 52 - Join vào miền doly.vn

– Hộp thoại chứng thực hiện lên, phải dùng một user trên DC để join, user này phải có quyền Add Workstation to Domain. Mỗi user chỉ được phép join 10 lần. Điều này tránh trường hợp user khi nào cần dùng tài nguyên thì join vào, khi không cần không join dẫn đến DC không quản lý được → Chứng thực bằng Administrator → Nhấn nút <***OK***> để tiến hành join.

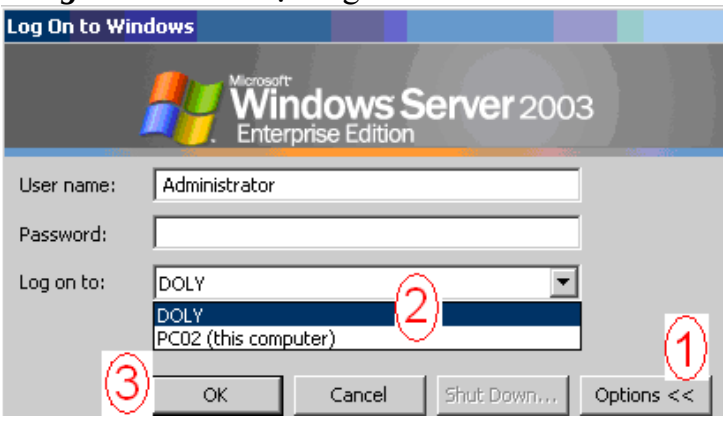


Hình 7. 53 - Dùng Administrator để join domain

– Hộp thoại <***Welcome to the doly.vn domain***> báo join vào miền thành công → Nhấn nút <***OK***> → Nhấn nút <***Finish***> → Khởi động lại máy tính.

Hình 7. 54 - Join thành công

– Hộp thoại <***Log On to Windows***> → Nhấn nút <***Option***> → Click mũi tên xuống của <***Log on to***> → Chọn logon vào miền <***DOLY***> → Nhấn nút <***OK***>.



Hình 7. 55 - Đăng nhập vào miền

Quản trị đối tượng (Object) trong AD

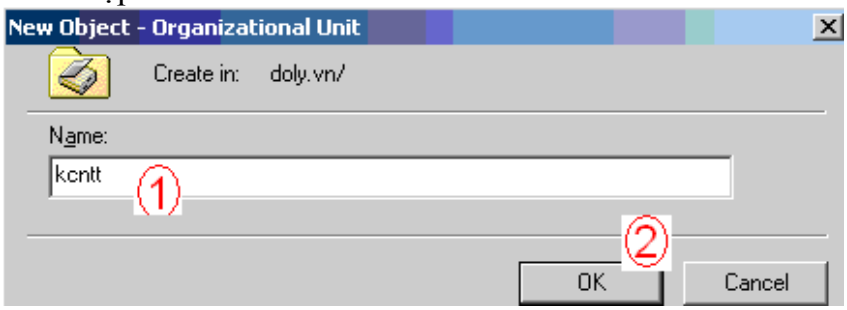
Tạo OU

Trong mô hình Workgroup đã khảo sát ở chương 6. Tạo user trong Computer Managerment trên chính máy local (máy nào lưu user của máy đó, user máy này không thể đăng nhập máy khác).

Trong môi trường Domain, tất cả các workstation và user do DC quản lý. User có thể dùng bất cứ máy nào trong miền để logon vào miền.

Để quản lý một tổ chức lớn như vậy phải phân ra nhiều tổ chức nhỏ. Ví dụ: Trường lytc.edu.vn có các đơn vị tổ chức là Ban giám hiệu, các khoa, các phòng ban chức năng... Trong các khoa có Khoa CNTT... Trong khoa CNTT có tổ mạng... Để quản lý một cách dễ dàng phải phân cấp ra các đơn vị tổ chức OU (Organization Unit). Các Object (user, computer, printer...) của tổ chức nào thì nằm trong OU đó.

– Vào <Start> → Chọn <All Programs> → Chọn <Administrative Tools> → Chọn <Active Directory Users and Computers> → Hộp thoại <Active Directory Users and Computers> hiện ra → Phải chuột lên tên miền <doly.vn> → Chọn menu <New> → Chọn menu <Organizational Unit> → Hộp thoại <New Object> hiện ra → Nhập tên OU vào <Name> → Nhấn nút <OK>.



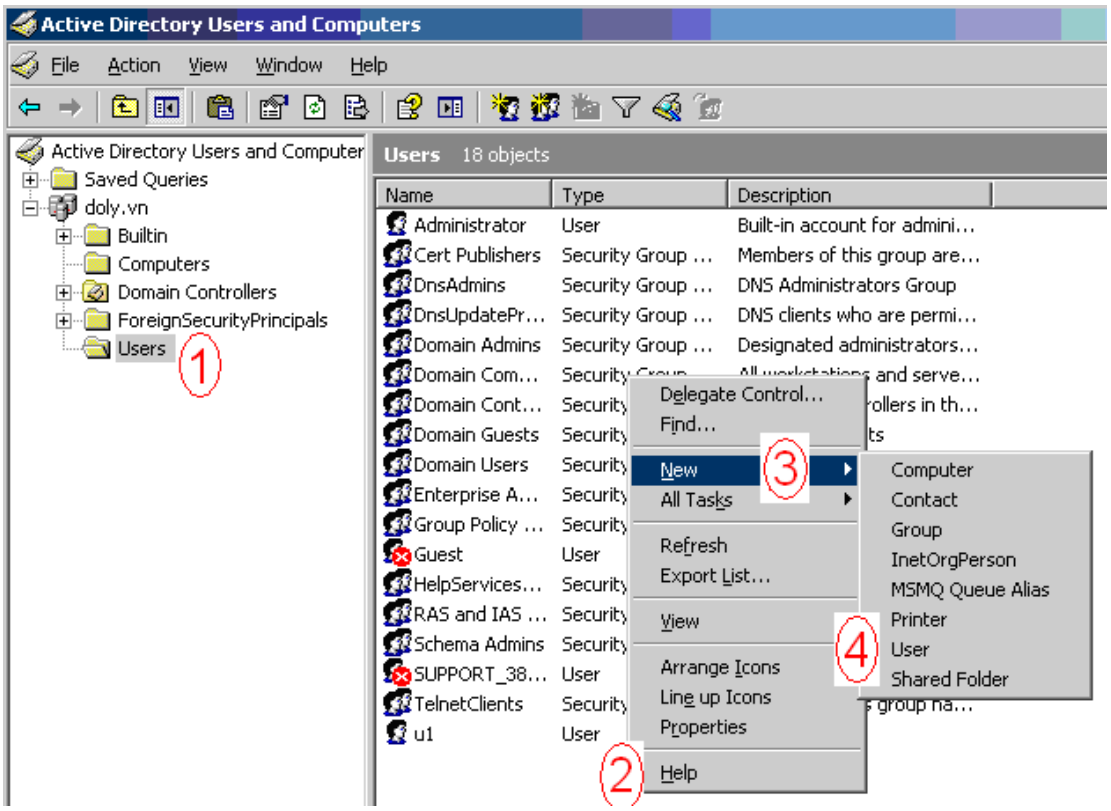
Hình 7. 56 - Tạo OU

Lưu ý: có thể tạo OU bằng dòng lệnh ***dsadd ou "ou=cntt,dc=doly,dc=vn"***

tạo tài khoản người dùng

Ở mô hình domain người dùng do AD quản lý trong ***Active Directory Users and Computer***. Tên user không chứa các ký tự: " / \ [ ] ; : | = , + * ? < >, có thể chứa các ký tự: khoảng trắng, dấu gạch ngang, dấu gạch dưới. Khuyến cáo không dùng ký tự đặc biệt vì sẽ gây khó khăn trong việc dùng dòng lệnh hay kịch bản.

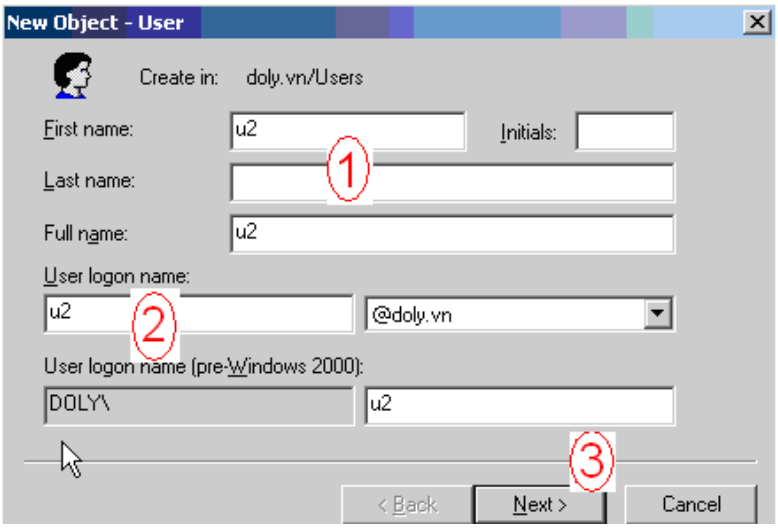
– Vào ***<Start>*** → Chọn ***<All Programs>*** → Chọn ***<Administrative Tools>*** → Chọn ***<Active Directory Users and Computers>*** → Hộp thoại ***<AD Users and Computers>*** hiện ra → Click vào dấu cộng tên miền ***<doly.vn>*** → Chọn ***<Users>*** → Phải chuột lên vùng trắng → Chọn menu ***<New>*** → Chọn menu ***<User>.***



Hình 7. 57 - Tạo user trong AD

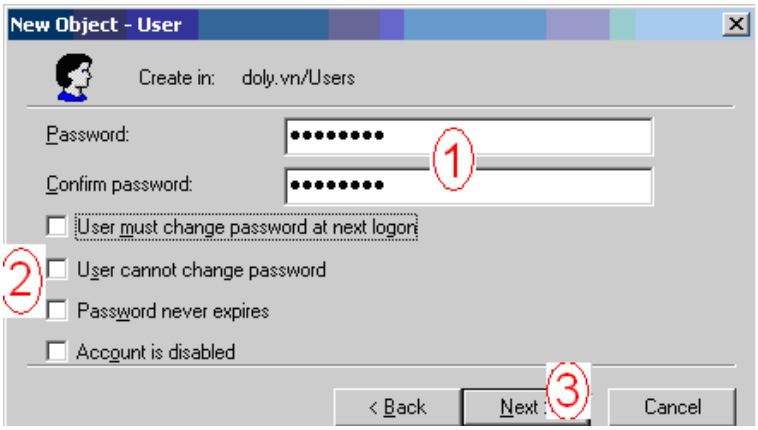
Lưu ý: có thể mở Active Directory Users and Computers bằng lệnh ***dsa.msc***

– Hộp thoại <***New Object – User***> → Nhập tên user <***u2***> trong <***First name***> → Nhập vào tên dùng để logon <***u2***> trong <***User logon name***> → Nhấn nút <***Next***>.



Hình 7. 58 - Nhập thông tin cho user

– Tiếp tục nhập vào password (phức tạp) trong <***Password***>, <***Confirm password***> → Gán các chính sách cho account → Nhấn nút <***Next***> → Nhấn nút <***Finish***>.



Hình 7. 59 - Gán các chính sách cho user

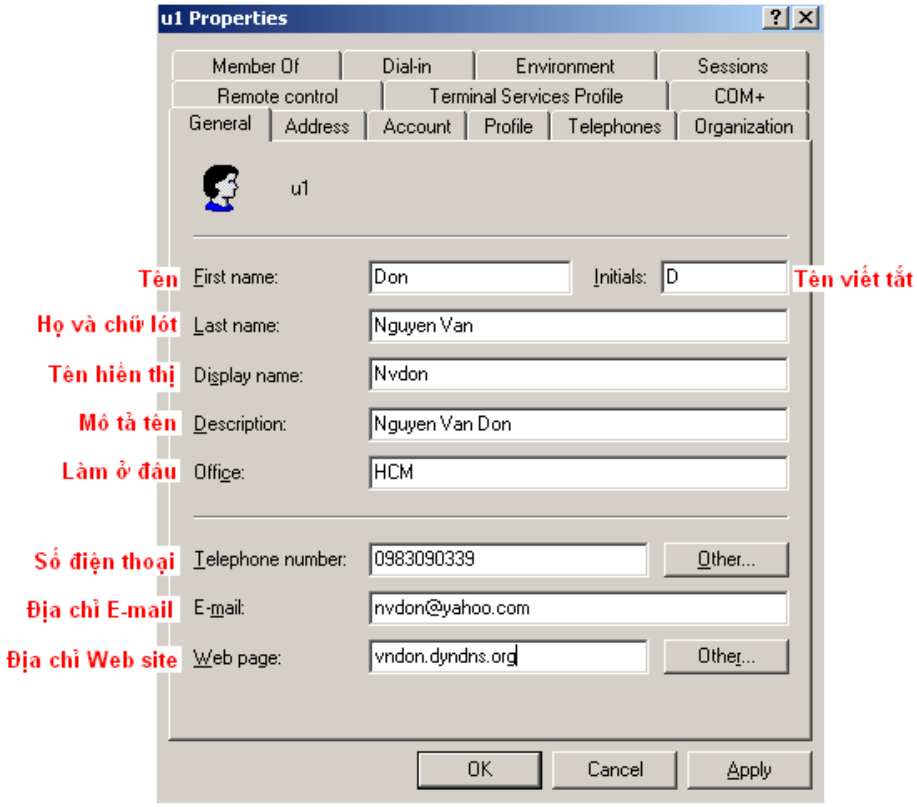
Lưu ý: có thể tạo user bằng dòng lệnh ***dsadd user "cn=u2,ou=kcntt,dc=doly,dc=vn" –pwd P@ssword*** (tạo user u3@doly.vn, nằm trong OU kcntt, có password là P@ssword).

Các thuộc tính tài khoản người dùng

Các thuộc tính của user được dùng để phục vụ cho công tác quản trị. Sau đây giới thiệu một số thuộc tính thông dụng của user.

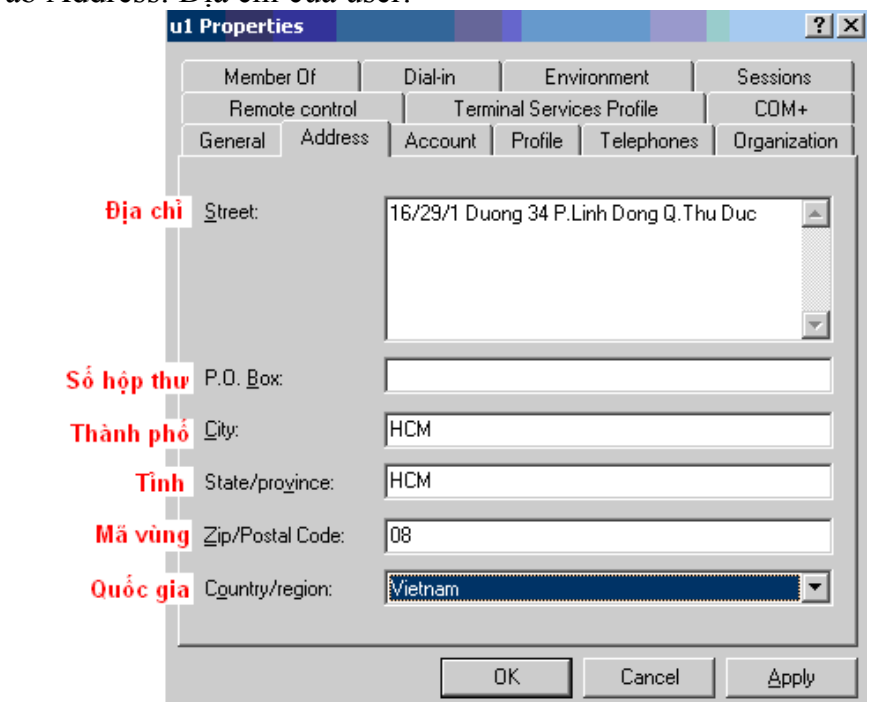
– Trong <***Active Directory Users and Computers***> → Phải chuột lên tên user → chọn menu <***Properties***> → Hộp thoại <***User properties***> hiện lên với 13 tab

– Tab General: những thông tin chung về user.



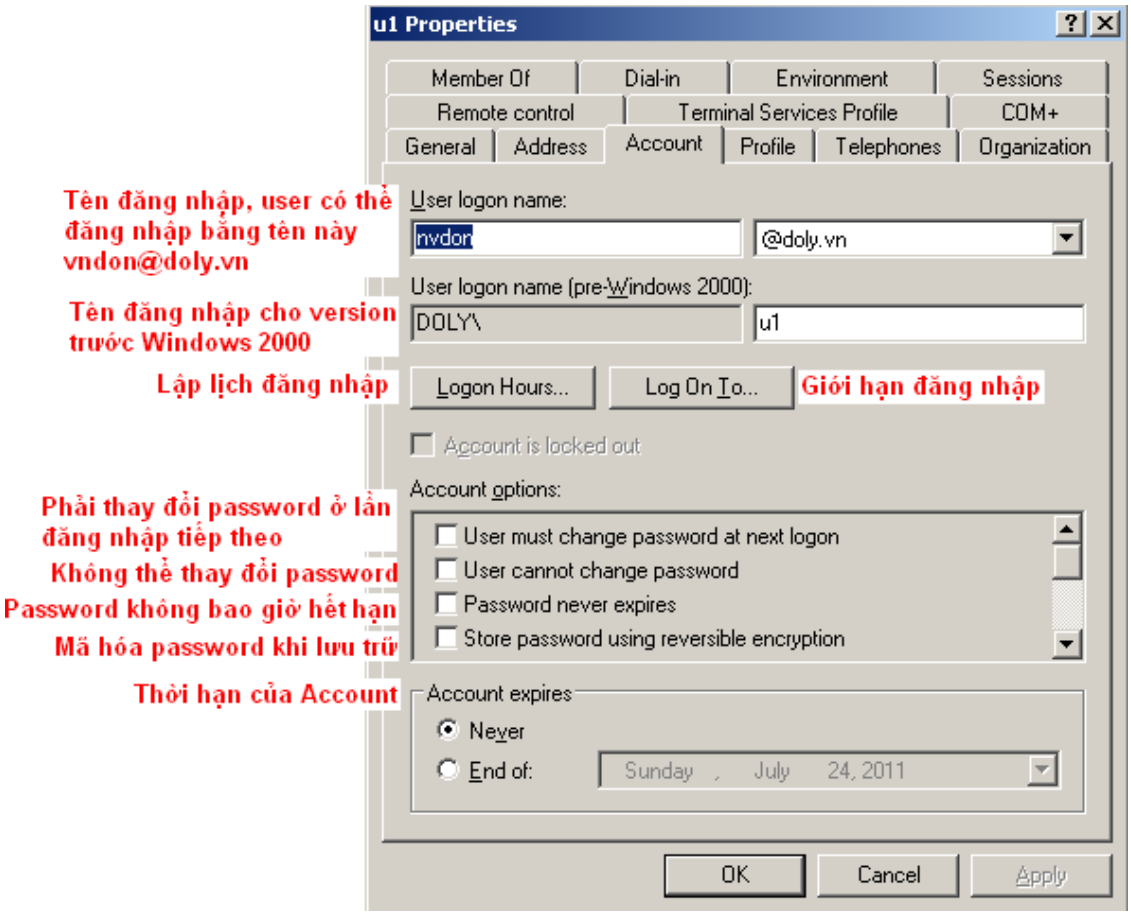
Hình 7. 60 - Cập nhật thông tin chung cho user

– Tab Address: Địa chỉ của user.



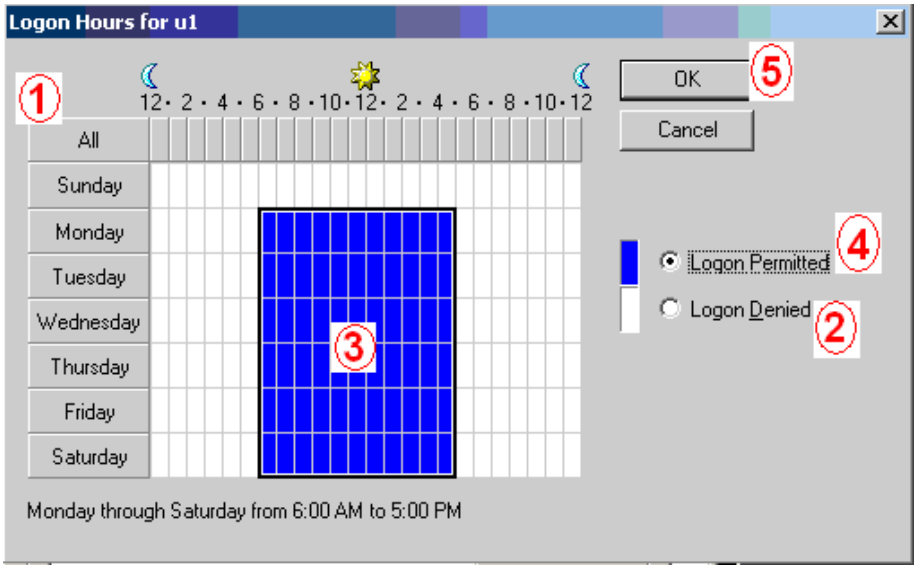
Hình 7. 61 - Cập nhật thông tin địa chỉ cho user

– Tab Account: các chính sách dành cho Account.



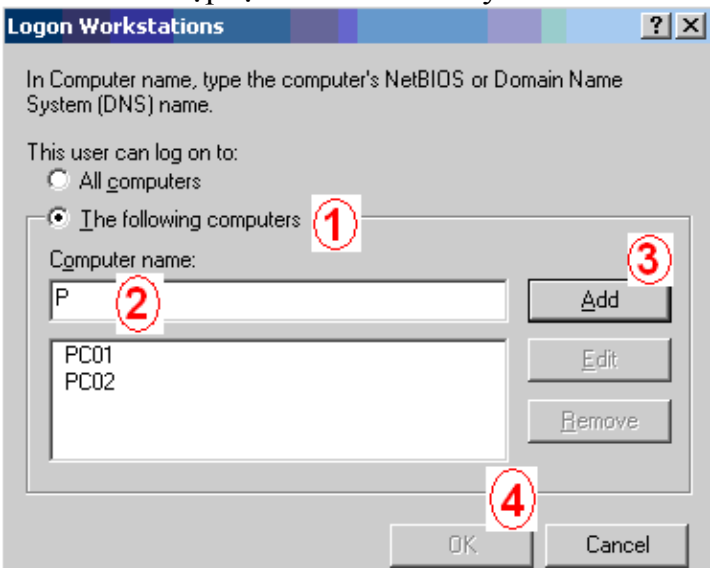
Hình 7. 62 - Cập nhật thông tin về account

- Lập lịch đăng nhập (Logon Hours):
  - Nhấn nút <***Logon Hours...***> trong tab <***Account***>. Mặc nhiên Account được phép đăng nhập 24/7. Thiết lập cho phép Account đăng nhập từ 6 đến 17 giờ các ngày từ thứ 2 đến thứ bảy.
  - Hộp thoại <***Hours for user***>, nhấn nút <***All***> → Chọn option <***Logon Denied***> → Kéo chọn vùng như hình bên dưới → Chọn option <***Logon Permited***> → Nhấn nút <***OK***>.



Hình 7. 63 - Lập lịch đăng nhập

- Giới hạn đăng nhập (Log On to):
  - Nhấn nút <***Log On to...***> trong tab <***Account***>. Mặc nhiên Account này được phép đăng nhập vào tất cả các máy trong miền. Do tính chất bảo mật nên chỉ cho phép Account này đăng nhập vào một số máy: PC01, PC02.
  - Hộp thoại <***Logon Workstations***>, chọn option <***The following computers***> → Nhập tên máy vào <***Computer name***> → Nhấn nút <***Add***> → Lặp lại cho các tên máy khác → Nhấn nút <***OK***>.

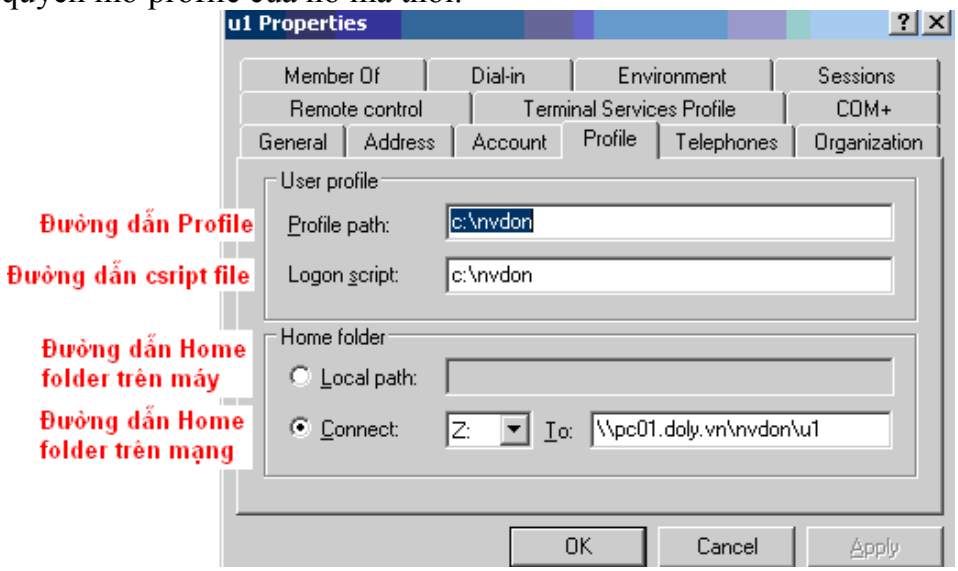


Hình 7. 64 - Giới hạn máy tính đăng nhập

– Tab Profile: nơi lưu thông tin, dữ liệu của người dùng.

- Profile: là thư mục chứa thông tin về môi trường làm việc của người dùng như: desktop, menu start, background, kiểu biểu tượng, sắp xếp biểu tượng... Mặc nhiên người dùng sẽ dùng profile chuẩn và được lưu trong thư mục

%Systemroot%\Documents and Settings\%Username%. User thường chỉ có quyền mở profile của nó mà thôi.

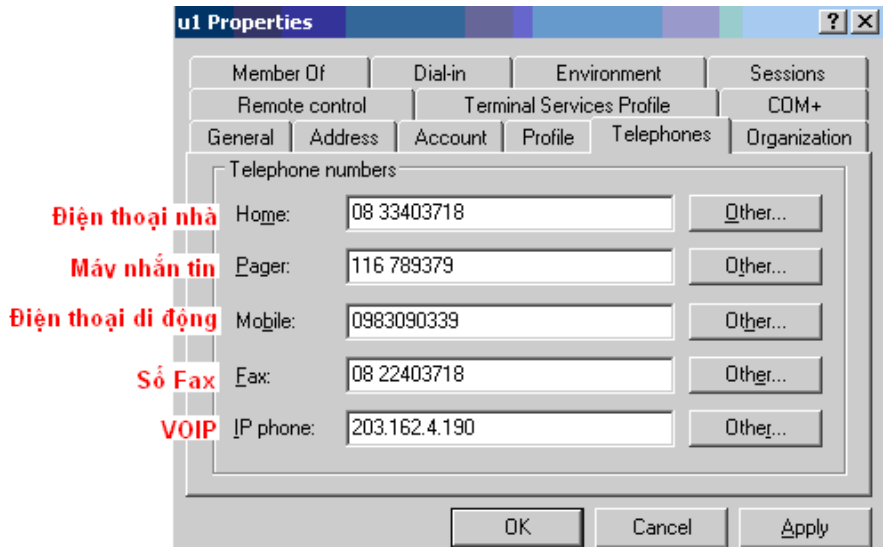


Hình 7. 65 - Nhập thông tin profile

- Script file: là nơi chứa các kịch bản khi đăng nhập, dùng trong trường hợp cần thực hiện một công việc nào đó khi đăng nhập (ví dụ: ánh xạ một ổ đĩa mạng). Kịch bản này có thể viết bằng các ngôn ngữ như VBScript, JScript...
- Home folder: là thư mục dành riêng cho mỗi user để lưu trữ dữ liệu.

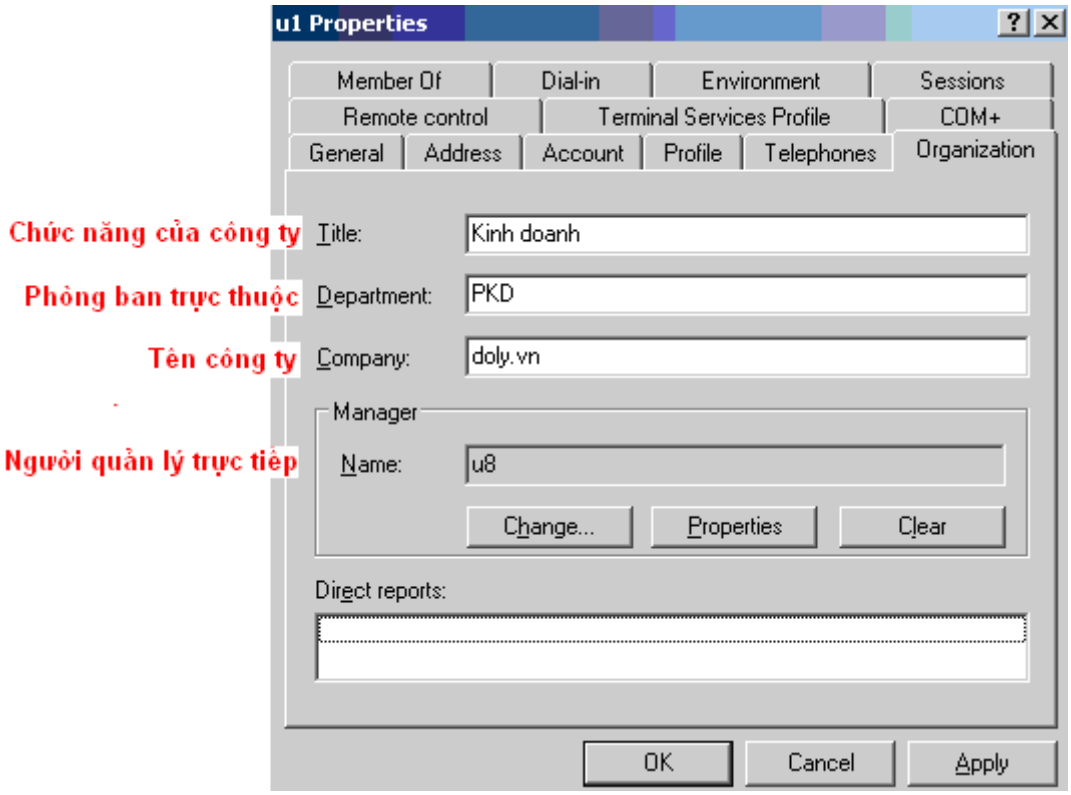
Trong môi trường domain các thông số trên không thiết lập tại đây, mà thường được áp đặt bằng GPO.

– Tab Telephones: chi tiết các số điện thoại của account.



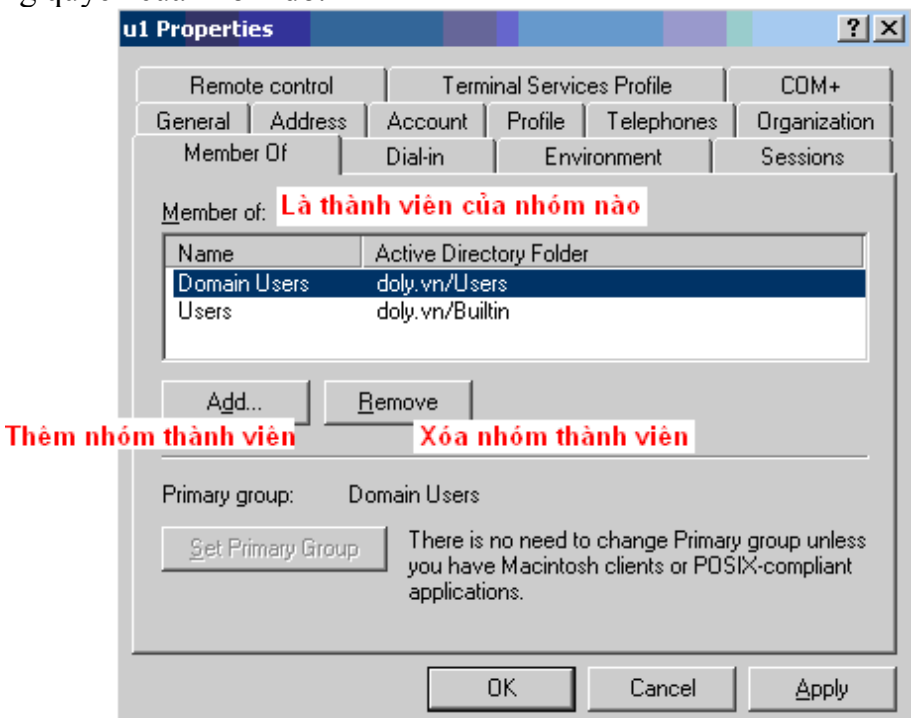
Hình 7. 66 - Cập nhật thông tin về điện thoại

– Tab Organization: thông tin về tổ chức.



Hình 7. 67 - Cập nhật thông tin về tổ chức

– Tab Member of: các nhóm mà user là thành viên. User thuộc nhóm nào thì thừa hưởng quyền của nhóm đó.



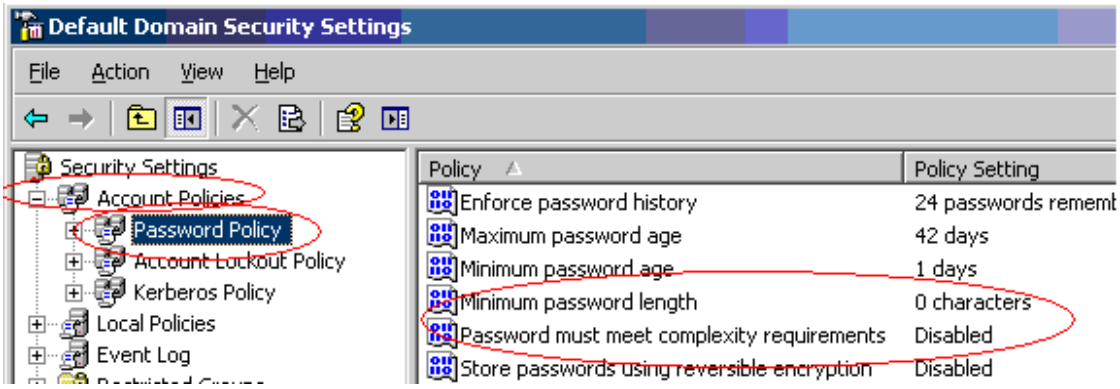
Hình 7. 68 - Thông tin nhóm làm việc

Một số chính sách bảo mật

Domain security policy

Là các chính sách được áp đặt trên domain, để bỏ chính sách thiết lập độ dài và độ phức tạp của password:

– Vào <Start> → Chọn <Administrative Tools> → Chọn <Domain security policy> → Hộp thoại <Default Domain Security Settings> hiện ra → Click vào dấu cộng <Account Policies> → Chọn <Password Policy> → Ở cửa sổ bên phải, double click vào <Minimum password length> → Chỉnh về 0 (nghĩa là không sử dụng) → Double click vào <Password must meet complexity requirement> → Chỉnh về <Disable> → Chạy lệnh gpupdate /force.

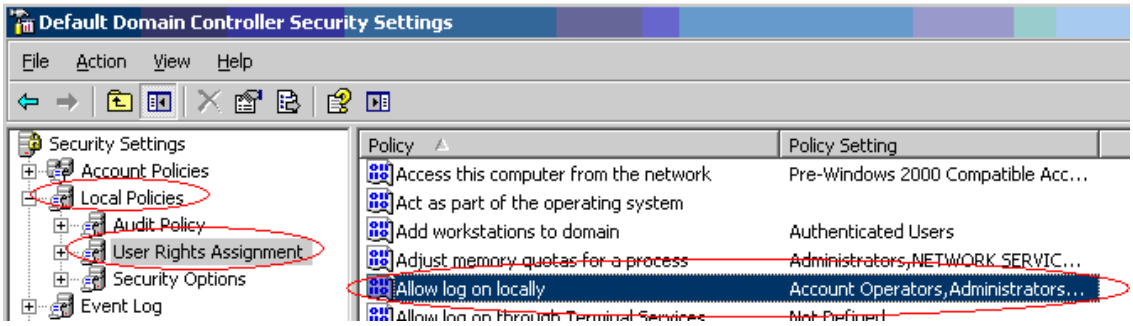


Hình 7. 69 - Password policy

Domain Controller Security Settings

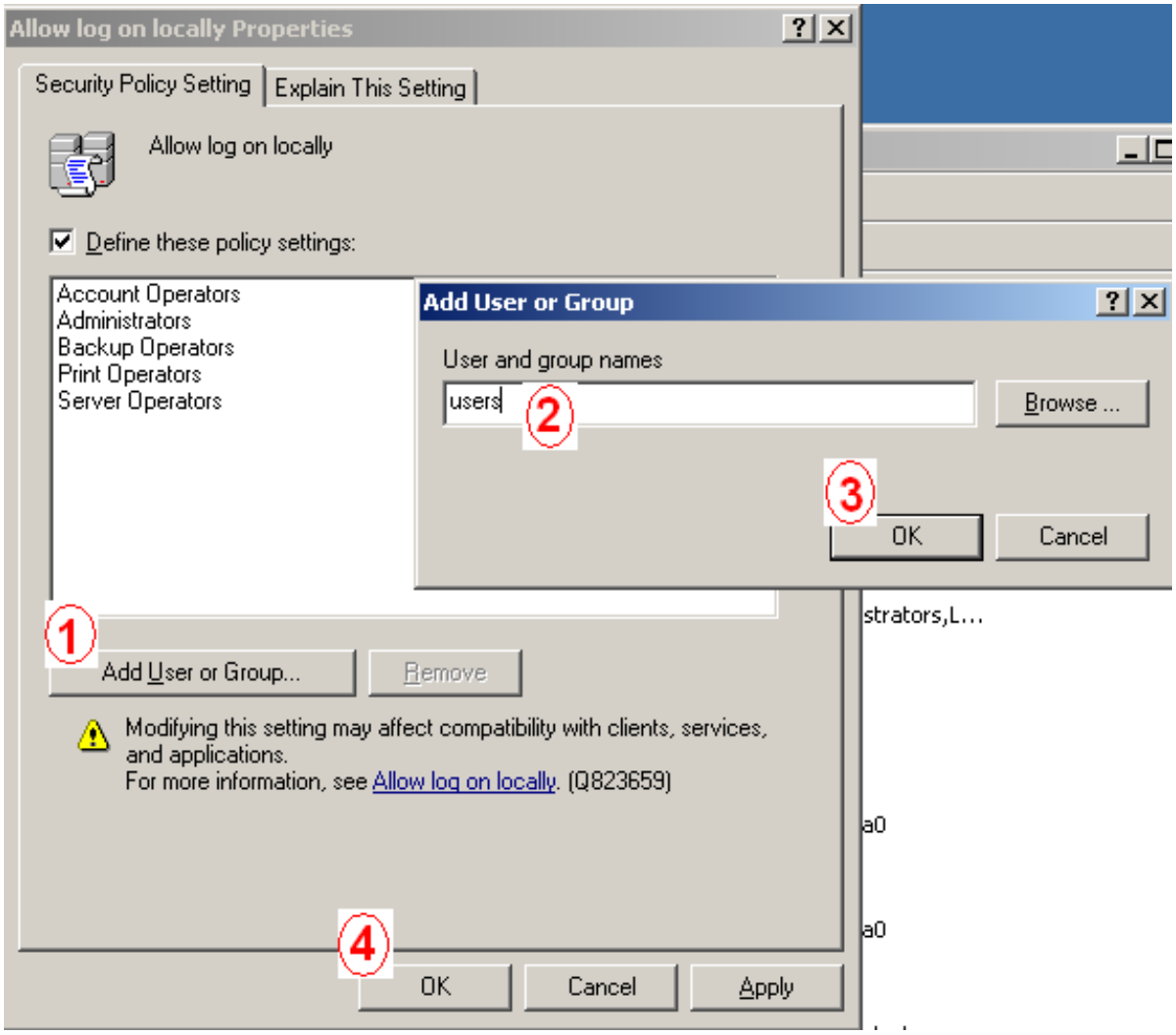
Là các chính sách áp dụng cho DC. Mặc nhiên các user được tạo ra không được phép logon và hệ thống. Cho phép nhóm Users được phép logon:

– Vào <Start> → Chọn <Administrative Tools> → Chọn <Domain Controller Security Settings> → Click vào dấu cộng <Local Policies> → Chọn <User Rights Assignment> → Cửa sổ bên phải, double click vào <Allow log on locally>.



Hình 7. 70 - User right assignment

– Hộp thoại <***Allow log on locally Properties***> → Nhấn nút <***Add User or Group...***> → Hộp thoại <***Add User or Group***> hiện lên → Nhập vào ***Users*** (nhớ có ký tự s sau cùng) trong <***User and group names***> → Nhấn nút <***OK***> → Chạy lệnh ***gpupdate /force***. Lúc này các user thuộc nhóm users mới có thể logon vào hệ thống.



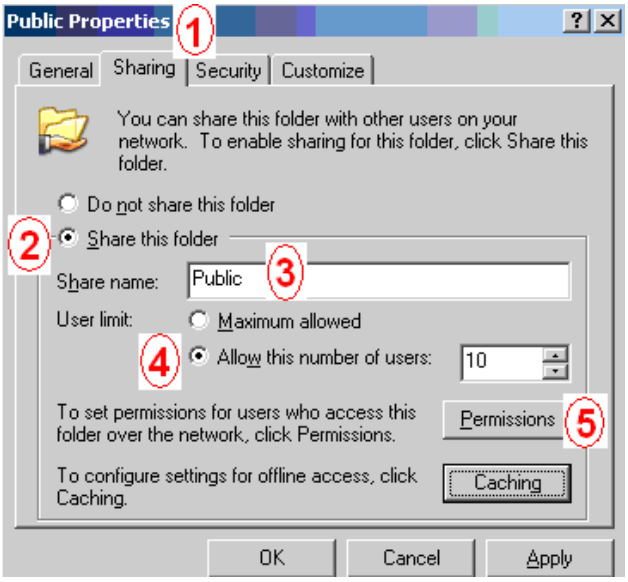
Hình 7. 71 - Cho phép nhóm Users đăng nhập

7.4. Share permission và NTFS permission

7.4.1. Share permission

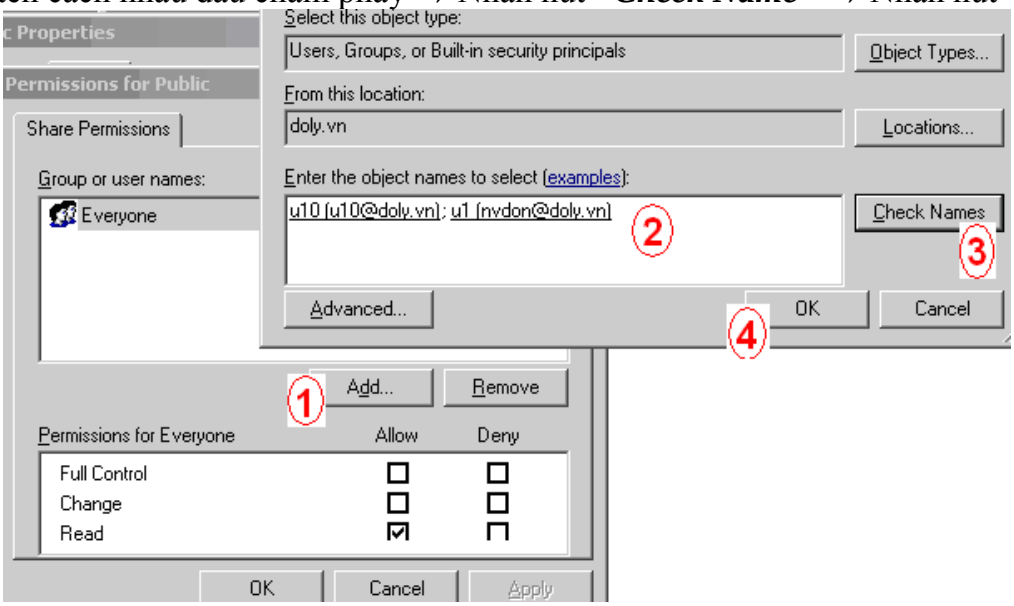
Các tài nguyên hệ thống như thư mục, ổ đĩa, máy in chia sẻ trên mạng cho người dùng sử dụng chung. Các tài nguyên này được phân quyền để đảm bảo rằng tài nguyên sử dụng hiệu quả và đúng mục đích. Trong Windows, khi user chứng thực vào hệ thống bằng quyền rights. Để sử dụng được tài nguyên mạng user đó phải có quyền Share permission.

– Để thiết lập Share permission cho tài nguyên mạng, phải chuột lên tài nguyên → Chọn menu <***Properties***> → Chọn tab <***Sharing***> → Mặc nhiên tài nguyên không được chia sẻ <Do not share this folder>, chọn option <***Share this folder***> để chia sẻ tài nguyên → Nhập tên tài nguyên trên mạng vào <***Share name***> → Nhập ghi chú và <***Comment***> → Mặc nhiên không giới hạn user truy cập cùng lúc, chọn option <***Allow this number of users***> → Nhập vào chỉ cho phép ***10*** user truy cập cùng lúc → Nhấn nút <***Permisstions***> để thiết lập quyền Share permission.



Hình 7. 72 - Share permission

– Hộp thoại <***Permission for Public***> → ở đây <Everyone> được quyền chỉ đọc, nhấn nút <***Add...***> → Nhập tên user vào <***Enter the object name to select***>, các tên cách nhau dấu chấm phẩy → Nhấn nút <***Check Name***> → Nhấn nút <***OK***>.



Hình 7. 73 – Thêm u1 và u10 vào ACL

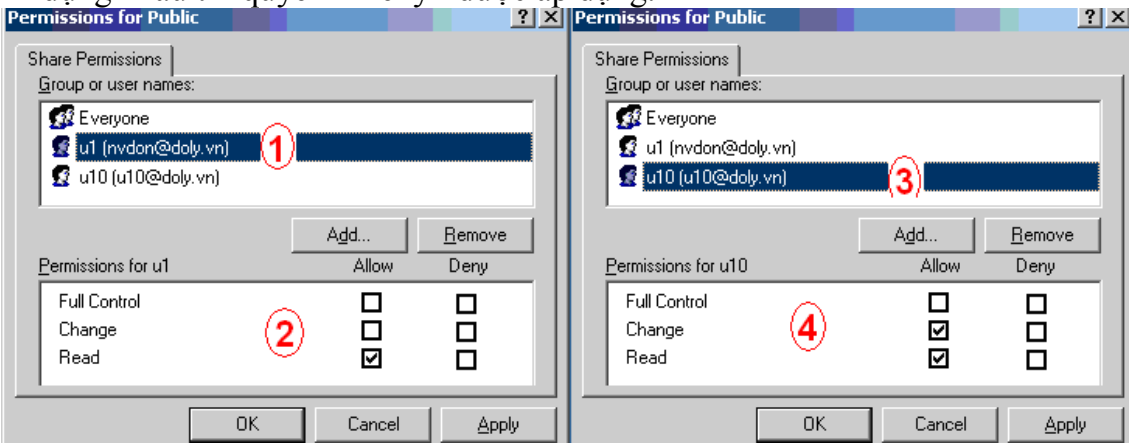
– Hộp thoại <***Permissions for Public***>**,** cho phép lập danh sách các đối tượng cần điều khiển truy cập, còn gọi là Access Control List (ACL) → Chọn <***u1***> → Gán quyền chỉ đọc <***Read***> cho u1. Có 3 quyền:

– Full Control: được toàn quyền đọc và thay đổi nội dung bên trong (thêm, xóa, sửa)

– Change: được quyền thay đổi thêm, xóa, sửa (ví dụ: đối với folder có thể tạo Sub-folder hay file bên trong...). Nếu chọn quyền này thì quyền <Read> tự động chọn luôn (không có quyền đọc thì không thể thay đổi được)

– Read: là quyền chỉ đọc, chỉ xem không được thay đổi gì cả.

– Quyền <Deny> (cấm) cao hơn quyền <Allow> (cho phép), nếu có 2 quyền đụng nhau thì quyền <Deny> được áp dụng.

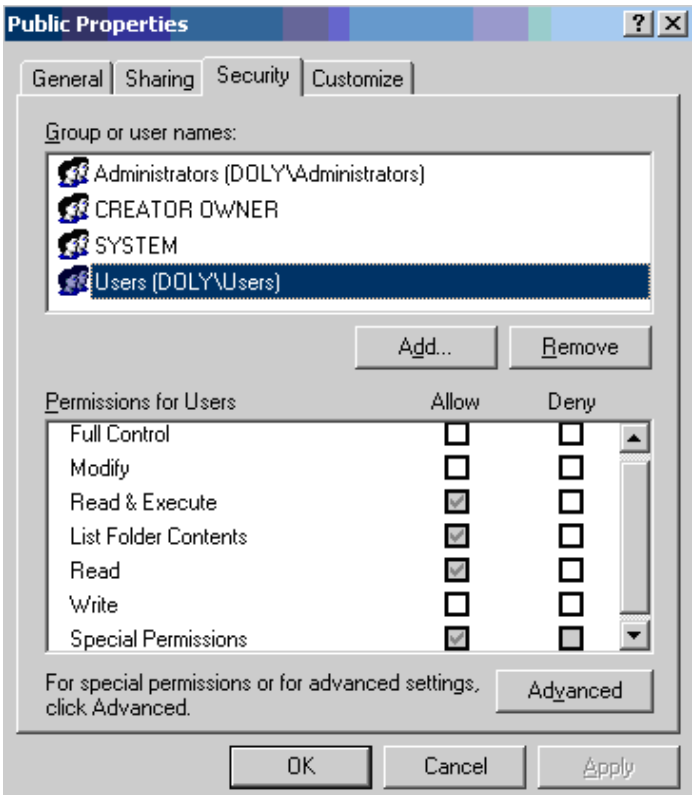


Hình 7. 74 - Phân quyền share cho u1 và u10

NTFS Permission

NTFS Permission chỉ áp dụng cho các tài nguyên định dạng NTFS, các ALC của NTFS Permission được lưu cùng tài nguyên đó nên có thể giữ lại dù hệ điều hành có thay đổi. Các ALC sẽ kiểm soát quyền truy cập tài nguyên.

– Phải chuột lên tài nguyên định dạng NTFS → Chọn menu <***Properties***> → Chọn tab <***Security***> → Chọn nhóm <***Users***> → Trong hộp thoại <***Permissions for Users***> nhóm Users có các quyền <Read & Execute> <List Folder Contents> <Read> <Special Permisstions>, không thể bỏ các quyền này vì nó kế thừa quyền từ object cha. Có các quyền chung sau:

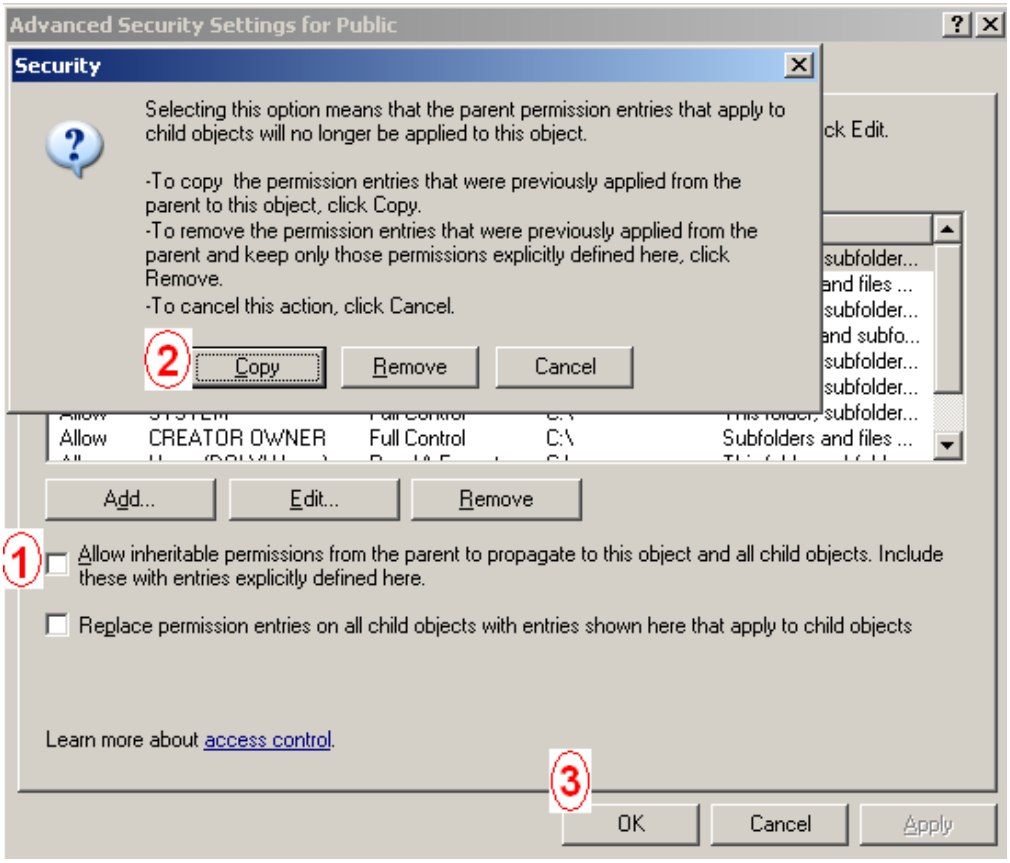


Hình 7. 75 - Quyền NTFS của nhóm Users

– Full Control: toàn quyền, check vào mục này toàn bộ cột đều bị check theo.
– Modify: có thể xem thuộc tính và định dạng, thêm xóa sửa. Nhưng không được chiếm quyền chủ sở hữu và thay đổi NTFS Permission.
– Read & Execute: có thể chạy các file thực thi (để chạy được phải có quyền đọc).
– List Folder Contents: có thể mở một folder xem nội dung bên trong.
– Read: có thể đọc và xem thuộc tính file.
– Write: có thể thay đổi nội dung file.
– Special Permissions: các quyền đặc biệt, để hiện các quyền này nhấn nút <Advanced>.

Thông thường để phân quyền cho các user nên xóa nhóm Users, và thêm các object vào để phân quyền. Vì nhóm Users được thừa hưởng quyền từ object cha nên không thể xóa nhóm Users. Muốn làm được điều này, phải bỏ quyền thừa hưởng.

– Trong hộp thoại <Public Properties> → Nhấn nút <Advanced> → Hộp thoại <Advanced Security Settings for Public> hiện ra → Bỏ check <Allow inheritable permissions from the parent...> → Hộp thoại <Security> hiện ra → Nhấn nút <Copy> → Nhấn nút <OK>, bây giờ có thể xóa nhóm Users.



Hình 7. 76 - Bỏ quyền thừa hưởng của nhóm Users

Kết hợp Share permission và NTFS permission

– Kết hợp 2 quyền cùng loại thì cho quyền lớn hơn (phép hội).
– Kết hợp 2 quyền khác loại thì cho quyền nhỏ hơn (phép giao).

7.5. Câu hỏi và bài tập

1. Hãy phân biệt quyền hệ thống (rights), quyền truy cập Share permission và NTFS permission?
2. Hãy tắt chính sách password phải lớn hơn 7 ký tự và phải phức tạp.
3. Hãy thiết lập chính sách cho phép nhóm users đăng nhập vào hệ thống.
4. Tại sao khi thăng cấp lên miền phải cài dịch vụ DNS và trỏ IP Preferrerd DNS về chính mình?
5. Trình bày điều kiện để một máy có thể gia nhập vào miền?
6. Trình bày kiến trúc của AD?
7. Trình bày khái niệm Profile và Home directory?
8. Cho bảng NTFS permission như sau

	Folder C:\Public	**Folder C:\Private**	**Folder C:\Limit**
u1	đọc, ghi	chỉ đọc	cấm đọc
u2	đọc, ghi	chỉ đọc	chỉ đọc

a/ Hãy tạo thư mục và thiết lập quyền như trong hình trên?
b/ Thiết lập quyền sao cho u1, u2 chỉ được quyền xóa file và folder do mình tạo ra trong thư mục C:\Public?

9. Cho biết kết quả của việc kết hợp các quyền permission?

Share permission	NTFS permission	Kết quả
Full	Modify	
Read	Read & List Folder Content	
Change	Read	
Read	Write	
Change	Modify	

10. Hãy tạo ra một file kịch bản cài đặt, tìm hiểu và ghi nhận lại các thông số trong file này?

DỊCH VỤ DHCP

∗ **Tóm tắt nội dung chương 8**

- Giới thiệu, trình bày nguyên tắc hoạt động của DHCP.
- Hướng dẫn chi tiết các bước cài đặt, cấu hình dịch vụ DHCP trên Windows Server 2003, router ADSL.
- Các lỗi thường gặp và cách khắc phục.

∗ **Mục tiêu chương 8**

Sau khi học xong sinh viên có khả năng:

- Trình bày được nguyên tắc hoạt động của dịch vụ DHCP.
- Cài đặt và cấu hình dịch vụ DHCP trên Windows Server 2003 và trên các router.
- Nêu các lỗi thường gặp và cách khắc phục.

Giới thiệu

DHCP (Dynamic Host Configuration Protocol) là dịch vụ cấp IP động cho các host trong mạng do IETF phát triển trong các RFC 1533, 1534, 1541, 1542. Tiền thân của DHCP là BOOTP, vẫn còn sử dụng trong hệ thống Bootrom. DHCP sử dụng port UDP 67.

∗ **Một số ưu điểm của dịch vụ DHCP:**

- Tiết kiệm chi phí quản trị cấp phát địa chỉ IP.
- Tránh việc đụng độ IP trên mạng giúp các host nhận IP một cách dễ dàng.
- Trong một môi trường các host không cố định (ví dụ: nhà ga, sân bay các máy tính chỉ gia nhập mạng một lần) thì việc cấp phát IP trở nên hiệu quả, tiện lợi.
- Các ISP cấp IP public động cho người sử dụng, việc này tiết kiệm IP một các hiệu quả.

Lưu ý: tất cả các server đều sử dụng IP tĩnh.

Hoạt động của DHCP

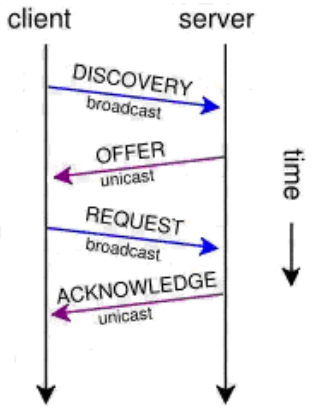
DHCP hoạt động theo mô hình Client/Server, quá trình hoạt động của DHCP gồm 4 bước:

∗ **Bước 1: máy Client cần thuê IP sẽ broadcast gói tin *DHCPDISCOVER* lên toàn mạng yêu cầu một server cung cấp IP cho mình. Trong gói tin này có địa chỉ MAC của client.**

∗ **Bước 2: các DHCP server trên mạng đều nhận được gói tin này. Nếu server có khả năng cung cấp IP nó sẽ gửi cho client gói tin *DHCPOFFER* đề nghị cho thuê IP trong khoảng thời gian nhất định, kèm theo các thông số (default gateway, dns...). IP này sẽ không được chào mời cho các client khác trong thời gian thương thuyết.**

∗ Bước 3: client chọn một IP trong số các IP đề nghị và broadcast gói tin *DHCPREQUEST* yêu cầu server cho thuê IP. Các server không được thuê IP sẽ rút IP lại.

∗ Bước 4: server gửi cho client một gói tin *DHCPACK* xác nhận việc cho thuê IP kèm theo các thông số.



Hình 8. 1 - Hoạt động của DHCP

Cài đặt DHCP trên Win2K3

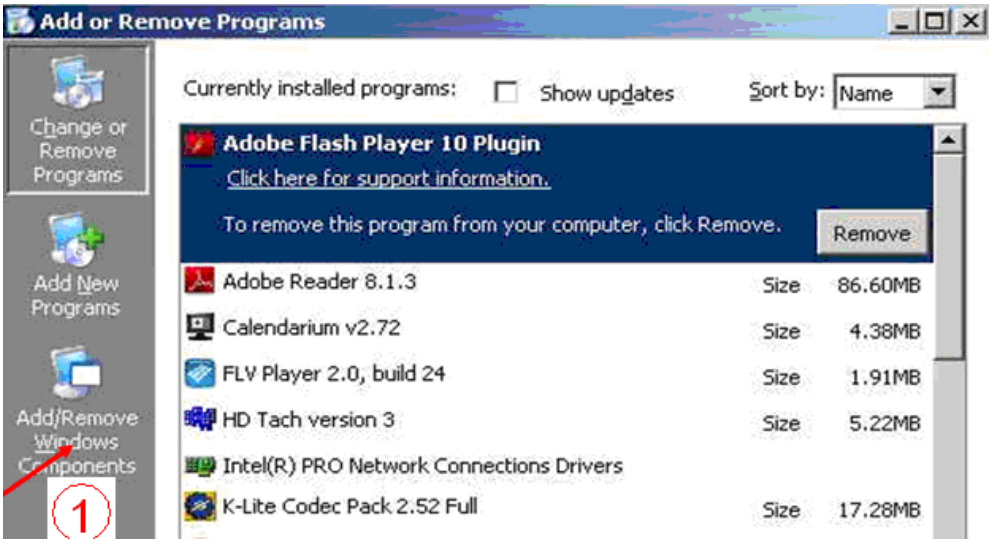
Yêu cầu

– Các interface của server dùng để cấp IP phải cấu hình IP tĩnh.
– User dùng cấu hình phải có quyền Admin.
– Phải có đĩa source Win2K3.

Cài đặt

• Vào <Start> → Chọn menu <Control Panel> → Chạy <Add/Remove Programs> → Nhấn nút <Add/Remove Windows Components>.

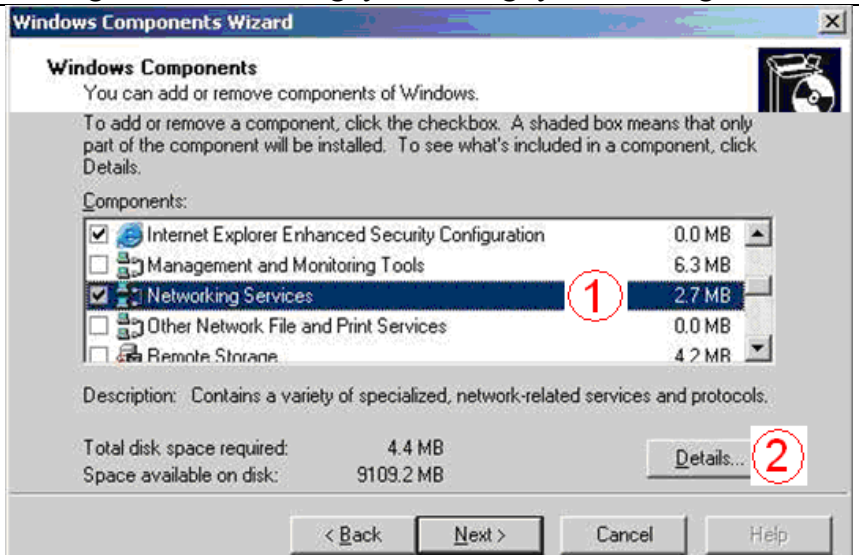
Lưu ý: có thể dùng lệnh ***appwiz.cpl***



Hình 8. 2 - Add/Remove programs

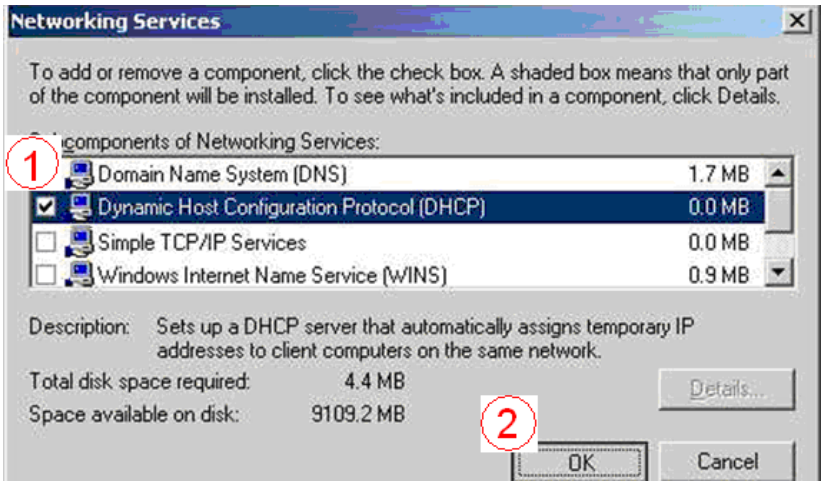
• Trong hộp thoại <Windows Components>, Chọn mục <Networking Services> → Nhấn nút <Details...>.

Lưu ý: không check vào ***<Networking Services>*** lúc đó các dịch vụ bên trong sẽ được cài đặt gây tốn tài nguyên hệ thống.



Hình 8. 3 - Networking services

• Trong hộp thoại <Subcomponents of Networking Services>, check vào <Dynamic Host Configuration Protocol (DHCP)> → Nhấn nút <OK>.



Hình 8. 4 - Cài đặt DHCP

• Trở lại hộp thoại <Windows Components Wizard> → Nhấn nút <Next>.

• Windows sẽ tiến hành cài đặt DHCP, kiểm tra IP tĩnh của Server, đòi hỏi đĩa source Win2K3.

• Cài xong hộp thoại <Completing the Windows Components Wizard> hiện lên → Nhấn nút <Finish>.

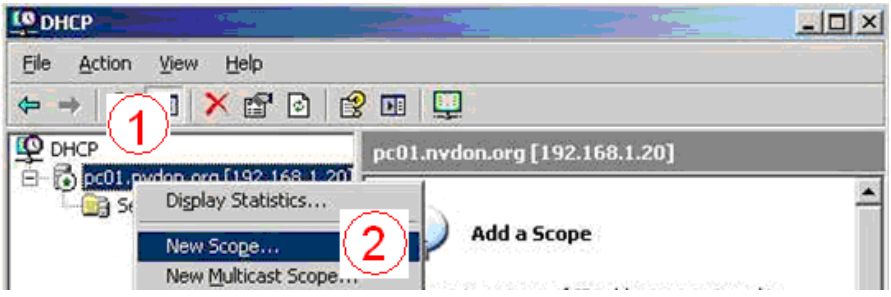
Cấu hình DHCP

Cấu hình DHCP để tạo ra phạm vi cấp IP, các thông số cấp kèm theo IP.

• Chọn <Start> → Chọn <Programs> → Chọn <Administrative Tools> → Chọn <DHCP>.

Lưu ý: có thể dùng lệnh ***dhcpmgmt.msc***.

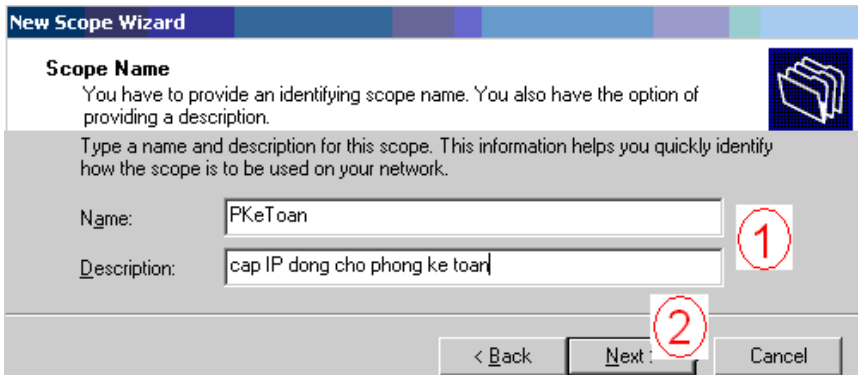
• Trong hộp thoại ***<DHCP>***, phải chuột lên tên server → Chọn menu ***<New Scope...>.***



Hình 8. 5 - Tạo scope

• Hộp thoại ***<Welcome>*** xuất hiện → Nhấn nút ***<Next>.***

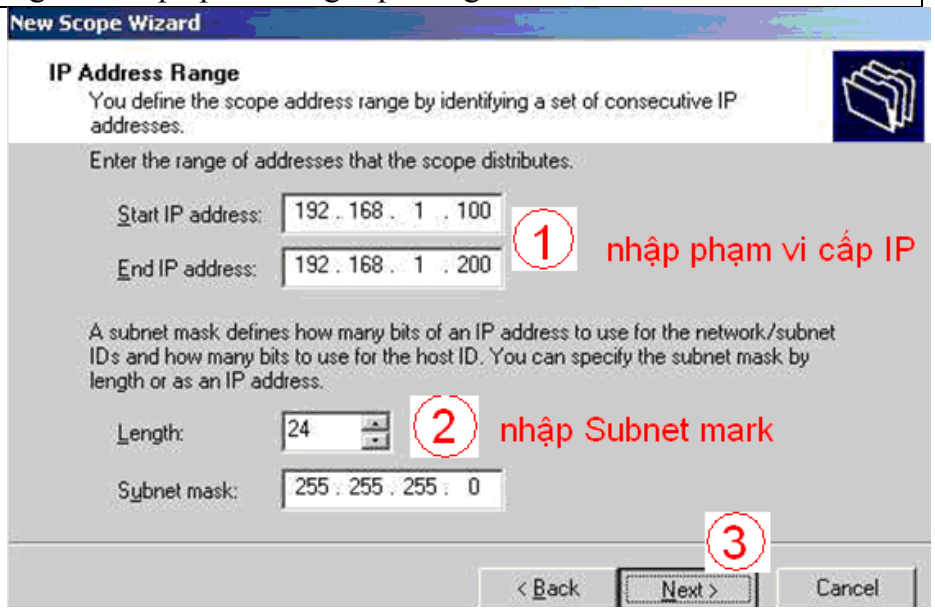
• Trong hộp thoại <***Scope Name***> → Nhập vào tên của scope muốn tạo trong <***Name***>, thường là tên gợi nhớ (vd: PKeToan) → Nhập vào mô tả cho scope trong <***Description***>, mô tả chức năng của scope này (vd: cap IP dong cho phong ke toan).



Hình 8. 6 - Nhập tên và mô tả cho scope

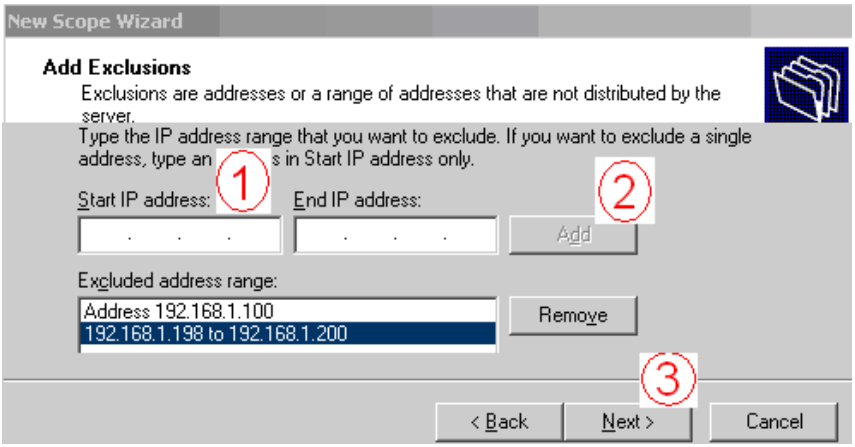
• Hộp thoại <***IP Address Range***> xuất hiện, yêu cầu nhập vào phạm vi cấp IP từ <***Start IP address***> đến <***End IP address***> và Subnet mark trong <***Length***> hay <***Subnet mark***> → Nhấn nút <***Next***>.

Lưu ý: Phạm vi cấp IP phải tránh các server trong mạng, lớp mạng của scope phải trùng lớp mạng của DHCP Server.



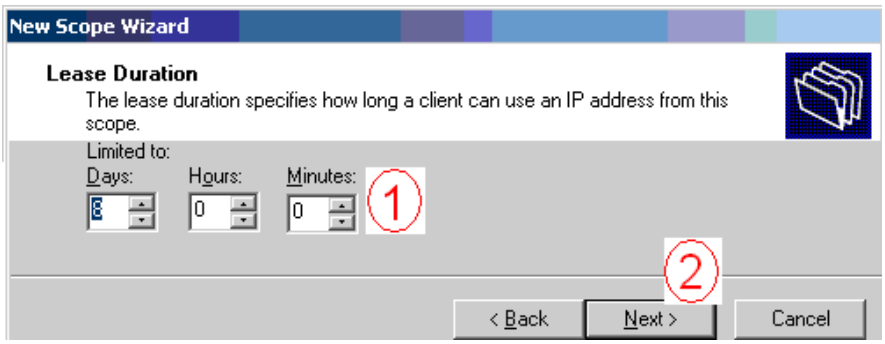
Hình 8. 7 - Phạm vi cấp IP của scope

• Trong hộp thoại <***Add Exclusions***>, thêm vào 1 IP hoặc một dãy IP bị loại ra trong phạm vi trên. Các IP này thường là IP đặc biệt dùng cho các trường hợp đặc biệt (vd: dùng cho các server...) → Nhập IP vào <***Start IP address***> → Nhấn nút <***Add***> để loại trừ một IP (nếu là dãy IP thì ghi thêm phần <***End IP address***>) → Nhấn nút <***Next***>.



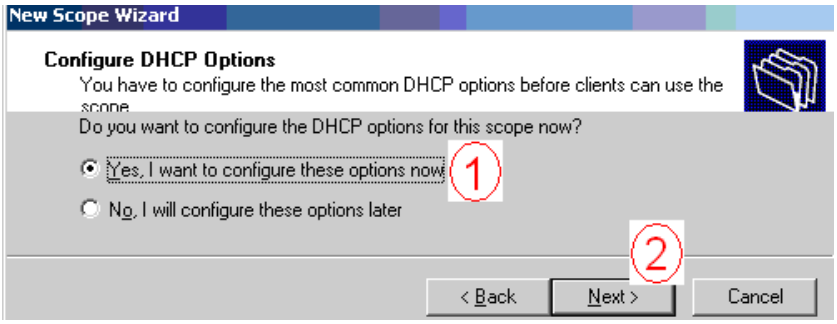
Hình 8. 8 - Loại trừ các IP trong phạm vi cấp

• Trong hộp thoại <***Lease Duration***>, quy định thời hạn cho thuê IP, thường là 8 ngày (sau một tuần làm việc client thuê IP lại). Nếu thời hạn nhỏ, các client sẽ broadcast thuê IP nhiều làm băng thông mạng giảm. Nếu thời hạn lớn, các máy bên ngoài vào chỉ dùng IP một lần làm mất IP. Vậy tùy theo nhu cầu mà xác định thời hạn này → Nhấn nút <***Next***>.



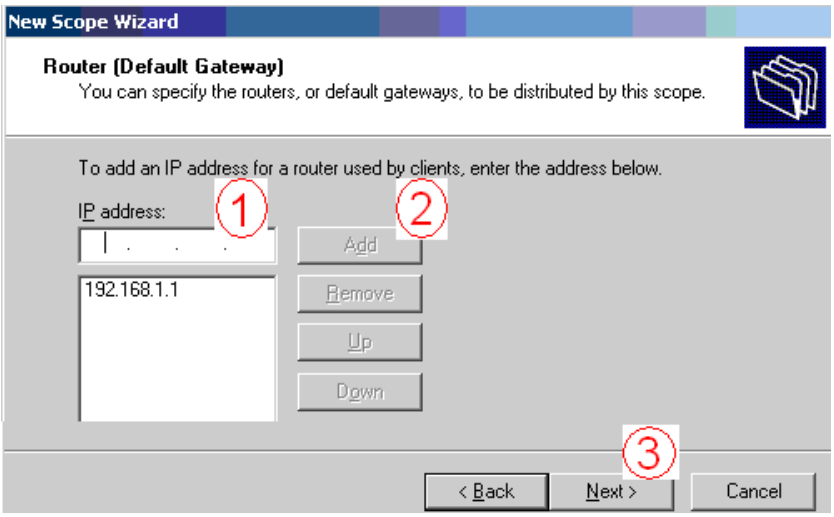
Hình 8. 9 - Thời hạn thuê IP

• Hộp thoại <***Configure DHCP Options***>**,** hỏi có cấu hình cấp các thông số kèm theo không. Cấu hình cấp luôn default gateway và DNS cho client → Chọn option <***Yes, I want to configure these options now***> → Nhấn nút <***Next***>**.**



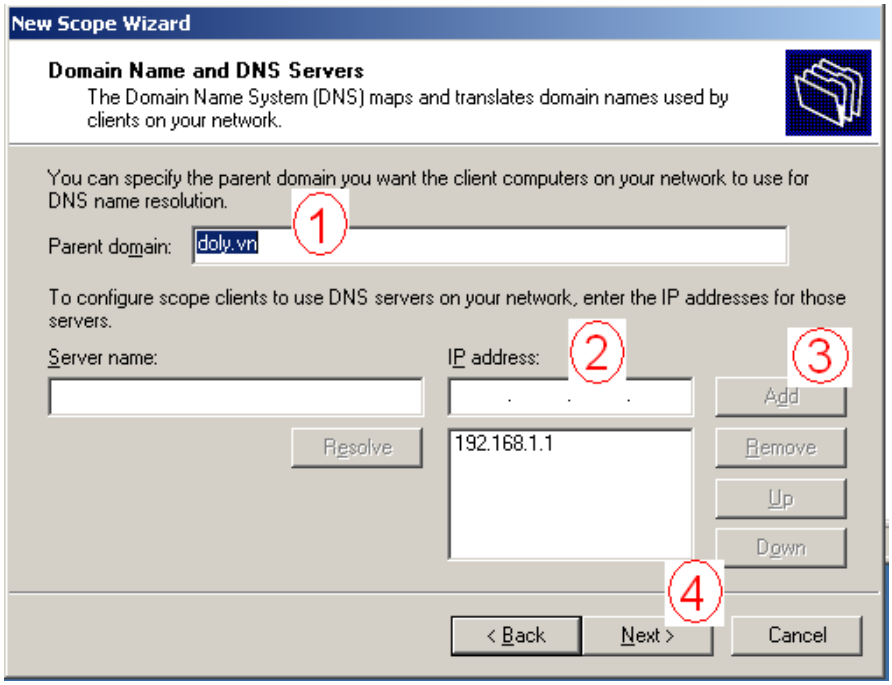
Hình 8. 10 - Cấp các thông số kèm theo

• Trong hộp thoại <***Router (Default Gateway)***> → Nhập IP default gateway vào <***IP address***> → Nhấn nút <***Add***> → Nhấn nút <***Next***>**.**



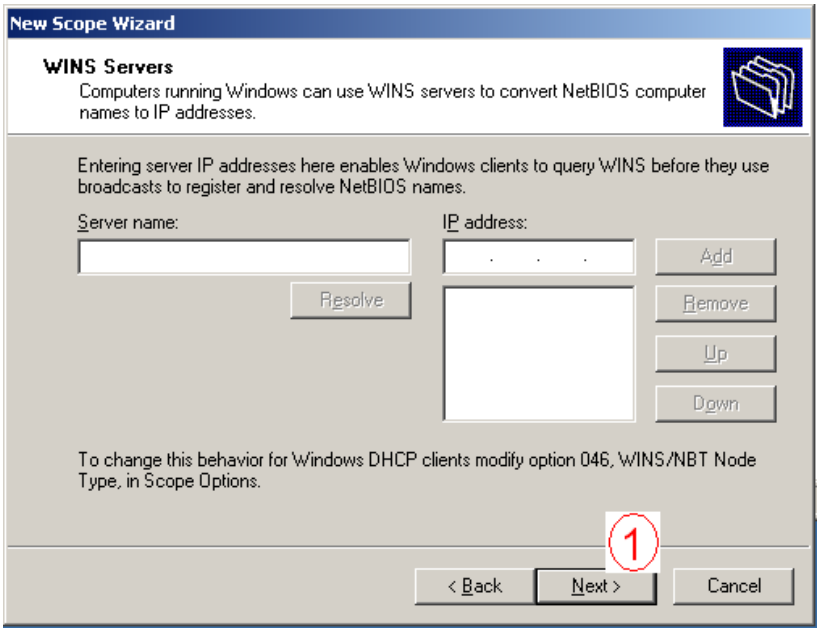
Hình 8. 11 - Cấp default gateway

• Trong hộp thoại <***Domain Name and DNS Servers***> → Nhập tên miền vào <***Parent domain***>. Khi client nhận được IP, tên máy của client sẽ biến thành dạng đầy đủ là ***tên máy.tên miền*** (vd: may01.doly.vn). Tên đầy đủ này sẽ được đăng ký vào DNS server một record có IP là IP của client. Mục <Server name> không cần khai báo, dùng trong trường hợp quên IP của DNS server → Nhập IP của DNS server vào <***IP address***> → Nhấn nút <***Add***> → Nhấn nút <***Next***>**.**



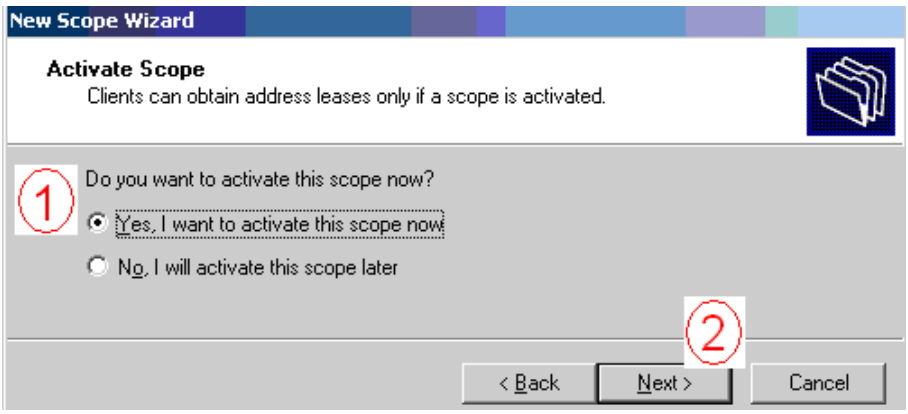
Hình 8. 12 - Cấp DNS server

• Trong hộp thoại <***WINS Servers***>, điền vào IP của WINS server. Dịch vụ WINS chạy trên các hệ thống Win2K trở về trước, các version sau này không cần cài WINS nên bỏ qua bước này → Nhấn nút <***Next***>.



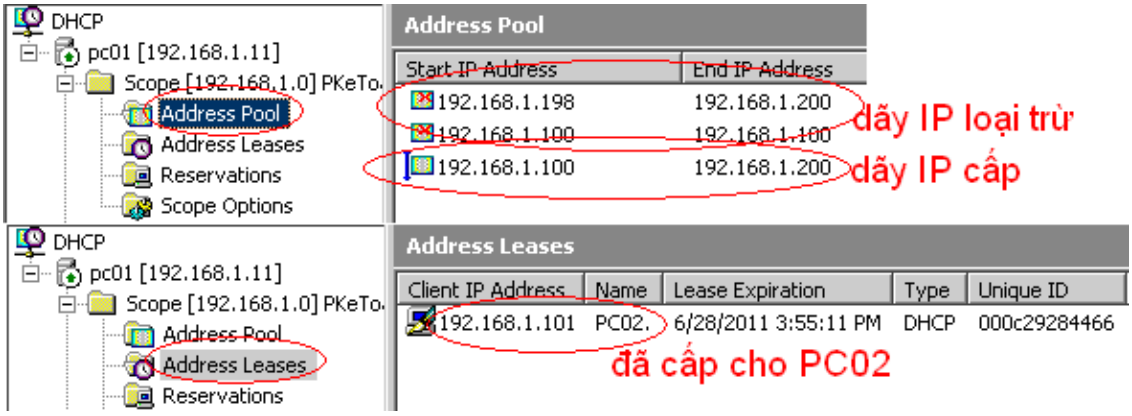
Hình 8. 13 - Cấp WINS

• Trong hộp thoại <***Activate Scope***> → Nếu muốn scope vừa tạo hoạt động cấp IP thì chọn option <***Yes, I want to activate scope now***> → Nhấn nút <***Next***>.



Hình 8. 14 - Kích hoạt scope

• Trong hộp thoại <***Completing the New Scope Wizard***> → Nhấn nút <***Finish***> để hoàn thành việc tạo một scope.



Hình 8. 15 - Thông tin về scope

∗ **Các thông tin trong scope:**

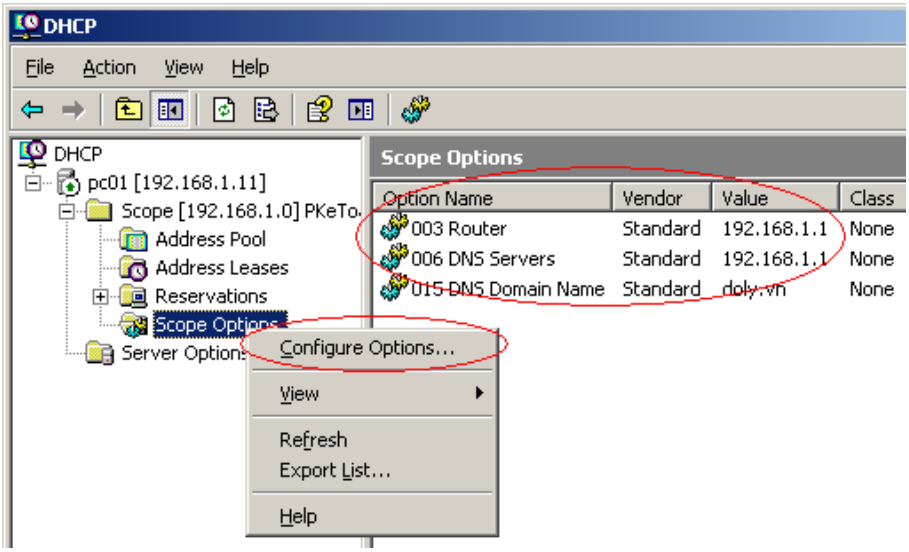
– Address Pool: các phạm vi cấp IP và loại trừ IP.
– Address Leases: danh sách các IP đã cho thuê.
– Reservations: danh sách các IP cấp riêng.
– Scope Options: các thông số cấp kèm theo IP.

Các thông số trong dịch vụ DHCP

∗ **Scope Options: các thông số cấp kèm theo IP, các thông số này chỉ có tác dụng trong scope này. Scope Options sẽ ghi đè lên Server Options.**

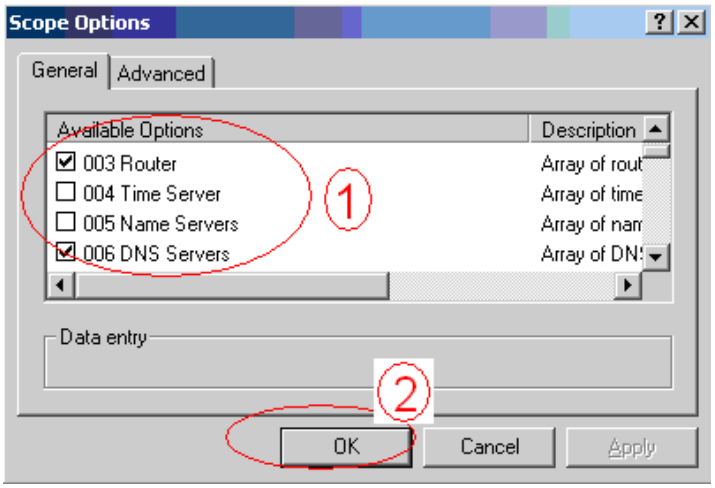
∗ **Server Options: tương tự Scope Options nhưng các thông số này sẽ được cấp trong các scope không cấu hình Scope Options.**

- Trong hộp thoại <DHCP>, phải chuột lên <Scope Options> → Chọn menu <Configure Options...>.



Hình 8. 16 - Cấu hình các thông số cho scope

• Trong hộp thoại <***Scope Options***>, có thể check để chọn các thông số cho scope → Nhấn nút <***OK***> để xác nhận.



Hình 8. 17 - Cấp default gateway và DNS server

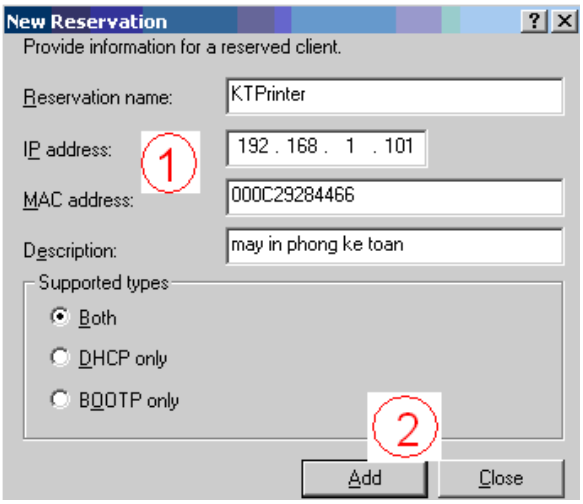
Cấu hình IP dành riêng

Một số client sử dụng IP trong một thời gian dài và cố định cần cấp IP dành riêng theo địa chỉ MAC.

• Trong hộp thoại <***DHCP***>, phải chuột lên <***Reservations***> → Chọn menu <***New Reservation...***>.

Hình 8. 18 - Cấu hình IP dành riêng

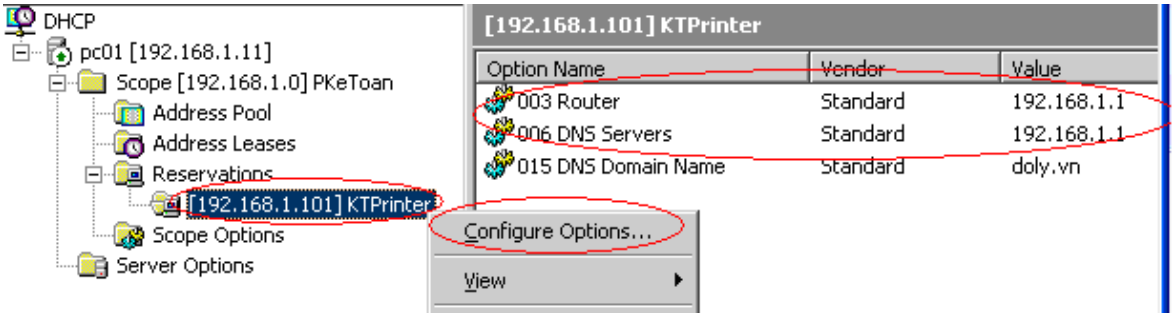
• Trong hộp thoại <***New Reservations***>, nhập tên của Reservations vào mục <***Reservations name***> → Nhập IP của máy client cần cấp IP riêng vào mục <***IP address***> → Nhập địa chỉ MAC của máy client cần cấp IP riêng vào mục <***MAC address***> → Nhập mô tả chức năng của IP riêng này vào mục <***Description***> → Chọn option <***Both***> trong <***Supported types***> để áp dụng cho cả hai giao thức DHCP và BOOTP → Nhấn nút <***Add***> → Nhấn nút <***Close***> để đóng hộp thoại lại.



Hình 8. 19 - IP cấp riêng cho một địa chỉ MAC

KTPrinter có các option kế thừa của scope, nếu muốn cấp các option khác.

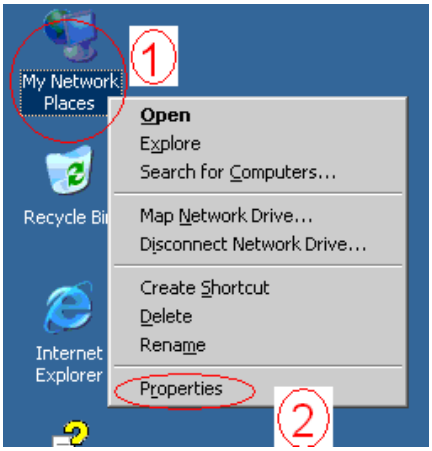
- Phải chuột lên <***KTPrinter***> → Chọn menu <***Configure Options..***> để cấu hình các thông số cho KTPrinter.



Hình 8. 20 - Các thông số cấp kèm theo IP

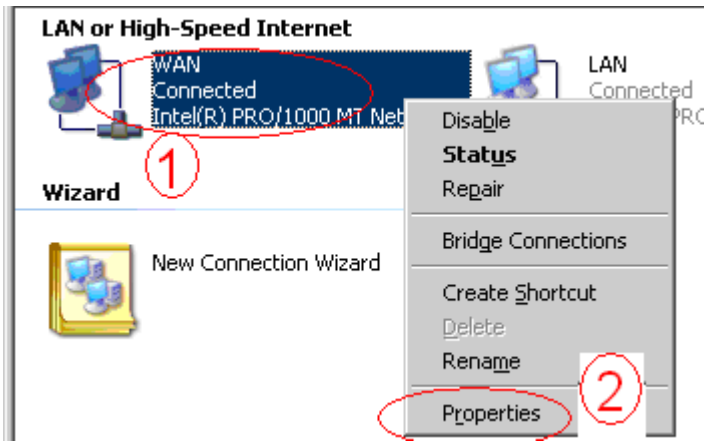
Cấu hình Client thuê IP từ Server

- Trên màn hình <***Desktop***>, phải chuột lên <***My Network Places***> → Chọn menu <***Properties***>.



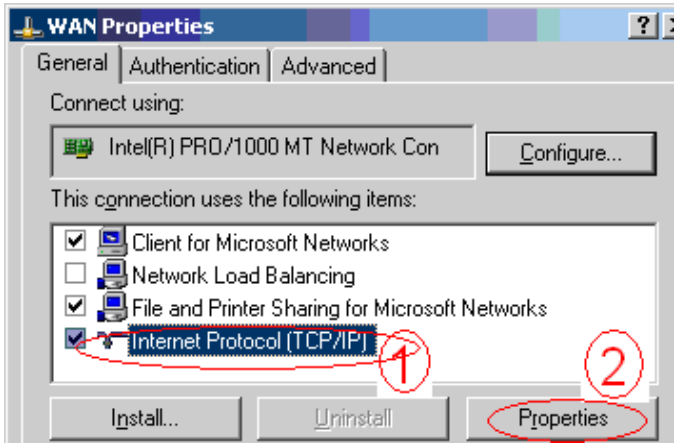
Hình 8. 21 - Mở Network Connections

• Trong hộp thoại <***Network Connections***>, phải chuột lên interface cần thuê IP <***WAN***> → Chọn menu <***Properties***>.



Hình 8. 22 - Cấu hình cho card mạng WAN

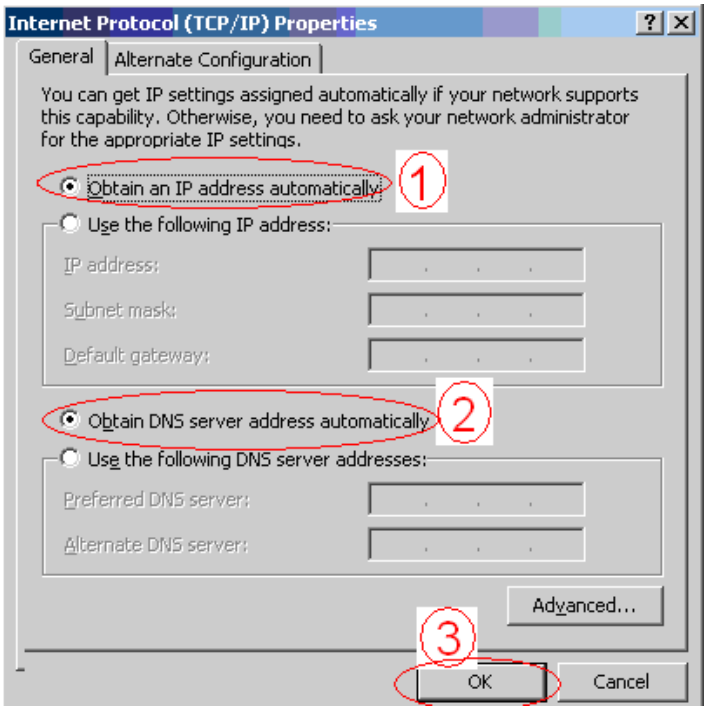
• Trong hộp thoại <WAN Properties>, chọn mục <Internet Protocol (TCP/IP)> → Nhấn nút <Properties>.



Hình 8. 23 - Cấu hình địa chỉ IP

• Trong hộp thoại <***Internet Protocol (TCP/IP) Properties***>, chọn option <***Obtain an IP address automatically***> để nhận IP động → Chọn option <***Obtain DNS server address automatically***> nếu muốn nhận DNS động → Nhấn nút <***OK***>. Lúc này quá trình thuê IP của client được thực hiện.

Lưu ý: có thể dùng các lệnh sau ***ipconfig /release*** xóa IP của client. ***ipconfig/renew*** thuê lại IP.



Hình 8. 24 - Cấu hình thuê IP động

- Dùng lệnh ***ipconfig /all*** để xem IP và các thông số được cấp phát

```
Ethernet adapter WAN:

   Connection-specific DNS Suffix  . : doly.vn
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-28-44-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.11
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   Lease Obtained. . . . . . . . . . : Monday, June 20, 2011 3:55:08 PM
   Lease Expires . . . . . . . . . . : Tuesday, June 28, 2011 3:55:08 PM
```

Hình 8. 25 - Xem IP được cấp

DHCP tích hợp trong hệ điều hành và thiết bị

Tất cả các hệ điều hành mạng Windows, Linux, Unix... đều tích hợp dịch vụ DHCP để cung cấp cho client. Ở phần trên đã trình bày dịch vụ DHCP của Win2K3. Trong Linux dịch vụ này có tên là dhcpd, là một dịch vụ chạy nền có sẵn trong đĩa cài đặt Linux.

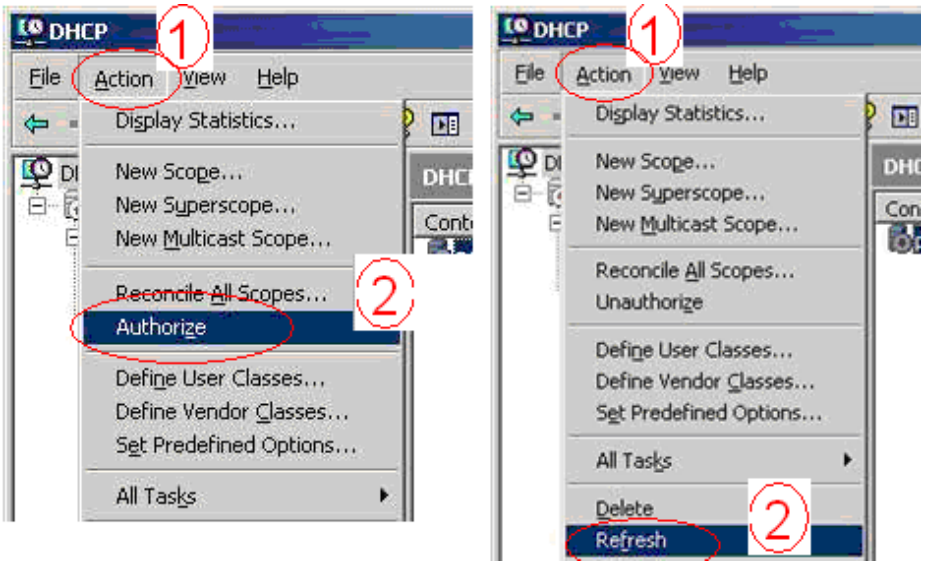
Tất cả các hệ điều hành client đều có chức năng thuê IP động.

∗ Chứng thực dịch vụ DHCP trong AD của Win2k3

Đối với Win2K3, trong môi trường domain để đảm bảo các server được chứng thực mới được cấp IP, dịch vụ DHCP phải được chứng thực. Việc này tránh tình trạng các DHCP server khác cấp IP không chính xác làm ảnh hưởng đến hoạt động của mạng.

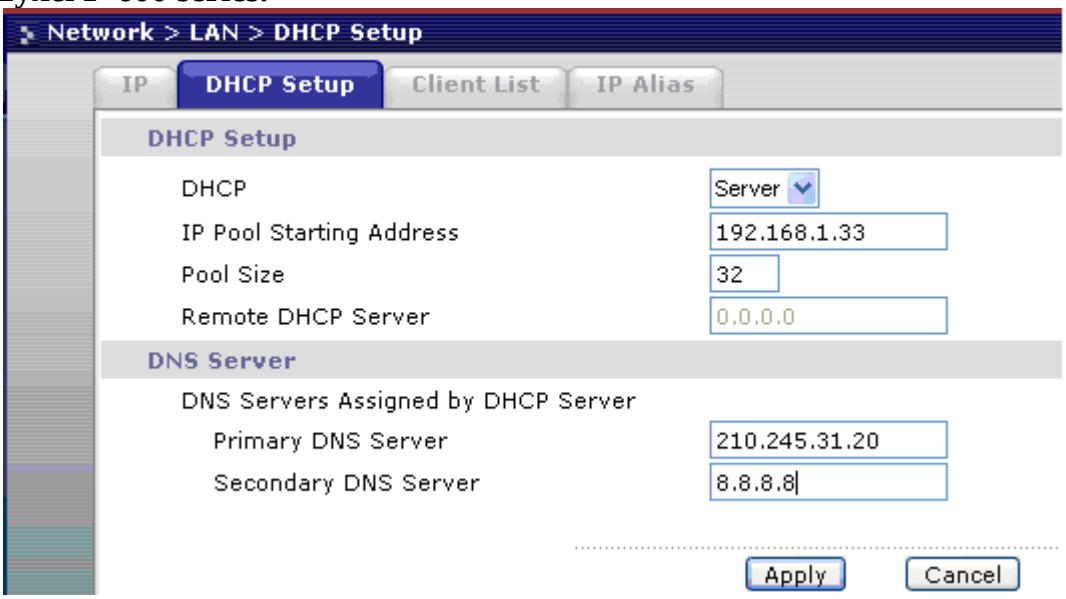
Đối với các hệ điều hành khác Windows NT, Unix... không cần chứng thực.

• Trong hộp thoại <***DHCP***>, chọn <***DHCP server***> cần chứng thực → Chọn menu <***Action***> → Chọn menu <***Authorize***> → Chọn lại menu <***Action***> → Chọn menu <***Refresh***> để áp dụng tác vụ chứng thực.



Hình 8. 26 - Chứng thực DHCP server trong AD

∗ DHCP cũng được tích hợp trong các router, sau đây là dịch vụ DHCP của router ADSL Zyxel P-600 series.



Hình 8. 27 - Cấu hình IP cho router ADSL Zyxel P-600 series

– DHCP: có giá trị <***Server***>, nghĩa là router đóng vai trò là DHCP server để cấp phát IP.
– IP Pool Starting Address: có giá trị bắt đầu phạm vi cấp <***192.168.1.33***>
– Pool Size: cấp cho <***32***> host từ 192.168.1.33 đến 192.168.1.65

– Primary DNS Server: option cấp kèm theo Perferred DNS là <***210.245.31.20***>, đây là DNS server của nhà cung cấp dịch vụ mạng FPT.

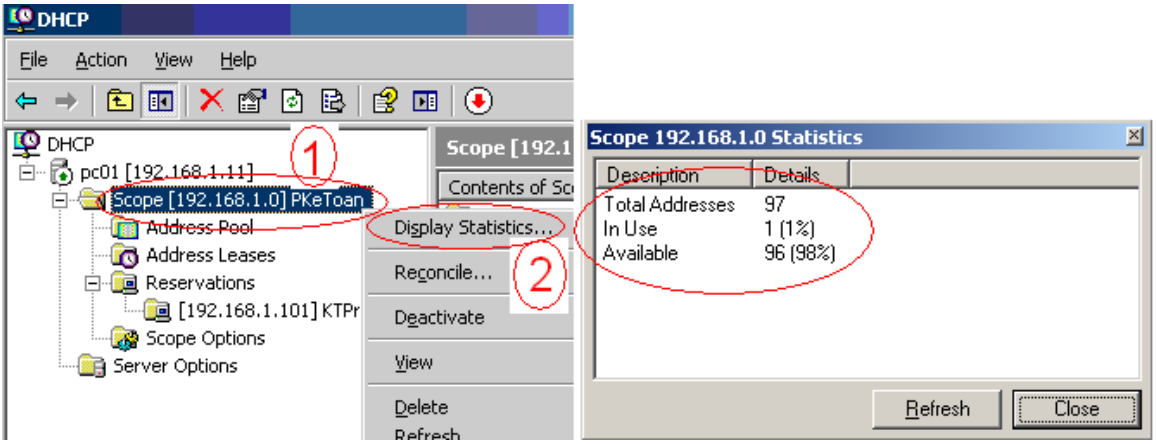
– Secondary DNS Server: Alternate DNS là <***8.8.8.8***>, đây là DNS server mở của Google.

Các gateway, router và access point đều cấu hình DHCP tương tự nhau. Ở đây không thấy cấp default gateway, vì tất nhiên default gateway trỏ về thiết bị này.

Một số sự cố và cách khắc phục

Sự cố hay gặp phải nhất là thuê IP không được, do DHCP server đã cấp hết IP. Lỗi này xảy ra có thể do phạm vi cấp IP quá nhỏ, thời gian thuê IP quá dài. Để khắc phục vào DHCP server mở rộng phạm vi, giảm thời gian cho thuê.

- Để xem thông tin sử dụng IP bằng cách, trong hộp thoại <***DHCP***> phải chuột lên <***Scope***> → Chọn menu <***Display Statistics...***>.

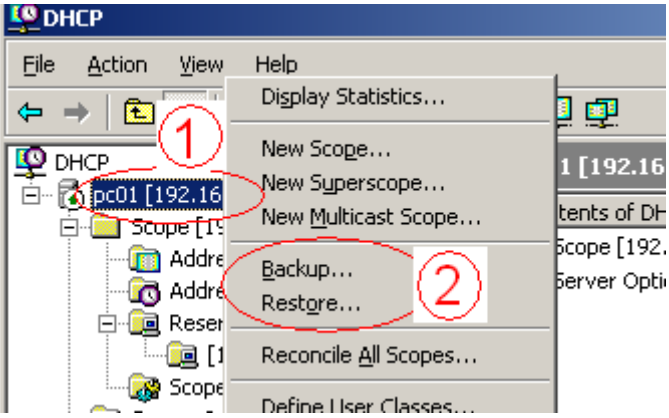


Hình 8. 28 - Thông tin cấp phát IP

Sự cố cũng thường gặp là trong một mạng có quá nhiều DHCP server, cấp IP nhiều mạng khác nhau với các thông số khác nhau. Khi Client thuê IP thì không vào được mạng mình cần vào. Cách khắc phục là phải quản lý các DHCP này và cấu hình đúng. Nếu trong môi trường domain thì kiểm tra lại các DHCP server được chứng thực.

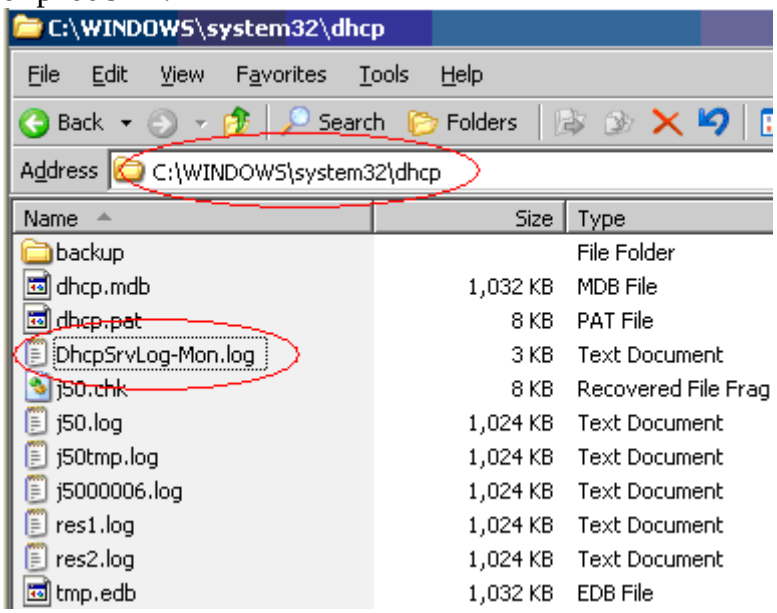
DHCP cung cấp 2 chức năng backup và restore, để sao lưu dự phòng và phục hồi khi cần thiết.

- Phải chuột lên <DHCP server> → Chọn menu <Backup...> hoặc <Restore...>.



Hình 8. 29 - Sao lưu dự phòng DHCP

DHCP lưu lại file log ***DhcpSrvLog-Mon*** trong ***C:\WINDOWS\system32\dhcp*** mỗi ngày phát sinh ra một file, qua tuần sau ghi lại file của tuần trước. Nên theo dõi log file để khắc phục các lỗi phát sinh.



Hình 8. 30 – Tên và vị trí lưu log file

> Lưu ý: thứ tự ưu tiên IP trong client: IP tĩnh, IP động (DHCP), Apipa (IP tự cấp phát), User configure.

Câu hỏi và bài tập

1. Trình bày quá trình hoạt động của DHCP?
2. Nêu các điều kiện để cài đặt DHCP?
3. Trình bày một số thông số cấp kèm IP mà bạn biết?
4. Trình bày khái niệm IP reservation?
5. Nêu các sự cố hay gặp và cách khắc phục sự cố đó?
6. Trong môi trường domain (Win2K3) muốn DHCP hoạt động phải làm gì, vì sao?
7. Trình bày và giải thích độ ưu tiên cấp IP trong hệ thống mạng?
8. Trình bày ý nghĩa của: Address Pool, Address Leases, Reservations, Scope Options.

TÀI LIỆU THAM KHẢO

[1] Dương Bảo Ninh. *Mạng máy tính.* Trường Đại Học Đà Lạt, 2009.

[2] Trần Văn Thành, Mang Thành Trung. *Mạng máy tính*. TTTH Trường Đại Học KHTN TP.HCM. 2004.

[3] Trung tâm khoa học tự nhiên và công nghệ quốc gia. *Thiết kế và xây dựng mạng LAN và WAN*, Viện công nghệ thông tin. 2004.

[4] Cisco. *CCNA Exploration 4.0.*

[5] Microsoft. *Advanced MCSA Full Labs.*

[6] Microsoft. *TechNet.*