TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THỦ ĐỨC
Khoa Công Nghệ Thông Tin

TÀI LIỆU GIẢNG DẠY | BẬC CAO ĐẲNG

MẠNG MÁY TÍNH

| *2019– Lưu hành nội bộ* |

LỜI TÁC GIẢ

Quyển giáo trình này được biên soạn dựa theo đề cương môn học "Mạng máy tính" của Khoa Công nghệ thông tin Trường Cao đẳng Công nghệ Thủ Đức.

Do giáo trình phát hành lần đầu nên sẽ không tránh khỏi những sai sót về nội dung lẫn hình thức, nhóm biên soạn rất mong nhận được sự góp ý chân thành từ quý thầy cô và các em sinh viên để giáo trình hoàn thiện hơn.

GIỚI THIỆU

Mạng máy tính là học phần cơ sở chuyên ngành giúp sinh viên ngành Công nghệ thông tin, ngành Truyền thông và mạng máy tính có nền tảng ban đầu về mạng máy tính: hiểu rõ khái niệm về mạng máy tính, nguyên lý hoạt động cũng như các yêu cầu về phần cứng và phần mềm cần thiết để kết nối mạng; sinh viên còn có thể phân biệt rõ các loại mạng khác nhau trong thực tế, hiểu rõ nguyên lý kết nối các mạng cục bộ với nhau tạo thành mạng diện rộng và mạng toàn cầu Internet; Sinh viên được cài đặt, cấu hình và quản trị một hệ thống mạng cụ thể. Thông qua các hoạt động học tập, sinh viên cũng hoàn thiện dần khả năng tư duy hệ thống, kỹ năng làm việc nhóm của mình.

Nhóm tác giả

MỤC LỤC

1. 1

GIỚI THIỆU CHUNG 1

1.1 | CÁC KHÁI NIỆM VỀ MẠNG MÁY TÍNH 2

1.2 | LỢI ÍCH KHI SỬ DỤNG MẠNG 3

1.3 | PHÂN LOẠI MẠNG MÁY TÍNH 3

1.3.1 | THEO KHOẢNG CÁCH ĐỊA LÝ 3

1.3.2 | THEO KỸ THUẬT CHUYỂN MẠCH 3

1.3.3 | THEO KIẾN TRÚC MẠNG 4

1.4 | INTERNET LÀ GÌ 6

1.5 | KIẾN TRÚC MẠNG INTERNET 6

1.6 | CÁC XU HƯỚNG CỦA MẠNG 10

1.6.1 | BYOD (BRING YOUR OWN DEVICE) 10

1.6.2 | CỘNG TÁC TRỰC TUYẾN (ONLINE COLLABORATION) 10

1.6.3 | HỘI NGHỊ TRUYỀN HÌNH (VIDEO CONFERENCING) 11

1.6.4 | ĐIỆN TOÁN ĐÁM MÂY 12

1.7 | BÀI TẬP CHƯƠNG I 13

2. 15

CÁC THÀNH PHẦN MẠNG 15

2.1 | CÁC THIẾT BỊ MẠNG 16

2.1.1 | ĐƯỜNG TRUYỀN 16

2.1.2 | CARD GIAO TIẾP MẠNG (NETWORK ADAPTER) 22

2.1.3 | REPEATER 23

2.1.4 | HUB 24

2.1.5 | BRIDGE 24

2.1.6 | SWITCH 25

2.1.7 | ROUTER 26

2.1.8 | GATEWAY 26

2.1.9 | WIRELESS ACCESS POINT 27

2.2 | CÁC HỆ ĐIỀU HÀNH MẠNG 27

2.2.1 | KHÁI NIỆM 27

2.2.2 | SỰ KHÁC NHAU GIỮA CLIENT SOFTWARE VÀ SERVER SOFTWARE 28

2.2.3 | HỆ ĐIỀU HÀNH MẠNG 29

2.3 | BÀI TẬP CHƯƠNG 2 37

2.3.1 | BÀI TẬP 1 – BÀI TẬP NHÓM 37

2.3.2 | BÀI TẬP 2 37

3. 39

MÔ HÌNH THAM CHIẾU OSI VÀ MÔ HÌNH TCP/IP 39

3.1 | KHÁI NIỆM GIAO THỨC 40

3.2 | GIỚI THIỆU GIAO THỨC TCP/IP 41

3.3 | CÁC TỔ CHỨC QUY ĐỊNH CHUẨN MẠNG 42

3.4 | MÔ HÌNH OSI 44

3.4.1 | GIỚI THIỆU MÔ HÌNH OSI 44

3.4.2 | TÍNH NĂNG CỦA MỖI LỚP TRONG MÔ HÌNH OSI 46

3.5 | MÔ HÌNH TCP/IP 63

3.5.1 | GIỚI THIỆU MÔ HÌNH TCP/IP 63

3.5.2 | TÍNH NĂNG CỦA CÁC LỚP TRONG MÔ HÌNH TCP/IP 65

3.5.3 | QUÁ TRÌNH TRUYỀN THÔNG 66

3.5.4 | CÁCH ĐÓNG GÓI DỮ LIỆU VÀ PDU 67
3.5.5 | QUÁ TRÌNH GỬI DỮ LIỆU 68
3.6 | SO SÁNH MÔ HÌNH OSI VÀ MÔ HÌNH TCP/IP 70
3.7 | BÀI TẬP CHƯƠNG 3 71

4. 72

ĐỊA CHỈ IP 72
4.1 | CHUYỂN ĐỔI GIỮA SỐ NHỊ PHÂN VÀ SỐ THẬP PHÂN 73
4.1.1 | CHUYỂN ĐỔI SỐ NHỊ PHÂN THÀNH SỐ THẬP PHÂN 73
4.1.2 | CHUYỂN ĐỔI SỐ THẬP PHÂN THÀNH SỐ NHỊ PHÂN 74
4.2 | ĐỊA CHỈ IPV4 75
4.2.1 | CẤU TRÚC ĐỊA CHỈ IPV4 76
4.2.2 | CÁC LỚP ĐỊA CHỈ IPV4 77
4.2.3 | NHỮNG LOẠI ĐỊA CHỈ TRONG MẠNG IPV4 81
4.2.4 | ĐỊA CHỈ PRIVATE VÀ ĐỊA CHỈ PUBLIC 82
4.2.5 | NHỮNG ĐỊA CHỈ IPV4 ĐẶC BIỆT 83
4.2.6 | CÁC LOẠI GIAO TIẾP 84
4.3 | SUBNET 87
4.3.1 | KHÁI NIỆM SUBNET 87
4.3.2 | CHIA SUBNET CƠ BẢN 89
4.3.3 | CHIA SUBNET THEO VARIABLE LENGTH SUBNET MASK (VLSM) 93
4.4 | ĐỊA CHỈ IPV6 102
4.4.1 | GIỚI THIỆU ĐỊA CHỈ IPV6 102
4.4.2 | CẤU TRÚC ĐỊA CHỈ IPV6 103
4.4.3 | CÁC LOẠI ĐỊA CHỈ IPV6 105
4.5 | BÀI TẬP CHƯƠNG 4 108

5. 112

THỰC HÀNH THIẾT LẬP MẠNG LAN 112
5.1 | CÀI ĐẶT THÔNG TIN CARD MẠNG 113
5.2 | CÁC LỆNH KIỂM TRA HỆ THỐNG MẠNG 116
5.3 | LOCAL USER ACCOUNT & GROUP ACCOUNT 119
5.4 | SHARE PERMISSION 122
5.5 | SECURITY PERMISSION (NTFS FILE PERMISSION) 129
5.6 | KHÁC NHAU GIỮA QUYỀN SHARE VÀ SECURITY 133
5.7 | XÂY DỰNG MÔ HÌNH MẠNG GIA ĐÌNH 133
5.8 | BÀI TẬP CHƯƠNG 5 137
5.8.1 | BÀI TẬP 1 137
5.8.2 | BÀI TẬP 2 138

1. GIỚI THIỆU CHUNG

Sau khi học xong chương này, sinh viên có thể:

- Trình bày các khái niệm cơ bản về mạng máy tính.
- Phân biệt các loại mạng máy tính.

1.1 | CÁC KHÁI NIỆM VỀ MẠNG MÁY TÍNH

Mạng máy tính là tập hợp các máy tính đơn lẻ được kết nối với nhau bằng các phương tiện truyền vật lý theo một kiến trúc mạng xác định để cùng nhau chia sẻ và khai thác các tài nguyên trên hệ thống.

Khi nói đến mạng máy tính, chúng ta muốn nói tới các khía cạnh sau:

Các thiết bị đầu -cuối (end system): các thiết bị tham gia vào mạng để khai thác các tài nguyên chung như máy tính, điện thoại di động, các thiết bị cầm tay như PDA... Người ta cũng dùng một thuật ngữ khác để gọi thiết bị đầu-cuối trong mạng: host - một máy tính chạy phần mềm của người sử dụng, đặt trong mạng để chia sẻ tài nguyên trên mạng. Mỗi host hình thành một nút của mạng.

Đường truyền: môi trường truyền dẫn dữ liệu, thông qua đó các thiết bị đầu cuối khai thác tài nguyên chung của mạng. Đường truyền có thể là hữu tuyến như dây cáp đồng trục, cáp xoắn, cáp quang; có thể là vô tuyến như sóng radio, hồng ngoại, vệ tinh, ...

Băng thông của đường truyền (Band-width): tốc độ tối đa mà dữ liệu được gửi hoặc nhận giữa hai máy tính qua mạng trong một khoảng thời gian xác định.

Đơn vị bandwidth:

Tên đơn vị	Kí hiệu	Giá trị quy đổi
bits per second	bps	1 bps là giá trị căn bản nhỏ nhất
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps

Sơ đồ đấu nối (topology): cách đấu nối các thiết bị đầu-cuối về phương diện hình học.

Giao thức của mạng (protocol): các quy ước truyền thông để các máy tính trong mạng có thể liên lạc, trao đổi thông tin với nhau.

1.2 | LỢI ÍCH KHI SỬ DỤNG MẠNG

- Cùng chia sẻ các tài nguyên chung như dữ liệu, phần mềm, thiết bị, ... , làm giảm bớt các chi phí về đầu tư trang thiết bị.
- Tạo môi trường giao tiếp giữa người với người, chinh phục được khoảng cách, con người có thể trao đổi, thảo luận trực tiếp với nhau dù cách xa nhau hàng nghìn km, có khả năng tổ chức và triển khai các đề án lớn thuận lợi và dễ dàng.
- Làm tăng độ tin cậy của hệ thống (dễ bảo trì máy móc và lưu trữ, khôi phục, dữ liệu chung), giúp công việc đạt hiệu suất cao.
- Xử lý thông tin chính xác, cập nhật đồng bộ dữ liệu một cách nhanh chóng.
- Cung cấp các nhiều dịch vụ tiện ích công cộng (website, file sharing, chatting, game…).

1.3 | PHÂN LOẠI MẠNG MÁY TÍNH

1.3.1 | THEO KHOẢNG CÁCH ĐỊA LÝ

Mạng cục bộ (Local Area Networks - LAN): cài đặt trong phạm vi tương đối hẹp, khoảng cách giữa các máy tính nối mạng là vài km.

Mạng đô thị (Metropolitan Area Networks - MAN): cài đặt trong phạm vi một đô thị, một trung tâm kinh tế xã hội.

Mạng diện rộng (Wide Area Networks - WAN): phạm vi của mạng có thể vượt qua biên giới quốc gia và thậm chí cả lục địa.

1.3.2 | THEO KỸ THUẬT CHUYỂN MẠCH

Mạch chuyển mạch kênh (circuit switched network): hai thực thể thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc.

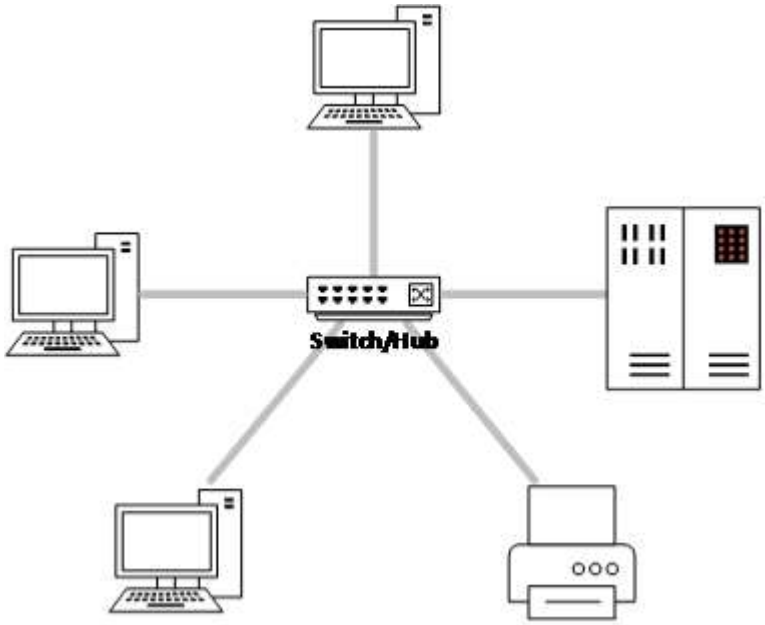
Mạng chuyển mạch thông báo (message switched network): Thông báo là một đơn vị dữ liệu qui ước được gửi qua mạng đến điểm đích mà không thiết lập kênh truyền cố định. Căn cứ vào thông tin tiêu đề mà các nút mạng có thể xử lý được việc gửi thông báo đến đích

Mạng chuyển mạch gói (packet switched network): mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

1.3.3 | THEO KIẾN TRÚC MẠNG

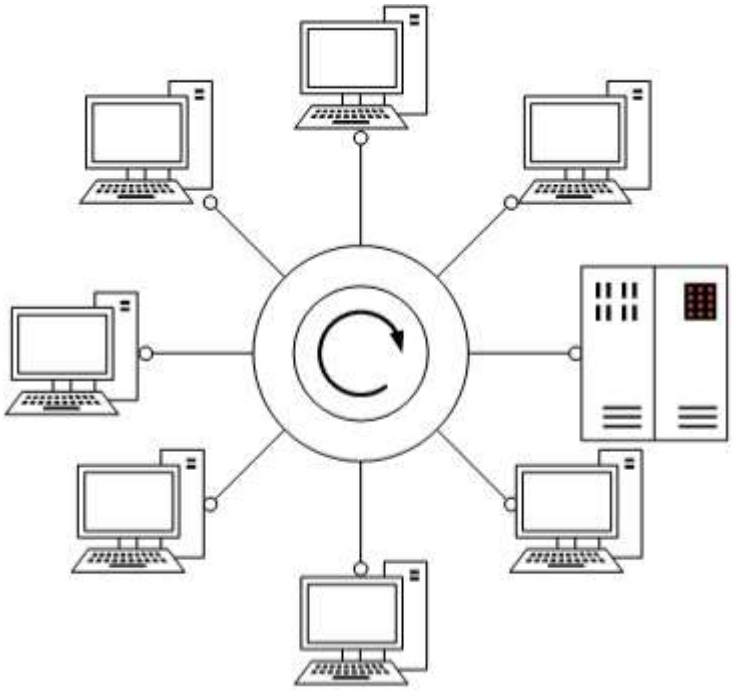
Kiến trúc của mạng bao gồm: Sơ đồ đấu nối mạng (Network topology) và giao thức mạng (Network protocol)

- **Phân loại theo topo mạng**
  - Sao:



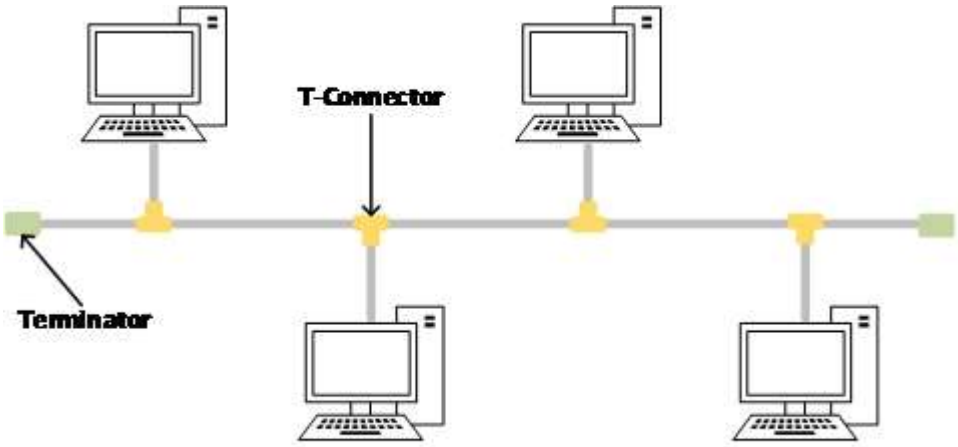
Hình 1.1: Mô hình SAO

  - Vòng:



Hình 1.2: Mô hình VÒNG

- Bus:



Hình 1.3: Mô hình BUS

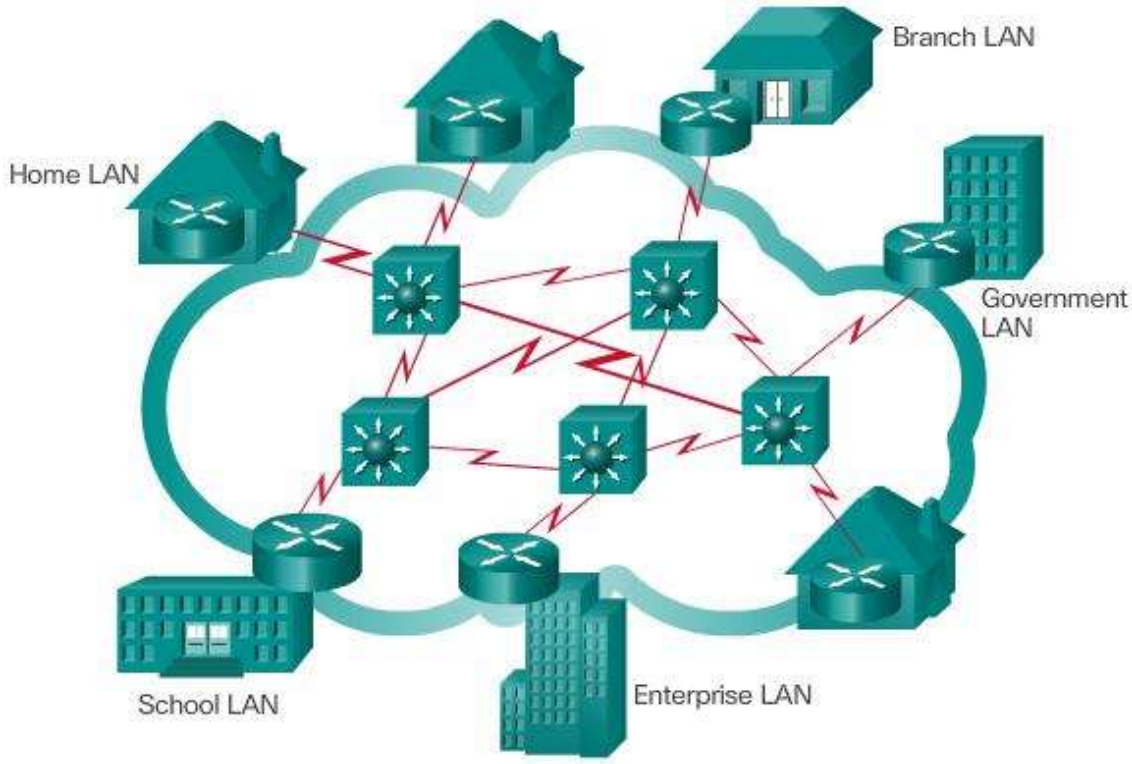
- **Phân loại theo giao thức mạng:**

  - TCP/IP (Transfer Control Protocol/Internet Protocol): gồm tập hợp một bộ nghi thức được xây dựng và công nhận bởi các tổ chức quốc tế. Đây là họ các giao thức được sử dụng phổ biến trên mạng Internet, mang tính mở nhất, phổ dụng nhất và được hỗ trợ của nhiều hãng kinh doanh.

- IPX (Internetworking Packet eXchange): là nghi thức mạng của Netware
- NetBios: là nghi thức mạng của của IBM, phục vụ cho mạng nhỏ.

1.4 | INTERNET LÀ GÌ

Internet là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu nối chuyển gói dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP). Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu và các trường đại học, của người dùng cá nhân và các chính phủ trên toàn cầu.



Hình 1.4: Các kết nối LAN và WAN

1.5 | KIẾN TRÚC MẠNG INTERNET

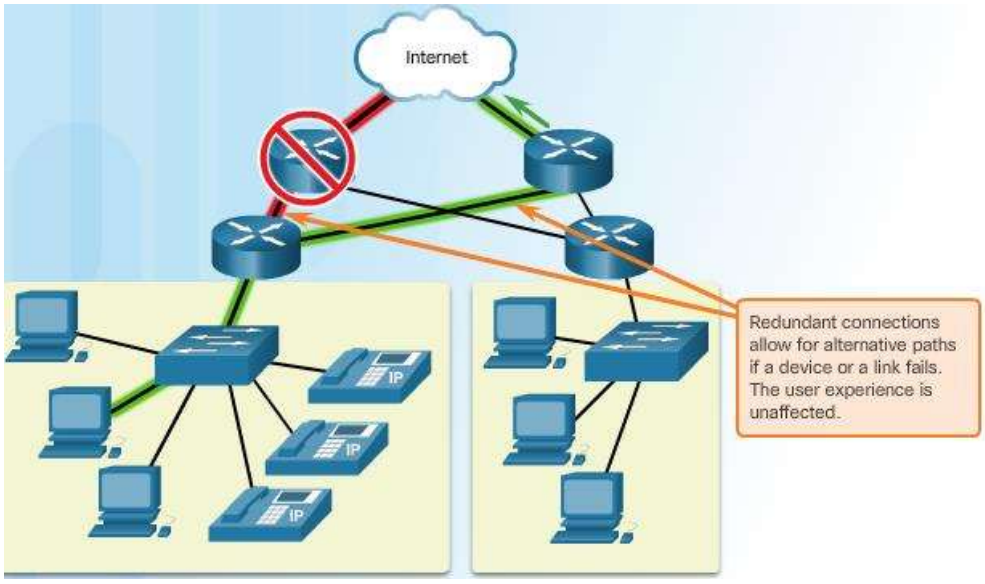
Mạng phải hỗ trợ nhiều ứng dụng và dịch vụ, cũng như hoạt động trên rất nhiều loại cơ sở hạ tầng vật lý khác nhau. Thuật ngữ kiến trúc mạng (network architecture) trong ngữ cảnh này nói các công nghệ hỗ trợ cơ sở hạ tầng, các dịch

vụ và giao thức được định nghĩa để vận chuyển các thông điệp trên cơ sở hạ tầng đó. Khi Internet và các mạng phát triển, có 4 vấn đề cần quan tâm để đáp ứng được các kỳ vọng của người dùng là:

- Tính chịu lỗi (fault tolerance)
- Khả năng mở rộng (scalability)
- Chất lượng dịch vụ (quality of service: QoS)
- Bảo mật (security)

Tính chịu lỗi

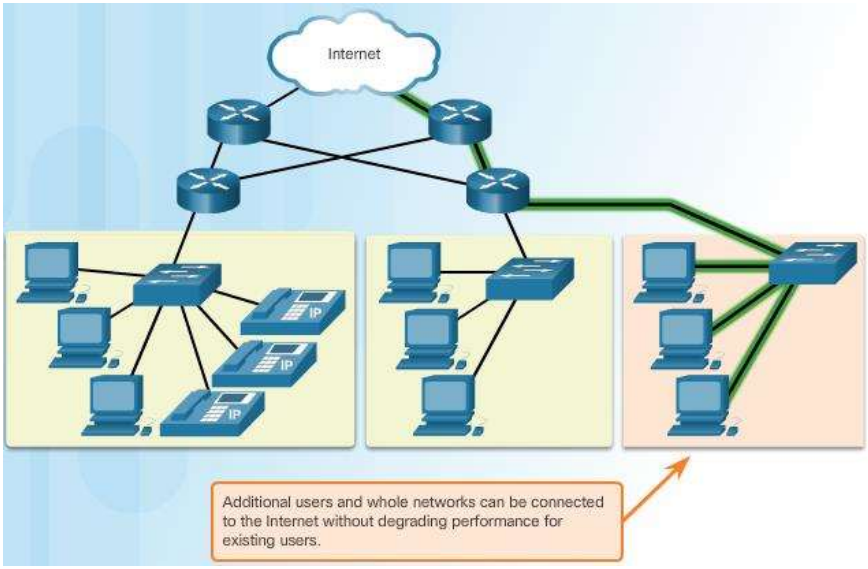
Kỳ vọng của người sử dụng Internet là làm sao mạng phải luôn sẵn sàng và truy cập với tốc độ cao. Vì vậy khi thiết kế và triển khai một mạng cần phải có tính năng chịu lỗi. Mạng có tính năng chịu lỗi là mạng giới hạn được tầm ảnh hưởng của lỗi phần cứng, phần mềm và có thể phục hồi nhanh chóng khi có sự cố xảy ra. Xây dựng mạng có tính năng chịu lỗi bằng cách tạo ra các kết nối hay các con đường đi dự phòng giữa nguồn và đích. Nếu một kết nối hay đường đi bị gián đoạn thì luôn luôn có một đường đi thay thế để mạng thông điệp đi. Quá trình chuyển đổi này là trong suốt đối với người dùng cũng như thiết bị đầu cuối. Cả cơ sở hạ tầng vật lý và các tiến trình luận lý hướng dẫn các thông điệp trên mạng được thiết kế phù hợp với tính năng này.



Hình 1.5: Tính chịu lỗi

Khả năng mở rộng

Mạng có tính triển khai là mạng có thể đáp ứng ngay khi có nhu cầu mở thêm kết nối và triển khai ứng dụng mới mà không ảnh hưởng đến hiệu quả của các dịch vụ đang chạy trên mạng cũng như những người dùng khác. Hàng ngàn người dùng và nhà cung cấp dịch vụ mới kết nối vào Internet mỗi ngày. Khả năng của mạng hỗ trợ các kiến trúc mới này phụ thuộc một thiết kế phân lớp của cơ sở hạ tầng vật lý và kiến trúc luận lý bên dưới. Hoạt động tại mỗi lớp cho phép người dùng hoặc nhà cung cấp dịch vụ có thể mở rộng mà không gây ngưng trệ toàn mạng. Công nghệ liên tục phát triển làm tăng khả năng mang các thông điệp và hiệu quả của các thành phần trong cơ sở hạ tầng tại mỗi lớp. Sự phát triển này – với các phương pháp mới cho phép xác định và định vị người dùng trong mạng – cho phép Internet theo kịp tốc độ phát triển của người dùng.

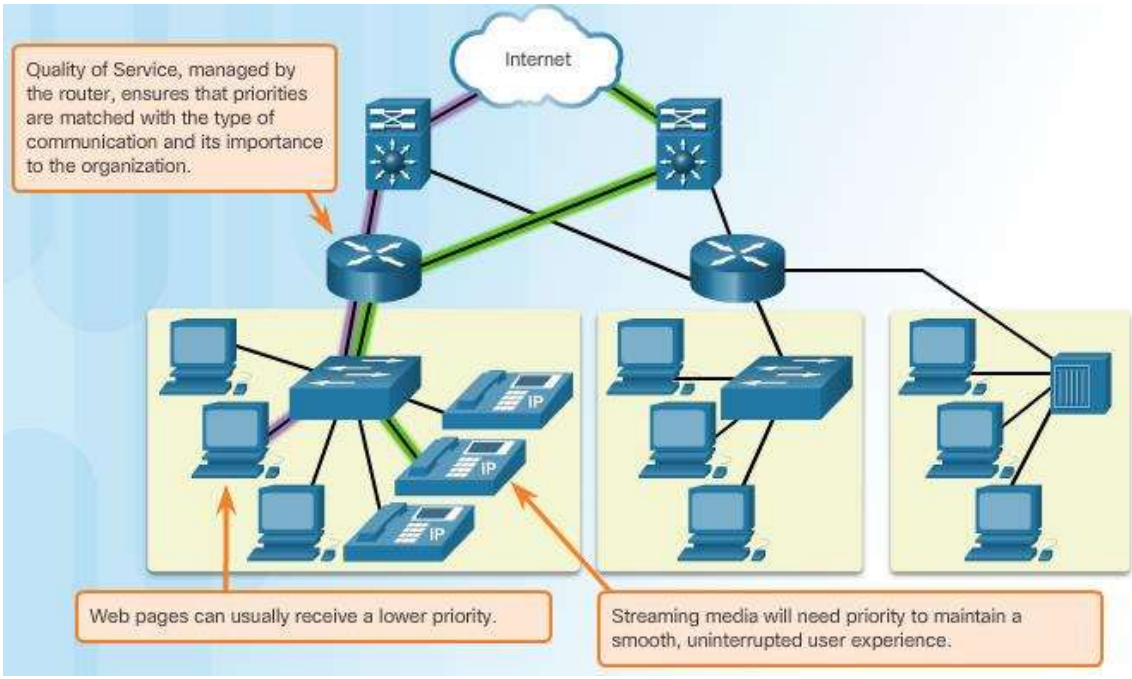


Hình 1.6: Khả năng mở rộng

Chất lượng dịch vụ (QoS)

Hiện nay người dùng có thể chấp nhận tính năng chịu lỗi và khả năng mở rộng của mạng Inernet cung cấp. Tuy nhiên, các ứng dụng mới mà người dùng có thể sử dụng trên mạng tạo ra các nhu cầu cao hơn về chất lượng dịch vụ. Các ứng dụng voice và video trực tuyến cần một chất lượng đường truyền cao hơn và không bị ngắt. Chất lượng của các dịch vụ này so sánh theo chất lượng thực nghiệm của cùng một ứng dụng được trình diễn trước người xem. Các mạng voice và video truyền thống được thiết kế dùng một kiểu môi trường truyền nhất định, và vì thế

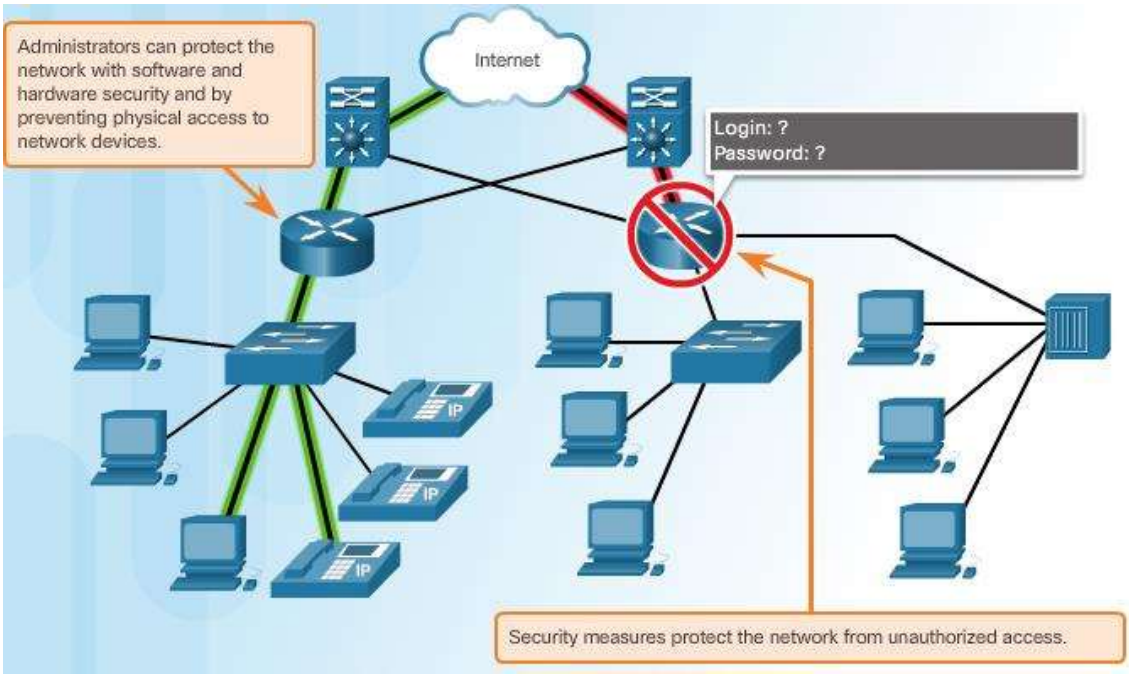
tạo ra một chất lượng có thể chấp nhận được. Các yêu cầu mới hỗ trợ cho chất lượng dịch vụ của mạng hội tụ đang làm thay đổi cách thiết kế và triển khai các kiến trúc mạng.



Hình 1.7: Chất lượng dịch vụ

Bảo mật

Internet phát triển từ một mạng được kiểm soát chặt chẽ bởi các tổ chức giáo dục và chính phủ trở thành một mạng được truy xuất rộng rãi cho các cá nhân hoặc doanh nghiệp giao tiếp với nhau. Kết quả là, các yêu cầu về bảo mật của Inetrnet đã thay đổi. Các kỳ vọng về bảo mật và tính riêng tư trong việc trao đổi các thông tin bí mật hoặc bí quyết kinh doanh đã vượt qua khỏi khả năng đáp ứng của kiến trúc mạng hiện đại. Nhiều mở rộng trong lãnh vực giao tiếp mà các mạng dữ liệu truyền thống không có làm tăng nhu cầu tích hợp bảo mật vào trong kiến trúc mạng. Kết quả là, có nhiều nỗ lực dành cho việc nghiên cứu và phát triển lãnh vực này. Đồng thời, nhiều công vụ và thủ tục được triển khai nhằm chống lại các điểm yếu về bảo mật trong kiến trúc mạng.



Hình 1.8: Bảo mật

1.6 | CÁC XU HƯỚNG CỦA MẠNG

1.6.1 | BYOD (BRING YOUR OWN DEVICE)

Đề cập đến chính sách cho phép nhân viên mang các thiết bị cá nhân (Laptop, Tablets và Smart phone) đến nơi làm việc, và cho phép dùng các thiết bị này truy cập vào tài nguyên của Doanh nghiệp.

Xu hướng BYOD đã trở thành một trong những xu thế có ảnh hưởng lớn nhất, đã và sẽ tác động tới mọi bộ phận CNTT cũng như tạo ra những thay đổi triệt để về cách thức các trang thiết bị được sử dụng trong môi trường làm việc và từ đó nâng cao năng suất lao động và đặc tính di động.

1.6.2 | CỘNG TÁC TRỰC TUYẾN (ONLINE COLLABORATION)

Cộng tác trực tuyến là cho phép một nhóm người dùng làm việc cùng nhau trong thời gian thực thông qua Internet. Những người tham gia có thể làm việc cùng nhau qua văn bản, thuyết trình… với tại những vị trí khác nhau, chỉ cần yêu cầu có kết nối Internet.

Cộng tác trực tuyến phù hợp cho tổ chức ở mọi quy mô khác nhau, không chỉ tốt khi làm việc với đồng nghiệp của mình mà nó còn rất phù hợp khi bạn trao đổi với khách của mình.

Internet cho phép một lực lượng lao động ngày càng phân tán và nó không là lạ khi ngày nay nhân viên làm việc từ khắp nơi trên thế giới. Cộng tác trực tuyến giảm bớt thời gian và tác động của khoảng cách địa lý.

1.6.3 | HỘI NGHỊ TRUYỀN HÌNH (VIDEO CONFERENCING)

Hội nghị truyền hình là hệ thống thiết bị (bao gồm cả phần cứng và phần mềm) truyền tải hình ảnh và âm thanh giữa hai hoặc nhiều địa điểm từ xa kết nối qua đường truyền mạng Internet, WAN hay LAN, để đưa tín hiệu âm thanh và hình ảnh của các phòng họp đến với nhau như đang ngồi họp cùng một phòng họp; Thiết bị này cho phép hai hoặc nhiều địa điểm cùng đồng thời liên lạc hai chiều thông qua video và truyền âm thanh.

Lợi ích của Hội nghị truyền hình

Hội nghị truyền hình là một bước phát triển đột phá của công nghệ thông tin, nó cho phép những người tham dự tại nhiều địa điểm từ những quốc gia khác nhau có thể nhìn thấy và trao đổi trực tiếp với nhau qua màn hình tivi như đang họp trong cùng một hội trường. Công nghệ này đã được ứng dụng rộng rãi trong nhiều lĩnh vực, đặc biệt trong hội họp và hội thảo. Ngoài ra, hội nghị truyền hình còn được ứng dụng rộng rãi trong giáo dục đào tạo, an ninh quốc phòng, y tế và chăm sóc sức khỏe.

- Tiết kiệm thời gian di chuyển.
- Tiết kiệm kinh phí.
- Thực hiện cuộc họp trực tuyến giữa nhiều địa điểm khác nhau.
- Nhanh chóng tổ chức cuộc họp.
- Lưu trữ toàn bộ nội dung cuộc họp.
- An toàn bảo mật.
- Chất lượng hội nghị ổn định.

- Độ ổn định của hình ảnh và âm thanh cao.
- Các quyết định và nội dung trao đổi được đưa ra kịp thời và đúng lúc.

1.6.4 | ĐIỆN TOÁN ĐÁM MÂY

Điện toán đám mây (cloud computing) là mô hình điện toán sử dụng các công nghệ máy tính và phát triển dựa vào mạng Internet. Thuật ngữ "đám mây" ở đây là lối nói ẩn dụ chỉ mạng Internet (dựa vào cách được bố trí của nó trong sơ đồ mạng máy tính) và như một liên tưởng về độ phức tạp của các cơ sở hạ tầng chứa trong nó.

Ở mô hình điện toán này, mọi khả năng liên quan đến công nghệ thông tin đều được cung cấp dưới dạng các "dịch vụ", cho phép người sử dụng truy cập các dịch vụ công nghệ từ một nhà cung cấp nào đó "trong đám mây" mà không cần phải có các kiến thức, kinh nghiệm về công nghệ đó, cũng như không cần quan tâm đến các cơ sở hạ tầng phục vụ công nghệ đó.

Như vậy, trước đây để có thể triển khai một ứng dụng (ví dụ một trang Web), bạn phải đi mua/thuê một hay nhiều máy chủ (server), sau đó đặt máy chủ tại các trung tâm dữ liệu (data center) thì nay điện toán đám mây cho phép bạn giản lược quá trình mua/thuê đi. Bạn chỉ cần nêu ra yêu cầu của mình, hệ thống sẽ tự động gom nhặt các tài nguyên rỗi (free) để đáp ứng yêu cầu của bạn. Chính vì vậy, có thể kể đến một vài lợi ích cơ bản của điện toán đám mây như sau:

- Sử dụng các tài nguyên tính toán động (Dynamic computing resources): Các tài nguyên được cấp phát cho doanh nghiệp đúng như những gì doanh nghiệp muốn một cách tức thời. Thay vì việc doanh nghiệp phải tính toán xem có nên mở rộng hay không, phải đầu tư bao nhiêu máy chủ thì nay doanh nghiệp chỉ cần yêu cầu "Hey, đám mây, chúng tôi cần thêm tài nguyên tương đương với 1 CPU 3.0 GHz, 128GB RAM…" và đám mây sẽ tự tìm kiếm tài nguyên rỗi để cung cấp cho bạn.
- Giảm chi phí: Doanh nghiệp sẽ có khả năng cắt giảm chi phí để mua bán, cài đặt và bảo trì tài nguyên. Rõ ràng thay vì việc phải cử một chuyên gia đi mua máy chủ, cài đặt máy chủ, bảo trì máy chủ thì nay bạn chẳng cần phải làm gì ngoài việc xác định chính xác tài nguyên mình cần và yêu cầu.

- Giảm độ phức tạp trong cơ cấu của doanh nghiệp: Doanh nghiệp sản xuất hàng hóa mà lại phải có cả một chuyên gia IT để vận hành, bảo trì máy chủ thì quá tốn kém. Nếu khoán ngoài được quá trình này thì doanh nghiệp sẽ chỉ tập trung vào việc sản xuất hàng hóa chuyên môn của mình và giảm bớt được độ phức tạp trong cơ cấu.

- Tăng khả năng sử dụng tài nguyên tính toán: Một trong những câu hỏi đau đầu của việc đầu tư tài nguyên (ví dụ máy chủ) là bao lâu thì nó sẽ hết khấu hao, tôi đầu tư như thế có lãi hay không, có bị outdate về công nghệ hay không. Khi sử dụng tài nguyên trên đám mây thì bạn không còn phải quan tâm tới điều này nữa.

Các nhà cung cấp dịch vụ điện toán đám mây cung cấp các dịch vụ của họ theo ba mô hình cơ bản:

- Cơ sở hạ tầng như một dịch vụ (IaaS)

- Nền tảng như một dịch vụ (PaaS)

- Phần mềm như một dịch vụ (SaaS)

Điện toán đám mây đang được phát triển và cung cấp bởi nhiều nhà cung cấp, trong đó có Amazon, Google, DataSynapse, và Salesforce cũng như những nhà cung cấp truyền thống như Sun Microsystems, HP, IBM, Intel, Cisco và Microsoft. Nó đang được nhiều người dùng cá nhân cho đến những công ty lớn như General Electric, L'Oréal, Procter & Gamble và Valeo chấp nhận và sử dụng.

1.7 | BÀI TẬP CHƯƠNG I

1. Nêu các khái niệm sau đây:
    a. Mạng máy tính
    b. Các thiết bị đầu cuối
    c. Đường truyền
    d. Bandwidth
    e. Topology
    f. Protocol

2. Cho 2 gói tin A và B, A được gửi đi với băng thông là 8000 bps, B được gửi đi với băng thông là 2 Mbps. Hỏi gói tin nào sẽ được nhận nhanh hơn?
3. Hãy cho biết những lợi ích khi sử dụng mạng?
4. Văn phòng khoa CNTT tại TDC có 5 máy tính kết nối với 1 máy in. Như vậy, kết nối mạng được sử dụng là gì?
5. Công ty Hyosung có trụ sở tại Hàn quốc và các văn phòng tại Trung Quốc và Việt Nam. Như vậy, kết nối mạng được sử dụng là gì?
6. Trình bày phân loại mạng theo kỹ thuật chuyển mạch.
7. Hãy vẽ hình minh họa các topo mạng Sao, Vòng, Bus.
8. Giao thức nào được sử dụng phổ biến nhất trên mạng Internet?
9. Internet là gì?
10. Trình bày kiến trúc mạng Internet

2. CÁC THÀNH PHẦN MẠNG

Sau khi học xong chương này, sinh viên có thể:

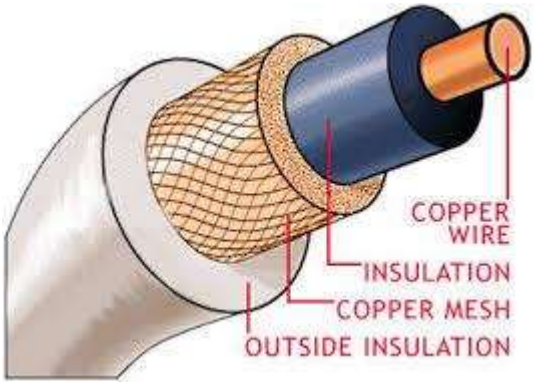
- Nhận biết và lựa chọn được các thiết bị cần thiết trong mạng LAN.
- Trình bày các hệ điều hành mạng.

2.1 | CÁC THIẾT BỊ MẠNG

2.1.1 | ĐƯỜNG TRUYỀN

❖ **Hữu tuyến**

- **Cáp đồng trục (Coaxial cable)**



Hình 2.1a: Cấu tạo cáp đồng trục

Hình 2.1b: Cấu tạo cáp đồng trục

➢ Cấu tạo

✓ Lớp dây dẫn điện bên trong cùng

✓ Lớp cách điện

- ✓ Lớp lưới dẫn điện bên ngoài
- ✓ Lớp nhựa bao phủ bên ngoài

➢ Tần số: 800KHz đến 500MHz, băng thông 500MHz

➢ Các chuẩn cáp đồng trục thường gặp:

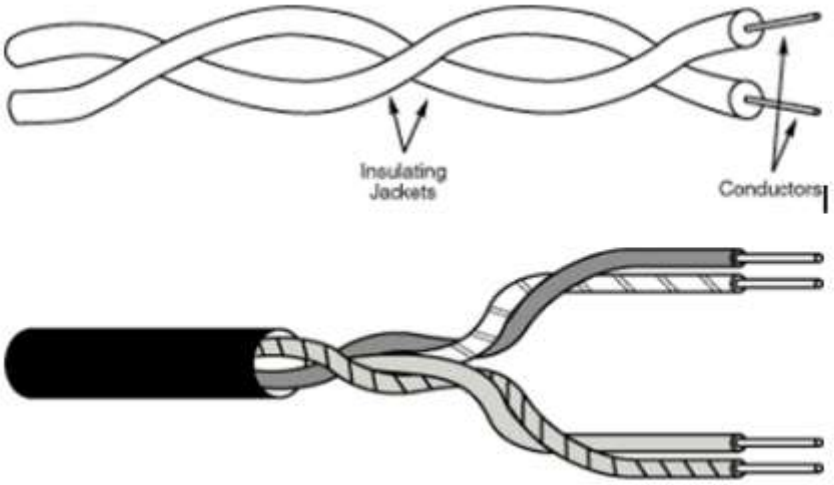
- ✓ RG-11: thick Ethernet
- ✓ RG-11: thick Ethernet
- ✓ RG-59: cáp TV

- **Cáp xoắn (twisted – pair cable)**

➢ Gồm nhiều cặp dây đồng xoắn lại với nhau nhằm chống phát xạ nhiễu điện từ.

➢ Được sử rất rộng rãi do giá thành thấp.

➢ Có 2 loại cáp xoắn đôi: STP (Shielded Twisted Pair), UTP (Unshielded Twisted Pair).



Hình 2.2: Cấu tạo cáp xoắn

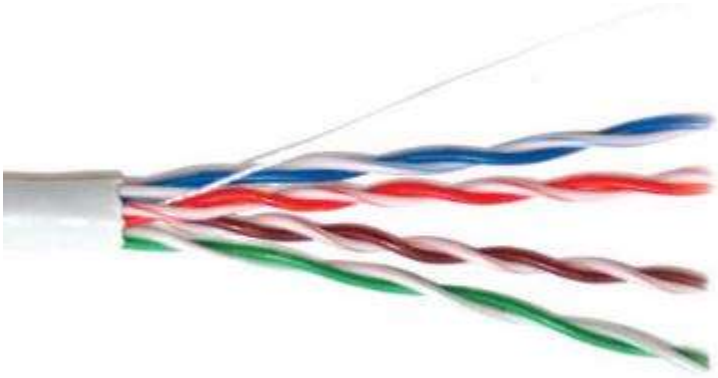
▪ Cáp STP (shielded twisted-pair):

- ✓ Gồm nhiều cặp xoắn được phủ bên ngoài 1 lớp vỏ làm bằng dây đồng bện.

- ✓ Lớp vỏ này có chức năng chống nhiễu từ bên ngoài và chống phát xạ nhiễu bên trong
- ✓ Lớp chống nhiễu này được nối đất để thoát nhiễu
- ✓ Tốc độ: 1Gbps với chiều dài 100m
- ✓ Đầu nối: DIN (DB-9), RJ45

Hình 2.3: Cấu tạo cáp STP

- Cáp UTP (Unshielded Twisted-Pair):

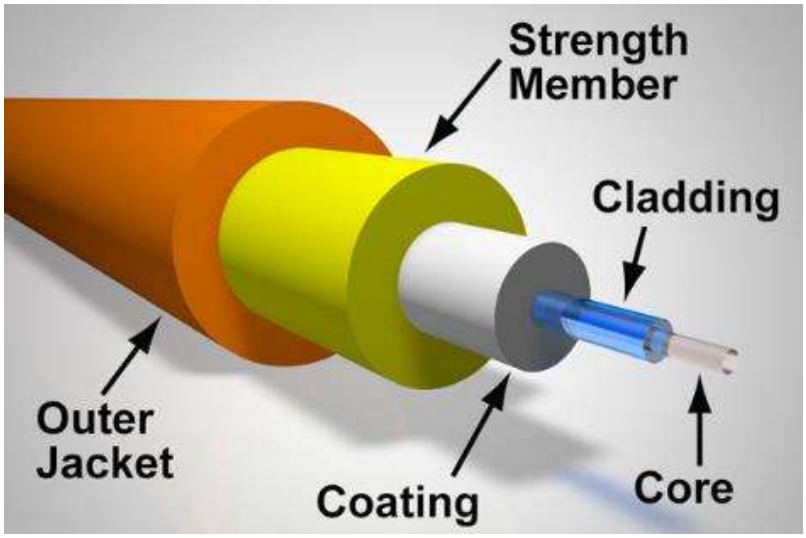


Hình 2.4: Cấu tạo cáp UTP

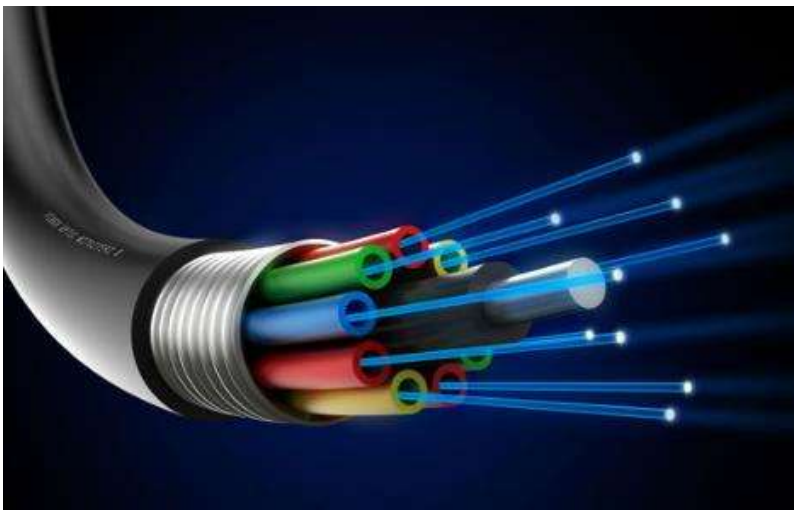
- ✓ Gồm nhiều cặp xoắn như cáp STP nhưng nó không có lớp vỏ bọc chống nhiễu.
- ✓ Độ dài tối đa của đoạn cáp là 100m.
- ✓ Dễ bị nhiễu khi đặt gần các thiết bị như: đường dây điện cao thế, nhiễu xuyên kênh…

✓ Dùng đầu nối RJ45.

- **Cáp quang (Fiber – optic cable).**



Hình 2.5a: Cấu tạo cáp quang



Hình 2.5b: Cấu tạo cáp quang

➢ Có cấu tạo gồm dây dẫn trung tâm là sợi thủy tinh hoặc plastic đã được tinh chế nhằm cho phép truyền đi tối đa các tín hiệu ánh sáng. Lõi cáp được bọc bởi lớp sơn phủ (cladding) tạo ra cáp quang. Lớp bọc ngoài có thể được cấu tạo từ nhiều chất liệu khác nhau bao gồm vỏ Teflon, plastic, plastic mạ kim loại hay lưới kim loại tùy theo các ứng dụng khác nhau và điều kiện lắp đặt.

- Cáp quang chỉ truyền sóng ánh sáng (không truyền tín hiệu điện) với băng thông cực cao.
- Không gặp các sự cố về nhiễu hay bị nghe trộm.
- Cáp quang có thể dài đến vài km.
- Băng thông cho phép đến 10Gbps.
- Giá thành cao, khó lắp đặt.
- Cáp quang hỗ trợ 2 chế độ: Multi-mode (đa chế độ) và Single-mode (chế độ đơn).
  - Multi-mode:
    - ✓ Sợi cáp thủy tinh có thể truyền được nhiều tia sáng trong cùng một khoảng thời gian
    - ✓ Khoảng cách đường truyền không xa bằng loại Single-mode
  - Single-mode:
    - ✓ Sợi cáp thủy tinh chỉ truyền 1 tia sáng duy nhất trên đường dây

❖ **<u>Vô tuyến (Wireless)</u>**

- **Cách truyền sóng:**
  - Lan truyền bề mặt: sóng lan truyền trong phần thấp nhất của khí quyển, sát mặt đất. Tại những tần số thấp nhất, tín hiệu tỏa ra theo nhiều hướng từ anten và đi theo bề mặt đất. Cự ly phát đi phụ thuộc vào công suất, công suất càng lớn thì đi càng xa. Lan truyền bề mặt cũng có thể đi theo mặt nước biển.
  - Lan truyền tầng đối lưu: có thể đi thẳng từ anten đến anten hay có thể truyền dẫn theo một góc rồi phản xạ lại xuống mặt đất nhiều lần khi chạm lớp bề mặt trên của tầng đối lưu.
  - Lan truyền tầng điện ly: sóng tần số cao có thể truyền đến tầng điện ly rồi phản xạ về mặt đất nhiều lần. Dạng lan truyền này cho phép truyền xa với công suất nhỏ.

- Lan truyền tầm thẳng: cần điều kiện là các anten phải nhìn thấy nhau. Như vậy, anten phải có tính định hướng, vị trí phải ở trên cao để không gặp chướng ngại vật.

- Lan truyền trong không gian: được dùng các bộ chuyển tiếp vệ tinh. Tín hiệu phát đi được vệ tinh thu và truyền tiếp về máy thu tại mặt đất. Dạng này đòi hỏi phải có các anten thu cực tốt do tín hiệu từ vệ tinh là yếu và bị suy giảm nhiều do cự ly xa.

- **Phân loại tần số:**

Dạng	Tần số	Cách truyền sóng
VLF (Very Low Frequency) VD: Sóng dài, thông tin hàng hải	3-30KHz	Lan truyền bề mặt
LF (Low Frequency) VD: Sóng dài, thông tin hàng hải	30-300KHz	Lan truyền bề mặt
MF (Middle Frequency) VD: Radio AM, hàng hải, radio định hướng, tần số báo nguy khẩn cấp	300KHz-3MHz	Lan truyền tầng đối lưu
HF (High Frequency) VD: amateur radio, citizen's band radio, truyền tin quốc tế, truyền tin quân sự, thông tin hàng hải, teleghaph, fax	3-30MHz	Lan truyền tầng điện ly
VHF (Very High Frequency) VD: sóng TV VHF, radio hàng không AM, hỗ trợ không lưu AM	30-300MHz	Lan truyền tầm thẳng và trong không gian
UHF (Ultra High Frequency) VD: sóng TV UHF, thông tin di động, paging, kết nối viba (sóng từ 1GHz của UHF đến SHF và EHF)	300MHz-3GHz	Lan truyền tầm thẳng và trong không gian

SHF (Super High Frequency) VD: thông tin viba mặt đất và vệ tinh, radar	3-30GHz	Lan truyền trong không gian
EHF (Extremely High Frequency) VD: thông tin không gian, radar, vệ tinh	30-300GHz	Lan truyền trong không gian

2.1.2 | CARD GIAO TIẾP MẠNG (NETWORK ADAPTER)

- Network adapater là thiết bị hoạt động đồng thời ở Datalink layer và Physical layer, có nhiệm vụ làm trung gian gắn kết máy tính với mạng.
- Mỗi Network Adapter sẽ có địa chỉ MAC riêng biệt được nhà sản xuất cài đặt.
- Có hai dạng Network Adapter:
  - Internal (dạng PCI).

Hình 2.6: Network Adapter - Internal

  - External (dạng usb).

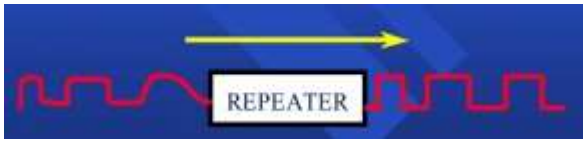
Hình 2.7: Network Adapter - External

- Mạng Ethernet sử dụng Network Adapter gọi là NIC (Network Interface Card).

2.1.3 | REPEATER

- Phục hồi tín hiệu, khuếch đại tín hiệu.
- Cho phép kéo dài khoảng cách mạng.
- Hoạt động ở Physical Layer của mô hình OSI

Hình 2.8a: Repeater



Hình 2.8b: Tín hiệu qua Repeater

2.1.4 | HUB

- Là Repeater nhiều cổng.
- Ứng dụng với băng thông thấp, kết nối số lượng người dùng nhỏ.
- Hoạt động ở Physical layer của mô hình OSI.

Hiện nay có 2 loại Hub phổ biến là Active Hub và Smart Hub:

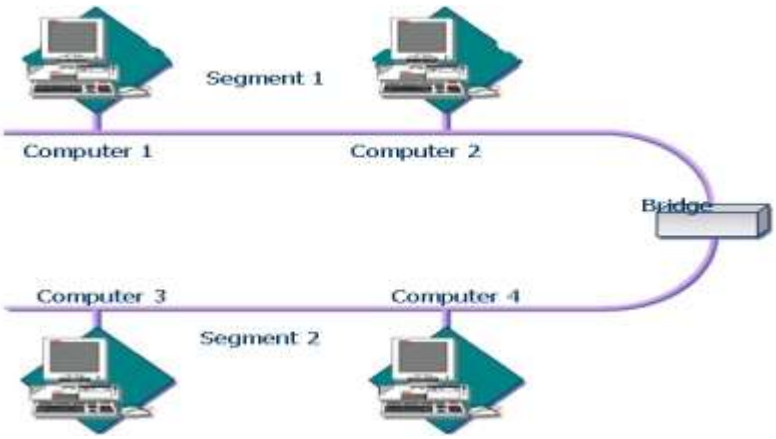
- Active Hub: loại Hub này thường được dùng phổ biến hơn rất nhiều, cần được cấp nguồn khi hoạt động. Active Hub dùng để khuếch đại tín hiện đến và chia ra những cổng còn lại để đảm bảo tốc độ tín hiệu cần thiết khi sử dụng.
- Smart Hub: hay còn gọi là Intelligent Hub cũng có chức năng làm việc tương tự như Active Hub, nhưng được tích hợp thêm chip có khả năng tự động dò lỗi trên mạng.

Hình 2.9: Hub

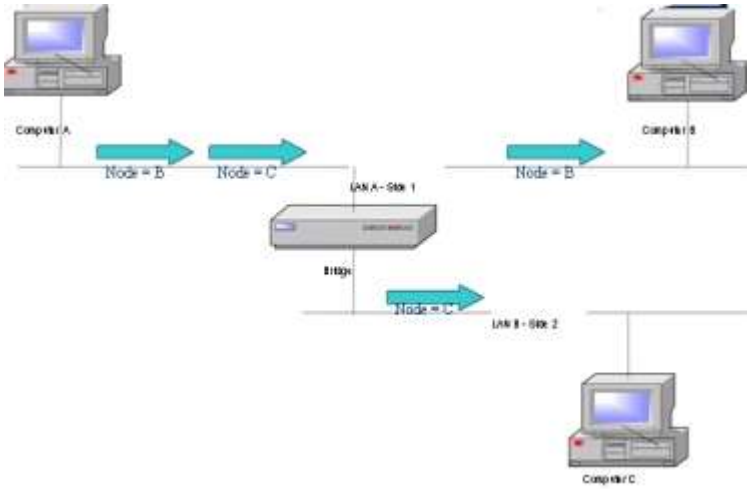
2.1.5 | BRIDGE

- Dùng để nối các đoạn mạng
- Chia đoạn mạng thành những đoạn nhỏ hơn nhằm tránh tắc nghẽn khi truyền thông
- Hoạt động ở Data Link layer của mô hình OSI

Hình 2.10a: Bridge



Hình 2.10b: Bridge



Hình 2.10c: Bridge

2.1.6 | SWITCH

- Có đặc điểm giống Hub.
- Băng thông cao, có cơ chế lọc khi gởi dữ liệu.

- Hoạt động ở Datalink layer của mô hình OSI.

Hình 2.11: Switch

2.1.7 | ROUTER

- Có nhiệm vụ kết nối hai hoặc nhiều mạng IP với nhau.
- Vì cần phải tính toán để tìm ra đường đi cho các gói tín hiệu, khả năng làm việc của Router chậm hơn Bridge, nhất là khi kết nối với các mạng không cùng tốc độ.
- Hoạt động ở Network layer của mô hình OSI.

Hình 2.12: Router

2.1.8 | GATEWAY

- Gateway kết nối hai mạng có giao thức khác nhau, như mạng dùng giao thức IP với mạng sử dụng giao thức IPX, Novell, DECnet, SNA...
- Gateway có khả năng phân biệt các giao thức, ứng dụng khi chuyển thư điện tử từ mạng này sang mạng khác, chuyển đổi một phiên làm việc từ xa.

Hình 2.13: Gateway

2.1.9 | WIRELESS ACCESS POINT

- Dùng trong mạng không dây, có tầng số radio là 2.4GHz và 5GHz.
- Hoạt động ở Datalink layer.

Hình 2.14: Wireless Access Point

2.2 | CÁC HỆ ĐIỀU HÀNH MẠNG

2.2.1 | KHÁI NIỆM

Hệ điều hành mạng (Network Operating System-NOS): NOS cung cấp các dịch vụ về mạng như dùng chung tập tin, máy in, quản lý tài khoản người dùng... Nếu máy trạm dựa vào các dịch vụ được cung cấp bởi máy chủ, một NOS được thiết kế tốt sẽ cung cấp cơ chế bảo vệ cũng như khả năng đa nhiệm, giúp tránh được các lỗi đáng tiếc xảy ra.

2.2.2 | SỰ KHÁC NHAU GIỮA CLIENT SOFTWARE VÀ SERVER SOFTWARE

Sự khác nhau giữa máy trạm và máy chủ phụ thuộc vào phần mềm được cài đặt trên đó.

- Client Software: Hệ điều hành dành cho máy trạm, nhận các yêu cầu từ người dùng.
  - ➢ Nếu yêu cầu đó được cung cấp bởi các phần mềm trên máy trạm đó thì nó sẽ xác định chương trình xử lý rồi gửi yêu cầu đến chương trình đó.
  - ➢ Nếu yêu cầu đó được cung cấp bởi các dịch vụ trên mạng nó sẽ gửi yêu cầu cho máy chủ để được phục vụ.
- Server Software: Hệ điều hành dành cho máy chủ.
  - ➢ Máy chủ tồn tại là để nhằm thỏa mãn các yêu cầu của các máy trạm. Máy chủ thường lưu trữ phần lớn dữ liệu của toàn mạng và thực hiện các nhiệm vụ như :
    - ✓ Quản lý tài khoản người dùng: NOS yêu cầu mỗi người dùng khi đăng nhập vào mạng phải có tài khoản (tên và mật khẩu truy cập). Sau khi đăng nhập vào mạng, người dùng có quyền sử dụng các tài nguyên của mạng tùy thuộc vào quyền truy cập của mình. Các tài khoản người dùng được tổ chức thành cơ sở dữ liệu và được quản lý bởi người quản trị mạng-người có quyền thêm, xóa, sửa các tài khoản người dùng.
    - ✓ Central Licensing: Theo luật bản quyền thì mỗi bản đăng ký chỉ dành cho một người dùng. Điều này gây khó khăn cả về mặt tài chính cũng như quá trình cài đặt cho nhiều người trong cùng một tổ chức hay

công ty cùng sử dụng một phần mềm nào đó. Central Licensing giúp phần mềm cài trên máy chủ cho phép mọi người cùng sử dụng.

- ✓ Bảo vệ an ninh mạng: máy chủ có thể quản lý được các tài nguyên mà mỗi người dùng được quyền truy cập. Người quản trị mạng có thể gán các quyền truy cập khác nhau cho những người dùng khác nhau. Điều này cho phép người dùng lưu trữ các thông tin cá nhân hay các thông tin nhạy cảm trên mạng một cách an toàn.
- ✓ Bảo vệ dữ liệu: do những dữ liệu quan trọng nhất thường được lưu trên máy chủ nên nó thường được cài đặt cơ chế bảo vệ dữ liệu rất chặt chẽ.

➢ Được thiết kế để hỗ trợ các tính năng đa nhiệm và đa xử lý.

- ✓ Multitasking: kỹ thuật thực thi nhiều nhiệm vụ cùng lúc chỉ sử dụng một CPU.
- ✓ Multiprocessing: kỹ thuật sử dụng nhiều CPU để xử lý một hoặc nhiều tiến trình, NOS sẽ thực hiện việc phân chia nhiệm vụ, quản lý quá trình thực hiện cho từng CPU.
- ✓ Multiuser: kỹ thuật có thể cho nhiều người sử dụng cùng truy cập vào một thời điểm.

2.2.3 | HỆ ĐIỀU HÀNH MẠNG

WINDOW SERVER 2008

Microsoft Windows Server 2008 là thế hệ kế tiếp của hệ điều hành Windows Server, có thể giúp các chuyên gia công nghệ thông tin có thể kiểm soát tối đa cơ sở hạ tầng của họ và cung cấp khả năng quản lý và hiệu lực chưa từng có, là sản phẩm hơn hẳn trong việc đảm bảo độ an toàn, khả năng tin cậy và môi trường máy chủ vững chắc hơn các phiên bản trước đây.

Windows Server 2008 cung cấp những giá trị mới cho các tổ chức bằng việc bảo đảm tất cả người dùng đều có thể có được những thành phần bổ sung từ các dịch vụ từ mạng. Windows Server 2008 cũng cung cấp nhiều tính năng vượt trội bên trong hệ điều hành và khả năng chuẩn đoán, cho phép các quản trị viên tăng được thời gian hỗ trợ cho các doanh nghiệp.

Windows Server 2008 được thiết kế để cung cấp cho các tổ chức có được nền tảng sản xuất tốt nhất cho ứng dụng, mạng và các dịch vụ web từ nhóm làm việc đến những trung tâm dữ liệu với tính năng động, tính năng mới có giá trị và những cải thiện mạnh mẽ cho hệ điều hành cơ bản.

Những cải thiện gồm có các vấn đề về mạng, các tính năng bảo mật nâng cao, truy cập ứng dụng từ xa, quản lý role máy chủ tập trung, các công cụ kiểm tra độ tin cậy và hiệu suất, nhóm chuyển đổi dự phòng, sự triển khai và hệ thống file.

Yêu cầu phần cứng

Cấu hình	Tối thiểu	Đề nghị	Tối ưu
Bộ nhớ RAM	512MB	1GB	2GB
Bộ vi xử lý	1Ghz	2Ghz	3Ghz
Ổ cứng (trống)	10GB	40GB	80GB

Lưu ý:

Cấu hình đề nghị trên chỉ là yêu cầu cần thiết để chạy hệ điều hành.

Các phiên bản Windows Server 2008

Windows Server 2008 có nhiều bản khác nhau, hỗ trợ vi xử lý x86, x64 và Itanium đồng thời hỗ trợ tính sẵn sàng cao, cân bằng tải và ảo hóa.

- Windows Web Server 2008
- Windows Server 2008 Standard
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Enterprise
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 Datacenter
- Windows Server 2008 Datacenter without Hyper-V

- Windows HPC Server 2008
- Windows Server 2008 for Itanium-Based Systems

Windows Web Server 2008

Windows Web Server 2008 có những cải tiến về kiến trúc trong IIS 7.0, ASP.NET và Microsoft .NET Framework. Đây là bản dùng để triển khai trang web, ứng dụng web và dịch vụ web.

Windows Web Server 2008 hỗ trợ:

- 32GB Ram trên hệ thống 64-bit (4GB trên hệ thống 32-bit)
- 4 bộ vi xử lý đa nhân

Windows Server 2008 Standard

Windows Server 2008 Standard là hệ điều hành mạnh mẽ cho máy chủ, được tích hợp nhiều tính năng nhằm cải thiện bảo mật, quản lý, và giảm chi phí cơ sở hạ tầng, bao gồm:

- Web services
- Hyper-V
- Terminal Services
- Presentation virtualization
- Application virtualization
- Network Access Protection (NAP)
- BitLocker
- RODCs
- Windows Service Hardening
- Bidirectional Windows Firewall

- Next-generation cryptography support
- Server Manager
- Windows Deployment Services
- Windows PowerShell
- Next-generation TCP/IP
- Server Core

Windows Server 2008 Standard hỗ trợ:

- 32GB Ram trên hệ thống 64-bit (4GB trên hệ thống 32-bit)
- 4 bộ vi xử lý đa nhân
- 250 kết nối dịch vụ truy cập mạng (Network Access Services - NAS)
- 50 kết nối máy chủ chính sách mạng (Network Policy Server - NPS)
- 250 kết nối máy phục vụ thiết bị đầu cuối (Terminal Server)
- Ảo hóa Hyper-V với một giải pháp miễn phí

Windows Server 2008 Enterprise

Windows Server 2008 Enterprise bổ sung tính sẵn sàng cao, những công nghệ bảo mật mới nhất và khả năng nâng cấp so với bản Standard. Sau đây là một vài tính năng nổi bật:

- Nhóm chuyển đổi dự phòng - tới 16 nút (Failover clustering)
- Đồng bộ hóa bộ nhớ bỏ qua lỗi (Fault-tolerant memory)
- Sao chép chéo
- Cấp phép tối đa 4 máy ảo bổ sung
- Active Directory Federation Services (ADFS)
- Advanced certificate services

- Active Directory Domain Services (ADDS)

Windows Server 2008 Enterprise hỗ trợ:

- 8 bộ vi xử lý
- 2TB Ram trên hệ thống 64-bit (64GB trên hệ thống 32-bit)
- Không giới hạn số kết nối VPN (mạng riêng ảo)
- Không giới hạn số kết nối dịch vụ truy cập mạng
- Không giới hạn số kết nối máy chủ chính sách mạng

Windows Server 2008 Datacenter

Đây là ấn bản dành cho nhu cầu ảo hoá quy mô lớn và được bổ sung khả năng nâng cấp cho ứng dụng trọng yếu trong cơ sở hạ tầng CNTT lớn. Sau đây là những tính năng nổi bật:

- Ảo hóa quy mô lớn - cho phép bạn thêm vô số giải pháp ảo
- Failover clustering
- Phân chia phần cứng động
- Windows Server High Availability Program

Windows Server 2008 Datacenter hỗ trợ:

- 2TB Ram trên hệ thống 64-bit (64GB trên hệ thống 32-bit)
- 64 bộ vi xử lý 64-bit x64 và 32 bộ vi xử lý 32-bit x86
- Không giới hạn quyền sử dụng ảnh ảo
- 16 nút failover clustering (nhóm liên kết chuyển đổi dự phòng)
- Thêm nóng / Thay nóng bộ nhớ và bộ vi xử lý trên phần cứng hỗ trợ
- Đồng bộ hóa bộ nhớ bỏ qua lỗi
- Sao chép chéo

- Không giới hạn số kết nối dịch vụ truy cập mạng
- Không giới hạn số kết nối máy chủ chính sách mạng
- 65,535 kết nối terminal server
- Quản lý nhận dạng tiên tiến

Windows HPC Server 2008

Dành riêng cho môi trường điện toán hiệu suất cao (HPC), ấn bản này cho phép bạn vươn tới quy mô hàng ngàn lõi vi xử lý. Điều này có lợi khi bạn là cân bằng tải khối lượng lớn công việc qua nhiều bộ vi xử lý và cần quản lý cũng như giám sát tính ổn định và sức khỏe môi trường HPC.

Windows Server 2008 for Itanium-Based Systems

Windows Server 2008 for Itanium-Based Systems cho phép bạn chạy Windows Server 2008 trên hệ thống nền tảng Itanium. Các bộ vi xử lý nền tảng Itanium có khả năng xử lý nhu cầu điện toán cấp tốc của các ứng dụng nghiệp vụ trong môi trường cấp doanh nghiệp. Bộ vi xử lý Itanium sử dụng cấu trúc mới hoàn toàn chứ không phải chỉ mở rộng từ cấu trúc 32-bit lên 64-bit. Một đặc điểm nữa của bộ vi xử lý này đó là kiến trúc Điện toán lệnh song song (EPIC) giúp cải thiện hiệu suất qua trạng thái song song cấp lệnh, tăng tối đa cơ hội thực thi câu lệnh song song. Tối đa sáu câu lệnh có thể được thực thi song song.

Windows Server 2008 for Itanium-Based Systems hỗ trợ:

- Phân chia phần cứng động
- Tận dụng ưu thế của Itanium (độ tin cậy, tính sẵn sàng và khả năng nâng cấp)
- 2TB RAM
- 64 bộ vi xử lý Itanium hoặc 64 nhân
- Thêm nóng / Thay nóng bộ nhớ RAM và bộ vi xử lý
- 8 nút failover clustering

- Đồng bộ hóa bộ nhớ bỏ qua lỗi
- Cấp phép không giới hạn giải pháp ảo với sản phẩm ảo hoá bên thứ ba

LINUX

Tổng quan về Linux

Linux là một hệ điều hành giống Unix đầy đủ và độc lập. Nó có thể chạy X-Window, TCP/IP, Web, thư điện tử, ... Hầu hết các phần mềm miễn phí và thương mại đều được chuyển lên Linux. Người ta thực hiện các phép đo benchmarks trên Linux và thấy rằng chúng thực hiện nhanh hơn khi thực hiện trên các máy trạm của Sun Microystem và Compaq, thậm chí nhiều khi còn nhanh hơn cả trên Windows 98 và WindowNT. Linux càng ngày càng trở nên mạnh mẽ, ổn định và độ tin cậy cao.

Ưu điểm của Linux

- Đa nền

Nó có thể vận hành trên các nền khác nhau như Alpha, Sparc, Dec, Sun, Power PC và một số nền 68000 như Atari, Amiga...Ngoài ra Linux còn chạy trên một số máy MIPS và các máy tính cá nhân mạnh.

- Đa chương trình

Một thời điểm một người sử dụng có thể thực hiện đồng thời nhiều tác vụ.

- Độc lập phần cứng

Vì được viết bằng ngôn ngữ cấp cao cho nên nó rất dễ cài đặt trên các cấu hình phần cứng khác. Hơn nữa với cách tổ chức các thiết bị là các tập tin đặc biệt nên việc thêm vào hay loại bỏ các thiết bị rất dễ dàng.

- Dùng chung thiết bị

Các thiết bị ngoại vi như máy in,v.v... có thể được dùng chung bởi nhiều người sử dụng.

- Tính ổn định

Nó ít bị lỗi khi sử dụng so với hầu hết các hệ điều hành khác. Người sử dụng Linux sẽ không phải lo lắng đến chuyện máy tính của mình bị hiện tượng "treo cứng" khi đang sử dụng nữa. Thông thường lý do để ta bắt buộc phải khởi động lại hệ thống là do mất điện, nâng cấp phần cứng hoặc phần mềm.

- Tính bảo mật

Khi làm việc trên Linux người dùng có thể an tâm hơn về tính bảo mật của hệ điều hành. Linux là hệ điều hành đa nhiệm, đa người dùng, điều này có nghĩa là có thể có nhiều người dùng vào phiên làm việc của mình trên cùng một máy tại cùng một thời điểm. Linux cung cấp các mức bảo mật khác nhau cho người sử dụng. Mỗi người sử dụng chỉ làm việc trên một không gian tài nguyên riêng, chỉ có người quản trị hệ thống mới có quyền thay đổi trong máy.

- Tính hoàn chỉnh

Bản thân Linux đã kèm theo các trình tiện ích cần thiết. Tất cả các trình tiện ích mà ta mong đợi đều có sẵn hoặc ở một dạng tương đương rất giống. Trên Linux, các trình biên dịch như C, C++, …, đều được chẩn hoá.

- Tính tương thích

Linux tương thích hầu như hoàn toàn với hầu hết các chuẩn Unix như IEEE POSIX.1, UNIX System V và BSD Unix. Trên Linux ta cũng có thể tìm thấy các trình giả lập DOS và Windows cho phép ta chạy các ứng dụng quen thuộc trên DOS và Windows. Linux cũng hỗ trợ hầu hết các phần cứng PC như đã nói trên.

- Hệ điều hành 32-bit đầy đủ

Ngay từ đầu Linux đã là hệ điều hành 32 bit đầy đủ. Điều đó có nghĩa là ta không còn phải lo về giới hạn bộ nhớ, các trình điều khiển EMM hay các bộ nhớ mở rộng,… khi sử dụng Linux. Linux hỗ trợ tốt cho tính toán song song và máy tính cụm (PC-cluster) là một hướng nghiên cứu triển khai ứng dụng nhiều triển vọng hiện nay.

- Linux có giao diện đồ hoạ (GUI):

Thừa hưởng từ hệ thống X-Window. Linux hỗ trợ nhiều giao thức mạng, bắt nguồn và phát triển từ dòng BSD. Thêm vào đó, Linux còn hỗ trợ tính toán thời gian thực

- Dễ cấu hình

Ta không còn phải bận tâm về giới hạn 640K và tiến hành tối ưu hoá bộ nhớ mỗi lần cài đặt một trình điều khiển mới. Linux cho ta toàn quyền điều khiển về cách làm việc của hệ thống.

Nhược điểm của Linux:

- Việc cài đặt Linux còn tương đối phức tạp và khó khăn. Khả năng tương thích của Linux với một số loại thiết bị phần cứng còn thấp do chưa có các trình điều khiển cho nhiều thiết bị.
- Phần mềm ứng dụng chạy trên nền Linux chưa phong phú khi so sánh với MS Windows.

2.3 | BÀI TẬP CHƯƠNG 2

2.3.1 | BÀI TẬP 1 – BÀI TẬP NHÓM

Bài tập nhóm: (mỗi nhóm khoảng 5 sinh viên)

Nội dung: Tìm hiểu và thuyết trình về các chủ đề:

- Đường truyền hữu tuyến
- Đường truyền vô tuyến
- Network adapter, Repeater, Hub, Bridge
- Switch, Router, Gateway, Wireless access point
- Window server 2008
- Linux

2.3.2 | BÀI TẬP 2

1. Trình bày cấu tạo cáp đồng trục. Vẽ hình minh họa.
2. Trình bày cấu tạo cáp xoắn. Vẽ hình minh họa.

3. Trình bày cấu tạo cáp quang. Vẽ hình minh họa.
4. Phân loại cách truyền sóng vô tuyến và tần số sóng vô tuyến.
5. Nêu công dụng của các thiết bị sau:
    a. Network adapter
    b. Repeater
    c. Hub
    d. Bridge
    e. Switch
    f. Router
    g. Gateway
    h. Wireless access point
6. Phân biệt sự khác nhau giữa Client Software và Server Software trong hệ điều hành mạng.
7. Trình bày tổng quan về hệ điều hành Window Server 2008.
8. Liệt kê các phiên bản của Window Server 2008.
9. Trình bày tổng quan về hệ điều hành Linux.
10. Ưu và nhược điểm của Linux.

3. MÔ HÌNH THAM CHIẾU OSI VÀ MÔ HÌNH TCP/IP

Sau khi học xong chương này, sinh viên có thể:

- Giải thích hoạt động của các lớp trong mô hình tham chiếu OSI.
- Giải thích hoạt động của các lớp trong mô hình TCP/IP.

3.1 | KHÁI NIỆM GIAO THỨC

Trong cuộc sống hàng ngày chúng ta thường liên lạc với những người khác bằng cách nói chuyện trực diện với nhau, nói chuyện qua điện thoại, gửi thư,... Nếu để ý, chúng ta sẽ thấy những quy tắc mà chúng ta cần tuân thủ trong quá trình liên lạc. Ví dụ, để một cuộc liên lạc thành công, trước tiên hai người phải thống nhất một ngôn ngữ để nói chuyện. Trong quá trình liên lạc nếu chúng ta không nghe rõ thì chúng ta có thể yêu cầu người đó nói lại, hoặc nếu chúng ta nghe không kịp chúng ta có thể yêu cầu người đó nói chậm lại, v.v..Tất cả những điều này tạo nên một tập hợp các quy tắc và được gọi là thể thức liên lạc. Trong môi trường mạng nó được gọi tắt là giao thức. Vậy giao thức là tập hợp các quy tắc chi phối quá trình giao tiếp giữa các thiết bị trên mạng. Đối với con người, tất cả các quy tắc đều dựa trên phong tục và thói quen chứ không có một văn bản nào quy định rõ những quy tắc này. Tuy nhiên, trong môi trường mạng, các giao thức mà các thiết bị sử dụng để truyền thông với nhau đòi hỏi phải được đặc tả một cách rõ ràng, chính xác.

Các giao thức sẽ đặc tả:

- Định dạng của một thông điệp.
- Tiến trình mà các thiết bị mạng chia sẻ thông tin về đường đi với các thiết bị mạng khác.
- Cách và khi nào những thông điệp hệ thống và những thông điệp lỗi được phát ra giữa các thiết bị.
- Thiết lập và ngắt các phiên truyền dữ liệu.

Hiện nay có rất nhiều giao thức khác nhau chi phối tất cả các phương thức truyền thông hiện có. Dưới đây là một số giao thức tiêu biểu.

- TCP (Transmission Control Protocol): thiết lập kết nối giữa các máy tính để truyền dữ liệu. Nó chia nhỏ dữ liệu thành những phân đoạn (segment) và đảm bảo việc truyền dữ liệu thành công.
- IP(Internet Protocol): định tuyến (route) các gói dữ liệu khi chúng được truyền qua Internet, đảm bảo dữ liệu sẽ đến đúng nơi cần nhận.

- HTTP (HyperText Transfer Protocol): cho phép trao đổi thông tin ở dạng siêu văn bản qua Internet.
- POP3 (Post Office Protocol, phiên bản 3): cho phép nhận scan thông điệp thư điện tử qua Internet.
- v.v...

Để các host trên mạng giao tiếp được thành công, phải dựa vào nhiều giao thức khác nhau và các giao thức này có sự tương tác với nhau. Một nhóm các giao thức liên quan cùng thực hiện một chức năng truyền thông được gọi là một họ giao thức. Ví dụ như họ giao thức TCP/IP. Chúng ta có thể cài đặt các giao thức này vào các thiết bị trên mạng thông qua phần mềm hoặc phần cứng.

3.2 | GIỚI THIỆU GIAO THỨC TCP/IP

Giao thức TCP/IP (Transmission Control Protocol/Internet Protocol) là họ các giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng. Vì lịch sử của TCP/IP gắn liền với Bộ quốc phòng Mỹ, nên việc phân lớp giao thức TCP/IP được gọi là mô hình DoD (Department of Defense). Đây là họ các giao thức được sử dụng phổ biến trên mạng Internet, mang tính mở nhất, phổ dụng nhất và được hỗ trợ của nhiều hãng kinh doanh.

Một số ứng dụng thường gặp của giao thức TCP/IP:

- FTP (File Transfer Protocol): Một giao thức chạy trên nền TCP cho phép truyền các file ASCII hoặc nhị phân dạng hai chiều.
- TFTP (Trivial File Transfer Protocol): Giao thức truyền file chạy trên nền UDP.
- SMTP (Simple Mail Transfer Protocol): Đây là giao thức dùng để phân phối thư điện tử.
- Telnet: Cho phép truy chập từ xa để cấu hình thiết bị.
- SNMP (Simple Netwrok Manahement Protocol): Là một ứng dụng chạy trên nền UDP, cho phép quản lý và giám sát các thiết bị mạng từ xa.

- DNS (Domain Name System): Giao thức phân giải tên miền, thường được hỗ trợ truy cập Internet.

3.3 | CÁC TỔ CHỨC QUY ĐỊNH CHUẨN MẠNG

Các chuẩn (standard) là các thỏa thuận bằng văn bản gồm những đặc tả kỹ thuật hay những tiêu chuẩn nghiêm ngặt khác quy định cách thiết kế và triển khai các sản phẩm dịch vụ cụ thể. Nhiều ngành khác nhau đều sử dụng các tiêu chuẩn để bảo đảm rằng các sản phẩm, quy trình, và dịch vụ phù hợp với mục đích của họ.

Ngày nay, do sự đa dạng trong việc sử dụng phần cứng và phần mềm, các chuẩn đóng một vai trò đặc biệt quan trọng trong lĩnh vực mạng. Nếu không có chuẩn, việc thiết kế sẽ trở nên khó khăn hơn vì bạn không thể chắc chắn rằng các phần mềm hay phần cứng từ những nhà sản xuất khác nhau có thể hoạt động cùng với nhau không. Ví dụ, nếu một nhà sản xuất thiết kế một cáp mạng với đầu cắm rộng 1cm và một công ty khác sản xuất ổ mạng âm tường với độ mở rộng 0,8 cm, bạn sẽ không thể đưa đầu cắm đó vào trong ổ mạng âm tường. Do đó, khi mua một thiết bị mạng, bạn cần xác định xem thiết bị có đạt chuẩn do mạng của bạn yêu cầu hay không.

Do ngành công nghiệp máy tính phát triển nhanh chóng vượt ra khỏi một số quy tắc về kỹ thuật, nhiều tổ chức khác nhau được mở ra để giám sát các chuẩn. Trong một số trường hợp, một số tổ chức chịu trách nhiệm về một lĩnh vực cụ thể trong ngành mạng máy tính. Ví dụ, cả Viện Tiêu chuẩn Quốc gia Hoa kỳ (ANSI) và Viện Kỹ nghệ Điện và Điện tử (IEEE) đều phát triển việc thiết lập chuẩn cho các mạng không dây. Trong khi ANSI quy định loại NIC (card giao tiếp mạng) mà người tiêu dùng cần để chấp nhận một kết nối không dây thì IEEE quy định cách mà mạng sẽ bảo đảm cho các phần khác nhau của một quá trình truyền thông được gửi qua mạng không dây đến đích theo đúng thứ tự.

Hình 3.1: Các tổ chức quy định chuẩn

IEEE (Institute of Electrical and Electronics Engineers - Viện Kỹ nghệ Điện và Điện tử), hay "I3E",

IEEE là một hiệp hội quốc tế gồm các chuyên gia kỹ thuật. Mục tiêu của nó là thúc đẩy sự phát triển và giáo dục trong các lĩnh vực kỹ thuật điện và khoa học máy tính. Với mục đích này, IEEE tổ chức nhiều hội nghị, hội thảo và các cuộc họp địa phương, đồng thời xuất bản nhiều tài liệu giáo dục những tiến bộ kỹ thuật cho các thành viên. Nó cũng duy trì một ban chuyên đặt ra các chuẩn riêng cho các ngành công nghiệp máy tính và điện tử, đồng thời đóng góp vào công việc của các cơ quan thiết lập tiêu chuẩn khác như ANSI. Các tài liệu kỹ thuật và các chuẩn của IEEE được đánh giá cao trong chuyên ngành mạng.

ANSI (American National Standards Institue - Viện Tiêu chuẩn Quốc gia Hoa Kỳ)

ANSI là một tổ chức gồm hơn một nghìn đại diện từ các ngành công nghiệp và chính phủ, những người đã cùng nhau quyết định các chuẩn cho ngành công nghiệp điện tử và các ngành khác, ví dụ như hóa học và kỹ thuật hạt nhân, sức khoẻ, an toàn, và xây dựng. ANSI cũng đại diện cho Hoa Kỳ trong việc thiết lập các chuẩn quốc tế. Tổ chức này không buộc các nhà sản xuất phải tuân thủ các chuẩn của nó, nhưng yêu cầu việc tự nguyên tuân thủ. Dĩ nhiên, các nhà sản xuất và nhà phát triển được lợi từ việc tuân thủ này, do nó đảm bảo các hệ thống là đáng tin cậy và có thể tích hợp được với cơ sở hạ tầng đã có. Những thiết bị điện tử và những phương thức phải trải qua quá trình kiểm tra nghiêm ngặt để chứng minh rằng chúng đáng được ANSI chấp thuận.

ITU (International Telecommunication Union - Liên minh Viễn thông Quốc tế).

ITU là một cơ quan chuyên môn thuộc Liên hiệp quốc, quy định ngành viễn thông quốc tế, bao gồm tần số vô tuyến và radio, thông số vệ tinh và điện thoại, cơ sở hạ tầng mạng và mức thuế quan áp dụng đối với toàn ngành truyền thông. Nó cũng hỗ trợ về chuyên gia kỹ thuật và thiết bị cho các nước đang phát triển để thúc đẩy cơ sở công nghệ của những quốc gia này.

Các tài liệu của ITU thường liên quan nhiều tới các vấn đề viễn thông toàn cầu hơn là những thông số kỹ thuật công nghiệp. Tuy nhiên, ITU liên quan mật thiết với việc triển khai các dịch vụ Internet toàn cầu. Ở những lĩnh vực khác, ITU hợp tác với một số tổ chức tiêu chuẩn khác.

ISO (International Organization for Standardization - Tổ chức Quốc tế về tiêu chuẩn hóa)

ISO, trụ sở chính tại Geneva, Thụy Sỹ, là một tập hợp các tổ chức tiêu chuẩn đại diện cho 162 quốc gia. Mục tiêu của ISO là thiết lập các tiêu chuẩn kỹ thuật quốc tế để tạo điều kiện thuận lợi cho việc trao đổi thông tin và xóa bỏ rào cản thương mại toàn cầu. Trên thực tế, ISO là từ Hy Lạp với nghĩa là bình đẳng. Việc sử dụng thuật ngữ này truyền tải sự cống hiến của tổ chức trong việc đặt ra các tiêu chuẩn.

Quyền của ISO là không chỉ giới hạn trong ngành truyền thông và xử lý thông tin. Nó còn được áp dụng vào các ngành như dệt may, bao bì, phân phối hàng hóa, khai thác và sản xuất năng lượng, đóng tàu, các dịch vụ tài chính và ngân hàng. Các thỏa thuận toàn cầu về ren ốc vít, thẻ ngân hàng, và thậm chí là tên của các đồng tiền tệ đều là sản phẩm từ hoạt động của ISO. Trên thực tế, có ít hơn 3000 trong hơn 18500 tiêu chuẩn của ISO được áp dụng vào các sản phẩm và chức năng liên quan tới máy tính.

3.4 | MÔ HÌNH OSI

3.4.1 | GIỚI THIỆU MÔ HÌNH OSI

Mô hình tham chiếu cung cấp một sự tham chiếu chung cho việc duy trì tính ổn định của các giao thức và dịch vụ mạng. Nó cung cấp thông tin chi tiết và đầy đủ để định nghĩa chính xác những dịch vụ trong kiến trúc mạng. Mục đích chính của mô hình tham chiếu là làm minh bạch hơn những tính năng và tiến trình có liên quan. Mô hình OSI (Open Systems Interconnection) là mô hình tham chiếu liên

mạng được phổ biến rộng rãi nhất. Nó được sử dụng trong việc mô tả hoạt động của mạng, thiết kế mạng và chẩn đoán xử lý lỗi.

Để các máy tính và các thiết bị mạng có thể truyền thông với nhau, ví dụ như truyền file (FTP), truy cập trang web (HTTP) hay đăng nhập từ xa (Telnet),... chúng ta bắt buộc phải tuân theo những quy tắc chung gọi là giao thức (protocol). Từ những ngày đầu tiên của mạng máy tính, các tập đoàn lớn như IBM, Digital Equipment Corporation,... đã đưa ra các giao thức dành riêng cho thiết bị họ sản xuất. Kết quả của việc này là các thiêt bị thuộc các hãng khác nhau không thể giao tiếp được với nhau, gây bất lợi lớn trong truyền thông.

Năm 1977, tổ chức tiêu chuẩn quốc tế - ISO (International Standard Organization) đã đề xuất ra mô hình hệ thống mở - OSI (Open System Interconnection) nhằm quy định thống nhất và chi tiết các hoạt động của máy tính và thiết bị mạng trong khi truyền thông, giúp các nhà sản xuất chế tạo ra các thiết bị tương thích với nhau. Đến năm 1984, mô hình tham chiếu OSI gồm bảy lớp được công bố, mỗi lớp có một nhiệm vụ riêng biệt trong quá trình truyền thông. Bảy lớp đó gồm:

- Lớp ứng dụng (Application)
- Lớp trình bày (Presentation)
- Lớp phiên (Session)
- Lớp vận chuyển (Transport)
- Lớp mạng (Network)
- Lớp liên kết dữ liệu (Data Link)
- Lớp vật lý (Physical)

Hình 3.2: Mô hình OSI

Việc chia lớp của mô hình OSI có nhiều tác dụng, ví dụ mô hình OSI giúp đơn giản hóa việc tìm hiểu và phân tích mạng, chuẩn hóa các thành phần mạng để cho phép phát triển mạng từ nhiều nhà sản xuất và ngăn chặn tình trạng thay đổi của một lớp làm ảnh hưởng đến các lớp khác, giúp mỗi lớp có thể phát triển độc lập và nhanh chóng hơn.

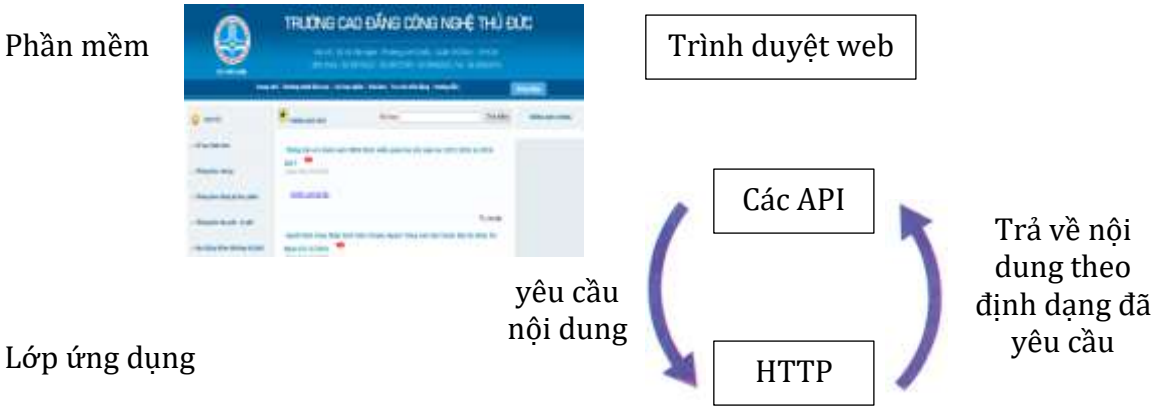
3.4.2 | TÍNH NĂNG CỦA MỖI LỚP TRONG MÔ HÌNH OSI

1. Lớp ứng dụng (Application Layer)

Lớp Application là lớp gần với người sử dụng nhất. Nó cung cấp phương tiện cho người dùng truy cập các thông tin và dữ liệu trên mạng thông qua các chương trình ứng dụng

Ví dụ, bạn chọn mở một trang web chẳn hạn online.tdc.edu.vn trên google chrome. Khi đó, API (Application programming interface – giao diện lập trình ứng dụng) của google chrome truyền yêu cầu của bạn tới giao thức HTTP. HTTP thúc đẩy các giao thức của lớp thấp hơn thiết lập kết nối giữa máy của bạn và Web server. Tiếp theo, HTTP định dạng yêu cầu gửi từ trang web và gửi nó đến Web server. Web server phản hồi gồm phần văn bản và phần hình ảnh tạo nên trang web, cộng thêm các đặc tả về nội dung chứa trong trang đó.

Sau khi nhận được phản hồi của web server, máy trạm sẽ sử dụng giao thức HTTP để thông dịch phản hồi này để google chrome có thể hiển thị trang web online.tdc.edu.vn theo định dạng mà bạn có thể nhận ra.



Hình 3.3: Chức năng của lớp Application khi truy xuất một trang web

2. Lớp trình bày (Presentation Layer)

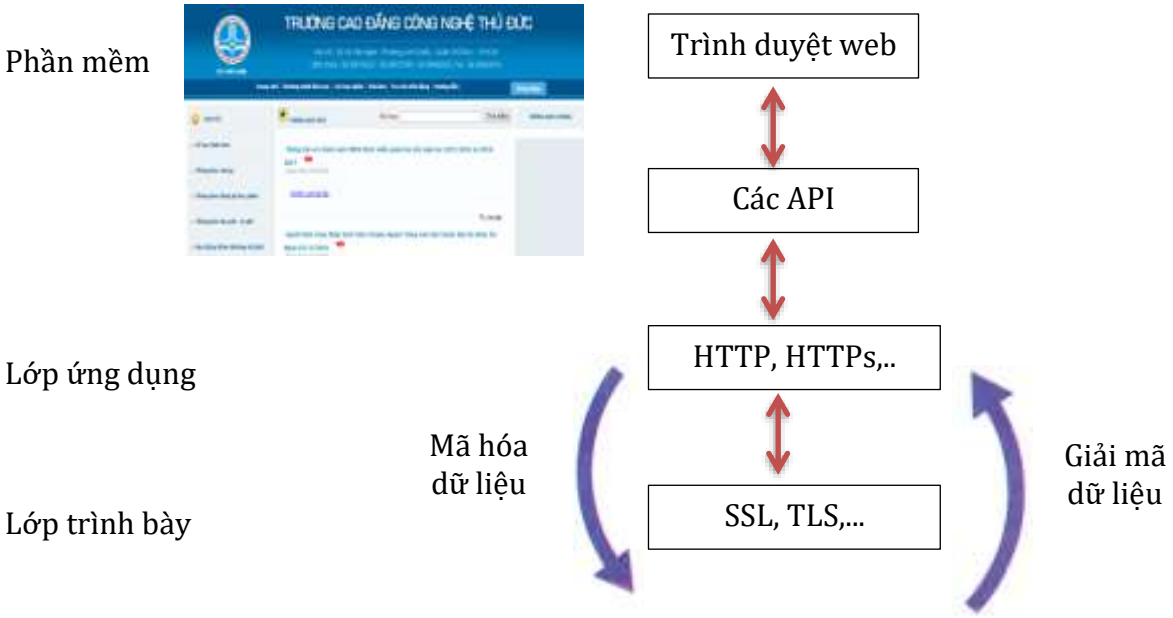
Lớp Presentation có các chức năng chính:

- Mã hóa và giải mã dữ liệu của lớp Application theo một kiểu định dạng chuẩn để đảm bảo rằng dữ liệu từ ứng dụng trên máy gửi có thể được hiểu bởi ứng dụng thích hợp trên máy nhận.

- Nén dữ liệu theo một kiểu nào đó mà thiết bị đích có thể giải nén được.

Trong đồ họa, những phương thức nén và mã hóa hình ảnh như GIF, JPG, TIF. MPEG và QuickTime là hai phương pháp nén và mã hóa dữ liệu âm thanh và video phổ biến. Ví dụ, định dạng âm thanh phổ biến MP3, sử dụng phương pháp nén MPEG. Nó có thể chuyển một ca khúc cần dung lượng đĩa CD 30MB vào một file không quá 3MB hay thậm chí nhỏ hơn nếu chấp nhận chất lượng thấp.

Những dịch vụ của lớp Presentation cũng quản lý việc mã hóa và giải mã dữ liệu. Ví dụ, đăng nhập vào trang online.tdc.edu.vn, bạn đang sử dụng một kết nối bảo mật, và các giao thức của lớp trình bày sẽ mã hóa dữ liệu tài khoản của bạn trước khi nó truyền đi. Bên nhận dữ liêu, lớp Presentation sẽ giải mã dữ liệu mà nó nhận được.



Hình 3.4: Các dịch vụ của lớp Presentation truy xuất một trang web bảo mật

3. Lớp phiên (Session Layer)

Như tên gọi của nó, tính năng của lớp này là tạo và duy trì những cuộc trao đổi giữa các ứng dụng nguồn và đích. Lớp session quản lý việc trao đổi thông tin về khởi tạo cuộc trao đổi, theo dõi chúng hoạt động và khởi tạo lại các session bị lỗi hoặc không hoạt động trong một thời gian dài.

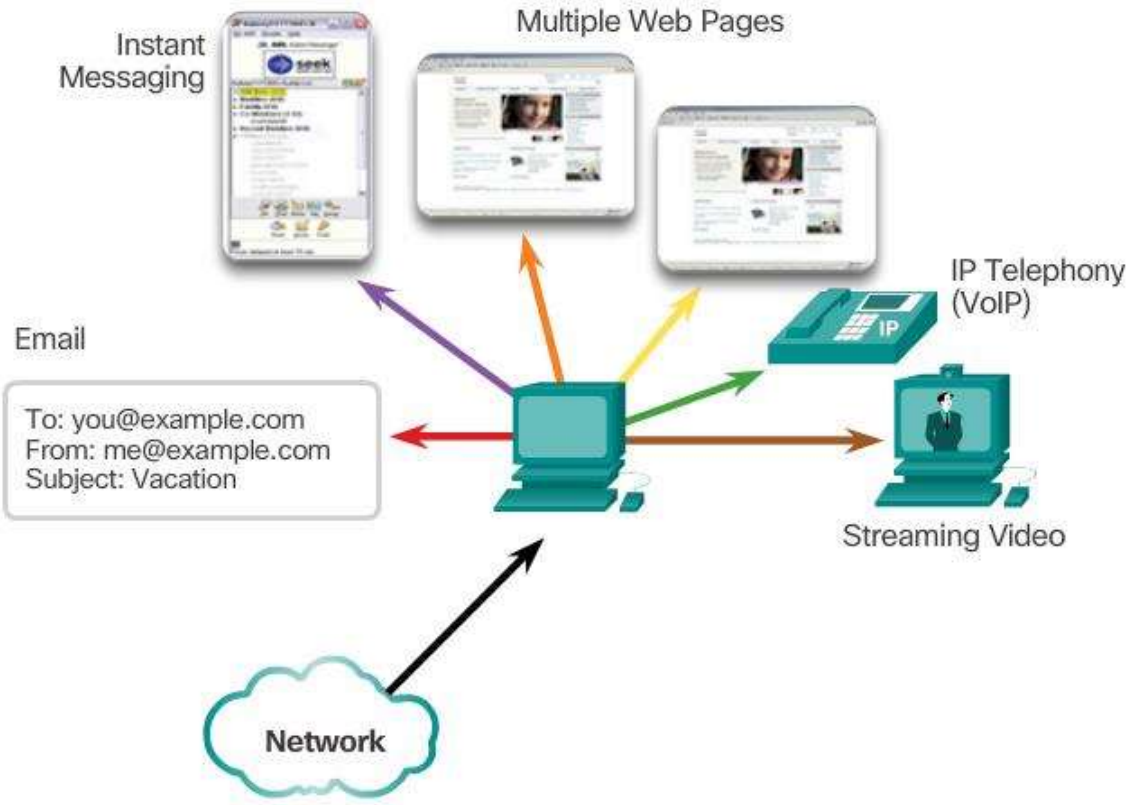
4. Lớp vận chuyển (Transport Layer)

Nhiệm vụ chính của lớp Transport:

- Theo dõi cuộc giao tiếp giữa các ứng dụng trên máy gửi và máy nhận
- Tại máy gửi, phân đoạn dữ liệu thành các segment và quản lý các segment này
- Tại máy nhận, sắp xếp các segment thành các chuỗi dữ liệu như ban đầu của ứng dụng
- Nhận dạng ứng dụng

Theo dõi các cuộc trao đổi riêng.

Như mô tả trên hình 4.5, bất kỳ máy tính nào cũng có thể mở nhiều ứng dụng để giao tiếp qua mạng. Mỗi ứng dụng này sẽ giao tiếp với một hay nhiều ứng dụng trên các máy tính ở xa. Ví dụ, tại một thời điểm bạn mở ra nhiều trình duyệt web và cùng truy cập đến một web site nào đó. Nhiệm vụ của lớp Transport là duy trì nhiều luồng truyền thông giữa các ứng dụng này.



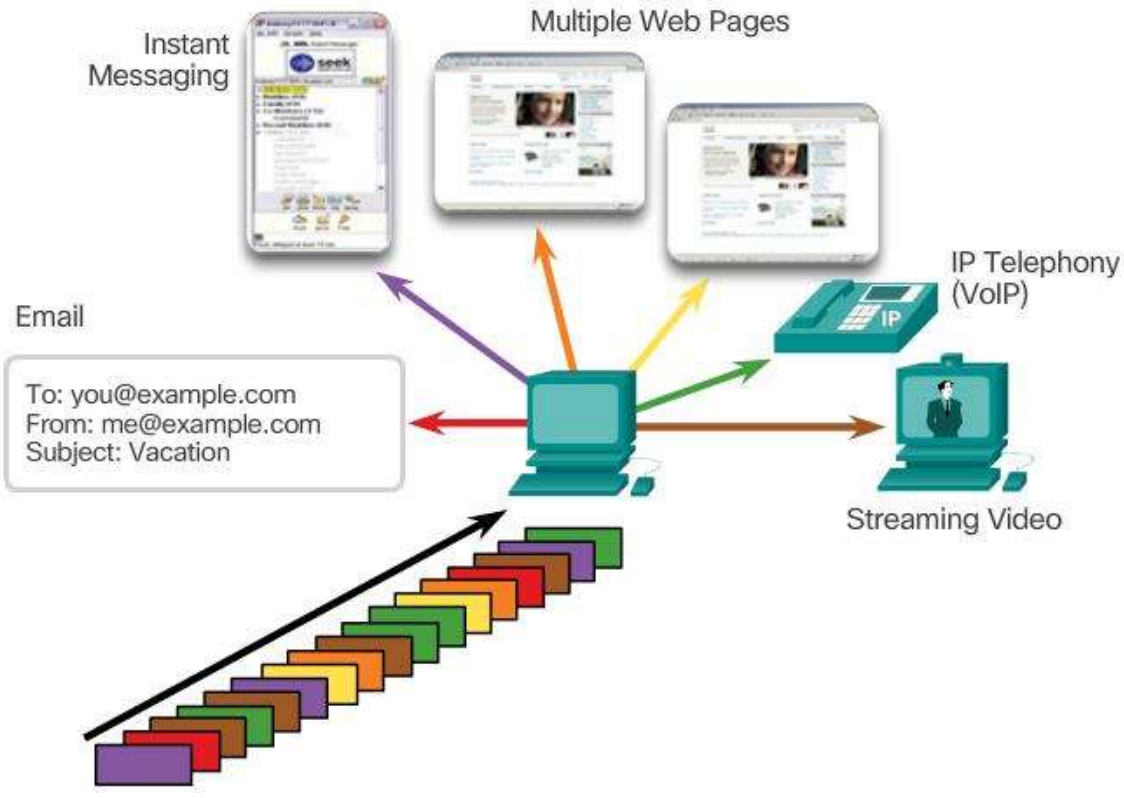
Hình 3.5: Theo dõi các cuộc trao đổi riêng

Phân đoạn dữ liệu

Tại máy gửi, dữ liệu của ứng dụng từ lớp Application được chuyển xuống lớp Transport. Các giao thức tại lớp Transport phân đoạn dữ liệu này thành các đoạn nhỏ hơn. Sau đó, gán thêm vào mỗi phân đoạn một header, đơn vị dữ liệu mới được gọi là segment. Header chứa đủ thông tin để giúp cho giao thức của lớp Transport hoàn thành được nhiệm vụ của nó. Tùy theo tính năng của mỗi giao thức mà thông tin trong header có thể phức tạp hay đơn giản. Nhưng nhìn chung trong header của các giao thức đều có:

- Port của ứng dụng nguồn.
- Port của ứng dụng đích.

Hai giao thức phổ biến của lớp Transport là TCP (Transmission Control Protocol) và UDP (User Datagram Protocol). Để phân biệt header của hai giao thức này ta gọi với tên TCP header và UDP Header.



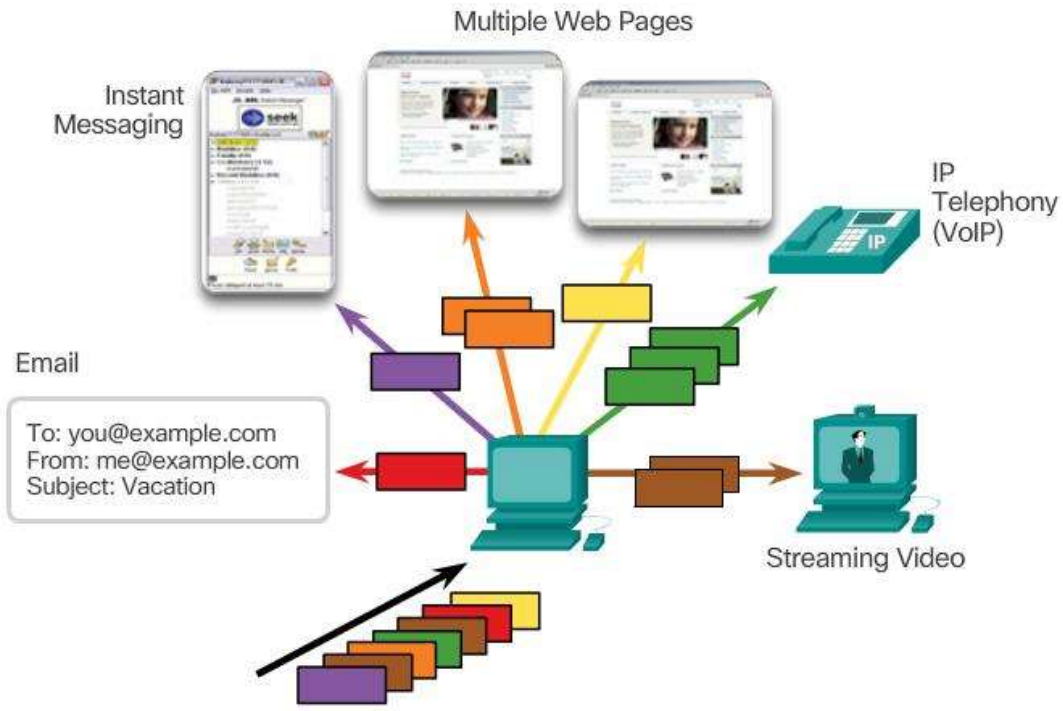
Hình 3.6: Phân đoạn dữ liệu

Sắp xếp lại segment

Nếu tại máy gửi giao thức tại lớp Transport đã đóng gói dữ liệu là giao thức TCP thì tại máy nhận giao thức TCP sẽ mở gói dữ liệu. Dựa vào thông tin của header lớp Transport có thể biết được dữ liệu này là của ứng dụng nào và sắp xếp chúng lại thành một chuỗi dữ liệu theo đúng trật tự ban đầu ở máy gửi. Sau đó, chuỗi dữ liệu này được gửi lên ứng dụng ở lớp Application.

Nhận dạng ứng dụng

Lớp Transport có nhiệm vụ vận chuyển dữ liệu giữa các ứng dụng cuối. Nó nhận dữ liệu từ các ứng dụng khác nhau ở lớp Application, phân đoạn, đóng gói thành các segment và chuyển chúng xuống lớp thấp hơn. Sau đó, chúng có thể được truyền trên nhiều đường khác nhau để đến máy nhận. Tại máy nhận, chúng được sắp xếp lại thành chuỗi dữ liệu ban đầu và chuyển đến đúng ứng dụng. Làm cách nào mà các giao thức tại lớp Transport chuyển dữ liệu đến đúng ứng dụng nhận nó. Để làm được điều này, lớp Transport gán cho mỗi ứng dụng ở lớp Application một con số và số này là duy nhất. Số này được gọi là port number. Ví dụ, dịch vụ HTTP có port 80 dịch vụ SMTP có port 110,v.v...Khi nhận dữ liệu, giao thức dựa vào thông tin port của ứng dụng đích trong header để chuyển đến đúng ứng dụng đích.



Hình 3.7: Nhận dạng ứng dụng

Các lớp thấp hơn không biết rằng có nhiều ứng dụng đang gửi dữ liệu trên mạng. Nhiệm vụ của chúng là nhận dữ liệu từ lớp Transport và phân phát chúng đến đúng thiết bị nhận mà không cần biết dữ liệu này là của ứng dụng nào. Việc đưa đến đúng ứng dụng đích trên thiết bị nhận là nhiệm vụ của lớp Transport.

TCP và UDP

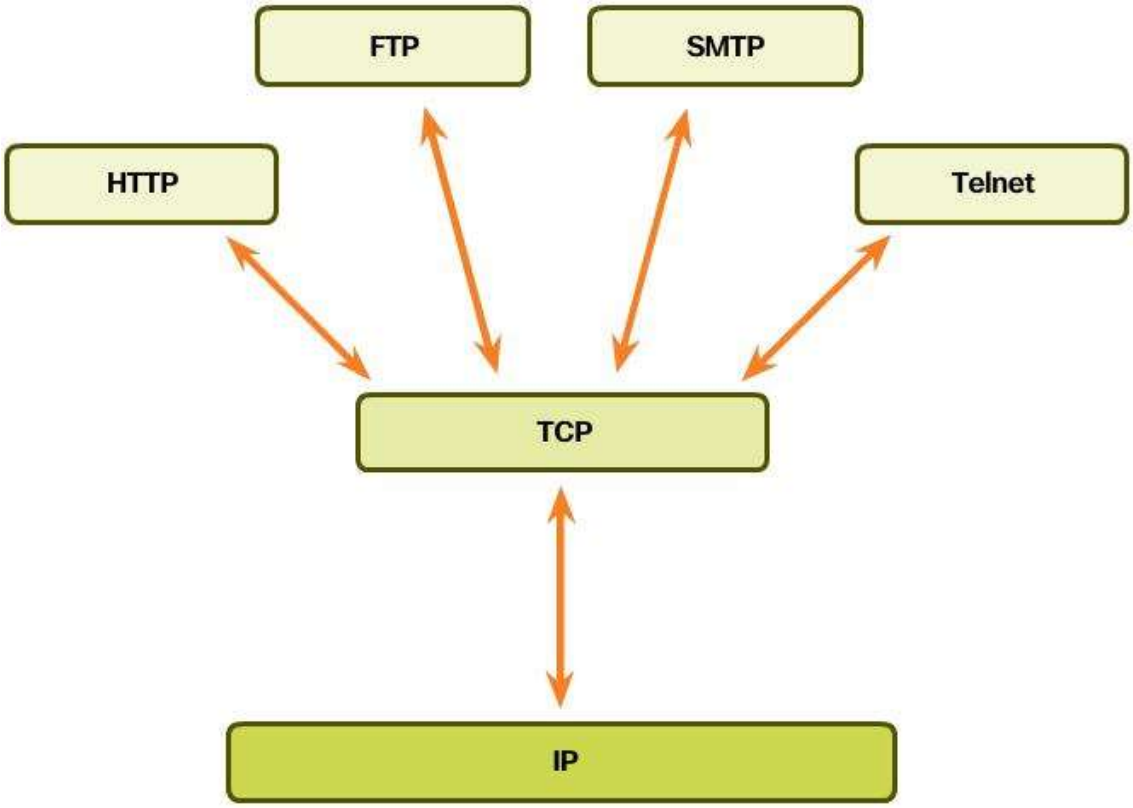
Hai giao thức phổ biến của họ giao thức TCP/IP tại lớp Transport là Transmission Control Protocol (TCP) và User Datagram Protocol (UDP). Cả hai giao thức này đều có nhiệm vụ là quản lý việc trao đổi dữ liệu giữa các ứng dụng. Sự khác nhau giữa hai giao thức này là tính năng của chúng: TCP là một giao thức tin cậy, còn UDP là một giao thức không tin cậy.

Transmission Control Protocol (TCP)

TCP là một giao thức hướng kết nối (oriented-connection), được mô tả trong RFC 793. Nó cung cấp một phương thức truyền dữ liệu song công hoàn toàn (full duplex) tin cậy. Đối với TCP, một kết nối phải được thiết lập trước khi một hoạt động truyền thông tin thực sự có thể bắt đầu. TCP chịu trách hiệm phân chia dữ liệu thành các segment, sắp xếp lại các segment thành dữ liệu ban đầu tại đích, truyền lại bất kỳ segment nào không thể nhận được. TCP cung cấp một mạch ảo giữa các ứng dụng. vì các tính năng trên, nên TCP phải phát sinh thêm thông tin điều khiển được trao đổi giữa các máy tính.

Các ứng dụng của TCP:

- Hypertext Transfer Protocol (HTTP).
- File Transfer Protocol (FTP).
- Simple Mail Transfer Protocol (SMTP).
- Telnet.
- v.v…



Hình 3.8: Các ứng dụng của TCP

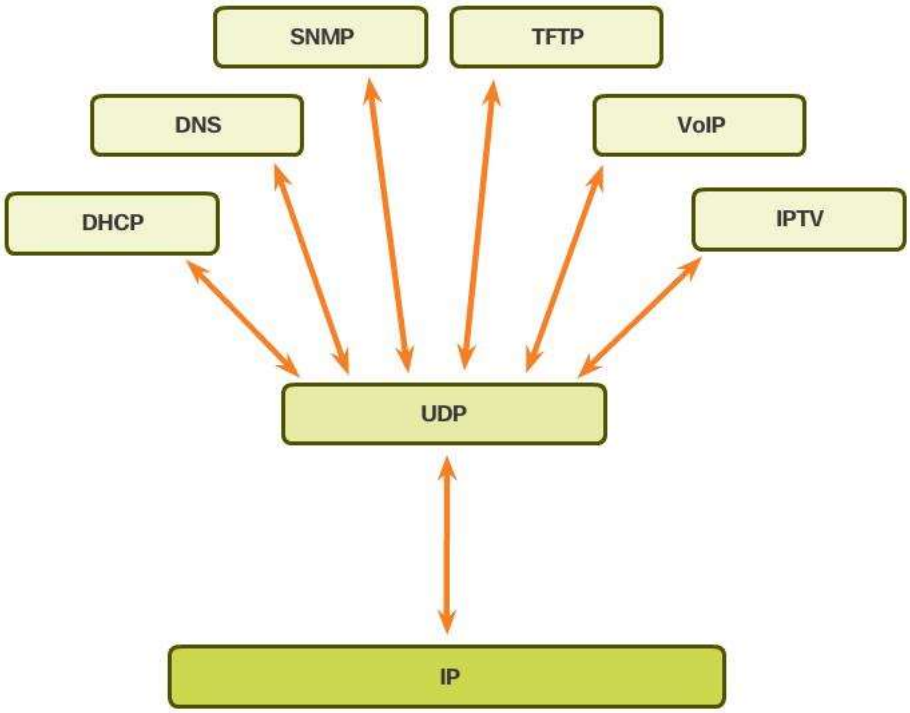
User Datagram Protocol (UDP)

UDP là một giao thức không kết nối (connectionless protocol). Nó là một giao thức đơn giản dùng để trao đổi các datagram mà không có báo nhận và cũng không có sự bảo đảm chuyển phát nào. Xử lý lỗi và truyền lại được giao phó cho giao thức lớp cao hơn. Nó truyền các datagram theo phương thức "best-effort". Do đó, ưu điểm của UDP là chi phí phân phối dữ liệu thấp. UDP được thiết kế cho các ứng dụng không cần sắp xếp lại các segment theo đúng thứ tự.

Các ứng dụng của UDP gồm:

- Dynamic Host Control Protocol (DHCP).
- Domain Name System (DNS).
- Simple Network Management Prorocol (SNMP).
- Trivial File Transfer Protocol (TFTP).
- Voice over IP (VoIP).

- Video streaming.
- v.v…



Hình 3.9: Các ứng dụng của UDP

5. Lớp mạng (Network Layer)

Mục đích của lớp Network là chọn đường đi tốt nhất để các gói dữ liệu (packet) di chuyển đến đích. Để hoàn thành nhiệm vụ này, lớp Network đưa ra 4 tiến trình cơ bản:

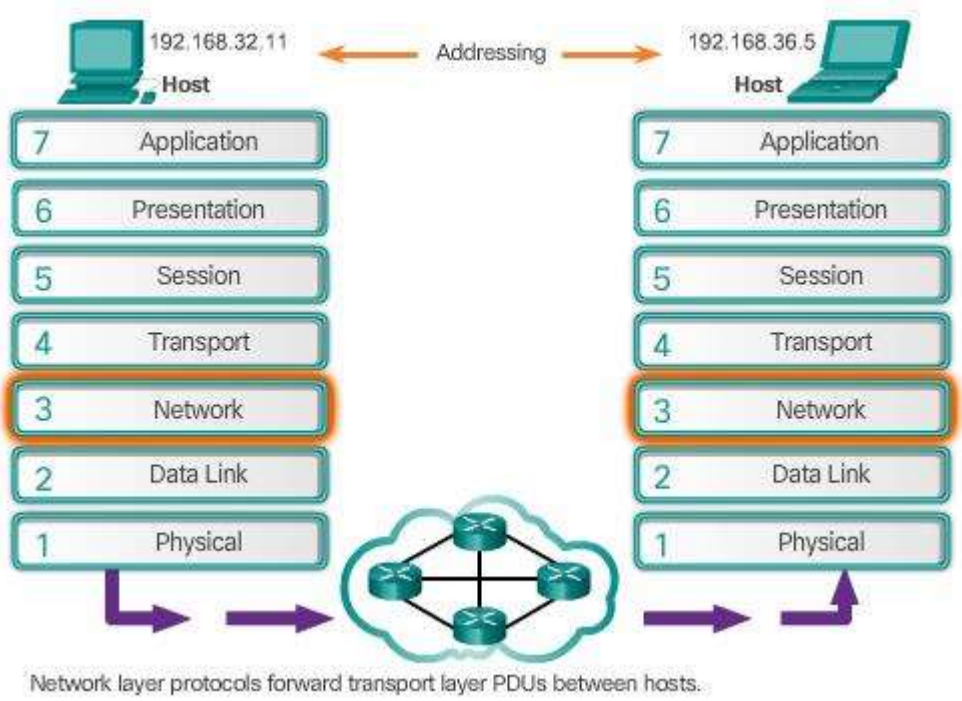
- Gán địa chỉ – Addressing
- Đóng gói – Encapsulation
- Định tuyến – Routing
- Mở gói – Decapsulation

Gán địa chỉ

Hai thiết bị giao tiếp với nhau có thể ở cùng một mạng hay ở hai mạng cách xa nhau. Làm sao nhận dạng được thiết bị này thuộc mạng nào để chuyển gói dữ liệu

đến đúng đích. Điều băn khoăn này đã được lớp Network giải quyết. Lớp Network cung cấp một cơ chế địa chỉ phân cấp để gán địa chỉ cho các thiết bị trong mạng. Địa chỉ này là địa chỉ duy nhất được dùng để nhận dạng thiết bị thuộc mạng nào. Nó bao gồm hai phần: phần mạng và phần host. Phần mạng được dùng để nhận dạng mạng, còn phần host được dùng để nhận dạng các thiết bị trên một mạng.

Ví dụ chúng ta có hai mạng A và B. Các thiết bị trong mỗi mạng được đánh số là A1, A2,… và B1, B2,…Chúng ta nói A, B là địa chỉ mạng, còn các số thứ tự 1, 2,..là địa chỉ máy.



Hình 3.10: Lớp Network

Lớp Network có nhiều giao thức, nhưng giao thức phổ biến nhất được sử dụng trên mạng Internet ngày nay là giao thức Internet Protocol, được viết tắt là IP. Hiện nay giao thức IP có hai phiên bản 4 và 6, phiên bản chúng ta đang đề cập lúc này là phiên bản 4 gọi tắt là IPv4. IP là giao thức trong họ giao thức TCP/IP. Khi sử dụng họ giao thức này, mỗi thiết bị hay máy tính trên mạng phải được gán một địa chỉ IP

Đóng gói

Tiến trình thứ hai của lớp Network là nhận các segment/datagram của lớp Transport chuyển xuống, thêm header vào và đóng gói thành các packet. Packet

chính là đơn vị dữ liệu của lớp Network. Trong header có nhiều thông tin, trong đó có hai cột: địa chỉ nguồn (Source IP Address) và địa chỉ đích (Destination IP Address). Hai địa chỉ này chính là các địa chỉ IP mà bạn đã gán cho thiết bị. Địa chỉ nguồn là địa chỉ của máy gửi, còn địa chỉ IP đích là địa chỉ của máy mà bạn muốn gửi dữ liệu đến.

Sau khi lớp Network hoàn thành tiến trình đóng gói, packet được chuyển xuống lớp Data Link để chuẩn bị truyền trên môi trường truyền.

Định tuyến

Kế tiếp, lớp Netwok phải cung cấp các dịch vụ để chuyển các packet đến mạng đích. Không phải lúc nào máy gửi và máy nhận cũng đều ở cùng một mạng. Để đi từ máy gửi đến máy nhận có thể chúng đi ngang qua rất nhiều mạng trung gian hay router. Router là thiết bị mạng trung gian nối các mạng khác nhau lại. Nó được gọi là các bộ định tuyến. Nó có nhiệm vụ trao đổi, thu thập thông tin đường đi với nhau để từ đó chọn được đường đi tốt nhất và chuyển packet trên đường đi đó. Quá trình này được gọi là quá trình định tuyến (routing).

Mỗi router mà packet phải đi qua để đến được đích được gọi là hop. Khi packet được chuyển qua các hop, nội dung của nó (PDU của lớp Transport) vẫn không bị thay đổi cho tới khi đến được máy nhận.

Mở gói

Cuối cùng, lớp Network trên máy đích nhận được gói dữ liệu. Nó đọc thông tin trong header và kiểm tra xem địa chỉ đích có phải là địa chỉ của máy này không. Nếu đúng vậy, lớp Network sẽ lấy header ra để còn lại PDU và chuyển nó lên lớp Transport.

Mỗi lớp trong mô hình OSI thực hiện một nhiệm vụ riêng biệt. Nếu như lớp Transport thực hiện việc vận chuyển dữ liệu giữa các tiến trình đang chạy trên các thiết bị cuối, thì các giao thức ở lớp Network chỉ ra cấu trúc của packet và quá trình mang dữ liệu từ một thiết bị này đến một thiết bị khác. Thao tác này không liên quan đến dữ liệu của ứng dụng mạng trong mỗi packet. Vì thế, các packet có thể mang nhiều loại dữ liệu của nhiều cuộc giao tiếp giữa các thiết bị.

Các giao thức của lớp Network:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

Trong đó IPv4 và IPv6 là giao thức được sử dụng rộng rãi nhất.

6. Lớp liên kết dữ liệu (Data Link Layer)

Cung cấp các phương pháp để trao đổi dữ liệu trên môi trường truyền cục bộ. Nó thực hiện hai nhiệm vụ cơ bản:

- Cho phép các lớp trên truy cập môi trường truyền bằng các kỹ thuật như framing
- Điều khiển cách thức dữ liệu được đặt vào môi trường truyền và được nhận từ môi trường truyền bằng các kỹ thuật điều khiển truy cập môi trường truyền và phát hiện lỗi.

Một số thuật ngữ thường dùng của lớp Data link:

- Frame – là một đơn vị dữ liệu giao thức (PDU) của lớp Data link
- Node – một node là một thiết bị trên mạng
- Media/medium – phương tiện vật lý trể mạng thông tin giữa hai node

Lớp cao hơn truy cập môi trường truyền

Các lớp trong mô hình OSI có một sự hỗ tương cho nhau. Trên tinh thần đó, lớp Data Link giúp đỡ các lớp trên bằng cách nhận dữ liệu từ lớp trên, sau đó đặt chúng vào môi trường truyền và ngược lại. Tùy vào mỗi loại môi trường truyền mà tiến trình thực hiện này của lớp Data Link sẽ khác nhau.

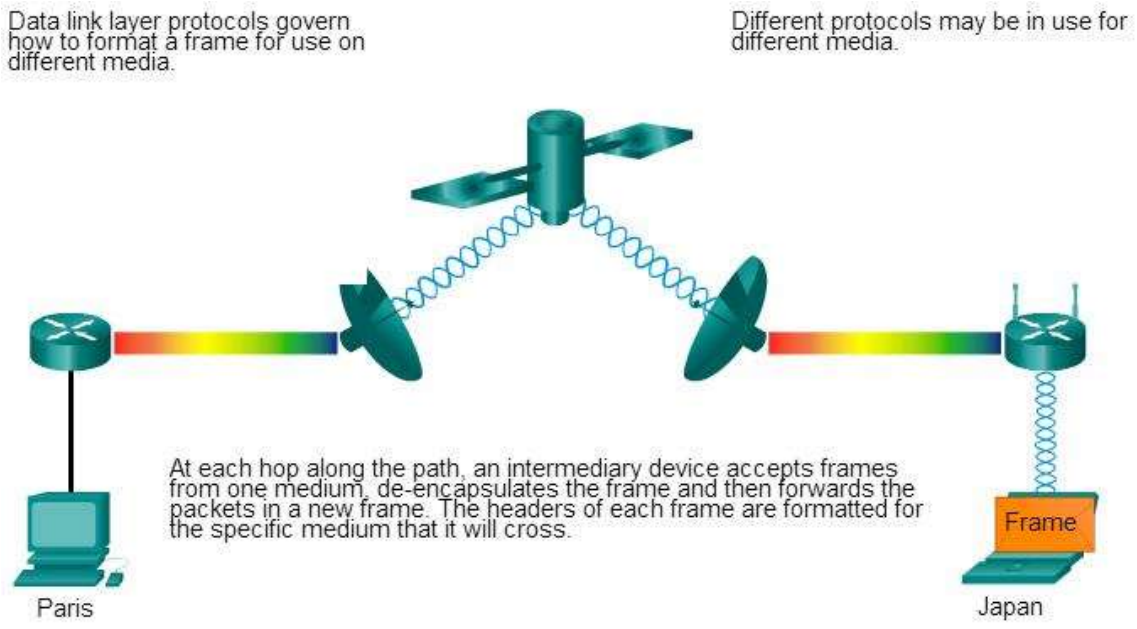
Trong bất kỳ một cuộc trao đổi packet nào của lớp Network, có thể có nhiều vị trí chuyển tiếp giữa các media và lớp Data Link. Tại mỗi hop thuộc đường đi, một thiết bị trung gian – thường là router – nhận các frame từ một media, mở frame

và sau đó chuyển tiếp packet trong một frame mới thích hợp với media của đoạn mạng vật lý này.

Tưởng tượng có một cuộc trao đổi dữ liệu giữa hai máy rất xa nhau, chẳn hạn một PC ở Paris với một server ở Japan. Mặc dù hai máy này giao tiếp với nhau thông qua các giao thức lớp Network (ví dụ IP), nhưng các giao thức ở lớp Data link được sử dụng để vận chuyển các packet IP qua rất nhiều loại LAN và WAN khác nhau. Các packet được trao đổi giữa hai thiết bị đòi hỏi các giao thức đa dạng ở lớp Data link. Một vị trí chuyển tiếp tại router có thể cần một giao thức lớp Data link khác để vận chuyển packet vào một môi trường truyền (media) mới.

Hình 4.11, bạn có thể thấy rằng mỗi liên kết giữa các thiết bị sử dụng một môi trường truyền khác nhau. Giữa PC và router là Ethernet, các router được kết nối qua vệ tinh, và máy laptop được kết nối tới router cuối cùng qua wireless.

Trong ví dụ này, khi một IP packet di chuyển từ PC đến laptop, packet này được đóng gói thành các Ethernet frame, mở gói, xử lý và lại đóng gói thành một frame mới để truyền vào môi trường truyền vệ tinh. Ở liên kết cuối, sử dụng wireless để di chuyển packet từ router đến laptop.



Hình 3.11: Lớp Data link

Lớp Data link tách rời các tiến trình giao tiếp tại các lớp cao hơn ra khỏi những thay đổi của môi trường truyền khi di chuyển packet từ đầu này đến đầu kia. Khi

nhận được một packet, nó sẽ chuyển trực tiếp đến một giao thức của lớp trên, trong trường hợp này là IPv4 hoặc IPv6 của lớp trên, giao thức này không cần biết rằng cuộc giao tiếp sẽ sử dụng môi trường truyền nào.

Không có lớp Data link, một giao thức của lớp network, như IP, sẽ phải tự kết nối đến mỗi loại media có thể tồn tại trên đường vận chuyển. Hơn nữa, IP phải tự điều chỉnh mỗi khi một kỹ thuật mạng hay media được phát triển. Tiến trình này sẽ làm cản trở sự đổi mới và phát triển của giao thức và media.

Điều khiển việc vận chuyển trong môi trường truyền cục bộ

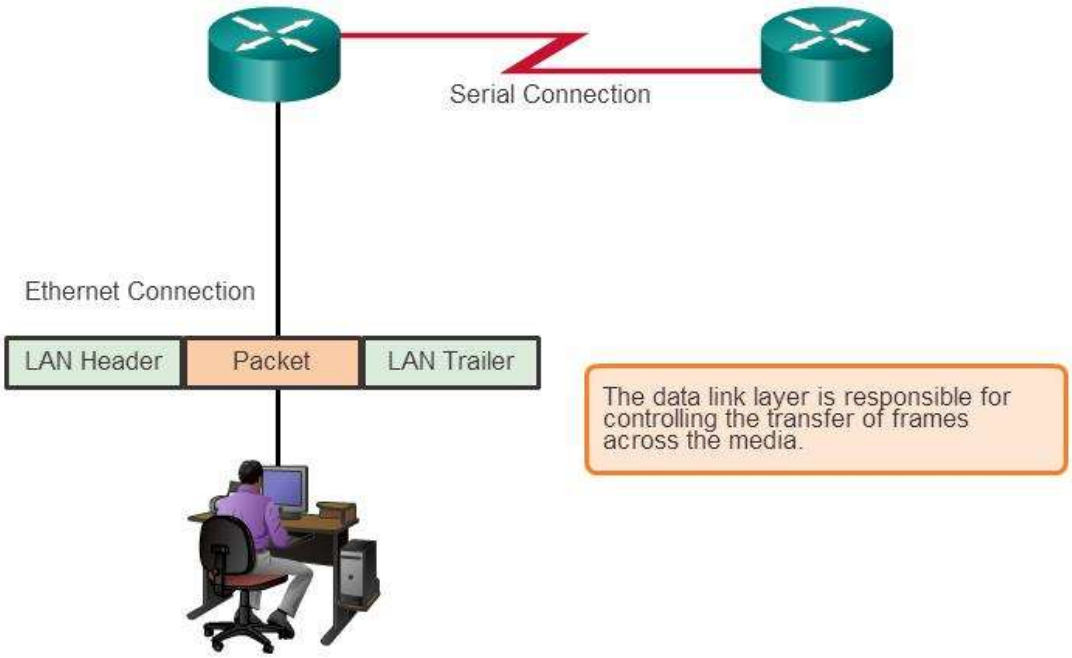
Các giao thức ở lớp 2 chỉ ra cách đóng gói một packet thành một frame và các kỹ thuật để truyền một packet đã được đóng gói vào và ra ở mỗi môi trường truyền. Kỹ thuật được dùng để truyền một frame vào và ra môi trường truyền được gọi là phương pháp điều khiển truy cập môi trường truyền (media access control). Để dữ liệu được truyền qua một số loại môi trường truyền khác nhau, phải có nhiều phương pháp điều khiển truy cập môi trường truyền khác nhau trong suốt quá trình trao đổi này.

Các giao thức lớp Data link mô tả các phương pháp điều khiển truy cập môi trường truyền bằng cách định nghĩa các tiến trình mà theo đó thiết bị mạng nào có thể truy cập môi trường truyền và truyền các frame.

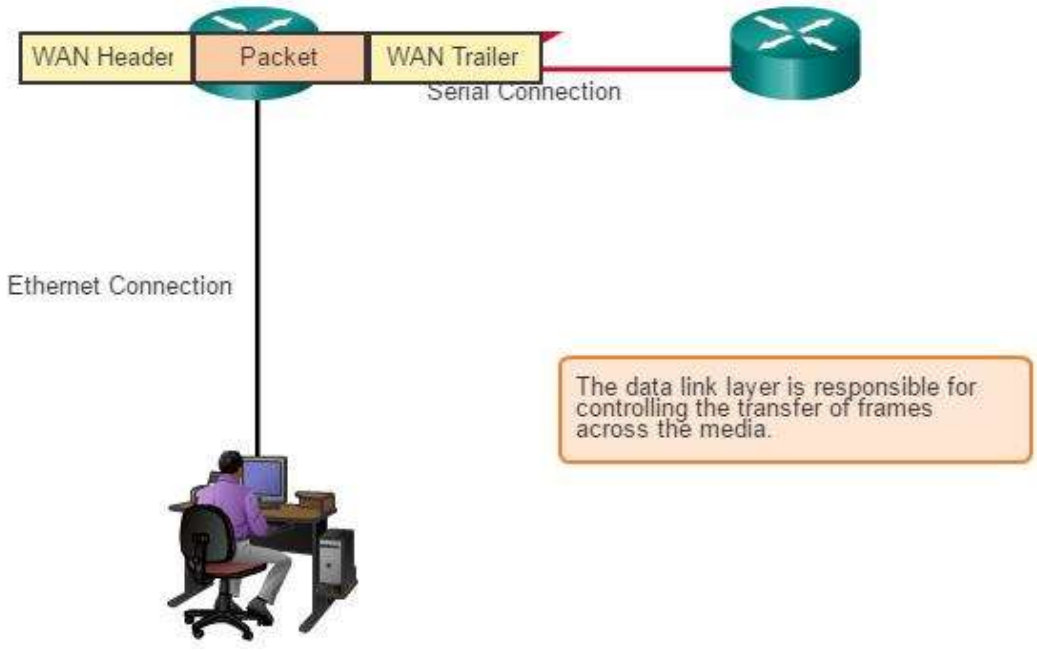
Một node là thiết bị cuối sử dụng card mạng dùng bộ điều hợp (adapter) để tạo kết nối đến mạng. Ví dụ, để kết nối đến một LAN, thiết bị sẽ dùng là một NIC phù hợp để kết nối đến môi trường truyền. Adapter quản lý việc định khung (framing) và điều khiển truy cập môi trường truyền.

Tại các thiết bị trung gian như router, mỗi mạng kết nối vào mỗi interface của router có thể có các môi trường truyền khác nhau. Các interface của router sẽ đóng gói packet thành frame thích hợp và một phương pháp điều khiển truy cập môi trường truyền thích hợp được dùng để truy cập mỗi đường liên kết. Router trong hình 4.12 trên có một cổng Ethernet để kết nối đến LAN và một cổng serial để kết nối đến WAN. Khi router xử lý các frame, nó sẽ dùng các dịch vụ của lớp Data link để nhận frame từ một môi trường truyền, mở nó ra thành PDU lớp 3, đóng gói lại PDU lớp 3 thành một frame mới và đặt frame vào môi trường tuyền của mạng kế tiếp.

Hình 4.12 và hình 4.13 cho bạn biết cách đóng gói một packet thành frame khi thay đổi môi tường truyền từ LAN sang WAN.



Hình 3.12: Truyền các frame



Hình 3.13: Truyền các frame

Tạo frame

Mô tả frame là nhiệm vụ chính của mỗi giao thức ở lớp Data link. Các giao thức ở lớp Data link cần các thông tin điều khiển để có thể hoạt động.

Các thông tin điều khiển này cho biết:

- Node nào đang giao tiếp với node nào.
- Giao tiếp giữa các node bắt đầu khi nào và kết thúc khi nào.
- Những lỗi nào đã xảy ra trong lúc các node đang giao tiếp.
- Những node nào sẽ giao tiếp kế tiếp.

Data link chuẩn bị một packet để truyền qua môi trường truyền cục bộ bằng cách đóng gói nó với một header và một trailer để tạo thành một frame.

Hình 3.14: Cấu trúc frame

Không giống với những PDU của các lớp khác, frame của Data link gồm:

- Data –packet từ lớp Network.
- Header – chứa thông tin điều khiển như địa chỉ và được đặt ở đầu PDU.
- Trailer – chứa thông tin điều khiển và được gán ở cuối PDU.

Các lớp con của lớp Data link

Để hỗ trợ nhiều tính năng khác nhau, lớp Data link được chia ra thành hai lớp con:

- **Logical Link Control (LLC):**

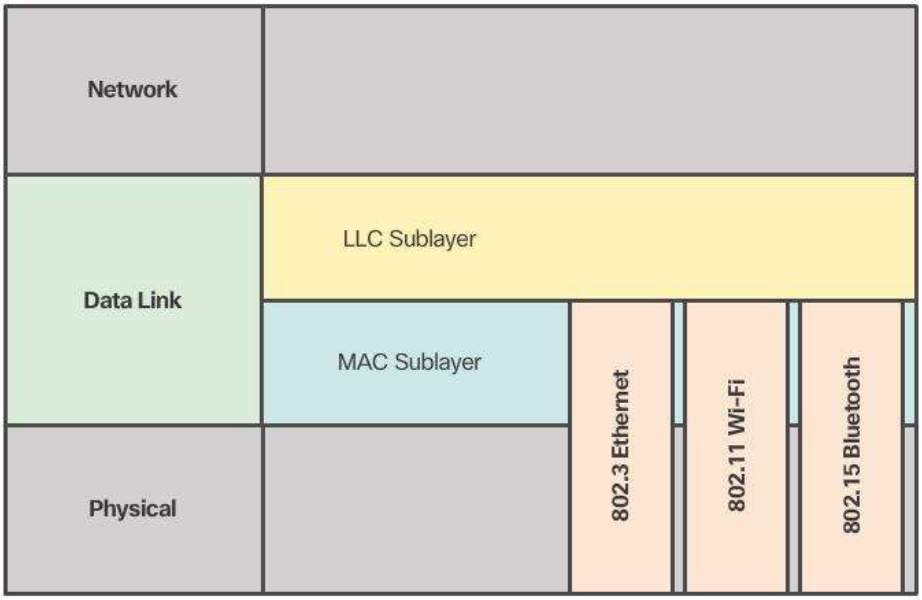
LLC định nghĩa các tiến trình phần mềm ma chúng cung cấp các dịch vụ cho các giao thức ở lớp Network.

LLC nhận dạng giao thức nào đang dùng ở lớp Network và đặt thông tin đó vào trong frame. Thông tin này cho phép nhiều giao thức ở lớp 3, như IP và IPX, sử dụng cùng NIC và media.

- **Media Access Control (MAC):**

MAC định nghĩa các tiến trình truy cập môi trường truyền được thực hiện bởi phần cứng.

MAC cung cấp việc đánh địa chỉ lớp Data link và định ranh giới của dữ liệu theo các yêu cầu về tín hiệu vật lý của môi trường truyền và loại giao thức ở lớp Data link đang được dùng.



Hình 3.15: Các lớp con của lớp Data link

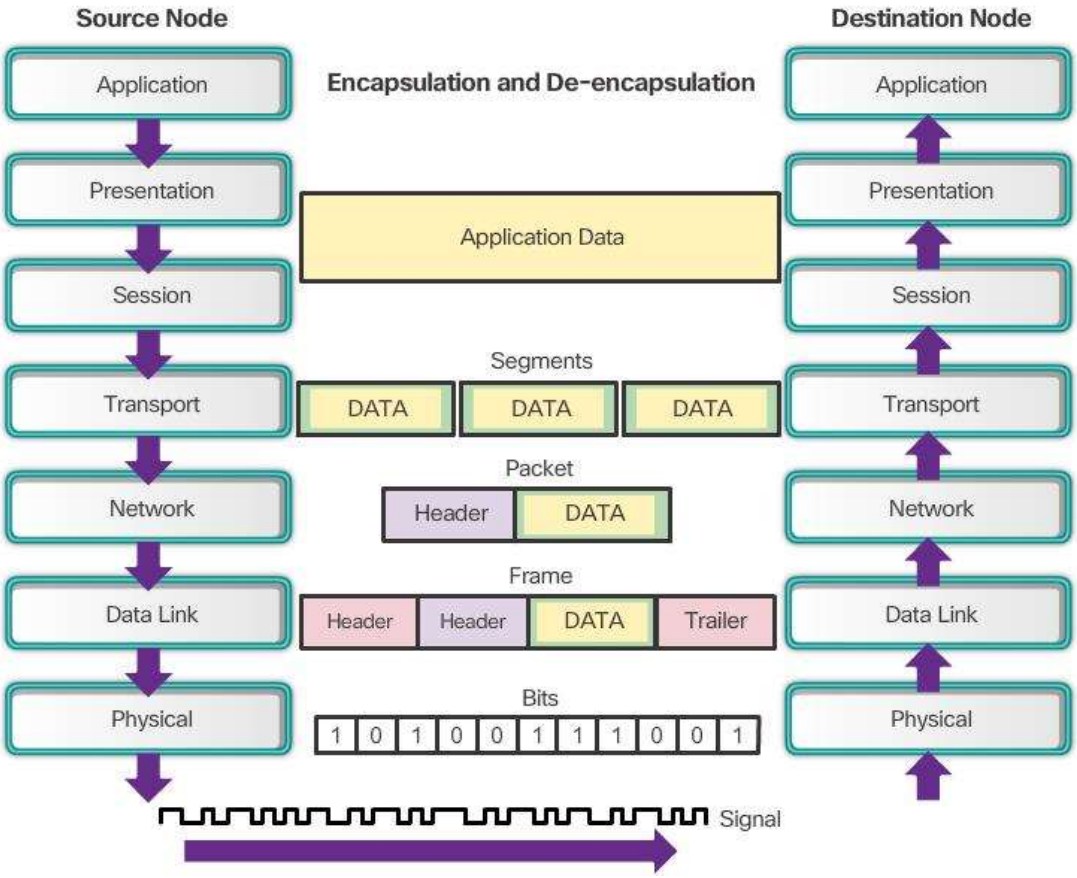
7. Lớp vật lý (Physical)

Mục đích của lớp Physical

Lớp Physical cung cấp các phương tiện để vận chuyển các bit từ lớp Data link qua môi trường truyền. Lớp này nhận một frame hoàn chỉnh từ lớp Data link và mã hóa nó thành một chuỗi các tín hiệu truyền vào môi trường truyền cục bộ.

Tính đến giai đoạn này của tiến trình truyền thông, lớp Transport đã phân đoạn dữ liệu của người dùng, lớp Network đóng gói thành packet và lớp Data link đóng gói thành frame. Mục đích của lớp Physical là tạo tín hiệu điện, quang hoặc vô tuyến để biểu diễn các bit của mỗi frame. Sau đó, những tín hiệu này được gửi lên môi trường truyền.

Lớp Physical có nhiệm vụ nhận các tín hiệu này từ môi trường truyền, tái tạo chúng thành các bit và chuyển các bit lên lớp Data Link như một frame hoàn chỉnh.



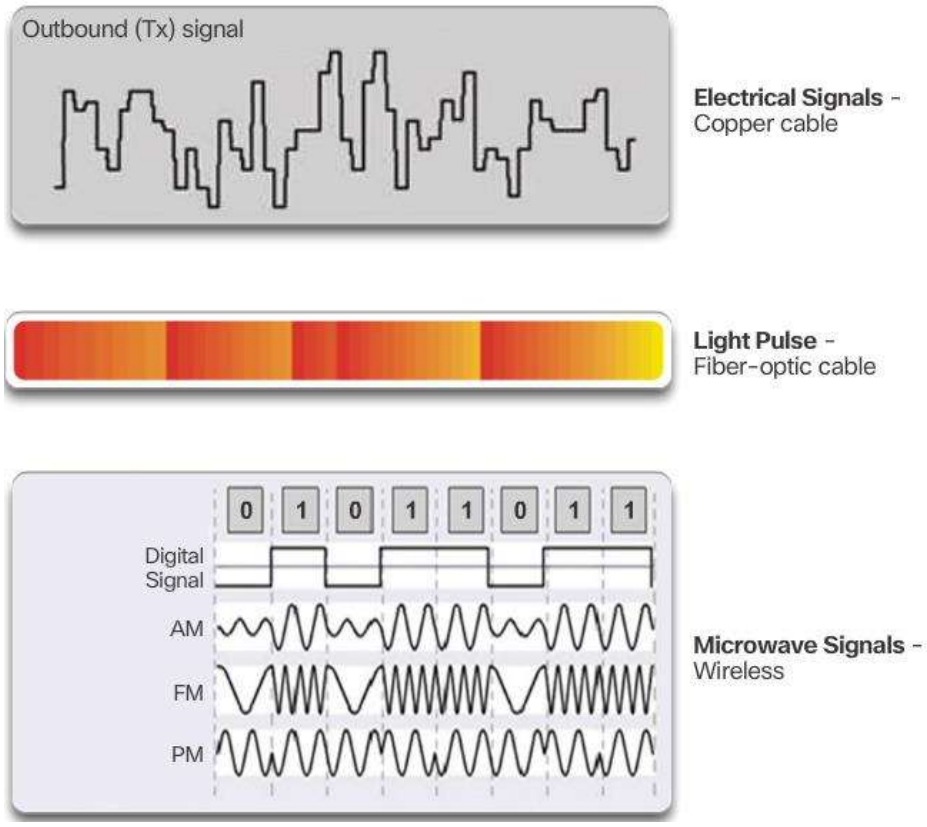
Hình 3.16: Biến đổi giao tiếp mạng thành các bit

Hoạt động của lớp Physical

Môi trường truyền không mang frame như là một thực thể đơn lẻ. Môi trường truyền mang các tín hiệu biểu diễn các bit của frame.

Có ba loại môi trường truyền cơ bản:

- Cáp đồng
- Cáp quang
- Sóng vô tuyến (wireless)



Hình 3.17:Biểu diễn các tín hiệu trên môi trường vật lý

3.5 | MÔ HÌNH TCP/IP

3.5.1 | GIỚI THIỆU MÔ HÌNH TCP/IP

Mạng Internet hiện đang sử dụng mô hình TCP/IP để quản lý việc truyền thông. TCP/IP được xem là giản lược của mô hình OSI với bốn lớp sau:

- Lớp Application (tích hợp 3 lớp trên cùng của mô hình OSI)
- Lớp Transport (tương ứng với lớp Transport của OSI)
- Lớp Internet (tương ứng với lớp Netwwork nhưng chỉ sử dụng giao thức IP để đánh địa chỉ logic cho các máy tính)
- Lớp Network Access (bao gồm hai lớp dưới cùng của mô hình OSI)

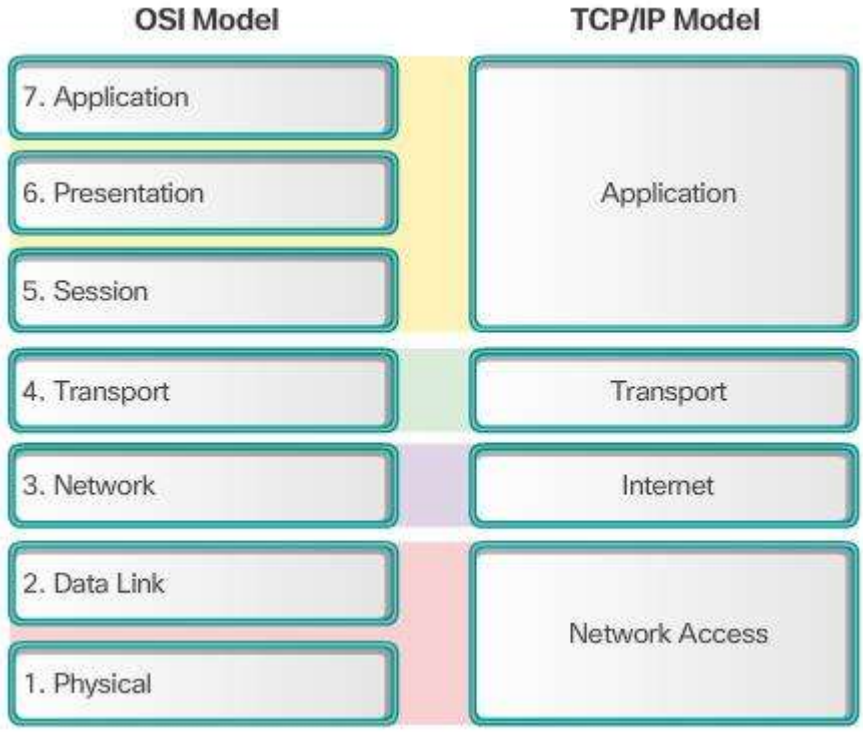
Do đó, tính năng của mỗi lớp trong mô hình TCP/IP chính là những tính năng của mỗi lớp trong mô hình OSI.

Một số giao thức thường gặp trong mô hình TCP/IP: IP, ICMP, TCP, UDP, Telnet, FTP, WWW, SMTP,...

Giao thức quan trọng nhất của mô hình TCP/IP là TCP và UDP.

TCP đảm bảo độ tin cậy truyền thong bằng cách ép buộc máy nhận phải thông báo cho máy gửi biết về những segment nào nhận được, segment nào bị lỗi,... để máy gửi tiếp tục truyền segment mới hay gửi lại segment bị lỗi. Các gói tin báo nhận này gọi tắt là ACK (Aclnowledgment). Nếu đường truyền bị lỗi quá nặng, các gói tin báo nhận này không đến được máy gửi thì sau một khoảng thời gian quy định, segment sẽ được gửi lại và nếu một segment được truyền lại quá nhiều lần, TCP sẽ ngắt kết nối với máy nhận và dừng việc truyền lại.

UDP không có cơ chế tin cậy (báo nhận bằng ACK), nên việc kiểm soát độ tin cậy phải do lớp Application đảm nhận. Tuy nhiên, với các ứng dụng yêu cầu tốc độ nhanh và chấp nhận tỷ lệ lỗi ở mức nào đó, sử dụng giao thức UDP là rất thích hợp do không phải báo nhận ACK nhiều lần. Việc linh động sử dụng giao thức TCP hay UDP trong các ứng dụng mạng phụ thuộc vào nhiều yếu tố như chất lượng đường truyền, tầm quan trọng của thông tin cần truyền,...



Hình 3.18: Mô hình OSI và Mô hình TCP/IP

3.5.2 | TÍNH NĂNG CỦA CÁC LỚP TRONG MÔ HÌNH TCP/IP

Lớp ứng dụng (Application Layer)

Lớp Application kiểm soát các giao thức lớp cao, các chủ đề về trình bày, biểu diễn thông tin, mã hóa và điều khiển hội thoại. Bộ giao thức TCP/IP tổ hợp tất cả các ứng dụng liên quan đến các chủ đề vào trong một lớp và đảm bảo số liệu này được đóng gói thích hợp trước khi chuyển nó đến lớp kế tiếp. Các giao thức hoạt động tại lớp Application: FTP, TFTP, SMTP, Telnet, SNMP, DNS,...

Lớp vận chuyển (Transport Layer)

Lớp Transport cung ứng dịch vụ vận chuyển từ host nguồn đến host đích. Lớp Transport thiết lập cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận. Giao thức hoạt động ở lớp Transport là giao thức TCP và UDP.

Lớp Internet

Mục đích của lớp Internet là chọn đường đi tốt nhất để chuyển các gói đến đích. Giao thức chính hoạt động ở lớp này là Internet Protocol (IP).

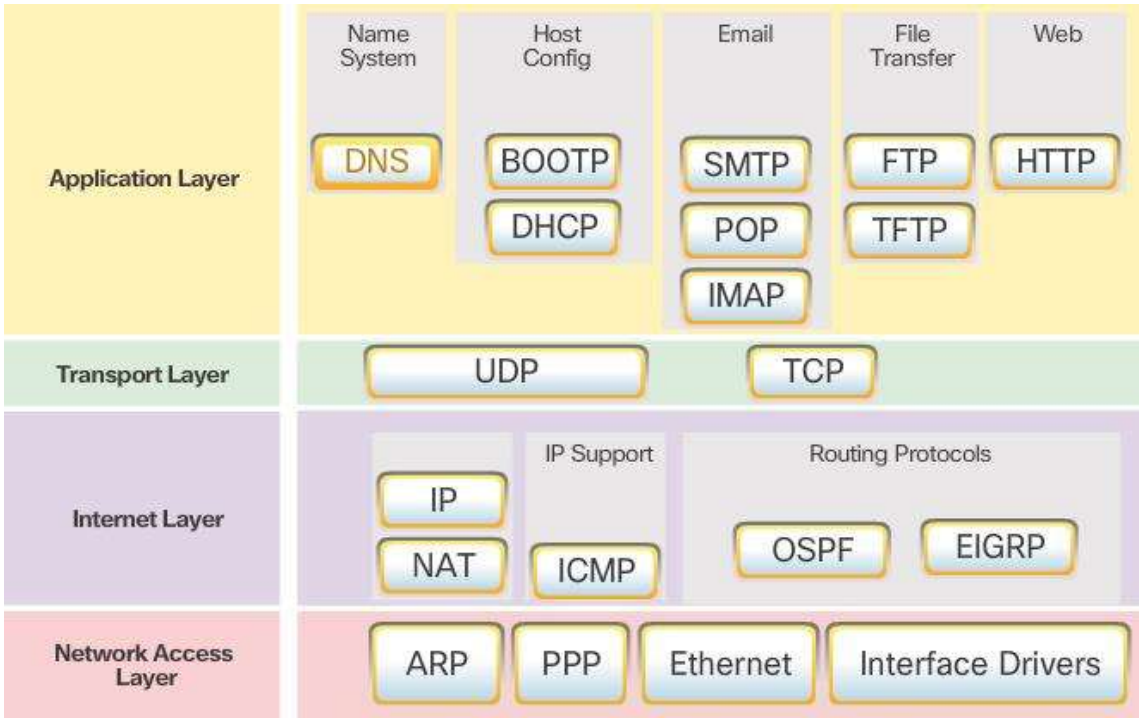
Các giao thức hoạt động tại lớp Intenet của mô hình TCP/IP:

- IP cung cấp connectionless, định tuyến chuyển gói theo best-effort, IP không quan tâm đến nội dung của các gói nhưng tìm kiếm đường đi tốt nhất để chuyển gói đến đích.
- ICMP (Internet Control Mesage Protocol): điều khiển và chuyển tiếp thông tin.
- ARP (Address Resolution Protocol): xác định điạc chỉ MAC khi biết địa chỉ IP.
- RARP (Reverse Address Resolution Protocol): xác định địa chỉ IP khi biết địa chỉ MAC.

Lớp truy cập mạng (Network Access Layer)

Lớp này liên quan đến chủ đề mà gói IP cần để tạo ra một liên kết vật lý đến môi trường truyền của mạng. Các chức năng của lớp Network Access bao gồm ánh xạ địa chỉ IP sang địa chỉ MAC, đóng gói các gói IP thành các frame. Căn cứ vào dạng

phần cứng và giao tiếp mạng, lớp Network Access sẽ xác lập kết nối với đường truyền vật lý của mạng.



Hình 3.19: Bộ giao thức TCP/IP

3.5.3 | QUÁ TRÌNH TRUYỀN THÔNG

Mô hình TCP/IP mô tả tính năng của các giao thức trong họ giao thức TCP/IP. Những giao thức này được cài đặt trên cả máy gửi và máy nhận, chúng tương tác với nhau để truyền tải dữ liệu giữa các ứng dụng trên mạng.

Một quá trình truyền hoàn chỉnh gồm những bước sau:

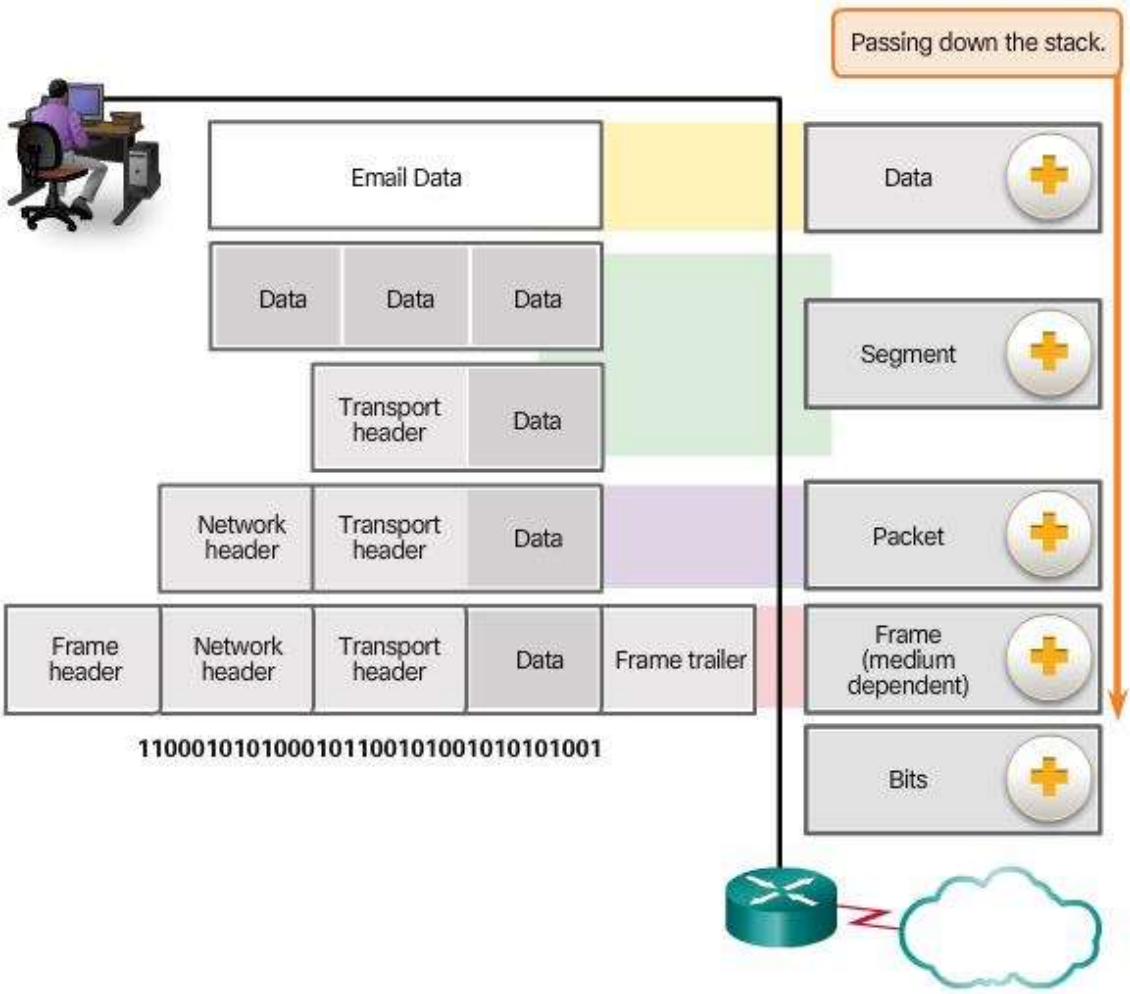
1. Tạo dữ liệu tại lớp Application của host nguồn.
2. Phân đoạn và đóng gói dữ liệu khi chúng di chuyển xuống dưới trong chồng giao thức của host nguồn.
3. Lớp Network Access của host nguồn đưa dữ liệu vào môi trường truyền.
4. Dữ liệu đi qua mạng bao gồm môi trường truyền và các thiết bị trung gian.
5. Lớp Network Access của host đích nhận được dữ liệu.

6. Mở gói và tổng hợp sắp xếp lại dữ liệu khi di chuyển lên phía trên của chồng giao thức của host đích.

7. Đưa dữ liệu đến ứng dụng đích tại lớp Application của host đích.

3.5.4 | CÁCH ĐÓNG GÓI DỮ LIỆU VÀ PDU

Tại máy gửi, dữ liệu sẽ đi xuống từ lớp Application đến lớp Network Access. Sau đó di chuyển qua mạng và cuối cùng đến máy nhận, dữ liệu sẽ đi từ lớp Network Access đến lớp Application. Khi qua mỗi lớp, giao thức tại mỗi lớp sẽ gán thêm thông tin của mình vào dữ liệu nhận được tạo thành một gói dữ liệu mới. Quá trình này gọi là quá trình đóng gói dữ liệu. Hình thức của gói dữ liệu mới tại mỗi lớp được gọi là PDU (Protocol Data Unit).



Hình 3.20: Quá trình đóng gói dữ liệu

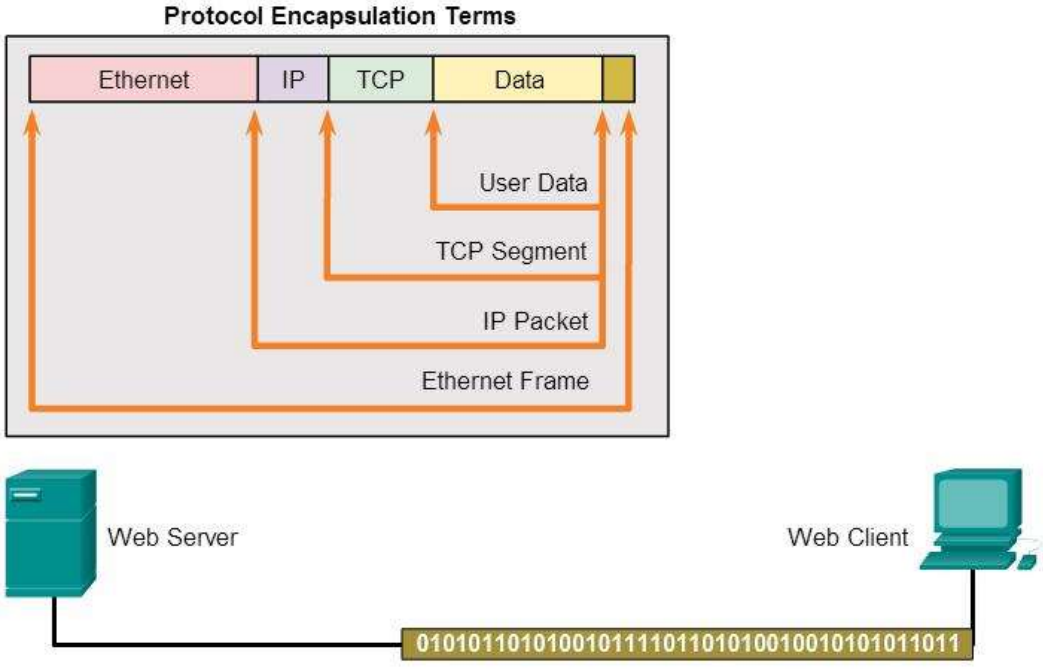
Trong tài liệu này, PDU của mỗi lớp được đặt tên theo các giao thức của họ giao thức TCP/IP.

- Data: thuật ngữ chung chỉ dữ liệu ban đầu tại lớp Application.
- Segment: tên gọi của PDU tại lớp Transport.
- Packet: tên gọi của PDU tại lớp Network.
- Fame: tên gọi của PDU tại lớp Network Access.
- Bits: đươc sử dụng khi truyền dữ liệu trên môi trường truyền.

3.5.5 | QUÁ TRÌNH GỬI DỮ LIỆU

Chúng ta sử dụng mô hình TCP/IP để mô tả quá trình web server gửi một trang HTML đến web client. Nó bao gồm những bước sau:

1. Tại lớp Application, HTTP bắt đầu quá trình bằng cách gửi dữ liệu trang web đã được định dạng theo HTML xuống lớp Transport.



Hình 3.21: Quá trình gửi dữ liệu

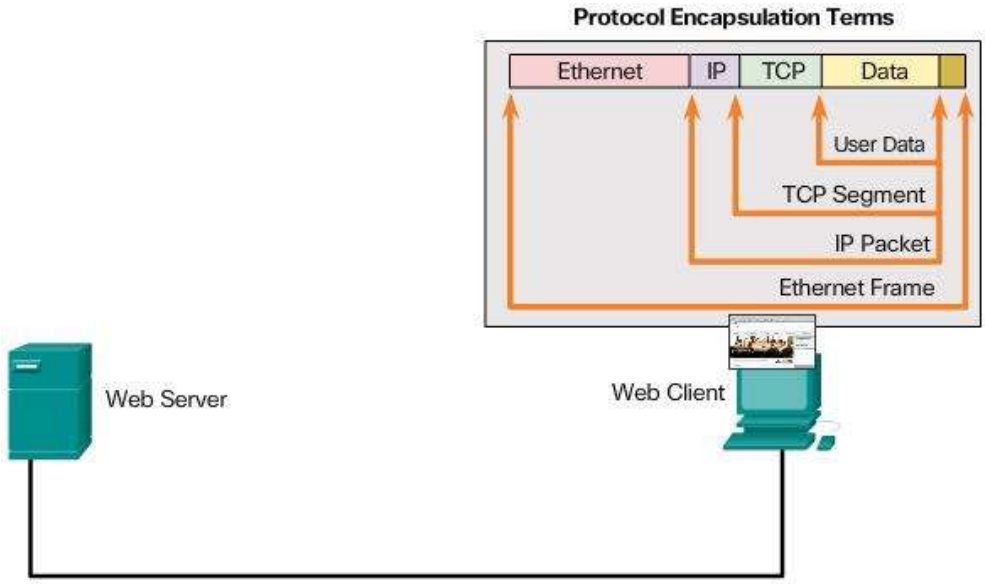
2. Giao thức TCP ở lớp Transport nhận được dữ liệu trang web và phân đoạn dữ liệu này thành các đoạn dữ liệu nhỏ hơn. Sau đó gắn thên nhãn được gọi

là TCP Header vào các đoạn dữ liệu nhỏ tạo thành các TCP segment. TCP Header có các thông tin giúp cho tiến trình nhận tại máy nhận tổng hợp và sắp xếp lại dữ liệu giống như ban đầu. Lớp Transport sẽ chuyển các TCP segment xuống lớp Internet.

3. Giao thức IP tại lớp Internet nhận được các TCP segment, nó gán thêm nhãn IP Header vào các TCP segment này để đóng gói thành IP packet. IP Header chứa địa chỉ IP của máy gửi và địa chỉ IP của máy nhận. Thông tin này rất cần thiết để các IP paket đến được đích. Sau đó, lớp Internet sẽ chuyển các IP packet xuống lớp kế tiếp là lớp Network Access.

4. Tại lớp Network Access, giao thức Ethernet sẽ gán thêm Frame Header vào đầu IP packet và Frame Trailer vào cuối IP packet để tạo thành Frame. Mỗi Frame Header chứa địa chỉ vật lý của máy gửi và máy nhận. Địa chỉ vật lý này còn gọi là địa chỉ MAC, nó là địa chỉ duy nhất dùng để phân biệt các thiết bị trong mạng cục bộ. Thông tin trong Frame Trailer được dùng để kiểm tra lỗi. Cuối cùng NIC sẽ mã hóa các bit thành các tín hiệu và đưa vào môi trường truyền Ethernet.

Tại web client, quá trình này thực hiện ngược lại. Dữ liệu đi lên từ lớp Network Access đến lớp Application. Nếu như tại máy gửi giao thức tại mỗi lớp đã thêm thông tin gì, thì tại máy nhận giao thức đó sẽ lấy thông tin ra và chuyển dữ liệu còn lại lên lớp trên.



Hình 3.22: Quá trình nhận dữ liệu

3.6 | SO SÁNH MÔ HÌNH OSI VÀ MÔ HÌNH TCP/IP

Các điểm giống nhau giữa mô hình OSI và mô hình TCP/IP:

- Đều phân lớp chức năng.
- Có lớp ứng dụng gồm một số dịch vụ.
- Đều có lớp vận chuyển và lớp mạng.
- Chuyển mạch gói.
- Đều giống nhau về mối quan hệ trên dưới và ngang hàng.

Các điểm khác nhau giữa mô hình OSI và mô hình TCP/IP:

- Mô hình TCP/IP gộp chức năng lớp trình bày và lớp phiên vào lớp ứng dụng.
- Mô hình TCP/IP gộp lớp vật lý và lớp liên kết dữ liệu thành một lớp.
- Mô hình TCP////IP đơn giản vì có ít lớp hơn.

Mô hình giao thức cung cấp một mô hình gần với cấu trúc của một họ giao thức cụ thể. Nó mô tả các tính năng cần thiết của các giao thức trong họ giao thức và sự tương tác giữa chúng để đảm bảo rằng các thiết bị trên mạng có thể truyền thông với nhau. Mô hình TCP/IP là một mô hình giao thức.

Mô hình tham chiếu cung cấp một sự tham chiếu chung cho việc duy trì tính ổn định của các giao thức và dịch vụ mạng. Nó cung cấp thông tin chi tiết và đầy đủ để định nghĩa chính xác những dịch vụ trong kiến trúc mạng. Mục đích chính của mô hình tham chiếu là minh bạch hơn những tính năng và tiến trình có liên quan. Mô hình OSI là mô hình tham chiếu liên mạng được sử dụng phổ biến nhất rộng rãi nhất. Nó được sử dụng trong việc mô tả hoạt đọng của mạng, thiết kế mạng và chẩn đoán xử lý lỗi.

Internet được phát triển bởi các tiêu chuẩn của giao thức TCP/IP. TCP/IP được tín nhiệm bởi các giao thức cụ thể của nó, ngược lại mô hình OSI không định ra

một giao thức cụ thể nào mà nó chỉ là một khuôn mẫu hướng dẫn để hiểu và tạo ra một quá trình truyền thông.

3.7 | BÀI TẬP CHƯƠNG 3

1. Giao thức là gì? Cho ví dụ.
2. Liệt kê các lớp của mô hình OSI theo thứ tự từ trên xuống.
3. Giải thích hoạt động của 7 lớp trong mô hình OSI.
4. Trình bày tính năng của giao thức TCP và UDP.
5. Quá trình dữ liệu di chuyển từ hệ thống máy tính này sang hệ thống máy tính khác phải trải qua những giao đoạn nào?
6. Nêu trình tự đóng gói dữ liệu khi truyền từ máy tính này đến máy tính khác?
7. PDU là gì? Trình bày cách đóng gói dữ liệu.
8. Trình bày quá trình gửi và nhận dữ liệu.
9. Giải thích hoạt động của 4 lớp trong mô hình TCP/IP.
10. So sánh mô hình OSI và mô hình TCP/IP.

4. ĐỊA CHỈ IP

Sau khi học xong chương này, sinh viên có thể:

- Giải thích cấu trúc địa chỉ IPv4
- Phân biệt các lớp địa chỉ IPv4
- Thực hiện kỹ thuật chia subnet
- Trình bày cấu trúc địa chỉ IPv6 và các loại địa chỉ IPv6

4.1 | CHUYỂN ĐỔI GIỮA SỐ NHỊ PHÂN VÀ SỐ THẬP PHÂN

4.1.1 | CHUYỂN ĐỔI SỐ NHỊ PHÂN THÀNH SỐ THẬP PHÂN

Khi thao tác trên địa chỉ IP, một trong những kỹ năng mà bạn cần phải có và thành thạo đó là chuyển đổi số nhị phân thành số thập phân.

Trong cuộc sống, dữ liệu nhị phân có thể được biểu diễn dưới nhiều hình thức dữ liệu khác nhau. Nhưng trong phạm vi quyển giáo trình này, chúng ta chỉ xét nó trong ngữ cảnh địa chỉ IPv4. Điều này có nghĩa rằng chúng ta xem mỗi byte (octet) như một số thập phân mà nó có giá trị trong khoảng từ 0 đến 255.

Trong số nhị phân 8 bit, vị trí biểu diễn như sau:

Radix	2	2	2	2	2	2	2	2
Position in #	7	6	5	4	3	2	1	0
Calculate	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Positional Value	128	64	32	16	8	4	2	1

Hệ thống số của cơ số 2 chỉ có 2 số: 0 và 1

Khi chúng ta đổi 1 byte (8 bit) dạng nhị phân thành một số thập phân, tại những vị trí có số 1 xuất hiện sẽ thu được giá trị và những vị trí có số 0 xuất hiện có giá trị bằng 0.

Ví dụ đổi số nhị phân11000000 sang thận phân

128	64	32	16	8	4	2	1
1	**1**	**0**	**0**	**0**	**0**	**0**	**0**
1*128	1*64	0*32	0*16	0*8	0*4	0*2	0*1
128	64	32	16	8	4	2	1
192							

Nếu 8 bit của 1 byte có giá trị là 1 hết thì số thập phân tương ứng của nó là:

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1

128+64+32+16+8+4+2+1 =255

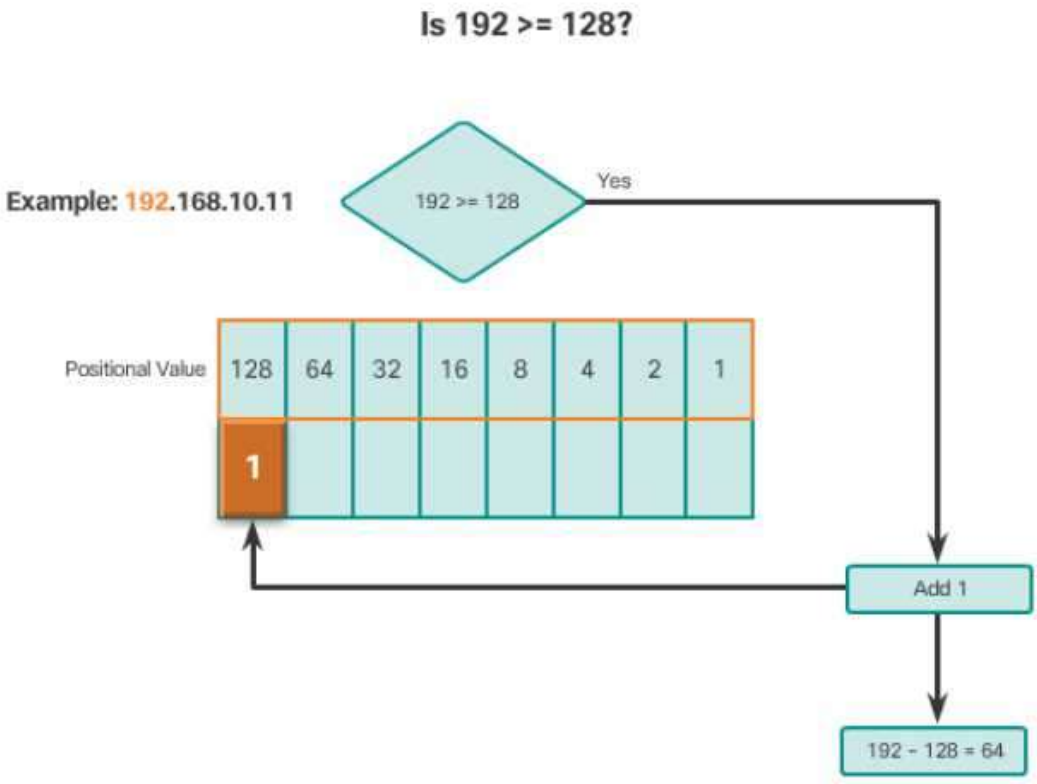
4.1.2 | CHUYỂN ĐỔI SỐ THẬP PHÂN THÀNH SỐ NHỊ PHÂN

Bởi vì biểu diễn các địa chỉ IPv4 dưới dạng số thập phân chỉ dừng lại ở một octet, nên chúng ta chỉ khảo sát quá trình chuyển đổi một số thập phân có giá trị từ 0 đến 255 thành số nhị phân 8 bit.

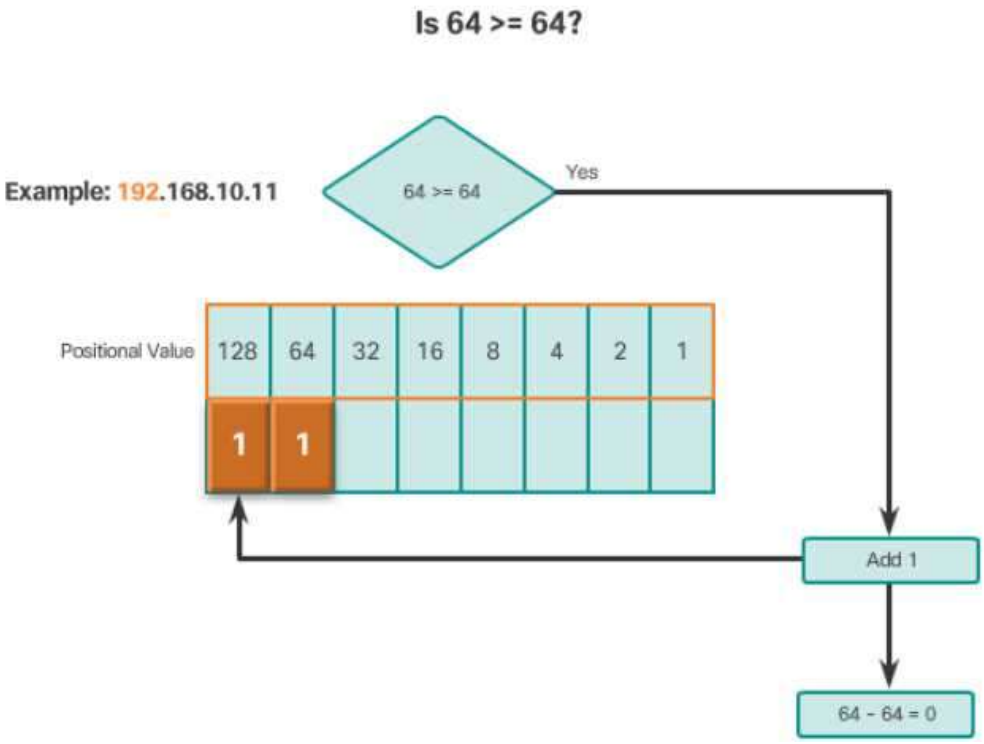
Có thể có nhiều cách chuyển đổi số thập phân thành nhị phân, đây là một cách điển hình

Bắt đầu quá trình chuyển đổi chúng ta so sánh số thập phân đã cho với giá trị thập phân của bit cao nhất – bit ngoài cùng bên trái. Nếu số thập phân bằng hay lớn hơn128 thì bit ngay tại giá trị 128 được bật lên 1, ngược lại nếu nhỏ hơn thì bit này bật lên 0. Tiếp theo lấy giá trị thập phân ban đầu trừ đi 128, sau đó giá trị còn lại tiếp tục so sánh như vậy với giá trị 64 của bit tiếp theo. Và tiếp tục thực hiện như thế cho tất cả các bit còn lại.

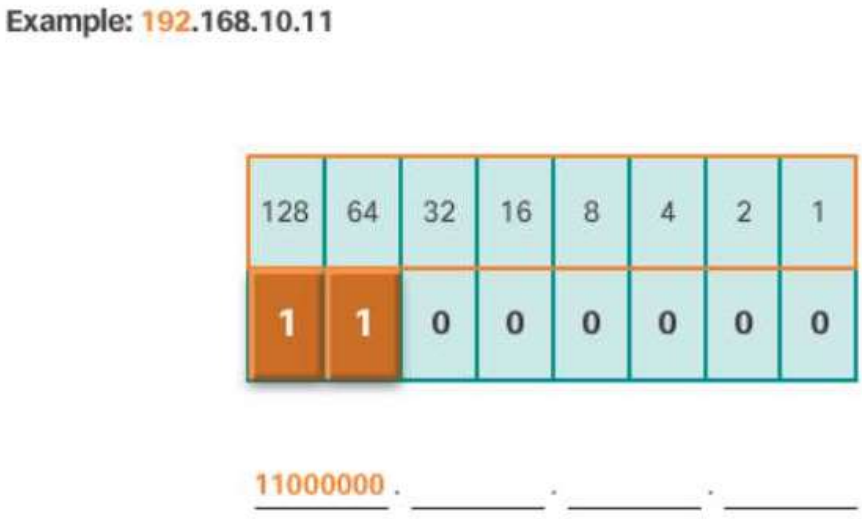
Ví dụ: Đổi số thập phân 192 thành số nhị phân



Hình 4.1: Đổi số thập phân sang số nhị phân



Hình 4.2: Đổi số thập phân sang số nhị phân



Hình 4.3: Đổi số thập phân sang số nhị phân

4.2 | ĐỊA CHỈ IPV4

Các thiết bị trên mạng giao tiếp với nhau đều phải có một định danh duy nhất; đó là địa chỉ IP. Địa chỉ IP là địa chỉ logic được sử dụng trong giao thức IP của lớp Internet thuộc mô hình TCP/IP (tương ứng với lớp Network của mô hình OSI).

4.2.1 | CẤU TRÚC ĐỊA CHỈ IPV4

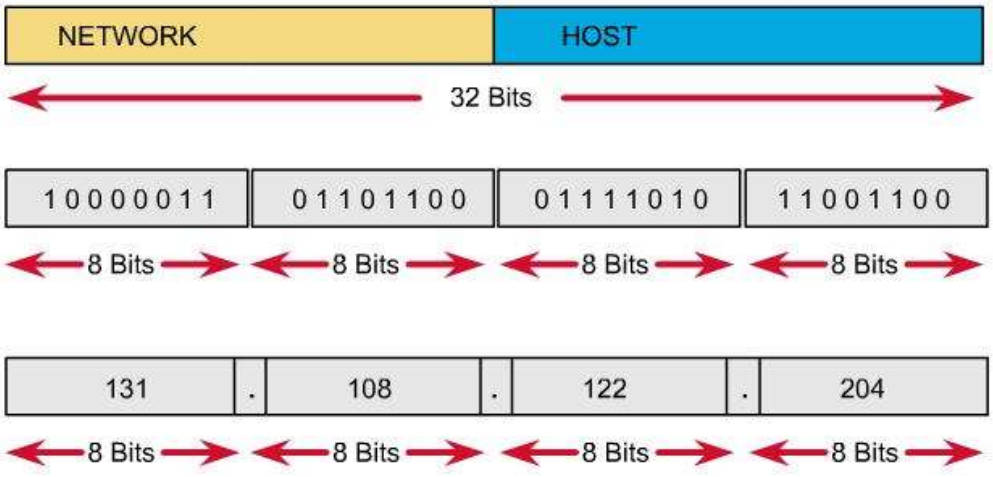
Địa chỉ IPv4 gồm 32 bit nhị phân, chia thành 4 cụm 8 bit (gọi là các octet). Các octet được biểu diễn dưới dạng thập phân và được ngăn cách nhau bằng các dấu chấm.

Địa chỉ IPv4 được chia thành hai phần: phần mạng (network) và phần host.

Chúng ta thử tìm hiểu qua cách phân phát thư của hệ thống bưu chính quốc gia. Khi thư được định tuyến, trước hết nó phải được chuyển đến bưu cục tại thành phố bằng zip code. Sau đó, bưu cục này sẽ định vị đích sau cùng trong thành phố này thông qua địa chỉ nhà và tên đường. Đây là hai bước xử lý. Theo cách tương tự, mỗi địa chỉ IP có hai phần. Phần đầu tiên định danh cho mạng, nơi mà thiết bị kết nối đến và phần thứ hai định danh cho một thiết bị trên mạng đó. Kiểu địa chỉ này được gọi là địa chỉ phân cấp bởi vì nó có nhiều mức khác nhau. Một địa chỉ IP phải kết hợp cả hai định danh này thành một số. Số này phải là duy nhất, bởi vì nếu địa chỉ trùng nhau sẽ làm cho quá trình định tuyến không thể thực hiện được.

Trong một mạng, phần mạng của tất cả các thiết bị phải giống nhau và phần host thay đổi để định danh cho mỗi thiết bị trong mạng. Số lượng bit trong phần host sẽ quyết định số lượng thiết bị tối đa có trong mạng đó.

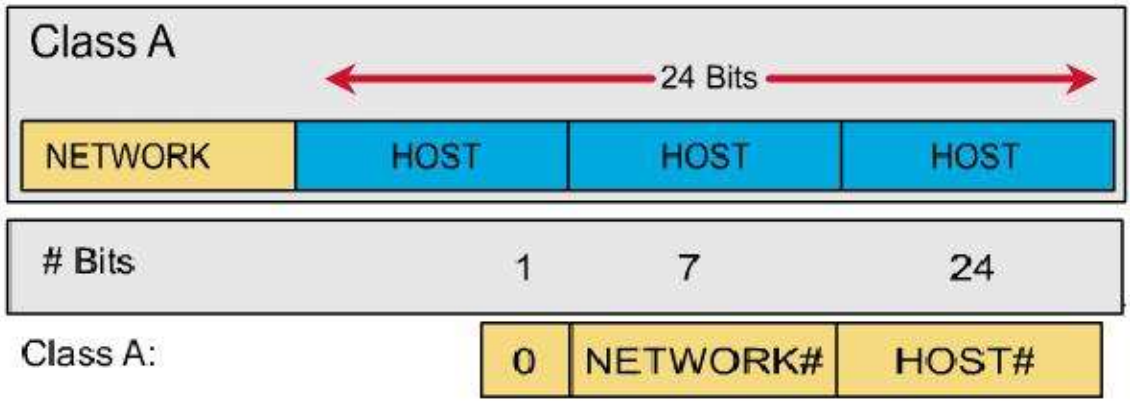
Ví dụ, nếu chúng ta cần nhiều nhất 200 địa chỉ IP để gán cho 200 thiết bị, khi đó chúng ta có thể sử dụng toàn bộ octet cuối cùng. Với 8 bit thuộc phần host, chúng ta có tổng số 256 giá trị. Điều này có nghĩa rằng những bit trong ba octet đầu sẽ biểu diễn phần mạng.



Hình 4.4: Cấu trúc địa chỉ IP

4.2.2 | CÁC LỚP ĐỊA CHỈ IPV4

Lớp A:



Hình 4.5: Cấu trúc địa chỉ lớp A

Địa chỉ lớp A sử dụng một octet đầu làm phần mạng, ba octet sau làm phần host.

Bit đầu của một địa chỉ lớp A luôn được giữ là 0. Do đó, khoảng địa chỉ mạng lớp A bị giới hạn từ 1.0.0.0/8 đến 127.0.0.0/8.

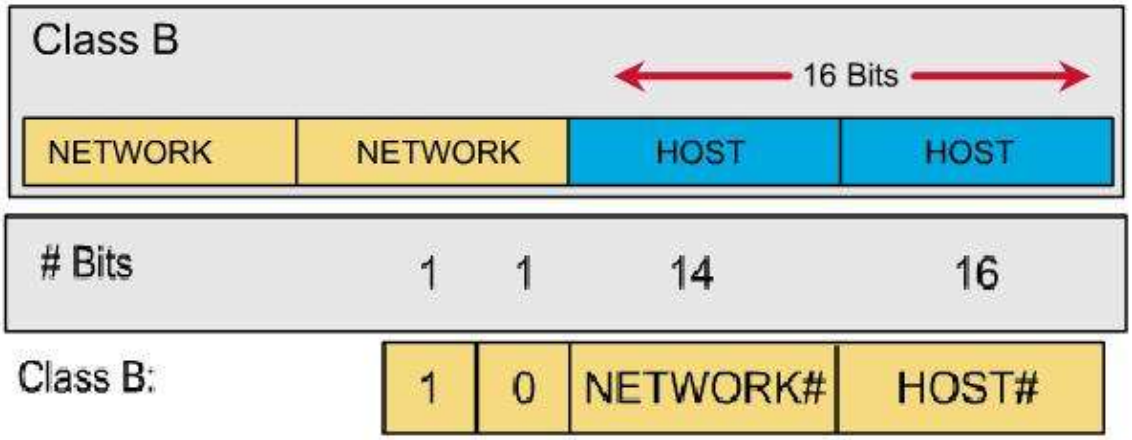
Tuy nhiên, mạng 127.0.0.0 được sử dụng làm mạng loopback nên địa chỉ mạng lớp A sử dụng được từ 1.0.0.0 đến 126.0.0.0 (126 mạng).

Phần host có 24 bit $\Rightarrow$ mỗi mạng lớp A có (2^{24}– 2) host.

Ví dụ: 10.0.0.1, 1.1.1.1, 2.3.4.5 là các địa chỉ lớp A.

Các địa chỉ thuộc lớp A được thiết kế để hỗ trợ những mạng rất lớn có số lượng thiết bị nhiều hơn 16 triệu.

Lớp B



Hình 4.6: Cấu trúc địa chỉ lớp B

Địa chỉ lớp B sử dụng hai octet đầu làm phần mạng, hai octet sau làm phần host.

Hai bit đầu của một địa chỉ lớp B luôn được giữ là 10. Do đó, khoảng địa chỉ mạng lớp B bị giới hạn:

Từ 128.0.0.0/16 đến 191.255.0.0/16.

Có tất cả 2^{14} mạng trong lớp B.

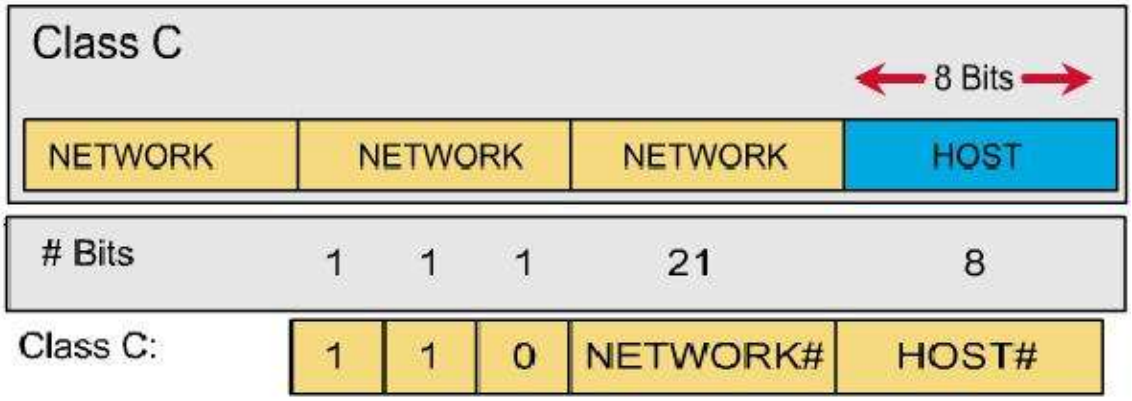
Phần host: 16 bit

Một mạng lớp B có (2^{16}– 2) = 65534 host.

Ví dụ: các địa chỉ 172.16.1.1, 158.0.2.1 là các địa chỉ lớp B.

Khoảng địa chỉ lớp B được thiết kế để hổ trợ cho những mạng có kích thước trung bình có số lượng thiết bị khoảng 65000.

Lớp C



Hình 4.7: Cấu trúc địa chỉ lớp C

Địa chỉ lớp C sử dụng ba octet đầu làm phần mạng, một octet sau làm phần host.

Ba bit đầu của một địa chỉ lớp C luôn được giữ là 1 1 0. Do đó, khoảng địa chỉ mạng lớp C bị giới hạn:

Từ 192.0.0.0/24 đến 223.255.255.0/24

Có tất cả 2^{21} mạng trong lớp C.

Phần host: 8 bit

Một mạng lớp C có $2^8 - 2 = 254$ host.

Ví dụ: các địa chỉ 192.168.1.1, 203.162.4.191 là các địa chỉ lớp C.

Lớp D

Địa chỉ mạng:

Từ 224.0.0.0 đến 239.0.0.0

Dùng làm địa chỉ multicast.

Ví dụ: 224.0.0.5 dùng cho giao thức định tuyến OSPF.

224.0.0.9 dùng cho giao thức định tuyến RIPv2.

Lớp E

Địa chỉ mạng từ 240.0.0.0 đến 255.0.0.0

Được dùng cho mục đích dự phòng, nghiên cứu.

Chú ý:

Các lớp địa chỉ IP có thể sử dụng để đặt cho các host là các lớp A, B, C.

Để thuận tiện cho việc nhận diện một địa chỉ IP thuộc lớp nào, ta quan sát octet đầu tiên của địa chỉ, nếu octet này có giá trị:

- Từ 1 đến 126: địa chỉ lớp A.
- Từ 128 đến 191: địa chỉ lớp B.
- Từ 192 đến 223: địa chỉ lớp C.
- Từ 224 đến 239: địa chỉ lớp D.
- Từ 240 đến 255: địa chỉ lớp E.

Subnet mask và số prefix

Một câu hỏi đặc biệt quan trọng đặt ra là: nhìn vào một địa chỉ IPv4, làm cách nào để chúng ta biết phần mạng có bao nhiêu bit và phần host có bao nhiêu bit? Câu trả lời là chúng ta phải có thông tin subnet mask đi kèm với địa chỉ IPv4.

Subnet mask

Subnet mask là một dải 32 bit nhị phân đi kèm với một địa chỉ IP, được các host sử dụng để xác định địa chỉ mạng của địa chỉ IP này. Để làm được điều đó, host sẽ đem địa chỉ IP thực hiện phép tính AND từng bit một của địa chỉ với subnet mask của nó, kết quả host sẽ thu được địa chỉ mạng tương ứng của địa chỉ IP.

Ví dụ: Xét địa chỉ 192.168.10.10 với subnet mask tương ứng là 255.255.255.0

Phép toán AND: 0 AND 0 = 0

0 AND 1 = 0

1 AND 0 = 0

1 AND 1 = 1

IP address	192	168	10	10
Binary	11000000	10101000	00001010	00001010
Subnet mask	255	255	255	0
Binary	11111111	111111111	11111111	00000000
AND Result	11000000	10101000	00001010	00000000
Netwwork Address	192	168	10	0

Đối với chúng ta, quy tắc gợi nhớ subnet mask rất đơn giản: phần mạng chạy đến đâu, bit 1 của subnet mask chạy đến đó, ứng với các bit phần host, các bit của subnet mask được thiết lập giá trị 0. Một số subnet mask chuẩn:

Lớp A : 255.0.0.0

Lớp B: 255.255.0.0

Lớp C: 255.255.255.0

Số prefix

Subnet mask được sử dụng kèm với địa chỉ IP để một host có thể căn cứ vào đó xác định được địa chỉ mạng tương ứng của địa chỉ này. Vì vậy, khi khai báo một địa chỉ IP ta luôn phải khai báo kèm theo một subnet mask. Tuy nhiên, subnet mask mặc dù đã được viết dưới dạng số thập phân vẫn khá dài dòng nên để mô tả một địa chỉ IP một cách ngắn gọn hơn, người ta dùng một đại lượng được gọi là số prefix. Số prefix đơn giản chỉ là số bit mạng trong một địa chỉ IP, được viết ngay sau địa chỉ IP, và được ngăn cách với địa chỉ này bằng một dấu "/".

Ví du: 192.168.1.1/24, 172.16.0.0/16 hay 10.0.0.0/8,...

4.2.3 | NHỮNG LOẠI ĐỊA CHỈ TRONG MẠNG IPV4

Trong khoảng địa chỉ của mỗi mạng IPv4, chúng ta có 3 loại địa chỉ:

- Địa chỉ mạng: địa chỉ mà chúng ta dùng để định danh cho một mạng.
- Địa chỉ broadcast: địa chỉ đặc biệt được dùng để gửi dữ liệu đến tất cả thiết bị trong mạng.

- Địa chỉ máy (địa chỉ host): địa chỉ được dùng để gán cho các thiết bị đầu cuối trong mạng.

Địa chỉ mạng

Địa chỉ mạng thường được dùng khi chúng ta muốn phân biệt giữa mạng này với mạng khác. Nếu các bit phần host đồng thời bằng 0, ta có một địa chỉ mạng.

Ví dụ: địa chỉ 192.168.1.0 là một địa chỉ mạng, không thể gán cho host được.

Địa chỉ broadcast

Địa chỉ broadcast là một địa chỉ đặc biệt cho mỗi mạng, nó cho phép truyền dữ liệu đến tất cả thiết bị trong mạng, nó chỉ cần dùng địa chỉ IP đích là địa chỉ broadcast của mạng đó.

Địa chỉ broadcast là địa chỉ cao nhất trong khoảng địa chỉ của mạng. Hay nói cách khác đây là địa chỉ mà tất cả các bit trong phần host đều bật lên 1.

Ví dụ: địa chỉ 192.168.1.255 là một địa chỉ broadcast

Địa chỉ host

Như chúng ta đã biết, khi dùng họ giao thức TCP/IP, bắt buộc mỗi thiết bị cuối phải có một địa chỉ IP duy nhất để trao đổi packet với nhau. Chúng ta gán địa chỉ cho các thiết bị cuối trong một mạng bằng cách lấy các địa chỉ trong khoảng giữa địa chỉ mạng và địa chỉ broadcast của mạng đó. Ví dụ: địa chỉ 192.168.1.1 là một địa chỉ có thể gán cho host.

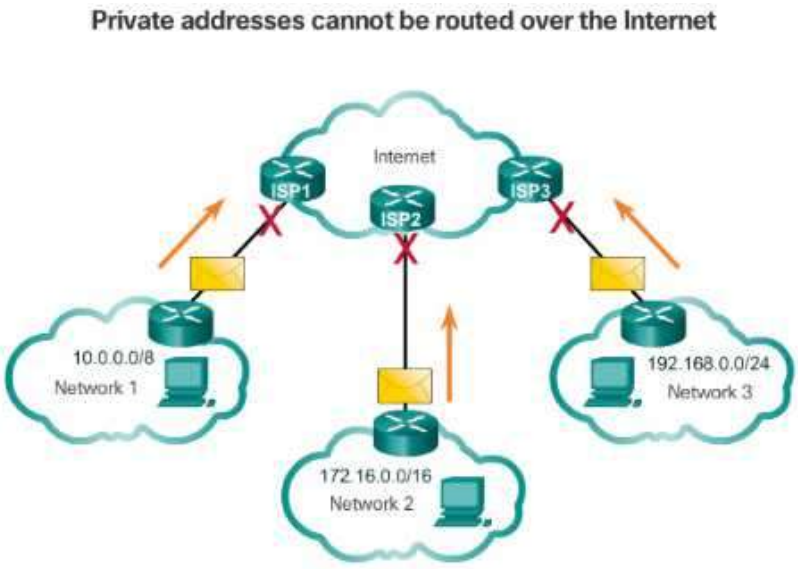
4.2.4 | ĐỊA CHỈ PRIVATE VÀ ĐỊA CHỈ PUBLIC

Khi muốn kết nối vào mạng Internet để trao đổi, chia sẻ thông tin với mọi ngươi trên khắp thế giới thì bắt buộc máy tính của bạn phải có một địa chỉ IP. Địa chỉ này được gọi là địa chỉ public.

Khi sử dụng địa chỉ public bạn có thể đăng ký ở các ISP và phải tốn phí. Nhưng với tốc độ phát triển Internet như vũ bão trong thời gian qua và hiện nay thì liệu 232 địa chỉ có đủ cung cấp cho nhu cầu muốn kết nối Internet của người dùng không. Do đó, người ta đưa ra nhiều giải pháp và một trong những giải pháp đó là địa chỉ private.

Trong mạng cục bộ hầu hết các máy tính được gán địa chỉ private chỉ trừ những máy tính hay thiết bị mạng giao tiếp trực tiếp với Internet thì được gán địa chỉ public. Bất kỳ ai cũng được phép sử dụng địa chỉ private mà không tốn một khoản phí nào hay xin phép ai cả. Nhiều mạng khác nhau có thể sử dụngg cùng địa chỉ private.

Một vấn đề đặt ra là khi các máy tính có địa chỉ private, như các mạng cục bộ của hình 5.2.4.1, muốn truy cập Internet thì làm cách nào để đạt được yêu cầu này. Khi đó, bạn có thể dùng một phương pháp là chuyển đổi địa chỉ mạng – Network Address Translation (NAT). NAT được cấu hình tại router biên, kết nối trực tiếp đến Internet. Nó có nhiệm vụ chuyển đổi địa chỉ private thành địa chỉ public để giao tiếp được với Internet.



Hình 4.8: Địa chỉ private không thể đia ra ngoài Internet

Các khoảng địa chỉ private là:

10.0.0.0 đến 10.255.255.255 (10.0.0.0/8)

172.16.0.0 đến 172.31.255.255 (172.16.0.0/12)

192.168.0.0 đến 192.168.255.255 (192.168.0.0/16)

4.2.5 | NHỮNG ĐỊA CHỈ IPV4 ĐẶC BIỆT

Có những địa chỉ không được phép gán cho các thiết bị vì những lý do khác nhau. Và cũng có những địa chỉ đặc biệt có thể gán cho những thiết bị nhưng khi đó các thiết bị giới hạn về cách tương tác trong mạng.

Địa chỉ mạng và địa chỉ broadcast

Hai địa chỉ này không được phép gán cho các thiết bị

Địa chỉ loopback

Địa chỉ trong khoảng từ 127.0.0.0 đến 127.255.255.255 được gọi là địa chỉ loopback. Địa chỉ này là địa chỉ đặc biệt mà các thiết bị sử dụng để trao đổi thông tin trực tiếp với chính mình. Nó được đưa ra nhằm tạo thuận lợi cho sự giao tiếp giữa các ứng dụng và dịch vụ TCP/IP chạy trên thiết bị. Bằng cách sử dụng địa chỉ loopback thay cho địa chỉ máy được gán. Bạn cũng có thể ping đến địa chỉ loopback để kiểm tra cấu hình TCP/IP của chính máy cục bộ.

Địa chỉ Link-local

Các địa chỉ IP trong khoảng từ 169.254.0.0 đến 169.254.255.255 (169.254.0.0/16) được gọi là các địa chỉ link-local. Hệ điều hành sử dụng những địa chỉ này để gán tự động cho máy cục bộ khi nó không được cấu hình một địa chỉ IP. Các địa chỉ này có thể được sử dụng trong một mạng nhỏ peer-to-peer hoặc một máy mà không thể tự động lấy một địa chỉ từ một DHCP server.

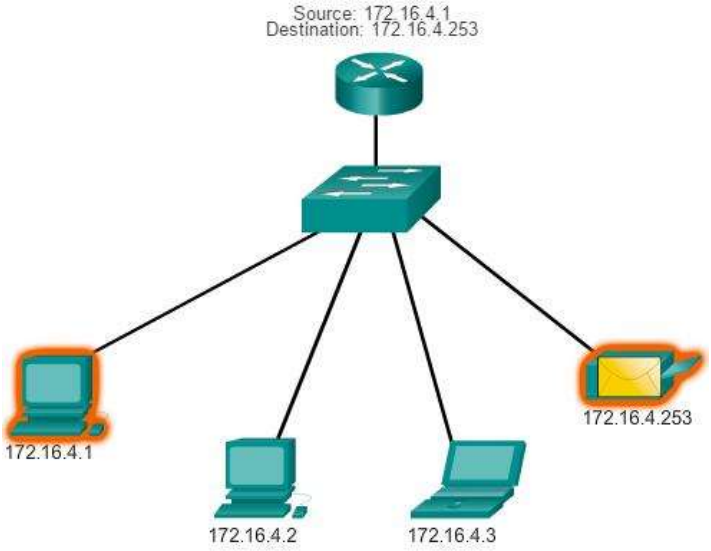
Địa chỉ TEST-NET

Khoảng địa chỉ từ 192.0.2.0 đến 192.0.2.255 (192.0.2.0/24) được dành riêng cho các mục đích dạy và học. Những địa chỉ này có thể được dùng trong các tài liệu và ví dụ mạng. không giống như các địa chỉ thí nghiệm, các thiết bị mạng vẫn chấp nhận những địa chỉ này trong cấu hình của chúng. Bạn thấy những địa chỉ này được sử dụng trong các domain name như example.com hoặc example.net ở các RFC và tài liệu về giao thức. Những địa chỉ trong khoảng này không được xuất hiện trên Internet.

4.2.6 | CÁC LOẠI GIAO TIẾP

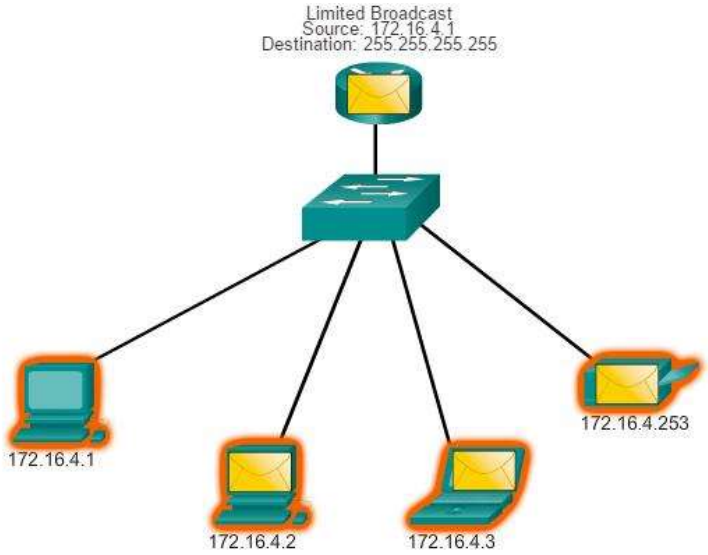
Trong mạng IPv4, sự giao tiếp giữa các thiết bị được phân thành 3 loại:

- **Unicast** – là quá trình gửi một packet từ một thiết bị đến một thiết bị khác



Hình 4.9: Giao tiếp Unicast

- **Broadcast** – là quá trình gửi một packet từ một thiết bị đến tất cả các thiết bị còn lại trong một mạng.



Hình 4.10: Giao tiếp Broadcast

Có hai loại broadcast: directed broadcast và limited broadcast.

- Directed broadcast

Một directed broadcast hữu ích khi muốn gửi một broadcast đến tất cả các thiết bị trong một mạng khác. Ví dụ, một máy ở ngoài mạng muốn gửi thông tin đến tất cả các máy trong mạng 172.16.4.0/24, địa chỉ đích của packet sẽ là 172.16.4.255.

Mặc định các router không chuyển directed boadcast, nhưng chúng có thể được cấu hình để làm điều này.

- Limited broadcast

Limited broadcast bị giới hạn trong một mạng cục bộ. Những packet này sử dụng địa chỉ đích là 255.255.255.255. Các router không chuyển các packet loại này. Các packet này chỉ xuất hiện trên mạng cục bộ. Vì lý do này mà mạng IPv4 được xem là một broadcast domain.

Ví dụ, trong hình 5.2.6.2 một máy trong mạng 172.16.4.0/24 sẽ quảng bá thông tin đến tất cả các máy còn lại trên mạng của nó bằng cách dùng một packet với địa chỉ đích là 255.255.255.255.

Các gói tin broadcast chiếm băng thông mạng và ảnh hưởng đến các thiết bị khác vì phải nhận và xử lý nó. Mạng càng lớn, broadcast càng tăng lên ảnh hưởng đến hiệu suất của mạng. Do đó, cần phải có giải pháp để giới hạn broadcast. Giải pháp có thể là bạn sử dụng router để chia một broadcast domain thành các subnet vì router hoạt động ở lớp Network có khả năng phân cách broadcast domain. Khi đó hiệu suất mạng được cải thiện.

- **Multicast** – là quá trình gửi một packet từ một thiết bị đến một nhóm các thiết bị được chọn trong một mạng.

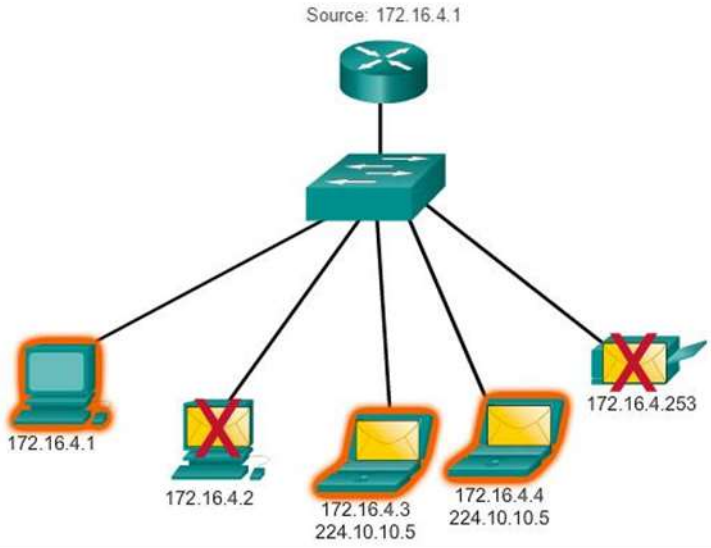
Multicast được thiết kế để bảo toàn băng thông của mạng IPv4. Nó làm giảm lưu lượng bằng cách cho phép một thiết bị gửi thông tin đến một nhóm các thiết bị. Nếu sử dụng unicast, khi muốn gửi thông tin gì đó đến một nhóm các thiết bị, máy gửi phải gửi từng packet riêng lẻ đến từng thiết bị trong nhóm. Nhưng với multicast, máy gửi chỉ cần gửi một packet với địa chỉ đích là địa chỉ multicast.

Một vài ví dụ về giao tiếp multicast:

- Truyền video và audio.
- Các giao thức định tuyến trao đổi thông tin.
- Cung cấp thông tin.

Những thiết bị nhận dữ liệu multicast được gọi là multicast client. Multicast client sử dụng các dịch vụ được khởi tạo bởi một chương trình client đồng ý tham gia vào nhóm multicast.

Mỗi nhóm multicast được biểu diễn bằng một địa chỉ đích multicast IPv4. Khi một thiết bị đồng ý vào nhóm multicast, thiết bị xử lý gói tin multicast giống như gói tin unicast. IPv4 dành một khoảng địa chỉ multicast từ 224.0.0.0 đến 239.255.255.255.



Hình 4.11: Giao tiếp Multicast

4.3 | SUBNET

4.3.1 | KHÁI NIỆM SUBNET

Một công ty nhỏ với khoảng vài người thì có thể không cần quan tâm đến vị trí ngồi của nhân viên, hay chia phòng ban và nhóm những người cùng phòng ban ngồi gần với nhau để dễ trao đổi trong công việc. Khi công ty phát triển với số lượng nhân viên tăng lên hàng trăm người, nếu chúng ta giữ nguyên cách tổ chức như cũ thì rất khó khăn trong việc quản lý nhân sự và công việc. Do đó, chúng ta phải chia phòng ban, sắp xếp những người cùng phòng ban ngồi cùng phòng hay gần nhau, v.v…Đối với mạng máy tính cũng vậy, khi số lượng thiết bị trên mạng tăng lên nhiều chúng ta cũng nên chia một mạng lớn thành các mạng con nhỏ hơn hay chúng ta thường gọi là chia subnet và kết nối chúng lại với nhau. Những mạng con này thường được gọi là subnet.

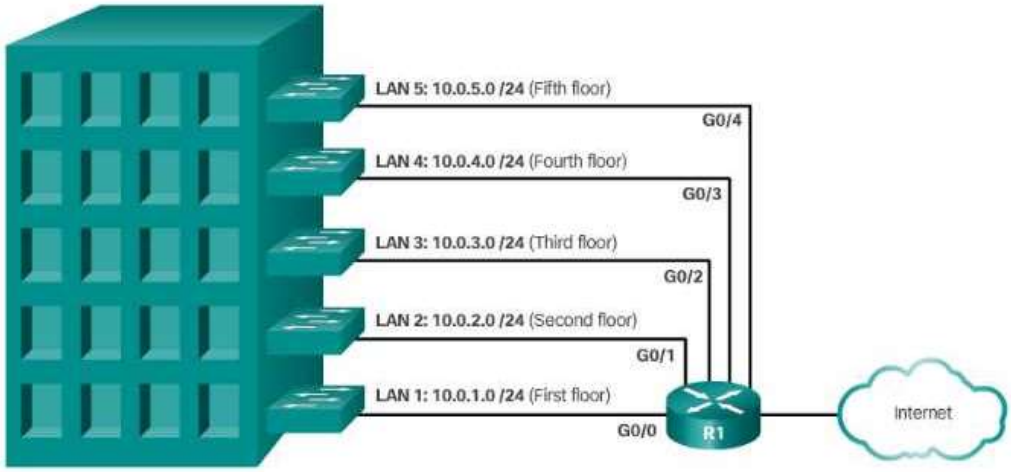
Thuật ngữ mạng và subnet thường dùng thay thế cho nhau khi đề cập đến mạng máy tính.

Chia subnet là một trong những giải pháp hữu dụng để xây dựng mạng nội bộ, vừa bảo mật, ngăn chặn broadcast, vừa tiết kiệm tài nguyên trong việc phân phát địa chỉ IP cho từng máy trạm.

Khi chia subnet, chúng ta thường nhóm các thiết bị dựa vào các tiêu chí:

- Vị trí địa lý

Chẳn hạn như mỗi tòa nhà trong một trường đại học, cao đẳng hay mỗi tầng trong một tòa nhà gồm nhiều tầng là một mạng con.



Hình 4.12: Chia mạng theo vị trí địa lý

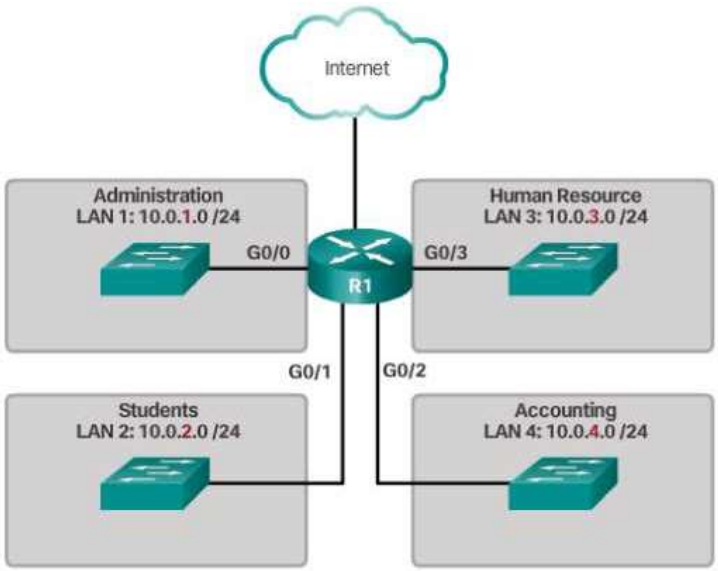
- Quyền sử dụng

Trong một mạng lớn việc định nghĩa và giới hạn quyền hạn truy cập của mỗi người dùng đến các tài nguyên trên mạng là điều rất quan trọng vì nó liên quan đến các chính sách bảo mật trên mạng. Do đó, chúng ta nên nhóm những người có quyền hạn giống nhau thành một mạng con để việc quản lý cấp phát quyền hạn và theo dõi nó được thuận tiện.

- Theo các mục đích đặc trưng

Chúng ta có thể chia mạng thành các mạng con dựa trên những tác vụ giống nhau của người dùng chẳng hạn như người cùng phòng ban. Những người này sử dụng cùng phần mềm, các công cụ hay tiện ích giống nhau. Với cách chia này làm cho sự

phân bổ tài nguyên trên mạng được thuận tiện và mang lại hiệu quả tốt cũng như sự chứng thực các truy cập đến các tài nguyên mạng này.



Hình 4.13: Chia mạng theo mục đích đặc trưng

4.3.2 | CHIA SUBNET CƠ BẢN

Chia subnet là thao tác chia một khoảng địa chỉ IP thành các khoảng nhỏ hơn cấp cho các mạng con.

Chúng ta chia subnet bằng cách mượn một số bit thuộc phần host. Như vậy số bit ở phần mạng sẽ tăng lên bao gồm: số bit phần mạng ban đầu + số bit phần host vừa mượn.

Lưu ý rằng: chúng ta mượn các bit host từ trái sang phải, càng mượn nhiều bit thì càng tạo ra nhiều subnet. Nhưng khi đó, sô bit thuộc phần host của mỗi subnet sẽ ít hơn làm cho số lượng địa chỉ của mỗi subnet giảm xuống.

Hình 4.14: Mượn thêm bit để chia subnet

Để tính số bit mượn, người thiết kế mạng cần tính toán có bao nhiêu thiết bị mà mạng con lớn nhất cần và số lượng mạng con cần đến. Sau đó chúng ta dùng công thức:

Số subnet có thể dùng = $2^{(\text{số bit mượn})}$ (*)

Số host có thể dùng = $2^{(\text{số bit host còn lại})}$-2 (địa chỉ mạng và địa chỉ broadcast) **(**)**

Lưu ý rằng, bất chấp lớp địa chỉ IP nào, chúng ta không mượn hai bit cuối cùng trong octet cuối cùng. Hai bit này được xem như hai bit có ý nghĩa sau cùng cho phần host. Với hai bit này, tối thiểu mỗi mạng con có 2 địa chỉ để gán cho thiết bị.

Ví dụ 1: cho địa chỉ mạng ban đầu 192.168.1.0/24. Chúng ta lần lượt tính subnet với các trường hợp sau:

Trường hợp 1: 2 subnet

Áp dụng công thức (*), ta xác định cần mượn 1 bit, bit này rơi vào octet cuối cùng. Giá trị octet này như sau:

192.168.1.**0**000 0000 = 192.168.1.**0**

192.168.1.**1**000 0000 = 192.168.1.**128**

Các subnet:

Subnet 1: 192.168.1.0/25

Subnet 2: 192.168.1.128/25

Sau khi mượn 1 bit để chia subnet thì số bit thuộc phần mạng là 25 (subnet mask sẽ là 255.255.255.128 hay /25) và số bit phần host của mỗi subnet bây giờ là 7. Như vậy mỗi subnet có: 2^7-2 =126 địa chỉ có thể sử dụng được.

Với Subnet 1: 192.168.1.0/25

- Địa chỉ IP đầu: 192.168.1.1/25
- Địa chỉ IP cuối: 192.168.1.126
- Địa chỉ broadcast: 192.168.1.127/25

Với Subnet 2: 192.168.1.128/25

- Địa chỉ IP đầu: 192.168.1.129/25

- Địa chỉ IP cuối: 192.168.1.254/25
- Địa chỉ broadcast: 192.168.1.255/25

Trường hợp 2: 4 subnet

Áp dụng công thức **(*)**, ta xác định cần mượn 2 bit, 2 bit này rơi vào octet cuối cùng. Giá trị octet này như sau:

192.168.1.**00**00 0000 = 192.168.1.**0**

192.168.1.**01**00 0000 = 192.168.1.**64**

192.168.1.**10**00 0000 = 192.168.1.**128**

192.168.1.**11**00 0000 = 192.168.1.**192**

Các subnet:

Subnet 1: 192.168.1.0/26

Subnet 2: 192.168.1.64/26

Subnet 3: 192.168.1.128/26

Subnet 4: 192.168.1.192/26

Tính số host / subnet = $2^6 - 2 = 62$ host

Ví dụ 2: cho địa chỉ mạng ban đầu 172.16.0.0/16. Tạo 100 subnet

Áp dụng công thức **(*)**, ta xác định số bit cần mượn là 7 bit, 7 bit này rơi vào octet thứ 3. Giá trị octet này như sau:

0000 0000 = 0

0000 0010 =2

0000 0100 = 4

0000 0110 = 6

…….

1111 11110 = 254

Số subnet = $2^n = 2^7 = 128$

Các subnet:

Subnet 1: 172.16.0.0/23

Subnet 2: 172.16.2.0/23

Subnet 3: 172.16.4.0/23

Subnet 4: 172.16.6.0/23

Subnet 5: 172.16.8.0/23

Subnet 6: 172.16.10.0/23

……

Subnet 128: 172.16.254.0/23

Tính số host / subnet = $2^9 – 2 = 510$ host

Ví dụ 3: cho địa chỉ mạng ban đầu 10.0.0.0/8. Tạo 1000 subnet

Áp dụng công thức **(*)**, ta xác định số bit cần mượn là 10 bit, 10 bit này rơi vào octet thứ 2 và octet thứ 3. Giá trị octet này như sau:

00000000 **00**00 0000 = 0. 0

00000000 **01**00 0010 = 0. 64

00000000 **10**00 0100 = 0. 128

00000000 **11**00 0110 = 0. 192

…….

11111111 **00**00 0000 = 255. 0

11111111 **01**00 0010 = 255. 64

11111111 **10**00 0100 = 255. 128

11111111 **11**00 0110 = 255.192

Số subnet = $2^n = 2^{10} = 1024$

Các subnet:

Subnet 1: 10.0.0.0/18

Subnet 2: 10.0.64.0/18

Subnet 3: 10.0.128.0/18

Subnet 4: 10.0.192.0/18

Subnet 5: 10.1.0.0/18

Subnet 6: 10.1.64.0/18

Subnet 7 10.1.128.0/18

Subnet 8: 10.1.192.0/18

Subnet 9: 10.2.0.0/18

Subnet 10: 10.2.64.0/18

……

Subnet 1024: 10.255.192.0/18

Tính số host / subnet = 2^{14}– 2 =16382 host

4.3.3 | CHIA SUBNET THEO VARIABLE LENGTH SUBNET MASK (VLSM)

Khi chia mạng thành mạng con không phải tất cả các mạng con đều cần số lượng địa chỉ IP giống nhau. Có thể có những mạng con cần số lượng địa chỉ rất lớn, nhưng cũng có những mạng con chỉ cần tối đa 2 địa chỉ chẳng hạn như liên kết WAN, point-to-point giữa hai router. Với cách chia subnet ở trên – căn cứ vào số lượng mạng con mà không quan tâm đến số lượng thiết bị trên mỗi mạng con – thì thật là lãng phí địa chỉ IP. Do đó, chúng ta sẽ chia subnet căn cứ trên số lượng thiết bị hiện tại và dự phòng phát triển trong tương lai của mỗi mạng con mà cấp

số lượng địa chỉ gần đúng như vậy để tránh lãng phí địa chỉ. Quá trình tính toán diễn ra như sau:

Bước 1: Xác định tổng số thiết bị

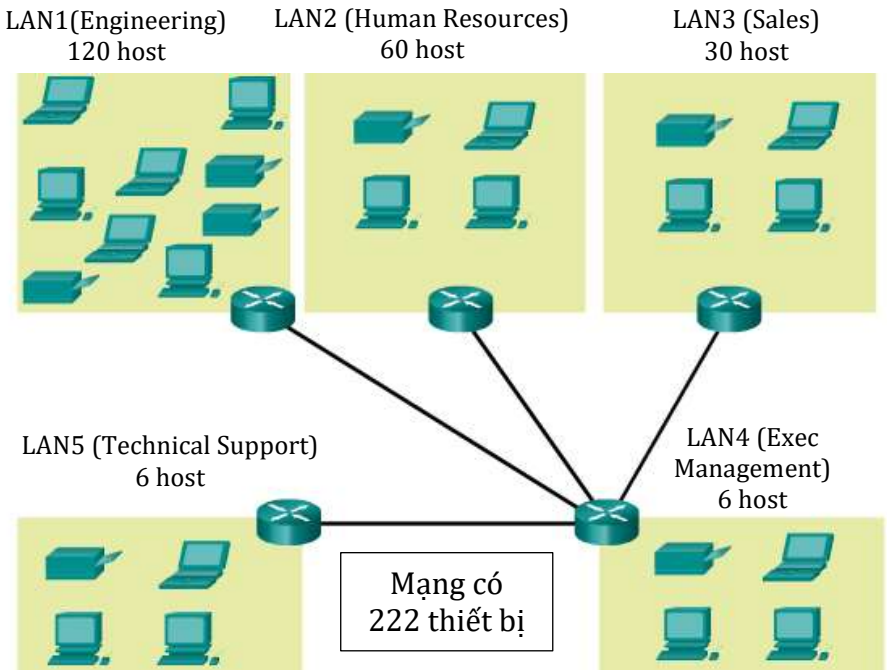
Đầu tiên, xem mạng công ty có bao nhiêu thiết bị. Từ đó chúng ta quyết định sử dụng một địa chỉ mạng nào mà có khoảng địa chỉ IP đủ lớn để đáp ứng cho yêu cầu của chúng ta. Các thiết bị cần địa chỉ IP bao gồm: các thiết bị của người dùng cuối, các server, các thiết bị trung gian và các cổng giao tiếp với router.

Bước 2: Xác định số lượng mạng con và kích thước của mỗi mạng con

Đây là bước xác định cần chia bao nhiêu mạng con và số lượng địa chỉ mạng con cần là bao nhiêu.

Chúng ta thường sử dụng các router để kết nối các mạng con lại. Mỗi liên kết giữa hai router hay liên kết WAN đều tạo thành một mạng. Do đó, chúng ta phải tính các mạng này khi chia subnet.

Với số lượng thiết bị là 222, chúng ta sẽ sử dụng địa chỉ mạng lớp C, chẳn hạn mạng 192.168.1.0/24, chúng ta chia thành 5 mạng con và nối chúng lại bằng các router



Hình 5.15

Thông thường mỗi mạng con tại mỗi vị trí sẽ được gán một subnet. Nhưng chúng ta có thể chia mạng con này thành các mạng con nhỏ hơn bằng cách dùng subnet mask có chiều dài thay đổi được gọi là Variable Length Subnet Mask (VLSM) và khi đó chúng ta cũng có thể chia subnet từ subnet đã cho để gán cho các mạng con nhỏ này.

Bước 3: Cấp phát địa chỉ

Sau khi xác định được số lượng mạng con và số lượng thiết bị (số host) trên mỗi chúng. Chúng ta bắt đầu việc cấp phát địa chỉ từ khoảng địa chỉ chúng ta đang có. Hình 5.34 cho biết số lượng thiết bị trên mỗi mạng con.

Sắp xếp các mạng theo thứ tự số host giảm dần (từ lớn đến nhỏ)

- LAN1: 120 host
- LAN2: 60 host
- LAN3: 30 host
- LAN 4: 6 host
- LAN5: 6 host
- 4 kết nối WAN (WAN1, 2, 3, 4), mỗi kết nối 2 host

Chúng ta bắt đầu chia subnet từ mạng con có số lượng thiết bị nhiều nhất (số host lớn nhất) và giảm dần xuống đến các liên kết point-to-point. Tiến trình này đảm bảo rằng các khoảng địa chỉ chỉ đủ lớn luôn có sẵn để cung cấp cho các thiết bị và các mạng ở những vị trí này.

Gọi n là số bit mượn, m là số bit host còn lại

Xét mạng LAN 1: 120 host

Ta phải xem mượn bao nhiêu bit thì đủ cho mạng này.

Điều kiện: $2^m-2>=120 \Rightarrow m=7$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-24-7=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

Các subnet:

1/ 192.168.1.0/25 (cấp cho LAN 1)

2/ 192.168.1.128/25

Xét LAN 2: 60 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=60 \Rightarrow m=6$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-25-6=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

Các subnet:

2.1/ 192.168.1.128/26 (cấp cho mạng LAN 2)

2.2/ 192.168.1.192/26

Xét mạng LAN 3: có 30 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=30 \Rightarrow m=5$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-26-5=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

Các subnet:

2.2.1/ 192.168.1.192/27 (cấp cho mạng LAN 3)

2.2.2/ 192.168.1.224/27

Xét mạng LAN 4 và LAN 5: có 6 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=6 \Rightarrow m=3$

$\Rightarrow$n = 32-số bit phần mạng – m = 32-27-3=2

$\Rightarrow$ số subnet = $2^n = 2^2 = 4$

Các subnet:

2.2.2.1/ 192.168.1.224/29 (cấp cho mạng LAN 4)

2.2.2.2/ 192.168.1.232/29 (cấp cho mạng LAN 5)

2.2.2.3/ 192.168.1.240/29

2.2.2.4/ 192.168.1.248/29

Xét mạng WAN 1, WAN 2, WAN 3, WAN 4: có 2 host

Điều kiện: $2^m-2>=2 \Rightarrow m=2$

$\Rightarrow$n = 32-số bit phần mạng – m = 32-29-2=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

2.2.2.3.1/ 192.168.1.240/30 (cấp cho WAN 1)

2.2.2.3.2/ 192.168.1.244/30 (cấp cho WAN 2)

2.2.2.4.1/ 192.168.1.248/30 (cấp cho WAN 3)

2.2.2.4.2/ 192.168.1.252/30 (cấp cho WAN 4)

Bảng chia subnet theo VLSM:

Địa chỉ mạng ban đầu	**LAN 1**	**LAN 2**	**LAN 3**	**LAN 4, LAN 5**	**WAN 1,2,3,4**
192.168.1.0/ 24	**192.168.1.0/25**				
	192.168.1.128/ 25	**192.168.1.128 /26**			
		192.168.1.192.26	**192.168.1.192. 27**		
			192.168.1.224/ 24	**192.168.1.224 /29**	
				192.168.1.232 /29	
				192.168.1.240/ 29	**192.168.1.240 /30**
					192.168.1.244

					/30
				192.168.1.248/29	**192.168.1.248 /30**
					192.168.1.252 /30

Bảng thông tin cụ thể của các mạng con

Mạng con	Địac chỉ subnet được cấp	Subnet mask	Khoảng địa chỉ có thể sử dụng	Địa chỉ broadcast
LAN 1	192.168.1.0/25	255.255.255.128	192.168.1.1 – 192.168.1.126	192.168.1.127
LAN 2	192.168.1.128/26	255.255.255.192	192.168.1.129 – 192.168.1.190	192.168.1.191
LAN 3	192.168.1.192/27	255.255.255.224	192.168.1.193 – 192.168.1.222	192.168.1.223
LAN 4	192.168.1.224/29	255.255.255.248	192.168.1.225 – 192.168.1.230	192.168.1.231
LAN 5	192.168.1.232/29	255.255.255.248	192.168.1.233 – 192.168.1.238	192.168.1.239
WAN 1	192.168.1.240/30	255.255.255.252	192.168.1.241 – 192.168.1.242	192.168.1.243
WAN 2	192.168.1.244/30	255.255.255.252	192.168.1.245 – 192.168.1.246	192.168.1.247
WAN 3	192.168.1.248/30	255.255.255.252	192.168.1.249 – 192.168.1.250	192.168.1.251
WAN 4	192.168.1.252/30	255.255.255.252	192.168.1.253 – 192.168.1.254	192.168.1.255

Ví dụ: Phân hoạch địa chỉ IPv4 cho hệ mạng có khoảng 800 host. Cụ thể như sau:

Comporate HQ: 500 host

Legal Office: 20 host

Sales Office: 200 host

HR: 50 host

3 liên kết WAN, mỗi liên kết 2 host

Bước 1: Xác định tổng số thiết bị

Có khoảng 800 thiết bị

Bước 2: Xác định số lượng mạng con và kích thước của mỗi mạng con

Với số lượng thiết bị khoảng 800, chúng ta sẽ sử dụng địa chỉ mạng 172.16.0.0/22. Chúng ta chia thành 4 mạng con và 3 kết nối WAN

Bước 3: Cấp phát địa chỉ

Sắp xếp các mạng theo thứ tự số host từ lớn đến nhỏ

- LAN 1 (HQ): 500 host
- LAN 2 (Sales): 200 host
- LAN 3 (HR): 50 host
- LAN 4 (Legal): 20 host
- 3 liên kết WAN (WAN 1,2,3): 2 host

Gọi n là số bit mượn, m là số bit host còn lại

Xét mạng LAN 1: 120 host

Ta phải xem mượn bao nhiêu bit thì đủ cho mạng này.

Điều kiện: $2^m-2>=500 \Rightarrow m=9$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-22-9=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

Các subnet:

1/ 172.16.0.0/23 (cấp cho mạng LAN 1)

2/ 172.16.2.0/23

Xét LAN 2: 200 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=200 \Rightarrow m=8$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-23-8=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

Các subnet:

2.1/ 172.16.2.0/24 (cấp cho mạng LAN 2)

2.2/ 172.16.3.0/24

Xét LAN 3: 50 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=50 \Rightarrow m=6$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-24-6=2

$\Rightarrow$ số subnet = $2^n = 2^2 = 4$

Các subnet:

2.2.1/ 172.16.3.0/26 (Cấp cho mạng LAN 3)

2.2.2/ 172.16.3.64/26

2.2.3/ 172.16.3.128/26

2.2.4/ 172.16.3.192/26

Xét LAN 4: 20 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=20 \Rightarrow m=5$

$\Rightarrow$n = 32-số bit phần mạng – m = 32-26-5=1

$\Rightarrow$ số subnet = $2^n = 2^1 = 2$

Các subnet:

2.2.2.1/ 172.16.3.64/27 (Cấp cho mạng LAN 4)

2.2.2.2/ 172.16.3.96/27

Xét mạng WAN 1, WAN 2, WAN 3: có 2 host

Tương tự ta phải xem mượn bao nhiêu bit thì phù hợp.

Điều kiện: $2^m-2>=2 \Rightarrow m=2$

$\Rightarrow$ n = 32-số bit phần mạng – m = 32-27-2=3

$\Rightarrow$ số subnet = $2^n = 2^3 = 8$

Các subnet:

2.2.2.2.1/ 172.16.3.96/30 (cấp cho mạng WAN 1)

2.2.2.2.2/ 172.16.3.100/30 (cấp cho mạng WAN 2)

2.2.2.2.3/ 172.16.3.104/30 (cấp cho mạng WAN 3)

v.v…

Bảng chia subnet theo VLSM:

Địa chỉ mạng ban đầu	**LAN 1**	**LAN 2**	**LAN 3**	**LAN 4**	**WAN 1,2,3**
172.16.0.0/22	**172.16.0.0/23**				
	172.16.2.0/23	**172.16.2.0/24**			
		172.16.3.0/24	**172.16.3.0/26**		
			172.16.3.64/26	**172.16.3.64/27**	
				172.16.3.96/27	**172.16.3.96/30**
					172.16.3.100/30
					172.16.3.104/30

Bảng thông tin cụ thể của các mạng con:

Mạng con	Địac chỉ subnet được cấp	Subnet mask	Khoảng địa chỉ có thể sử dụng	Địa chỉ broadcast
LAN 1	172.16.0.0	255.255.254.0	172.16.0.1 – 172.16.1.254	172.16.1.255
LAN 2	172.16.2.0	255.255.255.0	172.16.2.1 – 172.16.2.254	172.16.2.25
LAN 3	172.16.3.0	255.255.255.192	172.16.3.1 – 172.16.3.62	172.16.3.63
LAN 4	172.16.3.64	255.255.255.224	172.16.3.65 – 172.16.3.94	172.16.3.95
WAN 1	172.16.3.96	255.255.255.252	172.16.3.97 – 172.16.3.98	172.16.3.99
WAN 2	172.16.3.100	255.255.255.252	172.16.3.101 – 172.16.3.102	172.16.3.103
WAN 3	172.16.3.104	255.255.255.252	172.16.3.105 – 172.16.3.106	172.16.3.107

4.4 | ĐỊA CHỈ IPV6

4.4.1 | GIỚI THIỆU ĐỊA CHỈ IPV6

Địa chỉ IPv6 (Internet protocol version 6) là thế hệ địa chỉ Internet phiên bản mới được thiết kế để thay thế cho phiên bản địa chỉ IPv4 trong hoạt động Internet. Địa chỉ IPv4 có chiều dài 32 bit, biểu diễn dưới dạng các cụm số thập phân phân cách bởi dấu chấm, ví dụ 203.119.9.0. IPv4 là phiên bản địa chỉ Internet đầu tiên, đồng hành với việc phát triển của hoạt động Internet trong hơn hai thập kỷ vừa qua.

Do sự phát triển như vũ bão của mạng và dịch vụ Internet, nguồn IPv4 dần cạn kiệt, đồng thời bộc lộ các hạn chế đối với việc phát triển các loại hình dịch vụ hiện đại trên Internet. Phiên bản địa chỉ Internet mới IPv6 được thiết kế để thay thế cho phiên bản IPv4, với hai mục đích cơ bản:

- Thay thế cho nguồn IPv4 cạn kiệt để tiếp nối hoạt động Internet.
- Khắc phục các nhược điểm trong thiết kế của địa chỉ IPv4.

Địa chỉ IPv6 có chiều dài 128 bít, biểu diễn dưới dạng các cụm số hexa phân cách bởi dấu ::, ví dụ 2001:0DC8::1005:2F43:0BCD:FFFF. Với 128 bít chiều dài, không gian địa chỉ IPv6 gồm 2128 địa chỉ, cung cấp một lượng địa chỉ khổng lồ cho hoạt động Internet.

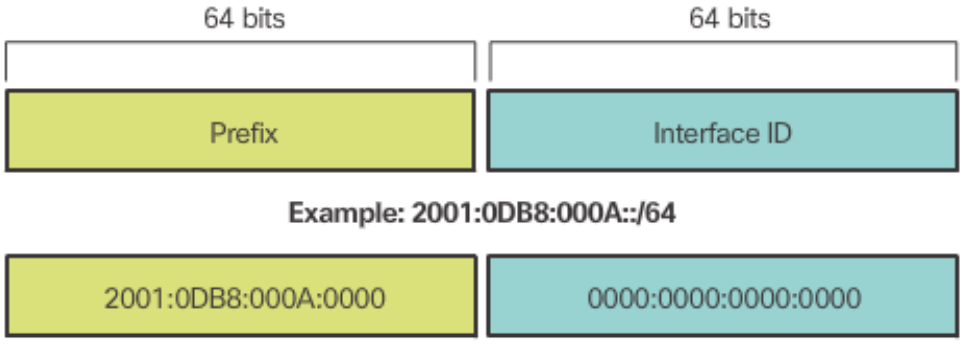
IPv6 được thiết kế với những tham vọng và mục tiêu như sau:

- Không gian địa chỉ lớn hơn và dễ dàng quản lý không gian địa chỉ.

- Khôi phục lại nguyên lý kết nối đầu cuối-đầu cuối của Internet và loại bỏ hoàn toàn công nghệ NAT.
- Quản trị TCP/IP dễ dàng hơn: DHCP được sử dụng trong IPv4 nhằm giảm cấu hình thủ công TCP/IP cho host. IPv6 được thiết kế với khả năng tự động cấu hình mà không cần sử dụng máy chủ DHCP, hỗ trợ hơn nữa trong việc giảm cấu hình thủ công.
- Cấu trúc định tuyến tốt hơn: Định tuyến IPv6 được thiết kế hoàn toàn phân cấp.
- Hỗ trợ tốt hơn Multicast: Multicast là một tùy chọn của địa chỉ IPv4, tuy nhiên khả năng hỗ trợ và tính phổ dụng chưa cao.
- Hỗ trợ bảo mật tốt hơn: IPv4 được thiết kế tại thời điểm chỉ có các mạng nhỏ, biết rõ nhau kết nối với nhau. Do vậy bảo mật chưa phải là một vấn đề được quan tâm. Song hiện nay, bảo mật mạng internet trở thành một vấn đề rất lớn, là mối quan tâm hàng đầu.
- Hỗ trợ tốt hơn cho di động: Thời điểm IPv4 được thiết kế, chưa tồn tại khái niệm về thiết bị IP di động. Trong thế hệ mạng mới, dạng thiết bị này ngày càng phát triển, đòi hỏi cấu trúc giao thức Internet có sự hỗ trợ tốt hơn.

4.4.2 | CẤU TRÚC ĐỊA CHỈ IPV6

IPv6 có tổng cộng là 128 bit được chia làm 2 phần: 64 bits đầu được gọi là Prefix, 64 bits còn lại được gọi là Interface ID.



Hình 4.15: Cấu trúc địa chỉ IPv6

Địa chỉ IPv6 có 128 bit, việc nhớ được địa chỉ này rất khó khăn. Cho nên để viết địa chỉ IPv6, người ta đã chia 128 bit ra thành 8 nhóm (nhóm còn gọi là hextet), mỗi hextet chiếm 16 bits, gồm 4 số được viết dưới dạng số hexa, và mỗi hextet được ngăn cách nhau bằng dấu hai chấm.

Ví dụ: 2001:0DB8:ACAD:0001:0000:0000:0000:0001

Lưu ý: Phần Prefix và Interface-ID trong IPv6 tương ứng với phân Network và phần Host trong IPv4

❖ **Luật rút gọn địa chỉ IPv6:**

- *Các số 0 đứng đầu hextet được quyền lược bỏ.*

Ví dụ 1:

2001:**0**DB8:**000**0:1111:**000**0:**000**0:**000**0:**0**200

→ 2001:DB8:0:1111:0:0:0:200

Ví dụ 2:

2001:0DB8:**000**0:A300:ABCD:**000**0:**000**0:1234

→ 2001:DB8:0:A300:ABCD:0:0:1234

- *Các hextet 0 liên tiếp được thay thế bằng một cụm hai dấu hai chấm "::", và chỉ được thay thế một lần duy nhất cho một địa chỉ.*

Ví dụ 1:

2001:**0**DB8:**000**0:1111:**000**0:**000**0:**000**0:**0**200

→ 2001:DB8:0:1111:**0:0:0**:200

→ 2001:DB8:0:1111::200

Ví dụ 2:

2001:**0**DB8:**000**0::**000**0:ABCD:**000**0:**000**0:**0**100

→2001:DB8::ABCD:0:0:100

Hoặc: 2001:DB8:0:0:ABCD::100

Ví dụ 3:

FF01:0000:0000:0000:0000:0000:0000:0000 → FF01::1

0000:0000:0000:0000:0000:0000:0000:0001 → ::1

0000:0000:0000:0000:0000:0000:0000:0001 → ::

Không gian địa chỉ IPv6 được quy hoạch theo khối ngay từ đầu. Các khối IP lớm sẽ được cấp cho các cơ quan quản lý IP cấp vùng (các Registry như ARIN hay APNIC,…), các cơ quan này lại chia thành các khối nhơ hơn và cấp xuống cho các ISP, các ISP lại tiếp tục chia nhỏ và cấp xuống cho các doanh nhiệp; cuối cùng , doanh nghiệp sẽ chia nhỏ khối IP được cấp thành các subnet.

Địa chỉ IPv6 không sử dụng subnet mask trong khai báo địa chỉ mà chỉ sử dụng định dạng prefix length.

Ví dụ: 2001:1111:2222:3333:4444:5555:6666:7777/64

4.4.3 | CÁC LOẠI ĐỊA CHỈ IPV6

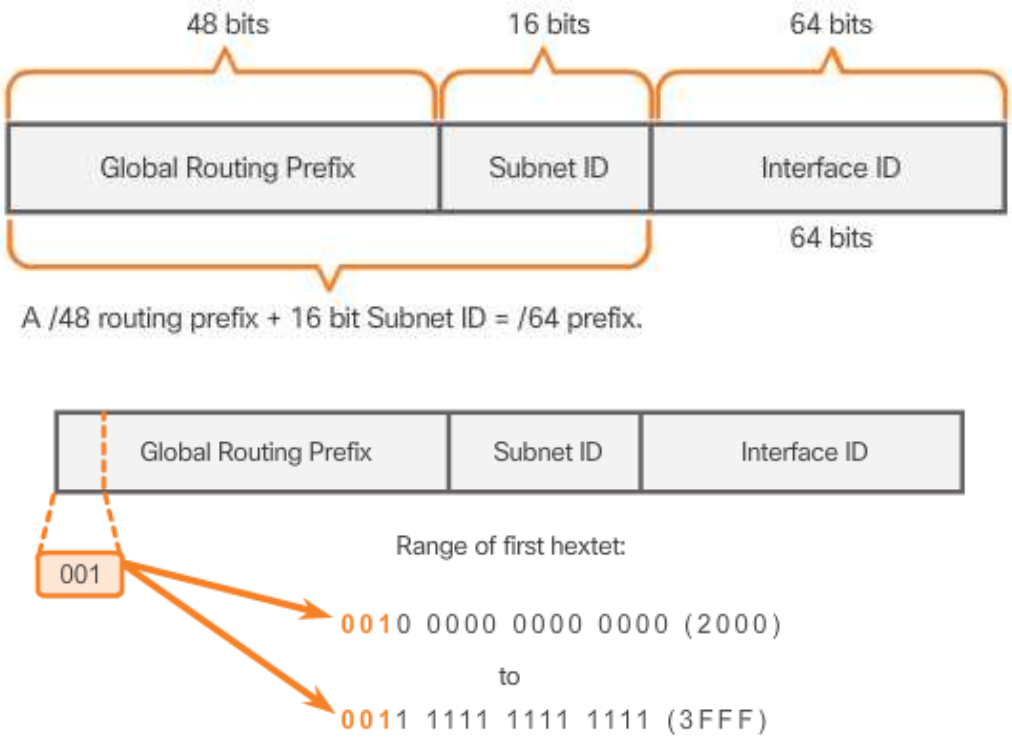
Địa chỉ IPv6 được chia làm ba loại chính: Unicast, Multicast, Anycast.

1. Địa chỉ Unicast

Là địa chỉ sử dụng trên host, được sử dụng để trao đổi dữ liệu unicast. Dãy địa chỉ IPv6 unicast lại chia thành 3 dãy khác nhau:

❖ **Global Unicast**

Là dãy IP được cấp phát và sử dụng cho các host trên Internet, dãy này tương đương với dãy IP public của không gian IPv4. Mọi địa chỉ global unicast đều bắt đầu bằng 3 bit “001”, và như vậy các địa chỉ loại này thuộc về dãy 2000::/3



Hình 4.16: Cấu trúc địa chỉ Global Unicast

❖ Link local Unicast

Địa chỉ Link local là địa chỉ sử dụng trên nội bộ một đường link, các gói tin với địa chỉ Link local không thể đi ra khỏi một đường link. Các địa chỉ Link local có thể trùng nhau miễn là chúng được đặt trên các link khác nhau.

Các địa chỉ link local thuộc về FE80::/10

❖ Unique Local Unicast

Được định nghĩa trong RFC 4193, là dãy địa chỉ tương đương với dãy IP private trong không gian IPv4. Giống như IPv4 private, địa chỉ Unique local chỉ được sử dụng trong nội bộ mạng doanh nghiệp, có thể sử dụng đi sử dụng lại từ mạng nội bộ này qua mạng nội bộ khác và không được sử dụng trên môi trường Internet

Địa chỉ Unique local là toàn bộ dãy FC00::/7.

Trước đây dãy này có tên là Site local, với các IP thuộc prefix FECO::/10. Dãy Unique local ra đời đã thay thế cho dãy Site local.

2. Địa chỉ Multicast

Trong địa chỉ IPv6 không còn tồn tại khái niệm địa chỉ Broadcast. Mọi chức năng của địa chỉ Broadcast trong IPv4 được đảm nhiệm thay thế bởi địa chỉ IPv6 Multicast. Địa chỉ Multicast giống địa chỉ Broadcast ở chỗ điểm đích của gói tin là một nhóm các máy trong một mạng, song không phải tất cả các máy. Trong khi Broadcast gửi trực tiếp tới mọi host trong một subnet thì Multicast chỉ gửi trực tiếp cho một nhóm xác định các host, các host này lại có thể thuộc các subnet khác nhau. Host có thể lựa chọn có tham gia vào một nhóm Multicast cụ thể nào đó hay không (thường được thực hiện với thủ tục quản lý nhóm internet - Internet Group Management Protocol), trong khi đó với Broadcast, mọi host là thành viên của nhóm Broadcast bất kể nó có muốn hay không.

Địa chỉ Multiacast là tất cả các IP nằm trong dãy FF00::/8. Nói cách khác, một địa chỉ IPv6 multicast luôn luôn có byte đầu tiên có giá trị là FF.

Một vài địa chỉ IPv6 multicast thường gặp:

Địa chỉ	**Ứng dụng**
FF02::1	Tất cả các host trên link
FF02::2	Tất cả các router trên link
FF02::5, FF02::6	OSPFv3
FF02::9	RIPng
FF02::A	EIGRPV6

3. Địa chỉ Anycast

Địa chỉ Anycast là địa chỉ đặc biệt có thể gán cho nhiều interface, gói tin chuyển đến điac chỉ Anycast sẽ được vận chuyển bởi hệ thống routing đến interface gần nhất. Hiện nay, địa chỉ Anycast được sử dụng rất hạn chế, rất ít tài liệu nói về cách sử dụng loại địa chỉ này. Hầu như địa chỉ Anycast chỉ được dùng để đặt cho router,

không đặt cho host, lý do là bởi vì hiện nay địa chỉ này chỉ được sử dụng vào mục đích cân bằng tải.

Ví dụ : khi một nhà cung cấp dịch vụ mạng có rất nhiều khách hàng muốn truy cập dịch vụ từ nhiều nơi khác nhau, nhà cung cấp muốn tiết kiệm nên chỉ để một server trung tâm phục vụ tất cả, họ xây dựng nhiều router kết nối khách hàng với server trung tâm, khi đó mỗi khách hàng có thể có nhiều con đường để truy cập dịch vụ. Nhà cung cấp dịch vụ đặt địa chỉ anycast cho các interfaces là các router kết nối đến server trung tâm, bây giờ mỗi khách hàng chỉ việc ghi nhớ và truy cập vào một địa chỉ anycast thôi, tự động họ sẽ được kết nối tới server thông qua router gần nhất. Đây thật sự là một cách xử lý đơn giản và hiệu quả.

4.5 | BÀI TẬP CHƯƠNG 4

1. Chuyển đổi các số nhị phân sau thành số thập phân
   a) 01110010 114
   b) 11100111 231
   c) 10000011 131
   d) 00011001 25
2. Chuyển đổi các số thập phân sau thành số nhị phân
   a) 195 11000011
   b) 140 10001100
   c) 120 01111000
   d) 69 01000101
3. Vẽ và giải thích cấu trúc địa chỉ lớp A, B, C. Cho ví dụ.
4. Nhận dạng các địa chỉ private và địa chỉ public trong các ví dụ sau:
   a) 172.16.35.2 pri
   b) 192.168.3.5 pri

c) 192.0.2.15 pub

d) 64.104.0.22 pub

e) 209.165.201.3 pub

f) 192.168.11.5 pri

g) 172.16.30.30 pri

h) 10.55.3.168 pri

5. Cho biết địa chỉ sau đây thuộc lớp nào (lớp A, B, C, D, E) và địa chỉ này có dùng để đặt cho host được không?

a) 150.100.255.255 B-broadcast - No

b) 175.100.255.18 B-Yes X.Y.0.1 X.Y.255.254

c) 195.234.253.0 C-No X.Y.Z.1 X.Y.Z.254

d) 100.0.0.23 A-Yes X.0.01 X.255.255.254

e) 188.258.221.176 No

f) 127.34.25.189 Localhost - No

g) 224.156.217.73 D-No

6. Cho địa chỉ mạng: 203.162.100.0 với subnet mask là 255.255.255.0. Chia địa chỉ trên thành 5 subnet hợp lệ. Ghi ra 5 subnet đó và số host tối đa của một subnet.

7. Cho mạng và số bit mượn. Hãy xác định :

- Số subnet có thể có.
- Số host/subnet.
- Với mỗi subnet, hãy xác định: địa chỉ mạng, địa chỉ host đầu, địa chỉ host cuối, địa chỉ broadcast (nếu số lượng mạng quá nhiều chỉ cần ghi ra một vài mạng đầu và mạng cuối cùng), subnet mask và số prefix.

a) 192.168.2.0/24 mượn 5 bit.

b) 192.168.12.0/24 mượn 3 bit.

c) 172.16.2.0/24 mượn 2 bit

d) 172.16.0.0/16 mượn 3 bit

e) 172.16.0.0/16 mượn 12 bit

f) 10.0.0.0/8 mượn 5 bit

g) 10.0.0.0/8 mượn 10 bit.

h) 10.0.0.0/8 mượn 18 bit

8. Cho các địa chỉ host sau đây. Hãy xác định các địa chỉ subnet tương ứng và cho biết địa chỉ này có thể dùng đặt cho host được không:

a) 192.168.1.130/29 10000010 11111000 10000000 = 128 192.168.1.128 - Yes

b) 172.16.34.57/18

c) 203.162.4.191/28

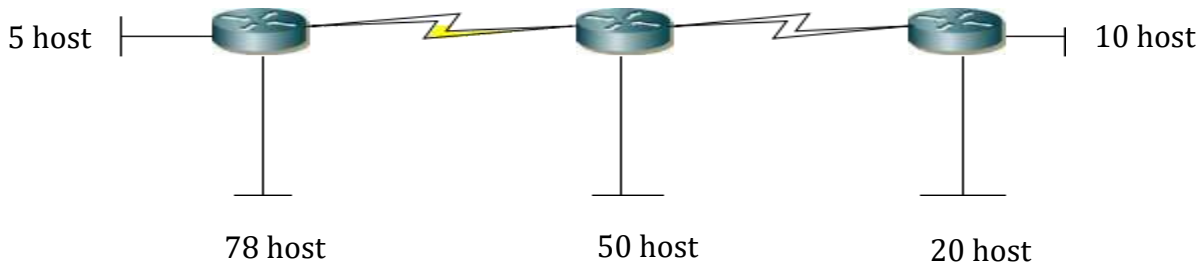
d) 1.1.1.1/30

e) 10.10.10.89/29

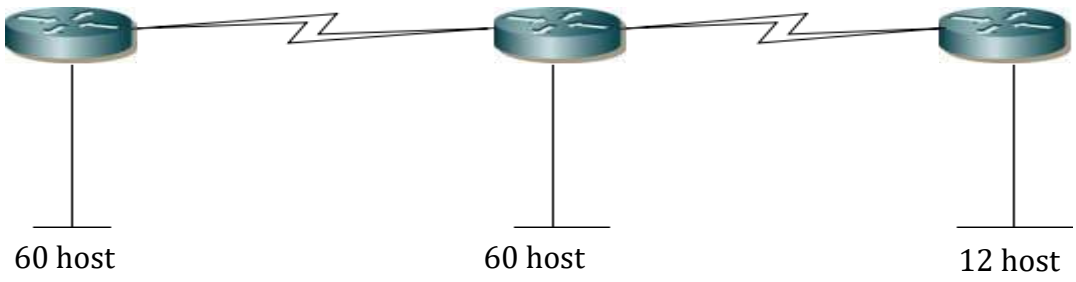
f) 70.9.12.35/30

g) 158.16.23.208/29

9. Cho mạng 172.16.5.0/24. Hãy chia subnet sao cho phù hợp với sơ đồ sau:



10. Cho mạng 192.168.5.0/24. Hãy chia subnet sao cho phù hợp với sơ đồ sau:



11. Trình bày cấu trúc địa chỉ IPv6?

12. Có mấy loại địa chỉ IPv6?

5. THỰC HÀNH THIẾT LẬP MẠNG LAN

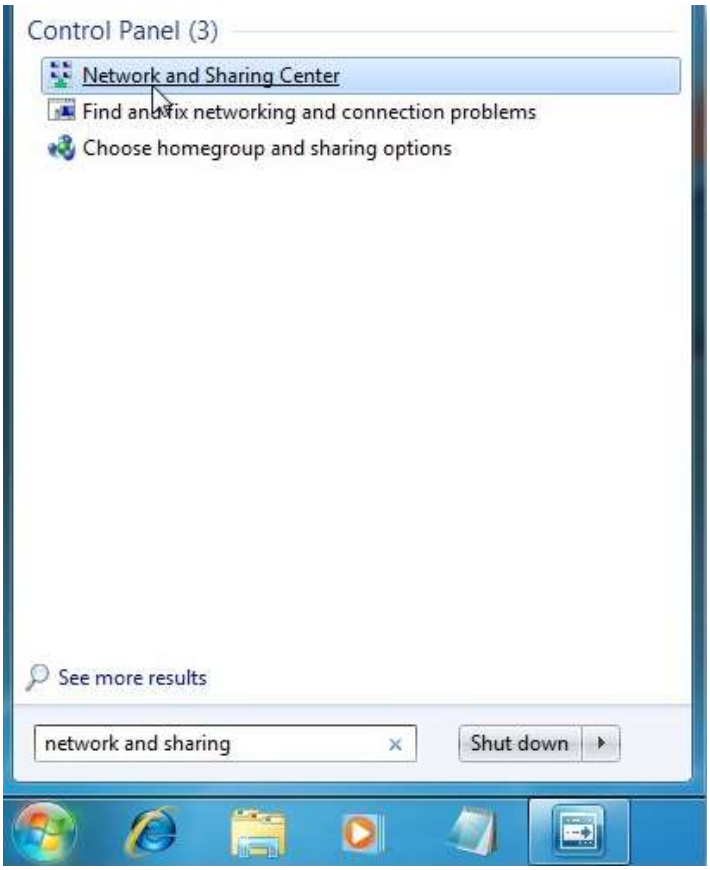
Sau khi học xong chương này, sinh viên có thể:

- Cài đặt và cấu hình được hệ thống mạng trên hệ điều hành Windows
- Thực hiện được việc phân quyền tài nguyên cho người dùng.
- Xác định mối quan hệ giữa các thành phần trong hệ thống mạng

5.1 | CÀI ĐẶT THÔNG TIN CARD MẠNG

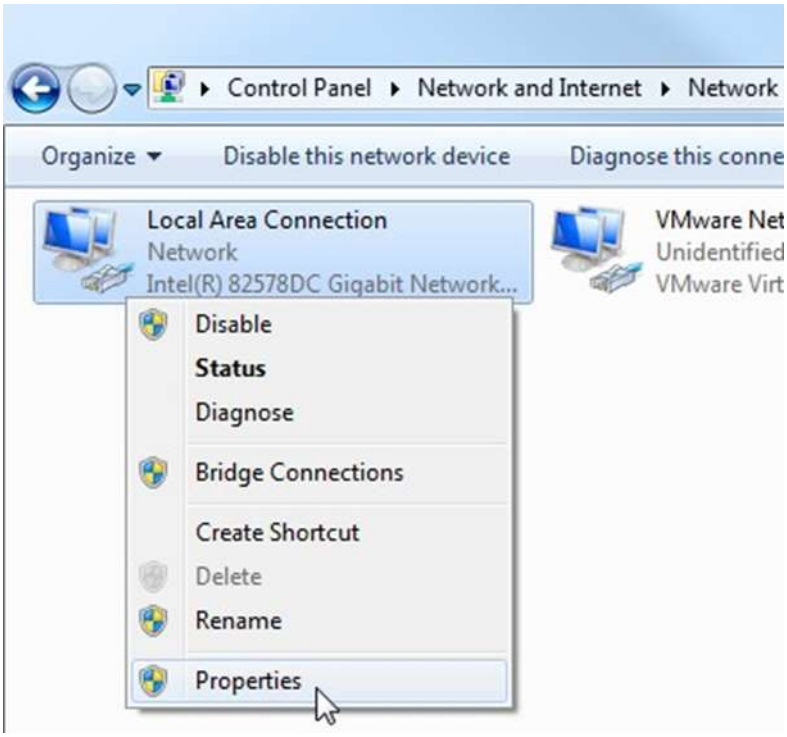
B1: Vào Start sau đó gõ Network and Sharing Center

Hoặc tại cửa sổ RUN gõ ncpa.cpl

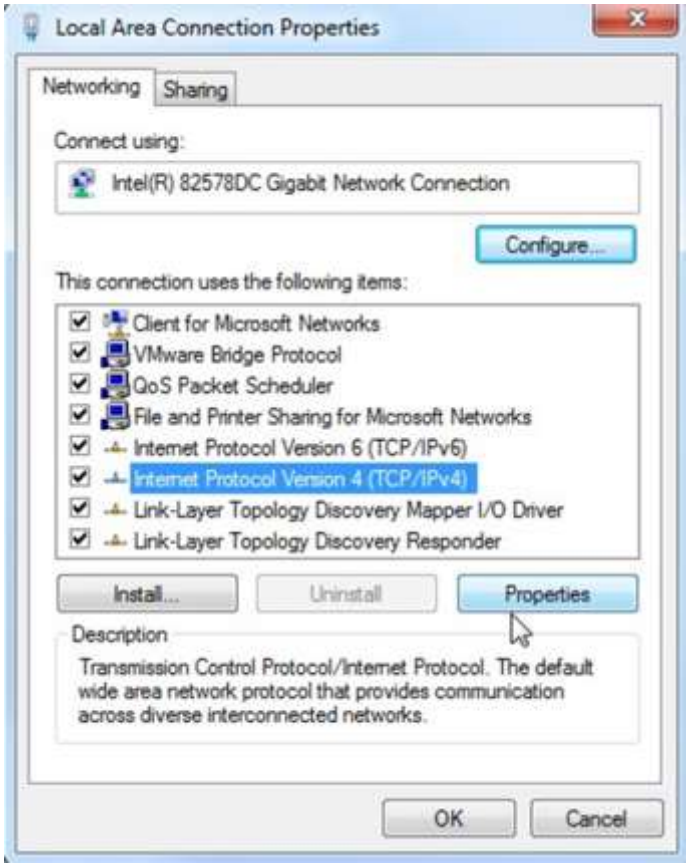


Sau đó, khi Network and Sharing Center mở ra, nhấp vào *Change Adapter Settings.*

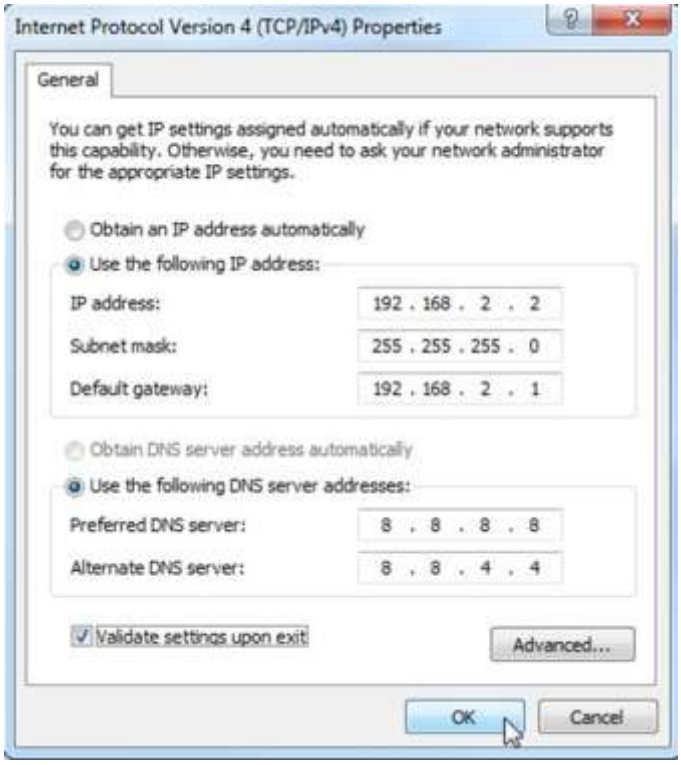
Nhấp chuột phải vào card mạng của → chọn Properties



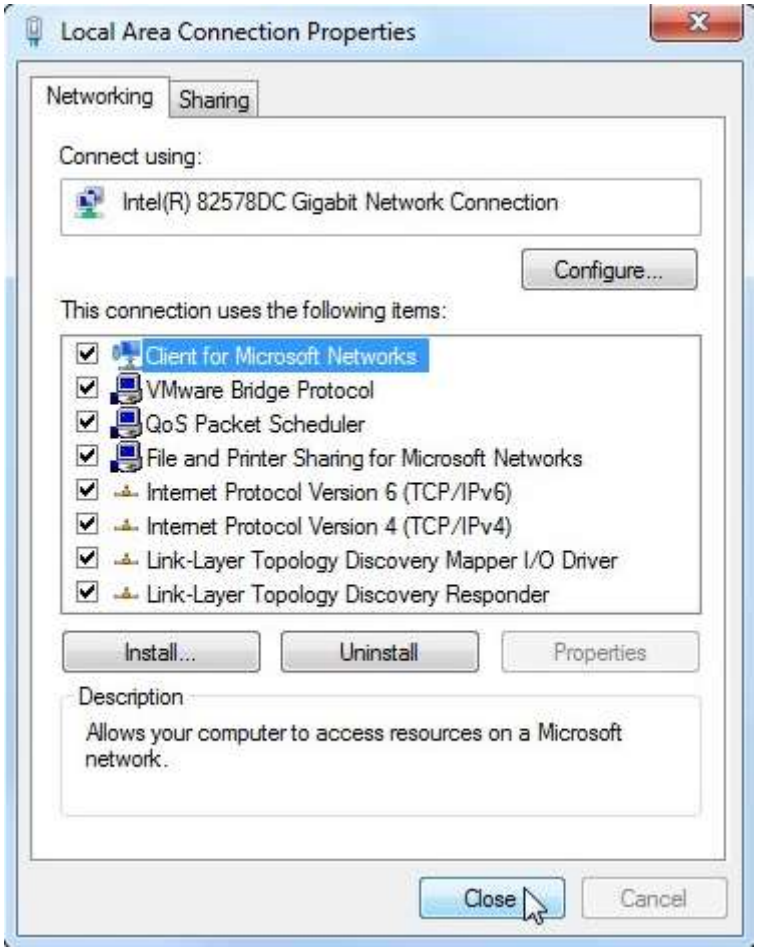
Trong Local Area Connection Properties cửa sổ nổi bật *Internet Protocol Version 4 (TCP/IPv4)* sau đó nhấn nút Properties.



B2: Điền đầy đủ các thông số về địa chỉ IP, Subnet, Default getway như hình dưới đây:



Bây giờ đóng trong cửa sổ Local Area Connections Properties.

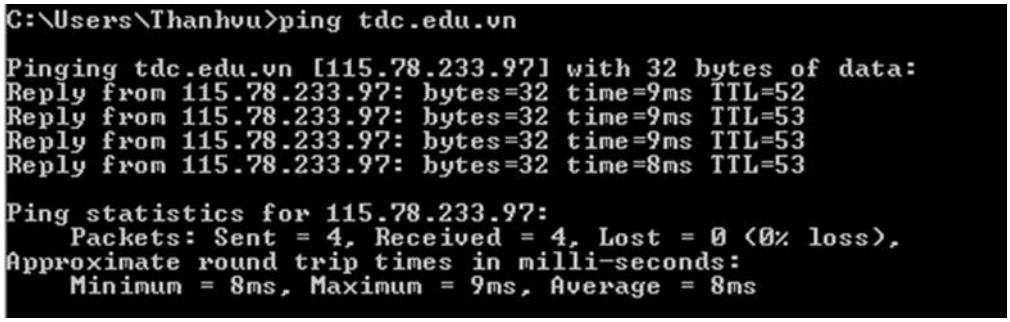


Bây giờ có thể mở cửa sổ lệnh và làm một *ipconfig* để xem cài đặt adapter mạng đã được thay đổi thành công.

5.2 | CÁC LỆNH KIỂM TRA HỆ THỐNG MẠNG

Lệnh **Ping và Tracert** là hai công cụ có thể được dùng khi ta muốn kiểm tra tình trạng kết nối mạng.

- Lệnh **ping** để kiểm tra xem một máy tính có thể kết nối tới một máy chủ (hay một máy bất kỳ trong mạng LAN) cụ thể nào đó hay không, và ước lượng khoảng thời gian trễ trọn vòng đi và về của gói dữ liệu cũng như tỉ lệ các gói dữ liệu có thể bị mất giữa hai máy.



Lệnh ipconfig kiểm tra thông tin card mạng(có thể thêm tham số /more để xem hướng dẫn)

Khi nhận được thông báo có dạng như trên thì có nghĩa là lệnh ping đã thực hiện thành công và hệ thống **không có lỗi:**

- **Địa chỉ IP** sau từ "Reply from" cho biết máy nào đang gửi thông điệp trả lời.
- **bytes=32** là kích thước của gói tin ICMP được gửi đi.
- **time=9ms** thời gian của quá trình hồi đáp
- **TTL=52**,... là giá trị "time to live" (thời gian sống) của gói tin ICMP. Hết thời gian này thì gói tin sẽ bị hủy.

Trong mạng LAN dùng lệnh ping địa chỉ IP của máy khác

Nếu nhận thông báo là **Request time out:**

Nếu không kết nối được với máy đích thì kết quả ping sẽ hiển thị thông báo là "Request timed out". Có nghĩa là **không có hồi đáp trả về**, nguyên nhân gây ra lỗi như sau:

- Thiết bị định tuyến Router bị tắt.
- Địa chỉ máy đích không có thật hoặc máy đích đang bị tắt, hoặc cấm ping.

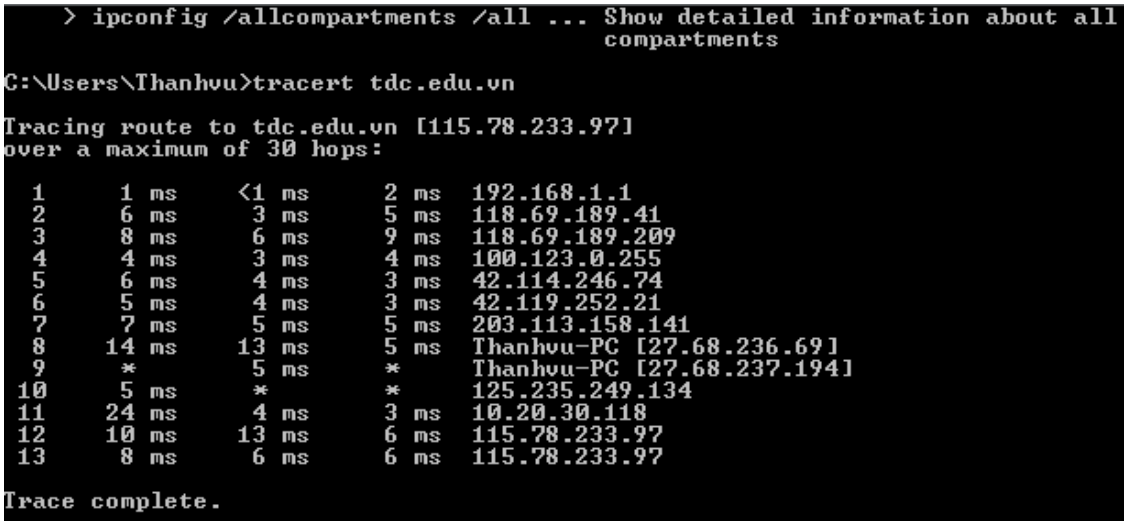
- Nếu máy đích khác đường mạng với máy nguồn thì nguyên nhân có thể do không có định tuyến ngược trở lại máy nguồn. Lúc này, nếu máy đích đang chạy, có thể kiểm tra đường đi về của gói tin bằng cách xem lại thông số **Default Gateway** trên máy đích, máy nguồn và router kết nối các đường mạng.

Nếu nhận thông báo là **Destination host unreachable**

Thông báo cho biết **không thể kết nối đến máy đích.**

Nguyên nhân gây ra lỗi này có thể là do kết nối vật lý của máy tính như cáp mạng bị đứt, không gắn cáp vào card mạng, card mạng bị tắt, Driver card mạng bị hư, chưa bật wifi, …

- Lệnh **Tracert** dùng để kiểm tra đường đi của gói tin tới máy đó.



Dòng 1 : là dòng kết nối giữa modem và máy tính, độ trễ tốt nhất là **1ms 1ms 1ms** ! Nếu cao hơn hoặc xuất hiện dấu * hay **Request timed out** thì kết nối modem và máy có vấn đề !

Dòng 2: nếu vẫn là **ip private** thì là kết nối giữa modem và modem đánh giá tương tự dòng 1. Nếu là **ip public** thì là kết nối giữa modem và mạng của ISP (nhà cung cấp mạng), độ trễ tốt nhất nên trong khoảng **10-40 ms** ! Cao hơn khoảng này hoặc xuất hiện dấu * hay **Request timed out** thì kết nối modem và mạng ISP có vấn đề !

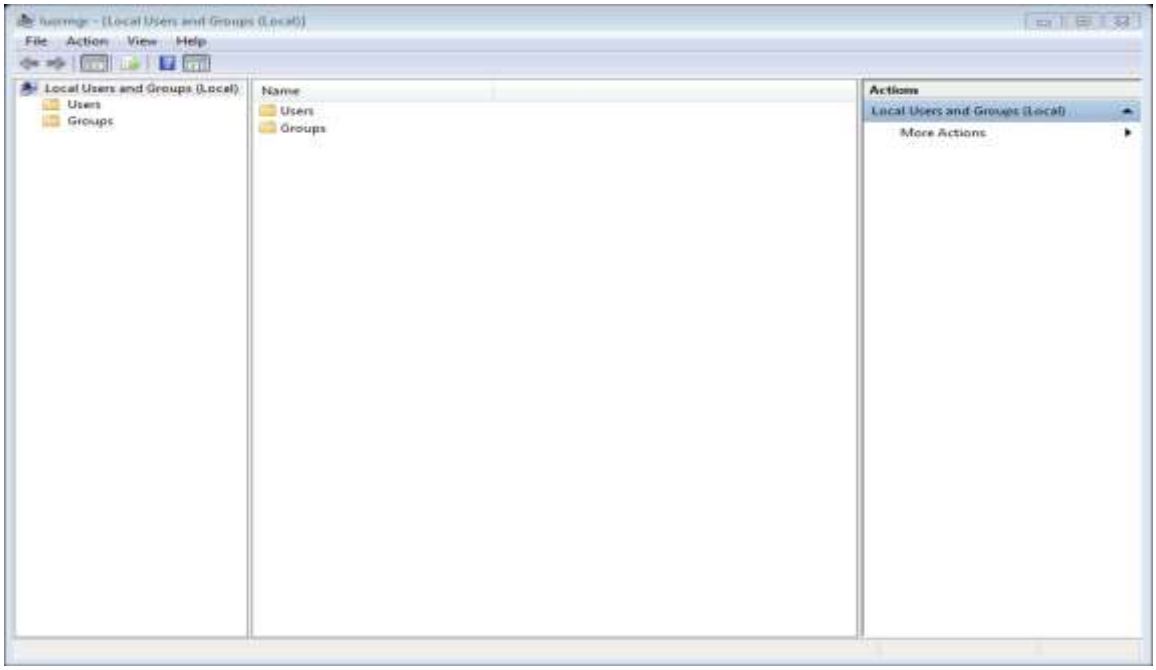
Dòng 3 trở đi tới **trace complete** : là kết nối trong mạng giữa các ISP với nhau , nếu xuất hiện dấu * hay **Request timed out** thì kết nối trong mạng ISP có vấn đề!

5.3 | LOCAL USER ACCOUNT & GROUP ACCOUNT

User và Group là những thành phần cơ bản để quản lý máy tính và tài nguyên trên máy tính. Tùy vào mức độ được cấp quyền mà người dùng có quyền truy xuất vào những tài nguyên nào trên máy tính, hoặc trong hệ thống mang. Nội dung này, chúng ta tìm hiểu vế cách tạo và quản lý user trên máy cục bộ (local host).

Khởi động trình quản lý Local user and Group, có 3 cách:

- **Cách 1**: Click chuột phải lên Computer (trên Windows 7,Windows 8, server 2008, Server 2008 R2, Windows server 2012, Vista), This PC (Windows 8.1, server 2012 R2) hoặc My Computer (trên Windows XP, Wondows server 2003) → chọn Manager →System tools → Chọn Local User and Group.
- **Cách 2**: Vào Run → MMC, sau khi vào cửa sổ MMC vào file Add/Remove Snap-in (hoặc nhấn tổ hợp phím Ctrl+M) → chọn Computer management → nhấn add → chọn Local computer → chọn Fnish → chọn OK →System tools → Local User and Group
- **Cách 3**: Vào Run gõ **lusrmgr.msc**



User account (hay còn gọi tắt là User) – Tài khoản người dùng:

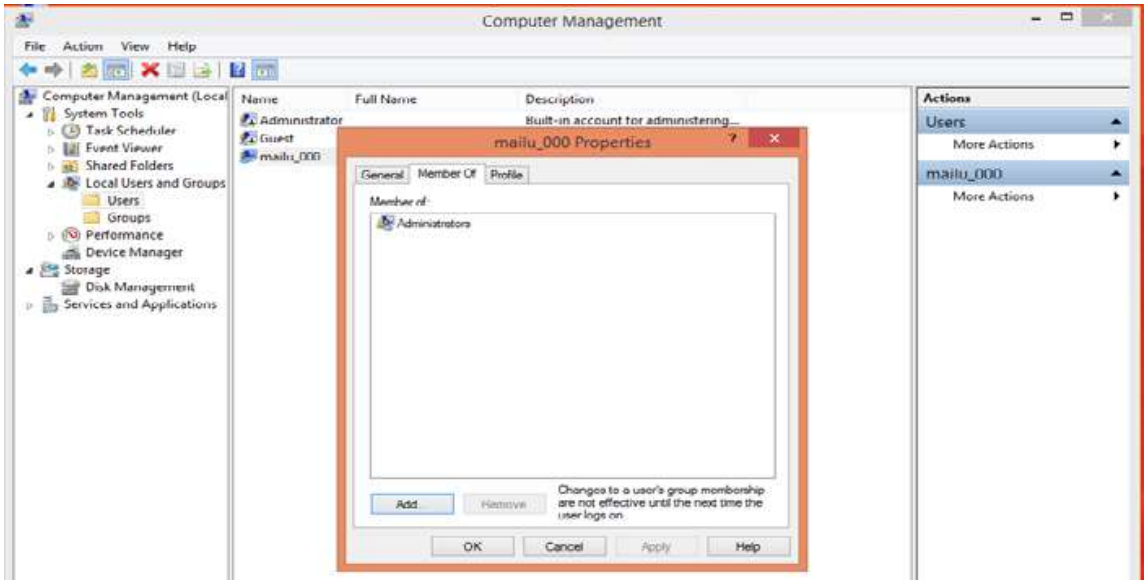
- User account là thông tin dối tượng bao gồm thông tin xác định người dùng của hệ điều hành Windows, dùng để đăng nhập vào máy tình, phân quyền sử dụng, áp đặt những chính sách bảo mật… Thông tin tồi thiểu của User account là User name và Password.

- Local user account (người dùng cục bộ).

- Là tài khoản được lưu trong file SAM (được tạo ra trong Users and Groups có trong Computer Management). Nó chỉ có giá trị trên máy chứa thông tin tài khoản đó.

- Có hai user account được tạo sẵn (Built-in account) là Administrator và Guest. Tài khoản Aministrator là tài khoản có quyền cao nhất trong hệ thống. Tài khoản Guest thường bị Disable.

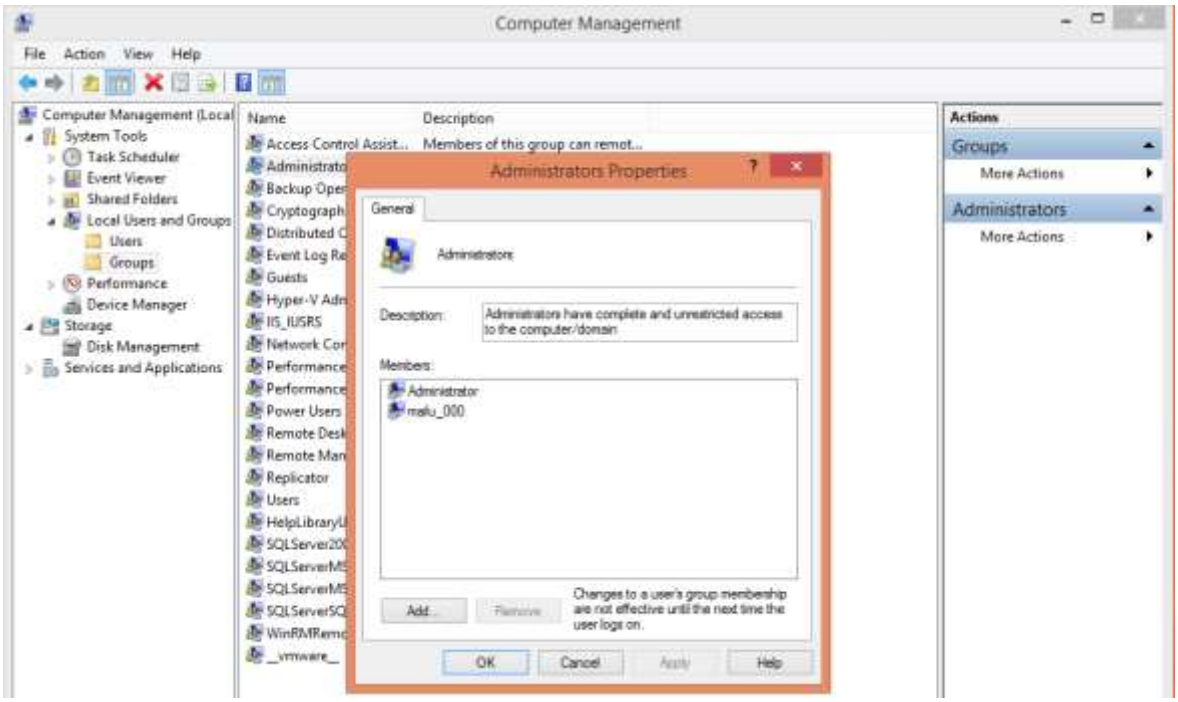
- Built-in account không thể xóa, nhưng có thể disable. Riêng user Administrator bị disabale thì vẫn có thể login vào chế độ Safe Mode, vì vậy việc tạo Password của user này là rất quan trọng để bảo mật cho hệ thống.



Group (nhóm người dùng)

Là tập hợp những user account có những tính chất nào đó (như có quyền làm gì, trên tài nguyên nào của hệ thống…) để giúp cho việc phân quyền trở nên dễ dàng hơn.

- Local group (nhóm người dùng trên máy cục bộ): Là nhóm chỉ có giá trị trên máy chứa nó và được lưu trữ trong file SAM



Những điều cần lưu ý:

- Khi cài đặt Windows, lúc hoàn tất cài đặt Windows cho phép tạo một user. User này có quyền tương đương Administrator, chúng ta nên sử dụng user này.

- User Administrator chỉ nên dùng nó ở những trường hợp cấp thiết, như quên mật khẩu của người dùng thì có thể vào để reset password, xóa profile người dùng khi có lỗi… không nên sử dụng user này như một user thông thường và phải có mật khẩu cho User Administrator.

5.4 | SHARE PERMISSION

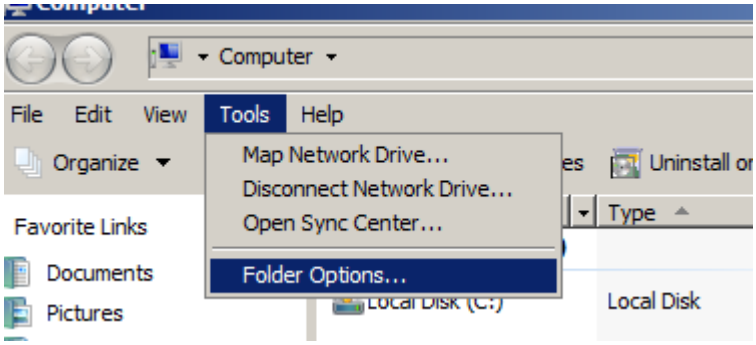
Việc chia sẻ các tài nguyên trên mạng là điều không thể thiếu trong bất kỳ hệ thống mạng nào, tuy nhiên việc chia sẻ này còn tùy thuộc vào nhu cầu người sử dụng & ý đồ của nhà quản trị mạng.

Ví dụ: Trong công ty có nhiều phòng ban và các phòng ban trong công ty có nhu cầu chia sẻ tài nguyên cho nhau tuy nhiên nhà quản trị mạng muốn không phải phòng ban nào cũng có thể truy cập vô tư các dữ liệu của phòng ban khác.

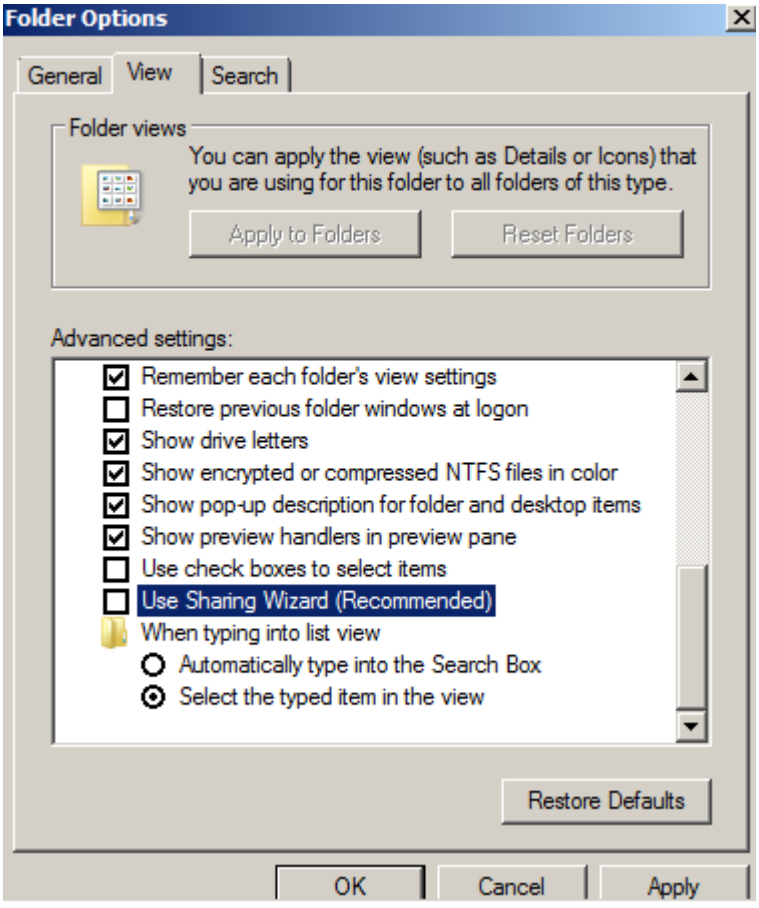
Chẳng hạn các nhân viên trong phòng kinh doanh thì có thể truy cập dữ liệu của phòng mình và phòng kỹ thuật thoải mái, nhưng với các nhân viên trong phòng kỹ thuật chỉ được phép truy cập tài nguyên trong phòng mình mà thôi và không được phép truy cập các tài liệu từ phòng kinh doanh. Tính năng **Sharing and Sercurity..** sẽ giúp ta giải quyết các yêu cầu trên.

Kể từ **Windows Vista** trở đi trình **Sharing** của **Windows** có giao diện khác hẳn với các phiên bản trước đó giao diện **Wizard** mới này rất thân thiện với người dùng phổ thông tuy nhiên rất khó khăn cho nhà quản trị mạng. Chính vì thế trước khi thực hiện **Share Folder** ta cần phải tùy chỉnh lại **Windows** chút xíu để trở lại giao diện **Sharing Classic** ngày nào.

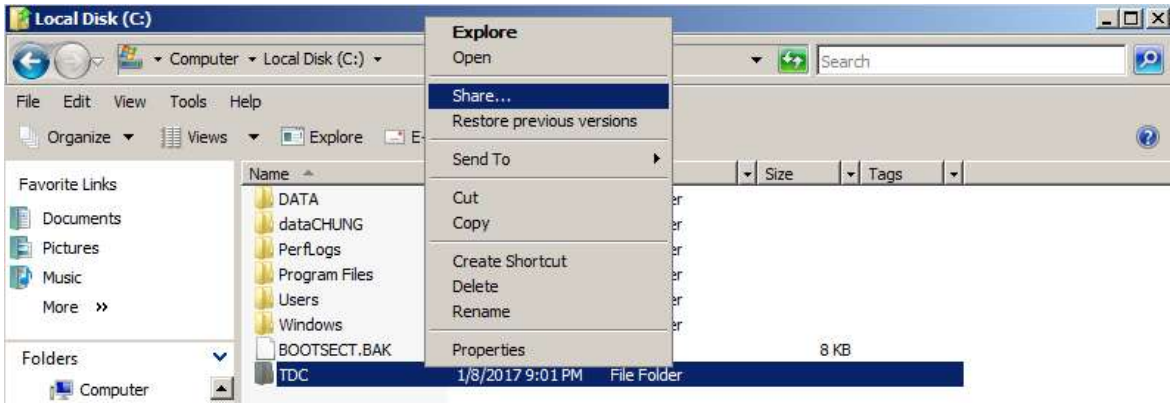
Đầu tiên, mở trình **Windows Explorer** ra chọn O**rganize** → **Folder and Search Options**



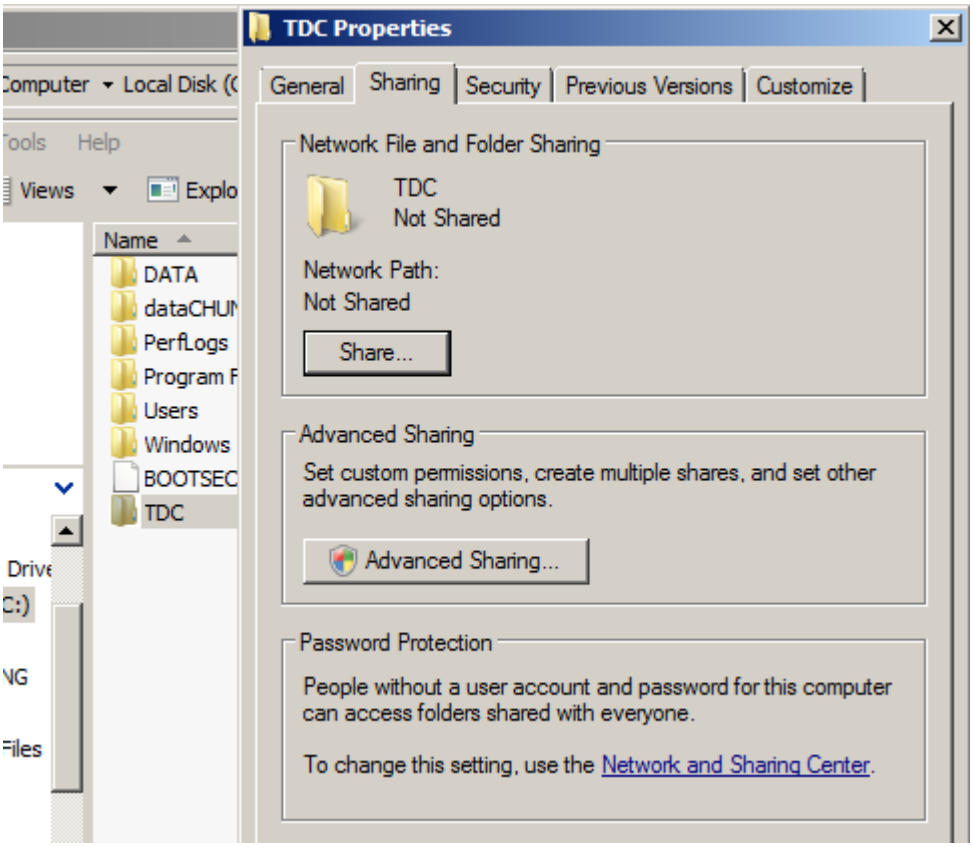
Chọn Tab **View** sau đó click bỏ chọn mục **Use Sharing Wizard (Recommended)**



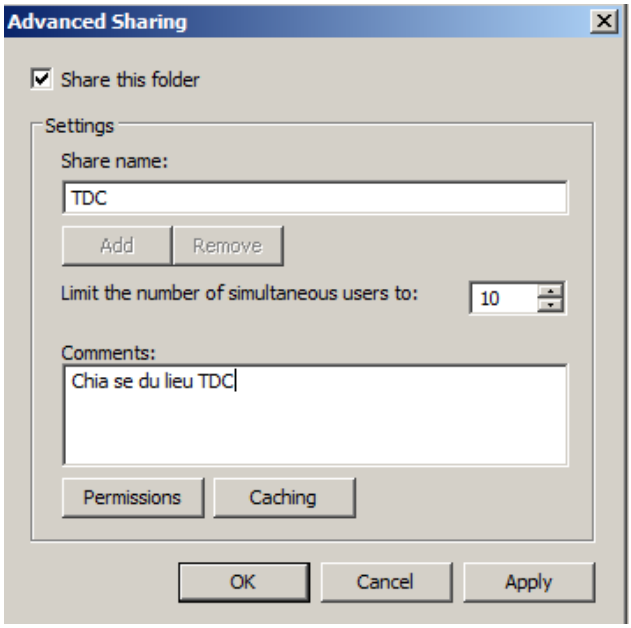
Trong **Windows server 2008** để chia sẻ một thư mục, ta nhấp chuột phải vào thư mục cần share chọn **Properties**



Nhấp chọn **Advanced Sharing...**



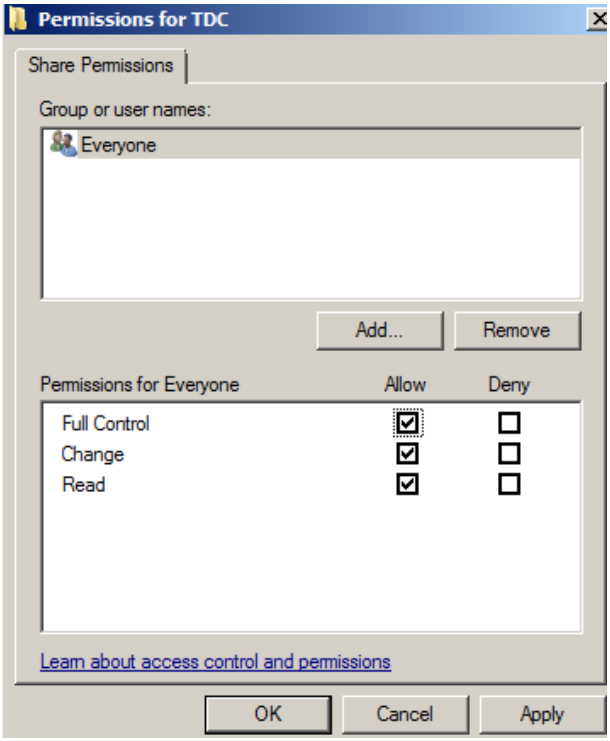
Ở ô **Share Name** máy sẽ tự lấy tên default là tên thư mục hiện hành có thể chỉnh sửa tên này tùy ý



Để phân quyền cho User truy cập → click chọn mục **Permissions**

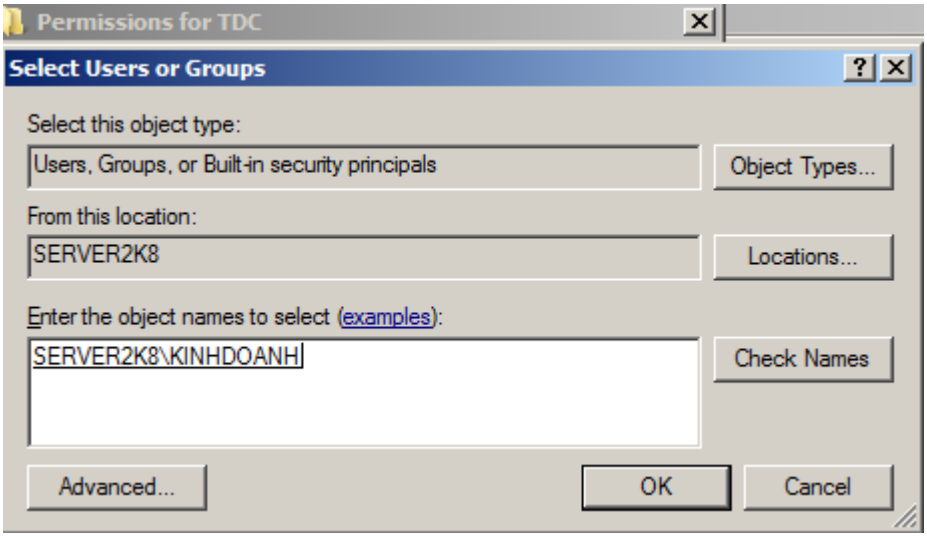
Trong này, chúng ta có thể giới hạn quyền cho từng group hoặc user với các quyền được giới hạn bởi các mục **Allow & Deny.**

Với các tùy chọn là **Allow**: User có quyền truy cập tài nguyên với quyền hạn tương ứng. Với các tùy chọn là **Deny**: User **không** có quyền truy cập tài nguyên với quyền hạn tương ứng.

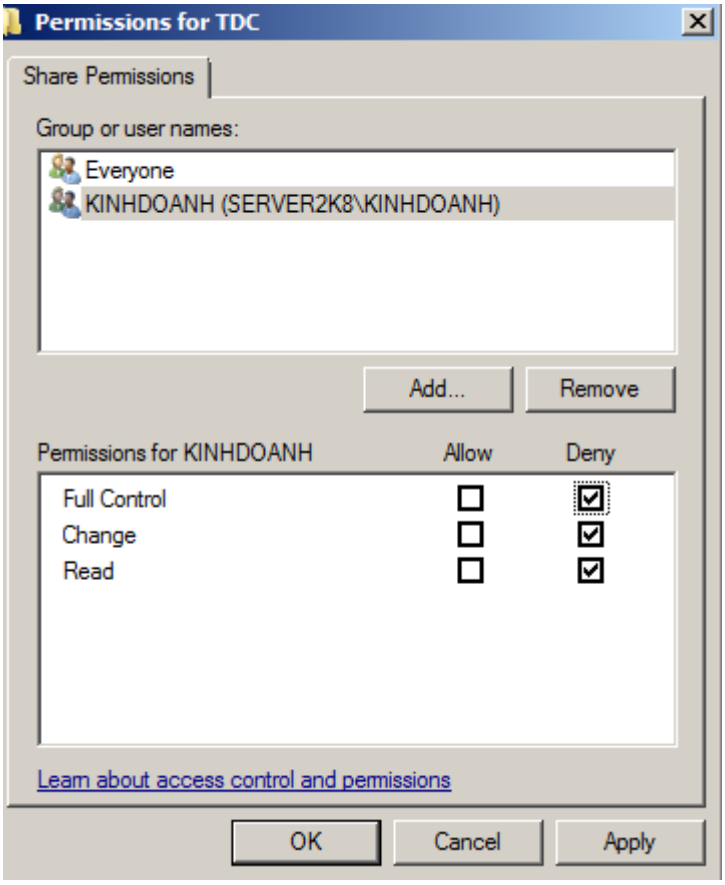


Trong ví dụ này **Group User** có toàn quyền (**Allow** tất cả các quyền **Read, Change, Full Control**…) nghĩa là **Group** này có quyền truy xuất tài nguyên, chỉnh sửa, xóa từ thư mục **Share**. Để thực hiện phân quyền cho các Group thi ta cần **Deny** tất cả các quyền của **Group User** này.

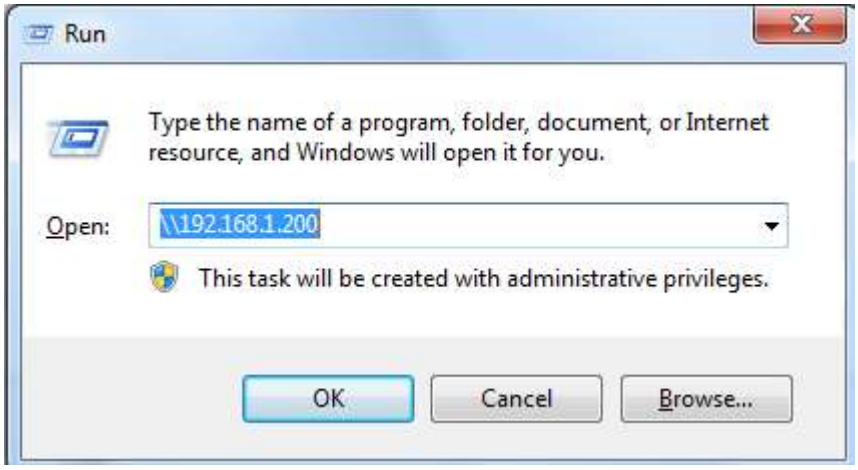
Sau khi Deny tất cả các quyền của **Group User** → nhấp nút **Add** thể thêm **Group** hoặc **User** vào.



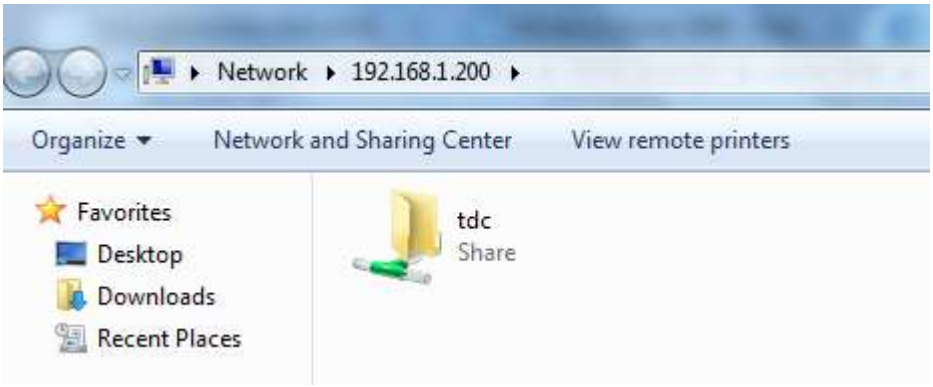
Trong này Add thêm Group **Kinh Doanh** và cũng Set quyền cho Group này là **Deny** tất cả mọi quyềnTương tự dAdd thêm Group **Ky Thuat** và Set quyền cho Group này là **Allow** tất cả mọi quyền



Để truy cập dữ liệu từ máy khác nhập **\\Địa chỉ IP\ShareName**

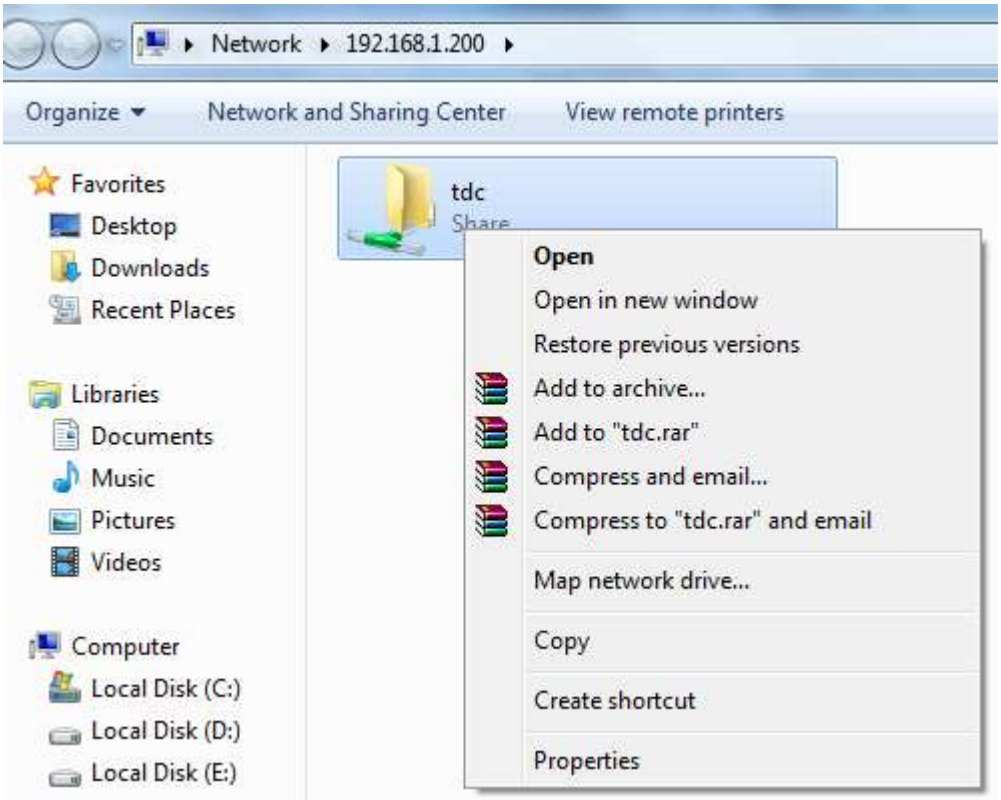


Kết quả sẽ thấy được thư mục TDC đã share

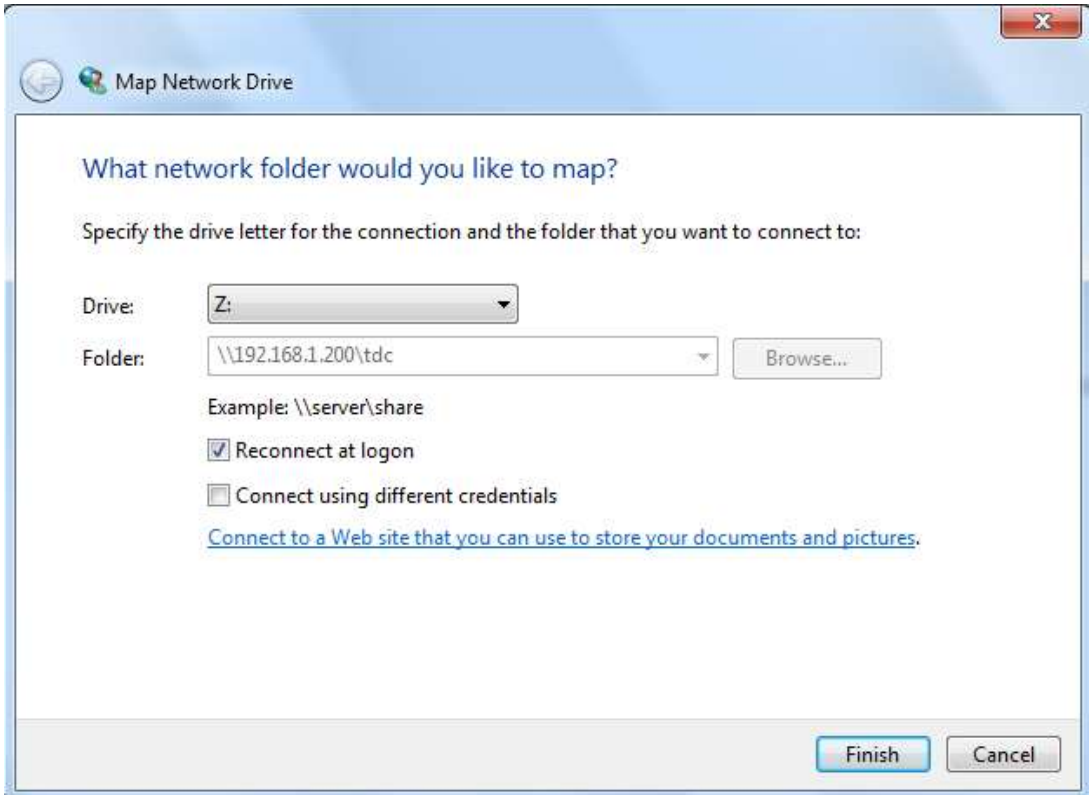


Để tạo một thư mục mà không muốn cho ai thấy (chỉ có gõ lệnh mới vào được) thì thêm dấu **$** vào ngay sau **Share Name**. Khi đó truy cập từ máy khác vào phải nhập là **\\Địa chỉ IP\ShareName$**

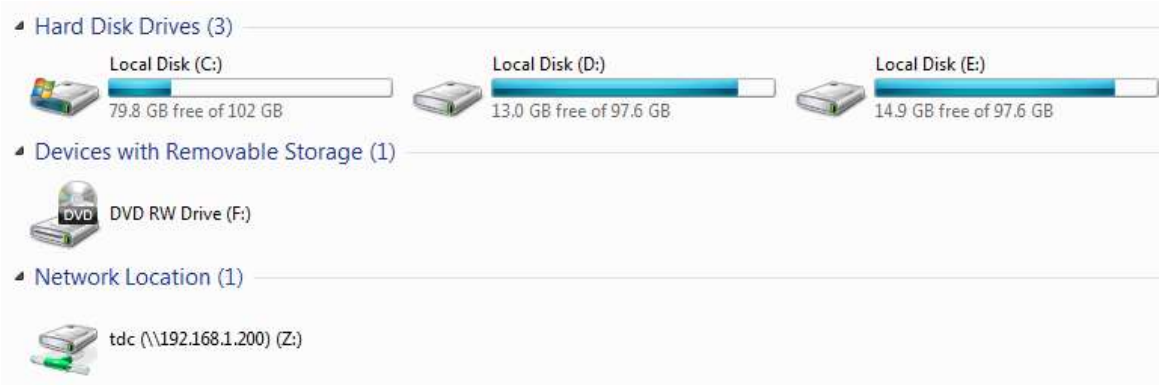
Để tránh phải mất công nhập dòng lệnh **\\[IP máy tới]\[thư mục share]** chúng ta có thể ánh xạ ổ đĩa đối với các thư mục **Share** thường xuyên truy cập bằng cách nhấp phải vào thư mục đã Share cần ánh xạ và chọn **Map Network Drive…**



Trong cửa sổ **Map Nerwork Drive** hiện ra → chọn tên ổ đĩa ánh xạ và click **Finish**



Bây giờ vào **Computer** sẽ thấy xuất hiện thêm ổ đĩa mới (Ổ đĩa ánh xạ) Nhấp vào đấy sẽ đi đến ngay thư mục vừa ánh xạ.



5.5 | SECURITY PERMISSION (NTFS FILE PERMISSION)

Security permission(NTFS file permission) xác định người dùng nào có thể xem hoặc cập nhật được các tập tin. Ví dụ sử dụng NTFS file permission cho phép phòng quản lý nhân sự được truy cập vào tập tin chứa các thông tin lí lịch của nhân viên trong khi đó không một nhân viên nào ở phòng khác có thể truy cập đến những tập tin này.

Mặc định NTFS file permission được sử dụng cho người dùng và các thư mục trong hệ thống. Những mặc định này dành cho 3 kiểu tập tin sau:

- **User files**: Những người dùng có toàn quyền kiểm soát đối với tập tin của họ. Những quản trị viên cũng có toàn quyền kiểm soát. Những người dùng khác ngoại trừ quản trị viên thì không thể đọc hoặc ghi lên những tập tin đó.
- **System files**: Người dùng có thể đọc, nhưng không thể ghi. Những tập tin này nằm trong thư mục hệ thống %SystemRoot% và các thư mục con trong đó.
- **Program files**: giống như permission trong các tập tin hệ thống, lưu trữ trong thư mục %ProgramFIles% ,cho phép người dùng chạy các ứng dụng và chỉ cho phép quản trị viên cài đặt ứng dụng. Những người dùng có quyền đọc và quản trị viên có toàn quyền kiểm soát.

Thêm vào đó, cũng có những thư mục mới được tạo ra ở ổ đĩa hệ thống và được gán toàn quyền kiểm soát đối với quản trị viên, người dùng chỉ có thể xem.

Trên File server, chúng ta cần gán quyền cho nhóm của người dùng để cho phép họ cộng tác làm việc cùng nhau. Ví dụ chúng ta có thể tạo một thư mục cho tất cả nhân viên thuộc nhóm Marketing được đọc và cập nhật nhưng những nhân viên bên ngoài nhóm này không có quyền truy cập. Quản trị viên có thể gán cho người dùng hoặc nhóm một số quyền hạn trên tập tin hoặc thư mục. NTFS PERMISSION bao gồm 6 bộ quyền STANDARD:

- **List Folder Content**: người dùng có thể mở được thư mục nhưng không mở được các tập tin trong đó.
- **Read:** người dùng có thể xem được nội dung trong một thư mục và mở được các tập tin trong đó. Nếu người dùng chỉ có quyền Read mà không có quyền Read & Execute thì họ cũng sẽ không thể thực thi được tập tin.
- **Read & Execute**: ngoài quyền Read như trên, quyền này cho phép người dùng có thể chạy được các ứng dụng, các tập tin.
- **Write**: người dùng có thể tạo những tập tin trong một thư mục nhưng không thể xem được chúng. Quyền này thật sự hữu ích nếu để tạo một thư mục và người dùng có thể đưa các tập tin lên thư mục này và không có quyền truy cập vào các tập tin của người khác cho dù họ thấy tập tin đó.
- **Modify**: những người dùng có thể xem, chỉnh sửa và xóa tập tin hoặc thư mục.

- **Full Controll**: người dùng có quyền này có thể thực hiện bất cứ thao tác nào trên tập tin hoặc thư mục, bao gồm việc tạo, xóa và thậm chí là sửa được quyền đối với những tập tin và thư mục.

Các bước để bảo vệ một file hoặc thư mục với NTFS:

B1. Mở **Windows Explorer.**

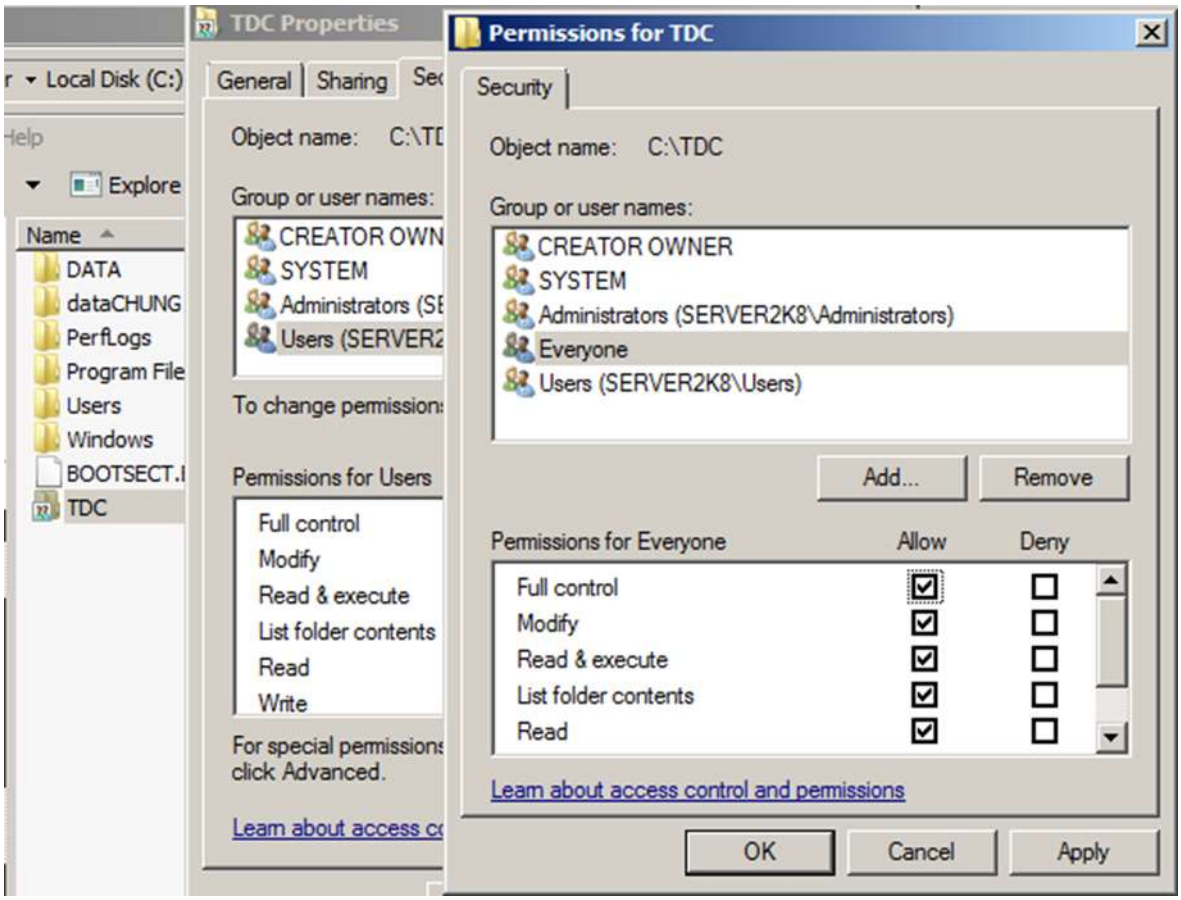
B2. R-click vào một tập tin hoặc thư mục, sau đó chọn **Properties.**

B3. Click vào tab **Security.**

B4. Click **Edit**. Hôp thoại **Permission** hiển thị.

B5. Nếu người dùng muốn cấu hình truy cập không hiển thị trong danh sách **Group or user names** → có thể click Add, sau đó nhập tên tài khoản và click **OK.**

B6. Ví dụ muốn cho tất cả người dùng có toàn quyền trên thư mục TDC→Add thêm Everyone → Đánh dấu chọn full control trong **Permission for TDC.**



B7. Thực hiện lại bước 5 và 6 cho những người dùng khác.

B8. Click OK hai lần để hoàn tất.

Lưu ý: Nếu cấu hình Full Control cho một người dùng trong nhóm nào đó nhưng lại hủy quyền Full Control đối vối nhóm đó thì người dùng đó cũng không có

quyền Full Control. Ví dụ, user cntt1 là nhân viên thuộc nhóm KhoaCNTT, được quản trị viên cấu hình Full Control. Tuy nhiên nếu quản trị viên đó hủy quyền Full Control đối với nhóm KhoaCNTT thì user cntt1 sẽ mất quyền Full Control.
Khung bị mờ là bộ quyền Spesial permissions (Chưa nói đến trên bộ quyền Standard)
Để phân quyền chi tiết hơn → SPECIAL PERMISSION (bao gồm13 BỘ QUYỀN)

- Traverse Folder /Execute File: Quyền nhảy cấp (tại thư mục này không có quyền nhưng lại có quyền tại thư mục bên trong)
- List Folder / read Data: Đi vào thư mục và đọc tài nguyên trong thư mục đó
- Read Attributes: Đọc thuộc tính. (thuộc tính Read, System, Hide, Achive...)
- Read Extended Attributes: Đọc thuộc tính mở rộng. (thuộc tính nén, mã hóa v.v...)
- Create Files / Write Data: Tạo tài nguyên và chỉnh sửa tài nguyên.
- Create Folders / Append Data: Tạo folder và ghi nối tiếp vào dữ liệu trên file.
- Write Attributes: Ghi thuộc tính (thêm bớt dữ liệu trên file)
- Write Extended Attributes: Ghi thuộc tính mở rộng (thêm bớt dữ liệu trên file nén, mã hóa...)
- Delete Subfolders and Files: Xóa folder và file bên trong subfolder.
- Delete: Xóa tài nguyên.
- Read Permissions: Đọc được bộ quyền.
- Change Permission: Cho phép thay đổi lại quyền.
- Take Ownership: Cướp quyền khi user(Adminisrator) đó không có quyền trên tài nguyên.

Ngoài ra còn có 7 thành phần trong APPLY ONTO liên kết đến 13 bộ quyền special

- This folder only: Chỉ có quyền tại Folder này (không có quyền trong subfolder)
- This folder, Subfolder and Files: Chỉ có quyền tại folder này nhưng file tại folder này không có quyền + (có quyền bên trong subfolder + trên những file bên trong subfolder)
- This folder and subfolder: Chỉ có quyền tại folder và subfolder
- This folder and files: Chỉ có quyền tại folder này và file tại folder này.
- Subfolder and file only: Chỉ có quyền tại subfolder và file bên trong subfolder.
- Subfolder only: Chỉ có quyền tại subfolder
- Files only: Chỉ có quyền tại file chỉ định

5.6 | KHÁC NHAU GIỮA QUYỀN SHARE VÀ SECURITY

Share Permission	Security Permission
• Là quyền hạn truy cập tài nguyên chia sẻ qua mạng • Quyền Share có 3 quyền chuẩn(Full control, Change, Read) • Quyền Share có trên cả phân vùng FAT và NTFS • Quyền Share phân quyền đơn giản với 3 quyền chuẩn • Quyền Share không có Apply Onto	• Là hệ thống tập hợp các quyền cho phép hoặc không cho phép người dùng (user) truy cập vào các đối tượng chứa trên một phân vùng NTFS bao gồm các thư mực (folder) và tập tin (file) • Quyền Security có 6 quyền chuẩn(Full control,Modify,Write,Read & Execute,Read,List Folder Content) • Quyền Security chỉ có trên phân vùng NTFS • Quyền Security phân quyền phức tạp hơn với 6 quyền chuẩn và dẫn xuất ra13 quyền chi tiết • Quyền Security có 7 thành phần trong Apply Onto

5.7 | XÂY DỰNG MÔ HÌNH MẠNG GIA ĐÌNH

❖ Giải pháp mô hình mạng gia đình

Với nhu cầu sử dụng internet cho gia đình, Khi thuê một đường truyền Internet từ nhà cung cấp dịch vụ(FPT, VIETTEL, VNPT,...) thì thường được tặng 1 con Modem ADSL(có thể có dạng Modem Wifi) cho phép các thiết bị kết nối. Tùy theo gói dịch vụ(thường dựa vào tốc độ đường truyền) sẽ có chi phí gói cước khác nhau đáp ứng nhu cầu khác hàng.

❖ Cài đặt cài đặt modem cáp quang FPT

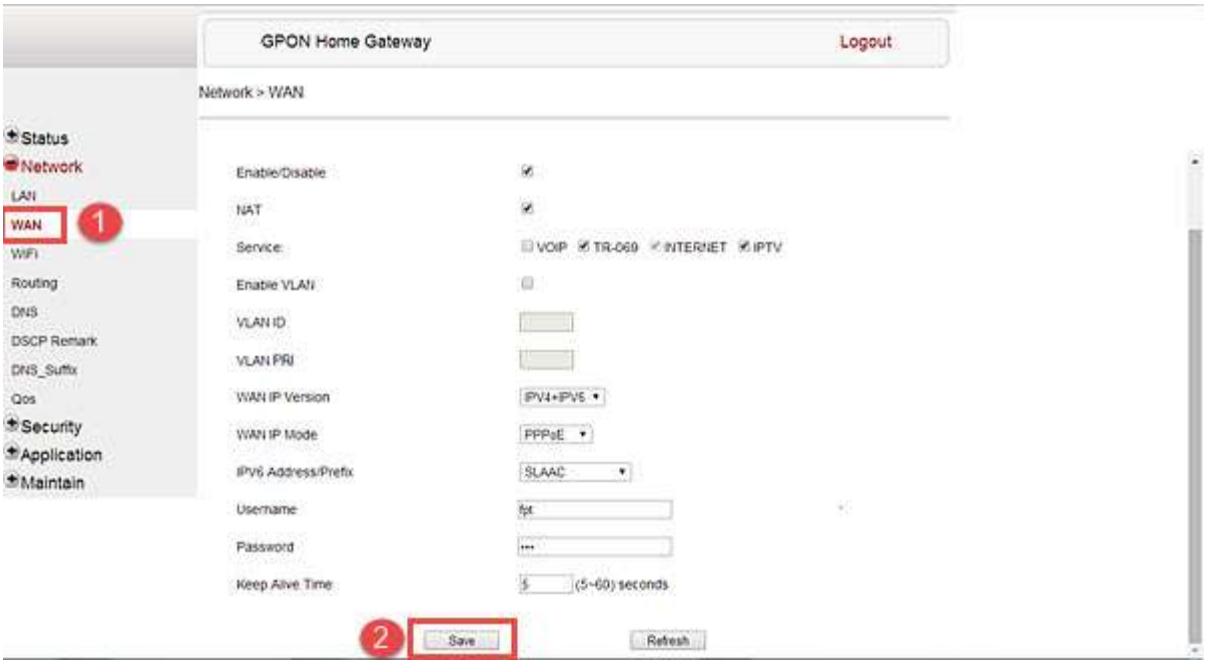
Bước 1: Kết nối modem cáp quang FPT với máy tính qua dây mạng. Đầu trên modem có thể cắm bất kỳ tại vị trí 1, 2, 3, 4 (nếu có 4 cổng LAN).

Bước 2: Truy cập địa chỉ 192.168.1.1 và điền thông tin sau:

- Username: Admin
- Pass: mặc định 1234 hoặc số hợp đồng của gia đình. Nếu không được liên hệ Tổng đài FPT để được hỗ trợ

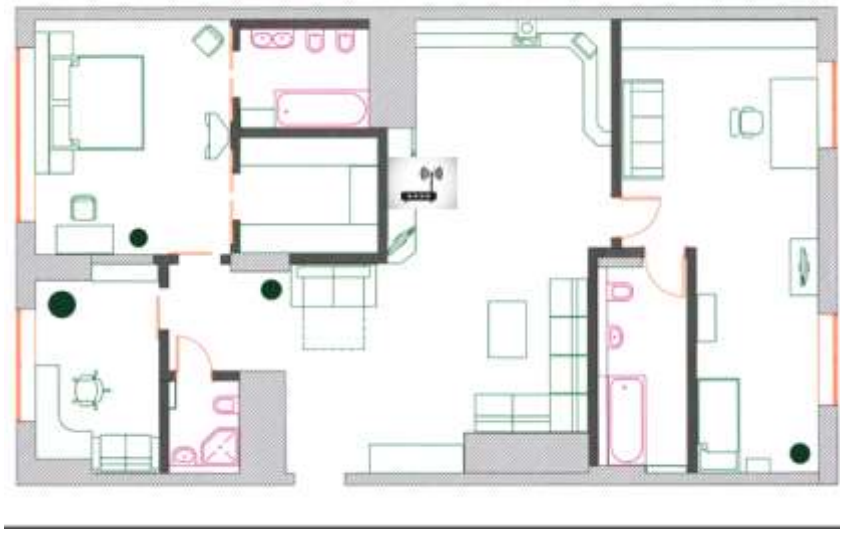
Bước 3: Chuyển qua tab WAN và điền thông số như sau.

- WAN IP Mode: PPPoE
- Username: fpt (có dạng hnfdl-123456-789)
- Password: Có dạng fd12345



Tiếp đến click vào nút **Save** để lưu lại

- Hướng dẫn đặt Modem Wifi, bộ phát wifi trong nhà tốt nhất
  - Đặt modem wifi ở vị trí trung tâm của căn nhà, Khi đó tất cả các vị trí trong ngôi nhà đều được phủ sóng wifi tốt, có thể di chuyển khắp nơi, không sợ bị rớt mạng.
  - Đặt modem wifi ở vị trí cao, thoáng không có các vật cản như tường bê tông, cánh cửa, hoặc các vật dụng khác. Không nên để modem ở dưới nền nhà mà phải được gắn lên tường hoặc lên giá đỡ. Vì sóng wifi được truyền theo hướng từ trong ra ngoài, từ trên xuống nên ở trị trí cao và không có vật cản sẽ làm cho thiết bị phát sóng tốt hơn.



Để ăng ten của modem wifi luôn hướng lên trên hoặc có thể đặt ăng ten theo chiều ngang để có thể phát tín hiệu tốt nhất theo chiều

Đối với nhà có nhiều tầng thì việc đặt ăng ten theo chiều ngang sẽ giúp cho các tầng trên bắt sóng wifi tốt hơn, còn việc đặt ăng ten hướng lên sẽ giúp cho phạm vi phủ sóng xa hơn, tốt hơn. Nếu modem wifi có 2 ăng ten thì nên để 1 cái hướng lên một cái nằm ngang. Còn nếu modem wifi không có ăng ten thì phải đặt theo đúng thiết kế của nhà sản xuất.

Ngoài ra cần lưu ý một số điểm sau:

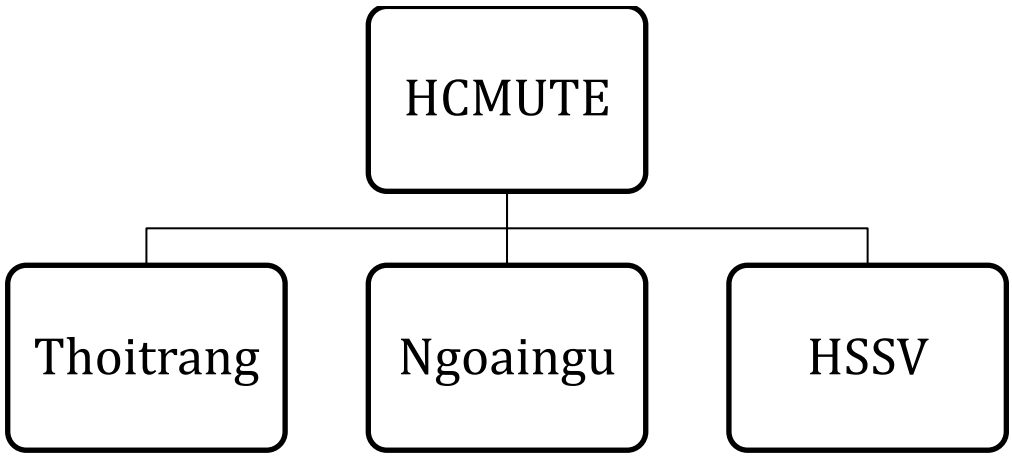
- Không đặt modem gần những vật dụng bằng kim loại vì kim loại sẽ làm cho khả năng phát sóng kém đi.

- Không đặt modem gần lò vi sóng, vì tần số của lò vi sóng gần giống với tần số của modem nên khi đó sóng sẽ bị can nhiễu gây ảnh hưởng tới chất lượng.
- Vậy, trên đây là những điều cần lưu ý khi chọn vị trí để đặt modem wifi, Access Point hay bộ phát wifi trong nhà để có thể phát sóng wifi tốt nhất có thể.
- Khi sử dụng password wifi modem trong thời gian dài, rất có thể mật khẩu sẽ bị rò rỉ ra bên ngoài. Chính vì vậy, nên đổi mật khẩu wifi để bảo mật hơn.

5.8 | BÀI TẬP CHƯƠNG 5

5.8.1 | BÀI TẬP 1

1. **Tạo thư mục theo sơ đồ:**



2. **Thực hiện tạo Users & Group trên máy Server:**

   "Tất cả password của user là 123"
   nhomTT(tt1, tt2)
   nhomNN(nn1, nn2)
   nhomHSSV(sv1, sv2)

3. **Phân quyền(Share Permission và NTFS Permission)**

- Quyền share: thư mục HCMUTE(full control cho everyone)
- Quyền security:
  - Mọi tài khoản(nhóm) chỉ có quyền đọc trên thư mục HCMUTE
  - Mọi tài khoản thuộc nhomTT sẽ toàn quyền trên thư mục Thoitrang, các tài khoản khác có quyền đọc
  - Mọi tài khoản thuộc nhomNN sẽ toàn quyền trên thư mục Ngoaingu, các tài khoản nhóm khách hàng không có quyền

- Mọi tài khoản thuộc nhomHSSV sẽ toàn quyền trên thư mục HSSV, các tài khoản khác không có quyền

4. **Tạo file logon.bat để kết nối đĩa mạng:**

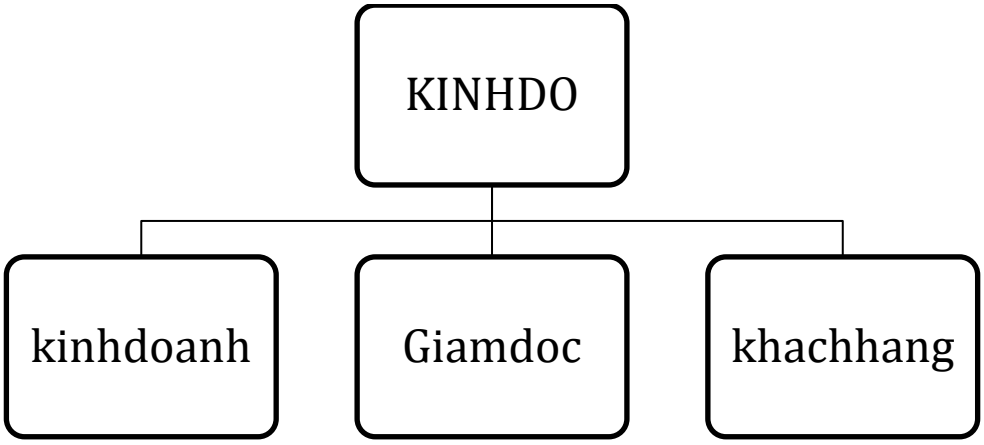
G: → Dùng thư mục Thoitrang, user: tt1

K: → Dùng thư mục Ngoaingu, user:tt1

H: → Dùng thư mục Hssv, user: tt1

5.8.2 | BÀI TẬP 2

1. **Tạo thư mục theo sơ đồ:**



2. **Thực hiện tạo Users & Group trên máy Server:**

"Tất cả password của user là 123"

nhomKD(kd1, kd2)

nhomGD(gd1, gd2)

nhomKH(kh1, kh2)

3. **Phân quyền(Share Permission và NTFS Permission)**

- Quyền share: thư mục KINHDO(full control cho everyone)
- Quyền security:
  - Mọi tài khoản(nhóm) chỉ có quyền đọc trên thư mục KINHDO
  - Mọi tài khoản thuộc nhomKD sẽ toàn quyền trên thư mục kinhdoanh, các tài khoản nhóm kinh doanh không có quyền
  - Mọi tài khoản thuộc nhomKH sẽ toàn quyền trên thư mục khachhang, các tài khoản nhóm khách hàng không có quyền
  - Mọi tài khoản thuộc nhomGD sẽ toàn quyền trên thư mục kinhdoanh, giamdoc va khách hàng, thư mục giám đốc chỉ có nhóm nhom GD toàn quyền, các tài khoản khác không có quyền

4. **Tạo file logon.bat để kết nối đĩa mạng:**

G: → Dùng thư mục kinhdoanh, user: kd1
K: → Dùng thư mục Giamdoc, user:kd1
H: → Dùng thư mục khachhang, user: kd1

TÀI LIỆU THAM KHẢO

[1] Nguyễn Thị Điệp, Nguyễn Hồng Sơn - Giáo trình hệ thống mạng máy tính CCNA, Version 4.0 - NXB Lao động -Xã hội – 2009

[2]. Đội ngũ giảng viên Vnpro, Hướng dẫn học CCNA Routing & Switching, nhà xuất bản Thông tin và Truyền thông, 2016

[3]. Tô Thanh Hải –Quản trị Windows Server 2008 – tập 1, 2- NXB Phương Đông

[4]. James Kurose, Computer Networking A Top-Down Approach, Pearson, 2012

[5] Andrew S.Tanenbaum, David J.Wetherall, Computer Networks, Pearson,

[6] Cisco Academy 2016 - CCNA Routing & Switching