

**HỌC PHẦN: Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện

2) Cao Văn Lợi

1. Bài (chương, mục): **Chương I: Tổng quan về mạng máy tính**

2. Thời lượng:

- GV giảng: 3 tiết.
- Thảo luận: 2 tiết,
- Thực hành: 0 tiết.
- Bài tập: 1 tiết.
- Tự học: 6 tiết

37281920,

3. Mục đích, yêu cầu:

Mục đích: Bài mở đầu giúp sinh viên nắm được tổng quan về chương trình, phạm vi kiến thức và ý nghĩa thực tế của môn học. Trang bị những khái niệm cơ bản và kiến thức tổng quan về mạng máy tính.

- Giới thiệu yêu cầu và nội dung của môn học
- Lịch sử phát triển của mạng máy tính
- Một số khái niệm cơ bản về MMT
- Phân loại mạng

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://http://fit.mta.edu.vn/~thiennd/>).
- Làm bài tập trên lớp và ở nhà.

4. Nội dung:

a) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

**1. Giới thiệu môn học**

- ✓ Mục đích, yêu cầu và ý nghĩa của môn học.
- ✓ Cấu trúc chương trình, kiểm tra và thi hết môn.
- ✓ Nội dung môn học và tài liệu tham khảo.
- ✓ Phương pháp học môn học: nghe giảng, tự học, làm bài tập, thực hành, thảo luận.
- ✓ Lịch sử phát triển của mạng máy tính.

**Tiến trình của môn học:**

- Lý thuyết (30 tiết): giảng bằng Slide và viết bảng – Nội dung lý thuyết xem đề cương chi tiết môn học (cung cấp trên mạng).
- Bài tập (9 tiết): giao bài tập cho sinh viên thực hiện trước tại nhà và trình bày trên lớp.
- Thảo luận (6 tiết): sẽ thực hiện xen kẽ với các nội dung lý thuyết.
- Thí nghiệm (15 tiết): thực hiện các nội dung theo sự phân công của giáo viên tại phòng thí nghiệm của bộ môn.

**Mục tiêu của học phần:**

- Kiến thức: Môn học cung cấp những kiến thức cơ bản về mô hình mạng OSI, TCP/IP, các kỹ thuật mạng LANs, WANs, các chuẩn IEEE và các dịch vụ mạng Internet. Các thiết bị mạng như repeater, hubs, switches, routers, bridge... khái niệm về an toàn mạng máy tính. Cùng với các kiến thức chuyên sâu như An ninh mạng, quản trị mạng,...

- **Kỹ năng:** Có khả năng đọc hiểu các kiến thức mở rộng của môn học mạng máy tính, tự tìm kiếm và đọc hiểu được các tài liệu tiếng anh. Có khả năng cấu hình một số thiết bị mạng và thiết kế xây dựng mạng LAN

**Trình bày sơ lược về nội dung của môn học** – xem đề cương chi tiết môn học (cung cấp trên mạng).

- Chương 1. Tổng quan về mạng máy tính
- Chương 2. Kiến trúc phân tầng và mô hình OSI
- Chương 3. Mạng cục bộ LAN
- Chương 4. Mạng diện rộng WAN
- Chương 5. Thiết bị mạng máy tính
- Chương 6. Mô hình TCP/IP và mạng Internet
- Chương 7. Một số vấn đề chuyên sâu về mạng máy tính

Định hướng ứng dụng của kiến thức trong thực tế.

Giới thiệu về giáo trình và tài liệu phục vụ môn học.

Hình thức thi: Vấn đáp.

Quy chế thi: Theo qui định của Học viện.

## **2. Lịch sử phát triển của mạng máy tính**

- 1) Mạng xử lý
- 2) Mạng truyền tin
- 3) Mạng truyền thông
- 4) Mạng máy tính

Xuất phát từ bộ quốc phòng Mỹ qua các thập kỷ 60, 70 đến thập kỷ 80 trở đi thì việc kết nối mạng mới được thực hiện rộng rãi nhờ tỷ lệ giữa giá thành máy tính và chi phí truyền tin đã giảm đi rõ rệt. Trong giai đoạn này bắt đầu xuất hiện những thử nghiệm đầu tiên về mạng diện rộng, mạng liên quốc gia và hình thành mạng internet ngày nay.

- 5) Mục đích xây dựng mạng máy tính:

- Làm cho các tài nguyên có giá trị cao (thiết bị, chương trình, dữ liệu,...) trở nên khả dụng đối với bất kỳ người sử dụng nào trên mạng (không cần quan tâm đến vị trí địa lý của tài nguyên và người sử dụng).
- Tăng độ tin cậy của hệ thống nhờ khả năng thay thế khi xảy ra sự cố đối với một máy tính nào đó.
- Quản lý điều hành và thương mại điện tử.

## **Tiết 2:**

### **3. Một số khái niệm cơ bản**

- 1) K/n **Mạng máy tính:** *Mạng máy tính là một hệ thống gồm nhiều máy tính và các thiết bị được kết nối với nhau bởi đường truyền vật lý theo một kiến trúc (Network Architecture) nào đó nhằm thu thập và chia sẻ tài nguyên cho nhiều người sử dụng.*
- 2) **Kiến trúc mạng (Network Architecture):** *Cách nối các máy tính và thiết bị với nhau và tập hợp các qui tắc, qui ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo.* Gồm 2 thành phần:

**Cách nối: Hình trạng mạng (Topology)**

Một số Topo mạng cơ bản:

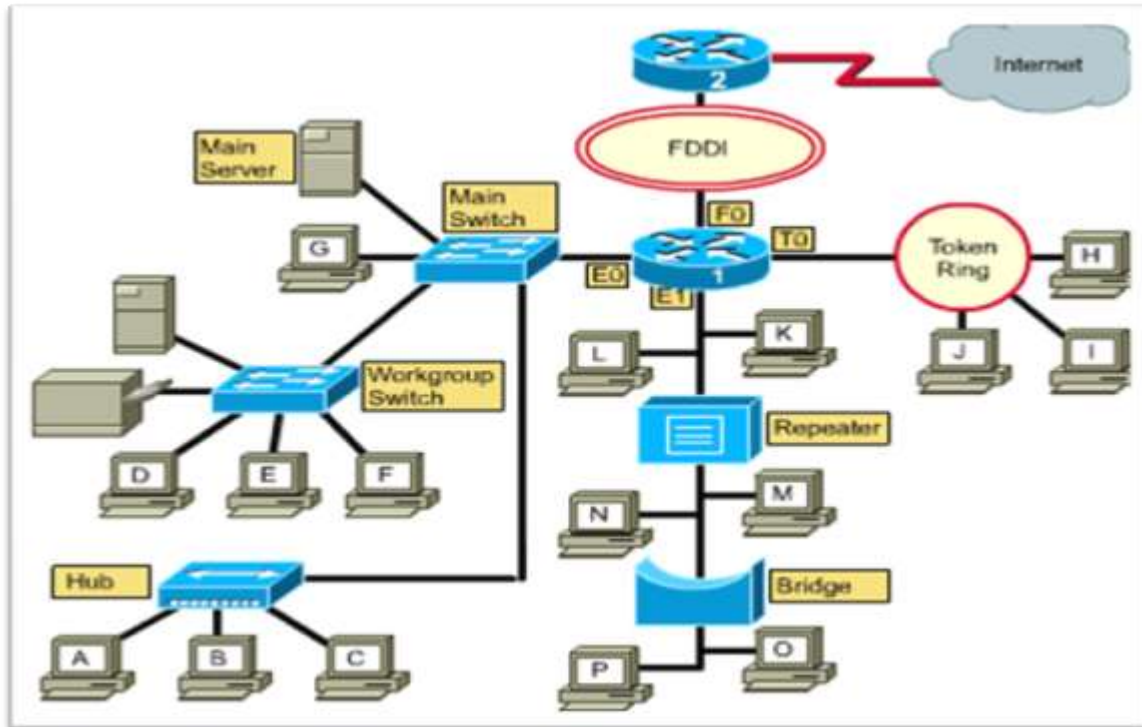
- + Dạng hình sao – Start
- + Dạng hình tuyến – Bus
- + Dạng hình vòng – Ring
- + Dạng hỗn hợp – Kết hợp các dạng trên.

**Qui tắc, qui ước: Giao thức mạng (Protocol)**

+ K/n: *Để các máy trên mạng có thể trao đổi thông tin với nhau được thì chúng phải tuân theo các qui tắc, qui ước về nhiều mặt: từ khuôn dạng kích thức, thủ tục gửi, thủ tục nhận, kiểm soát, cho đến việc xử lý lỗi, sự cố xảy ra và an toàn thông tin truyền như thế nào. Tập các qui tắc, qui ước đó chính là giao thức mạng.*

- + Chức năng của giao thức mạng.

- ✓ Đóng gói dữ liệu (Encapsulation)
- ✓ Phân đoạn và hợp lại
- ✓ Điều khiển liên kết
- ✓ Giám sát
- ✓ Điều khiển lưu lượng
- ✓ Điều khiển lỗi
- ✓ Đồng bộ hóa
- ✓ Địa chỉ hóa



Hình 1: Một ví dụ mô hình mạng

### 3) Hệ điều hành mạng( NOS - Network Operating Systems)

K/n: Hệ thống phần mềm có chức năng quản lý người dùng, dữ liệu, tính toán, xử lý và điều khiển truyền tin thống nhất trên mạng.

### 4) Địa chỉ mạng

Mạng phải xác lập một hệ thống định danh các thực thể tham gia mạng, trong đó mỗi đối tượng tham gia mạng phải được xác định duy nhất tại thời điểm truyền/nhận tin. Các hệ thống định danh như vậy gọi là địa chỉ mạng.

- ✓ Địa chỉ vật lý – MAC
- ✓ Địa chỉ logic- IP
- ✓ Địa chỉ cổng (port)

## Tiết 4:

### 4. Phân loại mạng:

#### 1) Theo qui mô và khoảng cách địa lý (4 loại)

##### i. Mạng cục bộ – LAN (Local Area Network)

Là mạng thường được lắp đặt trong các công ty, văn phòng nhỏ bán kính tối đa giữa các máy trạm khoảng dưới 1 Km với số lượng máy trạm thường không nhiều hơn 100 máy.

##### ii. Mạng thành phố – MAN (Metropolitan Area Network)

Là mạng được cài đặt trong phạm vi một đô thị hoặc một trung tâm KTXH có bán kính hàng trăm Km, số lượng máy trạm có thể lên đến hàng nghìn, đường truyền có thể sử dụng cơ sở hạ tầng của viễn thông. MAN hoạt động theo kiểu quảng bá, cung cấp các dịch vụ thoại và truyền hình cáp.

iii. Mạng diện rộng – WAN (Wide Area Network)

*Là mạng thường được lắp đặt trong phạm vi một quốc gia như Intranet phục vụ cho các công ty lớn, ngành kinh tế có bán kính hoạt động lớn, có thể liên kết nhiều mạng LAN, MAN, đường truyền có thể sử dụng cơ sở hạ tầng của viễn thông.*

iv. Mạng toàn cầu – GAN (Global Area Network)

*Là mạng có thể trải rộng trong nhiều quốc gia, phục vụ phát triển kinh tế xã hội cho những công ty siêu quốc gia hoặc nhóm các quốc gia, đường truyền có thể sử dụng cơ sở hạ tầng của viễn thông, mạng Internet là một mạng GAN.*

**2) Phân loại mạng theo kỹ thuật chuyển mạch (3 loại)**

i. Mạng chuyển mạch kênh (Circuit switched):

*Khi có hai máy cần trao đổi thông tin với nhau thì giữa chúng sẽ được thiết lập một kênh cố định và được duy trì cho đến khi một trong hai bên ngắt liên lạc. Các dữ liệu chỉ được truyền theo đường cố định đó. (VD: Các hệ thống điện thoại)*

ii. Mạng chuyển mạch thông báo

*TB là một đơn vị thông tin có chứa địa chỉ đích cần gửi đến. Căn cứ vào các thông tin này mỗi nút trung gian có thể chuyển TB đến nút kết tiếp để đến đích. Tùy theo cấu trúc mạng mà các TB có thể đi theo nhiều đường khác nhau. (VD: gửi tin nhắn ở điện thoại)*

iii. Mạng chuyển mạch gói (Packet switched network)

*TB được chia thành nhiều phần nhỏ hơn gọi là gói tin (Packet) có khuôn dạng qui định trước. Mỗi gói tin có chứa các thông tin điều khiển, địa chỉ nguồn (người gửi) và đích (người nhận). Các gói tin của một TB có thể được gửi đi qua mạng để tới đích bằng nhiều đường khác nhau. Vấn đề khó khăn: khôi phục TB ban đầu, phải có cơ chế “đánh dấu” gói tin để phục hồi các gói tin bị thất lạc, bị lỗi.*

b) Nội dung thảo luận:

**Tiết 4+5:**

Vai trò của mạng máy tính. Bao gồm các mặt cơ bản:

- Giải trí, giao tiếp:
  - + Cung cấp tin tức thời sự ..
  - + Ứng dụng mạng xã hội
  - + Ứng dụng chat, game, video ...
- Nghiệp vụ văn phòng
  - + Cổng thông tin điện tử
  - + Email
  - + Hội thảo trực tuyến
- Thương mại điện tử :
  - + Mua bán online.
  - + Quảng cáo trực tuyến.
  - + Ngân hàng trực tuyến.

c) Nội dung tự học

- Lịch sử mạng máy tính
- Nắm chắc các khái niệm cơ bản
- Trả lời câu hỏi phần ôn tập.

d) Bài tập (bắt buộc)

**Tiết 6:**

- Chuyển đổi các loại cơ số 2, 10 và 16
- Phân lớp địa chỉ IP

5. Tài liệu tham khảo (sách, báo – chỉ tiết đến chương, mục, trang)

- i. Bài giảng của giáo viên, Slide chương 1.
- ii. TL [1], chương 1; trang 11 - 68

6. Câu hỏi ôn tập:

- i.* Trình bày các khái niệm: Mạng máy tính, Kiến trúc mạng, hệ điều hành mạng, địa chỉ mạng
- ii.* Trình bày khái niệm và chức năng của giao thức mạng.
- iii.* Trình bày khái niệm, đặc điểm của mạng LAN, MAN, WAN và GAN.
- iv.* Trình bày khái niệm, ưu và nhược điểm của ba loại mạng chuyển mạch.

HỌC PHẦN: Mạng máy tính

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương 2: Kiến trúc phân tầng và mô hình OSI**

2. Thời lượng: 6,0,0,6 (GV giảng, thảo luận, thực hành, tự học)

3. Mục đích, yêu cầu:

Mục đích: Sinh viên nắm được ý nghĩa của việc chuẩn hóa mạng và phân tầng. Nắm được mô hình chuẩn OSI, vai trò và chức năng của các tầng của mô hình.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://fit.mta.edu.vn/~thiennd/>).
- Ôn tập theo các câu hỏi

4. Nội dung:

a) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

1) Giới thiệu bài: giới thiệu mục đích, yêu cầu nội dung của bài

I. Giới thiệu chung

II. Kiến trúc phân tầng

1. Nguyên tắc phân tầng

2. Truyền thông giữa các tầng

III . Mô hình OSI

1. Giới thiệu

2. Các giao thức chuẩn trong mô hình OSI

3. Vai trò và chức năng các tầng trong mô hình OSI

2) Kiến trúc phân tầng:

**Tại sao phải chuẩn hóa mạng?**

1- Giao thức là một phần rất quan trọng của kiến trúc mạng máy tính. Trong hệ thống mạng có rất nhiều giao thức, số giao thức và chức năng của nó phụ thuộc vào mục đích xây dựng mạng.

2- Sự khác nhau về các qui định truyền thông trong các hệ thống mạng của các tổ chức khác nhau.

3- Các sản phẩm mạng do các công ty sản xuất không theo một chuẩn truyền thông chung.

**Tổ chức tiêu chuẩn**

**ISO** (*International Standards Organization*): đưa ra mô hình chuẩn OSI - Open Systems Interconnection

Hệ thống giao thức là một trong các thành phần cốt lõi để thiết kế nên MMT, do vậy cần được xây dựng theo một mô hình thống nhất. Mỗi hệ thống MMT hiện nay đều được coi như cấu trúc đa tầng giao thức. Trong đó mỗi tầng cung cấp một số dịch vụ nhất định. Mô hình đó được gọi là kiến trúc phân tầng.

a. Nguyên tắc của kiến trúc phân tầng là:

1- Mỗi hệ thống trong mạng đều có cấu trúc tầng (số lượng tầng và chức năng của mỗi tầng là như nhau).

2- Giữa 2 tầng liền kề trong một hệ thống giao tiếp với nhau qua 1 giao diện qua đó xác định các hàm nguyên thủy và các dịch vụ tầng dưới cung cấp.

3-Giữa hai tầng đồng mức ở hai hệ thống giao tiếp với nhau thông qua các luật lệ, qui tắc được gọi là giao thức.

Bộ môn An ninh mạng

4-Trong thực tế, dữ liệu không được truyền trực tiếp từ tầng thứ i của hệ thống này sang tầng thứ i của hệ thống khác (trừ tầng thấp nhất). Mà việc kết nối giữa hai hệ thống được thực hiện thông qua hai loại liên kết: liên kết vật lý ở tầng thấp nhất và liên kết logic (ảo) ở các tầng cao hơn.

#### **Điểm truy cập dịch vụ:**

Kiến trúc phân tầng tồn tại hai dạng liên kết: liên kết giữa hai tầng đồng mức - liên kết ngang và liên kết giữa hai tầng liên kề - liên kết dọc. Các liên kết hai chiều hoặc là xảy ra đồng thời hoặc độc lập nhau.

#### **Truyền thông đồng tầng và quan hệ tầng liên kề**

**PCI (Protocol Control Information):** được thêm vào đầu các gói tin. N\_PCI là thông tin điều khiển tầng N.

- **SDU (Service Data Unit):** Là đơn vị dữ liệu truyền thông giữa các tầng kề nhau. Ký hiệu N\_SDU là đơn vị dữ liệu truyền từ tầng (N+1) xuống tầng N chưa thêm thông tin điều khiển.

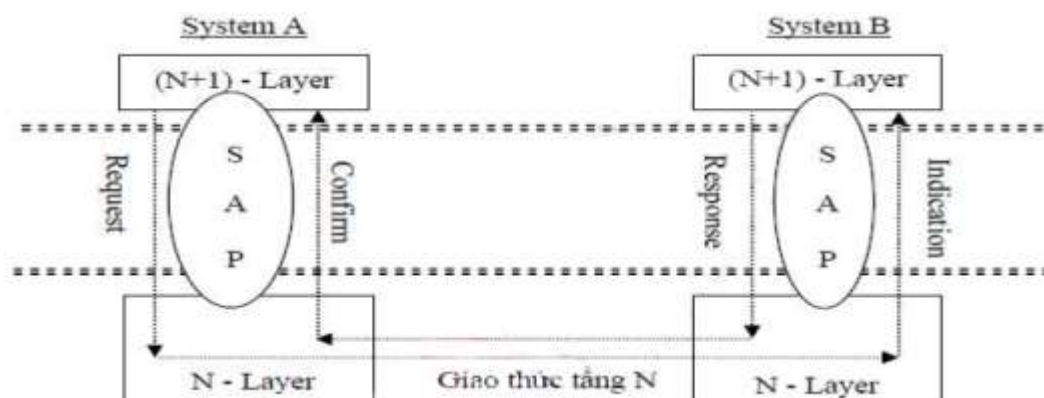
- **PDU (Protocol Data Unit) :**  $PDU = PCI + SDU$

### **Tiết 2 :**

#### **c. Các hàm dịch vụ nguyên thủy**

Việc liên kết giữa các tầng liên kề trong mô hình OSI được xây dựng theo nguyên tắc đáp ứng các dịch vụ thông qua các hàm nguyên thủy, có bốn kiểu hàm nguyên thủy:

- Request : Hàm yêu cầu
- Indication : Hàm chỉ báo
- Response : Hàm trả lời
- Confirm : Hàm xác nhận



Hình 2 : Hàm dịch vụ nguyên thủy

## **2. Mô hình OSI**

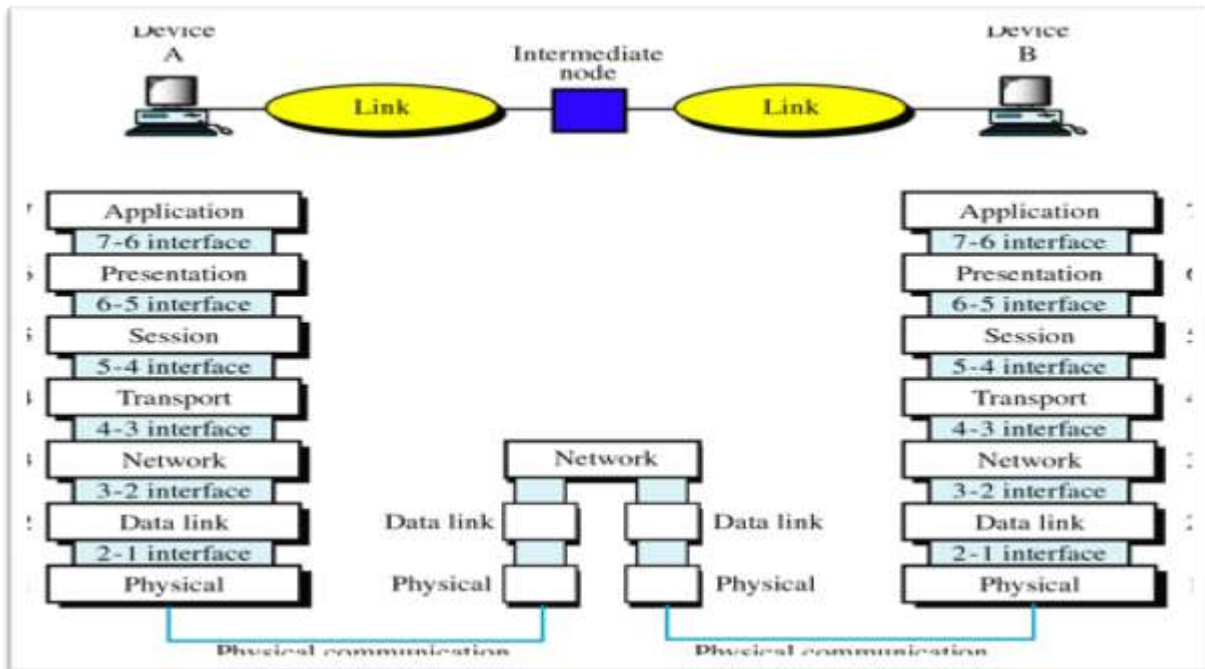
Kiến trúc phân tầng được đề cập như là một trong quan điểm chủ đạo trong việc xây dựng hệ thống giao thức. Vì lý do đó tổ chức tiêu chuẩn hoá quốc tế ISO (International Organization for Standardization) năm 1984 đã xây dựng xong *Mô hình tham chiếu cho việc kết nối các hệ thống mở OSI* (Open Systems Interconnection).

Mô hình OSI gồm 7 tầng giao thức với các nguyên tắc sau:

- ✓ Các tầng có tính độc lập tương đối với nhau thực hiện các chức năng riêng biệt
- ✓ Cho phép thay đổi chức năng hoặc giao thức trong một tầng không làm ảnh hưởng đến các tầng khác.
- ✓ Có thể chia một tầng thành các tầng con khi cần thiết.
- ✓ Cho phép huỷ bỏ các tầng con nếu thấy không cần thiết.
- ✓ Bảo đảm liên kết cho nhiều hệ thống mạng khác nhau
- ✓ Thích ứng với nhu cầu phát triển các công nghệ mới trong tương lai

Các tầng trong mô hình OSI

- 1) Tầng vật lý – Physical
- 2) Liên kết dữ liệu – Data Link
- 3) Mạng – Network
- 4) Vận chuyển – Transport
- 5) Phiên – Session
- 6) Trình diễn – Presentation
- 7) Ứng dụng - Application



Hình

3: Mô hình OSI

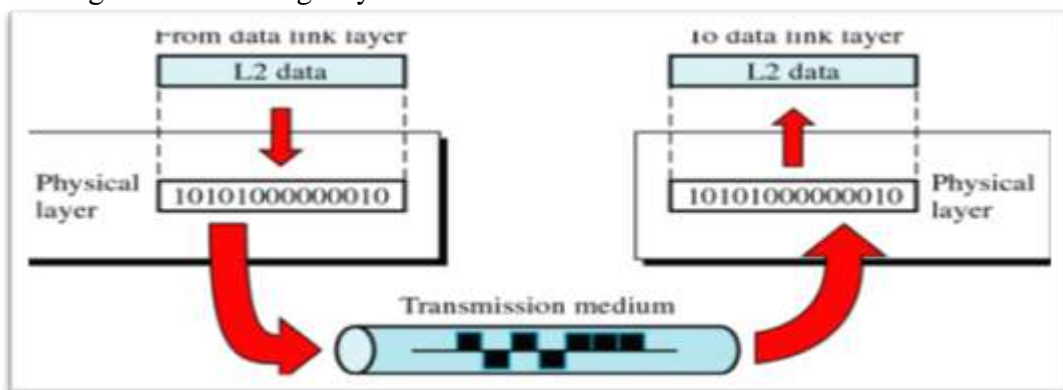
Cơ chế truyền tin của mô hình OSI

- 03 tầng trên là giao tiếp với người sử dụng, trình bày dữ liệu và tạo các phiên làm việc, không tham gia truyền tin
- 04 tầng dưới thực hiện truyền tin
- Qua mỗi tầng bên gửi đều có đính kèm header và đóng gói
- Qua mỗi tầng bên nhận đều có bóc tách header và tổng hợp dữ liệu

### Tiết 3:

#### 1) Tầng vật lý:

- Truyền dòng bit qua môi trường vật lý. Nó giải quyết các đặc tả kỹ thuật của giao diện cũng như môi trường truyền.



Hình

4: Mô phỏng hoạt động của tầng vật lý

#### Chức năng của tầng vật lý:

- ✓ Đặc tính vật lý của giao diện và môi trường



- ✓ Biểu diễn của các bit
- ✓ Tốc độ dữ liệu
- ✓ Sự đồng bộ hoá của các bit
- ✓ Cấu hình đường
- ✓ Topo vật lý
- ✓ Chế độ truyền: *simple, half-duplex, full duplex*

## 2) Tầng Liên kết dữ liệu:

Đảm bảo việc truyền dòng bit của tầng vật lý được tin cậy và chịu trách nhiệm truyền phát point – to – point. Xử lý các lỗi của dữ liệu nhận được từ tầng vật lý để đảm bảo dữ liệu không có lỗi khi lên các tầng trên.

### a. Chức năng của tầng liên kết dữ liệu

- ✓ Đóng khung dữ liệu (*Framing*)
- ✓ Gán địa chỉ vật lý MAC
- ✓ Điều khiển luồng
- ✓ Kiểm soát lỗi
- ✓ Điều khiển truy cập

### b. Các giao thức ở tầng liên kết dữ liệu

- ✓ Để thực hiện các chức năng trên người ta xây dựng rất nhiều giao thức cho tầng Liên kết dữ liệu, được gọi chung là DLP (*Data Link Protocol*). Các DLP được chia làm 2 loại dị bộ (*Asynchronous DLP*) và đồng bộ (*Synchronous DLP*).
- ✓ Giao thức CSMA, Token Bus, Token Ring, Ethernet

### c. Phương pháp kiểm tra lỗi (Giới thiệu)

## Tiết 4:

## 3) Tầng Mạng

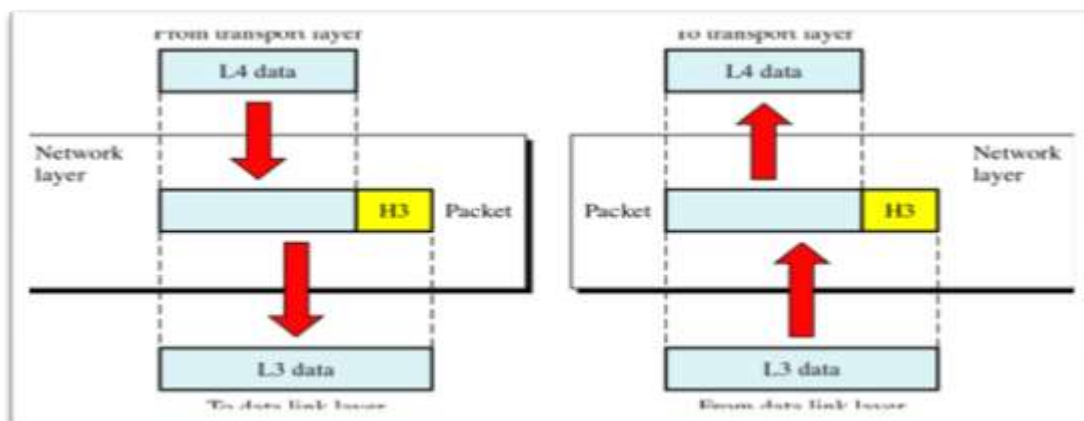
Chức năng chuyển phát nguồn và đích (*Source – Des, node to node*) của các gói tin trên đường truyền (nhiều mạng). Đảm bảo mỗi gói được chuyển từ điểm nguồn tới điểm đích.

Thiết bị kết nối trung gian giữa các mạng phải có chức năng tầng mạng.

### Chức năng chính:

- ✓ Đánh địa chỉ logic. Ví dụ địa chỉ IP
- ✓ Chọn đường (Định tuyến)

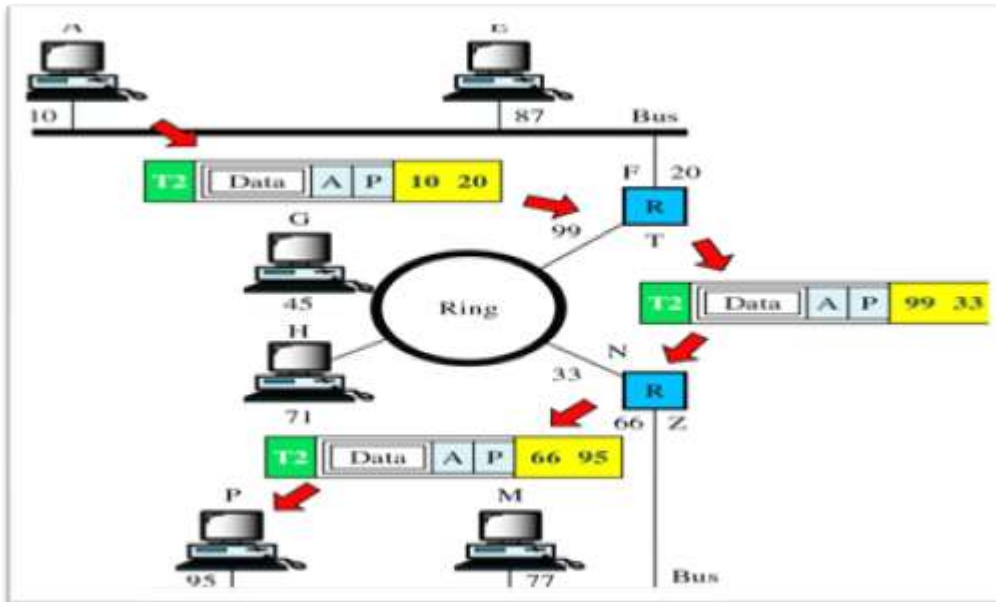
### Mô hình truyền thông:



Tầng Mạng

### Cơ chế đánh địa chỉ và định tuyến:

Hì  
nh 5:



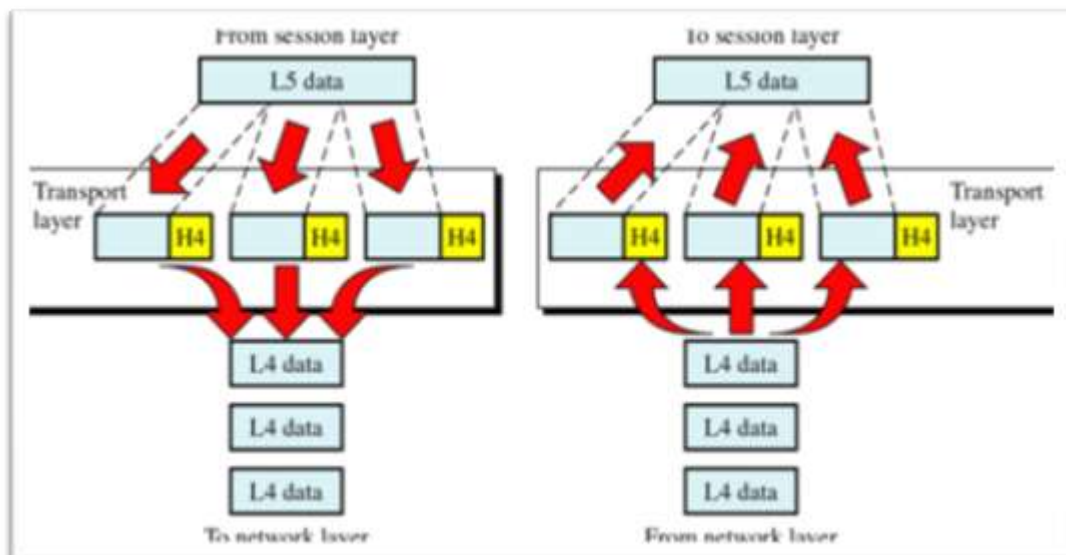
Hình 6: Sơ đồ mô phỏng đánh địa chỉ và định tuyến

#### 4) Tầng vận chuyển

Chuyển phát đầu cuối (end – to – end) của toàn bộ thông điệp và đảm bảo rằng toàn bộ thông điệp nhận được là toàn vẹn và đúng thứ tự, chúng cũng xem xét kiểm soát lỗi và luồng dữ liệu ở cấp độ đầu cuối. Để tăng thêm tính bảo mật có thể tạo ra một kết nối giữa 2 cổng.

**Các chức năng cụ thể của tầng giao vận:**

- ✓ Đánh địa chỉ điểm dịch vụ
- ✓ Cắt hợp dữ liệu
- ✓ Điều khiển kết nối
- ✓ Điều khiển luồng

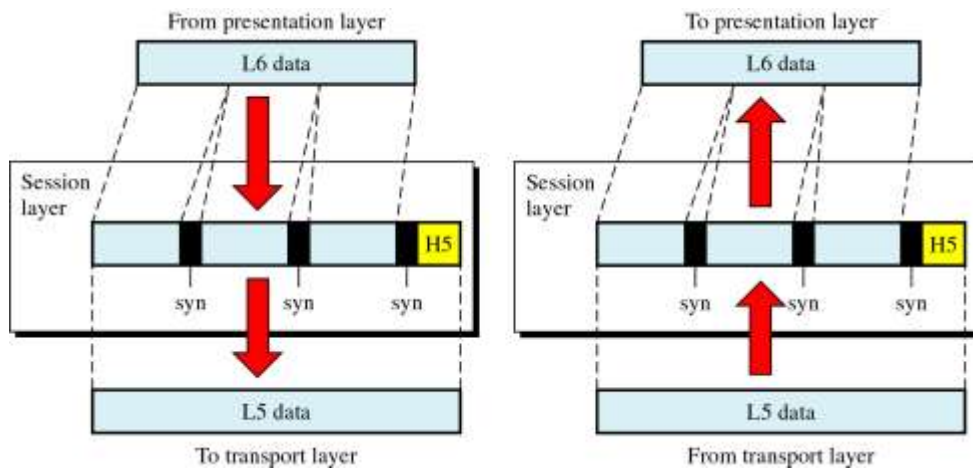


Hình 7: Hoạt động tầng giao vận

### Tiết 5:

#### 5) Tầng Phiên:

Các dịch vụ được cung cấp bởi 3 tầng đầu tiên là không đủ đối với một số tiến trình. Tầng phiên là bộ điều khiển hội thoại của mạng. Nó thiết lập duy trì và đồng bộ hoá giữa các hệ thống.



Hình 8: Hoạt động của tầng phiên

**Chức năng chính:**

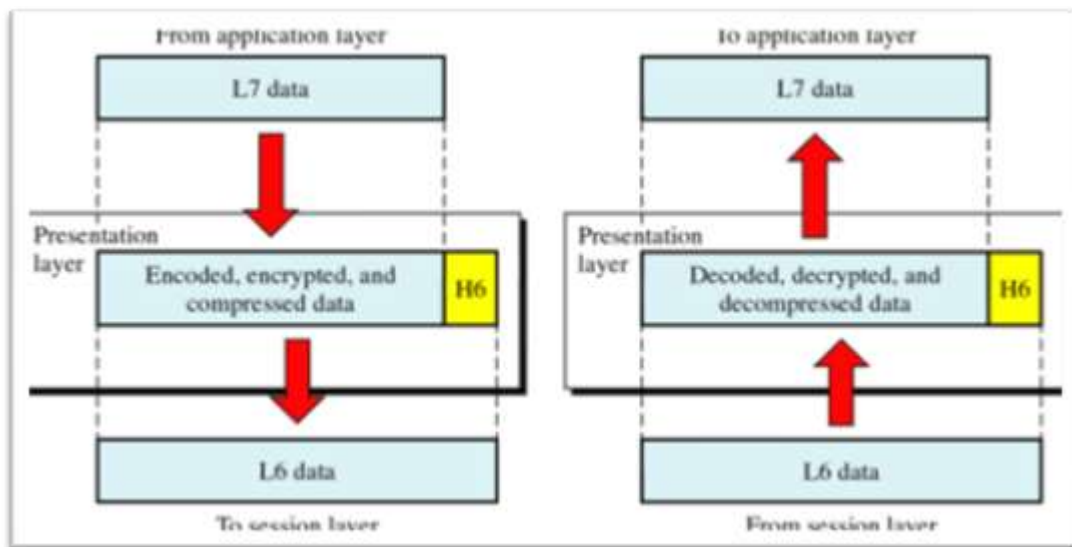
- ✓ Điều khiển hội thoại
- ✓ Đồng bộ hoá

#### 6) Tầng trình diễn

Tầng trình diễn liên quan đến **cú pháp và ngữ nghĩa của dữ liệu** giữa hai hệ thống. Chuyển đổi thông tin dưới dạng các chuỗi, các số... thành dòng bit. Tầng trình diễn ở trạm gửi chuyển thông tin về một khuôn dạng chung. Tầng trình diễn ở trạm nhận chuyển thông tin từ khuôn dạng chung về khuôn dạng của trạm. Thực hiện mã hóa dữ liệu đảm bảo tính bí mật. Thực hiện nén để giảm kích thước dữ liệu trước khi truyền.

**Chức năng của tầng trình diễn:**

- ✓ Chuyển đổi khuôn dạng dữ liệu.
- ✓ Mã hoá
- ✓ Nén

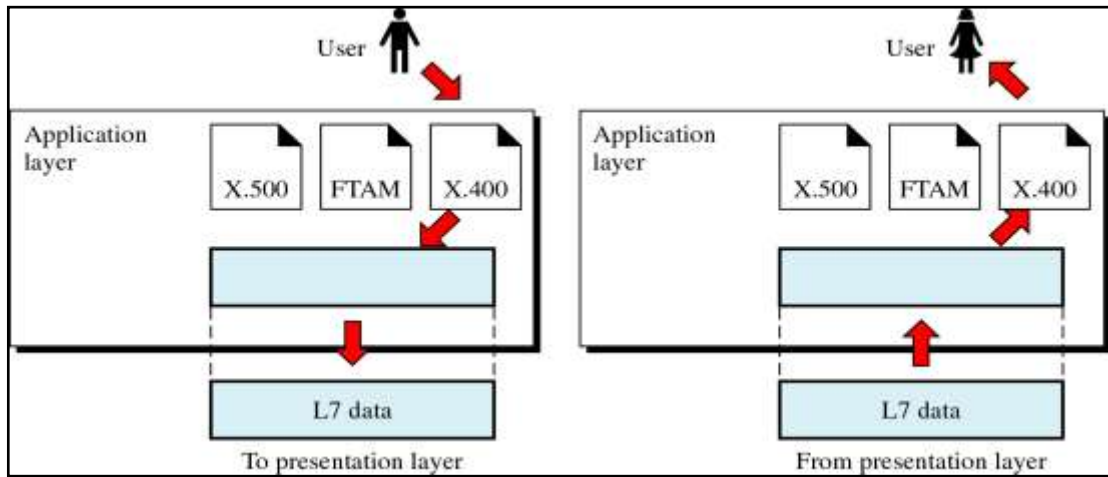


Hình 9: Hoạt động tầng trình diễn

### Tiết 6:

#### 7) Tầng Ứng dụng

Tầng ứng dụng cho phép người sử dụng, phần mềm truy cập vào mạng. Cung cấp giao diện NSD và hỗ trợ cho các dịch vụ như mail, truy cập/truyền file, chia sẻ CSDL và các dịch vụ phân tán khác.



Hình 10: Tầng ứng dụng

**Chức năng chính của tầng ứng dụng:**

- ✓ Cung cấp giao diện cho người dùng truy cập mạng
- ✓ Dịch vụ quản lý và truyền file FTAM, FTP
- ✓ Dịch vụ thư mục
- ✓ Dịch vụ email
- ✓ Dịch vụ DNS
- ✓ Dịch vụ Web
- ✓ ..

❖ **Sự khác nhau 3 tầng trên và 4 tầng dưới**

- ✓ *Physical, Data link, Network, Transport* : Các tầng này đảm nhiệm việc truyền dữ liệu, thực hiện quá trình đóng gói, kiểm duyệt và truyền từng nhóm dữ liệu. Nó không quan tâm đến loại dữ liệu nhận được từ, gửi cho tầng ứng dụng mà chỉ đơn thuần là giữa chúng đi.
- ✓ Chức năng 3 tầng trên *Session, Presentation, Application* liên quan chủ yếu đến việc đáp ứng các yêu cầu của người sử dụng để phát triển các ứng dụng của họ trên mạng thông qua các phương tiện truyền thông cung cấp bởi nhóm tầng thấp.

❖ **Làm rõ một số khái niệm:**

- ✓ Truyền phát : Point to Point, Node to Node và End to End
- ✓ Dạng dữ liệu: Message, Segment, packet và Frame
- ✓ Địa chỉ: Port, IP và MAC

❖ **Ôn tập chương 2**

- b) Nội dung thảo luận
- c) Nội dung tự học  
Mô hình OSI và chức năng của các tầng
- d) Bài tập (bắt buộc, mở rộng)

5. Tài liệu tham khảo (sách, báo – chỉ tiết đến chương, mục, trang)

- i. Bài giảng của giáo viên, Slide chương 2.
- ii. TL [1] , Chương 2,3,5 - 7;

6. Câu hỏi ôn tập

- i. Tại sao phải chuẩn hóa mạng
- ii. Nguyên tắc phân tầng và kiến trúc phân tầng
- iii. Mô hình OSI
- iv. Vai trò và chức năng của các tầng trong mô hình OSI
- v. Phân biệt :
  - ✓ Truyền phát : Point to Point, Node to Node và End to End
  - ✓ Dạng dữ liệu: Message, Segment, packet và Frame
  - ✓ Địa chỉ: Port, IP và MAC

HỌC PHẦN: **Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương II: Mạng cục bộ LAN**

2. Thời lượng:

- GV giảng: 6 tiết.
- Thảo luận: 0 tiết,
- Thực hành: 3 tiết.
- Bài tập: 0 tiết.
- Tự học: 15 tiết

3. Mục đích, yêu cầu:

Mục đích: Giúp sinh viên nắm được kiến thức về mạng LAN. Nắm được ý nghĩa trong thực tế, mô hình kiến trúc và thành phần của mạng. Hiểu được các cách thức điều khiển truy nhập đường truyền: Token bus, Token Ring, CSMA, Ethenet.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://fit.mta.edu.vn/~thiennd/>).
- Làm các bài tập thực hành.

4. Nội dung:

e) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

I. Giới thiệu nội dung của chương

- Giới thiệu ?
- Topology
- Đường truyền
- Thiết bị kết nối
- Các giao thức điều khiển truy cập đường truyền
- Chuẩn Ethernet

Khái niệm và đặc điểm của mạng LAN

*Là mạng thường được lắp đặt trong các công ty, văn phòng nhỏ bán kính tối đa giữa các máy trạm khoảng dưới 1 Km với số lượng máy trạm thường không nhiều hơn 100 máy.*

Đặc điểm:

- ✓ Tốc độ truyền dữ liệu cao 10Mbps → 10 Gbps, tỉ lệ lỗi và chi phí thấp.
- ✓ Phạm vi, qui mô nhỏ
- ✓ Sử dụng các kỹ thuật đơn giản
- ✓ Mô hình: Client/Server hoặc Peer-to-Peer

II. Những kỹ thuật mạng cục bộ

1) Topology:

i. MẠNG HÌNH SAO STAR

Bao gồm các thiết bị đầu cuối (*terminator*) được nối vào trung tâm điều khiển, theo mô hình Client/Server.

Bộ môn An ninh mạng

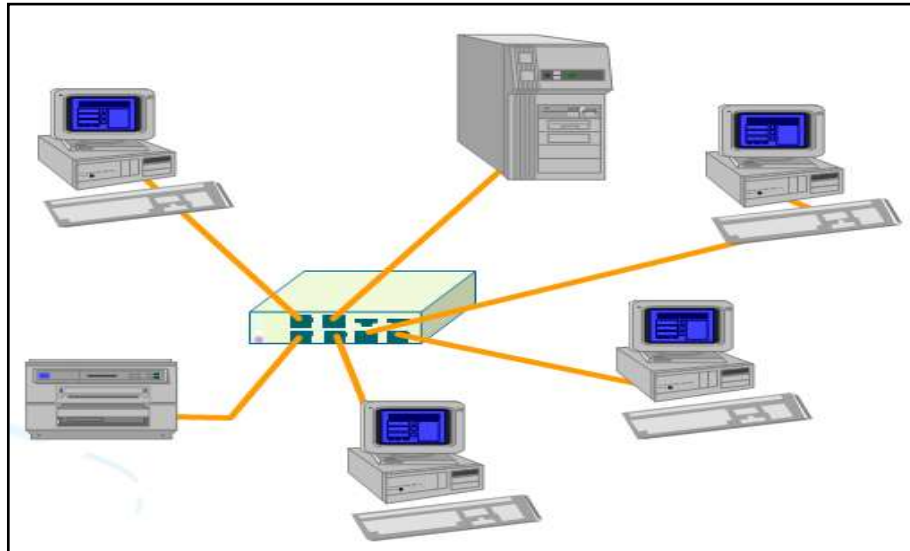
Thiết bị trung tâm sẽ thực hiện việc bắt tay giữa các cặp trạm cần trao đổi thông tin với nhau, thiết lập các liên kết điểm - điểm (*point to point*), xử lý quá trình trao đổi thông tin.

➤ **Ưu điểm:**

- ✓ Lắp đặt đơn giản, dễ dàng cấu hình lại
- ✓ Dễ dàng kiểm soát và khắc phục sự cố.
- ✓ Ít xảy ra va chạm, xung đột trên đường truyền
- ✓ Đạt tốc độ khá cao.

➤ **Nhược điểm:**

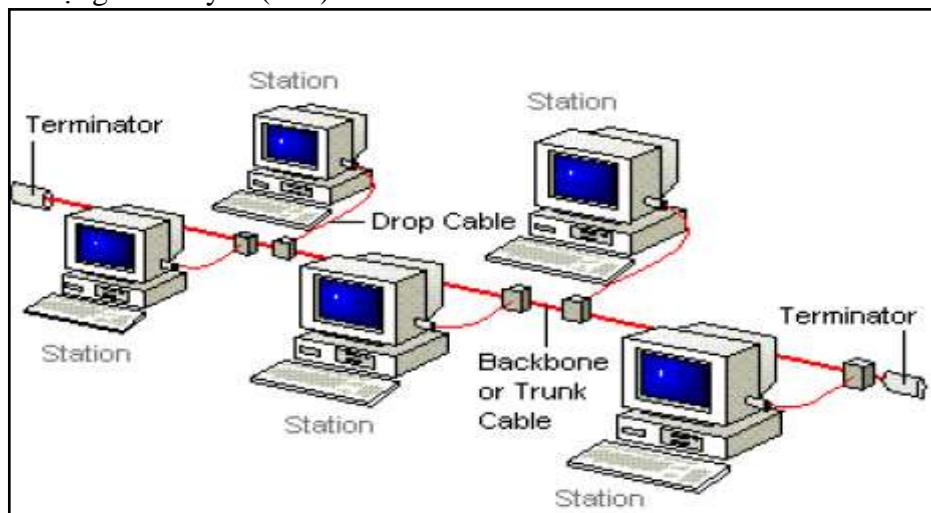
- ✓ Khoảng cách mạng hạn chế.



Hình 11: Mạng hình sao

**Tiết 2:**

ii. Mạng hình tuyến (Bus)



Hình 12: Mạng hình tuyến

Là mạng mà các máy được nối vào một đường trục (*backbone or Trunk Cable*). Ở hai đầu của đường trục có các *Terminator* thực hiện đánh dấu kết thúc và truyền lại dữ liệu.

➤ **Ưu điểm:**

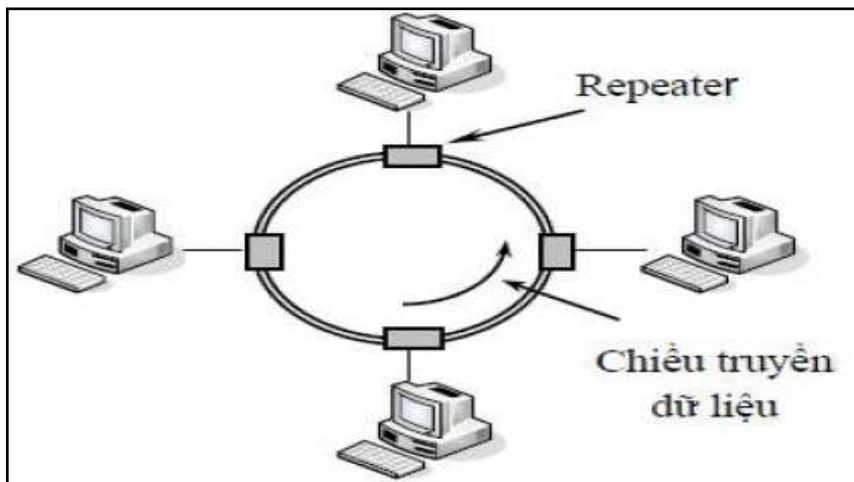
- Phạm vi lớn, tốc độ truyền cao.

➤ **Nhược điểm:**

- Cần giao thức điều khiển truy cập đường truyền
- Khi có sự cố khó kiểm soát và khắc phục, dễ gây ảnh hưởng tới toàn mạng hơn mạng star.



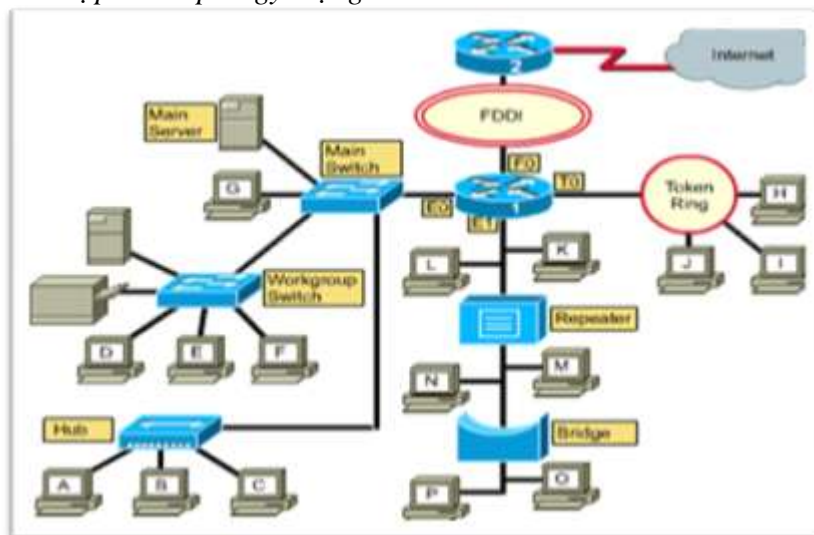
- Dễ xảy ra va chạm, xung đột trên đường truyền
- iii. Mạng hình vòng Ring
  - Mô tả:
  - Đường cáp chính làm thành một vòng khép kín.
  - Các thiết bị đầu cuối được nối với vòng thông qua **Repeater** có nhiệm vụ nhận tín hiệu rồi chuyển tới trạm kế tiếp trên vòng.
  - Tín hiệu được truyền cho nhau theo một chiều, tại một thời điểm chỉ một trạm được truyền.
  - Mỗi trạm khi nhận được một gói dữ liệu có thể nhận hoặc chuyển tiếp.
  - Giao thức điều khiển thẻ bài (Token)



Hình 13: Mạng hình vòng

- **Ưu điểm:**
  - ✓ Nới rộng vòng xa
- **Nhược điểm:**
  - ✓ Đường dây phải khép kín, nếu bị ngắt ở nơi nào đó thì hệ thống bị ngưng.
  - ✓ Giao thức điều khiển truyền dữ liệu phức tạp.
- iv. Mạng hỗn hợp
 

*Là kết hợp các topology mạng ở trên.*



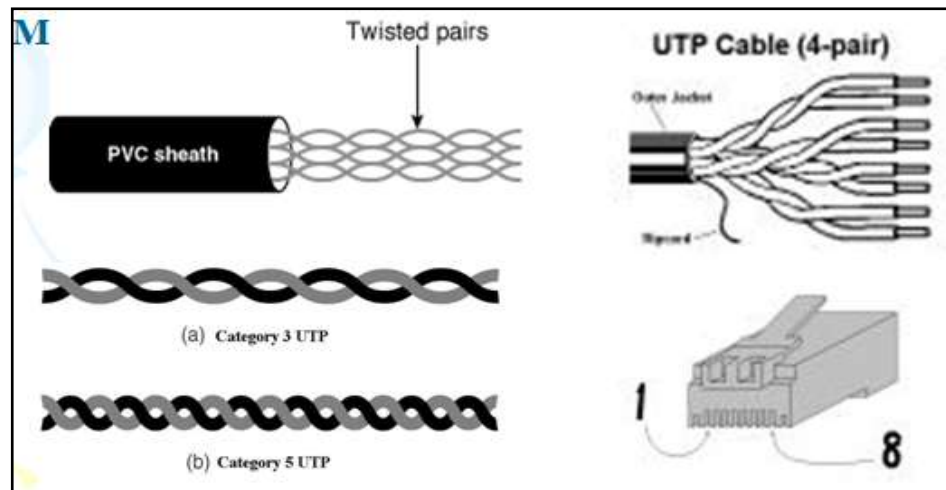
Hình 14: Topo mạng hỗn hợp

### Tiết 3:

#### 2) Môi trường truyền tin:

- i. Cáp dây xoắn (Twisted Pair)
  - Truyền dữ liệu ở cự li ngắn khoảng 100m.

- Gồm 8 sợi chia làm 4 cặp, lý thuyết là 500Mb/s, thực tế 100Mb/s



Hình 15: Cáp dây xoắn

- ii. Cáp đồng trục:  
Tốc độ cáp đồng trục có thể lên tới 35 Mbit/s và băng thông cáp hiện đạt gần đạt đến 1 GHz, dùng trong mạng LAN với khoảng cách 200m, thường dùng trong mạng hình Bus.
- iii. Cáp quang(Fiber Optics):  
Cáp sợi quang bao gồm một sợi thủy tinh cực mảnh(core), bên ngoài là lớp thủy tinh đồng tâm hay còn gọi là lớp phủ (cladding) có chỉ số khúc xạ thấp hơn. Tiếp đến là lớp nhựa mỏng bảo vệ bên ngoài.
- iv. Sóng Radio
- v. Sóng Viba
- vi. Sóng Hồng ngoại
- vii. Bluetooth

### 3) Các thiết bị kết nối trong mạng LAN (giới thiệu)

- ✓ Repeater
- ✓ Hub
- ✓ Bridge
- ✓ Switch
- ✓ Router
- ✓ Gateway

### Tiết 4:

#### 4) Các giao thức điều khiển truy nhập đường truyền

##### ➤ Hai phương pháp chính:

1. Các giao thức truy nhập ngẫu nhiên có thể truy cập phương tiện truyền theo thuật toán xác suất ngẫu nhiên: **CSMA, CSMA/CD (Carrier Sense Multiple Access/ Collision Detect)** (dùng cho đường bus)
2. Truy nhập có điều khiển là phương pháp điều khiển tranh chấp: **Token Bus, Token Ring** đây là 2 giao thức thích hợp nhất cho các mạng cục bộ.

##### i. Giao thức truy nhập ngẫu nhiên

Giao thức đường dây đa truy cập với cảm nhận va chạm:

- ✓ Một trạm sẽ kiểm tra đường truyền trước khi gửi gói dữ liệu của mình đi.
- ✓ Giao thức phải phát hiện được xung đột và các trạm phải ngưng truy nhập, chờ sau 1 thời gian ngẫu nhiên khác nhau truy cập lại.

##### a. CSMA (PP đường dây đa truy cập - LBT )

Khi truyền dữ liệu trước hết phải kiểm tra xem phương tiện truyền có rảnh không. Nếu rảnh thì bắt đầu truyền, nếu bận thì thực hiện 1 trong 3 giải thuật sau:



- 1) Tạm thời rút lui và chờ 1 khoảng thời gian ngẫu nhiên nào đó rồi lại bắt đầu nghe đường truyền. Giải thuật này tránh xung đột nhưng lại có thời gian chết.
- 2) Tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu đi. Giảm được thời gian chết nhưng nếu nhiều trạm cùng chờ thì xảy ra xung đột.
- 3) Tiếp tục kiểm tra đường truyền đến khi đường truyền rảnh thì truyền dữ liệu với xác suất  $p < 1$ . Giải thuật này giảm được xung đột và thời gian chết.

⇒ Không có khả năng phát hiện xung đột trong quá trình truyền, dẫn đến lãng phí đường truyền. Khắc phục bằng phương pháp CSMA/CD.

b. **CSMA/CD** (Đường dây đa truy cập với cảm nhận va chạm - LWT)

Trong khi đang truy nhập, máy trạm vẫn tiếp tục kiểm tra. Phương pháp này ngoài các chức năng như CSMA còn có chức năng tránh những xung đột trên mạng bằng các qui tắc sau:

- Khi đang truyền vẫn tiếp tục kiểm tra đường truyền
- Nếu phát hiện có xung đột thì ngừng truyền và tiếp tục gửi các thông báo cho các trạm cùng biết sự kiện xung đột này.
- Sau khi chờ một thời gian ngẫu nhiên thì trạm thử truyền lại bằng cách sử dụng các phương pháp của CSMA.

⇒ Với mạng sử dụng giao thức này thì thời gian chiếm dụng đường truyền giảm xuống và giảm được tối đa xung đột.

## **Tiết 5:**

### **ii. Giao thức truy nhập có điều khiển**

*Các phương pháp này chủ yếu dùng kỹ thuật chuyển thẻ bài để cấp phát quyền truy nhập đường truyền. Thẻ bài ở đây là một đơn vị dữ liệu đặc biệt, có kích thước và nội dung được qui định riêng cho mỗi phương pháp. Ta sẽ xét hai phương pháp tiêu biểu : Token bus, Token Ring.*

#### **a. Token Bus**

*Đây là giao thức truy nhập có điều khiển trong để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu.*

- ✓ Đầu tiên các trạm trên bus tạo nên một vòng logic, các vị trí được xác định theo thứ tự. Mỗi trạm được biết địa chỉ của trạm kế sau và trước nó.
- ✓ Các Token bus được luân chuyển trên vòng logic. Token chỉ được chuyển cho trạm tiếp theo trong vòng logic khi truyền xong hoặc hết thời hạn.

#### **Các chức năng:**

- [1] Khởi tạo vòng logic
- [2] Bổ sung và loại bỏ các trạm ra khỏi vòng logic.
- [3] Quản lý lỗi: trùng địa chỉ, mất thẻ bài dẫn đến treo, rơi vào trạng thái chờ lẫn nhau.

#### **Giải thuật cho các chức năng trên:**

- [4] Bổ sung 1 trạm vào vòng logic
- [5] Loại bỏ 1 trạm ra khỏi vòng logic
- [6] Quản lý lỗi

[7] Khởi tạo lại vòng logic

### **b. Token Ring**

- ✓ Trong Token ring có một bit biểu diễn trạng thái sử dụng của nó. Một trạm muốn truyền dữ liệu thì phải đợi đến khi nhận được một thẻ bài “rỗi”.
- ✓ Khi đó trạm sẽ đổi bit trạng thái thành “bận” và truyền một đơn vị dữ liệu cùng với thẻ bài đi theo chiều của vòng.
- ✓ Dữ liệu đến trạm đích sẽ được sao lại, sau đó cùng với thẻ bài đi tiếp đến khi về trạm nguồn.
- ✓ Trạm nguồn sẽ xoá dữ liệu, bit trạng thái -> rỗi và cho lưu chuyển trên vòng để các trạm khác có thể nhận được quyền truyền dữ liệu.

Đặc điểm:

- ✓ Hiệu quả hơn khi tải nặng và tránh được xung đột
- ✓ Việc truyền Token sẽ không thực hiện được nếu xoay vòng bị đứt đoạn.
- ✓ Phải có cơ chế kiểm tra Token để kiểm tra và khôi phục Token bị mất.

### ➤ **So sánh CSMA/CD và Tokens**

- ✓ Các phương pháp dùng thẻ bài phức tạp hơn so với CSMA/CD. Hiệu quả không cao trong điều kiện tải nhẹ: một trạm có thể phải đợi khá lâu mới đến lượt.
- ✓ Ưu điểm của các phương pháp dùng thẻ bài: khả năng điều hoà lưu thông trong mạng, lập chế độ ưu tiên cấp phát thẻ bài cho các trạm cho trước. Đặc biệt hiệu quả trong các trường hợp tải nặng.

## **Tiết 6:**

### **III. Chuẩn hóa mạng cục bộ**

#### **1) Giới thiệu**

- Ethernet được phát triển bởi các hãng Xerox, Digital, Intel vào đầu những năm 1970. Phiên bản đầu tiên của Ethernet được thiết kế như một hệ thống 2,94 Mbps để nối hơn 100 máy tính vào một sợi cáp dài 1 Km. Sau đó các hãng lớn đã thảo luận và đưa ra chuẩn dành cho Ethernet 10 Mbps. Ethernet được hình thành bởi định nghĩa chuẩn 802.3 của IEEE – Institute of Electrical and Electronics Engineers
- Ngày nay, mạng Ethernet trở nên quá thịnh hành đến nỗi khi nói đến "kết nối mạng LAN" hoặc "card mạng" người ta đã nghĩ ngay đến mạng Ethernet.
- Về căn bản, Ethernet là một môi trường mạng LAN có môi trường truyền thông được chia sẻ (shared media LAN). Tất cả các trạm trên mạng (network station) chia nhau tổng băng thông của mạng (LAN bandwidth). Băng thông này có thể là 10Mbps (megabit per second = megabit/giây), 100Mbps hoặc 1000Mbps. Ngày nay, người ta còn dùng khái niệm Switched Ethernet (Mạng Ethernet chuyển mạch) để nói về công nghệ mạng LAN Ethernet sử dụng Switch thay cho Hub.

#### **2) Thành phần và đặc điểm của Ethernet**

Mạng Ethernet có thể sử dụng cáp đồng trục (coaxial cable), cáp xoắn đôi (twisted-pair cable), cáp quang (Optical Fiber) hoặc vô tuyến (wireless)... và có thể sử dụng cả cấu trúc tuyến tính (bus) và hình sao (star)

Thành phần Ethernet bao gồm :

- DTE – data terminal equipment: các thiết bị truyền và nhận dữ liệu DTEs thường là PC, Workstation....

Bộ môn An ninh mạng

- DCE – data communication equipment: là các thiết bị kết nối mạng cho phép nhận và chuyển khung trên mạng
- Interconnecting media: cáp xoắn đôi, cáp đồng, cáp quang

Ethernet chuẩn thường có cấu hình bus, truyền với tốc độ 10Mbps và dựa vào CSMA/CD (Carrier Sense Multiple Access / Collision Detection) để điều chỉnh lưu thông trên đường cáp chính. Tóm lại những đặc điểm cơ bản của Ethernet như sau:

- Cấu hình: bus hoặc star.
- Phương pháp chia sẻ môi trường truyền: CSMA/CD.
- Quy cách kỹ thuật IEEE 802.3
- Vận tốc truyền: 10 – 100 Mbps.
- Cáp: cáp đồng trục mảnh, cáp đồng trục lớn, cáp UTP.
- Tên của chuẩn Ethernet thể hiện 3 đặc điểm sau:
- Con số đầu tiên thể hiện tốc độ truyền tối đa.
- Từ tiếp theo thể hiện tín hiệu dải tần cơ sở được sử dụng (Base hoặc Broad).

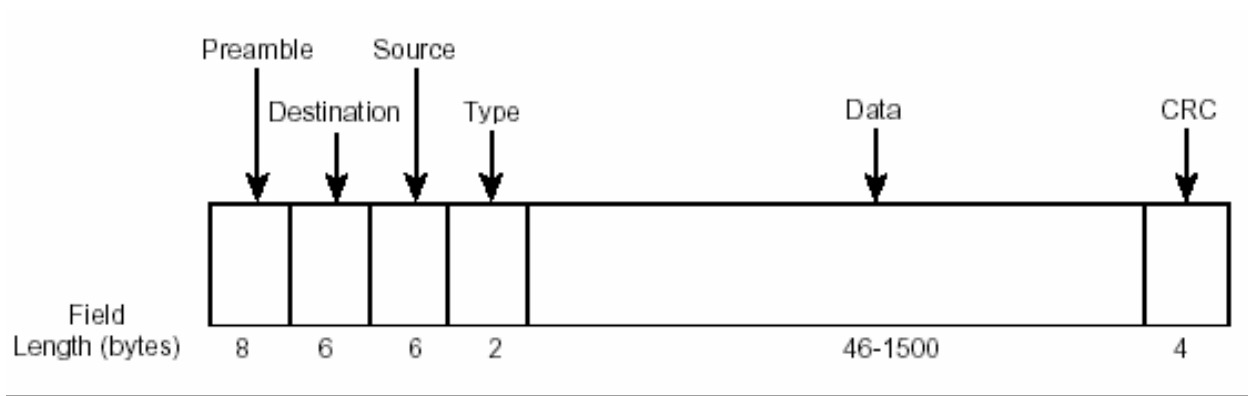
+ Ethernet dựa vào tín hiệu Baseband sẽ sử dụng toàn bộ băng thông của phương tiện truyền dẫn. Tín hiệu dữ liệu sẽ được truyền trực tiếp trên phương tiện truyền dẫn mà không cần thay đổi kiểu tín hiệu.

- + Trong tín hiệu Broadband (ethernet không sử dụng), tín hiệu dữ liệu không bao giờ gửi trực tiếp lên phương tiện truyền dẫn mà phải thực hiện điều chế.
- Các ký tự còn lại thể hiện loại cáp được sử dụng. Ví dụ: chuẩn 10Base2, tốc độ truyền tối đa là 10Mbps, sử dụng tín hiệu Baseband, sử dụng cáp Thinnet.

Card mạng Ethernet: hầu hết các NIC cũ đều được cấu hình bằng các jump (các chấu cắm chuyển) để ấn định địa chỉ và ngắt. Các NIC hiện hành được cấu hình tự động hoặc bằng một chương trình chạy trên máy chứa card mạng, nó cho phép thay đổi các ngắt và địa chỉ bộ nhớ lưu trữ trong một chip bộ nhớ đặc biệt trên NIC.

### 3) ***Định dạng khung Ethernet***

Ethernet chia dữ liệu thành nhiều khung (frame). Khung là một gói thông tin được truyền như một đơn vị duy nhất. Khung trong Ethernet có thể dài từ 64 đến 1518 byte, nhưng bản thân khung Ethernet đã sử dụng ít nhất 18 byte, nên dữ liệu một khung Ethernet có thể dài từ 46 đến 1500 byte. Mỗi khung đều có chứa thông tin điều khiển và tuân theo một cách tổ chức cơ bản.



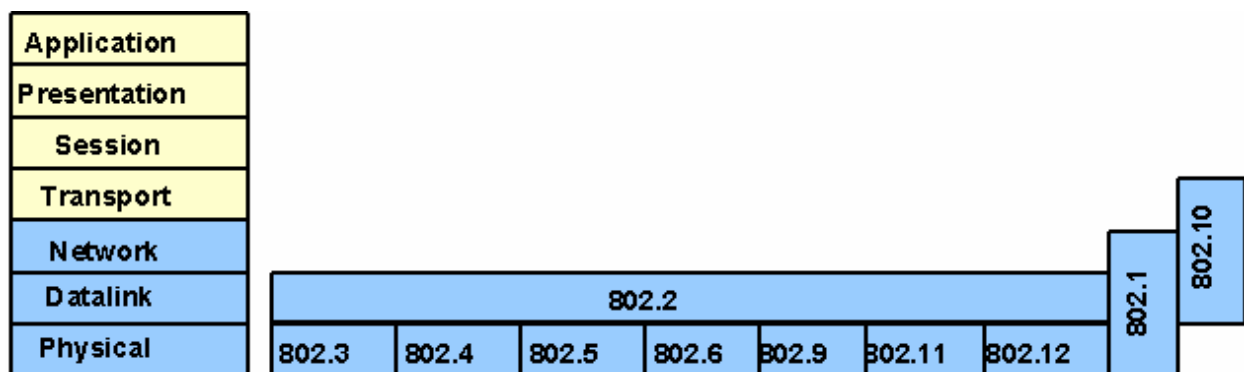
Hình 16: Cấu trúc khung Ethernet

#### 4) Các chuẩn IEEE 802.x

Trong LAN, tầng liên kết dữ liệu được chia làm 2 tầng con: LLC (Logical Link Control) và MAC. MAC quản lý việc truy cập đường truyền trong khi LLC đảm bảo tính độc lập của việc quản lý các liên kết dữ liệu với đường truyền vật lý và phương pháp truy cập đường truyền MAC. IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng cục bộ với dự án IEEE 802 nổi tiếng bắt đầu từ năm 1980. Sau đó, họ IEEE 802.x ra đời tạo nên tầng quan trọng trong việc thiết kế và cài đặt mạng nội bộ.

Họ IEEE 802.x bao gồm các chuẩn như sau:

- i. IEEE 802.1 : High Level Interface
- ii. IEEE 802.2 : Logical Link Control (LLC)
- iii. IEEE 802.3: CSMA/CD
- iv. IEEE 802.4: Token bus
- v. IEEE 802.5: Token ring
- vi. IEEE 802.6: MAN
- vii. IEEE 802.7: Broadband Technical Advisory Group
- viii. IEEE 802.8: Fiber Technical Advisory Group
- ix. IEEE 802.9: Intergrated Data and Voice Network
- x. IEEE 802.10: Standard for Interoperable LAN security
- xi. IEEE 802.11: Wireless LAN
- xii. IEEE 802.12: 100VG – AnyLAN



Hình 17: Quan hệ giữa các chuẩn IEEE 802.x và mô hình OSI

- f) Nội dung thảo luận:
- g) Nội dung tự học
  - i. K/n và đặc điểm mạng LAN

- ii.* Topology
- iii.* Đường truyền và thiết bị kết nối
- iv.* Các giao thức điều khiển truy cập đường truyền
- v.* Chuẩn Ethernet
- h) Bài tập (bắt buộc)
- i) Thực hành

**Tiết 7-9:**

- i.* Thiết kế mô hình mạng LAN cơ bản
  - ii.* Cấu hình mạng trên phần mềm mô phỏng Packet Tracer
  - iii.* Cài đặt modem ADSL, Wireless.
5. Tài liệu tham khảo (sách, báo – chỉ tiết đến chương, mục, trang)
- iii.* Bài giảng của giáo viên, Slide chương 3.
  - iv.* TL [1] , chương 2,3
  - v.* TL[2], 2.6 , 2.7, 2.8 trang 111;
6. Câu hỏi ôn tập:
- i.* Trình bày các khái niệm và đặc điểm mạng LAN
  - ii.* Trình bày các topology mạng LAN nêu rõ ưu nhược điểm
  - iii.* Trình bày các giao thức điều khiển truy nhập
  - iv.* Trình bày chuẩn Ethernet.

**HỌC PHẦN: Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương 4: Mạng diện rộng WAN**

2. Thời lượng:

- GV giảng: 3 tiết.
- Thảo luận: 0 tiết,
- Thực hành: 6 tiết.
- Bài tập: 3 tiết.
- Tự học: 12 tiết

3. Mục đích, yêu cầu:

Mục đích: Giúp sinh viên nắm được kiến thức và ứng dụng của mạng WAN. Nắm chắc nội dung về công nghệ và định tuyến trong mạng WAN. Có khả năng thiết kế được mạng WAN cơ bản.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://fit.mta.edu.vn/~thiennd/>).
- Làm bài tập trên lớp và ở nhà.
- Thực hành tại phòng thí nghiệm.

4. Nội dung:

a) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

➤ **Giới thiệu nội dung chương:**

1. Giới thiệu mạng WAN
2. Công nghệ kết nối mạng WAN
3. Định tuyến trong mạng WAN
  - 3.1. Kỹ thuật chọn đường
  - 3.2. Các giải thuật định tuyến
4. Một số giao thức truyền dẫn
  - 4.1. Mạng tích hợp đa dịch vụ số ISDN
  - 4.2. Mạng chuyển mạch gói X25
  - 4.3. Mạng chuyển mạch khung Frame Relay
  - 4.4. Phương thức truyền dẫn không đồng bộ ATM

1) Giới thiệu:

**Khái niệm:** mạng WAN Là mạng thường được lắp đặt trong phạm vi một quốc gia như Intranet phục vụ cho các công ty lớn, ngành kinh tế có bán kính hoạt động lớn, có thể liên kết nhiều mạng LAN, MAN, đường truyền có thể sử dụng cơ sở hạ tầng của viễn thông.

**Sự cần thiết của liên mạng:**

- ✓ Xuất phát từ nhu cầu trao đổi thông tin và chia sẻ tài nguyên dùng chung, vì vậy đòi hỏi hoạt động truyền thông không chỉ dừng lại ở phạm vi một mạng cục bộ mà phải vươn tới khuôn khổ một vùng, quốc gia và quốc tế.
- ✓ Phải kết nối nhiều mạng đơn lẻ thành một liên mạng (Internetworking) bao gồm nhiều mạng, loại mạng, khoảng cách địa lý khác nhau và chịu sự quản lý của các tổ chức quốc gia khác nhau.

## 2) Công nghệ kết nối mạng WAN

- Liên mạng có thể được liên kết từ: LAN to LAN, LAN to WAN và WAN to WAN. Có ba phương pháp liên kết liên mạng phổ biến:
  - i. **Liên kết tại tầng Physical:** các mạng có cùng cấu trúc và giao thức, bộ lặp **Repeater** được dùng để kết nối các mạng LAN làm tăng bán kính mạng.
  - ii. **Liên kết tại tầng Data link: Bridge và Switche** hoạt động tại tầng liên kết dữ liệu dùng để nối 2 mạng có LAN có cấu trúc và giao thức ở tầng vật lý khác nhau.
  - iii. **Liên kết tại tầng mạng:** các mạng khác nhau về phần cứng, phần mềm, giao thức và thường cung cấp những chức năng, ứng dụng khác nhau. Thực hiện định dạng gói tin từ một mạng đến một mạng khác (đ/c IP), chuyển đổi giao thức mạng. Thiết bị kết nối **Router** chức năng chủ yếu là liên kết các mạng khác nhau về vật lý và chuyển đổi các gói tin từ một mạng này sang một mạng khác, quyết định đường đi của các gói tin đến node đích.
  - iv. **Ở tầng vận chuyển:** Dùng các gateway vận chuyển, thiết bị có thể làm giao diện giữa hai đầu nối kết mức vận chuyển. Ví dụ gateway có thể làm giao diện trao đổi giữa hai nối kết TCP và NSA.
  - v. **Ở tầng ứng dụng:** Các gateway ứng dụng sẽ làm nhiệm vụ chuyển đổi ngữ cảnh của các thông điệp. Ví dụ như gateway giữa hệ thống email Internet và X.400 sẽ làm nhiệm vụ chuyển đổi nhiều trường trong header của email.
- **Kết nối liên mạng dùng router**
  - i. Truyền dữ liệu qua Router
 

Muốn nối nhiều đoạn mạng với các giao thức khác nhau, kiến trúc mạng khác nhau, ta phải cần một thiết bị không những biết **địa chỉ** của mỗi đoạn mạng mà còn **định tuyến** đường truyền tốt nhất để truyền dữ liệu và **lọc lưu lượng quảng bá** trên các đoạn mạng cục bộ. Nó được gọi là **bộ định tuyến Router** nó hoạt động trên *tầng mạng*.
  - ii. Ánh xạ địa chỉ mạng (IP) và địa chỉ MAC
  - iii. Chức năng của Router

## Tiết 2:

### 3) Định tuyến trong mạng WAN

- i. **Các kỹ thuật chọn đường:**

*Chọn đường là sự lựa chọn một con đường để truyền một đơn vị dữ liệu từ trạm nguồn đến trạm đích. Như vậy phải thực hiện hai chức năng chính sau :*

  - ✓ Quyết định chọn đường theo một tiêu chuẩn tối ưu nào đó.
  - ✓ Cập nhật thông tin chọn đường, tức là các thông tin để phục vụ cho chức năng

(1). Có nhiều kỹ thuật chọn đường khác nhau được xây dựng dựa vào các yếu tố sau :

  - [1] Sự phân tán của các chức năng chọn đường tại các nút trên mạng
  - [2] Sự thích nghi với trạng thái hiện hành của mạng

[3] Các tiêu chuẩn tối ưu để chọn đường

Dựa trên yếu tố (a) ta có kỹ thuật chọn đường tập trung hoặc phân tán. Dựa vào yếu tố (b) ta có chế độ chọn đường tĩnh hoặc thích nghi.

Yếu tố (c) có thể lựa chọn trong các tiêu chuẩn sau :

- Đo độ trễ trung bình của việc truyền gói tin
- Số lượng nút trung gian mà gói tin cần chuyển qua để đến đích
- Cước phí truyền tin.

**ii. Các giải thuật định tuyến**

**a. Định tuyến theo vector khoảng cách (RIP)**

Bộ định tuyến duy trì một bảng định tuyến (vector) cung cấp khoảng cách tốt nhất được biết đến mỗi đích (thường là bộ định tuyến). Thông tin của bảng này thường xuyên được cập nhật bằng cách trao đổi thông tin với các bộ định tuyến lân cận.

**Khoảng cách:** có thể là bước nhảy, thời gian trễ đo bằng ms, Thông thường sử dụng thời gian trễ.

**Giải thuật gồm bước sau:**

- [1] Bộ định tuyến tính khoảng cách từ nó đến các bộ định tuyến lân cận bằng cách gửi gói tin ECHO
- [2] Cứ sau T ms mỗi bộ định tuyến lại truyền đến bộ định tuyến lân cận một danh sách các khoảng cách ước lượng cho mỗi đích và nó cũng nhận từ các bộ lân cận khác.
- [3] Cập nhật bảng định tuyến với khoảng cách tốt nhất: ví dụ tính khoảng cách từ J  $\rightarrow$  A, I, H, K.

**b. Định tuyến theo liên kết trạng thái (Link State)**

*Link state được áp dụng rộng rãi trong mạng internet. Nhằm cải tiến thuật toán RIP.*

- ✓ RIP không tính đến băng thông của đường truyền, xem tất cả đường truyền có cùng băng thông.
- ✓ Mất quá nhiều thời gian để hội tụ

**Y tưởng thuật toán:** 5 bước.

- [1] Xác định các bộ định tuyến lân cận
- [2] Đo khoảng cách đến từng bộ lân cận
- [3] Bộ định tuyến xây dựng gói liên kết trạng thái
- [4] Truyền gói này đến tất cả bộ định tuyến khác
- [5] Tính đường đi ngắn nhất đến mỗi bộ định tuyến khác

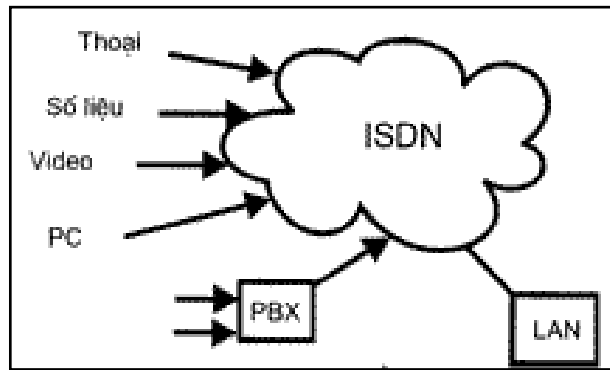
**Tiết 3:**

4) Một số giao thức truyền dẫn:

**i. ISDN**

- ISDN- Integrated Services Digital Network là dịch vụ viễn thông cho phép tiếng nói, văn bản, hình ảnh và video truyền đồng thời qua đường dây điện thoại thường. ISDN dựa trên kỹ thuật chuyển kênh và chuyển mạch gói. Tốc độ băng thông của nó từ 128Kbps đến 1,5Mbps. ISDN cung cấp khả năng truyền dẫn tốc độ cao (so với mạng tương tự hiện nay), chống nhiễu đường truyền, đạt chất lượng và độ chính xác cao, thông tin trung thực.





- Phương thức làm việc của ISDN là tách riêng lưu thông mạng với lưu thông của tiếng nói hay dữ liệu. Để làm được điều này, nó phân chia dung lượng của đường truyền thành một số kênh truyền độc lập. Một kênh trong số đó sẽ nhận trách nhiệm giao tiếp với thiết bị chuyển mạch của văn phòng chính trong khi những kênh khác cho phép người dùng thực hiện các cuộc gọi, hội đàm qua video và truy cập Internet hay mạng LAN.
- Đặc điểm của mạng ISDN :
  - ✓ Là một mạng đa dịch vụ, thay thế nhiều loại viễn thông khác nhau đang cùng tồn tại bằng một mạng duy nhất có khả năng cấp cấp tất cả các dịch vụ hiện tại và các dịch vụ tương lai với một giao tiếp thuê bao duy nhất.
  - ✓ ISDN có hệ thống báo hiệu số 7 và các node chuyển mạch thông minh.
  - ✓ Kiến trúc ISDN tương thích với mô hình OSI. Các giao thức đã được phát triển có liên quan tới các ứng dụng của mô hình OSI có thể được sử dụng trong ISDN. Các giao thức có thể phát triển sử dụng một cách độc lập cho các tầng khác nhau, cho các chức năng riêng của từng tầng mà không ảnh hưởng tới các tầng kề nhau.
- Ứng dụng phổ biến của ISDN:
  - ✓ Kết nối LAN - LAN giữa 2 văn phòng cách xa nhau.
  - ✓ Dịch vụ video, thoại thấy hình: cho phép truyền đồng thời hình ảnh và âm thanh giữa 2 điểm, nhờ vậy hai bên có thể cùng lúc đàm thoại và thấy hình ảnh của nhau.
  - ✓ Truyền Fax qua ISDN đạt tốc độ và chất

## ii. Mạng chuyển mạch gói X.25

X.25 là chuẩn giao của ITU-T (International Telecommunication Union - telecommunications), nó phù hợp cho mạng chuyển mạch gói trong giao tiếp mạng WAN. X.25 hoạt động ở 3 cấp độ tương ứng với 3 tầng đầu trong mô hình OSI

- ✓ **Tầng vật lý:** Tương ứng với tầng vật lý mô hình OSI, giao thức X.25 xác định các vấn đề về điện, hàm, thủ tục và kiểu các bộ đầu chuyển được sử dụng. Bao gồm các chuẩn của CCITT X26/27 và EIA (USA Electronic Institute Association), RS :X.21, X.21 Bis, V.32...
- ✓ **Tầng liên kết dữ liệu:** X.25 cung cấp các liên kết giữa hai thiết bị đầu cuối của một tuyến thông tin có độ tin cậy cao, kiểm soát luồng và kiểm soát lỗi. LAP-B (Link Access Procedure Balanced) là giao thức LLC tầng con của Liên kết dữ liệu, chuẩn hướng bit, hoạt động theo chế độ song công và đồng bộ.
- ✓ **Tầng cấp mạng:** X.25 là giao thức giữa một DTE và một DCE. DTE có thể là một PAD còn DCE có thể là một thiết bị X.25. Giao thức X.25 cung cấp các khả năng chọn mạch ảo thường trực hay theo nhu cầu. X.25 yêu cầu cung cấp dịch vụ tin cậy và tính năng điều khiển luồng dữ.

**iii. Frame relay hay chuyển tiếp khung:**

Trong kỹ thuật này thì cả hai thiết bị ở hai đầu nối đều tiến hành kiểm lỗi. Chuyển tiếp khung dùng các gói (hay khung) có độ dài khác nhau và hoạt động ở tầng liên kết dữ liệu (*data link layer*) trong mẫu OSI. Vận tốc 56Kbps trong các mạch điện thoại, hay T-1 (1.544 Mbps) và T-3 (45 Mbps). Kỹ thuật này sẽ không dùng tới việc sửa lỗi

**iv. ATM hay là một vận chuyển không đồng bộ (*Asynchronous Transfer Mod*)**

Thường được dùng để vận chuyển các loại thông tin đa dạng như là âm thanh, hình ảnh và dữ liệu. Các gói dữ liệu có cỡ bằng nhau cố định là 53 bit gọi là *cell*. Mỗi cell có 5 byte cho phần đầu và 48 byte cho phần dữ liệu. Kỹ thuật này dùng thiết bị phần cứng để tiến hành các động thái nối-chuyển. Đặc điểm của ATM là dùng kỹ thuật băng thông cao, thời gian ngưng thấp (*low-delay*) và nén kênh (*multiplexing*). Vận tốc từ 155Mbps đến 622 Mbps.

b) Nội dung thảo luận:

c) Nội dung tự học

- i. Công nghệ kết nối trong mạng WAN
- ii. Các phương pháp định tuyến
- iii. Một số giao thức truyền dẫn

d) Bài tập (bắt buộc)

**Tiết 4-6:**

- i. Cấu hình định tuyến tĩnh
- ii. Tính toán định tuyến theo vector khoảng cách.

e) Thực hành:

- i. Thiết kế mạng WAN đơn giản.
- ii. Cấu hình định tuyến tĩnh cho router
- iii. Cấu hình định tuyến động RIP
- iv. Cấu hình cho các phương pháp định tuyến khác.

5. Tài liệu tham khảo (sách, báo – chỉ tiết đến chương, mục, trang)

- i. Bài giảng của giáo viên, Slide chương 4.
- ii. TL [1] chương 5; trang 259
- iii. TL [2] chương 3, 4. Trang 164

6. Câu hỏi ôn tập:

- i. Khái niệm và tầm quan trọng của mạng WAN.
- ii. Các kỹ thuật kết nối trong mạng WAN.
- iii. Kỹ thuật định tuyến và các phương pháp định tuyến.
- iv. Các kỹ thuật truyền dẫn.

HỌC PHẦN: **Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương V: Thiết bị mạng máy tính**

2. Thời lượng:

- GV giảng: 3 tiết.
- Thảo luận: 0 tiết,
- Thực hành: 3 tiết.
- Bài tập: 0 tiết.
- Tự học: 6 tiết

3. Mục đích, yêu cầu:

Mục đích: Giúp sinh viên nhận biết và nắm chắc chức năng của các thiết bị mạng. Biết các lắp đặt và cấu hình cho các thiết bị. Trên cơ sở đó thiết kế và cài đặt được các mạng LAN, WAN cơ bản đã học.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://http://fit.mta.edu.vn/~thiennd/>).
- Làm bài thực hành trên lớp và ở nhà.

4. Nội dung:

j) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

1) Giới thiệu mục đích, yêu cầu và nội dung của chương

- i. Môi trường truyền và dây nối
- ii. Repeater
- iii. Hub
- iv. Bridge
- v. Switch
- vi. Router
- vii. Gateway

2) Môi trường truyền và dây nối (Nhắc lại và làm chi tiết thêm nội dung đã học ở chương 3)

3) Repeater

- ✓ Là thiết bị đơn giản nhất trong các thiết bị liên kết mạng, hoạt động tầng vật lý của mô hình OSI.
- ✓ Repeater dùng để nối 2 mạng giống nhau, đoạn mạng.
- ✓ Repeater nhận được một tín hiệu từ một phía của mạng thì nó sẽ phát tiếp vào phía kia của mạng.
- ✓ Repeater loại bỏ các tín hiệu méo, nhiễu, khuếch đại tín hiệu đã bị suy hao. Việc sử dụng Repeater làm tăng thêm chiều dài của mạng.

➤ Hai loại Repeater chính

- ✓ **Repeater điện:** hai phía là tín hiệu điện
  - Repeater điện có thể làm tăng khoảng cách mạng, nhưng vẫn bị hạn chế do độ trễ của tín hiệu.

- Ví dụ với mạng sử dụng cáp đồng trục 50 thì khoảng cách tối đa là 2.8 km, cho dù sử dụng thêm Repeater.
- ✓ **Repeater điện quang:** liên kết với một đầu cáp quang và một đầu là cáp điện.
  - Việc sử dụng Repeater không thay đổi nội dung các tín hiệu đi qua nên nó chỉ được dùng để nối hai mạng có cùng giao thức truyền thông.

#### 4) Hub

Thường được dùng để nối các mạng hình sao. Hub được chia thành 3 loại như sau :

##### i. Hub bị động (Passive Hub) :

Không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng.

##### ii. Hub chủ động (Active Hub) :

có các linh kiện điện tử có thể khuếch đại và xử lý các tín hiệu.

- ✓ Làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách mạng có thể tăng lên.
- ✓ Giá thành cao hơn nhiều Hub bị động.

##### iii. Hub thông minh (Intelligent Hub)

- ✓ Là Hub chủ động, nhưng có bộ vi xử lý và bộ nhớ vì vậy nó có thể hoạt động như bộ tìm đường hay một cầu nối.
- ✓ Nó có thể cho phép các gói tin tìm đường rất nhanh trên các cổng của nó, các gói tin được định tuyến.

### Tiết 2:

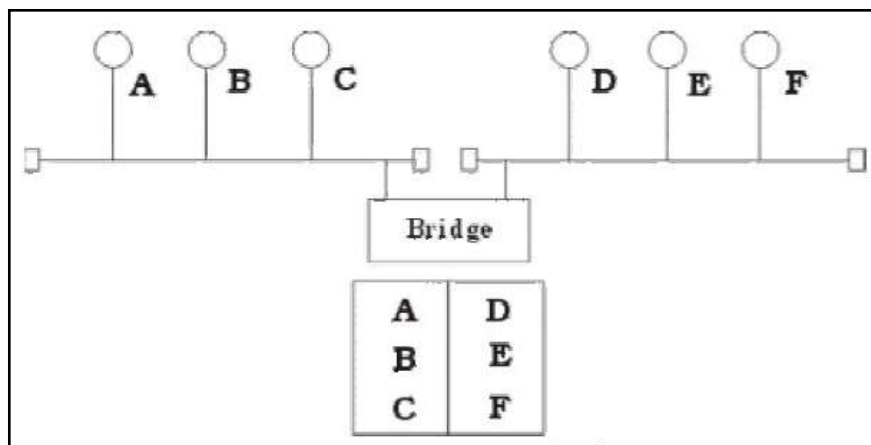
#### 5) Bridge

Bridge là một thiết bị có xử lý dùng để nối hai mạng giống nhau hoặc khác nhau, nó có thể được dùng với các mạng có các giao thức khác nhau.

Bridge hoạt động trên tầng liên kết dữ liệu, nó đọc và xử lý các gói tin của tầng liên kết dữ liệu trước khi quyết định có chuyển đi hay không.

➤ Để thực hiện điều này Bridge cung cấp cơ chế:

- ✓ Mỗi phía có một bảng các địa chỉ các trạm kết nối.
- ✓ Quyết định gửi gói tin sang mạng khác hay không.
- ✓ Bổ sung địa chỉ máy trạm cho bảng địa chỉ

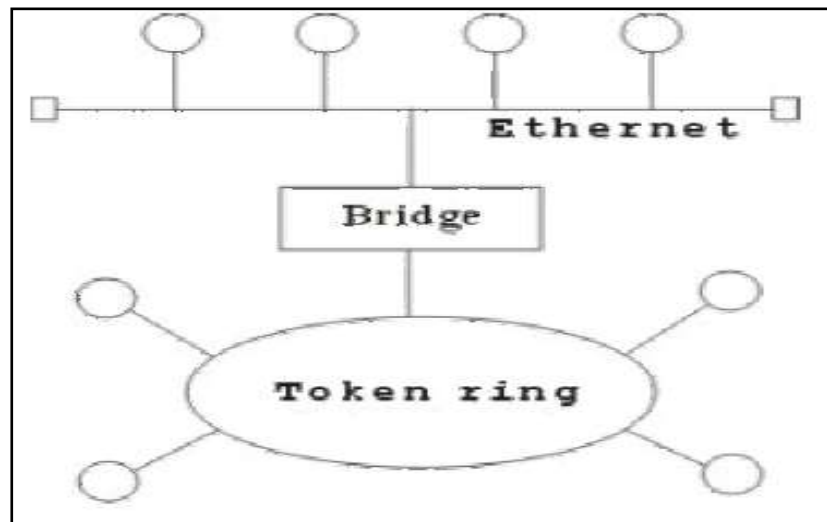


Hình 5.1 Kết nối và bảng địa chỉ của bridge

➤ Để đánh giá một Bridge người ta đưa ra hai khái niệm : *Lọc* và *chuyển vận*.

- ✓ Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của Bridge.

- ✓ Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển các gói tin từ mạng này sang mạng khác.
- Hiện nay có hai loại Bridge đang được sử dụng là *Bridge vận chuyển* và *Bridge biên dịch*.
  - ✓ **Bridge vận chuyển** dùng để nối hai mạng LAN có giao thức ở tầng LKDL giống nhau, nhưng có thể có loại dây nối khác nhau.  
Nó không có khả năng thay đổi cấu trúc các gói tin mà chỉ quan tâm việc định tuyến.
  - ✓ **Bridge biên dịch** dùng để nối hai mạng LAN có giao thức khác nhau nó có khả năng chuyển một gói tin thuộc mạng này sang gói tin thuộc mạng kia, cùng kích thước.

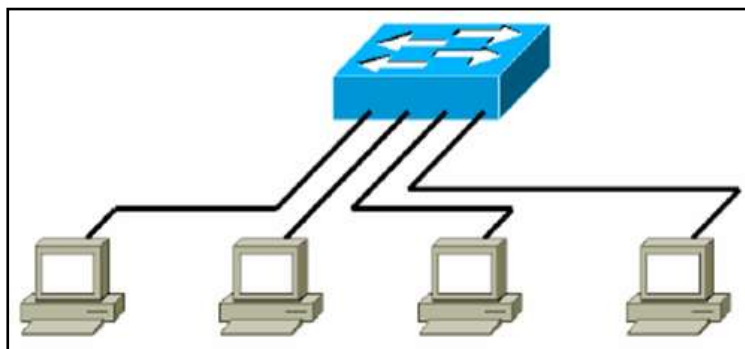


Hình 5.2 Bridge biên dịch

- Sử dụng Bridge trong các trường hợp sau :
  - ✓ Mở **rộng** mạng hiện tại khi đã đạt tới khoảng cách tối đa
  - ✓ Giảm bớt tắc nghẽn mạng
  - ✓ Để nối các mạng có giao thức khác nhau.

#### 6) Switch

*Switch tương tự như một Bridge có nhiều cổng. Switch cũng có khả năng "học" thông tin của mạng thông qua các gói tin và sử dụng các thông tin này để xây dựng lên bảng Switch.*



Hình 5.3 Switch

- Đặc điểm Switch:
  - ✓ Chuyển các khung dữ liệu từ nguồn đến đích, và xây dựng các bảng Switch.
  - ✓ Switch hoạt động ở tốc độ cao hơn nhiều so với Repeater và có thể cung cấp nhiều chức năng hơn như khả năng tạo mạng LAN ảo (VLAN).

- ✓ Hiện nay có nhiều loại switch có khả năng hoạt động ở tầng mạng. Được gọi là Switch tầng 3.

### **Tiết 3:**

#### **7) Router**

*Hoạt động trên tầng mạng, chức năng chính là định tuyến (tìm được đường đi tốt nhất cho các gói tin qua nhiều mạng).*

##### **i. Hoạt động:**

- ✓ Router có địa chỉ nên nó nhận và xử lý các gói tin gửi đến nó mà thôi.
- ✓ Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.
- ✓ Để chọn đường tối ưu cho các gói tin Router có một bảng định tuyến. Cập nhật bảng dựa trên các Router gần đó và các mạng trong liên mạng nhờ thuật toán xác định trước.

##### **ii. Router được chia thành hai loại.**

- ✓ **Router phụ thuộc giao thức:** Chỉ thực hiện việc tìm đường và truyền gói tin từ mạng này sang mạng khác, có chung một giao thức truyền thông.
- ✓ **Router không phụ thuộc vào giao thức:** dùng liên kết các mạng có giao thức khác nhau và kích thích các gói tin có thể khác nhau (chia nhỏ một gói tin).

##### **iii. Các lý do sử dụng Router:**

- ✓ **Router** thường được sử dụng trong khi nối các mạng thông qua các đường dây thuê bao đắt tiền do nó không truyền dư lên đường truyền.
- ✓ **Router** có thể dùng trong một liên mạng có nhiều vùng, mỗi vùng có giao thức riêng biệt.

##### **iv. Một số giao thức hoạt động chính của Router**

- ✓ **RIP** (Routing Information Protocol): sử dụng SPX/IPX và TCP/IP, RIP hoạt động theo phương thức véc tơ khoảng cách.
- ✓ **NLSP** (Netware Link Service Protocol): được phát triển bởi Novell dùng để thay thế RIP hoạt động theo phương thức vectơ khoảng cách, mỗi Router được biết cấu trúc của mạng và việc truyền các bảng định tuyến giảm đi.
- ✓ **OSPF** (Open Shortest Path First): là một phần của TCP/IP với phương thức trạng thái tĩnh, trong đó có xét tới ưu tiên, giá đường truyền, mật độ truyền thông...
- ✓ **OSPF-IS** (Open System Interconnection Intermediate System to Intermediate System): giống như OSPF

#### **8) Gateway**

*Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng LAN, WAN, interne và điện thoại; việc chuyển đổi thực hiện trên cả 7 tầng.*

**Ví dụ:** mạng của bạn sử dụng giao thức IP và mạng của ai đó sử dụng giao thức IPX, Novell, DECnet, SNA... thì Gateway sẽ chuyển đổi từ loại giao thức này sang loại khác.

##### **k) Nội dung thảo luận:**

##### **l) Nội dung tự học**

##### **i. Chức năng, ứng dụng và cách cài đặt cấu hình cho các thiết bị**

- Repeater
- Hub
- Bridge
- Switch

- Router
- Gateway

m) Bài tập (bắt buộc)

n) Thực hành

Thiết kế và cài đặt mạng đơn giản mô phỏng hoạt động của từng thiết bị ở trên

Thiết kế và cài đặt mạng sử dụng kết hợp các thiết bị Hub, Switch và Router.

5. Tài liệu tham khảo (sách, báo – chỉ tiết đến chương, mục, trang)

vi. Bài giảng của giáo viên, Slide chương 5.

vii. TL [4] , chương 4; trang 234

viii. Tài liệu về các thiết bị của các hãng sản xuất: Cissco, D-Link,..

6. Câu hỏi ôn tập:

v. Trình bày chức năng và ứng dụng của các thiết bị mạng đã học trong bài.

vi. Để nối hai mạng có giao thức tầng mạng khác nhau ta phải dùng thiết bị nào?

vii. Repeater có khả năng nối mạng token bus với mạng token ring hay không?

**HỌC PHẦN: Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương VI: Mô hình TCP/IP và mạng Internet**

2. Thời lượng:

- GV giảng: 6 tiết.
- Thảo luận: 3 tiết,
- Thực hành: 3 tiết.
- Bài tập: 0 tiết.
- Tự học: 12 tiết

3. Mục đích, yêu cầu:

Mục đích: Sinh viên nắm được mô hình mạng thực tế TCP/IP là một tham chiếu của mô hình OSI. Nắm được hoạt động, chức năng của các tầng và các giao thức cụ thể trong tầng đó. Trình bày rõ cấu trúc, hoạt động và các ứng dụng của mạng Internet.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://http://fit.mta.edu.vn/~thiennd/>).
- Chuẩn bị bài thảo luận.
- Chuẩn bị và tham gia thực hành tại phòng thí nghiệm

4. Nội dung:

o) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

➤ Giới thiệu nội dung chương

1. Mô hình TCP/IP

1.1. Mô hình kiến trúc TCP/IP

1.2. Vai trò và chức năng các tầng

2. Các giao thức cơ bản của mô hình TCP/IP

3. Mạng Internet

3.1. Giới thiệu chung về mạng Internet

3.2. Cấu trúc mạng Internet

3.3. Công nghệ kết nối mạng Internet

3.4. Một số dịch vụ cơ bản trên mạng Internet

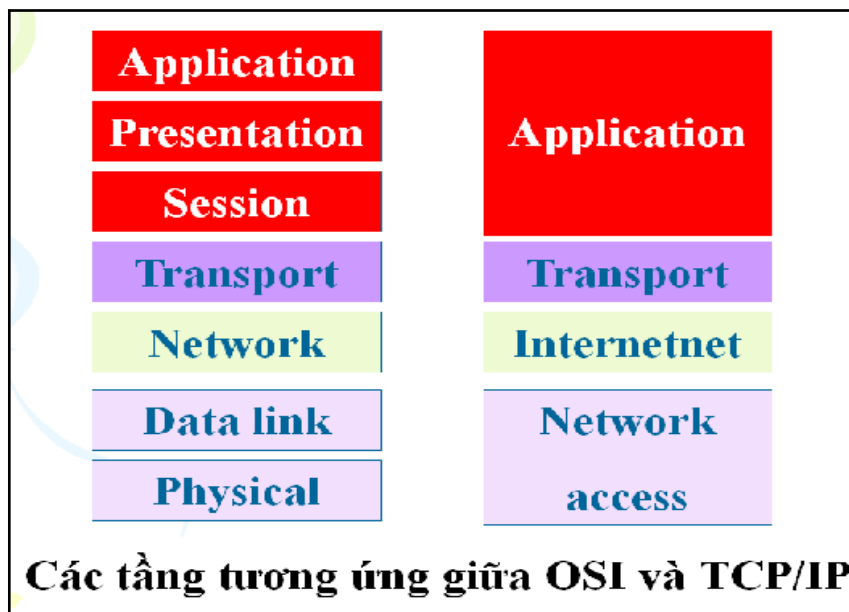
1) Mô hình TCP/IP

i. Giới thiệu:

- ✓ Cuối năm 1960 và đầu 1970, Trung tâm nghiên cứu cấp cao (Advanced Research Projects Agency - ARPA) bộ quốc phòng Mỹ (DoD) được giao trách nhiệm phát triển mạng ARPANET.
- ✓ Đầu năm 1980, bộ giao thức TCP/IP ra đời làm giao thức chuẩn cho mạng ARPANET và các mạng của DoD.
- ✓ Mô hình TCP/IP có 4 tầng
  - Tầng ứng dụng (Application Layer)
  - Tầng giao vận (Transport Layer)



- Tầng Internet (Internet Layer)
- Tầng truy cập mạng (Network access Layer)



Hình 6.1: Sự tương ứng giữa mô hình TCP với OSI

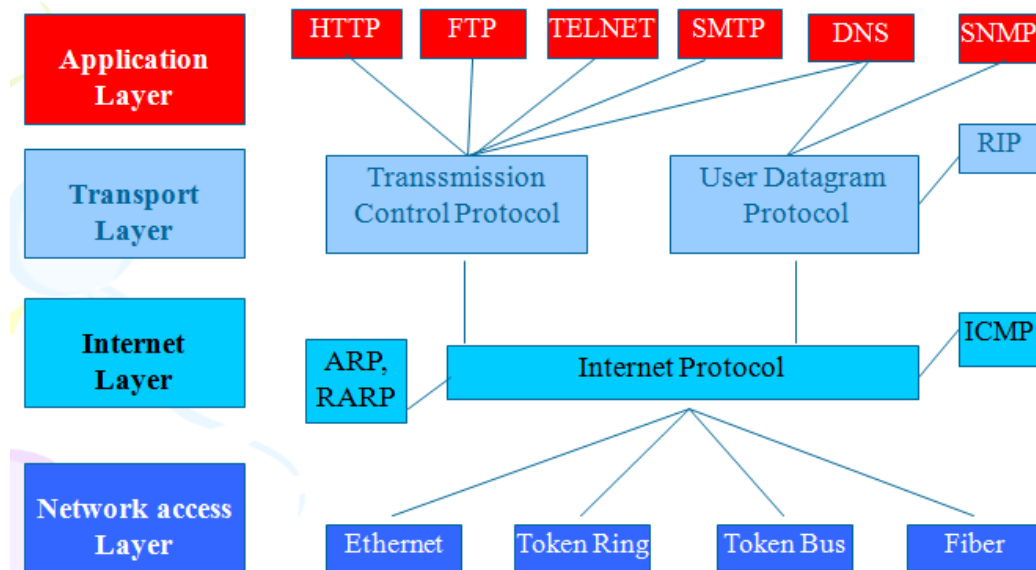
## ii. Chức năng của các tầng

- [1] **Application layer:** Chức năng tương ứng như ba tầng: Ứng dụng, trình diễn và phiên trong mô hình OSI. Hỗ trợ các ứng dụng cho các giao thức tầng Host-to-Host. Cung cấp giao diện cho người sử dụng mô hình TCP/IP. Thực hiện chuyển đổi cú pháp dữ liệu, mã hóa nén; Tạo và quản lý các phiên làm việc. Các giao thức ứng dụng gồm HTTP, TELNET, FTP, SMTP, POP3, ..
- [2] **Transport layer:** Chức năng tương ứng tầng vận chuyển trong mô hình OSI. Thực hiện những kết nối giữa hai máy chủ trên mạng bằng 2 giao thức cơ bản: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol). Thực hiện tạo socket, phân đoạn và hợp dữ liệu.
- [3] **Internet Layer:** Chức năng tương ứng tầng mạng trong mô hình OSI. Giao thức IP cùng với các giao thức định tuyến RIP, OSPF tầng mạng cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring, X.25... ánh xạ địa chỉ MAC-IP bằng giao thức ARP và RARP.
- [4] **Network Access Layer:** Chức năng tương ứng tầng liên kết dữ liệu và tầng vật lý trong mô hình OSI. Cung cấp các phương tiện kết nối vật lý cáp, bộ chuyển đổi, Card mạng, giao thức kết nối, giao thức truy nhập đường truyền CSMA/CD, Token Ring, Token Bus... Cung cấp các dịch vụ cho tầng Internet.

## Tiết 2:

### 2) Giao thức cơ bản:

- ✓ Tầng ứng dụng : HTTP, FTP, TELNET, SMTP, DNS,...
- ✓ Tầng vận chuyển: TCP, UDP..
- ✓ Tầng internet : IP, ICMP,
- ✓ Tầng truy cập mạng: Ethernet, Token Ring, Token Bus,...



Hình 6.2: Sơ đồ giao thức mô hình TCP/IP

i. Giới thiệu tổng quan các giao thức:

- ✓ **HTTP** (Hyper Text Transfer Protocol): Giao thức truyền siêu văn bản (text, image, video, controls..). Ví dụ ứng dụng web.
- ✓ **FTP** (File transfer Protocol): Giao thức truyền tệp và thư mục. Hoạt động theo mô hình Client – Server. Thực hiện quản lý tệp và thư mục trên máy chủ, tải và cập nhật tệp và thư mục cho máy chủ.
- ✓ **Telnet**: Chương trình cho phép người dùng login vào một máy chủ, thiết bị (router) từ một máy tính trên mạng. Giúp việc quản trị và cấu hình được dễ dàng.
- ✓ **SMTP** (Simple Mail Transfer Protocol): Giao thức gửi email.
- ✓ **POP3** – giao thức nhận email.
- ✓ **DNS** (Domain Name server): Giao thức quản lý và phân giải tên miền; chuyển đổi từ địa chỉ IP sang tên miền và ngược lại.
- ✓ **SNMP** (Simple Network Monitoring Protocol): Giao thức quản trị mạng cung cấp những công cụ quản trị mạng từ xa.
- ✓ **RIP** (Routing Internet Protocol): Giao thức định tuyến.
- ✓ **ICMP** (Internet Control Message Protocol): Giao thức điều khiển thông báo trong tầng mạng.
- ✓ **UDP** (User Datagram Protocol): Giao thức truyền không kết nối cung cấp dịch vụ truyền không tin cậy nhưng tiết kiệm chi phí truyền.
- ✓ **TCP** (Transmission Control Protocol): Giao thức hướng kết nối cung cấp dịch vụ truyền thông tin cậy.
- ✓ **IP** (Internet Protocol): chuyển giao các gói tin qua các máy tính đến đích.
- ✓ **ARP** (Address Resolution Protocol): Cơ chế chuyển địa chỉ IP thành địa chỉ vật lý của các thiết bị mạng.
- ✓ **RARP**: Ngược lại với ARP; nó ánh xạ địa chỉ vật lý sang địa chỉ IP.

ii. Giao thức IP:

*IP là giao thức không liên kết, chức năng chủ yếu là cung cấp các dịch vụ Datagram và các khả năng kết nối liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram, thực hiện tiến trình định địa chỉ và chọn đường.*

*Cấu trúc gói dữ liệu IP: gọi là các Datagram, mỗi Datagram có phần Header chứa các thông tin điều khiển.*

➤ **Cấu trúc của gói tin IP:**

|                        |          |              |                  |                 |
|------------------------|----------|--------------|------------------|-----------------|
| VERS                   | HLEN     | SERVICE TYPE | TOTAL LENGTH     |                 |
| IDENTIFICATION         |          |              | FLAG             | FRAGMENT OFFSET |
| TIME TO LIVE           | PROTOCOL |              | HEADER CHECK SUM |                 |
| SOURCE IP ADDRESS      |          |              |                  |                 |
| DESTINATION IP ADDRESS |          |              |                  |                 |
| IP OPTION (IF ANY)     |          |              |                  | PADDING         |
| DATA                   |          |              |                  |                 |
| * * *                  |          |              |                  |                 |
| DATA                   |          |              |                  |                 |

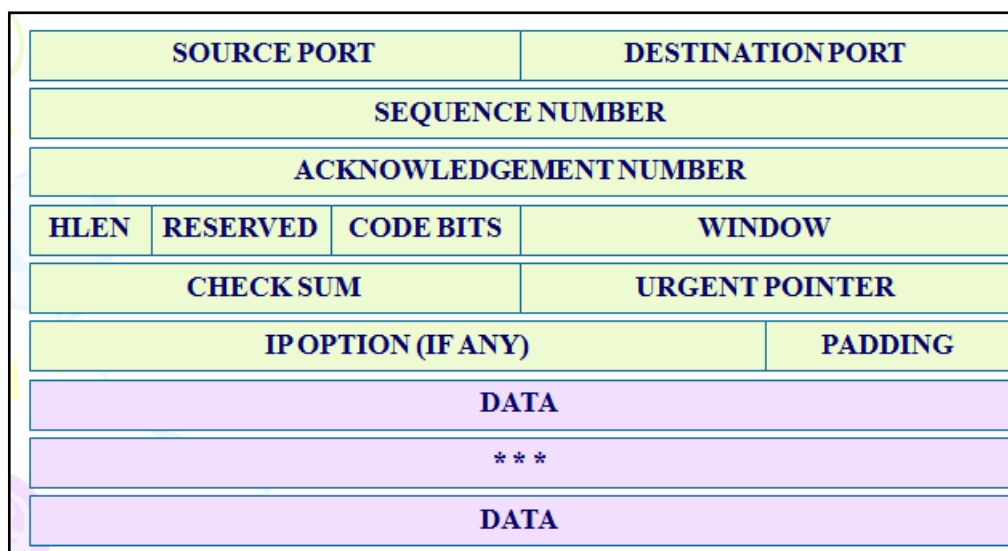
*Hình 6.3: Cấu trúc của gói tin IP*

- ✓ VER (4 bits): Version hiện hành của IP được cài đặt.
- ✓ IHL (4 bits): độ dài phần header, tính theo đơn vị word.
- ✓ Type of service(8 bits): Thông tin về loại dịch vụ
- ✓ Total Length (16 bits): Chỉ độ dài Datagram.
- ✓ Identification (16bits): Định danh cho một Datagram .
- ✓ Flags(3 bits): Liên quan đến sự phân đoạn các Datagram
- ✓ Fragment Offset (13 bits): Chỉ vị trí của Fragment trong Datagram.
- ✓ Time To Live (TTL-8 bits): Thời gian sống
- ✓ Protocol (8 bits): Chỉ giao thức tầng trên: TCP hay UDP.
- ✓ Header Checksum (16 bits): Mã kiểm soát lỗi CRC
- ✓ Source Address (32 bits): địa chỉ của trạm nguồn.
- ✓ Destination Address (32 bits): Địa chỉ của trạm đích.
- ✓ Option (có độ dài thay đổi): Sử dụng trong trường hợp bảo mật, định tuyến đặc biệt.
- ✓ Padding (độ dài thay đổi): Vùng đệm cho phần Header luôn kết thúc ở 32 bits
- ✓ Data (độ dài thay đổi): Độ dài dữ liệu tối đa là 65.535 bytes, tối thiểu là 8 bytes.

**Tiết 3:**

**iii. Giao thức TCP**

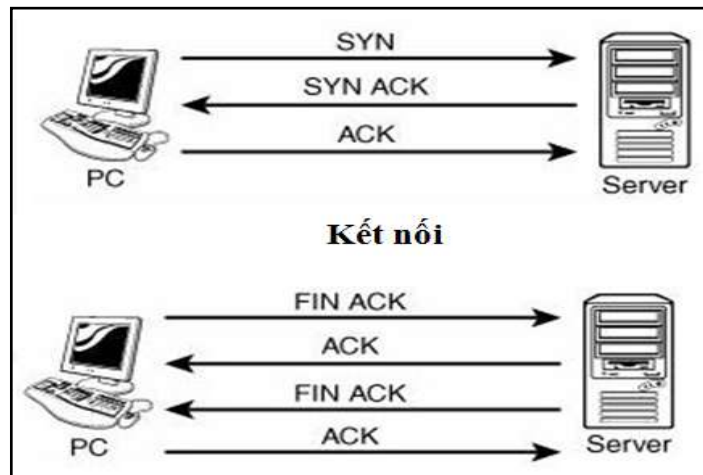
- Chức năng:
  - ✓ Thiết lập, duy trì, giải phóng liên kết giữa hai thực thể TCP. Phân phát gói tin một cách tin cậy.
  - ✓ Tạo số thứ tự các gói dữ liệu, điều khiển lỗi.
  - ✓ Cung cấp khả năng đa kết nối thông qua số hiệu cổng.
  - ✓ Truyền dữ liệu theo chế độ song công
  - ✓ TCP sắp xếp lại các Datagram IP khi đến đích.
  - ✓ Phát lại có chọn lọc.
- Cấu trúc gói tin TCP



*Hình 6.4 Cấu trúc của gói tin TCP*

- ✓ Source Port (16 bit), Destination Port (16 bit)
- ✓ Sequence Number: 32 bits, số thứ tự khi phát.
- ✓ Acknowledgment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.
- ✓ HLEN (4 bits)
- ✓ Reserved (6 bit): 0, dành cho tương lai.
- ✓ Control bits: Các bits điều khiển
  - URG : Vùng con trỏ khẩn có hiệu lực.
  - ACK : Vùng báo nhận (ACK number) có hiệu lực .
  - PSH: Chức năng PUSH.
  - RST: Khởi động lại liên kết.
  - SYN : Đồng bộ các số liệu tuần tự (sequence number).
  - FIN : Không còn dữ liệu từ trạm nguồn .

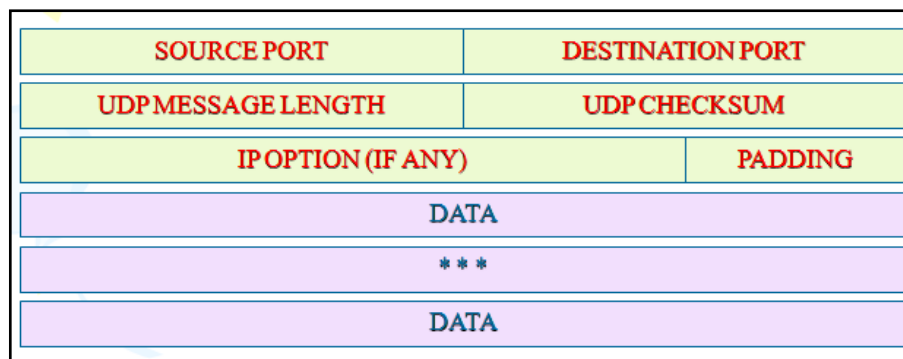
- ✓ Window (16bits): Số lượng các Byte dữ liệu trong vùng cửa sổ bên phát.
- ✓ Checksum (16bits): theo phương pháp CRC
- ✓ Urgent Pointer (16 bits): Số thứ tự của Byte dữ liệu khẩn, khi URG được thiết lập .
- ✓ Option (thay đổi): Khai báo độ dài tối đa của TCP Data trong một Segment.
- ✓ Padding (thay đổi): Phần chèn thêm vào Header.
- Quá trình kết nối và hủy kết nối



Hình 6.5: Quá trình kết nối và hủy kết nối

#### iv. Giao thức UDP

- Đặc điểm và chức năng
  - ✓ UDP là giao thức không liên kết, sử dụng cho các tiến trình không yêu cầu về độ tin cậy cao, không có cơ chế xác nhận ACK, không đảm bảo chuyển giao các gói đến đích và theo đúng thứ tự và không thực hiện loại bỏ các gói tin trùng lặp.
  - ✓ Nó cho phép ứng dụng trao đổi thông tin qua mạng với ít thông tin điều khiển nhất.
  - ✓ Nó cung cấp cơ chế gán và quản lý các số hiệu cổng để định danh duy nhất cho các ứng dụng chạy trên một Client của mạng.
- Cấu trúc gói tin:



Hình 6.6: Cấu trúc gói tin UDP

- Vì sao lựa chọn UDP
  - ✓ Nếu một số lượng lớn các gói tin nhỏ được truyền, thông tin cho việc kết nối và sửa lỗi có thể lớn hơn nhiều so với thông tin cần truyền. Trong trường hợp này, UDP là giải pháp hiệu quả nhất.
  - ✓ Những ứng dụng kiểu "Query-Response" cũng rất phù hợp với UDP, câu trả lời có thể dùng làm sự xác nhận của một câu hỏi. Một số ứng dụng đã tự nó cung cấp công nghệ riêng để chuyển giao thông tin tin cậy.

#### **Tiết 4:**

##### **v. Giao thức ICMP**

*ICMP là giao thức điều khiển của tầng IP, sử dụng để trao đổi các thông tin điều khiển dòng dữ liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP.*

- Chức năng:
  - ✓ Điều khiển lưu lượng
  - ✓ Thông báo lỗi
  - ✓ Định hướng lại các tuyến
  - ✓ Kiểm tra các trạm ở xa

Có hai loại: thông điệp truy vấn và thông điệp thông báo lỗi.

| Nhóm                     | Loại bản tin  |
|--------------------------|---|
| Thông điệp truy vấn      | Hỏi và phúc đáp Echo (Echo Request và Echo Reply)                               |
|                          | Hỏi và phúc đáp nhãn thời gian (Timestamp Request và Timestamp Reply)           |
|                          | Yêu cầu và phúc đáp mặt nạ địa chỉ (Address mask Request và Address mask Reply) |
|                          | Yêu cầu và quảng bá bộ định tuyến (Router solicitation và Router advertisement) |
| Thông điệp thông báo lỗi | Không thể đạt tới đích (Destination Unreachable)                                |
|                          | Yêu cầu ngừng hoặc giảm tốc độ phát (Source Quench)                             |
|                          | Định hướng lại (Redirection)  |
|                          | Vượt ngưỡng thời gian (Time Exceeded)   |

*Hình 6.7 : Thông điệp của ICMP*

##### **vi. Giao thức phân giải địa chỉ ARP**

- ✓ Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích khi biết địa chỉ IP.
- ✓ Mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC (ARP Cache) nó chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ tương ứng mới.
- ✓ Trước khi trao đổi dữ liệu, node nguồn phải xác định địa chỉ MAC của node đích bằng cách tìm kiếm trong bảng địa chỉ IP. Nếu không tìm thấy, node

nguồn gửi quảng bá một gói yêu cầu ARP (ARP Request) chứa địa chỉ IP đích.

➤ Tiến trình của ARP được mô tả như sau:

- [1] Trạm yêu cầu: có IP, yêu cầu địa chỉ MAC.
- [2] Trạm yêu cầu: tìm kiếm trong bảng ARP.
- [3] Nếu tìm thấy sẽ trả lại địa chỉ MAC.
- [4] Nếu không tìm thấy, tạo ARP Request phát quảng bá tới các trạm khác.
- [5] Tuỳ theo gói tin trả lời, ARP cập nhật vào bảng ARP.

**vii. Giao thức phân giải địa chỉ RARP**

RARP là giao thức phân giải địa chỉ ngược, cho trước địa chỉ MAC, tìm địa chỉ IP tương ứng. Khác ARP là gói tin trả lời chỉ Server được trả lời RARP Reply.

**viii. Giao thức Telnet**

- ✓ Telnet cho phép người sử dụng từ trạm làm việc của mình có thể đăng nhập (login) vào một trạm xa như là một đầu cuối (terminal) nối trực tiếp với trạm xa đó.
- ✓ Đặc tả về Telnet có thể tìm thấy trong RFC 854..861, 884, 885, 1091, 1097 và 1116

**ix. Simple Network Monitoring Protocol - SNMP**

- ✓ Giao thức quản trị mạng cung cấp phương thức liên lạc giữa manager, các đối tượng được quản trị và các agent
- ✓ Giao thức quản trị mạng cài đặt trong bộ giao thức TCP/IP sử dụng giao thức không kết nối UDP
- ✓ Đặc tả SNMP có thể tìm thấy trong RFC 1155..1158

**x. Giao thức FTP**

- ✓ *Giao thức truyền tệp và thư mục. Hoạt động theo mô hình Client – Server. Thực hiện quản lý tệp và thư mục trên máy chủ, tải và cập nhật tệp và thư mục cho máy chủ.*
- ✓ Chương trình sử dụng giao thức này dùng cổng 21 và thiết lập hai kênh truyền logic.
  - Kênh truyền lệnh tồn tại suốt phiên làm việc
  - Kênh truyền dữ liệu được thiết lập mỗi khi có dữ liệu truyền và giải phóng sau khi sử dụng
- ✓ Giao thức này được đặc tả trong RFC 959

**Tiết 5:**

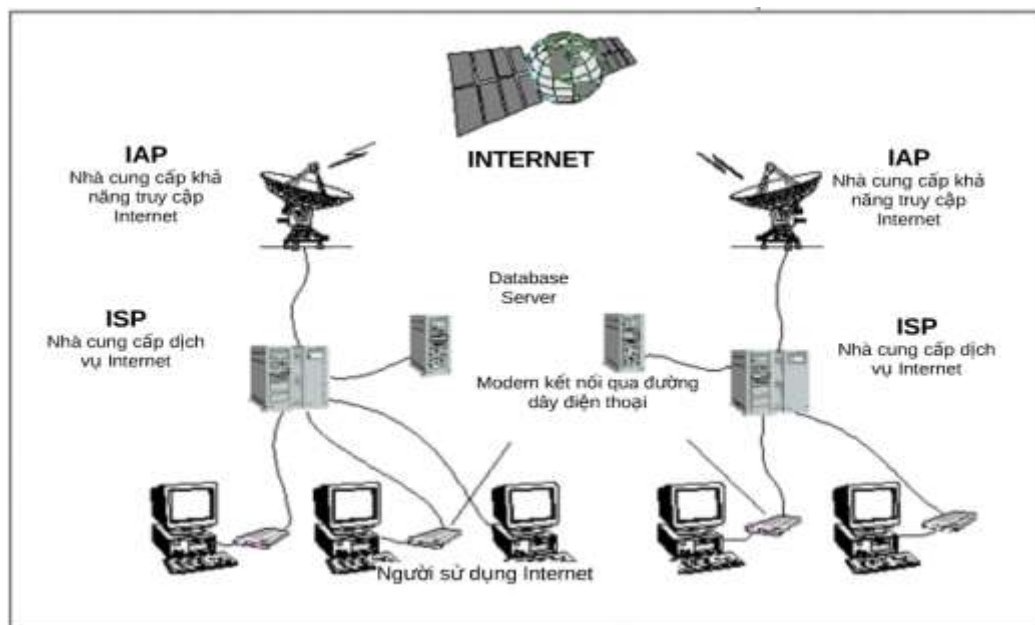
**3) Mạng Internet**

**i. Giới thiệu chung về mạng Internet**

- ✓ **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 triệu 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
- ✓ Tiền thân của mạng Internet ngày nay là mạng ARPANET. Cơ quan quản lý dự án nghiên cứu phát triển ARPA thuộc bộ quốc phòng Mỹ liên kết 4 địa điểm đầu tiên vào tháng 7 năm 1969 bao gồm: Viện nghiên cứu Stanford, Đại học California, Los Angeles, Đại học Utah và Đại học California, Santa Barbara. Đó chính là mạng liên khu vực (Wide Area Network - WAN) đầu tiên được xây dựng.
- ✓ Thuật ngữ "Internet" xuất hiện lần đầu vào khoảng năm 1974. Lúc đó mạng vẫn được gọi là ARPANET. Năm 1983, giao thức TCP/IP chính thức được coi như một chuẩn đối với ngành quân sự Mỹ và tất cả các máy tính nối với ARPANET phải sử dụng chuẩn mới này. Năm 1984, ARPANET được chia ra thành hai phần: phần thứ nhất vẫn được gọi là ARPANET, dành cho việc nghiên cứu và phát triển; phần thứ hai được gọi là MILNET, là mạng dùng cho các mục đích quân sự.

## ii. Cấu trúc mạng và kết nối Internet

Internet là một mạng GAN dựa trên kết nối liên mạng WAN, sử dụng mô hình TCP/IP. Việc kết nối và truy cập Internet của người dùng được cung cấp bởi các nhà cung cấp dịch vụ Internet ISP (Internet Service Provider). Các ISP phải thuê đường và cổng của một IAP.



Hình 6.8 : Sơ đồ tổng quan mạng internet

### 4) Một số dịch vụ cơ bản trên mạng Internet :

#### i. Dịch vụ phân giải tên miền DNS

##### ➤ Giới thiệu :



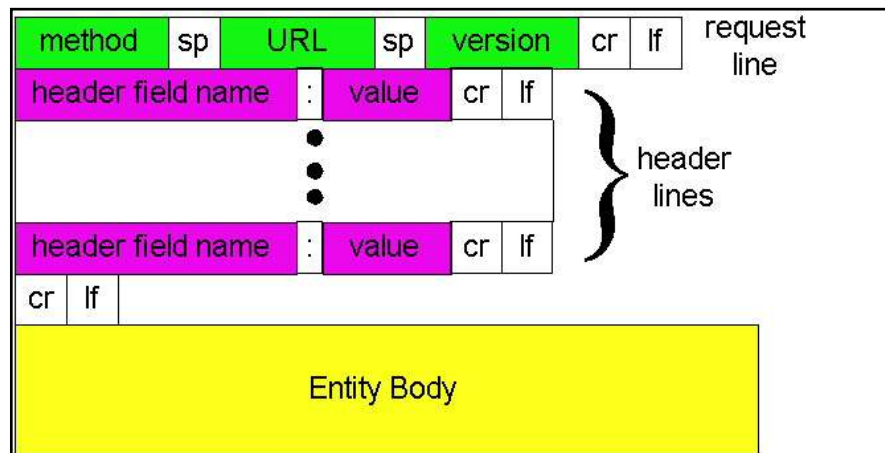
- ✓ Máy tính muốn bắt tay với nhau cần phải biết địa chỉ **IP** của nhau, tuy nhiên việc nhớ địa chỉ **IP** là rất khó.
- ✓ Ngoài địa chỉ **IP** ra còn có hostname, tên máy thường dễ nhớ vì có tính trực quan và gọi nhớ hơn địa chỉ **IP**. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính và ngược lại.
- ✓ Bắt đầu từ mạng ARPANET: Một tập tin đơn HOSTS.TXT (trên 1 máy chủ) và tên máy chỉ là 1 chuỗi văn bản không phân cấp. Tuy nhiên HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng.
- Cơ chế hoạt động của dịch vụ DNS
  - ✓ Hoạt động theo mô hình Client-Server:
  - ✓ Phần Server gọi là máy chủ phục vụ tên Name Server, chứa các thông tin CSDL của DNS.
  - ✓ Phần Client là trình phân giải tên Resolver, nó chỉ là các hàm thư viện dùng để tạo các query và gửi chúng đến Name Server.
  - ✓ DNS được thi hành như một giao thức tầng Application trong mạng TCP/IP.
- DNS là một CSDL phân tán:
  - ✓ Người quản trị cục bộ quản lý phần dữ liệu nội bộ của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình Client - Server.
  - ✓ Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (replication) và lưu tạm (caching). Một hostname trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.).
- **Phân giải tên thành địa chỉ IP**
  - ✓ **Root name server** : quản lý các **Server** ở mức **top-level domain**. Khi có truy vấn về một tên miền nào đó thì **Root Name Server** phải cung cấp **tên** và địa chỉ **IP** của **Server** quản lý **top-level domain**.
  - ✓ Các **Server** của **top-level domain** cung cấp danh sách các **tên** và **IP** của **Server** quản lý **second-level domain** mà tên miền này thuộc vào.
  - ✓ Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.
- **Phân giải IP thành tên máy tính**
  - ✓ Để có thể phân giải tên máy tính của một địa chỉ IP, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ IP, có tên miền là in-addr.arpa.
  - ✓ Mỗi nút trong miền in-addr.arpa có một tên nhãn là chỉ số thập phân của địa chỉ IP.

## **Tiết 6:**

### **ii. Dịch vụ WEB**

- ✓ Dịch vụ WEB (WWW - World Wide Web) dựa trên giao thức HTTP, được xây dựng và hoạt động theo mô hình Client/Server. Các client dùng một phần mềm gọi là Web Browser. Web Browser tiếp nhận thông tin yêu cầu từ người dùng sau đó gửi các yêu cầu tới máy Server xử lý.
- ✓ Web Server cũng là một phần mềm chạy trên các máy phục vụ (IIS, Apache), nhận Request thực hiện theo yêu cầu rồi trả thông tin (Response) cho người sử dụng.
- ✓ Mô hình và ví dụ hoạt động của HTTP.

- ✓ Dạng tổng quát của HTTP request:



Hình 6.9: Header của HTTP request

- ✓ Khuôn dạng của HTTP response:

```
HTTP/1.0 200 OK
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 1998 .....
Content-Length: 6821
Content-Type: text/html

data data data data data ...
```

Hình 6.10 Khuôn dạng của HTTP response

- ✓ Quá trình xác thực
- ✓ Tạo lưu trữ tạm thời caching

### iii. Dịch vụ thư điện tử :

- ✓ Có 3 thành phần chủ yếu:

- Tác nhân sử dụng (user agent)
- Mail servers
- Giao thức truyền và nhận thư : SMTP, POP3

#### [1] User Agent

- Soạn, sửa, đọc, xóa .. Email. Ví dụ: Eudora, Outlook, elm, Netscape Messenger.
- Mail gửi đi (outgoing), và nhận về (incoming) được lưu trữ trên server

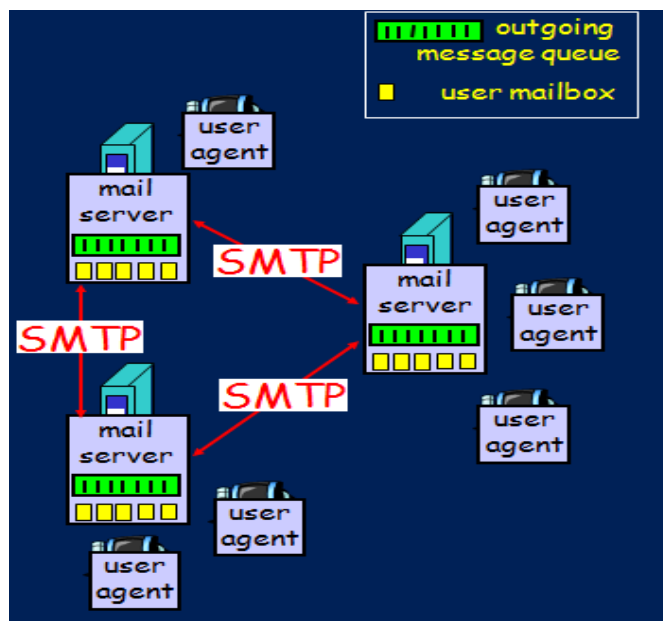
#### [2] Mail Servers

- Mailbox chứa các thư đến của người sử dụng.
- Message queue quản lý các thư người sử dụng gửi đi.

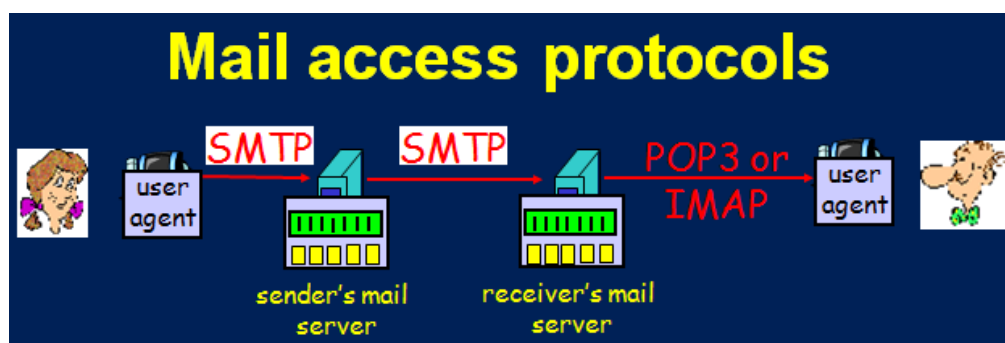
#### [3] Giao thức truyền và nhận thư:

SMTP: Phân phát/lưu trữ đến Server nhận.

- **SMTP** (Simple Mail Transfer Protocol): Giao thức gửi email.
- **POP3, IMAP** – giao thức nhận email.



Hình 6.11: Hệ thống Email



Hình 6.12: Giao thức nhận và gửi Email.

p) Nội dung thảo luận:

**Tiết 7-9:**

- i. Ứng dụng thương mại điện tử
- ii. Ứng dụng truyền file FTP và phân giải tên miền DNS
- iii. Ứng dụng thư điện tử

q) Nội dung tự học

- i. Mô hình TCP/IP
- ii. Cấu trúc và hoạt động của các giao thức cơ bản trong mô hình.
- iii. Các dịch vụ internet.

r) Bài tập (bắt buộc)

s) Thực hành:

**Tiết 9 -12:**

- i. Mô phỏng hoạt động và tìm hiểu cấu trúc của các giao thức trong mô hình TCP/IP sử dụng Packet Tracer
- ii. Bắt và phân tích gói tin sử dụng WireShark

5. Tài liệu tham khảo (sách, báo – chỉ tiết đến chương, mục, trang)

- i. Bài giảng của giáo viên, Slide chương 6.

**ii.** TL [1] , chương 7; trang 444

**iii.** TL [2], chương 5, chương 9.

6. Câu hỏi ôn tập:

**i.** Trình bày mô hình TCP/IP, so sánh với mô hình OSI

**ii.** Cấu trúc và hoạt động của các giao thức cơ bản trong mô hình TCP/IP.

**iii.** Trình bày và phân tích ứng dụng của các dịch vụ internet.

**HỌC PHẦN: Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương VI: Mô hình TCP/IP và mạng Internet**

2. Thời lượng:

- GV giảng: 6 tiết.
- Thảo luận: 3 tiết,
- Thực hành: 3 tiết.
- Bài tập: 0 tiết.
- Tự học: 12 tiết

3. Mục đích, yêu cầu:

Mục đích: Sinh viên nắm được mô hình mạng thực tế TCP/IP là một tham chiếu của mô hình OSI. Nắm được hoạt động, chức năng của các tầng và các giao thức cụ thể trong tầng đó. Trình bày rõ cấu trúc, hoạt động và các ứng dụng của mạng Internet.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://http://fit.mta.edu.vn/~thiennd/>).
- Chuẩn bị bài thảo luận.
- Chuẩn bị và tham gia thực hành tại phòng thí nghiệm

4. Nội dung:

t) Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

➤ Giới thiệu nội dung chương

4. Mô hình TCP/IP

4.1. Mô hình kiến trúc TCP/IP

4.2. Vai trò và chức năng các tầng

5. Các giao thức cơ bản của mô hình TCP/IP

6. Mạng Internet

6.1. Giới thiệu chung về mạng Internet

6.2. Cấu trúc mạng Internet

6.3. Công nghệ kết nối mạng Internet

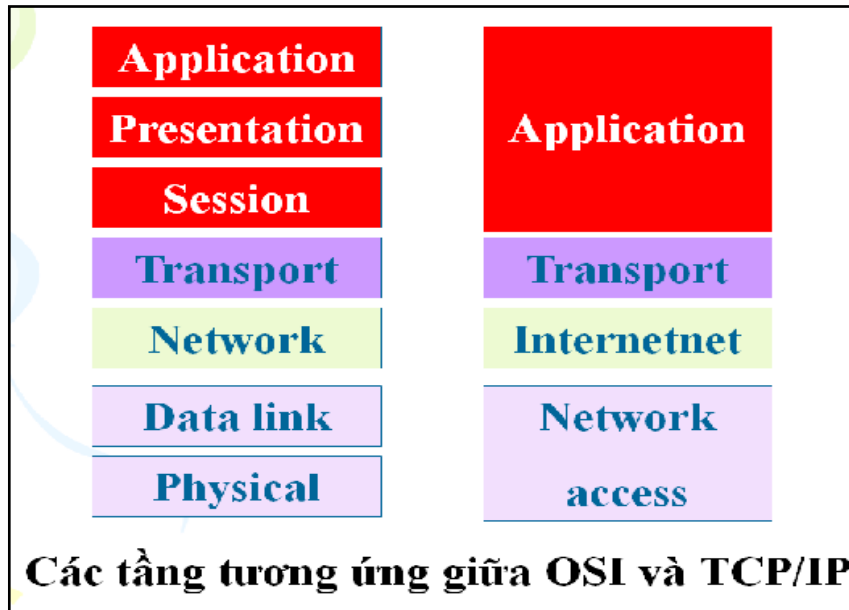
6.4. Một số dịch vụ cơ bản trên mạng Internet

1) Mô hình TCP/IP

iii. Giới thiệu:

- ✓ Cuối năm 1960 và đầu 1970, Trung tâm nghiên cứu cấp cao (Advanced Research Projects Agency - ARPA) bộ quốc phòng Mỹ (DoD) được giao trách nhiệm phát triển mạng ARPANET.
- ✓ Đầu năm 1980, bộ giao thức TCP/IP ra đời làm giao thức chuẩn cho mạng ARPANET và các mạng của DoD.
- ✓ Mô hình TCP/IP có 4 tầng
  - Tầng ứng dụng (Application Layer)
  - Tầng giao vận (Transport Layer)

- Tầng Internet (Internet Layer)
- Tầng truy cập mạng (Network access Layer)



Hình 6.1: Sự tương ứng giữa mô hình TCP với OSI

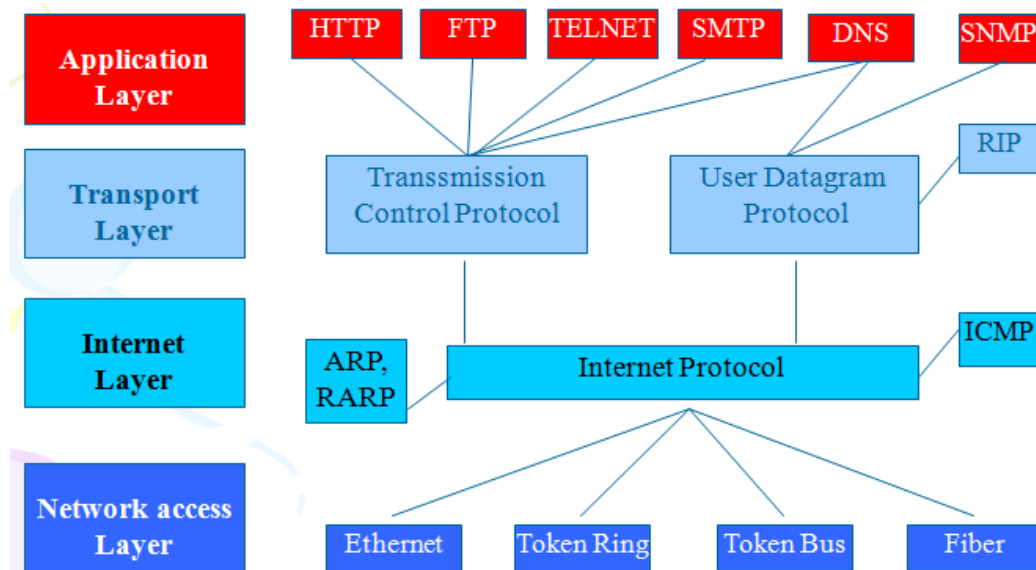
#### iv. Chức năng của các tầng

- [5] **Application layer:** Chức năng tương ứng như ba tầng: Ứng dụng, trình diễn và phiên trong mô hình OSI. Hỗ trợ các ứng dụng cho các giao thức tầng Host-to-Host. Cung cấp giao diện cho người sử dụng mô hình TCP/IP. Thực hiện chuyển đổi cú pháp dữ liệu, mã hóa nén; Tạo và quản lý các phiên làm việc. Các giao thức ứng dụng gồm HTTP, TELNET, FTP, SMTP, POP3, ..
- [6] **Transport layer:** Chức năng tương ứng tầng vận chuyển trong mô hình OSI. Thực hiện những kết nối giữa hai máy chủ trên mạng bằng 2 giao thức cơ bản: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol). Thực hiện tạo socket, phân đoạn và hợp dữ liệu.
- [7] **Internet Layer:** Chức năng tương ứng tầng mạng trong mô hình OSI. Giao thức IP cùng với các giao thức định tuyến RIP, OSPF tầng mạng cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring, X.25... ánh xạ địa chỉ MAC-IP bằng giao thức ARP và RARP.
- [8] **Network Access Layer:** Chức năng tương ứng tầng liên kết dữ liệu và tầng vật lý trong mô hình OSI. Cung cấp các phương tiện kết nối vật lý cáp, bộ chuyển đổi, Card mạng, giao thức kết nối, giao thức truy nhập đường truyền CSMA/CD, Token Ring, Token Bus... Cung cấp các dịch vụ cho tầng Internet.

#### Tiết 2:

##### 2) Giao thức cơ bản:

- ✓ Tầng ứng dụng : HTTP, FTP, TELNET, SMTP, DNS, ..
- ✓ Tầng vận chuyển: TCP, UDP..
- ✓ Tầng internet : IP, ICMP,
- ✓ Tầng truy cập mạng: Ethernet, Token Ring, Token Bus, ..



Hình 6.2: Sơ đồ giao thức mô hình TCP/IP

**xi. Giới thiệu tổng quan các giao thức:**

- ✓ **HTTP** (Hyper Text Transfer Protocol): Giao thức truyền siêu văn bản (text, image, video, controls..). Ví dụ ứng dụng web.
- ✓ **FTP** (File transfer Protocol): Giao thức truyền tệp và thư mục. Hoạt động theo mô hình Client – Server. Thực hiện quản lý tệp và thư mục trên máy chủ, tải và cập nhật tệp và thư mục cho máy chủ.
- ✓ **Telnet**: Chương trình cho phép người dùng login vào một máy chủ, thiết bị (router) từ một máy tính trên mạng. Giúp việc quản trị và cấu hình được dễ dàng.
- ✓ **SMTP** (Simple Mail Transfer Protocol): Giao thức gửi email.
- ✓ **POP3** – giao thức nhận email.
- ✓ **DNS** (Domain Name server): Giao thức quản lý và phân giải tên miền; chuyển đổi từ địa chỉ IP sang tên miền và ngược lại.
- ✓ **SNMP** (Simple Network Monitoring Protocol): Giao thức quản trị mạng cung cấp những công cụ quản trị mạng từ xa.
- ✓ **RIP** (Routing Internet Protocol): Giao thức định tuyến.
- ✓ **ICMP** (Internet Control Message Protocol): Giao thức điều khiển thông báo trong tầng mạng.
- ✓ **UDP** (User Datagram Protocol): Giao thức truyền không kết nối cung cấp dịch vụ truyền không tin cậy nhưng tiết kiệm chi phí truyền.
- ✓ **TCP** (Transmission Control Protocol): Giao thức hướng kết nối cung cấp dịch vụ truyền thông tin cậy.
- ✓ **IP** (Internet Protocol): chuyển giao các gói tin qua các máy tính đến đích.
- ✓ **ARP** (Address Resolution Protocol): Cơ chế chuyển địa chỉ IP thành địa chỉ vật lý của các thiết bị mạng.
- ✓ **RARP**: Ngược lại với ARP; nó ánh xạ địa chỉ vật lý sang địa chỉ IP.

**xii. Giao thức IP:**

*IP là giao thức không liên kết, chức năng chủ yếu là cung cấp các dịch vụ Datagram và các khả năng kết nối liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram, thực hiện tiến trình định địa chỉ và chọn đường.*

*Cấu trúc gói dữ liệu IP: gọi là các Datagram, mỗi Datagram có phần Header chứa các thông tin điều khiển.*

➤ **Cấu trúc của gói tin IP:**

|                        |          |              |                  |                 |
|------------------------|----------|--------------|------------------|-----------------|
| VERS                   | HLEN     | SERVICE TYPE | TOTAL LENGTH     |                 |
| IDENTIFICATION         |          |              | FLAG             | FRAGMENT OFFSET |
| TIME TO LIVE           | PROTOCOL |              | HEADER CHECK SUM |                 |
| SOURCE IP ADDRESS      |          |              |                  |                 |
| DESTINATION IP ADDRESS |          |              |                  |                 |
| IP OPTION (IF ANY)     |          |              |                  | PADDING         |
| DATA                   |          |              |                  |                 |
| * * *                  |          |              |                  |                 |
| DATA                   |          |              |                  |                 |

*Hình 6.3: Cấu trúc của gói tin IP*

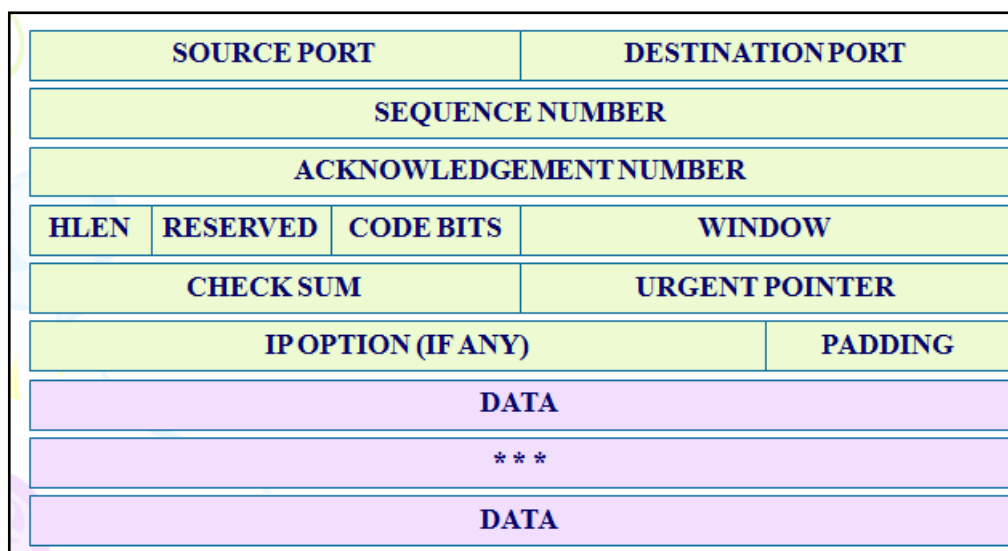
- ✓ VER (4 bits): Version hiện hành của IP được cài đặt.
- ✓ IHL (4 bits): độ dài phần header, tính theo đơn vị word.
- ✓ Type of service(8 bits): Thông tin về loại dịch vụ
- ✓ Total Length (16 bits): Chỉ độ dài Datagram.
- ✓ Identification (16bits): Định danh cho một Datagram .
- ✓ Flags(3 bits): Liên quan đến sự phân đoạn các Datagram
- ✓ Fragment Offset (13 bits): Chỉ vị trí của Fragment trong Datagram.
- ✓ Time To Live (TTL-8 bits): Thời gian sống
- ✓ Protocol (8 bits): Chỉ giao thức tầng trên: TCP hay UDP.
- ✓ Header Checksum (16 bits): Mã kiểm soát lỗi CRC
- ✓ Source Address (32 bits): địa chỉ của trạm nguồn.
- ✓ Destination Address (32 bits): Địa chỉ của trạm đích.
- ✓ Option (có độ dài thay đổi): Sử dụng trong trường hợp bảo mật, định tuyến đặc biệt.
- ✓ Padding (độ dài thay đổi): Vùng đệm cho phần Header luôn kết thúc ở 32 bits
- ✓ Data (độ dài thay đổi): Độ dài dữ liệu tối đa là 65.535 bytes, tối thiểu là 8 bytes.

**Tiết 3:**

**xiii.            Giao thức TCP**



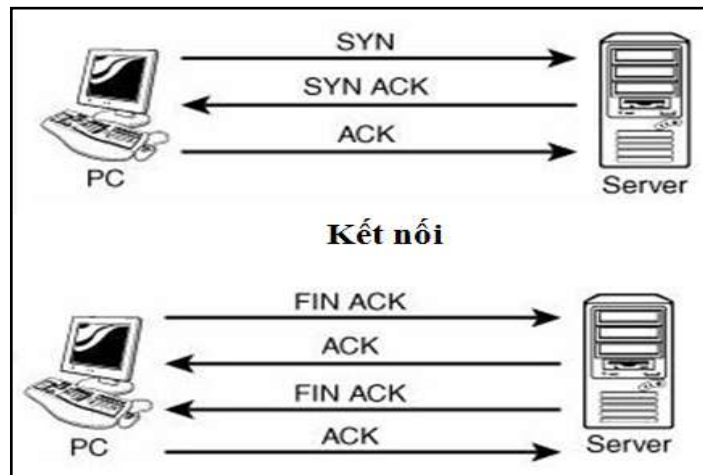
- Chức năng:
  - ✓ Thiết lập, duy trì, giải phóng liên kết giữa hai thực thể TCP. Phân phát gói tin một cách tin cậy.
  - ✓ Tạo số thứ tự các gói dữ liệu, điều khiển lỗi.
  - ✓ Cung cấp khả năng đa kết nối thông qua số hiệu cổng.
  - ✓ Truyền dữ liệu theo chế độ song công
  - ✓ TCP sắp xếp lại các Datagram IP khi đến đích.
  - ✓ Phát lại có chọn lọc.
- Cấu trúc gói tin TCP



*Hình 6.4 Cấu trúc của gói tin TCP*

- ✓ Source Port (16 bit), Destination Port (16 bit)
- ✓ Sequence Number: 32 bits, số thứ tự khi phát.
- ✓ Acknowledgment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.
- ✓ HLEN (4 bits)
- ✓ Reserved (6 bit): 0, dành cho tương lai.
- ✓ Control bits: Các bits điều khiển
  - URG : Vùng con trỏ khẩn có hiệu lực.
  - ACK : Vùng báo nhận (ACK number) có hiệu lực .
  - PSH: Chức năng PUSH.
  - RST: Khởi động lại liên kết.
  - SYN : Đồng bộ các số liệu tuần tự (sequence number).
  - FIN : Không còn dữ liệu từ trạm nguồn .

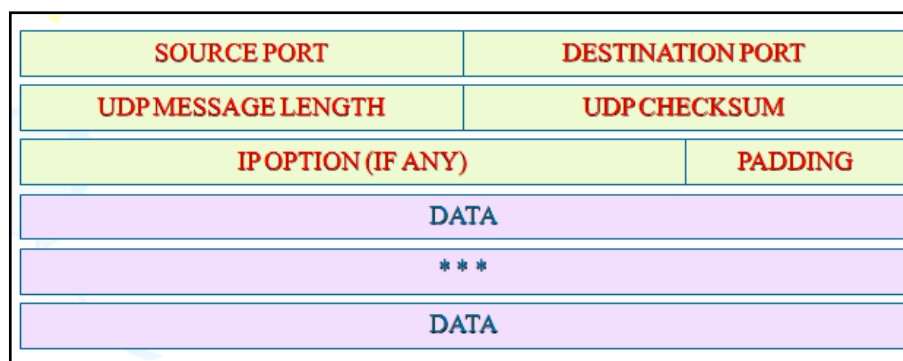
- ✓ Window (16bits): Số lượng các Byte dữ liệu trong vùng cửa sổ bên phát.
- ✓ Checksum (16bits): theo phương pháp CRC
- ✓ Urgent Pointer (16 bits): Số thứ tự của Byte dữ liệu khẩn, khi URG được thiết lập .
- ✓ Option (thay đổi): Khai báo độ dài tối đa của TCP Data trong một Segment.
- ✓ Padding (thay đổi): Phần chèn thêm vào Header.
- Quá trình kết nối và hủy kết nối



Hình 6.5: Quá trình kết nối và hủy kết nối

#### xiv. Giao thức UDP

- Đặc điểm và chức năng
  - ✓ UDP là giao thức không liên kết, sử dụng cho các tiến trình không yêu cầu về độ tin cậy cao, không có cơ chế xác nhận ACK, không đảm bảo chuyển giao các gói đến đích và theo đúng thứ tự và không thực hiện loại bỏ các gói tin trùng lặp.
  - ✓ Nó cho phép ứng dụng trao đổi thông tin qua mạng với ít thông tin điều khiển nhất.
  - ✓ Nó cung cấp cơ chế gán và quản lý các số hiệu cổng để định danh duy nhất cho các ứng dụng chạy trên một Client của mạng.
- Cấu trúc gói tin:



Hình 6.6: Cấu trúc gói tin UDP

- Vì sao lựa chọn UDP
  - ✓ Nếu một số lượng lớn các gói tin nhỏ được truyền, thông tin cho việc kết nối và sửa lỗi có thể lớn hơn nhiều so với thông tin cần truyền. Trong trường hợp này, UDP là giải pháp hiệu quả nhất.
  - ✓ Những ứng dụng kiểu "Query-Response" cũng rất phù hợp với UDP, câu trả lời có thể dùng làm sự xác nhận của một câu hỏi. Một số ứng dụng đã tự nó cung cấp công nghệ riêng để chuyển giao thông tin tin cậy.

#### **Tiết 4:**

##### **xv. Giao thức ICMP**

*ICMP là giao thức điều khiển của tầng IP, sử dụng để trao đổi các thông tin điều khiển dòng dữ liệu, thông báo lỗi và các thông tin trạng thái khác của bộ giao thức TCP/IP.*

- Chức năng:
  - ✓ Điều khiển lưu lượng
  - ✓ Thông báo lỗi
  - ✓ Định hướng lại các tuyến
  - ✓ Kiểm tra các trạm ở xa

Có hai loại: thông điệp truy vấn và thông điệp thông báo lỗi.

| Nhóm                     | Loại bản tin  |
|--------------------------|---|
| Thông điệp truy vấn      | Hỏi và phúc đáp Echo (Echo Request và Echo Reply)                               |
|                          | Hỏi và phúc đáp nhãn thời gian (Timestamp Request và Timestamp Reply)           |
|                          | Yêu cầu và phúc đáp mặt nạ địa chỉ (Address mask Request và Address mask Reply) |
|                          | Yêu cầu và quảng bá bộ định tuyến (Router solicitation và Router advertisement) |
| Thông điệp thông báo lỗi | Không thể đạt tới đích (Destination Unreachable)                                |
|                          | Yêu cầu ngừng hoặc giảm tốc độ phát (Source Quench)                             |
|                          | Định hướng lại (Redirection)  |
|                          | Vượt ngưỡng thời gian (Time Exceeded)   |

*Hình 6.7 : Thông điệp của ICMP*

##### **xvi. Giao thức phân giải địa chỉ ARP**

- ✓ Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích khi biết địa chỉ IP.
- ✓ Mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC (ARP Cache) nó chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ tương ứng mới.
- ✓ Trước khi trao đổi dữ liệu, node nguồn phải xác định địa chỉ MAC của node đích bằng cách tìm kiếm trong bảng địa chỉ IP. Nếu không tìm thấy, node

nguồn gửi quảng bá một gói yêu cầu ARP (ARP Request) chứa địa chỉ IP đích.

➤ Tiến trình của ARP được mô tả như sau:

[6] Trạm yêu cầu: có IP, yêu cầu địa chỉ MAC.

[7] Trạm yêu cầu: tìm kiếm trong bảng ARP.

[8] Nếu tìm thấy sẽ trả lại địa chỉ MAC.

[9] Nếu không tìm thấy, tạo ARP Request phát quảng bá tới các trạm khác.

[10] Tuỳ theo gói tin trả lời, ARP cập nhật vào bảng ARP.

**xvii.** Giao thức phân giải địa chỉ RARP

RARP là giao thức phân giải địa chỉ ngược, cho trước địa chỉ MAC, tìm địa chỉ IP tương ứng. Khác ARP là gói tin trả lời chỉ Server được trả lời RARP Reply.

**xviii.** Giao thức Telnet

- ✓ Telnet cho phép người sử dụng từ trạm làm việc của mình có thể đăng nhập (login) vào một trạm xa như là một đầu cuối (terminal) nối trực tiếp với trạm xa đó.
- ✓ Đặc tả về Telnet có thể tìm thấy trong RFC 854..861, 884, 885, 1091, 1097 và 1116

**xix.** Simple Network Monitoring Protocol - SNMP

- ✓ Giao thức quản trị mạng cung cấp phương thức liên lạc giữa manager, các đối tượng được quản trị và các agent
- ✓ Giao thức quản trị mạng cài đặt trong bộ giao thức TCP/IP sử dụng giao thức không kết nối UDP
- ✓ Đặc tả SNMP có thể tìm thấy trong RFC 1155..1158

**xx.** Giao thức FTP

- ✓ *Giao thức truyền tệp và thư mục. Hoạt động theo mô hình Client – Server. Thực hiện quản lý tệp và thư mục trên máy chủ, tải và cập nhật tệp và thư mục cho máy chủ.*
- ✓ Chương trình sử dụng giao thức này dùng cổng 21 và thiết lập hai kênh truyền logic.
  - Kênh truyền lệnh tồn tại suốt phiên làm việc
  - Kênh truyền dữ liệu được thiết lập mỗi khi có dữ liệu truyền và giải phóng sau khi sử dụng
- ✓ Giao thức này được đặc tả trong RFC 959

**Tiết 5:**

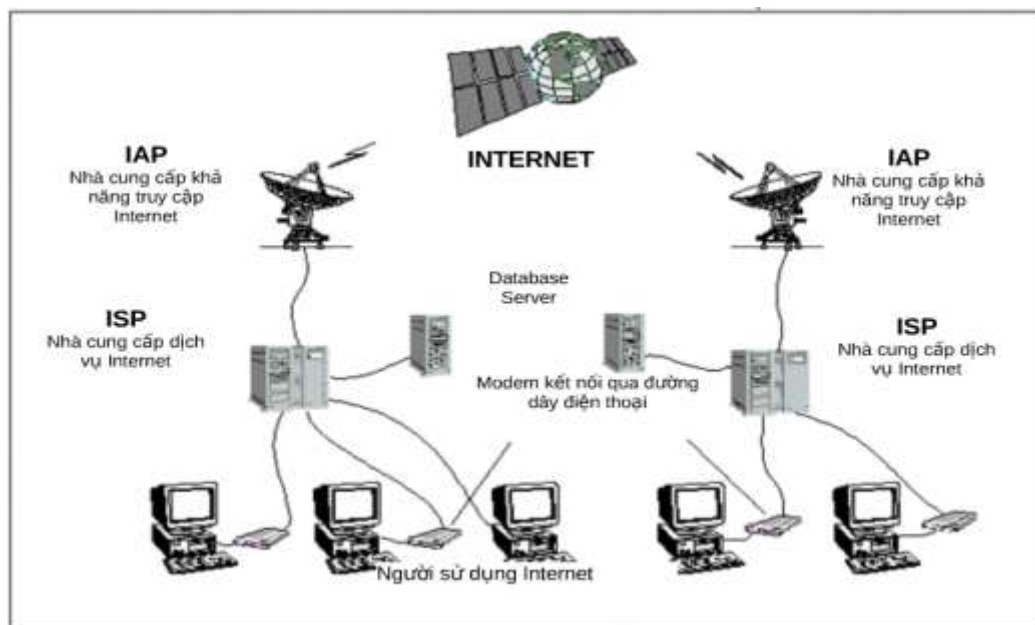
3) Mạng Internet

**iii.** Giới thiệu chung về mạng Internet

- ✓ **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 triệu 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
- ✓ Tiền thân của mạng Internet ngày nay là mạng ARPANET. Cơ quan quản lý dự án nghiên cứu phát triển ARPA thuộc bộ quốc phòng Mỹ liên kết 4 địa điểm đầu tiên vào tháng 7 năm 1969 bao gồm: Viện nghiên cứu Stanford, Đại học California, Los Angeles, Đại học Utah và Đại học California, Santa Barbara. Đó chính là mạng liên khu vực (Wide Area Network - WAN) đầu tiên được xây dựng.
- ✓ Thuật ngữ "Internet" xuất hiện lần đầu vào khoảng năm 1974. Lúc đó mạng vẫn được gọi là ARPANET. Năm 1983, giao thức TCP/IP chính thức được coi như một chuẩn đối với ngành quân sự Mỹ và tất cả các máy tính nối với ARPANET phải sử dụng chuẩn mới này. Năm 1984, ARPANET được chia ra thành hai phần: phần thứ nhất vẫn được gọi là ARPANET, dành cho việc nghiên cứu và phát triển; phần thứ hai được gọi là MILNET, là mạng dùng cho các mục đích quân sự.

#### iv. Cấu trúc mạng và kết nối Internet

Internet là một mạng GAN dựa trên kết nối liên mạng WAN, sử dụng mô hình TCP/IP. Việc kết nối và truy cập Internet của người dùng được cung cấp bởi các nhà cung cấp dịch vụ Internet ISP (Internet Service Provider). Các ISP phải thuê đường và công của một IAP.



Hình 6.8 : Sơ đồ tổng quan mạng internet

#### 4) Một số dịch vụ cơ bản trên mạng Internet :

##### iv. Dịch vụ phân giải tên miền DNS

- Giới thiệu :

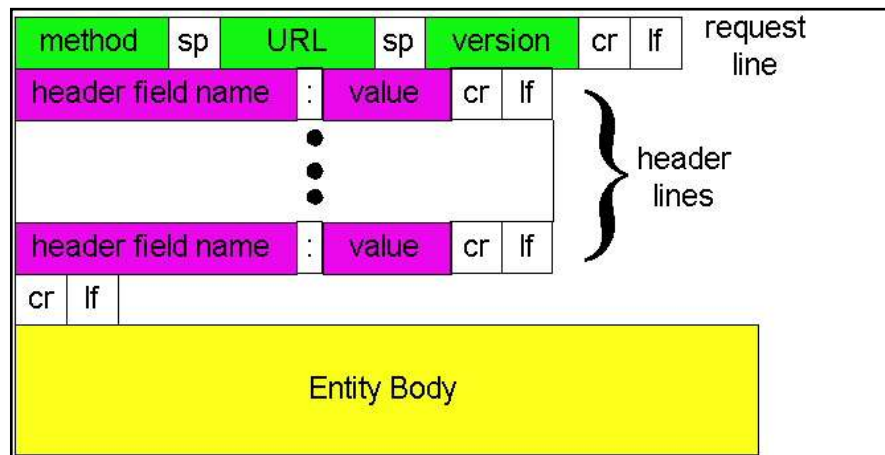
- ✓ Máy tính muốn bắt tay với nhau cần phải biết địa chỉ **IP** của nhau, tuy nhiên việc nhớ địa chỉ **IP** là rất khó.
- ✓ Ngoài địa chỉ **IP** ra còn có hostname, tên máy thường dễ nhớ vì có tính trực quan và gọi nhớ hơn địa chỉ **IP**. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính và ngược lại.
- ✓ Bắt đầu từ mạng ARPANET: Một tập tin đơn HOSTS.TXT (trên 1 máy chủ) và tên máy chỉ là 1 chuỗi văn bản không phân cấp. Tuy nhiên HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng.
- Cơ chế hoạt động của dịch vụ DNS
  - ✓ Hoạt động theo mô hình Client-Server:
  - ✓ Phần Server gọi là máy chủ phục vụ tên Name Server, chứa các thông tin CSDL của DNS.
  - ✓ Phần Client là trình phân giải tên Resolver, nó chỉ là các hàm thư viện dùng để tạo các query và gửi chúng đến Name Server.
  - ✓ DNS được thi hành như một giao thức tầng Application trong mạng TCP/IP.
- DNS là một CSDL phân tán:
  - ✓ Người quản trị cục bộ quản lý phần dữ liệu nội bộ của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình Client - Server.
  - ✓ Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (replication) và lưu tạm (caching). Một hostname trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.).
- **Phân giải tên thành địa chỉ IP**
  - ✓ **Root name server** : quản lý các **Server** ở mức **top-level domain**. Khi có truy vấn về một tên miền nào đó thì **Root Name Server** phải cung cấp **tên** và địa chỉ **IP** của **Server** quản lý **top-level domain**.
  - ✓ Các **Server** của **top-level domain** cung cấp danh sách các **tên** và **IP** của **Server** quản lý **second-level domain** mà tên miền này thuộc vào.
  - ✓ Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.
- **Phân giải IP thành tên máy tính**
  - ✓ Để có thể phân giải tên máy tính của một địa chỉ IP, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ IP, có tên miền là in-addr.arpa.
  - ✓ Mỗi nút trong miền in-addr.arpa có một tên nhãn là chỉ số thập phân của địa chỉ IP.

## **Tiết 6:**

### **v. Dịch vụ WEB**

- ✓ Dịch vụ WEB (WWW - World Wide Web) dựa trên giao thức HTTP, được xây dựng và hoạt động theo mô hình Client/Server. Các client dùng một phần mềm gọi là Web Browser. Web Browser tiếp nhận thông tin yêu cầu từ người dùng sau đó gửi các yêu cầu tới máy Server xử lý.
- ✓ Web Server cũng là một phần mềm chạy trên các máy phục vụ (IIS, Apache), nhận Request thực hiện theo yêu cầu rồi trả thông tin (Response) cho người sử dụng.
- ✓ Mô hình và ví dụ hoạt động của HTTP.

- ✓ Dạng tổng quát của HTTP request:



Hình 6.9: Header của HTTP request

- ✓ Khuôn dạng của HTTP response:

```
HTTP/1.0 200 OK
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 1998 .....
Content-Length: 6821
Content-Type: text/html

data data data data data ...
```

Hình 6.10 Khuôn dạng của HTTP response

- ✓ Quá trình xác thực
- ✓ Tạo lưu trữ tạm thời caching

#### vi. Dịch vụ thư điện tử :

- ✓ Có 3 thành phần chủ yếu:

- Tác nhân sử dụng (user agent)
- Mail servers
- Giao thức truyền và nhận thư : SMTP, POP3

##### [4] User Agent

- Soạn, sửa, đọc, xóa .. Email. Ví dụ: Eudora, Outlook, elm, Netscape Messenger.
- Mail gửi đi (outgoing), và nhận về (incoming) được lưu trữ trên server

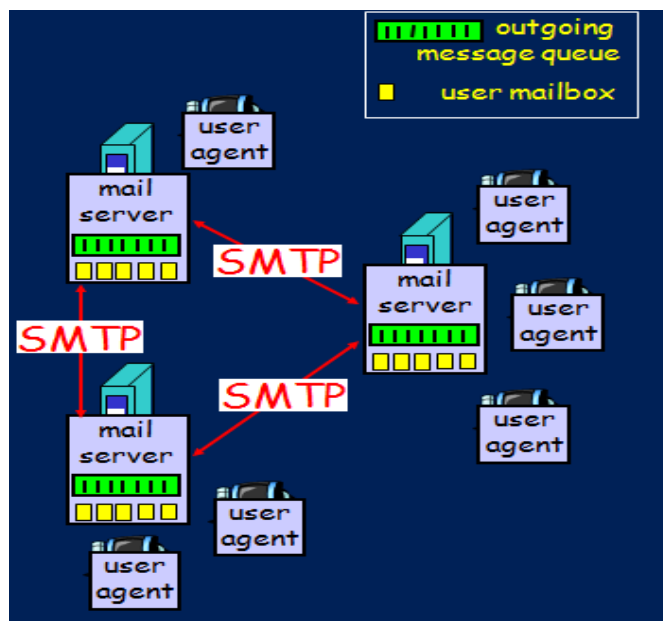
##### [5] Mail Servers

- Mailbox chứa các thư đến của người sử dụng.
- Message queue quản lý các thư người sử dụng gửi đi.

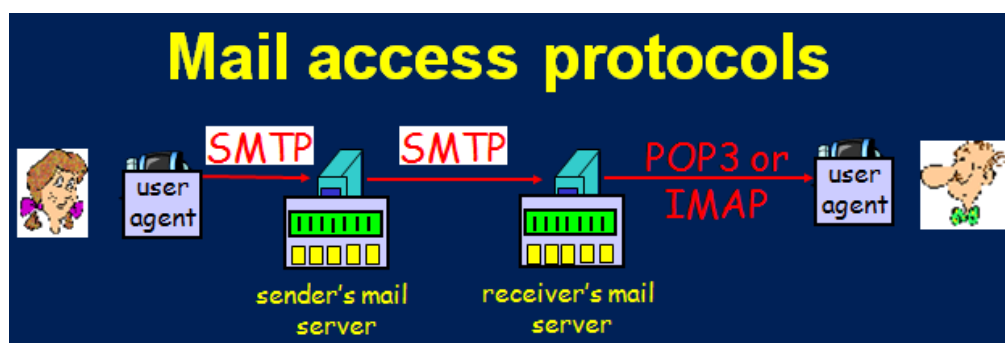
##### [6] Giao thức truyền và nhận thư:

SMTP: Phân phát/lưu trữ đến Server nhận.

- **SMTP** (Simple Mail Transfer Protocol): Giao thức gửi email.
- **POP3, IMAP** – giao thức nhận email.



Hình 6.11: Hệ thống Email



Hình 6.12: Giao thức nhận và gửi Email.

u) Nội dung thảo luận:

**Tiết 7-9:**

- iv. Ứng dụng thương mại điện tử
- v. Ứng dụng truyền file FTP và phân giải tên miền DNS
- vi. Ứng dụng thư điện tử
- v) Nội dung tự học
- iv. Mô hình TCP/IP
- v. Cấu trúc và hoạt động của các giao thức cơ bản trong mô hình.
- vi. Các dịch vụ internet.

w) Bài tập (bắt buộc)

x) Thực hành:

**Tiết 9 -12:**

- iii. Mô phỏng hoạt động và tìm hiểu cấu trúc của các giao thức trong mô hình TCP/IP sử dụng Packet Tracer
- iv. Bắt và phân tích gói tin sử dụng WireShark

5. Tài liệu tham khảo (sách, báo – chi tiết đến chương, mục, trang)

- i. Bài giảng của giáo viên, Slide chương 6.



**ii.** TL [1] , chương 7; trang 444

**iii.** TL [2], chương 5, chương 9.

6. Câu hỏi ôn tập:

**iv.** Trình bày mô hình TCP/IP, so sánh với mô hình OSI

**v.** Cấu trúc và hoạt động của các giao thức cơ bản trong mô hình TCP/IP.

**vi.** Trình bày và phân tích ứng dụng của các dịch vụ internet.

**HỌC PHẦN: Mạng máy tính**

Bộ môn: An Ninh Mạng

Giáo viên: 1) Nguyễn Đức Thiện  
2) Cao Văn Lợi

1. Bài (chương, mục): **Chương VII: Một số vấn đề chuyên sâu về mạng máy tính**

2. Thời lượng:

- GV giảng: 3 tiết.
- Thảo luận: 3 tiết,
- Thực hành: 0 tiết.
- Bài tập: 3 tiết.
- Tự học: 9 tiết

3. Mục đích, yêu cầu:

Mục đích: Giúp sinh viên nắm được một số vấn đề chuyên sâu hơn về mạng máy tính. Bao gồm vấn đề rất quan trọng và cấp bách hiện nay là an toàn và bảo mật mạng máy tính. Bên cạnh đó có hệ thống, công nghệ được sử dụng nhiều ở các công ty cơ quan là mạng riêng ảo. Ngoài ra, sơ lược về nội dung quản trị mạng và các ứng dụng khác cũng được đề cập trong chương.

Yêu cầu:

- Học viên tham gia học tập đầy đủ.
- Nghiên cứu trước các nội dung có liên quan đến bài giảng (đã có trên <http://http://fit.mta.edu.vn/~thiennd/>).
- Chuẩn bị bài thảo luận.
- Chuẩn bị bài tập ở nhà và làm trên lớp.

4. Nội dung:

a. Nội dung chi tiết: (công thức, định lý, hình vẽ)

**Tiết 1:**

- Giới thiệu nội dung chương
  - ✓ An toàn và bảo mật mạng máy tính
  - ✓ Kỹ thuật mạng riêng ảo
  - ✓ Quản trị mạng
  - ✓ Một số lĩnh vực ứng dụng

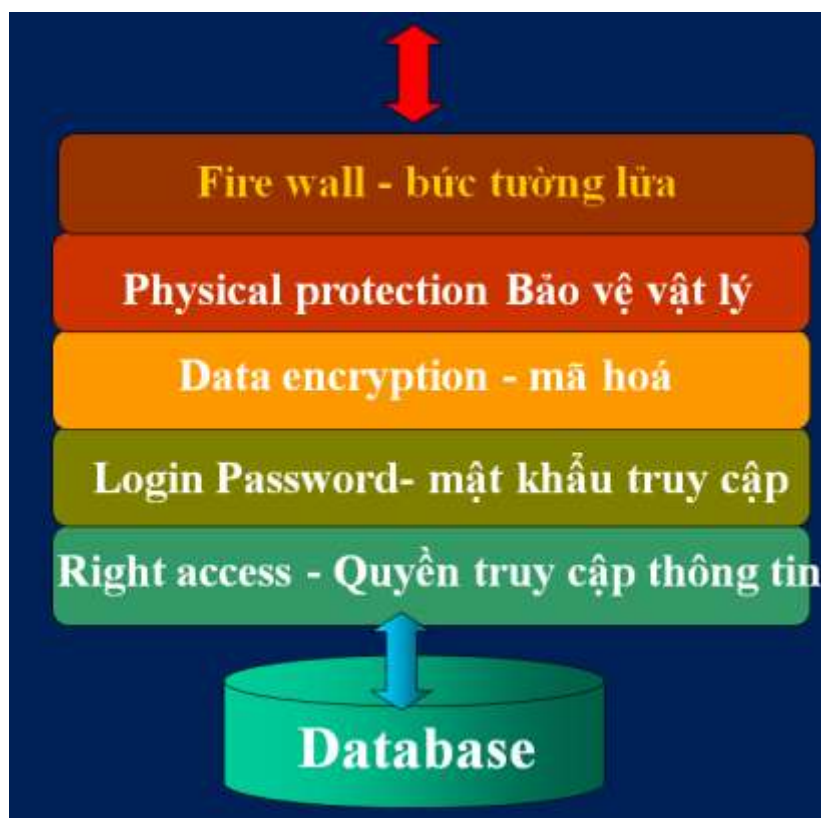
**1) An toàn và bảo mật mạng máy tính**

**i. Giới thiệu:**

- ✓ Mạng máy tính ngày càng mở rộng và phát triển, tài nguyên thông tin ngày càng được chia sẻ cho người sử dụng, tuy nhiên trong thực tế tồn tại những thông tin cần phải được bảo vệ và chia sẻ một cách có chọn lọc, do đó cần phải có cơ chế bảo đảm sự an toàn thông tin trên mạng.
- ✓ Cơ chế an toàn thông tin trên mạng phải thoả mãn hai mục tiêu cơ bản sau:
  - Bảo đảm điều kiện thuận lợi cho những người sử dụng hợp pháp trong quá trình khai thác và sử dụng tài nguyên trên mạng
  - Ngăn chặn có hiệu quả những kẻ truy cập và khai thác, phá hoại các tài nguyên bất hợp pháp.
- ✓ Về bản chất nguy cơ các vi phạm bất hợp pháp được chia làm hai loại: vi phạm thụ động và vi phạm chủ động. Vi phạm thụ động đôi khi do vô tình

hoặc không cố ý, còn vi phạm chủ động có mục đích phá hoại rõ ràng và hậu quả khôn lường.

**ii. Mô hình các lớp bảo vệ thông tin trên mạng**



*Hình 7.1: Mô hình các lớp bảo vệ thông tin trên mạng*

**iii. Mã hóa dữ liệu:**

- Mã hóa cổ điển
  - ✓ Phương pháp thay thế
  - ✓ Phương pháp dịch chuyển
  - ✓ Phương pháp hoán vị
- Mã hóa đối xứng (mã hóa bí mật)
  - ✓ DES
  - ✓ AES
- Mã hóa bất đối xứng (Mã hóa công khai)
  - ✓ Hệ mật RSA
  - ✓ Hệ mật Elgamal
  - ✓ Phương pháp ECC
- Chức năng cơ bản của mật mã hiện đại
  - ✓ Tính bí mật
  - ✓ Tính toàn vẹn
  - ✓ Tính xác thực
  - ✓ Tính chống chối từ
- Hàm băm, chữ ký số và PKI

**Tiết 2:**

**2) Mạng riêng ảo VPN**

**i. Giới thiệu**

- Mạng riêng ảo VPN – Virtual Private Network, là phương pháp làm cho một mạng công cộng hoạt động như một mạng cục bộ kết hợp với các giải pháp bảo mật trên đường truyền. VPN cho phép thành lập các kết nối riêng với người dùng ở xa, các

văn phòng chi nhánh của công ty và các đối tác của công ty đang sử dụng chung một mạng công cộng.

- Khái niệm định đường hầm (Tunneling): Là cơ chế dùng cho việc đóng gói một giao thức trong một giao thức khác. Định đường hầm cho phép che dấu giao thức lớp mạng nguyên thủy bằng cách mã hoá gói dữ liệu và chứa gói đã mã hoá vào trong một vỏ bọc IP.
- Chất lượng dịch vụ  
VPN còn cung cấp các thỏa thuận về chất lượng dịch vụ (QoS), định ra một giới hạn trên cho phép về độ trễ trung bình của gói trong mạng.

VPN= Định đường hầm + Bảo mật + Các thỏa thuận QoS

**ii. Tại sao phải xây dựng VPN?**

- Giảm chi phí đường truyền
- Giảm chi phí đầu tư.
- Giảm chi phí quản lý và hỗ trợ.
- Truy cập mọi lúc mọi nơi.

**iii. Phân loại mạng riêng ảo**

- Truy cập từ xa (Remote Access)
- Kết nối chi nhánh của công ty (Site to Site)
- Mạng mở rộng (ExtranetVPN)

**iv. Kiến trúc VPN**

- Không duy trì kết nối thường trực giữa các điểm cuối, thay vào đó một nối chỉ được tạo ra giữa hai site khi cần thiết, khi không còn cần thiết nữa thì nó sẽ bị huỷ bỏ, tài nguyên mạng sẵn sàng cho những kết nối khác.
- Đối với người sử dụng VPN những thành phần vật lý của mạng được các ISP giấu đi. Việc che giấu cơ sở hạ tầng của ISP và Internet được thực hiện bởi khái niệm gọi là định đường hầm (Tunneling)
- Việc tạo đường hầm tạo ra một kết nối đặc biệt giữa hai điểm cuối. Để tạo ra một đường hầm điểm cuối nguồn phải đóng các gói của mình trong những gói IP (IP Packet) cho việc truyền qua Internet. Trong VPN việc đóng gói bao gồm cả việc mã hoá gói gốc. Điểm cuối nhận, cổng nối (Gateway) gỡ bỏ tiêu đề IP và giải mã gói nếu cần và chuyển gói đến đích của nó.
- Việc tạo đường hầm cho phép những dòng dữ liệu và thông tin người dùng kết hợp được truyền trên một mạng chia sẻ trong một ống ảo (virtual pipe). Ống này làm cho việc định tuyến trên mạng hoàn toàn trở nên trong suốt đối với người dùng.

**v. Các dịch vụ bảo mật VPN**

- ✓ Authentication: Bảo đảm dữ liệu đến có nguồn gốc rõ ràng.
- ✓ Access control: Ngăn chặn những người dùng bất hợp pháp.
- ✓ Confidentiality: Hạn chế việc dữ liệu bị phá hoại trên đường truyền.
- ✓ Data integrity: Bảo không ai có thể thay đổi nội dung dữ liệu trên đường truyền.

**vi. Một số giao thức cho VPN:**

- ✓ Point to Point Tunneling Protocol (PPTP)
- ✓ Layer 2 Tunneling Protocol (L2TP)

### **Tiết 3:**

#### **3) Quản trị mạng**

**i. Thiết kế, xây dựng, nâng cấp và đảm bảo hoạt động của hệ thống mạng.**

- ✓ Quản trị thiết kế.
- ✓ Quản trị xây dựng
- ✓ Quản trị điều hành
- ✓ Quản trị đảm bảo an toàn và bảo mật

**ii. Quản trị thiết bị mạng**

- ✓ Lắp đặt hệ thống mạng
- ✓ Cấu hình hoạt động của các thiết bị và hệ thống
- ✓ Cài đặt đảm bảo an ninh cho các thiết bị
- iii. Quản trị hệ điều hành
  - Quản trị hệ điều hành mạng Windows Server
    - ✓ Giới thiệu Windows Server
    - ✓ Active Directory
    - ✓ Chính sách hệ thống và người dùng
  - Quản trị hệ điều hành Linux
- 4) Một số lĩnh vực ứng dụng khác.
  - ✓ Ứng dụng thoại VoIP
  - ✓ Ứng dụng hội thảo truyền hình
  - ✓ Công nghệ điện toán đám mây.

b. Nội dung thảo luận:

**Tiết 4-6:**

Kỹ thuật mạng riêng ảo VPN và các vấn đề bảo mật cho mạng riêng ảo.

c. Nội dung tự học

i. Tổng quan về an toàn và bảo mật thông tin. Khái niệm, mục tiêu và mô hình.

ii. Kỹ thuật mạng riêng ảo

iii. Vấn đề quản trị mạng

d. Bài tập (bắt buộc)

**Tiết 7-9:**

i. Phương pháp mã hóa cổ điển

ii. Phương pháp mã hóa công khai

iii. Cài đặt VPN

5. Tài liệu tham khảo (sách, báo – chi tiết đến chương, mục, trang)

i. Bài giảng của giáo viên, Slide chương 7.

ii. TL [1], chương 8; trang 557

iii. TL [2], chương 8, trang 578.

6. Câu hỏi ôn tập:

i. Đối tượng và mục tiêu đảm bảo an toàn và bảo mật

ii. Mô hình đảm bảo an toàn và bảo mật

iii. Tại sao phải xây dựng VPN

iv. Giao thức định đường hầm

v. Đặc điểm và cấu trúc Active Directory trong Windows Server.

vi. Chính sách phân quyền và chính sách hệ thống