

## CHƯƠNG 6: MÔ HÌNH TCP/IP VÀ MẠNG INTERNET

1. Thời lượng: GV giảng: 6; Thảo luận: 3; Thực hành: 3; Tự học: 12.

2. 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://fit.mta.edu.vn/~thiennd/>).

Chuẩn bị bài thảo luận.

Chuẩn bị và tham gia thực hành tại phòng thí nghiệm

1

### I. Mô hình TCP/IP

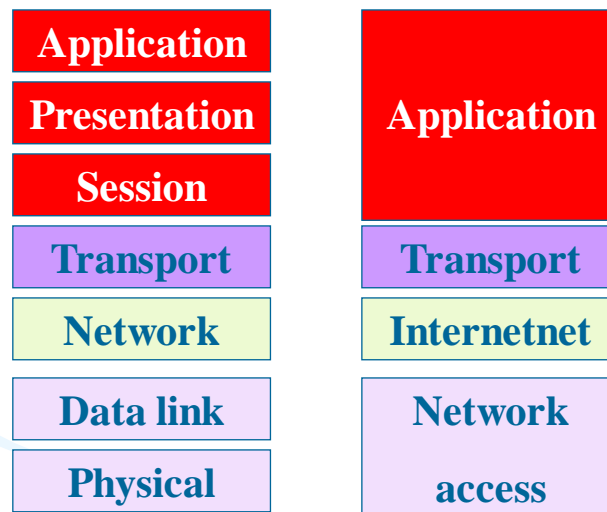
- Cuối năm 1960 và đầu 1970, Trung tâm nghiên cứu cấp cao (Advanced Research Projects Agency - ARPA) bộ quốc phòng Mỹ (DoD) được giao trách nhiệm phát triển mạng ARPANET.
- Đầu năm 1980, bộ giao thức TCP/IP ra đời làm giao thức chuẩn cho mạng ARPANET và các mạng của DoD.

2

## I.1. Mô hình kiến trúc TCP/IP

- Bộ giao thức TCP/IP được phân làm 4 tầng
  - Tầng ứng dụng (Application Layer)
  - Tầng giao vận (Transport Layer)
  - Tầng Internet (Internet Layer)
  - Tầng truy cập mạng (Network access Layer)

3



Các tầng tương ứng giữa OSI và TCP/IP


4



## I.2. Chức năng của các tầng

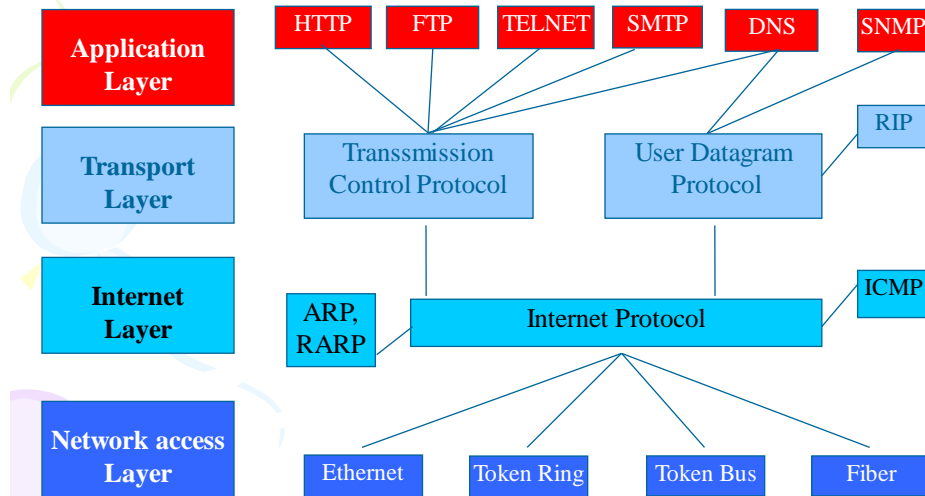
- **Application layer:** hỗ trợ các ứng dụng cho các giao thức tầng Host-to-Host. Cung cấp giao diện cho người sử dụng mô hình TCP/IP. Các giao thức ứng dụng gồm HTTP, TELNET, FTP, SMTP ,...
- **Transport layer:** thực hiện những kết nối giữa hai máy chủ trên mạng bằng 2 giao thức: TCP (Transmission Control Protocol) và UDP ( User Datagram Protocol).

5

- 
- **Internet Layer:** 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.
  - **Network Access Layer:** 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, Tolen Ring, Token Bus... Cung cấp các dịch vụ cho tầng Internet.

6

## Các giao thức tương ứng với các lớp trong mô hình TCP/IP



7

- **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.

8



- **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



9



- **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): Nghi thức thông báo.



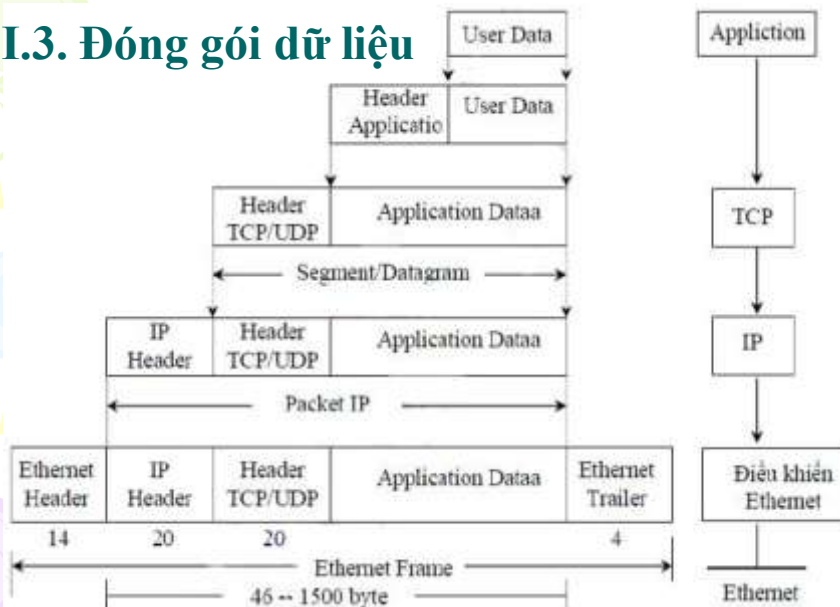
- **UDP** (User Datagram Protocol): Giao thức truyền không kết nối cung cấp dịch vụ truyền không tin cậy nhưng tiết kiệm chi phí truyền.

10

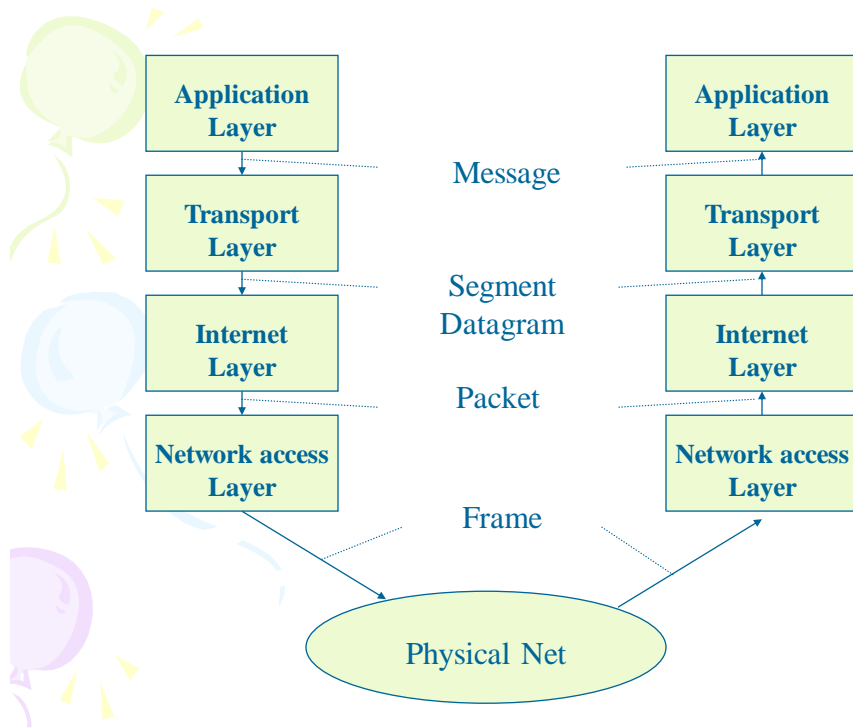
- **TCP** (Transmission Control Protocol): Giao thức hướng kết nối cung cấp dịch vụ truyền thông tin cậy.
- **IP** (Internet Protocol): chuyển giao các gói tin qua các máy tính đến đích.
- **ARP** (Address Resolution Protocol): Cơ chế chuyển địa chỉ TCP/IP thành địa chỉ vật lý của các thiết bị mạng.

11

### I.3. Đóng gói dữ liệu



12



13

## Mạng con và mặt nạ mạng con

- Mạng Internet sử dụng địa chỉ IP 32 bit và phân chia ra các lớp rất mềm dẻo. Tuy nhiên, với một hệ thống địa chỉ như vậy việc quản lý vẫn rất khó khăn.
- Nếu như một mạng được cấp một địa chỉ lớp A thì có nghĩa nó chứa tới  $16 \times 1.048.576$  máy tính
- Do vậy người ta dùng mặt nạ bit để phân chia mạng ra thành những mạng con gọi là Subnet.

14



## II. Giao thức trong mô hình TCP/IP

1. IP
2. TCP
3. UDP
4. ICMP
5. ARP/ RARP

15



### II.1. Internet Protocol - 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.

16



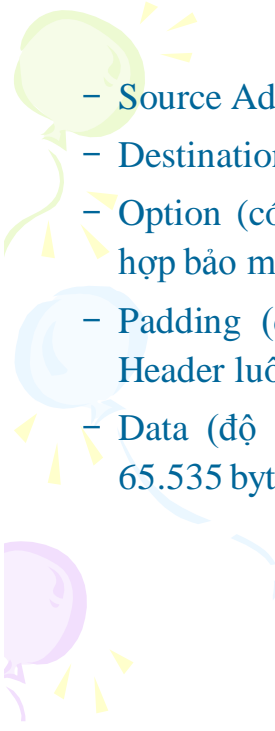
## Cấu trúc gói tin trong giao thức IP

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				

17

- 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.

18

- 
- 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.

19



## II.2. Transmission Control Protocol

- 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.

20

## Cấu trúc gói tin TCP

SOURCE PORT			DESTINATION PORT		
SEQUENCE NUMBER					
ACKNOWLEDGEMENT NUMBER					
HLEN	RESERVED	CODE BITS	WINDOW		
CHECK SUM			URGENT POINTER		
IP OPTION (IF ANY)				PADDING	
DATA					
* * *					
DATA					

21

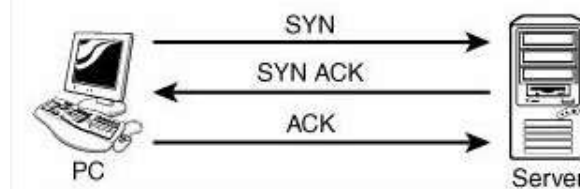
- Source Port (16 bit), Destination Port (16 bit)
- Sequence Number: 32 bits, số thứ tự khi phát.
- Acknowledgment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.
- HLEN (4 bits)
- Reserved (6 bit): 0, dành cho tương lai.
- Control bits: Các bits điều khiển
  - URG : Vùng con trỏ khẩn có hiệu 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 .

22

- 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.

23

## Quá trình kết nối và hủy kết nối của TCP



### Kết nối



### Hủy kết nối

24

## II.3. User Datagram Protocol

- 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.

25

## Cấu trúc gói tin UDP

SOURCE PORT	DESTINATION PORT
UDP MESSAGE LENGTH	UDP CHECKSUM
IP OPTION (IF ANY)	PADDING
DATA	
* * *	
DATA	

26



## 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

27



## II.4. ICMP(Internet Control Message Protocol)

- 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.
- Có hai loại: thông điệp truy vấn và thông điệp thông báo lỗi.
  - Điều khiển lưu lượng
  - Thông báo lỗi
  - Định hướng lại các tuyến
  - Kiểm tra các trạm ở xa

28

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)

29

## II.5. Giao thức phân giải địa chỉ ARP

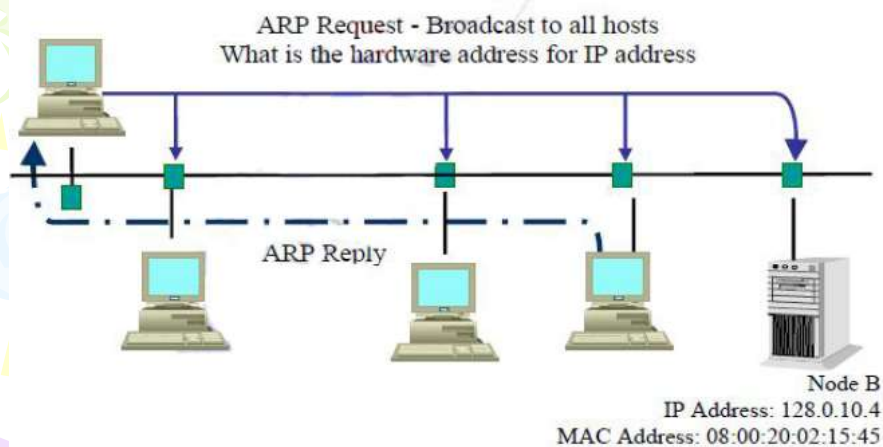
- Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích khi biết IP.
- Mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC (ARP Cache) nó chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ tương ứng mới.
- Trước khi trao 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.

30

### Tiến trình của ARP được mô tả như sau:

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

31



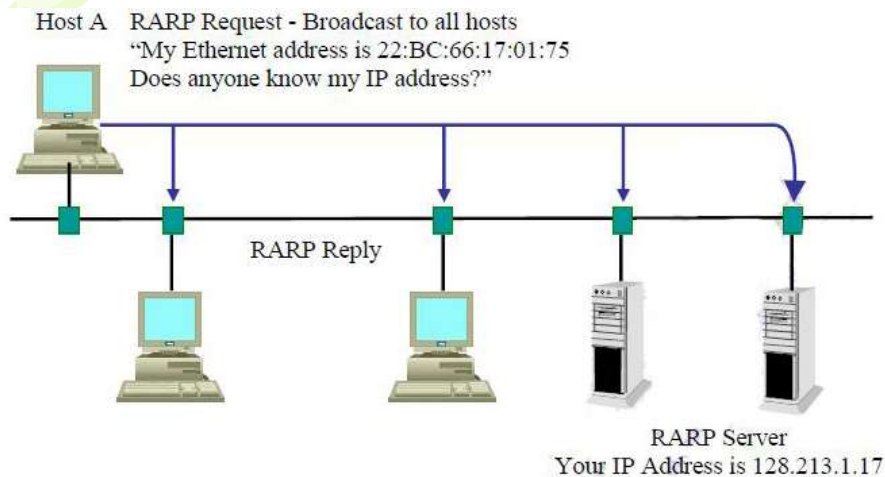
32



## II.6. 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

33



34



## Các giao thức ứng dụng

- File Transfer Protocol - FTP
- Domain Name System - DNS
- Simple Net Management Protocol - SNMP
- Simple Mail Transfer Protocol - SMTP
- Hyper Text Transfer Protocol - HTTP



35



## File Transfer Protocol - FTP


- Đây là một giao thức ứng dụng cung cấp cho người dùng phương pháp sao chép tệp từ một máy tính ở xa
- 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



36



## Sử dụng FTP




```
$ ftp sco5
Connected to sco5.
220-
220 sco5.cse.com.vn FTP server (Version 2.1WU(1)) ready.
User (sco5.cse.com.vn:(none)):binhnn
331 Password required for binhnn.
Password:
230 User binhnn logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get nettcp.c
local: nettcp.c remote: nettcp.c
200 PORT command successful.
150 Opening BINARY mode data connection for nettcp.c (46 bytes).
226 Transfer complete.
46 bytes received in 0 seconds (0.04 Kbytes/s)
ftp> bye
221 Goodbye.
$
```

37



## Domain Name System - DNS

- 
- Địa chỉ IP không mang thông tin về địa lý, tổ chức hay người dùng.
  - Người ta xây dựng hệ thống đặt tên gọi là Domain Name System để cung cấp cho người dùng cách đặt tên cho các máy tính với cách đặt tên thông thường quen thuộc
  - Tên\_người\_dùng@Tên\_miền

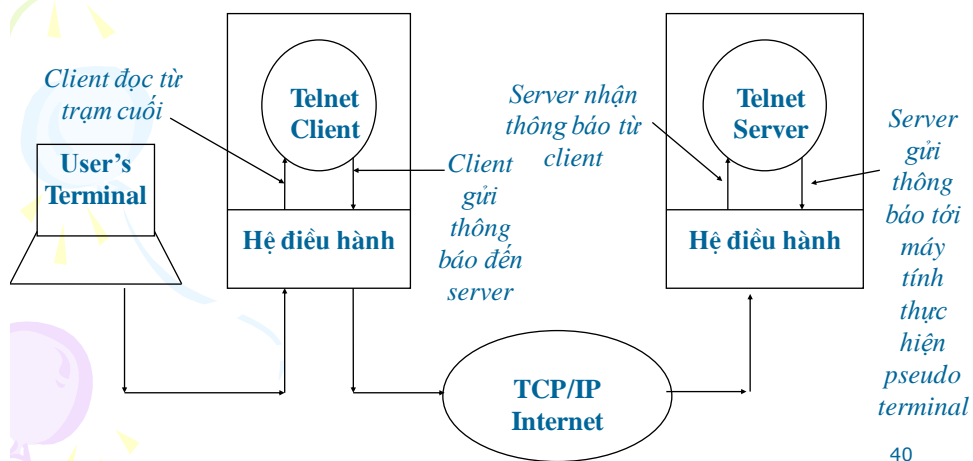
38

# 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

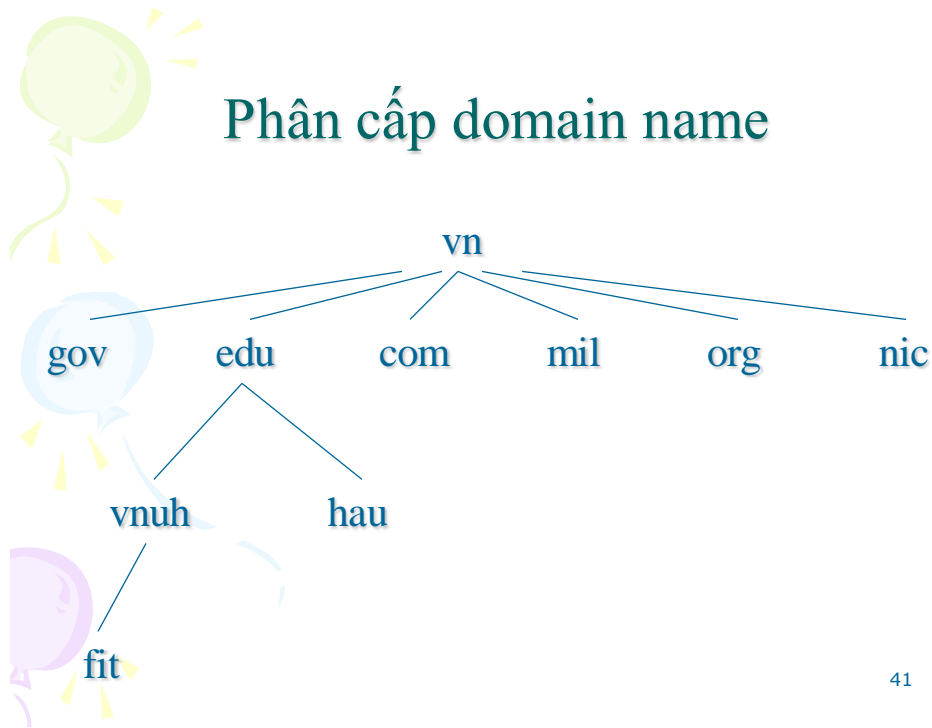
39

# Telnet



40

## Phân cấp domain name



41

## Domain Name System

- Một máy tính có thể có nhiều tên trên mạng
- Mỗi tên là duy nhất
- Việc ánh xạ địa chỉ IP - Domain Name được thực hiện bởi
  - Name server cài đặt tại các máy server
  - Name resolver cài đặt tại các máy trạm
- DNS được đặc tả trong RFC 1034, 1035

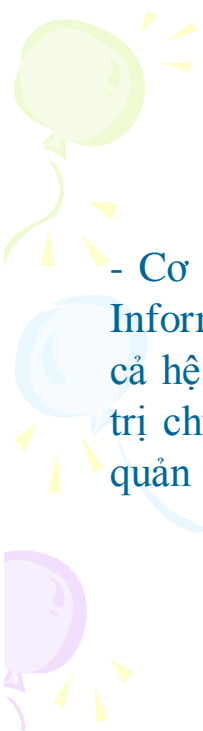
42

A decorative graphic on the left side of the slide featuring three balloons in green, blue, and purple, each with yellow streamers and small yellow starburst shapes.

## Simple Network Monitoring Protocol - SNMP

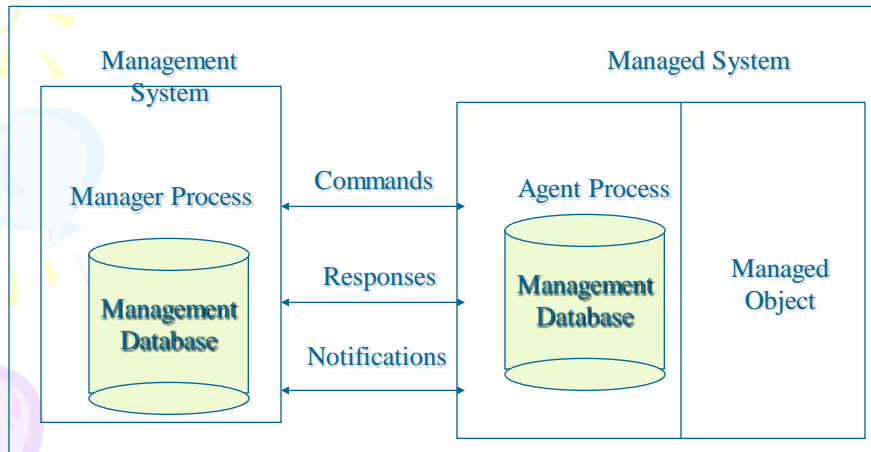
- Hệ thống quản trị mạng còn gọi là mô hình Manager/Agent bao gồm
  - Tiến trình quản trị cung cấp giao diện giữa người quản trị mạng với các thiết bị được quản trị
  - Hệ bị quản trị bao gồm tiến trình Agent thực hiện các thao tác quản trị và các đối tượng được quản trị như máy chủ, hub, kênh truyền...

43

- 
- A decorative graphic on the left side of the slide featuring three balloons in green, blue, and purple, each with yellow streamers and small yellow starburst shapes.
- Cơ sở thông tin quản trị (Management Information Base - MIB) được lưu trữ ở cả hệ thống quản trị và hệ thống bị quản trị chứa các thông tin cần thiết cho việc quản trị

44

## Mô hình Manager/Agent của hệ thống quản trị mạng



45

## 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

46

A decorative graphic on the left side of the slide featuring three balloons in green, blue, and purple, each with yellow streamers and small yellow starburst shapes.

## Simple Mail Transfer Protocol - SMTP

- Là giao thức sử dụng cho việc trao đổi thư điện tử giữa các người dùng trên mạng
- Chỉ ra cách thức một hệ thống phân phát mail chuyển các thông điệp qua một kết nối từ một máy này đến một máy khác.
- Đặc điểm nổi bật là việc xử lý không trực tuyến - off line, thư điện tử được lưu tại hòm thư của người sử dụng ở một trung tâm máy tính nào đó

47

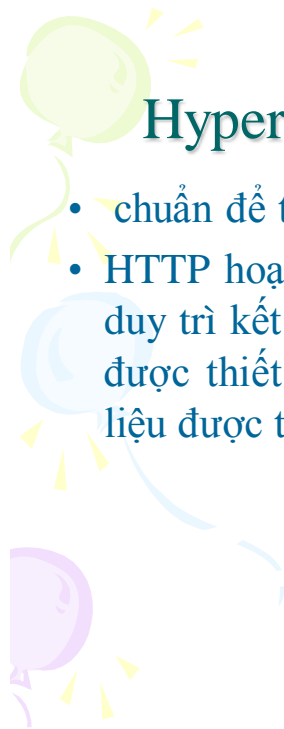
A decorative graphic on the left side of the slide featuring three balloons in green, blue, and purple, each with yellow streamers and small yellow starburst shapes.

## Simple Mail Transfer Protocol

- Tiến trình server cần có quyền ROOT để ghi vào hòm thư của mọi người, đây là một “lỗ hổng” trong vấn đề bảo vệ an toàn thông tin trên mạng
- Đặc tả cho SMTP có trong RFC 821

48

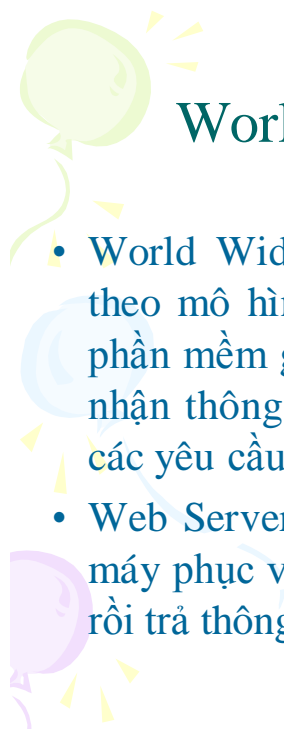




## Hyper Text Transfer Protocol

- chuẩn để truyền các siêu văn bản trên Web.
- HTTP hoạt động gần giống FTP nhưng không duy trì kết nối truyền lệnh, kênh truyền dữ liệu được thiết lập và giải phóng ngay sau khi tài liệu được truyền - nhận

49

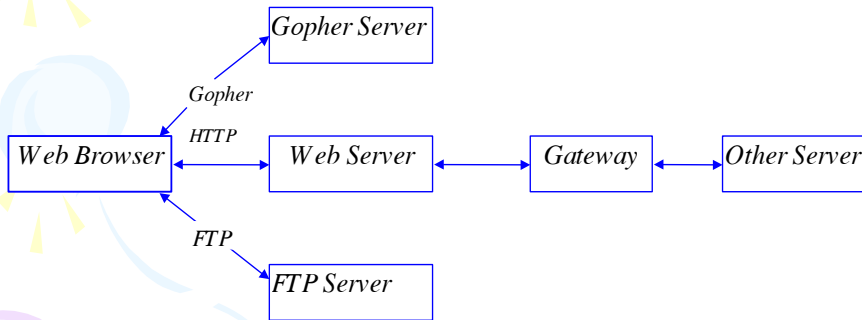


## World Wide Web - WWW

- World Wide Web 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, nhận Request thực hiện theo yêu cầu rồi trả thông tin (Response) cho người sử dụng.

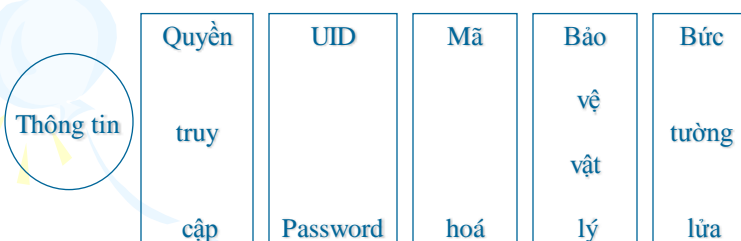
50

## Trao đổi thông tin Web Browser - Server



51

## Các lớp rào chắn bảo vệ thông tin

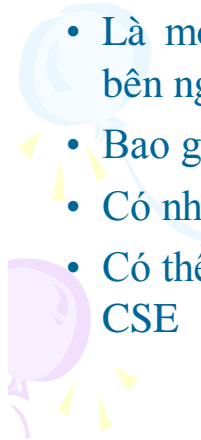


Mạng  
ngoài

52



## Bức tường lửa



- Một giải pháp an toàn thông tin được sử dụng rộng rãi nhất hiện nay trên Internet
- Là một tấm chắn giữa mạng nội bộ và mạng bên ngoài
- Bao gồm cả phần cứng và phần mềm
- Có nhiều loại bức tường lửa khác nhau
- Có thể xem chi tiết trong tài liệu Firewall của CSE

53



## Tài liệu tham khảo



- Andrew S.T., *Computer Network*, Prentice Hall, 1988.
- Douglas E.C., *Internetworking With TCP/IP*, v.2, Prentice Hall, 1994.
- Request for Comments - RFCs

54