



TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN

Bộ môn: Kỹ thuật máy tính và mạng

MÔN HỌC: MẠNG MÁY TÍNH

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC



Chương 1: Tổng quan về mạng máy tính

Chương 2: Mô hình kết nối các hệ thống mở OSI

Chương 3: Mô hình TCP/IP

Chương 4: Kỹ thuật mạng cục bộ LAN

Chương 5: Các thiết bị và dịch vụ mạng

CHƯƠNG 3: GIAO THỨC TCP/IP

1

- Mô hình TCP/IP

2

- Giao thức TCP/UDP

3

- Giao thức IP

4

- Giao thức ICMP

5

- Giao thức ARP/RARP

6

- Giao thức IPv6

7

- Kỹ thuật định tuyến

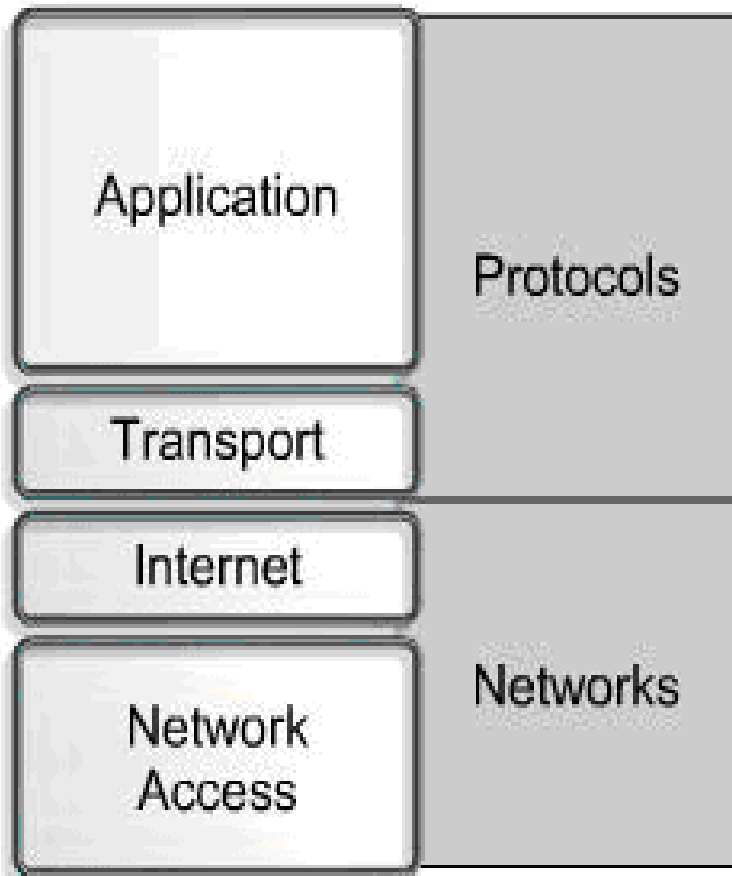
I. MÔ HÌNH TCP/IP

❖ Khái niệm về TCP và IP

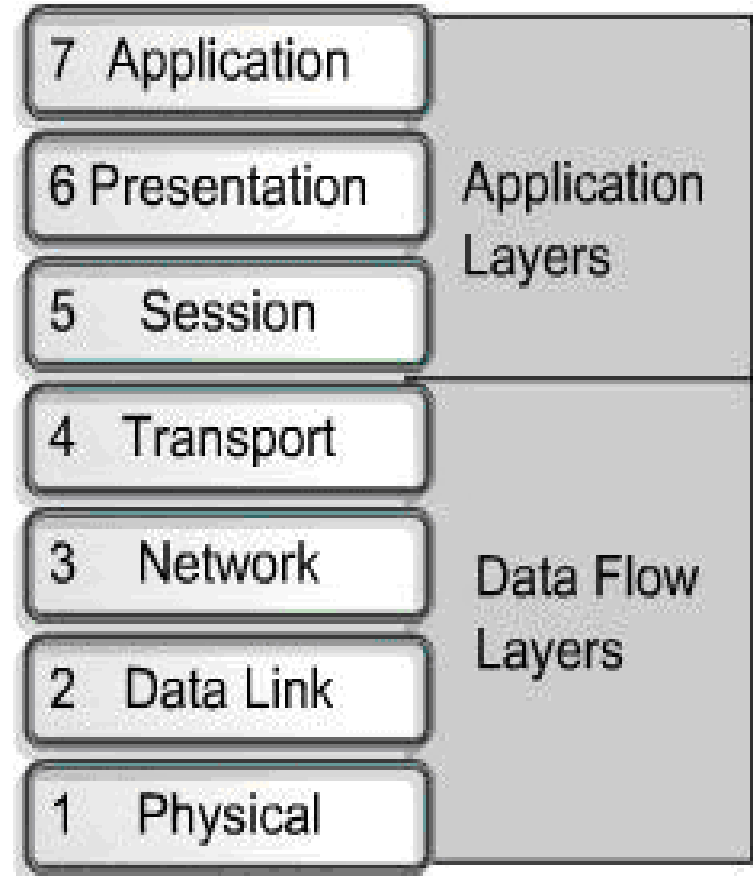
- TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển (Transport Layer) và là một giao thức hướng kết nối (connected-oriented).
- IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI và là một giao thức không kết nối (connectionless).
- ❖ Mô hình tham chiếu TCP/IP gồm 4 lớp tương ứng với mô hình OSI 7 lớp.

MÔ HÌNH OSI VÀ TCP/IP

TCP/IP Model



OSI Model



SO SÁNH MÔ HÌNH OSI VÀ TCP/IP

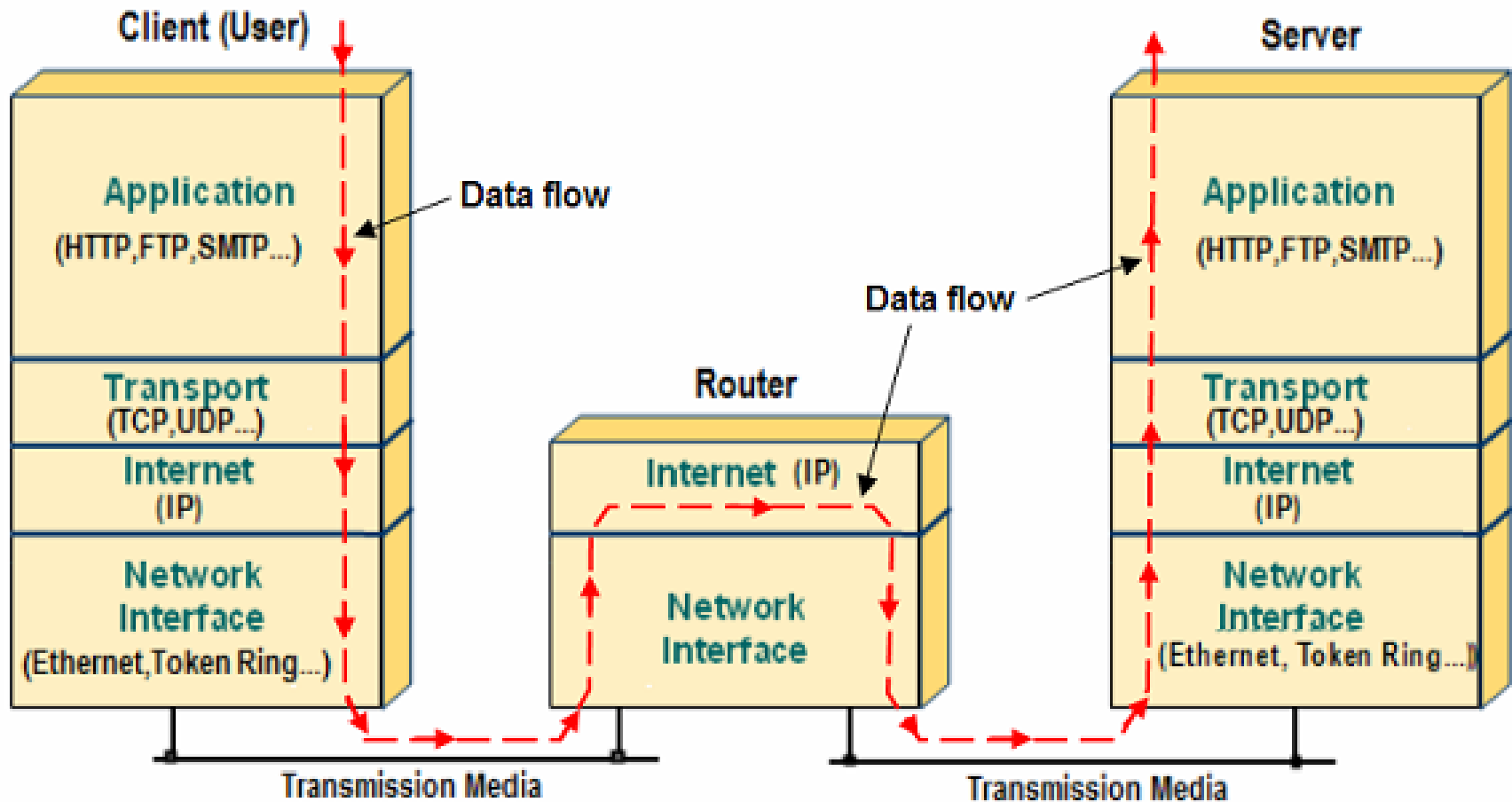
❖ Giống nhau

- Điều phân lớp chức năng
- Điều có lớp vận chuyển và lớp mạng.
- Chuyển gói là hiển nhiên.
- Điều có mối quan hệ trên dưới, ngang hàng.

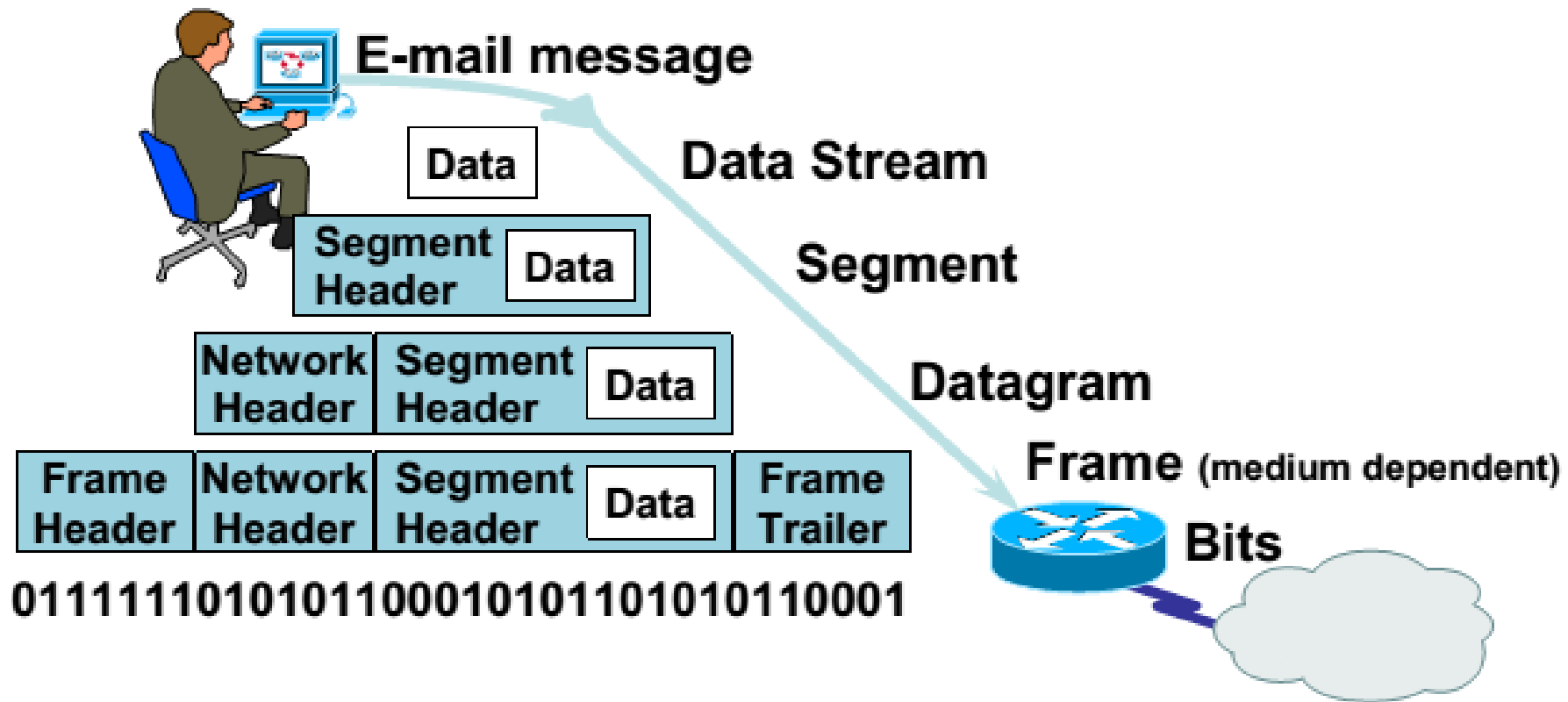
■ Khác nhau

- TCP/IP gộp lớp trình bày và lớp phiên vào lớp ứng dụng.
- TCP/IP gộp lớp vật lý và lớp liên kết dữ liệu vào lớp truy nhập mạng.
- TCP/IP đơn giản vì có ít lớp hơn.
- OSI không có khái niệm chuyển phát thiếu tin cậy ở lớp 4 như UDP của TCP/IP

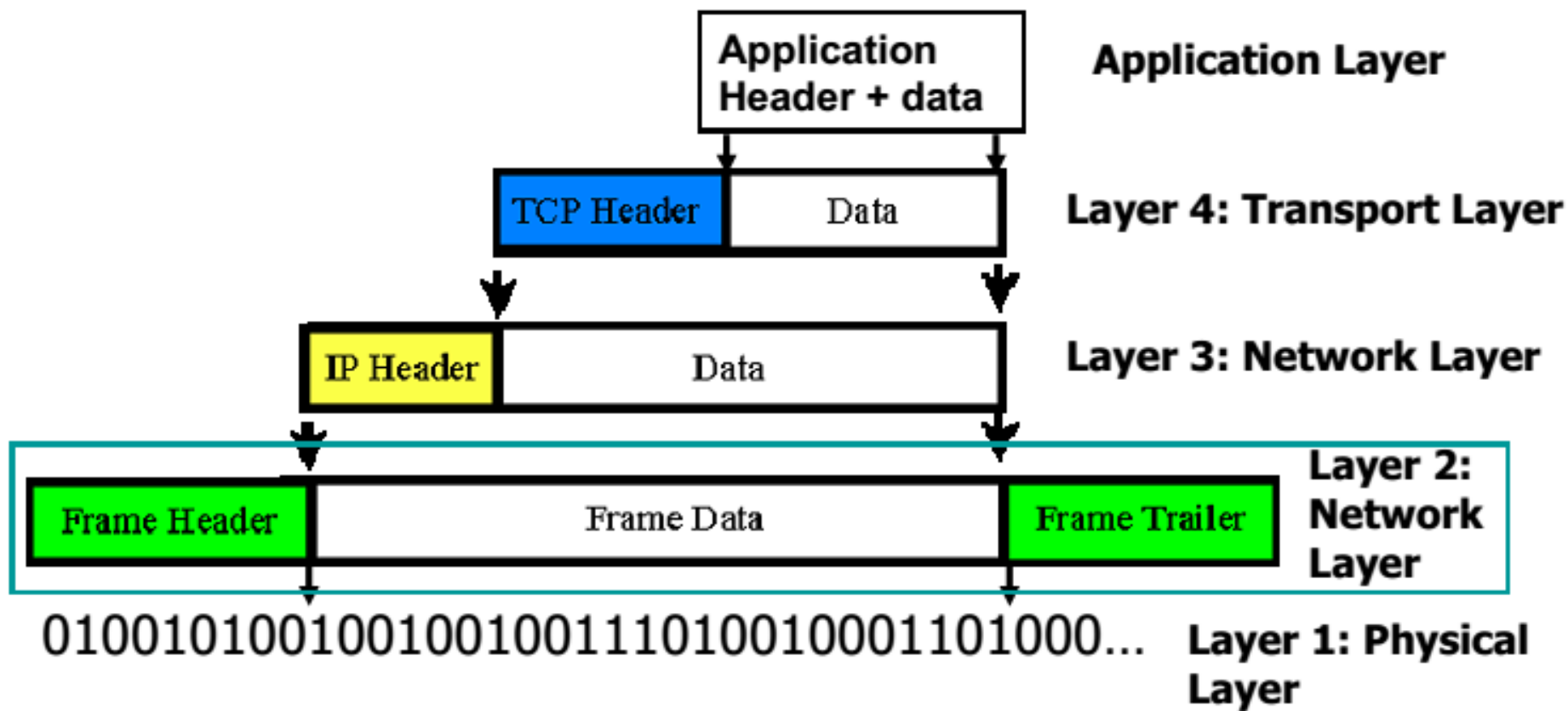
TRUYỀN TIN TRÊN MÔ HÌNH TCP/IP



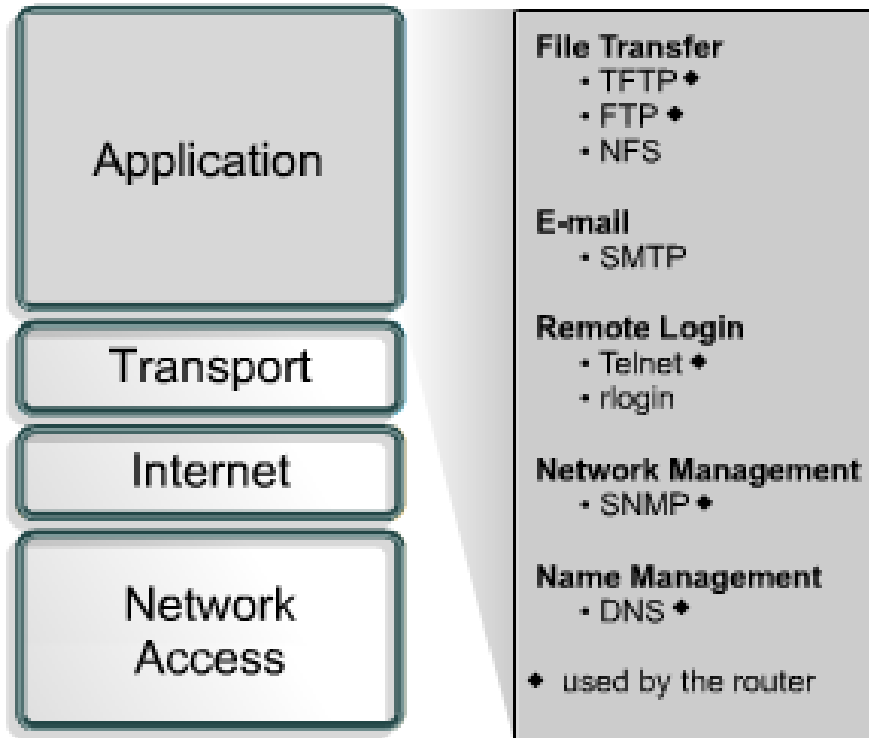
ĐÓNG GÓI GÓI TIN TRONG TCP/IP



VÍ DỤ ĐÓNG GÓI DỮ LIỆU



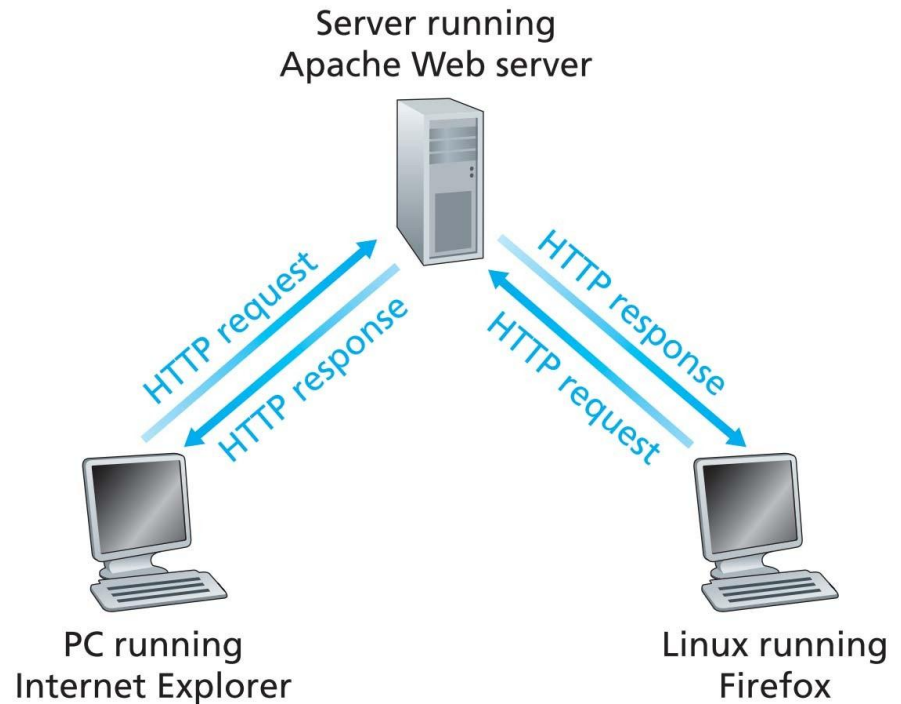
LỚP ỨNG DỤNG



- ❖ Kiểm soát các giao thức lớp cao, các chủ đề về định dạng dữ liệu, biểu diễn thông tin, mã hóa và điều khiển hội thoại.
- ❖ Lớp ứng dụng liên quan đến các chương trình ứng dụng.

Giới thiệu về HTTP

- ❖ HyperText Transfer Protocol (HTTP): Giao thức tầng ứng dụng của Web
 - ❖ RFC 1945 và RFC 2616
 - ❖ RFC 7540 (May 2015)
- ❖ HTTP sử dụng TCP làm giao thức tầng giao vận
- ❖ HTTP là giao thức không trạng thái (**stateless protocol**)



Quan sát HTTP message: Tạo HTTP request dùng trình duyệt

1. Chạy phần mềm Wireshark để ghi lại dữ liệu gửi nhận (Chọn Capture -> Start)
2. Mở trình duyệt vào trang web: tlu.edu.vn
3. Dừng việc ghi dữ liệu của phần mềm Wireshark
4. Gõ Filter: `http.host == "tlu.edu.vn"`
5. Quan sát HTTP message

*Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http.host=="tu.edu.vn"

No.	Time	Source	Destination	Protocol	Length	Info
99	12.989123	192.168.0.100	203.113.135.55	HTTP	880	[TCP ACKed unseen segment] GET /Tin-tuc HTTP/1.1
147	13.073781	203.113.135.55	192.168.0.100	HTTP	682	HTTP/1.1 200 OK (text/html)
226	13.681145	192.168.0.100	203.113.135.55	HTTP	784	GET /DesktopModules/cmsview/api/newscategory. HTTP/1.1
227	13.684633	192.168.0.100	203.113.135.55	HTTP	785	[TCP ACKed unseen segment] GET /DesktopModules/cmsview/api/newscategory. HTTP/1.1
228	13.684922	192.168.0.100	203.113.135.55	HTTP	759	[TCP ACKed unseen segment] GET /DesktopModules/cmsview/api/newscategory. HTTP/1.1
230	13.720480	192.168.0.100	203.113.135.55	HTTP	858	[TCP ACKed unseen segment] GET /DesktopModules/cmsview/api/newscategory. HTTP/1.1
234	13.746582	203.113.135.55	192.168.0.100	HTTP	128	HTTP/1.1 200 OK (application/json)
322	13.958649	203.113.135.55	192.168.0.100	HTTP	626	HTTP/1.1 200 OK (application/json)
339	14.015633	203.113.135.55	192.168.0.100	HTTP	76	HTTP/1.1 200 OK (application/json)
411	14.165279	192.168.0.100	203.113.135.55	HTTP	743	GET /Portals/0/2020/Thang9/hoc5.jpg HTTP/1.1
416	14.166601	192.168.0.100	203.113.135.55	HTTP	743	GET /Portals/0/2020/Thang9/hoc1.jpg HTTP/1.1

- Frame 227: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface 0
- Ethernet II, Src: Azurewav_8f:3b:b1 (28:c2:dd:8f:3b:b1), Dst: Tp-LinkT_e1:31:d2 (34:e8:94:e1:31:d2)
- Internet Protocol Version 4, Src: 192.168.0.100, Dst: 203.113.135.55
- Transmission Control Protocol, Src Port: 49893, Dst Port: 80, Seq: 1, Ack: 2, Len: 731
- Hypertext Transfer Protocol

```

0000  34 e8 94 e1 31 d2 28 c2 dd 8f 3b b1 08 00 45 00  4...1.(...;...E.
0010  03 03 7e a2 40 00 80 06 65 9d c0 a8 00 64 cb 71  ...~@... e....d.q
0020  87 37 c2 e5 00 50 bd 6a 5b ba 8a ef e4 05 50 18  .7...P.j[.....P.
0030  fe b5 6b 99 00 00 47 45 54 20 2f 44 65 73 6b 74  ..k...GE T /Deskt
0040  6f 70 4d 6f 64 75 6c 65 73 2f 63 6d 73 76 69 65  opModule s/cmsvie
0050  77 2f 61 70 69 2f 6e 65 77 73 63 61 74 65 67 6f  w/api/ne wscatego
0060  72 79 2f 6c 69 73 74 62 79 73 65 74 74 69 6e 67  ry/listb ysetting
0070  3f 4d 6f 64 75 6c 65 49 64 3d 31 35 35 35 26 50  ?ModuleI d=1555&P
0080  6f 72 74 61 6c 49 64 3d 30 20 48 54 54 50 2f 31  ortalId= 0 HTTP/1

```

***Wireless Network Connection**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host=="tlu.edu.vn"

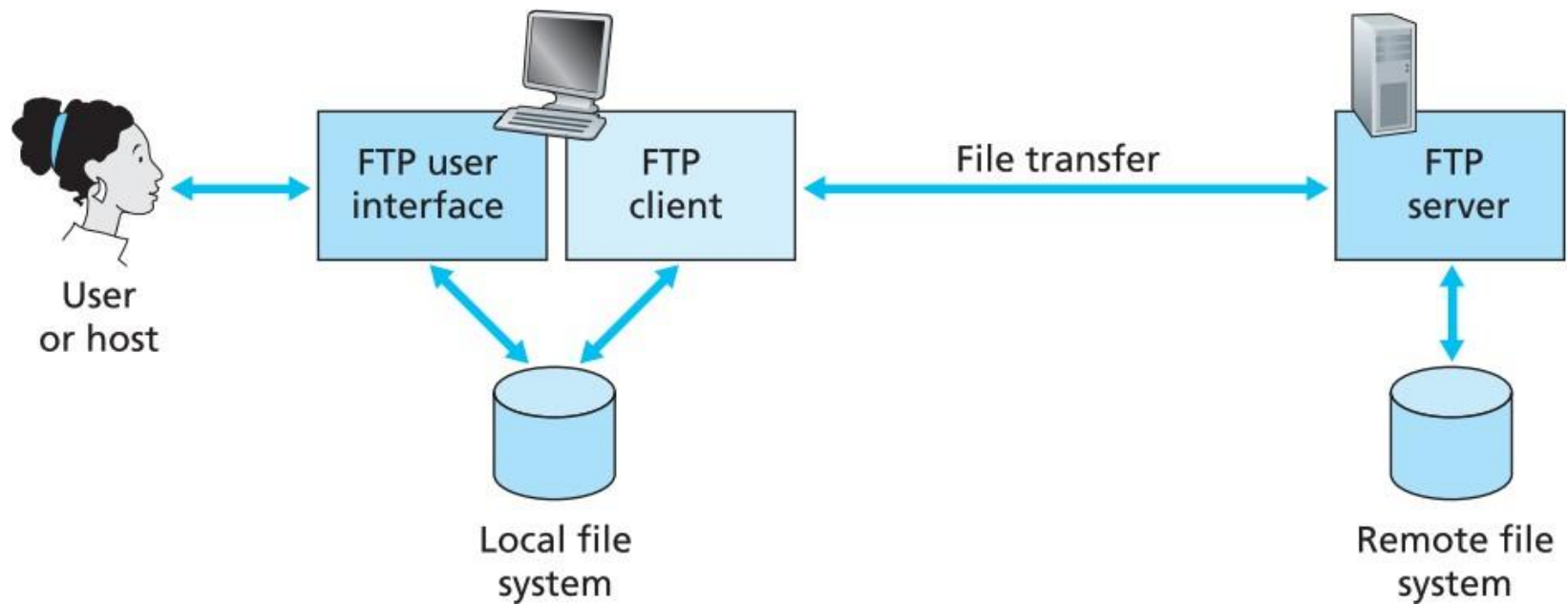
No.	Time	Source	Destination	Protocol	Length	Info
99	12.989123	192.168.0.100	203.113.135.55	HTTP	880	[TCP ACKed unseen segment] GET /Tin-tuc HTTP/
147	13.073781	203.113.135.55	192.168.0.100	HTTP	682	HTTP/1.1 200 OK (text/html)
226	13.681145	192.168.0.100	203.113.135.55	HTTP	784	GET /DesktopModules/cmsview/api/newscategory/
227	13.684633	192.168.0.100	203.113.135.55	HTTP	785	[TCP ACKed unseen segment] GET /DesktopModule
228	13.684922	192.168.0.100	203.113.135.55	HTTP	759	[TCP ACKed unseen segment] GET /DesktopModule
230	13.720480	192.168.0.100	203.113.135.55	HTTP	858	[TCP ACKed unseen segment] GET /DesktopModule
234	13.746582	203.113.135.55	192.168.0.100	HTTP	128	HTTP/1.1 200 OK (application/json)
322	13.958649	203.113.135.55	192.168.0.100	HTTP	626	HTTP/1.1 200 OK (application/json)
339	14.015633	203.113.135.55	192.168.0.100	HTTP	76	HTTP/1.1 200 OK (application/json)
411	14.165279	192.168.0.100	203.113.135.55	HTTP	743	GET /Portals/0/2020/Thang9/hoc5.jpg HTTP/1.1
416	14.166601	192.168.0.100	203.113.135.55	HTTP	743	GET /Portals/0/2020/Thang9/hoc1.jpg HTTP/1.1

▶ Frame 234: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
 ▶ Ethernet II, Src: Tp-LinkT_e1:31:d2 (34:e8:94:e1:31:d2), Dst: Azurewav_8f:3b:b1 (28:c2:dd:8f:3b:b1)
 ▶ Internet Protocol Version 4, Src: 203.113.135.55, Dst: 192.168.0.100
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49891, Seq: 2762, Ack: 706, Len: 74
 ▶ [3 Reassembled TCP Segments (2834 bytes): #232(1380), #233(1380), #234(74)]
 ▶ **Hypertext Transfer Protocol**
 ▶ JavaScript Object Notation: application/json

```

0000  28 c2 dd 8f 3b b1 34 e8 94 e1 31 d2 08 00 45 00  ( ...; 4...1...E
0010  00 72 86 ef 40 00 78 06 67 e1 cb 71 87 37 c0 a8  r...@x g...q.7
0020  00 64 00 50 c2 e3 66 18 e5 3d 60 45 5c 97 50 18  d.P...f...=E\P
0030  03 fd bc f7 00 00 65 4c 69 6e 6b 22 3a 66 61 6c  ....eL ink":fal
0040  73 65 2c 22 53 74 61 74 75 73 22 3a 31 2c 22 49  se,"Stat us":1,"I
0050  73 48 6f 6d 65 56 69 65 77 22 3a 6e 75 6c 6c 2c  sHomeVie w":null,
0060  22 49 73 52 6f 6f 74 22 3a 6e 75 6c 6c 2c 22 49  "IsRoot" :null,"I
0070  73 44 65 6c 65 74 65 64 22 3a 66 61 6c 73 65 7d  sDeleted ":false}
  
```

Truyền tập tin: FTP

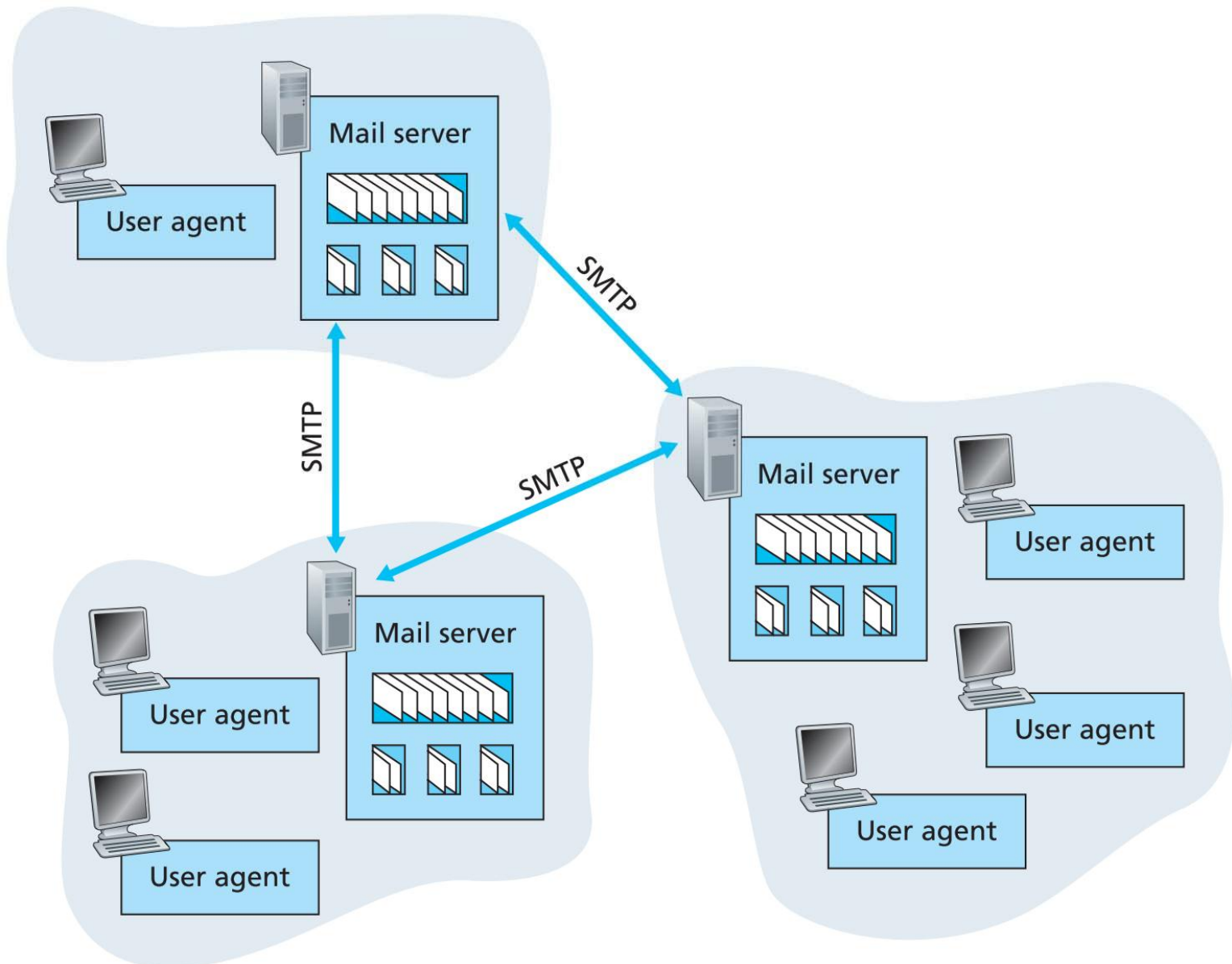


Truyền tập tin: FTP



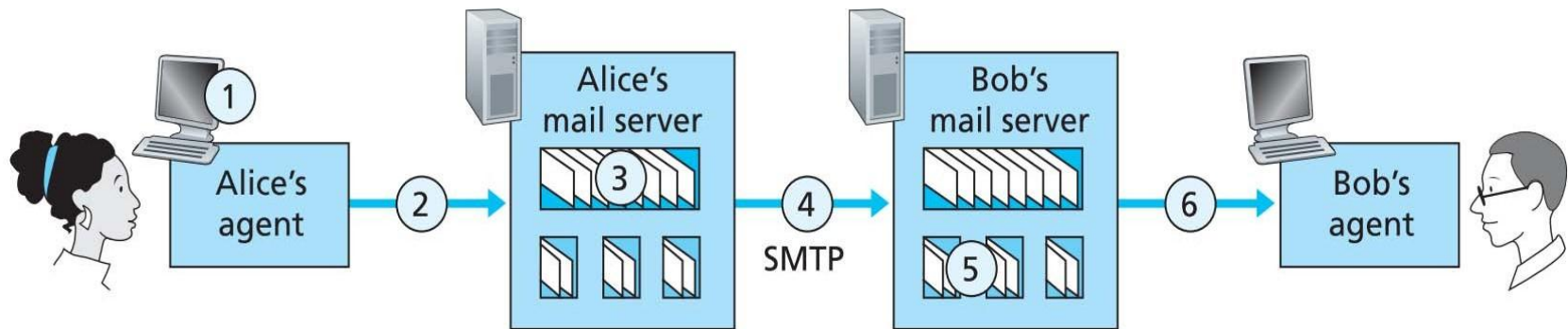
- ❖ Kết nối điều khiển (control connection): dùng riêng
 - ❖ HTTP connection: dùng chung
- ❖ FTP server duy trì trạng thái: thư mục hiện tại, xác thực
 - ❖ HTTP không duy trì trạng thái

GIAO THỨC: SMTP

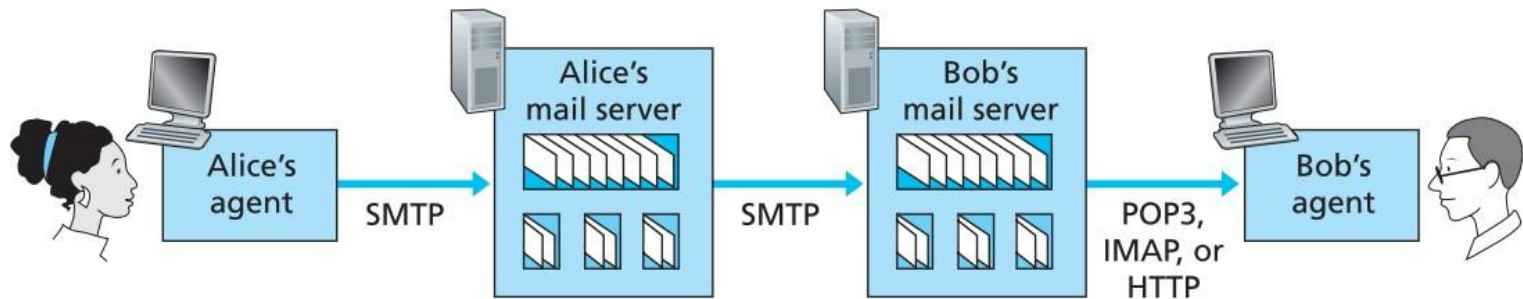


GIAO THỨC: SMTP

- ❖ RFC 2821
- ❖ Sử dụng TCP để truyền tin cậy bản tin email từ client tới server, cổng 25
- ❖ Gửi trực tiếp: server gửi tới server nhận
- ❖ Giao tiếp kiểu command/response (giống HTTP, FTP)
 - ❖ Commands: ASCII text
 - ❖ Response: mã trạng thái (status code) và thông điệp (phrase)
- ❖ Bản tin phải là 7-bit ASCII

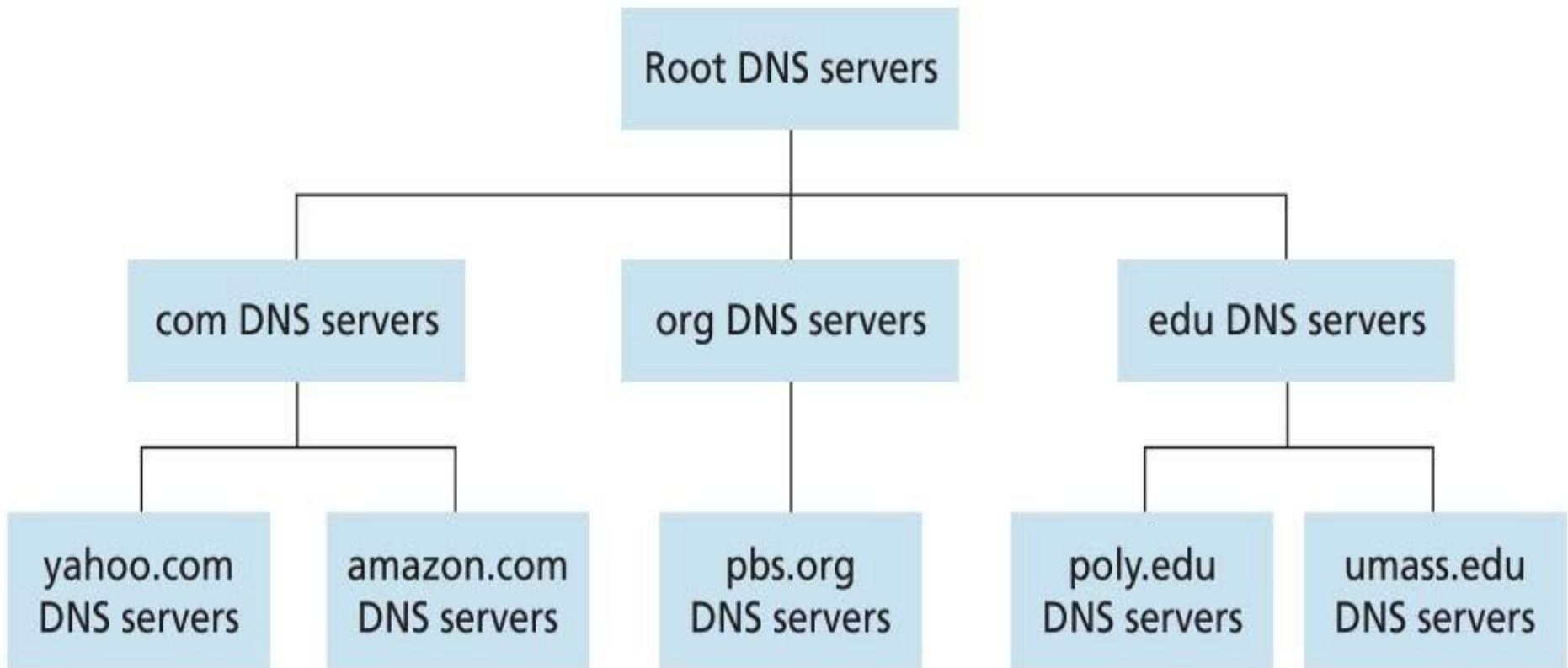


Giao thức truy cập thư điện tử



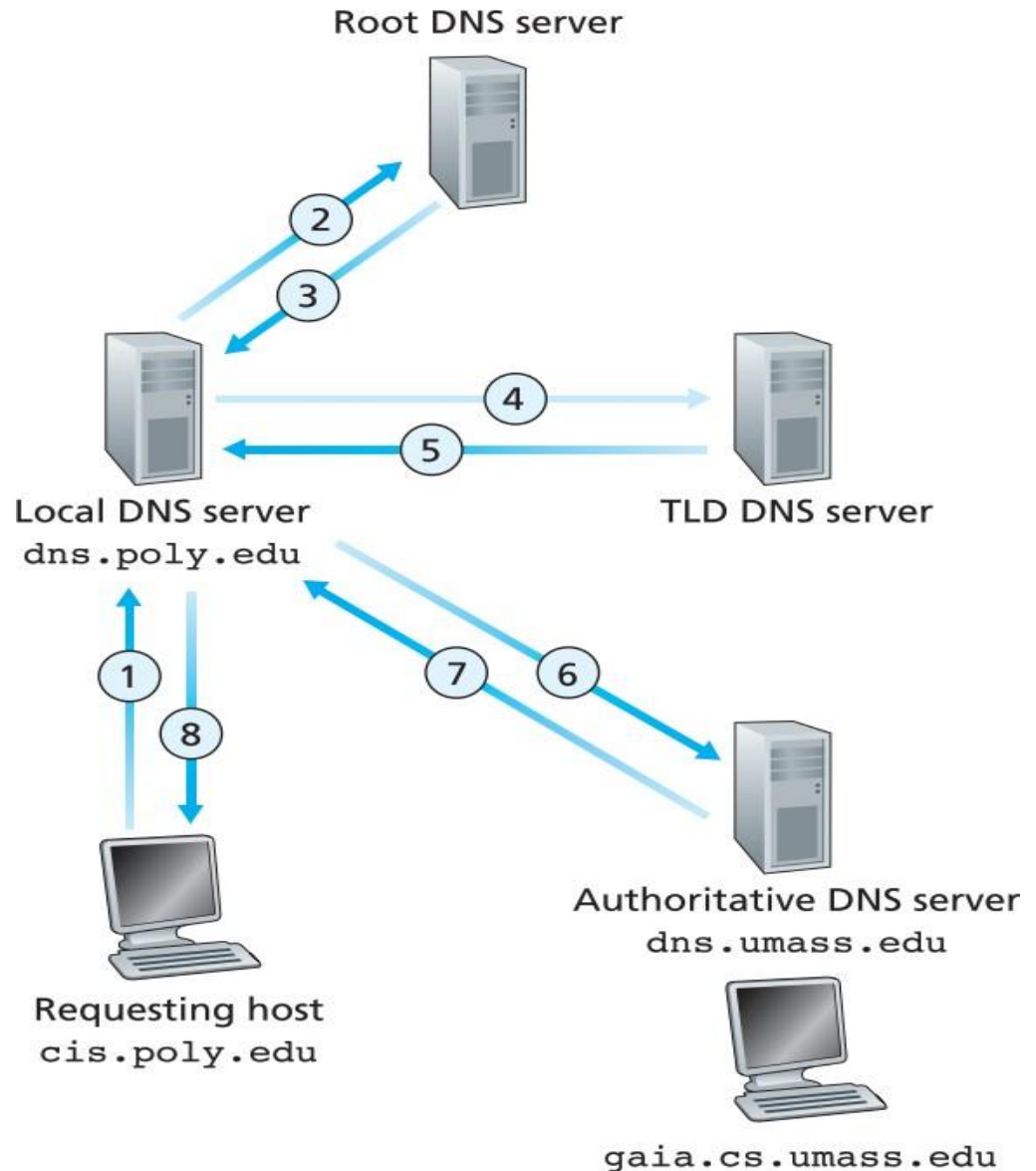
- ❖ **SMTP**: chuyển email tới server của người nhận
- ❖ Giao thức truy cập thư điện tử (mail access protocol): lấy email từ server
 - ❖ **POP**: Post Office Protocol [RFC 1939]: xác thực, tải về
 - ❖ **IMAP**: Internet Mail Access Protocol [RFC 1730]: có nhiều thao tác hơn, ví dụ thao tác với email trên server
 - ❖ **HTTP**: gmail, Hotmail, Yahoo! Mail,...

DỊCH VỤ DNS



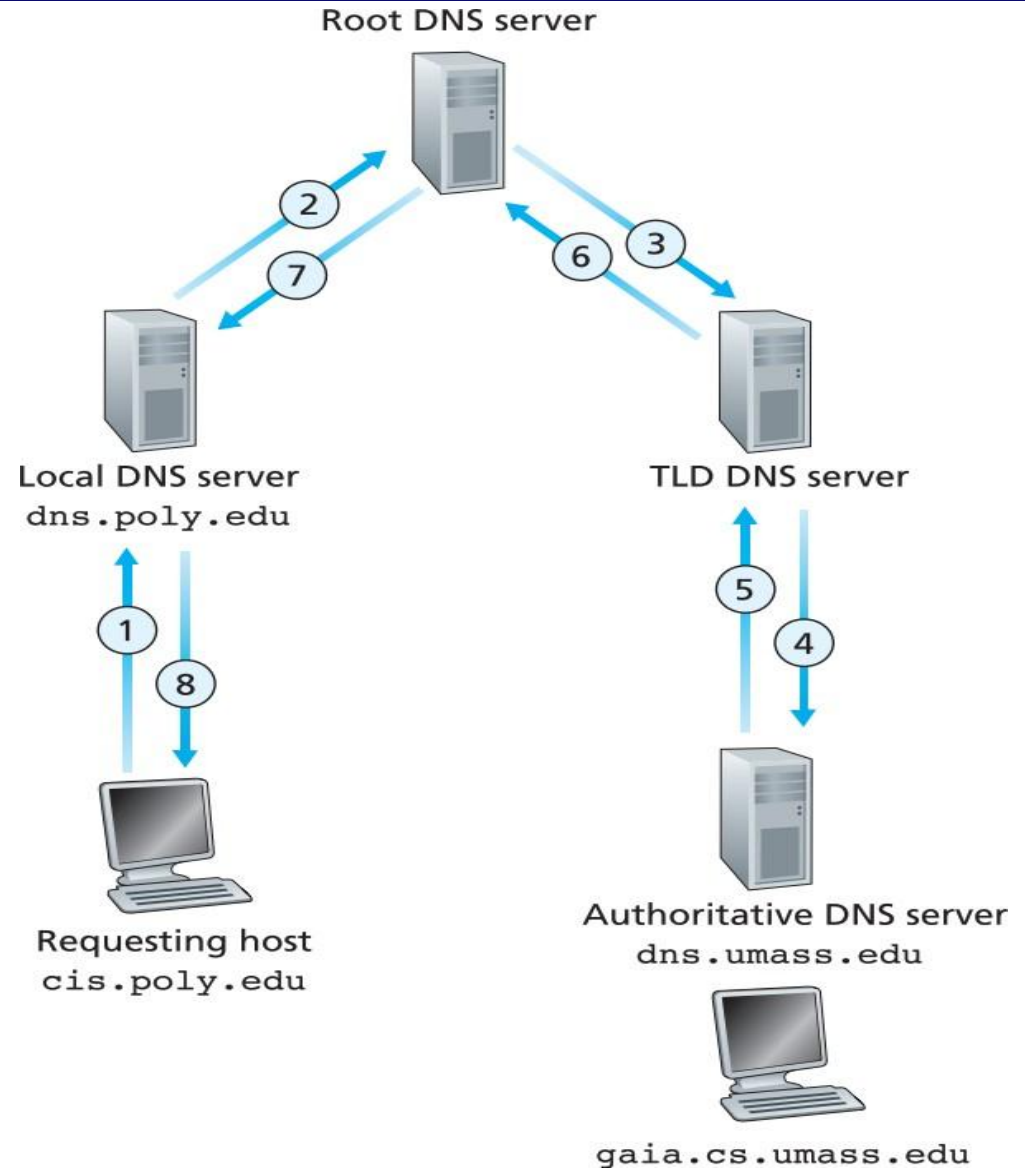
Giao tiếp giữa DNS server

- ❑ Yêu cầu lặp (iterated query): 2-3, 4-5, 6-7



Giao tiếp giữa DNS server

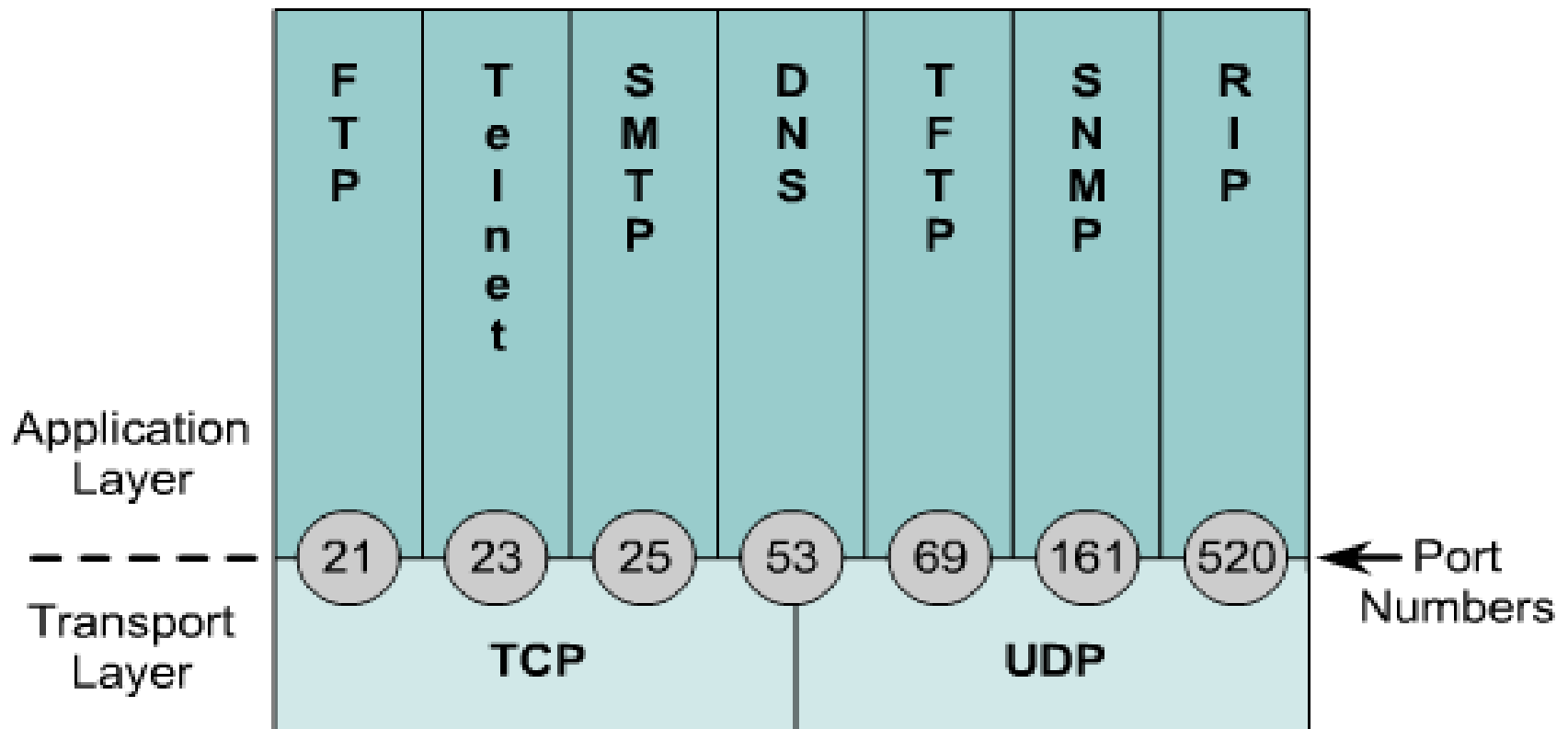
- ❑ Yêu cầu đệ quy (Recursive queries)



Hoạt động của DNS

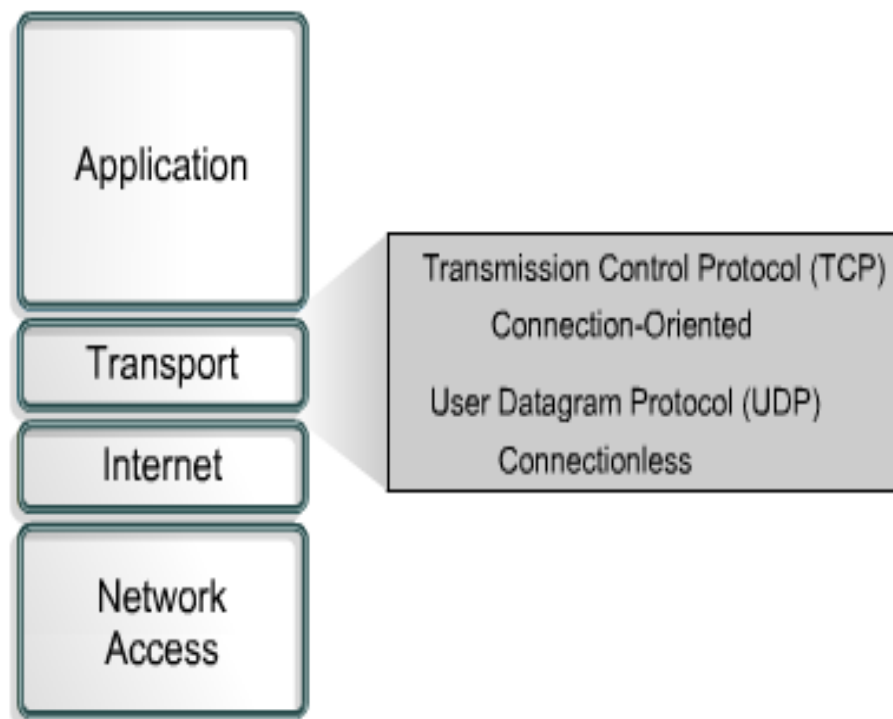
- ❖ Khi name server nhận biết được mapping, name server sẽ lưu (*cache*) mapping
 - ❖ Thông tin lưu trong cache entry, và bị xóa sau một khoảng thời gian (TTL)
 - ❖ TLD server thường được lưu trong các local name server
 - ❖ Vì vậy root name server sẽ không thường xuyên được truy vấn
- ❖ Các cached entry có thể không được cập nhật
 - ❖ Nếu host name thay đổi địa chỉ IP của nó, địa chỉ IP này có thể không được cập nhật tới khi TTL quá hạn
- ❖ Cơ chế cập nhật: RFC 2136

CÁC CÔNG PHỐ BIẾN DÙNG CHO CÁC GIAO THỨC LỚP ỨNG DỤNG



LỚP VẬN CHUYỂN

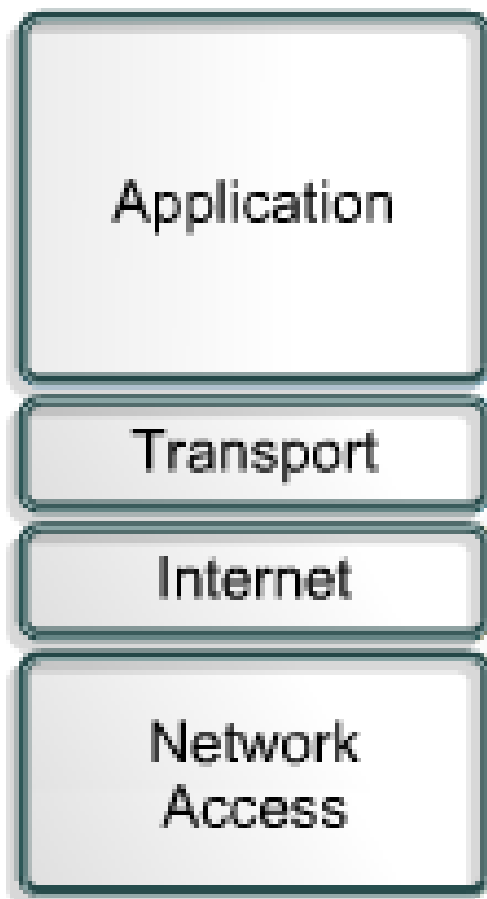
- ❖ Thực hiện chức năng đảm bảo việc vận chuyển dữ liệu từ host nguồn đến host đích.
- ❖ Thiết lập một cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận.



- ❖ TCP: Truyền tin cậy, chuyển đảm bảo thứ tự điều khiển tắc nghẽn, điều khiển luồng, thiết lập kết nối.
- ❖ UDP: Truyền không tin cậy, chuyển không đảm bảo thứ tự: các dịch vụ không cung cấp: đảm bảo độ trễ, đảm bảo băng thông

LỚP INTERNET

Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích, liên quan đến địa chỉ IP. Thiết bị hoạt động ở lớp này là Router



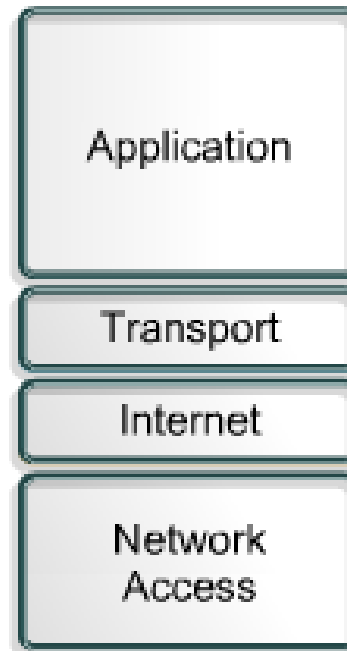
Internet Protocol (IP)
Internet Control Message Protocol (ICMP)
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)

LỚP INTERNET

- ❖ IP: không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích.
- ❖ ICMP (Internet Control Message Protocol): đem đến khả năng điều khiển và chuyển thông điệp trong lớp Internet.
- ❖ ARP (Address Resolution Protocol): xác định địa chỉ lớp liên kết số liệu (MAC address) khi đã biết trước địa chỉ IP.
- ❖ RARP (Reverse Address Resolution Protocol): xác định các địa chỉ IP khi biết trước địa chỉ MAC.

LỚP TRUY NHẬP MẠNG

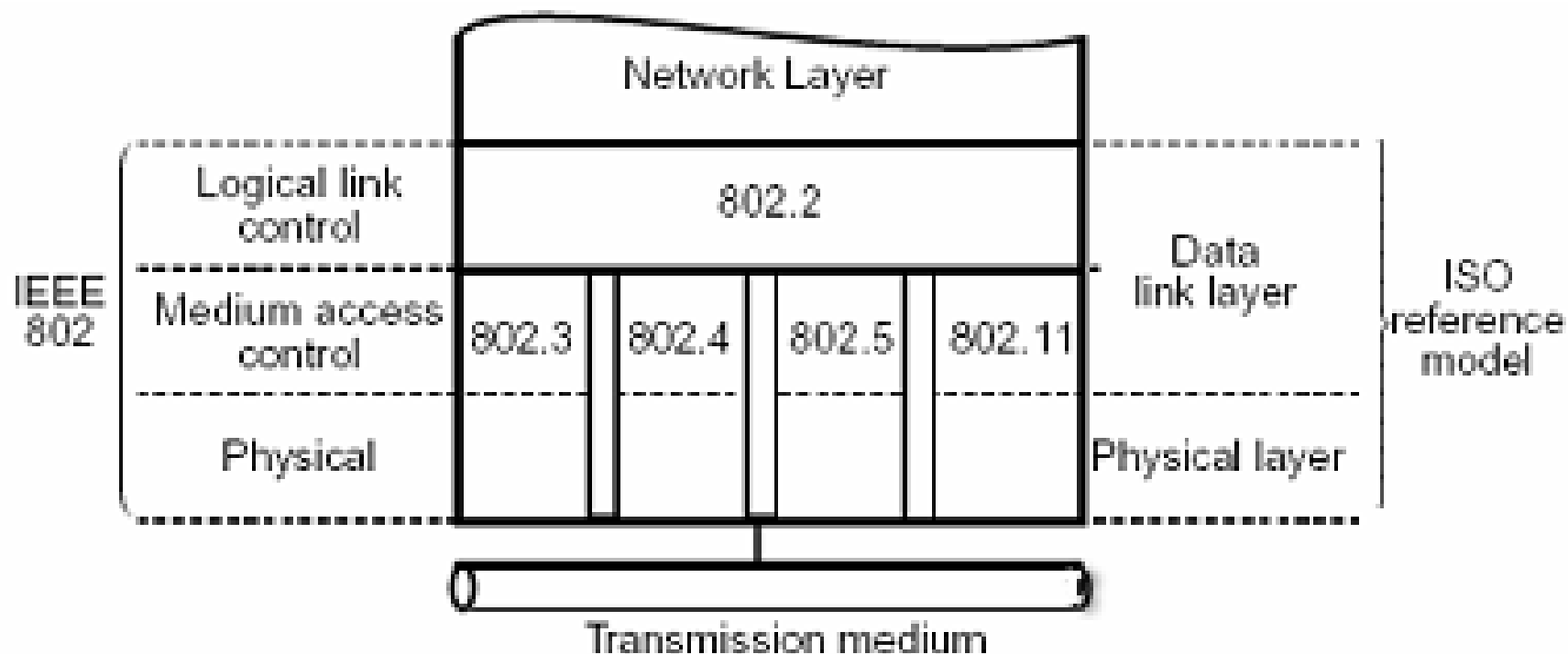
Định ra các thủ tục để giao tiếp với phần cứng mạng và truy nhập môi trường truyền. Có nhiều giao thức hoạt động tại lớp này.



- Ethernet
- Fast Ethernet
- SLIP & PPP
- FDDI
- ATM, Frame Relay & SMDS
- ARP
- Proxy ARP
- RARP

Thiết bị hoạt động ở lớp này là HUB, SWITCH

GIAO THỨC LỚP TRUY NHẬP MẠNG



802.2 = Logical link control protocol

802.3 = CSMA/CD

802.4 = Token bus

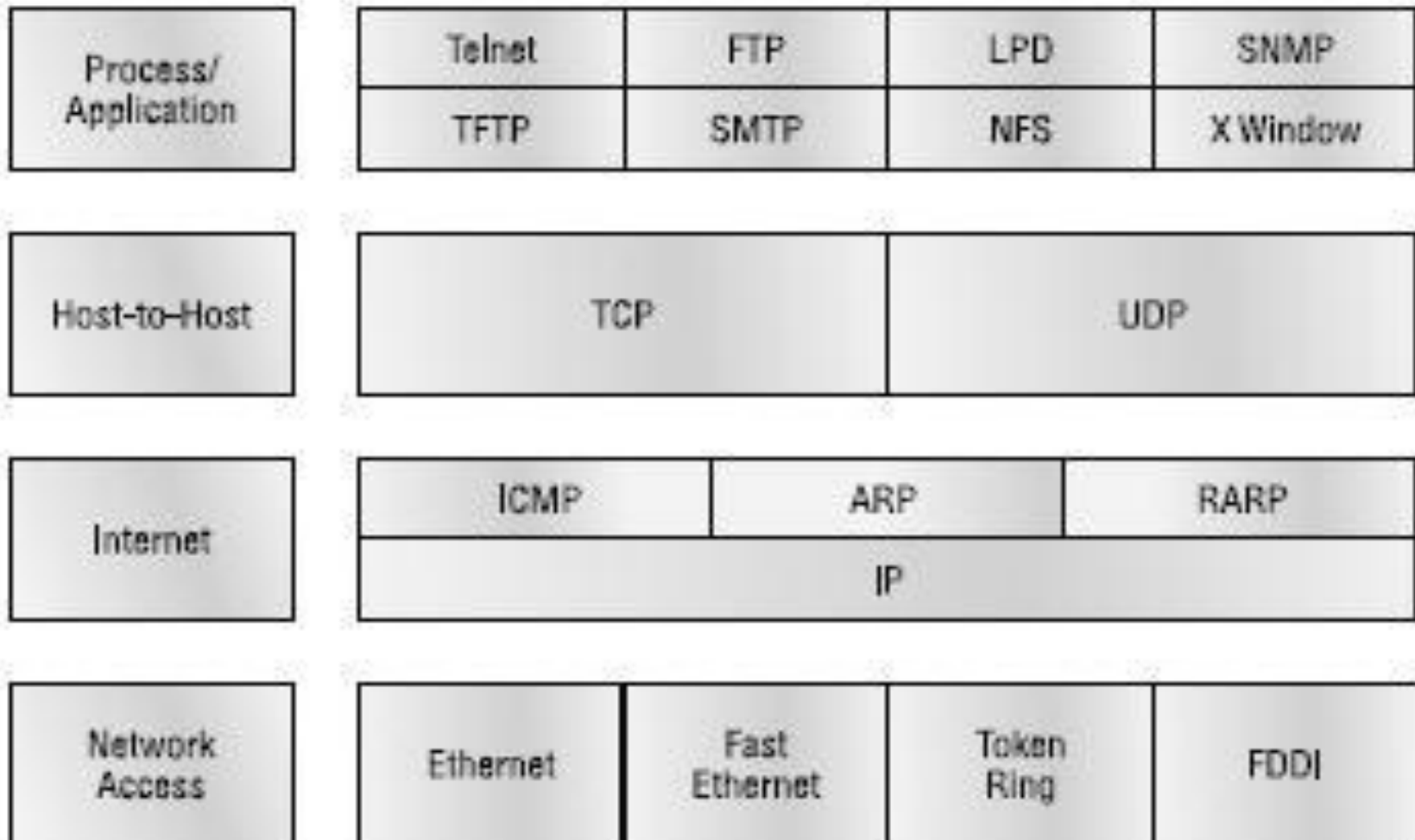
802.5 = Token ring

802.11 = Wireless

Medium access control protocols

CÁC GIAO THỨC TRONG MÔ HÌNH TCP/IP

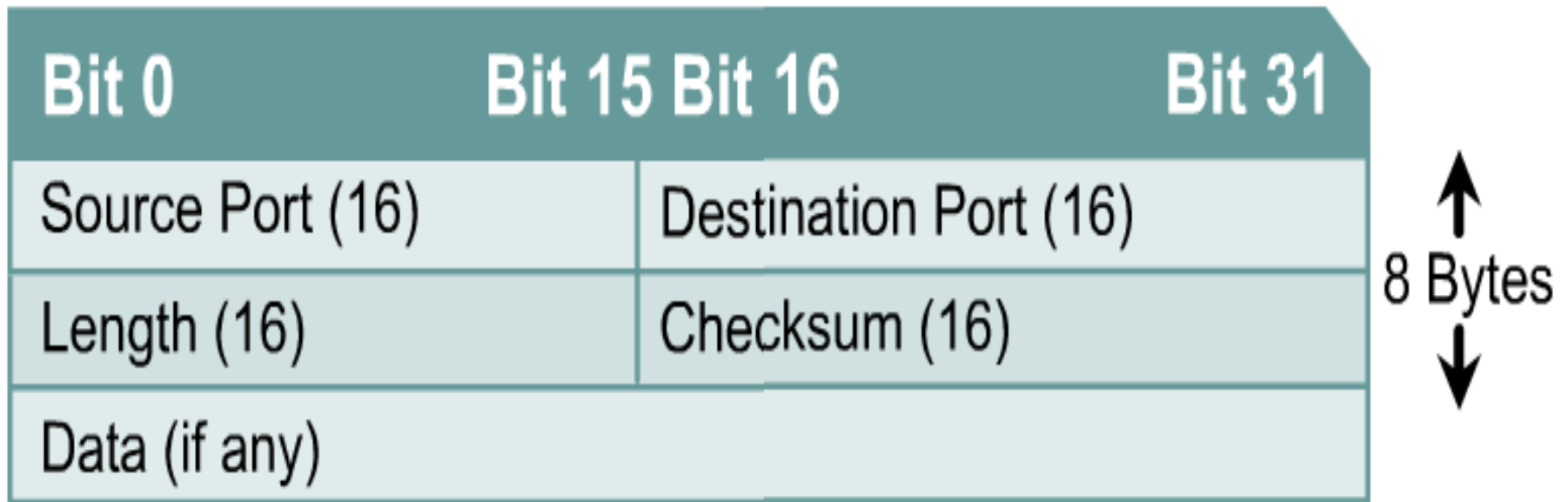
DoD Model



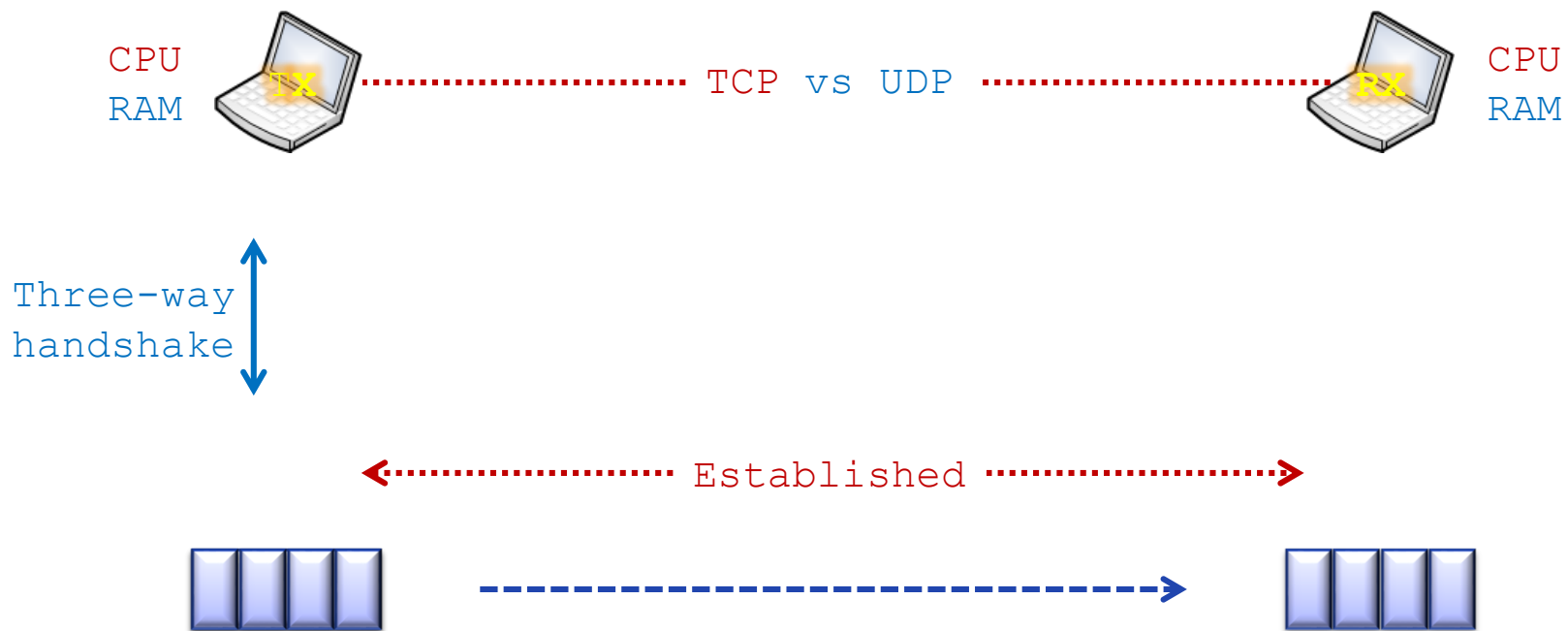
II. GIAO THỨC TCP/UDP

- ❖ **Giao thức gói tin người sử dụng UDP** (User Datagram Protocol) UDP là giao thức không liên kết (Connectionless).
- ❖ UDP 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 dữ liệu đến đích và theo đúng thứ tự và không thực hiện loại bỏ các gói tin trùng lặp.
- ❖ UDP thường sử dụng kết hợp với các giao thức khác, phù hợp cho các ứng dụng yêu cầu xử lý nhanh như các giao thức SNMP và VoIP.

Khuôn dạng gói tin UDPv4



GIAO THỨC UDP

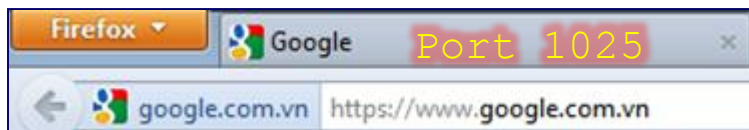


S.Port vs D.Port



Segment	S.Port 1025	D.Port 443
Segment	S.Port 443	D.Port 1025

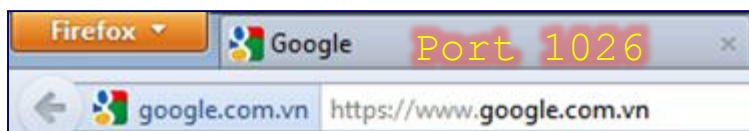
Segment	S.Port 1025	D.Port 443
Segment	S.Port 443	D.Port 1025



Established →

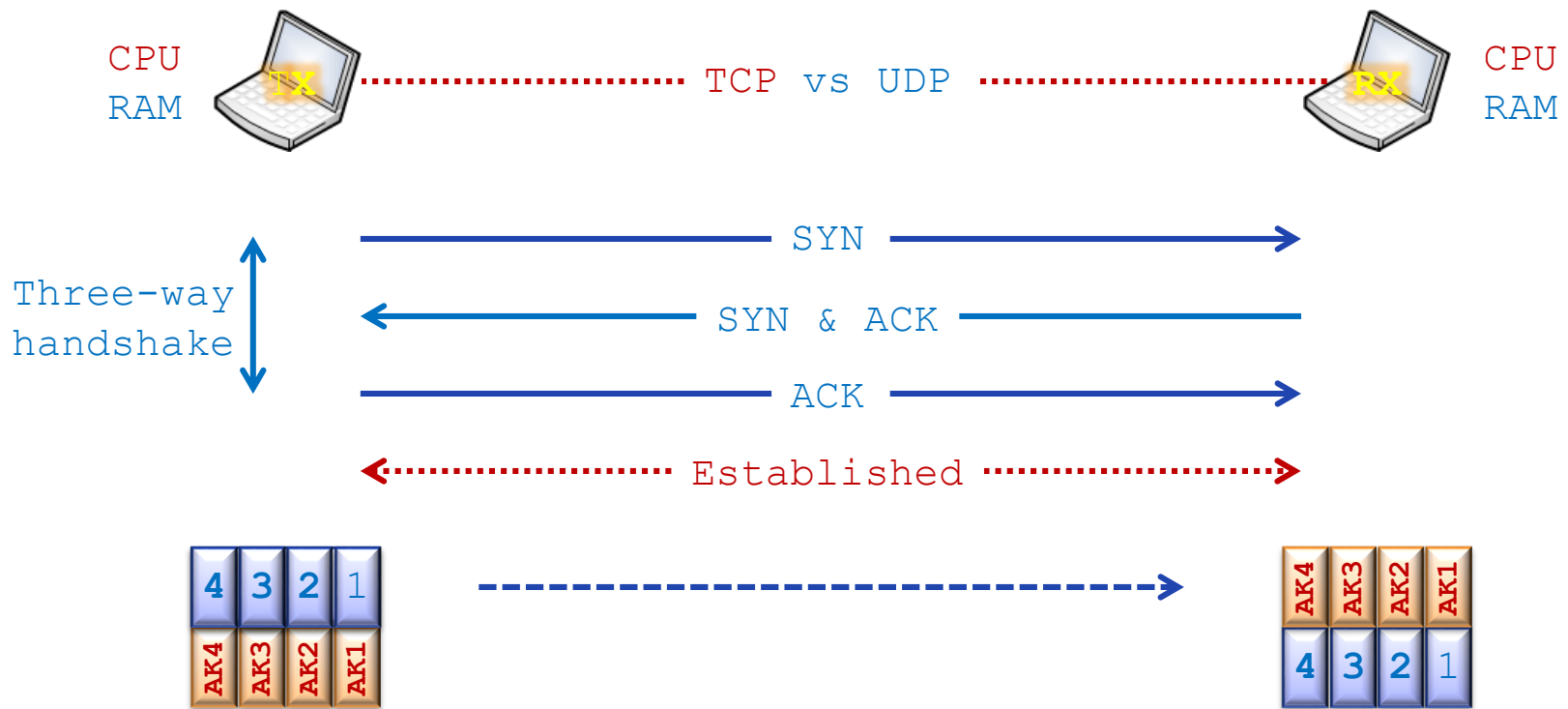
← Port 1025

Established →

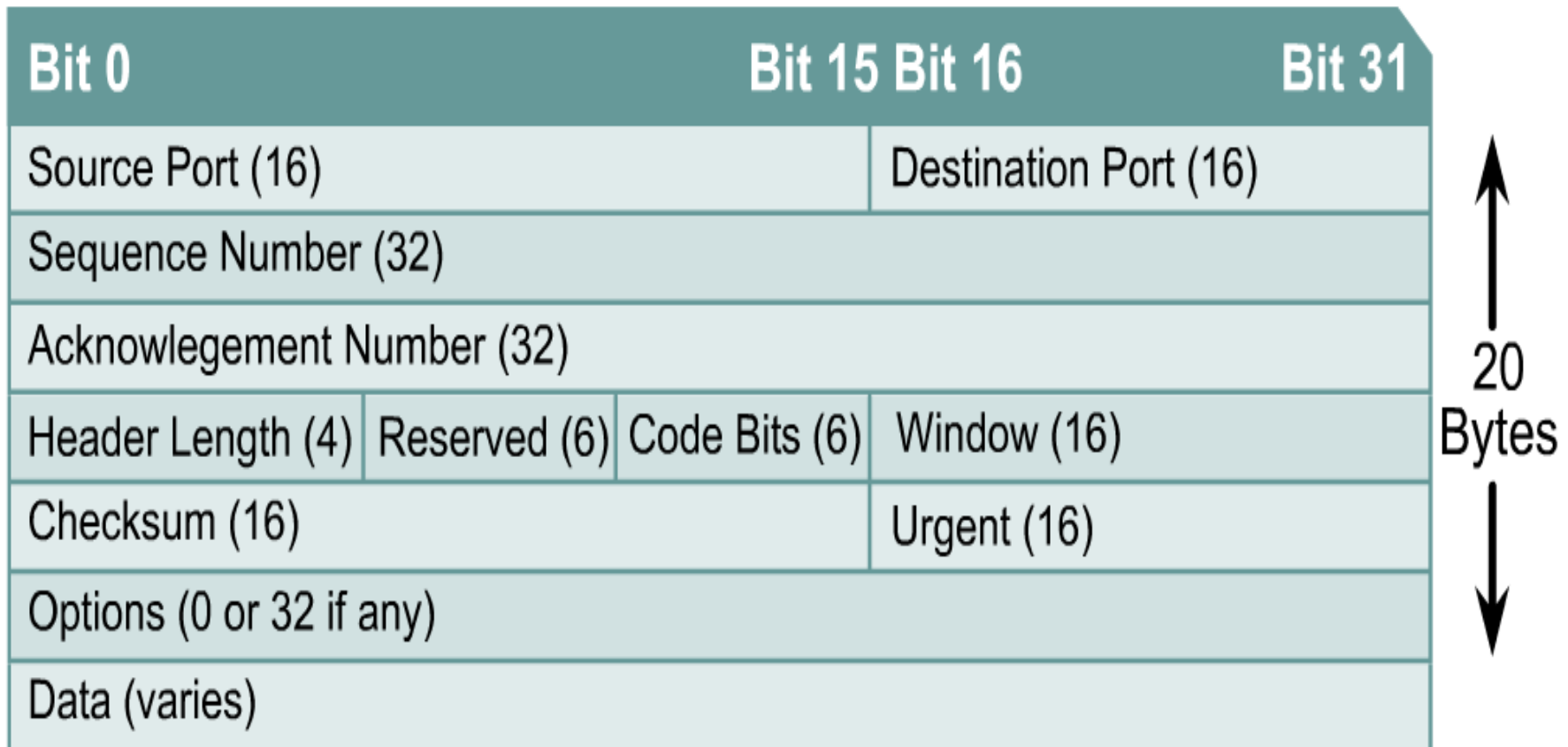


- ❖ Giao thức điều khiển truyền TCP (Transmission Control Protocol) là một giao thức hướng liên kết (Connection Oriented)
- ❖ TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các thành trong liên mạng.
- ❖ Cung cấp các chức năng kiểm tra tính chính xác của dữ liệu khi đến đích và truyền lại dữ liệu khi có lỗi xảy ra.
- ❖ Trước khi thực hiện truyền dẫn 2 bên thu và phát thương lượng để thiết lập một kết nối logic tạm thời, tồn tại trong quá trình truyền số liệu.

GIAO THỨC TCP



Cấu trúc gói tin TCPv4



CHỨC NĂNG CÁC TRƯỜNG TRONG TCP

- ❖ Cổng nguồn (Source Port): 16 bit, số hiệu cổng nguồn.
- ❖ Cổng đích (Destination Port): Độ dài 16 bit, chứa số hiệu cổng đích.
- ❖ Sequence Number: 32 bits, số thứ tự của gói số liệu khi phát.
- ❖ Acknowledgment Number (32 bits), Bên thu xác nhận thu được dữ liệu đúng.
- ❖ Header length (4 bits): Độ dài Header gói tin TCP.
- ❖ Reserved (6 bit) lưu lại: Lấp đầy bằng 0 để dành cho tương lai.
- ❖ Code bits: Các bits điều khiển

CHỨC NĂNG CÁC TRƯỜNG TRONG TCP

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

Quan sát giao thức TCP - UDP

1. Chạy phần mềm Wireshark để ghi lại dữ liệu gửi nhận (Chọn Capture -> Start)
2. Mở trình duyệt vào trang web: tlu.edu.vn
3. Dừng việc ghi dữ liệu của phần mềm Wireshark
4. Gõ Filter: `tcp.port == 80` và `udp.port == 80`
5. Quan sát các gói tin TCP và UDP

CHƯƠNG 3: GIAO THỨC TCP/IP

1

- Mô hình TCP/IP

2

- Giao thức TCP/UDP

3

- Giao thức IP

4

- Giao thức ICMP

5

- Giao thức ARP/RARP

6

- Giao thức IPv6

7

- Kỹ thuật định tuyến

III. GIAO THỨC IP

- ❖ IP (Internet Protocol) là giao thức không liên kết.
- ❖ Chức năng của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram.
- ❖ Để thực hiện được giao thức IP thực hiện tiến trình định địa chỉ và chọn đường từ nguồn tới đích (định tuyến).
- ❖ Giao thức IP có 2 version là IP version 4 (IPv4) và IP version 6 (IPv6)

Cấu trúc gói tin IPv4

VER	IHL	Type of services	Total lenght	
Identification			Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source address				
Destination address				
Options + Padding				
Data				

CHỨC NĂNG CÁC TRƯỜNG

- ❖ VER (4 bits): Version hiện hành của IP được cài đặt.
- ❖ IHL(4 bits): Internet Header Length của Datagram, tính theo đơn vị word (32 bits).
- ❖ Type of service (8 bits): Thông tin về loại dịch vụ và mức ưu tiên của gói IP:
- ❖ Total Length (16 bits): Chỉ độ dài Datagram,
- ❖ Identification (16bits): Định danh cho một Datagram trong thời gian sống của nó.
- ❖ Flags (3 bits): Liên quan đến sự phân đoạn (Fragment) các Datagram.
- ❖ Fragment Offset (13 bits): Chỉ vị trí của Fragment trong Datagram.

CHỨC NĂNG CÁC TRƯỜNG

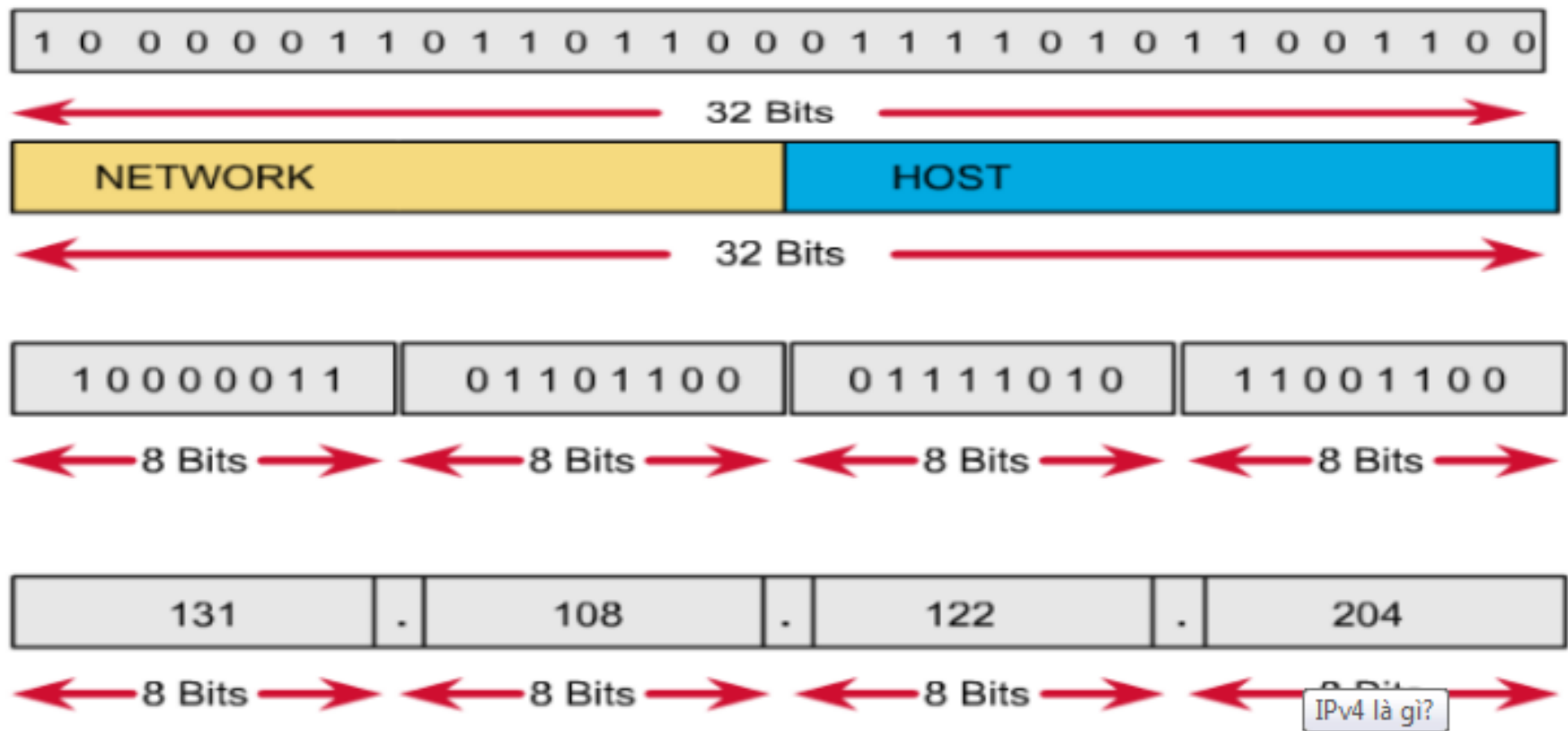
- ❖ Time To Live (TTL-8 bits): Thời gian sống của một gói dữ liệu.
- ❖ Protocol (8 bits): Chỉ giao thức sử dụng TCP hay UDP.
- ❖ Header Checksum (16 bits): Mã kiểm soát lỗi CRC (Cycle Redundancy Check).
- ❖ Source Address (32 bits): địa chỉ của trạm nguồn.
- ❖ Destination Address (32 bits): Địa chỉ của 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.

ĐỊA CHỈ IPv4

- ❖ Địa chỉ IP: Mỗi một trạm (Host) được gán một địa chỉ duy nhất gọi là địa chỉ IP.
- ❖ Mỗi địa chỉ IPV4 có độ dài 32 bit được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu diễn dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân.
- ❖ Cách viết phổ biến nhất là dưới dạng thập phân có dấu chấm để tách giữa các vùng.
- ❖ Địa chỉ IP được chia thành 5 lớp ký hiệu là A, B, C, D, E với cấu trúc mỗi lớp được xác định. Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0-lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D, 11110 - lớp E).

Địa chỉ IPv4 và các lớp địa chỉ

Địa chỉ IPv4 có độ dài 32 bit chia thành 4 octet chia thành 2 phần là network_id và host_id.



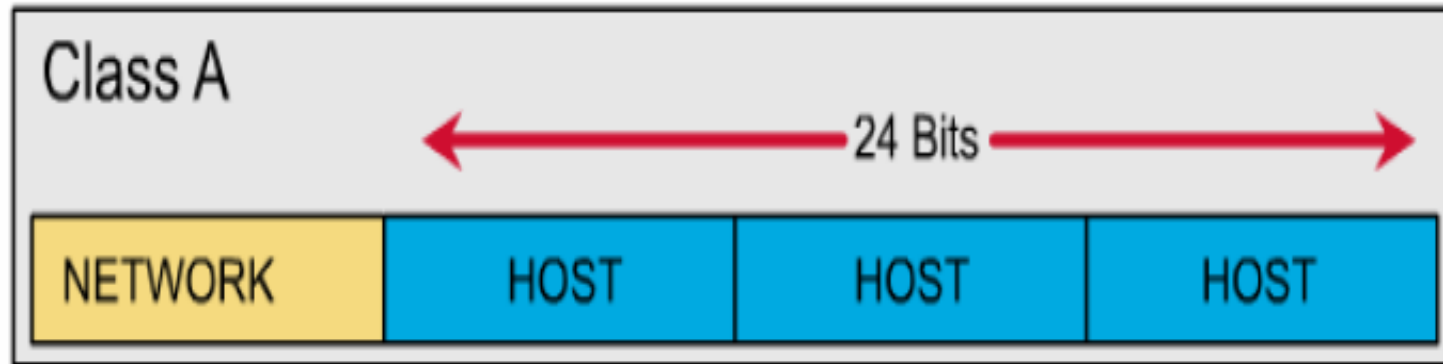
Cấu trúc địa chỉ IPv4

Các lớp địa chỉ IPv4

- Không gian địa chỉ IPv4 được chia thành 5 lớp (class) A, B, C, D và E.
- Các lớp A, B và C được triển khai để đặt cho các host trên mạng Internet.
- Lớp D dùng cho các nhóm multicast, còn lớp E phục vụ cho mục đích nghiên cứu.

Lớp A (Class A)

Dành 1 byte cho phần network_id và 3 byte cho phần host_id.



Class A:



Lớp A (Class A)

- ❖ Bit đầu tiên của byte đầu tiên phải là bit 0. Dạng nhị phân của octet này là 0xxxxxxx
- ❖ Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 (=00000000₍₂₎) đến 127 (=01111111₍₂₎) sẽ thuộc lớp A.
- ❖ Ví dụ: 50.14.32.8.

Lớp A (Class A)

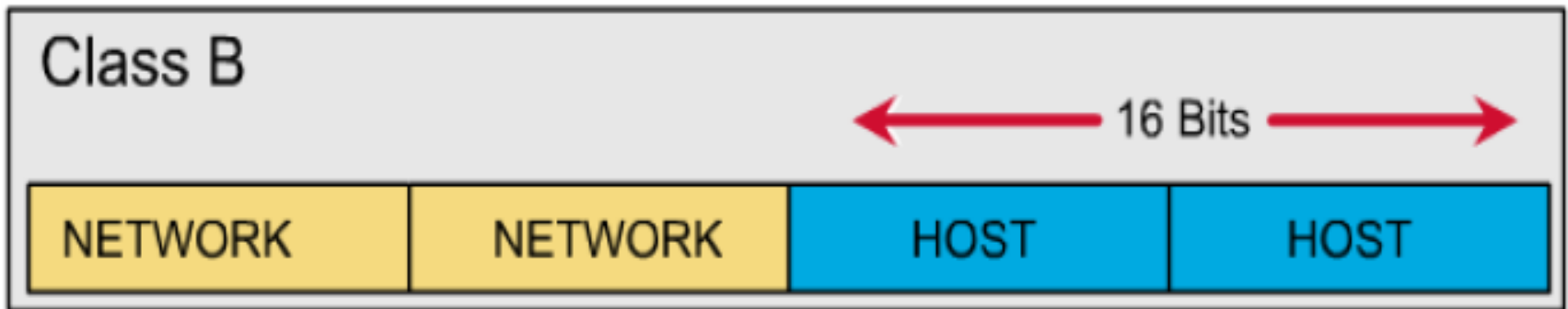
- ❖ Byte đầu tiên này cũng chính là `network_id`, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại 7 bit để đánh thứ tự các mạng, ta được $128 (=2^7)$ mạng lớp A khác nhau.
- ❖ Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.

Lớp A (Class A)

- ❖ Phần host_id chiếm 24 bit, nghĩa là có $2^{24} = 16.777.216$ host khác nhau trong mỗi mạng. Bỏ đi hai trường hợp đặc biệt (phần host_id chứa toàn các bit 0 và bit 1). Còn lại: 16.777.214 host.
- ❖ Ví dụ đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.

Lớp B (Class B)

Dành 2 byte cho phần network_id và 2 byte cho phần host_id.



Class B:



Lớp B (Class B)

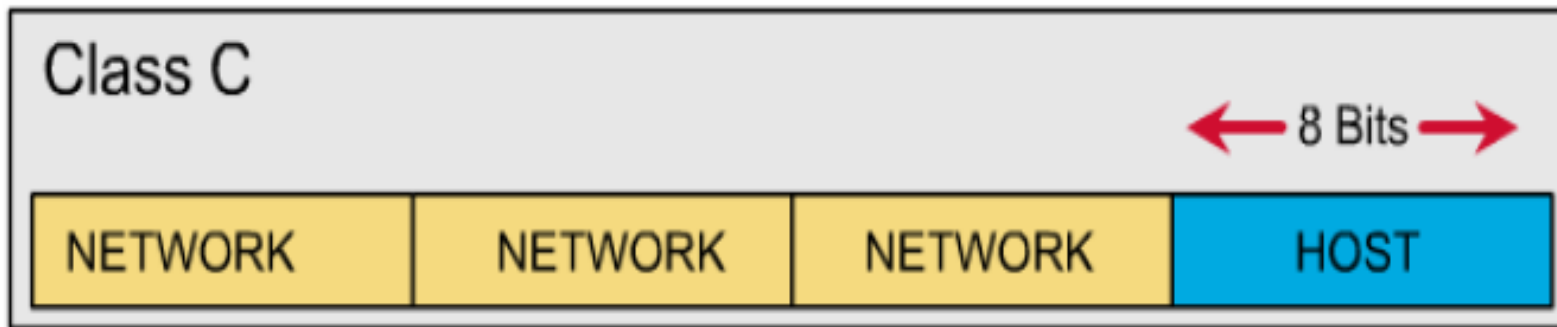
- ❖ Hai bit đầu tiên của byte đầu tiên phải là 10. Dạng nhị phân của octet này là 10xxxxxx
- ❖ Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 128 ($=10000000_{(2)}$) đến 191 ($=10111111_{(2)}$) sẽ thuộc về lớp B
- ❖ Ví dụ: 172.29.10.1.

Lớp B (Class B)

- ❖ Phần network_id chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự $16.384 (=2^{14})$ mạng khác nhau (128.0.0.0 đến 191.255.0.0).
- ❖ Phần host_id dài 16 bit hay có 65.536 ($=2^{16}$) giá trị khác nhau. Trừ đi 2 trường hợp đặc biệt còn lại 65.534 host trong một mạng lớp B.
- ❖ Ví dụ đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.

Lớp C (Class C)

Dành 3 byte cho phần `network_id` và 1 byte cho phần `host_id`.



Class C:



Lớp C (Class C)

- ❖ Ba bit đầu tiên của byte đầu tiên phải là 110. Dạng nhị phân của octet này là 110xxxxx
- ❖ Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 192 (=11000000₍₂₎) đến 223 (=11011111₍₂₎) sẽ thuộc về lớp C.
- ❖ Ví dụ: 203.162.41.235

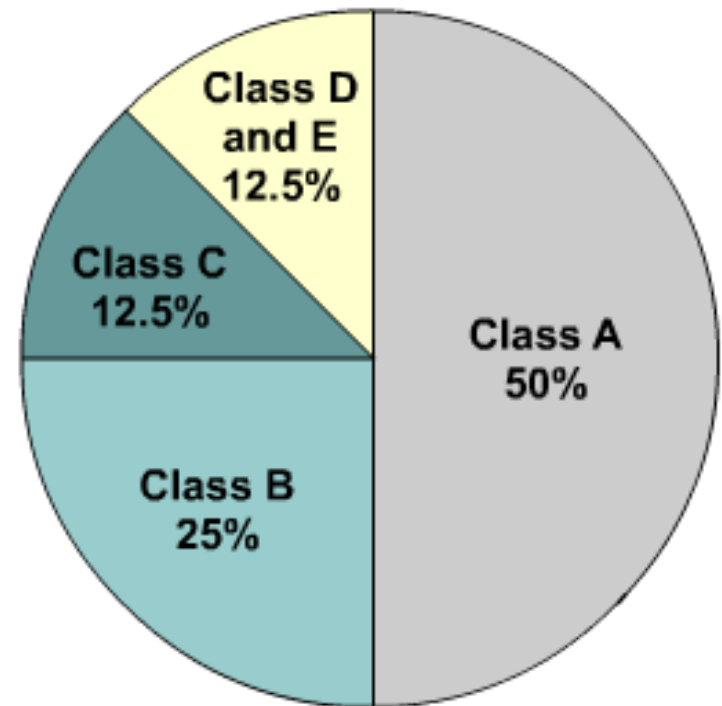
Các lớp địa chỉ IP

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

Các lớp địa chỉ IP

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)



Địa chỉ dành riêng

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Địa chỉ nào sử dụng trong mạng nội bộ

❖ 150.100.255.255

❖ 172.19.255.18

❖ 195.234.253.0

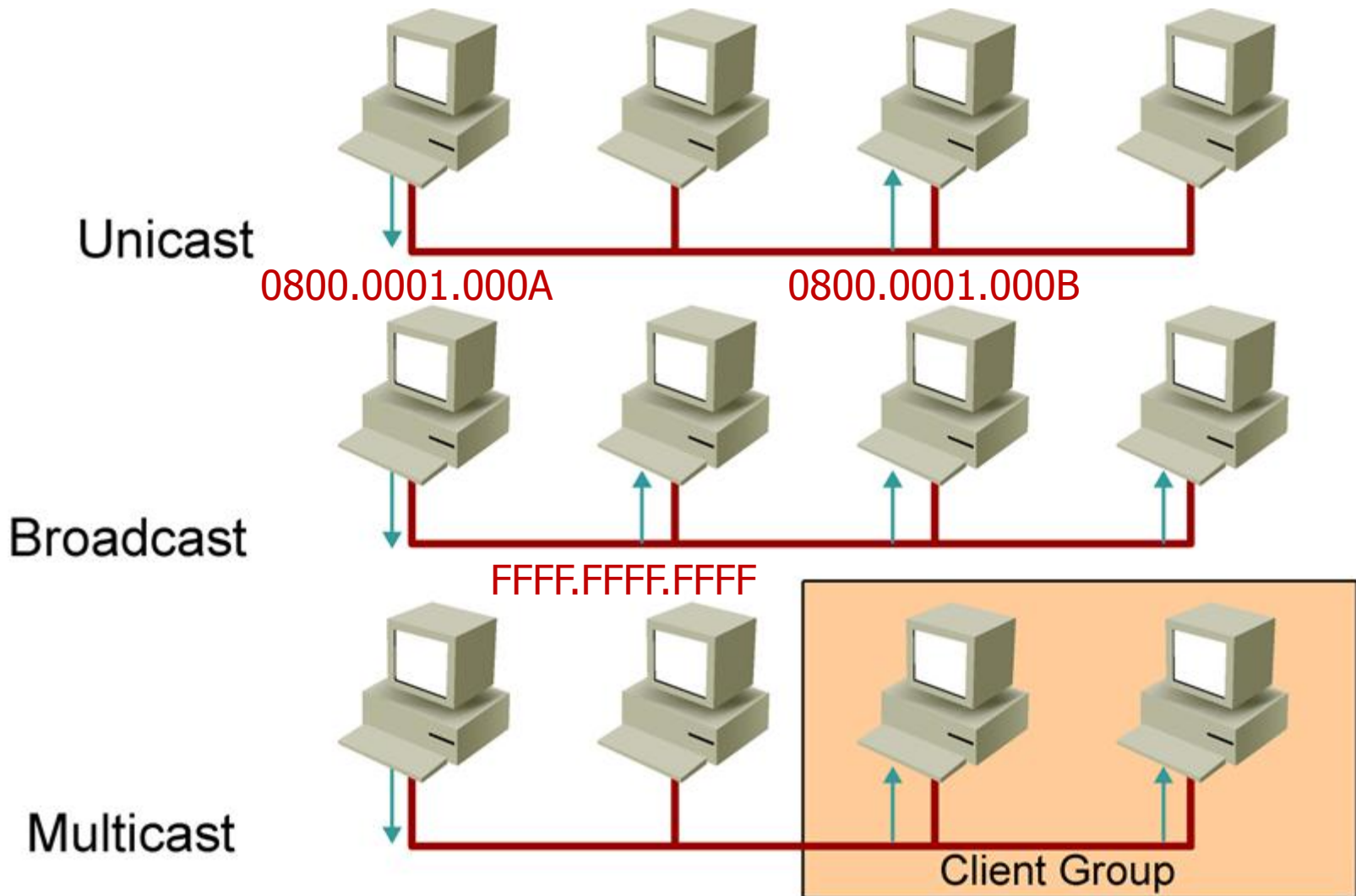
❖ 10.10.110.23

❖ 192.168.221.176

❖ 127.34.25.189

❖ 203.162.217.73

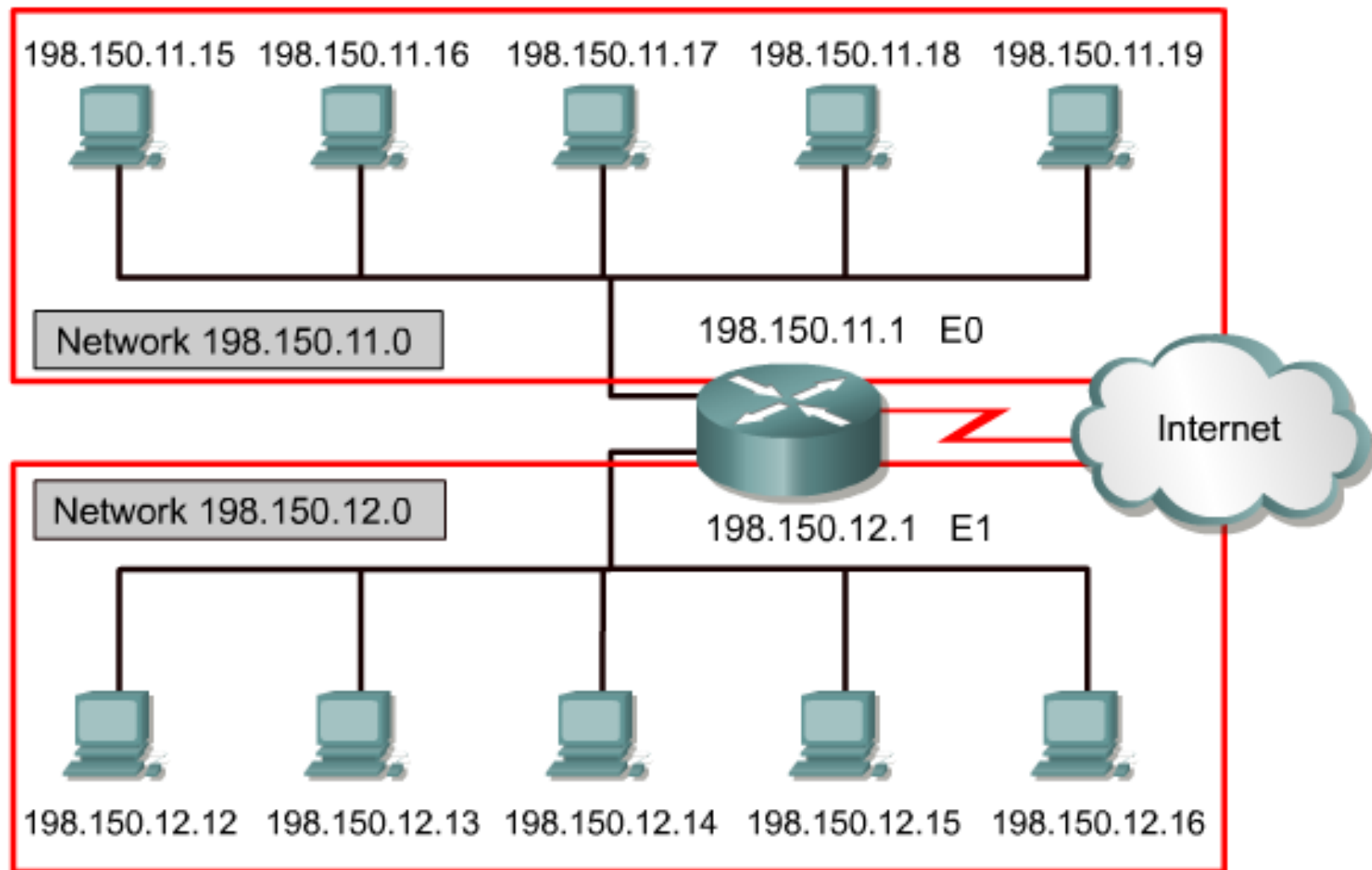
Phân loại địa chỉ IPv4



Địa chỉ mạng, địa chỉ Broadcast

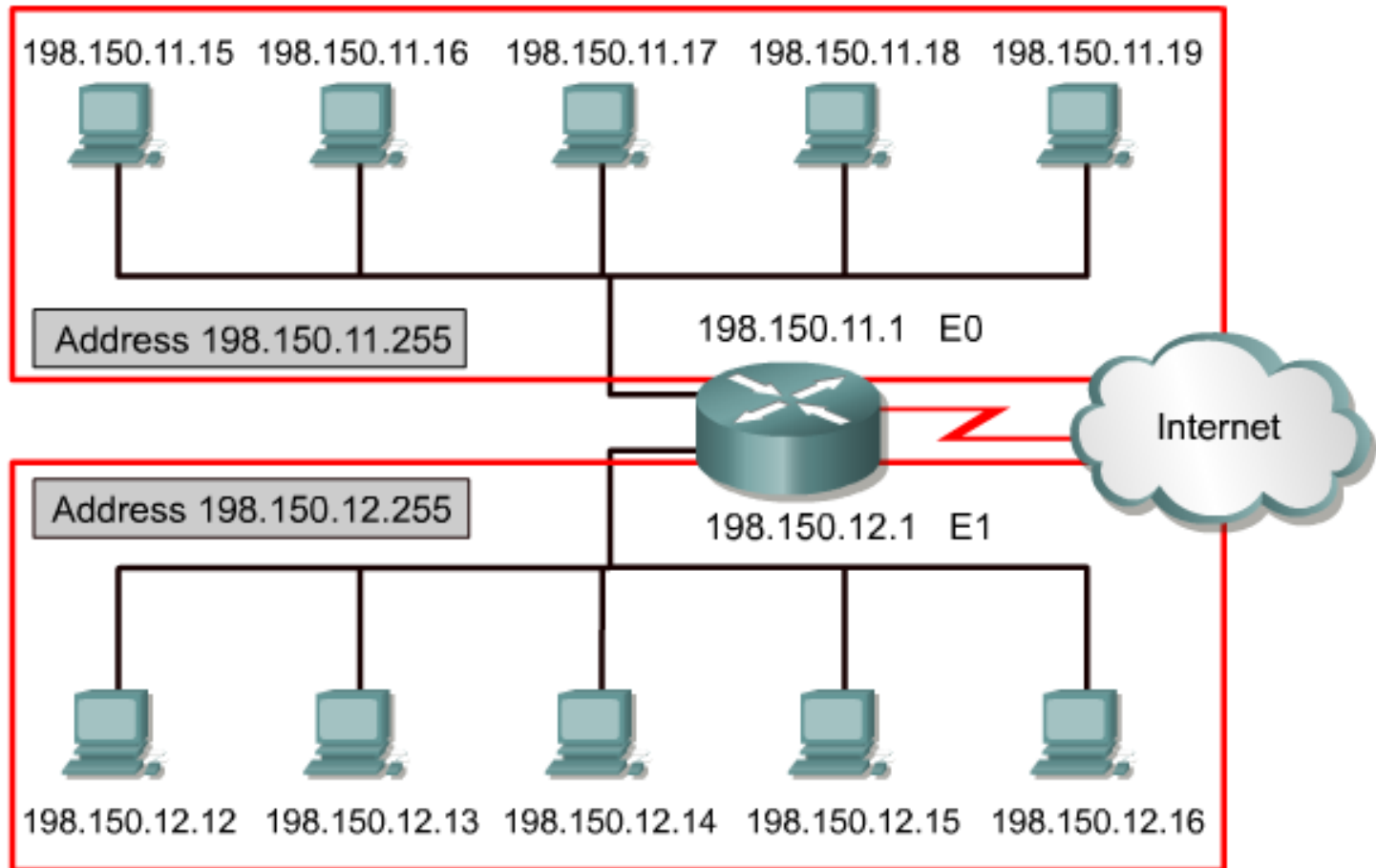
- ❖ Địa chỉ mạng (network address): là địa chỉ IP dùng để đặt cho các mạng. Phần host_id của địa chỉ chỉ chứa các bit 0. Ví dụ: 172.29.0.0
- ❖ Địa chỉ Broadcast: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chỉ chứa các bit 1. Ví dụ: 172.29.255.255.

Địa chỉ mạng (network address)



Địa chỉ mạng

Địa chỉ Broadcast



Địa chỉ broadcast

CHIA MẠNG CON

❖ Tại sao phải chia mạng con

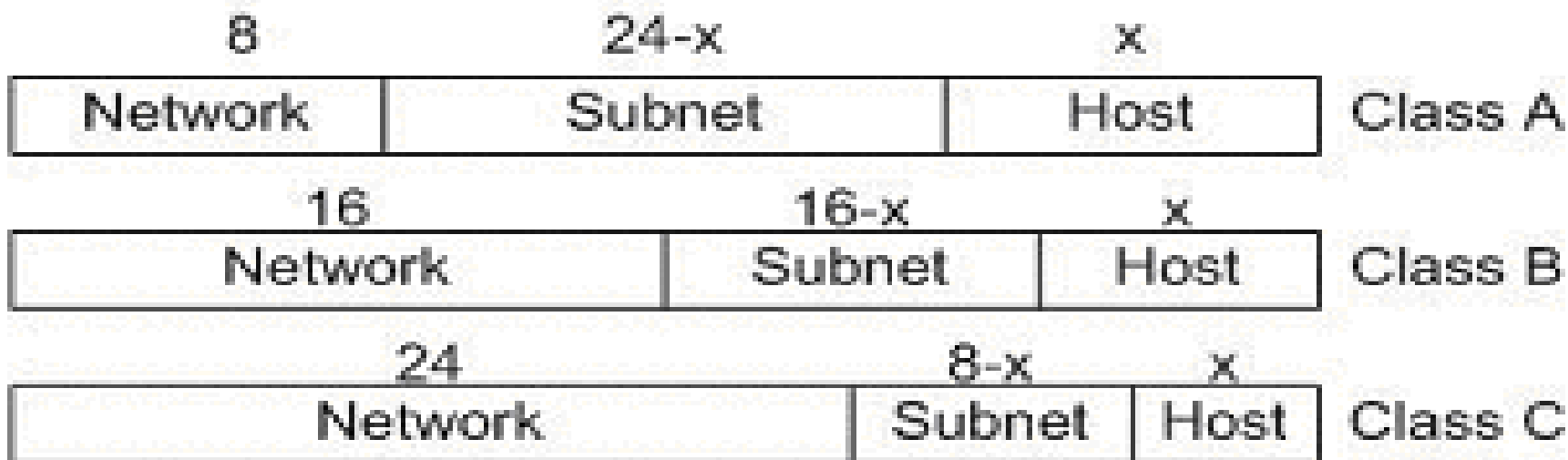
- Mỗi lớp mạng A có đến $2^{24} - 2 = 16.777.214$ địa chỉ IP hay lớp B có $2^{16} - 2 = 65534$ địa chỉ IP.
- Khó có hệ thống đạt số host quá lớn như vậy
- Khó khăn trong công tác quản lý.

Lợi ích khi chia mạng con

- Giảm nghẽn mạng bằng cách tái định hướng các giao vận và giới hạn phạm vi của các thông điệp quảng bá.
- Giới hạn trong phạm vi từng mạng con các trục trặc có thể xảy ra (không ảnh hưởng tới toàn mạng LAN).
- Giảm % thời gian sử dụng CPU do giảm lưu lượng của các giao vận quảng bá.
- Tăng cường bảo mật (các chính sách bảo mật có thể áp dụng cho từng mạng con)
- Cho phép áp dụng các cấu hình khác nhau trên từng mạng con.

Kỹ thuật chia mạng con

- ❖ Mượn một số bit trong phần host_id ban đầu để đặt cho các mạng con
- ❖ Cấu trúc của địa chỉ IP lúc này sẽ gồm 3 phần: network_id, subnet_id và host_id.



Kỹ thuật chia mạng con

- ❖ Số bit dùng trong subnet_id tùy thuộc vào chiến lược chia mạng con. Tuy nhiên số bit tối đa có thể mượn phải tuân theo công thức:

$$\text{Subnet_id} \leq \text{host_id} - 2$$

- ❖ Số lượng bit tối đa có thể mượn:
 - Lớp A: 22 (= 24 - 2) bit -> chia được $2^{22} = 4194304$ mạng con
 - Lớp B: 14 (= 16 - 2) bit -> chia được $2^{14} = 16384$ mạng con
 - Lớp C: 06 (= 8 - 2) bit -> chia được $2^6 = 64$ mạng con

Kỹ thuật chia mạng con

- ❖ Số bit trong phần subnet_id xác định số lượng mạng con. Với số bit là x thì 2^x là số lượng mạng con có được.
- ❖ Ngược lại từ số lượng mạng con cần thiết theo nhu cầu, tính được phần subnet_id cần bao nhiêu bit. Nếu muốn chia 6 mạng con thì cần 3 bit ($2^3=8$), chia 12 mạng con thì cần 4 bit ($2^4 \geq 12$).

Một số khái niệm mới

- ❖ Địa chỉ mạng con (địa chỉ đường mạng): gồm cả phần network_id và subnet_id, phần host_id chỉ chứa các bit 0
- ❖ Địa chỉ broadcast trong một mạng con: tất cả các bit trong phần host_id là 1.
- ❖ Mặt nạ mạng con (subnet mask): tất cả các bit trong phần host_id là 0, các phần còn lại là 1.

Quy ước ghi địa chỉ IP

- ❖ Nếu có địa chỉ IP như 172.29.8.230 thì chưa thể biết được host này nằm trong mạng nào, có chia mạng con hay không và có nếu chia thì dùng bao nhiêu bit để chia. Chính vì vậy khi ghi nhận địa chỉ IP của một host, phải cho biết subnet mask của nó
- ❖ Ví dụ: 172.29.8.230/ 255.255.255.0 hoặc 172.29.8.230/24 (có nghĩa là dùng 24 bit đầu tiên cho NetworkID).

Kỹ thuật chia mạng con

❖ Thực hiện 3 bước:

- Bước 1: Xác định lớp (class) và subnet mask mặc nhiên của địa chỉ.
- Bước 2: Xác định số bit cần mượn và subnet mask mới, tính số lượng mạng con, số host thực sự có được.
- Bước 3: Xác định các vùng địa chỉ host và chọn mạng con muốn dùng.

VÍ DỤ

Hãy xét đến một địa chỉ IP class B, 139.12.0.0, với subnet mask là 255.255.0.0. Một Network với địa chỉ thể này có thể chứa 65534 nodes hay computers. Đây là một con số quá lớn, trên mạng sẽ có đầy broadcast traffic.

Hãy chia network thành 5 mạng con.

Bước 1: Xác định Subnet mask

- ❖ Để chia thành 5 mạng con thì cần thêm 3 bit (vì $2^3 > 5$).
- ❖ Do đó Subnet mask sẽ cần: 16 (bits trước đây) + 3 (bits mới) = 19 bits
- ❖ Địa chỉ IP mới sẽ là 139.12.0.0/19 (để ý con số 19 thay vì 16 như trước đây).

Bước 2: Liệt kê ID của các Subnet mới

Subnet mask với dạng nhị phân	Subnet mask với dạng thập phân
11111111.11111111.11100000.00000000	255.255.224.0

NetworkID của bốn Subnets mới

TT	Subnet ID với dạng nhị phân	Subnet ID với dạng thập phân
1	10001011.00001100.00000000.00000000	139.12.0.0/19
2	10001011.00001100.00100000.00000000	139.12.32.0/19
3	10001011.00001100.01000000.00000000	139.12.64.0/19
4	10001011.00001100.01100000.00000000	139.12.96.0/19
5	10001011.00001100.10000000.00000000	139.12.128.0/19

Bước 3: Cho biết vùng địa chỉ IP của các HostID

TT	Dạng nhị phân	Dạng thập phân
1	10001011.00001100.00000000.00000001 10001011.00001100.00011111.11111110	139.12.0.1/19 - 139.12.31.254/19
2	10001011.00001100.00100000.00000001 10001011.00001100.00111111.11111110	139.12.32.1/19 - 139.12.63.254/19
3	10001011.00001100.01000000.00000001 10001011.00001100.01011111.11111110	139.12.64.1/19 - 139.12.95.254/19
4	10001011.00001100.01100000.00000001 10001011.00001100.01111111.11111110	139.12.96.1/19 - 139.12.127.254/19
5	10001011.00001100.10000000.00000001 10001011.00001100.10011111.11111110	139.12.128.1/19 - 139.12.159.254/19

Ví dụ tính nhanh vùng địa chỉ IP

❖ Cho địa chỉ: 192.168.0.0/24 Chia thành 16 mạng con

❖ Với $n=4 \rightarrow M=16 (= 2^{8-4}) \rightarrow$

- Network 1: 192.168.0.0. Host range: 192.168.0.1–192.168.0.14. Broadcast: 192.168.0.15
- Network 2: 192.168.0.16. Host range: 192.168.0.17–192.168.0.30. Broadcast: 192.168.0.31
- Network 3: 192.168.0.32. Host range: 192.168.0.33–192.168.0.46. Broadcast: 192.168.0.47
- Network 4: 192.168.0.48. Host range: 192.168.0.49–192.168.0.62. Broadcast: 192.168.0.63
-

Tính nhanh vùng địa chỉ IP

- ❖ n – số bit làm subnet
- ❖ Số mạng con: $S = 2^n$
- ❖ Số địa chỉ host trong mạng con: $M = 2^{8-n}$ ($n \leq 8$)
- Byte cuối của IP địa chỉ mạng, ví dụ lớp C: $(k-1)*M$ (với $k=1,2,\dots$)
- Byte cuối của IP broadcast, ví dụ lớp C: $k*M - 1$ (với $k=1,2,\dots$)
- Byte cuối của IP host đầu tiên, ví dụ lớp C: $(k-1)*M + 1$ (với $k=1,2,\dots$)
- Byte cuối của IP host cuối cùng, ví dụ lớp C: $k*M - 2$ (với $k=1,2,\dots$)

Kỹ thuật chia mạng con

192.168.1.0 - 255 /24

192.168.1.0 - 127 /25

192.168.1.128 - 255 /25

192.168.1.0000	0000
192.168.1.0000	0001
192.168.1.0000	0010
192.168.1.0000	0011
192.168.1.0000	0100
192.168.1.0000	0101
192.168.1.0000	0110
192.168.1.0111	1111

192.168.1.1000	0000
192.168.1.1000	0001
192.168.1.1000	0010
192.168.1.1000	0011
192.168.1.1000	0100
192.168.1.1000	0101
192.168.1.1000	0110
192.168.1.1111	1111

192.168.1.0 - 255 /24

192.168.1.0 - 63 /26

192.168.1.64 - 127 /26

192.168.1.128 - 191 /26

192.168.1.192 - 255 /26

192.168.1.0000 0000
192.168.1.0000 0001
192.168.1.0000 0010
192.168.1.0000 0011

192.168.1.0011 1111

192.168.1.0100 0000
192.168.1.0100 0001
192.168.1.0100 0010
192.168.1.0100 0011

192.168.1.0111 1111

192.168.1.1000 0000
192.168.1.1000 0001
192.168.1.1000 0010
192.168.1.1000 0011

192.168.1.1011 1111

192.168.1.1100 0000
192.168.1.1100 0001
192.168.1.1100 0010
192.168.1.1100 0011

192.168.1.1111 1111

192.168.1.0 - 255 /24

192.168.1.0 - 31 /27

192.168.1.32 - 63 /27

192.168.1.64 - 95 /27

192.168.1.96 - 127 /27

192.168.1.128 - 159 /27

192.168.1.160 - 191 /27

192.168.1.192 - 223 /27

192.168.1.224 - 255 /27

192.168.1.0000 0000

192.168.1.0001 1111

192.168.1.0010 0000

192.168.1.0011 1111

192.168.1.0100 0000

192.168.1.0101 1111

192.168.1.0110 0000

192.168.1.0111 1111

192.168.1.1000 0000

192.168.1.1001 1111

192.168.1.1010 0000

192.168.1.1011 1111

192.168.1.1100 0000

192.168.1.1101 1111

192.168.1.1110 0000

192.168.1.1111 1111

Kỹ thuật chia mạng con

192.168.1.0 - 255 /24

192.168.1.0 - 15 /28

192.168.1.16 - 31 /28

192.168.1.32 - 47 /28

192.168.1.48 - 63 /28

192.168.1.64 - 79 /28

192.168.1.80 - 95 /28

192.168.1.96 - 111 /28

192.168.1.112 - 127 /28

192.168.1.128 - 159 /28

192.168.1.144 - 191 /28

192.168.1.160 - 223 /28

192.168.1.176 - 223 /28

192.168.1.192 - 255 /28

192.168.1.208 - 255 /28

192.168.1.224 - 255 /28

192.168.1.240 - 255 /28

192.168.1.0000 0000

192.168.1.0001 0000

192.168.1.0010 0000

192.168.1.0011 0000

192.168.1.0100 0000

192.168.1.0101 0000

192.168.1.0110 0000

192.168.1.0111 0000

192.168.1.1000 0000

192.168.1.1001 0000

192.168.1.1010 0000

192.168.1.1011 0000

192.168.1.1100 0000

192.168.1.1101 0000

192.168.1.1110 0000

192.168.1.1111 0000

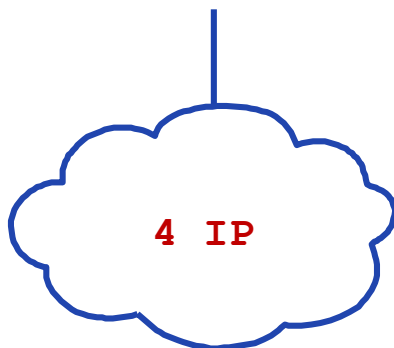
Kỹ thuật chia mạng con

192.168.1.0/29



192.168.1.0000	0000	/ 29
192.168.1.0000	0001	/ 29
192.168.1.0000	0010	/ 29
192.168.1.0000	0011	/ 29
192.168.1.0000	0100	/ 29
192.168.1.0000	0101	/ 29
192.168.1.0000	0110	/ 29
192.168.1.0000	0111	/ 29

192.168.1.0/30



192.168.1.0000	0000	/ 30
192.168.1.0000	0001	/ 30
192.168.1.0000	0010	/ 30
192.168.1.0000	0011	/ 30

Kỹ thuật chia mạng con

Subnet	Network	Host
192.168.1.0 0000000 /25	2 mạng	128 IP
192.168.1.00 000000 /26	4 mạng	64 IP
192.168.1.000 00000 /27	8 mạng	32 IP
192.168.1.0000 0000 /28	16 mạng	16 IP
192.168.1.00000 000 /29	32 mạng	8 IP
192.168.1.000000 00 /30	64 mạng	4 IP
192.168.1.0000000 0 /30	128 mạng	2 IP

	/24	/25	/26	/27	/28
172.16.0.0	0-255	0-127	0-63	0-31	0-15
		128-255	64-127	32-63	16-31
			128-191	64-95	32-47
			192-255	96-127	48-63
				128-159	64-79
				160-191	80-95
				192-223	96-111
				224-255	112-127
					128-143
					144-159
					160-175
					176-191
					192-207
					208-223
					224-239
					240-255

Ví dụ 2

Xác định địa chỉ mạng, địa chỉ Broadcast và dải địa chỉ của mạng sau: 172.16.0.122 /26

B1: Chuyển địa chỉ IP và Subnet Mask về dạng nhị phân và thực hiện phép tính IP and Subnet Mask.

	172	16	0	122
IP	10101100	00001000	00000000	01111010
Subnet mask	11111111	11111111	11111111	11000000
Kết quả AND	10101100	00001000	00000000	01000000

B2: Xác định Network_Id và Host_Id, dải host.

Kết quả AND	10101100	00001000	00000000	01000000
Network_Id	172	16	0	64
Host_Id				58
Host đầu	172	16	0	65
Host cuối	172	16	0	126
Broadcast	172	16	0	127

Ví dụ 3

Xác định địa chỉ mạng, địa chỉ Broadcast và dải địa chỉ của mạng sau:

172.16.0.200 /27

172.16.0. 192 (Network Address)

172.16.0. 193

172.16.0. 194

172.16.0. 223 (Broadcast Address)

Ví dụ 4

172.16.0. 50 /28

172.16.0. 48 (Network Address)

172.16.0. 49

172.16.0. 50

172.16.0. 63 (Broadcast Address)

CHƯƠNG 3: GIAO THỨC TCP/IP

1

- Mô hình TCP/IP

2

- Giao thức TCP/UDP

3

- Giao thức IP

4

- Giao thức ICMP

5

- Giao thức ARP và RARP

6

- Giao thức IPv6

7

- Kỹ thuật định tuyến

IV. GIAO THỨC ICMP

- ❖ Giao thức thông báo điều khiển mạng ICMP (Internet Control Message Protocol) 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.
- ❖ Các loại thông điệp ICMP: Các thông điệp ICMP được chia thành hai nhóm: các thông điệp truy vấn và các thông điệp thông báo lỗi.
- ❖ ICMP sử dụng địa chỉ IP nguồn để gửi thông điệp thông báo lỗi cho node nguồn của gói IP.

CÁC CHỨC NĂNG GIAO THỨC ICMP

- ❖ Điều khiển lưu lượng (Flow Control): Khi các gói dữ liệu đến quá nhanh, thiết bị đích hoặc thiết bị định tuyến ở giữa sẽ gửi một thông điệp ICMP trở lại thiết bị gửi, yêu cầu thiết bị gửi tạm thời ngừng việc gửi dữ liệu.
- ❖ Thông báo lỗi: Trong trường hợp không tới được địa chỉ đích thì hệ thống sẽ gửi một thông báo lỗi "Destination Unreachable".

Các chức năng giao thức ICMP

- ❖ Định hướng lại các tuyến (Redirect Router): Một Router gửi một thông điệp ICMP cho một trạm thông báo nên sử dụng Router khác. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với hai thiết bị định tuyến.
- ❖ Kiểm tra các trạm ở xa: Một trạm có thể gửi một thông điệp ICMP "Echo" để kiểm tra trạm có hoạt động hay không.

CÁC THÔNG điệp ICMP

Nhóm	Loại bản tin	Type
Thông điệp truy vấn (ICMP Queries)	Hỏi và phúc đáp Echo (Echo Request và Echo Reply)	8/0
	Hỏi và phúc đáp nhãn thời gian (Timestamp Request và Timestamp Reply)	13/14
	Yêu cầu và phúc đáp mặt nạ địa chỉ (Address mask Request và Address mask Reply)	17/18
	Yêu cầu và quảng bá bộ định tuyến (Router solicitation và Router advertisement)	10/9
Thông điệp thông báo lỗi (ICMP Error Reports)	Không thể đạt tới đích (Destination Unreachable)	3
	Yêu cầu ngừng hoặc giảm tốc độ phát (Source Quench)	4
	Định hướng lại (Redirection)	5
	Vượt ngưỡng thời gian (Time Exceeded)	11

CHƯƠNG 3: GIAO THỨC TCP/IP

1

- Mô hình TCP/IP

2

- Giao thức TCP/UDP

3

- Giao thức IP

4

- Giao thức ICMP

5

- Giao thức ARP và RARP

6

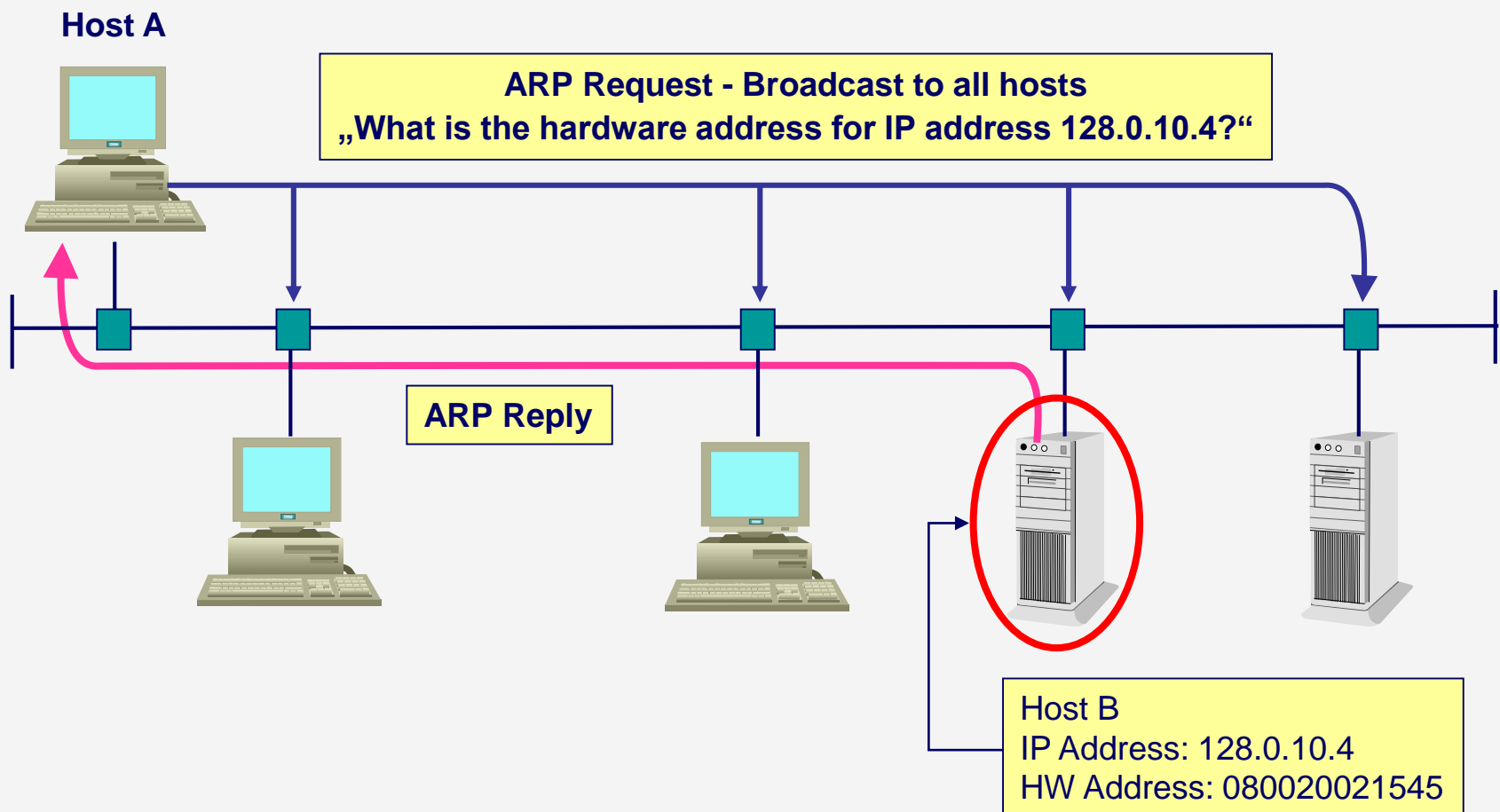
- Giao thức IPv6

7

- Kỹ thuật định tuyến

V. GIAO THỨC ARP

Giao thức TCP/IP sử dụng ARP (Address Resolution Protocol) để tìm địa chỉ vật lý của trạm đích khi biết địa chỉ IP.

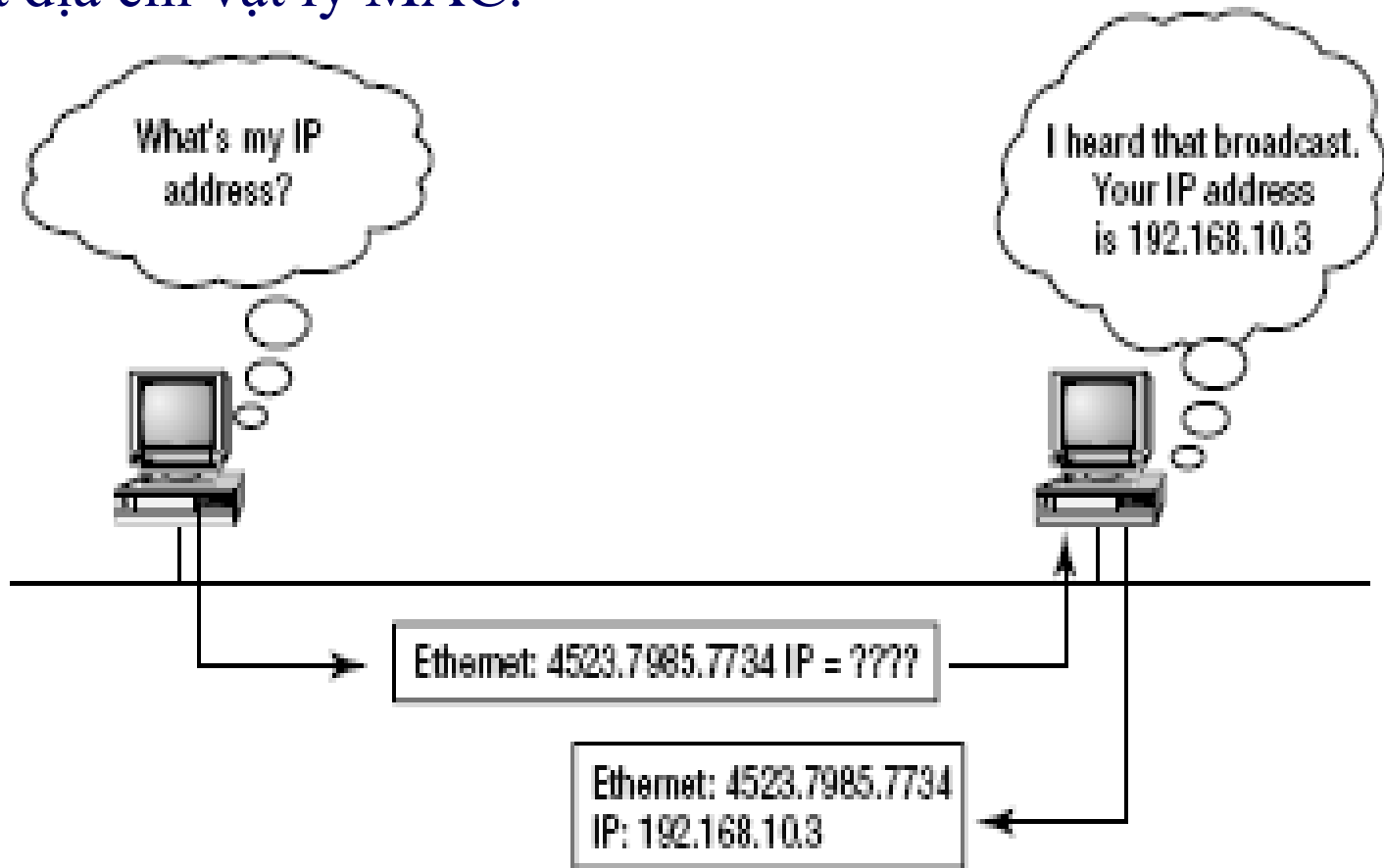


TIẾN TRÌNH CỦA ARP

- ❖ IP yêu cầu địa chỉ MAC
- ❖ Tìm kiếm trong bảng ARP Cache.
- ❖ Nếu tìm thấy sẽ trả lại địa chỉ MAC.
- ❖ Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
- ❖ Tùy theo gói tin trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC cho IP.

GIAO THỨC RARP

Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol), RARP được sử dụng để phát hiện địa chỉ IP, khi biết địa chỉ vật lý MAC.



CHƯƠNG 3: GIAO THỨC TCP/IP

1

- Mô hình TCP/IP

2

- Giao thức TCP/UDP

3

- Giao thức IP

4

- Giao thức ICMP

5

- Giao thức ARP và RARP

6

- Giao thức IPv6

7

- Kỹ thuật định tuyến

VI. GIAO THỨC IPv6

❖ Những hạn chế của IPv4

- Sự thiếu hụt địa chỉ
- Cấu trúc định tuyến không hiệu quả
- Hạn chế tính bảo mật và kết nối đầu cuối – đầu cuối

IPv6 là phiên bản kế thừa phát triển từ IPv4 còn gọi là giao thức IPng (Next General Internet Protocol).

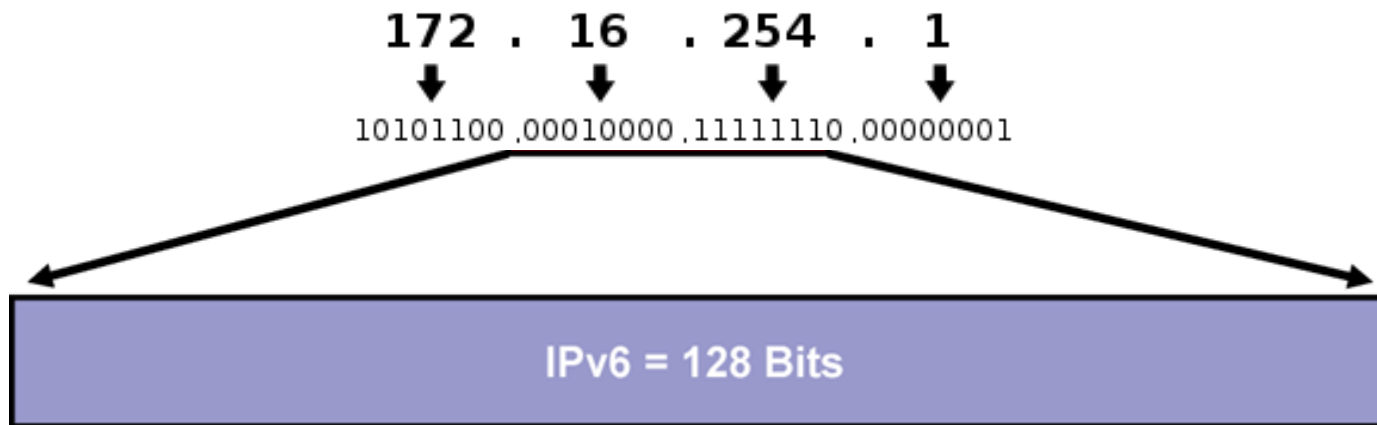
CÁC ĐẶC TRƯNG CỦA IPV6

- ❖ Đơn giản hoá Header: Một số trường trong Header của IPv4 bị bỏ hoặc chuyển thành các trường tùy chọn. Giảm thời gian xử lý và tăng thời gian truyền.
- ❖ Không gian địa chỉ lớn: Độ dài địa chỉ IPv6 là 128 bit, gấp 4 lần độ dài địa chỉ IPv4. Địa chỉ IPv6 không bị thiếu hụt trong tương lai.
- ❖ Khả năng địa chỉ hoá và chọn đường linh hoạt: IPv6 cho phép nhiều lớp địa chỉ với số lượng các node. Cho phép các mạng đa mức và phân chia địa chỉ thành các mạng con riêng lẻ.
- ❖ Có khả năng tự động trong việc đánh địa chỉ. Mở rộng khả năng chọn đường bằng cách thêm trường “Scop” vào địa chỉ quảng bá (Multicast).

CÁC ĐẶC TRƯNG CỦA IPV6

- ❖ Tự động cấu hình địa chỉ: Khả năng tự cấu hình của IPv6 được gọi là khả năng cắm và chạy (Plug and Play). Tính năng này cho phép tự cấu hình địa chỉ cho giao diện mà không cần sử dụng các giao thức DHCP.
- ❖ Khả năng bảo mật: IPsec bảo vệ và xác nhận các gói tin IP:
- ❖ Chất lượng dịch vụ QoS (Quality Of Service): Do cơ chế xác nhận gói tin ngay trong Header nên việc hỗ trợ QoS có thể thực hiện được ngay cả khi gói tin được mã hóa qua IPsec.
- ❖ Khả năng mở rộng: Thêm vào trường Header mở rộng tiếp ngay sau Header, IPv6 có thể được mở rộng thêm các tính năng mới một cách .
- ❖ Tính di động: IPv6 cho phép nhiều thiết bị di động kết nối vào Internet qua mạng công cộng nhờ sóng vô tuyến.

ĐẠI CHỈ IPV6



IPv4: 32 bits chia làm 4 octat, mỗi octat 1 bytes

— \approx 4,200,000,000 địa chỉ

IPv6

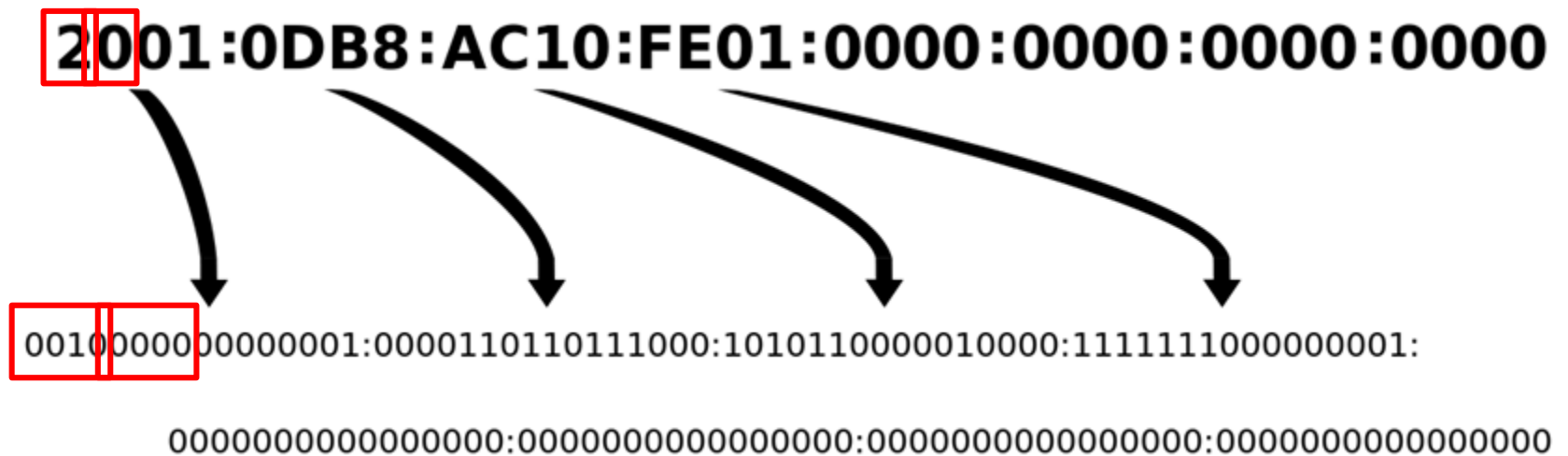
- 128 bits or 16 bytes: số bit gấp 4 lần IPv4

— $\approx 3.4 * 10^{38}$ địa chỉ

— $\approx 340,282,366,920,938,463,374,607,432,768,211,456$

— $\approx 5 * 10^{28}$ địa chỉ cho một người

Biểu diễn địa chỉ IPv6



Biểu diễn địa chỉ IPv6

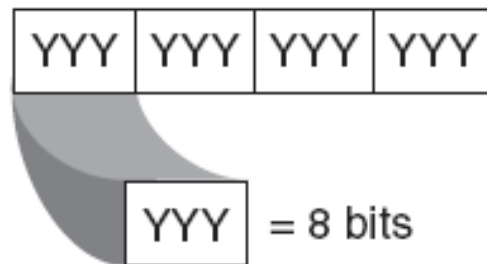
2001:0ABC:00AB:000A:0000:0000:0000:1001

2001:ABC:AB:A:0:0:0:1001 0: 0: 0:1001

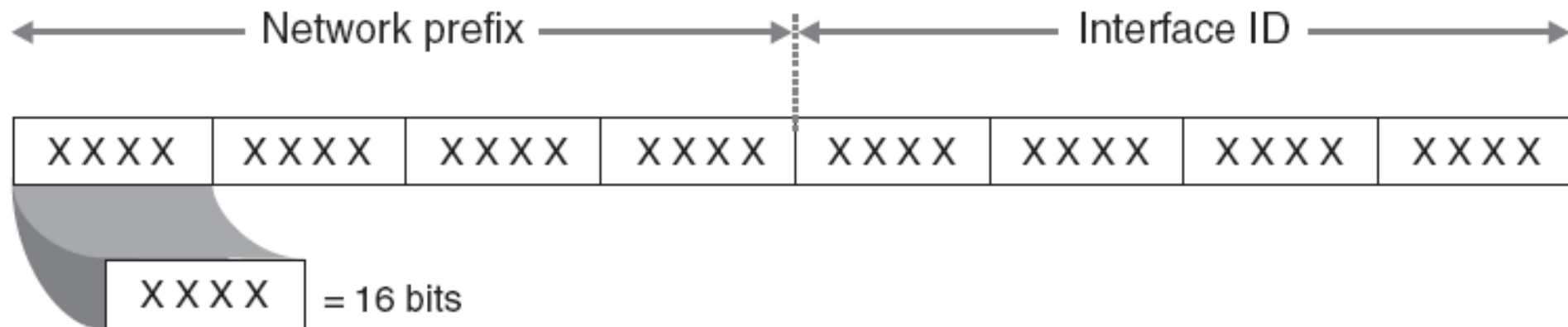
2001:ABC:AB:A::1001

Cấu trúc IPv6

32-bit IPv4 address

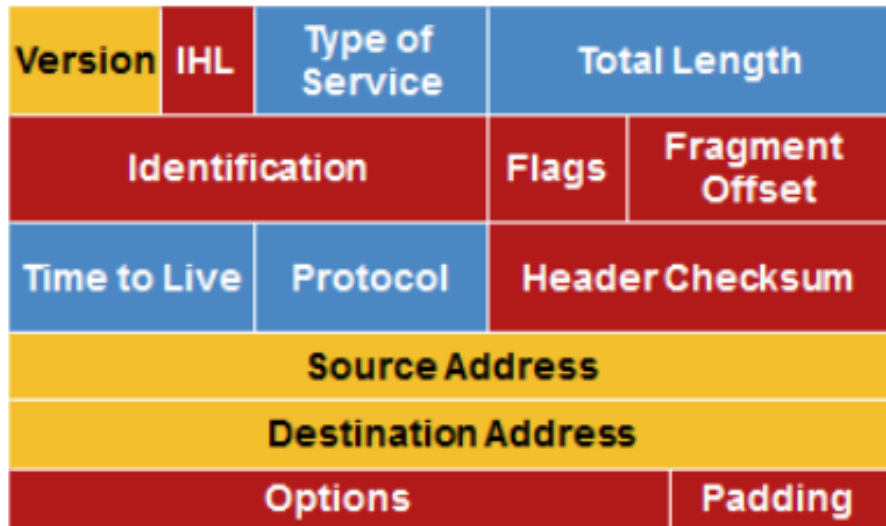


128-bit IPv6 address



TIÊU ĐỀ ĐỊA CHỈ IP

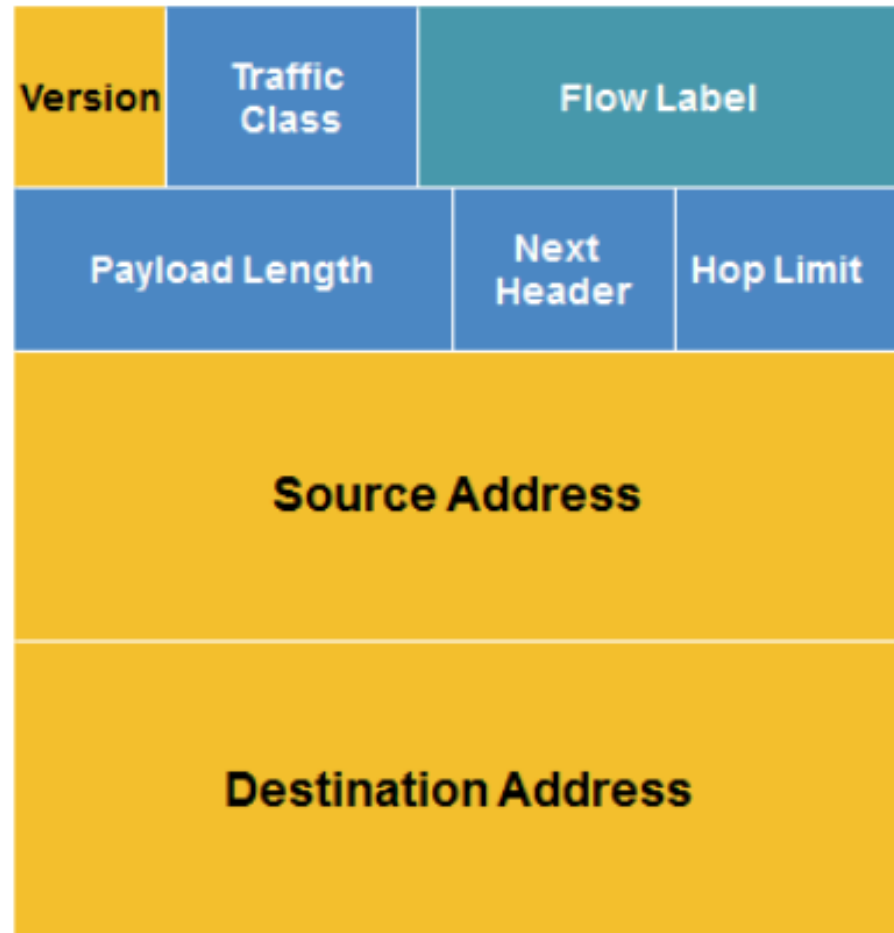
IPv4 Header



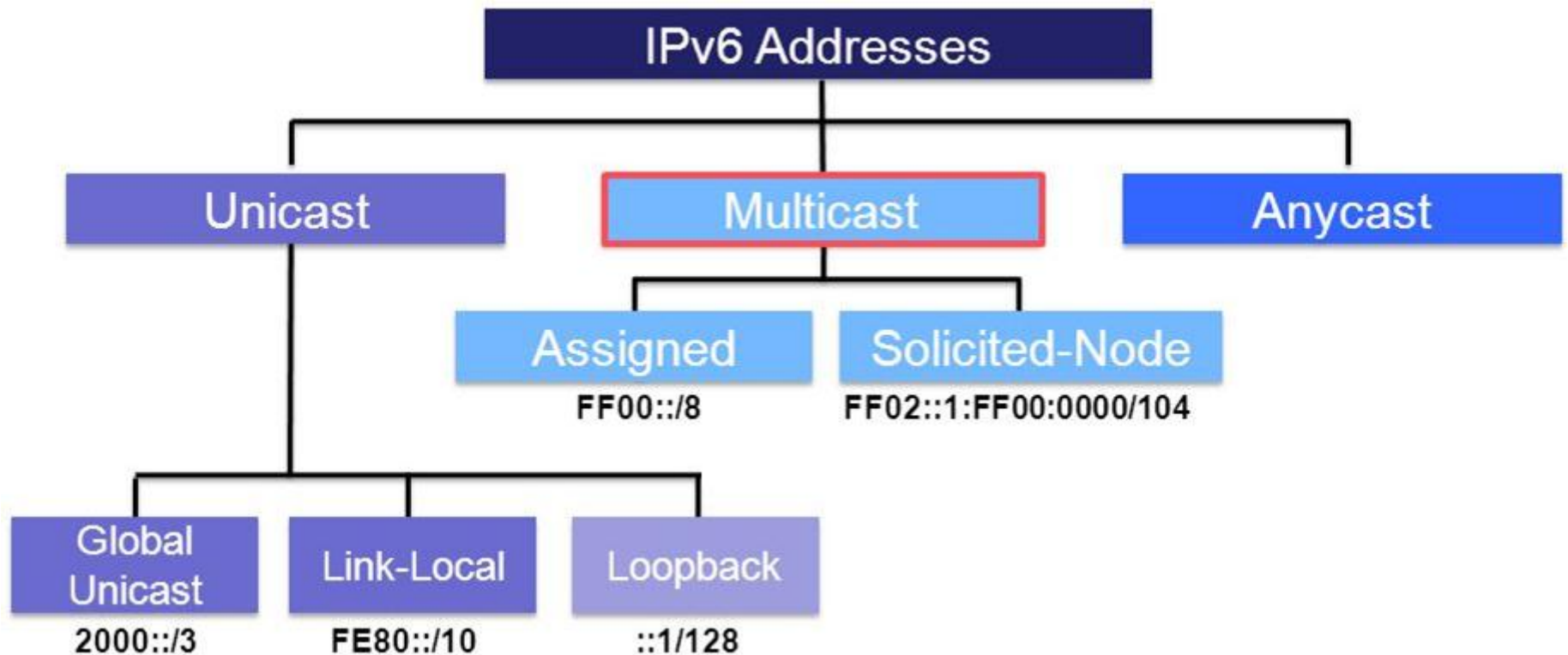
Legend

- Field's Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6

IPv6 Header

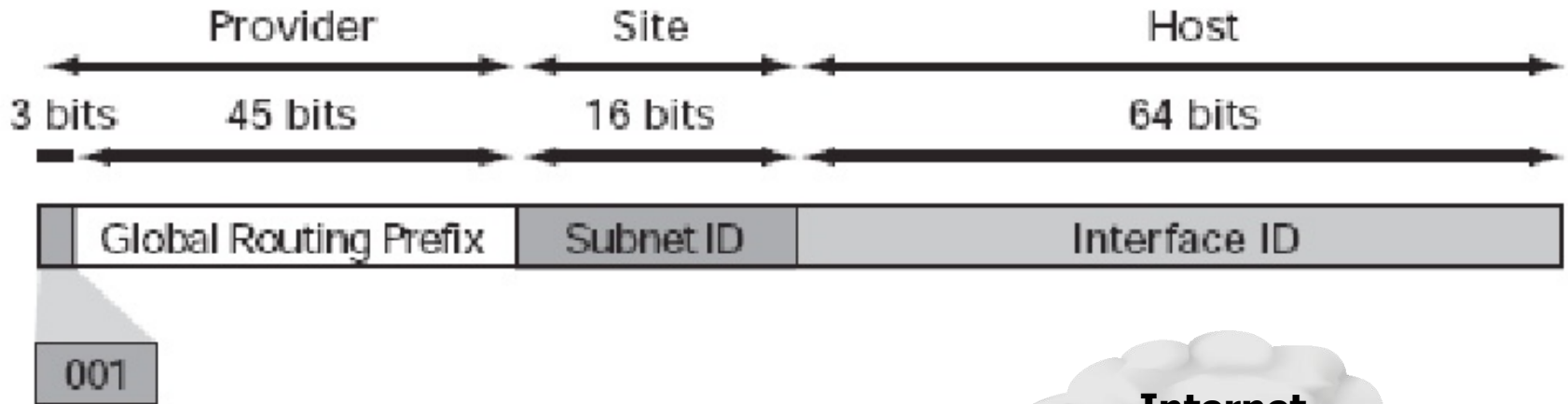


Phân loại IPv6



IPv6 does not have a Broadcast Address

IPv6: Global Unicast Address (2000::/3)



2001:0000:0000::/48

2001:0000:0000:0001:: /64

2001:0000:0000:0002:: /64

2001:0000:0000:0003:: /64

2001:0000:0000:XXXX:: /64

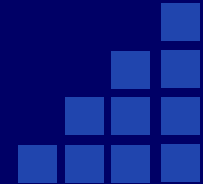


2001:0:0:0001:: /64

2001:0:0:0003:: /64

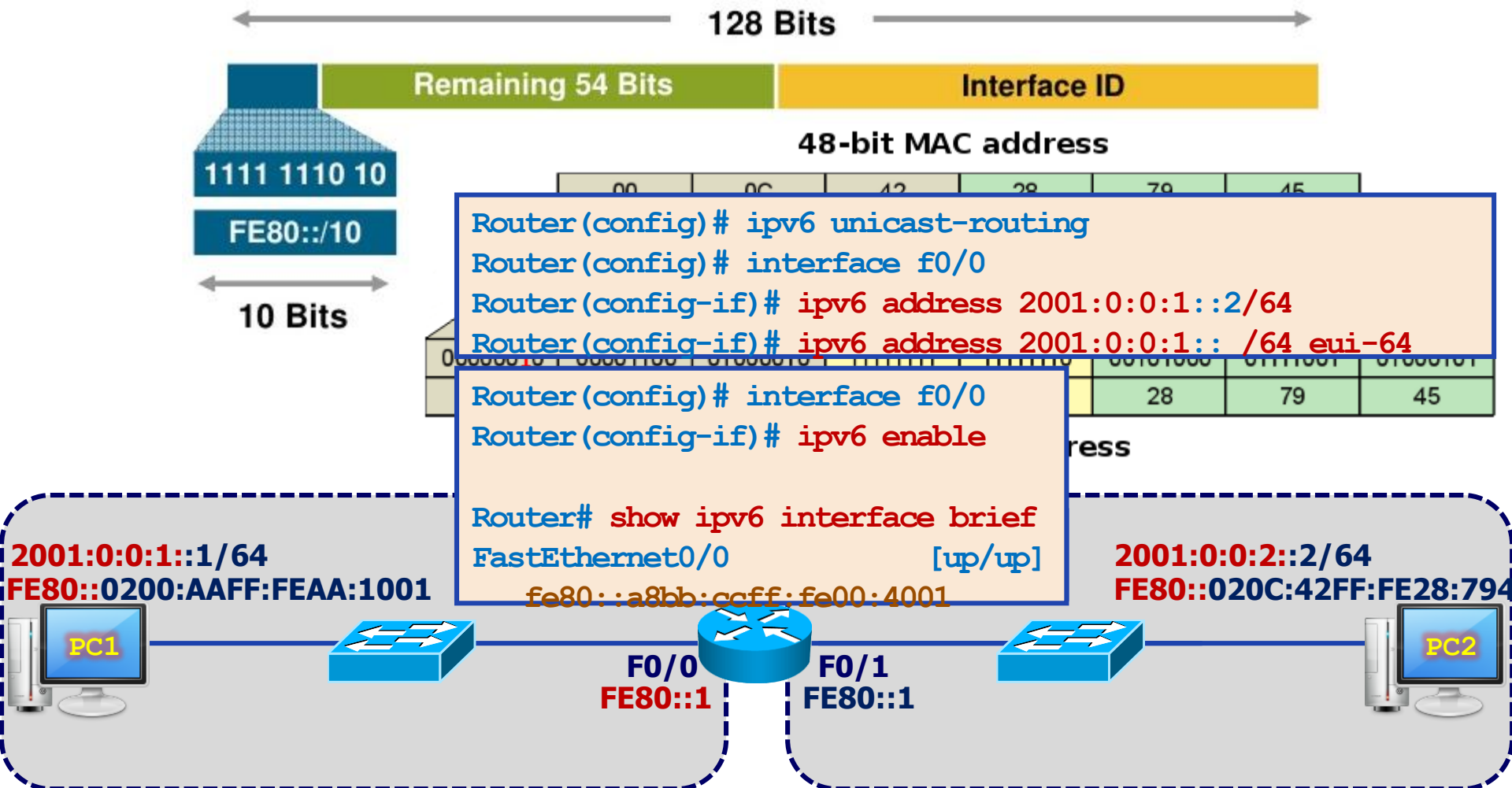
2001:0:0:0002:: /64

IPv6: Multicast Address



IPv6		IPv4	
Address(s)	Description	Address(es)	Description
		224.0.0.0	Base Address (Reserved)
FF02:0:0:0:0:0:0:1	All Nodes Address	224.0.0.1	All Systems on this Subnet
FF02:0:0:0:0:0:0:2	All Routers Address	224.0.0.2	All Routers on this Subnet
FF02:0:0:0:0:0:0:3	Unassigned	224.0.0.3	Unassigned
FF02:0:0:0:0:0:0:4	DVMRP Routers	224.0.0.4	DVMRP Routers
FF02:0:0:0:0:0:0:5	OSPF/IGMP	224.0.0.5	OSPF/IGMP OSPF/IGMP All Routers
FF02:0:0:0:0:0:0:6	OSPF/IGMP Designated Routers	224.0.0.6	OSPF/IGMP OSPF/IGMP Designated Routers
FF02:0:0:0:0:0:0:7	ST Routers	224.0.0.7	ST Routers
FF02:0:0:0:0:0:0:8	ST Hosts	224.0.0.8	ST Hosts
FF02:0:0:0:0:0:0:9	RIP Routers	224.0.0.9	RIP2 Routers
FF02:0:0:0:0:0:0:A	EIGRP Routers	224.0.0.10	EIGRP Routers
FF02:0:0:0:0:0:0:B	Mobile-Agents	224.0.0.11	Mobile-Agents
FF02:0:0:0:0:0:0:C	SSDP	224.0.0.12	DHCP Server / Relay Agent
FF02:0:0:0:0:0:0:D	All PIM Routers	224.0.0.13	All PIM Routers
FF02:0:0:0:0:0:0:E	RSVP-ENCAPSULATION	224.0.0.14	RSVP-ENCAPSULATION

IPv6: Link-Local Address



IPv6: Link-Local Address



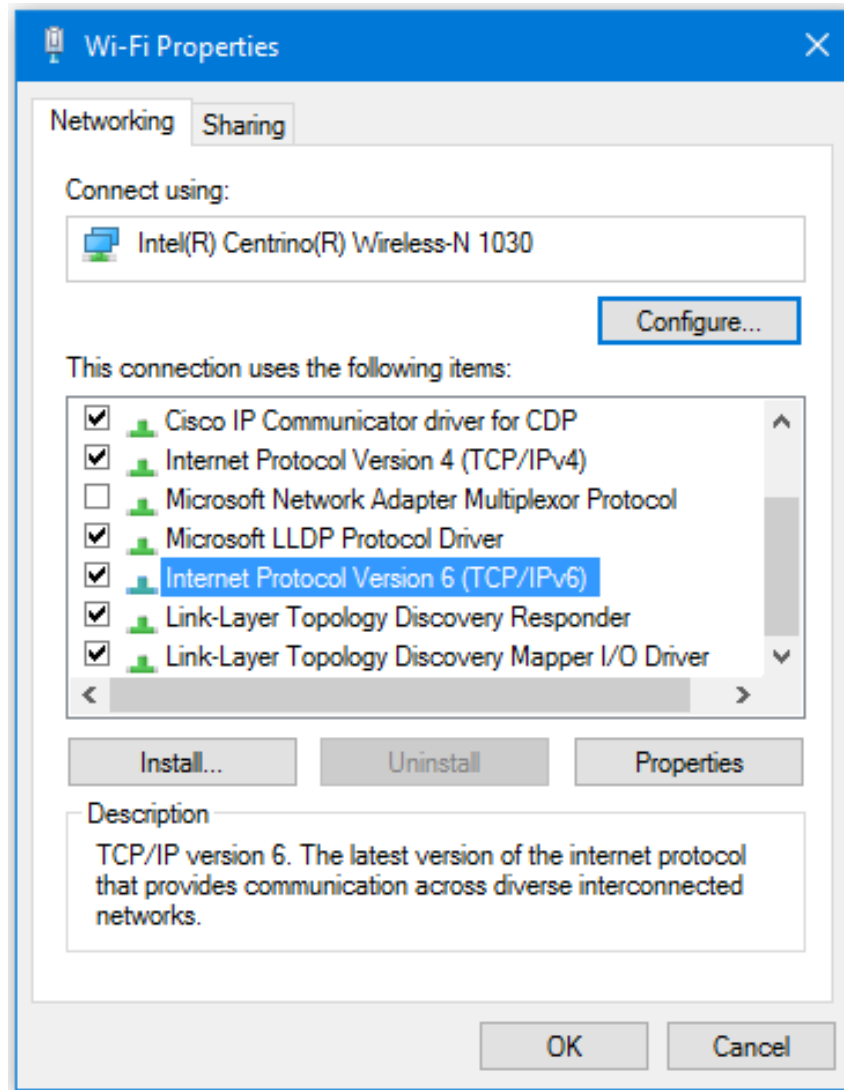
```
C:\Users\Admin>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
IPv6 Address . . . . . : fcab:bebc:abac:100::1000  
Link-local IPv6 Address . . . . . : fe80::88c2:66c3:3049:1172%10  
IPv4 Address . . . . . : 192.168.1.145  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

IPv6: Configuring Address



IPv6: Configuring Address

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001::2

Subnet prefix length: 64

Default gateway: 2001::1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

SO SÁNH IPv4 VÀ IPv6

IPv4 Address	IPv6 Address
Phân lớp địa chỉ (Lớp A, B, C và D)	Không phân lớp địa chỉ. Cấp phát theo tiền tố
Lớp D là Multicast (224.0.0.0/4)	Địa chỉ multicast có tiền tố FF00::/8
Sử dụng địa chỉ Broadcast	Không có Broadcast, thay bằng Anycast
Địa chỉ unspecified là 0.0.0.0	Địa chỉ Unspecified là ::
Địa chỉ Loopback 127.0.0.1	Địa chỉ Loopback là ::1
Sử dụng địa chỉ Public	Tương ứng là địa chỉ Unicast toàn cầu
Địa chỉ IP riêng (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Địa chỉ Site-Local (FEC0::/48)
Địa chỉ tự cấu hình (169.254.0.0/16)	Địa chỉ Link-Local (FE80::/64)
Dạng biểu diễn: chuỗi số thập phân cách nhau bởi dấu chấm	Dạng biểu diễn: chuỗi số Hexa cách nhau bởi dấu hai chấm; có thể nhóm chuỗi số 0 liên nhau vào một ký tự
Sử dụng mặt nạ mạng con	Chỉ sử dụng ký hiệu tiền tố để chỉ mạng
Phân giải tên miền DNS: bản ghi tài nguyên địa chỉ máy chủ IPv4 (A)	Phân giải tên miền DNS: bản ghi tài nguyên địa chỉ máy chủ IPv6 (AAAA)
Tên miền ngược: IN-ADDR.ARPA	Tên miền ngược: IP6.INT domain

CHƯƠNG 3: GIAO THỨC TCP/IP

1

- Mô hình TCP/IP

2

- Giao thức TCP/UDP

3

- Giao thức IP

4

- Giao thức ICMP

5

- Giao thức ARP và RARP

6

- Giao thức IPv6

7

- Kỹ thuật định tuyến

VII KỸ THUẬT ĐỊNH TUYẾN

1. ROUTING - ĐỊNH TUYẾN

- Định tuyến là chức năng của Router giúp xác định quá trình tìm đường đi cho các gói tin để truyền dữ liệu từ nguồn tới đúng đích cần gửi.



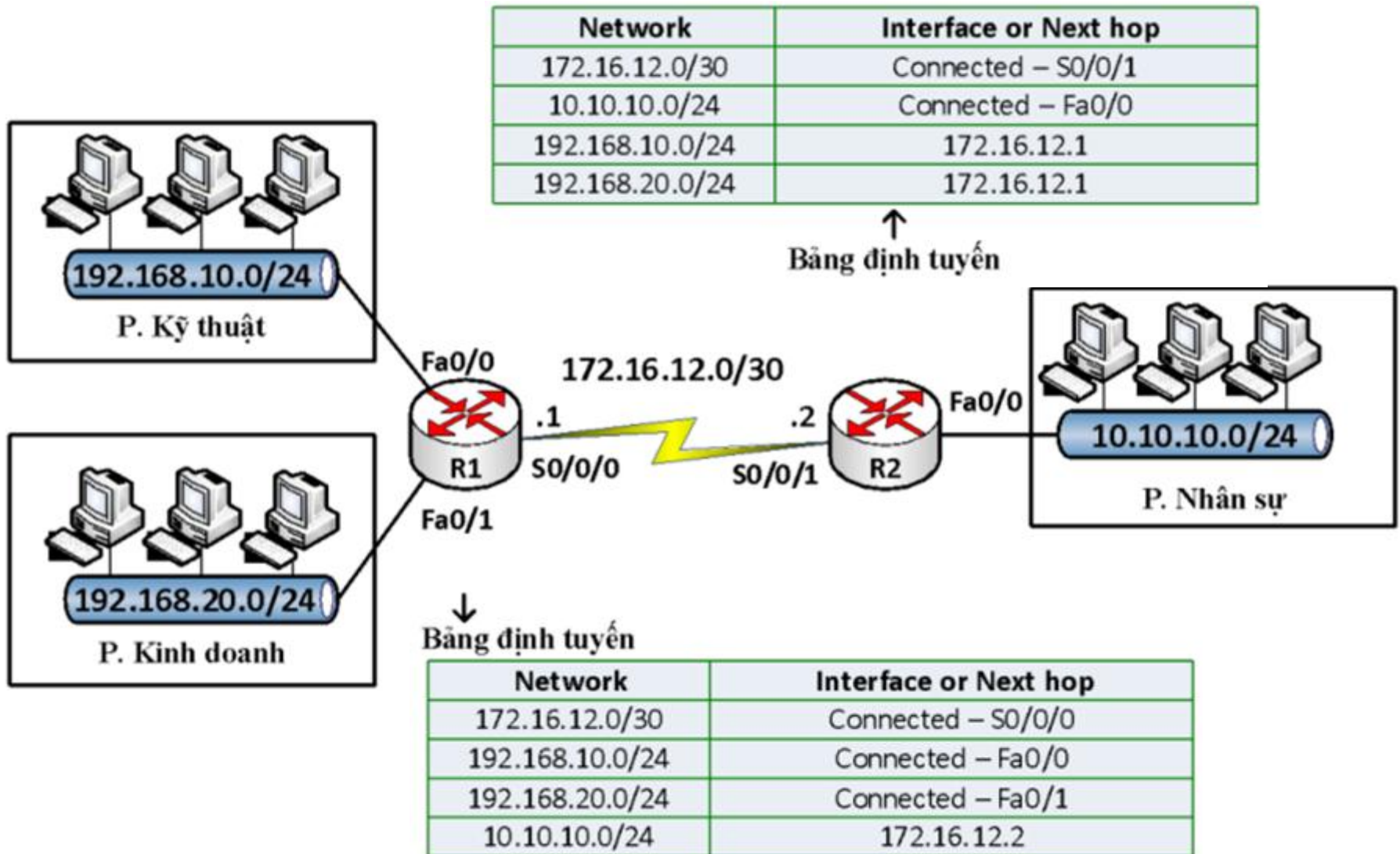
ROUTER

- ❖ Router là một thiết bị ở lớp 3. Router quyết định chuyển gói dựa trên địa chỉ mạng của gói dữ liệu. Router sử dụng bảng định tuyến để ghi lại địa chỉ lớp 3 của các mạng kết nối trực tiếp vào router và các mạng mà router học được từ các router láng giềng.
- ❖ Mục tiêu của router là thực hiện các việc sau:
 - Kiểm tra dữ liệu lớp 3 của gói nhận được
 - Chọn đường tốt nhất cho gói dữ liệu
 - Chuyển mạch gói ra cổng tương ứng
- ❖ Router ko bị bắt buộc phải chuyển các gói quảng bá

ROUTING - ĐỊNH TUYẾN

- Router dựa vào địa chỉ IP đích (destination IP) trong các gói tin và sử dụng bảng định tuyến (routing table) để xác định đường đi cho chúng.
- Trong bảng định tuyến, mỗi mạng mà router có thể chuyển đi (mạng đích) thể hiện bằng một dòng.
- Mỗi mạng này có được có thể do chúng đang kết nối trực tiếp với router đang xét hay router học được thông qua việc cấu hình định tuyến.

BẢNG ĐỊNH TUYẾN



Router>en

Router#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 20.0.0.0/24 is directly connected, Serial0/1/0
L 20.0.0.2/32 is directly connected, Serial0/1/0
S* 0.0.0.0/0 is directly connected, Serial0/1/0
[1/0] via 20.0.0.1

Router#

2. PHÂN LOẠI ĐỊNH TUYẾN

❖ Có 2 phương pháp định tuyến:

- Định tuyến tĩnh (Static Route)
- Định tuyến động (Dynamic Route)

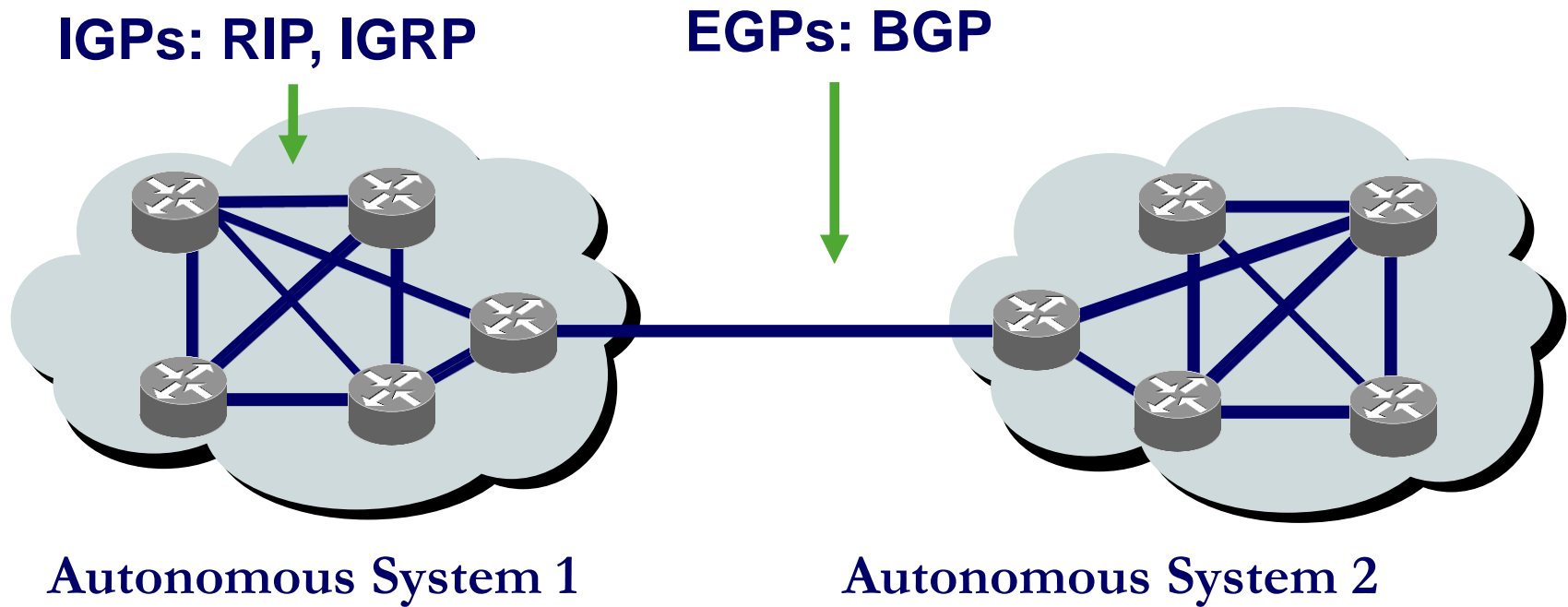
❖ Định tuyến tĩnh (Static Route)

- Định tuyến tĩnh là loại định tuyến mà trong đó router sử dụng các tuyến đường đi tĩnh để vận chuyển dữ liệu đi.
- Các tuyến đường đi tĩnh này có được do người quản trị cấu hình thủ công vào các router.

ĐỊNH TUYẾN ĐỘNG - DYNAMIC ROUTING

- ❖ Định tuyến động là loại định tuyến mà trong đó router sử dụng các tuyến đường đi động để vận chuyển dữ liệu đi.
- ❖ Các tuyến đường đi động này có được do các router sử dụng các giao thức định tuyến động trao đổi thông tin định tuyến với nhau tạo ra.
- ❖ Một số giao thức định tuyến động phổ biến: RIP, OSPF, EIGRP,....

ĐỊNH TUYẾN ĐỘNG - DYNAMIC ROUTING



ĐỊNH TUYẾN ĐỘNG - DYNAMIC ROUTING

❖ Kỹ thuật định tuyến động chia làm hai nhóm:

➤ Định tuyến ngoài EGP (Exterior Gateway

Protocol): là giao thức trao đổi thông tin giữa các AS (Autonomous System) khác nhau. Tiêu biểu là giao thức BGP (Border Gateway Protocol)

➤ Định tuyến trong IGP (Interior Gateway

Protocol): là giao thức định tuyến bên trong 1 AS như (RIP, IGRP, EIGRP, OSPF...).

IGP (Interior Gateway Protocol)

- ❖ IGP lại được chia thành 4 nhóm:
- ❖ Distance – vector: Mỗi router gửi cho láng giềng của nó toàn bộ bảng định tuyến của nó theo định kì. Giao thức tiêu biểu là RIP.
- ❖ Link – state: Mỗi router sẽ gửi bản tin trạng thái đường link (LSA) cho các router khác. Các Router sau khi xây dựng xong bảng định tuyến sẽ vẽ ra được một bản đồ mạng của toàn bộ hệ thống. Tiêu biểu là giao thức OSPF.
- ❖ Hybrid: tiêu biểu là giao thức EIGRP. Loại hình này kết hợp các đặc điểm của hai loại trên.
- ❖ Path-vector: Sử dụng trong giao thức định tuyến ngoại vùng BGP

IGP (Interior Gateway Protocol)

- ❖ Các giao thức IGP cũng có thể chia làm 2 loại:
- Các giao thức Classfull: Router sẽ không gửi kèm subnet-mask trong bảng tin định tuyến của mình. Từ đó giao thức classful không hỗ trợ sơ đồ VLSM và mạng gián đoạn (Discontiguos networks). Giao thức tiêu biểu là RIPv1 .
- Các giao thức Classless: ngược lại với classful, Router có thể gửi kèm subnet-mask trong bảng định tuyến. Từ đó các giao thức classless có hỗ trợ sơ đồ VLSM và mạng gián đoạn. Các giao thức tiêu biểu là: RIPv2, OSPF, EIGRP.

3. Thuật toán Distance Vector (1)

Công thức Bellman-Ford (quy hoạch động)

Định nghĩa

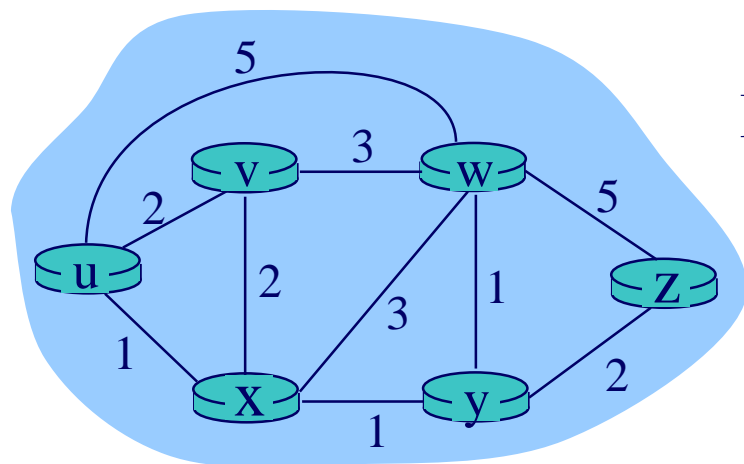
$d_x(y) :=$ chi phí của đường đi chi phí thấp nhất từ x tới y

Thì

$$d_x(y) = \min \{ c(x,v) + d_v(y) \}$$

Trong đó, min được tính với tất cả các hàng xóm của x

Ví dụ Bellman-Ford (2)



Dễ thấy, $d_v(z) = 5$, $d_x(z) = 3$, $d_w(z) = 3$

Công thức B-F:

$$\begin{aligned} d_u(z) &= \min \{ c(u,v) + d_v(z), \\ &\quad c(u,x) + d_x(z), \\ &\quad c(u,w) + d_w(z) \} \\ &= \min \{ 2 + 5, \\ &\quad 1 + 3, \\ &\quad 5 + 3 \} = 4 \end{aligned}$$

Nút đạt giá trị nhỏ nhất là next hop trong đường đi ngắn nhất
→ bảng chuyển tiếp

Thuật toán Distance Vector (3)

- ❖ $D_x(y)$ = chi phí thấp nhất từ x tới y
- ❖ Distance vector: $D_x = [D_x(y): y \in N]$
- ❖ Nút x biết chi phí tới mỗi hàng xóm v: $c(x,v)$
- ❖ Node x duy trì $D_x = [D_x(y): y \in N]$
- ❖ Node x cũng duy trì các distance vector của các hàng xóm của nó
 - Đối với hàng xóm v, x duy trì $D_v = [D_v(y): y \in N]$

Thuật toán Distance vector (4)

Ý tưởng:

- ❖ Mỗi nút định kỳ gửi tính toán distance vector của nó tới các hàng xóm
- ❖ Khi nút x nhận tính toán DV mới từ hàng xóm, nó cập nhật DV của nó sử dụng công thức B-F:

$$D_x(y) \leftarrow \min_v \{c(x,v) + D_v(y)\} \quad \text{với mỗi } y \in N$$

- Ước lượng $D_x(y)$ hội tụ tới chi phí thấp nhất thực tế của $d_x(y)$

Thuật toán Distance Vector (5)

Lặp, không đồng bộ: Mỗi vòng

lặp cục bộ thực hiện khi:

- ❖ Chi phí liên kết cục bộ thay đổi
- ❖ Bản tin cập nhật DV từ hàng xóm

Phân tán:

- ❖ Mỗi nút thông báo cho hàng xóm chỉ khi DV của nó thay đổi
 - Sau đó, các hàng xóm thông báo cho các hàng xóm của nó nếu cần

Mỗi nút:

đợi for (thay đổi chi phí liên kết cục bộ, bản tin từ hàng xóm)

tính lại

Nếu DV tới đích nào đó thay đổi, *thông báo* cho hàng xóm

$$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\} \\ = \min\{2+0, 7+1\} = 2$$

$$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\} \\ = \min\{2+1, 7+0\} = 3$$

Bảng nút x

		chi phí tới		
		x	y	z
từ	x	0	2	7
	y	∞	∞	∞
	z	∞	∞	∞

Bảng nút y

		chi phí tới		
		x	y	z
từ	x	∞	∞	∞
	y	2	0	1
	z	∞	∞	∞

Bảng nút z

		chi phí tới		
		x	y	z
từ	x	∞	∞	∞
	y	∞	∞	∞
	z	7	1	0

		chi phí tới		
		x	y	z
từ	x	0	2	3
	y	2	0	1
	z	7	1	0

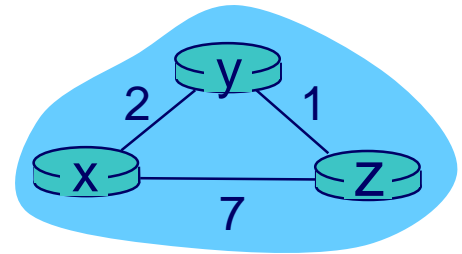
		chi phí tới		
		x	y	z
từ	x	0	2	7
	y	2	0	1
	z	7	1	0

		chi phí tới		
		x	y	z
từ	x	0	2	7
	y	2	0	1
	z	3	1	0

		chi phí tới		
		x	y	z
từ	x	0	2	3
	y	2	0	1
	z	3	1	0

		chi phí tới		
		x	y	z
từ	x	0	2	3
	y	2	0	1
	z	3	1	0

		chi phí tới		
		x	y	z
từ	x	0	2	3
	y	2	0	1
	z	3	1	0

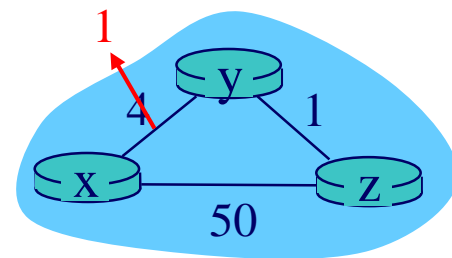


→ thời gian

Distance Vector: chi phí liên kết thay đổi

Chi phí liên kết thay đổi:

- ❑ Nút phát hiện chi phí liên kết cục bộ thay đổi
- ❑ Cập nhật thông tin dẫn đường, tính lại DV
- ❑ Nếu DV thay đổi, thông báo cho các hàng xóm



Tại thời điểm t_0 , y phát hiện chi phí liên kết thay đổi, cập nhật DV của nó và thông báo cho hàng xóm của nó.

“Tin mới
đi nhanh”

Tại thời điểm t_1 , z nhận cập nhật từ y và cập nhật bảng của nó. Nó tính chi phí thấp nhất mới tới x và gửi DV của nó tới các hàng xóm của nó.

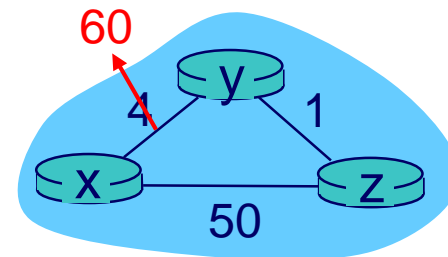
Tại thời điểm t_2 , y nhận cập nhật của z và cập nhật bảng khoảng cách của nó.

Chi phí thấp nhất của y không thay đổi và vì vậy y *không* gửi bất kỳ bản tin nào tới z

Distance Vector: chi phí liên kết thay đổi

Chi phí liên kết thay đổi:

- ❑ Tin mới đi nhanh
- ❑ Tin xấu đi chậm – vấn đề “đếm vô hạn”!



Kỹ thuật “Poisoned reverse”:

- ❑ Nếu Z qua Y tới X :
 - ❑ Z nói với Y khoảng cách của Z tới X là vô hạn (vì vậy, Y không dẫn đường tới X qua Z)
- ❑ Giải quyết bài toán “đếm vô hạn”?

So sánh thuật toán LS và DV

Sự phức tạp bản tin

- ❖ LS: n nút, E liên kết, $O(nE)$ bản tin gửi đi
- ❖ DV: chỉ trao đổi giữa các hàng xóm
 - Thời gian hội tụ thay đổi

Tốc độ hội tụ

- ❖ LS: Thuật toán $O(n^2)$ đòi hỏi $O(nE)$ bản tin
 - Có thể không ổn định
- ❖ DV: Thời gian hội tụ thay đổi
 - Có thể dẫn đường lặp
 - Vấn đề “đếm vô hạn”

Tính chịu lỗi: Điều gì xảy ra khi router bị lỗi?

LS:

- Nút có thể thông báo chi phí *liên kết* sai
- Mỗi nút chỉ tính toán bảng của nó

DV:

- Nút có thể thông báo chi phí *đường đi* sai
- Mỗi bảng của nút sử dụng bởi nút khác
 - Lan truyền lỗi qua mạng

4. THUẬT TOÁN DẪN ĐƯỜNG LINK-STATE

Thuật toán Dijkstra

- ❖ Mọi nút đều biết topology của mạng, chi phí của liên kết
 - Thực hiện bằng “link state broadcast”
 - Mọi nút có thông tin giống nhau
- ❖ Tính toán đường đi có chi phí thấp nhất từ một nút (nguồn) tới tất cả các nút khác.
 - Cho kết quả là **bảng chuyển tiếp** của nút đó
- ❖ **Lặp:** sau k vòng lặp, biết đường đi có chi phí thấp nhất tới k đích

Chú thích:

- ❖ **$c(x,y)$:** chi phí liên kết từ nút x tới nút y; $= \infty$ nếu không là hàng xóm trực tiếp
- ❖ **$D(v)$:** giá trị hiện tại của chi phí đường đi từ nguồn tới đích v
- ❖ **$p(v)$:** nút trước của v trong đường đi từ nguồn tới v
- ❖ **N' :** tập các nút mà đường đi có chi phí thấp nhất đã xác định

Thuật toán Dijkstra

1 **Khởi tạo:**

2 $N' = \{u\}$

3 for <mọi nút v >

4 if < v kề u >

5 then $D(v) = c(u, v)$

6 else $D(v) = \infty$

7

8 **Lặp**

9 Tìm w không trong N' thỏa mãn $D(w)$ nhỏ nhất

10 Thêm w vào N'

11 Cập nhật $D(v)$ với mọi v kề với w và không trong N' :

12 $D(v) = \min(D(v), D(w) + c(w, v))$

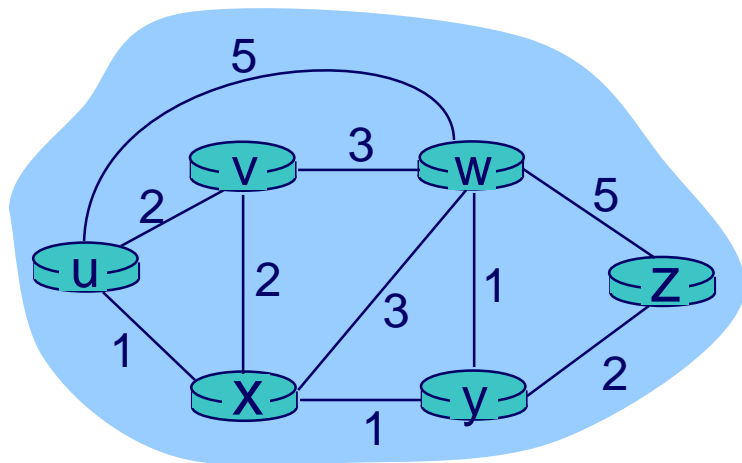
13 /* Chi phí mới tới v là chi phí cũ tới v hoặc là chi phí đường đi

14 ngắn nhất tới w đã biết cộng với chi phí từ w tới v */

15 **Tới khi mọi nút trong N'**

Thuật toán Dijkstra: ví dụ

Bước	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					



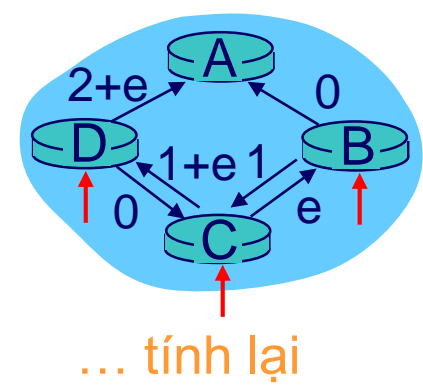
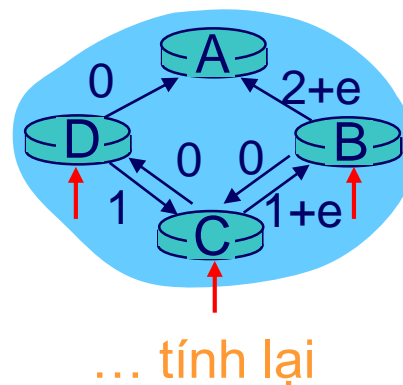
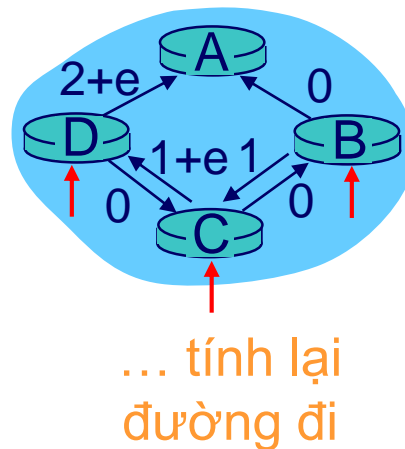
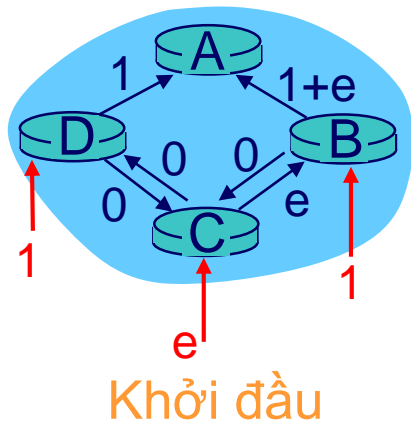
Thuật toán Dijkstra: thảo luận

Độ phức tạp của thuật toán: n nút

- ❖ Mỗi vòng lặp: cần kiểm tra mọi nút, w , không trong N
- ❖ $n(n+1)/2$ lần so sánh: $O(n^2)$
- ❖ Cài đặt có thể hiệu quả hơn: $O(n \log n)$

Trường hợp không ổn định:

- ❖ Ví dụ: chi phí liên kết = lượng lưu lượng đã mang



BÀI TẬP

- ❖ Cấu hình giao thức định tuyến RIP
- ❖ Cấu hình giao thức định tuyến OSPF

