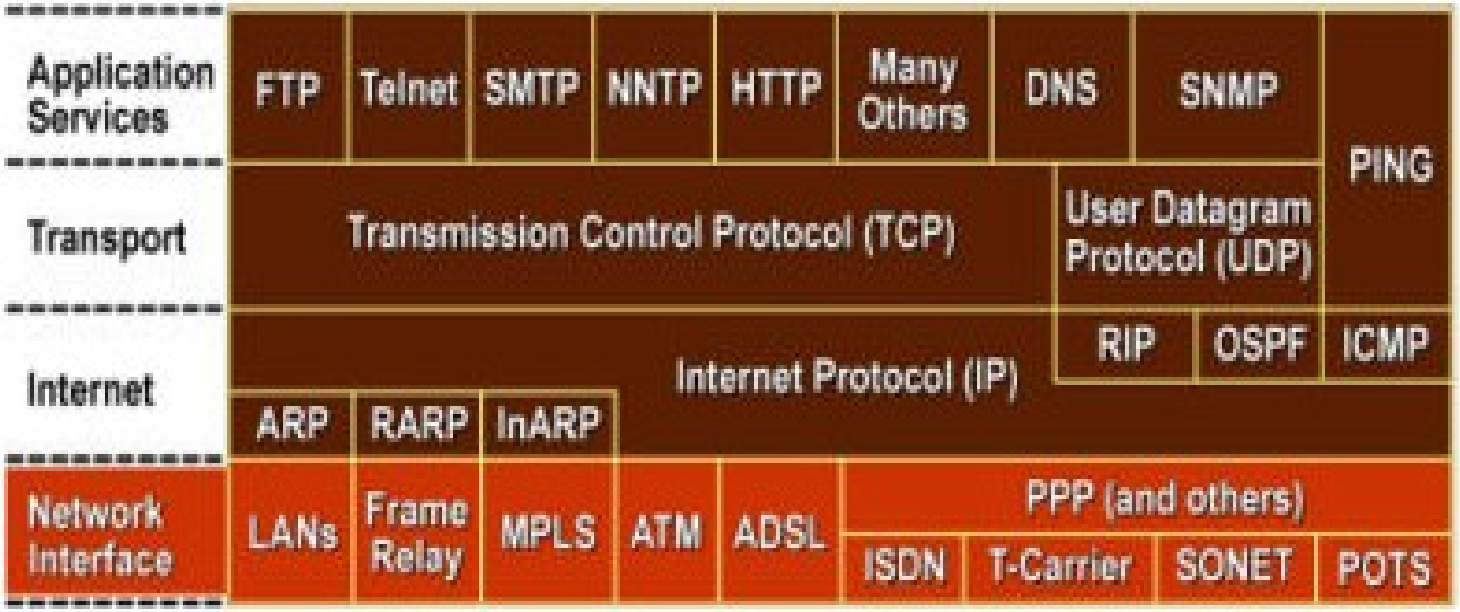
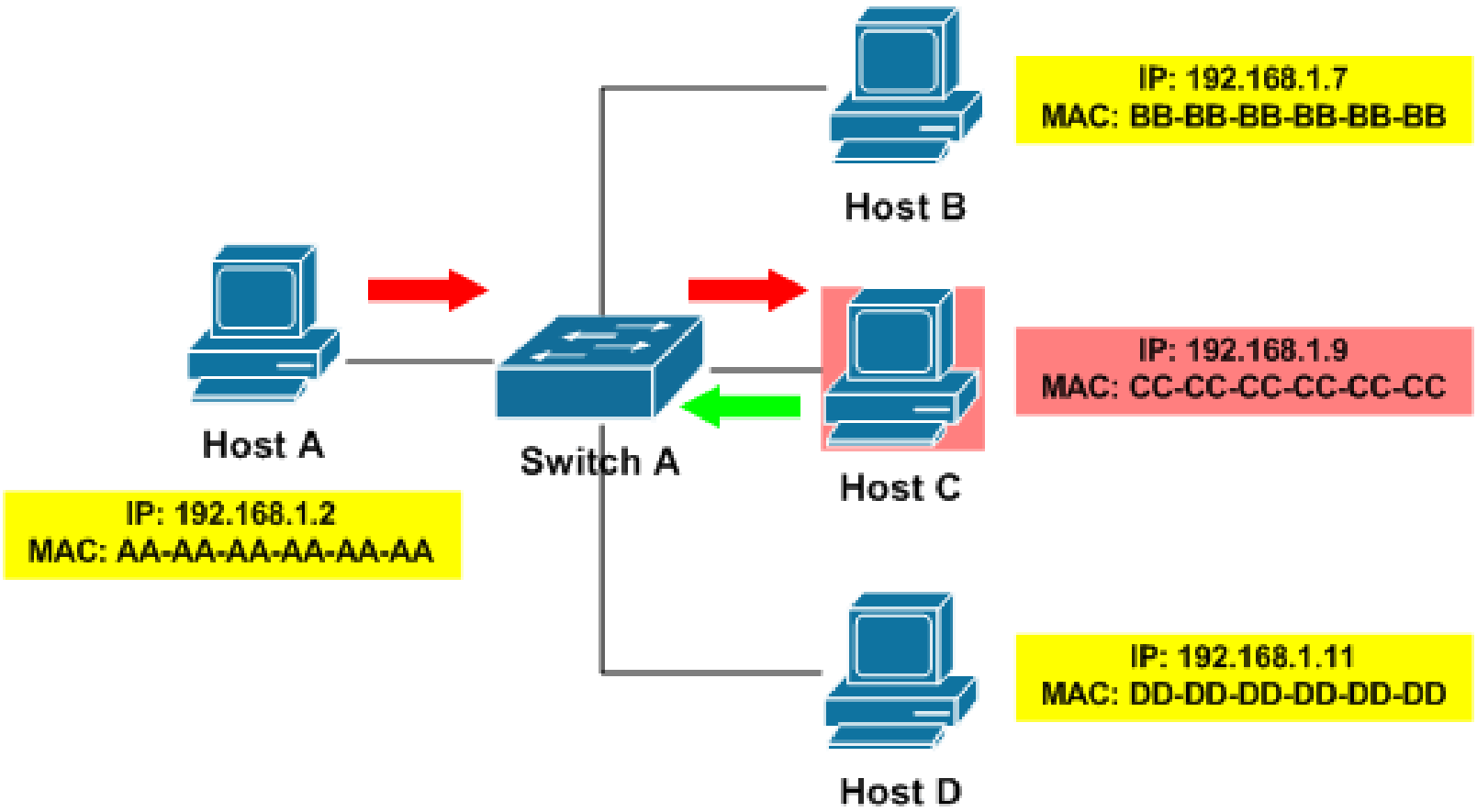
Chương 4 : Các giao thức tầng liên mạng

Giảng viên : Nguyễn Hữu Lộc



Giao thức phân giải địa chỉ ARP
(Address Resolution Protocol)



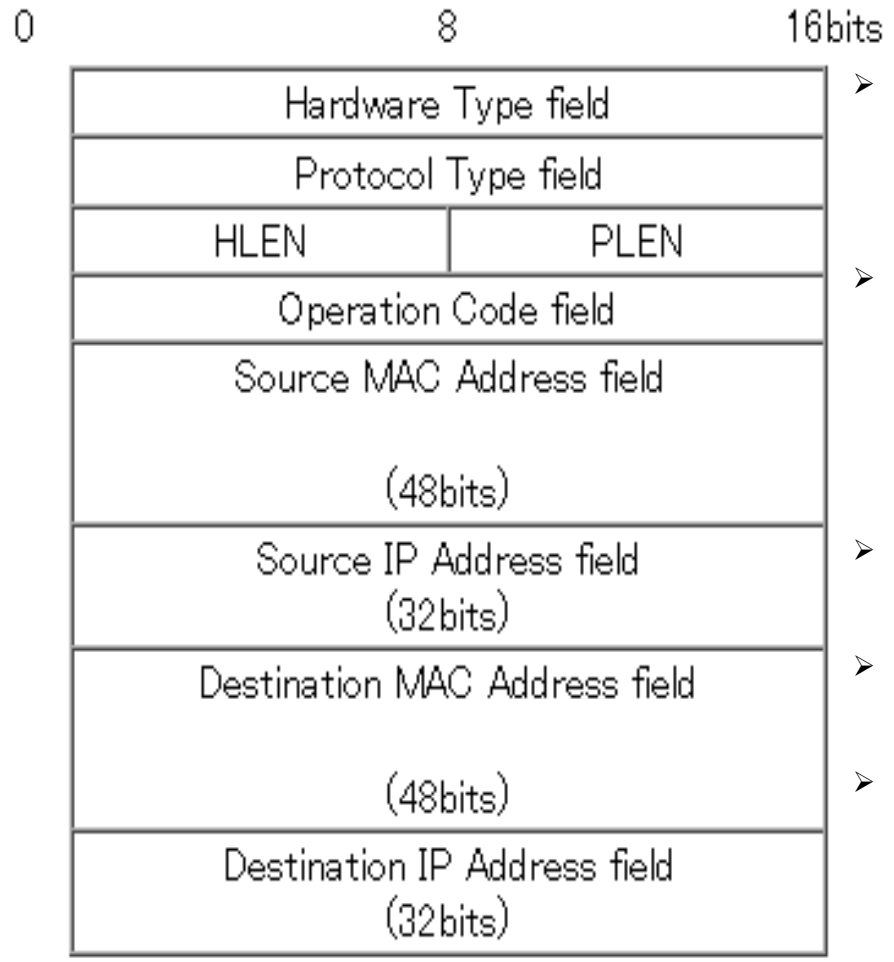
Giới thiệu

- ARP là phương thức phân giải địa chỉ động giữa địa chỉ IP và địa chỉ MAC
- Quá trình thực hiện bằng cách: một thiết bị trong mạng gửi một gói tin broadcast đến toàn mạng yêu cầu thiết bị có địa chỉ IP tương ứng gửi trả lại địa chỉ phần cứng (địa chỉ MAC) của mình

Các loại bản tin ARP

- Có hai dạng bản tin trong ARP : một được gửi từ nguồn đến đích, và một được gửi từ đích tới nguồn.
  - ARP Request : Khởi tạo quá trình, gói tin được gửi từ thiết bị nguồn tới thiết bị đích yêu cầu địa chỉ MAC máy đích
  - ARP Reply : Là quá trình đáp trả gói tin ARP Request, được gửi từ máy đích đến máy nguồn kèm theo địa chỉ MAC máy đích

Cấu trúc khung ARP



HLEN: Hardware (MAC) address Length field
PLEN: Protocol (IP) address Length field

- Hardware Type field : chỉ định loại giao thức mạng (Ethernet : 1)
- Protocol Type field : chỉ định loại giao thức tầng liên mạng (giao thức IP : 0x0800)
- HLEN: chiều dài địa chỉ vật lý (byte)
- PLEN: chiều dài địa chỉ IP (byte)
- Operation Code field : chỉ định hoạt động mà người gửi thực hiện (ARP Request : 1, ARP Reply: 2)
- Các trường còn lại là địa chỉ MAC và IP của máy nguồn và máy đích

Cấu trúc khung ARP

Hardware Type "0001" (Hexadecimal number)	
Protocol Type "0800" (Hexadecimal number)	
HLEN "48" (Decimal number)	PLEN "32" (Decimal number)
Operation Code "1" (Decimal number)	
Source MAC Address (48bits) "A's MAC address"	
Source IP Address (32bits) "A's IP address"	
Destination MAC Address (48bits) Enter "0" because it is unknown.	
Destination IP Address (32bits) "K's IP address"	

A → K
ARP Request

Hardware Type "0001" (Hexadecimal number)	
Protocol Type "0800" (Hexadecimal number)	
HLEN "48" (Decimal number)	PLEN "32" (Decimal number)
Operation Code "2" (Decimal number)	
Source MAC Address (48bits) "K's MAC address"	
Source IP Address (32bits) "K's IP address"	
Destination MAC Address (48bits) "A's MAC address"	
Destination IP Address (32bits) "A's IP address"	

K → A
ARP Reply

ARP Caching

- ARP là một giao thức phân giải địa chỉ động. Quá trình gửi gói tin Request và Reply sẽ tiêu tốn băng thông mạng. Chính vì vậy càng hạn chế tối đa việc gửi gói tin Request và Reply sẽ càng góp phần làm tăng khả năng hoạt động của mạng.Từ đó sinh ra nhu cầu của ARP Caching
- ARP Cache có dạng giống như một bảng tương ứng giữa địa chỉ MAC và địa chỉ IP. Có hai cách đưa các thành phần tương ứng vào bảng ARP : Static and Dynamic ARP Cache Entries

ARP Caching

- Static ARP Cache Entries: Đây là cách mà các thành phần tương ứng trong bảng ARP được đưa vào lần lượt bởi người quản trị. Công việc được tiến hành một cách thủ công
- Dynamic ARP Cache Entries: Đây là quá trình mà các thành phần địa chỉ MAC/IP được đưa vào ARP cache một cách hoàn toàn tự động bằng phần mềm sau khi đã hoàn tất quá trình phân giải địa chỉ. Chúng được lưu trong cache trong một khoảng thời gian và sau đó sẽ được xóa đi

ARP Caching

- Các thông tin trong static cache sẽ không tự động xóa trong các chu kỳ cập nhật ARP cache, chỉ bị xóa đi khi máy được khởi động lại
- Các thông tin trong dynamic cache sẽ được tự động xóa sau một khoảng thời gian thường là 10 hoặc 20 phút. Lần sử dụng sau, thông tin sẽ được cập nhật trở lại

Cơ chế hoạt động

- **1. Source Device Checks Cache** : Trong bước này, thiết bị sẽ kiểm tra cache (bộ đệm) của mình. Nếu đã có địa chỉ IP đích tương ứng với MAC nào đó rồi thì lập tức chuyển gói tin đến máy đích
- **2. Source Device Generates ARP Request Message** : Bắt đầu khởi tạo gói tin ARP Request với các trường địa chỉ theo cấu trúc khung ARP
- **3. Source Device Broadcasts ARP Request Message** : Thiết bị nguồn quảng bá gói tin ARP Request trên toàn mạng

Cơ chế hoạt động

- **4. Local Devices Process ARP Request Message** : Các thiết bị trong mạng đều nhận được gói tin ARP Request. Gói tin được xử lý bằng cách các thiết bị đều nhìn vào trường địa chỉ Destination IP Address. Nếu trùng với địa chỉ của mình thì tiếp tục xử lý, nếu không thì hủy gói tin

Cơ chế hoạt động

- **5. Destination Device Generates ARP Reply Message** : Thiết bị với IP trùng với IP trong trường Destination IP Address sẽ bắt đầu quá trình khởi tạo gói tin ARP Reply bằng cách lấy các trường Source MAC Address và Source IP Address trong gói tin ARP nhận được đưa vào làm địa chỉ đích trong gói tin gửi đi. Đồng thời thiết bị sẽ lấy địa chỉ MAC của mình để đưa vào trường Source MAC Address trong gói tin ARP gửi đi

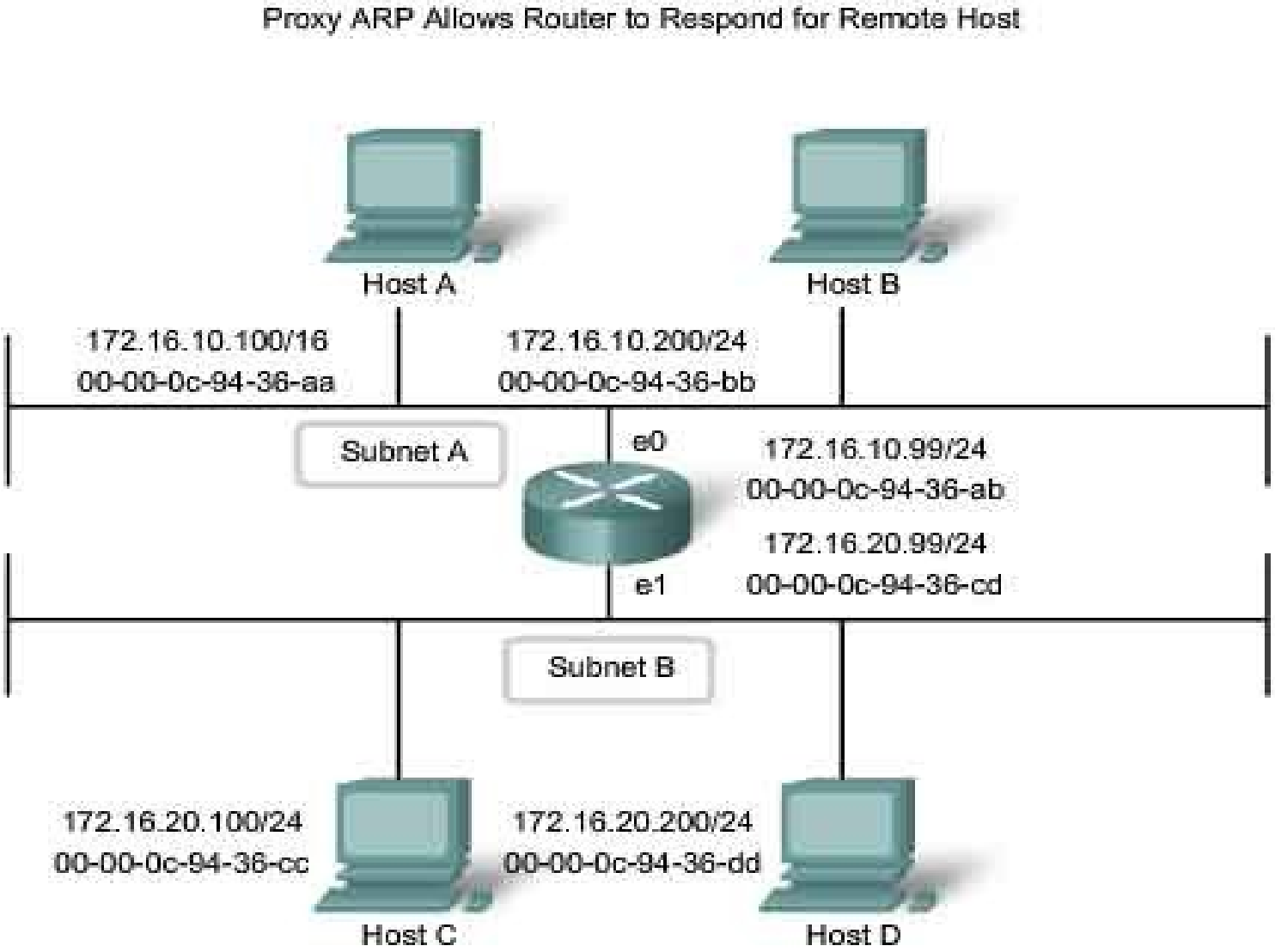
Cơ chế hoạt động

- **6. Destination Device Updates ARP Cache** : Thiết bị đích (thiết bị khởi tạo gói tin ARP Reply) đồng thời cập nhật bảng ánh xạ địa chỉ IP và MAC của thiết bị nguồn vào bảng ARP cache của mình để giảm bớt thời gian xử lý cho các lần sau
- **7. Destination Device Sends ARP Reply Message** : Thiết bị đích bắt đầu gửi gói tin Reply đã được khởi tạo đến thiết bị nguồn. Gói tin reply là gói tin gửi unicast

Cơ chế hoạt động

- **8. Source Device Processes ARP Reply Message** : Thiết bị nguồn nhận được gói tin reply và xử lý bằng cách lưu trường Source MAC Address trong gói reply như địa chỉ phần cứng của thiết bị đích
- **9. Source Device Updates ARP Cache** : Thiết bị nguồn update vào ARP cache của mình giá trị tương ứng giữa địa chỉ network và địa chỉ MAC của thiết bị đích. Lần sau sẽ không còn cần tới request

Proxy ARP


Proxy ARP Allows Router to Respond for Remote Host
Host A
Host B
172.16.10.100/16
00-00-0c-94-36-aa
172.16.10.200/24
00-00-0c-94-36-bb
Subnet A
e0
172.16.10.99/24
00-00-0c-94-36-ab
172.16.20.99/24
00-00-0c-94-36-cd
e1
Subnet B
172.16.20.100/24
00-00-0c-94-36-cc
172.16.20.200/24
00-00-0c-94-36-dd
Host C
Host D

Proxy ARP

- ARP được thiết kế cho các thiết bị nằm trong nội mạng, có tính chất local
- Hai thiết bị A và B bị chia cắt bởi 1 router thì chúng sẽ được coi như là không local với nhau nữa. Khi A muốn gửi thông tin đến B, A sẽ không gửi trực tiếp được đến B theo địa chỉ MAC vì A không thể quảng bá bản tin ARP Request qua Router được

Hoạt động của Proxy ARP

- Router nằm giữa 2 mạng local sẽ được cấu hình để đáp ứng các gói tin broadcast gửi từ A thay cho B
- Router sẽ không gửi cho A địa chỉ MAC của B, vì dù thế nào A và B cũng nằm trên hai mạng khác nhau và không thể gửi trực tiếp đến nhau được

Hoạt động của Proxy ARP

- Thay vào đó router sẽ gửi cho A các địa chỉ MAC của chính router. A sau đó sẽ gửi các gói tin cho router, và router sẽ forward sang cho B
- Quá trình cũng hoàn toàn diễn ra tương tự khi B muốn gửi thông tin cho A, hay cho bất cứ thiết bị nào mà đích đến của gói tin là một thiết bị ở một mạng khác.

Giao thức RARP
(Reverse Address Resolution Protocol)

- Giao thức RARP hay còn gọi là giao thức phân giải địa chỉ ngược là một giao thức mạng máy tính được sử dụng bởi một máy chủ yêu cầu giao thức Internet(IPv4) dùng để xác định địa chỉ IP(địa chỉ logic) từ địa chỉ vật lý của thiết bị
- Được sử dụng bởi các trạm làm việc không đĩa cứng do đó không lưu cấu hình mạng

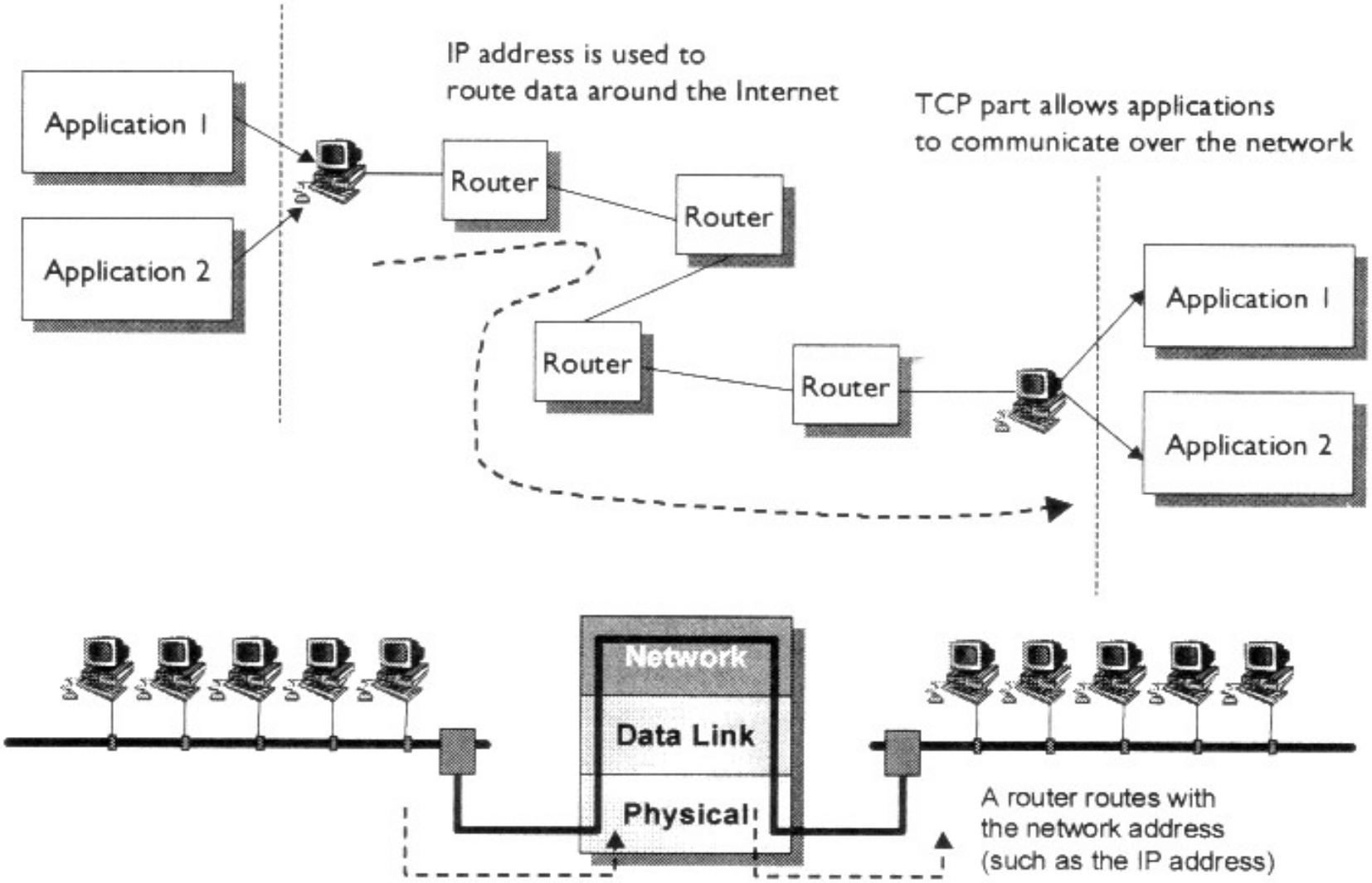
Giao thức RARP
(Reverse Address Resolution Protocol)

- Trước khi có thể nối kết đến được server, các trạm làm việc cần phải biết được địa chỉ IP của nó. Giao thức RARP được dùng trong trường hợp này
- RARP sử dụng cùng định dạng yêu cầu của ARP nhưng trường Operation có giá trị là 3 cho yêu cầu và 4 cho trả lời.

Giao thức RARP
(Reverse Address Resolution Protocol)

- Trên server duy trì một bảng mô tả mối tương quan giữa địa chỉ vật lý và địa chỉ IP của các máy trạm
- Khi nhận được yêu cầu RARP, server tìm trong bảng địa chỉ và trả về địa chỉ IP tương ứng cho máy trạm đã gởi yêu cầu.
- Hiện nay giao thức RARP đã được thay thế bằng các giao thức BOOTP, DHCP

Giao thức Internet
(Internet Protocol - IP)



Giao thức Internet
(Internet Protocol - IP)

- IP là giao thức không liên kết có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.
- Chức năng chủ yếu của IP là cung cấp các dịch vụ Datagram và các khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu với phương thức chuyển mạch gói IP Datagram
- Thực hiện tiến trình định địa chỉ và chọn đường

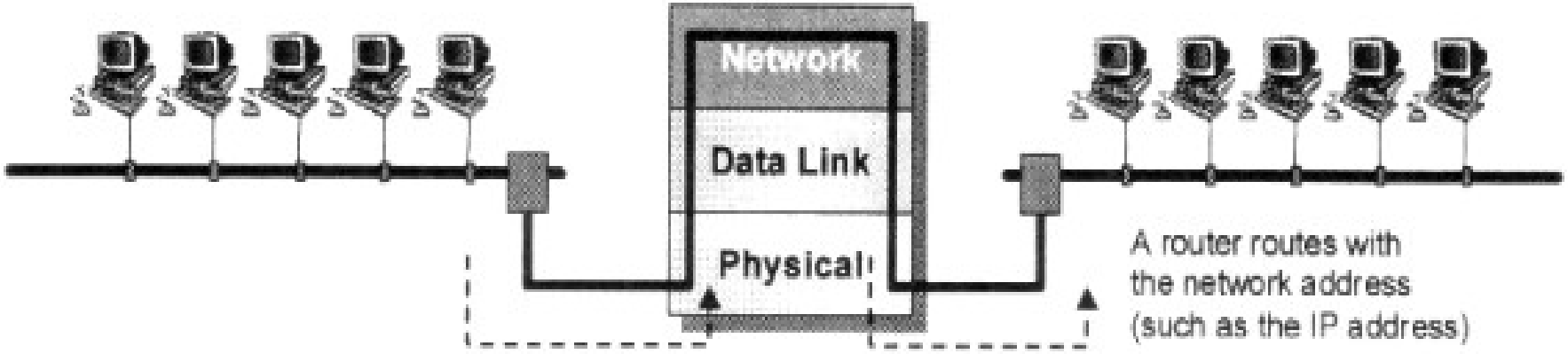
Giao thức Internet
(Internet Protocol - IP)

- Dữ liệu trong một liên mạng IP được gửi theo các khối được gọi là các gói (packet hoặc datagram)
- Giao thức IP cung cấp một dịch vụ gửi dữ liệu không đảm bảo, nghĩa là nó hầu như không đảm bảo gì về gói dữ liệu. Gói dữ liệu có thể đến nơi mà không còn nguyên vẹn, nó có thể đến không theo thứ tự , nó có thể bị trùng lặp hoặc bị mất hoàn toàn

Giao thức Internet
(Internet Protocol - IP)

- Khi giao thức IP được khởi động, nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Các bước hoạt động của IP



Các bước hoạt động của IP

- Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:
  - Tạo một IP datagram dựa trên tham số nhận được.
  - Tính checksum và ghép vào header của gói tin.
  - Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
  - Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Các bước hoạt động của IP

- Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:
  - Tính chesksum, nếu sai thì loại bỏ gói tin.
  - Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.
  - Ra quyết định chọn đường.
  - Phân đoạn gói tin, nếu cần.
  - Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.
  - Chuyển datagram xuống tầng dưới để chuyển qua mạng.

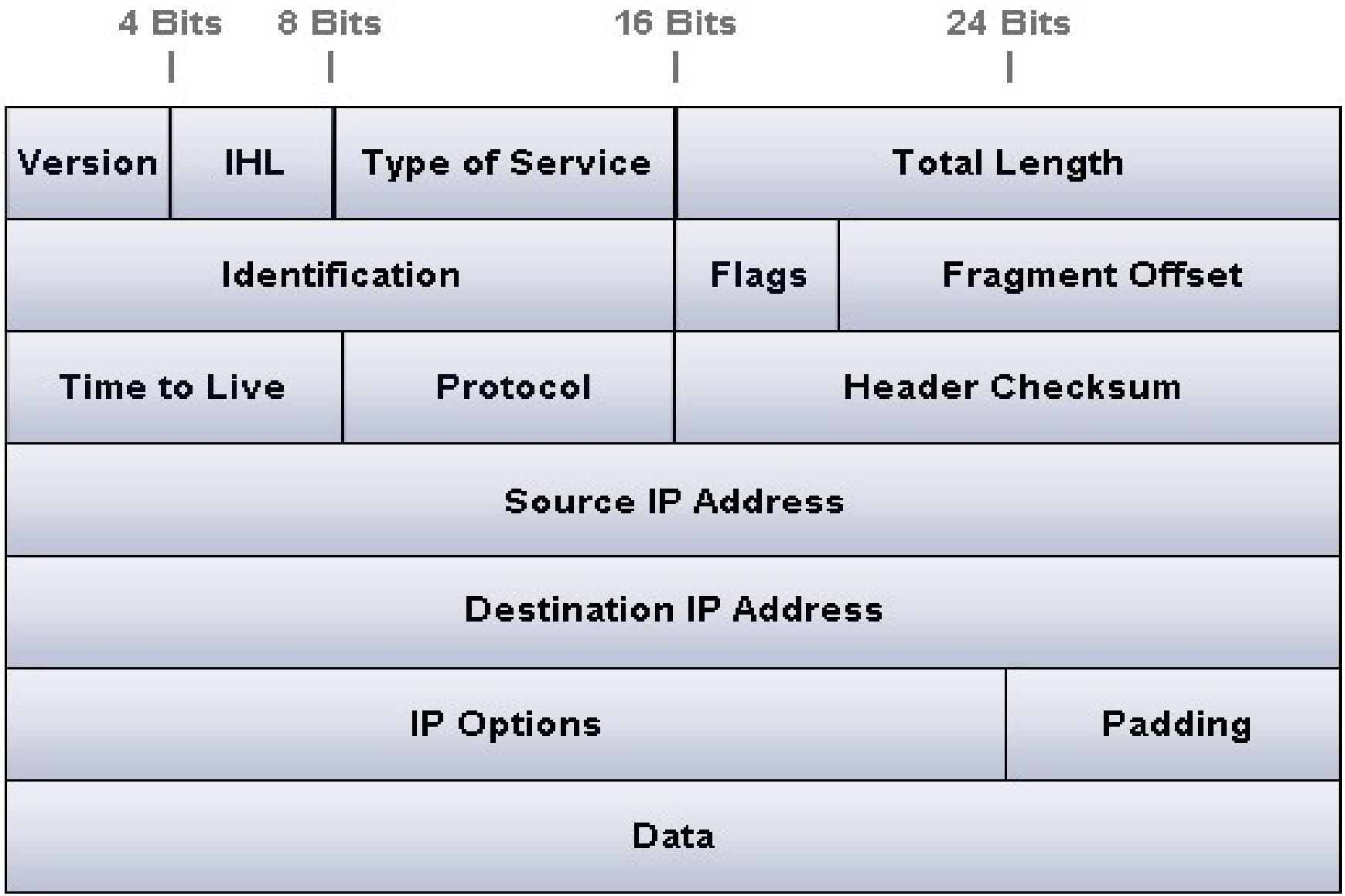
Các bước hoạt động của IP

- Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ được thực hiện bởi các công việc sau:
  - Tính checksum. Nếu sai thì loại bỏ gói tin.
  - Tập hợp các đoạn của gói tin (nếu có phân đoạn)
  - Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

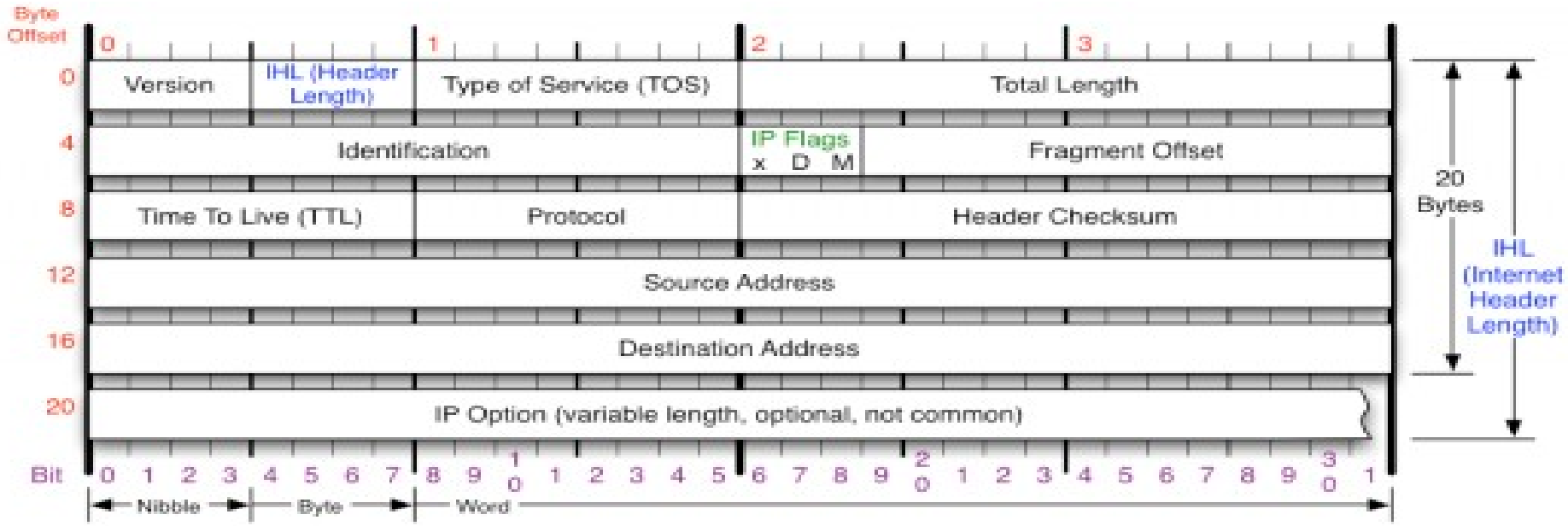
Khuôn dạng gói tin IP

- Các gói dữ liệu IP được gọi là các Datagram
- IPv4 datagram được chia làm 2 phần: header và payload.
  - Phần header lưu trữ thông tin của địa chỉ và các trường điều khiển
  - Phần payload mang dữ liệu thật sự cần truyền.

Khuôn dạng gói tin IP



IPv4 Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

Khuôn dạng gói tin IP

Trường	Size (bits)	Mô tả
Version	4	phiên bản IP dùng để tạo ra IP datagram. Với IPv4,đương nhiêntrường này có giá trị 4. Mục đích của trường này là đảm bảo tương thích giữa các thiết bị sử dụng phiên bản IP khác nhau.Thông thường,các thiết bị sử dụng phiên bản IP cũ sẽ từ chối IP datagram đươc tạo ra từ phiên bản mới hơn,do các phiên bản cũ không thể phiên dịch một cách chính xác IP datagram của phiên bản mới tạo ra
IHL	4	Định ra độ dài phần header, tính theo 32-bit words.Nó cũng bao gồm độ dài trường option và padding.Thông thường giá trị của trường này khi không có option là 5 (5 32-bit words = 5*4 = 20 bytes).

Khuôn dạng gói tin IP

Trường	Size (bits)	Mô tả
TOS	8	Type Of Service (TOS): Trường này được tạo ra để mang thông tin về chất lượng dịch vị,như ưu tiên chuyển Các trường trong TOS +Precedence(3 bits):Định ra mức độ ưu tiên của IP datagram với mức độ từ thấp đến cao +D(1 bit): nếu bit D = 1: yêu cầu truyền gấp +T(1 bit) : nếu bit T = 1: yêu cầu truyền với đường truyền chất lượng cao +R(1 bit) : nếu bit R = 1: yêu cầu truyền đảm bảo +Reserved(2 bits) : không dùng

Khuôn dạng gói tin IP

Trường	Size (bits)	Mô tả
Total Length (TL)	16	Tổng độ dài của IP datagram, tính theo bytes.Độ dài tối đa của 1 IP datagram là 65,535 bytes,hầu hết là nhỏ hơn nhiều
Identif-ication	16	Định danh IP datagram để xác định IP datagram là duy nhất trên mạng
Flags	3	Gồm 3 trường nhỏ +Reserved(1 bit):không dùng +DF(1 bit) : Don't Fragment:nếu là 1 thì IP datagram không bị phân mảnh +MF(1 bit) : More Fragment:nếu là 1 thì vẫn còn Fragment
Fragment Offset	13	Khi có sự phân mảnh, trường này sẽ có giá trị offset, hay là vị trí của mảnh(Fragment),thông thường là bội số của 8. Fragment đầu tiên có giá trị 0.

Khuôn dạng gói tin IP

Trường	Size (bits)	Mô tả
TTL	4	Time To Live (TTL): Định ra thời gian IP datagram được sống trên mạng,dựa vào số trạm trung gian (router hop).Khi qua mỗi router,giá trị TTL sẽ giảm đi 1.Nếu giá trị TTL trở về 0,router sẽ discard nó
Protocol	4	Định ra giao thức dùng trong IP datagram,một số giao thức thông dụng 01h 1:ICMP 02h 2:IGMP 06h 6:TCP 11h 17:UDP
Header Checksum	16	Header Checksum:Dùng để kiểm tra xem IP datagram có bị lỗi trên đường truyền không

More Protocols

Khuôn dạng gói tin IP

Trường	Size (bits)	Mô tả
Source Address	32	Địa chỉ IP nơi gửi. Địa chỉ này được giữ nguyên trong suốt quá trình truyền.
Destination Address	32	Địa chỉ IP nơi nhận. Địa chỉ này được giữ nguyên trong suốt quá trình truyền.
Options	Variable	Lựa chọn,độ dài phần option có thể thay đổi
Padding	Variable	Nếu có nhiều option,mà số bit ko phải là bội số của 32,các bit 0 sẽ được thêm lót để số bit là bội số 32(4 bytes)
Data	Variable	Dữ liệu

Phân mảnh và ghép gói tin IP

- Giá trị Maximum Transmission Unit (MTU) của một mạng là kích thước tối đa của một gói tin IP được chuyển đi trong mạng đó (bao gồm của phần header và phần dữ liệu)
  - Ví dụ, MTU của Ethernet là 1500 byte; các giao thức trên data link layer khác có thể có các giá trị MTU khác, ví dụ Token ring có MTU là 4464 byte, X.25 là 576 byte

Phân mảnh và ghép gói tin IP

- Khi một gói tin IP được gửi từ một mạng có MTU lớn hơn sang một mạng có MTU nhỏ hơn, gói tin này phải được phân mảnh thành nhiều phần nhỏ hơn (với DF=0)
- Tất cả các phần phân mảnh sẽ được ghép lại tại đích đến của gói tin

Phân mảnh và ghép gói tin IP

- Các thông tin trong phần header hỗ trợ cho việc phân mảnh gói tin như sau: Identification(16 bit), Flags(3 bit), Fragment Offset(13 bit)
  - Ví dụ: Một gói tin được truyền tới một mạng với MTU là 576 byte. Gói tin này có IP header chiếm 20 byte và phần dữ liệu chiếm 1504 byte. Gói tin này cần được phân mảnh như sau :
    - Chiều dài tối đa của một phân mảnh là 576-20=556 byte
    - Ta thiết lập giá trị tối đa này là 552 để thỏa mãn yêu cầu về bội số của 8

Phân mảnh và ghép gói tin IP

- Ví dụ về phân mảnh gói tin

	Tổng chiều dài	ID	MF	Fragment Offset
Gói tin gốc	1504	x	0	0
Phân mảnh 1	552	x	1	0
Phân mảnh 2	552	x	1	69
Phân mảnh 3	400	x	0	138

Giao thức ICMP
(Internetwork Control Message Protocol)

- Giao thức ICMP (Internetwork Control Message Protocol) cho phép việc thử nghiệm và khắc phục các sự cố của giao thức TCP/IP.
- ICMP định nghĩa các các thông điệp được dùng để xác định khi nào một hệ thống mạng có thể phân phối các gói tin
- ICMP được sử dụng trong một vài trường hợp, một gateway hoặc một máy đích sẽ cần giao tiếp với máy nguồn để báo cáo lại các lỗi xảy ra trong quá trình xử lý gói tin

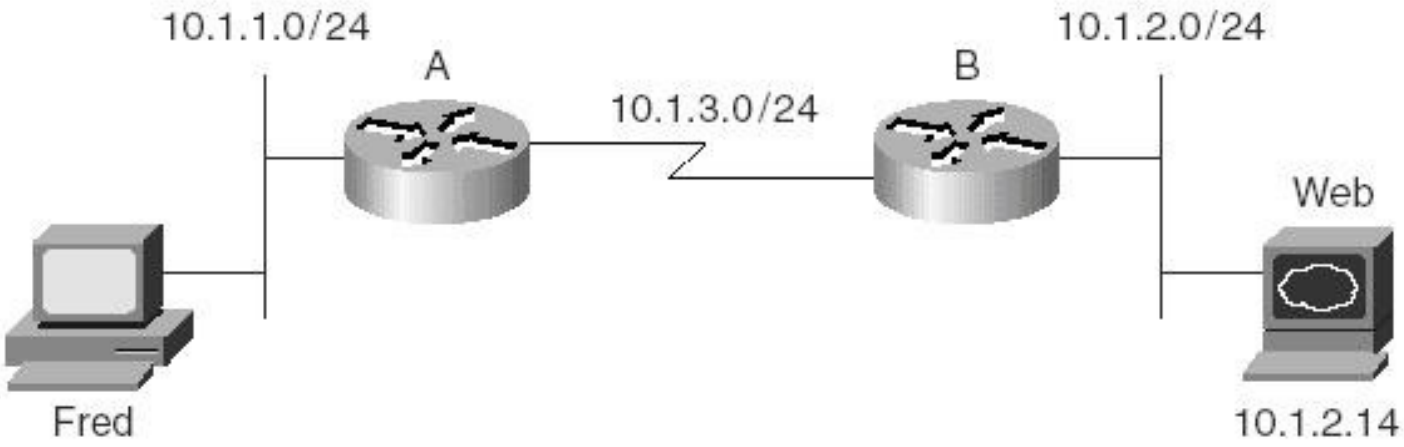
Giao thức ICMP
(Internetwork Control Message Protocol)

- Một số thông điệp ICMP

Loại thông điệp ICMP	Mục đích
Destination Unreachable	Thông báo cho máy nguồn là có một vấn đề trong phân phối gói tin
Time Exceed	Thời gian để chuyển một gói tin là quá lớn. Gói tin bị loại bỏ.
Source Quench	Máy nguồn đang gửi dữ liệu ở mức nhanh hơn mà máy đích có thể xử lý. Thông điệp này yêu cầu máy gửi gửi chậm lại.
Redirect	Được dùng bởi một router thông báo cho một host dùng một địa chỉ router khác tốt hơn cho những lần gửi khác sắp tới.
Echo	Được dùng bởi lệnh ping để kiểm tra kết nối.
Address/mask request/reply	Được dùng để học và để truy vấn địa chỉ IP/ mask được dùng.
Router Advertisement and Selection	Được dùng để cho phép các host học địa chỉ IP của các router gắn vào subnet.

Thông điệp ICMP Unreachable

- Khi một thiết bị nhận ra rằng một gói tin không thể được đưa đến địa chỉ đích ghi trong gói tin, thiết bị sẽ gửi ngược về một thông điệp ICMP Unreachable



Thông điệp ICMP Unreachable

- Các giá trị của thông điệp ICMP Unreachable:

Unreachable code	Ý nghĩa	Ví dụ
Network Unreachable	Router không có đường đi trong trong bảng định tuyến trùng với địa chỉ đích của gói tin	Router A không có tuyến đi về 10.1.2.0. Router A gửi Unreachable về Fred
Host Unreachable	Gói tin đã đến được router cuối cùng, nhưng host không trả lời ARP request	Máy web bị tắt. Router B gửi cho Fred một thông điệp host unreachable
Can't fragment	Một gói tin có kích thước lớn hơn MTU nhưng gói tin có bit DF (Don't fragment) được thiếp lập.	Router A có MTU là 1500 bytes. Gói tin có kích thước 1600 bytes và có DF=1.
Protocol Unreachable	Gói tin đã đến được host đích nhưng trên host đích không có cài giao thức đó	Host Web không có cài giao thức TCP. Host web trả lời Unreachable cho Fred.
Port Unreachable	Gói tin được gửi đến host đích. Không có tiến trình nào lắng nghe trên port đích	Máy web đang làm việc nhưng web server không hoạt động. Máy web gửi port unreachable về cho Fred.

Thông điệp Time Exceeded ICMP

- Thông điệp ICMP Time Exceed lưu ý một host khi một gói tin mà máy đó đã gửi bị loại bỏ bởi vì bị hết thời gian (timeout)
- Khi truyền dữ liệu trên mạng thì các gói tin truyền cần phải được định nghĩa thời gian truyền, để ngăn cản việc gói tin đó được truyền mãi sẽ gây ra lặp vòng, mỗi một gói tin đều có một IP header trong đó có một trường được gọi là TTL (Time to Live)

Thông điệp Time Exceeded ICMP

- Router trừ giá trị TTL của gói tin đi 1 mỗi khi router chuyển một gói tin đi. Nếu một router nhận được một gói tin và sau đó trừ giá trị TTL xuống còn 0, router sẽ loại bỏ gói tin
- Router thực hiện loại bỏ gói tin sẽ làm thêm một động tác là gửi ngược về một thông điệp ICMP Time Exceed đến máy gửi ban đầu.

Các giao thức tầng liên mạng