



Bộ giao thức liên mạng (IPs - Internet Protocols)

Bởi:
unknown

Bộ giao thức liên mạng (IPs - Internet Protocols)

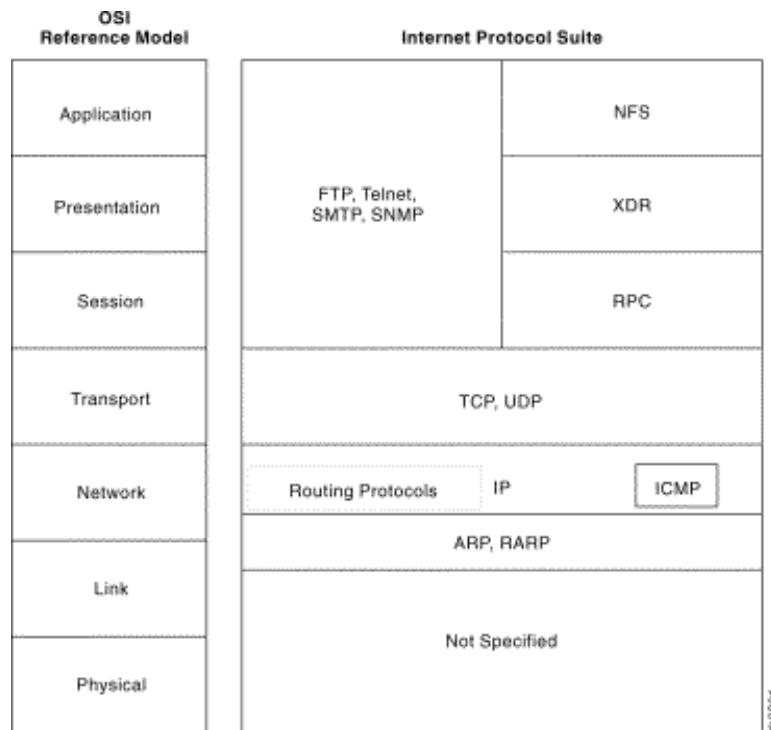
Giới thiệu

Các giao thức liên mạng là bộ giao thức cho các hệ thống mở nổi tiếng nhất trên thế giới bởi vì chúng có thể được sử dụng để giao tiếp qua bất kỳ các liên mạng nào cũng như thích hợp cho các giao tiếp trong mạng LAN và mạng WAN. Các giao thức liên mạng bao gồm một bộ các giao thức truyền thông, trong đó nổi tiếng nhất là Giao thức điều khiển truyền tải (TCP - Transmission Control Protocol) và Giao thức liên mạng (IP – Internet Protocol) hoạt động ở tầng 4 và tầng 3 trên mô hình OSI. Ngoài hai giao thức này, bộ giao thức IP còn đặc tả nhiều giao thức cho tầng ứng dụng, ví dụ như giao thức cho dịch vụ thư điện tử, giao thức mô phỏng thiết bị đầu cuối và giao thức truyền tải tập tin.

Bộ giao thức liên mạng lần đầu tiên được phát triển vào giữa những năm của thập niên 70 khi Văn phòng các dự án nghiên cứu chuyên sâu của bộ quốc phòng Mỹ (DARPA - Defense Advanced Research Projects Agency) quan tâm đến việc xây dựng một mạng chuyển mạch gói (packet-switched network) cho phép việc trao đổi thông tin giữa các hệ thống máy tính khác nhau của các viện nghiên cứu trở nên dễ dàng hơn. Với ý tưởng nổi các hệ thống máy tính không đồng nhất lại với nhau, DARPA đã cấp kinh phí nghiên cứu cho đại học Stanford, Bolt, Beranek, and Newman (BBN) về vấn đề này. Kết quả của những nỗ lực phát triển của dự án này là bộ giao thức Liên mạng đã được hoàn thành vào những năm cuối của thập niên bảy mươi.

Sau đó TCP/IP được tích hợp vào hệ điều hành UNIX phiên bản BSD (Berkeley Software Distribution) trở thành nền tảng cho mạng Internet và dịch vụ WWW (World Wide Web).

Bộ giao thức liên mạng (IPs - Internet Protocols)



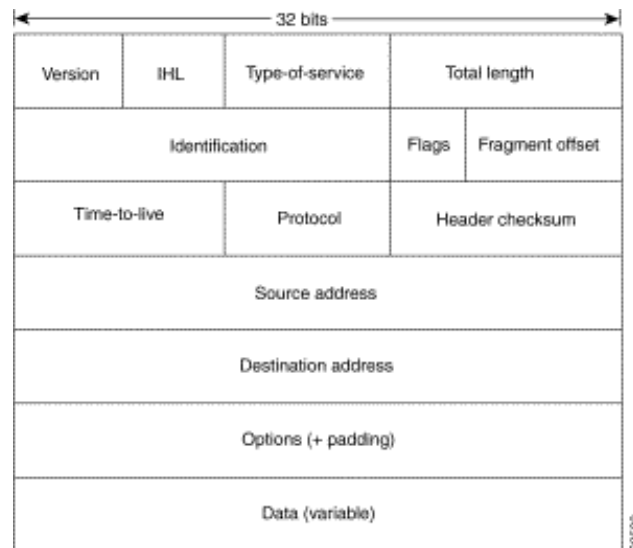
Kiến trúc của mạng TCP/IP so với mô hình OSI (H6.29)

Giao thức liên mạng IP (Internet Protocol)

Giao thức liên mạng, thường gọi là giao thức IP (Internet Protocol) là một giao thức mạng hoạt động ở tầng 3 của mô hình OSI, nó qui định cách thức định địa chỉ các máy tính và cách thức chuyển tải các gói tin qua một liên mạng. IP được đặc tả trong bảng báo cáo kỹ thuật có tên RFC (Request For Comments) mã số 791 và là giao thức chủ yếu trong Bộ giao thức liên mạng. Cùng với giao thức TCP, IP trở thành trái tim của bộ giao thức Internet. IP có hai chức năng chính : cung cấp dịch vụ truyền tải dạng không nối kết để chuyển tải các gói tin qua một liên mạng ; và phân mảnh cũng như tập hợp lại các gói tin để hỗ trợ cho tầng liên kết dữ liệu với kích thước đơn vị truyền dữ liệu là khác nhau.

Định dạng gói tin IP (IP Packet Format)

Hình sau mô tả cấu trúc của một gói tin IP



Cấu trúc gói tin IP (H6.30)

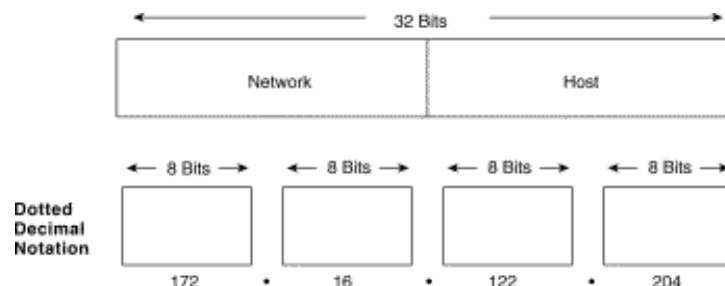
Ý nghĩa của các trường được mô tả như sau:

- **Version (Phiên bản):** Xác định phiên bản của giao thức đang được sử dụng.
- **IP Header Length (Chiều dài của phần tiêu đề):** Xác định chiều dài của phần tiêu đề của gói tin, tính bằng đơn vị là từ - 32 bits (32-bit word).
- **Type-of-Service (Kiểu của dịch vụ):** Đặc tả mức độ quan trọng mà giao thức phía trên muốn xử lý gói tin.
- **Total Length (Tổng chiều dài gói tin):** Đặc tả chiều dài, tính bằng byte, của cả gói tin IP, bao gồm cả phần dữ liệu và tiêu đề.
- **Identification (Số nhận dạng):** Số nguyên nhận dạng gói tin dữ liệu hiện hành. Trường này được sử dụng để ráp lại các phân đoạn của gói tin.
- **Flags (Cờ hiệu):** Gồm 3 bit, bit có trọng số nhỏ để xác định gói tin có bị phân đoạn hay không. Bit thứ 2 xác định có phải đây là phân đoạn cuối cùng của gói tin hay không. Bit có trọng số lớn nhất chưa sử dụng.
- **Fragment Offset (Vị trí của phân đoạn):** Biểu thị vị trí của phân đoạn dữ liệu so với vị trí bắt đầu của gói dữ liệu gốc, nó cho phép máy nhận xây dựng lại gói tin ban đầu.
- **Time-to-Live (Thời gian sống của gói tin):** Lưu giữ bộ đếm thời gian, giá trị sẽ được giảm dần đến khi nó có giá trị là 0 thì gói tin sẽ bị xóa. Điều này giúp ngăn ngừa tình trạng gói tin được truyền đi lòng vòng không bao giờ đến được đích.
- **Protocol (Giao thức):** Biểu hiện giao thức ở tầng trên sẽ nhận gói tin khi nó đã được giao thức IP xử lý.
- **Header Checksum (Tổng kiểm tra lỗi tiêu đề):** kiểm tra tính toàn vẹn của phần tiêu đề.
- **Source Address: Địa của máy gửi gói tin.**
- **Destination Address: Địa chỉ của máy nhận gói tin.**

- **Options:** Tùy chọn cho phép để hỗ trợ một số vấn đề, chẳng hạn vấn đề bảo mật.
- **Data:** Chứa dữ liệu của tầng trên gửi xuống cần truyền đi.

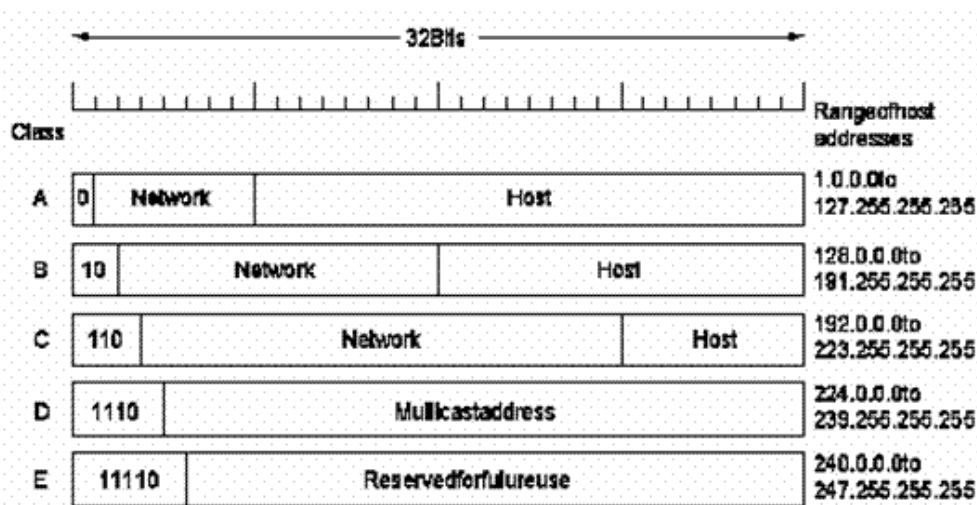
Cấu trúc địa chỉ IP

Mỗi máy tính trên mạng TCP/IP phải được gán một địa chỉ luận lý có chiều dài 32 bits, gọi là địa chỉ IP.



Cấu trúc địa chỉ IP (H6.31)

32 bits của địa chỉ IP được chia thành 2 phần : Phần nhận dạng mạng (network id) và phần nhận dạng máy tính (Host id). Phần nhận dạng mạng được dùng để nhận dạng một mạng và phải được gán bởi Trung tâm thông tin mạng Internet (InterNIC - Internet Network Information Center) nếu muốn nối kết vào mạng Internet. Phần nhận dạng máy tính dùng để nhận dạng một máy tính trong một mạng.



Phân lớp địa chỉ IP (H6.32)

Để dễ dàng cho việc đọc và hiểu bởi con người, 32 bits của địa chỉ IP được nhóm lại thành 4 bytes và được phân cách nhau bởi 3 dấu chấm (.). Giá trị của mỗi bytes được viết lại dưới dạng thập phân, với giá trị hợp lệ nằm trong khoản từ 0 đến 255.

Câu hỏi được đặt ra là bao nhiêu bits dành cho phần nhận dạng mạng và bao nhiêu bits dành cho phần nhận dạng máy tính. Người ta phân các địa chỉ ra thành 5 lớp : A, B, C, D và E. Trong đó, chỉ có lớp A, B và C được dùng cho các mục đích thương mại. Các bits có trọng số cao nhất chỉ định lớp mạng của địa chỉ. Hình sau mô tả cách phân chia lớp cho các địa chỉ IP.

Thông tin chi tiết về các lớp được mô tả như bảng sau :

Lớp	Dạng	Mục đích	Các bits cao nhất	Khoản địa chỉ	Số bit phần nhận dạng mạng / Số bit phần nhận dạng máy tính	Tổng số máy tính trong một mạng
A	N.H.H.H	Cho một số ít các tổ chức lớn	0	1.0.0.0 đến 126.0.0.0	7/24	16.777. 214 ($2^{24} - 2$)
B	N.N.H.H	Cho các tổ chức có kích thước trung bình	10	128.1.0.0 đến 191.254.0.0	14/16	65. 543 ($2^{16} - 2$)
C	N.N.N.H	Cho các tổ chức có kích thước nhỏ	110	192.0.1.0 đến 223.255.254.0	21/8	254 ($2^8 - 2$)
D		Truyền nhóm	1110	224.0.0.0 đến 239.255.255.255		
E		Dành cho thí nghiệm	1111	240.0.0.0 đến 254.255.255.255		

Ghi chú H : Host, N=Network

Một số địa chỉ IP đặc biệt

- Địa chỉ mạng (Network Address): là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 0, được sử dụng để xác định một mạng.

Bộ giao thức liên mạng (IPs - Internet Protocols)

- Ví dụ : 10.0.0.0; 172.18.0.0 ; 192.1.1.0
- Địa chỉ quảng bá (Broadcast Address) : Là địa chỉ IP mà giá trị của tất cả các bits ở phần nhận dạng máy tính đều là 1, được sử dụng để chỉ tất cả các máy tính trong mạng.
 - Ví dụ : 10.255.255.255, 172.18.255.255, 192.1.1.255
- Mặt nạ mạng chuẩn (Netmask) : Là địa chỉ IP mà giá trị của các bits ở phần nhận dạng mạng đều là 1, các bits ở phần nhận dạng máy tính đều là 0. Như vậy ta có 3 mặt nạ mạng tương ứng cho 3 lớp mạng A, B và C là :
 - Mặt nạ mạng lớp A : 255.0.0.0
 - Mặt nạ mạng lớp B : 255.255.0.0
 - Mặt nạ mạng lớp C : 255.255.255.0

Ta gọi chúng là các mặt nạ mạng mặc định (Default Netmask)

Lưu ý : Địa chỉ mạng, địa chỉ quảng bá, mặt nạ mạng không được dùng để đặt địa chỉ cho các máy tính

- Địa chỉ mạng 127.0.0.0 là địa chỉ được dành riêng để đặt trong phạm vi một máy tính. Nó chỉ có giá trị cục bộ (trong phạm vi một máy tính). Thông thường khi cài đặt giao thức IP thì máy tính sẽ được gán địa chỉ 127.0.0.1. Địa chỉ này thông thường để kiểm tra xem giao thức IP trên máy hiện tại có hoạt động không.
- Địa chỉ dành riêng cho mạng cục bộ không nối kết trực tiếp Internet : Các mạng cục bộ không nối kết trực tiếp vào mạng Internet có thể sử dụng các địa chỉ mạng sau để đánh địa chỉ cho các máy tính trong mạng của mình :
 - Lớp A : 10.0.0.0
 - Lớp B : 172.16.0.0 đến 172.32.0.0
 - Lớp C : 192.168.0.0

Ý nghĩa của Netmask

Với một địa chỉ IP và một Netmask cho trước, ta có thể dùng phép toán AND BIT để tính ra được địa chỉ mạng mà địa chỉ IP này thuộc về. Công thức như sau :

Network Address = IP Address & Netmask

Ví dụ : Cho địa chỉ IP = 198.53.147.45 và Netmask = 255.255.255.0. Ta thực hiện phép toán AND BIT (&) hai địa chỉ trên:

	Biểu diễn thập phân	Biểu diễn nhị phân
IP Address	198.53.147.45	11000110 00110101 10010011 00101101
Netmask	255.255.255.0	11111111 11111111 11111111 00000000

Network Address	198.53.147.0	11000110 00110101 10010011 00000000
-----------------	--------------	-------------------------------------

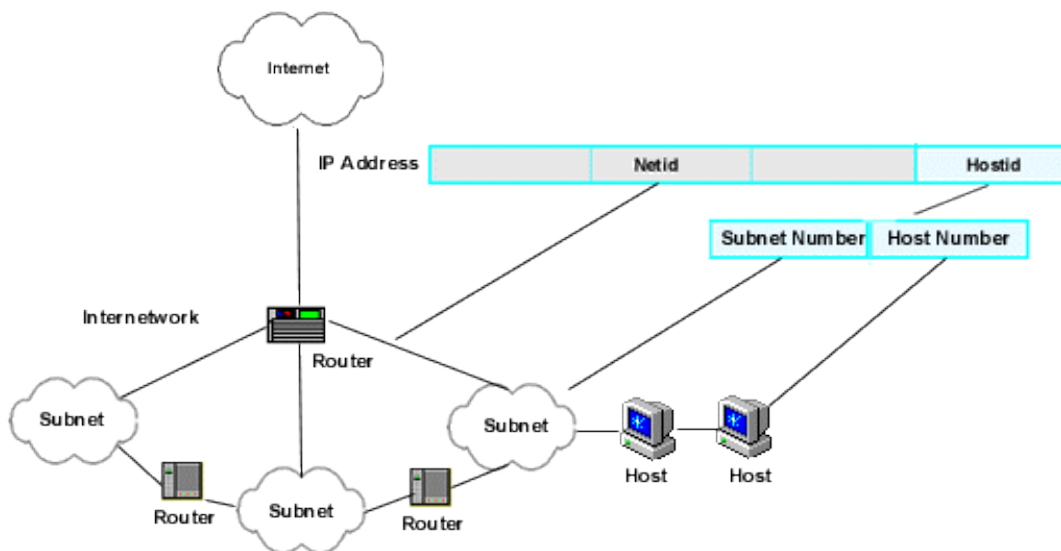
Phân mạng con (Subnetting)

Giới thiệu

Phân mạng con là một kỹ thuật cho phép nhà quản trị mạng chia một mạng thành những mạng con nhỏ, nhờ đó có được các tiện lợi sau :

- Đơn giản hóa việc quản trị : Với sự trợ giúp của các router, các mạng có thể được chia ra thành nhiều mạng con (subnet) mà chúng có thể được quản lý như những mạng độc lập và hiệu quả hơn.
- Có thể thay đổi cấu trúc bên trong của mạng mà không làm ảnh hưởng đến các mạng bên ngoài. Một tổ chức có thể tiếp tục sử dụng các địa chỉ IP đã được cấp mà không cần phải lấy thêm khối địa chỉ mới.
- Tăng cường tính bảo mật của hệ thống : Phân mạng con sẽ cho phép một tổ chức phân tách mạng bên trong của họ thành một liên mạng nhưng các mạng bên ngoài vẫn thấy đó là một mạng duy nhất.
- Cô lập các luồng giao thông trên mạng : Với sự trợ giúp của các router, giao thông trên mạng có thể được giữ ở mức thấp nhất có thể.

Subnetted IP Appearance on the Internetwork



Địa chỉ mạng con đối với thế giới bên ngoài (H6.33)

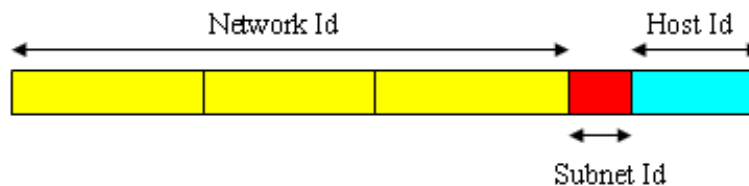
Hình trên mô tả một địa chỉ IP đã được phân mạng con xuất hiện với thế giới Internet bên ngoài và với mạng Intranet bên trong. Internet chỉ đọc phần nhận dạng mạng và các router trên Internet chỉ quan tâm tới việc vạch đường cho các gói tin đến được router giao tiếp giữa mạng Intranet bên trong và mạng Internet bên ngoài. Thông thường ta gọi router này là cửa khẩu của mạng (Gateway). Khi một gói tin IP từ mạng bên ngoài đến router cửa khẩu, nó sẽ đọc phần nhận dạng máy tính để xác định xem gói tin này thuộc

về mạng con nào và sẽ chuyển gói tin đến mạng con đó, nơi mà gói tin sẽ được phân phát đến máy tính nhận.

Phương pháp phân mạng con

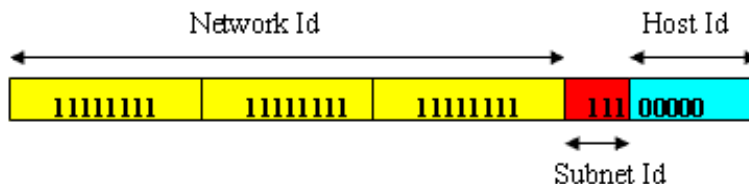
Nguyên tắc chung để thực hiện phân mạng con là :

- Phần nhận dạng mạng (Network Id) của địa chỉ mạng ban đầu được giữ nguyên.
- Phần nhận dạng máy tính của địa chỉ mạng ban đầu được chia thành 2 phần : Phần nhận dạng mạng con (Subnet Id) và Phần nhận dạng máy tính trong mạng con (Host Id).



Cấu trúc địa chỉ IP khi phân mạng con (H6.33)

Để phân mạng con, người ta phải xác định mặt nạ mạng con (subnetmask). Mặt nạ mạng con là một địa chỉ IP mà giá trị các bit ở phần nhận dạng mạng (Network Id) và Phần nhận dạng mạng con (Subnet Id) đều là 1 trong khi giá trị của các bits ở Phần nhận dạng máy tính (Host Id) đều là 0. Hình H6.34 mô tả mặt nạ phân mạng con cho một mạng ở lớp C.



Mặt nạ mạng con khi phân mạng con (H6.34)

Khi có được mặt nạ mạng con, ta có thể xác định địa chỉ mạng con (Subnetwork Address) mà một địa chỉ IP được tính bằng công thức sau :

$$\text{Subnetwork Address} = \text{IP} \& \text{Subnetmask}$$

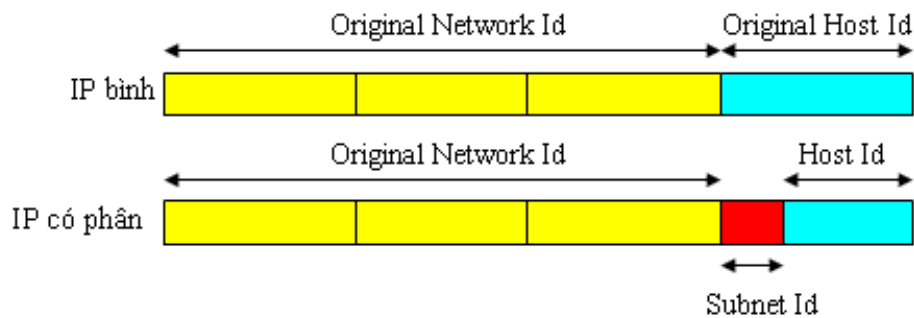
Có hai chuẩn để thực hiện phân mạng con là : Chuẩn phân lớp hoàn toàn (Classfull standard) và chuẩn Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing). Thực tế, CIDR chỉ mới được đa số các nhà sản xuất thiết bị và hệ điều hành mạng hỗ trợ nhưng vẫn chưa hoàn toàn chuẩn hóa.

Phương pháp phân lớp hoàn toàn (Classfull Standard)

Chuẩn này qui định địa chỉ IP khi phân mạng con sẽ gồm 3 phần :

- Phần nhận dạng mạng của địa chỉ ban đầu (Network Id):
- Phần nhận dạng mạng con (Subnet Id) : Được hình thành từ một số bits có trọng số cao trong phần nhận dạng máy tính (Host Id) của địa chỉ ban đầu
- Và cuối cùng là phần nhận dạng máy tính trong mạng con (Host Id) bao gồm các bit còn lại.

Ví dụ : Hình sau mô tả cấu trúc địa chỉ IP lớp C khi thực hiện phân mạng con



Địa chỉ IP phân mạng con theo chuẩn Phân lớp hoàn toàn (H6.35)

Số lượng bits thuộc phần nhận dạng mạng con xác định số lượng mạng con. Giả sử phần nhận dạng mạng con chiếm 4 bits. Như vậy, về mặt lý thuyết ta có thể phân ra thành $2^4=16$ mạng con. Tuy nhiên phần nhận dạng mạng con gồm toàn bit 0 hoặc bit 1 không được dùng để đánh địa chỉ cho mạng con vì nó trùng với địa chỉ mạng và địa chỉ quảng bá của mạng ban đầu.

Ví dụ : Cho địa chỉ mạng lớp C : 192.168.1.0 với mặt nạ mạng mặc định là 255.255.255.0.

Xét trường hợp phân mạng con cho mạng trên sử dụng 2 bits để làm phần nhận dạng mạng con. Mặt nạ mạng trong trường hợp này là 255.255.255.192. Khi đó ta có các địa chỉ mạng con như sau :

Địa chỉ IP	Biểu diễn dạng thập phân	Biểu diễn dạng nhị phân			
Mạng ban đầu	192.168.1.0	1100 0000	1010 1000	0000 0001	0000 0000
Mạng con 1	192.168.1.0	1100 0000	1010 1000	0000 0001	0000 0000

Bộ giao thức liên mạng (IPs - Internet Protocols)

Mạng con 2	192.168.1.64	1100 0000	1010 1000	0010 0001	0100 0000
Mạng con 3	192.168.1.128	1100 0000	1010 1000	0000 0001	1000 0000
Mạng con 4	192.168.1.192	1100 0000	1010 1000	0000 0001	1100 0000

Ta nhận thấy rằng:

- Địa chỉ mạng con thứ nhất 192.168.1.0 trùng với địa chỉ mạng ban đầu.
- Địa chỉ mạng con thứ tư 192.168.1.192 có địa chỉ quảng bá trùng với địa chỉ quảng bá của mạng ban đầu .

Chính vì thế mà hai địa chỉ này (có phần nhận dạng mạng con toàn bit 0 hoặc toàn bit 1) không được dùng để đánh địa chỉ cho mạng con.

Nói tóm lại, với n bits làm phần nhận dạng mạng con ta chỉ có thể phân ra được $2^n - 2$ mạng con mà thôi. Mỗi mạng con cũng có địa chỉ quảng bá. Đó là địa chỉ mà các bits ở phần nhận dạng máy tính đều có giá trị là 1.

Ví dụ :

Địa chỉ IP	Biểu diễn dạng thập phân	Biểu diễn dạng nhị phân			
Mạng con 1	192.168.1.64	1100 0000	1010 1000	0010 0001	0100 0000
Địa chỉ quảng bá	192.168.1.127	1100 0000	1010 1000	0010 0001	01 11 <u>1111</u>
Mạng con 2	192.168.1.128	1100 0000	1010 1000	0000 0001	1000 0000
Địa chỉ quảng bá	192.168.1.191	1100 0000	1010 1000	0000 0001	10 11 <u>1111</u>

Như vậy qui trình phân mạng con có thể được tóm tắt như sau :

- Xác định số lượng mạng con cần phân, giả sử là N .
- Biểu diễn $(N+1)$ thành số nhị phân. số lượng bit cần thiết để biểu diễn $(N+1)$ chính là số lượng bits cần dành cho phần nhận dạng mạng con. Ví dụ $N=6$, khi

đó biểu diễn của (6+1) dưới dạng nhị phân là 111. Như vậy cần dùng 3 bits để làm phần nhận dạng mạng con

- Tạo mặt nạ mạng con
- Liệt kê tất cả các địa chỉ mạng con có thể, trừ hai địa chỉ mà ở đó phần nhận dạng mạng con toàn các bits 0 và các bit 1.
- Chọn ra N địa chỉ mạng con từ danh sách các mạng con đã liệt kê.

Phương pháp Vạch đường liên miền không phân lớp CIDR (Classless Inter-Domain Routing)

CIDR là một sơ đồ đánh địa chỉ mới cho mạng Internet hiệu quả hơn nhiều so với sơ đồ đánh địa chỉ cũ theo kiểu phân lớp A, B và C.

CIDR ra đời để giải quyết hai vấn đề bức xúc đối với mạng Internet là :

- Thiếu địa chỉ IP
- Vượt quá khả năng chứa đựng của các bảng chọn đường.

Vấn đề thiếu địa chỉ IP

Với sơ đồ đánh địa chỉ truyền thống, các địa chỉ được phân ra thành các lớp A, B và C. Mỗi địa chỉ có 2 phần, phần nhận dạng mạng và phần nhận dạng máy tính. Khi đó số lượng mạng và số máy tính tối đa cho từng mạng được thống kê như bảng sau :

Lớp mạng	Số lượng mạng	Số máy tính tối đa trong mạng
A	126	16.777.214
B	65.000	65.534
C	Hơn 2 triệu	254

Bởi vì các địa chỉ của mạng Internet thường được gán theo kích thước này dẫn đến tình trạng lãng phí. Trường hợp bạn cần 100 địa chỉ, Bạn sẽ được cấp một địa chỉ lớp C. Như vậy còn 154 địa chỉ không được sử dụng. Chính điều này dẫn đến tình trạng thiếu địa chỉ IP cho mạng Internet. Theo thống kê, chỉ có khoảng 3% số địa chỉ đã được cấp phát được sử dụng đến. Chính vì thế sơ đồ đánh địa chỉ mới CIDR ra đời để khắc phục tình trạng trên.

Vấn đề vượt quá khả năng chứa đựng của các bảng chọn đường

Khi số lượng mạng trên mạng Internet tăng cũng đồng nghĩa với việc tăng số lượng router trên mạng. Trong những năm gần đây, người ta dự đoán rằng các router đường

trục của mạng Internet đang nhanh chóng tiến đến mức ngưỡng tối đa số lượng router mà nó có thể chấp nhận được.

Thậm chí với những công nghệ hiện đại dùng để sản xuất các router thì về mặt lý thuyết kích thước tối đa của một bảng chọn đường cũng chỉ đến 60.000 mục từ (đường đi). Nếu không có những cải tiến thì các router đường trục sẽ đạt đến con số này và như thế không thể mở rộng mạng Internet hơn nữa.

Để giải quyết hai vấn đề trên, cộng đồng Internet đã đưa ra các giải pháp sau :

- Sửa đổi lại cấu trúc cấp phát địa chỉ IP để tăng hiệu quả
- Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường.

Sửa đổi lại cấu trúc cấp phát địa chỉ IP

CIDR được sử dụng để thay thế cho sơ đồ cấp phát cũ với việc qui định các lớp A, B, C. Thay vì phân nhận dạng mạng được giới hạn với 8, 16 hoặc 24 bits, CIDR sử dụng phân nhận dạng mạng có tính tổng quát từ 13 đến 27 bits. Chính vì thế các khối địa chỉ có thể được gán cho mạng nhỏ nhất với 32 máy tính đến mạng lớn nhất hơn 500.000 máy tính. Điều này đáp ứng gần đúng yêu cầu đánh địa chỉ của các tổ chức khác nhau.

Địa chỉ CIDR

Một địa chỉ theo cấu trúc CIDR, gọi tắt địa chỉ CIDR, bao gồm 32 bits của địa chỉ IP chuẩn cùng với một thông tin bổ sung về số lượng các bit được sử dụng cho phân nhận dạng mạng.

Ví dụ : Với địa chỉ CIDR 206.13.01.48/25 thì chuỗi số "/25" chỉ ra rằng 25 bits đầu tiên trong địa chỉ IP được dùng để nhận dạng duy nhất một mạng, số bits còn lại dùng để nhận dạng một máy tính trong mạng.

Bảng sau so sánh giữa sơ đồ đánh địa chỉ theo kiểu CIDR và sơ đồ đánh địa chỉ theo chuẩn phân lớp hoàn toàn.

Số bits nhận dạng mạng trong địa chỉ CIDR	Lớp tương ứng trong chuẩn phân lớp hoàn toàn	Số lượng máy tính trong mạng
/27	1/8 lớp C	32
/26	¼ lớp C	64
/25	1/2 lớp C	128
/24	1 lớp C	256
/23	2 lớp C	512
/22	4 lớp C	1.024
/21	8 lớp C	2.048
/20	16 lớp C	4.096
/19	32 lớp C	8.192
/18	64 lớp C	16.384
/17	128 lớp C	32.768
/16	256 lớp C (= 1 lớp B)	65.536
/15	512 lớp C	131.072
/14	1,024 lớp C	262.144
/13	2,048 lớp C	524.288

Kết hợp việc chọn đường có cấu trúc để giảm tối đa số lượng các mục từ trong bảng chọn đường.

Sơ đồ đánh địa chỉ theo theo CIDR cũng cho phép kết hợp các đường đi, ở đó mục từ trong bảng chọn đường ở mức cao có thể đại diện cho nhiều router ở mức thấp hơn trong các bảng chọn đường tổng thể.

Sơ đồ này giống như hệ thống mạng điện thoại ở đó mạng được thiết lập theo kiến trúc phân cấp. Một router ở mức cao (quốc gia), chỉ quan tâm đến mã quốc gia trong số điện thoại, sau đó nó sẽ vạch đường cho cuộc gọi đến router đường trục phụ trách mạng quốc gia tương ứng với mã quốc gia đó. Router nhận được cuộc gọi nhìn vào phần đầu của số điện thoại, mã tỉnh, để vạch đường cho cuộc gọi đến một mạng con tương ứng với mã tỉnh đó, và cứ như thế. Trong sơ đồ này, các router đường trục chỉ lưu giữ thông tin về mã quốc gia cho mỗi mục từ trong bảng chọn đường của mình, mỗi mục từ như thế đại diện cho một số không lồ các số điện thoại riêng lẻ chứ không phải là một số điện thoại cụ thể.

Thông thường, các khối địa chỉ lớn được cấp cho các nhà cung cấp dịch vụ Internet (IP-Internet Service Providers) lớn, sau đó họ lại cấp lại các phần trong khối địa chỉ của họ cho các khách hàng của mình.

Hiện tại, mạng Internet sử dụng cả hai sơ đồ cấp phát địa chỉ Classfull standard và CIDR. Hầu hết các router mới đều hỗ trợ CIDR và những nhà quản lý Internet thì khuyến khích người dùng cài đặt sơ đồ đánh địa chỉ CIDR.

Tham khảo thêm về CIDR ở địa chỉ <http://www.rfc-editor.org/rfcsearch.html> với các RFC liên quan sau:

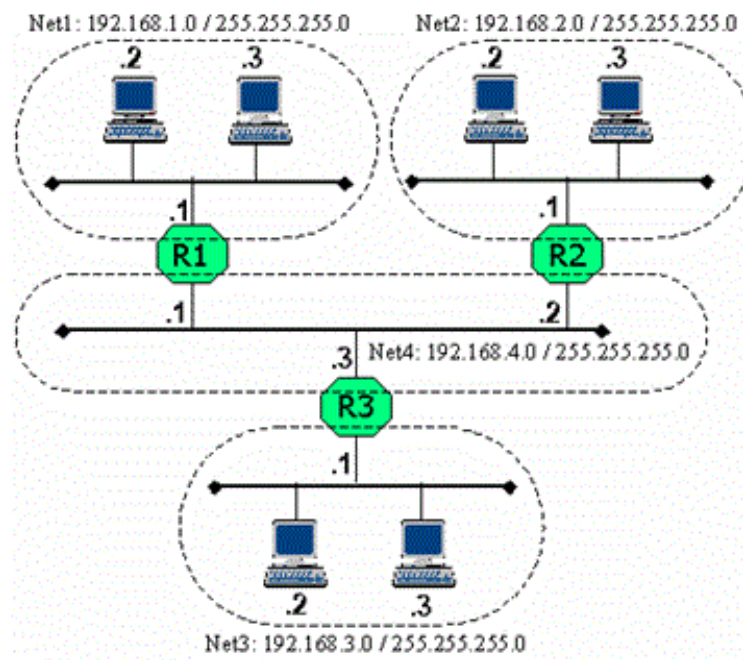
- RFC 1517: Applicability Statement for the Implementation of CIDR
- RFC 1518: An Architecture for IP Address Allocation with CIDR
- RFC 1519: CIDR: An Address Assignment and Aggregation Strategy
- RFC 1520: Exchanging Routing Information Across Provider Boundaries in the CIDR Environment

Vạch đường trong giao thức IP

Cho ba mạng Net1, Net2 và Net3 nối lại với nhau nhờ 3 router R1, R2 và R3. Mạng Net4 nối các router lại với nhau. Công việc đầu tiên trong thiết kế mạng liên mạng IP là chọn địa chỉ mạng cho các nhánh mạng. Trong trường hợp này ta chọn mạng lớp C cho 4 mạng như bảng sau:

Mạng	Địa chỉ mạng	Mặt nạ mạng
Net1	192.168.1.0	255.255.255.0
Net2	192.168.2.0	255.255.255.0
Net3	192.168.3.0	255.255.255.0
Net4	192.168.4.0	255.255.255.0

Kế tiếp, gán địa chỉ cho từng máy tính trong mạng. Ví dụ trong mạng Net1, các máy tính được gán địa chỉ là 192.168.1.2 (Ký hiệu .2 là cách viết tắt của địa chỉ IP để mô tả Phần nhận dạng máy tính) và 192.168.1.3. Mỗi router có hai giao diện tham gia vào hai mạng khác nhau. Ví dụ, giao diện tham gia vào mạng NET1 của router R1 có địa chỉ là 192.168.1.1 và giao diện tham gia vào mạng NET4 có địa chỉ là 192.168.4.1.



Ví dụ về liên mạng một liên mạng sử dụng giao thức IP (H6.36)

Để máy tính của các mạng có thể giao tiếp được với nhau, cần phải có thông tin về đường đi. Bảng chọn đường của router có thể tạo ra thủ công hoặc tự động. Đối với mạng nhỏ, nhà quản trị mạng sẽ nạp đường đi cho các router thông qua các lệnh được cung cấp bởi hệ điều hành của router. Bảng chọn đường trong giao thức IP có 4 thông tin quan trọng là :

- Địa chỉ mạng đích
- Mặt nạ mạng đích
- Router kế tiếp sẽ nhận gói tin (Next Hop)
- Giao diện chuyển gói tin đi

Trong ví dụ trên, các router sẽ có bảng chọn đường như sau :

R1-Routing table		
Network/Netmask	NextHop	Interface
192.168.1.0/255.255.255.0	local	local
192.168.2.0/255.255.255.0	192.168.4.2	192.168.4.1
192.168.3.0/255.255.255.0	192.168.4.3	192.168.4.1
192.168.4.0/255.255.255.0	local	local

R2-Routing table		
Network/Netmask	NextHop	Interface
192.168.1.0/255.255.255.0	192.168.4.1	192.168.4.2
192.168.2.0/255.255.255.0	local	local
192.168.3.0/255.255.255.0	192.168.4.3	192.168.4.2
192.168.4.0/255.255.255.0	local	local

R3-Routing table		
Network/Netmask	NextHop	Interface
192.168.1.0/255.255.255.0	192.168.4.1	192.168.4.3
192.168.2.0/255.255.255.0	192.168.4.2	192.168.4.3
192.168.3.0/255.255.255.0	local	local
192.168.4.0/255.255.255.0	local	local

Các máy tính cũng có bảng chọn đường. Dưới đây là bảng chọn đường của máy tính có địa chỉ 192.168.3.3 :

192.168.3.3 - Routing table		
Network/Netmask	NextHop	Interface
192.168.3.0/255.255.255.0	local	local
default	192.168.3.1	local

Mạng đích default ý nói rằng ngoài những đường đi đến các mạng đã liệt kê phía trên, các đường đi còn lại thì gửi cho NextHop của mạng default này. Như vậy, để gửi gói tin cho bất kỳ một máy tính nào nằm bên ngoài mạng 192.168.3.0 thì máy tính 192.168.3.3 sẽ chuyển gói tin cho router 3 ở địa chỉ 192.168.3.1.

Đường đi của gói tin

Để hiểu rõ có chế hoạt động của giao thức IP, ta hãy xét hai trường hợp gửi gói tin : Trường hợp máy tính gửi và nhận nằm trong cùng một mạng và trường hợp máy tính gửi và máy tính nhận nằm trên hai mạng khác nhau.

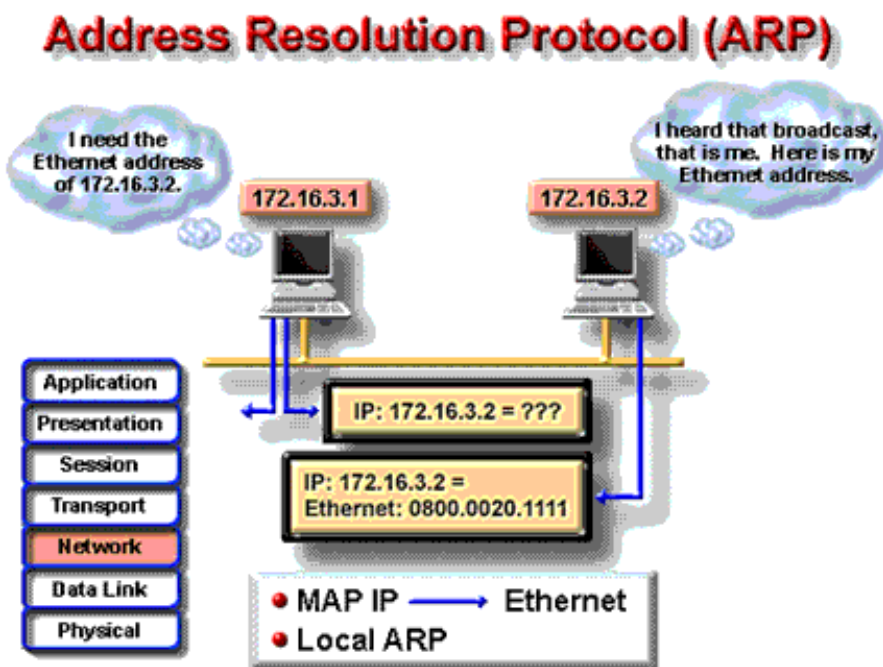
Giả sử máy tính có địa chỉ 192.168.3.3 gửi một gói tin cho máy tính 192.168.3.2. Tầng hai của máy gửi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của máy nhận và gói khung lên đường truyền NET3, trên đó máy tính nhận sẽ nhận được gói tin.

Bây giờ ta xét trường hợp máy tính có địa chỉ 192.168.3.3 trên mạng NET3 gửi gói tin cho máy tính có địa chỉ 192.168.1.2 trên mạng Net1. Theo như bảng chọn đường của máy gửi, các gói tin có địa chỉ nằm ngoài mạng 192.168.3.0 sẽ được chuyển đến router R3 (địa chỉ 192.168.3.1). Chính vì thế, máy tính gửi sẽ đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của giao diện 192.168.3.1 và đưa lên đường truyền NET3. Nhận được gói tin, R3 phân tích địa chỉ IP của máy nhận để xác định đích đến của gói tin. Bảng chọn đường cho thấy, với đích đến là mạng 192.168.1.0 thì cần phải chuyển gói tin cho router R1 ở địa chỉ 192.168.4.1 thông qua giao diện 192.168.4.3. Vì thế R3 đặt gói tin vào một khung với địa chỉ nhận là địa chỉ vật lý của giao diện 192.168.4.1 của router R1 và đưa lên đường truyền NET4. Tương tự, R1 sẽ chuyển gói tin cho máy nhận 192.168.1.2 bằng một khung trên đường truyền NET1.

Ta nhận thấy rằng, để đi đến được máy nhận, gói tin được chuyển đi bởi nhiều khung khác nhau. Mỗi khung sẽ có địa chỉ nhận khác nhau, tuy nhiên địa chỉ của gói tin thì luôn luôn không đổi.

Giao thức phân giải địa chỉ (Address Resolution Protocol)

Nếu một máy tính muốn truyền một gói tin IP nó cần đặt gói tin này vào trong một khung trên đường truyền vật lý mà nó đang nối kết vào. Để có thể truyền thành công khung, máy tính gửi cần thiết phải biết được địa chỉ vật lý (MAC) của máy tính nhận. Điều này có thể thực hiện được bằng cách sử dụng một bảng để ánh xạ các địa chỉ IP về địa chỉ vật lý. Giao thức IP sử dụng giao thức ARP (Address Resolution Protocol) để thực hiện ánh xạ từ một địa chỉ IP về một địa chỉ MAC.



Giao thức ARP (H6.37)

Một máy tính xác định địa chỉ vật lý của nó vào lúc khởi động bằng cách đọc thiết bị phần cứng và xác định địa chỉ IP của nó bằng cách đọc tập tin cấu hình, sau đó lưu thông tin về mối tương ứng giữa địa chỉ IP và MAC của nó vào trong vùng nhớ tạm (ARP cache). Khi nhận được một địa chỉ IP mà ARP không thể tìm ra được địa chỉ vật lý tương ứng dựa vào vùng nhớ tạm hiện tại, nó sẽ thực hiện một khung quảng bá có định dạng như sau :

Tổng quát	Các trường	Kích thức (byte)	Các giá trị
Ethernet Header	Ethernet Destination Address	6	Địa chỉ máy nhận, trong trường hợp này là một địa chỉ quảng bá
	Ethernet Source Address	6	Địa chỉ của máy gửi thông điệp
	Frame Type	2	Kiểu khung, có giá trị là 0x0806 khi ARP yêu cầu và 0x8035 khi ARP trả lời
ARP request/reply	Hardware Type	2	Giá trị là 1 cho mạng Ethernet
	Protocol Type	2	Có giá trị là 0x0800 cho địa chỉ IP
	Hardware Address Size in bytes	1	Chiều dài của địa chỉ vật lý, có giá trị là 6 cho mạng Ethernet
	Protocol Address Size in bytes	1	Chiều dài địa chỉ của giao thức, có giá trị là 4 cho giao thức IP
	Operation	2	Là 1 nếu là khung yêu cầu, là 2 nếu là khung trả lời
	Sender Ethernet Address	6	-
	Sender IP Address	4	-
	Destination Ethernet Address	6	Không sử dụng đến trong yêu cầu của ARP
	Destination IP Address	4	-

Nhờ vào việc gửi các yêu cầu này, một máy tính có thể bổ sung thông tin cho vùng cache của giao thức ARP, nhờ đó cập nhật kịp thời mọi sự thay đổi của sơ đồ mạng. Thông thường thời gian quá hạn (Time-out) cho một thông tin trong vùng cache là 20 phút. Một yêu cầu ARP cho một máy tính không tồn tại trên nhánh mạng được lặp lại một vài lần xác định nào đó.

Nếu một máy tính được nối kết vào nhiều hơn một mạng bằng giao diện mạng, khi đó sẽ tồn tại những vùng cache ARP riêng cho từng giao diện mạng.

Lưu ý, ARP trên một máy tính chỉ thực hiện việc xác địa chỉ vật lý cho các địa chỉ cùng địa chỉ mạng / mạng con với nó mà thôi. Đối với các gói tin gửi cho các máy tính có địa chỉ IP không cùng một mạng / mạng con với máy gửi sẽ được chuyển hướng cho một router nằm cùng mạng với máy gửi để chuyển đi tiếp.

Vì các yêu cầu ARP được quảng bá rộng rãi, cho nên bất kỳ một máy tính nào đang duy trì một vùng cache đều có thể theo dõi tất cả các yêu cầu được quảng bá này để lấy thông tin về địa chỉ vật lý và địa chỉ IP của máy gửi yêu cầu và bổ sung vào vùng cache của nó khi cần thiết. Khi một máy tính khởi động, nó gửi một yêu cầu ARP (có thể cho chính nó) như để thông báo với các máy tính khác về sự xuất hiện của nó trong mạng cục bộ.

Có thể gán nhiều hơn một địa chỉ IP cho một địa chỉ vật lý. Chú ý rằng, định dạng của yêu cầu ARP thì được thiết kế để có thể hỗ trợ được cho các giao thức khác ngoài IP và Ethernet.

Giao thức phân giải địa chỉ ngược RARP (Reverse Address Resolution Protocol)

Ngày nay, các trạm làm việc không đĩa cứng (Diskless workstation) được sử dụng rộng rãi. Mỗi máy tính chỉ cần bộ xử lý và bộ nhớ, tất cả không gian lưu trữ được cung cấp từ một máy chủ (Server) sử dụng một hệ thống tập tin mạng theo một chuẩn nào đó. Do không có các tập tin cấu hình, tiến trình khởi động của các máy tính này thường sử dụng một giao thức truyền tải tập tin rất đơn giản như TFTP. Tuy nhiên, 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. 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 gửi yêu cầu.

Giao thức thông điệp điều khiển Internet ICMP (Internet Control Message Protocol)

Giao thức ICMP được cài đặt trong hầu hết tất cả các máy tính TCP/IP. Các thông điệp của giao thức được gửi đi trong các gói tin IP và được dùng để gửi đi các báo lỗi hay các thông tin điều khiển.

ICMP tạo ra nhiều loại thông điệp hữu ích như :

- Đích đến không tới được (Destination Unreachable),
- Thăm hỏi và trả lời (Echo Request and Reply),
- Chuyển hướng (Redirect),
- Vượt quá thời gian (Time Exceeded),
- Quảng bá bộ chọn đường (Router Advertisement)
- Cô lập bộ chọn đường (Router Solicitation)
-

Nếu một thông điệp không thể phân phát được thì nó sẽ không được gửi lại. Điều này để tránh tình trạng di chuyển không bao giờ dừng của các thông điệp ICMP.

Nếu một thông điệp « Đích đến không tới được » được gửi đi bởi một router, điều đó có nghĩa rằng router không thể gửi gói tin đến đích được. Khi đó router sẽ xóa gói tin ra khỏi hàng đợi của nó. Có hai nguyên nhân làm cho một gói tin không thể đi đến nơi được. Phần lớn là máy gửi mô tả một địa chỉ nhận mà nó không tồn tại trên thực tế. Trường hợp ít hơn là router không biết đường đi đến nơi nhận gói tin.

Thông điệp Đích đến không tới được được chia thành bốn loại cơ bản là :

- Mạng không đến được (Network unreachable) : Có nghĩa là có sự cố trong vấn đề vạch đường hoặc địa chỉ nhận của gói tin.
- Máy tính không đến được (Host unreachable) : Thông thường dùng để chỉ trực tiếp trong vấn đề phân phát, như là sai mặt nạ mạng con chẳng hạn.
- Giao thức không đến được (Protocol unreachable) : Máy nhận không hỗ trợ giao thức ở tầng cao hơn như gói tin đã mô tả.
- Cổng không đến được (Port unreachable) : Socket của giao thức TCP hay cổng không tồn tại.

Một thông điệp « Thăm hỏi và trả lời » được tạo ra bởi lệnh ping từ một máy tính để kiểm tra tính liên thông trên liên mạng. Nếu có một thông điệp trả lời, điều đó biểu hiện rằng giữa máy gửi và máy nhận có thể giao tiếp được với nhau.

Một thông điệp « Chuyển hướng » được gửi bởi một router đến máy đã gửi gói tin để khuyến cáo về một đường đi tốt hơn. Router hiện tại vẫn chuyển tiếp gói tin mà nó nhận được. Thông điệp chuyển hướng giữ cho bảng chọn đường của các máy tính được nhỏ bởi vì chúng chỉ cần chứa địa chỉ của một router mà thôi, thậm chí router đó cung cấp đường đi không phải là tốt nhất. Đôi khi sau khi nhận được thông điệp chuyển hướng, thiết bị gửi vẫn sử dụng đường đi cũ.

Một thông điệp « Vượt quá thời hạn » được gửi bởi một router nếu thời gian sống (Time-to-live) của gói tin, tính bằng số router hay giây, có giá trị là 0. Thời gian sống

Bộ giao thức liên mạng (IPs - Internet Protocols)

của gói tin giúp phòng ngừa trường hợp gói tin được gửi đi lòng vòng trên mạng và không bao giờ đến nơi nhận. Router sẽ bỏ đi các gói tin đã hết thời gian sống.