### 18.4 GIAO THỨC INTERNET

Trong phần này, chúng ta xem xét phiên bản 4 của IP, được xác định chính thức trong RFC 791.Mặc dù dự định rằng IPv4 cuối cùng sẽ được thay thế bằng IPv6, nhưng hiện tại nó là IP tiêu chuẩn được sử dụng trong mạng TCP / IP.

Giao thức Internet (IP) là một phần của bộ TCP / IP và là giao thức làm việc internet được sử dụng rộng rãi nhất. Như với bất kỳ tiêu chuẩn giao thức nào, IP được chỉ định trong hai phần (xem Hình 2.9):

* Giao diện với một lớp cao hơn (ví dụ: TCP), chỉ định các dịch vụ mà IP cung cấp
* Định dạng và cơ chế giao thức thực tế

Trong phần này, chúng tôi kiểm tra các dịch vụ IP đầu tiên và sau đó là giao thức. Tiếp theo là một cuộc thảo luận về các định dạng địa chỉ IP. Cuối cùng, Giao thức Tin nhắn Điều khiển Internet (ICMP), một phần không thể thiếu của IP, được mô tả.

#### Dịch vụ IP

Các dịch vụ được cung cấp trên các lớp giao thức liền kề (ví dụ: giữa IP và TCP) được thể hiện dưới dạng nguyên thủy và các tham số. Một nguyên thủy chỉ định chức năng được thực hiện và các tham số được sử dụng để truyền dữ liệu và kiểm soát thông tin. Hình thức thực tế của một nguyên thủy là phụ thuộc vào thực hiện. Một ví dụ là một cuộc gọi thủ tục.

IP cung cấp hai dịch vụ nguyên thủy tại giao diện cho lớp cao hơn tiếp theo. Send nguyên thủy được sử dụng để yêu cầu truyền một đơn vị dữ liệu. Deliver primitive được IP sử dụng để thông báo cho người dùng về sự xuất hiện của một đơn vị dữ liệu. Các tham số liên quan đến hai nguyên thủy như sau:

* **Địa chỉ nguồn:** Địa chỉ Internetwork của việc gửi thực thể IP.
* **Địa chỉ đích:** Địa chỉ Internetwork của thực thể IP đích.
* **Giao thức:** Thực thể giao thức người nhận (người dùng IP, chẳng hạn như TCP).
* **Các chỉ số loại dịch vụ:** Được sử dụng để chỉ định việc xử lý đơn vị dữ liệu trong việc truyền tải thông qua các mạng thành phần.
* **Nhận dạng:** Được sử dụng kết hợp với địa chỉ nguồn và đích và giao thức người dùng để xác định đơn vị dữ liệu duy nhất. Tham số này là cần thiết để lắp ráp lại và báo cáo lỗi.
* **Không phân mảnh định danh:** Cho biết liệu IP có thể phân mảnh dữ liệu để hoàn thành phân phối hay không.
* **Thời gian sống:** Được tính bằng giây.
* **Độ dài dữ liệu:** Độ dài của dữ liệu được truyền đi.
* **Dữ liệu tùy chọn:** Tùy chọn theo yêu cầu của người dùng IP.
* **Dữ liệu:** Dữ liệu người dùng được truyền đi.

Nhận *dạng, không phân mảnh nhận dạng*và thời gian *để sống* các tham số có mặt trong Gửi nguyên thủy nhưng không phải trong Deliver primitive. Ba tham số này cung cấp hướng dẫn cho IP mà người dùng IP người nhận không quan tâm.

Tham số tùy chọn cho phép mở rộng trong tương lai và bao gồm các tham số thường không được gọi. Các tùy chọn hiện được xác định như sau:

* **Bảo mật:** Cho phép gắn nhãn bảo mật vào datagram.
* **Định tuyến nguồn:** Một danh sách các địa chỉ bộ định tuyến được sắp xếp theo dõi. Định tuyến có thể nghiêm ngặt (chỉ có thể truy cập các bộ định tuyến được xác định) hoặc lỏng lẻo (các bộ định tuyến trung gian khác có thể được truy cập).
* **Ghi tuyến đường:** Một trường được phân bổ để ghi lại chuỗi bộ định tuyến được truy cập bởi datagram.
* **Nhận dạng luồng: Tên dành riêng cho tài nguyên được sử dụng cho dịch vụ** luồng. Dịch vụ này cung cấp xử lý đặc biệt cho lưu lượng truy cập định kỳ dễ bay hơi (ví dụ: giọng nói).
* **Dấu thời gian:** Thực thể IP nguồn và một số hoặc tất cả các bộ định tuyến trung gian thêm dấu thời gian (độ chính xác đến mili giây) vào đơn vị dữ liệu khi nó đi qua.

#### Giao thức Internet

Giao thức giữa các thực thể IP được mô tả tốt nhất với tham chiếu đến định dạng datagram IP, được hiển thị trong Hình 18. 6. Các trường như sau:

* **Phiên bản (4 bit):** Chỉ ra số phiên bản, để cho phép tiến hóa giao thức; giá trị là 4.

**Phiên bản**

**ECN**

**DS**

**IHL**

**Tổng chiều dài**

**Xác định**

**Cờ**

**Bù đắp mảnh vỡ**

**Thời gian để sống**

**Protocol**

**Checkum tiêu đề**

**Tùy chọn**

**Padding**

**Địa chỉ Nguồn**

**Địa chỉ Đích**

**Bit:**

**0**

**4**

**8**

**16**

**19**

**31**

**octets**

**20**

**14**

**Hình 18.6** Tiêu đề IPv4

* **Chiều dài tiêu đề Internet (IHL) (4 bit): Chiều dài tiêu đề trong các từ** 32 bit. Giá trị tối thiểu là năm, cho chiều dài tiêu đề tối thiểu là 20 octets.
* **DS/ECN (8 bit): Trước khi giới thiệu các** dịch vụ khác biệt, trường này được gọi là trường Loại Dịch vụ và các thông số độ tin cậy, ưu tiên, độ trễ và thông lượng được chỉ định. Cách giải thích này hiện đã được thay thế. Sáu bit đầu tiên của trường này hiện được gọi là trường DS (Dịch vụ khác biệt), được thảo luận trong Chương 19.2 bit còn lại được dành riêng cho trường ECN (Thông báo tắc nghẽn rõ ràng), hiện đang trong quá trình tiêu chuẩn hóa. Trường ECN cung cấp tín hiệu rõ ràng về tắc nghẽn theo cách tương tự như đã thảo luận để chuyển tiếp khung hình (Mục 13.5).
* **Tổng chiều dài (16 bit): Tổng chiều dài** datagram, bao gồm tiêu đề cộng với dữ liệu, trong octets.
* **Nhận dạng (16 bit):** Một số thứ tự, cùng với địa chỉ nguồn, địa chỉ đích và giao thức người dùng, nhằm xác định một biểu đồ dữ liệu duy nhất. Do đó, con số này phải là duy nhất cho địa chỉ nguồn, địa chỉ đích và giao thức người dùng của datagram trong thời gian mà datagram sẽ vẫn còn trong internet.
* **Flags (3 bit):** Hiện tại chỉ có hai trong số các bit được xác định. More bit được sử dụng để phân mảnh và lắp ráp lại, như đã giải thích trước đây. Bit Don't Fragment cấm phân mảnh khi đặt. Bit này có thể hữu ích nếu người ta biết rằng đích đến không có khả năng lắp ráp lại các mảnh vỡ. Tuy nhiên, nếu bit này được thiết lập, datagram sẽ bị loại bỏ nếu nó vượt quá kích thước tối đa của mạng trên đường. Do đó, nếu bit được thiết lập, có thể nên sử dụng định tuyến nguồn để tránh các mạng có kích thước gói tối đa nhỏ.
* **Fragment Offset (13 bit):** Chỉ ra nơi trong biểu đồ dữ liệu ban đầu, mảnh này thuộc về, được đo bằng đơn vị 64 bit. Điều này ngụ ý rằng các mảnh vỡ khác ngoài mảnh cuối cùng phải chứa một trường dữ liệu có chiều dài 64 bit.
* **Thời gian để sống (8 bit):** Xác định thời gian, trong vài giây, một datagram được phép ở lại trong internet. Mỗi bộ định tuyến xử lý một datagram phải giảm TTL ít nhất một, vì vậy TTL tương tự như số lượng hop.
* **Giao thức (8 bit):** Chỉ ra giao thức cấp cao hơn tiếp theo là nhận trường dữ liệu tại đích;do đó,trườngnày xác định loại tiêu đề tiếp theo trong gói sau tiêu đề IP. Giá trị ví dụ là TCP = 6; UDP = 17; ICMP = 1. Một danh sách đầy đủ được duy trì ở http://www.iana.org/ bài tập / số giao **thức**.
* **Tiêu đề Checksum (16 bit): Mã phát hiện lỗi chỉ** áp dụng cho tiêu đề. Bởi vì một số trường tiêu đề có thể thay đổi trong quá trình vận chuyển (vídụ: Thời gian để sống, các trường liên quan đến phân mảnh), điều này được tôn kính và uy tín tại mỗi bộ định tuyến. Checkum được hình thành bằng cách lấy những bổ sung của những cái 16 bit bổ sung cho tất cả các từ 16 bit trong tiêu đề. Đối với mục đích tính toán, trường checksum tự nó được khởi tạo thành giá trị bằng không.[[1]](#footnote-1)
* **Địa chỉ nguồn (32 bit):** Được mã hóa để cho phép phân bổ biến các bit để chỉ định mạng và hệ thống cuối được gắn vào mạng được chỉ định, như đã thảo luận sau đó.
* **Địa chỉ đích (32 bit):** Các đặc điểm tương tự như địa chỉ nguồn.
* **Tùy chọn (biến):** Mã hóa các tùy chọn theo yêu cầu của người dùng gửi.
* **Padding (biến):** Được sử dụng để đảm bảo rằng tiêu đề datagram có chiều dài 32 bit.
* **Dữ liệu (biến):** Trường dữ liệu phải là bội số nguyên dài 8 bit. Chiều dài tối đa của datagram (trường dữ liệu cộng với tiêu đề) là 65.535 octets.

Cần phải rõ ràng các dịch vụ IP được chỉ định trong bản đồ Gửi và Phân phối nguyên thủy vào các trường của biểu đồ dữ liệu IP như thế nào.

#### Địa chỉ IP

Các trường địa chỉ nguồn và đích trong tiêu đề IP chứa địa chỉ internet toàn cầu 32 bit, thường bao gồm mã định danh mạng và mã định danh máy chủ.

**Lớp Mạng** Địa chỉ được mã hóa để cho phép phân bổ thay các bit để chỉ định mạng và máy chủ, như được mô tả trong Hình 18.7. Mã hóa này cung cấp sự linh hoạt trong việc gán địa chỉ cho máy chủ và cho phép kết hợp kích thước mạng trên internet. Ba lớp mạng chính phù hợp nhất với các điều kiện sau:

* **Lớp A:** Ít mạng, mỗi mạng có nhiều máy chủ
* **Lớp B:** Số lượng mạng trung bình, mỗi mạng có số lượng máy chủ trung bình
* **Lớp C:** Nhiều mạng, mỗi mạng có một vài máy chủ

**Biểu đồ 18.7** Định dạng Địa chỉ IPv4

**Lớp A**

**Host (24 bit)**

**Mạng (7 bit)**

**0**

**Hạng B**

**1**

**0**

**Mạng (14 bit)**

**Host (16 bit)**

**Hạng C**

**Lớp D**

**1**

**1**

**Mạng (21 bit)**

**Máy chủ (8 bit)**

**0**

**1**

**1**

**Multicast**

**1**

**0**

**Lớp E**

**1**

**1**

**Sử dụng trong tương lai**

**1**

**1**

**0**

Trong một môi trường cụ thể, tốt nhất là sử dụng các địa chỉ từ một lớp. Ví dụ: một internetwork của công ty bao gồm một số lượng lớn các mạng khu vực địa phương của bộ phận có thể cần phải sử dụng các địa chỉ Loại C độc quyền. Tuy nhiên, định dạng của các địa chỉ sao cho có thể trộn cả ba lớp địa chỉ trên cùng một internetwork; Đây là những gì được thực hiện trong trường hợp của chính Internet. Một hỗn hợp các lớp học là thích hợp cho một internetwork bao gồm một vài mạng lớn, nhiều mạng nhỏ, cộng với một số mạng cỡ trung bình.

Địa chỉ IP thường được viết **bằng ký hiệu thập phân chấm,**với số thập phân đại diện cho mỗioctets của địa chỉ 32 bit. Ví dụ: địa chỉ IP 11000000 11100100 00010001 00111001 được viết là 192.228.17.57.

Lưu ý rằng tất cả các địa chỉ mạng loại A bắt đầu bằng nhị phân 0. Địa chỉ mạng có octet đầu tiên là 0 (nhị phân 00000000) và 127 (01111111 nhị phân) được đặt trước, vì vậy có 126 số mạng Loại A tiềm năng, có số thập phân chấm đầu tiên trong phạm vi từ 1 đến 126. Địa chỉ mạng loại B bắt đầu bằng nhị phân 10, do đó phạm vi của số thập phân đầu tiên trong địa chỉ Loại B là 128 đến 191 (nhị phân 10000000 đến 10111111). Octet thứ hai cũng là một phần của địa chỉ Loại B, do đó có 214  = 16.384 địa chỉ Loại B. Đối với địa chỉ Loại C, số thập phân đầu tiên dao động từ 192 đến 223 (11000000 đến 11011111). Tổng số địa chỉ hạng C là 221  = 2.097.152.

**Mạng con và Mặt nạ mạng con** Khái niệm mạng con được giới thiệu để giải quyết các yêu cầu sau đây. Hãy xem xét một internet bao gồm một hoặc nhiều WAN và một số trang web, mỗi trang web có một số LA.Chúng tôi muốn cho phép sự phức tạp tùy ý của các cấu trúc LAN được kết nối với nhau trong một tổ chức trong khi cách ly internet tổng thể chống lại sự tăng trưởng bùng nổ về số mạng và độ phức tạp định tuyến. Một cách tiếp cận cho vấn đề này là gán một số mạng duy nhất cho tất cả các 222 tại một trang web. Từ quan điểm của phần còn lại của internet, có một mạng duy nhất tại trang web đó, giúp đơn giản hóa việc giải quyết và định tuyến. Để cho phép các bộ định tuyến trong trang web hoạt động bình thường, mỗi mạng LAN được gán một số mạng con. Phần  *máy chủ* của địa chỉ internet được phân vùng thành số mạng con và số máy chủ để phù hợp với cấp độ địa chỉ mới này.

Trong mạng ngầm, các bộ định tuyến cục bộ phải định tuyến trên cơ sở số mạng mở rộng bao gồm phần *mạng* của địa chỉ IP và số mạng con. Các vị trí bit chứa số mạng mở rộng này được chỉ định bằng mặt nạ địa chỉ. Việc sử dụng mặt nạ địa chỉ cho phép máy chủ xác định xem một datagram đi được dành cho một máy chủ trên cùng một MẠNG LAN (gửi trực tiếp) hoặc lan khác (gửi datagram đến bộ định tuyến). Người ta cho rằng một số phương tiện khác (ví dụ: cấu hình thủ công) được sử dụng để tạo mặt nạ địa chỉ và làm cho chúng được biết đến với các bộ định tuyến địa phương.

Bảng 18.3a hiển thị các tính toán liên quan đến việc sử dụng mặt nạ mạng con. Lưu ý rằng hiệu ứng của mặt nạ mạng con là xóa phần của trường máy chủ đề cập đến một máy chủ thực tế trên mạng con. Những gì còn lại là số mạng và số mạng con. Hình 18.8 cho thấy một ví dụ về việc sử dụng mạng con. Con số này cho thấy một khu phức hợp địa phương bao gồm ba LAN và hai bộ định tuyến. Đối với phần còn lại của internet, tổ hợp này là một mạng duy nhất với địa chỉ Loại C của biểu mẫu 192.228.17. *x*, trong đó ba octets ngoài cùng bên trái là số mạng và octet ngoài cùng bên phải chứa số máy chủ *x.* Cả hai bộ định tuyến R1 và R2 đều được cấu hình với mạng con

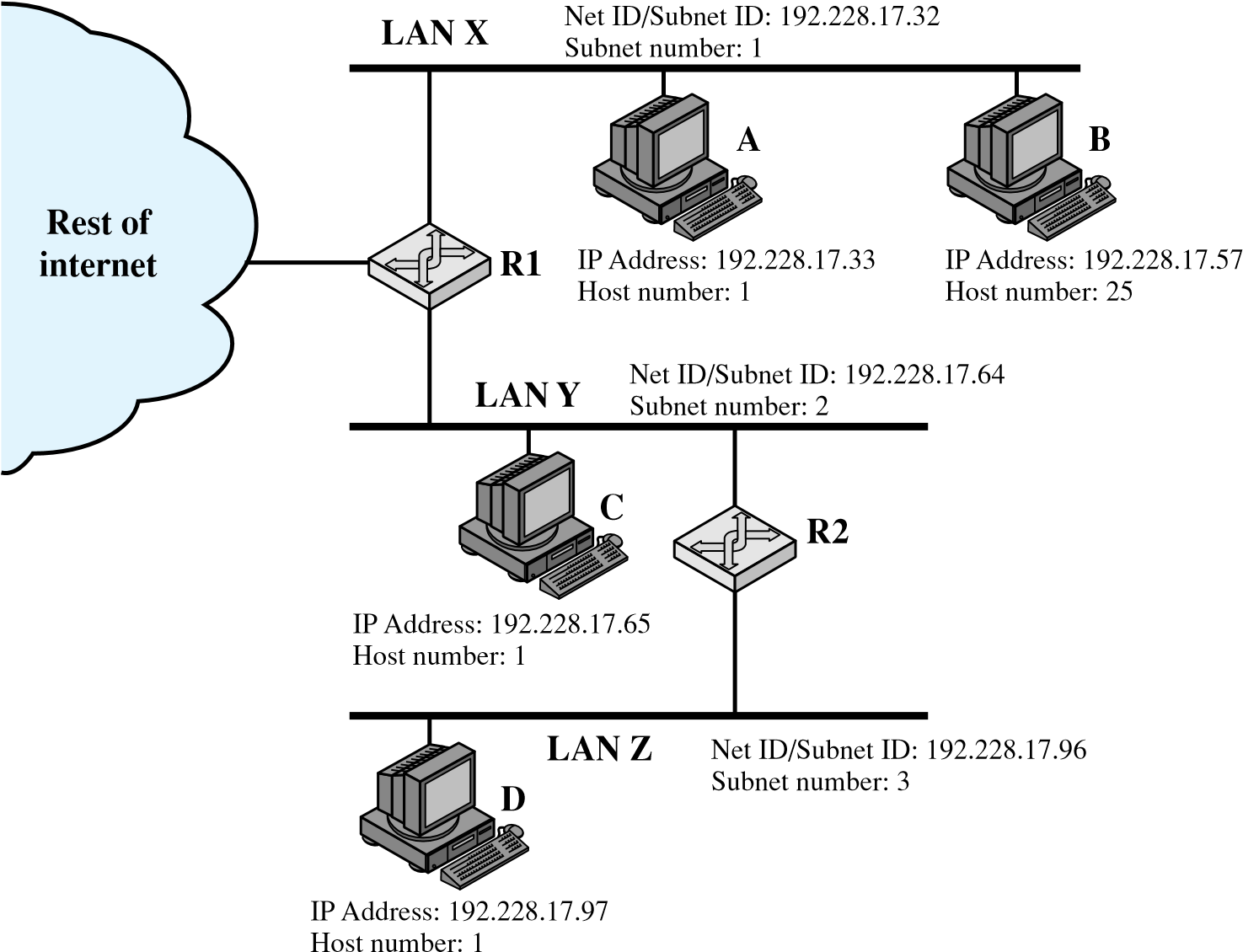
**Bảng 18.3** Địa chỉ IP và Mặt nạ mạng con [STEI95]

1. Các biểu diễn thập phân và nhị phân chấm của địa chỉ IP và mặt nạ mạng con

|  |  |  |
| --- | --- | --- |
|  | **Đại diện nhị phân** | **Thập phân chấm** |
| **Địa chỉ IP** | 11000000.11100100.00010001.00111001 | 192.228.17.57 |
| **Mặt nạ mạng con** | 11111111.11111111.11111111.11100000 | 255.255.255.224 |
| **Bitwise AND của địa chỉ và mặt nạ**  **( số mạng/mạng con** **kết quả)** | 11000000.11100100.00010001.00100000 | 192.228.17.32 |
| **Số mạng con** | 11000000.11100100.00010001.001 | 1 |
| **Số máy chủ** | 00000000.00000000.00000000.00011001 | 25 |

1. Mặt nạ mạng con mặc định

|  |  |  |
| --- | --- | --- |
|  | **Đại diện nhị phân** | **Thập phân chấm** |
| **Mặt nạ mặc định loại A** | 11111111.00000000.00000000.00000000 | 255.0.0.0 |
| **Ví dụ mặt nạ lớp A** | 11111111.11000000.00000000.00000000 | 255.192.0.0 |
| **Mặt nạ mặc định loại B** | 11111111.11111111.00000000.00000000 | 255.255.0.0 |
| **Mặt nạ loại B ví dụ** | 11111111.11111111.11111000.00000000 | 255.255.248.0 |
| **Mặt nạ mặc định loại C** | 11111111.11111111.11111111.00000000 | 255. 255. 255.0 |
| **Mặt nạ Lớp C ví dụ** | 11111111.11111111.11111111.11111100 | 255. 255. 255.252 |



**Biểu đồ 18.8** Ví dụ về subnetworking

khẩu trang có giá trị 255.255.255.224 (xem Bảng 18.3a). Ví dụ: nếu một datagram với địa chỉ đích 192.228.17.57 đến R1 từ phần còn lại của internet hoặc từ LAN Y, R1 áp dụng mặt nạ mạng con để xác định rằng địa chỉ này đề cập đến mạng con 1, đó là LAN X, và do đó chuyển tiếp datagram đến LAN X. Tương tự như vậy, nếu một datagram với địa chỉ đích đó đến R2 từ LAN Z, R2 áp dụng mặt nạ và sau đó xác định từ cơ sở dữ liệu chuyển tiếp của nó rằng các biểu đồ dữ liệu dành cho mạng con 1 nên được chuyển tiếp đến R1. Máy chủ cũng phải sử dụng mặt nạ mạng con để đưa ra quyết định định tuyến.

Mặt nạ mạng con mặc định cho một lớp địa chỉ nhất định là mặt nạ null (Bảng 18.3b), mang lại cùng một mạng và số máy chủ nhưđịa chỉ khôngđược phép thuê.

#### Giao thức Thông báo Điều khiển Internet (ICMP)

Tiêu chuẩn IP quy định rằng việc thực hiện tuân thủ cũng phải thực hiện ICMP (RFC 792). ICMP cung cấp một phương tiện để chuyển tin nhắn từ bộ định tuyến và các máy chủ khác sang máy chủ. Về bản chất, ICMP cung cấp phản hồi về các vấn đề trong môi trường giao tiếp. Ví dụ về việc sử dụng nó là khi một datagram không thể đến đích, khi bộ định tuyến không có khả năng đệm để chuyển tiếp biểu đồ dữ liệu và khi bộ định tuyến có thể chỉ đạo trạm gửi lưu lượng truy cập trên một tuyến đường ngắn hơn. Trong hầu hết các trường hợp, một tin nhắn ICMP được gửi để đáp ứng với một datagram, hoặc bởi một bộ định tuyến dọc theo đường dẫn của datagram hoặc bởi máy chủ đích dự định.

**0 8 16 31 0 8 16 31**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Kiểu** | **Mã** | **Checkum** |  | **Kiểu** | **Mã** | **Checkum** |
| **Không sử dụng** | | | **Định danh** | | **Số thứ tự** |
| **IPHeader 64 bit datagram gốc** | | | **Dấu thời gian bắt nguồn** | | |

1. **Điểm đến không thể tiếp cận; thời gian vượt quá; nguồn dập tắt (e) Timestamp**

**0 8 16 31 0 8 16 31**

|  |  |  |
| --- | --- | --- |
| **Kiểu** | **Mã** | **Checkum** |
| **Định danh** | | **Số thứ tự** |
| **Dấu thời gian bắt nguồn** | | |
| **Nhận dấu thời gian** | | |
| **Truyền dấu thời gian** | | |

|  |  |  |
| --- | --- | --- |
| **Kiểu** | **Mã** | **Checkum** |
| **Con trỏ** | **Không sử dụng** | |
| **Tiêu đề IP 64**  **bit datagram gốc** | | |

1. **Vấn đề tham số**

**(f) Dấu thời gian trả lời**

**0 8 16 31 0 8 16 31**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Kiểu** | **Mã** | **Checkum** | | **Địa chỉ Internet cổng kết nối** | | | | **Tiêu đề IP 64**  **bit datagram gốc** | | | | |  |  |  | | --- | --- | --- | | **Kiểu** | **Mã** | **Checkum** | | **Định danh** | | **Số thứ tự** | |

**(g) Yêu cầu mặt nạ địa chỉ (c) Chuyển hướng**

**0 8 16 31 0 8 16 31**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Kiểu** | **Mã** | **Checkum** | | **Định danh** | | **Số thứ tự** | | **Dữ liệu tùy chọn** | | | | |  |  |  | | --- | --- | --- | | **Kiểu** | **Mã** | **Checkum** | | **Định danh** | | **Số thứ tự** | | **Mặt nạ địa chỉ** | | | |

**(d) Echo, echo reply (h) Trả lời mặt nạ địa chỉ**

**Biểu đồ 18.9** Định dạng Thư ICMP

Mặc dù ICMP, trên thực tế, ở cùng cấp độ với IP trong kiến trúc TCP / IP, nó là người dùng IP. Một thông điệp ICMP được xây dựng và sau đó được truyền lại cho IP, gói gọn thông điệp bằng tiêu đề IP và sau đó truyền biểu đồ dữ liệu kết quả theo cách thông thường. Bởi vì tin nhắn ICMP được truyền trong datagram IP, việc phân phối chúng không được đảm bảo và việc sử dụng chúng không thể được coi là đáng tin cậy.

Hình 18.9 hiển thị định dạng của các loại tin nhắn ICMP khác nhau. Một thông báo ICMP bắt đầu với một tiêu đề 64-bit bao gồm các như sau:

* **Nhập (8 bit):** Chỉ định loại tin nhắn ICMP.
* **Mã (8 bit):** Được sử dụng để chỉ định các tham số của thư có thể được mã hóa trong một hoặc một vài bit.
* **Checksum (16 bit):** Checkum của toàn bộ thông điệp ICMP. Đây là thuật toán checkum tương tự được sử dụng cho IP.
* **Tham số (32 bit):** Được sử dụng để chỉ định các tham số dài hơn.

Các trường này thường được theo sau bởi các trường thông tin bổ sung chỉ định thêm nội dung của thư.

Trong những trường hợp mà thông điệp ICMP đề cập đến biểu đồ dữ liệu trước đó, trường thông tin bao gồm toàn bộ tiêu đề IP cộng với 64 bit đầu tiên của trường dữ liệu của biểu đồ dữ liệu gốc. Điều này cho phép máy chủ nguồn khớp với thông báo ICMP đến với biểu đồ dữ liệu trước đó. Lý do để bao gồm 64 bit đầu tiên của trường dữ liệu là điều này sẽ cho phép mô-đun IP trong máy chủ xác định giao thức hoặc giao thức cấp trên nào có liên quan. Đặc biệt, 64 bit đầu tiên sẽ bao gồm một phần tiêu đề TCP hoặc tiêu đề cấp vận tải khác.

Thông điệp **không thể tiếp cận đích** bao gồm một số tình huống bất ngờ. Bộ định tuyến có thể trả về thông báo này nếu nó không biết cách tiếp cận mạng đích. Trong một số mạng, một bộ định tuyến đính kèm có thể xác định xem một máy chủ cụ thể có thể truy cập được không và trả về tin nhắn. Bản thân máy chủ đích có thể trả về thông báo này nếu giao thức người dùng hoặc một số điểm truy cập dịch vụ cấp cao hơn là không thể truy cập được. Điều này có thể xảy ra nếu trường tương ứng trong tiêu đề IP được đặt không chính xác. Nếu biểu đồ dữ liệu chỉ định một đường dẫn nguồn không sử dụng được, thư sẽ được trả về. Cuối cùng, nếu bộ định tuyến phải phân mảnh một datagram nhưng cờ Don't Fragment được đặt, biểu đồ dữ liệu sẽ bị loại bỏ và một tin nhắn được trả về.

Bộ định tuyến sẽ trả về một thông báo **vượt quá thời gian** nếu tuổi thọ của datagram hết hạn. Máy chủ sẽ gửi thông báo này nếu nó không thể hoàn thành lắp ráp lại trong một giới hạn thời gian.

Lỗi cú pháp hoặc ngữ nghĩa trong tiêu đề IP sẽ khiến thông báo **sự cố tham số** được trả về bởi bộ định tuyến hoặc máy chủ. Ví dụ, một đối số không chính xác có thể được cung cấp với một tùy chọn. Trường Tham số chứa một con trỏ đến octet trong tiêu đề ban đầu nơi phát hiện lỗi.

Thông điệp **làm quen nguồn** cung cấp một hình thức kiểm soát dòng chảy thô sơ. Bộ định tuyến hoặc máy chủ đích có thể gửi tin nhắn này đến máy chủ nguồn, yêu cầu nó giảm tốc độ gửi lưu lượng truy cập đến đích internet. Khi nhận được thông báo dập tắt nguồn, máy chủ nguồn sẽ cắt giảm tốc độ gửi lưu lượng truy cập đến đích được chỉ định cho đến khi nó không còn nhận được tin nhắn dập tắt nguồn. Thông báo dập nguồn có thể được sử dụng bởi một bộ định tuyến hoặc máy chủ phải loại bỏ các biểu đồ dữ liệu vì bộ đệm đầy đủ. Trong trường hợp đó, bộ định tuyến hoặc máy chủ sẽ phát hành thông báo dập tắt nguồn cho mọi datagram mà nó loại bỏ. Ngoài ra, một hệ thống có thể dự đoán tắc nghẽn và phát hành thông điệp dập tắt nguồn khi bộ đệm của nó tiếp cận dung lượng. Trong trường hợp đó, biểu đồ dữ liệu được đề cập trong thông điệp dập tắt nguồn cũng có thể được gửi. Do đó, việc nhận thông điệp dập tắt nguồn không có nghĩa là việc phân phối hoặc không giao dịch của biểu đồ dữ liệu tương ứng.

Bộ định tuyến gửi thông báo **chuyển hướng** đến máy chủ trên bộ định tuyến được kết nối trực tiếp để tư vấn cho máy chủ của một tuyến đường tốt hơn đến một điểm đến cụ thể. Sau đây là một ví dụ, sử dụng Hình 18.8. Router R1 nhận được một datagram từ host C trên mạng Y, mà R1 được đính kèm. R1 kiểm tra bảng định tuyến của nó và có được địa chỉ cho bộ định tuyến tiếp theo, R2, trên tuyến đường đến mạng đích internet của datagram, Z. Bởi vì R2 và máy chủ được xác định bởi địa chỉ nguồn internet của datagram là trên cùng một mạng, R1 gửi một thông báo chuyển hướng đến C. Thông báo chuyển hướng khuyên máy chủ gửi lưu lượng truy cập của mình cho mạng Z trực tiếp đến bộ định tuyến R2, bởi vì đây là một đường dẫn ngắn hơn đến đích. Bộ định tuyến chuyển tiếp biểu đồ dữ liệu ban đầu đến đích internet của nó (thông qua R2). Địa chỉ của R2 được chứa trong trường tham số của thông điệp chuyển hướng.

Các thông điệp trả lời **tiếng vang**  và **tiếng vang** cung cấp một cơ chế để kiểm tra rằng giao tiếp có thể giữa các thực thể. Người nhận thư echo có nghĩa vụ trả lại thư trong thư trả lời tiếng vang. Số nhận dạng và số thứ tự được liên kết với thông báo tiếng vang được khớp trong thư trả lời tiếng vang. Mã định danh có thể được sử dụng như một điểm truy cập dịch vụ để xác định một phiên cụ thể và số thứ tự có thể được tăng lên trên mỗi yêu cầu tiếng vang được gửi.

Dấu **thời gian**  và dấu thời gian **trả lời** tin nhắn cung cấp một cơ chế để lấy mẫu các đặc điểm chậm trễ của internet. Người gửi thư dấu thời gian có thể bao gồm số nhận dạng và số thứ tự trong trường tham số và bao gồm thời gian thư được gửi (dấu thời gian bắt nguồn). Người nhận ghi lại thời gian nhận được tin nhắn và thời gian truyền thông báo trả lời trong thư trả lời dấu thời gian. Nếu thông báo dấu thời gian được gửi bằng cách sử dụng định tuyến nguồn nghiêm ngặt, thì các đặc điểm chậm trễ của một tuyến đường cụ thể có thể được đo lường.

Yêu **cầu mặt nạ địa chỉ**  và thông báo trả lời mặt nạ **địa chỉ** rất hữu ích trong môi trường bao gồm mạng con. Yêu cầu mặt nạ địa chỉ và tin nhắn trả lời cho phép máy chủ tìm hiểu mặt nạ địa chỉ cho mạng LAN mà nó kết nối. Máy chủ phát thông báo yêu cầu mặt nạ địa chỉ trên MẠNG LAN. Bộ định tuyến trên MẠNG LAN trả lời bằng thông báo trả lời mặt nạ địa chỉ có chứa mặt nạ địa chỉ.

#### Giao thức Giải quyết Địa chỉ (ARP)

Trước đó trong chương này, chúng tôi đã đề cập đến các khái niệm về địa chỉ toàn cầu (địa chỉ IP) và một địa chỉ phù hợp với sơ đồ địa chỉ của mạng mà máy chủ được đính kèm (địa chỉ mạng con). Đối với mạng cục bộ, địa chỉ sau là địa chỉ MAC, cung cấp địa chỉ vật lý cho cổng máy chủ gắn liền với mạng LAN. Rõ ràng, để cung cấp một datagram IP cho một máy chủ đích, một bản đồ phải được thực hiện từ địa chỉ IP đến địa chỉ mạng con cho bước nhảy cuối cùng đó. Nếu một datagram đi qua một hoặc nhiều bộ định tuyến giữa máy chủ nguồn và đích, thì việc lập bản đồ phải được thực hiện trong bộ định tuyến cuối cùng, được gắn vào cùng một mạng con với máy chủ đích. Nếu một bảng dữ liệu được gửi từ máy chủ này sang máy chủ khác trên cùng một mạng con, thì máy chủ nguồn phải thực hiện bản đồ. Trong cuộc thảo luận sau đây, chúng tôi sử dụng *hệ thống* thuật ngữ để chỉ thực thể thực hiện lập bản đồ.

Để lập bản đồ từ địa chỉ IP đến địa chỉ mạng con, một số cách tiếp cận có thể, bao gồm

* Mỗi hệ thống có thể duy trì một bảng địa chỉ IP cục bộ và khớp địa chỉ mạng con cho các phóng viên có thể. Cách tiếp cận này không phù hợp với việc bổ sung dễ dàng và tự động của máy chủ mới vào mạng con.
* Địa chỉ mạng con có thể là một tập hợp con của phần mạng của địa chỉ IP. Tuy nhiên, toàn bộ địa chỉ internet dài 32 bit và đối với hầu hết các loại mạng con (ví dụ: Ethernet), trường Địa chỉ máy chủ dài hơn 32 bit.
* Một thư mục tập trung có thể được duy trì trên mỗi mạng con có chứa bản đồ địa chỉ ip-mạng con. Đây là một giải pháp hợp lý cho nhiều mạng.
* Một giao thức giải quyết địa chỉ có thể được sử dụng. Đây là một cách tiếp cận đơn giản hơn so với việc sử dụng một thư mục tập trung và rất phù hợp với các NHÀ GIAO DỊCH.

RFC 826 định nghĩa Giao thức giải quyết địa chỉ (ARP), cho phép phân phối động thông tin cần thiết để xây dựng bảng để dịch địa chỉ IP A thành địa chỉ Ethernet 48 bit; giao thức có thể được sử dụng cho bất kỳ mạng phát sóng nào. ARP khai thác tài sản phát sóng của mạng LAN; cụ thể là, việc truyền từ bất kỳ thiết bị nào trên mạng được nhận bởi tất cả các thiết bị khác trên mạng. ARP hoạt động như sau:

* 1. Mỗi hệ thống trên MẠNG LAN duy trì một bảng ánh xạ địa chỉ ip-subnetwork đã biết.
  2. Khi cần một địa chỉ mạng con cho địa chỉ IP và bản đồ không được tìm thấy trong bảng của hệ thống, hệ thống sử dụng ARP trực tiếp trên giao thức LAN (vídụ: IEEE 802) để phát yêu cầu. Thông báo phát sóng chứa địa chỉ IP mà cần một địa chỉ mạng con.
  3. Các máy chủ khác trên mạng con nghe tin nhắn ARP và trả lời khi trận đấu xảy ra. Câu trả lời bao gồm cả IP và địa chỉ mạng con của máy chủ trả lời.
  4. Yêu cầu ban đầu bao gồm địa chỉ IP và địa chỉ mạng con của máy chủ yêu cầu. Bất kỳ máy chủ quan tâm nào cũng có thể sao chép thông tin này vào bảng địa phương của mình, tránh sự cần thiết của các tin nhắn ARP sau này.
  5. Thông báo ARP cũng có thể được sử dụng đơn giản để phát địa chỉ IP và địa chỉ mạng con của máy chủ, vì lợi ích của những người khác trên mạng con.

### 18.7 CÁC TRANG WEB VÀ ĐỌC ĐƯỢC KHUYẾN NGHỊ

[RODR02] cung cấp phạm vi bảo hiểm rõ ràng về tất cả các chủ đề trong chương này. Phạm vi bảo hiểm tốt của internetworking và IPv4 có thể được tìm thấy trong [COME06] và [STEV94]. [SHAN02] và [KENT87] cung cấp các cuộc thảo luận hữu ích về sự phân mảnh. [LEE05] là một mô tả kỹ thuật kỹ lưỡng IPv6. [KESH98] cung cấp một cái nhìn hướng dẫn về chức năng router hiện tại và tương lai. [METZ02] và [DOI94] mô tả tính năng anycast IPv6. Đối với người đọc quan tâm đến một cuộc thảo luận chuyên sâu hơn về địa chỉ IP, [SPOR03] cung cấp rất nhiều chi tiết.

**Come06** Comer, D. *Internetworking với TCP / IP, Tập I: Nguyên tắc, Giao thức và Kiến trúc*. Sông Upper Saddle, NJ: Prentice Hall, 2006.

**DOI04** Doi, S., et al. "IPv6 Anycast for Simple and Effective Communications." *Tạp chí Truyền thông IEEE,*tháng 5 năm 2004.

**HUIT98** Huitema,C. *IPv6: Giao thức Internet mới*. Upper Saddle River, NJ:P rentice Hall, 1998.

**KENT87** Kent, C., và Mogul, J." Sự phân mảnh được coi là có hại". *Đánh giá truyền thông máy tính ACM,*tháng 10 năm 1987.

**KESH98** Keshav, S., và Sharma, R." Các vấn đề và xu hướng trong thiết kế router". *Tạp chí Truyền thông IEEE,*tháng 5 năm 1998.

**Lee05** Lee, H. *Hiểu IPv6.* New York: Springer-Verlag, 2005.

**METZ02** Metz C." IP Anycast." *Điện toán Internet IEEE,*tháng 3 năm 2002.

**RODR02** Rodriguez, A., et al. *Hướng dẫn TCP / IP và Tổng quan kỹ thuật*. Sông Upper Saddle: NJ: Prentice Hall, 2002.

**SHAN02** Shannon, C.; Moore, D.; Và Claffy,K. "Beyond Folklore: Observations on Fragmented Traffic." *Giao dịch IEEE/ACM trên mạng,*tháng 12 năm 2002.

**SPOR03** Sportack,M. *IP giải quyết các nguyên tắc cơ bản*. Indianapolis, IN: Cisco Press, 2003.

**STEV94** Stevens, W. *TCP /IP Minh họa, Tập 1: Các giao thức*. Đọc, MA: Addison-Wesley, 1994.

#### CHƯƠNG 18 / GIAO THỨC INTERNET

**Các trang web được đề xuất:**

* **IPv6:** Thông tin về IPv6 và các chủ đề liên quan.
* **Nhóm làm việc IPv6:** Được IETF điều lệ để phát triển các tiêu chuẩn liên quan đến IPv6.Trang web bao gồm tất cả các bản nháp RFC và Internet có liên quan.
* **Diễn đàn IPv6:** Một tập đoàn công nghiệp quảng bá các sản phẩm liên quan đến IPv6. Bao gồm một số sách trắng và bài viết.

### 18.8 THUẬT NGỮ CHÍNH, XEM LẠI CÂU HỎI VÀ VẤN ĐỀ

#### Điều khoản chính

|  |  |  |
| --- | --- | --- |
| phát sóng datagram trọn đời hệ thống phân mảnh hệ thống trung gian  Internet  Giao thức Thông báo Điều khiển Internet (ICMP) | Giao thức Internet (IP) internetworking  bộ định tuyến đa đúc IPv4 IPv6 trong mạng | phân đoạn mạng con mặt nạ mạng con  lớp giao thông unicast |

#### Xem lại Câu hỏi

**18.1.** Đưa ra một số lý do để sử dụng phân mảnh và lắp ráp lại.

**18.2.** Liệt kê các yêu cầu đối với cơ sở làm việc internet.

**18.3.** Ưu và nhược điểm của việc hạn chế lắp ráp lại điểm cuối so với việc cho phép lắp ráp lại trên đường là gì?

**18.4.** Giải thích chức năng của ba lá cờ trong tiêu đề IPv4.

**18.5.** Kiểm tra tiêu đề IPv4 được tính như thế nào?

**18.6.** Sự khác biệt giữa lớp lưu lượng truy cập và trường nhãn dòng chảy trong tiêu đề IPv6 là gì?

**18.7.** Giải thích ngắn gọn ba loại địa chỉ IPv6.

**18.8.** Mục đích của mỗi loại tiêu đề IPv6 là gì?

#### Vấn đề

**18.1** Mặc dù không được nêu rõ ràng, đặc điểm kỹ thuật Giao thức Internet (IP), RFC 791, xác định kích thước gói tối thiểu mà công nghệ mạng phải hỗ trợ để cho phép IP chạy qua nó.

1. Đọc Phần 3.2 của RFC 791 để tìm hiểu giá trị đó. Nó là gì?
2. Thảo luận về lý do để áp dụng giá trị cụ thể đó.

**18.2** Trong cuộc thảo luận về IP, người ta đã đề cập rằng định *danh, không phân mảnh nhận dạng*và các tham số thời gian để *trực tiếp* có trong Gửi nguyên thủy nhưng không phải trong Deliver nguyên thủy vì chúng chỉ quan tâm đến IP. Đối với mỗi tham số này, cho biết liệu nó có đáng lo ngại hay không cho thực thể IP trong nguồn, các thực thể IP trong bất kỳ bộ định tuyến trung gian nào và thực thể IP trong các hệ thống cuối đích. Biện minh cho câu trả lời của bạn.

##### 18.8 / THUẬT NGỮ CHÍNH, CÂU HỎI ÔN TẬP VÀ CÁC VẤN ĐỀ

**18.3** Tiêu đề trên cao trong giao thức IP là gì?

**18.4** Mô tả một số trường hợp mà có thể mong muốn sử dụng định tuyến nguồn thay vì để các bộ định tuyến đưa ra quyết định định tuyến.

**18.5** Do sự phân mảnh, một datagram IP có thể đến trong một số mảnh, không nhất thiết phải theo thứ tự chính xác. Thực thể IP tại hệ thống đầu nhận phải tích lũy các mảnh này cho đến khi biểu đồ dữ liệu ban đầu được khôi phục lại.

1. Hãy xem xét rằng thực thể IP tạo ra một bộ đệm để lắp ráp trường dữ liệu trong biểu đồ dữ liệu gốc. Khi lắp ráp tiến hành, bộ đệm sẽ chứa các khối dữ liệu và "lỗ hổng" giữa các khối dữ liệu. Mô tả một thuật toán để lắp ráp lại dựa trên khái niệm này.
2. Đối với thuật toán một phần (a), cần phải theo dõi các lỗ. Mô tả một cơ chế đơn giản để làm điều này.
   1. Một datagram 4480 octet sẽ được truyền đi và cần phải được phân mảnh vì nó sẽ đi qua ethernet với tải trọng tối đa 1500 octets. Hiển thị tổng chiều dài, cờ nhiều hơn và giá trị Bù trừ Mảnh trong mỗi đoạn kết quả.
   2. Hãy xem xét một tiêu đề bao gồm 10 octets, với checkum trong hai octets cuối cùng (điều này không tương ứng với bất kỳ định dạng tiêu đề thực tế) với nội dung sau (trong hexadecimal): 01 00 F6 F7 F4 F5 F2 03 00 00
3. Tính toán checkum. Hiển thị tính toán của bạn.
4. Hiện gói kết quả.
5. Xác minh checkum.
   1. Checkum IP cần được tính toán lại tại các bộ định tuyến vì những thay đổi đối với tiêu đề IP, chẳng hạn như trường trọn đời. Có thể tính toán lại checkum từ đầu. Đề xuất một thủ tục liên quan đến tính toán ít hơn. *Gợi*ý: Giả sử giá trị trong octet *k* được thay đổi bởi Z = new\_value - old\_value; xem xét ảnh hưởng của thay đổi này đốivới checkum.
   2. Một datagram IP sẽ bị phân mảnh. Những tùy chọn nào trong trường tùy chọn cần được sao chép vào tiêu đề của từng mảnh và chỉ cần giữ lại trong đoạn đầu tiên? Biện minh cho việc xử lý từng lựa chọn.
   3. Một thông báo lớp vận chuyển bao gồm 1500 bit dữ liệu và 160 bit tiêu đề được gửi đến một lớp internet, kết hợp thêm 160 bit tiêu đề. Điều này sau đó được truyền qua hai mạng, mỗi mạng sử dụng tiêu đề gói 24 bit. Mạng đích có kích thước gói tối đa là 800 bit. Có bao nhiêu bit, bao gồm cả tiêu đề, được gửi đến giao thức lớp mạng tại đích đến?
   4. Kiến trúc được đề xuất bởi Hình 18.2 sẽ được sử dụng. Những chức năng nào có thể được thêm vào các bộ định tuyến để giảm bớt một số vấn đề gây ra bởi các mạng cục bộ và đường dài không phù hợp?
   5. Internetworking có nên quan tâm đến định tuyến nội bộ của mạng không? Tại sao hoặc tại sao không?
   6. Cung cấp các giá trị tham số sau đây cho từng lớp mạng A, B và C. Hãy chắc chắn xem xét bất kỳ địa chỉ đặc biệt hoặc dành riêng nào trong tính toán của bạn. **a.** Số bit trong phần mạng của địa chỉ
6. Số bit trong phần lưu trữ của địa chỉ
7. Số lượng mạng riêng biệt được phép
8. Số lượng máy chủ riêng biệt trên mỗi mạng được phép
9. Phạm vi số nguyên của octet đầu tiên
   1. Bao nhiêu phần trăm trong tổng không gian địa chỉ IP mà mỗi lớp mạng đại diện?
   2. Sự khác biệt giữa mặt nạ mạng con cho địa chỉ Loại A với 16 bit cho ID mạng con và địa chỉ loại B với 8 bit cho ID mạng con là gì?
   3. Mặt nạ mạng con 255.255.0.255 có hợp lệ cho địa chỉ hạng A không?

**18.17** Với địa chỉ mạng 192.168.100.0 và mặt nạ mạng con 255.255.255.192,

1. Có bao nhiêu mạng con được tạo ra?
2. Có bao nhiêu máy chủ trên mỗi mạng con?

**18.18** Với một công ty với sáu bộ phận riêng lẻ và mỗi bộ phận có mười máy tính hoặc thiết bị nối mạng, mặt nạ nào có thể được áp dụng cho mạng công ty để cung cấp mạng con cần thiết để chia mạng như nhau?

**18.19** Trong định tuyến và địa chỉ hiện đại, ký hiệu thường được sử dụng được gọi là định tuyến liên danh không lớp hoặc CIDR. Với CIDR, số lượng bit trong mặt nạ được chỉ định theo cách sau: 192.168.100.0/24. Điều này tương ứng với mặt nạ 255.255.255.0. Nếu ví dụ này sẽ cung cấp cho 256 địa chỉ máy chủ trên mạng, có bao nhiêu địa chỉ được cung cấp với những điều sau đây? **a.** 192.168.100.0/23

**b.** 192.168.100.0/25

**18.20** Tìm hiểu về mạng của bạn. Sử dụng lệnh "ipconfig"",nếu tự tin", hoặc "winipcfg", chúng ta có thể tìm hiểu không chỉ địa chỉ IP của chúng ta mà còn các tham số mạng khác. Bạn có thể xác định mặt nạ, cổngvà số lượng địa chỉ có sẵn trên mạng của bạn không? **18.21**  Sử dụng địa chỉ IP và mặt nạ của bạn, địa chỉ mạng của bạn là gì? Điều này được xác định bằng cách chuyển đổi địa chỉ IP và mặt nạ thành nhị phân và sau đó tiến hành một hoạt động AND hợp lý một chút. Ví dụ: với địa chỉ 172.16.45.0 và mặt nạ 255.255.224.0, chúng tôi sẽ phát hiện ra rằng địa chỉ mạng sẽ là 172.16.32.0.

**18.22** So sánh các trường riêng lẻ của tiêu đề IPv4 với tiêu đề IPv6. Tài khoản cho chức năng được cung cấp bởi mỗi trường IPv4 bằng cách hiển thị cách chức năng tương tự được cung cấp trong IPv6.

**18.23** Biện minh cho thứ tự được đề xuất trong đó tiêu đề mở rộng IPv6 xuất hiện (tức là tại sao tiêu đề Tùy chọn Hop-by-Hop trước, tại sao tiêu đề Định tuyến trước tiêu đề Fragment, v.v.).

**18.24** Tiêu chuẩn IPv6 tuyên bố rằng nếu một gói có nhãn dòng chảy nonzero đến bộ định tuyến và bộ định tuyến không có thông tin cho nhãn dòng chảy đó, bộ định tuyến nên bỏ qua nhãn dòng chảy và chuyển tiếp gói.

1. Những nhược điểm của việc coi sự kiện này là lỗi, loại bỏ gói và gửi tin nhắn ICMP là gì?
2. Có những tình huống trong đó định tuyến gói như thể nhãn dòng chảy của nó bằng không sẽ gây ra kết quả sai? Giải thích.

**18.25** Cơ chế dòng chảy IPv6 giả định rằng trạng thái liên quan đến một nhãn dòng chảy nhất định được lưu trữ trong các bộ định tuyến, vì vậy họ biết cách xử lý các gói mang nhãn dòng chảy đó. Một yêu cầu thiết kế là xả các nhãn dòng chảy không còn được sử dụng (nhãn dòng chảy cũ) từ các bộ định tuyến.

1. Giả sử rằng một nguồn luôn gửi thông báo điều khiển đến tất cả các bộ định tuyến bị ảnh hưởng xóa nhãn luồng khi nguồn kết thúc với luồng đó. Trong trường hợp đó, làm thế nào một nhãn dòng chảy cũ có thể tồn tại?
2. Đề xuất bộ định tuyến và cơ chế nguồn để khắc phục vấn đề nhãn dòng chảy cũ.
   1. Câu hỏi đặt ra là gói nào được tạo ra bởi một nguồn nên mang nhãn dòng chảy nonzero IPv6. Đối với một số ứng dụng, câu trả lời là hiển nhiên. Trao đổi dữ liệu nhỏ nên có nhãn dòng chảy bằng không vì không đáng để tạo luồng cho một vài gói. Dòng chảy thời gian thực nên có nhãn dòng chảy; những dòng chảy như vậy là lý do chính khiến nhãn dòng chảy được tạo ra. Một vấn đề khó khăn hơn là phải làm gì với các đồng nghiệp gửi một lượng lớn lưu lượng truy cập nỗ lực tốt nhất (ví dụ: kết nối TCP). Tạo trường hợp để gán nhãn luồng duy nhất cho mỗi kết nối TCP dài hạn. Hãy làm một trường hợp vì đã không làm điều này.
   2. Các thông số kỹ thuật IPv6 ban đầu kết hợp các trường Traffic Class và Flow Label thành một trường Flow Label 28-bit duy nhất. Điều này cho phép các dòng chảy để xác định lại việc giải thích các giá trị ưu tiên khác nhau. Đề xuất lý do tại sao đặc điểm kỹ thuật cuối cùng bao gồm trường Ưu tiên như một trường riêng biệt.
   3. Đối với định tuyến IPv6 loại 0, hãy chỉ định thuật toán để cập nhật tiêu đề IPv6 và Định tuyến theo các nút trung gian.

1. Một cuộc thảo luận về checkum này được chứa trong Phụ lục K. [↑](#footnote-ref-1)