

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG.

Khoa Đào tạo sau đại học

-----🙞🙜🕮🙞🙜-----



**TIỂU LUẬN**

SO SÁNH IPv4 VÀ IPv6

|  |  |  |
| --- | --- | --- |
| Giảng viên | : | TS. Nguyễn Chiến Trinh |
| Học viên | : | Phí Mạnh Kiên - B19CHCS007  Nguyễn Diệu Linh - B19CHCS008  Phạm Hoàng Long - B19CHCS010 |
| Lớp | : | M19CQCS01-B |

Hà Nội, 07/2020

Mục lục

[Mục lục i](#_Toc45972046)

[CHƯƠNG 1. Tìm hiểu IPv4 1](#_Toc45972047)

[1.1. Cấu trúc địa chỉ IPv4 1](#_Toc45972048)

[1.1.1. Giới thiệu 1](#_Toc45972049)

[1.1.2. Thành phần và khuôn dạng địa chỉ IPv4 1](#_Toc45972050)

[1.1.3. Phân lớp địa chỉ IPv4 2](#_Toc45972051)

[1.1.4. Đánh địa chỉ IPv4 4](#_Toc45972052)

[1.1.5. Địa chỉ mạng con và mặt nạ mạng con 5](#_Toc45972053)

[1.2. Khuôn dạng gói tin IPv4 6](#_Toc45972054)

[1.3. Giải pháp định tuyến theo địa chỉ IPv4 9](#_Toc45972055)

[1.3.1. Các phần tử cơ bản của một hệ thống định tuyến. 9](#_Toc45972056)

[1.3.2. Xử lý gói tin ở bộ định tuyến. 11](#_Toc45972057)

[1.3.3. Xử lý gói tin khi tới đích. 11](#_Toc45972058)

[1.3.4. Định tuyến trên mạng Internet 12](#_Toc45972059)

[1.4. Những hạn chế của IPv4 14](#_Toc45972060)

[1.4.1. Sự giới hạn về kích thước địa chỉ 14](#_Toc45972061)

[1.4.2. Cấu trúc định tuyến không hiệu quả 15](#_Toc45972062)

[1.4.3. Hạn chế về tính bảo mật và kết nối đầu cuối – đầu cuối 15](#_Toc45972063)

[1.5. Kết luận. 15](#_Toc45972064)

[CHƯƠNG 2. Tìm hiểu IPv6 17](#_Toc45972065)

[2.1. Đặc điểm của IPv6 17](#_Toc45972066)

[2.1.1. Kiểu định dạng tiêu đề mới 17](#_Toc45972067)

[2.1.2. Không gian địa chỉ mở rộng 17](#_Toc45972068)

[2.1.3. Cơ sở hạn tầng định tuyến và đánh địa chỉ phân cấp và hiệu quả 17](#_Toc45972069)

[2.1.4. Cấu hình địa chỉ Stateful và Stateless 18](#_Toc45972070)

[2.1.5. Bảo mật 18](#_Toc45972071)

[2.1.6. Hỗ trợ tốt hơn cho QoS 18](#_Toc45972072)

[2.1.7. Giao thức mới cho sự tương tác Node láng giềng 18](#_Toc45972073)

[2.1.8. Có khả năng mở rộng 19](#_Toc45972074)

[2.2. Sự khác biệt giữa IPv4 và IPv6 19](#_Toc45972075)

[2.3. Đánh địa chỉ Ipv6 20](#_Toc45972076)

[2.3.1. Không gian địa chỉ IPv6 20](#_Toc45972077)

[2.3.2. Cú pháp địa chỉ IPv6 20](#_Toc45972078)

[2.3.3. Prefix của IPv6 21](#_Toc45972079)

[2.3.4. Các dạng địa chỉ IPv6 22](#_Toc45972080)

[2.3.5. Sự tương thích địa chỉ 28](#_Toc45972081)

[2.3.6. Địa chỉ IPv4 và sự tương đương IPv6 29](#_Toc45972082)

[2.4. Khuôn dạng gói tin IPv6 30](#_Toc45972083)

[2.4.1. Khuôn dạng gói tin IPv6 30](#_Toc45972084)

[2.4.2. So sánh khuôn dạng IPv4 và IPv6 31](#_Toc45972085)

[2.4.3. Các tiêu đề mở rộng của IPv6 33](#_Toc45972086)

[2.5. Những ưu nhược điểm và khó khăn khi triển khai IPv6 34](#_Toc45972087)

[2.5.1. Ưu nhược điểm IPv6 34](#_Toc45972088)

[2.5.2. Khó khăn gặp phải khi triển khai Ipv6 34](#_Toc45972089)

[2.6. Kết luận 35](#_Toc45972090)

[CHƯƠNG 3. TRIỂN KHAI MẠNG IPv6 36](#_Toc45972091)

[3.1. Triển khai mạng Ipv6 trên nền Ipv4 36](#_Toc45972092)

[3.1.1. Các vấn đề chung 36](#_Toc45972093)

[3.1.2. Mục đích 37](#_Toc45972094)

[3.2. Các cơ chế chuyển đổi 38](#_Toc45972095)

[**3.2.1. Lớp IP song song ( Dual IP layer).** 40](#_Toc45972096)

[**3.2.2. Kỹ thuật đường hầm** 41](#_Toc45972097)

[**3.2.3. Kỹ thuật biên dịch (NAT-PT)** 50](#_Toc45972098)

[3.3. Kết luận 52](#_Toc45972099)

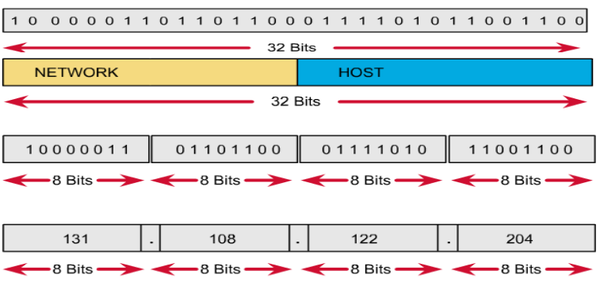
1. Tìm hiểu IPv4
   1. Cấu trúc địa chỉ IPv4
      1. Giới thiệu

IPv4 (tên tiếng anh là Internet Protocol version 4): giao thức internet phiên bản 4, là phiên bản thứ tư trong quá trình phát triển của các giao thức Internet (IP). Đây là phiên bản đầu tiên của IP được sử dụng rộng rãi và là cơ sở của mạng Internet.

Giao thức này được công bố bởi IETF trong phiên bản RFC 791 (tháng 9 năm 1981), thay thế cho phiên bản RFC 760 (công bố vào tháng 1 năm 1980). Giao thức này cũng được chuẩn hóa bởi bộ quốc phòng Mỹ trong phiên bản MIL-STD-1777.

* + 1. Thành phần và khuôn dạng địa chỉ IPv4

Địa chỉ IPv4 gồm 32 bit chia thành 4 Octet (mỗi Octet gồm 8 bit tương đương với 1 byte), cách đếm từ trái qua phải từ bit 1 cho đến bit 32. Các Octet phân tách nhau bằng một dấu chấm (.). Địa chỉ IPv4 có thể được viết dưới dạng nhị phân hoặc thập phân. Dạng thập phân được sử dụng phổ biến do thân thiện với con người hơn.

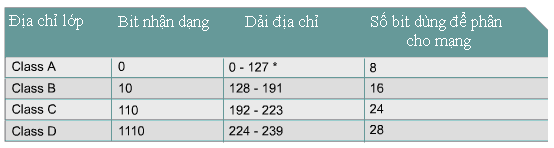


Khuôn dạng địa chỉ IPv4.

Ban đầu, địa chỉ IPv4 được chia thành hai thành phần là Network ID và Host ID. Với cách chia này, số lượng network bị giới hạn ở con số 256, quá ít so với nhu cầu thực tế. Để vượt qua giới hạn này, việc phân lớp mạng đã được định nghĩa, địa chỉ IPv4 có thêm thành phần bit nhận dạng lớp ở đầu.

* + 1. Phân lớp địa chỉ IPv4

Địa chỉ IPv4 được chia thành các lớp, A, B, C, D, E. Hiện tại đã dùng hết lớp A, B và gần hết lớp C, còn lớp D và E Tổ chức Internet đang để dành cho mục đích khác không phân, nên chúng ta chỉ nghiên cứu 3 lớp đầu.

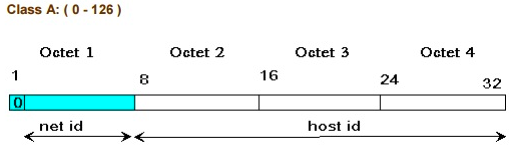


Cấu trúc các lớp địa chỉ IPV4

Qua cấu trúc các lớp địa chỉ IPv4 chúng ta có nhận xét sau:

* Bit nhận dạng nằm đầu địa chỉ IP: của lớp A là 0, của lớp B là 10, của lớp C là 110.
* Địa chỉ lớp A: Địa chỉ mạng ít và địa chỉ máy chủ trên từng mạng nhiều.
* Địa chỉ lớp B: Địa chỉ mạng vừa phải và địa chỉ máy chủ trên từng mạng vừa phải.
* Địa chỉ lớp C: Địa chỉ mạng nhiều và địa chỉ máy chủ trên từng mạng ít.
* Lớp D có 4 bit đầu tiên để nhận dạng là 1110, còn lớp E có 5 bit đầu tiên để nhận dạng là 11110.

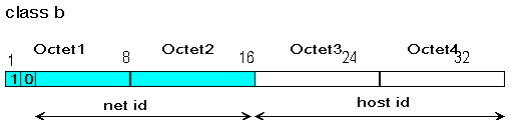
***Lớp A*** thực hiện trong những mạng lớn có khả năng hỗ trợ trên 16 triệu máy. Chỉ bao gồm octet đầu tiên được sử dụng để chỉ ra địa chỉ mạng, 3 octet còn lại sử dụng để xác định địa chỉ của host trong mạng.



Cấu trúc địa chỉ IPv4 lớp A.

Bit đầu tiên của lớp A luôn bằng 0. Số thấp nhất của octet đầu tiên có thể thể hiện là 0, và giá trị lớn nhất là 127. Tuy nhiên giá trị 0 và 127 của octet đầu tiên không được sử dụng trong việc định địa chỉ mạng, do đó tất cả các địa chỉ mạng của lớp A sẽ thực hiện giá trị từ 1 tới 126 của octet đầu tiên.

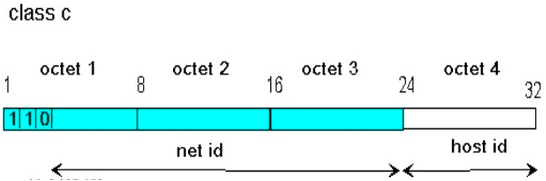
***Lớp B*** được thiết kế để hỗ trợ những nhu cầu cho những mạng lớn. Địa chỉ lớp B sử dụng 2 trong số 4 octet đầu tiên làm địa chỉ mạng, 2 octet còn lại được sử dụng để chỉ ra địa chỉ host.



Cấu trúc địa chỉ IPv4 lớp B.

Hai bit đầu của octet đầu tiên của một địa chỉ thuộc lớp B luôn là 10, 6 bit còn lại của octet đầu tiên có thể thay đổi là 0 hoặc 1. Do đó giá trị nhỏ nhất của octet đầu tiên của một địa chỉ lớp B sẽ là 10000000 = 128, giá trị lớn nhất sẽ là 10111111 = 191. Bất cứ địa chỉ nào có giá trị của octet đầu tiên nằm trong khoảng từ 128 – 191 đều là những địa chỉ mạng của lớp B.

***Lớp C*** có giá trị 3 bit đầu tiên của một địa chỉ luôn là 110. Do đó giá trị nhỏ nhất của octet đầu tiên của một địa chỉ lớp C có thể là 11000000 = 192, giá trị lớn nhất là 11011111 = 223. Nếu một địa chỉ mạng có giá trị của octet đầu tiên rơi vào trong khoảng 191 – 223 thì đó là một địa chỉ IPV4 thuộc lớp C. Lớp C thực hiện 3 octet là địa chỉ mạng còn 1 octet còn lại được sử dụng làm địa chỉ host. Nó có khả năng hỗ trợ 254 địa chỉ host cho mỗi mạng thuộc về lớp C.



Cấu trúc địa chỉ IPv4 lớp C.

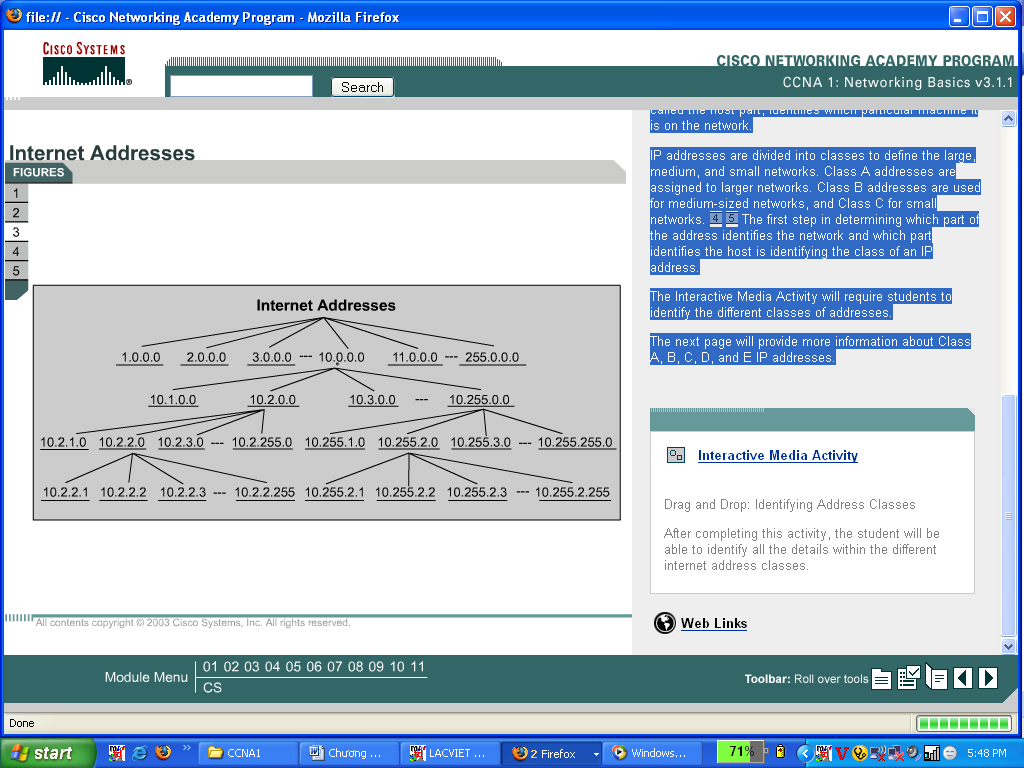
Lớp D được tạo ra để tạo khả năng về địa chỉ multicast. Một địa chỉ IPV4 multicast là một địa chỉ có khả năng thực hiện việc truyền thông tin tới một nhóm các máy trạm với địa chỉ IPV4 unicast. Do đó, một máy trạm khi sử dụng địa chỉ multicast có khả năng truyền đồng thời một gói tin tới nhiều người nhận.

Bốn bit đầu tiên của một địa chỉ IPV4 của lớp D luôn là 1110. Do đó octet đầu tiên của một địa chỉ mạng thuộc về lớp C có giá trị nhỏ nhất là: 11100000 = 224 và giá trị lớn nhất sẽ là 11101111 = 239.

Địa chỉ lớp E thực hiện trong phòng thí nghiệm phục vụ mục đích nghiên cứu. Bốn bit đầu tiên của một địa chỉ của lớp E là 1111. Do đó khoảng giá trị của octet đầu tiên của một địa chỉ lớp E sẽ là: 240 – 255.

* + 1. Đánh địa chỉ IPv4

Một bộ định tuyến sử dụng địa chỉ IPV4 để chuyển tiếp gói tin từ mạng nguồn tới mạng đích. Gói tin phải chỉ ra cả địa chỉ mạng nguồn và mạng đích. Khi một gói được nhận tại bộ định tuyến, nó sẽ xác định địa chỉ mạng đích và xác định đường đi của gói tin và chuyển tiếp gói tin qua cổng tương ứng. Mỗi địa chỉ IPV4 cũng gồm có 2 phần: nhận dạng địa chỉ mạng - chỉ ra mạng, và nhận dạng địa chỉ host - chỉ ra host. Mỗi octet đều có thể chia thành những nhóm địa chỉ mạng khác nhau, quá trình chia địa chỉ có thể được thực hiện theo mô hình phân cấp.



Mô hình phân cấp địa chỉ IPv4.

Các địa chỉ được thực hiện theo mô hình phân cấp bởi nó chứa nhiều mức khác nhau. Một địa chỉ IPV4 thực hiện 2 chỉ số về địa chỉ mạng và địa chỉ host trong cùng một địa chỉ. Địa chỉ này phải là duy nhất, bởi khi thực hiện một địa chỉ trùng lặp sẽ dẫn đến những vấn đề về định tuyến. Phần đầu là địa chỉ mạng (hay địa chỉ của hệ thống), phần thứ 2 là địa chỉ host trong mạng.

* + 1. Địa chỉ mạng con và mặt nạ mạng con

Trước khi nghiên cứu vấn đề này chúng ta cần phải hiểu qua một số khái niệm liên quan tới việc phân địa chỉ các mạng con.

***Mặt nạ mặc định (Default Mask):*** được định nghĩa trước cho từng lớp địa chỉ A, B, C. Thực chất là giá trị thập phân cao nhất (khi tất cả 8 bit đều bằng 1) trong các Octet dành cho địa chỉ mạng – Net ID.

Mặt nạ mặc định:

* Lớp A: 255.0.0.0
* Lớp B: 255.255.0.0
* Lớp C: 255.255.255.0

***Mặt nạ mạng con (Subnet Mask):*** là kết hợp của mặt nạ mặc định với giá trị thập phân cao nhất của các bit lấy từ các Octet của địa chỉ máy chủ sang phần địa chỉ mạng để tạo địa chỉ mạng con.

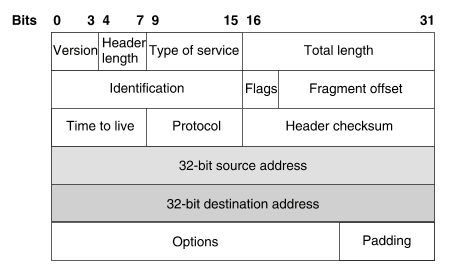
Mặt nạ mạng con bao giờ cũng đi kèm với địa chỉ mạng tiêu chuẩn để cho người đọc biết địa chỉ mạng tiêu chuẩn này dùng cả cho 254 máy chủ hay chia ra thành các mạng con. Mặt khác nó còn giúp bộ định tuyến trong việc định tuyến cuộc gọi.

***Nguyên tắc chung***

* Lấy bớt một số bit của phần địa chỉ máy chủ để tạo địa chỉ mạng con.
* Lấy đi bao nhiêu bit phụ thuộc vào số mạng con cần thiết mà nhà khai thác mạng quyết định sẽ tao ra.

***Một số địa chỉ đặc biệt:***

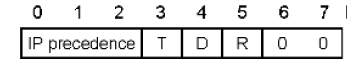
* Địa chỉ mạng IP là địa chỉ IP mà tất cả các bit thuộc phần định danh máy (host ID) = 0.
* Địa chỉ quảng bá tới tất cả các máy trong mạng LAN. VD: 255.255.255.255
* Địa chỉ tất cả các máy của mạng X.Y.Z ở xa. VD: X.Y.Z.255
* Địa chỉ Loopback có số 127 ở đầu 127.X.Y.Z Mục đích để thử tại chỗ các phần mềm IP.
* Địa chỉ 0.0.0.0 dùng để chỉ mạng này. Địa chỉ 0.0.0.5 dùng để chỉ máy số 5 ở mạng này (mạng đang cài đặt).
* Địa chỉ mạng sử dụng cho mạng riêng (mạng nội bộ, không sử dụng làm địa chỉ internet)
* Lớp A: 10.0.0.0
* Lớp B: 172.16.0.0 to 172.31.255.255
* Lớp C: 192.168.0.0 to 192.168.255.25
  1. Khuôn dạng gói tin IPv4



Khuôn dạng gói tin IPv4.

1. ***Version IPv4:*** Khi gói tin tới bộ định tuyến, bộ định tuyến sẽ phân tích nếu thấy phiên bản cũ hơn thì bộ định tuyến sẽ hủy bỏ gói tin và thông báo cho trạm nguồn biết.
2. ***Header length:*** độ dài của gói tin tính theo đơn vị 32 bit.
3. ***Type of service:***

Kiểu dịch vụ được sử dụng trong tiêu đề gói tin IP để chỉ ra quan hệ ưu tiên cho việc chuyển các gói tin, thông thường các gói tin IP được xử lý theo nguyên tắc FIFO, các bit 0, 1, 2 trong trường kiểu dịch vụ chỉ ra các thông tin về trễ, thông lượng và độ tin cậy. Thông thường 2 trong số 3 thông tin đó sẽ được đặt, nhưng trường chức năng này không buộc tất cả các bộ định tuyến phải xử lý.



Trường Type of service.

* Ý nghĩa các giá trị của IP precedence được cho bởi bảng sau:

Ý nghĩa các giá trị của IP precedence

|  |  |
| --- | --- |
| **Giá trị IP precedence** | **Ý nghĩa** |
| 7 (111) | Network Control |
| 6 (110) | Internetwork Control |
| 5 (101) | CRITI/ECP (critical / exceptional) |
| 4 (100) | Flash Override |
| 3 (011) | Flash |
| 2 (010) | Immediate |
| 1 (001) | Priority |
| 0 (000) | Routine |

* D ( Delay): độ trễ
  + D=0: yêu cầu truyền trễ bình thường.
  + D=1: yêu cầu trễ thấp.
* T ( Throughput): thông lượng
  + T=0: thông lượng bình thường.
  + T=1: thông lượng cao.
* R ( Reliability): độ tin cậy
  + R=0: độ tin cậy bình thường.
  + R=1: độ tin cậy cao.

1. ***Total length:*** độ dài toàn bộ của gói tin Max 216=64 KB, thông thường ngắn hơn.
2. ***ID:*** số định danh của gói tin. Nếu 1 gói tin phải phân thành nhiều mảnh để truyền đi thì tất cả các mảnh phải có cùng định danh.
3. ***Flags:*** là một trường gồm 3 bit thông tin

* Bit 0: Không dùng
* Bit 1: Cho biết gói có phân mảnh hay không.
* Bit 2: Nếu gói tin bị phân mảnh thì cho biết mảnh này có phải là mảnh cuối không.

1. ***Offset:*** Cho biết vị trí của mảnh tin trong gói tin, đơn vị tính là 8 byte. Tại trạm thu, 3 trường (5), (6), (7) cho phép ghép các mảnh tin thành gói tin.

VD: Một gói tin có dung lượng 4000 byte, gồm có 20 byte header + 3980 byte dữ liệu. Mà trên đường truyền chỉ cho phép truyền tối đa là 1500 byte thì sẽ phải phân gói tin thành 3 mảnh nhỏ. Mỗi mảnh đều có header là 20 byte, còn phần dữ liệu lần lượng của 3 mảnh lần lượt là 1480 byte , 1480 byte , 1020 byte. Giả sử ID gói tin là 5 ta có:

ID DF MF offset

5 0 1 0

5 0 1 1480

5 0 0 2960

1. ***Time to live (TTL):*** Chỉ ra số bước nhảy (hop) mà một gói có thể đi qua. Con số này sẽ giảm đi 1 khi gói tin đi qua một router. Khi router nào nhận gói tin thấy TTL đạt tới 0 gói này sẽ bị loại khỏi mạng. Đây là giải pháp nhằm ngăn chặn tình trạng lặp vòng vô hạn của gói tin trên mạng.
2. ***Protocol:*** Cho biết giao thức được sử dụng ở tầng trên.

* Nếu tầng giao vận là TCP thì có mã là 6.
* Nếu tầng giao vận là UDP thì có mã là 17.
* Nếu là ICMP thì có mã là 1.

1. ***Header checksum:*** Dùng để kiểm tra xem gói tin có bị lỗi không.
2. ***Source Address:*** Địa chỉ nguồn, nơi gói tin được gửi đi.
3. ***Destination Address:*** Địa chỉ đích, nơi gói tin được gửi tới.
4. ***Options:*** Các trường tùy chọn

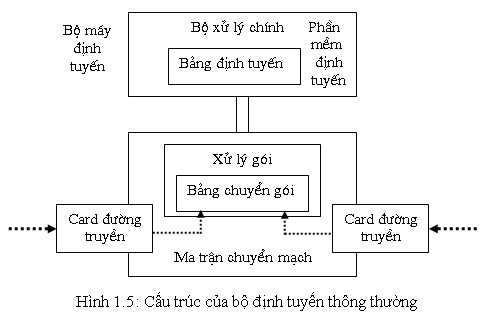
* Time stamp: Ghi lại thời gian mà gói tin đi qua bộ định tuyến. Có 3 cách ghi:
  + Khi gói tin đi qua bộ định tuyến, ghi lại danh sách thời gian gói tin đi qua.
  + Ghi địa chỉ IP và thời gian tương ứng khi gói tin đi qua.
  + Trạm nguồn sẽ ghi sẵn một số địa chỉ cần đo thời gian và gói tin tới bộ định tuyến có địa chỉ tương ứng thì sẽ được ghi thời gian vào.
* Security: Cho phép bộ định tuyến nhận gói dữ liệu không, nếu không thì gói sẽ bị hủy
* Record router: Lưu danh sách địa chỉ IP của router mà gói tin đi qua. Độ dài của trường lựa chọn này do trạm nguồn quy định. Nếu số bộ định tuyến mà gói tin đi qua quá nhiều thì địa chỉ của các bộ định tuyến sau sẽ không được ghi vào gói tin.
* Source route: Bắt buộc đi qua bộ định tuyến nào đó. Lúc này sẽ không cần dùng bảng định tuyến ở mỗi bộ định tuyến nữa.

1. Padding: Các số 0 sẽ được thêm vào trường này để đảm bảo phần header của gói tin sẽ luôn có độ dài là bội số của 32 bit.
   1. Giải pháp định tuyến theo địa chỉ IPv4
      1. Các phần tử cơ bản của một hệ thống định tuyến.

Bộ định tuyến là một thiết bị lớp 3 trong mô hình OSI 7 lớp. Nó có hai chức năng cơ bản đó là định tuyến và chuyển mạch gói tin IP từ đầu vào đến đầu ra. Quá trình định tuyến là quá trình tập hợp các thông tin về cấu trúc topo mạng nhằm tạo ra một bảng định tuyến. Quá trình chuyển mạch gói tin là sao chép một gói từ một giao diện đầu vào tới một giao diện đầu ra thích hợp dựa trên thông tin chứa trong bảng chuyển tiếp gói. Bất kỳ hệ thống định tuyến nào đều cần 4 phần tử cơ bản để thực hiện quá trình định tuyến và chuyển mạch gói tin đó là:

* Các phần mềm định tuyến.
* Bộ phận xử lý gói.
* Một ma trận chuyển mạch.
* Card đường truyền.

Bốn phần tử cơ bản này cấu thành một bộ định tuyến theo cấu trúc như sau:



Cấu trúc của một bộ định tuyến thông thường.

***Bộ xử lý chính*** thi hành phần mềm định tuyến, phần mềm định tuyến này thực hiện các chức năng định tuyến và duy trì các thông tin về cấu trúc mạng Internet thông qua các giao thức định tuyến.

***Ma trận chuyển mạch*** thực hiện hoạt động chuyển mạch gói tin bằng cách sử dụng bộ xử lý gói, bộ xử lý này thường là một ASIC (Application Specific Integrated Circuit - Mạch tích hợp đặc trưng cho ứng dụng) được tối ưu để thực hiện nhiệm vụ cụ thể với tốc độ cao. Ở điểm này thì nó phù hợp với bộ định tuyến trên đường trục hiện nay. Ngoài ra bộ định tuyến thường xuyên duy trì một bảng khác gọi là bảng chuyển gói, bảng này có trong các bộ máy chuyển tiếp gói (FE-Forwarding Engine). FE thực hiện việc đọc địa chỉ đích từ tiêu đề gói đến, thực hiện việc tìm kiếm tuyến, tìm tiền tố phù hợp dài nhất (Longest Prefix Matching) và chuyển gói đến giao diện đầu ra đã được xác định. Về cơ bản thì bảng chuyển gói bắt nguồn từ bảng định tuyến nhưng nó ít được cập nhật hơn. Bảng định tuyến được duy trì bởi phần mềm định tuyến, phần mềm này thực hiện quá trình xử lý tương đối chậm trong khi cập nhật bảng và khi bảng đã được cập nhật, bản sao của nó sẽ được chuyển đến bộ máy chuyển gói. Bản sao này có thể là một tập hợp con của toàn bộ bảng định tuyến và có thể được biến đổi để phù hợp với phiên bản nhỏ hơn. Ma trận chuyển mạch là thành phần cốt yếu của một bộ máy chuyển gói. Về bản chất, một bộ định tuyến bao gồm phương tiện định tuyến được thực hiện trong phần mềm và sử dụng CPU chính của bộ định tuyến để tiến hành hoạt động phức tạp hơn như thực hiện các giao thức định tuyến, các đặc điểm kĩ thuật lưu lượng, đảm bảo QoS, biến đổi tiêu đề gói trước khi truyền đi và các đặc điểm dựa trên các phần mềm khác của bộ định tuyến. Ngoài ra, FE còn tiến hành các nhiệm vụ đơn giản hơn tại tốc độ cao.

* + 1. Xử lý gói tin ở bộ định tuyến.

Các gói tin ở bộ định tuyến căn cứ vào bộ đệm của bộ định tuyến và các thông số ở phần tiêu đề của gói IP để đưa ra các quyết định phù hợp với gói tin.

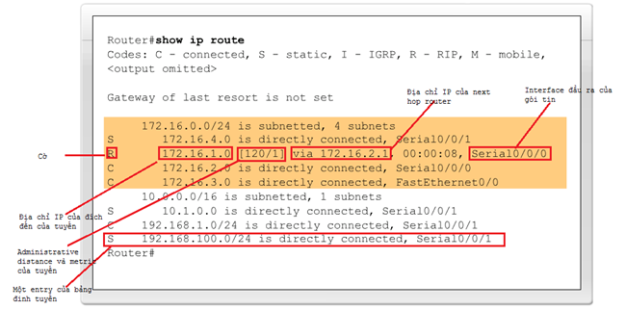
* Kiểm tra gói tin IP
  + Header checksum nếu có lỗi thì bộ định tuyến hủy gói tin.
  + Kiểm tra 1 số thông số: Version, Header length, Total length, Protocol nếu sai hủy bỏ gói tin.
  + Kiểm tra xem nếu TTL=0 thì hủy gói tin.
  + Nếu bộ đệm của bộ định tuyến đầy không chứa được gói tin thì hủy gói tin.
* Chuẩn bị truyền :
  + Phân tích trường (Type of service) để tìm ra đường đi tương ứng.
  + Xác định gói tin có phân mảnh không?
    - Nếu phân mảnh thì thực hiện chia gói tin.
    - Nếu không được phân mảnh nhưng bộ định tuyến lại không có khả năng truyền cả gói tin thì sẽ hỏi các bộ định tuyến láng giềng và nhờ bộ định tuyến láng giềng chuyển gói tin. Nếu không có bộ định tuyến láng giềng nào chuyển được gói tin thì bộ định tuyến sẽ hủy gói tin và thông báo cho trạm nguồn.
* Tính toán lại một số thống số của gói tin:
  + TTL - 1 (khi qua một bộ định tuyến).
  + Điền các thông số cho trường hợp phân mảnh.
  + Điền các trường tùy chọn (Options).
  + Tính lại Header checksum.
    1. Xử lý gói tin khi tới đích.
* Kiểm tra gói tin IP.
  + Header checksum: Nếu có lỗi thì máy đích hủy gói tin.
  + Kiểm tra một số thông số: Version, Header length, Total length, Protocol. Nếu sai hủy bỏ gói tin.
  + Kiểm tra xem nếu TTL=0 thì hủy gói tin.
  + Nếu bộ đệm của bộ định tuyến đầy không chứa được gói tin thì hủy gói tin.
* Chuẩn bị
  + Không kiểm tra Type of service vì đây là trạm đích nên không cần chuyển đến trạm khác.
  + Kiểm tra xem gói tin có phân mảnh không: Khi nhận được mảnh tin đầu tiên của gói tin phân mảnh, trạm đích sẽ khởi động một đồng hồ thời gian, nếu hết thời gian quy định mà mảnh tin cuối cùng chưa đến thì trạm đích sẽ hủy bỏ tất cả các mảnh tin đã nhận. Nếu các mảnh tin đến đúng giờ thì trạm đích sẽ ghép các mảnh tin thành gói tin gốc.
* Chuyển gói tin lên tầng trên để xử lý tiếp.
  + 1. Định tuyến trên mạng Internet
       1. Bảng định tuyến

Bảng định tuyến là một phần rất quan trọng trong mạng IP nói chung, và nó liên quan đến một vấn đề then chốt trong mọi công nghệ truyền thông – chuyển mạch (switching) và định tuyến (routing).

Trong mạng IP sử dụng chuyển mạch gói, khi số lượng người dùng và số node mạng trung chuyển là rất lớn, yêu cầu đặt ra là các node mạng phải thông minh hơn, tự động tìm được tuyến đường tốt nhất để đi đến đích (best route). Vì vậy, người ta đã sinh ra các giao thức định tuyến (Routing Protocol) để tìm được best route. Và các best route này sẽ được lưu lại trong một database để khi có gói tin đến, router sẽ tra database và tìm ra được đường đi cho gói tin. Database này chính là bảng định tuyến (Routing Table).

Một bảng định tuyến gồm nhiều bản ghi, mỗi bản ghi chứa thông tin về các tuyến đường đến các đích khác nhau. Cấu trúc của một bản ghi bao gồm:

* Địa chỉ IP đích (destination IP): Địa chỉ này có thể là địa chỉ của một host cụ thể, hoặc là một địa chỉ của một mạng. Nếu là địa chỉ host, bản ghi này sẽ có host-ID khác 0 để nhận diện một host. Nếu là địa chỉ mạng, phần host-ID = 0.
* Địa chỉ IP của next-hop router (next-hop IP), hoặc địa chỉ của một mạng kết nối trực tiếp (directly connected IP address): Là địa chỉ của đích đến tiếp theo (router) có thể chuyển tiếp gói tin đến đích.
* Network interface: Là cổng của router được sử dụng để gửi gói tin đến next-hop.
* Cờ (flags): Cho biết nguồn cập nhật của tuyến (route). Ví dụ: S – Static Route, C – Connected Route, O – OSPF Route…
* Metric: Là thông tin về metric của một tuyến đường, thể hiện “khoảng cách” từ router hiện tại đến destination IP. Giá trị này chỉ có ý nghĩa so sánh khi các route sử dụng cùng một giao thức định tuyến.
* Administrative Distance (AD): Tham số ưu tiên mà người quản trị đặt cho các tuyến trong bảng định tuyến, được gán cho các giao thức. Nếu tuyến được cập nhật từ giao thức, nó sẽ mang giá trị AD của giao thức đó. Giá trị này nằm trong khoảng từ 0 đến 255, càng bé càng ưu tiên. 255 có nghĩa là tuyến không bao giờ được sử dụng.



Một bản ghi trong bảng định tuyến.

* + - 1. Giao thức định tuyến

Chức năng của giao thức định tuyến

* Thiết lập bảng tìm đường.
* Cập nhật bảng tìm đường.
* Tính toán quãng đường đi ngắn nhất để chọn địa chỉ của bộ định tuyến tiếp theo nhằm chuyển gói tin đi nhanh nhất.

Giao thức định tuyến đơn giản là giao thức dựa vào topo mạng để lập bảng tìm đường bằng tay và cập nhật bằng tay nhằm tìm đường ngắn nhất. Giao thức này chỉ sử dụng cho mạng đơn giản.

Giao thức định tuyến trên Internet, sử dụng trong mạng phức tạp.

* Cập nhật tự động.
* Tự động tính toán để tìm ra bộ định tuyến tiếp theo dựa trên hiện trạng của mạng.

Tiêu chuẩn đánh giá giao thức định tuyến:

* Thích nghi rất nhanh với thay đổi của mạng.
* Tính được con đường tối ưu.
* Dễ dàng nâng cấp khi mạng phát triển.
* Tiết kiệm tài nguyên của máy.
* Băng thông tiết kiệm nhất.
  + - 1. Số đo được sử dụng trên trong mạng Internet

Số đo được tính như sau:

* Số bước nhảy mà gói tin đi qua.
* Số bước nhảy mà gói tin đi qua nhưng có trọng số.
* Tổng hợp từ nhiều thông số như băng thông, độ trễ, tải hiện tại, giá thành....

Thuật toán dựa trên số đo để tính đường đi ngắn nhất gọi là DVA (Distance Vector Algorithm). Giao thức RIP sử dụng thuật toán DVA.

Thuật toán trạng thái liên kết gọi là LSA (Link State Algorithm). Giao thức OSPF sử dụng thuật toán LSA.

* 1. Những hạn chế của IPv4
     1. Sự giới hạn về kích thước địa chỉ

Do IPv4 chỉ dùng 32 bit để đánh địa chỉ nên không gian địa chỉ IPv4 chỉ có 232 địa chỉ. Với sự phát triển mạnh mẽ của Internet hiện nay, tài nguyên địa chỉ IPv4 đã gần cạn kiệt. Như vậy IPv4 ngày nay hầu như không còn đáp ứng được nhu cầu sử dụng của mạng Internet. Hai vấn đề lớn mà IPv4 đang phải đối mặt là việc thiếu hụt các địa chỉ, đặc biệt là các không gian địa chỉ tầm trung (lớp B) và việc phát triển về kích thước rất nguy hiểm của các bảng định tuyến trong Internet.

Để giải quyết vấn đề thiếu hụt địa chỉ IP, người ta đã sử dụng rất nhiều phương pháp như: Subneting, VLSM, CIDR, NAT. Thêm vào đó, nhu cầu tự động cấu hình (Auto-config) ngày càng trở nên cần thiết. Địa chỉ IPv4 trong thời kỳ đầu được phân loại dựa vào dung lượng của địa chỉ đó (số lượng địa chỉ IPv4). Địa chỉ IPv4 được chia thành 5 lớp A, B, C, D, E. 3 lớp đầu tiên được sử dụng phổ biến nhất. Các lớp địa chỉ này khác nhau ở số lượng các bit dùng để định nghĩa Network ID.

* + 1. Cấu trúc định tuyến không hiệu quả

Địa chỉ IPv4 có cấu trúc định tuyến vừa phân cấp, vừa không phân cấp. Mỗi router phải duy trì bảng thông tin định tuyến lớn, đòi hỏi router phải có dung lượng bộ nhớ lớn. IPv4 cũng yêu cầu router phải can thiệp xử lý nhiều đối với gói tin IPv4.

* + 1. Hạn chế về tính bảo mật và kết nối đầu cuối – đầu cuối

Trong cấu trúc thiết kế của địa chỉ IPv4 không có cách thức bảo mật nào đi kèm. IPv4 không cung cấp phương tiện hỗ trợ mã hóa dữ liệu. Kết quả là hiện nay, bảo mật ở mức ứng dụng được sử dụng phổ biến, không bảo mật lưu lượng truyền tải giữa các host. Nếu áp dụng IPSec là một phương thức bảo mật phổ biến tại tầng IP, mô hình bảo mật chủ yếu là bảo mật lưu lượng giữa các mạng, việc bảo mật lưu lượng đầu cuối – đầu cuối được sử dụng rất hạn chế.

Nguy cơ thiếu hụt không gian địa chỉ, cùng những hạn chế của IPv4 thúc đẩy sự đầu tư nghiên cứu một giao thức internet mới, khắc phục những hạn chế của giao thức IPv4 và đem lại những đặc tính mới cần thiết cho dịch vụ và cho hoạt động mạng thế hệ tiếp theo. Tổ chức Internet IETF đã đưa ra quyết định thúc đẩy thay thế cho IPv4 là IPv6 (Internet Protocol version 6), giao thức Internet phiên bản 6, còn được gọi là giao thức IP thế hệ mới (IP Next Generation – IPng). Địa chỉ Internet phiên bản 6 có chiều dài gấp 4 lần chiều dài địa chỉ IPv4, bao gồm 128 bit.

* 1. Kết luận.

Trong chương này, bài tiểu luận đã trình bày phần tìm hiểu về IPv4. Địa chỉ IPv4 có hai chức năng cơ bản: địa chỉ các giao diện mạng (cung cấp một địa chỉ duy nhất cho những giao diện khi tham gia vào mạng Internet), hỗ trợ cho định tuyến (để truyền tải thông tin từ mạng này sang mạng khác). Chương tiếp theo sẽ trình bày về địa chỉ Internet phiên bản 6 - IPv6, đây là phiên bản được thiết kế nhằm khắc phục những hạn chế của giao thức Internet IPv4.

1. Tìm hiểu IPv6
   1. Đặc điểm của IPv6

Giao thức Internet phiên bản 4 (IPv4) tuy đang được sử dụng rỗng rãi hiện nay nhưng có một số nhược điểm:

+ Địa chỉ Ip có 32 bit, cho tới nay đã gần cạn kiệt, cần phải được mở rộng.

+ Phần đầu (phần tiêu đề) của khuôn dạng gói tin IPv4 có những thông tin dư thừa.

+ An ninh thông tin chưa thật đảm bảo, còn thiếu.

+ Chưa hỗ trợ tốt cho việc truyền thông đa phương tiện (multimedia).

Sự ra đời của IPv6 sẽ khắc phục những nhược điểm trên.

* + 1. Kiểu định dạng tiêu đề mới

Tiêu đề của IPv6 có một kiểu định dạng mới được thiết kế để giữ cho tiêu đề bên trên ở mức tối thiểu. Điều này đạt được bằng cách chuyển cả các trường hợp không cần thiết và các trường lựa chọn sang phần tiêu đề mở rộng, phần mở rộng này đi theo sau phần tiêu đề của IPv6. Tiêu đề IPv6 được tổ chức tốt, xử lý hiệu quả hơn tại các bộ định tuyến trung gian.

Các tiêu đề IPv4 và IPv6 là không gắn liền. IPv6 không phải là siêu tập của chức năng mà tương thích ngược với IPv4. Một host hoặc một bộ định tuyến phải dùng một sự bổ sung của IPv4 và IPv6 để nhận ra và xử lý cả 2 kiểu định dạng tiêu đề. Tiêu đề IPv6 mới chỉ rộng gấp 2 lần IPv4 mặc dù địa chỉ IPv6 rộng gấp 4 lần IPv4.

* + 1. Không gian địa chỉ mở rộng

IPv6 có địa chỉ IP dài 128 bit. Mặc dù 128 bit có thể biểu diễn hơn 3.4x1038 tổ hợp, không gian địa chỉ rộng của IPv6 được thiết kế cho phép nhiều mức subneting và chia vùng điạ chỉ từ địa chỉ gốc Internet đến các mạng riêng trong cùng một tổ chức.

Mặc dù chỉ một số lượng nhỏ địa chỉ hiện tại được chia phần cho host, vẫn còn nhiều địa chỉ cho tương lai. Với một số lượng địa chỉ lớn như vậy thì các kỹ thuật để tiết kiệm địa chỉ như NAT là không cần thiết nữa.

* + 1. Cơ sở hạn tầng định tuyến và đánh địa chỉ phân cấp và hiệu quả

Các địa chỉ IPv6 toàn cầu được dùng trong phần IPv6 của Internet được thiết kế để tạo một cơ sở hạ tầng định tuyến có thể tóm tắt, phân cấp và hiệu quả. Cơ sở hạ tầng này được dựa trên sự triển khai chung nhiều cấp độ của các nhà cung cấp dịch vụ ISP.

* + 1. Cấu hình địa chỉ Stateful và Stateless

Để đơn giản hóa cấu hình host, IPv6 hỗ trợ cả hai kiểu cấu hình là stateful, như là cấu hình địa chỉ trong sự có mặt của một DHCP server và stateless (cấu hình địa chỉ trong không có mặt của một DHCP). Với kiểu cấu hình địa chỉ stateless thì các host trên một liên kết sẽ tự động cấu hình với địa chỉ IPv6 cho liên kết (đươc gọi là địa chỉ liên kết nội bộ) và với các địa chỉ được phân phát từ Prefixes quảng cáo bởi các bộ định tuyến nội bộ. Ngay cả khi không có các bộ định tuyến thì các host trên cùng một liên kết vẫn có thể tự động cấu hình với các đại chỉ liên kết nội bộ và liên lạc với nhau mà không cần cấu hình nhân công.

* + 1. Bảo mật

Trong hoạt động Internet, bảo mật tại tầng IP được thực hiện phổ biến bằng công nghệ IPSec. IPSec thực hiện chức năng xác định nơi gửi và mã hóa đường kết nối, do vậy đảm bảo có kết nối bảo mật. Công nghệ IPSec hỗ trợ cả địa chỉ IPv4 và IPv6. Tuy nhiên trong IPv6, IPSec được định nghĩa như là một đặc tính bắt buộc của địa chỉ IPv6 khi các thủ tục bảo mật của IPSec được đưa vào thành hai đặc tính là hai tiêu đề mở rộng của địa chỉ IPv6. Đó là tiêu đề Xác thực, và tiêu đề Mã hóa.

* + 1. Hỗ trợ tốt hơn cho QoS

Các trường mới trong tiêu đề của IPv6 định nghĩa cách thức mà lưu lượng quản lý và nhận dạng. Sự nhận dạng lưu lượng dùng một trường nhãn lưu lượng trong tiêu đề IPv6 cho phép các bộ định tuyến nhận dạng và cung cấp việc quản lý đặc biệt cho các gói thuộc cùng một luồng, một seri các gói giữa nguồn và đích. Bởi vì lưu lượng được nhận dạng trong tiêu đề IPv6, việc hỗ trợ QoS có thể đạt được ngay cả khi trọng tải của gói được mã hóa thông qua IPSec.

* + 1. Giao thức mới cho sự tương tác Node láng giềng

Giao thức tìm kiếm láng giềng cho IPv6 là một seri của ICMP cho các bản tin của IPv6, chúng quản lý việc tương tác giữa các node làng giềng. Tìm kiếm láng giềng thay thế cho các bản tin giao thức ARP dựa vào việc broadcast, các bản tin ICMPv4 bộ định tuyến tìm kiếm và multicast hiệu quả.

* + 1. Có khả năng mở rộng

IPv6 có thể dễ dàng được mở rộng cho các tính năng mới bằng cách thêm vào các tiêu đề mở rộng vào sau tiêu đề của IPv6. Không giống như các lựa chọn của tiêu đề IPv4 chỉ có thể hỗ trợ 40 byte option, kích thước của tiêu đề mở rộng của IPv6 khống chế bởi kích thước của gói IPv6.

* 1. Sự khác biệt giữa IPv4 và IPv6

|  |  |
| --- | --- |
| IPv4 | IPv6 |
| Dùng địa chỉ 32 bit | Dùng địa chỉ 128 bit |
| IPSec là tùy chọn | IPSec là bắt buộc |
| Không có xác nhận luồng gói cho việc quản lý QoS bởi các bộ định tuyến trong phần tiêu đề | Việc xác nhận luồng gói cho quản lý QoS bởi các bộ định tuyến được dùng trong trường nhãn luồng. |
| Phân mảnh được thực hiện bởi host và bộ định tuyến | Phân mảnh chỉ thực hiện bởi host gửi |
| Tiêu đề bao gồm cả phần checksum | Tiêu đề không bao gồm phần checksum |
| Tiêu đề có phần tùy chọn | Tất cả dữ liệu tùy chọn được chuyển sang phần tiêu đề mở rộng. |
| ARP dùng broadcast ARP Request frames để chuyển một địa chỉ IPv4 sang địa chỉ MAC | ARP Request frames thay thế bằng các bản tin Neighbor Solicitation multicast |
| IGMP được dùng để quản lý các local subnet group membership. | IGMP được thay thế bởi các bản tin Multicast Listener Discovery (MLD). |
| ICMP bộ định tuyến tìm kiếm được dùng để xác định đia chỉ IPv4 default gateway tốt nhất và đây là một tùy chọn | ICMP bộ định tuyến tìm kiếm được thay bằng các bản tin ICMPv6 bộ định tuyến Solicitation và bộ định tuyến quảng cáo và đây là 1 yêu cầu. |
| Phải được cấu hình nhân công hoặc thông qua DHCP | Không yêu cầu cấu hình nhân công hoặc thông qua DHCP |
| Dùng các bảng ghi tài nguyên trong miền DNS để ánh xạ địa chỉ IPv4 sang tên host | Dùng các bảng ghi tài nguyên con trỏ trong miền DNS để ánh xạ địa chỉ IPv6 sang tên host |
| Phải hỗ trợ một kích thước gói là 576 byte ( có thể được phân mảnh) | Phải hỗ trợ một kích thước gói là 128 byte ( không phân mảnh) |
| Dùng các bảng ghi tài nguyên địa chỉ host trong DNS để ánh xạ tên host sang IPv4 | Dùng các bảng ghi tài nguyên địa chỉ host trong DNS để ánh xạ tên host sang IPv6 |
| Địa chỉ broadcast được dùng để gửi thông tin tới tất cả các node trên cùng một subnet | Không có địa chỉ broadcast. Thay vào đó là địa chỉ link-local scope all-node multicast |

Sự khác biệt giữa IPv4 và IPv6.

* 1. Đánh địa chỉ Ipv6
     1. Không gian địa chỉ IPv6

Kích thước địa chỉ IPv6 là 128 bit, rộng gấp 4 lần địa chỉ của IPv4. Không gian địa chỉ 32 bit cho phép 232 hay 4.294.967.296 địa chỉ. Không gian địa chỉ 128 bit cho phép 2128 địa chỉ hay 340.282.366.920.938.463.463.374.607.431.768.211.456 (3.4x1038) địa chỉ.

Vào những năm cuối thập niên 70 của thế kỷ trước khi mà không gian địa chỉ IPv4 được thiết kế thì người ta chưa tưởng tượng được rằng nó sẽ cạn kiệt trong tương lai. Tuy nhiên do có nhiều sự thay đổi trong kỹ thuật và thực tế phân vùng không thấy trước được sự bùng nổ của các host trên Internet và không gian địa chỉ IPv4 đã được phân phát hết vào năm 1992, do đó cần 1 không gian địa chỉ mới thay thế.

Với IPv6 thật khó có thể tưởng tượng được rằng nó sẽ được phân phát hết bởi vì theo ước tính không gian địa chỉ IPv6 sẽ cung cấp cho mỗi m2 bề mặt trái đất là 655.570.793.348.866.943.898.599 (6.5x1023) địa chỉ. Kích thước tương đối lớn của địa chỉ IPv6 được thiết kế để chia nhỏ thành các miền định tuyến phân cấp phản ánh topo của Internet hiện nay. Việc sử dụng 128 bit cho phép nhiều mức độ phân cấp và tính linh động trong việc thiết kế định tuyến và đánh địa chỉ phân cấp.

* + 1. Cú pháp địa chỉ IPv6

Địa chỉ IPv6 128 bit được chia thành 8 khối mỗi khối 16 bit, mỗi khối này được chuyển sang dạng số hexa 4 bit và được phân biệt với nhau bằng dấu hai chấm.

Ví dụ: cho 1 địa chỉ IPv6 dưới dạng nhị phân như sau:

00100001110110100000000011010011000000000000000000101111001110110000001010101010000000001111111111111110001010001001110001011010

Địa chỉ này được chia ra thành các khối 16bit như sau:

0010000111011010 0000000011010011 0000000000000000 0010111100111011 0000001010101010 0000000011111111 1111111000101000 1001110001011010. Mỗi khối này được chuyển sang chữ số hexa và chia cách nhau bằng dấu hai chấm, kết quả là: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Việc viết địa chỉ IPv6 có thể đơn giản hóa bằng cách xóa bỏ 0 đứng đầu trong mỗi khối 16 bit. Tuy nhiên mỗi khối phải có ít nhất một số đơn. Trong ví dụ trên, địa chỉ trên được đơn giản hóa thành: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.

*Nén các chữ số 0*

- Một số loại địa chỉ chứa các chuỗi dài các số 0. để đơn giản hóa trong cách viết, một chuỗi liên tiếp các khối 16 bit có giá trị 0 trong kiểu định dạng theo số hexa phân cách nhau bằng dấu : được nén thành “::” và được gọi là dấu hai chấm kép.

Ví dụ: địa chỉ link-local FE80:0:0:0:2AA:FF:FE9A:4CA2 được nén thành FE80::2AA:FF:FE9A:4CA2, và địa chỉ multicast FF02:0:0:0:0:0:0:2 nén thành FF02::2.

Việc nén 0 chỉ có thể được dùng để nén một chuỗi các khối 16 bit liên tiếp đơn mà thôi. Ta không thể nén 0 với các số 0 là một phần của khối 16 bit. Ví dụ như ta không thể nén địa chỉ FF02:30:0:0:0:0:0:5 thành FF02:3::5, mà ta chỉ có thể nén thành FF02:30::5.

Để xác định có bao nhiêu con số 0 đứng giữa “::” thì ta có công thức sau:

N = (8-n)\*16

trong đó n là số khối bit 16 bit địa chỉ còn lại được biểu diễn ở dạng số hexa.

Việc nén 0 chỉ được dùng 1 lần đối với 1 địa chỉ cho trước, nếu không thì ta sẽ không thể xác định được con số không được giản lược.

* + 1. Prefix của IPv6

Prefix là một phần của địa chỉ IPv6, nó chỉ ra các bit có giá trị cố định hoặc là các bit đóng vai trò là ID của mạng. Các prefix cho định danh mạng con của IPv6, các tuyến, các vùng địa chỉ được biểu diễn như trong ký hiệu CIDR (classless Inter-Domain Routing) cho IPv4. Ví dụ 21DA::/48 cho một địa chỉ Prefix tuyến và 21DA:D3:0:2F3B::/64 cho 1 prefix mạng con. Trong đó IPv6 chỉ dùng prefix chứ không dùng mặt nạ mạng con như IPv4.

* + 1. Các dạng địa chỉ IPv6

• ***Địa chỉ unicast***

Một địa chỉ unicast xác định một giao diện đơn trong phạm vi của loại địa chỉ unicast. Với một topology định tuyến unicast thích hợp, các gói được đánh địa chỉ unicast được chuyển đến một giao diện đơn.

• ***Địa chỉ multicast***

Một địa chỉ multicast xác định nhiều giao diện. Với topo định tuyến thích hợp thì các gói được đánh địa chỉ multicast sẽ được chuyển tới tất cả các giao diện mà được xác định bởi địa chỉ này. Một địa chỉ multicast được dùng trong truyền thông một-nhiều, được chuyển đến nhiều giao diện.

• ***Địa chỉ anycast***

Một địa chỉ Anycast xác định nhiều giao diện. Với topology định tuyến thích hợp thì các gói được đánh địa chỉ anycast được chuyển đến một giao diện đơn gần nhât được xác định bởi địa chỉ anycast này. Khái niệm giao diện gần nhất được xác định gần nhất trong giới hạn khoảng cách định tuyến. Địa chỉ anycast được dùng trong truyền thông 1-1 trong nhiều.

* + - 1. Địa chỉ unicast IPv6

Địa chỉ unicast IPv6 bao gồm các loại sau: địa chỉ unicast toàn cầu, địa chỉ link-local, địa chỉ site-local và địa chỉ đặc biệt.

• Địa chỉ Unicast toàn cầu

Địa chỉ Unicast toàn cầu tương ứng với địa chỉ public của IPv4. Nó có thể định tuyến toàn cầu trong Internet. Không giống như Internet dựa trên IPv4 có sự định tuyến trên cả dạng phẳng và phần phân cấp Internet IPv6 được thiết kế từ nền móng của nó là hỗ trợ cho việc định tuyến và đánh địa chỉ phân cấp và hiệu quả.

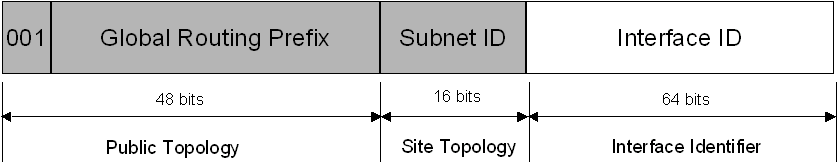
Các trường của địa chỉ Unicast toàn cầu được mô tả như sau:

- Phần cố định được gán cho giá trị là 001.

- Prefix định tuyến toàn cầu: chỉ prefix định tuyến toàn cầu cho một site của một tổ chức cụ thể. Ba bit cố định cùng với 45 bit prefix định tuyến toàn cầu tạo thành một prefic site 48 bit, prefix này được cấp cho một site cá nhận của một tổ chức. Một khi đã được cấp các bộ định tuyến trên Internet IPv6 sẽ chuyển lưu lượng IPv6 phù hợp với prefix 48 bit đến các bộ định tuyến thuộc site của tổ chức.

- Subnet ID: Subnet ID được dùng cho site của tổ chức để xác định các mạng con. Kích thước của trường này là 16 bit. Site của tổ chức có thể dùng 16 bit này với site của nó để tạo 65.536 mạng con hoặc nhiều mức độ của sự phân cấp đánh địa chỉ và một cơ sở hạ tầng định tuyến hiệu quả.

- Giao diện ID: chỉ giao diện trên một subnet cụ thể của một site. Kích thước của trường này là 16 bit. Các trường với địa chỉ unicast toàn cầu tạo ra cấu trúc 3 cấp như hình vẽ:



Địa chỉ Unicast toàn cầu.

Topology công cộng là tập hợp của các ISP lớn hơn và nhỏ hơn mà cung cấp truy nhập vào Internet IPv6. Topo của site là tập hợp của các mạng con trong cùng site của tổ chức. Chỉ thị giao diện chỉ một giao diện cụ thể trên một mạng con trong cùng site của một tổ chức.

• Địa chỉ Unicast dùng nội bộ.

Có 2 loại: địa chỉ link-local và địa chỉ site-local

\* Địa chỉ Link-Local.

Các địa chỉ link-local được dùng bởi các node khi truyền thông với các node láng giềng trên cùng 1 liên kết. Ví dụ như trên mạng IPv6 liên kết đơn không có bộ định tuyến, các địa chỉ link-local được dùng để truyền thông giữa các host trên link.

Một địa chỉ link-local cần thiết cho các quá trình xử lý tìm kiếm láng giềng và luôn luôn được tự động được cấu hình ngay cả khi không có tất cả các địa chỉ unicast khác.

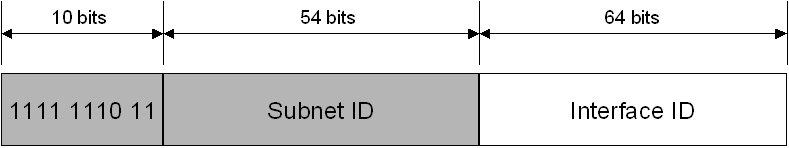


Mô tả cấu trúc của địa chỉ link-local.

Các địa chỉ link-local luôn luôn bắt đầu với FE80. Với 64 bit xác định giao diện. Prefix cho địa chỉ link-local luôn luôn là FE80::/64. Một bộ định tuyến IPv6 chuyển lưu lượng link-local vượt ngoài giới hạn liên kết.

\* Địa chỉ Site khu vực (Site-Local).

Các địa chỉ site-local tương ứng với không gian địa chỉ IPv4 riêng (10.0.0.0, 172.16.0.0/24 và 192.168.0.0/16). Ví dụ các mạng nội bộ riêng mà không có một hướng, định tuyến kết nối đến Internet IPv6 có thể dùng các địa chỉ site-local mà không xung đột với các địa chỉ Unicast toàn cầu. Các địa chỉ site-local không đến được từ các site khác và các bộ định tuyến phải không được chuyển lưu lượng site-local ra ngoài site. Các địa chỉ site-local có thể được dùng thêm vào các địa chỉ unicast toàn cầu. Một site là một mạng tổ chức hoặc 1 phần của mạng tổ chức mà được định nghĩa về mặt địa lý, như 1 cơ quan hay 1 tổ hợp cơ quan, một trường học. Không giống như các địa chỉ link-local, các địa chỉ site-local không được tự động cấu hình và được cấp phát bởi các quá trình cấu hình địa chỉ stateful hay stateless. Cấu trúc của địa chỉ site-locak như sau:



Mô tả cấu trúc của địa chỉ Site-Local.

10 bit đầu tiên luôn luôn cố định cho các địa chỉ site-local ( FEC0::/10). Sau 10 bit cố định là trường ID Subnet cung cấp 54 bit mà ta có thể tạo ra một cơ sở hạ tầng định tuyến có thể tóm tắt và phân cấp trong cùng 1 site. Sau trường ID mạng con là 64 bit trường ID giao diện mà chỉ thị một giao diện cụ thể trên một subnet.

• Địa chỉ IPv6 đặc biệt.

\* Địa chỉ không chỉ rõ.

Địa chỉ 0:0:0:0:0:0:0:0 hay :: chỉ được dùng để chỉ sự không có mặt của một địa chỉ. Nó tương thích với địa chỉ không rõ trong IPv4 là 0.0.0.0. Địa chỉ không chỉ rõ thường được dùng như là một địa chỉ nguồn cho các gói cố gắng để xác nhận sự có mặt duy nhất của một địa chỉ không chỉ rõ. Địa chỉ không chỉ rõ không được cấp cho 1 giao diện hoặc là dùng như 1 địa chỉ đích đến.

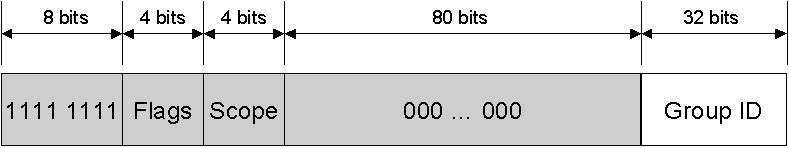
\* Địa chỉ loopback.

Địa chỉ loopback 0:0:0:0:0:0:0:1 hoặc ::1 được dùng để xác định 1 giao diện loopback cho phép 1 node có thể gửi các gói gửi ngược về chính nó. Nó tương đương với địa chỉ loopback 127.0.0.1 trong IPv4. Các gói được đánh địa chỉ cho địa chỉ loopback phải không được gửi trên đường liên kết hoặc được chuyển tiếp bởi 1 bộ định tuyến IPv6.

* + - 1. Địa chỉ Multicast IPv6

Trong IPv6 lưu lượng multicast hoạt động giống như ở IPv4. Các node IPv6 được định vị tùy ý có thể lắng nghe lưu lượng multicast trên 1 địa chỉ multicast tùy ý. Các node IPv6 được định vị tùy ý có thể lắng nghe nhiều địa chỉ multicast tại cùng 1 thời điểm. Các node có thể tham gia hoặc rời khỏi nhóm multicast bất cứ lúc nào.

Địa chỉ multicast IPv6 có 8 bit đầu tiên là 1111 1111. Một địa chỉ IPv6 multicast có thể dễ dàng nhận ra vì nó luôn bắt đầu bằng FF. Các địa chỉ multicast không thể được dùng như là các địa chỉ nguồn hoặc là các đích trung gian trong 1 tiêu đề định tuyến. Phía sau 8 bit đầu tiên địa chỉ multicast bao gồm cấu trúc thêm vào để xác định các cờ, phạm vi và nhóm multicast.



Mô tả cấu trúc của địa chỉ Multicast.

Các trường trong địa chỉ multicast là:

- Cờ: chỉ các cờ được thiết lập trong địa chỉ multicast. Kích thước của trường này là 4 bit. Như RFC 3513 cờ chỉ được định nghĩa là cờ T (transient: tạm thời). Cờ T dùng bit bậc thấp của trường cờ. Khi được set về 0 cờ T chỉ ra rằng địa chỉ multicast là một địa chỉ multicast được cấp thường trực, được cấp phát bởi IANA

(Internet Assigned Number Authority). Khi được set lên 1, cờ T chỉ ra địa chỉ multicast này là địa chỉ multicast tạm thời.

- Phạm vi: chỉ phạm vi của liên mạng IPv6 cho lưu lượng multicast được dự định. Kích thước của trường này là 4 bit. Thêm vào đó thông tin cung cấp bởi các giao thức định tuyến multicast , các bộ định tuyến dùng phạm vi multicast để xác định nơi mà lưu lượng multicast sẽ được chuyển đi. Các giá trị thông thường nhất cho trường phạm vi là 1 (phạm vi giao diện cục bộ), 2 (phạm vi liên kết nội bộ) và 5 (phạm vi site nội bộ). Ví dụ lưu lượng với địa chỉ multicast là FF02::2 có 1 phạm vi liên kết nội bộ thì 1 bộ định tuyến IPv6 sẽ không chuyển lưu lượng này ra liên kết nội bộ.

- ID nhóm: chỉ nhóm multicast và là duy nhất đối với mỗi phạm vi. Kích thước của trường này là 112 bit. Các ID nhóm được gán thường trực không phụ thuộc vào phạm vi. Các ID nhóm tạm thời chỉ liên quan đến 1 phạm vi cụ thể. Các địa chỉ từ FF01:: đến FF0F:: là các địa chỉ để lưu trữ và được biết đến nhiều. Để xác định tất cả các node cho các phạm vi liên kết nội bộ và giao diện nội bộ, các địa chỉ sau được định nghĩa:

FF01::1 (giao diện-local scope all-nodes multicast address)

FF02::1 (link-local scope all-node multicast address

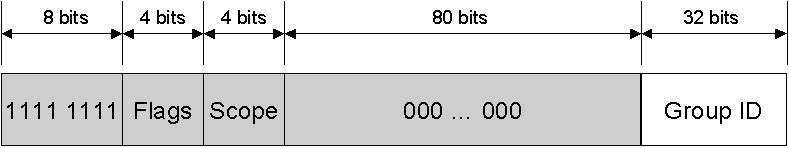
Để xác định tất cả các bộ định tuyến cho phạm vi giao diện nội bộ và site nội bộ, các địa chỉ sau được định nghĩa:

FF01::2 (giao diện-local scope all-bộ định tuyếns multicast address)

FF02::2 (link-local scope all-bộ định tuyếns multicast address)

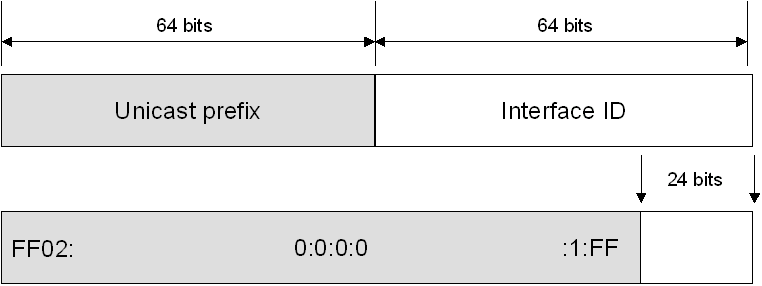
FF05::2 (site-local scope all-bộ định tuyếns multicast address)

Với 112 bit cho ID nhóm thì có thể có 2112 ID nhóm địa chỉ. Tuy nhiên theo cách mà các điạ chỉ multicast IPv6 ánh xạ sang các địa chỉ MAC multicast của Ethernet nên RFC 3513 khuyến cáo cấp phát ID nhóm từ 32 bit bậc thấp của địa chỉ multicast IPv6 và xét các bit ID nhóm còn lại là 0. Bằng cách chỉ sử dụng 32 bit bậc thấp mỗi ID nhóm ánh xạ 1 địa chỉ MAC multicast duy nhất. Hình sau mô tả điều ta vừa trình bày:



* + - 1. Địa chỉ Node Solicited

Điạ chỉ node solicicated làm cho thuận tiện trong việc query các node mạng trong việc chuyển địa chỉ. Trong IPv4, các khung ARP Request được gửi sang broadcast cấp độ MAC, gửi đến tất cả các node trong từng đoạn mạng, bao gồm các địa chỉ không chạy IPv4. IPv6 dùng các bản tin Neighbor Solicitation để thực hiện việc chuyển đổi địa chỉ. Tuy nhiên thay vì dùng địa chỉ multicast tất cả các node phạm vi liên kết nội bộ như các đích bản tin Neighbor Solicitation, sẽ gửi đến tất cả các node IPv6 trên liên kết nội bộ, địa chỉ multicast solicited node được dùng. Địa chỉ multicast solicited node bao gồm prefix FF02::1:FF00:0/104 và 24 bit sau cùng của điạ chỉ IPv6 được chuyển sang. Hình sau mô tả điều ta vừa trình bày.



Mô tả cấu trúc của địa chỉ Node Solicited.

* + - 1. Địa chỉ Anycast IPv6

Một địa chỉ anycast được cấp cho nhiều giao diện. Các địa chỉ được đánh địa chỉ anycast được chuyển sang giao diện gần nhất mà địa chỉ anycast được cấp. Để dễ dàng cho việc phân phát, cơ sở hạ tầng phải nhận biết được các giao diện được gán địa chỉ anycast và khoảng cách của chúng trong giới hạn của metric định tuyến. Hiện tại thì địa chỉ anycast chỉ được dùng như các địa chỉ đích và chỉ được gán cho các bộ định tuyến. Các địa chỉ anycast cấp không gian địa chỉ unicast và phạm vi của một địa chỉ unicast là phạm vi của kiểu địa chỉ unicast từ địa chỉ anycast được cấp.

Địa chỉ anycast Subnet - Route được định nghĩa trước và là cần thiết. Nó được tạo ra từ prefix mạng con cho một giao diện cho trước. Để thiết kế địa chỉ anycast Subnet-Bộ định tuyến, các bit trong prefix subnet được cố định tại các giá trị thích hợp và các bit còn lại được xét về 0. Tất cả các giao diện của bộ định tuyến kết nối đến đến 1 mạng con được cấp địa chỉ anycast Subnet - Route cho mạng con đó. Địa chỉ anycast Subnet- Route được dùng cho việc truyền thông với một trong nhiều bộ định tuyến được nối đến mạng con ở xa.

* + 1. Sự tương thích địa chỉ

Nhằm chuyển đổi từ IPv4 sang IPv6 và sự tồn tại của cả 2 loại host, các địa chỉ sau được định nghĩa:

• Địa chỉ tương thích IPv4.

Địa chỉ IPv6, địa chỉ 0:0:0:0:0:0:w.x.y.z hoặc ::w.x.y.z được dùng bởi các node IPv6/IPv4 mà truyền thông dùng IPv6. Các node IPv6/IPv4 là các node dùng cả 2 giao thức IPv4 và IPv6. Khi địa chỉ tương thích IPv4 được dùng như 1 đích đến IPv6 thì lưu lượng IPv6 sẽ tự động đóng gói với 1 tiêu đề của IPv4 và gửi đến đích dùng cơ sở hạ tầng IPv4.

• Địa chỉ được ánh xạ sang IPv4

Địa chỉ được ánh xạ sang IPv4 0:0:0:0:0:FFFF:w.x.y.z hoặc ::FFFF:w.x.y.z được dùng để diến tả 1 node chỉ dùng IPv4 sang 1 node IPv6. Nó chỉ được dùng cho diễn tả nội bộ. Địa chỉ được ánh xạ sang IPv4 không được dùng như là một địa chỉ nguồn hoặc đích của 1 gói IPv6.

• Địa chỉ 6 sang 4.

Địa chỉ 6 sang 4 được dùng cho truyền thông giữa 2 node chạy cả IPv4 và IPv6 trên 1 cơ sở hạ tầng định tuyến IPv6. Địa chỉ 6 sang 4 được hình thành bằng cách kết hợp prefix 2002::/16 với 32 bit của 1 địa chỉ IPv4 public của node và hình thành nên 1 prefix 48 bit.

• Địa chỉ IPv6 cho 1 Host.

Một host IPv4 với một bộ thích ứng mạng đơn thường có một địa chỉ IP đơn được cấp cho bộ thích ứng đó. Tuy nhiên, 1 host IPv6 thường có nhiều địa chỉ IPv6, ngay cả với giao diện đơn. Một host IPv6 được cấp cho các địa chỉ unicast sau đây:

- Một địa chỉ liên kết nội bộ cho mỗi giao diện.

- Địa chỉ unicast cho mỗi giao diện (có thể là 1 địa chỉ site nội bộ và 1 hoặc nhiều địa chỉ unicast toàn cầu )

- Địa chỉ loopback (::1) cho giao diện loopback.

Các host IPv6 thông thường là logically multihomed bởi vì chúng có ít nhất 2 địa chỉ mà chúng có thể nhận các gói, 1 địa chỉ liên kết nội bộ cho lưu lượng liên kết nội bộ và 1 địa chỉ toàn cầu hoặc site nội bộ có thể định tuyến được.

Thêm vào đó, mỗi host lắng nghe lưu lương trên các địa chỉ multicast sau:

- Địa chỉ multicast tất cả các node phạm vi giao diện nội bộ (FF01::1)

- Địa chỉ multicast tất cả các node phạm vi liên kết nội bộ (FF02::1)

- Địa chỉ soliticated cho mỗi địa chỉ unicast trên mỗi giao diện.

- Các địa chỉ multicast của các nhóm được tham gia trên mỗi giao diện.

• Địa chỉ IPv6 cho 1 Bộ định tuyến.

Một bộ định tuyến IPv6 được cấp các địa chỉ unicast sau đây:

- Một địa chỉ liên kết nội bộ cho mỗi giao diện.

- Các địa chỉ unicast cho mỗi giao diện (có thể là 1 địa chỉ site nội bộ và 1 hoặc nhiều địa chỉ unicast toàn cầu)

- 1 địa chỉ anycast subnet bộ định tuyến.

- Các địa chỉ anycast thêm vào (option).

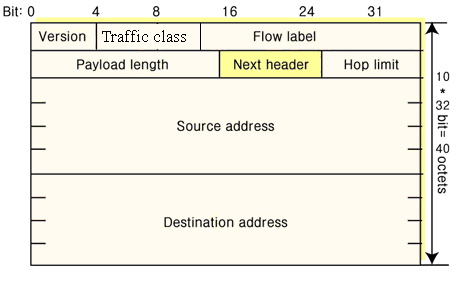
- Địa chỉ loopback (::1) cho giao diện loopback.

* + 1. Địa chỉ IPv4 và sự tương đương IPv6

|  |  |
| --- | --- |
| IPv4 Address | IPv6 Address |
| Các lớp địa chỉ Internet | Không tương xứng trong IPv6 |
| Địa chỉ multicast IPv4 (224.0.0.0/4) | Địa chỉ multicast IPv6 (FF00::/8) |
| Các địa chỉ broadcast | Không tương xứng trong IPv6 |
| Địa chỉ không rõ ràng 0.0.0.0 | Địa chỉ không rõ ràng :: |
| Địa chỉ loopback 127.0.0.1 | Địa chỉ loopback ::1 |
| Public IP address | Global unicast address |
| Địa chỉ IP riêng ( 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16) | Địa chỉ site cục bộ ( FEC0::/10) |
| Địa chỉ tự động được cấu hình (169.254.0.0/16) | Địa chỉ liên kết cục bộ ( FF80::/64) |
| Cách thể hiện: ký hiệu dấu chấm thập phân phân cách | Cách thể hiện: dùng dấu hai chấm có giản lược các số 0 và nén các số 0 liên tiếp |
| Thể hiện các bit mạng: dùng Mặt nạ mạng con hoặc chiều dài prefix | Thể hiện các bit mạng: chỉ dùng chiều dài prefix |
| Chuyển đối tên DSN: bảng ghi tài nguyên địa chỉ host IPv4 | Chuyển đối tên DSN: bảng ghi tài nguyên địa chỉ host IPv6 |
| Chuyển đối ngược DNS | Chuyển đối ngược DNS |

Địa chỉ IPv4 và sự tương đương IPv6

* 1. Khuôn dạng gói tin IPv6
     1. Khuôn dạng gói tin IPv6



Khuôn dạng của gói tin IPv6.

• Phiên bản : 6.

• Lớp vận chuyển : tương tự các kiểu dịch vụ ( Type of service) trong IPv4.

• Nhãn luồng: dùng để đánh dấu tất cả các gói tin cùng thuộc một luồng dữ liệu.

VD: cùng tiếng nói, cùng video.

Trạm nguồn muốn các Bộ định tuyến trung gian xử lý các thông tin cùng luồng giống nhau.

- Các gói tin cùng luồng phải có địa chỉ nguồn, địa chỉ đích và số nhãn luồng giống nhau.

- Số nhãn luồng được phát sinh ngẫu nhiên nhưng không được dùng lại khi thời gian sống của luồng vẫn còn tồn tại trên mạng.

- Nhãn luồng phục vụ cho truyền thông đa phương tiện.

• Độ dài tải: Chứa thông tin hữu ích trong gói tin.

• Tiêu đề tiếp theo:

- Tiêu đề thêm vào phụ thuộc tùy chọn bổ sung. Nó được đặt giữa tiêu đề của IPv6 với tiêu đề của tầng trên.

- Tiêu đề này chỉ được đưa vào khi cần thiết, tránh việc truyền những thông tin dư thừa.

- Một số lựa chọn :

+ Routing: yêu cầu gói tin phải đi qua đường nào.

+ Flagment: Trong trường hợp cần phân mảnh.

+ Yêu cầu được xử lý trên đường truyền: hop by hop.

+ Yêu cầu xử lý gói tin khi đến đích.

+ Thông tin xác thực để trạm thu nhận biết thông tin đích thực của máy nguồn không bị giả danh, không bị thay đổi.

+ Mã hóa nội dung của gói tin.

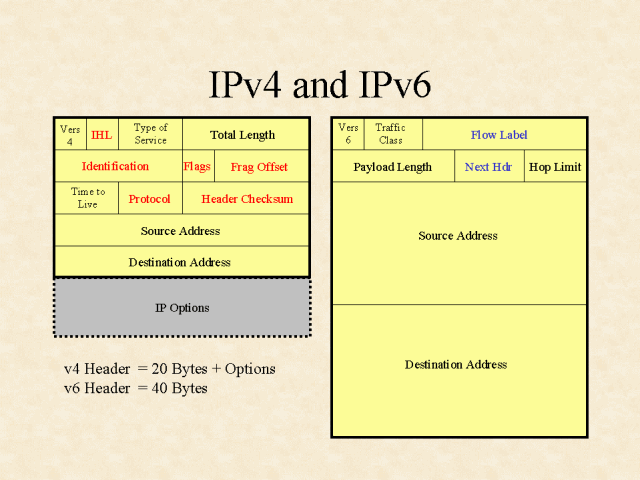
• Giới hạn bước nhảy : số Bộ định tuyến mà gói tin được phép đi qua.

• Địa chỉ nguồn.

• Địa chỉ đích.

- Địa chỉ nguồn và địa chỉ đích có 128bit.

* + 1. So sánh khuôn dạng IPv4 và IPv6



Khuôn dạng gói tin IPv4/IPv6.

|  |  |
| --- | --- |
| IPv4 | IPv6 |
| Version | Cùng trường nhưng với các số phiên bản khác nhau. |
| Tiêu đề Length | Được loại bỏ trong IPv6. IPv6 không chứa trường Tiêu đề Length bởi vì tiêu đề của IPv6 luôn luôn cố định là 40 byte. Mỗi tiêu đề mở rộng có kích thước cố định hoặc có địa chỉ của riêng nó. |
| Type of Service | Được thay thế bằng trường Traffic Class |
| Total Length | Được thay thế bằng trường Payload Length chỉ kích thước của trọng tải. |
| Identification, Fragmentation, Fragment Offset | Được loại bỏ trong IPv6. Thông tin phân mảnh không có trong tiêu đề của IPv6. Nó được chứa trong tiêu đề mở rộng phân mảnh. |
| Time to live | Được thay thế bằng trường Hop Limit. |
| Protocol | Được thay thế bằng trường Next Header. |
| Tiêu đề Checksum | Được loại bỏ trong IPv6. Trong IPv6 việc phát hiện lỗi cấp độ bit cho cả gói IPv6 được thực hiện bởi lớp liên kết. |
| Source Address | Trường này giống nhau chỉ khác là địa chỉ IPv6 có 128 bit. |
| Destination Address | Trường này giống nhau chỉ khác là địa chỉ IPv6 có 128 bit. |
| Options | Được loại bỏ trong IPv6. IPv4 options được thay thế bởi IPv6 extension header. |

So Sánh khuôn dạng gói tin IPv4/ IPv6

* + 1. Các tiêu đề mở rộng của IPv6

Tiêu đề của IPv4 bao gồm tất cả các option. Vì thế, mỗi bộ định tuyến trung gian phải kiểm tra sự tồn của chúng và xử lý chúng khi chúng hiện diện. Điều này làm giảm hiệu suất vận chuyển trong việc vẫn chuyển các gói IPv4. Với IPv6, các option phân phát và được chuyển sang các tiêu đề mở rộng. Tiêu đề mở rộng duy nhất phải được xử lý tại mỗi bộ định tuyến trung gian là tiêu đề mở rộng Hop-by-Hop Option. Điều này sẽ tăng tốc độ xử lý tiêu đề và tăng khả năng xử lý chuyển tiếp.

RFC 2460 định nghĩa các tiêu đề mở rộng IPv6 sau đây phải được hỗ trợ bởi tất cả các node IPv6:

- Hop-by-Hop Option tiêu đề.

- Destination Options tiêu đề.

- Routing tiêu đề.

- Fragment tiêu đề.

- Authentication tiêu đề.

- Encapsulation Security Trọng tải tiêu đề.

Trong 1 gói IPv6 thông thường thì không có mặt tiêu đề mở rộng nào. Nếu việc điều khiển đặc biệt được yêu cầu bởi các bộ định tuyến trung gian hoặc đích thì 1 hoặc nhiều tiêu đề mở rộng được thêm vào bởi host gửi. Mỗi tiêu đề mở rộng có phạm vi 64 bit. Các tiêu đề mở rộng có kích thước thay đổi chứa 1 trường tiêu đề Extension Length và phải dùng đệm khi cần để chắc chắn rằng kích thước của chúng là 1 bội số của 8.

* 1. Những ưu nhược điểm và khó khăn khi triển khai IPv6
     1. Ưu nhược điểm IPv6

*Ưu điểm:*

- Số lượng không hạn chế: IPv6 có chiều dài 128 bít, gấp 4 lần chiều dài bít của địa chỉ IPv4 nên đã mở rộng không gian địa chỉ từ khoảng hơn 4 tỷ địa chỉ lên tới một con số khổng lồ là 2128 địa chỉ.

- Khả năng tự động cấu hình địa chỉ.

- Quản lý định tuyến tốt hơn: Địa chỉ IPv6 được thiết kế có cấu trúc đánh địa chỉ và phân cấp định tuyến thống nhất. Phân cấp định tuyến toàn cầu dựa trên một số mức cơ bản đối với các nhà cung cấp dịch vụ. Cấu trúc định tuyến phân cấp giúp cho địa chỉ IPv6 tránh khỏi nguy cơ quá tải bảng thông tin định tuyến toàn cầu khi chiều dài địa chỉ lên tới 128 bít.

- Hỗ trợ đa dạng các dịch vụ mới: Với công nghệ IPv6 bằng cách loại bỏ dịch vụ NAT (Network Adress Translation), các máy trạm sẽ trực tiếp kết nối với nhau trên nền IP, hỗ trợ mở rộng các dịch vụ mới. Các kết nối ngang hàng sẽ dễ dàng được tạo mới và duy trì, việc kiểm soát chất lượng dịch vụ như VoIP hay Quality of Service (QoS) sẽ trở nên mạnh mẽ hơn.

- Hỗ trợ cho quản lý chất lượng mạng: Những cải tiến trong thiết kế của IPv6 như không phân mảnh, định tuyến phân cấp, gói tin IPv6 được thiết kế với mục đích xử lý thật hiệu quả tại thiết bị định tuyến tạo ra khả năng hỗ trợ tốt hơn cho chất lượng dịch vụ QoS. IPv6 có nhiều trường thông tin về QoS hơn so với địa chỉ IPv4.

*Nhược điểm:*

Những nguy cơ về tồn tại lỗ hổng bảo mật của IPv4: IPv6 chưa thể tự giải quyết tất cả các tồn tại trong IPv4 về ngăn chặn các loại tấn công.

* + 1. Khó khăn gặp phải khi triển khai Ipv6

- Phần lớn thiết bị đầu cuối cũ của người sử dụng hiện nay đều không hỗ trợ IPv6 nên việc triển khai các dịch vụ IPv6 sẽ gặp một số khó khăn nhất định.

- Việc chuyển đổi từ IPv4 sang IPv6 đòi hỏi sự tốn kém cả về thời gian và kinh phí.

* 1. Kết luận

Trong chương 2, bài tiểu luận giới thiệu các dạng địa chỉ, cấu trúc đánh địa chỉ IPv6, qua đó thấy được sự khác biệt và thay đổi trong địa chỉ IPv6. Đây là phiên bản được thiết kế nhằm khắc phục những hạn chế của IPv4 và bổ sung những tính năng mới cần thiết trong hoạt động và dịch vụ mạng thế hệ sau. Chương tiếp theo sẽ đề cập đến việc triển khai mạng IPv6 trên nền mạng đã sử dụng IPv4.

1. TRIỂN KHAI MẠNG IPv6
   1. Triển khai mạng Ipv6 trên nền Ipv4
      1. Các vấn đề chung

Trước đây, giao thức IPv4 nắm vai trò “độc tôn” trong lĩnh vực kết nối mạng.Tuy nhiên, với sự bùng nổ mãnh mẽ của cuộc “cách mạng internet” đã dẫn đến những nguy cơ về việc không đảm bảo được an ninh mạng cũng như thiếu không gian truy cập. Nếu không có biện pháp xử lý kịp thời, máy tính sẽ không thể kết nối mạng. Vì thế yêu cầu nâng cấp và cải tiến hệ thống giao thức đã trở nên bức thiết. Sự ra đời của IPv6 đã giải quyết những bất cập trong hệ thống internet mà IPv4 vẫn còn thiếu sót, từ đó tạo ra một bước tiến nhảy vọt trong thời kỳ công nghệ số. Có rất nhiều lợi ích khiến người dùng cần chuyển đổi từ IPV4 sang cấu trúc địa chỉ PV6 .

Đầu tiên là địa chỉ IPV6 có khả năng cung cấp số lượng lớn địa chỉ IP cao hơn so với IPV4. Nếu như IPV4 chỉ cung cấp được 4,3 tỷ địa chỉ có giới hạn, thì IPV6 có thể cung cấp đến hàng tỷ tỷ địa chỉ IP cho người dùng Internet trên toàn thế giới.

Mặt khác IPV6 có khả năng tương thích ngược với IPV4. Điều này giúp cho các nhà sản xuất phần cứng dễ dàng nâng cấp địa chỉ IP bất cứ lúc nào mà không làm ảnh hưởng sự phát triển của dữ liệu internet. Nhờ tính năng trên, IPV6 được dự đoán sẽ thay thế hoàn toàn IPV4 trong tương lại.

Thêm một động lực thúc đẩy mọi người chuyển đổi từ IPV4 sang IPV6 là IPV6 sở hữu công nghệ mã hóa thông minh. Sản phẩm được cung cấp tính năng xác thực an toàn hơn IPV4. Điều này được thể hiện rõ nét khi IPsec được xem là thành phần bắt buộc của IPV6. Trong khi IPsec chỉ là một thành phần bảo mật của IPV4.

Sau tất cả, địa chỉ IPV6 cho hiệu suất hoạt động tốt hơn IPV4. Nhất là khi IPV6 có khả năng hạn chế tối đa tình trạng mất dữ liệu. Dựa vào đây công nghệ đem đến độ tin cậy cao hơn nhờ hiệu quả kết nối tốt hơn IPV4.

Tuy nhiên hai giao thức IPv4 và IPv6 không thực sự tương thích với nhau Mặt khác, hệ thống IPv4 đã phát triển mạnh mẽ và hiện nay đã hình thành một mạng Internet toàn cầu có quy mô hết sức rộng lớn cả về kiến trúc mạng và dịch vụ trên mạng. Do vậy, trong một tương lai gần không thể chuyển đổi mạng từ IPv4 sang IPv6 được. Để triển khai mạng IPv6 hiệu quả và thiết thực, các nhà thiết kế đã đưa ra giải pháp là triển khai mạng IPv6 trên nền mạng IPv4.

* + 1. Mục đích

Thách thức mà IPv6 phải đối mặt là khả năng chuyển đổi “ trọn vẹn” các gói tin IPv6 từ định dạng theo giao thức IPv6 sang IPv4 để từ đó có thể vận chuyển trên nền hạ tầng là mạng IPv4; vì hầu hết các thiết bị kết nối mạng Internet hiện nay đều được thiết kế cho IPv4.

Để thực hiện yêu cầu này, quá trình triển khai IPv6 phải đảm bảo tính linh động một cách tối đa, nhưng điều này lại mâu thuẫn với quy mô rộng lớn của mạng Internet. Do vậy, đây cũng có thể coi là một điểm chính trong quá trình thiết kế IPv6, đảm bảo sự thành công của mạng IPv6. Không đảm bảo được yêu cầu trên sẽ không có sự thành công của mạng IPv6.

VD: Trước đây đã có một vài giao thức được thiết kế để thử thay thế TCP/IP, như XTP nhưng đã không thể thành công là do không có khả năng chạy song song (dual stack), hay không có tính tương thích lẫn nhau giữa các họ giao thức cũ vào mới. Những tính năng mới của các giao thức này, nếu một mình nó sẽ không đủ thuyết phục để người sử dụng chuyển sang sử dụng.

IPv6 cũng vậy, nếu với các đặc tính ưu việt của nó so với IPv4 cũng chưa đủ để thuyết phục người dùng bỏ mạng IPv4 hiện nay để xây dựng mạng IPv6, do vậy cần phải đảm bảo tính tương thích trên cơ sở các chức năng của IPv4 trong quá trình chuyển đổi sang IPv6.

Để triển khai mạng IPv6 có các phương thức diễn ra đồng thời là xây dựng mạng IPv6 trên nền hạ tầng là mạng IPv4 hiện nay, sau đó thay thế dần mạng IPv4 hiện nay.

Mục đích của các cơ chế chuyển đổi là đảm bảo một số chức năng chính như sau:

• Đảm bảo thực hiện các đặc tính ưu việt của mạng IPv6 so với mạng IPv4

• Tận dụng hạ tầng sẵn có của mạng IPv4 trong giai đoạn chuyển tiếp sang một mạng thuần IPv6

• Tăng cường khả năng nâng cấp và triển khai. Việc chuyển đổi đối với các host/bộ định tuyến không bị phụ thuộc vào nhau.

• Tối thiểu hoá sự phụ thuộc trong các quá trình nâng cấp. Một trong những điều kiện bắt buộc để nâng cấp host với IPv6 là hệ thống DNS server phải được nâng cấp đầu tiên bởi DNS là dịch vụ hỗ trợ việc tìm kiếm địa chỉ phục vụ cho các ứng dụng khác. Cách thức cài đặt và cấu hình DNS server IPv6 sẽ được trình bày trong phần thử nghiệm. Các điều kiện đối với các bộ định tuyến như hỗ trợ các giao thức định tuyến BGP4+, hỗ trợ IPv6 … chưa phải là bắt buộc.

• Gán và cấp phát các loại địa chỉ thuận tiện. Khi các hệ thống IPv4 được cài đặt được gán các địa chỉ IPv4; mặt khác địa chỉ IPv4 là một tập con của của địa chỉ IPv6, do vậy có thể tiếp tục sử dụng với các địa chỉ IPv4 sẵn có. Chỉ gán các địa chỉ IPv6 thật sự cần thiểt cho các kết nối tới 6Bone và tuân theo các kế hoạch phân bổ địa chỉ của tổ chức đó.

• Giá thành khởi điểm thấp. Vì không cần chuẩn bị cần thiết để nâng cấp các hệ thống từ IPv4 sang IPv6 khi triển khai một hệ thống IPv6 mới. Cơ chế này được thực hiện hoàn toàn trên nền IPv4 đã có.

Cơ chế chuyển đổi của IPv6 là có thể kết hợp các trạm IPv6 cùng làm việc với các trạm IPv4 ở bất kỳ nới nào trên Internet cho đến khi địa chỉ IPv4 không còn tồn tại, và cho phép các trạm IPv6 và IPv4 trong một không gian giới hạn để cùng làm việc sau đó. Các cơ chế này đảm bảo khoản đầu tư to lớn của người dùng trong việc xây dựng hệ thống mạng IPv4 đồng thời triển khai được mạng IPv6.

* 1. Các cơ chế chuyển đổi

Hiện nay số lượng các mạng IPv4 là rất lớn; hầu hết các dịch vụ và các giao dịch trên mạng đều dựa trên hạ tầng mạng IPv4; do vậy xuất hiện nhiều cơ chế chuyển đổi cho phép kết nối các host IPv6 qua mạng IPv4.

Việc xây dựng lại giao thức của tầng Internet trong mô hình TCP/IP đã dẫn đến nhiều thay đổi. Trong đó vấn đề thay đổi lớn nhất của IPv6 với IPv4 là việc thay đổi cấu trúc địa chỉ. Sự thay đổi này ảnh hưởng đến các vấn đề sau:

• Ảnh hưởng tới hoạt động của các giao thức ở tầng trên ( Tầng giao vận và tầng ứng dụng)

• Ảnh hưởng tới các phương thức định tuyến.

Mặt khác , một yêu cầu quan trọng trong việc triển khai IPv6 là phải thực hiện được mục tiêu ban đầu đề ra khi thiết kế giao thức IPv6 đó là : IPv6 phải làm việc được trong môi trường sử dụng giao thức IPv4. Sẽ có hiện tượng chỉ có những host dùng duy nhất IPv6 và đồng thời cũng tồn tại những host chỉ duy nhất IPv4. Đồng thời những host “thuần” IPv6 đó phải giao tiếp được với những host IPv4 trong khi đó vẫn đảm bảo địa chỉ IPv4 là có tính thống nhất toàn cầu. Do vậy, để đảm bảo thực hiện các sự tương thích giữa IPv4 và IPv6, các nhà thiết kế IPv6 đã xây dựng một số cơ chế chuyển đổi khác nhau.

Các cơ chế chuyển đổi này có những đặc điểm chung như sau:

- Đảm bảo các host/bộ định tuyến cài đặt IPv6 có thể làm việc được với nhau trên nền IPv4.

- Hỗ trợ các khả năng triển khai các host và bộ định tuyến hoạt động trên nền IPv6 với mục tiêu thay thế dần các host đang hoạt động IPv4.

- Có một phương thức chuyển đổi dễ dàng, thực hiên được ở các cấp khác nhau từ phía người dùng cuối tới người quản trị hệ thống, các nhà quản lý mạng và cung cấp dịch vụ.

Các cơ chế này là một tập các giao thức thực hiên đối với các host và các bộ định tuyến, kèm theo là các phương thức như gán địa chỉ và triển khai, thiết kế để làm quá trình chuyển đổi Internet sang IPv6 làm việc với ít rủi ro nhất có thể được.

Vì vậy cần có những công nghệ phục vụ cho việc chuyển đổi từ địa chỉ IPv4 sang địa chỉ IPv6. Những công nghệ chuyển đổi này, cơ bản có thể phân thành ba loại như sau:

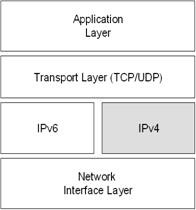
- Công nghệ đường hầm (Tunnel): Công nghệ sử dụng cơ sở hạ tầng mạng IPv4 để truyền tải gói tin IPv6, phục vụ cho kết nối IPv6.

- Dual-stack: Cho phép IPv4 và IPv6 cùng tồn tại trong cùng một thiết bị mạng.

- Công nghệ biên dịch: Thực chất là một dạng thức công nghệ NAT, cho phép thiết bị chỉ hỗ trợ IPv6 có thể giao tiếp với thiết bị chỉ hỗ trợ IPv4.

**3.2.1. Lớp IP song song ( Dual IP layer).**

**3.2.1.1. Tổng quan về kỹ thuật Dual stack:**

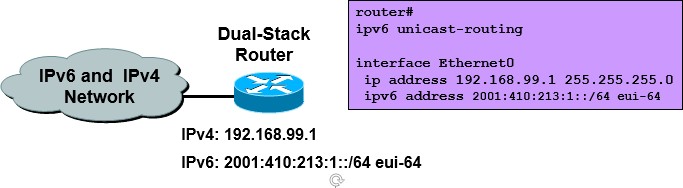
Dual-stack là hình thức thực thi TCP/IP bao gồm cả tầng IP layer của IPv4 và tầng IP layer của IPv6.

Hình vẽ 3.1: Kiến trúc Dual stack

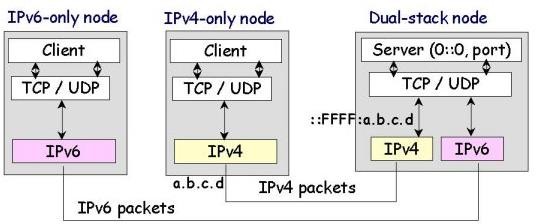
Ứng dụng hỗ trợ dual stack sẽ hoạt động được cả với địa chỉ IPv4 và địa chỉ IPv6.

Về ứng dụng hiện nay hoạt động dual stack, có thể lấy ví dụ: hệ điều hành Window XP, 7, 8, 10 … hệ điều hành của router Cisco.

Dual stack trong hệ điều hành Cisco: Khi người quản trị mạng cấu hình đồng thời cả hai dạng địa chỉ cho một giao diện trên Cisco router, nó sẽ hoạt động dual stack.

  
Hình vẽ 3.2: Khai báo Dual stack trên thiết bị định tuyến

**3.2.1.2. Nguyên tắc hoạt động của kỹ thuật Dual stack**



*Hình vẽ 3.3: Nguyên tắc hoạt động của Dual stack*

Khi một Host chạy ở chế độ Dual stack, Host này sẽ có thể giao tiếp được với cả mạng IPv4 và mạng IPv6.

Khi truyền tải dữ liệu với mạng IPv4, Host Dual stack sẽ đóng địa chỉ IPv4 trong Packet lớp 3 của gói tin.

Khi truyền tải dữ liệu với mạng IPv6, Host Dual stack sẽ đóng gói địa chỉ IPv6 trong Packet lớp 3 của gói tin.

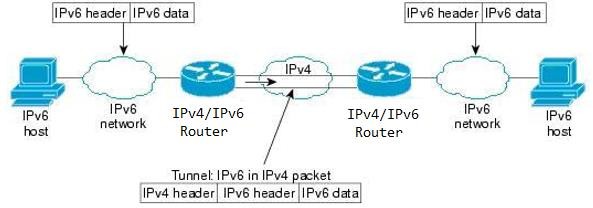
**3.2.1.3. Ứng dụng của kỹ thuật Dual stack**

Trong quá trình chuyển đổi từ IPv4 sang IPv6 việc triển khai kỹ thuật Dual stack là yêu cầu bắt buộc để đảm bảo hai hệ thống mạng hoạt động song song, có thể triển khai kỹ thuật này trên toàn mạng lưới hoặc tại một vài vị trí trên mạng.asd?

**3.2.2. Kỹ thuật đường hầm**

**3.2.2.1. Tổng quan về kỹ thuật đường hầm:**

Công nghệ đường hầm là một phương pháp sử dụng cơ sở hạ tầng sẵn có của mạng IPv4 để thực hiện các kết nối IPv6 bằng cách sử dụng các thiết bị mạng có khả năng hoạt động dual-stack tại hai điểm đầu và cuối nhất định. Các thiết bị này “bọc” gói tin IPv6 trong gói tin IPv4 và truyền tải đi trong mạng IPv4 tại điểm đầu và gỡ bỏ gói tin IPv4, nhận lại gói tin IPv6 ban đầu tại điểm đích cuối đường truyền IPv4.



*Hình vẽ 3.4: Quá trình chuyển tiếp gói tin qua đường hầm*

Giá trị của trường Protocol Field trong IPv4 header luôn được xác lập có giá trị 41 để xác định đây là gói tin IPv6 được bọc trong gói tin IPv4. Do vậy để các gói tin có thể truyền đi trên cơ sở hạ tầng mạng IPv4, nếu trên đường kết nối có sử dụng firewall, firewall này cần phải được thiết lập để cho phép gói tin có giá trị Protocol 41 đi qua.

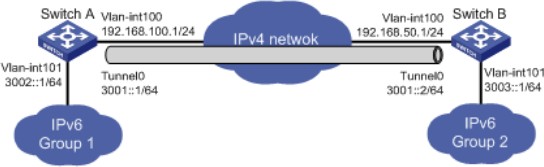
Điểm kết thúc tunnel có thể được xác định tại host hoặc router tạo nên kết nối như sau:

Router-tới-Router

Host-tới-Router hoặc Router-tới-Host

Host-tới-Host

Nguyên tắc hoạt động của việc tạo đường hầm:



*Hình vẽ 3.5: Nguyên tắc tạo đường hầm*

**3.2.2.2. Nguyên tắc của việc tạo đường hầm trong công nghệ tunnel**

Xác định thiết bị kết nối tại các điểm đầu và cuối đường hầm. Hai thiết bị này phải có khả năng hoạt động với cả địa chỉ IPv4 và IPv6.

Xác định địa chỉ IPv4 và địa chỉ IPv6 nguồn và đích của giao diện tunnel (hai đầu kết thúc tunnel).

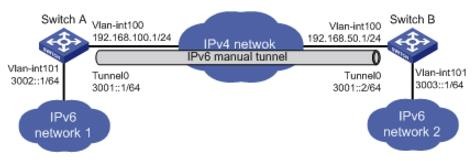
Trên hai thiết bị kết nối tại đầu và cuối tunnel, thiết lập một giao diện tunnel (giao diện ảo, không phải giao diện vật lí) dành cho những gói tin IPv6 sẽ được bọc trong gói tin IPv4 đi qua.

Gắn địa chỉ IPv6 cho giao diện tunnel.

Tạo tuyến (route) để các gói tin IPv6 đi qua giao diện tunnel. Tại đó, chúng được bọc trong gói tin IPv4 có giá trị trường Protocol 41 và chuyển đi dựa trên cơ sở hạ tầng mạng IPv4 và nhờ định tuyến IPv4.

Phân loại kỹ thuật đường hầm:

Tùy theo công nghệ tunnel, các điểm bắt đầu và kết thúc đường tunnel có thể được cấu hình bằng tay bởi người quản trị, hoặc được tự động suy ra từ địa chỉ nguồn và địa chỉ đích của gói tin IPv6. Đường kết nối tunnel sẽ có dạng kết nối điểm - điểm hay điểm - đa điểm. Dựa theo cách thức thiết lập điểm đầu và cuối đường hầm (tunnel), công nghệ tunnel có thể phân thành ba loại: tunnel bằng tay (Manual Tunnel), tunnel bán tự động (Semi- automated) và tunnel tự động (Automatic).

Tunnel bằng tay

*Hình vẽ 3.6: Đường hầm bằng tay*

Tunnel bằng tay là hình thức tạo đường hầm kết nối IPv6 trên cơ sở hạ tầng mạng IPv4, trong đó đòi hỏi phải có cấu hình bằng tay các điểm kết thúc tunnel. Trong tunnel cấu hình bằng tay, các điểm kết cuối đường hầm này sẽ không được suy ra từ các địa chỉ nằm trong địa chỉ nguồn và địa chỉ đích của gói tin.

Thông thường, hình thức tạo đường hầm bằng tay này thường được cấu hình để tạo đường hầm giữa router tới router (hai border router) nhằm kết nối hai mạng IPv6 xác định sử dụng cơ sở hạ tầng mạng IPv4. Nó cũng có thể được cấu hình giữa router và host để kết nối IPv6 host vào một mạng IPv6 từ xa.

Việc cấu hình giao diện tunnel, bao gồm địa chỉ IPv6 gắn cho giao diện tunnel, địa chỉ IPv4 của các điểm kết thúc tunnel cần phải được cấu hình bằng tay cùng với tuyến sẽ sử dụng giao diện tunnel.

Tunnel cấu hình bằng tay tương đương với một đường link vĩnh viễn (permanent link) giữa hai miền IPv6 trên cơ sở hạ tầng mạng IPv4, cho một kết nối ổn định giữa hai điểm xác định. Dạng kết nối tunnel này là kết nối điểm - điểm, tạo nên một đường kết nối ổn định, bảo mật, riêng biệt. Tính chất này tương tự như khi ta cấu hình định tuyến tĩnh (static route) so với định tuyến động (dynamic route). Tuy nhiên, nó đòi hỏi cấu hình, quản trị thủ công. Nếu muốn kết nối tới nhiều điểm, sẽ phải tạo nhiều giao diện tunnel và nhiều đường tunnel.

Trong trường hợp một tổ chức có hai phân mạng IPv6 tại hai vùng địa lý và chỉ có cơ sở hạ tầng IPv4 giữa hai phân mạng này. Trong trường hợp đó, để có thể có kết nối IPv6, tạo một tunnel cấu hình bằng tay giữa hai router gateway của hai phân mạng có thể là sự lựa chọn tốt nhất để có một kết nối ổn định.

Tunnel bán tự động (Tunnel Broker):

Tunnel Broker là hình thức tunnel, trong đó một tổ chức đứng ra làm trung gian, cung cấp kết nối tới Internet IPv6 cho những thành viên đăng ký sử dụng dịch vụ Tunnel Broker do tổ chức cung cấp.

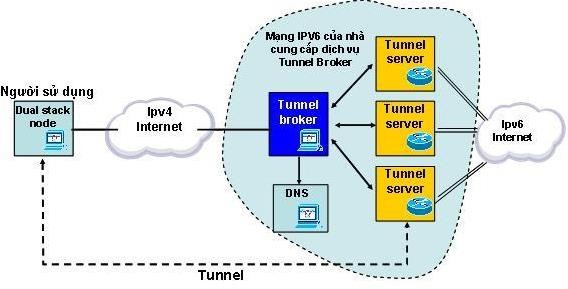


*Hình vẽ 3.7: Đường hầm Broker*

Tổ chức cung cấp dịch vụ Tunnel Broker có vùng địa chỉ IPv6 độc lập, toàn cầu, xin cấp từ các tổ chức quản lý địa chỉ IP quốc tế, mạng IPv6 của tổ chức có kết nối tới Internet IPv6 và những mạng IPv6 khác. Thành viên đăng ký và được cấp quyền sử dụng dịch vụ Tunnel Broker sẽ nhận được những thông tin từ tổ chức quản lý Tunnel Broker để thiết lập đường hầm tunnel từ host hoặc từ router gateway mạng IPv6 của tổ chức mình tới mạng của tổ chức duy trì Tunnel Broker, từ đó kết nối tới được Internet IPv6 hay những mạng IPv6 khác mà tổ chức duy trì Tunnel Broker có kết nối tới.

Người sử dụng sẽ kết nối tới được IPv6 Internet và các mạng IPv6 khác khi đăng ký và được phép sử dụng dịch vụ Tunnel Broker của nhà cung cấp. Người sử dụng sẽ được cung cấp thông tin để thiết lập đường hầm từ host hoặc mạng của mình đến mạng của tổ chức duy trì Tunnel Broker và dùng mạng này như một trung gian để kết nối tới các mạng IPv6 khác. Người đăng ký sử dụng dịch vụ Tunnel Broker sẽ được cấp một vùng địa chỉ thuần IPv6, tuỳ theo nhu cầu sử dụng từ không gian địa chỉ IPv6 của nhà cung cấp dịch vụ tunnel broker và được chuyển giao một không gian tên miền cấp dưới không gian tên miền của nhà cung cấp dịch vụ Tunnel Broker. Đây là địa chỉ và tên miền hợp lệ toàn cầu, thành viên của Tunnel Broker có thể sử dụng tên miền này để thiết lập IPv6 Website cho phép những mạng IPv6 có kết nối tới mạng của nhà cung cấp dịch vụ Tunnel Broker truy cập tới.

Đường hầm thiết lập giữa người sử dụng và mạng của nhà cung cấp dịch vụ Tunnel Broker được cấu hình trên nguyên lý Tunnel bằng tay.

*Mô hình của Tunnel Broker:*

*Hình vẽ 3.8: Các thành phần của đường hầm Broker*

Tunnel Broker: là những máy chủ dịch vụ làm nhiệm vụ quản lý thông tin đăng ký, cho phép sử dụng dịch vụ, quản lý việc tạo đường hầm, thay đổi thông tin đường hầm cũng như xoá đường hầm. Trong hệ thống dịch vụ Tunnel Broker của nhà cung cấp, máy chủ Tunnel Broker sẽ liên lạc với

Tunnel Server (thực chất là các dual-stack router) và máy chủ tên miền của nhà cung cấp Tunnel Broker để thiết lập đường hầm phía nhà cung cấp dịch vụ Tunnel Broker và tạo bản ghi tên miền cho người đăng ký sử dụng dịch vụ Tunnel Broker. Người sử dụng thông qua mạng Internet IPv4 sẽ truy cập máy chủ Tunnel Broker và đăng ký tài khoản sử dụng dịch vụ Tunnel Broker thông qua mẫu đăng ký dưới dạng Web.

Tunnel Server: Thực chất là các router dual-stack làm nhiệm vụ cung cấp kết nối để người đăng ký sử dụng dịch vụ kết nối tới để truy cập vào mạng IPv6 của tổ chức cung cấp Tunnel Broker. Các router này là điểm kết thúc tunnel phía nhà cung cấp dịch vụ Tunnel Broker. Tunnel Server nhận yêu cầu từ máy chủ Tunnel Broker và tạo, hoặc xoá đường tunnel phía nhà cung cấp Tunnel Broker.

*Liên hệ giữa người sử dụng, Tunnel broker, Tunnel Server, máy chủ tên miền*

Đăng ký sử dụng địch vụ Tunnel Broker: Nếu người sử dụng chỉ muốn kết nối một host vào mạng IPv6 của nhà cung cấp tunnel broker, sẽ đăng ký dạng host và yêu cầu cấp một địa chỉ (/128). Nếu người sử dụng muốn kết nối một mạng, cần đăng ký và Tunnel Broker sẽ cấp cho một vùng địa chỉ theo nhu cầu (thường là prefix /64 nếu mạng IPv6 của tổ chức chỉ có một subnet duy nhất hoặc prefix /48 nếu mạng IPv6 của tổ chức có nhiều subnet và cần nhiều hơn một prefix /64).

Thiết lập đường hầm phía nhà cung cấp dịch vụ Tunnel Broker: Khi nhận được thông tin đăng ký và chấp nhận yêu cầu, máy chủ Tunnel Broker sẽ liên hệ với Tunnel Server, máy chủ tên miền của nhà cung cấp dịch vụ Tunnel Broker để thiết lập đường hầm phía nhà cung cấp Tunnel Broker và tạo bản ghi tên miền rồi gửi các thông tin cần thiết phục vụ cho người sử dụng tạo đường hầm phía người sử dụng (thông qua email, hoặc web form).

Thông tin được gửi tới người sử dụng thường bao gồm:

Địa chỉ IPv4 phía client (người sử dụng, địa chỉ này do người sử dụng cung cấp cho Tunnel Broker khi đăng ký). Đây sẽ là địa chỉ IPv4 của đầu tunnel phía người sử dụng.

Địa chỉ IPv4 phía server (địa chỉ IPv4 của một dual-stack router của nhà cung cấp Tunnel Broker, là các Tunnel server). Đây là địa chỉ IPv4 của đầu tunnel phía nhà cung cấp dịch vụ tunnel broker.

Địa chỉ IPv6 phía client. Đây là địa chỉ IPv6 thuộc vùng địa chỉ IPv6 của nhà cung cấp dịch vụ Tunnel Broker cấp cho người đăng ký để sử dụng cho mạng IPv6 và cho kết nối.

Địa chỉ IPv6 phía server (Địa chỉ IPv6 của dual-stack router của nhà cung cấp Tunnel Broker)

Tên miền nhà cung cấp Tunnel Broker cấp cho người sử dụng. Đây là tên miền hợp lệ toàn cầu, đăng ký trên máy chủ tên miền của nhà cung cấp dịch vụ Tunnel Broker.

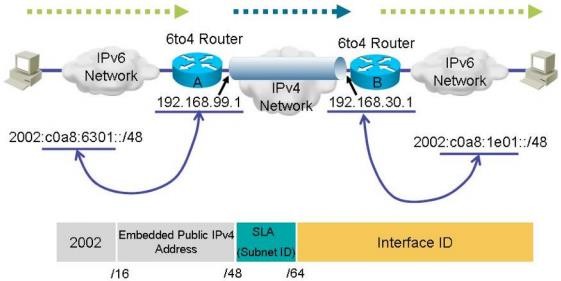
Thiết lập đường hầm phía người sử dụng:

Dựa trên những thông tin nhận được, người sử dụng sẽ cấu hình bằng tay trên host hoặc router của mình đường hầm tunnel kết nối với mạng của nhà cung cấp dịch vụ tunnel broker. Trên các hệ điều hành khác nhau và các thiết bị mạng khác nhau có hỗ trợ IPv6 sẽ cung cấp các tập hợp lệnh tương ứng để cấu hình tunnel.

Trong nhiều trường hợp, tổ chức cung cấp dịch vụ Tunnel Broker xây dựng các chương trình Client giúp người sử dụng không phải trực tiếp gõ lệnh để thiết lập tunnel mà chỉ việc cài đặt chương trình và giao tiếp với chương trình qua giao diện.

Tunnel tự động (6to4 tunnel)

Tunnel tự động là công nghệ tunnel trong đó không đòi hỏi phải cấu hình địa chỉ IPv4 của điểm bắt đầu và kết thúc tunnel bằng tay.



*Hình vẽ 3.9: Đường hầm 6to4*

Đường hầm tự động, là kỹ thuật 6to4 tunnel. Kỹ thuật 6to4 tunnel cho phép truy cập Internet IPv6 mà không cần nhiều thủ tục hay cấu hình phức tạp, bằng cách sử dụng địa chỉ IPv6 đặc biệt có tiền tố prefix 2002::/16 đã được IANA cấp dành riêng cho công nghệ 6to4, kết hợp với địa chỉ IPv4 toàn cầu.

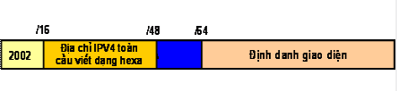
Tunnel 6to4 cho phép những miền IPv6 6to4 tách biệt có thể kết nối qua mạng IPv4 tới những miền IPv6 6to4 khác. Điểm khác biệt cơ bản nhất giữa tunnel tự động 6to4 và tunnel cấu hình bằng tay là ở chỗ đường hầm 6to4 là dạng kết nối điểm - đa điểm. Trong đó, các router không được cấu hình thành từng cặp mà chúng coi môi trường kết nối IPv4 là một môi trường kết nối vật lý ảo. Chính địa chỉ IPv4 gắn trong địa chỉ IPv6 sẽ được sử dụng để tìm thấy đầu bên kia của đường tunnel.

Kỹ thuật tunnel 6to4 được sử dụng khi kết nối nhiều mạng IPv6 riêng biệt, trong đó mỗi mạng có ít nhất một đường kết nối tới mạng IPv4 chung sử dụng địa chỉ IPv4 toàn cầu.

*Địa chỉ IPv6 sử dụng trong 6to4 tunnel*

IANA đã phân bổ dành riêng một prefix địa chỉ cho công nghệ tunnel 6to4 toàn cầu. Đó là 2002::/16

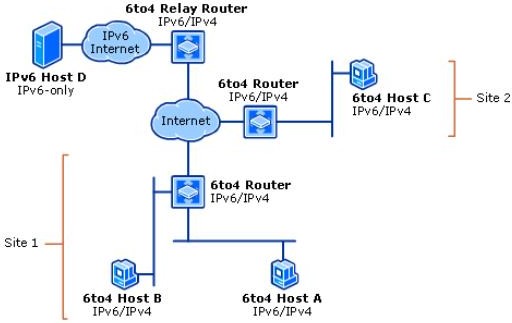
Prefix địa chỉ này, kết hợp với 32 bít địa chỉ IPv4 sẽ tạo nên một prefix địa chỉ 6to4 kích cỡ /48 duy nhất toàn cầu sử dụng cho một mạng IPv6.

Prefix /48 địa chỉ IPv6 tương ứng một địa chỉ IPv4 toàn cầu được tạo nên theo nguyên tắc theo hình vẽ:

*Hình vẽ 3.10: Cấu trúc địa chỉ sử dụng trong đường hầm 6to4*

Ví dụ, nếu một router đang nối vào Internet IPv4 với địa chỉ 203.119.9.15. Khi đó chúng ta sẽ có một vùng địa chỉ IPv6 6to4 như sau: 2002:cb77:090f::/48

*Các thành phần của tunnel 6to4, cung cấp kết nối IPv6 toàn cầu*



*Hình vẽ 3.11: Sơ đồ kết nối sử dụng đường hầm 6to4*

6to4 host: Là bất kỳ host IPv6 nào được cấu hình với ít nhất một địa chỉ 6to4, địa chỉ 6to4 có thể được tự động cấu hình.

6to4 router: Là một router dual-stack hỗ trợ sử dụng giao diện 6to4. Router này sẽ chuyển tiếp lưu lượng có gán địa chỉ 6to4 giữa những 6to4 host trong một site và tới những router 6to4 khác hoặc tới 6to4 relay router trong mạng IPv4 Internet.

6to4 relay router: Là một dual stack router thực hiện chuyển tiếp lưu lượng có địa chỉ 6to4 của những router 6to4 trên Internet và host trên IPv6 Internet (sử dụng địa chỉ IPv6 chính thức, cung cấp bởi tổ chức quản lý địa chỉ toàn cầu). 6to4 relay router là một 6to4 router được cấu hình để hỗ trợ chuyển tiếp định tuyến giữa địa chỉ 6to4 và địa chỉ IPv6 chính thức (địa chỉ IPv6 định danh toàn cầu). 6to4 relay router sẽ là gateway kết nối giữa mạng 6to4 và IPv6 Internet. Nhờ đó giúp cho những mạng IPv6 6to4 có thể kết nối tới Internet IPv6.

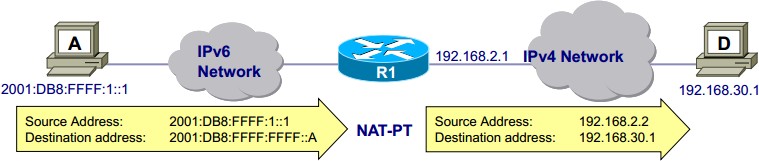
**3.2.2.3. Ứng dụng của kỹ thuật đường hầm**

Kỹ thuật đường hầm được sử dụng trong trường hợp cần kết nối giữa các phân hệ mạng IPv6 thông qua mạng trung gian IPv4.

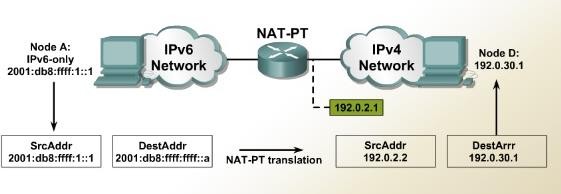
**3.2.3. Kỹ thuật biên dịch (NAT-PT)**

**3.2.3.1. Tổng quan về kỹ thuật biên dịch**

Kỹ thuật biên dịch thực chất là một dạng kỹ thuật NAT, thực hiện biên dịch địa chỉ, cho phép host chỉ hỗ trợ IPv6 có thể nói chuyện với host chỉ hỗ trợ IPv4. Công nghệ phổ biến được sử dụng là NAT-PT. Thiết bị cung cấp dịch vụ NAT-PT sẽ biên dịch header và địa chỉ cho phép IPv6 host nói chuyện với IPv4 host.



*Hình vẽ 3.12: Hình vẽ mô tả quá trình chuyển dịch IPv6 sang IPv4*

**3.2.3.2. Nguyên tắc hoạt động của kỹ thuật biên dịch**

*Hình vẽ 3.13: Nguyên tắc hoạt động của kỹ thuật NAT-PT*

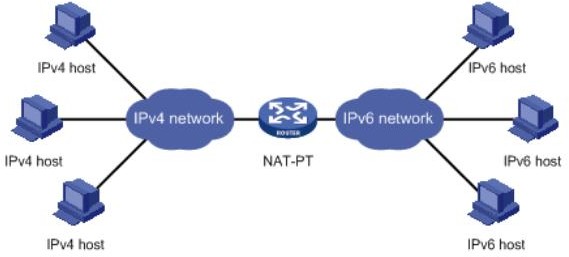
Các gói tin từ mạng IPv4 sang mạng IPv6 khi qua bộ định tuyến NAT-

PT sẽ được chuyển đổi gói tin IPv6 với địa chỉ nguồn là một địa chỉ IPv6 nằm trong NAT Prefix. Trong trường hợp NAT tĩnh mỗi địa chỉ trong NAT Prefix tương ứng với một địa chỉ IPv4 ban đầu (ánh xạ 1:1). Trong trường hợp NAT động một địa chỉ IPv6 trong NAT Prefix này có thể dùng cho một hoặc nhiều địa chỉ IPv4. Các gói tin trao đổi qua lại giữa các site IPv4 và IPv6 cần có sự thay đổi về cấu trúc. Khi gói tin rời khỏi mạng IPv4 sang mạng IPv6 (hay ngược lại IPv6 sang IPv4) thông qua bộ định tuyến NAT - PT, phần đầu IPv4 được tách ra và thay thế bởi phần đầu IPv6.

Trên hình vẽ, Node A (IPv6) muốn giao tiếp được với Node D (IPv4), thì địa chỉ của Node A (IPv6) cần được chuyển đổi thành IPv4 khi đi qua thiết bị NAT-PT, cũng như vậy Node D (IPv4) muốn giao tiếp được với Node A (IPv6) thì địa chỉ của Node D (IPv4) cần được chuyển đổi thành IPv6 khi đi qua thiết bị NAT-PT.

**3.2.3.3. Ứng dụng của kỹ thuật biên dịch**

Kỹ thuật biên dịch thường được triển khai trên thiết bị biên giữa mạng IPv4 và mạng IPv6, cho phép mạng IPv4 và mạng IPv6 có thể giao tiếp được với nhau thông qua việc chuyển đổi địa chỉ.



*Hình vẽ 3.14: Mô hình ứng dụng của kỹ thuật NAT-PT*

* 1. Kết luận

Tình trạng cạn kiệt tài nguyên IPv4 không chỉ là vấn đề cho nhà cung cấp dịch vụ ISP hay những người sử dụng Internet mà là vấn đề của toàn cầu .Vì vậy việc chuyển đổi từ Ipv4 sang Ipv6 là điều tất yếu .Chương này đã trình bày những phương pháp để giải quyết nhu cầu đó.Môi phương pháp có những ưu nhược điểm riêng và tùy vào từng tình huống để sử dụng sao cho hợp lý.