BAN CÔNG TÁC THÚC ĐẨY PHÁT TRIỂN IPV6 QUỐC GIA
TRUNG TÂM INTERNET VIỆT NAM

Biên soạn: Ths Nguyễn Thị Thu Thủy – Trung tâm Internet Việt Nam
Thẩm định: Tiến sỹ Hà Hải Nam; Tiến sỹ Nguyễn Hồng Sơn – Học viện Công nghệ Bưu chính Viễn thông

GIỚI THIỆU VỀ ĐỊA CHỈ INTERNET THẾ HỆ MỚI IPV6

Hà nội 11/2014

MỤC LỤC

CHƯƠNG 1: LÝ DO RA ĐỜI IPV6

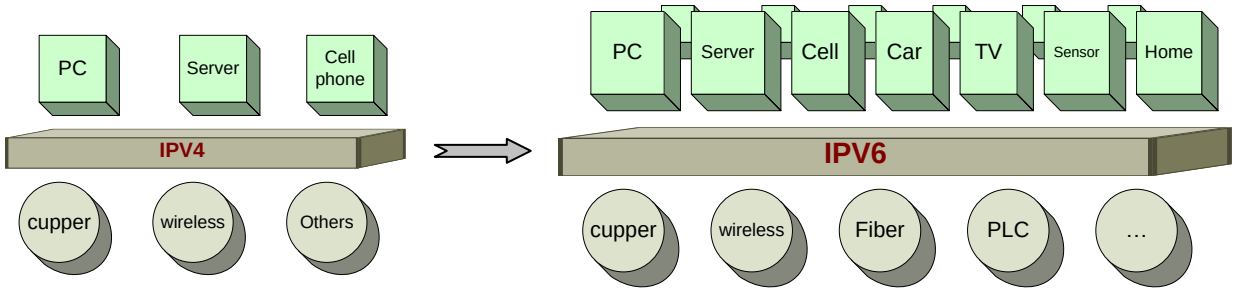
1.1 NHỮNG HẠN CHẾ CỦA IPV4

1.1.1 Sự cạn kiệt không gian địa chỉ IPv4

Kể từ năm 2003, khi tốc độ tiêu thụ địa chỉ IPv4 bắt đầu tăng vọt do Internet phát triển tại những khu vực dân cư đông đảo như Trung Quốc, Ấn Độ kết hợp với sự phát triển của các loại hình dịch vụ và phương thức kết nối mạng tiêu tốn địa chỉ (những dạng dịch vụ mới đòi hỏi không gian địa chỉ IP cố định và tỉ lệ sử dụng địa chỉ/khách hàng là 1:1 với kết nối dạng đầu cuối – đầu cuối như: dịch vụ xDSL, dịch vụ Internet qua đường cáp truyền hình,…), khả năng cạn kiệt nguồn IPv4 toàn cầu đã trở thành chủ đề nóng được bàn thảo nhiều trên các diễn đàn, thông tin về hoạt động của mạng Internet.

Những năm tiếp theo, vùng địa chỉ IPv4 dự trữ cho hoạt động Internet toàn cầu được quản lý bởi IANA ngày càng vơi đi nhanh, việc IPv4 sẽ hết trở nên rõ ràng và tất yếu. Năm 2007, toàn bộ 5 tổ chức quản lý tài nguyên địa chỉ cấp vùng (RIR) đã đồng loạt ban hành nghị quyết thông báo địa chỉ IPv4 sẽ cạn kiệt trong khoảng 2 đến 4 năm sau đó và kêu gọi cộng đồng triển khai địa chỉ IPv6 để thay thế, đảm bảo sự phát triển không gián đoạn của hoạt động Internet.

Tại thời điểm cuối năm 2007, căn cứ trên tốc độ tiêu thụ IPv4 toàn cầu, các tổ chức quốc tế đã dự báo thời điểm cạn kiệt IPv4 là giữa năm 2012. Tuy nhiên các năm sau đó, tốc độ xin cấp địa chỉ IPv4 tăng lên rất nhanh, tốc độ cấp phát địa chỉ IPv4 của các tổ chức quản lý địa chỉ cấp vùng ngày càng tăng cao. Đến giữa năm 2008, thời điểm hệ thống quản lý địa chỉ toàn cầu hết IPv4 được dự báo rơi vào khoảng tháng 11/2011.



Hình 1: Sự biến đổi của Internet

Trên thực tế, thời điểm cạn kiệt IPv4 toàn cầu diễn ra nhanh hơn dự báo. Ngày 3 tháng 2 năm 2011, IANA đã chính thức công bố cạn kiệt kho địa chỉ dự trữ cấp phát cho các RIR. Toàn bộ yêu cầu xin cấp IPv4 cho các hoạt động Internet toàn cầu chỉ sử dụng các vùng địa chỉ dữ trữ của các tổ chức cấp vùng (RIR). Việc cạn kiệt hoàn toàn địa chỉ IPv4 tại từng khu vực tùy thuộc theo tốc độ tiêu thụ tại khu vực.

Theo mô hình quản lý toàn cầu, không gian địa chỉ IP các loại và số hiệu mạng được quản lý thống nhất bởi tổ chức IANA. IANA sau đó cấp các không gian địa chỉ lớn cho các tổ chức quản lý tài nguyên cấp khu vực RIR (regional Internet registry). Trên thế giới có tổng cộng 5 RIR bao gồm APNIC phụ trách khu vực Châu Á Thái Bình Dương, RIPE NCC phụ trách khu vực Châu Âu và Trung Đông, ARIN phụ trách khu vực Bắc Mỹ, LACNIC

phụ trách khu vực Châu Mỹ La tin và AFRINIC phụ trách khu vực Châu Phi. Các RIR sau khi nhận tài nguyên từ IANA sẽ chịu trách nhiệm quản lý, phân bổ các tài nguyên đó trong phạm vi khu vực.

Với tốc độ tiêu thụ tài nguyên IPv4 lớn nhất trên toàn cầu, Châu Á – Thái Bình Dương là khu vực đầu tiên chính thức bước vào giai đoạn cạn kiệt IPv4 kể từ ngày 15/4/2011 khi toàn bộ khối lượng địa chỉ IPv4 dự trữ của APNIC được tiêu thụ, chỉ còn lại duy nhất một khối /8 để phục vụ cho việc chuyển đổi sang sử dụng địa chỉ IPv6.

Tiếp theo đó, ngày 14/9/2012, RIPE NCC, tổ chức quản lý địa chỉ khu vực Châu Âu và Trung Đông thông báo đã chính thức hết IPv4 để cấp theo chính sách thông thường và chuyển sang chính sách cấp phát hạn chế IPv4 từ khối /8 cuối cùng. Muộn hơn một chút, các khu vực khác là Châu Mỹ La tin (LACNIC) và Bắc Mỹ (ARIN) đều hết IPv4 vào đầu năm 2014.

Ở thời điểm hiện tại (tháng 11/2014), chỉ còn duy nhất khu vực Châu Phi (do AFRINIC quản lý) chưa rơi vào tình trạng cạn kiệt địa chỉ IPv4.

1.1.2 Hạn chế về công nghệ và nhược điểm của IPv4

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, ví dụ thực hiện phân mảnh, điều này tiêu tốn CPU của router và ảnh hưởng đến hiệu quả xử lý (gây trễ, hỏng gói tin).

Hạn chế về tính bảo mật và kết nối đầu cuối – đầu cuối:

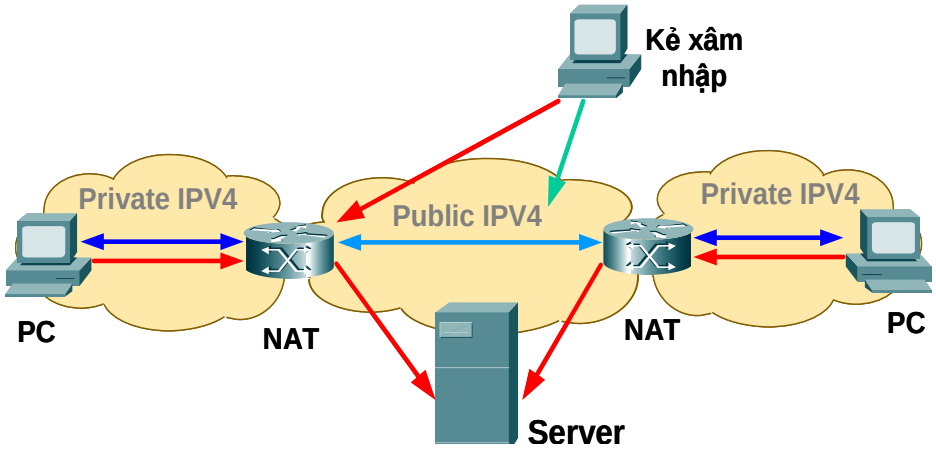
Trong cấu trúc thiết kế của địa chỉ IPv4 không có cách thức bảo mật nào đi kèm. IPv4 không cung cấp phương tiện hỗ trợ mã hóa dữ liệu. Kết quả là hiện nay, bảo mật ở mức ứng dụng được sử dụng phổ biến, không bảo mật lưu lượng truyền tải giữa các host. Nếu áp dụng IPSec[1] là một phương thức bảo mật phổ 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.

Để giảm nhu cầu tiêu dùng địa chỉ, hoạt động mạng IPv4 sử dụng phổ biến công nghệ biên dịch NAT. Trong đó, máy chủ biên dịch địa chỉ can thiệp vào gói tin truyền tải và thay thế trường địa chỉ để các máy tính gắn địa chỉ riêng (private) có thể kết nối vào mạng Internet.

Mô hình sử dụng NAT của địa chỉ IPv4 có nhiều nhược điểm:

- Khó thực hiện được kết nối điểm – điểm và gây trễ: Làm khó khăn và ảnh hưởng tới nhiều dạng dịch vụ (VPN, dịch vụ thời gian thực). Đối với nhiều dạng dịch vụ cần xác thực port nguồn/ đích, sử dụng NAT là không thể được. Trong khi đó, các ứng dụng mới hiện nay, đặc biệt các ứng dụng client-server ngày càng đòi hỏi kết nối trực tiếp đầu cuối – đầu cuối.
- Việc gói tin không được giữ nguyên tình trạng từ nguồn tới đích, có những điểm trên đường truyền tải tại đó gói tin bị can thiệp, như vậy tồn tại những lỗ hổng về bảo mật.

[1] IPSec : Một công nghệ cung cấp bảo mật, xác thực và những dịch vụ an ninh khác tại tầng IP.



Hình 2: Mô hình thực hiện NAT của địa chỉ IPv4

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. Giao thức Internet mà IETF[2] 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, gồm 128 bít.

1.1.3 Mục tiêu trong thiết kế IPv6:

IPv6 được thiết kế với những tham vọng và mục tiêu như sau:

- Không gian địa chỉ lớn hơn và dễ dàng quản lý không gian địa chỉ.
- Hỗ trợ kết nối đầu cuối-đầu cuối và loại bỏ hoàn toàn công nghệ NAT
- Quản trị TCP/IP dễ dàng hơn: DHCP được sử dụng trong IPv4 nhằm giảm cấu hình thủ công TCP/IP cho host. IPv6 được thiết kế với khả năng tự động cấu hình mà không cần sử dụng máy chủ DHCP, hỗ trợ hơn nữa trong việc giảm cấu hình thủ công.
- Cấu trúc định tuyến tốt hơn: Định tuyến IPv6 được thiết kế hoàn toàn phân cấp.
- Hỗ trợ tốt hơn Multicast[3]: Multicast là một tùy chọn của địa chỉ IPv4, tuy nhiên khả năng hỗ trợ và tính phổ dụng chưa cao.
- Hỗ trợ bảo mật tốt hơn: IPv4 được thiết kế tại thời điểm chỉ có các mạng nhỏ, biết rõ nhau kết nối với nhau. Do vậy bảo mật chưa phải là một vấn đề được quan tâm. Song hiện nay, bảo mật mạng internet trở thành một vấn đề rất lớn, là mối quan tâm hàng đầu.

[2] IETF: Internet Engineering Taskforce - Tổ chức tiêu chuẩn hoá, viết các tài liệu tiêu chuẩn hoá (RFC) phục vụ hoạt động Internet toàn cầu.
[3]Multicast: Công nghệ cho phép gửi một gói tin IP đồng thời tới một nhóm xác định các thiết bị mạng.

- Hỗ trợ tốt hơn cho di động: Thời điểm IPv4 được thiết kế, chưa tồn tại khái niệm về thiết bị IP di động. Trong thế hệ mạng mới, dạng thiết bị này ngày càng phát triển, đòi hỏi cấu trúc giao thức Internet có sự hỗ trợ tốt hơn.

1.2 TÌNH HÌNH TRIỂN KHAI IPV6

1.2.1 Tiêu chuẩn hóa IPv6

Ý tưởng về việc phát triển giao thức Internet mới được giới thiệu tại cuộc họp IETF 25 tháng 7 năm 1994, trong RFC1752[4], giới thiệu thủ tục IP phiên bản mới.

Quá trình phát triển, xem xét, sửa đổi, hoàn thiện hóa các thủ tục Internet phiên bản 6 được thực hiện bởi nhóm làm việc về IPv6 của IETF. Sau nhiều năm nghiên cứu, những hoạt động cơ bản của thế hệ địa chỉ này đã được định nghĩa và công bố năm 1998 trong một chuỗi tài liệu tiêu chuẩn từ RFC2460 tới RFC2467. Trong đó nổi bật nhất là tiêu chuẩn hóa địa chỉ IPv6 RFC 2460[5] , và hai thủ tục thiết yếu trong hoạt động của IPv6, hỗ trợ cho IPv6, đó là: RFC2461[6] mô tả một thủ tục mới, phụ trách giao tiếp giữa các node IPv6 trong một đường kết nối nội bộ và RFC2463[7] mô tả ICMPv6.

Cũng trong năm 1998, IETF công bố hai tài liệu chi tiết hơn về địa chỉ IPv6, RFC2373[8], mô tả cấu trúc địa chỉ IP phiên bản 6 và RFC2374[9], mô tả dạng địa chỉ IPv6 định danh toàn cầu. Trải qua thời gian dài điều chỉnh, cả hai tài liệu này được thay thế cập nhật bởi hai RFC mới. Đó là RFC3513[10], cấu trúc đánh địa chỉ IP phiên bản 6 và RFC3587[11], mô tả dạng thức địa chỉ IPv6 định danh và định tuyến toàn cầu.

Đồng thời, rất nhiều RFC khác được công bố, định nghĩa tiêu chuẩn hóa cho những chức năng của IPv6, mô tả phiên bản mới hỗ trợ IPv6 cho các dịch vụ như DNS, DHCP…

Thời điểm hiện nay, những tiêu chuẩn cơ bản cho hoạt động của giao thức Internet phiên bản 6 đã được hoàn thiện. Tuy nhiên, chúng sẽ tiếp tục được sửa đổi nhằm đáp ứng yêu cầu thực tế, song song với việc phát triển đầy đủ những đặc tính mới trong giao thức IPv6. Nội dung cuốn sách này mô tả hoạt động cơ bản IPv6 theo những tài liệu RFC mới nhất hiện hành. Bạn có thể tìm hiểu thêm thông tin về tiêu chuẩn hóa IPv6 tại trang web của nhóm làm việc về IPv6 của IETF (http://www.ietf.org/html.charters/IPv6-charter.html) và những nhóm làm việc khác liên quan đến IPv6 của IETF.

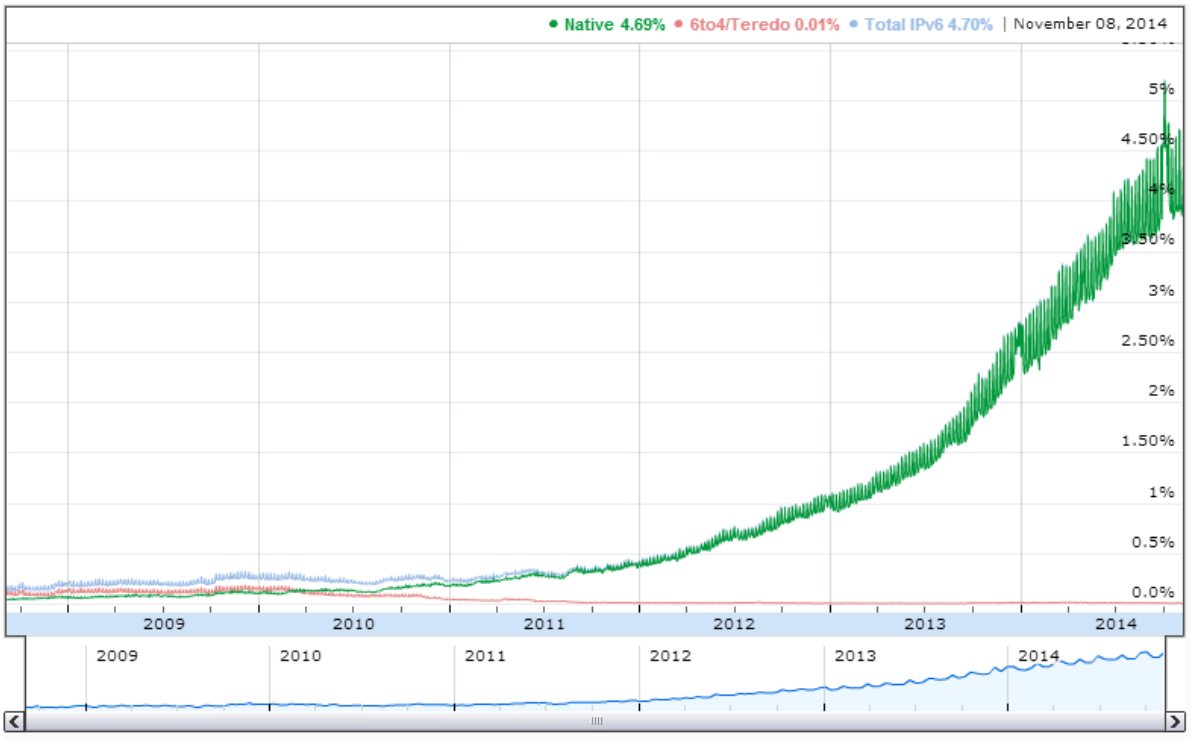
1.2.2 Tình hình triển khai IPv6 trên thế giới

Nếu trước 2010 chủ yếu tập trung vào hoạt động nghiên cứu thử nghiệm thì sau 2010 đặc biệt là sau thời điểm thế giới cạn kiệt IPv4 (tháng 3/2011) thì các nhà mạng tập trung mạnh vào hoạt động triển khai mạng lưới và cung cấp dịch vụ IPv6 chính thức.

Để đánh giá kết quả triển khai hay mức độ sẵn sàng với IPv6 của một mạng lưới, một quốc gia hay khu vực các tổ chức đánh giá có uy tín thường dựa vào một số tiêu chí cơ bản như tỉ lệ % các vùng địa chỉ IPv6 được quảng bá trên bảng định tuyến toàn cầu so với các vùng địa chỉ IPv4, lưu lượng Internet trao đổi trên IPv6, vv… và đích đến là số lượng người sử dụng IPv6. Trong thời gian qua, trước các nỗ lực triển khai rất tích cực của toàn

[4] RFC1752 - The Recommendation for the IP Next Generation Protocol
[5] RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
6 RFC 2461 - RFC 2461 - Neighbor Discovery for IP Version 6 (IPv6)
7 RFC 2463 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
8 RFC2373 - IP Version 6 Addressing Architecture
9 RFC2374 - An IPv6 Aggregatable Global Unicast Address Format
10 RFC3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
11 RFC3587 - IPv6 Global Unicast Address Format

thế giới, con số người sử dụng IPv6 vẫn đang rất khiêm tốn (chỉ chiếm khoảng gần 5% theo kết quả thống kê của Google tại thời điểm tháng 11/2014).



Hình 3: Sự tăng trưởng người sử dụng IPv6 trên thế giới tính đến tháng 11/2014 (nguồn Google)

Tại lab của mình, Cisco cũng đưa ra các kết quả đánh giá tổng hợp dựa trên những tiêu chí chi tiết về tình hình, kết quả triển khai IPv6 của từng quốc gia/vùng lãnh thổ trên thế giới (chi tiết tham khảo tại http://6lab.cisco.com/stats/index.php).

Quốc gia	Chỉ số phát triển chung	Tỉ lệ quảng bá IPv6	Tỉ lệ số hiệu mạng quảng bá IPv6	Tỉ lệ nội dung IPv6	Người sử dụng	Tổng điểm (trên 10)
Mỹ	28.16%	40.23%	59.97%	45.11%	6.83%	6.5
Pháp	30.14%	45.09%	73.74%	49.72%	4.9%	6.3
Nhật	27.79%	45.91%	81.37%	28.7%	3.44%	4.9
Trung Quốc	10.56%	13.24%	38.2%	2.5%	0.73%	1.4
Úc	20.92%	28.15%	68.18%	46.86%	0.57%	3.3

Campuchia	9.01%	25%	30.36%	51.48%	0.07%	1.4
Indonesia	16.1%	28.52%	51.5%	48.81%	0.38%	2.6
Malaysia	21.64%	30.97%	66.52%	53.78%	0.83%	3.7
Philippines	14.59%	23.88%	55.37%	50.38%	0.02%	1.8
Thái Lan	22.22%	43.04%	80.14%	49.84%	0,17%	3
Việt Nam	7.22%	21.43%	28.87%	35.04%	0%	0.8

Bảng 1: Đánh giá kết quả triển khai IPv6 theo một số tiêu chí cơ bản của Việt Nam trong tương quan so sánh với một số quốc gia hàng đầu và các quốc gia trong khu vực Đông Nam Á tại thời điểm tháng 3/2014 (nguồn http://6lab.cisco.com/stats/index.php)

1.2.3. Tình hình thúc đẩy và triển khai IPv6 tại Việt Nam

- Tháng 5/2008, Bộ trưởng Bộ Thông tin và Truyền thông ban hành Chỉ thị số 03/2008/CT-BTTTT về việc thúc đẩy sử dụng địa chỉ Internet thế hệ mới IPv6, trong đó xác định việc chuyển sang sử dụng thế hệ địa chỉ mới IPv6 thay thế cho IPv4 là một yêu cầu cấp thiết, vừa để nhằm đảm bảo cho sự phát triển liên tục của hoạt động Internet, vừa phát huy các lợi thế vượt trội về công nghệ mới của IPv6 so với IPv4. Để ghi nhớ ngày ra đời Chỉ thị 03/2008/CT-BTTTT, ngày 06/05 hàng năm được lựa chọn là ngày IPv6 Việt Nam.
- Tháng 01/2009, Bộ Thông tin và Truyền thông thành lập Ban Công tác thúc đẩy phát triển IPv6 quốc gia làm đầu mối thúc đẩy, giám sát các hoạt động triển khai IPv6 (các hoạt động của Ban Công tác, tình hình triển khai IPv6 của Việt Nam, cập nhật tình hình triển khai IPv6 thế giới, phổ biến về kiến thức về IPv6 cho cộng đồng có tại các Website WWW.IPv6.VN).
- Ngay trước thềm thời điểm Khu vực Châu Á - Thái Bình Dương hết IPv4, ngày 29/3/2011, Bộ Thông tin và Truyền thông đã ban hành Kế hoạch hành động quốc gia về IPv6. Đây là động thái mạnh và kịp thời, khẳng định quyết tâm và lộ trình triển khai thành công việc chuyển đổi sang IPv6 của Việt Nam. Kế hoạch hành động Quốc gia về IPv6 có mục tiêu chung là bảo đảm trước năm 2020 toàn bộ mạng lưới và dịch vụ Internet Việt Nam được chuyển đổi để hoạt động một cách an toàn, tin cậy với địa chỉ IPv6 (tương thích với công nghệ IPv6).

Lộ trình chuyển đổi từ IPv4 sang IPv6 cho Internet Việt Nam được chia thành ba giai đoạn sau đây:

Giai đoạn 1 (Từ 2011- đến 2012): Giai đoạn chuẩn bị

- Đánh giá thực trạng và tính sẵn sàng của mạng lưới Internet cho việc chuyển đổi sang IPv6;

- Hình thành mạng thử nghiệm IPv6 quốc gia phục vụ cho việc thử nghiệm công nghệ IPv6 tại Việt Nam;

- Tổ chức truyền thông và trang bị kiến thức, trao đổi kinh nghiệm và đào tạo nguồn nhân lực phục vụ cho việc chuyển đổi sang IPv6.

Giai đoạn 2 (Từ 2013- đến 2015): Giai đoạn khởi động

- Chuyển đổi mạng lưới từ IPv4 sang hỗ trợ đồng thời IPv4 và IPv6;

- Xây dựng và hình thành mạng cơ sở hạ tầng IPv6 quốc gia;

- Cung cấp dịch vụ IPv6 thử nghiệm tới người sử dụng.

Giai đoạn 3 (Từ 2016- đến 2019): Giai đoạn chuyển đổi

- Hoàn thiện mạng lưới và dịch vụ IPv6, đảm bảo hoạt động ổn định với địa chỉ IPv6;

- Các tổ chức, doanh nghiệp chính thức sử dụng và cung cấp dịch vụ trên nền tảng công nghệ IPv6.

Trên phương diện triển khai, ngày 06/5/2013, nhân sự kiện hội thảo kỷ niệm ngày IPv6 Việt Nam lần đầu, "lễ khai trương dịch vụ IPv6" đánh dấu sự hình thành chính thức mạng IPv6 Quốc gia và hàng loạt dịch vụ IPv6 đươc các nhà cung cấp dịch vụ công bố khai trương và sẵn sàng cung cấp cho khách hàng tại Việt Nam.

Để đánh giá sự triển khai trên thực tế đối với mạng lưới và các dịch vụ IPv6 sau lễ khai trương, cuối năm 2013, Thường trực Ban Công tác thúc đẩy IPv6 Quốc gia - Trung tâm Internet Việt Nam đã thực hiện cuộc khảo sát nhỏ với một số doanh nghiệp Internet tiêu biểu và thu được kết quả sau đây:

Tại NetNam:

- **Kết nối trong nước**: NetNam đã thực hiện kết nối IPv6 tới mạng IPv6 Quốc gia tại Hà Nội và TP HCM với dung lượng 2Gbps và băng thông trung bình giờ hành chính đạt 50kb.
- **Kết nối quốc tế**: NetNam có kết nối thuần IPv6 tới NTT Hồng Kông với dung lượng là 1Gbps và băng thông quốc tế trung bình trong giờ hành chính đạt 5Mb.
- **Hệ thống DNS**: Đã hỗ trợ IPv6
- **Dịch vụ truy cập**: NetNam sẵn sàng cung cấp dịch vụ truy cập Internet IPv6 nếu khách hàng có nhu cầu.
- **Dịch vụ nội dung**: Các trang web chính thức của NetNam như netnam.vn; go6.vn đã chạy IPv6. Nhiều website .vn hosting tại NetNam cũng đã tham gia lễ khai trương IPv6 tại Viêt Nam.
- **Các dịch vụ khác**: NetNam đã cung cấp dịch vụ tunnel broker thông qua trang web tunnelbroker.netnam.vn với tổng số hơn 20000 đường hầm đã được khởi tạo.

Tại Viettel:

- **Kết nối trong nước**: Có kết nối đến mạng IPv6 Quốc gia.
- **Kết nối quốc tế**: Đang duy trì kết nối IPv6 đến 9 đối tác quốc tế bao gồm HKIX, AKAMAI, HE, Google, Microsoft, Yahoo, vv…
- **Hệ thống DNS**: Đã nâng cấp phần mềm để hỗ trợ IPv6
- **Dịch vụ truy cập**: Viettel mới dừng ở việc cung cấp thử nghiệm các dịch vụ kết nối IPv6 một bộ phận nhỏ các thuê bao ADSL, Data 3G là 2 loại hình thuê bao có tốc độ phát triển nhanh và chiếm phần lớn nguồn tài nguyên IPv4 public của Viettel. Cụ thể: Viettel đã đưa vào thử nghiệm 1000 thuê bao ADSL chạy dualstack IPv4/IPv6, 1000 thuê bao USB 3G chạy IPv6 tại Hà Nội. Trong năm 2013, Viettel cũng thực hiện nâng cấp hệ thống thiết bị phân mạng truy nhập của các dịch vụ băng rộng có dây và dịch vụ 3G để hỗ trợ IPv6. Cụ thể, hoàn thành đầu tư mua sắm 13 BRAS mới hỗ trợ IPv6 cho thuê bao ADSL, FTTx và 4 GGSN hỗ trợ song song IPv6/IPv4
- **Dịch vụ nội dung**: Không có.

- **Các công tác khác:** Về công tác sản xuất thiết bị tương thích IPv6, Viettel tập trung vào nghiên cứu và sản xuất các dòng thiết bị đầu cuối cho dịch vụ ADSL như wifi router modem, EOC Slave và các phẩm thiết bị đầu cuối cho dịch vụ mobile data như điện thoại 3G và USB 3G.

Tại FPT Telecom:

- **Kết nối trong nước**: Có kết nối đến mạng IPv6 Quốc gia.
- **Kết nối quốc tế**: FPT Telecom hiện đang thiết lập và duy trì tổng cộng 10 kết nối IPv6 đến các đối tác cung cấp dịch vụ quốc tế như Tata, pccw, yahoo, google, vv….
- **Hệ thống DNS**: Đã hỗ trợ IPv6
- **Dịch vụ truy cập**: Hiện tại, toàn bộ hệ thống truyền tải mạng (router, switch) của FPT Telecom đã hoàn toàn triển khai xong việc chạy song song IPv4/IPv6 dual-stack và sẵn sàng đáp ứng cung cấp các dịch vụ IPv6 đến khách hàng có nhu cầu. FPT Telecom cũng đã chuẩn bị một lượng thiết bị đầu cuối phù hợp để có thể sẵn sàng triển khai cho khách hàng băng rộng, FTTX ngay khi có nhu cầu.
- **Dịch vụ nội dung**: Tuy chưa triển khai chính thức nhưng FPT đang nỗ lực chuyển đổi hỗ trợ IPv6 đối với các dịch vụ nội dung số do FPT Telecom làm chủ như website vnexpress.net và một số trò chơi trực tuyến.

Tại Công ty VTC Công nghệ và Truyền thông số:

- **Kết nối trong nước và quốc tế**: Đã triển khai kết nối BGP Dual stack cả trong nước (đến mạng IPv6 Quốc gia) và quốc tế.
- **Hệ thống DNS**: Đã hỗ trợ IPv6
- **Dịch vụ nội dung**:VTC đã triển khai mạng xã hội GO.VN chạy dual-stack, trở thành mạng xã hội đầu tiên ở Việt Nam chạy được trên nền tảng IPv6.
  Triển khai IPv6 cho các dịch vụ thương mại điện tử bao gồm cổng thanh toán điện tử trực tuyến http://paygate.vtv.vn, dịch vụ mua hàng trực tuyến http://ohay.vn; http://gmua.vn.
  Triển khai IPv6 cho các dịch vụ điện toán đám mây, bao gồm dịch vụ cho thuê máy chủ ảo http://vps.vtc.vn; dịch vụ cung cấp website cho khách hàng http://esites.vn.

Tại VNPT:

- **Kết nối trong nước**: VNPT đã triển khai kết nối dual-stack trên các kết nối với VNNIC tại Hà Nội và TP HCM.
- **Kết nối quốc tế**: Đã triển khai kết nối dual-stack trên một số hướng kết nối quốc tế với SingTel, NTT,… hiện nay vẫn đang tiếp tục triển khai với các đối tác quốc tế khác.
- **Hệ thống DNS**: Đã hỗ trợ IPv6
- **Dịch vụ truy cập**: Chưa có kế hoạch triển khai.
- **Dịch vụ nội dung**: website vnpt.com.vn và trang web mic.gov.vn của Bộ Thông tin Truyền thông hosting tại VDC đã hỗ trợ IPv6.
- **Các dịch vụ khác**: Tháng 10/2013, VNPT đã triển khai IPv6 trên mạng lưới thực tế trên quy mô nhỏ để đánh giá hiệu năng thiết bị và các tính năng khác như: xác thực, tính cước.

Về phía mạng IPv6 Quốc gia:

Nhân lễ khai trương Internet Việt Nam ngày 6/5/2013, mạng IPv6 quốc gia được hình thành trên cơ sở kết nối song song IPv4/IPv6 hệ thống mạng DNS quốc gia, trạm trung chuyển Internet quốc gia VNIX, mạng Internet của các ISP.

Bên cạnh đó, VNNIC vẫn tiếp tục duy trì mạng Promote IPv6 như một hệ thống thành phần của mạng IPv6 quốc gia cung cấp cho cộng đồng và các thành viên kết nối các dịch vụ cơ bản trên nền IPv6 nhằm khuyến khích, thúc đẩy việc ứng dụng địa chỉ IPv6 tại Việt Nam: DNS, Web, Email, VOIP, Tunnel ...

Hiện tại mạng IPv6 quốc gia đang được duy trì với 10 ISP đã kết nối tới hệ thống VNIX trong nước và hàng chục hướng kết nối đi quốc tế. Về hệ thống DNS Quốc gia, trong năm 2013 thống kê được tỉ lệ truy vấn bản ghi IPv6 trên hệ thống DNS Quốc gia là 17.6% tăng 4,2% so với năm 2012.

Cũng theo thống kê tại hệ thống lab của APNIC (labs.apnic.net), tổng băng thông IPv6 quốc tế của Việt Nam năm 2013 có tăng so với năm 2012 nhưng không đáng kể. Tuy nhiên băng thông IPv6 trong nước qua mạng IPv6 quốc gia (hệ thống VNIX) còn thấp chứng tỏ vẫn chưa có lưu lượng IPv6 trao đổi giữa các ISP trong nước thể hiện phần nội dung về IPv6 trong nước vẫn chưa phát triển.

Hỏi – đáp cuối chương 1:

1. Tên gọi của giao thức Internet mới đã được quyết định thúc đẩy sử dụng thay thế cho phiên bản hiện thời của giao thức Internet là gì?

T: Giao thức Internet mới là thủ tục Internet phiên bản 6 (Internet Protocol Version 6 -IPv6)

2. Giao thức IPv6 được kỳ vọng mang lại những đặc điểm mới nào cho hoạt động Internet toàn cầu ?

T: Thế hệ địa chỉ IPv6 được đưa ra nhằm đảm bảo hoạt động của mạng Internet toàn cầu khi không gian địa chỉ IPv4 có nguy cơ cạn kiệt. IPv6 được thiết kế khắc phục những hạn chế vốn có của địa chỉ IPv4 như không gian địa chỉ hạn chế (địa chỉ IPv4 chỉ có độ dài 32 bít) dẫn tới việc sử dụng công nghệ NAT, hạn chế trong cấu trúc định tuyến, bảo mật đầu cuối – đầu cuối tầng IP, đồng thời đem lại những đặc tính mới thỏa mãn các nhu cầu dịch vụ của thế hệ mạng mới như khả năng tự động cấu hình mà không cần hỗ trợ của máy chủ DHCP, cấu trúc định tuyến tốt hơn, hỗ trợ tốt hơn multicast, hỗ trợ bảo mật tốt hơn, hỗ trợ tốt hơn cho di động.

3. Theo kế hoạch đã định thời điểm nào Internet Việt Nam sẽ bắt đầu và hoàn tất chuyển đổi sang IPv6 ?

T : 2016, 2020

CHƯƠNG 2: CẤU TRÚC, CÁCH THỨC BIỂU DIỄN VÀ CÁC DẠNG ĐỊA CHỈ IPV6

Cấu trúc đánh địa chỉ là nơi có thể quan sát rất rõ những khác biệt giữa IPv4 và IPv6. Địa chỉ IPv6 được thiết kế có chiều dài 128 bít, gấp 4 lần chiều dài của địa chỉ IPv4. Cấu trúc cũng như mô hình địa chỉ có những thay đổi lớn so với phiên bản IPv4. Phần nội dung này xin giới thiệu với bạn đọc về các dạng địa chỉ, cấu trúc đánh địa chỉ IPv6.

Chương 2 bao gồm những mục chính sau đây :

- Cách thức biểu diễn và cấu trúc địa chỉ IPv6
- Cấu trúc đánh địa chỉ. Các dạng địa chỉ IPv6.
- Tóm tắt về địa chỉ IPv6.

2.1 CÁCH THỨC BIỂU DIỄN VÀ CẤU TRÚC ĐỊA CHỈ IPV6

2.1.1 Tổng quan về địa chỉ IPv6, khác biệt so với IPv4

Địa chỉ IPv6 có chiều dài gấp 4 lần chiều dài địa chỉ IPv4, gồm 128 bít. Trong việc đánh số thiết bị bằng địa chỉ IPv6, so với địa chỉ IPv4 có hai điểm khác biệt cơ bản sau:

- ***Địa chỉ IPv6 có nhiều loại***

Không gian địa chỉ IPv6 phân thành nhiều loại địa chỉ khác nhau. Mỗi loại địa chỉ có chức năng nhất định trong phục vụ giao tiếp. Có loại chỉ sử dụng trong giao tiếp nội bộ trên một đường kết nối. Có loại sử dụng trong giao tiếp toàn cầu tương đương như địa chỉ IPv4 hiện nay. Có loại khi host sử dụng chỉ giao tiếp với một host khác duy nhất. Có loại khi host sử dụng sẽ giao tiếp đồng thời với nhiều host khác.

Kết quả là :

- Để một thiết bị IPv6 hoạt động bình thường, nó phải được gắn đồng thời nhiều loại địa chỉ khác nhau.
- Trong cấu trúc địa chỉ IPv6 cần có một cách thức nào đó để nhận dạng các loại địa chỉ IPv6.

- ***Địa chỉ IPv6 được gắn cho giao diện (interface). Một giao diện có thể đồng thời gắn nhiều địa chỉ.***

Nếu đặt câu hỏi: chúng ta gắn bao nhiêu địa chỉ cho một node trên mạng IPv4 Internet. Có thể nhận được câu trả lời như sau: một máy tính IPv4 với một card mạng chỉ được gắn một địa chỉ IPv4 và xác định trên mạng Internet bằng địa chỉ này. Như vậy đồng nghĩa với địa chỉ IPv4 được gắn cho các node. Chỉ có router IPv4 được gắn trên mỗi giao diện (tương đương một card mạng) một địa chỉ IPv4 vì router có trách nhiệm làm cầu nối liên lạc giữa các mạng khác nhau.

Thế hệ địa chỉ IPv6 có những thay đổi cơ bản về mô hình địa chỉ. Địa chỉ IPv6 được gắn cho các giao diện, không phải gắn cho các node, bởi vì một giao diện có thể gắn đồng thời nhiều địa chỉ, cùng loại hoặc khác loại. Mỗi địa chỉ khi được gắn cho một giao diện sẽ có thời gian sống hợp lệ tương ứng. Node IPv6 dù chỉ có một card mạng cũng sẽ có nhiều giao diện. Đây có thể là giao diện vật lý, hoặc là các giao diện ảo dành cho công nghệ đường hầm (tunnel)[12].

2.1.2 Biểu diễn địa chỉ IPv6

Người ta không biểu diễn địa chỉ IPv6 dưới dạng số thập phân. Địa chỉ IPv6 được viết hoặc theo 128 bít nhị phân, hoặc thành một dãy chữ số hexa decimal. Tuy nhiên, nếu viết một dãy số 128 bít nhị phân quả là không thuận tiện, và để nhớ chúng thì không thể. Do vậy, địa chỉ IPv6 được biểu diễn dưới dạng một dãy chữ số hexa.

Để biểu diễn 128 bít nhị phân IPv6 thành dãy chữ số hexa decimal, người ta chia 128 bít này thành các nhóm 4 bít, chuyển đổi từng nhóm 4 bít thành số hexa tương ứng và nhóm 4 số hexa thành một nhóm phân cách bởi dấu ":". Kết quả, một địa chỉ IPv6 được biểu diễn thành một dãy số gồm 8 nhóm số hexa cách nhau bằng dấu ":", mỗi nhóm gồm 4 chữ số hexa.

[12] Công nghệ đường hầm (tunnel) được mô tả trong chương 4 của tài liệu

Địa chỉ IPV6: 128 bit

0010 0000 …00… 1100 1011 1010 0010 0011 1001 1011 0111

↓

32 cụm 4 bit = 32 chữ số hexa = 8 cụm 4 chữ số hexa

↓

2000:0000:0000:0000:0000:0000:CBA2:39B7

2.1.2.1 Rút gọn cách viết địa chỉ IPv6

Dãy 32 chữ số hexa của một địa chỉ IPv6 có thể có rất nhiều chữ số 0 đi liền nhau. Nếu viết toàn bộ và đầy đủ những con số này thì dãy số biểu diễn địa chỉ IPv6 thường rất dài. Do vậy, có thể rút gọn cách viết địa chỉ IPv6 theo hai quy tắc sau đây:

Quy tắc 1: Trong một nhóm 4 số hexa, có thể bỏ bớt những số 0 bên trái. Ví dụ cụm số "0000" có thể viết thành "0", cụm số "09C0" có thể viết thành "9C0"

Quy tắc 2: Trong cả địa chỉ IPv6, một số nhóm liền nhau chứa toàn số 0 có thể không viết và chỉ viết thành "::". Tuy nhiên, chỉ được thay thế một lần như vậy trong toàn bộ một địa chỉ IPv6. Điều này rất dễ hiểu. Nếu chúng ta thực hiện thay thế hai hay nhiều lần các nhóm số 0 bằng "::", chúng ta sẽ không thể biết được số các số 0 trong một cụm "::" để từ đó khôi phục lại chính xác địa chỉ IPv6 ban đầu.

Ví dụ về biểu diễn và rút gọn địa chỉ IPv6:

Trong ví dụ trên, địa chỉ "2031:0000:130F:0000:0000:09C0:876A:130B" áp dụng quy tắc thu gọn thứ nhất có thể viết lại thành "2031:0:130F:0:0:9C0:876A:130B". Áp dụng quy tắc rút gọn thứ hai có thể viết lại thành "2031:0:130F::9C0:876A:130B".

Địa chỉ IPv6 còn được biểu diễn theo cách thức liên hệ với địa chỉ IPv4. 32 bít cuối của địa chỉ IPv6 tương ứng địa chỉ IPv4 được biết theo cách viết thông thường của địa chỉ IPv4, như trong ví dụ trên.

2.1.2.2 Biểu diễn một dải địa chỉ IPv6

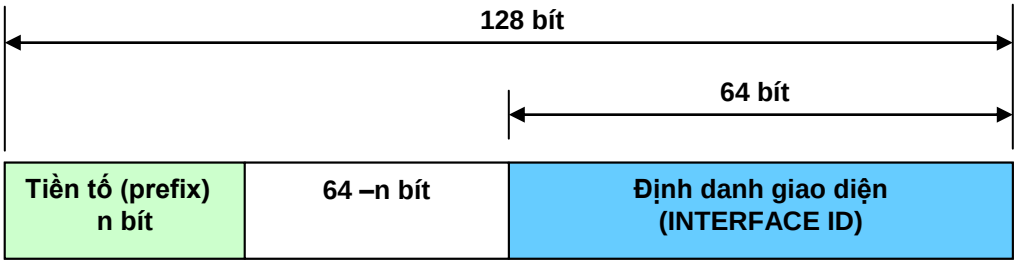
Tương tự như IPv4, một dải địa chỉ IPv6 được viết dưới dạng một địa chỉ IPv6 đi kèm với số bít xác định số bít phần mạng (bít tiền tố), như sau: *Địa chỉ IPv6/số bít mạng*

Ví dụ:

- Vùng địa chỉ FF::/8 tương ứng với dải địa chỉ bắt đầu từ FF00:0:0:0:0:0:0:0 đến FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
- Vùng địa chỉ 2001:DC8:0:0::/64 tương ứng với dải địa chỉ bắt đầu từ 2001:0DC8:0:0:0:0:0:0 đến 2001:0DC8:0:0:FFFF:FFFF:FFFF:FFFF

2.1.3 Cấu trúc của một địa chỉ IPv6

Cấu trúc chung của một địa chỉ IPv6 thường thấy như sau (một số dạng địa chỉ IPv6 không tuân theo cấu trúc này):



Hình 4: Cấu trúc thường thấy của một địa chỉ IPv6

Trong 128 bít địa chỉ IPv6, có một số bít thực hiện chức năng xác định. Đây là điểm khác biệt so với địa chỉ IPv4:

- ***Bít xác định loại địa chỉ IPv6 (bít tiền tố - prefix):***

Như đã đề cập, địa chỉ IPv6 có nhiều loại khác nhau. Mỗi loại địa chỉ có chức năng nhất định trong phục vụ giao tiếp. Để phân loại địa chỉ, một số bít đầu trong địa chỉ IPv6 được dành riêng để xác định dạng địa chỉ, được gọi là các bít tiền tố (prefix). Các bít tiền tố này sẽ quyết định địa chỉ thuộc loại nào và số lượng địa chỉ đó trong không gian chung IPv6.

Ví dụ: 8 bít tiền tố "1111 1111" tức "FF" xác định dạng địa chỉ multicast. Địa chỉ multicast chiếm 1/256 không gian địa chỉ IPv6. Ba bít tiền tố "001" xác định dạng địa chỉ unicast định danh toàn cầu, tương đương với địa chỉ IPv4 chúng ta vẫn thường sử dụng hiện nay.

- ***Các bít định danh giao diện (interface ID):***

Ngoại trừ dạng địa chỉ multicast và một số dạng địa chỉ cho mục đích đặc biệt, địa chỉ IPv6 sử dụng trong giao tiếp toàn cầu, cũng như link-local (là địa chỉ dùng trong giao tiếp giữa các IPv6 node trên một đường kết nối), site-local (địa chỉ được thiết kế cho giao tiếp trong phạm vi một site) đều có 64 bít cuối cùng được sử dụng để xác định một giao diện duy nhất trên một đường kết nối (tương đương với một mạng con "subnet").

Như vậy, một phân mạng con nhỏ nhất của địa chỉ IPv6 sẽ có kích thước /64.

2.1.4 Định danh giao diện (interface identifier) trong địa chỉ IPv6

Định danh giao diện là 64 bít cuối cùng trong một địa chỉ IPv6. Số định danh này sẽ xác định một giao diện trong phạm vi một mạng con (subnet). Định danh giao diện phải là số duy nhất trong phạm vi một subnet. 64 bít định danh này có thể được cấu thành tự động theo một trong những cách thức sau đây:

- Ánh xạ từ dạng thức địa chỉ EUI-64 của giao diện.
- Tự động tạo một cách ngẫu nhiên
- Gắn giao diện bằng thủ tục gắn địa chỉ DHCPv6 .

2.1.4.1 Tự động tạo 64 bít định danh giao diện từ địa chỉ MAC của card mạng

Hiện nay, card mạng được định danh duy nhất toàn cầu theo cách thức định danh EUI-48 và EUI-64. Địa chỉ đánh theo cách thức này xác định duy nhất một card mạng trên toàn cầu, được gọi là địa chỉ MAC.

Dạng thức EUI-48:

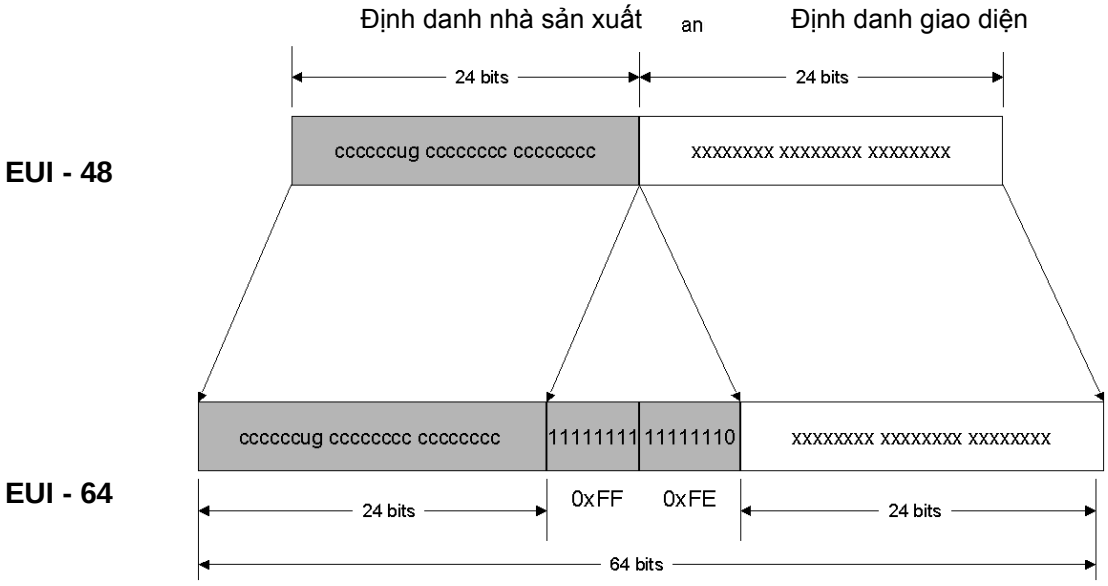
Dạng thức đánh địa chỉ EUI-48 dùng 48 bít. Trong đó, 24 bít đầu sử dụng để định danh nhà sản xuất thiết bị và 24 bít sau là phần mở rộng, để định danh card mạng. Việc kết hợp một số định danh 24 bít duy nhất của một nhà sản xuất card mạng, và một số định danh 24 bít duy nhất của card nhà sản xuất đó cung cấp ra thị trường, sẽ tạo nên một con số 48 bít, xác định một card mạng duy nhất trên toàn cầu, được gọi là địa chỉ MAC (hay còn gọi địa chỉ vật lý, địa chỉ Ethernet), viết dưới dạng hexa decimal.

Dạng thức EUI-64:

Nhằm tạo nên một không gian định danh thiết bị lớn hơn cho các nhà sản xuất, IEEE đưa ra một phương thức đánh số mới cho các giao diện mạng gọi là EUI-64, trong đó giữ nguyên 24 bít định danh nhà sản xuất thiết bị và phần mở rộng tăng lên thành 40 bít. Nếu giao diện mạng được định danh theo dạng thức này, địa chỉ phần cứng của nó sẽ gồm 64 bít.

Ánh xạ từ EUI-48 sang EUI-64:

Dạng thức định danh EUI-48 được ánh xạ thành EUI-64 bằng cách thêm 16 bít có giá trị 11111111 11111110 (viết dưới dạng hexa sẽ là OxFFFE) vào giữa 48 bít của EUI-48 .



Hình 5: Ánh xạ từ EUI-48 tới EUI-64

Cấu thành 64 bít định danh giao diện IPv6 từ địa chỉ MAC:

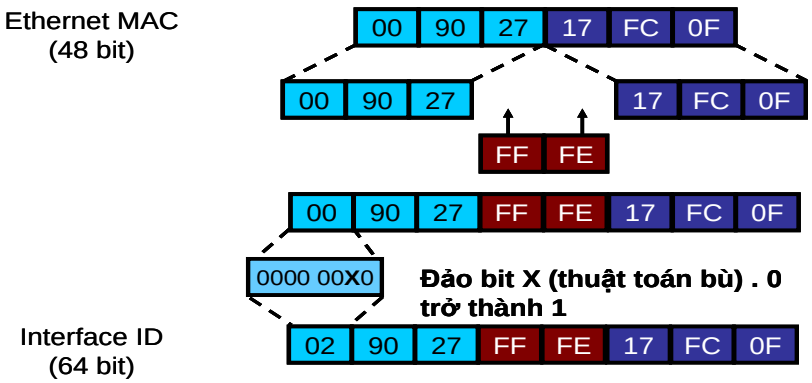
64 bít định danh giao diện trong địa chỉ IPv6 được tự động tạo nên từ 64 bít định danh dạng EUI-64 của giao diện mạng theo quy tắc như sau:

Trong số 24 bít xác định nhà cung cấp thiết bị, có một bít được quy định là bít U (xxxx xxUx xxxx xxxx xxxx xxxx). Thông thường bít này có giá trị 0. Người ta tiến hành đảo bít bít U này (từ 0 thành 1 và từ 1 thành 0), và lấy 64 bít sau khi thực hiện như vậy làm 64 bít định danh giao diện trong địa chỉ IPv6.

Ví dụ :

Tạo 64 bít định danh giao diện của địa chỉ IPv6 từ địa chỉ MAC 00-90-27-17-FC-0F :

1. Tách địa chỉ MAC 48 bít EUI-48 (00-90-27-17-FC-0F) làm 2 phần, thêm vào 16 bít FFFE để trở thành dạng thức EUI-64 (00-90-27-FF-FE-17-FC-0F)
2. Tiến hành đảo bít U của dạng thức EUI-64 trên, sẽ thu được 64 bít định danh giao diện: 02-90-27-FF-FE-17-FC-0F



Hình 6: Tự động cấu hình 64 bít định danh giao diện từ địa chỉ MAC

2.1.4.2 Tự động tạo 64 bít định danh giao diện một cách ngẫu nhiên

Khi sử dụng phương thức dialup để kết nối vào Internet qua mạng của một nhà cung cấp dịch vụ, mỗi lần kết nối, người sử dụng sẽ nhận được một địa chỉ IPv4 khác nhau. Nếu căn cứ vào địa chỉ IP, việc tìm kiếm lưu lượng của một người sử dụng dialup thường khó khăn.

Trong địa chỉ IPv6, 64 bít định danh giao diện có thể tự động tạo nên từ địa chỉ card mạng. Nếu 64 bít định danh giao diện luôn luôn được tạo nên từ địa chỉ card mạng, hoàn toàn có thể truy cứu được lưu lượng của một node nhất định, từ đó xác định được người sử dụng và việc sử dụng Internet. Để đảm bảo vấn đề về quyền riêng tư, IETF đưa ra một cách thức khác (mô tả trong RFC3041)[13] để tạo 64 bít định danh giao diện, trên nguyên tắc sử dụng thuật toán gắn một số ngẫu nhiên làm 64 bít định danh giao diện. Định danh đó là tạm thời và sẽ thay đổi theo thời gian.

13 RFC3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6

2.2 CÁC DẠNG ĐỊA CHỈ IPV6

2.2.1 Tổng quan về phân loại địa chỉ IPv6

Theo cách thức gói tin được gửi tới đích, trong địa chỉ IPv4, tồn tại khái niệm ba loại địa chỉ:

- *Broadcast:* Địa chỉ broadcast được node sử dụng để gửi một gói tin tới đồng thời toàn bộ các node IPv4 trong một mạng. Trong vùng địa chỉ của một mạng, địa chỉ với các bít xác định host toàn 1 sẽ được sử dụng làm địa chỉ broadcast. Ví dụ trong mạng 203.119.9.0/27, địa chỉ broadcast sẽ là 203.119.9.31
- *Unicast:* Địa chỉ unicast IPv4 chính là dạng địa chỉ chúng ta gắn cho thiết bị mạng để kết nối vào mạng Internet. Địa chỉ này xác định duy nhất một IPv4 node trên mạng Internet toàn cầu. Gói tin gửi đến địa chỉ đích unicast sẽ chỉ đến duy nhất một node IPv4.
- *Multicast:* Khi thiết kế IPv4, IETF dành riêng vùng địa chỉ lớp D (từ 224.0.0.0 đến 239.255.255.255) sử dụng cho một công nghệ truyền tải gói tin gọi là multicast. Công nghệ multicast cho phép gửi một gói tin IP đồng thời tới một nhóm xác định các thiết bị mạng. Các thiết bị mạng này có thể thuộc nhiều tổ chức và định vị ở các vị trí địa lý khác nhau.

Địa chỉ IPv6 không còn duy trì khái niệm broadcast. Theo cách thức gói tin được gửi đến đích, IPv6 bao gồm ba loại địa chỉ sau:

- ***Unicast:*** Địa chỉ unicast xác định một giao diện duy nhất. Trong mô hình định tuyến, các gói tin có địa chỉ đích là địa chỉ unicast chỉ được gửi tới một giao diện duy nhất. Địa chỉ unicast được sử dụng trong giao tiếp một – một
- ***Multicast:*** Địa chỉ multicast định danh một nhóm nhiều giao diện. Gói tin có địa chỉ đích là địa chỉ multicast sẽ được gửi tới tất cả các giao diện trong nhóm được gắn địa chỉ đó. Địa chỉ multicast được sử dụng trong giao tiếp một – nhiều.

  Trong địa chỉ IPv6 không còn tồn tại khái niệm địa chỉ broadcast. Mọi chức năng của địa chỉ broadcast trong IPv4 được đảm nhiệm thay thế bởi địa chỉ IPv6 multicast. Ví dụ chức năng broadcast trong một mạng của địa chỉ IPv4 được đảm nhiệm bằng một loại địa chỉ multicast IPv6 có tên gọi địa chỉ multicast mọi node phạm vi link (FF02::1)
- ***Anycast:*** Anycast là khái niệm mới của địa chỉ IPv6. Địa chỉ anycast cũng xác định tập hợp nhiều giao diện. Tuy nhiên, trong mô hình định tuyến, gói tin có địa chỉ đích anycast chỉ được gửi tới một giao diện duy nhất trong tập hợp. Giao diện đó là giao diện "gần nhất" theo khái niệm của thủ tục định tuyến.

Như đã trình bày, không gian IPv6 được phân chia thành rất nhiều dạng địa chỉ. Mỗi dạng địa chỉ có chức năng nhất định trong phục vụ giao tiếp. Có dạng chỉ sử dụng trong giao tiếp nội bộ trên một đường kết nối, có dạng sử dụng trong kết nối toàn cầu. Do vậy, địa chỉ IPv6 unicast và IPv6 multicast lại bao gồm nhiều dạng địa chỉ khác nhau. Các dạng địa chỉ này có phạm vi hoạt động nhất định.

2.2.2 Những dạng địa chỉ thuộc loại UNICAST

Địa chỉ unicast bao gồm năm dạng sau đây:

1) *Địa chỉ đặc biệt*
2) *Địa chỉ Link-local*
3) *Địa chỉ Site-local*
4) *Địa chỉ định danh toàn cầu (Global unicast address)*
5) *Địa chỉ tương thích (Compatibility address)*

2.2.2.1 Địa chỉ đặc biệt

IPv6 sử dụng hai địa chỉ đặc biệt sau đây trong giao tiếp:

- **0:0:0:0:0:0:0:0** hay còn được viết **"::"** là loại địa chỉ "không định danh" được IPv6 node sử dụng để thể hiện rằng hiện tại nó không có địa chỉ. Địa chỉ "::" được sử dụng làm địa chỉ nguồn cho các gói tin trong quy trình hoạt động của một IPv6 node khi tiến hành kiểm tra xem có một node nào khác trên cùng đường kết nối đã sử dụng địa chỉ IPv6 mà nó đang dự định dùng hay chưa. Địa chỉ này không bao giờ được gắn cho một giao diện hoặc được sử dụng làm địa chỉ đích.
- **0:0:0:0:0:0:0:1** hay **"::1"** được sử dụng làm địa chỉ xác định giao diện loopback, cho phép một node gửi gói tin cho chính nó, tương đương với địa chỉ 127.0.0.1 của IPv4. Các gói tin có địa chỉ đích ::1 không bao giờ được gửi trên đường kết nối hay chuyển tiếp đi bởi router. Phạm vi của dạng địa chỉ này là phạm vi node

2.2.2.2 Địa chỉ link-local

Khái niệm node lân cận (neighbor node) trong hoạt động của địa chỉ IPv6:

Trong IPv6, các node trên cùng một đường link coi nhau là các node lân cận (neighbor node). Trong mô hình hoạt động của IPv6, giao tiếp giữa các node lân cận trên một đường kết nối là vô cùng quan trọng. IPv6 đã phát triển một thủ tục mới, tên gọi Neighbor Discovery (ND) là một thủ tục thiết yếu, phục vụ giao tiếp giữa các neighbor node. Địa chỉ link-local cần thiết cho các quy trình mà thủ tục Neighbor Discovery phụ trách.

Địa chỉ link-local:

Link-local là loại địa chỉ phục vụ cho giao tiếp nội bộ, giữa các IPv6 node trên cùng một đường kết nối. IPv6 được thiết kế với tính năng "plug-and-play", tức khả năng cho phép IPv6 host tự động cấu hình địa chỉ, các tham số phục vụ giao tiếp bắt đầu từ chưa có thông tin cấu hình nào. Tính năng đó có được là nhờ IPv6 node luôn luôn có khả năng tự động cấu hình nên một dạng địa chỉ sử dụng giao tiếp nội bộ. Đó chính là địa chỉ link-local.

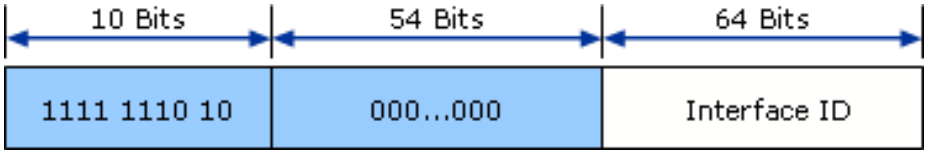
Địa chỉ link-local luôn được node IPv6 cấu hình một cách tự động, khi bắt đầu hoạt động, ngay cả khi không có sự tồn tại của mọi loại địa chỉ unicast khác . Địa chỉ này có phạm vi trên một đường link, phục vụ cho giao tiếp giữa các node lân cận. Sở dĩ IPv6 node có thể tự động cấu hình địa chỉ link-local là do IPv6 node có thể tự động cấu hình 64 bít định danh giao diện[14]. Địa chỉ link-local được tạo nên từ 64 bít định danh giao diện Iinterface ID) và một tiền tố (prefix) quy định sẵn cho địa chỉ link-local là FE80::/10.

Cấu trúc địa chỉ link-local

[14] Tham khảo mục 2.1.4 về định danh giao diện trong địa chỉ IPv6

Khi không có router, các node IPv6 trên một đường link sẽ sử dụng địa chỉ link-local để giao tiếp với nhau. Phạm vi của dạng địa chỉ unicast này là trên một đường kết nối (phạm vi link).

Cấu trúc của địa chỉ link-local như sau.



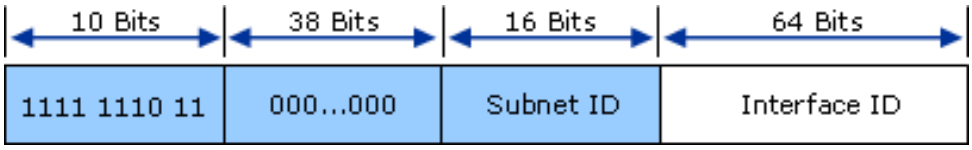
Hình 7: Cấu trúc địa chỉ link-local

Địa chỉ link-local bắt đầu bởi 10 bít tiền tố FE80::/10, theo sau bởi 54 bit 0. 64 bít còn lại là định danh giao diện (Interface ID).

2.2.2.3 Địa chỉ site-local

Trong thời kỳ ban đầu của IPv6, dạng địa chỉ IPv6 Site-local được thiết kế với mục đích sử dụng trong phạm vi một mạng, tương đương với địa chỉ dùng riêng (private) của IPv4. Phạm vi tính duy nhất của dạng địa chỉ này là phạm vi trong một mạng dùng riêng (ví dụ một mạng office, một tổ hợp mạng office của một tổ chức...). Các router biên IPv6 không chuyển tiếp gói tin có địa chỉ site-local ra khỏi phạm vi mạng riêng của tổ chức. Do vậy, một vùng địa chỉ site-local có thể được dùng trùng lặp bởi nhiều tổ chức mà không gây xung đột định tuyến IPv6 toàn cầu. Địa chỉ site-local trong một mạng dùng riêng không thể được truy cập tới từ một site khác.

Địa chỉ Site-local có tiền tố FEC0::/10 và có cấu trúc như sau:



Hình 8: Cấu trúc địa chỉ Site-local

Địa chỉ site-local bắt đầu bằng 10 bít prefix FEC0::/10. Tiếp theo là 38 bít 0 và 16 bít mà tổ chức có thể phân chia subnet, định tuyến trong phạm vi site của mình. 64 bít cuối là 64 bít định danh giao diện cụ thể trong một subnet.

Địa chỉ Site-local được định nghĩa trong thời kỳ đầu phát triển IPv6. Trong quá trình sử dụng IPv6, người ta nhận thấy nhu cầu sử dụng địa chỉ dạng site-local trong tương lai phát triển của thế hệ địa chỉ IPv6 là không thực tế và không cần thiết. ***Do vậy, IETF đã sửa đổi RFC3513, loại bỏ đi dạng địa chỉ site-local***.

Tại đây, chúng ta đề cập đến địa chỉ Site-local với mục đích tìm hiểu, biết được trong quá trình phát triển IPv6, đã từng có dạng địa chỉ này.

2.2.2.4 Địa chỉ unicast định danh toàn cầu (Global unicast address)

Đây là dạng địa chỉ tương đương với địa chỉ IPv4 public hiện nay sử dụng cho mạng Internet toàn cầu. Tính duy nhất của dạng địa chỉ này được đảm bảo trong phạm vi toàn cầu. Chúng được định tuyến và có thể liên kết tới trên

phạm vi toàn bộ mạng Internet. Việc phân bổ và cấp phát dạng địa chỉ này do hệ thống các tổ chức quản lý địa chỉ quốc tế đảm nhiệm.

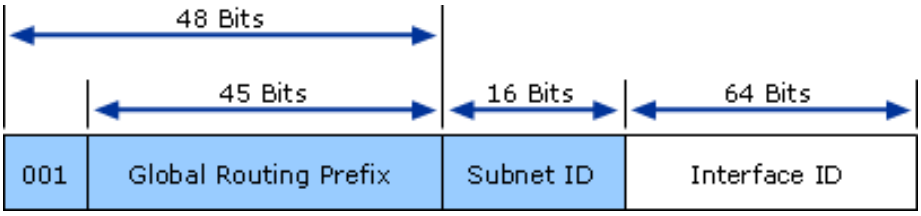
Địa chỉ unicast toàn cầu có tiền tố prefix bao gồm ba bít 001::/3. Phạm vi tính duy nhất của địa chỉ unicast định danh toàn cầu là toàn bộ mạng Internet IPv6.

Như chúng ta đã biết, node IPv6 ngay từ khi khởi tạo đã có khả năng giao tiếp, do luôn có khả năng tự động tạo nên dạng địa chỉ link-local. Tuy nhiên với địa chỉ này, node chỉ có thể thực hiện giao tiếp trong phạm vi một đường kết nối. Để có giao tiếp toàn cầu, IPv6 node cần được gán ít nhất một địa chỉ unicast định danh toàn cầu. Cũng như IPv4, địa chỉ này có thể được cấu hình bằng tay cho node. Tuy nhiên, giao thức IPv6 được thiết kế với đặc tính hỗ trợ IPv6 node khả năng tìm kiếm và tự động gắn địa chỉ unicast định danh toàn cầu, qua những giao tiếp nội bộ sử dụng địa chỉ link-local[15]

Không như địa chỉ IPv4, với cấu trúc định tuyến vừa phân cấp, vừa không phân cấp, địa chỉ Internet IPv6 được cải tiến trong thiết kế để đảm bảo có một cấu trúc định tuyến và đánh địa chỉ phân cấp rõ ràng.

Ba mục tiêu quan trọng nhất trong quản lý địa chỉ IPv4 là "sử dụng hiệu quả, tiết kiệm", "tính tổ hợp" và "tính có đăng ký". Tuy nhiên, đối với địa chỉ IPv6, mục tiêu đầu tiên được đặt lên hàng đầu là "tính tổ hợp". Điều này rất dễ hiểu. Với chiều dài 128 bit, không gian địa chỉ vô cùng rộng lớn. Nếu địa chỉ IPv6 không được tổ hợp thật tốt, có cấu trúc định tuyến phân cấp rõ ràng hiệu quả thì không thể xử lý được một khối lượng thông tin khổng lồ đặt lên bảng thông tin định tuyến toàn cầu.

2.2.2.4.1 Cấu trúc địa chỉ Unicast toàn cầu



Hình 9: Cấu trúc địa chỉ Unicast toàn cầu

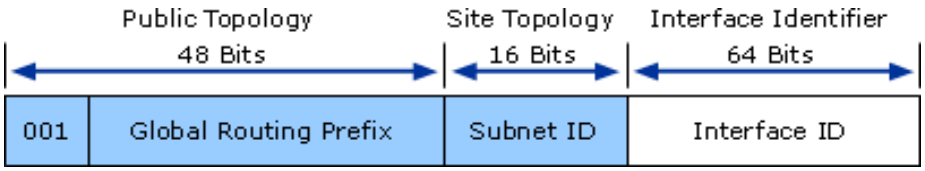
Địa chỉ unicast định danh toàn cầu được bắt đầu với 3 bít tiền tố 001.

Theo cách thức biểu diễn dạng số hexa, hiện nay hoạt động liên kết mạng IPv6 toàn cầu đang sử dụng địa chỉ thuộc vùng 2000::/3 (bắt đầu từ 2000:0:0:0:0:0:0:0 đến 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF), do hệ thống tổ chức quản lý địa chỉ IP quốc tế cấp phát, phân bổ lại cho hoạt động Internet toàn cầu. Nếu một địa chỉ IPv6, được bắt đầu bởi 2000::/3, chúng ta biết đó là vùng địa chỉ định tuyến toàn cầu.

Trong thời gian đầu tiên sử dụng địa chỉ IPv6, IANA cấp phát trong vùng 2001::/16 cho hoạt động Internet IPv6. Tới thời điểm hiện nay, nhu cầu sử dụng IPv6 gia tăng, các vùng địa chỉ khác bắt đầu được cấp phát, như 2400::/16.

[15] Tham khảo mục 3.1.5 về quy trình tự động tạo địa chỉ toàn cầu của thiết bị IPv6

2.2.2.4.2 Phân cấp định tuyến địa chỉ IPv6 Unicast toàn cầu



Hình 10: Phân cấp định tuyến địa chỉ IPv6 Unicast toàn cầu

Theo RFC3587[16] mô tả dạng thức địa chỉ IPv6 Unicast toàn cầu, địa chỉ IPv6 định danh toàn cầu được phân cấp định tuyến như sau:

- *Phần cố định:* 3 bít đầu tiên 001 xác định dạng địa chỉ unicast định danh toàn cầu.
- *Phần định tuyến toàn cầu*: 45 bit tiếp theo. Các tổ chức quản lý sẽ phân cấp quản lý vùng địa chỉ này, chuyển giao lại cho các tổ chức khác. Kích thước vùng địa chỉ nhỏ nhất quảng bá ra ngoài phạm vi một mạng của một tổ chức thông thường theo cấu trúc này là /48.

  Theo chính sách quản lý địa chỉ hiện tại, kích thước vùng địa chỉ nhỏ nhất được phân bổ cho một ISP là /32 và kích thước vùng địa chỉ thông thường cấp cho mạng của người sử dụng cuối cùng là /48. Tuy nhiên đây không phải những con số cố định. Chính sách quản lý địa chỉ toàn cầu luôn được thay đổi và xem xét để phù hợp nhất với nhu cầu và hoạt động mạng.
- *Vùng định tuyến trong site:* 16 bít tiếp theo là không gian địa chỉ mà tổ chức có thể tự mình quản lý, phân bổ, cấp phát và tổ chức định tuyến bên trong mạng của mình. Với một vùng địa chỉ /48, tổ chức có thể tạo nên 65,536 subnet cỡ /64 hoặc nhiều cấp định tuyến phân cấp hiệu quả sử dụng trong mạng của tổ chức.

2.2.2.5 Địa chỉ tương thích (Compatibility address)

Địa chỉ IPv6 phát triển khi mạng Internet là một thế giới kết nối IPv4. Cần có những công nghệ phục vụ cho việc chuyển đổi từ địa chỉ IPv4 sang địa chỉ IPv6, cũng như những cách thức cho phép lợi dụng cơ sở hạ tầng mạng Internet IPv4 để kết nối các mạng, hoặc các host IPv6. Địa chỉ IPv6 tương thích được định nghĩa để sử dụng trong những công nghệ chuyển đổi từ địa chỉ IPv4 sang địa chỉ IPv6, bao gồm:

- Sử dụng trong công nghệ biên dịch giữa địa chỉ IPv4 – IPv6 (cho phép mạng IPv4 giao tiếp được mạng IPv6)
- Sử dụng cho một hình thức chuyển đổi được gọi là "đường hầm – tunnel", trong đó lợi dụng cơ sở hạ tầng sẵn có của mạng IPv4 để kết nối các mạng IPv6 bằng cách bọc gói tin IPv6 vào trong gói tin đánh địa chỉ IPv4 để truyền đi trên mạng cơ sở hạ tầng IPv4, sử dụng cấu trúc định tuyến IPv4.

Do phục vụ cho công nghệ chuyển đổi giữa giao tiếp IPv4, IPv6, địa chỉ IPv6 tương thích được cấu hình nên từ

[16] RFC3587: IPv6 Global Unicast Address Format

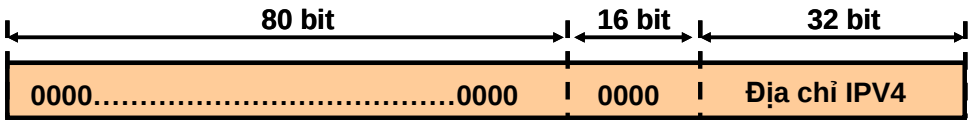
địa chỉ IPv4 và có nhiều dạng tuỳ thuộc theo các công nghệ chuyển đổi khác nhau, trong đó, có những dạng hiện nay đã không còn được sử dụng nữa. Chúng ta sẽ tìm hiểu ba trong số những dạng địa chỉ tương thích: địa chỉ IPv4-compatible, địa chỉ IPv4-mapped, địa chỉ 6to4.

2.2.2.5.1 Địa chỉ IPv4-compatible

Địa chỉ IPv4-compatible được tạo từ 32 bít địa chỉ IPv4 theo cách thức gắn các bít toàn 0 vào phía trước 32 bít địa chỉ IPv4 và được viết như sau:

0:0:0:0:0:0:*w.x.y.z hoặc* ::*w.x.y.z*

Trong đó w.x.y.z là địa chỉ IPv4 viết theo cách thông thường.



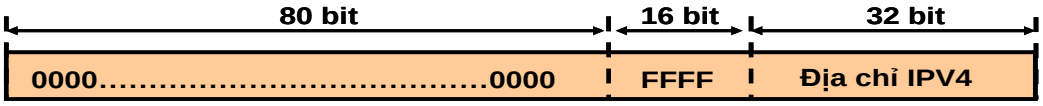
Hình 11: Địa chỉ IPv4-Compatible

Dạng địa chỉ IPv4-compatible được sử dụng trong một công nghệ tạo đường hầm được có tên gọi tunnel tự động. Khi một gói tin IPv6 có địa chỉ nguồn và đích dạng IPv4-compatible, gói tin IPv6 đó sẽ được tự động bọc trong gói tin có IPv4 header và gửi tới đích sử dụng cơ sở hạ tầng mạng IPv4.

Hiện nay, nhu cầu về dạng kết nối tunnel tự động này không còn nữa. Do vậy, dạng địa chỉ này cũng đã được loại bỏ không còn sử dụng trong giai đoạn phát triển tiếp theo của địa chỉ IPv6.

2.2.2.5.2 Địa chỉ IPv4-mapped

Địa chỉ IPv4-mapped được tạo nên từ 32 bít địa chỉ IPv4 theo cách thức gắn 80 bít 0 đầu tiên, tiếp theo là 16 bít có giá trị hexa FFFF với 32 bít địa chỉ IPv4. Địa chỉ IPv4-mapped được viết như sau:
0:0:0:0:0:FFFF:*w.x.y.z* hoặc ::FFFF:*w.x.y.z*
Trong đó w.x.y.z là địa chỉ IPv4 viết theo cách thông thường.



Hình 12: Địa chỉ IPv4-mapped

Địa chỉ IPv4 mapped được sử dụng để biểu diễn một node thuần IPv4 thành một node IPv6 để phục vụ trong công nghệ biên dịch địa chỉ IPv4 – địa chỉ IPv6[17] (ví dụ công nghệ NAT-PT, phục vụ giao tiếp giữa mạng thuần địa chỉ IPv4 và mạng thuần địa chỉ IPv6). Địa chỉ IPv4-mapped không bao giờ được dùng làm địa chỉ nguồn hay địa chỉ đích của một gói tin IPv6.

[17] Công nghệ chuyển đổi giao tiếp IPv4 - IPv6 được đề cập trong chương 5 của tài liệu

2.2.2.3 Địa chỉ 6to4

Trong vùng địa chỉ unicast định danh toàn cầu (xác định bằng 3 bít đầu 001), IANA dành riêng một vùng địa chỉ, đặt tên là Địa chỉ 6to4, là một dạng địa chỉ tương thích phục vụ cho một công nghệ tạo đường hầm có tên gọi công nghệ tunnel 6to4. Địa chỉ 6to4 được sử dụng trong giao tiếp giữa hai node chạy đồng thời cả hai thủ tục IPv4 và IPv6 trên mạng cơ sở hạ tầng định tuyến của IPv4.

Địa chỉ 6to4 được hình thành từ địa chỉ IPv4 bằng cách như sau:

- Trong vùng địa chỉ unicast định danh toàn cầu (xác định bằng ba bít đầu 001), IANA đã cấp phát một prefix địa chỉ dành riêng 2002::/16 để tạo nên địa chỉ 6to4.
- Địa chỉ 6to4 được tạo nên bằng cách gắn 16 bít dành riêng nói trên với 32 bít địa chỉ IPv4 viết dưới dạng hexa, từ đó tạo nên một vùng địa chỉ IPv6 kích thước /48. Vùng địa chỉ này sẽ được sử dụng để tạo nên mạng IPv6 6to4. Các mạng này sẽ kết nối với nhau trên cơ sở hạ tầng mạng Internet IPv4.

Các công nghệ chuyển đổi IPv4 – IPv6 nói chung, và công nghệ tạo đường hầm 6to4 nói riêng được đề cập chi tiết trong chương 5 của tài liệu.

2.2.3 Những dạng địa chỉ thuộc loại MULTICAST

Địa chỉ multicast, là một phần phức tạp song rất đặc thù của giao thức IPv6. Trong hoạt động của giao thức IPv6, không tồn tại loại địa chỉ với chức năng broadcast. Chức năng của địa chỉ broadcast IPv4 được đảm nhiệm bởi một trong số các dạng địa chỉ IPv6 multicast. Địa chỉ IPv6 multicast thay thế cho cả địa chỉ broadcast và multicast trong IPv4.

IPv6 có rất nhiều dạng địa chỉ multicast. Mỗi dạng có phạm vi hoạt động tương ứng. Một node IPv6 nhất định sẽ được thiết kế để "nghe" lưu lượng của một số loại địa chỉ IPv6 multicast. Node có thể nghe lưu lượng của nhiều loại địa chỉ multicast tại cùng thời điểm. Node cũng có thể gia nhập hoặc rời bỏ một nhóm multicast tại bất cứ thời điểm nào.

Multicast IPv6 không cần thêm cấu hình gì nếu thực hiện trong phạm vi một đường kết nối. Các node IPv6 mặc định tham gia các nhóm multicast cần thiết cho các quy trình hoạt động của IPv6 trên một đường kết nối, ví dụ nhóm xác định mọi node trên đường kết nối, hay nhóm xác định mọi router trên đường kết nối. Tuy nhiên nếu lưu lượng multicast đi vượt qua router, ra ngoài phạm vi một đường kết nối, khi đó cần có những cấu hình thực hiện định tuyến multicast.

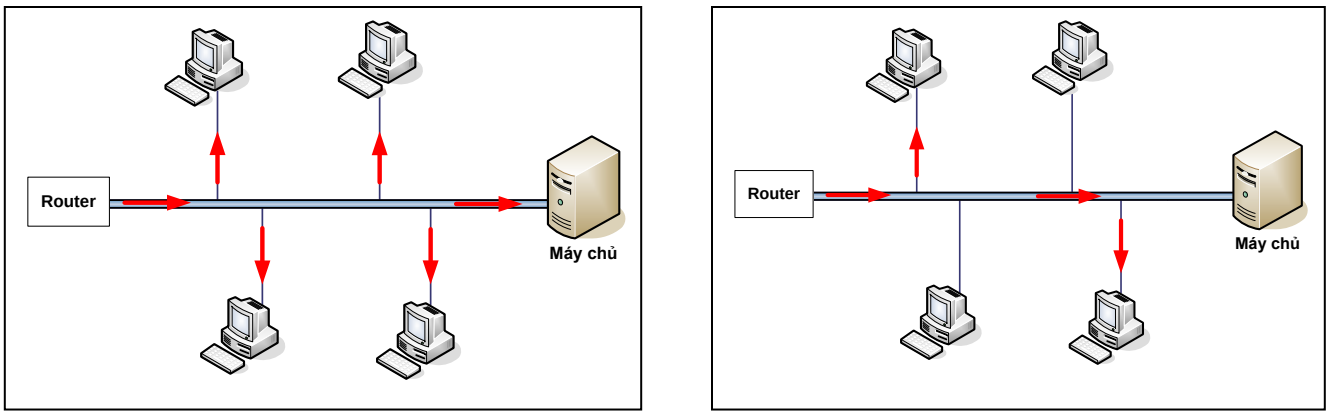
2.2.3.1 Multicast và broadcast trong giao thức IPv4

Broadcast:

Như chúng ta đã biết, trong IPv4, địa chỉ broadcast được sử dụng trong các thủ tục ARP[18], DHCP và các thủ tục khác thực hiện chức năng tìm kiếm (discovery), phục vụ cho những quy trình hoạt động cốt yếu của IPv4. Trong một mạng, địa chỉ IPv4 có giá trị các bít trong phần host toàn 1 được sử dụng làm địa chỉ broadcast trong mạng.

[18] ARP: Address Resolution Protocol - Thủ tục phân giải địa chỉ, sử dụng trong IPv4 để phân giải địa chỉ IPv4 thành địa chỉ lớp hai tương ứng, ví dụ địa chỉ Ethernet MAC.

Gói tin gửi tới địa chỉ đích IPv4 broadcast sẽ được chuyển tới và xử lý tại toàn bộ các node trên mạng. Tại lớp hai, địa chỉ Ethernet FF:FF:FF:FF:FF:FF là địa chỉ broadcast mức Ethernet.



Broadcast Multicast

Hình 13: Multicast và Broadcast trong địa chỉ IPv4

Trong IPv4, multicast là một công nghệ được thiết kế cũng cho phép gửi một gói tin đồng thời tới nhiều đích. Tuy nhiên multicast khác broadcast ở điểm, gói tin không phải được gửi tới mọi node trong phạm vi một mạng mà được gửi tới nhóm các node xác định, các node này có vị trí địa lý khác nhau, và có thể thuộc nhiều tổ chức khác nhau. Khi thực hiện multicast, router trên các mạng có node tham gia nhóm multicast phải hỗ trợ thủ tục định tuyến multicast. Host có thể lựa chọn có tham gia vào một nhóm multicast nào đó hay không. Việc quản lý quan hệ nhóm multicast trong IPv4 được thực hiện bằng thủ tục quản lý nhóm IGMP[19]. Trong khi đó với broadcast, mọi node trong phạm vi một subnet là thành viên của nhóm broadcast bất kể nó có muốn hay không. Khi thiết kế IPv4, toàn bộ địa chỉ lớp D (từ 224.0.0.0 đến 239.255.255.255) được dành riêng để sử dụng cho công nghệ Multicast. Tuy được đánh giá hiệu quả và các tiêu chuẩn kỹ thuật đã được thiết kế hoàn thiện, song công nghệ multicast không được áp dụng rộng rãi trong hoạt động của Internet IPv4 do nhiều nguyên nhân về đòi hỏi cấu hình.

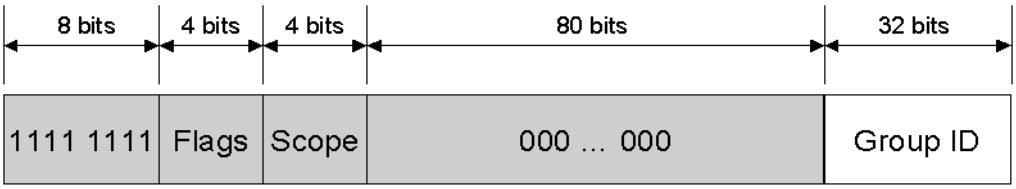
2.2.3.2 Cấu trúc địa chỉ IPv6 Multicast

Địa chỉ Multicast IPv6 được thiết kế để thực hiện cả chức năng broadcast và multicast. Do vậy có nhiều dạng địa chỉ multicast IPv6. Có những dạng địa chỉ IPv6 multicast mà IPv6 node bắt buộc phải nhận lưu lượng, phục vụ cho những quy trình hoạt động thiết yếu của IPv6. Có những dạng địa chỉ multicast IPv6 sử dụng trong công nghệ truyền gói tin tương tự như multicast của IPv4. Mỗi dạng địa chỉ multicast IPv6 có phạm vi hoạt động nhất định. Lưu lượng của địa chỉ IPv6 multicast sẽ được chuyển tới toàn bộ các node trong một phạm vi nào đó hay chỉ được chuyển tới nhóm các node trong phạm vi là tùy thuộc vào dạng địa chỉ multicast.

Vùng địa chỉ có tiền tố FF::/8 (8 bít đầu là 1111 1111), chiếm 1/256 không gian địa chỉ IPv6 được dành riêng để làm địa chỉ IPv6 multicast.

Cấu trúc của địa chỉ IPv6 multicast như sau:

[19] IGMP: Internet Group Management Protocol



Hình 14: Cấu trúc địa chỉ IPv6 multicast

Địa chỉ IPv6 multicast luôn được bắt đầu bởi 8 bít prefix 1111 1111 và rất dễ phân biệt. Địa chỉ multicast không bao giờ được sử dụng làm địa chỉ nguồn của một gói tin IPv6 .

Trong cấu trúc địa chỉ IPv6 multicast có các nhóm bít thực hiện các chức năng sau đây:

Cờ (Flag) 4 bít : Trường này có bốn bít "0T00", trong đó 3 bít hiện chưa sử dụng được đặt giá trị 0, bít T sẽ xác định đây là dạng địa chỉ IPv6 multicast được IANA gắn vĩnh viễn (permanent-assigned), sử dụng thống nhất trong hoạt động Internet IPv6 toàn cầu, hoặc là dạng địa chỉ IPv6 multicast do người sử dụng tự quy định (non permanent-assigned). Khái niệm này cũng tương tự như khái niệm well-known port trong thủ tục TCP/IP.

- Nếu Bít T=0, đây là địa chỉ multicast IPv6 vĩnh viễn được IANA quy định. Danh sách các địa chỉ này được cung cấp trong RFC2375[20]. Trong đó có những dạng địa chỉ phục vụ cho những quy trình hoạt động cốt yếu của IPv6, sử dụng cho những giao tiếp khi một node cần giao tiếp với toàn bộ hoặc với nhóm các node xác định trên một đường kết nối.

  Ví dụ:

  FF02:: 1 là địa chỉ multicast để gửi tới mọi node trên một đường link

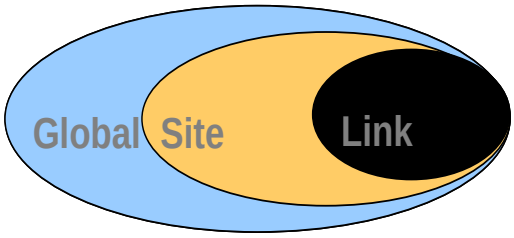
  FF02::2 là địa chỉ multicast để gửi tới mọi router trên một đường link.

- Nếu Bít T=1, đây là dạng địa chỉ multicast được tạo nên bởi người sử dụng, trong một phạm vi nhất định. Địa chỉ multicast sẽ không có ý nghĩa ngoài phạm vi đó. Một cách thức để tạo nên địa chỉ này là tổ chức sử dụng tiền tố (prefix) của vùng địa chỉ unicast toàn cầu của mình để gắn cùng với tiền tố FF để tạo nên địa chỉ multicast.

Phạm vi (Scope) 4 bít: Trường này gồm 4 bít xác định phạm vi của nhóm địa chỉ multicast. Hiện nay đang định nghĩa các giá trị như sau:

1: Phạm vi Node
2: Phạm vi Link
5: Phạm vi Site
8: Phạm vi tổ chức Organisation
E: Phạm vi toàn cầu Global

Các giá trị khác hiện nay chưa gán.



Hình 15: Phạm vi (scope) của địa chỉ IPv6

[20] *RFC2375* - IPv6 Multicast Address Assignments

Giải thích một cách rõ ràng hơn, nếu ta thấy 4 bít trường scope là "0001" (tức giá trị Scope là 1) khi đó phạm vi của địa chỉ multicast này là phạm vi node. Gói tin multicast sẽ chỉ được gửi trong phạm vi các giao diện trong một node mà thôi.

Nếu 4 bít này là "0010", giá trị trường Scope là 2, phạm vi của địa chỉ multicast là phạm vi link. Gói tin multicast được gửi trên phạm vi toàn bộ đường kết nối.

Router sử dụng giá trị trường Scope của địa chỉ multicast để quyết định có chuyển tiếp lưu lượng multicast hay không. Ví dụ địa chỉ multicast FF02::2 có phạm vi link-local, router sẽ không bao giờ chuyển tiếp gói tin này ra khỏi phạm vi đường kết nối.

Nhóm (Group ID) 32 bít – Thực hiện chức năng định danh các nhóm multicast. Trong một phạm vi, có nhiều nhóm multicast (ví dụ nhóm multicast các router, nhóm multicast mọi node, nhóm multicast mọi máy chủ DHCP…). Giá trị các bít Group ID sẽ định danh các nhóm multicast. Trong một phạm vi, số định danh này là duy nhất. Lưu lượng có địa chỉ đích multicast sẽ được chuyển tới các máy thuộc nhóm multicast xác định bởi Group ID, trong phạm vi xác định bởi Scope.

Trong địa chỉ IPv6, 32 bít cuối được sử dụng để xác định nhóm multicast. Theo thiết kế ban đầu, Group ID gồm 112 bít. Với 112 bít, có thể định danh 2^{112} nhóm. Tuy nhiên, để có thể truyền đi trên mạng tới đích, dữ liệu phải chứa thông tin địa chỉ IP (lớp network) và địa chỉ lớp link-layer (địa chỉ MAC trong trường hợp kết nối Ethernet) tương ứng. Để có được ánh xạ 1-1 từ một địa chỉ IPv6 multicast tới một địa chỉ Ethernet multicast MAC duy nhất, số lượng bít của Group ID được khuyến nghị là 32 bít.

2.2.3.3 Một số địa chỉ multicast IPv6 vĩnh viễn

Khi thiết bị được kích hoạt hỗ trợ IPv6, các node phải tham gia vào một số nhóm multicast bắt buộc. Node phải tham gia vào nhóm multicast dành cho mọi node trong phạm vi node và phạm vi đường kết nối. Router phải tham gia vào nhóm multicast dành cho mọi router phạm vi node, phạm vi đường kết nối.

Multicast tới mọi node:

Nhóm multicast mọi node hiện nay được gắn giá trị Group ID 1

Địa chỉ IPv6 multicast	Tên gọi	Giá trị Scope	Giá trị Group ID	Chú thích
FF01::1	Địa chỉ multicast mọi node phạm vi node	1 Xác định phạm vi node	1 Xác định nhóm multicast mọi node	
FF02::1	Địa chỉ multicast mọi node phạm vi link	2 Xác định phạm vi link	1 Xác định nhóm multicast mọi node	Xác định mọi node IPv6 trong phạm vi một đường kết nối

Bảng 2: Địa chỉ multicast mọi node

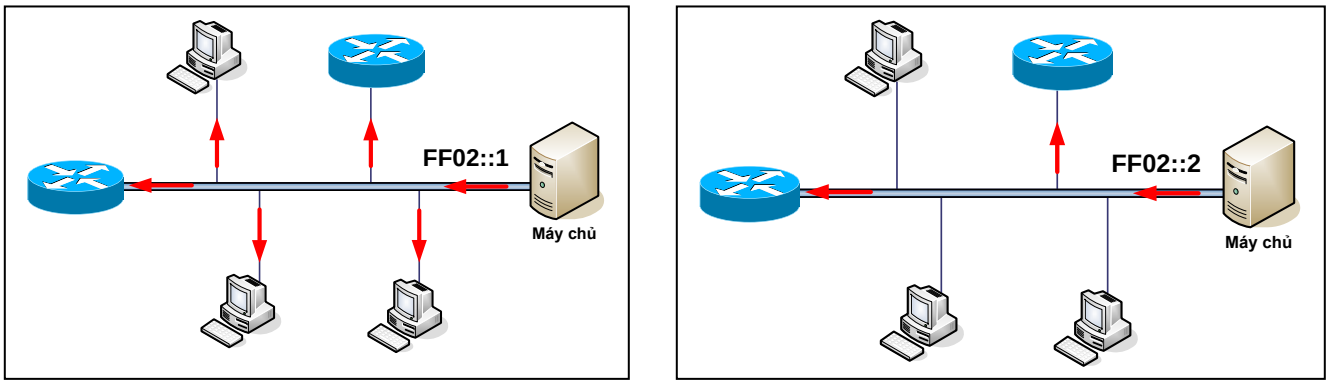
Multicast tới mọi router:

Nhóm multicast mọi router hiện nay được gắn giá trị Group ID 2

Địa chỉ IPv6 multicast	Tên gọi	Giá trị Scope	Giá trị Group ID	Chú thích
FF01::2	Địa chỉ multicast mọi router phạm vi node	1 Xác định phạm vi trong node	2 Xác định nhóm multicast mọi router	
FF02::2	Địa chỉ multicast mọi router phạm vi link	2 Xác định phạm vi link	2 Xác định nhóm multicast mọi router	Xác định mọi router IPv6 trong phạm vi một đường kết nối
FF05::2	Địa chỉ multicast mọi router phạm vi site	5 Xác định phạm vi site	2 Xác định nhóm multicast mọi router	Xác định mọi router IPv6 trong phạm vi một site

Bảng 3: Địa chỉ Multicast mọi router

Những giá trị IPv6 multicast vĩnh viễn khác, có thể tìm hiểu trong *RFC2375* - IPv6 Multicast Address Assignments.



Hình 16: Multicast trong phạm vi link

2.2.3.4 Địa chỉ multicast Solicited-node

Một trong những quy trình hoạt động cốt yếu của IPv4 là thực hiện phân giải giữa địa chỉ IPv4 32 bít thành địa chỉ lớp 2 tương ứng (ví dụ địa chỉ MAC Ethernet 48 bít). Địa chỉ IPv4 thực hiện chức năng này bằng thủ tục ARP (Address Resolution Protocol). Nguyên lý hoạt động cơ bản của thủ tục này là giao tiếp yêu cầu/đáp ứng trong đó một node khi không biết địa chỉ lớp vật lý của một node khác trên đường link sẽ gửi gói tin ARP tới toàn bộ node gắn trên một Ethernet (sử dụng địa chỉ broadcast). Gói tin này có chứa địa chỉ IP của node mà nó muốn giao tiếp. Các node trên Ethernet đều nhận và xử lý gói tin này, node có địa chỉ IP trùng khớp với địa chỉ IP chứa trong gói tin sẽ gửi thông tin đáp trả. Thủ tục ARP của địa chỉ IPv4 có một hạn chế: do sử dụng địa chỉ broadcast nên khi

một node khi thực hiện thủ tục phân giải địa chỉ, vốn là quy trình diễn ra thường xuyên đã "làm phiền" tới mọi node trên mạng LAN, làm giảm hiệu quả của mạng.

Trong địa chỉ IPv6, chức năng phân giải địa chỉ được đảm nhiệm bằng một thủ tục mới, phụ trách giao tiếp của các node trên một đường link, có tên gọi thủ tục Neighbor Discovery[21], qua việc trao đổi các thông điệp ICMPv6[22]. Trong quá trình phân giải địa chỉ[23], để tránh tác động đến toàn bộ các node trên đường kết nối (vốn là một hạn chế của thủ tục ARP IPv4), địa chỉ IPv6 không sử dụng dạng địa chỉ multicast mọi node phạm vi link (FF02::1) là dạng địa chỉ thực hiện chức năng tương tự như địa chỉ broadcast trong mạng LAN của IPv4 làm địa chỉ đích của gói tin truy vấn. Thay vì đó, quá trình phân giải địa chỉ của IPv6 sử dụng một dạng địa chỉ IPv6 multicast đặc biệt, có tên gọi địa chỉ ***multicast solicited-node***.

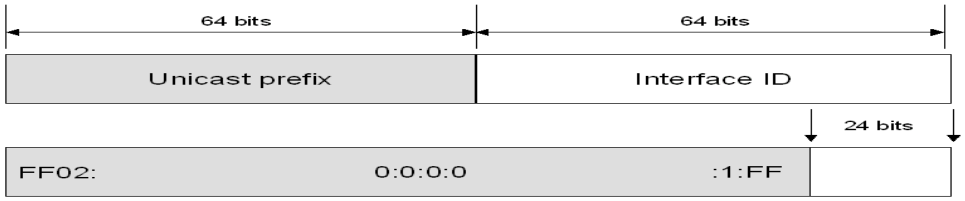
Địa chỉ *multicast solicited-node* được cấu thành từ địa chỉ unicast đã gán cho node. Mỗi một địa chỉ unicast được gắn cho node, sẽ có một địa chỉ multicast solicited node tương ứng.

Cấu thành địa chỉ Solicited node từ địa chỉ unicast:

Địa chỉ solicited-node được cấu thành từ địa chỉ unicast bằng cách gắn 104 bít tiền tố prefix FF02::1:FF/104 với 24 bít cuối cùng chính là 24 bít cuối của địa chỉ unicast.

Để có thể giao tiếp, node cần phân giải được các địa chỉ IPv6 unicast đã gán cho node thành địa chỉ lớp hai tương ứng, do vậy với mỗi một địa chỉ unicast được gắn cho node sẽ có một địa chỉ multicast solicited node. IPv6 node sẽ vừa nghe lưu lượng tại địa chỉ unicast, vừa nghe lưu lượng tại địa chỉ multicast solicited-node tương ứng địa chỉ unicast đó.

Do trường Scope trong địa chỉ solicited-node có giá trị 2, đây là địa chỉ multicast có phạm vi trên đường kết nối. Địa chỉ multicast solicited node sẽ tự động được tạo ra khi host được gắn các địa chỉ unicast.



Hình 17: Cấu thành địa chỉ solicited-node multicast từ địa chỉ unicast

Ví dụ cụ thể:

Một node IPv6:

- Có địa chỉ link-local "FE80::2AA:FF:FE3F:2A1C" . Địa chỉ Multicast Solicited node tương ứng địa chỉ link-local này là "FF02::1:FF3F:2A1C"
- Nếu node được gắn địa chỉ unicast toàn cầu 2001:dc8::3005:BC68. Địa chỉ Multicast Solicited node tương ứng địa chỉ unicast này là "FF02::1:FF3F:BC68"

[21] Tham khảo thủ tục Neighbor Discovery trong mục 4.2
[22] Tham khảo thủ tục ICMPv6 trong mục 4.1
[23] Tham khảo quy trình phân giải địa chỉ của IPv6 trong mục 4.3.1

2.2.4 Dạng địa chỉ ANYCAST

Địa chỉ anycast được gắn cho một nhóm nhiều giao diện. Gói tin được gửi tới địa chỉ anycast sẽ được chuyển đi theo cấu trúc định tuyến tới giao diện gần nhất trong nhóm (tính theo thủ tục định tuyến). RFC3513[24] định nghĩa địa chỉ anycast với những đặc điểm như sau:

- Anycast không có không gian địa chỉ riêng mà thuộc vùng địa chỉ unicast. Khi một địa chỉ unicast được gắn đồng thời cho nhiều giao diện, nó sẽ trở thành địa chỉ anycast.
- Một địa chỉ anycast có thể được gắn cho nhiều giao diện của nhiều node.

Địa chỉ anycast không bao giờ được sử dụng làm địa chỉ nguồn của một gói tin IPv6. Hiện nay, địa chỉ anycast không được gắn cho IPv6 host mà chỉ được gắn cho IPv6 router. Một trong những ứng dụng mong muốn của địa chỉ anycast là sử dụng để xác định một tập các router thuộc về một nhà cung cấp dịch vụ Internet.

Hiện nay, mới chỉ có một dạng địa chỉ anycast được định nghĩa và ứng dụng, có tên gọi địa chỉ anycast Subnet-Router. Trên một subnet IPv6, có thể có nhiều router phụ trách kết nối và chuyển tiếp gói tin cho các host thuộc subnet sang những mạng khác. Khi được sử dụng, địa chỉ anycast Subnet-Router đồng thời được gắn cho các router IPv6 trong một mạng (subnet). Gói tin sử dụng địa chỉ này làm địa chỉ đích sẽ đến được một trong số các router này và sẽ tới được mạng.

Cách thức tạo địa chỉ Anycast Subnet-Router từ prefix của subnet:

Người ta giữ nguyên các bít tiền tố (prefix) của subnet và đặt mọi bít khác về giá trị 0. Lấy địa chỉ thu được làm địa chỉ anycast Subnet-router của subnet. Mọi giao diện router gắn với mạng con này được đồng thời gắn địa chỉ anycast Subnet-Router trên. Địa chỉ này được sử dụng để một node từ xa giao tiếp với một trong số những router của subnet.

2.2.5 Lựa chọn địa chỉ mặc định trong IPv6

Cấu trúc địa chỉ IPv6 cho phép nhiều địa chỉ, thuộc nhiều dạng có thể gắn cho cùng một giao diện. Việc có nhiều địa chỉ trên một giao diện khiến cho các thực thi IPv6 thường xuyên đối diện với tình trạng nhiều địa chỉ nguồn và địa chỉ đích khi khởi tạo giao tiếp. Cần phải có một thuật toán mặc định, chung cho mọi thực thi để lựa chọn địa chỉ nguồn và địa chỉ đích.

Thuật toán cho phép lựa chọn địa chỉ này sử dụng nhiều yếu tố để cân nhắc. Trong đó có một số yếu tố như sau:

- *Tình trạng địa chỉ*: Mỗi một địa chỉ IPv6 gắn cho IPv6 node đi kèm với khoảng thời gian "sống" hợp lệ. Node IPv6 quản lý tình trạng địa chỉ theo thời gian sống, trong đó "preferred" tức địa chỉ còn được lựa chọn và "deprecated" tức địa chỉ đã bỏ đi. Khi lựa chọn địa chỉ để sử dụng trong giao tiếp, IPv6 node sẽ không sử dụng những địa chỉ "deprecated".
- *Bảng chính sách "Policy Table"*: Thuật toán lựa chọn địa chỉ còn sử dụng một bảng lưu trữ gọi là Policy Table. Bảng này lưu trữ các prefix địa chỉ được gắn cho node với hai giá trị đi kèm là giá trị chỉ quyền ưu tiên (Precedence) và giá trị nhãn (Label)
  - Giá trị quyền ưu tiên (Precendence) được sử dụng để sắp xếp địa chỉ đích.

[24] RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture

- Giá trị nhãn (Label) sử dụng để lựa chọn một prefix nguồn nhất định tương ứng với một prefix đích nhất định. Các thuật toán thường hay sử dụng địa chỉ nguồn (S) tương ứng với địa chỉ đích (D) khi Label(S) = Label(D).

Khi lựa chọn giá trị nhãn trùng khớp trong bảng policy table, địa chỉ sẽ được lựa chọn:

Nguồn là địa chỉ thuần IPv6 ---> Đích là địa chỉ thuần IPv6

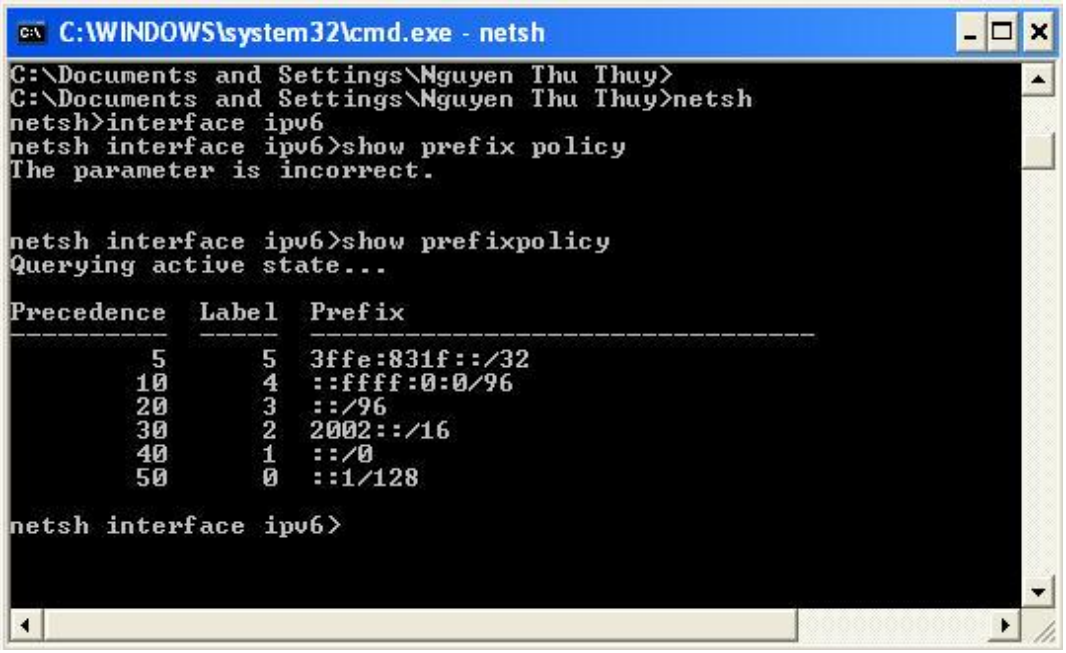
Nguồn là địa chỉ 6to4 ---> Đích là địa chỉ 6to4

Nguồn là địa chỉ IPv4-compatible ---> Đích là địa chỉ IPv4-compatible

Nguồn là địa chỉ IPv4-map ---> Đích là địa chỉ IPv4-map

Trong hệ điều hành window, chúng ta có thể xem giá trị của bảng Policy Table bằng lệnh:

Netsh> interface IPv6> show prefixpolicy



Hình 18: Lựa chọn địa chỉ trong HĐH window

- *Sử dụng thứ tự trả về của DNS:* Khi node IPv6 A kết nối tới một node B nào đó, node A có thể lựa chọn địa chỉ đích cho giao tiếp trong số những địa chỉ của B dựa trên thứ tự trả về từ truy vấn DNS.

2.3 TÓM TẮT VỀ ĐỊA CHỈ IPV6

Những mục trước đã đề cập và mô tả nhiều dạng địa chỉ IPv6. Bây giờ, chúng ta sẽ thống kê lại các tiền tố (prefix) và tổng kết lại những dạng địa chỉ mà để hoạt động được, IPv6 host, IPv6 router cần được gán.

2.3.1 Thống kê về các dạng địa chỉ IPv6

Bảng sau thống kê một số các tiền tố prefix và dạng địa chỉ thường gặp của IPv6.

Bit	Dạng địa chỉ	Chú thích
::	Địa chỉ đặc biệt	

::1	Địa chỉ loopback	
FE80::/10	Địa chỉ link-local	
FEC0::/10	Địa chỉ site local	Đã được hủy bỏ
2000::/3	Địa chỉ unicast định danh toàn cầu. Trong đó: 2002::/16 – Địa chỉ của tunnel 6to4	
::*w.x.y.z*	Địa chỉ IPv4-compatible	Dùng cho công nghệ tunnel tự động.
::FFFF:*w.x.y.z*	Địa chỉ IPv4 - map	Dùng trong biên dịch địa chỉ IPv6-IPv4. Khi cần thiết phải biểu diễn một node thuần IPv4 thành node IPv6.
FF::/8	Địa chỉ multicast *FF01::1 - Địa chỉ multicast mọi node phạm vi node* *FF02::1 - Địa chỉ multicast mọi node phạm vi link* *FF01::2 - Địa chỉ multicast mọi router phạm vi node* *FF02::2 - Địa chỉ multicast mọi router phạm vi link* *FF05::2 - Địa chỉ multicast mọi router phạm vi site* *FF02::1:FF/104 – Địa chỉ multicast Solicited node*	Sử dụng thay thế cho chức năng broadcast của địa chỉ IPv4 và phục vụ những quy trình hoạt động của IPv6 như phân giải địa chỉ, quy trình giao tiếp giữa các node trên một đường kết nối.

Bảng 4: Bảng tóm tắt về các dạng địa chỉ IPv6

2.3.2 Những dạng địa chỉ IPv6 host nghe lưu lượng và xử lý

Một IPv6 host sẽ nghe lưu lượng để nhận và xử lý gói tin tại những địa chỉ sau đây:

- Một địa chỉ link-local cho mỗi giao diện.
- Những địa chỉ unicast cho mỗi giao diện: Địa chỉ sử dụng cho giao tiếp Internet toàn cầu, hoặc các dạng địa chỉ unicast khác.
- Địa chỉ loopback

Ngoài ra còn nghe lưu lượng tại những địa chỉ multicast

- Địa chỉ multicast mọi node phạm vi node (FF01::1)
- Địa chỉ multicast mọi node phạm vi link (FF02::1)
- Địa chỉ solicited node cho mỗi địa chỉ unicast của mỗi giao diện
- Địa chỉ các nhóm multicast khác mà các giao diện tham gia (khi host được cấu hình để nhận lưu lượng trong công nghệ truyền tải multicast (tương tự như công nghệ multicast của IPv4)

2.3.3 Những dạng địa chỉ IPv6 router nghe lưu lượng và xử lý:

Chúng ta cũng biết, một router cần phải được gán mọi loại địa chỉ mà một IPv6 host được gán. Ngoài ra, IPv6 router còn được gán những địa chỉ sau đây:

- Địa chỉ Subnet router anycast
- Các địa chỉ anycast khác (nếu cần)

IPV6 router cũng nghe lưu lượng tại mọi địa chỉ mà nó được gán và mọi địa chỉ multicast IPv6 host cần nghe lưu lượng. Ngoài ra, để phục vụ cho hoạt động của router, IPv6 router còn phải nghe, nhận và xử lý các gói tin tại những địa chỉ multicast sau:

- Địa chỉ multicast mọi router phạm vi giao diện (FF01::2)
- Địa chỉ multicast mọi router phạm vi link (FF02::2)
- Địa chỉ multicast mọi router phạm vi site (FF05::2)

Người sử dụng không cần thiết phải cấu hình router để gắn những địa chỉ multicast trong phạm vi một đường kết nối. Khi router được kích hoạt hỗ trợ IPv6, hệ điều hành (ví dụ Cisco OS) sẽ tự động gắn những địa chỉ này cho IPv6 router.

Hỏi – đáp cuối chương 2:

1. Địa chỉ IPv6 được biểu diễn như thế nào ?

T: Địa chỉ IPv6 có chiều dài 128 bít nhị phân, được biểu diễn dưới dạng số hexa decimal. Một địa chỉ IPv6 là một dãy số gồm 8 nhóm số hexa cách nhau bằng dấu ":", mỗi nhóm có 4 chữ số hexa.

2. Khi biểu diễn địa chỉ IPv6, có phải viết đầy đủ toàn bộ 32 chữ số hexa hay không?

T Không cần. Địa chỉ IPv6 có thể viết gọn lại bằng hai quy tắc thu gọn như sau:

Quy tắc 1: Trong một nhóm 4 số hexa, có thể bỏ bớt những số 0 bên trái

Quy tắc 2: Trong cả địa chỉ IPv6, một số nhóm liền nhau chứa toàn số 0 có thể không viết và thay thế bằng "::". Tuy nhiên chỉ được phép thay thế một lần như vậy trong toàn bộ một địa chỉ IPv6.

Khi biểu diễn thu gọn theo hai quy tắc như vậy, địa chỉ IPv6 đầy đủ hoàn toàn có thể được xây dựng lại từ địa chỉ IPv6 thu gọn.

3. Ba loại địa chỉ unicast, multicast, anycast của IPv6 khác nhau tại điểm gì?

T: Ba loại địa chỉ IPv6 khác nhau ở cách thức gửi gói tin đến giao diện gắn địa chỉ đích. Gói tin có địa chỉ đích là địa chỉ unicast chỉ được gửi tới một giao diện duy nhất. Gói tin có địa chỉ đích là địa chỉ multicast sẽ được gửi tới tất cả các giao diện trong nhóm được gắn địa chỉ đó. Gói tin có địa chỉ đích anycast được gửi tới giao diện gần nhất trong nhóm được gắn địa chỉ (tính theo thủ tục định tuyến).

4. Trong địa chỉ IPv6, chức năng broadcast của IPv4 được đảm nhiệm bằng dạng địa chỉ nào?

T Địa chỉ IPv6 không còn tồn tại khái niệm địa chỉ broadcast. Chức năng của địa chỉ broadcast trong IPv4 được đảm nhiệm thay thế bởi địa chỉ IPv6 multicast.

5. Trên phương diện gắn địa chỉ cho host, địa chỉ IPv6 khác IPv4 ở điểm nào?

T Một host IPv6 chỉ có một card mạng cũng sẽ có nhiều giao diện, có thể là giao diện vật lý, hoặc giao diện ảo dành cho công nghệ đường hầm tunnel. Một giao diện IPv6 có thể được gắn đồng thời nhiều địa chỉ IPv6

6. IPv6 sử dụng địa chỉ nào làm địa chỉ loopback?

T Địa chỉ loopback của IPv6 là 0:0:0:0:0:0:0:1**,** hay còn được viết là ::1.

7. Khi cần tới địa chỉ IPv4 cho hoạt động mạng, chúng ta xin cấp từ các tổ chức quản lý địa chỉ quốc tế. Dạng địa chỉ IPv6 nào tương đương với địa chỉ IPv4 trên?

T Dạng địa chỉ IPv6 tương đương với IPv4 sử dụng trong định tuyến Internet toàn cầu, hiện nay đang được các tổ chức quản lý địa chỉ cấp phát, phân bổ cho hoạt động Internet là địa chỉ unicast định danh toàn cầu (global unicast address). Loại địa chỉ này có ba bít prefix ban đầu 001 (trừ vùng địa chỉ 2002::/16 là địa chỉ 6to4).

8. Dạng địa chỉ IPv6 nào IPv6 node có thể sử dụng để giao tiếp với các node khác trong một đường link cho dù nó chưa được cấu hình địa chỉ phạm vi toàn cầu?

T Đó là địa chỉ link-local. Địa chỉ link-local có 10 bít tiền tố prefix là FE80::/64. IPv6 host có khả năng tự động tạo địa chỉ link-local, cho dù chưa được cấu hình bất cứ địa chỉ phạm vi toàn cầu nào. Do vậy, IPv6 host có thể sử dụng địa chỉ link-local này để giao tiếp với nhau trên một đường link, ngay cả khi chưa được cấu hình các dạng địa chỉ khác.

9. Các công nghệ chuyển đổi IPv6 - IPv4 sử dụng dạng địa chỉ IPv6 nào? Lấy ví dụ?

T Các công nghệ chuyển đổi IPv6-IPv4 sử dụng dạng địa chỉ tương thích (Compatibility address). Những địa chỉ này được xây dựng từ địa chỉ IPv4 và phục vụ những công nghệ chuyển đổi khác nhau. Ví dụ địa chỉ IPv4-compatible (::w.x.y.z) dùng cho tunnel tự động (hiện nay không còn dùng nữa), địa chỉ IPv4-mapped (0:0:0:0:0:FFFF:w.x.y.z) dùng trong công nghệ biên dịch, địa chỉ 6to4 (có prefix dành riêng 2002::/16) dùng cho công nghệ đường hầm 6to4.

10. Bạn cho biết, địa chỉ multicast IPv6 được nhận dạng bằng cách nào ?

T: Địa chỉ IPv6 multicast được nhận dạng bằng 8 bít tiền tố FF (1111 1111)

11. Nếu một host gửi gói tin có địa chỉ đích FF02::2 thì những IPv6 node nào sẽ nhận được, nếu gửi gói tin có địa chỉ đích FF02::1 thì những IPv6 node nào sẽ nhận được ?

T Địa chỉ multicast FF02::2 có giá trị trường Scope = 2 là phạm vi đường link, giá trị group ID = 2 là nhóm multicast mọi router. Như vậy, khi gói tin có địa chỉ đích này, sẽ được gửi tới mọi router trên phạm vi đường link.

Địa chỉ multicast FF02::1 có giá trị trường Scope = 2 là phạm vi đường link, giá trị group ID = 1 là nhóm multicast mọi node. Như vậy, khi gói tin có địa chỉ đích này, sẽ được gửi tới mọi node (router, host) trên phạm vi đường link.

12. Quá trình phân giải địa chỉ của IPv6 sử dụng dạng thức địa chỉ multicast nào?

T Để tăng tính hiệu quả, quá trình phân giải địa chỉ của IPv6 không sử dụng địa chỉ multicast mọi node phạm vi link mà sử dụng địa chỉ multicast solicited node. Mỗi địa chỉ unicast gắn cho IPv6 node sẽ tương ứng với một địa chỉ multicast solicited node. Khi được gắn địa chỉ unicast, IPv6 node không chỉ nghe lưu lượng tại địa chỉ unicast này mà đồng thời, cũng sẽ nghe lưu lượng tại địa chỉ multicast solicited node tương ứng địa chỉ unicast.

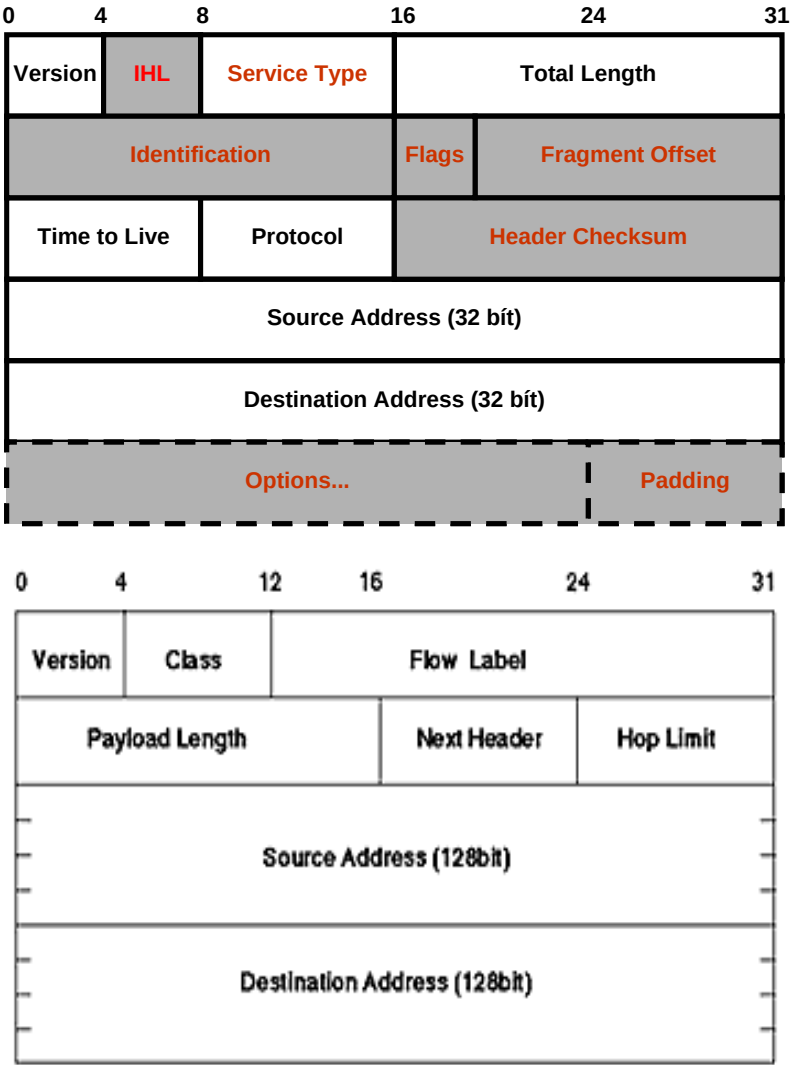
CHƯƠNG 3: GIAO THỨC IPV6 – CÁC ĐẶC ĐIỂM SO SÁNH VỚI IPV4

Trong chương này, bạn sẽ tìm hiểu về những khác biệt, thay đổi và cải tiến về phương diện giao thức trong IPv6 so với IPv4. Cụ thể là IPv6 header.

3.1 IPV6 HEADER

Hoạt động của Internet dựa trên các giao thức, là tập các quy trình phục vụ cho giao tiếp. Trong giao thức Internet, những thông tin như địa chỉ IP của nơi gửi và nơi nhận gói tin, và những thông tin cần thiết khác được đặt phía trước dữ liệu. Phần thông tin đó được gọi là phần mào đầu (header).

IPV6 header là phiên bản cải tiến, được tổ chức hợp lý hơn so với IPv4 header. Trong đó loại bỏ đi một số trường không cần thiết hoặc ít khi sử dụng và thêm vào những trường hỗ trợ tốt hơn cho lưu lượng thời gian thực.



Hình 19: IPv6 header

Thực hiện so sánh hai dạng thức header IPv4 và IPv6, sẽ thấy một số trường được giữ nguyên, một số trường trong IPv6 header thực hiện chức năng tương tự trường của IPv4 header, có trường được thêm vào và một số trường được bỏ đi.

Để thấy những thay đổi và nâng cấp trong IPv6 header, chúng ta sẽ nhắc lại về các trường trong IPv4 header và chức năng của chúng, sau đó sẽ so sánh với header IPv6.

3.1.1 IPV4 header

IPV4 header có các trường sau đây:

Version – Chỉ định phiên bản của IP, có giá trị 4.

Internet Header Length – Chỉ định chiều dài IPv4 header (đơn vị đo là khối 4 byte).

Service Type – Chỉ định dịch vụ mong muốn khi truyền các gói tin qua router. Trường này có 8 bít, xác định quyền ưu tiên, độ trễ, thông lượng, các đặc tính chỉ định độ tin cậy khác. Trường Service Type gồm TOS (Type of Service) và Precedence. TOS xác định loại dịch vụ, bao gồm: giá trị, độ tin cậy, thông lượng, độ trễ hoặc bảo mật. Precedence xác định mức ưu tiên, sử dụng 8 mức từ 0-7.

Total Length – Chỉ định tổng chiều dài gói tin IPv4 (cả phần mào đầu và phần dữ liệu). Kích thước 16 bít, chỉ định rằng gói tin IPv4 có thể dài tới 65,535 byte.

Identification – Định danh gói tin. Kích thước 16 bít. Định danh cho gói tin được lựa chọn bởi nguồn gửi gói tin. Nếu gói tin IPv4 bị phân mảnh, mọi phân mảnh sẽ giữ lại giá trị trường định danh này, mục đích để node đích có thể nhóm lại các mảnh, phục vụ cho việc phục hồi lại gói tin.

Flags – Xác định cờ cho quá trình phân mảnh. Kích thước 3 bít. Có hai cờ: một xác định gói tin bị phân mảnh và cờ kia chỉ định xem có thêm phân mảnh khác nữa tiếp theo phân mảnh hiện thời hay không.

Fragment Offset – Chỉ định vị trí của phân mảnh trong phần dữ liệu (payload) của gói tin ban đầu. Trường này có kích thước 13 bít.

Time to Live – Chỉ định số lượng link tối đa mà một gói tin IPv4 có thể đi qua trước khi bị hủy bỏ. Trường này dài 8 bít. TTL được sử dụng như một bộ đếm thời gian mà router IPv4 dùng để quyết định độ dài thời gian cần thiết (bằng giây) để chuyển tiếp gói tin IPv4. Router hiện đại chuyển tiếp gói tin chưa đến một giây song theo quy ước, luôn giảm giá trị trường này 1 đơn vị. Khi giá trị TTL trở về 0, gói tin sẽ được hủy đi và thông điệp lỗi được gửi trả lại địa chỉ IPv4 nguồn.

Protocol – Xác định thủ tục lớp cao hơn gói tin sẽ được chuyển tiếp. Trường này gồm 8 bít. Ví dụ một số giá trị: 6 là TCP, 17 là UDP, 1 là ICMP.

Header Checksum – Cung cấp kiểm tra checksum cho IPv4 header. Có kích thước 16 bít. Phần dữ liệu của gói tin IPv4 (payload) không bao gồm trong checksum này mà chứa checksum riêng của nó. Các IPv4 node nhận gói tin sẽ kiểm tra IPv4 header checksum và loại bỏ gói tin nếu giá trị checksum tính toán được không trùng khớp với số checksum trong phần mào đầu của gói tin nhận được, bởi vì như vậy chứng tỏ đã có sai lệch thông tin khi truyền tải. Khi router chuyển tiếp đi một gói tin IPv4, nó phải giảm giá trị trường TTL, do vậy trường Header Checksum được tính toán lại tại mỗi router giữa nguồn và đích.

Source Address – Chứa địa chỉ nguồn gửi gói tin IPv4. Kích thước 32 bit.

Destination Address – Chứa địa chỉ IPv4 đích. Kích thước 32 bit.

Options – Chứa một hoặc nhiều hơn tùy chọn trong IPv4. Kích thước trường này là một số nguyên lần của khối 4 byte (32 bít) . Nếu các option không dùng hết và làm lẻ khối 32 bít, các giá trị 0 (gọi là phần đệm - Padding) sẽ được thêm vào để đảm bảo IPv4 header là một số nguyên của khối 4 byte, như vậy chiều dài IPv4 header mới có thể chỉ định được bằng giá trị cuả trường Internet Header Length.

3.1.2 IPV6 Header - Thay đổi, cải tiến so với IPv4

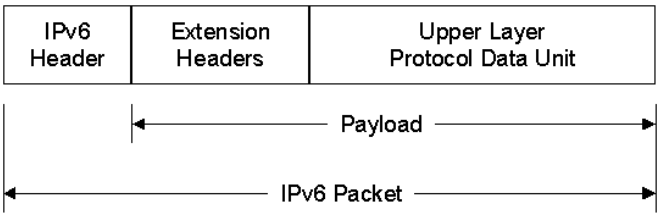
IPv6 header có những thay đổi gì so với thế hệ địa chỉ IPv4 ?

3.1.2.1 Chiều dài của header

Như trên mô tả, IPv4 header có một trường chiều dài không cố định, đó là Options. Trường Options được sử dụng để thêm các thông tin về các dịch vụ tuỳ chọn khác nhau trong IPv4, ví dụ thông tin liên quan đến mã hoá. Do đó, chiều dài của IPV4 header thay đổi tuỳ theo tình trạng. Do sự thay đổi đó, các router điều khiển giao tiếp dựa trên những thông tin trong IP header không thể biết trước chiều dài của phần header. Điều này cản trở việc tăng tốc xử lý gói tin.

Khác với địa chỉ IPv4, gói tin IPv6 có hai dạng header: header cơ bản (basic header) và header mở rộng (extension header). Phần Header cơ bản có chiều dài cố định 40 byte, chứa những thông tin cơ bản trong xử lý gói tin IPv6, thuận tiện hơn cho việc tăng tốc xử lý gói tin. Những thông tin liên quan đến dịch vụ mở rộng kèm theo được chuyển hẳn tới một phân đoạn khác gọi là header mở rộng (extension header).

Cấu trúc một gói tin IPv6:



Hình 20: Cấu trúc gói tin IPv6

Mặc dù trường địa chỉ nguồn và địa chỉ đích trong IPv6 header có chiều dài 128 bít, gấp 4 lần số bít địa chỉ IPv4, song chiều dài header của IPV6 chỉ gấp hai lần header IPv4. Đó là nhờ dạng thức của header đã được đơn giản hoá đi trong IPV6 bằng cách bỏ bớt đi những trường không cần thiết và ít được sử dụng.

3.1.2.2 Những trường bỏ đi trong IPv6 header

Options: Một trong những thay đổi quan trọng là không còn tồn tại trường Options trong IPV6 header, do những thông tin liên quan đến dịch vụ kèm theo (vốn được mô tả bằng trường Options của header IPv4) được chuyển đặt riêng trong header mở rộng, theo sau header cơ bản. Vì vậy, chiều dài header cơ bản của IPv6 là cố định (40 byte).

Header Checksum: Trong IPv4 header, Header Checksum là một số sử dụng để kiểm tra lỗi trong thông tin header, được tính toán ra dựa trên những thông tin phần header. Do giá trị của trường TTL (Time to Live) thay đổi

mỗi khi gói tin được truyền qua một router, header checksum cần phải được tính toán lại mỗi khi gói tin đi qua một router IPv4. IPv6 đã giải phóng router khỏi công việc này, nhờ đó giảm được trễ. Do lớp TCP phía trên lớp IP có kiểm tra lỗi thông tin nên việc thực hiện phép tính tương tự tại tầng IP là không cần thiết và dư thừa, do vậy Header Checksum được loại bỏ khỏi IPv6 header.

Internet Header Length: Chiều dài phần header cơ bản của gói tin IPv6 cố định là 40 byte, do vậy không cần thiết có trường này.

Identification – Flags - Fragment Offset: Trong IPv4, đây là những trường phục vụ cho việc phân mảnh gói tin. Trong IPv6, thông tin về phân mảnh không bao gồm trong header cơ bản mà được chuyển hẳn sang một header mở rộng có tên gọi Fragment (Fragment extension header). Router IPv6 không tiến hành phân mảnh gói tin. Việc thực hiện phân mảnh do ứng dụng thực hiện ngay tại host nguồn. Do vậy, các thông tin hỗ trợ phân mảnh được bỏ đi khỏi phần header cơ bản là phần được xử lý tại các router và được chuyển sang phần header mở rộng, là phần được xử lý tại đầu cuối.

3.1.2.3 Những trường trong IPv6 header thực hiện chức năng tương tự IPv4 header

Version – 4 bít: Cùng tên với trường trong địa chỉ IPv4. Chỉ khác giá trị thể hiện địa chỉ phiên bản 6.

Traffic Class – 8 bít:: Thực hiện chức năng tương tự trường "Service Type" của địa chỉ IPv4. Trường này được sử dụng để biểu diễn mức ưu tiên của gói tin, ví dụ gói tin nên được truyền với tốc độ nhanh hay thông thường, hướng dẫn thiết bị thông tin xử lý gói một cách tương ứng.

Payload Length – 16 bít: Trường này thay thế cho trường Total length của địa chỉ IPv4. Tuy nhiên, nó chỉ xác định chiều dài phần dữ liệu (payload). Phần dữ liệu trong gói tin IPv6 được tính bao gồm cả header mở rộng. Bằng 16 bit, trường Payload Length có thể chỉ định chiều dài phần dữ liệu của gói tin IPv6 lên tới 65,535 byte.

Hop Limit - 8 bit: Thay thế trường Time to live của địa chỉ IPv4.

Next Header – 8 bít: Thay thế trường Protocol. Trường này chỉ định đến header mở rộng đầu tiên của gói tin IPv6 (nếu có) đặt sau header cơ bản, hoặc chỉ định tới thủ tục lớp trên như TCP, UDP, ICMPv6 khi trong gói tin IPv6 không có phần header mở rộng. Nếu sử dụng để chỉ định thủ tục lớp trên, trường này sẽ có giá trị tương tự như trường Protocol của địa chỉ IPv4.

Source Address: Địa chỉ nguồn, chiều dài là 128 bít.

Destination Address: Địa chỉ đích, chiều dài là 128 bít.

3.1.2.4 Trường thêm mới của IPv6 header

Flow Label: Trường Flow Label có chiều dài 20 bít, là trường mới được thiết lập trong IPV6. Trường này được sử dụng để chỉ định rằng gói tin thuộc một dòng (flow) nhất định giữa nguồn và đích, yêu cầu IPv6 router phải có cách xử lý đặc biệt. Flow Label được dùng khi muốn áp dụng chất lượng dịch vụ (Quality of Service - QoS[25]) không mặc định, ví dụ QoS cho dữ liệu thời gian thực (voice, video). Bằng cách sử dụng trường này, nơi gửi gói tin có thể xác định một chuỗi các gói tin, ví dụ gói tin của dịch vụ thoại VoIP, thành 1 dòng, và yêu cầu chất lượng

[25] QoS: Quality of Service: Khái niệm trong truyền tải lưu lượng, đảm bảo lưu lượng mạng đi đến đích theo một chất lượng nhất định (mức độ lỗi, thời gian truyền tải lưu lượng...)

dịch vụ cụ thể cho dòng đó. Theo mặc định, Flow Label được đặt giá trị 0. Có thể có nhiều dòng giữa nguồn và đích, sẽ được xác định bởi những giá trị tách biệt của Flow Label.

3.1.2.5 Header mở rộng (extension header) trong IPV6

Header mở rộng (extension header) là đặc tính mới của thế hệ địa chỉ IPV6.

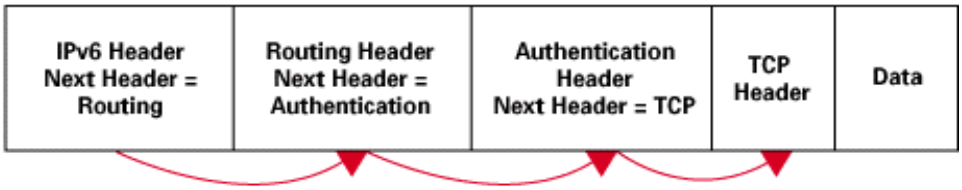
Trong IPv4, thông tin liên quan đến những đặc tính mở rộng (ví dụ xác thực, mã hoá) được để trong phần Options của IPv4 header. Địa chỉ IPv6 đưa những đặc tính mở rộng và các dịch vụ thêm vào thành một phần riêng, tách biệt khỏi header cơ bản của gói tin, được gọi là header mở rộng. Gói tin IPv6 có thể có một hay nhiều header mở rộng, được đặt sau header cơ bản. Các header mở rộng được đặt nối tiếp nhau theo thứ tự quy định, mỗi dạng có cấu trúc trường riêng.

Header cơ bản (kích thước 40 byte) trong gói tin IPv6 là phần thông tin được xử lý tại mọi router gói tin đi qua. Thông thường, các header mở rộng được xử lý tại đích. Tuy nhiên, cũng có dạng Header mở rộng được xử lý tại mọi router mà gói tin đi qua, đó là dạng header mở rộng Hop-by-Hop.

Trường Next Header trong các header IPv6:

Header cơ bản và mọi header mở rộng IPv6 đều có trường Next Header (chiều dài 8 bít).

Trong Header cơ bản, trường Next Header sẽ xác định gói tin có tồn tại header mở rộng hay không. Nếu không có, giá trị của trường sẽ xác định header của tầng cao hơn (TCP hay UDP, ..), phía trên tầng IP. Nếu có, giá trị trường Next Header chỉ ra loại header mở rộng đầu tiên theo sau header cơ bản. Tiếp theo, trường Next Header của Header mở rộng thứ nhất sẽ trỏ tới header mở rộng thứ hai, đứng kế tiếp nó. Trường Next Header của header mở rộng cuối cùng sẽ có giá trị xác định header tầng cao hơn.



Hình 21: Header mở rộng của địa chỉ IPv6

Giá trị Next header:

Giá trị Next Header	Dạng header mở rộng tương ứng
0	***Hop-By-Hop***
43	***Routing***
44	***Fragment***
50	***Encapsulating Security Payload (ESP)***

51	***Authentication Header (AH)***
60	***Destination***

Bảng 5: Giá trị Next-header

Hiện nay, có sáu dạng header mở rộng tương ứng sáu dịch vụ đang được định nghĩa: Hop-by-Hop, Destination, Routing, Fragment, Authentication, và ESP (Encapsulating Security Payload). Thứ tự các header mở rộng trong gói tin được đặt theo một quy tắc nhất định. Chúng ta sẽ tìm hiểu chi tiết về các header mở rộng, chức năng và thứ tự của chúng trong gói tin IPv6.

3.1.2.5.1 Các dạng header mở rộng

Dưới đây là những dạng header mở rộng hiện nay đang được định nghĩa cho địa chỉ IPV6. Nhờ tách biệt các dịch vụ gia tăng khỏi các dịch vụ cơ bản và đặt chúng trong header mở rộng, đồng thời phân loại header mở rộng theo chức năng, địa chỉ IPv6 đã giảm tải nhiều cho router, và thiết lập nên được một hệ thống cho phép bổ sung một cách linh động các chức năng, khi có những yêu cầu mới nảy sinh trong quá trình phát triển ứng dụng địa chỉ IPv6.

- **Hop-by-Hop**

Hop-by-Hop là header mở rộng được đặt đầu tiên ngay sau header cơ bản. Header này được sử dụng để xác định những tham số nhất định tại mỗi bước (hop) trên đường truyền dẫn gói tin từ nguồn tới đích. Do vậy sẽ được xử lý tại mọi router trên đường truyền dẫn gói tin.

- **Destination**

Header mở rộng Destination được sử dụng để xác định các tham số truyền tải gói tại đích tiếp theo hoặc đích cuối cùng trên đường đi của gói tin.

- Nếu trong gói tin có header mở rộng Routing, thì header mở rộng Destination mang thông tin tham số xử lý tại mỗi đích tới tiếp theo.
- Nếu trong gói tin không có header mở rộng Routing, thông tin trong header mở rộng Destination là tham số xử lý tại đích cuối cùng.

- **Routing**

Header mở rộng Routing đảm nhiệm xác định đường dẫn định tuyến của gói tin. Nếu muốn gói tin được truyền đi theo một đường xác định, chứ không tuỳ thuộc vào việc lựa chọn đường đi của các thuật toán định tuyến, node IPv6 nguồn có thể sử dụng header mở rộng routing để xác định tuyến, bằng cách liệt kê địa chỉ của các router mà gói tin phải đi qua. Các địa chỉ thuộc danh sách này sẽ được lần lượt dùng làm địa chỉ đích của gói tin IPV6 theo thứ tự được liệt kê và gói tin sẽ được gửi từ router này đến router khác, theo danh sách liệt kê trong header mở rộng Routing.

- **Fragment**

Header mở rộng Fragment mang thông tin hỗ trợ cho quá trình phân mảnh[26] và tái tạo gói tin IPv6. Header mở rộng Fragment được sử dụng khi nguồn IPV6 gửi đi gói tin lớn hơn giá trị MTU[27] nhỏ nhất trong toàn bộ đường dẫn từ nguồn tới đích. Trong hoạt động của địa chỉ IPV4, mọi router trên đường dẫn cần tiến hành phân mảnh gói tin theo giá trị của MTU đặt cho mỗi giao diện. Tuy nhiên, chu trình này áp đặt một gánh nặng lên router. Bởi vậy trong địa chỉ IPV6, router không thực hiện phân mảnh gói tin. Việc này được thực hiện tại nguồn gửi gói tin.

Node nguồn IPV6 sẽ thực hiện thuật toán tìm kiếm giá trị MTU nhỏ nhất trên toàn bộ một đường dẫn nhất định từ nguồn tới đích (gọi là giá trị Path MTU)[28], và điều chỉnh kích thước gói tin tuỳ theo giá trị này trước khi gửi chúng. Nếu ứng dụng tại nguồn áp dụng phương thức này, nó sẽ gửi dữ liệu có kích thước tối ưu, và không cần thiết xử lý tại tầng IP. Tuy nhiên, nếu ứng dụng không sử dụng phương thức này, nó phải chia nhỏ gói tin có kích thước lớn hơn Path MTU. Trong trường hợp đó, những gói tin này cần được phân mảnh tại tầng IP của node nguồn và header mở rộng Fragment được sử dụng để mang những thông tin phục vụ cho quá trình phân mảnh và tái tạo gói tin IPv6 tại các đầu cuối đường kết nối.

- **Authentication and ESP** (Encapsulating Security Payload)

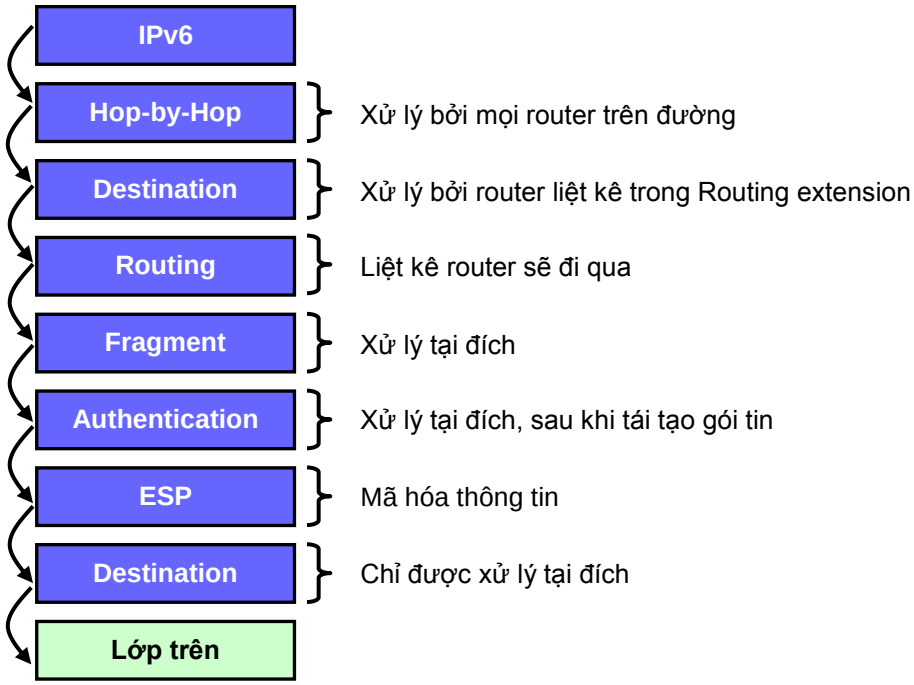
IPSec[29] là phương thức mã hóa bảo mật dữ liệu tại tầng IP được sử dụng phổ biến (ví dụ khi thực hiện VPN[30]). Trong thế hệ địa chỉ IPv4, khi có sử dụng IPsec trong bảo mật kết nối dạng đầu cuối - đầu cuối, thông tin hỗ trợ bảo mật và mã hóa được đặt trong trường Option của header IPv4.

Trong hoạt động của địa chỉ IPv6, thực thi IPsec được coi là một đặc tính bắt buộc. Tuy nhiên, IPsec có thực sự được sử dụng trong giao tiếp hay không tùy thuộc vào từng trường hợp. Khi IPsec được sử dụng, gói tin IPv6 cần có các dạng header mở rộng Authentication và ESP. Authentication header dùng để xác thực và bảo mật tính đồng nhất của dữ liệu, ESP header dùng để xác định những thông tin liên quan đến mã hoá dữ liệu.

3.1.2.5.2 Thứ tự đặt các header mở rộng

Khi sử dụng cùng lúc nhiều header mở rộng, các header mở rộng này sẽ có thứ tự như sau trong gói tin IPv6:

[26] Tham khảo mục II.3.7 về phân mảnh gói tin IPv6
[27] MTU: Maximum Transmission Unit – Kích thước gói tin lớn nhất có thể truyền tải trên một đường kết nối.
[28] Tham khảo mục II.3.7 về quá trình tìm kiếm giá trị MTU nhỏ nhất trên toàn bộ đường kết nối (PathMTU của IPv6).
[29] IPSec: Công nghệ cung cấp bảo mật, xác thực và những dịch vụ an ninh khác tại tầng IP.
[30] VPN: Virtual Private Network. Được nhắc tới như một mạng trong đó có các phần mạng cách nhau bởi vị trí địa lý được kết nối thông qua Internet công cộng song dữ liệu truyền qua Internet được mã hoá, do vậy toàn bộ mạng được xem như một mạng riêng "ảo"



Hình 22: Thứ tự xử lý các header mở rộng

Host đích sẽ tiến hành xử lý các header mở rộng lần lượt, theo đúng thứ tự của chúng trong gói tin IPv6.

3.2 ĐẶC TÍNH ƯU VIỆT CỦA GIAO THỨC IPV6

3.2.1 Tổng quát chung

Giao thức Internet thế hệ sau, IPv6, được phát triển do nguyên nhân về nguy cơ cạn kiệt không gian địa chỉ IPv4. Tuy nhiên, đó không phải là lí do duy nhất. Hoạt động Internet đã đến thời điểm cần có giao thức ưu việt hơn, đáp ứng được các yêu cầu về dịch vụ càng ngày phong phú trên mạng Internet, cũng như xu hướng tích hợp mạng Internet với mạng viễn thông, cung cấp đa dạng dịch vụ trên một cơ sở hạ tầng mạng thống nhất. Giao thức IPv6 có nhiều đặc tính ưu việt, được cải tiến so với thế hệ trước - IPv4. Trong đó, nhiều đặc tính đã được tiêu chuẩn hóa, cũng còn nhiều đặc tính chưa được tiêu chuẩn hóa hoàn thiện, cần tiếp tục phát triển; nhiều đặc tính được áp dụng rộng rãi và bắt buộc khi IPv6 hoạt động, một số còn chưa được áp dụng rộng rãi. Tuy nhiên có một điểm chắc chắn, IPv6 sẽ được sử dụng, đóng góp trong mạng thế hệ mới, và phát huy những ưu điểm của mình.

Giao thức IPv6 được nhắc đến với những đặc tính sau:

- ***Không gian địa chỉ rộng lớn hơn***

Mở rộng không gian địa chỉ là một trong những lí do chính để phát triển thế hệ địa chỉ IPv6. Địa chỉ IPv6 có chiều dài 128 bít, gấp 4 lần chiều dài bít của địa chỉ IPv4. Về lý thuyết, mở rộng không gian địa chỉ từ 4 tỉ lên tới một con số khổng lồ ($2^{128} = 3{,}4 \times 10^{38}$) địa chỉ. Một số nhà phân tích tính toán và kết luận rằng, cho dù sử dụng như thế nào, chúng ta cũng không thể dùng hết địa chỉ IPv6. Nếu trong chính sách quản lý địa chỉ IPv4, mục tiêu cơ bản cần đạt được là "sử dụng hiệu quả" thì đối với IPv6, mục tiêu này không còn được đặt lên hàng đầu, thay vào đó là "tính tổ hợp". Song gần đây, nhiều nhà phân tích cho rằng, quản lý địa chỉ IPv6 cần phải thắt chặt hơn, ở thời điểm này chúng ta chưa thể lường trước được mạng Internet sẽ phát triển như thế nào, cũng giống như tại thời điểm ban đầu của IPv4, người ta đã buông lỏng, không quản lý chặt chẽ không gian địa chỉ. Do vậy, gần đây, các chính sách quản lý địa chỉ IPv6 đang được điều chỉnh thích hợp hơn.

- ***Phân cấp đánh địa chỉ và phân cấp định tuyến rõ rệt hơn***

Đối với địa chỉ IPv4, chúng ta có thể sử dụng bất cứ độ dài tiền tố (prefix) nào trong phạm vi 32 bít. Việc đánh địa chỉ IPv4 vừa có tính phân cấp, vừa không phân cấp. Chính điều này làm ảnh hưởng tới khả năng tổ hợp định tuyến và đem lại nguy cơ gia tăng bảng thông tin định tuyến toàn cầu. Địa chỉ IPv6 được thiết kế có một cấu trúc đánh địa chỉ và phân cấp định tuyến thống nhất. Ví dụ trong 128 bít địa chỉ, 64 bít cuối cùng được sử dụng làm định danh giao diện. Một mạng con nhỏ nhất (subnet) có kích thước /64. 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 với chiều dài địa chỉ lên tới 128 bít.

- ***Đơn giản hóa dạng thức của header***

IPv6 header có dạng thức mới, không tương thích với header IPv4. Host hoặc router phải thực thi cả IPv4 và IPv6 để có khả năng nhận dạng và xử lý cả hai dạng header.

Mặc dù chiều dài bít địa chỉ IPv6 gấp 4 lần chiều dài bít IPv4, kích thước header IPv6 chỉ gấp 2 lần IPv4. Những trường không thiết yếu được bỏ đi và các tùy chọn (option) được đưa thành phần header mở rộng (extension header) đặt sau header cơ bản. Phần header cơ bản có kích thước cố định giúp tăng hiệu quả xử lý cho router. Việc

đặt các tuỳ chọn sang header mở rộng cho phép nâng cao tính linh hoạt, có thể có những tuỳ chọn mới trong tương lai.

- ***Khả năng cấu hình địa chỉ tự động và đánh số lại***

Để có thể gán địa chỉ và những thông số hoạt động cho IPv6 host khi nó kết nối vào mạng mà không cần nhân công cấu hình bằng tay, có thể sử dụng DHCPv6. Đây được gọi là dạng thức cấu hình tự động có trạng thái (stateful autoconfiguration). Bên cạnh đó, IPv6 host còn có khả năng tự động cấu hình địa chỉ và các thông số hoạt động mà không cần có sự hỗ trợ của máy chủ DHCP. Đó là đặc điểm mới trong thế hệ địa chỉ IPv6, được gọi là dạng thức cấu hình không trạng thái (stateless autoconfiguration)[31] .

- ***Hỗ trợ cho chất lượng dịch vụ (Quality-of-service)***

IPv6 header có một trường mới Flow Label cho phép định dạng lưu lượng IPv6. Flow Label cho phép router định dạng và cung cấp cách thức xử lý đặc biệt những gói tin thuộc một dòng (flow) nhất định giữa nguồn và đích. Ví dụ, nơi gửi có thể yêu cầu chất lượng dịch vụ khác mặc định cho dịch vụ dạng thời gian thực.

- ***Hỗ trợ bảo mật (IP Sec)***

Khả năng hỗ trợ bảo mật trong địa chỉ IPv6 sử dụng các header mở rộng authentication và encryption extension header và một số đặc tính khác.

- ***Thủ tục mới cho giao tiếp giữa các Node lân cận trên một đường link***

Trong hoạt động của địa chỉ IPv6, trao đổi, giao tiếp giữa các node trong một đường kết nối là vô cùng quan trọng. Địa chỉ IPv6 có một thủ tục mới, phụ trách hoạt động giao tiếp này, có tên gọi Neighbor Discovery (ND). ND sử dụng một chuỗi các thông điệp ICMPv6, phụ trách các quy trình giao tiếp giữa các IPv6 node trên một đường kết nối, thực hiện chức năng của các thủ tục sau đây trong địa chỉ IPv4: thủ tục phân giải địa chỉ Address Resolution Protocol (ARP), thủ tục tìm kiếm router ICMPv4 Router Discovery, ICMPv4 Redirect và một số chức năng khác nữa. [32]

- ***Khả năng mở rộng (Extensibility)***

Địa chỉ IPv6 được thiết kế có tính năng mở rộng. Các tính năng mở rộng được đặt trong một phần header mở rộng riêng sau header cơ bản. Không giống như IPv4 header, chỉ có thể hỗ trợ 40 byte cho phần tuỳ chọn (Option), địa chỉ IPv6 có thể dễ dàng có thêm những tính năng mới bằng cách thêm những header mở rộng sau header cơ bản.

3.2.2 Quality-of-Service (QoS) trong thế hệ địa chỉ IPv6

Trong hoạt động mạng, "Chất lượng - Quality" tức là truyền tải dữ liệu "tốt hơn mức bình thường". Bao gồm: độ mất dữ liệu, trễ (hay còn gọi độ dịch - jitter), băng thông... "Dịch vụ - Service" là những gì cung cấp cho người sử dụng, có thể là kết nối đầu cuối - đầu cuối, các ứng dụng chủ - khách, truyền tải dữ liệu ....

[31] Tham khảo mục III.3.5 về tự động cấu hình địa chỉ không trạng thái (Stateless Autoconfiguration) của thiết bị IPv6.
[32] Tham khảo mục III.2 về thủ tục Neighbor Discovery

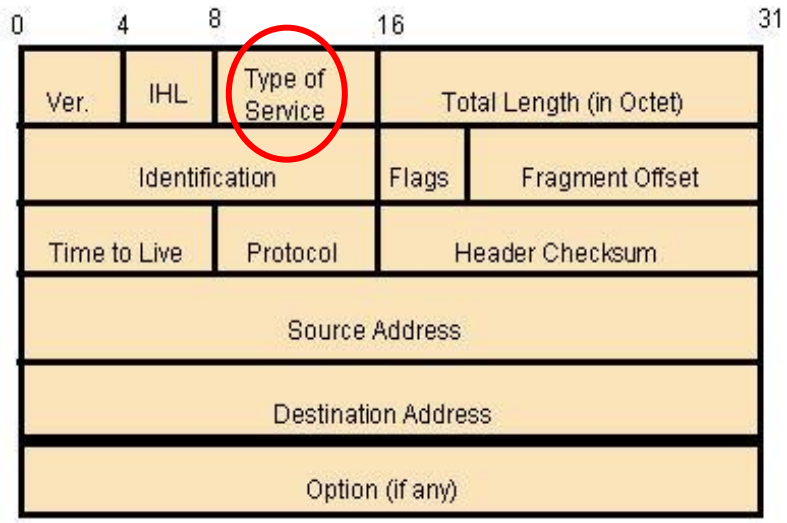
Một cách lý thuyết, QoS được nhắc đến là phương thức đo đạc cách thức cư xử của mạng (của các router) đối với lưu lượng, trong đó có để ý tới những đặc tính nhất định của những dịch vụ xác định. Thông tin để router thiết lập cách thức cư xử cụ thể đối với gói tin có thể được chuyển tới bằng một thủ tục điều khiển, hoặc bằng chính thông tin chứa trong gói tin.

3.2.2.1 Hỗ trợ QoS trong địa chỉ IPv4

Header của địa chỉ IPv4 có trường Service Type 8 bít, được sử dụng để phân định mức độ ưu tiên và một số giá trị khác dành cho lưu lượng IPv4.

Trong số 8 bít của trường Service Type:

- 3 bít đầu xác định độ ưu tiên (precedence) của gói tin . Với 3 bít, có thể có 8 mức độ ưu tiên khác nhau đối với lưu lượng IPv4.
- 4 bít tiếp theo được gọi là ToS (Type of Service) giúp xác định dịch vụ và một số các thông số khác như độ trễ, thông lượng, độ tin cậy.



Hình 23: Hỗ trợ QoS trong địa chỉ IPv4

Tuy nhiên, sử dụng các giá trị của Service Type trong việc phân định loại dịch vụ và mức ưu tiên phục vụ cho QoS có một số vấn đề như sau:

- Trường này cung cấp một mô hình cố định và hạn chế trong việc phân dạng loại dịch vụ
- Về giá trị độ ưu tiên: Chỉ mã hoá một cách tương đối mức ưu tiên

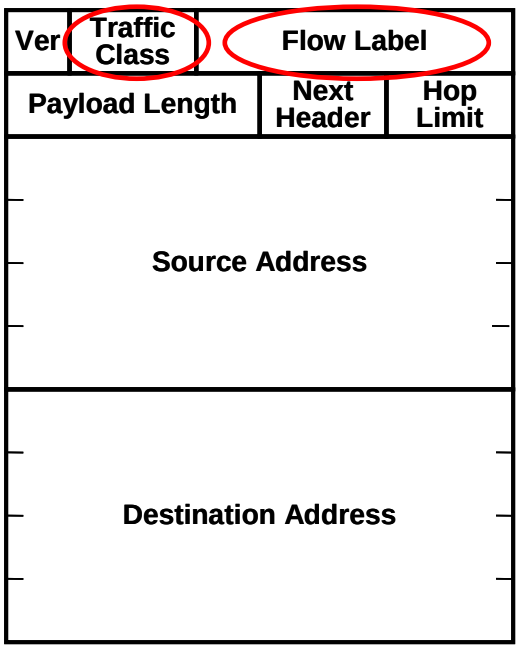
Do mô hình hoạt động, địa chỉ IPv4 còn có những hạn chế như sau trong hỗ trợ QoS:

- Phân mảnh gói tin trong IPv4: Việc thực hiện phân mảnh gói tin tại router là một vấn đề điển hình của IPv4. Nó dẫn đến khả năng làm tắc nghẽn mạng, tiêu tốn bằng thông và CPU của thiết bị.
- Quá tải về quản lý: ICMPv4 có quá nhiều tuỳ chọn

Những yếu tố đó ảnh hưởng đến khả năng hỗ trợ QoS trong IPv4, đặc biệt trong phạm vi rộng lớn.

3.2.2.2 Hỗ trợ QoS trong địa chỉ IPv6

Địa chỉ IPv6 được thiết kế có một cấu trúc hỗ trợ tốt hơn cho QoS:



Hình 24: Hỗ trợ QoS trong địa chỉ IPv6

IPv6 header có hai trường dữ liệu Traffic Class (8 bít) và Flow label (20 bít) được sử dụng để phục vụ QoS. IPv6 node có thể sử dụng hai trường này để phân dạng gói tin và yêu cầu IPv6 router có những cách cư xử đặc biệt nào đó.

Traffic Class: Trường Traffic Class thực hiện chức năng tương tự trường "Service Type" của địa chỉ IPv4. Trường này được sử dụng để biểu diễn mức ưu tiên của gói tin. Node gửi gói tin cần thiết lập giá trị phân loại độ ưu tiên nhất định cho gói tin IPv6, sử dụng trường Traffic Class. Router khi xử lý chuyển tiếp gói tin cũng sử dụng trường này cho mục đích tương tự.

Đối với thế hệ địa chỉ IPv6, trường Traffic Class với số bít nhiều hơn sẽ giúp phân định tốt hơn mức độ ưu tiên cho gói tin.

Flow Label

Trường Flow Label sử dụng để định danh một dòng dữ liệu giữa nguồn và đích. Flow Label là trường mới của IPv6 header, khi được sử dụng, trường này sẽ hỗ trợ tốt hơn thực thi QoS. Một nguồn IPv6 có thể sử dụng 20 bít flow label trong IPv6 header làm số định danh để xác định gói tin gửi đi trong một dòng nhất định, yêu cầu cách thức cư xử đặc biệt của router, ví dụ yêu cầu chất lượng khác mặc định cho những dịch vụ thời gian thực.

Khái niệm một dòng (flow):

Một dòng là một chuỗi các gói tin được gửi từ một nguồn tới một đích nhất định. Nguồn sẽ yêu cầu các router có các cư xử đặc biệt đối với các gói tin thuộc một dòng. Tham số xác định cách thức cư xử đối với gói tin có thể được truyền tới router bằng một thủ tục điều khiển, hoặc có thể là thông tin chứa trong chính gói tin của dòng, ví dụ các thông số trong header mở rộng hop-by-hop của gói tin.

Giữa một nguồn và một đích có thể có nhiều dòng. Việc kết hợp giữa địa chỉ nguồn và một số Flow Label khác 0 sẽ xác định một dòng duy nhất. Những gói tin không thuộc dòng nào cả sẽ được thiết lập toàn bộ các bít Flow Label có giá trị 0.

Mọi gói tin thuộc một dòng sẽ có cùng địa chỉ nguồn, cùng địa chỉ đích, và cùng một số Flow Label khác 0. Router xử lý gói tin sẽ thiết lập trạng thái xử lý đối với một số Flow Label cụ thể. Router có thể lựa chọn lưu trữ (cache) thông tin, sử dụng giá trị địa chỉ nguồn và flow label làm khoá. Đối với những gói tin sau đó, có cùng địa chỉ nguồn và giá trị flow label, router có thể áp dụng cách thức xử lý dựa trên thông tin hỗ trợ từ vùng cache.

Tại thời điểm hiện nay, việc sử dụng trường Flow Label trong thực thi QoS cho IPv6 vẫn nằm ở mức thử nghiệm, các tiêu chuẩn hoá đối với trường này còn chưa hoàn thiện và chưa có một cấu trúc thông dụng cho việc sử dụng nó. Nhiều router, host chưa hỗ trợ việc sử dụng trường Flow Label. IETF đang tiếp tục tiêu chuẩn hoá và đưa ra những yêu cầu rõ ràng hơn về hỗ trợ trường Flow Label. Đối với những router và host chưa hỗ trợ trường này, toàn bộ các bít của trường Flow Label sẽ được thiết lập giá trị 0 và router, host bỏ qua trường đó khi nhận được gói tin.

Những cải tiến trong IPv6 header, cùng với những ưu điểm khác của IPv6 như: không phân mảnh, định tuyến phân cấp, đặc biệt gói tin IPv6 được thiết kế với mục đích xử lý thật hiệu quả tại router. Tất cả tạo ra khả năng hỗ trợ tốt hơn cho chất lượng dịch vụ QoS. Tuy nhiên để đạt tới trạng thái hoàn thiện và sử dụng rộng rãi thống nhất, còn cần thời gian và công sức của những tổ chức nghiên cứu và tiêu chuẩn hoá.

3.2.3 Hỗ trợ tốt hơn về bảo mật (Security) trong thế hệ địa chỉ IPv6

Internet hiện nay gặp nhiều vấn đề về bảo mật, một phần do thiếu phương thức hiệu quả để xác thực và bảo vệ tính riêng tư dưới tầng ứng dụng. Trong hoạt động Internet, bảo mật tại tầng IP được thực hiện phổ biến bằng công nghệ IPSec.

IPSec thực hiện chức năng xác thực nơi gửi và mã hóa đường kết nối, do vậy đảm bảo có kết nối bảo mật. IPSec có hai phương thức làm việc: “tunnel mode” và “transport mode”. Tunnel mode áp dụng IPSec bằng cách: thiết bị thực hiện IPSec (ví dụ firewall) sẽ thêm một header mới và lấy toàn bộ gói tin IP trước kia làm phần dữ liệu (payload). Chế độ này thường được sử dụng trong VPN, sử dụng hai thiết bị thực hiện Ipsec bảo mật giữa hai mạng. Transport mode áp dụng IPSec cho truyền gói tin IP bởi host, được sử dụng trong bảo mật kết nối đầu cuối - đầu cuối giữa các node.

Về cấu trúc IP Sec bao gồm hai thủ tục bảo mật Authentication Header (AH) và Encapsulating Security Payload (ESP), các cơ sở dữ liệu lưu trữ tham số và chính sách về bảo mật và các thủ tục để trao đổi khóa.

Công nghệ IPSec hỗ trợ cả địa chỉ IPv4 và IPv6. Tuy nhiên, trong IPv6, thực thi 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 hai đặc tính là hai header mở rộng của địa chỉ IPv6. Đó là *Authentication Header (AH)* và *Encapsulating Security Payload* (ESP). Hai header này có thể được sử dụng cùng lúc, hoặc riêng rẽ để cung cấp các mức bảo mật khác nhau cho những người sử dụng khác nhau.

- *Authentication Header* (AH) cung cấp dịch vụ chứng thực. Mở rộng này hỗ trợ nhiều công nghệ chứng thực khác nhau. Sử dụng AH loại bỏ được nhiều dạng tấn công mạng, bao gồm cả tấn công giả mạo host.
- *Encapsulating Security Payload* (ESP) cung cấp dịch vụ bảo đảm tính toàn vẹn và tính tin cậy cho gói tin IPv6. Mặc dù đơn giản hơn một số thủ tục bảo mật tương tự, song ESP vẫn giữ được tính mềm dẻo và không phụ thuộc vào thuật toán.

Cấu trúc của IPSec trong IPv6 cũng được cải tiến, ví dụ trong thủ tục trao đổi khóa, phục vụ cho bảo mật.

Trong hoạt động mạng IPv4, công nghệ biên dịch địa chỉ NAT được sử dụng vô cùng rộng rãi. Thiết bị thực hiện NAT can thiệp và thay đổi header của gói tin, điều này gây cản trở trong việc thực hiện IPSec. Thế hệ địa chỉ IPv6 với không gian địa chỉ vô cùng rộng lớn được mong chờ rằng IPSec sẽ được sử dụng rộng rãi trong các giao tiếp đầu cuối – đầu cuối.

IPSec được coi là một trong những đặc tính cơ bản của địa chỉ IPv6. Chúng ta rất hay gặp những kết luận "IPv6 tăng cường độ bảo mât, IPsec là bắt buộc". Tuy nhiên tại thời điểm hiện nay, dù nhiều hệ điều hành có hỗ trợ IPSec, việc sử dụng IPSec trong IPv6 cho kết nối đầu cuối – đầu cuối là chưa phổ biến. Một trong những nguyên nhân là do mô hình kết nối có firewall hiện nay và thói quen sử dụng những thủ tục bảo mật tại tầng ứng dụng khiến cho việc áp dụng IPSec cho kết nối đầu cuối – đầu cuối chưa phổ biến. Nhóm làm việc của IETF vẫn đang thực hiện sửa đổi hoàn thiện các tiêu chuẩn hóa liên quan đến IPSec như về AH, ESP và nỗ lực tiến tới mục đích mọi IPv6 node đều có khả năng IPSec, đưa IPSec phổ dụng cùng với sự phổ biến ngày càng nhiều của địa chỉ IPv6.

Hỏi – đáp cuối chương 3:

1. Khác với địa chỉ IPv4, địa chỉ IPv6 có hai dạng header, là hai dạng header nào?

T: Địa chỉ IPv6 có hai dạng header. Đó là header cơ bản và header mở rộng (extension header).

2. Tại sao phần header cơ bản của địa chỉ IPv6 có chiều dài cố định?

T Trong địa chỉ IPv4, các dịch vụ tuỳ chọn kèm theo được thêm vào bởi các trường Option của IPv4 header. Trường Option không có độ dài cố định do vậy chiều dài của IPv4 header là không cố định. Địa chỉ IPv6 được thiết kế nâng cấp. Các dịch vụ tùy chọn được thêm vào bằng header mở rộng tách biệt khỏi header cơ bản. Do đó phần header cố định của địa chỉ IPv6 có chiều dài cố định 40 byte. Đó là một ưu điểm của IPv6 khiến router xử lý gói tin dễ dàng hiệu quả hơn.

3. Nếu gói tin IPv6 được phân mảnh, phần IPv6 header của gói tin sẽ có thêm dạng header mở rộng nào?

T Đó là header mở rộng fragment. Router IPv6 không đảm nhiệm phân mảnh gói tin. Gói tin IPv6 được phân mảnh tại đầu cuối. Host nguồn và host đích sẽ thực hiện xử lý header mở rộng này.

4. Trong hầu hết trường hợp, router IPv6 không xử lý các header mở rộng. Tuy nhiên dạng header mở rộng nào sẽ được xử lý tại mọi node trên đường truyền dẫn?

T Hop-by-Hop là header mở rộng xác định những tham số nhất định tại mỗi bước trên đường truyền dẫn từ nguồn tới đích. Do vậy sẽ được xử lý tại mọi router trên đường truyền dẫn gói tin. Do IPv6 node xử lý các header mở rộng theo thứ tự nằm trong gói tin IPv6 nên header mở rộng này luôn được đặt ngay sau header cơ bản.

CHƯƠNG 4: CÁC THỦ TỤC VÀ QUY TRÌNH HOẠT ĐỘNG CƠ BẢN

Thủ tục lớp mạng (Internet Protocol –IP) cung cấp phương thức để kết nối những mạng nội bộ riêng rẽ thành một mạng lớn hơn, được gọi là liên mạng (internetwork). Những thủ tục lớp cao coi liên mạng như một mạng nội bộ phạm vi rộng lớn, bởi vì những lớp thấp hơn đã giấu đi những chi tiết "liên kết" những mạng nhỏ riêng biệt thành liên mạng. Trên phương diện các thủ tục lớp cao và các ứng dụng, các thiết bị coi nhau như những đối tượng ngang hàng. Tuy nhiên trên phương diện các lớp thấp hơn, có một sự khác biệt rất quan trọng giữa thiết bị thuộc mạng nội bộ và những thiết bị bên ngoài. Thiết bị thuộc mạng nội bộ sẽ có những giao tiếp đặc biệt với nhau.

Thế hệ địa chỉ IPv4, để hỗ trợ những giao tiếp này và những yêu cầu hoạt động khác, bên cạnh thủ tục Internet Protocol (version 4), có nhiều thủ tục hỗ trợ khác như ARP[33] cho phép thiết bị phân giải địa chỉ lớp hai từ địa chỉ lớp ba; thủ tục ICMP[34] cung cấp các thông điệp điều khiển, hỗ trợ giao tiếp. Những thủ tục và quy trình hoạt động này hiện đang phục vụ tốt cho hoạt động mạng với phiên bản IPv4, tuy nhiên, cũng tồn tại nhiều hạn chế.

Thủ tục IP phiên bản 6 có những thay đổi lớn, thực hiện tiêu chuẩn hoá và tổ hợp nhiều chức năng, quy trình riêng biệt của giao tiếp giữa những thiết bị nội bộ. Đối với hoạt động của một mạng máy tính được gắn địa chỉ IPv6, giao tiếp giữa các node trên một đường kết nối là vô cùng quan trọng. Do vậy, IPv6 phát triển một thủ tục mới đảm nhiệm giao tiếp giữa những node thuộc một đường kết nối (được khái niệm hoá là những node lân cận), có tên gọi IPv6 Neighbor Discovery – ND. Địa chỉ IPv6 cũng thực hiện đồng nhất hoá các thông điệp sử dụng trong quá trình giao tiếp nội bộ. Toàn bộ những quy trình giao tiếp này sử dụng các thông điệp ICMPv6[35]. Ba thủ tục ICMPv6, ND[36] (Neighbor Discovery), MLD[37] (Multicast Listener Discovery) là những thủ tục thiết yếu cho hoạt động của IPv6. Trong đó MLD và ND hoạt động trên nền các thông điệp ICMPv6.

Phần nội dung này mô tả với bạn đọc các thủ tục và quy trình hoạt động cơ bản của địa chỉ IPv6. Qua đó, giúp bạn đọc hình dung được cách thức hoạt động của thế hệ địa chỉ mới IPv6, những đặc tính của địa chỉ IPv6. Để minh hoạ lý thuyết, bạn đọc sẽ được hướng dẫn thực hiện một bài thực hành quan sát giao tiếp và hoạt động của các node IPv6 trên một đường kết nối.

Chương bốn bao gồm những nội dung chính sau:

- Thủ tục ICMPv6 (Internet control message protocol version 6)
- Thủ tục Neighbor Discovery (ND)
- Một số quy trình hoạt động cơ bản trong IPv6

---

[33] ARP: Address Resolution Protocol - Thủ tục phân giải địa chỉ, sử dụng trong IPv4 để phân giải địa chỉ IPv4 thành địa chỉ lớp hai tương ứng, ví dụ địa chỉ Ethernet MAC.

[34] ICMP: Internet Control Message Protocol - Thủ tục của những thông điệp điều khiển, sử dụng trao đổi những thông điệp báo lỗi giao tiếp, thông điệp chẩn đoán mạng trong hoạt động của IP.

[35] ICMPv6 : Internet Control Message Protocol version 6

[36] ND: Neighbor Discovery - Một thủ tục mới, được phát triển trong hoạt động IPv6. ND sử dụng các thông điệp ICMPv6 để đảm nhiệm các quy trình giao tiếp cần thiết giữa các node trên một đường kết nối như quy trình phân giải địa chỉ (thực hiện bằng thủ tục ARP trong IPv4), quy trình tìm kiếm router …

[37] MLD: Multicast Listener Discovery – Là một thủ tục, sử dụng các thông điệp ICMPv6, cho phép các router khám phá ra những địa chỉ IPv6 multicast nào đang được « nghe » lưu lượng trên một đường kết nối.

- Thủ tục multicast listener discovery (MLD)
- Hướng dẫn thực hành quan sát giao tiếp và hoạt động của các node IPv6.

4.1 THỦ TỤC ICMPV6 (INTERNET CONTROL MESSAGE PROTOCOL VERSION 6)

4.1.1 Tổng quát về vai trò của thủ tục ICMPv6 trong hoạt động của IPv6

Trong hoạt động Internet phiên bản 4, Internet Control Message Protocol (ICMP), là một thủ tục của các thông điệp điều khiển, hỗ trợ cho hoạt động mạng. Các thông điệp ICMP, truyền tải bằng những gói tin, được sử dụng trong IPv4 với mục đích báo lỗi và điều khiển truyền tải IP, cũng như thực hiện những chức năng chẩn đoán mạng. Thông điệp ICMP phân loại thành hai dạng: thông điệp lỗi, hoặc thông điệp "hỏi - đáp". Khi có lỗi xảy ra trong quá trình truyền tải gói tin IP, router đang xử lý hoặc node nhận gói tin sẽ thông báo vấn đề cho node gửi để node gửi có thể truyền lại gói tin hoặc tiếp tục thực hiện những chu trình xử lý lỗi khác. Những chương trình dò tìm như ping, traceroute sử dụng những thông điệp "hỏi - đáp" của ICMP để thực hiện chẩn đoán mạng. Thông điệp ICMP cũng phục vụ cho quá trình redirect, là quá trình router thông báo cho host về một đích tiếp theo (next hop) tốt hơn để chuyển lưu lượng tới một đích nhất định.

Một số chức năng của ICMP:

- Thông báo lỗi mạng.
- Thông báo tắc nghẽn mạng.
- Hỗ trợ xử lý sự cố, cho các chương trình chẩn đoán mạng.
- Thông báo thời gian hết thời gian sống của gói tin.
- Thực hiện redirect.

Trong hoạt động Internet phiên bản 6, ICMPv6 được tổ hợp với IPv6. Mọi node hỗ trợ IPv6 phải thực thi hoàn toàn ICMPv6. ICMPv6 là phiên bản được biến đổi, nâng cấp của ICMP trong IPv4.

Phiên bản 4, ICMP chỉ bao gồm các thông điệp điều khiển, hỗ trợ hoạt động mạng. Còn các quy trình hoạt động cần thiết khác được đảm nhiệm bằng những thủ tục riêng. Ví dụ: quá trình phân giải địa chỉ được đảm nhiệm bằng thủ tục ARP. Nếu IPv4 host tham gia vào quá trình định tuyến multicast[38], việc quản lý quan hệ thành viên nhóm multicast được đảm nhiệm bằng thủ tục IGMP[39], sử dụng tập hợp thông điệp riêng.

Phiên bản địa chỉ IPv6 thực hiện quy chuẩn hoá các thông điệp phục vụ cho những quy trình hoạt động trong mạng nội bộ. Các quy trình hoạt động, giao tiếp giữa các node IPv6 trong một mạng nội bộ, bao gồm quá trình phân giải từ địa chỉ lớp hai thành địa chỉ lớp 3 và nhiều quy trình khác được đảm nhiệm bằng thủ tục mới – ND (Neighbor Discovery). Toàn bộ những thông điệp sử dụng trong các quá trình này là thông điệp ICMPv6. Nếu node IPv6 tham gia vào quá trình định tuyến multicast, thì việc quản lý quan hệ thành viên nhóm multicast được đảm nhiệm bằng thủ tục MLD (Multicast Listener Discovery). Thủ tục này cũng sử dụng các thông điệp ICMPv6.

[38] Multicast: Công nghệ cho phép gửi một gói tin IP đồng thời tới một nhóm xác định các thiết bị mạng. Các thiết bị mạng này có thể thuộc nhiều tổ chức và định vị ở các vị trí địa lý khác nhau.

[39] IGMP: Internet Group Management Protocol - Thủ tục sử dụng trong công nghệ multicast IPv4 để thiết lập quan hệ thành viên nhóm multicast trong một mạng. Thủ tục này cho phép một host thông báo với router trên mạng của nó rằng nó muốn nhận lưu lượng của một địa chỉ multicast nhất định.

Do vậy, thủ tục ICMPv6 và những thông điệp ICMPv6 đóng vai trò vô cùng quan trọng trong hoạt động của thế hệ địa chỉ IPv6. Các quy trình giao tiếp cốt yếu giữa host với host, giữa host với router IPv6 trên một đường kết nối, vốn là nền tảng cho hoạt động của IPv6 node, đều dựa trên việc trao đổi các thông điệp ICMPv6.

So với IPCMv4, ICMPv6 được đơn giản hoá bằng cách bỏ bớt đi những dạng thông điệp không hoặc hiếm khi sử dụng, nhưng lại đảm nhiệm nhiều chức năng hơn ICMPv4. Thông điệp ICMPv6 ngoài thực hiện chức năng báo lỗi, chẩn đoán, điều khiển hoạt động mạng, còn phục vụ cho nhiều quy trình không tồn tại trong IPv4 hoặc được cung cấp bởi các thủ tục riêng trong IPv4, ví dụ thực thi quá trình phân giải địa chỉ.

ICMPv6 được mô tả trong RFC2463[40]. Do thông điệp ICMPv6 được sử dụng trong các quy trình hoạt động của hai thủ tục cốt yếu khác của IPv6, nên ICMPv6 được coi là cung cấp cơ cấu hoạt động cho hai thủ tục này. Đó là :

- Multicast Listener Discovery (MLD) - Thủ tục quản lý quan hệ thành viên multicast, phục vụ cho định tuyến multicast
- Neighbor Discovery (ND) - Đảm nhiệm thực thi giao tiếp giữa các node trong một đường kết nối.

4.1.2 Phân loại thông điệp ICMPV6

4.1.2.1 Gói tin ICMPv6

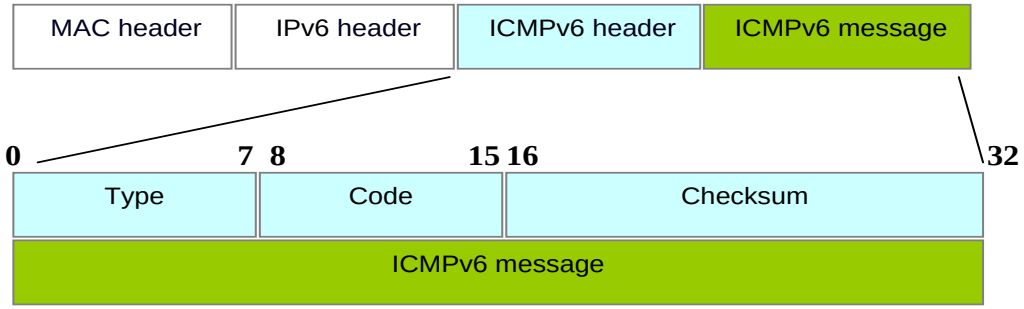
Gói tin ICMPv6 bắt đầu sau header cơ bản hoặc một header mở rộng của IPv6 và được xác định bởi giá trị trường Next-Header 58 của header IPv6 này. Gói tin ICMPv6 bao gồm phần ICMPv6 header và phần thông điệp (ICMPv6 message).

ICMPv6 header bao gồm ba trường: Type (8 bít), Code (8 bít) và Checksum (16 bít)

Hai trường Type và Code của ICMPv6 header được sử dụng để phân loại thông điệp ICMPv6.

- ***Type***: Giá trị bít đầu tiên của trường type sẽ xác định đây là thông điệp lỗi, hay thông điệp thông tin.
- ***Code:*** 8 bít trường code sẽ phân dạng sâu hơn gói tin ICMPv6, định rõ đây là gói tin dạng gì trong từng loại thông điệp ICMPv6.

Trường Checksum cung cấp giá trị sử dụng để kiểm tra lỗi cho toàn bộ gói tin ICMPv6.



Hình 25: Cấu trúc gói tin ICMPv6

[40] RFC2463 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Cũng như ICMPv4, ICMPv6 được sử dụng để trao đổi các thông điệp điều khiển, bao gồm những thông điệp đảm nhiệm báo cáo tình trạng hoạt động của mạng, báo cáo lỗi, hỗ trợ chẩn đoán mạng. Tuy nhiên, nhằm phục vụ thực hiện những quy trình hoạt động cơ bản của địa chỉ IPv6, ICMPv6 còn bao gồm những dạng thông điệp mới, phục vụ cho các thủ tục và những quy trình giao tiếp của các node IPv6. Các thông điệp ICMP đươc phân chia làm hai loại: ***Thông điệp lỗi*** và ***Thông điệp thông tin***.

4.1.2.2 Thông điệp lỗi (Error message)

Các thông điệp lỗi được sử dụng để báo lỗi trong quá trình chuyển tiếp và phân phối gói tin IPv6, thực hiện bởi node đích hoặc router đang xử lý gói tin. Các thông điệp này có giá trị của 8 bít trường Type từ 0 đến 127 (bít đầu tiên được đặt giá trị 0). Các thông điệp lỗi bao gồm: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

Dạng (type)	Mô tả	Giá trị trường code
1	Destination unreachable.	0 – Không có tuyến tới đích 1 – Giao tiếp tới đích bị cấm 2 – Chưa gán 3 - Địa chỉ không kết nối được. 4 – Port không kết nối tới được.
2	Packet too big.	0
3	Time exceeded.	0 – Vượt quá giới hạn hop limit 1 – Thời gian tạo lại gói tin vượt quá giới hạn cho phép
4	Parameter problem.	0 – Lỗi header 1 – Không nhận dạng được Next Header 2 – Không nhận ra IPv6 option

Bảng 6: Các thông điệp lỗi

Thông điệp lỗi "Destination unreachable" được gửi khi một node không thể chuyển tiếp gói tin vì một số lí do nào đó (không phải do tắc nghẽn mạng). Node gửi thông báo lỗi về nguồn của gói tin, trường code sẽ chỉ định nguyên nhân, như trong bảng 6.

Node gửi thông điệp lỗi "Packet Too Big" khi kích thước gói tin vượt quá giá trị MTU của đường kết nối. Trong IPv6, việc phân mảnh không được thực hiện bởi router, chỉ có node nguồn thực hiện phân mảnh. Thông điệp "Packet Too Big" còn được sử dụng trong quy trình tìm kiếm giá trị MTU nhỏ nhất trên toàn bộ đường truyền dẫn của IPv6, là một quy trình do thủ tục Neighbor Discovery đảm nhiệm [41].

[41] Tham khảo mục 4.3.7 về quy trình tìm kiếm giá trị PathMTU phục vụ cho việc phân mảnh gói tin IPv6

Khi giá trị Hop limit trong header gói tin IPv6 đạt tới 0, gói tin sẽ bị huỷ bỏ và thông điệp lỗi " Time Exceeded" được gửi.

Thông điệp lỗi "Parameter Problem" được gửi nếu một node nhận thấy có vấn đề trong header cơ bản, hoặc trong một header mở rộng của gói tin IPv6. Dạng lỗi được chỉ định bằng giá trị trường code, như trong bảng 6.

4.1.2.3 Thông điệp thông tin

Thông điệp thông tin ICMPv6 chia thành hai nhóm: ***Thông điệp thông tin cơ bản*** và ***Thông điệp thông tin mở rộng***. Trường Type của gói tin thông điệp thông tin ICMPv6 có giá trị trong khoảng 128 - 255 (bít đầu tiên được thiết lập giá trị 1).

Thông điệp thông tin cơ bản: Bao gồm "Echo request" và "Echo reply" . Hai dạng thông điệp này được sử dụng trong các chương trình dò tìm như ping, traceroute, thực hiện chức năng chẩn đoán mạng.

Thông điệp thông tin mở rộng: Là những thông điệp ICMPv6 được sử dụng bởi thủ tục thực hiện chức năng giao tiếp giữa các node lân cận trong một đường kết nối Neighbor Discovery - ND và thủ tục quản lý quan hệ thành viên nhóm multicast Multicast Listener Discovery - MLD, phục vụ cho các quy trình hoạt động cốt yếu của địa chỉ IPv6. Những thông điệp này được liệt kê trong bảng 8. Trong đó Multicast Listener Query, Multicast Listener Report, Multicast Listener Done phục vụ cho thủ tục MLD, năm thông điệp Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement và Redirect phục vụ cho thủ tục ND

Type	Mô tả	Code
128	Echo request.	0
129	Echo reply.	0

Bảng7: Thông điệp thông tin cơ bản

Type	Mô tả	Code
130	Multicast Listener Query.	0
131	Multicast Listener Report.	0
132	Multicast Listener Done.	0
133	Router Solicitation.	0
134	Router Advertisement.	0
135	Neighbor Solicitation.	0
136	Neighbor Advertisement.	0

137	Redirect.	0

Bảng 8: Thông điệp thông tin mở rộng

Chúng ta sẽ tìm hiểu chi tiết hơn về những thông điệp thông tin mở rộng trong những mục sau, khi mô tả chi tiết về các quy trình hoạt động cơ bản của địa chỉ IPv6.

4.2 THỦ TỤC NEIGHBOR DISCOVERY - ND

Neighbor Discovery - ND là một thủ tục được phát triển mới trong phiên bản IPv6. ND hoạt động trên nền những thông điệp ICMPv6 và phụ trách các quy trình giao tiếp giữa các node IPv6 trên cùng một đường kết nối. Những quy trình hoạt động giao tiếp này (giữa host với host, giữa host với router) là thiết yếu đối với hoạt động của thế hệ địa chỉ IPv6. ND sử dụng ICMPv6 để đảm nhiệm những chức năng phân giải địa chỉ, tìm kiếm router, Redirect, đồng thời cũng cung cấp nhiều chức năng khác nữa.

Khi một node IPv6 khởi tạo, để có thể tiến hành giao tiếp, node cần biết một số điểm:

- Địa chỉ của node
- Thông tin về prefix của chính nó để node biết được cách thức gửi gói tin tới những node khác thuộc những prefix khác.
- Biết được router trên đường kết nối
- Quyết định được đích tiếp theo (next hop) trong đường dẫn tới một đích.
- Cần phân giải để nhận được địa chỉ lớp hai (link-layer) từ một địa chỉ lớp ba (network-layer) đã biết.
- Cần biết nó có thể gửi gói tin có độ lớn bao nhiêu.

Đồng thời, để giao tiếp tiến hành được suôn sẻ, node cũng cần:

- Biết được về những node lân cận trên cùng đường kết nối.
- Có khả năng dò kiểm tra được tình trạng node lân cận không còn kết nối tới được, để nó không gửi gói tin tới node đó nữa.
- Biết được địa chỉ nó đang định dùng liệu có bị một node khác sử dụng rồi hay không.
- Có khả năng lái (redirect) gói tin tới một node chuyển tiếp khác tốt hơn (nếu có)

Tất cả những điều trên sẽ thực hiện được bằng những quy trình hoạt động mà thủ tục Neighbor Discovery phụ trách. Nhờ những quy trình giao tiếp giữa host với host, host với router trên cùng đường kết nối, IPv6 node có khả năng tự động cấu hình địa chỉ và những tham số hoạt động khác mà không cần có sự hiện diện của máy chủ DHCP.

Trên một đường kết nối:

Node (host và router) sẽ sử dụng ND để:

- ❖ Thực hiện phân giải địa chỉ lớp link-layer của một node lân cận từ địa chỉ IPv6.
- ❖ Quyết định xem node lân cận có còn kết nối tới được hay không.

Host sẽ sử dụng ND để:

- ❖ Tìm kiếm router trên đường kết nối.
- ❖ Tìm kiếm thông tin về địa chỉ, prefix địa chỉ của đường kết nối và những thông tin cấu hình khác phục vụ cho việc cấu hình địa chỉ và hoạt động của host.

Router sẽ sử dụng ND để:

- Quảng bá sự hiện diện của mình, quảng bá những thông tin cấu hình cần thiết cho host, quảng bá prefix địa chỉ của đường link.
- Thông báo cho host về địa chỉ next-hop tốt hơn để có thể chuyển tiếp gói tin đến một đích nhất định.

4.2.1 Thông điệp ICMPv6 sử dụng trong thủ tục ND

ND sử dụng tập hợp 5 thông điệp ICMPv6 sau đây:

- Router Advertisement
- Router Solicitation
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

Những thông điệp này được trao đổi giữa các node lân cận trên một đường kết nối, trong các quy trình hoạt động cần thiết của địa chỉ IPv6.

4.2.1.1 Thông điệp quảng bá của router (Router Advertisement-RA)

Thông điệp này tương ứng dạng ICMPv6 Type 134.

Router IPv6 ngoài chức năng chuyển tiếp gói tin cho các host trên một đường kết nối, còn đảm nhiệm một chức năng rất quan trọng là quảng bá thông tin giúp các host trên đường kết nối biết được sự hiện diện của router và nhận được những thông số trợ giúp cho hoạt động. Nhờ phương thức quảng bá thông tin từ router, host IPv6 có khả năng tự động cấu hình địa chỉ toàn cầu, cấu hình các tham số phục vụ cho giao tiếp.

Trong số những thông điệp ICMPv6 được trao đổi giữa các node trên đường kết nối, thông điệp Router Advertisement có một vai trò đặc biệt. Router Advertisement được router trên đường link gửi định kỳ tới địa chỉ đích multicast mọi node phạm vi link (FF02::1), có nghĩa gửi tới mọi node trên đường kết nối.

Thông điệp quảng bá của router được gửi cho những mục đích sau đây:

1. Thông báo địa chỉ link layer của router
2. Thông báo cách thức cấu hình địa chỉ toàn cầu cho node trên đường kết nối.
3. Thông báo network prefix cho các node trên đường kết nối.
4. Thông báo giá trị hop limit, MTU, những tham số hoạt động cho những node trên đường kết nối.

Router thông báo địa chỉ của mình cho những node trên đường kết nối, để các node có thể xác định được router mặc định sẵn sàng chuyển tiếp gói tin cho host. Thông tin về thời gian (Router lifetime) cũng được gửi kèm để node xác định được thời gian bao lâu nó có thể coi router là router mặc định.

Từ thông tin quảng bá đã nhận được từ router, IPv6 node sẽ xây dựng danh sách các router mặc định (default router). Đối với IPv4 host, cần phải cấu hình bằng tay router mặc định. Khi thời gian Router lifetime hết, router sẽ bị loại bỏ khỏi danh sách router mặc định.

Thông điệp quảng bá của router cũng chứa thông tin xác định cách thức đang được sử dụng để tự động cấu hình địa chỉ cho các node trên một đường kết nối. IPv4 host được cấu hình bằng tay để xác định rằng nó nhận các thông tin cấu hình IP từ DHCP. IPv6 host có hai phương thức tự động cấu hình địa chỉ. Tự động cấu hình địa chỉ có sự hỗ trợ của máy chủ DHCPv6 được gọi tên là cách thức tự động cấu hình có trạng thái (stateful), ngoài ra IPv6 host còn khả năng tự động cấu hình địa chỉ không cần máy chủ DHCPv6, gọi là cách thức tự động cấu hình không trạng thái (stateless). Phương thức nào đang được áp dụng trên một đường kết nối được xác định bằng thông điệp quảng bá của router trên đường kết nối.

Khi đường kết nối sử dụng phương thức tự động cấu hình địa chỉ không trạng thái, thông điệp Router Advertisement sẽ bao gồm network prefix của đường kết nối. Tương ứng với mỗi prefix sẽ có tham số thời gian sống (bao gồm hai giá trị: Valid Lifetime và Preferred Lifetime). Giá trị Valid Lifetime xác định bằng giây khoảng thời gian prefix địa chỉ là hợp lệ trên đường kết nối. Giá trị Preferred Lifetime xác định bằng giây khoảng thời gian mà địa chỉ được tự động cấu hình nên từ prefix có trạng thái ưu tiên - "preferred". Thông điệp Router Advertisement cũng chứa thông tin về hop limit[42] và MTU để các node sử dụng trong quá trình giao tiếp.

Một đặc điểm ưu việt của địa chỉ IPv6 là khi một host khởi động, nó có thể tự mình khởi tạo ngay địa chỉ link local để sử dụng trong giao tiếp trên một đường kết nối. Khi host nhận được network prefix từ thông điệp Router Advertisement của router, prefix này sẽ được host kết hợp với định danh giao diện đã được tự động tạo ra của để tự động cấu hình nên địa chỉ dùng cho giao tiếp toàn cầu.

Thông điệp Router Advertisement chỉ có thể gửi bởi router và được gửi định kỳ tới địa chỉ multicast mọi node phạm vi link. Tuy nhiên, router cũng sẽ tạo ngay thông điệp RA đáp trả yêu cầu của một host trên đường link nếu nó nhận được gói tin truy vấn router (Router Solicitation). Trong trường hợp đó, thông điệp RA sẽ được gửi tới địa chỉ đích unicast là địa chỉ của nơi gửi thông điệp truy vấn router.

4.2.1.2 Thông điệp truy vấn router (Router Solicitation-RS)

Thông điệp này có ICMPv6 type 133.

IPv6 host truyền gói tin Router Solicitation để nhắc router trên cùng đường kết nối lập tức tạo thông điệp Router Advertisement gửi thông tin cho host.

Thông điệp này sử dụng địa chỉ nguồn hoặc là một địa chỉ unicast đã được gắn cho giao diện gửi gói tin, hoặc, trong trường hợp địa chỉ này không tồn tại, nó sử dụng địa chỉ đặc biệt 0:0:0:0:0:0:0:0. Địa chỉ đích thông thường là địa chỉ multicast mọi router phạm vi link (FF02::2). Do quá trình tự động cấu hình và định tuyến phụ thuộc vào khả năng tìm thấy router và prefix địa chỉ, thông điệp này là cần thiết trước khi bất cứ giao tiếp nào được thiết lập.

4.2.1.3 Thông điệp truy vấn node lân cận (Neighbor Solicitation-NS)

Thông điệp này có ICMPv6 type 135.

Thông điệp Neighbor Solicitation được một node sử dụng để yêu cầu các node khác trên đường kết nối cung cấp địa chỉ lớp link layer của chúng. Chức năng này giống như thủ tục ARP trong IPv4. Node được hỏi sẽ sử dụng thông điệp Neighbor Advertisement để trả lời về địa chỉ lớp link-layer của nó.

[42] Một trường của IPv6 header, xác định số đường kết nối tối đa mà gói tin có thể đi qua trước khi bị huỷ bỏ

Thông điệp Neighbor Solicitation còn được sử dụng cho quá trình kiểm tra trùng lặp địa chỉ khi một node cần xác nhận rằng không có một node nào khác trên đường link được gắn trùng địa chỉ của nó. Neighbor Solicitation cũng được sử dụng trong quy trình kiểm tra tính kết nối tới được của node lân cận.

Địa chỉ nguồn của thông điệp này hoặc là địa chỉ unicast giao diện truyền gói tin hoặc là địa chỉ đặc biệt 0:0:0:0:0:0:0:0.

Thông điệp Neighbor Solicitation sẽ được gửi tới địa chỉ multicast khi một node cần phân giải một địa chỉ IPv6 thành địa chỉ lớp link layer tương ứng, hoặc gửi tới địa chỉ unicast khi một node muốn kiểm tra tính kết nối tới được của node lân cận trên cùng đường kết nối.

Các thông điệp Neighbor Solicitation và Neighbor Advertisement được sử dụng cho nhiều mục đích: tự động cấu hình địa chỉ, kiểm tra trùng lặp địa chỉ, dò tìm khả năng kết nối tới được. Trong tất cả những quy trình đó, các thông điệp này chỉ được trao đổi trong phạm vi đường kết nối nội bộ, và cần có trước khi các giao tiếp có thể được thiết lập.

4.2.1.4 Thông điệp quảng bá của node (Neighbor Advertisement-NA)

Thông điệp này có ICMPv6 type 136.

Node gửi gói tin Neighbor Advertisement để đáp trả gói tin truy vấn Neighbor Solicitation. Khi thông tin của một node ví dụ địa chỉ lớp hai thay đổi, nó cũng gửi thông điệp Neighbor Advertisement cập nhật sự thay đổi đó cho các node lân cận trên cùng đường kết nối.

Địa chỉ nguồn của thông điệp là địa chỉ unicast, địa chỉ đích là địa chỉ unicast của node hỏi thông tin hoặc là địa chỉ multicast mọi node phạm vi link (FF02::1). Cũng như thông điệp Neighbor Solicitation, các gói tin này chỉ được gửi trong phạm vi đường kết nối và cần có trước khi các giao tiếp được thiết lập.

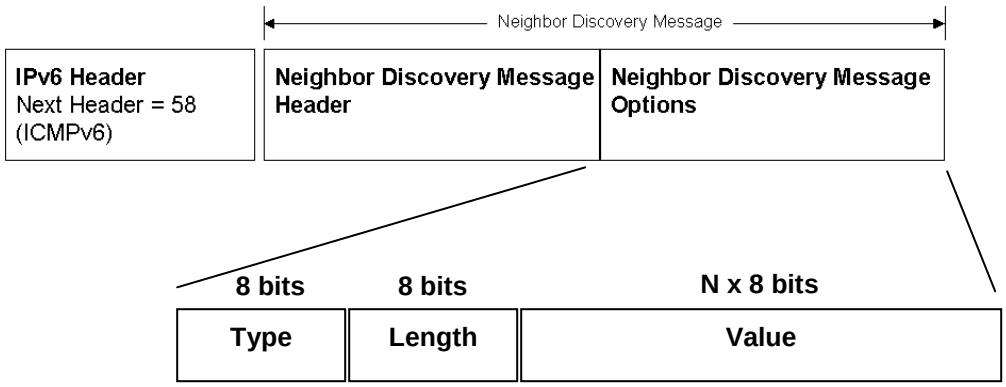
4.2.1.5 Thông điệp Redirect

Thông điệp này có ICMPv6 type 137.

Thông điệp Redirect luôn được gửi giữa các địa chỉ unicast. Thông điệp này được gửi bởi router để thông báo cho host IPv6 rằng có một router khác tốt hơn có thể sử dụng làm next hop để gửi gói tin đến một đích nhất định. Địa chỉ nguồn của thông điệp là địa chỉ link-local của giao diện router. Địa chỉ đích là địa chỉ nguồn của gói tin đã khiến cho router phải gửi thông điệp Redirect.

4.2.2 Tìm hiểu về gói tin ND

Gói tin ND là gói tin ICMPv6 thuộc một trong năm dạng thông điệp nêu trên. Gói tin ND sẽ chứa các thông tin cần thiết trao đổi giữa các node lân cận trên một đường kết nối và có cấu trúc như sau:



Hình 26: Cấu trúc thông điệp ND

Thông điệp ND bao gồm một ND header, và có hoặc không có các tuỳ chọn Option ND.

ND option:

ND option sử dụng để chứa đựng các thông tin mà thông điệp Neighbor Discovery cần truyền tải: địa chỉ MAC, network prefix của đường kết nối, thông tin MTU của đường kết nối, các tham số hoạt động, dữ liệu phục vụ cho việc redirect.

một ND option được cấu thành từ ba trường Type/Lengh/Value

Trường Type chỉ định dạng của ND Option, hiện nay trong RFC2461[43], có các dạng sau đây:

Type	Tên Option
1	Source Link-Layer Address
2	Target Link-Layer Address
3	Prefix Information
4	Redirected Header
5	MTU

Bảng 9: Các dạng Option ND

- *Type 1:* Source Link-Layer Address chỉ định địa chỉ lớp link-layer của nơi gửi thông điệp ND. Option này có trong các thông điệp Neighbor Solicitation, Router Solicitation, và Router Advertisement. Các quy trình sử dụng những thông điệp trên cần có Option này để thông báo địa chỉ lớp link-layer của nơi gửi thông điệp ND (ví dụ quá trình phân giải địa chỉ).

[43] RFC2461: Neighbor Discovery for IP Version 6 (IPv6)

- *Type 2:* Target Link-Layer Address chỉ định địa chỉ lớp link-layer của node mà gói tin IPV6 nên được gửi tới. Option này có trong thông điệp Neighbor Advertisement và Redirect.

- *Type 3:* Prefix Information

  Option "Prefix Information" có trong thông điệp *Router Advertisement* để chỉ định prefix địa chỉ trên đường link kết nối với router, đồng thời cũng mang thông tin chỉ định về tự động cấu hình địa chỉ. Trong một thông điệp Router Advertisement, có thể có đồng thời nhiều Option Prefix Information để thông báo cùng lúc nhiều prefix địa chỉ trên một đường link.

  Trong thông điệp có chứa Option Prefix Information, phần "value" sẽ là N nhóm 8 bít, trong đó chứa các thông tin về chiều dài prefix, thông tin về thời gian tồn tại hợp lệ của prefix, cờ để xác định xem prefix có được sử dụng để cấu hình địa chỉ tự động hay không, và một số các thông tin khác nữa.

- *Type 4:* Redirected Header

  Option này có trong thông điệp Redirect để xác định gói tin IPv6 khiến cho router phải gửi thông điệp redirect. Nó có thể bao gồm một phần hoặc tất cả gói tin IPv6, tùy thuộc vào kích cỡ gói tin đã được gửi ban đầu.

- *Type 5:* Option MTU

  Option này có trong thông điệp Router Advertisement để chỉ định giá trị MTU trên đường link. Giá trị của MTU này sẽ được dùng thay cho giá trị MTU cung cấp bởi giao diện phần cứng.

4.2.3 Những quy trình liên quan đến thủ tục Neighbor Discovery

Với nguyên liệu là năm thông điệp ICMPv6 mô tả như trên, thủ tục Neighbor Discovery tham gia vào thực hiện những quy trình sau đây:

Quy trình	Mô tả
Tìm kiếm router (Router discovery)	Quy trình mà nhờ đó, một host khám phá ra router trên đường kết nối sẵn sàng chuyển tiếp gói tin cho host.
Tìm kiếm prefix (Prefix discovery)	Quy trình mà nhờ đó, host tìm thấy tiền tố mạng (network prefix) trên đường kết nối của mình.
Tìm kiếm thông số (Parameter discovery)	Quy trình mà nhờ đó, host tìm được những tham số hoạt động như giá trị MTU của đường kết nối, giá trị hop limit mặc định để gửi gói tin.
Tự động cấu hình địa chỉ (Address autoconfiguration)	Quy trình mà nhờ đó, node có thể cấu hình thông tin địa chỉ IP cho các giao diện, theo phương thức có hoặc không có sự hiện diện của máy chủ DHCPv6.

Phân giải địa chỉ (Address resolution)	Quy trình mà nhờ đó, node có thể phân giải địa chỉ lớp link-layer của một node lân cận từ địa chỉ IPv6 đã biết (tương đương chức năng của thủ tục ARP trong địa chỉ IPv4).
Quyết định đích tiếp theo (Next-hop determination)	Quy trình mà nhờ đó, node có thể quyết định địa chỉ IPv6 của đích tiếp theo gói tin sẽ được chuyển tiếp tới, dựa trên địa chỉ đích. Địa chỉ này sẽ hoặc chính là địa chỉ đích cuối cùng, hoặc là địa chỉ của của router mặc định trên đường kết nối.
Khám phá khả năng có thể kết nối tới được của node lân cận (Neighbor unreachability detection)	Quy trình mà nhờ đó, node quyết định được một node lân cận có thể còn nhận được gói tin hay không.
Kiểm tra trùng lặp địa chỉ (Duplicate address detection)	Quy trình mà nhờ đó, node có thể biết địa chỉ IPv6 nó dự định sử dụng hiện đã có một node nào khác trên đường kết nối sử dụng rồi hay chưa.
Chức năng lái (Redirect function)	Quy trình thông báo cho một host địa chỉ IPv6 đích tiếp theo (next hop) tốt hơn có thể sử dụng để tới được đích cuối cùng.

Bảng 10: Quy trình thủ tục ND cung cấp

4.3 MỘT SỐ QUY TRÌNH HOẠT ĐỘNG CƠ BẢN TRONG IPV6

4.3.1 Quy trình phân giải địa chỉ lớp hai (link layer) từ địa chỉ IPv6 lớp ba (network layer)

Trong hoạt động của thủ tục IP phiên bản 4, quy trình này được đảm nhiệm bởi thủ tục ARP. Node cần phân giải địa chỉ sẽ gửi gói tin truy vấn tới địa chỉ đích là địa chỉ broadcast của mạng, do vậy sẽ tác động đến mọi node khác trên đường kết nối, làm giảm hiệu suất mạng.

Trong hoạt động của địa chỉ IPv6, đây là một trong số những quy trình do thủ tục Neighbor Discovery đảm nhiệm. Để phục vụ cho việc phân giải tương ứng địa chỉ lớp mạng và địa chỉ vật lý, các node IPv6 duy trì một bảng cache thông tin về các node lân cận, gọi là "neighbor cache". Trong HĐH window, chúng ta có thể xem thông tin trong bảng này với lệnh **netsh>interface IPv6>show neighbors.**

Khi một IPv6 node cần tìm địa chỉ lớp hai (ví dụ địa chỉ MAC trên một Ethernet) tương ứng với một địa chỉ IPv6 nào đó, thay vì gửi gói tin truy vấn tới địa chỉ multicast mọi node phạm vi link (FF02::1) để tác động tới mọi node trên đường kết nối tương đương địa chỉ broadcast trong IPv4, node đó chỉ gửi tới địa chỉ Multicast Solicited Node[44] tương ứng địa chỉ unicast cần phân giải.

Như đã đề cập trong chương 2, node IPv6, khi được gắn một địa chỉ unicast, ngoài việc lắng nghe lưu lượng tại địa chỉ unicast này, node IPv6 sẽ lập tức nghe và nhận lưu lượng của một địa chỉ multicast tương ứng địa chỉ unicast là Multicast Solicited Node.

Như vậy, trong quá trình phân giải địa chỉ của IPv6, chỉ những node đang nghe lưu lượng tại địa chỉ Multicast Solicited Node phù hợp mới nhận và xử lý gói tin. Điều này giảm thiểu việc tác động đến mọi node trên đường kết nối, tăng hiệu quả hoạt động. Đây là một trong những cải tiến của IPv6 so với phiên bản IPv4.

Để thực hiện quy trình phân giải địa chỉ, hai node IPv6 trao đổi thông điệp *Neighbor Solicitation* và *Neighbor Advertisement.*

Khi một node cần phân giải địa chỉ, nó gửi đi trên đường kết nối thông điệp Neighbor Solicitation:

- Địa chỉ nguồn: Địa chỉ IPv6 của giao diện gửi gói tin.
- Địa chỉ đích: địa chỉ IPv6 Multicast Solicited Node tương ứng địa chỉ unicast cần phân giải địa chỉ
- Thông tin chứa trong phần dữ liệu có chứa địa chỉ lớp link-layer của nơi gửi (nằm trong Option Source Link-Layer Address của gói tin ND).

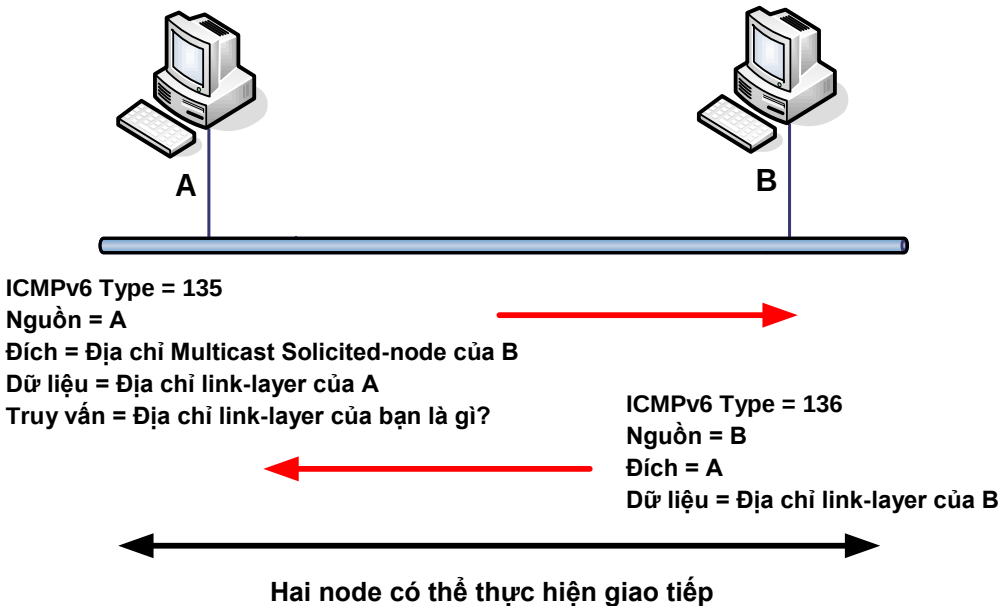
Trên đường link, node đang nghe lưu lượng tại địa chỉ Multicast Solicited Node trùng với địa chỉ đích của gói tin sẽ nhận được thông tin. Nó thực hiện những hành động sau:

- Cập nhật địa chỉ lớp link-layer của nơi gửi vào bảng neighbor cache.

[44] Tham khảo lại mục II.2.3.4 về địa chỉ Multicast Solicited Node

- Gửi thông điệp Neighbor Advertisement đáp trả tới địa chỉ đích là địa chỉ nguồn đã gửi gói tin, thông tin trong phần dữ liệu có địa chỉ lớp link-layer của nó (chứa trong Option Target Link-Layer Address của gói tin ND).

Khi nhận được thông điệp Neighbor Advertisement, node cần phân giải địa chỉ sẽ cập nhật thông tin vào bảng neighbor cache của mình và sử dụng thông tin trong đó để thực hiện liên lạc.



Hình 27: Quy trình phân giải địa chỉ

4.3.2 Kiểm tra trùng lặp địa chỉ trên một đường kết nối (Duplicate Address Detection - DAD)

Mọi node IPv6 thực hiện thuật toán kiểm tra sự trùng lặp về địa chỉ trên một đường kết nối trước khi chính thức gán địa chỉ unicast cho một giao diện, nhằm ngăn ngừa việc xung đột về địa chỉ. Quy trình này được áp dụng dù địa chỉ được gắn bằng tay hoặc bằng hình thức cấu hình tự động nào. Chừng nào host vẫn còn đang thực hiện DAD và chưa quyết định được là địa chỉ không có sự trùng lặp, thì địa chỉ được coi là địa chỉ "thăm dò".

DAD sử dụng hai thông điệp ICMPv6 *Neighbor Solicitation* và *Neighbor Advertisement*. Tuy nhiên một số thông tin của gói tin này khác với gói tin sử dụng trong quá trình phân giải địa chỉ.

Khi một node cần kiểm tra trùng lặp địa chỉ, nó gửi gói tin truy vấn node lân cận Neighbor Solicitation

- Địa chỉ IPv6 nguồn: Là địa chỉ đặc biệt "::".
- Địa chỉ đích: là địa chỉ Multicast Solicited Node tương ứng địa chỉ đang kiểm tra trùng lặp.
- Gói tin Neighbor Solicitation sẽ chứa địa chỉ IPv6 đang được kiểm tra trùng lặp.

Sau khi gửi NS, node sẽ đợi. Nếu không có phản hồi, có nghĩa địa chỉ này chưa được sử dụng. Nếu địa chỉ này đã được một node nào đó sử dụng rồi, node này sẽ nhận được thông điệp NS và gửi thông điệp quảng bá Neighbor Advertisement đáp trả:

Nếu node đang kiểm tra địa chỉ trùng lặp nhận được thông điệp RA phản hồi lại RS mình đã gửi, nó sẽ hủy bỏ việc sử dụng địa chỉ này.

4.3.3 Kiểm tra tính có thể kết nối tới được của node lân cận (Neighbor Unreachability Detection)

Thông điệp Neighbor Solicitation và Neighbor Advertisement được sử dụng trong quá trình phân giải địa chỉ, kiểm tra trùng lặp địa chỉ, cũng được sử dụng cho những mục đích khác, như quá trình kiểm tra tính có thể kết nối tới được của một node lân cận. Các IPv6 node duy trì bảng thông tin về các node lân cận của mình trong bảng neighbor cache, và sẽ cập nhật bảng này khi có sự thay đổi tình trạng mạng. Bảng này lưu thông tin đối với cả router và host.

Biết được node lân cận có thể kết nối tới được hay không rất quan trọng đối với một node vì nó sẽ điều chỉnh cách thức cư xử của mình. Ví dụ khi biết một node lân cận không kết nối tới được, host sẽ ngừng gửi gói tin, biết một router đang không thể kết nối tới được, host có thể thực hiện quy trình tìm kiếm một router khác.

Nếu một host muốn kiểm tra tình trạng có thể nhận gói tin của node lân cận, nó gửi thông điệp Neighbor Solicitation, nếu nhận được Neighbor Advertisement phúc đáp, nó biết tình trạng của node lân cận là có thể kết nối được và sẽ cập nhật thông tin này vào bảng neighbor cache của mình. Tất nhiên tình trạng này chỉ được coi là tạm thời và có một khoảng thời gian dành cho nó, trước khi node cần thực hiện kiểm tra lại trạng thái node lân cận. Khoảng thời gian quy định này, cũng như một số các tham số hoạt động khác host sẽ nhận được từ thông tin quảng bá Router Advertisement của router trên đường kết nối.

4.3.4 Tìm kiếm router trên đường kết nối (Router Discovery)

Đối với hoạt động của địa chỉ IPv6, sự trao đổi giữa các host với nhau, giữa host với router trên cùng một đường kết nối là rất quan trọng. Trong mạng, router là thiết bị đảm nhiệm việc chuyển tiếp lưu lượng của các host từ mạng này sang mạng khác. Một host phải nhờ vào router để có thể gửi thông tin tới những node nằm ngoài đường kết nối của mình. Do vậy, trước khi một host có thể thực hiện các hoạt động giao tiếp với mạng bên ngoài, nó cần tìm một router và học được những thông tin quan trọng về router, cũng như về mạng. Trong thế hệ địa chỉ IPv6, để có thể cấu hình địa chỉ, cũng như có những thông số cho hoạt động, IPv6 host cần tìm thấy router và nhận được những thông tin từ router trên đường kết nối. Router IPv6 ngoài việc đảm trách chuyển tiếp gói tin cho host còn đảm nhiệm một hoạt động không thể thiếu là quảng bá sự hiện diện của mình và cung cấp các tham số trợ giúp host trên đường kết nối cấu hình địa chỉ và các tham số hoạt động. Thực hiện những hoạt động trao đổi thông tin giữa host và router là một nhiệm vụ rất quan trọng của thủ tục Neighbor Discovery.

Quá trình tìm kiếm, trao đổi giữa host và router thực hiện dựa trên hai dạng thông điệp sau:

- *Router Solicitation* được gửi bởi host tới các router trên đường link. Do vậy, gói tin được gửi tới địa chỉ đích multicast mọi router phạm vi link (FF02::2). Host gửi thông điệp này để yêu cầu router quảng bá ngay các thông tin nó cần cho hoạt động ví dụ khi host chưa được gắn địa chỉ, chưa có các tham số mặc định cần thiết để xử lý gói tin…
- *Router Advertisement* chỉ được gửi bởi các router để quảng bá sự hiện diện của router và các tham số cần thiết khác cho hoạt động của các host. Router gửi định kỳ thông điệp này trên đường kết nối và gửi thông điệp này bất cứ khi nào nhận được Router Solicitation từ các host trong đường kết nối.

Router Discovery là quá trình trao đổi giữa router và host trên một đường link, trong đó:

Router :

- Quảng bá gói tin Router Advertisement: Nhiệm vụ cơ bản một IPv6 router thực hiện trong ND là gửi định kỳ gói tin Router Advertisement quảng bá sự hiện diện của nó trên đường kết nối và các thông số khác. Khoảng thời gian cách giữa hai thông điệp được cấu hình trên router. RA cũng được gửi khi có bất cứ tình huống đặc biệt nào xảy ra, ví dụ khi thông tin quan trọng nào đó của router thay đổi như địa chỉ của nó.
- Duy trì những thông số cơ bản cho mạng: Router cũng đảm nhiệm việc duy trì những thông số cơ bản phục vụ cho hoạt động mạng. Những thông số này sẽ được thông báo nhờ các trường trong RA.
- Nhận và xử lý thông điệp Router Solicitation. Router sẽ lắng nghe thông điệp này của các host và nếu nhận được gói tin này, nó sẽ lập tức gửi RA phúc đáp.

Host:

- Nhận và xử lý gói tin Router Advertisement: Host sẽ lắng nghe nhận các thông điệp RA, khi nhận được thông điệp này, nó sẽ:
    - Xác lập những giá trị thông số hoạt động theo những giá trị được gửi trong các trường của RA. Bao gồm cả việc duy trì và cập nhật một số dữ liệu như danh sách prefix địa chỉ, router mặc định.
    - Nếu host mới khởi động và chưa được gắn địa chỉ, nó sẽ theo những thông tin hướng dẫn trong RA để tự động cấu hình thông tin cho chính nó: địa chỉ IP, các tham số khác.
    - Tạo gói tin Router Solicitation: Trong những trường hợp nhất định, host sẽ tạo gói tin RS và gửi đi trên đường link để có thể nhận ngay RA phúc đáp mà không đợi theo định kỳ.

Nhờ quá trình trao đổi như trên, những thông tin sau liên quan đến đường kết nối được thiết lập:

- Router mặc định cho các host trên đường kết nối. Trong thông điệp RA có trường Router Lifetime, giá trị của nó xác định thời gian router gửi RA có thể được coi là router mặc định. Tuy nhiên, nếu còn thời gian hợp lệ mà host nhận thấy router không liên lạc được (qua quy trình kiểm tra tính có thể kết nối tới của node lân cận), nó sẽ không sử dụng router làm router mặc định nữa.
- Host có thông tin để quyết định mình cần sử dụng cách thức cấu hình IP nhờ máy chủ DHCPv6 hay tự cấu hình địa chỉ. Trong quảng bá của router có thông tin chỉ dẫn cho host phương thức nhận thông tin cấu hình địa chỉ.
- Một số tham số mặc định trên đường kết nối, phục vụ cho hoạt động của host:
    - Giá trị mặc định của Hop Limit cho các gói tin IPv6.
    - Thời gian host thực hiện lại quá trình kiểm tra tính có thể kết nối được của các node lân cận.
    - Giá trị MTU mặc định của đường kết nối.
    - Danh sách các tiền tố mạng (prefix) của đường kết nối. Mỗi prefix sẽ gồm có cả thông tin về thời gian sống. Nếu trên đường kết nối đang sử dụng phương thức tự động cấu hình không cần

máy chủ DHCPv6 (gọi là cách thức tự động cấu hình không trạng thái), host sẽ sử dụng prefix nhận được từ thông tin quảng bá của router, gắn với định danh giao diện đã tự động tạo ra để tạo nên địa chỉ toàn cầu của host.

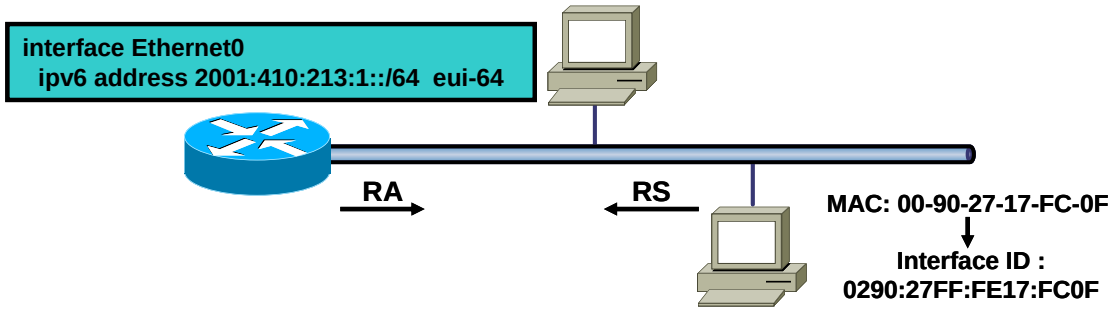
4.3.5 Tự động cấu hình địa chỉ không trạng thái (Stateless Autoconfiguration) của thiết bị IPv6

Thiết bị IPv4 khi kết nối vào mạng phải được cấu hình bằng tay các thông số địa chỉ, mặt nạ mạng, router mặc định, máy chủ tên miền. Để giảm cấu hình thủ công, máy chủ DHCP được sử dụng để có thể cấp phát địa chỉ IP và thông số cho IPv4 host khi nó kết nối vào mạng. Địa chỉ IPv6 tiến thêm một bước xa hơn khi cho phép một IPv6 node có thể tự động cấu hình địa chỉ và các tham số hoạt động mà không cần sự hỗ trợ của máy chủ DHCPv6. Do vậy, địa chỉ IPv6 có hai phương thức tự động cấu hình địa chỉ:

- Sử dụng máy chủ DHCPv6 để cung cấp địa chỉ và thông số cho các host IPv6. Cách thức này tương tự như việc sử dụng DHCP của địa chỉ IPv4. Tuy nhiên, việc hướng dẫn IPv6 host nhận địa chỉ và thông số từ máy chủ DHCPv6 do router trên đường kết nối quảng bá thông tin, không phải thực hiện cấu hình xác định bằng tay như IPv4 host. Phương thức tự động cấu hình này được gọi là ***"tự động cấu hình có trạng thái – stateful autoconfiguration".*** Hiện nay, các tài liệu tiêu chuẩn hoá cho DHCPv6 đã được hoàn thiện đầy đủ.
- IPv6 host tự động cấu hình địa chỉ cho mình mà không cần sự hỗ trợ của máy chủ DHCPv6. Host thực hiện cấu hình IP bắt đầu từ trạng thái chưa có thông tin hỗ trợ cấu hình, do vậy phương thức cấu hình này được gọi là ***"tự động cấu hình không trạng thái – stateless autoconfiguration"***

Giảm tối thiểu cấu hình thủ công là một trong những đặc điểm hoàn toàn mới và là một ưu điểm nổi bật của địa chỉ IPv6. Khả năng tự động cấu hình không trạng thái của thiết bị IPv6 dựa trên một số đặc tính mới của địa chỉ IPv6, bao gồm: khả năng tự tạo 64 bít định danh giao diện từ địa chỉ lớp hai, từ đó tự động tạo địa chỉ link-local, khả năng trao đổi của host với router trên một đường kết nối nhờ thủ tục Neighbor Discovery để nhận các thông tin về tiền tố địa chỉ mạng của đường kết nối và các tham số hoạt động khác .

Không cần sự hỗ trợ của máy chủ DHCP, host thực hiện các bước sau để tự động cấu hình địa chỉ và các thông số hoạt động cho mình:



Hình 28: Tự động cấu hình địa chỉ của IPv6 host

Bước 1: Tạo địa chỉ link-local:

Địa chỉ link-local bắt đầu bởi 10 bít prefix FE80::/10, theo sau bởi 54 bit 0. 64 bít còn lại là định danh giao diện (interface ID)

Khi khởi động, 64 bít định danh giao diện sẽ được host tự động tạo từ địa chỉ lớp hai. Bạn có thể tham khảo lại chi tiết quy trình tạo định danh giao diện trong mục II.1.4.

Với ví dụ cụ thể trong hình vẽ trên, từ địa chỉ MAC 00-90-27-17-FC-0F, host sẽ tạo được 64 bít định danh giao diện 0290:27FF:FE17:FC0F. Từ đó tạo được địa chỉ link-local FE80::0290:27FF:FE17:FC0F

Ngoài phương thức tạo định danh giao diện từ địa chỉ vật lý, 64 bít định danh giao diện còn có thể được gắn bằng một dãy số ngẫu nhiên.

Bước 2: Thực hiện thuật toán kiểm tra trùng lặp địa chỉ (Duplicate Address Detection)

Trước khi thực sự sử dụng địa chỉ link-local vừa tạo được, host sẽ thực hiện quy trình kiểm tra trùng lặp địa chỉ để chắc chắn địa chỉ link-local mình dự định sử dụng là duy nhất trong phạm vi đường kết nối nhằm tránh xung đột.

Thuật toán DAD, như đã đề cập trong mục trước, dựa trên hai dạng thông diệp Neighbor Solicitation và Neighbor Advertisement.

Bước 3: Gắn địa chỉ link-local

Sau khi gửi thông điệp Neighbor Solicitation, nếu host không nhận được thông điệp Neighbor Advertisement phúc đáp, có nghĩa chưa có node nào trên đường kết nối sử dụng địa chỉ này. Khi đó host sẽ gắn địa chỉ link-local cho mình và lấy địa chỉ này để thực hiện giao tiếp với các node khác trên mạng LAN.

Bước 4: Liên hệ với router.

Trong gói tin Router Advertisement do router trên đường kết nối quảng bá sẽ có các thông tin hướng dẫn host về cách thức cấu hình địa chỉ, về prefix địa chỉ của đường kết nối, và các tham số khác. Do vậy, host sẽ đợi gói tin này trong thông điệp được router gửi một cách định kỳ, hoặc sẽ có gắng liên hệ với các router trên đường kết nối.

Để liên hệ với router, host gửi gói tin truy vấn – RS tới địa chỉ đích multicast mọi router phạm vi link - FF02::2. Router trên đường kết nối sẽ gửi thông điệp quảng bá – RA phúc đáp. Trong đó chứa dữ liệu về tiền tố mạng của đường kết nối và các thông số khác. Nếu đường kết nối đang sử dụng phương thức cấu hình nhờ máy chủ DHCPv6, trong quảng bá của router sẽ không có tiền tố mạng và sẽ có thông tin hướng dẫn host sử dụng máy chủ DHCPv6 để nhận thông tin cấu hình.

Trong hình vẽ, router sẽ quảng bá cho host prefix của đường kết nối là 2001:410:213:1::/64

Bước 5: Cấu hình địa chỉ và xác lập các giá trị thông số hoạt động.

Từ thông tin nhận được trong quảng bá RA của router, host sẽ cấu hình địa chỉ và xác lập các thông số hoạt động

- Từ thông tin về prefix:
    - Host tạo địa chỉ IPv6 toàn cầu bằng cách gắn prefix này với 64 bít định danh giao diện. Để có thể tự động cấu hình địa chỉ, prefix địa chỉ do router quảng bá phải có độ dài /64.

- Đồng thời host cũng thiết lập giá trị thời gian sống cho địa chỉ theo giá trị có trong thông điệp quảng bá của router.
- Host đăng ký địa chỉ Multicast Solicited Node tương ứng địa chỉ unicast vừa tạo với card mạng để nhận lưu lượng của địa chỉ này.

❖ Host xác lập các giá trị thông số hoạt động: Hop Limit, thời gian mặc định host thực hiện quy trình kiểm tra khả năng có thể kết nối được của các node lân cận, giá trị MTU của đường kết nối.

Trong trường hợp cụ thể, như hình vẽ trên, host sẽ cấu hình được địa chỉ toàn cầu IPv6:

Địa chỉ IPv6 = Tiền tố mạng + Định danh giao diện = 2001:410:213:1::90:27FF:FE17:FC0F

4.3.6 Đánh số lại thiết bị IPv6

Đánh số lại mạng IPv4 là điều những nhà quản trị rất ngại. Nó ảnh hưởng tới hoạt động mạng lưới và tiêu tốn nhân lực cấu hình lại thông tin cho host, node trên mạng.

Địa chỉ IPv6 được thiết kế có một cách thức đánh số lại mạng một cách dễ dàng hơn. Một địa chỉ IPv6 gắn cho node sẽ có hai trạng thái, đó là "còn được sử dụng – preferred" và "loại bỏ - deprecated" tuỳ theo thời gian sống của địa chỉ đó. Host luôn cố gắng sử dụng các địa chỉ có trạng thái "còn được sử dụng". Thời gian sống của địa chỉ được thiết lập từ thông tin quảng bá của router. Do vậy, các host trên mạng IPv6 có thể được đánh số lại nhờ thông báo của router đặt thời gian hết thời hạn có thể sử dụng cho một tiền tố mạng (network prefix). Sau đó, router thông báo prefix mới để các host tạo lại địa chỉ IP. Trên thực tế, các host có thể duy trì sử dụng địa chỉ cũ trong một khoảng thời gian nhất định trước khi xóa bỏ hoàn toàn.

4.3.7 Quy trình tìm kiếm giá trị PathMTU phục vụ cho việc phân mảnh gói tin IPv6

Mạng, quy mô lớn hay nhỏ, bao gồm các đường kết nối vật lý khác nhau. Mỗi đường kết nối có một giá trị giới hạn về kích thước cực đại của gói tin mà host có thể gửi trên đường kết nối, được gọi là MTU (Maximum Transmition Unit). Trong hoạt động của thế hệ địa chỉ IPv4, trong quá trình chuyển tiếp gói tin, nếu IPv4 router nhận được gói tin lớn hơn giá trị MTU của đường kết nối, router sẽ thực hiện phân mảnh gói tin (fragment) thành những gói tin nhỏ hơn. Sau quá trình truyền tải, gói tin được xây dựng lại nhờ những thông tin trong header.

Địa chỉ IPv6 áp dụng một mô hình khác để phân mảnh gói tin. Mọi IPv6 router không tiến hành phân mảnh gói tin, nhờ đó tăng hiệu quả, giảm thời gian xử lý gói tin. Việc phân mảnh gói tin được thực hiện tại host nguồn, nơi gửi gói tin. Do vậy, trong header cơ bản IPv6, các trường hỗ trợ cho việc phân mảnh và kết cấu lại gói tin (tương ứng IPv4 header) đã được bỏ đi. Những thông tin trợ giúp cho việc phân mảnh và tái tạo gói tin IPv6 được để trong một header mở rộng của gói tin IPv6 (gọi là Fragment Header)[45].

Giá trị MTU tối thiểu mặc định trên đường kết nối IPv6 là 1280 byte. Tuy nhiên, để đến được đích, gói tin sẽ đi qua nhiều đường kết nối có giá trị MTU khác nhau, việc phân mảnh gói tin được thực hiện tại host nguồn, không thực hiện bởi các router trên đường truyền tải. Do vậy, host nguồn cần biết được giá trị MTU nhỏ nhất trên toàn bộ đường truyền từ nguồn tới đích để điều chỉnh kích thước gói tin phù hợp.

Có hai khái niệm về giá trị MTU trong IPv6, đó là:

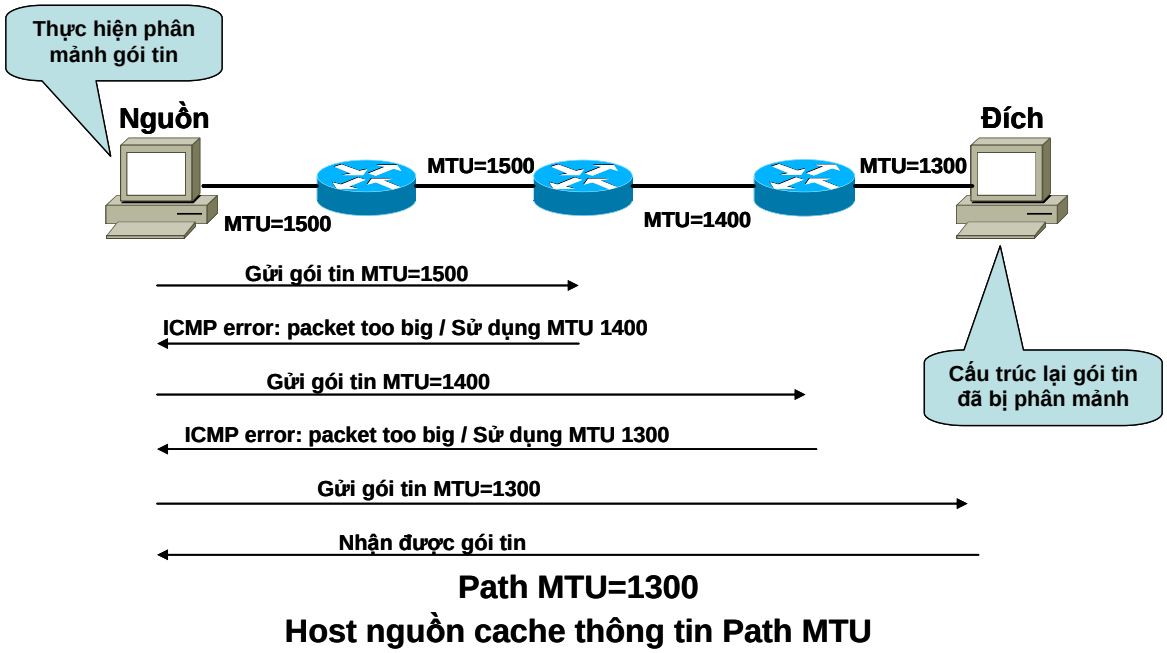
[45] Tham khảo mục II.4.2.5 về header mở rộng của gói tin IPv6

- LinkMTU: Là giá trị MTU trên đường kết nối trực tiếp của host
- PathMTU: Là giá trị MTU nhỏ nhất trên toàn bộ một đường truyền từ nguồn tới đích.

Host nguồn sẽ sử dụng quy trình có tên gọi *Path MTU Discovery* để tìm ra giá trị MTU nhỏ nhất trên đường dẫn từ nguồn đến đích. Khi tìm được, nó sẽ lưu giữ (cache) giá trị này để sử dụng trong giao tiếp.

Quy trình tìm kiếm Path MTU được thực hiện nhờ thông điệp Packet Too Big phản hồi từ router.

Để tìm PathMTU, host nguồn gửi gói tin sử dụng giá trị MTU mặc định trên đường kết nối trực tiếpc của mình. Nếu trên đường truyền, kích thước gói tin vượt quá giá trị MTU của một đường link nào đó, router của đường link phải hủy bỏ gói tin và gửi thông điệp Packet Too Big thông báo, trong gói tin có chứa giá trị MTU của đường kết nối mà router phụ trách. Khi nhận được thông tin này, host sẽ sử dụng giá trị MTU này để gửi lại gói tin. Cứ như vậy cho đến khi gói tin tới được đích và host sẽ lưu giữ lại thông tin về giá trị MTU nhỏ nhất đã dùng (PathMTU) để thực hiện gửi lần sau.



Hình 29: Quy trình thực hiện tìm kiếm Path MTU

4.4 THỦ TỤC MULTICAST LISTENER DISCOVERY (MLD)

4.4.1 Tổng quát về thủ tục MLD

Multicast không phải là một khái niệm mới. Dù được đánh giá là hữu ích và đã được thiết kế hoàn chỉnh, công nghệ multicast không được triển khai rộng rãi trong hoạt động Internet IPv4, do nhiều nguyên nhân: multicast không được kích hoạt một cách mặc định, yêu cầu rất nhiều cấu hình thủ công. Khi định tuyến multicast IPv4 được sử dụng, thủ tục hỗ trợ multicast để quản lý quan hệ thành viên nhóm multicast là IGMP[46]. Thủ tục này sử dụng một tập hợp thông điệp riêng.

Trong hoạt động của thế hệ địa chỉ IPv6, multicast là bắt buộc. Multicast trong IPv6 thay thế cho cả chức năng broadcast. Việc broadcast gói tin trong một phạm vi nào đó tương ứng với việc gửi thông tin tới nhóm địa chỉ IPv6 multicast mọi node trong phạm vi đó.

Đối với IPv6, multicast sẽ không đòi hỏi cấu hình gì nếu chỉ thực hiện trong phạm vi một đường kết nối. Chúng ta cũng thấy các IPv6 node tham gia các nhóm multicast trên đường kết nối và gửi thông điệp tới các địa chỉ multicast mọi node phạm vi link (FF02::1), địa chỉ multicast mọi router phạm vi link (FF02::2) khi tiến hành các quy trình của thủ tục Neighbor Discovery. Tuy nhiên khi lưu lượng multicast được router chuyển tiếp ra ngoài phạm vi một đường kết nối thì khi đó cần thêm những yếu tố phục vụ thực thi multicast. Đó là thủ tục định tuyến multicast và thủ tục hỗ trợ, quản lý quan hệ thành viên multicast.

Khi thực hiện multicast IPv6 ra ngoài phạm vi một đường kết nối, thủ tục thực hiện quản lý quan hệ thành viên multicast có tên gọi Multicast Listener Discovery-MLD. Thủ tục này thay thế cho IGMP của IPv4. Tuy nhiên, thủ tục này có một điểm khác biệt cơ bản với IGMP là nó hoạt động trên nền các thông điệp ICMPv6, chứ không định nghĩa tập hợp thông điệp riêng.

Multicast Listener Discovery sử dụng một nhóm ba thông điệp ICMPv6. Các thông điệp này được trao đổi giữa router và node, cho phép một router khám phá ra trên mỗi giao diện gắn trực tiếp với nó những node là thành viên của một nhóm multicast, sẵn sàng nhận gói tin được gửi tới địa chỉ multicast đó (node đang "nghe" lưu lượng), cũng như những địa chỉ multicast đang được các node này quan tâm.

Thông tin này được cung cấp bất cứ khi nào thủ tục định tuyến multicast được kích hoạt trên các router, để đảm bảo rằng các gói tin multicast được truyền tải đến mọi đường kết nối nơi có những node muốn nhận lưu lượng này.

MLD phân định cách thức cư xử khác nhau cho router và cho host nghe lưu lượng multicast. Nếu tại một địa chỉ multicast, router vừa đóng vai trò router, bản thân cũng nghe và muốn nhận lưu lượng tại địa chỉ này, thì router cần thực hiện cả hai phần của thủ tục: phần thủ tục cho router và phần thủ tục cho host nghe lưu lượng multicast.

Router sử dụng MLD để tìm ra xem địa chỉ multicast nào có node đang chờ nhận lưu lượng trên mỗi đường kết nối trực tiếp của nó. Mỗi router duy trì một danh sách, cho mỗi đường kết nối, chứa thông tin về địa chỉ multicast có node muốn nhận lưu lượng trên đường kết nối đó. MLD chỉ tìm ra danh sách những địa chỉ multicast mà ít nhất có một node đang nhận lưu lượng, chứ không phải là danh sách những node đang nghe lưu lượng tương ứng với mỗi địa chỉ multicast.

[46] IGMP: Internet Group Management Protocol

4.4.2 Ba thông điệp ICMPv6 sử dụng trong thủ tục MLD:

Thủ tục MLD sử dụng ba thông điệp ICMPv6 sau đây:

Multicast Listener Query (giá trị ICMPv6 type 130)

Multicast Listener Query được sử dụng bởi router để truy vấn về những node đang nghe lưu lượng multicast trên một đường kết nối. Có hai dạng thông điệp Multicast Listener Query: *Truy vấn thông thường* và *Truy vấn gắn với địa chỉ multicast cụ thể* . Truy vấn thông thường được sử dụng để truy vấn mọi node của mọi địa chỉ multicast. Truy vấn gắn với địa chỉ multicast cụ thể được sử dụng để truy vấn những node đang nghe một địa chỉ multicast nhất định.

Multicast Listener Report (giá trị ICMPv6 type 131)

Multicast Listener Report được node đang nghe lưu lượng tại một địa chỉ multicast sử dụng để báo cáo rằng mình đang sẵn sàng nhận lưu lượng multicast. Thông điệp này cũng được sử dụng để đáp trả lại thông điệp truy vấn Multicast Listener Query của router.

Multicast Listener Done (giá trị ICMPv6 type 132)

Multicast Listener Done được node đang nghe lưu lượng multicast sử dụng để thông báo rằng nó không còn muốn nhận lưu lượng của địa chỉ multicast cụ thể nào đó nữa.

Khi một node từ bỏ không còn nhận lưu lượng của một địa chỉ multicast, nó gửi một thông điệp Multicast Listener Done tới địa chỉ multicast mọi router phạm vi link (FF02::2), thông tin mang trong gói tin là địa chỉ multicast mà nó không còn muốn nghe lưu lượng.

4.5 HƯỚNG DẪN THIẾT LẬP MÔ HÌNH MẠNG THỰC HÀNH QUAN SÁT GIAO TIẾP VÀ HOẠT ĐỘNG CỦA CÁC NODE IPV6.

4.5.1 Cấu hình IPv6 trên Cisco router

Thiết bị mạng của Cisco hỗ trợ IPv6 từ rất sớm, tuy nhiên không phải mọi phiên bản HĐH của Cisco router đều hỗ trợ IPv6. Bạn đọc có thể truy cập website của Cisco tại http://www.cisco.com để kiểm tra phiên bản OS mình đang sử dụng có hỗ trợ IPv6 hay không.

Trong hệ điều hành có hỗ trợ IPv6, định tuyến IPv6 mặc định được tắt đi trong Cisco IOS. Để kích hoạt định tuyến IPv6, trước tiên cần kích hoạt chuyển tiếp lưu lượng IPv6 trên router và gắn địa chỉ IPv6 cho các giao diện của router.

Để thực hiện kích hoạt định tuyến IPv6 trên một router Cisco, bạn cần thực hiện những thao tác sau đây:

- Kích hoạt xử lý IPv6 toàn diện (bắt buộc)
- Cấu hình địa chỉ cho giao diện (bắt buộc)
- Kiểm tra lại hoạt động của IPv6 và cấu hình địa chỉ (tuỳ chọn)

Cấu hình địa chỉ IPv6 cho router cisco

Một địa chỉ IPv6 cần phải được cấu hình trên giao diện để router có thể chuyển tiếp lưu lượng trên giao diện. Việc cấu hình một địa chỉ toàn cầu trên một giao diện router Cisco sẽ tự động cấu hình địa chỉ IPv6 link-local và kích hoạt IPv6 cho giao diện đó. Giao diện được cấu hình tự động tham gia những nhóm multicast bắt buộc sau đây cho đường kết nối:

- Nhóm multicast Solicited-node FF02:0:0:0:0:1:FF00::/104 cho mỗi địa chỉ unicast và anycast được gắn cho giao diện.
- Nhóm multicast mọi node phạm vi link FF02:0:0:0:0:0:0:1
- Nhóm multicast mọi router phạm vi link FF02:0:0:0:0:0:0:2

Bảng sau đây giới thiệu một số lệnh cơ bản kích hoạt và cấu hình địa chỉ IPv6 trên giao diện router Cisco. Tập hợp các lệnh làm việc với IPv6 các bạn có thể tìm kiếm trên website Cisco.

Kích hoạt IPv6 protocol toàn diện	
Trong chế độ global config Router(config)# **IPv6 unicast-routing**	Lệnh này sẽ kích hoạt chuyển tiếp gói tin IPv6 unicast
Cấu hình địa chỉ IPv6 cho giao diện Cần vào chế độ cấu hình giao diện Router(config)# **interface** *interface-type interface-number*	

1. Router(config-if)# **IPv6 address** *IPv6-prefix/ prefix-length* [**eui-64**]	Lệnh này gắn địa chỉ IPv6 toàn cầu cho một giao diện của router và kích hoạt xử lý IPv6 trên giao diện đó. Nếu cuối lệnh không có từ khóa **eui-64**. địa chỉ IPv6 trong lệnh phải là địa chỉ cụ thể (128 bít), router sẽ gắn cho giao diện địa chỉ IPv6 toàn cầu, với prefix trong lệnh. Khi từ khóa **eui-64** được sử dụng, prefix địa chỉ bắt buộc phải là /64. Trong trường hợp đó, địa chỉ IPv6 được gắn cho giao diện sẽ dựa trên 64 bít prefix địa chỉ đã cung cấp, 64 bít định danh giao diện sẽ được router tự động xây dựng từ địa chỉ card mạng. Chú ý: Trong trường hợp sử dụng router quảng bá thông tin để các host trong mạng LAN tự động cấu hình địa chỉ, thì prefix địa chỉ gắn cho giao diện router bắt buộc phải là /64.
2. Router(config-if)# **IPv6 address** *IPv6-address* {*/prefix-length* | **link-local**}	Lệnh thực hiện gắn địa chỉ cho giao diện và kích hoạt xử lý IPv6 trên giao diện. Nếu dùng lệnh **IPv6 address** *IPv6-address* không có từ khóa **link-local**, lệnh sẽ gắn địa chỉ toàn cầu cho giao diện và kích hoạt IPv6. Địa chỉ link-local của giao diện sẽ được tự động cấu hình Nếu dùng lệnh **IPv6 address** có từ khóa **link-local** sẽ cấu hình địa chỉ link-local trên giao diện. Địa chỉ link-local này được sử dụng thay vì địa chỉ link-local được tự động cấu hình khi IPv6 được kích hoạt trên giao diện đó.
3. Router(config-if)# **IPv6 unnumbered** *interface-type interface-number*	Xác định giao diện không đánh số và kích hoạt xử lý IPv6 trên giao diện đó. Địa chỉ IPv6 toàn cầu của giao diện xác định bởi *interface-type interface-number* sẽ được sử dụng. (Địa chỉ link-local sẽ tự động tạo ra trên giao diện không đánh số khi xử lý IPv6 được kích hoạt)
4. Router(config-if)# **IPv6 enable**	Tự động tạo địa chỉ link-local trên giao diện và kích hoạt xử lý IPv6. Địa chỉ link-local này chỉ có thể được sử dụng để giao tiếp với các node trên cùng một đường link.
Quan sát cấu hình và thông tin	

Những cấu hình đối với IPv6 có thể quan sát được khi sử dụng lệnh

Router# **show running-config**

Và

Router# **show IPv6**

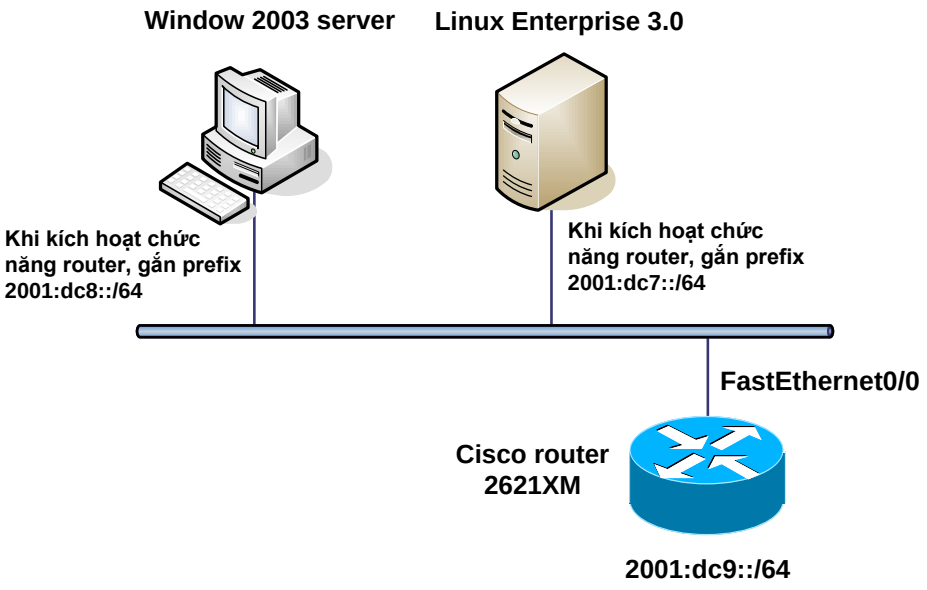
access-list	- Tổng hợp access lists
cef	- Cisco Express Forwarding cho IPv6
interface	- Tình trạng giao diện và cấu hình
neighbors	- Hiển thị IPv6 neighbor cache
prefix-list	- Liệt kê IPv6 prefix
protocols	- Thủ tục định tuyến IPv6
route	- Hiển thị bảng thông tin định tuyến
routers	- Hiển thị các IPv6 router local
traffic	- Thống kê lưu lượng IPv6
tunnel	- Tóm tắt về IPv6 tunnel

Bảng 11: Một số lệnh cấu hình IPv6 trên router Cisco

4.5.2 Hướng dẫn thiết lập mạng và thực hành

Mục tiêu thực hành: Quan sát hoạt động của thủ tục TCP/IPv6: quan sát giao tiếp của các node IPv6, cách thức tự động cấu hình địa chỉ, quảng bá thông tin của router IPv6.

Chuẩn bị: Mạng thực hành được thiết lập như hình vẽ sau. Bao gồm một máy tính cài HĐH Window 2003 server, một máy tính cài HĐH Linux Enterprise 3.0 và một router Cisco 2621XM, sử dụng hệ điều hành c2600-j1s3-mz.123-9.



Hình 30: Mạng thực hành chương 3

Tóm tắt:

- Kích hoạt IPv6 trên router Cisco để router quảng bá thông tin.
- Quan sát cách thức các node trên một đường kết nối giao tiếp với nhau. Quan sát các node tự động cấu hình tự động địa chỉ. Kiểm tra kết nối bằng địa chỉ tự động cấu hình.
- Kích hoạt chức năng router trên máy tính HĐH Linux, window 2003 server.

Các bước thực hiện:

I. Kích hoạt IPv6 trong những máy tính trên mạng LAN

Thực hiện kích hoạt IPv6 protocol trên các máy tính trong mạng LAN. Tắt chức năng tự động tạo định danh giao diện của máy tính cài HĐH window. Tham khảo bài thực hành mục II.6. Chú ý: chỉ kích hoạt IPV6 protocol. Không thực hiện gắn địa chỉ bằng tay. Như vậy những máy tính trong mạng LAN hiện tại chỉ tự động cấu hình được địa chỉ link-local.

1. *Kiểm tra thông tin địa chỉ link-local và chỉ mục giao diện*

ipconfig /all (Máy window)

ifconfig (Máy linux)

2. *Kiểm tra kết nối trong mạng LAN bằng địa chỉ link-local:*

Ping -6 -t *địa_chỉ_link-local_của_máy-linux***%***index_của_giao_diện* (Máy window)

ping6 -I eth0 *địa_chỉ_link-local_của_máy-window* (Máy linux)

3. *Kiểm tra bảng lưu trữ neighbor cache:*

Trên máy window

netsh> interface IPv6>
show neighbors

Trên máy linux

ip -6 neigh show dev eth0

Bạn sẽ thấy hai máy lưu trữ thông tin về các node lân cận (địa chỉ IP, địa chỉ MAC...)

II. Kích hoạt IPv6 và quảng bá thông tin của router Cisco.

4. *Kiểm tra version của HĐH*

show version

Lưu ý: với version phù hợp mới có hỗ trợ IPv6 protocol

Trong bài thực hành này sử dụng c2600-j1s3-mz.123-9

5. *Kiểm tra xem HĐH có hỗ trợ IPv6 không*

Cần vào chế độ cấu hình và kiểm tra xem có tồn tại tập lệnh IPv6 hay không

Vào chế độ cấu hình và đặt tên cho router là "router-IPv6"

Enable

Conf t

Hostname router-IPv6

Kiểm tra xem có tồn tại tập lệnh IPv6 hay không

IPv6 ?

Nếu lệnh không hiển thị tập hợp các lệnh của IPv6 thì hệ điều hành không hỗ trợ thủ tục IPv6.

6. *Kích hoạt xử lý IPv6 trên router*

IPv6 unicast-routing	- kích hoạt một cách toàn diện IPv6 protocol trên router Cisco
ip cef	- kích hoạt chức năng cef router Cisco
IPv6 cef	- kích hoạt chức năng cef cho IPv6

7. *Thực hiện một số lệnh quan sát cấu hình*

Ra khỏi chế độ cấu hình và thực hiện lệnh quan sát thông tin

show IPv6 ?

show IPv6 interface fastethernet 0/0

show IPv6 route

8. *Cấu hình địa chỉ IPv6 cho giao diện*

Khi cấu hình địa chỉ cho một giao diện router, xử lý IPv6 trên router đó sẽ tự động được kích hoạt và theo mặc định, router sẽ quảng bá thông tin qua giao diện đó.

Vào chế độ cấu hình cho giao diện FastEthernet 0/0

Conf t

interface fastethernet 0/0

Đặt prefix cho router cisco và hướng dẫn cho router rằng tự build phần bít còn lại từ địa chỉ MAC

IPv6 address 2001:dc9::/64 eui-64

No shutdown

Sau khi được gắn prefix địa chỉ, router sẽ quảng bá thông tin qua giao diện FastEthernet 0/0

Chú ý: Để các host trong LAN có thể tự động cấu hình địa chỉ, router trong mạng LAN chỉ có thể gắn prefix /64.

9. *Thực hiện một số lệnh quan sát cấu hình*

Ra khỏi chế độ cấu hình và thực hiện lệnh quan sát thông tin

show IPv6 interface fastethernet 0/0

show IPv6 route

show IPv6 traffics

10. Quan sát quảng bá thông tin của router

Bạn có thể quan sát router đang quảng bá thông tin bằng cách bật một cửa sổ bắt gói tin máy tính linux nhận được .

Bật một cửa sổ dòng lệnh mới trên máy linux và sử dụng tcpdump để bắt gói tin

tcpdump -t -n -i eth0 -s 512 -vv ip6 or proto IPv6

Bạn sẽ quan sát thấy *router-IPv6* đang quảng bá thông tin về prefix và những tham số khác cho các máy tính trên đường kết nối.

11. Quan sát tự động cấu hình địa chỉ, tự động cấu hình route

Quan sát lại các host trong mạng LAN (linux, window) trước đây chỉ có địa chỉ link-local bây giờ đã nhận được thông tin quảng bá của router và tự động cấu hình địa chỉ nên địa chỉ IPv6 toàn cầu

Trên máy tính window:

ipconfig

Ghi lại địa chỉ IPv6 của máy tính window:

netsh> interface IPv6>

show routes

Khi nhận được thông tin quảng bá từ router, host sẽ tự động cấu hình địa chỉ, đồng thời route tương ứng prefix địa chỉ quảng bá bởi router cũng sẽ được tự động thiết lập, sử dụng router đã quảng bá thông tin làm gateway mặc định.

Trên máy tính Linux:

ifconfig

ip -6 route show dev eth0

Ghi lại địa chỉ IPv6 của máy tính linux:

12. Sử dụng chương trình ping kiểm tra kết nối bằng địa chỉ vừa tự động tạo

13. Quan sát lại bảng thông tin lưu trữ node lân cận. Bạn sẽ thấy thông tin về những địa chỉ mới này trong bảng lưu trữ thông tin về node lân cận.

III. Kích hoạt máy tính linux, window thực hiện chức năng router.

Trong mạng thử nghiệm, nếu không có thiết bị router chuyên nghiệp Cisco, bạn đọc hoàn toàn có thể sử dụng máy tính (window, linux) làm chức năng router thay thế. Trong phần thực hành này, bạn đọc sẽ được hướng dẫn để

kích hoạt chức năng này trên máy tính và quan sát thấy trên một mạng LAN IPv6, có thể có nhiều router, quảng bá nhiều prefix khác nhau và một giao diện của một IPv6 host có thể một lúc được cấu hình nhiều địa chỉ.

14. Kích hoạt chức năng router của máy window.

Kích hoạt chức năng chuyển tiếp gói tin và quảng bá thông tin trên giao diện vật lý "Local Area Connection"

netsh> interface IPv6>

set interface "Local Area Connection" forwarding=enabled advertise=enabled store=active

Gắn prefix địa chỉ cho giao diện, tạo tuyến và xác định quảng bá thông tin qua giao diện:

add route 2001:dc8::/64 "Local Area Connection" publish=yes

15. Kích hoạt chức năng router của máy Linux:

Để máy tính cài HĐH Linux có thể thực hiện chức năng chuyển tiếp gói tin và quảng bá thông tin của router IPv6, cần cài đặt gói tin radvd và sửa đổi thông tin cấu hình cần thiết (trong file cấu hình /etc/radvd.conf)

Cài đặt gói tin radvd-0.7.2-9.i386.rpm

Bạn đọc có thể download gói tin tại website www.rpmfind.net và lưu vào một thư mục trên máy linux. Chuyển đến thư mục lưu trữ gói tin và thực hiện lệnh cài đặt:

rpm –Uvh radvd-0.7.2-9.i386.rpm

Kích hoạt chức năng IPv6 forwarding và debug

sysctl -w net.IPv6.conf.all.forwarding=1

hoặc sửa bằng tay (sử dụng vi) file **/proc/sys/net/IPv6/conf/all/forwarding.** Đặt giá trị là ***1***

radvd --debug 0

Sửa đổi file cấu hình của radvd để router quảng bá đúng prefix cần thiết.

Cách thức cư xử của router, thông tin quảng bá được cấu hình trong file cấu hình của radvd (/etc/radvd.conf)

vi /etc/radvd.conf

Cấu hình prefix cần thiết (**2001:dc7::/64**) thay thế cho prefix 3FFE::/64 mặc định

Kích hoạt radvd

/etc/init.d/radvd start

IV. Quan sát lại thông tin cấu hình của các máy tính.

Tiến hành quan sát lại thông tin cấu hình của các máy tính trong mạng LAN thử nghiệm, bạn sẽ thấy giao diện vật lý của các máy đồng thời được gắn nhiều địa chỉ tự động tạo ra tương ứng các prefix địa chỉ quảng bá bởi router và tự động tạo các route tương ứng các prefix đã được quảng bá bởi các router trong mạng LAN.

Hỏi – đáp cuối chương 4:

1. Bạn cho biết hai loại thông điệp ICMPv6 ?

T: Các thông điệp ICMPv6 đươc phân chia làm hai loại: ***Thông điệp lỗi*** và ***Thông điệp thông tin***. Các thông điệp lỗi được sử dụng để báo lỗi trong quá trình chuyển tiếp và phân phối gói tin IPv6, thực hiện bởi node đích hoặc router. Thông điệp thông tin ICMPv6 được sử dụng để cung cấp chức năng chẩn đoán và những chức năng mở rộng khác, phục vụ cho các quy trình hoạt động của địa chỉ IPv6.

2. Tại sao nói ICMPv6 cung cấp cơ cấu hoạt động cho hai thủ tục Multicast Listener Discovery (MLD) và Neighbor Discovery (ND) ?

T Thủ tục IP phiên bản 6 thực hiện thực hiện tiêu chuẩn hoá và tổ hợp nhiều chức năng, quy trình riêng biệt của giao tiếp giữa các node trên một đường kết nối. Các quy trình, thủ tục này đều sử dụng thông điệp ICMPv6. Multicast Listener Discovery (MLD) - Thủ tục quản lý quan hệ thành viên multicast, phục vụ cho định tuyến multicast và Neighbor Discovery (ND) – thủ tục đảm nhiệm thực thi giao tiếp giữa các node trong một đường kết nối đều sử dụng thông điệp ICMPv6. Do vậy nói ICMPv6 cung cấp cơ cấu hoạt động cho hai thủ tục này.

3. Để định danh các dạng gói tin ICMPv6, người ta sử dụng những trường thông tin nào trong ICMPv6 header ?

T ICMPv6 header có hai trường phục vụ phân loại các dạng gói tin IPMPv6. Đó là trường Type (8 bít) và trường Code (8 bít).

4. Thủ tục ND sử dụng những loại thông điệp ICMPv6 nào?

T: Trong các quy trình giao tiếp thủ tục ND phụ trách, sử dụng năm loại thông điệp ICMPv6 sau đây:

   a. Router Solicitation
   b. Router Advertisement
   c. Neighbor Solicitation
   d. Neighbor Advertisement
   e. Redirect

5. Hãy nêu khái quát chức năng của thủ tục Neighbor Discovery (ND) ?

T Neighbor Discovery (ND) là thủ tục mới trong IPv6. Trong hoạt động của địa chỉ IPv6, giao tiếp giữa các node trên cùng một đường kết nối là vô cùng quan trọng. Thủ tục ND đảm nhiệm những quy trình giao tiếp giữa các node trên một đường kết nối (gọi là các node lân cận): host với host, host với router. Nhờ vậy, một IPv6 node khám phá ra các node lân cận, những thông tin về chúng, và những thông số quan trọng khác phục vụ cho giao tiếp. ND còn đảm nhiệm những chức năng như phân giải địa chỉ, tham số giao tiếp, tự động cấu hình địa chỉ và một số quy trình khác nữa.

6. Nếu một router IPv6 muốn quảng bá sự hiện diện của mình và thông báo cho các node khác trên cùng đường link các tham số hoạt động, nó sẽ gửi đi thông điệp ICMPv6 nào?

T Trong số những thông điệp ICMPv6 sử dụng trong thủ tục Neigbor Discovery, thông điệp Router Advertisement có một vai trò đặc biệt. Router IPv6 sẽ định kỳ gửi gói tin Router Advertisement tới địa

chỉ đích multicast mọi node phạm vi link (FF02::1) nhằm thông báo sự hiện diện của mình và thông báo cho các node khác trên đường link những tham số cần thiết cho hoạt động giao tiếp.

7. Tại sao nói quá trình phân giải địa chỉ của địa chỉ IPv6 có ưu điểm so với địa chỉ IPv4 ?

T: Quy trình phân giải địa chỉ, để một node có thể tìm được địa chỉ lớp link-layer tương ứng địa chỉ IP diễn ra rất thường xuyên trên một đường link. Khi một IPv6 node thực hiện quy trình này, nó không thực hiện gửi gói tin truy vấn tới mọi node trên đường link bằng địa chỉ multicast mọi node phạm vi link (FF02::1), mà chỉ gửi tới địa chỉ Multicast Solicited Node tương ứng địa chỉ unicast cần phân giải. Do vậy chỉ có node có địa chỉ đang cần phân giải phải xử lý gói tin. Điều này là một ưu điểm so với địa chỉ IPv4.

8. Khi một IPv6 host muốn kiểm tra trùng lặp địa chỉ, nó sẽ sử dụng địa chỉ nào làm địa chỉ nguồn trong gói tin truy vấn?

T Host sẽ sử dụng địa chỉ đặc biệt "::" để thể hiện rằng hiện tại nó chưa được gắn địa chỉ.

9. Router IPv6 ngoài chức năng chuyển tiếp gói tin cho các host, còn thực hiện chức năng nào khác so với router IPv4 ?

T Ngoài chức năng chuyển tiếp gói tin cho IPv6 host, IPv6 router còn thực hiện một chức năng vô cùng quan trọng trong hoạt động của thế hệ địa chỉ IPv6, đó là quảng bá sự hiện diện của mình và quảng bá những thông tin, tham số hỗ trợ hoạt động của IPv6 host qua việc định kỳ gửi gói tin Router Advertisement và gửi RA đáp trả khi nhận được thông điệp yêu cầu (Router Solicitation) từ các host. Chính nhờ sự quảng bá của router, IPv6 host có thể cấu hình địa chỉ và nhận được các tham số cho hoạt động giao tiếp.

CHƯƠNG 5: CÁC CÔNG NGHỆ CHUYỂN DỊCH TỪ IPV4 SANG IPV6

Thay thế chuyển đổi một giao thức Internet không phải điều dễ dàng. Trong lịch sử hoạt động Internet toàn cầu, địa chỉ IPv6 không thể tức khắc thay thế IPv4, trong thời gian ngắn. Đây phải là quá trình dần dần. Thế hệ địa chỉ IPv6 phát triển khi IPv4 đã hoàn thiện và hoạt động trên mạng lưới rộng khắp toàn cầu. Trong thời gian đầu phát triển, kết nối IPv6 cần thực hiện trên cơ sở hạ tầng mạng lưới IPv4. Mạng IPv6 và IPv4 sẽ cùng song song tồn tại trong thời gian dài, thậm chí mãi mãi. Trong phần nội dung này, bạn đọc sẽ tìm hiểu các công nghệ chuyển đổi IPv6 – IPv4 và thực hiện một bài thực hành thiết lập và sử dụng dịch vụ tạo đường hầm (tunnel) miễn phí hiện đang được cung cấp trên Internet để có được địa chỉ IPv6 sử dụng trong mạng Lab cũng như kết nối được mạng Lab của mình tới Internet IPv6 và những mạng IPv6 khác, sử dụng kết nối Internet IPv4.

Chương 5 có các nội dung chính sau:

- Tổng quan về các công nghệ chuyển dịch từ IPv4 sang IPv6
- Một số công nghệ tạo đường hầm tunnel
- Hướng dẫn thực hành thiết lập và sử dụng đường hầm

5.1 TỔNG QUAN VỀ CÁC CÔNG NGHỆ CHUYỂN DỊCH IPV4/IPV6

Chuyển đổi sử dụng từ thủ tục IPv4 sang thủ tục IPv6 không phải là một điều dễ dàng. Trong trường hợp thủ tục IPv6 đã được tiêu chuẩn hóa hoàn thiện và hoạt động tốt, việc chuyển đổi có thể được thúc đẩy thực hiện trong một thời gian nhất định đối với một mạng nhỏ, mạng của một tổ chức. Tuy nhiên khó có thể thực hiện ngay được đối với một mạng lớn. Đối với Internet toàn cầu, có thể nói là không thể. Thủ tục IPv6 phát triển khi IPv4 đã được sử dụng rộng rãi, mạng lưới IPv4 Internet hoàn thiện, hoạt động dựa trên thủ tục này. Trong quá trình triển khai thế hệ địa chỉ IPv6 trên mạng Internet, không thể có một thời điểm nhất định mà tại đó, địa chỉ IPv4 được hủy bỏ, thay thế hoàn toàn bởi thế hệ địa chỉ mới IPv6. Hai thế hệ mạng IPv4, IPv6 sẽ cùng tồn tại trong một thời gian rất dài. Trong quá trình phát triển, các kết nối IPv6 sẽ tận dụng cơ sở hạ tầng sẵn có của IPV4.

Do 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:

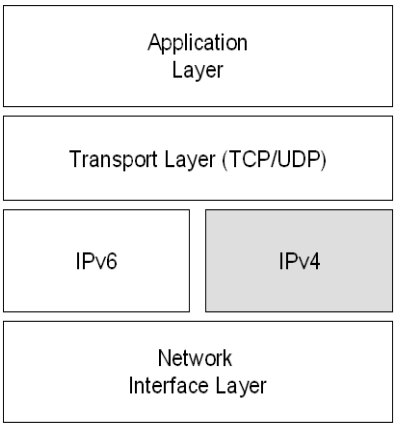
(1) Dual-stack: Cho phép IPv4 và IPv6 cùng tồn tại trong cùng một thiết bị mạng.

(2) 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.

(3) 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.

5.1.1 Dual-stack

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



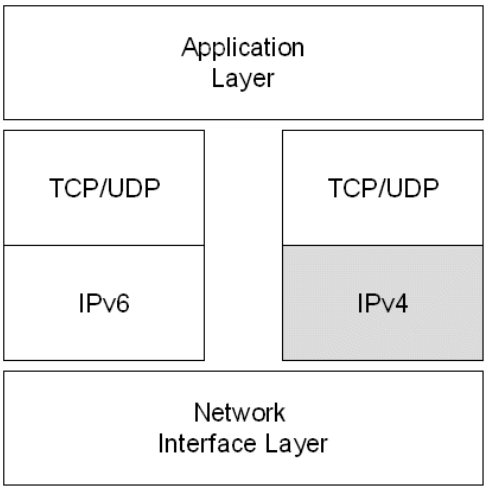
Hình 31: Dual-stack

Ứng dụng hỗ trợ dual-stack sẽ hoạt động được cả với địa chỉ IPv4 và địa chỉ IPv6. Việc lựa chọn địa chỉ có thể tdựa trên kết quả trả về của truy vấn DNS. Thông thường, địa chỉ IPv6 trong kết quả trả về của DNS sẽ được lựa chọn so với địa chỉ IPv4.

Về ứng dụng hiện nay hoạt động dual-stack, có thể lấy ví dụ: HĐH Window XP, Window 2003, HĐH của router Cisco.

Dual stack trong HĐH window:

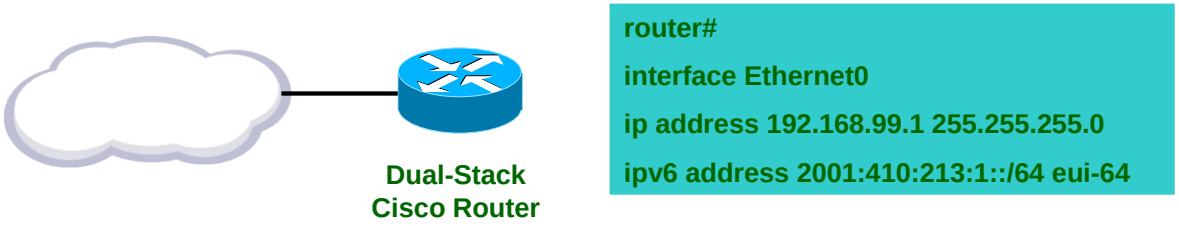
Thực tế, thủ tục IPv6 trong HĐH window chưa phải là dual-stack đúng nghĩa. Driver của IPv6 protocol (Tcpip6.sys) chứa hai thực thi tách biệt của TCP, UDP, tuy nhiên cũng được đề cập như một thực thi dual-stack.



Hình 32: Dual-stack trong HĐH Window

Dual stack trong HĐH 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.



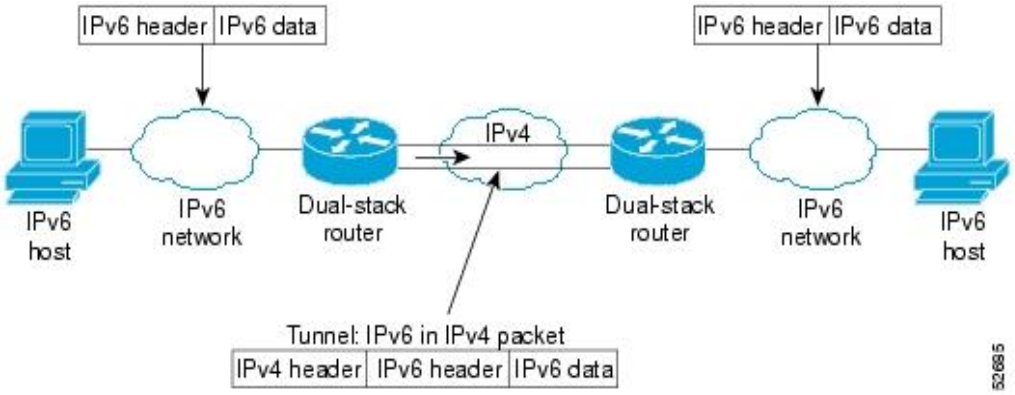
Hình 33: Dual-stack trong HĐH Cisco

5.1.2 Công nghệ đường hầm (Tunnel)

Địa chỉ IPv6 phát triển khi Internet IPv4 đã sử dụng rộng rãi và có một mạng lưới toàn cầu. Trong thời điểm rất dài ban đầu, các mạng IPV6 sẽ chỉ là những ốc đảo, thậm chí là những host riêng biệt trên cả một mạng lưới IPv4 rộng lớn. Làm thế nào để những mạng IPv6, hay thậm chí những host IPv6 riêng biệt này có thể kết nối với nhau, hoặc kết nối với mạng Internet IPV6 khi chúng chỉ có đường kết nối IPv4. Sử dụng chính cơ sở hạ tầng mạng IPv4 để kết nối IPv6 là mục tiêu của công nghệ 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 có header IPv4 và truyền tải đi trong mạng IPv4 tại điểm đầu và gỡ bỏ IPv4 header, nhận lại gói tin IPv6 ban đầu tại điểm đích cuối đường truyền IPv4.



Hình 34: Công nghệ đường hầm - Tunnel

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 đường hầm 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

Với nhiều công nghệ tạo đường hầm khác nhau, các IPv6 host, hay mạng IPv6 riêng biệt hiện nay trên Internet đều có thể có kết nối IPv6, và kết nối vào mạng Internet IPV6 để thử nghiệm, tìm hiểu, trao đổi thông tin. Tất nhiên các host và mạng này phải có kết nối Internet IPv4 và lựa chọn một công nghệ đường hầm phù hợp.

Một số công nghệ đường hầm sẽ được mô tả cụ thể trong các mục tiếp theo giúp bạn đọc có thể hình dung và lựa chọn công nghệ phù hợp với mục đích và nhu cầu của mình.

5.1.2.1 Phân loại công nghệ Tunnel

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 hầm sẽ có dạng kết nối điểm-điểm hay điểm – đa điểm. Dựa theo cách thức thiết lập điểm đầu và cuối đường hầm, công nghệ tunnel có thể phân thành hai loại: *tunnel bằng tay* và *tunnel tự động*

- ***Tunnel bằng tay (Configured)***

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 tại các điểm kết thúc đường hầm. 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 IPv6.

❖ ***Tunnel tự động (Automatic)***

Tunnel tự động là công nghệ tạo đường hầm trong đó không đòi hỏi cấu hình địa chỉ IPv4 của điểm bắt đầu và kết thúc đường hầm bằng tay. Địa chỉ IPv4 của điểm bắt đầu và kết thúc đường hầm được suy ra từ địa chỉ nguồn và địa chỉ đích của gói tin IPv6.

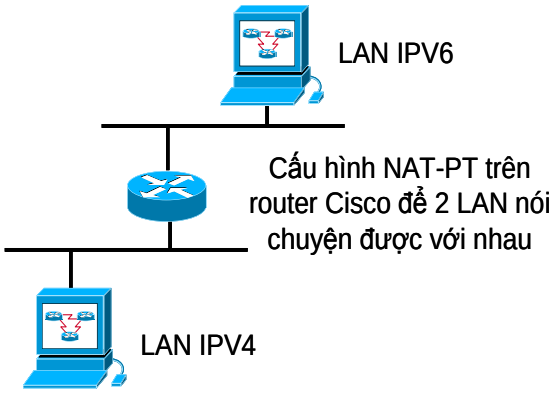
5.1.2.2 Nguyên tắc hoạt động của việc tạo đường hầm:

Nguyên tắc của việc tạo đường hầm trong công nghệ tunnel như sau:

- ❖ Xác định thiết bị kết nối tại các điểm đầu và cuối đường hầm. Hai thiết bị này phải có khả năng hoạt động dual-stack[47].
- ❖ Trên hai thiết bị mạng (có kết nối Internet IPv4) tại đầu và cuối đường hầm, 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.
- ❖ Xác định địa chỉ IPv4 và địa chỉ IPv6 tại nguồn và đích của giao diện tunnel. 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.

5.1.3 Công nghệ chuyển dịch

Công nghệ chuyển đổi thực chất là một dạng công nghệ NAT, thực hiện biên dịch địa chỉ và dạng thức của header, 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 lại header và địa chỉ cho phép mạng IPv6 nói chuyện với mạng IPv4.



Hình 35: Công nghệ biên dịch NAT-PT

[47] Dual-stack: Một dual-stack node là một node làm việc với cả IPv4 và IPv6.

5.2 MỘT SỐ CÔNG NGHỆ TẠO ĐƯỜNG HẦM TUNNEL

5.2.1 Đường hầm cấu hình nhân công

Đây là hình thức tạo đường hầm được áp dụng khi muốn có một kết nối ổn định, riêng biệt, thường giữa hai mạng IPv6, có kết nối IPv4 thông qua hai router biên. Nếu hai router biên này có khả năng hoạt động dual stack, người ta có thể cấu hình bằng tay một đường hầm (tunnel) giữa hai router biên nhằm kết nối hai mạng IPV6 sử dụng cơ sở hạ tầng mạng IPv4. Đường hầm bằng tay cũng được sử dụng để cấu hình giữa router và host nhằm kết nối một IPv6 host vào một mạng IPv6 từ xa. Cấu hình bằng tay đường hầm giữa host và router được áp dụng trong công nghệ Tunnel Broker, đề cập chi tiết tại mục sau.

Trên hai thiết bị tại hai điểm bắt đầu và kết thúc đường hầm, người quản trị sẽ cấu hình bằng tay giao diện tunnel; địa chỉ IPv4, địa chỉ IPv6 gắn cho giao diện tunnel tại các thiết bị được cấu hình bằng tay cùng với tuyến (route) để các lưu lương IPv6 đi qua giao diện tunnel.

Tunnel cấu hình bằng tay tương đương với một đường kết nối IPv6 ảo vĩnh viễn giữa hai miền IPv6 trên cơ sở hạ tầng mạng IPv4, cho một kết nối ổn định, riêng biệt giữa hai điểm xác định. Dạng kết nối tunnel này là kết nối điểm – điểm. Tuy nhiên, nó đòi hỏi cấu hình, quản trị thủ công. Nếu muốn kết nối tới nhiều điểm, sẽ phải tạo nhiều cặp giao diện tunnel và nhiều đường tunnel.

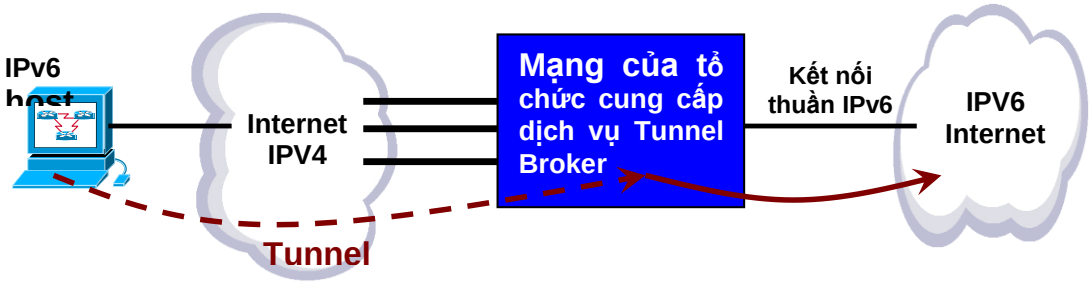
Trong trường hợp một tổ chức có hai phân mạng IPv6 tại hai vùng địa lý và chỉ có cơ sở hạ tầng IPv4 giữa hai phân mạng này. Khi đó, để kết nối hai phân mạng IPv6, tạo một tunnel cấu hình bằng tay giữa hai router biên của hai phân mạng có thể là sự lựa chọn tốt nhất để có một kết nối ổn định.

5.2.2 Tunnel Broker

Trong thời điểm ban đầu triển khai IPv6 hiện nay, việc chia sẻ thông tin, cũng như hỗ trợ, kết nối với nhau là rất quan trọng. Nhiều tổ chức lớn, ISP lớn có khả năng xây dựng đường truyền IPv6, kết nối với nhau và với những mạng IPv6 lớn, hình thành nên Internet IPv6 toàn cầu. Nhiều tổ chức, hay cá nhân khác không có được những đường truyền thuần IPv6 như vậy. Để hỗ trợ về kết nối IPv6, trên Internet hiện nay có nhiều tổ chức đứng ra làm trung gian, cho phép các tổ chức, cá nhân khác thiết lập đường hầm IPv6 trên cơ sở hạ tầng mạng IPv4 tới mạng của tổ chức trung gian, từ đó kết nối tới được Internet IPv6 hoặc các mạng IPv6 khác mà mạng lưới của tổ chức trung gian có nối tới. Một trong những công nghệ được sử dụng để thực hiện điều này là 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.

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 cung cấp Tunnel Broker có kết nối tới Internet IPV6 và những mạng IPv6 khác. 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. Công nghệ tạo đường hầm trong Tunnel Broker là tạo đường hầm bằng tay.



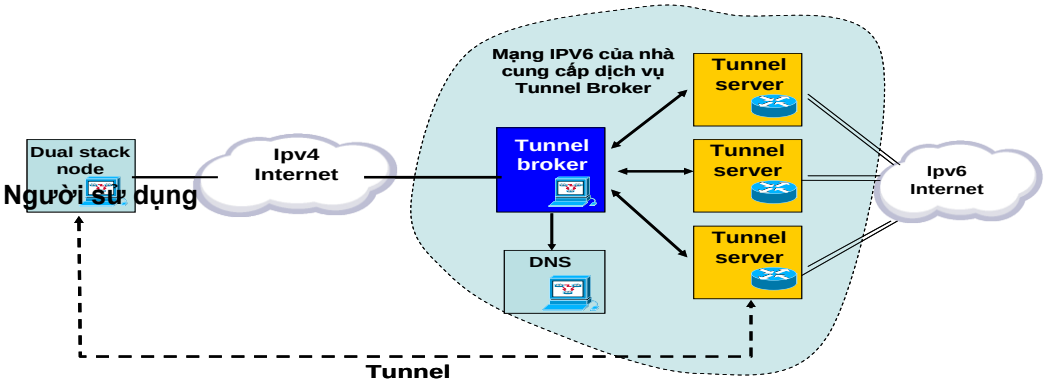
Hình 36: Kết nối IPv6 với Tunnel Broker

Tổ chức duy trì Tunnell Broker sẽ cung cấp cho người sử dụng:

- Một vùng địa chỉ IPv6 từ không gian địa chỉ IPv6 của nhà cung cấp dịch vụ tunnel broker, thoả mãn nhu cầu của người sử dụng.
- Chuyển giao cho người sử dụng một tên miền cấp dưới không gian tên miền của nhà cung cấp dịch vụ Tunnel Broker. Đây là 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
- Các thông tin và hướng dẫn để người sử dụng thiết lập đường hầm (tunnel) đến mạng của tổ chức cung cấp Tunnel Broker.

5.2.2.1 Mô hình tunnel broker

Mô hình của một Tunnel Broker như sau:



Hình 37: Mô hình của Tunnel Broker

Trong đó

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 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.

5.2.2.2 Liên hệ giữa người sử dụng và tổ chức cung cấp Tunnel Broker.

Đăng ký sử dụng dịch vụ Tunnel Broker

Nếu người sử dụng chỉ muốn kết nối một host vào mạng IPv6 của nhà cung cấp tunnel broker, sẽ được cấp một địa chỉ (/128). Nếu người sử dụng muốn thiết lập và kết nối một mạng thì sẽ được 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 cần nhiều hơn một subnet)

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 đường hầm phía người sử dụng.
- Địa chỉ IPv4 phía server (địa chỉ IPv4 của một dual-stack router của nhà cung cấp Tunnel Broker). Đây là địa chỉ IPv4 của đầu đường hầm 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. Đây là địa chỉ IPv6 của dual-stack router của nhà cung cấp Tunnel Broker, là địa chỉ IPv6 của đường hầm phía nhà cung cấp dịch vụ.
- 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 kết nối tới mạng của nhà cung cấp dịch vụ tunnel broker. Đây là tunnel cấu hình bằng tay. Trên các hệ điều hành khác nhau, tập hợp lệnh để cấu hình đường hầm bằng tay sẽ khác nhau. .

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

5.2.2.3 Một số tổ chức cung cấp dịch vụ Tunnel Broker

Hiện nay ở Việt Nam và trên thế giới, có rất nhiều tổ chức cung cấp dịch vụ Tunnel Broker miễn phí. Ban có thể tham khảo danh sách sau đây và đăng ký sử dụng dịch vụ Tunnel của các tổ chức này:

http://ipv6.vn (Ban Công tác thúc đẩy IPv6 Quốc gia – Trung tâm Internet Việt Nam)

http://go6.vn (NetNam – Việt Nam)

http://tunnelbroker.IPv6.net.au (Úc)
http://tunnel.be.wanadoo.com (Bỉ)
http://www.hexago.com/ (Canada)
http://tb.6test.edu.cn/ (Trung Quốc)
http://tunnelbroker.IPv6.estpak.ee/ (Estonia)
http://tb.ngnet.it (Italia)
http://www.iij.ad.jp/en/IPv6/zikken-e.html (Nhật Bản)
http://tbroker.manis.net.my/ (Malaysia)
http://www.sixxs.net/ (Hà Lan)
http://www.uninett.no/ (Nauy)
http://tb.ptin.euro6ix.org/ (Thổ Nhĩ Kỳ)
http://tunnel-broker.singnet.com.sg/ (Singapore)
http://www.xs26.net (Slovakia)
http://tunnelbroker.as8758.net/ (Thuỵ Sĩ)
http://tb.IPv6.chttl.com.tw/ (Đài Loan)
http://tb.IPv6.btexact.com (Anh)
http://tunnelbroker.net (Mỹ)

5.2.3 Công nghệ tunnel 6to4

6to4 là công nghệ sử dụng địa chỉ IPv4 toàn cầu tạo ra các khối địa chỉ IPv6 riêng, khác biệt với địa chỉ IPv6 cấp bởi các tổ chức quản lý tài nguyên quốc tế (thường được gọi là địa chỉ thuần IPv6). Những khối địa chỉ tạo nên từ IPv4 này sẽ dùng cho các mạng IPv6 6to4, đồng thời thiết lập đường hầm tự động kết nối các mạng này, coi cơ sở hạ tầng IPv4 như một môi trường kết nối vật lý ảo.

IANA cấp riêng một tiền tố địa chỉ 2002::/16 thuộc vùng địa chỉ unicast định danh toàn cầu dành cho công nghệ 6to4. Tiền tố địa chỉ này sẽ kết hợp với một địa chỉ IPv4 toàn cầu để tạo nên một khối địa chỉ IPv6, được gọi là địa chỉ 6to4. Các mạng, thiết bị IPv6 sử dụng dạng địa chỉ này được gọi tên là mạng IPv6 6to4. Các mạng và thiết bị 6to4 kết nối với nhau bằng công nghệ tunnel tự động, sử dụng cơ sở hạ tầng mạng IPv4, tạo nên một thế giới 6to4

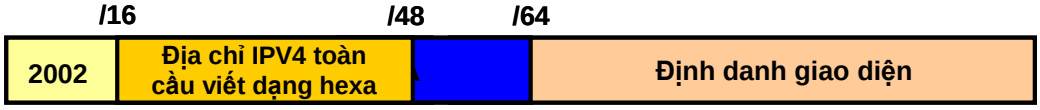
riêng. Tuy nhiên, các mạng 6to4 không chỉ kết nối với nhau, chúng còn có thể kết nối tới Internet sử dụng địa chỉ thuần IPv6 bằng một thiết bị thực hiện vai trò cầu nối. Thiết bị này có tên gọi 6to4 relay router.

Công nghệ tunnel 6to4 còn cho phép một host có địa chỉ IPv4 toàn cầu dễ dàng trở thành một IPv6 6to4 host và truy cập Internet IPv6 mà không cần cấu hình phức tạp. Hệ điều hành Window XP, Window 2003 server hỗ trợ tự động cấu hình sẵn giao diện ảo 6to4 tunnel khi máy tính được kích hoạt thủ tục IPv6 protocol. Khi tiến hành kích hoạt thủ tục IPv6 trên một máy tính có kết nối Internet IPv4 với một địa chỉ IPv4 toàn cầu gắn cho card mạng, hệ điều hành sẽ tự động biến máy tính thành 6to4 host và cấu hình định tuyến mặc định kết nối máy tính với mạng 6to4 của Microsoft. Người sử dụng không cần thiết phải thực hiện thao tác nào để có một đường hầm kết nối tới Internet IPV6. Chúng ta sẽ tìm hiểu đặc điểm này qua bài thực hành mục IV.3

5.2.3.1 Địa chỉ IPv6 sử dụng trong 6to4 tunnel

Prefix địa chỉ 6to4 2002::/16 , kết hợp với 32 bít của một 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 sau:



Hình 38: Cấu trúc đia chỉ IPv6 6to4

Ví dụ, nếu router của bạn đang nối vào Internet IPv4 với địa chỉ 203.119.9.15. Khi đó bạn đang sử hữu một vùng địa chỉ IPv6 6to4 như sau:

2002:cb77:090f::/48

Prefix địa chỉ này được tạo nên bằng cách gắn 16 bít prefix dành riêng của tunnel 6to4 2002::/16 với cb77:090f chính là 32 bít địa chỉ IPv4 được viết dưới dạng hexa.

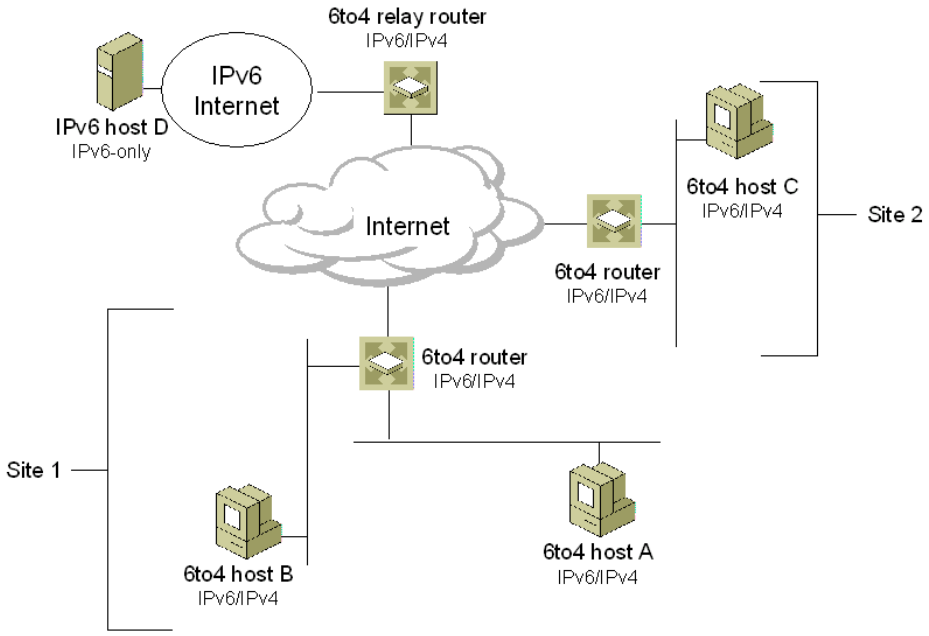
Vùng địa chỉ /48 này bạn có thể sử dụng để phân bổ tạo nên một mạng IPv6 cho tổ chức mình, không cần xin cấp địa chỉ thuần IPv6 từ những tổ chức quản lý địa chỉ quốc tế. Một subnet trong IPv6 được gắn prefix /64. Như vậy, với vùng địa chỉ /48, bạn có 16 bít, và có thể đánh số tới 65536 mạng LAN 6to4. Đây là con số rất lớn và bạn khó có thể sử dụng hết vùng địa chỉ /48 mình đã tạo ra, chỉ từ một địa chỉ IPv4.

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

Tunnel 6to4 là một công nghệ tunnel tự động, 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 không phải kết nối điểm – điểm. Tunnel 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. Tất nhiên, thiết bị tại hai đầu tunnel phải hỗ trợ cả IPv6 và IPv4.

Khung cảnh ứng dụng tunnel 6to4 đon giản nhất là kết nói nhiều IPv6 site riêng biệt, mỗi mạng có ít nhất một đường kết nối tới mạng IPv4 chung qua router biên được gắn địa chỉ IPv4 toàn cầu.

Các thành phần của 6to4 tunnel như sau:



Hình 39: Các thành phần của 6to4 tunnel

Trong đó:

- **6to4 host**

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

- **6to4 router**

  6to4 router là một router dual-stack hỗ trợ sử dụng giao diện 6to4. Router này sẽ chuyển tiếp lưu lượng của một mạng 6to4 tới những router 6to4 thuộc mạng khác. Việc cấu hình router 6to4 đòi hỏi cấu hình bằng tay.

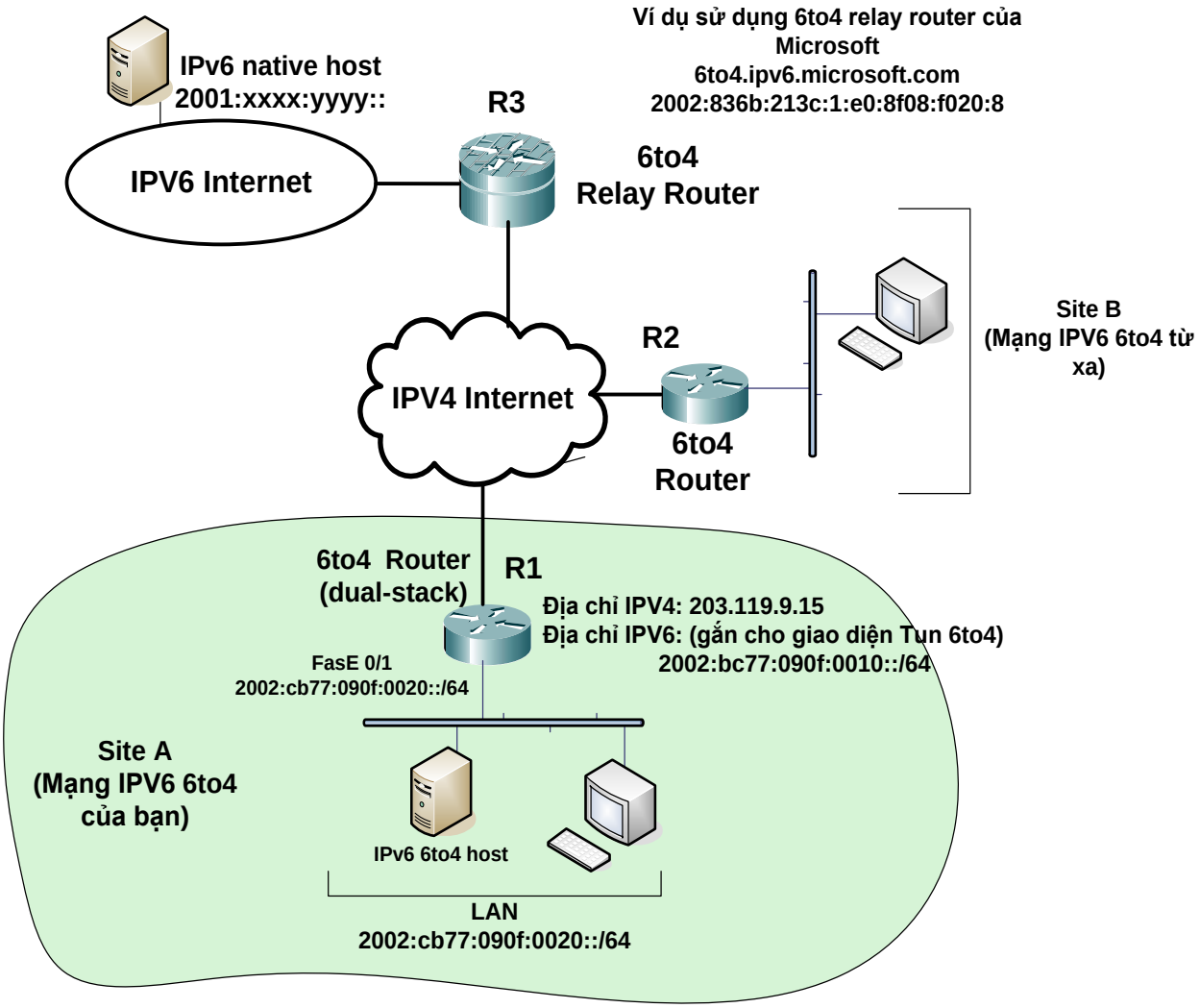
- **6to4 relay router**

  6to4 relay router là một 6to4 router, song được cấu hình để có khả năng chuyển tiếp lưu lượng có địa chỉ 6to4 tới những host trên IPv6 Internet (sử dụng địa chỉ thuần IPv6, được phân bổ bởi hệ thống tổ chức quản lý địa chỉ toàn cầu). 6to4 relay router được cấu hình để hỗ trợ chuyển tiếp định tuyến giữa địa chỉ 6to4 và địa chỉ IPv6 chính thức định danh toàn cầu. 6to4 relay router đóng vai trò cầu nối giữa mạng IPv6 6to4 và IPv6 Internet. Nhờ đó giúp cho những mạng IPv6 6to4 có thể kết nối tới Internet IPV6.

5.2.3.3 Sử dụng 6to4 kết nối Internet IPv6

Lấy một ví dụ về tạo và sử dụng địa chỉ 6to4 kết nối với mạng Internet IPv6 toàn cầu như trong hình vẽ sau:

Một mạng kết nối với Internet IPv4 toàn cầu qua router biên R1 có địa chỉ 203.119.9.15. Từ địa chỉ này, sẽ tạo được một vùng địa chỉ 6to4 2002:cb77:090f::/48. Tổ chức sử dụng vùng địa chỉ 6to4 này để tạo mạng IPv6 và cấu hình R1 thành 6to4 router, nhằm kết nối mạng 6to4 của mình tới các mạng 6to4 khác, và tới Internet IPv6.



Hình 40: Sử dụng tunnel 6to4 kết nối Internet IPv6

Mạng IPv6 có một LAN nội bộ, được gắn vùng địa chỉ 2002:cb77:090f:0020::/64. Để cấu hình R1 thành 6to4 router, cần phải tạo một giao diện ảo cho đường hầm 6to4, gọi tên là "Tun 6to4". Giao diện ảo cho tunnel 6to4 này được gắn subnet 2002:cb77:090f:0010::/64.

Mạng IPv6 6to4 của tổ chức có kết nối Internet IPv4 qua router R1 với địa chỉ 203.119.9.15 gắn tại giao diện FasE 0/1. Nếu tổ chức cấu hình router R1 thành 6to4 router và cấu hình định tuyến mặc định trên router này trỏ tới một 6to4 relay router, ví dụ sử dụng 6to4 relay router của Microsoft, khi đó, mạng IPv6 6to4 của tổ chức (Site A) đã có thể có những kết nối IPv6 sau đây:

- Router R1 sẽ quảng bá prefix 2002:cb77:090f:0020::/64 trên FasE 0/1. Các host trong mạng LAN nội bộ sẽ tự động cấu hình địa chỉ từ prefix quảng bá này và trở thành 6to4 host.

Trên các 6to4 host, định tuyến tương ứng 2002:cb77:090f:0020::/64 route và tuyến mặc định ::/0 trỏ tới R1 cũng được tự động cấu hình.

Các IPv6 6to4 host bên trong mạng LAN giờ hoàn toàn có thể kết nối với nhau.

- 6to4 host trong site A có thể kết nối tới 6to4 host trên các mạng 6to4 khác trong Internet (ví dụ Site B)

  Khi được cấu hình thành 6to4 router, router R1 có cấu hình định tuyến 2002::/16 route đi qua giao diện tunnel 6to4. Do vậy những lưu lượng thuộc địa chỉ 6to4 sẽ được giao diện này đóng gói trong gói tin IPv4 và gửi qua mạng IPv4 tới router biên R2 của site B là đầu kia của đường hầm. Tại đó, R2 sẽ gỡ bỏ IPv4 header, lấy gói tin IPv6 và dựa theo bảng thông tin định tuyến của nó, chuyển tiếp gói tin tới host 6to4 đích trên site B.

- 6to4 host thuộc site A có thể giao tiếp với một host IPv6 được gắn địa chỉ thuần IPV6 (ví dụ địa chỉ có prefix 2001::) của IPv6 Internet.

  Trên router 6to4 của site A có cấu hình định tuyến mặc định ::/0 trỏ tới 6to4 relay router (ví dụ của Microsoft). Khi 6to4 host trong site A chuyển tới router 6to4 R1 những gói tin có địa chỉ thuần IPV6, không phải địa chỉ 6to4, R1 sẽ chuyển những gói tin này qua đường hầm tới 6to4 relay router R3. R3 kết nối tới IPv6 Internet và được cấu hình để thực hiện chức năng chuyển tiếp định tuyến giữa địa chỉ 6to4 và địa chỉ thuần IPV6. 6to4 relay router R3 sẽ chuyển tiếp gói tin tới mạng Internet IPv6.

Chú ý:

Nếu mạng IPv6 6to4 (site A) không chỉ có một phân mạng LAN như trên hình vẽ mà bao gồm nhiều phân mạng con, khi đó cần có cấu trúc định tuyến bên trong site A để định tuyến giữa những mạng LAN 6to4 này. Định tuyến bên ngoài site A chính là định tuyến gói tin IPv4.

5.3 HƯỚNG DẪN THỰC HÀNH THIẾT LẬP VÀ SỬ DỤNG ĐƯỜNG HẦM

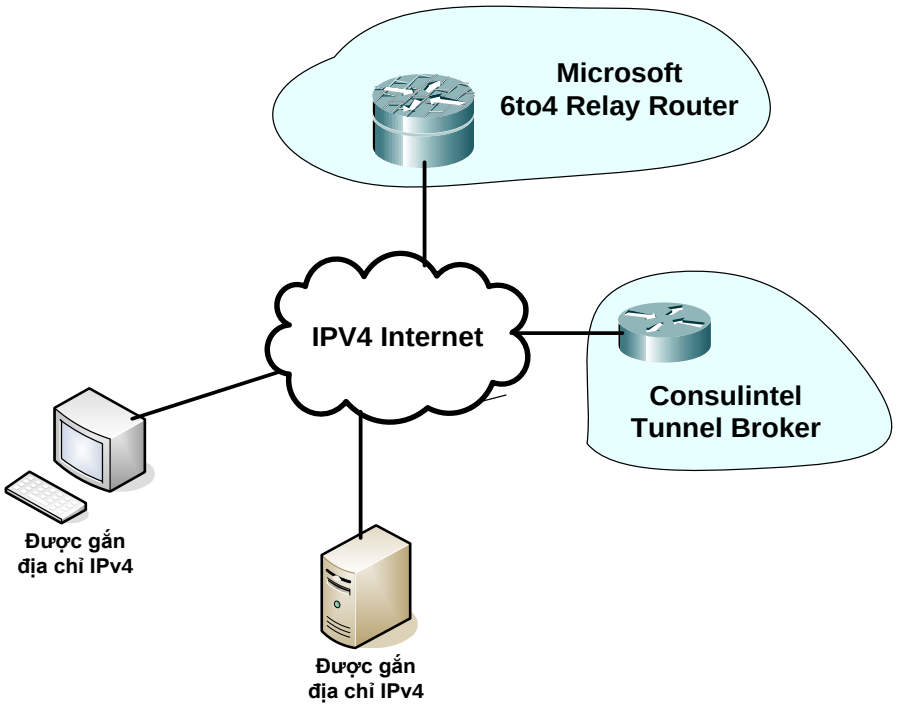
Hiện nay với một máy tính, hay một mạng, bạn đều có thể kết nối vào mạng Internet IPv6 toàn cầu. sử dụng công nghệ tunnel trên cơ sở hạ tầng mạng IPv4 sẵn có.

Thực hành:

Mục tiêu: Sử dụng dịch vụ tunnel để có kết nối IPv6.

Chuẩn bị: Một máy tính cài HĐH window 2003 và một máy tính cài HĐH linux có kết nối Internet IPv4 và được gắn địa chỉ IPv4.

Chú ý: Nếu trong mạng của bạn có sử dụng firewall, bạn cần mở firewall cho protocol 41 vì những gói tin IPv6 sẽ được "bọc" trong gói tin IPv4 có protocol 41. Như vậy bạn mới có thể kết nối được tới những tổ chức đầu kia đường tunnel.



Hình 41: Thực hành sử dụng các dịch vụ tunnel miễn phí

Tóm tắt:

- Sử dụng dịch vụ tunnel 6to4 sẵn có của window để kết nối máy tính vào mạng Internet IPv6.
- Đăng ký sử dụng một dịch vụ Tunnel Broker miễn phí để kết nối máy tính vào mạng Internet IPv6.

Các bước thực hiện:

I. Sử dụng dịch vụ tunnel 6to4 sẵn có của window

Khi bạn kích hoạt IPv6 protocol trên một máy tính có kết nối mạng Internet IPv4 và được gắn sẵn địa chỉ IPv4, window sẽ tự động tạo một giao diện ảo cho tunnel 6to4 và một route mặc định kết nối máy tính với 6to4 relay router của Microsoft. 6to4 relay router của Microsoft được kết nối với 6Bone, do vậy người sử dụng có thể dùng giao diện tunnel 6to4 này để kết nối tới các máy tính 6to4 khác và kết nối với những site thuộc 6Bone sử dụng công nghệ tunnel 6to4 mà không đòi hỏi thêm bất cứ cấu hình bằng tay nào.

1. *Kích hoạt IPv6 protocol trên máy tính window 2003*.

   Tham khảo bài thực hành mục II.6 . Chú ý không gắn địa chỉ IPv6 bằng tay.

2. *Quan sát giao diện ảo dành cho tunnel 6to4*

ipconfig /all

Quan sát phần thông tin liên quan đến giao diện "Tunnel Adapter 6to4 Tunneling Pseudo-Interface"

Ghi lại một số thông tin:

Địa chỉ 6to4 máy tính đã tạo cho giao diện ảo này:

Địa chỉ 6to4 của gateway (chính là 6to4 relayrouter của microsoft)

netsh> interface IPv6

show routes

Bạn sẽ quan sát thấy một số route đã được tự động tạo ra dành cho tunnel 6to4 để định tuyến các gói tin thuộc vùng địa chỉ 2002::/16 qua giao diện "6to4 Tunneling Pseudo-Interface" và một route mặc định cho mọi lưu lượng khác đi qua giao diện "6to4 Tunneling Pseudo-Interface" tới gateway là 6to4 relayrouter của microsoft.

3. *Kiểm tra kết nối IPv6 bằng tunnel 6to4*

Lúc này máy tính của bạn đã có kết nối IPv6, có thể kết nối tới các 6to4 host khác trên toàn cầu. Đồng thời có thể kết nối với mạng thuần IPv6 nhờ có 6to4 relay router của Microsoft.

Kiểm tra kết nối tới 6to4 gateway của Microsoft

ping -6 –t 6to4.IPv6.microsoft.com

Kiểm tra kết nối tới một IPv6 site mà gateway của Microsoft đã giúp kết nối:

ping -6 –t www.kame.net

tracert -6 www.kame.net

4. *Dùng trình duyệt IE kết nối tới một số trang web có hỗ trợ IPv6 và chỉ định thông tin địa chỉ của client.*

Bạn sẽ thấy trên các website này thông báo bạn đang kết nối bằng địa chỉ IPv6 6to4, không phải bởi địa chỉ IPv4.

www.kame.net

www.apnic.net

www.IPv6tf.org

Qua phần thực hành trên, bạn đã kết nối máy tính của mình vào mạng Internet IPv6 mà không cần thêm cấu hình gì nhờ đường kết nối tunnel 6to4 cung cấp bởi Microsoft. Nếu muốn xây dựng một mạng thử nghiệm, bạn cũng có thể xây dựng mạng IPv6 của mình, sử dụng địa chỉ 6to4 và cấu hình router gateway kết nối IPv4 thành 6to4 router để kết nối mạng thử nghiệm tới các mạng 6to4 khác và tới Internet IPv6.

II. Đăng ký sử dụng dịch vụ Tunnel Broker

Trong phần thực hành này, chúng ta sẽ thực hiện đăng ký sử dụng dịch vụ Tunnel Broker miễn phí cung cấp bởi Consulintel, một tổ chức tương đối tích cực trong thúc đẩy thế hệ địa chỉ IPv6, và sử dụng địa chỉ thuần IPv6 cung cấp bởi tổ chức này để kết nối vào mạng Internet IPv6.

Đăng ký sử dụng dịch vụ cung cấp tại website www.IPv6tf.org

Tunnel giữa người sử dụng và mạng của consulintel là công nghệ tunnel bằng tay. Để cấu tạo được đường tunnel, tại mỗi đầu đường hầm, cần phải có thông tin về địa chỉ IPv4 và địa chỉ IPv6 của các đầu tunnel. Người sử dụng cần cung cấp địa chỉ IPv4 phía mình khi đăng ký sử dụng Tunnel Broker. Địa chỉ IPv6 cùng thông tin khác (ví dụ tên miền trong hệ thống tên miền quốc tế) sẽ nhận được từ Tunnel Broker.

5. *Truy cập vào trang web www.IPv6tf.org, đăng ký một account sử dụng dịch vụ Tunnel broker.*

Khi được chấp nhận và kích hoạt, bạn truy cập bằng account đó và đăng ký tạo đường hầm tunnel. Giao diện web sẽ yêu cầu bạn cung cấp thông tin về địa chỉ IPv4 đầu đường kết nối phía bạn, hệ điều hành của thiết bị tại đầu đường kết nối phía bạn (ví dụ Window, linux, hay Cisco), và thông tin khác: bạn yêu cầu kết nối và vùng địa chỉ cho một host duy nhất, hay bạn yêu cầu kết nối và vùng địa chỉ cho một mạng IPv6, người đăng ký sử dụng dịch vụ Tunnel Broker cần chú ý đăng ký đúng vùng địa chỉ theo nhu cầu sử dụng.

- Từ thông tin về HĐH của thiết bị đầu đường tunnel phía người sử dụng, tổ chức duy trì Tunnel Broker sẽ cung cấp hướng dẫn tương ứng cho người sử dụng thiết lập đường hầm vì mỗi hệ điều hành sẽ có tập lệnh hoặc cách thức tạo giao diện và đường tunnel khác.
- Tunnel Broker của Consulitel cung cấp /127 nếu người sử dụng chỉ kết nối một máy tính IPv6, /64 nếu người sử dụng kết nối một mạng IPv6 chỉ có duy nhất một subnet, /48 nếu người sử dụng kết nối một mạng nhiều subnet..

Tiến hành đăng ký dịch vụ và ghi lại những thông tin sau:

Phía người sử dụng:

Vùng địa chỉ IPv6 Consulintel cấp cho tổ chức:

Tên miền quốc tế Consulintel chuyển giao cho tổ chức:

Thông tin về đầu kết nối tunnel phía người sử dụng (Tunnel client):

Địa chỉ IPv4:

Địa chỉ IPv6:

Thông tin về đầu kết nối tunnel phía tổ chức cung cấp Tunnel Broker (Tunnel server)

Địa chỉ IPv4:

Địa chỉ IPv6:

6. *Thiết lập đường hầm theo những thông tin được cung cấp:*

Tùy theo đăng ký thiết lập tunnel cho một host (điểm kết thúc tunnel phía người sử dụng là một host), hay một mạng (điểm kết thúc đường tunnel phía người sử dụng là một router) và HĐH chạy trên thiết bị gắn với đầu tunnel phía người sử dụng, Consulintel sẽ gửi thông tin hướng dẫn thiết lập dịch vụ tunnel tương ứng.

Trong phần thực hành này, chúng ta thực hiện tunnel để có kết nối một host tới mạng Internet IPv6.

❖ Trên máy tính sử dụng HĐH Window 2003

Tạo một giao diện dành cho tunnel, đặt tên là Consulintel

Netsh > interface IPv6

add v6v4tunnel Consulintel *địa_chỉ_IPv4_tunnel_client địa_chỉ_IPv4_tunnel_server*

Gắn địa chỉ IPv6 mà Consulintel đã cung cấp cho giao diện này

add address Consulintel *địa_chỉ_IPv6_tunnel_client*

Tạo tuyến (route) để các lưu lượng IPv6 đi qua giao diện tunnel này.

add route 0::/0 Consulintel publish=yes

Các gói tin IPv6 sẽ được đóng gói trong gói tin IPv4 có protocol 41 và gửi qua cơ sở hạ tầng mạng IPv4. Giả sử host chỉ sử dụng một giao diện tunnel này cho các lưu lượng IPv6, lệnh trên đã tạo một tuyến mặc định (default route) để mọI lưu lượng IPv6 đi qua giao diện này.

❖ Trên máy tính sử dụng HĐH Linux

Nếu đầu kết thúc tunnel phía này là máy tính cài HĐH Linux, đường tunnel tớI Consulintel được tạo như sau:

Tạo một giao diện dành cho tunnel, đặt tên là TunnelBroker

ip tunnel add TunnelBroker mode sit ttl 255 remote *địa_chỉ_IPv4_tunnel_server* **local** *địa_chỉ_IPv4_tunnel_client*

Kích hoạt giao diện này lên

ip link set dev TunnelBroker up

Gắn địa chỉ IPv6 mà Consulintel đã cung cấp cho giao diện này

ip -6 addr add *địa_chỉ_IPv6_tunnel_client* **dev TunnelBroker**

Tạo một tuyến để mọi lưu lượng IPv6 đi qua giao diện này.

ip -6 route add 2000::/3 via *địa_chỉ_IPv6_tunnel_server* **dev tunnelbroker**

Chú ý: Tuyến vớI prefix 2000::/3 sẽ bao gồm mọI lưu lượng của địa chỉ unicast toàn cầu (có ba bít đầu 001)

7. *Kiểm tra kết nối IPv6 bằng TunnelBroker*

Kiểm tra kết nốI tớI một site thuộc internet IPv6

Trên máy window:

ping -6 –t www.kame.net

ping -6 –t www.IPv6tf.org

tracert -6 www.kame.net

Trên máy Linux:

ping6 www.kame.net

ping6 www.IPv6tf.org

traceroute6 www.kame.net

8. *Dùng trình duyệt (IE của window, Mozilla của linux) kết nối tới một số trang web có hỗ trợ IPv6 và chỉ định thông tin địa chỉ của client.*

www.kame.net
www.apnic.net
www.IPv6tf.org

Trên các website này sẽ thông báo bạn đang kết nối bằng địa chỉ IPv6. Bạn sẽ quan sát thấy địa chỉ IPv6 bạn đang sử dụng là địa chỉ thuần IPv6 (thường bắt đầu bởI prefix 2001) mà bạn đã được cung cấp từ tổ chức duy trì Tunnel Broker.

Trong phần thực hành phía trên, bạn đã kết nối một máy tính vào mạng Internet IPv6. Nếu bạn muốn thử nghiệm một mạng và kết nối mạng vào Internet IPv6, thiết bị tại đầu đường hầm phía người sử dụng phải là một router và bạn đăng ký từ tổ chức cung cấp dịch vụ Tunnel Broker một vùng địa chỉ IPv6 sử dụng trong mạng IPv6 của mình.

Hỏi – đáp cuối chương 5:

1. Bạn cho biết mục đích của công nghệ tunnel?

T: Công nghệ tunnel tiến hành "bọc" gói tin IPv6 trong gói tin IPv4 để có thể truyền gói tin IPv6 đi trên cơ sở hạ tầng mạng IPv4 với mục đích sử dụng cơ sở hạ tầng mạng Internet IPv4 để cung cấp kết nối IPv6.

2. Tại sao nói công nghệ Tunnel Broker là dựa trên tunnel cấu hình bằng tay và công nghệ Tunnel 6to4 là tunnel cấu hình tự động ?

T Trong công nghệ Tunnel Broker (TB), tổ chức cung cấp dịch vụ TB sẽ cung cấp thông tin cho người sử dụng để người sử dụng cấu hình bằng tay giao diện tunnel, địa chỉ của điểm đầu và cuối đường hầm. Đó là hình thức đường hầm cấu hình bằng tay.

Địa chỉ IPv6 sử dụng trong công nghệ Tunnel 6to4 được tạo nên từ địa chỉ toàn cầu IPv4 theo quy tắc gắn 32 bít địa chỉ IPv4 (viết dưới dạng hexa) với 16 bít prefix 2002::/16 để tạo nên /48 địa chỉ IPv6. Từ địa chỉ IPv6 6to4 hoàn toàn có thể suy ra địa chỉ IPv4 đã tạo nên vùng địa chỉ. Do vậy, điểm bắt đầu và kết thúc đường tunnel được tự động suy ra từ gói tin IPv6. Đó là cách thức tunnel tự động.

3. Nếu hiện tại bạn chưa sở hữu vùng địa chỉ IPv6 nào, và chỉ có kết nối tới Internet IPv4, bạn có thể xây dựng mạng thử nghiệm có kết nối IPv6 hay không?

T Bạn có thể xây dựng và thiết lập kết nối thử nghiệm dựa trên những dịch vụ tunnel các tổ chức đang cung cấp miễn phí hiện nay. Bạn đọc có thể sử dụng địa chỉ IPv6 6to4 tạo nên từ địa chỉ IPv4 cho mạng IPv6 của mình. Nếu bạn muốn sử dụng địa chỉ thuần IPv6, bạn có thể đăng ký dịch vụ Tunnel Broker miễn phí của một tổ chức và sử dụng vùng địa chỉ IPv6 tổ chức đó cấp cho mạng thử nghiệm của mình.

TÀI LIỆU THAM KHẢO

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

RFC 3513 IP Version 6 Addressing Architecture

RFC 3587 IPv6 Global Unicast Address Format

RFC 2375 IPv6 Multicast Address Assignments

RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses

RFC 3879 Deprecating Site Local Addresses

RFC 3177 IAB/IESG Recommendations on IPv6 Address Allocations to Sites

RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses

RFC 2462 IPv6 Stateless Address Autoconfiguration

RFC 3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6

RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

RFC 1981 Path MTU Discovery for IP version 6

RFC 1981 Neighbor Discovery for IP Version 6 (IPv6)

RFC 2710 Multicast Listener Discovery (MLD) for IPv6

RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

RFC 3697 IPv6 Flow Label Specification

RFC 3596 DNS Extensions to Support IP Version 6

RFC 3363 Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)

How IPv6 works – Tài liệu của Microsoft.

Introduction to IP Version 6 – Tài liệu của Microsoft

IPv6 Transition Technologies – Tài liệu của Microsoft.

The ABCs of IP version 6 – Tài liệu của Cisco

IPv6 for Cisco IOS – Tài liệu của Cisco

Cisco routing TCPIP – Tác giả Jeff Doyle. Nhà xuất bản Cisco Press

IPv6 Network Administration – Tác giả David Malone, Niall Murphy. Nhà xuất bản O'Reilly

Nội dung được biên soạn trong sách "Giới thiệu về thế hệ địa chỉ Internet mới IPv6" còn được tham khảo và tổng hợp từ những tài liệu tại những địa chỉ Website sau đây:

http://www.microsoft.com

http://www.cisco.com

http://www.IPv6tf.org

http://ns.IPv6style.jp

http://www.tcpipguide.com

http://www.apnic.net

http://www.ripe.net

MỘT SỐ KHÁI NIỆM VÀ TỪ VIẾT TẮT

Anycast

Cách thức gửi gói tin đến một đích bất kỳ trong một nhóm các máy.

APNIC

Asia Pacific Network Information Centre. Tổ chức quản lý địa chỉ IP, số hiệu mạng cấp vùng, phụ trách khu vực Châu Á – Thái Bình Dương.

ARIN

American Registry for Internet Number - Tổ chức quản lý địa chỉ IP, số hiệu mạng cấp vùng, phụ trách khu vực Bắc Mỹ.

ARP

Address Resolution Protocol - Thủ tục phân giải địa chỉ, sử dụng trong IPv4 để phân giải địa chỉ IPv4 thành địa chỉ lớp hai tương ứng, ví dụ địa chỉ Ethernet MAC.

Broadcast

Một gói tin có địa chỉ đích broadcast sẽ được truyền tải tới và được xử lý bởi mọi máy trong một mạng.

DAD

Duplicate Address Detection, một quá trình cho phép IPv6 node đảm bảo được rằng một địa chỉ chưa được sử dụng trên đường kết nối trước khi IPv6 node quyết định sử dụng địa chỉ.

DHCP

Dynamic Host Configuration Protocol - Thủ tục cấu hình địa chỉ động, cấp địa chỉ tạm thời cho IPv4 host. Được sử dụng cho phép một IPv4 host tìm địa chỉ IP và những thông tin khác như máy chủ tên miền nội bộ, mà không cần tới cấu hình thủ công và lưu trữ những thông tin này trên máy.

DHCPv6

Dynamic Host Configuration Protocol version 6 - Thủ tục cấu hình địa chỉ động phiên bản 6.

Dual stack

Một dual-stack node là một node làm việc với cả IPv4 và IPv6.

Header

Phần mào đầu, chứa các thông tin phục vụ cho việc xử lý thông tin tại các lớp trong mô hình hoạt động của thủ tục TCP/IP.

Hop limit

Một trường của IPv6 header, xác định số đường kết nối tối đa mà gói tin có thể đi qua trước khi bị huỷ bỏ.

IANA

Internet Assigned Numbers Authority - Tổ chức quản lý tài nguyên số (địa chỉ IP, số protocol, số port...) quốc tế

ICANN

Internet Corporation for Assigned Names and Numbers. Tổ chức phi lợi nhuận, đảm nhiệm vai trò quản lý về tài nguyên số (địa chỉ IP, các thông số thủ tục) và tên (hệ thống tên miền), đồng thời quản lý hệ thống máy chủ tên miền root toàn cầu.

ICMP

Internet Control Message Protocol - Thủ tục của những thông điệp điều khiển, sử dụng trao đổi những thông điệp báo lỗi giao tiếp, thông điệp chẩn đoán mạng trong hoạt động của IP.

ICMPv4

Internet Control Message Protoco version 4 - Thủ tục ICMP phiên bản 4. Khái niệm này đồng nhất với khái niệm ICMP.

ICMPv6

Internet Control Message Protoco version 6 - Thủ tục ICMP phiên bản 6, là phiên bản đã được sửa đổi, nâng cấp của ICMP, phục vụ cho hoạt động của IPv6.

IETF

Internet Engineering Taskforce - Tổ chức tiêu chuẩn hoá, viết các tài liệu tiêu chuẩn hoá (RFC) phục vụ hoạt động Internet toàn cầu.

IGMP

Internet Group Management Protocol - Thủ tục sử dụng trong công nghệ multicast IPv4 để thiết lập quan hệ thành viên nhóm multicast trong một mạng. Thủ tục này cho phép một host thông báo với router trên mạng của nó rằng nó muốn nhận lưu lượng của một địa chỉ multicast nhất định.

IPSec

Một công nghệ cung cấp bảo mật, xác thực và những dịch vụ an ninh khác tại tầng IP.

IPv4

Internet Protocol version 4 – Phiên bản 4 của thủ tục Internet. Hiện đang được sử dụng phổ biến trong hoạt động mạng Internet toàn cầu.

IPv6

Internet Protocol version 6 – Phiên bản 6 của thủ tục Internet, được phát triển nhằm thay thế IPv4, khắc phục những hạn chế của phiên bản IPv4 và cải thiện thêm nhiều đặc tính mới.

LACNIC

Latin American and Caribbean Internet Addresses Registry - Tổ chức quản lý địa chỉ IP, số hiệu mạng cấp vùng, phụ trách khu vực Mỹ Latinh và biển Caribe.

MLD

Multicast Listener Discovery – Là một thủ tục, sử dụng các thông điệp ICMPv6, cho phép các router khám phá ra những địa chỉ IPv6 multicast nào đang được « nghe » lưu lượng trên một đường kết nối.

MTU

Maximum Transmission Unit – Kích thước gói tin lớn nhất có thể truyền tải trên một đường kết nối.

Multicast

Công nghệ cho phép gửi một gói tin IP đồng thời tới một nhóm xác định các thiết bị mạng. Các thiết bị mạng này có thể thuộc nhiều tổ chức và định vị ở các vị trí địa lý khác nhau.

NAT

Network Address Translation - Một công nghệ thay thế địa chỉ trong gói tin IP khi gói tin đi ra, hoặc vào một mạng, cho phép nhiều thiết bị mạng đánh địa chỉ riêng (private) có thể chia sẻ cùng một địa chỉ toàn cầu (public) và kết nối vào Internet.

ND

Neighbor Discovery - Một thủ tục mới, được phát triển trong hoạt động IPv6. ND sử dụng các thông điệp ICMPv6 để đảm nhiệm các quy trình giao tiếp cần thiết giữa các node trên một đường kết nối như quy trình phân giải địa chỉ (thực hiện bằng thủ tục ARP trong IPv4), quy trình tìm kiếm router …

Path MTU Discovery

Quy trình tìm kiếm giá trị MTU nhỏ nhất trên một đường kết nối từ nguồn tới đích

Prefix

Là một khối địa chỉ IPv4 hoặc IPv6, được quyết định bằng việc cố định một số bít đầu tiên của địa chỉ. Ví dụ 203.119.9.0/24 là tập hợp các địa chỉ IPv4 từ 203.119.9.0 đến 203.119.9.255. Đối với IPv6, 2000::/3 là tập hợp các địa chỉ IPv6 có ba bít đầu tiên là 001 (chữ cái hexa đầu tiên trong địa chỉ là 2 hoặc 3).

QoS

Quality of Service: Khái niệm trong truyền tải lưu lượng, đảm bảo lưu lượng mạng đi đến đích theo một chất lượng nhất định (mức độ lỗi, thời gian truyền tải lưu lượng...)

RFC

Request For Comments - Những tài liệu tiêu chuẩn cho Internet, được soạn thảo và xuất bản bởi IETF.

RIPE NCC

Réseaux IP Européens Tổ chức quản lý địa chỉ IP, số hiệu mạng cấp vùng, phụ trách khu vực Châu Âu.

RIR

Regional Internet Registry - Tổ chức quản lý và phân bổ địa chỉ IP cấp vùng cho các hoạt động Internet. Những tổ chức này cũng có những vai trò trong việc hỗ trợ quản lý cơ sở hạ tầng Internet và phát triển chính sách quản lý tài nguyên địa chỉ IP, số hiệu mạng ASN.

TCP/IP

Transmission Control Protocol/Internet Protocol - Một bộ các giao thức giao tiếp, phục vụ cho việc kết nối các host trên Internet.

Tunnel

Đường hầm – Là một cách thức truyền gói tin IPv6 từ một điểm tới một điểm khác trên mạng, sử dụng cơ sở hạ tầng mạng IPv4 bằng cách bọc gói tin IPv6 trong gói tin IPv4, do vậy chúng có thể đi được trong cơ sở hạ tầng mạng IPv4.

Unicast

Cách thức gửi gói tin thông thường. Trong đó gói tin chỉ được gửi đến một đích duy nhất. Những cách thức gửi gói tin khác bao gồm anycast, broadcast và multicast

VPN

Virtual Private Network. Được nhắc tới như một mạng trong đó có các phần mạng cách nhau bởi vị trí địa lý được kết nối thông qua Internet công cộng song dữ liệu truyền qua Internet được mã hoá, do vậy toàn bộ mạng được xem như một mạng riêng “ảo”