HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Đức Khương

CHUYỂN ĐỔI IPv4-IPv6 TRONG MẠNG BĂNG RỘNG VNPT VÀ KHÍA CẠNH BẢO MẬT CÓ LIÊN QUAN

LUẬN VĂN THẠC SĨ KỸ THUẬT

(*Theo định hướng ứng dụng*)

HÀ NỘI - NĂM 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Đức Khương

CHUYỂN ĐỔI IPv4-IPv6 TRONG MẠNG BĂNG RỘNG VNPT VÀ KHÍA CẠNH BẢO MẬT CÓ LIÊN QUAN

Chuyên ngành: Kỹ thuật Viễn thông

Mã số: 8.52.02.08

LUẬN VĂN THẠC SĨ KỸ THUẬT

(***Theo định hướng ứng dụng***)

NGƯỜI HƯỚNG DẪN KHOA HỌC : GS.TS. NGUYỄN BÌNH

HÀ NỘI - NĂM 2020

LỜI CAM ĐOAN

Em xin cam đoan đề tài: *"Chuyển đổi Ipv4-Ipv6 trong mạng băng rộng VNPT và khía cạnh bảo mật có liên quan"* là một công trình nghiên cứu độc lập dưới sự hướng dẫn của GS - TS Nguyễn Bình. Ngoài ra không có bất cứ sự sao chép của người khác. Đề tài, nội dung luận văn là sản phẩm mà em đã nỗ lực nghiên cứu trong quá trình học tập tại trường và tìm hiểu qua các tài hiệu, trang web vv… Các số liệu, kết quả trình bày trong báo cáo là hoàn toàn trung thực, em xin chịu hoàn toàn trách nhiệm về luận văn của riêng em.

Người cam đoan

Nguyễn Đức Khương

LỜI CẢM ƠN

Đầu tiên xin trân trọng gửi lời cảm ơn sâu sắc đến quý thầy cô Học viện Công nghệ Bưu chính Viễn thông trong thời gian qua đã dìu dắt và tận tình truyền đạt cho em những kiến thức, kinh nghiệm vô cùng quý báu để em có được kết quả ngày hôm nay.

Xin trân trọng cảm ơn GS.TS. Nguyễn Bình, người hướng dẫn khoa học của luận văn, đã hướng dẫn tận tình và giúp đỡ về mọi mặt để hoàn thành luận văn.

Xin trân trọng cảm ơn quý thầy cô Khoa Đào tạo sau đại học đã hướng dẫn và giúp đỡ em trong quá trình thực hiện luận văn.

Cuối cùng là sự biết ơn tới gia đình, bạn bè và người thân đã luôn động viên, giúp đỡ tác giả trong suốt quá trình học tập và thực hiện luận văn.

Hà Nội, tháng năm 2020

Học viên thực hiện

Nguyễn Đức Khương

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Nghĩa tiếng Anh	Nghĩa tiếng Việt
APIPA	Automatic Private IP Addressing	Địa chỉ IP riêng tự động
BIS	Bump into the Stack	Bump vào ngăn xếp
DSTM	Dual Stack Translation Mode	Chế độ dịch hai ngăn xếp
DNS	Domain Name Service	Dịch vụ tên miền
IPSec	Internet Protocol Security	Bảo mật giao thức Internet
IPv4	*nternet Protocol version 4*	Giao thức internet phiên bản 4
IPv6	*nternet Protocol version 6*	Giao thức internet phiên bản 6
IANA	Internet Assigned Numbers Authority	Tổ chức cấp phát số hiệu Internet
ISATAP	Intra-site Automatic Tunnel Addressing Protocol	Giao thức địa chỉ đường hầm tự động nội bộ
IPX	Internetwork Packet Exchange	Trao đổi gói mạng
ICMPv6	Internet Control Message Protocol version 6	Giao thức tin nhắn điều khiển Internet phiên bản 6
LAN	Local Area Network	Mạng lưới khu vực địa phương
NLA	Next Level Aggregation	Tập hợp cấp độ tiếp theo
NAT-PT	Network Address Translation – Protocol Translation	Dịch địa chỉ mạng - Dịch giao thức
NAT	Network Address Translation	Dịch địa chỉ mạng
NSAP	National Social Assistance Programme	Chương trình trợ giúp xã hội quốc gia
OSI	Open Systems Interconnection Reference Model	Mô hình tham chiếu kết nối hệ thống mở
QoS	Quality of Service	Chất lượng dịch vụ
TOS	Type-of-service	Loại dịch vụ
TLA	Top Level Aggregation	Tập hợp cấp cao nhất
VPN	Virtual Private Network	Mạng riêng ảo

MỞ ĐẦU

Như chúng ta đã biết internet là một mạng máy tính toàn cầu do hàng nghìn mạng máy tính từ khắp mọi nơi nối lại tạo lên và lượng thuê bao internet tăng đột biến, đứng trước sự phát triển mạnh mẽ về số lượng thiết bị mạng như vậy thì nguy cơ thiếu hụt không gian địa chỉ IPv4 là điều sẽ không tránh khỏi; cùng với những hạn chế trong công nghệ và những nhược điểm của IPv4 đã thúc đẩy sự ra đời của một thế hệ địa chỉ Internet mới là IPv6 với cấu trúc định tuyến tốt hơn, hỗ trợ tốt hơn cho multicast, hỗ trợ bảo mật và di động tốt hơn. Quan điểm chính khi thiết kế IPv6 là từng bước thay thế IPv4, không tạo ra sự biến động lớn đối với hoạt động của mạng Internet nói chung và của từng dịch vụ trên Internet nói riêng, đảm bảo tính tương thích tuyết đối với mạng Internet dùng IPv4 hiện tại. Những chức năng đã được kiểm nghiệm thành công trong IPv4 sẽ vẫn duy trì trong IPv6. Những chức năng không được sử dụng trong IPv4 sẽ bị loại bỏ và đồng thời triển khai một số chức năng mới liên quan đến địa chỉ, bảo mật, và triển khai các dịch vụ mới.

Với lượng khách hàng băng rộng tại Hải Dương tương đối lớn (khoảng 140.000 thuê bao) để tất cả các thiết bị đầu cuối khách hàng này tương thích với IPv6 là rất khó vì một số thiết bị đầu cuối khách hàng không hỗ trợ IPv6 vậy để tồn tại và hỗ trợ hai giao thức IPv4 và IPv6 trên cùng đường truyền thì chúng ta cần một giải phát để giải quyết vấn đề này; tuy nhiên việc chuyển đổi IPv4-IPv6 cũng cần một cơ chế bảo mật; do vậy đề tài em nghin cứu là *"Chuyển đổi IPv4-IPv6 trong mạng băng rộng VNPT và khía cạnh bảo mật liên quan"* ; trong đề tài này em nghi cứu sâu về phương pháp chuyển đổi IPv4-IPv6 bằng phương pháp Dual Stack; dual stack còn gọi là cơ chế chồng giao thức, là cơ chế cơ bản nhất cho phép nút mạng đồng thời hỗ trợ cả hai giao thức IPv4 và IPv6, có được khả năng trên do một trạm Dual Stack cài đặt cả hai giao thức IPv6 và IPv4; lý do em chọn phương pháp Dual Stack là phương pháp này dễ triển khai.

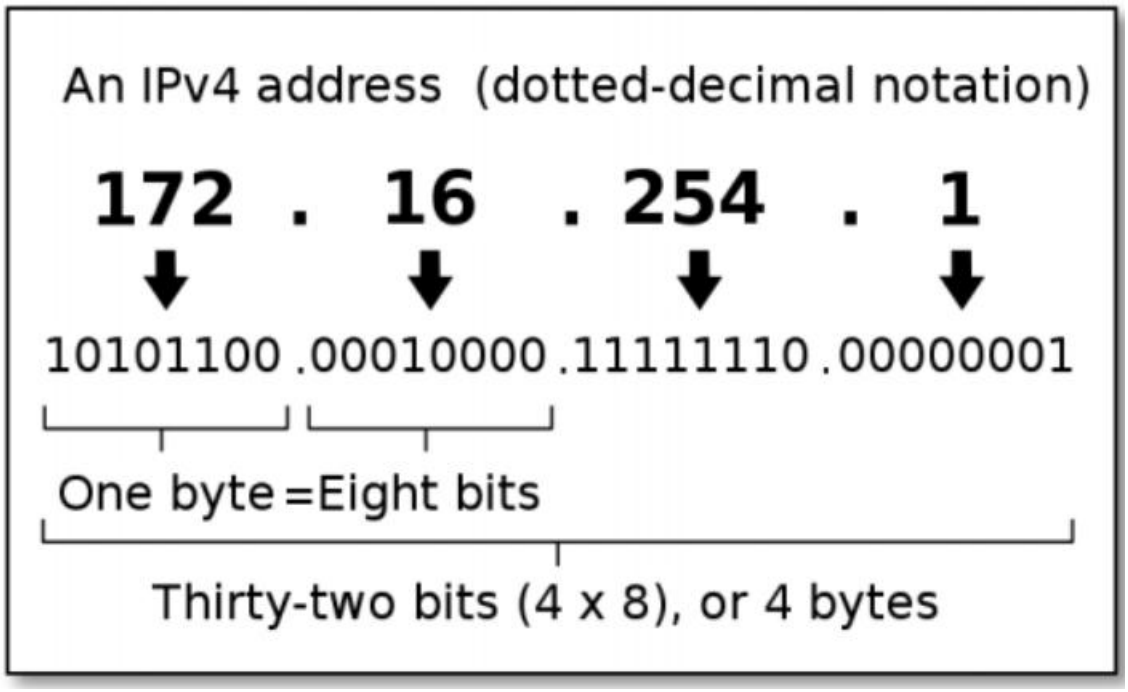
CHƯƠNG 1: TỔNG QUAN VỀ IPV4 VÀ IPV6

1.1. Tổng quan về IPv4

1.1.1. IPv4

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

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



Hình 1. 1: IPv4 được viết dưới dạng nhị phân

1.1.2. Cấu trúc địa chỉ IPv4

Địa chỉ IP được chia thành 2 phần là **network** (phần mạng) và phần **Host**

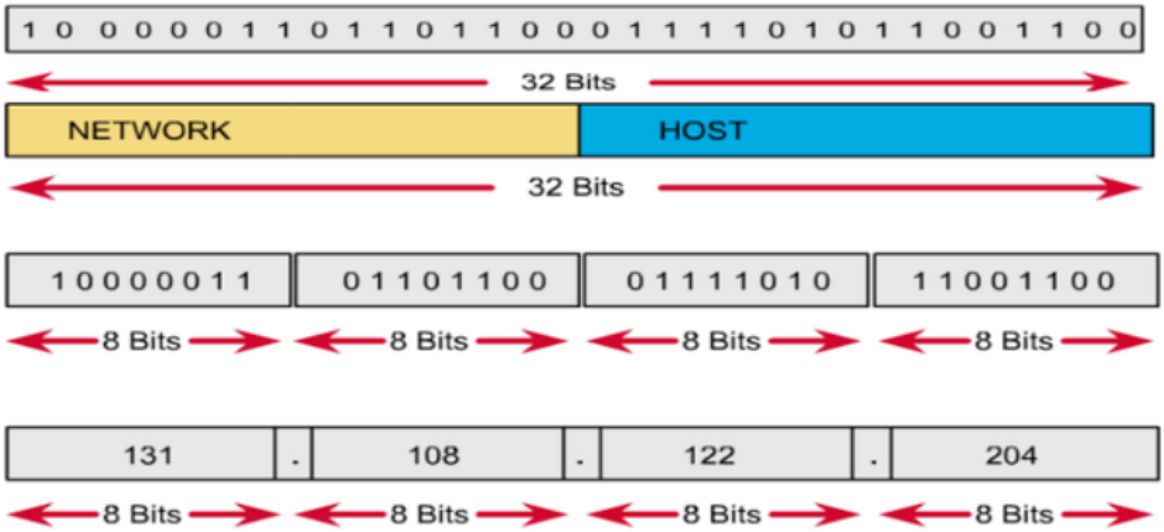
Địa chỉ IP có 32 bit nhị phân và được chia thành các octet (4 cụm, 8 bit)

Các quy tắc được áp dụng khi đặt địa chỉ IP:

- Các bit phần mạng không được phép đặt đồng thời bằng 0 (**Ví dụ**: Không hợp lệ nếu đặt địa chỉ 0.0.0.1 với phần mạng 0.0.0 và phần Host là 1).

- Sẽ có một địa chỉ mạng nếu các bit phần Host đồng thời có giá trị bằng 0 (**Ví dụ** : Địa chỉ 192.168.1.1 có thể gán cho Host nhưng thay giá trị 0 vào 192.168.1.0 sẽ thành địa chỉ mạng và không thể gán cho Host).

- Sẽ có địa chỉ Broadcast cho mạng nếu các bit phần Host đồng thời bằng 1 (**Ví dụ**: Mạng 192.168.1.0 có địa chỉ 192.168.1.255 là địa chỉ Broadcast).



Hình 1. 2: Cấu trúc địa chỉ IPv4

1.1.3. Các lớp của địa chỉ IPv4

+ Lớp A:

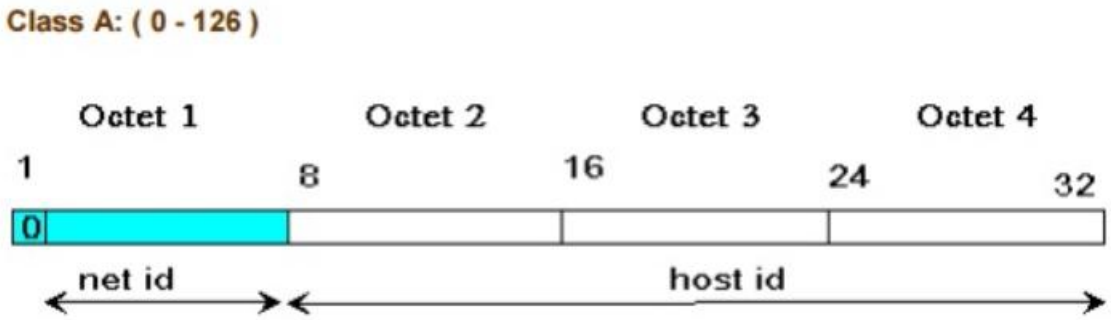
- Lớp A của địa chỉ IPv4 sử dụng octet đầu làm phần mạng và 3 octet sau làm Host

- 0 luôn được chọn là bit đầu của địa chỉ lớp A

- Các địa chỉ mạng lớp A gồm 1.0.0.0 => 126.0.0.0

- Mạng Lookback là 127.0.0.0

- Phần Host gồm 24 bit, mỗi mạng lớp A có 224 – 2 Host



Hình 1. 3: Lớp A của địa chỉ IPv4

+ Lớp B

- Hai octet đầu của địa chỉ lớp B được dùng làm phần mạng, 2 octet sau được dùng làm Host

- 1 và 0 luôn được giữ cho hai bit đầu của địa chỉ lớp B

- Địa chỉ mạng lớp B gồm 128.0.0.0 đến 191.255.0.0 (tổng cộng có 214 mạng trong lớp B)

- Một mạng lớp B có 216 – 2 Host vì phần Host của lớp này dài 16 bit

Hình 1. 4: Lớp B của địa chỉ IPv4

+ Lớp C:

- Địa chỉ lớp C dùng 3 octet đầu làm phần mạng và octet sau làm phần Host

- 1 , 1 và 0 được giữ cho ba bit đầu của địa chỉ lớp C

- Mạng lớp C bao gồm các địa chỉ 192.0.0 đến 223.255.255.0 (tổng cộng 221 mạng trong lớp C)

- Một mạng lớp C có 28 – 2 Host do phần Host của lớp này dài 8 bit

Hình 1. 5 Lớp C của đại chỉ IPv4

+ Lớp D:

- Lớp D bao gồm các địa chỉ từ 224.0.0.0 đến 239.255.255

- Lớp D được dùng làm địa chỉ Multicast. VD: 224.0.0.5 dùng cho OSPF hay 224.0.0.9 dùng cho RIPv2

+ Lớp E:

- Gồm các địa chỉ từ dải 240.0.0.0 trở đi

- Địa chỉ lớp E được dùng với mục đích dự phòng

1.1.4. Một số lưu ý về các lớp của IPv4

- Các lớp địa chỉ IP gồm A, B, C được dùng để đặt cho các Host

– Khi muốn xác định địa chỉ IP thuộc lớp nào, nên quan sát octet ở vị trí đầu tiên của địa chỉ đó. Octet nằm trong khoảng giá trị từ:

1 đến 126: địa chỉ lớp A

128 đến 191: địa chỉ lớp B

192 đến 223: địa chỉ lớp C

224 đến 239: địa chỉ lớp D

240 đến 255: địa chỉ lớp E

1.1.5. Hạn chế của IPv4

Hình 1. 6 Hạn chế của IPv4

- Không có bất cứ cách thức bảo mật nào đi kèm trong cấu trúc thiết kế của địa chỉ IPv4: Phương tiện hỗ trợ mã hóa dữ liệu cũng không được tích hợp trong IPv4. Do đó, lưu lượng truyền tải giữa các Host không được bảo mật mà chỉ bảo mật phổ biến ở mức ứng dụng. Áp dụng IPSec – một phương thức bảo mật phổ biến tại tầng IP thì việc bảo mật lưu lượng đầu cuối bị hạn chế.

- Một hạn chế nữa của IPv4 đó là việc thiếu hụt không gian địa chỉ: Do phiên bản này chỉ sử dụng 32 bit để đánh địa chỉ nên không gian của nó chỉ có 232 địa chỉ. Như vậy, cùng với sự bùng nổ của internet thì tài nguyên địa chỉ IPv4 đang dần cạn kiệt. Phiên bản này gần như đáp ứng không đủ so với nhu cầu sử dụng.

Để khắc phục những hạn chế của **IPv4** đồng thời mang lại những đặc tính mới cho hoạt động mạng thế hệ tiếp, người ta đã đầu tư nghiên cứu và cho ra đời một giao thức internet mới. Giao thức IP thế hệ mới (**thế hệ 6: IPv6**) ra đời để khắc phục những nhược điểm của phiên bản tiền nhiệm. IPv6 bao gồm 128 bit, có chiều dài gấp 4 lần so với địa chỉ IPv4.

1.2. Các tính năng của IPv6

1.2.1. Dạng mào đầu gói tin mới

Phần header của IPv6 được giảm xuống mức tối thiểu bằng việc chuyển tất cả các trường phụ hoặc không cần thiết xuống phần header mở rộng nằm sau phần IPv6 header. Việc tổ chức phần header hợp lý này làm tăng hiệu quả xử lý tại các router trung gian. IPv6 header và IPv4 header là không tương thích với nhau, do đó các node phải được cài đặt cả 2 phiên bản IP mới có thể xử lý các header khác nhau này.

1.2.2. Không gian địa chỉ lớn hơn:

IPv6 sử dụng 128 bit để đánh dấu địa chỉ nên số lượng địa chỉ có được là rất lớn khoảng 3,4.1038. Với không gian địa chỉ lớn như vậy cho phép phân chia địa chỉ thành nhiều mức khác nhau từ mạng trục, mạng trung gian đến địa chỉ cho mạng riêng của từng tổ chức. Hiện tại mới chỉ có một số ít các địa chỉ dùng cho các host nên số lượng địa chỉ dự phòng cho tương lai là rất nhiều do đó sẽ không cần phải sử dụng kỹ thuật NAT nữa.

1.2.3. Tự động cấu hình địa chỉ:

Tương tự như IPv4 với IPv6 cũng cung cấp khả năng cấu hình địa chỉ tự động sử dụng DHCP. Đồng thời nó còn đưa ra khả năng tự động cấu hình địa chỉ khi không có DHCP server. Trong một mạng các host có thể tự động cấu hình địa chỉ của nó bằng cách sử dụng IPv6 prefix nhận được từ router (gọi là địa chỉ link – local). Hơn nữa nếu trong một mạng mà không có router thì host cũng có thể tự động cấu hình địa chỉ link – local cho nó để thông tin với các host khác. Với sự phát triển nhanh chóng của mạng Internet cũng bị hạn chế bởi sự phức tạp trong việc sử dụng nên giao thức IPv6 được xây dựng với tiêu chí đơn giản dễ sử dụng ngay cả với người không hiểu biết về công nghệ. Điều này đưa đến một đặc điểm của IPv6 chỉ yêu cầu một phần nhỏ cho việc cấu hình và bảo dưỡng mạng.

1.2.4. An ninh thông tin:

Các cơ chế bảo mật được tăng cường, có phần tiều đề dành cho bảo mật tương ứng với hai kỹ thuật bảo mật trong Ipsec là: AH và ESP. Giao thức IPv6 hỗ trợ toàn bộ các tính năng của IPsec và cho phép sử dụng các thuật toán mã hóa, chứng thực và tính toàn vẹn dữ liệu Đây là một tiêu chuẩn cho an ninh mạng đồng thời mở rộng khả năng làm việc được với nhau của các loại sản phẩm.

1.2.5. Hỗ trợ qos tốt hơn:

Phần header của IPv6 được đưa thêm một số trường mới. Trường Flow Label trong IPv6 header được dùng để nhận dạng luồng dữ liệu. Từ đó router có thể có những chính sách khác nhau với các gói tin có luồng dữ liệu khác nhau. Do trường Flow

Label nằm trong IPv6 header nên QoS vẫn được đảm bảo khi phần tải trọng có mã hóa bởi IPSec.

1.2.6. Giao thức mới cho thông tin giữa các host liền kề:

Giao thức khám phá node liền kề (Neighbor Discovery) của IPv6 bao gồm hàng loạt các mesage điều khiển dạng ICMPv6 nhằm điều khiển sự tương tác giữa các node trong cùng một mạng kết nối. Giao thức này thay thế cho các bản tin phát quảng bá phân giải địa chỉ ARP, bản tin tìm kiếm router ICMP Router Discovery, ICMP redirect của IPv4 bằng các bản tin unicast và mutlticast Neighbor Discovery.

1.3. Cấu trúc, phân bổ và cách viết địa chỉ IPv6

1.3.1. Cấu trúc gói tin IPv6 trong mạng lan

Giao thức IPv6 được đưa ra nhằm thay thế giao thức IPv4 hiện nay do đó nó gần như chỉ liên quan tới các lớp trên trong mô hình OSI. Đối với các lớp dưới như lớp datalink và lớp vật lý thì không bị ảnh hưởng. Gói tin IPv6 được truyền trong mạng nội bộ LAN có cấu trúc như sau:

Phần header và trailer: phần được đóng gói của gói tin IPv6 khi ở lớp 2.

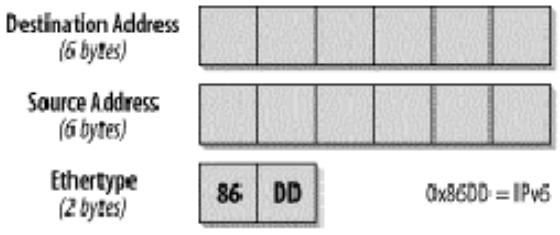
IPv6 header: phần mào đầu của gói tin IPv6

Payload (tải trong): mang thông tin của các lớp trên.

Link layer Header	IPv6 Header	Payload	Link Layer Trailer

Hình 1. 7 Cấu trúc khung của IPv6 tại lớp 2 trong mạng LAN

Đóng gói kiểu Ethernet II: dạng khung truyền dẫn của IPv6 có dạng như hình 2 với giá tị của trường EtherType là 0x86DD (của IPv4 là 0x800). Kích thước của gói tin IPv6 sử dụng kiểu đóng gói Ethernet II là từ 46 tới 1500 byte. Destination Address: địa chỉ MAC nguồn, Source Address: địa chỉ MAC đích.



Hình 1. 8: Cấu trúc khung truyền dẫn IPv6 trong mạng Ethernet II

1.3.2. Phân bổ địa chỉ IPv6

Tương tự như IPv4 không gian địa chỉ IPv6 cũng được phân chia dựa theo giá trị của các bít đầu hay còn gọi là phương thức định dạng theo tiền tố FP (Format Prefix). Hiện tại không gian địa chỉ IPv6 được định dạng theo tiền tố như bảng sau (theo rfc2373):

Phân bổ	Tiền tố	Tỉ trong trong không gian địa chỉ
Dự trữ	0000 0000	1/256
Chưa gán	0000 0001	1/256
Dự trữ phân bổ cho NSAP	0000 001	1/128
Dư trữ phân bổ cho IPX	0000 010	1/128
Chưa gán	0000 011	1/128
Chưa gán	0000 1	1/32
Chưa gán	0001	1/16
Các địa chỉ dành cho Global Unicast	001	1/8
Chưa gán	010	1/8
Chưa gán	011	1/8
Chưa gán	100	1/8
Chưa gán	101	1/8
Chưa gán	110	1/8
Chưa gán	1110	1/16
Chưa gán	1111 0	1/32
Chưa gán	1111 10	1/64
Chưa gán	1111 110	1/128
Chưa gán	1111 1110 0	1/512
Địa chỉ Link-local Unicast	1111 1111 10	1/1024
Địa chỉ Site-local Unicast	1111 1111 11	1/1024
Địa chỉ Multicast	1111 1111	1/256

Bảng 1. 1: Bảng phân bổ các loại địa chỉ IPv6

Theo sự phân bổ này, có một phần được dành cho địa chỉ NSAP, địa chỉ lPX và địa chỉ trong các mang riêng ảo (VPN). Phần còn lại của không gian địa chỉ chưa được gán sẽ được sử dụng trong tương lai. Nhưng phần này có thể được sử dụng để mở rộng những địa chỉ đang sử dụng (như thêm các nhà cung cấp địa chỉ) hay những người sử dụng mới (ví dụ những mạng cục bộ hay những người dùng đơn

lẻ). Chú ý rằng nhóm địa chỉ anycast không được chỉ ra ở trong bảng vì sự phân bố của chúng đã được bảo trùm bởi không giãn địa chỉ loại unicast.

Theo sự phân bổ này, có một phần được dành cho địa chỉ NSAP, địa chỉ lPX và địa chỉ trong các mạng riêng ảo (VPN). Phần còn lại của không gian địa chỉ chưa được gán sẽ được sử dụng trong tương lai. Nhưng phần này có thể được sử dụng để mở rộng những địa chỉ đang sử dụng (như thêm các nhà cung cấp địa chỉ) hay những người sử dụng mới (ví dụ những mạng cục bộ hay những người dùng đơn lẻ). Chú ý rằng nhóm địa chỉ anycast không được chỉ ra ở trong bảng vì sự phân bố của chúng đã được bảo trùm bởi không giãn địa chỉ loại unicast.

Theo dự đoán có khoảng 15 % không gian địa chỉ sẽ được sử dụng vào giai đoạn đầu, còn lại khoảng 85 % sẽ được dự trữ cho tương lai. Để quản lý không gian địa chỉ hiệu quả và hợp lý, các nhà thiết kế giao thức IPv6 đã đưa ra hai cơ chể cấp phát địa chỉ như sau.

1.4.2.1. Cơ chế cấp phát chung

Rút kinh nghiệm từ việc phân bố địa chỉ của IPv4, các nhà thiết kế IPv6 đã xây dựng một có thể phân bố địa chỉ hoàn toàn mở, nghĩa là nó không phụ thuộc vào giai đoạn ban đầu, hoàn toàn có thể thay đổi tùy thuộc vào những biến động trong tương lai về việc cấp phát và sử dụng địa chỉ cho các dịch vụ, các vùng khác nhau. Mặt khác, những người thiết kế IPv6 đã dự đoán trước những khả năng có thể phải sửa đổi một vài điểm như cấu trúc các loại địa chỉ, mở rộng một số loại địa chỉ ... trong tương lai. Điều này là hoàn toàn dùng đắn đối với một giao thức đang trong giai đoạn xây dựng và hoàn thiện.

Phân loại địa chỉ IPv6 không phải chi để cung cấp đầy đủ các dạng khuôn mẫu và đang tiền tố của các loại địa chỉ khác nhau. Việc phân loại địa chỉ theo các đang tiền tố một mặt cho phép các host nhận dạng ra các loại địa chỉ. Ứng với mỗi loại địa chỉ cho các ứng dụng khác nhau. Chẳng hạn địa chỉ có đang tiền tố FE80::/16 host sẽ nhận dạng đó là địa chỉ link-local chỉ để kết nốt các host trong cùng một mạng ...; hoặc với địa chỉ có đang tiền tố 3FEE::/16 sẽ hiểu đó là địa chỉ của mạng 6Bone cung cấp. Mặt khác, với định dạng các địa chỉ theo tiền tố cũng cho phép đơn giản trong các bảng định tuyến vì khi đó các đầu vào của các bảng

router sẽ là những tiền tố đơn giản, chiều dài của nó sẽ biến đổi từ 1 tới 128 bít. Chỉ có ngoại lệ duy nhất khi những địa chỉ đó liên quan tới những địa chỉ đặc biệt. Các host và router thực sự phải nhận ra các địa chỉ "muticast", những địa chỉ này không thể được xử lý giống như các địa chỉ "unicast " và "anycast". Chúng cũng phải nhận ra các địa chỉ đặc biệt, tiêu biểu như địa chỉ "link local". Trong cấu trúc cũng để dành tiền tố cho các địa chỉ tương thích với NSAP (địa chỉ điểm truy nhập dịch vụ mạng: Network service Access Point) và các địa chỉ tương thích IPX.

1.4.2.2 Cấp phát địa chỉ theo nhà cung cấp

Theo cấu trúc bằng phân bố địa chỉ ở trên, một trong số những loại địa chỉ IPv6 quan trọng nhất là đang địa chỉ Global Unicast. Dạng địa chỉ này cho phép định danh một giao diện trên mạng Internet (mang IPv6) có tính duy nhất trên toàn cầu. Ý nghĩa loại địa chỉ này giống như địa chỉ IPv4 định danh một host trong mạng Internet hiện nay. Không gian của dạng địa chỉ Global Unicast là rất lớn; để quản lý và phân bố hợp lý các nhà thiết kế IPv6 đã đưa ra mô hình phân bố địa chỉ theo cấp các nhà cung cấp dịch vụ Internet.

Đang địa chỉ này gồm 3 bít tiền tố 010 theo sau bởi 5 thành phần mà mỗi thành phần này được quản lý bởi các nhà cung cấp dịch vụ theo các cấp độ khác nhau. Tùy theo việc phân bố địa chỉ các thành phần này có một chiều dài biến đổi. Điều này một lần nữa cho thấy tính "động" trong việc cấp phát và quản lý địa chỉ IPv6.

3 bit	n bit	m bit	o bit	p bit	125-m-n-o-p bit
010	ID đăng ký	ID của nhà cung cấp	ID của thuê bao	ID của mạng con	ID của giao tiếp

Hình 1. 9 Cấu trúc địa chỉ IPv6 dang Global Unicast

Thành phần đầu tiên là ID của các nhà cung cấp dịch vụ hàng đầu tiền TLA (Top Level Aggregation). Cũng giống như IPv4, Có ba tổ chức quản lý việc cấp phát địa chỉ IPv6.

Các tổ chức này cấp phát các giá trị TLA ID đầu tiên. Cụ thể các tổ chức này như sau:

Khu vực Bắc Mỹ là ARIN (American Registry for Internet Numbers), tổ chức này quản lý và đăng ký số hiệu IP của các khu vực Bắc Mỹ, Nam Mỹ, Caribe và một phần châu Phi.

Khu vực châu Âu là NCC (Network Coordinoction Center) của RIPE (hiệp hội mang IP châu Âu).

Khu vực châu Á và Thái Bình Dương là tổ chức APNIC.

Ngoài ra còn có một tổ chức chung có thể cấp phát địa chỉ cho các khu vực khác nhau là IANA.

Các nhà cung cấp dịch vụ Internet IPv6 phải có một " ID của nhà cung cấp " từ những nhà đăng ký trên. Theo kế hoạch cấp phát địa chỉ " ID của nhà cung cấp " là một số 16 bít, 8 bit tiếp theo sẽ được cho bằng 0 trong giải đoạn đầu, 8 bit này chưa sử dụng, được để dành cho các mở rộng tương lai. Chi tiết về việc quản lý và phân bố địa chỉ Global Unicast theo các cấp độ nhà cung cấp sẽ được trình bày trong phần địa chỉ Global Unicast.

Trong cấu trúc hiện tại, những điểm đăng ký chính được bổ sung bởi một số lớn các điểm đăng ký vùng hoặc quốc gia ví dụ French NIC quản lý bởi INRIA cho các mạng của Pháp, những điểm đăng ký này sẽ không được nhận dạng bằng một số đăng ký, thay vào đó họ sẽ nhận được phạm vi nhận dạng của các nhà cung cấp từ các cơ sở đăng ký chính.

Với cấu trúc dang địa chỉ mới này cho phép các khách hàng lớn có thể có được các định danh ngắn hơn và điều đó sẽ cho họ khả năng thêm vào các lớp mạng mới trong phân tầng mạng con của họ. Thực tế các khách hàng lớn còn có thể đòi được chấp nhận như nhà cung cấp của chính họ và lấy được ID nhà cung cấp từ các điểm đăng ký mà không phải lệ thuộc vào nhà cung cấp dịch vụ Internet ISP.

1.3.3. Cách viết địa chỉ IPv6

Địa chỉ IPv6 có chiều dài 128 bít, nên vấn đề nhỏ địa chỉ là hết sức khó khăn. Nếu viết theo dạng thông thường của địa chỉ IPv4 thì một địa chỉ IPv6 có 16 nhóm số hệ cơ sở 10. Do vậy, các nhà thiết kế đã chọn cách viết 128 bít địa chỉ thành 8 nhóm, mỗi nhóm chiếm 2 byte, mỗi byte biểu diễn bằng 2 số hệ 16, mỗi nhóm ngăn cách nhau bởi dấu hai chấm.

Ví dụ: 1080:0000:0000:0000:0008:0800:2000: 417A.

Ký hiệu hexa có lợi là gọn gàng và nhìn đẹp hơn, tuy nhiên cách viết này dùng gây những phức tạp nhất định cho người quản lý hệ thống mạng, nhìn chung mỗi người thường sử dụng theo tên các máy trạm thay bằng các địa chỉ (điều này được áp dụng từ IPv4 khi mà địa chỉ còn đơn giản hơn rất nhiều).

Một cách để làm cho đơn giản hơn là các quy tắc cho phép viết tắt, vì khởi điểm ban đầu chứng tỏ sẽ không sử dụng tất cả 128 bit chiều dài địa chỉ do đó sẽ có rất nhiều số 0 ở các bit đầu.

Một cải tiến đầu tiên là được phép bỏ qua những số không đứng trước mỗi thành phần hệ 16, viết 0 thay vì viết đầy đủ 0000, ví dụ viết 8 thay vì 0008, viết 800 thay vì 0800, qua cách viết này cho chúng ta những địa chỉ ngắn gọn hơn.

Ví dụ trên: 1080:0:0:0:8:800:2000: 417A.

Ngoài ra xuất hiện một quy tắc rút gọn khác đó là quy ước về viết hai dấu hai chấm, trong một địa chỉ, một nhóm liên tiếp các số 0 có thể được thay thế bởi hai hai đầu chấm. Ví dụ: ta có thể thay thế 3 nhóm số 0 liên tiếp trong ví dụ tr và được rút gọn hơn.

1080::8:800:2000:417A

Từ địa chỉ viết tắt này, ta có thể viết lại địa chỉ chính xác ban đầu nhờ quy tắc sau: căn trái các số bên trái của đâu 2 chấm lớp trong địa chỉ, sau đó căn phải tất cả các số bên phải đâu 2 chấm và điền đầy bằng các số 0.

Ví dụ: FEDC:BA98::7654:3210

có địa chỉ đầy đủ là: FEDC:BA98:0:0:0:0:7654:3210

Ví dụ khác:

: FEDC :BA9 8 : 7 6 5 4 : 3210

có địa chỉ đầy đủ là: 0:0:0:0:FEDC:BA98:7654:3210

Quy ước dấu hai đầu chấm chỉ có thể được sử dụng một lần với một địa chỉ.

Ví dụ 0:0:0:BA98:7654:0:0:0

có thể được viết tắt thành ::BA98:7654:0:0:0 hoặc

0:0:0:0:BA98:7654:: những không thẻ viết là ::BA98:7654::

vì như thế sẽ gây nhầm lẫn khi dịch ra địa chỉ đầy đủ.

Một số địa chỉ IPv6 có được hình thành bằng cách gắn 96 bit 0 vào địa chỉ IPv4. (Điều này dễ dàng nhận biết được vì không giãn địa chỉ IPv4 chỉ là một tập con của tập địa chỉ IPv6), để giảm nhỏ nguy cơ nhầm lẫn trong chuyển đổi giữa ký hiệu chấm thập phân của IPv4 và hai dấu chấm thập phân của ký hiệu IPv6, các nhà thiết kế IPv6 cũng đã đưa ra một khuôn mẫu đặc biệt cho cách viết những địa chỉ loại này như sau: Thay vì viết theo cách của 1 địa chỉ IPv6 là:

0:0:0:0:0:0:A00:1

ta có thể vẫn để 32 bít cuối theo mẫu chấm thập phân.

::10.0.0.1

Ngoài ra còn có thể viết địa chỉ mạng theo các tiền tố là các bít cao của địa chỉ IPv6. Điều này có lợi trong việc định tuyến, một địa chỉ IPv6 theo sau bởi một dấu chéo và một số hệ 10 mô tả chiều dài các bit tiền tố. Ví dụ ký hiệu:

FEDC:BA98:7600::/40

mô tả một tiền tố dài 40 bít giá trị nhị phân tương ứng là:

11111110111001011101010011000011101l0

1.4. Các loại địa chỉ IPv6

1.4.1. Địa chỉ unicast

Unicast là một tên mới thay thế cho kiểu địa chỉ điểm - điểm đã được sử dụng trong IPv4, loại địa chỉ này được sử dụng để định danh cho một giao diện trên mạng, một gói dữ liệu có địa chỉ đích là dạng địa chỉ Unicast sẽ được chuyển tới giao diện định danh bởi địa chỉ đó.

Địa chỉ Unicast được chia thành các nhóm nhỏ như sau:

Địa chỉ Global Unicast: được sử dụng để định dạng các giao diện; cho phép thực hiện kết nốt các host trong mạng Internet IPv6 toàn cầu, tính chất loại địa chỉ này cũng giống như địa chỉ IPv4 định danh một host trong mạng Internet hiện nay.

Địa chỉ Site-local: được sử dụng để định dạng các giao diện; cho phép thực hiện các kết nốt giữa các host trong mạng local.

Địa chỉ link-local: được sử dụng để định danh một giao diện.

Ngoài ra còn có một số dạng địa chỉ Unicast khác như NSAP address, IPX address.

1.4.1.1. Địa chỉ global unicast

Theo RFC 2374 mô tả cấu trúc các đang địa chỉ Unicast, dạng địa chỉ này được sử dụng để hỗ trợ cho những nhà cung cấp dịch vụ hiện đang là các đầu mối kết nốt Internet (các ISP), ngoài ra đang địa chỉ này con được sử dụng để hỗ trợ các nhà cung cấp dịch vụ mới có nhu cầu kết nốt toàn cầu, cấu trúc loại địa chỉ này được xây dựng theo kiến trúc phân cấp rõ ràng cụ thể như sau:

3	13 bit	8 bit	24 bit	16 bit	64 bit
FP	TLA	RES	NLA ID	SLA ID	Interface ID

Hình 1. 10: Cấu trúc dạng địa chỉ Unicast

Trong đó:

001: Định dạng tiền tố đối với loại địa chỉ Global Unicast

TLA ID: Định danh cho nhà cung cấp cao nhất trong hệ thống các Nhà cung cấp dịch vụ (Top Level Aggregation)

RES: Chưa sử dụng

NLA ID: Định danh của nhà cung cấp tiếp theo trong hệ thống các nhà cung cấp dịch vụ (Next Level Aggregation)

SLA ID: Định danh các Site của các khách hàng cuối

Interface ID: Định danh của giao tiếp của các host trên mạng trong site của khách hàng cuối; định danh này xác định theo chuẩn EUI-64.

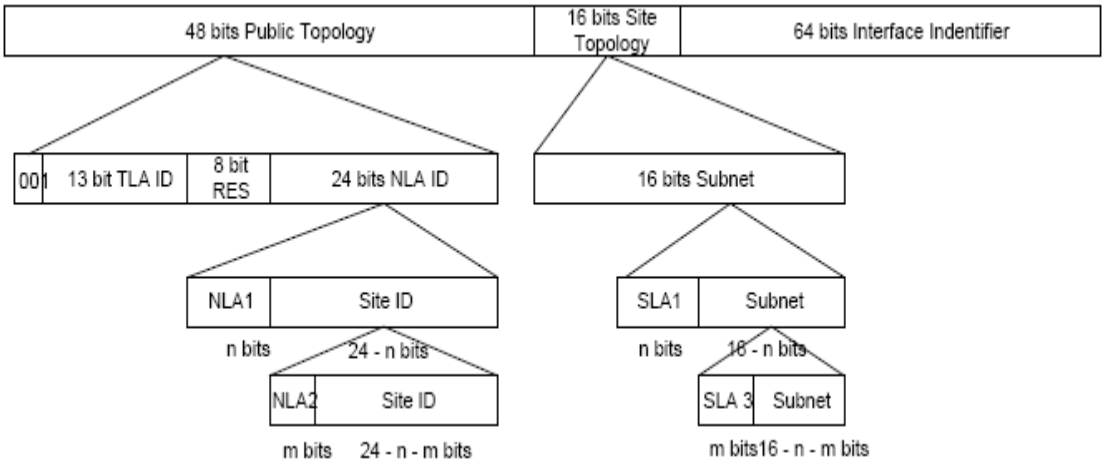
Như vậy loại địa chỉ Global Unicast được thiết kế phân cấp, cấu trúc của nó được chia thành 3 phần :

48 bits Public Topology

16 bits Site Topology

64 bits định danh giao diện

Trong mỗi phần có thể chia làm nhiều cấp con, hình sau minh họa cấu trúc phân cấp này:



Theo hình trên phần giá trị TLA ID c6 ý nghĩa định danh nhà cung cấp dịch vụ IPv6 hàng đầu trên thẻ giới. Có tổng số 213 = 8192 tối đa các TLA, để có được một TLA ID, phải yêu cầu xin cấp qua một số tổ chức quốc tế

Các tổ chức cấp phát TLA ID đã trình bày trong phần phân bố địa chỉ IPv6 ở trên, đối với một ISP (chẳng hạn như VDC) - trong mô hình này đóng vai trò là một NLA (Next Level Aggregation) cần phải xin cấp giá trị NLA ID của mình thông qua các tổ chức TLA, hiện nay có một số phương thức xin cấp giá trị NLA ID như sau:

Xin cấp qua 6Bone Community: Khi đó giá trị TLA ID của tổ chức này là 3FFE::/16. 6Bone là một mang thử nghiệm IPv6 trên toàn cầu, sau khi thỏa mãn một số yêu cầu của tổ chức này 6Bone sẽ cấp phát giá trị NLA ID cho ISP xin cấp địa chỉ.

Xin cấp qua International Regional Internet Registry (RIP).

Giả lập địa chỉ IPv6 từ địa chỉ IPv4 - gọi là 6to4 (Có thể 6to4), với phương thức này thuận lợi cho việc thử nghiệm kết nốt IPv6 dựa trên nền IPv4, từ một máy trạm sử dụng địa chỉ IPv4 ta có một địa chỉ IPv6 dạng Global Unicast như sau: TLA ID có tiền tố 2002::/16, 32 bits còn lại là địa chỉ IPv4 của host đó.

Đối với một tổ chức TLA, sau khi có TLA ID có thể cấp phát tiếp đến các tổ chức cấp dưới, với mọi TLA cho phép định danh tới 224 các tổ chức khác nhau, đối với cấu trúc của NLA ID được phân ra thành các phần nhỏ, sử dụng n bits trong số

24 bits NLA để định danh tổ chức đó, 24 - n bit còn lại dùng để định danh các máy trạm trong mạng.

Mặt khác trong phần địa chỉ NLA ID có thể phân thành các NLA cấp thấp hơn để cho phép cung cấp tới nhiều site sử dụng (end-user-site) khác nhau, đối với một end-user-site sau khi yêu cầu xin địa chỉ sẽ nhận được các thông tin về TLA ID, NLA ID, sẽ gán các giá trị SLA ID để định danh các site trong tổ chức đó và để định dạng các subnets trong mạng con, giá trị này cũng tương tự như với phân bổ các địa chỉ đối với mỗi tổ chức sau khi nhận dtroc một vùng địa chỉ trong IPv4, ngoại trừ là số lượng mạng con trong một site có thể lên tới 65,535 mạng con khác nhau).

Phần còn lại trong cấu trúc địa chỉ Global Unicast là định danh giao diện (Interface ID), định danh này được mô tả theo chuẩn EUI-64, tùy thuộc vào chuẩn các giao tiếp khác nhau mà có các giá trị Interface ID khác nhau. Ví dụ với chuẩn giao tiếp Ethernet có phương thức tạo giá trị Interface ID như sau:

64 bits định dạng EUI-64 được xây dựng từ 48 bits địa chỉ MAC của giao diện cần gán địa chỉ.

Chèn Oxff-fe vào giữa byte thứ 3 và byte thứ 4 trong địa chỉ MAC

Thực hiện đảo bits đối với bit thứ 2 trong byte thứ nhất của địa chỉ MAC

Ví dụ: Ta có địa chỉ MAC của một giao diện như sau: 00-60-08-52- 49-d8

Chèn Oxff-fe vào vị trí giữa byte 0x08 và 0x52 của địa chỉ MAC, do vậy tờ có địa chỉ EUI-64 như sau: 00-60-00-ff-fe-52-49-d8

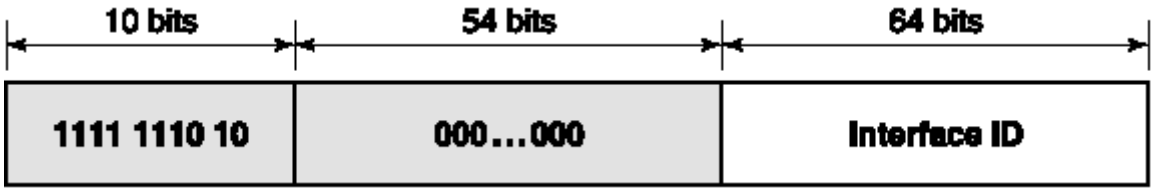
Thực hiện đảo bit đối với bit thấp thứ hai trong byte đầu của địa chỉ MAC. Vì bit thứ hai trong byte đầu của địa chỉ MAC là 0 (0000 0000) do vậy sẽ chuyển thành 1 (0000 0010), nên byte đầu có dạng 0x02.

Cuối dùng ta có phân định đang EUI-64 như sau: 02-60-08-ff-fe-52- 49-d8 với địa chỉ MAC: 00-60-08-52-f9-d8.

1.4.1.2. Địa chỉ local unicast:

Địa chỉ đơn hướng dùng nội bộ, được sử dụng cho một tổ chức có mạng máy tính riêng (dùng nội bộ) chưa kết nối với mạng Internet nhưng sẵn sàng kết nối mang khi cần, địa chỉ này chia làm hai loại là địa chỉ Link Local và Site Local.

Địa chỉ Link Local: Dùng trên mỗi liên kết cho việc tự cấu hình địa chỉ, nhận dạng đường kết nói nội bộ, các router sẽ không chuyển các gói dữ liệu sử dụng Link Local, chúng chỉ cho truyền tin cục bộ trên một đoạn mạng. FP = 1111 1110 10 (FE80::/10), dạng địa chỉ này mang ý nghĩa tương đương với APIPA (Automatic Private IP Addressing) trong IPv4 được tự động gán chó các máy chạy trên nền hệ điều hành MS Window với dải địa chỉ 169.254.0.0/16, cấu trúc của dạng địa chỉ này:



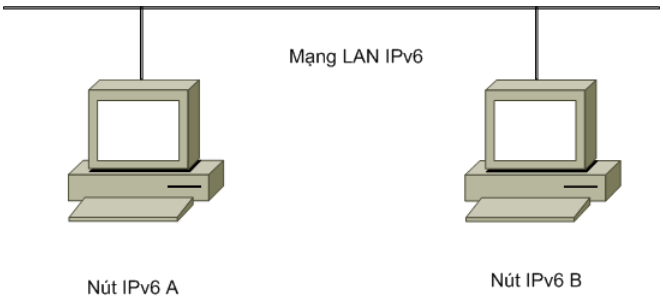
Hình 1. 12 Cấu trúc của địa chỉ Link-local như sau

Giá trị Interface ID được mô tả giống với dạng địa chỉ Global Unicast, nhưng địa chỉ này chỉ được định nghĩa trong phạm vi kết nốt point-to-point (điểm - điểm) và chỉ có thể được sử dụng bởi các trạm kết nốt với cùng một liên kết hay cũng một mạng địa phương.

Qui tắc định tuyến đối với dạng địa chỉ link-local: Một router không thể chuyển bất kỳ gói tin nào có địa chỉ nguồn hoặc địa chỉ đích là địa chỉ link-local

Giả sử có một mạng LAN nhỏ với một ít PC kết nối với nhau và không cần router, lúc đó sẽ dùng địa chỉ Link Local.

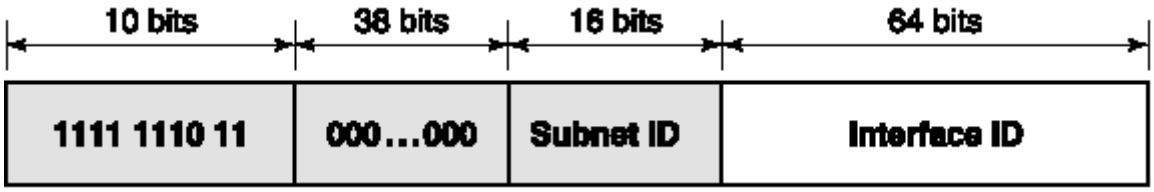
Ví dụ: Kết nốt trực tiếp 2 máy trạm dùng link-local



Hình 1. 13: Hai máy trạm kết nối dùng địa chỉ Link Local

Địa chỉ Site Local: Được dùng để định danh các giao diện, cho phép thực hiện các kết nối giữa các máy trạm trong mạng của công ty hoặc tổ chức. Các router sẽ chuyển các gói tin sử dụng loại địa chỉ này, nhưng không vượt ra ngoài mạng Internet. Nó là địa chỉ dùng cho việc thay thế IPv4 trong mạng intranet. Vì vậy lý tưởng cho các tổ chức không kết nối tới internet toàn cầu. FP = 1111 1110 11 (FEC0::/10). Địa chỉ Site Local tương tự như các dải địa chỉ trong IPv4: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Cấu trúc địa chỉ Site Local:



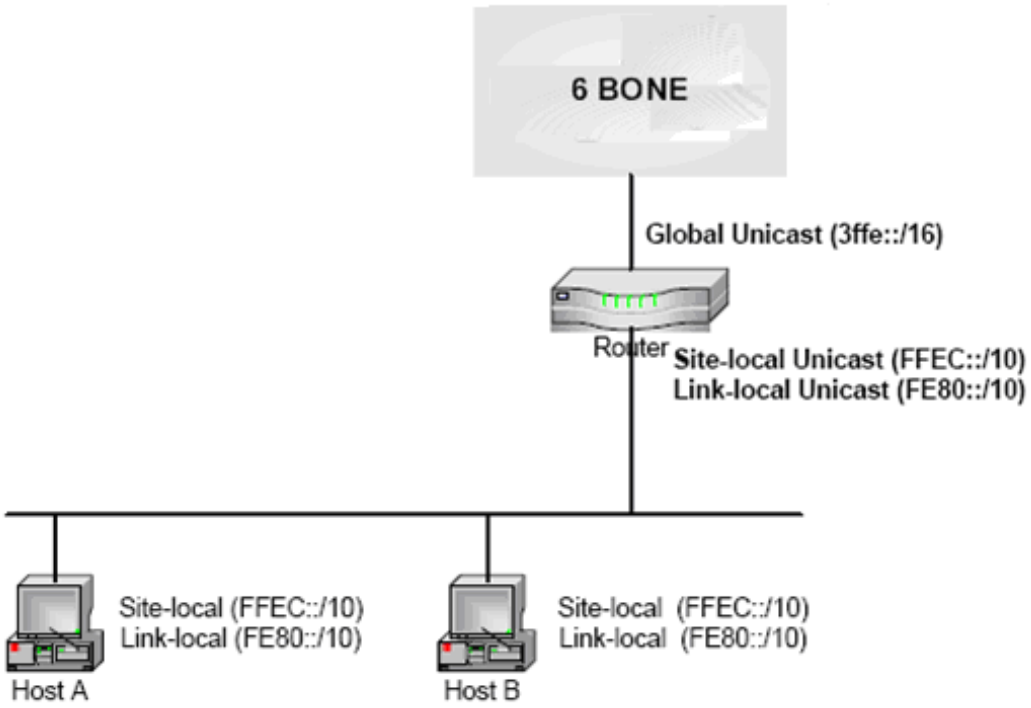
Hình 1. 14: Cấu trúc địa chỉ Site-local

Phần giá trị Interface ID được mô tả giống với dạng địa chỉ Global Unicast Sử dụng link-local để thực hiện kết nốt giữa hai host trực tiếp với nhau.

Sử dụng địa chỉ Site-local Unicast gắn với một giao diện để thực hiện các liên kết với các host trong một site.

Quy tắc định tuyến đối với dạng địa chỉ Site-local: Một router không thể chuyển các gói tin có địa chỉ nguồn hoặc địa chỉ dích là địa chỉ Site-Local Unicast ra ngoài mạng đó. Các địa chỉ site local không thể được chọn đường trên toàn bộ mạng internet. Phạm vi của chúng chỉ được đăng báo phạm vi một site. Chúng chỉ có thể dùng cho các chuyển đổi giữa hai trạm của cùng một site.

Như phần trên đã trình bày, một giao diện có thể gồm nhiều loại địa chỉ khác nhau. Hình sau minh họa các loại địa chỉ được gán cho một host nói chung khi thực hiện kết nốt tới mạng Internet IPv6 (ví dụ mang 6Bone):



Hình 1. 15: Các loại địa chỉ cần gán đối với một Site vào mạng IPv6

1.4.1.3. Địa chỉ unicast theo chuẩn ipx

Là giao thức kết nối không tin cậy (connectionless), dùng trao đổi các gói số liệu giữa các mạng, giao thức cơ bản trong hệ điều hành Novell Netware, địa chỉ này gồm hai phần: 6 byte đầu chứa địa chỉ giao tiếp, 4 byte sau chứa ID của segment (tương tự subnet trong IP), cấu trúc của địa chỉ IPX theo chuẩn của địa chỉ IPv6 có định dạng như sau:

7 bit	121 bit
0000 010	Tự định nghĩa

Hình 1. 16 Cấu trúc địa chỉ IPX theo IPv6

Chi tiết về loại địa chỉ IPX theo chuẩn IPv6 chưa được xác định vì còn đang trong giai đoạn nghiên cứu.

1.4.2. Địa chỉ anycast

Địa chỉ Anycast được gán cho một nhóm các giao diện (thông thường là những nodes khác nhau) và những gói tin có địa chỉ này sẽ được chuyển đổi giao diện gần nhất có địa chỉ này. Khái niệm gần nhất ở đây dựa vào khoảng cách gần

nhất xác định qua giao thức định tuyến sử dụng, thay vì gửi 1 gói tin đến 1 server nào đó, nó gửi gói tin đến địa chỉ chung mà sẽ được nhận ra bởi tất cả các loại server trong loại nào đó, và nó tin vào hệ thống đình tuyến để đưa gói tin đến các server gần nhất này.

Trong giao thức IPv6, địa chỉ anycast không có cấu trúc đặc biệt, các địa chỉ Anycast nằm trong một phần không gian của địa chỉ unicast. Do đó, về mặt cấu trúc địa chỉ Anycast không thể phân biệt với địa chỉ Unicast, khi những địa chỉ Unicast được gán nhiều hơn cho một giao diện nó trở thành địa chỉ Anycast, đối với những node được gán địa chỉ này phải được cấu hình với ý nghĩa của địa chỉ anycast.

Trong cấu trúc của bất kỳ một địa chỉ anycast đều có một phần tiền tố P dài nhất để xác định phạm vi (vùng) mà địa chỉ anycast đó gán cho các giao diện, theo cấu trúc này tiền tố P cho phép thực hiện các qui tắc định tuyến đối với địa chỉ anycast như sau:

Đối với phần phía trong của mạng (vùng): Các giao diện được gần các địa chỉ anycast phải khai báo trong bảng định tuyến trên router của hệ thống đó là những mục riêng biệt với nhau.

Đối với giao tiếp bên ngoài mang, khai báo trên router chỉ gồm một mục là phần tiền tố P (có thể hiểu phần tiền tố này định danh cho một subnet của mạng trong).

Chú ý: Trong trường hợp phần tiền tố P của địa chỉ anycast là một tập các giá trị 0, khi đó các giao diện được gán địa chỉ anycast này không nằm trong một vùng ("vùng" ở đây được hiểu là vùng logic). Do vậy phải khai báo trên các bảng định tuyến như đối với dạng địa chỉ Global Unicast (nghĩa là phải khai báo riêng rẽ từng giao diện).

Qua cơ chế định tuyến đối với dạng địa chỉ Anycast mô tả ở trên ta thấy mục đích thiết kế của loại địa chỉ Anycast để hỗ trợ nhưng tổ chức mà cấu trúc mạng của nó được chia theo cấu trúc phân cấp, trong đó địa chỉ anycast được gán cho các router - mà các router này được chia thành các vùng hay các "đoạn", khi một gói tin đến router cấp cao nhất trong hệ thống nó sẽ được chuyển đến đồng thời các router trong một "đoạn”, sử dụng địa chỉ anycast có những hạn chế như sau:

Một địa chỉ anycast không được sử dụng làm địa chỉ nguồn của một gói tin IPv6.

Một địa chỉ anycast không được phép gán cho một host IPv6 do vậy nó chỉ được gán cho một router IPv6.

Có một loại địa chỉ anycast đặc biệt được sử dụng để định danh cho một subnet. Cấu trúc của loại địa chỉ này như sau:

N bit	128 – n bit
Subnet prefix	000…00

Hình 1. 17: Cấu trúc địa chỉ anycast

Phần subnet prefix trong cấu trúc địa chỉ này xác định một liên kết cụ thể, tính chất của loại địa chỉ anycast giống với địa chỉ unicast link-local gán cho các giao diện trong đó phân định danh giao diện được đặt là 0.

Loại địa chỉ này được sử dụng cho những node cần giao tiếp đồng thời với một tập các router trên mạng. Ví dụ người dùng di động có nhu cầu đồng thời cũng một lúc giao tiếp với các máy cố định và với các máy trong mạng di động.

1.4.3. Địa chỉ multicast

1.4.3.1. Cấu trúc chung

Địa chỉ multicast được gán cho một nhóm các giao diện (thông thường là những nodes khác nhau), một gói tin có địa chỉ multicast sẽ được chuyển tới tất cả các giao diện có gán địa chỉ multicast này.

Trong IPv6, hoạt động của các gói dữ liệu Multicast tương tự như ở IPv4, một node IPv6 bất kỳ có thể tiếp nhận các gói tin Multicast có địa chỉ Multicast bất kỳ hay một node IPv6 có thể đồng thời tiếp nhận nhiều gói tin với địa chỉ Multicast khác nhau, một gói tin có địa chỉ Multicast sẽ chuyển tới tất cả các giao diện có gán địa chỉ này.

Địa chỉ Multicast IPv6 không được dùng làm địa nguồn hay một địa chỉ đích trung gian trong phần header của các bản tin định tuyến.

Các thủ tục mới cho phép nhận dạng địa chỉ Multicast mà tất cả các router sẽ nhận ra, chúng liên kết các hàm (chức năng) ICMP của IPv4 trong thủ tục ICMPv6, chúng đảm bảo rằng tất cả router có thể định tuyến các gói tin Multicast.

8 bit	4 bit	4 bit	112 bit
1111 1111	Flags	Scope	Group ID

Hình 1. 18: Cấu trúc của địa chỉ Multicast

Flag(cờ): 4 bít cờ thì có bit thứ 4 được dùng cho IPv6, 3 bít còn lại chưa được định nghĩa và được gán giá trị 0. Cụ thể như sau:

0	0	0	T

Nếu bit T có giá trị là 0 thì địa chỉ Multicast IPv6 này là địa chỉ được phân cố định bởi IANA (địa chỉ Multicast well-known), nếu bit T bằng 1 thì địa chỉ Multicast này được gán tạm thời không được phân cố định.

Scope (phạm vi) được mã hóa 4 bit, nó được dùng để giới hạn phạm vi nhóm địa chỉ Multicast trong mạng IPv6, ngoài các thông tin có được từ giao thức định tuyến Multicast, các router phải sử dụng thêm thông tin trong trường phạm vi để xét xem có tiếp tục chuyển tiếp các gói tin Multicast nữa không. Các giá trị của trường này như sau:

Giá trị	Phạm vì
0	Chưa sử dụng
1	Node- local (node có phạm vi địa phương)
2	Link Local (liên kết có phạm vi địa phương)
5	Site Local (site có phạm vi địa phương)
8	Organization-local (Tổ chức có phạm vi địa phương)
E	Global (Phạm vi tổng thể)
F	Chưa sử dụng

Bảng 1. 2: Các giá trị của trường phạm vi

Ví dụ: Địa chỉ Multicast FF02::2 chỉ có phạm vi trong link-local, các router sẽ không thực hiện chuyển tiếp gói tin ra khỏi kết nối đó.

Group IP (nhận dạng nhóm): nhận dạng nhóm Multicast là duy nhất trong phạm vi xác định, bao gồm 112 bit, các định dạnh nhóm cố định là độc lập với các phạm vi, chỉ có các định dang tạm thời mới có liên quan tới một phạm vi nhất định. Các địa chỉ Multicast từ FF01:: tới FF0F là nhóm địa chỉ được dành riêng. Ví dụ

xác định tất cả các node trong phạm vi kiểu node-local hoặc link-local thì sử dụng các địa chỉ sau:

FF01::1 - Địa chỉ Multicast cho tất cả các node trong phạm vi node-local

FF02::1 - Địa chỉ Multicast cho tất cả các node trong phạm vi link-local.

Để xác định tất cả các router trong phạm vi site-local, link-local hay node-local thì sử dụng các địa chỉ sau:

FF01::2 - Địa chỉ Multicast cho tất cả các router trong phạm vi node-local.

FF02::2 - Địa chỉ Multicast cho tất cả các router trong phạm vi link-local.

FF03::2 - Địa chỉ Multicast cho tất cả các router trong phạm vi site-local.

Với 112 bit sử dụng cho nhận dạng nhóm do đó có thể có tới 2112 nhận dạng nhóm khác nhau, tuy nhiên do việc địa chỉ IPv6 được ánh xạ vào địa chỉ Multicast MAC Ethernet nên sử dụng 32 bit cuối cùng của địa chỉ IPv6 Multicast cho nhận dạng nhóm và đặt các bit còn lại là bit "0", với việc sử dụng 32 bit cuối của địa chỉ IPv6 Multicast mỗi một nhận dạng nhóm được ánh xạ vào một địa chỉ MAC multicast Ethernet duy nhất. Cấu trúc địa chỉ Multicast IPv6 bây giờ có dạng như sau:

8 bit	4 bit	4 bit	80 bit	32 bit
1111 1111	Flags	Scope	000…. 00	Group ID

Bảng 1. 3: Cấu trúc địa chỉ Multicast được phân bố lại

1.4.3.2. Địa chỉ solicited-node

Dạng địa chỉ này tạo điều kiện cho quá trình phân giải địa chỉ của các node trong mạng một cách hiệu quả hơn, cũng là giúp cho quá trình định tuyến thực hiện hiệu quả hơn. Trong IPv4 các khung mang nội dung phân giải địa chỉ ARP Request được gửi quảng bá tại lớp 2 trong mạng tới tất cá các node trên phan đoạn mạng đó cho dù node đó không sử dụng giao thức IPv4. Với IPv6 quá trình phân giải địa chỉ được thực hiện bằng các bản tin tìm hàng xóm (Network Solicitation), tuy nhiên thay bằng việc sẻ dụng các bản tin tìm kiếm hàng xóm với địa chỉ đích là địa chỉ Multicast cho tấ cả các node trong phạm vi link-local bằng các bản tin có địa chỉ

đích là Multicast Solicited-node. Điều này sẽ hạn chế số lượng node trong phạm vi link-local phải nhận các bản tin phân giải địa chỉ. Địa chỉ multicast Solicited-node bao gồm 104 bit đầu có dạng FF02::1 tới FF00::0/104 và 24 bit cuối của địa chỉ IPv6 sẽ được phân giải.

Ví dụ: Một node A được gán địa chỉ link-local là FE80::2AA:FF:FE28:9C5A đang tiếp nhận các gói tin với địa chỉ multicast dạng Solicited-node FF02::1:FF28:9C5A (phần gạch dưới chỉ 6 số hệ 16 cuối cùng), tại node B thuộc cùng một link-local cần phải phân giải địa chỉ link-local của node A là FE80:2AA:FF:FE28:9C5A thành địa chỉ ở lớp 2 tương ứng của node B.Node B sẽ thực hiện gửi bản tin Network Solicited với địa chỉ Solicited-node là FF02::1:FF28:9C5A vào link-local, do node A đang tiếp nhận các gói tin với địa chỉ multicast này nên nó sẽ xử lý bản tin tìm kiếm hàng xóm này và gửi trả lời lại bằng bản tin unicast thông báo hàng xóm (Network Advertisement).

Kết quả của việc sử dụng địa chỉ multicast dạng Solicited-node là sự phân giải địa chỉ trong một kế nối hiệu quả hơn do khong phải tất cả các node trong mạng đều phải nhận bản tin yêu cầu địa chỉ. Trong thực tế do mối quan hệ giữa địa chỉ MAC trong mạng Ethernet và phần nhận dạng giao diện trong địa chỉ IPv6 nên địa chỉ multicast Solicited-node đóng vai trò như một địa chỉ unicast giả (pseudo-unicast).

1.4.4. Các dạng địa chỉ IPv6 khác

1.4.4.1. Địa chỉ không xác định:

Địa chỉ 0:0:0:0:0:0:0:0 được gọi là địa chỉ không xác định. Địa chỉ này không thật sự được gán cho một giao diện nào, một host khi khởi tạo có thể sử dụng địa chỉ này như là địa chỉ nguồn của nó trước khi nó biết được địa chỉ thật của nó, một địa chỉ không xác định không bao giờ có thể đóng vai trò là địa chỉ đích trong ghi tin IPv6 hay trong phần header của quá trình định tuyến.

1.4.4.2. Địa chỉ loopback

Địa chỉ 0:0:0:0:0:0:0:1 được gọi là địa chỉ loopback. Một nodes có thể sử dùng địa chỉ này để gửi một gói tin IPv6 cho chính nó, địa chỉ loopback không bao giờ được sử dụng như địa chỉ nguồn của bất kỳ ghi tin IPv6 nào để gửi ra ngoài

nodes. Một gói tin với địa chỉ loopback là địa chỉ đích sẽ không bao giờ có thể ra khỏi node đó.

1.4.4.3. Địa chỉ tương thích

Để phục vụ cho quá trình chuyển đổi từ IPv4 sang IPv6 và sự song song tồn tại của cả hai loại máy trạm (host) dùng cả hai kiểu địa chỉ trên, những loại địa chỉ sau đã được định nghĩa:

Địa chỉ IPv4-compatible: địa chỉ này có định dạng 0:0:0:0:0:w.x.y.z hay ::w.x.y.z (với w.x.y.z địa chỉ IPv4), nó được các node đôi sử dụng khi giao tiếp với các node IPv6 trên hạ tầng IPv4, ta gọi loại này là địa chỉ IPv4 tương thích IPv6, khi địa chỉ loại này được sẻ dụng làm địa chỉ IPv6 đich thì các gói tin IPv6 sẽ được đóng gói cùng IPv4 header và gửi đến node đích bằng hạ tầng IPv4.

Địa chỉ IPv4-mapped: là địa chỉ dạng 0:0:0:0:0:FFFF:w.x.y.z hoặc ::FFFF:w.x.y.z, được dùng để chỉ một node thuần IPv4 đối với một node IPv6, địa chỉ này cỉ được dùng trong việc mô tả bên trong mà thôi, nó không bao giờ được dùng làm địa chỉ nguồn hay địa chỉ đích trong một gói tin IPv6, địa chỉ IPv4-mapped này được sử dụng trong vài kiểu triển khai IPv6 khi đóng vai trò là một node thuần IPv4 sang node thuần IPv6.

Địa chỉ dạng 6over4: Địa chỉ này là việc kết hợp 64 bit tiền tố hợp lệ của địa chỉ Unicast và địa chỉ giao diện ::WWXX:YYZZ (với WWXX:YYZZ là địa chỉ dạng hệ số 16 của địa chỉ w.x.y.z – địa chỉ IPv4 gán cho giao diện). Ví dụ: host được gán địa chỉ IPv4 là 131.107.4.92 thì địa chỉ link-lcal 6over4 của hsot sẽ là FE80::836B:45C. Địa chỉ dạng này được dùng cho một host khi sử dụng cơ chế tunnel tự động 6over4 (xác định bởi RFC 2529).

Địa chỉ dang 6to4: Địa chỉ này bắt đầu là tiền tố 2002 và có dạng như sau: 2002: WWXX:YYZZ/48 (Với WWXX:YYZZ là địa chỉ dạng hệ số 16 của địa chỉ w.x.y.z – địa chỉ IPv4 gán cho giao diện), địa chỉ này chỉ sử dụng trong phương thức chuyển đổi theo cơ chế đường hầm 6to4 .

Địa chỉ ISATAP: Địa chỉ ISATAP (Intra-site Automatic Tunnel Addressing Protocol) này được tạo thành từ 64 bit tiền tố hợp lệ của địa chỉ unicast và địa chỉ giao diện ::0:5EFE:w.x.y.z (với w.x.y.z là địa chỉ IPv4 gán cho giao diện). Ví dụ:

địa chỉ lik-local ISATAP là FE80::5EFE:131.107.4.92, địa chỉ kiểu ISATAP này được gán cho một hót sử dụng cơ chế tunnel tự động ISATAP, cơ chế tunnel tự động này được xác định trong bản thảo về Internet với tiêu đề 'Intra-site Automatic Tunnel Addressing Protocol" (draft-ietf-íatap-06.txt).

1.4.5. Phương thức gán địa chỉ IPv6

Theo đặc tả của giao thức IPv6, tất cả các loại địa chỉ IPv6 được gán cho các giao diện, không gán cho các nút (khác với IPv4), mỗi địa chỉ IPv6 loại Unicast (gọi tắt của địa chỉ Unicast) được gán cho một giao diện đơn, vì mỗi giao diện thuộc về một nút đơn như vậy mỗi địa chỉ Unicast định danh một giao diện sẽ định danh một nút.

Các địa chỉ IPv6 được gán cho một nút:

- Một địa chỉ link-local cho mỗi giao diện gắn với host đó.
- Các địa chỉ Unicast cho mỗi giao diện. Có thể là một địa chỉ site-local và một hay nhiều địa chỉ global Unicast.
- Mỗi địa chỉ loopback cho giao diện loopback(::1).

Một host IPv6 bình thường có thể được coi một cách logic là đa vị trí (multihome) bởi nó có ít nhất là hai địa chỉ. Một là địa chỉ link-local cho giao tiếp với các trong cùng kết nối, hai là địa chỉ site-local hay global unicast để thông tin với các node khác trong cùng một site hay ở các site khác. Ngoài ra một host còn có các địa chỉ multicast sau:

- FF01::1 địa chỉ multicast cho tất cả các node trong phạm vi node-local.
- FF02::1 địa chỉ multicast cho tất cả các node trong phạm vi link-local.
- Địa chỉ solicited-node cho mỗi một địa chỉ Unicast trên mõi giao diện
- Các địa chỉ multicast để gia nhập nhóm trên mỗi giao diện.

Các địa chỉ IPv6 được gán cho một router:

- Địa chỉ link-local cho mỗi giao diện của router.
- Các địa chỉ Unicast cho mỗi giao diện, có thể là một địa chỉ site-local và một hay nhiều địa chỉ global unicast.
- Một địa chỉ anycast dạng Subnet-router
- Các địa chỉ anycast khác

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

Ngoài ra router còn được gán các địa chỉ multicast như sau:

- FF01::1 địa chỉ multicast cho tất cả các node trong phạm vi node-local
- FF01::2 địa chỉ multicast cho tất cả các router trong phạm vi node-local
- FF02::1 địa chỉ multicast cho tất cả các node trong phạm vi link-local
- FF02::2 địa chỉ multicast cho tất cả các router trong phạm vi link-local
- FF05::2 địa chỉ multicast cho tất cả các router trong phạm vi site-local
- Địa chỉ solicited-node cho mỗi địa chỉ Unicast trên mỗi giao diện
- Các địa chỉ multicast để ra nhập nhóm trên mỗi giao diện.

1.5.6. So sánh giữa IPv4 và IPv6 về địa chỉ

Bảng dưới đây liệt kê sự tương ứng giữa các khái niệm địa chỉ trong IPv4 và IPv6.

Khái niệm	**địa chỉ IPv4**	**địa chỉ IPv6**
Các lớp địa chỉ trên internet	Các lớp A, B, C	Không tồn tại trong IPv6
Dải địa chỉ multicast	224.0.0.0/4	FF00::/8
Địa chỉ broadcast	là địa chỉ cao nhất thuộc một phân mạng	không tồn tại trong IPv6
Địa chỉ không xác định	0.0.0.0	::
Địa chỉ loopback	127.0.0.1	::1
Các địa chỉ IP công cộng	địa chỉ IP công cộng	Địa chỉ global unicast
Các địa chỉ IP cho mạng riêng	10.0.0.0/8, 172.16.0.0/12, và 192.168.0.0/16	các địa chỉ site-local (FEC0::/48)
Dải địa chỉ tự động cấu hình	169.254.0.0/16	Link-local (FE80::/64)
Cách biểu diễn địa chỉ (cách viết)	Dạng bốn chữ số thập phân ngăn bởi dấu chấm. các địa chỉ được viết ở dạng thập phân có ngăn cách bằng dấu chấm.	Các khối 4 chữ số hệ 16 ngăn cách nhau bởi dấu ":" có thể thực hiện thu gọn các số không dấu mỗi khối và thay thế các khối mang giá trị 0 liên tiếp bằng 2 dấu chấm
Các bit đại diện cho mạng	Dạng mặt nạ mạng được viết dưới dạng thập phân hoặc theo dạng chiều dài tiền tố	Chỉ được viết ở dạng chiều dài tiền tố

Bảng 1. 4 So sánh địa chỉ IPv4 và IPv6

1.5. Kết luận Chương 1

Chương này đã đưa ra sự hạn chế của IPv4, những vấn đề cần thiết phải chuyển đổi sang IPv6, trong nội dung chương đưa ra cấu trúc, phân bổ cà cách đánh địa chỉ IPv6, các tính năng và các loại địa chỉ IPv6 mang tính ưu việt hơn địa chỉ IPv4.

CHƯƠNG 2: CÁC GIẢI PHÁP CHUYỂN ĐỔI HẠ TẦNG TỪ IPV4 SANG IPV6

2.1. Mục đích chuyển đổi IPv4 – IPv6

Giao thức IPv6 có nhiều ưu điểm vượt trội so với IPv4, đáp ứng được nhu cầu ph triển của mạng Internet hiện tại và trong tương lai. Do đó, giao thức IPv6 sẽ thay thế IPv4. Tuy nhiên, không thể chuyển đổi toàn bộ các nút mạng IPv4 hiện nay sang IPv6 trong một thời gian ngắn, hơn nữa nhiều ứng dụng mạng hiện tại chưa hỗ trợ IPv6, theo dự báo của tổ chức ISOC, IPv6 sẽ thay thế IPv4 vào khoảng 2020-2030. Các cơ chế chuyển đổi (transition mechanism) phải đảm bảo khả năng tương tác giữa các trạm, các ứng dụng IPv4 hiện có với các trạm và ứng dung IPv6. Ngoài ra các cơ chế cũng cho phép chuyển tiếp các luồng thông tin IPv6 trên hạ tầng định tuyến hiện có, trong giai đoạn chuyển đổi, điều quan trọng là phải đảm bảo sự hoạt động bình thường của mạng IPv4 hiện tại. Từ đó đặt ra yêu cầu đối với các cụ thể chuyển đổi:

Việc thử nghiệm IPv6 không ảnh hưởng đến các mang IPv4 hiện đang hoạt động kết nốt và các dịch vụ IPv4 tiếp tục hoạt động bình thường.

Hiệu năng hoạt động của mạng IPv4 không bị ảnh hưởng, giao thức IPv6 chỉ tác động đến các mạng thử nghiệm.

Quá trình chuyển đổi diễn ra từng bước, không nhất thiết phải chuyển đổi toàn bộ các nút mạng sang giao thức mới.

Các cơ chế chuyển đổi phân thành 3 nhóm:

Kết nối các nút mạng IPv6 qua hạ tầng IPv4 hiện có, cơ chế này gọi là: Đường hầm (Tunnel).

Kết nối các nút mạng IPv4 với các nút mạng IPv6, đây là cơ chế chuyển dịch (Translation).

Thực hiện hoạt động song song cả IPv4 sang IPv6 trên mỗi nút mạng, cơ chế này gọi là Dual Stack.

Trong cơ chế đường hầm có các cơ chế sau:

Đường hầm cấu hình bằng tay.

Đường hầm tự động: Đường hầm 6to4, đường hầm 6over4, Compatible IPv4 (tương thích IPv4), ISATAP, Tunnel Broker.

Trong cơ chế chuyển dịch có các cơ chế:

BIS (Bump into the Stack)

DSTM (Dual Stack Translation Mode)

NAT-PT (Network Address Translation – Protocol Translation)

SOCKs

TCP-UDP Relay

Trong chương này sẽ tập trung phân tích một số cơ chế được sử dụng phổ biến:

Đường hầm 6to4

Đường hầm ISATAP

Dual Stack

Mỗi cơ chế có ưu nhược điểm và phạm vi áp dụng khác nhau, tùy từng thời điểm trong giai đoạn chuyển đổi, mức độ sử dụng các cơ chế chuyển đổi sẽ khác nhau:

Giai đoạn đầu: Giao thức IPv4 chiếm ưu thế, các mạng IPv6 kết nối với nhau trên nền hạ tầng IPv4 hiện có thông qua các đường hầm IPv6 qua IPv4.

Giai đoạn tiếp theo: Giao thức IPv4 và IPv6 được triển khai về phạm vi ngang nhau trên mạng, các mạng IPv6 kết nối với nhau qua hạ tầng định tuyến IPv6, các mạng IPv4 kết nối với các mạng IPv6 sử dụng các phương thức chuyển đổi địa chỉ giao thức như NAT-PT.

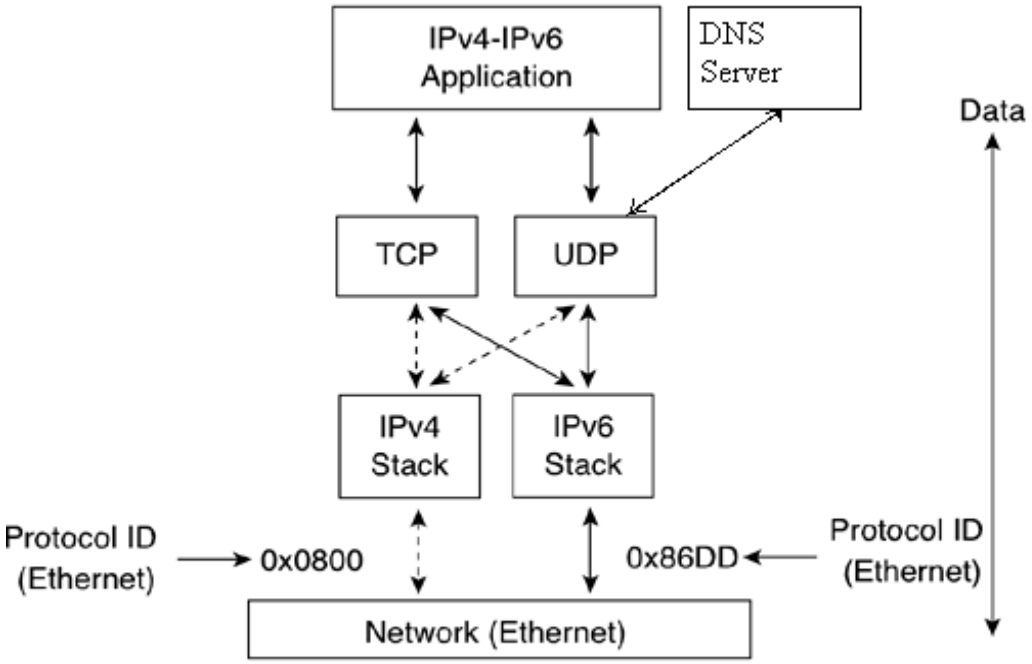
Giai đoạn cuối: Giao thức IPv6 chiếm ưu thế, các mạng IPv4 còn lại kết nối với nhau trên hạ tầng định tuyến IPv6 thông qua các đường hầm IPv4 qua IPv6 trước khi chuyển hoàn toàn sang IPv6.

Tiếp sau đây sẽ mô tả một số cơ chế chuyển đổi thông dụng.

2.2. Cơ chế dual stack

Dual Stack còn gọi là cơ chế chồng giao thức, là cơ chế cơ bản nhất cho phép nút mạng đồng thời hỗ trợ cả hai giao thức IPv4 và IPv6, có được khả năng trên do một trạm Dual Stack cài đặt cả hai giao thức IPv6 và IPv4, trạm Dual Stack sẽ giao

tiếp bằng giao thức IPv4 với các trạm IPv4 và bằng giao thức IPv6 với các trạm IPv6.



Hình 2. 1: Chồng hai giao thức

2.2.1. Cấu hình địa chỉ

Do hoạt động của cả hai giao thức, nút mạng kiểu này cần ít nhất một địa chỉ IPv4 và một địa chỉ IPv6, địa chỉ IPv4 có thể được cấu hình trực tiếp hoặc thông qua cơ chế DHCP, địa chỉ IPv6 được cấu hình trực tiếp hoặc thông qua khả năng tự động cấu hình địa chỉ.

Dual stack đáp ứng được hầu hết các yêu cầu về phân giải DNS và lựa chọn địa chỉ. Trang thái mặc định mà một nút phải quan sát là các câu hỏi DNS phải dự định phân giải cho địa chỉ IPv6 trước tiên và nếu không hợp lệ sẽ quay trời lại địa chỉ IPv4, các node sử dụng cơ chế của IPv4 (ví dụ DHCP) để yêu cầu các địa chỉ IPv4 và sử dụng các cơ chế giao thức IPv6 (ví dụ tự cấu hình địa chỉ không trạng thái) để yêu cầu địa chỉ IPv6.

2.2.2. Dịch vụ cung cấp tên miền (dns)

DNS (Domain Name Service) được sử dụng trong cả IPv4 và IPv6 để ánh xạ giữa tên máy và các địa chỉ,một bản ghi tài nguyên mới gọi là A6 được định nghĩa

cho IPv6 với sự hỗ trợ của một bản ghi trước đây gọi là AAAA, nút mạng hỗ trợ các ứng dụng với cả hai giao thức. Chương trình tra cứu tên miền có thể tra cứu đồng thời cả các truy vấn kiểu A lẫn kiểu AAAA (A6). Nếu kết quả trả về là bản ghi kiểu A, ứng dụng sẽ sử dụng giao thức IPv4, nếu kết quả trả về là bản ghi A6, ứng dụng sẽ sử dụng giao thức IPv6, nếu cả hai kết quả được trả về, chương trình sẽ lựa chọn trả về cho ứng dụng một trong hai kiểu địa chỉ hoặc ca hai, nếu nó trả về cả hai thì bộ phân giải có thể lựa chọn sử dụng thứ tự địa chỉ IPv6 trước hoặc IPv4 trước.

2.2.3. Ưu điểm của dual stack

Đây là cơ chế cơ bản nhất để nút mạng có thể hoạt động đồng thời với cả hai giao thức nên nó được hỗ trợ trên nhiều nền tảng hệ điều hành khác nhau như: FreeBSD, Linux, Solaris, Window.

Cơ chế này dễ triển khai, cho phép duy trì các kết nối bằng cả hai giao thức IPv4, IPv6.

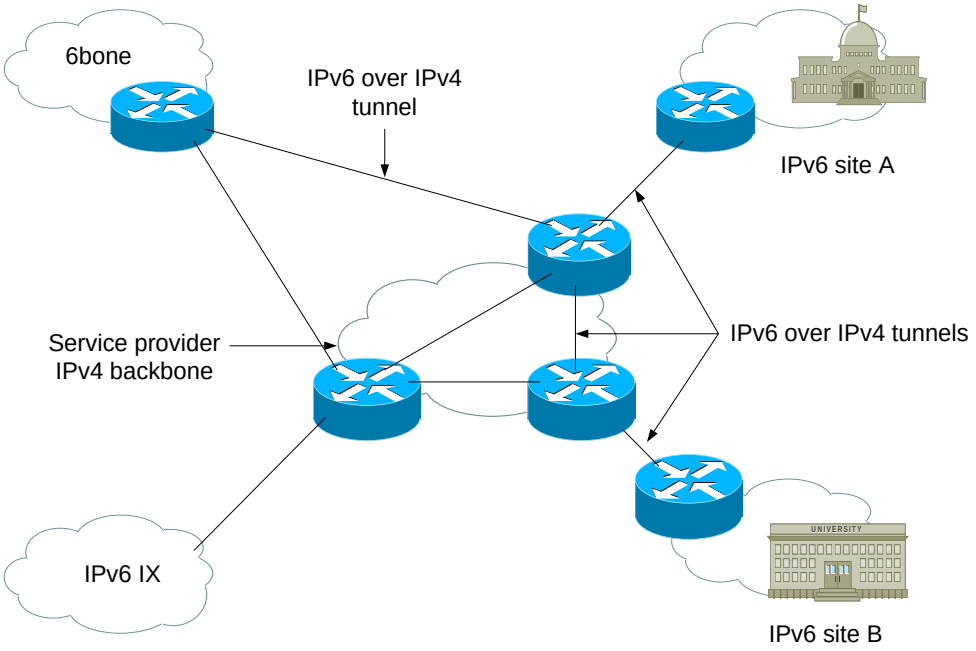
2.2.4. Nhược điểm của dual stack

Cấu hình mạng có thể sử dụng hai bảng định tuyến và hai quy trình định tuyến thuộc hai giao thức định tuyến, IPv6 có cơ chế bảo mật tích hợp còn IPv4 thì lại phải có phần mềm riêng nên khả năng mở rộng kém vì phải sử dụng địa chỉ IPv4.

2.3. Đường hầm IPv6 qua IPv4

Đường hầm cho phép kết nối các nút mạng IPv6 qua hạ tầng định tuyến IPv4 hiện có vì vậy cho phép các lưu lượng IPv6 được mang qua IPv4, đường hầm là chiến lược triển khai quan trọng cho cả ISP và các công ty trong mạng đồng tồn tại IPv4 và IPv6.

Đường hầm cho phép nhà cung cấp dịch vụ cung cấp các dịch vụ đến tận đầu cuối (end-to-end) mà không phải nâng cấp cấu trúc mạng và không ảnh hưởng đến các dịch vụ IPv4 đang có, đường hầm giúp cho các công ty có thể liên hoạt động với các miền IPv6 bị cách ly thông qua cấu trúc IPv4 hiện tại của họ hoặc để kết nối với mạng IPv6 từ xa như là 6Bone.



Hình 2. 2: Triển khai các đường hầm IPv6 thông qua IPv4

Có một số cơ chế đường hầm được sử dụng thông dụng như sau:

Các đường hầm tạo thủ công như đường hầm IPv6 được cấu hình bằng tay.

Các đường hầm tự động : 6to4, Tunnel Broker, ISATAP, …

Các trạm và các router IPv6 thực hiện định đường hầm bằng cách gói các gói tin IPv6 trong gói tin IPv4. Nếu phân loại đường hầm theo đầu cuối thì có có 4 loại:

Đường hầm từ router đến router.

Đường hầm từ trạm tới router.

Đường hầm từ trạm tới trạm.

Đường hầm từ router tới trạm.

Các cách thực hiện đường hầm khác nhau ở vị trí của đường hầm trong tuyến đường giữa hai nút mạng. Trong hai cách đầu, gói tin được định đường hầm tới một router trung gian sau đó router này chuyển tiếp gói tin đến đích. Với hai cách sau, gói tin được định đường hầm thẳng tới đích.

Để thực hiện đường hầm, hai điểm đầu đường hầm phải là các nút mạng hỗ trợ cả hai giao thức. Khi cần chuyển tiếp gói tin IPv6, điểm đầu đường hầm sẽ đóng gói gói tin IPv4 bằng cách thêm phần mở đầu mào đầu IPv4 phù hợp.

Khi gói tin IPv4 đến điểm cuối đường hầm, gói tin IPv6 sẽ được tách ra để xử lý tùy theo kiểu đường hầm.

Gói tin ban đầu:

IPv6 header	Dữ liệu

Gói tin đường hầm:

IPv4 header	IPv6 header	Dữ liệu

Gói tin ra khỏi đường hầm

IPv6 header	Dữ liệu

Hình 2. 3: Quy trình chuyển gói tin qua đường hầm

Tiếp đây ta xét một số đường hầm thông dụng.

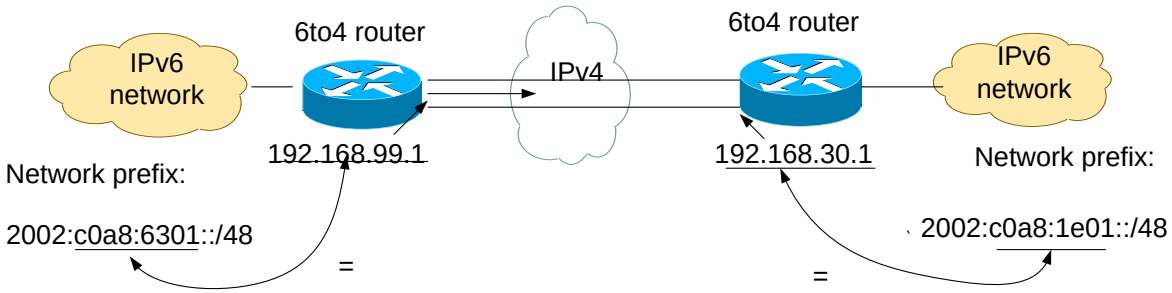
Cấu hình đường hầm tự động

Đặc điểm của đường hầm tự động là địa chỉ điểm cuối đường hầm được xác định một cách tự động. Đường hầm được tạo ra một cách tự động và cũng tự động mất đi.

2.3.1. Cơ chế cấu hình tự động 6to4

6to4 về bản chất là một cơ chế đường hầm tự động router đến router, cho phép kết nối các mạng IPv6 với nhau thông qua hạ tầng IPv4 ngăn cách, cho phép các miền IPv6 cách ly có thể được nối với nhau thông qua mạng IPv4, cơ chế này được cài đặt tại các router ở biên của mạng, mỗi miền IPv6 phải có một router Dual Stack mà nó nhận dạng đường hầm IPv4 bởi một tiền tố duy nhất trong địa chỉ IPv6.

Địa chỉ IPv6 sử dụng trong các mạng 6to4 có cấu trúc đặc biệt và được cấp phát riêng một lớp địa chỉ có tiền tố FP = 001 và giá trị trường TLA = 0x0002 tạo thành tiền tố địa chỉ 2002::/16, mỗi mạng sẽ có tiền tố chuyển đổi mạng hình thành bằng cách kết hợp 16 bit tiền tố chung với 32 bit địa chỉ IPv4 của router tương ứng, tiền tố này có độ lớn 48 bit và có thể biểu diễn dưới dạng 2002:V4ADDR::/48. V4ADDR (địa chỉ IPv4) được hiển thị dạng hệ số 16 dạng abcd:efgh.



Hình 2. 4: Cơ chế 6to4

Khuôn dạng của một địa chỉ 6to4 như sau:

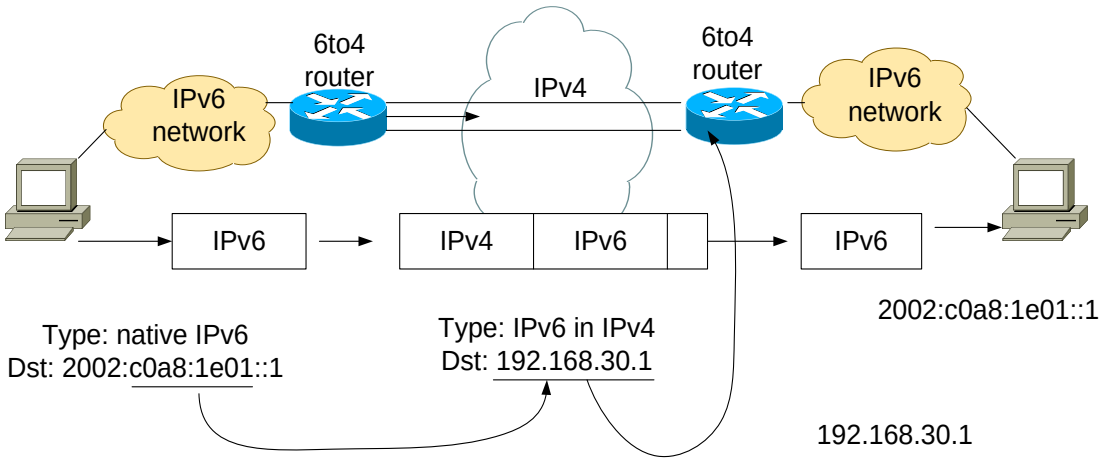
FP	TLA	IPv4ADDR	SLA ID	Interface ID

Hình 2. 5: Khuôn dạng địa chỉ 6to4

Host 6to4: Bất kỳ một host IPv6 nào được cấu hình ít nhất một địa chỉ 6to4 (địa chỉ global với tiền tố 2002::/16). Các host 6to4 không yêu cầu cấu hình băng tay và sử dụng cơ chế tự cấu hình địa chỉ.

Router 6to4: Một router 6to4 sử dụng giao tiếp đường hầm 6to4 và được sử dụng đặc trưng cho việc chuyển lưu lượng có địa chỉ 6to4 giữa các host 6to4 trong một site hoặc các router 6to4 khác hoặc router chuyển tiếp 6to4 trên một liên mạng IPv4 (như Intemet). Router này thực hiện mã hoa/giải mã (encapsulation/decapsulation) gói tin và có thể thêm yêu cầu cấu hình bằng tay.

Cơ chế hoạt động:



Hình 2. 6: Cơ chế hoạt động 6to4

Khi có một gói tin IPv6 với địa chỉ đích có dạng 2002::/16 được gửi đến một router 6to4, router 6to4 tách địa chỉ IPv4 (địa chỉ IPv4 vừa tách được chính là địa chỉ IPv4 ccuar router 6to4 đích), bọc gói tin IPv6 trong gói tin IPv4 với địa chỉ đích là địa chỉ IPv4 vừa tách được, sau đó các gói tin sẽ được chuyển tiếp trên hạ tầng IPv4, khi router 6to4 đích nhận được gói tin, gói tin IPv6 sẽ được tách ra và chuyển đến nút mạng IPv6 đích.

Ưu điểm của cơ chế 6to4:

Các nút không bắt buộc phải dùng địa chỉ IPv6 kiểu tương thích IPv4 như các đường hầm tự động khác.

Không cần thiết nhiều cấu hình đặc biệt như đường hầm cấu hình bằng tay.

Không bị ảnh hưởng bởi các hệ thống tường lửa của mạng, chỉ cần router của mạng có địa chỉ IPv4 toàn cục có thể định tuyến.

Nhược điểm:

Chỉ thực hiện với một lớp địa chỉ đặc biệt.

Có nguy cơ bị tấn công theo kiểu của đường hầm tự động nếu phần địa chỉ IPv4ADDR trong địa chỉ của gói tin 6to4 là địa chỉ broadcast hay multicast.

2.3.2. Cơ chế cấu hình tự động isatap(intra-site automatic tunnel addressing protocol)

ISATAP tạm dịch là "giao thức đánh địa chỉ đường hầm tự động trong site", là cơ chế chuyển đổi tương tự như đường hầm 6to4, cho phép việc triển khai từ các node IPv6 trong mạng IPv4 đã có. Nhưng trong cơ chế này có ít nhất một đầu cuối là trạm (ví dụ như máy tính).

Đường hầm ISATAP có sẵn cho việc sử dụng thông qua các mang trường sở (campus) hoặc cho việc chuyển đổi các site cục bộ. ISATAP cung cấp việc định tuyến IPv6 trong cả hai miền định tuyến IPv6 site-local và global và đường hầm tự động qua các vị trí của mạng IPv4 của một site mà không cần sự hỗ trợ của bất kỳ mạng IPv6 gốc nào.

ISATAP cung cấp các tính năng sau:

- Cho phép triển khai các host IPv6 trong các site IPv4 mà không cần mở rộng tại gateway biển. Như vậy nó có các kiểu cấu hình: trạm đến trạm, trạm đến router, router đến trạm.

- Hỗ trợ cả hai kiểu cấu hình. địa chỉ: kiểu không trạng thái và kiểu bằng tay.

- Hỗ trợ các mạng riêng (private) IPv4 và mạng toàn cục (global) IPv4.

Truyền các gói tin IPv6 thông qua các liên kết ISATAP:

Các liên kết ISATAP truyền gói tin IPv6 thông qua đường hầm tự động bằng việc sử dụng cấu trúc IPv4 như là một tầng liên kết, gói tin IPv6 được bao bọc tự động trong gói tin IPv4.

Cấu trúc của bộ nhận dạng giao tiếp ISATAP:

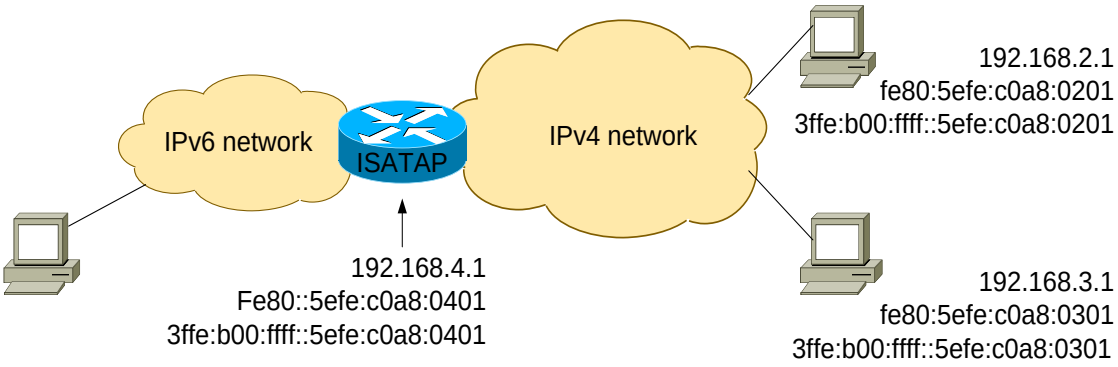
Việc tạo địa chỉ ISATAP tuân theo một quy trình nhất đinh, đầu tiên bộ nhận dạng giao tiếp ISATAP được tạo ra bằng việc sử dụng địa chỉ IPv4 dạng:

::0:5EFE:32bit IPv4 (32bit IPv4 được chuyển hệ số 16), bộ nhận dạng giao tiếp này là duy nhất một cách cục bộ, nó sử dụng để tạo ra địa chỉ ISATAP link-local và với địa chỉ đó nó có thể truyền tin với router ISATAP, ISATAP sử dụng một tiền tố mạng 64 bit để từ đó các địa chỉ ISATAP được tạo ra. Bộ nhận dạng giao tiếp 64 bit được tạo ra bởi việc kết hợp 0000:5EFE và địa chỉ IPv4 của nút Dual Stack.

Ví dụ:

3FFE:0B00:0C18:0001:0:5EFE.192.168.99.1 là địa chỉ ISATAP

Bởi vì đường hầm ISATAP chỉ xảy ra trong các đường biên của site, do vậy địa chỉ embeded IPv4 không cần là global. Hình sau chỉ ra một ví dụ về cơ chế đường hầm ISATAP:



Hình 2. 7: Đường hầm ISATAP

Như vậy mỗi node sẽ có một địa chỉ IPv4 và một (vài) địa chỉ IPv6 tương ứng với IPv4 được nhúng vào 32 bit sau cùng.

Địa chỉ tự cấu hình không trạng thái và Link-local

Các địa chỉ ISATAP là các địa chỉ unicast, sử dụng bộ nhận dạng giao tiếp như sau:

Tiền tố link-local, site-local hoặc global unicast	0000:5EFE	Địa chỉ IPv4 của liên kết ISATAP

Hình 2. 8: Dạng địa chỉ ISATAP

Các địa chỉ ISATAP: Link-local, site-local, and global được tạo ra một cách chính xác (ví dụ bằng việc tự cấu hình hoặc cấu hình bằng tay). Ví dụ: 3FFE:lA05:510:1111:0:5EFE:8CAD:8108 có một tiền tố

3FFE:1 a05:510:1111::/64 và bộ nhận dạng giao tiếp ISATAP là địa chỉ IPv4 nhúng: “140.173.129.8”. Địa chỉ trên có thể viết cách khác là:

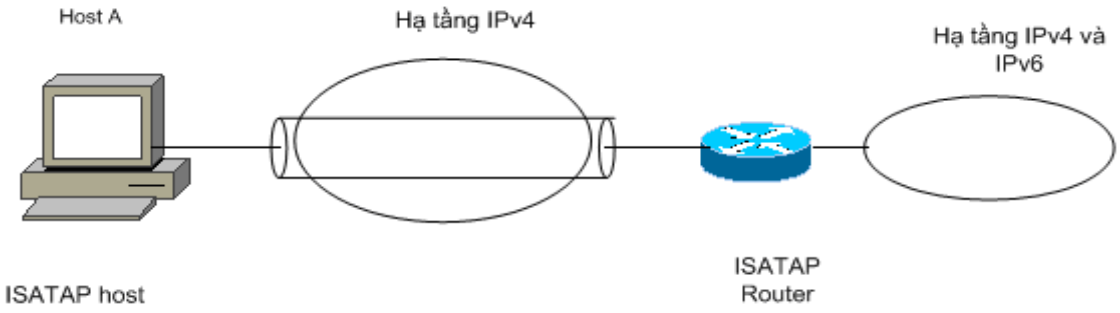
3FFE:1A05:510:1111:0:5EFE:140.173.129.8. Và địa chỉ ISATAP Link Local và Site local tương ứng:

FE80::0:5EFE:140.173.129.8 (10 bit đầu tiên là 1111111010) FEC0::1111:0:5EFE:140.173.129.8 (10 bít đầu tiên là 1111111011 và 16 bít định danh mạng con là 1111 1111 1111 1111 dạng nhị phân).

Router ISATAP

Việc sử dụng địa chỉ link-local ISATAP cho phép các host IPv6/IPv4 truyền tin với nhau trên cùng một mạng con IPv4, nhưng không truyền tin được với các địa

chỉ nằm trên mạng con (subnet) khác. Để truyền tin được ra bên ngoài mạng con thì sử dụng địa chỉ global. Các host sử dụng địa chỉ ISATAP phải định đường hầm các gói tin từ router ISATAP. Cấu hình này được mô tả như hình sau:



Hình 2. 9: ISATAP Router

Một router ISATAP là một router IPv6 thực hiện các chức năng sau:

Chuyển các gói tin giữa các host ISATAP trên một mạng con logic (một mạng IPv4) và các host trên cùng mạng con khác. Các mạng con khác có thể là mạng IPv4 hoặc mạng con trong một miền (domain) IPv6.

Hoạt động như một router mặc định củ các host ISATAP.

Quảng bá tiền tố địa chỉ để nhận dạng mạng con logic trên các host ISATAP mà chúng đang thuộc về. Các host ISATAP sử dụng tiền tố địa chỉ đã quảng bá để cấu hình địa chỉ global ISATAP.

Cách thức hoạt động của ISATAP:

ISATAP là duy nhất trong cách nó xử lý router và tìm kiếm hàng xóm (Neighbor Discovery). Việc khám phá router ban đầu được thực hiện thông qua tên (name lookup). Lúc một giao tiếp ISATAP của nút ISATAP khởi động, nó sẽ thực hiện tra tên "ISATAP". Điều này sẽ phân giải địa chỉ của tất cả router ISATAP trong AS (Autonomous System: vùng tự trị). Quy trình này gọi là Potential Router List (PRL). Nút (node) ISATAP lúc đó sẽ gửi một bản tin liên kết Router (Router Soicitation) tới địa chỉ link-local ISATAP cho mỗi router trong PRL. Lúc truyền tin xảy ra giữa hai nút ISATAP, một nút sẽ biết rằng đích là một nút ISATAP dựa vaog bộ nhận dạng giao tiếp. Dựa trên tiền tô, nếu địa chỉ đích là nằm trong AS thì gói tin IPv6 sẽ được bao bọc trong một gói tin IPv4 và địa chỉ đích IPv4 sẽ xuất phát từ địa

chỉ IPv4 được nhúng vào trong địa chỉ đích IPv6 ISATAP. Nếu địa chỉ đích thuộc AS, gói tin IPv6 sẽ vẫn được bọc trong IPv4 và đích là một router ISATAP mặc định dùng cho việc chuyển tiếp gói tin, sau này cũng đúng cho các gói tin được chuyển tới đích mà không phải là ISATAP.

Ưu điểm của ISATAP:

Cung cấp việc triển khai dần dần IPv6 để từng bước lấp đầy các nút IPv6 trong AS. Nó được hỗ trợ trên bất cứ nền tảng nào, làm việc với không gian địa chỉ riêng của IPv4.

Nhược điểm của ISATAP:

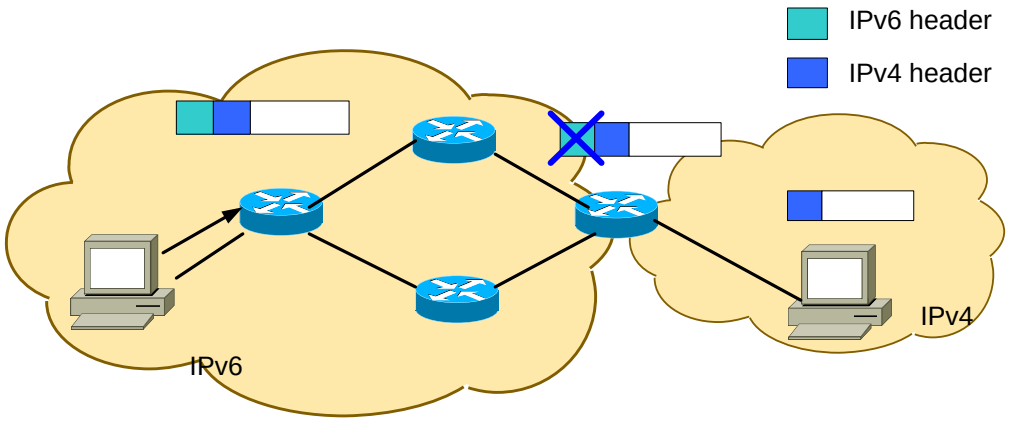
Yêu cầu nhiều quy trình hơn các phương pháp khác, hiện tại không phải là một chuẩn chính thức, một vài vấn đề bảo mật liên quan đến việc sử dụng router ISATAP bởi các nút không mong muốn (undesirable).

2.4. Cơ chế dịch địa chỉ (address translation)

Trên đây đã nghiến cứu các phương pháp chuyển đổi từ IPv4 sang IPv6 bằng các đường hầm tự động và cấu hình bằng tay, các phương pháp trên được sử dụng trong trường hợp các trạm (host hoặc router) IPv6 phải kết nối với nhau thông qua mang IPv4. Riêng cơ chế dịch địa chỉ lại thực hiện việc chuyển đổi giữa hai mạng nằm kề nhau và thực hiện truyền tin giữa host chỉ có IPv4 và các host chỉ có IPv6. Sau đây là một số chuyển đổi thông dụng cho loại này.

+ Dstm (dual stack transition mechanism):

DSTM là "cơ chế chuyển đổi chồng giao thức", dựa vào việc sử dụng các đường hầm IPv4 qua IPv6 để mang lưu lượng trong một mạng IPv6 và cung cấp một phương pháp để cấp phát một địa chỉ IPv4 tạm thời tới các nút có khả năng hỗ trợ cả IPv4 và IPv6 (nút IPv4/IPv6), DSTM cũng đồng thời là một cách để tránh việc sử dụng NAT trong việc truyền tin với các nút và các ứng dụng IPv4.



Hình 2.10: Mô hình hoạt động của DSTM

a. Cấu trúc một dstm:

Máy chủ DSTM (DSTM Server):

Cấp phát địa chỉ IPv4 trong mạng IPv6 cho các máy khách (client).

Máy khách DSTM (DSTM Client):

Là chương trình chạy trên máy khách mà nó yêu cầu địa chỉ IPv4 từ máy chủ DSTM .

Gateway (Tunnel End Point - TEP):

Đây là điểm cuối đường hầm thực hiện công việc mã hóa/ giải mã gói tin.

DSTM Host:

Hỗ trợ IPv4/IPv6.

Yêu cầu và tự cấu hình địa chỉ IPv4.

Thiết lập đường hầm 4over6 về phía TEP.

b. Hoạt động của các nút DSTM:

Cách xác định lúc nào thì cần một địa chỉ IPv4:

IPv4 là kết quả của một truy vấn DNS (DNS Query)

Một ứng dụng mở một cổng IPv4.

Cách để cấu hình IPv4:

Yêu cầu một địa chỉ/cổng IPv4 từ DSTM Server

Cấu hình giao tiếp 4over6 với giá trị IPv4 vừa nhận được.

Chuyển tất cả lưu lượng IPv4 tới giao tiếp 4over6

Cách nút biết được địa chỉ TEP:

Cấu hình tĩnh.

Học từ gói tin trả lời DNS (DNS Answer) của máy phục vụ DNS.

c. Hoạt động của DSTM TEP:

Cách nó được cấu hình:

Cấu hình bằng tay (không được khuyến nghị)

Thông qua máy chủ DSTM

Cấu hình động.

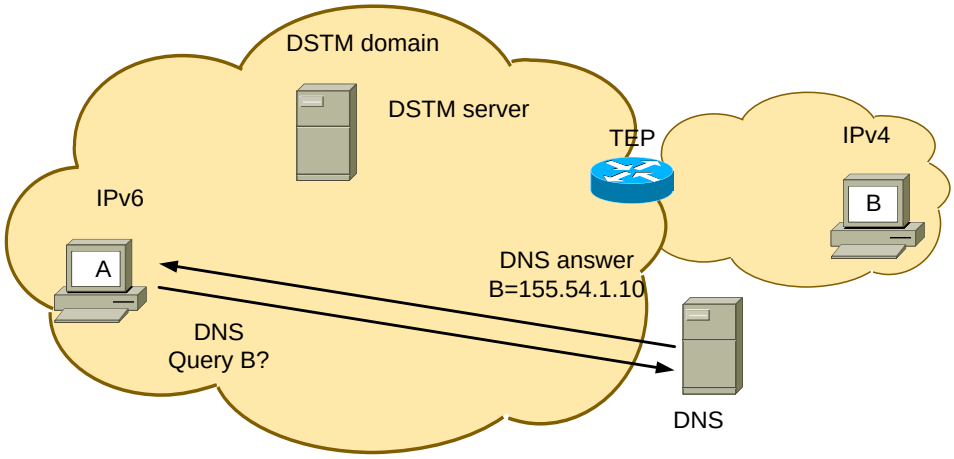
DSTM TEP cấu hình việc ánh xạ IPv4 và IPv6 và cổng

d. Hoạt động của máy chủ DSTM:

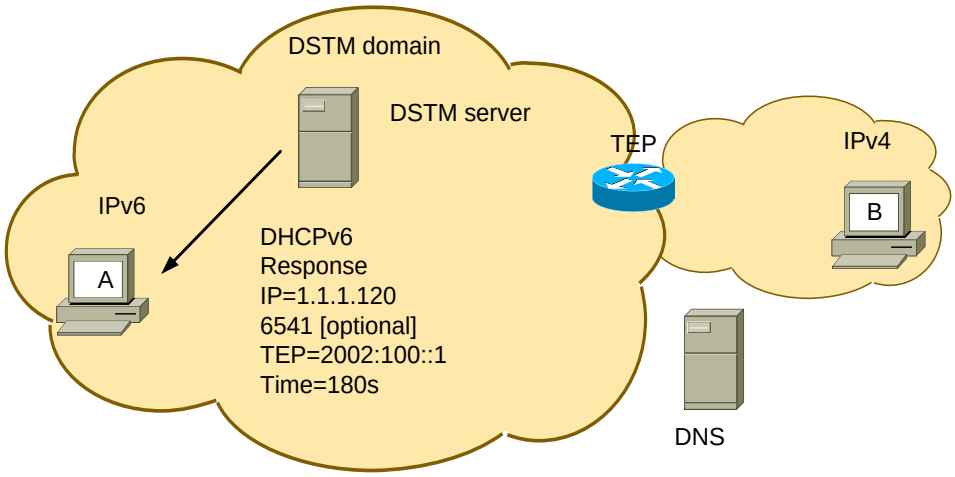
Sau khi nhận được gói tin truy vấn thì máy chủ DSTM trả lại với các tham số (IPv4, cổng, TEP, khoảng thời gian (Duration)) và lưu giữ bản ánh xạ giữa IPv4 và IPv6.

Sau đây là một ví dụ điển hình về việc truyền tin giữa một Host A (thuộc mạng IPv6) và host B (thuộc mạng IPv4):

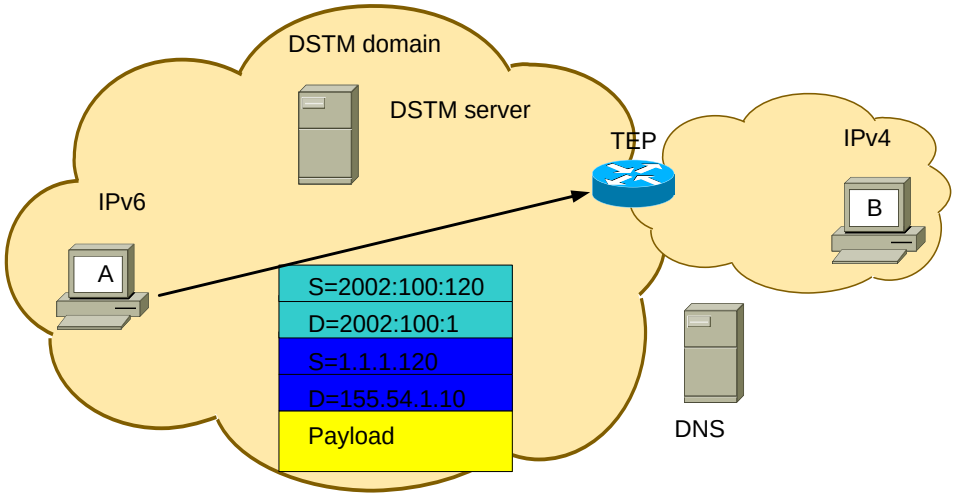
A bắt đầu truyền tin với B:



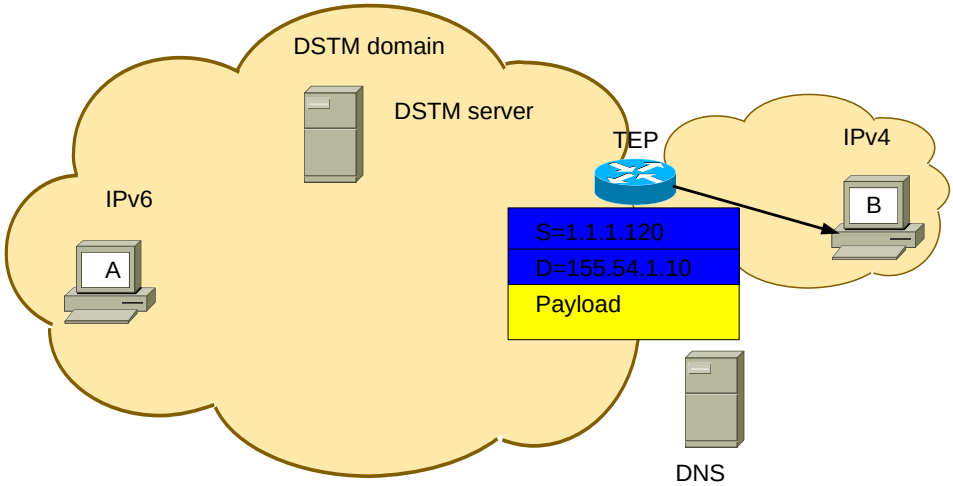
Hình 2. 11: A sẽ yêu cầu DNS cho các tham số về B, DNS sẽ trả lời với một địa chỉ IPv4 của B (155.54.1.10)



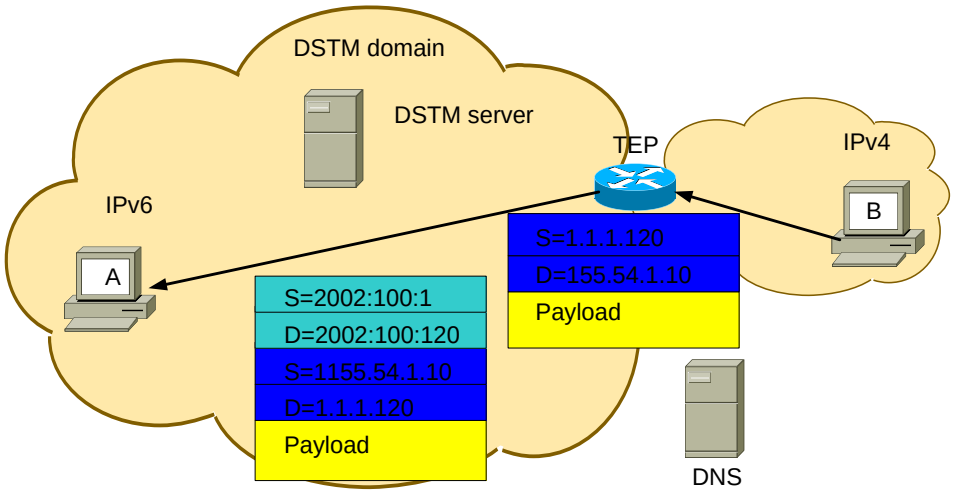
Hình 2. 12: Bản ghi DNS của IPv4 sẽ khởi động yêu cầu DHCP



Hình 2. 13: Gói tin IPv4 sẽ gửi thông qua 4over6 về phía TEP



Hình 2. 14: TEP tách gói tin và gửi nó như bình thường



Hình 2. 15: Lúc đó TEP đã lưu giữ việc ánh xạ và việc định tuyến ngược lại là dễ dàng

e. Ưu điểm của DSTM:

Trong suốt với mạng: Bởi gói tin IPv4 đã được bao bọc trong IPv6, không cần yêu cầu định tuyến.

Trong suốt với ứng dụng: Không cần sự thay đổi nào đến ứng dụng.

DHCPv6 cho phép cấp phát động địa chỉ IPv4.

Dựa vào giao thức chuẩn.

Dễ quản lý.

d. Nhược điểm của DSTM:

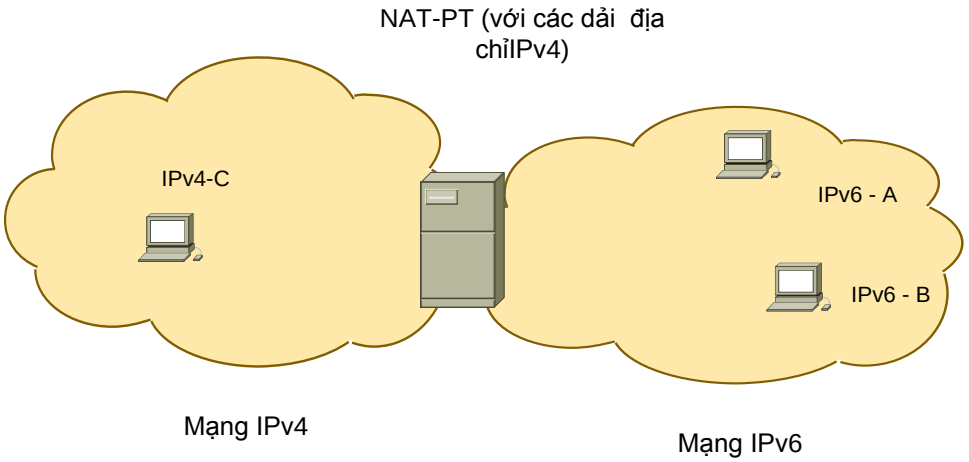
Không hỗ trợ đường truyền đối xứng.

Trễ ban đầu có thể lớn.

2.5. Biên dịch NAT-PT (netwokr address translation - otocol translation)

NAT-PT là cơ chế "chuyển đổi địa chỉ mạng –chuyển đổi giao thức mạng", mô tả một bộ chuyển đổi IPv6/IPv4, NAT-PT cho phép các host thuần IPv6 (tức là chỉ nằm trong mang IPv6) và truyền tin với các host thuần IPv4 và ngược lại. Một thiết bị NAT-PT đặt tại biên của mạng IPv4 và IPv6, mội thiết bị NAT-PT chiếm một vùng địa chỉ global IPv4 có khả năng định tuyến, dùng để gán tới các nút IPv6 một cách động. Ngoài việc chuyển đổi địa chỉ thì cũng thực hiện chuyển đổi mào đầu. Nếu có khác biệt về địa chỉ: Dịch địa chỉ IPv4-IPv6, nếu khác biệt về phần mào đầu: Dịch giao thức thay đổi mào đầu gói tin.

Thiết bị NAT-PT được cài đặt tại biên giữa mạng IPv4 với IPv6, cơ chế này không đòi hỏi các cấu hình đặc biệt tại các máy trạm và sự chuyển đổi gói tin tại thiết bị NAT-PT hoàn toàn trong suốt với người dùng.



Hình 2. 16: NAT-PT

Mỗi thiết bị duy trì một tập các địa chỉ IPv4 dùng để ánh xạ các yêu cầu địa chỉ IPv6.

NAT-PT có thể mở rộng thành NAPT-PT tức là thêm khả năng dịch số hiệu cổng. NAPT-PT cho phép sử dụng một địa chỉ IPv4 cho nhiều phiên làm việc khác nhau.

NAT-PT cũng NAT trong IPv4 không có khả năng hoạt động với các gói tin có chứa địa chỉ trong phần tải tin, do đó NAT-PT đi kèm với cơ chế cổng tầng ứng dụng ALG (Application Layer Gateway), cơ chế này cho phép xử lý các gói tin ứng với từng dịch vụ nhất định như DNS hay FTP, ...

2.5.1. Hoạt động của NAT-PT

Hình 2.16: trong đó IPv6-A có địa chỉ FEDC:BA98::7654:3210, IPv6-B có địa chỉ FEDC:BA98::7654:3211 và IPv4-C có địa chỉ 132.146.243.30. và giả sử NAT-PT có vùng địa chỉ IPv4 là 120.130.26.0/24. Các địa chỉ trong vùng địa chỉ có thể cấp phát theo kiểu 1-1 tới các địa chỉ IPv6 trong trường hợp số địa chỉ IPv6 nhỏ hơn hoặc bằng số địa chỉ IPv4, trong trường hợp sau đây giả sử mạng IPv6 có

số nút nhiều hơn so với vùng IPv4 vì vậy mà cần cơ chế cấp phát động. Khi nút IPv6-A truyền tin với nút IPv4-C thì nút A tạo ra một gói tin với:

Địa chỉ nguồn: FEDC:BA98:7654:3210

Địa chỉ đích: Prefix::132.146.243.30

Chú ý rằng Prefix::/96 được quảng bá trong miền cụt (stub domain) bởi NAT-PT và các gói tin được đưa đến Prefix (phần tiếp đầu) này sẽ được định tuyến tới NAT-PT, Prefix được cấu hình trước chỉ cần có khả năng định tuyến trong miền cụt và vì vậy nó có thể là bất cứ Prefix nào có khả năng định tuyến mà nhà quản lý mạng chọn.

Nếu gói tin là một gói khởi đầu phiên, NAT-PT sẽ gán cho gói tin một địa chỉ IPv4 trong vùng cấp phát của nó (ví dụ 120.130.26.10/24 như trên), các tham số chuyển đổi sẽ được nhớ lại trong khoảng thời gian của phiên.

Gói tin IPv4 sau đó có địa chỉ nguồn 120.130.26.10 và địa chỉ đích 132.146.243.30. NAT-PT sẽ giữ lại trạng thái ánh xạ giữa 120.130.26.10 và FEDC:BA98::7654:3210 cho việc truyền tin tiếp theo trong cùng phiên đó cho đến khi kết thúc phiên.

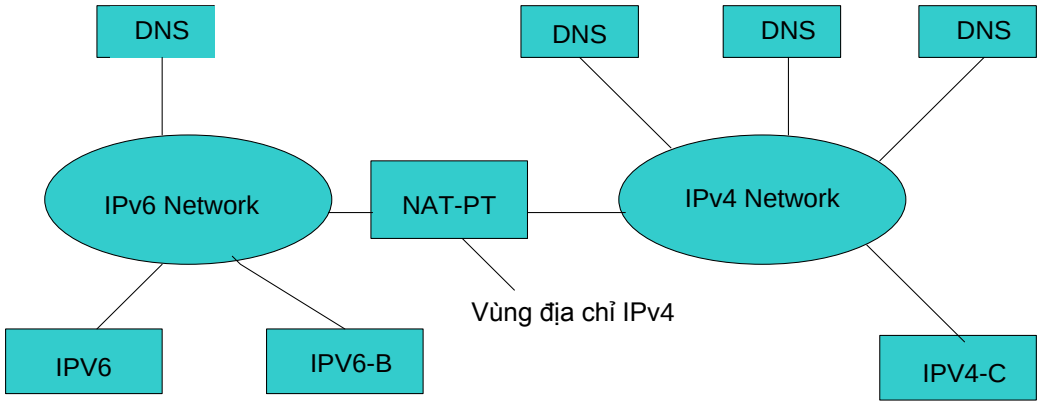
Bất kỳ lưu lượng nào quay ngược lại từ IPv4 sang IPv6 thuộc về cùng một phiên sẽ được nhận ra bởi NAT-PT. NAT-PT sẽ sử dụng thông tin trạng thái để chuyển gói tin, lúc này địa chỉ nguồn là 132.146.243.30 và địa chỉ đích là 120.130.26.10 (phía IPv4), NAT-PT sẽ thay đổi địa chỉ nguồn thành Prefix:132.146.243.30 và địa chỉ đích là FEDC:BA98::7654:3210 (node IPv6-A). Chú ý rằng gói tin này bây giờ có thể được chuyển trong các mạng chỉ IPv6 như bình thường.

2.5.2. Sử dụng DNS cho việc gán địa chỉ:

Một địa chỉ IPv4 gán bởi NAT-PT tới mỗi nút IPv6 lúc NAT-PT nhận dạng điểm bắt đầu của phiên inbound (đi vào) hay outbound (đi ra ngoài), việc nhận dạng điểm bắt đầu của của một phiên inbound mới được thực hiện khác so với outbound. Tuy nhiên vùng địa chỉ IPv4 được sử dụng cho việc gần các node IPv6 không liên quan đến việc một phiên outbound khởi đầu từ một nút IPv6 hay inbound khởi đầu từ một nút IPv4.

Việc ánh xạ tên sang địa chỉ của IPv4 được lưu giữ trong DNS Server (máy phục vụ DNS) với các bản ghi A. Còn việc ánh xạ từ tên sang địa chỉ của IPv6 trong một DNS Server với bản ghi AAAA (A6).

Gán địa chỉ cho các kết nối đầu vào (IPv4 sang IPv6)



Hình 2. 17: Truyền tin IPv6 đến IPv4

Nút IPv6-A địa chỉ IPv6 -> FEDC:BA98::7654:3210

Nút IPv6-B có địa chỉ IPv6 -> FEDC:BA98::7654:3211

Nút IPv4-C có địa chỉ IPv4 -> 132.146.243.30

NAT-PT có một vùng địa chỉ bao gồm mạng con IPv4: 120.130.26.0/24

Theo hình trên lúc bộ phân giải tên của IPv4-C gửi một yêu cầu tìm kiếm (lookup) cho nút A, yêu cầu lookup được đưa đến máy phục vụ DNS (DNS server) trên mạng IPv6 thông qua router NAT-PT vì DNS bên mạng IPv4 không tìm thấy nút. DNS-ALG trên thiết bị NAT-PT sẽ điều chỉnh các câu hỏi DNS cho bản ghi A đi vào miền IPv6 để thực hiện phân giải từ địa chỉ nút thành tên nút (và ngược lại) và ngược lại DNS-ALG sẽ chuyện các câu hỏi cho bạn ghi AAAA (A6) từ miền IPv6 sang miền IPv4 (Chú ý rằng gửi tin DNS TCP/UDP được nhận dạng bởi số cổng nguồn và cổng đích là 53).

Ví dụ node IPv4-C muốn bắt đầu một phiền với node IPv6-A thì nó thực hiện một sự tra tên (bản ghi A) cho nut A, yêu cầu này sẽ được chuyện tới DNS vùng (miền IPv4) và từ đó nó được chuyển qua DNS server của miền IPv6, DNS-ALG sẽ dịch yêu cầu A thành yêu cầu AAAA (hoặc A6) và sẽ chuyển qua máy phục vụ DNS trong miền IPv6:

Nút A AAAA FEDC:BA98::7654:3210

Sau đó địa chỉ này lại được chuyển quay lại máy phục vụ DNS (của IPv6) và được dịch ra bởi DNS-ALG như sau:

Nút A 120.130.26.1

DNS-ALG sẽ gửi lại việc ánh xạ FEDC:BA98::7654:3210 và 120.130.26.1 trong NAT-PT, bản ghi lúc đó sẽ chuyển tới node IPv4-C. Bây giờ C có thể bắt đầu một phiên làm việc như sau:

Địa chỉ nguồn: 132.146.243.30, cổng TCP nguồn: 1025 và

Địa chỉ đích: 120.130.26.1, cổng TCP đích: 80

Gói tin sẽ được chuyển tới NAT-PT, NAT-PT đã giữ ánh xạ giữa FEDC:BA98::7654:3210 và 120.130.26.1 do đó có thể chuyển gói tin với tham số:

Địa chỉ nguồn: Prefix::132.146.243.30, cổng TCP nguồn: 1025

Địa chỉ đích: FEDC:BA98::7654:3210, cổng TCP đích: 80

Và việc truyền tin bây giờ sẽ diễn ra bình thường.

2.5.3. Gán địa chỉ cho các kết nối đầu ra (IPv6 sang IPv4)

Việc truyền tin từ IPv6 sang IPv4 cũng được thực hiện thông qua máy phục vụ DNS ở mỗi miền (domain), nút A sẽ thực hiện tra bảng (lookup) nút C thông qua máy phục vụ DNS của IPv6, yêu cầu này sẽ được chuyển tới NAT-ALG ở router NAT-PT và chuyển sang máy phục vụ DNS của IPv4. Máy phục vụ DNS ở IPv4 sẽ trả lời yêu cầu và chuyển tới NAT-ALG, lúc này NAT-ALG sẽ thêm tiền tố (Prefix) vào địa chỉ IPv4 để thành địa chỉ IPv6 và chuyển địa chỉ này tới nút A. Bây giờ nút A có thể sử dụng IP này như bất kỳ IP bình thường nào khác.

2.5.4. Ưu điểm của nat-pt

Quản trị tập trung tại thiết bị NAT-PT.

Có thể triển khai nhiều thiết bị NAT-PT để tăng hiệu nặng hoạt động.

2.5.5. Nhược điểm của NAT-PT

Tạo nên một điểm gây lỗi tại thiết bị NAT-PT nếu việc truyền tin là quá lớn.

Sự thiếu hụt bảo mật đầu cuối tới đầu cuối (end-to-end), do IPv6 hỗ trợ IPsec những IPv4 không hỗ trợ, vì vậy không dùng IPSEc trong trường hợp này.

2.5.6. Phạm vi ứng dụng

NAT-PT được ứng dụng tại dải biên của mạng chỉ có các host IPv6 và mạng chỉ có các host IPv4.

Theo dạng đơn giản nếu NAT-PT không hỗ trợ NAT-ALG, sẽ cung cấp một sự truyền tin giữa mạng IPv6 và mạng IPv4 với chỉ các phiên khởi đầu tại các nút trong miền IPv6. Trong khi đó các phiên được khởi đầu tại miền IPv4 sẽ bị đánh rơi.

NAT-PT kết nối với NAT-ALG sẽ cho khả năng truyền tin hai hướng với việc khởi đầu phiên ở IPv4 hoặc IPv6.

2.6. Kết luận Chương 2

Trong chương này đã giới thiệu một số cơ chế chuyển đổi ứng với từng nút mạng: Tunnel; Translation; Dual Stack, biên dịch NAT-PT; phân tích ưu nhược điểm của các cơ chế chuyển đổi; phương pháp gán địa chỉ và gán cấu hình tự động trong quá trình chuyển đổi từ IPv4 - IPv6.

CHƯƠNG 3: CHUYỂN ĐỔI IPV4 – IPV6 TRONG MẠNG KHÁCH HÀNG VNPT HẢI DƯƠNG

3.1. Chuyển đổi IPv4 – IPv6 trong mạng băng rộng vnpt

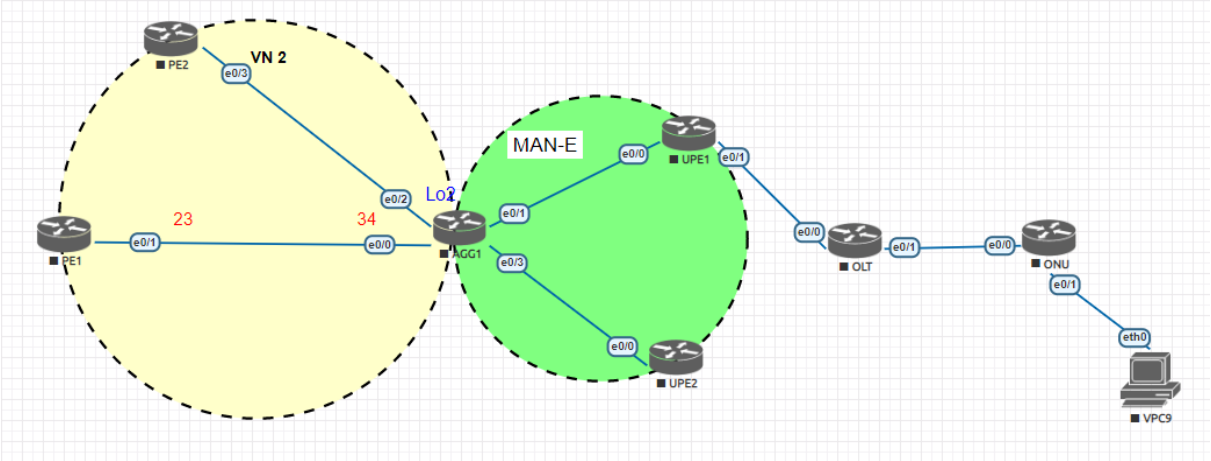
3.1.1 Mô hình cung cấp dịch vụ internet tại vnpt hải dương.

VNPT Hải Dương là đơn vị trực thuộc tập đoàn VNPT, cung cấp các dịch vụ của VNPT tại địa bàn Hải Dương, theo chủ trương phát triển của tập đoàn hiện tại VNPT Hải Dương đã quang hóa tất cả đường truyền Internet đến nhà khách hàng, hoàn thành mục tiêu 100% k/h của VNPT sử dụng các gói FTTH.

VNPT Hải Dương có 37 thiết bị UPE, 3 thiết bị AGG tạo thành các ring MAN-E nội tỉnh dung lượng các ring từ 30G đến 50G. 3 AGG có 500G kết nối đến 5 BRAS thuộc miền VN2 của Core VNPT, cùng hệ thống mạng quang truy nhập nội tỉnh, VNPT Hải Dương đã triển khai cung cấp dịch vụ Fiber đến gần 140.000 khách hàng bằng hệ thống GPON.

Lưu lượng Internet từ các BRAS thông qua hệ chuyển mạch nhãn MPLS trong miền MAN-E sẽ đến các UPE, các OLT GPON kết nối đến UPE bằng các giao diện 1G hoặc 10G, mỗi UPE được quy hoạch một VLAN riêng cho Internet để thuận lợi cho quá trinh khai thác và xử lý lỗi. Thông qua mạng quang thụ động, các ONU kết nối về OLT, ONU sử dụng đồng nhất VLAN 11 để truyền tải kết nối OLT – ONU. Các ONU sử dụng phương pháp PPPOE xác thực với lớp trên để nhận IP từ BRAS và áp các giới hạn lưu lượng theo gói đã đăng ký.

ONU VNPT Hải Dương sử dụng chủ yếu là ONU Igate do VNPT Technology sản xuất, Router này có cấu hình manh, đáp ứng được IPv6 – IPv4 Dual – stack.

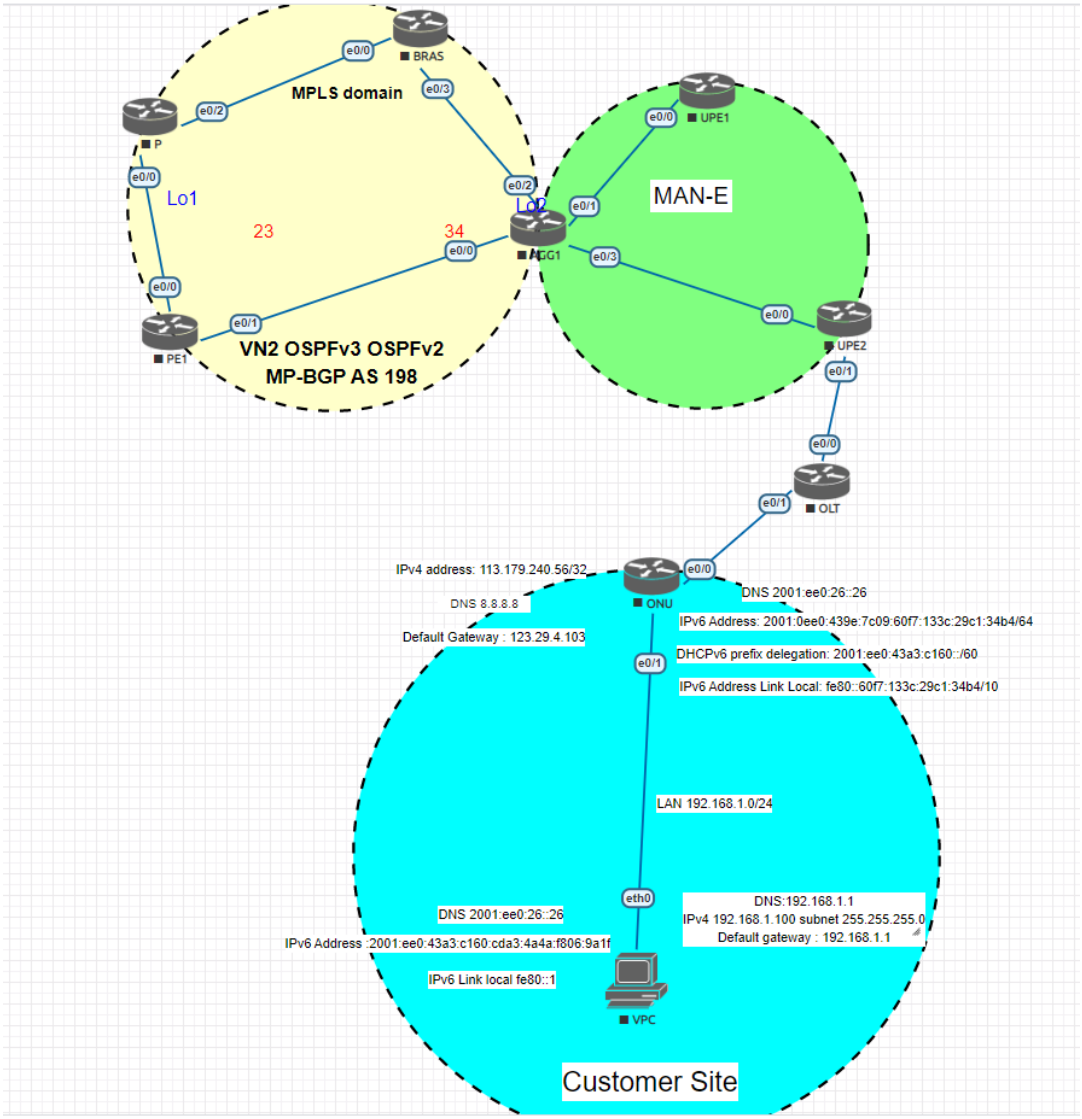


Hình 3. 1: Mô hình cung cấp dịch vụ Internet VNPT hải Dương.

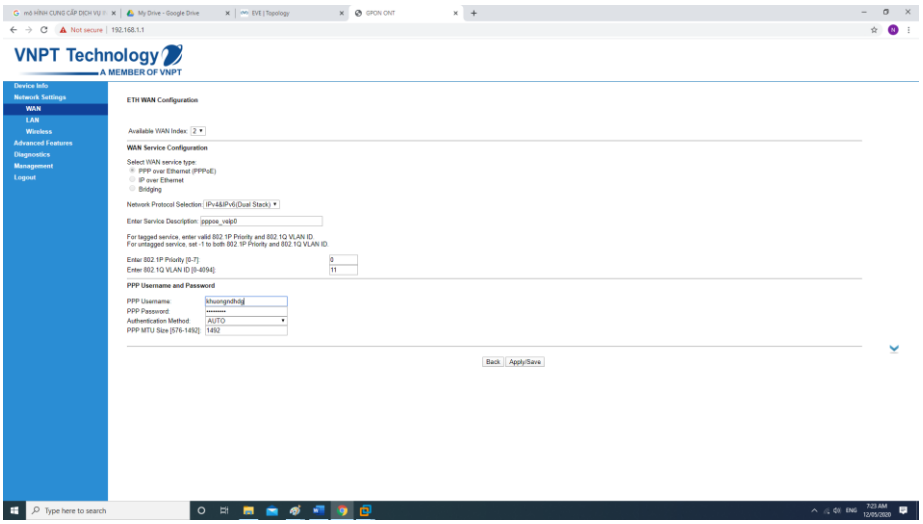
Với tập khách hàng ngày càng mở rộng và yêu cầu cao về chất lượng dịch vụ, cùng su hướng phát triển của Internet toàn cầu, VNPT nói chung và VNPT Hải Dương nói riêng định hướng triển khai IPv6 đến tất cả khách hàng, phương thức cung cấp là IPv6 – IPv4 Dual – Stack.

3.1.2 Phương án cung cấp IPv6 – IPv4 dual – stack đến khách hàng

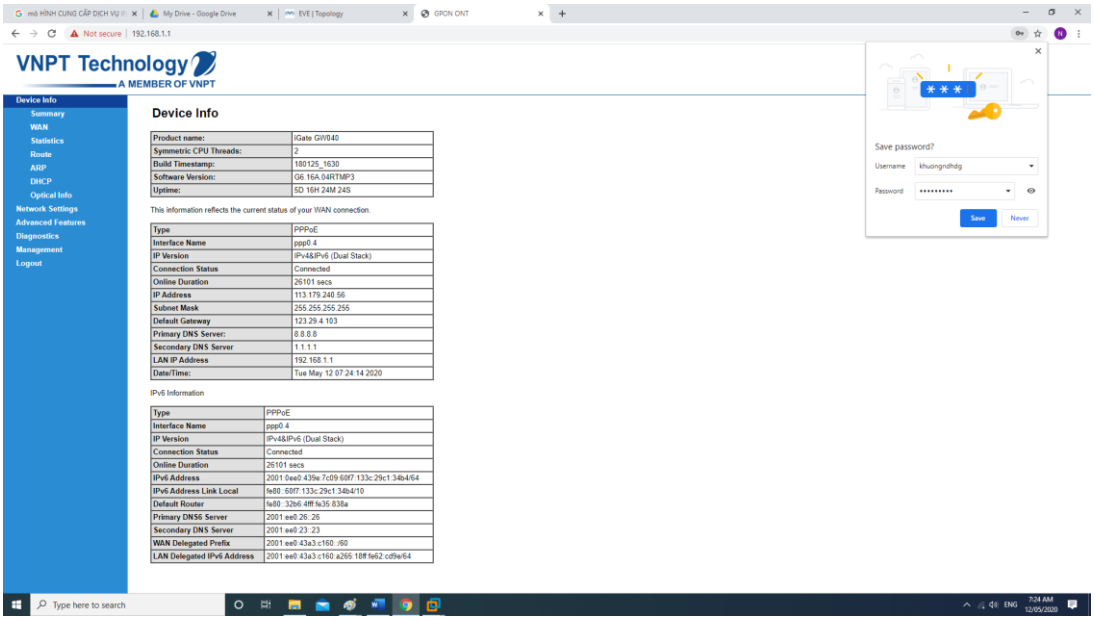
Áp dụng các phương pháp định tuyến như trong mô phỏng, IPv6 và OSPFv3, IPv4 và bật OSPFv2, kết hợp với DHCPv6 tại các BRAS, hiện tại VNPT Hải Dương đã cung cấp thành công đến mỗi ONU một IPv6/60. Các thiết bị kết nối trực tiếp với ONU được cấp một IPv6/64.



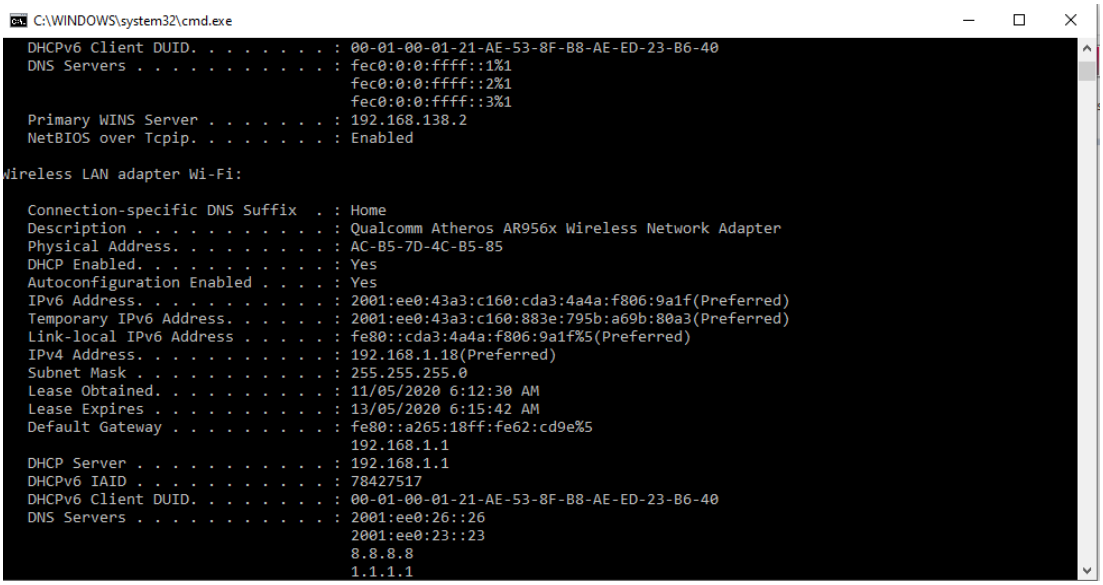
Hình 3. 2: Mô hình cung cấp IPv6-IPv4 Dual Stack tại VNPT Hải Dương.



Hình 3. 3: Cấu hình thiết bị đầu cuối để triển khai IPv6- IPv4 Dual – Stack

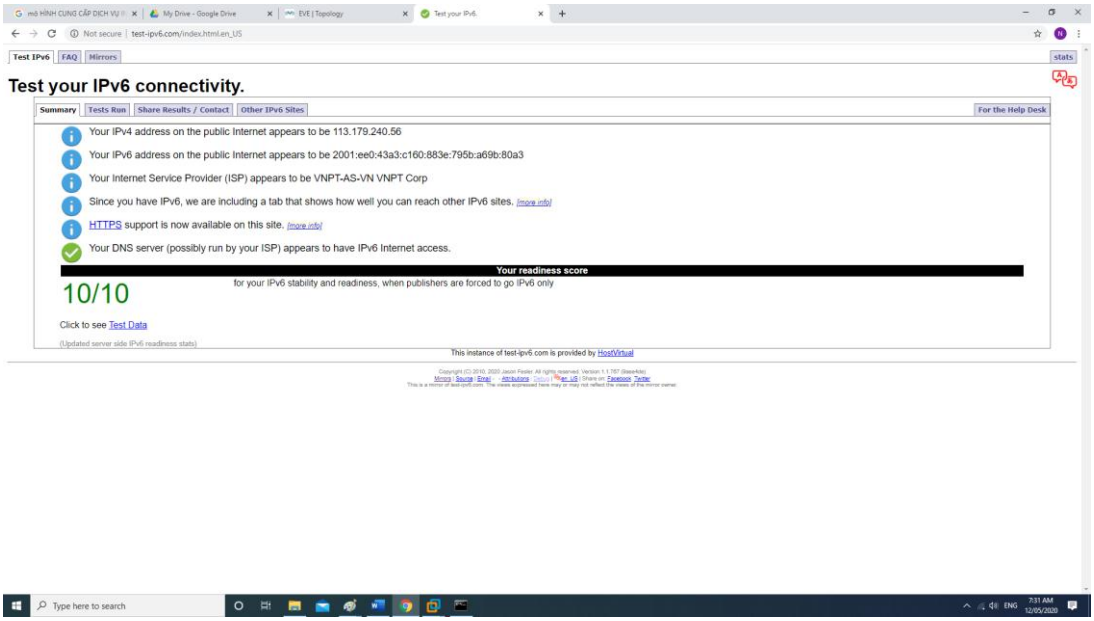


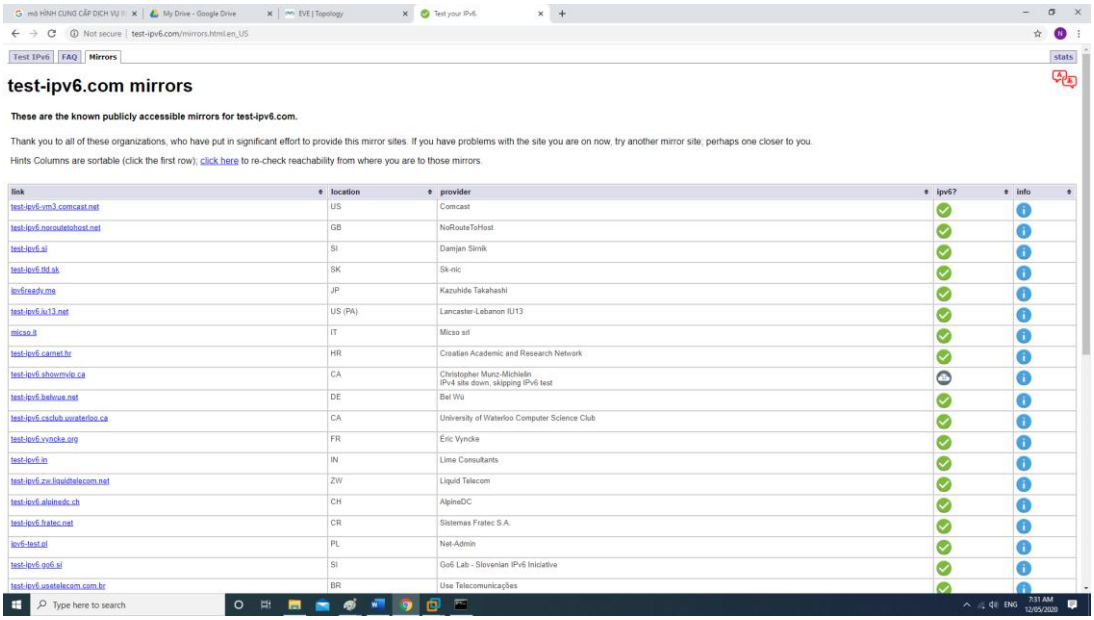
Hình 3. 4: Các địa chỉ IP cấp cho ONU chạy IPv6- IPv4 Dual – Stack



Hình 3. 5: IPv6- IPv4 Dual – Stack tại các PC của khách hàng.

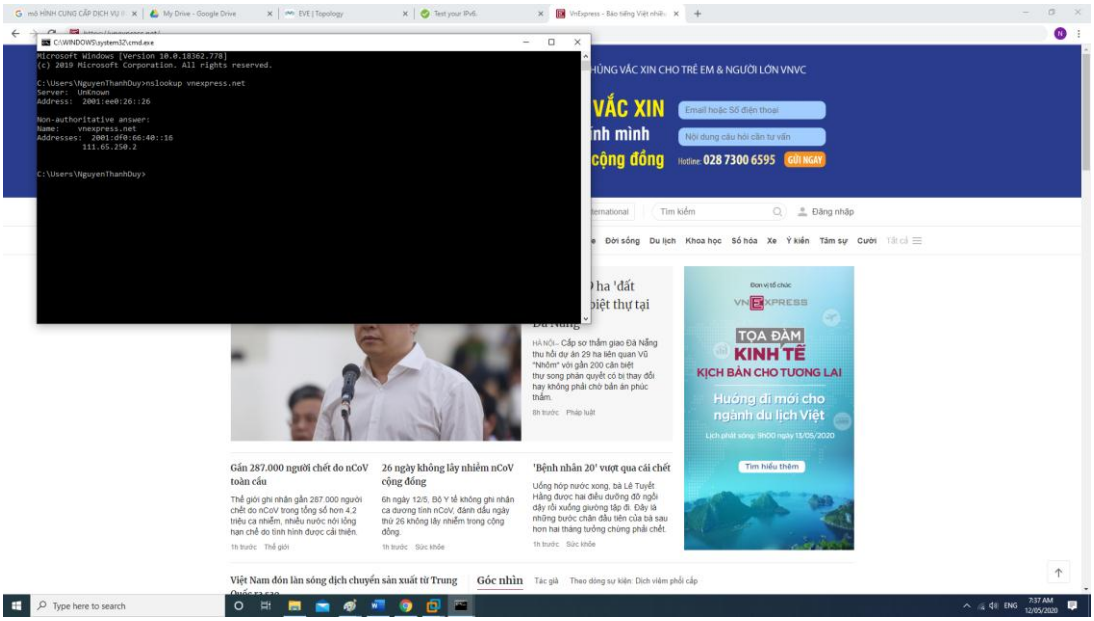
Sau khi chuyển đổi IPv6- IPv4 Dual – Stack đến k/h, kiểm tra kết nối IPv6 và IPv4 đến các server trong và ngoài nước.



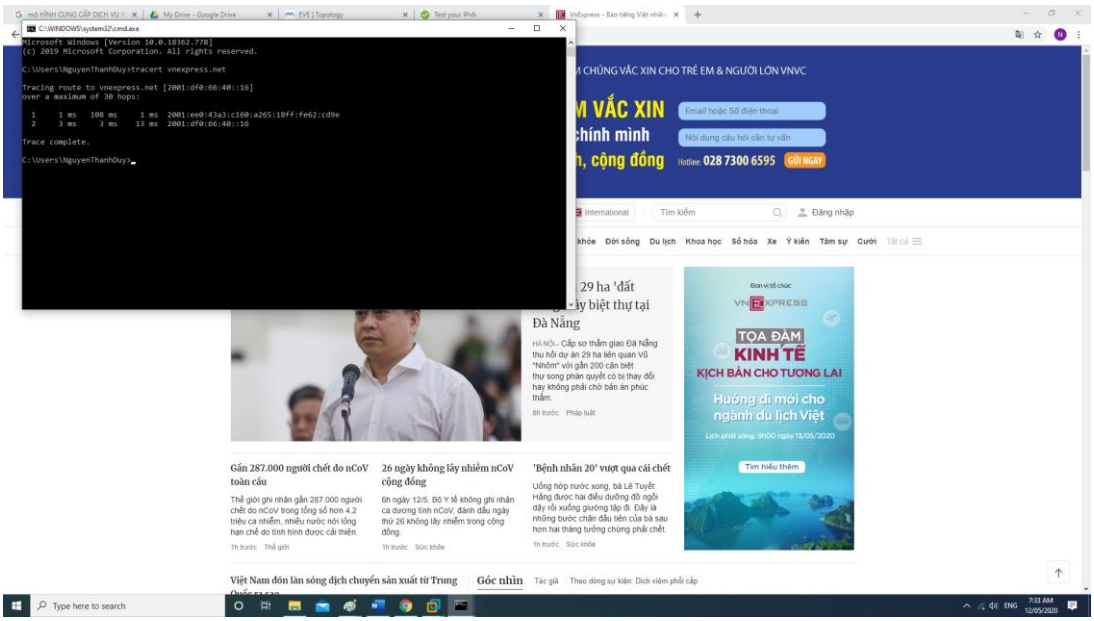


Hình 3. 6: Kiểm tra kết nối IPv6 IPv4 đến các điểm test trong và ngoài nước.

Đối với các điểm đầu xa cùng sử dụng IPv6- IPv4 Dual – Stack (VD: https://vnexpress.net/) Kiểm tra từ PC đã ưu tiên sử dụng các kết nối IPv6.



Hình 3. 7: Host đầu xa sử dụng IPv6- IPv4 Dual – Stack

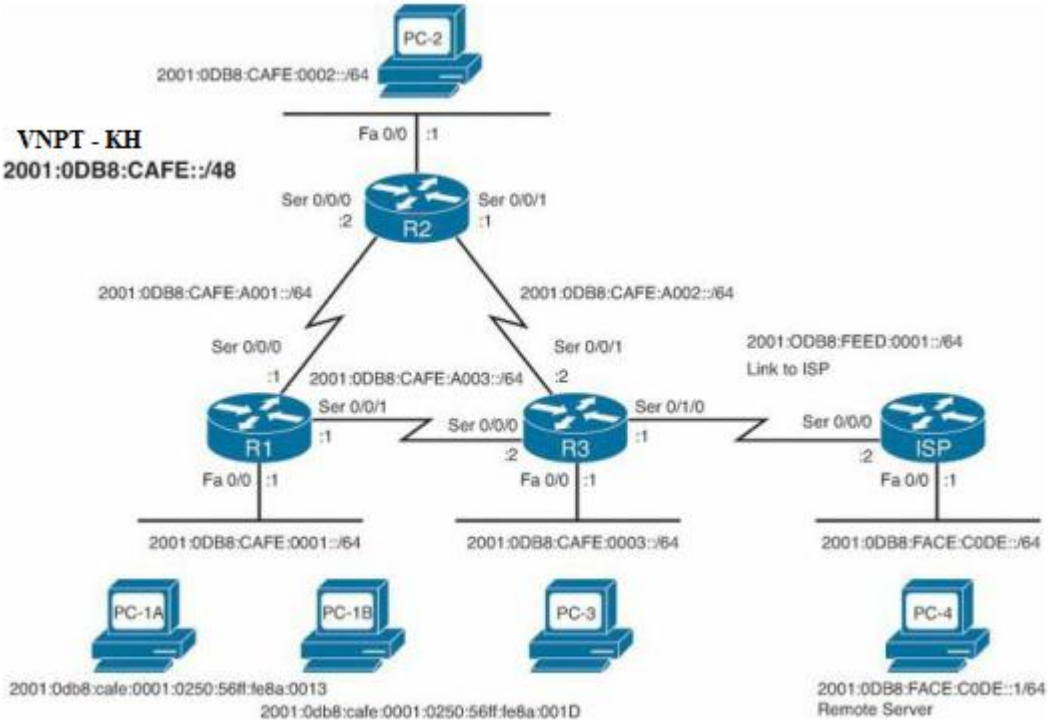


Hình 3. 8: Kiểm tra routing đến host đầu xa dùng IPv6- IPv4 Dual – Stack

VNPT Hải Dương đã triển khai IPv6- IPv4 Dual – Stack đến toàn bộ tập khách hàng bao gồm cả nhóm khách hàng cá nhân, k/h doang nghiệp trên địa bàn VNPT Hải Dương. Với các doanh nghiệp lớn có hệ thống mạng nội bộ phức tạp, VNPT Hải Dương hỗ trợ khách hàng cấu hình hệ thống theo các mô phỏng đã chuẩn bị trước giúp k/h sử dụng được các ưu điểm của hệ thống IPv4 và IPv6, nâng cao chất lượng và giá trị hình ảnh của VNPT Hải Dương

3.2. Cấu hình định tuyến IPv4 – IPv6 dual-stack trong môi trường giả lập.

Thực hiện giả lập mạng VNPT-KH Cấu hình IPv4 – IPv6 Dual – Stack gồm 3 router và 3 máy chủ dual- stack. Xây dựng định tuyến trong mạng sử dụng IPv6 và OSPFv3, các router bật dual – stack bằng cách cấu hình IPv4 và OSPFv2. Các máy chủ dual- stack thực hiện gửi cả gói IPv4 và IPv6 qua mạng VNPT-KH.



Hình 3. 9: Mô hình giả lập

3.2.1. Cấu hình địa chỉ IPv6:

Mạng bao gồm ba bộ định tuyến, R1, R2 và R3. Mỗi bộ định tuyến có một mạng LAN được gắn vào giao diện Ethernet 0/0:

R1: 2001:0db8:cafe:0001::/64

R2: 2001:0db8:cafe:0002::/64

R3: 2001:0db8:cafe:0003::/64

Trong nội bộ, mỗi bộ định tuyến được kết nối với một liên kết nối tiếp điểm-điểm. Để giúp xác định tốt hơn kết nối nối tiếp, ID mạng con bắt đầu bằng a. Ba mạng nối tiếp nội bộ là:

R1 và R2—2001:0db8:cafe:a001:/64

R2 và R2—2001:0db8:cafe:a002:/64

R1 và R3—2001:0db8:cafe:a003:/64

VNPT- KH được kết nối với ISP của mình thông qua mạng 2001: 0db8: feed: 0001: / 64. Như một ví dụ về một máy chủ từ xa, bộ định tuyến ISP có máy chủ 2001: 0db8: face: c0de :: 1/64 được kết nối với giao diện Fast Ethernet 0/0. Tất cả các địa chỉ được hiển thị trong Hình 3.1 là các địa chỉ unicast toàn cầu. Tiếp theo cấu hình các địa chỉ unicast toàn cầu trên mỗi bộ định tuyến sau đí kiểm tra lại cấu hình trên các router

R1# conf t

R1(config)# interface fastethernet 0/0

R1(config-if)# IPv6 address 2001:0db8:cafe:0001::1/64

R1(config-if)# exit

R1(config)# interface serial 0/0/0

R1(config-if)# IPv6 address 2001:0db8:cafe:a001::1/64

R1(config-if)# exit www.AdminPro.ir

R1(config)# interface serial 0/0/1

R1(config-if)# IPv6 address 2001:0db8:cafe:a003::1/64

R1(config-if)# end

R1#

R1# show IPv6 interface brief

FastEthernet0/0 [up/up]

FE80::21B:CFF:FEC2:82D8

2001:DB8:CAFE:1::1

Serial0/0/0 [up/up]

FE80::21B:CFF:FEC2:82D8

2001:DB8:CAFE:A001::1

Serial0/0/1 [up/up]

FE80::21B:CFF:FEC2:82D8

2001:DB8:CAFE:A003::1

R1#

Ta thấy Cả địa chỉ liên kết cục bộ và địa chỉ unicast toàn cầu của mỗi giao diện đều được hiển thị. Địa chỉ liên kết được tạo tự động bằng EUI-64 bất cứ khi nào có địa chỉ unicast toàn cầu.

Tương tự đối với R2 và R3

R2(config)# interface fastethernet 0/0

R2(config-if)# IPv6 address 2001:0db8:cafe:0002::1/64

R2(config-if)# exit

R2(config)# interface serial 0/0/0

R2(config-if)# IPv6 address 2001:0db8:cafe:a001::2/64

R2(config-if)# exit

R2(config)# interface serial 0/0/1

R2(config-if)# IPv6 address 2001:0db8:cafe:a002::1/64

R2(config-if)# end

R2#

R2# show IPv6 interface brief

FastEthernet0/0 [up/up]

FE80::21B:53FF:FE87:C050

2001:DB8:CAFE:2::1

Serial0/0/0 [up/up]

FE80::21B:53FF:FE87:C050

2001:DB8:CAFE:A001::2

Serial0/0/1

FE80::21B:53FF:FE87:C050

2001:DB8:CAFE:A002::1

R2#

Địa chỉ liên kết cục bộ được tạo tự động khi bạn gán địa chỉ unicast toàn cầu cho giao diện. Trừ khi được định cấu hình thủ công, các địa chỉ liên kết cục bộ được tạo bằng tiền tố FE80 :: / 10 và ID giao diện sử dụng EUI-64 hoặc giá trị được tạo

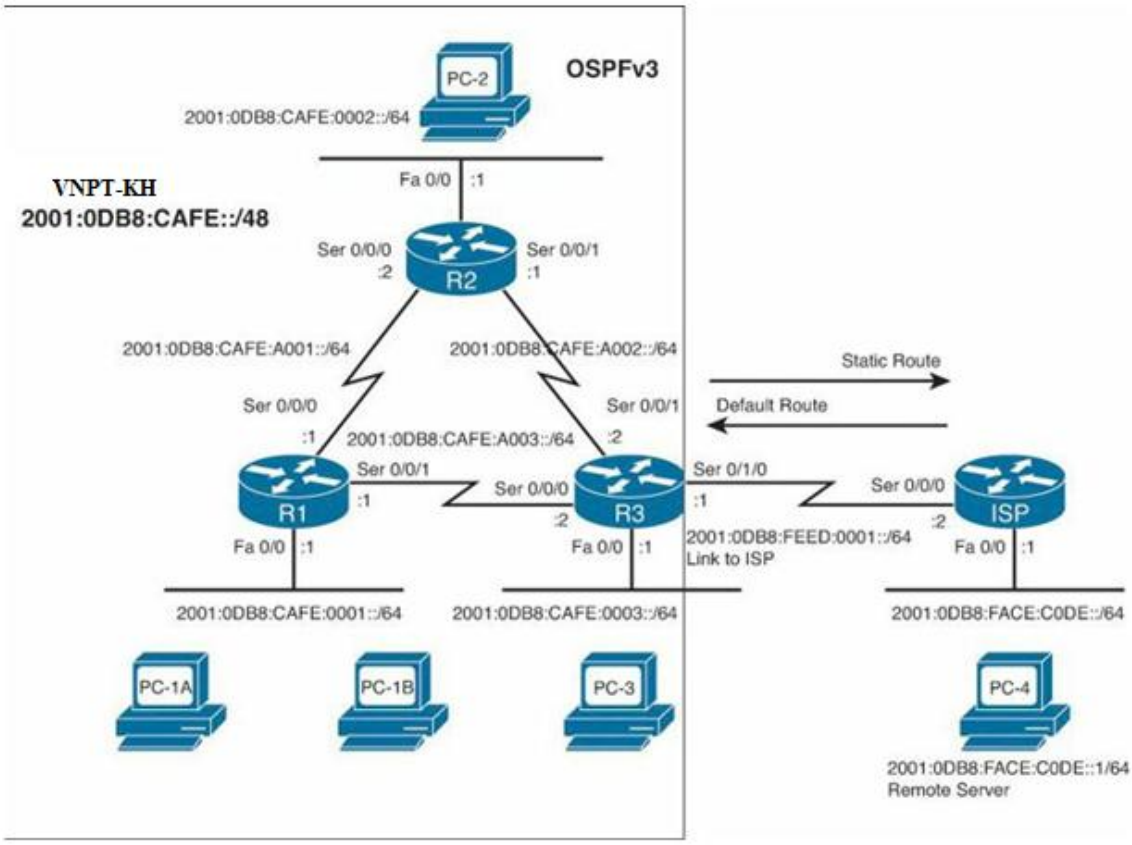
ngẫu nhiên. Cisco IOS sử dụng định dạng EUI-64. Như đã lưu ý trước đó, EUI-64 liên quan đến việc sử dụng địa chỉ MAC Ethernet 48 bit, chèn FFFE vào giữa và lật bit thứ bảy. Đối với giao diện nối tiếp, Cisco sử dụng địa chỉ MAC của Fast Giao diện Ethernet. Bởi vì các bộ định tuyến có một giao diện Fast Ethernet duy nhất và ít nhất một nối tiếp giao diện, điều này dẫn đến nhiều giao diện có cùng địa chỉ liên kết cục bộ. Điều này được chấp nhận. Để dễ theo dõi tiến trình phô phỏng, ta đặt lại các địa chỉ liên kết cục bộ.

```
R1(config)# interface fastethernet 0/0
R1(config-if)# IPv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# IPv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# IPv6 address fe80::1 link-local
R1(config-if)# end
R1#
R1# show IPv6 interface brief
FastEthernet0/0
FE80::1
                                        [up/up]
2001:DB8:CAFE:1::1
Serial0/0/0
[up/up]
FE80::1
2001:DB8:CAFE:A001::1
Serial0/0/1
                                [up/up]
FE80::1
2001:DB8:CAFE:A003::1
R1#
```

Kích hoạt IPv6 trên từng Interface.

Router(config-if)# IPv6 enable

3.2.2. Cấu hình định tuyến ospfv3



Hình 3. 10: Cấu hình Bộ định tuyến R1, R2 và R3 để chia sẻ thông tin định tuyến sử dụng OSPFv3

Trong miền định tuyến IGP. R3 được cấu hình với một tuyến mặc định thông qua bộ định tuyến ISP.Sử dụng OSPFv3, cấu hình R3 để phân phối tuyến mặc định tới các bộ định tuyến OSPFv3 khác. ISP vẫn được định cấu hình với tuyến tĩnh 2001:0DB8: CAFE :: / 48. Cả ISP và R3 định tuyến tĩnh.

R3(config)# IPv6 route ::/0 serial 0/1/0
ISP(config)# IPv6 route 2001:db8:cafe::/48 serial 0/0/

Lệnh định tuyến unicast IPv6 được sử dụng để cho phép định tuyến IPv6 trên R1. Tiếp theo, bắt đầu quá trình cấu hình của OSPFv3 trên Bộ định tuyến R1 với bộ định tuyến IPv6 ospf 1 toàn cầuchỉ huy. Lệnh này tương tự như lệnh ospf process-id của bộ định tuyến được sử dụng trong OSPFv2. GiốngOPSFv2, id quá trình trong OSPFv3 chỉ có ý nghĩa cục bộ và không cần phải giống nhau trên các bộ định tuyến

khác trong miền OSPF. Trong chế độ cấu hình bộ định tuyến, lệnh id-bộ định tuyến được sử dụng để cấu hình ID bộ định tuyến OSPF. Lệnh id bộ định tuyến OSPF này phải được cấu hình trên tất cả các bộ định tuyến trong cấu trúc liên kết vì nó chưa được cấu hình như một địa chỉ IPv4 trên bất kỳ giao diện nào. Do đó, bộ định tuyến không thể tự động chọn ID bộ định tuyến và ID bộ định tuyến phải theo cách cấu hình thủ công.

```
R1(config)# IPv6 unicast-routing
R1(config)# IPv6 router ospf 1
R1(config-rtr)# router-id 10.1.1.1
R1(config-rtr)# exit
R1(config)# interface fastethernet 0/0
R1(config-if)# IPv6 ospf 1 area 0
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# IPv6 ospf 1 area 0
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# IPv6 ospf 1 area 0
R1(config-if)# end
R1#
```

Cấu hình tương tự với R2 và R3:

```
R2(config)# IPv6 unicast-routing
R2(config)# IPv6 router ospf 1
R2(config-rtr)# router-id 10.2.2.2
R2(config-rtr)# exit
R2(config)# interface fastethernet 0/0
R2(config-if)# IPv6 ospf 1 area 0
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# IPv6 ospf 1 area 0
```

R2(config-if)# exit

R2(config)# interface serial 0/0/1

R2(config-if)# IPv6 ospf 1 area 0

R2(config-if)# end

R2#

Để hoàn tất cấu hình của OSPFv3, cấu hình quản bá tuyến mặc định trên R3 đến các bộ định tuyến khác trong Tên miền OSPF. Lệnh khởi tạo thông tin cấu hình bộ định tuyến được cấu hình trênR3:

R3(config-rtr)# default-information originate

R3(config-rtr)# end

R3#

3.2.3. Cấu hình IPv4 và ospfv2

Bắt đầu với Bộ định tuyến R1, cấu hình các địa chỉ IPv4 trên giao diện Fast Ethernet của nó và cả hai giao diện nối tiếp. Sau khi các giao diện đã được cấu hình, cấu hình định tuyến OSPFv2. Các giao diện R1, cho IPv4 và bật OSPFv2 trên cả ba giao diện. Đây là những cấu hình luôn được sử dụng với IPv4. Như thể IPv6 đã không tồn tại trên mạng.

R1(config)# interface FastEthernet0/0

R1(config-if)# ip address 10.1.0.1 255.255.0.0

R1(config-if)# exit

R1(config)# interface Serial0/0/0

R1(config-if)# ip address 10.10.10.1 255.255.255.252

R1(config-if)# exit

R1(config)# interface Serial0/0/1

R1(config-if)# ip address 10.10.10.9 255.255.255.252

R1(config-if)# exit

R1(config)# router ospf 2

R1(config-rtr)# network 10.1.0.0 0.0.255.255 area 0

R1(config-rtr)# network 10.10.10.0 0.0.0.3 area 0

R1(config-rtr)# network 10.10.10.8 0.0.0.3 area 0

Kiểm tra cấu hình đang chạy của R1, không giống như OSPFv2, OSPFv3 không sử dụng lệnh mạng để kích hoạt OSPF trên giao diện. Với OSPFv3, lệnh IPv6 opsf được sử dụng để kích hoạt OSPF trực tiếp trên giao diện.Bộ định tuyến R1 là bộ định tuyến xếp chồng kép, đội mũ hai chiếc, một chiếc cho IPv4 và một chiếc cho IPv6. Cấu hình tương tự cho Router R2 và R3:

```
R2(config)# interface fastethernet 0/0
R2(config-if)# ip address 10.2.0.1 255.255.255.0
! Replaces the OSPFv2 network command:
R2(config-if)# ip ospf 2 area 0
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 10.10.10.2 255.255.255.252
! Replaces the OSPFv2 network command:
R2(config-if)# ip ospf 2 area 0
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# ip address 10.10.10.5 255.255.255.252
! Replaces the OSPFv2 network command:
R2(config-if)# ip ospf 2 area 0
R2(config-if)#
```

Cấu hình định tuyến tĩnh giữa R3 và ISP, sau đó cấu hình quản bá tuyến default route này trong OSPFv2

```
R3(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1/0
R3(config)# router ospf 2
R3(config-rtr)# default-information originate
```

3.2.4. Kiểm tra định tuyến IPv4 và IPv6, kiểm tra IPv4 - IPv6 dual – stack

Lệnh show ip route được sử dụng để hiển thị tất cả các tuyến IPv4 được kết nối trực tiếp, tĩnh và được học động, trong khi lệnh show IPv6 route được sử dụng để làm tương tự cho các mạng IPv6. Kiểm tra các tuyến học qua OSPFv2, OSPFv3.

R1# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - ISIS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.10.10.10 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks

10.10.10.8/30 is directly connected, Serial0/0/1

10.2.0.0/16 [110/65] via 10.10.10.2, 01:20:14, Serial0/0/0

10.3.0.0/16 [110/65] via 10.10.10.10, 01:20:14, Serial0/0/1

10.10.10.0/30 is directly connected, Serial0/0/0

10.1.0.0/16 is directly connected, FastEthernet0/0

10.10.10.4/30 [110/128] via 10.10.10.2, 01:20:14, Serial0/0/0

O*E2 0.0.0.0/0 [110/1] via 10.10.10.10, 01:15:51, Serial0/0/1

R1#

R1# show IPv6 route

IPv6 Routing Table - 12 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

OE 2 ::/0 [110/1], tag 1

via FE80::3, Serial0/0/1

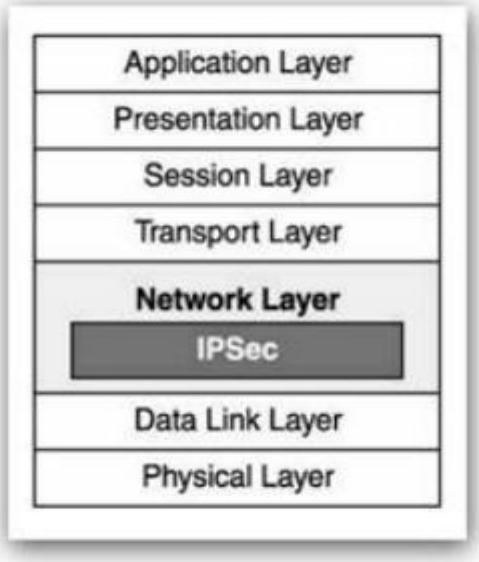
C 2001:DB8:CAFE:1::/64 [0/0]

via ::, FastEthernet0/0

3.4 Bảo mật trong IPv6

3.4.1 Ip sec (ip security)

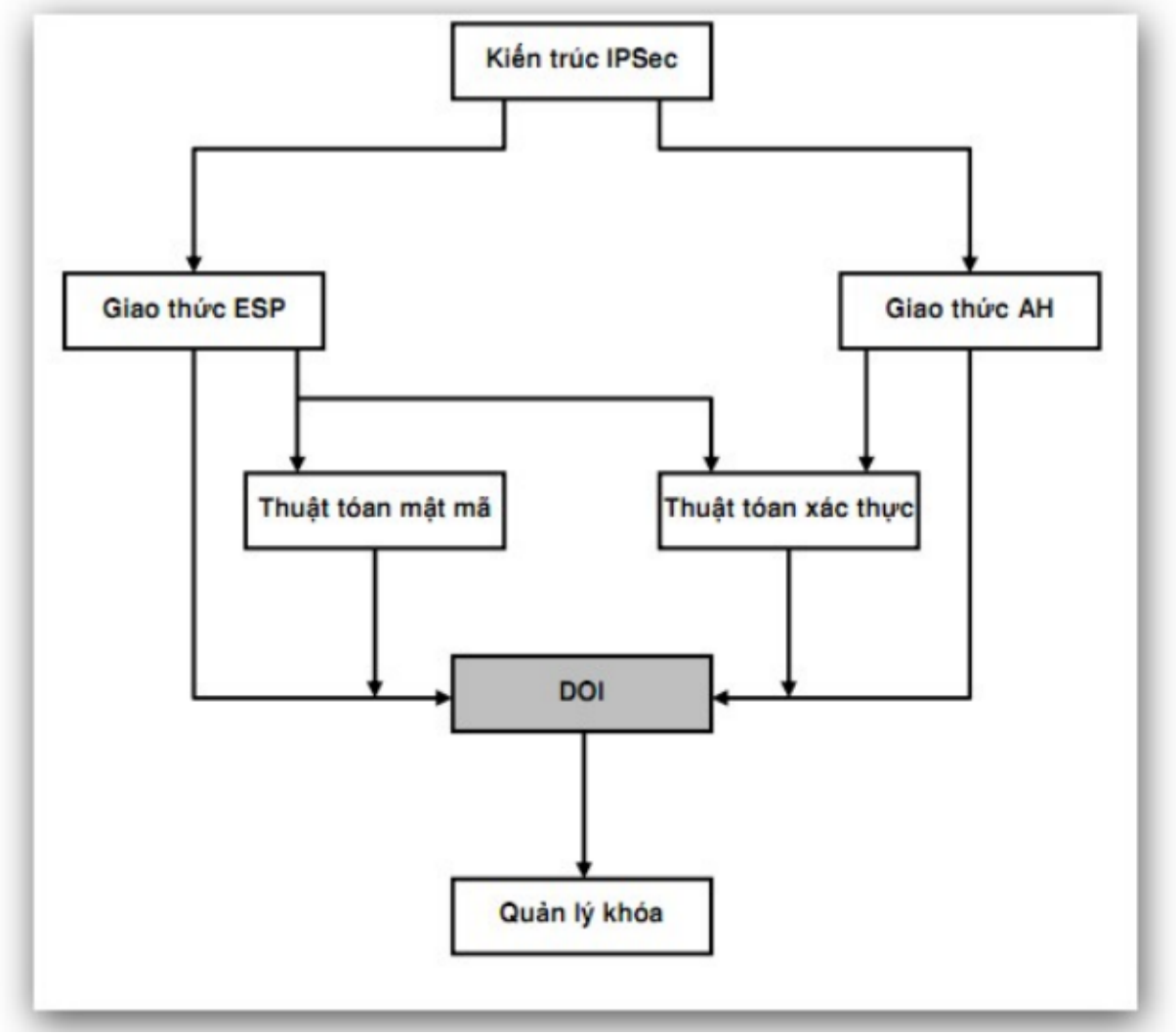
Giao thức IPsec được làm việc tại tầng Network Layer – layer 3 của mô hình OSI. Các giao thức bảo mật trên Internet khác như SSL, TLS và SSH, được thực hiện từ tầng transport layer trở lên (Từ tầng 4 tới tầng 7 mô hình OSI). Điều này tạo ra tính mềm dẻo cho IPsec, giao thức này có thể hoạt động từ tầng 4 với TCP, UDP, hầu hết các giao thức sử dụng tại tầng này. IPsec có một tính năng cao cấp hơn SSL và các phương thức khác hoạt động tại các tầng trên của mô hình OSI. Với một ứng dụng sử dụng IPsec mã (code) không bị thay đổi, nhưng nếu ứng dụng đó bắt buộc sử dụng SSL và các giao thức bảo mật trên các tầng trên trong mô hình OSI thì đoạn mã ứng dụng đó sẽ bị thay đổi lớn..



Hình 3. 11: Kiến trúc mô hình OSI

3.4.2. Kiến trúc ipsec:

IPSec là một giao thức phức tạp, dựa trên nền của nhiều kỹ thuật cơ sở khác nhau như mật mã, xác thực, trao đổi khoá… Xét về mặt kiến trúc, IPSec được xây dựng dựa trên các thành phần cơ bản sau đây, mỗi thành phần được định nghĩa trong một tài liệu riêng tương ứng:



Hình 3. 12: Kiến trúc IPsec

- Kiến trúc IPSec (RFC 2401): Quy định các cấu trúc, các khái niệm và yêu cầu của IPSec. - Giao thức ESP (RFC 2406): Mô tả giao thức ESP, là một giao thức mật mã và xác thực thông tin trong IPSec.

- Giao thức AH (RFC 2402): Định nghĩa một giao thức khác với chức năng gần giống ESP. Như vậy khi triển khai IPSec, người sử dụng có thể chọn dùng ESP hoặc AH, mỗi giao thức có ưu và nhược điểm riêng.

- Thuật toán mật mã: Định nghĩa các thuật toán mã hoá và giải mã sử dụng trong IPSec. IPSec chủ yếu dựa vào các thuật toán mã hoá đối xứng.

- Thuật toán xác thực: Định nghĩa các thuật toán xác thực thông tin sử dụng trong AH và ESP.

- Quản lý khoá (RFC 2408): Mô tả các cơ chế quản lý và trao đổi khoá trong IPSec.

- Miền thực thi (Domain of Interpretation – DOI): Định nghĩa môi trường thực thi IPSec. IPSec không phải là một công nghệ riêng biệt mà là sự tổ hợp của nhiều cơ chế, giao thức và kỹ thuật khác nhau, trong đó mỗi giao thức, cơ chế đều có nhiều chế độ hoạt động khác nhau. Việc xác định một tập các chế độ cần thiết để triển khai IPSec trong một tình huống cụ thể là chức năng của miền thực thi. Xét về mặt ứng dụng, IPSec thực chất là một giao thức hoạt động song song với IP nhằm cung cấp 2 chức năng cơ bản mà IP nguyên thuỷ chưa có, đó là mã hoá và xác thực gói dữ liệu. Một cách khái quát có thể xem IPSec là một tổ hợp gồm hai thành phần: -Giao thức đóng gói, gồm AH và ESP -Giao thức trao đổi khoá IKE (Internet Key Exchange).

3.4.3. Hiện trạng

IPsec là một phần bắt buộc của IPv6, có thể được lựa chọn khi sử dụng IPv4. Trong khi các chuẩn đã được thiết kết cho các phiên bản IP giống nhau, phổ biến hiện nay là áp dụng và triển khai trên nền tảng IPv4.

Các giao thức IPsec được định nghĩa từ RFCs 1825 – 1829, và được phổ biến năm 1995. Năm 1998, được nâng cấp với các phiên bản RFC 2401 – 2412, nó không tương thích với chuẩn 1825 – 1929. Trong tháng 12 năm 2005, thế hệ thứ 3 của chuẩn IPSec, RFC 4301 – 4309. Cũng không khác nhiều so với chuẩn RFC 2401 – 2412 nhưng thế hệ mới được cung cấp chuẩn IKE second. Trong thế hệ mới này IP security cũng được viết tắt lại là IPsec.

Sự khác nhau trong quy định viết tắt trong thế hệ được quy chuẩn bởi RFC 1825 – 1829 là ESP còn phiên bản mới là ESPbis. IPsec được cung cấp bởi Transport mode (end-to-end) đáp ứng bảo mật giữa các máy tính giao tiếp trực tiếp

với nhau hoặc sử dụng Tunnel mode (portal-to-portal) cho các giao tiếp giữa hai mạng với nhau và chủ yếu được sử dụng khi kết nối VPN.

IPsec có thể được sử dụng trong các giao tiếp VPN, sử dụng rất nhiều trong giao tiếp. Tuy nhiên trong việc triển khai thực hiện sẽ có sự khác nhau giữa hai mode này.

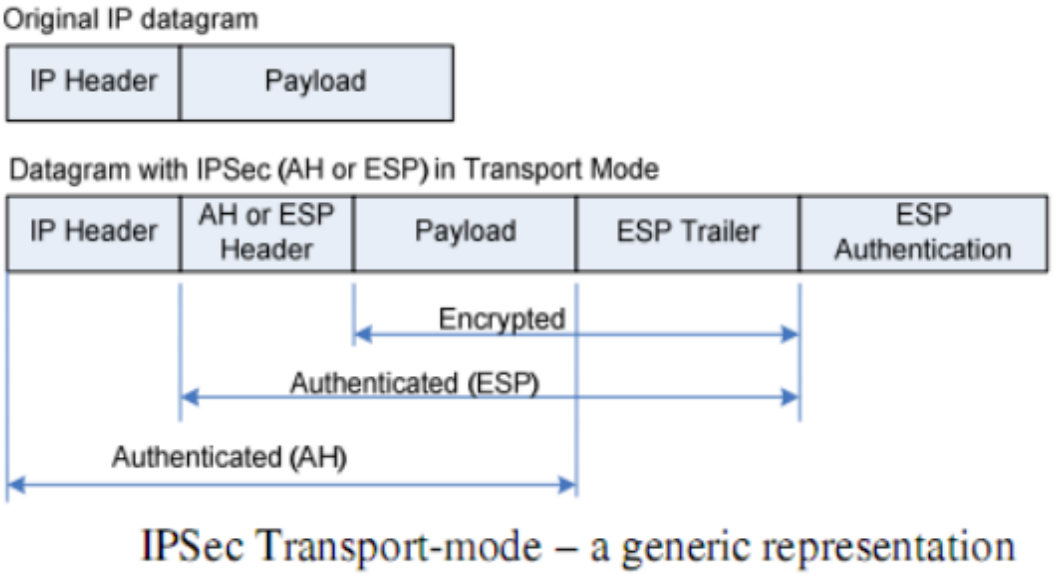
Giao tiếp end-to-end được bảo mật trong mạng Internet được phát triển chậm và phải chờ đợi rất lâu. Một phần bở lý do tính phổ thông của no không cao, hay không thiết thực, Public Key Infrastructure (PKI) được sử dụng trong phương thức này.

IPsec đã được giới thiệu và cung cấp các dịch vụ bảo mật:

1. Mã hoá quá trình truyền thông tin
2. Đảm bảo tính nguyên vẹn của dữ liệu
3. Phải được xác thực giữa các giao tiếp
4. Chống quá trình replay trong các phiên bảo
5. Modes – Các mode

Có hai mode khi thực hiện IPsec đó là: Transport mode và tunnel mode.

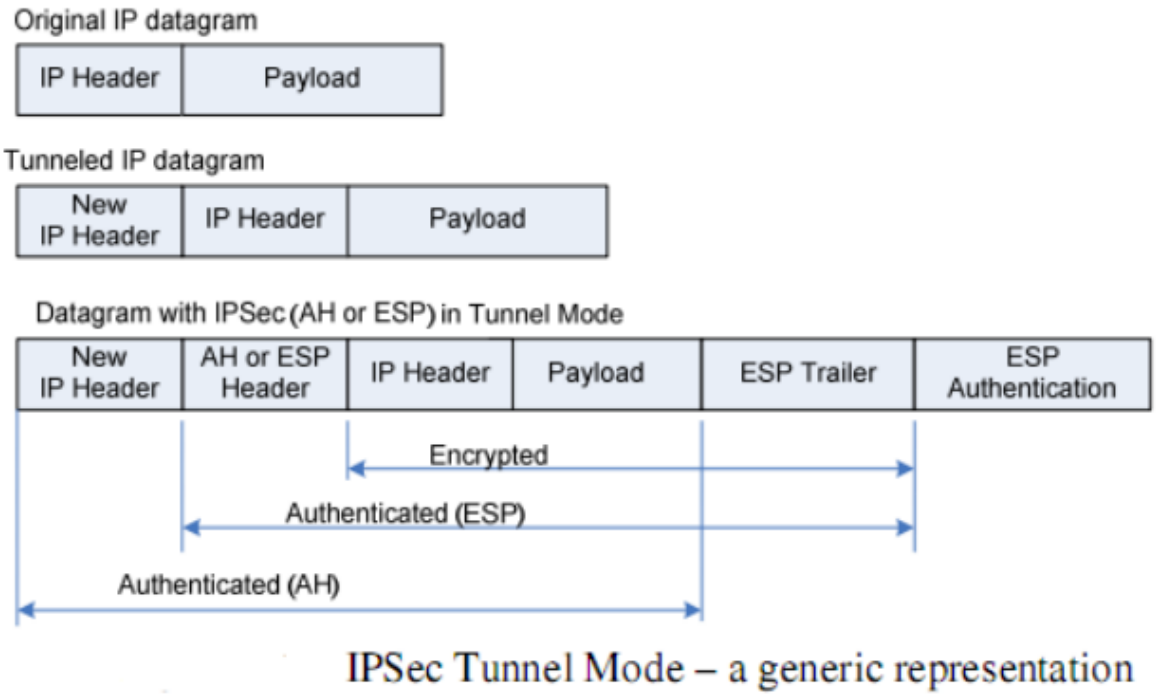
Transport Mode (chế độ vận chuyển) - Transport mode cung cấp cơ chế bảo vệ cho dữ liệu của các lớp cao hơn (TCP, UDP hoặc ICMP). Trong Transport mode, phần IPSec header được chèn vào giữa phần IP header và phần header của giao thức tầng trên, như hình mô tả bên dưới, AH và ESP sẽ được đặt sau IP header nguyên thủy. Vì vậy chỉ có tải (IP payload) là được mã hóa và IP header ban đầu là được giữ nguyên vẹn. Transport mode có thể được dùng khi cả hai host hỗ trợ IPSec. Chế độ transport này có thuận lợi là chỉ thêm vào vài bytes cho mỗi packets và nó cũng cho phép các thiết bị trên mạng thấy được địa chỉ đích cuối cùng của gói. Khả năng này cho phép các tác vụ xử lý đặc biệt trên các mạng trung gian dựa trên các thông tin trong IP header. Tuy nhiên các thông tin Layer 4 sẽ bị mã hóa, làm giới hạn khả năng kiểm tra của gói.



Hình 3. 13 Một đại diện chung mô hình vận chuyển IPsec

- Không giống Transport mode, Tunnel mode bảo vệ toàn bộ gói dữ liệu. Toàn bộ gói dữ liệu IP được đóng gói trong một gói dữ liệu IP khác và một IPSec header được chèn vào giữa phần đầu nguyên bản và phần đầu mới của IP.Toàn bộ gói IP ban đầu sẽ bị đóng gói bởi AH hoặc ESP và một IP header mới sẽ được bao bọc xung quanh gói dữ liệu. Toàn bộ các gói IP sẽ được mã hóa và trở thành dữ liệu mới của gói IP mới. Chế độ này cho phép những thiết bị mạng, chẳng hạn như router, hoạt động như một IPSec proxy thực hiện chức năng mã hóa thay cho host. Router nguồn sẽ mã hóa các packets và chuyển chúng dọc theo tunnel. Router đích sẽ giải mã gói IP ban đầu và chuyển nó về hệ thống cuối. Vì vậy header mới sẽ có địa chỉ nguồn chính là gateway.

- Với tunnel hoạt động giữa hai security gateway, địa chỉ nguồn và đích có thể được mã hóa. Tunnel mode được dùng khi một trong hai đầu của kết nối IPSec là security gateway và địa chỉ đích thật sự phía sau các gateway không có hỗ trợ IPSec.



Hình 3. 14: Một đại diện chung mô hình đường hầm IPsec

3.4.4. Technical details - chi tiết kỹ thuật

Có hai giao thức được phát triển và cung cấp bảo mật cho các gói tin của cả hai phiên bản IPv4 và IPv6:

IP Authentication Header giúp đảm bảo tính toàn vẹn và cung cấp xác thực.

IP Encapsulating Security Payload cung cấp bảo mật, và là option bạn có thể lựa chọn cả tính năng authentication và Integrity đảm bảo tính toàn vẹn dữ liệu.

Thuật toán mã hoá được sử dụng trong IPsec bao gồm HMAC-SHA1 cho tính toàn vẹn dữ liệu (integrity protection), và thuật toán TripleDES-CBC và AES-CBC cho mã mã hoá và đảm bảo độ an toàn của gói tin. Toàn bộ thuật toán này được thể hiện trong RFC 4305.

a. Authentication Header (AH)

AH được sử dụng trong các kết nối không có tính đảm bảo dữ liệu. Hơn nữa nó là lựa chọn nhằm chống lại các tấn công replay attack bằng cách sử dụng công nghệ tấn công sliding windows và discarding older packets. AH bảo vệ quá trình truyền dữ liệu khi sử dụng IP. Trong IPv4, IP header có bao gồm TOS, Flags,

Fragment Offset, TTL, và Header Checksum. AH thực hiện trực tiếp trong phần đầu tiên của gói tin IP. dưới đây là mô hình của AH header.

Các modes thực hiện

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

Hình 3. 15: Mô hình của tiêu đề AH

Ý nghĩa của từng phần:

Next header

Nhận dạng giao thức trong sử dụng truyền thông tin.

Payload length

Độ lớn của gói tin AH.

RESERVED

Sử dụng trong tương lai (cho tới thời điểm này nó được biểu diễn bằng các số 0).

Security parameters index (SPI)

Nhận ra các thông số bảo mật, được tích hợp với địa chỉ IP, và nhận dạng các thương lượng bảo mật được kết hợp với gói tin.

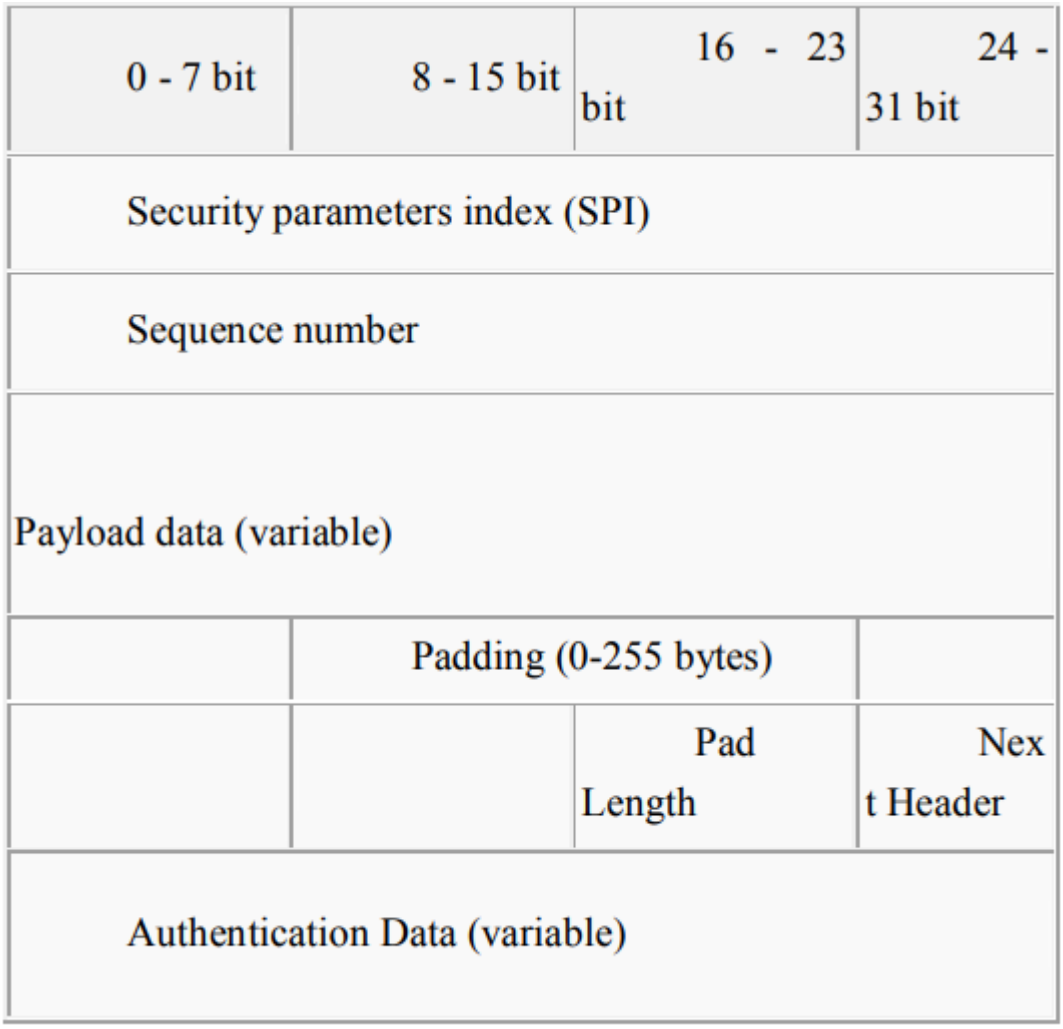
Sequence number Một số tự động tăng lên mỗi gói tin, sử dụng nhằm chống lại tấn công dạng replay attacks.

Authentication data

Bao gồm thông số Integrity check value (ICV) cần thiết trong gói tin xác thực.

b. Encapsulating Security Payload (ESP)

Giao thức ESP cung cấp xác thực, độ toàn vẹn, đảm bảo tính bảo mật cho gói tin. ESP cũng hỗ trợ tính năng cấu hình sử dụng trong tính huống chỉ cần bảo mã hoá và chỉ cần cho authentication, nhưng sử dụng mã hoá mà không yêu cầu xác thực không đảm bảo tính bảo mật. Không như AH, header của gói tin IP, bao gồm các option khác. ESP thực hiện trên top IP sử dụng giao thức IP và mang số hiệu 50 và AH mang số hiệu 51.



Hình 3. 16: Mô hình giao thức ESP cung cấp xác thực

Ý nghĩa của các phần:

Security parameters index (SPI)

Nhận ra các thông số được tích hợp với địa chỉ IP.

Sequence number

Tự động tăng có tác dụng chống tấn công kiểu replay attacks.

Payload data

Cho dữ liệu truyền đi

Padding

Sử dụng vài block mã hoá

Pad length

Độ lớn của padding.

Next header

Nhận ra giao thức được sử dụng trong quá trình truyền thông tin.

Authentication data

Bao gồm dữ liệu để xác thực cho gói tin.

KẾT LUẬN

Việc chuyển đổi địa chỉ IPv4 sang IPv6 là xu hướng tất yếu đối với tất cả các nhà cung cấp dịch vụ trên thế giới cũng như tại Việt Nam. Tập đoàn Bưu Chính viễn thông Việt nam nói chung, VNPT – Hải Dương nói riêng cần chuẩn bị sẵn phương án để chuyển đổi từ IPv4 – IPv6 nhưng vẫn đảm bảo tính bình thường của hệ thống và thuê bao, hiện nay VNPT Hải Dương cung cấp dịch vụ internet cho 140.000 thuê bao các loại; để chuẩn bị chuyển đổi từ giao thức cũ IPv4 sang IPv6 vào năm 2021 bằng phương pháp dual stack cho lượng khách hàng trên đồng bộ được với hệ thống vấn đề lớn nhất không phải hạ tầng mạng mà là thiết bị cung cấp cho người dùng cuối (CPEs chưa hỗ trợ IPv6. Ngay cả hệ thống mạng 3G, 4G của VNPT Hải Dương hiện nay cũng chưa hỗ trợ giao thức mới này).

- Sau một thời gian nghiên cứu, luận văn của em đã đi sâu vào phương án chuyển đổi IPv4 – IPv6 bằng phương pháp dual stack tại mạng khách hàng VNPT Hải Dương.

- Kết quả quá trình nghiên cứu: hiện em đã thực hiện mô phỏng cấu hình chuyển đổi từ IPv4 sang IPv6 bằng phương pháp dual stack trong môi trường giả lập và cũng đã thực nghiệm tại thiết bị đầu cuối khách hàng, kết quả đã thu lại kết quả khả quan qua các bài test, nội dung mô phỏng cũng là tài liệu tham khảo để triển khai chuyển đổi trong thực tế trong giai đoạn chuyển đổi tại đầu cuối khách hàng vào những năm sau.

- Nắm bắt được cơ chế bảo mật trong IPv6.

- Vì thời gian nghin cứu có hạn do vậy luận văn của em không tránh được những thiếu sót, em rất kính mong các thầy tham gia đóng góp để em được hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

+ TiếngViệt

[1] Nguyễn Thị Thu Thủy, Giới thiệu về thế hệ địa chỉ Internet mới IPv6, NXB Bưu Điện 2006.

+ **Tiếng Anh**

[2] Arafat, Muhammad Yeasir, Feroz Ahmed, and M. AbdusSobhan. ”On the Migration of a Large Scale Network from IPv4 to IPv6 Environment.” International Journal of Computer Networks & Communications (IJCNC) 6.2 (2014): 111-126

[3] IPv6 Country Statistics, http://6lab.cisco.com/stats/search.php , (last accessed at 13-10-2016)

[4] Shannon McFarland, MuninderSambi, Nikhil Sharma, and Sanjay Hooda IPv6 for Enterprise Networks, Copyright © 2011 Cisco Systems, Inc

+ Trang web

[5] Website: https://www.vnnic.vn/ cập nhật ngày 25/04/2020