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*)

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **Giáo sư, Tiến Sĩ: Nguyễn Bình**

Phản biện 1: **PGS.TS. Nguyễn Hữu Trung**

Phản biện 2: **TS. Nguyễn Chiến Trinh**

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 08 giờ 30 ngày 20 tháng 06 năm 2020

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

MỤC LỤC

MỤC LỤC HÌNH VẼ

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: BỐI CẢNH, LÝ DO CẦN THIẾT PHẢI TRIỂN KHAI IPV4-IPV6

1.1. Cấu trúc địa chỉ IPv4

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

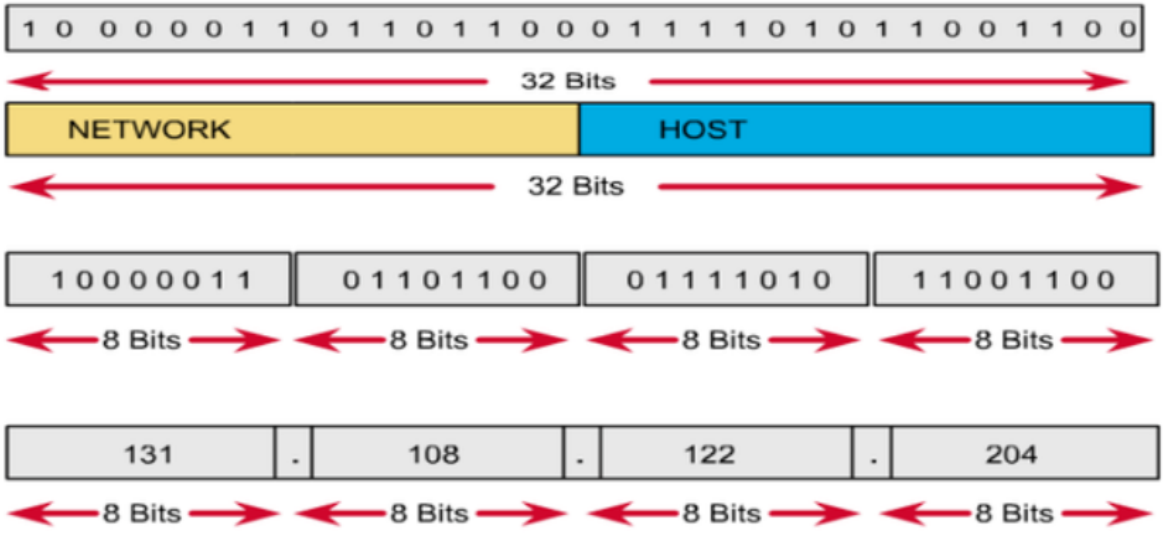
Địa chỉ IP có 32 bit nhị phân và được chia thành các octet (4 cụm, 8 bit)

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. 1: Cấu trúc địa chỉ IPv4

1.2. 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. 2 Cấu trúc khung của Ipv6 tại lớp 2 trong mạng LAN

1.3. Các loại địa chỉ IPv6

1.3.1. 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.

1.3.1.1 Địa chỉ Global Unicast:

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. 3: 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.

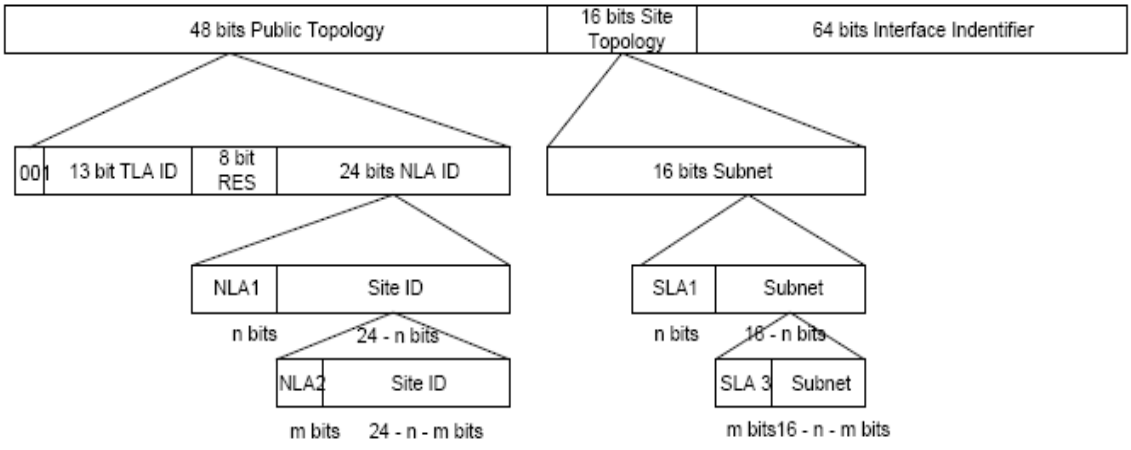
Như vậy, loại địa chỉ Global Unicast được thiết kế phân cấp, cấu trúc của nó được chia thành 3 phần :

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:

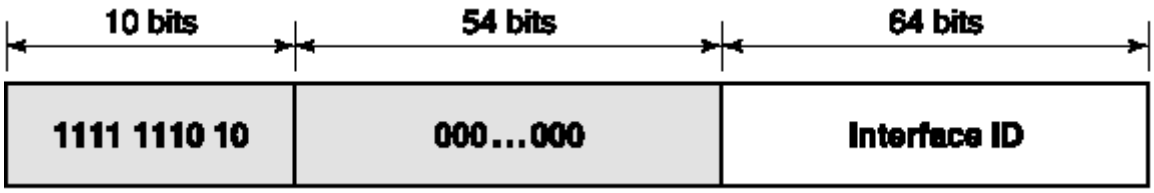


Hình 1. 4: Ba phần của chia chỉ Unicast

1.3.1.2. Địa chỉ Local Unicast:

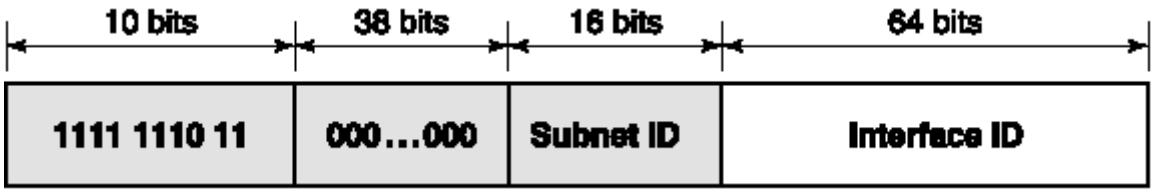
Địa chỉ đơn hướng dùng nội bộ, được sử dụng cho một tổ chức có mạng máy tính riêng (dùng nội bộ) chưa kết nối với mạng Internet nhưng sẵn sàng kết nối mang khi cần. Địa chỉ này chia làm hai loại là địa chỉ Link Local và Site Local.

Địa chỉ Link Local:



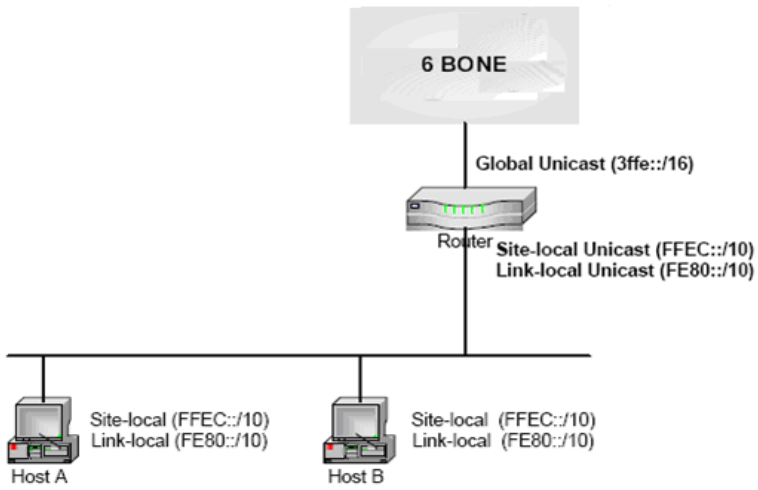
Hình 1. 5: Cấu trúc của địa chỉ Link-local như sau

Cấu trúc địa chỉ Site Local:



Hình 1. 6: Cấu trúc địa chỉ Site-local

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. 7 Các loại địa chỉ cần gán đối với một Site vào mạng IPv6

1.3.2. 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 1.7 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.

1.3.2.1 Địa chỉ anycast

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.

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. 8 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 đóphân 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.

1.3.2.2. 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.

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).

1.5. 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. 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 lPv4 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:

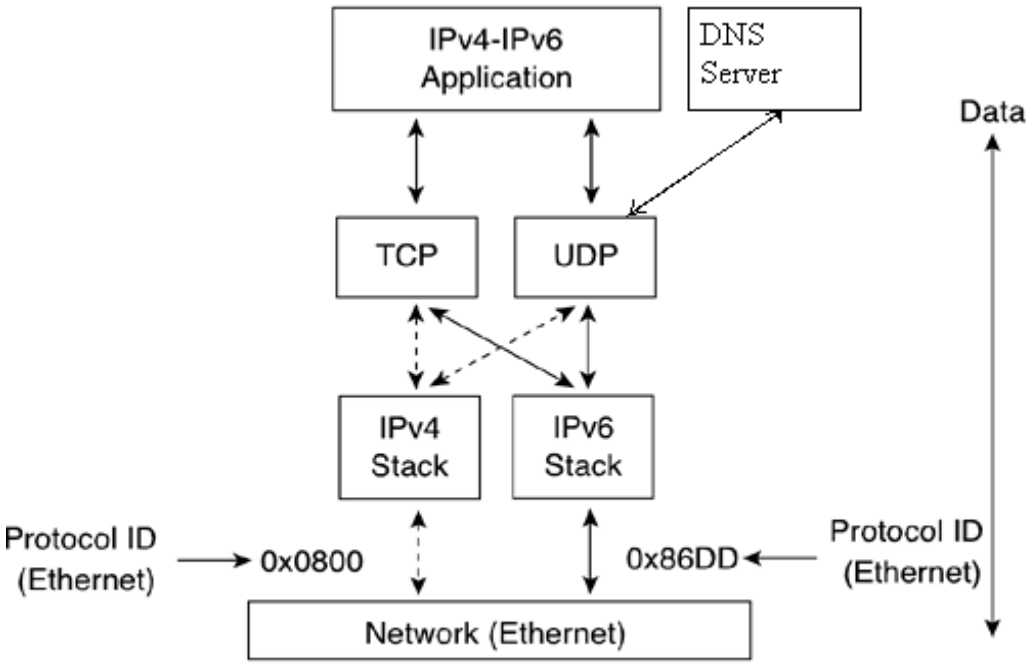
Đường hầm 6to4

Đường hầm ISATAP

Dual Stack

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 đượ 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.

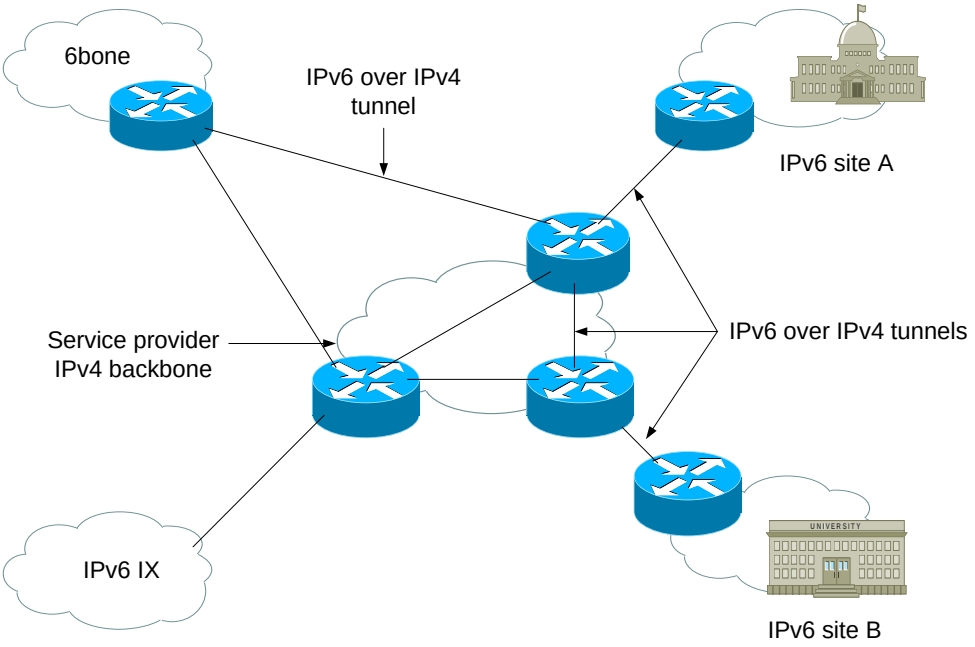
2.2.2. Dịch vụ cung cấp tên miền (DNS)

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.

2.3. 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 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, …

*** Đường hầm cấu hình tự động:**

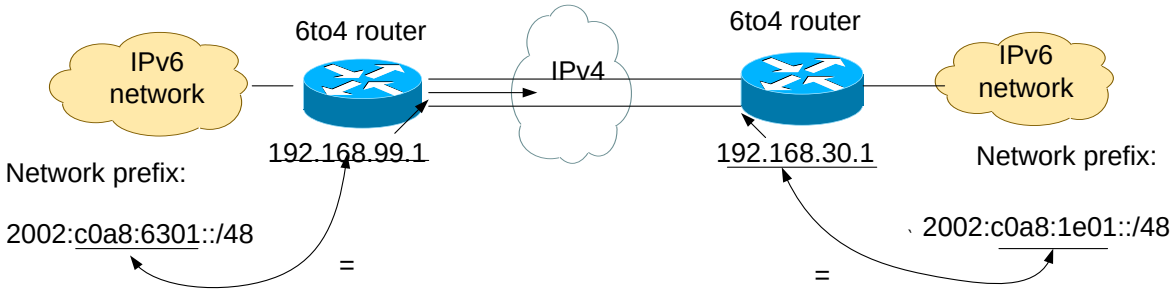
Đặc điểm của đường hầm tự động là địa chỉ điểm cuối đường hầm được xác định một cách tự động. Đường hầm được tạo ra một cách tự động và cũng tự động mất đi.

a) Cơ chế 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. 3: Cơ chế 6to4

Khuôn dạng của một địa chỉ 6to4 như sau:

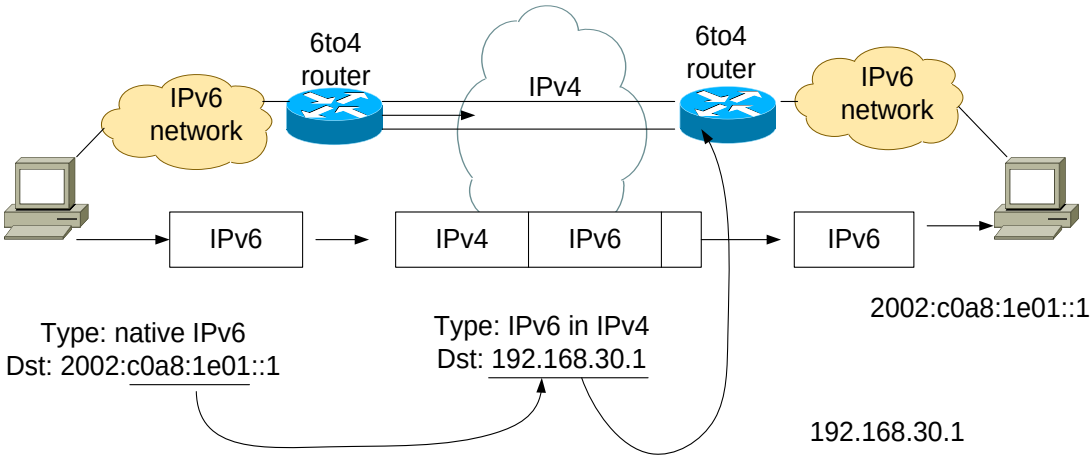
FP	TLA	Ipv4ADDR	SLA ID	Interface ID

Hình 2. 4: 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. 5: 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.

b) Cơ chế 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 it 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.

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

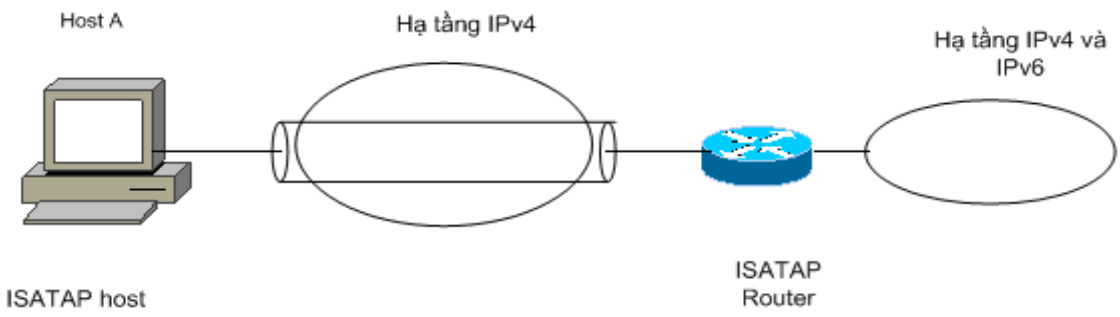
3FFE:1 a05:510:1111::/64 và bộ nhận dạng giao tiếp ISATAP là địa chỉ Ipv4 nhúng: “140.173.129.8”. Địa chỉ trên có thể viết cách khác là:

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. 6: ISATAP Router

Một router ISATAP là một router Ipv6 thực hiện các chức năng sau:

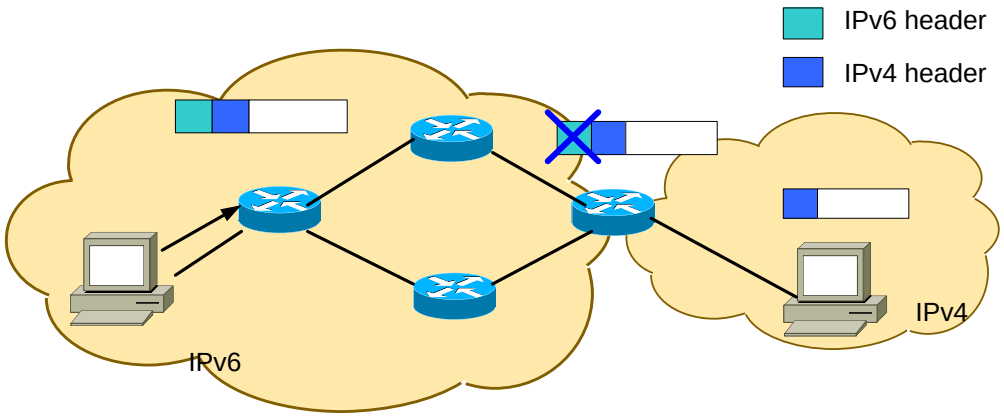
Chuyển các gói tin giữa các host ISATAP trên một mạng con logic (một mạng Ipv4) và các host trên cùng mạng con khác. Các mạng con khác có thể là mạng Ipv4 hoặc mạng con trong một miền (domain) Ipv6.

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 translation stack 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. 7: Mô hình hoạt động của DSTM

2.4.1. 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.

2.4.2. 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.

2.4.3. 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

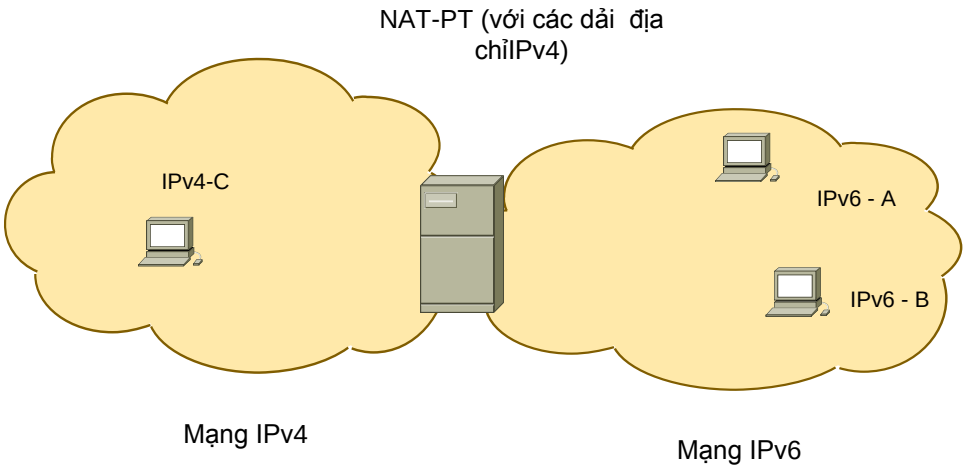
2.4.1.4. Hoạt động của Máy chủ DSTM

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.

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.

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 tram và sự chuyển đổi gói tin tại thiết bị NAT-PT hoàn toàn trong suốt với người dùng.



Hình 2. 8: 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 đo, 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, ...

2.6. 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

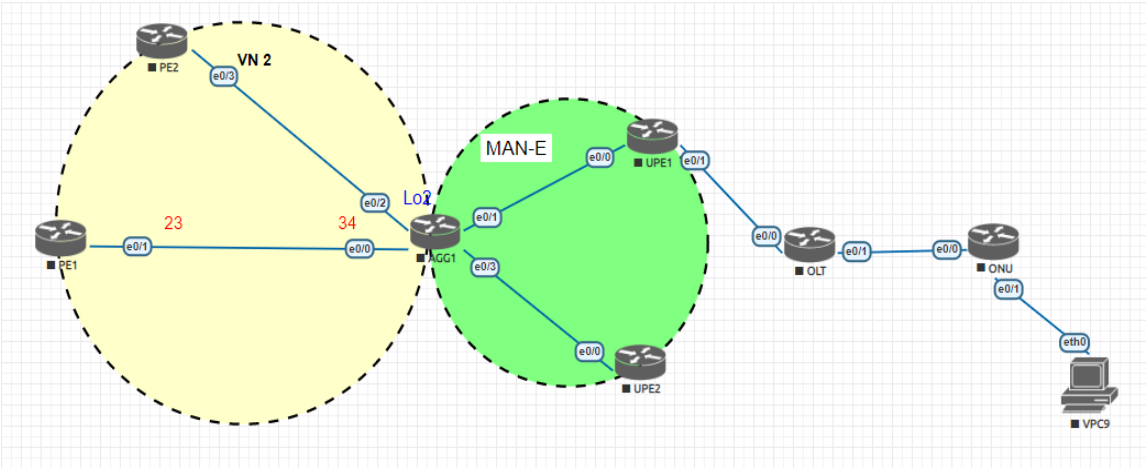
3.1.1 Mô hình cung cấp dịch vụ internet tại vnpt Hải Dương.

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.

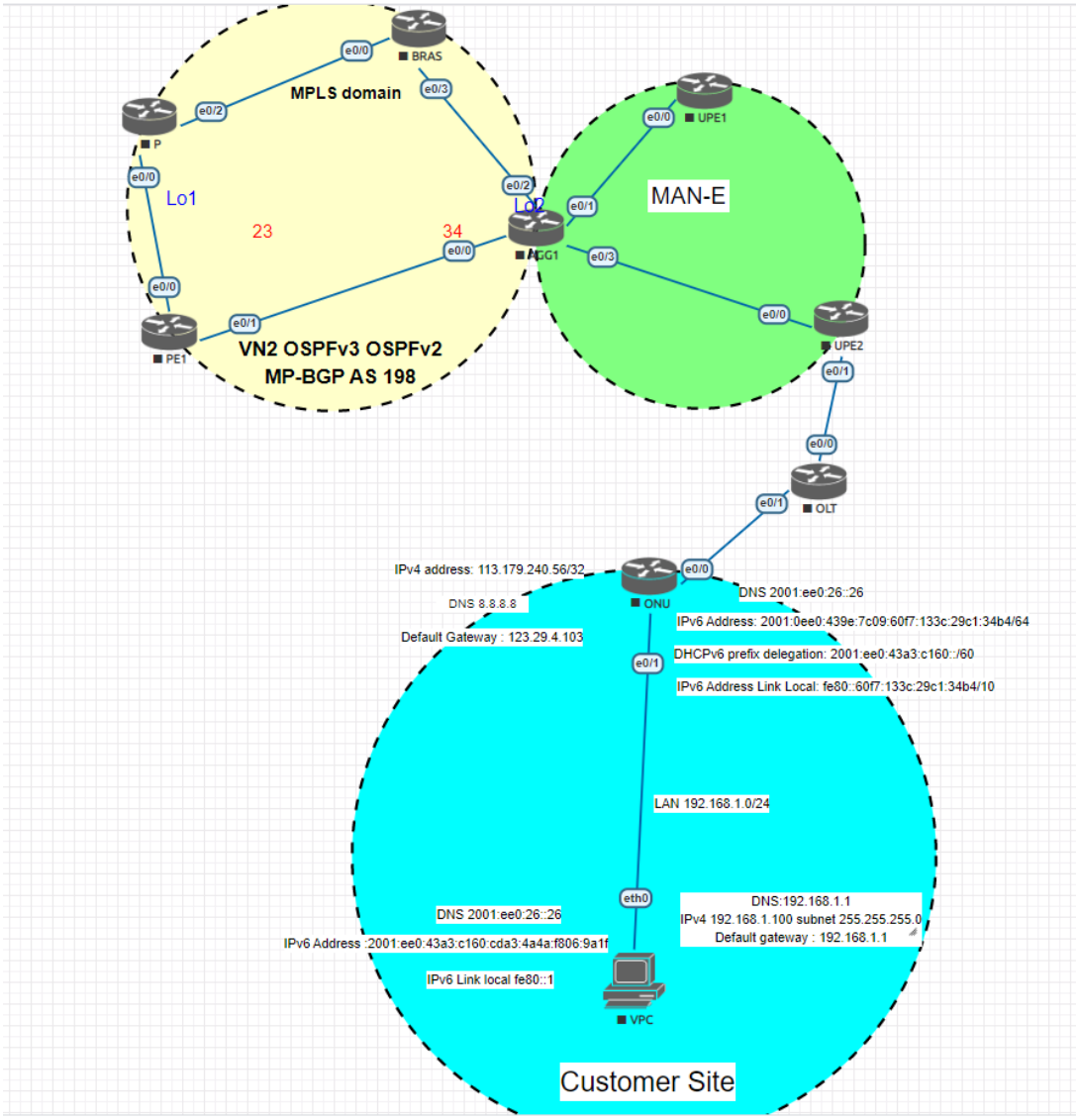


Hình 3. 1: Mô hình cung cấp dịch vụ Internet VNPT hải Dương.

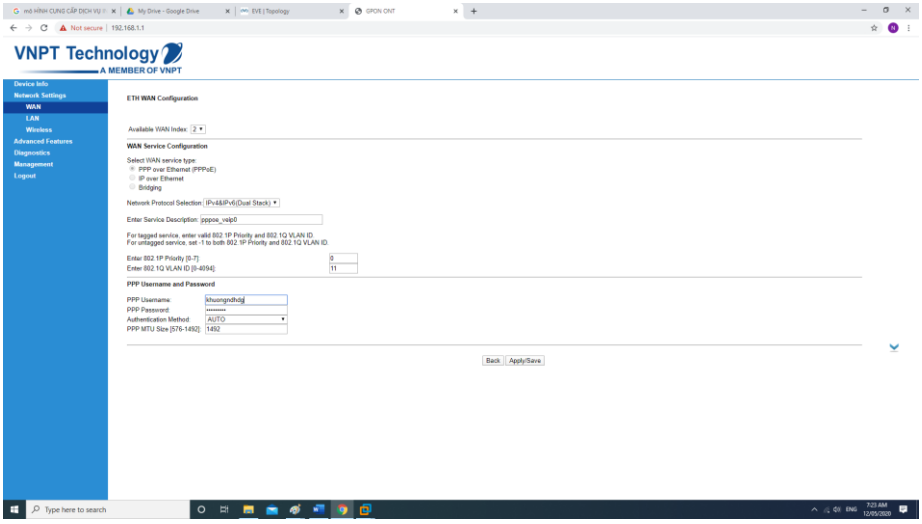
Với tập khách hàng ngày càng mở rộng và yêu cầu cao về chất lượng dịch vụ, cùng su hướng phát triển của Internet toàn cầu, VNPT nói chung và VNPT Hải Dương nói riêng định hướng triển khai Ipv6 đến tất cả khách hàng, phương thức cung cấp là Ipv6 – Ipv4 Dual – Stack.

3.1.2 Phương án cung cấp Ipv6 – Ipv4 Dual – Stack đến khách hàng

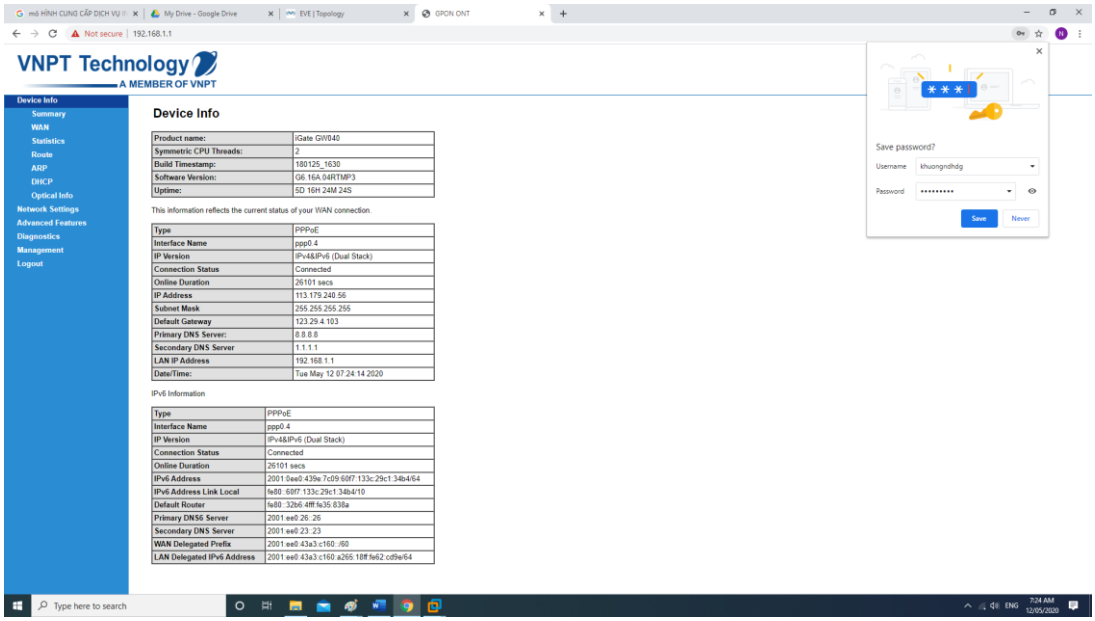
Áp dụng các phương pháp định tuyến như trong mô phỏng, IPv6 và OSPFv3, IPv4 và bật OSPFv2, kết hợp với DHCPv6 tại các BRAS, hiện tại VNPT Hải Dương đã cung cấp thành công đến mỗi ONU một Ipv6/60. Các thiết bị kết nối trực tiếp với ONU được cấp một Ipv6/64.



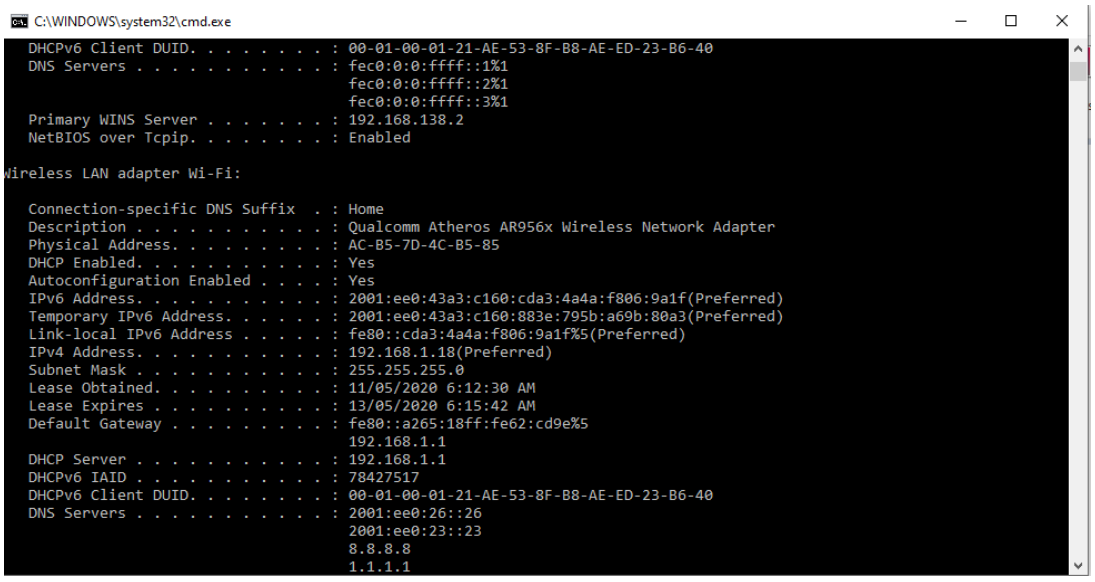
Hình 3. 2 Mô hình cung cấp Ipv6-Ipv4 Dual Stack tại VNPT Hải Dương.



Hình 3. 3 : Cấu hình thiết bị đầu cuối để triển khai Ipv6- Ipv4 Dual – Stack

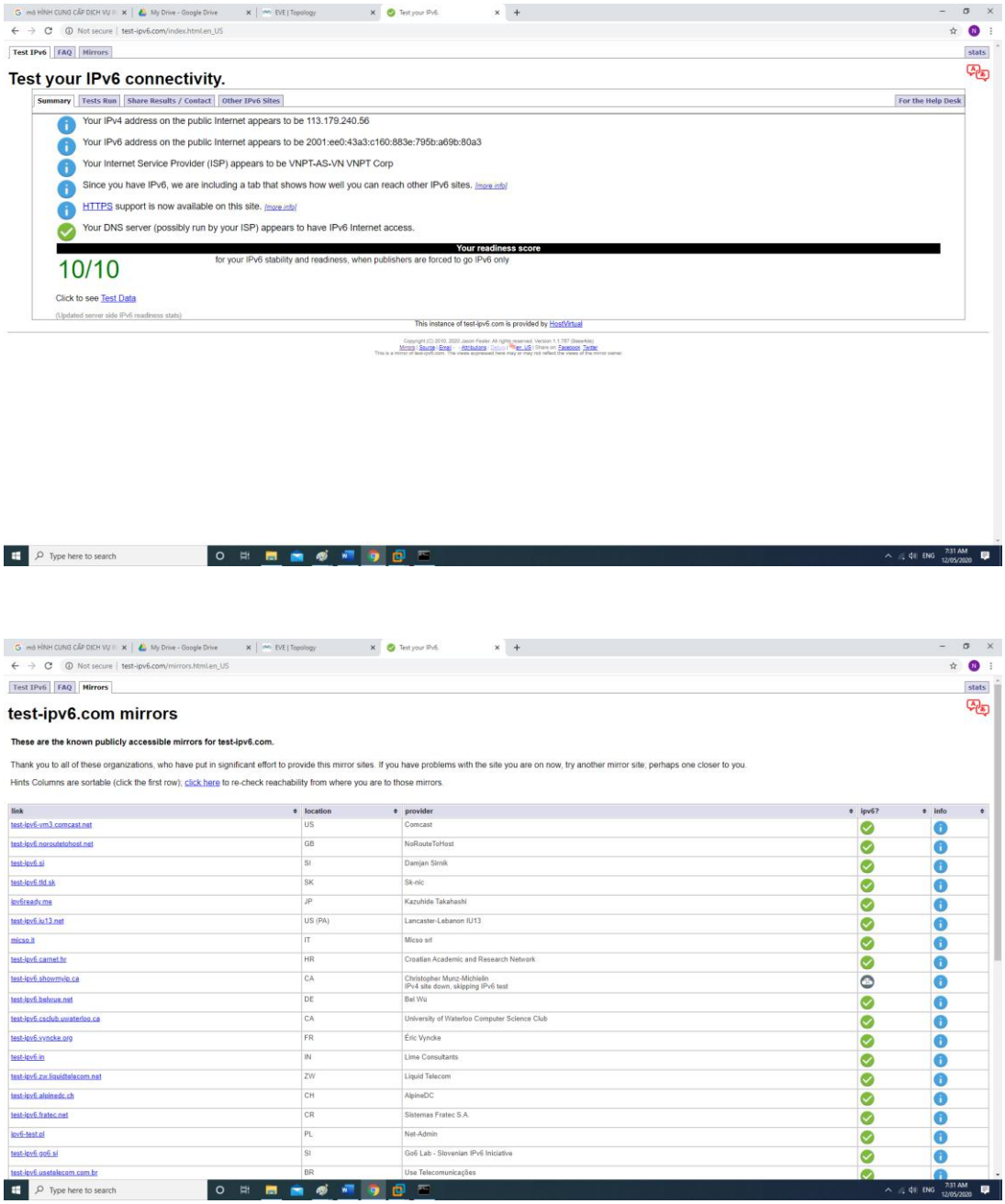


Hình 3. 4 : Các địa chỉ IP cấp cho ONU chạy Ipv6- Ipv4 Dual – Stack



Hình 3. 5: Ipv6- Ipv4 Dual – Stack tại các PC của khách hàng.

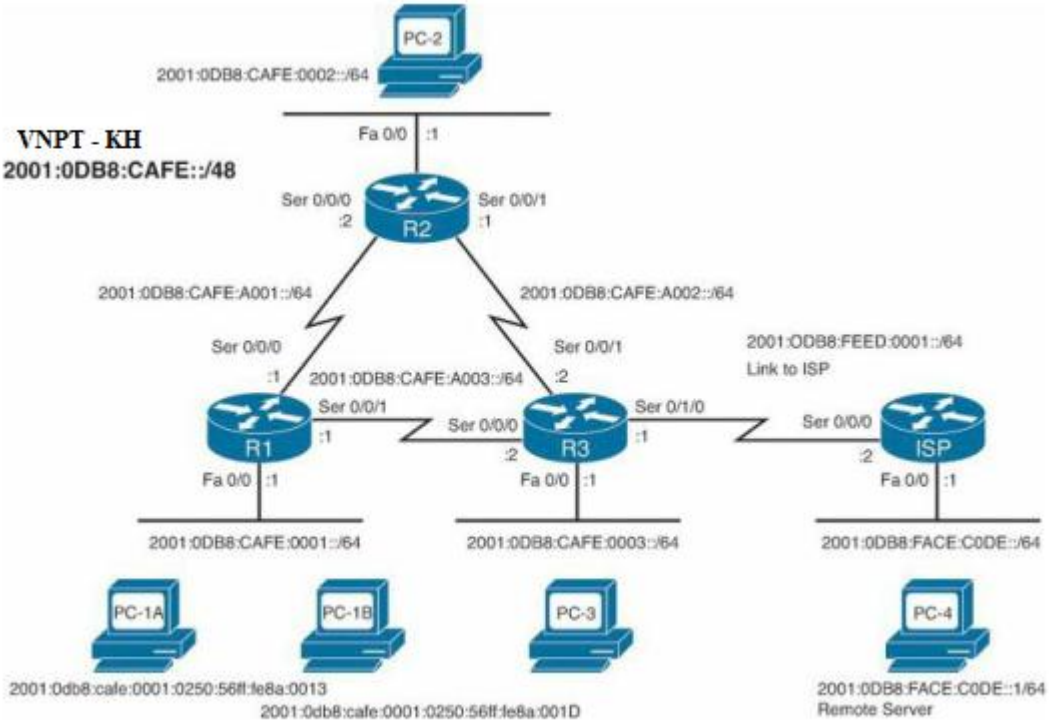
Sau khi chuyển đổi Ipv6- Ipv4 Dual – Stack đến k/h, kiểm tra kết nối Ipv6 và Ipv4 đến các server trong và ngoài nước.



Hình 3. 6: Kiểm tra kết nối ipv6 ipv4 đến các điểm test trong và ngoài nước

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. 7: Mô hình giả lập

+ 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

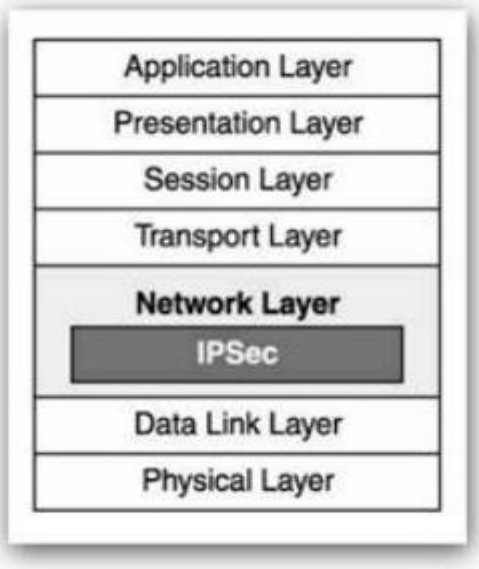
```
R2(config)# interface fastethernet 0/0
R2(config-if)# ipv6 address 2001:0db8:cafe:0002::1/64
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ipv6 address 2001:0db8:cafe:a001::2/64
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# ipv6 address 2001:0db8:cafe:a002::1/64
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#
```

3.3 Bảo mật trong IPv6

*** IP sec (IP security)**

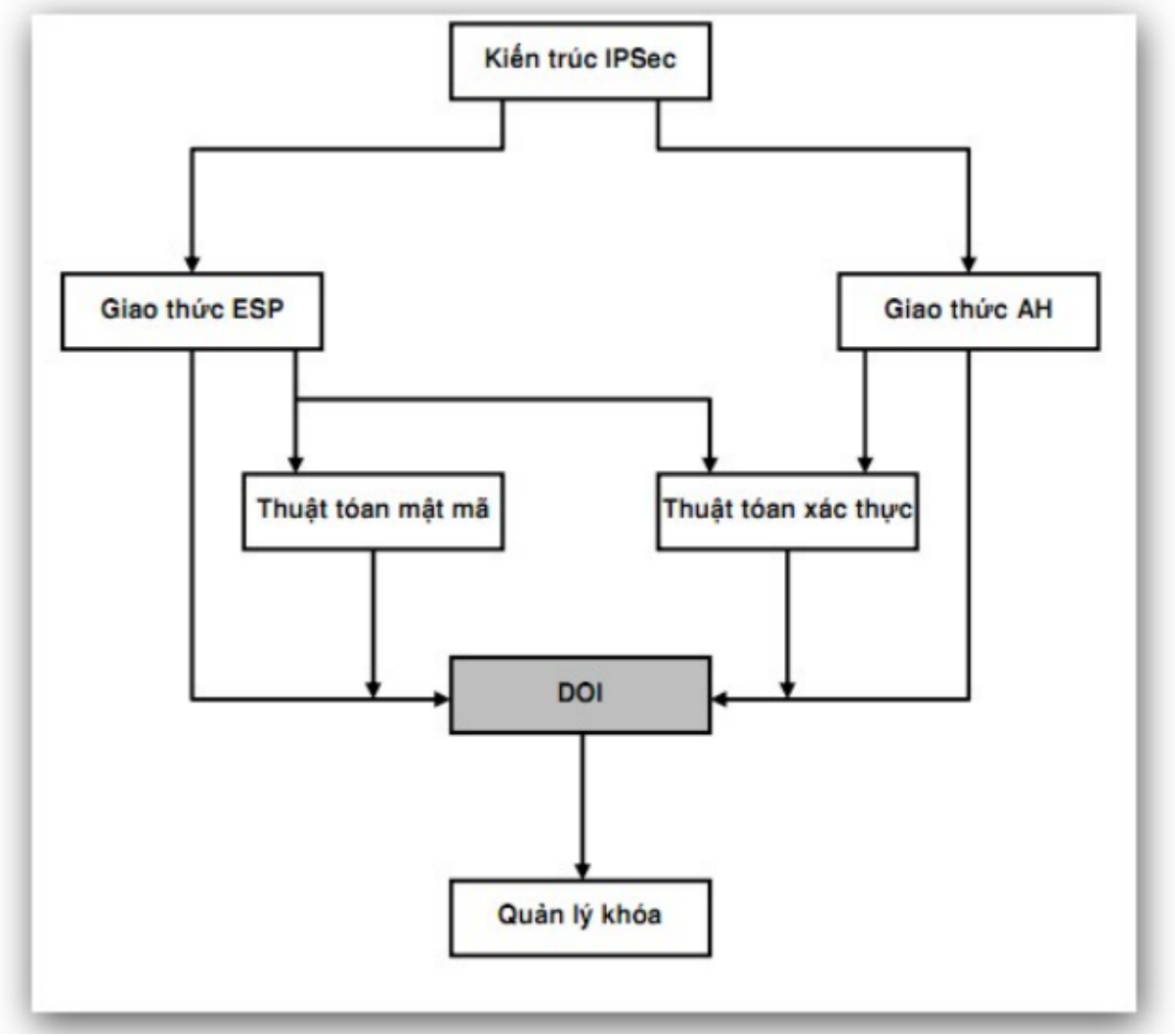
Giao thức IPsec được làm việc tại tầng Network Layer – layer 3 của mô hình OSI. Các giao thức bảo mật trên Internet khác như SSL, TLS và SSH, được thực hiện từ tầng transport layer trở lên (Từ tầng 4 tới tầng 7 mô hình OSI). Điều này tạo ra tính mềm dẻo cho IPsec, giao thức này có thể hoạt động từ tầng 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. 8: Kiến trúc mô hình OSI

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. 9: Kiến trúc 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).

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.

Em xin trân thành cám ơn./.

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