TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG

THỰC TẬP
TỐT NGHIỆP ĐẠI HỌC

Đề tài: TÌM HIỂU CÁC GIẢI PHÁP CHUYỂN ĐỔI TỪ IPv4 SANG IPv6

Sinh viên thực hiện: Nguyễn Văn Thuật

Lớp : DT5-K55

SHSV : 20102274

Giảng viên hướng dẫn: THS. PHÙNG THỊ KIỀU HÀ

Hà Nội, 3-2015

Lời nói đầu

Ngày nay, khoa học kỹ thuật đang diễn ra rất mạnh mẽ trên toàn thế giới thúc đẩy con người bước sang một kỷ nguyên mới, kỷ nguyên của cách mạng khoa học kỹ thuật. Trong đó , viễn thông và công nghệ thông tin là những ngành mũi nhọn thúc đẩy sự phát triển của một xã hội trong tương lai. Cùng với sự phát triển đó, mạng internet và cách mạng sử dụng giao thức IP cũng trở nên rất quan trọng trong cuộc sống xã hội. Ngay từ khi ra đời, giao thức IP đã thể hiện được những ưu điểm nhằm đáp ứng được nhu cầu kết nối và truyền tải thông tin của người sử dụng. Và điều này làm cho số lượng thiết bị sử dụng giao thức IP ngày càng gia tăng. Tuy nhiên, với tốc độ tăng quá nhanh đã làm cho giao thức IPv4 với không gian địa chỉ 32 bit không thể đáp ứng được sự phát triển của Internet, và giao thức IPv6 là phiên bản mới của giao thức IPv4 đã được thiết kế nhằm khắc phục được những hạn chế này. Vấn đề đặt ra là cần phải quá trình chuyển đổi từ giao thức IPv4 ngày nay sang giao thức IPv6.

Thủ tục IPv6 phát triển khi IPv4 đã được sử dụng rộng rãi, mạng lưới IPv4 Internet hoàn thiện, hoạt động tốt. Trong quá trình triển khai thế hệ địa chỉ IPv6 trên mạng Internet, không thể có một thời điểm nhất định mà tại đó, địa chỉ IPv4 được hủy bỏ, thay thế hoàn toàn bởi thế hệ địa chỉ mới IPv6. Hai thế hệ mạng IPv4, IPv6 sẽ cùng tồn tại trong một thời gian rất dài. Trong quá trình phát triển, các kết nối IPv6 sẽ tận dụng cơ sở hạ tầng sẵn có của IPv4. Do vậy, cần có những công nghệ phục vụ cho việc chuyển đổi từ địa chỉ IPv4 sang địa chỉ IPv6 và đảm bảo không phá vỡ cấu trúc Internet cũng như làm gián đoạn hoạt động của mạng Internet. Do đó em đã lựa chọn đề tài chuyển đổi từ IPv4 sang IPv6 làm đề tài thực tập tốt nghiệp.

Em xin trân trọng bày tỏ lòng biết ơn sâu sắc đến cô giáo ThS. Phùng Thị Kiều Hà- Bộ môn Hệ Thống Viễn Thông – Viện Điện Tử Viễn Thông – Đại Học Bách Khoa Hà Nội đã không tiếc thời gian công sức, tận tình giúp đỡ, chỉ bảo, hướng dẫn giúp em hoàn thành tốt đề tài này.

Em xin chân thành cảm ơn!

Hà Nội,18 tháng 3 năm 2012

Sinh viên thực hiện: Nguyễn Văn Thuật

Tóm tắt đồ án thực tập tốt nghiệp

Nội dung đồ án gồm 4 chương:

Chương 1: Giới thiệu tổng quan về giao thức IPv4 bao gồm cấu trúc gói tin, cấu trúc địa chỉ IPv4, các loại địa chỉ và cách dùng của từng loại địa chỉ.

Chương 2: Trình bày về giao thức IPv6 gồm cấu trúc gói tin IPv6, các trường trong IPv6 header, so sánh với IPv4 header, đặc điểm và cấu trúc của IPv6, các loại địa chỉ trong IPv6.

Chương 3: Trình bày các giải pháp chuyển đổi từ IPv4 sang IPv6 gồm có cơ chế Dual-stack, công nghệ biên dịch NAT-PT, công nghệ đường hầm tunneling. Ngoài ra, đi sâu tìm hiểu một số loại "Tunneling" đặc biệt.

Chương 4: Thực hiện mô phỏng mô hình tạo đường hầm "Tunneling" theo 2 cách khác nhau là static tunnel và 6to4 tunnel.

Mục lục

Danh sách hình vẽ

Danh sách bảng biểu

Chương1: Giao thức liên mạng IPv4

1.1 Tổng quan về IPv4

Giao thức IP là giao thức hệ thống mở phổ biến trên thế giới vì giao thức này được dùng để truyền thông qua bất cứ mạng nào được kết nối với nhau , nó phù hợp với mạng Lan và cả mạng Wan.

IP thực hiện hai chức năng cơ bản : định địa chỉ và phân đoạn. Các module liên mạng sử dụng các địa chỉ được mang trong phần mào đầu để truyền dẫn các gói dữ liệu đến đích của chúng. Việc phân đoạn và nối ghép lại các gói dữ liệu sử dụng các trường cong IP.

IP không có cơ cấu để tăng cường độ tin cậy dữ liệu end-to-end, điều khiển luồng, sắp xếp theo trình tự hoặc các dịch vụ khác trong các giao thức host-to-host. Tuy nhiên, IP có thể tận dụng các dịch vụ của các mạng để cung cấp các loại dịch vụ và chất lượng của dịch vụ đa mạng.

Các module liên mạng được sử dụng trong mỗi host được đặt trước trong liên mạng thông tin và trong mỗi bộ định tuyến liên kết các mạng. Những module này chia sẻ các quy tắc chung về việc phiên dịch các trường địa chỉ và vấn đề phân đoạn, nối lại các bản tin. Các module này có các thủ tục thực hiện các quyết định định tuyến và các chức năng khác.

IP xử lý mỗi gói tin như một thực thể độc lập không liên kết đến bất kỳ gói tin nào khác. Vì vậy, không có kết nối hoặc các mạch logic. IP sử dụng 4 cơ cấu chính trong việc cung cấp dịch vụ : loại dịch vụ, thời gian sống, tổng kiểm tra phần mào đầu, phần tùy chọn

- Thời gian sống : Xác định giới hạn thời gian để một gói tin được phép tồn tại trong mạng . Giá trị thời gian sống sẽ được thiết lập tại gởi và nó sẽ được giảm đi ở các điểm dọc tuyến nơi mà nó đi qua. Nếu thời gian sống đạt giá trị 0 trước khi đến đích, thì gói tin sẽ bị hủy. Time-to-live giống như cơ cấu tự hủy.
- Loại dịch vụ (Type of Service) : Xác định chất lượng dịch vụ được yêu cầu. Đây là bảng tóm tắt các đặc định được cung cấp cho các mạng hình thành liên mạng. Việc xác định loại dịch vụ được sử dụng tại bộ định tuyến để lựa chọn các tuyến kế tiếp khi chuyển tiếp gói tin.

Phần tùy chọn (Options) : Cung cấp cho các chức năng điều khiển cần thiết. Nó hữu ích trong một vài trường hợp không cần thiết cho hầu hết các truyền thông chung. Options tạo timestamp, security và việc định tuyến đặc biệt

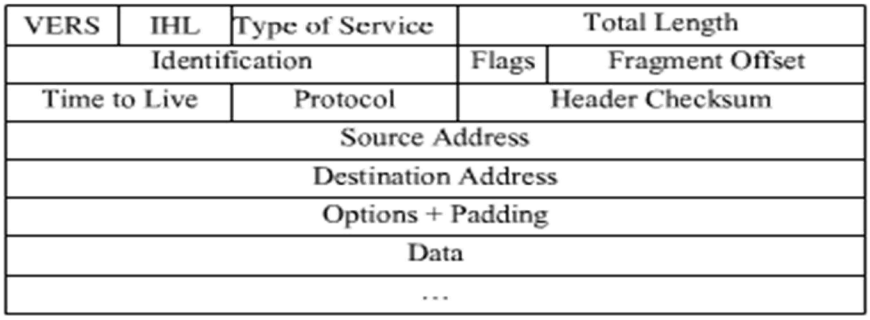
Tổng kiểm tra phần mào đầu (Header checksum): Cung cấp việc kiểm chứng thông tin trong gói tin đã truyền đúng. Nếu header checksum không đúng, thì gói tin bị hủy bỏ

1.2 Gói tin IPv4

1.2.1 Cấu trúc gói tin IP

Cũng giống như một khung truyền vật lý, một gói tin IP bao gồm hai phần, phần đầu và phần dữ liệu. Phần đầu của gói tin bao gồm địa chỉ nguồn, địa chỉ đích và một vùng kiểu để xác định nội dung của gói tin.

Cấu trúc các gói tin IPv4 được mô tả bằng hình vẽ :



Hình 1 : Cấu trúc gói tin IPv4

Các trường trong gói tin:

- Version
  Gồm 4 bit, trường này là phiên bản của giao thức IP đã dùng để tạo gói dữ liệu.
- IHL (IP header Length)
  Gồm 4 bit, cung cấp thông tin về độ dài phần đầu của gói dữ liệu.
- Type of Service
  Gồm 8 bit, dùng để xác định loại dịch vụ được truyền tải để xác định phương thức định tuyến gói tin phù hợp nhất.
- Total Length
  Gồm 16 bit, xác định tổng chiều dài của gói tin, bao gồm IP header và data. Kích thước tối đá của trường này là 2^16 = 65 535 octet.
- Identification

Gồm 16 bit, chưa một số nguyên duy nhất xác định gói tin. Mục đích của trường này là để máy đích biết các phân đoạn đến thuộc gói tin nào khi thực hiện ghép chúng lại.

- Flags

  Gồm 3 bit để điều khiển việc phân đoạn có cấu trúc như sau

0	DF	MF
0	1	2

  Bit 0 : chưa được sử dụng, luôn có giá trị 0.

  DF: chiều dài bit, nếu có giá trị 1 thì gói tin đó không được phép chia nhỏ.

  MF: dài 1 bit, nếu MF=1, điều này có nghĩa là còn có gói nhỏ sau nó trong thao tác phân mảnh gói tin, ngược lại MF=0 nghĩa là gói cuối cùng trong một loạt các gói nhỏ được phân mảnh.

- Fragment Offset

  Gồm 13 bit, xác định vị trí tương đối trong gói tin ban đầu của dữ liệu được truyền tải trong phân đoạn, được tính theo đơn vị 8 octet bắt đầu từ zero.

- Time to Live

  Gồm 8 bit, xác định thời gian lớn nhất mà một gói tin được phép tồn tại trên hệ thống mạng. Khi giá trị này bằng 0 thì gói dữ liệu sẽ bị hủy. Thời gian sống được đo bằng đơn vị giây. Mỗi gói dữ liệu đi qua một thực thể thì giá trị này sẽ bị giảm đi 1.

- Protocol

  Gồm 8 bit, xác định giao thức lớp trên nào được sử dụng để tạo thông điệp truyền tải trong vùng data của gói dữ liệu.

- Header Checksum

  Gồm 16 bit,

- Source Address

  Gồm 32 bit, chứa địa chỉ 32 bit của nơi gửi gói dữ liệu.

- Destination address

  Gồm 32 bit, chứa địa chỉ của nơi nhận gói dữ liệu.

- Option

  Trường này có thể có hoặc không trong gói dữ liệu. Các lựa chọn thêm vào chủ yếu cho việc kiểm tra và bắt lỗi trên mạng.

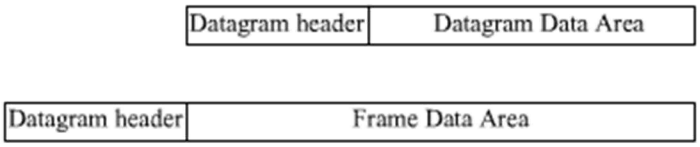
- Data

  Chứa thông tin của lớp trên.

Như vậy , tất cả các vùng trong phần đầu có độ dài cố định ngoại trừ vùng Options và vùng Padding tương ứng. Phần đầu thông thường nhất, không có Options và Padding, dài 20 Octets và có độ dài phần đầu bằng 5.

1.2.2 Đóng gói gói tin.

Khi gói tin di chuyển từ máy này sang máy khác, chúng phải di chuyển bởi mạng vật lý cơ sở. Mỗi gói tin được truyền tải trong một frame vật lý riêng biệt. Đối với mạng cơ sở, một gói tin giống như bất kỳ một thông điệp khác gửi tới một máy tới máy khác. Phần cứng không nhận biết định dạng gói tin, cũng như không biết địa chỉ IP đích. Việc đóng gói này mô tả bằng hình vẽ:



Hình 2 : Đóng gói gói tin

Từ hình vẽ ta thấy khi một máy gửi một gói tin IP tới máy khác, toàn bộ gói tin sẽ được di chuyển trong phần dữ liệu của frame mạng.

1.3 Cấu trúc địa chỉ IPv4

1.3.1 Các thành phần của địa chỉ IPv4

Cũng giống như các giao thức lớp mạng khác, địa chỉ IP dùng để định tuyến cho các gói tin IP đi đến đích mong muốn. Mỗi host trên mạng TCP/IP được ấn định một địa chỉ IPv4 duy nhất. Địa chỉ IPv4 gồm 2 phần:

Hình 3 :Thành phần địa chỉ IPv4

- Phần mạng (Network) : dùng để nhận dạng các mạng. Phần này do trung tâm liên mạng phân phối nếu đây là một mạng thành viên của internet.
- Phần host: dùng để nhận dạng host. Phần này được ấn định bởi các nhà quản lý mạng địa phương.

1.3.2 Khuôn dạng địa chỉ IPv4

Địa chỉ được phân thành 4 nhóm, mỗi nhóm 8 bit gọi là một octet. Các octet đặt cách nhau bằng một dấu chấm (.) và được thể hiện dưới dạng thập phân. Mỗi bit trong octet có một trọng số khác nhau (128,64,32,16,8,4,2,1). Giá trị thấp nhất của một octet là 0 (8 bit đều có giá trị 0) và giá trị cao nhất của một octet là 255 (giá trị tất cả các bit là 1). Khuôn dạng cơ bản của địa chỉ IP có thể được mô tả bằng hình vẽ:

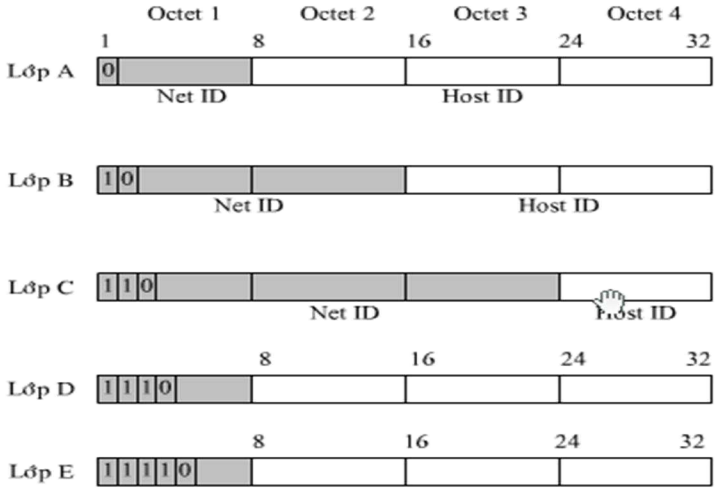
	Example			
An IP address is a 32-bit binary number	10101100	00010000	10000000	00010001
For readability, the 32-bit binary number can be divided into four 8-bit octets	10101100	00010000	10000000	00010001
Each octet (or byte) can be converted to decimal	172	16	128	17
The address can be written in dotted decimal notation	172.	16.	128.	17

Hình 4 **:** Khuôn dạng địa chỉ IP

Địa chỉ IP thường được biểu diễn dưới dạng thập phân để dễ nhớ. Có các phép toán giúp chuyển đổi địa chỉ từ dạng thập phân sang nhị phân và ngược lại.

1.3.3 Các lớp địa chỉ IPv4

Địa chỉ IP được chia ra thành 5 lớp: A,B,C,D,E.



Hình 5: Mô hình phân lớp của địa chỉ IP

Qua cấu trúc các lớp địa chỉ IP chúng ta thấy rằng:

- Bit nhận dạng là những bit đầu tiên : của lớp A là 0, lớp B là 10, lớp C là 110, lớp D có 4 bit đầu tiên là 1110, còn lớp E là 11110.
- Địa chỉ lớp A: địa chỉ net có 8 bit và địa chỉ host có 24 bit
- Địa chỉ lớp B: 16 bit net và 16 bit host
- Địa chỉ lớp C: 24 bit net và 8 bit host

Địa chỉ lớp	Vùng địa chỉ lý thuyết	Số mạng tối đa sử dụng	Số máy chủ tối đa trên từng mạng
A	Từ 0 .0.0.0 đến 127.0.0.0	126	16777214
B	Từ 128.0.0.0 đến 191.255.0.0	16382	65534
C	Từ 192.0.0.0 đến 223.255.255.0	2097150	254
D	Từ 224.0.0.0 đến 240.0.0.0	Không phân	Không phân
E	Từ 241.0.0.0 đến 255.0.0.0	Khôngphân	Không phân

Hình 6 : Phân lớp vùng địa chỉ

1.4 Các loại địa chỉ IPv4

1.4.1 Địa chỉ unicast

Đây là một loại địa chỉ xác định duy nhất cho một máy tính tham gia vào mạng Internet. Trong trường địa chỉ đích của phần mào đầu IP, nếu sử dụng một địa chỉ unicast, thì đích đến của gói IP chứa phần mào đầu này sẽ là một máy duy nhất trên mạng. Khi phát gói tin trên mạng, nếu dùng địa chỉ unicast thì việc tắc nghẽn ít xảy ra và ít tiêu tốn bang tần cho các loại gói tin này.

1.4.2 Địa chỉ broadcast

Địa chỉ IP broadcast có tất cả các bit thuộc phần host-ID đều bằng 1. Khi một gói được gửi đến một địa chỉ như thế, chỉ có một phiên bản của gói được truyền trên internet. Các bộ định tuyến trên Internet sẽ sử dụng phần Net-ID của địa chỉ khi chọn đường đi cho các gói, chúng không xem xét đến phần host-ID. Một khi gói dữ liệu đi đến được bộ định tuyến mà được nối trực tiếp vào mạng đích, bộ định tuyến này sẽ kiểm tra phần hót-ID của địa chỉ để xác định đích đến của gói tin. Nếu thấy tất cả các bit trong phần host-ID là 1, bộ định tuyến sẽ gửi broadcast gói dữ liệu với tất cả các host thuộc mạng đó.

Ngoài ra còn có địa chỉ broadcast cục bộ bao gồm 32 bit 1. Với loại địa chỉ này nó cho phép một máy được phát broadcast trong phạm vi một mạng cục bộ mà không cần biết địa chỉ cụ thể của mạng đó.

1.4.3 Địa chỉ multicast

Loại địa chỉ này cho phép phát các gói tin đến một nhóm các host. Địa chỉ này khác với địa chỉ broadcast ở chỗ là nó không phát gói tin đến toàn bộ các host có trong một mạng cụ thể, mà nó phát đến một nhóm các host có tham gia vào một địa chỉ multicast.

IP dành riêng các địa chỉ lớp D cho việc phát multicast. Miền địa chỉ multicast bao gồm 224.0.0.0 đến 239.255.255.255.

Chương 2: Giao thức IPv6

2.1 Tổng quan về IPv6

IPv6 là phiên bản mới của IPv4 được công bố chính thức năm 1981, nó thay thế cho IPv4. IPv6 ra đời đã mang lại nhiều ưu điểm nổi trội so với IPv4.

Ưu điểm nổi trội đầu tiên của IPv6 là cung cấp một không gian địa chỉ lớn hơn rất nhiều so với IPv4. Nếu IPv4 chỉ sử dụng 32 bit nhị phân để cấu thành địa chỉ IP, thì IPv6 sử dụng tới 128 bit nhị phân để cấu thành một địa chỉ IP. Với 32 bit nhị phân, không gian của IPv4 cung cấp được tối đa 2^32 địa chỉ, tức là xấp xỉ 4 tỉ địa chỉ IP; với 128 bit nhị phân, không gian IPv6 cung cấp được tối đa 2^128 địa chỉ, hay xấp xỉ 3,4.10^38 địa chỉ IP. Như vậy, với dân số thế giới vào năm 2013 là hơn 7 tỷ người, số lượng địa chỉ IPv6 được phân bổ cho từng người sẽ xấp xỉ 5.10^28 IP . Về mặt lý thuyết, sau khi triển khai xong IPv6, mỗi người trên Trái Đất có thể cấp phát 50 tỉ tỉ tỉ địa chỉ IP. Một con số vô cùng lớn và ta có thể xem như vô hạn.

2.1.1 Cấu trúc gói tin IPv6

Header IPv6 là một phiên bản được tổ chức lại của header IPv4. Nó loại trừ vùng không cần thiết hoặc ít có và thêm vào các vùng để cung cấp tốt hơn việc hỗ trợ "real-time traffic".

IPv6 Header	Extension header	Upper layer protocol data unit

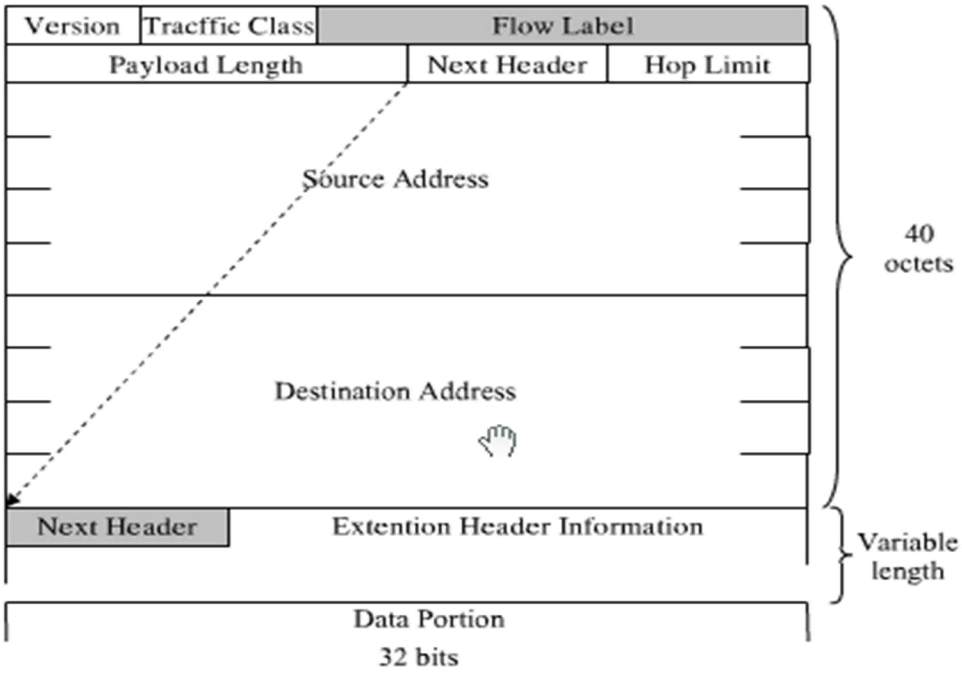
Hình 7 : Cấu trúc gói tin IPv6

- IPv6 header chiếm 40 byte, là phần mào đầu của gói tin.
- Extension header

  Vùng này có chiều dài thay đổi. Trong mỗi extension header có vùng next header , nó chỉ định ra vùng extension header tiếp theo. Extension header cuối cùng chỉ ra giao thức lớp trên (như TCP.UDP hoặc ICMPv6) bao gồm trong khối dữ liệu lớp trên
- Upper layer protocol data unit

  còn gọi là PDU (Protocol Data Unit), thường bao gồm header giao thức lớp trên . Thông thường , nó dài 65535 byte, payload lớn hơn 65535 byte trong phần Length có thể được dùng để gửi "Jumbo Payload Option" trong "Hop by hop Option Extension Header".

2.1.2 Cấu trúc IPv6 header



Hình 8 : Cấu trúc IPv6 heade

Header Ipv6 luôn luôn tồn tại và chiếm 40 byte. Vùng header trong IPv6 cụt thể gồm:

- Version : 4 bit được dùng để chỉ định phiên bản của IP là phiên bản 6
- Traffic class: chỉ định lớp hoặc mức độ ưu tiên của gói IPv6. Nó có kích thước là 8 bit. Trường này cung cấp các chức năng giống như trường type of service của IPv4. Giá trị của trường này không được định nghĩa. Tuy nhiên, nó được yêu cầu để cung cấp các ý nghĩa cho giao thức lớp ứng dụng để ghi rõ giá trị của trường traffic class cho việc thử nghiệm.
- Flow label: chỉ định gói dữ liệu thuộc chỉ số đặc biệt trong các gói giữa nguồn và đích, yêu cầu điều khiển đặc biệt bằng các router IPv6 trung gian. Trường này gồm 20 bit. Flow label được sử dụng để nâng cao chất lượng của các dịch vụ kết nối, như những loại cần thiết bằng giữ liệu thời gian thực (real-time data) như voice và video. Trường hợp điều khiển của router không đủ, flow label được thiết lập giá trị 0. Lúc này, ở router này có thể có nhiều luồng giữa một nguồn và đích.
- Payload length: Chỉ định độ dài của payload IPv6. Trường này có kích thước 16 bit. Trường này bao gồm Extension Headers và PDU lớp cao hơn. Với 16 bit, Payload IPv6 tương đương 65535 byte có thể chỉ định. Trường hợp độ dài lớn hơn 65535 byte, trường này sẽ thiết lập trạng thái 0 và

"Jumbo payload Option" được sử dụng trong "Hop-by-Hop Option Extension Header".

- Hop Limit: chỉ định số lớn nhất của các liên kết mà gói IPv6 có thể truyền trước khi bị hủy. trường này có kích thước là 8 bit. Trường này giống với trường TTL của IPv4. Khi hop limit bằng 0, một bản tin ICMPv6 được gửi đến địa chỉ nguồn và gói dữ liệu sẽ bị hủy.
- Source address: lưu trữ địa chỉ IPv6 host gửi. kích thước 128 bit
- Destination address: lưu trữ địa chỉ IPv6 của host đích. (128 bit).
- Giá trị của trường "NEXT HEADER"

Giá trị	Header
0	Hop by hop Option header
6	TCP
17	UDP
41	Encapsulated IPv6 header
43	Routing header
44	Fragment header
46	Resource reservation protocol
50	Encapsulating security payload
51	Authentication header
58	ICMPv6
59	No next header
60	Destination option header

Bảng 1 : Giá trị trường Next Header

2.1.3 So sánh Header IPv4 và Header IPv6

Trường IPv4 header	Trường IPv6 header
Version	Trường này giống nhau nhưng các số phiên bản thì khác nhau
IHL(internet header length)	Không có trong IPv6. IPv6 không có trường này vì IPv6 luôn luôn có kích thước gắn vào là 40
Type of service	Được thay thế bằng trường traffic class trong IPv6
Total length	Được thay thế bằng trường Payload Length, nó chỉ xác định kích thước của payload
Identification Fragmentation Flags Fragmentation Offset	Không có trong IPv6. Thông tin về phân đoạn không nằm trong header IPv6 mà nó có chưa trong "Fragment

	Extension Header".
Time to live	Được thay thế bằng trường hop limit trong IPv6
Protocol	Được thay thế bằng trường next header
Header checksum	Không có trong IPv6. Trong IPv6, việc phát hiện lỗi gói IPv6 được thực hiện bởi lớp vật lý
Source Address	Trường này thì giống nhau ngoại trừ địa chỉ IPv6 dài tới 128 bit.
Option	Không có trong IPv6, Option của IPv4 được thay thế bằng "Extension Header".

Bảng 2 : So sánh header IPv4 và header IPv6

2.2 Đặc điểm địa chỉ IPv6

Giao thức IPv6 có những đặc điểm:

- Dạng header mới
- Không gian địa chỉ lớn
- Có hiệu quả, phân cấp địa chỉ và việc định tuyến hạ tầng kiến trúc.
- Cấu hình địa chỉ stateful hoặc stateless.
- Gắn liền với sự an toàn
- Hỗ trợ tốt hơn cho QoS
- Giao thức mới cho việc tác động qua lại giữa các node mạng gần nhau.
- Có thể mở rộng

2.2.1 Dạng header mới

Header có dạng mới là được thiết kế để giữ Header ở phần đầu sao cho nhỏ nhất. Điều này đạt được khi di chuyển cả vùng Padding và vùng Option để kéo dài phần phía sau phần đầu của Header.

Header Ipv6 chỉ lớn bằng 2 lần header IPv4, còn không gian thì bằng 4 lần địa chỉ IPv4.

2.2.2 Không gian địa chỉ rộng

Ipv6 có phần địa chỉ IP 128 bit (16 byte) nguồn và địa chỉ IP đích. Mặc dù 128 bit rõ rang có thể trên 3,4.10^38 khả năng kết hợp, không gian địa chỉ rộng của IPv6 được thiết kế cho nhiều mức mạng con và địa chỉ cục bộ từ mạng internet chính đến các mạng cá

nhân trong một tổ chức.chỉ có một số nhỏ các địa chỉ được chỉ định để dùng cho các host, có nhiều địa chỉ sẵn có cho tương tai sử dụng. với một số lớn các địa chỉ sẵn có, kỹ thuật giữ địa chỉ, cũng như triển khai của NAT, là không cần thiết lâu dài.

2.2.3 Có hiệu quả, phân cấp địa chỉ và việc định tuyến hạ tầng kiến trúc

Địa chỉ toàn cầu IPv6 sử dụng trên phần IPv6 của internet được thiết kế đã tạo ra một hiệu suất cao và hạ tầng kiến trúc định tuyến là cơ sở chung việc xảy ra nhiều mức mà dịch vụ internet cung cấp.

2.2.4 Cấu hình địa chỉ stateful hoặc stateless

Để cấu hình host đơn, IPv6 hỗ trợ cả cấu hình địa chỉ stateful, cũng như cấu hình địa chỉ với sự có mặt của dịch vụ DHCP và cấu hình địa chỉ Stateless, các Host trên đường truyền tự động cấu tạo bản thân chúng với địa chỉ IPv6 cho đường truyền và các địa chỉ nhận được từ tiền tố báo cho biết bởi các Router cục bộ. Cùng trong sự vắng mặt của Router, các host trên đường truyền giống nhau có thể tự động cấu tạo bản thân chúng với các địa chỉ đường truyền cục bộ và truyền thông tin bên ngoài cấu hình nhân công.

2.2.5 Tăng cường bảo mật

Hỗ trợ IPSec là một yêu cầu của bộ giao thức IPv6. Yêu cầu này cung cấp phương thức cơ bản tiêu chuẩn cho mạng đảm bảo an toàn là cần thiết.

2.2.6 Hỗ trợ tốt hơn cho QoS

Các vùng mới trong IPv6 header định nghĩa như thế nào sự vận chuyển được điều khiểu và nhận biết. Nhận biết sự vận chuyển thì sử dụng một vùng nhãn lưu lượng trong IPv6 Header để cho các Router nhận ra và cung cấp điều khiển đặc biệt cho gói thuộc về một lưu lượng, một chuỗi các gói giữa một nguồn và đích. Vì sự vận chuyển được nhận biết trong IPv6 Header, nên nó hỗ trợ cho QoS có thể đạt được cao khi gói tải được mã hóa xuyên qua IPSec.

2.2.7 Giao thức mới cho việc tác động qua lại giữa các node mạng gần nhau

Giao thức phát hiện các máy gần đó là một chuỗi các thông điệp giao thức thức điều khiển lỗi IPv6 (ICMPv6) nó quản lý hoạt động của các node mạng bên cạnh. Việc phát hiện ra máy bên cạnh thay thế mạng cơ bản ARP (Address Resolution Protocol).

2.2.8 Có thể mở rộng

Ipv6 dễ dàng mở rộng trong tương lai bằng cách coongjt hêm phần đầu vào sau IPv6 header. Không giống Option trong IPv4 header, nó chỉ có thể hỗ trợ 40 byte Option, còn kích thước của IPv6 mở rộng phần đầu chỉ là ép buộc bởi kích thước IPv6.

2.3 Địa chỉ IPv6

2.3.1 Cấu trúc địa chỉ IPv6

Địa chỉ IPv6 là một dãy nhị phân dài 128 bit, được thể hiện dưới dạng hexa trong các giao diện với người dùng. Cứ 4 bit nhị phân ta đổi sang được một số hexa nên một địa chỉ IPv6 sẽ được biểu diễn thành 32 số hexa. 32 số hexa này lại được chia thành 8 cụm 4 số gọi là các trường (field).

Ví dụ : 1021:2312:3212:1000:0000:3212:786A:AB21

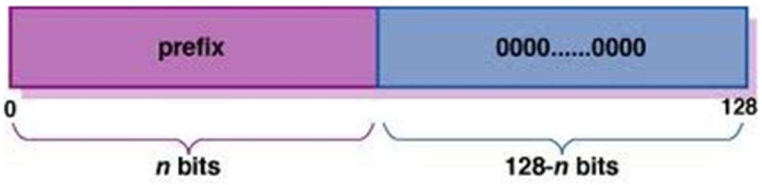
Địa chỉ IPv6 rất dài, khó ghi chép nên có một vài luật cho phép rút gọn địa chỉ IPv6:

- Các số 0 dẫn đầu trong một trường được quyền lược bỏ
- Các trường 0 liên tiếp của một địa chỉ IPv6 được phép thay thế bằng một cụm hai dấu chấm "::", và chỉ được thay thế một lần duy nhất cho một địa chỉ.

  Ví dụ rút gọn địa chỉ IPv6:
  Địa chỉ "2001:0001:0000:0000:0000:0002:AB00:0012" có thể rút gọn như sau:
  2001:1:0:0:0:2:AB00:12 hoặc
  2001:1::2:AB00:12

Địa chỉ IPv6 cũng được chia thành hai phần giống như IPv4 nhưng không dùng tên gọi là "phần Network" và "phần Host" mà có tên là "phần Prefix" và "phần interface-id" (hình 9). Địa chỉ IPv6 cũng không sử dụng subnet-mask mà sử dụng phương thức biểu diễn đính kèm prefix-length.

Ví dụ :2001:1A21:2311:3211::1/64



Hình 9 : Phần prefix và interface-id

2.3.2 Các loại địa chỉ IPv6

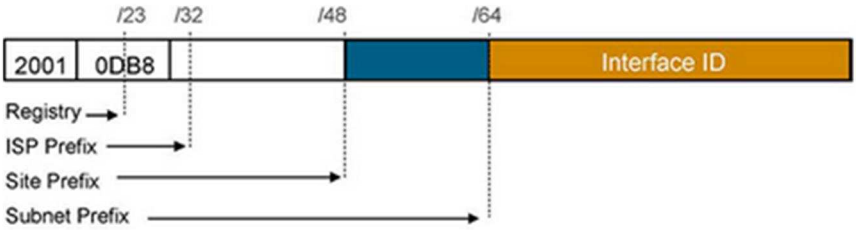
2.3.2.1 Địa chỉ Unicast

Là địa chỉ sử dụng được cho một host, dùng trong trao đổi dữ liệu unicast. Dải địa chỉ Unicast của không gian IPv6 lại được chia thành 3 dải unicast khác nhau:

a. Global Unicast

Là dải IP được cấp phát và sử dụng được trên Internet, dải này tương đương với dải IP Public của không gian IPv4. Mọi địa chỉ Global unicast đều bắt đầu bằng 3 bit "001", và như vậy các địa chỉ loại này thuộc về dải 2000::/3, bao gồm các địa chỉ từ 2000:: đến 3FFF::.

Việc cấp phát IPv6 Global unicast được thực hiện theo cơ chế phân cấp (hierachical) (hình 10), thông qua các cơ quan đăng ký Internet cấp vùng như ARIN hay APNIC,….



Hình 10 : Phân cấp địa chỉ IPv6 global unicast

Mặc dù dải Global unicast là một dải đặc biệt lớn chiếm tới 1/8 tổng số địa chỉ của không gian IPv6 nhưng hiện tại mới chỉ có dải 2001::/16 đang được cấp phát. Một số dải Global unicast khác được sử dụng cho những mục đích đặc biệt, ví dụ: dải 2002::/16 được sử dụng cho kỹ thuật 6to4 tunnel.

b. Link-local Unicast

Địa chỉ link – local là loại địa chỉ chỉ sử dụng trên nội bộ một đường link, các gói tin với các địa chỉ link – local không thể đi qua lại được giữa các interface và vì vậy các địa chỉ link – local có thể trùng nhau miễn là chúng được đặt trên các link khác nhau.

Các địa chỉ link – local thuộc về dải IPv6 FE80::/10. Dải link – local này tương đương với dải IP 169.254.0.0/16 của IPv4.

Các gói tin với địa chỉ link – local hầu hết được sử dụng bởi hoạt động trao đổi thông tin trên nội bộ đường link của các giao thức control – plane của router, ví dụ như các giao thức định tuyến. Khi một interface được kích hoạt sử dụng IPv6, một địa chỉ link – local sẽ được tự động phát sinh ra trên interface ấy.

c. Unique-local Unicast

Được định nghĩa trong RFC – 4193, là dải địa chỉ tương đương với dải IP Private trong không gian IPv4. Giống như IPv4 Private, địa chỉ Unique – local chỉ được sử dụng

trong nội bộ mạng doanh nghiệp, có thể sử dụng đi sử dụng lại cùng một dải từ mạng nội bộ này qua mạng nội bộ khác và không được sử dụng trên môi trường Internet.

Địa chỉ Unique – local là toàn bộ dải FC00::/7.

2.3.2.2 Địa chỉ Multicast

Trong IPv4, dải IP dùng cho multicast là IP lớp D từ 224.0.0.0 đến 239.255.255.255. Trong IPv6, địa chỉ multicast là tất cả các IP nằm trong dải FF00::/8. Nói cách khác, một địa chỉ IPv6 multicast luôn luôn có byte đầu tiên có giá trị là FF. Một vài địa chỉ IPv6 Multicast thường gặp trong các ứng dụng mạng:

Địa chỉ	*Ứng dụng*
FF02::1	Tất cả các host trên link
FF02::2	Tất cả các router trên link
FF02::5,FF02::6	OSPFv3
FF02::9	RIPng
FF02::A	EIGRPv6

Bảng 3 : Một số địa chỉ multicast thông dụng

2.3.2.3 Địa chỉ Anycast

Chính là dải địa chỉ Global unicast (2000::/3) nhưng mỗi địa chỉ trên dải này được phép đặt trên nhiều host của mạng IP.

Chương 3: Giải pháp chuyển đổi từ IPv4 sang IPv6

3.1 Lý do chuyển đổi từ IPv4 sang IPv6

Hiện nay không gian IPv4 trên toàn cầu đã cạn kiệt. Vào tháng 02/2011, tổ chức IANA (Internet Assigned Numbers Authority), tổ chức quản lý địa chỉ IP và số hiệu mạng trên toàn thế giới đã công bố rằng địa chỉ IPv4 đã được cấp phát hết. Dải IPv4 còn sử dụng đến ngày nay đều nằm trong kho IP của các cơ quan quản lý IP cấp vùng hoặc các ISP; không còn IP mới để cấp phát. Việc sử dụng IPv4 hiện nay đều được các ISP quy hoạch hết sức cẩn thận để không gây lãng phí một tài nguyên mạng đã cạn kiệt.

Mặc dù đã dùng rất nhiều các biện pháp như sử dụng CIDR cho giao thức IPv4 và chia không gian IPv4 thành hai không gian Private IP và Public IP đồng thời sử dụng kỹ thuật NAT để chuyển đổi Private-Public. Nhưng cuối cùng không gian IP vẫn cạn kiệt. Để giải quyết triệt để "vấn nạn" thiếu hụt IP cũng như khắc phục những hạn chế vốn có của giao thức IPv4 cũ, một phiên bản mới hoàn toàn của giao thức IP đã được phát triển và đưa vào sử dụng. Phiên bản mới của giao thức IP này được gọi là IP version 6 – IPv6.

Ngoài lý do, địa chỉ IPv4 đã hết thì về mặt hoạt động, IPv6 cũng cải tiến rất nhiều điểm từ IPv4:

- *Tích hợp trong giao thức IP các cơ chế Mobile – IP và IP Security:* Với IPv4, để có thể sử dụng được các tính năng này, các thiết bị mạng phải chạy các hệ điều hành có tích hợp các module phần mềm tương ứng. Với IPv6, các tính năng này được tích hợp sẵn trong giao thức IP, các hệ điều hành có hỗ trợ IPv6 mặc định có thể sử dụng các tính năng này.
- *Không sử dụng địa chỉ Broadcast*: IPv6 không sử dụng địa chỉ Broadcast như với IPv4. IPv6 chỉ sử dụng cơ chế Multicast cho các hoạt động trao đổi dữ liệu theo nhóm.
- *Sử dụng gói tin với cấu trúc header đơn giản hơn nhưng hiệu quả hơn so với IPv4:* Số lượng trường thông tin được giảm hẳn, một số trường không còn cần thiết được lược bỏ, một số trường mới được thêm vào. Với header đơn giản hơn, hiệu suất của các hoạt động chuyển mạch và định tuyến trên các thiết bị lớp 3 sẽ tăng lên đáng kể.

Tuy mang nhiều ưu điểm xuất sắc như trên nhưng không dễ dàng để chỉ trong một thời gian ngắn IPv6 có thể thay thế hoàn toàn cho IPv4. Thực ra, cũng không có bất kỳ

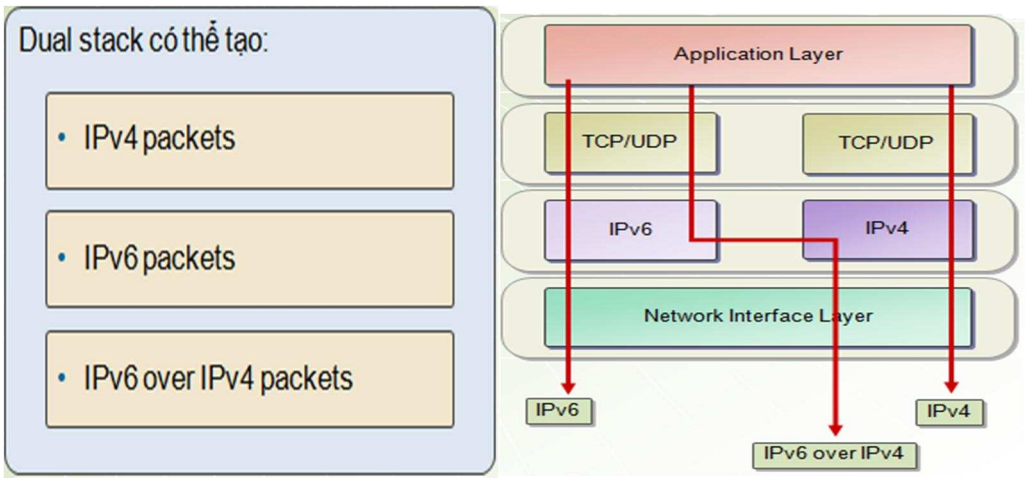
một quy định ràng buộc nào được đưa ra để yêu cầu chuyển đổi ngay từ IPv4 sang IPv6 và quá trình chuyển đổi hiện nay trên thế giới cũng đang diễn ra một cách từ tốn, chậm rãi nhưng chắc chắn và hoàn toàn trong suốt với người dùng. Có nhiều phương pháp chuyển đổi được đưa ra để hỗ trợ cho quá trình chuyển đổi này:

- *Dual – Stack:* Mạng sẽ vừa chạy IPv4 vừa chạy IPv6 trong quá trình chuyển đổi.
- *Các kỹ thuật Tunnel:* Giúp cho các host IPv6 có thể trao đổi dữ liệu với nhau thông qua một hệ thống mạng IPv4.
- *NAT – PT:* Giúp cho một host IPv6 có thể trao đổi dữ liệu với một host IPv4

3.2 Các giải pháp chuyển đổi từ IPv4 sang IPv6

3.2.1 Cơ chế Dual stack

Dual-stack là hình thức thực thi TCP/IP bao gồm cả tầng IP của IPv4 và IP của IPv6. Thiết bị hỗ trợ cả 2 giao thức IPv4 và IPv6, cho phép hệ điều hành hay ứng dụng lựa chọn một trong hai giao thức cho từng phiên liên lạc. Sự lựa chọn giao thức nào để sử dụng trong tầng internet sẽ dựa vào thông tin được cung cấp bởi dịch vụ named qua DNS server.



Hình 11 : Cơ chế Dual-stack

Cơ chế này được gọi là "thẳng hướng" nhất để đảm bảo một nodes IPv6 hoàn toàn tương thích với những node IPv4 khác. Những node vừa hỗ trợ IPv6 vừa hỗ trợ IPv4 như

vậy gọi là IPv4/IPv6. Những node này vừa có khả năng gửi và nhận cả gói tin IPv4 và IPv6. Chúng có thể làm việc trực tiếp với các host thuần IPv4 qua các giao thức IPv4 , lại vừa có thể làm việc trực tiếp với các host IPv6 chạy giao tức IPv6. Hạn chế mô hình Dual-stack là phải gán thêm một địa chỉ Ipv4 đối với mỗi node IPv6 mới.

Đối với mỗi host sử dụng kỹ thuật Dual IP Layer, có thể kết hợp với cơ chế chuyển đổi IPv6 over IPv4 Tunneling. Đối với những node này, có thể sử dụng kết hợp với các cơ chế Tunneling tự động hoặc Tunneling tĩnh, hoặc cả hai kỹ thuật này. Do đó có 3 cơ chế chuyển đổi đối với mỗi node IPv4/IPv6 là:

- Node IPv4/IPv6 không kết hợp sử dụng kỹ thuật Tunneling
- Nodes IPv4/IPv6 sử dụng kết hợp Tunneling tĩnh
- Nodes IPv4/IPv6 sử dụng kết hợp cả Tunneling tĩnh và động.

Để triển khai mạng Ipv6 trong mạng LAN, người ta thường vận dụng mô hình Dual-stack "hạn chế". Mô hình Dual-stack "hạn chế" được mô tả như sau: Một site khi thiết kế theo mô hình Dual-stack chỉ có những node làm "sever" là các node "dual-stack". Những node đóng vai trò Client chỉ là những node thuần IPv6. Node server đóng vai trò là điểm cung cấp các dịch vụ như DNS, Web, file sharing… Với phương thức này, chỉ có một địa chỉ IPv4 được gán cho server, giảm thiểu các địa chỉ IPv4 gán cho các node trong site.

Đối với một host/router khi hỗ trợ cả Dual-stack IP song song cần phải điều khiển hai bộ dịa chỉ khác nhau, nhưng các giao thức Automatic Neighbour Discovery của IPv6 nên làm cho stack này là trong suốt đối với nhà quản lý. Đặc biệt nếu như chúng ta muốn so sánh nó với các giá của việc cấu hình các trạm IPv5 ngày nay. Việc nâng cấp router để hỗ trợ IPv6 phức tạp hơn. Các router phải được trang bị mã để forward các gói IPv6, trang bị các giao thức định tuyến IPv6 và giao thức quản lý IPv6.

Các máy chủ Dual-stack sẽ sử dụng các giao thức Lookup ngược mới. Chúng sẽ nhặt ra các địa chỉ tốt nhất ngoài danh sách được trả về và sử dụng các địa chỉ này trong yêu cầu kết nối TCP hoặc coi như các địa chỉ đích cho các gói tin UDP. Các giao thức vận chuyển Dual-stack sẽ quyết định hoặc sử dụng Ipv6 nếu như các địa chỉ là thuần IPv6 howacj đơn giản chỉ dùng địa chỉ Ipv4 nếu nhue các địa chỉ là địa chỉ được map bởi Ipv4. Theo quá trình thực hiện, sự tăng lên của các máy chủ Internet sẽ đáp ứng cho các địa chỉ Ipv6 và chuyển đổi vào DNS. Sự chuyển tiếp (Ipv4 sang Ipv6) sẽ xảy ra một cách tự nhiên, ngày càng nhiều kết nối sử dụng Ipv6. Sẽ không có bất kỳ một ngày nào mà việc thay thế này trở nên rõ nét tuy nhiên cuối cùng việc thay thế này sẽ bao phủ toàn bộ. Các thủ tục DNS là trong suốt với bản ghi. Chỉ server và giao diện nào mà cần cung cấp hoặc truy nhập tới địa chỉ IPv6 mới phải được nâng cấp.

Các yêu cầu để thực hiện cơ chế Dual-stack:

Thông số	Giá trị
Phạm vi áp dụng	Site
Địa chỉ Ipv4 cần gán	Một địa chỉ đối với một host, nhiều địa chỉ đối với Router
Yêu cầu đối với host	Cài đặt cả IPv4/Ipv6
Yêu cầu đối với Router	Cài đặt cả IPv4/Ipv6 , các giao thức định tuyến phải hỗ trợ cả Ipv6

Bảng 4 : Các yêu cầu để thực hiện Dual-stack

Yêu cầu về gán địa chỉ: Vì các host này sử dụng cả giao thức ở tầng IP là IPv4 và Ipv6, do vậy cần gán cả hai loại địa chỉ Ipv4 và Ipv6 ở mỗi host này. Không nhất thiết phải có sự quan hệ giữa hai địa chỉ này. Do vậy, những host IPv4/IPv6 có thể gán những địa chỉ Ipv4 và IPv6 không có quan hệ với nhau. Đối với những node có cơ chế chuyển đổi này cần gán một địa chỉ Ipv6 được tạo bởi địa chỉ IPv4 gán đối với host đó. Đối với những node Ipv4/Ipv6, có thể có địa chỉ Ipv4 theo bất kỳ một giao thức cấu hình địa chỉ Ipv4 nào hợp lệ. Đối với địa chỉ loopback, theo cấu hình địa chỉ IPv4, địa chỉ loopback sẽ có dạng 127.0.0.1; địa chỉ chuyển sang Ipv6 có dạng ::127.0.0.1.

Khai báo DNS : trong một hệ thống có cài đặt các node hỗ trợ cơ chế Dual-stack thì điều kiện tối thiểu cần thiết là dịch vụ DNS của hệ thống phải hỗ trợ IPv6. Đối với các nodes IPv4/IPv6 cần phải khai báo cả hai loại bản ghi trong DNS server. Hay nói cách khác là cần phải cấu hình DNS đối với cả hai loại địa chỉ mà host đó được gán. Đối với mỗi địa chỉ IPv6, cấu trúc bản ghi DNS có dạng AAA. Đối với mỗi địa chỉ IPv4, cấu trúc bản ghi DNS có dạng A.

3.2.2 Công nghệ biên dịch NAT-PT

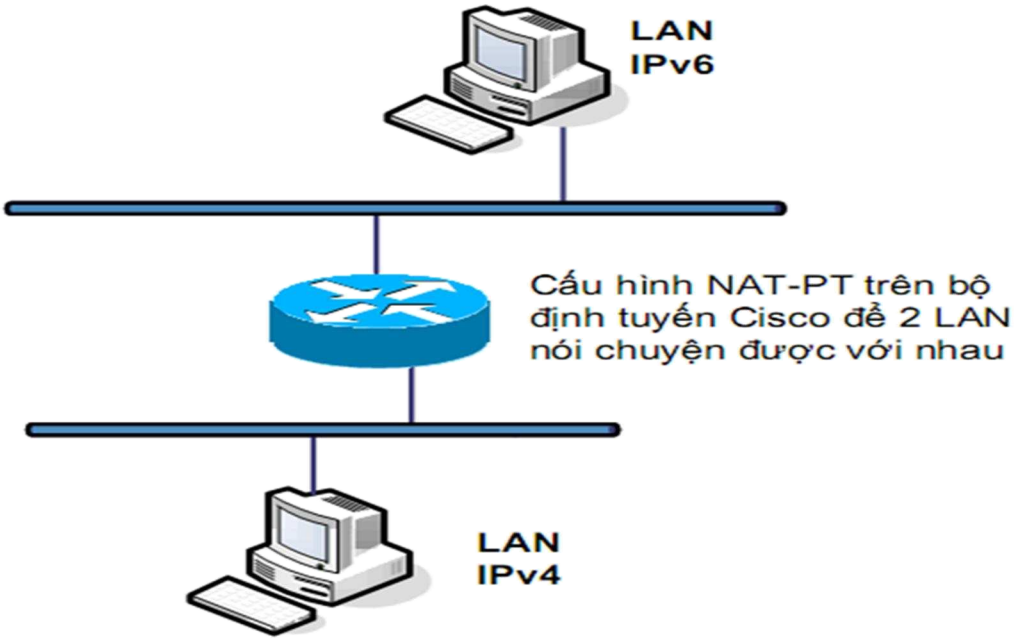
NAT-PT được phát triển trên cơ sở cơ chế NAT trong IPv4 nhằmcho phép các nút mạng IPv4 và IPv6 kết nối với nhau. Cơ chế này hoạtđộng trên cơ sở chuyển đổi các khác biệt giữa các gói tin IPv4 và IPv6:

- Khác biệt về địa chỉ: Dịch địa chỉ IPv4 - IPv6.
- Khác biệt về phần mở đầu header: Dịch giao thức thay đổi header gói tin.

Thiết bị NAT-PT được cài đặt tại ranh giới giữa mạng IPv4 với IPv6.Cơ chế này không đòi hỏi cấu hịnh đặc biệt tại các máy trạm và sự chuyểnđổi gói tin tại thiết bị NAT-PT hoàn toàn thông suốt với người dùngMỗi thiết bị NAT-PT duy trì một tập các địa chỉ IPv4 dùng để ánh xạcác yêu cầu với địa chỉ IPv6 NAT-PT có thể mở rộng thành

Network Address Port Translation -Protocol Translation (NAPT-PT) cho phép sử dụng một địa chỉ IPv4 chonhiều phiên làm việc khác nhau

Mô hình NAT-PT



Hình 12 : Mô hình NAT-PT

Để router có thể dịch địa chỉ từ IPv4 sang IPv6 hoặc ngược lại thìtrên thiết bị NAT-PT phải duy trì một tập địa chỉ IPv4 cũng như IPv6 đểánh xạ qua lại.

Ngoài ra cơ chế NAT-PT còn cần một prefix để nhận biết các địa chỉcần được xử lý. Prefix này cùng với một địa chỉ IPv4 sẽ cấu tạo nên mộtđịa chỉ IPv6 hoàn chỉnh, do đó prefix này sẽ có độ dài là /96

Dựa vào đây ta sẽ có cơ chế chuyển đổi như sau:

- Dịch từ header IPv4 sang header IPv6
- Địa chỉ nguồn: 32 bit của địa chỉ nguồn cùng với 96 bit prefix sẽ tạonên một địa chỉ IPv6. Địa chỉ này sẽ được chuyển tiếp qua thiết bị NAT-PT
- Địa chỉ đích: thiết bị NAT-PT sẽ lưu giữ một bảng ánh xạ giữa dạngIPv4 và IPv6 của địa chỉ đích. Khi đó địa chỉ đích dạng IPv4 sẽ được ánhxạ tương ứng sang dạng IPv6 dựa vào bảng ánh xạ.
- Dịch từ header IPv6 sang header IPv4

- Địa chỉ nguồn: Tương tự, thiết bị NAT-PT sẽ lưu trữ một bảng ánhxạ giữa dạng IPv4 và IPv6 của địa chỉ nguồn. Địa chỉ nguồn dạng IPv6 sẽđược ánh xạ sang IPv4 dựa vào bảng ánh xạ
- Địa chỉ đích: Địa chỉ IPv6 này bao gồm 32 bit cuối là địa chỉ đíchdạng IPv4. Dựa vào prefix thiết bị NAT-PT sẽ tách địa chỉ IPv4 ra khỏi địachỉ IPv6 này.

Ưu điểm:

- Quản trị tập trung tại thiết bị NAT-PT.
- Có thể triển khai nhiều thiết bị NAT-PT để tăng hiệu năng hoạt động.

Nhược điểm:

- NAT-PT cũng như NAT trong IPv4, không có khả năng hoạt độngvới các gói tin có chứa địa chỉ trong phần tải tin. Do đó, NAT-PT thường đikèm với cơ chế Application Level Gateway - ALG. Cơ chế này cho phépxử lý các gói tin ứng với từng dịch vụ nhất định như DNS hay FTP,… Tuynhiên bản thân các dịch vụ này đều có khả năng phát triển nên tiếp tục cậpnhật cài đặt ALG là không thể tránh khỏi.
- Ngay cả khi có thể giữ cho cơ chế ALG luôn được cập nhật thì cơ chế chuyển dịch địa chỉ vẫn có thể hoạt động tốt nếu không có sự mã hóa.
- NAPT-PT có thể gây ra những lỗi về định tuyến khi có quá nhiều phiên cùng sử dụng chung một port vì khi đấy NAPT- PT sẽ không có cơ sở để xác định chính xác từng dịch vụ.
- Và một nhược điểm khác của NAT-PT cũng như các thuật toán dịchđịa chỉ khác là vẫn không giải quyết được vấn đề về bản ghi định tuyến ở trên router trung gian.

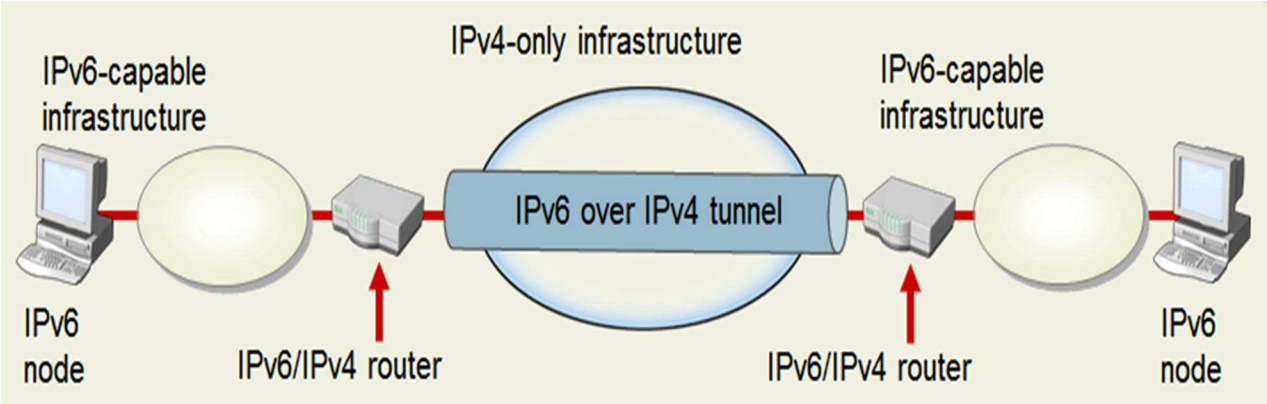
3.2.3 Công nghệ đường hầm Tunneling

3.2.3.1 Giới thiệu

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

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

Nói chung, công nghệ đường hầm đã "gói" gói tin IPv6 trong gói tin IPv4 để truyền đi được trên cơ sở hạ tầng mạng IPv4. Tức thiết lập một đường kết nối ảo (một đường hầm) của IPv6 trên cơ sở hạ tầng mạng IPv4.



Hình 13 : Công nghệ đường hầm

3.2.3.2 Phân loại công nghệ đường hầm

Đường hầm bằng tay (manual tunnel): là hình thức tạo đường hầm kết nối IPv6 trên cơ sở hạ tầng mạng IPv4, trong đó đòi hỏi phải có cấu hình bằng tay tại các điểm kết cuối đường hầm. Trong đường hầm cấu hình bằng tay, các điểm kết cuối đường hầm này sẽ không được suy ra từ các địa chỉ nằm trong địa chỉ nguồn và địa chỉ đích của gói tin IPv6. Điển hình là công nghệ Tunnel Broker sẽ được giới thiệu ở phần sau.

Đường hầm tự động (automatic tunnel): là công nghệ tạo đường hầm trong đó không đòi hỏi cấu hình địa chỉ IPv4 của điểm bắt đầu và kết thúc đường hầm bằng tay. Địa chỉ IPv4 của điểm bắt đầu và kết thúc đường hầm được suy ra từ địa chỉ nguồn và địa chỉ đích của gói tin IPv6. Điển hình cho kiểu đường hầm này là 6to4 và ISATAP.Một số loại đường hầm đặc biệt .

3.2.3.3 Một số loại đường hầm đặc biệt

a. Tunnel Broker

Khi chúng ta muốn có một kết nối ổn định, riêng biệt, thường giữa hai mạng IPv6, có kết nối IPv4 thông qua hai bộ định tuyến router biên. Nếu hai router biên này có khả năng hoạt động dual-stack, người ta có thể cấu hình bằng tay một đường hầm giữa hai router biên nhằm kết nối hai mạng IPv6 sử dụng cơ sở hạ tầng mạng IPv4. Đường hầm bằng tay cũng được sử dụng để cấu hình giữa router và máy tính nhằm kết nối một máy tính IPv6 vào một mạng IPv6 từ xa. Cấu hình bằng tay đường hầm giữa máy tính và router được áp dụng trong công nghệ Tunnel Broker.

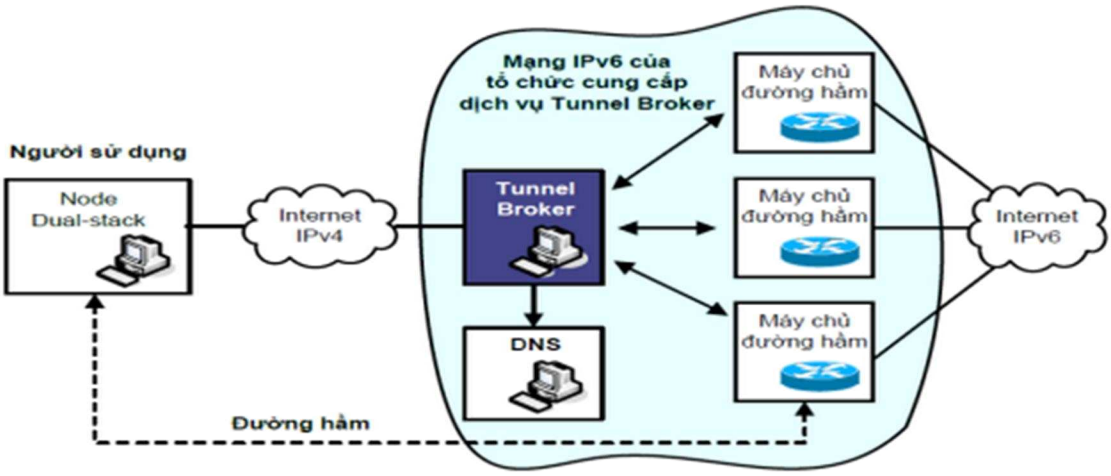
Đây là công nghệ tạo đường hầm đó một tổ bằng tay, trong chức đứng ra làm trung gian, cung cấp kết nối tới Internet IPv6 cho những thành viên đăng ký sử dụng dịch vụ Tunnel Broker do tổ chức cung cấp dịch vụ có vùng Tunnel Broker địa chỉ IPv6 độc lập, toàn cầu, xin cấp từ các tổ chức quản lý địa chỉ IP quốc tế, mạng IPv6 của tổ chức cung cấp Tunnel Broker có kết nối tới Internet IPv6 và những mạng IPv6 khác. Người sử dụng sẽ được cung cấp thông tin để thiết lập đường hầm từ máy tính hoặc mạng của mình đến mạng của tổ chức duy trì Tunnel Broker và dùng mạng này như một trung gian để kết nối tới các mạng IPv6 khác.

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

- Một vùng địa chỉ IPv6 từ không gian địa chỉ IPv6 của nhà cung cấp dịch vụ Tunnel Broker, thoả mãn nhu cầu của người sử dụng.

  Chuyển giao cho người sử dụng một tên miền cấp dưới không gian tên miền của nhà cung cấp dịch vụ Tunnel Broker. Đây là tên miền hợp lệ toàn cầu, thành viên của Tunnel Broker có thể

- sử dụng tên miền này để thiết lập website IPv6, Website cho phép những mạng IPv6 có kết nối tới mạng của nhà cung cấp dịch vụ Tunnel Broker truy cập tới.
- Các thông tin và hướng dẫn để người sử dụng thiết lập đường hầm (tunnel) đến mạng của tổ chức cung cấp Tunnel Broker.



Hình 14 : Mô hình Tunnel Broker

Trong đó:

Tunnel Broker: Là những máy chủ dịch vụ làm nhiệm vụ quản lý thông tin đăng ký, cho phép sử dụng dịch vụ, quản lý việc tạo đường hầm, thay đổi thông tin đường hầm cũng như xoá đường hầm. Trong hệ thống dịch vụ Tunnel Broker của nhà cung cấp, máy chủ Tunnel Broker sẽ liên lạc với máy chủ đường hầm (thực chất là các bộ định tuyến dual-stack) và máy chủ tên miền (DNS) của nhà cung cấp Tunnel Broker để thiết lập đường hầm phía nhà cung cấp dịch vụ và tạo bản ghi tên miền cho người đăng ký sử dụng dịch vụ Tunnel Broker. Người sử dụng thông qua mạng Internet IPv4 sẽ truy cập máy chủ Tunnel Broker và đăng ký tài khoản sử dụng dịch vụ Tunnel Broker thông qua mẫu đăng ký dưới dạng Web.

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

b. Đường hầm 6to4

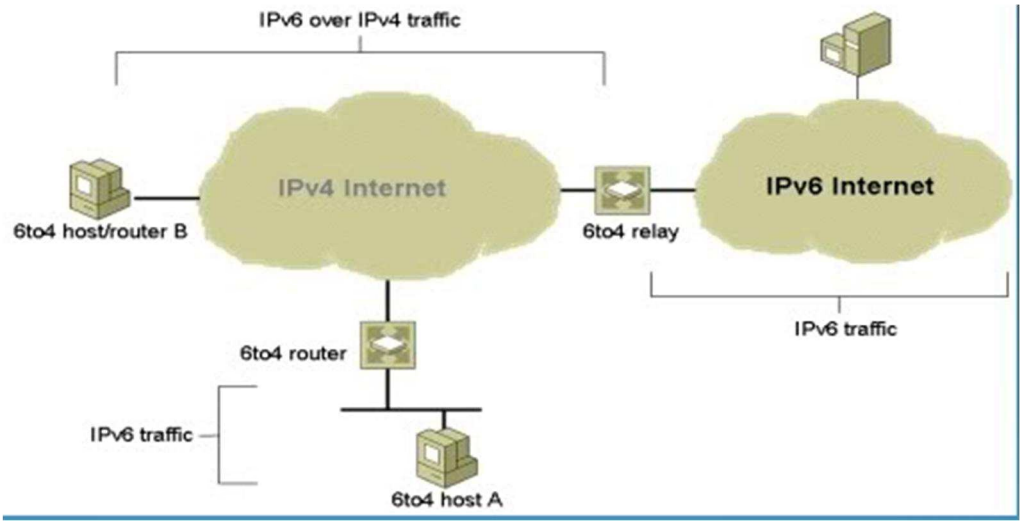
6to4 là một công nghệ đường hầm tự động dùng để cung cấp kếtnối IPv6 giữa các subnet cũng như host dựa trên cơ sở hạ tần IPv4.

IANA đã phân bổ dành riêng một prefix địa chỉ cho công nghệ tunnel 6to4 toàn cầu. Đó là 2002::/16. Prefix địa chỉ này kết hợp với 32 bit địa chỉ IPv4 sẽ tạo nên một prefix địa chỉ 6to4 kích cỡ /48 toàn cầu duynhất sử dụng cho một mạng IPv6.

Hình 15 : Cấu trúc địa chỉ 6to4

Vùng địa chỉ /48 này có thể sử dụng để phân bổ tạo nên một mạngIPv6 cho một tổ chức. Một subnet trong IPv6 được gắn prefix /64. Vớivùng địa chỉ 6to4 /48, ta có 16 bit có thể sử dụng để đánh số các mạng LAN 6to4 IPv6 trong site, và có thể đánh số tới 65.536 mạng, một con sốrất lớn và khó có thể sử dụng hết vùng địa chỉ, chỉ từ một địa chỉ IPv4.

IPv4Mô hình đường hầm 6to4:



Hình 16 : Mô hình đường hầm 6to4

- 6to4 host: Tất cả các host trong mạng có sử dụng công nghệ đườnghầm 6to4 đều được gán một địa chỉ IPv6 dạng 6to4 (với prefix là2002::/16). Các host 6to4 không cần bất cứ một thiết lập bằng tay nào và sẽtự tạo địa chỉ dạng 6to4 bằng các thuật toán tự động cấu hình
- 6to4 router: Là một router dual - stack hỗ trợ sử dụng giao diện 6to4.Router này sẽ chuyển tiếp lưu lượng có gán địa chỉ 6to giữa những 6to4host trong một site và tới những router 6t04 khác hoặc tới 6to4 relay router trong mạng IPv4 Internet. Việc cấu hình router 6to4 cần phải có cấu hình bằng tay
- 6to4 relay: 6to4 relay router là một dual - stack router thực hiệnchuyển tiếp lưu lượng có địa chỉ 6to4 của những router 6to4 trên Internetvà host trên

IPv6 Internet (sử dụng địa chỉ IPv6 chính thức, cung cấp bởi tổchức quản lý địa chỉ toàn cầu). 6to4 relay router là một 6to4 router đượccấu hình để hỗ trợ chuyển tiếp định tuyến giữa địa chỉ 6to4 và địa chỉ IPv6chính thức (địa chỉ IPv6 định danh toàn cầu). 6to4 relay router sẽ là gateway kết nối giữa mạng 6to4 và IPv6 Internet. Nhờ đó giúp cho những mạng IPv6 6to4 có thể kết nối tới Internet IPv6.

Đường hầm 6to4 thực hiện những chức năng sau:

- Chỉ định một không gian địa chỉ IPv6 cho bất cứ một host hoặcmạng nào có địa chỉ publich IPv4.
- Đóng gói các gói tin IPv6 vào các gói tin IPv4 để chuyển qua mạngIPv4.

6to4 nhúng các gói tin IPv6 vào phần payload của gói tin IPv4 với trường protocol được đặt thành 41, chỉ ra rằng đây là một gói tin IPv6 được nhúng trong IPv4. Địa chỉ đích IPv4 cho gói tin IPv6 được đóng gói bằngcách tách 32 bit tiếp theo của host hoặc router đã gửi gói tin. Gói tin IPv4 được đóng gói sẽ được gửi đến địa chỉ đích như các gói tin IPv4 thông thường

- Định tuyến giữa mạng IPv6 và 6to4: relay router ra đời để cho phép host và mạng sử dụng địa chỉ IPv6 dạng 6to4 có thể liên lạc với các host sử dụng địa chỉ IPv6 thuần (được cung cấp bởi ISP).

Relay router sẽ kết nối trực tiếp đến mạng IPv4 và IPv6. Gói tin 6to4được gửi đến relay router thông qua giao diện địa chỉ IPv4 sẽ có phần payload được chuyển sang mạng IPv6, trong khi các gói tin IPv6 thuần sẽ được gửi đến relay router qua giao diện địa chỉ IPv6 với địa chỉ IPv6 có prefix là 2002::/64 sẽ được đóng gói vào trong một gói tin IPv4 và chuyểnsang mạng IPv4.

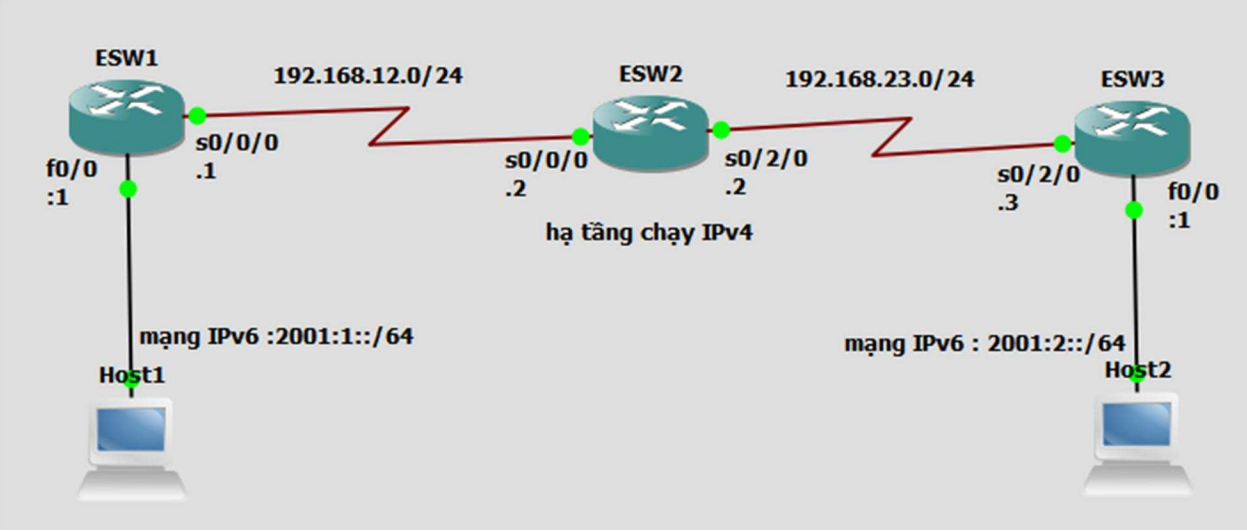
Chương 4: Mô phỏng công nghệ đường hầm Tunneling

4.1 Static Tunnel

Ý tưởng của kỹ thuật tunnel là khi một gói tin IPv6 cần được vận chuyển qua một đám mây IPv4, nó sẽ được đóng gói vào một gói tin IPv4 để đi qua các thiết bị mạng chỉ chạy IPv4. Khi gói tin này đi qua hết đảm mây IPv4 để bước vào lại hạ tầng IPv6, nó sẽ được gỡ khỏi gói tin IPv4 và trả lại nguyên dạng là gói tin IPv6 để tiếp tục di chuyển trong hạ tầng IPv6 và đi đến đích.

Sau đây ta cùng khảo sát một ví dụ để tìm hiểu kỹ hơn về cách thức cấu hình thiết bị để nắm rõ hơn chi tiết về mặt kỹ thuật cần quan tâm.

Sơ đồ bài lab:



Hình 17 : Sơ đồ bài lab cấu hình static tunnel

Mô tả :

Trên sơ đồ hình 17 là một sơ đồ mạng đang trong quá trình chuyển đổi từ IPv4 sang IPv6 và chạy song song hai hạ tầng IPv4 và IPv6 với quy hoạch chỉ ra như hình vẽ. Yêu cầu đặt ra là cấu hình static tunnel để các prefix IPv6 có thể đi đến được với nhau.

Thực hiện:

Bước 1: Cấu hình ban đầu cho sơ đồ lab

- Thực hiện đặt địa chỉ IPv4 và IPv6 cho các cổng của router theo quy hoạch IP như trên hình.
- Cấu hình giao thức định tuyến bất kỳ để các địa chỉ IPv4 nhìn thấy nhau.

- Note: router ESW1 và router ESW3 đều hỗ trợ chạy cả 2 giao thức IPv4 và IPv6 vì đây là các router biên.

Trên router ESW1 cấu hình:

Cấu hình cho cổng fa0/0:

- *ESW1(config)#interface f0/0*
- *ESW1(config-if)#no shut*
- *ESW1(config-if)#ipv6 address 2001:1::1/64*
- *ESW1(config-if)#exit*

Cấu hình cho cổng s0/0/0:

- *ESW1(config)#interface s0/0/0*
- *ESW1(config-if)#no shut*
- *ESW1(config-if)#ip address 192.168.12.1 255.255.255.0*
- *ESW1(config-if)#exit*

Cấu hình giao thức định tuyến tĩnh:

- *ESW1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0*

Trên router ESW3 cấu hình tương tự:

- *ESW3(config)#interface f0/0*
- *ESW3(config-if)#no shut*
- *ESW3(config-if)#ipv6 address 2001:2::1/64*
- *ESW3(config-if)#exit*
- *ESW3(config)#interface s0/2/0*
- *ESW3(config-if)#no shut*
- *ESW3(config-if)#ip address 192.168.23.3 255.255.255.0*
- *ESW3(config-if)#exit*
- *ESW3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0*

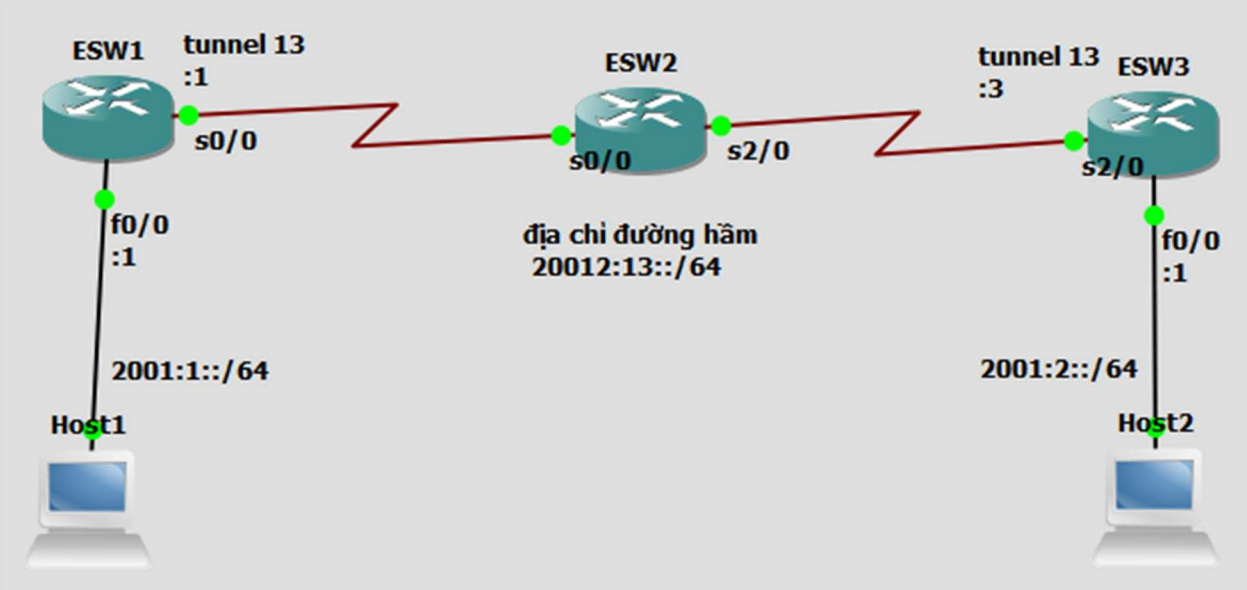
Trên router ESW2 cấu hình:

- *ESW2(config)#interface s0/2/0*
- *ESW2(config-if)#no shut*

- *ESW2(config-if)#ip address 192.168.23.2 255.255.255.0*
- *ESW2(config-if)#exit*
- *ESW2(config)#interface s0/0/0*
- *ESW2(config-if)#no shut*
- *ESW2(config-if)#ip address 192.168.12.2 255.255.255.0*
- *ESW2(config-if)#exit*

Bước 2: Cấu hình cho các tunnel

Thực hiện cấu hình static tunnel chuyên dùng vận chuyển lưu lượng Ipv6 qua hạ tầng mạng IPv4. Tunnel này được đặt tên như chỉ ra trên hình 18



Hình 18 : Tunnel đấu nối giữa hai router 1 và 3

Trên router ESW1cấu hình tunnel:

ESW1 (config)#interface tunnel 13
ESW1 (config-if)#tunnel source 192.168.12.1
ESW1 (config-if)#tunnel destination 192.168.23.3
ESW1 (config-if)#tunnel mode ipv6ip
ESW1 (config-if)#ipv6 address 2001:13::1/64
ESW1 (config-if)#exit

Trên router ESW3 cấu hình tunnel:

ESW3 (config)#interface tunnel 13
ESW3 (config-if)#tunnel source 192.168.23.3
ESW3 (config-if)#tunnel destination 192.168.12.1

ESW3 (config-if)#tunnel mode ipv6ip
ESW3 (config-if)#ipv6 address 2001:13::1/64
ESW3 (config-if)#exit

Chú ý: câu lệnh "R(config-if)#tunnel mode ipv6ip" sẽ chuyển tunnel sang hoạt động ở chế độ mode chuyên dụng cho trung chuyển IPv6 qua IPv4. Nếu không sử dụng lệnh này, tunnel được tạo ra sẽ hoạt động ở mode GRE – là một loại tunnel thông dụng để vận chuyển nhiều loại dữ liệu khác nhau (trong đó có IPv6) qua hạ tầng IPv4 – tuy nhiên, loại tunnel GRE này sẽ gây tốn overhead hơn so với loại tunnel chuyên dụng chỉ dùng cho trung chuyển IPv6 qua hạ tầng IPv4.

Sau khi cấu hình xong các tunnel, các "ốc đảo" IPv6 đã được đấu nối với nhau, chúng ta chỉ cần chạy một hình thức định tuyến IPv6 bất kỳ là các prefix IPv6 ở nhiều khu vực khác nhau có thể đi đến được nhau.

Bước 3 : Cấu hình định tuyến OSPFv3

Cấu hình định tuyến OSPFv3 trên 2 router ESW1 và ESW3. Đảm bảo rằng mọi địa chỉ IPv6 trên sơ đồ hình 18 thấy được nhau.

Trên router ESW1 cấu hình:

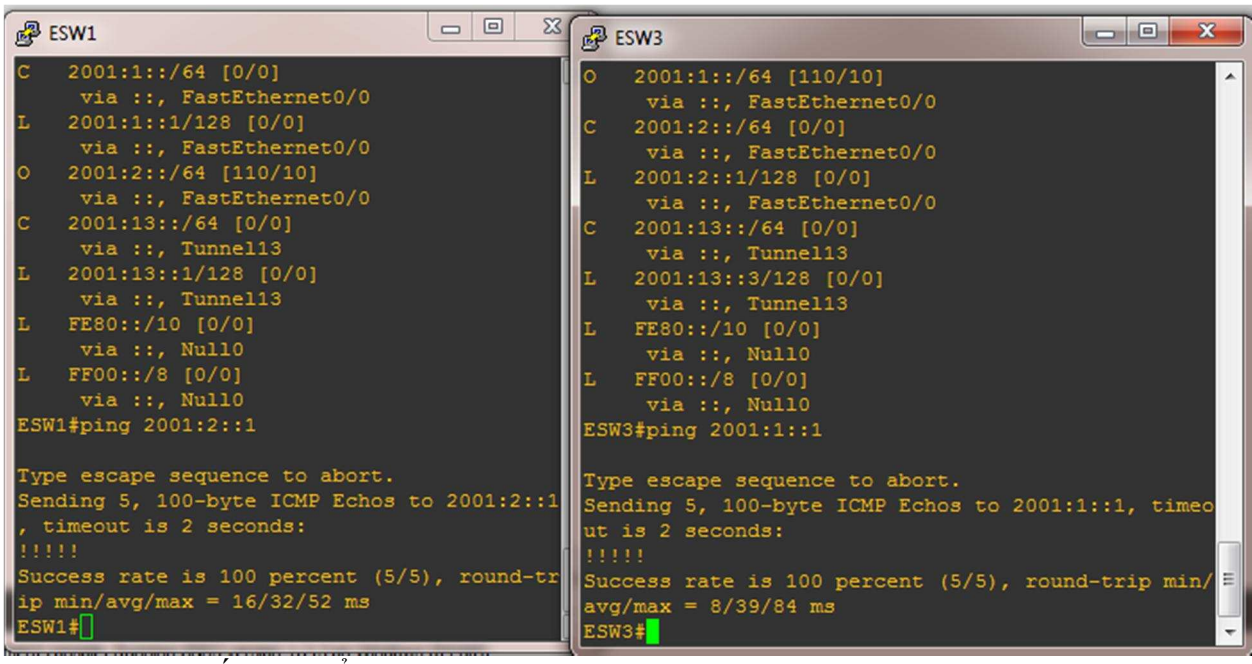
ESW1(config)#ipv6 unicast-routing
ESW1 (config)#interface tunnel 13
ESW1 (config-if)#ipv6 ospf 1 area 0
ESW1 (config-if)#exit
ESW1 (config)#interface f0/0
ESW1 (config-if)#ipv6 ospf 1 area 0
ESW1 (config-if)#exit

Trên router ESW3 cấu hình :

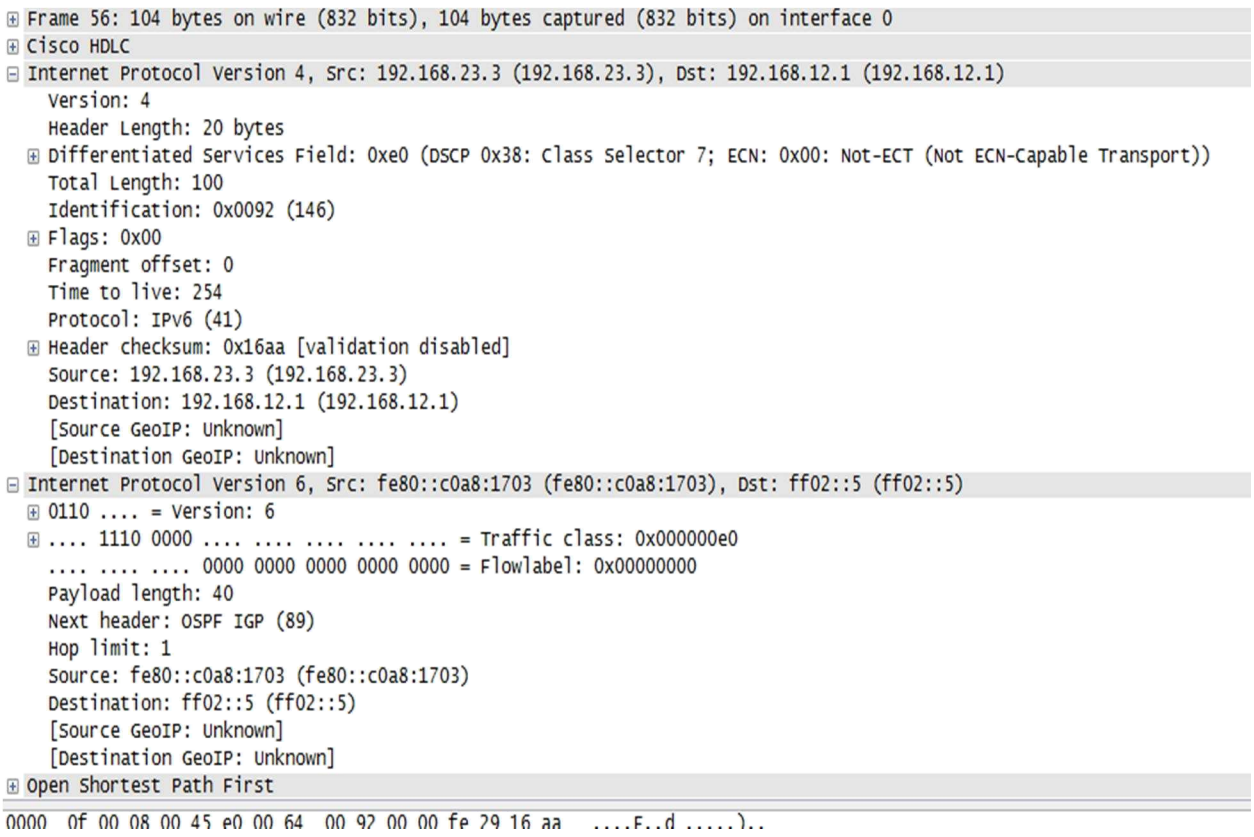
ESW3 (config)#ipv6 unicast-routing
ESW3 (config)#interface tunnel 13
ESW3 (config-if)#ipv6 ospf 1 area 0
ESW3 (config-if)#exit
ESW3 (config)#interface f0/0
ESW3 (config-if)#ipv6 ospf 1 area 0
ESW3 (config-if)#exit

Kết quả mô phỏng:

- Kiểm tra bảng định tuyến: các IPv6 đã hiển thị trong bảng định tuyến
- Các prefix IPv6 trên các router ESW1, ESW3 lúc này đã có thể đến được với nhau thông qua tunnel qua đám mây IPv4.



Hình 19 : kết quả kiểm tra route và thực hiện lệnh ping



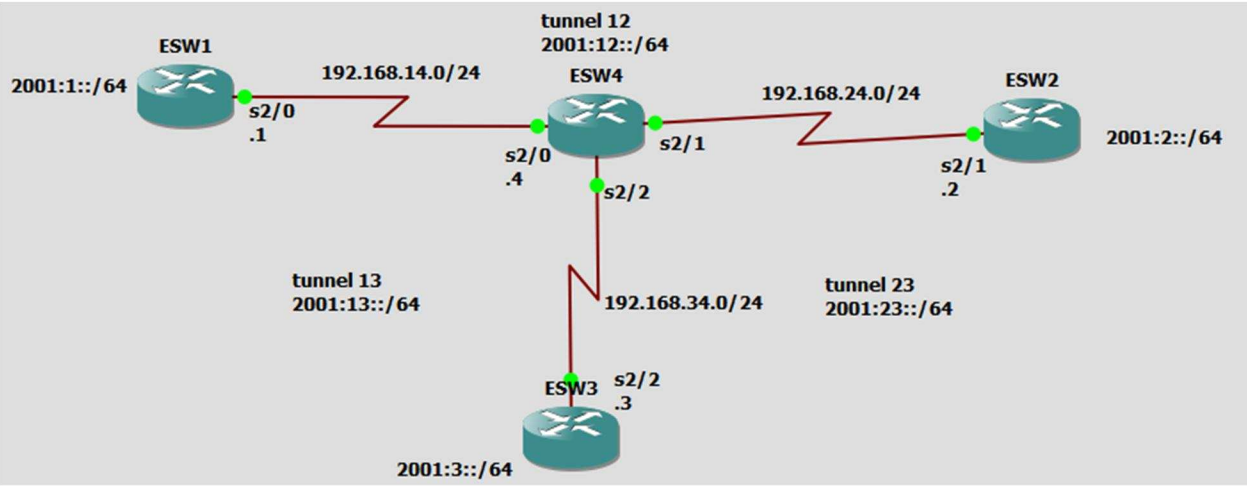
Hình 20 : Gói tin hello của giao thức OSPF bắt được trên cổng s0/0 của ESW1

Ta thấy rằng trong trường protocol của IPv4 có giá trị bằng 41, điều đó chứng tỏ gói tin IPv6 khi đi qua hạ tầng mạng đã được đóng gói vào trong gói tin IPv4 và được vận chuyển qua mạng IPv4 dựa vào cách thức định tuyến của giao thức IPv4.

4.2 6to4 Tunnel

Cũng giống như static tunnel thì 6to4 tunnel cho phép người quản trị kết nối nhiều "ốc đảo" IPv6 qua một mạng IPv4. Tuy nhiên, khác với kỹ thuật static tunnel, kỹ thuật 6to4 cho phép các tunnel được tạo ra một cách tự động mỗi khi xuất hiện gói tin có nhu cầu đi xuyên qua đảm mây IPv4 để đến một vùng IPv6 khác. Để thấy sự khác biệt giữa 2 cách tạo đường hầm, chúng ta cùng tìm hiểu một ví dụ về cách tạo 6to4 tunnel.

Sơ đồ bài lab về cấu hình 6to4 tunnel:



Hình 21: Sơ đồ bào lab 6to4 tunnel

Mô tả :

Trên sơ đồ hình 21 là một sơ đồ mạng đang trong quá trình chuyển đổi từ IPv4 sang IPv6 và chạy song song hai hạ tầng IPv4 và IPv6 với quy hoạch IP được chỉ ra như trên hình vẽ. Yêu cầu của bài lab này là thực hiện cấu hình giải pháp 6to4 tunnel để các prefix IPv6 trên hình 21 có thể đi đến được nhau.

Thực hiện :

Bước 1: Cấu hình ban đầu cho sơ đồ lab

Thực hiện đặt địa chỉ IPv4 và IPv6 cho các cổng của các router theo quy hoạch IP trên hình 21. Cấu hình một hình thức định tuyến bất kỳ đảm bảo mọi địa chỉ IPv4 trên sơ đồ thấy nhau.

Trên ESW1 cấu hình :

ESW1(config)#interface f0/0
ESW1(config-if)#no shutdown
ESW1(config-if)#ipv6 address 2002:C0A8:E01::1/64
ESW1(config-if)#exit
ESW1(config)#interface s2/0
ESW1(config-if)#no shutdown
ESW1(config-if)#ip address 192.168.14.1 255.255.255.0
ESW1(config-if)#exit
ESW1(config)#ip route 0.0.0.0 0.0.0.0 s2/0
Trên ESW2 cấu hình:
ESW2 (config)#interface f0/0
ESW2 (config-if)#no shutdown
ESW2 (config-if)#ipv6 address 2002:C0A8:1802::1/64
ESW2 (config-if)#exit
ESW2 (config)#interface s2/1
ESW2 (config-if)#no shutdown
ESW2 (config-if)#ip address 192.168.24.2 255.255.255.0
ESW2 (config-if)#exit
ESW2 (config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Trên ESW3 cấu hình :
ESW3 (config)#interface f0/0
ESW3 (config-if)#no shutdown
ESW3 (config-if)#ipv6 address 2002:C0A8:2203::1/64
ESW3 (config-if)#exit
ESW3 (config)#interface s2/2
ESW3 (config-if)#no shutdown
ESW3 (config-if)#ip address 192.168.34.3 255.255.255.0
ESW3 (config-if)#exit
ESW3 (config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Trên ESW4 cấu hình:
ESW4 (config)#int s2/0
ESW4 (config-if)#no shutdown
ESW4 (config-if)#ip address 192.168.14.4 255.255.255.0

ESW4 (config-if)#exit
ESW4 (config)#interface s2/1
ESW4 (config-if)#no shutdown
ESW4 (config-if)#ip address 192.168.24.4 255.255.255.0
ESW4 (config-if)#exit
ESW4 (config)#interface s2/2
ESW4 (config-if)#no shutdown
ESW4 (config-if)#ip address 192.168.34.4 255.255.255.0
ESW4 (config-if)#exit

Bước 2: Cấu hình 6to4 tunnel

Sử dụng các địa chỉ IPv4 trên các cổng s2/0;s2/1;s2/2 của các router ESW1, ESW2 và ESW3 để xây dựng các đường hầm 6to4 kết nối các mạng IPv6 trên các router này. Sử dụng static route sau khi đã cấu hình tunnel đảm bảo mọi địa chỉ IPv6 trên sơ đồ hình 1 thấy nhau.

Chú ý:

Kỹ thuật 6to4 tunnel là một loại đường hầm đa điểm và được xây dựng một cách tự động. Các đường hầm không được thiết lập trước giống như với static tunnel mà chỉ được thiết lập tự động khi xuất hiện gói tin cần đi từ vùng IPv6 này qua vùng IPv6 kia.

Để các địa chỉ IPv6 của những vùng IPv6 khác nhau có thể đi đến được nhau thông qua 6to4 tunnel, các địa chỉ này cần phải được đặt trong những prefix tuân theo một quy ước cho trước. Kỹ thuật 6to4 tunnel chỉ cho phép truyền tải thông tin giữa các prefix thuộc dải 2002::/16. Các địa chỉ cụ thể thuộc các vùng IPv6 cụ thể phải được lấy từ các subnet của prefix 2002::/16 theo quy ước như sau:

- Trên ESW1, IPv6 prefix được sử dụng là 2002:C0A8:E01::/64. Ta thấy, 32 bit tiếp theo sau "2002" chính là dạng hexa của địa chỉ IPv4 trên cổng S2/0 của ESW1: C0 – 192, A8 – 168, E – 14 và 01 – 1 hay "C0A8:E01" chính là "192.168.14.1".
- Trên ESW2, IPv6 prefix được sử dụng là 2002:C0A8:1802::/64. Ta thấy, 32 bit tiếp theo sau "2002" chính là dạng hexa của địa chỉ IPv4 trên cổng S2/1 của ESW2: C0 – 192, A8 – 168, 18 – 24 và 02 – 2 hay "C0A8:1802" chính là "192.168.24.2".
- Trên ESW3, IPv6 prefix được sử dụng là 2002:C0A8:2203::/64. Ta thấy, 32 bit tiếp theo sau "2002" chính là dạng hexa của địa chỉ IPv4 trên cổng S2/2 của ESW3: C0 – 192, A8 – 168, 22 – 34 và 03 – 3 hay "C0A8:2203" chính là "192.168.34.3".

Khi một gói tin IPv6 muốn đi từ vùng IPv6 này qua vùng IPv6 kia, nó sẽ được đóng vào gói tin tunnel với các địa chỉ source IPv4 và destination IPv4 sẽ được rút ra từ các địa chỉ mạng IPv6 tương ứng.

Cấu hình

Trên ESW1:

ESW1 (config)#interface tunnel 0
ESW1 (config-if)#tunnel source s2/0

ESW1 (config-if)#tunnel mode ipv6ip 6to4
ESW1 (config-if)#ipv6 address FC00:123::1/64
ESW1 (config-if)#exit
ESW1 (config)#ipv6 route 2002::/16 Tunnel0

Trên ESW2:

ESW2 (config)#interface tunnel 0
ESW2 (config-if)#tunnel source s2/1
ESW2 (config-if)#tunnel mode ipv6ip 6to4
ESW2 (config-if)#ipv6 address FC00:123::2/64
ESW2 (config-if)#exit
ESW2 (config)#ipv6 route 2002::/16 Tunnel0

Trên ESW3:

ESW3 (config)#interface tunnel 0
ESW3 (config-if)#tunnel source s2/2
ESW3 (config-if)#tunnel mode ipv6ip 6to4
ESW3 (config-if)#ipv6 address FC00:123::3/64
ESW3 (config-if)#exit
ESW3 (config)#ipv6 route 2002::/16 Tunnel0

Kết luận

Giao thức IPv6 có nhiều ưu điểm vượt trội so với IPv4, đáp ứng được nhu cầu phát triển của mạng Internet hiện tại và trong tương lai. Do đó , giao thức IPv6 sẽ sớm thay thế IPv4. Tuy nhiên, để chuyển đổi toàn bộ các node mạng IPv4 hiện nay sang Ipv6 trong một thời gian ngắn là không thể. Hơn nữa, nhiều ứng dụng mạng hiện tại vẫn chưa còn hỗ trợ IPv6. Ngoài ra, các cơ chế chuyển đổi phải đảm bảo khả năng tương tác giữa các trạm, các ứng dụng IPv4 hiện có với các trạm và ứng dụng IPv6. Và các cơ chế cũng cho phếp chuyển tiếp các luồng thông tin IPv6 trên hạ tầng Ipv4 hiện có.

Tài liệu tham khảo:

- Trung tâm internet Việt Nam-VNNIC (http://daotaoipv6.vnnic.vn/ch1/1_0_0/index.html/) ,Giới thiệu về IPv6.
- Trung tâm tin học NTPS (http://www.ntps.edu.vn/) , Cấu hình static tunnel và 6t04 tunnel.
- https://tools.ietf.org/html/rfc7059 , A Comparison of IPv6-over-IPv4 Tunnel Mechanisms
- http://tools.ietf.org/html/rfc4213 , Basic Transition Mechanisms for IPv6 Hosts and Routers
- http://en.wikipedia.org/wiki/IPv6_transition_mechanisms , IPv6 transition mechanisms.
- Lê Doãn Tuấn DT5-K52, Đồ án tốt nghiệp nghiên cứu triển khai RPL và Ipv6 trong mạng cảm biến không dây.
- Triển khai IPv6 trong mạng nghiên cứu và đào tạo Việt Nam (VinaREN).
- http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-tunnel.html , Implementing Tunneling for IPv6.
- http://vnexperts.net/forum/120-Basic-concepts/10811-T%C3%ACm-hi%E1%BB%83u-IPV6-v%C3%A0-h%C6%B0%E1%BB%9Bng-chuy%E1%BB%83n-%C4%91%E1%BB%95i-IPV4-sang-IPV6.html, Tìm hiểu IPV6 và hướng chuyển đổi IPV4 sang IPV6.