TRUNG TÂM INTERNET VIỆT NAM

HƯỚNG DẪN VỀ QUY HOẠCH, QUẢN LÝ VÀ SỬ DỤNG ĐỊA CHỈ IPV6

Tháng 11-2013

MỤC LỤC

DANH MỤC HÌNH VẼ

KHÁI NIỆM VÀ TỪ VIẾT TẮT

Anycast

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

APNIC

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

Blacklist

Danh sách "đen", các vùng địa chỉ vi phạm.

Broadcast

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

DHCP

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

DHCPv6

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

IANA

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

ICANN

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

IETF

Internet Engineering Taskforce - Tổ chức tiêu chuẩn hoá, viết các tài liệu tiêu chuẩn hoá (RFC) phục vụ hoạt động Internet toàn cầu.

IPv4

Internet Protocol version 4 – Phiên bản 4 của thủ tục Internet. Hiện đang được sử dụng phổ biến trong hoạt động mạng Internet toàn cầu.

IPv6

Internet Protocol version 6 – Phiên bản 6 của thủ tục Internet, được phát triển nhằm thay thế IPv4, khắc phục những hạn chế của phiên bản IPv4 và cải thiện thêm nhiều đặc tính mới.

Multicast

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

NIR

National Internet Registry: Tổ chức quản lý địa chỉ cấp quốc gia

Prefix

Là một khối địa chỉ IPv4 hoặc IPv6, được quyết định bằng việc cố định một số bít đầu tiên của địa chỉ. Ví dụ 203.119.9.0/24 là tập hợp các địa chỉ IPv4 từ 203.119.9.0 đến 203.119.9.255. Đối với IPv6, 2000::/3 là tập hợp các địa chỉ IPv6 có ba bít đầu tiên là 001 (chữ cái hexa đầu tiên trong địa chỉ là 2 hoặc 3).

RFC

Request For Comments - Những tài liệu tiêu chuẩn cho Internet, được soạn thảo và xuất bản bởi IETF.

RIPE NCC

Réseaux IP Européens Tổ chức quản lý địa chỉ IP, số hiệu mạng cấp vùng, phụ trách khu vực Châu Âu.

RIR

Regional Internet Registry - Tổ chức quản lý và phân bổ địa chỉ IP cấp vùng cho các hoạt động Internet. Những tổ chức này cũng có những vai trò trong việc hỗ trợ quản lý cơ sở hạ tầng Internet và phát triển chính sách quản lý tài nguyên địa chỉ IP, số hiệu mạng ASN.

Unicast

Cách thức gửi gói tin thông thường. Trong đó gói tin chỉ được gửi đến một đích duy nhất. Những cách thức gửi gói tin khác bao gồm anycast, broadcast và multicast

LỜI NÓI ĐẦU

Địa chỉ IPv4 đã cạn kiệt. IPv6 là thế hệ địa chỉ tiếp theo được phát triển, thúc đẩy sử dụng để thay thế cho IPv4 tiếp nối hoạt động Internet. Với chiều dài 128 bít, IPv6 cung cấp một không gian địa chỉ khổng lồ đủ để đảm bảo cho nhu cầu phát triển dài hạn của Internet toàn cầu. IPv6 được thiết kế và cấu trúc khác biệt so với IPv4, chính vì vậy, việc quy hoạch, quản lý, sử dụng địa chỉ cũng có nhiều điểm khác biệt.

Để hỗ trợ các tổ chức đã được cấp phát IPv6 tại Việt Nam trong việc đưa địa chỉ vào sử dụng thực tế, góp phần thực hiện tốt các nhiệm vụ của Kế hoạch Hành động Quốc gia về IPv6, Trung tâm Internet Việt Nam (VNNIC) biên soạn tài liệu hướng dẫn về quy hoạch, quản lý, sử dụng địa chỉ IPv6. Tài liệu hướng dẫn các tổ chức thành viên địa chỉ đã được cấp vùng IPv6 các nguyên tắc cơ bản trong phân hoạch địa chỉ IPv6 cho mạng lưới, sự khác biệt đối với IPv4, các kinh nghiệm và các điểm cần lưu ý trong quá trình phân hoạch tài nguyên địa chỉ, bên cạnh đó là các phương thức đánh số và quản lý địa chỉ cho các máy trạm, máy chủ, thiết bị trên mạng lưới và các vấn đề cần nắm bắt, cách thức xử lý vấn đề phát sinh trong quá trình sử dụng địa chỉ IPv6, đáp ứng các quy định quản lý của Việt Nam và khu vực.

Tài liệu là nguồn tham khảo phù hợp cho các các cán bộ kỹ thuật, quản lý mạng thực hiện công tác phân hoạch, quản lý địa chỉ mạng lưới của các tổ chức, đã có kinh nghiệm kiến thức làm việc với thế hệ địa chỉ IPv4.

CHƯƠNG 1: THÔNG TIN CƠ BẢN VỀ ĐỊA CHỈ IPV6

1.1 Giới thiệu về IPv6

IPv6 (Internet Protocol Version 6) là phiên bản địa chỉ Internet mới, được thiết kế để thay thế cho phiên bản IPv4, với hai mục đích cơ bản: Khắc phục các nhược điểm trong thiết kế của địa chỉ IPv4 và thay thế cho nguồn địa chỉ IPv4 cạn kiệt để phát triển hạ tầng thông tin và Internet bền vững.

Đặc điểm cơ bản so sánh IPv4 – IPv6:

Loại địa chỉ	Không gian địa chỉ	Định dạng – cách viết địa chỉ
IPv4	$2^{32} = 4.3*10^{9}$	203.110.0.1
IPv6	$2^{128} = 3.4*10^{38}$	2001:2104:AC0D::1

1.2. Biểu diễn địa chỉ IPv6.

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

Địa chỉ IPV6: 128 bit

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

↓

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

↓

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

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

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

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

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

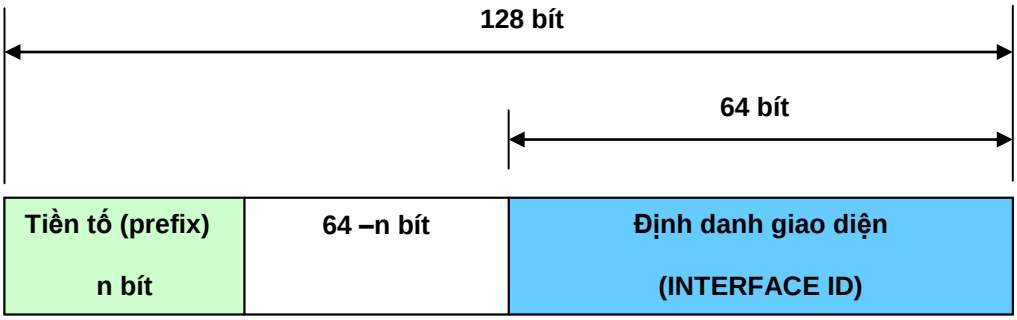
Một dải địa chỉ IPv6 được viết dưới dạng một địa chỉ IPv6 đi kèm với số bít xác định số bít phần mạng (bít tiền tố), như sau: Địa chỉ IPv6/số bít mạng

Ví dụ:

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

1.3. Cấu trúc của địa chỉ IPv6

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



Hình 1: Cấu trúc thường thấy của một địa chỉ IPv6.

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

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

Để phân loại địa chỉ, một số bít đầu trong địa chỉ IPv6 được dành riêng để xác định dạng địa chỉ, được gọi là các bít tiền tố (prefix). Các bít tiền tố này sẽ

quyết định địa chỉ thuộc loại nào và số lượng địa chỉ đó trong không gian chung IPv6.

Ví dụ: 8 bít tiền tố "1111 1111" tức "FF" xác định dạng địa chỉ multicast. Ba bít tiền tố "001" xác định dạng địa chỉ unicast định danh toàn cầu.

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

Ngoại trừ địa chỉ multicast và một số dạng địa chỉ cho mục đích đặc biệt, địa chỉ IPv6 đều có 64 bít cuối cùng được sử dụng để xác định một giao diện duy nhất trên một đường kết nối (tương đương với một mạng con "subnet"). Như vậy, một phân mạng con nhỏ nhất của địa chỉ IPv6 sẽ có kích thước /64.

Định danh giao diện là 64 bít cuối cùng trong một địa chỉ IPv6 và có thể được cấu thành tự động theo một trong những cách thức sau đây:

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

1.4. Các dạng địa chỉ IPv6

1.4.1 Phân loại địa chỉ IPv6

Không gian IPv6 được phân chia thành rất nhiều dạng địa chỉ. Mỗi dạng địa chỉ có chức năng nhất định trong phục vụ giao tiếp. Có dạng chỉ sử dụng trong giao tiếp nội bộ trên một đường kết nối, có dạng sử dụng trong kết nối toàn cầu.

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

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

  Trong địa chỉ IPv6 không còn tồn tại khái niệm địa chỉ broadcast. Mọi chức năng của địa chỉ broadcast trong IPv4 được đảm nhiệm thay thế bởi địa chỉ IPv6 multicast. Ví dụ chức năng broadcast trong

một mạng của địa chỉ IPv4 được đảm nhiệm bằng một loại địa chỉ multicast IPv6 có tên gọi địa chỉ multicast mọi node phạm vi link (FF02::1)

- ***Anycast:*** Anycast là khái niệm mới của địa chỉ IPv6. Địa chỉ anycast cũng xác định tập hợp nhiều giao diện. Tuy nhiên, trong mô hình định tuyến, gói tin có địa chỉ đích anycast chỉ được gửi tới một giao diện duy nhất trong tập hợp. Giao diện đó là giao diện "gần nhất" theo khái niệm của thủ tục định tuyến.

1.4.2 Địa chỉ UNICAST

Địa chỉ unicast bao gồm năm dạng sau đây:

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

a. Địa chỉ đặc biệt

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

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

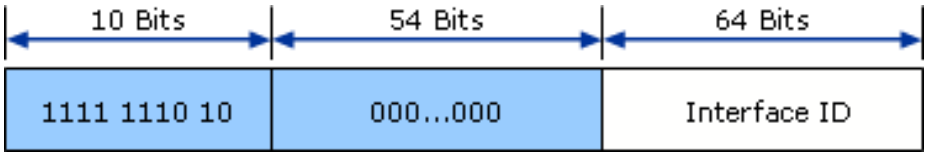
b. Địa chỉ link-local

Link-local là loại địa chỉ phục vụ cho giao tiếp nội bộ, giữa các IPv6 node trên cùng một đường kết nối. IPv6 được thiết kế với tính năng "plug-and-play", tức khả

năng cho phép IPv6 host tự động cấu hình địa chỉ, các tham số phục vụ giao tiếp bắt đầu từ chưa có thông tin cấu hình nào. Tính năng đó có được là nhờ IPv6 node luôn luôn có khả năng tự động cấu hình nên một dạng địa chỉ sử dụng giao tiếp nội bộ. Đó chính là địa chỉ link-local.

Địa chỉ link-local luôn được node IPv6 cấu hình một cách tự động, khi bắt đầu hoạt động, ngay cả khi không có sự tồn tại của mọi loại địa chỉ unicast khác . Địa chỉ này có phạm vi trên một đường link, phục vụ cho giao tiếp giữa các node lân cận. Sở dĩ IPv6 node có thể tự động cấu hình địa chỉ link-local là do IPv6 node có thể tự động cấu hình 64 bít định danh giao diện. Địa chỉ link-local được tạo nên từ 64 bít định danh giao diện Iinterface ID) và một tiền tố (prefix) quy định sẵn cho địa chỉ link-local là FE80::/10. Địa chỉ link-local bắt đầu bởi 10 bít tiền tố FE80::/10, theo sau bởi 54 bit 0. 64 bít còn lại là định danh giao diện.

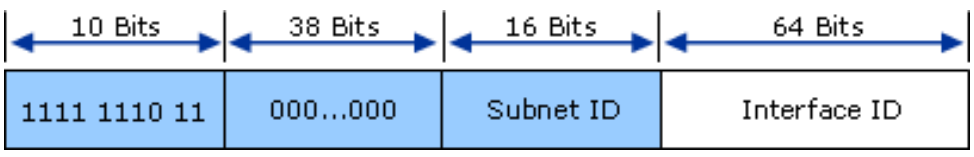
Khi không có router, các node IPv6 trên một đường link sẽ sử dụng địa chỉ link-local để giao tiếp với nhau. Phạm vi của dạng địa chỉ unicast này là trên một đường kết nối (phạm vi link).



Hình 2: Cấu trúc địa chỉ link-local

c. Địa chỉ site-local

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



Hình 3: Cấu trúc địa chỉ Site-local

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

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

d. Địa chỉ unicast định danh toàn cầu (Global unicast address)

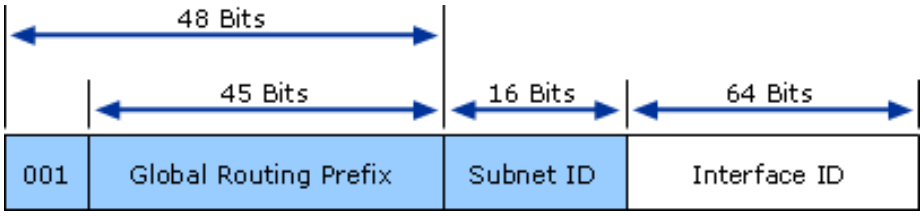
Đây là dạng địa chỉ tương đương với địa chỉ IPv4 public đang sử dụng cho mạng Internet toàn cầu. Tính duy nhất của dạng địa chỉ này được đảm bảo trong phạm vi toàn cầu. Chúng được định tuyến và có thể liên kết tới trên phạm vi toàn bộ mạng Internet. Việc phân bổ và cấp phát dạng địa chỉ này do hệ thống các tổ chức quản lý địa chỉ quốc tế đảm nhiệm.

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

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

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

Cấu trúc địa chỉ Unicast định danh toàn cầu:



Hình 4: Cấu trúc địa chỉ Unicast toàn cầu

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

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

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

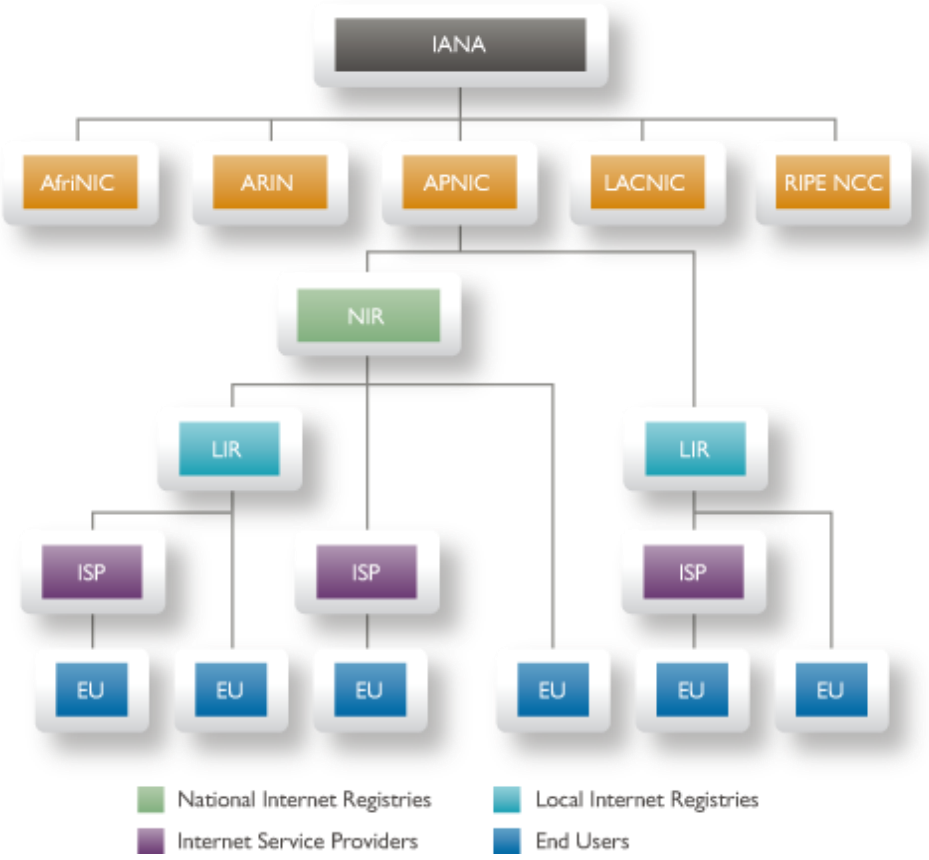
Địa chỉ Unicast định danh toàn cầu chính là không gian địa chỉ IPv6 được các tổ chức quản lý tài nguyên IP/ASN quản lý và phân bổ lại cho các tổ chức tham gia hoạt động Internet. Việc phân hoạch, quản lý được đề cập trong tài liệu hướng dẫn này là để hỗ trợ các tổ chức có thể xây dựng kế hoạch tài nguyên khi đưa vào sử dụng vùng địa chỉ IPv6 Unicast định danh toàn cầu mà mình đã được cấp phát.

Trong các mục sắp tới, khái niệm "địa chỉ IPv6" được đề cập là cách viết thu gọn của "địa chỉ IPv6 định danh toàn cầu".

1.5. Phân cấp quản lý và phân bổ địa chỉ IPv6

1.5.1 Mô hình quản lý địa chỉ Internet (IPv4/IPv6) toàn cầu

Theo mô hình chung, không gian địa chỉ IP các loại và số hiệu mạng được quản lý thống nhất bởi tổ chức IANA. IANA sau đó cấp các không gian địa chỉ lớn theo /8 đối với IPv4, /12 đối với IPv6 và từng khối 1024 số đối với ASN cho các tổ chức quản lý tài nguyên cấp khu vực (Regional Internet Registry - RIR). Các RIR sau đó chịu trách nhiệm quản lý, phân bổ các khối địa chỉ và số nhận được từ IANA trong phạm vi khu vực mà mình phụ trách. Tổ chức quản lý địa chỉ khu vực Châu Á – Thái Bình Dương là Trung tâm mạng khu vực Châu Á – Thái Bình Dương (APNIC). Trong khu vực, APNIC ủy quyền quản lý địa chỉ trong phạm vi quốc gia cho một số Tổ chức quản lý địa chỉ quốc gia (National Internet Registry – NIR). Trung tâm Internet Việt Nam (VNNIC) được công nhận là NIR tại Việt Nam.



Hình 5: Phân cấp quản lý địa chỉ IP toàn cầu

1.5.2. Xin cấp địa chỉ IPv6 tại Việt Nam

Khi có nhu cầu đăng ký sử dụng IP, các tổ chức Việt Nam có thể xin cấp từ một trong hai nguồn sau đây:

a. Tại các nhà cung cấp dịch vụ Internet (ISP).

Hiện tại 100% các nhà cung cấp dịch vụ Internet lớn ở Việt Nam đều đã sẵn sàng về tài nguyên địa chỉ IPv6 để cung cấp cho khách hàng. Khách hàng kết nối của các ISP này có thể liên hệ với các nhà cung cấp dịch vụ của mình để xin cấp địa chỉ IPv6. Tuy nhiên, cũng giống như IPv4, địa chỉ IPv6 cấp từ ISP là địa chỉ phụ thuộc. Có nghĩa là khi khách hàng không ký hợp đồng đấu nối với ISP nữa, khách hàng phải trả lại vùng địa chỉ IPv6 đã xin cho ISP và chuyển sang sử dụng IPv6 của nhà cung cấp dịch vụ mới.

b. Tại Trung tâm Internet Việt Nam (VNNIC).

Trung tâm Internet Việt Nam (VNNIC) là tổ chức quản lý địa chỉ cấp quốc gia, quản lý thống nhất toàn bộ không gian địa chỉ (IPv4, IPv6) tại Việt Nam. Toàn bộ các ISP tại Việt Nam sử dụng các vùng địa chỉ IP cấp phát từ VNNIC để phục vụ cho hoạt động mạng và cấp lại cho khách hàng. Cũng giống như IPv4, địa chỉ

IPv6 được cấp từ VNNIC là địa chỉ độc lập. Tổ chức đã được cấp địa chỉ IPv6 có thể mang vùng địa chỉ đã cấp kết nối tới bất kỳ nhà cung cấp dịch vụ kết nối nào.

Theo quy định tại thông tư số 189/2010/TT-BTC ngày 24/11/2010 của Bộ Tài chính quy định về phí, lệ phí tên miền quy định mức thu, chế độ thu, nộp và quản lý sử dụng phí, lệ phí tên miền quốc gia và địa chỉ Internet của Việt Nam, các tổ chức đã được cấp và đang duy trì sử dụng địa chỉ IPv4 sẽ có quyền lợi được sử dụng miễn phí một lượng địa chỉ IPv6 tương ứng với số lượng địa chỉ IPv4 đang duy trì.

Quy định, quy trình thủ tục xin cấp IPv6 được công bố tại Website: www.diachiip.vn.

1.6. Tiêu chuẩn hóa địa chỉ IPv6 và các khuyến nghị về tuân thủ tiêu chuẩn IPv6.

Ý tưởng về việc phát triển giao thức Internet mới thay thế IPv4 được giới thiệu tại cuộc họp IETF ngày 25 tháng 7 năm 1994, trong RFC1752[1], giới thiệu thủ tục IP phiên bản mới. Sau nhiều năm nghiên cứu, những hoạt động cơ bản của thế hệ địa chỉ này đã được định nghĩa và công bố năm 1998 trong một chuỗi tài liệu tiêu chuẩn từ RFC2460 tới RFC2467. Tiếp theo, IETF công bố RFC2373[2], mô tả cấu trúc địa chỉ IP phiên bản 6 và RFC2374[3], mô tả dạng địa chỉ IPv6 định danh toàn cầu. Trải qua thời gian dài điều chỉnh, cả hai tài liệu này được thay thế cập nhật bởi hai RFC mới. Đó là RFC3513[4], cấu trúc đánh địa chỉ IP phiên bản 6 và RFC3587[5], mô tả dạng thức địa chỉ IPv6 định danh và định tuyến toàn cầu. Đồng thời, rất nhiều RFC khác được công bố, định nghĩa tiêu chuẩn hóa cho những chức năng của IPv6, mô tả phiên bản mới hỗ trợ IPv6 cho các dịch vụ như DNS, DHCP…

Thời điểm hiện nay, những tiêu chuẩn cơ bản cho hoạt động của giao thức Internet phiên bản 6 đã được hoàn thiện. Tài liệu chuẩn hóa các đặc tính gia tăng, các tiêu chuẩn mở rộng đã và đang được tiếp tục phát triển, sửa đổi nhằm đáp ứng yêu cầu thực tế.

Để đảm bảo hoạt động ổn định của thủ tục IPv6 trên mạng lưới và dịch vụ, nhiều tổ chức chuyên gia quốc tế đã tiến hành các nghiên cứu và đưa ra khuyến nghị về yêu cầu phải đảm bảo tuân thủ các đặc tính quy định bởi bộ RFC IPv6 đối

[1] RFC1752 - The Recommendation for the IP Next Generation Protocol
2 RFC2373 - IP Version 6 Addressing Architecture
3 RFC2374 - An IPv6 Aggregatable Global Unicast Address Format
4 RFC3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
5 RFC3587 - IPv6 Global Unicast Address Format

với một số thể thức mô hình mạng (gọi là tài liệu đặc tả khuyến nghị về thủ tục IPv6).

Tổ chức sử dụng IPv6 có thể tham khảo bộ bộ đặc tả được ban hành bởi Ủy ban khuyến nghị tiêu chuẩn viễn thông của Cơ quan quản lý viễn thông Singapore IDA. Tài liệu có tiêu đề "Singapore Internet Protocol Version 6 (IPv6) Profile – Singapore, được cung cấp tại Website của IDA: http://www.ida.gov.sg.

Thông tin chi tiết về tài liệu tiêu chuẩn hóa IPv6 được cung cấp tại trang web của nhóm làm việc về IPv6 của IETF (http://www.ietf.org/html.charters/IPv6-charter.html) và những nhóm làm việc khác liên quan đến IPv6 của IETF.

CHƯƠNG 2: HƯỚNG DẪN VỀ PHÂN HOẠCH VÀ SỬ DỤNG ĐỊA CHỈ IPV6 CHO MẠNG LƯỚI.

Xây dựng kế hoạch phân bổ địa chỉ cho mạng lưới (phân hoạch địa chỉ) là việc làm cần thiết của mọi tổ chức khi đưa vùng địa chỉ đã được cấp phát, phân bổ vào sử dụng. Một tổ chức đã có mạng lưới IPv4 tất yếu đã có sẵn một kế hoạch địa chỉ IPv4 cho mô hình mạng (network topology). Sang thời kỳ cạn kiệt IPv4, khi triển khai sử dụng IPv6, sẽ thật tiện lợi nếu có thể sử dụng luôn sơ đồ phân hoạch của IPv4 để chuyển đổi áp dụng sang IPv6. Tuy nhiên điều này là không thể do các đặc trưng khác biệt trong thiết kế và hoạt động của hai thế hệ địa chỉ Internet. Vì vậy, tổ chức cần có các định hướng suy nghĩ riêng để quy hoạch sử dụng IPv6 một cách tốt nhất, nhằm xây dựng một kế hoạch phân hoạch địa chỉ phù hợp cho mạng lưới.

2.1. Mục tiêu trong phân hoạch vùng địa chỉ IPv6. Sự khác biệt so với phân hoạch IPv4

Phân hoạch địa chỉ IPv4 hạn chế tổ chức sử dụng địa chỉ trong một số tùy chọn nhất định do sự hạn chế của số lượng IPv4. Địa chỉ IPv4 được phân hoạch chủ yếu theo hiệu quả sử dụng địa chỉ. Yếu tố cơ bản để phân mạng con (subnet) trong IPv4 là dựa trên số lượng host thuộc về subnet.

Trong phân hoạch địa chỉ IPv6, đây không còn là các yếu tố hàng đầu điều khiển toàn bộ việc tạo kế hoạch phân hoạch địa chỉ, thay vì đó là việc bao quát mô hình mạng, phác thảo kế hoạch an ninh an toàn và tính thuận lợi giản tiện trong việc quản trị, vận hành.

Lượng địa chỉ khổng lồ cùng với việc IPv6 được thiết kế có một số quy định cơ bản về cấu trúc đánh số (ví dụ định danh giao diện 64 bít) để phục vụ cho các thủ tục hoạt động thiết yếu khiến cho việc chuẩn bị một kế hoạch phân hoạch địa chỉ tối ưu là rất cần thiết. Khi phân hoạch địa chỉ IPv6, tổ chức phải tạm quên một số nguyên tắc, cũng như các thói quen sử dụng quá thông dụng đến mức trở thành nguyên lý của IPv4 . Ví dụ như việc gắn prefix /30 cho đường kết nối. Đối với IPv6, mặc dù chỉ sử dụng có 2 địa chỉ, nhưng các khuyến nghị đều khẳng định cần quy hoạch dành cả /64 (2^{64} địa chỉ cho đường kết nối).

Một kế hoạch địa chỉ phù hợp là nhân tố hỗ trợ đắc lực cho công tác quản lý mạng. Kế hoạch phân hoạch IPv6 hiệu quả cần đảm bảo được các mục tiêu:

- Chính sách an ninh bảo mật có thể dễ dàng thực hiện. Dễ dàng cấu hình access list và firewall.
- Địa chỉ dễ dàng được tra vết. Trong cấu trúc phân hoạch địa chỉ có thông tin giúp xác định rõ loại mục đích sử dụng (use type) hoặc vị trí mà địa chỉ đó được sử dụng.
- Kế hoạch địa chỉ có khả năng mở rộng.Có quy hoạch dành cho mục đích sử dụng mới và vị trí mới.

Để thực hiện được một kế hoạch phân hoạch vùng địa chỉ IPv6 tối ưu, người phụ trách phải xác định được một số lựa chọn cụ thể. Tuy nhiên, việc cố gắng đạt được sự hiệu quả trong phân hoạch theo mục đích và mô hình sử dụng có thể dẫn tới sự "lãng phí" một lượng lớn tài nguyên địa chỉ. Việc cần thiết là cân nhắc một cách hiệu quả nhất mô hình phân hoạch địa chỉ . Tài liệu hướng dẫn này sẽ giúp các tổ chức sử dụng tài nguyên xác định được các tinh thần nguyên tắc cơ bản trong phân hoạch vùng địa chỉ IPv6.

2.2. Cấu trúc cơ bản trong phân hoạch địa chỉ

Về cơ bản, phân hoạch địa chỉ là căn cứ một số yếu tố cơ bản của mạng lưới (mô hình - topology mạng; chính sách định tuyến – routing policy; chính sách bảo mật – security plan) để xác định các thông số và phân chia vùng địa chỉ gốc thành các khối phù hợp với mô hình mạng. Trong đó, cơ bản nhất là các thông số về vị trí (location), dạng mục đích sử dụng (use type). Chi tiết hơn, trong một mạng lưới có thể có các yếu tố sau đây được lấy làm căn cứ để xây dựng kế hoạch phân hoạch địa chỉ:

- Vùng hoặc vị trí địa lý.
- Vùng cấp dưới của một vùng địa lý lớn.
- Dạng mục đích sử dụng (ví dụ backbone, data center, remote connectivity, desktop…).
- Loại khách hàng (staff, guest, student, vendor)
- Phòng ban (sales, marketing, tech)
- Virtual LAN (VLAN)

Đối với hai thông số (vị trí) và mục đích sử dụng (use type), tùy theo lựa chọn của tổ chức sử dụng, việc phân hoạch địa chỉ có thể lấy các bít đầu phân bổ vị trí trước, tiếp theo là mục đích sử dụng hoặc phân bổ theo mục đích sử dụng trước và vị trí sau.

2.2.1 Phân hoạch theo vị trí trước

Khi vị trí được ưu tiên phân hoạch trước tiên, có nghĩa có thể là mỗi tòa nhà, vị trí chi nhánh mạng … được phân một nhóm địa chỉ nhất định. Ưu điểm nổi bật của việc đưa lựa chọn phân hoạch theo vị trí lên trước tiên đó là tối ưu hóa bảng thông tin định tuyến. Tất cả các mạng trong một vị trí địa lý cụ thể sẽ được tổ hợp trong một route duy nhất trong bảng thông tin định tuyến, vì vậy thông tin trong bảng thông tin định tuyến sẽ được tối ưu hóa.

Ví dụ về phân hoạch theo vị trí trước:

2001:db8:1234:	L	L	L	L	T	T	T	T	B	B	B	B	B	B	B	B	::/64

Trong ví dụ này, tổ chức được cấp vùng địa chỉ 2001:db8:1234::/48 đã dành 4 bít đầu (bít L) để phân hoạch cho vị trí (location), như vậy có thể có 16 phân mạng theo vị trí địa lý. 4 bít tiếp theo (bít T) là để phân hoạch mục đích sử dụng. Như vậy trong mỗi phân mạng vị trí địa lý có thể có 16 nhóm theo mục đích sử dụng khác nhau và trong mỗi phân mạng theo mục đích sử dụng tại một vị trí địa lý nhất định có thể có 2^8 = 256 mạng con (subnet).

2.2.2 Phân hoạch theo mục đích sử dụng trước

Nếu lấy mục đích sử dụng làm yếu tố ưu tiên phân hoạch trước, việc tối ưu hóa bảng thông tin định tuyến là không đạt được, bởi vì cùng một mục đích sử dụng, sẽ có nhiều vùng địa chỉ được phân hoạch cho các vị trí khác nhau. Trên thực tế, đây cũng không phải là vấn đề quá lớn đối với router, trừ các mạng quá lớn với rất nhiều vị trí địa lý khác nhau.

Ưu điểm lớn nhất của mô hình phân hoạch theo mục đích sử dụng trước là sự thuận lợi dễ dàng trong việc áp dụng chính sách bảo mật (security policy). Phần lớn việc thiết lập chính sách bảo mật trên tường lửa (firewall) là căn cứ vào mục đích sử dụng chứ không căn cứ vào vị trí của mạng. Đó là lí do tại sao các tường lửa thường yêu cầu một chính sách (policy) cho một mục đích sử dụng.

Ví dụ về phân hoạch theo mục đích sử dụng trước

2001:db8:1234:	T	T	T	T	L	L	L	L	B	B	B	B	B	B	B	B	::/64

Tùy thuộc vào mục tiêu của tổ chức sử dụng tài nguyên địa chỉ, mô hình mạng, mô hình chính sách bảo mật, tổ chức quyết định lựa chọn việc phân hoạch

theo vị trí hay mục đích sử dụng trước. Đối với các mạng quy mô nhỏ, các chuyên gia khuyến nghị nên lựa chọn theo mục đích sử dụng trước tiên để dễ dàng tổ hợp với chính sách bảo mật sẵn có của mạng.

Đối với đa phần các mạng lớn, việc phân chia chỉ theo một tầng (vị trí và mục đích sử dụng) thường không đáp ứng được nhu cầu của mạng. Do vậy bên cạnh tầng phân cấp chính đầu tiên, sẽ là xen kẽ thêm các tầng phân cấp thứ cấp tiếp theo để xây dựng nên một mô hình phân hoạch địa chỉ mạng.

- Khuyến nghị về quyết định số lượng nhóm

Để xây dựng một mô hình phân hoạch địa chỉ đầy đủ hiệu quả, cán bộ thực hiện cần có tổng hợp tổng thể về mô hình mạng, số lượng nhóm vị trí cần thiết, số lượng mục đích sử dụng cần thiết, quyết định số lượng phân tầng chính – phụ. Một số khuyến nghị lưu ý như sau:

- Trước tiên xác định số lượng vị trí hoặc số lượng mục đích sử dụng trong tổ chức.
- Cộng thêm số lượng này một nhóm (yêu cầu cho mạng backbone và các mạng cơ sở hạ tầng khác).
- Đối với phân mạng theo vị trí, cộng thêm một nhóm cho tất cả các mạng mà không có vị trí cố định. Đây là những mạng cho VPN và cho đường hầm.
- Thêm một hoặc hai nhóm cho mục đích mở rộng trong tương lai.

2.3. Một số mức phân cấp mặc định của địa chỉ IPv6 định danh toàn cầu

Ngay từ thiết kế tiêu chuẩn ban đầu, địa chỉ IPv6 đã có một số mức phân cấp mặc định mà toàn bộ hoạt động Internet toàn cầu cần tuân thủ. Cụ thể như sau:

2.3.1. Định danh giao diện và kích cỡ mạng con (subnet)

Định danh giao diện (Interface ID) là 64 bít cuối cùng trong một địa chỉ IPv6. Số định danh này sẽ xác định một giao diện trong phạm vi một mạng con (subnet). Định danh giao diện phải là số duy nhất trong phạm vi một subnet.

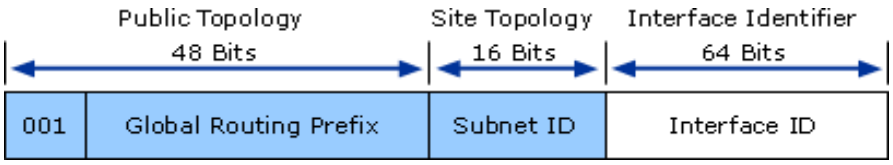
Kích thước subnet của IPv6 luôn là /64. Đây là điểm khác biệt hoàn toàn so với IPv4. Khi phân hoạch địa chỉ IPv4, kích thước mạng con được quyết định theo dung lượng máy trạm sao cho hiệu quả sử dụng địa chỉ là tối đa (ví dụ subnet IPv4 cần 2 địa chỉ, sẽ có kích thước /30; subnet cần 6 địa chỉ, sẽ được quy hoạch kích thước /29). Trong khi đó dù mạng con lớn hay nhỏ, IPv6 đã quy chuẩn kích thước subnet là /64.

Trên lý thuyết, IPv6 có thể có các kích thước subnet khác tuy nhiên việc này có thể dẫn đến hoạt động không ổn định của thiết bị do kích thước subnet /64 đã được quy định thành tiêu chuẩn hóa trong RFC của IETF. Chính vì vậy trong IPv6, subnet có số lượng địa chỉ sử dụng rất nhỏ như đường kết nối point-to-point cũng sẽ được phân hoạch cùng kích thước /64 như đối với một mạng con subnet có số lượng địa chỉ sử dụng rất lớn.

2.3.2.Phân cấp định tuyến và phân bổ

Địa chỉ IPv6 định danh toàn cầu được phân cấp định tuyến theo một số mức cố định như sau:

- *Phần cố định:* 3 bít đầu tiên 001 xác định dạng địa chỉ unicast định danh toàn cầu.
- *Phần định tuyến toàn cầu*: 45 bit tiếp theo. Các tổ chức quản lý sẽ phân cấp quản lý vùng địa chỉ này, chuyển giao lại cho các tổ chức khác. Kích thước vùng địa chỉ nhỏ nhất quảng bá ra ngoài phạm vi một mạng của một tổ chức (một site) theo cấu trúc này là /48.
- *Vùng định tuyến trong site:* 16 bít tiếp theo là không gian địa chỉ mà một mạng người sử dụng (site) có thể tự mình quản lý, phân bổ, cấp phát và tổ chức định tuyến bên trong mạng của mình. Với một vùng địa chỉ /48, tổ chức có thể tạo nên 65,536 subnet cỡ /64 hoặc nhiều cấp định tuyến phân cấp hiệu quả sử dụng trong mạng của tổ chức.



Hình 6: Phân cấp định tuyến địa chỉ IPv6 Unicast toàn cầu

RFC 5375 quy định kích thước phân bổ mặc định cho ISP là /32. Theo chính sách quản lý địa chỉ hiện tại, kích thước vùng địa chỉ mà các tổ chức quản lý địa chỉ cấp khu vực (RIR) phân bổ cho ISP là /32 (ngoại trừ các trường hợp đặc biệt, giải trình được quy mô lớn của mạng). Kích thước vùng địa chỉ thông thường cấp cho mạng của người sử dụng cuối cùng là /48.

Như vậy, cấu trúc phân bổ địa chỉ IPv6 định danh toàn cầu như sau:

<table>
<tr><td>3 bits</td><td>9 bits</td><td>20 bits</td><td>16 bits</td><td>16 bits</td><td>64 bits</td></tr>
<tr><td>001</td><td>IANA to RIR</td><td>RIR to ISP</td><td>ISP to End Site</td><td>Net</td><td>Interface ID</td></tr>
<tr><td>001</td><td>IANA to RIR</td><td colspan="2">RIR to End Site</td><td>Net</td><td>Interface ID</td></tr>
<tr><td>3 bits</td><td>9 bits</td><td colspan="2">36 bits</td><td>16 bits</td><td>64 bits</td></tr>
</table>

Hình 7: Cấu trúc phân bổ địa chỉ IPv6 định danh toàn cầu

Dưới đây là các khuyến nghị gốc khuyến nghị kích thước không gian IPv6 cho người sử dụng (end-user):

- /48 (65536 mạng con subnet) cho các mạng (site) thông thường, ngoại trừ trường hợp người sử dụng cực lớn.
- /64 (một mạng con) khi biết chắc rằng chỉ có duy nhất một mạng con là cần thiết trong mô hình phân hoạch.
- /128 (một địa chỉ) khi biết chắc chắn tuyệt đối rằng chỉ một thiết bị duy nhất kết nối.

Mặc dù các RFC gốc chỉ khuyến nghị kích thước /48 cấp cho mạng (site), sau thời gian ứng dụng thực tiễn IPv6, RFC 6177 (còn được nhắc đến là Best Curren Practice 157) thay đổi điều này và khuyến nghị rằng trong phân hoạch cấp tài nguyên địa chỉ IPv6, kích cỡ block/prefix nên cân nhắc sao cho phù hợp nhất với kích thước nhu cầu của người sử dụng. Ví dụ /48 là quá lớn cho nhu cầu của một người sử dụng tại nhà, tuy nhiên nếu cấp /64 thì lại chỉ có duy nhất một subnet do vậy giới hạn khả năng phát triển. Vì vậy khối địa chỉ /56 hoặc /60 có thể là kích thước phù hợp hơn đối với khách hàng.

RFC 6177 cũng nhấn mạnh việc phân hoạch địa chỉ, đặc biệt cho mạng khách hàng cần đảm bảo yếu tố "hơn" chứ không nên "kém". Có nghĩa cần tránh tối đa nguy cơ việc mạng khách hàng phải đánh số lại khi chuyển sử dụng một khối lớn hơn hoặc cấp thêm vùng địa chỉ. Chính vì vậy, cần cấp cho khách hàng /56 nếu có bất cứ nghi ngờ nào là /60 sẽ không đáp ứng được nhu cầu dài hạn của khách hàng; cấp /48 cho khách hàng nếu có bất cứ nghi ngờ nào là /56 sẽ không đáp ứng được nhu cầu dài hạn.

Theo hướng dẫn của Trung tâm quản lý mạng khu vực Châu Á – Thái Bình Dương (APNIC), các ISP nên áp dụng các kích thước phân cấp sau đây:

- Kích cỡ vùng địa chỉ cấp phát cho mạng sử dụng cuối lớn nhất là /48, nhỏ nhất là /64. Nếu cấp thêm /48 cho một mạng sử dụng cuối, cần thẩm định các tài liệu, văn bản về cấu trúc mạng.
- Các mạng vận hành (POP) được cấp /48.
- Đối với khách hàng:
    - Phân khách hàng thành các loại và cấp địa chỉ: /56 hoặc /60 hoặc /64. Ví dụ: /64 nếu chắc chắn chỉ có một LAN; /60 nếu là mạng nhỏ; /56 cho mạng trung bình; /48 cho mạng lớn.
    - Đối với khách hàng Broadband: DHCPv6 pool là một /48. DHCPv6 cấp /60 cho mỗi khách hàng.
    - Đối với khách hàng leasedline: Về nguyên tắc cấp /48 tuy nhiên có thể cấp trước /56 và dự trữ cả /48 cho việc phát triển của mạng khách hàng.

2.4. Phân hoạch một cách linh hoạt cho nhu cầu mở rộng trong tương lai

Thông thường, số lượng vị trí cũng như số lượng mục đích sử dụng có thể thay đổi một cách không tính đếm được tại thời điểm tiến hành xây dựng kế hoạch phân hoạch địa chỉ. Trong trường hợp này, IETF có tiêu chuẩn RFC 3531 khuyến nghị chiến lược phân hoạch một cách linh động để có thể tùy biến tốt nhất với việc mở rộng trong tương lai, tránh phải đánh số lại trong quá trình phát triển mạng lưới.

Theo RFC3531, nguyên tắc phân hoạch cơ bản vẫn là phân chia các vùng bít theo các yếu tố xác định phân nhóm (ví dụ vị trí, loại dịch vụ) tuy nhiên khi sử dụng thực tế các phân mạng, việc đánh số bít trong nhóm phân mạng không áp dụng mặc định thứ tự đếm thông thường của binary mà được áp dụng theo ba nguyên tắc sau:

- Từ trái qua trước (leftmost) đối với nhóm bên trái. Đây là thứ tự đảo ngược của đếm số binary thông thường

Thứ tự Đánh số
1 00000000
2 10000000
3 01000000
4 11000000
5 00100000
6 10100000
7 01100000
8 11100000
9 00010000
...

- Từ phải qua trước (rightmost) với nhóm bên phải. Đây là thứ tự đếm binary thông thường

Thứ tự Đánh số
1 00000000
2 00000001
3 00000010
4 00000011
5 00000100
6 00000101
7 00000110
8 00000111
9 00001000
...

- Từ trung tâm ra hai bên (centermost) đối với nhóm ở giữa theo thuật toán như sau:
  - Vòng đầu tiên lựa chọn duy nhất bít giữa. Tiếp theo tạo tất cả các tổ hợp có thể với bít đã lựa chọn.
  - Vòng thứ hai bổ sung thêm một bít. Sau đó lại tạo tất cả các tổ hợp có thể với bít đã thêm và cứ thể lặp lại cho đến khi hết toàn bộ việc đánh số phân vùng địa chỉ.

Thứ tự Đánh số
1 00000000
2 00001000
3 00010000
4 00011000
5 00000100
6 00001100
7 00010100
8 00011100
9 00100000
...

Khi áp dụng ba thứ tự đánh số như trên, thực tế sử dụng các bit địa chỉ để đánh số mạng lan dần từ trái qua phải, giữa sang hai bên và phải sang trái, trong khi các bít gần biên giới ban đầu vẫn còn được giữ nguyên giá trị 0 khi chưa dùng đến. Do vậy, biên giới giữa các nhóm có thể xác định lại nếu nhu cầu mạng lưới theo thời gian thay đổi. Tất nhiên, nếu tổ chức xác định lại vị trí biên, các nguyên tắc bảo mật của firewall và cấu hình định tuyến trên router phải cập nhật lại.

Ví dụ cụ thể như sau. Trong các hình vẽ minh họa, gạch đậm là biên giới ban đầu của phân vùng địa chỉ. Biên giới này sau đó di động khi tổ chức sử dụng thực tế dần các vùng địa chỉ.

2001:db8:1234:	L	L	L						T	T						B	::/64
2001:db8:1234:	L	L	L						T	T			B	B	B	B	::/64
2001:db8:1234:	L	L	L					T	T	T			B	B	B	B	::/64
2001:db8:1234:	L	L	L	L	L	L		T	T	T			B	B	B	B	::/64
2001:db8:1234:	L	L	L	L	L	L		T	T	T	T		B	B	B	B	::/64

2.5. Sử dụng số VLAN

Một cách tiếp cận khác khi phân hoạch địa chỉ là sử dụng số VLAN là số subnet. Trong những mạng mà phần lớn subnet là VLAN sẽ có sẵn số VLAN, do vậy việc sử dụng số VLAN là số subnet sẽ khiến cho quá trình quản trị VLAN đơn giản hơn do chỉ có một số cần quản lý.

Ví dụ trong một mạng /48 (tức có 16 bít đánh mạng subnet), mô hình phân mạng có thể dễ dàng áp dụng luôn như sau (kích thước số VLAN là 12 bít):

2001:db8:1234:	V	V	V	V	V	V	V	V	V	V	V	V	B	B	B	B	::/64
2001:db8:1234:	B	B	B	B	V	V	V	V	V	V	V	V	V	V	V	V	::/64

Do số VLAN được viết theo dạng decimal, còn địa chỉ IPv6 thì lại được viết theo dạng hexadecimal, nếu tiếp cận theo hướng như trên thì phải chuyển đổi dạng thức hiển thị giữa decimal, hexadecimal, do vậy cũng không thể đạt được sự đơn giản trong quản trị mạng VLAN.

Để tránh điều này, có thể lấy luôn con số biểu diễn thập phân của VLAN thay cho số hexadecimal của subnet. Trong ví dụ trên, VLAN 2783 sẽ trở thành phân mạng 2001:db8:1234:2783::/64. Đối với lựa chọn này, ngoài các subnet là số VLAN, sẽ còn lại 4 bít không tổ hợp với số VLAN để sử dụng cho các mạng khác.

Trong cả hai cách đánh số theo số VLAN nói trên, có thể thấy không có bít đánh mã vị trí và mục đích sử dụng. Do vậy cách đánh số này chỉ phù hợp khi phân hoạch đánh số VLAN ID.

Bảng sau cho thấy ví dụ ánh xạ của cả hai lựa chọn

VLAN ID	IPv6 decimal	IPv6 hexadecimal (bít B ở trước)	IPv6 hexadecimal (bít B ở sau)
1	2001:db8:1234:0001::/ 64	2001:db8:1234:0010::/ 64	2001:db8:1234:0001::/ 64
12	2001:db8:1234:0012::/ 64	2001:db8:1234:00c0::/ 64	2001:db8:1234:000c::/ 64
2783	2001:db8:1234:2783::/ 64	2001:db8:1234:adf0::/ 64	2001:db8:1234:0adf::/ 64
4094	2001:db8:1234:4094::/ 64	2001:db8:1234:ffe0::/ 64	2001:db8:1234:0ffe::/ 64

2.6. Đánh địa chỉ cho đường kết nối Point-to-Point

Trong thiết kế ban đầu, tài liệu tiêu chuẩn RFC4291 của IETF quy định gắn /64 cho kết nối trực tiếp Point-to-Point. Tuy nhiên qua quá trình sử dụng thực tế, các chuyên gia kỹ thuật nhận thấy có những trường hợp việc sử dụng /64 cho đường kết nối point-to-point gây ra vấn đề cho mạng, xảy ra trong một số cấu hình router khi router gửi gói tin tới các địa chỉ không sử dụng trong subnet được router phía bên kia tiếp nhận, xử lý và gửi lại. Sau đó lại tiếp tục được nhận, xử lý và gửi lại bởi router bên này, dẫn đến vòng lặp đi lặp lại tạo tải dư thừa ảnh hưởng đến hiệu năng mạng lưới.

Chính vì vậy trên thực tế, các chuyên gia kỹ thuật khuyến nghị có thể sử dụng các kích thước vùng mạng khác /64 trong đường kết nối. Cụ thể:

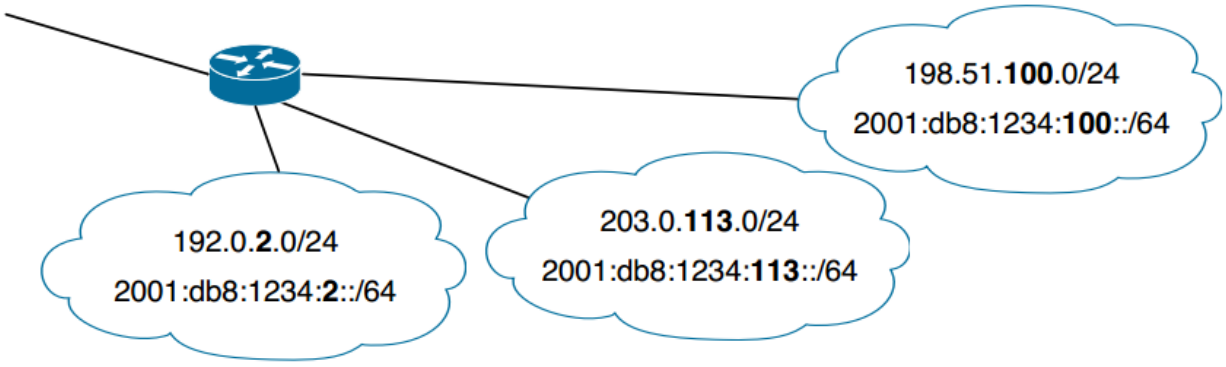
- /127: có thể là phù hợp do IPv6 không có địa chỉ broadcast. Tuy nhiên khi sử dụng /127 (gồm 2 địa chỉ trong một phân mạng), địa chỉ toàn 0 theo quy chuẩn của IETF là địa chỉ anycast của router "all router anycast address", có nghĩa tất cả các router trên mạng đều tiếp nhận địa chỉ này. Trước đây có ý kiến cho rằng, một số nhà sản xuất thiết bị không kích hoạt tính năng anycast toàn bộ router khi đó việc sử dụng /127 cho đường kết nối là phù hợp nhưng nếu thay thế thiết bị bằng thiết bị của một số nhà sản xuất khác, khi đó có thể gây ra vấn đề trong hoạt động mạng lưới. Tuy nhiên gần đây, sử dụng /127 cho đường kết nối đã được khuyến nghị trong tiêu chuẩn hóa RFC 6164.
- /126: Việc sử dụng subnet /126 cho phép tránh được địa chỉ toàn 0. Tuy nhiên theo RFC 2526, địa chỉ cao nhất 128 trong các subnet được dành cho địa chỉ various anycast. Trên thực tế cho thấy việc sử dụng /126 cho đường kết nối không gặp vấn đề ảnh hưởng nào.
- /120: Cho phép tránh được tất cả các trường hợp địa chỉ đã được quy hoạch dành cho địa chỉ anycast.
- /112: Cho phép tránh được tất cả các địa chỉ anycast và còn có ưu điểm là toàn bộ 4 bít hexa sau colon cuối cùng trong định danh địa chỉ IPv6 trong phân mạng.

Như vậy, có vẻ kích thước mạng /112 là phương án tối ưu. Tuy nhiên việc tối thiểu hóa các địa chỉ dư thừa trên phân mạng đường kết nối cũng nên được tính toán đến để tránh các tấn công theo kiểu tận dụng bảng neighbor cache, trong đó kẻ tấn công quét toàn bộ các địa chỉ trong một subnet và router phải xử lý thuật toán Neighbor Discovery cho toàn bộ các địa chỉ này gây cạn kiệt hiệu năng hoạt động. do vậy tốt nhất, có thể sử dụng phân mạng kích thước 127, /126 hoặc /120 nhưng phân hoạch toàn bộ /64 cho đường kết nối.

2.7. Một số kinh nghiệm ánh xạ địa chỉ trực tiếp IPv4 – IPv6 để trực quan và tạo điều kiện thuận lợi cho quản trị

2.7.1. Ánh xạ mạng con subnet

Nếu mạng IPv4 sẵn có đang sử dụng subnet /24, có thể ánh xạ trực tiếp subnet này thành subnet /64 của địa chỉ IPv6 bằng cách gắn luôn cụm cuối của số IPv4 trong prefix (ví dụ số 113 của subnet 203.0.113.0/24) vào thành subnet IPv6. Ví dụ: subnet IPv4 203.0.113.0/24 ánh xạ sang thành subnet 2001:db8:1234:113::/64 trong phân hoạch hình dưới.



Hình 8: Ánh xạ mạng con IPv4 – IPv6

Đối với thiết bị mạng thiết yếu (router, switch, firewall, máy chủ), có thể sử dụng số cuối cùng của địa chỉ IPv4 làm địa chỉ IPv6 để gợi nhớ sự liên hệ giữa IPv4 – IPv6, tạo thuận lợi cho việc quản trị. Ví dụ địa chỉ IPv4 192.0.2.123 trong subnet 192.0.2.0/24 có thể ánh xạ vào địa chỉ IPv6 2001:db8:1234:2::123 trong subnet 2001:db8:1234:2::/64.

Khi ánh xạ như thế này, việc liên kết giữa IPv4 và IPv6 rất dễ dàng nhận ra được. Tuy nhiên việc ánh xạ này chỉ thực hiện được khi IPv4 subnet là /24 do nếu kích thước mạng nhỏ hơn /24, không thể có sự ánh xạ mỗi một subnet /24 IPv4 tương ứng với một subnet /64 của IPv6. Ví dụ, với hai địa chỉ 172.31.5.14 và 172.31.5.18 của hai mạng 172.31.5.0/28 và 172.31.5.16/28 ánh xạ sang 2 địa chỉ cùng một subnet 2001:db8:1234:5::/64. Còn đối với kích thước mạng IPv4 lớn hơn

/24, ví dụ hai địa chỉ 10.0.8.250 và 10.0.9.5, thuộc cùng subnet 10.0.8.0/23 thì ánh xạ thành các địa chỉ 2001:db8:1234:8::250 và 2001:db8:1234:9::5, thuộc hai subnet /64 khác nhau của IPv6.

2.7.2. Ánh xạ trực tiếp địa chỉ IPv4 – với địa chỉ IPv6.

Nếu địa chỉ IPv4 không thuộc subnet /24, có thể ánh xạ trực tiếp địa chỉ IPv4 sang địa chỉ IPv6 bằng cách lấy 32 bít địa chỉ IPv4 thành 32 bit cuối của địa chỉ IPv6. Tuy nhiên do cách biểu diễn địa chỉ khác nhau (IPv4 biểu diễn dạng decimal, IPv6 biểu diễn dạng hexa. Do đó khi 32 bít IPv4 được chuyển đổi thành dạng số hexa, con số biểu diễn 32 bít đó chuyển dạng thức dẫn đến việc ánh xạ trực quan giữa hai địa chỉ không đạt được.

Ví dụ địa chỉ IPv4 192.0.2.123 ánh xạ vào địa chỉ IPv6: 2001:db8:1234:c0:ff:ee:192.0.2.123, chuyển viết sang dạng hexa thành 2001:db8:1234:c0:ff:ee:c000:27b

Tuy không có được sự ánh xạ trực quan gợi nhớ nhưng đây cũng là một cách thức ánh xạ có liên kết giữa IPv4 sẵn có và IPv6 gắn mới cho thiết bị, máy chủ.

2.8. Đánh số và quản lý địa chỉ các máy trạm, thiết bị trên mạng

Sau khi đã phân hoạch địa chỉ mạng, việc đánh số các máy trạm trên mạng có thể được thực hiện theo một trong các cách sau đây:

- Cấu hình địa chỉ tự động không trạng thái (stateless address configuration).
- Cấu hình địa chỉ bằng DHCPv6.
- Cấu hình bằng tay.

Đối với các máy trạm, các chuyên gia khuyến nghị áp dụng cách đánh địa chỉ tự động hoặc DHCPv6. Việc đánh số cấu hình địa chỉ bằng tay được khuyến nghị áp dụng cho các thiết bị như router, switch, firewall và máy chủ.

2.8.1. Cấu hình địa chỉ tự động không trạng thái.

Host sẽ tự cấu hình địa chỉ từ địa chỉ MAC và thông tin quảng bá của router (router advertisement - RA). Đối với cấu hình địa chỉ tự động, hiện các hệ điều hành phần lớn áp dụng thuật toán riêng tư (privacy), trong đó 64 bít định danh giao diện (interface indentifier) được thay thế bởi dãy số tạo ra theo thuật toán ngẫu nhiên, có thay đổi thay vì dùng 64 bít định danh tạo ra từ địa chỉ MAC. Việc sử dụng thuật toán privacy cho phép tránh được việc trùng lặp địa chỉ đối với các dạng thiết bị có trùng địa chỉ MAC, hoặc việc lần ngược địa chỉ MAC của thiết bị để giả mạo trạm trên mạng.

2.8.2. Cấu hình tự động bằng DHCPv6

Hiện phần lớn các hệ điều hành đã hỗ trợ DHCPv6. DHCPv6 có thể cung cấp địa chỉ cũng như các thông tin khác như địa chỉ máy chủ tên miền (name server), tương tự như trong DHCP IPv4. Vì vậy DHCPv6 có thể được ứng dụng theo 2 cách:

- DHCPv6 dùng để phân phối địa chỉ, đồng thời cung cấp thêm cho host các thông tin khác.
- Địa chỉ của máy trạm được cấu hình bằng thể thức cấu hình tự động không trạng thái và DHCPv6 chỉ mang thông tin hỗ trợ khác như địa chỉ máy chủ DNS.

Hai cờ trong thông điệp quảng bá của router sẽ xác định tùy chọn nào được sử dụng, chính vì lí do này và do DHCPv6 không cung cấp địa chỉ router mặc định (default gateway), các router IPv6 luôn luôn phải gửi các thông điệp quảng bá kể cả trong trường hợp trên mạng không sử dụng phương thức cấu hình địa chỉ tự động không trạng thái.

Chú ý rằng tùy thuộc vào cách thức thông điệp RA được quảng bá, việc sử dụng DHCPv6 và cấu hình địa chỉ tự động không trạng thái, một máy trạm có thể nhận được 2 địa chỉ và thậm chí là 3 nếu thuật toán privacy được áp dụng. Nếu địa chỉ được gắn bởi DHCPv6, các chuyên gia khuyến nghị nên cấu hình các bộ chuyển mạch switch để host chỉ sử dụng địa chỉ gắn cho chúng thông qua DHCPv6.

2.8.3. Cấu hình địa chỉ bằng tay

Các chuyên gia khuyến nghị, thực hiện cấu hình bằng tay địa chỉ các thiết bị như router, switch, firewall và máy chủ. Việc cấu hình tự động các thiết bị này có thể ảnh hưởng tới hoạt động của mạng lưới và dịch vụ. Ví dụ nếu một card mạng trên một máy chủ được thay thế, việc cấu hình địa chỉ tự động từ địa chỉ MAC sẽ làm địa chỉ của máy chủ hoặc thiết bị mạng thay đổi, trong khi thay đổi địa chỉ của các thiết bị mạng, máy chủ phải hạn chế tối đa để đảm bảo sự hoạt động ổn định của mạng lưới.

Đối với các thiết bị, máy chủ được cấu hình địa chỉ bằng tay, để tạo điều kiện dễ dàng hơn cho việc quản trị mạng, có một khuyến nghị là sử dụng cách đánh địa chỉ IPv6 có liên kết, gợi nhớ từ địa chỉ IPv4 sẵn có của thiết bị, máy chủ khi có thể.

2.9. Các lưu ý trong việc phân hoạch và đánh số địa chỉ IPv6

2.9.1. Lưu ý trong phân hoạch địa chỉ

Trên cơ sở các trải nghiệm kinh nghiệm thực tế, các chuyên gia khuyến nghị tổ chức sử dụng IPv6 lưu ý các điểm nên áp dụng và cần phải tránh dưới đây:

a) *Nên sử dụng biên theo danh giới số hexa (nibble boundaries) nhiều nhất khi có thể*

Tất cả các khuyến nghị và các tổ chức quản lý địa chỉ đều khuyến nghị tổ chức sử dụng IPv6 sử dụng biên giới số hexa (nibble boundary) nhiều nhất có thể làm ranh giới phân mạng để có một kế hoạch phân mạng rõ ràng dễ hiểu. Tuy nhiên, hạn chế của việc phân hoạch sử dụng biên giới số hexa là số lượng thể loại trong một cụm hạn chế ở số 16 (nếu dùng một số hexa duy nhất) hoặc 256 (nếu dùng 2) hoặc 4096 nếu sử dụng ba. Các kích thước prefix chia hết cho bốn đáp ứng được điều kiện biên giới theo ranh giới số hexa được sử dụng rất thông dụng: /32, /36, /40, /48, /52, /56, /60 và /64.

Việc phân hoạch không trùng biên số hexa dẫn đến khó nhớ và khó quản trị. Ví dụ dải địa chỉ không theo biên số hexa: 2001:db8::/61 gồm các địa chỉ từ 2001:0db8:0000:0000:0000:0000:0000:0000 đến 2001:0db8:0000:0007:ffff:ffff:ffff:ffff. Địa chỉ từ 2001:0db8:0000:0008:0000:0000:0000:0000 tới 2001:0db8:0000:000f:ffff:ffff:ffff:ffff lại thuộc phân mạng 2001:db8:0:8::/61, rất khó nhớ và khó quản trị.

b) *Sai lầm nếu quá quán triệt tinh thần "tiết kiệm" và giữ nguyên các tư tưởng trong phân hoạch sử dụng IPv4.*

Việc quá quán triệt tinh thần "tiết kiệm" và tư tưởng của việc sử dụng IPv4 có thể dẫn đến các sai lầm sau:

- *Không sử dụng kích thước /64 cho mạng con (subnet)*

Quá quán triệt tinh thần của IPv4, một tổ chức có thể lựa chọn sử dụng kích thước mạng con khác /64, ví dụ /120 thay vì /64 với các lí do: sợ lãng phí địa chỉ; để đảm bảo không dư thừa địa chỉ không sử dụng, hạn chế việc scan các địa chỉ không sử dụng như tư tưởng bảo mật trong IPv4.

Do địa chỉ IPv6 được thiết kế kích thước subnet cố định /64 (RFC 4291 "IPv6 Addressing Architecture"; RFC 5375 "IPv6 Addressing Considerations"), nếu tổ chức lựa chọn mạng con khác /64, các tính năng dưới đây không hoạt động:

- Neighbor Discovery
– Secure Neighbor Discovery
– Stateless Address Autoconfiguration (SLAAC)
– Microsoft DHCPv6
– Multicast with Embedded-RP
– Mobile-IPv6

Tổ chức phân hoạch địa chỉ sẽ không có được một kế hoạch hiệu quả nếu cho rằng:

– /64 cho mạng con là lãng phí

– /64 for đường kết nối (point-to-point) là lãng phí

– /48 cho một mạng (site) là lãng phí

- *Không cấp /48 cho mạng khách hàng và cho rằng /48 cho một mạng là quá lớn.*

Với 16 bít để phân hoạch cho các mạng khách hàng, tổ chức được cấp 32 có thể có 2^{16}= 65536 vùng /48 để cấp cho các site. Việc quy hoạch cấp /48 cho một mạng khách hàng đã được tiêu chuẩn hóa và sẽ đem lại sự đơn giản thuận lợi trong việc quản trị.

Việc một tổ chức quá quán triệt vào tư tưởng tính đếm kích thước của mạng khách hàng để phân hoạch vùng địa chỉ cấp cho site sẽ khiến tổ chức rơi quay trở lại vào bài toán phân hoạch theo tinh thần tiết kiệm tuyệt đối của IPv4.

c) Sai lầm nếu tập trung vào việc tính đếm "host" thay vì tính đếm "mạng con"

Trong IPv6, có một điểm lợi thế là mạng con subnet là kích cỡ /64. Với 2^{64} địa chỉ, một mạng con IPv6 có lượng địa chỉ đủ cho bất kỳ dung lượng nào. Khi phân hoạch IPv6, tư tưởng tập trung vào việc tính đếm dung lượng máy trạm (host) của IPv4 cần được thay thế bằng việc tập trung cân nhắc tính đếm số lượng mạng con cũng như mô hình mạng (network topology) (links,subnets, VLANs, ...) để từ đó tạo được một kế hoạch phân hoạch hiệu quả.

2.9.2. Một số điểm lưu ý trong đánh số máy trạm, thiết bị

Tổ chức nên lưu ý một số vấn đề sau:

a) Đảm bảo quảng bá của router

Trong hoạt động của IPv6, các thiết bị định tuyến router luôn luôn phải gửi các thông điệp quảng bá (RA) trên mạng mà mình phụ trách để giúp cho máy trạm lấy được các thông tin quan trọng. Chính vì vậy, trong các trường hợp sai sót trong cấu hình dẫn đến các quảng bá không hợp lệ từ thiết bị router khác hoặc thậm chí từ một host trên mạng sẽ làm sai lệch hoạt động của mạng. Điều này còn xảy ra trong trường hợp các RA giả mạo được chèn vào để tấn công mạng. Để hạn chế tuyệt đối khả năng này, IETF thiết kế tiêu chuẩn RFC 6105 cung cấp một hệ thống gác cho quảng bá định tuyến (RA Guard). Hệ thống này sẽ ngăn chặn các thông điệp quảng bá không hợp lệ được truyền tải đi trên mạng. Đặc tính RA Guard được thiết lập thông qua cấu hình trên thiết bị lớp 2 (Ethernet switch) để thiết bị chuyển mạch lọc

bỏ toàn bộ các thông điệp quảng bá không hợp lệ, chỉ cho phép các thông điệp quảng bá hợp lệ từ các nguồn tin cậy xác định trước được lan truyền đi trên mạng.

Khuyến nghị: Khi mua các thiết bị chuyển mạch lớp 2, tổ chức nên lưu ý kiểm tra khả năng hỗ trợ tính năng RA Guard của thiết bị.

b) Cấu hình địa chỉ cho máy chủ DNS.

Máy chủ DNS là một trong những thành phần có vai trò rất quan trọng trong hoạt động mạng. Địa chỉ của máy chủ DNS là một trong những dạng địa chỉ được gõ nhiều nhất, xuất hiện nhiều nhất trong các cấu hình nội bộ. Chính vì vậy, việc gắn địa chỉ cho máy chủ DNS cần đảm bảo tiêu chí ngắn gọn, dễ nhớ và đảm bảo tính ổn định. Do vậy với IPv6, nên quy hoạch riêng một subnet /64 cho máy chủ DNS với cấu hình địa chỉ ngắn gọn nhằm tránh khỏi nguy cơ phải đánh số lại khi có các thay đổi vật lý liên quan đến thiết bị. Lưu ý có thể áp dụng việc ánh xạ gợi nhớ giữa địa chỉ IPv4 tới địa chỉ IPv6 của máy chủ DNS.

Ví dụ:

DNS1: 2001:db8:1234:a::53
DNS2: 2001:db8:1234:b::53

CHƯƠNG 3: XỬ LÝ VẤN ĐỀ PHÁT SINH VỀ QUẢN LÝ VÙNG ĐỊA CHỈ TRONG QUÁ TRÌNH SỬ DỤNG .

3.1. Quy định của APNIC trong việc quản lý, xử lý các vấn đề phát sinh liên quan đến IPv6

Chính sách quản lý, sử đụng địa chỉ IPv6 của khu vực Châu Á – Thái Bình Dương được APNIC quy định cụ thể tại tài liệu chính sách APNIC-089 "IPv6 address allocation and assignment policy", với các nội dung chính như sau:

- Phải đảm bảo các mục tiêu cơ bản trong sử dụng tài nguyên:
  - Giữ mục tiêu phát triển ổn định của Internet.
  - Đảm bảo tính duy nhất.
  - Đảm bảo tính có đăng ký.
  - Đảm bảo tính tổ hợp cao nhất.
  - Không lãng phí tài nguyên.

- Việc phân bổ lại các vùng IPv6 từ ISP cho các ISP cấp thấp hơn hoặc cấp phát cho khách hàng do các ISP quyết định nhưng phải đảm bảo các nguyên tắc nêu trên.

- Các tổ chức sử dụng IPv6 có trách nhiệm quản lý và xử lý các vấn đề phát sinh từ mạng lưới sử dụng vùng địa chỉ. Cụ thể:

  - Khai báo thông tin các vùng địa chỉ đã cấp phát tới mạng sử dụng cuối (/48) vào cơ sở dữ liệu của RIR/NIR.
  - Khai báo tên miền ngược cho vùng địa chỉ đã sử dụng và cấp phát. Mọi vùng địa chỉ được cấp trước khi sử dụng trên mạng phải được thực hiện thủ tục khai báo chuyển giao tên miền ngược. Tổ chức có trách nhiệm hỗ trợ khai báo bản ghi ngược cho mọi khách hàng sử dụng địa chỉ IP thuộc phạm vi quản lý của mình.
  - Xử lý các hiện tượng lạm dụng mạng khi nhận được yêu cầu của RIR/NIR. Có trách nhiệm xác minh và xử lý ngay các địa chỉ IPv4 thuộc phạm vi quản lý của mình có liên quan đến các hành vi vi phạm pháp luật như hacker, spam, phishing khi nhận được thông báo của RIR/NIR hoặc của các tổ chức khác.

Các nguyên tắc trên được thể chế cụ thể trong các quy định chi tiết như sau

3.2. Khai báo thông tin trên cơ sở dữ liệu.

Tương tự như trong quản lý IPv4, thông tin chi tiết về một vùng địa chỉ IPv6 được đưa vào sử dụng là phần thông tin quan trọng nhất trong cơ sở dữ liệu quản lý. Vùng địa chỉ nhỏ nhất tồn tại trong cơ sở dữ liệu chính là vùng địa chỉ thành viên đã cấp phát lại cho khách hàng. Nếu trong quá trình sử dụng, thành viên không cập nhật thông tin khách hàng, trong cơ sở dữ liệu quản lý chỉ lưu trữ bản ghi dữ liệu vùng địa chỉ lớn mà thành viên đã được phân bổ. Điều này sẽ rất bất lợi cho thành viên mỗi khi có các hành vi lạm dụng mạng (network abuse) xuất phát từ một trong các vùng địa chỉ thành viên đã cấp phát cho khách hàng mà không được cập nhật. Thay vì tra cứu được thông tin chi tiết về mạng lưới nơi xuất phát các hành vi lạm dụng mạng, người bị hại sẽ chỉ tra cứu được thông tin chung về thành viên và cả dải địa chỉ lớn mà thành viên được phân bổ. Kết quả, cả vùng địa chỉ lớn của thành viên có nguy cơ bị chặn khi các hiện tượng lạm dụng mạng không được giải quyết triệt để.

Tại Việt Nam, yêu cầu cụ thể về việc cập nhật thông tin sử dụng địa chỉ IPv6 như sau: vùng địa chỉ IPv6 được cấp từ APNIC và các vùng địa chỉ từ /56 đã cấp phát tới mạng sử dụng cuối phải được cập nhật lưu trữ trong cơ sở dữ liệu của cơ quan quản lý (VNNIC và APNIC) với đầy đủ thông tin về tổ chức được cấp vùng địa chỉ và các cá nhân (người) chịu trách nhiệm quản lý việc sử dụng vùng địa chỉ. Cũng trong bản ghi địa chỉ này, phải có thông tin về địa chỉ tiếp nhận, xử lý đối với vấn đề lạm dụng mạng và thông tin ánh xạ tới đối tượng xử lý vấn đề mạng lưới (IRT - Incident Report Team).

Mẫu bản ghi cập nhật thông tin sử dụng địa chỉ trong CSDL APNIC như sau:

```
inet6num:       2001:df2:f000:0:/56
netname:        ABC-NET
descr:          ABC Network
descr:          Hanoi
admin-c:        VTL3-AP
tech-c:         VHN5-AP
remarks:        send spam and abuse report to abc@companyname.vn
country:        VN
mnt-by:         MAINT-VN-VNNIC
mnt-irt:        IRT-VNNIC-AP
status:         ASSIGNED PORTABLE
source:         APNIC

irt:            IRT-VNNIC-AP
address:        Ha Noi, VietNam
phone:          +84-4-35564944
fax-no:         +84-4-37821462
e-mail:         hm-changed@vnnic.net.vn
abuse-mailbox:  hm-changed@vnnic.net.vn
admin-c:        PT174-AP
tech-c:         NTTT1-AP
auth:           # Filtered
```

```
mnt-by:         MAINT-VN-VNNIC
changed:        hm-changed@vnnic.net.vn 20101108
source:         APNIC

person:         Nguyen Van A
nic-hdl:        NVA-AP
e-mail:         nva@companyname.vn
address:        ABC Company
address:        Ha Noi
phone:          +84-4-xxxxxxxx
fax-no:         +84-4-xxxxxxxx
country:        VN
mnt-by:         MAINT-VN-VNNIC
source:         APNIC
```

Khi cần tìm kiếm thông tin, mọi tổ chức, cá nhân chỉ cần tra cứu whois cơ sở dữ liệu quản lý địa chỉ của APNIC tại địa chỉ www.apnic.net, toàn bộ các thông tin chi tiết liên quan đến vùng địa chỉ sẽ được cung cấp, phục vụ cho xác thực quyền sử dụng, cũng như cung cấp thông tin về tổ chức, cá nhân có trách nhiệm xử lý các vấn đề liên quan đến việc sử dụng tài nguyên.

Tại Việt Nam, việc cập nhật thông tin về các vùng địa chỉ đã được cấp phát, sử dụng lên cơ sở dữ liệu APNIC được thực hiện thông qua VNNIC.

- Đối với các vùng địa chỉ gốc cấp từ APNIC, VNNIC sẽ chủ động tạo các bản ghi vùng địa chỉ và các đối tượng, thông tin liên hệ trên cơ sở thông tin, dữ liệu tổ chức cung cấp trong bản khai đăng ký. Thành viên địa chỉ có trách nhiệm gửi thông báo cập nhật thông tin tới VNNIC (thông qua hộp thư giao dịch info@vnnic.vn) khi có sự thay đổi thông tin.

- Đối với các vùng cấp phát lại trong khối địa chỉ của thành viên, thành viên có trách nhiệm quản lý đầy đủ thông tin về người sử dụng các vùng địa chỉ IPv6 đã cấp, cung cấp thông tin sử dụng chi tiết khi có yêu cầu của cơ quan có thẩm quyền. Việc khai báo, cập nhật cho VNNIC thông tin sử dụng các vùng địa chỉ IPv6 từ /56 thuộc các vùng địa chỉ đã được cấp được thực hiện thông qua gửi email tới hộp thư giao dịch info@vnnic.vn.

Thông tin khách hàng gửi khai báo với Trung tâm Internet Việt Nam có định dạng bản ghi như sau:

inet6num:	Thông tin dải địa chỉ IPv6
netname:	Tên mạng khách hàng
descr:	Tên giao dịch khách hàng
descr:	Địa chỉ khách hàng

country: VN
remarks: send abuse report to: email khách hàng hoặc thành viên

person: Tên người quản lý, quản lý kỹ thuật
e-mail: Email liên hệ
address: Tên giao dịch khách hàng
address: Địa chỉ liên hệ
phone: Điện thoại liên hệ của khách hàng
fax-no: Fax của khách hàng

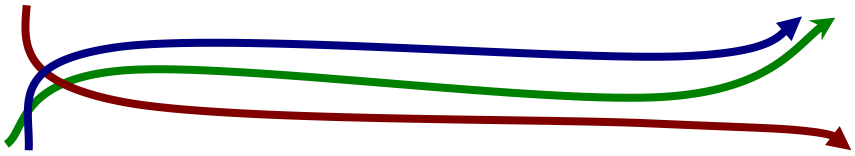
3.3. Khai báo tên miền ngược cho vùng địa chỉ IPv6

Không gian tên miền ngược của địa chỉ IPv6 không nằm dưới miền "in-addr.arpa" như IPv4 mà nằm dưới miền ".ip6.arpa". Trong IPv6, không còn khái niệm classful như IPv4 (/8, /16 và /24). Địa chỉ IPv6 được khai báo chuyển giao tên miền ngược theo các biên 4 bit (1 chữ số hexa). Để ánh xạ địa chỉ IPv6 tới tên miền, hệ thống tên miền sử dụng kiểu bản ghi PTR với dạng thức mới như sau:

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.ip6.arpa IN PTR www.abc.test
```

Địa chỉ IPv6 được đảo chiều, tách và bổ sung dấu chấm giữa các số hexa để ánh xạ từ địa chỉ IPv6 thành tên miền:

4.3.2.1.0.0.0.0.0.0.0.1.0.0.0.2.0.0.0.3.0.0.0.4.0.5.6.7.8.9.a.b



b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.ip6.arpa.

Theo đúng cấu trúc phân cấp quản lý tài nguyên địa chỉ IP trên toàn cầu, APNIC (www.apnic.net) là tổ chức quản lý và khai thác các zone tên miền ngược cao nhất tại khu vực Châu Á, Thái Bình Dương. Đối với các vùng địa chỉ IPv6 đã cấp phát cho các tổ chức tại Việt Nam, Trung tâm Internet Việt Nam (VNNIC) sẽ hỗ trợ thành viên địa chỉ thực hiện khai báo chuyển giao tên miền ngược tương ứng các vùng địa chỉ tổ chức được cấp (chỉ theo hai kích thước tiêu chuẩn là /32 và /48) từ máy chủ APNIC về máy chủ tên miền của thành viên địa chỉ. Khi cấp phát, phân bổ các vùng địa chỉ cấp dưới cho khách hàng, thành viên địa chỉ có trách nhiệm khai báo trên máy chủ của mình để chuyển giao tên miền ngược tương ứng về máy chủ khách hàng, hoặc trực tiếp khai báo bản ghi hỗ trợ khách hàng.

Để thực hiện khai báo tên miền ngược cho vùng IPv6, thành viên phải thực hiên khai báo tên miền ngược cho toàn dải địa chỉ mình được cấp trên tối thiểu 2 máy chủ DNS. Sau khi đã hoàn tất khai báo, gửi yêu cầu về địa chỉ email info@vnnic.vn để VNNIC hỗ trợ, kèm thêm các thông tin: dải địa chỉ IPv6 của mình (/32 hoặc /48), tên hai (02) máy chủ DNS.

3.4. Xử lý các hiện tượng lạm dụng mạng khi nhận được phản ánh từ cộng đồng hoặc VNNIC

Trên cơ sở thông tin về đầu mối quản lý, địa chỉ tiếp nhận phản hồi abuse và thông tin xử lý vấn đề mạng lưới (IRT) cung cấp trong bản ghi thông tin vùng địa chỉ, cộng đồng Internet sẽ có các phản ánh về việc lạm dụng mạng, cũng như các vấn đề vi phạm xuất phát từ mạng lưới sử dụng vùng địa chỉ. Các tổ chức quản lý địa chỉ cấp vùng (APNIC), cấp quốc gia (VNNIC) cũng sẽ căn cứ theo các thông tin liên lạc này để thông báo về các hành vi vi phạm.

Thành viên có trách nhiệm xác minh và xử lý ngay các hành vi vi phạm xuất phát từ vùng địa chỉ IPv6 thuộc phạm vi quản lý của mình có liên quan đến các hành vi vi phạm pháp luật như hacker, spam, phishing khi nhận được thông báo của VNNIC hoặc các tổ chức khác. Đồng thời cần đảm bảo các yêu cầu sau đây:

- Thông tin liên lạc, địa chỉ email tiếp nhận thông báo abuse phải là email chính xác, có hoạt động.
- Các hiện tượng lạm dụng mạng được xử lý kịp thời.

Trong trường hợp không đảm bảo các yêu cầu trên, vùng địa chỉ của tổ chức có thể bị các tổ chức quốc tế đưa vào danh sách cấm định tuyến (blacklist), ảnh hưởng tới hoạt động của toàn bộ mạng lưới. Đây cũng là lí do các tổ chức thành viên địa chỉ cần khai báo trong cơ sở dữ liệu APNIC các vùng đia chỉ đã cấp phát, phân bổ cho khách hàng (theo thông tin chi tiết của khách hàng), nhằm tránh nguy cơ toàn bộ vùng địa chỉ lớn của ISP bị đưa vào blacklist khi hoạt động lạm dụng mạng xuất phát từ một vùng địa chỉ nhất định của khách hàng.

3.5. Định tuyến và khai báo đối tượng thông tin định tuyến

Theo quy định, các tổ chức Việt Nam phải định tuyến mọi vùng địa chỉ IPv6 được cấp bởi VNNIC và có trách nhiệm hỗ trợ lẫn nhau trong việc khai báo định tuyến các vùng địa chỉ IPv6 này.

Đặc biệt, trong những năm gần đây, để việc quảng bá định tuyến đối với vùng địa chỉ IP của thành viên thông suốt trên toàn cầu, các thành viên bắt buộc

phải khai báo đối tượng thông tin định tuyến trong các cơ sở dữ liệu quản lý thông tin định tuyến (IRR - Internet Routing Registry).

Đối tượng thông tin định tuyến là các đối tượng liên quan đến định tuyến và mô tả chính sách định tuyến trong một cơ sở dữ liệu thông tin định tuyến IRR. Có nhiều lớp đối tượng bao gồm:

- aut-num: chỉ định số hiệu mạng
- route: chỉ định tuyến được quảng bá trên Internet
- inet-rtr: biểu diễn một router trong cơ sở dữ liệu lưu trữ thông tin định tuyến
- as-set: một nhóm các số hiệu mạng có cùng chính sách định tuyến
- filter-set: mô tả chính sách lọc áp dụng cho một tập các tuyến –route.
- peering-set (xác định một tập hợp các peering), route-set (xác định một tập hợp các tuyến), rtr-set (xác định một tập hợp các router).

Việc khai báo thông tin định tuyến là để ngăn chặn việc quảng bá những vùng địa chỉ không rõ nguồn gốc, không được cấp phát một cách hợp lệ ra bảng thông tin định tuyến toàn cầu. Trước khi chấp nhận quảng bá cho 1 vùng địa chỉ, người quản trị mạng hoặc thiết bị định tuyến sẽ phải kiểm tra xem liệu một tuyến được quảng bá có phải là tuyến hợp lệ. Việc kiểm tra này sẽ dựa trên những thông tin đăng ký trong một hệ thống lưu trữ thông tin định tuyến IRR.

Để khai báo thông tin định tuyến cho vùng địa chỉ của mình, thành viên có thể lựa chọn một trong các cách thức sau:

- Thành viên gửi yêu cầu đến VNNIC qua địa chỉ info@vnnic.vn để được khai báo trên cơ sở dữ liệu của APNIC.
- Thành viên tự khai báo tại cơ sở dữ liệu IRR của các đối tác cung cấp kết nối đến mình như NTT, SingTel, vv…

PHỤ LỤC: VÍ DỤ VỀ PHÂN HOẠCH VÙNG ĐỊA CHỈ

1. Ví dụ tổng quát

Hiện nay, mỗi ISP được phân bổ một vùng địa chỉ IPv6 /32 từ RIR/NIR. Một ví dụ trong việc áp dụng mô hình phân hoạch như sau:

- ISP phân loại các PoP (Các điểm truy nhập mạng) của ISP thành 3 mức, tùy theo số lượng khách hàng và nhu cầu sử dụng địa chỉ của PoP:
  - PoP Level-1 (PoP cỡ lớn).
  - PoP Level-2 (PoP cỡ trung bình).
  - PoP Level-3 (PoP cỡ nhỏ).
- Tiếp theo, phân loại khách hàng thành 2 loại:
  - Khách hàng cá nhân.
  - Khách hàng doanh nghiệp, tổ chức.

Từ không gian địa chỉ /32 ban đầu, các ISP phân chia thành các block /40, sau đó phân chia tiếp thành các block nhỏ hơn /48,/56,/64…và có thể tham khảo qui hoạch dải địa chỉ của mình như sau:

a. 1 x /40 : Block dành cho các địa chỉ quản lí hạ tầng mạng của ISP (Infrastructure Addresses)

- 1 x /48 cho toàn bộ các PoP : Dành cho đia chỉ loopback và quản lí
  - 1 x /56 cho toàn bộ các PoPs : Dành cho địa chỉ loopback của tất cả các PoP.
    - 1 x /64: Mỗi phân hệ Loopback được chia 1 x 64.
      - 1 x /128: Mỗi giao diện Loopback Interface sử dụng 1x/128.
  - 1 x /56 cho mỗi PoP : Dành cho địa chỉ quản lí của tất cả các PoP.
    - 1 x /64 : Mỗi LAN được chia một /64 dành cho quản lý LAN.
- 1 x /48 cho toàn bộ các PoPs để dự trữ.
- 1 x /48 cho mỗi PoP : Mỗi PoP được chia 1x /48 dành cho Mạng nội bộ (Internal Network).

- X1 x /56 : Routers P2P Links
  - 1 x /64 mỗi Routers P2P Link.
- X2 x /56 : Routers LANs
  - 1 x /64 mỗi Routers LAN
- X3 x /56 : Hosts LANs
  - 1 x /64 mỗi Hosts LAN
- X4 x /56 : Servers LANs
  - 1 x /64 mỗi Servers LAN
- X5 x /56 : Dành cho các mục đích khác.
  - 1 x /64 mỗi mục đích khác.

- 1 x /48 per PoP : Mỗi PoP được chia 1x /48 dành cho Internal Networks.
  - X1 x /56 : Routers P2P Links
    - 1 x /64 mỗi Routers P2P Link
  - X2 x /56 : Routers LANs
    - 1 x /64 mỗi Routers LAN
  - X3 x /56 : Hosts LANs
    - 1 x /64 mỗi Hosts LAN
  - X4 x /56 : Servers LANs
    - 1 x /64 mỗi Servers LAN
  - X5 x /56 : Dành cho các mục đích khác.
    - 1 x /64 mỗi mục đích.

b. A x /40 : Không gian địa chỉ qui hoạch cho các khách hàng PoP Level -1

- N1 x /40 per PoP : Mỗi PoP qui hoạch 1 không gian N1x /40 dành cho khách hàng doanh nghiệp, tổ chức.
  - 1 x /48 mỗi Khách hàng lớn
  - 1 x /56 mỗi Khách hàng nhỏ
- N2 x /40 mỗi PoP : Mỗi PoP qui hoạch 1 không gian N1x /40 dành cho khách hàng cá nhân.

- 1 x /56 mỗi Customer LAN
- 1 x /64 mỗi Customer WAN

c. B x /40 : Không gian địa chỉ qui hoạch cho các khách hàng PoP Level-2

- M1 x /40 mỗi PoP : Mỗi PoP qui hoạch 1 không gian M1x /40 dành cho khách hàng doanh nghiệp, tổ chức.
  - 1 x /48 mỗi Khách hàng lớn
  - 1 x /56 mỗi Khách hàng nhỏ
- M2 x /40 mỗi PoP : Mỗi PoP qui hoạch 1 không gian M2x /40 dành cho khách hàng cá nhân.
  - 1 x /56 mỗi Customer LAN
  - 1 x /64 mỗi Customer WAN

d. C x /40 : Không gian địa chỉ qui hoạch cho các khách hàng PoP Level-3

- L1 x /40 per PoP : Mỗi PoP qui hoạch 1 không gian L1x /40 dành cho khách hàng doanh nghiệp, tổ chức.
  - 1 x /48 mỗi Khách hàng lớn
  - 1 x /56 mỗi Khách hàng nhỏ
- L2 x /40 per PoP : Mỗi PoP qui hoạch 1 không gian L2x /40 dành cho khách hàng cá nhân.
  - 1 x /56 mỗi Customer LAN
  - 1 x /64 mỗi Customer WAN

e. D x /40 : Không gian địa chỉ dự trữ.

f. Tính toán các tham số

Các tham số A,B,C,D,X,N,M,L được nêu trên có thể được tính toán, định cỡ như sau:

- A, B, C được xác định bằng tổng số /40 cần sử dụng cho mỗi loại PoP (A>B>C).
- N1,N2,M1,M2,L1,L2 phụ thuộc vào số lượng khách hàng của mỗi loại PoP (N1>M1>L1 & N2>M2>L2).
- Tổng (N1 x /40 + N2 x /40) của mọi PoP Level-1 = A x /40.
- Tổng (M1 x /40 + M2 x /40) của mọi PoP Level-2 = B x /40.

- Tổng (L1 x /40 + L2 x /40) của mọi PoP Level-3 = C x /40.

2. Ví dụ chi tiết

Một 1 ISP được cấp phát 1 không gian địa chỉ: 2406:6400::/32. ISP qui hoạch không gian địa chỉ /32 được phân bổ như sau:

✓ Trường hợp 1: ISP phát triển khách hàng truy cập internet.

✓ Trường hợp 2: ISP phát triển khách hàng truy cập internet và dịch vụ lưu trữ trung tâm dữ liệu.

a. ISP phát triển khách hàng truy cập internet.

Bảng 1: Phân chia địa chỉ cấp 1 cho hạ tầng mạng và khách hàng

Block#	Prefix	Description	Reverse Domain	SOR	Registration
1	**2406:6400::/32**	**Parent Block**	**0.0.4.6.6.0.4.2.ip6.arpa.**	**N/A**	**APNIC**
2	2406:6400:0000:0000::/33	Infrastructure + DC + CS P2P + Cust net	7~0.0.0.4.6.6.0.4.2.ip6.arpa.[x8]	No	Optional
3	2406:6400:8000:0000::/33	Customer network	f~8.0.0.4.6.6.0.4.2.ip6.arpa. [x8]	Not yet	Optional

Bảng 2: Phân chia địa chỉ cấp 2 cho hạ tầng mạng

Block#	Prefix	Description	Reverse Domain	SOR	Registration
2	**2406:6400:0000:0000::/33**	**Infrastructure + DC + CS P2P + Cust**	**7~0.0.0.4.6.6.0.4.2.ip6.arpa**	**N/A**	**Optional**
4	2406:6400:0000:0000::/48	Loopback, Transport & P2P [Infra]			
5	2406:6400:0001:0000::/48	CS P2P			
6	2406:6400:0002:0000::/48	CS P2P			
7	2406:6400:0003:0000::/48	CS P2P			
8	2406:6400:0004:0000::/48	CS P2P			
9	2406:6400:0005:0000::/48	DC (DNS, Mail, WWW, Hosting Cust)			
10	2406:6400:0006:0000::/48	DC (DNS, Mail, WWW, Hosting Cust)			
11	2406:6400:0007:0000::/48	DC (DNS, Mail, WWW, Hosting Cust)			
12	2406:6400:0008:0000::/48	DC (DNS, Mail, WWW, Hosting Cust)			
13	2406:6400:0009:0000::/48				
14	2406:6400:000A:0000::/48	Customer network			
15	2406:6400:000B:0000::/48	Customer network			
16	2406:6400:000C:0000::/48	Customer network			
17	2406:6400:000D:0000::/48	Customer network			
18	2406:6400:000E:0000::/48	Customer network			
19	2406:6400:000F:0000::/48	Customer network			
	2406:6400:7FFF:0000::/48	Customer network			

Bảng 3: Phân chia địa chỉ chi tiết cho loopback, vận chuyển và hạ tầng mạng WAN

Block#	Prefix	Description	Reverse Domain	SOR	Registration
4	**2406:6400:0000:0000::/48**	**Loopback, Trans, Infra WAN**	**0.0.0.0.0.0.4.6.6.0.4.2.ip6.arpa.**		**Optional**
32773	2406:6400:0000:0000::/64	Loopback		No	No
32774	2406:6400:0000:0001::/64				
32775	2406:6400:0000:0002::/64	Transport		No	No
32776	2406:6400:0000:0003::/64			No	No
32777	2406:6400:0000:0004::/64			No	No
32778	2406:6400:0000:0005::/64	Infra WAN		No	No
32779	2406:6400:0000:0006::/64	Infra WAN		No	No
32780	2406:6400:0000:0007::/64	Infra WAN		No	No
32781	2406:6400:0000:0008::/64	Infra WAN		No	No
32782	2406:6400:0000:0009::/64	Infra WAN		No	No
32783	2406:6400:0000:000a::/64	Infra WAN		No	No
32784	2406:6400:0000:000b::/64	Infra WAN		No	No
32785	2406:6400:0000:000c::/64	Infra WAN		No	No
32786	2406:6400:0000:000d::/64	Infra WAN		No	No
32787	2406:6400:0000:000e::/64	Infra WAN		No	No
32788	2406:6400:0000:000f::/64	Infra WAN		No	No
	2406:6400:0000:ffff::/64	Infra WAN		No	No

Bảng 4: Phân chia địa chỉ chi tiết cho khách hàng

Block#	Prefix	Description	Reverse Domain	SOR	Registration
3	2406:6400:8000:0000::/33				
	2406:6400:8000:0000::/48	Customer 1	0.0.0.8.0.0.4.6.6.0.4.2.ip6.arpa.	Yes	Yes
	2406:6400:8001:0000::/48	Customer2	1.0.0.8.0.0.4.6.6.0.4.2.ip6.arpa.	Yes	Yes
	2406:6400:8002:0000::/48				
	2406:6400:8003:0000::/48				
	2406:6400:8004:0000::/48				
	2406:6400:8005:0000::/48				
	2406:6400:8006:0000::/48				
	2406:6400:8007:0000::/48				
	2406:6400:8008:0000::/48				
	2406:6400:8009:0000::/48				
	2406:6400:800A:0000::/48				
	2406:6400:800B:0000::/48				
	2406:6400:800C:0000::/48				
	2406:6400:800D:0000::/48				
	2406:6400:800E:0000::/48				
	2406:6400:800F:0000::/48				
	2406:6400:FFFF:0000::/48				

b. ISP phát triển khách hàng truy cập internet và dịch vụ lưu trữ trung tâm dữ liệu.

Bảng 1: Phân chia địa chỉ mức cao nhất cho hạ tầng mạng và khách hàng

Block#	Prefix	Description	Reverse Domain	SOR	Registration
1	**2406:6400::/32**	***Parent Block***	0.0.4.6.6.0.4.2.ip6.arpa.	N/A	APNIC
2	2406:6400:0000:0000::/36	Infrastructure + DC	0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Optional
3	2406:6400:1000:0000::/36	Customer network	1.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
4	2406:6400:2000:0000::/36	Customer network	2.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
5	2406:6400:3000:0000::/36	Customer network	3.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
6	2406:6400:4000:0000::/36	Customer network	4.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
7	2406:6400:5000:0000::/36	Customer network	5.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
8	2406:6400:6000:0000::/36	Customer network	6.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
9	2406:6400:7000:0000::/36	Customer network	7.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
10	2406:6400:8000:0000::/36	Customer network	8.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
11	2406:6400:9000:0000::/36	Customer network	9.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
12	2406:6400:a000:0000::/36	Customer network	a.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
13	2406:6400:b000:0000::/36	Customer network	b.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
14	2406:6400:c000:0000::/36	Customer network	c.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
15	2406:6400:d000:0000::/36	Customer network	d.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
16	2406:6400:e000:0000::/36	Customer network	e.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional
17	2406:6400:f000:0000::/36	Customer network	f.0.0.4.6.6.0.4.2.ip6.arpa.	Not yet	Optional

Bảng 2: Phân chia địa chỉ chi tiết cho hạ tầng mạng

Block#	Prefix	Description	Reverse Domain	SOR	Registration
2	***2406:6400:0000:0000::/36***	***Infrastructure***	0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Optional
18	2406:6400:0000:0000::/40	Loopback, Transport & WAN [Infra+CS]	0.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Optional
19	2406:6400:0100:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	1.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
20	2406:6400:0200:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	2.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
21	2406:6400:0300:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	3.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
22	2406:6400:0400:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	4.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
23	2406:6400:0500:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	5.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
24	2406:6400:0600:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	6.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
25	2406:6400:0700:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	7.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
26	2406:6400:0800:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	8.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
27	2406:6400:0900:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	9.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
28	2406:6400:0a00:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	a.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
29	2406:6400:0b00:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	b.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
30	2406:6400:0c00:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	c.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
31	2406:6400:0d00:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	d.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
32	2406:6400:0e00:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	e.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended
33	2406:6400:0f00:0000::/40	DC (DNS, Mail, WWW, Hosting Cust)	f.0.0.0.4.6.6.0.4.2.ip6.arpa.	No	Recommended

Bảng 3: Phân chia địa chỉ chi tiết cho loopback, transport và WAN

Block#	Prefix	Description	Reverse Domain	SOR	Registration
18	***2406:6400:0000:0000::/40***	***Loopback, Transport & Infra WAN***	*0.0.0.0.4.6.6.0.4.2.ip6.arpa.*		
19	2406:6400:0000:0000::/48	Loopback, Transport, Infra WAN		No	Recommended
20	2406:6400:0001:0000::/48	Customet poing-to-point Link		No	Recommended
21	2406:6400:0002:0000::/48	Customet poing-to-point Link		No	Recommended
22	2406:6400:0003:0000::/48	Customet poing-to-point Link		No	Recommended
23	2406:6400:0004:0000::/48	Customet poing-to-point Link		No	Recommended
24	2406:6400:0005:0000::/48	Customet poing-to-point Link		No	Recommended
25	2406:6400:0006:0000::/48	Customet poing-to-point Link		No	Recommended
26	2406:6400:0007:0000::/48	Customet poing-to-point Link		No	Recommended
27	2406:6400:0008:0000::/48	Customet poing-to-point Link		No	Recommended
28	2406:6400:0009:0000::/48	Customet poing-to-point Link		No	Recommended
29	2406:6400:000A:0000::/48	Customet poing-to-point Link		No	Recommended
30	2406:6400:000B:0000::/48	Customet poing-to-point Link		No	Recommended
31	2406:6400:000C:0000::/48	Customet poing-to-point Link		No	Recommended
32	2406:6400:000D:0000::/48	Customet poing-to-point Link		No	Recommended
33	2406:6400:000E:0000::/48	Customet poing-to-point Link		No	Recommended
34	2406:6400:000F:0000::/48	Customet poing-to-point Link		No	Recommended
275	2406:6400:00FF:0000::/48	Customet poing-to-point Link		No	Recommended

Bảng 4: Phân chia địa chỉ chi tiết cho loopback, transport và hạ tầng mạng WAN

Block#	Prefix	Description	Reverse Domain	SOR	Registration
19	***2406:6400:0000:0000::/48***	***Loopback, Transport & Infra WAN***	*0.0.0.0.4.6.6.0.4.2.ip6.arpa.*		Optional
276	2406:6400:0000:0000::/64	Loopback		No	No
277	2406:6400:0000:0001::/64				
278	2406:6400:0000:0002::/64	Transport		No	No
279	2406:6400:0000:0003::/64			No	No
280	2406:6400:0000:0004::/64			No	No
281	2406:6400:0000:0005::/64	Infra WAN		No	No
282	2406:6400:0000:0006::/64	Infra WAN		No	No
283	2406:6400:0000:0007::/64	Infra WAN		No	No
284	2406:6400:0000:0008::/64	Infra WAN		No	No
285	2406:6400:0000:0009::/64	Infra WAN		No	No
286	2406:6400:0000:000a::/64	Infra WAN		No	No
287	2406:6400:0000:000b::/64	Infra WAN		No	No
288	2406:6400:0000:000c::/64	Infra WAN		No	No
289	2406:6400:0000:000d::/64	Infra WAN		No	No
290	2406:6400:0000:000e::/64	Infra WAN		No	No
291	2406:6400:0000:000f::/64	Infra WAN		No	No
65811	2406:6400:0000:ffff::/64	Infra WAN		No	No

Bảng 5: Phân chi cụ thể các block cho khách hàng

Block#	Prefix	Description	Reverse DNS	SOR	Registration
3	2406:6400:1000:0000::/36	Customer network			
	2406:6400:1000:0000::/48	Customer 1		Yes	Yes
	2406:6400:1001:0000::/48	Customer 2		Yes	Yes
	2406:6400:1002:0000::/48				
	2406:6400:1003:0000::/48				
	2406:6400:1004:0000::/48				
	2406:6400:1005:0000::/48				
	2406:6400:1006:0000::/48				
	2406:6400:1007:0000::/48				
	2406:6400:1008:0000::/48				
	2406:6400:1009:0000::/48				
	2406:6400:100a:0000::/48				
	2406:6400:100b:0000::/48				
	2406:6400:100c:0000::/48				
	2406:6400:100d:0000::/48				
	2406:6400:100e:0000::/48				
	2406:6400:100f:0000::/48				
	2406:6400:1fff:0000::/48				

TÀI LIỆU THAM KHẢO

1. IPv6 Addressing Plan Fundamentals / RIPE NCC.
2. Preparing an IPv6 Address plan / SURFNET & RIPE NCC
3. Information about IPv6 Operational Issues/APNIC
4. Guidelines, Rules, Best Practice / DREN.
5. Một số RFC/IETF:
    - RFC 5375 - IPv6 Unicast Address Assignment
    - RFC 6177 - IPv6 Address Assignment to End Sites
    - RFC 3531 - A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block
    - RFC 4291 - IP Version 6 Addressing Architecture
    - RFC 6164 - Using 127-Bit IPv6 Prefixes on Inter-Router Links
    - RFC 5375 - IPv6 Addressing Considerations
    - RFC 6105 - IPv6 Router Advertisement Guard
    - RFC 3177: Recommendations on IPv6 Address Allocations to Sites.
    - …
6. Giới thiệu về thế hệ địa chỉ Internet mới IPv6/VNNIC
7. Understanding IPv6 3rd edition / Joseph Davies
8. IPv6, Perspective from small to medium ISP / INETHK.Asia.
9. Creating an IPv6 Addressing Plan / Infoblox.