HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Tô Viết Sơn

GIAO THỨC IPV6 VÀ TRIỂN KHAI IPV6 TRONG MẠNG BĂNG RỘNG VNPT

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Tô Viết Sơn

GIAO THỨC IPV6 VÀ TRIỂN KHAI IPV6 TRONG MẠNG BĂNG RỘNG VNPT

Chuyên Ngành : Kỹ thuật Viễn thông

Mã Số : 8.52.02.08

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. NGUYỄN TIẾN BAN

HÀ NỘI – 2020

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này là kết quả nghiên cứu của riêng tôi. Việc sử dụng kết quả, trích dẫn tài liệu tham khảo trên các tạp chí, các trang web tham khảo đảm bảo theo đúng quy định. Các nội dung trích dẫn và tham khảo các tài liệu, sách báo, thông tin được đăng tải trên các tác phẩm, tạp chí và trang web theo danh mục tài liệu tham khảo của luận văn.

Tối xin chịu hoàn toàn trách nhiệm cho lời cam đoan của mình.

Tác giả luận văn

Tô Viết Sơn

LỜI CẢM ƠN

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

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

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

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

Hà Nội, tháng năm 2020

Học viên thực hiện

Tô Viết Sơn

MỤC LỤC

LỜI CAM ĐOAN i

LỜI CẢM ƠN ii

LỜI MỞ ĐẦU 1

CHƯƠNG 1 Bối cảnh, lý do cần thiết phải triển khai IPv6 2

1.1 Giới thiệu về IPv6 2

1.2 Một số phương pháp chuyển đổi từ IPv4 sang IPv6 2

1.3 Cấu trúc tiêu đề IPv6 3

1.4 Sự cần thiết phải triển khai IPv6 5

1.5 Kết luận chương 1 6

CHƯƠNG 2 CÁC Giao thỨc trong IPV6 7

2.1 Địa chỉ IPv6 7

2.1.1 Biểu diễn địa chỉ IPv6 7

2.1.2 Độ dài tiền tố IPv6 7

2.1.3 Tóm tắt về các loại địa chỉ IPv6 8

2.1.4 Cấu trúc của địa chỉ Global Unicast Address (GUA) 9

2.1.5 Ứng dụng các kiểu địa chỉ trong IPv6 14

2.2 Giao thức ICMPv6 và giao thức Neighbor Discovery Protocol 34

2.2.1 ICMP Error Messages 36

2.2.2 ICMP Informational Messages 40

2.3 Kết luận chương 2 54

CHƯƠNG 3 GiẢI pháp triỂn khai IPv6 cho vnpt hẢi dương 55

3.1 Kế hoạch triển khai 55

3.2 Dịch vụ triển khai 57

3.3 Một số phướng án cấp phát IPv6 cho thiết bị đầu cuối từ nhà cung cấp dịch vụ 59

3.4 Triển khai IPv6 trong mạng băng rộng VNPT 59

3.5 Mô phỏng cấp phát IPv6 cho đầu cuối từ ISP bằng giả lập EVE-NG theo phương pháp DHCP-PD.....60

3.5.1 Thực hiện mô phỏng việc cấp phát IPv6 từ ISP đến khách hàng 60

3.5.2 Kiểm tra trạng thái và kiểm tra kết nối 63

3.6 Kết luận chương 3 68

KẾT LUẬN 70

DANH MỤC HÌNH VẼ

Hình 1.1 Các giao thức khác nhau đóng gói trong IPv6 và được đóng gói trong gói IPv4 2
Hình 1.2: Chuyển đổi giữa IPv4 và IPv6 2
Hình 1.3: Toàn bộ mạng chạy IPv6 3
Hình 1.4: Tiêu đề IPv6 3
Hình 2.1: Cấu trúc một địa chỉ GUA điển hình 9
Hình 2.2: Địa chỉ GUA và quy luật 3-1-4 10
Hình 2.3: IPv6 Topology 10
Hình 2.4: Subnet Prefix 11
Hình 2.5: /112 Subnet Prefix 12
Hình 2.6: Mở rộng /64 subnet prefix thêm 4 bit 12
Hình 2.7: Thực hiện Subnetting trong 1 Nibble 13
Hình 2.8: Subnetting trong Nibble 14
Hình 2.9: Dải địa chỉ Global unicast 15
Hình 2.10: Dải địa chỉ Global Unicast 15
Hình 2.11: NDP Router Advertisement và Router Solicitation Messages 18
Hình 2.12: Stateful addressing using DHCPv6 21
Hình 2.13: Link-local Unicast 23
Hình 2.14: Dải địa chỉ Link-local Unicast 23
Hình 2.15: Phát hiện địa chỉ Link-local trùng lặp 25
Hình 2.16: Biểu diễn địa chỉ IPv6 Loopback 25
Hình 2.17: IPv4-Compatible IPv6 Address (Deprecated) 28
Hình 2.18: IPv4-Mapped IPv6 Addresses 29
Hình 2.19: Multicast Address 30
Hình 2.20: Multicast Scope 31

Hình 2.21: Địa chỉ Solicited-Node Multicast.....33
Hình 2.22: Ví dụ về sử dụng địa chỉ Anycast 34
Hình 2.23: Khuôn dạng tổng quát của ICMPv6.....35
Hình 2.24: ICMPv6 Destination Unreachable Message 37
Hình 2.25: Path MTU Discovery 39
Hình 2.26: ICMPv6 Echo Request and Echo Reply Messages 42
Hình 2.27: ICMPv6 ND Router Solicitation Message.....46
Hình 2.28: ICMPv6 ND Router Advertisement Message.....47
Hình 2.29: ICMPv6 ND Neighbor Solicitation Message 50
Hình 2.30: ICMPv6 ND Neighbor Advertisement Message 51
Hình 2.31: Các trường trong ICMPv6 Redirect Message.....53
Hình 2.32: ICMPv6 Redirect Message 54
Hình 3.1: LAB mô phỏng cấp phát DHCP-PD.....61

THUẬT NGỮ VÀ TỪ VIẾT TẮT

Viết tắt	Chú giải tiếng Anh	Chú giải tiếng Việt
APNIC	Asia Pacific Network INTERNET Center	Trung tâm mạng INTERNET châu Á- Thái Bình Dương.
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ.
BGP	Border Gateway Protocol	Giao thức cổng biên
CIDR	Classless Inter-Domain Routing	Phương pháp biểu diễn IP bằng prefix mask
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình địa chỉ động.
ICMP	INTERNET Control Message Protocol	Giao thức thông điệp điều khiển.
IGMP	INTERNET Group Management Protocol	Giao thức INTERNET để các host kết nối, hủy kết nối từ các nhóm multicast.
IPv4	INTERNET Protocol Version 4	Phiên bản 4 của giao thức INTERNET.
IPv6	INTERNET Protocol Version 6	Phiên bản 6 của giao thức INTERNET.
MTU	Maximum Transmission Unit	Đơn vị truyền tối đa.
IANA	INTERNET Assigned Numbers Authority	Tổ chức quản lý tài nguyên số
ISP	INTERNET Service Provider	Cung cấp dịch vụ INTERNET
GUA	Global unicast address	Địa chỉ unicast toàn cầu
ICMPv6	INTERNET Group Management Protocol version 6	Giao thức thông điệp điều khiển phiên bản 6
NDP	Neighbor Discovery Protocol	Giao thức khám phá hàng xóm
QoS	Quality of service	Chất lượng dịch vụ
VoIP	Voice over IP	Thoại trên IP
IPng	IP Next Generation	IP thế hệ tiếp theo
TTL	Time to live	Thời gian tồn tai gói tin
RFC	Request For Comments	Tài liệu chuẩn cho INTERNET
ICANN	Internet Corporation for Assigned Names and Numbers	Tổ chức cấp phát tên và số hiệu

EUI-64	Extended Unique Identifier	Danh định mở rộng duy nhất
SLAAC	Stateless Address Autoconfiguration	Tự động cấu hình địa chỉ không trạng thái
RA	Router Advertisement	Quảng bá router
RS	Router Solicitation	Dò tìm router
NS	Neighbor Solicitation	Dò tìm hàng xóm
NA	Neighbor Advertisement	Quảng bá hàng xóm
DAD	Duplicate Address Detection	Phát hiện địa chỉ xung đột
LLU	Link local unicast	Địa chỉ unicast cục bộ
PMTU	Path Maximum Transmission Unit	Đơn vị truyền tối đa trên đường
SSM	Source Specific Multicast	Nguồn multicast cụ thể
MLD	Multicast Listener Discovery	Xác định thiết bị lắng nghe multicast

LỜI MỞ ĐẦU

Đứng trước sự phát triển mạnh mẽ của công nghệ truyền thông, đặc biệt là trong lĩnh vực mạng máy tính, ngoài việc giải quyết vấn đề về lưu lượng cho mạng thì địa chỉ của các thiết bị mạng là một trong những vấn đề nan giải cần phải được quan tâm thực sự. Hiện nay, địa chỉ của các máy tính trên Internet đang được đánh số theo thế hệ địa chỉ phiên bản 4 (IPv4) gồm 32 bits. Trên lý thuyết, không gian IPv4 bao gồm hơn 4 tỉ địa chỉ. Tuy nhiên đứng trước sự phát triển mạnh mẽ về số lượng thiết bị mạng như vậy thì nguy cơ thiếu hụt không gian địa chỉ IPv4 là điều sẽ không tránh khỏi; cùng với những hạn chế trong công nghệ và những nhược điểm của IPv4 đã thúc đẩy sự ra đời của một thế hệ địa chỉ Internet mới là IPv6 với cấu trúc định tuyến tốt hơn, hỗ trợ tốt hơn cho multicast, hỗ trợ bảo mật và di động tốt hơn. Hiện nay IPv6 đã được chuẩn hóa và từng bước đưa vào ứng dụng thực tế. Vì vậy học viên đã chọn đề tài luận văn của mình là "Giao thức IPv6 và triển khai IPv6 trong mạng băng rộng VNPT".

Nội dung luận văn đề cập đến các vấn đề kĩ thuật của địa chỉ IPv6, giao thức ICMPv6 và giao thức NDP. Sau đó luận văn đi sâu vào nghiên cứu phương pháp triển khai giao thức IPv6 trong mạng băng rộng của VNPT Hải Dương.

Bố cục của luận văn được trình bày như sau:

- Chương 1 trình bày tổng quan về IPv6, cấu trúc tiêu đề IPv6, phân tích sự cần thiết phải triển khai IPv6.
- Chương 2 trình bày cấu trúc địa chỉ IPv6, giao thức ICMPv6, giao thức NDP và phân tích các bản tin liên quan.
- Chương 3 trình bày giải pháp triển khai IPv6 cho VNPT Hải Dương, trong đó đề cập đến cách thức cấp phát địa chỉ động từ ISP đến khách hàng, chọn lựa phương thức tối ưu và đang được sử dụng trong thực tế, đồng thời cũng thực hiện mô phỏng toàn bộ quá trình cấp phát địa chỉ động bằng phương pháp DHCPv6-PD.

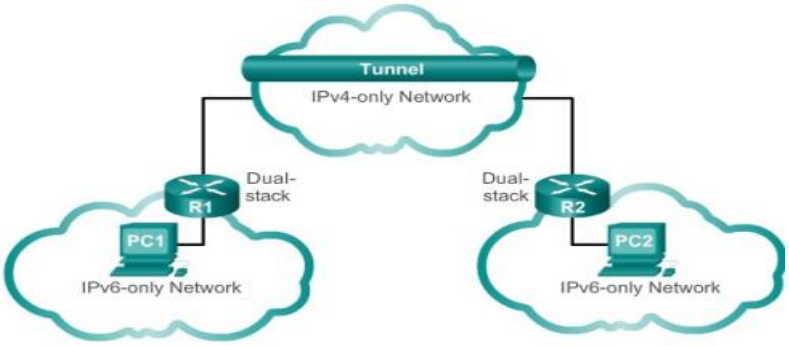
CHƯƠNG 1 BỐI CẢNH, LÝ DO CẦN THIẾT PHẢI TRIỂN KHAI IPV6

1.1 Giới thiệu về IPv6

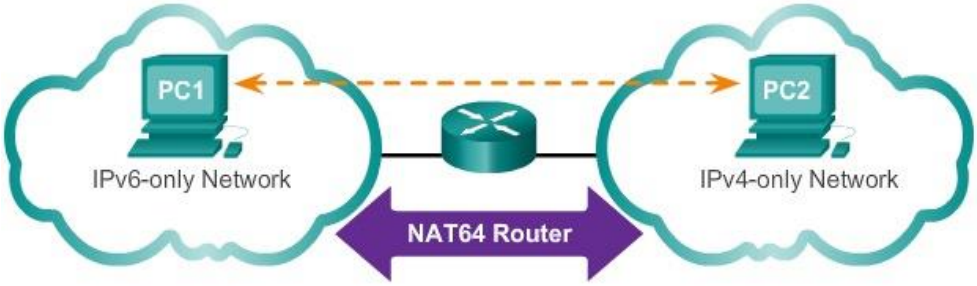
Giao thức Internet phiên bản 6 (IPv6) được thiết kế để trở thành giao thức kế thừa cho IPv4. IPv6 được phát triển từ giữa đến cuối những năm 1990 với không gian địa chỉ 128 bit, được viết bằng hệ thập lục phân. IPv6 không chỉ giải quyết về mặt địa chỉ mà còn cung cấp các khả năng:

- Tự động cấu hình địa chỉ.
- Kết nối End to End không cần NAT (End-to-end reachability without private addresses and NAT).
- Hỗ trợ tốt hơn cho việc di chuyển (Better support for mobility).
- Kết nối mạng ngang hàng dễ dàng hơn để tạo và duy trì và các dịch vụ như VoIP.
- Chất lượng dịch vụ (QoS) trở nên tốt hơn.

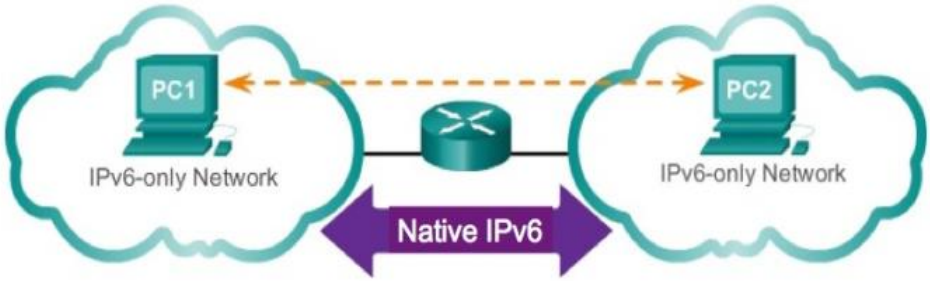
1.2 Một số phương pháp chuyển đổi từ IPv4 sang IPv6



Hình 1.1 Các giao thức khác nhau đóng gói trong IPv6 và được đóng gói trong gói IPv4



Hình 1.2: Chuyển đổi giữa IPv4 và IPv6

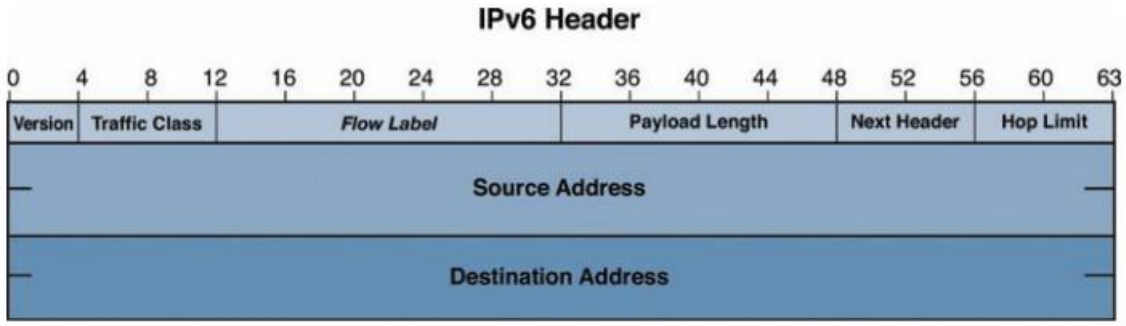


Hình 1.3: Toàn bộ mạng chạy IPv6

1.3 Cấu trúc tiêu đề IPv6

Tiêu đề IPv6

IPv6 được định nghĩa trong RFC 2460, Giao thức Internet, Phiên bản 6 (IPv6). Hình sau cho thấy cấu trúc cơ bản của tiêu đề IPv6 hoặc đôi khi được gọi là tiêu đề chính IPv6. Tiêu đề chính IPv6 cũng có thể bao gồm một hoặc nhiều tiêu đề mở rộng IPv6. Hình 1.4 mô tả tiêu đề chính IPv6 là bắt buộc và bao gồm các trường như trên hình.



Hình 1.4: Tiêu đề IPv6

Tiêu đề chính IPv6 là bắt buộc và bao gồm các trường sau:

Version (4 bit): Trường này chứa số phiên bản của giao thức Internet. Trong IPv6, trường này luôn có giá trị là 6.

Traffic Class (8 bit): Trường này có các chức năng tương tự như trường loại dịch vụ (ToS) trong tiêu đề IPv4. Nó có cùng kích thước với trường ToS trong IPv4, chỉ thay đổi tên. Trường Lớp lưu lượng được sử dụng để xác định và phân biệt giữa các lớp hoặc mức độ ưu tiên khác nhau của các gói IPv6. IPv6 sử dụng kỹ thuật Dịch vụ khác biệt được chỉ định trong RFC 2474, Định nghĩa về trường Differentiated Services (Trường DS) trong Tiêu đề IPv4 và IPv6. Sử dụng 6 bit cho DSCP cho

phép khả năng đánh dấu 64 điểm. Điều này cung cấp mức độ chi tiết cao hơn nhiều trong lựa chọn ưu tiên so với 3 bit của IPv4.

Flow Label (20 bit): Trường Nhãn lưu lượng được sử dụng để Tag a sequence or flow of IPv6 packets được gửi từ một nguồn tới một hoặc nhiều nút đích. Flow này có thể được sử dụng bởi một nguồn để gắn nhãn cho các chuỗi gói mà nó yêu cầu xử lý đặc biệt bởi các bộ định tuyến IPv6, chẳng hạn như dịch vụ thời gian thực trực tuyến. Trường Flow Label được sử dụng để giúp xác định tất cả các gói trong cùng một luồng để đảm việc hiệu quả trong xử lý tại các bộ định tuyến IPv6.

Payload Length (16 bit): Đây là độ dài tải, nói cách khác là phần dữ liệu của gói. Nếu gói IPv6 có một hoặc nhiều tiêu đề mở rộng, chúng sẽ coi là một phần của tải trọng.

Trường Độ dài tải trọng IPv6 tương tự như trường Tổng chiều dài trong tiêu đề IPv4, ngoại trừ một khác biệt quan trọng.

Trường Tổng chiều dài của IPv4 bao gồm cả tiêu đề và dữ liệu IPv4, trong khi trường Độ dài tải trọng IPv6 chỉ xác định số lượng byte dữ liệu, nó không bao gồm 40 byte của tiêu đề IPv6 chính.

Tiêu đề IPv4 có thể khác nhau về độ dài do các trường Padding và Options, trong khi tiêu đề IPv6 được cố định ở mức 40 byte.

Trường Độ dài tải trọng là 16 bit, cho phép kích thước tải trọng tối đa là 65.535 byte. IPv6 có tiêu đề mở rộng Jumbogram để hỗ trợ kích thước gói lớn hơn nếu cần. RFC 2675, IPv6 Jumbograms, chỉ định trường 32 bit bổ sung để cho phép truyền các gói IPv6 có tải trọng trong khoảng từ 65.536 đến 4.294.967.295 byte.

Next Header (8 bit): Trường này có hai lợi ích. Chỉ ra tiêu đề mở rộng tiếp theo. Trong tình huống khi chỉ có tiêu đề IPv6 chính và không có tiêu đề mở rộng, trường Next Header chỉ định giao thức được mang trong phần dữ liệu của gói IPv6. Điều này tương tự như trường Giao thức trong tiêu đề IPv4. Các giá trị tương tự được sử dụng trong trường Giao thức IPv4 được sử dụng trong trường Next Header của IPv6.

Hop Limit (8 bit): Trường Giới hạn Hop, tương đương với trường Time to Live (TTL) trong tiêu đề IPv4.

Source Address (128 bit): Trường này chứa địa chỉ IP 128 bit của người khởi tạo gói IPv6. Như với IPv4, đây là địa chỉ của nút ban đầu đã gửi gói. Địa chỉ nguồn phải là một địa chỉ unicast.

Destination Address (128 bit): Đây là địa chỉ IP 128 bit của đích đến cuối cùng dự định hoặc người nhận gói IPv6. Nó đại diện cho đích đến cuối cùng, có thể là một địa chỉ unicast hoặc multicast. Không giống như IPv4, không có địa chỉ quảng bá, tuy nhiên, có thể là một địa chỉ multicast cho tất cả các nút.

1.4 Sự cần thiết phải triển khai IPv6

Do sự phát triển như vũ bão của mạng và dịch vụ Internet, nguồn IPv4 dần cạn kiệt, đồng thời bộc lộ các hạn chế đối với việc phát triển các loại hình dịch vụ hiện đại trên Internet. Phiên bản địa chỉ Internet mới IPv6 được thiết kế để thay thế cho phiên bản IPv4, với mục đích thay thế cho nguồn IPv4 cạn kiệt để tiếp nối hoạt động Internet và khắc phục các nhược điểm trong thiết kế của địa chỉ IPv4.

Địa chỉ IPv6 có chiều dài 128 bit, biểu diễn dưới dạng các cụm số hexa phân cách bởi dấu ::. Với 128 bit chiều dài, không gian địa chỉ IPv6 gồm 128 bit địa chỉ, cung cấp một lượng địa chỉ khổng lồ cho hoạt động Internet. IPv6 được thiết kế với những mục tiêu như sau:

- Không gian địa chỉ lớn hơn và dễ dàng quản lý không gian địa chỉ.
- Khôi phục lại nguyên lý kết nối đầu cuối - đầu cuối của Internet và loại bỏ hoàn toàn công nghệ NAT.
- Quản trị TCP/IP dễ dàng hơn: DHCP được sử dụng trong IPv4 nhằm giảm cấu hình thủ công TCP/IP cho host. IPv6 được thiết kế với khả năng tự động cấu hình mà không cần sử dụng máy chủ DHCP, hỗ trợ hơn nữa trong việc giảm cấu hình thủ công.
- Cấu trúc định tuyến tốt hơn: Định tuyến IPv6 được thiết kế hoàn toàn phân cấp.

- Hỗ trợ tốt hơn Multicast: Multicast là một tùy chọn của địa chỉ IPv4, tuy nhiên khả năng hỗ trợ và tính phổ dụng chưa cao.
- Hỗ trợ bảo mật tốt hơn: IPv4 được thiết kế tại thời điểm chỉ có các mạng nhỏ, biết rõ nhau kết nối với nhau. Do vậy bảo mật chưa phải là một vấn đề được quan tâm. Song hiện nay, bảo mật mạng internet trở thành một vấn đề rất lớn, là mối quan tâm hàng đầu.
- Hỗ trợ tốt hơn cho di động: Thời điểm IPv4 được thiết kế, chưa tồn tại khái niệm về thiết bị IP di động. Trong thế hệ mạng mới, dạng thiết bị này ngày càng phát triển, đòi hỏi cấu trúc giao thức Internet có sự hỗ trợ tốt hơn

  Số liệu thống kê triển khai IPv6 tại Việt Nam tính đến tháng 6 năm 2020

  + Thống kê tại website VNNIX:

  Số lượng địa chỉ IPv6 qui đổi theo đơn vị /64 đã cấp: 416620150784 /64 địa chỉ.

  + Thống kê IPv6 của APNIC (Tổ chức quản lý địa chỉ khu vực châu Á - Thái Bình Dương):

  Triển khai IPv6 tại Việt Nam đạt 42,90%

1.5 Kết luận chương 1

Chương này đã đưa ra sự hạn chế của IPv4, những vấn đề cần thiết phải chuyển đổi sang IPv6, một số giải pháp chuyển đổi ngắn hạn và dài hạn. Trong nội dung chương cũng đưa ra so sánh sự tương đồng và sự khác biệt giữa hai giao thức. Tiêu đề IPv6 có ít trường hơn và đơn giản hơn. Một số trường chuyển từ IPv4 sang IPv6 vẫn giữ nguyên, một số trường có thay đổi tên với sự khác biệt về chức năng, một số trường khác đã bị xóa hoàn toàn và có trường Flow Label được thêm vào. Tiêu đề mở rộng là một điểm mới của IPv6, chúng cung cấp sự linh hoạt hơn và hiệu quả tốt hơn cho IPv6.

CHƯƠNG 2 CÁC GIAO THỨC TRONG IPV6

2.1 Địa chỉ IPv6

2.1.1 Biểu diễn địa chỉ IPv6

Địa chỉ IPv6 có độ dài 128 bit và được viết dưới dạng một chuỗi các chữ số thập lục phân (hexa). Cứ 4 bit được biểu thị bằng một chữ số thập lục phân duy nhất, với tổng số 32 giá trị thập lục phân. Các ký tự chữ và số được sử dụng trong thập lục phân không phân biệt chữ hoa chữ thường.

2.1.2 Độ dài tiền tố IPv6

Trong IPv4, tiền tố hoặc phần mạng của địa chỉ có thể được xác định bằng một netmask thập phân, thường được gọi là mặt nạ mạng con. Ví dụ: 255.255.255.0 chỉ ra rằng phần mạng hoặc prefix length của địa chỉ IPv4 là 24bit ngoài cùng bên trái. Như được định nghĩa trong RFC 4291, trong IPv6, việc thể hiện các tiền tố địa chỉ IPv6 tương tự như cách các tiền tố địa chỉ IPv4 được viết theo ký hiệu (CIDR) định tuyến liên vùng không phân lớp. Một tiền tố địa chỉ IPv6 (phần mạng của địa chỉ) được thể hiện bằng định dạng sau:

ipv6-address/prefix-length

Prefix-length là một giá trị thập phân cho biết số lượng bit tiếp giáp ngoài cùng bên trái của địa chỉ. Prefix-length xác định Prefix hoặc phần của địa chỉ mạng.

Ví dụ: 2001: 0DB8: AA AA: 1111: 0000: 0000: 0000: 0000/64.

Độ dài tiền tố /64 xác định tiền tố hay phần mạng của địa chỉ IPv6. Độ dài tiền tố /64 có nghĩa là còn 64 bit khác, đó là phần Interface ID của địa chỉ IPv6, được gọi là phần địa chỉ Host trong IPv4. Một dải địa chỉ IPv6 hoặc một route luôn biểu diễn dạng: *địa chỉ IPv6/số bit tiền tố.*

Vùng địa chỉ FF00::/8 tương ứng với dải địa chỉ bắt đầu từ FF00:0:0:0:0:0:0:0 đến FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

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

2.1.3 Tóm tắt về các loại địa chỉ IPv6

Trong IPv6 không có địa chỉ quảng bá. IPv6 có 3 loại địa chỉ là: *Unicast, Anycast* và *Multicast.*

Địa chỉ unicast

Một địa chỉ unicast xác định duy nhất một giao diện trên thiết bị IPv6. Một gói tin gửi đến một địa chỉ unicast nó sẽ được gửi đến giao diện được xác định bởi địa chỉ đó. Một địa chỉ IPv6 xác định một giao diện trên máy chủ chứ không phải chính máy chủ (1 giao diện chứ không phải cả cái máy chủ). Một giao diện đơn có thể có nhiều địa chỉ IPv6 và cả địa chỉ IPv4.

Có một số loại địa chỉ unicast trong IPv6, đặc biệt là:

Global unicast.

Unique local unicast.

Link-local unicast.

Unspecified address.

Loopback address

Địa chỉ anycast

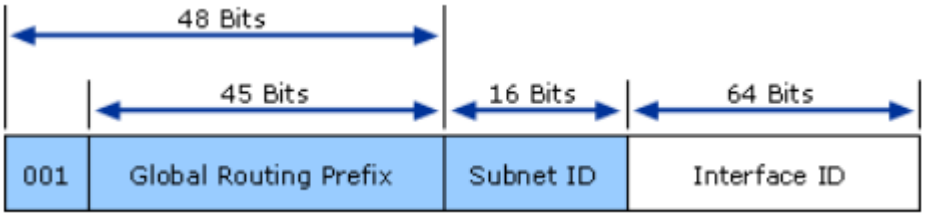
Địa chỉ anycast là một địa chỉ unicast được gán cho một số thiết bị. Một gói được gửi đến một địa chỉ anycast thì gói tin đó chỉ được gửi đến một trong các thiết bị được cấu hình với địa chỉ đó. Gói anycast sẽ được chuyển đến thiết bị gần nhất. Trong IPv6, các thiết bị được gán địa chỉ anycast được định cấu hình rõ ràng để nhận biết rằng đó là địa chỉ anycast.

Địa chỉ multicast

Một địa chỉ multicast xác định một nhóm giao diện, thường thuộc về các thiết bị khác nhau. Một gói được gửi đến một địa chỉ multicast sẽ được gửi đến tất cả các thiết bị được xác định bởi địa chỉ đó. Tất cả các thành viên của nhóm multicast sẽ xử lý gói. Vì vậy, sự khác biệt giữa một địa chỉ anycast và một địa chỉ multicast là một gói anycast chỉ được gửi đến một thiết bị, trong khi một gói multicast gửi đến nhiều thiết bị. Không có địa chỉ quảng bá trong IPv6.

2.1.4 Cấu trúc của địa chỉ Global Unicast Address (GUA)

Đây là những địa chỉ có thể định tuyến toàn cầu và có thể truy cập trên Internet IPv6. Chúng tương đương với các địa chỉ IPv4 public.



Hình 2.1: Cấu trúc một địa chỉ GUA điển hình

Hình 2.1 chỉ ra địa chỉ unicast định danh toàn cầu được bắt đầu với 3 bit 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.

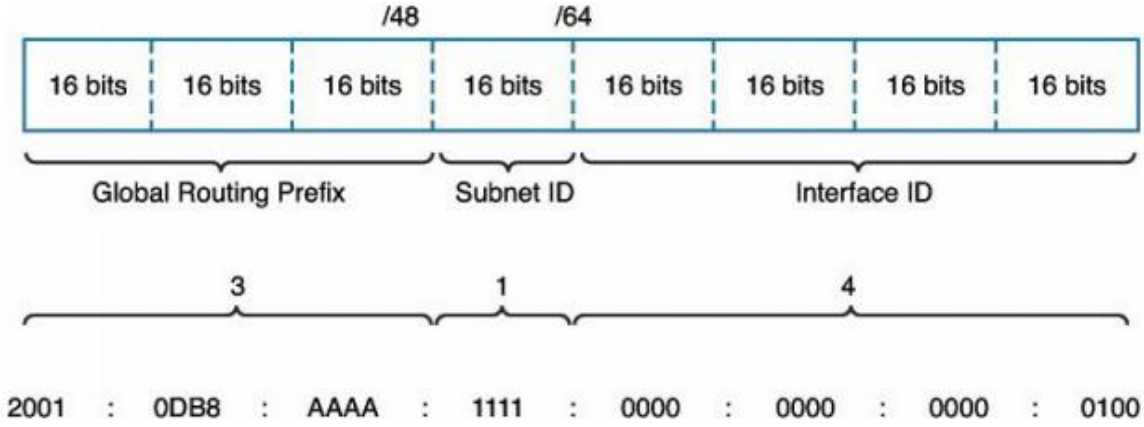
Trong thời gian đầu tiên sử dụng địa chỉ IPv6, IANA cấp phát trong vùng 2001::/16 cho hoạt động Internet IPv6. Tới thời điểm hiện nay, nhu cầu sử dụng IPv6 gia tăng, các vùng địa chỉ khác bắt đầu được cấp phát, như 2400::/16.

Global Routing Prefix: Global Routing Prefix là tiền tố hoặc phần mạng của địa chỉ được chỉ định bởi nhà cung cấp, chẳng hạn như ISP, cho khách hàng hoặc Sites. Mặc dù không còn khuyến nghị độ dài tiền tố cụ thể cho các mạng có kích thước khác nhau, nhưng các RIR như ARIN vẫn có chính sách cho các End Sites sử dụng tiền tố 48 bit (/48).

Subnet ID: ID mạng con Một sự khác biệt lớn giữa địa chỉ IPv4 và IPv6 là vị trí của phần mạng con của địa chỉ. Trong IPv4, các bit được mượn từ phần host của địa chỉ để tạo các mạng con. Với IPv6, ID mạng con là một trường riêng biệt và không phải là một phần của interface ID.

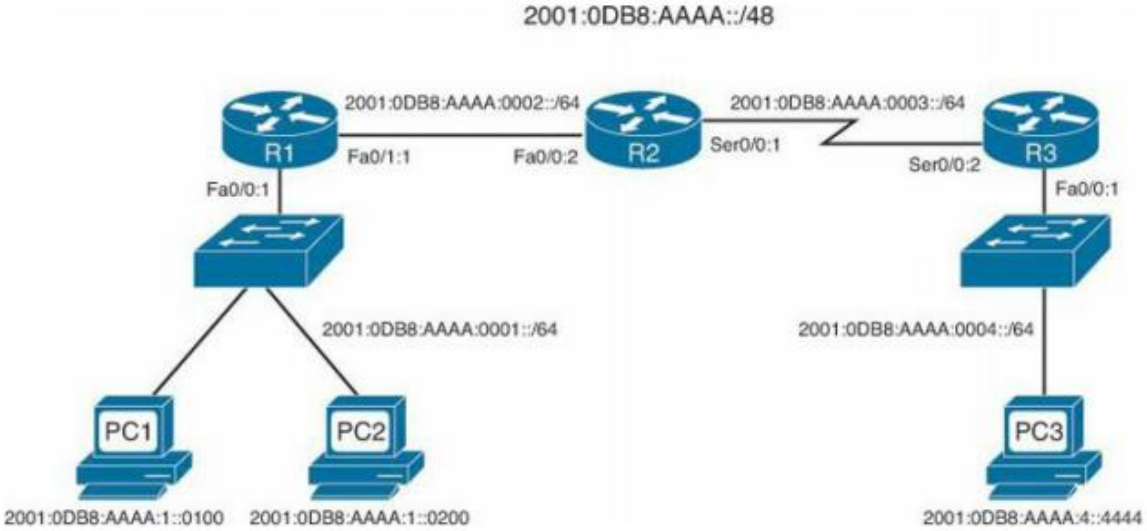
Như hình 2.2, địa chỉ IPv6 có ID 16bit cho subnet. Điều này cho phép có tất cả 65.536 mạng con.

Interface ID: Interface ID xác định duy nhất giao diện trên mạng con. Interface ID 64bit cho phép 18,446,744,073,709,551,616 địa chỉ cho mỗi mạng con. Thuật ngữ giao diện được sử dụng thay vì host, máy chủ vì một máy chủ duy nhất có thể có rất nhiều giao diện, mỗi giao diện lại có 1 hoặc nhiều địa chỉ IPv6. Một sự khác biệt quan trọng khác giữa địa chỉ IPv6 và địa chỉ IPv4 là địa chỉ all-0 và all-1 là địa chỉ giao diện hợp lệ. Interface ID IPv6 có thể chứa tất cả 0 hoặc tất cả 1. Trong IPv4, tất cả 0 trong phần host của địa chỉ được gọi là địa chỉ mạng hoặc địa chỉ mạng con. Tất cả 1 trong phần host của địa chỉ IPv4 chỉ ra địa chỉ quảng bá.



Hình 2.2: Địa chỉ GUA

Ví dụ một topo IPv6 từ việc được cung cấp 1 dải /48 như hình 2.3.

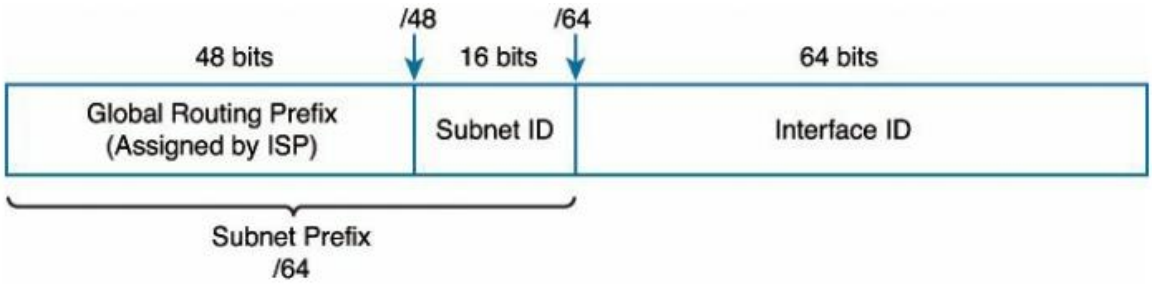


Hình 2.3: IPv6 Topology

Subnetting

Tùy thuộc vào kích thước của mạng, về cơ bản việc subnetting địa chỉ IPv6 rất đơn giản. Có thể thực hiện theo nhiều cách, nó đơn giản hơn nhiều so với việc subnetting một địa chỉ IPv4.

Điều quan trọng là làm rõ một vài thuật ngữ để tránh nhầm lẫn. Như được minh họa trong Hình 2.4, có cả Subnet ID và Subnet Prefix. Thuật ngữ Subnet ID đề cập đến nội dung của trường 16bit được sử dụng để phân bổ các mạng con riêng lẻ. Subnet Prefix đề cập đến Global Routing Prefix và các bit địa chỉ Subnet ID.



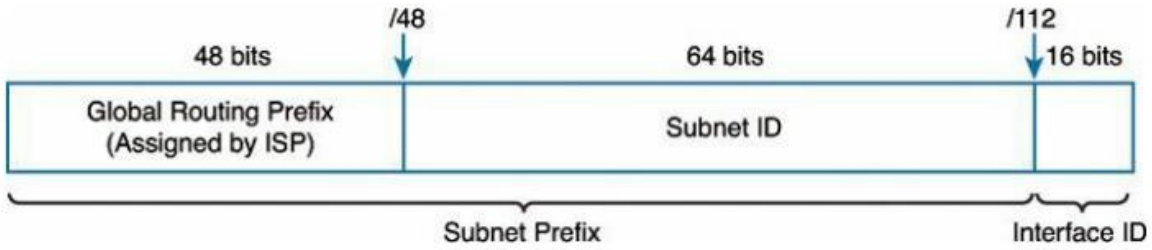
Hình 2.4: Subnet Prefix

Một IPv6 site prefix thường sẽ có /48 được cấp phát bởi nhà cung cấp dịch vụ ISP. Điều này tạo ra một Subnet ID 16 bit cho phép tạo 65.536 mạng con. Các mạng con all-0 và all-1 là các mạng con hợp lệ trong IPv6. Việc cấp phát này cũng dễ dàng thiết lập 64 bit cho Interface ID cung cấp số lượng interface ID là rất lớn trong một mạng con. Với 16 bit Subnet ID, các giá trị có thể nằm trong khoảng từ 0000 đến FFFF. Việc chia mạng con bằng cách sử dụng Subnet ID 16 bit rất dễ thực hiện.

Mở rộng Subnet Prefix

Việc chia mạng con không bị giới hạn trong 16-bit Subnet ID. Cũng giống như với IPv4, nếu muốn mở rộng số lượng mạng con hoặc giảm số lượng Host trên mỗi mạng con, phải mượn bit từ phần dành cho Interface ID. Điều quan trọng cần lưu ý là thực tế chỉ ra rằng điều này chỉ nên được thực hiện trên các liên kết cơ sở hạ tầng mạng (Kết nối Router - Router...). Bất kỳ phân đoạn nào bao gồm các thiết bị đầu cuối đều phải có tiền tố /64. Độ dài tiền tố /64 là bắt buộc để hỗ trợ tự động cấu hình địa chỉ (Stateless Address Autoconfiguration).

Như hình 2.5, có thể sử dụng prefix length /112, mở rộng prefix length gốc /48 thêm 64 bit (bốn đoạn mã), tạo cho nó prefix length là /112.



Hình 2.5: /112 Subnet Prefix

4 Subnet đầu tiên /64 sẽ là

2001:0DB8:AAAA:0000:0000:0000:0000::/112

2001:0DB8:AAAA:0000:0000:0000:0001::/112

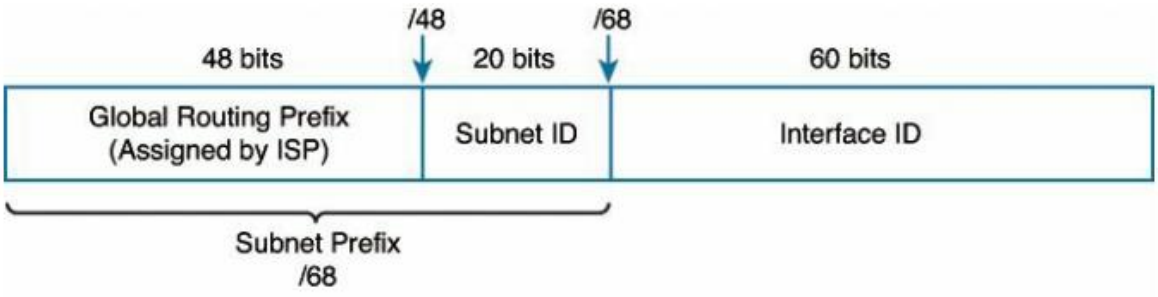
2001:0DB8:AAAA:0000:0000:0000:0002::/112

2001:0DB8:AAAA:0000:0000:0000:0003::/112

Ngay cả khi mở rộng Subnet ID, việc chia mạng con rất đơn giản miễn là chia trên ranh giới một số hecxa (4 bit).

Thực hiện Subnetting ở biên của Nibble

Nếu thực hiện mở rộng Subnet ID, có nghĩa là sử dụng các bit từ Interface ID, thì cách tốt nhất là chia mạng con trên ranh giới nibble (số hexa 4 bit). Trong hình 2.6 mở rộng /64 subnet prefix thêm 4 bit, một nibble, thành /68. Điều này làm tăng Subnet ID từ 16 bit lên 20 bit. Bằng cách đó cho phép nhiều mạng con hơn nhưng giảm kích thước của Interface ID. Bằng cách mở rộng Subnet Prefix thêm 4 bit hoặc một nibble như trong hình 2.6.



Hình 2.6: Mở rộng /64 subnet prefix thêm 4 bit

Dễ dàng thực hiện subnetting vào biên của Nibble (4 bit)

2001:0DB8:AAAA:**0000:0**000::/68

2001:0DB8:AAAA:**0000:1**000::/68

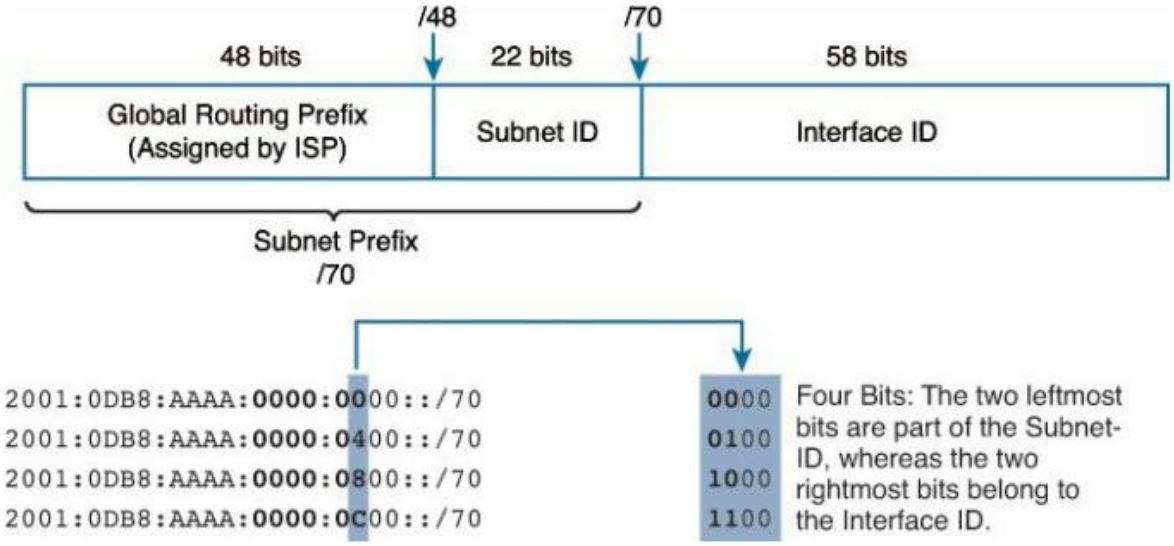
2001:0DB8:AAAA:**1111:2**000::/68

Đến

2001:0DB8:AAAA:FFFF:F000::/68

Thực hiện Subnetting trong 1 Nibble

Đối với hầu hết các mạng của khách hàng, không nên subnetting vào trong một nibble. Nó không có lợi ích gì mà chỉ làm cho việc thực hiện và xử lý sự cố trở nên khó khăn hơn.



Hình 2.7: Thực hiện Subnetting trong 1 Nibble

Trên hình 2.7 là ví dụ về 4 subnet đầu tiên khi thực hiện chia /70.

2001:0DB8:AAAA:**0000:00**00::/70

2001:0DB8:AAAA:**0000:04**00::/70

2001:0DB8:AAAA:**0000:08**00::/70

2001:0DB8:AAAA:**0000:0C**00::/70

Mạng con đầu tiên ngay lập tức nhìn ra, nhưng có thể thấy rằng mạng con thứ hai đòi hỏi một chút suy nghĩ. Địa chỉ IPv6 sử dụng các giá trị thập lục phân để thể hiện bằng 1 giá trị ta sử dụng 4 bit. Vì muốn subnetting /70, nên nửa đầu của chữ số thập lục phân (2 bit) thuộc về Subnet ID và nửa còn lại thuộc về Interface ID như hình 2.8.

Subnetting Within a Nibble	Last Digit of Subnet ID Binary to Hexadecimal
2001:0DB8:AAAA:0**000**:**0**000::/70	0000 = 0
2001:0DB8:AAAA:**0000**:**04**00::/70	0100 = 4
2001:0DB8:AAAA:**0000**:**08**00::/70	1000 = 8
2001:0DB8:AAAA:**0000**:**0C**00::/70	1100 = C

Hình 2.8: Subnetting trong Nibble

2.1.5 Ứng dụng các kiểu địa chỉ trong IPv6

2.1.5.1 Unicast Address

Một địa chỉ unicast xác định duy nhất một giao diện trên thiết bị IPv6. Một gói được gửi đến một địa chỉ unicast nó sẽ được nhận bởi giao diện nào được gán cho địa chỉ đó. Tương tự như IPv4, địa chỉ IPv6 nguồn phải là địa chỉ unicast. Phần này bao gồm các loại địa chỉ unicast khác nhau, sau đây là từng loại địa chỉ unicast:

Global unicast: Một địa chỉ IPv6 có thể định tuyến trong miền Internet, tương tự như các địa chỉ public IPv4.

Link-local: Chỉ được sử dụng để liên lạc với các thiết bị trên cùng một liên kết cục bộ.

Loopback: Một địa chỉ không được gán cho bất kỳ giao diện vật lý nào và có thể được sử dụng cho một host để gửi một gói IPv6 đến chính nó.

Unspecified address: Chỉ được sử dụng làm địa chỉ nguồn trong quá trình chưa cấp phát được IPv6.

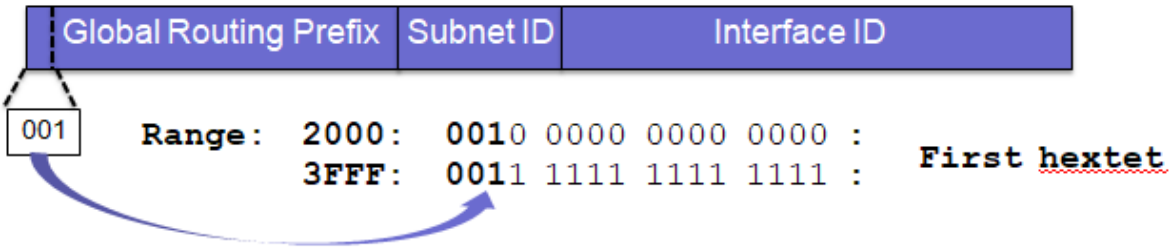
Unique local: Tương tự như các địa chỉ riêng trong IPv4 (RFC 1918). Các địa chỉ này không nhằm mục đích có thể định tuyến trong Internet. Tuy nhiên, không giống như các địa chỉ RFC 1918, các tiền tố Unique local có xác suất cực kỳ cao là duy nhất trên toàn cầu.

IPv4 embedded: Nhúng 32 bít địa chỉ IPv4 vào một địa chỉ IPv6.

2.1.5.1.1 Global Unicast Address

Còn được gọi là địa chỉ unicast toàn cầu, có thể định tuyến toàn cầu và có thể truy cập trong Internet IPv6. Chúng tương đương với các địa chỉ IPv4 public. Chúng

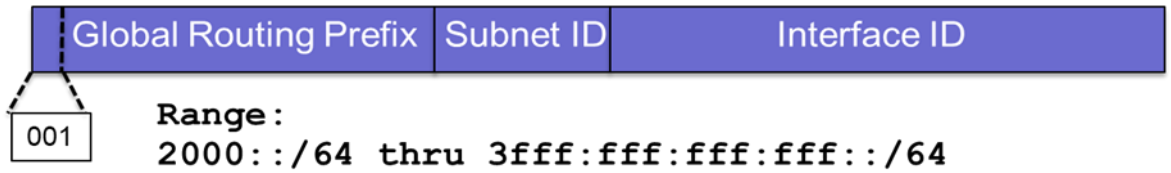
đóng một vai trò quan trọng trong kiến trúc địa chỉ IPv6. Một trong những động lực chính để chuyển sang IPv6 là sự cạn kiệt IPv4.



Hình 2.9: Dải địa chỉ Global unicast

Hình 2.9 cho thấy không gian địa chỉ có thể được phân bổ cho Cơ quan đăng ký Internet khu vực (RIR) và nhà cung cấp dịch vụ Internet (ISP). Đây là các phân bổ tối thiểu, có nghĩa là RIR sẽ nhận được / 23 hoặc ngắn hơn, ISP sẽ nhận được / 32 hoặc ngắn hơn và một Site sẽ có được / 48 hoặc ngắn hơn.

Internet Corporation for Assigned Names and Numbers (ICANN), phân bổ các khối địa chỉ IPv6 cho 5 châu lục RIR. IANA bắt đầu bằng giá trị nhị phân 001 hoặc tiền tố 2000 :: / 3. Vậy dải địa chỉ unicast toàn cầu từ có giá trị 2000 :: / 3 đến 3FFF :: /3 Giá trị tiền tố 2000 :: / 3 Trong Nibble đầu tiên, có 3 bit đầu tiên là 001x. Bit thứ tư, x, có thể là 0 hoặc 1. Vậy điều này dẫn đến trong hextet đầu tiên là 2 (0010) hoặc 3 (0011). 12 bit còn lại trong hextet (16 bit) có thể là 0 hoặc 1, được minh họa như hình 2.10



Hình 2.10: Dải địa chỉ Global Unicast

Một interface có thể được cấp phát nhiều địa chỉ IPv6 thuộc cùng một mạng hoặc các mạng khác nhau.

Một interface không nhất thiết phải được cấu hình địa chỉ global unicast nhưng ở mức tối thiểu, nó phải được gán với một địa chỉ link local unicast. Nói cách khác, nếu một interface có địa chỉ global unicast, thì nó phải có một địa chỉ link local

unicast. Tuy nhiên, nếu một giao diện có một địa chỉ link local unicast, thì nó không nhất thiết phải có một địa chỉ global unicast. Địa chỉ global unicast được thảo luận trong phần tiếp theo.

Tương tự như IPv4, để cấu hình địa chỉ IPv6 ta cũng có các cách là cấu hình tự động hoặc cấu hình bằng nhân công.

Static Global Unicast

Việc cấu hình thủ công một địa chỉ global có một số tùy chọn sau:

Static configuration: Cấu hình tĩnh tương tự như cấu hình địa chỉ IPv4 tĩnh. Địa chỉ IPv6 và độ dài tiền tố đều được cấu hình trên giao diện.

EUI-64: Loại cấu hình này cho phép bạn chỉ định prefix và prefix length trong khi interface ID được tạo tự động.

IP unnumbered: Trong IPv6 tương tự như trong IPv4, nó cho phép một giao diện sử dụng địa chỉ IP của một giao diện khác từ cùng một thiết bị.

Dynamic IPv6 Address Allocation

Địa chỉ Global unicast cũng có thể được cấu hình tự động, mà không cần bất kỳ thao tác cấu hình thủ công nào. Hai cách để định cấu hình tự động các địa chỉ Global unicast như sau:

Tự động cấu hình địa chỉ không trạng thái (SLAAC): Sử dụng phương pháp này, Interface ID được tạo bằng EUI-64 trong khi prefix và prefix length được xác định từ các bản tin ND Router Advertisement.

DHCPv6: Giao thức cấp phát địa chỉ động (DHCP) cho IPv6 tương tự như DHCP cho IPv4. Một thiết bị có thể tự động nhận thông tin địa chỉ IPv6 bằng cách sử dụng các dịch vụ của DHCPv6 server.

Stateless Address Autoconfiguration (SLAAC) Tự động cấu hình địa chỉ không trạng thái:

Là phương pháp đầu tiên trong hai phương thức tự động được thảo luận để gán địa chỉ global unicast cho các giao diện. SLAAC được định nghĩa trong RFC 4862.

SLAAC sử dụng định dạng EUI-64. Bằng cách sử dụng địa chỉ MAC Ethernet của mình, quy trình này cho phép một thiết bị tạo Interface ID (host portion) của địa chỉ.

Kết hợp với một quy trình khác, Neighbor Discovery Protocol, một host có thể xác định toàn bộ địa chỉ global unicast của nó mà không cần bất kỳ cấu hình thủ công hoặc máy chủ DHCPv6 nào. ND (Neighbor Discovery) và SLAAC được thảo luận chi tiết hơn trong Chương sau. ND được giới thiệu ở đây để hiểu cơ bản về SLAAC. ND được định nghĩa trong RFC 4861, Neighbor Discovery trong IPv6. ND sử dụng ICMPv6 để trao đổi các thông điệp cần thiết cho các chức năng của nó, cụ thể là 5 bản tin ICMPv6 mới:

Router Advertisement (RA) messages

Router Solicitation (RS) messages

Neighbor Solicitation (NS) messages

Neighbor Advertisement (NA) messages

Redirect messages

ICMPv6 là một giao thức mạnh mẽ hơn nhiều so với ICMPv4. ICMPv6 chứa các chức năng và cải tiến mới. Chỉ có 4 bản tin đầu tiên có liên quan đến SLAAC. Chi tiết các bản tin này sẽ được đưa ra trong chương tiếp theo.

Một địa chỉ được cấu hình tự động theo SLAAC sẽ ở 1 trong các trạng thái sau:

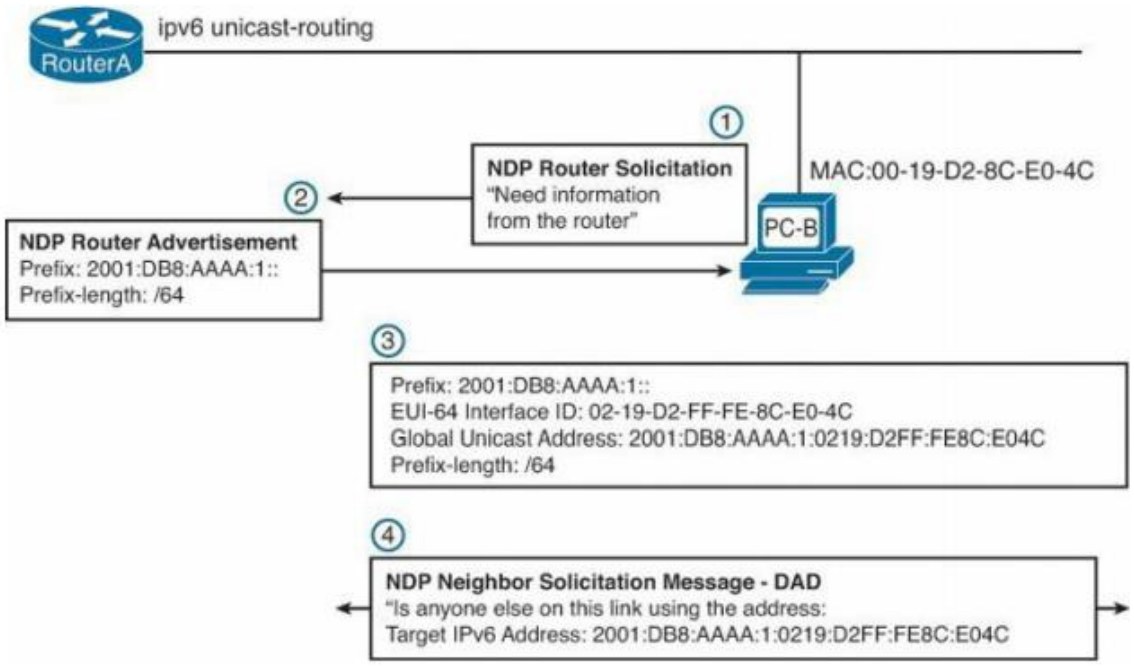
Tentative (Dự kiến): Tính duy nhất của địa chỉ đang trong quá trình xác minh. Một địa chỉ dự kiến không được coi là được gán cho một giao diện. Một giao diện sẽ loại bỏ các gói đã nhận được gửi đến một địa chỉ dự kiến, nhưng chấp nhận các gói Neighbor Discovery liên quan đến Phát hiện địa chỉ trùng lặp cho địa chỉ dự kiến. (DAD).

Preferred (Ưu tiên): Địa chỉ giao diện đã được xác minh là duy nhất. Thiết bị có thể gửi và nhận lưu lượng sử dụng địa chỉ này. Khoảng thời gian mà một địa chỉ có thể vẫn ở trạng thái dự kiến và trạng thái ưu tiên được bao gồm trong thông báo Router Advertisement message.

Deprecated: (Không dùng nữa): Địa chỉ được gán cho giao diện vẫn hợp lệ nhưng việc triển khai không được khuyến khích. Một địa chỉ không dùng nữa sẽ không còn được sử dụng làm địa chỉ nguồn trong các liên lạc mới. Một địa chỉ không dùng nữa có thể tiếp tục được sử dụng làm địa chỉ nguồn trong các liên lạc hiện có.

Valid (Hợp lệ): Địa chỉ là địa chỉ ưu tiên hoặc địa chỉ không dùng nữa. Một địa chỉ hợp lệ có thể là địa chỉ nguồn hoặc đích của gói. Lượng thời gian mà một địa chỉ vẫn ở trạng thái dự kiến và hợp lệ được bao gồm trong thông báo Router Advertisement message.

Invalid: Địa chỉ hợp lệ trở thành không hợp lệ khi hết hạn sử dụng. Địa chỉ không hợp lệ sẽ không xuất hiện dưới dạng địa chỉ đích hoặc địa chỉ nguồn của gói.



Hình 2.11: NDP Router Advertisement và Router Solicitation Messages

Trong hình 2.11, bộ định tuyến A định kỳ gửi tin nhắn ND Router Advertisement (RA) messages. Các thông báo RA được khởi tạo bởi các bộ định tuyến để advertise sự hiện diện và các tham số dành riêng cho liên kết của chúng như prefix, prefix length, default gateway, và link maximum transmission unit (MTU). Router Advertisements được gửi đến địa chỉ multicast tất cả các nút (FF02 :: 1), về cơ bản giống như quảng bá. Địa chỉ Multicast sẽ được thảo luận sau trong chương này. Router Advertisements được gửi định kỳ và cũng để phản hồi lại các Router Solicitation (RS) message.

Message RS được khởi tạo bởi các host để yêu cầu bộ định tuyến gửi Router Advertisement. Thông điệp RS được gửi đến địa chỉ multicast của tất cả các bộ định tuyến (FF02 :: 2), Massage này sẽ được xử lý bởi bất kỳ bộ định tuyến IPv6 nào

trên Link. Để bộ định tuyến gửi tin nhắn Router Advertisement và để chạy giao thức định tuyến IPv6, nó phải được cấu hình bằng lệnh **ipv6 unicast-routing** (RouterA(config)# ipv6 unicast-routing).

Quy trình SLAAC bao gồm các bước sau:

Bước 1. Như đã lưu ý trong Hình 2-21, PC-B được cấu hình để tự động lấy địa chỉ IP của nó. Kể từ khi khởi động, PC-B không thấy thông báo Router Advertisement message, do đó, nó sẽ gửi một thông báo Router Solicitation message để thông báo cho local IPv6 router rằng nó cần một RA message.

Bước 2. Router A nhận được Router Solicitation message và trả lời với một Router Advertisement. Bao gồm trong RA message prefix and prefix length của link, cùng với địa chỉ của chính nó là default gateway. Địa chỉ default gateway mà RouterA truyền bá là địa chỉ link-local address của nó, không phải là địa chỉ global unicast address.

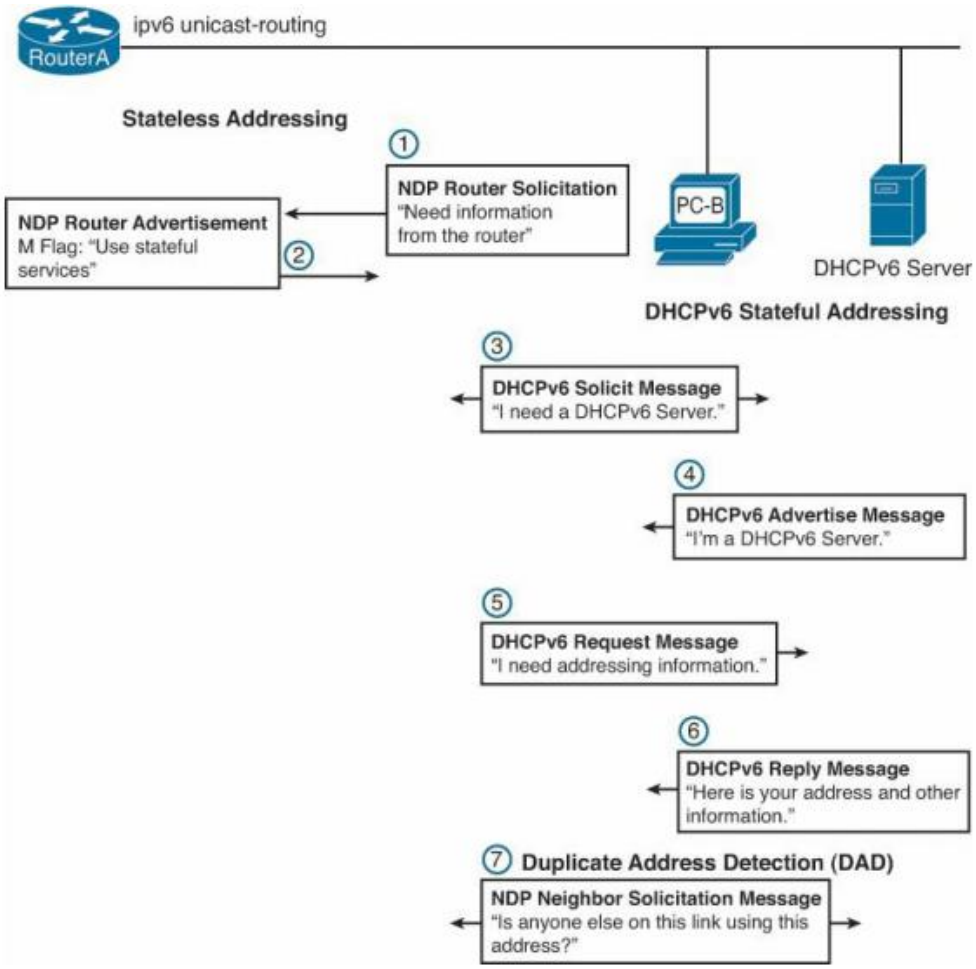
Bước 3. PC-B nhận Router Advertisement, bao gồm prefix and prefix length cho local network, 2001: DB8: AAAA: 1:: / 64. Địa chỉ MAC của PC-B là 00-19-D2-8C-E0-4C. Sử dụng EUI-64 đã sửa đổi, FF-FE được chèn giữa OUI và số nhận dạng thiết bị của địa chỉ MAC. Bit thứ bảy được lật từ 0 thành 1, thay đổi giá trị thập lục phân thứ hai từ 0 thành 2. Kết quả là, ID giao diện được gán giá trị 64 bit 02-19-D2-FF-FE-8C-E0-4C. PC-B lấy tiền tố 2001: DB8: AAAA: 1 :: từ Router Advertisement để tạo địa chỉ unicast toàn cầu năm 2001: DB8: AAAA: 1: 02-19-D2-FF-FE-8C-E0-4C. Địa chỉ ở trạng thái tentative (dự kiến) cho đến khi tính duy nhất của nó được xác minh trong bước tiếp theo.

Bước 4. Vì SLAAC là một quy trình không trạng thái, nên không có bất kỳ thiết bị nào theo dõi tất cả các địa chỉ unicast toàn cầu trên liên kết để ngăn ngừa trùng lặp. Vì vậy, tùy thuộc vào host để đảm bảo rằng nó đã không tạo cho mình một địa chỉ đã được sử dụng bởi một thiết bị khác. Quá trình ND này được gọi là Phát hiện địa chỉ trùng lặp (DAD).

Điều này tương tự như một gratuitous ARP request trong IPv4. PC-B gửi tin nhắn Neighbor Solicitation (NS) tương tự như một yêu cầu ARP của IPv4, với địa

chỉ global unicast 2001: DB8: AAAA: 1: 02-19-D2- FF-FE-8C-E0-4C như một mục tiêu. Nếu một thiết bị khác có địa chỉ này, nó sẽ trả lời bằng tin nhắn Neighbor Advertising, tương tự như trả lời ARP trong IPv4. Thông điệp NS được gửi đến một solicited node multicast address. Mục đích của địa chỉ solicited node multicast address tương tự như địa chỉ quảng bá nhưng hiệu quả hơn nhiều. Các địa chỉ solicited node multicast address sẽ được thảo luận sau trong chương này. Nếu PC-B không nghe thấy phản hồi về tin nhắn Neighbor Solicitation dưới dạng Neighbor Advertisement, thì có thể yên tâm rằng địa chỉ global unicast của nó là duy nhất. Địa chỉ hiện đang ở trạng thái ưu tiên (preferred).

Việc một host lấy thông tin địa chỉ tự động sử dụng SLAAC hoặc DHCPv6 tùy thuộc vào việc cấu hình bản tin Router Advertisement message trong Router. Thông báo RA có thể được cấu hình để chỉ cho các thiết bị sử dụng statefull, DHCPv6 thay vì tự động cấu hình stateless. Khả năng cho phép thiết bị tự động xác định địa chỉ global unicast mà không cần máy chủ DHCPv6 lợi thế đáng kể trong IPv6. Trong một mạng “Internet of things,” các thiết bị IPv6 như webcam và cảm biến chỉ cần được bật nguồn và có thể lấy tất cả thông tin địa chỉ của chúng từ bộ định tuyến và xử lý theo cách dùng EUI-64. Mô phỏng Stateful addressing using DHCPv6 như hình 2.12.



Hình 2.12: Stateful addressing using DHCPv6

Các bước như sau:

Bước 1. PC-B gửi ra bản tin Router Solicitation nếu nó không nhận được bản tin Router Advertisement

Bước 2. Router gửi ra bản tin Router Advertisements có trường 1bit được gọi là quản lý cờ cấu hình địa chỉ hoặc cờ M:

Khi cờ này được đặt thành 0, nó sẽ thông báo cho các thiết bị sử dụng Tự động cấu hình địa chỉ không trạng thái (SLAAC).

Nếu cờ được đặt thành 1, nó cho biết thiết bị cần sử dụng DHCPv6.

Bây giờ PC-B nhận ra rằng nó phải sử dụng stateful autoconfiguration, nó bắt đầu quá trình để lấy thông tin địa chỉ của nó từ máy chủ DHCPv6.

Bước 3. PC-B gửi một tin nhắn DHCPv6 Solicit đến một địa chỉ multicast đặc biệt dành riêng cho các máy chủ DHCPv6 là FF02 :: 1: 2.

Bước 4. Một hoặc nhiều máy chủ DHCPv6 sẽ phản hồi với thông báo DHCPv6 Advertise message, cho biết rằng chúng có sẵn cho dịch vụ DHCPv6. Nếu PC-B nhận được nhiều tin DHCPv6 Advertise message từ các Server khác nhau, sẽ có một quy trình tạo ra giá trị Tùy chọn Máy chủ mà nó sẽ sử dụng để chọn máy chủ DCHPv6 thích hợp

Bước 5. PC-B sẽ trả lời máy chủ được chọn bằng cách gửi tin nhắn Request message để yêu cầu tham số cấu hình, bao gồm địa chỉ IP.

Bước 6. Máy chủ DHCPv6 trả lời bằng Reply message có chứa các địa chỉ được gán và các tham số cấu hình khác tương tự như các thông số được sử dụng với DHCP cho IPv4. Mặc dù PC-B có được địa chỉ từ DHCPv6, một stateful service, nó vẫn sẽ sử dụng quy trình Phát hiện địa chỉ trùng lặp (DAD) để đảm bảo rằng không có bất kỳ thiết bị nào khác trên liên kết sử dụng địa chỉ này.

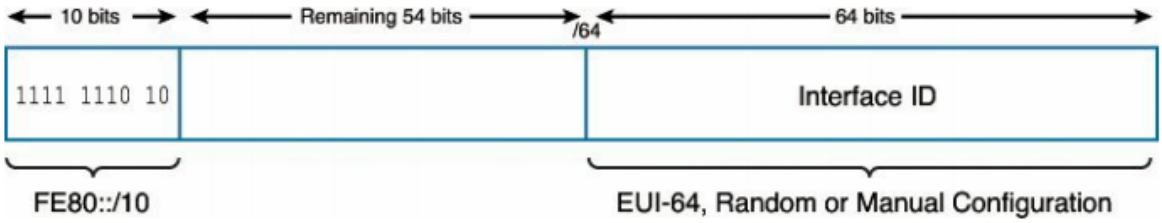
Bước 7. PC-B gửi thông báo Neighbor Solicitation (NS) với địa chỉ global unicast mới vừa nhận được từ DHCPv6 server tới tất cả các thiết bị trên liên kết. Địa chỉ nguồn là một địa chỉ không xác định (địa chỉ "::") Địa chỉ đích là solicited node multicast address, như đã đề cập trước đó, tương tự như địa chỉ quảng bá. Nếu bất kỳ thiết bị nào trong liên kết có cùng địa chỉ, thiết bị đó sẽ phản hồi với thông báo Neighbor Advertisement message.

2.1.5.1.2 Link-local Unicast

Là địa chỉ unicast được giới hạn trong một liên kết duy nhất. Tính duy nhất của chúng phải được xác nhận trên liên kết đó. Nói cách khác, các bộ định tuyến sẽ không chuyển tiếp bất kỳ gói tin nào có link-local source hoặc destination addresses Link-local Unicast được cấu hình theo 1 trong 3 cách sau:

- Dynamically sử dụng EUI-64.
- Tạo Random interface ID
- Static manual link-local address

Một thiết bị có thể tự tạo hoàn toàn địa chỉ Link-local addresses của mình mà không cần máy chủ DHCPv6 hoặc bản tin Router Advertisement message. Như hình 2.13.



Hình 2.13: Link-local Unicast

Sử dụng prefix và prefix length này (FE80::/10) sẽ cung cấp phạm vi địa chỉ link-local từ FE80 :: / 10 đến FEBF :: / 10.

FE80::/ 10 chỉ ra rằng 10 bit đầu tiên phải khớp với prefix. Prefix là FE80, hoặc 1111 1110 10 ở dạng nhị phân. Vì vậy, miễn là 10bit đầu tiên này khớp với nhau, 54 bit còn lại có thể có giá trị bất kỳ. Do đó, hextet đầu tiên có thể là bất kỳ giá trị nào trong phạm vi FE80 đến FEBF, như hình 2.14.

Link-local Unicast Address (Hexadecimal)	Range of First Hextet	Range of First Hextet in Binary
FE80::/10	FE80	1111 1110 1000 0000
	FEBF	1111 1110 1011 1111

Hình 2.14: Dải địa chỉ Link-local Unicast

IPv6 link-local addresses được sử dụng theo các cách sau:

- Routers sử dụng link-local address của nó làm địa chỉ default gateway trong Router Advertisements.
- Routers chạy các giao thức như EIGRP cho IPv6 và OSPFv3 sử dụng các địa chỉ link-local addresses của chúng để thiết lập các liên kết.
- Các tuyến động (Dynamic routes) trong các bảng định tuyến IPv6 sử dụng link-local address làm địa chỉ hop tiếp theo của chúng.

Dynamic Link-local Address: EUI-64

EUI-64 Theo mặc định, các thiết bị tự động tạo địa chỉ link-local unicast của riêng chúng mà không cần sự hỗ trợ của thiết bị khác như máy chủ DHCP hoặc Router.

Randomly Generated Interface IDs

EUI-64 là một kỹ thuật thuận tiện để tự động tạo Interface ID 64bit từ địa chỉ MAC 48 bit. Tuy nhiên, điều này gây lo ngại cho một số người dùng bởi khả năng theo

dõi địa chỉ IPv6 thông qua địa chỉ MAC 48bit được sử dụng để tạo Interface ID. Để giảm bớt mối lo ngại về quyền riêng tư này, các thiết bị có thể sử dụng Interface ID 64bit được tạo ngẫu nhiên.

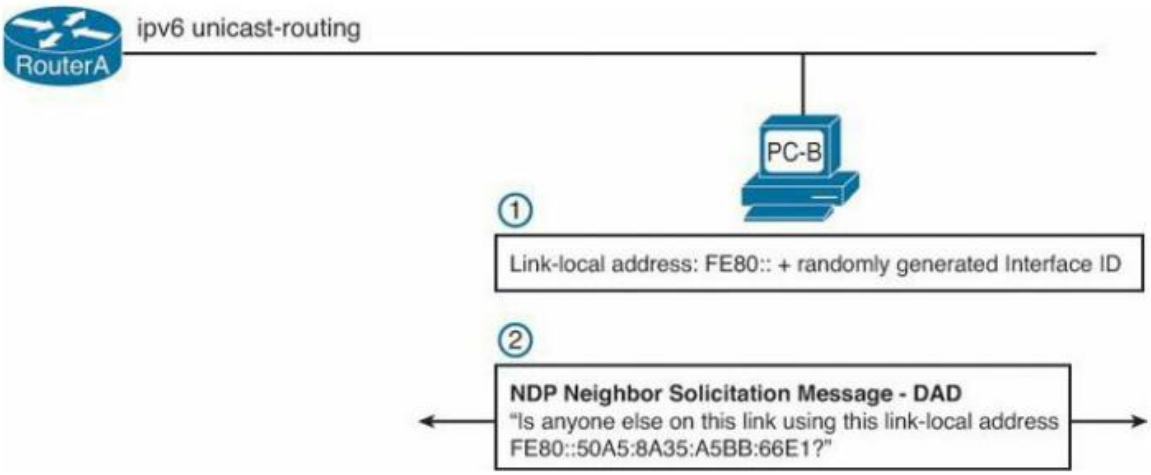
Việc một thiết bị sử dụng EUI-64 hay Interface IDs được tạo ngẫu nhiên đều phụ thuộc vào hệ điều hành. Bộ định tuyến của Cisco sử dụng EUI-64. Các hệ điều hành Windows cũ hơn XP sử dụng một số ngẫu nhiên cho ID giao diện. Các hệ điều hành Windows mới hơn sử dụng EUI-64. Xu hướng chung là để các hệ điều hành, máy chủ tạo ngẫu nhiên Interface ID của chúng

Static Link-local Address

Địa chỉ link-local addresses được gán động là lý tưởng cho hầu hết các thiết bị như máy chủ. Nhược điểm là Interface ID dài, có thể khó nhận biết hoặc ghi nhớ khi khắc phục sự cố hoặc xác minh các hoạt động mạng. Bởi vì các giao thức định tuyến động như EIGRP cho IPv6 và OSPFv3 sử dụng các địa chỉ link-local addresses để thiết lập các quan hệ láng giềng và chuyển các thông báo khác, nên việc sử dụng các địa chỉ link-local addresses được cấu hình thủ công sẽ dễ nhận biết hơn.

Link-local Addresses and Duplicate Address Detection

Như đã thảo luận trước đây với các địa chỉ global unicast, các thiết bị sử dụng Phát hiện địa chỉ trùng lặp (DAD) để xem liệu một thiết bị khác trên liên kết có sử dụng địa chỉ mà nó sắp sử dụng hay không. Cho dù địa chỉ link-local address được tạo tự động hay được cấu hình thủ công, trước khi thiết bị sử dụng địa chỉ link-local address, nó sẽ thực hiện DAD để đảm bảo rằng nó là duy nhất trên liên kết như hình 2.15.



Hình 2.15: Phát hiện địa chỉ Link-local trùng lặp

Link-local Addresses and Default Gateways

Giao thức Neighbor Discovery Protocol (ND or NDP đã được thảo luận trước đó. Sử dụng bản tin Router Solicitation và Router Advertisement, hosts có thể tự động lấy thông tin địa chỉ IP, chẳng hạn như prefix, prefix length, và default gateway address. Trong hình 73, PC1 đã được cấu hình để tự động lấy địa chỉ IP của nó. PC1 gửi thông báo Giới thiệu Bộ định tuyến ND và Bộ định tuyến R1 phản hồi với Router Advertisement. Vì PC1 đang chạy Windows Vista, thay vì sử dụng EUI-64, nó sử dụng một số ngẫu nhiên cho ID giao diện của nó và thêm prefix từ bản tin Router Advertisement.

2.1.5.1.3 Loopback Address

Địa chỉ loopback IPv6 là địa chỉ all-0 ngoại trừ bit cuối cùng, được đặt thành 1. Nó tương đương với địa chỉ loopback IPv4 127.0.0.1, biểu diễn như hình 2.16.

Representation	IPv6 Loopback Address
Preferred	0000:0000:0000:0000:0000:0000:0000:0001
No leading 0s	0:0:0:0:0:0:0:1
Compressed	::1

Hình 2.16: Biểu diễn địa chỉ IPv6 Loopback

Địa chỉ loopback có thể được sử dụng bởi một Node để gửi gói IPv6 đến chính nó, thường là khi kiểm tra TCP/IP stack. Điều này tương đương với địa chỉ 127.0.0.0/8 trong IPv4. Địa chỉ Loopback có các đặc điểm sau:

- Không thể gán địa chỉ loopback cho giao diện vật lý.
- Địa chỉ loopback chỉ có thể là địa chỉ nguồn nếu gói không được gửi bên ngoài thiết bị.
- Địa chỉ loopback chỉ có thể là địa chỉ đích nếu gói không được gửi bên ngoài thiết bị.
- Một Router không bao giờ có thể chuyển tiếp một gói có địa chỉ đích là địa chỉ loopback.
- Thiết bị phải hủy gói tin nhận được trên interface mà có địa chỉ đích là địa chỉ loopback.

2.1.5.1.4 Unspecified Address

Địa chỉ unicast không xác định là địa chỉ gồm toàn bit 0. Nó không thể được gán cho một giao diện. Một địa chỉ unicast không xác định được sử dụng làm địa chỉ nguồn để chỉ ra sự tạm vắng của một địa chỉ (chưa lấy được IP, ví dụ: dùng làm IP tạm trong quá trình DAD xem có bị xung đột không).

Unspecified addresses có những đặc điểm sau:

- Unspecified addresses có thể được chỉ định cho giao diện vật lý.
- Một Unspecified addresses cho biết sự vắng mặt của một địa chỉ.
- Unspecified addresses có thể được sử dụng làm địa chỉ đích.
- Một Router sẽ không bao giờ chuyển tiếp một gói có địa chỉ nguồn là địa chỉ Unspecified addresses.

2.1.5.1.5 Unique Local Address

Địa chỉ Unique local và còn được gọi là địa chỉ local IPv6 addresses. Các địa chỉ này dự kiến là duy nhất trên toàn cầu nhưng không thể định tuyến trên Internet toàn cầu. Chúng phải được sử dụng trong một khu vực hạn chế hơn, chẳng hạn như trong một Site hoặc được định tuyến giữa một số lượng hạn chế của các Sites.

Unique local addresses có các đặc điểm sau:

- Có prefix duy nhất trên toàn cầu hoặc ít nhất có xác suất duy nhất rất cao.
- Cho phép các Site được kết hợp hoặc kết nối riêng tư mà không có xung đột địa chỉ hoặc yêu cầu đánh số lại địa chỉ.
- Độc lập với bất kỳ nhà cung cấp dịch vụ Internet nào và có thể được sử dụng trong một Site mà không cần kết nối Internet.
- Nếu vô tình bị rò rỉ bên ngoài một Site bằng cách định tuyến hoặc Hệ thống tên miền (DNS), thì cũng sẽ không xảy ra xung đột với bất kỳ địa chỉ nào khác.
- Có thể được sử dụng giống như một địa chỉ unicast toàn cầu.

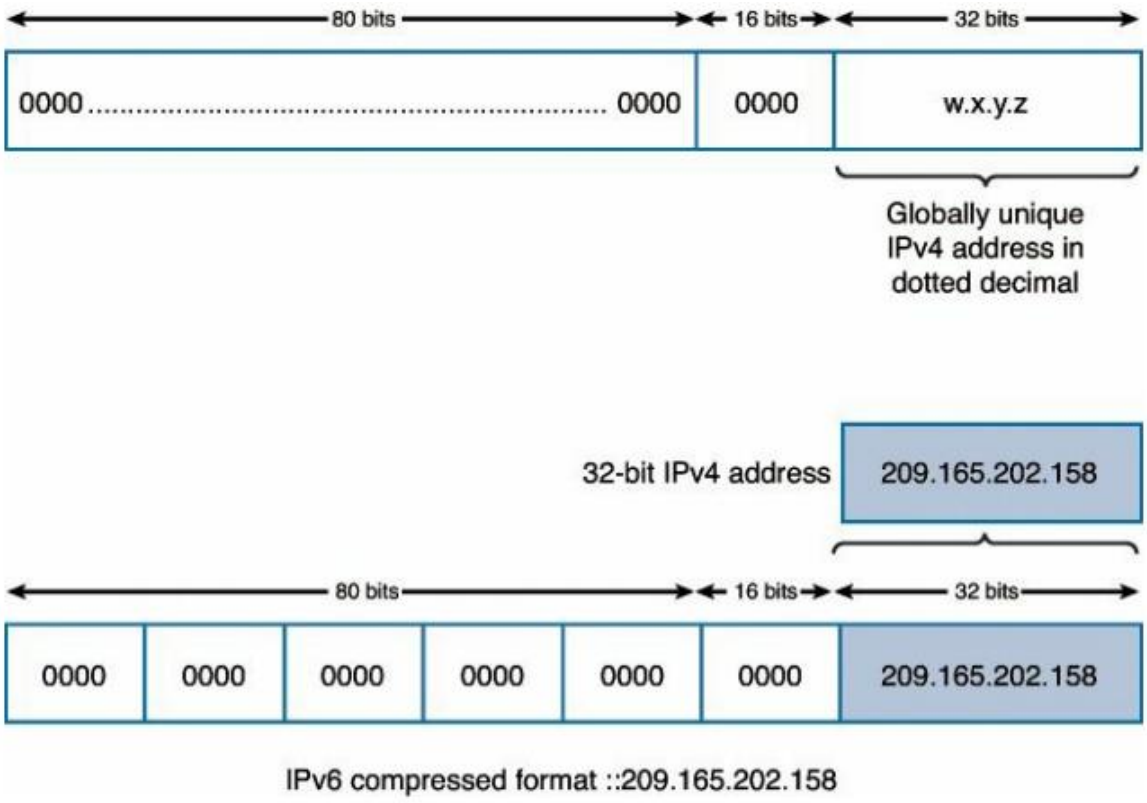
2.1.5.1.6 IPv4 Embedded Address

Địa chỉ unicast cuối cùng là địa chỉ IPv4 Embedded. Địa chỉ IPv4 Embedded là địa chỉ IPv6 được sử dụng để giúp chuyển đổi từ IPv4 sang IPv6. Các địa chỉ này được sử dụng để thể hiện địa chỉ của IPv4 bên trong địa chỉ IPv6. RFC 4291 định nghĩa hai loại địa chỉ IPv4 embedded addresses:

- Địa chỉ IPv6 tương thích với IPv4 (IPv4-Compatible IPv6 Addresses) (không còn dùng nữa).
- Địa chỉ IPv6 được ánh xạ IPv4 (IPv4-Mapped IPv6 Addresses).

IPv4-Compatible IPv6 Addresses

Địa chỉ IPv6 tương thích với IPv4 được sử dụng bởi các thiết bị dual-stack hỗ trợ cả IPv4 và IPv6. 96 bit đầu tiên được đặt thành tất cả 0, bao gồm segment 16 bit, được sử dụng để phân biệt với địa chỉ IPv6 được ánh xạ IPv4. 32 bit cuối cùng là địa chỉ IPv4 được thể hiện bằng ký hiệu thập phân. Vì vậy, 96 bit đầu tiên được biểu diễn dưới dạng thập lục phân với 32 bit cuối cùng chứa địa chỉ IPv4 theo ký hiệu thập phân. Biểu diễn như hình 2.17.



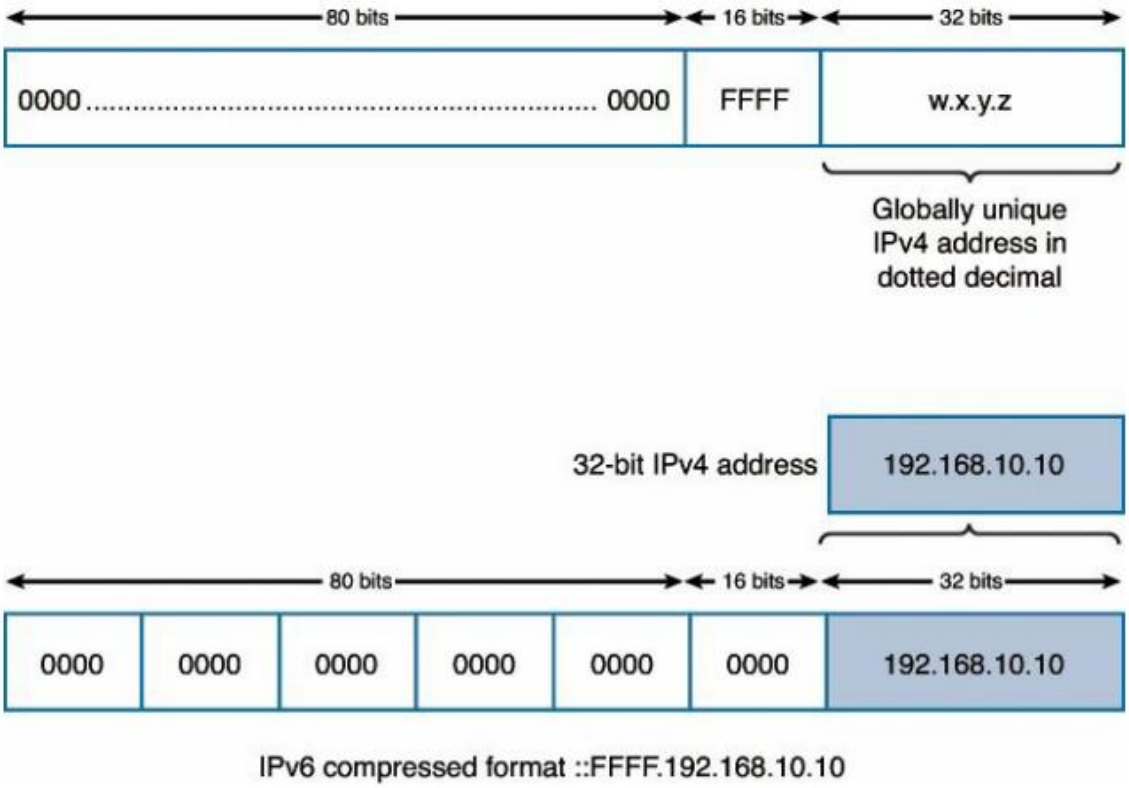
Hình 2.17: IPv4-Compatible IPv6 Address (Deprecated)

Địa chỉ IPv4 được sử dụng trong "IPv4-compatible IPv6 address", phải là địa chỉ unicast duy nhất trên toàn cầu. Địa chỉ "IPv4-compatible IPv6 address" hiếm khi được sử dụng và hiện không dùng nữa. Các cơ chế chuyển đổi IPv6 hiện tại không còn sử dụng loại địa chỉ này.

IPv4-Mapped IPv6 Addresses

IPv4-Mapped IPv6 Addresses tương tự như địa chỉ IPv4-Compatible IPv6 Addresses. IPv4-Mapped IPv6 Addresses được sử dụng để thể hiện địa chỉ của các thiết bị chỉ có IPv4. Một thiết bị IPv6 có thể sử dụng địa chỉ này để gửi một gói đến một thiết bị chỉ có IPv4.

Địa chỉ IPv4-mapped IPv6 address gần giống với địa chỉ IPv4-Mapped IPv6 Addresses, ngoại trừ phân đoạn 16bit trước địa chỉ IPv4 32bit là tất cả là 1 như hình 2.18



Hình 2.18: IPv4-Mapped IPv6 Addresses

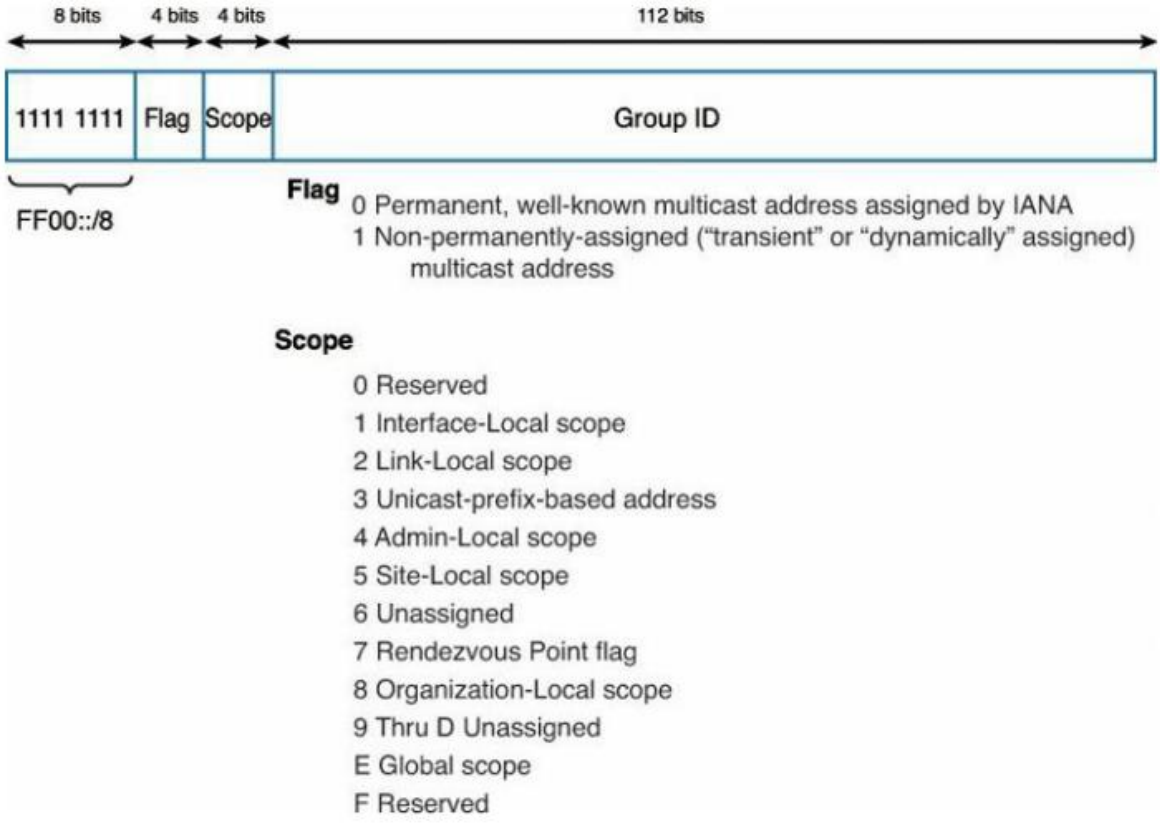
IPv4-Mapped IPv6 Addresses và địa chỉ IPv4-Compatible IPv6 Addresses được sử dụng bởi các cơ chế chuyển đổi trên máy chủ và bộ định tuyến để tạo đường hầm IPv4 cung cấp các gói IPv6 qua mạng IPv4. Các địa chỉ này và các cơ chế chuyển đổi sử dụng chúng sẽ được thảo luận chi tiết hơn trong chương chuyển đổi địa chỉ.

2.1.5.2 Multicast

Multicast là một kỹ thuật được sử dụng cho một thiết bị để gửi một gói tin đến nhiều đích cùng lúc (một-nhiều) trái ngược với một địa chỉ unicast, gửi một gói đến một đích (một-một). Nhiều điểm đến có thể là nhiều giao diện trên cùng một thiết bị nhưng chúng thường là các thiết bị khác nhau.

Một địa chỉ multicast IPv6 xác định một nhóm thiết bị được gọi là nhóm multicast. Nó là tương đương với IPv4 của 224.0.0.0/4. Một gói được gửi đến một nhóm multicast luôn có một địa chỉ nguồn unicast. Một địa chỉ multicast không bao giờ có thể là địa chỉ nguồn. Địa chỉ multicast IPv6 có tiền tố FF00 :: /8.

Cấu trúc của một địa chỉ multicast IPv6. 8bit đầu tiên là những bít 1 (FF), tiếp theo là Cờ 4 bit và Phạm vi 4 bit. Còn 112 bit tiếp theo đại diện cho ID nhóm (hình 2.19).



Hình 2.19: Multicast Address

Cờ (Flag): Chỉ thị kiểu địa chỉ Multicast, có 2 kiểu địa chỉ Multicast

Permanent (0): Đây là các địa chỉ multicast được chỉ định bởi Cơ quan cấp phát số và gán Internet (IANA), sẽ được thảo luận trong phần tiếp theo.

Nonpermanent (1): Đây là các địa chỉ multicast được gán một cách linh hoạt

Phạm vi (Scope): Phạm vi là trường 4bit được sử dụng để xác định phạm vi của gói Multicast. Các giá trị có thể cho phạm vi là:

0: Reserved

1: Interface-Local scope

2: Link-Local scope

3: Unicast-Prefix-based address

4: Admin-Local scope

5: Site-Local scope

6: Unassigned

7: Rendezvous Point flag

8: Organization-Local scope

9: Unassigned

A: Unassigned

B: Unassigned

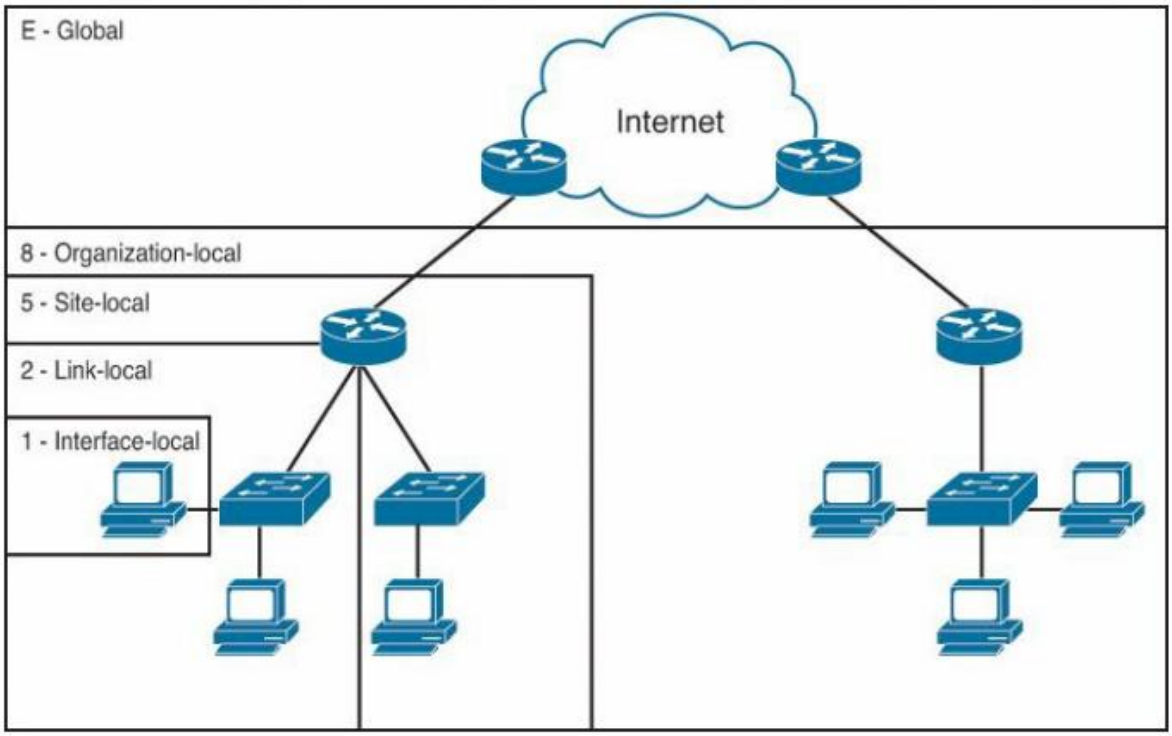
C: Unassigned

D: Unassigned

E: Global scope

F: Reserved

Trường scope cho phép các thiết bị xác định phạm vi của gói multicast cho phép các Router xác định mức độ lan truyền của nó. Điều này cải thiện hiệu quả bằng cách loại bỏ lưu lượng truy cập khỏi bên ngoài khu vực dự định (hình 2.20).



Hình 2.20: Multicast Scope

Assigned Multicast Addresses:

IPv6 Multicast Address Assignments đây là những địa chỉ multicast dành riêng cho các nhóm thiết bị được xác định trước. Các địa chỉ Assigned multicast addresses có tiền tố FF00:: / 8

Cùng một Group ID có thể có phạm vi khác nhau. Tùy thuộc vào phạm vi, một gói được gửi đến Group ID của tất cả các Router 0: 0: 0: 0: 0: 2 có thể được giới hạn trên một liên kết đơn (FF02:: 2) hoặc toàn bộ các Sites (FF05 :: 2)

Solicited-Node Multicast Addresses

Ngoài mọi địa chỉ unicast được gán cho một giao diện, một thiết bị cũng sẽ có một địa chỉ multicast đặc biệt được gọi là địa chỉ Solicited-Node Multicast Addresses. Các địa chỉ multicast này được tạo tự động bằng cách sử dụng ánh xạ địa chỉ unicast của thiết bị với prefix là prefix FF02:0:0:0:0:1:FF00::/104.

Không giống như IPv4, IPv6 không có địa chỉ quảng bá. Quá trình ARP của IPv4 sẽ gửi một quảng bá Lớp 2 tới tất cả các thiết bị trên mạng khi nó chỉ cố gắng kết nối tới một thiết bị duy nhất. Với mục đích là biến IPv6 thành một giao thức hiệu quả hơn. Không cần thiết bắt các thiết bị trong mạng đều phải xử lý bản tin ARP trong khi chỉ có 1 thiết bị trong mạng cần xử lý bản tin ARP đó. (Có MAC đó). IPv6's solicited-node multicast address cung cấp một giải pháp hiệu quả hơn. Bản tin IPv6's solicited-node multicast có thể đến mọi thiết bị trên liên kết nhưng không bắt các thiết bị đó phải xử lý nội dung của gói. Các IPv6's solicited-node multicast address được sử dụng cho hai cơ chế IPv6 thiết yếu, cả hai phần của giao thức Neighbor Discovery Protocol (NDP):

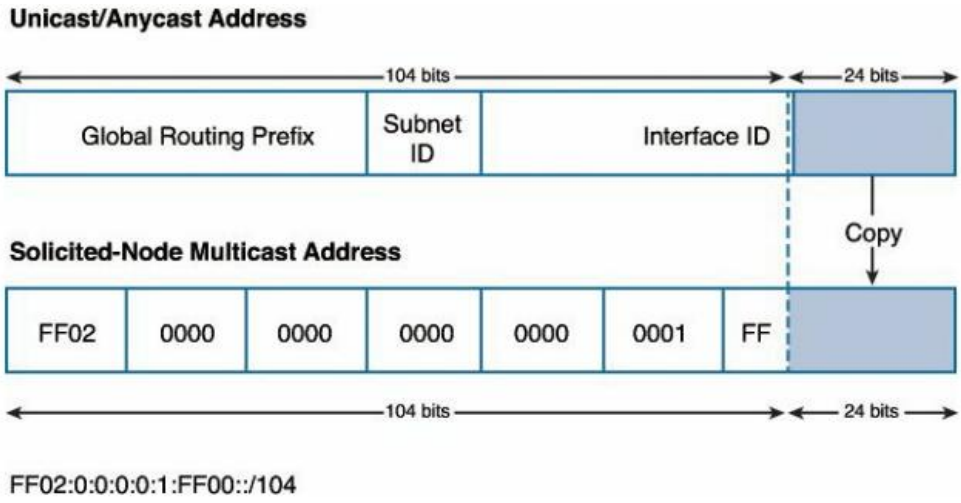
Phân giải địa chỉ (Address resolution)

Tương đương với ARP trong IPv4, một thiết bị IPv6 gửi thông báo Neighbor Solicitation đến Solicited-node multicast address để tìm hiểu địa chỉ lớp liên kết (thường là Ethernet address MAC) của một thiết bị trên cùng một liên kết. Thiết bị biết địa chỉ IPv6 của đích trên liên kết đó nhưng cần biết địa chỉ MAC.

Phát hiện địa chỉ trùng lặp Duplicate Address Detection (DAD)

DAD cho phép một thiết bị xác minh rằng địa chỉ unicast (hoặc anycast) của nó, được tạo bằng cách Tự động cấu hình địa chỉ không trạng thái (SLAAC), là duy

nhất trên liên kết. Một thông báo Neighbor Solicites được gửi đến thiết bị địa chỉ solicited-node của thiết bị để xác định xem có ai khác có cùng địa chỉ này không. Mô tả như hình 2.21



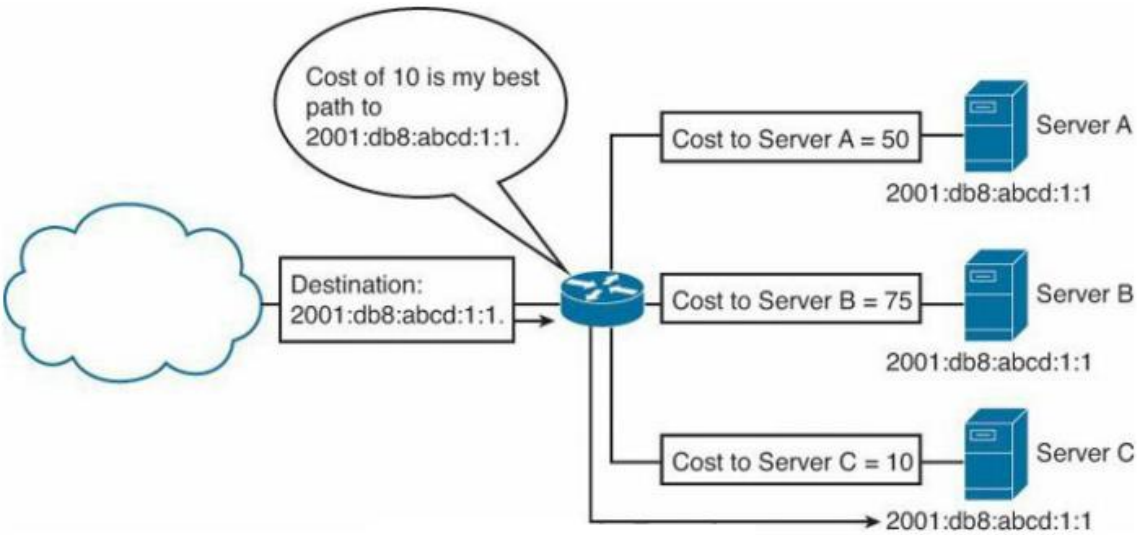
Hình 2.21: Địa chỉ Solicited-Node Multicast

Địa chỉ solicited-node multicast được tự động tạo cho mọi địa chỉ unicast trên thiết bị. Tiền tố solicited-node multicast FF02: 0: 0: 0: 0: 1: FF00 :: / 104 được gắn thêm 24 bit thứ tự thấp của địa chỉ unicast.

2.1.5.3 Địa chỉ Anycast

Địa chỉ anycast IPv6 là một địa chỉ có thể được gán cho nhiều giao diện (thường là các thiết bị khác nhau). Nói cách khác, nhiều thiết bị có thể có cùng một địa chỉ anycast. Một gói tin được gửi đến một địa chỉ anycast được định tuyến đến giao diện gần nhất có thể có địa chỉ đó, theo bảng định tuyến của bộ định tuyến. Địa chỉ Anycast có trong cả IPv4 và IPv6, Anycast có ý nghĩa và lợi ích khi sử dụng cho các dịch vụ như DNS và HTTP nhưng vẫn chưa phổ biến triển khai như thiết kế mong muốn.

Không có prefix đặc biệt cho một địa chỉ IPv6 anycast. Địa chỉ anycast IPv6 sử dụng cùng dải địa chỉ với địa chỉ unicast toàn cầu. Mỗi thiết bị tham gia sẽ được cấu hình để có cùng một địa chỉ anycast, ví dụ như trong hình 2.22.



Hình 2.22: Ví dụ về sử dụng địa chỉ Anycast

2.2 Giao thức ICMPv6 và giao thức Neighbor Discovery Protocol

ICMP là một trong những giao thức cốt lõi của bộ giao thức TCP / IP. Nó được sử dụng bởi các hệ điều hành để gửi tin nhắn giữa các thiết bị. Các loại thông báo có thể là thông báo thông tin hoặc thông báo lỗi, chẳng hạn như Echo Request cho lệnh ping hoặc thông báo cho người gửi rằng Router không thể chuyển tiếp gói. ICMP được sử dụng với các ứng dụng như ping và traceroute để kiểm tra kết nối mạng giữa hai thiết bị.

ICMPv6 được mô tả trong RFC 4443. Giao thức tin nhắn điều khiển Internet (ICMPv6) phiên bản 6 (IPv6). ICMPv6 mạnh hơn ICMPv4 rất nhiều, chứa các chức năng và cải tiến mới.

Phần này trình bày định dạng thông báo chung cho ICMPv6 bằng cách sử dụng các trường Type và Code tương tự được tìm thấy trong ICMPv4. Nó kiểm tra hai loại thông báo ICMPv6, thông báo lỗi và thông báo thông tin.

Thông báo lỗi ICMPv6 (Error messages)

Destination Unreachable

Packet Too Big

Time Exceeded

Parameter Problem

Thông báo thông tin sử dụng cho lệnh Ping (Information messages for Ping)

Echo Request

Echo Reply

Thông báo thông tin sử dụng cho MLD (Information message for Multicast Listener Discovery)

Multicast Listener Query

Multicast Listener Report

Multicast Listener Done

Thông báo thông tin sử dụng cho ND (Information messages for Neighbor Discovery)

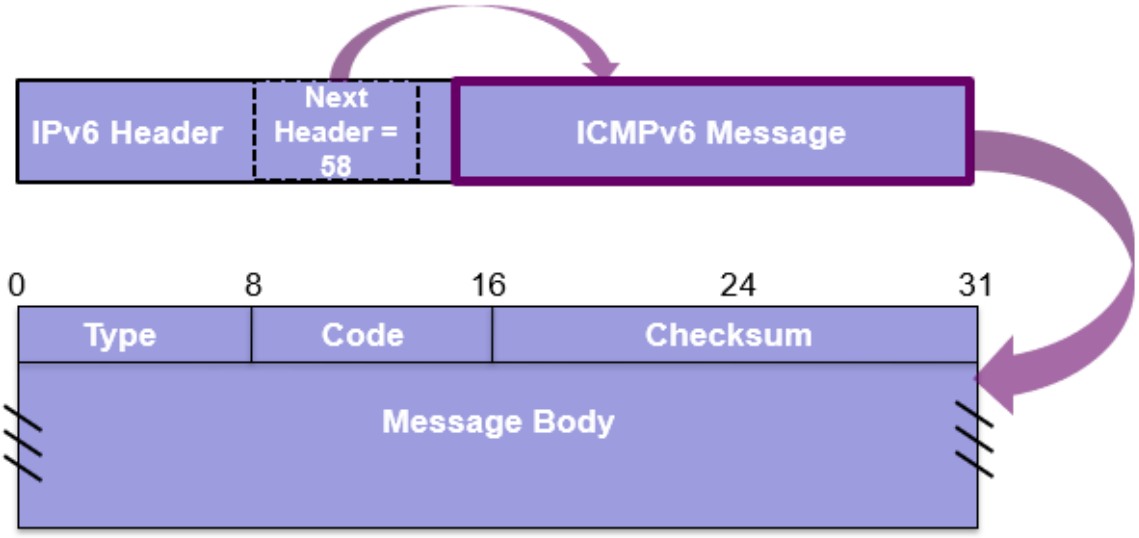
Router Solicitation Message

Router Advertisement Message

Neighbor Solicitation Message

Neighbor Advertisement Message

Redirect Message



Hình 2.23: Khuôn dạng tổng quát của ICMPv6

Hình 2.23 mô tả định dạng chung của bản tin ICMPv6 tương tự như ICMPv4. Một tiêu đề IPv6 có giá trị Next Header là 58 sẽ là giao thức ICMPv6. (Trong IPv4, trường Giao thức được đặt thành 1 để chỉ ra thông báo ICMPv4). Tiêu

đề trước không nhất thiết phải là tiêu đề main IPv6. Nó cũng có thể là một trong những IPv6 extension headers

Ba trường trong IPv6 massage như sau:

Type (8 bit): Cho biết loại tin nhắn ICMPv6, chẳng hạn như Echo Request, Destination Unreachable, hoặc Packet Too Big.

Code (8 bit): Cung cấp độ chi tiết hơn cho trường Type. Ý nghĩa của nó sẽ phụ thuộc vào loại tin nhắn. Ví dụ: nếu loại thông báo là Destination Unreachable, trường Code sẽ đưa ra lý do cụ thể tại sao gói không thể đến đích, ví dụ: không thể truy cập máy chủ hoặc bộ định tuyến không có tuyến đến máy chủ trong bảng định tuyến của nó.

Checksum (16 bit): Được sử dụng để phát hiện lỗi dữ liệu trong thông điệp ICMPv6 và các phần của tiêu đề IPv6.

Trường Type được sử dụng để nhóm các ICMPv6 messages thành hai classes:

Error messages (Type = 0 đến 127)

Information messages (Type = 128 đến 255)

Thông báo lỗi được xác định bởi high-order bit 0 (0xxxxxx) trong trường Loại thông báo (Type). Điều này dẫn đến một thông báo lỗi có giá trị Loại từ 0 đến 127. Do đó, thông báo thông tin có bit high-order 1 sẽ có giá trị Loại từ 128 đến 255.

Error messages: Thông báo cho thiết bị về lý do tại sao gói tin được gửi không thể được gửi.

ICMP informational messages: Không được sử dụng để báo cáo lỗi nhưng cung cấp thông tin cần thiết cho các chức năng kiểm tra, chẩn đoán và hỗ trợ khác nhau. Hai ICMP informational messages phổ biến được tìm thấy trong cả ICMP cho IPv4 và IPv6 là các tin nhắn Echo Request và Echo Reply được sử dụng bởi lệnh ping.

2.2.1 ICMP Error Messages

Các thiết bị lớp 3, chẳng hạn như máy chủ và bộ định tuyến, sử dụng ICMP Error Messages để thông báo cho người gửi về lý do tại sao một gói không thể được gửi

Có bốn loại thông báo lỗi:

Không thể truy cập đích (Destination Unreachable)

Gói quá lớn (Packet too Big)

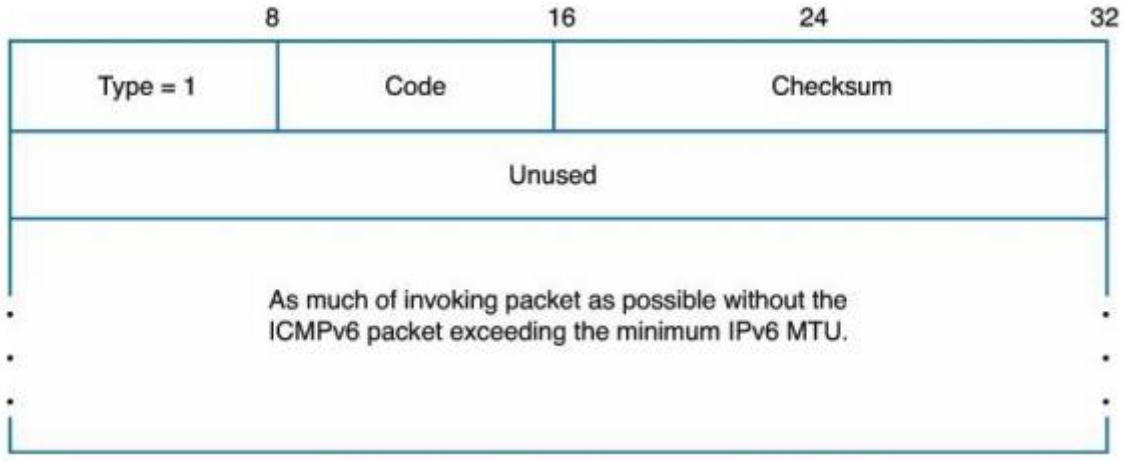
Quá thời gian (Time Exceeded)

Vấn đề về tham số (Parametter Problem)

2.2.1.1 Destination Unreachable

Một tin nhắn ICMPv6 Destination Unreachable được gửi khi một gói không thể được gửi đến đích vì lý do khác hơn là tắc nghẽn. Các thông báo phản hồi này được sử dụng để giúp cung cấp một số thông tin hữu ích cho người gửi về lý do tại sao. Một bộ định tuyến hoặc tường lửa thường tạo ra các thông báo Destination Unreachable messages.

Khuôn dạng bản tin ICMPv6 Destination Unreachable như sau, trong đó trường Type = 1 mô tả như hình 2.24.



Hình 2.24: ICMPv6 Destination Unreachable Message

Có một số lý do tại sao unreachable. Trường Code được sử dụng để cung cấp thông tin chi tiết hơn về lý do gói không được gửi. Có 7 Code:

- *Code = 0*, No route to destination (Không có tuyến đến đích): Không thể gửi gói tin vì bộ định tuyến không có tuyến đến đích này. Điều này chỉ có thể xảy ra nếu bộ định tuyến không có tuyến mặc định trong bảng định tuyến. Thông báo này tương đương với thông báo Network Unreachable message trong ICMPv4.

- *Code* = 1, Communications with destination administratively prohibited: Gói bị chặn do danh sách kiểm soát truy cập hoặc lọc gói khác
- *Code = 2*, Beyond scope of source address: Thông báo lỗi này được tạo khi địa chỉ nguồn là địa chỉ link-local address và địa chỉ đích là địa chỉ global unicast address.
- Code = 3, Address unreachable: Thông báo lỗi này cho biết đã xảy ra sự cố khi gửi gói vì không thể truy cập máy chủ được chỉ định trong địa chỉ đích. Điều này có thể xảy ra nếu địa chỉ đích không thể được phân giải thành địa chỉ liên kết dữ liệu tương ứng (địa chỉ MAC trên mạng LAN) hoặc địa chỉ đích không chính xác. Điều này tương đương với tin nhắn Host Unreachable trong ICMPv4.
- *Code = 4*, Port unreachable: Thông báo lỗi này xảy ra do cổng đích được chỉ định trong tiêu đề TCP hoặc UDP không tồn tại hoặc đích không nghe trên cổng đó. Ví dụ: nếu một gói được gửi với cổng đích TCP 80 nhưng máy chủ nhận không chạy dịch vụ web HTTP, thông báo Port unreachable sẽ được truyền đi.
- *Code = 5*, Source address failed ingress/egress policy: Thông báo lỗi này cho biết gói có địa chỉ nguồn này bị chặn do danh sách kiểm soát truy cập hoặc lọc gói khác. Code 5 là tập con của Code 1.
- *Code = 6*, Reject route to destination: Thông báo lỗi này sẽ xảy ra khi các gói có prefix cụ thể bị chặn bởi danh sách kiểm soát truy cập hoặc lọc gói khác. Code 6 là tập con của Code 1.

2.2.1.2 Packet Too Big

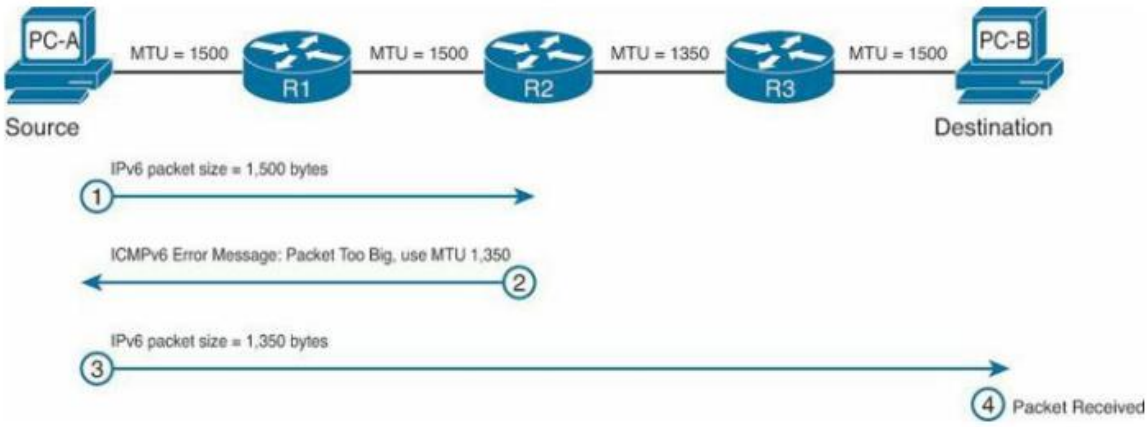
Một thay đổi đáng kể đối với IPv6 có liên quan đến phân mảnh và sắp xếp lại gói. Trong IPv4, các bộ định tuyến có thể phân mảnh một gói khi đơn vị truyền tối đa (MTU) của liên kết đi nhỏ hơn kích thước của gói. Thiết bị đích sẽ chịu trách nhiệm lắp ráp lại các gói bị phân mảnh. Điều này là không hiệu quả. IPv6 đã loại bỏ tác vụ này khỏi bộ định tuyến, chỉ cho phép nguồn của gói thực hiện phân mảnh. Khi bộ định tuyến IPv6 nhận được gói lớn hơn MTU của giao diện đầu ra, bộ định

tuyến sẽ loại bỏ gói đó và gửi thông báo Gói quá lớn của ICMPv6 về nguồn. Thông báo Packet Too Big bao gồm kích thước MTU (số byte) của liên kết theo để nguồn có thể thay đổi kích thước của gói để truyền lại.

Thông báo ICMPv6 Packet Too Big có Type = 2 và Code = 0. MTU là đơn vị truyền tối đa của liên kết hop tiếp theo. Thông báo ICMPv6 Packet Too Big này cũng được sử dụng như một phần của Path MTU Discovery

Path MTU Discovery

Path MTU Discovery được định nghĩa trong RFC 1981, Path MTU Discovery cho IPv6. Khi một thiết bị có số lượng gói lớn để truyền, tốt nhất là các gói này càng lớn càng tốt, cho phép ít gói hơn (Byte to thì số lượng gói ít đi). Điều này đòi hỏi thiết bị phải biết MTU liên kết tối thiểu (MTU nhỏ nhất) của tất cả các liên kết trong đường dẫn đến đích. Điều này cho phép người gửi truyền kích thước gói lớn nhất có thể mà không có nguy cơ bộ định tuyến làm rơi gói dọc theo đường dẫn vì MTU của liên kết gửi đi của nó quá nhỏ. Kích thước của gói này được gọi là Đường dẫn MTU (PMTU). Mô tả như hình 2.25.



Hình 2.25: Path MTU Discovery

Bước 1. Một thiết bị giả định rằng kích thước Đường dẫn MTU (PMTU) của gói bằng với MTU của liên kết gửi đi của nó đến bộ định tuyến bước đầu tiên.

Bước 2. Nếu kích thước gói lớn hơn MTU của bộ định tuyến liên kết hop tiếp theo, gói sẽ bị hủy và thông báo Gói quá lớn của ICMPv6 được gửi trở lại nguồn, bao gồm trong tin nhắn là MTU của liên kết hop tiếp theo.

Bước 3. Thiết bị nguồn sử dụng thông tin trong thông báo Packet Too Big message để giảm kích thước gói phù hợp với MTU có trong message. Thiết bị nguồn sẽ gửi các gói tiếp theo bằng MTU nhỏ hơn này.

Bước 4. Quá trình này của các bộ định tuyến gửi các gói tin ICMPv6 Packet Too Big và nguồn giảm kích thước gói tiếp tục cho đến khi gói đến đích.

Bởi vì đường dẫn từ một nguồn cụ thể đến một đích nhất định có thể thay đổi, nên PMTU cũng vậy. Vì vậy, có thể các thiết bị nguồn có thể phải tự động sửa đổi kích thước PMTU của các gói của chúng. Các thiết bị không bắt buộc phải thực hiện Path MTU, nhưng nó được khuyến nghị trong RFC 4443.

2.2.1.3 Time Exceeded

Trước khi bộ định tuyến chuyển tiếp gói IPv6, nó sẽ giảm trường Hop Limit đi 1. Điều này giống hệt với trường TTL trong IPv4 nhưng với tên phản ánh rõ hơn chức năng của nó. Nếu Hop Limit dẫn đến 0, gói bị hủy và thông báo ICMPv6 Time Exceeded được gửi đến nguồn. Đây là một cơ chế trong cả IPv4 và IPv6 để đảm bảo rằng các gói không bị chuyển vô tận trên khắp các mạng.

2.2.1.4 Parameter Problem

Thông báo lỗi tham số ICMPv6 được tạo khi thiết bị xử lý gói tìm thấy sự cố với trường trong tiêu đề IPv6 chính hoặc tiêu đề mở rộng. Điều này có nghĩa là thiết bị nhận đã không hiểu thông tin trong tiêu đề IPv6 và phải loại bỏ nó. Điều này xảy ra nếu các thông tin trong tiêu đề mở rộng không hợp lệ hoặc nếu tiêu đề mở rộng không được thiết bị này hỗ trợ.

2.2.2 ICMP Informational Messages

Các thiết bị sử dụng ICMPv6 error messages để cho người gửi biết lý do tại sao một gói không thể được gửi. ICMPv6 informational messages được sử dụng để giúp các thiết bị khám phá và chia sẻ thông tin với nhau. Có một số loại messages thông tin sau:

Sử dụng bởi ping command (RFC 4443):

Echo Request

Echo Reply

Sử dụng cho Multicast Listener Discovery (RFC 2710 and RFC 3810):

Multicast Listener Query

Multicast Listener Report

Multicast Listener Done

Sử dụng cho Neighbor Discovery (RFC 4861):

Router Solicitation message

Router Advertisement message

Neighbor Solicitation message

Neighbor Advertisement message

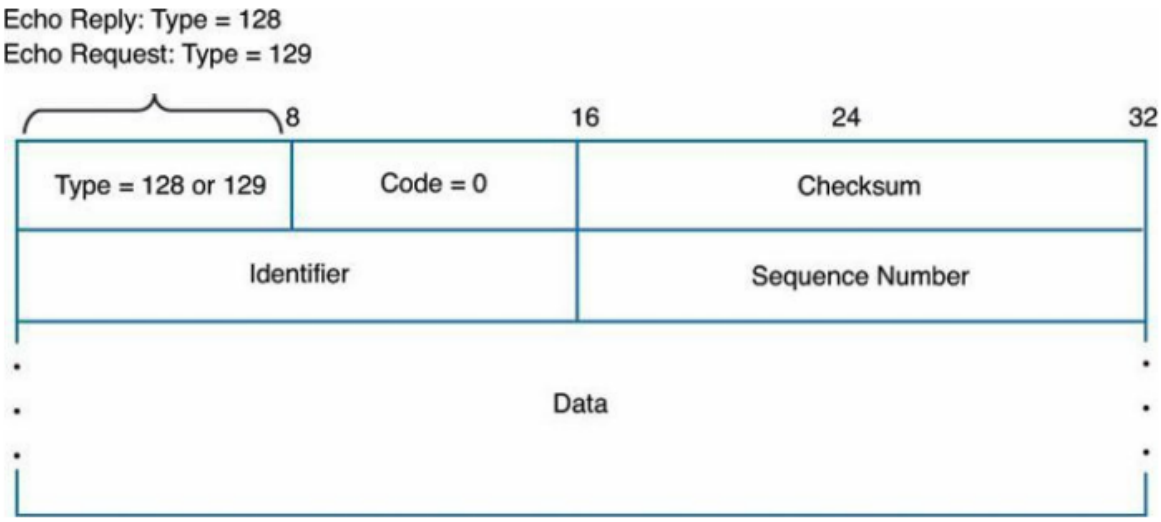
Redirect message

2.2.2.1 Echo Request and Echo Reply

Là hai thông điệp ICMP được sử dụng bởi ping, một tiện ích TCP/IP rất phổ biến. Ping thường được sử dụng để kiểm tra kết nối lớp mạng giữa hai thiết bị.

Một thiết bị gửi Echo Request để nhắc đích đến trả về Echo Reply để xác minh kết nối lớp mạng. Nếu người gửi không nhận được Echo Reply tương ứng, điều đó không nhất thiết có nghĩa là không thể đến đích. Có thể các thiết bị mạng nội bộ trong đường dẫn đang loại bỏ Echo Request hoặc Echo Reply. Cũng có thể là đích đến không chấp nhận hoặc trả lời các Echo Request.

Cấu trúc của Echo Request và Echo Reply messages giống hệt nhau ngoại trừ giá trị trong trường Type. Echo Request có trường Type = 128, trong khi Echo Reply = 129. Trường Code luôn được đặt thành 0, mô tả như hình 2.26



Hình 2.26: ICMPv6 Echo Request and Echo Reply Messages

Các trường trong tiêu đề ICMPv6

Type: Trong cho Request, Type = 128 và trong Echo Reply, Type = 129

Code: Bị người nhận bỏ qua, Code luôn là 0 cho cả Echo Request và Echo Reply

Checksum: Tổng kiểm tra xác thực tiêu đề ICMPv6

Identifier: Trường này được sử dụng để giúp khớp Echo Request và Echo Reply tương ứng của chúng

Sequence: Trường này cũng giúp khớp với Echo Request và Echo Reply, cung cấp độ chi tiết hơn một chút. Echo Request được tạo với số thứ tự và Echo Reply tương ứng của nó bao gồm cùng số thứ tự. Echo Request tiếp theo tăng số thứ tự lên 1 và người nhận sử dụng cùng giá trị đó trong Trả lời Echo Reply của nó.

Data: Echo Request thêm 0 hoặc nhiều byte dữ liệu tùy ý. Thiết bị nhận sao chép dữ liệu này vào Echo Reply và trả lại.

2.2.2.2 Multicast Listener Discovery

Địa chỉ Multicast được sử dụng để gửi một gói hoặc nhiều khả năng là một luồng gói đến nhiều thiết bị cùng một lúc. Điều này hiệu quả hơn nhiều so với việc sao chép các gói này dưới dạng truyền phát unicast riêng biệt cho mỗi đích.

Trong IPv4, việc quản lý các multicast groups được thực hiện bằng cách sử dụng Giao thức quản lý nhóm Internet (IGMP). Các host sử dụng IGMP để tự động đăng ký trong một nhóm multicast groups trên một mạng cụ thể. Điều này được

thực hiện bằng cách gửi các tin nhắn IGMP đến Router multicast groups cục bộ của chúng, thông báo cho Router về địa chỉ Multicast mà nó muốn nhận lưu lượng. Router được cấu hình lăng nghe bản tin IGMP từ Host. Router định kỳ gửi các truy vấn để khám phá multicast groups nào vẫn hoạt động, nói cách khác, các nhóm có host vẫn muốn nhận lưu lượng truy cập cho địa chỉ multicast đó. Điều này cho phép Router xác định địa chỉ Multicast nào không hoạt động và không còn host yêu cầu lưu lượng đó. Với phiên bản đầu tiên của IGMP, không có cách nào để một host chủ động rời khỏi một multicast groups, thông báo cho Router rằng nó muốn rời khỏi nhóm đó. IGMPv2 bao gồm một cơ chế dời nhóm để host thông báo cho Router rằng nó đã rút khỏi nhóm Multicast đó.

IPv6 sử dụng ICMPv6 Multicast Listener Discovery (MLD) cho cùng các dịch vụ, dựa trên chức năng của nó trên IGMPv2. Vì vậy, nếu bạn đã quen thuộc với IGMP, MLD rất giống nhau. MLD được định nghĩa trong RFC 2710.

Multicast Listener Discovery cho IPv6. MLDv2 đã được xác định trong RFC 3810, Multicast Listener Discovery Phiên bản 2 (MLDv2) cho IPv6. Dựa trên IGMPv3, MLDv2 mở rộng phiên bản MLD đầu tiên để hỗ trợ Nguồn phát multicast cụ thể (SSM Source Specific Multicast) và tương thích ngược với MLDv1. SSM cung cấp khả năng cho một host yêu cầu các gói multicast từ một địa chỉ nguồn cụ thể. MLDv2 là phiên bản mặc định cho Cisco IOS.

Có ba loại thông báo MLD:

Multicast Listener Query (Type = decimal 130): Router truyền định kỳ các thông báo truy vấn thành viên để xác định multicast groups nào vẫn có thành viên trên các mạng được gắn trực tiếp vào Router. Có hai kiểu con của Multicast Listener Query

General Query:

Được sử dụng để tìm hiểu địa chỉ multicast nào có người nghe trên một liên kết. General Query được gửi đến địa chỉ multicast tất cả các nút phạm vi liên kết FF02 :: 1, đến tất cả các thiết bị IPv6 trên liên kết.

Multicast-Address-Specific Query:

Được sử dụng để tìm hiểu xem một địa chỉ multicast cụ thể (multicast group) có bất kỳ trình nghe nào trên một liên kết hay không.

Multicast Listener Report (Type = decimal 131): Thông báo này được gửi bởi người nghe để đăng ký một multicast group. Người nghe có thể gửi tin nhắn này để đáp lại một query hoặc có thể gửi mà không cần chờ một truy vấn từ Router.

Nếu để trả lời một truy vấn, chỉ một thành viên của multicast group cần gửi Multicast Listener Report. Trong MLDv1, các Multicast Listener Report này được gửi đến địa chỉ multicast được Report. Điều này đã được thay đổi trong MLDv2, Multicast Listener Report được gửi đến một địa chỉ multicast đặc biệt FF02 :: 16, tất cả các Router có dịch vụ MLDv2

Multicast Listener Done (Type = decimal 132): Khi người nghe không còn muốn nhận lưu lượng truy cập cho một multicast group cụ thể, nó sẽ gửi một thông báo Multicast Listener Done để thông báo cho Router rằng nó sẽ rời khỏi nhóm multicast đó. Listener Done messages được gửi đến địa chỉ multicast của bộ định tuyến trên liên kết (FF02 :: 2).

2.2.2.3 Neighbor Discovery Protocol

(ND hoặc NDP) được định nghĩa trong RFC 4861, Neighbor Discovery bao gồm các quy trình tương tự từ IPv4 như ARP, ICMP Router Discovery và Redirect, nhưng có sự khác biệt đáng kể. ND cũng bao gồm chức năng mới như Phát hiện địa chỉ trùng lặp (DAD) và Phát hiện không thể truy cập hàng xóm (NUD). NDP đóng vai trò quan trọng trong việc tự động cấu hình địa chỉ IPv6.

Các thiết bị (hosts và routers) sử dụng Neighbor Discovery vì các lý do sau:

Tự động cấu hình địa chỉ không trạng thái (SLAAC), để tự động xác định tiền tố mạng, default gateway và thông tin cấu hình khác (DNS ..).

Để xác định xem một địa chỉ link-local unicast hoặc global unicast mà nó sắp sử dụng đã được sử dụng bởi một thiết bị khác hay chưa (DAD).

Để xác định địa chỉ liên kết dữ liệu Lớp 2 (thường là Ethernet) của thiết bị trên mạng.

Để theo dõi những hàng xóm nào có thể tiếp cận.

Khi bộ định tuyến hoặc đường dẫn đến bộ định tuyến bị lỗi, Host sẽ chủ động tìm kiếm các chức năng thay thế.

Có năm tin nhắn ICMPv6 được Neighbor Discovery sử dụng:

Router Solicitation message

Router Advertisement message

Neighbor Solicitation message

Neighbor Advertisement message

Redirect message

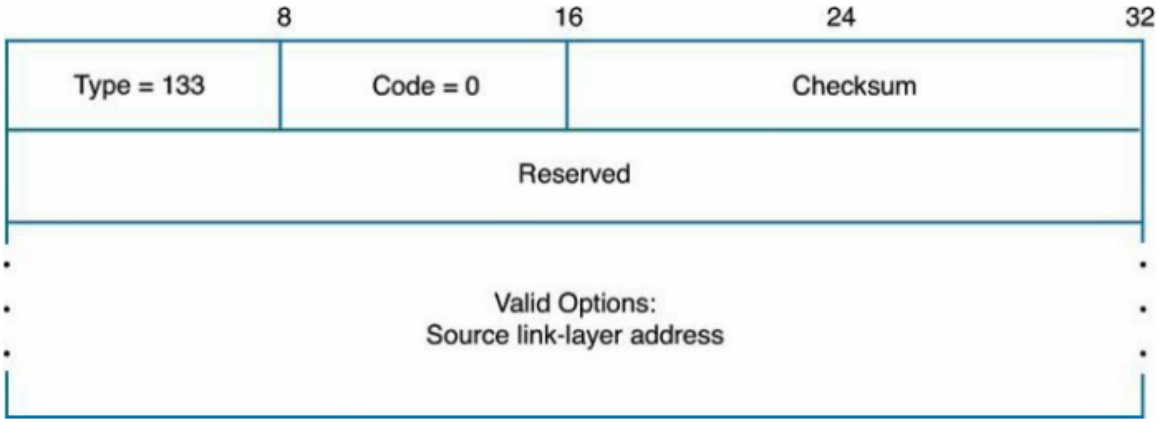
Phần sau đây kiểm tra từng loại thông báo và các phương thức được sử dụng để xác định tiền tố, phân giải địa chỉ và Phát hiện địa chỉ trùng lặp.

Router Solicitation và Router Advertisement Messages

Thiết bị IPv6 có thể được tách thành hai loại, Router và Host. Messages Router Solicitation và Router Advertisement là giao tiếp giữa Host và Router. Router gửi định kỳ tin nhắn Router Advertisement hoặc trả lời khi nhận được massage Router Solicitation từ một Host trên liên kết.

Một Host gửi một massage Router Solicitation (RS) khi nó cần prefix, prefix length, default gateway và các thông tin khác cho việc tự động cấu hình địa chỉ không trạng thái (SLAAC). Điều này thường xảy ra khi một Host vừa được bật nguồn và được cấu hình để tự động lấy địa chỉ IP. SLAAC có thể sử dụng định dạng EUI-64 hoặc tạo ngẫu nhiên interface ID 64bit của địa chỉ unicast của nó. Host nhận được prefix và prefix length từ message Router Advertisement (RA). Host có thể đợi bản tin RA định kỳ tiếp theo hoặc gửi bản tin RS để Router sẽ gửi RA khi nhận được RS.

Các trường trong ICMPv6 ND Router Solicitation Message như trong hình 2.27.



Hình 2.27: ICMPv6 ND Router Solicitation Message

IPv6 header:

Source address: Đây là địa chỉ IPv6 đã được gán cho giao diện gửi hoặc địa chỉ không xác định nếu không có địa chỉ nào được chỉ định. Nhớ rằng, link-local addresses được thiết bị tạo ngẫu nhiên hoặc tự động bằng tiền tố FE80 :: / 10 và tạo Interface ID bằng EUI-64.

Destination address: Địa chỉ đích thường là địa chỉ all-routers multicast address FF02:: 2.

ICMPv6 fields:

Type: Trường Loại được đặt thành 133, cho biết đây là bản tin Router Solicitation message

Code: Mã được đặt thành 0 và bị người nhận bỏ qua

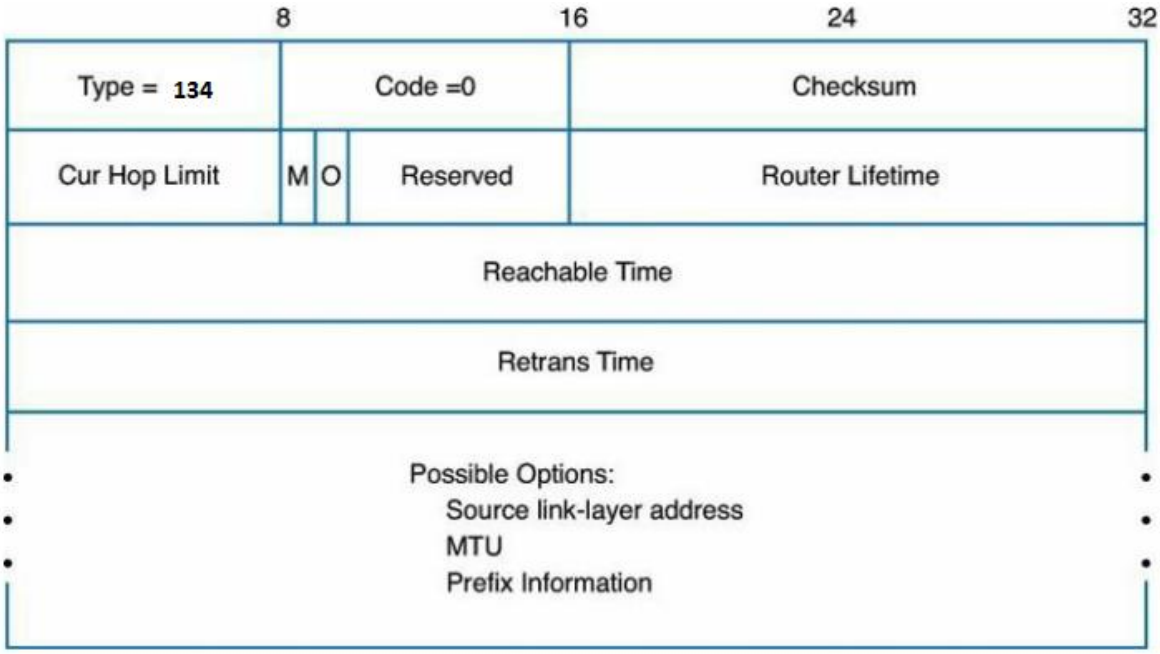
Checksum: Đây là để kiểm tra tiêu đề ICMPv6

Reserved: Trường này không được sử dụng

Source Link Layer Address: Đây là địa chỉ lớp liên kết lớp 2 (hoặc lớp liên kết dữ liệu) của người gửi

Router Advertisement message được gửi định kỳ hoặc phản hồi lại một Router Solicitation message. Nó được sử dụng để cung cấp cho Host địa chỉ và thông tin cấu hình khác và là một phần quan trọng của Tự động cấu hình địa chỉ không trạng thái (SLAAC)

Các trường trong ICMPv6 ND Router Advertisement Message như trong hình 2.28



Hình 2.28: ICMPv6 ND Router Advertisement Message

IPv6 header:

Source address: Địa chỉ nguồn là địa chỉ liên kết cục bộ của bộ định tuyến được gán cho giao diện.

Destination address: Địa chỉ đích thường là địa chỉ multicast all-nodes multicast address FF02 :: 1.

Hop limit: Giới hạn hop luôn được đặt thành 255.

ICMPv6 fields:

Type: Trường Loại được đặt thành 134, cho biết đây là thông báo Router Advertisement message.

Code: Mã được đặt thành 0 và bị người nhận bỏ qua.

Checksum: Để kiểm tra tiêu đề ICMPv6.

Cur Hop Limit: Đây là số mà bộ định tuyến khuyến nghị cho các Host trên mạng sử dụng làm trường Giới hạn Hop cho các gói IP của chúng. Giá trị 0 có nghĩa là bộ định tuyến không đề xuất giới hạn hop và Host nên xác định giá trị của chính nó

M Flag: Đây là cờ Cấu hình địa chỉ được quản lý. Khi được đặt thành 0, các Host trên mạng sử dụng Tự động cấu hình địa chỉ không trạng thái (SLAAC). Khi được đặt thành 1, điều này sẽ thông báo cho Host sử dụng cấu hình trạng thái (DHCPv6).

O Flag: Đây là cờ Cấu hình khác. Khi được đặt thành 0, không có thông tin bổ sung nào từ máy chủ DHCPv6. Khi được đặt thành 1, thông báo này cho Host biết rằng thông tin bổ sung sẽ lấy từ máy chủ DHCPv6, chẳng hạn như thông tin liên quan đến DNS.

Bên cạnh cờ M và cờ O, Quảng cáo Bộ định tuyến cũng chứa cờ cấu hình địa chỉ tự động hoặc cờ A. Cờ A cho biết liệu Prefix trong RA có thể được sử dụng cho SLAAC hay không. Theo mặc định, cờ A được đặt thành 1, cho phép sử dụng Prefix cho SLAAC.

Reserved: Không được sử dụng.

Router Lifetime: Thông báo cho Host thời lượng, tính bằng giây, rằng Router sẽ được sử dụng làm default gateway. Time life = 0 chỉ ra rằng Router không phải là default gateway. Host làm mới bộ đếm thời gian của chính nó mỗi khi nhận được Router Advertisement.

Reachable Time (Thời gian có thể truy cập): Cho biết thời gian, tính bằng mili giây, có thể truy cập sau khi nhận được xác nhận khả năng tiếp cận. Được sử dụng bởi Neighbor Unreachability Detection (NUD). Giá trị 0 nghĩa là Router không chỉ định giá trị

Retrans Timer (Hẹn giờ truyền lại): Thông báo cho Host khoảng thời gian, tính bằng mili giây, rằng nó sẽ đợi trước khi truyền lại tin nhắn Neighbor Solicitation. Điều này được sử dụng trong address resolution và Neighbor Unreachability Detection (NUD).

Source Link Layer Address: Đây là địa chỉ lớp liên kết lớp 2 (hoặc lớp liên kết dữ liệu) của người gửi, địa chỉ MAC Ethernet của người gửi.

MTU: Để thông báo cho Host đơn vị truyền tối đa (MTU) cho mạng. Các Host sử dụng thông tin này để tối đa hóa kích thước của gói IPv6.

Prefix Information: Thông báo cho Host biết prefix (phần mạng của địa chỉ) và prefix length (tương tự mặt nạ mạng con IPv4) của mạng là gì.

Neighbor Solicitation và Neighbor Advertisement Messages

Neighbor Solicitation và Neighbor Advertisement Messages là hai giao thức sử dụng trong ICMPv6 Neighbor Discovery. Các tin nhắn này được một thiết bị sử dụng để yêu cầu địa chỉ Lớp 2, thông tin link layer address từ một thiết bị khác trên cùng mạng hoặc để cung cấp thông tin này cho thiết bị yêu cầu. Neighbor Solicitation và Neighbor Advertisement Messages là một phần của ba quy trình quan trọng:

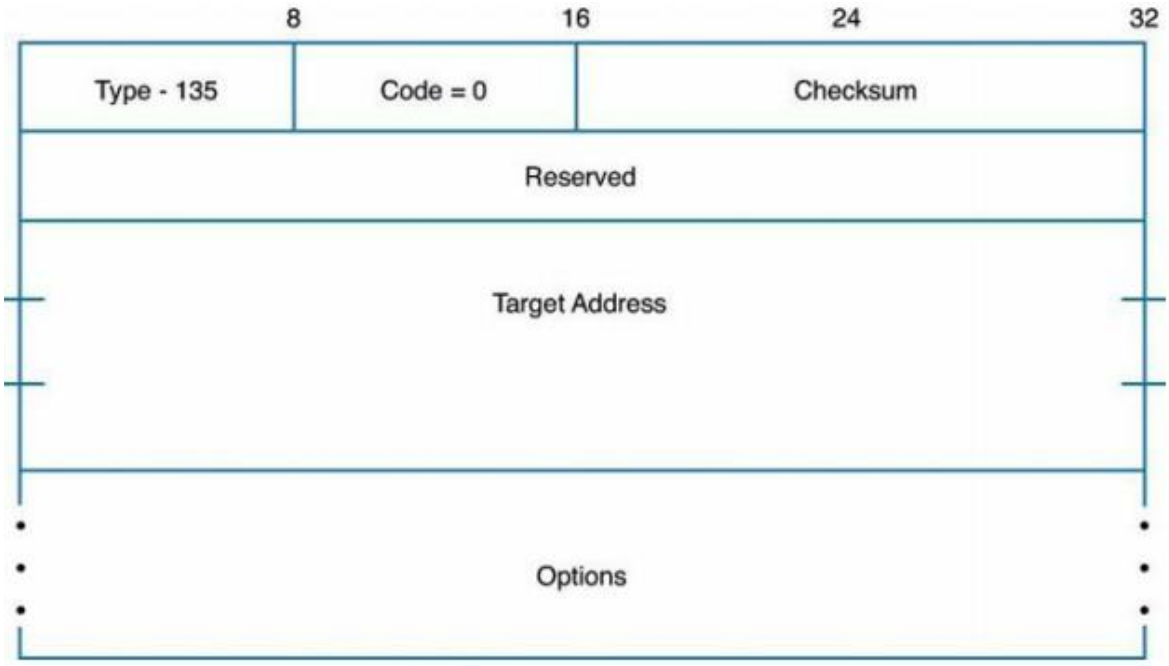
Address resolution

Duplicate Address Detection (DAD)

Neighbor Unreachability Detection (NUD)

Neighbor Solicitation và Neighbor Advertisement messages rất giống với ARP Requests và ARP Replies trong IPv4. Neighbor Solicitations được gửi để yêu cầu Lớp 2, địa chỉ lớp liên kết của thiết bị đích trong khi cũng cung cấp địa chỉ lớp liên kết của chính nó cho mục tiêu. Các địa chỉ lớp liên kết này thường là các địa chỉ MAC Ethernet.

Neighbor Advertisements được truyền đi để đáp lại Neighbor Solicitations và cũng được gửi khi nó cần thiết để truyền bá thông tin mới một cách nhanh chóng. Hãy cùng xem các định dạng tin nhắn Neighbor Solicitation and Neighbor Advertising và xem chúng được sử dụng như thế nào với các quy trình được đề cập trước đó.



Hình 2.29: ICMPv6 ND Neighbor Solicitation Message

IPv6 header:

Source address: Địa chỉ IPv6 đã được gán cho giao diện gửi hoặc, nếu thông báo này được gửi như một phần của Duplicate Address Detection, địa chỉ unicast không xác định

Destination address: Hoặc là địa chỉ solicited node multicast address với chính mục tiêu hoặc địa chỉ đích

Hop limit: Luôn được đặt thành 255

ICMPv6 fields:

Type: Đặt thành 135, cho biết đây là tin nhắn Neighbor Solicitation

Code: Đặt thành 0 và bị người nhận bỏ qua.

Checksum: Kiểm tra tiêu đề ICMPv6.

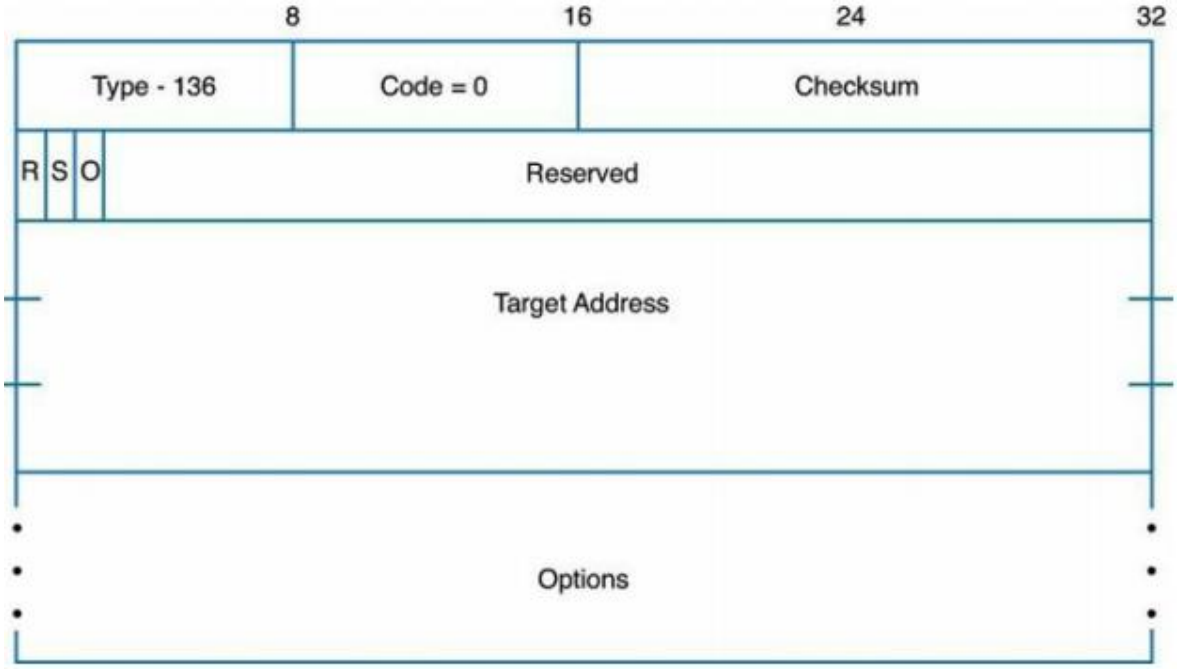
Reserved: Trường này không được sử dụng.

Target Address: Địa chỉ IPv6 của đích, thiết bị mà người gửi biết địa chỉ IPv6 nhưng không phải là địa chỉ lớp 2, lớp liên kết. Địa chỉ không thể là một địa chỉ multicast.

Source Link Layer Address: Lớp 2, địa chỉ lớp liên kết của người gửi. Địa chỉ này không được đưa vào khi địa chỉ IPv6 nguồn là địa chỉ không xác định.

Neighbor Advertisement messages được gửi để phản hồi Neighbor Solicitations

Hình 2.30 Các trường trong ND Neighbor Advertisement message:



Hình 2.30: ICMPv6 ND Neighbor Advertisement Message

IPv6 header:

Source address: Địa chỉ IPv6 được gán cho giao diện gửi.

Destination address: Nếu địa chỉ nguồn trong Neighbor Solicitation tương ứng là một địa chỉ unicast không xác định, thì địa chỉ đích sẽ là địa chỉ multicast FF02 :: 1. Nếu không, địa chỉ đích sẽ là địa chỉ nguồn được sử dụng trong message Neighbor Solicitation.

Hop limit: Giới hạn hop luôn được đặt thành 255

ICMPv6 fields:

Type: Đặt thành 136, cho biết đây là Neighbor Advertisement message. Code: Đặt thành 0 và bị người nhận bỏ qua.

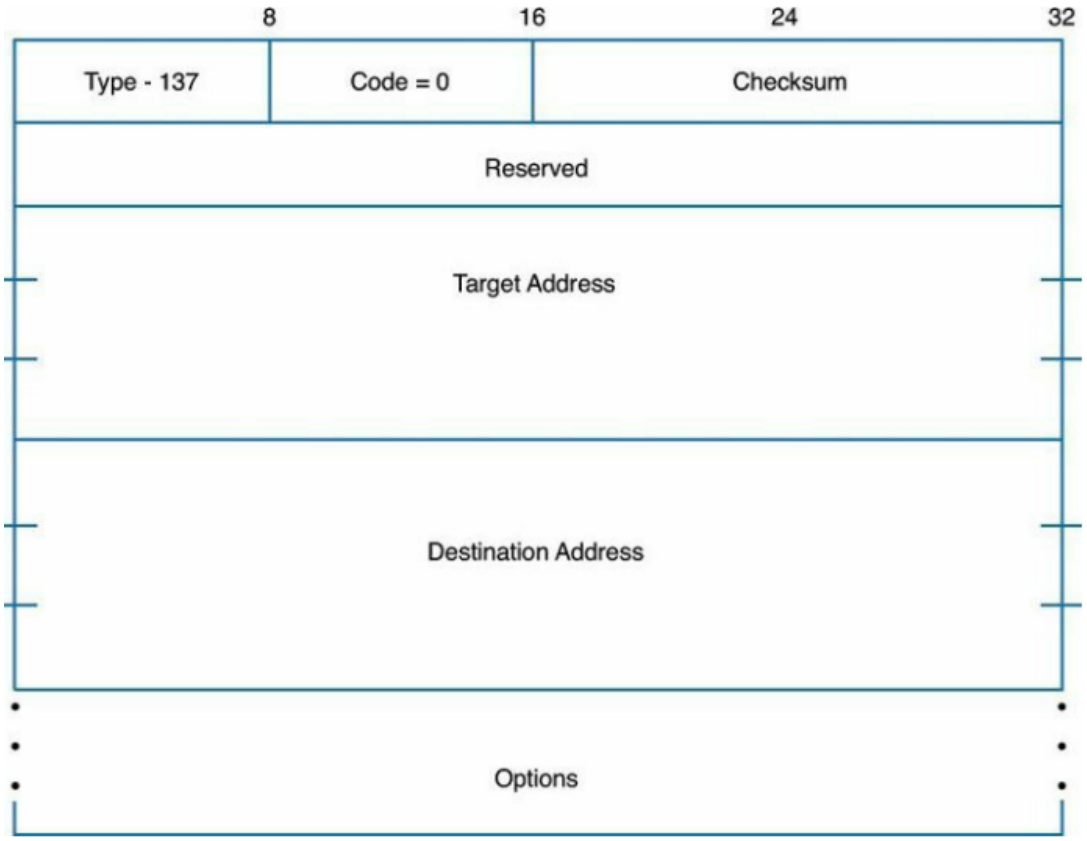
Checksum: Kiểm tra tiêu đề ICMPv6.

R (R-bit hoặc cờ Bộ định tuyến): Khi bit R được đặt thành 1, nó cho biết rằng người gửi là một bộ định tuyến. Bit R được sử dụng bởi Neighbor Unreachability Recognition để phát hiện bộ định tuyến thay đổi thành máy chủ.

S (S-bit hoặc Solicited flag): Khi bit S được đặt thành 1, nó cho biết rằng Neighbor Advertisement này đã được gửi để phản hồi lại Neighbor Solicitation. S-bit được sử dụng như một xác nhận khả năng tiếp cận trong Neighbor Unreachability Detection.
O (O-bit hoặc cờ ghi đè): Khi bit O được đặt thành 1, nó cho biết Neighbor Advertisement này sẽ ghi đè mục nhập bộ đệm Neighbor hiện tại (tương đương với bộ đệm ARP của IPv4) bằng cách cập nhật địa chỉ Lớp 2 được lưu trong bộ nhớ cache cho Địa chỉ IPv6. Khi không được đặt, Neighbor Advertisement này sẽ không cập nhật địa chỉ lớp liên kết được lưu trong bộ nhớ cache mà chỉ tạo một địa chỉ nếu chưa tồn tại.
Reserved: Trường này không được sử dụng.
Target Address: Khi Neighbor Advertisement phản hồi với Neighbor Solicitation, địa chỉ đích là địa chỉ IPv6 được tìm thấy trong trường Địa chỉ mục tiêu của solicitation. Nói cách khác, đó là địa chỉ IPv6 của thiết bị gửi advertisement này.
Source Link Layer Address: Đây là lớp 2, địa chỉ lớp liên kết của người gửi. Không có giá trị gì khi địa chỉ IPv6 nguồn là địa chỉ không xác định.

Redirect Messages

Một tin nhắn chuyển hướng ICMPv6 được sử dụng để thông báo cho thiết bị rằng có bộ định tuyến cho HOP đầu tốt hơn. Nó hoạt động giống như thông báo Redirect được sử dụng trong IPv4. Hình sau cho thấy định dạng của thông báo Chuyển hướng ND ICMPv6.



Hình 2.31: Các trường trong ICMPv6 Redirect Message

Hình 2.31 Mô tả cho các trường trong tiêu đề IPv6 và ICMPv6 cho bản tin Redirect như sau:

Type: Giá trị = 137, cho biết đây là tin nhắn Redirect.

Code: Giá trị = 0, bị người nhận bỏ qua

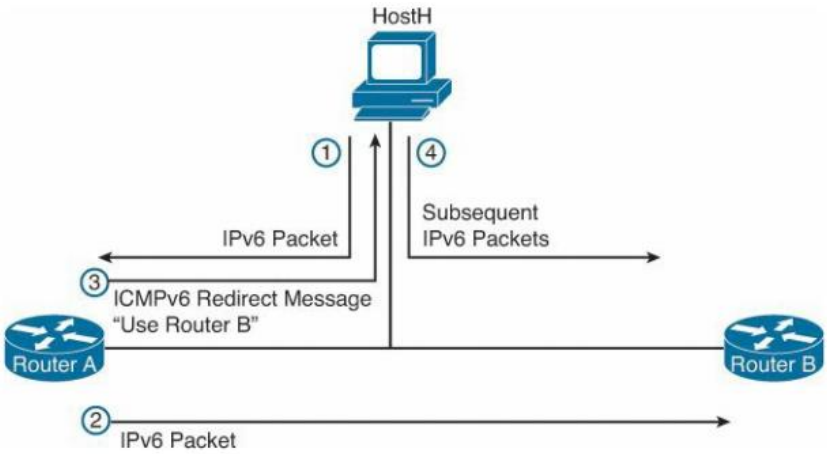
Checksum: Kiểm tra tiêu đề ICMPv6

Reserved: Trường không sử dụng

Target Address: Địa chỉ IPv6 là hop đầu tiên tốt hơn để sử dụng

Destination Address: Địa chỉ IP của đích đã được chuyển hướng đến địa chỉ đích

Possible Option – Target Link Layer Address: Địa chỉ lớp liên kết của địa chỉ đích, bộ định tuyến bước tiếp theo được đề xuất. Điều này tạo thuận lợi cho Host không phải phân giải địa chỉ lớp liên kết của bộ định tuyến khác (bộ định tuyến bước tiếp theo).



Hình 2.32: ICMPv6 Redirect Message

Bốn bước để redirect được thể hiện như hình 2.32.

- *Bước 1.* Host H gửi gói đến Router A, Router A đang là default gateway của Host H.
- *Bước 2.* Router A chuyển tiếp gói này đến Router B.
- *Bước 3.* Router A nhận ra rằng đây là cùng một mạng mà nó nhận được gói, nó sẽ gửi tin nhắn chuyển hướng ICMPv6 đến Host H, thông báo về việc có một Router tốt hơn.
- *Bước 4.* Host H nhận được tin nhắn Redirect và gửi các tin nhắn tiếp theo trực tiếp đến Router B.

2.3 Kết luận chương 2

Trong chương này đã giới thiệu 3 loại địa chỉ IPv6 là Unicast, Multicast và Anycast, trình bày cách biểu diễn địa chỉ IPv6, các phương pháp rút gọn địa chỉ. Phân tích cấu trúc của các loại địa chỉ, cách thức chia mạng con trong IPv6 từ đó phân tích ưu nhược điểm của các cách chia

Chương này cũng nghiên cứu các phương thức cấp phát địa chỉ IPV6 theo phương pháp cấp tĩnh và phương pháp cấp động. Giao thức ICMPv6 và giao thức NDP cũng được tìm hiểu, phân tích khuôn dạng của ICMPv6, phần tích các thông điệp trong ICMPv6. Tìm hiểu việc quản lý các nhóm multicast, các loại thông báo trong MLD. Chương tiếp theo sẽ thực hiện mô phỏng quá trình cấp phát động IPv6 bằng phương pháp DHCP-PD.

CHƯƠNG 3 GIẢI PHÁP TRIỂN KHAI IPV6 CHO VNPT HẢI DƯƠNG

3.1 Kế hoạch triển khai

Theo lộ trình Kế hoạch hành động quốc gia về IPv6 ban hành theo Quyết định số 433/QĐ-BTTTT ngày 19/3/2011; điều chỉnh bổ sung theo Quyết định số 1509/QĐ-BTTTT ngày 20/10/2014 của Bộ trưởng Bộ Thông tin và Truyền thông, Việt Nam đang ở năm cuối của Kế hoạch hành động quốc gia về IPv6. Kết quả triển khai IPv6 Việt Nam đã đạt được nhiều kết quả nổi bật trên nhiều phương diện. Cụ thể như sau:

Tính đến tháng 7/2019, Việt Nam đã có hơn 9 triệu thuê bao FTTH (chủ yếu là thuê bao của Tập đoàn VNPT, Tập đoàn Viettel và FPT Telecom); 9 triệu thuê bao di động (của 03 nhà mạng lới nhất Việt Nam gồm: Viettel, Vinaphone, Mobifone) và hơn 6.000 Website dưới tên miền ".vn" hoạt động tốt với IPv6; trong đó có 61 Website của cơ quan nhà nước, tiêu biểu có cổng thông tin của Bộ Thông tin và Truyền thông, Bộ Tài nguyên và Môi trường, UBND Tp. Đà Nẵng, UBND Tp. HCM, Đồng Nai, nhiều sở TTTT ....

Tỷ lệ ứng dụng IPv6 của Việt Nam đạt 42.90%, Việt Nam đứng thứ 10 trên thế giới, đứng sau Malaysia và đứng thứ 2 khu vực (nguồn APNIC), với hơn 20.000.000 người sử dụng IPv6 (nguồn Cisco). Mạng Internet IPv6 Việt Nam hoạt động ổn định, dịch vụ IPv6 được cung cấp rộng rãi tới người sử dụng đã góp phần đảm bảo cho hoạt động Internet Việt Nam bắt kịp với xu thế công nghệ mới.

Kế hoạch triển khai được chia thành các giai đoạn:

GIAI ĐOẠN 1 - GIAI ĐOẠN CHUẨN BỊ (2011-2012)

Mục tiêu:

- Hoàn thành việc phổ cập kiến thức cơ bản về IPv6 cho cộng đồng công nghệ thông tin và truyền thông. Tất cả các doanh nghiệp Internet, các tổ chức, doanh nghiệp lớn có hạ tầng công nghệ thông tin thực hiện các chương trình đào tạo nhân lực về IPv6;

- Hoàn thiện các văn bản quy phạm pháp luật, văn bản hướng dẫn về yêu cầu đảm bảo thiết bị phải tương thích với IPv6 và ưu tiên hỗ trợ triển khai IPv6 cho các dự án công nghệ thông tin sử dụng ngân sách nhà nước.
- Hình thành mạng thử nghiệm IPv6 quốc gia. Thiết lập đường kết nối thuần IPv6 từ Việt Nam đi quốc tế;
- Tất cả các doanh nghiệp Internet từng bước chuẩn bị các điều kiện cần thiết về kế hoạch, nhân lực và kỹ thuật để triển khai IPv6 tại doanh nghiệp. Các doanh nghiệp Internet có cung cấp hạ tầng mạng hoàn thành việc thử nghiệm IPv6;
- Các Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước được đấu nối thử nghiệm và sẵn sàng cho việc chuyển đổi sang IPv6;
- Hoàn thành cơ bản việc đánh giá và chuẩn bị các điều kiện cần thiết về kiến thức, hạ tầng kỹ thuật và nhân lực phục vụ cho việc chuyển đổi sang IPv6 tại Việt Nam

GIAI ĐOẠN 2 - GIAI ĐOẠN KHỞI ĐỘNG (2013-2015)

Mục tiêu:

- Hình thành cơ sở hạ tầng mạng IPv6 quốc gia;
- Triển khai rộng rãi việc cho phép đấu nối và thử nghiệm IPv6 trên cơ sở hạ tầng mạng IPv6 quốc gia;
- Tất cả các doanh nghiệp Internet sẵn sàng hoạt động song song IPv4/IPv6;
- Bắt đầu cung cấp chính thức một số dịch vụ trên nền công nghệ IPv6 cho khách hàng;
- Các tổ chức, doanh nghiệp lớn có hạ tầng công nghệ thông tin bước đầu triển khai việc chuyển đổi hạ tầng từ IPv4 sang hỗ trợ song song IPv4/IPv6;
- Chính thức áp dụng IPv6 cho Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;
- Mạng Internet Việt Nam sẵn sàng cung cấp các dịch vụ trên nền công nghệ IPv6.

GIAI ĐOẠN 3 - GIAI ĐOẠN CHUYỂN ĐỔI (2016-2019)

Mục tiêu:

- Hoàn thiện và nâng cấp mạng cơ sở hạ tầng IPv6 quốc gia, hoàn thiện việc chuyển đổi mạng lưới, dịch vụ, ứng dụng, phần mềm và thiết bị trên toàn bộ mạng Internet

Việt Nam, đảm bảo cho Internet Việt Nam hoạt động một cách an toàn, tin cậy với địa chỉ IPv6 (hoàn toàn tương thích với IPv6).

- Mạng lưới của các tổ chức, doanh nghiệp, Mạng của chuyên dùng của các cơ quan Đảng, Nhà nước chính thức sử dụng và cung cấp dịch vụ với IPv6.

3.2 Dịch vụ triển khai

Với tốc độ tăng trưởng trung bình 200% một năm, tỉ lệ truy cập Internet qua IPv6 toàn cầu đã đạt 26% vào cuối tháng 4/2019. Năm 2020, tỉ lệ ứng dụng IPv6 toàn cầu đạt khoảng 50% và giao thức IPv4 sẽ dần ngừng hoạt động. Sau hơn 11 năm thúc đẩy triển khai IPv6, bám sát thực hiện lộ trình Kế hoạch hành động quốc gia về IPv6, Việt Nam được đánh giá là một trong những nước có kết quả tốt trong triển khai chuyển đổi IPv6. Mạng Internet Việt Nam cũng được ghi nhận chính thức cung cấp trên diện rộng các dịch vụ ứng dụng công nghệ thế hệ mới trên nền tảng IPv6.

Hiện nay tỉ lệ ứng dụng IPv6 của Việt Nam đạt 42,90% với hơn 9 triệu thuê bao cáp quang và 9 triệu thuê bao di động sử dụng IPv6. Với kết quả này, Việt Nam đứng thứ 10 trên toàn thế giới, thứ 4 khu vực Châu Á - Thái Bình Dương, đứng thứ 2 khu vực ASEAN về tỉ lệ ứng dụng IPv6.

Để hoàn thành Kế hoạch hành động quốc gia về IPv6, Bộ trưởng Bộ Thông tin và Truyền thông đã ban hành Kế hoạch thúc đẩy triển khai IPv6, trong đó có các mục tiêu chính:

- Thúc đẩy ứng dụng IPv6 trong cơ quan nhà nước và doanh nghiệp nội dung số;
- Mở rộng triển khai IPv6 trên mạng dịch vụ di động 4G LTE/5G;
- Thúc đẩy triển khai IPv6 cho hệ thống máy chủ tên miền (DNS) của các doanh nghiệp cung cấp dịch vụ Internet; triển khai hỗ trợ IPv6 trong hệ thống máy chủ tên miền và hệ thống cung cấp dịch vụ đăng ký, duy trì tên miền ".VN" của các Nhà đăng ký.

- Tiếp tục thúc đẩy doanh nghiệp chuyển đổi hoàn toàn IPv6 cho thuê bao FTTH; dịch vụ kết nối của ISP; tăng cường lưu lượng kết nối IPv6 qua Trạm trung chuyển lưu lượng Internet quốc gia (VNIX).
- - Tăng cường vị thế, hình ảnh, xếp hạng của Việt Nam trong khu vực và thế giới về công tác triển khai ứng dụng IPv6.

Trong kế hoạch thúc đẩy chuyển đổi IPv6 năm 2019, tăng cường ứng dụng triển khai IPv6 trong cơ quan nhà nước được coi là nhiệm vụ trọng tâm. Mặc dù dịch vụ IPv6 đã được các doanh nghiệp triển khai rộng rãi, mức độ ứng dụng triển khai IPv6 trong khối cơ quan nhà nước còn hạn chế. Trong khi người sử dụng Internet tại Việt Nam đã chuyển sang kết nối Internet qua IPv6, phần lớn các cổng thông tin điện tử, dịch vụ công trực tuyến của các cơ quan nhà nước vẫn duy trì sử dụng IPv4.

Theo khảo sát của Ban Công tác thúc đẩy phát triển IPv6 quốc gia, trong số khoảng 6.000 Website dưới tên miền ".VN" đang hoạt động tốt với IPv6, mới có 61 Website của khối cơ quan nhà nước. Đây là điều chưa phù hợp xu thế quốc tế khi các quốc gia khác đều đưa công tác chuyển đổi IPv6 trong mạng lưới, dịch vụ của cơ quan nhà nước lên làm nhiệm vụ trọng tâm (tại Mỹ, tiêu chuẩn về triển khai IPv6 trong mạng lưới và ứng dụng CNTT của cơ quan nhà nước được công bố từ năm 2008; tại Trung Quốc, tỉ lệ Website cơ quan Nhà nước hoạt động với IPv6 là trên 67,7%; ở Malaysia là trên 50%,…).

Nhằm đảm bảo kết nối Internet thông suốt, an toàn cho hệ thống mạng lưới, dịch vụ của cơ quan nhà nước, trong văn bản gửi tới các Bộ, ngành, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương, Bộ TT&TT đã đề nghị tăng cường hoạt động triển khai ứng dụng IPv6 trên mạng lưới, dịch vụ của đơn vị, thông qua các hoạt động:

- Xây dựng đề án chuyển đổi IPv6 trong hạ tầng mạng lưới, dịch vụ phù hợp với Kế hoạch hành động quốc gia về IPv6 và phù hợp với kế hoạch phát triển chính phủ điện tử, thành phố thông minh tại địa bàn: bổ sung hạng mục về IPv6 trong các đề án ứng dụng CNTT; đầu tư, mua sắm các thiết bị mới có

hỗ trợ công nghệ IPv6; yêu cầu hỗ trợ IPv6 đối với các dịch vụ ứng dụng CNTT thuê ngoài,…

- Kích hoạt hỗ trợ IPv6 trên Website chính và cổng thông tin điện tử của đơn vị.
- Triển khai chuyển đổi mạng lưới và dịch vụ sang hỗ trợ IPv4/IPv6, đặc biệt là triển khai IPv6 trong hệ thống chính phủ điện tử và mạng lưới cung cấp dịch vụ công trực tuyến mức độ 3, mức độ 4.

3.3 Một số phướng án cấp phát IPv6 cho thiết bị đầu cuối từ nhà cung cấp dịch vụ

- Kích hoạt hỗ trợ IPv6 trên Website chính và cổng thông tin điện tử của đơn vị.
- Triển khai chuyển đổi mạng lưới và dịch vụ sang hỗ trợ IPv4/IPv6, đặc biệt là triển khai IPv6 trong hệ thống chính phủ điện tử và mạng lưới cung cấp dịch vụ công trực tuyến mức độ 3, mức độ 4.
- Quy hoạch địa chỉ IPv6 theo các loại hình dịch vụ: Băng rộng cố định, di động, khách hàng doanh nghiệp, IoT…
- Trong dải địa chỉ lớn đã quy hoạch cho mỗi dịch vụ, tiếp tục quy hoạch theo vùng, căn cứ thực tế thiết kế mạng, chính sách định tuyến, vận hành khai thác.
- Đơn vị quy hoạch cơ sở (Tương ứng với 1 khách hàng hộ gia đình) quy hoạch theo dải /64, /60, /56.
- Dải địa chỉ IPv6 khuyến nghị quy hoạch theo bội số của 4 để thuận tiện cho việc quản lý, phân bổ tiếp cho các vùng thiết bị mạng: /64, /60, /56, /52, /48, /44, /40, /36, /32.

3.4 Triển khai IPv6 trong mạng băng rộng VNPT

- Ngày 11/1/2017 VNPT ban hành QĐ 18/VNPT-CNM về việc ban hành nguyên tắc quy hoạch IPv6 trong giai đoạn 2016-2020. Nội dung quy hoạch IPv6 theo các dịch vụ: Băng rộng cố định, di động, IoT, khách hàng doanh

nghiệp. Toàn dải IPv6 của VNPT được quy hoạch theo dự báo thuê bao phát triển đến 2020.

- Ngày 17/7/2019 Ban công nghệ mạng ban hành QĐ 1016/VNPT-CN về việc bổ sung quy hoạch cho địa chỉ IPv6. Nội dung bổ sung quy hoạch IPv6 cho thuê bao Leaseline. Cấp 01 dải 2001:0EE0:0400::/40 cho tổng công ty Media. Phân bổ dải cho dịch vụ IPv6 tĩnh đối với dịch vụ Fiber VNN cho 3 miền Bắc, Trung, Nam.
- Ngày 01/8/2019 VNPT NET-KTM đưa ra thông báo số 3196 về việc báo cáo thử nghiệm cấp IPv4, IPv6 tĩnh giao diện LAN, WAN cho thuê bao Fiber VNN. Các hệ thống Visa, LDAP, Radius sử dụng 7 thuộc tính để truyền các giá trị địa chỉ IPv4, IPv6 xuống thuê bao. Số lượng địa chỉ IPv6 được cấp như sau: 1 IPv6 cho WAN = 1 subnet /64, 1 IPv6 LAN tĩnh = 1 subnet /56.
- Ngày 22/8/2019 Viễn thông Hà Nội báo cáo kết quả thử nghiệm kỹ thuật cấp IPv4, IPv6 tĩnh cho thuê bao Fiber VNN dùng PPPoE.
- Ngày 19/9/2019 Ban công nghệ ban hành hướng dẫn số 4475/VNPT-CN về việc hướng dẫn cung cấp IPv4, IPv6 tĩnh cho thuê bao Fiber VNN dùng PPPoE.

3.5 Mô phỏng cấp phát IPv6 cho đầu cuối từ ISP bằng giả lập EVE-NG theo phương pháp DHCP-PD

3.5.1 Thực hiện mô phỏng việc cấp phát IPv6 từ ISP đến khách hàng

Các phương thức gán địa chỉ IPv6 khác nhau như sau:

Manual Assignment

Stateless Address Autoconfiguration (RFC2462)

Stateful DHCPv6

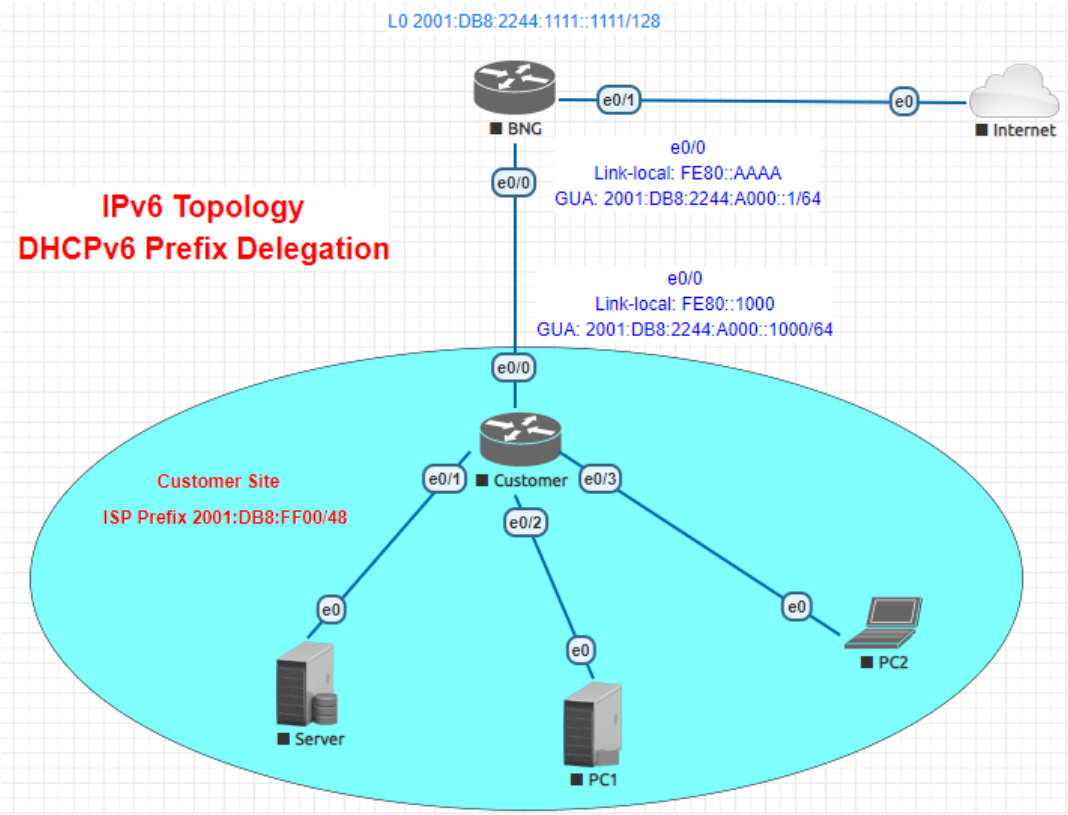
Stateless DHCPv6

DHCPv6-PD

DHCPv6 Prefix Delegation (DHCPv6-PD) là một phần mở rộng của DHCPv6 và được chỉ định trong RFC3633. Classical DHCPv6 thường được tập trung khi gán tham số từ máy chủ DHCPv6 đến thiết bị IPv6 Một ví dụ thực tế gán

stateful address "2001: db8 :: 1" từ máy chủ DHCPv6 đến máy khách DHCPv6. Tuy nhiên DHCPv6-PD nhằm mục đích gán các mạng con và các tham số mạng từ máy chủ DHCPv6-PD cho máy khách DHCPv6-PD. Điều này có nghĩa là thay vì chỉ định một địa chỉ, DHCPv6-PD sẽ chỉ định một tập hợp các "mạng con" IPv6.

Một ví dụ có thể là việc gán "2001: db8 :: / 60" từ máy chủ DHCPv6-PD cho máy khách DHCPv6-PD. Điều này sẽ cho phép máy khách DHCPv6-PD (thường là thiết bị CPE) chia không gian địa chỉ IPv6 nhận được và gán nó một cách linh hoạt cho các giao diện hỗ trợ IPv6. Mô hình 3.1 giả lập việc cấp phát DHCPv6 Prefix Delegation (DHCPv6-PD) từ ISP đến khách hàng.



Hình 3.1: LAB mô phỏng cấp phát DHCP-PD

Trong mô hình giả lập bao gồm các thiết bị:

BNG: Broadband Network Gateway, cung cấp kết nối từ BNG xuống Router khách hàng và cung cấp thêm 01 dải với /48 (2001:DB8:FF00::/48)

Router Customer: nhận 02 dải địa chỉ IPv6. Một dải cung cấp cho kết nối WAN, một dải /48 phân dùng cho các phân đoạn mạng khác trong mạng khách hàng

Có thể sử dụng phần mềm EVE-NG, GNS3, Packet tracert. Chọn EVE-NG bởi phần mềm chạy với image thật của Cisco.

Server, *PC1*, *PC2*: Các thiết bị nhận địa chỉ IPv6 được cấp phát tự động sau khi Router Customer chia từ /48 ra.

Các lệnh chính thực hiện trong Router BNG

```
BNG(config)#ipv6 unicast-routing
BNG(config)#ipv6 dhcp pool DHCP_POOL
BNG(config-dhcpv6)#prefix-delegation pool my_prefix_pool
BNG(config)#interface Ethernet0/0
BNG(config-if)#ipv6 address FE80::AAAA link-local
BNG(config-if)#ipv6 address 2001:DB8:2244:A000::1/64
BNG(config-if)#ipv6 dhcp server DHCP_POOL
BNG(config)#ipv6 route 2001:DB8:FF00::/48 Ethernet0/0
FE80::1000
BNG(config)#ipv6 local pool my_prefix_pool
2001:DB8:FF00::/40 48
```

Các lệnh chính thực hiện trong Router Customer

```
Customer(config)# ipv6 unicast-routing
Customer(config)#interface Ethernet0/0
Customer(config-if)# ipv6 address FE80::1000 link-local
Customer(config-if)# ipv6 address
2001:DB8:2244:A000::1000/64
Customer(config-if)# ipv6 dhcp client pd ISP_PREFIX
Customer(config)#interface Ethernet0/1
Customer(config-if)# ipv6 address ISP_PREFIX
::1:0:0:0:1/64
Customer(config)#interface Ethernet0/2
Customer(config-if)# ipv6 address ISP_PREFIX
::2:0:0:0:1/64
Customer(config)#interface Ethernet0/3
```

```
Customer(config-if)# ipv6 address ISP_PREFIX
::3:0:0:0:1/64
Customer(config)#ipv6 route ::/0 Ethernet0/0 FE80::AAAA
Customer(config)#ipv6 route ::/0 Ethernet0/0 FE80::AAAA
```

Các lệnh chính thực hiện trong Server, PC

```
Server(config)interface Ethernet0
Server(config-if)#no ip address
Server(config-if)#ipv6 address autoconfig
PC1(config)interface Ethernet0
PC1(config-if)#no ip address
PC1(config-if)#ipv6 address autoconfig
PC2(config)interface Ethernet0
PC2(config-if)#no ip address
PC2(config-if)#ipv6 address autoconfig
```

3.5.2 Kiểm tra trạng thái và kiểm tra kết nối

BNG#show ipv6 dhcp pool

```
DHCPv6 pool: DHCP_POOL
  Prefix pool: my_prefix_pool
               preferred lifetime 604800, valid lifetime
2592000
  Active clients: 1
```

Log bên trên chỉ ra rằng, BNG đang cấp DHCP cho 1 Client và đang sử dụng pool my_prefix_pool.

BNG#show ipv6 dhcp binding

```
Client: FE80::1000
  DUID: 00030001AABBCC002000
  Username : unassigned
  VRF : default
  Interface : Ethernet0/0
```

```
  IA PD: IA ID 0x00030001, T1 302400, T2 483840
    Prefix: 2001:DB8:FF00::/48
            preferred lifetime 604800, valid lifetime
2592000
            expires at Jun 08 2020 06:17 AM (2591414
seconds)
```

Log trên chỉ ra Prefix được gán cho Client

```
Customer#show ipv6 dhcp interface
Ethernet0/0 is in client mode
  Prefix State is OPEN
  Renew will be sent in 3d11h
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::AAAA
    DUID: 00030001AABBCC001000
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 302400, T2 483840
        Prefix: 2001:DB8:FF00::/48
                preferred lifetime 604800, valid
lifetime 2592000
                expires at Jun 08 2020 06:35 AM (2591805
seconds)
      DNS server: 2001:4860:4860::8888
      Domain name: sontv.hdg
      Information refresh time: 0
  Prefix name: ISP_PREFIX
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

Ở trên, chỉ ra đã nhận được tiền tố từ ISP, bao gồm một số chi tiết khác như máy chủ DNS và tên miền.

```
Customer#show ipv6 general-prefix
IPv6 Prefix ISP_PREFIX, acquired via DHCP PD
  2001:DB8:FF00::/48 Valid lifetime 2591692, preferred
lifetime 604492
   Ethernet0/1 (Address command)
   Ethernet0/2 (Address command)
   Ethernet0/3 (Address command)
Server#show ipv6 interface brief
Ethernet0                  [up/up]
    FE80::D203:22FF:FEF6:1
    2001:DB8:FF00:1:D203:22FF:FEF6:1
PC1#show ipv6 interface brief
Ethernet0                  [up/up]
    FE80::D204:72FF:FE27:1
    2001:DB8:FF00:2:D204:72FF:FE27:1
PC2#show ipv6 interface brief
Ethernet0                  [up/up]
    FE80::D205:73FF:FE3F:1
    2001:DB8:FF00:3:D205:73FF:FE3F:1
```

Kiểm tra các kết nối từ Server

```
Server#ping 2001:DB8:FF00:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FF00:1::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/11/20 ms
Server#ping 2001:DB8:2244:A000::1000
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:DB8:2244:A000::1000, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/0/4 ms
Server#ping 2001:DB8:2244:A000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2244:A000::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/4/16 ms
Server#ping 2001:DB8:2244:1111::1111
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:DB8:2244:1111::1111, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/2/8 ms
Kiểm tra các kết nối từ PC1
PC1#ping 2001:DB8:FF00:2::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FF00:2::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/12/20 ms
PC1#ping 2001:DB8:2244:A000::1000
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to
2001:DB8:2244:A000::1000, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/0/3 ms
PC1#ping 2001:DB8:2244:A000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2244:A000::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/4/15 ms
PC1#ping 2001:DB8:2244:1111::1111
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:DB8:2244:1111::1111, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/2/7 ms
```

Kiểm tra các kết nối từ PC2

```
PC2#ping 2001:DB8:FF00:3::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FF00:3::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/12/18 ms
PC2#ping 2001:DB8:2244:A000::1000
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to
2001:DB8:2244:A000::1000, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/0/2 ms
PC2#ping 2001:DB8:2244:A000::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2244:A000::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/4/14 ms
PC2#ping 2001:DB8:2244:1111::1111
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to
2001:DB8:2244:1111::1111, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 0/2/8 ms
```

3.6 Kết luận chương 3

Trong chương 3 đã trình bày kế hoạch triển khai IPv6 theo lộ trình của quốc gia. Kế hoạch triển khai được chia thành các giai đoạn: chuẩn bị, khởi động và chuyển đổi. Các dịch vụ được triển khai cũng được phân tích dựa trên các mục tiêu chính:

- Thúc đẩy ứng dụng IPv6 trong cơ quan nhà nước và doanh nghiệp nội dung số.
- Mở rộng triển khai IPv6 trên mạng dịch vụ di động 4G LTE/5G.
- Thúc đẩy triển khai IPv6 cho hệ thống máy chủ tên miền (DNS) của các doanh nghiệp cung cấp dịch vụ Internet; triển khai hỗ trợ IPv6 trong hệ thống

máy chủ tên miền và hệ thống cung cấp dịch vụ đăng ký, duy trì tên miền ".VN" của các Nhà đăng ký.

Tiếp theo trình bày một số phướng án cấp phát IPv6 cho thiết bị đầu cuối từ nhà cung cấp dịch vụ, cụ thể hóa bằng việc trình bày việc triển khai IPv6 trong mạng băng rộng VNPT. Phần cuối cùng của chương đã thực hiện việc mô phỏng cấp phát IPv6 cho đầu cuối từ ISP bằng giả lập GNS3, Packet tracert, EVE-NG.

KẾT LUẬN

Với tốc độ phát triển đến chóng mặt của INTERNET ngày nay, xu thế công nghệ hóa toàn cầu, INTERNET of Things … thì việc cạn kiệt tài nguyên địa chỉ IPv4 sẽ không còn xa do vậy việc triển khai IPv6 trên hệ thống mạng toàn cầu là điều vô cùng cần thiết. Nhưng việc chuyển đổi hoàn toàn sang mạng IPv6 từ mạng IPv4 đang chạy ổn định là điều không hề đơn giản, thực hiện trong thời gian ngắn được, việc chuyển đổi phải được thực hiện từng bước, với các phương pháp chuyển đổi thích hợp giữa IPv4 và IPv6.

Luận văn đã thực hiện nghiên cứu được kỹ thuật cấp phát IPv6 động từ ISP đến các thiết bị đầu cuối tại khách hàng tối ưu nhất. Thực hiện giả lập toàn bộ quá trình cấp phát địa chỉ để nhận ra được nhưng ưu nhược điểm trong triển khai thực tế.

Tuy nhiên chưa có được đánh giá cụ thể khi triển khai, áp dụng ngoài thực tiễn do vậy thời gian tới em sẽ tìm hiểu đưa triển khai thực tế tại mô hình mạng của công ty để có cái nhìn tốt nhất về phương pháp cấp phát địa chỉ động kiểu này.

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Nguyễn Thị Thu Thủy, Giới Thiệu Về Thế Hệ Địa Chỉ Internet Mới IPv6, NXB Bưu Điện 2006,

Tiếng Anh

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

[3] Analysis of ipv6 transition, International Journal of Computer Networks &

Communications (IJCNC) Vol.6, No.5, September 2014

[4] IPv4-to-IPv6 Transition and Co-Existence Strategies By Tim Rooney Director, Product Management BT Diamond IP, Revised and Updated 2011 Edition

[5] A Detail Comprehensive Review on IPv4-to-IPv6 Transition and CoExistence Strategies, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 4, April 2015

[6] Rick Graziani, IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, Cisco Press, First Printing October 2012

Trang Web

[7] Website: https://www.vnnic.vn/

[8] Website: http://www.cisco.com/; https://www.gns3.com/