

**BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM**



**CẨM NANG
HƯỚNG DẪN TRIỂN KHAI MẠNG TRUY CẬP IPV6 ONLY
CHO CƠ QUAN NHÀ NƯỚC, TỔ CHỨC VÀ DOANH NGHIỆP**

Hà Nội, tháng 5 năm 2025

MỤC LỤC

PHẦN 1: GIỚI THIỆU CHUNG	4
1.1. Mục đích và phạm vi của cẩm nang.....	4
1.2. Tổng quan về IPv6 only	4
1.3. Lý do cần triển khai IPv6 only trong mạng truy cập	7
PHẦN 2: HẠ TẦNG VÀ CÁC YÊU CẦU KỸ THUẬT.....	8
2.1. Các thành phần trong mô hình mạng truy cập IPv6 only	8
2.2. Các điều kiện cần thiết trước khi triển khai	9
PHẦN 3: CÁC MÔ HÌNH TRIỂN KHAI IPv6 ONLY	11
3.1. Mô hình mạng IPv6 only sử dụng DNS64/NAT64	11
3.2. Mô hình mạng IPv6 only sử dụng Proxy Dual Stack	14
3.3. Mô hình mạng IPv6 native.....	15
3.4. Đánh giá lựa chọn mô hình triển khai.....	15
PHẦN 4: TRIỂN KHAI MẠNG TRUY CẬP IPV6 ONLY	17
4.1. Tổng quan quy trình triển khai.....	17
4.2. Hướng dẫn kỹ thuật chi tiết.....	18
4.3. Các vấn đề thường gặp và giải pháp	25
4.4. Bảo mật cơ bản trên IPv6.....	27
PHỤ LỤC	31
1. Danh mục tài liệu tham khảo, liên hệ hỗ trợ kỹ thuật.....	31
2. Checklist rà soát, đánh giá hiện trạng hệ thống trước khi triển khai	32
3. Checklist về kiểm tra dịch vụ sau khi triển khai.....	33
4. Danh sách các công dịch vụ để triển khai chính sách an toàn bảo mật	35

MỞ ĐẦU

Internet ngày nay đã phát triển một cách vượt bậc, là hạ tầng có vai trò quan trọng trong mọi hoạt động kinh tế, chính trị, xã hội. IPv6 là thế hệ tiếp theo của giao thức Internet và đang được triển khai cung cấp dịch vụ trên mạng Internet nhằm thay thế hoàn toàn IPv4 đã cạn kiệt và để đáp ứng được xu thế phát triển công nghệ như IoT, 5G. Để chuyển đổi từ IPv4 sang IPv6 cần qua nhiều giai đoạn cũng như căn cứ theo tình hình thực tế của mạng lưới và nhu cầu sử dụng. Bên cạnh đó, kế hoạch hành động quốc gia về IPv6 giai đoạn 2021 - 2025 khẳng định rõ yêu cầu triển khai IPv6 trong hạ tầng mạng của cơ quan nhà nước, tổ chức, doanh nghiệp làm nền tảng cho các dịch vụ chính phủ điện tử và chính phủ số.

Với vai trò là đơn vị quản lý tài nguyên Internet quốc gia, Trung tâm Internet Việt Nam (VNNIC) luôn đi đầu trong nghiên cứu, ứng dụng và thúc đẩy triển khai các công nghệ mới của Internet. Việc triển khai IPv6 only cho mạng truy cập tại VNNIC không chỉ thể hiện tinh thần tiên phong công nghệ mà còn nhằm đánh giá toàn diện các khía cạnh kỹ thuật, vận hành, từ đó xây dựng mô hình ứng dụng thực tiễn, hiệu quả. Đây cũng là bước chuẩn bị quan trọng để lan tỏa kinh nghiệm, hỗ trợ các đơn vị trong quá trình chuyển đổi sang IPv6 một cách thuận lợi và an toàn.

Dựa trên kết quả nghiên cứu, triển khai thực tế, VNNIC đã xây dựng cẩm nang hướng dẫn chuyển đổi mô hình mạng truy cập IPv6 only điển hình có thể áp dụng rộng rãi cho các cơ quan nhà nước, tổ chức, doanh nghiệp góp phần đẩy nhanh tiến độ chuyển đổi IPv6, phát triển hạ tầng số an toàn, hiện đại tại Việt Nam.

PHẦN 1: GIỚI THIỆU CHUNG

1.1. Mục đích và phạm vi của cẩm nang

a. Mục đích

Cẩm nang hướng dẫn các cơ quan nhà nước, tổ chức, doanh nghiệp triển khai mạng IPv6 only một cách đồng bộ, hiệu quả và giúp các đơn vị hiểu rõ các yêu cầu kỹ thuật, mô hình kiến trúc, công nghệ chuyển đổi cũng như các bước triển khai cần thực hiện để đạt được mục tiêu chuyển đổi mạng truy cập sử dụng IPv6 only.

b. Phạm vi

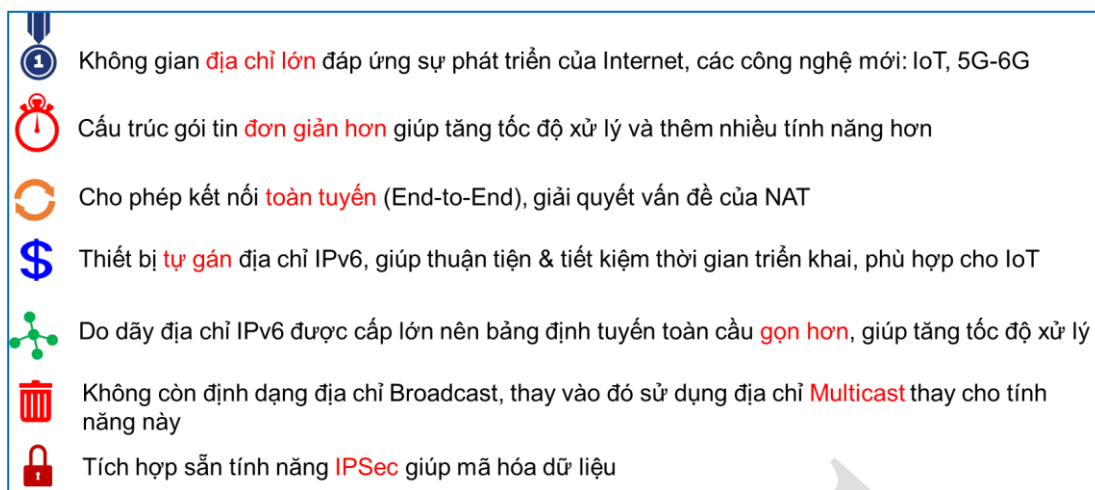
Cẩm nang tập trung chủ yếu vào việc chuyển đổi, triển khai IPv6 only cho mạng truy cập, các thành phần bao gồm: Mạng truy cập có dây, không dây và các thành phần kỹ thuật liên quan.

1.2. Các khái niệm về IPv6 only

a. Khái niệm, lợi ích và sự khác biệt so với mạng Dual Stack

Mạng IPv6 only là mô hình mạng trong đó toàn bộ hạ tầng, thiết bị, dịch vụ, ứng dụng được thiết lập và hoạt động hoàn toàn dựa trên giao thức IPv6, loại bỏ hoàn toàn sự tồn tại và phụ thuộc vào giao thức IPv4. Đây là mô hình mạng phản ánh đầy đủ nhất mục tiêu phát triển của Internet thế hệ mới, nơi không gian địa chỉ rộng lớn của IPv6 trở thành nền tảng cho mọi kết nối, trao đổi dữ liệu và cung cấp dịch vụ.

Trải qua một thời gian tối ưu, bổ sung tính năng cho các giao thức liên quan như: ICMPv6, NDP, SLAAC, MLD, DHCPv6, NPTv6, DNS64, NAT64, 6LowPAN... Chính việc này đã giúp cho IPv6 có nhiều tính năng mới và ưu việt hơn so với IPv4. Cấu trúc bản tin IPv6 gọn gàng và tối ưu hơn (số trường ít hơn, kích thước Header cố định 40-byte) nên tốc độ xử lý bản tin IPv6 sẽ nhanh hơn rất nhiều. Với độ dài 128 bit các dãy địa chỉ IPv6 phân bổ cho các đơn vị sẽ lớn hơn, giúp bản định tuyến gọn hơn và tính năng NAT không cần được sử dụng. Cấu trúc Extension Header tăng cường khả năng bảo mật cho IPv6. Dưới đây là những lợi ích mà giao thức IPv6 mang lại so với IPv4.



Hình 1: Những lợi ích của giao thức IPv6

Ngoài những lợi ích do chính IPv6 mang lại thì việc chuyển từ cơ chế hoạt động Dual Stack sang IPv6 only còn đem đến những lợi ích quan trọng khác như sau:

- Chấm dứt phụ thuộc IPv4: Việc sử dụng song song cả IPv4 và IPv6 làm cho hệ thống tiếp tục phụ thuộc vào địa chỉ IPv4. Địa chỉ IPv4 ngày càng cạn kiệt và sự thiếu hụt địa chỉ IPv4 sẽ khiến hệ thống không được mở rộng, phát triển và thậm chí ngừng trệ. Nếu chuyển sang IPv6 only thì tất cả những hạn chế của IPv4 sẽ được giải quyết hoàn toàn và ngay lập tức.

- Đơn giản hóa công tác vận hành, khai thác hệ thống: Thay vì quản lý đồng thời cả hai giao thức, việc sử dụng một mình IPv6 sẽ làm giảm đáng kể sự phức tạp trong quy hoạch, quản lý, giám sát và xử lý sự cố. Các sai sót trong vận hành khai thác cũng được giảm thiểu.

- Tối ưu hóa hiệu suất, tài nguyên thiết bị: Khi các khai báo cho IPv4 không còn thì bảng định tuyến sẽ gọn hơn, các cơ chế chuyển đổi giữa hai giao thức không được sử dụng nữa, các giao thức, dịch vụ cũng nhẹ nhàng hơn. Toàn bộ tài nguyên của thiết bị chỉ dành cho IPv6 nên hiệu suất hoạt động sẽ tăng lên và tốc độ xử lý nhanh hơn.

- Cải thiện bảo mật: Thay vì quản lý bảo mật cho cả IPv4 và IPv6 thì công tác bảo mật chỉ tập trung vào IPv6. Các vấn đề bảo mật liên quan đến IPv4 được loại bỏ hoàn toàn. Cơ chế bảo mật của IPv6 sẽ được khai thác và sử dụng.

Tổng quan một số điểm khác biệt chính giữa IPv6 only và Dual Stack:

	IPv6 only	Dual Stack
Giao thức mạng	Chỉ sử dụng IPv6	Sử dụng cả IPv4 và IPv6 song song
Quản lý	Đơn giản hơn, chỉ quản lý một giao thức	Phức tạp do sử dụng hai giao thức
Chuyển đổi	Giai đoạn cuối cùng của quá trình chuyển đổi	Giai đoạn trung gian trong quá trình chuyển đổi
Tính tương thích	Cần các cơ chế biên dịch/Tunnel/Proxy để truy cập tài nguyên IPv4	Tương thích trực tiếp với IPv4 và IPv6
Chi phí	Thấp	Cao

Bảng 1: So sánh khác biệt giữa mạng IPv6 only và Dual Stack

b. Bối cảnh thúc đẩy chuyển đổi IPv6 tại Việt Nam

Việt Nam đã và đang duy trì vị thế là một trong những quốc gia tiên phong và đạt được những thành tựu vượt trội trong quá trình chuyển đổi sang IPv6. Tính đến tháng 5/2025, tỷ lệ sử dụng IPv6 của Việt Nam thường xuyên nằm trong top 10 thế giới, chứng minh sự quyết tâm và hiệu quả của các chính sách và nỗ lực triển khai. Bối cảnh thúc đẩy quá trình này rất rõ ràng và mang tính chiến lược, đặc biệt khi Việt Nam đang mạnh mẽ hướng tới kinh tế số và xã hội số:

- **Thiếu hụt trầm trọng địa chỉ IPv4:** Đây vẫn là động lực hàng đầu và không đổi. Địa chỉ IPv4 đã cạn kiệt trên toàn cầu từ lâu (IANA hết địa chỉ từ năm 2011, các RIR cũng đã phân bổ gần hết). Việt Nam, với dân số đông và tốc độ tăng trưởng người dùng Internet, thiết bị kết nối.

- **Chính phủ số, kinh tế số, xã hội số:** Trong chiến lược phát triển quốc gia về Chính phủ số, Kinh tế số và Xã hội số đều xác định IPv6 là hạ tầng nền tảng quan trọng. Để xây dựng một nền tảng số mạnh mẽ, có khả năng kết nối rộng khắp và an toàn, việc chuyển đổi sang IPv6 là bắt buộc.

- **Sự phát triển của các công nghệ mới:** Các công nghệ như: 5G, IoT, AI, Blockchain,... đã và đang tạo ra nhu cầu kết nối cho hàng tỷ thiết bị. Mỗi cảm biến, mỗi thiết bị thông minh (camera, thiết bị gia dụng, xe cộ,...) đều cần một địa chỉ IP duy nhất để có thể giao tiếp trực tiếp. IPv6 với không gian địa chỉ khổng lồ

(2¹²⁸ địa chỉ) là giải pháp duy nhất và bền vững cho kỷ nguyên siêu kết nối và đảm bảo mỗi thiết bị có thể có một địa chỉ để cho phép giao tiếp end-to-end.

1.3. Lý do cần triển khai IPv6 only trong mạng truy cập

Triển khai mạng truy cập IPv6 only cho mạng truy cập để trải nghiệm và đánh giá về công nghệ, giải pháp, chuẩn bị sẵn sàng cho chuyển đổi toàn mạng. Đây là một bước quan trọng để chuẩn bị cho việc triển khai rộng rãi cho ứng dụng, dịch vụ hoạt động trên IPv6 only và đã được đề cập trong lộ trình “03 Giai đoạn – 10 bước” của chương trình IPv6 For Gov.

III	Giai đoạn 3 - Chuyển đổi		
8	Chuyển đổi IPv6 cho Trung tâm tích hợp dữ liệu	- Hệ thống mạng lõi, kết nối Internet; - Hệ thống DNS - Cổng thông tin điện tử và Cổng dịch vụ công trực tuyến. - Các dịch vụ Internet cơ bản: Email, phần mềm ứng dụng nội bộ ...	2022-2025
9	Chuyển đổi IPv6 cho kết nối WAN tới các đơn vị	- Mở rộng triển khai mạng LAN. - Thực hiện chuyển đổi hỗ trợ đồng thời IPv4/IPv6 cho mạng diện rộng (WAN) Bộ, Ngành, địa phương.	
10	Hoàn thiện chuyển đổi IPv6, thử nghiệm IPv6-only	- Chuyển đổi toàn bộ hệ thống công nghệ thông tin (IT) nội bộ. - Chuyển đổi các dịch vụ có kết nối Internet còn lại. - Thử nghiệm dịch vụ thuần IPv6, - Sẵn sàng triển khai mạng thuần IPv6.	

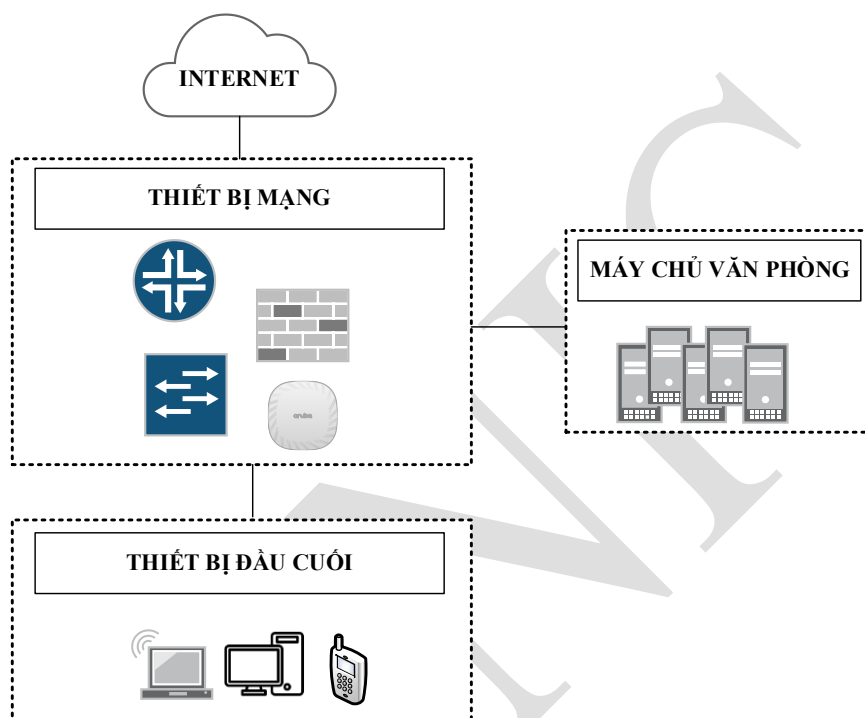
Hình 2: Nội dung thử nghiệm IPv6 only của chương trình IPv6 For Gov

Việc triển khai mạng truy cập IPv6 only sẽ đảm bảo hạ tầng mạng Internet của các đơn vị hoạt động hoàn toàn trên nền IPv6, loại bỏ dần sự phụ thuộc IPv4 và phù hợp xu thế quốc tế; Tạo nền tảng kết nối Internet hiện đại, ổn định, an toàn, sẵn sàng đáp ứng nhu cầu sử dụng dịch vụ công trực tuyến, dịch vụ số, dịch vụ đám mây và các công nghệ mới như 5G, IoT, AI; Tăng cường khả năng quản lý, bảo mật, giảm chi phí vận hành mạng nhờ loại bỏ các giải pháp tạm thời như NAT, Dual Stack; Nâng cao năng lực đội ngũ kỹ thuật, đảm bảo có khả năng tự chủ triển khai, vận hành, khai thác và duy trì hệ thống IPv6 only bền vững.

PHẦN 2: HẠ TẦNG VÀ CÁC YÊU CẦU KỸ THUẬT

2.1. Các thành phần trong mô hình mạng truy cập IPv6 only

Kiến trúc mạng truy cập mô tả cách tổ chức và kết nối các thành phần trong hệ thống mạng để cung cấp khả năng truy cập Internet hoặc dịch vụ khác cho người dùng cuối. Tùy theo mô hình triển khai, kiến trúc mạng truy cập có thể thay đổi nhưng thường bao gồm 03 thành phần chính như sau:



Hình 3: Các thành phần trong mạng truy cập Internet điển hình

- Thiết bị mạng là các thiết bị cung cấp kết nối giữa thiết bị đầu cuối đến mạng biên của nhà cung cấp dịch vụ, gồm:

- + Router: định tuyến gói tin trong mạng LAN và định tuyến gói tin ra Internet dựa theo thông tin địa chỉ IP nguồn, IP đích.

- + Firewall: kiểm soát truy cập giữa các phân mạng dựa theo thông tin địa chỉ IP nguồn, IP đích.

- + Switch: chuyển mạch gói tin trong mạng LAN, dựa theo địa chỉ MAC nguồn, MAC đích.

- + Access Point: phát sóng WIFI trong mạng không dây.

- Máy chủ văn phòng là máy chủ quản lý tài nguyên mạng, hỗ trợ người dùng kết nối, xác thực, phân quyền và truy cập các dịch vụ, gồm

+ Máy chủ AD: quản lý thông tin về người dùng, máy tính, thiết bị ... dưới dạng một cơ sở dữ liệu có cấu trúc phân cấp

+ Máy chủ DNS: phân giải tên miền thành địa chỉ IP tương ứng (resolver), giúp các thiết bị trong mạng có thể xác định và kết nối đến nhau dễ dàng trên Internet hoặc trong mạng nội bộ.

+ Máy chủ DHCP: Quản lý và cấp phát địa chỉ IP cho các thiết bị đầu cuối.

- Thiết bị đầu cuối: Là các thiết bị mà người dùng trực tiếp sử dụng để truy cập mạng, gồm máy tính, điện thoại, máy in

2.2. Các điều kiện cần thiết trước khi triển khai

a. Yêu cầu về thiết bị và hạ tầng mạng

Thông tin cụ thể về hỗ trợ NAT64 theo từng phiên bản hệ điều hành của các vendor giúp xác định chính xác những phiên bản nào có khả năng hỗ trợ và các tính năng liên quan. Dưới đây là chi tiết về hỗ trợ NAT64 theo phiên bản cho một số vendor phổ biến:

- Cisco: Cisco IOS XE, từ phiên bản IOS XE 15.2(4)S, Cisco ASA 9.0 và các phiên bản cao hơn hỗ trợ NAT64 bao gồm cả Stateful và Stateless. Đối với phiên bản IOS XE 3.x trở lên cũng hỗ trợ NAT64 nhưng tùy vào dòng sản phẩm và kiến trúc phần cứng cụ thể.

- Juniper Networks: Junos-OS 14.2 và cao hơn hỗ trợ cả Stateful và Stateless NAT64.

- Palo Alto Networks: PAN-OS 10.1 và cao hơn NAT64 được hỗ trợ, bao gồm cả Stateful và Stateless NAT64.

- Fortinet: Forti-OS 7.2.5 và cao hơn hỗ trợ NAT64 chủ yếu là Stateful NAT64..

Theo tiêu chuẩn RFC8200, kích thước MTU tối thiểu được yêu cầu đối với IPv6 là 1280 byte. Đây là kích thước tối thiểu của một gói tin IPv6, bao gồm cả

phần tiêu đề, dữ liệu và mọi liên kết trong mạng IPv6 phải hỗ trợ chuyển tiếp gói tin mà không cần phân mảnh.

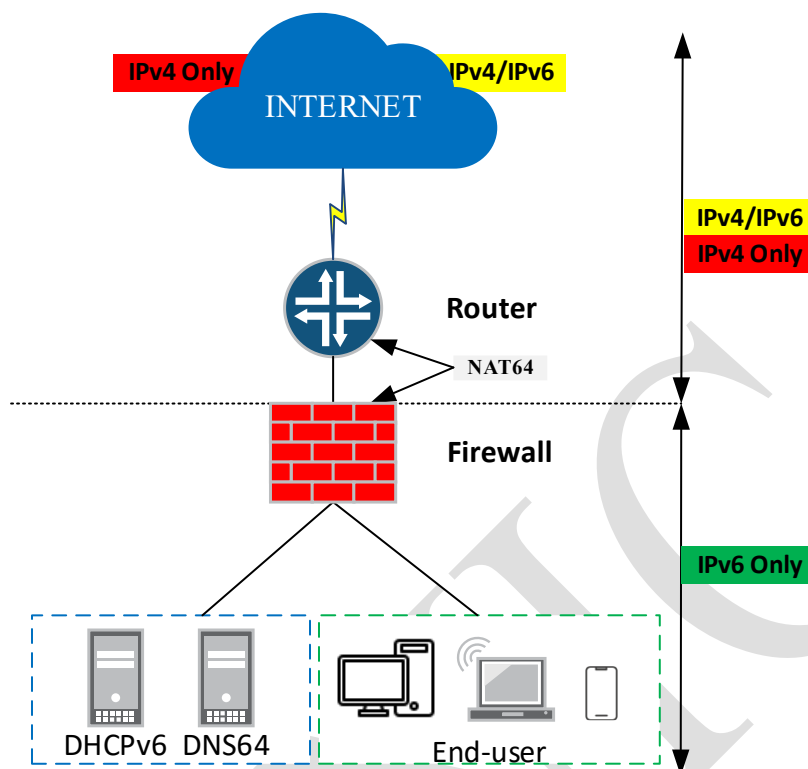
b. Yêu cầu về phần mềm, hệ điều hành

BIND là phần mềm DNS phổ biến nhất trên Internet và được phát hành bởi ISC (Internet System Consortium, <http://www.isc.org>). Phiên bản tối thiểu hỗ trợ DNS64: BIND 9.8.0 trở lên và khuyến nghị sử dụng BIND 9.11 trở lên (LTS) hoặc phiên bản mới nhất để đảm bảo bảo mật và hỗ trợ đầy đủ các tính năng DNS64. Tài nguyên máy chủ tối thiểu: CPU: 2 core; RAM: 2 GB; HDD: 50GB ; Hệ điều hành Ubuntu 24.04 LTS hoặc mới nhất

DHCP là một giao thức mạng thiết yếu, cho phép tự động cấp phát địa chỉ và các thông tin cấu hình mạng cho các thiết bị đầu cuối. Microsoft đã hỗ trợ DHCPv6 từ phiên bản Windows Server 2008, tuy nhiên để đảm bảo an toàn bảo mật khuyến nghị sử dụng các phiên bản Windows Server 2019 trở lên. Tài nguyên máy chủ tối thiểu: CPU: 2 core; RAM: 4 GB; HDD: 50GB.

PHẦN 3: MÔ HÌNH TRIỂN KHAI IPv6 ONLY

3.1. Mô hình mạng IPv6 only sử dụng DNS64/NAT64



Hình 4: Mô hình mạng IPv6 only sử dụng NAT64/DNS64

Thuyết minh, mô tả:

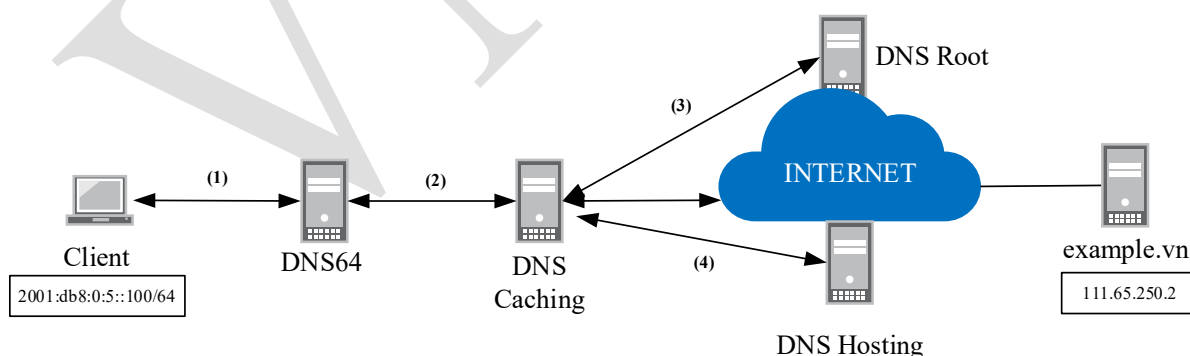
STT	Thành phần	Chức năng	Nguyên lý hoạt động
1	Thiết bị định tuyến (Router)	Định tuyến giữa các phân mạng và định tuyến ra Internet	- Router sử dụng giao thức định tuyến như: BGP, Static route,...kết nối với các ISP, VNIX để trao đổi thông tin định tuyến và lưu lượng mạng ra Internet trong nước, quốc tế. - Hỗ trợ song song cả IPv4, IPv6 (Dual Stack)
2	Thiết bị tường lửa (Firewall)	Thực hiện việc lọc gói tin và kiểm soát truy cập giữa các phân mạng.	- Hệ thống tường lửa phân chia mạng thành 2 phần: INSIDE và OUTSIDE. - Phía OUTSIDE kết nối lên thiết bị định tuyến và chạy Dual Stack - Phía INSIDE có thể phân chia thành các phân mạng IPv6 only. Mỗi phân mạng được kết nối đến 1 interface hoặc sub interface của tường lửa và gán tương ứng với 1 vlan.
3	Máy chủ DNS64	- Thực hiện chuyển tiếp truy vấn tên miền	- Trỏ forwarder về DNS Caching để phân giải tất cả zone tên miền - Bật chức năng DNS64

		- Ảnh xạ bản ghi A sang AAAA theo dải địa chỉ prefix	
4	Máy chủ DHCPv6	Quản lý và tự động cấp phát địa chỉ IPv6 cho thiết bị	- Thiết bị gửi yêu cầu đến máy chủ DHCPv6 để xin địa chỉ IPv6 và thông tin cấu hình mạng. Tường lửa sẽ thực hiện relay yêu cầu đến máy chủ DHCPv6. - Máy chủ DHCPv6 sẽ cấp phát địa chỉ cùng các thông số như DNSv6, thời gian tồn tại và ghi nhớ thiết bị để quản lý.

Triển khai mạng truy cập Internet IPv6 only sẽ thực hiện tại các thành phần: Thiết bị định tuyến/tường lửa (thực hiện NAT64), DNS64 (resolver). Tùy theo hiện trạng hệ thống để thực hiện việc quy hoạch, triển khai mới các máy chủ DNS hoặc sử dụng các máy chủ DNS64 Public của Trung tâm Internet Việt Nam. Để quản lý và cấp phát địa chỉ IPv6 cho thiết bị đầu cuối sẽ sử dụng SLAAC, tính năng trên các thiết bị định tuyến/tường lửa hỗ trợ IPv6 và RA để quảng bá thêm thông tin về máy chủ DNS. Ngoài ra có thể kết hợp thêm với máy chủ DHCPv6 trong việc quản lý và cấp phát địa chỉ IP. Lưu ý, thiết bị đầu cuối sử dụng hệ điều hành Android chưa hỗ trợ DHCPv6.

Dưới đây là mô tả về nguyên lý hoạt động của hệ thống, trong đó NAT64 sẽ được triển khai tại thiết bị tường lửa.

- Trường hợp giao tiếp giữa IPv6 only với IPv4 only



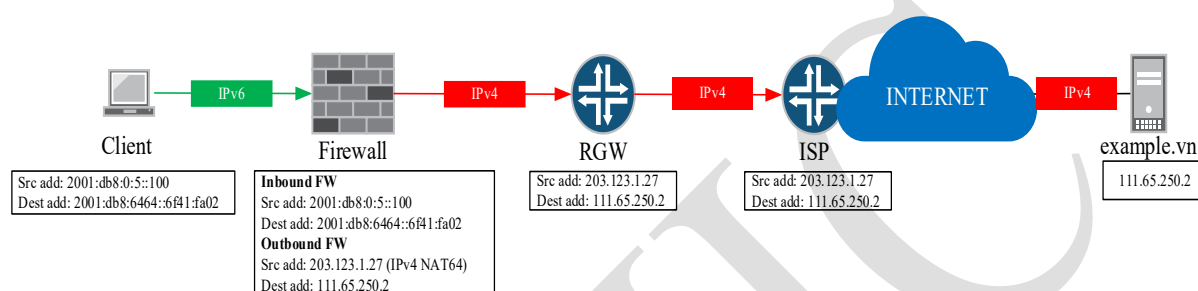
Hình 5: Quá trình client phân giải tên miền chỉ khai báo bản ghi A

+ **Bước 1:** Client gửi yêu cầu truy vấn tên miền website (vd: example.vn) đến DNS64.

+ **Bước 2:** DNS64 thực hiện truy vấn đệ quy, nếu trong local tồn tại bản ghi của tên miền website sẽ phản hồi, trường hợp không có sẽ forward truy vấn đến DNS caching.

+ **Bước 3, 4:** DNS Caching thực hiện truy vấn đệ quy để tìm ra câu trả lời cuối cùng (sẽ thực hiện truy vấn từ DNS Root đến DNS hosting).

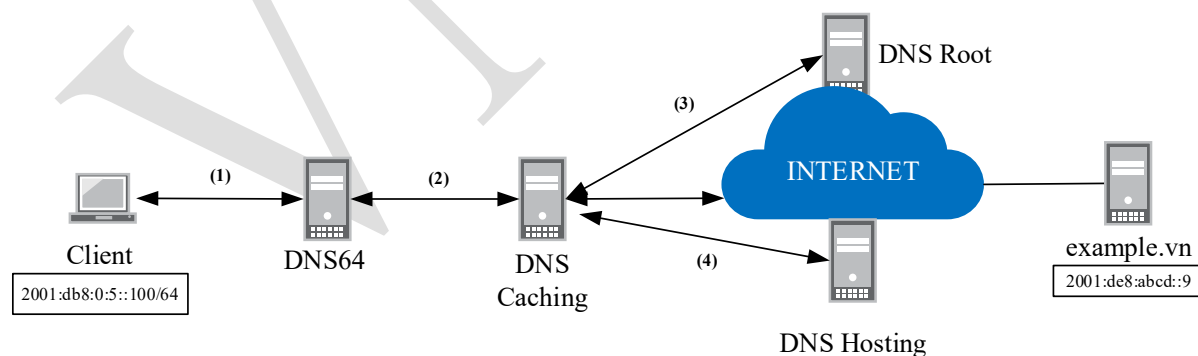
Vì kết quả truy vấn tên miền website chỉ có bản ghi A (IPv4), DNS64 sẽ thực hiện tổng hợp thành bản ghi AAAA với địa chỉ “IPv6 ảo“, sử dụng prefix 2001:dc8:6464::/96 (vd: 2001:dc8:6464::6f41:fa02).



Hình 6: Quá trình gửi gói tin client đến máy chủ dịch vụ web sử dụng IPv4

Dựa trên kết quả truy vấn ở trên, gói tin từ client IPv6 đến máy chủ IPv4 sẽ đi qua các hop lớp 3 được mô tả trong hình vẽ ở trên. Thiết bị tường lửa sẽ thực hiện NAT64 khi thấy gói tin đi vào (chiều từ client đến máy chủ) có địa chỉ IP đích thuộc dải NAT64 đã được định nghĩa thành địa chỉ IPv4 public để có thể giao tiếp được với máy chủ IPv4.

- Trường hợp giao tiếp giữa IPv6 only với IPv6 only

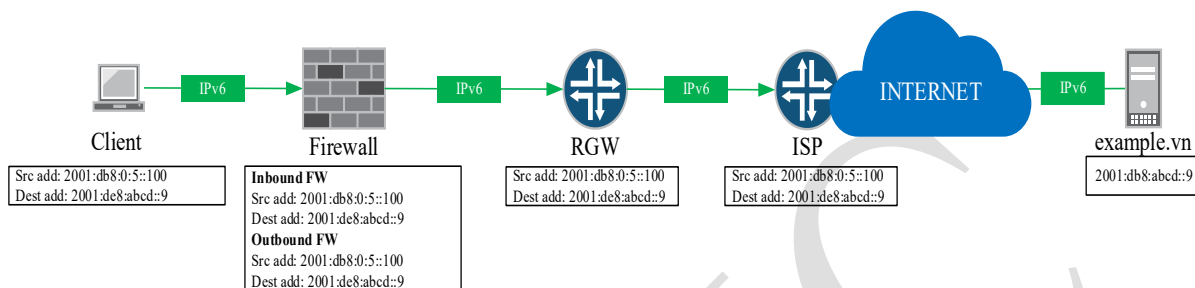


Hình 7: Quá trình client phân giải tên miền có khai báo bản ghi AAAA

+ **Bước 1:** Client gửi yêu cầu truy vấn tên miền website (vd: example.vn) đến DNS64.

+ **Bước 2:** DNS64 thực hiện truy vấn đệ quy, nếu trong local tồn tại bản ghi của tên miền website sẽ phản hồi, trường hợp không có sẽ forward truy vấn đến DNS caching.

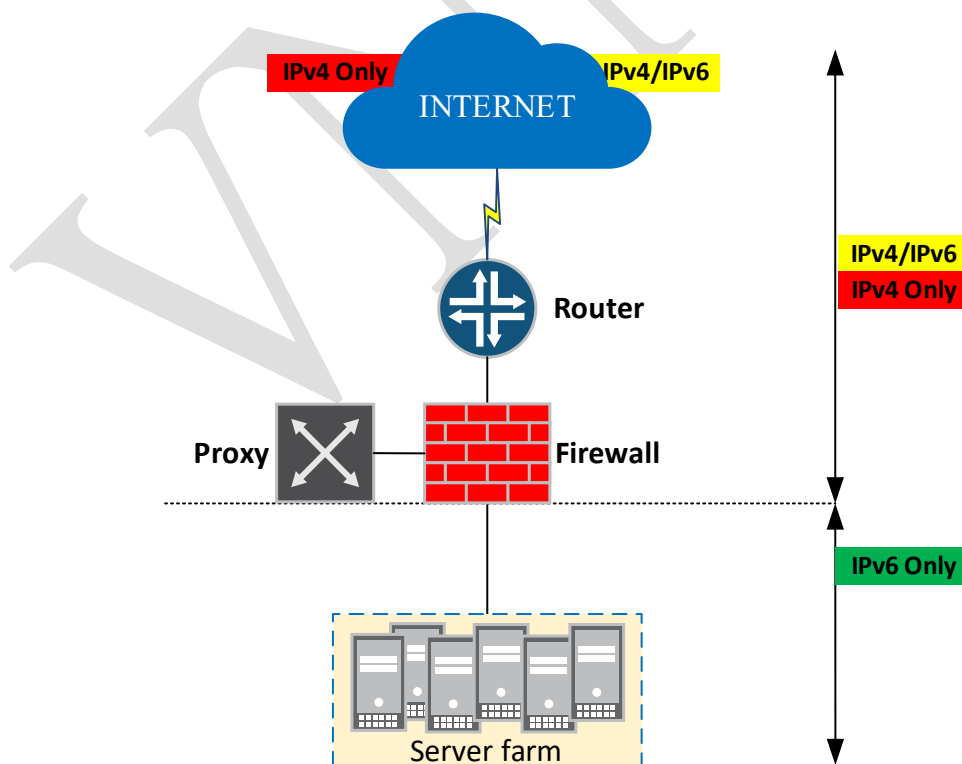
+ **Bước 3, 4:** DNS Caching thực hiện truy vấn đệ quy để tìm ra câu trả lời cuối cùng (sẽ thực hiện truy vấn từ DNS Root đến DNS hosting). Vì kết quả truy vấn tên miền website có bản ghi AAAA (IPv6) nên DNS64 sẽ trả kết quả này cho phía client.



Hình 8: Quá trình gửi gói tin client đến máy chủ dịch vụ web hỗ trợ IPv6

Dựa trên kết quả truy vấn ở trên, gói tin từ client IPv6 đến máy chủ IPv6 sẽ đi qua các hop lớp 3 được mô tả trong hình vẽ ở trên. Thiết bị tường lửa sẽ thực hiện chuyển tiếp gói tin đúng theo IPv6 nguồn đến IPv6 đích thông qua việc định tuyến thông thường đến Router và sẽ không thực hiện NAT64.

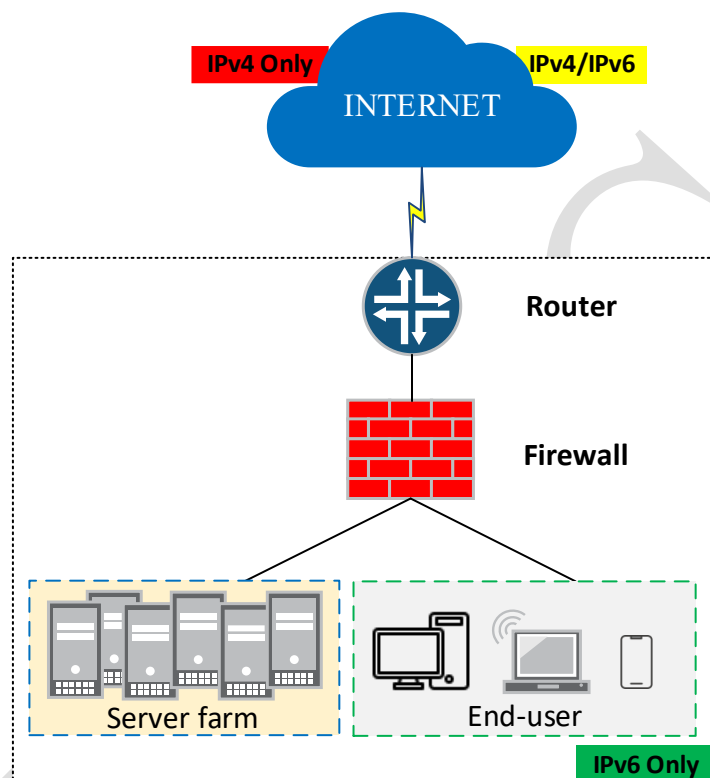
3.2. Mô hình mạng IPv6 only sử dụng Proxy Dual Stack



Hình 9: Mô hình mạng IPv6 only sử dụng Proxy

Trong mô hình này, toàn bộ máy chủ chỉ sử dụng địa chỉ IPv6 để kết nối và thông qua thiết bị Proxy trung gian đến truy cập các dịch vụ trên Internet chỉ hỗ trợ IPv4.

3.3. Mô hình mạng IPv6 native



Hình 10: Mô hình mạng native IPv6

Mô hình mạng IPv6 Native là một mạng mà trong đó tất cả các thiết bị, hệ thống và ứng dụng đều được cấu hình và hoạt động hoàn toàn dựa trên IPv6. Trong môi trường này, không có địa chỉ IPv4 nào được gán cho các giao diện mạng của thiết bị và không có sự phụ thuộc vào IPv4 để giao tiếp nội bộ. Đây là mục tiêu cuối cùng của quá trình chuyển đổi IPv6, nhằm thay thế hoàn toàn mạng IPv4 lỗi thời và giải quyết triệt để các hạn chế của nó. Các Router và thiết bị mạng chỉ cần duy trì các bảng định tuyến IPv6 và không sử dụng các giải pháp NAT, Tunnel giúp quá trình tra cứu và chuyển tiếp gói tin nhanh và hiệu quả.

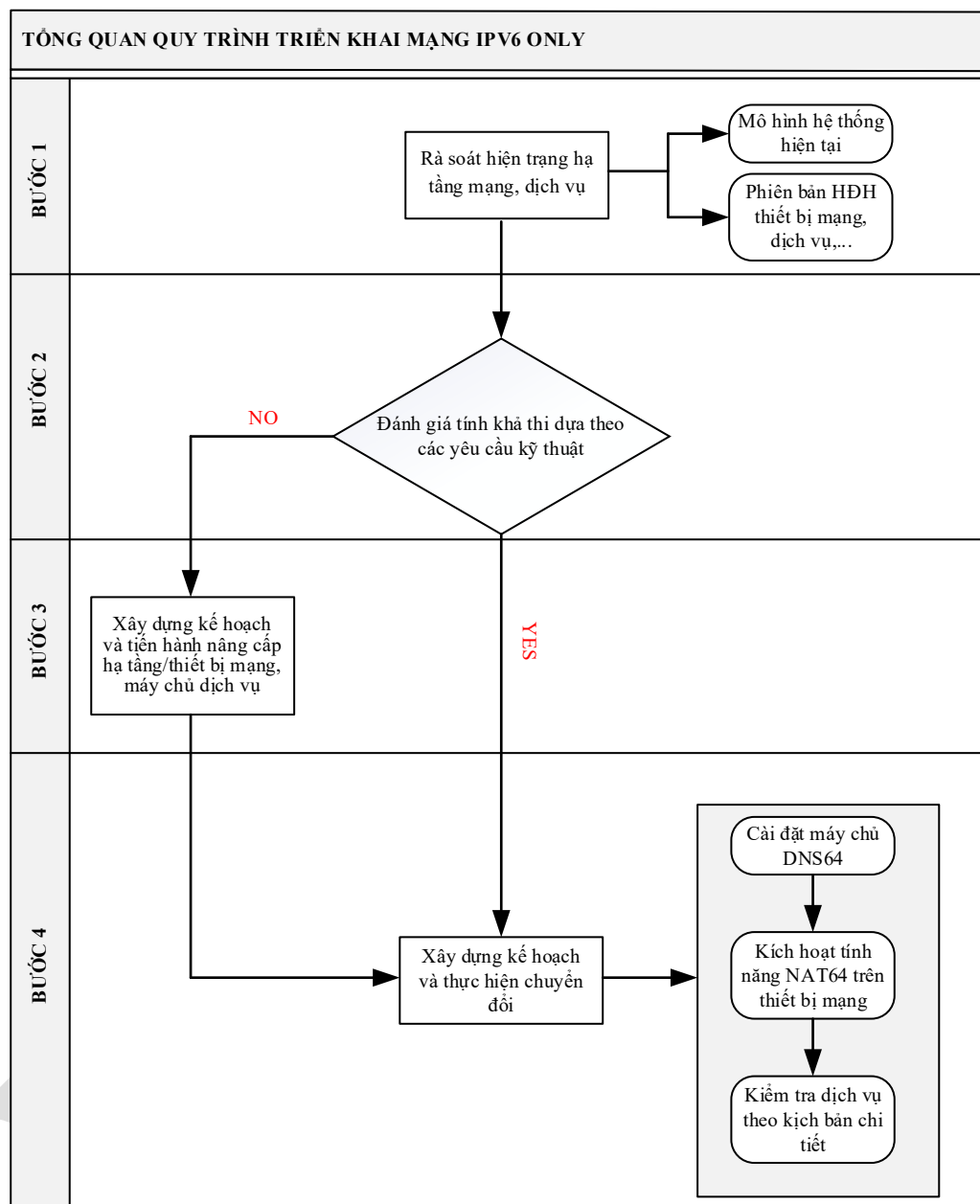
3.4. Đánh giá lựa chọn mô hình triển khai

Kể từ thời điểm ra mắt, việc triển khai IPv6 trên toàn cầu đã diễn ra theo xu hướng tăng dần và ổn định qua các năm. Dù tốc độ triển khai khác nhau giữa

các khu vực và tổ chức, nhưng tỷ lệ sử dụng IPv6 toàn cầu vẫn ghi nhận sự tăng trưởng liên tục, phản ánh sự chuyển dịch dần dần từ IPv4 sang IPv6. Tuy nhiên, việc triển khai mạng IPv6 only trong thời điểm quá độ không khả thi do vẫn tồn tại các ứng dụng dịch vụ trên mạng Internet chỉ sử dụng IPv4 dẫn tới phải triển khai thêm các giải pháp hỗ trợ kết nối giữa mạng IPv6 và IPv4. Dựa theo nghiên cứu về kinh nghiệm triển khai thực tế, giải pháp proxy phù hợp với mạng trung tâm dữ liệu để cung cấp dịch vụ ra bên ngoài và chỉ có một đơn vị triển khai thành công (Facebook) với phần mềm tự nghiên cứu phát triển. Đối với giải pháp NAT64/DNS64 đã được triển khai thành công trên thực tế bởi rất nhiều đơn vị, mặc khác các hãng sản xuất thiết bị cũng hỗ trợ tính năng trên các sản phẩm thương mại. Do đó, mô hình mạng IPv6 only sử dụng giải pháp NAT64/DNS64 phù hợp để triển khai cho mạng truy cập của CQNN, tổ chức và doanh nghiệp.

PHẦN 4: TRIỂN KHAI MẠNG TRUY CẬP IPV6 ONLY

4.1. Tổng quan quy trình triển khai



Hình 11: Tổng quan quy trình triển khai mạng truy cập IPv6 only

Giải thích quy trình:

+ **Bước 1:** Trước hết cần thực hiện rà soát hạ tầng mạng, dịch vụ; bao gồm mô hình hệ thống hiện tại, phiên bản hệ điều hành các thiết bị định tuyến, tường lửa, các thông số máy chủ DNS, DHCP,... đang được sử dụng để có thể nhìn một cách tổng quát về hệ thống hiện tại. Chi tiết tham khảo checklist rà soát hiện trạng hệ thống

+ **Bước 2:** Đánh giá mức độ ảnh hưởng và tính khả thi khi triển khai IPv6 only đối với hệ thống hiện tại dựa trên các thông số đã rà soát ở bước trên và các yêu cầu trước khi triển khai.

- Nếu hệ thống chưa đáp ứng được các yêu cầu trước khi triển khai IPv6 only thì chuyển sang Bước 3.
- Nếu hệ thống hoàn toàn có thể đáp ứng mọi yêu cầu, chuyển sang Bước 4.

+ **Bước 3:** Xây dựng kế hoạch và tiến hành nâng cấp hạ tầng/thiết bị mạng, máy chủ dịch vụ để đáp ứng các yêu cầu đặt ra, và chuyển qua Bước 4

+ **Bước 4:** Xây dựng kế hoạch và thực hiện chuyển đổi. Trong bước này sẽ thực hiện chi tiết các công việc, và kiểm tra hoạt động của các dịch vụ cơ bản theo kịch bản. Chi tiết tham khảo checklist kiểm tra dịch vụ

4.2. Hướng dẫn kỹ thuật chi tiết

a, Cài đặt máy chủ DNS64

- **Bước 1:** Cấu hình địa chỉ IP cho máy chủ

```
#sudo nano /etc/netplan/50-cloud-init.yaml
```

Ví dụ:

```
network:
  ethernets:
    ens160:
      dhcp4: no
      dhcp6: no
      addresses:
        - 192.109.0.64/24
        - 1001:db8:a:b:c::6464/64
      routes:
        - to: default
          via: 192.109.0.1
        - to: default
          via: 1001:db8:0::1
      version: 2
```

- **Bước 2:** Cấu hình hostname cho máy chủ

```
#sudo hostnamectl set-hostname <Tên máy chủ>
```

- **Bước 3:** Cấu hình múi giờ & đồng bộ thời gian cho máy chủ

```
#sudo timedatectl set-timezone Asia/Ho_Chi_Minh
#sudo apt install systemd-timesyncd -y (nếu chưa có)
```

```
#sudo systemctl status systemd-timesyncd
#sudo systemctl start systemd-timesyncd
#sudo systemctl enable systemd-timesyncd
```

- **Bước 4:** Cập nhật package hệ điều hành

```
#sudo apt update && apt upgrade
```

- **Bước 5:** Cài đặt phần mềm cơ bản

```
#sudo apt install net-tools traceroute snmp snmpd
```

- **Bước 6:** Cài đặt Bind9

```
#sudo apt install bind9 bind9utils bind9-doc
```

- **Bước 7:** Tạo folder ghi log truy vấn

```
# cd /etc/bind/
#sudo mkdir logs
#sudo chmod 777 logs
#sudo cd logs
#sudo touch log_query
#sudo chmod 664 log_query
```

- **Bước 8:** Thiết lập file cấu hình dịch vụ DNS trên Bind9

```
#sudo nano /etc/bind/named.conf.options
```

Ví dụ:

```
acl clients {                                //Định nghĩa danh sách client được truy vấn đến
    localhost;
    1001:db8:0:1::/64;
    1001:db8:0:2::/64;
};

options {
    directory "/var/cache/bind";
    forwarders {
        1001:abcd:1:2::100;                //Định nghĩa máy chủ DNS Cache để chuyển tiếp
        1001:cafe:1:2::100;                //Khuyến nghị sử dụng tối thiểu 02 máy chủ để dự phòng
    };
    forward only;
    listen-on { none; };                    //Tắt nhận truy vấn từ client đến IPv4 của máy chủ
    listen-on-v6 { 1001:db8:a:b:c::6464; }; //Định nghĩa IPv6 nhận truy vấn từ client
    allow-query { clients; };               //Cho phép client thuộc danh sách được phép truy vấn
    dns64 64:ff9b::/96 {};                 //Định nghĩa dải tiền tố IPv6 để synthesizing và NAT64
    recursion yes;                          //Bật cho phép truy vấn đệ quy
    dnssec-validation no;                   //Tắt chức năng DNSSEC
    max-cache-size 256M;                    //Đặt giới hạn cache theo năng lực máy chủ
};

logging {
    channel log_query {
        file "/etc/bind/logs/log_query" versions 50 size 100m; //Đặt giới hạn 50 phiên bản file
        log với kích thước mỗi file là 100MB
        severity info;
    };
};
```

```
print-category yes;  
print-severity yes;  
print-time yes;  
};  
category "queries" { "log_query"; };  
};
```

- **Bước 9:** Khởi động lại dịch vụ Bind9 và kiểm tra log truy vấn, trạng thái máy chủ

```
#sudo systemctl restart bind9  
#sudo systemctl status bind9  
#tail -f /etc/bind/logs/log_query
```

b, Triển khai tính năng stateful NAT64 trên thiết bị mạng

Đối với thiết bị định tuyến Cisco

- **Bước 1:** Bật chức năng NAT64 trên Interface

```
Router(config)#interface <tên cổng>  
Router(config-if)#nat64 enable
```

- **Bước 2:** Cấu hình dải địa chỉ IPv6 muốn NAT64

```
Router(config)#ipv6 access-list <tên ACL>  
Router(config-ipv6-acl)#permit ipv6 <dải địa chỉ IPv6> any
```

- **Bước 3:** Cấu hình dải địa chỉ IPv6 DNS64 (nếu không có sẽ tự động sử dụng well-known Prefix: 64:FF9B::/96)

```
Router(config)#nat64 prefix stateful <dải địa chỉ IPv6/96>
```

- **Bước 4:** Cấu hình dải địa chỉ IPv4 Public

```
Router(config)#nat64 v4 pool <tên pool> <IP bắt đầu> <IP kết thúc>
```

- **Bước 5:** Cấu hình dynamic NAT64

```
Router(config)#nat64 v6v4 list <tên ACL IPv6> pool <tên pool> overload
```

- **Bước 6:** Kiểm tra trạng thái bảng NAT

```
Router#show nat64 translations  
Router#show nat64 statistics
```

Đối với thiết bị tường lửa Cisco

- **Bước 1:** Cấu hình dải địa chỉ IPv6 DNS64

```
FW-ASA(config)#object network <tên object IPv6 DNS64>  
FW-ASA(config-network-object)#subnet <dải địa chỉ IPv6/96>
```

- **Bước 2:** Cấu hình mapping từ IPv4 bên ngoài vào IPv6 DNS64

```
FW-ASA(config)#object network <tên object IPv4 internet>  
FW-ASA(config-network-object)#subnet 0.0.0.0 0.0.0.0  
FW-ASA(config-network-object)#nat(<Zone Outside>,<Zone Inside>) static <tên object IPv6 DNS64> dns
```

- **Bước 3:** Cấu hình dải địa chỉ IPv4 Public

```
FW-ASA(config)#object network <tên object IPv4 public>
```

```
FW-ASA(config-network-object)#subnet <địa chỉ IPv4> <Subnet mask>
```

- Bước 4: Cấu hình dynamic NAT64

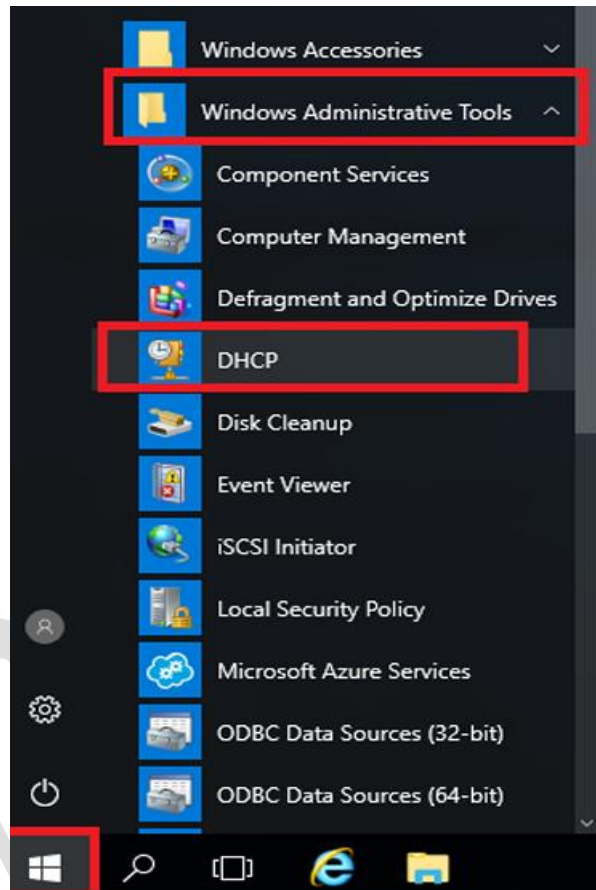
```
FW-ASA(config)#object network <tên object IPv6 cần NAT64>
```

```
FW-ASA(config-network-object)#subnet <dải địa chỉ IPv6>
```

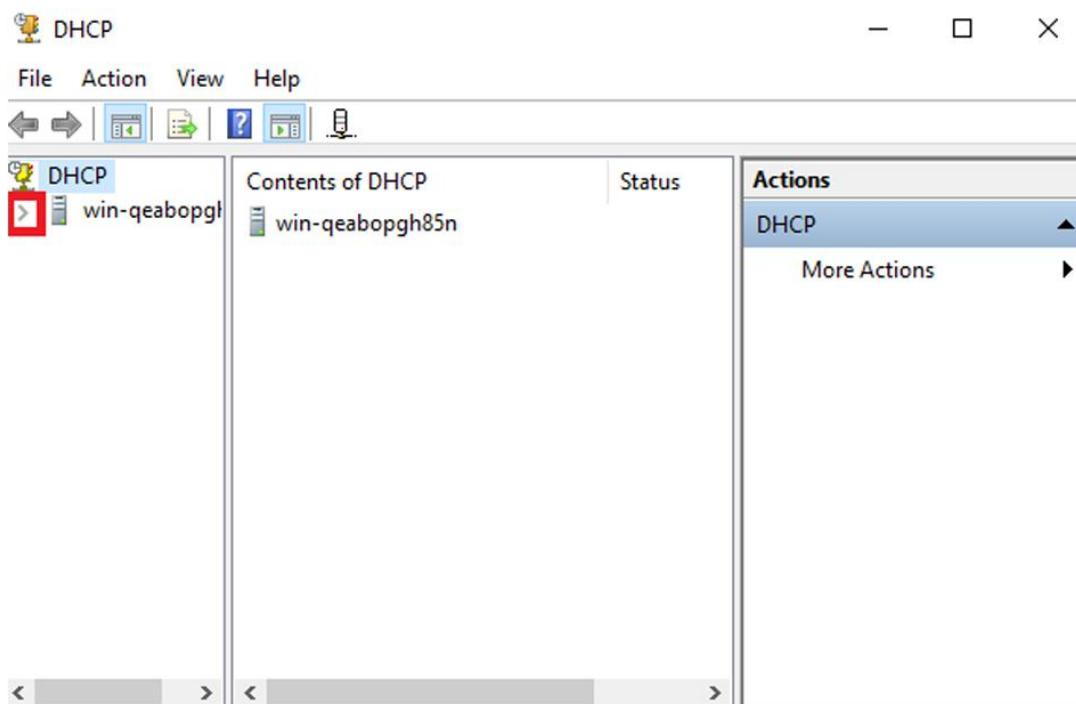
```
FW-ASA(config-network-object)#nat (<Zone Inside>, <Zone Outside>) dynamic <tên object IPv4 public>
```

c, Cấu hình máy chủ DHCPv6

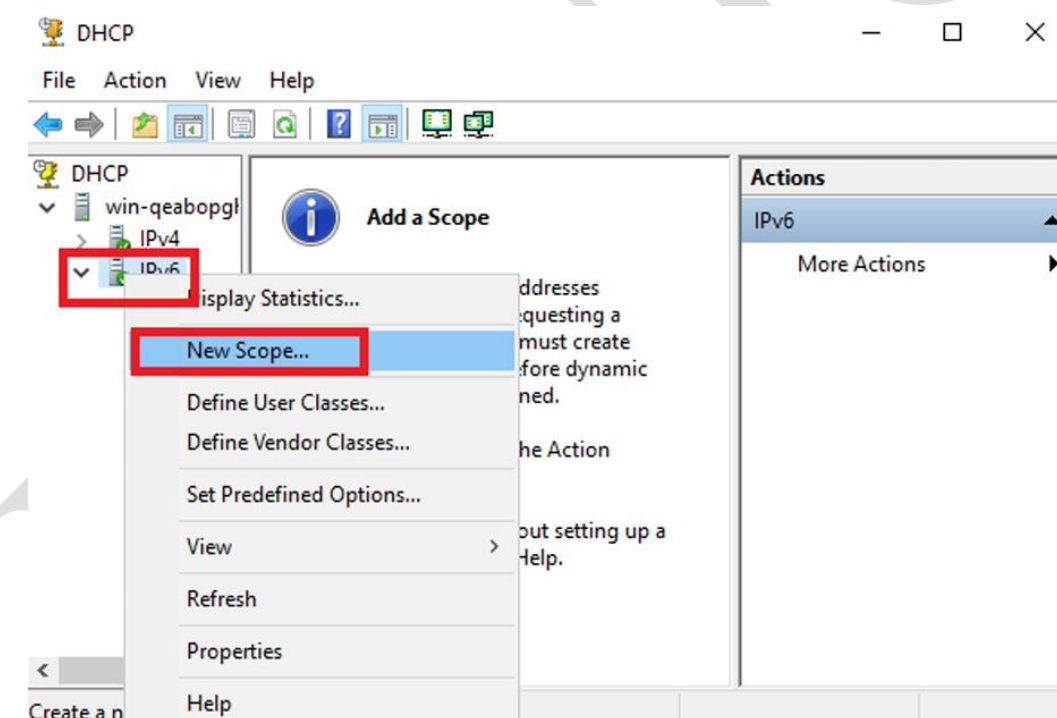
- **Bước 1:** Logon đến máy chủ server với quyền administrator.
- **Bước 2:** Click vào Start | Windows Administrator Tools | DHCP



Nhấn vào dấu “>” bên cạnh tên của máy chủ



- **Bước 3:** Chuột phải vào IPv6 và chọn “New scope”



Nhấn vào “Next” và cung cấp tên cho Scope

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

- Bước 4: Nhập phạm vi tiền tố (Scope prefix), vd: 2407:100:100:1::/64

New Scope Wizard

Scope Prefix

You have to provide a prefix to create the scope. You also have the option of providing a preference value for the scope.



Enter the IPv6 Prefix for the addresses that the scope distributes and the preference value for the scope.

Prefix: /64

Preference:

Loại trừ một dải địa chỉ IP cho địa chỉ IP tĩnh, vd: dải địa chỉ 0000 đến 00ff

New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IPv6 address range that you want to exclude for the given scope. If you want to exclude a single address, type an identifier in Start IPv6 Address only.

Start IPv6 Address: 2407:100:100:1:

End IPv6 Address: 2407:100:100:1:

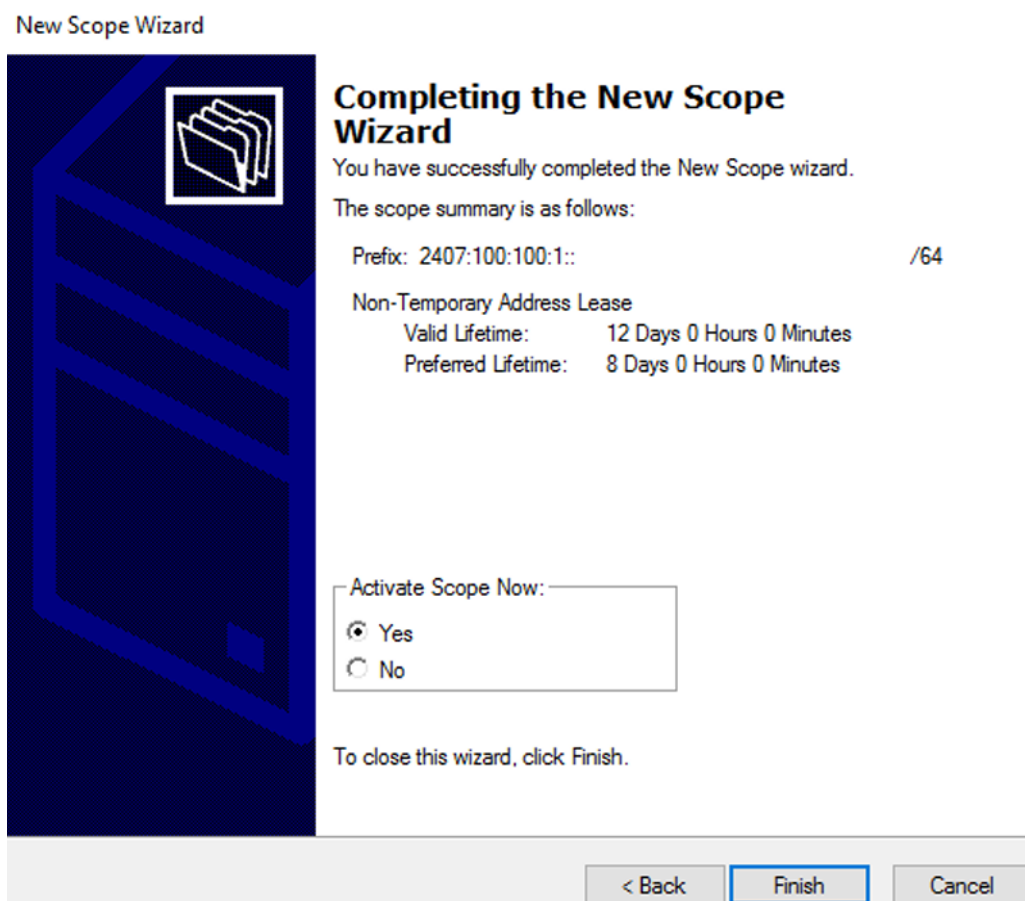
Add

Excluded address range:

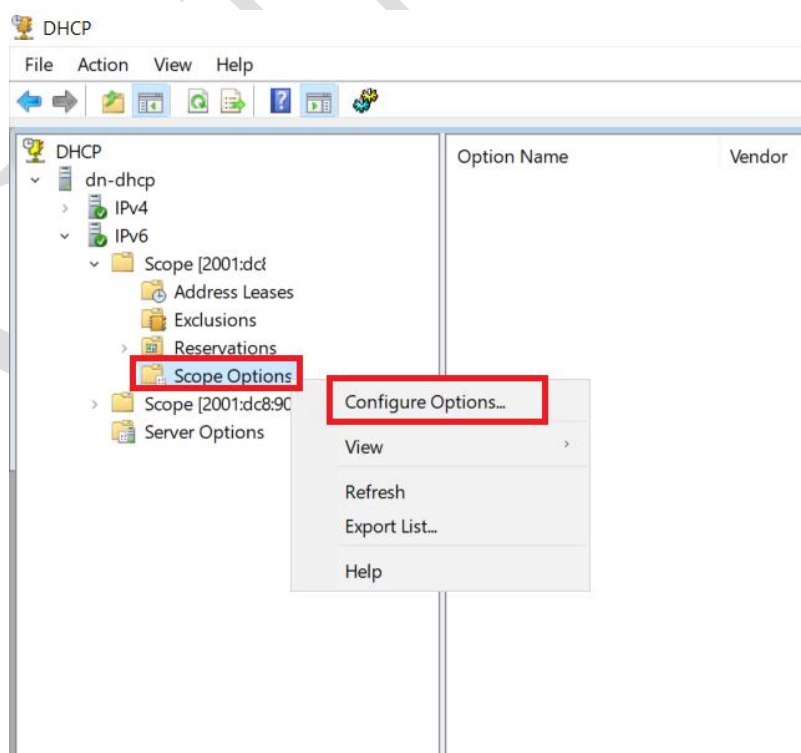
2407:100:100:1:: to 2407:100:100:1:ff

Remove

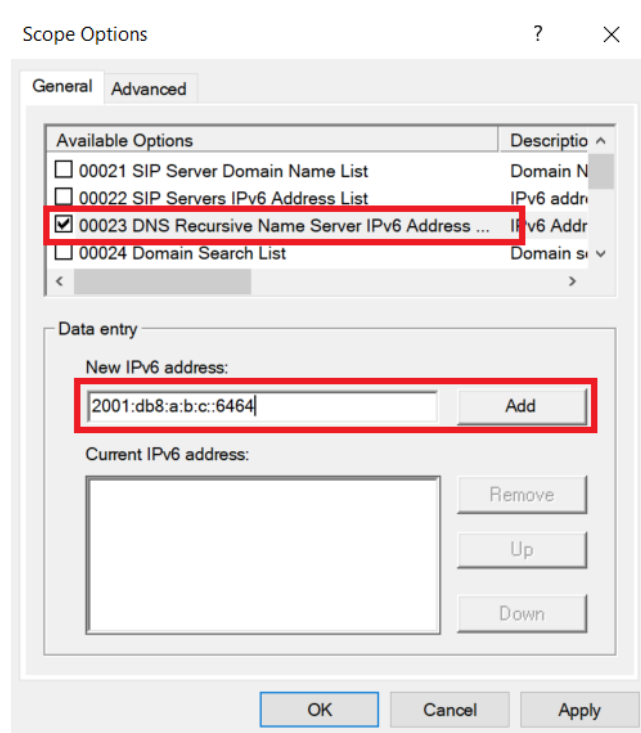
- Bước 5: Nhấn Finish để hoàn thành cấu hình và active scope vừa tạo



- **Bước 6:** Chuột phải vào Scope Option và chọn “Configure Options”



Tick vào DNS Recursive Name Server Ipv6 Address và nhập thông tin các máy chủ DNS64 rồi nhấn “OK”

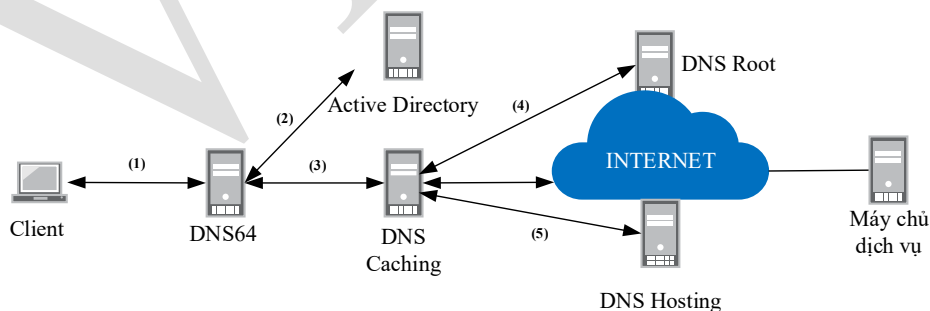


Sau khi hoàn tất triển khai, tham khảo checklist tại phụ lục để kiểm tra dịch vụ.

4.3. Các vấn đề thường gặp và giải pháp

a. Phân giải DNS

Thực tế triển khai sẽ có trường hợp một số vùng (zone) tên miền nội bộ đang được quản lý bởi hệ thống khác, ví dụ: Máy chủ DNS thuộc Active Directory. Vì vậy cần cấu hình cụ thể zone tên miền nội bộ sẽ được phân giải trên máy chủ DNS nội bộ để đảm bảo truy vấn thành công.



Hình 12: Mô hình chuyển tiếp truy vấn từ DNS64 đến các máy chủ DNS khác

Dưới đây là hướng dẫn bổ sung thiết lập file cấu hình dịch vụ DNS trên Bind9.

```
#sudo nano /etc/bind/named.conf.default-zones
```

Ví dụ:

```
view "local-ad" {           //Định nghĩa tên của view
    zone "local.domain.vn" { //Định nghĩa cụ thể zone tên miền cần chỉ định truy vấn
        type forward;
        forward only;
        forwarders {
            192.111.0.21;    //Định nghĩa máy chủ DNS sẽ tiếp nhận và phân giải
            192.111.0.22;    //Nếu có 02 máy chủ DNS thì cấu hình để dự phòng
        };
    };
};
```

b. Captive portal trên WIFI công cộng

Captive portal là một cơ chế kiểm soát truy cập mạng, thường được sử dụng trong các hệ thống WIFI công cộng như quán cà phê, khách sạn, sân bay, trường học hoặc doanh nghiệp, nhằm chặn người dùng truy cập Internet cho đến khi họ hoàn thành một hành động xác thực nhất định qua trình duyệt web. Sau khi nhận được địa chỉ IP, hầu hết các hệ điều hành trên thiết bị đầu cuối đều có một tính năng tích hợp gọi là Captive Network Assistant (CNA). Tính năng này được thiết kế để tự động phát hiện xem có Captive Portal hay không và bật lên trang đăng nhập cho người dùng. CNA hoạt động bằng cách gửi một yêu cầu HTTP/HTTPS đến một URL cụ thể được định nghĩa sẵn trong hệ điều hành. Nếu yêu cầu này bị chuyển hướng thì hệ điều hành sẽ xác định rằng có một captive portal đang hoạt động. Đối với hệ điều hành Windows của Microsoft sẽ sử dụng URL <http://www.msftconnecttest.com/redirect>. Tuy nhiên, qua thử nghiệm khi các thiết bị hoạt động trong mạng IPv6 only không thể phân giải domain www.msftconnecttest.com dẫn đến không thể chuyển hướng đến Captive Portal của WIFI công cộng. Để xử lý vấn đề trên cần thực hiện khai báo bổ sung zone tên miền msftconnecttest.com cục bộ trên DNS64. Sau đây là hướng dẫn bổ thiết lập file cấu hình dịch vụ DNS trên Bind9.

```
#sudo nano /etc/bind/named.conf.default-zones
```

Ví dụ:

```
view "local-CNA" {           //Định nghĩa tên của view
    zone "msftconnecttest.com" { //Định nghĩa cụ thể zone tên miền cần chỉ định truy vấn
        type master;
        file "/etc/bind/db.msftconnecttest"; //Định nghĩa file chứa các bản ghi của zone
    };
};
```

```
};  
};
```

Tạo file chứa giá trị bản ghi

```
#sudo nano /etc/bind/db.msftconnecttest
```

Ví dụ:

```
$TTL 86400  
@ IN SOA admin.msftconnecttest.com. root.msftconnecttest.com. (  
    20240218 ; Serial  
    3600     ; Refresh  
    1800     ; Retry  
    604800   ; Expire  
    86400 )  ; Minimum TTL  
@ IN NS ns1.msftconnecttest.com.  
www IN AAAA 1001:a:b:c:d::100 //Địa chỉ IPv6 của Captive Portal  
ns1 IN AAAA 1001:db8:a:b:c::6464 //Địa chỉ IPv6 của DNS64
```

c. Thiết bị đầu cuối không nhận được IPv6

Vấn đề trên xảy ra trên các thiết bị di động sử dụng hệ điều hành Android hoạt động trong mạng truy cập IPv6 only sử dụng DHCPv6. Nguyên nhân do hệ điều hành Android chưa hỗ trợ đầy đủ các tiêu chuẩn theo RFC3315 (DHCPv6) nên phải chuyển sang sử dụng giải pháp cấp địa chỉ IPv6 thông qua SLAAC trên các thiết bị mạng hỗ trợ IPv6.

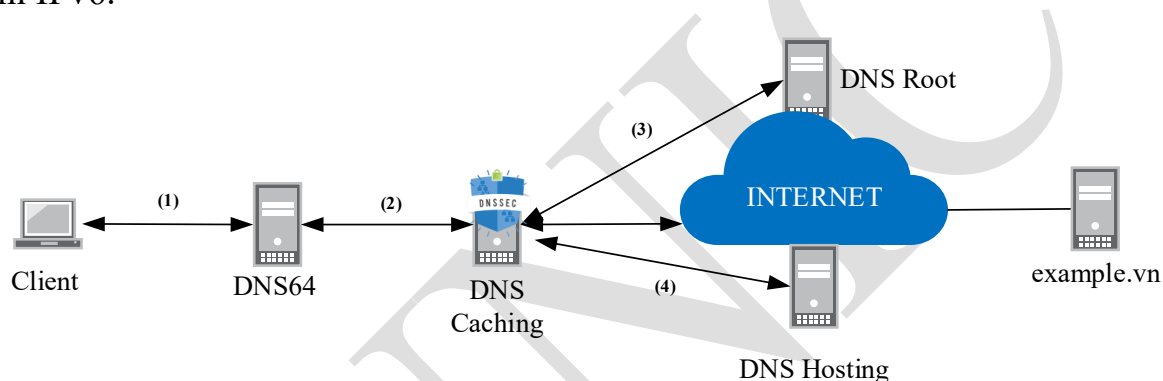
d. Trình duyệt không truy cập được một số trang

Thực tế triển khai sẽ có trường hợp một số trang web không thể truy cập từ trình duyệt trên máy tính sử dụng hệ điều hành Windows nhưng khi truy cập trên trình duyệt thiết bị di động (Android, iOS) bình thường. Nguyên nhân chính liên quan đến vấn đề trên là tên miền của website đã khai báo bản ghi AAAA (IPv6) nhưng máy chủ dịch vụ web không hoạt động trên IPv6 nên giải pháp NAT64/DNS64 không hoạt động và Microsoft chưa hỗ trợ CLAT trên hệ điều hành Windows dẫn đến không thể tự chuyển sang IPv4 để kết nối. Giải pháp tạm thời cho vấn đề trên là liên hệ đơn vị chủ quản kiểm tra lại dịch vụ web trên IPv6 hoặc xóa bản ghi AAAA để sử dụng giải pháp NAT64/DNS64 khi kết nối.

4.4. Bảo mật cơ bản trên IPv6

a. Mô hình DNS64 kết hợp với DNSSEC

DNS64 có thể hoạt động cùng với DNSSEC để đảm bảo rằng các bản ghi AAAA được tạo ra từ các bản ghi A cũng được xác thực. Điều này giúp đảm bảo rằng máy khách IPv6 nhận được thông tin chính xác và an toàn. Khi DNSSEC được triển khai, các bản ghi DNS64 mà được tạo ra cần phải được ký và xác thực để đảm bảo tính toàn vẹn của thông tin nếu không sẽ không thể trả kết quả về cho máy khách IPv6 đang truy vấn. Để đơn giản hoá việc triển khai, DNS64 thường cần được triển khai “nằm phía sau” các máy chủ DNS Caching (bật chức năng DNSSEC) nên sẽ không cần phải bật chức năng DNSSEC để xác thực giá trị bản ghi mà sẽ tập trung vào việc giải quyết vấn đề khi các tên miền không hỗ trợ bản ghi IPv6.



Hình 13: Mô hình nguyên lý phân giải tên miền DNS64 kết hợp DNSSEC

b. Cấu hình bảo mật dịch vụ

Cấu hình bảo mật dịch vụ là quá trình thiết lập và duy trì các cài đặt, chính sách và biện pháp kiểm soát an ninh trên các dịch vụ (ví dụ: máy chủ DNS, DHCP,...) nhằm giảm thiểu rủi ro, ngăn chặn truy cập trái phép, bảo vệ dữ liệu và đảm bảo tính sẵn sàng của dịch vụ. Mục tiêu chính là giảm thiểu các lỗ hổng mà kẻ tấn công có thể khai thác. Tùy thuộc theo hiện trạng hệ thống có thể sử dụng các thiết bị tường lửa chuyên dụng hoặc tường lửa hệ điều hành để triển khai chính sách an toàn bảo mật. Dưới đây là hướng dẫn triển khai trên tường lửa hệ điều hành linux

- Bước 1: Cập nhật package hệ điều hành

```
#sudo apt update && apt upgrade
```

- **Bước 2:** Cài đặt tường lửa hệ điều hành và cấu hình chính sách kiểm soát truy cập

```
#sudo apt install iptables-persistent
```

- **Bước 3:** Cấu hình chính sách kiểm soát truy cập. Tham khảo chi tiết danh sách công dịch vụ tại phụ lục

```
#iptables -A INPUT -s <địa chỉ IP nguồn> -p <tcp/udp> -m <tcp/udp> --dport <port đích> -j <ACCEPT/DROP>
#ip6tables -A INPUT -s <địa chỉ IP nguồn> -p <tcp/udp> -m <tcp/udp> --dport <port đích> -j <ACCEPT/DROP>
#cat /etc/iptables/rules.v4
#cat /etc/iptables/rules.v6
```

Ví dụ: Rule ipv4

```
#cat /etc/iptables/rules.v4
#Created by VNNIC's Network Team
*filter
:INPUT DROP [0:0] //Mặc định drop gói tin
:FORWARD DROP [0:0] //Mặc định drop gói tin
:OUTPUT DROP [0:0] //Mặc định drop gói tin
### Inbound
# SSH Protocol
-A INPUT -s 192.168.1.0/24 -d 192.101.1.64/32 -p tcp -m tcp --dport 22 -j ACCEPT
# SNMP Protocol
-A INPUT -s 192.168.10.100/32 -d 192.101.1.64/32 -p udp -m udp --dport 161 -j ACCEPT
# ICMP Protocol
-A INPUT -s 192.168.10.100/32 -d 192.101.1.64/32 -p icmp -m icmp --icmp-type 8 -j ACCEPT
# RND C Bind
-A INPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT
-A OUTPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT
# Disable ICMP timestamp
-A INPUT -d 192.101.1.64/32 -p icmp --icmp-type timestamp-request -j DROP
-A OUTPUT -s 192.101.1.64/32 -p icmp --icmp-type timestamp-reply -j DROP
# Stateful Firewall
-A INPUT -d 192.101.1.64/32 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
### Outbound
-A OUTPUT -d 192.168.1.0/16 -j ACCEPT
### Default
-P INPUT DROP
-P OUTPUT DROP
-P FORWARD DROP
COMMIT
```

Ví dụ: Rule ipv6

```
#cat /etc/iptables/rules.v6
#Created by VNNIC's Network Team
*filter
:INPUT DROP [0:0] //Mặc định drop gói tin
:FORWARD DROP [0:0] //Mặc định drop gói tin
:OUTPUT DROP [0:0] //Mặc định drop gói tin
### Inbound
# ICMPv6-ND
-A INPUT -p ipv6-icmp -j ACCEPT
-A OUTPUT -p ipv6-icmp -j ACCEPT
```

```

-A INPUT -d ff00::/8 -j ACCEPT
-A OUTPUT -d ff00::/8 -j ACCEPT
#SNMP Protocol
-A INPUT -s 1001:a:b:cafe:10::100 -d 1001:a:b:c::6464 -p udp -m udp --dport 161 -j
ACCEPT
#Public-DNS
-A INPUT -s 1001:a:b::/48 -d 2001:a:b:c::6464 -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -s 1001:a:b::/48 -d 2001:a:b:c::6464 -p udp -m udp --dport 53 -j ACCEPT
# Stateful Firewall
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
### Outbound
-A OUTPUT -d 1001:a:b::/48 -j ACCEPT

### Default
-P INPUT DROP
-P OUTPUT DROP
-P FORWARD DROP
COMMIT

```

- **Bước 4:** Khởi động lại dịch vụ tường lửa để kích hoạt chính sách kiểm soát truy cập

```

#sudo systemctl restart iptables
#sudo systemctl restart ip6tables

```

- **Bước 5:** Kiểm tra trạng thái tường lửa hệ điều hành và chính sách kiểm soát truy cập

```

#sudo systemctl status iptables

```

Mặc định hệ điều hành Ubuntu sử dụng tất cả các thuật toán hàm băm SSH, trong đó có những phiên bản đã cũ và bị khai thác lỗ hổng. Vì vậy cần định nghĩa cụ thể các phiên bản mới để đảm bảo quản trị truy cập từ xa.

```

#sudo nano /etc/ssh/sshd_config
# Security Hardening by VNNIC's Network Team
MACs hmac-sha2-512,hmac-sha2-256
Ciphers aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr
KexAlgorithms curve25519-sha256,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-
nistp256
ClientAliveInterval 300
ClientAliveCountMax 0

```

PHỤ LỤC

1. Danh mục tài liệu tham khảo, liên hệ hỗ trợ kỹ thuật

a. Tài liệu tham khảo

- [1] Căn cứ theo quyết định số 38/QĐ-BTTTT ngày 14/01/2021 phê duyệt “Chương trình thúc đẩy, hỗ trợ chuyển đổi IPv6 cho cơ quan nhà nước giai đoạn 2021-2025”
- [2] Căn cứ theo quyết định số 306/QĐ-BKHCN ngày 28/03/2025 phê duyệt “Kế hoạch thúc đẩy chuyển đổi IPv6, IPv6 for gov năm 2025”
- [3] Hướng dẫn cấu hình trên thiết bị Cisco: [Link tham khảo](#)
- [4] Hướng dẫn cấu hình trên thiết bị Juniper: [Link tham khảo](#)
- [5] Hướng dẫn cấu hình trên thiết bị Palo Alto: [Link tham khảo](#)

b. Thông tin liên hệ, hỗ trợ

Trong quá trình triển khai mạng IPv6 only nếu cần hỗ trợ hoặc tư vấn các đơn vị có thể liên hệ đầu mối của VNNIC theo thông tin sau:

- Phòng Hợp tác - Quản lý tài nguyên, Trung tâm Internet Việt Nam (Email: info@vnnic.vn, Điện thoại: 024-35564944 số máy lẻ 102).
- Bộ phận quản trị mạng: Email mang-admin@vnnic.vn; Điện thoại: 024-35564944 số máy lẻ 905.

2. Checklist rà soát, đánh giá hiện trạng hệ thống trước khi triển khai

STT	THÔNG TIN			
1	Đối tượng	Cơ quan nhà nước		Doanh nghiệp
2	Loại hình kết nối mạng	FTTH	Leased line	IP/ASN độc lập
3	Thông tin kết nối	IPv4 only	Dual Stack	IPv6 only
	a. IPv4 Prefix			
	b. IPv6 Prefix			
	c. ASN (nếu có)			
4	Phương pháp gán tiền tố IPv6	SLAAC	DHCPv6	Manual
5	Thông tin thiết bị/máy chủ	Computer	Mobile Phone	Khác:
	a. Phiên bản hệ điều hành	ví dụ: Windows 11		
	b. Phiên bản ứng dụng	ví dụ: Chrome 136.0.7103.114		

3. Checklist về kiểm tra dịch vụ sau khi triển khai

- Checklist tương thích thiết bị đầu cuối

TT	Thiết bị	Hệ điều hành	Phân loại	Yêu cầu/Chỉ tiêu	Hướng dẫn thực hiện	Kết quả
1	iPhone 11	iOS 15.7.2	Điện thoại	Thiết bị đầu cuối nhận được địa chỉ IPv6, DNSv6 khi kết nối thành công đến hệ thống mạng truy cập	Trên thiết bị di động: - Bước 1: + Đối với iOS: Truy cập Cài đặt > WIFI + Đối với Android: Truy cập Cài đặt > Kết nối > WIFI - Bước 2: Chọn WIFI đang kết nối và nhấn biểu tượng "i" hoặc "bánh xe" để xem chi tiết thông tin - Bước 3: Kiểm tra thông tin địa chỉ IPv6 tại mục địa chỉ IP, địa chỉ DNSv6 tại mục DNS - Bước 4: Điền kết quả vào file checklist Trên máy tính Windows: - Bước 1: Mở hộp thoại Run và nhập "cmd" - Bước 2: Tại cửa sổ hiện ra, nhập lệnh: ipconfig /all - Bước 3: Kiểm tra thông tin địa chỉ IPv6 tại mục địa chỉ IP, địa chỉ DNSv6 tại mục DNS - Bước 4: Điền kết quả vào file checklist	Đạt/Không đạt
...	...	...	...	...	...	...

- Checklist truy cập website

TT	Thiết bị	Hệ điều hành	Trình duyệt	Website	Yêu cầu/Chỉ tiêu	Hướng dẫn thực hiện	Kết quả
1	Laptop Điện thoại	Windows 11 iOS Android	Google Chrome Microsoft Edge	vnexpress.net	Các website phổ biến khi được truy cập thông qua trình duyệt trên thiết bị đầu cuối	Trên thiết bị di động: - Bước 1: Truy cập vào trình duyệt phổ biến. Vd: Chrome, Safari, Firefox - Bước 2: Nhập tên trang web tại mục URL	Đạt/Không đạt
2				thanhnienvn.vn			Đạt/Không đạt
3				dantri.com.vn			Đạt/Không đạt
4				tuoitre.vn			Đạt/Không đạt

5			Safari	vietnamnet.vn	chạy HĐH Windows,	- Bước 3: Kiểm tra các tiêu chí hiển thị	Đạt/Không đạt
6			Firefox	24h.com.vn	Android, iOS đều phải	- Bước 4: Thực hiện tải xuống/tải lên file	Đạt/Không đạt
7				kenh14.vn	đạt tiêu chí:	ảnh, Video	Đạt/Không đạt
8				baomoi.com	- Kết nối đến trang	- Bước 5: Điền kết quả vào file checklist	Đạt/Không đạt
9				shopee.vn	web thành công	Trên máy tính Windows:	Đạt/Không đạt
10				lazada.vn	- Tải đầy đủ nội dung,	- Bước 1: Truy cập vào trình duyệt phổ	Đạt/Không đạt
11				tiki.vn	hình ảnh	biến. Vd: Chrome, Safari, Firefox	Đạt/Không đạt
12				sendo.vn	- Chất lượng hình ảnh	- Bước 2: Nhập tên trang web tại mục URL	Đạt/Không đạt
13				thegioididong.com	không bị nhoè, vỡ	- Bước 3: Nhấn F12 để mở devtool, chọn	Đạt/Không đạt
14				facebook.com	- Định dạng font chữ	thẻ Network để hiển thị trạng thái kết nối	Đạt/Không đạt
15				tiktok.com	đồng nhất, không bị	- Bước 4: Kiểm tra các tiêu chí hiển thị và	Đạt/Không đạt
16				instagram.com	méo, lỗi	thông tin kết nối theo IPv6 Global hay	Đạt/Không đạt
17				linkedin.com	- Tải xuống/tải lên file	NAT64	Đạt/Không đạt
18				x.com	hình ảnh/video thành	- Bước 5: Thực hiện tải xuống/tải lên file	Đạt/Không đạt
19				youtube.com	công	ảnh, Video	Đạt/Không đạt
20				chat.zalo.me		- Bước 6: Điền kết quả vào file checklist	Đạt/Không đạt

- Checklist ứng dụng

TT	Thiết bị	Hệ điều hành	Ứng dụng	Yêu cầu/Chỉ tiêu	Hướng dẫn thực hiện	Kết quả
1	Điện thoại	iOS, Android	Facebook	Các ứng dụng phổ biến khi được truy cập trên thiết bị đầu cuối chạy HĐH Android, iOS đều phải đạt tiêu chí: - Kết nối đến trang web thành công - Tải đầy đủ nội dung, hình ảnh - Chất lượng hình ảnh không bị nhoè, vỡ - Định dạng font chữ đồng nhất, không bị méo, lỗi	- Bước 1: Truy cập vào các ứng dụng phổ biến theo danh sách khảo sát - Bước 2: Kiểm tra các tiêu chí hiển thị - Bước 3: Thực hiện tải xuống/tải lên file ảnh, Video	Đạt/Không đạt
2			Messenger			Đạt/Không đạt
3			Zalo			Đạt/Không đạt
4			Tiktok			Đạt/Không đạt
5			Skype			Đạt/Không đạt
6			Viber			Đạt/Không đạt
7			Telegram			Đạt/Không đạt

8			Youtube	- Chất lượng cuộc gọi/video nghe/nói không bị vọng, mất tiếng - Tải xuống/tải lên file hình ảnh/video thành công	- Bước 4: Thực hiện cuộc gọi thoại/video - Bước 5: Điền kết quả vào file checklist	Đạt/Không đạt
9			Shopee			Đạt/Không đạt
10			Microsoft Team			Đạt/Không đạt

4. Danh sách các cổng dịch vụ để triển khai chính sách an toàn bảo mật

TT	IP Nguồn	IP Đích	Port nguồn	Port đích	Dịch vụ	Chú thích
1	Địa chỉ IP của máy chủ DNS64	Địa chỉ IP của máy chủ DNS Caching, DNS AD	Any	TCP/53 UDP/53	DNS	DNS Forwarder
2	Địa chỉ IP của Client	Địa chỉ IP của máy chủ DNS64	Any	TCP/53 UDP/53	DNS	DNS Resolver
3	Địa chỉ IP của Client	Địa chỉ IP của máy chủ DHCP	Any	UDP/67 UDP/547	DHCP	DHCP Relay
4	Địa chỉ IP của RODC	Địa chỉ IP của RWDC	Any	TCP/88 UDP/88	Kerberos	Replicate
				UDP/123	NTP	
				TCP/135 UDP/135	Endpoint Mapper	
				TCP/49152-65535	RPC Dynamic	
				TCP/445	Microsoft CIFS	
				TCP/53 UDP/53	DNS	
				UDP/138	NetBIOS datagram service	
				TCP/139	NetBIOS session service	

				TCP/636	LDAPS	
				TCP/137	Netbios name	
				TCP/3268	Global Catalog	
				TCP/3269	Global Catalog SSL	
				TCP/464 UDP/464	Kerberos Password Change	
				TCP/389 UDP/389	LDAP	
5	Địa chỉ IP của RWDC	Địa chỉ IP của RODC	Any	TCP/135 UDP/135	Endpoint Mapper	Replicate
				TCP/53 UDP/53	DNS	
				UDP/123	NTP	
				TCP/49152-65535	RPC Dynamic	
6	Địa chỉ IP của Client	Địa chỉ IP của DC	Any	TCP/88 UDP/88	Kerberos	AD SERVICES
				UDP/123	NTP	
				TCP/135 UDP/135	Endpoint Mapper	
				TCP/445	Microsoft CIFS	
				TCP/53 UDP/53	DNS	
				TCP/389 UDP/389	LDAP	

				TCP/464 UDP/464	Kerberos Password Change	
				TCP/49152-65535	RPC Dynamic	
				TCP/636	LDAPS	
				UDP/138	NetBIOS datagram service	
				TCP/139	NetBIOS session service	
				TCP/137	Netbios name	
				TCP/3268	Global Catalog	
7	Địa chỉ IP máy chủ giám sát	Địa chỉ IP của máy chủ DNS64, DHCP	Any	ICMP, ICMPv6 UDP/161		Giám sát