

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



BÁO CÁO ĐỒ ÁN

Môn: QUẢN TRỊ MẠNG VÀ HỆ THỐNG

Đề tài: IPv6 (routing, DHCPv6, NAT)

Giảng viên hướng dẫn: Th.S. Trần Thị Dung

Nhóm: 11

Sinh viên thực hiện:

1. Lê Hồng Hiền – 22520416
2. Trương Đức Hào – 225220407
3. Đỗ Mạnh Hùng – 22520500
4. Ngô Quang Huy – 22520555

Thời gian thực hiện: 10/2024 – 12/2024

MỤC LỤC

1.	Tổng quan.....	3
1.1	Giới thiệu	3
1.2	Thành phần.....	3
1.3	Một số quy trình hoạt động của IPv6.....	4
1.3.1	Phân giải địa chỉ (Address Resolution).....	4
1.3.2	Router Discovery	6
1.3.3	Cấu hình tự động địa chỉ cho IPv6 node	6
1.3.4	Kiểm tra trùng lặp địa chỉ (Duplicate Address Detection)	7
1.3.5	Routing trong IPv6	7
1.3.6	DHCPv6 (Dynamic Host Configuration Protocol for IPv6)	8
1.3.7	IPv4/IPv6 Communication.....	8
2.	Triển khai	10
2.1	Mô hình	10
2.1.1	Thành phần	10
2.1.2	Mục tiêu	10
2.2	Cài đặt và Cấu hình:	11
2.2.1	Kích hoạt IPv6 trên Router:	11
2.2.2	Cài đặt địa chỉ cho các Interface:	11
2.2.3	Cấu hình DHCPv6 Server:	12
2.2.4	Cấu hình Static:	14
2.2.5	Cài đặt Default Route:.....	14
2.2.6	Cấu hình RIPng (RIP for next-generation):	14
2.2.7	Cấu hình OSPFv3:.....	15
2.2.8	Giao tiếp với IPv4:	17
3.	Kết quả và kết luận:	22
3.1.	Kết quả:.....	22
3.2.	Kết luận:.....	22
4.	Tài liệu tham khảo	23
	Phụ lục	24

1. Tổng quan

1.1 Giới thiệu

- IPv6 (Internet Protocol version 6) là phiên bản mới nhất của Giao thức Internet, được phát triển nhằm mục đích nâng cấp giao thức liên mạng IPv4 hiện đang truyền dẫn cho hầu hết lưu lượng truy cập Internet nhưng đã hết địa chỉ.
- IPv6 cung cấp một không gian địa chỉ lớn hơn rất nhiều, hỗ trợ tốt hơn cho các thiết bị kết nối Internet hiện đại, và mang lại nhiều cải tiến về hiệu suất, bảo mật, cũng như khả năng mở rộng. Bên cạnh việc mở rộng không gian địa chỉ, IPv6 còn bao gồm các tính năng như tự động cấu hình địa chỉ và hỗ trợ bảo mật tích hợp.
- Việc triển khai IPv6 bao gồm các thành phần quan trọng như định tuyến (IPv6 routing), giao thức cấp phát địa chỉ tự động (DHCPv6) và dịch địa chỉ mạng (NAT) nhằm tối ưu hóa khả năng truyền thông tin qua mạng. Đồng thời, sự giao tiếp giữa các mạng IPv4 và IPv6 cũng là một yếu tố cần thiết trong quá trình chuyển đổi này, giúp đảm bảo các hệ thống có thể tương tác và vận hành hiệu quả trong môi trường mạng kết hợp.

1.2 Thành phần

- Địa chỉ IPv6 được viết dưới dạng hexa decimal. Địa chỉ IPv6 có độ dài 128 bit nhị phân. 128 bit nhị phân này được chia thành các nhóm 4 bit, chuyển đổi viết theo dạng số hexa decimal và nhóm 4 số hexa thành một nhóm phân cách bởi dấu ":".
- Có ba loại địa chỉ IPv6:
 - o Địa chỉ Unicast: Được dùng cho một thiết bị hoặc giao diện duy nhất.
 - o Địa chỉ Multicast: Được dùng để gửi đến một nhóm thiết bị.
 - o Địa chỉ Anycast: Được dùng để gửi đến một trong các thiết bị gần nhất trong nhóm.
- Gói tin IPv6 : Gói tin IPv6 bao gồm:
 - o Đầu gói (Header): Đầu gói IPv6 ngắn hơn và đơn giản hơn so với IPv4, bao gồm các trường chính như Version, Traffic Class, Flow Label, Payload Length, Next Header, và Hop Limit.
 - o Dữ liệu tải (Payload): Phần chứa dữ liệu hoặc các tiêu đề mở rộng.
- Tiêu đề mở rộng (Extension Headers): IPv6 cho phép sử dụng nhiều tiêu đề mở

rộng để bổ sung thêm các tính năng như bảo mật, phân mảnh, hoặc chuyển tiếp. Một số tiêu đề mở rộng phổ biến:

- Hop-by-Hop Options: Chứa thông tin xử lý tại mỗi nút mạng trên đường đi.
 - Destination Options: Chứa thông tin xử lý tại đích hoặc một số điểm xác định.
 - Routing Header: Cho phép chỉ định một số lộ trình cụ thể trong mạng.
 - Fragment Header: Hỗ trợ phân mảnh gói tin, mặc dù phân mảnh không được thực hiện tại các router mà do thiết bị gửi thực hiện.
 - Authentication Header (AH) và Encapsulating Security Payload (ESP): Dùng trong IPSec để bảo mật gói tin.
- Cấu hình tự động (Stateless Address Autoconfiguration - SLAAC): IPv6 hỗ trợ thiết lập địa chỉ tự động cho các thiết bị mà không cần máy chủ DHCP, cho phép thiết bị tự tạo địa chỉ dựa trên tiền tố mạng từ router.
 - DHCPv6: Được sử dụng để cấp phát địa chỉ và thông tin cấu hình khác trong mạng IPv6. Khác với IPv4, DHCPv6 có thể làm việc kết hợp với SLAAC để tối ưu hóa cấu hình.
 - ICMPv6: Giao thức điều khiển bản tin Internet dành riêng cho IPv6, giúp thực hiện các chức năng như Neighbor Discovery (ND) để quản lý bảng địa chỉ MAC và IP, phát hiện router, và cấu hình địa chỉ tự động.
 - Chất lượng dịch vụ (QoS): IPv6 có trường Traffic Class và Flow Label để phân loại và ưu tiên các luồng dữ liệu, hỗ trợ QoS tốt hơn so với IPv4.
 - IPv6 Network Topology: IPv6 cung cấp khả năng mở rộng mạng nhờ số lượng địa chỉ lớn, giúp thiết lập mạng với cấu trúc phân cấp dễ quản lý hơn.

1.3 Một số quy trình hoạt động của IPv6

1.3.1 Phân giải địa chỉ (Address Resolution)

- Trong địa chỉ IPv4, quy trình này được đảm nhiệm bởi thủ tục ARP. Node cần phân giải địa chỉ sẽ gửi gói tin truy vấn tới địa chỉ đích là địa chỉ broadcast, tác động đến mọi node khác trên đường link.
- Trong địa chỉ của IPv6, đây là một trong số những quy trình thủ tục Neighbor Discovery đảm nhiệm. Để phục vụ cho việc phân giải tương ứng địa chỉ lớp mạng và địa chỉ vật lý, các node IPv6 đều duy trì một bảng cache thông tin về

các node lân cận gọi là "neighbor cache".

- Khi một IPv6 node cần tìm địa chỉ lớp link-layer (ví dụ địa chỉ MAC trên đường link Ethernet) tương ứng với một địa chỉ unicast IPv6 nào đó, thay vì gửi gói tin truy vấn tới địa chỉ multicast mọi node phạm vi link (FF02::1) để tác động tới mọi node trên đường link tương đương địa chỉ broadcast trong IPv4, node đó chỉ gửi tới địa chỉ Multicast Solicited Node tương ứng địa chỉ unicast cần phân giải.
- Một node IPv6, khi được gán một địa chỉ unicast, ngoài việc lắng nghe lưu lượng tại địa chỉ unicast đó, node IPv6 sẽ lập tức nghe và nhận lưu lượng của một dạng địa chỉ multicast tương ứng là Multicast Solicited Node tương ứng địa chỉ unicast này.
- Như vậy, trong quá trình phân giải địa chỉ của IPv6, chỉ những node đang nghe lưu lượng tại địa chỉ Multicast Solicited Node phù hợp mới nhận và xử lý gói tin. Điều này giảm thiểu việc tác động đến mọi node trên đường link, tăng hiệu quả hoạt động.
- Để thực hiện quy trình phân giải địa chỉ, hai node IPv6 trong một đường link trao đổi thông điệp Neighbor Solicitation và Neighbor Advertisement.
- Khi một node cần phân giải địa chỉ, nó gửi đi trên đường link thông điệp Neighbor Solicitation:
 - o Địa chỉ nguồn: Địa chỉ IPv6 của giao diện gửi gói tin.
 - o Địa chỉ đích: địa chỉ IPv6 Multicast Solicited Node tương ứng địa chỉ unicast cần phân giải địa chỉ
 - o Thông tin chứa trong phần dữ liệu có chứa địa chỉ lớp link-layer của nơi gửi.
- Trên đường link, node đang nghe lưu lượng tại địa chỉ Multicast Solicited Node trùng với địa chỉ đích của gói tin sẽ nhận được thông tin. Nó thực hiện những hành động sau:
 - o Cập nhật địa chỉ lớp link-layer (địa chỉ MAC trong trường hợp kết nối Ethernet) của nơi gửi vào bảng neighbor cache.
 - o Gửi thông điệp Neighbor Advertisement đáp trả tới địa chỉ đích là địa chỉ nguồn đã gửi gói tin, thông tin trong phần dữ liệu có địa chỉ lớp link-layer của nó (chứa trong Option Target Link-Layer Address).

- Khi nhận được thông điệp Neighbor Advertisement, node cần phân giải địa chỉ sẽ sử dụng thông tin trong đó để thực hiện liên lạc đồng thời cập nhật thông tin vào bảng neighbor cache của mình.

1.3.2 Router Discovery

- Trong IPv6, để có thể cấu hình địa chỉ, cũng như có những thông số cho hoạt động, IPv6 host cần tìm thấy router và nhận được những thông tin từ router trên đường kết nối. Router IPv6 ngoài việc đảm trách chuyển tiếp gói tin cho host còn đảm nhiệm một hoạt động không thể thiếu là quảng bá sự hiện diện của mình và cung cấp các tham số trợ giúp host trên đường kết nối cấu hình địa chỉ và các tham số hoạt động. Thực hiện những hoạt động trao đổi thông tin giữa host và router là một nhiệm vụ rất quan trọng của thủ tục Neighbor Discovery.
- Quá trình tìm kiếm, trao đổi giữa host và router thực hiện dựa trên hai dạng thông điệp sau:
 - o Router Solicitation (RS) được gửi bởi host tới các router trên đường link. Do vậy, gói tin được gửi tới địa chỉ đích multicast mọi router phạm vi link (FF02::2). Host gửi thông điệp này để yêu cầu router quảng bá ngay các thông tin nó cần cho hoạt động ví dụ khi host chưa được gán địa chỉ, chưa có các tham số mặc định cần thiết để xử lý gói tin...
 - o Router Advertisement (RA) chỉ được gửi bởi các router để quảng bá sự hiện diện của router và các tham số cần thiết khác cho hoạt động của các host. Router gửi định kỳ thông điệp này trên đường kết nối và gửi thông điệp này bất cứ khi nào nhận được -Router Solicitation từ các host trong đường kết nối.

1.3.3 Cấu hình tự động địa chỉ cho IPv6 node

- Host IPv6 có thể tự động tạo ra các địa chỉ IP nội bộ bằng cách sử dụng cấu hình tự động địa chỉ không trạng thái (stateless address autoconfiguration: SLAAC) hoặc nó có thể được cấp một địa chỉ và những thông số hoạt động với DHCPv6. Đây là dạng thức cấu hình tự động địa chỉ có trạng thái (stateful autoconfiguration).
- Stateful autoconfiguration: Hoạt động tương đương với hoạt động của một nút IPv4 sử dụng DHCPv4 để nhận toàn bộ cấu hình IP của nó. Trong trường hợp

này, M flag (M = Managed Configuration) được thiết lập trong gói tin quảng bá của router, nó chỉ thị cho nút lấy một địa chỉ IPv6 từ máy chủ DHCPv6 bên cạnh những thông số khác.

- Stateless address autoconfiguration: Trong trường hợp này, cờ O (O = Other Configuration) được thiết lập trong gói tin quảng bá của router (Router Advertisement), chỉ dẫn nút tự tạo ra địa chỉ IPv6 cho nó, chỉ sử dụng DHCPv6 để lấy các thông số cấu hình khác có sẵn (ví dụ: địa chỉ máy chủ DNS, DNS-Suffix, NTP-Server...)

1.3.4 Kiểm tra trùng lặp địa chỉ (Duplicate Address Detection)

- Tự động cấu hình địa chỉ là một trong những đặc tính nổi bật của IPv6. Đặc tính này có được nhờ việc node IPv6 có khả năng tự cấu hình 64 bit Interface ID từ địa chỉ MAC, hoặc nhận ID là một con số ngẫu nhiên. Do 64 bit interface ID có thể là con số ngẫu nhiên, hoàn toàn có khả năng trên đường kết nối, địa chỉ IPv6 node dự định sử dụng đã được một node khác sử dụng rồi. Do vậy chúng cần một quy trình để kiểm tra sự trùng lặp địa chỉ trong đường link. Đó là quy trình DAD. DAD cũng sử dụng hai thông điệp ICMPv6 Neighbor Solicitation và Neighbor Advertisement.
- Khi một node cần kiểm tra trùng lặp địa chỉ, nó gửi gói tin Neighbor Solicitation
 - o Địa chỉ IPv6 nguồn: Là địa chỉ unspecified "::".
 - o Gói tin Neighbor Solicitation sẽ chứa địa chỉ IPv6 đang được kiểm tra trùng lặp.
- Sau khi gửi NS, node sẽ đợi. Nếu không có phản hồi, có nghĩa địa chỉ này chưa được sử dụng. Nếu địa chỉ này đã được một node nào đó sử dụng rồi, node này sẽ gửi thông điệp Neighbor Advertisement đáp trả:
 - o Địa chỉ nguồn: Địa chỉ IPv6 node giao diện gửi gói tin
 - o Địa chỉ đích: Địa chỉ IPv6 multicast mọi node phạm vi link (FF02::1)
 - o Gói tin sẽ chứa địa chỉ bị trùng lặp
- Nếu node đang kiểm tra địa chỉ trùng lặp nhận được thông điệp RA phản hồi lại RS mình đã gửi, nó sẽ hủy bỏ việc sử dụng địa chỉ này.

1.3.5 Routing trong IPv6

- Quá trình định tuyến trong IPv6 diễn ra như sau:

- Bước 1: Cấu hình địa chỉ IPv6 trên các thiết bị
- Mỗi thiết bị trong mạng được gán địa chỉ IPv6 thông qua cấu hình thủ công hoặc tự động bằng SLAAC (Stateless Address Autoconfiguration) hoặc DHCPv6.
- Bước 2: Quảng bá thông tin tuyến đường
Các router sử dụng giao thức định tuyến (như OSPFv3, EIGRP for IPv6 hoặc RIPng) để trao đổi thông tin về mạng mà chúng quản lý. Mỗi router xây dựng bảng định tuyến chứa các tuyến đường tối ưu.
- Bước 3: Chuyển tiếp gói tin
Khi nhận được gói tin, router kiểm tra bảng định tuyến để tìm tuyến đường tối ưu dựa trên địa chỉ đích IPv6. Sau đó, gói tin được chuyển tiếp đến bước tiếp theo cho đến khi đến đích.

1.3.6 DHCPv6 (Dynamic Host Configuration Protocol for IPv6)

- DHCPv6 là giao thức cung cấp địa chỉ IPv6 động cho các thiết bị trong mạng.

Quy trình gồm:

- Bước 1: Gửi yêu cầu
Thiết bị client gửi gói Solicit để yêu cầu địa chỉ IPv6 từ server DHCPv6.
- Bước 2: Trả lời từ server
Server DHCPv6 gửi gói Advertise để cung cấp các thông tin như địa chỉ IPv6, DNS, và thông tin mạng.
- Bước 3: Chấp nhận địa chỉ
Client chọn một địa chỉ từ danh sách, gửi gói Request để yêu cầu xác nhận.
- Bước 4: Gán địa chỉ
Server gửi gói Reply để hoàn tất quy trình cấp phát.

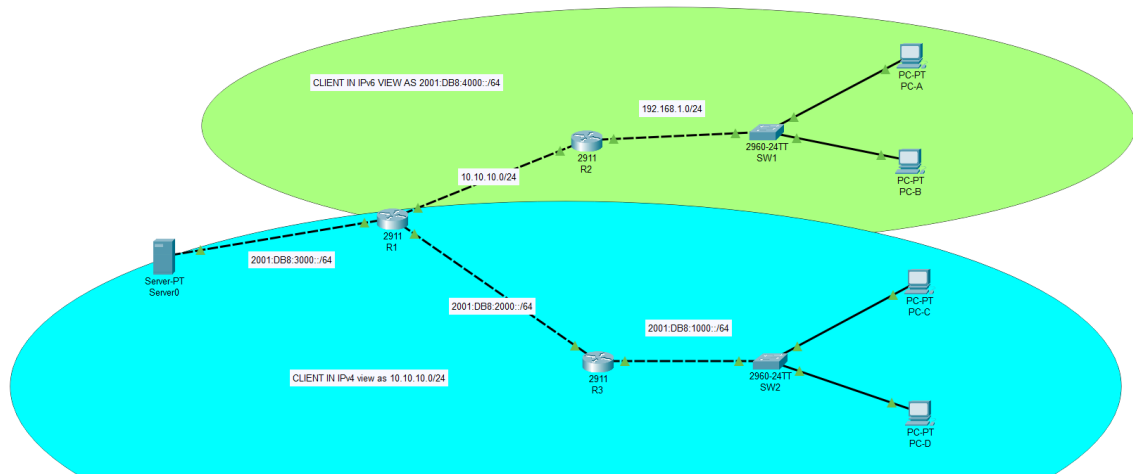
1.3.7 IPv4/IPv6 Communication

- Do sự chuyển đổi từ IPv4 sang IPv6 chưa hoàn toàn, các cơ chế giao tiếp giữa hai giao thức này là cần thiết. Quy trình có thể sử dụng các phương pháp sau:
- Dual Stack (Ngăn xếp kép):
- Dual Stack là việc cấu hình cả IPv4 và IPv6 trên cùng một thiết bị (router, switch, hoặc host). Thiết bị này có thể xử lý cả hai loại giao thức song song, cho phép giao tiếp với mạng IPv4 và IPv6.

- Các thiết bị chạy cả hai giao thức IPv4 và IPv6, cho phép giao tiếp độc lập giữa hai mạng..
 - Khi thiết bị nhận được gói tin IPv4, nó xử lý bằng ngăn xếp IPv4; tương tự với IPv6.
 - Tunneling (Đường hầm):
 - Tunneling là kỹ thuật "bọc" gói tin IPv6 trong một gói tin IPv4 để truyền qua mạng chỉ hỗ trợ IPv4. Khi đến đầu nhận, gói tin được "mở bọc" để tiếp tục xử lý dưới dạng gói tin IPv6.
- Gói tin IPv6 được đóng gói bên trong gói IPv4 để truyền qua mạng chỉ hỗ trợ IPv4. Một số phương pháp thường dùng:
- 6to4 Tunneling: Đóng gói tự động qua mạng IPv4 công cộng.
 - ISATAP: Sử dụng để giao tiếp trong mạng nội bộ.
- NAT-PT (Network Address Translation - Protocol Translation)
 - NAT-PT là kỹ thuật dịch địa chỉ và giao thức giữa IPv4 và IPv6, cho phép các thiết bị IPv4 và IPv6 giao tiếp trực tiếp mà không cần cả hai hỗ trợ song song.
- Sử dụng NAT64 để dịch gói tin giữa IPv4 và IPv6.
- Địa chỉ IPv4 sẽ được ánh xạ với địa chỉ IPv6 theo cấu hình của NAT64 và ngược lại, cho phép hai thiết bị giao tiếp qua router trung gian.

2. Triển khai

2.1 Mô hình



2.1.1 Thành phần

Tên thành phần	Loại
R1, R2, R3	Router-2911
PC-A, PC-B, PC-C, PC-D	PC-PT
SW1, SW2	2960-24TT
Server0	Server-PT

2.1.2 Mục tiêu

- Thiết lập mạng IPv6 cơ bản: Xây dựng một mô hình mạng IPv6 đơn giản bao gồm các thành phần thiết yếu như router và các thiết bị đầu cuối, đảm bảo rằng các thiết bị có thể giao tiếp qua IPv6.
- Cấu hình định tuyến IPv6: Triển khai định tuyến IPv6 giữa các thiết bị trong cùng một mạng hoặc các mạng con. Cài đặt giao thức định tuyến cơ bản như static hoặc dynamic để các thiết bị có thể định tuyến gói tin IPv6.
- Cài đặt và cấu hình DHCPv6: Triển khai DHCPv6 server để tự động cấp phát địa chỉ IPv6 cho các thiết bị trong mạng, giúp giảm thiểu việc cấu hình thủ công.
- Thử nghiệm NAT64 để kết nối IPv6 - IPv4: Cấu hình NAT64 để các thiết bị IPv6 có thể truy cập tài nguyên IPv4, giúp đảm bảo tính tương thích ngược

giữa hai hệ thống mạng.

- Kiểm tra và xác minh kết nối: Kiểm tra tính khả dụng của các tính năng cơ bản, đảm bảo rằng các thiết bị có thể nhận địa chỉ IPv6, thực hiện định tuyến, và giao tiếp với các tài nguyên IPv4 qua NAT64.

2.2 Cài đặt và Cấu hình:

- Môi trường giả lập: Ứng dụng Cisco Packet Tracer
- Cấu hình thiết bị:

2.2.1 Kích hoạt IPv6 trên Router:

- Sử dụng Ipv6 unicast-routing để bật tính năng định tuyến IPv6, cho phép router gửi thông báo Router Advertisement (RA) để hỗ trợ cấu hình IPv6 cho các thiết bị khác qua SLAA, cho phép router xử lý và chuyển tiếp các gói tin IPv6 giữa các giao diện

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
```

2.2.2 Cài đặt địa chỉ cho các Interface:

- Sử dụng int interface => ipv6 address <IP>: Tương tự với ipv4.
- Sử dụng ipv6 enable dùng để kích hoạt giao thức IPv6 trên Interface, giao diện sẽ tự động gán một địa chỉ link-local (fe80::/10)

```
R1(config)#int g0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:db8:3000::1/64
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#int g0/2
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:db8:2000::1/64
R1(config-if)#no shut

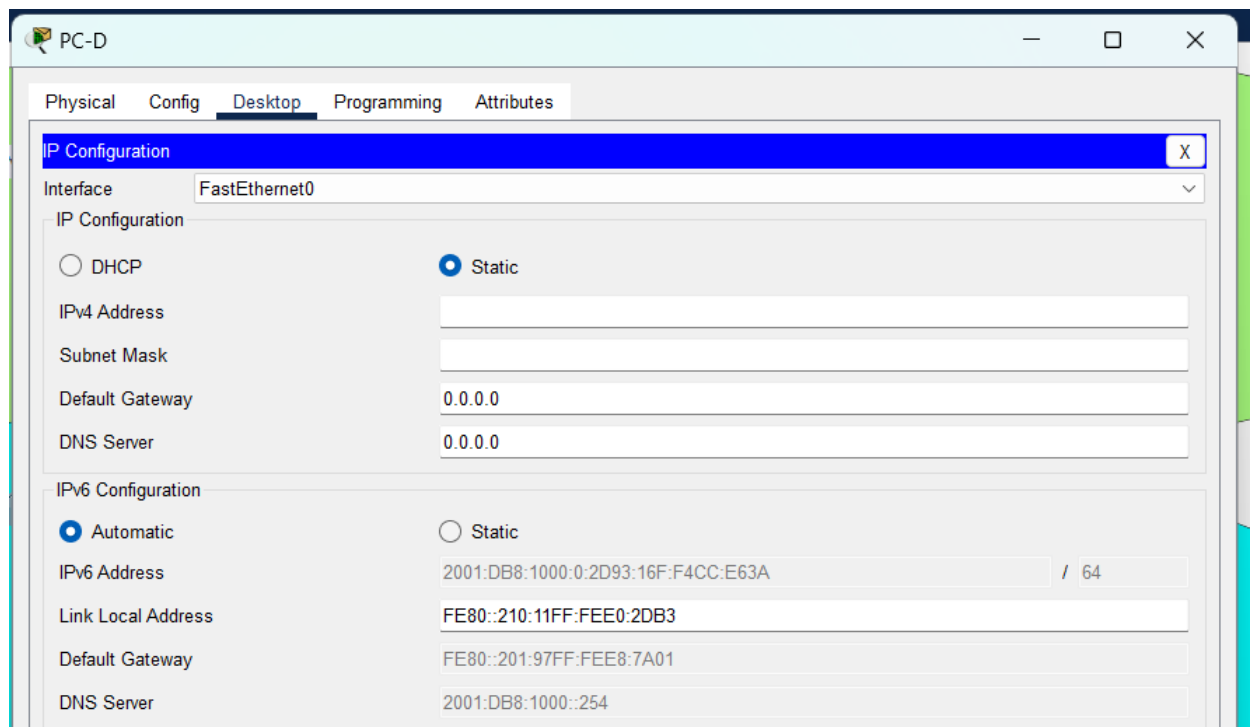
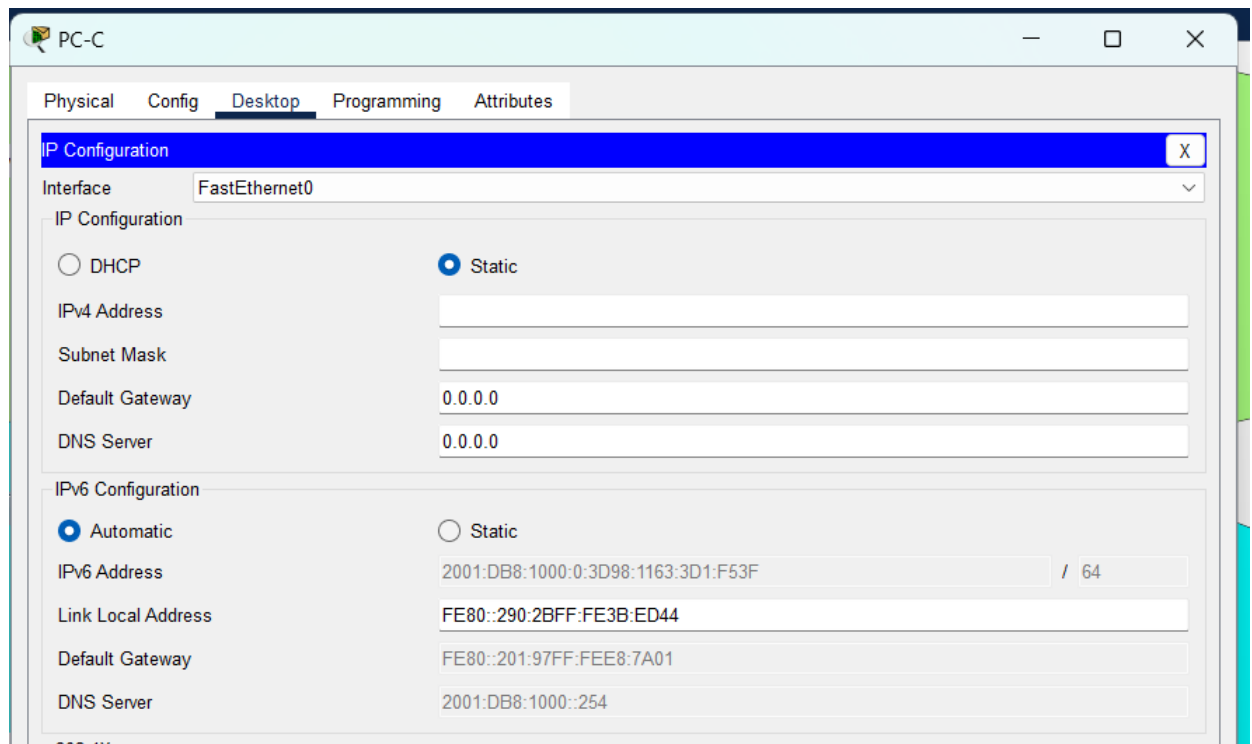
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

R1(config-if)#exit
```

2.2.3 Cấu hình DHCPv6 Server:

- Ipv6 dhcp pool <name>: Tạo một pool DHCPv6 để chứa các thông số mà router sẽ cấp phát cho các thiết bị.
- Address prefix 2001:db8:1000::/64: Xác định dải địa chỉ Ipv6 sẽ cấp phát cho các thiết bị.
- Dns-server <IPv6-address>: Chỉ định địa chỉ máy chủ DNS mà thiết bị khách sẽ sử dụng để phân giải tên miền.
- Domain-name <domain-name>: Cấp phát tên miền để dễ dàng quản lý.
- Interface <interface> => ipv6 dhcp server <name-pool>: Gắn pool đã tạo vào giao diện để tiến hành cấp phát.
- Ipv6 address <IP>: Tạo Ipv6 cho giao diện.
- Ipv6 nd managed-config-flag: Bật cờ M để các thiết bị không sử dụng SLAAC mà sẽ sử dụng DHCPv6 để nhận địa chỉ IPv6 và các thông tin khác (cờ O thì sẽ sử dụng SLAAC nhưng dùng DHCPv6 để bổ sung thông tin).
- Ta cấu hình DHCPv6 ở Router3:

```
R3(config-if)#exit
R3(config)#ipv6 dhcp pool DHCPv6-pool
R3(config-dhcpv6)#address prefix 2001:db8:1000::/64
R3(config-dhcpv6)#dns-server 2001:db8:1000::254
R3(config-dhcpv6)#domain-name stateful.com
R3(config-dhcpv6)#exit
R3(config)#int g0/0
R3(config-if)#ipv6 address 2001:db8:1000::1
% Incomplete command.
R3(config-if)#ipv6 address 2001:db8:1000::1/64
R3(config-if)#ipv6 dhcp server DHCPv6-pool
R3(config-if)#ipv6 nd managed-config-flag
R3(config-if)#exit
R3(config)#
```



```

R3>en
R3#sh ipv6 dhcp pool
DHCPv6 pool: DHCPv6-pool
  Address allocation prefix: 2001:db8:1000::/64 valid 172800 preferred 86400 (12 in use, 0
conflicts)
  DNS server: 2001:DB8:1000::254
  Domain name: state.com
  Active clients: 2
R3#

```

2.2.4 Cấu hình Static:

- Sử dụng ipv6 route <destination> <next-hop>: Tương tự IPv4

```
R3(config)#ipv6 route 2001:db8:3000::/64 2001:db8:2000::1
```

2.2.5 Cài đặt Default Route:

```
R3(config)#ipv6 route ::/0 2001:db8:2000::1  
R3(config)#
```

2.2.6 Cấu hình RIPng (RIP for next-generation):

- Sử dụng: ipv6 router rip <A> => int interface => ipv6 rip <A> enable
- Cấu hình RIP trên router và chỉ định tên, sau đó kích hoạt trên giao diện.









```
R1(config)#ipv6 unicast-routing  
R1(config)#ipv6 router rip nhom11  
R1(config-rtr)#int g0/0  
R1(config-if)#ipv6 rip nhom11 enable  
R1(config-if)#exit  
R1(config)#int g0/2  
R1(config-if)#ipv6 rip nhom11 enable  
R1(config-if)#
```

```
R3(config)#ipv6 router rip nhom11  
R3(config-rtr)#int g0/0  
R3(config-if)#ipv6 rip nhom11 enable  
R3(config-if)#exit  
R3(config)#int g0/1  
R3(config-if)#ipv6 rip nhom11 enable  
R3(config-if)#exit  
R3(config)#exit  
R3#
```

- Kiểm tra bằng sh ipv6 route:

```
R1#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:DB8:1000::/64 [120/2]
    via FE80::2D0:BAFF:FE97:1602, GigabitEthernet0/2
C   2001:DB8:2000::/64 [0/0]
    via GigabitEthernet0/2, directly connected
L   2001:DB8:2000::1/128 [0/0]
    via GigabitEthernet0/2, receive
C   2001:DB8:3000::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:3000::1/128 [0/0]
    via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

- Kiểm tra ping thành công:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-C	Server0	ICM...		0.000	N	0	(edit)	(delete)
	Successful	Server0	PC-C	ICM...		0.000	N	1	(edit)	(delete)
	Successful	PC-D	Server0	ICM...		0.000	N	2	(edit)	(delete)
	Successful	Server0	PC-D	ICM...		0.000	N	3	(edit)	(delete)

2.2.7 Cấu hình OSPFv3:

- Ngoài ra có thể sử dụng OSPFv3:
 - o Sử dụng ipv6 router OSPF <ID> => router-id (ví dụ: 1.1.1.1) => int <interface> => IPv6 ospf <ID> <Area-ID> : Kích hoạt OSPFv3 trên router và id để nhận diện quá trình OSPF này, router-id để nhận diện router trong mạng OSPF, sau đó kích hoạt OSPF ở các giao diện.

```
R1(config-router)#exit
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 2.2.2.2
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#exit
R1(config)#int g0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#int g0/2
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config-if)#
```

```

R3(config-rtr)#ipv6 router ospf 1
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#passive-interface g0/0
R3(config-rtr)#exit
R3(config)#int g0/0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#exit
R3(config)#int g0/1
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#exit
R3(config)#

```

- Kiểm tra lại bằng sh ipv6 route:

```

R1#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2001:DB8:1000::/64 [110/2]
    via FE80::201:97FF:FEE8:7A02, GigabitEthernet0/2
C   2001:DB8:2000::/64 [0/0]
    via GigabitEthernet0/2, directly connected
L   2001:DB8:2000::1/128 [0/0]
    via GigabitEthernet0/2, receive
C   2001:DB8:3000::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:3000::1/128 [0/0]
    via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#

```

```

R3#sh ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
    via 2001:DB8:2000::1
C   2001:DB8:1000::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:1000::1/128 [0/0]
    via GigabitEthernet0/0, receive
C   2001:DB8:2000::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:2000::2/128 [0/0]
    via GigabitEthernet0/1, receive
O   2001:DB8:3000::/64 [110/2]
    via FE80::2E0:8FFF:FEB5:4503, GigabitEthernet0/1
L   FF00::/8 [0/0]
    via Null0, receive
R3#

```


2.2.8 Giao tiếp với IPv4:

2.2.8.1 Sử dụng Nat-PT:

- Đây là một công nghệ chuyển đổi địa chỉ mạng, cho phép các thiết bị sử dụng giao thức IPv6 giao tiếp với các thiết bị sử dụng giao thức IPv4. Khi một gói tin IPv6 được gửi đến một địa chỉ IPv4, NAT-PT sẽ chuyển đổi địa chỉ này thành một địa chỉ IPv6 đặc biệt và chuyển tiếp gói tin đến mạng IPv4.
- Câu lệnh `ipv6 nat` được sử dụng trong cấu hình trên giao diện của một router khi bạn muốn thực hiện NAT-PT (Network Address Translation - Protocol Translation) để chuyển đổi giữa địa chỉ IPv4 và IPv6. Đây là một tính năng được sử dụng để hỗ trợ giao tiếp giữa các mạng IPv4 và IPv6, thường gặp trong quá trình chuyển đổi từ IPv4 sang IPv6.

2.2.8.1.1 Static NAT-PT:

- Cấu hình tĩnh cho phép 1 địa chỉ Ipv4 map với 1 Ipv6 và ngược lại được định nghĩa thủ công.

```
R1(config)#int g0/0
R1(config-if)#ipv6 nat
R1(config-if)#it
^
% Invalid input detected at '^' marker.

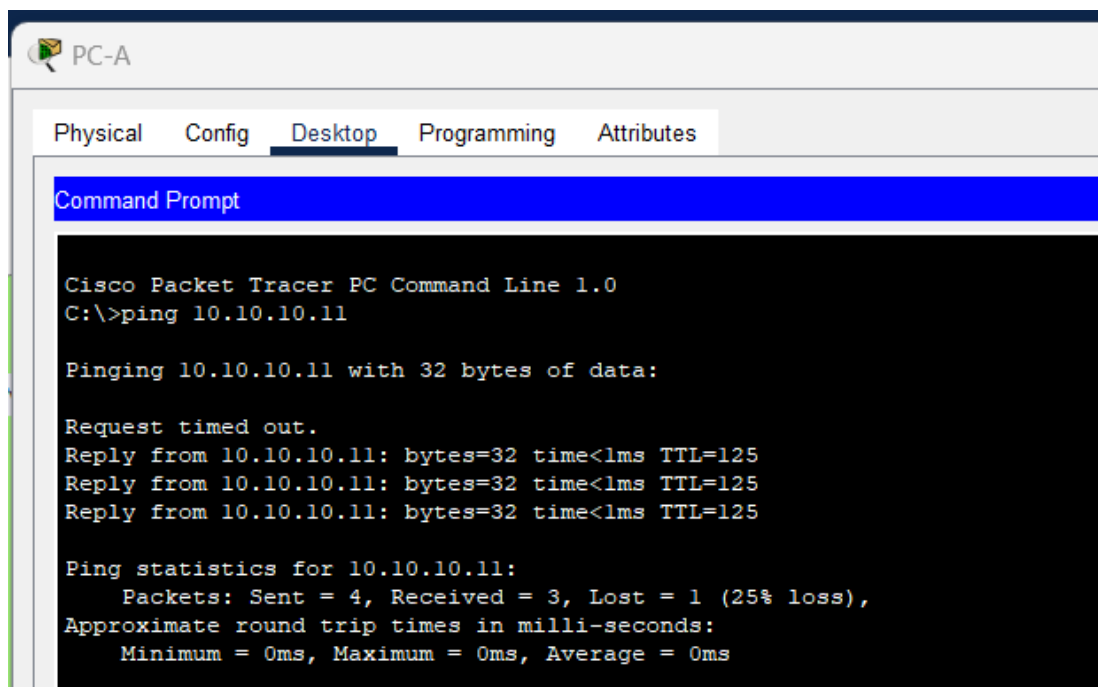
R1(config-if)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 nat
R1(config-if)#exit
R1(config)#int g0/2
R1(config-if)#ipv6 nat
R1(config-if)#exit
R1(config)#ipv6 nat
```

- `Ipv6 nat v4v6 source 192.168.1.2 2001:db8:4000::1`
- Câu lệnh này cấu hình **NAT-PT (Network Address Translation - Protocol Translation)** để ánh xạ (map) một địa chỉ IPv4 **192.168.1.2** sang một địa chỉ IPv6 tương ứng là **2001:db8:4000::1**.
- Ngược lại `ipv6 nat v6v4 source 2001:db8:3000::2 10.10.10.10` ánh xạ IPv6 thành Ipv4 tương ứng.
- Quá trình này cho phép một thiết bị sử dụng địa chỉ IPv4 (trong mạng IPv4)

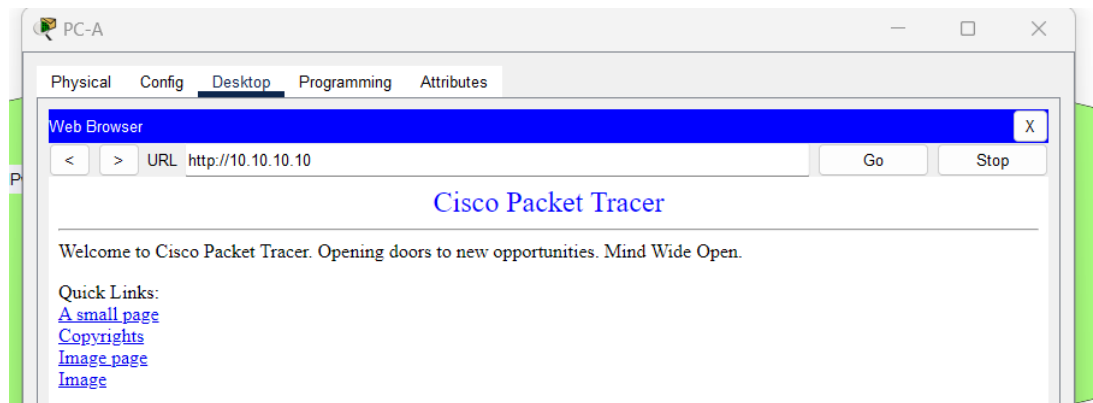
giao tiếp với thiết bị sử dụng địa chỉ IPv6 (trong mạng IPv6), thông qua quá trình dịch địa chỉ và ngược lại.

```
R1(config)#ipv6 nat v4v6 source 192.168.1.2 2001:db8:4000::1
R1(config)#ipv6 nat v4v6 source 192.168.1.3 2001:db8:4000::2
R1(config)#ipv6 nat v6v4 source 2001:db8:1000::2 10.10.10.11
R1(config)#ipv6 nat v6v4 source 2001:db8:1000::3 10.10.10.12
R1(config)#ipv6 nat v6v4 source 2001:db8:3000::2 10.10.10.10
R1(config)#ipv6 nat prefix 2001:db8:4000::/96
```

- Sử dụng Ipv6 nat prefix để kiểm tra địa chỉ đích 2001:db8:4000::/96 bởi NAT-PT thay vì drop.
- Kiểm tra ping từ máy A đến máy C:



- Máy A truy cập url bằng địa chỉ IP 10.10.10.10 (của server 2001:db8:3000::2/64):



2.2.8.1.2 Dynamic NAT-PT

- Hoạt động bằng cách ánh xạ động giữa các địa chỉ IPv6 và IPv4.
- Đầu tiên với Ipv6 chuyển đổi thành Ipv4:
- Ipv6 nat v6v4 source {list access-list-name | route-map map-name} pool name: Sử dụng list name và pool để lấy thông tin về access-list và pool chứa dải địa chỉ.
- Ipv6 nat v6v4 pool name start-ipv4 end-ipv4 prefix-length prefix-length: Chỉ định pool chứa địa chỉ Ipv4 để sử dụng dynamic NAT-PT.
- Ipv6 access-list access-list-name: Định nghĩa access list cần sử dụng
- Permit Protocol: Định nghĩa rule của access list.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 nat v6v4 source list pt-list1 pool v4pool
R1(config)#ipv6 nat v6v4 pool v4pool 10.10.10.10 10.10.10.15 prefix-length 24
R1(config)#ipv6 access-list pt-list1
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Đối với Ipv4 chuyển đổi thành Ipv6:
- Câu lệnh tương tự Ipv6 mapping Ipv4 với pool chứa dải địa chỉ Ipv6 và access-list dành cho Ipv4.

```
R1(config)#ipv6 nat v4v6 source list 1 pool v6pool
R1(config)#ipv6 nat v4v6 pool v6pool 2001:db8:4000::1 2001:db8:4000::5 prefix-length 96
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
```

2.2.8.1.3 PAT NAT-PT:

- Khi một gói tin IPv6 cần được chuyển thành IPv4, PAT NAT-PT sẽ ánh xạ địa chỉ IPv6 thành một địa chỉ IPv4 duy nhất (với cổng khác nhau) trong pool NAT, thay vì chỉ ánh xạ địa chỉ. Điều này giúp giảm thiểu số lượng địa chỉ IPv4 cần thiết.

Giao thức	Mạng bên trong	Hướng chuyển đổi	Mạng IPv4
	IPv6		IPv4
v6v4	2001:a:b:c::1/64	====>	
	2001:a:b:c::2/64	====>	192.168.40.199
	2001:a:b:c::3/64	====>	
v4v6	2001:c018:28c8/96	<====	192.168.40.200

- Do sự thiếu hụt Ipv4 nên PAT NAT-PT cũng là một giải pháp được ưu tiên sử dụng.

```
R1(config)#ipv6 nat v6v4 source list pt-list1 pool v4pool overload
R1(config)#ipv6 nat v6v4 pool v4pool 10.10.10.10 10.10.10.20 prefix-length 24
R1(config)#ipv6 access-list pt-list1
R1(config-ipv6-acl)#permit ipv6 2001:db8::/96 any
R1(config-ipv6-acl)#
```

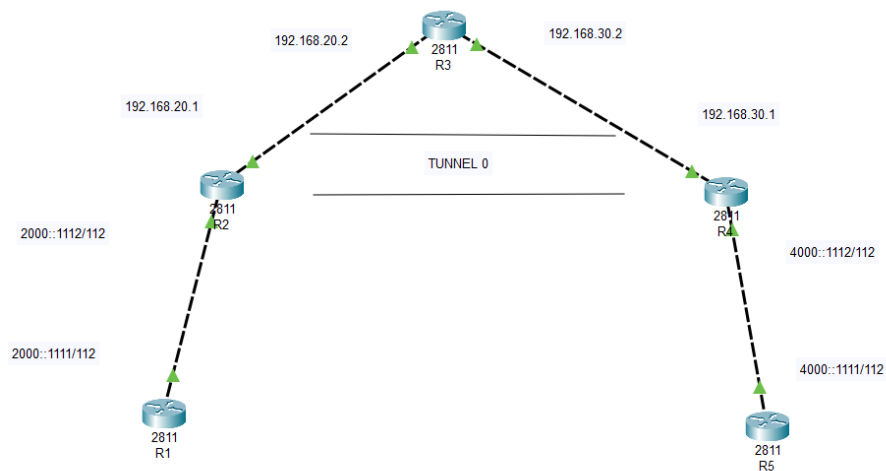
2.2.8.1.4 IPv4 Mapped:

- Do trên thực tế số Hosts sử dụng Ipv4 là rất nhiều, do đó giải pháp của Ipv4 Mapped là cho phép các hệ thống IPv6 giao tiếp với các hệ thống IPv4 mà không cần phải thay đổi hoàn toàn địa chỉ của mình.
- Ví dụ địa chỉ Ipv4-mapped Ipv6 sẽ có định dạng ::ffff:<IPv4_address>.

```
R1(config)#int g0/1
R1(config-if)#ipv6 nat prefix 2001::/96 v4-mapped v4mapacl
R1(config-if)#ipv6 access-list v4mapacl
R1(config-ipv6-acl)#permit ipv6 any 2001::/96
R1(config-ipv6-acl)#exit
```

2.2.8.2 Tunneling và Dual Stack:

- Ta có mô hình thử nghiệm dưới đây:



- Router dual stack là R2 và R4.
- Ở R2:
 - Int Tunnel0 để định nghĩa giao diện Tunnel0, sau đó cài đặt địa chỉ ipv6 cho giao diện dùng định tuyến RIP.
 - Tunnel source fa0/1: Xác định giao diện vật lý cho đường hầm dùng làm đầu vào.
 - Tunnel destination 192.168.30.1: Chỉ định địa chỉ IPv4 là điểm cuối của đường hầm.
 - Tunnel mode ipv6ip: Chỉ định chế độ của đường hầm là IPv6-over-IPv4.

```
!
interface Tunnel0
  no ip address
  mtu 1476
  ipv6 address 3000::1/112
  ipv6 rip 6bone enable
  tunnel source FastEthernet0/1
  tunnel destination 192.168.30.1
  tunnel mode ipv6ip
!
```









- Tương tự ở R4:

```

!
interface Tunnel0
 no ip address
 mtu 1476
 ipv6 address 3000::2/112
 ipv6 rip 6bone enable
 tunnel source FastEthernet0/0
 tunnel destination 192.168.20.1
 tunnel mode ipv6ip
!

```

- Kiểm tra Ping từ R1 đến R5 thành công:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	D
	Successful	R1	R5	ICM...		0.000	N	0	(edit)	
	Successful	R5	R1	ICM...		0.000	N	1	(edit)	
	Successful	R2	R4	ICM...		0.000	N	2	(edit)	
	Successful	R4	R2	ICM...		0.000	N	3	(edit)	

3. Kết quả và kết luận:

3.1. Kết quả:

Kiểm tra Routing IPv6: Đảm bảo các thiết bị có thể giao tiếp giữa các subnet IPv6 khác nhau.

Kiểm tra DHCPv6: Xác minh việc cấp phát địa chỉ IPv6 cho các thiết bị trong mạng.

Kiểm tra NAT64: Kiểm tra tính năng dịch địa chỉ giữa IPv6 và IPv4 bằng cách truy cập web.

3.2. Kết luận:

Thông qua việc triển khai, cấu hình, và kiểm tra hệ thống mạng IPv6, dự án mang lại cái nhìn sâu sắc về các ưu điểm của IPv6 so với IPv4 cũng như những thách thức khi chuyển đổi hệ thống mạng.

4. Tài liệu tham khảo

- Biểu diễn địa chỉ Ipv6 (Chuyên đề đào tạo Ipv6 – Phần 1)
<https://waren.vn/chuyen-de/bieu-dien-dia-chi-ipv6-chuyen-de-dao-tao-ipv6-phan-1.html>
- Cấu trúc đánh địa chỉ, các dạng địa chỉ Ipv6 (Chuyên đề đào tạo Ipv6 – Phần 2)
<https://www.waren.vn/chuyen-de/cau-truc-danh-dia-chi-cac-dang-dia-chi-ipv6-chuyen-de-dao-tao-ipv6-phan-2.html>
- Tìm hiểu Ipv6 Header (Chuyên đề đào tạo Ipv6 – Phần 6)
<https://www.waren.vn/chuyen-de/tim-hieu-ipv6-header-chuyen-de-dao-tao-ipv6-phan-6.html>
- Một số quy trình hoạt động của địa chỉ Ipv6 (Chuyên đề đào tạo Ipv6 – Phần 11)
<https://waren.vn/chuyen-de/mot-so-quy-trinh-hoat-dong-cua-dia-chi-ipv6-chuyen-de-dao-tao-ipv6-phan-11.html>
- Quy tắc chuyển đổi giữa IPv4 và IPv6: Dual Stack
<https://vnpro.vn/thu-vien/quy-tac-chuyen-doi-giua-ipv4-va-ipv6-dual-stack-2170.html>
- Công nghệ đường hầm Tunnel (Chuyên đề đào tạo Ipv6 – Phần 15)
<https://waren.vn/chuyen-de/cong-nghe-duong-ham-tunnel-chuyen-de-dao-tao-ipv6-phan-15.html>
- Static NAT-PT for IPv6 Configuration Example
<https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/113275-nat-ptv6.html>

Phụ lục

1. Phân chia công việc

MSSV	Thành viên	Nhiệm vụ	Phần trăm thực hiện
22520407	Trương Đức Hào	Tìm hiểu về Ipv6, chỉnh sửa file báo cáo, thuyết trình, quay và chỉnh sửa video demo.	100%
22520416	Lê Hồng Hiền	Tìm hiểu về Ipv6, viết và chỉnh sửa file báo cáo, làm powerpoint thuyết trình, chỉnh sửa video demo.	100%
22520500	Đỗ Mạnh Hùng	Tìm hiểu về Ipv6, chỉnh sửa file báo cáo, thuyết trình, quay và chỉnh sửa video demo.	100%
22520555	Ngô Quang Huy	Tìm hiểu về Ipv6, viết và chỉnh sửa file báo cáo, làm powerpoint thuyết trình, chỉnh sửa video demo.	100%

2. Tự đánh giá

Tiêu chí	Mức điểm
Report format	1
Presentation	1
Theory	2
Demonstration	5
Quiz after presentation	1

3. Trả lời câu hỏi

1. IPv6 có thể thay thế hoàn toàn IPv4 được không?

⇒ IPv6 có thể thay thế hoàn toàn IPv4 trong tương lai. Tuy nhiên, để điều này trở thành hiện thực, cần thời gian và sự hợp tác từ nhiều phía:

- Các doanh nghiệp và tổ chức cần xây dựng kế hoạch chuyển đổi IPv6 rõ ràng.
- Chính phủ cần ban hành chính sách hỗ trợ và thúc đẩy mạnh mẽ việc triển khai IPv6-Only.
- Người dùng cá nhân và doanh nghiệp cần nâng cấp thiết bị, phần mềm để tương thích với IPv6.

2. Có bao nhiêu địa chỉ IPv6 khả dụng so với IPv4?

⇒ IPv4 chỉ cung cấp 2^{32} địa chỉ. Do sự bùng nổ của các thiết bị kết nối Internet, không gian địa chỉ IPv4 đã cạn kiệt tại nhiều khu vực trên thế giới. Trong khi đó IPv6 cung cấp 2^{128} địa chỉ IP. Đây là một con số rất lớn, nó đảm bảo đủ số lượng địa chỉ IP cho sự phát triển của internet trong tương lai.

3. Khác biệt giữa IPv6 và IPv4 (bộ cục, vị trí,...), nếu một doanh nghiệp đã cấu hình IPv4 ổn định thì có nên chuyển hoàn toàn sang IPv6 không?

⇒ Khác biệt giữa IPv6 và IPv4:

Tiêu chí	IPv4	IPv6
Độ dài địa chỉ	32 bit	128 bit
Dạng biểu diễn	Thập phân, 4 nhóm	Thập lục phân, 8 nhóm
Không gian địa chỉ	2^{32}	2^{128}
Khả năng tự cấu hình	Cấu hình thủ công hoặc qua DHCP	SLAAC hoặc DHCPv6
Bảo mật	IPsec là tùy chọn	IPsec là bắt buộc
Khả năng tương thích	Phụ thuộc vào NAT và IPv4-only	Yêu cầu dual-stack hoặc gateway

Nếu một doanh nghiệp đã cấu hình IPv4 ổn định, việc chuyển đổi hoàn toàn sang IPv6 cần xem xét các yếu tố sau:

- Lợi ích: IPv6 cung cấp không gian địa chỉ rộng hơn, giúp mở rộng quy mô mà không lo thiếu địa chỉ IP. Hơn nữa, các tính năng bảo mật và hiệu suất tốt hơn của IPv6 có thể là yếu tố thúc đẩy việc chuyển đổi.
- Chi phí và thời gian: Chuyển đổi sẽ đòi hỏi thời gian và chi phí, bao gồm nâng cấp phần cứng, phần mềm và đào tạo nhân viên.
- Tương thích: Đảm bảo rằng tất cả các thiết bị và ứng dụng hiện tại tương thích với IPv6 hoặc có thể cập nhật để hỗ trợ.

Có thể xem xét phương pháp chuyển đổi từng bước, giữ cả hai hệ thống IPv4 và IPv6 (Dual Stack) trong một khoảng thời gian trước khi chuyển đổi hoàn toàn sang IPv6.

4. Làm thế nào để tích hợp IPv6 routing vào các hệ thống SDN (Software-Defined Networking) hiện đại?

⇒ Để tích hợp IPv6 routing vào SDN, ta cần:

Đầu tiên, cần cập nhật phần mềm SDN Controller: Đảm bảo rằng SDN Controller hỗ trợ IPv6. Các phiên bản mới của các SDN Controller phổ biến như OpenDaylight, ONOS đều có hỗ trợ IPv6.

Bước 2, cấu hình IPv6 trên các thiết bị mạng: Đảm bảo rằng tất cả các thiết bị trong mạng, bao gồm switch, router và host đều được cấu hình để hỗ trợ và sử dụng địa chỉ IPv6.

Bước 3, cấu hình các chính sách và quy tắc routing: Sử dụng SDN Controller để tạo và quản lý các quy tắc routing IPv6. Điều này bao gồm việc xác định các tuyến đường, thiết lập các chính sách ưu tiên và đảm bảo an ninh.

Bước 4, giám sát và quản lý: Sử dụng các công cụ giám sát SDN để theo dõi hiệu suất và tính khả dụng của các kết nối IPv6. Đảm bảo rằng tất cả các phần tử trong mạng hoạt động đúng và không có sự cố.