

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



NGUYỄN VĂN KHI

NGHIÊN CỨU GIẢI PHÁP CGNAT CHO
NHÀ CUNG CẤP DỊCH VỤ VIỄN THÔNG

Chuyên Ngành : Kỹ thuật Viễn thông
Mã Số : 8.52.02.08

TÓM TẮT LUẬN VĂN THẠC SỸ
(Theo định hướng ứng dụng)

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TS. LÊ NHẬT THĂNG

Phản biện 1:

Phản biện 2:

Luận văn này được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc:

Có thể tìm hiểu luận văn này tại:

Thư viện của Học viện Công nghệ Bưu chính Viễn thông

CHƯƠNG 1 TỔNG QUAN VỀ NAT

1.1 Giới thiệu về NAT

Kết nối Internet hiện đại ngày nay đều phải sử dụng đến kỹ thuật NAT. NAT cho phép một (hay nhiều) địa chỉ IP nội miền được ánh xạ với một (hay nhiều) địa chỉ IP ngoại miền.

Địa chỉ IP là chuỗi số có chiều dài 32 bit (IPv4) hoặc 128 bit (IPv6) dùng để định danh một thiết bị mạng trên hệ thống mạng giúp chúng nhận diện và liên lạc với nhau. Trong một mô hình mạng, mỗi một thiết bị mạng chỉ có một địa chỉ IP duy nhất.

Cùng với sự bùng nổ Internet như hiện nay và nhu cầu sử dụng hệ thống mạng ngày càng gia tăng, không gian địa chỉ IPv4 bắt đầu bị giới hạn. Giải pháp đưa ra là thiết kế lại định dạng địa chỉ IP, cho phép nhiều địa chỉ IP hơn nữa (cụ thể là IPv6). Tuy nhiên giải pháp này vẫn đang khó khăn trong quá trình triển khai tại những mô hình mạng thực tế của các tổ chức doanh nghiệp cũng như các hộ gia đình. Do đó giải pháp tốt nhất là sử dụng đến kỹ thuật NAT. NAT cho phép một thiết bị như bộ định tuyến - Router hoạt động như một thiết bị đại diện trung gian giữa Internet và mạng nội bộ, cho phép các thiết bị trong mạng nội bộ được kết nối ra ngoài mạng internet với thiết bị đại diện là Router thực hiện chức năng NAT [8].

1.1.1 Nhiệm vụ của NAT

NAT giống như một Router, chuyển tiếp các gói tin giữa những lớp mạng khác nhau trên một mạng lớn. NAT dịch hay thay đổi một hoặc cả hai địa chỉ bên trong một gói tin khi gói tin đó đi qua một Router, hay một số thiết bị khác. Thông thường NAT thường thay đổi địa chỉ thường là địa chỉ riêng (IP Private) của một kết nối mạng thành địa chỉ công cộng (IP Public).

NAT cũng có thể coi như một Firewall (tường lửa) cơ bản. NAT duy trì một bảng thông tin về mỗi gói tin được gửi qua. Khi một máy tính trên mạng kết nối đến 1 website trên Internet header của địa chỉ IP nguồn được thay thế bằng địa chỉ Public đã được cấu hình sẵn trên NAT sever, sau khi có gói tin trở về NAT dựa vào bảng ghi mà nó đã lưu về các gói tin, thay đổi địa chỉ IP đích thành địa chỉ của PC trong mạng và chuyển tiếp đi. Thông qua cơ chế đó quản trị mạng có khả năng lọc các gói tin được gửi đến hay gửi từ một địa chỉ IP và cho phép hay ngăn truy cập đến một port cụ thể [6].

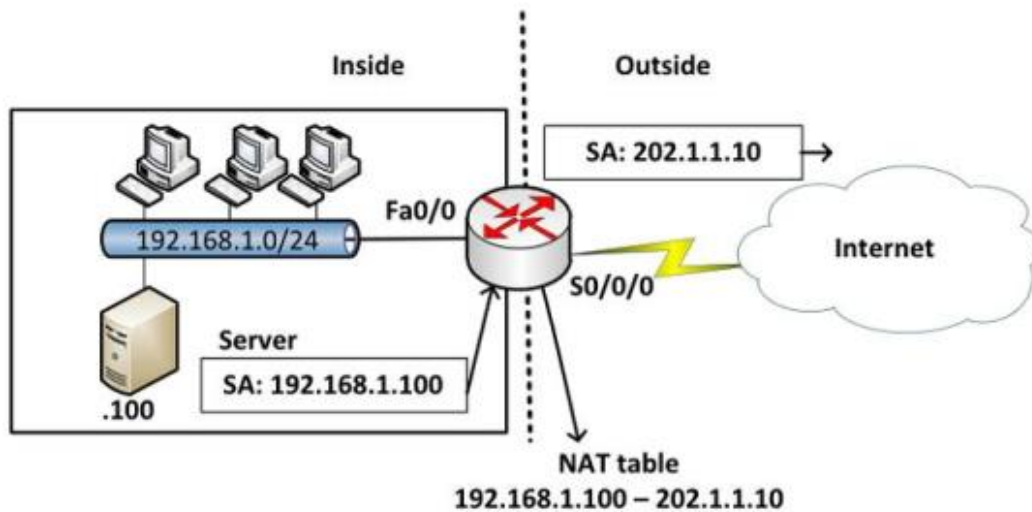
Triển khai NAT có thể thực hiện tại các vị trí:

- Thực hiện NAT tại thiết bị đầu cuối khách hàng

- Thực hiện NAT tại nhà cung cấp dịch vụ.

1.1.2 Thực hiện NAT tại thiết bị đầu cuối khách hàng

Static NAT (NAT tĩnh):



Hình 1-1: Static NAT

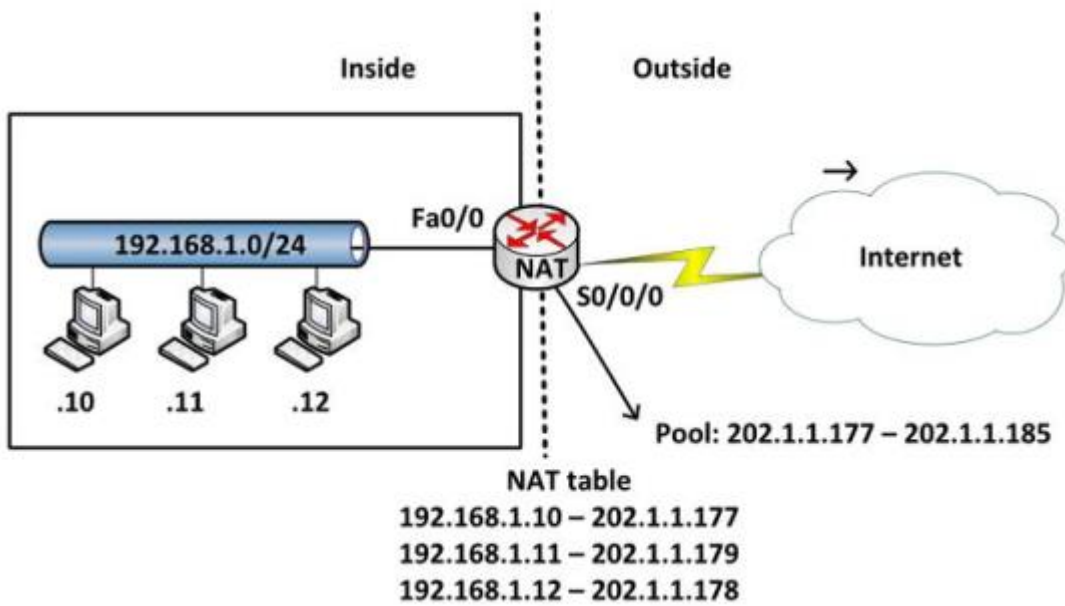
Static NAT (NAT tĩnh) là phương thức NAT một - một. Một IP trong mạng nội bộ, mạng khách hàng sẽ được ánh xạ với một IP công cộng.

NAT tĩnh được sử dụng khi thiết bị cần truy cập từ bên ngoài mạng.

Trong hình 1-1 Static NAT (NAT tĩnh), địa chỉ IP của máy tính là 192.168.1.100 luôn được Router biên dịch đến địa chỉ IP 202.1.1.10.

Dynamic NAT (NAT động):

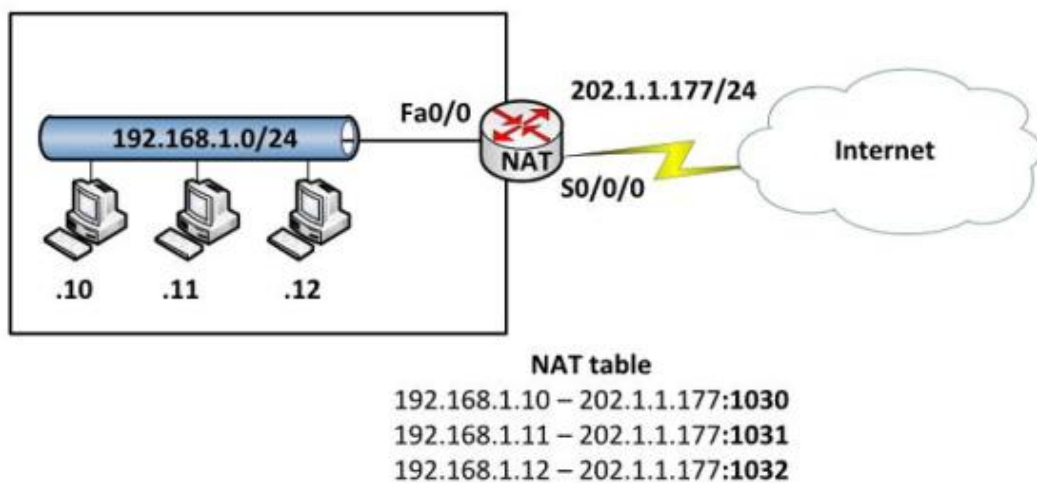
Dynamic NAT được dùng để ánh xạ một địa chỉ IP này sang một địa chỉ khác một cách tự động, thông thường là ánh xạ từ một địa chỉ cục bộ sang một địa chỉ được đăng ký. Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán một thiết bị bên trong mạng.



Hình 1-2: Dynamic NAT

NAT Overload:

NAT Overload là một dạng của Dynamic NAT (NAT động), nó thực hiện ánh xạ nhiều địa chỉ IP thành một địa chỉ (many - to - one) và sử dụng các địa chỉ số cổng khác nhau để phân biệt cho từng chuyển đổi. NAT Overload còn có tên gọi là PAT (Port Address Translation). Chỉ số cổng được mã hóa 16 bit, do đó có tới 65536 địa chỉ nội bộ có thể được chuyển đổi sang một địa chỉ công cộng.



Hình 1-3: Nat Overload

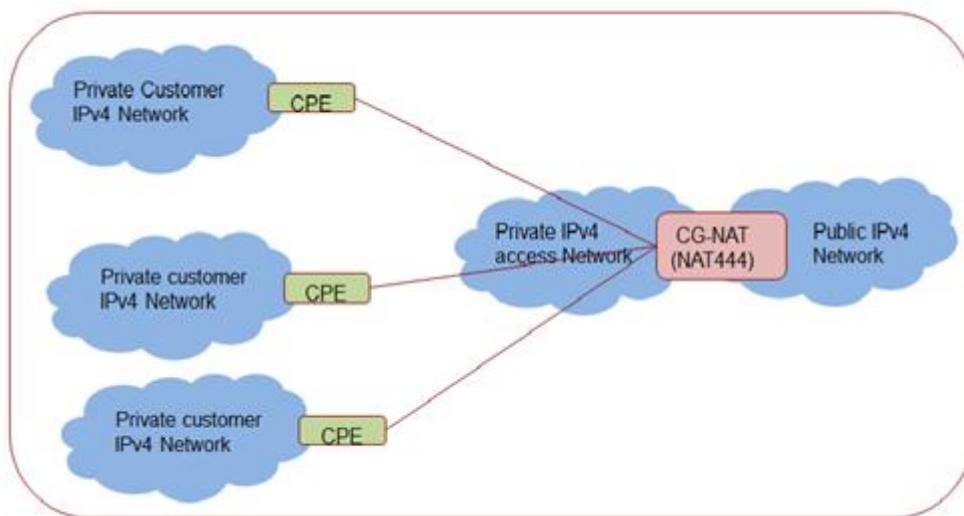
1.1.3 Thực hiện NAT tại nhà cung cấp dịch vụ

Carrier Grade Network Address Translation (CGN) – Dịch địa chỉ mạng tại nhà cung cấp dịch vụ.

Địa chỉ là yếu tố cơ bản đối với cách thức hoạt động của Internet. Sự phát triển vượt bậc của Internet đã dẫn đến việc Internet hết địa chỉ ở định dạng hiện tại, IPv4. Sự phát triển này đã được dự đoán từ lâu và một định dạng kế nhiệm, được gọi là IPv6, đã sẵn sàng được áp dụng.

Tuy nhiên, quá trình chuyển đổi từ IPv4 sang IPv6 sẽ mất nhiều năm. Quá trình chuyển đổi sẽ yêu cầu nâng cấp các ứng dụng Internet, thiết bị, dịch vụ, thiết bị điện tử tiêu dùng và mạng. Trong quá trình chuyển đổi này, các nhà khai thác mạng sẽ chạy các mạng mà IPv4 và IPv6 cùng tồn tại. Có một số lượng lớn các cơ chế chuyển đổi IPv4 sang IPv6, tất cả đều vẫn yêu cầu địa chỉ IPv4, mặc dù không gian địa chỉ IPv4 sắp cạn kiệt.

Do đó, điều quan trọng là phải tìm cách sử dụng tối đa các địa chỉ IPv4 có sẵn. Một phương pháp để tiết kiệm tài nguyên IPv4 là sử dụng phương pháp dịch địa chỉ mạng tại nhà cung cấp dịch vụ (CG-NAT) [1]



Hình 1-4: Mô hình CGNAT

1.2 Quá trình chuyển đổi IPv4 sang IPv6

Thách thức trong việc chuyển đổi sang IPv6:

Tương thích phần cứng và phần mềm:

Độ dài và Khối lượng địa chỉ IPv6:

Giao diện địa chỉ IPv6:

Xếp chồng kép với IPv4 và IPv6:

Các bước để thực hiện chuyển đổi IPv4 sang IPv6.

Bước 1 – Xác định mạng IP của tổ chức, cá nhân muốn chuyển đổi.

Bước 2 - Lập kế hoạch triển khai IPv6

Bước 3 - Lập mô hình mạng Dual-stacking

Bước 4 - Ảnh xạ IPv4 và IPv6 với nhau

Bước 5 - Thực hiện Kế hoạch, Mô hình và Lập bản đồ

Bước 6 - Quản lý mạng Dual-Stacked Network mới.

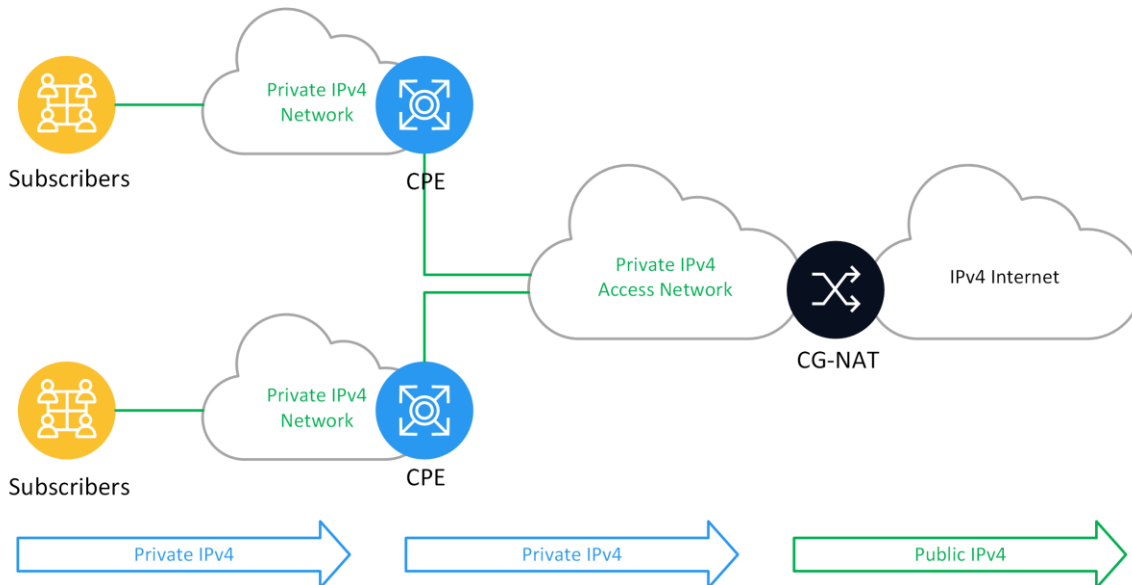
1.3 Kết luận chương 1

Tính đến năm 2018, tất cả năm RIR đã hết địa chỉ IPv4. Việc chuyển đổi toàn bộ sang địa chỉ IPv6 mang lại rủi ro cho tổ chức trong việc gián đoạn liên lạc và mất doanh thu cũng như khách hàng tiềm năng do các thiết bị mạng trong hạ tầng của tổ chức và doanh nghiệp chưa hòa toàn sẵn sàng triển khai kết nối toàn bộ sang IPv6. Việc chuyển đổi cần đưa ra kế hoạch cụ thể, từng bước để chuyển đổi. Mặc dù vậy, việc thực hiện nhiệm vụ này vẫn đòi hỏi thời gian và nỗ lực từ phía tổ chức. Hỗ trợ việc lập kế hoạch và từng bước thực hiện, các tổ chức có thể sử dụng các công cụ để giám sát và quản lý lộ trình chuyển đổi của hệ thống. Nhằm hỗ trợ khách hàng trong giai đoạn chuyển đổi hệ thống từ IPv4 sang IPv6, các tổ chức cung cấp dịch vụ mạng thường triển khai hệ thống dịch địa chỉ tại phía nhà mạng để hỗ trợ khách hàng của mình kéo dài thời gian sử dụng địa chỉ IPv4 và có thời gian để chuyển đổi hệ thống mạng sang IPv6, tại phía khách hàng việc chuyển đổi sẽ mất nhiều thời gian cần có lộ trình và kế hoạch cụ thể, phụ thuộc vào kinh phí đầu tư của tổ chức, cá nhân bỏ ra để chuyển đổi hệ thống. Giải pháp được các nhà cung cấp dịch vụ Viễn thông – Công nghệ thông tin triển khai đó là CGNAT (Carrier Grade Network Address Translation).

CHƯƠNG 2 GIẢI PHÁP CGNAT

2.1 Khái niệm CGNAT

Carrier-grade NAT (CGN hay CGNAT) NAT còn được gọi là NAT quy mô lớn (LSN), là một loại dịch địa chỉ mạng (NAT) để sử dụng trong thiết kế mạng IPv4. Với CGNAT, các mạng phía khách hàng đặc biệt là các mạng dân cư, được định cấu hình với các địa chỉ mạng riêng được dịch sang địa chỉ IPv4 công cộng bằng các thiết bị NAT trung gian được đặt trong mạng của nhà cung cấp dịch vụ ISP, cho phép chia sẻ các nhóm nhỏ địa chỉ công cộng giữa nhiều kết cuối phía khách hàng. Điều này thay đổi chức năng NAT và cấu hình của nó từ cơ sở của khách hàng sang mạng của nhà cung cấp dịch vụ Internet (mặc dù NAT "thông thường" tại cơ sở của khách hàng thường sẽ được sử dụng). NAT mức nhà cung cấp dịch vụ thường được sử dụng để giảm thiểu tình trạng cạn kiệt địa chỉ IPv4 [1], [11], [12].



Hình 2-1: Carrier-grade NAT

Một kịch bản sử dụng của CGN đã được gán nhãn là NAT444, vì một số kết nối của khách hàng với dịch vụ Internet trên Internet công cộng sẽ đi qua ba miền địa chỉ IPv4 khác nhau: mạng riêng của khách hàng, mạng riêng của nhà cung cấp dịch vụ và Internet công cộng.

Một kịch bản CGN khác là Dual-Stack Lite, trong đó mạng của nhà cung cấp dịch vụ sử dụng IPv6 và do đó chỉ cần hai miền địa chỉ IPv4.

Nếu ISP triển khai CGN và sử dụng không gian địa chỉ RFC 1918 (địa chỉ thuộc RFC 1918 không có khả năng định tuyến trên mạng Internet công cộng, còn gọi là địa chỉ private) để đánh số các cổng của khách hàng, nguy cơ xung đột địa chỉ và do đó lỗi định tuyến sẽ phát sinh khi mạng khách hàng đã sử dụng không gian địa chỉ RFC 1918.

Nhược điểm

NAT cấp nhà cung cấp dịch vụ thường ngăn không cho khách hàng ISP sử dụng chuyển tiếp công, vì quá trình dịch địa chỉ mạng (NAT) thường được thực hiện bằng cách ánh xạ các cổng của thiết bị NAT trong mạng với các cổng khác trong giao diện bên ngoài. Điều này được thực hiện để bộ định tuyến có thể ánh xạ các phản hồi đến đúng thiết bị; trong mạng NAT cấp nhà cung cấp dịch vụ, mặc dù bộ định tuyến ở đầu cuối của người tiêu dùng có thể được định cấu hình để chuyển tiếp công, nhưng "bộ định tuyến chính" của ISP, chạy CGN, sẽ chặn chuyển tiếp công này vì cổng thực tế sẽ không phải là cổng được định cấu hình bởi người tiêu dùng.

Trong trường hợp cấm lưu lượng truy cập dựa trên địa chỉ IP, hệ thống có thể chặn lưu lượng truy cập của người dùng gửi thư rác bằng cách cấm địa chỉ IP của người dùng. Nếu người dùng đó tình cờ sử dụng NAT cấp nhà cung cấp dịch vụ, những người dùng khác chia sẻ cùng địa chỉ công khai với người gửi spam sẽ bị chặn nhầm.

2.2 Triển khai về kỹ thuật

2.2.1 Tại sao cần CGNAT

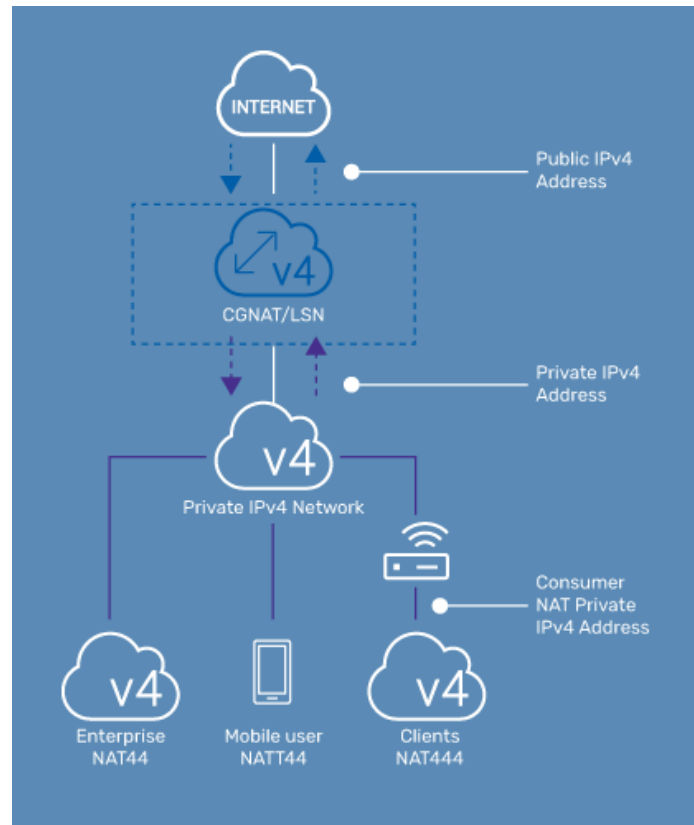
Các kịch bản triển khai CGN

Động lực để triển khai CGN

2.2.2 Kỹ thuật thực hiện CGNAT

Các nhà cung cấp dịch vụ, bao gồm ISP, cáp băng thông rộng và các nhà khai thác di động, đã sớm yêu cầu một công nghệ để hỗ trợ khách hàng tiếp tục sử dụng được IPv4 trước khi toàn mạng được chạy IPv6, đáp ứng một số yêu cầu về hiệu suất và tính năng riêng tại khách hàng.

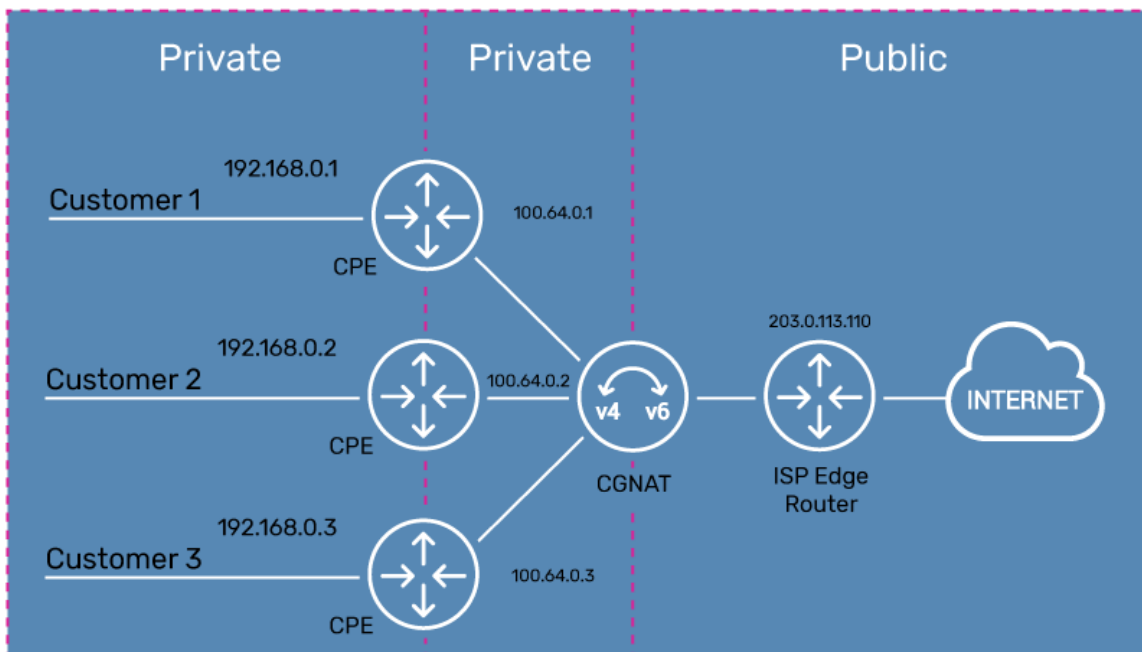
NAT quy mô lớn (LSN) hoặc NAT 444. NAT cấp sóng mang (CGNAT) là một công nghệ hoàn thiện để triển khai



Hình 2-2: Các kịch bản triển khai chung cho NAT44 và NAT444

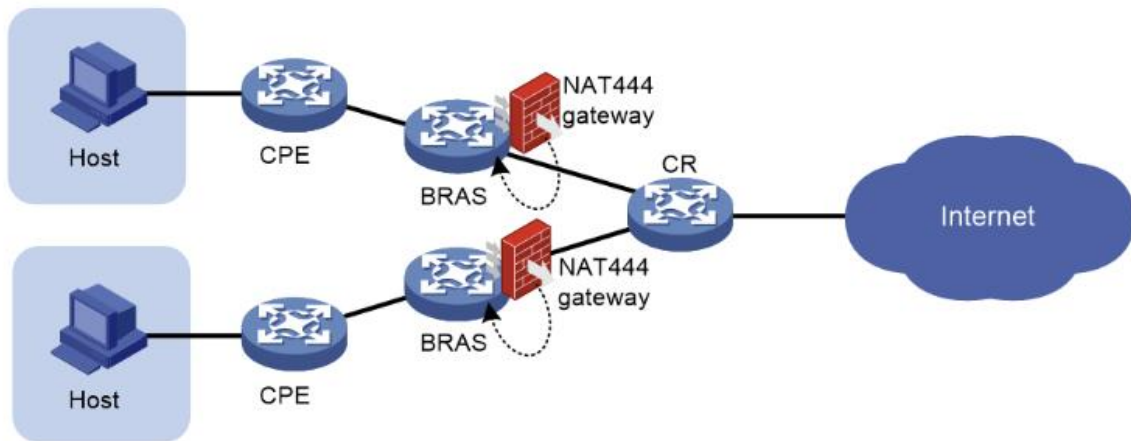
Triển khai NAT444

Sơ đồ hình 2-3 cho thấy việc triển khai NAT444 (private, private, public) với ba mạng khách hàng, tất cả đều sử dụng cùng một không gian địa chỉ IPv4 nội bộ với các địa chỉ IPv4 bên ngoài dành riêng cho ISP dùng chung một địa chỉ IPv4 công cộng.

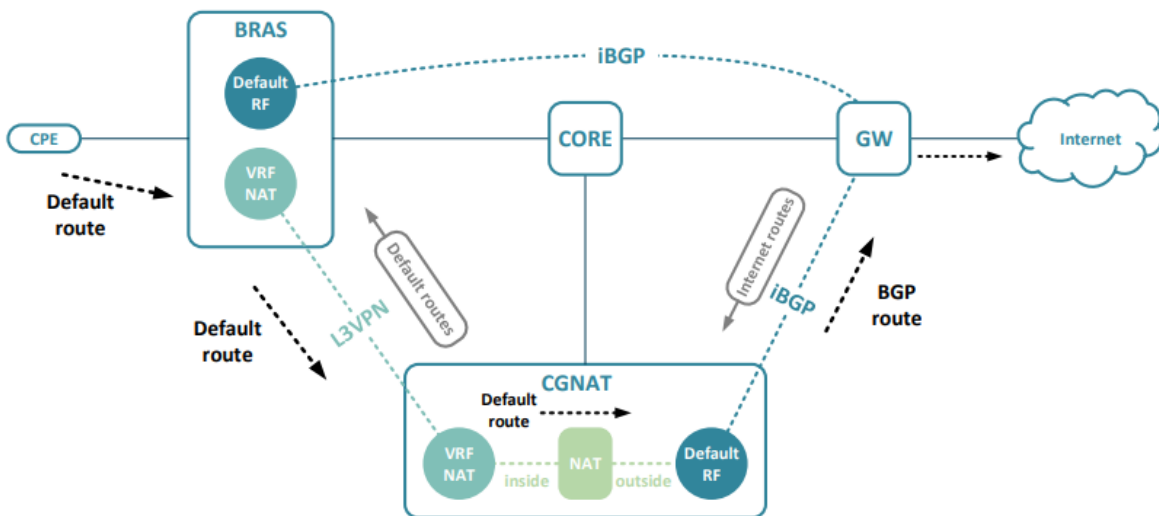


Hình 2-3: CGNAT triển khai NAT444 với dịch địa chỉ mạng private to private to public

Trong chương 1 đã trình bày về NAT truyền thống (NAT Overload) được gọi là NAT44 vì nó dịch một địa chỉ IPv4 cho một địa chỉ IPv4 khác (4 thành 4). Với CGNAT gọi là NAT444, còn được gọi là NAT cấp độ nhà cung cấp (CGN) tại một thời điểm và hiện được gọi là NAT quy mô lớn (LSN) NAT bộ ba (IPv4 đến IPv4 đến IPv4). Kỹ thuật này thực hiện nhân đôi NAT, có nghĩa là tăng gấp đôi sự can thiệp với lưu lượng mạng và cản trở nguyên tắc trong suốt từ đầu cuối này đến đầu cuối kia.

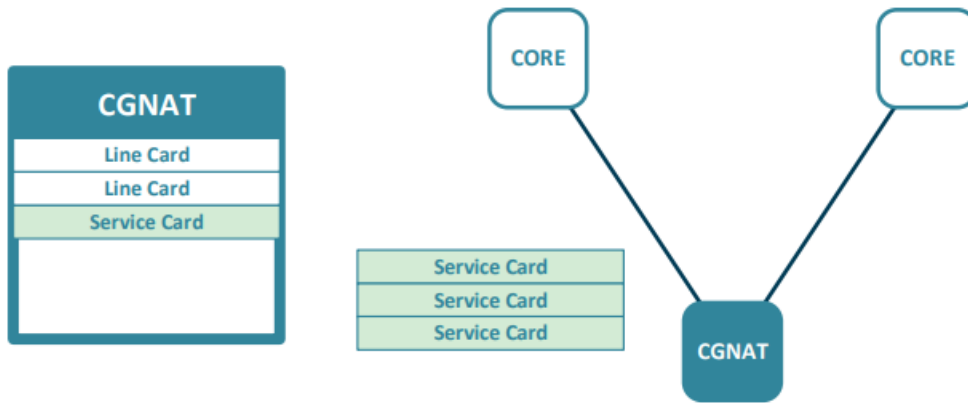


Hình 2-4: Mô hình NAT 444



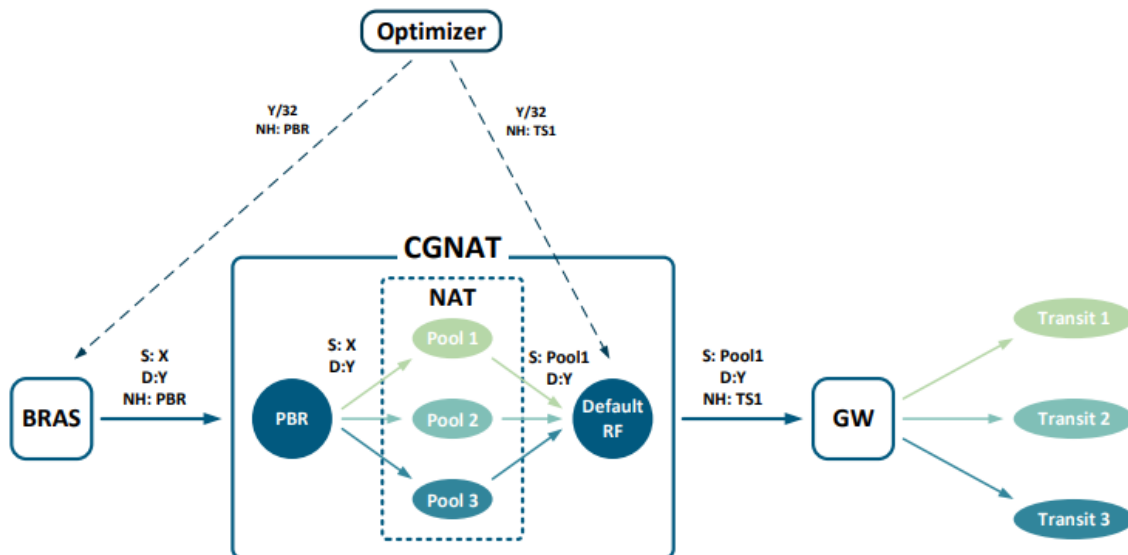
Hình 2-5: Luồng lưu lượng từ khách hàng ra Internet qua CGNAT

Thiết kế đảm bảo dự phòng



Hình 2-6: Thiết kế dự phòng cho hệ thống CGNAT

Thiết kế tối ưu hóa tuyến đường đi qua mạng



Hình 2-7: Tối ưu hóa tuyến đường

2.3 Một số dòng thiết bị để thực hiện giải pháp CGNAT tại các ISP

Để triển khai giải pháp CGNAT tại các ISP, các hãng thiết bị thường được sử dụng như Huawei, Juniper, Cisco [9], [10].



Thiết bị Huawei:

Hình 2-8: Huawei ME60 Series

Thiết bị Juniper:

Hệ điều hành Junos cho phép người dùng triển khai và mở rộng các giải pháp CGNAT (NAT quy mô lớn) của họ dựa trên loại giao diện dịch vụ được sử dụng để triển khai.



Hình 2-9: Juniper MX Series

Thiết bị Cisco:

Đối với thiết bị Cisco, các dòng thiết bị cần chạy hệ điều hành Cisco IOS XR software Release 3.9.1 hoặc cao hơn để cung cấp chức năng CGNAT.

Ví dụ dòng sản phẩm Cisco ASR 1000 Router series:



Hình 2-10: Cisco ASR 1000 Router series

Đối với thiết bị Cisco, CGN được kích hoạt trên mode toàn cục. Cấu hình NAT cũ phải được xóa trước khi bật CGN. Tính năng gì được bật bằng lệnh:

ASR1000(config)# ip nat settings mode cgn

2.4 Kết luận chương 2

Trong chương này đã trình bày về khái niệm CGNAT, kỹ thuật triển khai CGNAT tại nhà cung cấp dịch vụ. Phân tích những kỹ thuật NAT 444, những dịch vụ không ảnh hưởng, những dịch vụ có khả năng bị ảnh hưởng. Phân tích những lưu ý cần quan tâm khi triển khai hệ thống CGNAT như Hiệu suất thiết bị, khả năng sẵn sàng, khả năng quản lý tập trung, khả năng bảo mật hệ của hệ thống cũng như phương pháp quản trị rủi ro để đảm bảo an toàn mạng lưới khi triển khai hệ thống. Trong chương 2 cũng đã giới thiệu một số hãng thiết bị được các nhà cung cấp dịch vụ viễn thông, công nghệ thông tin có thể sử dụng trên mạng để cung cấp chức năng CGNAT như Huawei, Juniper, Cisco.

CHƯƠNG 3 TRIỂN KHAI CGNAT TRONG MẠNG BĂNG RỘNG CỐ ĐỊNH CỦA VNPT

3.1 Giải pháp triển khai CGNAT trong mạng VNPT

Mục đích triển khai CGNAT trong mạng VNPT

Hệ thống CGNAT được triển khai nhằm mục đích giải quyết vấn đề cạn kiệt địa chỉ IPv4 public cấp cho thuê bao Internet trong khi hiện nay các dịch vụ/ứng dụng sử dụng IPv4 vẫn còn phổ biến.

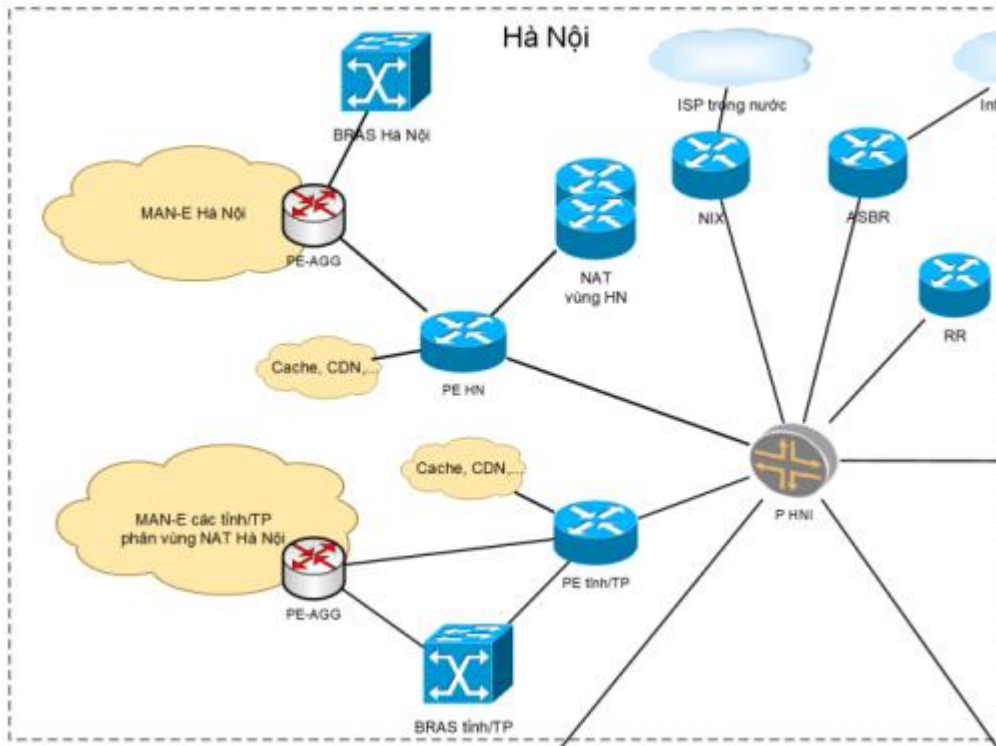
Phương án triển khai

Mô hình kết nối

Mạng băng rộng VNPT được tổ chức thành 3 vùng lớn. Hà Nội, Thành phố. Hồ Chí Minh, Đà Nẵng và cần thực hiện triển khai cả 03 vùng.

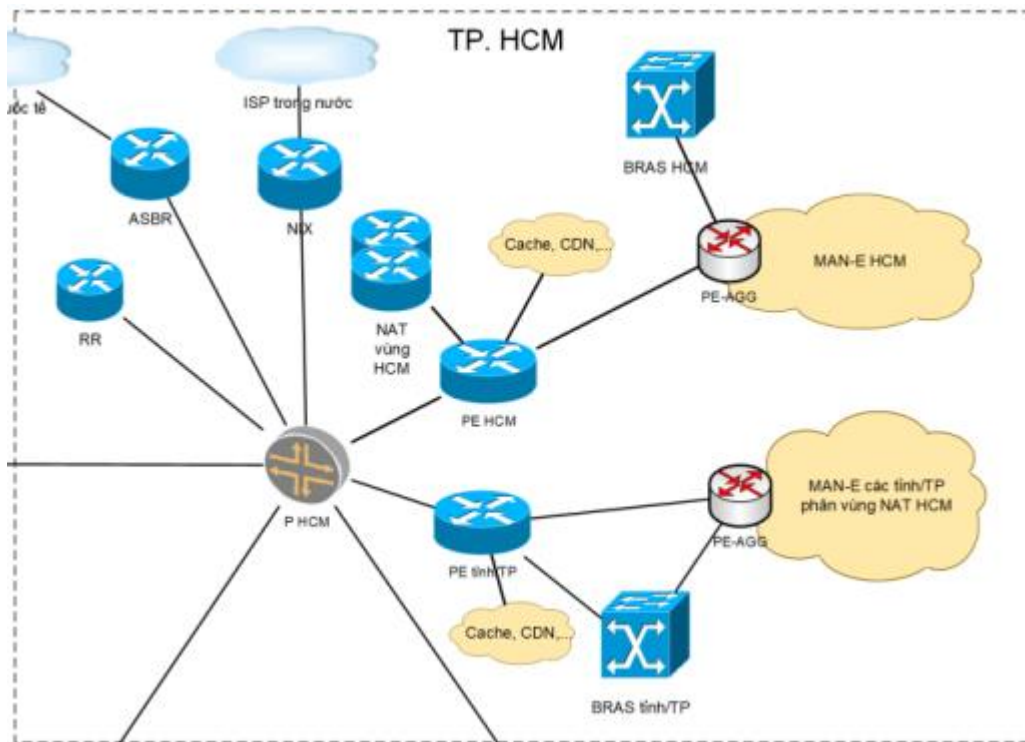
Thiết bị CGNAT trong mỗi vùng phục vụ thuê bao Internet của các tỉnh/Thành phố thuộc vùng đó, không dự phòng giữa các vùng để giảm mức độ phức tạp định tuyến lưu lượng, tránh xung đột địa chỉ IP.

Các thiết bị CGNAT trong mỗi vùng đảm bảo dự phòng cho nhau.



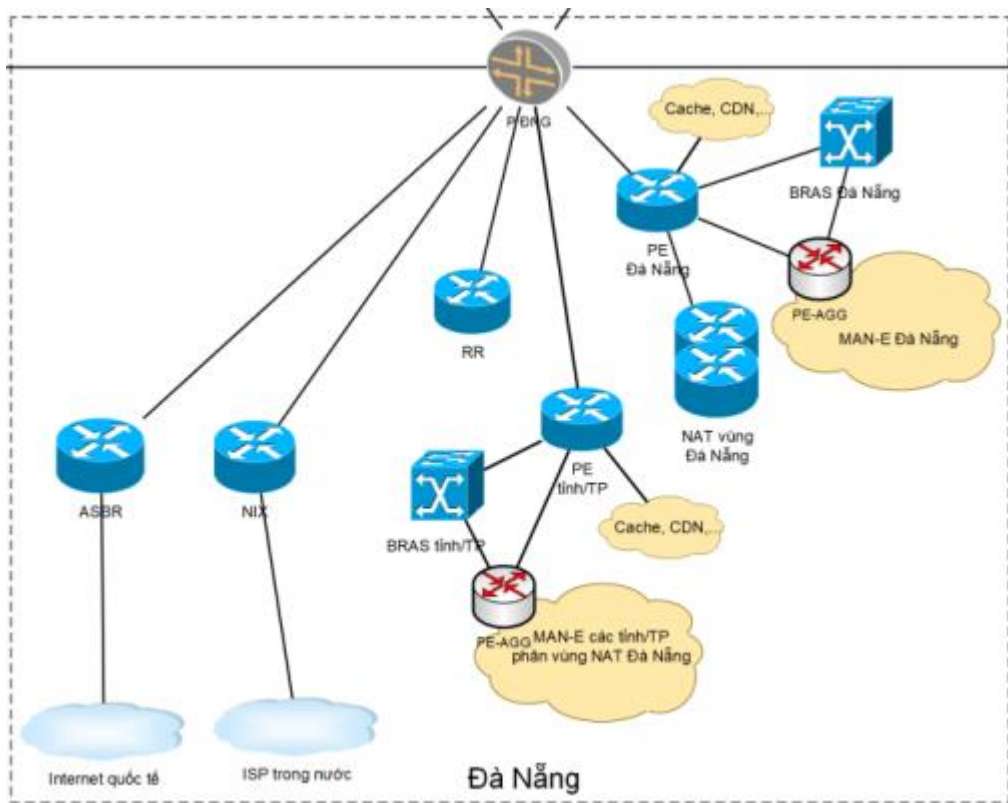
Hình 3-1: Kết nối thiết bị CGNAT tại vùng Hà Nội

Các thiết bị CGNAT được quy hoạch và gắn trực tiếp vào miền PE tại Hà Nội, từ thiết bị PE sẽ kết nối vào Router core P Hà Nội để đi vào mạng Internet.



Hình 3-2: Kết nối thiết bị CGNAT tại vùng thành phố Hồ Chí Minh

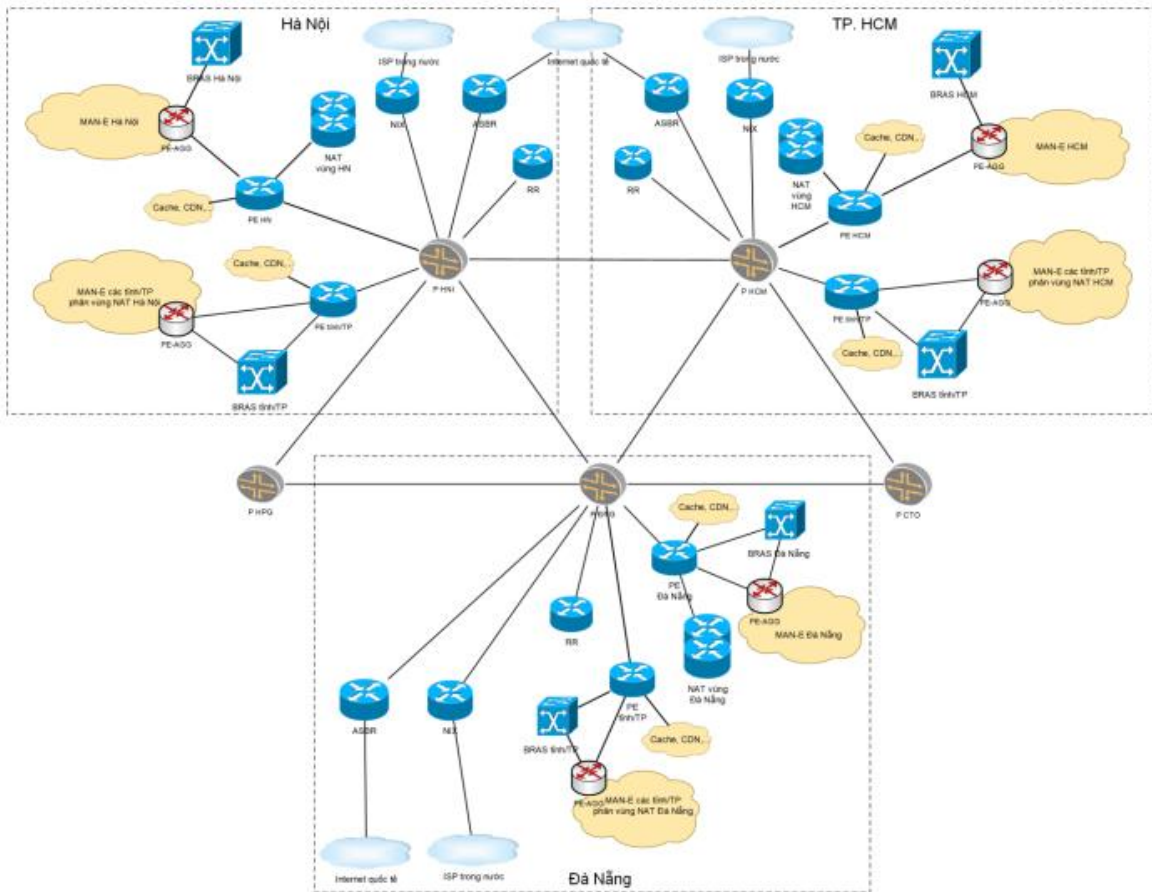
Các thiết bị CGNAT được quy hoạch và gắn trực tiếp vào miền PE tại Hồ Chí Minh, từ thiết bị PE sẽ kết nối vào Router core P Hồ Chí Minh để đi vào mạng Internet.



Hình 3-3: Kết nối thiết bị CGNAT tại vùng Đà Nẵng

Các thiết bị CGNAT được quy hoạch và gắn trực tiếp vào miền PE tại Đà Nẵng, từ thiết bị PE sẽ kết nối vào Router core P Đà Nẵng để đi vào mạng Internet.

Các vùng được kết nối với nhau như Hình 3-4: Kết nối các vùng



Hình 3-4: Kết nối CGNAT tại 3 vùng

Ba vùng được kết nối với nhau bởi các P tại, Hà Nội, Đà Nẵng, Thành phố Hồ Chí Minh.

Cấp địa chỉ IP cho thuê bao

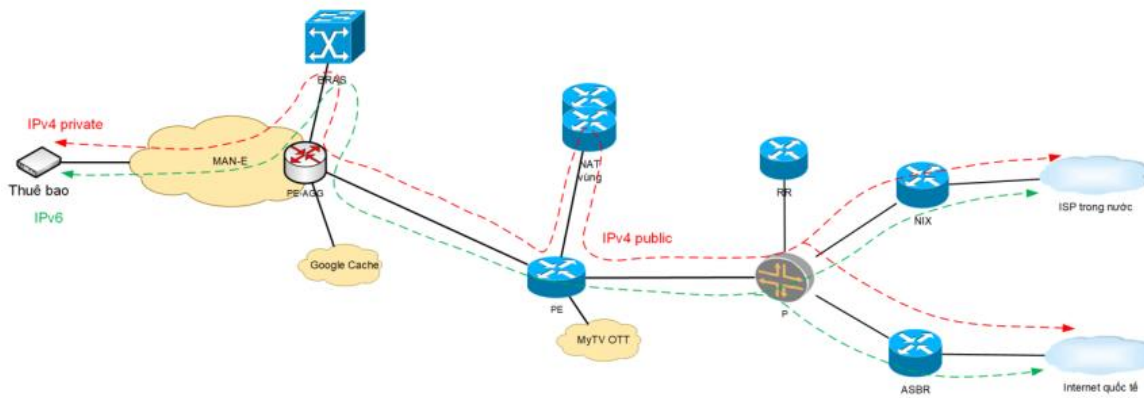
Thuê bao CGNAT được cấp địa chỉ IP theo mô hình dual-stack, nhận đồng thời địa chỉ IPv4 private và địa chỉ IPv6.

Mô hình lưu lượng dịch vụ

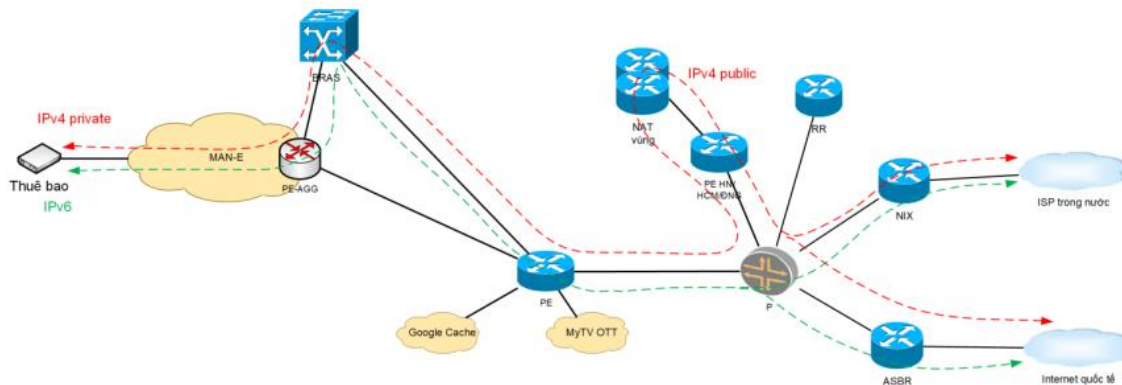
Dịch vụ Internet

Lưu lượng IPv4 private được truyền tải qua thiết bị CGNAT để thực hiện NAT IPv4 private thành IPv4 public trước khi ra Internet IPv4.

Lưu lượng IPv6 được truyền tải trực tiếp với Internet IPv6 như mô hình dualstack hiện nay VNPT đang triển khai.



Hình 3-5: Mô hình dịch vụ Internet tại Hà Nội và thành phố Hồ Chí Minh



Hình 3-6: Mô hình dịch vụ Internet tại các tỉnh/Thành phố

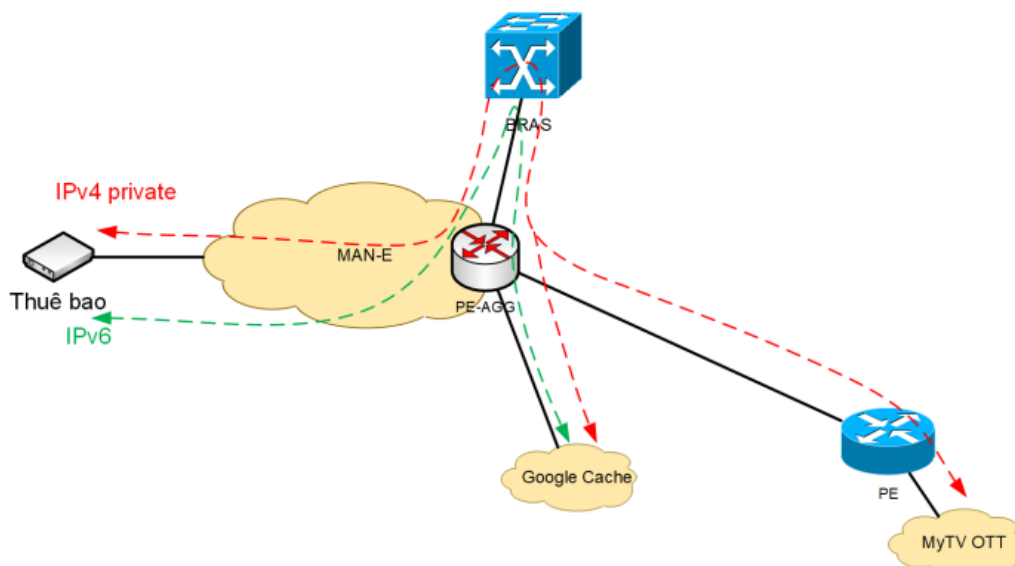
Kết nối với Google Cache, MyTV OTT:

Khi thực hiện triển khai CGNAT trong mạng, điều rất cần quan tâm là định tuyến các lưu lượng không cần thiết phải đi qua CGNAT để tránh ảnh hưởng đến năng lực CGNAT và chất lượng dịch vụ của khách hàng. Như đối với các dịch vụ IPv6, Google Cache, MyTV OTT.

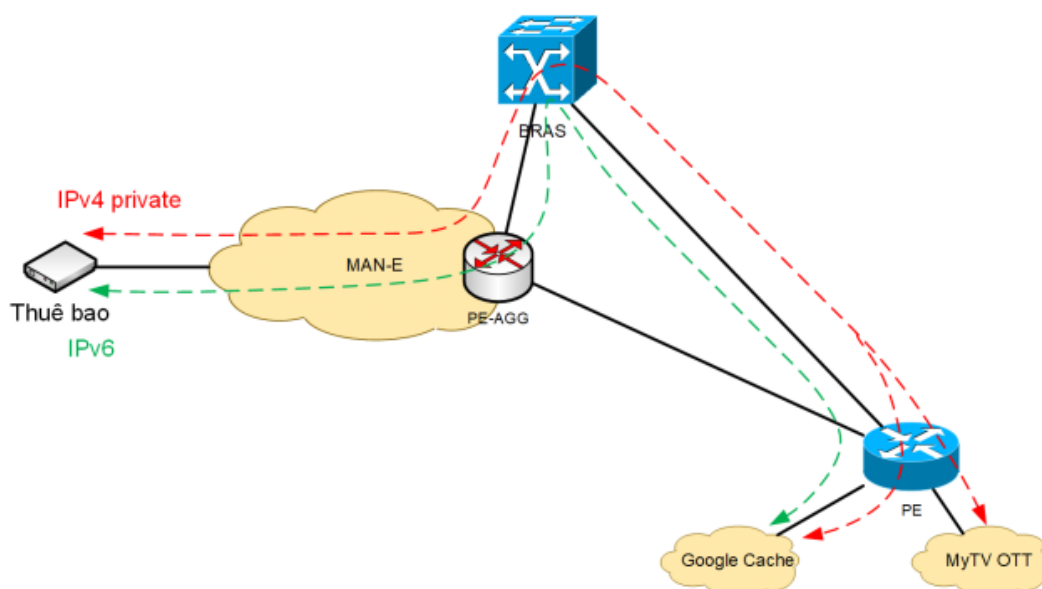
Lưu lượng IPv4 private và IPv6 được truyền tải trực tiếp với các hệ thống Cache. Lưu lượng IPv4 private được truyền tải trực tiếp với hệ thống MyTV OTT.

Triển khai các kết nối để xử lý hướng tuyến cho các dịch vụ này cần triển khai như sau:

- Phân tách lưu lượng MyTV OTT
- Phân tách lưu lượng IPv6
- Phân tách lưu lượng đến các Cache



Hình 3-7: Mô hình kết nối Google Cache, MyTV OTT tại Hà Nội, thành phố Hồ Chí Minh



Hình 3-8: Mô hình kết nối Google Cache, MyTV OTT tại các tỉnh/Thành phố

Kế hoạch thực hiện:

Giai đoạn 1: Triển khai nhanh để giải phóng địa chỉ IPv4 public phục vụ phát triển thuê bao FiberVNN mới.

Giai đoạn 2: Triển khai toàn mạng.

3.2 Cài đặt thực hiện.

Giai đoạn 1:

Thực hiện nhanh trong giai đoạn đầu triển khai CGNAT để giải phóng khoảng 100.000 địa chỉ IPv4 public phục vụ phát triển thuê bao FiberVNN mới.

Hạn chế tác động đến mạng lưới, thiết bị ONT (kết cuối mạng quang), không ảnh hưởng đến chất lượng dịch vụ đang cung cấp cho thuê bao.

Các bộ phận kỹ thuật phối hợp thực hiện thuận lợi, thời gian triển khai nhanh

Phương án thực hiện:

Phân bổ tạm thời 01 dải địa chỉ IPv4 public dành cho thuê bao NAT (tạm gọi là địa chỉ "IP before NAT").

ONT (kết cuối mạng quang), của thuê bao NAT được BRAS/BNG cấp "IP before NAT", về bản chất chính là địa chỉ IPv4 public nên không ảnh hưởng đến hoạt động bình thường của ONT hiện tại.

Thiết bị CGNAT thực hiện NAT "IP before NAT" thành IPv4 public thông thường để kết nối ra Internet.

Dải địa chỉ "IP before NAT" được sử dụng lại ở các vùng mà không gây xung đột địa chỉ và tiết kiệm tài nguyên.

Địa chỉ và lưu lượng IPv6 được cấp phát, truyền tải như mô hình hiện nay.

Các bước thực hiện

- Quy hoạch địa chỉ "IP before NAT", IPv4 public trên CGNAT
- Khai báo dải địa chỉ "IP before NAT" trên các BRAS/BNG cung cấp cho thuê bao NAT tại một số tỉnh thành phố.
- Rà soát CSDL số lượng thuê bao và các gói cước kỹ thuật của các thuê bao để lựa chọn thuê bao chuyển sang NAT:
- Chỉ chuyển các thuê bao Fiber16 sử dụng IP động (không chuyển IP tĩnh)
- Thống kê danh sách các thuê bao theo tỉnh/TP (để chuyển theo từng bước tránh ảnh hưởng diện rộng).
- Cấu hình thiết bị mạng cung cấp IPpool và VRF cho thuê bao Fiber16.
- Tạo các profile trên VISA, hệ thống DHSXKD,... tương ứng với các profile của gói Fiber16 (nhưng thêm thông tin CGNAT: Pool-IP và VRF).
- Cập nhật/điều chỉnh hệ thống VISA, CSDL, hỗ trợ cung cấp dịch vụ cho thuê bao NAT.
- Cấu hình thiết bị mạng thực hiện NAT.
- Thử nghiệm chuyển khoảng 10 thuê bao để đánh giá chất lượng dịch vụ.

- Lựa chọn, chuyển đổi dần dần các thuê bao FiberVNN gói cước thấp, dịch vụ đơn giản tại 05 tỉnh/TP sang sử dụng NAT.
- Mục tiêu giải phóng khoảng 100.000 địa chỉ IPv4 public.

Giai đoạn 2: Triển khai toàn mạng

Phạm vi triển khai:

Triển khai trên toàn mạng, quy mô triển khai tại từng tỉnh/Thành phố căn cứ tình hình phát triển dịch vụ thực tế.

Mục tiêu:

- Hoàn thiện hệ thống kỹ thuật: ONT, CGNAT, các hệ thống CNTT hỗ trợ.
- Hoàn thiện quy trình cung cấp dịch vụ, hỗ trợ khách hàng, xử lý sự cố
- Triển khai giải pháp CGNAT toàn trình.
- Đáp ứng cung cấp dịch vụ cho khoảng 1.400.000 thuê bao, phân bổ số lượng thuê bao qua CGNAT tại 03 vùng.

Phương án:

- Quy hoạch dải địa chỉ IPv4 private và IPv4 public dành cho thuê bao NAT.
- ONT (kết cuối mạng quang), của thuê bao NAT được BRAS/BNG cấp IPv4 private.
- Thiết bị CGNAT thực hiện NAT địa chỉ IPv4 private thành địa chỉ IPv4 public để kết nối ra Internet.
- Dải địa chỉ IPv4 private được sử dụng lại ở các vùng mà không gây xung đột địa chỉ và tiết kiệm tài nguyên.
- Địa chỉ và lưu lượng IPv6 được cấp phát, truyền tải từ thiết bị đầu cuối, đến các router hỗ trợ IPv6 trong mạng core, đi vào các bảng định tuyến IPv6 và ra ngoài internet.

Các bước thực hiện:

- Quy hoạch địa chỉ IPv4 public trên các node CGNAT.
- Quy hoạch địa chỉ IPv4 private cấp cho thuê bao NAT tại các tỉnh/TP.
- Quy hoạch địa chỉ IPv6 cho thuê bao NAT để thuận tiện cho việc quản lý, phân biệt với thuê bao FiberVNN khác (nếu cần).
- Cập nhật firmware ONT cho phép nhận dải địa chỉ IPv4 private NAT trên giao diện WAN của ONT.
- Cập nhật firmware ONT cho phép nhận dải địa chỉ IPv4 private trên giao diện WAN của ONT phục vụ các hệ thống quản lý

- Trên giao diện WAN ONT, chặn các dải địa chỉ IPv4 public không phải của VNPT và chặn các dải địa chỉ IPv4 private ngoài các dải quy hoạch.
- Phương án kết nối các node CGNAT với mạng VN2, định tuyến lưu lượng giữa CGNAT với Google Cache, MyTV CDN.
- Phương án phân tải thuê bao, dự phòng sự cố giữa các node trong 1 cụm CGNAT.
- Đánh giá hoạt động của ONT và chất lượng dịch vụ khi ONT nhận địa chỉ IPv4 private trên giao diện WAN.
- Theo dõi chất lượng dịch vụ, tổng hợp các tình huống, sự cố kỹ thuật, có thể xảy ra để lưu ý hướng dẫn các đơn vị khi triển khai thực tế trên mạng lưới.
- Hoàn thiện firmware (nếu cần).

Cấu hình trên thiết bị Juniper MX960 đóng vai trò CGNAT

```
juniper@HNI-CGNAT1_RE0> show configuration services | no-more | display set
set services service-set CGNAT syslog mode stream
set services service-set CGNAT syslog source-address 123.29.4.29
set services service-set CGNAT syslog stream SYSLOG_CGNAT category session-open
set services service-set CGNAT syslog stream SYSLOG_CGNAT category session-close
set services service-set CGNAT syslog stream SYSLOG_CGNAT host 123.29.11.91
set services service-set CGNAT syslog stream SYSLOG_CGNAT host port 514
set services service-set CGNAT syslog stream SYSLOG_CGNAT host log-tag HNI-
CGNAT-01
deactivate services service-set CGNAT syslog
set services service-set CGNAT service-set-options inactivity-non-tcp-timeout 300
set services service-set CGNAT service-set-options session-timeout 86400
set services service-set CGNAT service-set-options max-sessions-per-subscriber 2048
set services service-set CGNAT service-set-options tcp-session tcp-tickles 3
set services service-set CGNAT service-set-options tcp-session inactivity-tcp-timeout 1800
set services service-set CGNAT service-set-options tcp-session ignore-errors tcp
set services service-set CGNAT nat-rule-sets CGNAT-RULE
set services service-set CGNAT next-hop-service inside-service-interface ams0.10
set services service-set CGNAT next-hop-service outside-service-interface ams0.20
set services nat source pool TNN-PUBLIC address 14.191.28.0/24
set services nat source pool TNN-PUBLIC address 14.191.29.0/24
```

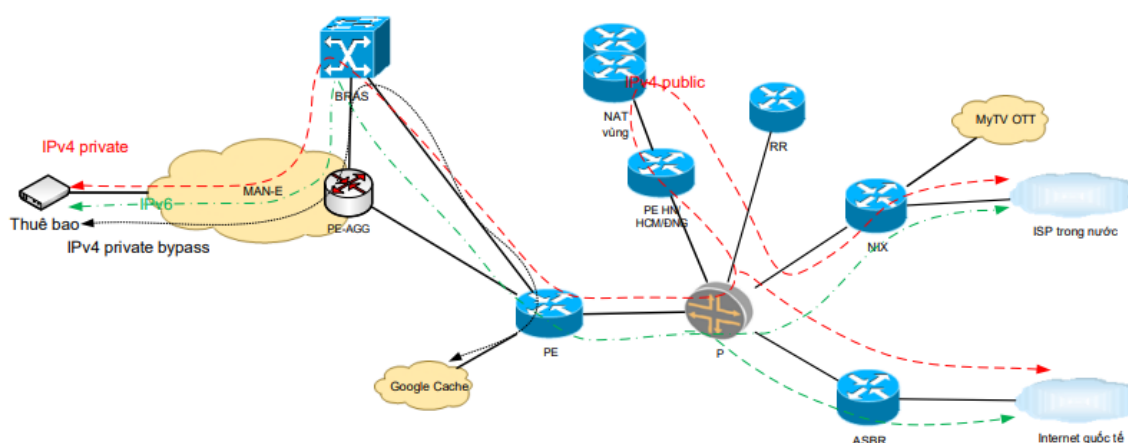
```
set services nat source pool TNN-PUBLIC port automatic random-allocation
set services nat source pool TNN-PUBLIC mapping-timeout 120
set services nat source rule-set CGNAT-RULE rule TNN-ALG match source-address-name
TNN-PRIVATE
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-sip
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-
pptp
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-ftp
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-rtsp
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-
traceroute
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-
icmp-all
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-ike
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-
dns-udp
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-
dns-tcp
set services nat source rule-set CGNAT-RULE rule TNN-ALG then source-nat pool TNN-
PUBLIC
set services nat source rule-set CGNAT-RULE rule TNN-ALG then source-nat mapping-
type address-pooling-paired
set services nat source rule-set CGNAT-RULE rule TNN-INTERNET match source-
address-name TNN-PRIVATE
set services nat source rule-set CGNAT-RULE rule TNN-INTERNET then source-nat pool
TNN-PUBLIC
set services nat source rule-set CGNAT-RULE rule TNN-INTERNET then source-nat
mapping-type address-pooling-paired
set services nat source rule-set CGNAT-RULE match-direction input
set services address-book global address TNN-POOL2-PRIVATE 113.188.192.0/19
set services address-book global address-set TNN-PRIVATE address TNN-POOL1-
PRIVATE
```

```
set services address-book global address-set TNN-PRIVATE address TNN-POOL2-PRIVATE
```

3.3 Đánh giá tính hiệu quả của giải pháp

Thực hiện giải pháp CGNAT, VNPT đã thực hiện giải phóng được khoảng 1.400.000 địa chỉ IPv4. Các hướng lưu lượng IPv6, Google Cache được đảm bảo, không xảy ra hiện tượng suy giảm chất lượng do được đi theo hướng tuyến khác.

- Lưu lượng IPv6 được khai báo trong suốt khi đi qua CGNAT bằng cách cấu hình tại route tại PE tỉnh.
- Lưu lượng IPv4 GGC được khai báo trong suốt khi đi qua CGNAT bằng cách cấu hình tại route tại PE tỉnh.
- Lưu lượng IPv4 còn lại, bao gồm cả lưu lượng MyTV OTT được dịch địa chỉ mạng qua các thiết bị CGNAT.



Hình 3-9: Hướng đi của các lưu lượng các thuê bao CGNAT

Trong giai đoạn chuyển đổi mạng sang IPv6, không phải tất cả các tổ chức, khách hàng sẵn sàng thực hiện được việc chuyển đổi, chính vì vậy song hành cùng với khách hàng, các nhà cung cấp dịch vụ, giải pháp triển khai để đảm bảo được việc vẫn cung cấp IPv4 cho khách hàng và hỗ trợ khách hàng dần chuyển đổi sang IPv6.

3.4 Kết luận chương 3

Trong chương này đã trình bày về giải pháp triển khai CGNAT trong mạng băng rộng cố định của VNPT

- Phân tích rõ kế hoạch, phương pháp triển khai
- Mô hình dịch vụ liên quan sau triển khai.

- Phân tích rõ từng giai đoạn thực hiện.
- Mục tiêu của mỗi giai đoạn.
- Đưa ra cách cài đặt cho các thiết bị CGNAT tại các vùng.
- Tổng kết đánh giá lại giải pháp triển khai CGNAT.

KẾT LUẬN

Nhu cầu sử dụng hệ thống mạng ngày càng gia tăng, không gian địa chỉ IPv4 bắt đầu bị giới hạn. Giải pháp đưa ra là thiết kế lại định dạng địa chỉ IP, cho phép nhiều địa chỉ IP hơn nữa (cụ thể là IPv6). Tuy nhiên giải pháp này vẫn đang khó khăn trong quá trình triển khai tại những mô hình mạng thực tế của các tổ chức doanh nghiệp cũng như các hộ gia đình. Do đó giải pháp tốt nhất là sử dụng đến kỹ thuật NAT.

NAT tại mức nhà cung cấp dịch vụ là một giải pháp khả thi. Tên kỹ thuật của CGNAT đề cập đến cách hoạt động của công nghệ, người dùng cuối được chỉ định một địa chỉ IP không thể định tuyến công khai mà đi qua một mạng trung gian được điều hành bởi nhà cung cấp băng thông rộng. Điều này cho phép các mạng của khách hàng (với không gian địa chỉ mạng nội bộ của riêng họ) định tuyến qua nhóm địa chỉ IPv4 Internet công cộng của ISP để truy cập Internet. Bằng cách chia sẻ địa chỉ IP công cộng cho nhiều địa chỉ IP riêng. Do đó, NAT đã trở thành một giải pháp quan trọng để kéo dài thời gian sử dụng địa chỉ IPv4 và chuyển đổi thành công sang IPv6. Các nhà cung cấp băng thông rộng trên toàn thế giới hiện đang triển khai NAT để chia sẻ một địa chỉ IP toàn cầu duy nhất giữa nhiều người đăng ký.

Luận văn đã thực hiện nghiên cứu:

- Việc chuyển đổi toàn bộ sang địa chỉ IPv6 mang lại rủi ro đáng kể cho tổ chức trong việc mất liên lạc và mất doanh thu cũng như khách hàng tiềm năng. Cần thận trọng là bắt đầu lập kế hoạch cho tương lai. Mặc dù vậy, việc thực hiện nhiệm vụ này vẫn đòi hỏi thời gian và nỗ lực từ phía tổ chức. Mạng phải được phân tích và lập kế hoạch cho mạng IPv6. IPAM có thể hỗ trợ việc này bằng cách sử dụng một số công cụ tự động.
- Trong giai đoạn chuyển đổi này, không phải tất cả các tổ chức, khách hàng sẵn sàng thực hiện được việc chuyển đổi, chính vì vậy song hành cùng với khách hàng, các nhà cung cấp dịch vụ cần có những giải pháp triển khai để đảm bảo được việc cung cấp dịch vụ cho khách hàng và hỗ trợ khách hàng dần chuyển đổi sang IPv6. Giải

pháp được các nhà cung cấp dịch vụ Viễn thông – Công nghệ thông tin triển khai đó là CGNAT (Carrier Grade Network Address Translation).

- Trình bày về khái niệm CGNAT, kỹ thuật triển khai CGNAT tại nhà cung cấp dịch vụ. Phân tích những kỹ thuật NAT 444, những dịch vụ không ảnh hưởng, những dịch vụ có khả năng bị ảnh hưởng cũng những lưu ý cần quan tâm khi triển khai hệ thống CGNAT như Hiệu suất thiết bị, khả năng sẵn sàng, khả năng quản lý tập trung, khả năng bảo mật hệ của hệ thống cũng như phương. Trong chương 2 cũng đã giới thiệu một số hãng thiết bị được các nhà cung cấp dịch vụ viễn thông, công nghệ thông tin có thể sử dụng trên mạng để cung cấp chức năng CGNAT như Huawei, Juniper, Cisco.
- Giải pháp triển khai CGNAT trong mạng băng rộng cố định của VNPT
Phân tích rõ kế hoạch, phương pháp triển khai. Mô hình dịch vụ liên quan sau triển khai. Phân tích rõ từng giai đoạn thực hiện. Mục tiêu của mỗi giai đoạn. Đưa ra cách cài đặt cho các thiết bị CGNAT tại các vùng. Tổng kết đánh giá lại giải pháp triển khai CGNAT.

Tuy nhiên, do việc triển khai CGNAT mới bắt đầu được thực hiện, việc đánh giá được kết quả thực hiện có đạt được mục tiêu đề ra về đảm bảo chất lượng dịch vụ không, tôi sẽ tiếp tục tìm hiểu và nghiên cứu, đánh giá lại trong thời gian triển khai 1 năm tới đây để tiếp tục hoàn thiện nghiên cứu của mình.