HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Văn Khi

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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2022

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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. LÊ NHẬT THĂNG

HÀ NỘI – 2022

LỜI CAM ĐOAN

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

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

Tác giả luận văn

Nguyễn Văn Khi

LỜI CẢM ƠN

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

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

Xin trân trọng cảm ơn quý thầy, cô Khoa Đào tạo Sau Đại học đã hướng dẫn và giúp đỡ tôi trong quá trình thực hiện luận văn.

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

Hà Nội, tháng năm 2022

Học viên thực hiện

Nguyễn Văn Khi

MỤC LỤC

DANH MỤC HÌNH VẼ

THUẬT NGỮ VÀ TỪ VIẾT TẮT

Viết tắt	Nghĩa tiếng Anh	Nghĩa tiếng Việt
6to4	Internet Protocol version 6 (IPv6) to version 4 (IPv4)	Giao thức IPv6 thành giao thức IPv4
ASBR	Autonomous System Boundary Router	Bộ định tuyến ranh giới hệ thống tự trị
BoD	bandwidth on demand	Băng thông theo yêu cầu
BRAS	Broadband remote access server	Máy chủ truy cập từ xa băng thông rộng
CDN	Content delivery network	Mạng phân phối nội dung
CGNAT	Carrier Grade Network Address Translation	Dịch địa chỉ mạng tại nhà cung cấp dịch vụ
Cisco ASR	Cisco Aggregation Services Routers	Bộ định tuyến dịch vụ tổng hợp của Cisco
CPE	Customer premises equipment	Thiết bị của khách hàng
CSDL		Cơ sở dữ liệu
DDA	Destination address accounting	Tính toán địa chỉ đích
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình máy chủ
DHCP6	Dynamic Host Configuration Protocol version 6	Giao thức cấu hình máy chủ phiên bản ipv6
DNS	Domain Name System	Hệ thống tên miền
DPC	Dense Port Concentrator	Bộ tập trung cổng dày đặc
Dynamic NAT	Dynamic network address translation	Dịch địa chỉ mạng động
EDSG	Enhanced dynamic service gateway	Cổng dịch vụ động nâng cao
FTP	File Transfer Protocol	Giao thức truyền tập tin

GW	Gateway	Cổng ra
iBGP	Internal Border Gateway Protocol	Giao thức cổng biên nội bộ
IP Private	Internet protocol private	Địa chỉ IP nội bộ
IP puclic	Internet protocol public	Địa chỉ IP công cộng
IPAM	Internet protocol Address Management	Quản lý Địa chỉ IP
IPSec	Internet protocol security	Giao thức mật mã bảo vệ lưu lượng dữ liệu qua mạng Internet Protocol (IP)
IPv4	Internet protocol version 4	Giao thức internet phiên bản 4
IPv6	Internet protocol version 6	Giao thức internet phiên bản 6
ISP	Internet Service Provider	Nhà cung cấp dịch vụ internet
L3VPN	Layer 3 virtual private network	Mạng riêng ảo lớp 3
LSN	Large-scale NAT	Dịch địa chỉ mạng quy mô lớn
MAN	Metropolitan area network	mạng lưới khu vực đô thị
NAT	Network address translation	Dịch địa chỉ mạng
NAT Overload	Network address translation overload	Quá tải dịch địa chỉ mạng
NAT sever	Network address translation server	Máy chủ dịch địa chỉ mạng
NAT444	Network address translation 444	Dịch địa chỉ mạng 444
NIX		Internet trong nước
ONU	Optical network unit	Đơn vị mạng quang
OTT	Over the top	Nội dung phim và truyền hình được cung cấp qua đường truyền internet tốc độ cao

P Router	Provider Router	Router nhà cung cấp
PAT	Port Address Translation	Dịch địac hỉ cổng
PBR	Policy base routing	Định tuyến theo chính sách
PE	Provider Egde	Router biên của mạng nhà cung cấp dịch vụ
RADIUS	Remote Authentication Dial-In User Service	Dịch vụ người dùng quay số xác thực từ xa
RFC	Request for Comments	Đề nghị duyệt thảo và bình luận
RIR	Regional Internet registry	Đăng ký Internet khu vực
Router		Thiết bị định tuyến
SCB	Switching control board	Bảng điều khiển chuyển mạch
SIP	Session Initiation Protocol	Giao thức khởi tạo phiên
SSL	Secure Sockets Layer	Lớp socket an toàn
Static NAT	Static network address translation	Dịch địa chỉ tĩnh
TCP	Transmission Control Protocol	Giao thức điều khiển truyền dẫn
UDP	User Datagram Protocol	Giao thức Dữ liệu Người dùng
VNPT	Vietnam Posts and Telecommunications Group	Tập đoàn Bưu chính Viễn thông Việt Nam
Voip	Voice over Internet Protocol	Truyền giọng nói trên giao thức IP
VPN	Virtual Private Network	Mạng riêng ảo
VRF	Virtual routing and forwarding	Định tuyến và chuyển tiếp ảo
WAN	Wide Area Network	Mạng diện rộng

LỜI MỞ ĐẦU

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 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.

Nội dung luận văn đề cập đến các vấn đề kỹ thuật CGNAT, giải pháp triển khai CGNAT trong mạng băng rộng cố định của Tập đoàn Bưu chính Viễn thông Việt Nam - VNPT.

Bố cục của luận văn được trình bày như sau:

- Chương 1 trình bày tổng quan về NAT, khó khăn trong quá trình chuyển đổi IPv4 sang IPv6.
- Chương 2 trình bày kỹ thuật triển khai CGNAT và cấu hình trên một số dòng thiết bị.
- Chương 3 trình bày giải pháp triển khai CGNAT trong mạng VNPT.

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

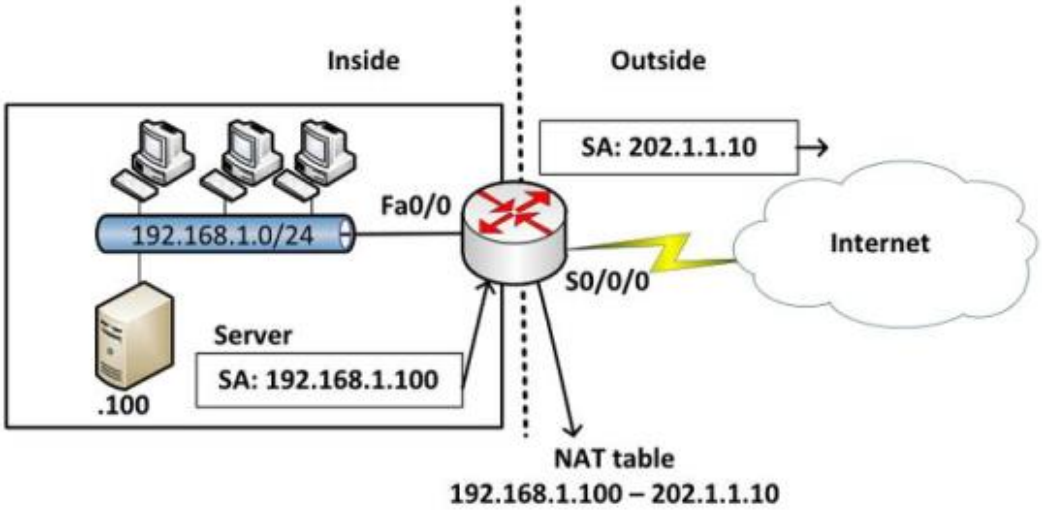
ghi mà nó đã lưu về các gói tin, thay đổi địa chỉ IP đích thành địa chỉ của PC trong mạng và chuyển tiếp đi. Thông qua cơ chế đó quản trị mạng có khả năng lọc các gói tin được gửi đến hay gửi từ một địa chỉ IP và cho phép hay ngăn truy cập đến một port cụ thể [6].

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

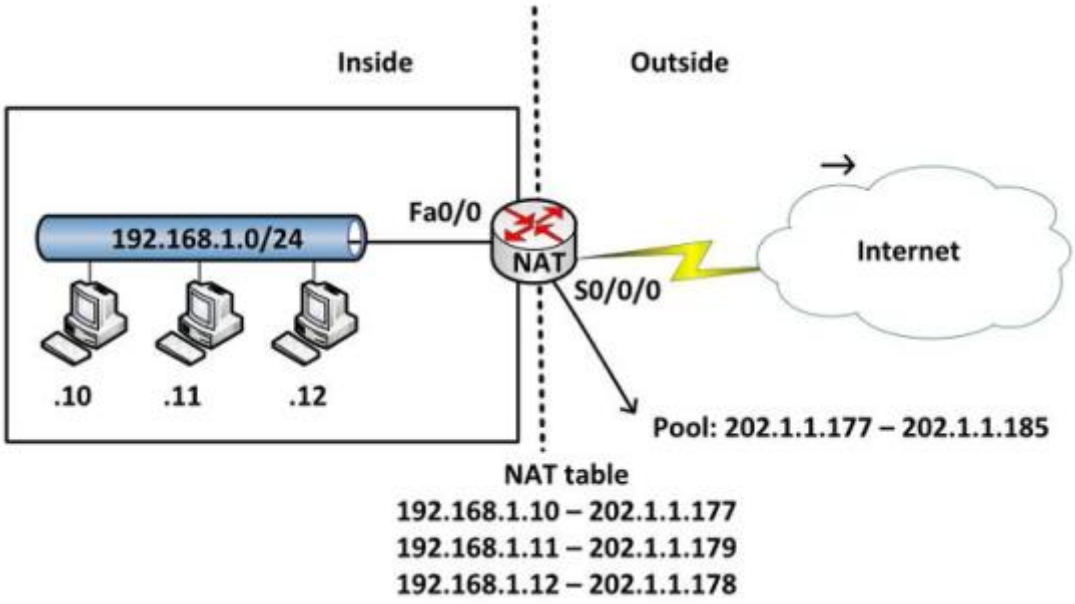
Static NAT (NAT tĩnh) là phương thức NAT một - một. Một IP trong mạng nội bộ, mạng khách hàng sẽ được ánh xạ với một IP công cộng.

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):

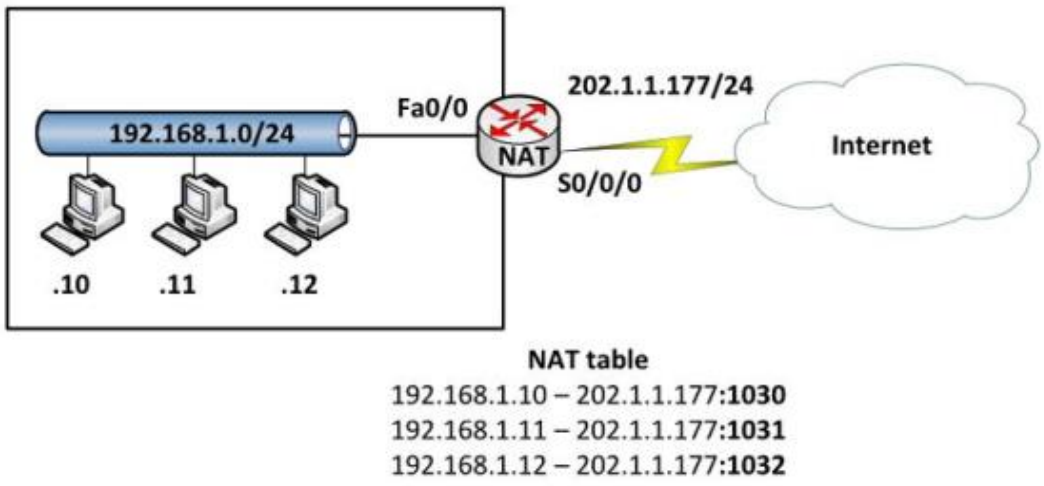
Dynamic NAT được dùng để ánh xạ một địa chỉ IP này sang một địa chỉ khác một cách tự động, thông thường là ánh xạ từ một địa chỉ cục bộ sang một địa chỉ được đăng ký. Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán một thiết bị bên trong mạng.



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

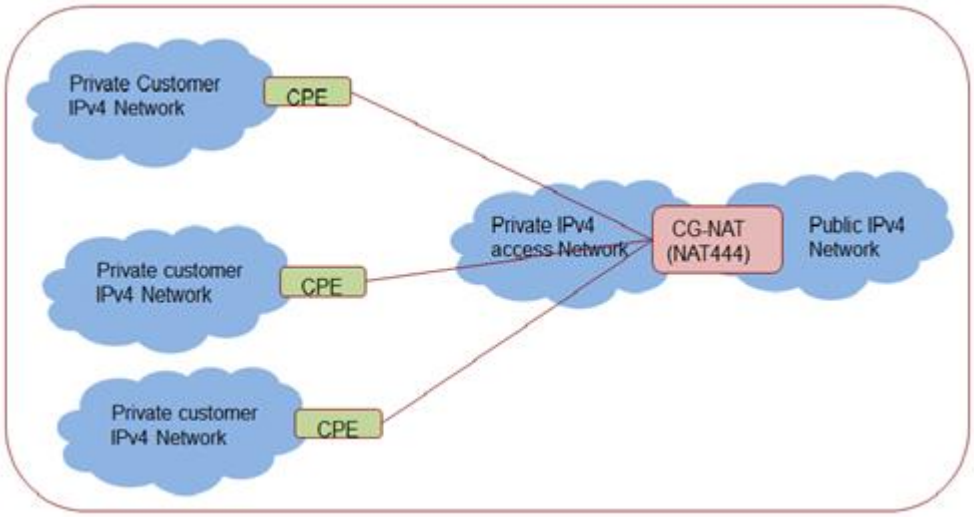
1.1.3 Thực hiện NAT tại nhà cung cấp dịch vụ

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

Sự bùng nổ của Internet trong những năm gần đây đã dẫn đến nguồn tài nguyên địa chỉ Internet IPv4 được tiêu thụ một cách nhanh chóng. Với tổng số khoảng 4 tỷ địa chỉ IPv4, cộng đồng Internet toàn cầu đã cạn kiệt. Việc chuyển sang sử dụng thế hệ địa chỉ mới IPv6 thay thế cho IPv4 đang là một yêu cầu cấp thiết, vừa để nhằm đảm bảo cho sự phát triển liên tục của hoạt động Internet, vừa phát huy các lợi thế vượt trội về công nghệ mới của IPv6 so với IPv4. Thực tế những năm vừa qua, trong khi nhiều nước đã triển khai cung cấp dịch vụ trên IPv6 thì tại Việt Nam, nhận thức của nhiều cơ quan, tổ chức, doanh nghiệp về sự cần thiết phải chuyển đổi sang sử dụng IPv6 vẫn còn hạn chế, việc đăng ký sử dụng IPv6 tại Việt Nam còn tiến triển rất chậm.

IPv6 là giải pháp cho vấn đề địa chỉ IP. Đây không phải là một tiêu chuẩn mới, nhưng là một tiêu chuẩn đã bị bỏ qua phần lớn trong những năm gần đây do vẫn còn quá nhiều địa chỉ IPv4. Việc tiếp tục bỏ qua IPv6 có thể gây ra bất kỳ vấn đề tiềm ẩn nào bao gồm không thể chuyển sang IPv6 khi không còn sự lựa chọn, mất hoàn toàn kết nối với Internet và không còn khả năng cạnh tranh với các tổ chức khác có hệ thống đã sẵn sàng cho IPv6 để chuyển sang thế hệ tiếp theo của địa chỉ và sử dụng Internet.

IPv4 và IPv6 có thể cùng tồn tại trong một mạng và điều này rất tốt vì quá trình chuyển đổi sẽ mất nhiều năm. Các tổ chức sẽ phải hỗ trợ cả hai ít nhất trong thời gian tạm thời để duy trì hoạt động Internet liên tục. Kỹ thuật hỗ trợ cả hai phiên bản IP cùng một lúc được gọi là Dual-stacking. Nó được phát triển do những hạn chế của phiên bản IPv4, IPv4 và v6 không tương thích và không thể nói chuyện với nhau. Vì vậy, hỗ trợ cho cả hai phải được duy trì để sử dụng chúng cùng một lúc trong quá trình chuyển dịch. Dịch chuyển quá nhanh hoặc chỉ hỗ trợ cái này hay cái kia sẽ mất một số kết nối hoặc liên lạc cho đến khi hoàn tất quá trình chuyển đổi

toàn cầu đầy đủ. Để hỗ trợ các tổ chức thực hiện việc chuyển đổi này, các giải pháp Quản lý Địa chỉ IP (IPAM) sẽ được triển khai [7].

Thách thức trong việc chuyển đổi sang IPv6:

Cho đến nay các nhà mạng cung cấp dịch vụ Internet đã được cấu hình để cấp phát IPv6 cho các tổ chức và cá nhân, nhưng trong quá trình chuyển đổi IPv4 sang IPv6 tại các tổ chức và cá nhân vẫn còn gặp rất nhiều vấn đề lớn [11]:

Việc chuyển sang IPv6 sẽ tốn nhiều thời gian và công sức, nhưng có thể dễ dàng hơn nhiều với việc lập kế hoạch hợp lý. Các công cụ như IPAM sẽ trở thành tiêu chuẩn, nhưng nó cũng sẽ phụ thuộc rất nhiều vào kiến thức của của các tổ chức về hệ thống của mình và mức độ lên kế hoạch kỹ lưỡng. Có một số yếu tố cần xem xét khi lập kế hoạch chuyển đổi IPv4 sang IPv6.

Tương thích phần cứng và phần mềm:

Phải đảm bảo rằng thiết bị hiện có trong mạng của tổ chức, gia đình, đặc biệt là thiết bị truyền thông cốt lõi kết nối mạng, phải có khả năng hỗ trợ IPv6. Điều này có thể đơn giản như một bản vá hoặc nâng cấp phần sụn hoặc có thể yêu cầu phần cứng hoặc phần mềm hoàn toàn mới. Nếu nó là quan trọng và cần thiết, cần xác định ngay thay vì tìm hiểu khi nó không hoạt động. Tuy nhiên, tính đến năm 2020, tất cả các hệ điều hành chính đều hỗ trợ IPv6. Các ứng dụng phần mềm được phát triển nội bộ hoặc nguồn thương mại, có thể phải xử lý một yếu tố khác vì IPv6 có thể không được hỗ trợ trong chính ứng dụng đó. Tổ chức và cá nhân có thể cần xem xét việc nâng cấp phần mềm của mình.

Độ dài và Khối lượng địa chỉ IPv6:

IPv6 ở dạng thập lục phân và cực kỳ lớn, có nghĩa là không thân thiện với người dùng. Ngay cả các quản trị viên mạng và những người rất quen thuộc với việc quản lý máy tính và mạng cũng có thể sẽ gặp khó khăn, cuối cùng gây ra lỗi và các vấn

đề liên tục. Độ dài của địa chỉ cũng sẽ gây ra vấn đề cho các dịch vụ DHCP và DNS, có nghĩa là cần có khả năng xử lý việc đặt tên và địa chỉ IPv6 (DHCP6 đã được xác định là ưu tiên).

Giao diện địa chỉ IPv6:

Địa chỉ IPv6 cũng đã thay đổi so với IPv4 và quản trị viên phải hiểu sự thay đổi này trong trường hợp yêu cầu nhiều địa chỉ trên một giao diện, cũng như tự làm quen với từ vựng mới. Có rất nhiều loại địa chỉ mới tương tự như những gì chúng ta biết ngày nay. Ví dụ như địa chỉ unicast toàn cầu chỉ ra một địa chỉ công cộng duy nhất. Địa chỉ IP riêng duy nhất cục bộ là địa chỉ unicast riêng tư duy nhất không có hai địa chỉ trên mạng. Địa chỉ liên kết cục bộ tương tự như địa chỉ IPv4 không thể định tuyến và không rời khỏi mạng. Địa chỉ loopback "::1″ tương đồng với địa chỉ 127.0.0.1, được định nghĩa là chỉ loopback, nhằm mục đích kiểm tra chồng giao thức TCP/IP có hoạt động tốt hay không, nó có cùng chức năng nhưng khác nhau ở cách biểu diễn địa chỉ.

Xếp chồng kép với IPv4 và IPv6:

Dual-stacking có nghĩa là chạy IPv4 và IPv6 trong cùng một mạng. Nó cung cấp cho các thiết bị tương thích IPv6 sự lựa chọn để sử dụng và mặc dù vẫn bị giới hạn ở số lượng địa chỉ IPv4 có sẵn, nhưng lợi ích của việc triển khai IPv6 đã sẵn sàng để chuyển đổi. Đây là môi trường mà các tổ chức có thể sẽ chạy trước khi chuyển hoàn toàn sang IPv6. Có các tùy chọn khác như "6to4" truyền IPv6 qua IPv4 nhưng có cùng giới hạn về số lượng địa chỉ IPv4.

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 đầu tiên, và tính năng IPAM đáng chú ý, là xác định. IPAM trước tiên có thể xác định phạm vi IPv4 hiện có, được sử dụng và khả dụng trên mạng thông qua việc

sử dụng một công cụ tự động. Có thể tiến hành kiểm kê kỹ lưỡng các nút trên mạng (các nút là PC, máy in, bất cứ thứ gì được cắm vào mạng). Điều này sẽ cho phép IPAM xác định IPv6 đã sẵn sàng, được kích hoạt và không tương thích. Thông tin chi tiết sẽ bao gồm những gì cần được nâng cấp hoặc thay thế liên quan đến phần cứng và phần mềm. Giai đoạn cuối cùng của quá trình xác định đề cập đến DHCP và DNS, đảm bảo tương thích với IPv6 và có thể phân giải và phân phối địa chỉ IPv6. Mục tiêu của việc xác định IPAM là biết mạng của tổ chức cá nhân như thế nào và khả năng của nó đối với IPv6 tốt hơn hay tệ hơn để có thể lập kế hoạch ngay bây giờ, không muộn hơn khi thời gian ngừng hoạt động trở nên nhiều hơn. Thách thức với các chức năng xác định mạng IP là yêu cầu quyền truy cập sẵn sàng vào toàn bộ mạng để có hiệu quả. Điều quan trọng là cũng phải đánh giá các tùy chọn có thể mở rộng hơn. Lý tưởng nhất là hệ thống IPAM sẽ tích hợp với hệ thống giám sát mạng hiện có để điền dữ liệu IP và thiết bị. Nếu có thể, hệ thống IPAM nên có tùy chọn tích hợp với RIR và thiết bị định tuyến để hiểu thêm về khối IP nào đang được tính trên mạng.

Bước 2 - Lập kế hoạch triển khai IPv6

Bước tiếp theo là lập kế hoạch sử dụng chính sách và thông tin xác định IPAM mà đang sử dụng trong tổ chức và cá nhân. Xác định những thứ cần mua để nâng cấp hoặc thay thế phần cứng hoặc phần mềm, các lớp đào tạo để hỗ trợ quản trị viên và người dùng, hoặc kế hoạch yêu cầu tổ chức hoàn chỉnh ở cấp độ cao. Xác định những gì phải thay đổi hoặc sửa đổi, và cách tốt nhất để hoàn thành những nhiệm vụ này với thời gian và chi phí thấp nhất.

Bước 3 - Lập mô hình mạng Dual-stacking

Khi quá trình xác định và lập mô hình đã hoàn thành. Tổ chức, cá nhân sẽ xác định IPv6 sẽ có cái nhìn tổng thể khi mạng của mình chuyển dịch sang IPv6, các thiết bị cần chạy Dual-stacking trong giai đoạn chuyển đổi. Điều quan trọng là sử dụng mô hình hóa để xác định những tác động trong việc triển khai địa chỉ IPv6 trên mạng,

có thể cần thay đổi đối với bộ định tuyến, giao diện, chính sách bảo mật, … Các công cụ IPAM sẽ hỗ trợ ánh xạ dữ liệu IP tới các phòng ban, mức độ ưu tiên hoặc cơ sở hạ tầng bằng cách sử dụng bản đồ trực quan và mô hình của cơ sở hạ tầng mới tiềm năng.

Bước 4 - Ánh xạ IPv4 và IPv6 với nhau

Với việc lập mô hình hoàn chỉnh và cách IPv6 sẽ được triển khai vào mạng, chuyển sang việc lập bản đồ, ánh xạ các thiết bị IPv4 tới địa chỉ IPv6 của chúng và ngược lại. Vai trò của IPAM trong bước này là hỗ trợ mạng IPv4 hiện tại và mạng IPv6 chạy đồng thời, Trong giai đoạn triển khai này, các tổ chức cũng có thể thay đổi IP của họ nếu họ muốn, vì các địa chỉ cũng đang được ánh xạ tại thời điểm này. Tuy nhiên, cần cẩn thận. Sự cố có thể xảy ra nếu mọi thứ không được ánh xạ chính xác.

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

Sau khi các giai đoạn lập kế hoạch đã hoàn thành, đã đến lúc thực hiện tính năng dual-stacking. Các thành phần chính ở đây đang sử dụng tất cả thông tin IPAM cho đến thời điểm này và tuân theo kế hoạch để triển khai thành công. Tất nhiên, không ai có thể lập kế hoạch cho mọi thứ, và có thể xảy ra sai sót dù đã lên kế hoạch cẩn thận nhất, hoặc có thể phát sinh những trường hợp không lường trước được. IPAM cũng sẵn sàng hỗ trợ tại đây bằng cách nhanh chóng định cấu hình các phân đoạn địa chỉ IPv6 mới, phân đoạn này sẽ hoạt động tự động do DNS IPv6 là một phần của quá trình triển khai. Nếu không, sẽ cần được thực hiện thủ công. Sau khi thực hiện, điều quan trọng là phải kiểm tra các tính năng mạng để đảm bảo chúng hoạt động bình thường. Các mục như chính sách bảo mật và các hệ thống phụ thuộc IPv4 cụ thể khác có thể cần được sửa đổi để giải quyết mọi vấn đề về kết nối hoặc lỗ hổng bảo mật.

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

Tất cả các dự án và triển khai đều yêu cầu bảo trì và việc chuyển dịch IP này cũng tương tự. Tiếp tục sử dụng IPAM để theo dõi và quản lý địa chỉ IPv6 và mạng sẽ giảm bớt thời gian và nỗ lực cần thiết để quản lý mạng mạng Dual-Stacked và mạng IPv6. Bằng cách sử dụng một số công cụ tương tự được sử dụng trong quá trình triển khai cũng sẽ hữu ích để khắc phục vô số vấn đề từ kết nối chung đến các vấn đề về bảo mật và tuân thủ chính sách. Việc tích hợp các dịch vụ DNS và DHCP với IPAM cũng sẽ cung cấp nhiều thông tin hơn nữa thông qua giải pháp IPAM, nâng cao tầm quan trọng và chức năng của nó đối với tổ chức.

1.3 Kết luận chương 1

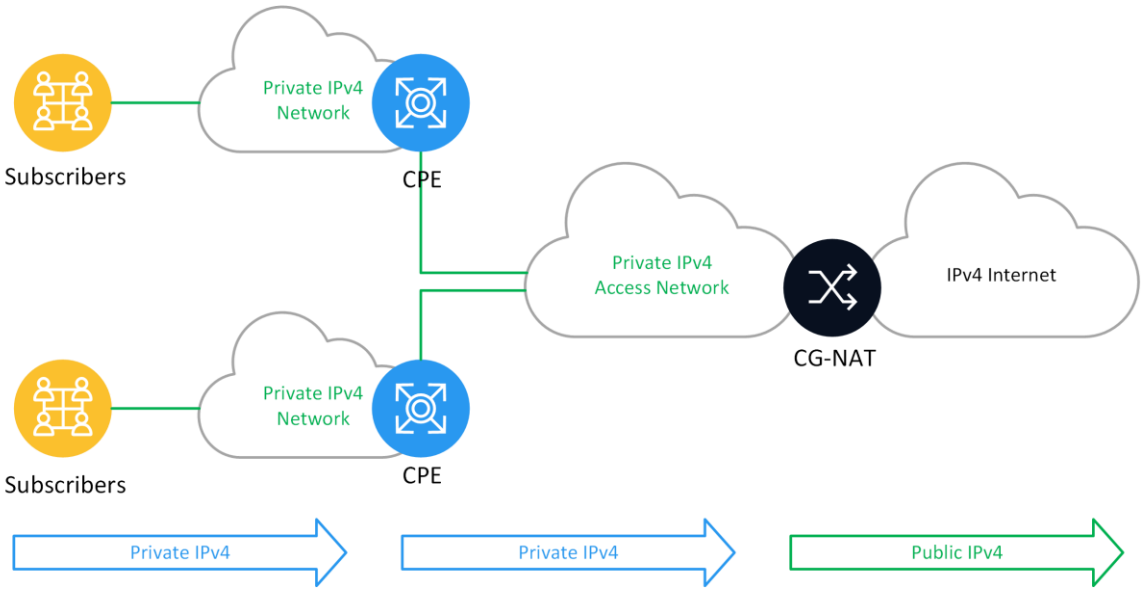
Tính đến năm 2018, tất cả năm RIR đã hết địa chỉ IPv4. Việc chuyển đổi toàn bộ sang địa chỉ IPv6 mang lại rủi ro cho tổ chức trong việc gián đoạn liên lạc và mất doanh thu cũng như khách hàng tiềm năng do các thiết bị mạng trong hạ tầng của tổ chức và doanh nghiệp chưa hòa toàn sẵn sàng triển khai kết 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 gắn 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 cổng, 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 cổng, nhưng "bộ định tuyến chính" của ISP, chạy CGN, sẽ chặn chuyển tiếp cổng 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

Internet được thiết kế với mỗi máy chủ hoặc nút được gán một hoặc nhiều địa chỉ IPv4 duy nhất trên toàn cầu. Vào giữa những năm 1990, rõ ràng không gian địa chỉ IPv4 không đủ cho Internet ngày càng phát triển và nó sẽ cạn kiệt nếu không thực hiện hành động. Kết quả là, các địa chỉ bắt đầu được chia sẻ. Chia sẻ địa chỉ được thực hiện bằng cách sử dụng một kỹ thuật gọi là Dịch địa chỉ mạng (NAT). Ngày nay hình thức NAT này được gọi là NAT44. NAT44 đã trì hoãn việc cạn kiệt không

gian địa chỉ IPv4 trong hơn một thập kỷ, giúp tiết kiệm Internet một cách hiệu quả. NAT44 chỉ trì hoãn việc cạn kiệt không gian địa chỉ IPv4. Sự gia tăng người dùng Internet và các ứng dụng và dịch vụ Internet mới tiếp tục đòi hỏi số lượng địa chỉ IPv4 công cộng ngày càng tăng. Bản thân NAT44 yêu cầu một nhóm địa chỉ IPv4 toàn cầu có thể được chia sẻ. Vì vậy, mặc dù NAT44 làm chậm việc tiêu thụ địa chỉ IPv4, nhưng nó vẫn tiêu thụ địa chỉ IPv4.

NAT cấp độ nhà cung cấp dịch vụ (CGN), còn được gọi là NAT quy mô lớn (LSN) hoặc NAT444, là một kỹ thuật cho phép sử dụng ít địa chỉ IPv4 công cộng hơn để hỗ trợ nhiều khách hàng hơn [12].

CGNAT và IPv6

IPv6 là giải pháp lâu dài duy nhất cho vấn đề cạn kiệt địa chỉ. IPv6 là đang được triển khai rộng rãi. Giờ đây, các trang web và nhà cung cấp dịch vụ lớn như Google, Facebook, Akamai, Netflix đã hỗ trợ IPv6, các ISP ở nước ngoài nhận thấy rằng có tới 33% lưu lượng của người cài đặt Dual-stacking là lưu lượng IPv6.

Sự chậm trễ trong việc triển khai IPv6 có nghĩa là IPv4 vẫn được yêu cầu rộng rãi bởi các dịch vụ và ứng dụng chỉ IPv4. Điều này có nghĩa là IPv4 phải tiếp tục được hỗ trợ trong nhiều năm mặc dù địa chỉ IPv4 đã cạn kiệt. CGN sẽ đóng một vai trò quan trọng trong việc cho phép các ISP cung cấp dịch vụ IPv4 cho khách hàng trong quá trình chuyển đổi sang IPv6.

Các kịch bản triển khai CGN

CGN không thích hợp cho tất cả các trường hợp thiếu địa chỉ IPv4. CGN chủ yếu là một công cụ để ISP triển khai trong mạng truy cập của họ.

CGN thích hợp cho:

- Mạng truy cập - đối với mạng truy cập di động nhiều hơn so với mạng truy cập cố định.
- Truy cập Internet cơ bản - cung cấp quyền truy cập vào mạng cơ bản và được thiết lập tốt.
- Các giao thức Internet - chẳng hạn như thư điện tử và các dịch vụ World Wide Web cơ bản.

Truy cập máy khách - đó là các kết nối được khởi tạo từ mạng phía thuê bao.

CGN không thích hợp cho:

- Mạng của nhà cung cấp dịch vụ - cung cấp kết nối Internet backhaul
- Mạng của nhà cung cấp nội dung - ví dụ: lưu trữ ứng dụng, dịch vụ đám mây và lưu trữ web)
- Khách hàng doanh nghiệp
- ISP cung cấp dịch vụ cho doanh nghiệp

CGN rất khó thích hợp cho:

- Các thuê bao muốn kết nối và kinh doanh trực tiếp trên nền tảng internet
- Những người đăng ký có nhu cầu mạng nâng cao hơn - ví dụ: web-cam, truy cập từ xa và VPN.
- Người đăng ký sử dụng các ứng dụng ngang hàng - bao gồm một số trò chơi nhiều người chơi

Điều quan trọng là CGN không thể áp dụng cho nhiều loại người dùng cuối. Bất kỳ người dùng cuối nào yêu cầu một hoặc nhiều địa chỉ IPv4 công khai đều không được đặt sau CGN. Chúng bao gồm nhiều doanh nghiệp yêu cầu địa chỉ IPv4 công cộng để vận hành các dịch vụ Internet công cộng.

Động lực để triển khai CGN

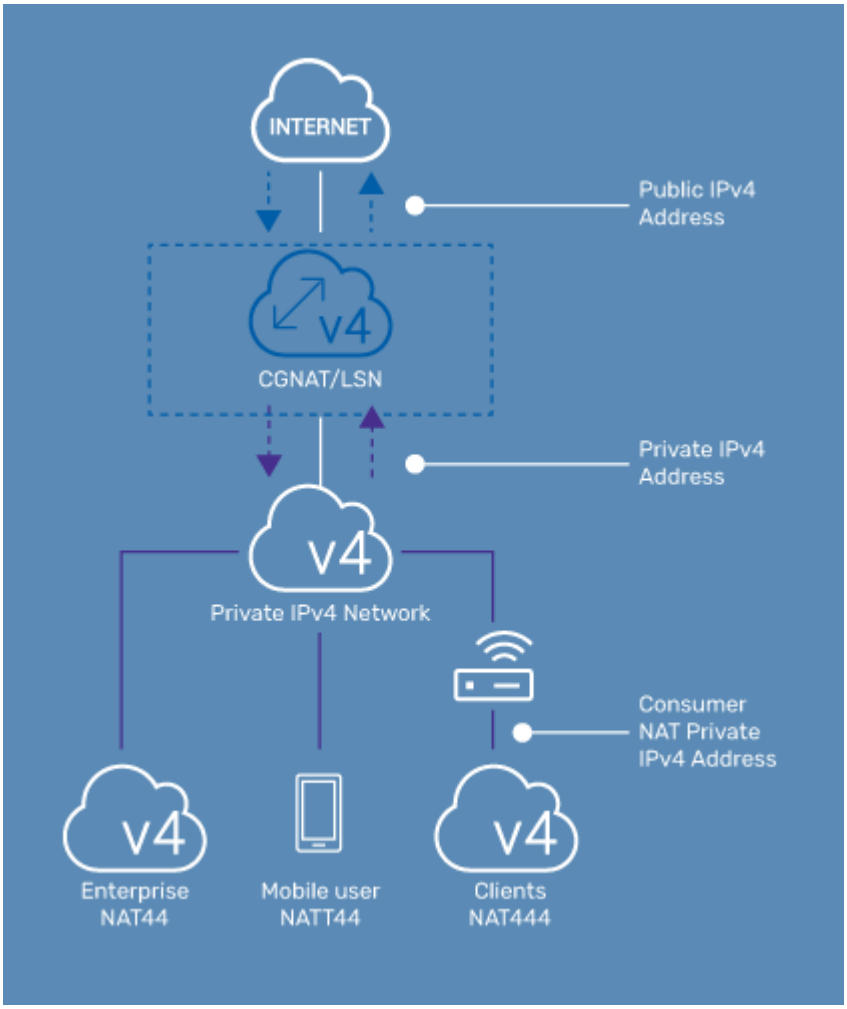
Động lực chính để triển khai CGN là sự khan hiếm địa chỉ IPv4 đang chưa được giải quyết. Các ISP có lý do kinh tế và kỹ thuật để kéo dài nhóm địa chỉ IPv4 của họ. Với việc tài nguyên địa chỉ IPv4 đang trở nên khan hiếm, dịch địa chỉ mạng tại cấp nhà cung cấp dịch vụ cho phép nhà cung cấp dịch vụ triển khai phương pháp để kéo dài thời gian sử dụng của thiết bị chỉ IPv4 và thiết bị mạng yêu cầu IPv4 trong thời gian nhà mạng và các tổ chức cá nhân và doanh nghiệp chưa có đủ thiết bị cung cấp kết nối IPv6.

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

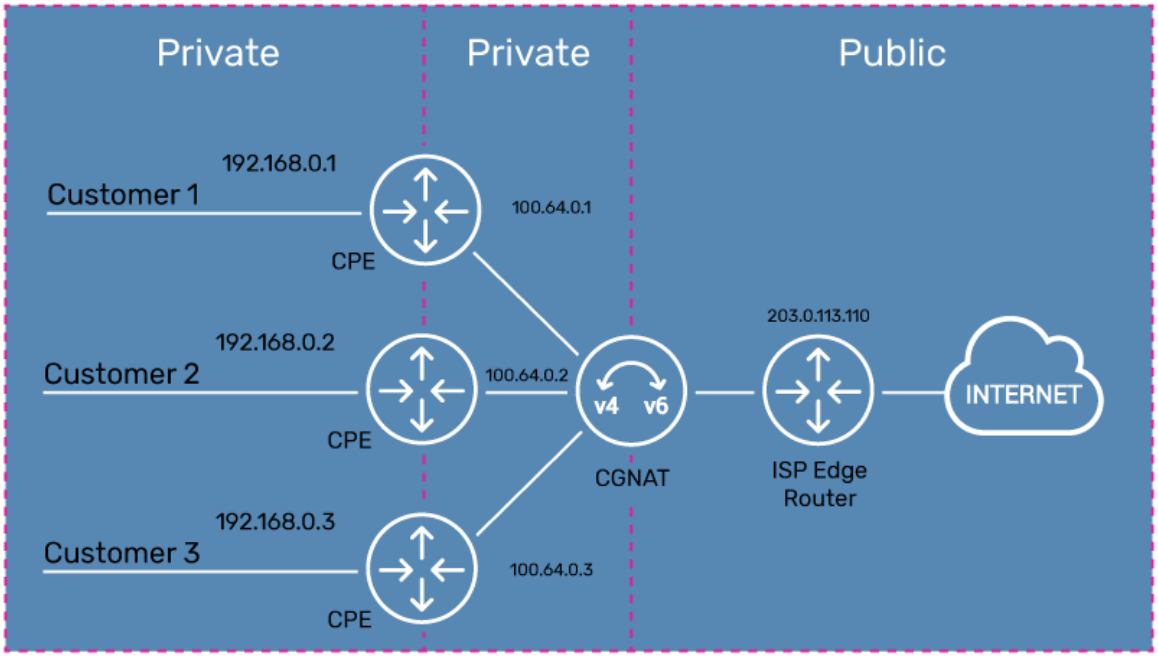
Trong khi NAT tiêu chuẩn dịch địa chỉ IPv4 riêng thành địa chỉ IPv4 công khai, NAT cấp độ nhà cung cấp dịch vụ (CGNAT) thêm một lớp dịch bổ sung. Điều này cho phép ISP duy trì địa chỉ IPv4 công khai của riêng ISP, thông thường, NAT cấp sóng mang (CGNAT) được sử dụng trong kịch bản NAT 444 [4],[5], nghĩa là:

Từ khách hàng (sử dụng IPv4 private) đi đến ISP (sử dụng IPv4 private). Từ địa chỉ IPv4 private của ISP sẽ được dịch sang IPv4 public và đi ra ngoài mạng Internet.

Kết quả của việc triển khai NAT444 (private to private to public) là nó cho phép nhiều khách hàng có không gian địa chỉ mạng nội bộ của riêng họ định tuyến qua không gian địa chỉ mạng nội bộ của ISP và chia sẻ địa chỉ IPv4 Internet công cộng duy nhất của ISP để truy cập vào Internet

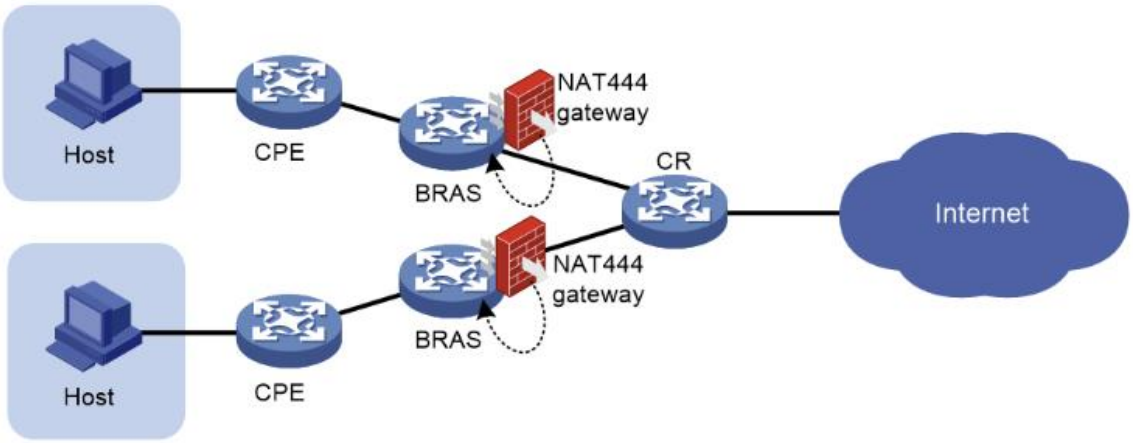
Triển khai NAT444

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

Phân tích mô hình NAT 444 trong hình 2-4

NAT quy mô lớn cho IPv4 sẽ được triển khai xếp chồng kép với IPv6 toàn cầu (“công khai”).

NAT Quy mô lớn thêm một lớp NAT thứ hai và do đó một khu vực thứ hai là "riêng tư". Điều này đã tiết kiệm được IPv4 Public.

NAT444 làm trầm trọng thêm tất cả các vấn đề mà NAT44 truyền thống đã đưa ra. Ngoài việc thêm lớp NAT thứ hai gây ra các vấn đề lớn với việc thực thi Rule và ghi log cũng như vị trí địa lý đã được cấp phát của IPv4 (tất cả là do nhiều khách hàng khác nhau đứng sau một địa chỉ nhà cung cấp). Ngoài ra cần phải đối mặt với thực tế là lớp thứ hai của NAT sẽ không tham gia vào UPnP, NAT-PMP hoặc các giao thức truyền tải NAT dựa trên mạng LAN khác. Không có ISP (Nhà cung cấp dịch vụ Internet) nào sẽ mở bộ định tuyến của riêng họ (hoặc các thiết bị mạng khác) để khách hàng kiểm soát - đó chính xác là những gì các giao thức này yêu cầu. Vì đơn giản là không an toàn và rủi ro một khách hàng có thể ảnh hưởng đến dịch vụ của khách hàng khác là quá lớn. Các ứng dụng sẽ không bị ảnh hưởng bởi NAT 444 và còn hoạt động tốt như sau:

- Web browsing
- Email

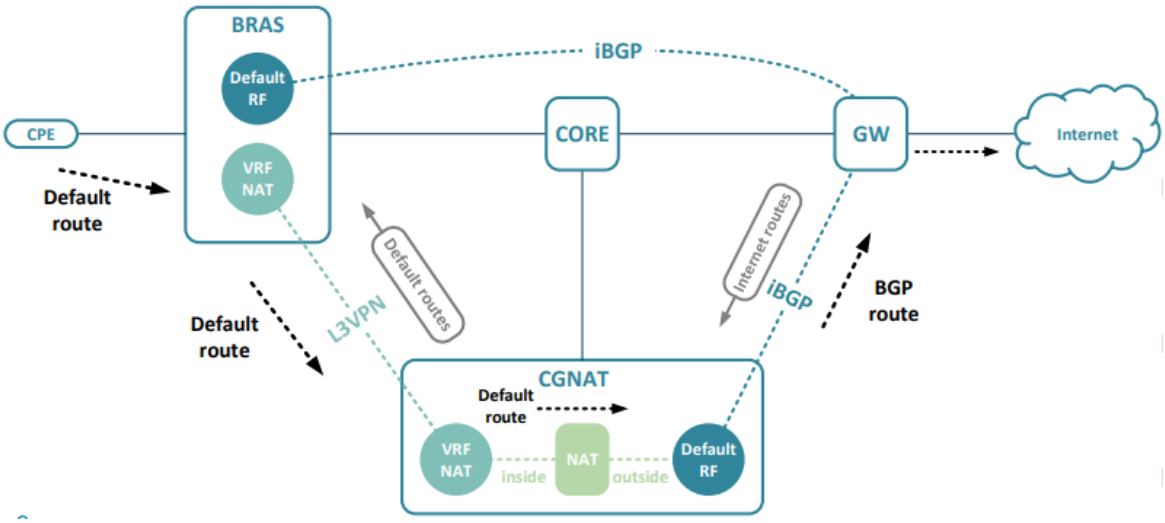
- FTP download
    - Small files
- BitTorrent and Limewire
    - Leeching (download)
- Skype video and voice calls
- Instant messaging
- Facebook and Twitter chat

Một số ứng dụng sẽ có thể ảnh hưởng khi triển khai CGNAT:

- FTP download
    - Large files
- BitTorrent and Limewire
    - Seeding (upload)
- On-line gaming
    - Xbox
    - PlayStation
    - Etc.
- Video streaming
    - Hulu
    - Netflix
    - Slingcatcher
    - Etc.
- Webcam
    - Remote viewing
- Tunneling
    - 6to4
    - Teredo
    - Etc.
- VPN & Encryption
    - IPSec

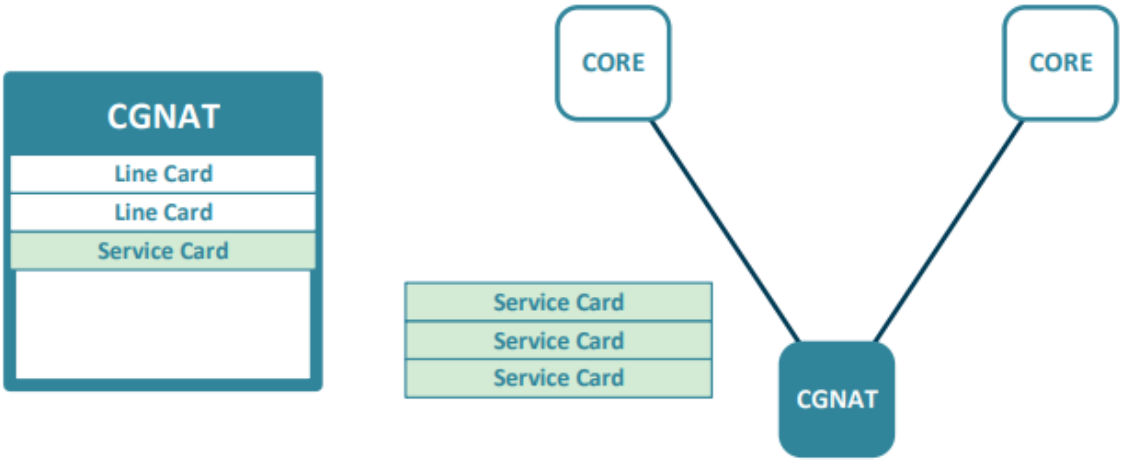
- SSL
- VoIP
  - Limited ALG/SIP support

Để giải quyết những khó khăn và tồn tại trên, giải pháp đúng duy nhất là triển khai IPv6. Đây là lý do tại sao mô hình NAT444 bao gồm IPv6 toàn cầu, các nhà cung cấp dịch vụ sẽ hỗ trợ tối đa khách hàng của mình trong trường hợp bắt buộc phải sử dụng IPv4 nên giải pháp CGNAT vẫn sẽ triển khai tại các ISP, song hành cùng với CGNAT các ISP sẽ triển khai dual-stack, thực hiện kiểm soát và phân loại lưu lượng tại các vùng biên, nếu thiết bị hỗ trợ IPv6 sẽ được đẩy thẳng vào miền IPv6, những thiết bị IPv4 sẽ được chuyển qua CGNAT, do cần đạt được 2 mục đích, vừa hỗ trợ các khách hàng còn chưa thể thay đổi hệ thống mạng sang IPv6, vừa đảm bảo được khả năng thiếu hụt IPv4 nên giải pháp CGNAT vẫn cần được triển khai và tồn tại cho đến khi mạng Internet sử dụng thuần IPv6.



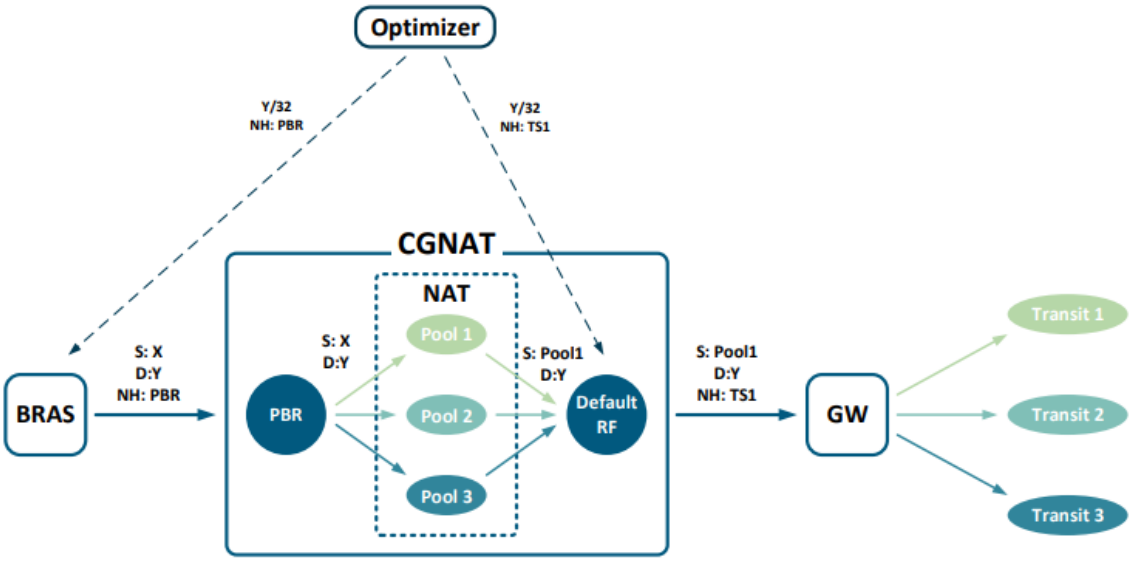
Hình 2-5: Luồng lưu lượng từ khách hàng ra Internet qua CGNAT

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

Triển khai CGNAT cần đảm bảo các chỉ tiêu:

Mạng di động, doanh nghiệp lớn, tổ chức giáo dục đại học và ISP đòi hỏi khả năng NAT cấp độ nhà cung cấp (CGNAT) phức tạp hơn nhiều so với mạng người tiêu dùng và doanh nghiệp nhỏ vì chúng cũng có các yêu cầu quan trọng về hiệu suất, độ tin cậy và khả năng quản lý.

Hiệu suất - Các giải pháp NAT cấp độ nhà cung cấp dịch vụ phải hỗ trợ hàng triệu kết nối mạng đồng thời.

Mở rộng quy mô - Các giải pháp của nhà cung cấp dịch vụ phải có khả năng mở rộng quy mô động, bổ sung thêm thông lượng nếu cần mà không làm gián đoạn lưu lượng mạng hiện có.

Tính sẵn sàng cao - Các giải pháp NAT cấp độ nhà cung cấp dịch vụ yêu cầu tính khả dụng rất cao 24/7, không có gián đoạn dịch vụ cho người dùng. Điều này yêu cầu chuyển đổi dự phòng liền mạch trong trường hợp có bất kỳ lỗi thành phần nào với tính năng bảo toàn phiên.

Quản lý tại trung tâm - Các giải pháp NAT cấp độ nhà cung cấp dịch vụ phải có khả năng tích hợp với các nền tảng quản lý mạng trung tâm chính và cơ sở hạ tầng để ghi nhật ký (Log) phục vụ cho việc giám sát và phân tích sự cố cũng như năng lực mạng lưới.

Advanced Logging - Tất cả các thiết bị kết nối với Internet tạo ra vô số phiên, do đó, việc theo dõi tất cả các phiên sẽ tạo ra một lượng lớn thông báo trong nhật ký. Các giải pháp NAT cấp độ nhà cung cấp dịch vụ phải cung cấp các kỹ thuật nâng cao để giảm khối lượng nhật ký, chẳng hạn như phân chia cổng, ghi nhật ký bằng không và ghi nhật ký gọn nhẹ cũng như lọc để cung cấp thông tin chi tiết có liên quan, có thể hành động.

Bảo mật – Rất quan trọng đối với việc triển khai CGNAT là yêu cầu về bảo mật và phòng thủ chuyên sâu cụ thể chống lại các cuộc tấn công như các cuộc tấn công từ chối dịch vụ phân tán (DDoS) được nhắm mục tiêu vào nhóm CGNAT.

Hạn ngạch người dùng - Khả năng quản trị viên giới hạn số lượng cổng TCP và UDP có thể được sử dụng bởi một thuê bao là rất quan trọng trong môi trường ISP và Nhà cung cấp mạng di động để duy trì sự công bằng trong việc chia sẻ tài nguyên giữa các thuê bao. Nếu không được quản lý, kết nối cho những thuê bao, khách hàng có thể dễ dàng bị xâm phạm bởi những kẻ tấn công bên ngoài.

Các nhà cung cấp dịch vụ cần thực hiện chiến lược dịch địa chỉ mạng bao gồm cả kế hoạch ngắn hạn để giải quyết việc duy trì phân bổ địa chỉ IPv4 hiện có và kế

hoạch dài hạn để chuyển đổi liền mạch sang cơ sở hạ tầng IPv6. Điều này đòi hỏi một giải pháp cung cấp một tập hợp mạnh mẽ các khả năng Dịch địa chỉ mạng cấp nhà cung cấp dịch vụ và giải quyết toàn bộ vòng đời của quá trình chuyển đổi từ IPv4 sang IPv6.

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

Dòng ME60 là một loạt các cổng điều khiển đa dịch vụ - một loại Máy chủ truy cập từ xa băng thông rộng (BRAS) - được Huawei phát triển để phục vụ như một nền tảng cho việc quản lý và truy cập thống nhất của người dùng và phù hợp nhất cho các ngành như phát thanh truyền hình, truyền hình và giáo dục. Dựa trên nền tảng 2T, dòng sản phẩm này định tuyến dung lượng lớn (480G) cộng với dịch vụ NAT dung lượng lớn (160G)

Có thể triển khai NAT với chất lượng tốt với các dịch vụ sau:

Web Authentication:

Trong giải pháp xác thực Web, một địa chỉ được cấp cho người dùng để truy cập trang web cổng thông tin. Sau khi người dùng nhập tên người dùng và mật khẩu đăng nhập, máy chủ RADIUS xác thực máy khách. Nếu xác thực thành công, máy khách yêu cầu một địa chỉ khác để người dùng truy cập vào mạng bên ngoài. Khi

người dùng cần chuyển sang chế độ ngoại tuyến, ứng dụng khách cũng bắt đầu một yêu cầu ngoại tuyến

BoD

Băng thông theo yêu cầu (BoD) là một dịch vụ giá trị gia tăng có tính năng phân bổ băng thông động. Khi người dùng cần điều chỉnh băng thông đã đăng ký, họ có thể tự động kích hoạt hoặc hủy kích hoạt dịch vụ BoD thông qua máy chủ Portal. Theo cách này, các băng thông đã đăng ký được thay đổi động mà không cần sự can thiệp của các nhà khai thác.

DDA

Destination address accounting (DAA) thực hiện tính toán phân biệt, giới hạn tỷ lệ và lập lịch ưu tiên dựa trên địa chỉ đích lưu lượng truy cập.

DAA có thể được sử dụng trong các tình huống sau trong NAT444:

DAA được sử dụng để thay đổi loại dịch vụ và nhóm người dùng cũng được thay đổi tương ứng.

DAA được sử dụng để tăng tốc băng thông, với nhóm người dùng không bị thay đổi. Thay vào đó, băng thông của người dùng được điều chỉnh bằng cách sử dụng mẫu dịch vụ DAA.

Enhanced dynamic service gateway (EDSG)

Cổng dịch vụ động nâng cao (EDSG), một cải tiến cho DAA, xác định độc lập một phần lưu lượng truy cập của người dùng và thực hiện giới hạn tốc độ, tính toán và quản lý độc lập cho lưu lượng truy cập.

Cấu hình CGNAT trên thiết bị Huawei

Bật chức năng chuyển tiếp gói IPv6:

```
<CGN> system-view
[CGN] ipv6
```

Đặt chế độ chọn bảng băm thành chế độ băm dựa trên địa chỉ nguồn:

```
[CGN] firewall hash-mode source-only
```

Định cấu hình địa chỉ IP cho giao diện và thêm giao diện vào vùng bảo mật:

```
[CGN] interface GigabitEthernet 1/0/0
```

[CGN-GigabitEthernet1/0/0] ip address 1.1.1.1 255.255.255.0

[CGN-GigabitEthernet1/0/0] quit

[CGN] firewall zone untrust

[CGN-zone-untrust] add interface GigabitEthernet 1/0/0

[CGN-zone-untrust] quit

Định cấu hình chính sách bảo mật. Định cấu hình chính sách bảo mật chính sách 1 cho phép gửi các gói từ mạng riêng đến mạng công cộng:

[CGN] security-policy

[CGN-policy-security] rule name policy1

[CGN-policy-security-policy1] source-zone trust

[CGN-policy-security-policy1] destination-zone untrust

[CGN-policy-security-policy1] destination-address 1.1.1.0 24

[CGN-policy-security-policy1] destination-address 5000:: 64

[CGN-policy-security-policy1] action permit

[CGN-policy-security-policy1] quit

Cấu hình NAT để dịch địa chỉ IPv4 riêng của nhà cung cấp dịch vụ thành địa chỉ IPv4 công khai:

[CGN] nat address-group addressgroup1

[CGN-address-group-addressgroup1] mode pat

[CGN-address-group-addressgroup1] route enable

[CGN-address-group-addressgroup1] section 1 1.1.2.1 1.1.2.5

[CGN-address-group-addressgroup1] port-block-size 256

[CGN-address-group-addressgroup1] quit

Định cấu chính sách NAT:

[CGN] nat-policy

[CGN-policy-nat] rule name policy_nat_1

[CGN-policy-nat-rule-policy_nat_1] source-zone trust

[CGN-policy-nat-rule-policy_nat_1] destination-zone untrust

[CGN-policy-nat-rule-policy_nat_1] source-address 10.1.1.0 24

[CGN-policy-nat-rule-policy_nat_1] action source-nat address-group addressgroup1

[CGN-policy-nat-rule-policy_nat_1] quit

[CGN-policy-nat] quit

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

Nền tảng định tuyến chung **MX960** 5G là một bộ định tuyến cạnh được tối ưu hóa Ethernet. **Bộ định tuyến MX960** cho phép một loạt các ứng dụng và dịch vụ dành cho doanh nghiệp và dân cư, bao gồm dịch vụ VPN và truyền tải tốc độ cao, dịch vụ nhiều người sử dụng băng thông rộng thế hệ tiếp theo, Internet tốc độ cao, chức năng CGNAT.

Khung **MX960** cung cấp khả năng dự phòng và khả năng phục hồi. Hệ thống phần cứng hoàn toàn dự phòng, bao gồm bộ nguồn, khay quạt, Động cơ định tuyến và Bảng điều khiển công tắc.

Bộ định tuyến MX960). Ba bộ định tuyến có thể được xếp chồng lên nhau trong một giá. Bộ định tuyến cung cấp 14 khe cắm có thể chứa 11 hoặc 12 Bộ tập trung cổng dày đặc (DPC) hoặc Bộ tập trung cổng mô-đun (MPC), sáu Bộ tập trung PIC

linh hoạt (FPC) và hai Bảng điều khiển chuyển mạch (SCB) trong cấu hình không dự phòng.

Bộ định tuyến MX960 cung cấp công suất kết cấu chuyển mạch tổng hợp lên đến 10,56 Tbps, với thông lượng tốc độ đường truyền trên 264 cổng Ethernet 10-Gigabit, 22 cổng 100-Gigabit Ethernet và 44 cổng 10-Gigabit Ethernet và 66 cổng 40-Gigabit Ethernet .

Nền tảng định tuyến đa năng **MX960** hỗ trợ SDN đã được chứng minh trong nhà cung cấp dịch vụ, mạng cáp, di động và trung tâm dữ liệu lớn nhất thế giới. Cung cấp dung lượng hệ thống lên đến 12 Tbps, với sự hỗ trợ cho các giao diện 10GbE, 40GbE, 100GbE và 400GbE mật độ cao.

MultiServices Denser Port Concentrator (MS-DPC) — Gói dịch vụ lớp 3 được sử dụng để cấu hình NAT cho các PIC dịch vụ thích ứng MS-DPC. Cần phải cấu hình gói dịch vụ lớp 3 trước khi thực hiện NAT trên MS-DPC. Giải pháp này cung cấp chức năng NAT cho các dòng MS-DPC, MS-MPC và MS-MIC.

Cấu hình CGNAT trên thiết bị Juniper:

```
juniper@HNI-CGNAT1_RE0> show configuration services | no-more
service-set CGNAT {
   inactive: syslog {
      mode stream;
      source-address 123.29.4.29;
      stream SYSLOG_CGNAT {
         category session-open;
         category session-close;
         host {
            123.29.11.91;
            port 514;
            log-tag HNI-CGNAT-01;
         }
      }
```

```
    }
    service-set-options {
        inactivity-non-tcp-timeout 300;
        session-timeout 86400;
        max-sessions-per-subscriber 2048;
        tcp-session {
            tcp-tickles 3;
            inactivity-tcp-timeout 1800;
            ignore-errors tcp;
        }
    }
    nat-rule-sets CGNAT-RULE;
    next-hop-service {
        inside-service-interface ams0.10;
        outside-service-interface ams0.20;
    }
}
nat {
    source {
        pool TNN-PUBLIC {
            address {
                14.191.28.0/24;
                14.191.29.0/24;
            }
            port {
                automatic {
                    random-allocation;
                }
            }
```

```
        mapping-timeout 120;
    rule-set CGNAT-RULE {
        rule TNN-ALG {
            match {
                source-address-name TNN-PRIVATE;
                application [ junos-sip junos-pptp junos-ftp junos-rtsp junos-traceroute
junos-icmp-all junos-ike junos-dns-udp junos-dns-tcp ];
            }
            then {
                source-nat {
                    pool {
                        TNN-PUBLIC;
                    }
                    mapping-type address-pooling-paired;
                }
            }
        }
        rule TNN-INTERNET {
            match {
                source-address-name TNN-PRIVATE;
            }
            then {
                source-nat {
                    pool {
                        TNN-PUBLIC;
                    }
                    mapping-type address-pooling-paired;
                }
            }
```

```
        }

    }
}
address-book {
    global {
        address TNN-POOL2-PRIVATE 113.188.192.0/19;
        address-set TNN-PRIVATE {
            address TNN-POOL1-PRIVATE;
            address TNN-POOL2-PRIVATE;
        }
    }
}
```

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.

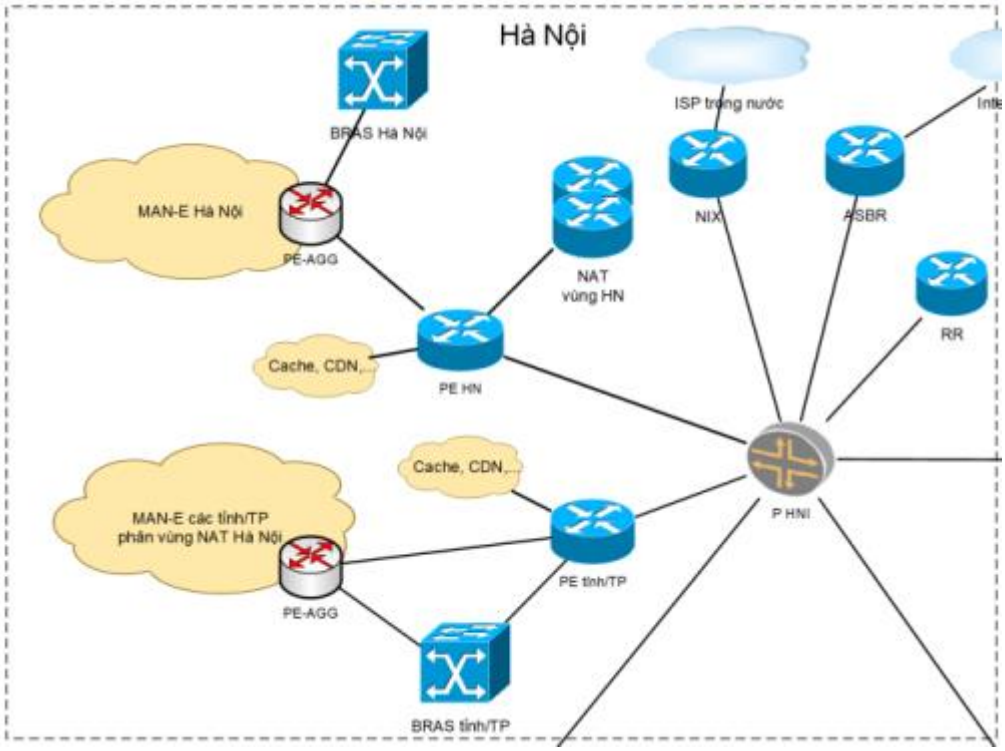
Phương án triển khai

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.

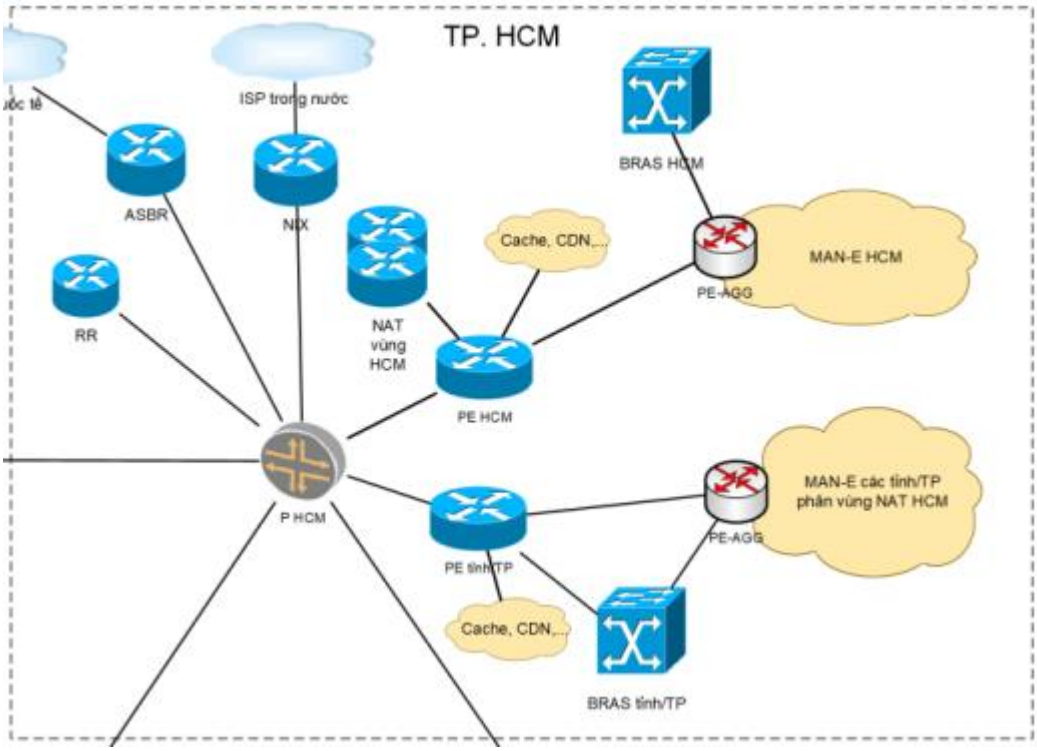
Thiết bị CGNAT trong mỗi vùng phục vụ thuê bao Internet của các tỉnh/Thành phố thuộc vùng đó, không dự phòng giữa các vùng để giảm mức độ phức tạp định tuyến lưulượng, tránh xung đột địa chỉ IP.

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



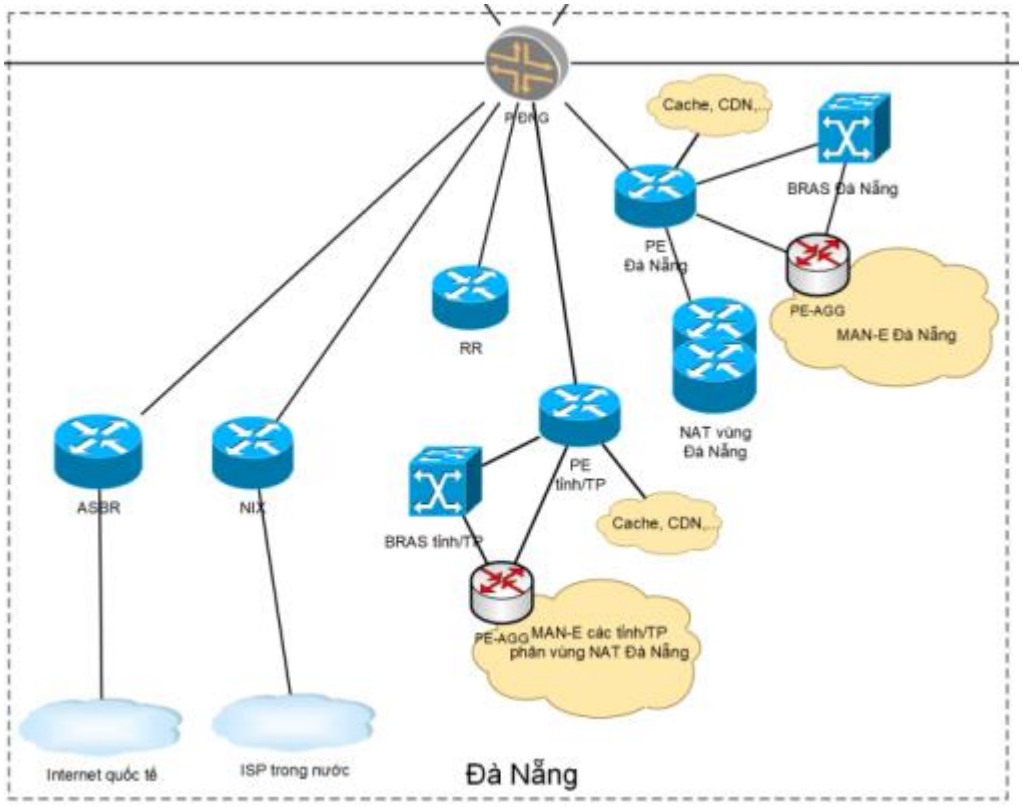
Hình 3-1: Kết nối thiết bị CGNAT tại vùng Hà Nội

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

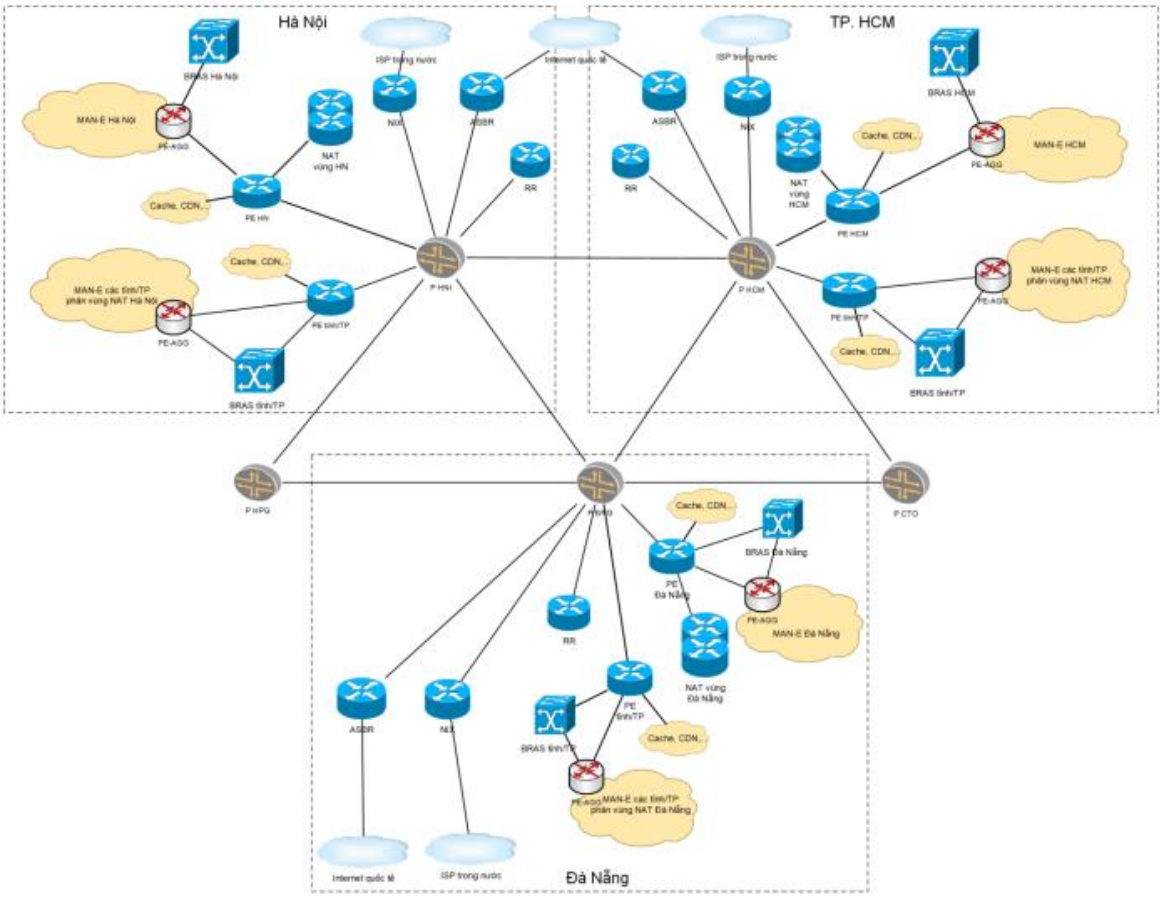
Các thiết bị CGNAT được quy hoạch và gắn trực tiếp vào miền PE tại Hồ Chí Minh, từ thiết bị PE sẽ kết nối vào Router core P Hồ Chí Minh để đi vào mạng Internet.



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

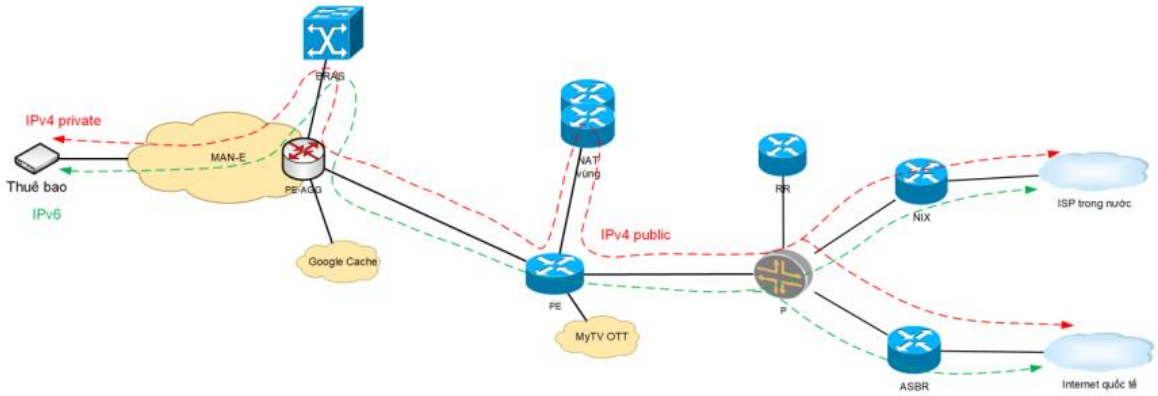
Thuê bao CGNAT được cấp địa chỉ IP theo mô hình dual-stack, nhận đồng thời địa chỉ IPv4 private và địa chỉ IPv6.

Mô hình lưu lượng dịch vụ

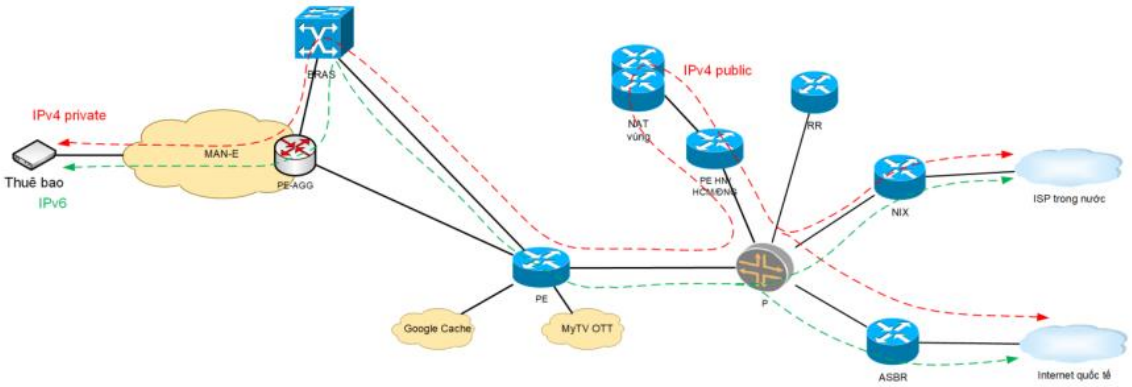
Dịch vụ Internet

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

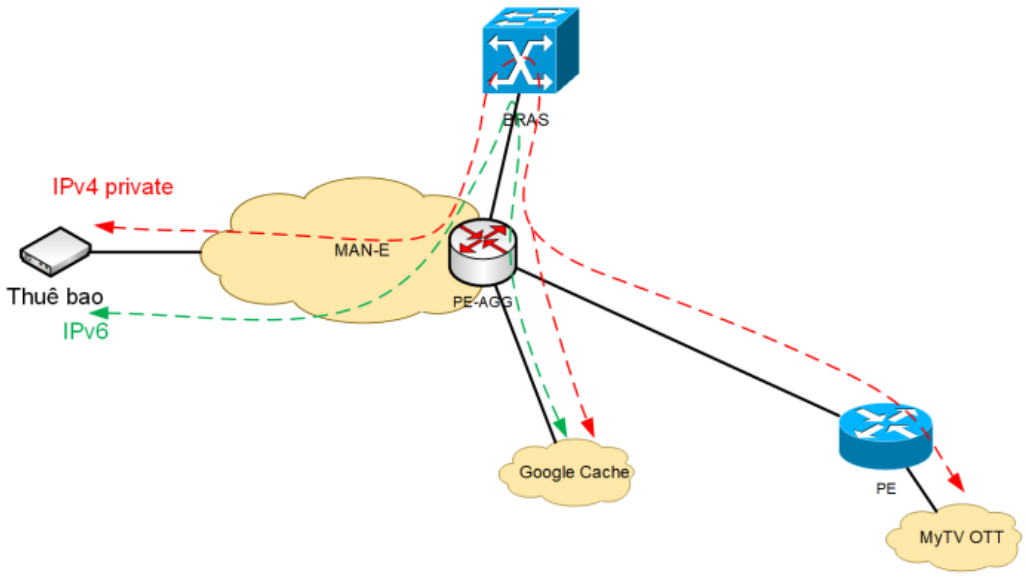
Kết nối với Google Cache, MyTV OTT:

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.

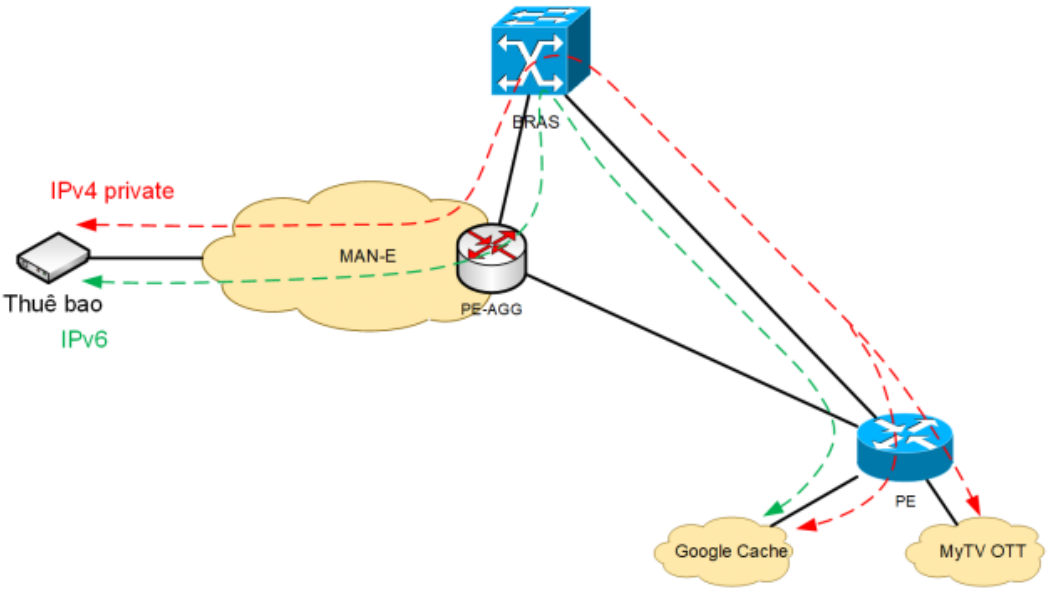
Lưu lượng IPv4 private và IPv6 được truyền tải trực tiếp với các hệ thống Cache. Lưu lượng IPv4 private được truyền tải trực tiếp với hệ thống MyTV OTT.

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 ĐHSXKD,.... 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

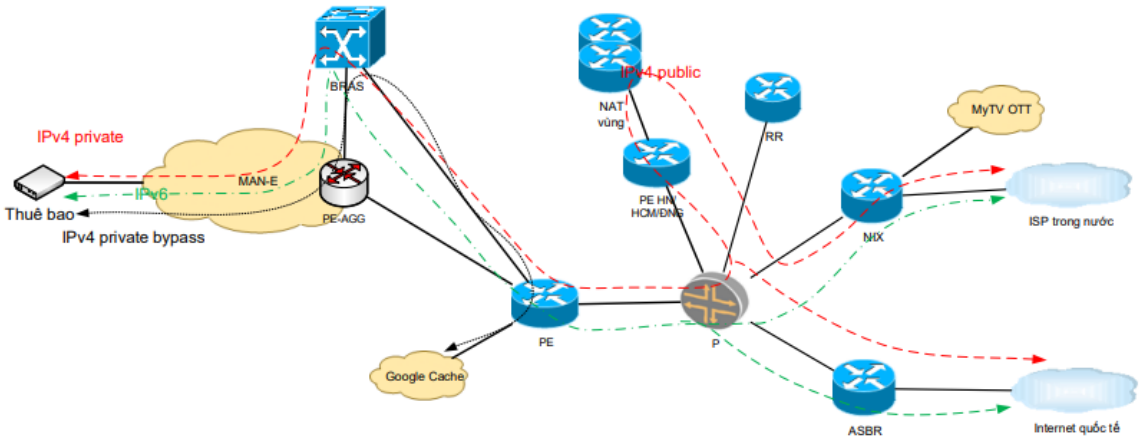
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-ftp
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-rtsp
set services nat source rule-set CGNAT-RULE rule TNN-ALG match application junos-traceroute
set services nat source rule-set CGNAT-RULE 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 lại 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 để 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.

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

Tiếng Anh

[1] An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition (RFC 6264)

[2] Issues with IP Address Sharing (RFC 6269)

[3] Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion (RFC 6333)

[4] IANA-Reserved IPv4 Prefix for Shared Address Space (RFC 6598)

[5] 464XLAT: Combination of Stateful and Stateless Translation (RFC 6877)

[6] Network Protocols Handbook - Javvin Technologies Inc, 1/1/2005

[7] Network address translation Second Edition by Gerardus Blokdyk (Author)

Trang Web

[8] Website: https://en.wikipedia.org/wiki/Carrier-grade_NAT

[9] Website: http://www.cisco.com/

[10] Website: https://www.juniper.net/

[11]. Tabdili. Carrier Grade NAT: Requirements and Challenges in the Real World.
http://www.menog.org/presentations/menog−10/Amir%20Tabdili%20−%20Carrier%20Grade%20NAT.pdf.

[12] A10 Networks. Carrier Grade NAT (CGN)Deployment Guide. https://www.a10networks.com/sites/default/files/resource−files/A10−DG−Carrier_Grade_NAT_%28CGN%29_Large_Scale_NAT_%28LSN%29.pdf.