FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Aron Caio Terense

Estudo sobre a viabilidade de uso de NAT no IPv6

Americana, SP

2015

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Aron Caio Terense

Estudo sobre a viabilidade de uso de NAT no IPv6

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Prof.(º) Esp. Rogério Nunes de Freitas.

Área de concentração: Segurança da Informação.

Americana, SP

2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Terense, Aron Caio
T294e Estudo sobre a viabilidade de uso de NAT no IPv6. / Aron Caio Terense. – Americana: 2015.
61f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Rogério Nunes de Freitas

1. Comunicação de dados 2. Internet – rede de computadores I. Freitas, Rogério Nunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Aron Caio Terense

Estudo sobre a viabilidade de uso de NAT no IPv6

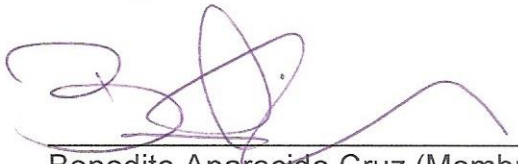
Trabalho de conclusão de curso apresentado à Faculdade de Tecnologia de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

Área de concentração: Segurança da Informação.

Americana, 07 de dezembro de 2015.

Banca Examinadora:

Rogério Nunes de Freitas (Presidente)
Especialista
FATEC Americana



Benedito Aparecido Cruz (Membro)
Graduado
FATEC Americana

Leandro Halle Najm (Membro)
Mestre
FATEC Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus, pois sem Ele nada seria possível. Gostaria de agradecer também a minha esposa e família que me estimularam do começo ao fim de minha vida acadêmica, fazendo com que eu persistisse mesmo quando as dificuldades me eram impostas. Deixo aqui também meu agradecimento a todos os docentes da FATEC Americana, não só por terem realizado seus papéis de educadores, mas também pelo empenho e amizade construída, em especial ao meu excelentíssimo orientador, o Sr. Rogério Nunes de Freitas. Também gostaria de agradecer a todos os amigos que dividi minha experiência acadêmica e que por muitas vezes me auxiliaram em trabalhos excelentes que tive o prazer de participar.

DEDICATÓRIA

A Deus que me capacitou para realizar todas as coisas. A minha esposa, família e amigos que não mediram esforços para que eu chegasse até esta etapa de minha vida.

RESUMO

Este trabalho de conclusão de curso possui como objetivo abordar o surgimento do Protocolo da Internet e estabelecer com referenciais bibliográficos suas características nas versões quatro e seis. Demonstram-se as principais características de cada versão do protocolo e seus funcionamentos, além de explanar também suas principais peculiaridades estruturais. Com base nos fundamentos do Protocolo da Internet em ambas as versões, visa ainda demonstrar as funcionalidades e características do NAT na comunicação entre redes distintas, de forma a explicar sua utilização no Protocolo da Internet em sua versão quatro e analisar a viabilidade de sua utilização com a nova versão seis do protocolo. São apresentados conceitos básicos de redes e roteamento para facilitar o entendimento de todo o tema abordado. Por fim será utilizada uma análise experimental em um ambiente controlado de simulação de redes, a fim de complementar os referenciais teóricos sobre a viabilidade do NAT na versão seis do Protocolo da Internet.

Palavras-chave: NAT, IPv6, Internet.

ABSTRACT

This essay's objective is to approach the appearance of the Internet Protocol and stablish the bibliographic references and characterizations of the versions 4 and 6. It will demonstrate the main features of each version and their working protocols and the explanation of their main structure peculiarities. Based on the besides the explanation demonstration of their functionalities and NAT characteristics on the communication of two distinct networks to explain its use in the Internet Protocol in the version 4 and analyze the viability of its use in the new version 6. There will be presented basic concepts of network and routing to help the understanding of the presented theme. In the end, it will be used an experimental analysis of a controlled environment of network simulation to complement the theoretical references about the viability of NAT 6 for the Internet Protocol.

Keywords: *NAT, IPv6, Internet.*

LISTA DE ILUSTRAÇÕES

Figura 1 - Crescimento da World Web Wide (WWW)....17
Figura 2 - Formato do datagrama IPv4 18
Figura 3 - Endereço IPv4 19
Figura 4 - Classes de Endereçamento 19
Figura 5 - Endereços válidos....20
Figura 6 - Endereço de sub-redes e interfaces 21
Figura 7 - Endereço de sub-redes....21
Figura 8 - Hierarquia na governança da Internet....22
Figura 9 - Interação cliente-servidor DHCP....25
Figura 10 - Cabeçalho protocolo IPv6 29
Figura 11 - Cabeçalhos de extensão....30
Figura 12 - Regras de abreviação de endereço 32
Figura 13 - Estrutura endereço IPv6 33
Figura 14 - Tipos de endereço IPv6 34
Figura 15 - Algoritmo EUI-64....35
Figura 16 - Endereço unique-local 36
Figura 17 - Cabeçalho ICMPv6 38
Figura 18 - NAT - Rede stub 41
Figura 19 - Tipos de endereços NAT 42
Figura 20 - NAT estático 44
Figura 21 - NAT dinâmico 45
Figura 22 - NAPT 47
Figura 23 - NAPT - Próxima porta disponível....48
Figura 24 - Diferença de NAT e NAPT 49
Figura 25 – Cenário 1 – NAT-PT....51
Figura 26 – Cenário 1 – R1 52
Figura 27 – Cenário 1 – R2 52
Figura 28 – Cenário 1 – R3 53
Figura 29 – Cenário 1 – NAT-PT translations....53
Figura 30 – Cenário 1 – Traceroute 54
Figura 31 – Cenário 2 – IPv6....54
Figura 32 – Cenário 2 – Roteador 1 55

Figura 33 – Cenário 2 – Roteador 2 55
Figura 34 – Cenário 2 – Traceroute Roteador 1 56
Figura 35 – Cenário 2 – Tracert PC 56

LISTA DE TABELAS

Tabela 1 - Interação cliente-servidor DHCP 28
Tabela 2 - Encadeamento cabeçalhos de extensão (RFC 2460) 30
Tabela 3 - Endereços multicast IPv6 (RFC 2375) 37

LISTA DE SIGLAS

ACM: Association for Computing Machinery

ARPA: Advanced Research Projects Agency

ARPANET: Advanced Research Projects Agency Network

CIDR: Classless Inter-Domain Routing

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

IANA: Internet Assigned Numbers Authority

ICMPv6: Internet Message Control Protocol for IPv6

IMP: Interface Message Processor

IP: Internet Protocol

ISP: Internet Service Provider

LAN: Local Area Network

MAC Address: Media Access Control Address

NAPT: Network Address Port Translation

NAT: Network Address Translation

NCP: Network Control Protocol

NDP: Neighbor Discovery Protocol

PAT: Port Address Translation

PC: Personal Computer

RFC: Request for Comments

RIR: Regional Internet Registry

SSH: Secure Shell

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

ULA: Unique Local Addressing

VLSM: Variable Lenght Subnet Mask

WWW: World Wide Web

SUMÁRIO

1 INTRODUÇÃO 12
2 IPv4 15
2.1 Início e expansão da Internet 15
2.2 Datagrama IPv4 17
2.3 Endereçamento 18
2.4 Esgotamento dos Endereços 22
2.4.1 CIDR 23
2.4.2 DHCP 24
3 IPv6 27
3.1 Cabeçalho 28
3.1.1 Cabeçalhos de extensão 29
3.2 Endereço 31
3.2.1 Tipos de endereço 33
3.3 ICMPv6. 37
3.3.1 NDP – Descoberta de vizinhança 39
4 NAT 40
4.1 Conceitos 40
4.1.1 Tipos de endereço 41
4.2 Tipos de NAT 43
4.2.1 NAT estático 43
4.2.2 NAT dinâmico 44
4.2.3 Network Address Port Translation (NAPT) 46
4.2.4 Diferenças entre NAT (estático e dinâmico) e NAPT 48
4.3 Coexistência entre IPv4 e IPv6 com NAT-PT 49
5 ANÁLISE EXPERIMENTAL 50
6 CONSIDERAÇÕES FINAIS 57
6.1 Trabalhos Futuros 58
REFERÊNCIAS BIBLIOGRÁFICAS 59

1 INTRODUÇÃO

A Internet se desenvolveu desenfreadamente desde seu início (com a Arpanet) e, a partir de sua criação e crescimento, novas tecnologias foram surgindo e se voltando para consumidores finais, que a utilizam para realizar seus afazeres diários (BRITO, 2014, p. 23).

O crescimento do uso da Internet ocasionou uma grande demanda de utilização do protocolo de comunicação *Internet Protocol* (IP), que em sua versão 4 suportava 4.294.967.296 de endereços válidos na rede. Com essa utilização em massa do protocolo, foram se esgotando os endereços válidos na rede. Uma das soluções encontradas para se manter o protocolo em uso em sua versão 4 foi a *Network Address Translation* (NAT). NAT consiste em uma tradução de vários endereços não válidos de uma rede privada para um endereço válido na Internet. (KUROSE; ROSS, 2010, p. 255).

Com o esgotamento de endereços válidos na Internet se agravando, mesmo com a utilização de NAT, foi criada uma nova versão do IP, a versão 6, que por sua vez suporta 340.282.366.920.938.463.374.607.431.768.211.456 (340 undecilhões) endereços válidos na rede. O principal benefício desta grande quantidade de endereços válidos na rede é o fato de cada *host* poder possuir um endereço válido, não sendo mais necessária a utilização de técnicas como NAT para propiciar a utilização da Internet por *host*s pertencentes a redes locais, ou também conhecidas como *Local Area Network* (LAN) (BRITO, 2014, p. 51).

No IPv6, o número limitado de endereços IP públicos disponíveis não é mais o problema como foi com o IPv4. No IPv4, a tecnologia NAT foi e continua sendo uma solução para resolver esta questão e tem um outro benefício para os usuários em termos de preocupações de segurança: traz privacidade. Usuários que se conectam a Internet através de NAT, ficam um pouco escondidos atrás de seus perímetros pelo fato de seu endereço IP não estar aberto diretamente para a Internet. É por isso que algumas pessoas apoiam o uso de NAT no IPv6 também. Existem outras soluções para sustentar essa vantagem em IPv6. Uma delas é o

Unique Local Addressing (ULA), que é definido na *Request for Comments* (RFC) 4139. O uso de endereços privados, definido na RFC 4941 também podem ajudar os usuários a proteger seus endereços IP. Como resultado, juntamente com outros motivos de ordem técnica, o NAT não é necessário e é até mesmo desestimulado em redes IPv6 (ÇALIşKAN, 2014, p.7).

O **problema** abordado no trabalho é se com a implementação do protocolo IPv6, ainda é viável a utilização de *Network Address Translation* (NAT), sendo que a falta de endereços válidos na Internet não é mais um problema, o que remeteu à seguinte **pergunta**: Até que ponto é necessário a utilização de NAT em uma rede local IPv6 com comunicação a Internet?

Algumas **hipóteses** foram abordadas durante o decorrer do trabalho, dentre as quais:

a) A implementação do IPv6 em uma rede LAN faz com que não seja necessária a utilização de NAT, pois o protocolo em sua nova versão possui endereços válidos o suficiente para dispensar seu uso, além de proporcionar maior velocidade na troca de informações.

b) Tanto o IPv6 quanto o IPv4 possuem a mesma necessidade na utilização de NAT como meio de auxílio a segurança da rede com comunicação com a Internet, mesmo esta não sendo a função da NAT.

c) O fato do IPv6 possuir cada *host* conectado à rede externa por um IP válido pode deixá-lo mais suscetível a ameaças.

O **objetivo geral** deste trabalho foi de identificar possíveis diferenças entre as versões 4 e 6 do protocolo IP no aspecto da necessidade da utilização de NAT em redes locais, devido a no protocolo IPv6 cada host possuir um endereço válido na Internet. Com isso os **objetivos específicos** utilizados para se alcançar o objetivo geral foram:

- Estudar o *Internet Protocol* (IP), conhecendo melhor suas características e propriedades.

- Estudar o NAT, verificando a eficácia de sua utilização na solução proposta para o problema.

- Verificar a viabilidade de se usar NAT em comunicação de redes locais IPv6 com a Internet IPv4.

- Analisar o funcionamento de uma rede local com o protocolo IPv6 se comunicando com outra rede externa IPv6, realizando um experimento para validar sua eficácia na comunicação nativa.

O tema foi **escolhido** devido ao fato de ser um tema atual e de grande potencial exploratório para a área de segurança da informação. A proposta inserida no trabalho foi a de utilizar um procedimento histórico para avaliar a viabilidade de se utilizar de NAT em redes locais IPv6 com comunicação com a Internet, expostas nos referenciais bibliográficos em conjunto com a realização de uma análise experimental e descritiva, utilizando procedimentos técnicos bibliográfico e documental dentro de um ambiente controlado.

No segundo capítulo deste trabalho, é descrito o surgimento da internet até a sua expansão, assim como em paralelo é demonstrado o protocolo IP, suas características estruturais e também os pontos que levaram a escassez de seus endereços válidos na Internet.

O terceiro capítulo aborda a nova versão do protocolo IP e suas características estruturais que permitem com que além de suprir a escassez de endereços válidos, aperfeiçoe falhas da antiga versão do protocolo.

O quarto capítulo expõe o enfoque principal do trabalho que é o NAT, onde são demonstradas suas características e formas de funcionamento.

Por fim o quinto capítulo demonstra uma análise experimental para fundamentar as informações tratadas nos capítulos anteriores de forma prática, seguido das considerações finais dos resultados obtidos ao decorrer da elaboração do trabalho.

2 IPV4

> O protocolo IP foi definido na RFC 791 para prover duas funções básicas: a fragmentação, que permite o envio de pacotes maiores que o limite de tráfego estabelecido num enlace, dividindo-os em partes menores; e o endereçamento, que permite identificar o destino e a origem dos pacotes a partir dos endereços armazenados no cabeçalho do protocolo. Sua versão de protocolo, utilizada desde aquela época até os dias atuais, é a 4, comumente referenciada com o nome do protocolo de IPv4 (A Internet e o TCP/IP,2012).

2.1 Início e expansão da Internet

Segundo (FOROUZAN, 2008), em meados dos anos 60 a *Advanced Research Projects Agency* (ARPA) do Departamento de Defesa (DOD) dos Estados Unidos da América, necessitava interligar computadores de locais físicos distintos a fim de possibilitar a seus pesquisadores o compartilhamento de seus conhecimentos, evitando assim também a duplicação de esforços em seus centros de pesquisas. Então em 1967 em uma reunião da *Association for Computing Machinery* (ACM) a ARPA apresentou a ideia da *Advanced Research Projects Agency Network* (ARPANET). A ARPANET consistia em conectar todos os computadores de grande porte utilizados pelos pesquisadores da ARPA a um computador especializado: o *Interface Message Processor* (IMP). Cada IMP por sua vez deveria ser capaz de se comunicar com os demais IMP's, dessa forma consolidando a comunicação entre todos os hosts.

Ainda segundo FOROUZAN (2008), em 1969 a ARPANET deixou de ser uma ideia para ser colocada em prática. Eram inicialmente quatro nós na rede: um na Universidade da Califórnia em Los Angeles (UCLA); outro na Universidade da Califórnia em Santa Bárbara (UCSB); outro em *Stanford Research Institute* (SRI) e por fim, o último na Universidade de Utah, sendo todos eles conectados da forma que havia sido projetado em 1967 na reunião da ACM, ou seja, através dos IMP's,

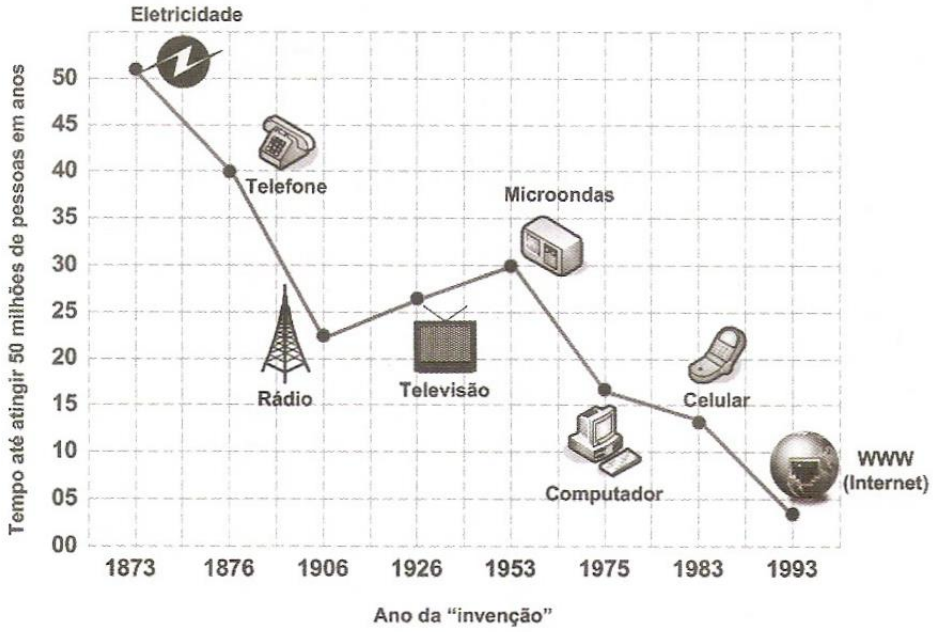
utilizando-se um software para fornecer a comunicação entre os hosts, que ficou conhecido como *Network Control Protocol* (NCP).

Foi em 1972 que Vicent Cerf e Bob Khan, participantes do grupo central da ARPANET, tiveram a ideia de interligar diferentes redes a fim de que os hosts dessas diferentes redes pudessem se comunicar e com isso criaram o que chamaram de *Internetting Project.* “Havia muitos problemas para superar: tamanhos de pacotes diversos, interfaces diferentes e taxas de transmissão distintas, assim como diferentes requisitos de confiabilidade” (FOROUZAN, 2008, p. 2). Um ano após terem a ideia de interligar redes diferentes, Cerf e Khan delinearam em um artigo as soluções para os problemas encontrados, onde entre elas estava uma nova versão do NCP, a utilização do *Transmission Control Protocol* (TCP), os conceitos de datagrama, encapsulamento e as funções de um *gateway*.

Foi então que em 1981 toda a estrutura da Internet que conhecemos atualmente foi fundamentada na RFC 791, ou seja, atualmente utilizamos uma estrutura que foi projetada há 34 anos e que inicialmente não vislumbrava o crescimento exponencial de seus usuários, como acabou ocorrendo. Foram 200 mil hosts distribuídos em 3000 redes em 1990. Em 1992, o milionésimo computador se conectou a rede e apenas um ano depois, aproximadamente 15 milhões de usuários possuíam acesso à Internet. Onde em 2003, atingia 160 milhões (STALLINGS, 2005).

Com seu crescimento de forma acelerada a Internet logo se voltou para sua versão comercial em 1993 e popularizou-se com a criação da *World Wide Web* (WWW). De acordo com (MORAIS, 2012, p 58) “A Web criou uma linguagem de comunicação própria, de apelo visual, com uma mistura intrigante de características de mídia impressa e televisiva. E isso mudou definitivamente a cara da Internet”, fazendo com que em menos de cinco anos após sua criação atingisse 50 milhões de usuários, como se pode observar na Figura 1.

Figura 1 – Crescimento da *World Web Wide* (WWW)



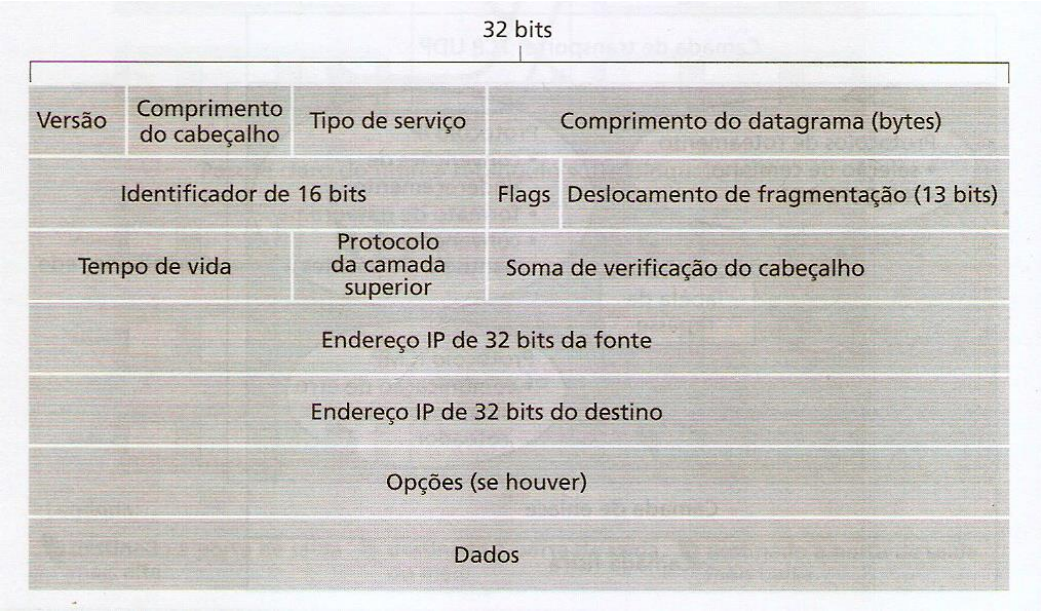
Fonte: BRITO (2014, p. 23)

2.2 Datagrama IPv4

Segundo Marine *et al* (1994, p 32) um datagrama pode ser definido como "uma entidade de dados completa e independente que contém informações suficientes para ser roteada da origem ao destino sem precisar confiar em trocas anteriores entre essa fonte, a máquina de destino e a rede de transporte". Sendo assim a comunicação que se utiliza de datagramas não é uma comunicação confiável, consecutivamente a comunicação do protocolo IP também não, pois não estabelece nenhum tipo de sessão para que a comunicação ocorra.

Essa característica faz com que o protocolo IP faça o que se chama de “melhor esforço”, ou seja, tenta entregar ao máximo a quantidade de pacotes, porém com a possibilidade de perder alguns pacotes durante a comunicação, entregá-los fora da sequência e até mesmo duplicá-los, ficando a cargo de outros protocolos a correção desses problemas, como por exemplo, o protocolo de controle de transmissão TCP.

Figura 2 – Formato do datagrama IPv4



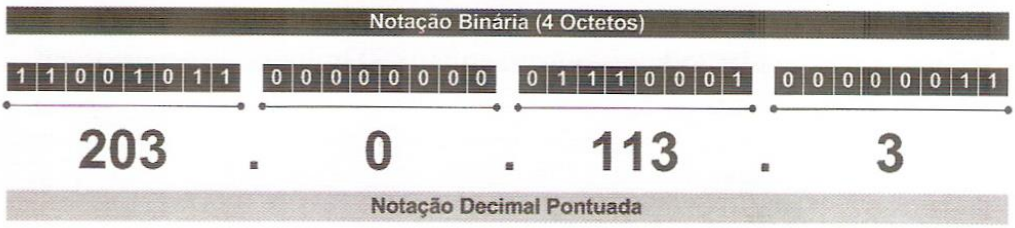
Fonte: KUROSE;ROSS (2010, p. 248)

2.3 Endereçamento

De acordo com Kurose e Ross (2010) antes de se entender o endereçamento do IPv4 é necessário entender como *hosts* e roteadores estão conectados na rede. Quando o IP do *host* quer enviar um datagrama ele utiliza-se de um enlace na rede, onde normalmente o *host* possui somente um, esse enlace por sua vez recebe o nome de interface. No caso do roteador, como se utiliza de vários enlaces para rotear os datagramas de um enlace para outro, possui várias interfaces. Sendo assim o endereço IP é associado a cada interface e não a um determinado *host* ou roteador.

Como visto anteriormente na Figura 2 o endereço IPv4 é composto por 32 bits, onde esses por sua vez são separados por quatro blocos de 8 bits (octetos). Para facilitar o entendimento para as pessoas, optou-se em escrevê-los através de números decimais de 0 a 255, dividindo seus octetos por meio de ponto como podemos ver na Figura 3.

Figura 3 – Endereço IPv4

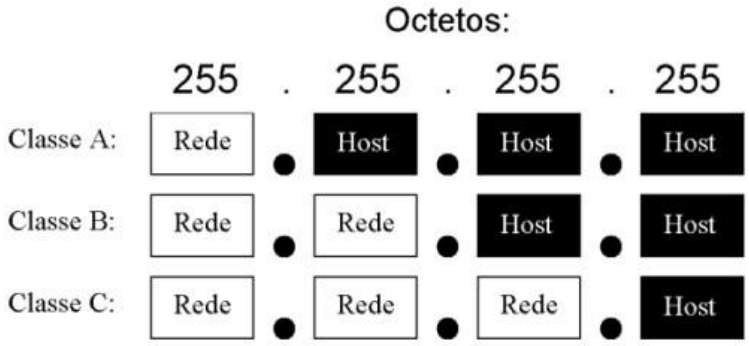


Fonte: BRITO (2014, p. 24)

> Considere o endereço IP 192.32.16.9. O 193 é o número decimal equivalente aos primeiros 8 bits do endereço; o 32 é o decimal equivalente ao segundo conjunto de 8 bits do endereço e assim por diante. Por conseguinte, o endereço 193.32.16.9, em notação binária é: 11000001 00100000 11011000 00001001 (KUROSE; ROSS, 2010, p.252)

Segundo Morimoto (2006) o endereço IP é dividido em duas partes, sendo a primeira (conhecida como prefixo) a que identifica a rede a qual o *host* pertence e a segunda (conhecida como sufixo) a qual identifica o próprio *host* dentro da rede. Sendo assim os endereços IP's foram divididos em 5 classes: A, B, C, D e E. Destas somente as classes A, B e C são utilizadas para endereçamento IP, sendo as classes D e E utilizadas apenas para futuras expansões. Na Figura 4 as classes são representadas de forma a demonstrar como são divididas, onde a classe A utiliza o primeiro octeto para identificar a rede, a classe B utiliza os dois primeiros octetos e a classe C utiliza os três primeiros octetos.

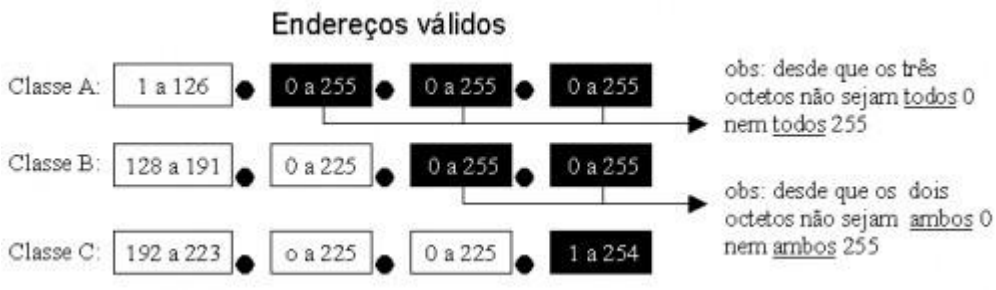
Figura 4 – Classes de Endereçamento



Fonte: MORIMOTO (2006, p. 133)

Sendo assim o que diferencia uma classe da outra é o seu primeiro octeto, onde a classe A possui o primeiro octeto entre 1 e 126, a classe B entre 128 e 191 e a mais comumente utilizada, a classe C, possui o primeiro octeto entre 192 e 223, conforme Figura 5. De acordo com Brito (2014) essa divisão fez com que a classe A comportasse 127 redes e 16 milhões de hosts, a classe B 16 mil redes e 65 mil hosts e a classe C 20 milhões de redes e 254 hosts.

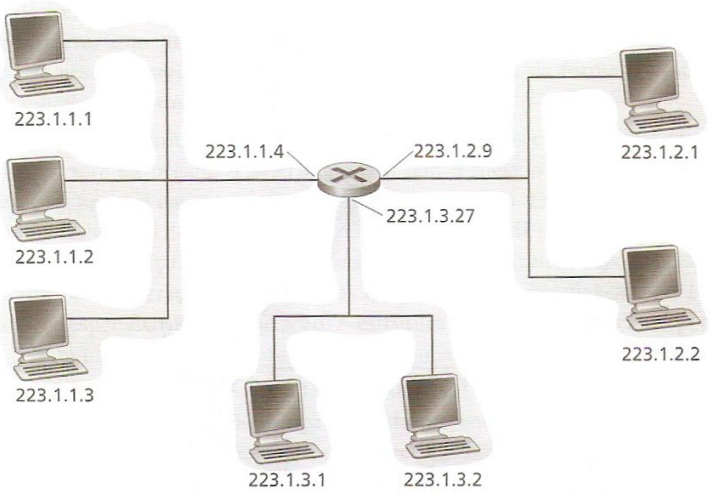
Figura 5 – Endereços válidos



Fonte: MORIMOTO (2006, p. 134)

Cada *host* ou roteador possuindo uma ou mais interface(s), necessariamente possui um endereço IP exclusivo e válido na Internet (com exceção das interfaces que estão por trás de NAT), entretanto esses endereços não são atribuídos aleatoriamente e nesse sentido a sub-rede na qual a interface está conectada, está ligada diretamente ao endereço determinado à interface, como se pode observar na Figura 6.

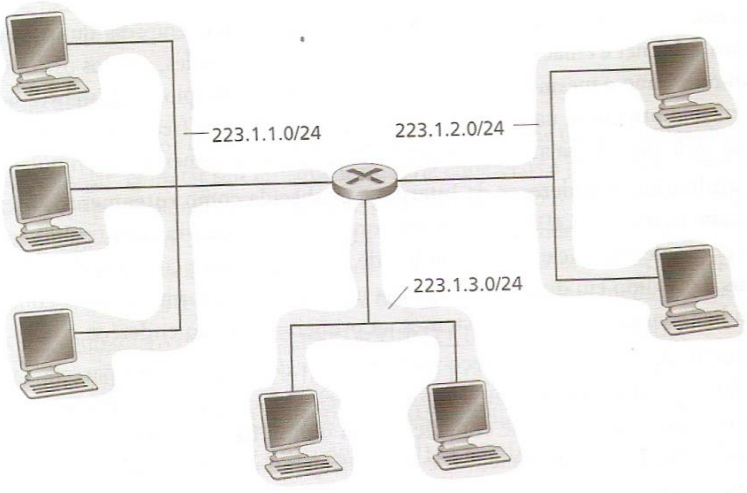
Figura 6 – Endereços de sub-redes e interfaces



Fonte: KUROSE; ROSS (2010, p. 253)

A Figura 6 representa um roteador com três interfaces e diferentes sub-redes cada uma, conectando sete *hosts*, onde os três *hosts* do lado superior esquerdo possuem a sub-rede 223.1.1.0/24 (sendo o “/24” conhecido como máscara de rede, indicando que os primeiros 24 bits do endereço IP da interface indicam a sub-rede à qual pertence), os dois *hosts* localizados na parte inferior possuem a sub-rede 223.1.3.0/24 e os dois *hosts* do lado superior direito possuem a sub-rede 223.1.2.0 /24, conforme Figura 7.

Figura 7 – Endereços de sub-redes



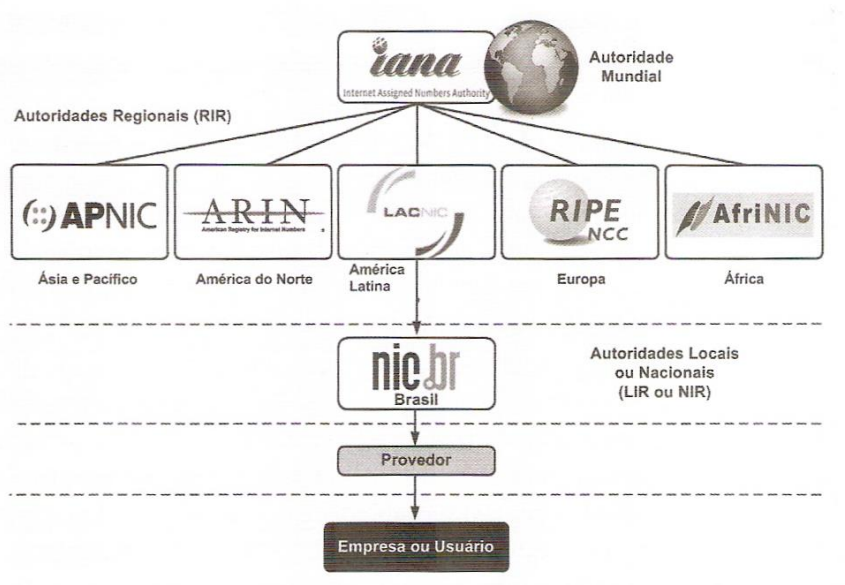
Fonte: KUROSE; ROSS (2010, p. 253)

2.4 Esgotamento dos Endereços

Como visto anteriormente o IP foi concebido inicialmente apenas para interligar algumas instituições como universidades e governos, e que também a mesma arquitetura utilizada naquela época é a utilizada atualmente com o IP em sua versão 4, sendo assim além dos problemas estruturais isso significa que com os 32 bits do datagrama IPv4 era possível obter o equivalente a 4.294.967.296 (aproximadamente 4 bilhões e 300 milhões) de endereços válidos, o que na época em que foi projetado era difícil de se imaginar que seria atingido, porém com a popularização do *Personal Computer* (PC) e da Internet, foi exatamente o que aconteceu.

Inicialmente a *Internet Assigned Numbers Authority* (IANA), que é a autoridade global que gerencia os endereços IP's e nomes de domínio, necessitou ampliar sua estrutura organizacional, para isso criou autoridades de abrangência regionais para manter a governabilidade sobre os recursos da Internet, essas autoridades por sua vez foram denominadas de *Regional Internet Registry* (RIR). A IANA então ficaria como autoridade mundial administrando todos os endereços IP's e nomes de domínio e os dividiria em blocos para cada RIR. Os RIR's por sua vez foram divididos da seguinte forma:

Figura 8 – Hierarquia na governança da Internet



Fonte: BRITO (2014, p. 26)

Ao estruturar sua hierarquia, a IANA começou então a realizar a distribuição dos endereços IP's disponíveis para cada RIR. O problema foi que em 2011, os estoques de endereços válidos que a IANA possuía, já haviam se esgotado, pois todos haviam sidos distribuídos para as RIR's e sendo assim, quando os estoques de endereços IP's válidos se esgotassem nas autoridades locais, logo a Internet não poderia mais crescer (BRITO, 2014).

Brito (2014) ainda afirma que esse esgotamento já era previsto desde o início da década de 1990, ou seja, desde quando a Internet começou a se tornar comercial já se previa o esgotamento dos endereços IP válidos e desde então se vinha criando esforços para criar uma nova versão do protocolo IP, que suportasse um número maior de endereços IP válidos. Porém com a eminente escassez dos endereços válidos, medidas paliativas para o mantimento da Internet com o IPv4 foram tomadas antes de se criar uma nova versão do protocolo IP, dentre as quais, as três mais importantes foram: NAT (que será abordado no capítulo 4), CIDR e DHCP.

2.4.1 CIDR

As classes de endereços foram divididas de forma com que de uma classe para outra o número de *hosts* e redes possuíam uma diferença brusca. Em uma empresa onde existiam 500 hosts seria necessário se utilizar a classe B, porém a mesma possui capacidade para 65 mil hosts, ou seja, seriam 64.500 endereços de *hosts* desperdiçados.

De acordo com Morimoto (2011), a fim de mitigar esse desperdício de endereços foi implementado o *Classless Inter-Domain Routing* (CIDR), através da RFC 1519 em 1993. A maior diferença entre as classes utilizadas anteriormente para o CIDR é que o mesmo não utiliza as mesmas máscaras de rede utilizadas nas classes (/8, /16 e /24) e sim máscaras de tamanhos variáveis, ou mais comumente conhecidas na área técnica como *Variable Lenght Subnet Mask* (VLSM). Isso permitiu com que fosse possível utilizar melhor os endereços disponíveis de forma que em uma rede com 500 *hosts*, ao invés de utilizar a classe B (máscara /16) que possui capacidade de endereçamento para 65 mil *hosts*, se utiliza a máscara /23,

fazendo com que a rede comporte endereços para até 510 *hosts*, desperdício de apenas 10 endereços neste caso (sem levarmos em conta um plano de expansão de endereços na rede em questão, apenas viabilizando estrutura compatível para a quantidade de *hosts* atuais da rede).

Além desta mudança, Morimoto (2011) ainda destaca que não é mais necessário utilizar os primeiros octetos do endereço IP da forma que foram definidos para cada classe, logo então a IANA atribui faixas de endereço para as autoridades regionais, que por sua vez atribuem faixas menores para as instituições (como provedoras) e por fim aos usuários finais.

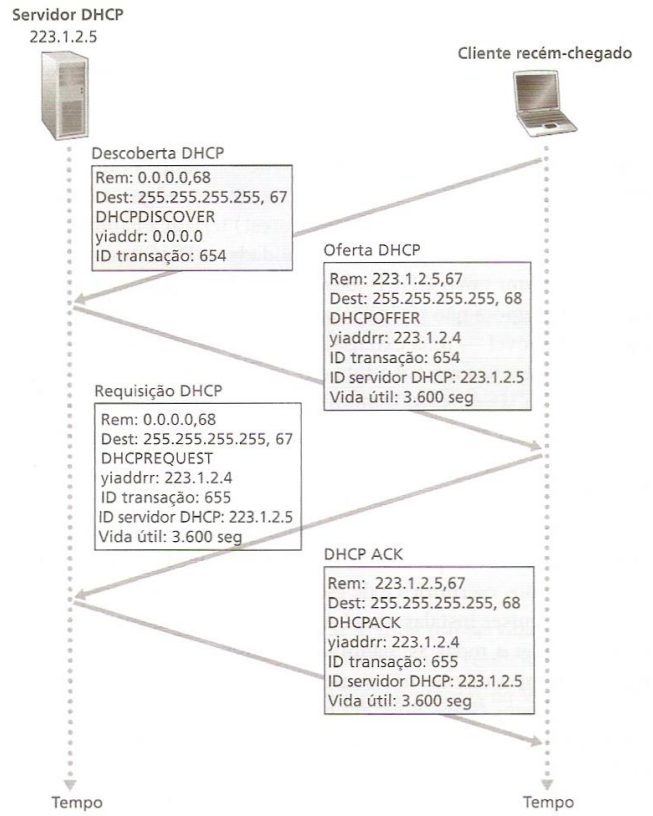
2.4.2 DHCP

De acordo com Forouzan (2008, p.463), “O DHCP (*Dynamic Host Configuration Protocol* – protocolo de configuração dinâmica de host) foi inventado para fornecer alocação de endereço estática e dinâmica, que pode ser manual ou automática”. Ao atuar com a alocação de endereços IP de forma estática é associado no servidor DHCP os endereços aos respectivos *Media Access Control Address* (MAC Address) de cada interface, ou seja, faz um vínculo do endereço IP com o identificador físico de cada interface, não possibilitando que o servidor DHCP distribua esse endereço IP vinculado a nenhuma outra interface.

Atuando com a distribuição de endereços IP de forma dinâmica o DHCP distribui aleatoriamente os endereços de forma com que as interfaces dos *hosts* ou roteadores vão necessitando e, além disso, permite aos *hosts*/roteadores que descubram automaticamente algumas informações, tais como: máscara de sub-rede, endereço do *gateway* da rede, endereço do servidor *Domain Name System* (DNS) (KUROSE; ROSS, 2010).

Ainda segundo Kurose e Ross (2010), o processo para que um *host* recém-conectado a uma rede que possui DHCP adquirir um endereço IP é composto por quatro etapas: Descoberta do servidor DHCP, Oferta(s) dos servidores DHCP, Solicitação DHCP e DHCP ACK, conforme se observa na Figura 9.

Figura 9 – Interação cliente-servidor DHCP



Fonte: KUROSE; ROSS (2010, p. 259)

Sendo assim, temos abaixo o papel que cada uma das etapas realiza na comunicação cliente-servidor DHCP:

- Descoberta do servidor DHCP – Na primeira etapa o recém-chegado *host* envia um pacote *User Datagram Protocol* (UDP) com uma mensagem de descoberta DHCP para a porta padrão 67, porém como não sabe ainda o endereço do servidor DHCP envia com o endereço IP de destino como 255.255.255.255 e com o IP do destinatário como 0.0.0.0, pois dessa forma quando o servidor DHCP receber o pacote solicitando a descoberta de seu endereço, irá responder a todos os *hosts* conectados na rede, que inclui o novo *host* conectado.
- Oferta(s) dos servidores DHCP – Como dito anteriormente, o servidor DHCP responde a todos os *hosts* a solicitação da mensagem de descoberta do servidor DHCP, onde envia para os *hosts* a mensagem de que a solicitação de descoberta foi recebida, o endereço IP proposto para

o *host*, a máscara de rede e o tempo de validade do endereço na rede (o que no caso pode variar de horas a até mesmo dias, dependendo da configuração realizada no servidor).

- Solicitação DHCP – Nesta etapa o *host* decide qual oferta do servidor DHCP irá escolher, no caso a qual endereço IP optou por utilizar, enviando então ao servidor DHCP a mensagem com as configurações escolhidas.
- DHCP ACK – Para finalizar o servidor DHCP envia uma mensagem DHCP ACK confirmando as configurações para o *host*, de endereço IP, máscara, etc.

3 IPV6

> O IPv6 é fundamental, então, para a expansão da Internet, possibilitando a continuidade da adição de novos usuários e o desenvolvimento da Internet das Coisas, interligando os mais diversos tipos de objetos inteligentes. Não é exagero dizer que o IPv6 é fundamental para a própria sobrevivência da Internet nos moldes em que a conhecemos atualmente. (MOREIRAS *et al*, 2015, p. 5).

A partir de junho de 2012, o IPv6 passou a ser considerado o novo padrão de protocolo a ser utilizado na Internet, isso faz com que todos os aparelhos fabricados a partir desta data que possuem conexão com a Internet, já possuam compatibilidade com o novo protocolo (ou deveriam possuir). Isso não quer dizer que o IPv4 ficará obsoleto em curto prazo, até porque seu uso em grande escala que acontece hoje em dia não permite que isso seja possível, fazendo assim com que o processo de transição leve alguns anos. Porém deve-se entender que essa transição não é somente necessária para que se tenham mais endereços válidos na Internet, assim como Brito (2014, p. 38) destaca, existem várias vantagens da adoção do novo protocolo, sendo elas:

- espaço quase “ilimitado” de endereços;
- cabeçalho simplificado e de tamanho fixo;
- processamento simplificado nos roteadores;
- recomendações internacionais de agregação de prefixos;
- dispensa adoção de NAT, preservando o modelo fim-a-fim;
- segurança embutida com o IPSec;
- suporte à mobilidade com o MIPv6.

3.1 Cabeçalho

O cabeçalho do IPv6 foi otimizado para apenas 8 campos, para que isso se tornasse possível foram retirados do cabeçalho IPv4 alguns campos desnecessários, sendo eles: IHL (comprimento do cabeçalho), identificação, flags, deslocamento de fragmentação, soma de verificação do cabeçalho e opções. Além da remoção destes campos, alguns campos foram renomeados para a utilização do cabeçalho no IPv6, conforme observa-se na Tabela 1.

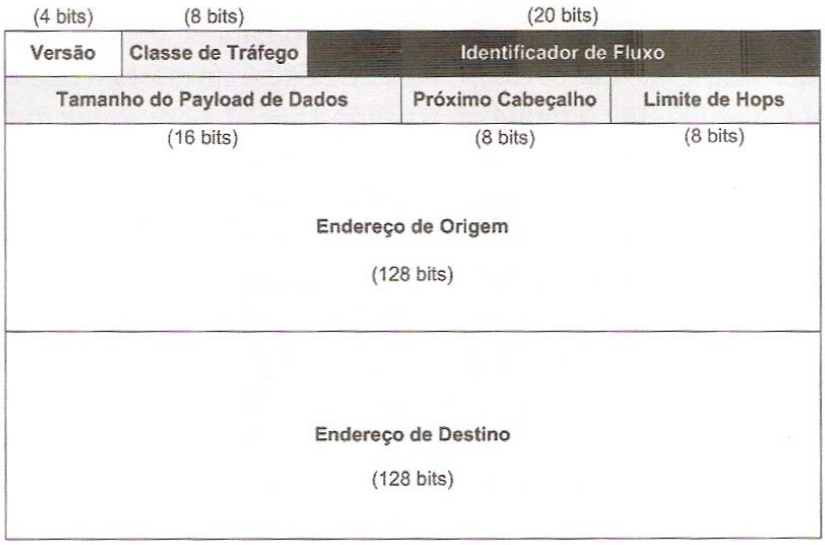
Tabela 1 – Interação cliente-servidor DHCP

IPv4 (Nome do campo)	IPv6 (Nome do campo)
Tipo de Serviço (ToS)	Classe de tráfego (TC)
Tamanho total	Tamanho do *payload* de dados
Protocolo	Próximo cabeçalho
Tempo de vida (TTL)	Limite de hops

Fonte: BRITO (2014, p. 43)

De acordo com Brito (2014) das alterações de nome dos campos de cabeçalhos da Tabela 1, destaca-se a renomeação do Tempo de vida (TTL) para Limite de hops, pois o TTL é medido pela quantidade de saltos (hops) que faz até chegar ao seu destino e não por algum mecanismo de tempo como era nomeado no protocolo IPv4. Com as readequações provenientes do cabeçalho do protocolo IPv4, pode-se observar na Figura 10 que o cabeçalho do protocolo IPv6 foi desenvolvido com um tamanho fixo de 40 bytes , o que é algo impactante no desempenho da rede, já que os roteadores não mais terão que analisar o campo IHL (comprimento do cabeçalho) para determinar o tamanho do cabeçalho antes de analisar as demais informações, simplificando o processo.

Figura 10 – Cabeçalho protocolo IPv6



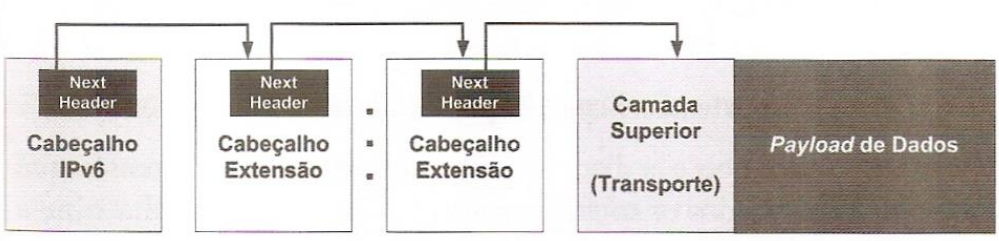
Fonte: BRITO (2014, p. 42)

3.1.1 Cabeçalhos de extensão

Conforme visto anteriormente, o cabeçalho IPv6 foi simplificado em 40 bytes, isso foi permitido graças a não existência do campo de opções do protocolo IPv4, pois todas as funcionalidades anteriormente utilizadas no campo de opções foram readequadas para novos cabeçalhos adicionais, denominados de cabeçalhos de extensão. Os cabeçalhos de extensão não são verificados pelos intermediadores (roteadores) da comunicação entre dois *hosts*, sendo assim a comunicação ganha em desempenho, pois não é necessário o processamento dos roteadores na comunicação, somente dos *hosts* (BRITO, 2014).

Dessa forma os cabeçalhos de extensão são interligados ao cabeçalho IPv6 de maneira encadeada através dos seus códigos de próximo cabeçalho, fazendo com que dessa forma diferentes funcionalidades sejam implementadas e não tirando a simplicidade do cabeçalho IPv6 conforme Figura 11.

Figura 11 – Cabeçalhos de extensão



Fonte: BRITO (2014, p. 45)

Esse encadeamento de cabeçalhos de extensão possui uma sequência a ser seguida de acordo com o código no campo próximo cabeçalho, conforme estabelece a RFC 2460 (Tabela 2). Porém de todos os cabeçalhos de extensão o único que é processado por todos os dispositivos da comunicação, inclusive os roteadores, é o *hop-by-hop*, por conta disso é necessário que seja o primeiro cabeçalho de extensão a ser interpretado, pois uma vez que possui o seu valor diferente de 0, significa que não existe mais nenhum outro cabeçalho de extensão a ser interpretado.

Tabela 2 – Encadeamento cabeçalhos de extensão (RFC 2460)

Ordem	Nome do cabeçalho	Código no campo "Next Header"
01	Cabeçalho IPv6 convencional	-
02	*Hop-by-Hop*	0
03	*Destination Options*	60
04	*Routing Header*	43
05	*Fragment Header*	44
06	*Authentication Header (AH)*	51
07	*Encapsulation Security Payload (ESP)*	50
08	*Destination Options*	60
09	*Mobility*	135
-	Ausência de próximo cabeçalho	59
Camada superior	ICMPv6	58
Camada superior	UDP	17
Camada superior	TCP	6

Fonte: BRITO (2014, p. 45)

3.2 Endereço

A mais drástica mudança do IPv6 em relação ao seu antecessor é sem dúvida o fato do aumento do campo de endereço de 32 bits para 128 bits, aumentando assim de forma exponencial a quantidade de endereços válidos na Internet. Esse aumento de bits para o campo de endereçamento fez com que a notação do endereço IPv6 fosse totalmente diferente do IPv4, ficando dessa forma dividido em oito blocos de 16 bits cada e não sendo mais representados como decimais e sim através de números hexadecimais de quatro dígitos sendo separados por dois pontos (SANTOS, 2004).

Um exemplo de notação de endereço IPv6 que podemos ter é o seguinte: 2001:0000:0000:cafe:0000:0000:0000:ca5a. Apesar de ser um endereço extenso, se optou por utilizar a notação hexadecimal por ser a forma mais simples de se representar um endereço IPv6, pois utilizando a notação binária e decimal o endereço seria mais difícil de se representar. A fim de facilitar o entendimento das pessoas, foram criadas duas regras para realizar abreviação de endereços IPv6 (BRITO, 2014).

A primeira regra consiste em omitir todos os zeros à esquerda de um octeto do endereço, fazendo com que 000b1 e b1 tenham o mesmo significado. Essa regra também pode ser aplicada a um quarteto que possuía somente zeros, sendo então abreviados para somente um zero. Essa regra é possível de ser aplicada graças ao fato de cada octeto possuir quatro algarismos hexadecimais, sendo assim a reversão do endereço abreviado para o original torna-se simples, pois quando o octeto possui somente 1, 2 ou 3 algarismos hexadecimais, automaticamente são preenchidos com zeros a esquerda.

A segunda regra permite que uma sequência de octetos que contenham somente zeros sejam abreviados em “::”, porém deve-se ressaltar de que essa regra pode ser aplicada somente uma vez no endereço. O ponto da segunda regra de aplica-la somente uma vez no endereço é por conta de que o sistema para inversão do endereço interpretar a quantidade de octetos que faltam para se formar o endereço e através da abreviação “::” posicionar os zeros nos octetos restantes.

Para melhor entendimento, exemplifica-se um endereço abreviado incorretamente da seguinte forma: 2001::café::ca5a. Neste endereço possui-se três octetos informados, logo para se obter os oito octetos padrão do endereço IPv6 deve-se preencher as abreviações com mais cinco octetos zerados. Porém como está informado em dois locais as abreviações, a inversão do endereço pode tomar duas formas finais para distribuir três octetos em uma posição e dois octetos em outra posição:

- 2001:0000:0000:0000:cafe:0000:0000:ca5a
- 2001:0000:0000:cafe:0000:0000:0000:ca5a

Sendo assim justifica-se o uso dessa segunda regra somente uma vez por endereço, podendo-se abreviar corretamente o endereço 2001:0000:0000:cafe:0000:0000:0000:ca5s no caso descrito como 2001:0000:0000:cafe::ca5a (2001:0:0:cafe::ca5a), onde em casos que se possui mais de uma sequência de zeros no endereço, é também recomendado aplicar a segunda regra sempre na maior sequência de zeros.

Figura 12 – Regras de abreviação de endereço

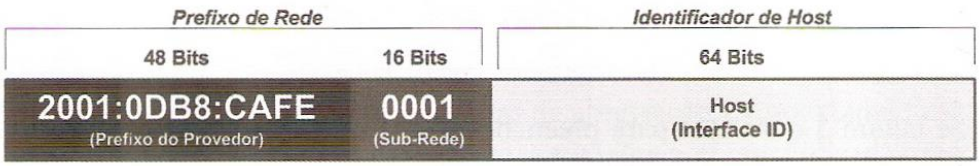
Fonte: BRITO (2014, p. 54)

Em relação a estrutura do endereço IPv6, optou-se por manter a utilização de prefixos e sufixos conforme era utilizado no IPv4, porém como não existe mais a necessidade de preocupação com a quantidade de endereços disponíveis para os *hosts* em cada sub-rede a fim de economia de endereços, desta forma não se faz mais necessário a utilização de máscara de rede, tornando-se obrigatória a

utilização da notação CIDR, já que se faz muito mais trabalhosa a escrita em endereços de 128 bits por conta de seu tamanho.

Em 2006 a RFC 4291 fundamentou que toda rede local deveria obrigatoriamente possuir o sufixo de seus endereços como /64, independentemente da quantidade de *hosts* que possui, assim como se observa na Figura 13.

Figura 13 – Estrutura endereço IPv6



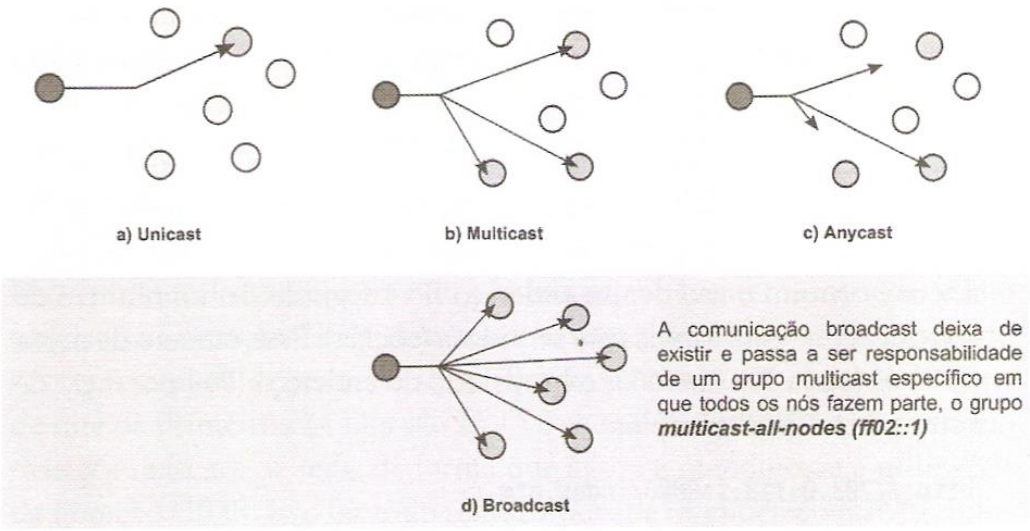
Fonte: BRITO (2014, p. 56)

3.2.1 Tipos de endereço

O IPv6 possui em sua arquitetura três tipos diferentes de endereços segundo SANTOS (2004), sendo eles:

- *Unicast*: identificador de uma única interface, sendo assim um pacote enviado à um endereço de *unicast* é entregue somente para a interface identificada pelo endereço.
- *Multicast*: identificador de um conjunto de interfaces (pertencentes a nós diferentes), desta forma um pacote enviado à um endereço de *multicast* é entregue a todas as interfaces identificadas por esse endereço (não existindo mais o endereço de *broadcast* como no IPv4).
- *Anycast*: assim como o *multicast* é um identificador de um conjunto de interfaces (pertencentes a nós diferentes). O pacote enviado para uma das interfaces identificadas pelo endereço *anycast* (a mais próxima em relação a saltos que o pacote deverá fazer).

Figura 14 – Tipos de endereço IPv6



Fonte: BRITO (2014, p. 58)

3.2.1.1 Unicast

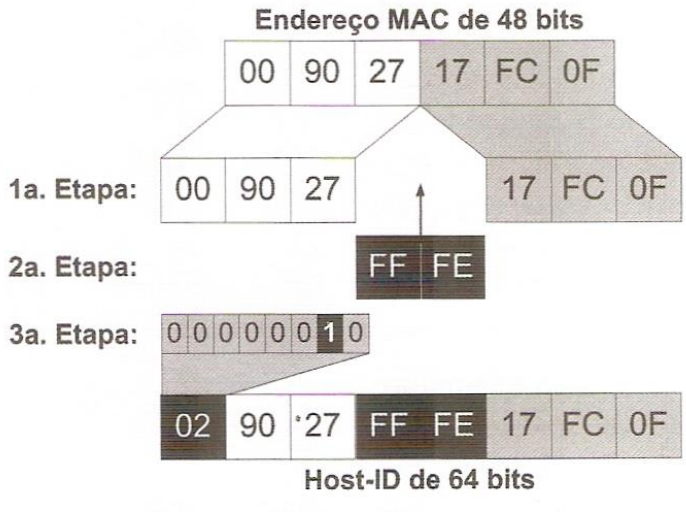
Os endereços *unicast* tem por finalidade identificar o *host* de maneira a ser único através de uma interface específica, de modo com que um pacote enviado a este endereço será recebido exclusivamente pelo mesmo. Isso faz com que o modelo fim-a-fim ao qual a Internet foi concebida seja reestabelecido. Os endereços *unicast* podem ser de três tipos: *link-local*, *unique-local* ou *global unicast* (BRITO, 2014).

Os endereços ***link-local*** são reservados de forma a serem exclusivos para comunicações locais e são fundamentais para assegurar várias funcionalidades fundamentais para o protocolo IPv6 (como por exemplo sua autoconfiguração). Os primeiros 10 bits do prefixo deste tipo de endereço compreende o seguinte intervalo: fe80::/10, fe90::/10, fea0::/10 e feb0::/10; sendo assim os demais 54 bits do prefixo são preenchidos com zeros.

Nesse caso o sufixo do endereço *link-local* é gerado automaticamente a partir do *MAC Address* da interface, através de um algoritmo de expansão denominado de EUI-64 (em sistemas operacionais *Microsoft Windows* não é utilizado o EUI-64 como padrão para gerar o endereço, o que é uma prática de privacidade proposta na RFC

4941). Este algoritmo possui três etapas distintas, sendo a primeira etapa a responsável por pegar o endereço físico da interface (que possui 48 bits) e separá-los em dois blocos de 24 bits. Na segunda etapa é acrescido os algarismos hexadecimais FFFE entre estes dois blocos de 24 bits, somando assim o total de 64 bits do sufixo do endereço, onde na terceira etapa este endereço passa por uma alteração, onde é invertido o sétimo bit do primeiro octeto do sufixo, finalizando então a atribuição do sufixo automático conforme Figura 15 (BRITO, 2014).

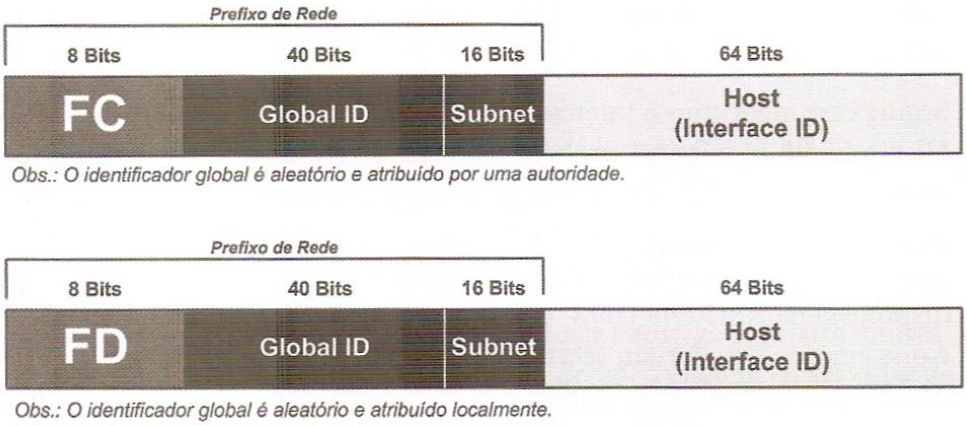
Figura 15 – Algoritmo EUI-64



Fonte: BRITO (2014, p. 92)

Endereços ***unique-local*** ou ULA são utilizados somente localmente, ou seja, não podem ser roteados com redes externas, são o equivalente aos endereços privados do IPv4. O prefixo deste tipo de endereço foi definido inicialmente em fc00::/7, porém ao longo do desenvolvimento do protocolo IPv6 foi dividido em dois blocos conforme estabeleceu a RFC 4193, sendo eles: fc00::/8 e fd00::/8.

Figura 16 – Endereço unique-local



Fonte: BRITO (2014, p. 61)

Os endereços ***global unicast*** por sua vez são o único tipo de endereço *unicast* que podem ser roteáveis através da Internet, pois são endereços públicos distribuídos pelas autoridades da Internet. A IANA inicialmente separou apenas uma porção de endereços IPv6 válidos para distribuir as RIR's, que são os endereços iniciados em 2000::/3. A previsão é de que a IANA distribua novos blocos de endereços IPv6 de acordo com a necessidade de utilização, desta forma liberando-os aos poucos.

3.2.1.2 Multicast

Os endereços de *multicast* são utilizados para enviar uma mesma mensagem para várias interfaces pertencentes ao mesmo grupo, assim como era utilizado no IPv4 através da classe D de IP's (que varia de 224.0.0.0 até 239.0.0.0). Utiliza-se este endereço somente como destino da comunicação, nunca como origem, uma vez que ele representa um grupo de múltiplos nós na rede.

Com o IPv6 todas as interfaces de uma rede local fazem parte de um grupo denominado de *multicast-all-nodes* (ff02::1) o que faz com que o *broadcast* utilizado no IPv4 seja dispensável, já que por padrão todas as máquinas pertencentes a uma rede local podem comunicar-se com todas as máquinas pertencentes a rede em questão (BRITO, 2014).

Tabela 3 – Endereços multicast IPv6 (RFC 2375)

Endereço	Escopo	Descrição
FF01::1	Interface	Todas as interfaces
FF02::1	Enlace	Todos os hosts no link
FF02::2	Enlace	Todos os roteadores no link
FF02::5	Enlace	Protocolo OSPFv3 (roteadores)
FF02::6	Enlace	Protocolo OSPFv3 (roteadores designados)
FF02::9	Enlace	Protocolo RIPng
FF02::A	Enlace	Protocolo Cisco®/EIGRP
FF02::1:FFXX:XXXX	Enlace	*Solicited-Node*
FF02::1:2	Enlace	Todos os servidores DHCP e relay-agents
FF05::1:3	Site	Todos os servidores DHCP
FF0X::101	Variável	Todos os servidores NTP

Fonte: BRITO (2014, p. 64)

3.2.1.3 Anycast

O endereço *anycast* segundo Jain e Sharma (2010) permite com que servidores que executam a mesma função (como servidores DHCP, DNS, *proxy,* etc) possam utilizar o mesmo endereço IPv6, pois desta forma o *host* irá estabelecer a comunicação com o servidor que estiver mais próximo (em relação ao número de saltos entre o *host* e o servidor) e em caso de indisponibilidade de um servidor, o outro assume a comunicação tomando o lugar de mais próximo, criando assim uma redundância do serviço.

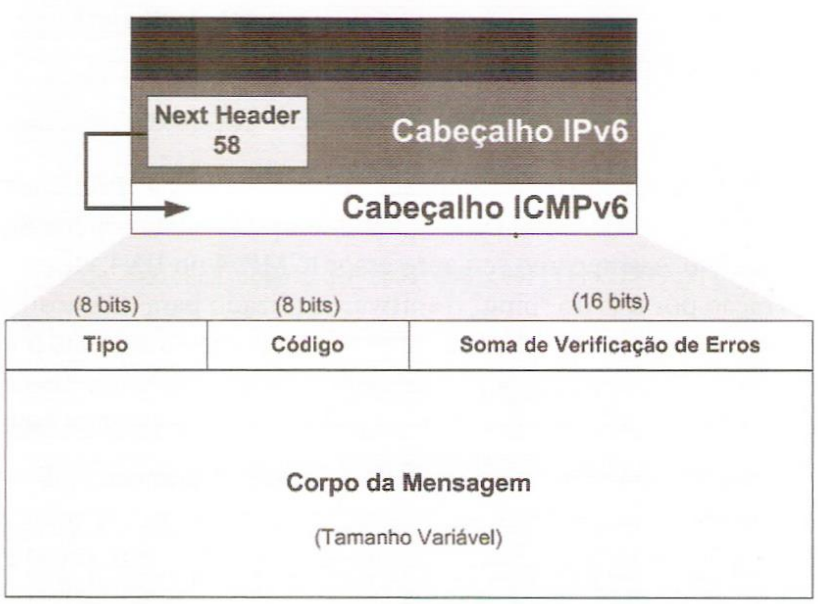
3.3 ICMPv6

O *Internet Message Control Protocol for IPv6* (ICMPv6) foi especificado na RFC 4443, sendo fundamental na operacionalização do protocolo IPv6, não sendo somente utilizado para funções como o comando *ping* no IPv4, como também compreende funcionalidades para comunicação entre máquinas vizinhas que são essenciais para o funcionamento correto da rede. Sendo assim a nova versão do ICMP não pode ser mais bloqueada por *firewalls* como ocorria no IPv4.

A integração entre o IPv6 e o ICMPv6 é feita através de cabeçalhos de extensão, onde na ordenação de encadeamento demonstrada na Tabela 2, o cabeçalho de extensão do ICMPv6 aplica o código 58 ao campo “próximo cabeçalho” do cabeçalho do protocolo IPv6.

O cabeçalho do ICMPv6 é simples, possuindo apenas 3 campos conforme Figura 16, onde os campos de tipo e código são utilizados para representar o formato das mensagens de controle e o campo “soma de verificação de erros” é utilizado para checar a integridade das mensagens enviadas.

Figura 17 – Cabeçalho ICMPv6



Fonte: BRITO (2014, p. 78)

As mensagens enviadas pelo ICMPv6 podem ser categorizadas em dois tipos, sendo mensagens de erro ou mensagens de informação, o campo do cabeçalho que permite com que seja possível identificar de qual grupo pertence a mensagem é justamente o campo “Tipo”, onde as mensagens de erro possuem o campo com o número 0 preenchido e as mensagens de informação possuem o campo com o número 1 preenchido. Por sua vez o campo código determina qual a mensagem de erro ou de informação que está sendo enviada, podendo variar de 0 a 127 para mensagens de erro e de 128 a 255 para mensagens de informação.

A importância do ICMPv6 para o funcionamento da rede IPv6 se dá graças as funções obtidas que no protocolo IPv4 pertenciam a outros protocolos (como ARP, RARP e IGMP) que não existem no protocolo IPv6 (BRITO, 2014).

3.3.1 NDP – Descoberta de vizinhança

O *Neighbor Discovery Protocol* (NDP) foi desenvolvido para descobrir a presença de nós vizinhos, desta forma solucionando alguns problemas de interação entre os mesmos, com isso é possível determinar os endereços MAC dos nós vizinhos, encontrar roteadores, descobrir prefixos de rede e manter informações dos nós vizinhos ativos. O NDP trabalha sobre dois aspectos fundamentais do IPv6, sendo eles a autoconfiguração de nós e a transmissão de pacotes, sendo assim é responsável por diversas funcionalidades podendo realizar as seguintes tarefas (IPv6.br, 2012; BRITO, 2014):

- Descoberta de parâmetros do enlace
- Autoconfiguração de endereços (SLAAC)
- Descoberta de roteadores e prefixos
- Resolução de endereços físicos (MAC)
- Detecção de endereços duplicados (DAD)
- Detecção de atividade no vizinho
- Redirecionamento de roteadores

4 NAT

> Para ajudar a prolongar a vida do IPv4 e seu esquema de endereçamento enquanto o novo protocolo IPv6 é desenvolvido e implantado, outras tecnologias têm sido desenvolvidas. Uma das mais importante delas é a Network Address Translation. Esta tecnologia permite que um pequeno número de endereços IP públicos possam ser compartilhados por um grande número de hosts usando endereços privados. Este pequeno "truque" essencial permite que a Internet global tenha realmente muito mais hosts sobre ela do que seu espaço de endereçamento normalmente suporta (KOZIEROK, 2005, p. 518).

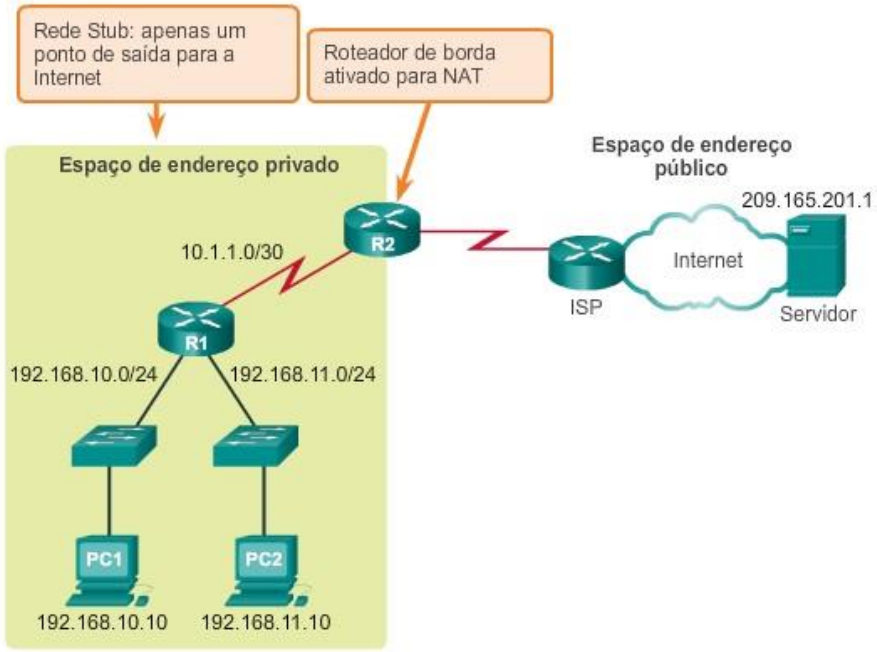
4.1 Conceitos

Segundo Morimoto (2011), o NAT basicamente permite que vários *hosts* de uma rede local acessem a Internet compartilhando de apenas um único endereço válido na rede externa, independente da forma com que você acessa a Internet. Para isso o NAT ao receber um pacote da rede local endereçado à Internet, substitui o endereço do *host* pelo seu (ficando assim como remetente do pacote para o destino) e ao receber a resposta do destino, altera o endereço do destinatário para o seu endereço, enviando a resposta para a máquina da rede local, dessa forma fazendo com que o *host* que se encontra na rede local enxergue que está se comunicando com o servidor, sem enxergar os demais *hosts* da Internet e o destinatário que se encontra na Internet enxergue que está se comunicando com o servidor, sem enxergar os hosts que estão na rede local. Durante o decorrer deste capítulo, serão abordadas as funcionalidades do NAT utilizando a forma como é utilizado atualmente, ou seja, com o protocolo IPv4.

Um roteador NAT pode ser configurado com um ou mais endereços públicos para acesso a rede externa, dependendo da necessidade da rede, esse endereço público configurado recebe o nome de *pool de NAT*. Esse roteador configurado com NAT recebe o nome de roteador de borda, pelo fato de ficar na borda da rede local,

realizando a comunicação com a rede externa. Normalmente o roteador de borda possui somente um endereço público configurado, ficando dessa forma apenas um ponto de saída e um ponto de entrada entre a comunicação da rede local com a rede externa, o que é conhecido como *rede stub* conforme se observa na Figura 18 (CISCO, 2013).

Figura 18 – NAT – Rede stub



Fonte: CISCO (2013, Módulo 11.1.1.2)

4.1.1 Tipos de endereço

No entendimento de NAT é importante salientar que uma rede interna é todo o conjunto de rede que se sujeita a conversão de endereços e uma rede externa é qualquer rede com a qual a comunicação será realizada. Quando se utiliza o NAT em redes locais IPv4, os endereços IP possuem nomenclaturas distintas por serem de tipos distintos dependendo de onde se localizam, sendo na rede interna ou na rede externa e se o tráfego do pacote é de entrada ou saída. Sendo assim, possuem-se as seguintes nomenclaturas segundo a CISCO (2013):

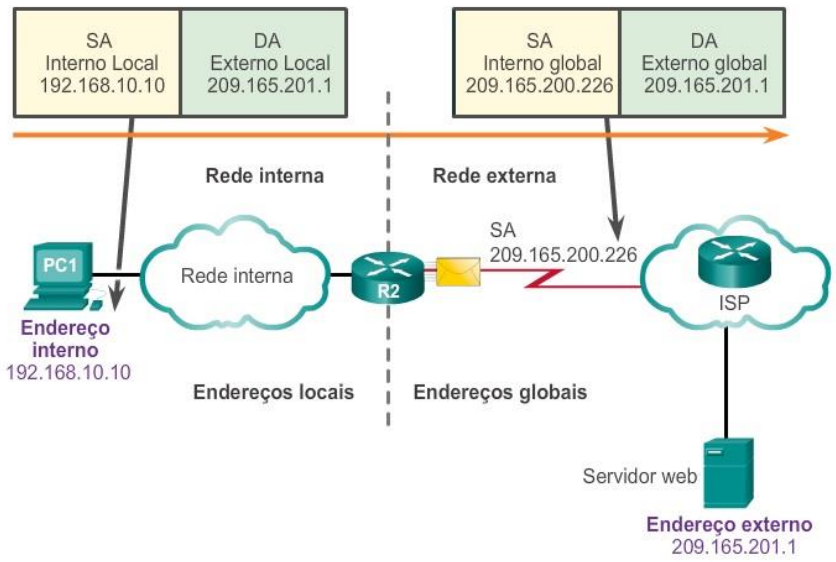
- Endereço local interno

- Endereço global interno
- Endereço local externo
- Endereço global externo

Um endereço interno é o endereço que está sendo traduzido pelo NAT, enquanto que o externo é o endereço do dispositivo destino do pacote. Da mesma forma um endereço local é qualquer endereço que se encontra dentro da rede e endereço global o que se encontra na parte externa da rede. Dessa forma foram combinados os termos interno e externo com os termos local e global a fim de se referenciar a endereços específicos no processo de tradução de endereços.

Ainda de acordo com a Cisco (2013), exemplifica-se a funcionalidade do NAT utilizando-se do exemplo demonstrado na Figura 19, onde o PC1, que pertence a uma rede que possui o NAT traduzindo endereços, necessita se comunicar com o servidor web pertencente à rede externa. Para que a comunicação ocorra, o PC1 que possui endereço local interno 192.168.10.10 tem o seu endereço convertido pelo roteador NAT (R2) para o endereço interno global 209.165.200.226. Ao converter o endereço, o pacote é encaminhado então para o servidor web (que possui o mesmo endereço global externo e local externo: 209.165.201.1, pois é o mesmo IP público).

Figura 19 – Tipos de endereços NAT



Fonte: CISCO (2013, Módulo 11.1.1.3)

A tradução de endereços feita pelo NAT é um processo que ocorre em tempo real, de forma a não causar um problema de latência considerável na conexão, porém quebrando o modelo fim a fim original da internet e como se trata de uma conexão que não divide o link com a rede externa entre as estações da rede interna, e sim o compartilha, dependendo da quantidade de estações e o consumo de banda que as mesmas realizam, pode sim ocasionar em um gargalo de rede, trazendo lentidão a rede interna (MORIMOTO, 2011).

4.2 Tipos de NAT

De acordo com Srisuresh *et al* (2001) na RFC 3022, o NAT tradicional possui três formas de tradução de endereços, onde são elas: NAT estático, NAT dinâmico e *Network Address Port Translation* (NAPT). Vale ressaltar que é possível encontrar autores que indicam outras formas de se utilizar o NAT, como por exemplo, NAPT, Twice NAT, NAT bi-direcional, NAT-PT, etc; porém como o escopo deste trabalho é a viabilidade do NAT em redes IPv6, não serão abordadas todas as formas existentes de se utilizar NAT, desta forma serão demonstradas somente as formas descritas na RFC 3022.

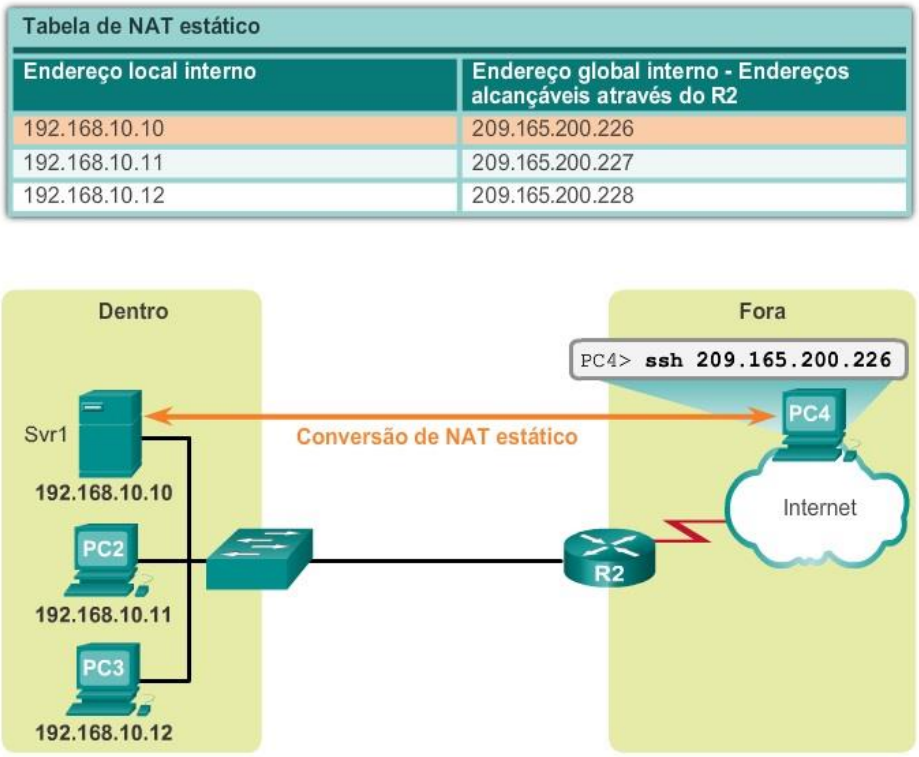
4.2.1 NAT estático

Como o próprio nome diz, esse tipo de NAT utiliza um mapeamento estático da tradução de endereços, de um para um, ou seja, o administrador de rede define os endereços de forma com que determinado endereço local sempre utilize determinado endereço global (KOZIEROK, 2005).

Utilizar o NAT estático pode ser muito útil para *hosts* que necessitam ter um endereço estático acessível pela internet, como por exemplo um servidor *web* que pode ser acessível remotamente através de *Secure Shell* (SSH). Porém essa mesma utilidade se não for configurada corretamente, pode deixar o host vulnerável a ataques provenientes da rede externa. Observa-se o exemplo citado através da Figura 20, onde cada *host* possui seu endereço global interno definido de forma

estática pelo administrador da rede e também o acesso remoto do servidor *web* (Svr1) através do *host* pertencente à rede externa (PC4).

Figura 20 – NAT estático



Fonte: CISCO (2013, Módulo 11.1.2.1)

4.2.2 NAT dinâmico

O NAT dinâmico trabalha com um *pool* de endereços globais, também definidos pelo administrador da rede no roteador de borda, onde esses endereços são distribuídos aos *hosts* conforme os mesmos solicitam um endereço válido na rede externa para se comunicarem com hosts externos. Dessa forma os endereços globais que não estiverem mais sendo utilizados vão ficando disponíveis novamente para que sejam distribuídos conforme novas solicitações de *hosts* da rede interna.

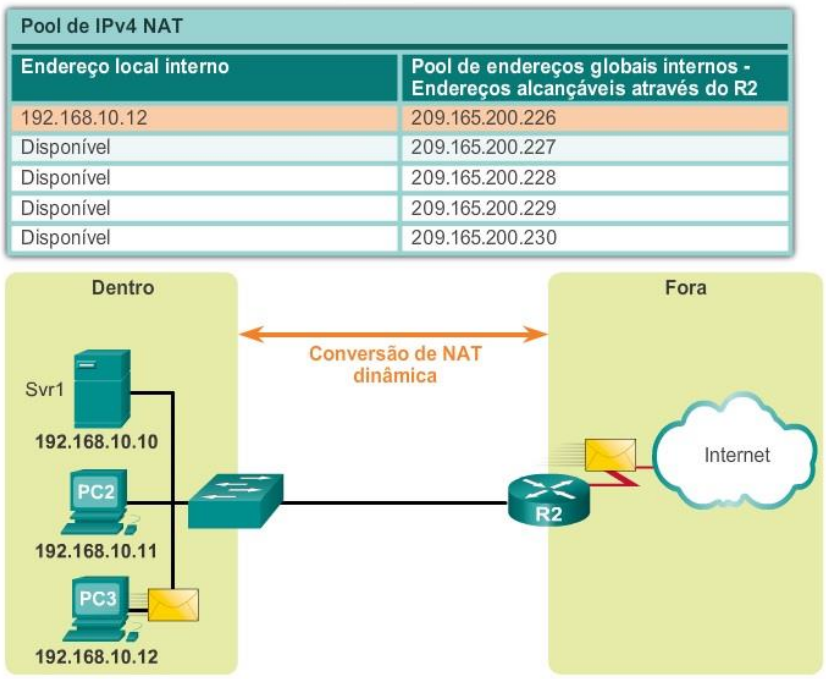
Esse tipo de configuração do NAT torna menos onerosa a tarefa de configuração do roteador do que o NAT estático, pois uma vez configurado o *pool* de endereços globais, a distribuição de IP's válidos na rede externa para *hosts* da rede

interna se torna automática, enquanto que no NAT estático a cada *host* incluído na rede é necessário alterar as configurações do NAT para atribuir ao mesmo um endereço global válido.

Essa forma de NAT é usada também para prover obscuridade a rede interna perante a rede externa, pois como o NAT distribui os endereços de forma dinâmica dependendo da ordem em que os *hosts* fazem a solicitação de um endereço global válido, o mesmo *host* pode possuir IP's diferentes dependendo do momento que solicita o endereço ao roteador de borda para se comunicar com a rede externa, dessa forma dificultando seu acesso à partir da rede externa, por exemplo, utilizando o SSH como visto no NAT estático (KOZIEROK, 2005).

Na Figura 21 analisa-se um exemplo de NAT dinâmico, onde o *host* PC3 (que possui o endereço local interno 192.168.10.12) deseja se comunicar com a internet. Para isso o roteador de borda que possui um *pool* de endereços globais interno viabiliza o primeiro endereço disponível (209.165.200.226) para o *host*, fazendo com que a comunicação com a rede externa seja possível.

Figura 21 – NAT dinâmico



Fonte: CISCO (2013, Módulo 11.1.2.2)

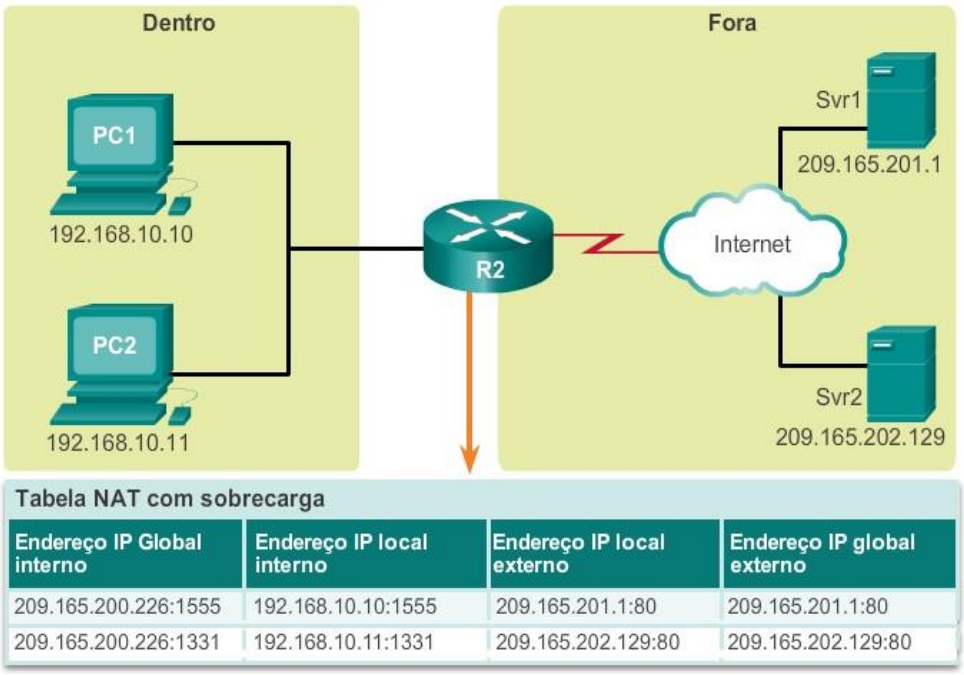
4.2.3 Network Address Port Translation (NAPT)

Faz-se importante que saibamos que a terminologia NAPT pode ser abordada de diferentes maneiras, como por exemplo, *Hide-Mode* NAT (denominação utilizada pela empresa *Check Point*), *Port Address Translation* (PAT, denominação utilizada pela Cisco), *SNAT/MASQUERADE* (denominação utilizada em iptables de firewalls Linux), *Internet Connection Sharing* (denominação utilizada pela Microsoft) e também o NAT *Overload* (tradução livre para sobrecarga de NAT) (MACIEL, 2009). Por fim, independente da nomenclatura adotada, os fundamentos desse tipo de NAT são os mesmos, porém utilizaremos a nomenclatura adotada na RFC 3022: NAPT.

O NAPT possibilita com que a conversão de endereços da rede interna para a rede externa seja possível utilizando apenas um único endereço IPv4 válido na rede externa. Isso é possível por conta que quando um *host* inicia uma sessão TCP/IP, é gerado um valor de porta de origem. Quando a comunicação passa pelo roteador de borda, o mesmo utiliza esse número de porta de origem para identificar a sessão e então atribui na conversão de endereços não somente o IP público válido que possui como também a porta do início da comunicação, fazendo assim com que vários *hosts* utilizem seu único IP válido para realizar a comunicação com a rede externa e distinguindo cada comunicação através de sua porta de origem, assim como se exemplifica na Figura 22.

Esse número de porta atribuído também é utilizado pelo roteador quando a resposta é recebida do *host* da rede externa, tornando-se assim o identificador para o roteador de borda saber a qual *host* da rede interna pertence o pacote recebido, para que assim possa encaminhá-lo corretamente (CISCO, 2013).

Figura 22 – NAPT



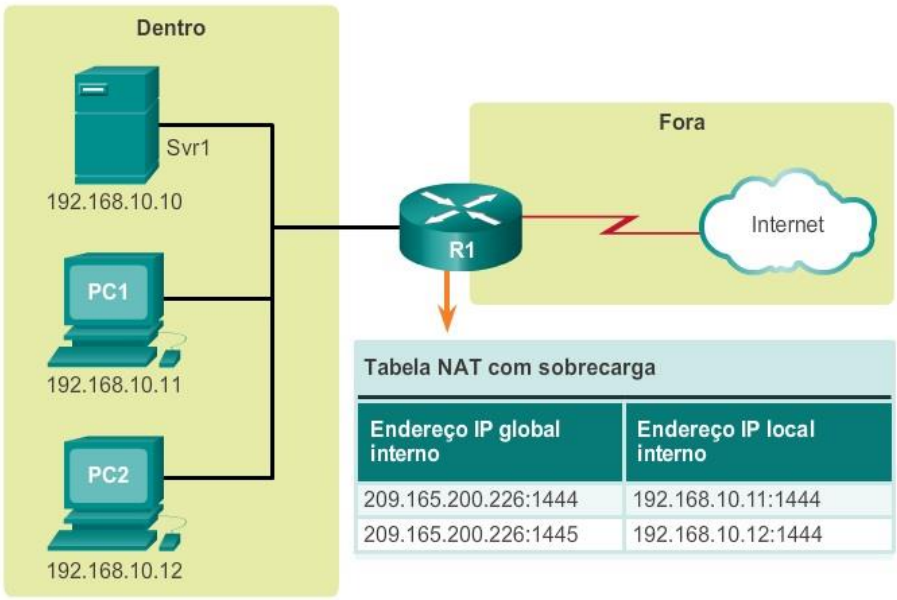
Fonte: CISCO (2013, Módulo 11.1.2.3)

O NAPT é o tipo de NAT mais utilizado segundo a Cisco (2013), pois é o que a maioria dos roteadores residenciais utiliza como padrão. Nesse cenário o *Internet Service Provider* (ISP) designa um endereço IP válido ao roteador que por sua vez o compartilha através do NAPT com os vários dispositivos que os usuários utilizam em suas residências (por exemplo: celulares, *notebook's*, computadores, *smart tv's*, etc).

Outra característica fundamental do NAPT é que o mesmo tenta preservar a porta de origem, pois é comum que vários dispositivos tentem utilizar a mesma porta de origem, porém como o NAPT atribui de forma dinâmica o endereço com a porta, caso já exista algum *host* utilizando o endereço em questão com a mesma porta de origem desejada, o NAPT atribui o primeiro próximo número de porta disponível. Exemplificando conforme a Figura 23, onde dois *hosts* (PC1 e PC2) tentam utilizar do mesmo endereço IP global interno (209.165.200.226:1444) com a Internet. Como o PC1 se comunicou com o roteador de borda primeiro, o NAPT atribuiu seu endereço IP global interno como 209.165.200.226:1444 e quando o PC2 foi realizar a comunicação, lhe foi atribuído o endereço IP global interno como 209.165.200.226:1445, ou seja, ao invés de utilizar a mesma porta do PC1 (1444),

foi atribuído ao PC2 a porta 1445, a próxima numeração de porta disponível (CISCO, 2013).

Figura 23 – NAPT – Próxima porta disponível



Fonte: CISCO (2013, Módulo 11.1.2.4)

4.2.4 Diferenças entre NAT (estático e dinâmico) e NAPT

A diferença essencial do NAT (estático e dinâmico) e NAPT é a forma como convertem os endereços IPv4 privados para endereços IPv4 públicos. Enquanto o NAT (estático e dinâmico) converte utilizando uma base de um para um (um endereço privado para um endereço público) o NAPT modifica o endereço e o número da porta, conforme Figura 24.

O NAT encaminha os pacotes de entrada para seu destino utilizando o endereço IP fornecido pelo *host* da rede externa, enquanto o NAPT utiliza as tabelas de NAT no roteador para associar os pares de portas públicos e internos, o que é chamado de rastreamento de conexão (CISCO, 2013).

Figura 24 – Diferença de NAT e NAPT

NAT

Pool de endereços globais internos	Endereço local interno
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

NAPT

Endereço global interno	Endereço local interno
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

Fonte: CISCO (2013, Módulo 11.1.2.5)

4.3 Coexistência entre IPv4 e IPv6 com NAT-PT

O período de transição do IPv4 para o IPv6 não é imediato, sendo assim existem algumas técnicas de coexistência entre as duas versões do protocolo IP, onde é necessário que redes com diferentes versões se comuniquem. Para que essa comunicação entre as versões diferentes do protocolo ocorra, o *Sirindhorn International Institute of Technology* (SIIT) propôs que o NAT fosse utilizado, fazendo com que endereços de uma rede IPv6 fossem traduzidos para endereços IPv4 e vice-versa. Assim então foi estabelecida a RFC 2766, com a criação do *Network Address Translation Protocol Translation* (NAT-PT). O NAT-PT por sua vez possui as mesmas características do NAT tradicional estabelecido na RFC 3022, podendo ser estático ou dinâmico (possuindo também a função de NAPT, porém alterando a nomenclatura para NAPT-PT) (TSIRTSIS G.; SRISURESH P, 2000).

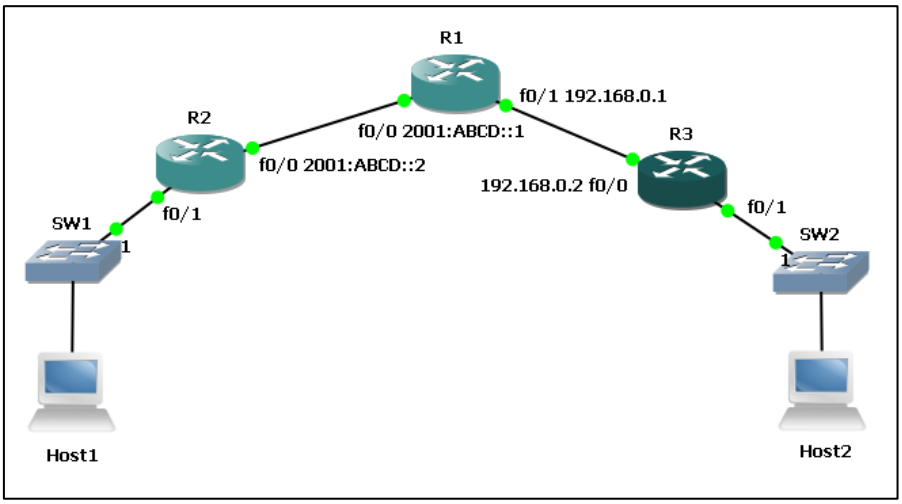
5 ANÁLISE EXPERIMENTAL

Nos capítulos anteriores foi abordado o surgimento do protocolo IP até sua expansão em sua versão 4, assim como suas características estruturais que levaram a escassez de endereços válidos na Internet e as medidas paliativas tomadas para prolongar seu uso. Além disso, foi abordada a nova versão do protocolo, a versão 6, onde com alterações estruturais não só foi possível solucionar o problema de escassez de endereços válidos na Internet como também solucionou várias outras falhas da versão anterior.

Após a abordagem do protocolo IP em suas versões 4 e 6 foi explanado o NAT, demonstrando seus conceitos e funcionalidades para a manutenção do IPv4 em funcionamento e uma breve demonstração de como também é utilizado para manter redes IPv4 e IPv6 coexistindo. Dessa forma agora se apresenta uma demonstração prática dos conceitos e técnicas até aqui abordadas com o auxílio do software de simulação de redes *Cisco Packet Tracer Student* (versão 6.2.0.0052), que por possuir limitações no *Cisco Express Forwarding* (CEF) não permite simular NAT tradicional ou NAT-PT, e por isso também foi utilizado o software de simulação de redes GNS3 (versão 1.3.11) que permite a simulação utilizando o roteador Cisco 3725.

O primeiro cenário é mostrado na Figura 25, onde uma rede IPv6 necessita se comunicar com uma rede IPv4 e para que a comunicação fosse possível foi utilizado o NAT-PT.

Figura 25 – Cenário 1 – NAT-PT



Fonte: Autoria própria.

Foram utilizados três roteadores no cenário, onde o **R1** é o roteador responsável pela comunicação e coexistência da rede com endereçamento IPv6 (representada pelo **R2**) e a rede com endereçamento IPv4 (representada pelo **R3**).

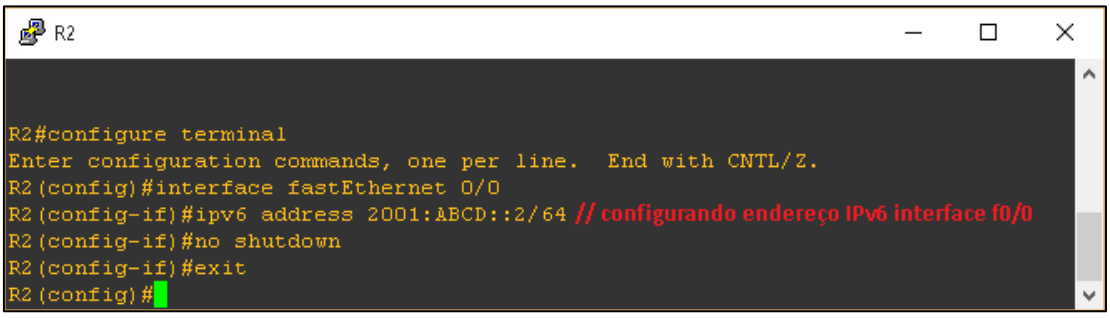
Na Figura 26, foram configurados manualmente no roteador R1 os endereços em suas respectivas interfaces de forma que a interface (f0/0) conectada ao R2 recebesse o endereço IPv6 2001:ABCD::1/64 e a interface (f/01) recebesse o endereço IPv4 192.168.0.1. Após a configuração dos endereços, foi habilitado o encaminhamento de pacotes IPv6. Com o endereçamento e roteamento configurados no R1, definiu-se o prefixo do endereço IPv6 utilizado para realizar o endereçamento dos endereços IPv4 traduzidos para IPv6, onde ao configurar o prefixo, também foi definido de forma estática a tradução de endereços, tanto de IPv4 para IPv6 quanto o contrário. Após realizar todas as configurações, foi habilitado o IPv6 em ambas as interfaces do R1.

Figura 26 – Cenário 1 – R1

Fonte: Autoria própria.

Após configurar o R1 para possibilitar a coexistência entre as redes IPv4 e IPv6, realizou-se então a configuração dos roteadores de cada versão do protocolo IP. Primeiramente foi configurado o R2 com o protocolo IPv6, onde para isso apenas foi configurado manualmente o endereço IPv6 na interface (f0/0) que realiza a comunicação com o R1, conforme observa-se na Figura 27.

Figura 27 – Cenário 1 – R2

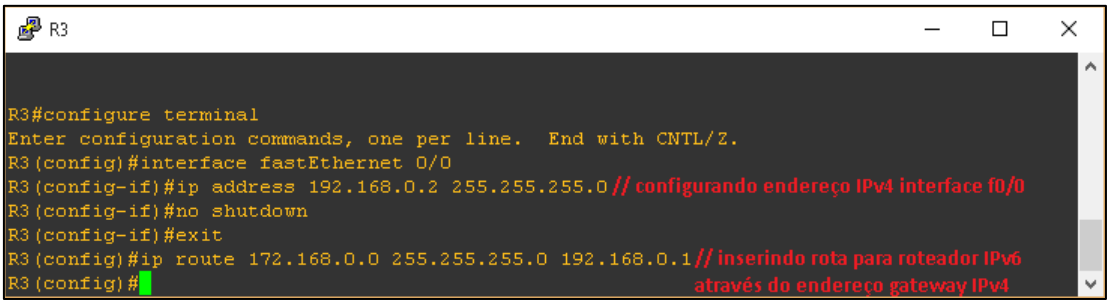


Fonte: Autoria própria.

Após a configuração do R2, foi configurado o R3 com IPv4, onde não somente foi configurado o endereço manualmente na interface (f0/0) que faz comunicação com o R1, como também foi configurada uma rota através do R1 para

que fosse possível a comunicação com o endereço de rede utilizado pelo R2 na tradução para endereço IPv4, como se pode observar na Figura 28.

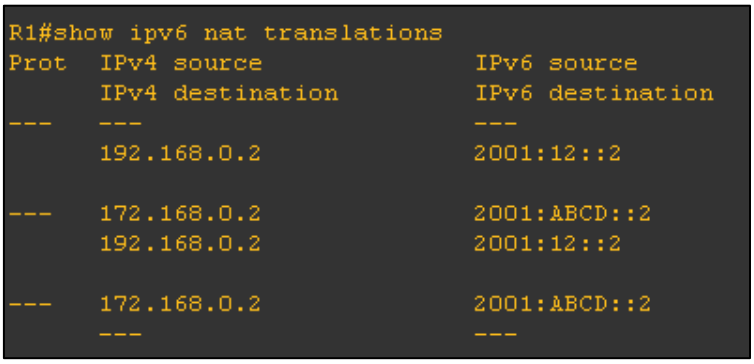
Figura 28 – Cenário 1 – R3



Fonte: Autoria própria.

Com as configurações de todos os roteadores realizadas, pode-se utilizar de alguns comandos para certificar-se de que o NAT-PT está configurado corretamente, conforme Figura 29 onde se podem observar as traduções de endereços que foram criadas de forma estática.

Figura 29 – Cenário 1 – NAT-PT translations



Fonte: Autoria própria.

Conforme apresentado anteriormente, o NAT quebra o modelo fim-a-fim da Internet, pois é necessário que o endereço seja traduzido para que tenha validade na rede externa. Como se observa na Figura 30 foi utilizado o comando *traceroute* no R2 para o R3, a fim de se analisar esse aspecto do NAT e o real impacto que o mesmo causa no roteamento do pacote em relação ao tempo (em msec) que o pacote demora a percorrer o caminho da origem até o destino.

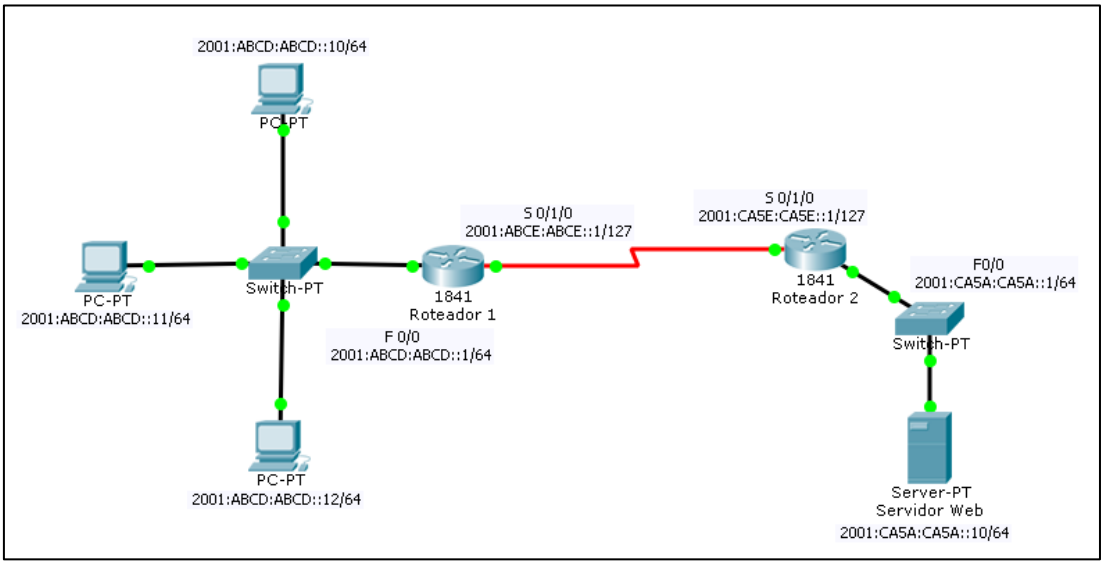
Figura 30 – Cenário 1 – Traceroute

```
R2#traceroute 2001:12::2

Type escape sequence to abort.
Tracing the route to 2001:12::2

  1 2001:ABCD::1 48 msec 40 msec 44 msec // tempo para realizar a rota até o R1
  2 2001:12::2 100 msec 52 msec 100 msec // tempo para realizar a rota até o R2
```

Fonte: Autoria própria.

Para que fosse possível realizar a análise de forma a procurar uma resposta ao problema apresentado durante o trabalho, sobre a viabilidade do NAT em redes IPv6, tornou-se necessária a criação de um segundo cenário onde uma rede IPv6 comunica-se com outra rede IPv6, sem o auxílio de NAT, conforme observa-se na Figura 31.

Figura 31 – Cenário 2 – IPv6



Fonte: Autoria própria.

No segundo cenário pode-se verificar que os comandos utilizados são os mesmos do R2 do cenário anterior, onde os endereços foram configurados manualmente nas interfaces e o encaminhamento de pacotes IPv6 foram habilitados. A única diferença conforme se observa na Figura 32 é a criação de rota IPv6 do **Roteador 1** para o **Roteador 2**.

Figura 32 – Cenário 2 – Roteador 1

```
Roteador1>enable
Roteador1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Roteador1(config)#ipv6 unicast-routing
Roteador1(config)#interface fastEthernet 0/0
Roteador1(config-if)#ipv6 enable
Roteador1(config-if)#ipv6 address 2001:ABCD:ABCD::1/64
Roteador1(config-if)#no shutdown
Roteador1(config-if)#exit
Roteador1(config)#interface serial 0/1/0
Roteador1(config-if)#ipv6 address 2001:ABCE:ABCE::1/127
Roteador1(config-if)#no shutdown
Roteador1(config-if)#exit
Roteador1(config)#ipv6 route 2001:CA5E:CA5E::1/127 s0/1/0 //criando rota de endereço IPv6 a partir da interface
Roteador1(config)#
```

Fonte: Autoria própria.

Da mesma forma para o Roteador 2 também foram realizadas as mesmas configurações, assim como a rota IPv6 para o Roteador 1, possibilitando assim a comunicação entre ambos como demonstra-se na Figura 33.

Figura 33 – Cenário 2 – Roteador 2

```
Roteador2>enable
Roteador2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Roteador2(config)#ipv6 unicast-routing
Roteador2(config)#interface fastEthernet 0/0
Roteador2(config-if)#ipv6 address 2001:CA5A:CA5A::1/64
Roteador2(config-if)#no shutdown
Roteador2(config-if)#exit
Roteador2(config)#interface serial 0/1/0
Roteador2(config-if)#ipv6 address 2001:CA5E:CA5E::1/127
Roteador2(config-if)#no shutdown
Roteador2(config-if)#exit
Roteador2(config)#ipv6 route 2001:ABCE:ABCE::1/127 s0/1/0 // criando rota de endereço IPv6 a partir da interface
```

Fonte: Autoria própria.

Com os endereços, roteamento habilitado e rotas criadas, a comunicação entre os roteadores e as redes pertencentes aos mesmos já é possível. Fazendo com que dessa forma seja possível analisar o tempo em que os pacotes levam para realizar a rota de um roteador para outro com o comando *traceroute*, assim como no cenário anterior. Sendo assim observa-se na Figura 34 que o resultado do comando no Roteador 1 para o Roteador 2, em uma rede sem o NAT e onde ocorre a comunicação fim-a-fim da Internet, acaba sendo substancialmente mais rápida que com a utilização do NAT.

Figura 34 – Cenário 2 – Traceroute Roteador 1

```
Roteador1#traceroute 2001:CA5E:CA5E::1
Type escape sequence to abort.
Tracing the route to 2001:CA5E:CA5E::1

  1   2001:CA5E:CA5E::1 0 msec    0 msec    3 msec
```

Fonte: Autoria própria.

Como no primeiro cenário a comunicação entre o R2 e o R3 não é direta, possuindo um intermediário (R1), para a validação do resultado do cenário 2, realizou-se o comando *tracert* de um computador pertencente a rede do Roteador 1 com destino ao Roteador 2, ficando assim o Roteador 1 como intermediário, e como pode-se observar na Figura 35, mesmo assim a comunicação ocorreu de forma mais eficaz que no primeiro cenário.

Figura 35 – Cenário 2 – Tracert PC

```
PC>tracert 2001:CA5E:CA5E::1

Tracing route to 2001:CA5E:CA5E::1 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      2001:ABCD:ABCD::1
  2    0 ms      0 ms      1 ms      2001:CA5E:CA5E::1

Trace complete.
```

Fonte: Autoria própria.

6 CONSIDERAÇÕES FINAIS

Durante o desenvolvimento do trabalho foram utilizados livros de autores conceituados nos temas apresentados além dos materiais de estudos elaborados pelas melhores companhias do mercado, assim como também foram utilizados as próprias normas elaboradas pelos órgãos regulamentadores da internet (como por exemplo, as RFC's utilizadas). Em posse deste material teórico apresentado, foi realizada uma análise experimental em busca de responder o problema apresentado na introdução do trabalho e assim as considerações finais serão apresentadas a seguir.

O surgimento da Internet e sua expansão através da sua versão comercial fizeram com que rapidamente o protocolo IP em sua versão 4 não pudesse mais suprir a grande demanda de endereços válidos para seus usuários. Neste quesito as medidas paliativas para o mantimento do protocolo em funcionamento foram de extrema importância, onde o NAT se destacou por conseguir prolongar o uso do IPv4 por anos após seu esgotamento, como atualmente ainda ocorre até que seja realizada a transição para o IPv6.

Por ter se tornado de extrema importância no IPv4, vários administradores de redes relutam para realizar a migração para o IPv6 sem a utilização do NAT, por entenderem de forma equívoca (como demonstrado durante o decorrer do trabalho) que o NAT além de um mecanismo de tradução de endereços, também é um mecanismo de segurança para a rede.

Logo então se questiona a viabilidade do uso do NAT no IPv6, onde como forma de se aprofundar mais no tema a fim de concluir uma resposta para o questionamento, a análise experimental foi de extrema importância. Através dela é possível verificar que o NAT em IPv6 não se torna mais necessário, pois além de ser mais oneroso o trabalho de configuração de um roteador IPv6 com NAT, também acarreta em uma comunicação mais lenta em relação ao tempo em que o roteador

demora a traduzir o endereço da rede interna para a rede externa, assim como observado na análise experimental. Outro ponto considerável como argumentação para a não utilização do NAT no IPv6 é o fato de que a Internet foi desenvolvida com o modelo fim-a-fim e o NAT quebra esse modelo.

Dessa forma conclui-se que o NAT foi e continua sendo um ótimo mecanismo no IPv4 para o mantimento de sua vida útil, porém com a nova versão do protocolo desenvolvida e uma iminente migração para a mesma em um futuro próximo, o NAT já não possui mais sua utilidade principal, pois não será mais necessário a tradução de endereços de uma rede para outra. Aliado ao fato de comprometer o modelo fim-a-fim da Internet e ocasionar lentidão em comunicação entre redes às quais intermedia, a conclusão final ao problema abordado é que não é viável a utilização de NAT com o protocolo IPv6.

6.1 Trabalhos Futuros

Durante o desenvolvimento deste trabalho alguns temas não foram tanto explorados por não serem de suma importância para o escopo proposto, porém seria de grande valia para o meio acadêmico e técnico um estudo mais elaborado sobre os mesmos. Neste cenário é proposto o desenvolvimento de um estudo mais elaborado sobre o ICMPv6 a fim de demonstrar todas as suas novas funcionalidades e seu papel de importância para o protocolo IPv6. Outro aspecto interessante que pode ser abordado com maior profundidade são os cabeçalhos de extensão do IPv6 pois além de agilizar a comunicação por conta de facilitar o processamento de pacotes pelos roteadores, também possui vários tipos, onde cada um exerce uma determinada função e a compreensão de cada função se faz importante neste cenário.

Outra sugestão para pesquisa futura seria estudar todas as formas de utilização do NAT no IPv4 e como essas formas permitem que o protocolo ainda seja o mais utilizado, mesmo já havendo uma nova versão desenvolvida com melhoramentos e quantidade de endereços válidos exponencialmente maior.

REFERÊNCIAS BIBLIOGRÁFICAS

BRITO, Samuel Henrique Bucke. **IPv6:** o novo protocolo da Internet. São Paulo: Novatec, 2014. 208 p.

CEPTRO, A Internet e o TCP/IP. Disponível em: <http://ipv6.br/entenda/introducao/>. Acesso em: 26 Ago. 2015.

CISCO Network Academy. Capítulo 11: Conversão de endereço de rede para IPv4. In: **CISCO Network Academy CCNA 5.0 – Princípios básicos de roteamento e switching**. Cisco Systems, Inc. 2013.

ÇALIşKAN, Emin. ***IPv6 transition and security threat report***, Tallinn: CCDCOE, 2014. Disponível em: <https://ccdcoe.org/publications/articles/IPv6-Report.pdf>. Acesso em: 29 Out. 2014.

FOROUZAN, B. A. **Protocolo TCP/IP**. Tradução da 3ª edição. São Paulo: McGraw-Hill Interamericana do Brasil Ltda., 2008.

IPV6.BR. **Funcionalidades Básicas**. Disponível em: <http://ipv6.br/post/funcionalidades-basicas/>. Acesso em: 27 Out. 2015.

JAIN, R.; SHARMA, S. ***IPv6 Addressing Strategy***. San Jose: Cisco Systems, Inc. 2010.

KOZIEROK, Charles M. *IP Network address translation (NAT) Protocol*. In: KOZIEROK, Charles M. ***The TCP/IP guide:*** *a comprehensive, illustrated Internet protocols reference*. San Francisco: No Starch Press, 2005. p. 518-544.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet:** Uma Abordagem Top-Down. Tradução da 5ª edição. São Paulo: Addison Wesley, 2010.

MACIEL, Marcus. **O que é um NAT ? O que é um PAT ?**. 2009. Disponível em: <https://under-linux.org/entry.php?b=1223>. Acesso em: 17 Set 2015.

MARINE A. et al. ***FYI on questions and answers:*** *answers to commonly asked "New Internet user" questions*, RFC 1594. 1994. Disponível em: <https://www.rfc-editor.org/rfc/rfc1594.txt>. Acesso em: 30 Ago. 2015.

MORAIS, Carlos T. Queiroz de. **Conceitos sobre Internet e Web**. Porto Alegre: Editora da UFRGS, 2012. 112 p.

MOREIRAS, Antonio M. et al. **Laboratório de IPv6:** aprenda na prática usando um emulador de redes. São Paulo: Novatec, 2015. 416 p. Disponível em: <http://ipv6.br/media/arquivo/ipv6/file/64/livro-lab-ipv6-nicbr.pdf>. Acesso em: 28 Set. 2015.

MORIMOTO, Carlos. **Redes:** guia prático. 2 ed. Rio Grande do Sul: GDH Press e Sul Editores. 2011. 560 p.

_____. **Guia prático:** redes e servidores Linux. 2 ed. Rio Grande do Sul: GDH Press e Sul Editores. 2006. 448 p.

POSTEL, Jon. ***Internet Protocol***, RFC 791. 1981. Disponível em: <https://www.rfc-editor.org/rfc/rfc791.txt>. Acesso em: 23 Ago. 2015.

SANTOS, Cleymone Ribeiro dos. **Integração de IPv6 em um ambiente cooperativo seguro**. 2004. 168 f. Dissertação (Mestrado em Ciência da Computação). Universidade Estadual de Campinas, Campinas.

SRISURESH P. et al. ***Traditional IP Network Address Translator (Traditional NAT)***, RFC 3022. 2001. Disponível em: <https://www.rfc-editor.org/rfc/rfc3022.txt>. Acesso em: 17 Out 2015.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. Tradução da 5ª edição. Rio de Janeiro: Elsevier Editora Ltda, 2005.

TSIRTSIS G.; SRISURESH P. ***Network Address Translation - Protocol Translation (NAT-PT)***, RFC 2766. 2000. Disponível em: <https://www.rfc-editor.org/rfc/rfc2766.txt>. Acesso em: 06 Nov 2015.