UNIVERSIDADE FEDERAL DO PARÁ

CAMPUS UNIVERSITÁRIO DE CASTANHAL

FACULDADE DE COMPUTAÇÃO

CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

CYDIANE CAMPOS DE OLIVEIRA

Simulação e avaliação de uma rede de computadores utilizando o protocolo de internet versão 6

CASTANHAL – PA

2019

CYDIANE CAMPOS DE OLIVEIRA

Simulação e avaliação de uma rede de computadores utilizando o protocolo de internet versão 6

Trabalho de conclusão de curso apresentado como exigência para obtenção do grau de Bacharel em sistemas de Informação, pela Universidade Federal do Pará - UFPA.
Orientador: José Jailton Henrique Ferreira Junior
Co-orientador: Luiz Fernando Gonçalves da Luz

CASTANHAL – PA
2019

CYDIANE CAMPOS DE OLIVEIRA

Simulação e avaliação de uma rede de computadores utilizando o protocolo de internet versão 6

Trabalho de conclusão de curso apresentado como exigência para obtenção do grau de Bacharel em sistemas de Informação, pela Universidade Federal do Pará - UFPA.
Orientador: Jailton Henrique Ferreira Junior
Co-orientador: Luiz Fernando Gonçalves da Luz

BANCA EXAMINADORA

_____

Prof. Dr. José Jailton Henrique Ferreira Junior

_____

Prof. Esp. Luiz Fernando Gonçalves da Luz

_____

Prof. Dr. Igor Ruiz Gomes

_____

Prof. Me. Felipe Andre da Costa Brito

CASTANHAL - PA

2019

Dedico esse trabalho, com muito amor e gratidão, à minha mãe, Lindete. Sem o seu incentivo e apoio não teria conseguido.

AGRADECIMENTOS

Primeiramente a Deus, que permitiu que eu chegasse até aqui.

Aos meus amados pais, Lindete Campos de Oliveira e Renato Vaz de Oliveira, pela força e confiança na realização dos meus sonhos.

Ao meu orientador, Prof. Jose Jailton pela orientação e paciência no desenvolvimento desse tralhado.

Ao meu co-orientador, Luiz Fernando, pela orientação e todos os ensinamentos passados.

Ao meu namorado, Neilson Junior, pelo incentivo e presença em todos os momentos difíceis.

As minhas amigas, Karine Araújo e Adrielle Veras, por sempre estarem disponíveis para as minhas dúvidas, que foram uma fonte inesgotável de ajuda durante todo o processo.

A meus amigos do trabalho, Ana Carolina e Nazareno Santiago pelo incentivo e apoio nessa trajetória.

E a todos que colaboraram direta ou indiretamente na execução desse trabalho.

RESUMO

Com o crescimento acelerado da rede mundial de computadores, ocasionado pelo grande número de hosts conectado, gerou a necessidade de mais endereços IP. Então, torna-se inevitável a utilização de um novo protocolo para resolver a escassez dos endereços IPv4. Desta forma, faz se necessário o uso do protocolo de endereçamento, o IPv6, tornando a solução para este problema e garantindo a continuidade do crescimento da internet. Sendo assim, o *Internet Protocol version* 6, visa suprir a escassez de endereços, pois possui uma faixa de endereçamento maior do que seu antecessor IPv4. Este trabalho tem como objetivo implementar e analisar o funcionamento de uma rede IPv6, explorando as funcionalidades dos protocolos DHCPv6, para o endereçamento dos hosts e o OSPFv3 para o roteamento na rede.

Palavras chaves: IPv6, DHCPv6.

ABSTRACT

With the accelerated growth of the worldwide computer network, caused by the large number of hosts connected, generated the need for more IP addresses. So it becomes inevitable to use a new protocol to solve the scarcity of IPv4 addresses. In this way, it makes necessary the use of the protocol of address, IPv6, making the solution to this problem and ensuring the continuity of the growth of the internet. Thus, the Internet Protocol version 6, to address the scarcity of addresses, has a range address bigger than its predecessor IPv4. This work aims to implement and analyze the operation of an IPv6 network, exploring the functionalities of DHCPv6 protocols, for the address of hosts and OSPFv3 for routing in the network.

Keywords: IPv6, DHCPv6.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

DARPA	Defense Advanced Research Projects Agency
IANA	Internet Assigned Numbers Authority
RIR	Registros Regionais de Internet
AFRINIC	African Network Information Centre
APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
LACNIC	Registro de Endereços da Internet para a América Latina e o Caribe
RIPE NCC	Réseaux IP Européens Network Coordination Centre
IETF	Internet Engineering Task Force
CIDR	Classless Inter Domain Routing
NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
RFC	Request for Comments
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol Version 6
OSPF	Open Shortest Path First
OSPFv3	Open Shortest Path First Version 6
LSA	Link State AdvertisementS
SPF	Shortest Path First
LSDB	Link State Data Base
AS	Sistema Autônomo
EVE-NG	Emulated Virtual Environment - Next Generation
WinSCP	Windows Secure CoPy
VNC	Virtual Network Computing
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol.
IGMP	Internet Group Management Protocol

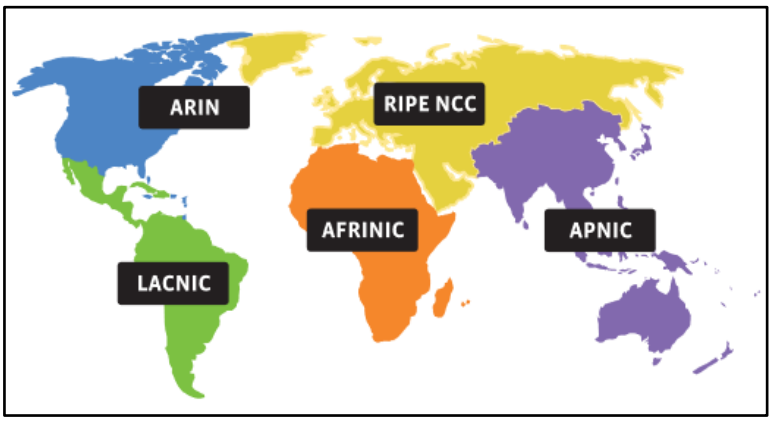
SUMÁRIO

1. Introdução

A rede mundial de computadores, mais conhecida como internet, hoje conecta bilhões de pessoas no mundo inteiro. Criada em meados de 1970, originalmente advinda de um projeto patrocinado pelo governo estadunidense , e que através da Agência de Projetos de Pesquisa Avançada de Defesa (*DARPA - Defense Advanced Research Projects Agency*), criaram a primeira rede, chamada ARPANET, assim dando início ao desenvolvimento da internet que hoje é formada pela interconexão de um grande número de redes.

Para que um dispositivo possa comunicar com outro, é necessário que o mesmo possua um endereço único, essa identificação é chamada de endereço IP. Dado que os endereços IP's não podem se repetir, existe uma estrutura para a distribuição de IP's, sendo formada por organizações que atuam de forma hierárquica para administrar os recursos. A gerência global dos IP's é realizada pela *Internet Assigned Numbers Authority* (IANA), a organização distribui grandes blocos de IP's para organizações regionais, chamadas de Registros Regionais de Internet (RIR), sendo eles, o AFRINIC (African Network Information Centre), na região da África, o APNIC (Asia-Pacific Network Information Centre), na região pacífica da Ásia, o ARIN (American Registry for Internet Numbers), no Canadá, EUA e algumas ilhas do Caribe, o LACNIC (Registro de Endereços da Internet para a América Latina e o Caribe), na América Latina e algumas ilhas do Caribe e o RIPE NCC (Réseaux IP Européens Network Coordination Centre), na Europa, Oriente Médio e Ásia Central, conforme apresentado na figura 1.

Figura 1. Registros Regionais de Internet



Fonte: IANA

Cada uma dessas organizações é responsável por definir as regras de distribuição dos endereços em sua respectiva área de atuação, e por implementá-las (Moreiras et.al, 2012, p.16). E no caso do Brasil temos o Núcleo de Informação e Coordenação do ponto BR (NIC.br) que é responsável pela distribuição de endereços IP.

O protocolo Internet (IP) é o responsável por identificar cada dispositivo presente na rede, por meio de números que chamamos de endereços, e por encapsular todos os dados que fluem através dela, agregando a eles informações suficientes para que cheguem a seus destinos (Moreiras et.al, 2012, p.8). Sendo assim é necessário que existam endereços IPs suficientes para todos os dispositivos que se conectam a internet.

A versão mais utilizada do IP é o *Internet Protocol Version 4* (IPv4), que se mostrou muito robusto e de fácil implementação, porém não foi previsto que o mesmo não suportaria a alta taxa de crescimento da internet e o seu possível esgotamento, e também o aumento da tabela de roteamento. Diante desse cenário, a IETF (*Internet Engineering Task Force*) passa a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e o problema do aumento da tabela de roteamento (Moreiras et.al, 2012, p.11). Sendo assim, algumas soluções tecnológicas foram adotadas para adiar o esgotamento dos endereços IPv4, sendo elas, CIDR (*Classless Inter Domain Routing*), NAT (*Network Address Translation*), Endereços privados e DHCP (*Dynamic Host Configuration Protocol*). Apesar que essas soluções não foram eficazes para suprir a necessidade por IP, que está diretamente ligada ao crescimento exponencial da internet.

Então foi criado uma nova versão do IP, *Internet Protocol Version 6* (IPv6). É considerado maduro o suficiente para suportar a operação da Internet na substituição do IPv4 (LACNIC,2019), desse modo assegurando a continuidade do crescimento da internet, visto como uma solução definitiva para o esgotamento do endereço IPv4. O IPv6 representa talvez a mudança mais importante na história da Internet uma vez que é necessária para que a rede de redes possa continuar sendo desenvolvida de forma segura e estável (LACNIC, 2019). Moreiras (2015, p.5) afirma que não é exagero dizer que o IPv6 é fundamental para a própria sobrevivência da Internet nos moldes em que a conhecemos atualmente.

Diante disso, surge a necessidade de estudar sobre as ferramentas que possam auxiliar no uso e atribuição de endereços aos hosts conectados em uma rede.

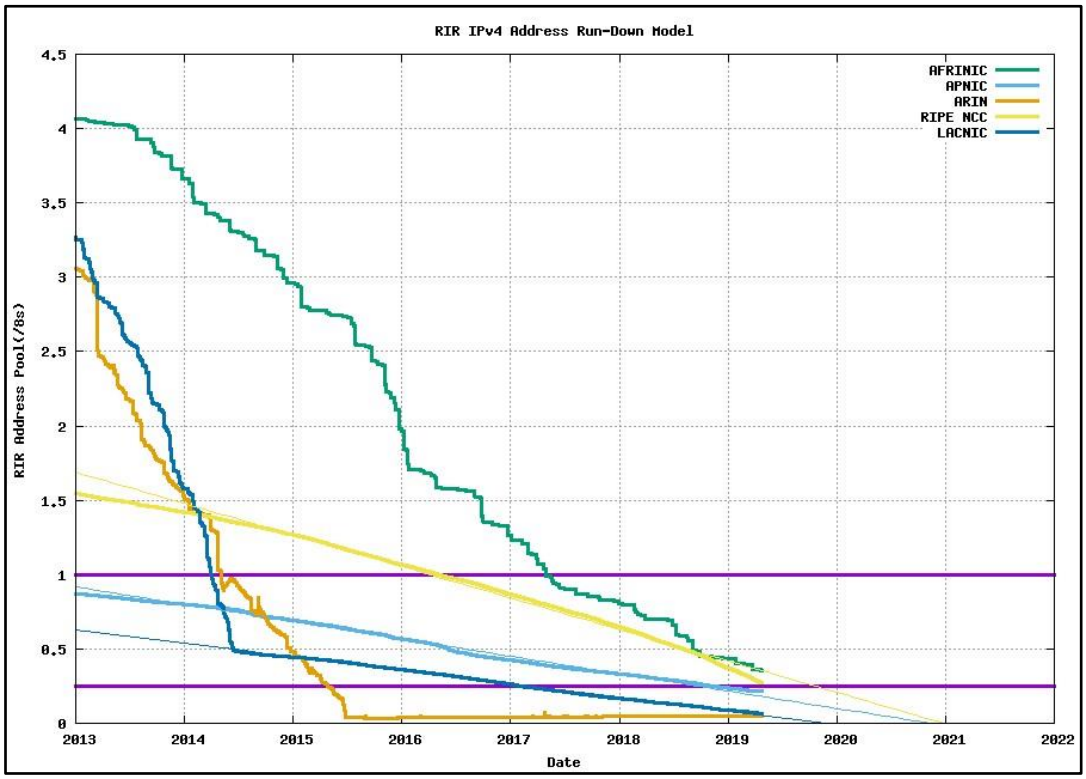
Nesta nova versão do protocolo, há a possibilidade de endereçamento pelo protocolo DHCPv6 (Dynamic Host Configuration Protocol for IPv6), é um protocolo de rede que opera somente por meio do protocolo IPv6 e distribui endereços IPv6, trabalha com duas modalidades, sendo elas, stateless e stateful.

1.1 Motivação e justificativa

Com a crescente quantidade de dispositivos que se conectam na rede mundial de computadores, surgiu a necessidade de um maior número de endereços ip na internet para atender de maneira eficiente as necessidades da constante evolução da internet.

O Ipv6.br informa que a previsão de esgotamento do IPv4 para endereços não alocados nos RIR, para ARIN e LACNIC no final de 2019, para APNIC no final de 2020 e para AFRINIC e RIPE NCC no início de 2021, conforme apresentado na figura 2.

Figura 2. Previsão de esgotamento nos RIR's

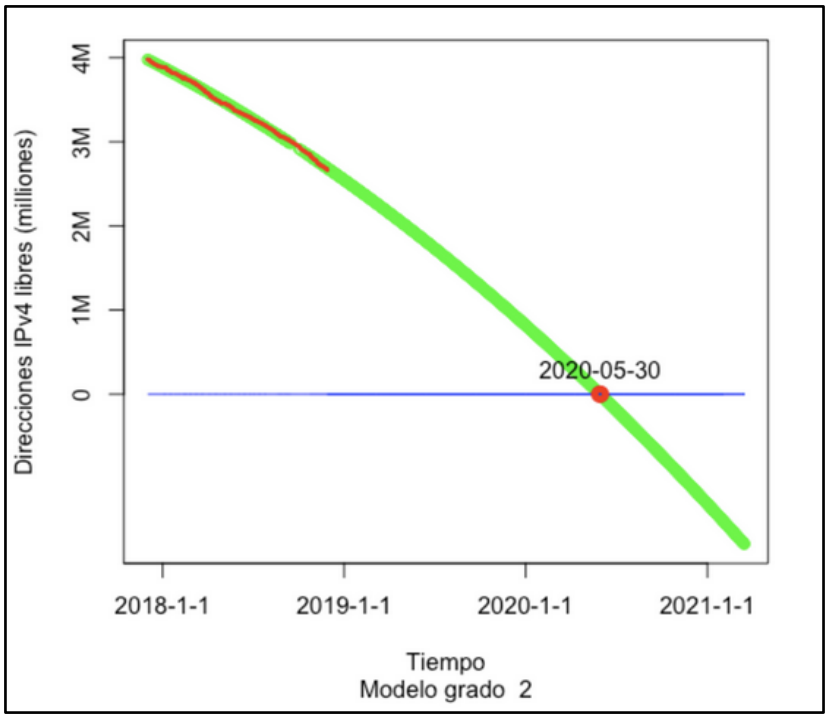


Fonte: ipv6.br,2019.

Segundo os dados do Registro de Endereçamento da Internet para a América Latina (LACNIC), levando em consideração o comportamento das alocações desde

fevereiro de 2017, afirma que a projeção para a possível data de esgotamento do endereço IPv4 e no ano de 2020. A figura 3 apresenta esses dados.

Figura 3. projeção de esgotamento



Fonte: LACNIC, 2019.

O IPv4 não foi projetado para suportar o crescimento de dispositivos conectados à Internet, então é necessário que haja a transição para o protocolo IPv6. Diante da situação, o presente estudo pretende expor os características e funcionalidades do protocolo IPv6, visto que a implantação ocorrerá em um futuro próximo, então se faz necessário um estudo do assunto.

1.2 Objetivo

Descrição dos objetivos geral e específicos que se pretende atingir com a realização desse trabalho.

1.2.1 Objetivo geral

O presente trabalho tem como objetivo principal ampliar os conhecimentos sobre as funcionalidades do protocolo IPv6, propondo a implementação em um ambiente simulado de uma rede IPv6 que faz uso dos protocolos DHCPv6 e OSPFv3.

1.2.2 Objetivos específicos

Os objetivos específicos deste trabalho são:

- Apresentar um estudo sobre o protocolo IPv6
- Demonstrar a importância do uso do endereçamento IPv6
- Descrever as etapas de configuração da topologia de Rede
- Proporcionar uma visão prática do uso e funcionamento do IPv6
- Demonstrar os resultados de conectividade do IPv6 da topologia de rede

1.3 Estrutura

A organização desse trabalho está segmentada em seções, a primeira é composta pelo referencial teórico no qual é abordado uma introdução sobre o protocolo IPv4, em que se faz necessário para uma melhor compreensão do IPv6 que é tratado em seguida. A segunda seção será apresentada os trabalhos correlatos. A terceira seção será abordada as tecnologias envolvidas e configurações realizadas para o desenvolvimento do trabalho, e logo depois os resultados obtidos e por último as conclusões do trabalho.

2. Referencial Teórico

Este capítulo aborda os conceitos fundamentais para o desenvolvimento e compreensão deste trabalho, bem como, a descrição dos protocolos IPv4 e IPv6, e também, os protocolos DHCP (*Dynamic Host Configuration Protocol)* na versão 6 e o OSPF (*Open Shortest Path First)* na versão 3.

2.1 Endereçamento IP (Internet Protocol)

A internet é formada por diversas redes que compõem a grande rede mundial de computadores, e cada dispositivo na internet recebe um endereço numérico único no mundo para identificá-lo. O endereço IP é o que permite que os pacotes de dados sejam enviados corretamente de uma rede para outra, desde o dispositivo de origem até alcançar seu destino final (Moreiras et.al, 2018, p.8). Há duas versões do endereço IP utilizadas hoje na Internet, primeiramente, será analisada a versão mais utilizada do IP, a versão 4, em seguida será analisada a versão 6 que foi proposta para substituir o IPv4.

2.2 IPv4

Definido na RFC 791, o protocolo IPv4 é o padrão pelo qual a internet funciona desde a sua criação, e significa Internet Protocol version 4, o mesmo possui endereçamento de 32 bits, que são divididos em quatro grupos de 8 bits cada, possibilitando gerar mais de 4 bilhões de endereços distintos, estes endereços são descritos em notação decimal onde cada byte é separado por um ponto.

2.2.1 Classes de endereçamento

Inicialmente, os endereços foram divididos em três classes de tamanhos fixos da seguinte forma:

- **Classe A:** definia o bit mais significativo como 0, utilizava os 7 bits restantes do primeiro octeto para identificar a rede, e os 24 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 1.0.0.0 até 126.0.0.0;

- **Classe B:** definia os 2 bits mais significativo como 10, utilizava os 14 bits seguintes para identificar a rede, e os 16 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 128.1.0.0 até 191.254.0.0;
- **Classe C:** definia os 3 bits mais significativo como 110, utilizava os 21 bits seguintes para identificar a rede, e os 8 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0;

Tabela 1: Classes de endereçamento IPv4.

ENDEREÇOS IP			
Classes	Número de End. por Rede	Intervalos de endereçamentos	Total de *Hosts*
Classe A	Até 256	0.0.0.0 até 127.0.0.0	Até 16.777.216
Classe B	Até 65.536	128.0.0.0 até 191.255.0.0	Até 65.536
Classe C	Até 16.777.216	192.0.0.0 até 223.255.255.0	Até 256

Fonte: MSDN - Microsoft.

Tanenbaum (2011, p.282) afirma que:

> Na época em que foi feita a decisão de criar as três classes, a Internet era uma rede de pesquisa conectando as principais universidades de pesquisa dos Estados Unidos, ninguém percebeu que a Internet se tornava um sistema de comunicação de mercado em massa.

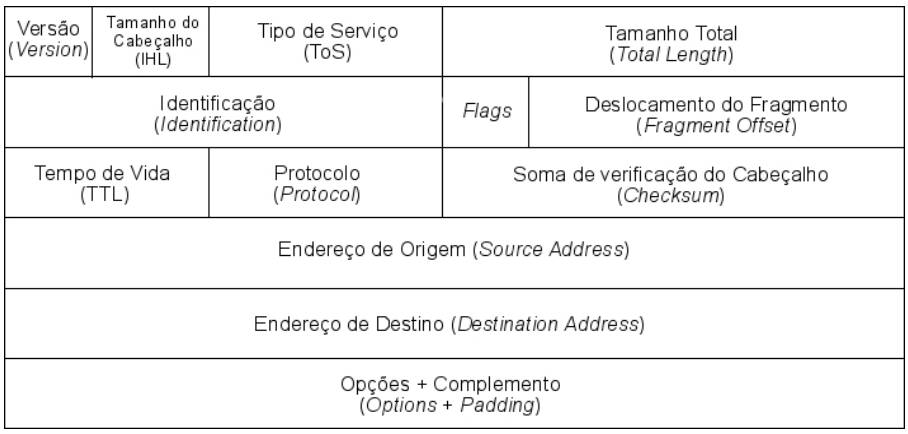
O intuito dessa divisão tenha era tornar a distribuição de endereços flexível, abrangendo redes de tamanhos variados, mas essa classificação mostrou-se na verdade rígida e muito ineficiente, levando a um grande desperdício de endereços (Moreiras et.al, 2012, p.10).

2.2.2 Cabeçalho IPv4

O cabeçalho IPv4 é composto por 12 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho varie de 20 a 60 Bytes. A figura 4 ilustra o formato do cabeçalho IPv4, os campos são destinados transmitir informações sobre:

- **Versão**: Esse campo determina a versão do protocolo IP utilizado.
- **Comprimento do cabeçalho**: Determina onde os dados do cabeçalho começam.
- **Tipo de serviço:** Estes bits estão incluídos no cabeçalho para poder diferenciar os diferentes tipos de datagramas IP que devem ser distinguidos uns dos outros.
- **Comprimento do datagrama**: Determina o comprimento total do datagrama IP, medido em bytes.
- **Identificador, flags, deslocamento de fragmentação:** Esses campos se referem a fragmentações que ocorreram no datagrama.
- **Tempo de vida**: Determina o tempo que o datagrama deve permanecer na rede, sendo decrementado cada vez que passar pelo roteador. Desta forma garante que o pacote não permaneça na rede infinitamente.
- **Protocolo**: o campo é usado somente quando um datagrama IP chega a seu destino final.
- **Soma de verificação do cabeçalho**: Auxilia um roteador na detecção de erros de bits em um datagrama IP recebido.
- **Endereço IP fonte e destino**: Nestes campos há o endereço de IP do remetente e o endereço IP do destinatário.
- **Opções**: Permite que um cabeçalho seja ampliado conforme a sua necessidade.

Figura 4. Cabeçalho IPv4



Fonte: ipv6.br

2.3 IPv6

Diante da previsão de esgotamento do endereçamento IPv4, no começo da década de 1990, a IETF iniciou um esforço para desenvolver o sucessor do protocolo. Uma motivação primária para esse esforço foi o entendimento de que o espaço de endereços IP de 32 bits estava começando a escassear, com novas sub-redes e nós IP sendo anexados à Internet a uma velocidade estonteante (Kurose, 2010, p.265).

Segundo Kurose (2010, p.265) os projetistas do IPv6 também aproveitaram essa oportunidade para ajustar e ampliar outros aspectos do IPv4 com base na experiência operacional acumulada sobre esse protocolo. O novo protocolo não foi criado somente para resolver a falta de endereços disponíveis, mas também para disponibilizar novos serviços e benefícios, dentre eles, podemos destacar o largo espaço de endereçamento, formato de cabeçalho simplificado para otimização de entrega de pacotes, suporte aos atuais protocolos de roteamento, entre outros benefícios.

2.3.1 Endereçamento IPv6

Definida pela RFC 2469, o IPv6 é a nova versão do Protocolo da Internet, possui um espaço de endereçamento de 128 bits, sendo possível obter aproximadamente 340 undecilhões de endereços distintos. Este valor representa aproximadamente 79 octilhões (7,9x1028) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões (5,6x1028) de endereços por ser humano na Terra (Moreiras et.al, 2012, p.33).

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais (0-F), por exemplo:

- 2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

E possível utilizar tanto caracteres maiúsculos quanto minúsculos no endereço IPv6, e também, regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequência longa de zeros por “::”.

É importante ressaltar que o IPv6 não é um complemento do IPv4, ou seja, os protocolos não são compatíveis. O protocolo IPv6 é o substituto do IPv4, criado para resolver os problemas do IPv4, como a carência de endereços IP, podendo os dois funcionarem paralelamente com a ajuda de mecanismos de transição.

2.3.2 Tipos de endereços IPv6

Conforme Moreiras et al. (2012, p.34) existem no IPv6 três tipos de endereços definidos:

- **Unicast** – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface.
- **Anycast** – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos.
- **Multicast** – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos.

2.3.3 Cabeçalho IPv6

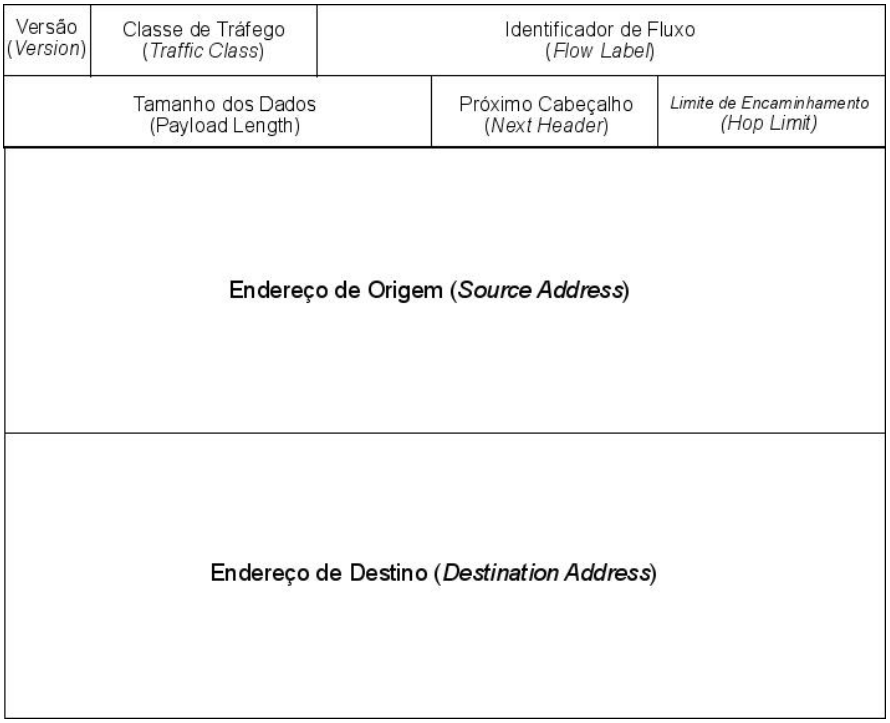
Algumas mudanças foram realizadas no formato do cabeçalho base do IPv6 de modo a torná-lo mais simples. O cabeçalho é mais simplificado, contém somente sete campos, ao contrário do IPv4 que possui treze e o tamanho foi fixado de 40 Bytes. Além disso, ele ficou mais flexível e eficiente com a adição de cabeçalhos de extensão que não precisam ser processados por roteadores intermediários (Moreiras et.al, 2012, p.24).

Conforme Moreiras et al. (2012, p.27) o cabeçalho do IPv6 está dividido nos seguintes campos:

- **Versão**: Identifica a versão do protocolo utilizado.

- **Classe de Tráfego:** Identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço do IPv4″
- **Identificador de Fluxo:** Identifica pacotes do mesmo fluxo de comunicação.
- **Tamanho do Dados:** Indica o tamanho, em Bytes, apenas dos dados enviados junto ao cabeçalho IPv6, o tamanho dos cabeçalhos de extensão também é somado nesse novo campo.
- **Próximo Cabeçalho:** Identifica o cabeçalho de extensão que segue o atual.
- **Limite de Encaminhamento:** Esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes

Figura 5. Cabeçalho Ipv6



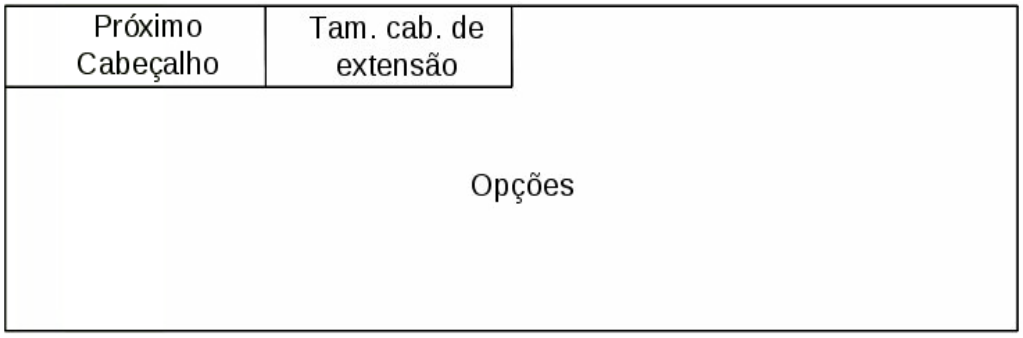
Fonte: ipv6.br

2.3.4 Cabeçalho de Extensão

Diferente do IPv4, que inclui no cabeçalho base todas as informações opcionais, o IPv6 trata essas informações através de cabeçalhos de extensão. Segundo Tanenbaum (2011, p.288) esses cabeçalhos podem ser criados com a

finalidade de oferecer informações extras, desde que elas sejam codificadas de maneira eficiente. A figura 6 demonstra o template de um cabeçalho de extensão.

Figura 6. Template do cabeçalho de extensão



Fonte: ipv6.br

As especificações do IPv6 definem seis cabeçalhos de extensão, mostrados na tabela 2.

Tabela 2. Cabeçalhos de extensão

Cabeçalho de extensão	**Descrição**
Hop-by-hop options	Informações diversas para os roteadores
Destination options	Informações adicionais para o destino
Routing	Lista parcial de roteadores a visitar
Fragmentation	Gerenciamento de fragmentos de datagramas
Authentication	Verificação da identidade do transmissor
Encrypet security payload	Informações sobre o conteúdo criptografado

Fonte: Tanenbaum, 2011

De acordo com Moreiras et al. (2012, p.28):

> A criação dos cabeçalhos de extensão do IPv6 teve a finalidade de aumentar a velocidade de processamento nos roteadores, visto que o único que deve ser processado em cada roteador é o Hop-by-Hop, enquanto que os demais são tratados apenas pelo nó de destino. Além disso, novos cabeçalhos podem ser definidos no protocolo sem a necessidade alterações no cabeçalho base.

2.4 ICMP

O ICMP (Internet Control Message Protocol) é um protocolo integrante do Protocolo IP**,** especificado pela RFC 792, é utilizado para detectar e relatar condições de erro a fonte original. Quando acontece algo inesperado durante o processamento do pacote em um roteador, o evento é relatado ao transmissor pelo ICMP (Tanenbaum, 2011, p. 291).

Segundo Tanenbaum (2011, p. 291) cerca de 12 tipos de mensagens de ICMP são definidos, sendo transportada e encapsulada dentro de um pacote IP. As mensagens mais importantes constam na tabela 3.

Tabela 3. Mensagens ICMP

Tipo de Mensagem	**Descrição**
Destination unreachable	O pacote não pode ser entregue
Time exceeded	O campo TTL atingiu 0
Parameter problem	Campos de cabeçalho inválido
Source quench	Restringe o envio de pacotes
Redirect	Ensina uma rota a um roteador
Echo e Echp reply	Verificam se uma máquina está ativa
Timestamp request/reply	O mesmo que Echo, mas com registro de tempo
Router advertisement/solicitation	Encontra um roteador próximo

Fonte: Tanenbaum, 2011

2.4.1 ICMPv6

Internet Control Message Protocol Version 6 (ICMPv6) é definido pela RFC 4443, é uma versão atualizada do protocolo ICMP para ser utilizada em conjunto com o IPv6. O mecanismo é considerado uma parte obrigatória do IP e precisa ser incluído em toda implementação IP (Comer, 2015, p.114). Sua implementação, portanto, é obrigatória em todos os nós da rede que utilizam IPv6 para se comunicar.

O ICMPv6 assume funções de outros protocolos, que existem isoladamente no IPv4. Segundo Moreiras et al. (2012, p.43) os protocolos usados no IPv4, que não existem mais no IPv6, cujas funcionalidades foram agregadas pelo ICMPv6, são**:**

- **ARP (*Address Resolution Protocol*)**: cujo o objetivo é mapear os endereços fisicos através dos endereços lógicos.
- **RARP (*Reverse Address Resolution Protocol*)**: que realiza o inverso do ARP, mapeando os endereços lógicos para endereços fisicos.
- **IGMP (*Internet Group Management Protocol*)**: que atua com o gerenciamento de membros de grupos multicast.

Tal mudança foi projetada com o simples intuito de reduzir a multiplicidade de protocolos, que é prejudicial por piorar a coerência e aumentar o tamanho das implementações (Moreiras et al,2012, p.43). Deve-se ter em mente que, de forma geral, o ICMPv6 é muito mais importante para o funcionamento do IPv6, do que o ICMP é para o funcionamento do IPv4.

2.5 DHCP

O *Dynamic Host Configuration Protocol* (DHCP) descrito nas RFCs 2131 e 2132, é um protocolo utilizado para distribuir dinamicamente endereços IP e parâmetros de configuração da rede (Moreiras et al,2015, p.51). O protocolo ajuda na configuração automática dos endereços, facilitando bastante o trabalho dos administradores de rede.

Póvoa (2016), informa que:

> O DHCP evita que endereços duplicados sejam inseridos por conta de algum erro manual e fornece para o usuário, de forma transparente, a configuração necessária para que os dispositivos possuam conectividade com a rede local automaticamente.

Segundo Moreiras et.al (2015, p.52) basicamente, a comunicação entre o servidor DHCP e as máquinas cliente se dá com a troca de quatro mensagens:

- ***Solicit***: enviada pelo cliente ao grupo *multicast all-dhcp-agents* (ff02::1:2) com o intuito de localizar o servidor DHCP.

- ***Advertise***: enviada pelo servidor DHCP, diretamente ao endereço *link-local* do cliente, para indicar que ele pode fornecer as informações necessárias para a configuração.
- ***Request***: enviada pelo cliente diretamente ao grupo *multicast all-dhcp-agents* (ff02::1:2) para requisitar ao servidor DHCP os dados de configuração.
- ***Reply***: enviada pelo servidor DHCP ao endereço de *link-local* do cliente como resposta à mensagem *Request*.

2.5.1 DHCPv6: Stateful e Stateless

O DHCPv6 é o protocolo DHCP para endereços IPv6 e trabalha em duas modalidades:

- ***Stateful***: o servidor DHCPv6 é responsável por informar aos clientes os endereços IPv6 que devem ser utilizados em suas interfaces de rede, mantendo o estado de qual endereço foi atribuído a determinado cliente.
- ***Stateless***: o servidor DHCPv6 informa apenas parâmetros de configuração como endereço dos servidores DNS ou servidores SIP da rede aos clientes, sem a necessidade de guardar qual informação individual de cada cliente. Nesse segundo caso, o cliente deverá obter o endereço IPv6 de sua interface de outra forma, seja manualmente ou SLAAC[1] (*Stateless Address Autoconfiguration*).

O DHCPv6 stateful é a portabilidade exata do DHCP no mundo do IPv6. Com essa abordagem, um identificador de servidor DHCPv6 concede informações extras, assim como o tradicional IPv4 DHCP (Maggio). Este trabalho tem foco no modo de operação do DHCPv6 stateful.

2.6 OSPF

O *Open Shortest Path First* (OSPF) definido na RFC 2328, usado no interior de um sistema autônomo (AS), é um protocolo responsável por encaminhar os pacotes de rede pelo melhor caminho possível. Segundo Comer (2015, p. 206) o protocolo

[1] É a maneira mais simples de fornecer um endereço IPv6 a um host

utiliza uma técnica de roteamento de estado de link (*Link State Advertisements)*, que usa um algoritmo gráfico SPF[2] (*Shortest Path First*) para calcular os caminhos mais curtos.

Bendjouya et. al (2012, p. 4) informa que o protocolo OSPF possui recursos que podem ser divididos em três categorias:

- Primeira: os roteadores formam uma relação de vizinhos que fornece a base para toda a comunicação continua do OSPF.
- Segunda: Depois que os roteadores se tornam vizinhos, eles trocam o conteúdo de seus respectivos LSDB (Link State Data Base - Banco de Dados Link-State). Cada roteador usa LSAs para construir o LSDB.
- Terceira: Assim que um roteador tem as informações de topologia em seu LSDB ele utiliza o algoritmo SPF para calcular as melhores rotas atuais e acrescenta-las à tabela de roteamento IP.

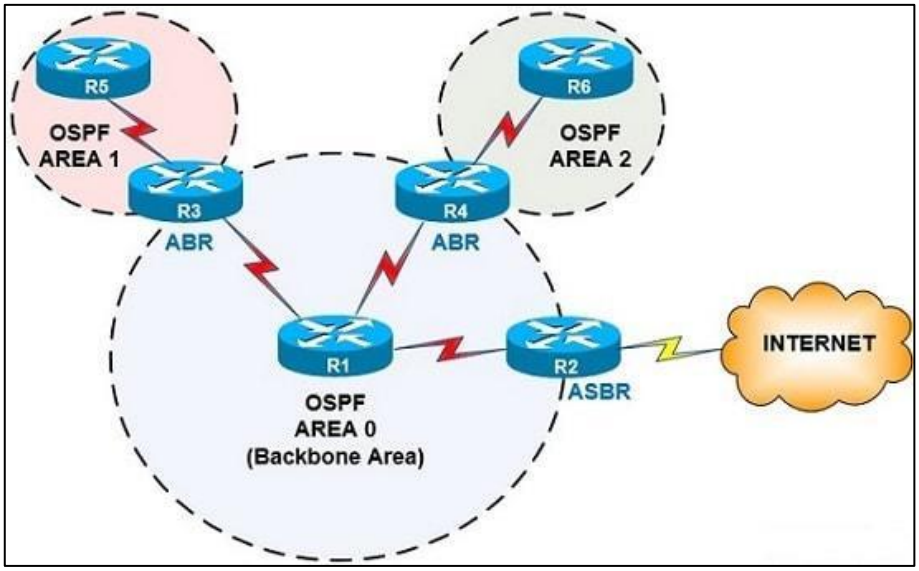
Segundo a RNP (2012) para melhor distribuir as tabelas de roteamento, o protocolo OSPF implementa o conceito de "Área":

> Uma rede pode ser dividida em diversas áreas. Cada área contém seus próprios roteadores e sua própria rede. Quando várias áreas são configuradas em uma mesmo AS, uma delas é chamada de *backbone* e o seu identificador é zero (área 0). O *backbone* é a área central e as outras áreas devem ser conectadas a ela através de roteadores, chamados de roteadores de borda de área (ABR). As informações de roteamento são enviadas para os roteadores no backbone, que propagam as informações para os roteadores nas bordas das áreas e assim por diante.

Na figura 7 tem-se um exemplo de uma topologia OSPF dividida em áreas:

[2] Também chamado de algoritmo de Dijkstra

Figura 7. Topologia OSPF



Fonte: Faq informatica, 2017

2.6.1 OSPFv3

Definido na RFC 2740, o protocolo OSPFv3 fornece suporte para o protocolo IPv6, é uma versão atualizada do OSPF. As duas versões do protocolo OSPF operam independentemente umas das outras, em bancos de dados separados. Não há compatibilidade com versões anteriores do OSPFv3 para o OSPF.

3. Trabalhos correlatos

Durante o levantamento dos trabalhos correlatos foram encontradas poucas pesquisas que abordam a temática semelhante à apresentada neste trabalho. Os trabalhos selecionados com a presente monografia foram elaborados no ano de 2014 e 2016.

Como a proposta do trabalho é a implementação de uma rede de computadores utilizando o protocolo IPv6, fazendo uso dos protocolos DHCPv6 e OSPFv3 em um ambiente de simulação, a partir do contexto, foram selecionados três trabalhos relacionados que serão expostos nos tópicos seguintes.

3.1 Redes de computadores usando IPv6 com protocolo DHCPv6

Araújo et al. (2014) concentram seu estudo em esclarecer conceitos básicos de aplicação de IPv6 em uma rede LAN utilizando o protocolo DHCP, para o endereçamento dos hosts. Os conceitos foram apresentados e aplicados em uma simulação realizada no *Cisco Packet Tracer,* onde foi criada uma topologia de rede, contendo 30 computadores conectados a dois switches e a um roteador com sua interface configurada em DHCPv6. Os autores relatam que é de suma importância a correta implementação da rede simulada e resolução de problemas para a configuração da mesma para que em um caso futuro possa ser usado como experiencia profissional de vivencia pratica em uma aplicação real em empresas.

No desenvolvimento do trabalho, foi utilizada uma metodologia de pesquisa conhecida como PDCA (Planejar, Executar, Verificar, Ajustar), trata-se de um ciclo de melhoria continua que tem como foco um constante planejamento e observação dos resultados dentro de um processo.

Para a realização desse trabalho os autores informam que foi necessário um maior conhecimento tanto no protocolo IPv6 quanto no protocolo DHCP, e concluíram que para replicação do trabalho no mundo real será necessário a colaboração de várias pessoas da área de tecnologia, pois a rede proposta e extremamente grande e com várias peculiaridades.

Esse trabalho possui grande semelhança com o trabalho proposto nessa monografia, os dois realizam a implementação de uma rede IPv6 em um ambiente

simulado, a diferença e que cada trabalho usa uma ferramenta de simulação diferente, e também a monografia explora o uso do protocolo de roteamento OSPFv3.

3.2 Implementação de IPv6 em um provedor de internet

Santos (2016) apresenta a implantação do protocolo IPv6 em um provedor de conexão, utilizando a técnica de pilha dupla, funcionando paralelo ao protocolo IPv4 sem interromper a operação da rede. Alguns requisitos foram necessários para a implementação, como, um plano de endereçamento, serviço de BGP para o roteamento da rede dinamicamente, servidores DNS que suportam requisições Quad-A e autenticação dos clientes para a entrega do endereço utilizando o DHCPv6. Para a implementação foi utilizado os protocolos BGP4 e OSPFv3, ambos para que seja possível a implementação do IPv6.

Os resultados do trabalho foram obtidos através do levantamento de tabelas de roteamento do roteador principal, das rotas do BGP e OSPF, verificação da aquisição de endereços IPv6, teste de conectividade (ping), teste de traceroute, navegação web utilizando endereço IPv6. Todos os testes foram realizados com os endereços reais. O autor relata que a proposta foi realizada com sucesso, visto que uma rede que comunicava unicamente em IPv4, foi transformada em uma rede pilha dupla, com comunicação transparente ao usuário. Santos concluiu que a documentação do processo, tem aumentado e facilitado a implementação do protocolo IPv6.

Diferente da proposta desta monografia, Santos propõe a implementação em um ambiente real, um provedor de conexão, e também fazendo uso dos protocolos explorados, o DHCPv6 e OSPFv3.

3.3 Implantação de uma rede utilizando os padrões do protocolo IPv6

Pedrozo (2014) propõe a implantação de uma rede IPv6 fazendo a utilização de um túnel para que a partir dele possa ser feita a comunicação via internet IPv4. As técnicas de tunelamento utilizadas, foram, *Tunnel Broker, Tunnel 6over4 e Tunnel GRE.* O cenário proposto pela autora simula um ambiente de rede contendo hosts atuando como clientes em uma rede IPv6, onde nesta rede implementada existe um servidor DHCP, um servidor DNS e um servidor de túnel. Os hosts foram emulados

em maquinas virtuais, contendo interfaces em IPv4 e IPv6 interligados a internet IPv4, e com o túnel ativo à internet IPv6.

Para obtenção dos resultados, foi realizado testes para validar o funcionamento dos tuneis. A validação do *Tunnel Broker* foi realizada através da comunicação com a internet via protocolo IPv6. E a *Tunnel 6over4* foi comprovada por meio da analisa dos pacotes recebidos no host destinatário. E por último, o *Tunnel GRE* onde foi verificado a conectividade entre dois hosts do túnel. A autora conclui que a técnica de tunelamento *Tunnel Broker* se apresentou como a solução para o problema proposto no estudo.

A proposta de Pedrozo segue uma vertente um pouco deferente, pois propõe a implementação de uma rede IPv6 utilizando técnicas de transição, o tunelamento.

Os trabalhos apresentados se tratam dos que mais se assemelham ao presente trabalho por abordarem questões similares, tal como a implementação de uma rede utilizando o protocolo IPv6.

4. Metodologia

A simulação é um recurso de extrema importância, utilizada para analisar uma rede real modelando o seu funcionamento e analisando o comportamento de tal, também podendo modificá-la e isolar parâmetros e extrair informações de interesse.

O seguinte trabalho foi realizado com o intuito de apresentar na prática o funcionamento de uma rede que faz uso do protocolo IPv6 e de seus recursos para implantação, para isso foi utilizado o emulador EVE-NG, que possibilita a configuração dos dispositivos emulado como se estivesse conectado a um dispositivo físico, assim gerando um ambiente em produção.

4.1 Ambiente de simulação

A simulação apresentada foi realizada com o auxílio do EVE-NG (Emulated Virtual Environment - Next Generation) é a versão mais recente da plataforma UnetLab, é uma ferramenta gratuita que permite a criação de cenários de redes utilizando imagens de dispositivos de diversos fabricantes. A lista de fabricantes que é possível emular no EVE-NG são, Cisco, Juniper, HP, Mikrotik, Fortinet, Palo Alto, Aruba, entre outros. A plataforma tem a vantagem de proporcionar que os laboratórios possam ser realizados através do navegador.

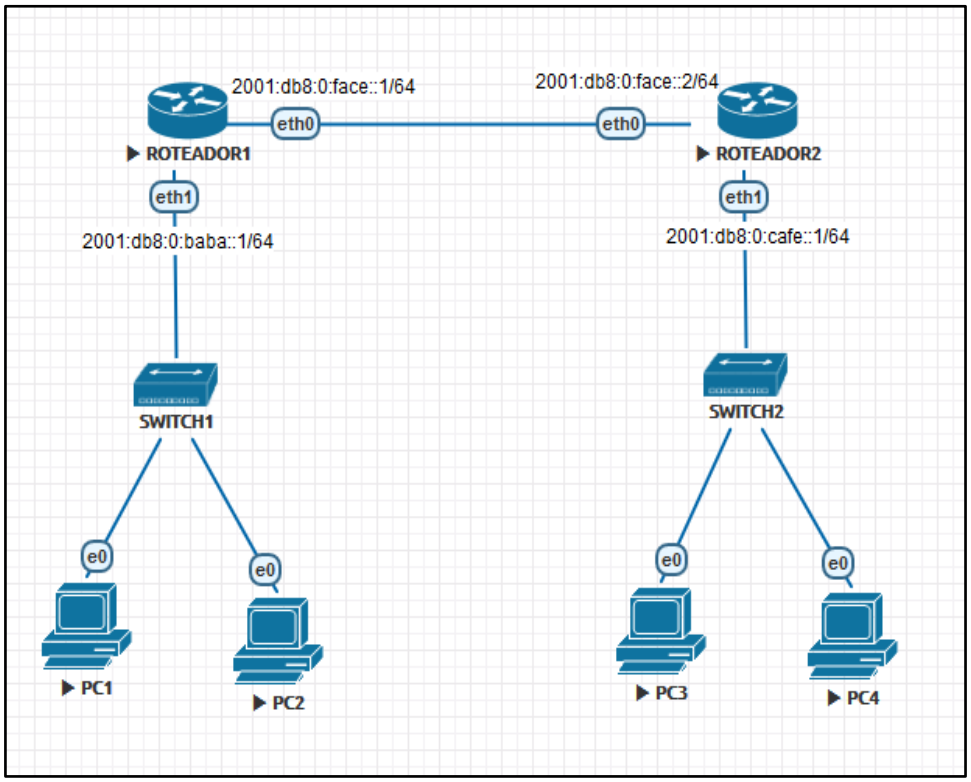
Para a execução da plataforma EVE-NG foi utilizada a máquina virtual VMware Workstation Player, o software permite a instalação e utilização de um sistema operacional dentro de outro dando suporte real a software de outros sistemas operativos. As imagens de dispositivos usadas no EVE-NG foram transferidas com a ajuda da ferramenta WinSCP (Windows Secure CoPy), sua função e a transferência de arquivos entre um computador local e um remoto. Os dispositivos na topologia de rede, foram acessados pelo VNC (Virtual Network Computing) é um sistema que permite conectar-se a um computador remotamente. Essas foram as ferramentas necessárias para a realização do trabalho.

4.2 Descrição do cenário

Para a simulação foi criada uma topologia de rede composta por dois roteadores com o sistema operacional de rede Vyos baseado em Debian Linux, fornecendo roteamento de rede baseado em software. e também dois switches e quatro computadores com o sistema operacional Linux CentOS 7, sendo uma distribuição Linux conhecida pelo seu alto nível de estabilidade, previsibilidade e pela possibilidade de ser configurada de múltiplas maneiras. Os sistemas operacionais devem ser associados aos dispositivos no EVE-NG.

Os ativos da rede estão identificados como ROTEADOR1 e ROTEADOR2, sendo eles, responsáveis por informar a rota por meio do protocolo de roteamento OSPFv3 e também atribuir o endereço IPv6 aos hosts conectados por meio do protocolo DHCPv6. Os switches estão identificados como SWITCH1 E SWITCH2 e os hosts como PC1, PC2, PC3 e PC4. A figura 8 esboça o cenário da topologia de rede.

Figura 8. Topologia de rede



Fonte: Autoria própria

A comunicação entre o ROTEADOR1 E O ROTEADOR2 ocorre graças ao protocolo de roteamento interno OSPFv3, que permite aos roteadores a troca de informações sobre as rotas que conhecem, a topologia de rede deste trabalho propõe apenas uma rota entre os roteadores, com o propósito de demonstrar o funcionamento do protocolo e que irá consequentemente possibilitar a comunicação entre os hosts na rede, ou seja, os hosts PC1 e PC2 conseguem ter comunicação com os hosts PC3 e PC4. Cada roteador também será responsável por executar o serviço DHCPv6, que foi configurado no modo stateful, com a função de atribuir um endereço IPv6 aos hosts conectados, mantendo um registro de informação de qual endereço foi atribuído a determinado host.

As configurações realizadas nos equipamentos da rede, serão expostos nos tópicos seguintes.

4.3 Roteiro experimental

Depois de obter as imagens necessárias para a criação da rede e agrupar os equipamentos e interliga-los foram realizadas as configurações nos roteadores 1 e 2.

4.3.1 Configuração da rota no roteador 1

As configurações realizadas no roteador 1 para criação da rota entre os roteadores que estão diretamente conectadas, foram as seguintes:

(a) Atribuição do IP na interface eth0 e eth1:

```
# set interfaces ethernet eth0 address '2001:db8:0:face::1/64'
# set interfaces ethernet eth1 address '2001:db8:0:baba::1/64'
```

(b) Criação do identificador único para permitir o uso do OSPFv3:

```
# set interfaces loopback 'lo'
```

(c) Ativação do OSPFv3 na eth0 e adição dessa interface na área 0.0.0.0 :

```
#  set protocols ospfv3 area 0.0.0.0 interface 'eth0'
```

(d) Adicionando um número de 32 bits para identificar o roteador 1:

```
#  set protocols ospfv3 parameters router-id '10.255.1.0'
```

(e) Comando utilizado para que o roteador divulgue as rotas diretamente conectadas:

```
#  set protocols ospfv3 redistribute 'connected'
```

4.3.2 Configuração do servidor DHCPv6 no roteador 1

As configurações realizadas para criar o servidor DHCP no roteador 1, segue abaixo:

(a) Comando utilizado para detectar endereços duplicados na rede, o processo realizado sempre que um novo endereço é atribuído a uma interface:

```
#  set interfaces ethernet eth1 ipv6 dup-addr-detect-transmits '1'
```

(b) Comando utilizado para informar via RA[3] (Router Advertisement) para os outros roteadores não realizarem a autoconfiguração (SLAAC) porque na rede encontra-se um servidor DHCP:

```
#  set interfaces ethernet eth1 ipv6 router-advert managed-flag 'true'
```

(c) Realização do anúncio do roteador (Router Advertisement) na rede:

```
#  set interfaces ethernet eth1 ipv6 router-advert send-advert 'true'
```

[3] Mensagem de anuncio de roteador

(d) Criação do servidor DHCP, informando também o prefixo que será utilizado na rede:

```
# set service dhcpv6-server shared-network-name LAN subnet 2001:db8:0:baba::/64 address-range prefix '2001:db8:0:baba::/64'
```

(e) Comando utilizado para informar o range da rede:

```
# set service dhcpv6-server shared-network-name LAN subnet 2001:db8:0:baba::/64 address-range start 2001:db8:0:baba::1000 stop '2001:db8:0:baba::ffff'
```

(f) Comando utilizado para informar o DNS da rede:

```
# set service dhcpv6-server shared-network-name LAN subnet 2001:db8:0:baba::/64 name-server '2001:db8:0:baba::bb'
```

4.3.3 Configuração da rota no roteador 2

As configurações realizadas no roteador 2 para criação da rota entre os roteadores que estão diretamente conectadas, foram as seguintes:

(a) Atribuição de ip na interface eth0 e eth1:

```
# set interfaces ethernet eth0 address '2001:db8:0:face::2/64
# set interfaces ethernet eth1 address '2001:db8:0:cafe::1/64'
```

(b) Criação de uma interface para permitir o uso do OSPFv3:

```
# set interfaces loopback 'lo'
```

(c) Ativação do OSPFv3 na eth0 e adição dessa interface na área 0.0.0.0 :

```
# set protocols ospfv3 area 0.0.0.0 interface 'eth0'
```

(d) Adicionando um número de 32 bits para identificar o roteador 2:

```
# set protocols ospfv3 parameters router-id '10.255.2.0'
```

(e) Comando utilizado para que o roteador divulgue as rotas diretamente conectadas:

```
# set protocols ospfv3 redistribute 'connected'
```

4.3.4 Configuração do servidor DHCPv6 no roteador 2

As configurações realizadas para criar o servidor DHCP no roteador 2, segue abaixo:

(a) Detecção de endereços duplicados na rede:

```
# set interfaces ethernet eth1 ipv6 dup-addr-detect-transmits '1'
```

(b) Comando utilizado para informar via RA (Router Advertisement) para os outros roteadores não realizarem a autoconfiguração (SLAAC) porque na rede encontra-se um servidor DHCP:

```
# set interfaces ethernet eth1 ipv6 router-advert managed-flag 'true'
```

(c) Anúncio do roteador (Router Advertisement) na rede:

```
# set interfaces ethernet eth1 ipv6 router-advert send-advert 'true'
```

(d) Comando utilizado para realizar a criação do servidor DHCP, informando também o prefixo que será utilizado na rede:

```
# set service dhcpv6-server shared-network-name LAN subnet 2001:db8:0:cafe::/64 address-range prefix '2001:db8:0:cafe::/64'
```

(e) Comando utilizado para informar o range da rede:

set service dhcpv6-server shared-network-name LAN subnet 2001:db8:0:cafe::/64 address-range start 2001:db8:0:cafe::1000 stop '2001:db8:0:cafe::ffff'

(f) Comando utilizado para informar o DNS da rede:

set service dhcpv6-server shared-network-name LAN subnet 2001:db8:0:cafe::/64 name-server '2001:db8:0:cafe::bb'

5. Análise dos resultados

Nessa seção são apresentados os resultados obtidos através da análise da conectividade entre os equipamentos na rede, a fim de validar o funcionamento da rota e do servidor DHCPv6 configurados. Os procedimentos realizados para validação das funcionalidades na rede, foram, a verificação de IP, testes de ping e traceroute. Os resultados serão expostos nos itens seguintes.

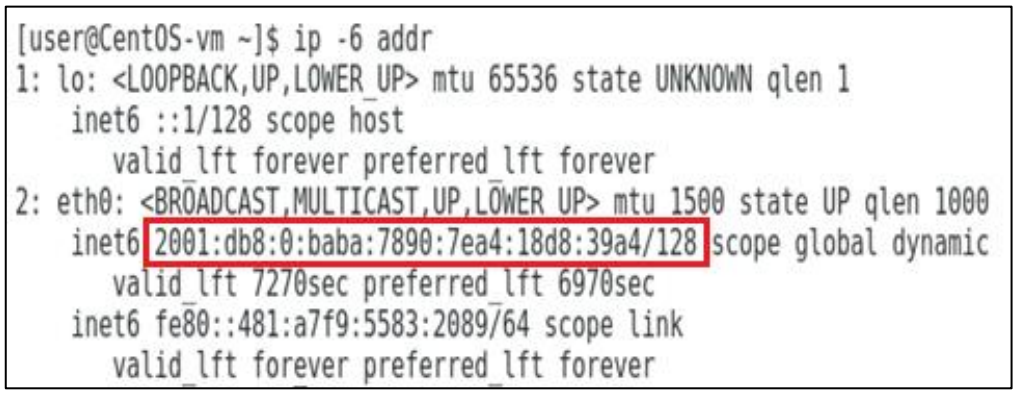
5.1 Verificação de concessão de IP

A verificação de concessão de endereço IPv6, foi realizada com a finalidade de corroborar o funcionamento do servidor DHCPv6, sendo responsável por distribuir endereços e parâmetros de rede as máquinas na rede. Nos terminais PC1, PC2, PC3 e PC4 foram realizadas as verificações de concessão de IP por parte dos roteadores na rede, o seguinte comando foi utilizado:

```
# ip -6 addr
```

No terminal PC1, o resultado do comando e representado na figura 9. Note o endereço IPv6 obtido.

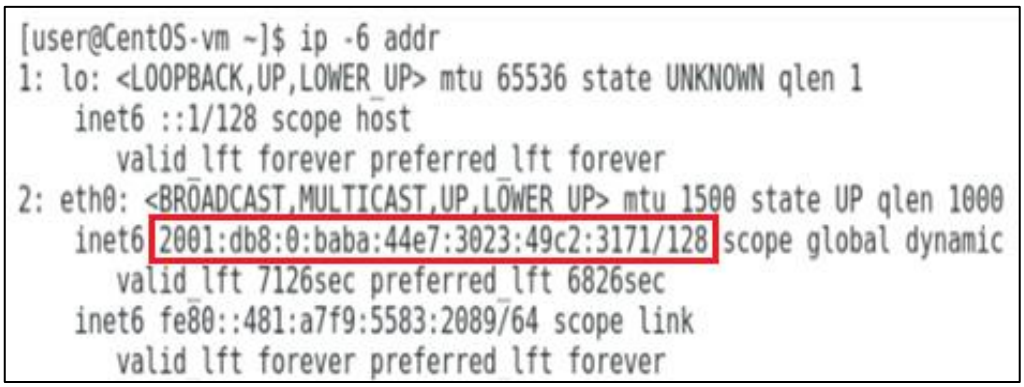
Figura 9. Endereço IPv6 no PC1



Fonte: Autoria própria

No terminal PC2 também foi realizada a verificação de IP, como representado na figura 10.

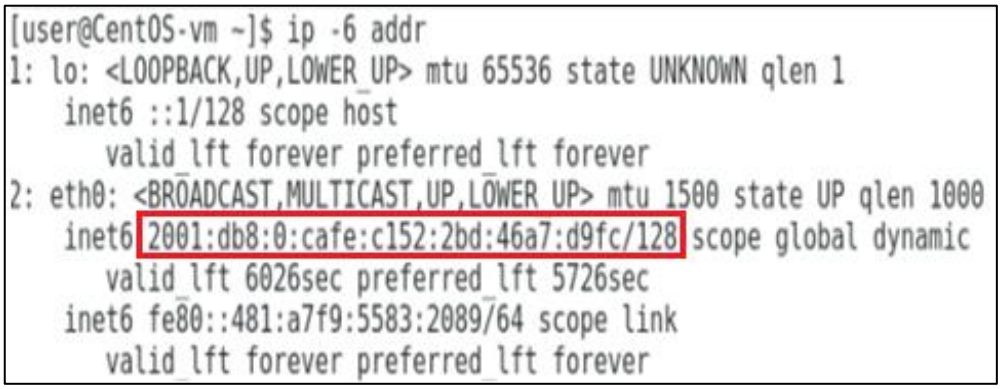
Figura 10. Endereço IPv6 no PC2



Fonte: Autoria própria

No terminal PC3 foi realizada a verificação de IP, como representado na figura 11.

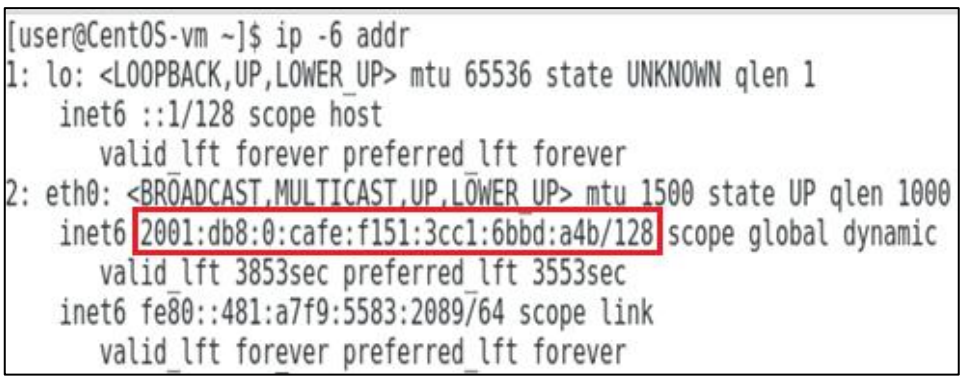
Figura 11. Endereço IPv6 no PC3



Fonte: Autoria própria

No terminal PC4 foi realizada a verificação de IP, como representado na figura 12.

Figura 12. Endereço IPv6 no PC4



Fonte: Autoria própria

As verificações de concessão de IP realizadas nos terminais PC1, PC2, PC3 e PC4 comprovaram o funcionamento do serviço DHCPv6, sendo responsável pela alocação automática de endereços IPv6 para os hosts na rede.

5.2 Teste de conectividade – ping

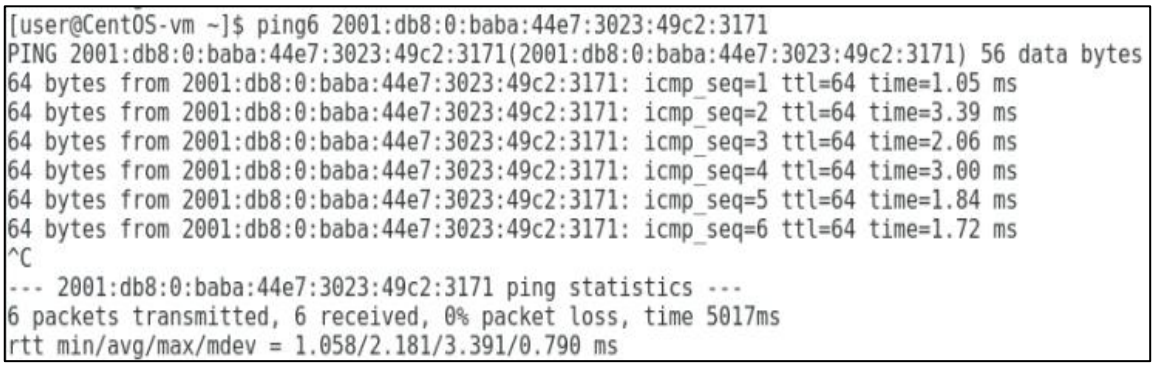
A palavra "ping" é a abreviação do termo em inglês "Packet Internet Network Grouper", que significa algo como "Agrupador de Pacotes da Internet". O ping é um teste que serve para avaliar a conectividade entre dois pontos da rede. O resultado é dado em uma unidade de tempo, geralmente de alguns milissegundos. Quanto maior o valor do PING, mais lenta é a transmissão de informações dentro daquela rede (Gomes, 2018).

O teste de ping tem como objetivo expor a conectividade entre os terminais, desta forma, sendo comprovado com o resultado dos testes. O comando abaixo foi utilizado para os testes de conectividade:

```
# ping6
```

O primeiro teste de ping foi realizado no terminal PC1 para o terminal PC2, conforme a figura 13, e possível verificar que houve conexão entre os terminais.

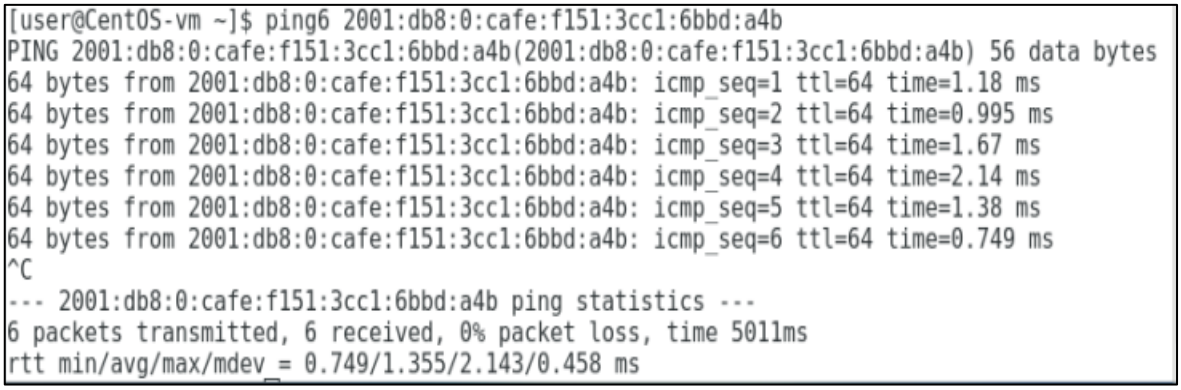
Figura 13. Teste de ping PC1 para PC2



Fonte: Autoria própria

O comando foi executado no terminal PC3 para o terminal PC4, como demonstra na figura 14.

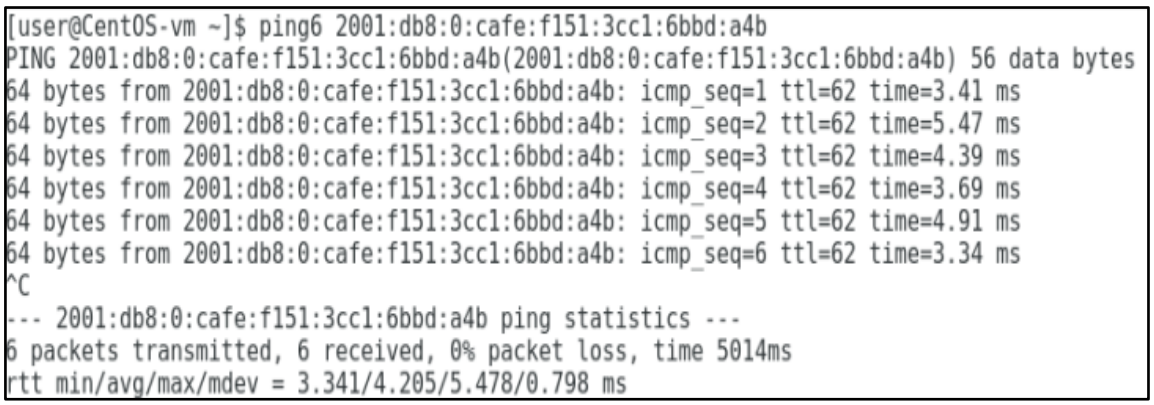
Figura 14. Teste de ping PC3 para PC4



Fonte: Autoria própria

O comando foi executado no terminal PC1 para o PC4, o resultado e exposto na figura 15. Com base no resultado desde teste, e possível analisar o primeiro indicio que a rota diretamente conectada entre os roteadores está funcionando perfeitamente.

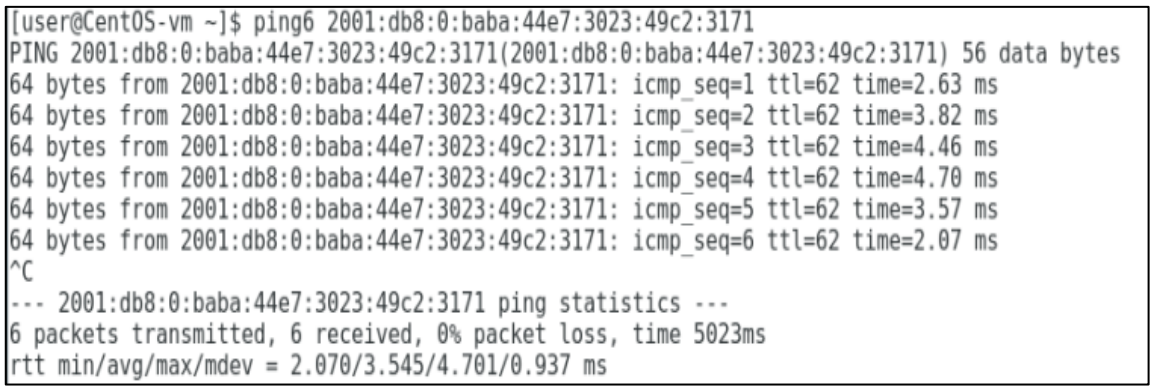
Figura 15. Teste de ping PC1 para PC4



Fonte: Autoria própria

O comando foi executado no terminal PC3 para o terminal PC2, como demonstra na figura 16.

Figura 16. Teste de ping PC3 para PC2



Fonte: Autoria própria

O processo de validação comprovou a conectividade entre os hosts que se encontram na rede, sendo possível estabelecer comunicação a partir de qualquer terminal para outro. É importante observar as informações que o ping fornece, como, a mensagem ICMP, que fornece relatórios de erros ao host que deu origem aos pacotes enviados na rede. E o TTL (Time to Live), sendo o tempo máximo em que o pacote tem de vida na rede.

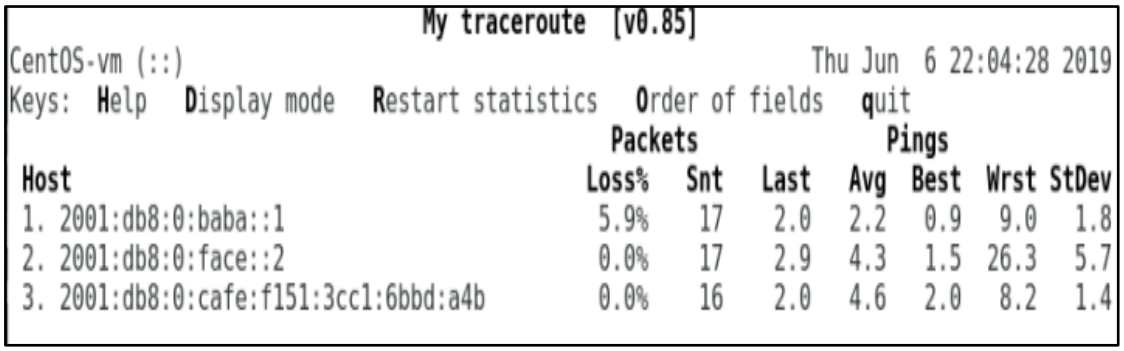
5.3 My Traceroute

O **MTR (*My Traceroute*)** é uma ferramenta de diagnóstico da rede que combina as funcionalidades dos comandos **ping** e **traceroute**, que permite exibir os percentuais e tempo de respostas da rota até o destino. Um repentino aumento na quantidade de pacotes perdidos ou no tempo de resposta é um indicador de que há um link ruim ou apenas sobrecarregado na rota. Segue abaixo o comando utilizado para a realização do teste.

#mtr

O traceroute tem o intuito de demostrar o caminho percorrido entre dois nós na rede, ou seja, ele é um teste ponto a ponto. A primeira verificação foi realizada no terminal PC1 para o PC4, a figura 17 representa o resultado do comando, onde e possível observar que as informações do caminho percorrido até o destino, sendo o primeiro salto no ROTEADOR1, logo depois no ROTEADOR2 e por fim no PC4.

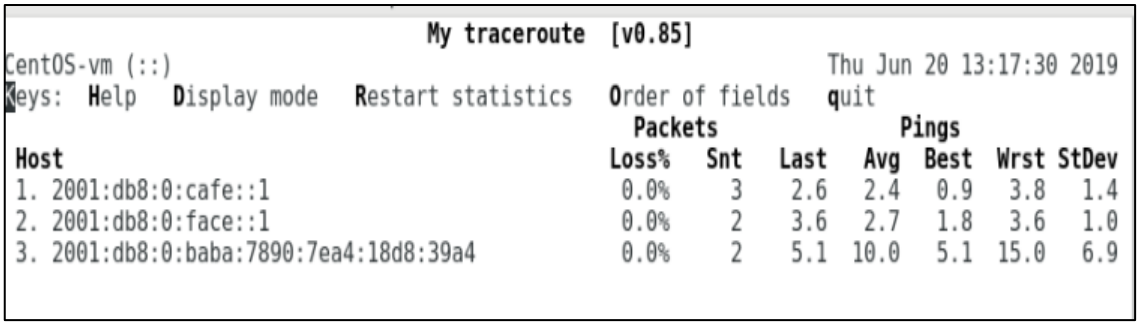
Figura 17. Teste de traceroute do PC1 para a PC4



Fonte: Autoria própria

O segundo teste foi executado no terminal PC3 para o terminal PC1, como representado na figura 18, sendo o primeiro salto no ROTEADOR2, logo depois no ROTEADOR1 e por fim no PC1.

Figura 18. Teste de traceroute do PC3 para a PC1



Fonte: Autoria própria

Abaixo é possível observar a descrição de cada dado apresentado pelo My Traceroute.

- Loss: porcentagem de perda em determinado salto.
- Snt: número de pacotes enviados.
- Last: tempo obtido para do último pacote.
- Avg: a média de tempo em determinado salto.
- Best: o melhor tempo em determinado salto.
- Wrst: o pior tempo em determinado salto.
- StDev: a média de tempo entre saltos.

Os dois testes de traceroute executados tem como finalidade demonstrar o caminho que um PC vai percorrer quando realizada a comunicar com um outro PC conectado a outro roteador, lembrando que para que essa comunicação só é possível entre os terminais graças ao protocolo de roteamento OSPFv3.

6. Considerações finais

Com o esgotamento dos endereços IPv4, e iminente que a internet poderia sofrer uma grande perda em relação a qualidade de serviços, e para que a internet não sofra com as limitações impostas por um número reduzido de endereços IP disponíveis, surge como a opção de substituição, um novo protocolo, o IPv6.

O presente estudo teve como objetivo aprofundar o conhecimento sobre as funcionalidades do protocolo IPv6, visto que a principal motivação para o desenvolvimento desse trabalho foi o esgotamento de endereços IPv4, que já é uma realidade em diversas redes, ocasionada pelo crescimento exponencial de dispositivos conectados à internet.

Conforme abordado, o IPv6 não somente tem a vantagem de disponibilizar uma grande quantidade de endereços válidos para a necessidade atual, mas também outras vantagens como, formato de cabeçalho simplificado para otimização de entrega de pacotes e suporte aos atuais protocolos de roteamento.

Neste trabalho foi desenvolvido uma topologia de rede que utiliza o protocolo IPv6 e algumas de suas funcionalidades, como o protocolo DHCP na versão 6 e o protocolo OSPF na versão 3, ambos destinados exclusivamente para o IPv6. Os resultados obtidos através da verificação de concessão de IP, teste de ping e traceroute, colaboraram para a compreensão do funcionamento dos protocolos em questão.

Nesse sentido, o estudo proposto poderá auxiliar na adoção do novo protocolo, assim facilitando e incentivando a implantação do mesmo.

Referências bibliográficas

ARAUJO, Ediney; TEIXEIRA, Everton. **Redes de computadores utilizando IPv6 com protocolo DHCPv6**. 2014. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3969/1/CT_COTEL_2014_2_03.pdf. Acesso em: 18 abr. 2019.

BENDJOUYA, Mauricio; MORAES, André. **Protocolos de roteamento dinâmico**. Disponível em: http://187.7.106.14/wiki2011_2/lib/exe/fetch.php?media=projeto13:artigo.pdf. Acesso em: 15 jun. 2019.

BRITO, Samuel. **Servidores DHCPv6 em Redes IPv6.** 2013. Disponível em: http://labcisco.blogspot.com/2013/05/servidores-dhcpv6-em-redes-ipv6.html. Acesso em: 20 abr. 2019.

COMER, Douglas. **Interligação em rede com TCP/IP - Princípios, Protocolos e Arquitetura**. 5. Ed. 1.vol. Rio de Janeiro: Campus, 2015.

GOMES, Pedro. **O que é PING e como funciona seu monitoramento**. 2019. Disponível em: https://www.opservices.com.br/o-que-e-ping/. Acesso em: 20 jun. 2019.

KACHORROSKI, Joabe. **Falando sobre protocolos de rede**. 2018. Disponível em: http://wsci.eti.br/noticia/falando_sobre_protocolos_de_rede_parte_2. Acesso em: 4 maio 2019.

KUROSE, James; ROSS, Keith. **Redes de Computadores e a Internet:** Uma abordagem top-down. 5.ed. São Paulo: Pearson, 2010.

LACNIC. **Fases de Esgotamento do IPv4**. 2019. Disponível em: https://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4. Acesso em: 6 abr. 2019.

MAGGIO, Alessandro. **DHCPv6 Configuration: SLAAC, Stateless e Stateful**. Disponível em: https://www.ictshore.com/free-ccna-course/dhcpv6-basics/. Acesso em: 21 abr. 2019.

MARTINS, Luciano. 2002. **Conceitos e experiências com os protocolos de roteamento IPv6 – enabled OSPFv3 e BGP4 + usando Zebra em sistemas Linux e Free BSD**. Disponível em: https://memoria.rnp.br/newsgen/0207/ipv6_ospfv3_bgp4.html. Acesso em: 18 maio 2019.

MOREIRAS, Antônio; PATARA, Ricardo. **Fascículos sobre a infraestrutura da internet endereços IP e ASNS alocação para provedores Internet**. Disponível em: https://nic.br/media/docs/publicacoes/13/fasciculos-sobre-a-infraestrutura-da-internet-endere%C3%A7os-ip-e-asns-alocacao-para-provedores-internet.pdf. Acesso em: 24 maio 2019.

MOREIRAS, et. al. **IPv6 Básico. 2012.** Disponível em: http://users.on.br/mscorrea/IPv6/ApostilaIPv62012.pdf. Acesso em: 2 abr. 2019.

NASCIMENTO, Marcelo. **Procotolo ICMP, Ping e traceroute**. 2015. http://www.dltec.com.br/blog/cisco/protocolo-icmp-ping-e-traceroute/. Acesso em: 8 jun. 2019.

PEDROZO, Raissa. **Implantação de uma rede utilizando os padrões do protocolo IPv6**. 2014. Disponível em: http://www.redes.ufsm.br/docs/tccs/Raissa_Monego.pdf. Acesso em: 9 maio 2019.

PÓVOA, Thiago. **Funcionamento do DHCP e DHCPv6**. Disponível em: https://webpov oa.com/dhcp/. Acesso em: 25 abr. 2019.

RODRIGUES, Rogerio. 2015. **DHCP Stateful para IPv6**. Disponível em: https://estudoscisco.wordpress.com/tag/dhcp-stateful/. Acesso em: 1 maio 2019.

SANTOS, Luciano. **Implementação de IPV6 em um provedor de internet**. 2016. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/7425/1/PG_COADS_2016_2_01.pdf. Acesso em: 28 abr. 2019.

TANENBAUM, Andrew; WETHERALL, David. **Redes de Computadores**. 5. ed. São Paulo: Pearson Education do Brasil, 2011.