UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS TECNOLÓGICAS
CURSO DE ENGENHARIA DE COMPUTAÇÃO

LUIZ CARLOS CHAVES LIMA JUNIOR

PLANEJAMENTO DE REDE DE COMUNICAÇÃO DE DADOS PARA TRANSIÇÃO DE ENDEREÇAMENTO DE IPV4 PARA IPV6

SÃO LUÍS – MA
2017

LUIZ CARLOS CHAVES LIMA JUNIOR

PLANEJAMENTO DE REDE DE COMUNICAÇÃO DE DADOS PARA TRANSIÇÃO DE ENDEREÇAMENTO DE IPV4 PARA IPV6

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Computação da Universidade Estadual do Maranhão como requisito parcial para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Carlos Henrique Rodrigues Oliveira.

SÃO LUÍS – MA
2017

DEDICATÓRIA

Aos meus avós Lucimar e Raimundo;

À minha tia Maria da Glória;

Aos amigos Benedito (Seu Bina) e Walter Gonzaga, pessoas muito importantes na minha vida e que sempre me incentivaram a seguir em frente, sempre em busca do melhor.

AGRADECIMENTOS

Agradeço, inicialmente, à minha mãe Conceição Matilde por todo apoio, incentivo, paciência, dedicação e amor oferecidos ao longo de toda minha vida, foi ela que tornou possível o início e a chegada ao fim dessa jornada.

Ao meu orientador, professor Dr. Carlos Henrique, que, além de um exemplo de profissional, é uma excelente pessoa e me deu todo o apoio necessário em todos os momentos que precisei.

Aos colegas Richardson e Caio pelo suporte durante a produção deste projeto.

Aos meus amigos “Suricates”, por todo apoio nos momentos difíceis e pelos momentos de descontração ao longo dessa jornada – Adriano, Thiarlleson, Marcelo, Daniel, Patrick, Cristiano, João Pedro e Rafael.

Às colegas Aurelianny e Ana Paula, pelo apoio e pelos momentos de diversão.

A todos os meus familiares e amigos que se fizerem presentes ao longo dessa jornada.

RESUMO

Este trabalho visa mostrar o planejamento da rede de dados do curso de Engenharia da Computação para transição do protocolo IPv4 para IPv6, utilizando o mecanismo de transição Pilha Dupla. Para isso, foram utilizados dispositivos reais, presentes no laboratório de Telecomunicações do próprio curso, nos quais foi possível checar se o mecanismo de transição escolhido funcionaria corretamente, em uma rede de testes separada, e como seria a atuação dessa rede em termos de endereçamento e conectividade em dois cenários diferentes. O primeiro cenário é composto apenas pela rede local, onde foi configurado um servidor *DHCP* que ficaria responsável por fornecer as configurações de endereçamento para os hosts pertencentes à essa rede. Já no segundo cenário, considera-se que o servidor *DHCP* se encontrava em uma rede externa e adicionou-se um novo roteador local no papel de *Relay Agent* ou agente de retransmissão que seria responsável por repassar as informações de configuração de endereços aos hosts da rede local. Para verificar se havia conectividade em ambos os cenários foram feitos testes usando o comando *ping* nos hosts da rede.

Palavras-chave: Internet, **Protocolo IPv4*;* Protocolo IPv6*;* Mecanismos de Transição de IPv4 para IPv6.**

ABSTRACT

This work aims to show the planning of the data network of the Computer Engineering course for the transition from IPv4 *to* IPv6*, using the Dual Stack transition mechanism. In order to do this, real devices were used, present in the Telecommunications Laboratory of the course itself, in which it was possible to verify if the chosen transition mechanism would work correctly, in a separate test network, and how would the network perform in terms of addressing and connectivity in two different scenarios. The first scenario consists only of the local network, where a DHCP server was configured that would be responsible for providing the addressing configurations for the hosts belonging to that network. In the second scenario, we consider that the DHCP server is in an external network and we added a new local router in the role of Relay Agent or Relay Agent that would be responsible for passing the configuration information of addresses to the hosts of the local network. To check if there was connectivity in both scenarios, tests were performed using the ping command on the network hosts.*

***Keywords: Internet,* IPv4 *Protocol;* IPv6 *Protocol; Transition Mechanisms from* IPv4 *to* IPv6.**

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

ARPANET	*Advanced Research Projects Agency Network*
CCT	Centro de Ciências Tecnológicas
CIDR	*Classless Inter-Domain Routing*
CNAME	*Canonical NAME*
DARPA	*Defense Advanced Research Projects Agency*
DHCP	*Dynamic Host Configuration Protocol*
DHCPv4	*Dynamic Host Configuration Protocol version 4*
DHCPv6	*Dynamic Host Configuration Protocol version 6*
DNS	*Domain Name System*
EUA	Estados Unidos da América
FTP	*File Transfer Protocol*
FE	*FastEthernet*
GE	*GigabitEthernet*
HTTP	*HyperText Transfer Protocol*
IANA	*Internet Assigned Numbers Authority*
ICMP	*Internet Control Message Protocol*
ICMPv4	*Internet Control Message Protocol version 4*
ICMPv6	*Internet Control Message Protocol version 6*
IEEE	*Institute of Electrical and Electronic Engineers*
IETF	*Internet Engineering Task Force*
IOS	*Internetwork Operating System*
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISP	*Internet Service Provider*
LAN	*Local Area Network*
MAC	*Media Access Control*
MIPv6	*Mobile IP version 6*
MTU	*Maximum Transmission Unit*
MX	*Mail eXchanger*
NAT	*Network Address Translation*
NCP	*Network Control Protocol*
NDP	*Neighbor Discovery Protocol*
NS	*Name Server*
NTI	Núcleo de Tecnologia da Informação
PTR	*PoinTeR*
QoS	*Quality of Service*
RFC	*Request for Comments*
RR	*Resource Records*
SLAAC	*Stateless Address Autoconfiguration*
SMTP	*Simple Mail Transfer Protocol*

SOA	*Start of Authority*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
TTL	*Time to Live*
UEMA	Universidade Estadual do Maranhão
UDP	*User Datagram Protocol*
VLAN	*Virtual Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais, podemos ver o crescente aumento da utilização da Internet tanto por usuários comuns, quanto nas áreas empresarial, industrial e acadêmica.

É muito comum nos depararmos com pessoas conectadas por meio de notebooks, smartphones, tablets e etc., para entretenimento próprio por meio das redes sociais e da infinidade de coisas disponíveis na Internet, bem como setores industriais e empresariais fazendo uso dela para agilizar e facilitar tarefas cotidianas. Na área acadêmica também não é diferente, haja vista que tem se tornado crescente o número de pesquisas para soluções de problemas do dia a dia, por meio da implementação de softwares e da construção de dispositivos inteligentes que funcionam por meio de uma rede.

Castelluci [1] considera que a existência de conexão entre todos estes dispositivos, assim como a expansão da Internet, só é possível graças a utilização, além de outros protocolos, de um protocolo muito conhecido e um dos mais importantes da Internet, o Internet Protocol (IP) ou, em português, Protocolo da Internet. É ele quem fornece endereços a estes dispositivos para serem identificados na rede. O que acontece, é que o número de endereços disponibilizados pela versão 4 do Protocolo IP (IPv4), a mais utilizada atualmente, tem se aproximado cada vez mais do fim e, uma vez que isso aconteça, o crescimento da Internet não seria mais possível, afirma a IANA [2], que é autoridade global da Internet criada para gerenciar de forma cuidadosa esses endereços. Para evitar que isso ocorra, várias medidas paliativas foram adotadas, como CIDR, DHCP e NAT, porém a ação mais efetiva para solucionar este problema seria migrar da versão 4 (IPv4) para a versão 6 (IPv6). Entretanto, devido ao atual cenário da Internet, onde a maioria dos endereços utilizados ainda são os IPv4, essa migração não pode ser feita de forma direta, ou seja, é necessário que seja feita aos poucos para evitar problemas de compatibilidade, dentre outros, ressalta Brito [3].

1.1 ESGOTAMENTO DOS ENDEREÇOS IPv4

Kurose [4] reitera que em fevereiro de 2011, a IANA alocou o último conjunto restante de endereços IPv4 a um registrador regional. Embora esses registradores ainda tenham endereços IPv4 disponíveis dentro de seus conjuntos, quando esses endereços se esgotarem, não haverá mais blocos de endereços disponíveis para serem alocados a partir de um conjunto central.

Devido a isso, foram criadas algumas soluções temporárias para garantir uma sobrevida para os endereços IPv4. Sendo assim, a ideia de ter classes de endereços padrões com

prefixo indicador da rede e dos *hosts* fixos, que foi um dos causadores do desperdício de uma grande quantidade de endereços IPs, foi substituída por uma medida que flexibilizou as classes padrões projetadas no IPv4, de maneira que os bits reservados para identificar redes e *hosts* poderiam variar de posição [3]. Essa medida chama-se CIDR, especificada na RFC 1519 [5], e foi muito importante para alocação de endereços, pois foi a partir dele que surgiu a máscara de rede. A máscara de rede, assim como os endereços IPv4, também possui 32 *bits* e é formada por um prefixo de *bits* 1s para identificar a área da rede e um sufixo de *bits* 0s que identifica a área dos *hosts*, sendo que não pode existir intercalação entre 0s e 1s, além disso, ela pode escrita de maneira simplificada apontando apenas quantidade de *bits* do prefixo da rede precedido por uma barra " / " [3] como, por exemplo, podemos utilizar os faixa reservada para endereços privados, que ficariam da seguinte forma: 10.0.0.0 /8, 172.16.0.0 /12 e 192.168.0.0/24. Desse modo, é possível gerenciar a distribuição dos endereços IPv4, reduzindo assim o desperdício destes endereços.

Outra solução para retardar o esgotamento dos endereços IPv4 foi a criação do NAT especificado na RFC 2663 [6], é um método pelo qual os endereços IP são mapeados de um domínio para outro, na tentativa de fornecer roteamento transparente para *hosts*. Tradicionalmente, os dispositivos NAT são usados para que se conecte um endereço privado, conhecido apenas no contexto local à um endereço público registrado na *Internet* [6].

Tanenbaum [7] afirma que a ideia básica por trás da NAT é atribuir um único endereço IP (ou no máximo, um número pequeno deles) para tráfego da *Internet*. Na rede local todo computador obtém um endereço IP exclusivo, usado para roteamento do tráfego interno. Porém, quando um pacote sai para *Internet*, ocorre uma conversão de endereço. Para tornar esse esquema possível, o NAT o utiliza os intervalos de endereços privados [8] para serem utilizados na rede local, e quando esses endereços chegam ao roteador de borda é feita a tradução desse endereço privado para o endereço público fornecido pela ISP e esse sim estará visível na *Internet*.

De acordo com Brito [3], outra medida utilizada para dar sobrevida ao IPv4 foi criação do DHCP que faz a distribuição automática de endereços IPs internos, entretanto fornece também um meio para economizar endereços por meio da configuração de um escopo com vários endereços públicos para fins de empréstimo desses endereços para os clientes, apenas durante o período que estiverem conectados à rede. Assim que usuário se desconecta da rede o endereço dinamicamente atribuído é devolvido para o ISP e pode ser reaproveitado para outros clientes. O DHCP foi um dos protocolos utilizados neste projeto e suas duas versões serão explicadas no tópico 2.4 deste documento.

Tanenbaum [7] também destaca que, embora o CIDR e a NAT ainda tenham alguns anos pela frente, pode-se perceber que o IP em sua forma atual (IPv4) está com os dias contados. Além desses problemas técnicos, há uma outra questão em paralelo. No início, a *Internet* era amplamente usada por universidades, indústrias de alta tecnologia e órgãos governamentais dos EUA (especialmente pelo Departamento de Defesa). Com a expansão da *Internet* a partir de meados da década de 1990, ela começou a ser usada por um grupo diferente de pessoas, em especial pessoas com necessidades específicas.

No começo da década de 1990, a IETF iniciou um esforço para desenvolver o sucessor do protocolo IPv4 e para atender a essa necessidade de maior espaço para endereços IP, foi desenvolvido uma nova versão protocolo IP, o IPv6. 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 [4].

1.2 OBJETIVOS

1.2.1 Objetivo geral

O objetivo geral deste trabalho foi realizar o planeamento da rede de dados do curso de Engenharia de Computação para migração gradual de IPv4 para IPv6, utilizando o mecanismo de transição Pilha Dupla, verificando a atuação de uma rede de testes em dois cenários.

1.2.2 Objetivos específicos

- Configurar um servidor DHCP local, para ambas as pilhas, para fornecer endereços IPv4 e IPv6 aos *hosts* no cenário 1;
- Configurar um servidor DHCP, também nas duas pilhas, em uma rede externa para fornecer endereços IPv4 e IPv6 aos *hosts* por meio de um *Relay Agent* no cenário 2;
- Verificar se os *hosts* estão sendo endereçados corretamente e se há conectividade por meio de testes de *ping*.

1.3 METODOLOGIA

Primeiramente, foi verificada a disponibilidade de equipamentos gerenciáveis para que houvesse possibilidade de atribuir as configurações necessárias. Em seguida, checar se além

dos equipamentos serem gerenciáveis, os firmwares estavam atualizados e tinham suporte à tecnologia IPv6.

Constatado o atendimento dos requisitos, tanto de *hardware*, como de *software*, foi possível iniciar a parte prática na qual foi feita a montagem das topologias e configurações de ambos os cenários e por fim foi realizada a parte de testes, na qual foi verificado a configuração dos endereços e conectividade entre os hosts da rede.

1.4 ESTRUTURA DO TRABALHO

Este trabalho será composto de cinco capítulos nos quais serão escritas todas as informações necessárias para a compreensão do ponto de vista teórico e prático do projeto. No Capítulo 2, Fundamentação Teórica, serão abordados conceitos importantes para o entendimento do modelo, técnicas e protocolos utilizados. O Capítulo 3 faz a descrição detalhada do projeto. Já o Capítulo 4, apresenta as conclusões obtidas e, por fim, no Capítulo 5, sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, inicialmente, serão abordados os conceitos sobre o modelo TCP/IP, fazendo uma breve apresentação da história da *Internet* e das características do modelo TCP/IP, e em seguida, serão apresentados outros conceitos importantes, como os protocolos IPv4 e IPv6 e outros protocolos que foram utilizados nas pilhas TCP/IPv4 e TCP/IPv6, bem como os mecanismos de transição entre as versões do protocolo IP.

2.1 HISTÓRIA DA *INTERNET* E MODELO TCP/IP

O surgimento da *Internet* ocorreu na década de 60, a partir de um projeto financiado por uma agência do Departamento de Defesa dos Estados Unidos, conhecida com DARPA, devido a constante preocupação com a indisponibilidade dos meios de comunicações, que funcionavam de forma centralizada, onde os pesquisadores tinham como meta a criação de uma rede experimental distribuída, ou seja, não centralizada, com foco principal na resiliência a falhas [3].

É importante ressaltar que, na época, a ideia era bem diferente da *Internet* atual, pois o objetivo era apenas interligar quatro universidades americanas, que foram os primeiros quatro nós da rede, que foi denominada de ARPANET, em 1969, que inicialmente, utilizava um protocolo chamado NCP para fazer a comunicação de *host* a *host*. Porém, esse protocolo se mostrou ineficiente com passar dos anos, devido ao acréscimo de novos *hosts* na rede, o que gerou o aumento de tráfego de dados e fez com que em 1974 um novo conjunto de protocolos de comunicação mais robusto fosse proposto e implementado em todo o ARPANET, com base no TCP para comunicação de rede de ponta a ponta [9].

Alguns anos depois, para evitar que os *gateways* intermediários tivessem que lidar com um protocolo de ponta a ponta, um novo projeto foi desenvolvido para dividir as responsabilidades entre um par de protocolos, o Protocolo de *Internet* (IP) para pacotes de roteamento e comunicação de dispositivo a dispositivo e TCP para comunicação de *host* confiável e de ponta a ponta [9].

Apesar do fato que TCP e o IP foram inicialmente concebidos funcionalmente como um único protocolo, o conjunto de protocolos que realmente se refere a uma grande coleção de protocolos e aplicativos geralmente é conhecido como pilha de protocolos TCP/IP, modelo que até hoje domina os processos de comunicação de dados e a conectividade entre um emissor e um receptor em uma rede de computadores [10].

Se tratando das características do modelo TCP/IP, este fornece conectividade de ponta a ponta especificando como os dados devem ser embalados, endereçados, transmitidos, encaminhados e recebidos no destino e é organizado em quatro camadas de abstração que são usadas para classificar todos os protocolos relacionados de acordo com o escopo da rede em questão, oferecendo serviços umas às outras [11]. Nath [11] faz um resumo de cada uma dessas camadas listadas a seguir e elas estão dispostas de acordo com a Figura 1:

- **Camada de Aplicação** – é onde os aplicativos criam dados do usuário e comunicam esses dados a outros aplicativos em outro ou no mesmo *host*. As aplicações, ou processos, fazem uso dos serviços fornecidos pelas camadas inferiores, especialmente a Camada de Transporte, que fornece meios confiáveis ou não confiáveis para outros processos. Esta é a camada em que todos os protocolos de nível superior, como SMTP, FTP, SSH, HTTP, dentre outros, operam.
- **Camada de Transporte** – executa comunicações de *host* para *host* e na rede local ou redes remotas separadas por roteadores, fornecendo um canal para as necessidades de comunicação das aplicações. UDP é o protocolo básico de camada de transporte, fornecendo um serviço de datagrama não confiável. O TCP fornece controle de fluxo, estabelecimento de conexão e transmissão confiável de dados.
- **Camada de *Internet*** – tem a tarefa de trocar datagramas por meio dos limites da rede, definindo as estruturas de endereçamento e roteamento usadas para o conjunto de protocolos TCP/IP. O protocolo principal desta camada é o IP, que define os endereços IP na rede. Sua função no roteamento é transportar datagramas para o próximo roteador IP que tenha a conectividade com uma rede mais próxima do destino de dados final.
- **Camada de Acesso à Rede** – define os métodos de rede dentro do escopo do *link* de rede local em que os *hosts* se comunicam sem roteadores intervenientes. Esta camada inclui os protocolos utilizados para descrever a topologia de rede local e as interfaces necessárias para efetuar a transmissão de datagramas de camada de *Internet* para *hosts* vizinhos. Como exemplos de protocolos que atuam nesta camada podemos citar: PPP, *Ethernet*, *Frame Relay* e outros.

Figura 1. Camadas do Modelo TCP/IP

Nos tópicos a seguir serão mostrados os protocolos utilizados no projeto, assim como algumas tecnologias e mecanismos de transição, onde se destaca o mecanismo em Pilha Dupla.

2.2 O PROTOCOLO IPv4

O protocolo IP, na sua primeira versão, conhecida como IPv4, foi projetado para uso em sistemas interconectados de redes de comunicação que funcionariam por comutação de pacotes entre os computadores. O IPv4 funciona transmitindo blocos de dados chamados datagramas das fontes para os destinos, que são *hosts* identificados por endereços de comprimento fixo e, além disso, é capaz de fazer a fragmentação e remontagem de datagramas longos, se necessário, para transmissão de pequenos pacotes por meio das redes [12].

2.2.1 CABEÇALHO IPv4

O cabeçalho IPv4 possui tamanho variável entre 20 e 60 *bytes* contendo informações essenciais para os serviços de entrega e roteamento [10], distribuídas em campos como mostrado na Figura 2.

Figura 2. Formato do Cabeçalho IPv4 [13]

Os campos que compõem o cabeçalho do datagrama IP são [4]:

i. **Versão** – trata-se de quatro *bits* que especificam a versão do protocolo IP do datagrama. Esse campo é preenchido com o valor 0100 em binário, que equivale a 4 em decimal.

ii. **Tamanho do Cabeçalho** – esses quatro *bits* são necessários para determinar onde, no datagrama IP, os dados começam de fato e pode conter um número variável de opções, porém, normalmente, a maior parte dos datagramas IP não contém opções; portanto, o datagrama IP típico tem um cabeçalho de 20 *bytes*.

iii. **Tipo de Serviço** – neste campo os *bits* de tipo de serviço foram incluídos no cabeçalho do IPv4 para poder diferenciar os diferentes tipos de datagramas *IP*, que devem ser distinguidos uns dos outros.

iv. **Tamanho Total** – indica o comprimento total do datagrama IP (cabeçalho mais dados) medido em *bytes*, onde, uma vez que esse campo tem 16 *bits* de comprimento, o tamanho máximo teórico do datagrama IP é 65.535 *bytes*, entretanto, datagramas raramente são maiores do que 1.500 *bytes*.

v. **Identificação –** um valor de identificação atribuído pelo remetente para auxiliar na montagem dos fragmentos de um datagrama [12].

vi. ***Flags* –** *flags* de controle dos fragmentos [12].

vii. **Deslocamento do Fragmento –** este campo indica onde pertence determinado fragmento no datagrama [12].

viii. **Tempo de Vida** – o campo de tempo de vida ou TTL é incluído para garantir que datagramas não fiquem circulando para sempre na rede. Esse campo é decrementado de uma unidade cada vez que o datagrama é processado por um roteador. Se o campo TTL chegar a 0, o datagrama deve ser descartado.

ix. **Protocolo** – usado somente quando um datagrama IP chega a seu destino final. O valor do campo indica o protocolo de camada de transporte específico ao qual a porção de dados desse datagrama IP deverá ser passada.
x. **Soma de Verificação do Cabeçalho** – a soma de verificação do cabeçalho auxilia um roteador na detecção de erros de bits em um datagrama IP recebido.
xi. **Endereços IP de Origem e de Destino** – estes campos possuem 32 *bits* cada um, e contém os endereços de origem e destino do datagrama IP.
xii. **Opções + Complemento** – o campo de opções e complemento permite que um cabeçalho IP seja estendido.

Agora veremos no tópico a seguir a questão dos endereços IPv4, que mostrará as principais características relacionadas a esse assunto.

2.2.2 ENDEREÇOS IPv4

O IPv4 possui um espaço de endereçamento de 32 *bits*, dividido em quatro campos de 8 *bits* chamados de octetos, que são representados na forma de um número decimal com intervalo de 0 a 255, separado por ponto [14], notação a qual, é conhecida como *notação decimal pontuada* [10], como, por exemplo o endereço "192.168.0.2". O espaço de endereçamento é equivalente a 2^{32}, o que gera a possibilidade de endereçar aproximadamente 4,3 bilhões de nós diferentes e, no início, estes endereços foram divididos em três classes principais de tamanhos fixos [15] e mais duas classes para fins especiais [16], 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* [15].
- **Classe B**: definia os 2 *bits* mais significativos como 10, utilizava os 14 *bits* seguintes para identificar a rede, e os 16 *bits* restantes para identificar o *host* [15].
- **Classe C**: definia os 3 *bits* mais significativos como 110, utilizava os 21 *bits* seguintes para identificar a rede, e os 8 *bits* restantes para identificar o *host* [15].
- **Classe D**: definia os 4 *bits* mais significativos como 1110 e era utilizada para endereçamento *multicast* [16].
- **Classe E**: definia os 4 *bits* mais significativos como 1111, e era reservado para uso futuro [16].

As faixas de endereços pertencentes a cada classe são mostradas na Tabela 1.

Tabela 1. Classes de Endereços IPv4 [adaptado 16]

Classe	Início	Fim
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

Algumas faixas de endereço nas classes A, B e C foram reservadas pela IANA para uso especial como mostrado na Tabela 2, não serão citados todos endereços, mas pode-se saber mais sobre o assunto consultando a RFC 3330 [17].

Tabela 2. Endereços IPv4 para uso especial [17]

Faixa de Endereços	Uso
127.0.0.0 a 127.255.255.255	*Loopback*
169.254.0.0 a 169.254.255.255	*Link Local*
192.0.2.0 a 192.0.2.255	Utilizados para documentação e exemplos
192.88.99.0 a 192.88.99.255	Conversão de IPv6 em IPv4
198.18.0.0 a 198.19.255.255	Teste de *benchmark* do dispositivo de interconexão de rede

Além desses endereços, também foram separadas pela IANA algumas faixas de endereços nas classes A, B e C, para serem usadas apenas para endereçamento local, ou seja, essas faixas de endereços não são roteáveis na *Internet*, e são conhecidos como IPs Privados, definidos pela RFC 1918 [8]. A Tabela 3 mostra essas faixas de endereçamento privado:

Tabela 3. Endereços IPv4 Privados [8]

Endereços IPv4 Privados	
Classe A	10.0.0.0 a 10.255.255.255
Classe B	172.16.0.0 a 172.31.255.255

Classe C	192.168.0.0 a 192.168.255.255

Os endereços IPv4 também podem ser classificados quanto ao tipo [14]:

- ***Unicast*** – atribuído a uma única interface de rede localizada em uma subrede específica na rede e utilizada para comunicações de um para um.
- ***Multicast*** – atribuído a uma ou mais interfaces de rede localizadas em várias subredes na rede e usadas para comunicações de um para muitos.
- ***Broadcast*** – atribuído a todas as interfaces de rede localizadas em uma subrede na rede e usadas para comunicações de um para todos.

2.3 PROTOCOLO IPv6

Para Torres [16], de maneira geral, o IPv6 funciona maneira similar ao IPv4, tendo o formato do datagrama alterado para comportar os endereços de 128 *bits*, porém algumas novas funções foram introduzidas.

A RFC 8200 [18], estabelece que o IP versão 6 (IPv6) é uma nova versão do protocolo *Internet*, projetado como o sucessor da versão IP 4 (IPv4) e que as mudanças do IPv4 para o IPv6 são principalmente nas seguintes categorias:

a) **Capacidades de endereçamento expandido** – O IPv6 aumenta o tamanho do endereço IP de 32 *bits* para 128 *bits*, para apoiar mais níveis de hierarquia de endereçamento, muito maior número de nós endereçáveis e configuração automática mais simples de endereços.

b) **Simplificação do formato do cabeçalho** – Alguns campos de cabeçalho IPv4 foram descartados ou feitos opcionalmente, para reduzir o custo de processamento de casos comuns de manipulação de pacotes e para limitar o custo da largura de banda do cabeçalho IPv6.

c) **Melhor suporte para extensões e opções** – Alterações na forma como as opções de cabeçalho IP são codificadas permitem encaminhamento mais eficiente, limites menos rigorosos sobre o comprimento de opções e maior flexibilidade para introduzir novas opções no futuro.

d) **Capacidade de rotulagem do fluxo** – Uma nova capacidade é adicionada para habilitar a rotulagem de pacotes pertencentes a um tráfego particular ("fluxos") para os quais o remetente solicita tratamento especial, como QoS ou serviços "em tempo real".

Brito [3] ressalta que, além das vantagens citadas, podemos acrescentar que o protocolo IPv6 dispensa a utilização do NAT, preservando o modelo fim-a-fim, possui meios de segurança já embutidos e também fornece meios para mobilidade.

2.3.1 CABEÇALHO IPv6

De acordo com o IPv6.Br [13], houve mudanças no formato do cabeçalho base do IPv6 de modo a torná-lo mais simples, como: a redução no número de campos, fixação do tamanho do cabeçalho em 40 *bytes* e adição de cabeçalhos de extensão que não precisam ser processados por roteadores intermediários. O novo formato do cabeçalho IPv6 é mostrado na Figura 3:

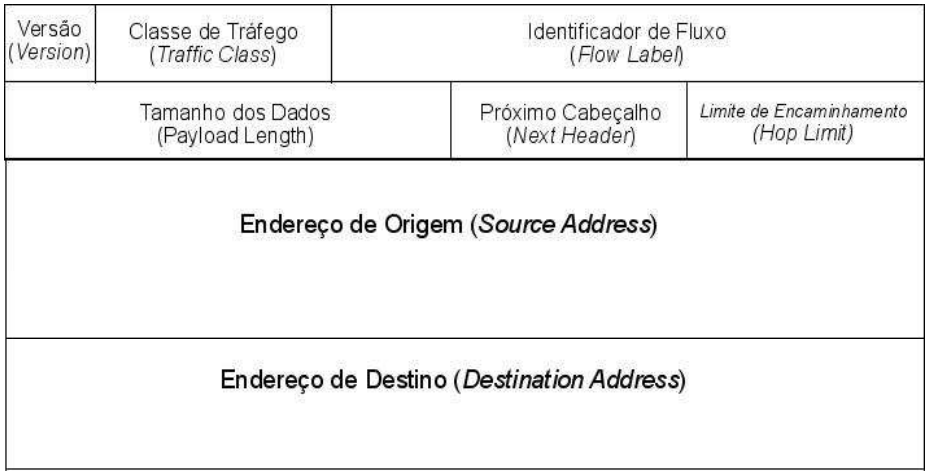


Figura 3. Formato do Cabeçalho IPv6 [13]

Observando a Figura 3, podemos perceber que o cabeçalho IPv6 possui um formato mais simples, com apenas 8 campos e que alguns campos foram removidos ou renomeados, se comparado com o cabeçalho IPv4, mostrado na Figura 2. Se tratando dos campos removidos do cabeçalho IPv4, o campo "Tamanho do Cabeçalho" foi excluído, pois o seu valor agora é fixo. Além deste, o campo "Soma de Verificação do Cabeçalho", também foi removido, já que verificação de erros se tornou desnecessária, pois esse serviço também é realizado por outras camadas, o que torna o processo redundante [3]. Da mesma forma, os campos "Identificação", "*Flags*", "Deslocamento do Fragmento" e "Opções + Complemento", não fazem mais parte do cabeçalho IPv6, visto que estes passaram a ter suas informações indicadas em cabeçalhos de extensão, restando apenas os campos que serão explicados a seguir [13]:

i. **Versão** – identifica a versão do protocolo utilizado e, neste caso, é preenchido com o valor 0110 em binário que em decimal equivale a 6.

ii. **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.
iii. **Identificador de Fluxo** – adiciona uma nova funcionalidade de QoS que consiste em associar vários pacotes de mesma natureza em um único fluxo para fins de classificação e filtragem de tráfego [3].
iv. **Tamanho dos Dados** – contém o tamanho, em *bytes*, apenas dos dados enviados junto ao cabeçalho IPv6.
v. **Próximo Cabeçalho** – identifica o cabeçalho de extensão que segue o atual.
vi. **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 de ser descartado.
vii. **Endereço de Origem** – indica o endereço de origem do pacote.
viii. **Endereço de Destino** – indica o endereço de destino do pacote.

Os campos que existiam no IPv4 e foram renomeados no IPv6, são mostrados na Tabela 4:

Tabela 4. Campos Renomeados no Cabeçalho IPv6

Nome do Campo no IPv4	Nome do Campo Equivalente no IPv6
Tipo de Serviço	Classe de tráfego
Tamanho Total	Tamanho dos Dados
Protocolo	Próximo Cabeçalho
Tempo de Vida	Limite de Encaminhamento

Outra mudança interessante, foi a adição de cabeçalhos de extensão, que agora são responsáveis pelas funcionalidades que, anteriormente, eram feitas por meio do campo “Opções + Complemento” e, um detalhe importante, é que os cabeçalhos de extensão devem seguir uma ordem de encadeamento, iniciada pelo cabeçalho IPv6 convencional, recomendadas pela RFC 8200 [18] por meio dos seus respectivos códigos de “Próximo Cabeçalho”, para que haja flexibilidade nas diferentes funcionalidades implementadas e, na Tabela 5, são mostradas a ordem, os códigos e um resumo das funcionalidades de alguns desses cabeçalhos [3]:

Tabela 5: Cabeçalhos de Extensão no IPv6

Ordem	Nome do Cabeçalho	Funcionalidade	Código
1	Cabeçalho IPv6 Convencional	Possui campos com informações para envio e recebimento de pacotes na rede	-
2	*Hop-by-Hop*	Cabeçalho de extensão examinado por todos os roteadores no caminho entre a origem e o destino	0
3	*Destination Options*	Cabeçalho de extensão que traz algumas opções adicionais que devem ser analisadas pelo destinatário do pacote	60
4	*Routing Header*	Cabeçalho de extensão responsável pelas funcionalidades de mobilidade de *IP*	43
5	*Fragment Header*	Cabeçalho de extensão que faz a fragmentação de pacotes.	44
6	*Authentication Header*	Cabeçalho de extensão que fornece integridade e autenticação de datagramas *IP* [19]	51
7	*Encapsulation Security Payload*	Cabeçalho de extensão que fornece uma combinação de serviços de segurança [20]	50

Ainda sobre os cabeçalhos de extensão, vale ressaltar que único interpretado por todos os roteadores intermediários é o *Hop-by-Hop*, sendo assim, os demais cabeçalhos de extensão não precisam ser verificados pelos roteadores ao longo da comunicação entre dois nós, fazendo com que haja ganho de desempenho na rede, devido à redução de processamento nestes roteadores, e por isso, é mandatório que ele venha primeiro que os outros cabeçalhos de

extensão. Além destes cabeçalhos de extensão, existem outros que podem ser consultados em detalhes na RFC 8200 [18].

2.3.2 ENDEREÇOS IPv6

Os endereços IPv6 também possuem diferenças consideráveis em relação ao seu antecessor IPv4, principalmente na quantidade de *hosts* possíveis de endereçar, em sua notação e nos tipos de endereços.

Quanto à questão de quantidade de endereços disponíveis para *hosts*, o IPv6 tem um número extremamente grande, pois passamos de uma versão de que tinha 32 *bits*, para uma que possui 128 *bits* e isso permite espaço de endereçamento de 2^{128}, capaz de atender a, aproximadamente, 340 undecilhões de nós na *Internet* [3].

Referente a notação do endereço IPv6, para torna-los um pouco mais inteligíveis, é utilizada *notação hexadecimal com dois pontos* [10]. Apesar de ter havido uma redução no comprimento dos endereços com a notação hexadecimal, os endereços ainda continuam extensos, então, para tornar sua visualização ainda mais "amigável", foram criadas duas regras: a omissão de zeros à esquerda e a substituição de zeros contínuos por "::" [3], como mostra a Figura 4:

Figura 4. Notação Hexadecimal e Regras para abreviação dos endereços IPv6 [adaptado 3]

Quantos aos tipos de endereços, podemos classificá-los como *unicast*, *multicast* e *anycast*. No IPv6, não existem mais endereços do tipo *broadcast.* Os endereços *broadcast* foram substituídos por um grupo *multicast* especial, conhecido por *multicast-all-nodes*, identificado pelo endereço ff02::1.

Os tipos de endereços IPv6 estão descritos a seguir de acordo com Forouzan [10]:

- **Endereços *Unicast*** – define um único computador, onde o pacote enviado para um endereço unicast deve ser entregue ao computador específico. Além disso, eles podem ser divididos em mais alguns subtipos, mostrados a seguir de acordo com o IPv6.Br [21]:

- *Global Unicast* – equivalente aos endereços públicos IPv4. O endereço *global unicast* é globalmente roteável e acessível na *Internet* IPv6 e é constituído por três partes: o prefixo de roteamento global, utilizado para identificar o tamanho do bloco atribuído a uma rede; a identificação da subrede, utilizada para identificar um enlace em uma rede; e a identificação da interface, que deve identificar de forma única uma interface dentro de um enlace. Podemos citar o endereço "2001:db8:EC::/64", como exemplo de IPv6 *global unicast*.
- *Link Local* – podendo ser usado apenas no enlace específico onde a interface está conectada, o endereço link local é atribuído automaticamente utilizando o prefixo FE80::/64.
- *Unique Local Address* – endereço com grande probabilidade de ser globalmente único, que atua apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces e utiliza o bloco de endereços FC00::/8.

- **Endereços *Anycast*** – define um grupo de computadores com endereços tendo o mesmo prefixo. Um pacote enviado para um endereço *anycast* deve ser entregue exatamente para um dos membros do grupo, o que estiver mais próximo ou mais facilmente acessível.
- **Endereços *Multicast*** – define um grupo de computadores que podem ou não compartilhar o mesmo prefixo, e também, podem ou não estar conectados à mesma rede física. Um pacote enviado a um endereço multicast deve ser entregue a cada membro do grupo.

Nos tópicos a seguir, iremos falar dos protocolos e serviços utilizados para a construção deste projeto, sempre mencionando suas características nas duas pilhas, iniciando pelo protocolo DHCP.

2.4 DHCPv4 E DHCPv6

O DHCP, é um protocolo que funciona como modelo cliente-servidor, onde o servidor *DHCPv4* fornece parâmetros de configuração para hosts da *Internet* e consiste em dois componentes: um protocolo para fornecer parâmetros de configuração específicos de um servidor DHCP para um *host*, denominado cliente, e um mecanismo de alocação endereços aos *hosts* da rede [*22*]. Atualmente esse protocolo possui duas versões: DHCPv4 e DHCPv6.

Segundo Kurose [4] o DHCPv4, versão destinada a atender o IPv4, permite que um *host* obtenha um endereço IP de maneira automática. Além disso, o DHCPv4 pode ser

configurado para que determinado *host* receba o mesmo endereço IP ou um endereço IP temporário diferente sempre que se conectar. Outra funcionalidade do DHCPv4, é fornecer ao *host* informações adicionais, como a máscara de subrede, o endereço do primeiro roteador e o endereço de seu servidor DNS local. Torres [16] explica que, quando um novo *host* é conectado à rede e está ajustado para receber configurações automaticamente via DHCPv4, ele não receberá o endereço de imediato, antes disso haverá um processo que é mostrado na Figura 5.

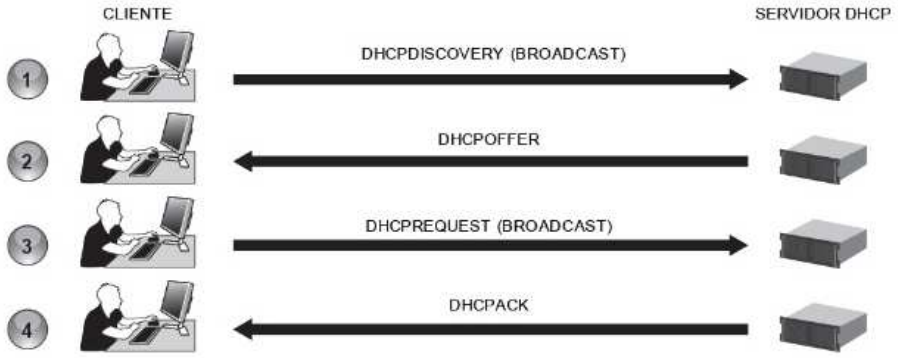


Figura 5. Requisição DHCP [16]

Ainda de acordo com Torres [16], esse processo acontece da seguinte forma:

a) A máquina cliente envia um pacote de dados em broadcast chamado *DHCPDISCOVERY* que é enviado utilizando o protocolo UDP.
b) O servidor DHCPv4 responderá com um pacote chamado *DHCPOFFER*, que conterá o endereço MAC do cliente, o endereço de IP oferecido pelo servidor DHCP, o endereço e a máscara de rede do servidor DHCPv4, além do tempo que o cliente poderá utilizar o endereço oferecido.
c) A máquina cliente enviará um pacote de dados via broadcast chamado *DHCPREQUEST* e, mesmo que haja mais de um servidor na rede, o cliente só aceitará um pedido.
d) O servidor DHCPv4 envia um pacote de confirmação chamado *DHCPACK* confirmando a configuração.

Se tratando do DHCPv6, definido pela RFC 3315 [23], a principal diferença entre ele e o DHCPv4 é que no DHCPv6 existem dois tipos de configuração [3]:

- ***Stateless*** – este modo aproveita um tipo de configuração nativa do IPv6 conhecida como SLAAC, onde as máquinas fazem suas configurações de endereços automaticamente, na qual a máquina executando o serviço não mantém nenhum registro de endereços. Nesse modo cabe

ao servidor DHCP oferecer informações complementares que são importantes para a rede como: endereço de servidor DNS, servidor de tempo, dentre outros.

- ***Stateful*** – esse modo já mais parecido com o DHCPv4, onde servidor acaba provendo todas as informações de endereçamento, já que o escopo configurado explicitamente e também é mantido um registro com informações relacionadas aos endereços. O pedido DHCPv6 funciona de forma similar ao DHCPv4, por meio de quatro mensagens básicas que são [3]:

  a) ***Solicit*** – um cliente envia uma mensagem *Solicit* para localizar servidores

  b) ***Advertise*** – um servidor envia uma mensagem *Advertise* para indicar que está disponível para o serviço DHCP, em resposta a uma mensagem *Solicit* recebida de um cliente.

  c) ***Request*** – um cliente envia uma mensagem *Request* para solicitar parâmetros de configuração, incluindo endereços IP, a partir de um servidor específico.

  d) ***Reply*** – um servidor envia uma mensagem *Reply* contendo endereços e parâmetros de configuração atribuídos em resposta a uma solicitação, solicitação, renovação, reenviar mensagem recebida de um cliente.

De acordo com a Equipe IPv6.Br [24], o DHCPv6 ainda possui uma opção que é específica desta versão do protocolo, o *Prefix Delegation*, onde sua função é informar prefixos de rede a roteadores solicitantes.

O tipo de configuração DHCPv6 *Stateful*, foi o escolhido para ser utilizado no trabalho, devido ao fato de que ele mostra o escopo de endereços definidos explicitamente e assim é possível verificar se as configurações de rede definidas no servidor estão realmente sendo recebidas pelos clientes.

2.4.1 DHCP *RELAY AGENT*

Um agente de retransmissão ou *Relay Agent* DHCP é qualquer host que encaminha pacotes DHCP entre clientes e servidores e são usados para encaminhar pedidos e respostas quando eles não estão na mesma rede física. O encaminhamento do agente de retransmissão é distinto do encaminhamento normal de um roteador IP, onde os datagramas IP são alternados entre as redes de forma um pouco transparente. Em contrapartida, os agentes de retransmissão recebem mensagens DHCP e, em seguida, geram uma nova mensagem DHCP para enviar em outra interface. O agente de retransmissão define o endereço do *gateway* e, se configurado, adiciona a opção de informações do agente de retransmissão no pacote e encaminha-o para o servidor DHCP [25].

A Figura 6 mostra como seria uma topologia utilizando *Relay Agent*:

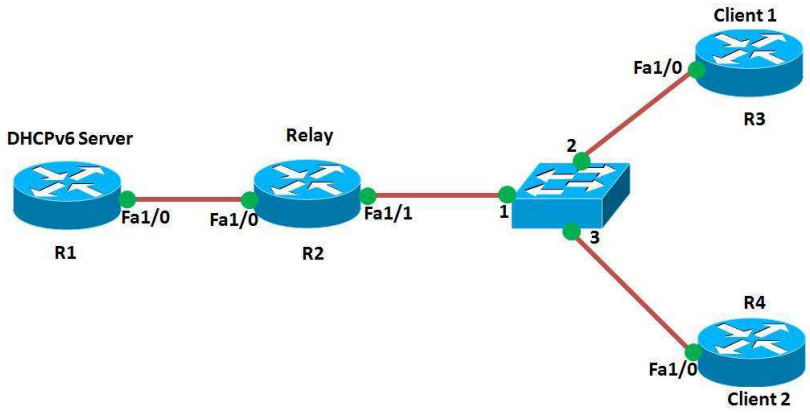


Figura 6. Roteador Intermediário funcionando como *Relay Agent* [26]

Em ambas as versões, DHCPv4 e DHCPv6, esta funcionalidade basicamente atua da mesma forma, havendo apenas mudanças no modo de configurar cada uma delas. Como por exemplo, neste trabalho, para configurar um ativo de rede da marca Cisco como *Relay Agent*, no DHCPv4 foi utilizado o comando *ip helper-address <IP address do servidor>*, enquanto que para o DHCPv6, o comando muda para *ipv6 dhcp relay destination <ipv6 address do servidor> <interface conectada ao servidor>*, ambos inseridos na interface que conecta o *Relay Agent* à rede local.

2.5 ICMPv4 E ICMPv6

O protocolo ICMP, estabelecido pela RFC 792 [27], é um protocolo que funciona na camada de rede, tem a função de informar erros e fazer testes na *Internet*, como por exemplo, nos testes de conectividade, atuando por trás do comando *ping*. Assim como o DHCP, o ICMP também possui duas versões que atuam de acordo com a versão do protocolo IP utilizada, sendo elas: a ICMPv4 e a ICMPv6. Iniciando pelo ICMPv4, suas mensagens são enviadas em várias situações, por exemplo: quando um datagrama não pode chegar ao destino, quando o *gateway* não possui a capacidade de *buffer* para encaminhar um datagrama ou quando o *gateway* pode direcionar o *host* para enviar tráfego em uma rota mais curta [27].

De acordo com Torres [16], o ICMPv4 é somente um mecanismo usado para informar à máquina transmissora da ocorrência de um erro com o datagrama enviado, por meio de mensagens enviadas pelos roteadores da rede, entretanto, ele não se preocupa em corrigir o erro e muito menos em verificar a integridade dos datagramas que circulam pela rede e, em

relação às mensagens ICMPv4, Tanenbaum [7] frisa que existe pelo menos uma dezena de tipos definidos e faz uma breve descrição dos mais importantes na Tabela 6:

Tabela 6. Principais tipos de mensagens ICMPv4 [adaptado 7]

Tipo de Mensagem	Descrição
Destination Unreachable	Não foi possível entregar o pacote
Time Exceeded	O campo Time to Live chegou a 0
Parameter Problem	Campo de cabeçalho inválido
Source Quench	O *host* deve desacelerar sua operação
Redirect	O pacote pode ter sido roteado incorretamente
Echo	Pergunta à máquina se ela está ativa
Echo Reply	Resposta da máquina dizendo que está ativa

Além disso, Tanenbaum [7] ainda se aprofunda mais na descrição das mensagens ICMPv4 citadas Tabela 6:

- ***Destination Unreachable*** – é usada quando a subrede ou um roteador não consegue localizar o destino.
- ***Time Exceeded*** – é enviada quando um pacote é descartado porque seu contador chegou a zero. Esse evento é um sintoma de que os pacotes estão entrando em *loop*, de que há um enorme congestionamento ou de que estão sendo definidos valores muito baixos para o *timer*.
- ***Parameter Problem*** – indica que um valor inválido foi detectado em um campo de cabeçalho. Esse problema indica a existência de um *bug* no software IP do *host* transmissor ou, possivelmente, no *software* de um roteador pelo qual o pacote transitou.
- ***Source Quench*** – é usada para ajustar os *hosts* que estivessem enviando pacotes demais. Quando essa mensagem é recebida, um *host* deve desacelerar sua operação.
- ***Redirect*** – é usada quando um roteador percebe que o pacote pode ter sido roteado incorretamente. Ela é usada pelo roteador para informar ao *host* transmissor o provável erro.

- ***Echo e Echo Reply*** – são usadas para verificar se um determinado destino está ativo e acessível. Ao receber a mensagem *Echo*, o destino deve enviar de volta uma mensagem *Echo Reply*.

Quanto ao ICMPv6, Torres [16] afirma que este funciona de forma idêntica ao seu antecessor ICMPv4, entretanto Brito [3] ressalta que o ICMPv6 é extremamente para a operacionalização do IPv6, pois compreende funcionalidades de comunicação entre máquinas vizinhas que são necessárias para o bom funcionamento da rede. O ICMPv6 engloba outros protocolos como, por exemplo, o NDP, um protocolo responsável por várias funcionalidades e de grande importância nas redes IPv6, inclusive ele substitui o protocolo ARP, utilizado em redes IPv4.

Além disso, Torres [16] também afirma que as principais diferenças entre as duas versões do ICMP, estão nos códigos das mensagens ICMPv6, que agora podem ser divididas em duas categorias mensagens de informação e mensagens de como mostradas na tabela 5 e 6, criadas baseadas na RFC 4443 [28]:

Tabela 7. Mensagens de Informação do ICMPv6 [28]

Tipo	Grupo	Código	Descrição
128	*Echo Request*	0	Utilizado no *ping*
129	*Echo Reply*	0	Utilizado no *ping*
-		-	Reservado para novas mensagens de informação

Tabela 8. Mensagens de Erro do ICMPv6 [28]

Tipo	Grupo	Código	Descrição
1	Destino Inalcançável	0	Sem rota para o destino
		1	Comunicação com destino administrativamente proibida
		2	Além do escopo do endereço da origem
		3	Endereço Inalcançável
		4	Porta Inalcançável

		5	Falha na política de ingresso/egresso
		6	Destino rejeitado
2	Pacote muito grande	0	Pacote Ultrapassou o MTU
3	Tempo excedido	0	Limite de saltos excedido
		1	Limite de remontagem de fragmentação excedido
4	Problema de Parâmetro	0	Campo inválido no cabeçalho IPv6
		1	Próximo cabeçalho inválido
		2	Opções inválidas
		-	Reservado para novas mensagens de erro

2.6 DNS

Segundo Tanenbaum [7], o DNS é responsável principalmente por mapear nomes de *hosts* e destinos de mensagens de correio eletrônico em endereços IP, mas também pode ser usado para outros objetivos.

Já a Equipe IPv6.Br [24], se refere ao DNS, como sendo uma imensa base de dados distribuída em uma estrutura hierárquica, utilizada para a tradução de nomes de domínios em endereços IP e vice-versa, na qual os dados associados aos nomes de domínio estão contidos em Registro de Recursos ou RRs, dentre os quais, os mais comuns estão listados na Tabela 9:

Tabela 9: Registro de Recursos do DNS [24]

RR	Descrição
SOA	Indica a autoridade sobre uma zona
NS	Indica um servidor de nomes para uma zona
A	Mapeamento de nome para endereço (IPv4).

AAAA	Mapeamento de nome para endereço (IPv6)
MX	Indica um servidor de e-mail
CNAME	Mapeia um nome alternativo (apelido)
PTR	Mapeamento de endereço para nome

O DNS tem três componentes principais, segundo Forouzan que são [10]:

a) **Espaço de nomes de domínio** – desenvolvido para oferecer uma estrutura hierárquica de nomes de espaço, onde, neste tipo de hierarquia, os nomes são definidos numa estrutura de árvore. Conceitualmente, cada nó e folha da árvore nomeia um conjunto de informações e são feitas operações de consulta para extrair tipos específicos de um determinado conjunto.

b) **Servidores de nome** – são programas de servidor que detêm informações sobre a estrutura da árvore de domínio e a informação do conjunto. Além disso, podem armazenar em cache a estrutura ou definir informações sobre qualquer parte da árvore de domínio e possuem ponteiros para outros servidores de nomes que podem ser usados para levar a informações de qualquer parte da árvore de domínio.

c) ***Resolvers*** – são programas que acessam o servidor de nomes mais próximo com uma consulta de mapeamento. Caso o servidor tenha a informação desejada ele entrega ao *resolver*. Do contrário, ele entrega a consulta a outros servidores DNS da rede para que algum deles resolva o nome em IP ou vice-versa.

Se tratando do protocolo IPv6, para que o DNS trabalhe com a versão 6 do protocolo Internet, algumas mudanças foram definidas na RFC 3596 [29]. Uma delas foi que, um novo tipo de RR foi criado para armazenar os endereços IPv6 de 128 bits, o AAAA. Sua função é a de traduzir nomes para endereços IPv6, de forma equivalente à do registro do tipo A no IPv4 [24]. Outra mudança foi que, para resolução reversa, foi adicionado ao registro PTR o domínio ip6.arpa, responsável por traduzir endereços IPv6 em nomes. Em sua representação, o endereço é escrito com o bit menos significativo colocado mais à esquerda, de modo que cada dígito hexadecimal seja separado pelo caractere ponto "." [24].

Nos próximos tópicos serão mostradas algumas tecnologias que fazem parte dos cenários deste trabalho, bem como uma breve explanação sobre mecanismos de transição de IPv4 para IPv6.

2.7 VLANS

Uma VLAN é um grupo de dispositivos em uma ou mais LANs que estão configuradas para se comunicar como se estivessem conectadas ao mesmo fio, quando na

verdade elas estão localizadas em vários segmentos de LAN diferentes e, como são baseadas em conexões lógicas em vez de físicas, elas são extremamente flexíveis e além disso as VLANS definem domínios de *broadcast* em uma rede de camada de enlace, algo que normalmente é delimitado por roteadores [30].

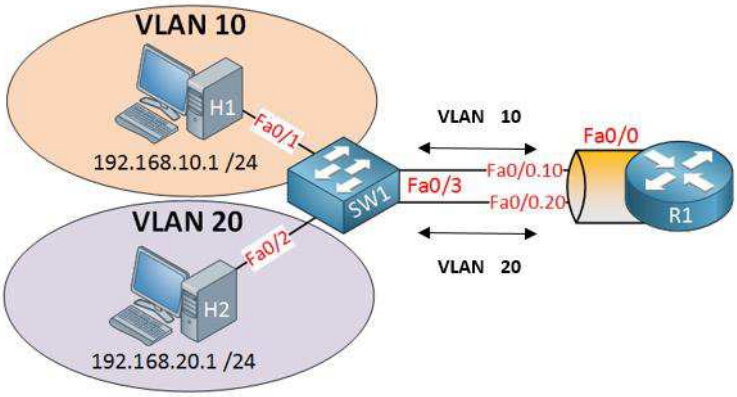


Figura 7: Topologia *" Router on a Stick"* utilizando VLANs [adaptado 31]

A Figura 7, mostra uma topologia de rede, conhecida como "*Router on a Stick*", onde há duas VLANs, VLAN 10 e VLAN 20. Pode-se notar que, apesar de termos um único meio físico conectando o *switch* SW1 ao roteador R1, característica deste tipo de topologia, existe tráfego de dados em ambas as VLANs. Isso ocorre porque existe um padrão conhecido como IEEE 802.1Q ou *DOT1Q*, que permite que haja tráfego, não de apenas duas, mas, de várias VLANS por meio de uma única interface, desde que ela esteja configurada como *trunking* [32]. Os *links trunk* fornecem a identificação de *VLAN* para quadros que viajam entre os *switches* ou entre *switches* e roteadores e devem ser configurados para permitir o *trunking* em cada extremidade do link [31].

A topologia mostrada na Figura 7, é muito similar ao Cenário 1, mostrado no tópico 3.1 deste documento, onde, para que o roteador possa receber os quadros e saber como encaminhar corretamente os pacotes à sua respectiva VLAN, é necessário utilizar uma configuração que permite que uma interface física possa atuar como uma ou várias interfaces virtuais, as quais damos o nome de "subinterfaces" e em cada uma delas inserir uma *tag DOT1Q* (etiqueta) com o número da VLAN para qual o pacote deve ser entregue.

2.8 MECANISMOS DE TRANSIÇÃO DE IPv4 PARA IPv6

De acordo com a RFC 4213 [33], a chave para uma transição IPv6 bem-sucedida é a compatibilidade com a grande base instalada de *hosts* IPv4 e roteadores. Mantendo a

compatibilidade com o IPv4 ao implantar o IPv6 agilizará a tarefa de transição da Internet para IPv6.

Segundo o IPv6.Br [34], o IPv4 e o IPv6 não são diretamente compatíveis, já que o IPv6 não foi projetado para ser uma extensão, ou complemento, do IPv4 e sim um substituto para resolver o problema do esgotamento de endereços. Embora não interoperem, os protocolos podem funcionar em paralelo nos mesmos equipamentos, possibilitando realizar a transição de forma gradual.

Brito [3] complementa dizendo que, para não haver impacto na percepção do conteúdo existente na Internet por parte dos usuários, será crucial a adoção de mecanismos de transição para tornar possível a interoperabilidade IPv4-IPv6, já que esses protocolos não são diretamente compatíveis entre si. Esses mecanismos são apresentados e brevemente descritos a seguir:

a) **Pilha Dupla** – técnica que consiste em instalar e operacionalizar ambos os protocolos IPv4 e IPv6 nas máquinas da rede e demais dispositivos de maneira gradativa, o que implica na existência de duas redes em paralelo. Nesse caso, os nós que estejam operando em Pilha Dupla podem conversar com nós que operem apenas com IPv4 *ou* IPv6 [3].

b) **Tunelamento** – é uma estratégia usada quando dois computadores usando IPv6 querem se comunicar entre eles por meio de um caminho que utiliza o IPv4. Dessa forma, o pacote IPv6 é encapsulado num pacote IPv4 quando entrar na região e, ao sair dela, é desencapsulado em IPv6. O processo também pode ocorrer se tratando de nós IPv4 querendo se comunicar por meio de um meio que utilize IPv6 [10]. Exemplos de técnicas de tunelamento são: túnel *6in4, 6to4*, *Tunnel Broker*, *ISATAP*, *Teredo*, dentre outros.

c) **Tradução** – Permitem que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes [34].

2.8.1 MECANISMO DE TRANSIÇÃO UTILIZADO

O mecanismo de transição Pilha Dupla, foi o escolhido para ser usado neste projeto, por se tratar de uma abordagem mais direta para introduzir nós IPv6 em uma rede que já possui *hosts* IPv4. Além disso, o IPv6.BR [34] alerta que, na atual fase de implantação do IPv6, não é aconselhável ter *hosts* com suporte apenas à versão 6 do protocolo IP, visto que muitos serviços e dispositivos na Internet ainda trabalham somente com IPv4 e afirma que, manter o IPv4 já existente funcionando de forma estável e implantar o IPv6 nativamente para que coexistam nos mesmos equipamentos, é a forma básica escolhida para a transição entre as versões do protocolo IP na *Internet*.

Sendo assim, entrando em mais detalhes sobre esse mecanismo, os nós que fornecem implementações IPv4 e IPv6 completas são chamados "nós IPv6 / IPv4" e podem interoperar diretamente com nós IPv4 usando pacotes IPv4 e também interagem diretamente com nós IPv6 usando pacotes IPv6 [33] e está ilustrado na Figura 8.

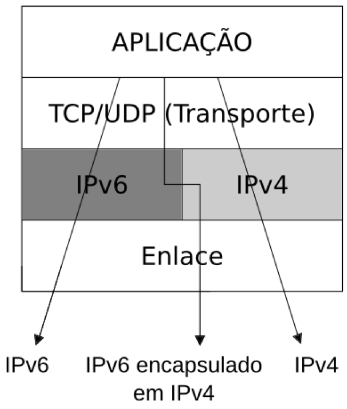


Figura 8: Funcionamento da Pilha Dupla [34]

Se tratando da questão de endereçamento, como os nós suportam ambos os protocolos, os nós IPv6/IPv4 podem ser configurados com os endereços IPv4 *e* IPv6, tanto estaticamente, quanto por meio uso de servidores DHCP, como será visto no capítulo 3.

Outro fator que deve ser levado em consideração se tratando do mecanismo Pilha Dupla, é o DNS. Como dito anteriormente, um novo tipo de *RR* chamado "AAAA" foi definido para endereços IPv6. Desde então, os nós IPv6/IPv4 devem poder interoperar diretamente com o IPv4 e os nós IPv6 devem fornecer bibliotecas de resolução capazes de lidar com os registros IPv4 "A", bem como com registros IPv6 "AAAA" [30] e, além disso, o protocolo por meio do qual é feita a consulta DNS não interfere na resposta. Ao receber endereços IPv6 e IPv4 como resposta a uma consulta no DNS a aplicação decide qual protocolo usar. Normalmente a preferência é pelo protocolo IPv6 e, em caso de falha, tenta-se o IPv4 [17].

3 PROJETO

O primeiro passo para execução do projeto, foi verificar a disponibilidade dos equipamentos, neste caso, se haveria equipamentos que poderiam ser usados para a montagem das topologias e a realização das configurações necessárias para os testes. Constatou-se que no laboratório de Telecomunicações do curso, havia quatro dispositivos disponíveis, um roteador e dois *switches* da marca Cisco integrados ao *rack*, além de mais um roteador sobressalente, também da marca Cisco.

Sendo assim, foi possível seguir para a próxima etapa que consistia em verificar se os dispositivos disponíveis atendiam aos requisitos de *software* necessários para as configurações em Pilha Dupla. Os *switches* e roteadores Cisco, são equipamentos de rede gerenciáveis, ou seja, além de fazer a conexão entre os dispositivos também contam com ferramentas que permitem administrá-los e já dão suporte às configurações de IPv4, contudo, foi preciso verificar se as versões dos *firmwares* davam suporte à tecnologia IPv6 e seus serviços. Para isso checou-se, em cada um dos dispositivos, o modelo do equipamento e a versão da IOS utilizada.

Verificando as versões de IOS mostradas na Tabela 10, focando principalmente nas dos roteadores, foi identificado que os IOS's dos roteadores oferecem suporte à configuração de endereçamento e aos serviços necessários de IPv6 para este projeto, baseado no próprio site da Cisco [35], que contém informações sobre as versões de IOS's que atendem à tecnologia IPv6. Os *switches* utilizados, apesar de oferecerem suporte ao IPv6, por se tratarem de *switches* que também atuam na camada de *internet*, servirão apenas para encaminhar os quadros *ethernet* por meio da rede.

Tabela 10: Modelos dos dispositivos e versões de IOS

Nome do Dispositivo	**Modelo**	**Versão do *Firmware* (*IOS*)**
R-LabTelecom	Cisco 2800 *series*	Cisco *IOS Software*, *Version* 12.4 (24)
R2-LabTelecom	Cisco 1841 *series*	Cisco *IOS Software*, *Version* 12.4 (9)
SW-LabTelecom-1	Cisco *Catalyst* 3750 *series*	Cisco *IOS Software*, *Version* 12.2 (50)

SW-LabTelecom-2	Cisco *Catalyst* 3750 *series*	Cisco *IOS Software*, *Version* 12.2 (50)

Após certificar-se que os requisitos de *hardware* e *software* para a execução do projeto foram atendidos, deu-se início à uma abordagem mais prática, onde foi feita a montagem das topologias e criada uma rede separada para testes, para observar como seria a atuação desta rede em Pilha Dupla, utilizando dois cenários.

No primeiro cenário a topologia é composta apenas pelos equipamentos SW-LabTelecom-1, SW-LabTelecom-2, R-LabTelecom e mais duas máquinas com sistema operacional *Windows* no papel de *hosts*. Neste cenário foi observado como ocorreria a distribuição de endereços IPv6 do tipo *global-unicast* e de endereços IPv4 privados, tornando o R-LabTelecom um servidor DHCP local responsável por distribuir endereços IPv4 e IPv6 simultaneamente aos dois *hosts* ligados ao *switch* SW-LabTelecom-2, em uma VLAN separada, via DHCPv4 e DHCPv6. Em seguida, verificou-se se havia conectividade entre os *hosts* em ambas as pilhas.

No segundo cenário, foi acrescentado à topologia o roteador R2-LabTelecom ligado ao R-LabTelecom por meio de uma rede externa, sendo que, o R2-LabTelecom, atuaria como um *Relay Agent*, apenas intermediando as requisições de endereços IPv4 e IPv6 que ainda estão vindo do R-LabTelecom que foi mantido como servidor DHCP para as duas pilhas. Assim como no primeiro cenário, havia dois *hosts* para receber os endereços IPv4 e IPv6 e, em seguida, verificar será verificada a existência de conectividade entre eles.

O Cenário 1 tem como objetivo apenas, observar se as configurações de DHCP funcionarão corretamente e se há comunicação entre os *hosts*, ocorrendo apenas em um ambiente local, antes da implementação do próximo cenário. Já o Cenário 2, almeja retratar como funcionaria a distribuição de endereços IP na rede, de uma forma mais próxima da realidade da comunicação de dados do curso de Engenharia da Computação, que ocorre obtendo endereços IP vindos de um servidor DHCP que se encontra no NTI da UEMA, no caso em outro prédio, por uma rede externa, e são encaminhados para a rede local por meio de um outro roteador, na função de *Relay Agent*, que está localizado no laboratório de Telecomunicações do curso no CCT.

Deve-se levar em conta que os dispositivos ligados integrados ao *rack* do laboratório de Telecomunicações possuem redes IPv4 ativas e que atendem ao curso de Engenharia da Computação fornecendo acesso à *Internet*. Por essa razão, optou-se por criar

duas VLANs apartadas, de números 500 e 600, para serem utilizadas para os testes, evitando assim possíveis impactos nas redes existentes durante os testes.

Os tópicos a seguir mostram detalhadamente como foram os processos de montagem e configuração dos equipamentos Cisco da topologia (*switches* e roteadores), além da verificação de endereçamento via servidor DHCP nos *hosts* e testes de conectividade entre eles.

3.1 CENÁRIO 1: REDE UTILIZANDO SERVIDOR DHCP LOCAL EM PILHA DUPLA

No Cenário 1, a meta é fazer com que a rede de testes utilizada para o projeto funcione utilizando o roteador R-LabTelecom como servidor DHCP local, de ambos os endereços IPv4 e IPv6, para fazer a distribuição dos IPs aos *hosts* conectados à VLAN 500, que tem portas de acesso configuradas no *switch* SW-LabTelecom-2.

O primeiro passo foi fazer a montagem da topologia física. Entretanto, a topologia do laboratório de Telecomunicações já utiliza, localmente, o modelo "*Router on a Stick*", uma topologia apropriada para situações em que se deseja utilizar apenas um roteador para atender mais de uma VLAN, então, nesse caso, não houve necessidade de alterar a posição dos equipamentos do *rack* e sim, somente configurar a VLAN de testes nos *switches*, que será demonstrada, a seguir, no tópico 3.1.1.

A Figura 9 nos dá uma ideia de como estes equipamentos estão dispostos fisicamente:

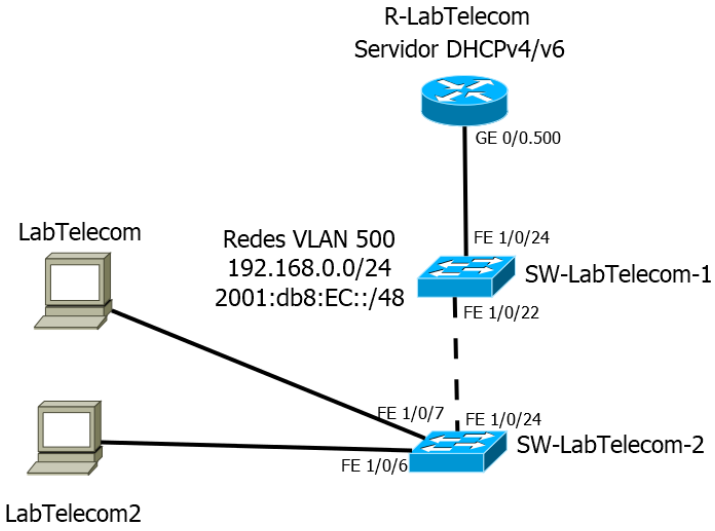


Figura 9. Topologia do Cenário 1

3.1.1 CONFIGURANDO OS *SWITCHES*

Como mencionado no tópico 3, os equipamentos utilizados para montagem das topologias se encontram no laboratório de Telecomunicações do curso de Engenharia da Computação e neles já estão configuradas algumas redes que fornecem *Internet* aos usuários. Nesse caso, para evitar que os testes feitos neste projeto de alguma maneira afetem o funcionamento dessas redes, optou-se, primeiramente, por criar uma VLAN separada para testes com o número 500, chamada *DUAL STACK* IPv4/IPv6 em ambos os *switches*.

O primeiro *switch* a serem feitas as configurações da VLAN 500 foi o SW-LabTelecom-1, no qual apenas houve o processo de criação, porém não foram designadas a ela portas de acesso, devido a sua função ser apenas o encaminhamento dos quadros *Ethernet* por meio da porta FE 1/0/22 que está conectada ao SW-LabTelecom-2 na porta FE 1/0/24, ambas configuradas em modo *trunk*.

```
SW-LabTelecom-1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2
90   VLAN0090                         active
91   VLAN0091                         active
92   VLAN0092                         active
208  CCT                              active    Fa1/0/13, Fa1/0/14
500  DualStack IPv4/IPv6              active
```

Figura 10. Criação da VLAN 500 no switch SW-LabTelecom-1

Partindo agora ao SW-LabTelecom-2, a configuração é basicamente a mesma, por se tratarem de dois *switches* de mesmo modelo de equipamento e mesma versão de *firmware*, contudo, neste *switch*, foram designadas portas de acesso que farão parte da VLAN 500, as quais foram escolhidas as portas FE 1/0/6, FE 1/0/7¸ FE 1/0/8, FE 1/0/9 e FE 1/0/10. Vale ressaltar, que nestes testes estaremos utilizando apenas duas ou três portas, mas, tendo em vista um possível aumento no número de equipamentos dessa rede, foram reservadas cinco portas de acesso. A Figura 11, também utilizando o comando *show vlan brief*, mostra que a VLAN 500 foi criada com sucesso, tem status *active*, e também quais portas são pertencentes a ela.

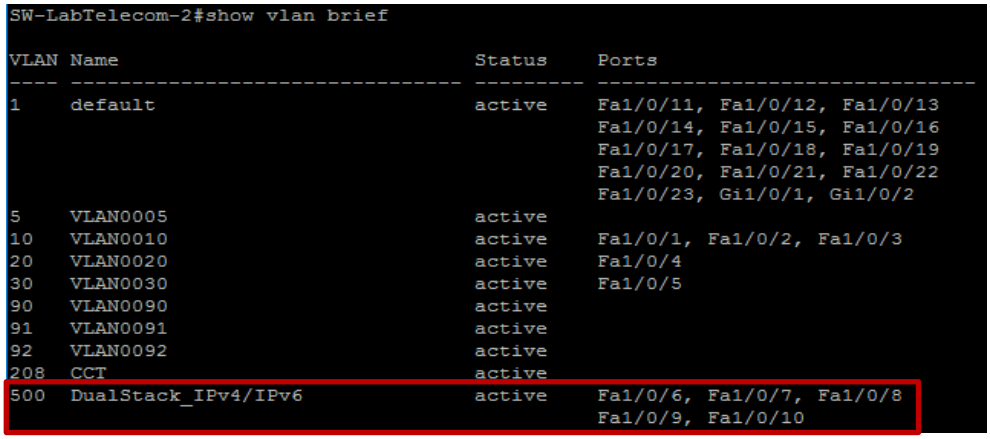


Figura 11. Criação da VLAN 500 e designação das portas de acesso em SW-LabTelecom-2

Agora, tendo os dois *switches* da rede configurados, o próximo passo é configurar o roteador R- LabTelecom como servidor DHCP (IPv4 e IPv6) para fornecer os endereços aos *hosts* conectados às portas designadas à VLAN 500 em SW-LabTelecom-2.

3.1.2 CONFIGURANDO R-LABTELECOM

O roteador R-LabTelecom é o equipamento atualmente responsável por fazer o roteamento entre as redes pertencentes ao curso de Engenharia de Computação servindo como *gateway* entre elas e também fazendo a conexão com o NTI, de onde é conectado à *Internet*.

Este equipamento é composto por apenas duas interfaces físicas que são: a GE 0/0 e a GE 0/1. A interface GE 0/1 é quem faz a conexão com a rede externa. Nesse caso, sobra apenas a interface GE 0/0, que foi dividida em uma quantidade de subinterfaces equivalente ao número de redes locais que estão separadas por meio de VLANs. Devido a isso, a primeira configuração feita no roteador antes de se configurar o DHCP foi criar a uma nova subinterface, a GE 0/0.500, que seria instruída a encaminhar apenas pacotes da VLAN de testes utilizando o comando *encapsulation dot1Q 500*.

A seguir, foi feito endereçamento da interface, utilizando as redes 192.168.0.0 /24 para IPv4 e 2001:db8:EC:: /48 para IPv6, atribuindo à esta interface o segundo endereço IP válido de cada uma delas, como mostrado na Figura 12. Um fato importante é que nos roteadores Cisco, o IPv6 não vem habilitado por padrão, então, para que todas as configurações possam funcionar, é necessário habilitá-lo utilizando, no modo de configuração do roteador, o comando *ipv6 unicast-routing*.

```
!
interface GigabitEthernet0/0.500
 encapsulation dot1Q 500
 ip address 192.168.0.2 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:EC::2/48
```

Figura 12. Criação da Subinterface GE 0.0/500 e atribuição de endereços IP em R-LabTelecom

Podemos notar na Figura 12 que no endereçamento IPv6, além do endereço *global unicast* 2001:db8:EC::2 /48, também houve a atribuição de um endereço de IPv6 *link-local* fe80::2 para facilitar a visualização do endereço do *gateway* na parte de atribuição do DHCP nos *hosts*.

Após a configuração de endereçamento do R-LabTelecom, que funcionará como servidor de endereços, foi feita a configuração do DHCP. Começando pelo DHCPv4, no modo de configuração do R-LabTelecom, uma faixa de endereços foi excluída por meio do comando *ip dhcp excluded-address*, para que estes não entrem nos endereços que serão atribuídos aos clientes DHCP, já que serão utilizados para dispositivos que necessitem de endereçamento estático, evitando assim, a duplicidade de endereços.

Em seguida, foi designado um escopo de endereços DHCP, de nome IPv4, com o comando *ip dhcp pool <nome do pool>*, na qual é fornecida a rede e máscara, bem como o *gateway* padrão, o servidor DNS e o domínio pertinentes aos clientes que fizerem requisições de endereçamento via DHCPv4. Feito isso os clientes conectados à VLAN 500, conectados ao SW-LabTelecom-2 por meio das portas de acesso atribuídas, ao escolherem o endereçamento dinâmico, receberão todas as configurações de endereçamento que foram atribuídas na configuração do DHCPv4, que pode ser vista na Figura 13.

A configuração do DHCPv6, por outro lado, tem algumas diferenças se comparada com o DHCPv4, ela pode ser *Stateful* ou *Stateless*, porém como desejamos mostrar explicitamente o prefixo configurado, foi adotado o tipo *Stateful* [36].

```
ip cef
ip dhcp excluded-address 192.168.0.1 192.168.0.5
!
ip dhcp pool IPv4
   network 192.168.0.0 255.255.255.0
   default-router 192.168.0.2
   dns-server 192.168.0.5
   domain-name engcomp_dualstack.uema.br
!
!
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool IPv6
 address prefix 2001:DB8:EC::/48
 dns-server 2001:DB8:EC::5
 domain-name engcomp_dualstack.uema.br
!
```

Figura 13. Configuração do DHCPv4 e DHCPv6 em R-LabTelecom

Na configuração do DHCPv6 mostrada na Figura 13, pode-se notar que na criação do *pool* IPv6, não é mais necessário indicar o *default-router* como no DHCPv4, mas que as outras informações, como servidor DNS e domínio (*domain-name*) ainda permanecem iguais, entretanto, o comando para indicar a rede mudou de *network* para *address prefix*, sendo este o comando utilizado para declarar explicitamente o escopo de endereços *global únicas* no DHCPv6 no modo *Stateful*. Além disso, a configuração do DHCPv6 se estende até a interface na qual os clientes farão as requisições.

```
interface GigabitEthernet0/0.500
 encapsulation dot1Q 500
 ip address 192.168.0.2 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:EC::2/48
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 dhcp server IPv6
```

Figura 14. Configuração do DHCPv6 na subinterface GE 0/0.500 em R-LabTelecom

Neste caso, configurações adicionais, como mostrado na Figura 14, foram feitas na interface GE 0/0.500 para que os clientes possam receber as configurações de endereçamento corretamente. Uma delas é a ativação do protocolo IPv6 na interface, com comando *ipv6 enable*, seguido de mais dois comandos que são: *ipv6 dhcp server <nome do pool>* e *ipv6 nd managed-config-flag*. O primeiro comando serve para habilitar o servidor DHCPv6 na interface e isso também irá indicar o endereço de *link-local* dessa interface como *gateway* padrão da rede e o segundo serve para instruir os clientes a receber todas as suas configurações de endereço por meio de *DHCPv6* do tipo *Stateful*, dessa forma é possível ver os prefixos explicitamente no formato *global unicast* [36].

Feitas estas configurações, a rede do Cenário 1 está preparada para fazer o endereçamento IPv4 e IPv6 via servidor DCHP para os clientes conectados à VLAN *500*, faltando apenas configurações nos *hosts* e testes de conectividade entre eles para comprovar que a comunicação em ambas as pilhas foi estabelecida corretamente.

3.1.3 CONFIGURAÇÃO DOS *HOSTS* DA REDE

Para representar os hosts da rede de testes, foram utilizadas duas máquinas com sistema operacional *Windows* 10, nomeadas de LabTelecom e LabTelecom2. Normalmente, as máquinas *Windows* já vêm com a opção de endereçamento automático habilitada por padrão em ambas as pilhas, mas caso esteja sendo utilizado o endereçamento estático, basta apenas habilitá-la nas propriedades de adaptador *ethernet*.

Acessando o *prompt* de comando ou "*cmd*" do *Windows*, por meio do comando *ipconfig*, constatou-se que os endereços IPv4 estavam sendo recebidos de forma correta como se era esperado nos dois *hosts.* Além disso, haviam sido recebidas todas as informações relativas à configuração do pool *DHCP* IPv4 configurada no roteador R-LabTelecom, como o nome do domínio e *gateway* padrão.

As Figuras 15 e 16 mostram as configurações de endereços via DHCPv4:

```
C:\Users\LabTelecom>ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet:

   Sufixo DNS específico de conexão. . . . . : engcomp_dualstack.uema.br
   Endereço IPv6 de link local . . . . . : fe80::352c:60d5:6096:e7c0%12
   Endereço IPv4. . . . . . . . . . . . . . : 192.168.0.7
   Máscara de Sub-rede . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . : 192.168.0.2
```

Figura 15. Endereçamento IP recebido via DHCPv4 em LabTelecom

```
C:\Users\LabTelecom2>ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet:

   Sufixo DNS específico de conexão. . . . . : engcomp_dualstack.uema.br
   Endereço IPv6 de link local . . . . . : fe80::d163:1bc:f331:7b26%9
   Endereço IPv4. . . . . . . . . . . . . . : 192.168.0.6
   Máscara de Sub-rede . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . : 192.168.0.2
```

Figura 16. Endereçamento IP recebido via DHCPv4 em LabTelecom2

Como os endereços IPv4 foram recebidos com sucesso, agora é necessário verificar se a pilha TCP/IPv6 também está recebendo as configurações de endereçamento via DHCPv6. Da mesma forma que o IPv4, basta apenas habilitar os *hosts* para recebimento de endereços de IP nas propriedades de adaptadores de rede, só que dessa vez na pilha TCP/IPv6.

Então, também utilizando o comando *ipconfig* no *prompt* de comando do *Windows*, foi possível verificar que os *hosts*, assim como o endereçamento IPv4, também estavam recebendo o endereçamento IPv6. Desse modo, podemos constatar que o servidor DHCP idealizado para funcionar localmente, em pilha dupla, consegue endereçar os *hosts* com ambos as versões do protocolo IP de forma correta, restando agora, verificar se esses endereços atribuídos automaticamente, estabelecem comunicação entre si, por meio de testes de conectividade.

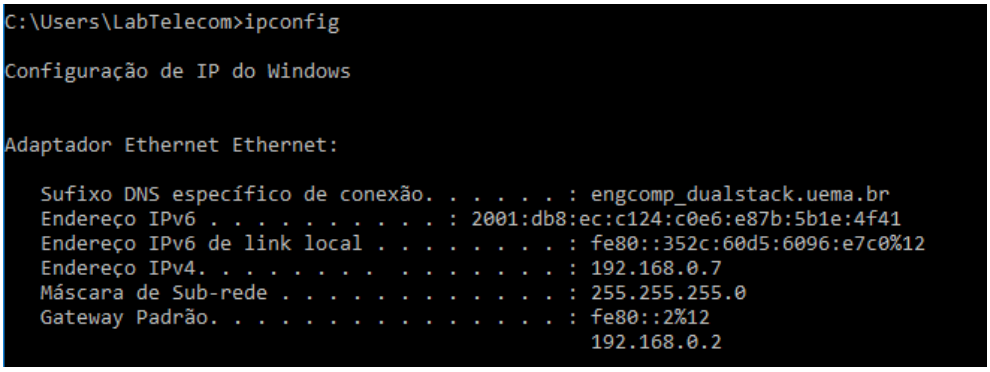


Figura 17. Endereçamento IPv6 recebido via DHCPv6 em LabTelecom

Figura 18. Endereçamento IPv6 recebido via DHCPv6 em LabTelecom2

3.1.4 TESTES DE CONECTIVIDADE ENTRE OS HOSTS

Para testar a conectividade entre os hosts, utilizamos o comando *ping*, o qual verificou se os mesmos estabeleciam comunicação entre si. Primeiramente os testes foram

feitos com os endereçamentos IPv4 como mostram as Figuras 19 e 20. Primeiro os pacotes são enviados de LabTelecom para Labtelecom2, em seguida de forma contrária.

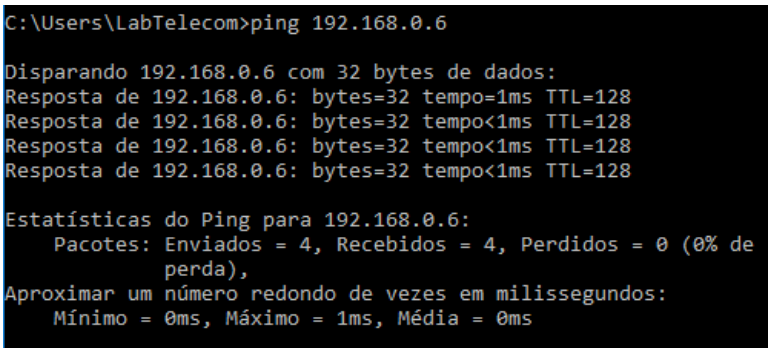


Figura 19. Teste de conectividade de LabTelecom para LabTelecom2 (IPv4)

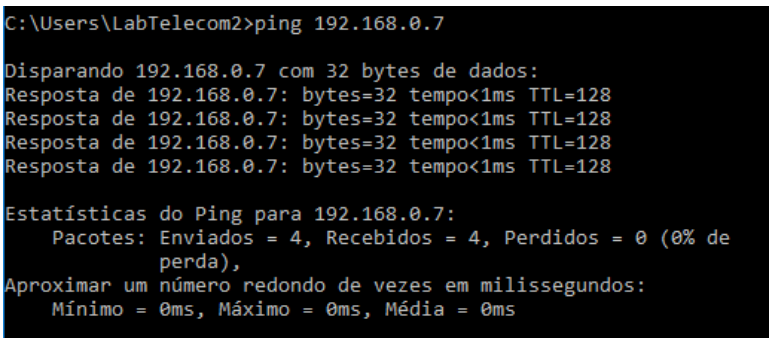


Figura 20. Teste de conectividade de LabTelecom2 para LabTelecom (IPv4)

Ainda observando as Figuras 19 e 20, pode-se perceber que nas duas situações, houve 0 % de perda dos pacotes, comprovando que há comunicação na pilha TCP/IPv4 entre as duas máquinas neste primeiro cenário. Agora, da mesma forma dos endereços IPv4, será utilizado o comando *ping* para testar a conectividade entre as maquinas utilizando os endereços IPv6, como mostrado nas Figuras 23 e 24. Assim como anteriormente, os pacotes serão enviados de LabTelecom para Labtelecom2 e, em seguida, no caminho inverso.

Da mesma forma que no IPv4, os endereços IPv6 também conseguem se comunicar, como constatado nas Figuras 21 e 22, pela porcentagem de perda dos pacotes enviados e recebidos que é de 0% de perda, demonstrando que a pilha TCP/IPv6 também está funcionando corretamente e sendo assim, é possível afirmar que o Cenário 1 está funcionando corretamente Pilha Dupla, visto que o endereçamento dos *hosts* está sendo configurado corretamente em ambas as pilhas e que há conectividade entre eles.

Logo, pôde-se dar início ao Cenário 2, que será mostrado no tópico a seguir.

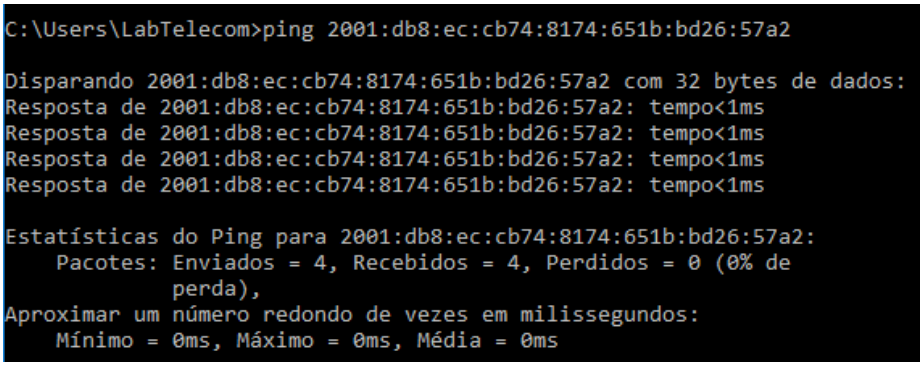


Figura 21. Teste de conectividade de LabTelecom para LabTelecom2 (IPv6)

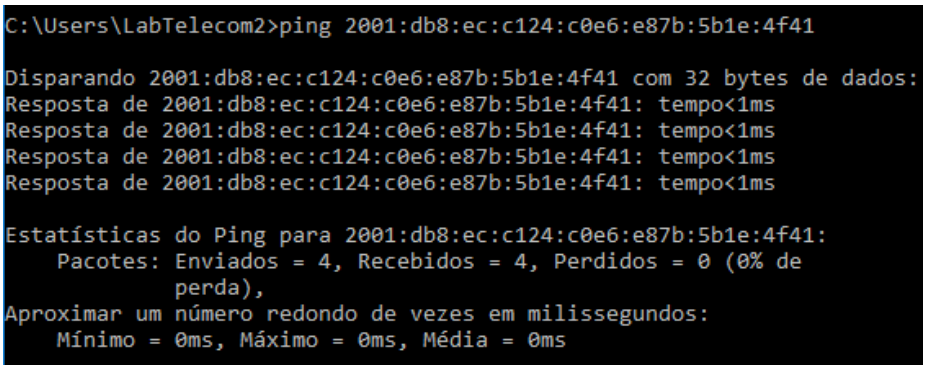


Figura 22. Teste de conectividade de LabTelecom2 para LabTelecom (IPv6)

3.2 CENÁRIO 2: REDE UTILIZANDO SERVIDOR DHCP REMOTO E UM RELAY AGENTE EM PILHA DUPLA

No cenário 2, onde funcionamento se dará também em Pilha Dupla, ocorrem algumas mudanças na topologia com a adição do roteador R2-LabTelecom para fazer a função de *Relay Agent* na rede local, enquanto o R-LabTelecom ainda se mantém como servidor DHCP, porém supõem-se que ele não se encontra localmente e sim no NTI de onde seria acessado remotamente por meio de uma rede externa, para fazer a distribuição dos endereços, apesar dele ainda estar localizado no laboratório de Telecomunicações e devido a algumas limitações de porta o R2-LabTelecom será conectado ao R-LabTelecom via *switch* SW-LabTelecom-1, por meio de uma VLAN separada.

A montagem da topologia física deste cenário foi feita de acordo com a Figura 23.

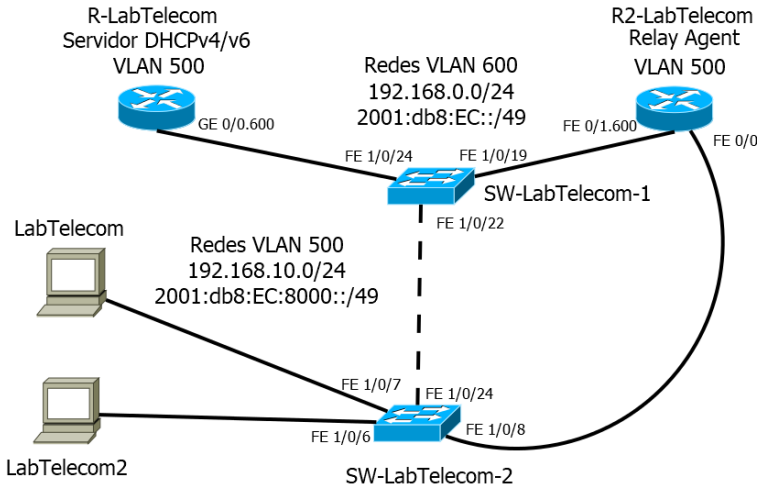


Figura 23. Topologia do Cenário 2

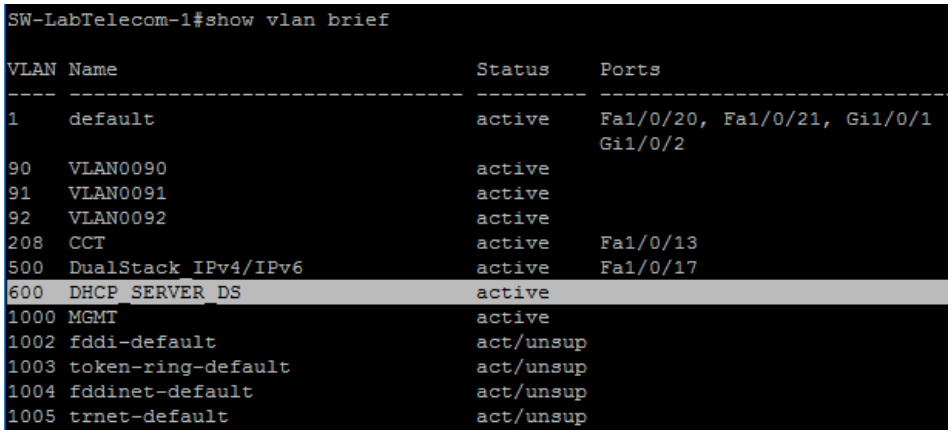
O objetivo deste cenário é fazer com que os clientes DHCP da VLAN 500, no caso os *hosts* LabTelecom e LabTelecom2, transmitam mensagens para o servidor R-LabTelecom, que se encontra na VLAN 600, ou seja, em redes diferentes, por meio de R2-LabTelecom, que atuará como agente de retransmissão (*Relay Agent*), intermediando a troca de mensagens DHCP entre eles. Nos tópicos a seguir, assim como no Cenário 1, serão demonstradas como foram feitas as configurações necessárias para o funcionamento deste cenário.

3.2.1 CONFIGURANDO OS *SWITCHES*

As configurações feitas nos dois *switches* da topologia são muito similares as feitas no cenário anterior, com a adição de poucas alterações. A primeira delas foi a criação de uma nova VLAN, com número 600, e chamada *DHCP_SERVER_DS*, para fazer a conexão entre os roteadores, colocando o servidor DHCP em uma rede diferente da qual os clientes pertencem, nesse caso, a VLAN 500.

Em seguida, devido à existência de uma única interface física disponível em R-LabTelecom, em SW-LabTelecom-1, além da criação da VLAN 600, a interface FE 1/0/19 foi atribuída como *trunk*, para fazer a conexão entre as subinterfaces dos roteadores, como visto na Figura 3.15. No *switch* SW-LabTelecom-2, apenas foi criada a VLAN 600 para garantir que não haveria nenhum tipo de bloqueio nas mensagens DHCP durante o processo de requisição de endereços.

Como o processo de criação da VLAN em ambos os *switches* é exatamente o mesmo, a Figura 24 mostra apenas as configurações feitas em SW-LabTelecom-1.



```
SW-LabTelecom-1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0/20, Fa1/0/21, Gi1/0/1
                                                Gi1/0/2
90   VLAN0090                         active
91   VLAN0091                         active
92   VLAN0092                         active
208  CCT                              active    Fa1/0/13
500  DualStack_IPv4/IPv6              active    Fa1/0/17
600  DHCP_SERVER_DS                   active
1000 MGMT                             active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 24. Criação da VLAN 600 para comunicação entre os roteadores em SW-LabTelecom-1

Observa-se que a VLAN 600 foi criada, encontra-se ativa e, assim como a VLAN 500, trata-se de uma VLAN criada separadamente para não afetar o funcionamento das redes ativas que se encontram nos dispositivos presentes no rack do Laboratório de Telecomunicações.

3.2.2 CONFIGURANDO R-LABTELECOM

As configurações em R-LabTelecom são basicamente iguais às do Cenário 1, havendo diferença apenas nas redes que serão utilizadas e nas subinterfaces, além do surgimento da necessidade de uma rota padrão. Neste cenário foram acrescentadas mais duas redes, uma IPv4 e uma IPv6, para endereçamento local, as quais serão definidas nos *pools* DHCP, e as redes que foram usadas no cenário anterior, desta vez, irão conectar os roteadores na VLAN 600.

Um detalhe importante, é que no endereçamento IPv6, foi feita a subdivisão da rede anterior 2001:db8:EC:: /48, em duas subredes, 2001:db8:EC:: /49 para a VLAN 600 e 2001:db8:EC:8000:: /49 para a VLAN 500, então por isso a mudança da máscara de subrede de /48 para /49 . No caso do IPv4, inicialmente houve uma subdivisão da rede 192.168.0.0 /24, também em duas subredes, porém ocorreram conflitos de endereços, e devido a isso, optou-se por mantê-la na VLAN 600 e utilizar a rede 192.168.10.0 /24 para endereçamento local.

```
ip dhcp excluded-address 192.168.10.1 192.168.10.5
!
ip dhcp pool IPv4
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.3
   dns-server 192.168.10.5
   domain-name engcomp_dualstack.uema.br
!
!
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool IPv6
 address prefix 2001:DB8:EC:8000::/49
 dns-server 2001:DB8:EC:8000::5
 domain-name engcomp_dualstack.uema.br
```

Figura 25. Criação dos *pools* DHCPv4 e DHCPv6 em R-LabTelecom

A Figura 25 mostra a configuração dos *pools* e é possível notar que a configuração é exatamente a mesma do cenário anterior, tendo mudanças apenas nos endereços que serão atribuídos aos *hosts* da rede local. No caso do IPv6, assim como anteriormente, para concluir a configuração do servidor é necessário informar que a subinterface GE 0/0.600 funcionará como servidor DHCPv6 utilizando o comando *ip dhcp* server <*nome do pool*> (o pool chama-se IPv6), dentro da subinterface como mostrado na Figura 26.

```
!
interface GigabitEthernet0/0.600
 encapsulation dot1Q 600
 ip address 192.168.0.2 255.255.255.0
 ipv6 address 2001:DB8:EC::2/49
 ipv6 enable
 ipv6 dhcp server IPv6
!
```

Figura 26. Configuração de GE 0/0.600 como servidor DHCPv6

Se tratando das mudanças nas configurações das subinterfaces, em relação ao Cenário 1, o que ocorreu foi a exclusão da subinterface GE 0/0.500 e a criação da interface GE 0/0.600, que recebeu o segundo endereço válido de cada rede, 192.168.0.2 na IPv4 e 2001:db8:EC::2 na IPv6, e fará a conexão com R2-LabTelecom. Além disso, o servidor DHCP precisa de um meio para alcançar a rede da VLAN 500, por isso houve a necessidade da configuração de rotas padrão IPv4 e IPv6 em R-LabTelecom, apontando para R2-LabTelecom como mostrado na Figura 27.

```
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.17.32.1
ip route 0.0.0.0 0.0.0.0 192.168.0.3
ip route 10.50.64.0 255.255.255.0 172.17.32.49
ip http server
no ip http secure-server
!
access-list 5 permit 10.5.0.0 0.0.255.255
access-list 6 permit 10.10.0.0 0.0.255.255
access-list 7 permit 10.20.0.0 0.0.255.255
access-list 8 permit 10.30.0.0 0.0.255.255
access-list 9 permit 10.100.0.0 0.0.255.255
access-list 10 permit 10.1.0.0 0.0.255.255
ipv6 route ::/0 2001:DB8:EC::3
!
```

Figura 27: Configuração de rotas padrão IPv4 e IPv6 em R-LabTelecom

Detalhando, as rotas padrões são necessárias e direcionadas para R2-LabTelecom, porque o mesmo está ligado diretamente em ambas as VLANs, e o servidor precisa saber para onde irá encaminhar as mensagens DHCP aos clientes, sendo assim toda vez que servidor receber mensagens dos clientes, ele enviará a resposta na subinterface FE 0/1.600, interface que conecta o R2-LabTelecom a R-LabTelecom.

3.2.3 CONFIGURANDO R2-LABTELECOM

A principal diferença deste cenário para o outro, está no acréscimo deste novo dispositivo, nomeado R2-LabTelecom, que foi configurado para fazer a retransmissão (*relay*) das mensagens DHCP entre os clientes da VLAN 500 e o servidor remoto na VLAN 600, além de funcionar como *gateway* padrão da rede local.

O R2-LabTelecom, trata-se de um dispositivo menos robusto e com versão de IOS menos atualizada, razão pela qual foi escolhido para a função de *relay*, que também possui apenas duas interfaces físicas, FE 0/0 e FE 0/1 e, assim como R-LabTelecom no primeiro cenário, foi necessário habilitar o funcionamento do IPv6, executando o comando i*pv6 unicast-routing* no modo de configuração, para em seguida iniciar os procedimentos para transformá-lo em um *Relay Agent*.

As configurações em R2-LabTelecom, serão feitas basicamente nas interfaces, começando pela interface FE 0/1, na qual foi criada a subinterface FE 0/1.600 para se conectar com o servidor R-LabTelecom via VLAN 600 e atribuídos estaticamente, endereços IPv4: 192.168.0.3 e IPv6: 2001:db8:EC::3, como mostra a Figura 28. Em seguida, foi verificado se havia conectividade entre os roteadores, para, aí sim, iniciar as configurações da rede local.

```
!
interface FastEthernet0/1.600
 encapsulation dot1Q 600
 ip address 192.168.0.3 255.255.255.0
 ipv6 address 2001:DB8:EC::3/49
 ipv6 enable
!
!
!
```

Figura 28. Criação e endereçamento IPv4 e IPv6 da subinterface FE 0/1.600 em R2-LabTelecom

Agora, partindo para interface FE 0/0, que fará parte da rede da VLAN 500 funcionando como *gateway* padrão, além de receber as configurações que tornam R2-LabTelecom um *Relay Agent*, inicia-se com o endereçamento estático de IPv4 e IPv6 como anteriormente. O endereço IPv4 atribuído para IPv4 foi o "192.168.10.3", definido como endereço do *default-router* no pool IPv4 mostrado na Figura 25, logo todos os clientes DHCPv4 o usarão como gateway de saída para outras redes IPv4. Já os endereços IPv6 atribuídos foram 2001:db8:EC:8000::2, *global unicast*, e FE80::3 *link-local* para servir como *gateway* de saída para os clientes DHCPv6.

Por fim, bastou transformar o R2-Telecom em *Relay Agent* por meio de comandos adicionais na interface FE 0/0 e conectá-lo em uma das portas de acesso da VLAN 500 que, neste caso, foi utilizada a interface FE 1/0/8 em SW-Telecom-2. O *relay* DHCPv4 é feito utilizando um comando bem simples associado ao endereço IPv4 do servidor *DHCP* que se encontra na rede externa e nesse caso seria o comando *ip helper-address* junto ao endereço 192.168.0.2.

Passando para o *relay* DHCPv6, o comando para efetuar essa configuração, é bem diferente do que foi feito no DHCPv4. Além de informar qual o endereço do servidor DHCP, também é preciso indicar qual a porta de saída para alcançá-lo, usando o comando *ipv6 dhcp relay destination*, seguido do endereço IPv6 do servidor, 2001:db8:EC::2, acrescido da interface que conecta o roteador local a ele FE 0/1.600.

Observando a Figura 29, podemos ver como são escritos exatamente os comandos IPv4 E IPv6, e na configuração IPv6, da mesma forma que no cenário anterior, foi necessário o comando *ipv6 nd managed-config-flag* para instruir os clientes a receber todas as suas configurações de endereço por meio de DHCPv6 do tipo *Stateful*.

```
!
interface FastEthernet0/0
 ip address 192.168.10.3 255.255.255.0
 ip helper-address 192.168.0.2
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:EC:8000::3/49
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2001:DB8:EC::2 FastEthernet0/1.600
!
```

Figura 29. Configuração do *Relay* DHCPv4 e DHCPv6 na subinterface FE 0/0 em R2-LabTelecom

3.2.4 ENDEREÇAMENTO E CONECTIVIDADE ENTRE OS HOSTS

Após a configuração do servidor e relay DHCP, foi necessário verificar se os hosts da rede, LabTelecom e LabTelecom2, estavam recebendo as configurações de endereçamento corretamente em ambas as pilhas, e também se havia conectividade entre eles, como no cenário anterior. Como estes *hosts* já haviam sido configuradas no Cenário 1, apenas será mostrado com o comando *ipconfig*, no *prompt d*e comando do *Windows* e também não serão mais mostrados os endereços de IP sendo recebidos separadamente e sim o resultado final, já em Pilha Dupla. As Figuras 30 e 31 mostram LabTelecom e LabTelecom2 recebendo endereçamento IP de ambas versões via *Relay Agent*.

```
C:\Users\LabTelecom>

Configuração de IP do Windows


Adaptador Ethernet Ethernet:

   Sufixo DNS específico de conexão. . . . . : engcomp_dualstack.uema.br
   Endereço IPv6 . . . . . . . . . . . . : 2001:db8:ec:f396:785c:dd26:1bd6:d321
   Endereço IPv6 de link local . . . . . . . . . : fe80::352c:60d5:6096:e7c0%12
   Endereço IPv4. . . . . . . . . . . . . . . . : 192.168.10.6
   Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . . : fe80::3%12
                                                   192.168.10.3
```

Figura 30. Endereçamento recebido via *Relay Agent* IPv4 e IPv6 em LabTelecom

```
C:\Users\LabTelecom2>ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet:

   Sufixo DNS específico de conexão. . . . . : engcomp_dualstack.uema.br
   Endereço IPv6 . . . . . . . . . . . . : 2001:db8:ec:c0ec:1ac6:593:c1da:9679
   Endereço IPv6 de link local . . . . . . . . . : fe80::d163:1bc:f331:7b26%9
   Endereço IPv4. . . . . . . . . . . . . . . . : 192.168.10.7
   Máscara de Sub-rede . . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . . : fe80::3%9
                                                   192.168.10.3
```

Figura 31. Endereçamento recebido via *Relay Agent* IPv4 e IPv6 em LabTelecom2

Observando as Figuras 30 e 31, percebe-se que o endereçamento em ambas as pilhas está correto, já que os endereços recebidos são equivalentes aos que foram definidos nos intervalos dos *pools* DHCP configuradas em R-LabTelecom, inclusive os endereços dos *gateways* padrão e domínio informados, restando agora o último passo que é verificar se há conectividade entre as máquinas.

Repetindo os passos do cenário anterior, foram feitos testes utilizando o comando *ping* mais o endereço de IPv4 e depois IPv6, partindo de LabTelecom para LabTelecom2 e verificado se havia resposta de LabTelecom2.

```
C:\Users\LabTelecom>ping 192.168.10.7

Disparando 192.168.10.7 com 32 bytes de dados:
Resposta de 192.168.10.7: bytes=32 tempo<1ms TTL=128
Resposta de 192.168.10.7: bytes=32 tempo<1ms TTL=128
Resposta de 192.168.10.7: bytes=32 tempo<1ms TTL=128
Resposta de 192.168.10.7: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 192.168.10.7:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms
```

Figura 32. Teste de conectividade na pilha TCP/IPv4 de LabTelecom para LabTelecom2

De acordo com as Figura 32, nota-se que a conectividade entre os *hosts* é existente, baseado nas informações dos pacotes recebidos e enviados que possuem perdas de 0% na pilha TCP/IPv4, restando apenas testar a conectividade entre os *hosts* na pilha TCP/IPv6.

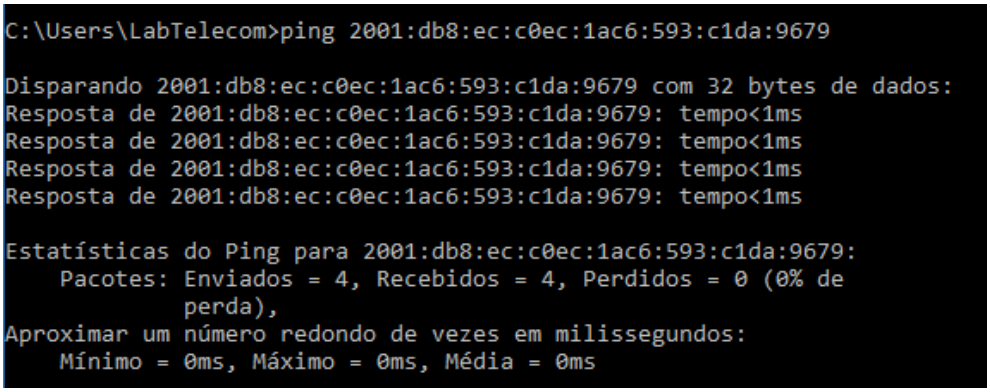


Figura 33. Teste de conectividade na pilha TCP/IPv6 de LabTelecom para LabTelecom2

Da mesma forma que na pilha TCP/IPv4, na pilha TCP/IPv6 existe conectividade entre os hosts, como observado na Figura 33. Desse modo, atesta-se que o Cenário 2 também funciona corretamente.

4 CONCLUSÃO E CONSIDERAÇÕES FINAIS

Como este projeto consiste em fazer o planejamento da transição da rede de comunicação de dados, baseando-se nas observações e testes feitos nos cenários apresentados no projeto, pode-se concluir que há total viabilidade para implantação de uma rede em Pilha Dupla, utilizando serviços de endereçamento, tanto local, quanto remoto e que a rede de testes contemplou os objetivos propostos.

Sendo assim, já é possível executar, futuramente, testes nas redes ativas, implementando uma rede IPv6 em paralelo com a rede IPv4, para atender aos usuários de ambas as versões, com garantias de que não haverá interferência de uma rede em outra, e com o tempo, à medida que o número de usuários do IPv6, tornar-se superior ao IPv4, a pilha IPv4 possa ser desativada, por se tratar de uma tecnologia que inevitavelmente se tornará legada.

Outros pontos percebidos durante a execução do projeto, foram que para implementação do IPv6, se tratando de redes onde o IPv4 já se encontra ativo, foi na questão do ICMPv6 e do DHCPv6. É comum encontrar algumas práticas realizadas por administradores de redes IPv4 como medidas de segurança, que, de certa forma, podem impedir o funcionamento correto de uma rede IPv6, como, por exemplo o bloqueio de mensagens ICMP por meio de regras de firewall. As mensagens ICMPv6 são de enorme importância para o funcionamento de uma rede IPv6, visto que elas carregam funcionalidades necessárias para comunicação entre hosts vizinhos, portanto essa prática é prejudicial no IPv6.

Quanto ao DHCPv6, é importante estar atento ao modo de configuração escolhido. Caso seja desejado ter um controle dos endereços, para fins de gerenciamento ou outras razões, o modo aconselhável é o *Stateful*, devido ao fato dos endereços do tipo *global-unicast*, equivalente aos endereços IPv4 públicos, aparecem de forma explícita nos hosts. Caso o interesse já apenas para fins de endereçamento local, pode se optar pelo modo *Staless*, no qual serão repassas apenas configurações complementares para as máquinas, já que o IPv6 já oferece suporte de autoconfiguração de endereços nativamente.

Um outro fato percebido é que a configuração de um servidor DNS para resolver nomes IPv6 na rede, se tornou extremamente importante. A razão disso é que o comprimento dos endereços IPv6, apesar de ter se tornado um pouco mais compreensível por meio da notação hexadecimal seguida de “ : ”, não são fáceis de memorizar. Desse modo, um servidor DNS tornou-se uma ferramenta indispensável para facilitar o gerenciamento e outras operações nas redes IPv6.

5 SUGESTÕES PARA TRABALHOS FUTUROS

Como este projeto visa apenas fazer o planejamento da migração das versões do protocolo IP da rede de dados por meio testes em uma rede apartada, a partir daí pode-se sugerir alguns trabalhos para serem executados futuramente:

- Implementação da Pilha TCP/IPv6 nas redes ativas, que no momento, só operam em IPv4;
- Implementar o suporte à mobilidade de IP utilizando o MIPv6;
- Configurar medidas de segurança na rede baseadas no protocolo IPv6;
- Realizar a migração total da versão IPv4 para a versão IPv6, desativando a pilha IPv4;
- Configuração de um servidor DNS para resolver nomes no IPv6.

REFERÊNCIAS

[1] CASTELUCCI, D. **Protocolos de comunicação em redes de computadores**. Disponível em: < https://daniellacastelucci.wordpress.com/2011/04/08/protocolos-de-comunicacao-em-redes-de-computadores/>. Acessado em 1 de agosto de 2017.

[2] IG TECNOLOGIA. **IANA distribui últimos endereços IPv4.** Disponível em: <http://tecnologia.ig.com.br/noticia/2011/02/03/icann+distribui+ultimos+enderecos+ipv4+10359904.html>. Acessado em 1 de agosto de 2017.

[3] BRITO, S. H. B. **IPv6 O Novo Protocolo da Internet**. 1. ed. – São Paulo: Novatec, 2013. 208p.

[4] KUROSE, J. F; ROSS, K.W. **Redes de computadores e a Internet: uma abordagem top-down.** 6. ed. – São Paulo: Pearson Education do Brasil, 2013. 634p.

[5] RFC 1519. **Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy**. Disponível em <https://tools.ietf.org/html/rfc1519>.Acessado em 12 de outubro de 2017.

[6] RFC 2663. **IP Network Address Translator (NAT) Terminology and Considerations.** Disponível em <https://tools.ietf.org/html/rfc2263>.Acessado em 20 de outubro de 2017.

[7]TANENBAUM, A. S**. Redes de Computadores**. 4. ed. – Rio de Janeiro: Elsevier, 2003.

[8] RFC 1918. **Address Allocation for Private Internets**. Disponível em <https://tools.ietf.org/html/rfc1918>.Acessado em 14 de outubro de 2017.

[9] KESSLER. G. **An Overview of TCP/IP Protocols and the Internet.**2014. Disponível em < https://www.garykessler.net/library/tcpip.html>. Acessado em 28 de outubro de 2017.

[10] FOROUZAN, B.A.; FEGAN S. C. **Comunicação de Dados e Redes de Computadores** – Porto Alegre : Bookman, 2006. - 3ª.

[11] NATH, P.B.; UDDIN M.M. **TCP-IP Model in Data Communication and Networking**. American Journal of Engineering Research (AJER).2015.

[12] RFC 791. **Internet Protocol**. DARPA Internet Program. Disponível em <https://tools.ietf.org/html/rfc791>.Acessado em 12 de outubro de 2017.

[13] IPv6.BR. **Cabeçalho**. Disponível em < http://ipv6.br/post/cabecalho/>. Acessado em 22 de outubro de 2017.

[14] MICROSFT. **IPv4.** Disponível em < https://technet.microsoft.com/en-us/library/82bb469e-8bdd-4b9c-8156-60da381d79b4/>. Acessado em 22 de outubro de 2017.

[15] IPv6.BR. **Introdução**. Disponível em < http://ipv6.br/post/introducao/ >. Acessado em 22 de outubro de 2017.

[16] TORRES, G. **Redes de computadores - Verão Revisada e Atualizada**. 2. ed – Rio de Janeiro: NovaTerra, 2014

[17] RFC 3330. **Special-Use IPv4 Addresses**. Setembro, 2002.

[18] RFC 8200. **Internet Protocol, Version 6 (IPv6) Specification.** Julho, 2017

[19] RFC 4302. **IP Authentication Header.** Dezembro, 2005

[20] RFC 4303. **IP Encapsulating Security Payload (ESP).** Dezembro, 2005

[21] IPv6.BR. **Endereçamento**. Disponível em < http://ipv6.br/post/enderecamento/>. Acessado em 22 de outubro de 2017.

[22] RFC 2131. **Dynamic Host Configuration Protocol.** Disponível em <https://tools.ietf.org/html/rfc2131>.Acessado em 15 de outubro de 2017.

[23] RFC 3315. **Dynamic Host Configuration Protocol for IPv6 (DHCPv6)**. Julho, 2003

[24] EQUIPE IPv6.BR. **Laboratório de IPv6 [livro eletrônico]: aprenda na prática usando um emulador de redes.** – São Paulo: Novatec Editora, 2015

[25] CISCO SYSTEMS. **Configuring the Cisco IOS DHCP Relay Agent.** Disponível em < https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html>. Acessado em 26 de outubro de 2017.

[26] CISCO SYSTEMS. **Cisco Support Community**. Disponível em <https://supportforums.cisco.com/t5/tkb/articleprintpage/tkb-id/4461-docs-network-infrastructure/article-id/4662>. Acessado em 26 de outubro de 2017.

[27] RFC 792. **Internet Control Message Protocol**. DARPA Internet Program. Disponível em <https://tools.ietf.org/html/rfc792>.Acessado em 12 de outubro de 2017.

[28] RFC 4443. **Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification**. Março, 2013

[29] RFC 3596. **DNS Extensions to Support IP Version 6**. Outubro, 2003

[30] HUCABY, D.; MCQUERRY S. **Cisco Field Manual: Catalyst Switch Configuration.** Disponível em <https://supportforums.cisco.com/t5/tkb/articleprintpage/tkb-id/4461-docs-network-infrastructure/article-id/4662>. Acessado em 26 de outubro de 2017.

[31] NETWORKLESSONS. **InterVlan Routing.** Disponível em < https://networklessons.com/switching/intervlan-routing/>. Acessado em 19 de outubro de 2017.

[32] HEDLUND, B. **VLAN Trunking using IEEE 802.1Q.** Disponível em < http://bradhedlund.com/2007/11/27/vlan-trunking-using-ieee-8021q/>. Acessado em 23 de outubro de 2017.

[33] RFC 4213. **Basic Transition Mechanisms for IPv6 Hosts and Routers**. Outubro, 2005.

[34] IPv6.BR. **Transição**. Disponível em < http://ipv6.br/post/transicao/>. Acessado em 22 de outubro de 2017.

[35] CISCO SYSTEMS. **Cisco IOS IPv6 Feature Mapping.** Disponível em < http://docwiki.cisco.com/wiki/Cisco_IOS_IPv6_Feature_Mapping#IPv6_Features>. Acessado em 26 de outubro de 2017.

[36] BRITO, S. H. B. **Servidores DHCPv6 em Redes IPv6.** Disponível em < http://labcisco.blogspot.com.br/2013/05/servidores-dhcpv6-em-redes-ipv6.html/>. Acessado em 23 de outubro de 2017.