UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

EDUARDO RENAN MANIKA

CONFIGURAÇÃO DE UM AMBIENTE DE SIMULAÇÃO DE REDES DEMONSTRANDO O MÉTODO DE TRANSIÇÃO DO PROTOCOLO IPv4 – IPv6: PILHA DUPLA E A CONFIGURAÇÃO DE UM SERVIÇO DHCP EM AMBOS OS PROTOCOLOS

MONOGRAFIA

CURITIBA

2014

EDUARDO RENAN MANIKA

CONFIGURAÇÃO DE UM AMBIENTE DE SIMULAÇÃO DE REDES DEMONSTRANDO O MÉTODO DE TRANSIÇÃO DO PROTOCOLO IPv4 – IPv6: PILHA DUPLA E A CONFIGURAÇÃO DE UM SERVIÇO DHCP EM AMBOS OS PROTOCOLOS

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR

Orientador: Prof. MSc. Lincoln Herbert Teixeira

CURITIBA

2014

RESUMO

MANIKA, Eduardo R. **Configuração de um ambiente de simulação de redes demonstrando o método de transição do Protocolo IPv4 – IPv6: Pilha Dupla e a configuração de um serviço DHCP em ambos os protocolos.** 2014. 103 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Essa monografia aborda o estudo para desenvolver um ambiente de simulação/emulação de uma rede local utilizando o *software* GNS3. Apresentando um cenário que aborda uma técnica de transição do protocolo IPv4-IPv6, denominada Pilha Dupla. Transição essa que inicialmente foi projetada para ser executada tecnicamente simples e de forma gradativa, porém não ocorrendo conforme o esperado e com o esgotamento do endereçamento IPv4 e o aumento da necessidade de novos endereços, o IPv6 se torna cada vez mais necessário. Além da Pilha Dupla, abordará a demonstração da configuração dos serviços de rede sendo implementado em ambos os protocolos, no caso o serviço de DHCP - *Dynamic Host Configuration Protocol*, que distribui os endereços IP aos hosts da rede. E para realizar o roteamento da rede será utilizado o protocolo de roteamento OSPF, que apresenta suporte a versão IPv4 e IPv6. O projeto trata-se de uma pesquisa teórica experimental, no qual é realizado um levantamento bibliográfico, seguido da configuração do ambiente de simulação e implementação dos serviços em ambos os protocolos e análise dos resultados obtidos. O resultado mostrará o impacto dessa transição na rede, nos serviços e na administração da rede.

Palavras-chave: IPv6. IPv4.Transição: IPv4-IPv6. Pilha Dupla. DHCP. DHCPv6. OSPF. OSPFv3.

ABSTRACT

MANIKA, Eduardo R. **Configuring a network simulation environment demonstrate the method of transition from IPv4 protocol - IPv6: Dual stack and configuring a DHCP service in both protocols.** 2014. 103 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) - Federal Technological University of Paraná. Curitiba, 2014.

This monograph discusses the study to develop an environment for simulation / emulation of a local area network using GNS3 software. Presenting a scenario that addresses a technique of transition from IPv4-IPv6 protocol, called Dual Stack. This transition that was initially designed to run technically simple and gradually, though not occurring as expected and with the exhaustion of IPv4 addresses and the increasing need for new addresses, IPv6 becomes increasingly necessary. Beyond the Double Stack, the demonstration will address the configuration of network services of DHCP service being implemented both protocols in the case - Dynamic Host Configuration Protocol, which distributes IP addresses to network hosts. And to perform network routing protocol OSPF routing, which provides support for IPv4 and IPv6 version will be used. The project comes up from a theoretical experimental research, in which a bibliographic survey, followed by the simulation environment configuration and deployment of services in both protocols and analysis of results is performed. The results show the impact of this transition on the network, services and network administration.

Keywords: IPv6, IPv4, Method of Transition: IPv4-IPv6. Dual Stack, DHCP, DHCPv6, OSPF, OSPFv3.

LISTA DE SIGLAS

ACL - *Access Control List*

CGN - *Carrier Grade NAT*

CIDR - *Classless Inter-Domain Routing*

DARPA - *Defense Advanced Research Projects Agency*

DHCP - *Dynamic Host Configuration Protocol*

DNS - *Domain Name Server*

HTML - *Hyper-Text Markup Language*

IANA - *Internet Assigned Numbers Authority*

ICANN - *Internet Corporation for Assigned Names e Numbers*

IETF - *Internet Engineering Task Force*

IP - *Internet Protocol*

LSN - *Large Scale NAT*

MAC - *Media Access Control*

MTU - *Maximum Transmission Unit*

NAT - *Network Address Translation*

OSPF - *Open Shortest Path First*

RFC - *Request for Comments*

RIR - *Regional Internet Registry*

ROAD - *Routing and Addressing*

TTL - *Time To Live*

ULA - *Unique Local Address*

WWW - *World Wide Web*

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão apresentados os motivos pelo qual levaram a implementação de um ambiente de simulação do mecanismo de transição de redes baseadas no Protocolo IP (*Internet Protocol*) versão 4 para o protocolo IP versão 6, demonstrando a configuração de um serviço *Dynamic Host Configuration Protocol* (DHCP), que distribui os endereços IP aos *hosts* da rede em com ambas as versões do Protocolo IP.

1.1 TEMA

Desde a criação das redes de computadores estão crescendo em tamanho, complexidade e utilização de banda. A quantidade de usuários na internet saltou de dezenas para mais de um bilhão e meio de usuários. Os equipamentos e aplicações de redes tiveram que evoluir rapidamente para suportar a demanda dos usuários (FILIPPETTI, 2014, p.128).

Quando a versão 4 do protocolo IP (IPv4) foi definido optou-se pela disponibilização de 32 bits para o endereçamento, o que seria suficiente para se endereçar cerca de 4 bilhões de máquinas. Porém essa distribuição não foi linear, mas hierárquico, o que significa que essa quantidade é um pouco mais da metade na prática. Segundo Filippetti (2014, p.129) a versão 6 do protocolo IP não foi elaborado como uma mera atualização do IPv4, trata-se de um protocolo novo, apresenta uma arquitetura de cabeçalhos completamente diferente, introduzindo novos serviços e aprimorando os já existentes. A respeito da escalabilidade o IPv6, quadriplica o número de bits, de 32 para 128 bits, o que possibilita 3,4x10E+34 endereços disponíveis, ou seja, 66.557.079.334.886.694.389 endereços IP por

centímetro quadrado do planeta Terra.

Os blocos de endereços IPv4 livres para atribuição a provedores de serviços já se esgotaram em diversas regiões do planeta. Especialistas preveem o fim definitivo desses endereços já no início de 2015, significando que o processo de transição entre o IPv4 para o IPv6 é inevitável e já deveria ter avançado há muitos anos, uma vez que o protocolo IPv6 foi definido em 1988 e não foi dada a devida atenção a esse processo de transição. (FILIPPETTI, 2014, p.129)

1.2 PROBLEMAS E PREMISSAS

A transição entre o protocolo IPv4 e IPv6 foi projetada para ser executada tecnicamente simples e forma gradativa, porém não ocorreu conforme esperado. O IPv6 não esta sendo amplamente utilizado e o esgotamento do endereçamento IPv4 está se tornando cada vez mais realidade. Com o crescimento da internet aliado com o aumento do poder computacional e o alcance das aplicações baseadas no IP, como equipamentos eletrônicos em especial dispositivos móveis como celulares e *tablets*, tem favorecido e muito para ocasionar essa redução nos endereços. (CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES, 2014).

Segundo o Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (2014) estimavam que por volta de 2010 a 2014 não haverá mais endereços para serem disponibilizados. Com isso os administradores de rede podem ser surpreendidos a disponibilizarem funcionalidade com suporte ao protocolo IPv6 com prazos reduzidos.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Desenvolver um ambiente de simulação utilizando a técnica de transição: Pilha Dupla na migração do protocolo IPv4 para IPv6, aplicando serviço de DHCP versão IPv4 e IPv6.

1.3.2 Objetivos Específicos

- Utilizar o Emulador GNS3 para configurar a simulação de uma Rede Local.
- Configurar os equipamentos para utilizar o Protocolo de Roteamento OSPF no IPv4 e OSPFv3 no IPv6.

1.4 JUSTIFICATIVA

Inicialmente a Internet foi concebida para conectar máquinas, dispositivos fixos, referenciada como a era da “Internet das Máquinas”. Com a popularização comercial da Internet, no início da década de 90, e a disseminação dos dispositivos móveis no início dos anos 2000, uma nova era surgiu, onde o elemento mais importante deixou de ser as máquinas e passou a ser as próprias pessoas. Ou seja, usuários conectados a Internet de qualquer lugar, através de vários dispositivos fixos ou móveis. Esta era é a era atual e é chamada de “Internet das Pessoas”. Atualmente a Internet encontra-se em uma fase de transição da era da “Internet das Pessoas” para a era da “Internet das Coisas”, onde qualquer coisa poderá ser conectada à Internet para os mais diversos fins, como carros, eletrodomésticos, lâmpadas, fechaduras, entre outros. Porém isso só será realmente viável quanto o IPv6 efetivamente se tornar operacional na Internet, pois com a capacidade limitada

de endereçamento da versão 4 não atende a demanda atual, no qual já se encontra em escassez, além de outros requisitos como: segurança e mobilidade. (BRITO, 2013, p. 36)

Segundo Brito (2013, p. 38) por conta desse panorama, profissionais preparados para trabalharem com o protocolo IPv6 serão recursos humanos cada vez mais valorizados e demandados pelo mercado. Desde junho de 2012, todos os novos dispositivos de rede fabricados no mundo devem ter suporte ao IPv6, isso não significa que o IPv4 será inutilizado a curto prazo em virtude do alto grau de disseminação do IPv4 na Internet.

Com isso nesse projeto permite abordar a questão dos mecanismos de transição do protocolo IP, uma vez que os dois protocolos IPv4 e IPv6 não são diretamente compatíveis, criando um ambiente de emulação para simular os impactos dessa transição em uma rede local. Além da implementação de rede utilizado a nova versão do protocolo IP e um serviço, no caso o serviço DHCP, utilizando suporte a versão IPv6.

1.5 PROCEDIMENTO METODOLÓGICO

Esse projeto trata-se de uma pesquisa teórica experimental, no qual é realizado um levantamento bibliográfico constituído principalmente de livros, artigos e revistas científicas sobre a migração do protocolo IPv4 para IPv6 e as técnicas transição e roteamento mais indicadas para serem implementadas e configuradas.

Juntamente com o levantamento bibliográfico será criado um ambiente para simular algumas destas técnicas de migração levantadas, entre elas a transição de pilha dupla. Esse ambiente de simulação será utilizado um *software Open Source* (GLP) chamado GNS3 que é um laboratório que permite à simulação a engenharia

de redes complexas e utiliza os softwares de equipamentos reais, obtendo resultados mais próximos da realidade. Será montado nesse ambiente uma topologia de rede local corporativa, com roteadores, switches e computadores, no qual será utilizado máquinas virtuais para testa as configurações e os serviços implementados (GNS3, 2014).

Próximo etapa será a configuração dos equipamentos como endereçamento IP com IPv4 e IPv6 e a implementação do protocolo de roteamento o Protocolo de Portal Interno (OSPF). Segundo Comer (2007, p. 337) o OSPF utiliza um algoritmo de estado de link para determinar as rotas de roteamento e propagar as informações de roteamento. Utilizam o algoritmo SPF de Dijkstra para computar os caminhos mais curtos com base nas nessas mensagens trocadas contendo o estado do link. É otimizado designando um único roteador para fazer *broadcast* na rede. A versão 3 desse protocolo será utilizada pois suporta o roteamento utilizando o protocolo IPv6.

Com o ambiente rede já funcional será implementado o serviço de *Dynamic Host Configuration Protocol* (DHCP). Segundo Comer (2006, p. 267) o DHCP segue o modelo cliente-servidor, ou seja, exige trocas de pacotes de um computador com o servidor DHCP para requisitar informações de endereço IP para acessar a rede, além de algumas informações adicionais como da rota *default* e endereço do *Domain Name Server* (DNS). Será implementado a versão DHCP para IPv6 que permite passar parâmetros de configuração de endereços IPv6 para hosts conectados via IPv6.

O DHCPv6 como é denominado, utiliza pacotes UDP, conforme Kurose (2010, p.150) é um protocolo da camada de transporte não orientado a conexão, sua função é multiplexação/demultiplexação e algumas verificações de erros e pouco adiciona ao IP. O cliente que utiliza DHCPv6 opera na porta 546 e o cliente na porta

547. Cada cliente e servidor apresentam um DUID – Identificador Único DHCP – utilizado para identificar clientes e selecionar parâmetros de configuração para associação de identidade para endereços não-temporários (IA – *Identity Association for Non-Temporary Addresses*). O DUID de um cliente ou servidor não deve mudar e nem alterado com o resultado de uma mudança de *hardware* de rede de um dispositivo.

Após a finalização da montagem da estrutura e de todas as configurações será realizado teste de conectividade e de funcionamento dos dois protocolos IP operando juntos em uma rede corporativa e qual esta o grau de dificuldade de configuração dos equipamentos na utilização das técnicas de transição do protocolo IP em especial a Pilha Dupla e de serviços operando com IPv6.

1.6 EMBASAMENTO TEÓRICO

Desde o surgimento da Internet com o padrão atual utilizando o protocolo TCP/IP em meados do início da década de 80, ocorre um crescimento ordenado da rede devido a eliminação das restrições de protocolos anteriores. O protocolo IP foi definido na RFC 791 que prover duas funções básicas: a fragmentação, envio de pacotes maiores que o limite de tráfego estabelecido num enlace, dividindo-os em partes menores; e o endereçamento, que permite a entrega da origem até o destino do pacote. (CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES, 2014).

A versão do protocolo IP utiliza desde o início é a 4, chamado de IPv4, embora seja uma versão muito robusta, de fácil implementação e interoperabilidade, seu projeto inicial não previu o crescimento das redes e um possível esgotamentos dos endereços. O IPv4 é composto de 32 bits reservados para endereços comporta

um total de aproximadamente 4.294.967.296 endereços exclusivos. Dentre esses foram inicialmente separados em 3 classes A,B,C e algumas faixas de endereços reservadas. Essa separação mostrou-se ineficientes pois algumas faixas um desperdício muito grande na quantidade de IPs e outras faltavam endereços em determinadas situações. Segundo o Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações nos anos 90 já existiam 313.000 dispositivos *(hosts)* conectados a rede e estudos já apontavam a falta de endereçamento. Com a criação do protocolo HTTP e a liberação comercial da internet ocorreu um salto de 2 milhões de *hosts*, em 1993 para 26 milhões em 1997 (CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES, 2014).

Diante disso alguma soluções começaram a ser apresentadas, em 1991 o grupo de trabalho ROAD (*Routing and Addressing*) elaborou a utilização de sub-classes – CIDR (*Classless Inter-domain Routing*) permitindo alocação de blocos de endereços apropriados a real necessidade de cada rede e a agregação de rotas, reduzindo o tamanho das tabelas de roteamento. Outra solução apresentada na RFC 2131 foi o protocolo DHCP – *Dynamic Host Configuration Protocol*, permitindo um *host* a obter endereçamento automaticamente e informações adicionais como: máscara de sub-rede, endereço do roteador padrão e o endereço do servidor DNS local. O DHCP permite atribuir endereços temporários para os dispositivos, através de uma lista de endereços IPs arbitrárias, e no momento que o *host* sai da rede o endereço é disponibilizado novamente (CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES, 2014).

O NAT – *Network Address Translation* foi outra técnica desenvolvida, definida na RFC 3022 o NAT realiza uma tradução do endereço IP privado, válido somente dentro de rede local, para uma IP público que é válido nas redes externas

permitindo ser roteável na internet. Nessa situação foram criados 3 faixas de endereços privados que somente são validados no roteamento local da rede. Porém esse modelo foge do modelo fim a fim da internet não permitindo conexões diretas entre dois *hosts*, dificultando o funcionamento de uma série de aplicações como VoIP, VPNs, além de aumentar o poder de processamento dos dispositivos tradutores de endereço.

Embora essa técnicas tenham diminuído o crescimento da utilização dos endereços isso não foi o suficiente para resolver o problema do esgotamento do IPv4, possibilitando sim mais tempo para desenvolver uma nova versão do IP que suprisse as falhas apresentadas como: escalabilidade, segurança, configuração e administração de rede, suporte a QoS, mobilidade, políticas de roteamento e já foi elaborado formas de transição. Várias foram as implementações de novas versões para o protocolo IPv4, porém a escolhida foi uma opção de deriva de uma da sugestões e foi denominada IPv6.

O IPv6 deve fornecer endereços suficientes para as necessidades futuras da internet por muitos anos. A IPv6 é composto por 128 bits, 4 vezes a mais que o IPv4 que é composto por 32 bits. A quantidade de endereços IPv6 disponíveis permite a atribuição de muitos trilhões de endereços a todas as pessoas do planeta. Além desse crescimento de endereços o IPv6 trata recursos novo e aprimorados que apresentam limitações no IPv4, um dos principais recursos que possui é a autoconfiguração, cabeçalhos mais simples melhorando a eficiência de roteamento, mobilidade permitindo que pessoas com dispositivos móveis movam-se entra as redes e segurança IP (IPSec). (CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES, 2014).

O IPv4 e IPv6 não são diretamente compatíveis entre si, porém podem

funcionar simultaneamente nos mesmos equipamentos. Esse funcionamento simultâneo é chamado de Pilha Dupla ou *Dual Stack.* Com base nesse fator a transição foi elaborada para ser realizada de forma gradual. No período de implantação da nova versão haveria a necessidade de técnicas auxiliares de transição, inicialmente conectar ilhas com IPv6 trafegando sobre o protocolo IPv4, para os equipamento que não possuem suporta a nova versão e posteriormente esse fluxo seria ao contrário de ilhas com IPv4 trafegando sobre IPv6. Esse método é chamado de transição é Tunelamento.

1.7 ESTRUTURA

Esse trabalho é estruturado em quatro capítulos. O primeiro capítulo abordará o tema do projeto, apresentando os problemas e premissas, justificativa de escolher esse tema, assim com os objetivos a serem atingido com o projeto. Além disso, apresenta um embasamento teórico, o procedimento metodológico e a estrutura do trabalho.

O segundo capítulo apresentará o referencial teórico do projeto, um breve histórico do surgimento do modelo da Internet atual; protocolo IP versão 4, sua estrutura, problemas apresentados, em especial a respeito do esgotamento dos endereçamentos; as medidas tomadas para resolver esse problema. Descrição do novo protocolo IP versão 6, sua estrutura, endereçamento; os métodos de transição do protocolo IPv4-IPv6, em especial a Pilha Dupla. Abordará também o protocolo de roteamento utilizado na simulação do ambiente, OSPFv3 e um serviço, DHCPv6 com suporte ao protocolo IPv6.

O terceiro capítulo abordará a parte prática do trabalho, apresentará os passos da configuração do ambiente de simulação de uma rede local sugerido para

demonstrar a técnica de transição do protocolo IPv4-IPv6, método da pilha-pilha dupla e a configuração de um serviço de rede, DHCP, com suporte ao novo protocolo IPv6. Além do impacto da implementação do protocolo IPv6 em uma rede local no qual já encontra-se operacional com o protocolo IPv4 e o impacto do novo protocolo nos serviços de rede, no caso o DHCP. Com essa simulação permitirá analisar os pacotes trafegando na rede, possibilitando verificar os pacotes e a operacionalização do IPv6 em uma rede local.

No quarto capítulo traz as conclusões do projeto, analisando o ambiente de simulação, apresentado o impacto na configuração do novo protocolo e de um serviço com suporte a este protocolo. E quais as considerações que os profissionais da área de redes devem ter com o referido assunto. Por fim apresentará o referencial bibliográfico utilizado para dar o embasamento teórico do trabalho.

2 REFERENCIAIS TEÓRICOS

2.1 INTERNET – SUA EVOLUÇÃO

No final da década de 60 pesquisadores financiados por uma agência do Departamento de Defesa dos EUA – *Defense Advanced Research Projects Agency* - DARPA projetaram uma rede experimental não centralizada. Em plena Guerra Fria havia constante medo a ataques aos meios de comunicação, podendo causando alguma indisponibilidade aos serviços de telecomunicação que originalmente era centralizada. A principal ideia era que rapidamente a comunicação pudesse ser restabelecida entre dois pontos em caso de falhas. Sem depender de elementos centralizadores permitindo assim que a rede se readequasse para realizar o encaminhamento da informação, utilizando caminhos alternativos disponíveis. (BRITO, 2013, p.19).

Nessa época foi instalado os quatro primeiros nós da rede, denominada ARPANET, interligando 4 universidades: Universidade da Califórnia em Los Angeles (UCLA), a Universidade da Califórnia em Santa Bárbara (UCSB), a Universidade de Utah e a Universidade de Stanford (SRI), conforme mostrado na Figura 1.

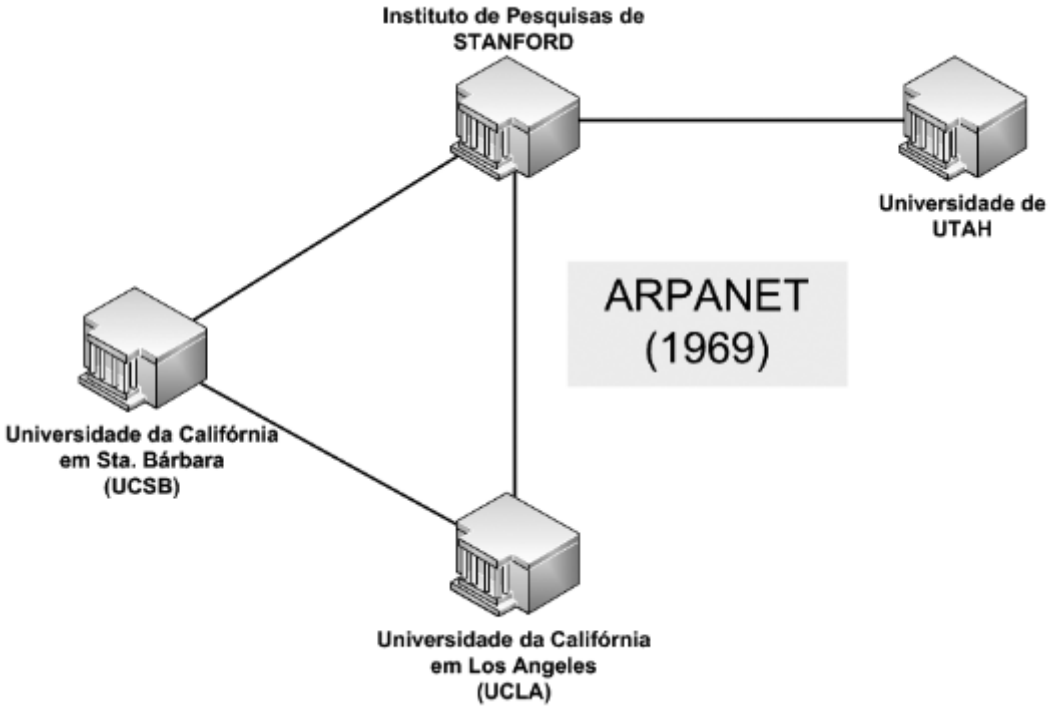

Figura 1 - Origem da Internet em 1969.
Fonte: Brito, 2013, p. 21.

A Internet com a estrutura conhecida atualmente, baseada no Protocolo IP, surgiu somente em 1983 com mais de 500 *hosts* conectados a rede. Devido a diversas pesquisas realizadas em todo mundo contribuiu para o desenvolvimento de um novo padrão de protocolos conhecido como TCP/IP e foram incorporados à rede. Segundo Brito (2013, p. 20) uma das principais características que possibilitou a Internet tornar-se o que é hoje foi devido a ser uma rede baseada em padrões abertos, onde as tecnologia que a compõem são publicadas pela *Internet Engineering Task Force* – IETF através de documentos públicos conhecidos como *Request for Comments* – RFCs, disponíveis a qualquer pessoa.

A Internet atual esta baseada no Protocolo IPv4 descrito na RFC 791 elabora nas décadas de 70 a 80. Atualmente esse protocolo é criticado como sendo um protocolo falho em vários aspectos, na época de sua elaboração não havia requisitos de escalabilidade, segurança ou mobilidade, muito requisitado nos dias

atuais. Naquele momento existiam dúvidas acerca do interesse das pessoas em computadores pessoais. E o objetivo era uma rede distribuída com a intenção de conectar algumas instituições de pesquisa (BRITO, 2013, p. 22).

Somente na década de 90 que a internet tornou-se algo comercial por meio da *World Wide Web* – WWW, com o surgimento dos primeiros servidores de páginas *Web* e o *Browser* que são *softwares* de clientes para navegação. A padronização do *Hyper-Text Markup Language* – HTML como sendo a linguagem universal para comunicação entre servidores e clientes *Web* também favoreceu para a Internet se tornar cada vez mais popular. Com o aumento na quantidade de conteúdos e serviços oferecidos, como sítios de pesquisa (buscadores), comercio eletrônico – *e-commerce*, banco *on-line*, entre outros, repercutiram no crescimento desenfreado da rede e a quantidade de usuários.

Segundo Brito (2013, p. 23) já na década de 1990 os primeiros problemas estruturais do protocolo IPv4 já ficaram evidentes tais como escalabilidade em virtude do endereçamento limitado, sem suporte à mobilidade para permitirem dispositivos móveis acessarem a rede e falta de suporte nativo à segurança de aplicações sigilosas.

2.2 PROTOCOLO IP

Segundo Filippetti (2014, p. 121) o protocolo IP define a camada internet no modelo TCP/IP e os demais protocolos dessa camada existem para suportá-lo de alguma forma. Todos os dispositivos de rede precisam de um endereço de identificação lógico denominado “endereço IP”. Esse endereço determina a origem e o destino de um pacote. Roteadores mantêm uma tabela chamada de “tabela de roteamento”, contendo informações das diferentes redes lógicas e suas respectivas

rotas (caminhos) para alcançá-las.

Um endereço IP possui duas partes: identificador de rede e identificador de host. Conforme Filippetti (2014, p. 122) o processo de identificação lógica dos dispositivos deve responder duas perguntas: qual rede IP o dispositivo encontra-se e qual a sua identificação de *host*? A primeira questão recai sobre o processo de endereçamento lógico da rede, definido pelo protocolo IP e gerenciados pelos roteadores da rede. A segunda questão há um interação entre seu endereço IP – identificador lógico do host e o endereço físico (*MAC Address*, no caso do *Ethernet*) – gerenciado pelo protocolo de camada de Enlace.

2.2.1 Protocolo IPv4

O endereço IPv4 é um identificador composto por 32 bits, separados em quatro blocos de 8 bits denominados octetos. Para facilitar sua identificação optou-se por escrevê-lo no sistema decimal e separar os octetos por pontos conhecido com notação decimal pontuada, conforme a Figura 2 (BRITO, 2013, p. 23).

Figura 2 - Notação do Endereço IPv4.
Fonte: Brito, 2013, p. 24.

O IPv4 composto por 32 bits permite endereçar 2E+32 nós da rede, equivalente a aproximadamente 4 bilhões e 300 milhões (4.294.967.296) de endereços únicos. Esse número na época que o protocolo foi concebido parecia absurdamente alto para a sua finalidade inicial e não poderia imaginar que esses endereços se esgotariam, já que não se costumavam ter computadores em casa.

(BRITO, 2013, p.25)

O protocolo IP recebe os segmentos da camada de Transporte e os encapsula em pacotes, esses pacotes recebem um cabeçalho IP contendo campos de controle, como o endereço IP de origem e endereço IP de destino. Os dispositivos da camada 3 denominados *routers* (roteadores) processam esses pacotes gerados analisando o IP de destino, identificando a porção de rede deste endereço e com base em suas tabelas de roteamento determinam qual a melhor rota para alcançar a rede remota. (FILIPPETTI, 2014, p.122)

O cabeçalho do protocolo IPv4 e seus campos pode ser analisado na Figura 3, cuja extensão é de 20 bytes.

Figura 3 - Cabeçalho do Pacote IPv4.
Fonte: http://ipv6.br/entenda/cabecalho/.

Segundo Filippetti (2014, p.122-123) os campos que compõem o cabeçalho IPv4 são:

- **Versão:** número da versão do protocolo, que pode ser 4 ou 6. Porém o protocolo versão 6 apresentar diferenças da versão 4 que serão apresentadas no decorrer do trabalho;

- **Tamanho do Cabeçalho:** campo com o comprimento do cabeçalho;
- **Tipo de Serviço (ToS):** representa a prioridade do pacote na rede, ou seja, como ele será tratado na rede em relação aos demais pacotes;
- **Tamanho Total:** campo que representa o tamanho total do pacote incluindo a porção de dados;
- **Identificação:** campo com um valor único para identificação do pacote;
- **Flags:** especifica se a fragmentação do pacote. Utilizado para transmissão segundo determinados protocolos de Enlace;
- **Deslocamento do Fragmento:** este campo permite a remontagem do pacote de dados no destino quando ocorre uma fragmentação, esse campo provê esse controle. A fragmentação pode ocorrer quando um pacote for maior que a *Maximum Transmission Unit* – MTU definida para um determinado tipo de frame. A MTU do padrão Ethernet é de 1500 bytes. Pacotes maiores que este tamanho sofrem fragmentação para serem transmitidos;
- **Tempo de Vida (TTL):** campo que estabelece o “tempo de vida” do pacote na rede. Esse valor é definido assim que o pacote é concebido na rede e decrementado por meio de contagem de saltos, ou seja, toda a vez que analisado por uma *router*. Caso o pacote não atinja seu destino antes do número máximo de saltos, o pacote será descartado. Esse procedimento impede que pacotes IP fiquem continuamente circulando na rede, gerando “*loops*” e ocupando

recursos.

- **Protocolo:** campo (em hexadecimal) usado para identificar o protocolo de camada superior (Transporte). O valor usado pelo IP para identificar o TCP é 0x6 e para UDP é 0x11;
- **Soma de verificação do Cabeçalho:** checagem de redundância cíclica aplicada apenas ao cabeçalho IP;
- **Endereço de Origem:** campo com o endereço IP de origem (4 byte ou 32 bits)
- **Endereço de Destino:** campo com o endereço IP de destino (4 bytes ou 32 bits);
- **Opções:** campo não utilizado;
- **Dados:** dados passados pela camada superior (Transporte).

A ICANN – *Internet Corporation for Assigned Names e Numbers* é a autoridade responsável pela coordenação global do sistema de identificadores exclusivos da Internet por meio da IANA – *Internet Assigned Numbers Authority*. É uma autoridade mundial responsável por gerenciar todos os endereços e nomes de domínios, que fazem a internet operar. Porém com a popularização da internet comercial na década de 90, os endereços IP começaram a serem consumidos rapidamente. Diante disso a IANA necessitou ampliar sua estrutura organizacional e autoridades de abrangência regional denominadas RIR – *Regional Internet Registry* possibilitando assim manter a governabilidade dos recursos da Internet. Essa estrutura atual é descrita na figura 4.

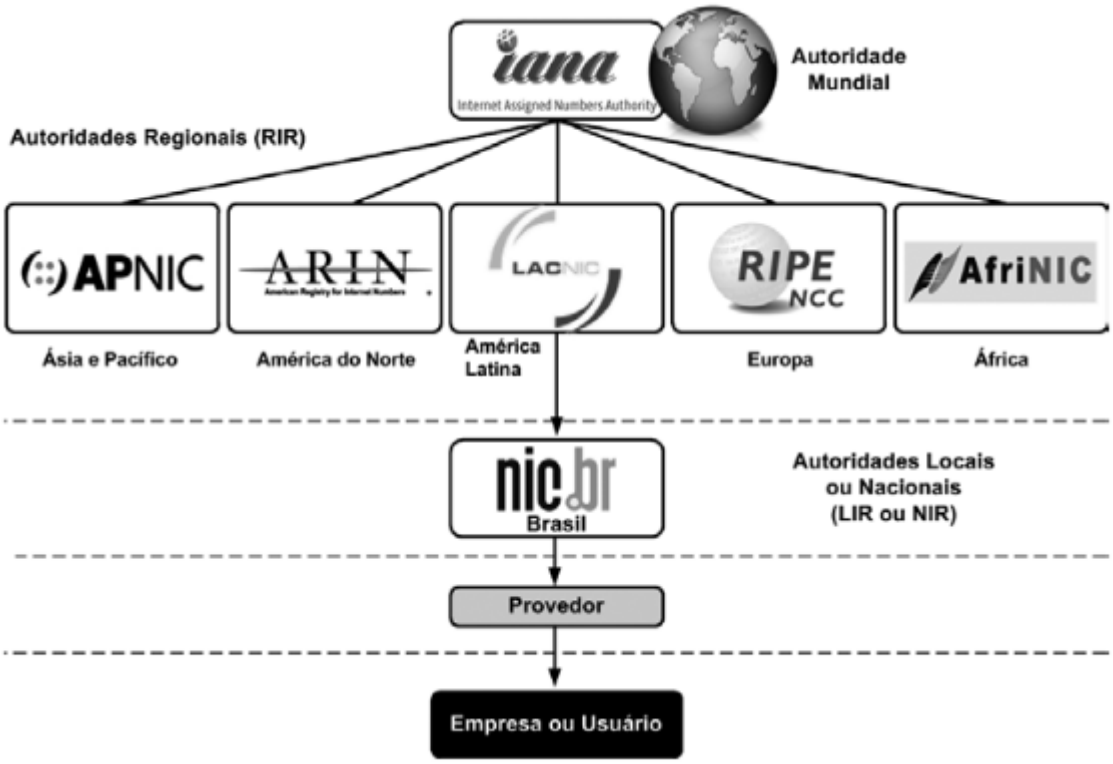

Figura 4 - Autoridades na Governança da Internet no Mundo.
Fonte: Brito, 2013, p. 26.

- ARIN – América do Norte
- LACNIC – América Latina e Caribe
- RIPE NCC – Europa
- APNIC – Ásia e Pacífico
- AfriNIC – África

A IANA na autoridade mundial gerencia a distribuição de alguns blocos às autoridades regionais que ficam responsáveis a administrar autoridades abaixo de sua hierarquia ou diretamente às operadoras e empresas de telecomunicações. No Brasil a responsabilidade fica a cargo do Núcleo de Informação e Coordenação do Ponto BR – NIC.br, autoridade nacional (NIR) que responde ao LACNIC.

O esgotamento do endereço IPv4 já era previsto pela academia desde o início da década de 90. Desde então se iniciou o desenvolvimento de um novo

protocolo, no então antes de sua elaboração foram desenvolvidos vários mecanismos paliativos. Estes mecanismos foram responsáveis por manter o IPv4 funcionando até hoje, quase 25 anos. Podemos destacar três medidas: CIDR, DHCP, NAT (BRITO, 2013, p. 26-27).

2.2.1.1 CIDR

Segundo Brito (2014, p. 28) na elaboração do protocolo IPv4 os endereços de rede foram divididos em 3 classes que especificavam dentre os 32 bits do endereço IPv4 quais representam os bits prefixo da rede e do sufixo de *hosts*. As classes foram denominadas A, B, C com 8, 16, 24 bits, respectivamente, reservados para o prefixo identificador de rede. Essa divisão permitia o endereçamento de variados tipos de rede. Redes classe A representa um ambiente com poucas redes de grande porte com muitos hosts; classe B representa redes de médio porte; e a classe C representa muitas redes de pequeno porte com poucos hosts. Conforme observado na figura 5.

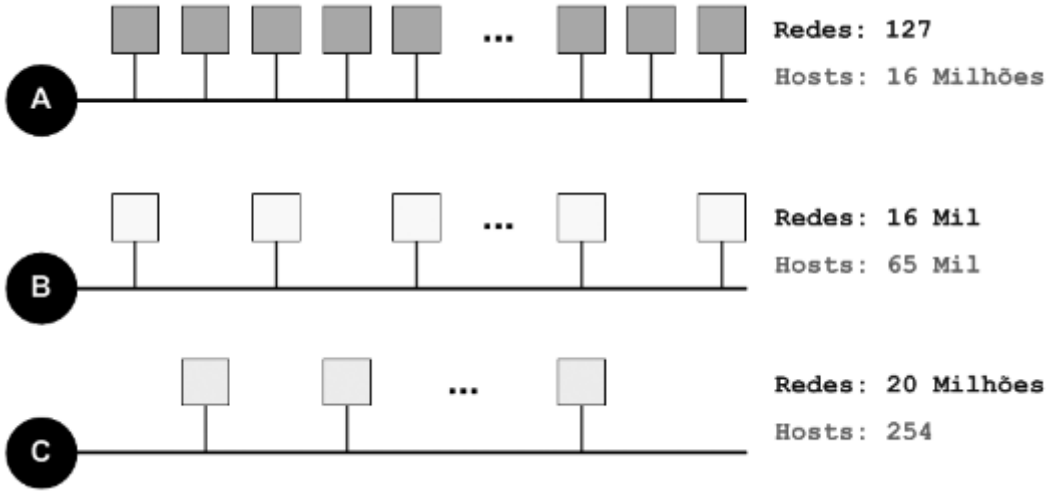

Figura 5 - Perfil das Classes Padrões de Redes/Hosts no IPv4.
Fonte: Brito, 2013, p. 28.

Essa divisão ficou a cargo dos primeiros bits do próprio endereço. Endereços

que iniciavam com 0 binários – de 1 a 127 - eram enquadrados na Classe A; os endereços que iniciavam com 10 binários - de 128 a 191 – eram enquadrados na Classe B; e os endereços iniciados em 100 binário – de 192 a 223 – eram enquadrados na Classe C.

Esse tipo de classes padrão acabou causando desperdício exagerados dos endereços na fase inicial de distribuição IPs. Isso porque empresas com mais de 254 hosts não podiam solicitar um bloco Classe C, com apenas 8 bits de identificador de hosts, era possível somente endereçar 254 hosts (2 elevado a 8 menos 2). O motivo por subtrair 2 endereços do total é que o primeiro e o último endereço de toda sub-rede são reservados para identificar a própria rede, o primeiro endereço, e para fins de *broadcast*, último endereço. Com isso essas empresas eram enquadradas em Classes superiores, no caso Classe B, com 16 bits de identificador de *hosts*, podendo assim endereçar até 65.534 *hosts*, muito acima da quantidade real necessária pela empresa. Com isso no final mais de 65 mil endereços dessa alocação eram desperdiçados.

O *Classless Inter-Domain Routing* – CIDR foi definido em setembro de 1993 na RFC 1519, no qual propõem a flexibilização dessas classes padrões, de maneira que os bits reservados para identificar a porção de rede e *host* pudessem ser localizada em qualquer posição dentre os 32 *bits* do endereço IP. Isso possibilitou otimizar a alocação de endereços, porém era necessário um novo elemento que representasse essa fronteira entre a porção de rede e hosts, esse elemento foi chamado: máscara de rede. A máscara de rede é representada em 32 bits, igual ao endereço IPv4, no qual é formada por um prefixo de bits 1s, que identifica a porção de rede e um sufixo de 0s, que identifica a porção de *hosts*, sendo que não há intercalação em 1s e 0s.

A máscara de rede pode ser escrita de forma simplificada, apontando apenas a quantidade de bit*s* do prefixo de rede procedido por uma barra “/”. Na figura 6 traz um exemplo das máscaras de rede das classes padrões: /8 (255.0.0.0), /16 (255.255.0.0) e /24 (255.255.255.0).

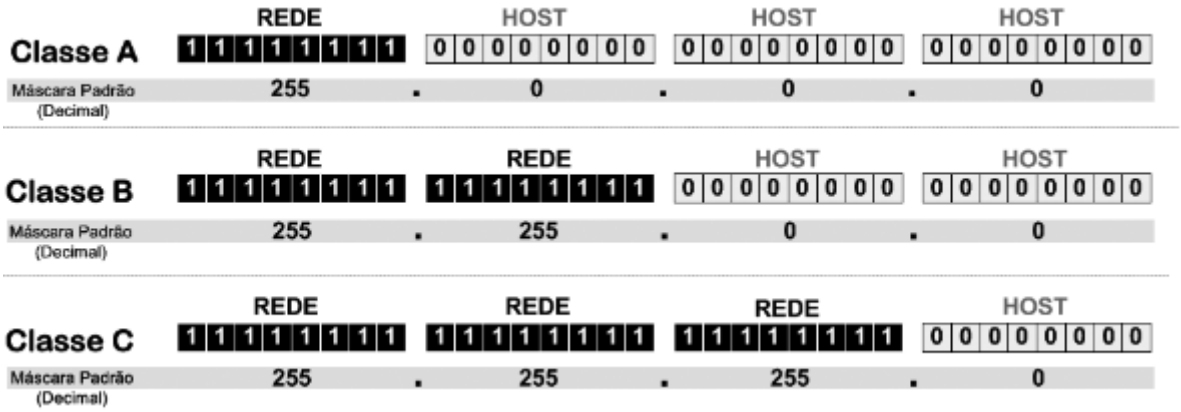

Figura 6 - Máscaras de Rede das Classes Padrões.
Fonte: Brito, 2013, p. 30.

Com o CIDR permite otimizar e muito a alocação de endereços, como citado anteriormente, empresas com mais de 254 *hosts* necessitavam uma alocação de um bloco B, caso um empresa necessitasse por exemplo 400 *hosts*, com o CIDR será necessário 9 bit*s* para identificar os *hosts*, onde 2 elevado a 9 permite até 510 hosts. Com isso um prefixo de rede com 23 bit*s* atenderia às necessidades da empresa sem implicar em tanto desperdício conforme demonstrado anteriormente. A figura 7 demonstra como ficaria a máscara de rede /23.

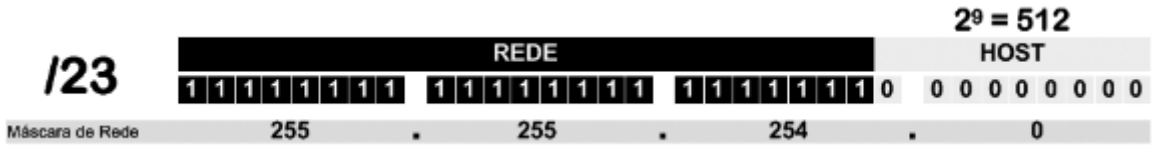

Figura 7 - Exemplo de CIDR na economia de endereços IPv4.
Fonte: Brito, 2013, p. 30.

Segundo Brito (2013, p. 31) o maior desperdício de endereços IPv4 aconteceu no início do processo de distribuição dos endereços, antes do CIDR grande empresas como *IBM, AT&T, HP, Apple* entre outras receberam blocos da

Classe A, no qual é importante destacar que cada bloco Classe A possui mais de 16 milhões e todos as 126 redes possíveis representam metade do total de endereços do IPv4.

2.2.1.2 DHCP

Segundo Brito (2013, p. 31) o *Dynamic Host Configuration Protocol* – DHCP foi especificado em outubro de 1993 e atualizado em 1997 na RFC 2131. É um protocolo que distribui os endereços automaticamente para os hosts da rede, diminuindo os esforços da configuração dos nós da rede. O DHCP foi outra medida paliativa para economizar endereços IPv4 roteáveis na Internet. Para os provedores de acesso à Internet denominados de ISP, esse protocolo possibilitou que seus clientes recebessem um endereço público por “empréstimo”, ou seja, recebiam IPs dinâmicos somente enquanto tivessem conectado à rede, quando desconectado esse endereço é devolvido para o ISP que poderia redistribuí-lo a outro cliente,

Com isso iniciou-se um novo modelo de negócio no qual as conexões residenciais se tornaram mais baratas, pois não havia a necessidade de um endereço exclusivo por cliente. Esse protocolo é ruim do ponto de vista de segurança, como os clientes não possuem um endereço fixo dificulta a identificação de cada cliente. Os servidores DHCP são de natureza *stateful*, ou seja, mantêm um registro dos endereços emprestados vinculando aos clientes, mesmo com esse mecanismo ainda é uma técnica que dificulta a identificação da rede.

2.2.2 Protocolo IPv6

O IPv6 é a nova versão do Protocolo IP e foi desenvolvido com o intuito de solucionar definitivamente o problema com a escassez do endereços disponíveis na

internet. Segundo Brito (2013, p. 51) O IPv6 é constituído de 128 bits, 4 vezes maior que seu antecessor – IPv4 (32 bits), isso não representa que o IPv6 seja 4 vezes maior na quantidade de endereços que IPv4. Pois vale lembrar que a adição de um bit no endereço IPv4 dobra a quantidade de endereços disponíveis, por se tratar de crescimento exponencial. Com isso, o IPv6 possibilita o endereçamento de:

340.282.366.920.938.463.374.607.421.768.211.456 (aproximadamente 340 undecilhões) nós públicos na internet. Isso equivale a 79 trilhões de trilhões de vezes a quantidade atual de endereços IPv4, que é aproximadamente 4 bilhões de endereços.

O cabeçalho IPv6 possui um formato otimizado com apenas 8 campos conforme descrito na figura 8. O cabeçalho possui um tamanho fixo de 40 bytes, um diferencial impactante no desempenho dos roteadores da rede, uma vez que não é necessário os equipamentos analisarem previamente o extinto campo: “IHL” (Tamanho do Cabeçalho) para determinar o tamanho do cabeçalho, antes de analisar as demais informações de controle (BRITO, 2013, p. 42)

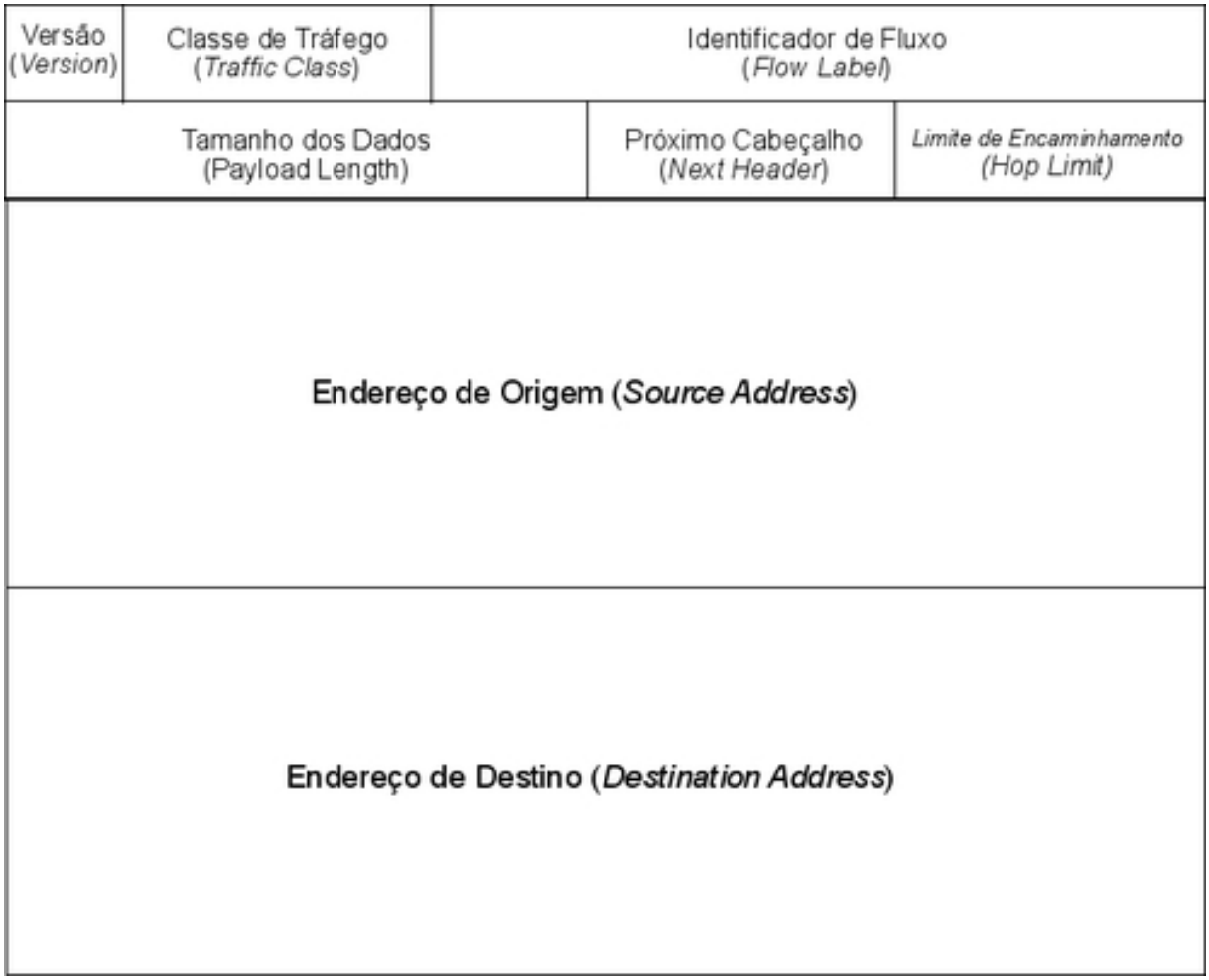

Figura 8 - Cabeçalho do protocolo IPv6.
Fonte: http://ipv6.br/entenda/cabecalho/.

Segundo o Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (2014) o cabeçalho IPv6 é dividido nos seguintes campos:

- **Versão (4 bits):** Identifica a versão do protocolo. Esse campo é 6.
- **Classe de Tráfego (8 bits):** Identifica os pacotes por classes de serviço ou prioridade. Mesmo funcionalidade do “Tipo de Serviço do IPv4”.
- **Identificador de Fluxo (20 bits):** Identifica pacotes do mesmo fluxo de comunicação.
- **Tamanho dos Dados (16 bits):** Indica o tamanho, em Bytes, apenas dos dados enviados juntos ao cabeçalho IPv6. Substitui o campo “Tamanho

Total do IPv4”, que apresentava o tamanho do cabeçalho mais o tamanho dos dados. Nesse campo os cabeçalhos de extensão também são somados.

- **Próximo Cabeçalho (8 bits):** Indica o cabeçalho de extensão que segue o atual. No IPv4 chamava-se “Protocolo”.
- **Limite de Encaminhamento (8 bits):** Campo decrementado a cada salto de roteamento e indica o número máximo de roteadores que o pacote pode passar antes de ser descartado. No IPv4 é denominava-se “TTL”, ou “Tempo de Vida”.
- **Endereço de Origem (128 bits):** Indica o endereço de origem do pacote.
- **Endereço de Destino (128 bits):** Indica o endereço de destino do pacote.

Segundo Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (2014) dentre as mudanças do entre o cabeçalho IPv4 e IPv6, destaca-se a remoção de seis campos, tanto do resultado da inutilização de suas funções quanto de sua reimplementação em cabeçalhos de extensão, conforme descrito na figura 9.

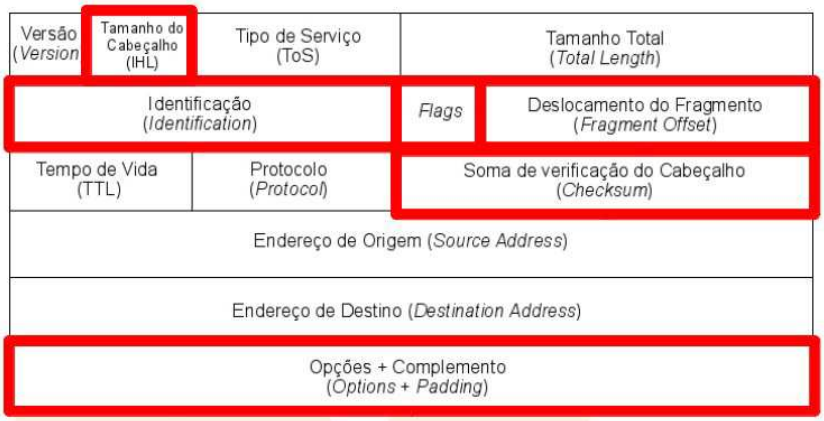

Figura 9 - Destaque dos campos do cabeçalho do protocolo IPv4 removido no cabeçalho do protocolo IPv6.
Fonte: http://ipv6.br/entenda/cabecalho/.

A primeira remoção foi o campo “Tamanho do Cabeçalho”, que se tornou desnecessário devido ao tamanho fixo do IPv6. Os campos: “Identificação”, “Flags”, “Deslocamento do Fragmento” e “Opções e Complementos” passaram a ser cabeçalhos de extensão apropriados. E o campo “Soma da verificação do Cabeçalho” foi removido com a finalidade de aumentar a eficiência do protocolo, uma vez que outras validações são realizadas pelos protocolos das camadas superiores. Outras alterações foram a renomeação e reposicionamento de quatro campos: “Tipo de Serviço” no IPv4 para “Classe de Serviço” no IPv6; “Tamanho Total” no IPv4 para “Tamanho dos Dados” no IPv6; “Tempo de Vida (TTL)” no IPv4 para “Limite de Encaminhamento” no IPv6 e “Protocolo” no IPv4 para “Próximo Cabeçalho” no IPv6. O campo “Identificador de Fluxo” foi adicionado no IPv6 para possibilitar o funcionamento de um mecanismo extra de suporte a QoS. Por fim os campos: ”Versão”, “Endereço de Origem”, “Endereço de Destino” foram mantidos, porém aumentaram de tamanho (CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES, 2014)

2.2.2.1 Cabeçalhos de Extensão

Segundo Brito (2013, p. 44) o cabeçalho IPv6 foi simplificado e pode ter sido

fixado em 40 bytes, devido a remoção do campo: “opções” do IPv4 para contemplar informações complementares que podiam nem existir no IPv4. No IPv6 os Cabeçalhos de Extensão, são cabeçalhos adicionais que fazem essa funcionalidade, antes feita através do campo: “opções” no IPv4. Esses cabeçalhos não precisam ser verificados pelos roteadores intermediários na comunicação, refletindo em melhor desempenho na rede em decorrência de menos processamento nos roteadores.

Um ou mais cabeçalhos de extensão são anexados ao cabeçalho IPv6 de maneira encadeada, através dos seus respectivos códigos de próximo cabeçalho, flexibilizando a implementação de diferentes funcionalidades. A RFC 2460 determina a sequência de encaminhamento dos cabeçalhos de extensão conforme descrito na figura 10 (BRITO, 2013, p. 45)

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

Figura 10 - Encadeamento de cabeçalhos de extensão no IPv6.
Fonte: Brito, 2013, p. 45.

Segundo Brito (2013, p. 45) dentre os pacotes de extensão o único que deve ser interpretado por todos os roteadores intermediários é o pacote: “*Hop-by-Hop*” , por isso é o primeiro cabeçalho de extensão, os demais tipo só são analisado no roteador de destino.

2.2.2.2 Notação do Endereço

O IPv6 é escrito em formato hexadecimal (base 16), sendo 128 bits divididos em 8 grupos de 16 bits cada um, separados pelo caractere: dois pontos - ”:” denominado quarteto. Exemplo de um endereço: (BRITO, 2013, p. 52)

2001:0db9:cafe:0000:8e77:6aff:faaa:10bc

A notação do endereço IPv6 permite utilizar letras maiúsculas ou minúsculas em sua descrição, considerando assim o mesmo endereço. Optou-se em utilizar a base hexadecimal por permitir a escrita dos endereços em menores tamanhos. Embora o hexadecimal diminua esse tamanho, o IPv6 é extenso e manipulá-lo é trabalhoso, motivo pelo qual o DNS – mecanismo de resolução de nomes – tornar-se ainda mais importante.

Duas técnicas de abreviação do endereço IPv6 foram criadas para simplificar sua representação. Uma das regras permite omitir todos os zeros à esquerda de um quarteto, ou seja, “00b2” pode ser representado por ”b2”; quando um quarteto apresentar somente zeros “0000” pode ser representado com apena um zero “0”.

Outra regra de abreviação permite representar uma sequência contínua de zeros através do caractere “::”, essa regra é permitida ser aplicada somente uma vez na representação do endereço IPv6. Pois pode representar uma ambiguidade, tornando impossível descobrir qual o endereço original (BRITO, 2013, p.54)

Um exemplo das regras de abreviação pode ser apresentada da seguinte forma, através do endereço IPv6:

2001:0db8:0000:0000:0000:0000:0000:00b1

Aplicando a regra de abreviação de 0s à esquerda, o endereço poderia ser descrito dessa forma:

2001:db8:0:0:0:0:0:b1

E aplicando a regra da abreviação de zeros contínuos, o endereço poderia ser descrito dessa forma:

2001:db8::b1

As três formas apresentadas representam o mesmo endereço, porém aplicando ou não as regras de abreviação.

Com a utilização do caractere: “:” para separação dos quarteto do endereço IPv6, pode causar uma confusão entre o endereço IPv6 e a porta quando o endereço for utilizado na URL dos navegadores. Devido a isso a RFC 2732 define que endereços IPv6 devem ser descritos entre colchetes na URL dos navegadores, exemplo:

http:///[2001:db7:abcd::1]:8080/index.html

O NIC.BR disponibiliza um guia didático de endereçamento IPv6, no qual demonstra a estrutura de um endereço IPv6 e como pode ser dividido, conforme observado na figura 11.

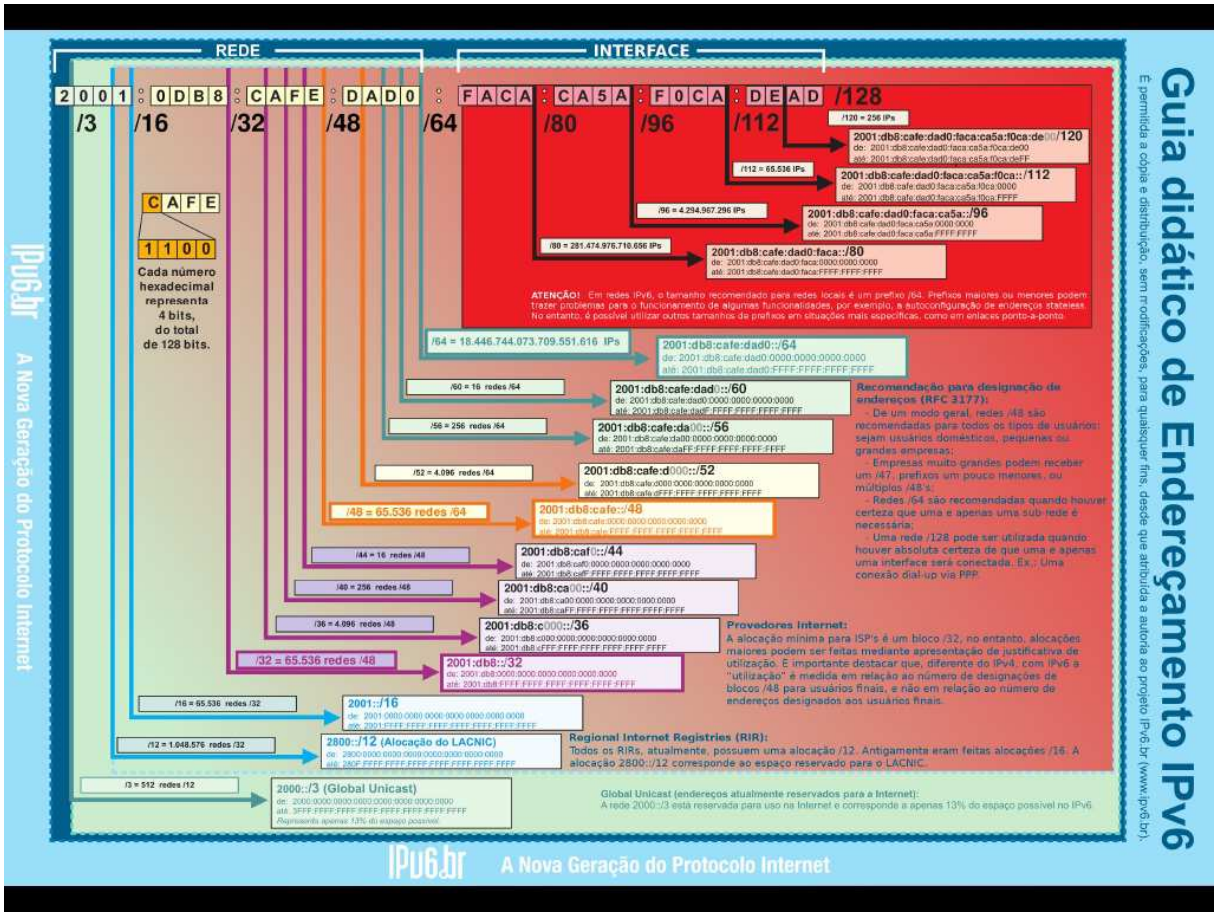

Figura 11 - Guia de didático de endereçamento IPv6.
Fonte: Florentino, 2011.

2.2.2.3 Tipo de Endereços

Existem tipos diferentes de endereços no que se refere à natureza da comunicação em redes de computadores. No IPv4 os endereços podem ser de três tipos: *unicast* é aquele destinado a um único nó da rede; *multicast* é aquele destinado para vários nós de um grupo; e o *broadcast* é aquele destinado a todos os nós da rede. No IPv6 ocorreram algumas mudanças, conforme pode ser observado na figura 12. Existem 3 tipo de comunicação: *unicast*, *multicast* e *anycast*. O *broadcast*, que no IPv4 consistia do último endereço válida de cada sub-rede, no IPv6 essa opção passa a ser responsabilidade de um grupo *multicast* específico, o *multicast-all-nodes*, no qual todos os nós fazem parte quando a interface é ativada e é identificado pelo endereço ff02::1 (BRITO, 2013, p. 57).

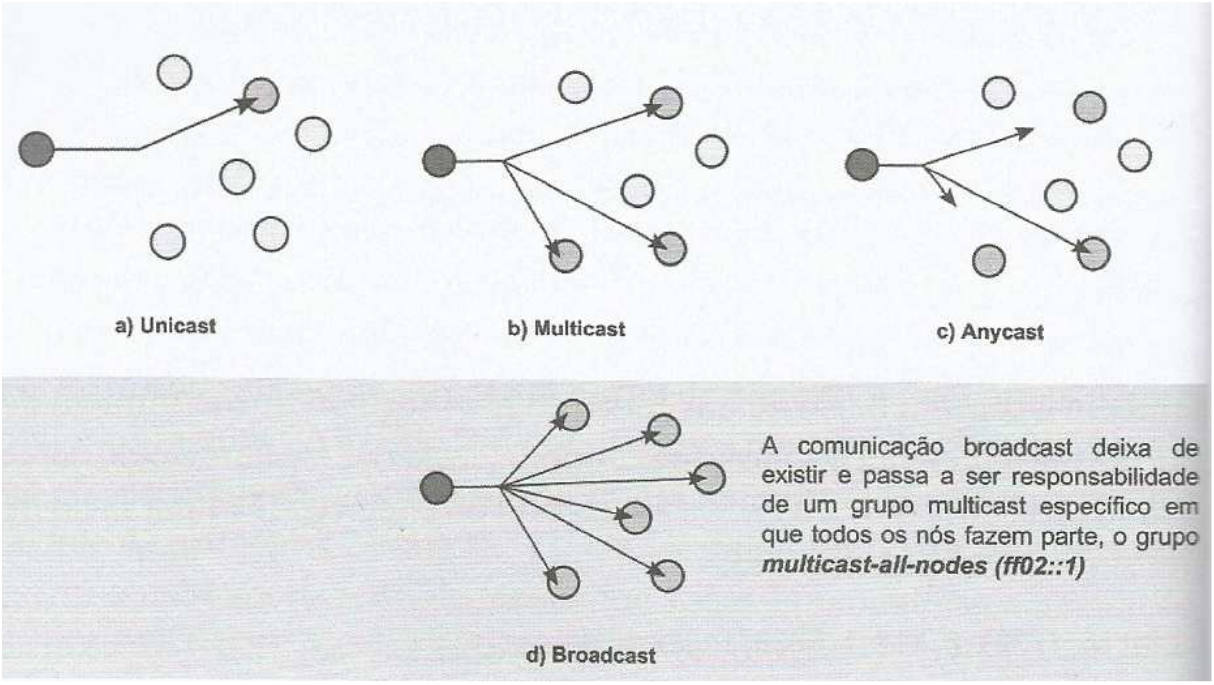

Figura 12 - Tipo de comunicação em redes.
Fonte: Brito, 2013, p. 58.

O *unycast* é novo modelo no IPv6 que consiste na comunicação destinada para o nó mais próximo de um grupo de nós, ou seja, permite a atribuição de um mesmo endereço para múltiplos nós, descrevendo a palavra *anycast* em sua configuração (BRITO, 2013, p. 58).

2.2.2.3.1 Endereços unicast

Segundo Brito (2013, p. 58) um endereço *unicast* identifica um *host* específico na rede, de modo que o envio de um pacote para esse endereço será entregue para uma única interface. Com o IPv6 viabiliza a manutenção do modelo fim-a-fim da internet, pois cada *host* da rede terá seu próprio endereço público. No IPv6 os endereços *unicast* podem ser de três tipos: *link-local*, *unique-local* ou *global unicast*.

2.2.2.3.1.1 Link-Local

Os endereços do tipo *link-local* sempre existem e são automaticamente

atribuídos as interfaces. São reservados para comunicação local em nível de enlace e são responsáveis por operacionalização de várias funcionalidades do IPv6 como: autoconfiguração, descoberta de vizinhança, protocolos de roteamento, entre outros. Pacotes com esses endereços não são encaminhados a outras redes, dando origem ao nome *link-local*, sendo restritos somente a rede local. Esses endereços são iniciados em fe80::/10, fe90/10, feA0::/10 e feB0::/10 (BRITO, 2013, p. 59).

2.2.2.3.1.2 Unique-Local Address (ULA)

Os endereços *unique local*, também denominados ULA, equivalem aos endereços privados do IPv4. São somente roteáveis no contexto local, no IPv6 foi reservado um bloco FC00::/7 para endereços privados.

Embora seja preferível a utilização de endereços públicos, pode haver o interesse de algumas empresas não atribuir endereços públicos para alguns dispositivos internos da rede, como por exemplo: impressoras ou mesmo para toda uma sub-rede sem acesso à Internet.

Segundo Brito (2013, p. 61) a questão de endereços privados no IPv6 gerou várias discussões, alguns favoráveis e outros contrários. Por conta dessa indefinição a ULA – estrutura de alocação de endereços - sofreu diversas mudanças, a recomendação atual é definida na RFC 4193.

2.2.2.3.1.3 Global Unicast

Os endereços desse tipo são públicos e roteáveis e ficam sob a responsabilidade das IANA a coordenação e distribuição de maneira coerente. O bloco separado para esse tipo se endereço o prefixo: 2000::/3, no qual equivale da faixa entre 2000:: até 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. A IANA distribui prefixos /12 para as

autoridades globais é possível criar assim 512 prefixos /12. Destes somente 6 foram distribuídos, permitindo uma sobresalência de mais de 500 prefixos /12. (BRITO, 2013, p. 62)

2.2.2.3.2 Endereço Multicast

Esse tipo de endereço não é exclusividade do IPv6, no IPv4 são representados pela Classe D, endereços de 224.0.0.0 a 239.0.0.0. E são utilizados por aplicações de comunicações, como por exemplo: serviços de teleconferência, monitoramento, entre outros. No IPv6, o *multicast* é fundamental para seu funcionamento, no momento que as interfaces são ativas elas passam a integrar a vários grupos padronizados que fazem parte da operacionalização do IPv6. Esses endereços iniciam-se com FF00::/8 , importante ressaltar que endereços iniciados com FF são sempre dessa natureza e não são utilizados na origem de uma comunicação, uma vez que representa um grupo de múltiplos nós da rede. Como citado anteriormente um grupo denominado *multicast-all-nodes* (FF02::1) substitui o broadcast do IPv4. Outro grupo fundamental no IPv6 é o *multicast-all-routers* (FF02::2) no qual esta associada a todas as interfaces dos roteadores (BRITO, 2013, p. 63).

Vários destes grupos *multicast* estão padronizados na RFC 2375, no qual de destacamos os grupos do Protocolo OSPFv3 (roteadores) endereço FF02::5, OSPFv3 (roteadores designados) endereço FF02::6, todos os servidores DHCP e *relay-agents* endereço FF02::1:2 (enlace) e Todos os servidores DHCP (site) FF05::1:3 (BRITO, 2013, p. 64).

2.2.2.3.3 Endereço Anycast

Novidade no IPv6, permite uma comunicação destinada para o nós mais próximo de um grupo de nós. Um exemplo deste tipo de endereço é quando existem vários servidores DNS pelo ambiente, esse tipo de endereço permite que os clientes sejam sempre direcionados para o servidor mais próximo, otimizando o desempenho da rede (BRITO, 2013, p. 65).

2.2.2.3.4 Endereços Especiais

Existem endereços especiais no IPv6 com no IPv4. Todo o bloco 127.0.0.0/8 no IPv4 é reservado para testes de conectividade local (*loopback*), no IPv6 para evitar um desperdício de 16 milhões de endereços, ao invés de todo um bloco foi destinado um endereço único de *loopback*: 0000:0000:0000:0000:0000:0000:0000:0001/128 ou ::1/128. Outro endereço especial é o ::/128 que corresponde ao 0.0.0.0/32 no IPv4, que representa um “endereço não especificado”. Endereço de rota padrão no IPv6 é denominado ::/0, que equivale ao 0.0.0.0/0 no IPv4 e são utilizados em roteadores para apontar a rota de saída quando não há um rota específica (BRITO, 2013, p. 65)

2.2.2.4 DHCPv6

O DHCP foi desenvolvido para otimizar a utilização dos endereços públicos no IPv4 e é responsável por manter uma tabela com o estado dos clientes associando os endereços físicos (MAC) com os endereços lógicos (IP), além de outras informações; esse tipo de serviço é de natureza *stateful*, no qual mantém esse registro com as informações dos cliente. No IPv6 nativamente as redes tem suporte ao processo de autoconfiguração *stateless*, onde as máquinas são capazes

de gerar seu próprio endereço IPv6. Devido a isso em redes IPv6 o DHCP seria algo indispensável, porém pode ser utilizado para fins de gerência ou apenas prover informações complementares que são importantes para a rede como: endereços de um servidor DNS, servidor de tempo – NTP, servidor TFTP para transferências de arquivos, necessários em algumas soluções com VoIP e *Wireless* (BRITO, 2013, p. 95)

O DHCPv6 é definido na RFC 3315, a comunicação ocorre nas portas 546/UDP e 547/UDP. No IPv6 o DHCPv6 permite duas modalidades: *stateless* e *stateful*. (BRITO, 2013, p. 96)

2.2.2.4.1 DHCPv6 Stateless

É uma modalidade bastante simplificada do DHCPv6, pois não salva o registro relacionado a máquina com o endereço IP, utiliza como base o processo de autoconfiguração do endereço, consome poucos recursos e atribui apenas informações complementares importantes na rede como: DNS, NTP, TFPT. Na figura 13 apresenta um exemplo de configuração de endereço no serviço DHCPv6 *stateless*

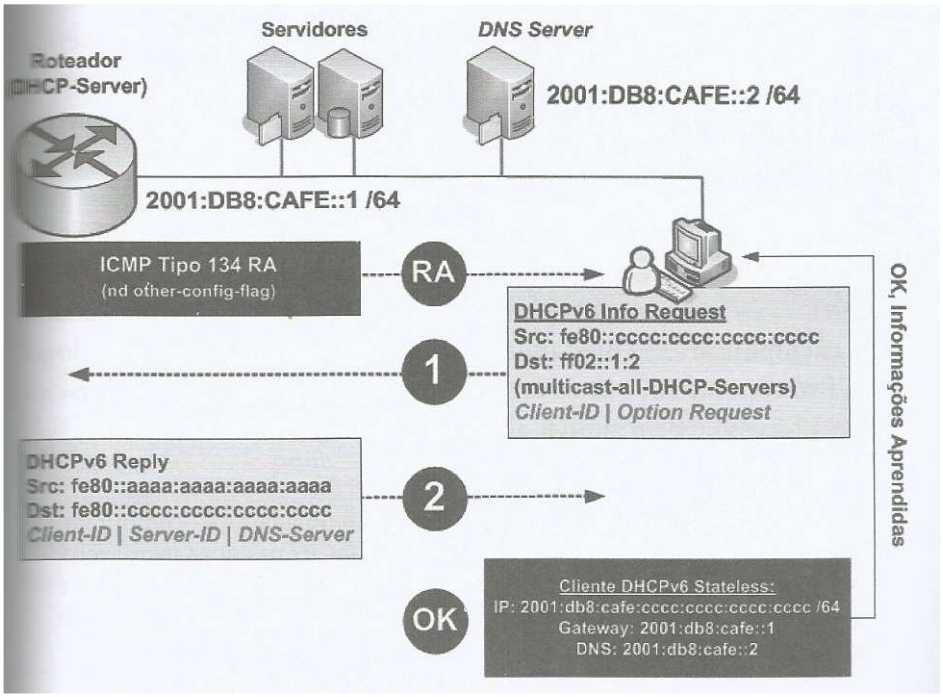

Figura 13 - Configuração de endereço no servidor DHCPv6 Stateless.
Fonte: Brito, 2013, p. 97.

2.2.2.4.2 DHCPv6 Stateful

A modalidade *stateful* acaba sendo uma reprodução do tradicional DHCPv4, o servidor acaba provendo todas as informações de endereçamento, mantém um registro com as informações dos clientes relacionadas aos endereços. É comumente empregado em servidores baseados em *Linux* e *Windows*, pois somente alguns roteadores têm suporte a essa modalidade. Nessa modalidade o “diálogo” DHCPv6 consiste em quatro mensagens básicas: *solicit, advertise, request* e *repl*, conforme mostrado na figura 14. Esse processo é bastante similar com o DHCPv4. (BRITO, 2013, p.99).

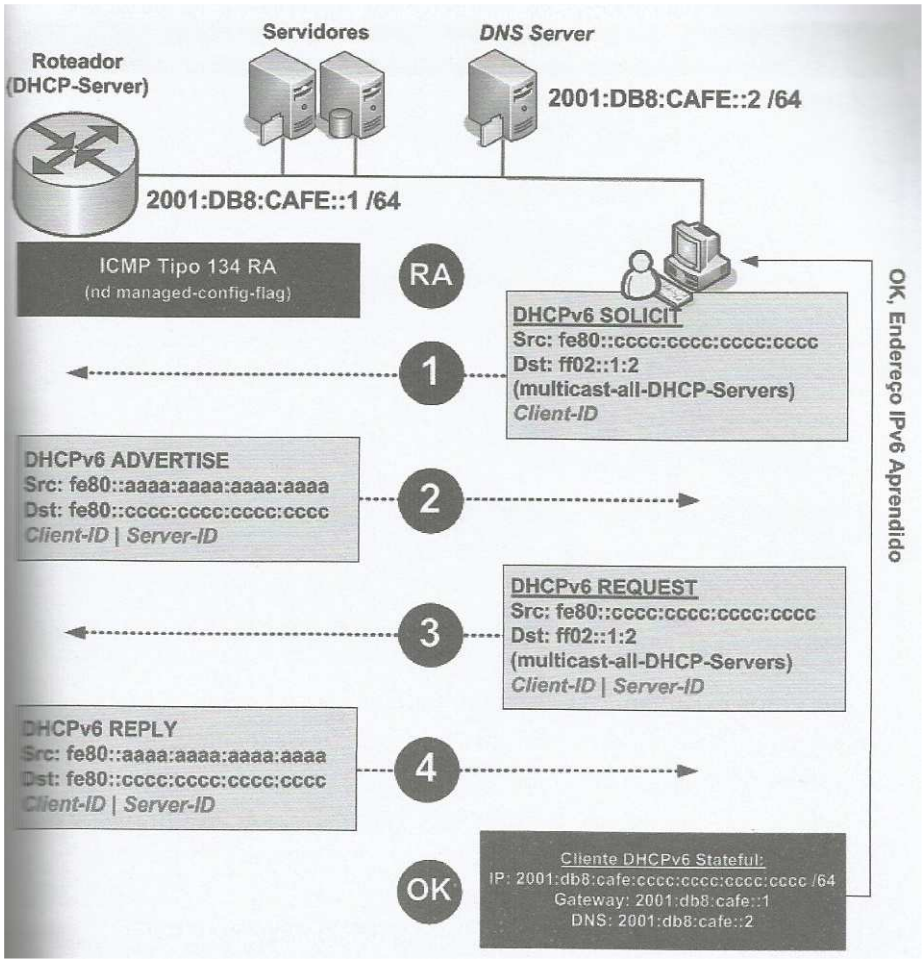

Figura 14 - Configuração de endereço no serviço DHCPv6 Stateful.
Fonte: Brito, 2013, p. 99.

2.2.2.3.3 DHCPv6 Delegação de Prefixos

Este é um recurso novo no DHCPv6, no qual o servidor recebe um prefixo da rede /56 e é capaz de gerar automaticamente subprefixos /64 e entregá-los às sub-redes diretamente conectadas. Esse recurso torna-se interessante para provedores, um exemplo desse recurso é descrito na figura 15 (BRITO, 2013, p.101).

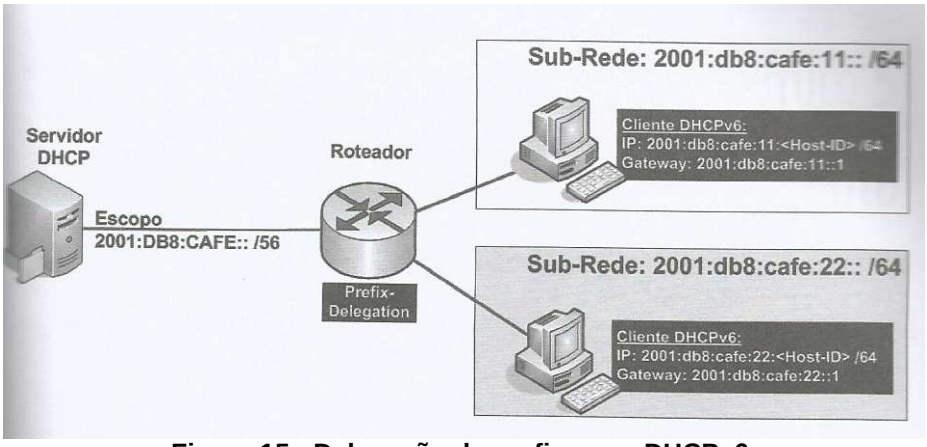

Figura 15 - Delegação de prefixos no DHCPv6.
Fonte: Brito, 2013, p. 101.

2.3 ROTEAMENTO

Segundo Brito (2013, p.103) o roteamento é a técnica que define por meio de um conjunto de regras como os dados originados em uma determinada rede devem alcançar outra. Existem duas formas de roteamento: estático e dinâmico. Estático é quando utilizada informações configuradas manualmente pelo administrador; vantagem dessa técnica: consome menos recursos de processamento do roteador e menos tráfego na rede, pois na utiliza de nenhum protocolo de roteamento dinâmico.

O roteamento dinâmico por sua vez necessita de informações de rotas no qual é aprendidas automaticamente através de troca de mensagens entre os roteadores. Podem ser de dois tipos: interno – IGP é um roteamento dentro de uma empresa; e externo – EGP é o roteamento utilizado no contexto da internet (BRITO, 2013, p. 103).

2.3.1 OSPFv3

O Protocolo OSPFv3 – *Open Shortest Path First v3* é definido na RFC 2740 é um protocolo de roteamento dinâmico do tipo *link-state*, ou seja, utiliza o estado do enlace na composição da métrica, contabilizando assim o custo de um determinado

caminho da origem até seu destino e utiliza o que possuir o melhor desempenho, ou seja, o menor custo. O OSPFv3 tem suporte a IPV6 e é o sucessor do protocolo OSPFv2 utilizado no IPV4. Assim com seu antecessor, se comunica com seus roteadores vizinhos por meio dos grupos *multicast*, no IPv4 utiliza os IPs: 224.0.0.5 e 224.0.0.6, no IPv6 utiliza os grupos *multicast*: FF02::5 e FF02::6 (BRITO, 2013, p. 115).

O OSPFv3 continua sendo, como seu antecessor, um protocolo hierárquico que permite a divisão lógica de ambientes grandes em regiões menores denominadas área. Onde sempre deve haver uma área principal de *backbone*, no qual as outras áreas são conectadas (BRITO, 2013, p. 116).

O OSPFv3 utiliza o identificar do roteador – *Router-ID* com 32 bits igual a versão IPv4, esse identificador é usado para identificar os roteadores da rede e qual será o roteador principal nos processos de roteamento. Na versão IPv4 quando esse identificador não era configurado manualmente era utilizado um endereço IPv4 previamente configurado em alguma interface física ou lógica. Como no IPv6 pode não haver esse endereço IPv4 configurado, esse identificador dever ser configurado manualmente. Outra diferença entre o OSPFv3 e OSPFv2 diz respeito a sua comunicação, na versão IPv6 ocorre por enlace enquanto a IPv4 é por sub-rede (BRITO, 2013, p. 117).

2.4 MECANISMOS DE TRANSIÇÃO

Segundo Brito (2013, p.178) os mecanismos de transição permite manter a internet como sendo uma só para os usuários, ou seja, apesar da complexidade de coexistência entre os dois protocolos IPv4 e IPv6 essas técnicas viabilizam a interoperabilidade entre as “ilhas” com protocolos IPs diferentes, de forma

transparente para o usuário. Será crucial a adoção de mecanismos de transição para que o usuário não seja prejudicado em relação à sua percepção do conteúdo existente na internet, pois até que essa transição seja concretizada pode levar alguns anos ou até mais que uma década, terá ilhas baseadas em IPv4 e outra baseadas em IPv6.

Há vários mecanismos de transição e todos podem ser classificados em três categorias: Pilha Dupla, Tunelamento e Tradução. Cada categoria tem sua particularidade, dessa forma não é possível afirmar com certeza qual é a melhor entre todas. Segundo Brito (2013, p.180) existem algumas recomendações que auxiliam a escolha dos mecanismos:

- Deve-se optar pelo método da Pilha Dupla sempre que possível, por ser uma estratégia de adoção nativa do IPv6 na infraestrutura e máquinas da rede;
- As técnicas que prolonguem a vida útil do IPv4 devem ser desencorajadas, pois retardarão mais o processo de transição da rede. Técnicas essas como: Tunelamento e Tradução;
- Nas técnicas de tunelamento é conveniente a escolha de natureza *stateless* do que *stateful*. A natureza *stateful* é mais onerosa, pois requer armazenamento de registros e informações, como consequência maior poder computacional dos dispositivos;
- Novos mecanismos são propostos e logo tornam se obsoletos, é importante analisar o grau de maturidade da técnica;
- O sucesso de uma técnica em determinado ambiente não representa que seja o melhor método em outros ambientes, pois cada

ambiente possui suas particularidades.

2.4.1 Pilha Dupla

É uma técnica que consiste em operacionalizar e configurar ambos os protocolos IPv4 e IPv6 na rede, de maneira gradativa, implicando na existência de duas redes em paralelo. Essa técnica de Pilha Dupla permite que redes que estejam operando em apenas um dos protocolos possam funcionar normalmente e essa estratégia tende a facilitar o processo de transição para o IPv6, até quando o ambiente seja consolidado todo baseado em IPv6, podendo assim ser desativado definitivamente o protocolo IPv4 em todos os nós. Na figura 16 mostra um exemplo de ambiente operando em Pilha Dupla (BRITO, 2013, p. 182).

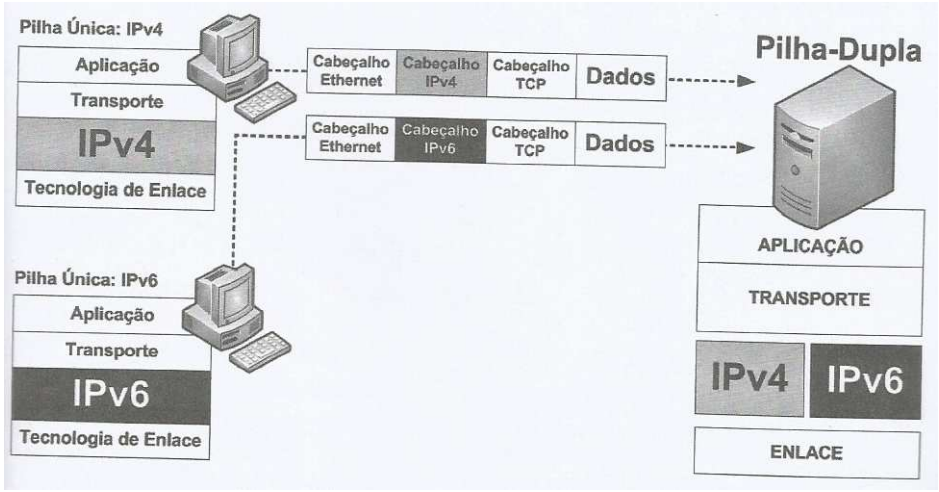

Figura 16 - Servidor operando em Pilha Dupla.
Fonte: Brito, 2013, p. 181.

A Pilha Dupla é considerada uma estratégia evolucionista, no qual o IPv6 esta sendo inserido na rede de forma gradativa, implicando em maior maturidade no processo de aprendizado da operacionalização do novo protocolo IPv6. Por outro lado é uma técnica que tendo a ser operar por um longo tempo e o fato de manter os dois protocolos ativos na rede traz maior complexidade a gestão da rede. Pois são protocolos distintos em operação, o que duplica os esforços de gestão e

operacionalização (BRITO, 2013, p. 182).

Com ambos os protocolos operando na rede, o serviço de resolução de nomes – DNS dava inicialmente prioridade para a resolução dos registros com IPv6 (AAAA), por ser um estratégia evolucionista, contudo começou a apresentar uma característica negativa e começou a tornar a Internet mais lenta, porque as aplicações ao realizarem uma busca por nome ficavam aguardando o retorno do registro IPv6 até seu tempo limite (*time out*) fosse esgotado, mesmo que o registro IPv4 (A) já estivesse sido resolvido. Isso fez com que os usuários inferissem que o desempenho da rede IPv6 fosse pior que a rede IPv4. Esse problema foi resolvido na RFC 6555, publicada em abril de 2012, no qual mantém a preferência pelo uso do IPv6, porém o registro que respondesse antes seria utilizado. Essa solução ficou conhecida como “*Happy Eyeballs*” ou “*Fast Fallback*” (BRITO, 2013, p. 182).

2.4.2 Tunelamento

Técnicas de tunelamento, segundo Brito (2013, p. 183), é uma técnica útil quando não pode ser utilizada a Pilha Dupla nos dispositivos e é amplamente adotada durante o período de transição do protocolo. É uma técnica que permite o tráfego baseado em um protocolo ser transportado por meio de outro protocolo, ou seja, quando pacotes IPv6 serem transportados (tunelados) sob pacotes IPv4. Inicialmente esperasse a necessidade de tunelamentos neste sentido, pacotes IPv6 em redes IPv4. Com a disseminação das redes IPv6, esperasse futuramente, uma maior quantidade de tunelamentos de pacotes IPv4 em redes IPv6, conforme mostrada na figura 17 (BRITO, 2013, p. 183).

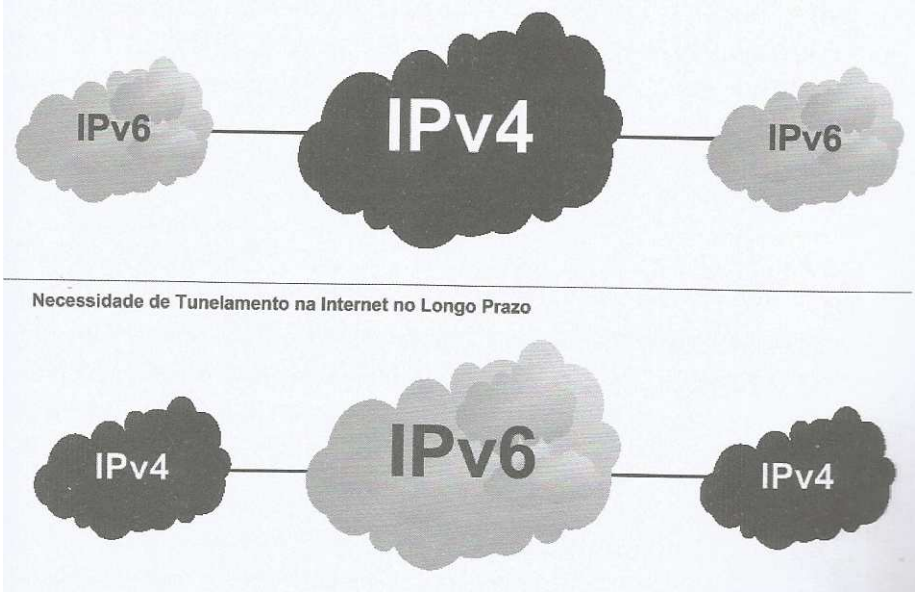

Figura 17 - Tunelamento na Internet.
Fonte: Brito, 2013, p. 183.

Por serem uma solução rápida para operacionalização das redes IPv4 e IPv6, são técnicas que pioram o desempenho da rede e não propiciam o desenvolvimento da Internet IPv6 propriamente dita, além de manter o IPv4 por mais tempo. Há várias técnicas de tunelamento publicadas em RFC, porém a cada dia são propostas novas estratégias e outras se tornam obsoletas. Dentre essas técnicas podem ser destacadas:

- Serviço de Tunnel Broker.
- Túnel Manual 6over4 (6in4).
- Túnel 6to4.
- Túnel 6rd.
- Túnel Teredo.
- Túnel ISATAP.

2.4.3 Tradução

Devido a fase de iminente esgotamento dos endereços IPv4 e pelo falta de maturidade em relação à adoção do IPv6 em larga escala, as operados de telecomunicações para tentarem contornar esse problema utilizam a técnica de tradução (NAT). De todos os métodos é considerada a pior técnica. O *Carrier Grade NAT* (CGN) ou *Large Scale NAT* (LSN) foi definido na RFC 6265, é uma técnica de tradução de grande porte, praticado nas operado de telecomunicações que não possuem mais endereços IPv4 disponíveis. Consiste em aplicar o NAT no próprio núcleo operacional da rede da operadora, antes de chegar o cliente final, ou seja, fazer “NAT do NAT”. (BRITO, 2013, p.198)

3 IMPLEMENTAÇÃO DO AMBIENTE DE SIMULAÇÃO

Neste capítulo abordará a implementação do ambiente de simulação de uma rede corporativa demonstrando a configuração do método de transição Pilha Dupla e a configuração de um serviço DHCP em ambas as versões do Protocolo IP. Serão realizados os testes do funcionamento dos protocolos IPv4 e IPv6 e demonstrar os resultados desse dois protocolos operando simultaneamente em uma rede e o impacto da implementação desse novo protocolo em relação com a rede operando somente com protocolo IP versão 4.

Por se tratar de uma pesquisa teórica experimental, inicialmente realizou-se um levantamento bibliográfico sobre o funcionamento e configuração dos protocolos IPv4 e IPv6 e o método de transição Pilha Dupla. Além da configuração dos serviços DHCP e DHCPv6.

Como citado anteriormente, nesse experimento foi utilizado o *software* GNS3 versão 0.8.7, que permite emular e testar um ambiente de rede. Esse software permite utilizar as mesmas imagens do Sistema Operacional para Interconexão de Redes (IOS) utilizadas nos roteadores físicos. Para realizar o experimento foi utilizado o roteador Cisco 7206VXR NPE-400 com 256 MB RAM, que tem suporte a IPv4 e IPv6, na figura 18 é apresentado a descrição do roteador.

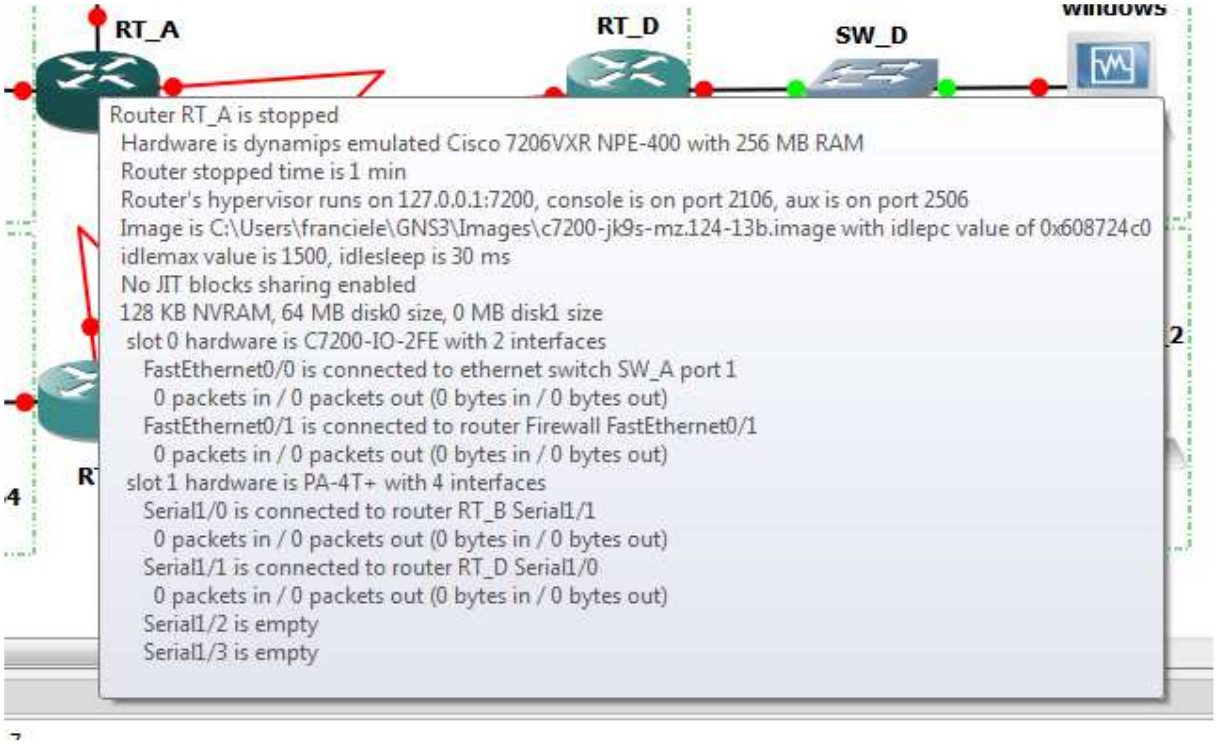

Figura 18 - Descrição do Roteador: Cisco 7206.
Fonte: Autoria Própria.

Para simular os servidores (DNS e WEB) e os hosts da rede foi utilizado o software *VirtualBox*, que permite virtualizar essas máquinas (*hosts*) da rede. Foram utilizados os sistemas operacionais *Linux*, distribuição "*Debian 7.0 - Server*" para os servidores DNS e WEB, a distribuição: "*Debian 7.7 – Desktop"* e a plataforma *Windows*, distribuição *XP* para simular os *hosts* da rede, conforme mostrada na figura 19.

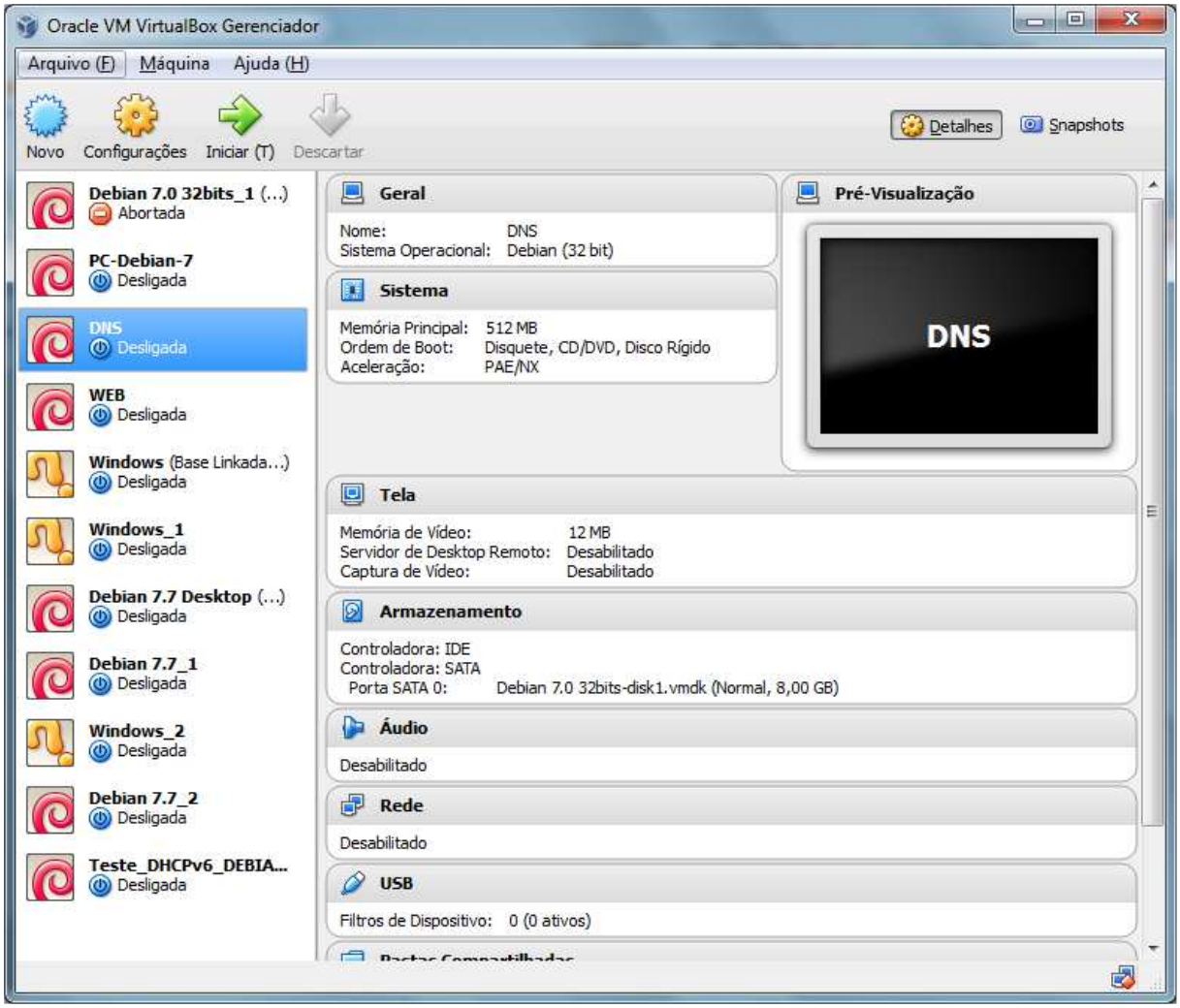

Figura 19 - Máquinas Virtuais criadas via o Software VirtualBox.
Fonte: Autoria Própria.

A próxima etapa definiu-se a topologia da rede, a topologia lógica e física, pode ser observado na figura 20. Na topologia física é utilizado cinco roteadores que são responsáveis por interconectar as redes; quatro *switches* que interligam os *hosts* locais aos respectivos roteadores; dois servidores: Servidor *Web*, que hospeda um página Web para ser realizado os testes *Web* com os dois protocolos, IPv4 e IPv6 e o servidor DNS que é responsável por traduzir o nome em endereço IP e vice-versa, servidor esse que é de suma importância no protocolo IPv6, devido a tamanho do endereço; e por fim quatro *hosts* que simbolizam usuários conectados as redes locais através do *switches*.

Nesse trabalho não será abordada a configuração dos servidores DNS e

Web descritos na topologia.

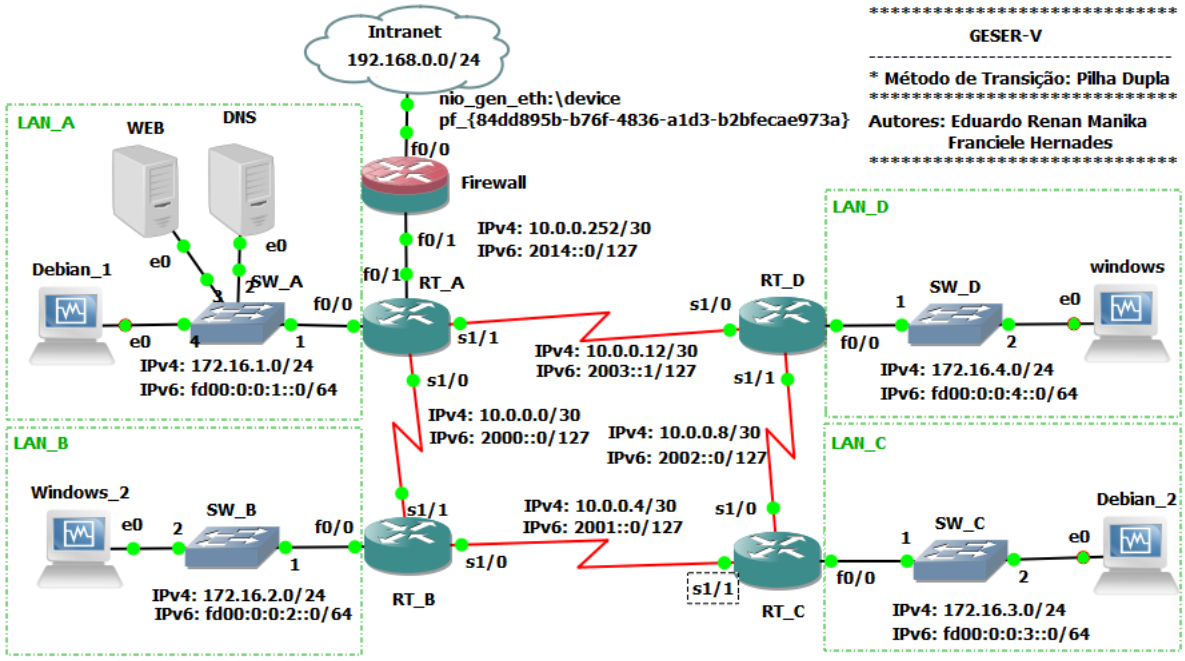

Figura 20 - Diagrama de Topologia Completo – IPv4 e IPv6.
Fonte: Autoria Própria.

Um roteador, denominado de *Firewall* faz a proteção da rede local e está diretamente conectado a rede externa, no caso denominado Intranet, é responsável por realizar os filtros dos pacotes permitidos para acessar a rede interna, através da Lista de Controle de Acesso (ACL), no qual não será abordada no trabalho. Os demais roteadores, RT_A, RT_B, RT_C, RT_D fazem a conexão e permitem que as redes locais LAN_A, LAN_B, LAN_C, LAN_D possam se comunicar entre si e com a internet passando através do *Firewall*.

Na tabela 1 é apresentada a tabela de endereços lógicos da rede.

Dispositivo	Interface	Endereço IPv4	Máscara IPv4	Gateway IPv4	Endereço IPv6	Máscara IPv6	Gateway IPv6
Firewall	f0/0	DHCP – Intranet	24	N/A	-	-	-
	f0/1	10.0.0.252	30	N/A	2014::0	127	N/A
RT_A	f0/0	172.16.1.1	24	N/A	FD00:0:0:1::0	64	N/A
	f0/1	10.0.0.253	30	N/A	2014::1	127	N/A
	s1/0	10.0.0.1	30	N/A	2000::0	127	N/A
	s1/1	10.0.0.14	30	N/A	2003::1	127	N/A

RT_B	f0/0	172.16.2.1	24	N/A	FD00:0:0:2::0	64	N/A
	s1/0	10.0.0.5	30	N/A	2001::0	127	N/A
	s1/1	10.0.0.2	30	N/A	2000::1	127	N/A
RT_C	f0/0	172.16.3.1	24	N/A	FD00:0:0:3::0	64	N/A
	s1/0	10.0.0.9	30	N/A	2002::0	127	N/A
	s1/1	10.0.0.6	30	N/A	2001::1	127	N/A
RT_D	f0/0	172.16.4.1	24	N/A	FD00:0:0:4::0	64	N/A
	s1/0	10.0.0.13	30	N/A	2003::0	127	N/A
	s1/1	10.0.0.10	30	N/A	2002::1	127	N/A
Servidor DNS	f0/0	172.16.1.2	24	172.16.1.1	FD00:0:0:1::1	64	FD00:0:0:1::0
Servidor WEB	f0/0	172.16.1.3	24	172.16.1.1	FD00:0:0:1::2	64	FD00:0:0:1::0

Tabela 1 – Tabela de Endereços Lógicos da Rede – IPv4 e IPv6.
Fonte: Autoria Própria.

Com a topologia definida, iniciou-se a configuração do ambiente para operarem com o protocolo IPv4 e posterior IPv6 e demonstrar o método de transição Pilha Dupla, além da configuração do serviço DHCP versão IPv4 e versão IPv6.

3.1 CONFIGURAÇÃO PROTOCOLO IPv4

Para configurar o ambiente de simulação com o IPv4 seguiu-se a topologia conforme demonstrado na figura 21.

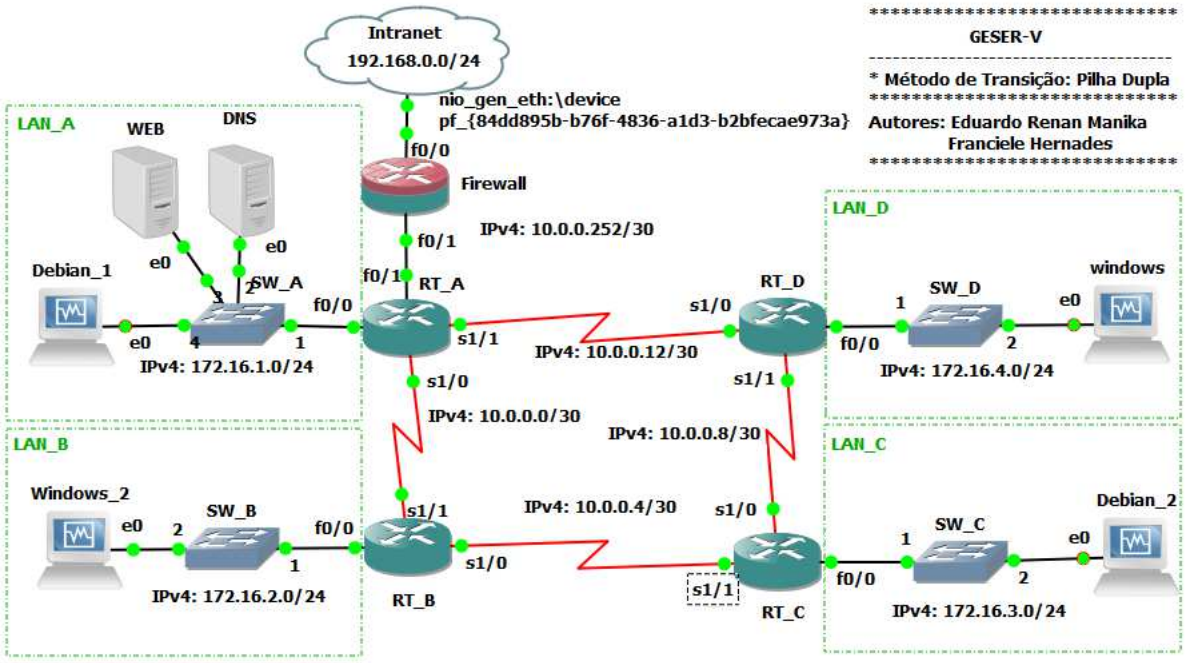

Figura 21 - Diagrama de Topologia IPv4.
Fonte: Autoria Própria.

3.1.1 Configuração das Interfaces – IPv4

Nessa simulação foram utilizadas as interfaces do tipo *FastEthernet* dos roteadores para configurar as redes locais e as interfaces do tipo *Serial* para interconectar os roteadores.

Na figura 22 pode-se observar a configuração das interfaces. Nesse exemplo de configuração foi demonstrada a configuração do roteador RT_A, no qual a interface *FastEthernet* 0/0 recebe o endereço: 172.16.1.1/24, sendo essa interface o *gateway* da rede LAN_A. A interface *Serial* 1/0 recebe o endereço 10.0.0.1/30, sendo a interface que faz a conexão com o roteador RT_B – interface *Serial* 1/1. A interface *Serial* 1/1 recebe o endereço 10.0.0.14/30, interface essa que se conecta com o roteador RT_D – interface *Serial* 1/0. E por fim, a interface *FastEthernet* 0/1 recebe o endereço 10.0.0.253/30 e faz a conexão com o *Firewall* – interface *FastEthernet* 0/1.

```
-----------------------------------------------------------------
              Configuração das Interfaces – IPv4
-----------------------------------------------------------------
RT_A>enable                        //Entra no modo exec privilegiado
RT_A#configure terminal            //Entra no modo de configuração
-----------------------------------------------------------------
Configurar a Interface f0/0:
-----------------------------------------------------------------
RT_A(config)#interface fastEthernet 0/0      //Entra na interface
RT_A(config-if)#ip address 172.16.1.1 255.255.255.0 //Seta o endereço
RT_A(config-if)#no shutdown     //Habilita a interface
RT_A(config-if)#exit           //Volta para o modo de conf. global
-----------------------------------------------------------------
Configurar a Interface f0/1:
-----------------------------------------------------------------
RT_A(config)#interface fastEthernet 0/1      //Entra na interface
RT_A(config-if)#ip address 10.0.0.253 255.255.255.252 //Seta o end.
RT_A(config-if)#no shutdown  //Habilita a interface
RT_A(config-if)#exit         // volta para o modo de conf. Global
-----------------------------------------------------------------
Configurar a Interface s1/0:
-----------------------------------------------------------------
RT_A(config)#interface serial 1/0              //Entra na interface
RT_A(config-if)#ip address 10.0.0.1 255.255.255.252 //Seta o end.
RT_A(config-if)#clock rate  64000 //(valor em bps) Configura a taxa
                                  clock, usado somente para as
                                  interfaces DCE
RT_A(config-if)#no shutdown  //Habilita a interface
RT_A(config-if)#exit         // volta para o modo de conf. Global
-----------------------------------------------------------------
Configurar a Interface s1/1:
-----------------------------------------------------------------
RT_A(config)#interface serial 1/1 //Entra na interface
RT_A(config-if)#ip address 10.0.0.14 255.255.255.252 //Seta o end.
RT_A(config-if)#no shutdown  //Habilita a interface
RT_A(config-if)#exit         // volta para o modo de conf. Global
-----------------------------------------------------------------
```

Figura 22 - Configuração Interfaces IPv4 – Roteador RT_A.
Fonte: Autoria Própria.

Esses comandos demonstrados na figura 23 são fragmentos dos comandos configurados e são utilizados na operacionalização do roteador. Esses comandos são descritos nos roteadores cisco através do comando:

```
RT_A#show running-config
```

```
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.253 255.255.255.252
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 10.0.0.1 255.255.255.252
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.0.14 255.255.255.252
 serial restart-delay 0
```

Figura 23 - Arquivo de Configuração do roteador RT_A, trecho da configuração das interfaces com o endereço IPv4.
Fonte: Autoria Própria.

Estes arquivos de configuração de todos os roteadores são demonstrados nos Apêndices A – Arquivo de Configuração do Roteador RT_A; Apêndices B – Arquivo de Configuração do Roteador RT_B; Apêndices C – Arquivo de Configuração do Roteador RT_C; Apêndices D – Arquivo de Configuração do Roteador RT_D, representando respectivamente cada roteador.

3.1.2 Configuração do OSPF – IPv4

Como citado anteriormente, foi especificado a utilização do protocolo de roteamento OSPF. Esse tipo de protocolo é um protocolo de roteamento dinâmico, *link-state* e permite divide a rede em áreas, no nosso experimento optou-se por configurar todos os roteadores na área 0. Na figura 24 é demonstrado os comandos de configuração do Roteador RT_A, através dos seguintes comando:

```
-------------------------------------------------------------------
                  Configuração do OSPF – IPv4
-------------------------------------------------------------------
RT_A>enable                        //Entra no modo exec privilegiado
RT_A#configure terminal            //Entra no modo de configuração
-------------------------------------------------------------------
Configurar o OSPF – id do processo:
-------------------------------------------------------------------
RT_A(config)#router ospf 1       //id do processo – (1 até 65535)
-------------------------------------------------------------------
Configurar o OSPF – redes diretamente conectadas:
#network <endereço_da_rede> <máscara_curinga> área <id_da_area(0 até
65535)>
-------------------------------------------------------------------
RT_A(config-router)#network 10.0.0.0 0.0.0.3 area 0
RT_A(config-router)#network 10.0.0.12 0.0.0.3 area 0
RT_A(config-router)#network 10.0.0.252 0.0.0.3 area 0
RT_A(config-router)#network 172.16.1.0 0.0.0.3 area 0
RT_A(config-router)#default-information originate //Adic. a rota
                                                  padrão ao proc. OSPF
RT_A(config-router)#exit        // Volta para o modo de conf. Global
-------------------------------------------------------------------
Configurar a Rota Padrão – que será disponibilizada aos demais
roteadores pelo processo OSPF:
-------------------------------------------------------------------
RT_A(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.254 //Configura uma rota
                                                   Padrão
```

Figura 24 - Configuração do OSPF no IPv4 – Roteador RT_A.
Fonte: Autoria Própria.

As configurações do OSPF podem ser observadas nos arquivos de configuração dos roteadores, conforme demonstrado na figura 25, que apresenta esse arquivo do roteador RT_A.

```
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
 network 10.0.0.252 0.0.0.3 area 0
 network 172.16.1.0 0.0.0.255 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 10.0.0.254
!
```

Figura 25 - Arquivo de Configuração do Roteador RT_A, trecho OSPF – IPv4.
Fonte: Autoria Própria.

3.1.3 Teste de Operação da Rede IPv4

Com todas as interfaces configuradas conforme especificado na topologia e configurado o protocolo OSPF em todos os roteadores e a rede já convergida, ou seja, os roteadores conhecem todas as redes locais e suas respectivas rotas, através do menor custo. É possível então realizar os primeiros testes de operacionalização da rede IPv4.

Pode-se verificar o funcionamento do protocolo de roteamento OSPF através das tabelas de roteamento aprendida pelos roteadores, após a rede ser convergida. Isso é apresentado nas figuras 26 e 27, nos quais apresentam a tabela de roteamento do roteador RT_A. Identificado pela legenda, as rotas que iniciam com “C” estão diretamente conectadas ao roteador RT_A; as rotas que iniciam com “O” são as rotas aprendidas pelo OSPF e a rota “S*” é a rota padrão que esta sendo informado pelo processo do OSPF.

```
RT_A#show ip ospf database

            OSPF Router with ID (172.16.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.254      10.0.0.254      1964        0x80000003 0x00AD60 1
172.16.1.1      172.16.1.1      1952        0x80000004 0x0035A0 6
172.16.2.1      172.16.2.1      17          0x80000004 0x000502 5
172.16.3.1      172.16.3.1      1972        0x80000002 0x00E40F 5
172.16.4.1      172.16.4.1      1989        0x80000003 0x006A77 5

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.0.0.253      172.16.1.1      1952        0x80000002 0x002A83

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.16.1.1      1952        0x80000002 0x00F9EF 1
```

Figura 26 - Tabelas de Roteamento do OSPF do Roteador RT_A – IPv4. Comando: show ip ospf database.
Fonte: Autoria Própria.

```
RT_A#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.254 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 4 subnets
O       172.16.4.0 [110/65] via 10.0.0.13, 00:10:51, Serial1/1
C       172.16.1.0 is directly connected, FastEthernet0/0
O       172.16.2.0 [110/65] via 10.0.0.2, 00:10:51, Serial1/0
O       172.16.3.0 [110/129] via 10.0.0.13, 00:10:51, Serial1/1
                   [110/129] via 10.0.0.2, 00:10:51, Serial1/0
     10.0.0.0/30 is subnetted, 5 subnets
O       10.0.0.8 [110/128] via 10.0.0.13, 00:10:51, Serial1/1
C       10.0.0.12 is directly connected, Serial1/1
C       10.0.0.0 is directly connected, Serial1/0
O       10.0.0.4 [110/128] via 10.0.0.2, 00:10:51, Serial1/0
C       10.0.0.252 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 10.0.0.254
```

Figura 27 - Tabelas de Roteamento do OSPF do Roteador RT_A – IPv4. Comando: show ip route.
Fonte: Autoria Própria.

Para realizar um dos testes foi utilizado o comando: *ping* que é uma ferramenta que utiliza o protocolo ICMP para realizar testes de conexão, enviando um pacote IPv4 para um *hosts* especificado, aguardando o pacote de resposta do referido *host*. Na figura 28 esse comando é executado no caso do *host* - *Debian_2* (LAN_C), IPv4: 172.16.3.2, solicitando a resposta do roteador RT_B - interface *FastEthernet* 0/0 *gateway* da LAN_B, IPv4: 172.16.2.1. Com essas respostas podemos comprovar o funcionamento da rede IPv4.

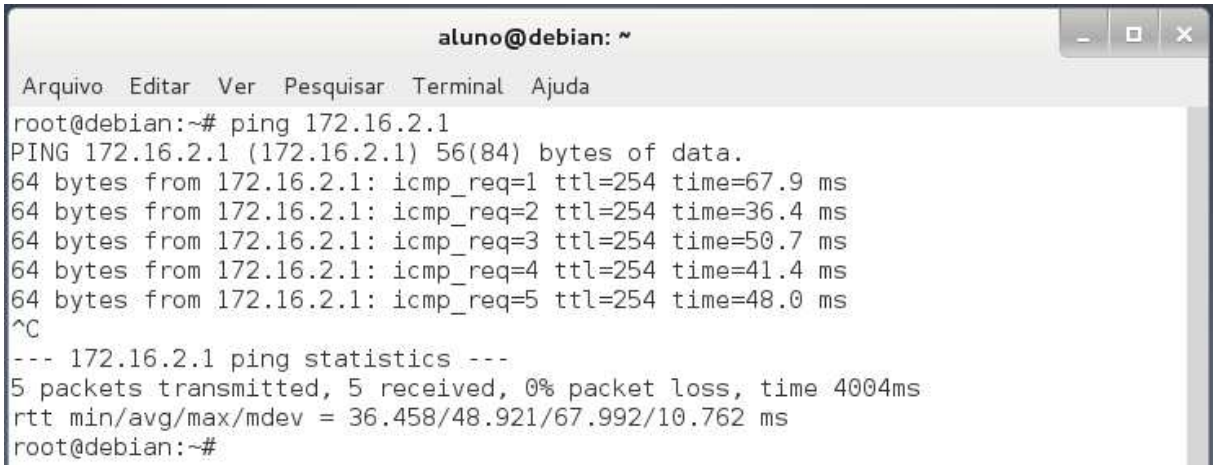

Figura 28 - Comando ping do host Debian_2 (LAN_C) para o Roteador RT_B – interface FastEthernet 0/0 – Gateway da LAN_B.
Fonte: Autoria Própria.

Outro teste que pode ser realizado é através da ferramenta: *traceroute*, que permite identificar por quais “caminhos”, roteadores, um pacote passou pela rede até atingir seu destino. Na figura 29 esse comando é executado do mesmo *host* Debian_2, utilizado no exemplo do *ping*, cliente da rede LAN_C enviando um pacote até o servidor *Web* da rede, através do endereço: *www.efmcorp.com.br*.

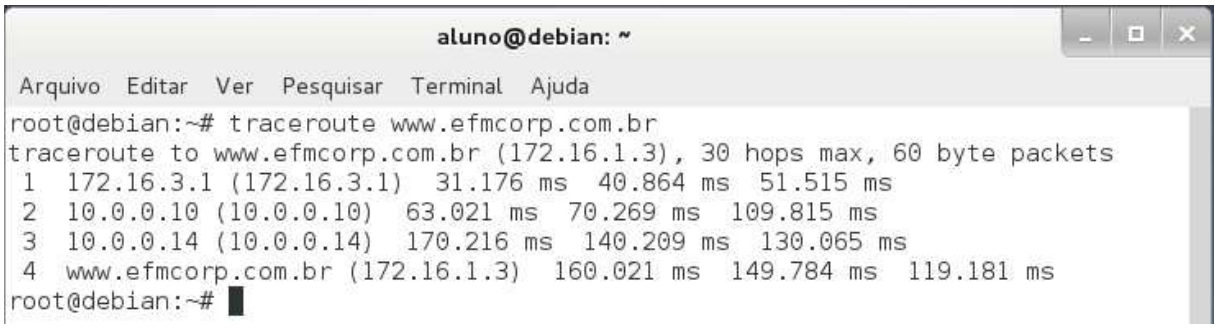

Figura 29 - Comando traceroute do host Debian_2 (LAN_C) para o Servidor Web na LAN_A.
Fonte: Autoria Própria.

3.2 CONFIGURAÇÃO PROTOCOLO IPv6

Conforme descrito anteriormente, para exemplifica o método de transição da Pilha Dupla requer que ambos os protocolos IP, versão 4 e 6, operem na rede simultaneamente. Com a rede já operando com o protocolo IPV4, conforme descrito

no tópico anterior, é necessário configurar a rede para operar com o protocolo IPv6. Essa configuração basicamente segue os mesmos passos da configuração do IPv4 e seguiu-se a topologia conforme demonstrado na figura 30.

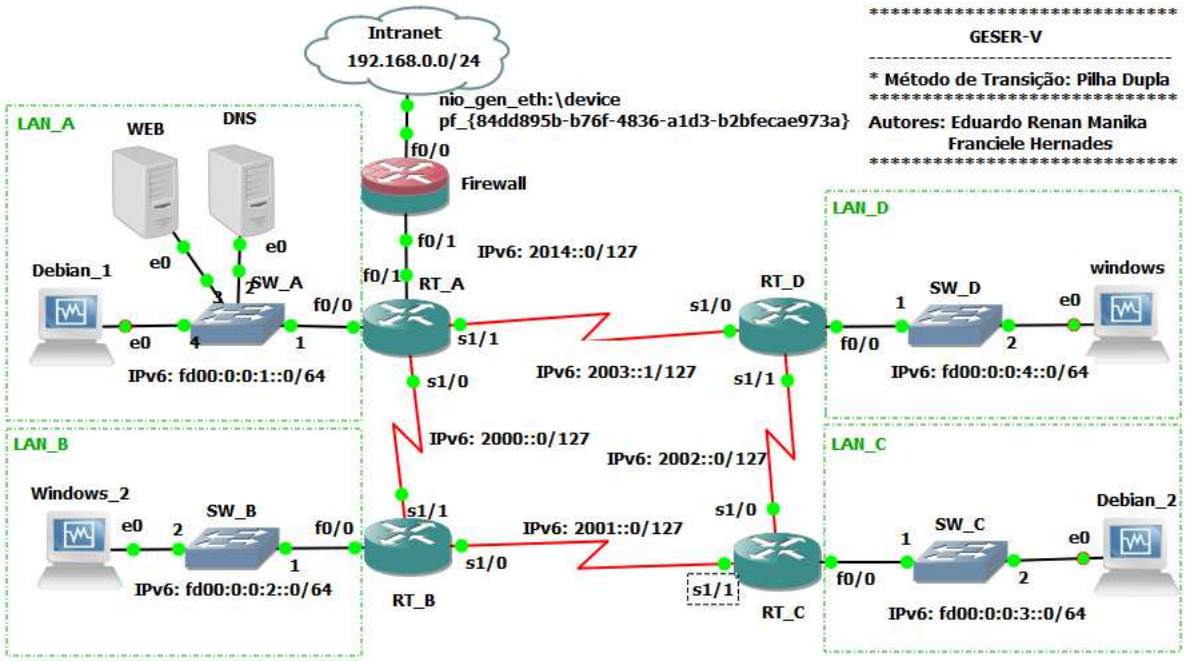

Figura 30 - Diagrama de Topologia IPv6.
Fonte: Autoria Própria.

3.2.1 Configuração das Interfaces

Conforme definido descrito na configuração do IPv4, o IPv6 utiliza as mesma interfaces, porém é adicionado o endereço IPv6. Na figura 31 é demonstrada essa configuração, no caso realizado no roteador RT_A.

```
-----------------------------------------------------------------------
                Configuração das Interfaces – IPv6
-----------------------------------------------------------------------
RT_A>enable                       //Entra no modo exec privilegiado
RT_A#configure terminal           //Entra no modo de configuração
-----------------------------------------------------------------------
Configurar a Interface f0/0:
-----------------------------------------------------------------------
RT_A(config)#interface fastEthernet 0/0       //Entra na interface
RT_A(config-if)#ipv6 address fd00:0:0:1::0/64 //Seta o endereço
RT_A(config-if)#exit              //Volta para o modo de conf. global
-----------------------------------------------------------------------
Configurar a Interface f0/1:
-----------------------------------------------------------------------
RT_A(config)#interface fastEthernet 0/1       //Entra na interface
RT_A(config-if)#ipv6 address 2014::1/127      //Seta o endereço
RT_A(config-if)#exit            // Volta para o modo de conf. global
-----------------------------------------------------------------------
Configurar a Interface s1/0:
-----------------------------------------------------------------------
RT_A(config)#interface serial 1/0              //Entra na interface
RT_A(config-if)#ipv6 address 2000::0/127       //Seta o endereço
RT_A(config-if)#exit            // Volta para o modo de conf. global
-----------------------------------------------------------------------
Configurar a Interface s1/1:
-----------------------------------------------------------------------
RT_A(config)#interface serial 1/1              //Entra na interface
RT_A(config-if)#ipv6 address 2003::1/127       //Seta o endereço
RT_A(config-if)#exit            // Volta para o modo de conf. Global
-----------------------------------------------------------------------
```

Figura 31 - Interfaces IPv6 – Roteador RT_A.
Fonte: Autoria Própria.

Na figura 32 é demonstrado o arquivos de configuração do roteador RT_A, trecho das configurações das interfaces, nessa figura apresenta os endereços IPv4 e IPv6 configurados.

```
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FD00:0:0:1::/64
!
interface FastEthernet0/1
 ip address 10.0.0.253 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2014::1/127
!
interface Serial1/0
 ip address 10.0.0.1 255.255.255.252
 ipv6 address 2000::/127
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.0.14 255.255.255.252
 ipv6 address 2003::1/127
```

Figura 32 - Arquivo de Configuração do roteador RT_A, trecho da configuração das interfaces com os endereços IPv4 e IPv6.
Fonte: Autoria Própria.

3.2.2 Configuração do Protocolo de Roteamento OSPFv3

Conforme utilizado na configuração do IPv4, o protocolo de roteamento utilizado foi o OSPF, porém com a versão 3, que suporta o roteamento do protocolo IPv6. Na figura 33 é demonstrada os comando de configuração do OSPFv3, no qual também foi utilizada a área 0 na configuração. Vale ressaltar que na configuração do OSPFv3 o *router-id* é um comando obrigatório e é composto de 32 bits, no qual o menor número é o responsável pela convergência da rede. No ambiente de simulação foi configurado o roteador RT_A para ser o responsável pela rede.

```
-----------------------------------------------------------------------
                  Configuração do OSPFv3 – IPv6
-----------------------------------------------------------------------
RT_A>enable                        //Entra no modo exec privilegiado
RT_A#configure terminal            //Entra no modo de configuração
-----------------------------------------------------------------------
Configurar o OSPFv3:
-----------------------------------------------------------------------
RT_A(config)#ipv6 unicast-routing
RT_A(config)#ipv6 router ospf 1           //id do processo OSPF
RT_A(config-rtr)#router-id 1.1.1.1        //identificador do roteador
RT_A(config-rtr)#exit             //Volta para o modo de conf. Global
-----------------------------------------------------------------------
Configurar o OSPFv3 –
Necessário entrar em cada interfaces e adicionar o comando:
#ipv6 ospf <id_processo> área <id_area>
-----------------------------------------------------------------------
RT_A(config)#interface fastEthernet 0/0  //Entra na interface
RT_A(config-if)#ipv6 ospf 1 area 0
RT_A(config-router)#exit        // Volta para o modo de conf. Global
RT_A(config)#interface fastEthernet 0/1  //Entra na interface
RT_A(config-if)#ipv6 ospf 1 area 0
RT_A(config-router)#exit        // Volta para o modo de conf. Global
RT_A(config)#interface serial 1/0  //Entra na interface
RT_A(config-if)#ipv6 ospf 1 area 0
RT_A(config-router)#exit        // Volta para o modo de conf. Global
RT_A(config)#interface serial 1/1  //Entra na interface
RT_A(config-if)#ipv6 ospf 1 area 0
RT_A(config-router)#exit        // Volta para o modo de conf. Global
-----------------------------------------------------------------------
```

Figura 33 - Configuração do OSPFv3 no IPv6 – Roteador RT_A.
Fonte: Autoria Própria.

Após a configuração das interfaces pode-se observar a configuração do OSPFv3 nas interfaces dos roteadores no arquivo de configura dos roteadores, trecho das configuração das interfaces, conforme demonstrado na figura 34.

```
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip helper-address 172.16.1.1
 duplex auto
 speed auto
 ipv6 address FD00:0:0:1::/64
 ipv6 nd managed-config-flag
 ipv6 dhcp server LAN6_A
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.0.0.253 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2014::1/127
 ipv6 ospf 1 area 0
!
interface Serial1/0
 ip address 10.0.0.1 255.255.255.252
 ipv6 address 2000::/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.0.14 255.255.255.252
 ipv6 address 2003::1/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
```

Figura 34 - Arquivo de Configuração do roteador RT_A, trecho da configuração das interfaces com o endereço IPv4 e IPv6 e OSPFv3 nas interfaces.
Fonte: Autoria Própria.

3.2.3 Teste de Operação da Rede IPv6

Com a configuração das interfaces com o endereço IPv6, configuração do protocolo de roteamento e a rede convergida, é possível realizar os primeiros testes de operação da rede IPv6.

Com a rede convergida pode-se observar as tabelas de roteamento aprendidas pelo protocolo OSPFv3, conforme observado nas figuras 35 e 36. As rotas iniciadas com “L” são rotas locais, “C” diretamente conectadas ao roteador RT_A e “O” aprendidas pelo OSPFv3.

```
RT_A#show ipv6 ospf database

            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

ADV Router      Age         Seq#       Fragment ID  Link count  Bits
1.1.1.1         1263        0x80000007 0            3           None
2.2.2.2         1249        0x80000006 0            2           None
3.3.3.3         1183        0x80000006 0            2           None
4.4.4.4         1255        0x80000006 0            2           None
9.9.9.9         1245        0x80000005 0            1           None

                Net Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Rtr count
9.9.9.9         1245        0x80000003 5          2

                Link (Type-8) Link States (Area 0)

ADV Router      Age         Seq#       Link ID    Interface
1.1.1.1         1263        0x80000004 7          Se1/1
4.4.4.4         1255        0x80000004 6          Se1/1
1.1.1.1         1263        0x80000004 6          Se1/0
2.2.2.2         1249        0x80000004 7          Se1/0
1.1.1.1         1263        0x80000004 5          Fa0/1
9.9.9.9         1246        0x80000004 5          Fa0/1
1.1.1.1         1264        0x80000003 4          Fa0/0

                Intra Area Prefix Link States (Area 0)
ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
1.1.1.1         1264        0x80000005 0          0x2001      0
2.2.2.2         1250        0x80000004 0          0x2001      0
3.3.3.3         1184        0x80000004 0          0x2001      0
4.4.4.4         1256        0x80000003 0          0x2001      0
9.9.9.9         1246        0x80000003 5120       0x2002      5
```

Figura 35 - Tabelas de Roteamento do OSPFv3 do Roteador RT_A – IPv6. Comando: show ipv6 ospf database.
Fonte: Autoria Própria.

```
RT_A#show ipv6 route
IPv6 Routing Table - 15 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2000::/127 [0/0]
     via ::, Serial1/0
L   2000::/128 [0/0]
     via ::, Serial1/0
O   2001::/127 [110/128]
     via FE80::C801:26FF:FE5C:8, Serial1/0
O   2002::/127 [110/128]
     via FE80::C803:24FF:FE68:8, Serial1/1
C   2003::/127 [0/0]
     via ::, Serial1/1
L   2003::1/128 [0/0]
     via ::, Serial1/1
C   2014::/127 [0/0]
     via ::, FastEthernet0/1
L   2014::1/128 [0/0]
     via ::, FastEthernet0/1
C   FD00:0:0:1::/64 [0/0]
     via ::, FastEthernet0/0
L   FD00:0:0:1::/128 [0/0]
     via ::, FastEthernet0/0
O   FD00:0:0:2::/64 [110/65]
     via FE80::C801:26FF:FE5C:8, Serial1/0
O   FD00:0:0:3::/64 [110/129]
     via FE80::C801:26FF:FE5C:8, Serial1/0
     via FE80::C803:24FF:FE68:8, Serial1/1
O   FD00:0:0:4::/64 [110/65]
     via FE80::C803:24FF:FE68:8, Serial1/1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura 36 - Tabelas de Roteamento do OSPFv3 do Roteador RT_A – IPv6. Comando: show ipv6 route.
Fonte: Autoria Própria.

Para o IPv6 também foram criadas as versões das ferramentas de teste de conectividade de rede como: *ping* versão IPv6 – *ping6* (roteadores CISCO) e o *traceroute6* (CISCO). Na figura 37 é utilizado a mesma operação do teste com *ping* realizado no IPv4, ou seja, entre o cliente Debian_2 da LAN_C com o roteador RT_B e pode se verificar a conectividade da rede operando com o protocolo IPv6.

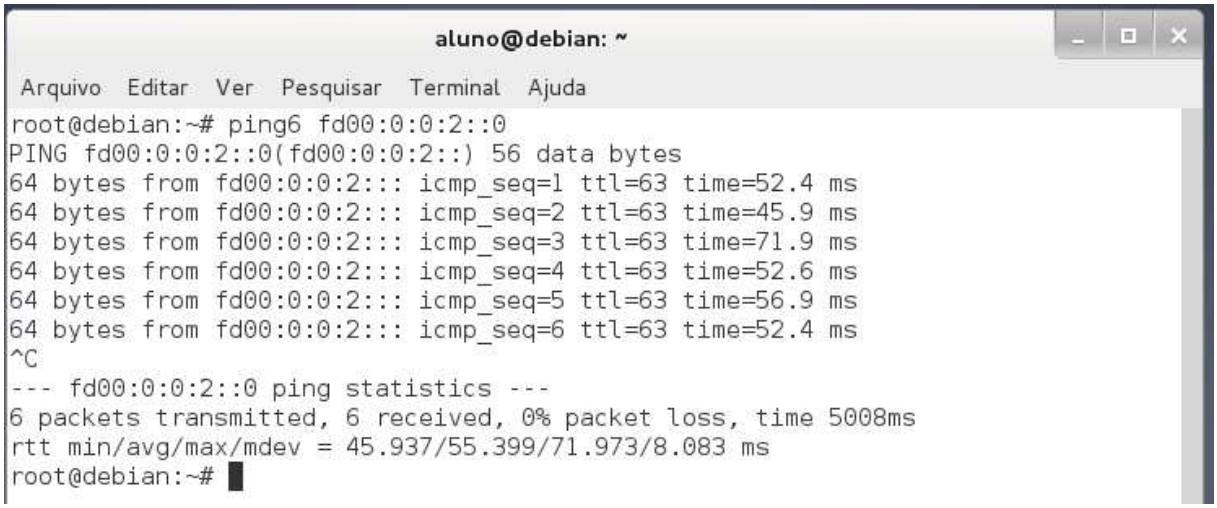

Figura 37 - Comando ping6 do host Debian_2 (LAN_C) para o Roteador RT_B – interface FastEthernet 0/0 – Gateway da LAN_B.
Fonte: Autoria Própria.

Seguindo a mesma linha de testes realizados no IPv4. Com o IPv6 também foi testado a conexão entre os *hosts* da rede LAN_A com o hosts da rede LAN_C, esse teste é demonstrado na figura 38 no qual demonstra o caminho percorrido pelo pacote IPv6 através do comando *traceroute6*.

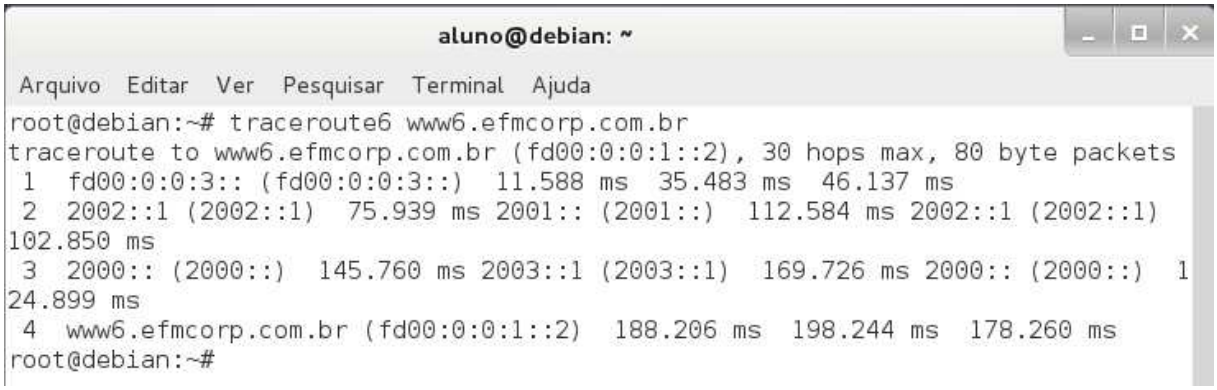

Figura 38 - Comando ping do host Debian_2 (LAN_C) para o Roteador RT_B – interface FastEthernet 0/0 – Gateway da LAN_B.
Fonte: Autoria Própria.

3.3 PILHA DUPLA

Com os dois protocolos IPv4 e IPv6 operando numa rede ao mesmo tempo é possível demonstrar o método de transição IPv4-IPv6: Pilha Dupla. Método esse que segundo especialistas é um dos melhores métodos de transição enquanto houver a

disponibilidade do endereço IPv4. Apesar de prolongar o uso do IPv4 por mais algum tempo, permite que com o passar do tempo o protocolo seja desativado com o aumento da utilização do IPv6 e com a configuração dos serviços da rede operando com IPv6.

Na figura 39 é possível observar um pacote de *ping* IPv4 capturado na rede através do software *Wireshark* que permite essa captura e a abertura do pacote para demonstra todos os detalhes dos campos do cabeçalhos e dos dados do pacote.

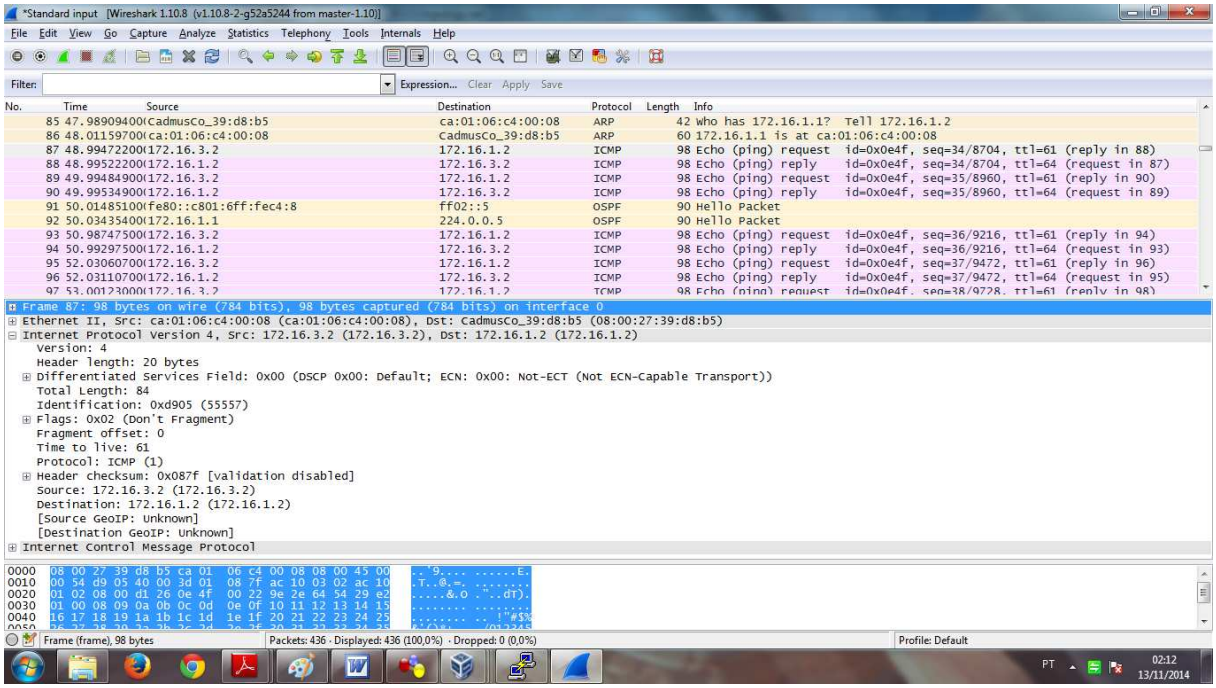

Figura 39 - Pacote ping ICMP - IPv4 capturado pelo Software Wireshark.
Fonte: Autoria Própria.

Na figura 40 é possível observar um pacote também de *ping*, porém do protocolo IPv6 trafegando na rede e capturado também pelo software *wireshark*.

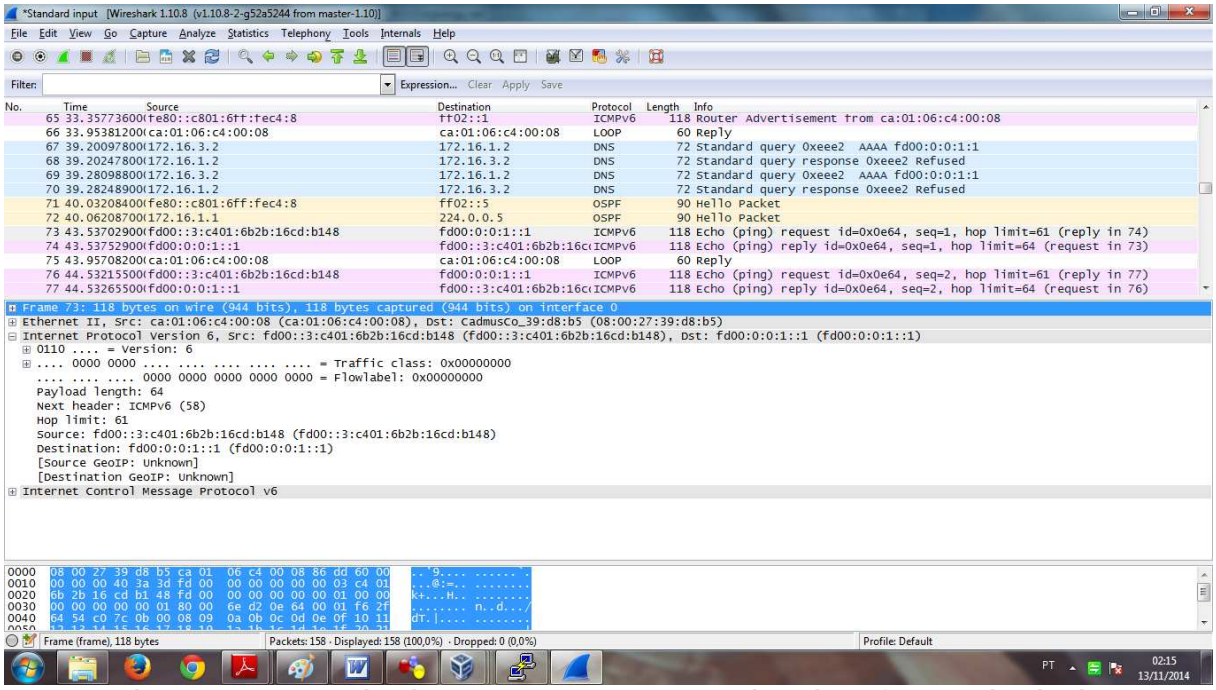

Figura 40 - Pacote de Ping ICMPv6 – IPv6 capturado pelo Software Wireshark.
Fonte: Autoria Própria.

Com isso é possível demonstrar que ambos os pacotes podem operar na mesma rede ao mesmo tempo, conforme observado na figura 41, onde tanto o pacote ICMP (IPv4) e ICMPv6 (IPv6) são observados na listada de pacotes trafegados pela rede.

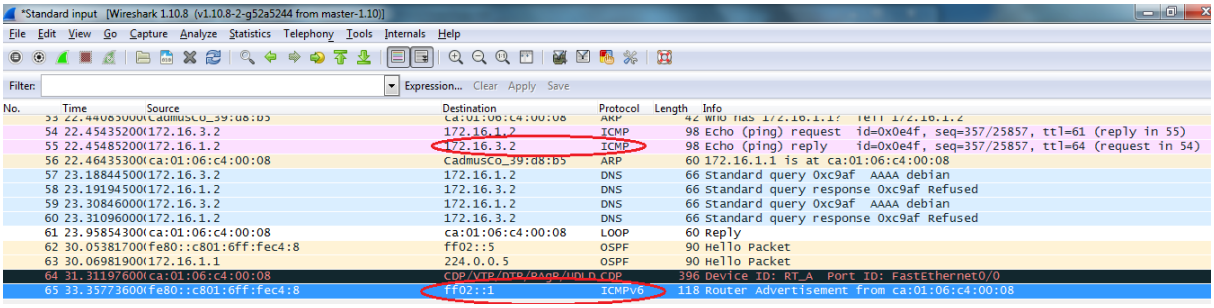

Figura 41 - Ambos os pacotes ICMP versão IPv4 e IPv6 trafegando na rede.
Fonte: Autoria Própria.

3.4 SERVIÇO DHCP e DHCPv6

Com a técnica da Pilha Dupla operando na rede, ou seja, ambos os protocolos operando na rede, pode-se realizar os testes de como a configuração dos serviços da rede serão impactados com a utilização do novo protocolo. No caso foi

escolhido o serviço de DHCP, como citado anteriormente, um dos serviços que ajudaram a prolongar os endereços IPv4, por ser um serviço que “empresta” o endereço IP ao usuário conectados na rede e quando desativados possibilita que esse mesmo endereço possa ser cedido ao um novo usuário na rede.

É um serviço que facilitou bastante a expansão da internet, pois o usuário não necessita de conhecimento de específicos para se conectar as redes, além dos administradores não necessitarem configurarem todos os hosts manualmente. Esse serviço pode ser configurado tanto em servidores *Linux* ou *Windows*, como também nos próprios roteadores.

3.4.1 Configuração do serviço DHCP

Para configurar o DHCP no IPv4 e no ambiente de simulação foi especificado a utilização do serviço no próprio roteador. Definindo o roteador RT_A como sendo o servidor de DHCP na rede IPv4, distribuindo os endereços IPv4 para as 4 redes locais: LAN_A, LAN_B, LAN_C, LAN_D. Essa configuração e demonstrada passo a passo na figura 42, no qual é necessário configurar os *pools* de serviço de cada rede, setando o endereço da rede e o servidor DNS da rede. Os endereços que não serão disponibilizados por esse serviço, no caso os gateway das redes locais os endereços: 172.16.1.1 (LAN_A), 172.16.2.1 (LAN_B), 172.16.3.1 (LAN_C), 172.16.4.1 (LAN_D) são excluídos do *range* a ser emprestados na rede.

```
-----------------------------------------------------------------
                  Configuração do DHCP – IPv4
-----------------------------------------------------------------
RT_A>enable                       //Entra no modo exec privilegiado
RT_A#configure terminal           //Entra no modo de configuração
-----------------------------------------------------------------
Configurar o DHCP – LAN_A:
-----------------------------------------------------------------
RT_A(config)#ip dhcp pool LAN_A       //Pool LAN_A
RT_A(dhcp-config)#network 172.16.1.0 255.255.255.0
RT_A(dhcp-config)#default-router 172.16.1.1
RT_A(dhcp-config)#dns-server 172.16.1.2
RT_A(dhcp-config)#domain-name efmcorp.com.br
RT_A(dhcp-config)#exit        // Volta para o modo de conf. Global
-----------------------------------------------------------------
Configurar o DHCP – LAN_B:
-----------------------------------------------------------------
RT_A(config)#ip dhcp pool LAN_B       //Pool LAN_B
RT_A(dhcp-config)#network 172.16.2.0 255.255.255.0
RT_A(dhcp-config)#default-router 172.16.2.1
RT_A(dhcp-config)#dns-server 172.16.1.2
RT_A(dhcp-config)#domain-name efmcorp.com.br
RT_A(dhcp-config)#exit        // Volta para o modo de conf. Global
-----------------------------------------------------------------
Configurar o DHCP – LAN_C:
-----------------------------------------------------------------
RT_A(config)#ip dhcp pool LAN_C       //Pool LAN_C
RT_A(dhcp-config)#network 172.16.3.0 255.255.255.0
RT_A(dhcp-config)#default-router 172.16.3.1
RT_A(dhcp-config)#dns-server 172.16.1.2
RT_A(dhcp-config)#domain-name efmcorp.com.br
RT_A(dhcp-config)#exit        // Volta para o modo de conf. Global
-----------------------------------------------------------------
Configurar o DHCP – LAN_D:
-----------------------------------------------------------------
RT_A(config)#ip dhcp pool LAN_D       //Pool LAN_D
RT_A(dhcp-config)#network 172.16.4.0 255.255.255.0
RT_A(dhcp-config)#default-router 172.16.4.1
RT_A(dhcp-config)#dns-server 172.16.1.2
RT_A(dhcp-config)#domain-name efmcorp.com.br
RT_A(dhcp-config)#exit        // Volta para o modo de conf. Global
-----------------------------------------------------------------
Excluir os endereços dos Pools:
-----------------------------------------------------------------
RT_A(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10 //range
RT_A(config)#ip dhcp excluded-address 172.16.2.1
RT_A(config)#ip dhcp excluded-address 172.16.3.1
RT_A(config)#ip dhcp excluded-address 172.16.4.1
```

Figura 42 - Configuração do DHCP versão IPv4.
Fonte: Autoria Própria.

Com esse serviço esta descentralizado em nosso cenário, ou seja, o roteador RT_A é o servidor DHCP da rede é necessário que os pacotes de DHCP possam ser encaminhados para outra rede. Essa configuração é mostrada na figura 43.

```
-----------------------------------------------------------------
                  Configuração do DHCP – IPv4
                    Setando o Servidor DHCP
-----------------------------------------------------------------
RT_B>enable                          //Entra no modo exec privilegiado
RT_B#configure terminal              //Entra no modo de configuração
-----------------------------------------------------------------
Configurar o DHCP – LAN_A:
-----------------------------------------------------------------
RT_B(config)#iinterface fastEthernet 0/0     //Interface f0/0
RT_B(dhcp-if)#ip helper-address 10.0.0.1    // IP RT_A – Servidor DHCP
RT_B(dhcp-config)#exit               // Volta para o modo de conf. Global
```

Figura 43 - Configuração do DHCP versão IPv4 – Setando o Servidor DHCP.
Fonte: Autoria Própria.

Após esta configuração do serviço DHCP ter sido realizada em todos os roteadores, pode ser demonstrados o serviço DHCP versão 4 operando na rede. Na figura 44 é demonstrado a interface do cliente "*windows*" da LAN_D configurada via DHCP.

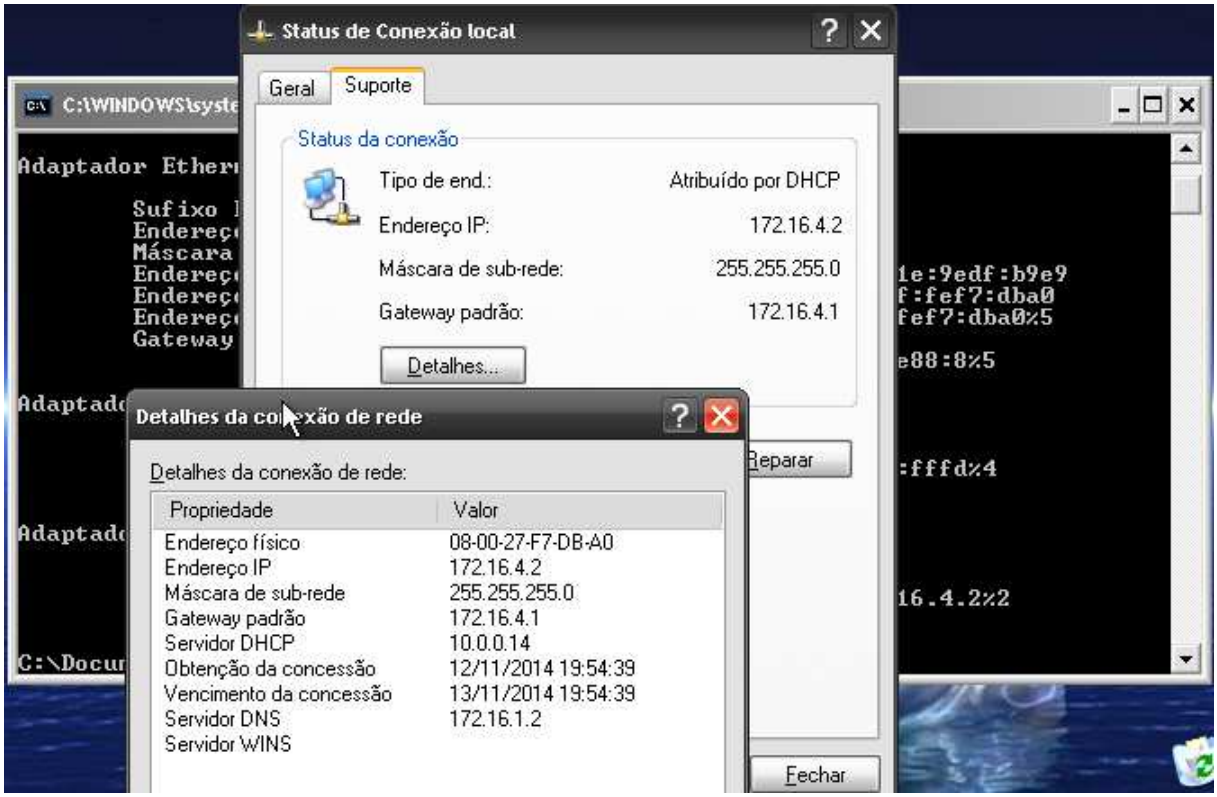

Figura 44 - Exemplo da Configuração da Interface do cliente Windows da LAN_D.
Fonte: Autoria Própria.

Na figura 45 é apresentado o comando: *show ip dhcp pool*, que permite realizar a verificação dos *pools* DHCP configurados no servidor DHCP, no caso roteador RT_A, apresentando todos os detalhes do *pool*.

```
RT_A#show ip dhcp pool

Pool LAN_A :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 172.16.1.1           172.16.1.1       - 172.16.1.254      0

Pool LAN_B :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 172.16.2.1           172.16.2.1       - 172.16.2.254      1

Pool LAN_C :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 172.16.3.1           172.16.3.1       - 172.16.3.254      1

Pool LAN_D :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 172.16.4.1           172.16.4.1       - 172.16.4.254      1
```

Figura 45 - Comando de verificação dos pools DHCP configurados no roteador RT_A.
Fonte: Autoria Própria.

Com o comando: *show ip dhcp binding* é possível verificar quais são os clientes que estão utilizando o serviço de DHCP do roteador RT_A, conforme apresentado na figura 46.

```
RT_A#show ip dhcp ?
  binding   DHCP address bindings
  conflict  DHCP address conflicts
  database  DHCP database agents
  import    Show Imported Parameters
  pool      DHCP pools information
  relay     Miscellaneous DHCP relay information
  server    Miscellaneous DHCP server information

RT_A#show ip dhcp bin
RT_A#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
172.16.2.2          0108.0027.4652.7d       Nov 15 2014 01:28 AM    Automatic
172.16.3.2          0800.2755.4634          Nov 15 2014 01:29 AM    Automatic
172.16.4.2          0108.0027.f7db.a0       Nov 15 2014 01:30 AM    Automatic
```

Figura 46 - Comando de verificação dos clientes utilizando o serviço de DHCP do roteador.
Fonte: Autoria Própria.

O comando: *show ip dhcp Server statistics* é possível verificar as estatísticas dos pacotes de DHCP trafegados na rede e solicitados ao roteador RT_A, conforme apresentado na figura 47.

```
RT_A#show ip dhcp server statistics
Memory usage         27753
Address pools        4
Database agents      0
Automatic bindings   3
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         3
DHCPREQUEST          6
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           3

Message              Sent
BOOTREPLY            0
DHCPOFFER            3
DHCPACK              7
DHCPNAK              0
```

Figura 47 - Estatísticas dos pacotes DHCP solicitados ao roteador RT_A.
Fonte: Autoria Própria.

3.4.2 Configuração do serviço DHCPv6

Segundo Brito (2014) nativamente o IPv6 têm o suporte ao processo autoconfiguração stateless, no qual a própria maquina é capaz de formar seu endereço IPv6. Devido a isso, um servidor DHCP poderia ser algo dispensável. Porém conforme descrito anteriormente, o serviço de DHCPv6, serviço DHCP com suporte ao protocolo IPv6, serve para identificar os demais serviços da rede, como o serviço o DNS, que no novo protocolo tem um importância muito grande devido ao tamanho do endereço.

Na configuração do DHCPv6 no ambiente foi utilizado a versão *stateless*, com o recurso de delegação de prefixos, até porque o roteador utilizado, Cisco 7206, não apresenta suporte ao DHCPv6 *stateful*. Outro detalhe foi a configuração desse serviço em cada roteador das LANs.

Os passos de configuração utilizados o DHCPv6 é descrito na figura 48.

```
-----------------------------------------------------------------
                  Configuração do DHCP – IPv6
                        Roteador RT_C
-----------------------------------------------------------------
RT_C>enable                      //Entra no modo exec privilegiado
RT_C#configure terminal          //Entra no modo de configuração
-----------------------------------------------------------------
Configurar o DHCPv6 - Pool
-----------------------------------------------------------------
RT_C(config)#ipv6 dhcp pool LAN6_C               //Pool LAN6_C
RT_C(config-dhcp)#prefix-delegation pool LAN6_C  //Delegaçãoo Prefixos
RT_C(config-dhcp)#dns-server fd00:0:0:1::1       //Servidor DNS
RT_C(config-dhcp)#exit           // Volta para o modo de conf. Global
RT_C(config)#ipv6 local pool LAN6_C fd00:0:0:3::10/64 64 //Escopo
-----------------------------------------------------------------
Configurar o DHCPv6 - Interface
-----------------------------------------------------------------
RT_C(config)#interface fastEthernet 0/0      //Interface f0/0
RT_C(config-if)#ipv6 dhcp server LAN6_C      //Seta o pool do DHCP
RT_C(config-if)#ipv6 nd managed-config-flag  //Inf. Aprendidas DHCPv6
RT_C(config-if)#exit             // Volta para o modo de conf. Global
```

Figura 48 - Configuração do DHCPv6 no roteador RT_C.
Fonte: Autoria Própria.

Inicialmente é configurado o *pool* do DHCPv6 com a opção de delegação do

prefixo e setando o servidor o DNS. Posteriormente seta o escopo do serviço DHCP e por fim, seta a interface F*astEthernet* 0/0 para fornecer o serviço configurado e o parâmetro: *nd managed-config-flag*, que é um sinalizador por meio de anúncios RA do roteador aos clientes, que todas as informações de endereçamento da rede devem ser aprendidas via DHCPv6.

No cliente deve estar marcado a opção de configuração do endereço IPv6 via DHCP e um exemplo do endereço recebido é apresentado na figura 49, no caso do cliente *Debian* da rede LAN_C, através do comando "*ifconfig*" realizado via linha de comando.

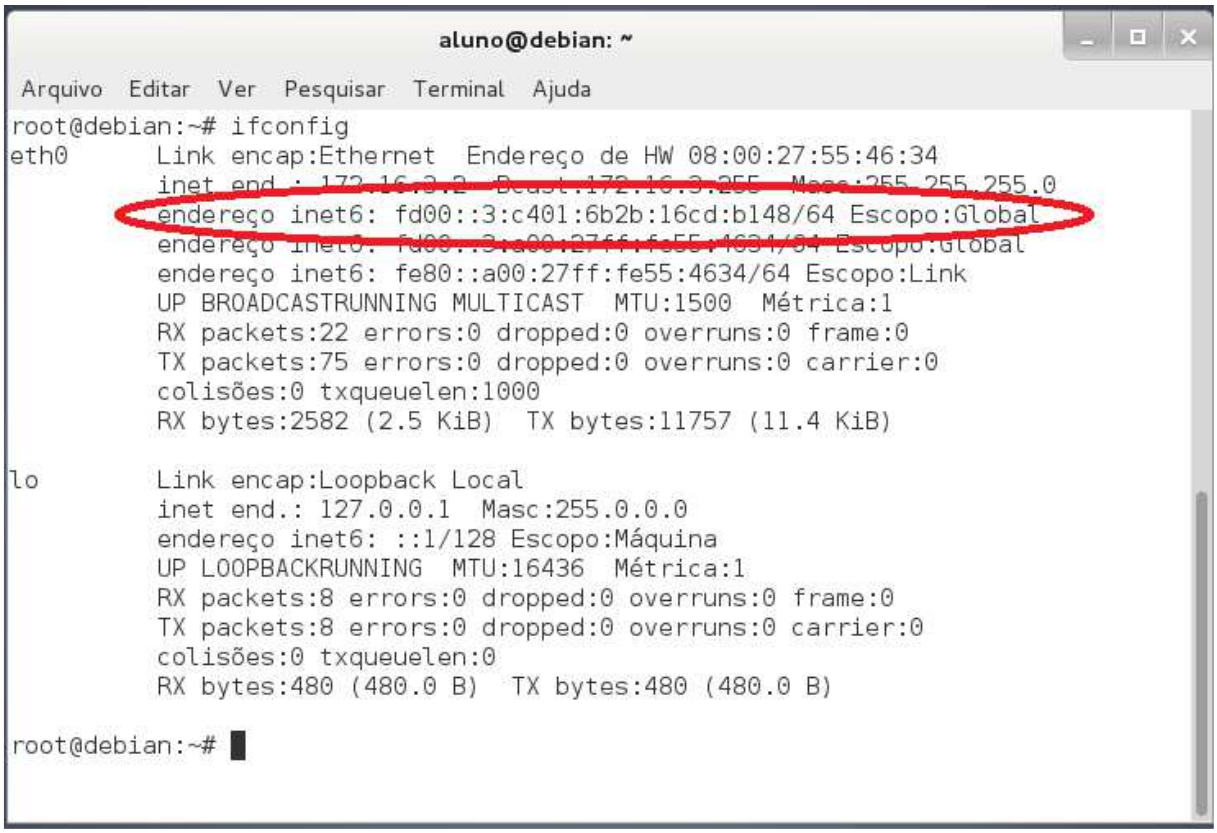

Figura 49 - Cliente Debian da LAN_C – Endereço IPv6 recebido via DHCPv6.
Fonte: Autoria Própria.

Na figura 50 mostra a configuração do endereço no mesmo cliente Debian da rede LAN_C, porém na interface gráfica.

Figura 50 - Cliente Debian da LAN_C – Endereço IPv6 recebido via DHCPv6, interface gráfica. Fonte: Autoria Própria.

4 CONCLUSÃO

Com a descrição dos passos de configuração do método de transição: Pilha Dupla e a configuração do serviço DHCP para ambos os protocolo, pode se dizer que os resultado obtidos foram positivos e que ambiente de simulação permitiu verificar o funcionamento e configuração de alguns pontos em ambos os protocolos. A rede operou tanto com protocolo IPv4 quanto com o protocolo IPv6 simultaneamente sem um interferir na operação do outro, o serviço de DHCP também funcionou sem problemas de operação. E a configuração do novo protocolo apresenta detalhes específicos na sua configuração, o que mudam o modo de configuração de alguns serviços realizada pelos administradores e requer o estudo e aprendizado dessas novas configurações.

Vale ressaltar que o protocolo IPv6 é diferente de IPv4 e ambos não são diretamente compatíveis, conforme afirma Brito (2013), o que requer a adoção de mecanismos de transição da rede IPv4-IPv6 complexos. O mecanismo apresentado nesse projeto a Pilha Dupla é considerado uma das melhores opções atualmente, enquanto estiver disponível endereços IPv4, porém não é o único e muitas vezes não é possível ser configurado em toda a rede local, pois requer que os equipamentos tenham suporte ao protocolo IPv6. A maioria dos equipamentos dos clientes tem suporte ao protocolo IPv6, porém muitas versões de ativos de rede, como roteadores, não apresentam esse suporte e requer outros métodos de transição como Tunelamento e Tradução, entre outros. Lembrando que novas técnicas surgirão e outras se tornarão obsoletas por se tratar de um período de transição.

O protocolo IPv6 trará várias vantagens, não somente a quantidade enorme

de endereços; conforme apresenta Brito (2013, p.37) apresentará outros pontos como: o cabeçalho simplificado e de tamanho fixo; processamento simplificado; dispensa do NAT, preservando modelo fim-a-fim; segurança embutida com o IPSec e suporte a mobilidade com o MIPv6. Filippetti (2014, p.129) complementa a essa lista com: “suporte a autoconfiguração; suporte à seleção de rota; suporte nativo a tráfego com demanda por Qualidade de Serviço (QoS) e suporte a extensões configuráveis (Ad hoc) “. Por ser um protocolo mais recente teve a possibilidade de corrigir várias vulnerabilidades e implementar várias necessidades, conforme citada, não especificada no surgimento do IPv4. Porém com o crescimento da utilização do IPv6, fatalmente novas modalidade de ataques surgirão e novas vulnerabilidades que sequer existiam no IPv4.

A questão de segurança do IPv6, por possuir suporte ao IPsec, pode surgir a impressão de que o IPv6 é um protocolo mais seguro, mas a segurança nativa significa que a solução de segurança IPsec faz parte da suíte de protocolos de arquitetura TCP/IPv6, isso não significa que a solução de segurança seja autoconfigurada. As principais soluções de segurança, com autenticação e criptografia requerem configurações manuais (BRITO, 2013, p.136). Por isso os administradores devem o quanto antes se aprofundar nos conhecimentos do novo protocolo IPv6 e se possível criar cenários e ambientes, como aqui descritos nesse trabalho, para testar as configurações na prática e as alterações nos serviços já gerenciados no IPv4. Além de poder realizar testes de segurança da rede, para não serem surpreendidos com a implementação do IPv6 de um dia para o outro sem a confiança e maturidade dos conhecimentos necessários do novo protocolo.

Outro impacto desse novo protocolo para os administradores de rede é o fato que inicialmente haverá a necessidade de configurar o protocolo IPv6 na rede toda,

em roteadores, servidores e serviços. O que muita vezes é trabalhoso, dependendo do tamanho da rede e a quantidade de pessoas na equipe, além de aumentar a quantidade de serviços que devem ser gerenciados na rede, pois terão que manter as Redes IPv4 e IPv6, durante esse período de transição, sendo protocolos distintos em operação, o que duplica os esforços de gestão e operacionalização

REFERÊNCIAS

BRITO, Samuel H. B. **IPv6.** O novo protocolo da internet. 1ª. ed, São Paulo: Novatec, 2013.

BRITO, Samuel H. B. **Servidores DHCPv6 em redes IPv6.** Disponível em < http://labcisco.blogspot.com.br/search?q=DHCPv6>. Acesso em 02/nov/2014 15:05.

CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIA DE REDES E OPERAÇÕES (CEPTRO.BR). **Cabeçalho**. Equipe IPv6.br. Disponível em <http://ipv6.br/entenda/cabecalho//>. Acesso em 08/jun/2014 18:40.

_____. **Introdução**. Equipe IPv6.br. Disponível em <http://ipv6.br/entenda/introducao/>. Acesso em 07/jun/2014 17:50.

COMER, Douglas E. **Interligação de redes com TCP/IP**. Vol. 1 princípios, protocolo e arquitetura. 5ª. ed. Rio de Janeiro: Campus, 2006.

COMER, Douglas E. **Redes de computadores e internet.** Abrange transmissão de dados, ligações inter-redes, web e aplicações. 4ª. ed. São Paulo: Artmed, 2007.

FILIPPETTI, Marco A. **CCNA 5.0.** Guia completo de estudo. Florianópolis: Visual Books, 2014.

FLORENTINO, Adilson. **Endereçamento IPv6**. 2011. Disponível em < http://ipv6.br/enderecamento-ipv6/>. Acesso em 02/Nov/2014 14:30.

GNS3. **What is GNS3**. Disponível em <http://www.gns3.net/>. Acesso em 13/jun/2014.

KUROSE, James F. **Redes de computadores e a internet.** 5ª. ed. São Paulo: Pearson, 2010.

APÊNDICE A – ARQUIVO DE CONFIGURAÇÃO DO ROTEADOR RT_A

```
RT_A#show running-config
Building configuration...

Current configuration : 2531 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RT_A
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp excluded-address 172.16.1.1 172.16.1.10
ip dhcp excluded-address 172.16.2.1
ip dhcp excluded-address 172.16.3.1
ip dhcp excluded-address 172.16.4.1
!
ip dhcp pool LAN_A
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.1
   dns-server 172.16.1.2 8.8.8.8
!
ip dhcp pool LAN_B
   network 172.16.2.0 255.255.255.0
   default-router 172.16.2.1
   dns-server 172.16.1.2 8.8.8.8
!
ip dhcp pool LAN_C
```

```
   network 172.16.3.0 255.255.255.0
   default-router 172.16.3.1
   dns-server 172.16.1.2 8.8.8.8
!
ip dhcp pool LAN_D
   network 172.16.4.0 255.255.255.0
   default-router 172.16.4.1
   dns-server 172.16.1.2 8.8.8.8
!
!
ipv6 unicast-routing
ipv6 dhcp pool LAN6_A
 prefix-delegation pool LAN6_A
 dns-server FD00:0:0:1::1
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip helper-address 172.16.1.1
 duplex auto
 speed auto
 ipv6 address FD00:0:0:1::/64
```

```
 ipv6 nd managed-config-flag
 ipv6 dhcp server LAN6_A
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.0.0.253 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2014::1/127
 ipv6 ospf 1 area 0
!
interface Serial1/0
 ip address 10.0.0.1 255.255.255.252
 ipv6 address 2000::/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.0.14 255.255.255.252
 ipv6 address 2003::1/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
 network 10.0.0.252 0.0.0.3 area 0
 network 172.16.1.0 0.0.0.255 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 10.0.0.254
```

```
!
no ip http server
no ip http secure-server
!
!
ipv6 local pool LAN6_A FD00:0:0:1::/64 64
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
End
```

APÊNDICE B – ARQUIVO DE CONFIGURAÇÃO DO ROTEADOR RT_B

```
RT_B#show running-config
Building configuration...

Current configuration : 1667 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RT_B
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
ipv6 unicast-routing
ipv6 dhcp pool LAN6_B
prefix-delegation pool LAN6_B
dns-server FD00:0:0:1::1
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
ip address 172.16.2.1 255.255.255.0
ip helper-address 10.0.0.1
duplex auto
speed auto
ipv6 address FD00:0:0:2::/64
ipv6 dhcp server LAN6_B
ipv6 ospf 1 area 0
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
ip address 10.0.0.5 255.255.255.252
ipv6 address 2001::/127
ipv6 ospf 1 area 0
serial restart-delay 0
clock rate 64000
!
interface Serial1/1
ip address 10.0.0.2 255.255.255.252
ipv6 address 2000::1/127
ipv6 ospf 1 area 0
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
```

```
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.3 area 0
network 10.0.0.4 0.0.0.3 area 0
network 172.16.2.0 0.0.0.255 area 0
!
!
no ip http server
no ip http secure-server
!
!
ipv6 local pool LAN6_B FD00:0:0:2::/64 64
ipv6 router ospf 1
router-id 2.2.2.2
log-adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
```

```
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
End
```

APÊNDICE C – ARQUIVO DE CONFIGURAÇÃO DO ROTEADOR RT_C

```
RT_C#show running-config
Building configuration...

Current configuration : 1696 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RT_C
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
ipv6 unicast-routing
ipv6 dhcp pool LAN6_C
 prefix-delegation pool LAN6_C
 dns-server FD00:0:0:1::1
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.3.1 255.255.255.0
 ip helper-address 10.0.0.1
 duplex auto
 speed auto
 ipv6 address FD00:0:0:3::/64
 ipv6 nd managed-config-flag
 ipv6 dhcp server LAN6_C
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 10.0.0.9 255.255.255.252
 ipv6 address 2002::/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.0.6 255.255.255.252
 ipv6 address 2001::1/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
```

```
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 172.16.3.0 0.0.0.255 area 0
!
!
no ip http server
no ip http secure-server
!
!
ipv6 local pool LAN6_C FD00:0:0:3::/64 64
ipv6 router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
End
```

APÊNDICE D – ARQUIVO DE CONFIGURAÇÃO DO ROTEADOR RT_D

```
RT_D#show running-config
Building configuration...

Current configuration : 1670 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RT_D
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
ipv6 unicast-routing
ipv6 dhcp pool LAN6_D
 prefix-delegation pool LAN6_D
 dns-server FD00:0:0:1::1
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.4.1 255.255.255.0
 ip helper-address 10.0.0.1
 duplex auto
 speed auto
 ipv6 address FD00:0:0:4::/64
 ipv6 dhcp server LAN6_D
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 10.0.0.13 255.255.255.252
 ipv6 address 2003::/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.0.10 255.255.255.252
 ipv6 address 2002::1/127
 ipv6 ospf 1 area 0
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
```

```
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
 network 172.16.4.0 0.0.0.255 area 0
!
!
no ip http server
no ip http secure-server
!
!
ipv6 local pool LAN6_D FD00:0:0:4::/64 64
ipv6 router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
```

```
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```