UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DEPARTAMENTO ACADÊMICO DE INFORMÁTICA

TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

LUCIANO SANTANA DOS SANTOS

IMPLEMENTAÇÃO DE IPV6 EM UM PROVEDOR DE INTERNET

TRABALHO DE CONCLUSÃO DE CURSO

PONTA GROSSA

2016

LUCIANO SANTANA DOS SANTOS

IMPLEMENTAÇÃO DE IPV6 EM UM PROVEDOR DE INTERNET

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Augusto Foronda

PONTA GROSSA

2016

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Ponta Grossa
Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Informática
Tecnologia em Análise e Desenvolvimento de Sistemas

TERMO DE APROVAÇÃO

IMPLEMENTAÇÃO DE IPV6 EM UM PROVEDOR DE INTERNET

por

LUCIANO SANTANA DOS SANTOS

Este Trabalho de Conclusão de Curso (TCC) foi apresentado em 22 de Novembro de 2016 como requisito parcial para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Augusto Foronda
Prof.(a) Orientador(a)

_____
Prof. MSc. Rafael dos Passos Canteri
Membro titular

_____
Prof. Dr. Richard Duarte Ribeiro
Membro titular

_____
Profª. Mônica Hoeldtke Pietruchinski
Responsável pelo Trabalho de Conclusão de Curso

_____
Profª. Dra. Mauren Louise Sguario
Coordenadora do curso

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à toda minha família
que sempre acreditou nos meus sonhos,
me incentivaram e tiveram minha
ausência por longo período.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, que me permitiu aproveitar esta oportunidade.

Aos meus pais, que me deram a vida.

À minha esposa, que sofreu com minha ausência.

Aos meus filhos que possam ver em mim um exemplo.

Aos meus professores, que compartilharam com tanta generosidade seu conhecimento.

E ao meu orientador Prof. Dr. Augusto Foronda, que com tenacidade e paciência soube me levar a um novo patamar de conhecimento.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

“Comutar ou não comutar? Eis a questão.
Será mais sábio sofrer, na rede, o
armazenar e o reencaminhar, na
indeterminação dos processos? Ou fazer
frente a esse mar de dados com linhas,
que, dedicadas, a eles irão servir? ”

CERF, Vinton, RFC 1121.

RESUMO

SANTOS, Luciano Santana dos. **Implementação de IPv6 em um Provedor de Internet**. 2016. 84 f. Trabalho de Conclusão de Curso Tecnologia em Análise e Desenvolvimento de Sistemas - Universidade Tecnológica Federal do Paraná. Ponta Grossa, 2016.

Este trabalho tem como aspiração, se tornar um modelo de referência em Língua Portuguesa para a implantação de redes de computadores utilizando o protocolo IPv6. A necessidade deste tipo de trabalho ocorre devido à parca documentação acessível na Língua Portuguesa. Atualmente o mercado de provimento de conexão de Internet é muito profícuo, com 2.138 provedores, sendo 90% de pequeno porte, com até 49 funcionários, e atendendo municípios abaixo de 100.000 habitantes (CGI.BR 2016). Discorre-se um referencial teórico do novo protocolo, assim como suas raízes históricas e a necessidade da troca do protocolo IPv4 apenas 11 anos após sua implementação na Internet. Se descreve um modelo de implementação orientado a uma configuração básica, com funcionamento em pilha-dupla executando, de forma conjunta, os protocolos IPv4 e IPv6 de forma conjunta. Esse modelo começa com a elaboração de uma programação baseada num plano de endereçamento *leftmost*, dos bits mais a esquerda para a direita, e posteriormente configuração do roteamento dinâmico, serviços necessários e, por fim, a conexão do cliente. Se conclui que o objetivo foi alcançado e a rede obteve o funcionamento esperado, com conectividade IPv4 e IPv6.

Palavras-chave: IPv6. Redes de Computadores. Internet.

ABSTRACT

SANTOS, Luciano Santana dos Santos. **IPv6 implementation in a Internet Service Provider**. 2016. 84 f. Trabalho de Conclusão de Curso Tecnologia em Análise e Desenvolvimento de Sistemas – Federal Technology University - Paraná. Ponta Grossa, 2016.

This paper has the intends to become a reference model, in Portuguese Language, for the deployment of computer networks using IPv6 protocol. The need for this kind of paper occurs due to the slender documentation available in Portuguese Language. Nowadays the Internet Service Provider market is very abundant, with 2.138 providers, and 90% of that are the small-sized companies, with up 49 workers, and serving cities under 100.000 dwellers (CGI.BR 2016). In this paper, we present a theoretical reference of the new protocol, has its historic roots and the necessity of the change the IPv4 protocol only eleven years after its deployment as the Internet prime protocol. There also presented an implementation model, oriented to a basic configuration, with the dual stack, joint operational with the IPv4 and IPv6 protocol. This model begins with a leftmost oriented address plan, from the leftmost bits to the right, and later the dynamic routing configuration needed services, and finally, the client's connection. It concludes that the objective was reached, and the network obtained the expected behavior, with IPv4 and IPv6 connectivity.

Keywords: IPv6. Computer Network. Internet.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE SIGLAS

BGP	*Border Gateway Protocol*
CETIC.BR	*Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação*
CGI.br	*Comitê Gestor da Internet no Brasil*
CIDR	*Classless Inter-Domain Routing*
CPE	*Customer Premises Equipment*
DHCP	*Dynamic Host Configuration Protocol*
DHCPv6	*Dynamic Host Configuration Protocol for IPv6*
DNS	*Domain Name Service*
DNSv6	*Domain Name Service for IPv6*
DSL	*Digital Subscriber Line*
HTML	*HyperText Markup Language*
HTTP	*HyperText Transfer Protocol*
IA	*Identity Association*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Message Protocol*
IGP	*Interior Gateway Protocol*
IP	*Internet Protocol*
IPng	*Internet Protocol next generation*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISC	*Internet Systems Consortium*
NCP	*Network Control Protocol*
OSI	*Open Systems Interconnection*
OSPF	*Open Short Path First*
PPPoE	*Point-to-Point Protocol over Ethernet*
PPPoE/v6	*Point-to-Point Protocol over Ethernet for IPv6*
QoS	*Quality of Service*
RA	*Router Advertisements*
RS	*Router Solicitation*
SPF	*Shortest Path First*
TCP	*Transmission Control Protocol*

LISTA DE ACRÔNIMOS

AFRINIC	*African Network Information Center*
APNIC	*Asia-Pacific Network Information Centre*
ARIN	*American Registry for Internet Numbers*
ARP	*Address Resolution Protocol*
ARPANET	*Advanced Research Projects Agency Network*
AS	*Autonomous System* (Sistema Autônomo)
BRAS	*Broadband Remote Access Server*
CEPTRO	Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações
CERN	*Conseil Européen pour la Recherche Nucléaire*
CGNAT	*Carrier-Grade Network Address Translator*
DAD	*Duplication Address Detection*
DIG	*Domain Information Groper*
DOCSIS	*Data Over Cable Service Interface Specification*
DUID	*DHCP Unique Identifier*
GEPON	*Gigabit Ethernet Passive Optical Network*
GNU	*GNU is Not Unix*
GPON	*Gigabit Passive Optical Network*
IANA	*Internet Assigned Numbers Authority*
ISO	*International Organization for Standardization*
LACNIC	*Latin America and Caribbean Network Information Centre*
NAT	*Network Address Translator*
NAT64	*Network Address Translator 6to4*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
OTAN	Organização do Tratado do Atlântico Norte
RADIUS	*Remote Authentication Dial In User Service*
RARP	*Reverse Address Resolution Protocol*
RIP	*Routing Information Protocol*
RIPE NCC	*Réseaux IP Européens Network Coordination Centre*
RIR	*Regional Internet Registry*
ROAD	*Routing and Addressing*
SLAAC	*Stateless Address Autoconfiguration*
TIC	*Tecnologias de Informação e Comunicação*

SUMÁRIO

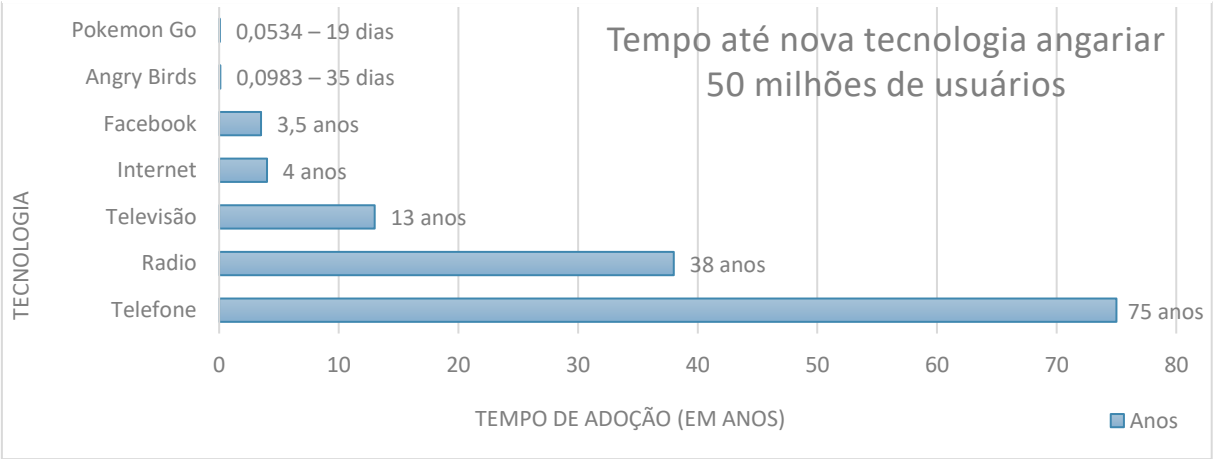
1 INTRODUÇÃO

Atualmente vive-se uma era de ouro no campo das redes de computadores. Uma revolução iniciada em 1983 com a adoção do *Internet Protocol* (*IPv4* ou *IP*) como base da rede ARPANET que viria a se torna a Internet (POSTEL 1981). Consolidada com grandes avanços conseguidos em relação a velocidade e largura de banda, no curto prazo de 32 anos. O desenvolvimento técnico é neste campo do conhecimento é notável. Porém este crescimento da Internet fica obscurecido com a limitação do protocolo de 32 bits, que dispõem de 4.294.967.296 de endereços totais (SANTOS *et al* 2010).

Neste contexto, uma pergunta torna-se particularmente relevante. Por que o IPv4 falhou como protocolo base da rede e precisou ser trocado apenas 11 anos após sua implantação? As razões são numerosas, e devem ser analisadas num contexto histórico e técnico de forma conjunta.

Historicamente, a tecnologia é adotada de forma cada vez mais rápida pela humanidade. Se no surgimento do telefone levou 75 anos para sua adoção por 50 milhões de usuários, hoje em dia um aplicativo demora apenas 19 dias para alcançar o mesmo número de usuários, como pode ser visto no Gráfico 1 (AEPPEL 2015).

Gráfico 1 - Tempo até nova tecnologia angariar 50 milhões de usuários



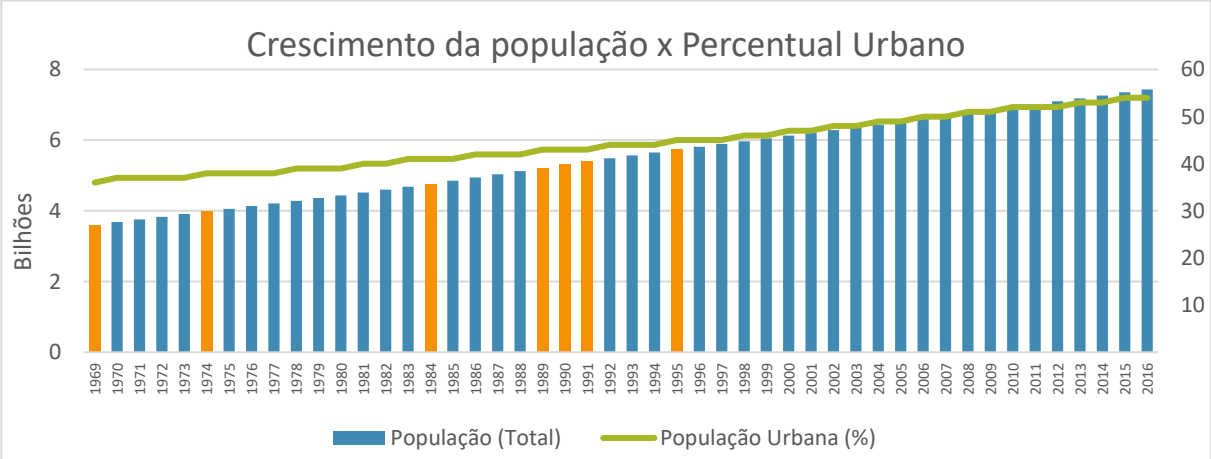
Fonte: Aeppel, T. (2015) e Nelson, R. (2016).

Além do alcance ser cada vez amplo e rápido, o perfil de usuários mudou muito desde o surgimento da ARPANET. Analisando dados históricos, entre as décadas de 60 e 80, pode-se constatar que ela era majoritariamente dominada por usuários acadêmicos e algumas poucas corporações militares e empresas civis. Mas

a partir do início da década de 90, com o surgimento do *HyperText Markup Language* (HTML) como linguagem padrão da Internet, permitindo um uso mais visual e prático, além da abertura da Internet para um perfil comercial, ela foi tomada por usuários comuns. O menor conhecimento técnico e o domínio de recursos básicos por esse perfil de usuário, foi o suficiente para fazer a rede crescer num ritmo exponencial, não previsto nem presenciado anteriormente (PATARA 2015). Esse crescimento só se acentuou com o surgimento de tecnologias que propiciaram a banda larga na década de 90 com surgimento de tecnologias como *Digital Subscriber Linei* (DSL), CableModem e telefones celulares (TANENBAUM 2011).

Nesse período de tempo entre 1969 e 2016, a população mudou não somente em quantidade, saindo de uma população em torno de 3,6 Bilhões de pessoas para quase 7,5 Bilhões de pessoas atualmente como apresenta o Gráfico 2, pode-se ver essa evolução, acompanhada de uma mudança da população urbana, que saltou de 44% para 56% hoje em dia.

Gráfico 2 - Crescimento da população x Percentual Urbano



Fonte: Worldometer (2016).

No quesito técnico, existem um conjunto de condições que cooperaram entre si para acarretar o problema citado. O protocolo IPv4 acabou adotado como padrão a partir de 1984, pois as redes dos Estados Unidos passaram a adotá-lo (KUROSE e ROSS 2010). No começo dos anos 80, as empresas requisitaram blocos IP e a se conectar na ARPANET também. Essa distribuição de endereços IPv4, fora realizada de maneira desregrada, onde os Estados Unidos e suas entidades, ficaram com a maior parte, e o resto do mundo dividiu o resto (HAGEN 2014). Eram alocados grandes blocos /8, equivalentes a 16.777.216 de endereços (TANENBAUM 2011).

Neste momento incipiente da Internet, e por esse perfil fortemente acadêmico, com apenas as grandes empresas se conectando na rede, e com muitos serviços e protocolos em desenvolvimento, as circunstâncias não permitiram aos cientistas e desenvolvedores da época vislumbrarem o futuro com precisão. Portanto a rede não teve foco nem em segurança, pois as transações comerciais não eram realizadas, e a troca de mensagens ocorriam em um meio totalmente controlado e bastante confiável. A escalabilidade que seria necessária também não foi levada em conta.

Essas necessidades só foram percebidas ao iniciar a Internet com perfil comercial, a partir de 1990. O protocolo IPv4 se mostrou pouco escalável e logo foi notado que seu esgotamento seria prematuro, limitando a rede. Atualmente, devido ao crescimento logarítmico da rede Internet, a mudança para o *Internet Protocol version 6* (*IPv6*) tem sido cada vez mais incentivada, contudo sua adoção segue um ritmo muito abaixo do pretendido. Tido como uma versão que se propõem justamente a combater o protocolo anterior e suas conhecidas fraquezas: conectividade fim-a-fim, escalabilidade, segurança. O IPv4 segue sem caminho sem paradas, até o esgotamento, sofrendo apenas algumas intervenções para estender sua vida útil, mas ainda assim, com um previsível fim de serviço no horizonte (PATARA 2015).

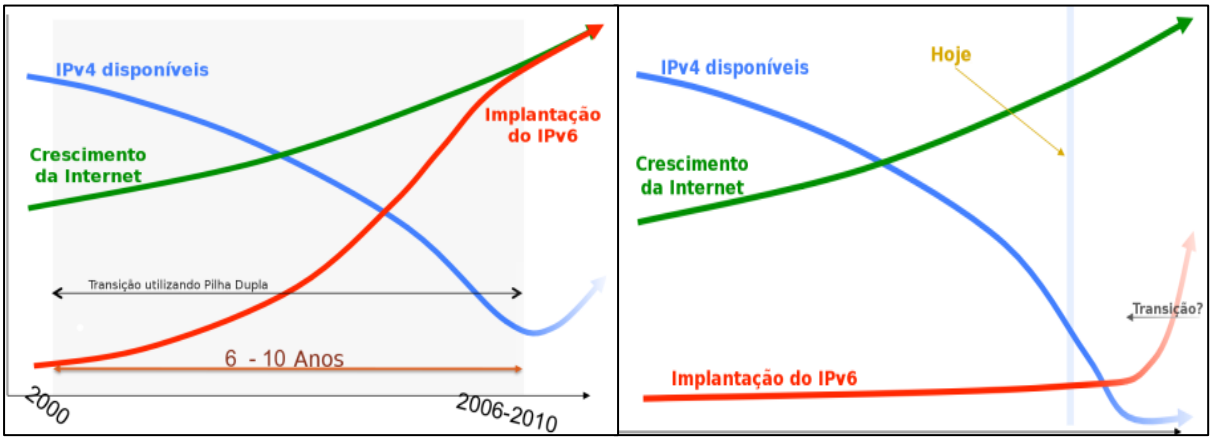
O surgimento deste novo protocolo, muito diferente do utilizado como pilar da Internet, gerou um atrito entre dois tipos distintos de empresas que tem a Internet como seu negócio principal: não havia conteúdo em IPv6, pois não existia conectividade, e não se ofertava conexão IPv6 visto não existir conteúdo.

É possível perceber no Gráfico 3 que entre o planejamento dos órgãos gestores da Internet e o efetivamente praticado, a partir de 2010, ocorreu um distanciamento muito grande.

Para combater essa disparidade, os órgãos gestores pensaram então em aumentar a oferta de conteúdo em um dia, para que houvesse maior interesse em realizar a conexão com o novo protocolo. Este incentivo ocorreu no dia 6 de junho de 2012, e ficou conhecido como *World IPv6 Launch*. Foi coordenado entre várias instituições, mas é possível destacar a *Internet Society*, e a *Internet Assigned Numbers Authority* (IANA) (ROBERTS 2011).

Através deste esforço, grandes empresas como Google, Facebook, Yahoo, Microsoft/MSN, entre tantas outras implementaram e ativaram de forma permanente o protocolo IPv6 em suas redes. Próximo de 400 empresas realizaram a ativação do protocolo em larga escala dentro de suas redes.

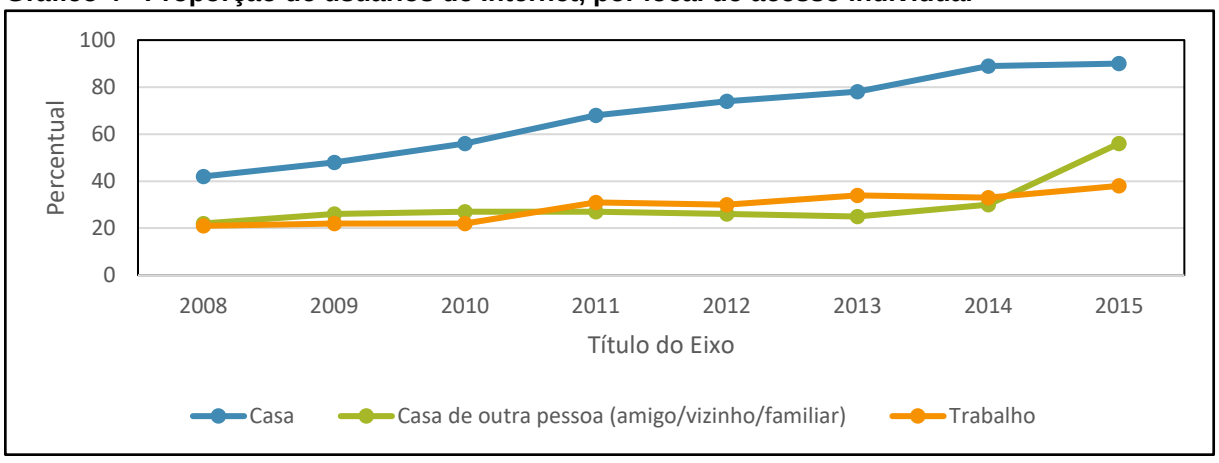
Gráfico 3 - Planejamento ideal comparado a execução atual da implementação do IPv6.



Autoria: Santos, R. R. dos; *et al*. (2010).

Uma outra mudança importante que ocorreu foi o adensamento de uso da Internet. Ela cresceu em tamanho e velocidade. A população tem utilizada a Internet de forma cada vez mais ubíqua, não somente em computadores e celulares, mas em toda a forma de dispositivo. As velocidades têm aumentado bastante ao longo do tempo, e a área de cobertura é cada vez maior, incluindo aí a área rural. Esse crescimento é facilmente observável no Gráfico 4.

Gráfico 4 - Proporção de usuários de Internet, por local de acesso individual



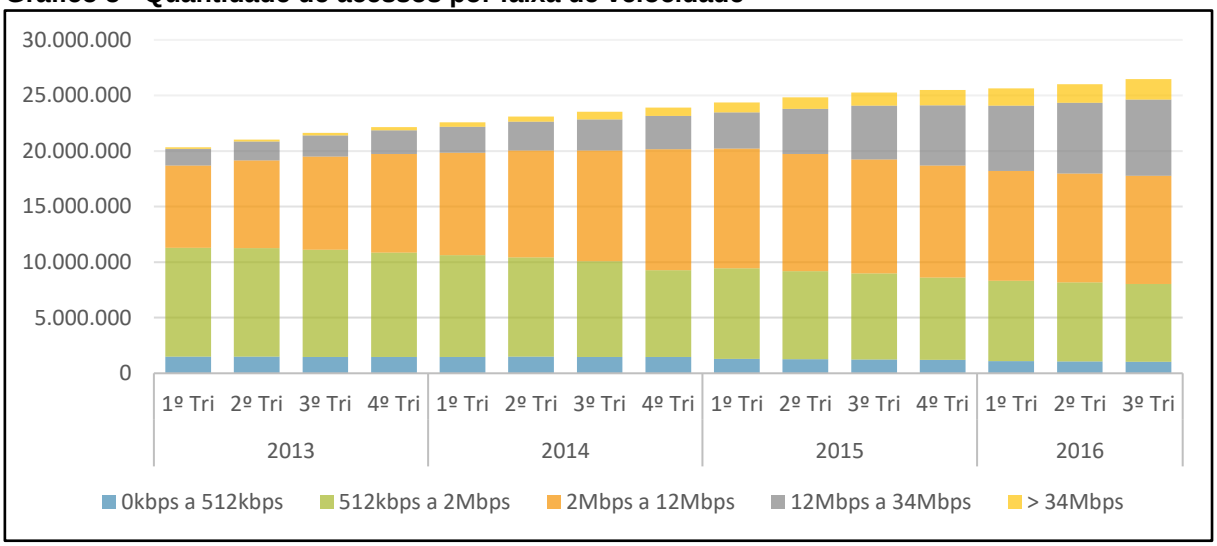
Fonte: CGI.br. TIC Domicílios 2015 (2016)

Essa mudança de velocidade tem sido importante para novas aplicações que tem surgido. Se no início à Internet era um ambiente primariamente de contato a

distância, com o surgimento de transações comerciais, novas aplicações têm sido criadas a cada ano: chamadas de voz sobre IP, vídeo sobre IP, consumo de vídeo sobre demanda, aplicações de vigilância e segurança, transações bancárias cada vez mais seguras e práticas, bens compartilhados reservados e pagos via Internet.

Essa maior oferta de velocidade pode ser visualizada no Gráfico 5. É possível notar um crescimento de 25% da base de acessos, e mais de 60% desses acessos já ocorrem com planos acima de 2Mbps.

Gráfico 5 - Quantidade de acessos por faixa de velocidade



Fonte: Dados Agência Nacional de Telecomunicações (2016)

Este aumento de consumo reflete diretamente no consumo de endereçamento. Quanto mais *hosts* conectados, maior a necessidade de endereços. A demanda aumenta numa razão inversamente proporcional a oferta.

Na implementação do protocolo *IPv6* existem três dificuldades principais: implementar o protocolo sem causar impacto negativo no desempenho da rede; a adaptação ao formato diferente de endereços; e a demanda de serviços como o DNSv6 e DHCPv6 ou SLAAC de forma mandatória para o pleno funcionamento da rede.

Deve-se trabalhar toda a estrutura da empresa onde será instalado o protocolo, visando criar um ambiente favorável ao pleno funcionamento. Isso gera alguns impactos nesse ambiente:

1. O ambiente pode precisar de mais equipamentos para implantação dos novos serviços necessários a operação do IPv6, à saber: o *Domain*

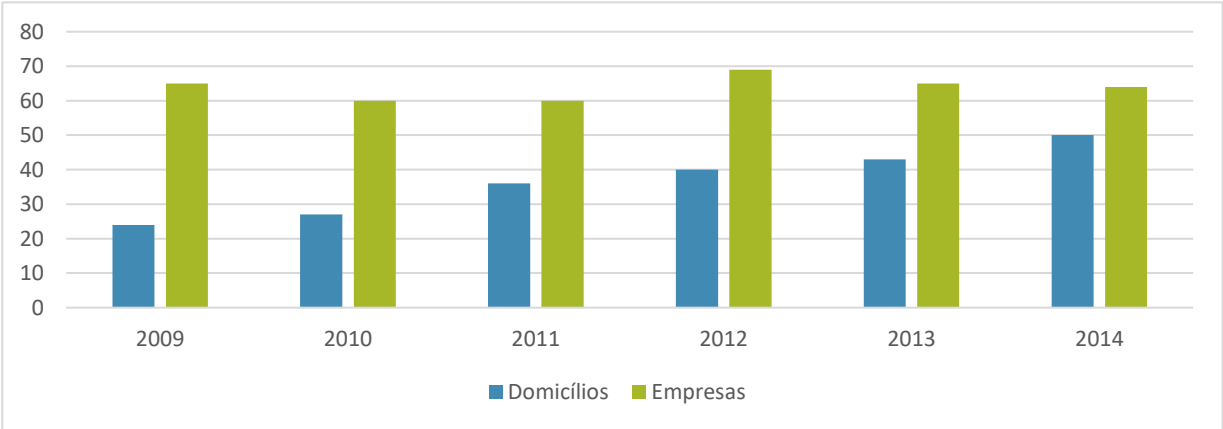
Name System for IPv6 (DNSv6), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6*) e o roteamento dinâmico (HAGEN 2014);

2. O uso de roteamento dinâmico provoca um aumento no consumo, à saber processamento e memória, dos recursos dos ativos intermediários da rede (roteadores, *switches* meios de trânsito);
3. Possibilidade de desempenho diferente entre os sites IPv4 e IPv6, pois os servidores podem estar em ambientes diferentes (SANTOS e al., Apostila - IPv6 Básico 2012).

Do ponto de vista do mercado consumidor, os clientes têm demandado endereçamento público, a fim de obter conectividade fim-a-fim, visando múltiplas aplicações: monitoramento de vídeo, telepresença, vídeos e música *on-demand* e jogos eletrônicos.

Esse mercado crescente, como é possível ver no Gráfico 6, demanda profissionais cada vez mais preparados. Mas esse mercado não tem uma regulamentação e muito menos formação específica.

Gráfico 6 - Percentual de acessos à Internet, em domicílios e empresas.



Fonte: CETIC.BR – Portal de Dados (2016)

Com tudo isso posto, é possível elencar alguns motivos para a elaboração deste trabalho. O primeiro deles é que o protocolo IPv6 é bem documentado tecnicamente, mas há poucos trabalhos na literatura que abordam o protocolo sobre a ótica de sua implementação prática.

Como o mercado é majoritariamente constituído de pequenas empresas, tornar esse conhecimento mais acessível pode facilitar a adoção por essa fatia do

mercado. Com um mercado de 2138 provedores (CGI.BR 2016)[1], não há capacitação especifica para seus postos de trabalho. Além disso as pequenas empresas não costumam possuir processos e funções bem definidos.

Ademais, as configurações exigidas possuem algumas peculiaridades que não possuem a devida relevância destacada na documentação oficial. A troca de informações entre os profissionais facilita e muito a configuração dos serviços. A documentação na Língua Portuguesa é insuficiente, com raríssimos livros disponíveis.

Com isso em vista, a oferta de uma metodologia clara e de cunho prático, mesmo envolvendo uma grande parcela do tempo na fase de elaboração e planejamento, visa facilitar a adoção do IPv6. A documentação proposta aspira uma linguagem acadêmica, mas de fácil compreensão, que possa estabelecer

Este trabalho destina-se, portanto, a migrar uma rede IPv4 totalmente operacional, que não pode sofrer impactos no seu funcionamento, e implementar uma rede de pilha-dupla[2], com os protocolos IPv4 e IPv6 sendo utilizados de forma conjugada. Esse processo deve ser documentado, aplicando o rigor científico, mas com um viés prático, podendo tornar-se uma documentação de auxílio a outros profissionais que buscam implementar o IPv6. É realizado também uma análise do atual desempenho do protocolo e seus eventuais incidentes.

1.1 OBJETIVO

1.1.1 Objetivo Geral

O objetivo geral, é a implantação do protocolo IPv6 em um provedor de conexão, utilizando a técnica de pilha dupla, funcionando paralelo ao protocolo IPv4, sem interromper a operação da rede. Com isso a rede ficará preparada para o crescimento futuro e a mudança operacional da Internet, que já está acontecendo.

---

[1] Dados do relatório de Tecnologias de Informação e Comunicação (TIC) Provedores 2014, divulgado em 2016 pelo Comitê Gestor da Internet no Brasil (CGI.BR).

[2] Costuma ser referido na documentação como *dual stack*, e refere-se ao ato de manter a conectividade IPv4 e IPv6 de forma conjunta, funcionando em paralelo.

1.1.2 Objetivo Específico

Como objetivos específicos, pode-se estabelecer:

- Motivar a migração para o IPv6, desmitificando o processo de implantação do novo protocolo;
- Proporcionar uma documentação do processo em Língua Portuguesa, visando tornar o processo mais acessível a trabalhadores de pequenas empresas;
- Expor algumas etapas sensíveis do processo, principalmente na configuração dos serviços;
- Formalizar uma metodologia de implantação, que facilite a replicação do processo por outras empresas;
- Permitir o acesso aos arquivos de configurações funcionais, para as versões presentes dos serviços.

1.1.3 Metodologia

Este trabalho se dispõe a realizar uma implementação completa do protocolo IPv6, em toda a estrutura de uma empresa de conexão a Internet. Será tomado como modelo um Provedor de Serviço de Internet na cidade de Bituruna/PR, possuidor de *Autonomous System* (AS)[3], conectado através de sessão *BGP Full Routing*[4], com a operadora Copel. O referido provedor possui atualmente 916 clientes ativos, conectados por meio de rádio digital na faixa livre de 5 GHz.

Sendo assim, implementa-se a configuração que permita o funcionamento pleno de uma rede de IPv6 desde o cliente final, até a Internet, por toda a sua estrutura, sem recursos artificiais tais como: *Network Address Translator 6to4* (*NAT64*), *Carrier-Grade Network Address Translator* (*CGNAT*), Tunelamento. Toda a rede trabalhará em pilha dupla permitindo assim a conexão dos assinantes aos serviços oferecidos na Internet tanto em IPv4 quanto em IPv6.

---

[3] Um Sistema Autônomo, comumente conhecido como AS, é constituído de um identificador único, e permite aos Provedores de Serviço de Internet publicar seus prefixos, e receber os prefixos de outros Sistemas Autônomos, sendo um dos pilares da Internet atual.
[4] É o ato de um AS trocar todos os prefixos da Internet com outro AS.

Serão respeitadas as seguintes etapas na implementação dessa rede:

- Plano de Endereçamento;
- Configuração do roteamento dinâmico externo, através de BGP4;
- Configuração do roteamento dinâmico interno da rede, através de OSPF;
- Dispor de um *firewall* básico para proteção da rede;
- Configuração dos serviços de *Domain Name Server* (DNS);
- Configuração do *Stateless Address Autoconfiguration* (SLAAC);
- Resultados dos testes pós configuração.

1.2 ORGANIZAÇÃO DO TRABALHO

Este trabalho é organizado através de quatro Capítulos e dois Apêndices. O Capítulo 1 é uma introdução ao tema, a justificação da necessidade deste documento e conteúdo desenvolvido nele, contendo ainda breve descrição dos passos realizados.

O Capítulo 2 realizou uma revisão teórica dos conceitos utilizados, bem como o modelo TCP/IP, endereçamento IPv6, BGPv4 IPv6, DHCPv6, DNSv6, roteamento dinâmico através do BGP e OSPF, e a entrega de endereços IPv6.

O Capítulo 3 apresenta o Estudo de Caso propriamente dito, contendo a topologia da rede, o planejamento da atividade, a implantação dos serviços implantados, bem como a configuração das soluções realizadas, além de testes para confirmar o funcionamento da rede em IPv6.

No Capítulo 4 retrata o resultado dos testes realizados. São indicadas as ferramentas utilizadas, a forma de teste e o resultado alcançado. Comenta-se ainda sobre eventuais problemas ocorridos após a configuração da rede em pilha dupla.

Por fim, o Capítulo 5 apresenta a conclusão deste trabalho, bem como os resultados obtidos após a implantação.

Os Apêndices 1 e 2 apresentaram os arquivos de configuração dos serviços necessários tais como: DNSv6, SLAAC, configurações de IPs e *firewall.*

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo serão explanados os fundamentos teóricos das redes baseadas em comutação de pacotes, seus protocolos principais, e o motivo pelo qual a adoção do IPv6 se faz necessária.

2.1 INTRODUÇÃO

Toda a comunicação de Internet é baseada em padrões abertos de comunicação. Os protocolos desenvolvidos a partir da década de 70, tiveram esse cuidado, para preservar a comunicação entre diferentes fabricantes (DIBONA, OCKMAN and STONE 1999). A Internet em si é fruto de uma comunicação baseada em três protocolos básicos: TCP, UDP e IP (KUROSE e ROSS 2010).

Atualmente a versão utilizada é a quarta, tornando-o conhecido como IPv4, ou mais popularmente IP. O IPv4 foi desenvolvido a partir do começo dos anos 70 para facilitar a comunicação e o compartilhamento de informação entre os pesquisadores governamentais e os acadêmicos nos Estados Unidos (HAGEN 2014).

O primeiro protocolo utilizado na incipiente *Advanced Research Projects Agency Network* (ARPANET) foi o *Network Control Protocol* (NCP). Ele esteve ativo entre 1970 e 1983, ano que foi substituído pelo robusto e flexível *Transmission Control Protocol*/*Internet Protocol* (TCP/IP). O planejamento desta mudança encontra-se detalhada na *Request For Comments* (RFC) 801 (POSTEL 1981). O TCP foi fruto do trabalho realizado por Vinton Cerf e Robert Kahn (KUROSE e ROSS 2010), em trabalho publicado em 1974 e que estabelecia as bases do protocolo TCP/IP.

Em uma época de rede fechada e com poucos institutos conectados, seu desenvolvimento não levou em consideração as questões de segurança ou qualidade de serviço. A escalabilidade prevista era gigante pois no final da década de 70, a ARPANET possuía em torno de 200 hosts, enquanto no fim da década de 80 haviam 100.000 *hosts* conectados (KUROSE e ROSS 2010). No ano seguinte já haviam três vezes mais redes (SANTOS et al 2010). Outra característica desse período, é que ele precedia a era dos computadores pessoais, e portanto, sendo este ambiente dominado especialistas.

O protocolo IP foi estabelecido na RFC 791 (POSTEL 1981), com duas capacidades intrínsecas: a fragmentação para envio de dados grandes em pequenos pacotes, conhecidos como datagramas, que podem ser transportados pela rede, e remontado no destino; endereçamento, que capacita a determinação de um endereço de origem e de destino (SANTOS et al 2010).

Nessa fase inicial, os escopos de endereços IP eram divididos em 3 blocos de tamanhos distintos:

- Redes de classe A – utilizando uma máscara de sub-rede 255.0.0.0 ou /8, estes blocos contêm 16.777.216 de endereços, equivalente a 2^{24} e com endereços entre 1.0.0.0 e 126.0.0.0;
- Redes de classe B – com a sub-rede 255.255.0.0 ou /16, equivalente a 2^{16}, totalizado 65536 endereços, entre o 128.1.0.0 e 191.254.0.0;
- Redes de classe C – esta é a sub-rede 255.255.255.0 ou /24, com um total de 256 endereços, ou 2^{8}, e escopo entre 192.0.1.0 e 223.255.254.0 (SANTOS et al 2010).

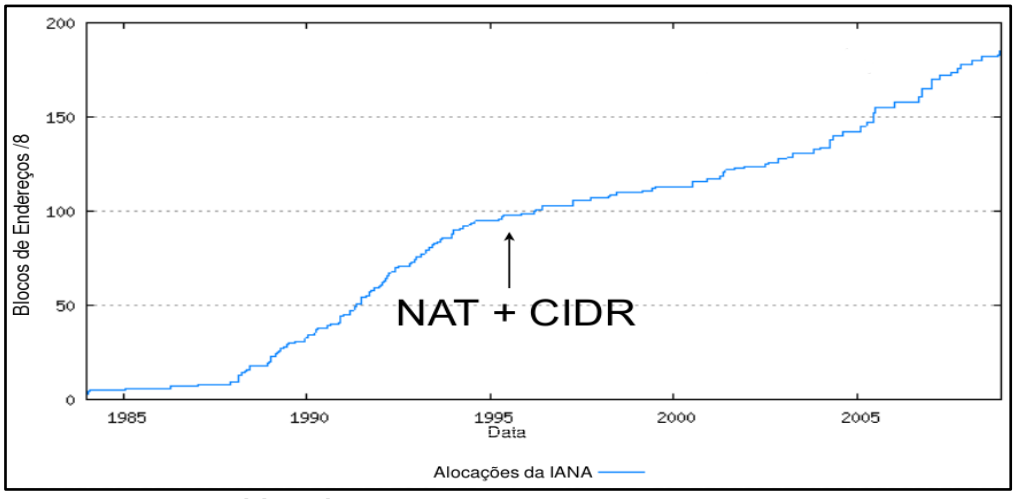
Além dessas classes existem ainda duas que são restritas: a classe D com os endereços entre 224 e 239 reservada para *Multicast*; e a classe E com os endereços entre 240 e 255. Estas duas classes de endereços porém são reservadas, não sendo possíveis serem utilizadas fora de aplicações específicas, e impedidas de serem usadas para conexão da Internet.

Além disso a Internet como se conhece, surge após o desenvolvimento da *World Wide Web* (WWW) por Tim Bernes-Lee entre 1989 e 1991, dentro do *Conseil Européen pour la Recherche Nucléaire* (CERN). Este conceito de interligaçãol baseado na ideia de hipertexto, apresentadas por Vannevar Bush em 1945 em um artigo intitulado “*As we may think*”, e por Ted Nelson em 1960, que inclusive cunha o termo hipertexto, através do Projeto Xanadu. Tim Bernes-Lee e sua equipe apresentaram em 1991 versões dos programas que são a base do que a Internet é hoje: *HyperText Markup Language* (HTML), *HyperText Transfer Protocol* (HTTP), Servidor WEB e um navegador de páginas HTML (KUROSE e ROSS 2010).

Com um crescimento exponencial da Internet, a *Internet Engineering Task Force* (IETF) passa a discutir formas de mitigar os efeitos do rápido esgotamento dos endereços IP. Em 1991 foi criado o grupo *Routing and Addressing* (ROAD) que apresenta três soluções (TANENBAUM 2011):

- *Classless Inter-Domain Routing* (CIDR) – definida através da RFC 1519 e posteriormente pela RFC 4632. Ela define blocos de endereço de tamanho variável através de prefixos de rede, permitindo um uso otimizado da tabela de roteamento pelas organizações;
- *Dynamic Host Configuration Protocol* (DHCP) – apresentada através da RFC 1514 e posteriormente pela RFC 2131, proveu a capacidade de um terminal de rede adquirir automaticamente um endereço IP, máscara de rede, *gateway* de saída e outras informações concernentes a rede. Dessa forma o endereço só é utilizado enquanto o equipamento está em uso, disponibilizando para outro equipamento caso seja desligado;
- *Network Address Translation* (NAT) – especificada através da RFC 1631 e mais tarde definida na RFC 3022, implementa a ideia de que um único endereço de IP público e com roteamento válido, possa ser utilizado para uma pequena rede, de forma que *hosts* possam ter acesso aos serviços fornecidos pela Internet. Ela o faz através do uso do conceito de redes privadas, estabelecida na RFC 1918. Esta RFC estabelece três endereços de redes, que passam a ter uso restrito a redes classificadas como internas ou redes privadas. Os endereços são: 10.0.0.0 – 10.255.255.255 /8, 172.16.0.0 – 172.31.255.255 /12 e 192.168.0.0 – 192.168.255.255 /16. (SANTOS et al 2010).

Gráfico 7 - Alocações de blocos /8 pela IANA e o impacto causado pela adoção do NA, o DHCP e o CIDR.



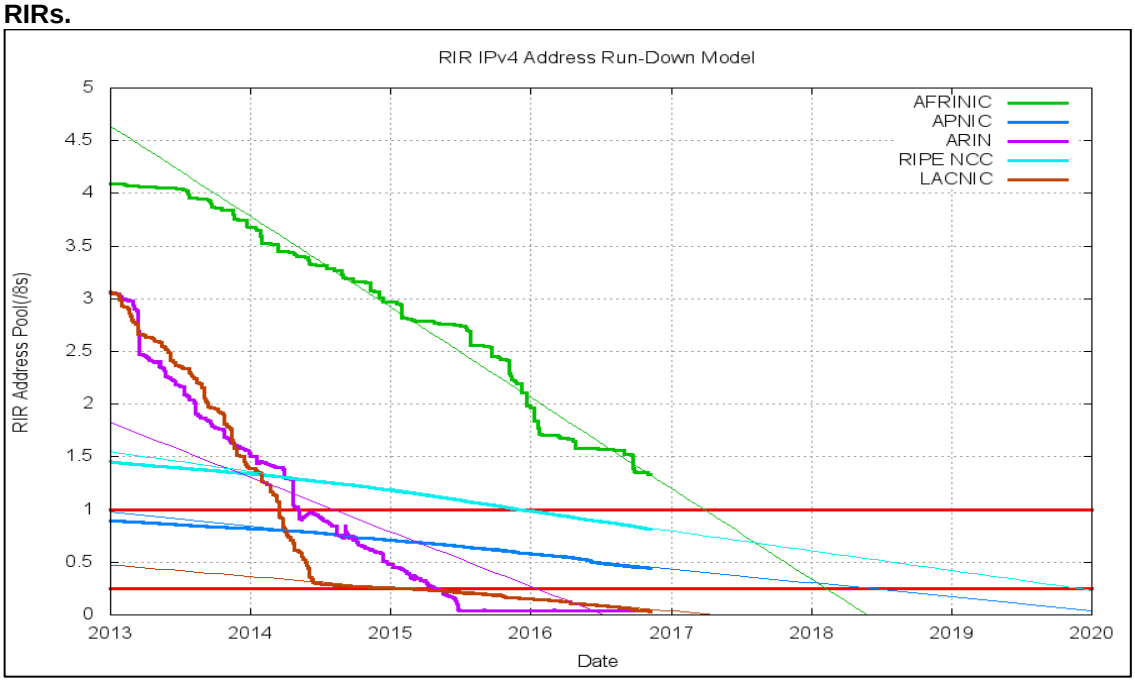
Fonte: Santos, et al (2010)

Essas tecnologias visavam alargar o horizonte do esgotamento do IPv4. Elas combatiam o problema em três frentes: melhorando a alocação para empresas através do CIDR, e promovendo o uso racional dos endereços nos usuários através de NAT e DHCP. No Gráfico 7 é possível ver como esses mecanismos atrasaram o esgotamento do IPv4 em 10 anos (SANTOS *et al* 2010).

Este esgotamento de endereços IPv4, foi finalmente alcançado em 3 de fevereiro de 2011, quando a IANA alocou seus últimos blocos para os *Regional Internet Registries* (RIR) (HUSTON, 2016). Já estes órgãos de registro regionais, também iniciaram com políticas de contenção, e tiveram seus blocos considerados exaustos, com as reservas já sendo alocadas. Estes dados podem ser conferidos conforme o Gráfico 8. Estes RIRs entraram em esgotamento da seguinte forma:

- *Asia-Pacific Network Information Centre* (APNIC) – 19 de abril de 2011;
- *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) – 14 de setembro de 2012;
- *Latin America and Caribbean Network Information Centre* (LACNIC) – 10 de junho de 2014;
- *American Registry for Internet Numbers* (ARIN) – 24 de setembro de 2015.

Gráfico 8 - Projeção do consumo dos blocos de endereços IPv4 remanescentes nos RIRs.



Fonte: Geoff Huston – http://www.potaroo.net/tools/ipv4/index.html (2016)

Atualmente o único RIR que possui uma reserva ativa é o africano *African Network Information Center* (AFRINIC), tendo estimada a chegada ao primeiro nível de alerta a partir de 2017.

Junto a este trabalho de contenção de esgotamento dos endereços IPv4, a IETF criou um novo grupo de trabalho em 1993 chamado de *Internet Protocol next generation* (IPng) (HAGEN 2014), e os itens relacionados através eram: escalabilidade, segurança, configuração e administração de rede, suporte a QoS, mobilidade, políticas de roteamento, transição (SANTOS et al 2010).

Em 1995 através da RFC 1752 o IPng apresentou um resumo das propostas mais promissoras:

- *TCP and UDP with Bigger Addresses* (TUBA) – definido nas RFCs 1347, 1526 e 1561, uma evolução do *Simple* CLNP;
- *Simple Internet Protocol Plus* (SIPP) – apresentado através da RFC 1710, que foi a integração das propostas *Simple Internet Protocol* (SIP) e *Paul's Internet Protocol* (PIP).
- *Common Architecture for the Internet* (CATNIP) – estabelecido através da RFC 1707 (SANTOS et al 2010).

Contudo todas estas propostas foram consideradas insuficientes e a recomendação para o novo protocolo foi a soma das melhores características de cada proposta, mais o endereçamento com base em 128 bits (HAGEN 2014).

Em dezembro de 1995 foi apresentada a RFC 1883, nomeada como *Internet Protocol, Version 6 (IPv6) Specification*, substituída em 1998 pela RFC 2460. As principais características do recém aprovado IPv6 foram:

- Capacidade de endereçamento ampliada – O endereçamento passa de uma base de 32 bits do IPv4 para uma base de 128 bits no IPv6;
- Autoconfiguração – Possivelmente o maior avanço do IPv6, é justamente sua característica de autoconfiguração, através do mecanismo de *Stateless Address Autoconfiguration* (SLAAC). Através dele um bloco /64 é alocado para o equipamento de uma rede, por exemplo um cliente, e este configura automaticamente todos os *hosts* da rede que tiverem suporte IPv6. Normalmente requer a ativação de uma opção no roteador da rede;

- Simplificação do cabeçalho – é um cabeçalho de tamanho fixo, com 40 bytes, com 16 *Bytes* para a origem, 16 *Bytes* para o destino e 8 *Bytes* para informações gerais, facilitando o trabalho do roteamento;
- Melhoria ao suporte de opções e extensões – ao utilizar opcionais na comunicação, como *IP Security Protocol* (IPSec)[5], é utilizado um cabeçalho de extensão, portanto, somente comunicações realmente necessárias carregam informação extra.

Pode-se ver no Quadro 1 um comparativo entre as duas versões do cabeçalho.

Quadro 1 - Comparativo das características dos protocolos IPv4 vs IPv6

	IPv4	**IPv6**
Endereço	32bits	128bits
Cabeçalho	Todos os cabeçalhos são processados, mesmo quando não são utilizados.	Cabeçalho simplificado, flexível e versátil.
Fragmentação	Em qualquer ponto	Apenas nas pontas.
NAT	Utilizado NAT para ampliar o espaço de endereços.	Não se utiliza NAT.
IPSec	Suporte IPSEC opcional.	IPSEC é opcional, mas o suporte é nativo.
Configuração	Manual ou via DHCP.	Manual, SLAAC ou via DHCPv6.
Tamanho mínimo de rede	Não há.	É de /64.

Fonte: Autoria Própria

2.2 MODELO OSI

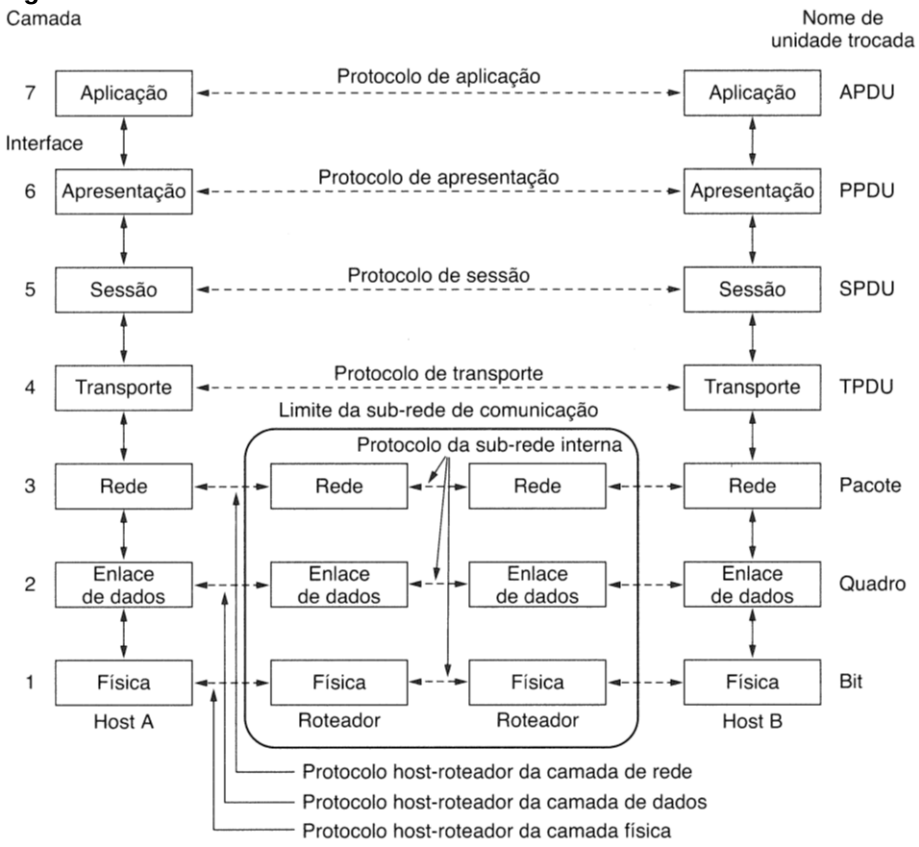
O Modelo *Open System Interconnection* (OSI) foi estabelecido no final da década de 1970 pela *International Organization for Standardization* (ISO) (FOROUZAN 2008). Este modelo teórico constituído de 7 camadas, faz uma distinção

[5] O IPSec, ou *IP Security Protocol*, é um protocolo que implementa segurança, aumentando a privacidade dos dados.

grande entre 3 conceitos fundamentais em cada camada: serviços, interfaces e protocolos.

Cada camada desde modelo estabelece serviços que são fornecidos as camadas superiores, definindo especificamente as funções daquela camada. Já as interfaces de cada camada estabelecem como os processos de cada camada podem ser acessados pelas camadas acima, definindo os parâmetros requisitados. Por fim, os protocolos são independentes entre as camadas, e podem ser utilizados os protocolos que se encaixem melhor para a tarefa, desde que provejam os serviços estabelecidos (TANENBAUM 2011).

Figura 1 - O modelo de referência OSI



Autoria: Tanenbaum, A. (2011)

Na Figura 1 é possível ver o modelo de referência OSI. Ele é constituído por:

1. A camada física – é a parte física da conexão entre dois computadores. Aqui são estabelecidos os valores elétricos e de tempo, envolvidos na conexão, a forma como se dará a conexão inicial e como ela será encerrada fisicamente. Nesta camada se definem a taxa de

transmissão de dados, a sincronização de bits, a configuração da linha e o modo de transmissão (TANENBAUM 2011);

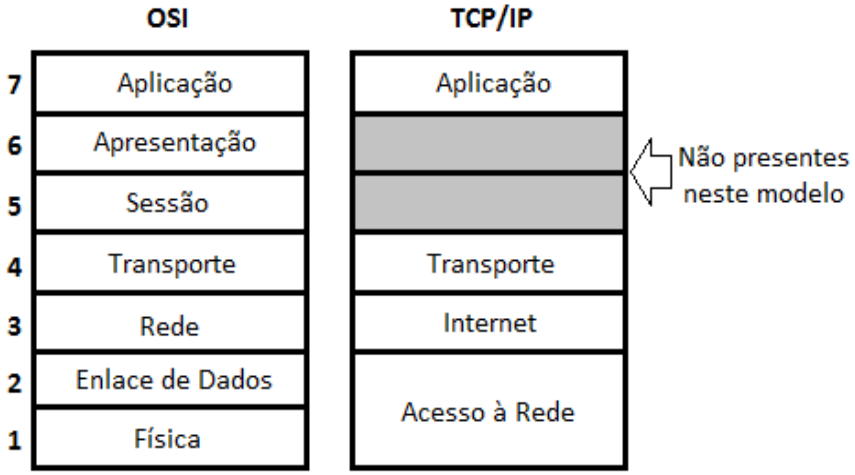
2. A camada de enlace de dados – é a camada que virtualiza o canal de transmissão em uma linha de transmissão robusta a erros. Os dados são divididos em quadros de dados contendo no máximo alguns Kilobytes e são transmitidos em sequência ordenada. As respostas são dadas por quadros de confirmação. Aqui também são definidos o endereçamento físico, o controle de fluxo e de erros, além do controle de acesso à rede (TANENBAUM 2011);
3. A camada de rede – é a camada que efetivamente controla a entrega dos dados ao destino, mesmo que estes dados trafeguem por uma rede distinta da origem. Aqui são definidos o endereçamento lógico e os roteamentos entre redes distintas (FOROUZAN 2008);
4. A camada de transporte – esta camada é responsável por organizar o processo de transmissão, garantindo a entrega dos dados de forma íntegra, ordenada e supervisionado o controle de erros e de fluxo do nível origem-destino da camada de rede (FOROUZAN 2008);
5. A camada de sessão – já aqui são estabelecidas sessões de comunicação entre *hosts*, oferecendo o controle de diálogo, e a sincronização através de verificações periódicas em longas transmissões para permitir recuperações em falhas de transmissões (TANENBAUM 2011);
6. A camada de apresentação – esta camada não se ocupa com a representação de bits em si, mas sim com a sintaxe utilizada e a semântica empregada nas informações transmitidas. Assim são estabelecidas estruturas de dados de forma abstrata, usando para isso uma codificação padronizada (TANENBAUM 2011);
7. A camada de aplicação – a camada superior, é responsável por prover a interface que permite que um usuário ou um outro *software*, possa acessar os recursos disponíveis na rede, através de protocolos específicos de aplicação, permitindo serviços como os de *HyperText Transfer Protocol* (HTTP) e email (TANENBAUM 2011).

2.3 MODELO TCP/IP

O desenvolvimento do modelo de referência TCP/IP é posterior aos protocolos envolvidos. Portanto ele tem uma melhor equivalência entre suas camadas e os protocolos envolvidos. Por outro lado, ele tem pouca distinção entre os serviços, interfaces e protocolos envolvidos e oferecidos. O modelo de referência TCP/IP é constituído por quatro camadas: *host*-rede, *internet*, transporte e aplicação (FOROUZAN 2008), como é possível notar na Figura 2. Sendo um conjunto de protocolos hierárquicos, distribuídos nas quatro camadas, e agregados na forma de módulos independentes, mas que podem ser combinados para trabalhar também de forma conjugada.

No objetivo de sua construção, estava a capacidade de comutar pacotes, independente da rota que fosse percorrida, e pudessem se reagrupados e interpretados no destino da comunicação. Seria uma rede tolerante a falhas, que poderia perder nós e ainda assim estar disponível.

Figura 2 - O modelo de referência TCP/IP



Fonte: Tanenbaum, 2011

2.3.1 Camada *host*-rede, ou acesso a rede

É correspondente às camadas física e de enlace de dados do modelo OSI. É coberto por grande conjunto de protocolos. Existem alguns padrões abertos como: Ethernet, 802.11. Também alguns padrões privados, tais como: DSL, GPON, GEPON

e DOCSIS. Todos esses protocolos são utilizados na padronização de equipamentos de comunicação em redes de computadores.

2.3.2 Camada internet

Conhecida como camada de interconexão de rede, definida em inglês como *internet*, é a camada dos protocolos básicos de comunicação. Essa camada é composta por:

- IP (*Internet Protocol)* - O protocolo IP é do tipo *best-effort*[6], sendo uma forma de transmissão não confiável e sem conexãoe sem diferenciação por serviço. Ele, portanto, não dispõem de mecanismos de verificação, correção de erros, ou garantia de entrega dos dados. Conjuga seus dados em datagramas que podem percorrer percursos diversos, de diferentes tamanhos, podendo chegando fora da ordem de envio (FOROUZAN 2008).
- ICMP (*Internet Controle Message Protocol*) - é um dispositivo utilizado para o envio de mensagens de consulta e informações sobre erros de comunicação (FOROUZAN 2008).
- IGMP (*Internet Group Message Protocol*) - utilizado na transmissão de uma mensagem de forma simultânea a um host ou um grupo de destinatários (FOROUZAN 2008).
- RARP (*Reverse Address Resolution Protocol*) - este protocolo é responsável pela descoberta de um endereço lógico IP, quando o *host* conhece apenas seu endereço físico MAC (FOROUZAN 2008).
- ARP (*Address Resolution Protocol*) - é o responsável por descobrir o endereço físico de um host quando se conhece apenas seu endereço lógico na rede.

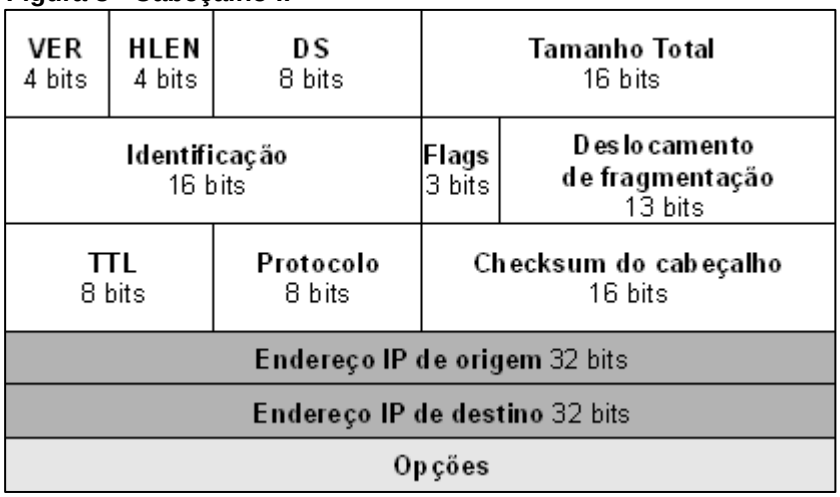
[6] Geoff Huston define uma rede baseada em *best-effort* como uma rede onde a qualidade de serviço não é praticada, e portanto, não há priorização de nenhum tipo de pacote em trânsito. Todos eles são tratados da mesma forma (HUSTON 2001).

2.4 INTERNET PROTOCOL (IP)

O protocolo IP é a base da comunicação digital, e como define Forouzan (2011), “é o protocolo da camada de rede que controla os processos de entrega *host-to-host* na Internet. É um protocolo orientado ao melhor esforço, e não se preocupa em garantir a entrega e é sem conexão. Possui apenas um mecanismo rudimentar para detecção de erros e os descarta em caso de corrupção dos pacotes, e trabalha na camada 3.

A confiabilidade na entrega da informação é garantida, quando combinado com o protocolo TCP (camada 4) e que será explicado na seção subsequente.

Figura 3 - Cabeçalho IP



Fonte: Forouzan (2011)

Os pacotes IP são denominados como datagramas, e pode-se ver uma descrição do cabeçalho desses pacotes na Figura 3. Com um tamanho total de 16 *bits*, o maior tamanho do pacote é de 65.536 *bytes*. Desse, o cabeçalho varia entre 20 e 60 bytes, para dados referentes aos dados e endereçamento (TANENBAUM 2011).

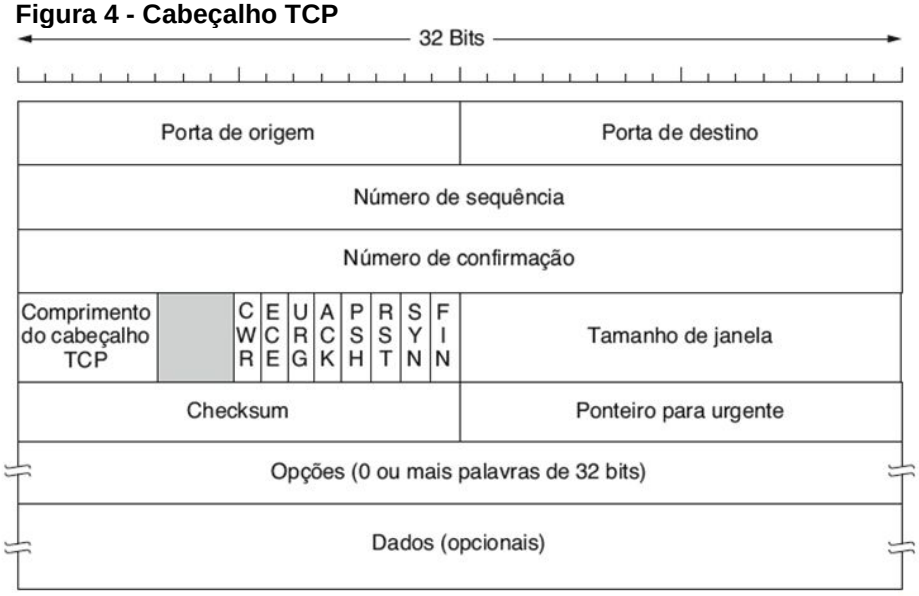
2.5 PROTOCOLO TCP

Este é o protocolo responsável por garantir a confiabilidade a todo o processo de comunicação entre redes que utilizam o conjunto TCP/IP. Forouzan (2011) o define como um protocolo que “orienta e fornece confiabilidade aos serviços da camada IP”.

Ele foi definido notadamente como um protocolo que fornece um fluxo de dados, em bytes, fim a fim, confiável em uma rede interligada não confiável. Isso acontece porque redes podem ter diferentes topologias, atrasos, larguras de banda, diferença no tamanho dos seus pacotes entre outros parâmetros (TANENBAUM 2011).

Na Figura 4 pode-se ver como é um cabeçalho do pacote TCP. Ele é constituído de 20 *Bytes* fixos, mais uma parte opcional. A limitação do datagrama TCP é relacionado ao tamanho máximo do IP, por este encapsular o protocolo TCP. Portanto a carga máxima do protocolo TCP é de 65.515 *Bytes* de tamanho. Como a rede padrão Ethernet costuma utilizar pacotes com tamanho máximo de 1500 bytes, esse costuma ser o tamanho do pacote. Com pacotes menores do que esse, pode ocorrer um fenômeno conhecido como fragmentação dos pacotes, onde a origem tentar passar uma informação total de 1500 bytes, e no meio do caminho esse pacote pode ser dividido para se adequar a um tamanho de rede menor, o que gera a necessidade de mais pacotes, podendo ocasionar lentidão e quebra de conexão. Podem ser enviados pacotes maiores, de até o tamanho limite do IP, e são conhecidos como *Jumboframes*, sendo trafegados em redes com características especiais (FOROUZAN 2008).

Figura 4 - Cabeçalho TCP



Fonte: Tanenbaum (2011).

Como o TCP é um protocolo orientado a conexão, cada pacote recebe um identificador único de 32 bits, são sequenciados, para poder serem agrupados no receptor.

2.6 TEORIA BÁSICA IPV6

Nesta seção será visto o que o IPv6 trouxe de diferencial ao que existia até então. Em primeiro lugar, quando foram requisitadas pesquisas sobre um substituto ao protocolo IP, a IETF especificou algumas as sequintes características desejadas:

- Possuir o endereçamento grande o suficiente para não voltar a se tornar uma preocupação em um futuro próximo;
- Simplificar o cabeçalho, para um processamento mais eficiente pelos roteadores;
- Otimizar as tabelas de roteamento;
- Disponibilizar segurança em sua forma nativa;
- Permitir a priorização de serviços específicos, como aplicações de tempo real;
- Obter uma rede autoconfigurável;
- Possibilitar a convivência com protocolo legado[7].

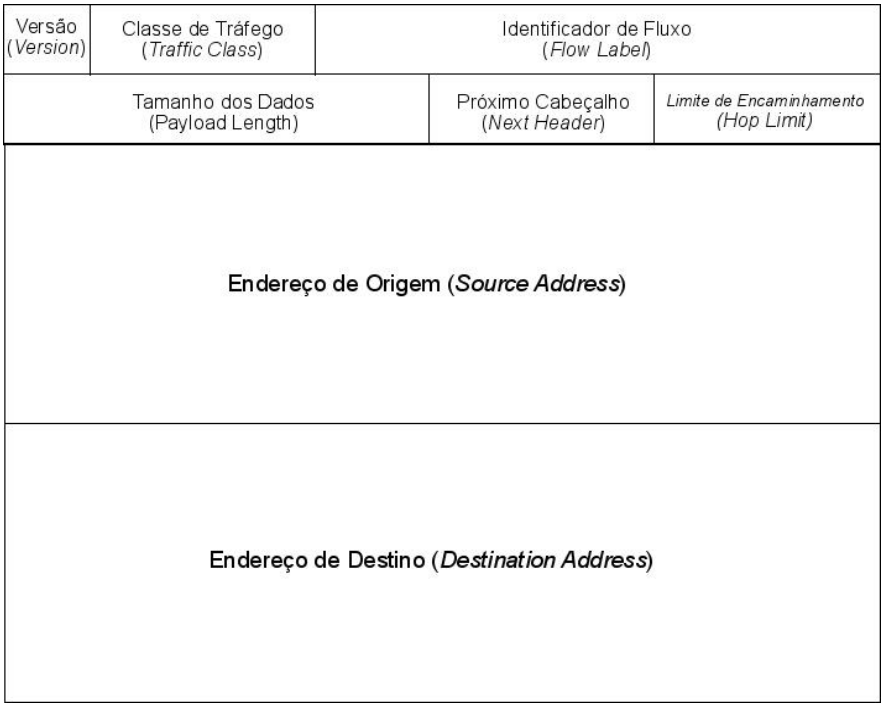
Em 1993 a IETF convocou os pesquisadores interessados através da RFC 1550, designada "*IP: Next Generation (IPng) White Paper Solicitation*". As 27 propostas iniciais, foram reduzidas para as sete mais interessantes, e posteriormente às 3 mais promissoras. Em 1995 a RFC 1752, nominada "*The Recommendation for the IP Next Generation Protocol*", determinou o primeiro escopo do protocolo, que seria denominado IPv6. Em 1998 foi adotado como *Internet Standard* pela IETF (SANTOS *et al* 2010).

Em suas características iniciais, foram inclusos um cabeçalho de tamanho fixo de 40 bytes, com apenas 7 campos para serem processados, ao invés dos 12 campos do cabeçalho do IPv4.

Além disso, o endereçamento é de 128 bits, com um total de 340.282.366.920.938.463.463.374.607.431.768.211.456 de endereços. Para se colocar em escala o que isso representa, seria o equivalente (estimado) a uma rede com 32 endereços para cada molécula de água do oceano (TANENBAUM 2011).

[7] Além do protocolo IPv4, existem ainda o ARP, RARP, ICMP, IGMP que devem conviver na mesma rede, sem conflitos de função (HAGEN 2014).

Figura 5 - Cabeçalho IPv6



Fonte: Tanenbaum (2011)

Na Figura 5 pode ser visto o cabeçalho IPv6. A necessidade de informação adicional, como quando se ativa o *Internet Security Protocol* (IPSec), é resolvido através do uso de Cabeçalhos de Extensão.

Outra diferença fundamental, é que o pacote engloba o cabeçalho e os dados, de forma separada, dando um *payload* total de 65.535 bytes, especificado sempre pelo campo de “Tamanho de Dados” (TANENBAUM 2011).

Um protocolo que ganhou muita importância no IPv6 foi o ICMPv6. Adquiriu funções que antes eram desempenhadas pelo ARP, pelo RARP e do IGMP. Além disso, tem como função a notificação de erros, realização de mensagens de consulta, como as mensagens de solicitação de roteador e anúncio de roteador (HAGEN 2014).

Quando se necessita de funções especiais, passa-se a utilizar um Cabeçalho de Extensão.

2.7 ENDEREÇAMENTO IPV6

Como o protocolo IPv6 tem um endereçamento de base 128 bits, foi necessário desenvolver uma nova forma de representação. A notação escolhida para

representar os 16 *Bytes* do endereçamento foi dividi-los em oito conjuntos, com quatro algarismos hexadecimais, separados pelo sinal de dois-pontos entre estes conjuntos (TANENBAUM 2011). A representação encontra-se no Quadro 2.

Quadro 2 - Formato do Endereço IPv6

2001:0db8:0000:0000:0123:4567:89ab:cdef

Fonte: Autoria Própria.

Ainda foi convencionado uma facilitação nessa representação. Cada zero à esquerda, dentro do conjunto, pode ser omitido. Se ocorrerem um ou mais conjuntos compostos por zeros, podem ser simbolizados por um par de dois pontos. Mas essa simplificação só pode ocorrer uma vez no endereço, no conjunto que compreender mais zeros, de forma a evitar ambiguidades. O mesmo endereço poderia ser representado no formato simplificado (HAGEN 2014) conforme descrito no Quadro 3.

Quadro 3 - Endereço IPv6 simplificado

2001:db8::123:4567:89ab:cdef

Fonte: Autoria Própria.

Na definição dos endereços, foram definidos também, alguns endereços especiais, assim como acontecia com o IPv4. Eles são, segundo HAGEN (2014), e SANTOS, *et al* (2012):

- 2000::/3 – endereços de *global unicast*. São os endereços efetivamente alocados pela IANA e os RIRs;
- fe80::/10 – endereços de *link-local unicast*. São endereços de uso local, sem possibilidade de roteamento;
- fc00::/7 – endereços *unique local IPv6*. É um endereço potencialmente único globalmente, mas que não deve ser roteado, sendo um identificador global, pseudo-randômico;
- 0:0:0:0:0:0:0:0 ou ::0 – endereço não especificado. É utilizado para indicar a ausência de endereços, como o 0.0.0.0 no IPv4;
- 0:0:0:0:0:0:0:1 ou ::1 – endereço de loopback. É utilizado para referenciar o próprio host;
- 2002::/16 – endereços utilizados na técnica de transição 6to4;

- 2001:0000::/32 – endereço utilizado com a técnica de transição TEREDO[8];
- 2001:db8::/32 – endereço utilizado para produção de documentação.

Além desses existem muitos endereços começados por FF0 reservados as comunicações *multicast*, especificados na RFC 2375 (HINDEN e DEERING 2016).

Uma mudança importante implementada pelo novo protocolo, foi a introdução do conceito de distribuição de redes ao invés de endereços. Uma das características que os pesquisadores implementaram, foi o de autoconfiguração. Para isso, o roteador da rede é configurado para responder a requisições de *Router Solicitation* (RS), com mensagens de *Router Advertisements* (RA) (HAGEN 2014).

Sempre que um endereço IPv6 é alocado, dá-se um processo de confirmação de disponibilidade desse endereço, chamado de *Duplicate Address Detection* (DAD). Nesse caso o host que recebe o endereço tenta descobrir se esse endereço é único na rede, enviando uma mensagem de *Neighbor Solicitation* no enlace. Essa mensagem é forjada com o campo origem nulo, e com o endereço de destino sendo o endereço que está sendo testado. É enviado então para o endereço de *Multicast Solicited Node*, e caso receba uma resposta do tipo *Neighbor Advertisement*, contendo no campo origem o mesmo endereço questionado, ou o campo destino com o endereço *Multicast All-Nodes*, a atribuição é interrompida (SANTOS e al., Apostila - IPv6 Básico 2012).

2.7.1 Plano de Endereçamento

Uma parte crucial na adoção de IPv6 em uma rede é o plano de endereçamento, que quando bem feito pode facilitar a implementação e a manutenção desta (HAGEN 2014). Se existe uma etapa na qual se deve dedicar tempo e planejamento é esta. Mas por quê? As redes distribuídas em IPv6 são enormes. O LACNIC por exemplo recomenda (SANTOS et al 2010):

- /32 – Rede mínima para provedores de internet. É o equivalente a 65.536 redes IPv6 /48, ou então 4.294.967.296 de redes IPv6 /64.

[8] A técnica de tunelamento automática TEREDO foi criada pela Microsoft e é definida na RFC 4380 (SANTOS e *et al* 2010).

Lembrando que hoje existe esse número em relação a quantidade de endereços IPv4 em toda a Internetmundial (2^{32} endereços);

- /48 – Para empresas. Equivale a 65.536 redes IPv6 /64. Pode-se ainda utilizar como rede mínima a /56, mas a recomendação para flexibilidade e planejamento futuro nas redes corporativas é uma /48;
- /64 – Para clientes domésticos. Equivale há 18.446.744.073.709.551.616 endereços IPv6 para um único cliente doméstico.

Este plano de endereçamento deve abordar todos os aspectos da rede: servidores envolvidos, localização geográfica e quantidade de redes clientes. Tudo isso levando em conta que o protocolo IPv6 foi planejado para roteamento de forma sumarizada (SANTOS *et al*. 2010). Esse planejamento ainda ajuda na configuração do IGP e do *firewall*. A medida que os endereços estão definidos, a configuração do IGP abstrai a questão dos endereçamentos, e a elaboração de regras do *firewall* é facilitada, pois os endereços a serem trabalhados já estão especificados. (SANTOS *et al* 2010)

Um mecanismo criado para facilitar o planejamento de endereçamento do IPv6 está definido na RFC 3531, conhecida como "*A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block*" (Marc Blanchet, 2003). Esta RFC aborda três métodos de endereçamento possíveis, escolhendo os endereços sobre os bits a serem manipulados.

Tomando uma rede /56 como exemplo, ela poderia ser fragmentada em 256 redes /64. Considerando-se o endereço 2001:0db8:0000:00<u>00</u>::/56, se alteram os *bits* sublinhados. Convertendo essa notação para binário haveria um escopo entre 00000000 e 11111111 serem realizados os ajustes.

A proposta de endereçamento de Marc Blanchet é:

- *Leftmost* – 10000000. As redes seriam alteradas da esquerda para direita. Portanto ele seria dividido em 80, 40, C0, etc;
- *Centermost* – 00010000. As redes são definidas a partir dos números centrais, gerando a sequência 10, 08, 18, etc;
- *Rightmost* – 00000001. É uma sequência numérica escalar simples: 00, 01, 02, etc;

A estratégia é sempre um assunto de cunho pessoal. Mas a estratégia recomendada, é a *leftmost*, pois ela permite acomodar espaços entre os endereços, e com isso acomoda o crescimento de longo prazo (SANTOS *et al*, 2012). Como os endereços não estão contíguos, caso um prefixo esteja esgotado e careça se expandido, pode anexar a rede vizinha. Essa prática otimiza o roteamento através de sumarização de rotas dinâmicas (SANTOS et al, 2010).

2.8 ROTEAMENTO IPV6

Para o roteamento, o IPv6 trouxe algumas novidades. Em primeiro lugar, pode ser utilizado um Cabeçalho de Roteamento, que pode especificar um ou mais nós que devem ser visitados no caminho para o destino (HAGEN 2014).

Além disso, os protocolos de roteamento dinâmico precisaram ser adequados à nova versão do IPv6. O IS-IS realizou apenas uma adaptação para implementar o IPv6. Ocorreu também o lançamento do OSPFv3 e do BGPv4 para adequar estes protocolos.

Uma das preocupações do roteamento do IPv6 é a sumarização de rotas. Esse é o motivo pelo qual com IPv6 se alocam redes e não endereços aos clientes. Com um endereço maior, as tabelas de roteamento poderiam crescer exponencialmente, resultando em necessidades de ajustes no *hardware*. Com a sumarização de rotas, espera-se que os mesmos equipamentos utilizados atualmente possam prover o roteamento do novo protocolo. O roteamento dinâmico é essencial na nova arquitetura com IPv6, pois são endereços que costumam ser sempre roteados.

A rota padrão, que é a designação de rota para todos os endereços que não estão explícitos na tabela de roteamento, também tem uma nova representação. No IPv6 ela tem a notação ::/0 (HAGEN 2014).

2.8.1 OSPFv3

A adaptação do protocolo OSPF para suportar as mudanças necessárias de semântica de comandos e tamanho de endereços, é descrita na RFC 2740 (COLTUN,

FERGUSON e MOY 1999). Sendo um *Interior Gateway Protocol* (IGP), o OSPF na sua versão atualizada mantém a característica de permitir ao sistema manter a tabela de rotas atualizadas de forma autônoma. O OSPF é um protocolo orientado pelo estado da conexão, conhecido como *link-state*. Ele mantém uma tabela com os roteadores principais e os classifica de acordo com a distância e um custo. Com esses dados os roteadores mantêm uma árvore dos roteadores da rede, e sempre encaminham os pacotes para o caminho mais curto. Para selecionar a rota mais curta, é utilizado o algoritmo *Shortest Path First* (SPF) de Dijkstra[9] (TANENBAUM 2011).

As mensagens utilizadas para comunicação no protocolo são conhecidas como *Link-State Advertisements* (LSA). Na versão 3, os endereços IPv6 não são utilizados em todas as mensagens, ficando de fora as mensagens de *Router-LSA* e *Network-LSA*. Os identificadores de *Area ID* e *Link State ID*, continuam sendo de 32 bits. Os roteadores designados e os reservas, são identificados pelo *Router ID*, e não mais pelos IPs dos roteadores. Mas convenciona-se utilizar o endereço IPv4 da *loopback*, para identificar o *Router ID* e organizar a configuração da rede.

Além disso o pacote utilizado no OSPFv3 é diferente do anterior. É comum a utilização de endereços *link-local unicast*, para a identificação de endereços de origem. Ele roda por enlace, e não mais por sub-rede. Inclusive é possível a utilização de múltiplas instâncias, visto a interface poder ter mais de um endereço. A comunicação utiliza também endereços de *multicast* FF02::5 (*all OSPF routers*) e FF02::6 (*all OSPF DRs*) (HOGG 2013).Caso seja configurada a autenticação para a instância, ela será realizada através de *IPSec*.

2.8.2 BGP4

Conforme definem Kurose e Ross: “O BGP é um protocolo absolutamente crítico para a Internet– em essência, é o protocolo que agrega tudo” (KUROSE e ROSS 2010).

[9] O Algoritmo de Dijkstra foi primeiramente descrito em 1959 em um artigo denominado: “*A note on two problems in connexion with graphs*”, publicado no Journal Numerische Mathematik, *Volume* 1, *Issue* 1, páginas 269-271. Soluciona o problema para encontrar o menor caminho entre dois nós de rede.

O protocolo BGP não possui uma versão específica para o protocolo IPv6, mas ao invés disso, em sua versão 4, ele utiliza a característica de trabalhar com outros protocolos da camada de rede. Ele possui uma extensão que suporta o IPv6 (HAGEN 2014).

O BGP é um protocolo que permite o uso como *Interior Gateway Protocol* (IGP), para a distribuição de rotas entre os roteadores que compõem um sistema autônomo (SANTOS et al 2010).

O BGP utiliza os números de Sistema Autônomo para comunicações entre os roteadores. Cada roteador conectado na Internet, quando configurado para trabalhar com tabela completa, mais conhecido como *full routing*, recebe uma lista de todos os roteadores e Sistemas Autônomos conectados àquela rede, permitindo assim conhecer todos os caminhos possíveis que um pacote deve percorrer entre o seu remetente e o destinatário.

Quando os sistemas autônomos envolvidos possuem identificadores distintos, o BGP se comporta como um *Exterior Gateway Protocol* (EGP). Ele é um protocolo já maduro, e que utiliza a porta TCP de número 179, para comunicação. Ele trabalha com mensagens do tipo: *OPEN*, *UPDATE*, *NOTIFICATION* e *KEEPALIVE*. Diferente do OSPF, o BGP trabalha com os endereços da versão do IP que estiver se comunicando naquela sessão (HAGEN 2014).

As mensagens do tipo *OPEN* são utilizadas para estabelecer a conexão entre dois *hosts*, normalmente conhecidos como *peers*. Eles verificam informações sobre o *peer* e estabelecem os parâmetros que serão utilizados. As mensagens do tipo UPDATE informam novas rotas, para o roteador que a originou. Já as do tipo NOTIFICATION informam quando ocorrem erros. As mensagens do tipo KEEPALIVE, não carregam informação, apenas mantem a conexão aberta e ativa (HAGEN 2014).

Atualmente as tabelas de roteamento pleno (*Full Routing*) possuem acima de 609.750 registros no IPv4, e maior que 32.000 registros no IPv6. Mas a adoção tem aumentado ao longo do tempo, como é possível perceber no Gráfico 9.

Gráfico 9 - Trânsito IPv4 e IPv6 de ASs

Fonte: 6lab Cisco – Cisco System, Inc. (2016).

2.9 DHCPV6

Como já explanado, uma das características do IPv6, é a autoconfiguração, chamada nesse caso de *Stateless* ou Sem Estado. Mas existem casos que são necessários controle sobre esse processo. A entrega de endereços a clientes em um provedor pode ser associada via endereço MAC e dessa forma implementado os controles de velocidade e qualidade de serviço necessários, por exemplo (SANTOS *et al* 2010).

O protocolo DHCP foi proposto pela primeira vez em outubro de 1993, na RFC 1531 (DROMS 1993). Ele visava o reaproveitamento de endereços, sendo um gestor de endereços da rede. A medida que os endereços que ficam ociosos, como quando um *host* era desligado, esse endereço retornava para o conjunto de endereços a serem alocados. Dessa forma os *hosts* podiam compartilhar endereços, em horários distintos, e otimizar o uso das redes (TANENBAUM 2011).

Já no DHCPv6 a intenção é a de prover algum controle sobre as redes, em vista das mesmas em clientes e corporações serem muito vastas. Os clientes finais devem receber uma rede /64, equivalente a $1.8446744e^{+19}$ de endereços. Já empresas devem receber no mínimo uma rede /56, que engloba um total de $4.7223665e^{+21}$ endereços (SANTOS *et al*, 2012).

Conjugado a um servidor DNS, pode facilitar a utilização de serviços de rede e compartilhamento de impressoras, por exemplo. Esse tipo de distribuição de endereços, utilizando um DHCPv6, é conhecido como *Stateful autoconfiguration*, ou Autoconfiguração com Estado (HAGEN 2014).

Os serviços de DHCP e DHCPv6 são independentes, podendo rodar em redes de pilha dupla. Mesmo quando já existe uma rede configurada, ainda que de forma estática, pode-se fornecer alguns dados extras, como servidores DNS e SIP (HAGEN 2014).

Uma outra característica importante do IPv6 é que ele pode fornecer múltiplos endereços para uma mesma interface. Além disso uma rede que possua um DHCPv6 pode ser configurada mesmo sem um roteador. Ele pode se comunicar com o serviço do DNSv6, de forma a registrar os endereços fornecidos pelo DHCPv6.

Uma última coisa que deve-se ressaltar é que cada cliente e servidor, possuem um identificado único, conhecido como *DHCP Unique Identifier* (DUID). Junto com eles é gerado também um objeto usado pelo servidor chamado de *Identity Association* (IA), utilizado para identificar e manipular grupos de endereços (HAGEN 2014).

No processo de comunicação, um cliente envia uma mensagem de solicitação multicast, para encontrar um servidor DHCPv6 disponível. Caso queira se conectar com algum servidor específico, ele utiliza uma DUID dentro da opção *Server Identifier Option*. Caso o cliente receba mais de uma resposta, ele utiliza um algoritmo de decisão, descrito por HAGEN (2014):

- Prioriza a mensagem com maior *Server Preference*;
- Se ocorre um empate, ele escolhe de forma randômica um dos servidores;
- Em último caso ele pode escolher através de uma mensagem com menor *Server Preference*, caso contenha parâmetros de configuração mais apropriados.

Além disso o cliente executa o processo de *Duplication Address Detection* (DAD), para cada endereço alocado pelo servidor. Isso evita que um endereço, seja ele gerado automaticamente ou alocado por um serviço, fique ativo na interface de rede (SANTOS *et al* 2010).

O DHCPv6 apesar de ser um serviço importante do protocolo IPv6, deve ser tratado de forma própria no *firewall*, para evitar que um atacante possa tentar obter

conexão com máquinas, através do fornecimento de um DHCPv6 *Relay* impróprio. Da mesma forma não se deve fornecer endereços para fora do roteador de borda da rede[10].

2.10 DNSV6

O serviço de nomes de domínio, comumente conhecido como DNS, é conhecido pela sua capacidade de transformar nomes inteligíveis e facilmente reconhecíveis ao ser humano, em endereços IP que são efetivamente processados pelos *hosts* de rede. Nas redes IPv6 esse papel tem uma maior relevância, dado o tamanho dos endereços, e os espaços de redes disponíveis (HAGEN 2014).

Em redes mistas IPv4 e IPv6 existem uma entrada para cada endereço necessário. Os registros IPv6 são definidos no tipo AAAA, também conhecido como *Quad-A*, e é definido pela RFC 3596 (HAGEN 2014).

Os registros AAAA e PTR do DNS, podem ter sintaxes diferentes, dependendo da implementação e do servidor configurado. Mas a resposta sempre será igual. No *daemon Berkeley Internet Name Domain* (*BIND*), essa sintaxe é (HAGEN 2014):

- www.example.com. IN AAAA 2001:db8::1
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA
  IN PTR www.example.com.

Essa capacidade que o DNS possui em responder endereços dos dois tipos, é fundamental também na utilização do algoritmo *happy eyeballs*. Esse algoritmo implementa uma forma na qual os programas decidam qual versão do protocolo IP utilizar. Definido na RFC 6555, o programa deve requisitar o endereço para o DNS, e ele faz essa requisição para os dois endereços com um pequeno atraso. Caso a conexão IPv6 não apresente resposta, a conexão se dará via IPv4. Essa é uma forma de evitar uma demora grande para estabelecer a conexão em redes de pilha dupla (HAGEN 2014).

[10] Roteador de borda, e a nomenclatura de um roteador que realiza a comunicação entre duas redes distintas (TANENBAUM 2011).

Uma outra característica é que o DHCPv6 e o DNSv6 podem ser conectados, de forma que ao delegar um endereço DHCP, já seja acrescentado um registro DNS. Dessa forma se facilita a utilização dos *hosts* de uma rede.

Uma rede deve-se ofertar, portanto dois tipos distintos de serviço de nomes de domínio:

- Consultas recursivas – quando um *host* da rede, deseja descobrir um endereço IP associado a um domínio de Internet;
- Consulta de autoridade sobre um registro – ocorre quando um *host* da Internet questiona a um servidor da rede se ele possui autoridade sobre um domínio específico. Necessário quando a rede oferece hospedagem, por exemplo.

3 ESTUDO DE CASO

Neste capítulo será vista a implementação do protocolo IPv6 em um ambiente já em produção, que encontra-se roteando unicamente IPv4.

Para a implementação do protocolo IPv6 em uma rede de computadores, se fazem necessários alguns requisitos:

- Um plano de endereçamento, com o planejamento de distribuição das redes;
- O recebimento das rotas IPv6 via EGP;
- Um serviço de IGP para o roteamento dessas redes dinamicamente;
- Dois servidores DNS que suportem requisições *Quad-A*;
- Autenticação dos clientes, para entrega do endereço e o controle de QoS contratado. Normalmente se utiliza um autenticador com *Remote Authentication Dial In User Service* (RADIUS), e o endereço é entregue via DHCPv6 ou PPPOE.

Todos os arquivos de configuração, serão disponibilizados em Apêndices. No Apêndice A estão os arquivos referentes as configurações do: servidor autoritativo de DNS *ISC-BIND*[11]; servidor recursivo de DNS *Unbounding*[12]. Já no Apêndice B estão disponibilizados o arquivo referente a configuração do roteador *Mikrotik*[13], rodando RouterOS: BGP, OSPFv3, *firewall*.

3.1 TOPOLOGIA DA REDE

Para este documento, estabelece-se alguns parâmetros para tratamento das configurações. Estes padrões referem-se aos endereços que serão utilizados na elaboração do documento e os padrões a serem utilizados nas configurações.

Como endereços IPv4, serão adotados o 192.168.0.0/16, 192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24, estabelecidos na RFC 5735. Para o IPv6 será

[11] ISC-BIND é o servidor DNS disponibilizado pela Internet Consortium. Pode ser utilizado tanto para consultas de autoridade sobre domínio, como consultas recursivas.
[12] *Unbouding* é um servidor DNS recursivo de alto desempenho.
[13] *Mikrotik* é uma marca de equipamento de rede da Letônia com grande adoção pelas pequenas empresas de Provimento de Serviço de Internet.

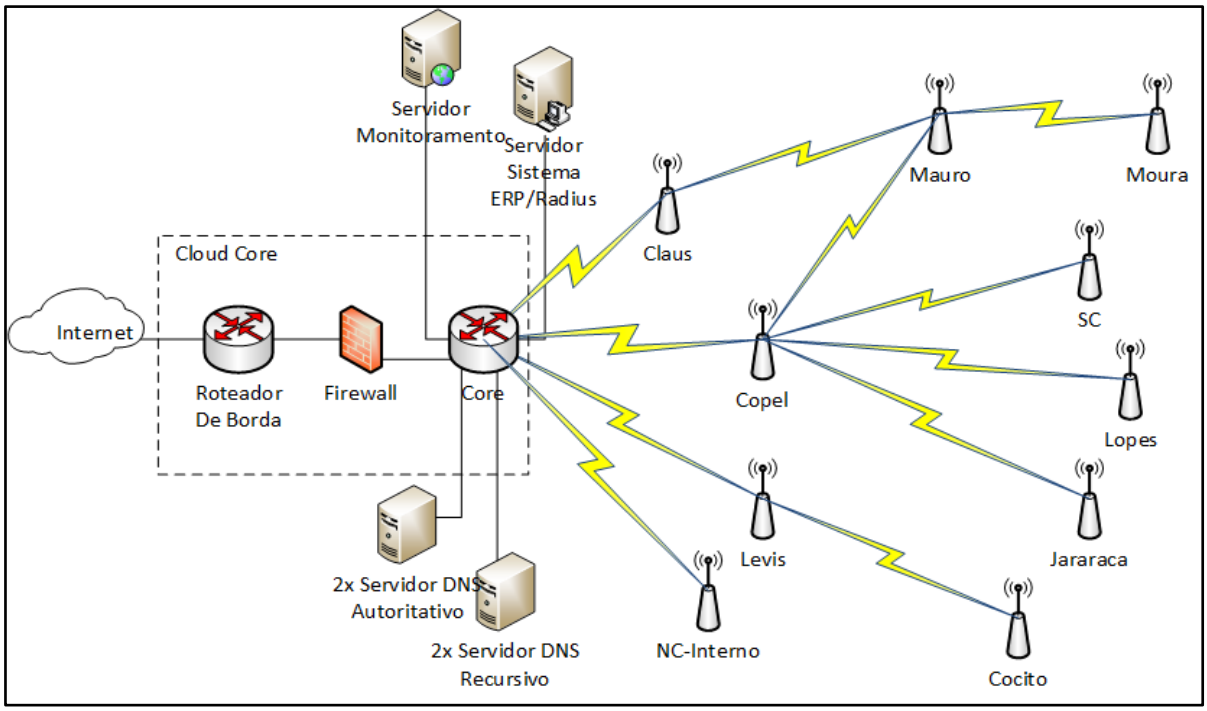
utilizado o endereço de documentação 2001:db8::/32, estabelecido na RFC 3849. Como IGP será configurado o OSPFv3. Para o EGP será o protocolo BGP4.

Serão estipulados endereços distintos para as duas localidades, considerando assim duas cidades distintas. Apesar de serem considerados duas localidades distintas, para fins didáticos na criação do endereçamento, todas as configurações propostas serão referentes a uma das localidades, pois esse modelo é facilmente replicável e escalável.

Deve-se também considerar alguns identificadores de AS. Neste documento serão considerados dois provedores de serviços, um com o AS 64496 e outro com o AS 64511, conectados na localidade 1. A rede a ser configurada será considerada com o AS 65550. As regras que definem o uso de AS de documentação estão na RFC 5398 (HUSTON, Autonomous System (AS) Number Reservation for Documentation Use 2008).

Para a interconexão dessa rede com a Internet, serão consideradas duas operadoras de conexão, estabelecidas aqui como Fornecedora1 e Fornecedora2. Elas proverão a conexão através de IPv4 e IPv6, utilizando o protocolo BGP como EGP da rede.

Figura 6 - Diagrama da rede proposta.



Fonte: Autoria Própria

Além disso as empresas que fornecem a conexão, também devem prover um endereço de conexão. Considerar-se-a para a Fornecedora1 o endereço como: 2001:db8:0:1::2/64 e o *gateway* 2001:db8:0:1::1. Já para a rede IPv4 será a 10.0.0.2/30 e *gateway* 10.0.0.1. Já para a Fornecedora2 os endereços serão: 2001:db8:0:2::2/64 e o *gateway* 2001:db8:0:2::1. A Fornecedora2 terá os IPv4 sendo os 10.0.1.2/30 e o *gateway* 10.0.1.1.

É disponibilizado também um modelo da rede que será abordada, para facilitar a compreensão desta topologia, através da Figura 6. Os dois roteadores e o *firewall*, definidos como *Cloud Core*, são na verdade um equipamento, e estão representados assim apenas para facilitar a compreensão das funções.

3.2 PLANO DE ENDEREÇAMENTO

Como visto no item 2.7.1 deste documento, existem três formas para realizar o planejamento da rede. Para a rede considerada neste estudo se utilizará o método *leftmost*.

Com base no endereço 2001:db8::/32 e utilizando o método *leftmost* a rede foi dividida em:

- 2001:db8:8000::/48 – Localidade 1. Esta localidade possuirá configurada a rede IPv4 192.168.128.0/17;
- 2001:db8:4000::/48 – Localidade 2. Esta localidade possuirá configurada a IPv4 192.168.0.0/17;

Além disso é descrito a necessidade de servidores para provimento dos serviços necessários para o funcionamento da rede. Será reservado para estes os endereços 2001:db8:8000:ffff::/64. No caso do IPv4 se utilizará o IP 192.0.2.0/28 para os servidores.

Em uma rede, uma boa prática é se trabalhar com *loopback* (GREEN e SMITH 2002). A maior vantagem da utilização de interfaces *loopback* para a configuração de roteamentos dinâmicos, é que essas interfaces não ficam com status de queda. No OSPF, por exemplo, que é um protocolo de estado de enlace, isso faz uma grande diferença. Para configuração dos endereços de *loopback* dos roteadores então, foram estabelecidos os endereços 2001:db8:8000:fffe::/64. Os endereços de IPv4 da *loopback* serão os 192.168.254.0/24.

Também é necessário estabelecer uma rede para os enlaces. Pela quantidade de redes, pode-se optar por trabalhar com 1 rede /64 por enlace, ou então pode-se trabalhar com enlaces utilizando a redes com máscara /127. Como não se utiliza o menor e o maior IP da rede para definir a rede e o broadcast, como no IPv4, não existe desperdício, e facilita a sumarização de rotas pelo OSPF. Já para o IPv4 será utilizada a rede 192.168.253.0/24

E por fim, para os clientes serão utilizados os *pools*[14] entre 2001:db8:8000:0::/64 e 2001:db8:8000:fff::/64, o que permite atender até 4096 clientes por localidade. Para os clientes serão distribuídos os endereços 172.16.0.0/12.

Serão considerados também como IPs válidos os endereços 192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24. Todos endereços referenciados na RFC 5735, para utilização em documentações.

Também é estabelecido que toda a distribuição dessas rotas se dará através de IGP, configurado na figura do popular OSPF. Como é um protocolo de estado de enlace, com um algoritmo bem conhecido, e com um desempenho bastante satisfatório. No OSPF quando um enlace estabelece conexão entre dois pontos, o processamento costuma levar em torno de 40 segundos, independentemente do número de nós (MOLLOY 1992). As alterações são propagadas em fração de segundos.

No Quadro 4 é apresentado um resumo do plano de endereçamento.

Quadro 4 - Plano de Endereçamento

Função na rede	**IPv4**	**IPv6**
Localidade 1	192.168.128.0/17	2001:db8:8000::/48
Localidade 2	192.168.0.0/17	2001:db8:4000::/48
Servidores	192.0.2.0/28	2001:db8:8000:ffff::/64
Loopback dos roteadores	192.168.254.0/24	2001:db8:8000:fffe::/64
Enlaces	192.168.253.0/24	2001:db8:8000:fffd::/64
Endereços/redes de atendimento aos usuários	172.16.0.0/12	2001:db8:8000::/52

[14] Um *pool* de endereçamento, é um conjunto de prefixos utilizados pelos serviços de alocação de IPs, como DHCP.

Endereços IP públicos	192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24	Todo IPv6 da classe 2001:db8::/32 é considerado público.
Fornecedor 1 – AS 64496	10.0.0.1	2001:db8:0:1::1/64
Fornecedor 2 – AS 64511	10.0.1.1	2001:db8:0:2::1/64
Empresa – AS 65550	10.0.0.2/30 10.0.1.2/30	2001:db8:0:1::2/64 2001:db8:0:2::2/64

Fonte: Autoria Própria.

Deve-se também já preestabelecer os endereços a serem utilizados nos servidores e roteadores, além das alocações dos clientes. Isso facilita bastante a implementação.

Quadro 5 - Endereços dos servidores da Localidade 1

Servidores	**Endereço IPv4**	**Endereço IPv6**
dnsa1.example.com	192.0.2.6	2001:db8:8000:ffff::6/64
dnsa2.example.com	192.0.2.7	2001:db8:8000:ffff::7/64
hosting.example.com	192.0.2.9	2001:db8:8000:ffff::9/64
dnsr1.example.com	192.0.2.11	2001:db8:8000:ffff::11/64
dnsr2.example.com	192.0.2.12	2001:db8:8000:ffff::12/64

Fonte: Autoria Própria

Conforme proposto, os endereços do Quadro 5, referem-se aos servidores hospedados na Localidade 1, que será tratada como a principal do provedor. Uma prática aceitável, como na divisão dos endereços, é deixar espaços entre os endereços, para melhor distribuição de novos servidores em uma expansão. Mas é uma prática estética, de cunho exclusivamente organizacional, não tendo nenhum efeito prático diferente, ou consequência na operação caso não seja seguido.

Quadro 6 - Endereços de *loopback* dos roteadores

Roteador	**Endereço IPv4**	**Endereço IPv6**
CORE	192.168.254.1	2001:db8:8000:fffe::1/128
LEVIS	192.168.254.2	2001:db8:8000:fffe::2/128
COPEL	192.168.254.3	2001:db8:8000:fffe::3/128
CLAUS	192.168.254.4	2001:db8:8000:fffe::4/128
MAURO	192.168.254.5	2001:db8:8000:fffe::5/128

MOURA	192.168.254.6	2001:db8:8000:fffe::6/128
SC	192.168.254.7	2001:db8:8000:fffe::7/128
LOPES	192.168.254.8	2001:db8:8000:fffe::8/128
JARARACA	192.168.254.9	2001:db8:8000:fffe::9/128
COCITO	192.168.254.10	2001:db8:8000:fffe::10/128
INTERNO	192.168.254.11	2001:db8:8000:fffe::11/128

Fonte: Autoria Própria.

Já no Quadro 6 é estabelecido os endereços de *loopback* dos roteadores da rede. Aqui se reforça a necessidade de utilizar os endereços de loopbacks para a conectividade e troca de informações do roteamento dinâmico. Eles proveem a comunicação independente do enlace, pois os endereços das interfaces físicas só funcionam quando elas estão ativas, estado definido como *UP*. Caso alguma interface perca a conexão física, fica em um estado administrativo inativo, ou *DOWN*. Porem ao trocar informações entre nós da rede pela *loopback*, através dos enlaces físicos, a sessão não fica sujeita ao estado físico da interface de rede física.

O Quadro 7 lista todos os endereços de enlaces entre os roteadores. Com todos os endereços estabelecidos, a configuração é bem mais prática.

Quadro 7 - Endereços destinados aos enlaces dos roteadores

Roteador	**Interface**	**Endereço IPv4**	**Endereço IPv6**
CORE	ether1-bgpas1	10.0.0.2/30	2001:db8:0:1::2/64
	ether2-bgpas2	10.0.1.2/30	2001:db8:0:2::2/64
	ether3-levis	192.168.253.1/30	2001:db8:8000:fffd::1/127
	ether4-copel	192.168.253.5/30	2001:db8:8000:fffd::3/127
	ether5-claus	192.168.253.9/30	2001:db8:8000:fffd::5/127
	ether6-interno	192.168.253.13/30	2001:db8:8000:fffd::7/127
LEVIS	ether1-core	192.168.253.2/30	2001:db8:8000:fffd::2/127
	ether2-cocito	192.168.253.17/30	2001:db8:8000:fffd::9/127
COPEL	ether1-core	192.168.253.6/30	2001:db8:8000:fffd::4/127
	ether2-mauro	192.168.253.21/30	2001:db8:8000:fffd::11/127
	ether3-sc	192.168.253.25/30	2001:db8:8000:fffd::13/127
	ether4-lopes	192.168.253.29/30	2001:db8:8000:fffd::15/127
	ether5-jararaca	192.168.253.33/30	2001:db8:8000:fffd::17/127

CLAUS	ether1-core	192.168.253.10/30	2001:db8:8000:fffd::6/127
	ether2-mauro	192.168.253.37/30	2001:db8:8000:fffd::19/127
MAURO	ether1-copel	192.168.253.18/30	2001:db8:8000:fffd::12/127
	ether2-claus	192.168.253.38/30	2001:db8:8000:fffd::20/127
	ether3-moura	192.168.253.41/30	2001:db8:8000:fffd::21/127
MOURA	ether1-mauro	192.168.253.42/30	2001:db8:8000:fffd::22/127
SC	ether1-copel	192.168.253.26/30	2001:db8:8000:fffd::14/127
LOPES	ether1-copel	192.168.253.30/30	2001:db8:8000:fffd::16/127
JARARACA	ether1-copel	192.168.253.34/30	2001:db8:8000:fffd::18/127
COCITO	ether1-levis	192.168.253.18/30	2001:db8:8000:fffd::10/127
INTERNO	ether1-core	192.168.253.14/30	2001:db8:8000:fffd::8/127

Fonte: Autoria Própria

3.3 CONFIGURAÇÃO DO BGP4

Para uma rede ser conectada na Internet, pode-se fazê-lo de duas formas. A mais comum para empresas e consumidores domésticos: a rede ou endereço é fornecida por algum provedor de conexão. Na segunda forma, a empresa é possuidora de um bloco de endereços e deve divulgá-lo para a Internet. Essa divulgação é realizada através do BGP (TANENBAUM 2011).

O BGP é o protocolo chave da Internet para prover conexão entre redes de domínios distintos, permitindo ainda a conexão conhecida como *multi-homing* (BURGESS 2009). Essa comunicação acontece recebendo as rotas da Internet e enviando os prefixos alocados para estes AS.

A primeira etapa ao se configurar o BGP é, portanto, estabelecer a comunicação entre os dois ASs. Normalmente o provedor de conexão fornece um endereço IP para o estabelecimento desse enlace.

Para configurar o BGP, é igualmente necessário a configuração de filtros, nomeados na literatura como *filter lists*, *distribute-lists* e ainda *prefix-lists*. Eles são utilizados para permitir a entrada de rotas desejadas, bloquear as indesejadas, e permitir a publicação dos prefixos do AS.

Uma parte importante na comunicação entre ASs, é bloquear o recebimento de prefixos *bogons*[15]. Esses endereços são os blocos de IPs válidos e públicos ainda não liberados pelos RIRs. Por se tratarem de endereços válidos, eles podem ser utilizados em ataques maliciosos, como o *spoofing*. Para proteger a rede, uma forma eficaz é a de desviar todos os prefixos *bogons* para um buraco negro. Em rede é o mesmo que jogar qualquer tentativa de comunicação com origem ou destino desses endereços para um beco sem saída, de forma que não ocorram tráfego desses prefixos (EquipeBCP 2012).

Existe uma entidade sem fins lucrativos conhecida como *Team CYMRU*[16] que realiza um trabalho sólido e consistente, bastante adotado e recomendado como boa prática, catalogando esses endereços *bogons*, e os distribuindo através de uma sessão BGP. Com os endereços recebidos, basta marcar esses prefixos para serem redirecionados para o buraco negro (CEREZO e GARCIA 2008). No caso do IPv6 a única rede que é alocada e disponível para roteamento por enquanto é a 2000::/3, equivalente a 13% do total de redes disponíveis (DEERING, HINDEN e NORDMARK 2003).

Outra boa prática é filtrar redes que não devem ser roteadas (BLANCHET, Special-Use IPv6 Addresses 2008). Entre elas estão:

- ::1/128;
- ::/128;
- ::FFFF:0:0/96;
- FE80::/10;
- FC00::/7;
- 2001:db8::/32;
- 2001:10::/28;
- ::/0;
- FF00::/8.

[15] Prefixos *Bogons* são normalmente definidos como prefixos IP que nunca deveria aparecer na tabela de roteamento da Internet, mas que acabam sendo roteados (VAIDYANATHAN, et al. 2012). Esses prefixos são constituídos pelos endereços ainda não alocados pelos RIRs, endereços de uso privado, e endereços reservados que não devem ser roteados.

[16] A Team CYMRU é uma organização sem fins lucrativos, estabelecida em Illinois, Estados Unidos. É custeada por grandes empresas que operam na infraestrutura da Internet. Mais informações podem ser obtidas no site deles: http://www.team-cymru.org/

Uma outra configuração que deve ser pensada é sobre como serão realizadas as sessões BGP. Tecnicamente é possível transferir prefixos IPv4 em sessões IPv6 e vice-versa. Inclusive uma boa prática, recomendada em cenários onde o BGP é configurado como IGP (SANTOS et al. 2010). Mas quando se trata de sessões de EGP, as boas práticas recomendam que o BGP envie a informação de *Next-Hop*, para o próximo roteador (BEIJNUM 2006). Portanto devemos separar os prefixos, trocando IPv4 via sessão IPv4 e o IPv6 via sessão IPv6. Na configuração proposta, não será utilizado o BGP como IGP.

3.4 CONFIGURAÇÃO DO OSPFV3

O OSPF será o protocolo utilizado para troca prefixos dentro da rede interna. Como na configuração proposta as comunicações se darão através de instâncias distintas, serão necessárias duas configurações. O IPv4 vai continuar sendo trocado via OSPFv2, e o IPv6 via OSPFv3.

Ao configurar a troca de prefixos, o OSPF permite alguma flexibilidade. Ele permite que as rotas a serem redistribuídas possam ser de uma das opções, ou de uma combinação delas: rota padrão, conectadas, estáticas, rotas *Routing Information Protocol* (RIP), rotas BGP e rotas OSPF de outras áreas (GREEN e SMITH 2002). Na versão 2 ainda é possível declarar sub-redes específicas para serem publicadas via OSPF, mas isso não acontece na versão 3 do OSPF.

Portanto o OSPFv3 será configurado para redistribuir as rotas conectadas, que são as rotas fornecidas a partir do roteador, para os equipamentos diretamente conectados.

O roteador principal, identificado nessa rede como CORE, será o único que redistribuirá a rota padrão. Dessa forma somente esse roteador terá a tabela completa de roteamento, recebida via BGP. Todos os outros roteadores da rede recebem apenas a rota padrão e compartilham as rotas do OSPF. Portanto todos os roteadores da rede recebem as rotas de outros roteadores conectados, mas não a tabela completa. Dessa forma a tabela de roteamento fica mais enxuta e otimizada.

3.5 CONFIGURAÇÃO DO DNS AUTORITATIVO

Os servidores de DNS autoritativo tem um papel imprescindível na rede, pois sãoeles que permitem que os servidores sejam encontrados. Sejam eles o de hospedagem e ou os próprios servidores de DNS. O servidor DNS autoritativo responderá ao domínio "*example.com*". Dessa forma essa configuração pode ser replicada para qualquer domínio.

Nessa rede, por questão de confiabilidade, serão configurados dois servidores distintos, um como principal, e um escravo. Optou-se pela implementação da *Internet Systems Consortium* (ISC) conhecido como *Berkeley Internet Name Domain* (*BIND*). Ele já existe desde os anos 80, possui um código bastante maduro, e possui um desempenho muito bom, apesar de apresentar uma complexidade de configuração maior que outras opções disponíveis.

Para que o *BIND* responda a consultas no endereço IPv6, é necessário ativar a opção "*listen-on-v6 { any; };*" no arquivo *named.conf.options*.

3.6 CONFIGURAÇÃO DO DNS RECURSIVO

O DNS recursivo é efetivamente utilizado pelos clientes na conversão dos domínios nos IPs. Eles são configurados na rede local, de forma a se ter controle sobre eles, confiabilidade e velocidade nas consultas dos servidores. Ao manter um servidor de DNS recursivo na rede dos clientes, mantém-se uma baixa latência nas consultas.

Os servidores devem ser protegidos no *firewall* contra consultas externas, para evitar ataques e desperdício de recursos. Eles serão configurados com ambos os endereços, IPv4 e IPv6, respondendo a ambas consultas IPv4 e IPv6 também. Uma requisição realizada ao servidor deve obter e encaminhar os registros do tipo A e AAAA, independente da versão do protocolo, pela qual ela seja realizada.

Apesar da implementação de servidor DNS do *Internet Systems Consortium* (*ISC) BIND* oferecer suporte as consultas recursivas e autoritativas, ele envolve muitas configurações adicionais. Por uma questão de desempenho e confiabilidade, optou-se por servidores distintos para os dois tipos de consulta. Para o servidor recursivo foi escolhido o *Unbound*, mantido pela NL Net Labs, pela facilidade de

configuração, excelente desempenho nas consultas, e que tende a dar uma resposta, mesmo que tardia, diferente de outras implementações que muitas vezes simplesmente não oferecem nenhuma resposta caso esta demore muito tempo (algo com maior que 500ms) (BOULAKHRIF 2015).

A configuração do *Unbound* foi realizada de forma muitos simples e rápida. Mas exige a configuração de duas opções específicas para habilitar as respostas a consultas no endereço IPv6 do servidor. São elas:

- interface: ::0
- do-ip6: yes

Além disso, por questões de segurança, foram limitadas as consultas recursivas aos DNS apenas aos endereços da rede. Para tal é utilizado o recurso de Listas de Acesso (*access-list*), conforme pode ser verificado no Apêndice A.

3.7 CONFIGURAÇÃO DA AUTENTICAÇÃO DE CLIENTES

A configuração dos clientes se dá em duas etapas. Na primeira se fornece um endereço, por SLAAC para fornecer os endereços da WAN dos equipamentos dos clientes, normalmente denominados *Customer Premises Equipment* (CPE). Na segunda é encaminhando um prefixo /64 através do *Dynamic Host Configuration Protocol version 6 – Prefix Delegation* (DHCPv6-PD), para a distribuição dos endereços IPv6 para a LAN dos equipamentos.

A opção por essa configuração, se deve ao fato de não acarretar impacto na rede e nas configurações já utilizadas nos equipamentos. Mas em configurações a partir do zero, deve-se considerar a adoção de DHCPv6 *Statefull* para a atribuição da WAN das CPEs, e DHCPv6-PD para a LAN (MORALES 2014).

Os equipamentos utilizados no provedor em questão já dão suporte ao IPv6, sejam eles da *Mikrotik*[17] ou da *Ubiquiti*[18], fabricantes costumeiramente adotados em pequenos e médios provedores de Internet no Brasil.

---

[17] O *RouterOS* da Mikrotik apresenta suporte desde a versão 3.0*beta*10, a partir de 30 de setembro de 2004. Changelog do firmware disponível em: http://forum.routerboard.com/viewtopic.php?f=1&t=16904

[18] O *AirOS V* da *Ubiquiti* passou a suportar o IPv6 na versão 5.6.1, de 3 de julho de 2015. Maiores informações em: http://dl.ubnt.com/firmwares/XN-fw/v5.6.1/changelog.txt

4 RESULTADOS

Com tudo configurado, puderam ser realizados os testes da rede. Foi realizado um levantamento das tabelas de roteamento do roteador principal, das rotas do IGP (OSPF), e de *traceroute* e conectividade dos endereços IPv6. Todos os testes foram realizados com os endereços reais, e se encontram aqui trocados pelos endereços de documentação, apenas por fim de registro e proteção da rede onde foram realizados os testes.

Para os testes, foi utilizado um servidor de virtualização, onde os serviços de DNS e hospedagem rodam. O servidor é gerenciado pela rede local do roteador NC-Interno. Também está conectada no roteador CORE, para conexão das máquinas virtuais. Possui endereçamento IPv4 e IPv6, e roda o sistema operacional Ubuntu 14.04.5 LTS em 64 *bits*.

4.1 TABELAS DE ROTEAMENTO BGP

O primeiro quesito que foi verificado, para confirmar se a rede obteve a conectividade IPv6 é a contagem de rotas da tabela de roteamento do BGP.

Figura 7 - Tabela de Rotas do BGP

```
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.30.4 (c) 1999-2015       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[admin@NC-CORE-CCR1016] > system clock print
                  time: 00:39:27
                  date: nov/07/2016
  time-zone-autodetect: no
        time-zone-name: America/Sao_Paulo
            gmt-offset: -02:00
           dst-active: yes
[admin@NC-CORE-CCR1016] > ipv6 route print count-only where bgp=yes
33743
[admin@NC-CORE-CCR1016] > ip route print count-only where bgp=yes
622597
```

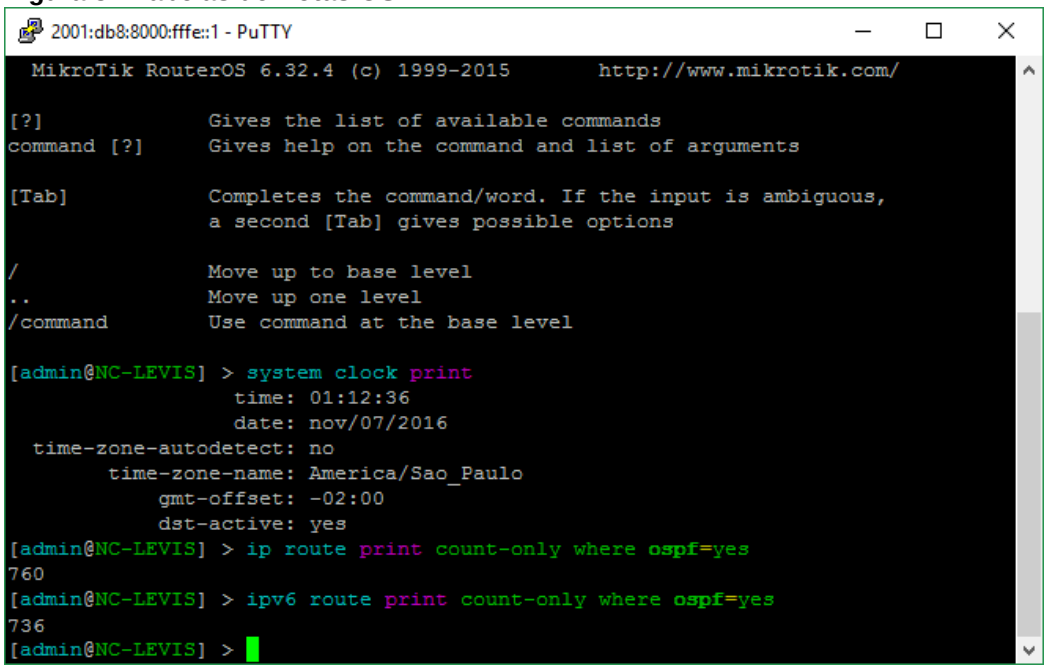
Fonte: Autoria Própria

A Figura 7 apresenta a quantidade de rotas constantes na *Forward Information Base* (FIB) do equipamento. Esta tabela possui as rotas que estão efetivas n o equipamento. Nela é possível ver a diferença entre os Sistemas Autônomos conectados via IPv4 e IPv6. Isso também comprova que a configuração BGP está funcional e ativa.

4.2 TABELAS DE ROTEAMENTO OSPF

A tabela do OSPF permitiu verificar a conexão entre os roteadores internos do provedor. O resultado da contagem dos prefixos IPv4 e IPv5OSPF é apresentado Figura 8 nessas tabelas.

Figura 8 - Tabelas de Rotas OSPF



Fonte: Autoria Própria.

Os dados apresentados pela contagem são constituído pelo total de rotas internas da rede, somando os clientes conectados mais as rotas dos roteadores.. Esse número oscila conforme o horário do dia, visto que a quantidade de clientes conectados também oscila.

Isso possibilita conexão entre todos os nós da rede. Com a possibilidade de mais de uma rota para os roteadores mais importantes da rede, ganha-se em

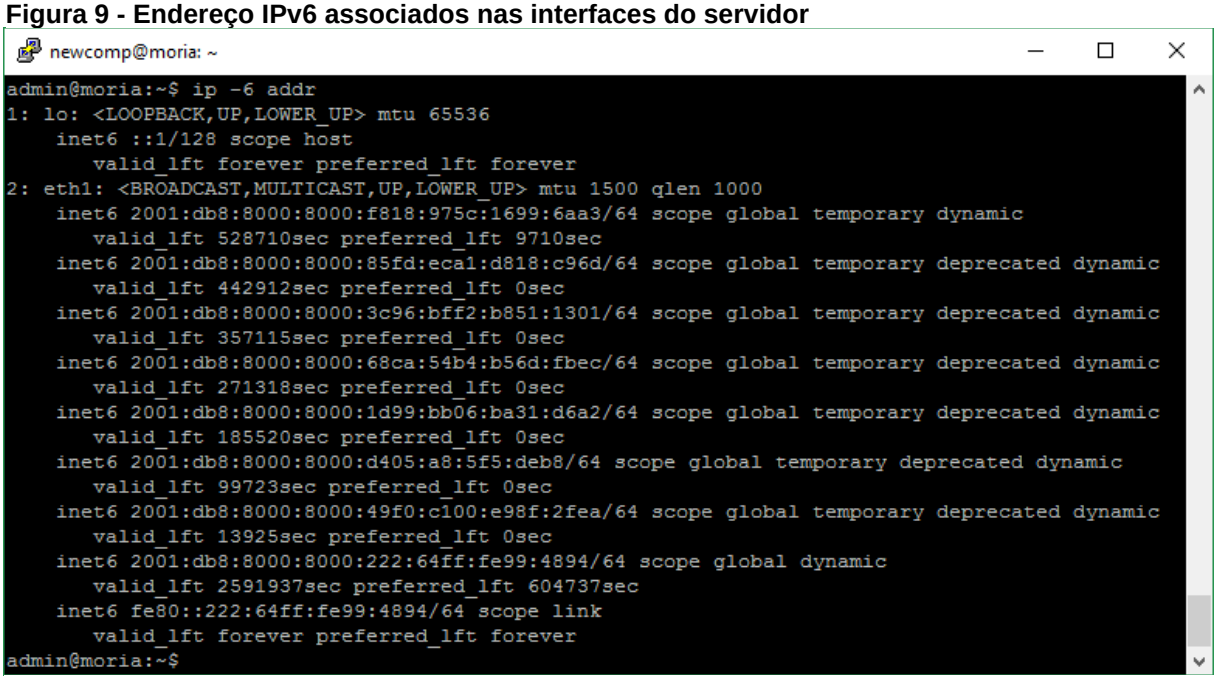
segurança. Esse arranjo permite uma redundância, com o equipamento podendo ser alcançado por múltiplos caminhos.

4.3 ENDEREÇAMENTO IPV4 E IPV6

Na aquisição dos endereços, percebeu-se algumas diferenças. Enquanto o DNS IPv4 fornece somente um endereço por *host*, o IPv6 fornece um endereço por interface. Como este servidor é um servidor de virtualização, existem muitas interfaces criadas para comunicação das máquinas virtuais. Cada uma delas aloca um endereço IPv6 diferente.

Isso por si só gera uma mudança no quesito segurança. Enquanto o IPv4 é uma rede mascarada, protegida por um *firewall* e não possui conectividade fim-a-fim, os endereços IPv6 permitem a conexão direta e com isso exige-se um cuidado maior com a segurança.

Figura 9 - Endereço IPv6 associados nas interfaces do servidor

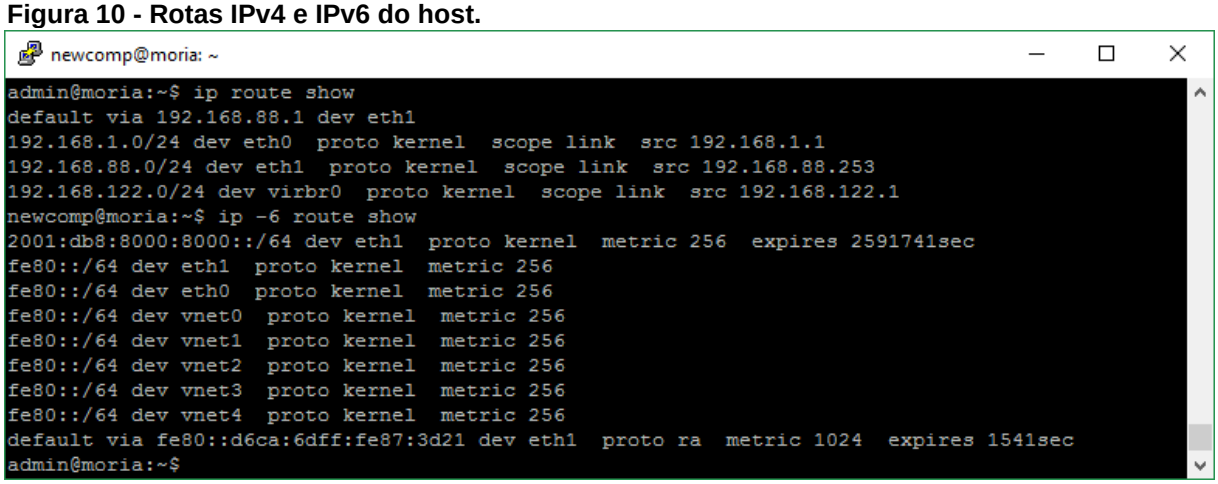


Fonte: Autoria Própria

Pode-se ver uma grande quantidade de endereços temporários criados na Figura 9, associados na interface física principal. Além dessa interface física, que recebe dois endereços, a interface do tipo *bridge*, criada junto com as máquinas virtuais, recebe um endereço IPv6 na interface física. Este servidor se torna acessível à partir da Internet por todos os endereços disponíveis. É possível notar também o

endereço *link-local*, por onde toda a comunicação efetiva da rede costuma acontecer. Mesmo quando se comunicam entre os endereços públicos, se os pacotes forem analisados, percebe-se que o endereço anexado aos pacotes, nos enlaces locais, é esse endereço *link-local*. Isso pode ser visto através das rotas do *host*, como apresentado pela Figura 10.

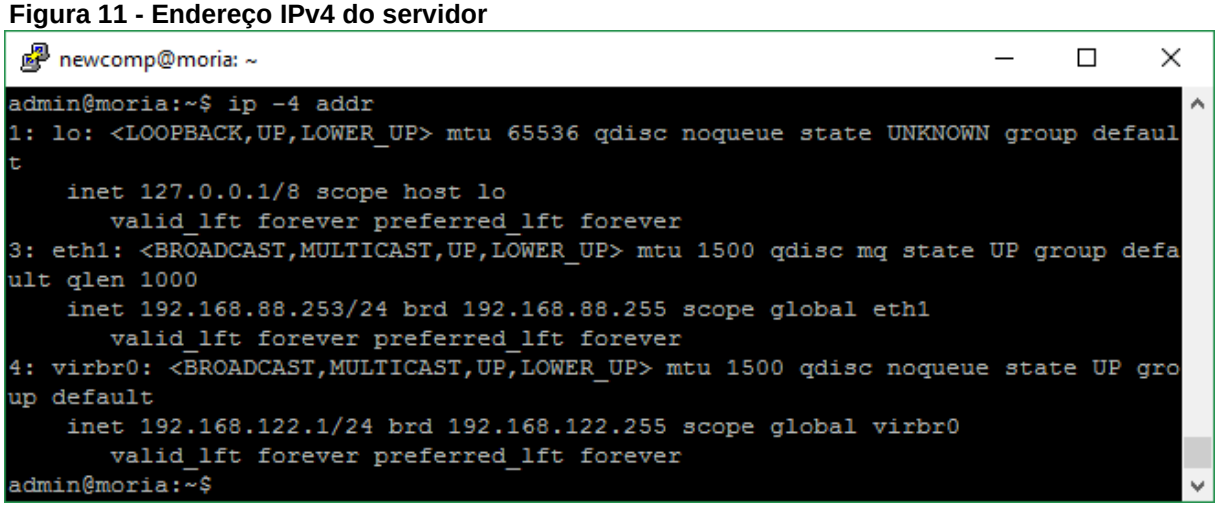
Figura 10 - Rotas IPv4 e IPv6 do host.



Fonte: Autoria Própria.

Já a Figura 11 apresenta os endereços IPv4 associados as mesmas interfaces anteriores. É notável a diferença na quantidade de endereços associados, em virtude da forma bastante diferente que os dois protocolos atuam.

Figura 11 - Endereço IPv4 do servidor



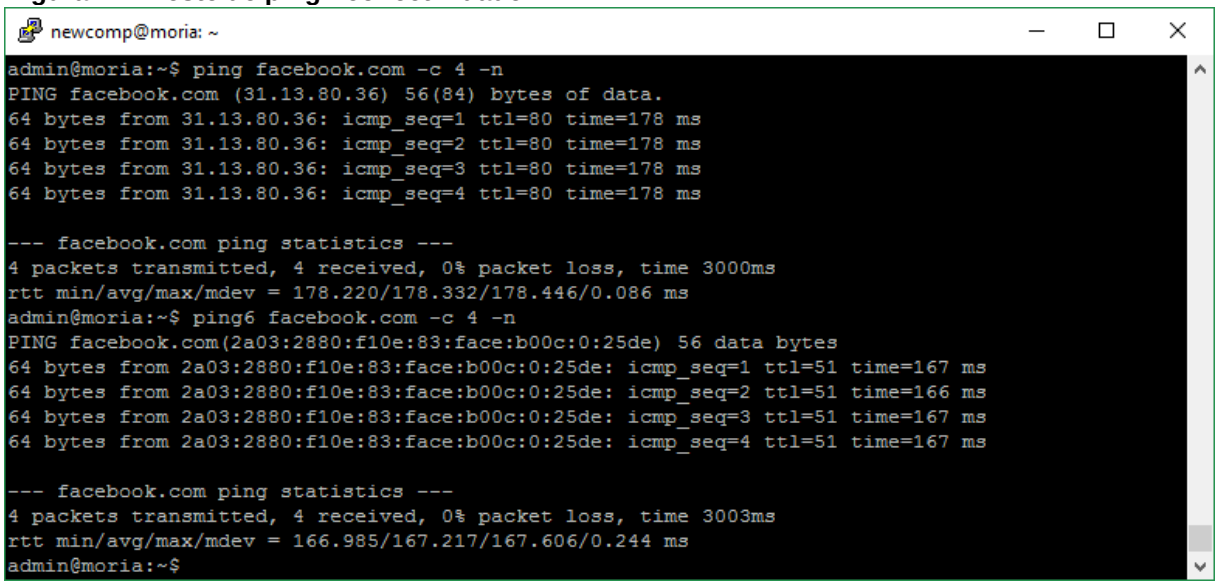
Fonte: Autoria Própria.

4.4 TESTE DE CONECTIVIDADE – *PING*

O teste de *ping* é apenas um teste básico de conectividade entre dois pontos da rede. Ele não informa muito mais que a latência existente no enlace, não fornecendo nenhum dado para identificar porque a rede está funcionando bem ou não.

Na Figura 12 é possível visualizar o resultado do teste de *ping* para o endereço *facebook.com*, tanto em IPv4 como em IPv6, e assim comparar o resultado. É possível através dele verificar que a latência entre os dois testes é diferente e, portanto, percorreram rotas diferentes.

Figura 12 - Teste de ping - conectividade.

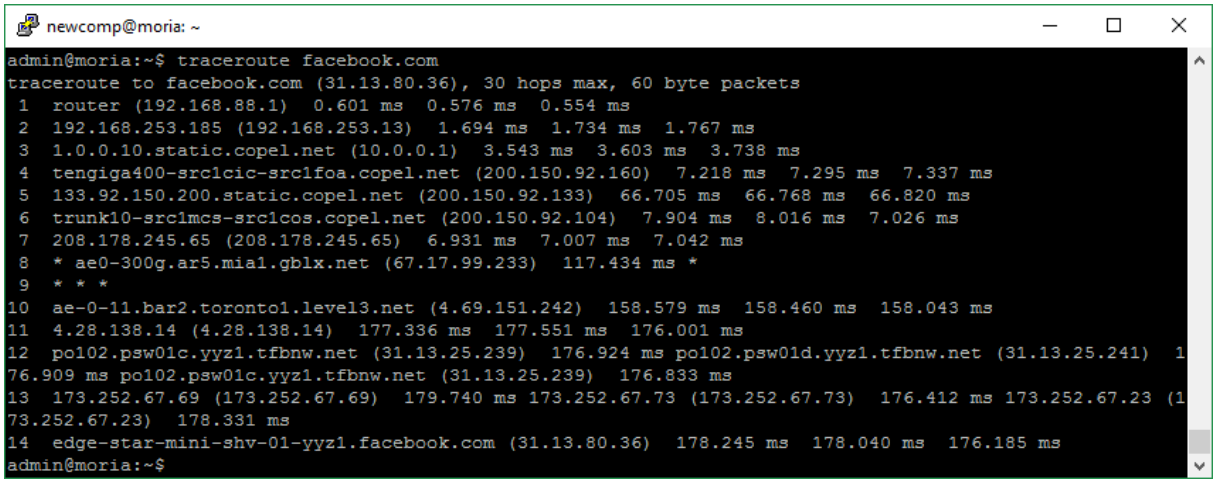


Fonte: Autoria Própria

4.5 TRACEROUTE

O teste do *traceroute* vai mostrar o caminho percorrido entre dois nós da internet. Reafirmando que o endereço IPv4 é mascarado, e o IPv6 é público, e muitas vezes eles podem percorrer rotas diferentes. Em primeiro lugar, na Figura 14 está o teste de *traceroute* para o *facebook.com*, através dos endereços IPv4.

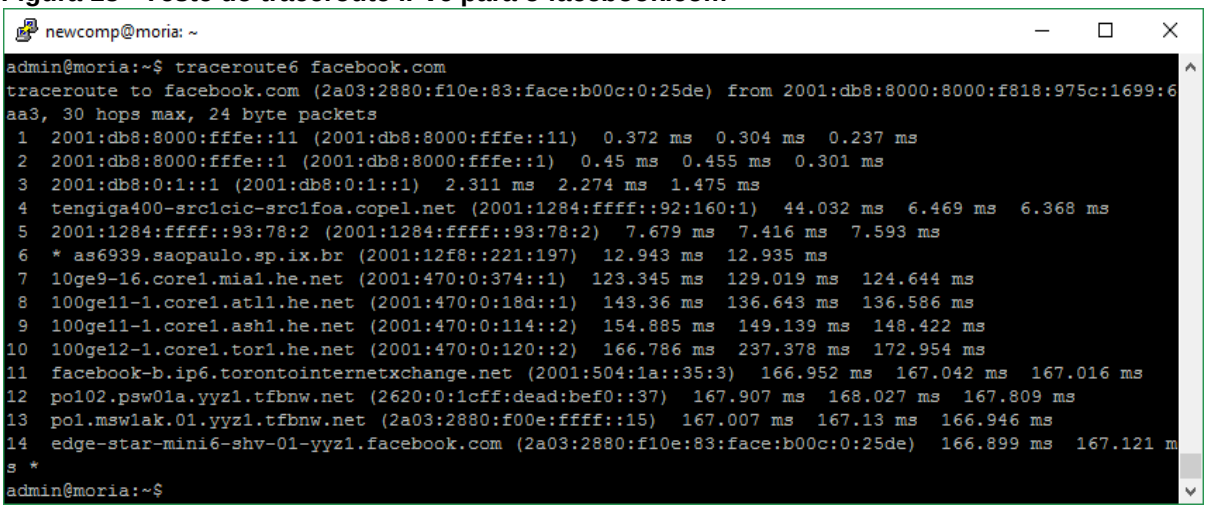
Figura 14 - Teste do *traceroute* IPv4 para o facebook.com



Fonte: Autoria Própria

Já a Figura 13 demostra o teste para o mesmo site, mas desta vez através do endereço IPv6. Comparando os dois testes, é possível ver que via IPv4, o transporte está acontecendo via *Global Crossing/Level 3*, logo após sair da Copel. Já via IPv6, o transporte sai através da rede da *Hurricane Eletric*, logo após passar pelo Ponto de Troca de Tráfego (PTT) de São Paulo.

Figura 13 - Teste do traceroute IPv6 para o facebook.com



Fonte: Autoria Própria.

4.6 CONSULTAS DNS

Para realizar o teste com o DNS, utilizou-se a ferramenta (*domain information groper*) *dig*. Ela é bastante difundida nos ambientes *Unix* e GNU/*Linux*, e junto com a ferramenta *nslookup* são as mais utilizadas para testes de consultas DNS.

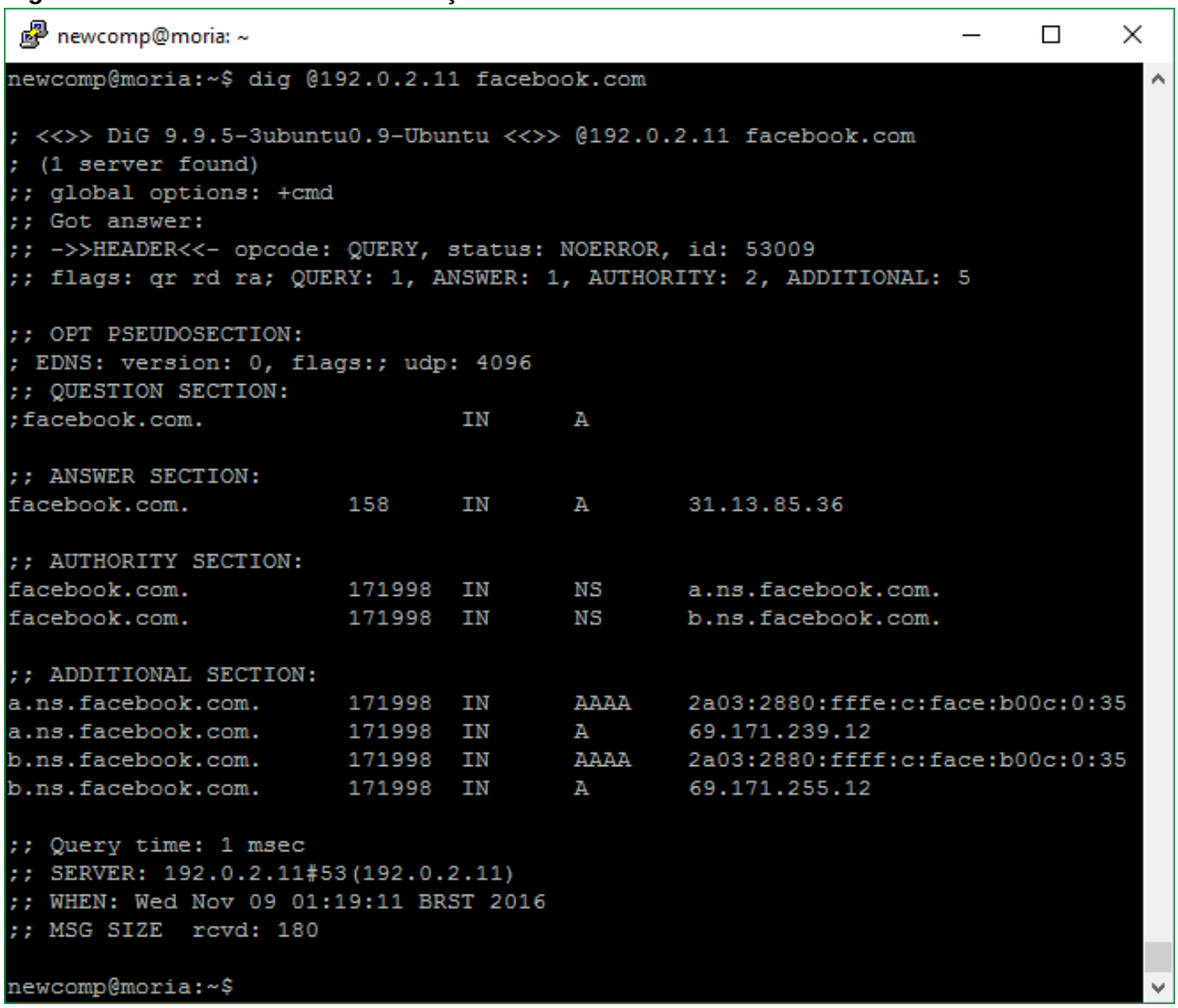
A opção pelo *dig* se dá apenas por ela ser uma ferramenta mais atual, com bom suporte a todos as operações que serão testadas. Com o *dig* pode ser definido o servidor que quer ser testado, o endereço a ser consultado, função conhecida pelo termo inglês *query*, e os tipos de registros que serão buscados.

Neste teste fora realizada uma consulta simples, sem especificação de tipo de registro, a um dos servidores DNS configurados para respostas recursivas, utilizando o *unbound*. O servidor consultado foram os de endereços IPv4 192.0.2.11 e IPv6 2001:db8:8000:ffff::11.

O comando utilizado para realizar a consulta é o:

- dig @endereço_servidor endereço_a_ser_consultado

Figura 15 - Consulta DNS no endereço IPv4



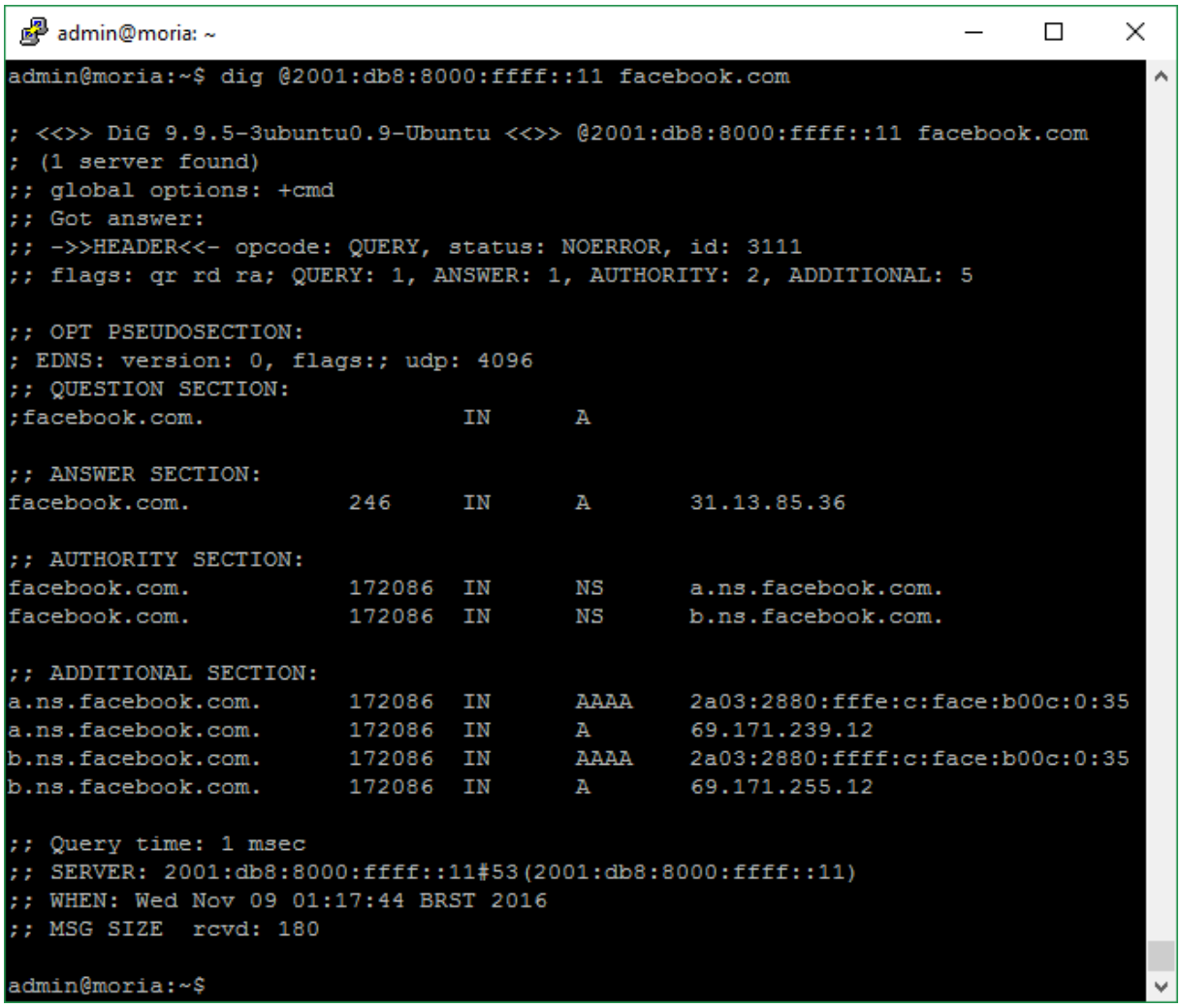
Fonte: Autoria Própria

A Figura 15 apresenta a consulta no endereço IPv4 do *server1*, e o resultado dessa consulta. Mesmo utilizando o *dig* apenas no endereço IPv4, o servidor responder com ambos os registros:

- A = 69.171.239.12;
- AAAA = 2a03:2880:ffff:c:face:b00c:0:35.

Já na Figura 16 testou-se o endereço IPv6 do servidor. Como é possível ver na resposta, ela é exatamente igual a outra consulta. O que é o resultado esperado, independente da consulta chegar pelo Ipv4 ou IPv6, deve produzir a mesma resposta.

Figura 16 - Consulta DNS no endereço IPv6



Fonte: Autoria Própria

4.7 NAVEGAÇÃO WEB

Foi realizado um teste básico de navegação, do computador, e todos os sites funcionaram satisfatoriamente, com apenas uma exceção. Foram testados o UOL, o *Facebook*, o *Web Whatsapp*, Banco do Brasil e o *Youtube*.

O único site que apresentou alguma inconsistência foi o *Youtube*. Alguns vídeos apresentavam a mensagem de que tem a reprodução restrita, quando executados via IPv6. Utilizando duas ferramentas de consulta distintas, Maxmind GeoIP2[19] e a Geo IP Tool[20], é possível notar que alguns serviços identificam a origem da comunicação IPv6 a partir de uma localização incorreta. Por isso o mesmo vídeo ao ser tocado com somente IPv4 na rede, funcionava normalmente. É possível ver essa discrepância através das Figura 17 e Figura 18.

Figura 17 - Teste realizado na ferramenta Maxmind GeoIP2

Endereço IP	Código do país	Localização	Código postal	Coordenadas aproximadas*	Raio de precisão	ISP	Organização	Domínio	Código metropolitano
2001:db8:ffff:ffff::1	BR	Brasil, América do Sul		-10, -55	100	Example Co.	Example Co.		

Fonte: Maxmind GeoIP2

Figura 18 - Teste realizado na ferramenta Geo IP Tool

Fonte: Geo IP Tool

[19] *Maxmind GeoIP2* está disponível em: https://www.maxmind.com/pt/geoip-demo
[20] *Geo IP Tool* pode ser acessada a partir de https://geoiptool.com/

O site do Banco do Brasil apesar de ser acessível via IPv6, não permite o acesso a conta através de IPv6, somente por IPv4. Essa constatação ocorreu ao realizar a captura de pacotes da rede, durante a comunicação com o Banco do Brasil.

5 CONSIDERAÇÕES FINAIS

Através das mudanças rápidas que tem acontecido no campo de redes de computadores, atualmente, pode-se entender a crescente relevância que as redes IPv6 vem proporcionando. Em um ambiente de esgotamento crescente de endereços IPv4, e um mercado consumidor cada vez maior, ela se torna imprescindível. Atualmente vive-se em um mundo de conexões móveis crescendo exponencialmente, não somente através dos celulares, mas também em *tablets*, Internet embarcada em automóveis e a Internet das Coisas, normalmente conhecida como *Internet of Things* (IoT), onde aparelhos diversos dentro das casas e trabalhos se conectarão a rede fornecendo e consumindo *Web Services* (LEE e LEE 2015).

O mercado consumidor formal, também tem se expandido, através de conexões cada vez mais rápidas e relevantes, mesmo em cidades pequenas, onde empresários locais costumam usar uma tecnologia atual, antes mesmo das grandes operadoras. A Anatel tem adotado políticas de expansão, visando não somente as grandes operadoras, mas também os pequenos e médios provedores regionais, que tem desde os idos dos anos 2000, implementado e operado redes de telecomunicações cada vez mais amplas (CGI.BR 2016).

No caso do estudo, um provedor com 900 conexões em uma cidade de pouco mais de 16000 habitantes (IBGE 2016), significa uma penetração de pouco mais de 20% das famílias locais.

Não somente os pequenos e médios empresários vem sofrendo com a ausência de endereços, como as grandes operadoras também. Isso tem limitado a expansão dos serviços em alguns casos, ou a adoção de equipamentos e soluções cada vez mais custosas para ampliar a vida do IPv4, como acontece com a adoção cada vez maior de CGNATs.

A solução imediata, de longo prazo, de menor custo na questão de equipamentos, pois a grande maioria dos equipamentos de rede já prove suporte, é a implementação efetiva do IPv6.

Apesar de experimentar alguns problemas menores conforme o teste constatou, como o acesso ao *Youtube*, que ainda não é reconhecido como na origem sendo o Brasil. É algo temporário, que há de ser reparado.

Neste sentido a proposta foi realizada, visto que uma rede que comunicava unicamente em IPv4, foi transformada em uma rede pilha dupla, com comunicação

transparente ao usuário, e com total suporte através dos equipamentos de fabricantes diversos.

Entre os serviços de Internet mais utilizados, que ainda não dão suporte pleno, podemos citar o acesso aos bancos. Apesar da maior parte dos sites já suportar, o acesso a área de transação, ainda se dá por IPv4, pelo menos no Brasil (MOREIRAS 2014). Mas a parte de conteúdo jornalístico e de lazer, os sites e serviços oferecidos na Internet já são suportados em IPv6, principalmente os oferecidos pelos grandes provedores de serviço.

Percebe-se também que a documentação apesar de deficiente, tem aumentado e facilitado a implementação do novo protocolo. As entidades que promovem a adoção de IPv6 tem demonstrado cada vez mais novos cenários e testado o suporte pelos equipamentos mais populares.

Entre os pontos que não puderam ser experimentados neste trabalho, e podem fazer parte de um futuro estudo, estão o desempenho nas aplicações de QoS sobre os equipamentos clientes, e um estudo aprofundado de *firewall* para proteção de redes.

REFERÊNCIAS

Anatel. **Dados – Agência Nacional de Telecomunicações**. 2016. Disponível em: <http://www. anatel.gov.br/dados/2015-02-04-18-32-09>. Acessado em: 6 novembro 2016.

AEPPEL, T. ***It Took the Telephone 75 Years To Do What Angry Birds Did in 35 Days. But What Does That Mean*?** Wallstreet Journal, 13 de março de 2015. Disponível em: <http://blogs.wsj.com/economics /2015/03/13/it-took-the-telephone-75-years-to-do-what-angry-birds-did-in-35-days-but-what-does-that-mean/>. Acessado em: 20 novembro 2016.

BEIJNUM, I. V. **Running IPv6. A practical guide to configuring IPv6 for Windows XP, MacOS X, FreeBSD, Red Hat Linux, Cisco routers, DNS and BIND, Zebra, and Apache 2**. 1. ed. Berkeley: Apress, 2006.

BLANCHET, M. **A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block**. Disponível em: <https://tools.ietf.org/html/rfc3531>. Acessado em: 16 setembro 2016.

BLANCHET, M. **Special-Use IPv6 Address**. Disponível em: <https://tools.ietf.org /html/rfc5156>. Acessado em: 16 setembro 2016.

BONEY, J. **Cisco IOS in a Nutshell, Second Edition**. 2. ed. Sebastopol: O'Reilly Media, 2005.

BOULAKHRIF, H. **Analysis of DNS Resolver Performance Measurements**.13 Julho 2016. Disponível em: <https://www.nlnetlabs.nl/downloads/publications/os3-2015-rp2-hamza-boulakhrif.pdf>. Acessado em: 2 novembro 2016.

BRAGA, J; et al. **O livro do IETF**. 1. Ed. São Paulo: Comitê Gestor da Internet no Brasil, 2014. Disponível em: <http://cgi.br/media/docs/publicacoes/1/o-livro-do-ietf.pdf>. Acessado em: 8 maio 2016.

BURGESS, D. **Learn RouterOS – 2nd Edition**. 2. ed. Estados Unidos: Lulu.com, 2009.

BUSH, V. **As we way think**. The Atlantic Monthly Magazine, 1945. Disponível em: < http://www.ps.uni-saarland.de/~duchier/pub/vbush/vbush.txt>. Acessado em: 24 maio 2016.

CEREZO, J. P.; GARCIA, F. **RIPE Anti-Spoofing Task Force HOW-TO**. Disponível em: <https://www.ripe.net/publications/docs/ripe-431>. Acessado em: 24 setembro 2016.

CERF, V.; et al. **Act One – The Poems**. 1989. Disponível em: <https://tools.ietf.org/html/rfc1121>. Acessado em: 8 maio 2016.

CETIC.BR. **Portal de Dados**. Disponível em: <http://data.cetic.br/cetic/explore>. Acessado em: 6 novembro 2016.

CIOFFI, J.; JAGANNATHAN, S.; LEE, W.; **Digital subscriber line (DSL)**. Scholarpedia, Vol. 3, Número 8, 2008. Disponível em: <http://www.scholarpedia.org/article/Digital_subscriber_line_(DSL)>. Acessado em: 27 novembro 2016.

Cisco System, Inc. **6lab Cisco – The place to monitor IPv6 adoption**. 2016. Disponível em: <http://6lab.cisco.com/stats/cible.php?country=world&option=network>. Acessado em: 22 novembro 2016.

Cisco System, Inc. **Cisco on Cisco Best Practices. Cisco IP Addressing policy**. Disponível em: < http://www.cisco.com/c/dam/en_us/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_IP_Addressing_Best_Practices.pdf>. Acessado em: 16 setembro 2016.

Cisco System, Inc. **IPv6 Configuration Guide, Cisco IOS – Release 15.2MT**. 15. ed. San Jose: Cisco Press, 2012. Disponível em: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6 /configuration/15-2mt/ipv6-15-2mt-book.pdf>. Acessado em: 24 setembro 2016.

COMER, D. E. **Interligação em rede com TCP/IP**. 3. ed. Rio de Janeiro: Campus, 1998.

Comitê Gestor da Internet no Brasil. **TIC Provedores 2014**. Pesquisa sobre o setor de provimento de serviços de Internetno Brasil. ed. São Paulo: CETIC.BR, 2016.

Comitê Gestor da Internet no Brasil. **TIC Domicílios 2015**. Pesquisa Sobre O Uso Das Tecnologias De Informação E Comunicação Nos Domicílios Brasileiros. ed. São Paulo: CETIC.BR, 2016.

Comitê Gestor da Internet no Brasil. **TIC Empresas 2014**. Pesquisa Sobre O Uso Das Tecnologias De Informação E Comunicação Nas Empresas Brasileiras. ed. São Paulo: CETIC.BR, 2015.

Comitê Gestor da Internet no Brasil. **Portal de Dados CETIC.BR**. 2016. Disponível em: <http://data.cetic.br/cetic/explore>. Acessado em: 22 novembro 2016.

COLTUN, R.; FERGUSON, D.; MOY, J. **OSPF for IPv6**. 1999. Disponível em: <https://tools.ietf.org/html/rfc2740>. Acessado em: 22 novembro 2016.

COTTON, M.; VEGODA, L. **Special Use IPv4 Address**. Disponível em: <https:// tools.ietf.org/html/rfc5735>. Acessado em: 19 setembro 2016.

DEERING, S. E.; HINDEN, R. M.; NORDMARK, E. **IPv6 Global Unicast Address Format**. Disponível em: <https://tools.ietf.org/html/rfc3587>. Acessado em: 24 setembro 2016.

DIBONA, C.; OCKMAN, S.; STONE, M. **Open Sources: Voices from the Open Source Revolution**. 1. ed. Sebastopol: O'Reilly Media, 1999.

DROMS, R. **Dynamic Host Configuration Protocol**. 1993. Disponível em: <https:// tools.ietf.org/rfc/rfc1531.txt>. Acessado em: 22 novembro 2016.

EquipeBCP (Best Current Practices). **Entenda a necessidade do Antispoofing**. Disponível em: <http://bcp.nic.br/ entenda-o-antispoofing/>. Acessado em 24 setembro 2016.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

GETSCHKO. D. **8º ISP – ABRINT. Neutralidade como motor de inovação**. Abril 2016. Disponível em: <http://www.abrint.com.br/wordpress/downloads/ apresentacoes/primeiro-dia/demi.ppt>. Acessado em: 6 novembro 2016.

GREEN, B. R.; SMITH, P. **Cisco ISP Essentials**. 1. ed. Indianapolis: Cisco Press, 2002.

HAGEN, S. **IPv6 Essentials, Third Edition**. 3. ed. California: O'Reilly Media, 2014.

HINDEN, R. M.; DEERING, S. E. **IPv6 Multicast Address Assignments**. 1998. Disponível em: <https://tools.ietf.org/html/rfc2375>. Acessado em: 22 novembro 2016.

HOGG, S. **OSPFv3 for IPv4 and IPv6**. 2 setembro 2013. Disponível em: <http://www.networkworld. com/article/2225270/cisco-subnet/ospfv3-for-ipv4-and-ipv6.html>. Acessado em: 12 outubro 2016.

HUSTON, G. **Autonomous System (AS) Number Reservation for Documentation Use**. Disponível em: <https://tools.ietf.org/html/rfc5398>. Acessado em: 16 setembro 2016.

HUSTON, G. **Best Efforts Networking**. 2001. Disponível em: <http://www.potaroo. net/ispcol/2001-09/2001-09-best.pdf>. Acessado em: 22 setembro 2016.

HUSTON, G. **IPv4 Address Report**. Arin, 31 maio 2016. Disponível em: <http:// www.potaroo.net/tools/ipv4/>. Acessado em: 31 maio 2016.

HUSTON, G.; LORD, A.; SMITH, P. **IPv6 Address Prefix Reserved for Documentation**. Disponível em: <https://tools.ietf.org/html/rfc3849>. Acessado em: 19 setembro 2016.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Disponível em: <http://cidades.ibge.gov.br/xtras/perfil.php?codmun=410290>. Acessado em: 22 novembro 2016.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**. 5. ed. São Paulo: Pearson Education do Brasil, 2010.

LAMMLE, T. **CCNA: Cisco Certified Network Associate study guide**. 7. ed. Indianapolis: Wiley Publishing, 2011.

LEE, I.; LEE, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. **Bussiness Horizons**.v. 58, i. 4, p. 431-440, jul/ago. 2015.

MOLLOY, M. Test focuses spotlight on interoperability of routers. **Network World The Newsweekly of Enterprise Network Strategies**, Framingham (Mass.), v. 9, n. 38, p. 1, 10, 12, 88, set. 1992.

MORALES, E. B. **IPv6 na última milha com PPPoE – minitutorial**. Nic.br, 2014. 1 vídeo do youtube (41m37s). Disponível em: <https://www.youtube.com/watch?v= nfTUWtRUE8k>. Acessado em: 2 novembro 2016.

MOREIRAS, A. M. **IPv6, um desafio técnico para a Internet**. Revista CIO. 4 fevereiro 2015. Disponível em: <http://cio.com.br/tecnologia/2014/02/04/ipv6-um-desafio-tecnico-para-a-internet/>. Acessando em: 22 novembro 2016.

MOREIRAS, A. M.; et al. **Laboratório de IPv6 [livro eletrônico].** São Paulo: Novatec Editora, 2015. Disponível em: <http://ipv6.br/media/arquivo/ipv6/file/64/livro-lab-ipv6-nicbr.pdf>. Acessado em: 8 maio 2016. (SANTOS e al., Apostila - IPv6 Básico 2012)

NELSON, R. **Pokémon GO Hit 50 Million Downloads in Record Time, Now at More Than 75 Million Worldwide**. Disponível em: < https://sensortower.com/blog/ pokemon-go-50-million-downloads>. Acessado em: 20 novembro 2016.

NELSON, T. **Project Xanadu**. 1960. Disponível em: <http://www.xanadu.net/>. Acessado em: 24 maio 2016.

PATARA. R. **Situação dos Recursos de Numeração IPv4 e IPv6**. VI Forum IPv6. 2015. Disponível em: <http://ipv6.br/forum/slides/6forumv6-RicardoPatara01.pdf>. Acessado em: 6 novembro 2016.

POSTEL, J. **Internet Protocol: DARPA Internet Program Protocol Specification**. IETF, setembro 1981. Disponível em: <https://tools.ietf.org/rfc/rfc791.txt>. Acessado em: 24 maio 2016.

POSTEL, J. **NCP/TCP Transition Plan**. IETF, novembro 1981.Disponível em: <https://tools.ietf.org/rfc/rfc801.txt>. Acessado em: 24 maio 2016.

ROBERTS, P. World IPv6 Day. **The Internet Protocol Journal**, San Jose (CA), v. 14, n. 1, p. 12-13, março 2011.

SANTOS, R. R. dos. et al. **Apostila - IPv6 Básico**. São Paulo: Núcleo de Informação e Coordenação do ponto BR, 2012. Disponível em: < http://ipv6.br/media/arquivo /ipv6/file/60/ApostilaIPv62012.zip>. Acessado em: 7 agosto 2016.

SANTOS, R. R. dos. et al. **Curso IPv6 Básico**. São Paulo: Núcleo de Informação e Coordenação do ponto BR, 2010. Disponível em: <http://ipv6.nic.br/media/arquivo /ipv6/file/48/IPv6-apostila.pdf>. Acessado em: 31 maio 2016.

STALLINGS, W. **Redes e sistemas de comunicação de dados**. 1. ed. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, A. **Redes de Computadores**. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

WorldOmeters. **World Population by Year**. 2016. Disponível em: <http://www. worldometers.info/world-population/world-population-by-year/>. Acessado em: 22 novembro 2016.

VAIDYANATHAN, R.; GHOSH, A.; SAWAYA, Y.; KUBOTA, A.; **On the use of Enhanced Bogon Lists (EBLs) to detect malicious traffic**. In: International Conference on Computing, Networking and Communications. 2012. Maui: HI. p. 1-6.

APÊNDICE A - Arquivo de configuração dos servidores GNU/Linux

APÊNDICE A

Arquivos referentes ao BIND do servidor dns1.

named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
//    If    you    are    just    adding    zones,    please    do    that    in
/etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

named.conf.local

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
include "/etc/bind/zones.rfc1918";

zone "example.com" {
        type master;
        file "/etc/bind/db.example.com ";
        allow-transfer { 192.0.2.6; };
        also-notify { 192.0.2.7; };
};

zone "2.0.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.2.0.192";
        allow-transfer { 192.0.2.6; };
        also-notify { 192.0.2.7; };
};

zone "100.51.198.in-addr.arpa" in {
        type master;
        file "/etc/bind/db.100.51.198";
```

```
        allow-transfer { 192.0.2.6; };
        also-notify { 192.0.2.7; };
};

zone "113.0.203.in-addr.arpa" in {
        type master;
        file "/etc/bind/db. 113.0.203";
        allow-transfer { 192.0.2.6; };
        also-notify { 192.0.2.7; };
};

zone "8.b.d.0.1.0.0.2.ip6.arpa" in {
        type master;
        file "/etc/bind/db.db8.2001";
        allow-transfer { 192.0.2.6; };
        also-notify { 192.0.2.7; };
};
```

named.conf.options

```
options {
        directory "/var/cache/bind";

        recursion no;
        allow-transfer { 192.0.2.6; };
        notify yes;
        // allow-recursion { 127.0.0.1/8; 192.0.2.0/28; };
        // dnssec-validation auto;
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        //  Uncomment the following block, and insert the addresses
replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
         allow-query { any; };
};
```

db.example.com

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                        2016081001      ; Serial
                            604800      ; Refresh
                             86400      ; Retry
                           2419200      ; Expire
                            604800 )    ; Negative Cache TTL
;
@       IN      NS      dns1.example.com.
@       IN      NS      dns2.example.com.
@       IN      A       192.0.2.9
@       IN      AAAA    2001:db8:ffff:ffff::9
@       IN      MX      5 mx.core.locaweb.com.br.
www     IN      CNAME   example.com.
ftp     IN      CNAME   example.com.
router  IN      A       192.0.2.1
router  IN      AAAA    2001:db8:ffff:ffff::1
ns      IN      A       192.0.2.3
ns      IN      AAAA    2001:db8:ffff:ffff::3
ns2     IN      A       192.0.2.4
ns2     IN      AAAA    2001:db8:ffff:ffff::4
dns1    IN      A       192.0.2.6
dns1    IN      AAAA    2001:db8:ffff:ffff::6
dns2    IN      A       192.0.2.7
dns2    IN      AAAA    2001:db8:ffff:ffff::7
webmail IN      A       192.0.2.10
webmail IN      AAAA    2001:db8:ffff:ffff::10
smtp    IN      CNAME   webmail.example.com.
pop     IN      CNAME   webmail.example.com.
imap    IN      CNAME   webmail.example.com.
spf     IN      CNAME   webmail.example.com.
@       IN      TXT     v=spf1 include:_spf.example.com ?all
```

db.2.0.192

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                        2016060701      ; Serial
```

```
                              604800      ; Refresh
                               86400      ; Retry
                             2419200      ; Expire
                              604800 )    ; Negative Cache TTL
;
@       IN      NS      dns1.example.com.
@       IN      NS      dns2.example.com.
;
1       IN      PTR     router.example.com.
3       IN      PTR     ns.example.com.
4       IN      PTR     ns2.example.com.
6       IN      PTR     dns1.example.com.
7       IN      PTR     dns2.example.com.
9       IN      PTR     rivendell.example.com.
10      IN      PTR     webmail.example.com.
;
$GENERATE 11-255 $ IN PTR $.ips.example.com.
```

db.100.51.198

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                        2016060701      ; Serial
                            604800      ; Refresh
                             86400      ; Retry
                           2419200      ; Expire
                            604800 )    ; Negative Cache TTL
;
@       IN      NS      dns1.example.com.
@       IN      NS      dns2.example.com.
;
$GENERATE 1-255 $ IN PTR $.ips.example.com.
```

db.113.0.203

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                        2016060701      ; Serial
                            604800      ; Refresh
```

```
                              86400      ; Retry
                            2419200      ; Expire
                             604800 )    ; Negative Cache TTL
;
@       IN      NS      dns1.example.com.
@       IN      NS      dns2.example.com.
;
$GENERATE 1-255 $ IN PTR $.ips.example.com.
```

db.db8.2001

```
;
; 2001:db8::/32
;
; Zone file built with the IPv6 Reverse DNS zone builder
; http://rdns6.com/
$ORIGIN 8.b.d.0.1.0.0.2.ip6.arpa.
$TTL 1h ; Default TTL
@       IN      SOA     ns.example.com.      root.example.com. (
                        2016060701      ; serial
                        1h              ; slave refresh interval
                        15m             ; slave retry interval
                        1w              ; slave copy expire time
                        1h              ; NXDOMAIN cache time
                        )

;
; domain name servers
;
@       IN      NS      dns1.example.com.
@       IN      NS      dns2.example.com.

; IPv6 PTR entries
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
router.example.com.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
ns.example.com.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
ns2.example.com.
6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
dns1.example.com.
7.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
dns2.example.com.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
rivendell.example.com.
10.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.f.f          IN          PTR
server1.example.com.
```

Arquivos referentes ao BIND do servidor dns2.

named.conf

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
include "/etc/bind/zones.rfc1918";

zone "example.com" {
        type slave;
        file "/etc/bind/db.example.com ";
        masters { 192.0.2.6; };
};

zone "2.0.192.in-addr.arpa" {
        type slave;
        file "/etc/bind/db.2.0.192";
        masters { 192.0.2.6; };
};

zone "100.51.198.in-addr.arpa" in {
        type slave;
        file "/etc/bind/db.100.51.198";
        masters { 192.0.2.6; };
};

zone "113.0.203.in-addr.arpa" in {
        type slave;
        file "/etc/bind/db. 113.0.203";
        masters { 192.0.2.6; };
};

zone "8.b.d.0.1.0.0.2.ip6.arpa" in {
        type slave;
        file "/etc/bind/db.db8.2001";
        masters { 192.0.2.6; };
};
```

Arquivos referentes ao unbound do servidor ns e ns2.

unbound.conf

```
# Unbound configuration file for Debian.
```

```
#
# See the unbound.conf(5) man page.
#
# See /usr/share/doc/unbound/examples/unbound.conf for a commented
# reference config file.
#
# The following line includes additional configuration files from the
# /etc/unbound/unbound.conf.d directory.
server:
    # The following line will configure unbound to perform cryptographic
    # DNSSEC validation using the root trust anchor.
    verbosity: 1
    auto-trust-anchor-file: "/var/lib/unbound/root.key"
    interface: 192.0.2.3
    interface: 2001:db8:8000:ffff::11
    #no server2 é: interface: 2001:db8:8000:ffff::12
    do-ip6: yes
    access-control: 192.0.2.0/24 allow
    access-control: 198.51.100.0/24 allow
    access-control: 203.0.113.0/24 allow
    access-control: 172.16.0.0/12 allow
    access-control: 192.168.0.0/16 allow
    access-control: 127.0.0.1 allow
    access-control: 2001:db8::/32 allow
    access-control: ::1 allow
    access-control: 0.0.0.0/0 deny
    chroot: ""
    statistics-interval: 0
    extended-statistics: yes
# set to yes if graphing tool needs it
    statistics-cumulative: no
```

APÊNDICE B - Arquivo de configuração dos equipamentos Mikrotik

APÊNDICE B

Configurações referentes ao roteamento dinâmico, e o firewall do roteador de borda Mikrotik, que executa RouterOS.

```
/routing bgp instance
set default as=65550 router-id=192.0.2.1
/routing ospf instance
set [ find default=yes ] distribute-default=always-as-type-1 router-id=\
    192.168.254.254
/routing ospf-v3 instance
set [ find default=yes ] distribute-default=always-as-type-1 \
    redistribute-connected=as-type-1 router-id=192.168.254.254
/routing bgp network
add network=192.0.2.0/24 synchronize=no
add network=198.51.100.0/24 synchronize=no
add network=203.0.113.0/24 synchronize=no
add network=2001:db8::/32 synchronize=no
/routing bgp peer
add address-families=ip in-filter=bgp-in-f1 multihop=yes name=fornecedora1
out-filter=bgp-out-f1   remote-address=10.0.0.1   remote-as=64496   ttl=5
update-source=10.0.0.2
add    address-families=ip,ipv6    in-filter=bgp-in-f1-v6    multihop=yes
name=fornecedora1v6           out-filter=bgp-out-f1-v6           remote-
address=2001:db8:0:1::1       remote-as=64496       ttl=5       update-
source=2001:db8:0:1::2
add address-families=ip in-filter=bgp-in-f2 multihop=yes name=fornecedora2
out-filter=bgp-out-f2  remote-address=10.0.1.1  remote-as=64511  update-
source=10.0.1.2
add  address-families=ip,ipv6  in-filter=bgp-in-f2-v6  multihop=yes  name=
fornecedora2v6  out-filter=bgp-out-f2-v6  remote-address=2001:db8:0:2::1
remote-as=64511 update-source=2001:db8:0:2::2
/routing filter
add action=reject chain=bgp-out-f1 prefix=0.0.0.0/0
add action=accept chain=bgp-out-f1 prefix=192.0.2.0/24
add action=accept chain=bgp-out-f1 prefix=198.51.100.0/24
add action=accept chain=bgp-out-f1 prefix=203.0.113.0/24
add action=accept chain=bgp-out-f1-v6 prefix=2001:db8::/32
add action=accept chain=bgp-in-f1 prefix=0.0.0.0/0
add action=reject chain=bgp-out-f2 prefix=0.0.0.0/0
add action=accept chain=bgp-out-f2 prefix=192.0.2.0/24
add action=accept chain=bgp-out-f2 prefix=198.51.100.0/24
add action=accept chain=bgp-out-f2 prefix=203.0.113.0/24
add action=accept chain=bgp-out-f1-v6 prefix=2001:db8::/32
add action=accept chain=bgp-in-f2 prefix=0.0.0.0/0 set-bgp-local-pref=50 \
    set-bgp-weight=50 set-distance=20
add action=accept chain=bgp-in-copel prefix=::/0 set-bgp-local-pref=50 \
    set-bgp-weight=50 set-distance=20
```

```
add action=discard chain=bgp-in-copel disabled=yes prefix=0.0.0.0/0 \
    set-bgp-local-pref=50 set-bgp-weight=50 set-distance=21
/routing ospf interface
add network-type=broadcast passive=yes priority=0
add interface=ether4-levis network-type=point-to-point
add interface=ether5-copel network-type=point-to-point
add interface=ether3-claus network-type=point-to-point
add interface=ether10-lan-loja network-type=broadcast
/routing ospf nbma-neighbor
add address=192.168.254.2 priority=1
add address=192.168.253.228 priority=1
add address=192.168.253.186 priority=1
add address=192.168.253.236 priority=1
/routing ospf network
add area=backbone network=200.150.115.64/27
add area=backbone network=192.168.254.0/24
add area=backbone network=192.168.249.0/29
add area=backbone network=192.168.250.0/29
add area=backbone network=192.168.253.0/24
add area=backbone network=192.168.0.0/24
add area=backbone network=189.85.19.192/28
add area=backbone disabled=yes network=192.168.253.224/29
add area=backbone network=192.168.252.0/24
add area=backbone network=192.168.120.0/24
add area=backbone disabled=yes network=192.168.253.232/29
add area=backbone network=200.71.116.0/22
/routing ospf-v3 interface
add area=backbone passive=yes
add area=backbone interface=ether3-claus network-type=point-to-point
add area=backbone interface=ether4-levis network-type=broadcast
add area=backbone interface=ether5-copel network-type=point-to-point
add area=backbone interface=ether10-lan-loja network-type=broadcast
/ipv6 firewall address-list
add address=2804:14d:4681:13db:29b9:1465:8ab0:3b62/128 list=acessoremoto
/ipv6 firewall filter
add chain=input src-address=::1/128
add chain=forward src-address=::1/128
add chain=forward dst-address=2804:1954::/32 src-address-list=acessoremoto
add action=add-src-to-address-list address-list="port scanners" address-
list-timeout=2w chain=input comment="NMAP FIN Stealth scan" protocol=tcp
tcp-flags=\
    fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" address-
list-timeout=2w chain=input comment="SYN/FIN scan" protocol=tcp tcp-
flags=fin,syn
add action=add-src-to-address-list address-list="port scanners" address-
list-timeout=2w chain=input comment="SYN/RST scan" protocol=tcp tcp-
flags=syn,rst
```

```
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input comment="FIN/PSH/URG scan" protocol=tcp tcp-flags=\
    fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input comment="ALL/ALL scan" protocol=tcp tcp-flags=\
    fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input comment="NMAP NULL scan" protocol=tcp tcp-flags=\
    !fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input comment="SSH que n\E3o \E9 dos nossos ips" dst-port=\
    21,23,3306 protocol=tcp src-address-list=!acessoremoto
add action=drop chain="Illegal Address" comment="DROP de endere\E7os BOGONS e depreciados" disabled=yes src-address=2001:db8::/32
add action=drop chain="Illegal Address" src-address=::/96
add action=drop chain="Illegal Address" src-address=::224.0.0.0/100
add action=drop chain="Illegal Address" src-address=::127.0.0.0/104
add action=drop chain="Illegal Address" src-address=::/104
add action=drop chain="Illegal Address" src-address=::255.0.0.0/104
add action=drop chain="Illegal Address" src-address=2002:e000::20/128
add action=drop chain="Illegal Address" src-address=2002:7f00::/24
add action=drop chain="Illegal Address" src-address=2002::/24
add action=drop chain="Illegal Address" src-address=2002:ff00::/24
add action=drop chain="Illegal Address" src-address=2002:a00::/24
add action=drop chain="Illegal Address" src-address=2002:ac10::/28
add action=drop chain="Illegal Address" src-address=2002:c0a8::/32
add action=drop chain="Illegal Address" src-address=fec0::/10
add action=drop chain="Illegal Address" src-address=fc00::/7
add action=drop chain="Illegal Address" src-address=ff00::/8
add action=drop chain="Illegal Address" src-address=3ffe::/16
add action=drop chain=ICMPv6 comment="DROP - RS e RA" icmp-options=133 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=134 protocol=icmpv6
add chain=ICMPv6 comment="ACCEPT com hop limit =255 - diretamente conectados" hop-limit=equal:255 protocol=icmpv6
add action=drop chain=ICMPv6 comment="DROP de tudo que n\E3o est\E1 diretamente conectado" icmp-options=130 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=131 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=132 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=135 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=136 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=137 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=141 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=142 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=143 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=148 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=149 protocol=icmpv6
```

```
add action=drop chain=ICMPv6 icmp-options=151 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=152 protocol=icmpv6
add action=drop chain=ICMPv6 icmp-options=153 protocol=icmpv6
add action=jump chain=input jump-target="Illegal Address"
add action=jump chain=input jump-target=ICMPv6
add action=jump chain=forward jump-target=ICMPv6
add action=jump chain=forward jump-target="Illegal Address"
```