UNIVERSIDADE FEEVALE

VINICIUS LINDEN

IPv6 nos provedores regionais na era do esgotamento do IPv4.
Do core ao cliente final

Novo Hamburgo

2021

VINICIUS LINDEN

IPv6 nos provedores regionais na era do esgotamento do IPv4

Do core ao cliente final

Trabalho de Conclusão de Curso, apresentado como requisito à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Feevale

Orientador: Me. Vandersilvio da Silva

Novo Hamburgo

2021

AGRADECIMENTOS

Agradeço a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial:

Aos meus pais, por todo o suporte financeiro e emocional, e ao meu irmão, que embarcou nessa jornada junto comigo.

A minha companheira de vida Camila Prates, pelo apoio ao longo de toda graduação.

A toda equipe da TCA Internet, que fez parte da construção de toda minha jornada profissional. Ao colega Gabriel Arthur Mineiro, grande responsável pelo meu conhecimento na área deste estudo.

E agradeço também meu orientador Vandersilvio, por todo o apoio durante a execução do trabalho.

RESUMO

A internet como um todo vem crescendo juntamente com a quantidade de novos dispositivos com acesso à internet. Tecnologias como a IOT – *Internet of Things* e o 5G, futuramente ofertado pelas grandes operadoras, são grandes impulsionadores deste crescimento. Atualmente são os provedores regionais de internet que somados possuem a maior participação de mercado no setor de banda larga fixa, superando a participação de gigantes do mercado como Vivo, Claro e Oi. Paralelo ao crescimento da banda larga fixa no país e dispositivos conectados, a internet lida com um limitante que é o esgotamento do IPv4, e, conforme anunciado pelo LACNIC, em agosto de 2020 houve o esgotamento total dos blocos de endereços IPv4, não havendo mais disponibilidade de endereços IP para os novos entrantes, e nem novas alocações para os sistemas autônomos já em operação. Com este cenário sendo uma realidade, o IPv6 é a ferramenta que está à disposição para possibilitar que a internet continue crescendo. Sendo assim, este trabalho tem por objetivo propor e testar um modelo de implantação de IPv6 em um provedor regional de internet. Este estudo de caso foi executado e teve êxito na implantação do protocolo IPv6 na técnica de pilha dupla.

Palavras-chave: IPv6. IPv4. Redes. ISP.

ABSTRACT

The internet as a whole has been growing along with the number of new devices with internet access. Technologies such as IOT – Internet of Things and 5G, which will be offered in the future by large operators, are great drivers of this growth. Currently it is the regional internet providers that together have the largest market share in the fixed broadband sector, surpassing the participation of market giants such as Vivo, Claro and Oi. Parallel to the growth of fixed broadband in the country and connected devices, the internet deals with a limitation of growth, which is the exhaustion of IPv4. But as announced by LACNIC, in August 2020 there was a complete exhaustion of IPv4 address blocks, with no more IP addresses available for new entrants, nor new allocations for autonomous systems already in operation. With this scenario being a reality, IPv6 is the tool that is available to enable the internet to continue growing. Therefore, this work aims to propose and test a model for the deployment of IPv6 in a regional internet provider. This case study was carried out and successfully implemented the IPv6 protocol using the double stack technique.

Keywords: IPv6. IPv4. Networks. ISP.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ASN	*Autonomus System Numver*
ARP	*Address Resolution Protocol*
BGP	*Border Gateway Protocol*
CGNAT	*Carrier Grade Network Address Translation*
CDN	*Content Delivery Network*
CPE	*Customer Premises Equipment*
DNS	*Domain Name System*
DHCP	*Dynamic Host Configuration Protocol*
DHCPv6	*Dynamic Host Configuration Protocol version 6*
EGP	*Exterior Gateway Protocol*
GRE	*Generic Routing Encapsulation*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IoT	*Internet of Things*
IP	*Internet Protocol*
IPV4	*Internet Protocol version 4*
IPV6	*Internet Protocol version 6*
ISP	*Internet Service Provider*
LACNIC	*Latin American and Caribbean Internet Addresses Registry*
Log	Registro de eventos em um sistema de computadores
NAT	*Network Address Translarion*
Nic.br	Núcleo de informação e coordenação do .br

OSPF	*Open Shortest Path First*
Qos	*Quality of Service*
Ping	*Packet Internet Grouper*
RFC	*Request for Comment*
SO	*Sistema Operacional*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
VLAN	*Virutal Local Area Network*
VoIP	*Voice over IP*

Sumário

INTRODUÇÃO

Estamos vivendo um constante crescimento de dispositivos conectados à internet. A comunicação via internet entre estes dispositivos se tornou parte essencial da infraestrutura das redes, e hoje é vista como uma das principais ferramentas tecnológicas, possibilitando a criação de novos negócios, difundindo a comunicação, acelerando o crescimento econômico, encurtando distâncias e ajudando na educação (SEBRAE, 2020).

Dados do IBGE (2020) apontam que o Brasil possui hoje pouco mais de 212 milhões de habitantes. No ano de 2010 este mesmo órgão contabilizou algo em torno de 194 milhões de habitantes, o que nos mostra um crescimento populacional constante. O mesmo IBGE projeta para o final do ano de 2030 que o Brasil possua algo em torno de 225 milhões de habitantes. Com uma quantidade cada vez maior de usuários conectados à internet e consumindo sistemas baseados em internet, a maior parcela do tráfego gerado na rede é utilizando o protocolo internet versão 4, ou como chamaremos daqui para frente: IPv4 (IBGE, 2020).

Segundo a Pesquisa Nacional por Amostra de Domicílios Contínua – Tecnologia da Informação e Comunicação (Pnad Contínua TIC), de 2018, divulgada em abril de 2020 pelo Instituto Brasileiro de Geografia e Estatística (IBGE), três em cada quatro pessoas no Brasil possuem acesso à internet. Grande parte deste desenvolvimento e abrangência da internet no Brasil se dá pela penetração dos *Internet Service Providers* (ISP) no mercado, muitas vezes atendendo locais remotos que não são economicamente viáveis para grandes operadoras (WICKLER, 2015).

Tecnologias como o *Internet of Things* (IOT), redes LTE e a chegada do 5G[1], contribuem significativamente para o aumento dos dispositivos conectados à rede. Hoje há duas formas para que os dispositivos possam estar conectados e visíveis na internet no que diz respeito ao protocolo de comunicação. Pode-se conectar através do IP – *Internet Protocol* versão 4 ou simplesmente IPv4, e através do IP – *Internet Protocol* versão 6 ou IPv6 (SEBRAE. 2020).

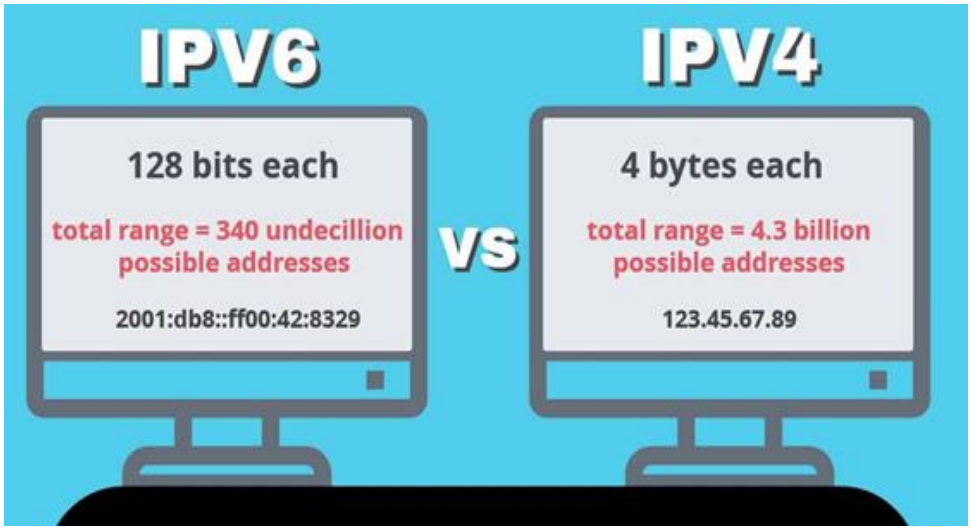
[1] 5G é a quinta geração de tecnologia para redes moveis, com maiores velocidades. Foi criada para ser a sucesso do 4G (Qualcomm.com, 2020).

Mas foi quando a internet já existia e possuía em torno de 500 hosts já conectados quando pesquisas de todo o mundo contribuíram para o desenvolvimento de um novo padrão de protocolo, conhecido como TCP/IP.

O IPv4 Foi o primeiro protocolo projetado na década de 1970-1980 publicado pelo *Internet Engineering Task Force* (*IETF***)** através da RFC 791 que foi difundido, e serviu como base para toda a estrutura da internet até os dias de hoje. Seu endereçamento foi baseado em um número de 32 bits separado em quatro octetos, resultando em uma capacidade para 4,3 bilhões de endereços. Foi desenvolvido pensando em suprir todas as demandas da rede na época e com capacidade para expansão. (Kurose. Ross, p.247, 2010)

Já o IPv6 começou a ser desenvolvido na década de 1990 pelo **IETF** para ser o sucessor do IPv4, uma vez que a comunidade já havia constatado que os 32 bits do protocolo versão quatro não seriam suficientes. Assim então uma nova versão do protocolo IP denominada versão 6 foi divulgada através da RFC 2460, agora com 128 bits de tamanho, representado por 8 blocos de 16 bits cada um, o IPv6 teve sua capacidade consideravelmente expandida em relação ao "irmão mais novo" com um total de 340 undecilhões de endereços disponíveis. (Kurose. Ross, p.265, 2010). Abaixo ilustrado pela figura 1.

Figura 1 – Comparação entre quantidades de endereços IPv4 e IPv6

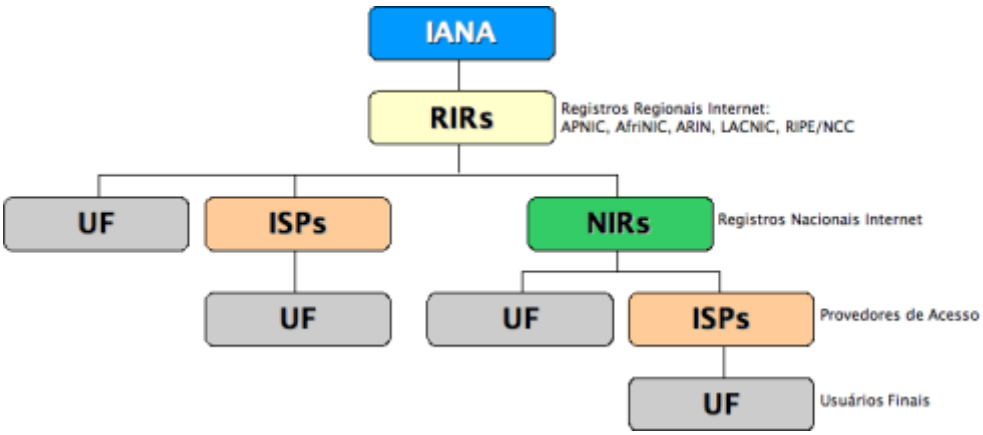


Fonte: COMPARITECH, 2020

No Brasil a responsabilidade de administração dos recursos da internet é do **Nic.br** (Núcleo da Informação e Coordenação do Ponto BR), que é uma autoridade nacional, ou *National Internet Registry* (NIR). O Nic.br responde ao **LACNIC**, que é uma autoridade

regional, ou *Regional Internet Registr* **(**RIR**)** que engloba a América Latina e Caribe. E por sua vez o **LACNIC** responde a **IANA** *(Internet Assigned Numbers Authority*), conforme apresentado em um organograma na figura 2.

Figura 2 – Organograma das autoridades responsáveis pelas designações dos blocos IP



Fonte: LACNIC, 2020

A notícia de que os estoques de IPv4 já haviam sido entregue as autoridades regionais veio em 2011 através da IANA (Iana.org).

Sabendo da limitação da quantidade de IPv4, o Nic.br iniciou um projeto chamado IPv6.br em 2008, com intuito de capacitar profissionais através de cursos, palestras e seminários. Porém, dados recentes apontam que mesmo com o esgotamento total do IPv4, apenas 1/3 do tráfego da internet se dá em IPv6. E em 2014 o LACNIC iniciou um processo controlado de alocações de novos blocos IPv4 com o objetivo de prolongar o estoque de endereços e permitir o ingresso de novos atores que queiram iniciar sua atividade de internet. Porém em agosto de 2020 o LACNIC informou que havia acabo a reserva de blocos IPv4, desta forma não conseguindo cobrir as necessidades de endereçamento IPv4 de seus associados (LACNIC, 2020).

Com este contexto de fim das reservas de IPv4, este trabalho está norteado pela seguinte questão de pesquisa: “Como aumentar a disseminação do IPv6 na internet através dos provedores regionais na era do esgotamento total do IPv4?”, e busca fazer um estudo sobre o protocolo, tecnologias e técnicas que permitam a implementação do IPv6 no usuário final pelos provedores regionais de internet, e com isso aumentar o tráfego IPv6 na rede e permitir o crescimento da internet.

O objetivo geral deste estudo é analisar como os provedores regionais podem – baseado em um cenário real de aplicação - contribuir para o crescimento da internet implementando o protocolo IPv6, em um contexto em que não há mais a possibilidade de novas alocações IPv4.

Tendo como objetivos específicos:

- Apropriar-se do conhecimento sobre arquiteturas de redes de provedores de serviço de internet (ISP);
- Apropriar-se do conhecimento sobre protocolo internet versão 6;
- Propor um modelo de implementação de IPv6 nos clientes finais;
- Realizar coleta de informações que permitam quantificar o tráfego IPv6 na rede;
- Realizar testes em cenário real e coletar informações para quantificar os principais problemas encontrados.

O estudo está dividido da seguinte forma: Introdução, onde será apresentado o assunto do trabalho. No segundo capítulo são abordados a teoria envolvendo os protocolos IP4, IPv6, técnicas de tradução, e será contextualizado com relação aos provedores regionais de internet. No terceiro capítulo são apresentados os trabalhos relacionados ao tema deste estudo. No quarto capítulo são apresentados a abordagem de pesquisa e definição dos passos. No quinto capítulo é descrito o estudo de caso. É apresentado toda parte prática de implementação do IPv6 e o resultado dos testes. As considerações finais contêm principais observações que o estudo proporcionou, percepções em relação ao cenário atual e estudos futuros.

2 REFERENCIAL TEÓRICO

Neste capítulo será tratado os fundamentos teóricos de redes de computadores baseado em comutação de pacotes, protocolos de endereçamento, os motivos pelos quais o IPv6 se faz necessário, e a contextualização sobre a importância do IPv6 para os provedores regionais, assim como sua importância para o contínuo crescimento da internet.

2.1 TCP/IP

As redes de computadores até os dias de hoje funcionam a um alto custo computacional e financeiro, por ter seu tráfego ainda predominantemente em IPv4, cada vez mais provedores de acesso precisam investir em equipamentos que façam a tradução dos endereços IP, devido ao esgotamento dos endereços IPv4 no Brasil e no mundo. O esgotamento já é um assunto conhecido e amplamente divulgado há anos, porém foi em agosto de 2020 que o LACNIC informou o esgotamento total dos endereços disponíveis para novas alocações (LACNIC, 2020).

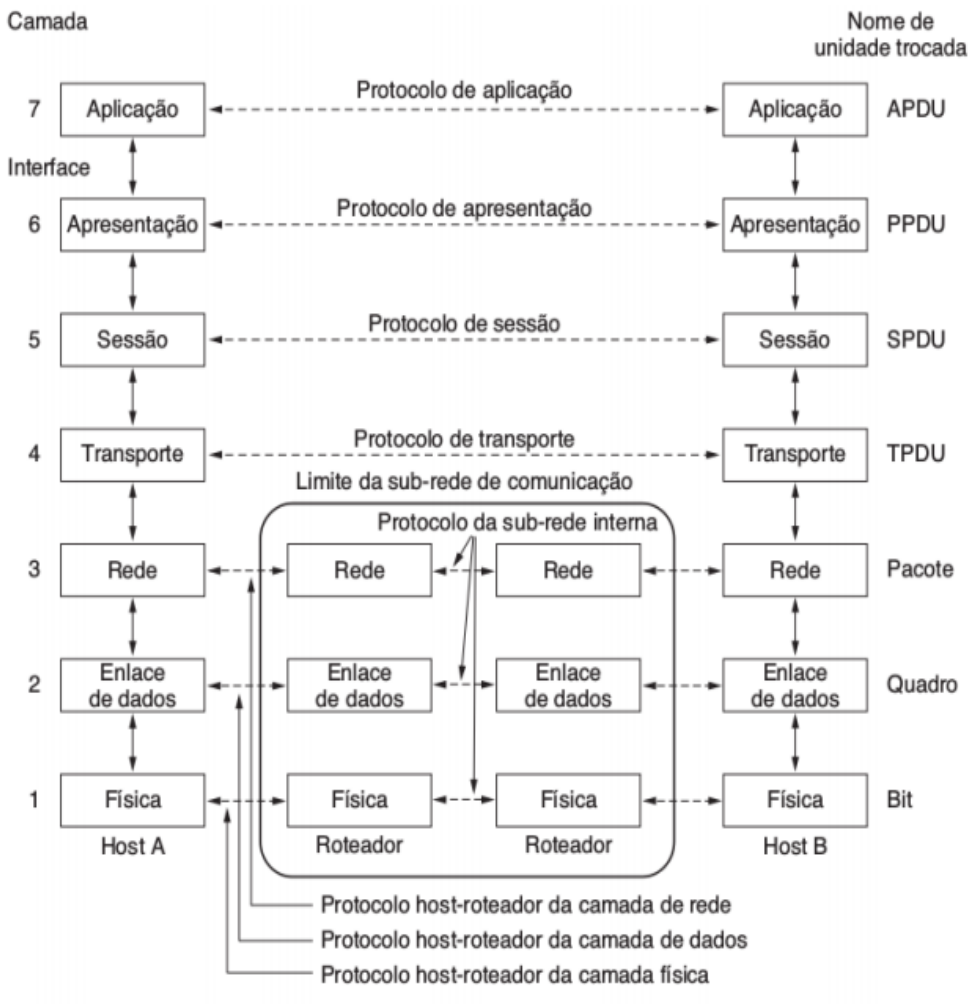
Isto significa que novos Sistemas Autônomos (ASs) não terão blocos IPv4 disponíveis para alocação, estes terão que ficar numa fila aguardando blocos que poderão ser recuperados de empresas que deixaram de operar nas redes (LACNIC, 2020). Conforme definem Kurose e Ross “Sistema Autônomo é um conjunto de roteadores que estão sob o mesmo controle administrativo e técnico e que rodam, todos, o mesmo protocolo de roteamento entre eles.” (Kurose. Ross, p.285, 2010)

Para entender o problema, é preciso entender o funcionamento dos principais protocolos e o que muda entre as versões 4 e 6 do protocolo internet, para então sumarizar o que pode ser uma das soluções para a continuidade do crescimento da internet no Brasil.

Tanenbaum define protocolo como “um conjunto de regras que controla o formato e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares contidas em uma camada”. Os protocolos têm por finalidade definir um padrão de comunicação entre os dispositivos de uma rede, para que consigam trocar informações entre si, utilizando um mesmo padrão. Nas redes de computadores, o protocolo utilizado atualmente é o TCP/IP, mas poderia ser outros, como o IPx/SPX que já foram utilizados e hoje são protocolos legados (Tanenmbaum. Wetherall, p.44, 2011).

A *International Organization for Standardization* (*ISO*) dos anos 1970 propôs um modelo onde as redes de computadores fossem organizadas em camadas, e tivessem seus protocolos de comunicação organizados através destas camadas. São sete camadas definidas pela ISO, em um modelo denominado *Open System Interconnection* (OSI) são elas: 1 - Física, 2 - Enlace, 3 - Rede, 4 - Transporte, 5 - Sessão, 6 - Apresentação e 7 – Aplicação (Figura 3).

Figura 3 - Modelo OSI

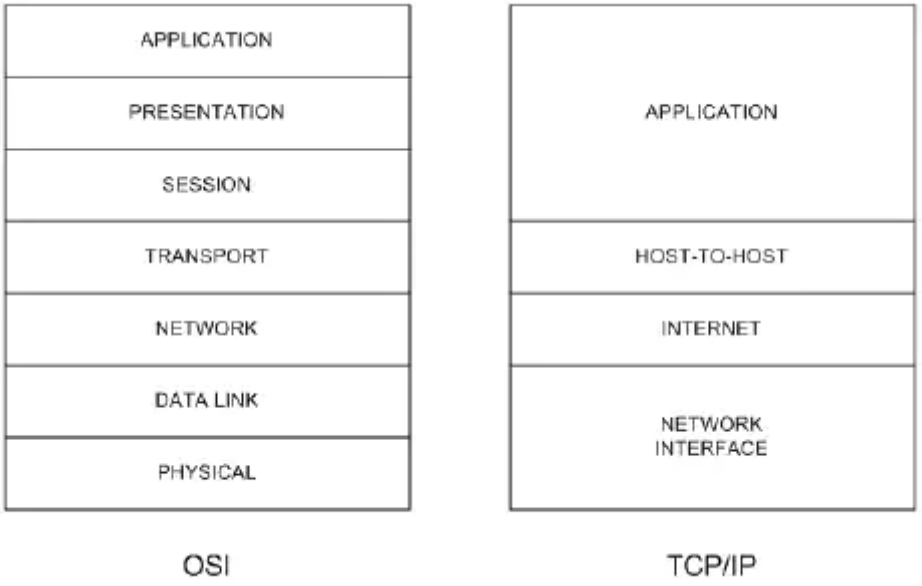


Fonte: Tanenbaum. Wetherall (2011, p.46)

O modelo OSI foi o primeiro grande esforço para criação de um modelo de comunicação de rede neutro, que não dependesse de fabricante e que siga um padrão. Comercialmente o modelo TCP/IP é o padrão historicamente mais utilizado para

dispositivos conectados à rede hoje. Este modelo incorpora algumas camadas do modelo OSI (figura 4) (Tanenmbaum. Wetherall, p.45, 2011).

Figura 4 - Protocolos TCP/IP com relação ao modelo OSI



Fonte: CISCO, 2005

2.2 IPV4

Inicialmente a internet foi projetada para abrigar um determinado número de hosts e funcionar através de comutação de pacotes. A comunicação entre dispositivos só foi possível quando se criou um conjunto de padrões garantindo a interoperabilidade da rede. Isto aconteceu em janeiro de 1983. O IP - *Internet Protocol* é um serviço de camada 3 implementado pelo conjunto de protocolos e serviços definidos no modelo TCP/IP (Tanenmbaum. Wetherall, p.66, 2011).

O protocolo não foi elaborado para rastrear e gerenciar o fluxo dos pacotes. Essas funções, se necessário, são realizadas por outros protocolos em outras camadas. (CISCO)

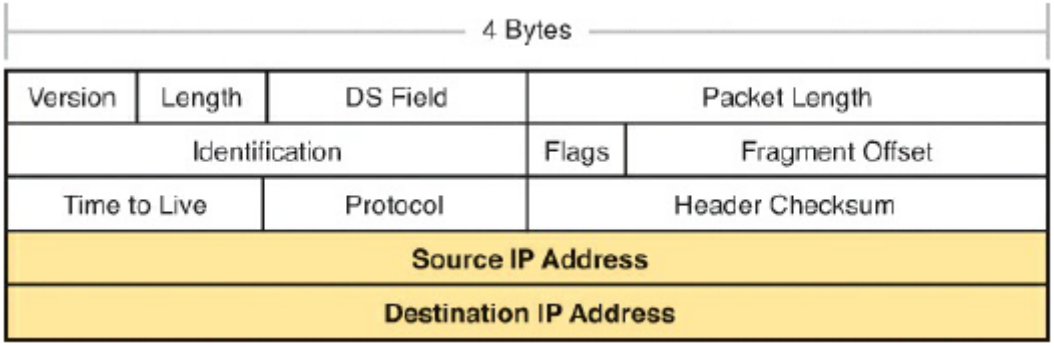
As características básicas do IP são:

- **Sem conexão -** Nenhuma conexão com o destino é estabelecida antes de encaminhar os pacotes de dados.
- **Melhor esforço (não confiável) -** A entrega do pacote não é garantida.

- **Independente de meio físico -** A operação é independente do meio físico que transporta os dados.

Conforme trazido por Kurose em 2010 o que define o IPv4 são seus 32 bits de endereçamento (equivalente a 4 bytes), é então o que possibilita uma quantidade de aproximadamente 4 bilhões de endereços IP (4.294.967.296). É este endereçamento que permite que os pacotes trafegados na rede saibam seu destino. Cada roteador no qual o pacote passa na rede tem seu endereço IP único, e como uma carta que possui endereço de origem e destino, o datagrama IP leva, além de outras informações, o endereço IP do dispositivo que está originando a conexão e o endereço IP de destino. A Figura 5 mostra o cabeçalho IPv4 e destaca IP de origem e destino (Kurose. Ross, p.252, 2010).

Figura 5 - Cabeçalho IPv4



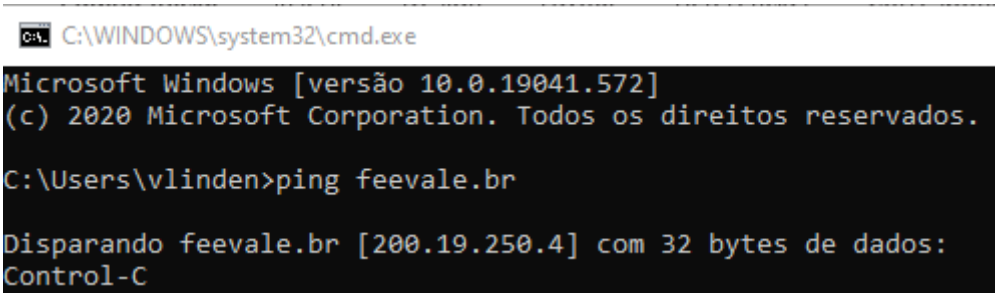
Fonte: Cisco ICDN 1 Cert Guide (2013, p. 144)

Os endereços IP são escritos em notação decimal separada por pontos, onde cada byte (8 bits) do endereço é representado de forma decimal e separado por ponto dos outros bytes do endereço (Kurose. Ross, 2010). Por exemplo, considerando o endereço IP 200.19.250.4. O 200 é o número decimal equivalente aos primeiros 8 bits do endereço; o 19 é o decimal equivalente ao segundo conjunto de 8 bits e assim por diante. A conversão binária resultante deste endereço IP que está em forma decimal é:

11001000.00010011.11111010.00000100

O endereço IP 200.19.250.4 é resultado da resolução DNS do site www.feevale.br.

Figura 6 – PING IPv4



Fonte: Criada pelo autor

Esta versão de endereços IP é a base da internet, mas como apontado pela equipe do IPv6.br, considerando que o IPv4 surgiu quase que junto com a concepção da internet na década de 70, o aumento de hosts conectados aumentou exponencialmente, não sendo mais possível que os 32 bits de capacidade de endereçamento continuem suportando este ritmo crescimento. Além disso, outras limitações para o protocolo IPv4 são comumente apontadas (Ipv6.br, 2012):

- Questões ligadas à segurança: ataques de *man-in-the-middle*, *ARP poisoning* e *IP spoofing;*
- Mobilidade;
- Suporte a parâmetros de *Quality of service* (QoS)

Como já apresentado anteriormente, na década de 90 foi publicada a proposta de uma nova geração do IP, ou IPv6. Com a proposta de resolver os problemas contidos no IPv4 na área de segurança, de quantidade de hosts e suporte à mobilidade.

2.3 IPv6

Na década de 1990 um esforço pela iniciativa do **IETF** foi iniciado para desenvolver o sucessor do IPv4, uma vez que a comunidade já havia constatado que os 32 bits do protocolo versão quatro não seriam suficientes. Assim então uma nova versão do protocolo IP denominada versão 6 foi divulgada através da RFC 2460, agora com 128 bits de tamanho, representado por 8 blocos de 16 bits cada um, o IPv6 teve sua capacidade consideravelmente expandida em relação ao seu antecessor, com um total de 340 undecilhões de endereços disponíveis. (Kurose. Ross, p.265-266, 2010).

Além da resolução do problema de quantidade de endereços, este novo endereço traz a solução para outras deficiências do seu antecessor, tais como suporte a roteamento e segmentação de pacotes na estação de origem, suporte à mobilidade e mecanismo de segurança. (LABORATÓRIO de IPv6, 2015)

Com o espaço de endereçamento de 128 bits, o IPv6 pode conter

340.282.366.920.938.463.463.374.607.431.768.211.456.

Este valor representa aproximadamente 79 octilhões de vezes a quantidade de endereços IPv4, e mais de 56 octilhões de endereços por ser humano no planeta Terra, levando em consideração uma população estimada de 6 bilhões de pessoas (Ipv6.br 2012).

A representação do IPv6 se difere um pouco do IPv4, visto que antes se tinha um espaço de endereçamento de 32 bits divididos em blocos de 8 bits separados por pontos e escritos de forma decimal. Já no IPv6, a representação divide o endereço em oito grupos de 16 bits separados por “:” e escritos com dígitos hexadecimais, que variam de 0 a 9, e de A a F. Por exemplo:

2a03:2880:f105:83:face:b00c:0:25de

Este endereço IPv6 é a resolução do host **facebook.com** feita a partir de dispositivo configurado com IPv6 (Figura 7).

Figura 7 - PING6 Facebook

Fonte: Criado pelo autor

A representação dos endereços IPv6 possuem uma característica única quando comparados com o IPv4. No IPv6 é possível abreviar os endereços para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de ser possível substituir uma sequência de zeros por “::” (Ipv6.br 2012). Por exemplo, o endereço **2804:023c:00cd:12ab:0000:0000:0000:0501** pode ser escrito como **2804:23c:cd:12ab:0:0:0:501** ou **2804:23c:cd:12ab::501**.

Há 3 tipos de endereços IPv6 definidos, são eles:

- ***Unicast*:** este tipo endereço identifica uma única interface, de forma que um pacote quando enviado a um endereço unicast é entregue a uma única interface.
- ***Anycast*:** identifica um conjunto de interfaces. Um pacote quando encaminhado é entregue a interface que pertence a este conjunto mais próxima da origem. Esta distância é medida pelos protocolos de roteamento. Endereço anycast é utilizado em comunicações de um para um de muitos
- ***Multicast*:** o endereço multicast também identifica um conjunto de interfaces, porém um pacote quando enviado a um endereço multicast é entregue a todas as interfaces que estão associadas a esse endereço. Endereço multicast é utilizado em comunicação de um para muitos. (IPv6.br. 2012)

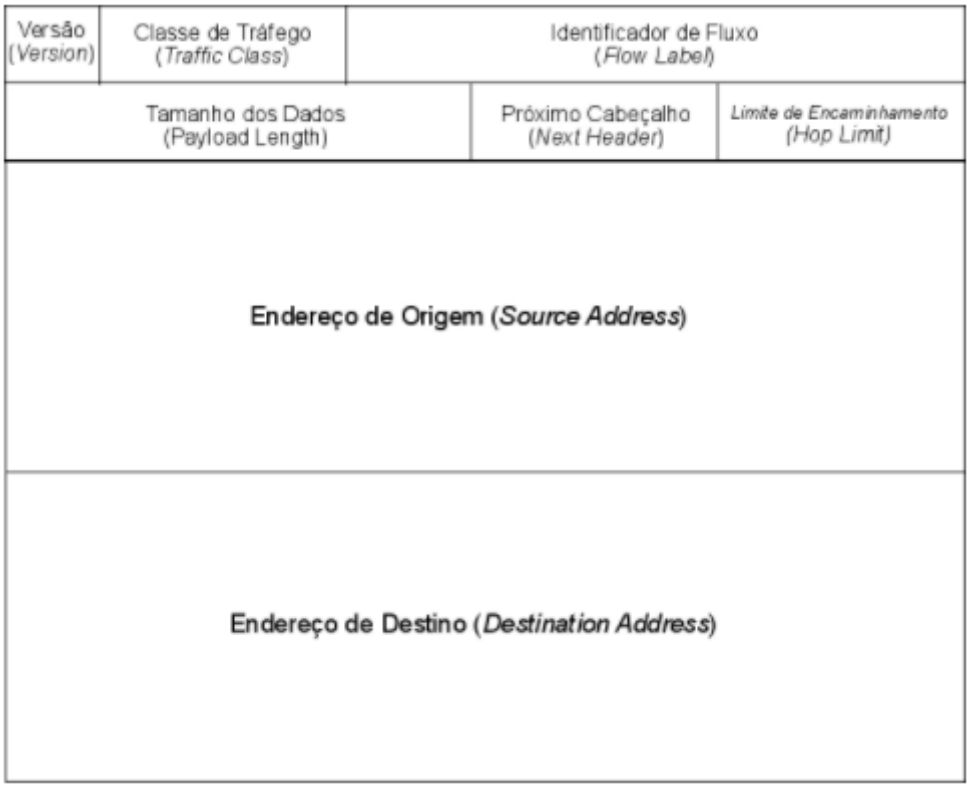
No que se refere ao cabeçalho do IPv6, há uma simplificação, onde alguns campos foram removido ou tornaram-se opcionais com o intuito de reduzir o processamento dos pacotes nos roteadores. Há o suporte a cabeçalhos de extensão, onde as opções não fazem mais parte do cabeçalho base, permitindo um roteamento mais eficaz e uma maior flexibilidade para introdução de novas opções no futuro. Com isso, suporte a autenticação e privacidade é mais uma mudança em relação ao IPv4, foram especificados cabeçalhos de extensão capazes de fornecer mecanismos de autenticação e garantir a integridade e confidencialidade dos dados que estão sendo transmitidos no enlace (Apostila IPv6.br, p.15, 2012).

Conforme exemplificado na figura 8, são os campos do datagrama IPv6:

- **Versão:** campo de 4 bits que identifica a versão do IP.
- **Classe de tráfego:** campo de 8 bits. Semelhando ao campo TOS do IPv4.
- **Rótulo de fluxos:** campo de 20 bits utilizado para identificar um fluxo de datagramas
- **Tamanho dos dados** (*Payload length)*: número inteiro que identifica o tamanho em bytes do datagrama IPv6 que se soma ao pacote do cabeçalho.
- **Próximo cabeçalho:** identifica o protocolo ao qual o conteúdo será entregue, eja ele TCP ou UDP. No IPv4 o campo se chamava **Protocolo.**

- **Limite saltos (TTL):** este campo teu valor decrementando a cada salto de roteamento na rede.
- **Endereço de origem e de destino:** campo contendo os vários formatos de endereços de 128 bits do IPv6.

Figura 8 – Cabeçalho IPv6



Fonte: Ipv6.br, 2012

É possível perceber que alguns campos do cabeçalho IPv4 não se repetem no cabeçalho do IPv6, e isto foi pensado para melhorar o desempenho de processamento dos pacotes. São os campos que deixaram de existir:

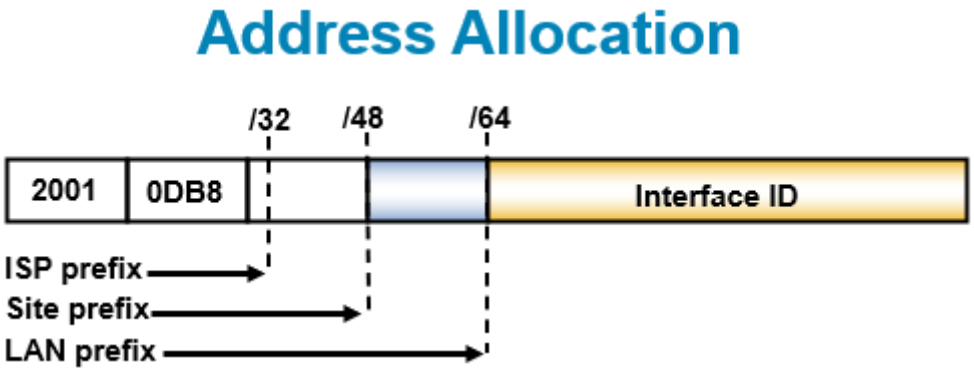
- **Fragmentação/remontagem:** o IPv6 não permite fragmentação e remontagem em roteadores que estão entre a origem e o destino. Quando um roteador intermediário não consegue repassar um pacote por causa do seu tamanho, o roteador não fragmenta ou descarta o pacote, ele devolve a origem com uma mensagem ICMP de erro “pacote muito grande” *(packet too big)* para que a origem possa reenviar o pacote.

- **Soma de verificação do cabeçalho:** funcionalidade que foi retirada do IPv6 por questões de redundância. Os projetistas viram que a soma de verificação é feita em protocolos da camada de transporte (TCP e UDP) e na camada de enlace (ethernet).
- **Opções:** não faz mais parte do cabeçalho IPv6. Ele agora pode ser adicionado no campo próximo cabeçalho, assim deixando o cabeçalho com um tamanho fixo de 40 bytes (Kurose, Ross, p.267, 2010).

O IPv6 utiliza uma hierarquia de três níveis para fazer a alocação de endereço para o dispositivo, diferente do IPv4 que utiliza uma hierarquia de dois níveis. No IPv4 um prefixo identifica a rede e outro prefixo identifica o host. Por exemplo, o IP 200.168.1.1/24 é atribuído ao computador, e a partir disso sabe-se que a rede em que ele está conectado é 200.168.1.0. Já no IPv6 a hierarquia de três níveis é composta por prefixo, sub-rede e computador (Figura 9). Esta forma de hierarquia permite que um bloco de endereços seja alocado para um cliente, ao invés de um único IP público como é feito no IPv4, e ainda na maioria das vezes este IP público estando atrás de CGNAT (*Carrier Grade Network Address Translation)*.

As políticas de alocações do IPv6 determinam que o ISP receba um prefixo /32. O NIC.br recomenda que seja alocado um /48 para cada segmento da rede e pelo menos uma rede /64 para cada cliente final residencial e, desta forma facilitando algumas funcionalidades como a autoconfiguração, além de já deixar a rede preparada para uma expansão futura. (IPv6.br, 2012).

Figura 9 – Alocação de endereços IPv6



Fonte: Cisco Ipv6 *Solutions Integration & Co-Existence*, 2020

No ano de 2017, em uma reunião do Grupo de Trabalho de Engenharia de Redes promovida pelo NIC.br, foi apresentada a BCOP (*Best Current Practice for Operators*) *"IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose"* que indica a entrega/alocação de pelo menos um /56 ao usuário final, mas manter a reserva de um /48. Entregando um prefixo /56 por usuário, é possível que um provedor que tenha um prefixo /32 alocado atender 16 milhões de clientes (Ripe.net, 2017).

2.4 TRANSIÇÃO IPV4 X IPV6

Observou-se até então característica, semelhanças, diferenças e particularidades que os protocolos internet possuem, e a partir do momento que estes protocolos não são compatíveis, ou seja, eles não conversam entre si, o IPv6 não vem como um complemento para resolver o problema da escassez de IPv4, e sim como um substituto. Para o período de transição, e coexistência, já que se fala de um longo período em que haverá roteadores e dispositivos lidando simultaneamente com IPv4 e IPv6, a RFC 4213 especifica dois mecanismos que podem ser implementados em roteadores e dispositivos para tal ação, são eles a pilha dupla e o tunelamento. (Ipv6.br 2012).

No ano de 2012 e equipe do grupo IPv6.br traz uma abordagem com três possibilidades, são elas:

- **Pilha dupla:** esta é a técnica padrão escolhida para transição. Consiste na convivência de IPv4 e IPv6 de forma nativa nos equipamentos.
- **Tuneis:** configuração que permite a comunicação de redes IPv4 através de uma rede IPv6.
- **Tradução *(NAT):*** habilita que dispositivos utilizando IPv6 possam se comunicar com outros dispositivos que usam IPv4, o que é feito através da conversão de pacotes.

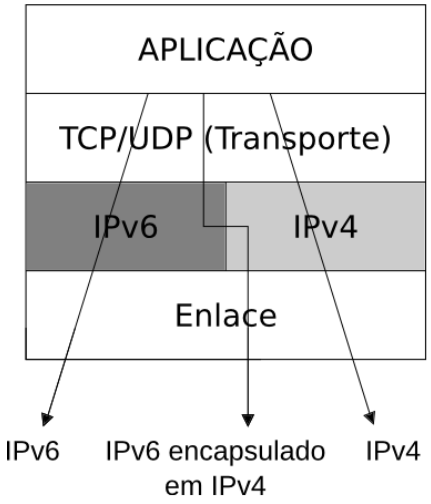
A equipe IPv6.br traz ainda que as técnicas de transição podem ser classificadas em *Stateful* ou *Stateless.* Técnicas classificadas como *stateful* precisam manter registro de estado da conexão em uma tabela, enquanto técnicas *stateless* não tem essa necessidade, cada pacote é tratado de maneira independente. Resumidamente técnicas *stateful* são mais caras pois exigem mais CPU e memória, o que de certa forma não as tornam bem escaláveis (Ipv6.br 2012).

2.4.1 PILHA DUPLA

A forma mais direta e comumente utilizada para iniciar com dispositivos habilitados com IPv6 em uma rede é através da pilha dupla, e é a recomendação que a equipe do IPv6.br desde o início do projeto IPv6.br coordenado pelo Nic.br. Esta recomendação se dá pela internet possuir um cenário estável e funcional com o IPv4, e implementar o IPv6 de forma que os dois protocolos coexistam é uma possibilidade viável para disseminar o uso do IPv6. Ainda neste cenário é necessário levar em consideração sites e aplicações legadas que não estão operando em IPv6, então a pilha dupla permite que o usuário acesse conteúdo de ambos os protocolos (Ipv6.br 2012).

Trazendo para um ambiente real, a pilha dupla é a configuração simultânea dos endereços IPv4 e IPv6 na placa de rede do dispositivo. Funcionando de forma hibrida, não há necessidade de mecanismo de tradução (Figura 10).

Figura 10 – Funcionamento Pilha Dupla



Fonte: IPv6.br, 2012

2.4.2 TÚNEIS

Túneis são uma alternativa quando a pilha dupla não é possível, pois fazem o encapsulamento de pacotes para que seja possível atravessar uma rede que não tenha suporte ao pacote que está em uso. Assim, pacotes IPv6 podem cruzar uma rede exclusivamente IPv4 para alcançar seu destino, e retornar a origem. Esta técnica também é discutida na RFC 4213.

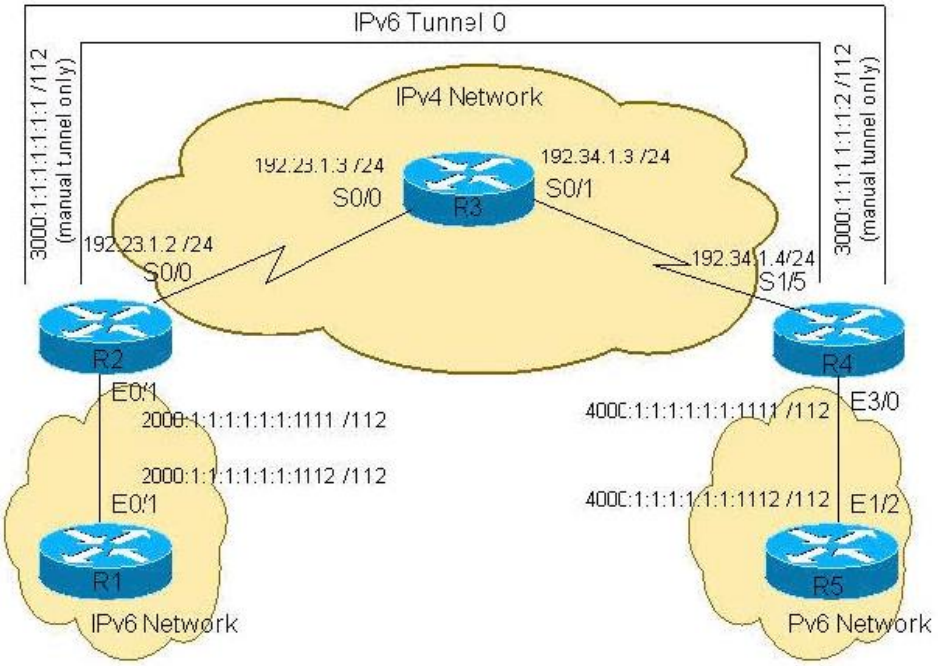
Conforme descrito na topologia apresentada por Kurose e Ross, 2010. Os pacotes IPv6 são transportados dentro da rede até chegarem a um roteador que possui ambos os protocolos e que fará o encapsulamento do pacote IPv6 em um pacote IPv4. Este pacote IPv4 viaja até chegar ao seu destino onde então é desencapsulado e entregue somente o pacote IPv6 ao destino. (Kurose. Ross, p.268-269, 2010)

Este trabalho apresentará as formas de tunelamento que foram apresentadas a comunidade da internet do Brasil pela equipe do IPv6.br. São eles, tuneis 6to4, túneis GRE e túnel brocker.

2.4.2.1 TÚNEL 6 *OVER* 4

Esta técnica de para transição do IPv4 para o IPv6 está descrita na RFC 4213 (IETF.org). Ela consiste em um nó IPv4 encapsular no seu pacote de transmissão o pacote vindo de um dispositivo com IPv6 gerado no dispositivo de origem. Neste pacote é adicionado o tipo 41 no seu cabeçalho, então quando o roteador de destino receber este pacote IPv4, ele desencapsula o pacote IPv6 contido no pacote IPv4 e entrega para o destino (Figura 11) (CISCO, 2006).

Figura 11 – Túnel 6 over 4



Fonte: Cisco, 2006

2.4.2.2 TÚNEL GRE

O túnel GRE é outra opção de tunelamento para transporte de redes IPv6 sob redes IPv4. Túnel GRE também é estático, e o acrônimo corresponde a *Generic Routing Encapsularion*, e está descrito na RFC 2784. Foi desenvolvido inicialmente pela Cisco com o objetivo de encapsular os diversos protocolos no túnel, inclusive o IS-IS protocolo proprietário Cisco, e o IPv6 (Ipv6.br 2012).

Seu funcionamento se dá de maneira simples. A origem gera os pacotes IPv6, quando cruzar o roteador que possui os dois protocolos e está fechando o túnel com a outra ponta, este roteador adiciona ao pacote o cabeçalho GRE e o cabeçalho IPv4 e envia ao IP de destino. Ao chegar na outra ponta, o roteador remove do pacote encapsulado os cabeçalhos IPv4 e GRE e entrega o pacote original ao destinatário.

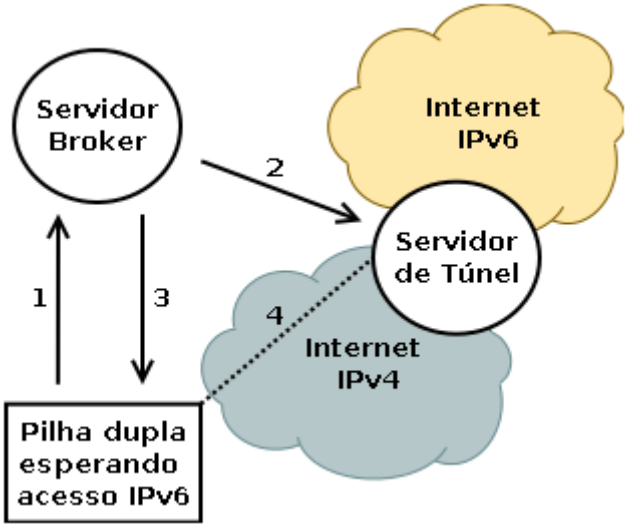
Assim como o túnel 6 over 4, sua configuração é feita de forma manual, e por isso pode ser uma forma não muito escalável para ser adotada como transição em uma rede. (Ipv6.br 2012)

2.4.2.3 TUNEL BROKER

Túnel Broker pode ser visto como um provedor de internet IPv6 virtual, que oferece conectividade IPv6 para usuário que estão conectados em uma rede IPv4, tornando na prática, dispositivos, ou uma rede, em pilha dupla, exemplificado na Figura 12. Seu funcionamento depende de o usuário realizar um cadastro em algum provedor que ofereça o serviço. O provedor realizará a configuração no dispositivo de forma automática ou semiautomática, através de scripts ou possibilitando ao usuário acesso a um passo-a-passo.

A equipe IPv6.br recomenda a utilização do Túnel Broker para usuários domésticos e corporativos que queiram testar o IPv6, ou começar um processo de implantação de suas redes, mas que os seus provedores de internet ainda não fornecem o IPv6 ao usuário final.

Figura 12 – Estrutura lógica de funcionamento do Túnel Broker



Fonte – Ipv6.br, 2012

2.4.3 TRADUÇÃO DE ENDEREÇOS

Com a escassez de IPv4 na internet técnicas foram sendo desenvolvidas e aprimoradas na tentativa de prolongar sua vida útil. Umas das primeiras técnicas de tradução de endereços privados em endereços públicos foi denominada *Network Address Translation* (NAT), descrita na RFC 3022, foi uma estratégia que se disseminou e hoje é utilizada mundialmente em todas as redes internas Ipv4. Uma empresa que possui 50 equipamentos na rede interna, antes de existir a técnica de NAT, utilizaria 50 IPs públicos Ipv4 para possibilitar que estes hosts se comunicassem com a internet, com o NAT o endereçamento interno das redes passou a utilizar IPs privados (RFC 1918). As redes descritas na RFC 1918 não são roteáveis na internet, estes Ips privados passam então pelo roteador de borda da empresa, que faz a tradução para um único endereço público e então sai para internet. O roteador de borda da empresa pode ser o modem do provedor, pode ser um firewall, ou um servidor com o serviço de NAT habilitado (IPv6.br 2012).

Mas mesmo com a técnica descrita acima, que visava diminuir o uso de Ipv4 públicos na internet, o crescimento exponencial da internet exigiu que novas técnicas fossem aplicadas como forma de transição para o novo protocolo internet que viria, e foi então que o CGNAT, ou NAT 444 surgiu.

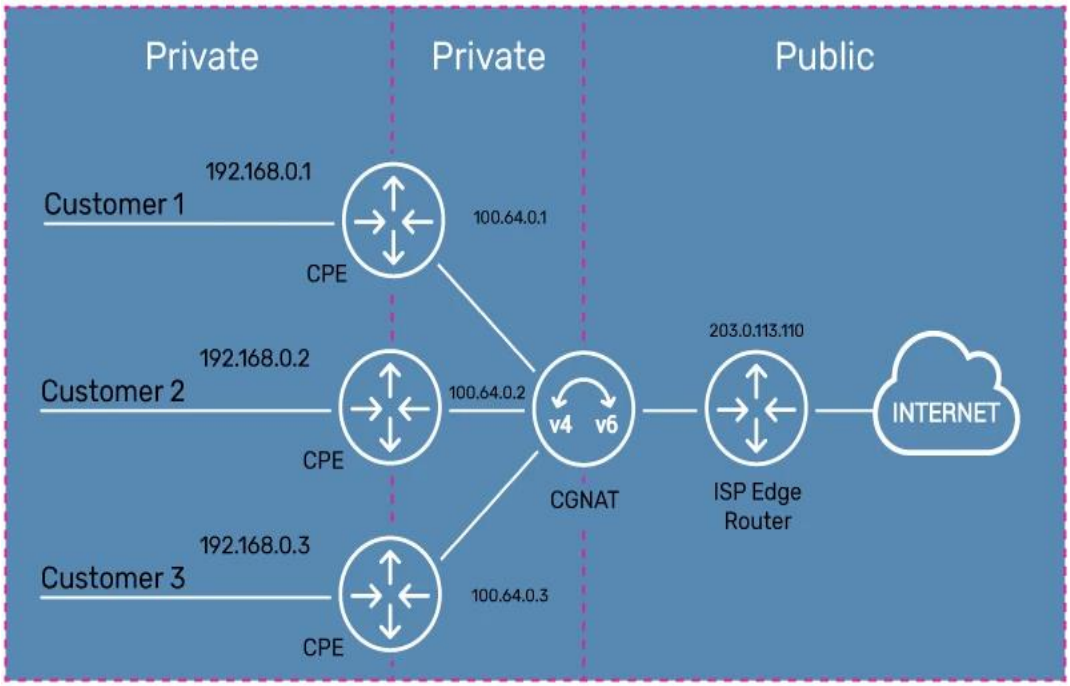
2.4.3.1 NAT 444

Contida na RFC 6264, o CGNAT ou NAT 444, é a tradução em grande escala (*Carrier Grade Network Address Translation*) feita por provedores de internet. Assim como o NAT é utilizado na rede interna do cliente, o CGNAT tem sido usado na borda do provedor com o cliente com o mesmo intuito, prolongar a vida útil dos endereços Ipv4. Assim como o NAT da rede interna, o CGNAT especifica uma faixa de IP para ser utilizada, contida na RFC 6598, dentro da rede do provedor, está rede passa pela tradução antes do roteador de borda, e então sai para internet com os IPs públicos do provedor (A10NETWORKS, 2020). Basicamente o funcionamento é da seguinte forma:

- ➔ Lado do cliente: Ipv4 privado da rede interna do cliente é traduzido para o Ipv4 privado do provedor.
- ➔ Lado do provedor: Ipv4 privado do provedor (100.64.0.0/10) é traduzido para o Ipv4 público do provedor para então ter conectividade com a internet.

O resultado do NAT 444 é que esta técnica permite que múltiplos clientes com suas próprias redes internas naveguem pelo IP privado de CGNAT do provedor e dividam um único IP de internet para acessar a rede, como exemplifica a Figura 13.

Figura 13 – Lógica de funcionamento do NAT 444



Fonte – A10 Networks, 2020

Segundo o Ipv6.br, o uso de NAT 444 deve ser acompanhado do Ipv6 nativo para os usuários, não deve ser implementado isoladamente, pois serviços de VoIP, conexões P2P e jogos online se tornam inviáveis com este tipo de tradução. Outro ponto que vale salientar nesta técnica é que ela custa caro, em dinheiro e processamento, pois o equipamento que fará a tradução precisa receber todo o tráfego dos clientes, analisar tabelo de conexões, traduzir o endereço e encaminhar para o destino. Um hardware específico para processamento de pacotes de CGNAT com capacidade para 25G custa $14900.00 (F5NETWORKS. 2020).

Atualmente o Google é um dos poucos provedores de conteúdo que permite que o provedor anuncie os blocos IP de CGNAT para os próprios caches do Google hospedados dentro do seu provedor. Com isso diminuindo o tráfego que necessita ser traduzido pelo equipamento de CGNAT (GOOGLE, 2020).

Outros provedores de conteúdo que possuem CDN (*Content Delivery Network*) espalhada nos provedores pelo mundo não possuem documentação específica tratando esta possiblidade.

2.5 ROTEAMENTO

O roteamento é uma técnica que define por meio de um conjunto de regras como os pacotes originados em uma rede A devem alcançar uma rede B, estando estas redes diretamente conectadas ou a saltos de distância (Kurose. Ross, p.285, 2010).

O roteador pode ser um equipamento fabricado especificamente para esta função onde o fabricante do hardware embarca neste equipamento também o software, ou pode ser até mesmo um computador com diversas placas de rede rodando alguma distribuição de software livre com um a função de roteamento (BRITO, p.95, 2013).

O roteador toma suas decisões de escolha de caminho para os pacotes baseado em informações inseridas manualmente pelo administrador de rede, em caso de configuração de roteamento estático. Ou dinamicamente baseado nas métricas definidas nos protocolos de roteamento dinâmicos. No roteamento dinâmico as rotas são automaticamente aprendidas através de troca de mensagens entre os roteadores. Tem-se dentro do roteamento dinâmico dois tipos de protocolos, o utilizado internamente, ou IGP (*Interior Gateway Protocol),* e o utilizado externamente, ou EGP (*Exterior Gateway Protocol*) (Kurose. Ross, p.285-287, 2010).

2.5.1 OSPFV3

O OSPF é um protocolo de roteamento dinâmico tipo LS (Link-State) ou estado de enlace, utilizado intra-AS co o IGP. Utiliza *broadcasting* como informação de estado de enlace e o algoritmo de Dijkstra para calcular o caminho com menor custo a ser percorrido na rede (Kurose. Ross, p.288, 2010).

As mensagens trocadas entre os roteadores para comunicação no protocolo são chamadas de *Link-State Advertisiments* (LSA). Na versão 3 (RFC 5340) do protocolo OSPF, onde o IPv6 é suportado, informações como o prefixo IPv6 da interface, a máscara de rede, o tipo de interface conectada, são trocadas através de mensagens LSA (CISCO).

A versão com suporte a IPv6 do protocolo opera diferente da versão 2 em alguns aspectos, mas a principal é que o protocolo opera por estado de link de interface, não sendo necessário declarar as redes que serão distribuídas pelo OSPF aos roteadores da rede. Na versão 3 endereços de rede IPv6 não são mais apresentados em todas as mensagens, exclui-se das mensagens *Router-LSA* e *Network-LSA.* Informações de OSPF *Router-ID, Area ID* e *LSA Link-State ID* permanecem 32 bits. Os roteadores vizinhos são identificados pelo *Router ID* e não mais pelo endereço IP de *Loopback* como era no IPv4. Porém, por boa prática utiliza-se o endereço IPv4 da interface *Loopback* do roteador como *Router ID* (Ipv6.br 2012) (CISCO, 2021).

2.5.2 BGP4

O protocolo BGP é o protocolo de roteamento externo padrão hoje. Tem-se o BGP como um protocolo crítico para o funcionamento da internet (Kurose. Ross, p.2912010).

O BGP não possui diferenciação de versão para ter compatibilidade com o IPv6, atualmente está na versão 4, e nesta versão mantém suporte tanto ao IPv4 quanto IPv6. É um protocolo que funciona baseado em sessões TCP que trocam mensagens na porta 179 (IPv6.br 2012).

Assim como o OSPF, o BGP pode ser utilizado como um IGP quando configurado entre roteadores do mesmo sistema autônomo. É através do número do AS que o protocolo fará a distinção de funcionamento. Quando configurado sessões entre o mesmo AS funcionará como IGP, e quando configurado sessões entre AS diferentes se comportará como EGP (*Exterior Gateway Protocol*) (Kurose. Ross, p.291, 2010).

O protocolo trabalha com quatro mensagens BGP para troca de informações e para manter o estado de conexão TCP. São estas mensagens: *OPEN, UPDATE, KEEPALIVE* e *NOTIFICATION.*

As mensagens *OPEN* são trocadas entre os *peers* após o estabelecimento da comunicação TCP, esta mensagem leva as informações para o estabelecimento da sessão BGP, tais como o ASN, versão do protocolo, IP etc. As mensagens de *UPDATE* são usadas para carregar informações de roteamento entre os vizinhos, estas informações serão utilizadas para construir o grafo que descreverá o relacionamento entre os vários ASs na internet. As mensagens *KEEPALIVE* são enviadas periodicamente para testar o estado da conexão TCP e manter as sessões ativas. E por fim as mensagens de *NOTIFICATION*, estas são enviadas quando há um erro, a perda da conexão TCP por exemplo, assim fechando a conexão BGP imediatamente após seu envio (IPv6.br 2012)

Os roteadores que estão na internet rodando BGP mantém uma tabela de roteamento, que nada mais é que uma lista com os prefixos alcançáveis no mundo. Uma tabela de roteamento completa, também conhecida pelo termo *Full-Routing*, carrega hoje em IPv6 em torno de 123 mil rotas. Em IPv4 a tabela global está com aproximadamente 880 mil rotas (CIDR-REPORT.ORG, 2021).

2.6 PROVEDORES REGIONAIS DE ACESSO

Provedor regional de internet por definição, é uma empresa que atua em região específica e atende menos clientes se comparado com as operadoras de âmbito nacional. Quando se refere a provedores regionais de internet, refere-se ao tipo da empresa, e não a qual região.

Os provedores regionais do brasil somados são hoje a maior operadora de telecomunicações do país. A Anatel contabilizou que os provedores regionais registraram 732 mil novos contratos de internet entre janeiro e maio de 2020. O aumento de demanda, aliado ao bom serviço prestado pelos provedores, fez com que o setor tivesse um crescimento tão elevado (TELESINTESE, 2020).

Segundo a Anatel, há pelo menos um provedor em operação em todas as cidades do país, e mais de 60% do mercado nacional de fibra óptica até os domicílios brasileiros vêm dos provedores regionais (ANATEL, 2020).

A ABRINT (Associação Brasileiro de Provedores de Internet e Telecomunicações) trouxe na apresentação “Provedores Regionais – Como Adicionar Valor à Banda Larga” feita para os associados uma série de paradigmas e abismos que os provedores regionais consegues resolver em relação as grandes operadoras. Atualmente os provedores de internet tem capacidade de prestar os mesmos serviços que as grandes operadoras e com qualidade igual ou melhor, pois, com menos clientes que as grandes operadoras os ISPs conseguem se posicionar com muito mais proximidade do cliente, o que facilita a comunicação e a resolução de problemas. Os provedores regionais hoje têm a sua disposição equipamento de alta qualidade e conseguem extrair deles uma qualidade que há anos era impensável para uma pequena empresa, se comparado a capacidade de investimento e agressividade exercida pelas grandes teles. (ABRINT, 2020)

Um exemplo dessa qualidade se dá também pela distância do conteúdo que é consumido pelos clientes estar muito mais próximo, as CDNs de grandes empresas como Google, Netflix e Facebook estão cada vez mais presentes nos Datacenters dos ISPs. CDN é o acrônimo para Rede de Entrega de Conteúdo (*Content Delivery Netowrk),* é uma plataforma de servidores, que hospeda conteúdo das empresas que a fornecem, altamente distribuída que ajuda a diminuir o atraso de entrega de conteúdo. E no caso dos provedores ajuda a poupar banda de internet, pois boa parte do conteúdo acessado pelos clientes está hospedado dentro da própria rede. (AKAMAI, 2020)

O Brasil hoje é um mercado diferente do resto do mundo no que se refere a provedores de internet. Tem-se os grandes operadores como nos países desenvolvidos Na América do Norte e Europa, mas a grande parcela dos usuários está nos provedores regionais. Além do que já foi citado, há um outro fator que contribuiu para este fenômeno, a Anatel (Agência Nacional de Telecomunicações), órgão regulador do setor, publicou em 2017 novo regulamento para obtenção da licença de SCM (Serviço de Comunicação Multimidia), não a exigindo para provedores com menos de 5 mil clientes, ou que não usem frequência de rádio do espectro licenciado (ANATEL, 2020).

A revista RTI, especializada em telecomunicações, traz na edição 241 de junho de 2020, informações sobre o mercado de provedores. Na matéria feita com os maiores provedores do norte e nordeste do país dados mostram que os provedores continuaram crescendo. A fala trazida pelo conselheiro administrativo da Abrint – Associação Brasileira de Provedores de Internet e Telecomunicações – “Estamos crescendo na crise”, evidencia como mercado brasileiro é diferente do resto do mundo (RTI, 2020).

3 TRABALHOS RELACIONADOS

Pesquisas relacionadas ao tema escolhido neste trabalho foram buscadas na plataforma Google Scholar. Inicialmente, uma pesquisa mais ampla foi feita para identificar áreas de interesse no tema relacionado a Ipv6. A *string* de busca (“ipv6” AND “provedor” AND “internet”) retornou cerca de 569 resultados, visto que o assunto de Ipv6 está sendo tratado há um certo tempo, e período de pesquisa data desde 2015.

Foram identificadas diversas áreas de estudo sobre o assunto geral, mas focou-se em quatro trabalhos que abordaram o Ipv6 como alternativa ao esgotamento do Ipv4, assim como trabalhos que de alguma forma adentraram sobre os padrões de rede dos provedores regionais, uma vez que há particularidade nas topologias de redes de provedores regionais. Dentre as propostas encontradas, decidiu-se focar naquelas aplicáveis aos provedores regionais, como pilha-dupla, túneis, e estudos que propuseram uma aplicação prática.

3.1 TRABALHO 1

Sousa (2018) traz em seu objeto de estudo uma implementação de Ipv6 em pilha dupla para transição de redes Ipv4 parar redes Ipv6. Como já tratado anteriormente neste trabalho na seção 1.4.1, a pilha dupla é a técnica recomendada pelo time do Ipv6.br para provedores de acesso, conteúdo e empresas que desejam operar com os dois protocolos e possam fazer isto de forma escalável.

No seu estudo, Sousa (2018) traz um ambiente simulado de comunicação entre um servidor WEB e uma estação de trabalho, ambos configurados com os dois protocolos de endereçamento, e a partir disso ele estabelece uma série de passos para execução do seu experimento, tais como:

- Levantar inventário de equipamentos (compatibilidade dos Sos com Ipv6)
- Verificar compatibilidade de sistemas da empresa
- Verificar nos ativos de rede se possuem suporte ao protocolo Ipv6
- Capacitar equipe
- Implantar Ipv6

Em seu processo, foi efetuado um plano de endereçamento seguindo padrões que ainda se encontram atuais, reservando uma rede /48 para clientes corporativos, e ressalta a importância de automatizar a distribuição de endereços dentro da rede através do DHCPv6 ou SLAAC.

Concluiu-se neste estudo que métodos paliativos de sobrevida do Ipv4, como o CGNAT, aumentam a preocupação com segurança, e que a pilha dupla é uma técnica sem traumas para transição do Ipv4 para o Ipv6, visto que aplicações legadas e softwares mais antigos continuarão funcionando, mesmo os protocolos não sendo compatíveis entre si.

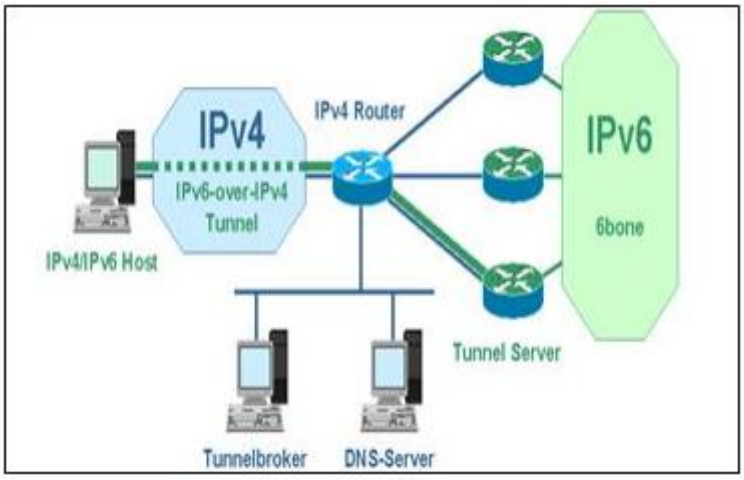
3.2 TRABALHO 2

Em um estudo intitulado “IPV6 – PROCESSO DE TRANSIÇÃO: IMPLANTAÇÃO DE TUNNEL BROKER PELA APLICAÇÃO GOGO6” os autores Thiago Lucas, Eduardo Morares e Carlos Tojeiro, trazem no ano de 2017 uma pesquisa relacionada ao processo de transição do protocolo Ipv4 para o Ipv6, com a técnica de tunelamento pela Gogo6, assim como os resultado alcançados na navegação em Ipv6 por esta técnica.

Apresenta-se neste estudo uma técnica de tunelamento para transição utilizando a ferramenta Gogo6. Esta ferramenta é gratuita, só solicita um cadastro no site e funciona através de um cliente que é instalado no computador em questão.

O cliente túnel envia um pacote pela internet Ipv4 para se autenticar no serviço de *Tunnel Broker*. Após isso, o próprio túnel de forma dinâmica atribui um endereço Ipv6 para o usuário assim como cria registros para utilização de nomes de Ipv6 no DNS. O servidor Broker funciona em pilha dupla e está conectado à internet global (Figura 14).

Figura 14 – Topologia *Tunnel Broker* implementada.



Fonte – "IPV6 – PROCESSO DE TRANSIÇÃO: IMPLANTAÇÃO DE TUNNEL BROKER PELA APLICAÇÃO GOGO6", 2017

3.3 TRABALHO 3

O estudo de Santos (2016) apresenta um modelo de referência para a implementação de redes de computadores utilizando o protocolo Ipv6. Traz-se neste estudo um cenário onde o Brasil possui 2138 provedores, sendo 90% de pequeno porta com até 49 funcionários, e atendendo cidades com até cem mil habitantes (CGI.br, 2016).

Descreve-se neste trabalho a implementação do Ipv6 em um provedor de internet utilizando a técnica de pilha-dupla. O modelo apresentado também referencia um plano de endereçamento chamado *leftmost*, além dos protocolos necessários. Traz-se um referencial bibliográfico e implementação dos protocolos de roteamento utilizado nas redes dos ISPs, como OSPF, BGP, além dos serviço de DNS.

Por fim o estudo apresenta um passo-a-passo com a configuração efetuada nos ativos de rede, assim como testes de ping, traceroute, e consulta DNS que evidenciam o funcionamento do modelo proposto pelo autor.

Assim como Santos, Moss (2015) também trouxe um modelo para implementação de Ipv6 em um provedor de internet que já possui Ipv4, mas ambos executados um período onde não havia o esgotamento do IPv4 e servidores de cache CDN nos provedores mencionados.

3.4 CONSIDERAÇÕES SOBRE OS ESTUDOS

Observa-se a partir dos resultados e conclusões apresentados nos trabalhos relacionados apresentados que o Ipv6 ainda é objeto de estudo, assim como as técnicas que permitirão a transição entre protocolos. Tem-se até o momento a pilha dupla como a técnica adotada na maioria dos estudos, e que mais se vê implementada em cenários reais onde o protocolo já está rodando, principalmente pela sua escalabilidade frente as técnicas de tunelamento.

Não se encontrou nos estudos apresentados impactos para a operação dos provedores no que diz respeito a necessidade de armazenamento de log de acesso do CGNAT por pelos menos 12 meses, visto que é uma exigência legal vinculada a lei do Marco Civil da Internet. Não se encontrou nos estudos anteriores citando provedores de internet a presença de CDNs nas redes dos provedores, e por isso não houve uma análise de como o Ipv6 se comporta na rede em relação ao acesso aos serviços dos provedores de conteúdo como Google, Netflix e Facebook, que estão hospedados nos provedores.

4 PROCEDIMENTO METODOLÓGICO

A metodologia a ser seguida neste trabalho tem caráter de pesquisa de natureza aplicada, pois apresenta uma solução onde gera conhecimento que pode ser aplicado de forma prática e imediata. No que diz respeito ao objetivo de estudo, o trabalho será realizado através de uma pesquisa exploratória. Inicialmente será realizada uma pesquisa bibliográfica sobre um referencial teórico e um estudo de cenário onde o objeto deste estudo ainda não foi aplicado completamente, visando embasar a proposta do trabalho como uma real necessidade do mercado para o crescimento das redes (Prodanov. Freitas, 2013).

Após a pesquisa teórica sobre os assuntos citados e o estudo de um cenário, será realizada uma pesquisa das técnicas de implementação do Ipv6, assim como técnicas que possibilitaram a longevidade do Ipv4. Após isso, será reproduzido em um simulador um ambiente de rede de um provedor regional, possibilitando que os testes de implementação ocorreram de forma a não impactarem em um ambiente de produção.

Elaboração da topologia e plano de endereçamento para todos os roteadores de acesso do provedor.

Com o cenário montado e os testes de comunicação em Ipv6 dos elementos de rede do provedor funcionando, o laboratório de testes será ampliado para contemplar os testes de entrega de Ipv6 para o usuário final, saindo dos elementos de rede do provedor até a CPE do cliente e então até o dispositivo do cliente. Será verificado no cenário tabela de distribuição de rotas, tanto IPv4 quanto IPv6.

Assim que este ambiente for finalizado e tiver o seu funcionamento validado, este estudo verificará na prática os testes que demonstrem o funcionamento do IPv6 ao acesso de conteúdos na internet. Será efetuado um teste de navegação apenas com IPv6, a fim de verificar o comportamento em relação a navegação, em sites de bancos, universidades e provedores de conteúdo como Netflix, Facebook e Google. Após a análise dos resultados dos testes propostos, a pesquisa pretende responder a seguinte questão: Como aumentar a disseminação do IPv6 na internet através dos provedores regionais na era do esgotamento total do IPv4?

Devido às etapas de análise e coleta de informações citadas anteriormente, este trabalho se propõe a uma pesquisa qualitativa, visto que serão coletadas informações

sobre o ambiente de produção proposto, além deste estudo se apropriar do resultado obtido com o estudo dos cenários para produzir um modelo de processo a ser aplicado nos provedores regionais (Prodanov. Freitas, 2013).

5 ESTUDO DE CASO

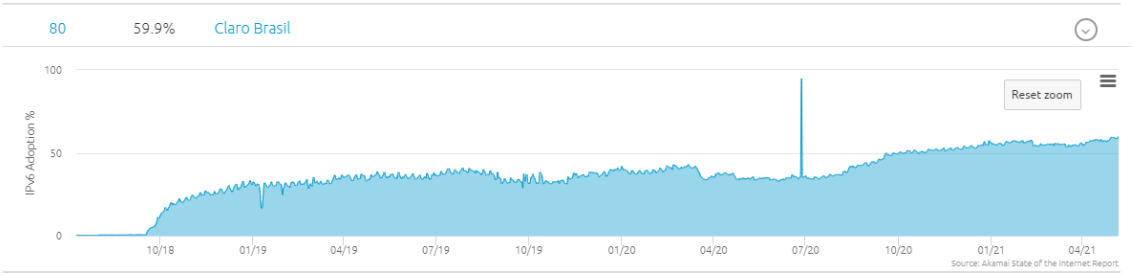
Neste capítulo será descrito toda atividade prática desenvolvida no provedor TCA Internet (ASN 53137) para realizar a implementação do protocolo de endereçamento IPv6 em um segmento da rede, estendendo este endereçamento até os dispositivos do cliente final.

Este estudo de caso motivou-se pela necessidade da implementação do protocolo IPv6, associada a contribuição acadêmica de um estudo com cenário atual e sem possiblidade de alocação de novos endereços IPv4.

Com este cenário exposto, viu-se a necessidade de entender como está a adoção de IPv4 no Brasil e no mundo. Dados levantados na plataforma 6lab da Cisco e no serviço de estatísticas mantido pelo Google (google.com/intl/pt-BR/ipv6/statistics.html#tab=per-country-ipv6-adoption), apontam uma adoção em torno de 38% de usuário navegando em IPv6 no Brasil (CISCO, 2021) (GOOGLE, 2021).

A Akamai mantém um ranking de adoção de IPv6 por países. Estados Unidos estão na primeira colocação com 68% do usuário ativos, o Brasil se encontra na décima terceira posição. Porém se formos analisar mais detalhadamente como o Brasil está nesta posição, vê-se que é puxado pelas grandes operadoras, conforme exemplificado pela figura 15, a Claro é a maior operadora do país e está com quase 60% dos seus usuários navegando em IPv6. Então, esta soma das grandes operadoras como Vivo, Claro e Oi contribuem para a escalada do Brasil no ranking, mas deixam uma dúvida sobre o que pode estar limitando os provedores menores a contribuir para a disseminação do IPv6 (AKAMAI, 2020).

Figura 15 – Adoção IPv6 por operadora



Fonte: AKAMAI, 2021

O site *iot-now.com* traz uma matéria de julho de 2020 chamada "*Why IPv6 adoption is still light years away*", onde o redator traz uma série de dificuldades levantadas para a adoção do IPv6, entre elas estão a limitação de investimentos, principalmente em tempos de pandemia onde seria difícil para que empresas renovem seu parque tecnológico para equipamentos mais novos com o suporte ao protocolo, além de aplicações legadas que também precisariam ser atualizadas. Outro ponto trazido é sobre não haver benefícios para os *Early adopters*, ou seja, para os primeiros a adotarem o novo protocolo, esta questão trouxe um gancho para alguns pontos que serão apontados por este trabalho, onde se percebe algumas desvantagens em ser o primeiro a adotar (IOT-NOW, 2020).

5.1 REQUISITOS

Inicialmente se levantou os requisitos para que a implementação pudesse ser desenvolvida em sua totalidade, tais requisitos são:

- Um plano de endereçamento para distribuição da redes IPv6.
- Recebimento de rotas IPv6 via protocolo eBGP dos Upstreams.
- Propagação das rotas IPv6 na internet via protocolo eBGP.
- Protocolo de roteamento interno.
- Validação das configurações na CPE (*CUSTOMER PROVIDER EDGE).*
- Controle de autenticação via servidor RADIUS e definição do bloco IPv6 a ser entregue ao cliente.

Os arquivos de configuração serão disponibilizados em formato texto nos apêndices deste trabalho. Os endereços IPv6 apresentados neste estudo foram substituídos pelo prefixo de documentação 2001:db8::/32, por questões de segurança. O endereços reservados para documentação são descritos na RFC 3849 (IETF, 2004).

5.2 PLANEJAMENTO

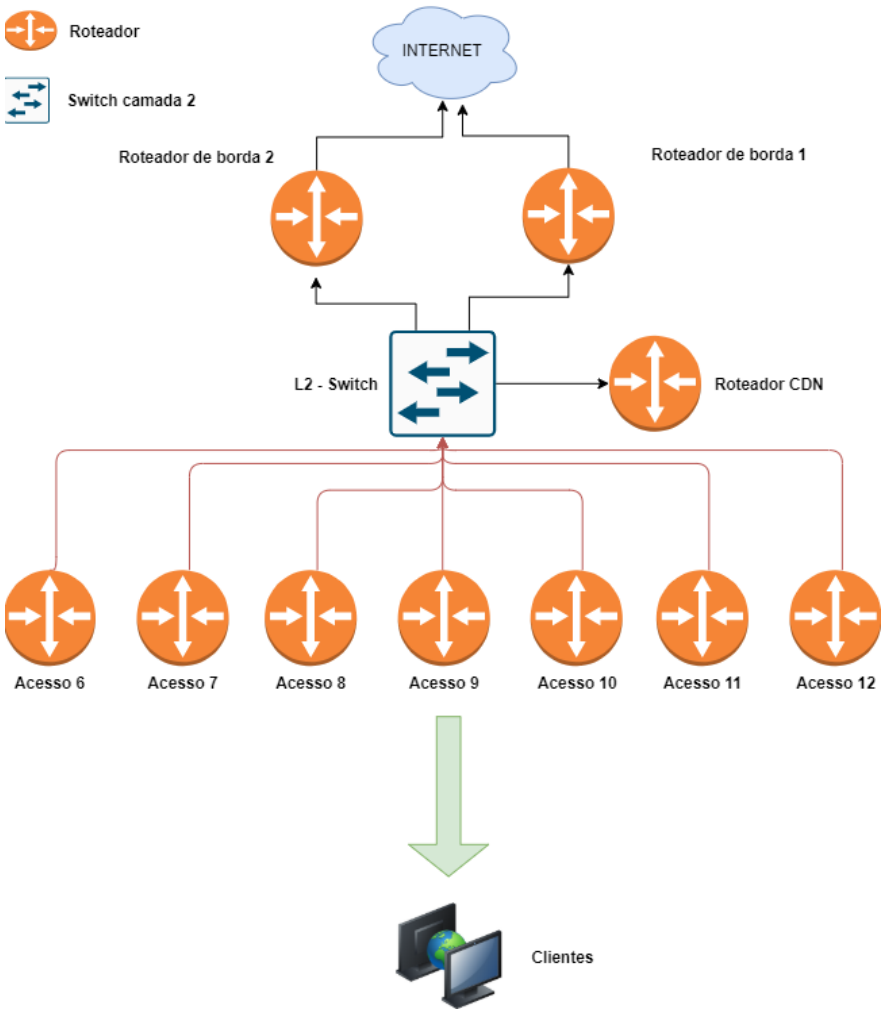
Na fase de planejamento, identificou-se a atual topologia da rede assim como o plano de endereçamento IPv4 que está implementado nos roteadores de acesso. Esta rede possui uma particularidade, uma vez que não há CGNAT rodando na rede, todos os clientes recebem um IPv4 público, desta forma não havendo o compartilhamento de IP nem divisão de portas para acesso à internet. Atualmente cada um dos sete roteadores de acesso possui uma rede pública IPv4 /22, totalizando 1024 IPs para distribuir aos clientes.

Conforme consulta na ferramenta de *whois* do registro.br o AS 53137 possui os blocos IPv4 186.193.160.0/20, 177.107.160.0/20, 200.34.224.0/19, 170.246.200.0/22, totalizando 17408 endereços. O bloco IPv6 designado conforme consulta é o 2804:33c::/32 (whois.registro.br).

5.3 TOPOLOGIA

Para esta etapa, segue-se o mesmo padrão de topologia que já está implementado em IPv4 (figura 16). Propõem-se a implementação OSPFv3 e iBGP em IPv6, na topologia existente para haver comunicação IPv6 entre os roteadores de acesso e os roteadores de borda. São 2 roteadores de borda configurados em *full-mesh* entre eles.

Figura 16 – Topologia



Fonte: Elaborada pelo autor

Utilizou-se o seguinte plano de endereçamento para fazer a comunicação via BGP entre as WANs dos roteadores de acesso e a borda 1 (quadro 1).

Quadro 1 –Redes de enlace para sessões BGP borda 1

Borda 1-> Acesso 6	2001:db8:504/64
Borda 1-> Acesso 7	2001:db8:503/64
Borda 1-> Acesso 8	2001:db8:502/64
Borda 1-> Acesso 9	2001:db8:510/64

Borda 1-> Acesso 10	2001:db8:507/64
Borda 1-> Acesso 11	2001:db8:511/64
Borda 1-> Acesso 12	2001:db8:513/64

Fonte: Elaborada pelo autor

Para comunicação entre os roteadores de acesso e a borda se utilizou as seguintes redes (quadro 2).

Quadro 2 –Redes de enlace para sessões BGP borda 2

Borda 2-> Acesso 6	2001:db8:504/64
Borda 2-> Acesso 7	2001:db8:503/64
Borda 2-> Acesso 8	2001:db8:502/64
Borda 2-> Acesso 9	2001:db8:510/64
Borda 2-> Acesso 10	2001:db8:507/64
Borda 2-> Acesso 11	2001:db8:511/64
Borda 2-> Acesso 12	2001:db8:513/64

Fonte: Elaborada pelo autor

Designou-se uma rede /64 para WAN, onde o primeiro IP de cada rede foi alocado para o roteador de borda, e o segundo IP para o roteador de acesso. Levando em consideração o cenário atual de rede do provedor, além do roteador de borda para comunicação com os Upstreams de trânsito, há também na rede um roteador de CDN. Este roteador é responsável por conectar à rede do provedor aos servidores de cache de provedores de conteúdo, neste caso Netflix e Google. Necessitando assim também da configuração de um enlace entre cada roteador de acesso

Posteriormente foi designado também uma rede /40 por roteador de acesso para ser distribuída aos clientes conectados (quadro 3). Na topologia da rede em estudo não há distinção por cidade ou região para distribuição dos IPs, portanto, clientes de uma mesma cidade podem se conectar em roteador diferentes, assim como clientes de cidades

diferentes podem se conectar em um mesmo roteador. Por este motivo a se definiu uma rede por roteador e não por região ou cidade.

Quadro 3 – Endereços para os clientes por roteador

Roteador acesso 6	2001:db8:7600::/40
Roteador acesso 7	2001:db8:7700::/40
Roteador acesso 8	2001:db8:e8000::/40
Roteador acesso 9	2001:db8:e9000::/40
Roteador acesso 10	2001:db8:ea00::/40
Roteador acesso11	2001:db8:7b00::/40
Roteador acesso 12	2001:db8:eb00::/40

Fonte: Elaborada pelo autor

Com as redes /64 estabelecidas para os enlaces entres os roteadores de acesso e o roteador de borda, e com as redes a serem entregues para as LANs dos clientes também definidas por roteador, o passo seguinte é validar as capacidades da CPE utilizada na rede.

A rede foi criada toda com um padrão de equipamento e configuração, onde a CPE no cliente é configurada em modo roteador, autenticando um usuário *PPPOE* e fazendo toda a função de gateway da rede do cliente. O modelo predominante na rede atualmente é da fabricante Park modelo Fiberlink 1100. Apesar de haver outros modelos da mesma fabricante na rede, os testes que serão descritos na seção 6.4 foram feitos em um cliente utilizando o modelo Fiberlink 1100. Por padrão criado como boa prática dentro da empresa, a rede interna do cliente em questão está configurada em modo *bridge*, com dispositivos conectados via *wireless* e cabo.

O protocolo *Point-to-Point Protocol over Ethernet* (PPPOE) é descrito na RFC 2516 (IETF). É um protocolo que roda em cima de camada 2, utilizado principalmente pela sua facilidade de gerenciamento e integração com o ERP do provedor. Com a utilização do

PPPOE é possível associar as conexões dos clientes a um usuário e senha, possibilitando a utilização do servidor RADIUS para controle das autenticações (MIKROTIK).

5.4 EXECUÇÃO

Após a etapa de planejamento, com todas as redes definidas, iniciou-se a parte de configuração dos equipamentos envolvidos na topologia. Decidiu-se previamente utilizar as mesmas VLANs da rede IPv4 pois o caminho entre o roteador de acesso e o roteador de borda já está configurado, e desta forma é possível compartilhar a mesma interface física com mais de uma rede, seja ela IPv4 ou IPv6. Nessa topologia são duas VLANs na mesma interface, uma para o roteador de borda 1 e outra para o roteador de borda 2.

VLAN é uma rede virtual local onde um grupo de dispositivos é configurado para funcionar como se estivessem conectados à mesma rede física, quando na realidade estão localizados em uma série de locais diferentes. A VLAN separa os dispositivos em domínios de broadcast diferentes, através da atribuição de Ids para os segmentos da rede (CISCO). A exemplo da configuração do cenário em questão, cada comunicação entre um roteador de acesso e roteador de borda está em um domínio de broadcast diferente definido por um Id de VLAN.

5.4.1 CONFIGURAÇÃO DO OSPFV3

O OSPF será o protocolo utilizado para o recebimento da rota *default* dos roteadores de acesso, e anúncio dos prefixos IPv6. Este será implementado utilizando a mesma instancia OSPF tanto em IPv4 quanto em IPv6, porém o recebimento das rotas IPv4 continuarão sendo via OSPFv2, e as rotas IPv6 serão via OSPv3.

O OSPF é um protocolo do tipo *Link State*, ou estado de enlace, portanto para haver a comunicação *P-2-P* entre os nós se faz necessário adicionar as interfaces vizinhas à mesma área OSPF (Kurose. Ross, p.290, 2010). Neste modelo de configuração foram adicionadas as interfaces lógicas, tanto para comunicação com o primeiro roteador de borda, quanto para o segundo roteador de borda, onde cada um possui um TAG de VLAN específico conforme definido e apresentado no quadro 4 e no quadro 5.

As interfaces da comunicação ponto-a-ponto entre os roteadores foram adicionadas a área OSPF e a adjacência estabelecida para troca de rotas internas de forma dinâmica. Definiu-se juntamente a esta configuração um custo maior para a comunicação com o

roteador identificado como Borda2, assim priorizando o tráfego de upload para o roteador identificado como Borda1.

Os roteadores de acesso receberão somente rota *default* e as rotas compartilhadas por OSPF dos roteadores de borda. Somente os roteadores de borda terão a tabela completa de roteamento recebida pelo Upstreams.

Uma particularidade é que não há comunicação via OSPF entre os roteadores de acesso e o roteador denominado como CDN. O anúncio das rotas para este roteador é feito via BGP. Esta configuração foi definida pois o roteador de CDN conecta a rede da TCA (AS53137) com a rede de conteúdo do Google (AS11344) e Netflix (AS40027), assim como outros clientes provedores de internet que compram internet da TCA e revendem, então se padronizou o BGP como protocolo para troca de rotas, assim cada roteador de acesso da TCA é tratado como um cliente do roteador de CDN, facilitando a operação da rede.

5.4.2 CONFIGURAÇÃO DO BGP4

Para que haja comunicação entre a rede do provedor e a internet é preciso configurar as sessões eBGP entre o roteador de borda do provedor e os fornecedores contratados. É através das sessões BGP que as redes IPv4 e IPv6 do provedor serão anunciadas, e por onde serão aprendidas as rotas paras os destinos da internet (Kurose. Ross, p.291 2010).

Primeiramente para se configurar o BGP é preciso estabelecer a conexão entre o AS do provedor com o AS do fornecedor/upstream. A maior parte das vezes o upstream designa uma rede de enlace, onde um IP da rede fica configurado do lado dele, e outro IP no lado do cliente provedor (Ipv6.br 2012).

O BGP é um protocolo extremamente complexo que conecta toda a internet (Kurose. Ross, 2010), e são através dos filtros BGP que os Sistemas Autônomos têm a capacidade de gerir o tráfego que entra e sai do seu domínio. Alguns roteadores são permissivos, caso nenhum filtro seja aplicado, aceitam tudo o que seus vizinhos enviam, e enviam tudo o que tem de informação também. É uma boa prática configurar filtros de entrada e de saída para cada vizinho BGP antes de estabelecer qualquer sessão (BCP.Nic.br).

O filtro de *bogons* é uma boa prática aplicada em casa sessão conectada. Os bogons são prefixos que não deveriam aparecer na tabela BGP (NIC.br). Estão contidos nos *bogons* endereços privados e endereços reservados definidos na RFC 1918, RFC 5735 e RFC 6598. Um estudo conduzido pela entidade sem fins lucrativos *Team CYMRU* investigou um site frequentemente atacado, e descobriu que 60% dos pacotes maliciosos com destino a este site eram oriundos de *bogons* (Ex: 127.1.2.3, 0.5.4.3, etc.) O filtro de *bogons* é um componente de *anti-spoofing*. Ataques DDOS são comumente originados de redes *bogons* que sofreram *spoofing* para alterar sua origem e não deixar rastro de origem do ataque (TEAM-CYMRU).

Em relação aos filtros de entrada do IPv,6 pode-se bloquear tudo por padrão e permitir somente o prefixo 2000::/3. Ou para seguir o mesmo padrão do IPv4, pode-se especificamente bloquear as redes que não deveriam ser roteadas na internet (BCP.Nic.br).

- :: /0
- :: /128
- ::1/128
- ::ffff:0:0/96
- 0100::/64
- 2000::/3
- 2001::/32
- 2001:10::/28
- 2001:db8::/32
- 2002::/16
- fc00:: /7
- fe80:: /10
- ff00:: /8

Tem-se no cenário também filtros de entrada para bloqueio de ASN privados ou reservados (Figura 17).

Figura 17 – ASN *bogons* e respectiva RFC

```
>     0                    # Reserved RFC7607
>     23456                # AS_TRANS RFC6793
>     64496-64511          # Reserved for use in docs and code RFC5398
>     64512-65534          # Reserved for Private Use RFC6996
>     65535                # Reserved RFC7300
>     65536-65551          # Reserved for use in docs and code RFC5398
>     65552-131071         # Reserved
>     4200000000-4294967294   # Reserved for Private Use RFC6996
>     4294967295           # Reserved RFC7300
```

Fonte: RIPE, 2021

Seguindo com a configuração do protocolo BGP, parte-se para configuração do iBGP, por um padrão criado na empresa, utilizou-se o primeiro IP de cada rede no lado do roteador de borda e o segundo IP no lado do roteador de acesso. Os endereços foram configurados na VLAN designada para estabelecer a comunicação entre a borda 1 e os roteadores de acesso (quadro 4).

Quadro 4 – IPs de enlace borda 1

VLAN	IP BORDA 1	IP ACESSO
504	2001:db8:30:504::1/64	2001:db8:30:504::2/64
503	2001:db8:30:503::1/64	2001:db8:30:503::2/64
502	2001:db8:30:502::1/64	2001:db8:30:502::2/64
510	2001:db8:30:510::1/64	2001:db8:30:510::2/64
507	2001:db8:30:507::1/64	2001:db8:30:507::2/64
511	2001:db8:30:511::1/64	2001:db8:30:511::2/64
513	2001:db8:30:513::1/64	2001:db8:30:513::2/64

Fonte – Elaborada pelo autor

Seguiu-se mesmo padrão de configuração para o roteador de borda 2 e os respectivos roteadores de acesso (quadro 5).

Quadro 5 – IPs de enlace borda 2

VLAN	IP BORDA 2	IP ACESSO
504	2001:db8:30:524::1/64	2001:db8:30:524::2/64
503	2001:db8:30:523::1/64	2001:db8:30:523::2/64
502	2001:db8:30:522::1/64	2001:db8:30:522::2/64
510	2001:db8:30:530::1/64	2001:db8:30:530::2/64
507	2001:db8:30:527::1/64	2001:db8:30:527::2/64
511	2001:db8:30:521::1/64	2001:db8:30:521::2/64
513	2001:db8:30:533::1/64	2001:db8:30:533::2/64

Fonte – Elaborada pelo autor

Com as redes de enlaces configuradas, as sessões iBGP foram estabelecidas.

5.5 RESULTADOS

Com a etapa de configuração concluída, foi possível realizar os testes na rede e validar o ambiente de produção. Foram levantadas as tabelas de rotas BGP IPv4 e IPv6, o estado da adjacência e distribuição de rotas pelo IGP (OSPF), distribuição dos prefixos IPv6 do provedor para a internet através de servidores *looking glass*, testes de ping e traceroute, testes de navegação em *dual-stack* e testes de navegação somente em IPv6.

Os testes de recebimento do prefixo de WAN em um cliente final foram executados na CPE do cliente, um equipamento Parks Fiberlink 1100 configurado em modo *router*, assim como o teste de funcionamento do DHCPv6-PD, onde ocorre a entrega da rede para os dispositivos da rede interna. Já os testes para validação da navegação em *dual-stack* e somente IPv6 foram executadas em um laptop com Windows 10. Os endereços IPv6 apresentados tanto no planejamento quanto nos testes são endereços reais do provedor e podem ser consultados nas tabelas globais de roteamento.

5.5.1 TABELAS DE ROTAS

A primeira verificação é a tabela de rotas IPv6 coletada no roteador borda 1 da fabricante americana *Juniper Networks*. Na figura 17 estão aparecendo um total de 487.746 rotas IPv6. Isto se dá pois há vários *peer* BGP IPv6 com fornecedores. Desta forma há mais de 1 rota para o mesmo destino, por isto vemos 119.092 destinos e 487.746 rotas.

Figura 18 – Tabela de rotas IPv6

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed May 26 18:09:23 2021 from 186.193.160.27
--- JUNOS 15.1R5-S4.2 built 2017-05-24 19:20:27 UTC
admin@bord01.tqr> show route table inet6.0

inet6.0: 119092 destinations, 487746 routes (118751 active, 0 holddown, 210678 hidden)
+ = Active Route, - = Last Active, * = Both
```

Fonte: Elaborado pelo autor

Em relação as rotas IPv4 se tem o mesmo cenário, múltiplos *peers* BGP e mais de uma rota para o mesmo destino. Tem-se então 850526 destinos para um total de 3.3372.736 rotas. Tem-se 849.340 rotas ativas neste roteador, que é o número total de rotas da tabela global.

Figura 19 – Tabela de rotas IPv4

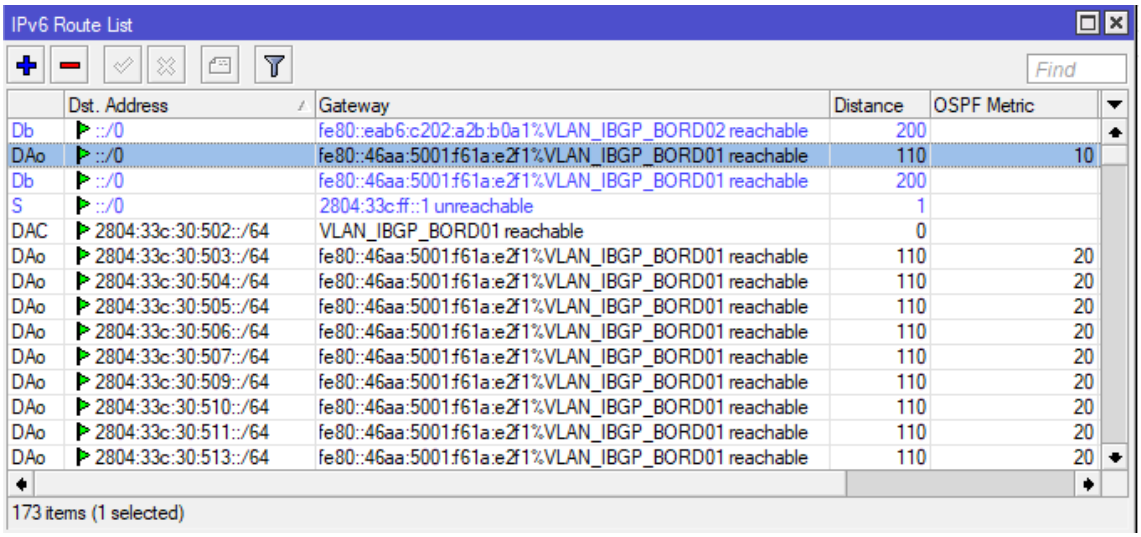
```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed May 26 18:14:51 2021 from 186.193.160.27
--- JUNOS 15.1R5-S4.2 built 2017-05-24 19:20:27 UTC
admin@bord01.tqr> show route table inet

inet.0: 850526 destinations, 3372736 routes (849340 active, 0 holddown, 365818 hidden)
@ = Routing Use Only, # = Forwarding Use Only
+ = Active Route, - = Last Active, * = Both
```

Fonte: Elaborado pelo autor

Com as tabelas de rotas externas validadas e funcionando, verifica-se a tabela de rotas internas com a distribuição dos prefixos pelo IGP (OSPF) e o aprendizado da rota *default* nos roteadores de acesso. Havendo estas informações é possível validar o funcionando do protocolo OSPF, com a adjacência entre nós estabelecida (Figura 20).

Figura 20 – Tabela de rotas IPv6 no roteador de acesso



Fonte: Elaborada pelo autor

A sigla *DAo*, na primeira coluna da tabela de rota, significa que a rota foi aprendida de forma dinâmica pelo protocolo OSPF e está ativa (MIKROTIK). Também é possível ver um total de 173 rotas IPv6.

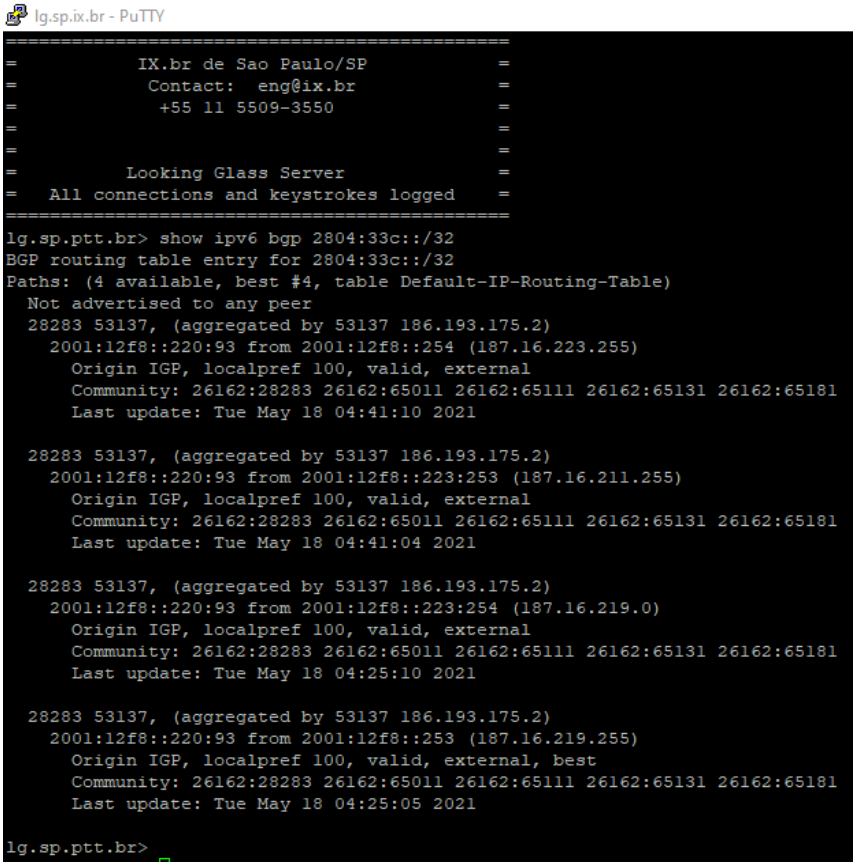
Na quarta linha da tabela de rotas se percebe o prefixo 2001:db8:ff::1 que está com o *status* de *unreachable*. Isto se dá pelo problema "IPv6 *recursive nexthops via iBGP*", onde não há rota recursiva no IPv6, ou seja, se o próximo salto não estiver em uma interface diretamente conectada, a rota fica inalcançável. Por este motivo as sessões BGP IPv6 são fechadas pelas redes de enlace e não pelo IP de *Loopback*, como é feito nas sessões IPv4.

Outro teste realizado para validação da propagação das rotas do provedor para a internet é feito através do servidor de *Looking Glass* do IX-BR em São Paulo. Através do comando "*show ipv6 bgp* 2001:db8::/32" é possível ver que o servidor de rotas do IX de São Paulo está aprendendo o bloco IPv6 e consequentemente repassando este prefixo para os outros participantes conectados a infraestrutura do IX-BR em São Paulo (Figura 21).

O IX-BR, ou *Internet Exchange*, de São Paulo é hoje um dos maiores ponto de troca de tráfego do mundo. É uma iniciativa do CGI.br e do NIC.br, que implanta e promove infraestrutura necessária para proporcionar interconexão entre as redes que compõem a internet no Brasil (IX.br). Em 16 de março de 2021 o IX-BR bateu recorde ao atingir 16 Tbit/s de pico de tráfego internet (IX.br, 2021).

Em uma consulta recente o IX-BR de São Paulo possuía 2295 participantes (IX.br). Estes participantes recebem e anunciam suas rotas para outros participantes através da infraestrutura do IX, e para que administradores de rede tenham como consultar quais redes estão ativas no ATM (Acordo de Troca Multilateral) a equipe do IX.br mantém os servidores de *Looking Glass*. Estes servidores são fonte em tempo real de informações de rotas BGP, eles coletam informações dos roteadores que falam BGP e armazenam para ser mostrado como fonte de consulta (IX.br, 2021) (NOCTION, 2021).

Figura 21 - *Looking Glass* IX-BR-SP



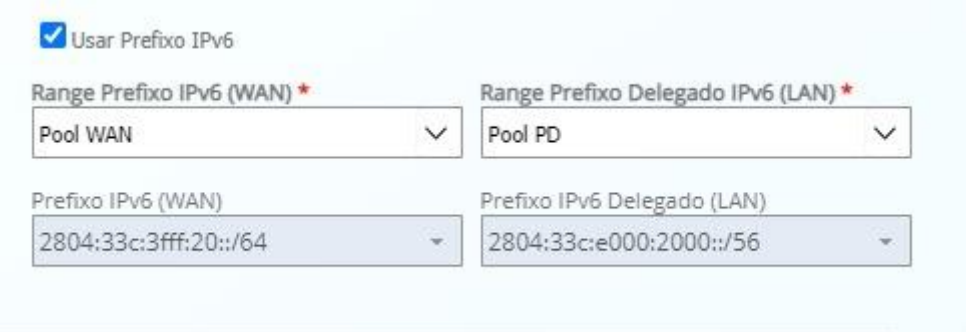
Fonte – Elaborada pelo autor

Após validado os testes de distribuição de rotas, tanto internas quanto externas do provedor, iniciou-se a etapa de configuração para que o cliente final possa usufruir do IPv6 em seus dispositivos na rede interna.

5.5.2 ENDEREÇAMENTO

Para isto foi preciso habilitar na conexão do cliente dentro do ERP Mksolutions utilizado pela empresa, que o cliente utilizaria prefixo IPv6, tanto na WAN quanto na LAN (Figura 22).

Figura 22 – Pool WAN e PD



Fonte: Elaborada pelo autor

O ERP possui integração com um servidor RADIUS que também é fornecido pela Mksolutions. RADIUS (*Remote Authentication Dial In User Service)* é um protocolo de autenticação que se baseia em pergunta e resposta, e utiliza o protocolo UDP para comunicação entre cliente e servidor. O RADIUS se utiliza de atributos que contém dados específicos para autorizar o cliente na rede e conceder acesso a determinados tipos de serviço, como por exemplo controle de banda (Teleco.com.br). Traz-se em sequência o LOG de autenticação do usuário que que foi configurado no ERP para receber IPv6 (Figura 23).

Figura 23 – LOG servidor Radius

```
Fri May 21 11:46:26 2021
        Packet-Type = Access-Accept
        Framed-Protocol = PPP
        Framed-Compression = Van-Jacobson-TCP-IP
        Framed-IP-Address == 200.34.227.241
        Framed-IPv6-Prefix := 2804:33c:3fff:20::/64  (entre bng e a wan cpe)
        Mikrotik-Delegated-IPv6-Pool := "2804:33c:e000:2000::/56"
        Acct-Interim-Interval == 900
        Mikrotik-Rate-Limit == "117m/390m 0k/0k 0k/0k 0/0 8 0K/0K"
        Simultaneous-Use == 1
```

Fonte: Elaborada pelo autor

Neste trecho de LOG é possível ver a hora que a autenticação ocorreu, o tipo de pacote, o protocolo PPP, o tipo de compressão utilizada pelo serviço, o IPv4 atribuído a conexão, o controle de velocidade, além do prefixo IPv6 utilizado entre a WAN da CPE e o roteador, assim como o pool IPv6 delegado para LAN.

Percebe-se uma particularidade neste LOG do servidor Radius. A entrega do prefixo IPv6 a ser delegado para LAN está sendo feita pelo atributo **Mikrotik-Delegated-IPv6-**

Pool, ao invés do parâmetro **Delegated-ipv6-Prefix.** Isto ocorre devido a um problema conhecido do roteador Mikrotik não tratar este parâmetro Radius (FORUM.MIKROTIK).

Para contornar é preciso então enviar por parâmetro Radius um pool IPv6 e cadastrar manualmente este pool nos roteadores (Figura 24).

Figura 24 – *Pool* IPv6 fixado no roteador

```
26  [vlinden@Aces08-PPPoE] > ipv6 pool print
27  Flags: D - dynamic
28   #    NAME                                      PREFIX
29  31   2804:33c:e000:2000::/56                   2804:33c:e000:2000::/56
30  [vlinden@Aces08-PPPoE] >
```

Fonte: Elaborada pelo autor

Com esta configuração replicada nos outros seis roteadores de acesso, independentemente de o cliente se autenticar em roteadores diferentes ele sempre receberá o mesmo prefixo na LAN.

A Mikrotik sugere uma configuração diferente e uma versão de software beta para contornar o problema, mas este teste não será executado neste estudo.

5.5.3 TESTES UTILIZANDO ICMP

O protocolo *Internet Cntrol Message Protocol* (ICMP) é um integrante do protocolo IP, definido na RFC 792. Equipamentos de rede utilizam deste protocolo para comunicar problemas na rede. Por exemplo, se um pacote maior que um roteador pode trafegar na rede é transmitido a ele, este roteador descarta o pacote e envia uma mensagem através do ICMP informando o problema. Em IPv6 o ICMPv6 agrega também funcionalidade que antes eram protocolos separados em IPv4, tais como ARP, RARP e IGMP (Ipv6.br 2012).

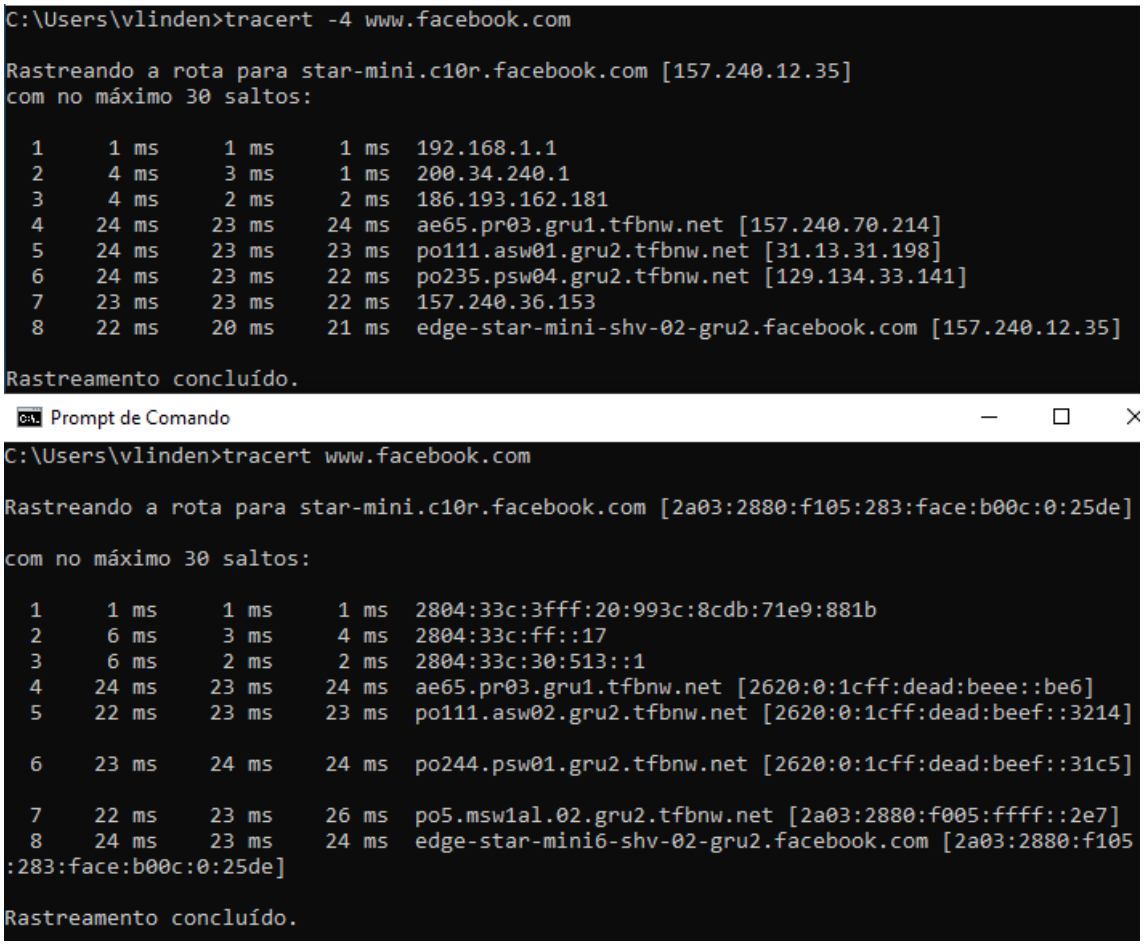
O protocolo ICMPv6 também é utilizado pelas seguintes funcionalidades:

- NDP (*Neighbor Discovery Protocol).*
- *Path MTU Discovery.*
- *Mobility Support.*
- Autoconfiguração *Stateless*
- MLD (*Multicast Listener Discovery)*

Com os testes de rotas e o teste de entrega de IPv6 ao cliente final validados, foi possível testar a internet a partir dos equipamentos da rede interna. Um teste para validar

o funcionamento da pilha feito foi o teste utilizando o utilitario *ping*, onde é possível validar a conectividade com o host de destino. Outro teste realizado em sequência, que também utiliza o protocolo ICMP, foi o teste de *traceroute*. Com ele é possível mapear os saltos desde a origem do pacote até o host de destino. Estes testes foram executados também para validar o funcionamento da pilha dupla.

Figura 25 – Teste de PING e TRECEROUTE



Fonte: Elaborada pelo autor

Percebe-se que não houve alteração de caminho percorrido para alcançar o host *www.facebook.com*, assim como o tempo de resposta para cada um dos hosts do caminho em IPv6 praticamente não tem diferença quando comparado com o IPv4.

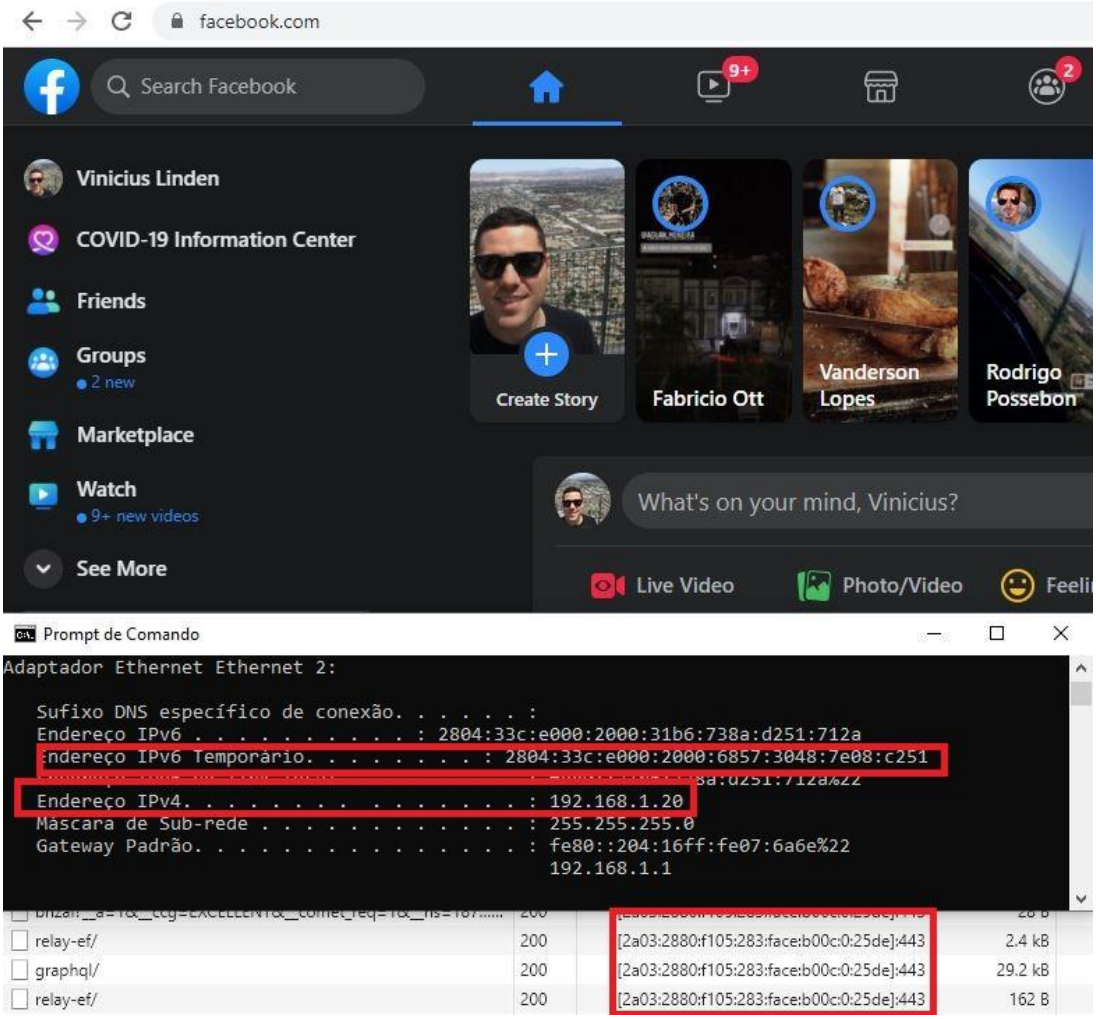
5.5.4 TESTES DE NAVEGAÇÃO

Nos testes de navegação se constatou a preferência das aplicações em utilizar o IPv6 sobre o IPv4. Inicialmente os sistemas operacionais por padrão priorizavam a conexão IPv6 e só fariam a tentativa em IPv4 em caso de timeout da conexão IPv6. Desta forma

havia uma penalização grande na experiencia de uso do usuário final, causada pelo atraso na abertura de um site, por exemplo (Ipv6.br 2012).

Para tentar corrigir estes problemas de decisão de conexão surgiu o algoritmo *Happy Eyeballs*, definido na RFC 6555. Seu funcionamento consiste em tentar a conexão nos dois protocolos e utilizar a que for estabelecida mais rapidamente, dando uma pequena preferência para o IPv6. Este algoritmo está implementado em navegadores como Google Chrome, Mozilla Firefox, Microsoft Edge, entre outros (IPv6.br 2012) (IETF.org). A figura 24 ilustra exatamente este comportamento, onde temos uma máquina Windows 10 rodando IPv4 e IPv6, acessando um vídeo do Youtube através do navegador Google Chrome e preferindo a conexão IPv6 para acessar conteúdo (Ipv6.br 2012).

Figura 26 - Testes de navegação em dual-stack



Fonte: Elaborada pelo autor

A lógica de funcionamento do algoritmo é a seguinte (Figura 27) (Ipv6.br 2012):

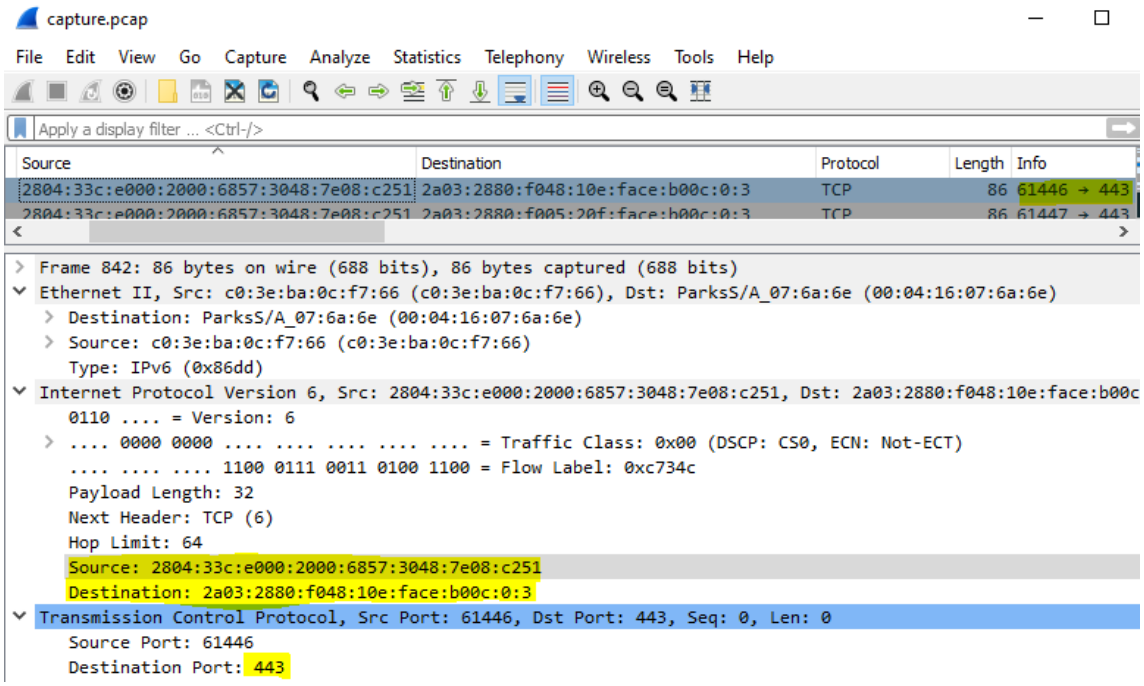
Figura 27 – Logico algoritmo *Happy-Eyebalss*

```
43  conectar (endereço) {
44              encontra IPs do endereço
45              tenta se conectar a o endereço IPv6
46              enquanto nenhuma conexão se estabelece e timeout não estoura {
47                      se passou tempo de vantagem dado ao IPv6 {
48                              tenta se conectar a um endereço IPv4 (uma única vez)
49                      }
50              }
51              se conseguiu conectar {
52                      mantém a conexão conectada
53                      fecha as demais conexões (sockets abertos)
54              } caso não conseguiu conectar (timeout) {
55                      fecha todas as conexões (sockets abertos)
56              }
57      }
```

Fonte: IPv6.br, 2012

O comportamento de prioridade do IPv6 sobre o IPv4 também pode ser verificado na coleta da ferramenta *TCP DUMP* feita a partir da CPE do cliente (Figura 28).

Figura 28 – Captura pacotes CPE



Fonte: Elaborada pelo autor

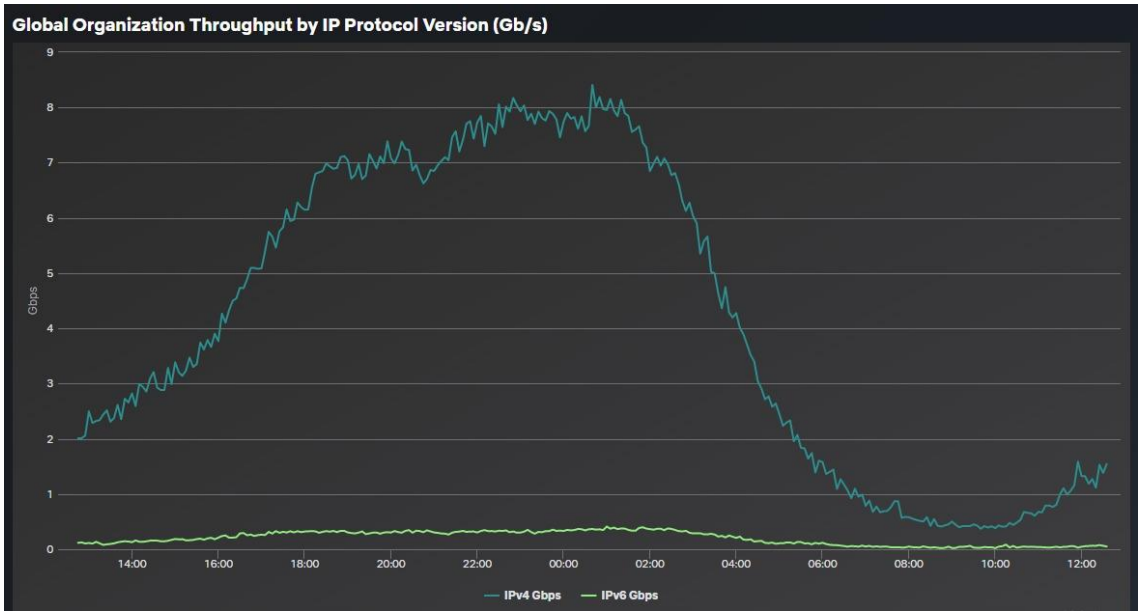
Executou-se este mesmo teste de navegação nos outros provedores de conteúdo, como UOL, Terra, Globo.com, Amazon, Netflix e o conglomerado do Facebook que inclui Whatsapp, Instagram e Messenger. Todos funcionaram perfeitamente em IPv6 sem qualquer diferença para melhor ou para pior em relação a performance.

Em contraste aos testes executados acima, encontraram-se resultados diferentes quanto ao funcionamento do IPv6 no site do banco Itau e da secretaria da fazenda do

estado do Rio Grande do Sul. No caso do Itau, encontra-se entrada DNS IPv6, porém ao se inspecionar o funcionamento do site, percebe-se que somente a *home page* responde em IPv6, após acesso à Internet Banking, todas as funcionalidades testadas fazem chamadas para endereços IPv4. Já o site do site da secretaria da fazenda do RS tem resposta diferente, neste caso não se encontra entrada DNS IPv6, e todos os links testados dentro do site também respondem somente IPv4.

Como a rede atualmente ainda possui uma baixa penetração de IPv6, percebe-se que os servidores de cache tem baixo tráfego neste protocolo, a maior parte do tráfego está em IPv4 (Figura 29). A linha verde indica o tráfego em IPv6 para o servidor do Netflix, e a linha azul que está chegando próximo aos 9Gbps, indica o tráfego em IPv4.

Figura 29 – Tráfego *cache* Netflix IPv4 e IPv6



Fonte: Elaborada pelo autor

Este comportamento de baixo tráfego nos servidores de cache CDN acontece também com os outros provedores, como Google e Facebook. Porém, percebe-se que há espaço para equilibrar o tipo de tráfego conforme a rede for recebendo mais clientes com IPv6.

CONCLUSAO

De acordo com os aspectos analisados e levantados no presente estudo de caso, em geral, o IPv6 parece se mostrar uma solução aplicável aos provedores de internet como alternativa ao esgotamento do IPv4. A técnica de pilha-dupla implementada neste estudo, permite o acesso a aplicações legadas em IPv4, e em IPv6 a aplicações que já implementam o novo protocolo internet. Esta técnica se mostra como uma solução para aumentar a disseminação do IPv6 pelos provedores regionais de internet.

Percebe-se a partir dos estudos realizados que a porcentagem de adoção de IPv6 no mundo está aumentando, e esta é uma tendência que deve continuar devido ao esgotamento total do IPv4. Não se encontrou ao longo deste estudo equipamentos que não estivessem aptos para receber o IPv6. Não foi necessário atualizar a versão de software ou substituir nenhum equipamento na rede para que se tivesse sucesso na implementação do IPv6.

No caso em estudo, implementou-se IPv6 no *backbone* e em um segmento da rede de acesso de um provedor com pouco mais de 6 mil clientes conectados. Com isso, percebe-se a importância de futuramente implementar IPv6 para o restante dos clientes já ativos e nos futuros novos clientes, pois desta forma é possível diminuir os custos em CGNAT e armazenamento de LOGs de conexão. Utilizou-se de um modelo de implementação diferente do que a grande maioria dos manuais e tutoriais encontrados na internet. Neste trabalho se utilizou do servidor *Radius* do ERP para fazer o controle de autenticação do usuário, via atributo *Radius* se enviou os prefixos IPv6 para o cliente. Os manuais e tutoriais encontrados internet utilizam o próprio roteador para entregar os prefixos IPv6, sem a existência de um servidor de autenticação para isso. Esta forma de implementação não foi testada neste trabalho devido a variação de cenário com múltiplos roteadores de acesso.

Os testes de navegação em pilha dupla confirmaram uma questão levantada no referencial teórico, em que se apontou sobre a prioridade do IPv6 sobre o IPv4, e principalmente quando trazido para a realidade dos provedores. O acesso aos servidores de conteúdo CDN da Netflix e Google e Facebook, que estão hospedados dentro do provedor, foram efetuados em IPv6, mesmo o cliente e o servidor tendo IPv4 e IPv6 configurado. No cenário analisado poderia se ter pelo menos 40% do tráfego total da rede em IPv6. Levando em consideração todos os clientes com pilha dupla, e levando em consideração também que 40% do tráfego total da rede se dá para destinos como Google,

Facebook e Netflix, e estes provedores de conteúdo tem servidor de cache CDN hospedado dentro da infraestrutura do ISP.

Desta forma foi possível cumprir com o objetivo geral, analisar como os provedores regionais podem contribuir para o crescimento da internet implementando IPv6 em um contexto de esgotamento total do IPv4. Os objetivos específicos também foram cumpridos em sua totalidade. Foi possível se apropriar do conhecimento sobre arquiteturas de redes de provedores de serviço de internet, e do conhecimento sobre o protocolo IPv6. Assim como foi proposto um modelo de implementação de IPv6 que atenda os clientes finais, realizar testes em um cenário real, coletar informações que serviram para identificar problemas no processo de execução da parte prática, e registrar soluções para contornar os problemas apontados.

Questões sobre segurança IPv6 não foram abordadas neste trabalho, mesmo que implementado filtros de *firewall* nos roteadores de acesso e de borda com regras básicas para bloqueio de portas de serviço, que não deveriam estar expostas à internet. Tem-se o espaço para aprofundar um estudo sobre questões de segurança. O Ripe traz em uma apresentação recente, datada de abril de 2021, sobre ameaças conhecidas do protocolo IPv6, como IP *Spoofing, Routing Header Threat, ICMPv6 Threats*, entre outras que valem um estudo mais aprofundado (RIPE, 2021).

Além de questões de segurança, o estudo aprofundado IPv6 abre possibilidade para trabalhos futuros relacionado ao ambiente de provedores de serviço, tais como *VPN* IP6 em cima de *MPLS*, *Segment Routing IPv6 (SRv6),* e *VxLANv6* (CISCO, 2019).

REFERÊCIAS BIBLIOGRÁFICAS

ADEYVISON, Mota de Sousa. **Implementação da técnica de pilha dupla para transição de redes IPv4 para redes IPv6**. Santa Catarina: IFSC, 2018.

AKAMAI. **O QUE é uma CDN?** Definição de CDN. 2020. Disponível em: https://www.akamai.com/br/pt/cdn/what-is-a-cdn.jsp. Acesso em: 18 out. 2020.

AKAMAI. **QUAIS são os benefícios de uma CDN?** 2020. Disponível em: https://www.akamai.com/br/pt/cdn/what-are-the-benefits-of-a-cdn.jsp. Acesso em: 28 out. 2020.

ALESSANDRO, Nucci de Siqueira. **Redes IPv6 e estratégia de implementação**. São Paulo: Universidade Presbiteriana Mackenzie, 2011.

ANATEL. **ANATEL simplifica regras para prestação do SCM**. 2017. Disponível em: https://www.anatel.gov.br/Portal/documentos/midias_teia/1897.pdf. Acesso em: 05 nov. 2020.

BRITO, Samuel. IPV6. **O Novo Protocolo da Internet**. 1ª ed. São Paulo: Novatec, 2013.

BUCCO, Rafael**. ISPS PASSAM A CLARO EM ASSINANTES DE BANDA LARGA FIXA**. 2020. Disponível em: https://www.telesintese.com.br/isps-passam-a-claro-em-numero-assinantes-de-banda-larga-fixa. Acesso em: 20 abr. 2021.

CISCO. **THE place to monitor IPv6 adoption**. 2021. Disponível em: <https://6lab.cisco.com/stats/cible.php?country=BR&option=all>. Acesso em 18 abr. 2021.

CISCO. **Túnel do IPv6 através de uma rede do IPv4**. 2006. Disponível em: https://www.cisco.com/c/pt_br/support/docs/ip/ip-version-6/25156-ipv6tunnel.html. Acesso em: 22 out. 2020.

CISCO. **Understanding and Configuring VLANs**. 2012. Disponível em: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ew/configuration/guide/config/vlans.pdf. Acesso em: 13 abr. 2021.

COLTUN, R. **OSPF for IPv6**. 2008. Disponível em: https://datatracker.ietf.org/doc/html/rfc5340. Acesso em: 12 abr. 2021.

D'MELLO, Anasia. **Why IPv6 adoption is still light years away**. 2020. Disponível em: https://www.iot-now.com/2020/07/22/104012-why-ipv6-adoption-is-still-light-years-away. Acesso em: 26 mar. 2021.

DUQUE, Luciano Henrique. **Banda Larga: Extração de Parâmetros da Qualidade do Serviço a partir do CDR (Call Detail Record)**. 2019. Disponível em: https://www.teleco.com.br/tutoriais/tutorialblcdr/default.asp. Acesso em: 10 abr. 2021.

FARINACCI, D. **Generic Routing Encapsulation (GRE).** 2020. Disponível em: https://tools.ietf.org/html/rfc2784. Acesso em: 10 nov. 2020

GLOBO. **Necessidade de internet mais rápida alimenta o mercado de provedores regionais. 2020**. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2020/08/11/necessidade-de-internet-mais-rapida-alimenta-o-mercado-de-provedores-regionais.ghtml. Acesso em: 15 nov. 2020.

GOOGLE. **CARRIER Grade NAT**. 2020. Disponível em: https://support.google.com/interconnect/answer/7658745?hl=en/. Acesso em: 05 nov. 2020.

IANA. **ETHERNET Numbers**. 2020. Disponível em: http://www.iana.org/assignments/ethernet-numbers/ethernet-numbers.xhtml. Acesso em: 05 nov. 2020.

IBGE. **POPULAÇÃO e Projeção. 2020**. Disponível em: https://www.ibge.gov.br/apps/populacao/projecao. Acesso em: 28 out. 2020.

IPV6.BR. **HAPPY Eyeballs**. 2012. Disponível em: http://ipv6.br/post/happy-eyeballs/. Acesso em: 20 maio 2021.

IX.BR. **IX.BR bate recorde histórico ao atingir 16 Tbit/s de pico de tráfego Internet**. 2021. Disponível em: https://ix.br/noticia/releases/ix-br-bate-recorde-historico-ao-atingir-16-tbit-s-de-pico-de-trafego-internet. Acesso em: 20 maio 2021.

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

LACNIC. **FASES de esgotamento do IPv4**. 2020. Disponível em: https://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4. Acesso em: 20 set. 2020.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 nov. 2020.

LEONARDO, Winckler de Bettio. **O crescimento da internet no Brasil, serviços e regulamentação**. Curitiba: UTFPR (Universidade Tecnológica Federal do Paraná), 2015.

MENDONÇA, Carlos Alberto Veríssimo de. **A Internet como Ferramenta de Negócios.** 2020. Disponível em: https://www.academia.edu/13225356/A_Internet_como_Ferramenta_de_Negocios. Acesso em: 15 maio 2021.

MIKROTIK. **MANUAL:INTERFACE/PPPOE**. 2009. Disponível em: https://wiki.mikrotik.com/wiki/Manual:Interface/PPPoE. Acesso em: 15 abr. 2021.

MIKROTIK. **REPORT "Delegated-IPv6-Prefix" attribute for PPPoE**. 2014. Disponível em: https://forum.mikrotik.com/viewtopic.php?t=89443. Acesso em: 22 maio 2021.

NOCTION. **What BGP Looking Glass servers are and how network administrators use them**. 2017. Disponível em: https://www.noction.com/blog/bgp-looking-glass-servers. Acesso em: 22 maio 2021.

NORDMARK, E; INC, Sun Microsystems; GILLIGAN, R; INC, Intransa. **Basic Transition Mechanisms for IPv6 Hosts and Routers**. 2005. Disponível em: https://datatracker.ietf.org/doc/html/rfc4213. Acesso em: 05 nov. 2020.

Prodanov; Freitas. **Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico**. 2 ed. Novo Hamburgo: Feevale Editora, 2013.

RESERVAS de IPv4 chegam ao fim! 2020. Disponível em: http://ipv6.br/post/fim-do-ipv4. Acesso em: 24 ago. 2020.

RTI. PROVEDORES de Internet confirma crescimento para 2020. 2020. Disponível em: http://3rnetwork.com.br/wp-content/uploads/2020/09/rti_junho2020.pdf. Acesso em: 28 out. 2020.

SAMUEL, Brito. Laboratórios de Tecnologias Cisco em infraestrutura de redes. 1 ed. São Paulo: Novatec, 2012.

SEBRAE. **TENDÊCIAS de tecnologia para observar em 2021**. 2021. Disponível em: https://respostas.sebrae.com.br/tendencias-de-tecnologia-para-observar-em-2021. Acesso em: 20 abr. 2021.

TANENBAUM; WETHERALL. Redes de Computadores. 5. Ed. São Paulo: Pearson, 2011.

TEAM-CYMRU. **BOGON Route Server Project**. 2021. Disponível em: https://team-cymru.com/community-services/bogon-reference/bogon-reference-bgp. Acesso em: 2 maio 2021.

TELESINTESE. **PROVEDORES Regionais: Como adicionar valor à banda larga**. 2013. Disponível em: https://www.telesintese.com.br/wp-content/uploads/2013/07/marcelo_couto_abrint.pdf. Acesso em: 20 maio 2021.

WING, D; A YOURTCHENKO,; CISCO. **Happy Eyeballs: Success with Dual-Stack Hosts.** 2012. Disponível em: https://datatracker.ietf.org/doc/html/rfc6555. Acesso em: 20 maio 2021.IPv6.br. Laboratório de IPv6: Aprenda na prática usando um emulador de redes. São Paulo: Novatec, 2015.

YAMAGATA, I. **NAT444**. 2012. Disponível em: https://tools.ietf.org/html/draft-shirasaki-nat444-05. Acesso em: 06 out. 2020.

Apêndice A - Configuração CPE cliente

```
CARLOS_HENRIQUE_LINDEN_7528# sh run
Building configuration...
Current configuration:
!
version 1.0
aaa username user level viewer password hash
$1$3RH0Gb70$B2QZTPpWsE9T50OunWRJi1
aaa username admin level priviledged password hash
$1$h2r8bYcT$EQw/Vsfav00Urjzablmul.
aaa accounting exec default none
aaa authorization exec default none
aaa authentication login default group radius local
access-policy permit
ip nat-rule redir
 tcp any any eq 22 change-destination-to 192.168.1.12
!
ip nat-rule masquerade
 ip any any change-source-to interface-address
!
hostname CARLOS_HENRIQUE_LINDEN_7528
opmode router
ip routing
ipv6 routing
clock timezone BRT -3 0
```

```
interface bridge0
 ip address 192.168.1.1/24
 ip dhcp server local
 ipv6 address IPv6-LAN ::/64
 ipv6 dhcp server DHCP-v6
 ipv6 nd other-config-flag
 multicast
 no ipv6 nd ra suppress
!
interface giga-ethernet0/0/1
 autonegotiation enabled
 no shutdown
!
interface iphost0/0
!
interface loopback0
!
interface virtual-ethernet0/0/0
!
interface virtual-ethernet0/0/0.10
 no multicast
 pppoe 1
 no shutdown
!
interface pppoe1
 ip address negotiated
```

```
 ip nat masquerade out
 ip nat redir in
 ipv6 address autoconfig
 ipv6 address dhcp pd IPv6-LAN
 ipv6 enable
 no multicast
 ppp authentication chap
 ppp ipcp default-route
 ppp ipcp dns-request
 ppp password guillinden@701
 ppp username salagui
 no shutdown
!
ip conntrack size 65536
ip dhcp pool local
 default-router 192.168.1.1
 dns-server 192.168.1.1
 network 192.168.1.10 192.168.1.100 255.255.255.0
!
ip dns relay
ip domain lookup
ip helper ftp
ip helper nat
ip name-server 186.193.161.2
ip name-server 2001:4860:4860::8888
ip name-server 2001:db8:853::1
```

```
ip telnet server
ip telnet server max-connections 5
ipv6 dhcp pool DHCP-v6
 dns-server 2001:db8:853::1
!
mtu 1500
radius-server host 172.25.0.20 key ciph
sntp 172.25.0.7
terminal timeout 5 0
vpn pass-through gre
!
```

Apêndice B – Configuração roteador de Acesso identificado como Aces06.tca

```
# RouterOS 6.42.7
# software id = TSH9-45G6
#
# model = CCR1036-8G-2S+
# serial number = 742B05396B0F
/interface bridge
add fast-forward=no name=BRIDGE-POOL-PRIVADO
add fast-forward=no name=LOOPBACK
/interface vlan
add interface=ether2 name=VLAN_OLT1_CEN vlan-id=3411
add interface=ether2 name=VLAN_OLT1_GDO vlan-id=3412
add interface=ether2 name=VLAN_OLT1_IJH_GPON vlan-id=3410
add interface=ether2 name=VLAN_OLT1_RTE vlan-id=3419
add interface=ether2 name=VLAN_OLT1_TSS vlan-id=3418
add interface=ether2 name=VLAN_OLT2_CEN vlan-id=3425
add interface=ether2 name=VLAN_OLT2_GDO vlan-id=3424
add interface=ether2 name=VLAN_OLT2_IJH vlan-id=3423
add interface=ether2 name=VLAN_OLT2_TQR vlan-id=3413
add interface=ether2 name=VLAN_OLT2_TSS vlan-id=3421
add interface=ether2 name=VLAN_OLT3_TQR vlan-id=3414
add interface=ether2 name=VLAN_OLT3_TSS vlan-id=3420
add interface=ether2 name=VLAN_OLT4_TQR vlan-id=3417
add interface=ether2 name=VLAN_OLT5_TQR vlan-id=3415
```

```
add interface=ether2 name=VLAN_OLT6_TQR vlan-id=3422
/ipv6 pool
add name=2001:db8:e000::/56 prefix=2001:db8:e000::/56 prefix-length=56
add name=2001:db8:e000:200::/56 prefix=2001:db8:e000:200::/56 prefix-length=\
    56
add name=2001:db8:e000:300::/56 prefix=2001:db8:e000:300::/56 prefix-length=\
    56
add name=2001:db8:e000:400::/56 prefix=2001:db8:e000:400::/56 prefix-length=\
    56
add name=2001:db8:e000:500::/56 prefix=2001:db8:e000:500::/56 prefix-length=\
    56
add name=2001:db8:e000:100::/56 prefix=2001:db8:e000:100::/56 prefix-length=\
    56
add name=2001:db8:e000:600::/56 prefix=2001:db8:e000:600::/56 prefix-length=\
    56
add name=2001:db8:e000:700::/56 prefix=2001:db8:e000:700::/56 prefix-length=\
    56
add name=2001:db8:e000:800::/56 prefix=2001:db8:e000:800::/56 prefix-length=\
    56
add name=2001:db8:e000:900::/56 prefix=2001:db8:e000:900::/56 prefix-length=\
    56
add name=2001:db8:e000:a00::/56 prefix=2001:db8:e000:a00::/56 prefix-length=\
    56
add name=2001:db8:e000:b00::/56 prefix=2001:db8:e000:b00::/56 prefix-length=\
    56
add name=2001:db8:e000:c00::/56 prefix=2001:db8:e000:c00::/56 prefix-length=\
```

```
    56
add name=2001:db8:e000:d00::/56 prefix=2001:db8:e000:d00::/56 prefix-length=\
    56
add name=2001:db8:e000:e00::/56 prefix=2001:db8:e000:e00::/56 prefix-length=\
    56
add name=2001:db8:e000:f00::/56 prefix=2001:db8:e000:f00::/56 prefix-length=\
    56
add name=2001:db8:e000:1000::/56 prefix=2001:db8:e000:1000::/56 \
    prefix-length=56
add name=2001:db8:e000:1100::/56 prefix=2001:db8:e000:1100::/56 \
    prefix-length=56
add name=2001:db8:e000:1200::/56 prefix=2001:db8:e000:1200::/56 \
    prefix-length=56
add name=2001:db8:e000:1300::/56 prefix=2001:db8:e000:1300::/56 \
    prefix-length=56
add name=2001:db8:e000:1400::/56 prefix=2001:db8:e000:1400::/56 \
    prefix-length=56
add name=2001:db8:e000:1500::/56 prefix=2001:db8:e000:1500::/56 \
    prefix-length=56
add name=2001:db8:e000:1600::/56 prefix=2001:db8:e000:1600::/56 \
    prefix-length=56
add name=2001:db8:e000:1700::/56 prefix=2001:db8:e000:1700::/56 \
    prefix-length=56
add name=2001:db8:e000:1800::/56 prefix=2001:db8:e000:1800::/56 \
    prefix-length=56
add name=2001:db8:e000:1900::/56 prefix=2001:db8:e000:1900::/56 \
```

```
    prefix-length=56
add name=2001:db8:e000:1a00::/56 prefix=2001:db8:e000:1a00::/56 \
    prefix-length=56
add name=2001:db8:e000:1b00::/56 prefix=2001:db8:e000:1b00::/56 \
    prefix-length=56
add name=2001:db8:e000:1c00::/56 prefix=2001:db8:e000:1c00::/56 \
    prefix-length=56
add name=2001:db8:e000:1d00::/56 prefix=2001:db8:e000:1d00::/56 \
    prefix-length=56
add name=2001:db8:e000:1e00::/56 prefix=2001:db8:e000:1e00::/56 \
    prefix-length=56
/ppp profile
add change-tcp-mss=yes dns-server=186.193.161.2 local-address=200.34.232.1 \
    name=PPPoE-LAN-1 on-down=":global onlineusers [ppp active print count-only\
    \_]\r\
    queue-type=ethernet-default remote-address=pppoe-pool-1 use-ipv6=default
/routing bgp instance
set default as=53137 redistribute-connected=yes router-id=186.193.175.34
/routing ospf instance
set [ find default=yes ] out-filter=OSPF-OUT redistribute-connected=as-type-1 \
    router-id=186.193.175.34
/routing ospf-v3 instance
set [ find default=yes ] redistribute-static=as-type-1 router-id=\
    186.193.175.34
/snmp community
set [ find default=yes ] addresses=186.193.160.0/24 write-access=yes
```

```
add addresses=186.193.160.20/32 name=RADIOS
/system logging action
set 0 memory-lines=10000
set 1 disk-lines-per-file=100
set 3 remote=0.0.0.1 remote-port=515
add name=DUDE remote=186.193.160.26 remote-port=515 src-address=\
    186.193.175.34 target=remote
add name=GRAYLOG remote=186.193.160.50 src-address=186.193.175.34 target=\
    remote
/user group
add comment="#RouterConfig#DO NOT EDIT THIS" name=Backup
policy="ssh,ftp,read,\
    write,sensitive,api,!local,!telnet,!reboot,!policy,!test,!winbox,!password\
    ,!web,!sniff,!romon,!dude,!tikapp"
add comment="#RouterConfig#DO NOT EDIT THIS" name=Viewer
policy="read,winbox,s\
    ensitive,api,tikapp,!local,!telnet,!ssh,!ftp,!reboot,!write,!policy,!test,\
    !password,!web,!sniff,!romon,!dude"
/ip neighbor discovery-settings
set discover-interface-list=none
/ipv6 settings
set max-neighbor-entries=1024
/interface pppoe-server server
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT1_IJH_GPON max-mru=1492 max-mtu=1492 mrru=1600 \
    one-session-per-host=yes pado-delay=800 service-name=PPPoE-OLT1-IJH
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
```

```
    VLAN_OLT1_CEN max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT1-CEN
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT1_GDO max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT1-GDO
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT2_TQR max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT2-TQR
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT5_TQR max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT5-TQR
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT4_TQR max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT4-TQR
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT3_TQR max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT3-TQR
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT1_TSS max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT1-TSS
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
```

```
    VLAN_OLT1_RTE max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT1-RTE
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT3_TSS max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT3-TSS
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT2_TSS max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT2-TSS
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT6_TQR max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT6-TQR
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT2_IJH max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT2-IJH
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT2_GDO max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT2-GDO
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_TESTE_DESCONEXOES_PPPOE max-mru=1492 max-mtu=1492
mrru=1600 \
    one-session-per-host=yes pado-delay=800 service-name=\
    PPPoE-Teste-Desconexoes
```

```
add authentication=chap default-profile=PPPoE-LAN-1 disabled=no interface=\
    VLAN_OLT2_CEN max-mru=1492 max-mtu=1492 mrru=1600 one-session-per-
host=\
    yes pado-delay=800 service-name=PPPoE-OLT2-CEN
/ip address
add address=186.193.175.34 interface=LOOPBACK network=186.193.175.34
add address=200.34.232.5 interface=BRIDGE-POOL-PRIVADO
network=200.34.232.5
add address=186.193.162.202/30 interface=VLAN_BORD01_514 network=\
    186.193.162.200
add address=186.193.162.206/30 interface=VLAN_BORD02_534 network=\
    186.193.162.204
add address=186.193.162.244/30 interface=VLAN_CDN_934 network=\
    186.193.162.242
/ip dns
set servers=186.193.161.2
/ipv6 address
add address=2001:db8:30:514::2 interface=VLAN_BORD01_514
add address=2001:db8:30:534::2 advertise=no interface=VLAN_BORD02_534
add address=2001:db8:ff::34/128 advertise=no interface=LOOPBACK
/ipv6 firewall filter
add action=accept chain=forward out-interface=VLAN_BORD01_514 src-address=\
    2001:db8::/32
add action=accept chain=forward out-interface=VLAN_BORD02_534 src-address=\
    2001:db8::/32
add action=drop chain=forward log=yes out-interface=VLAN_BORD01_514
add action=drop chain=forward log=yes out-interface=VLAN_BORD02_534
```

```
/ppp aaa
set interim-update=1m use-radius=yes
/radius
add address=186.193.160.26 comment="#RouterConfig#DO NOT EDIT THIS"
realm=\
    Mikrotik secret=*** service=login
add address=186.193.160.71 secret=*** service=ppp src-address=\
    186.193.175.34 timeout=900ms
add address=190.234.165.47 secret= service=ppp src-address=\
    186.193.175.34 timeout=900ms
/radius incoming
set accept=yes
/routing bgp peer
add hold-time=1m in-filter=IBGP-BORD01-IN-V4 name=Bord01_V4 nexthop-
choice=\
    force-self out-filter=IBGP-BORD01-OUT-V4 remote-address=186.193.175.1 \
    remote-as=53137 ttl=default update-source=LOOPBACK
add hold-time=1m in-filter=IBGP-BORD02-IN-V4 name=Bord02_V4 nexthop-
choice=\
    force-self out-filter=IBGP-BORD02-OUT-V4 remote-address=186.193.175.2 \
    remote-as=53137 ttl=default update-source=LOOPBACK
add address-families=ipv6 hold-time=1m in-filter=IBGP-BORD01-IN-V6 name=\
    Bord01_V6 nexthop-choice=force-self out-filter=IBGP-BORD01-OUT-V6 \
    remote-address=2001:db8:30:514::1 remote-as=53137 ttl=default \
    update-source=2001:db8:30:514::2
add address-families=ipv6 hold-time=1m in-filter=IBGP-BORD02-IN-V6 name=\
    Bord02_V6 nexthop-choice=force-self out-filter=IBGP-BORD02-OUT-V6 \
```

```
    remote-address=2001:db8:30:534::1 remote-as=53137 ttl=default \
    update-source=2001:db8:30:534::2
add in-filter=IBGP-ACESSCDN-IN-V4 name=AcessCDN_V4 out-filter=\
    IBGP-ACESSCDN-OUT-V4 remote-address=186.193.162.233 remote-as=53137
ttl=\
    default
add address-families=ipv6 in-filter=IBGP-ACESSCDN-IN-V6 name=AcessCDN_V6 \
    out-filter=IBGP-ACESSCDN-OUT-V6 remote-address=2001:db8:cd:922::1 \
    remote-as=53137 ttl=default
/routing filter
add chain="####################### OSPF"
add action=accept chain=OSPF-OUT prefix=186.193.175.34 prefix-length=32
add action=accept chain=OSPF-OUT disabled=yes prefix=200.34.226.0/23 \
    prefix-length=32
add action=discard chain=OSPF-OUT
add chain="####################### BGP"
add chain=LOCAL-ORIGINATE locally-originated-bgp=yes set-bgp-communities=\
    53137:53137,53137:600 set-bgp-local-pref=650
add append-bgp-communities=53137:1999 chain=LOCAL-ORIGINATE \
    locally-originated-bgp=yes prefix-length=22 set-bgp-local-pref=650
add append-bgp-communities=53137:1999,53137:2999,53137:5888 chain=\
    LOCAL-ORIGINATE locally-originated-bgp=yes prefix-length=23 \
    set-bgp-local-pref=650
add chain=LOCAL-ORIGINATE prefix=200.34.226.0/23 prefix-length=32 protocol=\
    connect set-bgp-communities=53137:53137
add action=return chain=LOCAL-ORIGINATE
```

```
add chain=LOCAL-ORIGINATE-V6 locally-originated-bgp=yes prefix=\
    2001:db8:e800::/40 set-bgp-communities=53137:53137 set-bgp-local-pref=650
add action=return chain=LOCAL-ORIGINATE-V6
add chain="####################### Bord01 - IPv6"
add action=accept chain=IBGP-BORD01-IN-V6 prefix=::/0 prefix-length=0
add action=discard chain=IBGP-BORD01-IN-V6 prefix=::/0 prefix-length=0-128
add action=jump chain=IBGP-BORD01-OUT-V6 jump-target=LOCAL-ORIGINATE-
V6
add action=accept bgp-communities=53137:53137 chain=IBGP-BORD01-OUT-V6
add action=discard chain=IBGP-BORD01-OUT-V6
add chain="####################### Bord02 - IPv6"
add action=accept chain=IBGP-BORD02-IN-V6 prefix=::/0 prefix-length=0
add action=discard chain=IBGP-BORD02-IN-V6 prefix=::/0 prefix-length=0-128
add action=jump chain=IBGP-BORD02-OUT-V6 jump-target=LOCAL-ORIGINATE-
V6
add action=accept bgp-communities=53137:53137 chain=IBGP-BORD02-OUT-V6
add action=discard chain=IBGP-BORD02-OUT-V6
add chain="####################### Bord01 - IPv4"
add action=accept chain=IBGP-BORD01-IN-V4 prefix=0.0.0.0/0 prefix-length=0
add action=discard chain=IBGP-BORD01-IN-V4 prefix=0.0.0.0/0 prefix-length=\
    0-32
add action=jump chain=IBGP-BORD01-OUT-V4 jump-target=LOCAL-ORIGINATE
add action=accept bgp-communities=53137:53137 chain=IBGP-BORD01-OUT-V4
add action=discard chain=IBGP-BORD01-OUT-V4
add chain="####################### Bord02- IPv4"
add action=accept chain=IBGP-BORD02-IN-V4 prefix=0.0.0.0/0 prefix-length=0
add action=discard chain=IBGP-BORD02-IN-V4 prefix=0.0.0.0/0 prefix-length=\
```

```
    0-32
add action=jump chain=IBGP-BORD02-OUT-V4 jump-target=LOCAL-ORIGINATE
add action=accept bgp-communities=53137:53137 chain=IBGP-BORD02-OUT-V4
add action=discard chain=IBGP-BORD02-OUT-V4
add chain="####################### AcessCDN - IPv6"
add action=accept bgp-communities=53137:5000 chain=IBGP-ACESSCDN-IN-V6
add action=discard chain=IBGP-ACESSCDN-IN-V6
add action=jump chain=IBGP-ACESSCDN-OUT-V6 jump-target=LOCAL-
ORIGINATE-V6
add action=accept bgp-communities=53137:53137 chain=IBGP-ACESSCDN-OUT-V6
\
    locally-originated-bgp=yes
add action=discard chain=IBGP-ACESSCDN-OUT-V6
add chain="####################### AcessCDN - IPv4"
add action=accept bgp-communities=53137:5000 chain=IBGP-ACESSCDN-IN-V4
add action=discard chain=IBGP-ACESSCDN-IN-V4
add action=jump chain=IBGP-ACESSCDN-OUT-V4 jump-target=LOCAL-
ORIGINATE
add action=accept bgp-communities=53137:53137 chain=IBGP-ACESSCDN-OUT-V4
add action=discard chain=IBGP-ACESSCDN-OUT-V4
/routing ospf interface
add network-type=broadcast passive=yes
add cost=12 interface=VLAN_BORD02_534 network-type=point-to-point
add interface=VLAN_BORD01_514 network-type=point-to-point
/routing ospf network
/routing ospf-v3 interface
add area=backbone passive=yes
```

```
add area=backbone interface=sfp-sfpplus1 network-type=point-to-point
add area=backbone interface=VLAN_BORD02_534 network-type=point-to-point
/snmp
set contact=snmp@tca.com.br enabled=yes src-address=
    trap-version=2
/system clock
set time-zone-name=America/Sao_Paulo
/system clock manual
set dst-delta=-03:00 dst-end="feb/17/2019 00:00:00" dst-start=\
    "nov/04/2018 00:00:00" time-zone=-03:00
```

Apêndice C – Configuração do roteador de borda

```
admin@bord01.tqr> show configuration protocols ospf
export OSPF-DEFAULT-ROUTE;
reference-bandwidth 100g;
area 0.0.0.0 {
    interface lo0.0 {
        passive;
    }
    interface ge-0/0/1.0 {
        passive;
    }
    interface ge-0/1/2.0 {
        interface-type p2p;
        metric 10;
    }
    interface ge-0/0/0.0 {
        passive;
    }
    interface xe-2/0/1.333 {
        passive;
    }
    interface xe-2/0/1.520 {
        interface-type p2p;
        metric 10;
        priority 1;
    }
    interface ae1.535 {
        interface-type p2p;
        metric 10;
        priority 1;
```

```
}
interface ae1.505 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.506 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.508 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.504 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.503 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.502 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.510 {
```

```
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.507 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.511 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.513 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.514 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.531 {
    interface-type p2p;
    metric 10;
    priority 1;
}
interface ae1.509 {
    interface-type p2p;
    metric 10;
```

```
        priority 1;
    }
    interface ae1.704 {
        interface-type p2p;
        metric 10;
        priority 1;
    }
}

admin@bord01.tqr>
admin@bord01.tqr> show configuration protocols bgp group iBGP-IPV6
type internal;
description iBGP-V6;
import IBGP-IPV6-IMPORT;
export IBGP-IPV6-EXPORT;
peer-as 53137;
neighbor 2001:db8:30:507::2;
neighbor 2001:db8:30:504::2;
neighbor 2001:db8:30:503::2;
neighbor 2001:db8:30:505::2;
neighbor 2001:db8:30:506::2;
neighbor 2001:db8:30:510::2;
neighbor 2001:db8:30:502::2;
neighbor 2001:db8:ff::20 {
    import IBGP-IPV6-ACESS-CDN-IMPORT;
    export IBGP-IPV6-ACESS-CDN-EXPORT;
}
neighbor 2001:db8:ff::25;
neighbor 2001:db8:30:511::2;
neighbor 2001:db8:30:513::2;
neighbor 2001:db8:30:514::2;
neighbor 2001:db8:30:f535::2 {
```

```
    export IBGP-IPV6-EXPORT-FULLROUTE;
}
neighbor 2001:db8:ff::89 {
    import IBGP-ROUTE-SERVER-IMPORT;
    export IBGP-ROUTE-SERVER-EXPORT;
    graceful-restart {
        disable;
    }
}
neighbor 2001:db8:ff::204;

admin@bord01.tqr>
```