Delegação de Prefixos IPv6 Utilizando RouterOS em Provedores de Acesso, com Ênfase na Entrega a Clientes Corporativos e Residenciais

Pedro Lucas Castro do Amaral

Faculdade de Computação (FACOMP) – Universidade Federal do Pará (UFPA)
Castanhal – PA – Brasil

engepedrolucas@gmail.com

Abstract. *This article aims to clarify the need to implement IPv6, explain the structure and operation of the protocol and actively contribute to the implementation process in ISPs, especially those whose ASN acquisition process is recent and have RouterOS equipment in their infrastructure. With the presentation of an addressing plan and emulated network similar to the infrastructure used in access providers, enabling the application of IPv6 delegation techniques for corporate and residential customers and their hosts. Demonstrating delivery results using different methods, connectivity established between hosts and the internet, in addition to scripts with the configurations performed in the built scenario.*

Keywords: *Implementation, protocol, delegation, IPv6, RouterOS, addressing, internet.*

Resumo. *Este artigo tem como finalidade esclarecer a necessidade de implantação do IPv6, explanar a estrutura e funcionamento do protocolo e contribuir ativamente no processo de implementação em ISPs, especialmente aqueles cujo o processo de aquisição de ASN é recente e possuem em sua infraestrutura equipamentos RouterOS. Com a apresentação de um plano de endereçamento e rede emulada similar a infraestrutura utilizada em provedores de acesso, viabilizando a aplicação das técnicas de delegação do IPv6 à clientes corporativos e residenciais e seus hosts. Demonstrando resultados de entrega usando diferentes métodos, conectividade estabelecida entre hosts e a internet, além de scripts com as configurações realizadas no cenário construído.*

Palavras chave: *Implementação, protocolo, delegação, IPv6, RouterOS, endereçamento, internet.*

1. Introdução

1.1. Justificativa

Atualmente, no que tange o avanço das telecomunicações, é importante ressaltar o crescimento da internet como recurso essencial para a sociedade em todos os âmbitos, como na comunicação e acesso a informação. O que reflete diretamente em alguns serviços como, por exemplo, as redes sociais, a qual reivindica a comunicação remota e

instantânea entre os usuários, transações bancárias, onde o acesso as informações legítimas e confiáveis são primordiáis, nas compras online, otimizando a interação entre vendedor e comprador, entre outros inúmeros serviços.

Com isso, devido a modernização do acesso a informação, a utilização de dispositivos que acessam a internet cresce de forma exponencial, em ambientes corporativos e residenciais.

Além disso, é previsível o crescimento de objetos físicos incorporados a sensores, *software* e outras tecnologias, com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet, popularmente conhecidos como Internet das Coisas (IoT), esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas, e sua presença no cenário real tende a alcançar valores próximos de 22 bilhões até o ano de 2025 (ORACLE, 2021).

De acordo com dados publicados em abril de 2021, quando a população mundial era de aproximadamente 7,85 bilhões, 1% a mais em relação ao mesmo período no ano anterior, existiam cerca de 5,25 bilhões de usuários móveis conectados, ou seja, mais de dois terços da população mundial acessava a internet (SIMON KEMP, 2021). Para suprir a demanda gerada nesse contexto, temos como principais atuantes as RIRs (Registro Regional da Internet), tratam-se de entidades divididas hierarquicamente para estabelecer organização na administração dos endereços IPs, em âmbito internacional, garantindo a disponibilidade e singularidade dos endereços para cada ASN (*Autonomous System Number*), conforme publicado no site IPLOCATION.NET, onde demonstra detalhadamente essa hierarquia entre as entidades envolvidas.

Com base no cenário exemplificado no parágrafo inicial, associado as informações disponibilizadas pela *Hurricane Eletric Internet Services* na Figura 2, onde são monitoradas em tempo real as quantidades de prefixos IPv4 em posse da IANA e as RIRs, chegamos ao fim de prefixos públicos em posse da própria IANA, ARIN e RIPE.

É evidente, conforme a Figura 2 demonstra, que há apenas 1024 endereços IPv4 em posse do LACNIC, além de, uma quantidade relativamente baixa em posse das RIRs AFRINIC e APNIC considerando o espaço amostral do IPv4 global.

Figura 2. Estatística de alocação IPv4 e IPv6 em tempo real por RIR
Fonte: Hurricane Electric IPv6

O protocolo IPv6 foi desenvolvido para suprir a necessidade gerada pela popularização da internet e o esgotamento do IPv4. Sua regulamentação e especificação foi realizada em dezembro de 1998 pela IETF (*Internet Engineering Task Force*), através da RFC 2460 oriunda da RFC 1550 de 1993, que conscistiu na requisição de novas pesquisas, projetos e propostas para nova versão do protocolo IP (BRADNER e MANKIN, 1993). Posteriormente tornou-se obsoleta à RFC 2460 devido as especificações e padrões estabelecidos para o protocolo quanto a estrutura do IPv6 (S. DEERING e R. HINDEN, 1998), os quais serão citados no decorrer deste artigo.

Após a criação e padronização do protocolo, um grande desafio para a comunidade IPv6 e principalmente para os ISPs (Internet Service Provider) que possuem ASN próprio com pelo menos um bloco IPv6 /32, é implementar e delegar o novo protocolo em sua rede com um bom plano de alocação seguindo as boas práticas recomendadas pelo próprio NIC.br.

Fato esse, que justifica o volume de tráfego IPv6 no cenário atual ser relativamente baixo, ao associarmos com a distribuição do novo protocolo por parte da RIR LACNIC, que chega a ser mais de 96% das organizações com ASN próprio na América Latina e Caribe (IPv6.br, 2020). Ou seja, o protocolo está sendo distribuído pelas organizações competentes, no entanto, o volume de tráfego IPv6 reforça que os acessos e serviços não estão majoritariamente atuando já com o novo recurso.

Conforme os dados coletados a partir dos acessos aos serviços disponibilizados pelo Google, é possível inferir que o tráfego segue em constante ascenção nos útimos 10 anos, representando pelo menos um terço do tráfego total. A Figura 3 mostra a porcentagem de usuários que acessam os serviços do Google por meio de IPv6.

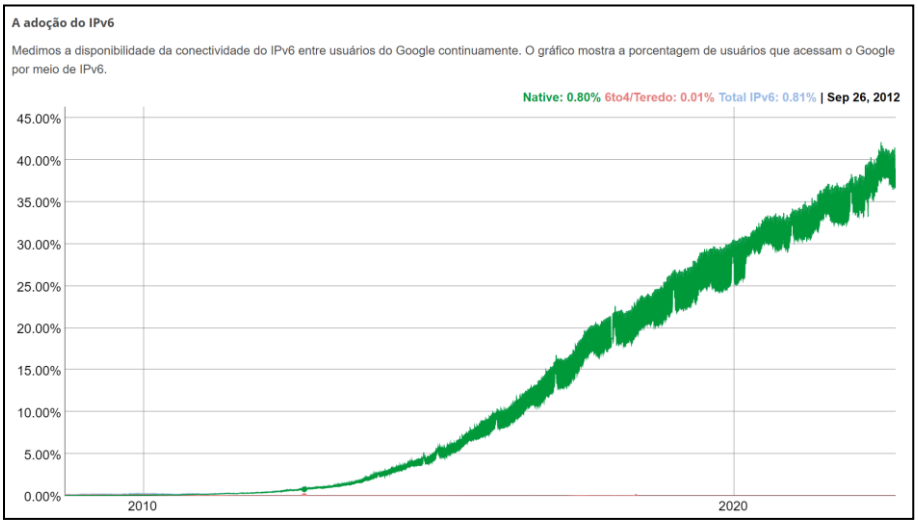

Figura 3. Percentual de acessos aos serviços do Google por meio de IPv6
Fonte: IPv6 - Google

1.2. Motivação

De acordo com os resultados de uma pesquisa realizada em 2020 pelo CETIC.br com 7007 provedores de macrorregiões brasileiras distintas, conforme a Tabela 1, concluiu-se que a cada macrorregião mais de 50% dos provedores de acesso que possuem ASN e prefixos IPv6, apresentam alguma dificuldade em sua implementação e consequentemente entrega aos seus clientes finais (CETIC.br, 2020), conforme ilustra a Figura 4.

Regiões	Total de entrevistados
Norte	427
Nordeste	2113
Sudeste	2546
Sul	1222
Centro-oeste	699
Total	7007

Tabela 1. Espaço amostral da pesquisa, total de provedores por macrorregião
Fonte: Portal de dados – CETIC.br

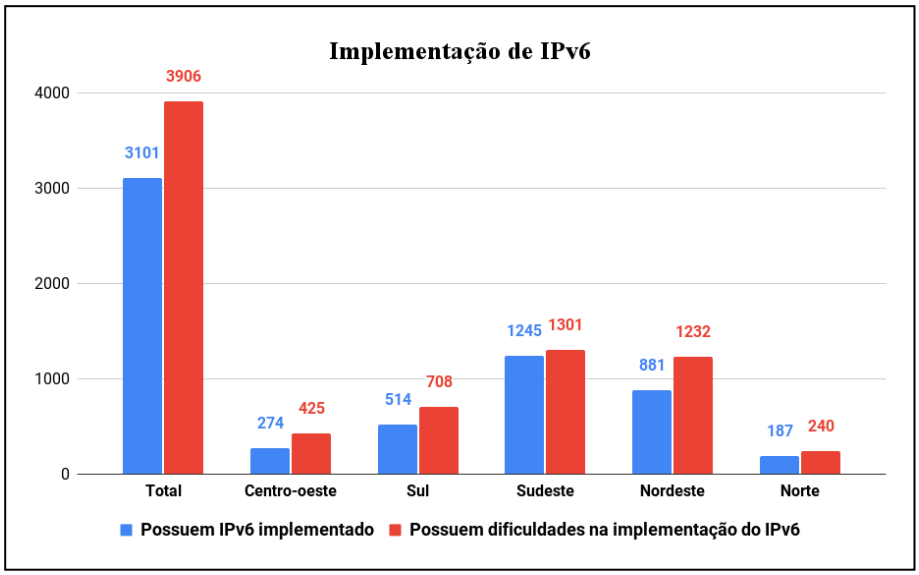

Figura 4. Dificuldades na implementação do IPv6
Fonte: O autor

Conforme os resultados da pesquisa, é possível restringir o espaço amostral entre os entrevistados que possuem dificuldades na implementação do IPv6, com isso, foram listadas algumas dificuldades comuns, as quais foram respondidas de forma objetiva por cada entrevistado. As principais dificuldades apresentadas foram: dificuldades em criar um plano de ativação, falta de pessoal capacitado, falta de equipamentos apropriados, alto custo do investimento, ausência de IPv6 entre os fornecedores, falta de interesse ou de conhecimento e outros motivos não listados. As Figuras a seguir correspondem aos valores coletados por dificuldade de ativação na pesquisa realizada pelo CETIC.br em 2020.

Na Figura 5, correspondente as dificuldades em criar um plano de ativação IPv6, é notório que pelo menos 47% do total de entrevistados que confirmaram dificuldades na implementação do novo protocolo, consideraram especificamente essa dificuldade como impecilho no processo de implementação, chegando a valores superiores a 50% de entrevistados que alegam dificuldades, quando restringimos o espaço amostral da pesquisa nas regiões Norte e Nordeste.

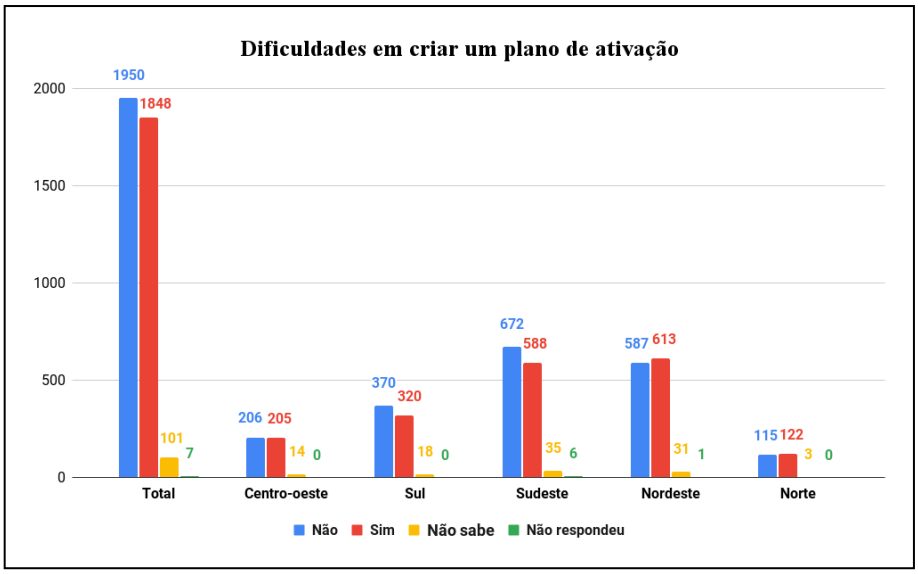

Figura 5. Dificuldades em criar um plano de ativação
Fonte: O autor

A Figura 6, corresponde a falta de pessoal capacitado, é coerente que mais de 50% do total de entrevistados que alegaram falta de pessoal capacitado, consideraram essa questão um dos obstáculos na implementação do IPv6 em seus ISPs, sendo uma dificuldade proporcionalmente comum a todas as macrorregiões ao analisarmos os valores individualmente.

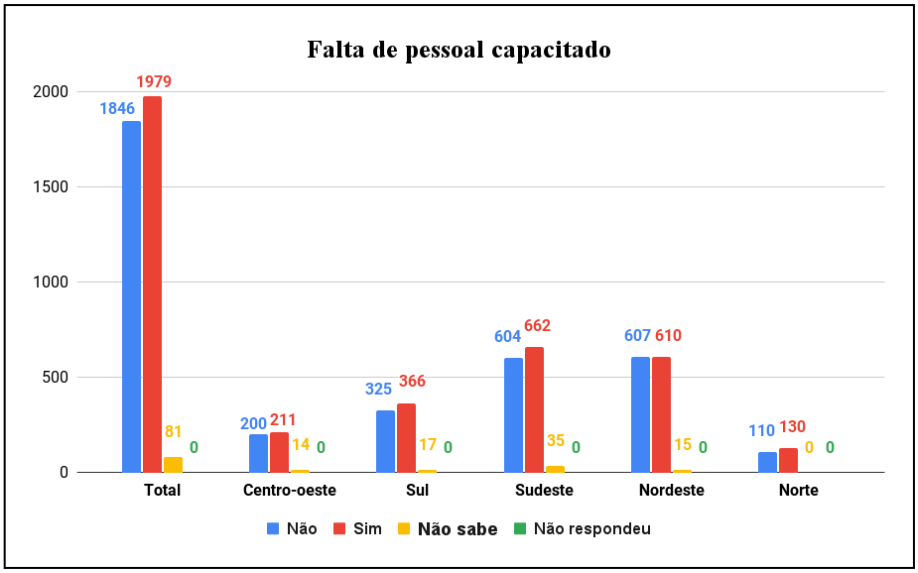

Figura 6. Falta de pessoal capacitado
Fonte: O autor

A falta de equipamentos apropriados é um problema comum nesse cenário, está relacionada a equipamentos que não possuem compatibilidade com o protocolo IPv6 ou não possuem as atualizações necessárias para operar em *dual stack* na rede, não sendo maioria no total dos entrevistados que alegaram dificuldades, no entando, representando

um certo equilíbrio entre os que alegaram e não alegaram tal dificuldade em cada macrorregião, conforme ilustra a Figura 7.

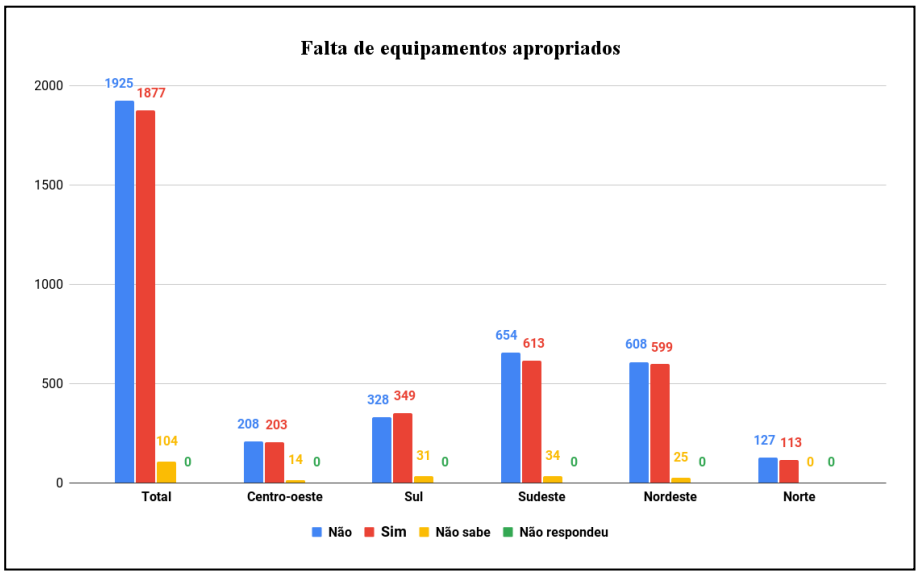

Figura 7. Falta de equipamento apropriado
Fonte: O autor

A Figura 8 demonstra os valores referentes a alto custo de investimento, tanto relacionada a mão de obra qualificada quanto a disponibilidade de equipamentos compatíveis com o novo protocolo, tendo em vista, os diferentes valores financeiros atribuídos aos recursos que qualificam essa dificuldade a cada macrorregião, é evidente que as regiões Norte e Nordeste sofrem mais com essa dificuldade.

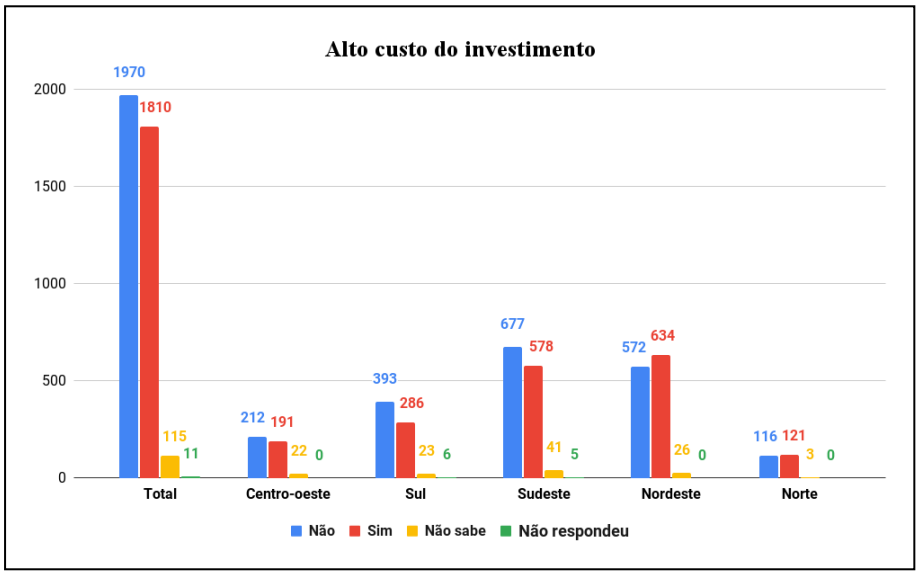

Figura 8. Alto custo do investimento
Fonte: O autor

A Figura 9 demonstra os valores referentes a ausência de IPv6 entre os fornecedores, é notório que em todas as macrorregiões a quantidade de entrevistados

que não possuem essa dificuldade é superior, no entanto, a ausência de IPv6 em provedores de acesso ainda é realidade.

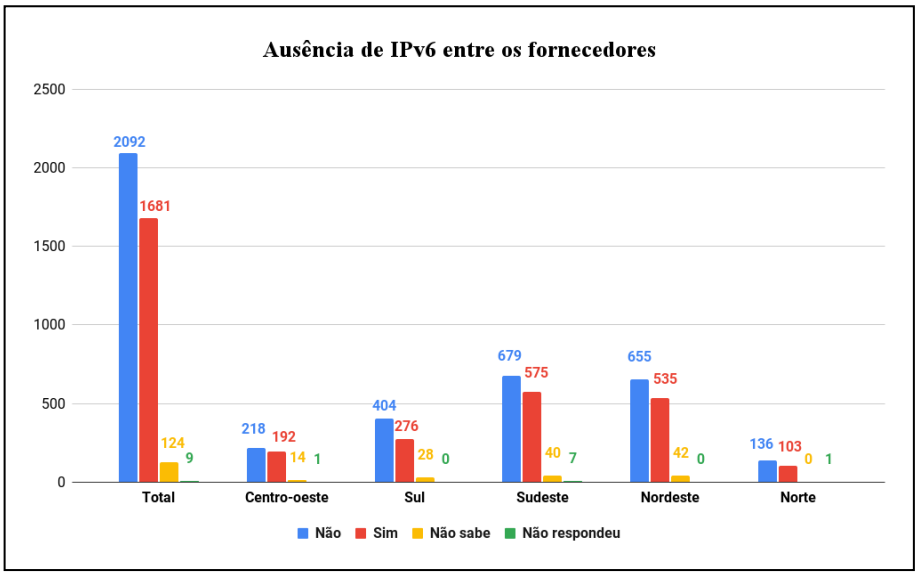

Figura 9. Ausência de IPv6 entre os fornecedores
Fonte: O autor

A falta de interesse ou de conhecimento não é apontado pela maioria dos entrevistados, conforme ilustra a Figura 10, ressaltando a relevância do protocolo IPv6 no mercado de provedores e o interesse em sua implementação.

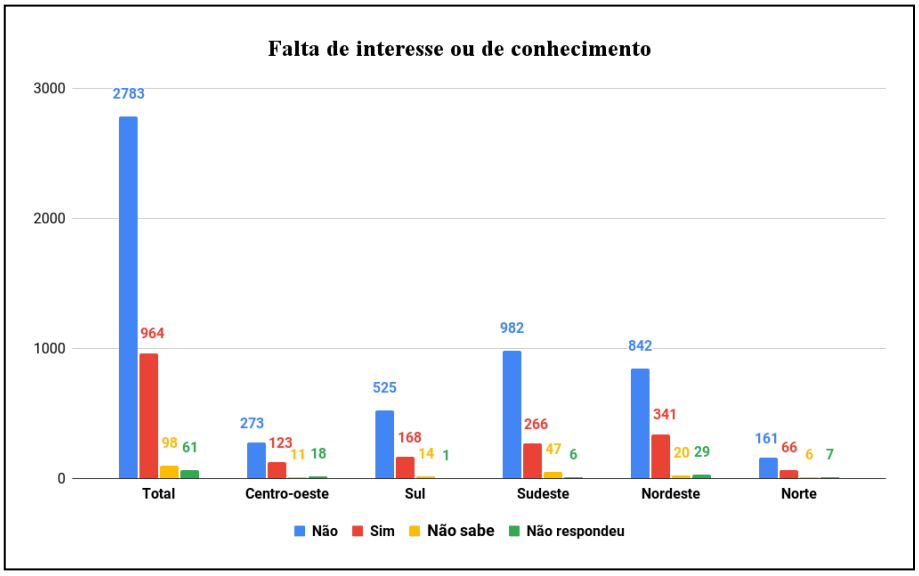

Figura 10. Falta de interesse ou de conhecimento
Fonte: O autor

A Figura 11 demonstra os valores relacionados a outras dificuldades não especificadas pela equipe do CETIC.br, mas foram contabilizadas nesse campo de modo geral.

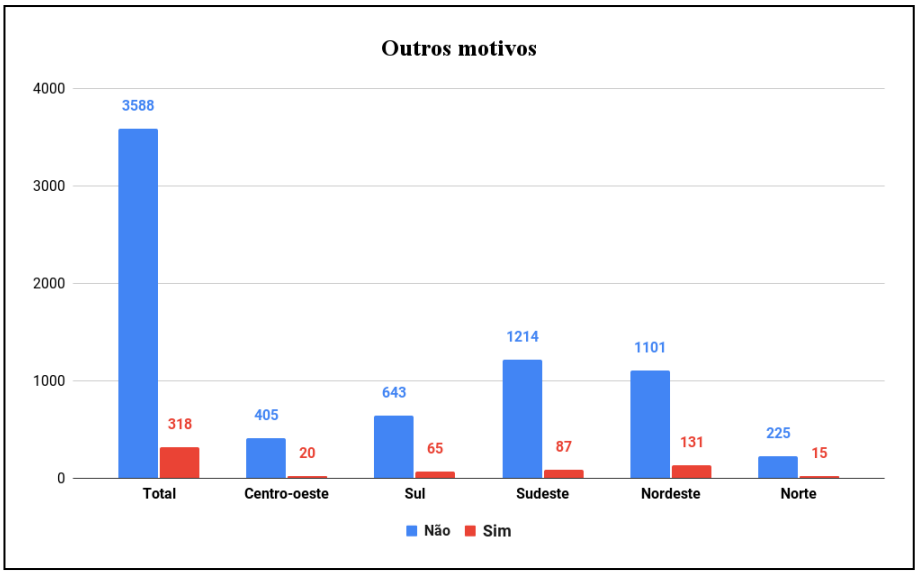

Figura 11. Outros motivos
Fonte: O autor

Com base nesses resultados, é indispensável a elaboração de um estudo que visa contribuir ativamente no processo de planejamento, distribuição e delegação de prefixos IPv6 aos clientes finais de maneira geral, utilizando equipamentos e sistemas operacionais acessíveis quanto a valor de mercado, interface de gerenciamento simplificada, disponibilidade de materiais instrucionais e popularidade no mercado de ISPs.

1.3. Objetivo Geral

O principal objetivo da construção deste trabalho, é estabelecer uma metodologia de fácil implementação de IPv6 em uma rede provedora e delegação de prefixos aos clientes finais, conforme o plano de alocação elaborado.

1.4. Objetivos Específicos

1. Construir um cenário de rede similar ao de um ISP utilizando ferramentas de simulações de redes, garantindo a funcionalidade da rede em *dual stack*.
2. Seguindo as boas práticas recomendadas pela comunidade do IPv6 e pelo NIC.br, provisionar um plano de endereçamento expansível.
3. Aplicar as configurações conforme o planejamento, utilizando ferramentas intuitivas e Sistema Operacional que possui presença no mercado de provedores, visando custo benefício.
4. Estabelecer comunicação ponto a ponto entre os ativos de rede.
5. Utilizar as técnicas e protocolos necessários para prover roteamento, implementação e delegação dos prefixos.
6. Extrair os resultados de entrega dos prefixos IPv4 e IPv6 aos roteadores dos clientes finais e seus *hosts*.
7. Extrair os resultados dos testes de conectividade via IPv4 e IPv6 entre os *hosts* e os ativos de rede.

2. Referencial Teórico

2.1. Estrutura do IPv6

Com a proposta de não apenas suprir a demanda gerada após o esgotamento do IPv4, mas consolidar um protocolo com sua estrutura desenvolvida para garantir a expansão da internet, sem prejuízos futuros relacionados a esgotamento de endereços públicos, preparando cada vez mais um cenário ideal.

O IPv6 tem sua estrutura baseada em 128 bits, possibilitando um número máximo de 2^{128} endereços, representando aproximadamente 79 octilhões de vezes a quantidade de endereços IPv4 (NIC.br, 2012). Além da quantidade exorbitante de possíveis formações de endereços, a sua representação se difere pela utilização de números hexadecimais e separação de cada hexadecateto (também chamados de duplo-octetos) por meio de ":". Algumas de suas particularidades referente a representação é a permissão para omitir zeros à esquerda, representar zeros contínuos por "::" (apenas uma vez por prefixo para não gerar ambiguidade) e indiferença entre caracteres maiúsculos ou minúsculos.

Nos exemplos abaixo destacam-se a representação de um endereço IPv6 em sua forma completa, oito duplo octetos com 16 bits cada um (ou 2 bytes), escrito em hexadecimais separados por ":" e a representação do mesmo prefixo na forma compactada respectivamente.

- 2001:0DB8:0000:0000:130F:0000:0000:140B
- 2001:DB8:0:0:130F::140B

Com a sua nova estrutura, os endereços do tipo *broadcast* foram extintos devido a apresentação de alguns problemas de transmissão na maioria das redes, além disso, um novo tipo de endereço foi definido pela RFC 1546 de 1993 chamados *Anycast*, totalizando três tipos, são eles (NIC.br, 2012):

- **Multicast:** Identifica um conjunto de interfaces, de modo que um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Um endereço *multicast* é utilizado em comunicações de um-para-muitos reservados no prefixo FF00::/8.
- **Anycast:** Também identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue a interface pertencente a este conjunto mais próxima da origem.
- **Unicast:** É um tipo de endereço que identifica uma única interface, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface.

Os endereços *unicast* são utilizados para comunicação entre dois nós, sua estrutura foi definida para permitir agregações com prefixos de tamanho flexível, assim como o CIDR do IPv4. Existem três tipos de endereços *unicast*, são eles:

- **Global Unicast:** São endereços globalmente roteáveis, representados pelo prefixo 2000::/3, para critérios de analogia, são similares aos endereços públicos IPv4 e totalizam 13% do total de endereços possíveis, considerando a estrutura do IPv6 a qual é demonstrada na Figura 12. Dentro do prefixo mencionado há

uma faixa reservada para documentação que deve ser sempre bloqueada na borda da rede, segue o prefixo reservado para documentação: 2001:db8::/32.

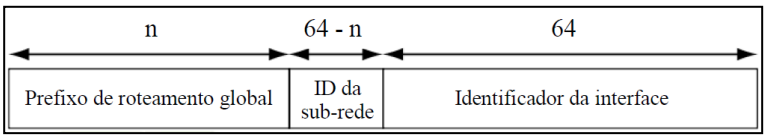

Figura 12. Estrutura de formação do endereço IPv6 Global Unicast
Fonte: Apostila Curso IPv6 básico – NIC.br

- **Link Local:** Endereços que devem ser utilizados apenas localmente e em ambos os protocolos não são roteáveis nem na rede local, analogicamente semelhantes aos endereços APIPA (Windows) no IPv4 que são reservados na faixa 169.254.0.0/16, e só são utilizados via autoconfiguração em casos em que a placa de rede do *host* não obtem endereços roteáveis, seja via DHCP ou qualquer outro protocolo, diferentemente do *Link Local* no IPv6, o qual é atribuído automaticamente (autoconfiguração *stateless*) na faixa FE80::/64 em todas as interfaces, sendo critério conclusivo no ato de validação da pilha IPv6 em pleno funcionamento em um determinado ativo de rede. A Figura 13 demonstra a estrutura de formação dos endereços IPv6 do tipo Unicast Link Local.

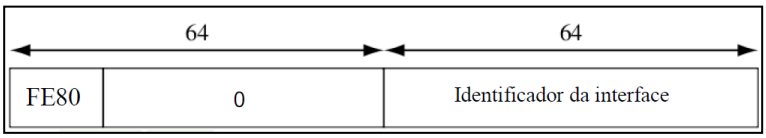

Figura 13. Estrutura de formação do endereço IPv6 Unicast Link Local
Fonte: Apostila Curso IPv6 básico – NIC.br

- **Unique Local (ULA):** Faixa reservada FC00::/7 prefixos que devem ser utilizados e roteados apenas na comunicação dentro de um enlace ou entre um conjunto limitado de enlaces, analogicamente semelhantes aos endereços privados no IPv4, os quais não devem ser roteados na internet, segue a estrutura de formação do tipo de endereço em questão representado pela Figura 14.

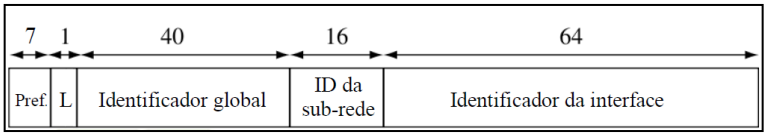

Figura 14. Estrutura de formação do endereço IPv6 Unique Local (ULA)
Fonte: Apostila Curso IPv6 básico – NIC.br

Assim como o IPv4, existem prefixos IPv6 reservados para usos especiais, como por exemplo, endereços IPv4 mapeados em IPv6, endereços de *loopback*, entre outros.

2.2. Comparativo IPv4 e IPv6

A principal diferença entre os protocolos é a quantidade de *bits* utilizados em sua estrutura, enquanto no IPv4 o total é de 32 bits possibilitando uma quantidade máxima de 2^{32} endereços, no IPv6 essa quantidade cresce de forma exorbitante, conforme citado no subtopico anterior.

Além de sua estrutura, o IPv6 trouxe algumas mudanças consideráveis como:

- **Maior endereçamento:** O espaço para endereçamento traz agora 128 bits, o IPv4 tem 32 bits de endereçamento, permitindo uma agregação mais específica de endereços.
- **Cabeçalho com formato simplificado:** foi definido um cabeçalho de tamanho único, retirando alguns campos do IPv4, com o intuito de reduzir o processamento nos roteadores.
- **Suporte a cabeçalhos de extensão:** as opções foram retiradas do cabeçalho base e passam a fazer parte de cabeçalhos de extensão, traz uma maior flexibilidade para a introdução de novas opções no futuro.
- **Capacidade de identificar fluxo de dados:** um novo recurso que permite identificar pacotes que pertençam a determinado fluxo, trazendo a possibilidade de oferecer tratamentos especiais a fluxos específicos.

O protocolo IPv4 tem seu cabeçalho com tamanho flexível, podendo ter seu tamanho alterado de 20 bytes até 60 bytes, com a finalidade de fornecer opções, como segurança, roteamento de origem, entre outras. Estas opções tem sido raramente utilizadas e a necessidade de processamento dessas informações pode afetar a performance da rede (HAGEM, 2006).

No IPv6 o tamanho do cabeçalho foi fixado em 40 bytes, e o número de campos foi reduzido para 8. As Figuras 15 e 16 demonstam uma comparação entre os cabeçalhos IPv4 e IPv6. Em relação ao cabeçalho do protocolo anterior, seis campos foram removidos (NIC.br, 2012):

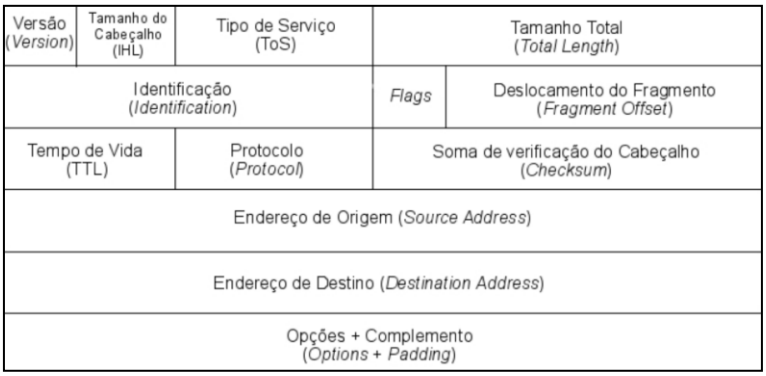

Figura 15. Cabeçalho IPv4
Fonte: Apostila IPv6 básico – NIC.br

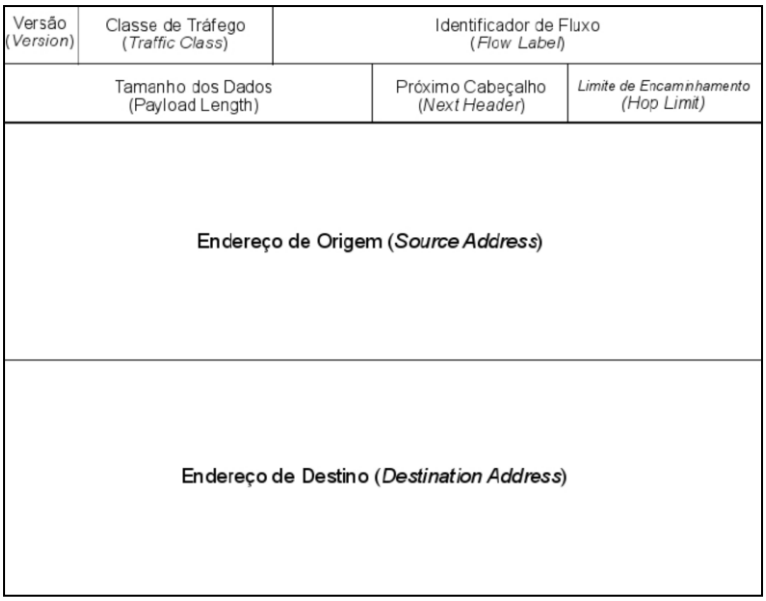

Figura 16. Cabeçalho IPv6
Fonte: Apostila IPv6 básico – NIC.br

O campo "Identificador de Fluxo" foi adicionado, oferecendo suporte ao funcionamento de mecanismos extras de QoS. Com um cabeçalho mais simples e um processamento mais rápido pelos nós intermediários, o IPv6 possui uma nova capacidade de lidar com as opções chamadas de cabeçalhos de extensão (HAGEM, 2006). Seis destes cabeçalhos foram definidos na especificação do IPv6 (S. DEERING e R. HINDEN, 1998):

- **Hop-by-hop:** Este cabeçalho se localiza na primeira posição da cadeia de cabeçalhos, sendo analisado por todos os nós intermediários até o destino, tem opções como ignorar e continuar o processamento, e descartar o pacote. Existem dois tipos de hop-by-hop: Router Alert e Jumbogram.
- **Destination Options:** É processado apenas pelo destino do pacote, oferecendo suporte ao mecanismo de mobilidade IPv6 e contém o endereço de destino do nó móvel.
- **Routing:** Desenvolvido para listar um ou mais nós intermediários que deveriam ser visitados até o pacote chegar ao destino final. Devido a problemas de segurança, esta função se tornou obsoleta na RFC 5095.
- **Fragmentation:** Este cabeçalho é utilizado quando o tamanho do pacote IPv6 é maior que o MTU dos roteadores do caminho. Não existe a fragmentação dos pacotes pelos roteadores, os pacotes são fragmentados apenas na origem.
- **Authentication Header e Encapsulating Security Payload:** Fazem parte do IPSec que tem a finalidade de tentar garantir a segurança em redes de comunicação de dados.

Alguns campos foram renomeados e reposicionados conforme a Tabela 2 (NIC.br, 2012):

IPv4	IPv6
Tipo de Serviço	Classe de Serviço
Tamanho Total	Tamanho dos Dados
Tempo de vida (TTL)	Limite de Encaminhamento
Próximo Protocolo	Cabeçalho

Tabela 2. Renomeação dos campos do protocolo IPv6
Fonte: Apostila IPv6 básico – NIC.br

2.3. Protocolo BGP

O BGP (*Border Gateway Protocol*), ou Protocolo de Roteador de Borda conforme sua tradução para o português, foi definido na RFC 1105 de 1989 (K. LOUGHEED e Y. REKHTER), trata-se de um protocolo de roteamento externo, responsável por conectar redes que formam a internet, é um protocolo que agrega tudo e usa o TCP como o protocolo de transporte na porta 179, lembrando que a conexão TCP é formada pela junção de dois roteadores BGP.

O protocolo BGP é um protocolo de vetor de distância que exerce controle sobre o caminho exato para cada destino na internet, em vez de manter o custo para cada destino como é comum no OSPF por exemplo.

Atualmente, o BGP é o protocolo padrão utilizado para roteamento entre sistemas autônomos na internet e se encontra na versão 4, regulamentada e atualizada conforme a RFC 4271 de 2006 (Y. HEKHTER, T. LI e S. HARES, 2006).

2.4. Protocolo OSPF

O OSPF é um protocolo de roteamento *link-state*, o qual foi projetado para ser executado internamente, ou seja, dentro de uma rede *backbone* de um provedor de serviços a fim de otimizar as politicas de roteamento na rede, utiliza uma tabela de roteamento onde é calculado e construído uma árvore do caminho (RFC 2328, 1998). Além de tudo, ele possui a vantegem de recalcular as rotas rapidamente diante de mudanças topológicas, algo muito comum em redes de longa distância.

2.5. Protocolo DHCPv6

O DHCPv6 foi definido na RFC 3315, trata-se de um protocolo de autoconfiguração *stateful* utilizado na distribuição de endereços IPv6 e outros parâmetros, como servidores DNS, NTP, SIP etc. dinamicamente em uma rede a partir de um servidor permite um controle maior na atribuição de endereços aos *hosts* garantindo a singularidade, possui um mecanismo de autoconfiguração de endereços *stateful* e *stateless* que podem ser utilizados simultaneamente, o protocolo é independente do DHCPv4, ou seja, em redes com pilha dupla precisam ser configurados separadamente (NIC.br, 2012).

No DHCPv6, a troca de mensagens entre cliente e servidor é realizada utilizando-se o protocolo UDP. Os clientes utilizam um endereço link-local para transmitir ou receber mensagens DHCP, enquanto que os servidores utilizam um

endereço multicast reservado (FF02::1:2 ou FF05::1:3) para receber mensagens dos clientes. Caso o cliente necessite enviar uma mensagem a um servidor que esteja fora de sua sub-rede, é utilizado um Relay DHCP (NIC.br, 2012).

3. Metodologia

3.1. Recursos Utilizados

Afim de aplicar o que foi estudado até esse tópico de forma experimental e conclusiva conforme o planejamento, seguindo o referencial teórico e as boas práticas recomendadas pelo NIC.br, alguns recursos foram imprescindíveis para construção do trabalho. Em seguida são apresentados os recursos utilizados neste trabalho e suas respectivas aplicações.

O VMware Workstation Player, versão gratuita do virtualizador de máquinas muito utilizado no âmbito computacional, assim como o VirtualBOX, foi um recurso ideal para executar os sistemas operacionais utilizados neste estudo.

O RouterOS é um Sistema Operacional baseado no kernel Linux v2.6, que oferece várias soluções voltadas para redes de computadores, possibilitando até transformar um computador (x86) em um potente roteador, até mesmo com aquele Pentium 100Mhz 64MB RAM, 8GB HD é possível instalar o RouterOS. Criado em 1997 pela empresa Mikrotik, fundada na Letônia em 1995, a instituição é voltada para o ramo de desenvolvimento de tecnologias e sistemas de roteamento completo e *firewall*, a qual posteriormente, em 2002 desenvolveu equipamentos RouterBOARD como *hardware* de fabricação própria embarcado com seu sistema operacional RouterOS. (PPLWARE, 2012).

A versão utilizada nesse trabalho foi a 6.48.6 *(long term),* imagem disponibilizada gratuitamente no site da desenvolvedora (Mikrotik) para emular redes, sendo a base de configuração do cenário, devido a solução proposta neste artigo. Por padrão, na versão *long term* atual (6.48.6), a pilha IPv6 não está habilitada, por esse motivo, antes de efetivar qualquer configuração relacionada ao protocolo, é fundamental que os pacotes IPv6 sejam devidamente habilitados no roteador.

Winbox versão 3.37, ferramenta que permite o acesso por meio de interface gráfica, disponibilizado pelo próprio desenvolvedor Mikrotik, utilizado para acesso aos equipamentos RouterOS, a fim de prover simplicidade nas configurações e familiaridade com o *layout* do sistema operacional, facilitando consideravelmente o processo de configuração do cenário

Os RouterBOARDs são *hardwares*, basicamente pequenos roteadores integrados com o sistema RouterOS, podendo atender vários tipos de ambientes, desde um ponto de acesso em um hotel até um roteador de borda em um *datacenter*. (VIVAOLINUX, 2011)

O grande diferencial dos RouterBOARDs é seu custo benefício e simplicidade na configuração, proveniente da possibilidade de gerenciamento pela ferramenta gráfica Winbox através da porta padrão 8291, o qual atualmente está na versão 3.37, disponibilizada gratuitamente no site oficial da fabricante.

Os acessos via ssh (porta padrão 22) e telnet (porta padrão 23) também são possíveis, com suas portas padrões editáveis possibilitando a comunicação dos mesmos

com outros serviços utilizados no ISP, como servidores *radius*, servidores FTP para *backups*, entre outros.

Windows 11, sistema operacional muito comum em ambientes residenciais, utilizado no cenário na função de *host* residencial, com a finalidade de evidenciar a funcionalidade da entrega do IPv6 em plataformas diversas.

Linux versão Ubuntu 18.04 virtualizado, imagem disponibilizada gratuitamente, utilizada no cenário na função de *host* corporativo, por se tratar de um sistema operacional muito comum em ambientes no qual há necessidade hospedar serviços, geralmente utilizados em servidores empresariais.

OpenWrt, é um Sistema operacional Linux voltado para sistemas embarcados. Em vez de tentar criar um único *firmware* estático, o OpenWrt fornece um sistema de arquivos totalmente gravável com gerenciamento de pacotes. Isso libera o ISP da seleção e configuração de aplicativos fornecidos e permite que seja livremente personalizado o dispositivo por meio do uso de pacotes para atender a qualquer aplicativo. Para desenvolvedores, OpenWrt é a estrutura para construir um aplicativo sem ter que construir um *firmware* completo em torno dele; para os usuários, isso significa a capacidade de personalização total (OPENWRT, 2022).

O PNETLab foi o simulador de redes utilizado para a construção do cenário, também virtualizado pelo VMware Workstation Player, trata-se de uma plataforma disponibilizada gratuitamente para *download* e instalação, contém seu modo *offline*, onde é possível inserir novas imagens para emular sistemas operacionais de diversos fabricantes e construir inúmeros cenários. Em seu modo *online* é possível acessar a loja de laboratórios prontos e até mesmo disponibilizar os de própria autoria para os demais usuários.

UltraVNC Viewer, é o software utilizado para acesso aos equipamentos Linux, recurso necessário quando se trata de virtualização de máquinas Linux e até mesmo Windows.

Calculadora IPv6 de sub-rede disponibilizada *online* pelo Site24x7, aplicação ideal para segmentação de sub-redes IPv6, sendo essencial na elaboração do planejamento de alocação dos prefixos IPv6.

Simulação RFC 3531, disponibilizada *online* pelo NIC.br, recurso ideal para alocação de sub-redes IPv4 e IPv6 e aplicação das diferentes técnicas de segmentação de prefixos.

3.2. Planejamento IPv6

No contexto em que não há mais aquisição de prefixos IPv4, o processo de implementação do IPv6 precisa ser prioridade. Um bom planejamento e plano de alocação de prefixos tem sido um grande desafio para os ISPs, principalmente aqueles que adquiriram seu número de ASN próprio recentemente, motivo esse que se deve ao fato da estrutura do endereço utilizar 128 bits e representação em hexadecimal, enquanto que o IPv4 utiliza em sua estrutura 32 bits e representação decimal.

O planejamento e delegação do IPv6 até o cliente final, parte primeiramente da divisão do prefixo principal em várias sub-redes de acordo com a sua finalidade, seja ela atender uma cidade, onde estará contida as demais sub-redes para atendimento de

clientes e tunelamentos diversos por exemplo, ou até mesmo da seleção dos prefixos do tipo **Unicast Unique Local (ULA)** que não serão roteados na internet, utilizados normalmente para estabelecer comunicação interna entre os equipamentos do provedor.

De acordo com as boas práticas recomendadas pelo NIC.br, são princípios essenciais em um bom plano de alocação:

- **Singularidade:** Cada bloco distribuído e/ou alocado deve ser único no mundo.
- **Registro:** O espaço de endereçamento tem que estar registrado na base de um RIR e as informações pertinentes ao registro devem ser acessíveis.
- **Agregação:** Sempre que possível distribuir os endereços de maneira hierárquica dentro da topologia. As políticas de endereçamento devem evitar a fragmentação, pois impacta diretamente na tabela de rotas no quesito memória e processamento afetando o desempenho do roteador de borda.
- **Conservação:** Mesmo com a grande quantidade de endereços deve-se evitar o uso de práticas que favoreçam o desperdício de endereços.

Por mais que o espaço amostral seja exorbitante, quando se trata de IPv6, é de suma importância destacar que um bom planejamento precisa ser realizado de forma responsável, visando as boas práticas, aplicando as técnicas de segmentação dos blocos para garantir a expansão da rede e realizando as alocações com o intuito de sumarizar de forma eficiente e otimizar os anúncios dos prefixos na borda da rede. Nesse sentido, é essencial aplicar as técnicas de segmentação de prefixos disponibilizadas na RFC 3531, a qual possui sua simulação disponibilizada pelo NIC.br, a seguir constam as especificações das principais técnicas de segmentação:

- **Rightmost:** Técnica de alocação sequencial, consiste em variar os bits da direita para criar uma distribuição de endereços de forma sequencial. A Figura 17 mostra a variação de 4 *bits* para a formação de 16 sub-redes utilizando a técnica *rightmost* a partir do simulador da RFC 3531 (CEPTRO.BR, 2013).

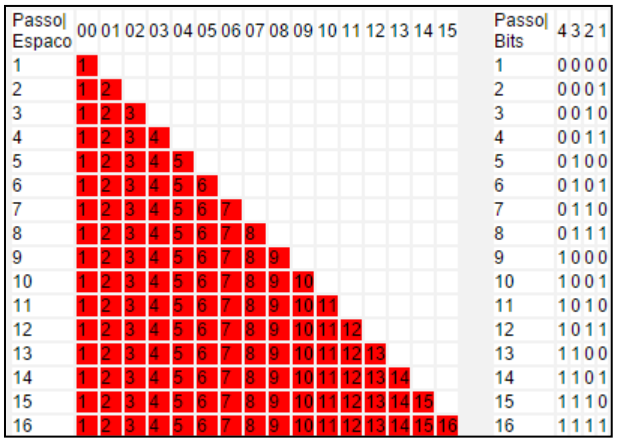

Figura 17. Técnica de alocação Rightmost
Fonte: IPv6.br - Simulação RFC 3531

Passo	Endereco IPv6
1	2001:db8:0000::/36
2	2001:db8:1000::/36
3	2001:db8:2000::/36
4	2001:db8:3000::/36
5	2001:db8:4000::/36
6	2001:db8:5000::/36
7	2001:db8:6000::/36
8	2001:db8:7000::/36
9	2001:db8:8000::/36
10	2001:db8:9000::/36
11	2001:db8:a000::/36
12	2001:db8:b000::/36
13	2001:db8:c000::/36
14	2001:db8:d000::/36
15	2001:db8:e000::/36
16	2001:db8:f000::/36

Figura 18. Divisão da rede /32 em 16 sub-redes com a técnica rightmost
Fonte: IPv6.br - Simulação RFC 3531

- **Leftmost:** Técnica de alocação intervalar, consiste em variar os *bits* da esquerda para criar uma distribuição de endereços de forma intercalada, tendo como propriedade garantir endereços ou blocos livres para expansão, reservando sempre o maior espaço disponível. Além disso, permite uma distribuição mais homogênea. A Figura 19 mostra a variação de 4 bits começando pela esquerda e sequência em que cada sub-rede é alocada dentro do espaço.

Passo| Espaco	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Passo| Bits	4	3	2	1
1	1																1	0	0	0	0
2	1								2								2	1	0	0	0
3	1				3				2								3	0	1	0	0
4	1				3				2				4				4	1	1	0	0
5	1		5		3				2				4				5	0	0	1	0
6	1		5		3				2		6		4				6	1	0	1	0
7	1		5		3		7		2		6		4				7	0	1	1	0
8	1		5		3		7		2		6		4		8		8	1	1	1	0
9	1	9	5		3		7		2		6		4		8		9	0	0	0	1
10	1	9	5		3		7		2	10	6		4		8		10	1	0	0	1
11	1	9	5		3	11	7		2	10	6		4		8		11	0	1	0	1
12	1	9	5		3	11	7		2	10	6		4	12	8		12	1	1	0	1
13	1	9	5	13	3	11	7		2	10	6		4	12	8		13	0	0	1	1
14	1	9	5	13	3	11	7		2	10	6	14	4	12	8		14	1	0	1	1
15	1	9	5	13	3	11	7	15	2	10	6	14	4	12	8		15	0	1	1	1
16	1	9	5	13	3	11	7	15	2	10	6	14	4	12	8	16	16	1	1	1	1

Figura 19. Técnica de alocação Leftmost
Fonte: IPv6.br - Simulação RFC 3531

Na Figura 20, é possível notar que utilizando essa técnica sempre as alocações visam reservar o maior espaço possível para expansão. Sendo a técnica utilizada como base para construção do plano de alocação no cenário deste trabalho.

Passo	Endereco IPv6
1	2001:db8:0000::/36
2	2001:db8:8000::/36
3	2001:db8:4000::/36
4	2001:db8:c000::/36
5	2001:db8:2000::/36
6	2001:db8:a000::/36
7	2001:db8:6000::/36
8	2001:db8:e000::/36
9	2001:db8:1000::/36
10	2001:db8:9000::/36
11	2001:db8:5000::/36
12	2001:db8:d000::/36
13	2001:db8:3000::/36
14	2001:db8:b000::/36
15	2001:db8:7000::/36
16	2001:db8:f000::/36

Figura 20. Divisão da rede /32 em 16 sub-redes com a técnica Leftmost
Fonte: IPv6.br - Simulação RFC 3531

Por padrão as RIRs possuem um prefixo /12 para distribuição em sua área de atuação, prefixo esse que oriundo dos prefixos do tipo *Global Unicast* /3 de responsabilidade da IANA disponibilizados para endereçamento público, além disso, adotam uma política de alocação de prefixos /32 para cada ISP que atende. Partindo desse princípio, é possível inferir que a IANA consegue atender um numero máximo de 512 RIRs (considerando a alocação mímina para cada uma de um /12) e o máximo de ISPs atendidos por RIR é de 1048576.

Seguindo o plano de alocação, o prefixo 2001:db8::/32 recebido pelo ASN 65008 será utilizado para o desenvolvimento do plano de endereçamento utilizado no cenário construído. A técnica de segmentação disponível na RFC 3531 utilizada na aplicação é a ***leftmost***, a qual foi especificada anteriormente. Com isso, a primeira segmentação é a definição do tamanho do prefixo para cada cidade ou região, sendo escolhido nesse cenário um prefixo /40, prefixo de tamanho suficiente para atender 255 cidades ou regiões considerando a reserva do primeiro /40 (2001:db8::/40) para infraestrutura de rede interna do provedor de acesso.

Após a aplicação da técnica *leftmost*, temos definido como segundo prefixo da primeira cidade a sub-rede 2001:db8:8000::/40, a qual foi utilizada como parâmetro para elaboração do plano de alocação desse trabalho de acordo com a Figura 21, correspondente ao fluxograma da segmentação da rede IPv6 do cenário.

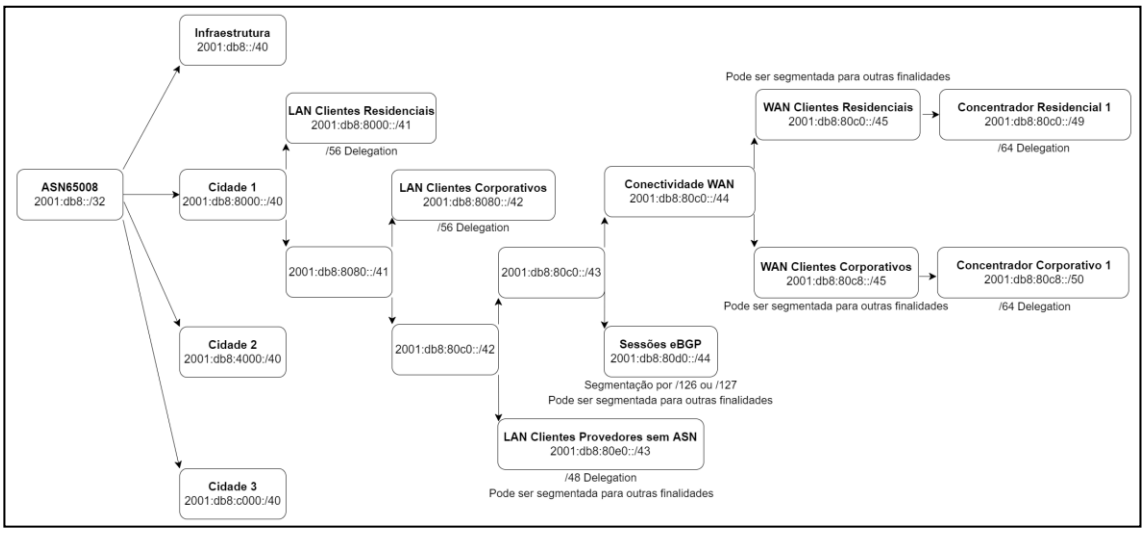

Figura 21. Fluxograma de segmentação do prefixo IPv6 /32 do Router-AS65008 para Cidade 1
Fonte: O autor

A primeira segmentação do prefixo designado para a Cidade 1 define um /41 (2001:db8:8000::/41) para delegação nas redes LANs dos clientes finais por /56, conforme as recomendações do NIC.br, possibilitando o atendimento de pelo menos 32768 redes LANs de clientes residenciais na Cidade 1.

Por outro lado, a segunda sub-rede /41 (2001:db8:8080::/41) é segmentada em dois prefixos /42 e define o primeiro prefixo (2001:db8:8080::/42) para delegação nas redes LANs dos clientes corporativos, a qual também será entregue por /56, atendendo a quantidade máxima de 16384 LANs de clientes corporativos.

A sub-rede 2001:db8:80c0::/42 foi segmentada de modo que o último prefixo /43 (2001:db8:80e0::/43) foi reservado para atendimento das LANs de clientes provedores que não possuem ASN próprio, serão entregues prefixos /48 para cada cliente dessa natureza. Conforme o planejamento, devido a abrangência dessa sub-rede, esse prefixo fica sujeito a segmentações, para atender futuras necessidades que possam surgir. Assim como os prefixos 2001:db8:80d0::/44 reservados para sessões eBGPs com clientes de trânsito IP e os prefixos 2001:db8:80c0::/45 e 2001:db8:80c8::/45 reservados para prover conectividades com as interfaces WANs dos clientes residenciais e corporativos respectivamente, todos eles oriundos da sub-rede 2001:db8:80c0::/43 (primeira sub-rede /43 do prefixo /42 inicialmente mencionado).

Por questão de proporcionalidade, considerando os valores possíveis referente a quantidade de redes LANs atendidas, conforme mencionado anteriormente, a aplicação no cenário efetivou apenas o primeiro prefixo /49 da sub-rede 2001:db8:80c0::/45 para o Concentrador-Residencial e o primeiro /50 do prefixo 2001:db8:80c8::/45 para o Concentrador-Corporativo, que serão delegados por /64 totalizando a quantidade máxima de 32768 e 16384 WANs atendidas por cada concentrador respectivamente, valor correspondente a quantidade de LANs atendidas por cada um deles.

3.3. Simulação

Com a finalidade de construir um cenário mais próximo do real possível, é imprescindível que sua implementação seja em *dual stack*, traduzindo para o português

“pilha dupla”, o termo faz referência as configurações tanto em IPv4 quanto em IPv6, protocolos que não se comunicam entre sí, porém, devido a disponibilidade dos serviços na internet e a grande necessidade de mudar a estrutura da rede garantindo sua expansão de forma otimizada, no cenário construído ambos os protocolos estão presentes. A Figura 22 ilustra o cenário trabalhado e em destaque os parâmetros IPv4 utilizados conforme o planejamento, enquanto que na Figura 23 constam os parâmetros IPv6 utilizados.

Os prefixos IPv4 e IPv6 e número de ASN utilizados para representação da borda da rede e a internet no cenário trabalhado, estão dispostos em tabela conforme o Apêndice 7.

A tabela referente a segmentaçao das sub-redes IPv4 do prefixo público 10.8.0.0/22 do Router-AS65008 está disponível em tabela no Apêdice 8.

A tabela correspondente a segmentação das sub-redes dos prefixos IPv4 privados, utilizados para comunicação interna entre os ativos, atendimento de clientes entre outras funções, estão dispostas na tabela do Apêndice 9.

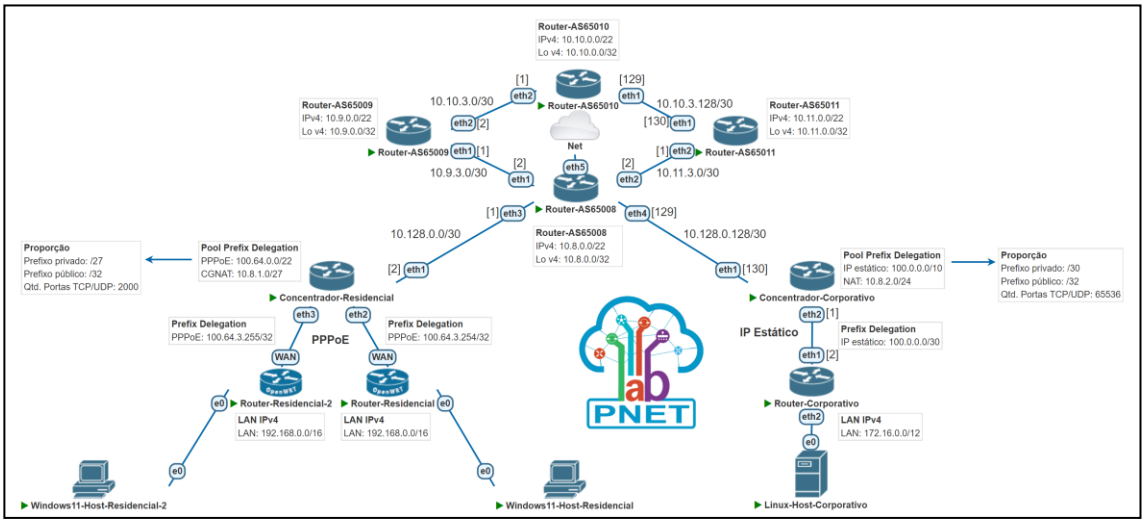

Figura 22. Cenário construído no PNETLAB e parâmetros considerando o planejamento IPv4

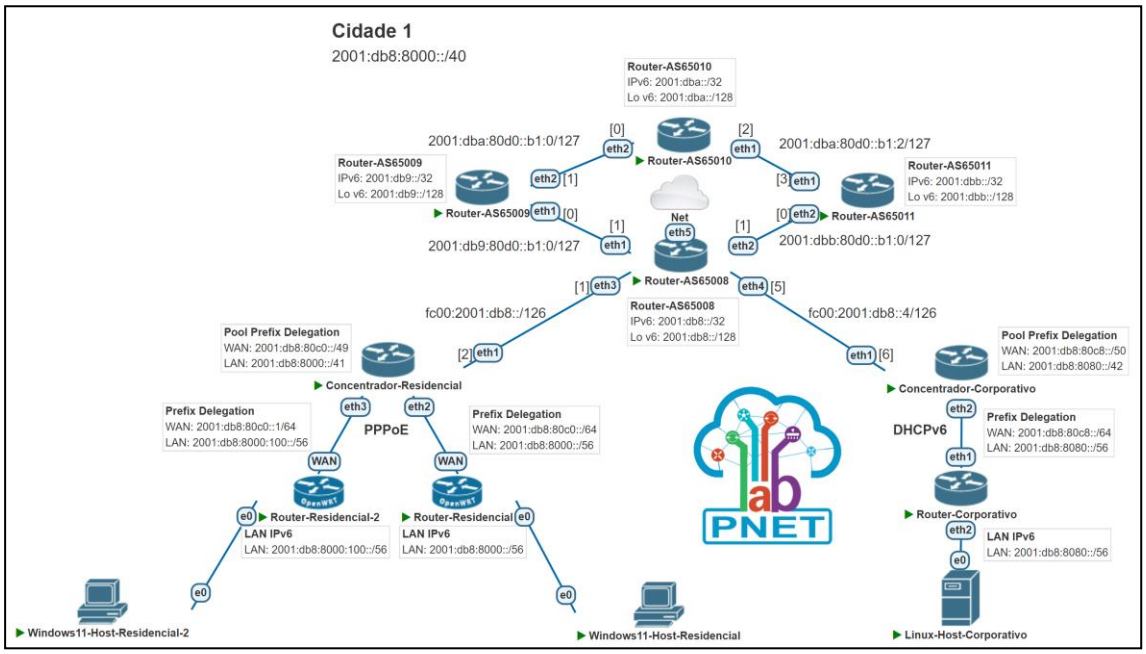

Figura 23. Cenário construído no PNETLAB e parâmetros considerando o planejamento IPv6

3.4. Configurações

- **Router-AS65008:** Na topologia, o Router-AS65008 representa a borda da rede do provedor, o qual estabelece sessões eBGP IPv4 e IPv6 com o Router-AS65009 e Router-AS65011, utilizando os parâmetros de endereçamento destacados nas Figuras 22 e 23 respectivamente, com a finalidade de receber rotas externas via protocolo BGP e anunciar seus prefixos à internet, ou seja, ambos do ponto de vista do Router-AS65008 são operadoras na qual o fornece trânsito IP. Além disso, nele há configurações referente a comunicação ponto a ponto por meio de IP estático com os concentradores Concentrador-Residencial e Concentrador-Corporativo com o objetivo de prover atendimento de clientes por tais equipamentos, disponibilizando prefixos IPv4 e IPv6, os quais possuem roteamento IPv4 para os mesmos por meio de rota estática e OSPF respectivamente, além de roteamento estático IPv6 para ambos. Na topologia desse trabalho, o protocolo OSPF foi aplicado apenas na comunicação IPv4 entre o Router-AS65008 e o Concentrador-Corporativo, no sentido de aprendizagem de rotas por parte do Router-AS65008, mais especificamente das rotas IPv4 criadas de forma manual e dinâmica no Concentrador-Corporativo no ato de ativação de um novo cliente. De contra partida, o Concentrador-Corporativo recebe apenas rota *default* do Router-AS65008, todas essas restrições são configuradas nos filtros OSPF de ambos os equipamentos. Na comunicação IPv6, há roteamento estático dos prefixos 2001:db8:8000::/41 e 2001:db8:80c0::/49 para o Concentrador-Residencial e os prefixos 2001:db8:8080::/42 e 2001:db8:80c8::/50 são roteados para o Concentrador-Corporativo. Sendo o /41 e o /42 paras as LANs dos clientes finais e o /49 e /50 para as interfaces WANs dos clientes. No Apêndice 1, consta o *script* referente a toda configuração aplicada no Router-AS65008 conforme o planejamento e os recursos reservados para a configuração.

- **Router-AS65009, Router-AS65010 e Router AS65011:** O Router-AS65009 e Router-AS65011 representam as operadoras do Router-AS65008 oferecendo trânsito IP para o mesmo conforme especificado anteriormente, estabelecendo sessão eBGP entre eles e o Router-AS65008. Além disso, ambos estabelecem sessões eBGP também com o Router-AS65010, com esse, as sessões segue o padrão de filtros de clientes trânsito, da mesma forma que são configurados os filtros eBGP das duas sessões no Router-AS65008 com as suas operadoras, ou seja, o Router-AS65009 e Router-AS65011 são clientes de trânsito IP do Router-AS65010. Nos Apêndices 2, 3 e 4 constam as configurações aplicadas nos três nós da topologia respectivamente (Router-AS65009, Router-AS65010 e Router-AS65011) que representam de modo geral a internet dentro do cenário construído.
- **Concentrador-Residencial:** O Concentrador-Residencial tem a finalidade de centralizar as autenticações dos clientes residenciais, ele estabelece comunicação ponto a ponto por IP estático *(dual stack)* com a borda da rede (Router-AS65008) e simultaneamente no cenário acima atua como última milha, ou seja, equipamento que faz a abordagem direta com o cliente final. Nas conexões residenciais, os IPs públicos (IPv4) são compartilhados por meio da aplicação da técnica de CGNAT (*Carrier Grade Network Address Translation*), a qual nesse cenário opera em uma proporção de um /27 privado para um /32 público, ou seja, um único IPv4 público atende 32 clientes residenciais com IP fixo compartilhado com 2000 portas TCP e UDP externas em um range exclusivo para cada cliente. O provisionamento do serviço em IPv4 por meio do Concentrador-Residencial é realizado através do protocolo PPPoE que possui suporte a entrega de prefixos IPv6 aos routers residenciais, Criando de forma dinâmica um DHCPv6 server, o qual é definido primeiramente dois *pools* de endereços, um /41 para as LANs, os quais serão delegados de forma seguimentada por conexão, sendo uma sub-rede /56 por cliente, enquanto que da mesma forma serão delegados um prefixo /64 oriundo do prefixo /49 do *pool* de IPv6 disponibilizado para as interfaces WANs dos clientes finais, esses *pools* são criados e referenciados no *profile* de autenticação PPPoE, conforme o plano de alocação apresentado. No Apêndice 5 constam as configurações em RouterOS aplicadas no Concentrador-Residencial.
- **Concentrador-Corporativo:** O Concentrador-Corporativo tem a finalidade de centralizar as autenticações dos clientes corporativos, clientes esses que comumente nos ISPs possuem atendimento direcionado, SLA (*Service Level Agreement*) de curto prazo e infraestrutura de rede mais complexa, pois normalmente possuem serviços hospedados em suas redes locais. A autenticação desse tipo de cliente no cenário está dissossiada em um equipamento dedicado a essa demanda, pelo fato de otimizar o *troubleshooting* em casos de falhas e intervenções preventivas, como todos os outros equipamentos, ele estabelece comunicação ponto a ponto por IP estático *(dual stack)* diretamente com a borda da rede (Router-AS65008) e simultaneamente no cenário acima atua como última milha, ou seja, equipamento que faz a abordagem direta com o cliente final como no Concetrador-Residencial. Nas conexões corporativas, os IPs públicos (IPv4) não são compartilhados e nem delegados de forma dinâmica, há a necessidade de delegar um endereço exclusivo e fixo para a conexão do

cliente. O provisionamento do serviço em IPv4 por meio do Concentrador-Corporativo é realizado através de uma comunicação ponto a ponto utilizando IP estático estabelecida com o Router-Corporativo, além disso, há a necessidade de configuração de uma rota estática para o prefixo IPv4 /32 disponibilizado para a conexão do cliente e o NAT, que é basicamente a tradução de IPv4 privado para IPv4 público, possibilitando o roteamento do pacote para a internet. De outro modo, a entrega de prefixos IPv6 e rota *defaut* IPv6 é realizada de forma dinâmica via protocolo DHCPv6, o qual é definido primeiramente dois *pools* de endereços, um /42 para as LANs, os quais serão delegados de forma seguimentada por conexão, sendo uma sub-rede /56 por cliente, enquanto que da mesma forma serão delegados um prefixo /64 oriundo do prefixo /50 do *pool* de IPv6 disponibilizado para as interfaces WANs do clientes finais, conforme o plano de alocação apresentado. No Apêndice 6 constam as configurações em RouterOS aplicadas no Concentrador-Corporativo.

- **Router-Residencial e Router-Residencial-2:** Os roteadores residenciais, comumente não são roteadores RouterOS, por esse motivo, no cenário trabalhado, foram utilizadas as imagens do OpenWrt, sistema *open source* de alta performance, indicado para utilização em roteadores residenciais de diversos fabricantes e modelos. Basicamente foi configurado um PPPoE *client* com as credenciais *residencial1* e *residencial2* nas interfaces WANs de cada roteador residencial (interface que estabelece comunicação física com o Concentrador-Residencial). As interfaces LANs por padrão estão atribuídas a uma *bridge* onde opera o DHCP e DHCPv6 *servers* conforme os prefixos IPv4 reservados para endereçamento privado especificados na RFC 1918 e prefixos IPv6 públicos recebidos do Concentrador-Residencial, configuração de mascaramento IPv4 e rotas *defaults* recebidas dinamicamente via protocolo PPPoE e DHCPv6.
- **Router-Corporativo:** O Router-Corporativo é o roteador responsável por receber o *link* da operadora e muita das vezes a aplicação das regras de *firewall*. No provisionamento foi configurada a comunicação ponto a ponto por meio de IPv4 estático e configuração de DHCPv6 *client* na interface *uplink* (interface que estabelece comunicação física com o Concentrador-Corporativo), uma interface *bridge* com as interfaces restantes atribuídas a ela com DHCP e DHCPv6 *servers* conforme os prefixos IPv4 reservados para endereçamento privado (RFC 1918) e prefixos IPv6 públicos recebidos do Concentrador-Corporativo e configuração de mascaramento IPv4. Nesse equipamento as rotas *defaults* foram configuradas de forma estática para comunicação IPv4 e recebidas de forma dinâmica por meio do DHCPv6.

É importante destacar que no cenário real, é comum a utilização entre concentrador e o cliente final, de um equipamento específico para realização de abordagem física com o cliente. Esses equipamentos são chamados de “equipamentos de última milha”. Nos casos de redes FTTH (Fiber-to-the-Home) são utilizadas as OLTs (*Optical Line Terminal*) enquanto que nas redes *ethernet* são utilizados *Switches Layer 2* (camada de enlace), e por fim, em redes de atedimento via rádio são utilizados os pontos de acesso.

Com a finalidade de simplificar o cenário e de enfatizar as configurações de roteamento e entrega de prefixos aos clientes, a adoção de equipamentos de última

milha foi dispensada no cenário apresentado, havendo uma comunicação física direta entre os concentradores e o equipamento do cliente final, no entanto, é válido ressaltar que não há qualquer impecílio ou divergência nas configurações aplicadas, caso houvesse equipamentos de última milha, ou seja, as configurações do cenário, podem evidentemente servir como base para aplicação em cenários reais.

4. Resultados

4.1. Delegação

Como principais resultados do projeto, é possível evidenciar com base nas imagens a seguir, a delegação de prefixos IPv6 dos *pools* designados as interfaces WANs e LANs por parte dos concetradores (Concentrador-Residencial e Concentrador-Corporativo) e atribuição conforme o planejamento, tanto de IPv4 quanto de IPv6 nas placas de rede das estações Windows11-Host-Residencial, Windows11-Host-Residencial-2 e Linux-Host-Corporativo.

A Figura 24 é pertinente a uma captura de tela do Winbox, que demonstra a delegação dos prefixos IPv6 via RouterOS por parte do Concentrador-Residencial, a qual é possível identificar os *pools* de IPv6 designados às LANs e WANs, que são atribuídos por /56 e /64 respectivamente, conforme o plano de alocação dos clientes residenciais.

Além disso, é evidente quais protocolos são utilizados na entrega dos prefixos, sendo DHCP para as redes LANs e PPPoE para interfaces WANs dos roteadores residenciais. Baseando-se nos endereços MACs e nas credenciais do protocolo PPPoE utilizados para cada cliente, é possível constatar que os prefixos 2001:db8:80c0::/64 e 2001:db8:8000::/56, assim como, os prefixos 2001:db8:80c0:1::/64 e 2001:db8:8000:100::/56, estão sendo atribuídos para os roteadores Router-Residencial e Router-Residencial-2 respectivamente.

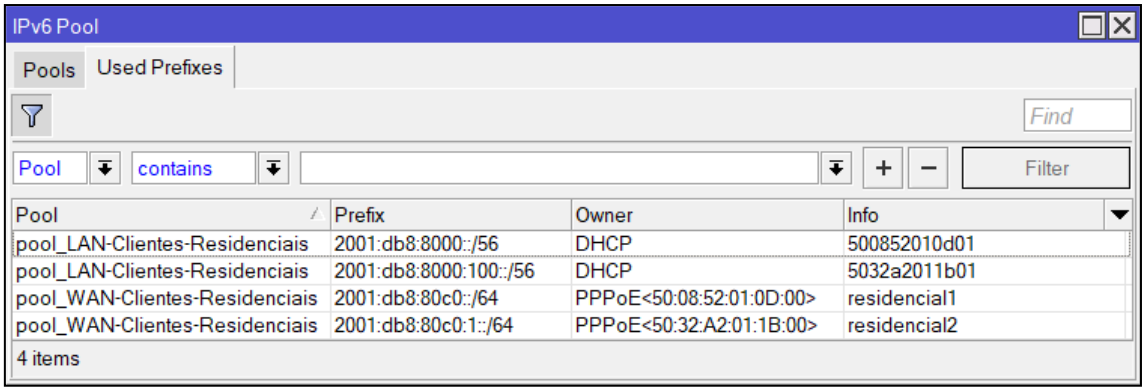

Figura 24. Delegação de prefixos IPv6 (WAN e LAN) pelo Concentrador-Residencial
Fonte: O autor

Também seguindo o plano de alocação, conforme ateriormente especificado e demonstrado nas Figuras 21 e 23, a Figura 25 evidencia por meio do Winbox, a delegação dos prefixos IPv6 via RouterOS por parte do Concentrador-Corporativo, onde é notório os *pools* de IPv6 designados às LANs e WANs, que são atribuídos por /56 e /64 respectivamente, aos clientes corporativos.

Nesse sentido, a entrega é realizada por meio de ponto a ponto estático utilizando o prefixo 2001:db8:80c8::/64 do *pool* designado às interfaces WANs, e a sub-rede 2001:db8:8080::/56 via DHCPv6 para as LANs dos clientes corporativos.

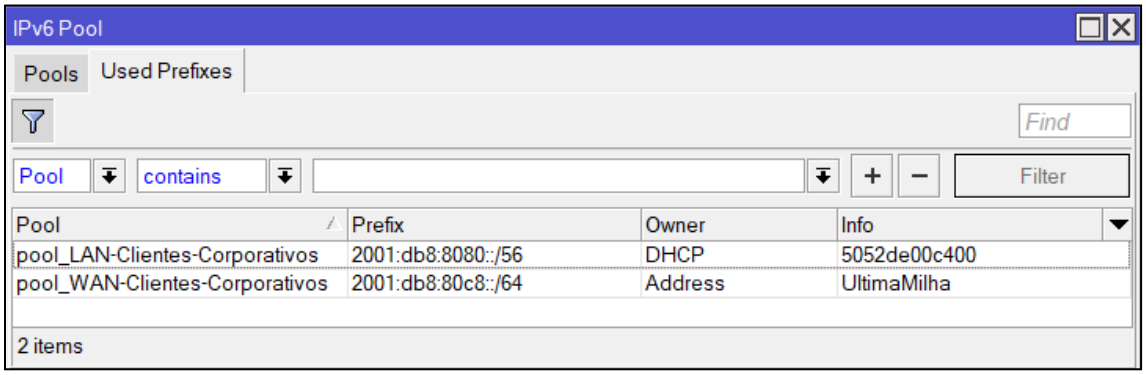

Figura 25. Delegação de prefixos IPv6 (WAN e LAN) pelo Concentrador-Corporativo
Fonte: O autor

As Figuras 26 e 27 demonstram o recebimento dos prefixos IPv4 e IPv6 no OpenWrt utilizado nos roteadores residenciais do cenário, Router-Residencial e Router-Residencial-2 respectivamente. É evidente que os prefixos IPv6 recebidos nas WANs e LANs estão de acordo com o planejamento anteriormente especificado, por padrão o OpenWrt entrega na LAN um prefixo /60 proveniente do prefixo /56 recebido para essa finalidade.

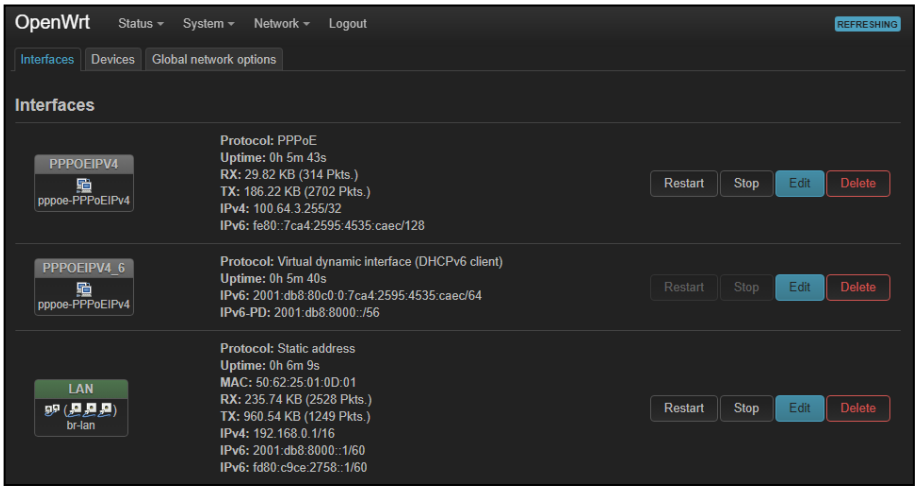

Figura 26. Recebimento de prefixos IPv4 e IPv6 no OpenWrt Router-Residencial
Fonte: O autor

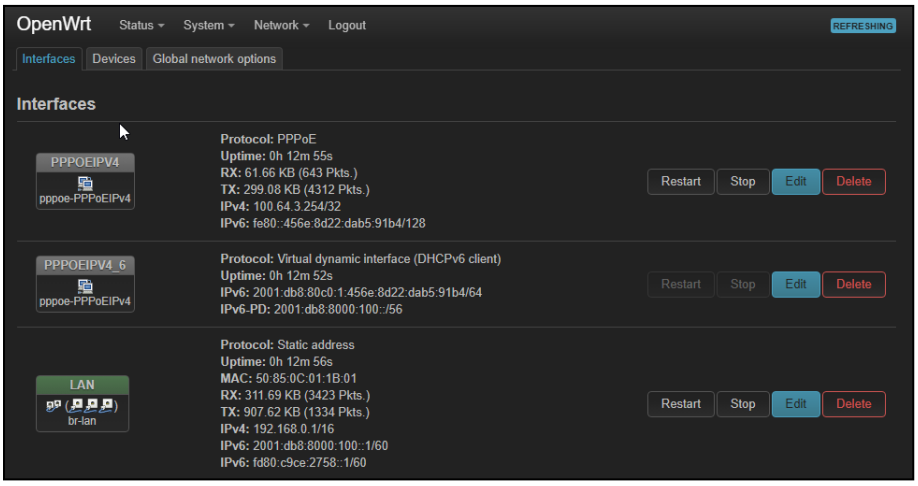

Figura 27. Recebimento de prefixos IPv4 e IPv6 no OpenWrt Router-Residencial-2
Fonte: O autor

As Figuras 28 e 29 são referentes a demonstração dos prefixos recebidos nas interfaces dos *hosts* Windows11-Host-Residencial e Windows11-Host-Residencial-2 respectivamente, por meio do comando "*ipconfig*" disponível no sistema operacional Windows, é possível identificar os prefixos IPv4 e IPv6 recebidos dos roteadores residenciais.

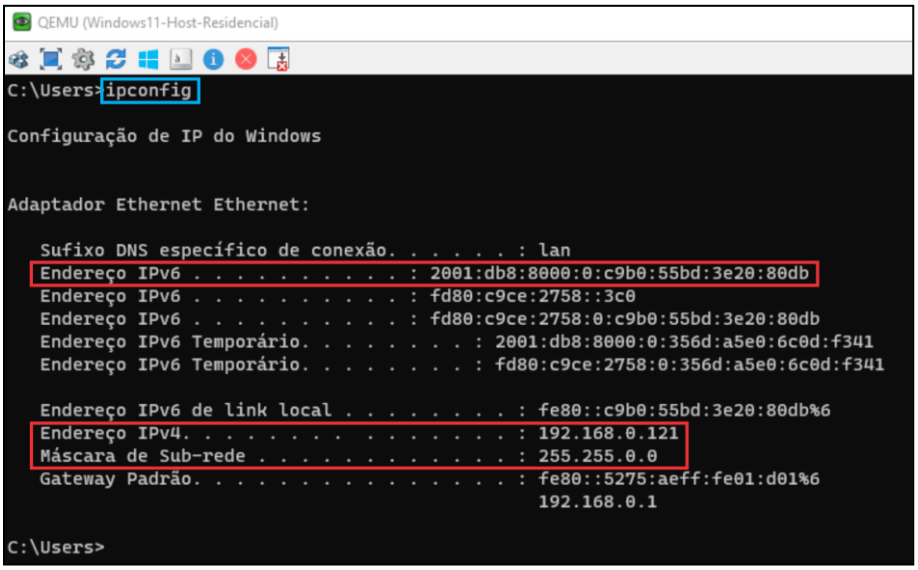

Figura 28. Atribuição de endereços IPv4 e IPv6 no Windows11-Host-Residencial
Fonte: O autor

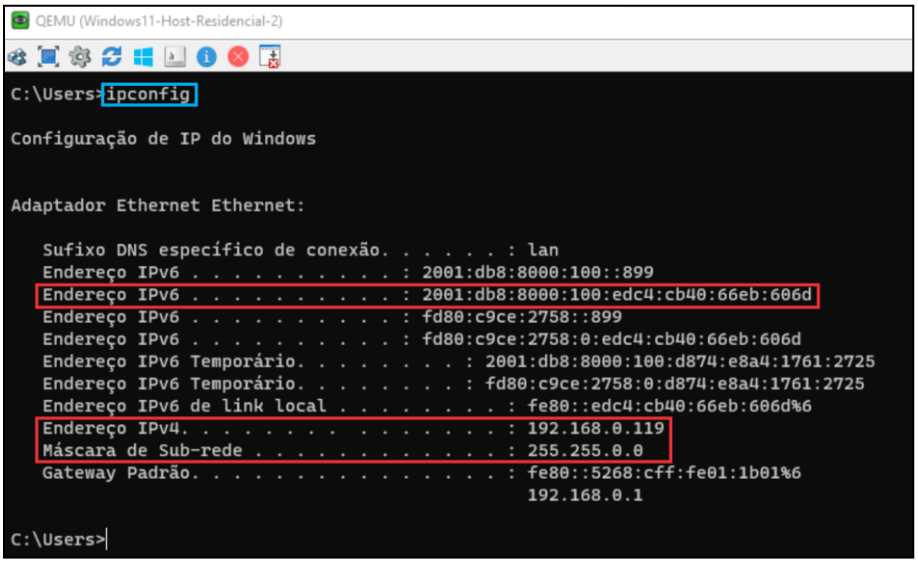

Figura 29. Atribuição de endereços IPv4 e IPv6 no Windows11-Host-Residencial-2
Fonte: O autor

A Figura 30 demonstra os prefixos recebidos na interface do *host* Linux-Host-Corporativo, por meio do comando "*ip address show*" disponível no sistema operacional Linux, é possível identificar os prefixos IPv4 e IPv6 recebidos do Router-Corporativo. Além de, rota *default* recebida via IP do tipo *Link Local* conforme o destaque na imagem abaixo, resultado obtido por meio do comando "*ip -6 route*".

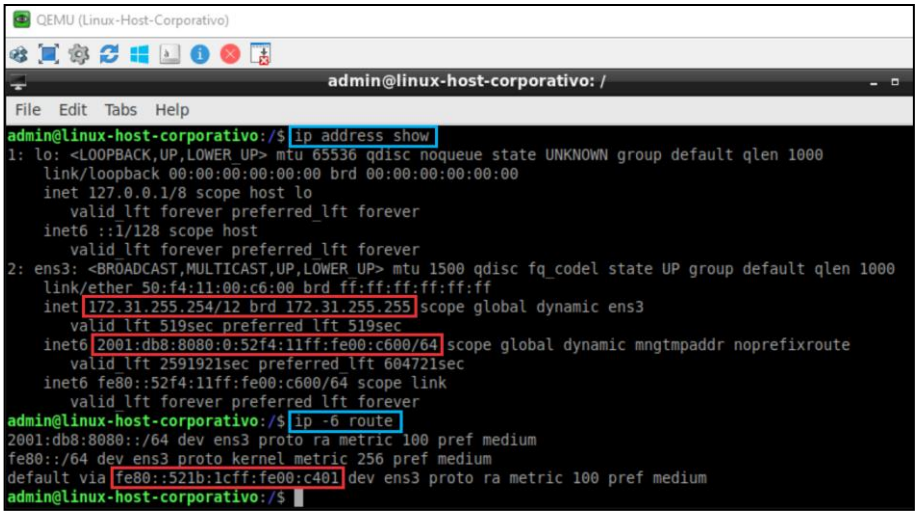

Figura 30. Atribuição de endereços IPv4 e IPv6 e rota default no Linux-Host-Corporativo
Fonte: O autor

4.2. Conectividade

Nas Figuras a seguir, constam as evidências dos testes de conectividade via sistema *traceroute* (no Windows *tracert*) entre os *hosts* (Windows11-Host-Residencial, Windows11-Host-Residencial-2 e Linux-Host-Corporativo) e o endereço IPv4 e IPv6 de *loopback* dos roteadores Router-AS65009, Router-AS65010 e Router-AS65011, os quais no cenário em questão representam a internet, além de, testes de conectividade por

meio das ferramentas *ping* e *tracert* entre os *hosts* Windows11-Host-Residencial e Linux-Host-Corporativo,

A Figura 31 é referente ao teste de conectividade entre o *host* Windows11-Host-Residencial e o Router-AS65009, o qual no cenário representa a internet, constatando a conectividade entre eles por meio do comando "*tracert*" que retorna o caminho dos pacotes salto a salto até o destino final.

Nesse sentido, é notório que há 4 saltos entre os nós da rede, a latência média para o destino é 3ms, os endereços IPs, tanto IPv4 quanto IPv6, estão de acordo com o planejamento especificado anteriormente e com as informações do Apêndice 9, correspondente a tabela de planejamento IPv4.

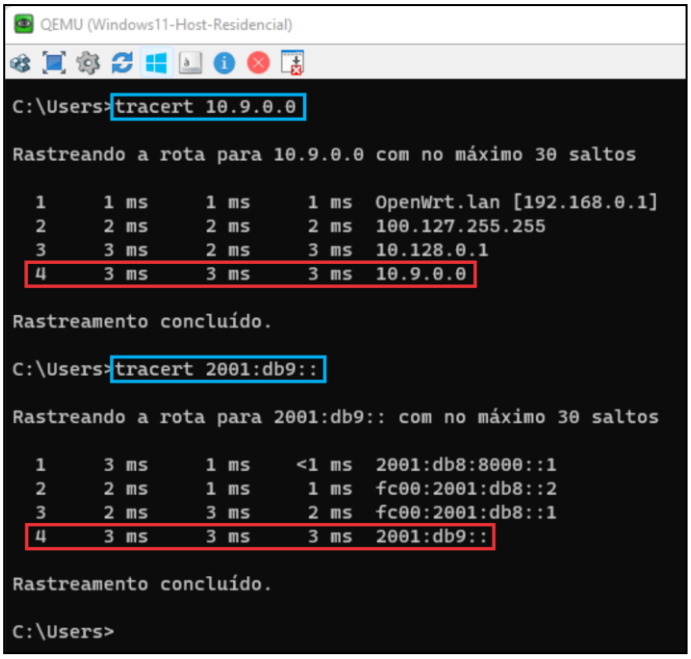

Figura 31. Tracert com origem Windows11-Host-Residencial e destino Router-AS65009
Fonte: O autor

A Figura 32 demonstra o teste de conectividade entre o *host* Windows11-Host-Residencial-2 e o Router-AS65011, o qual no cenário também representa a internet, evidenciando a comunicação entre eles por meio do comando "*tracert*". Assim como na Figura 31, a latência média para o destino final é 3ms, independente do protocolo utilizado no teste.

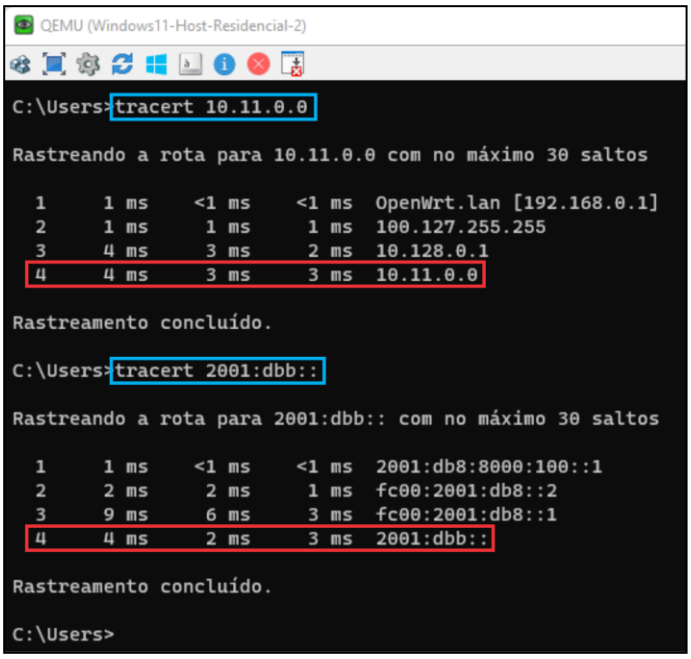

Figura 32. Tracert com origem Windows11-Host-Residencial-2 e destino Router-AS65011
Fonte: O autor

Na Figura 33 é evidente a comunicação estabelecida entre o *host* Linux-Host-Corporativo e o Router-AS65010, representando a internet no cenário, comprovando por meio do comando "*traceroute*" disponível no sistema operacional Linux, a conectividade entre eles.

É importante destacar que no resultado em questão, há um aumento considerável no valor médio de latência, devido o aumento de saltos para os pacotes lançados chegarem ao seu destino e até mesmo pela diferença do sistema operacional utilizado na origem.

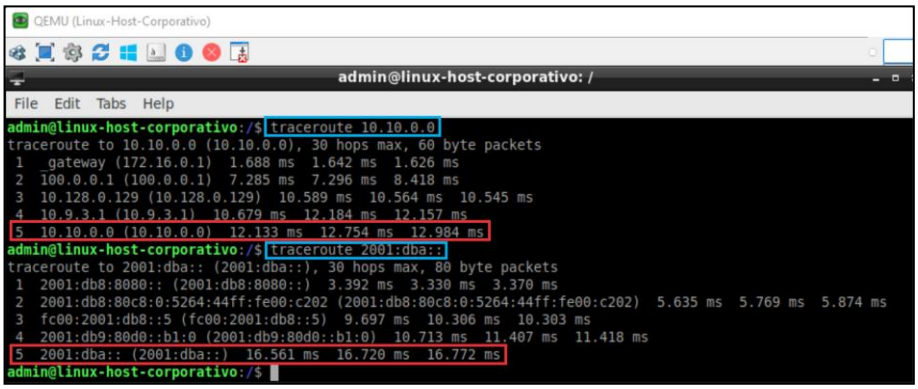

Figura 33. Traceroute com origem Linux-Host-Corporativo e destino Router-AS65010
Fonte: O autor

A Figura 34 corresponde a comunicação estabelecida por meio do protocolo IPv6 entre o *host* Windows11-Host-Residencial e o *host* Linux-Host-Corporativo, neste resultado, a comunicação não é efetivada por meio da internet, e sim, por meio da rede interna do próprio provedor de acesso, afinal, ambos são clientes da mesma operadora.

Os resultados foram obtidos por meio dos comandos disponibilizados no Windows "*ping*" e "*tracert*" garantido o acesso a qualquer serviço que esteja disponibilizado na rede local do Router-Corporativo com latência média de 6ms.

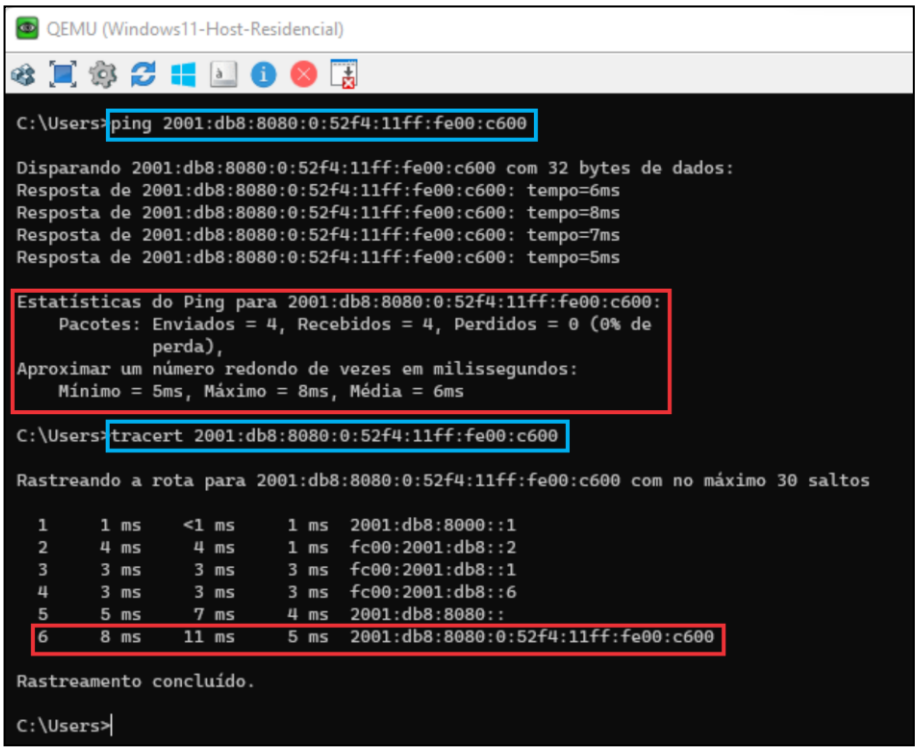

Figura 34. Ping e Tracert com origem Windows11-Host-Residencial e destino Linux-Host-Corporativo
Fonte: O autor

5. Conclusão

Com a incompatibilidade entre os protocolos IPv4 e IPv6, é evidente que haja um período de transição dos serviços na internet para a nova versão do protocolo, período esse, que nesse contexto é realidade. Com isso, várias técnicas foram desenvolvidas para amenizar os impactos gerados nesse cenário, técnicas que prolongam o uso do protocolo IPv4, afetando diretamente a comunicação fim a fim na internet sem a adoção concomitante do IPv6, assim como, técnicas que implicam na utilização de IPv6 nativo pelos usuários finais, de forma que túneis IPv4 dentro de IPv6 devem ser preferidos em detrimento de túneis IPv6 sobre IPv4, essas últimas devem ser sempre preferenciais.

O plano de segmentação e alocações de prefixos IPv6 é relativo, pois cada cenário pode apresentar uma demanda específica, a qual pode ou não está relacionada com o planejamento. No entanto, de acordo com a proposta apresentada pelo artigo, os resultados obtidos foram bem sucedidos, foram disponibilizados os *scripts* com as configurações em um *vendor* específico (Mikrotik) que se faz presente majoritariamente

na infraestrutura de rede dos ISPs, especialmente os mais recentes no mercado de provedores.

Os parâmetros lógicos utilizados (ASN, IPv4 públicos e privados no contexto do cenário e IPv6) foram antepostos com o objetivo de construir um plano genérico de segmentação e alocação, que facilmente podem ser substituídos em casos de aplicações em cenários reais.

Referências

Simon Kemp (2021) "60% of the world is online — 10 big takeaways on the state of the internet in 2021", https://thenextweb.com/news/60-of-the-world-is-online-10-big-takeaways-on-the-state-of-the-internet-in-2021

IPv6.br (2020) "ACABOUUUU: Reservas de IPv4 chegam ao fim!", https://ipv6.br/post/fim-do-ipv4/

Google IPv6 (2022) "Porcentagem de usuários que acessam o Google por meio de IPv6.", https://www.google.com/intl/pt-BR/ipv6/statistics.html

Hurricane Eletric Internet Services (2022), "Hurricane Electric IPv4 Exhaustion Counters", https://ipv6.he.net/statistics/

IP Location (2021). "What is IANA?", https://www.iplocation.net/what-is-iana

S. Deering e R. Hinden RFC 2460 (1998), "Internet Protocol, Version 6 (IPv6) Specification", https://www.rfc-editor.org/rfc/rfc2460

S. Bradner e A. Mankin RFC 1550 (1993), "IP: Next Generation (IPng) White Paper Solicitation", https://www.rfc-editor.org/rfc/rfc1550

Oracle (2021), "O que é IoT?", https://www.oracle.com/br/internet-of-things/what-is-iot/

Portal de dados CETIC.br (2020), "F4 - EMPRESAS PROVEDORAS, POR DIFICULDADE DE ATIVAÇÃO DO IPV6", https://data.cetic.br/explore/?pesquisa_id=19

Pedro Pinto PPLWARE (2012), "Vamos conhecer o RouterOS dos equipamentos Mikrotik", https://pplware.sapo.pt/microsoft/windows/vamos-conhecer-o-routeros-dos-equipamentos-mikrotik/

Mikrotik (2022), "About us", https://mikrotik.com/aboutus

VIVAOLINUX (2011), "Você conhece o RouterOS Mikrotik?", https://www.vivaolinux.com.br/artigo/Voce-conhece-o-RouterOS-Mikrotik?pagina=1

NIC.br (2010), "Curso IPv6 Básico", https://ipv6.br/media/arquivo/ipv6/file/48/IPv6-apostila.pdf

T. Mendez e W. Milliken RFC 1546 (1993), "Host Anycasting Service", https://www.rfc-editor.org/rfc/rfc1546

Hagen (2006), "IPv6 Essentials, 2ª ed. O'Reilly Media"

K. Lougheed e Y. Rekhter RFC 1105 (1989), "A Border Gateway Protocol (BGP)", https://www.rfc-editor.org/rfc/rfc1105

Y. Rekhter e S. Hares RFC 4271 (2006), “A Border Gateway Protocol 4 (BGP-4)”, https://www.rfc-editor.org/rfc/rfc4271

J. Moy RFC 2328 (1998), “OSPF Version 2”, https://www.rfc-editor.org/rfc/rfc2328.html

R. Droms RFC 3315 (2003), “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, https://www.rfc-editor.org/rfc/rfc3315

PNETLab (2022), “What is PNETLab?”, https://pnetlab.com/pages/documentation?slug=what-is-PNETlab

IPv6.br (2022), “Simulação RFC 3531”, https://ipv6.br/paginas/subnet

Julião Braga (2011), “Idéias sobre o que fazer com um bloco /32 do IPv6-I”, https://ii.blog.br/tag/ipv6/

Y. Rekhter e B. Moskowitz RFC 1918 (1996), “Address Allocation for Private Internets”, https://www.rfc-editor.org/rfc/rfc1918.html

7. Apêndices

Apêndice 1

Configuração RouterOS do Router-AS65008:

```
/interface bridge add name=Loopback
/interface ethernet set [ find default-name=ether1 ] comment=Router-AS65009
/interface ethernet set [ find default-name=ether2 ] comment=Router-AS65011
/interface ethernet set [ find default-name=ether3 ] comment=Concentrador-Residencial
/interface ethernet set [ find default-name=ether4 ] comment=Concentrador-Corporativo
/interface ethernet set [ find default-name=ether5 ] comment=Net
/interface wireless security-profiles set [ find default=yes ] supplicant-
identity=MikroTik
/routing bgp instance set default as=65008 router-id=10.8.0.0
/routing ospf instance set [ find default=yes ] distribute-default=always-as-type-1
redistribute-connected=as-type-1 redistribute-static=as-type-1 router-id=10.8.0.0
/ip address add address=10.128.0.1/30 comment=Concentrador-Residencial interface=ether3
network=10.128.0.0
/ip address add address=10.128.0.129/30 comment=Concentrador-Corporativo
interface=ether4 network=10.128.0.128
/ip address add address=10.8.0.0 comment=Loopback interface=Loopback network=10.8.0.0
/ip address add address=10.11.3.2/30 comment=Router-AS65011 interface=ether2
network=10.11.3.0
/ip address add address=10.9.3.2/30 comment=Router-AS65009 interface=ether1
network=10.9.3.0
/ip dhcp-client add disabled=no interface=ether1
/ip route add comment=CGNAT distance=1 dst-address=10.8.1.0/27 gateway=10.128.0.2
/ip route add comment=CGNAT distance=1 dst-address=100.64.0.0/22 gateway=10.128.0.2
/ipv6 address add address=2001:dbb:80d0::b1:1/127 advertise=no comment=AS65011
interface=ether2
/ipv6 address add address=2001:db9:80d0::b1:1/127 advertise=no comment=AS65009
interface=ether1
/ipv6 address add address=2001:db8::/128 advertise=no comment=Loopback
interface=Loopback
/ipv6 address add address=fc00:2001:db8::1/126 advertise=no comment=Concentrador-
Residencial interface=ether3
/ipv6 address add address=fc00:2001:db8::5/126 advertise=no comment=Concentrador-
Corporativo interface=ether4
/ipv6 route add comment=LAN-Clientes-Residenciais distance=1 dst-
address=2001:db8:8000::/41 gateway=fc00:2001:db8::2
/ipv6 route add comment=LAN-Clientes-Corporativos distance=1 dst-
address=2001:db8:8080::/42 gateway=fc00:2001:db8::6
/ipv6 route add comment=WAN-Clientes-Residenciais distance=1 dst-
address=2001:db8:80c0::/49 gateway=fc00:2001:db8::2
/ipv6 route add comment=WAN-Clientes-Corporativos distance=1 dst-
address=2001:db8:80c8::/50 gateway=fc00:2001:db8::6
```

```
/routing bgp network add network=10.8.0.0/22 synchronize=no
/routing bgp network add network=2001:db8::/32 synchronize=no
/routing bgp network add disabled=yes network=10.8.0.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.8.1.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.8.2.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.8.3.0/24 synchronize=no
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65009 name=AS65009 out-filter=OUT-
IPv4-65009 remote-address=10.9.3.1 remote-as=65009
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65011
name=AS65011 out-filter=OUT-IPv6-65011 remote-address=2001:dbb:80d0::b1:0 remote-
as=65011
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65009
name=AS65009 out-filter=OUT-IPv6-65009 remote-address=2001:db9:80d0::b1:0 remote-
as=65009
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65011 name=AS65011 out-filter=OUT-
IPv4-65011 remote-address=10.11.3.1 remote-as=65011
/routing filter add action=discard chain=IN-IPv4-65009 comment=Operadora
prefix=10.8.0.0/22 prefix-length=22-24
/routing filter add action=accept chain=IN-IPv4-65009 prefix=0.0.0.0/0
/routing filter add action=accept chain=IN-IPv4-65009
/routing filter add action=accept chain=OUT-IPv4-65009 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=discard chain=OUT-IPv4-65009
/routing filter add action=discard chain=IN-IPv6-65009 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=accept chain=IN-IPv6-65009 prefix=::/0
/routing filter add action=accept chain=IN-IPv6-65009
/routing filter add action=accept chain=OUT-IPv6-65009 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=OUT-IPv6-65009
/routing filter add action=discard chain=IN-IPv4-65011 comment=Operadora
prefix=10.8.0.0/22 prefix-length=22-24
/routing filter add action=accept chain=IN-IPv4-65011 prefix=0.0.0.0/0
/routing filter add action=accept chain=IN-IPv4-65011
/routing filter add action=accept chain=OUT-IPv4-65011 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=discard chain=OUT-IPv4-65011
/routing filter add action=discard chain=IN-IPv6-65011 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=accept chain=IN-IPv6-65011 prefix=::/0
/routing filter add action=accept chain=IN-IPv6-65011
/routing filter add action=accept chain=ospf-in prefix=10.8.0.0/22 prefix-length=22-32
/routing filter add action=accept chain=OUT-IPv6-65011 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=OUT-IPv6-65011
/routing filter add action=accept chain=ospf-in prefix=100.0.0.0/10 prefix-length=10-30
/routing filter add action=discard chain=ospf-in
/routing filter add action=accept chain=ospf-out prefix=0.0.0.0/0
/routing filter add action=discard chain=ospf-out
/routing ospf network add area=backbone network=10.128.0.128/30
/system identity set name=Router-AS65008
/tool romon set enabled=yes
```

Apêndice 2

Configuração RouterOS do Router-AS65009:

```
/interface bridge add name=Loopback
/interface ethernet set [ find default-name=ether1 ] comment=Router-AS65008
/interface ethernet set [ find default-name=ether2 ] comment=Router-AS65010
/interface wireless security-profiles set [ find default=yes ] supplicant-
identity=MikroTik
/routing bgp instance set default as=65009 router-id=10.9.0.0
/ip address add address=10.9.0.0 comment=Loopback interface=Loopback network=10.9.0.0
/ip address add address=10.10.3.2/30 comment=Router-AS65010 interface=ether2
network=10.10.3.0
/ip address add address=10.9.3.1/30 comment=Router-AS65008 interface=ether1
network=10.9.3.0
/ip dhcp-client add disabled=no interface=ether1
/ipv6 address add address=2001:db9:80d0::b1:0/127 advertise=no comment=AS65008
interface=ether1
```

```
/ipv6 address add address=2001:dba:80d0::b1:1/127 advertise=no comment=AS65010
interface=ether2
/ipv6 address add address=2001:db9::/128 advertise=no comment=Loopback
interface=Loopback
/routing bgp network add network=2001:db9::/32 synchronize=no
/routing bgp network add network=10.9.0.0/22 synchronize=no
/routing bgp network add disabled=yes network=10.9.1.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.9.2.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.9.3.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.9.0.0/24 synchronize=no
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65008 name=AS65008 out-filter=OUT-
IPv4-65008 remote-address=10.9.3.2 remote-as=65008
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65010 name=AS65010 out-filter=OUT-
IPv4-65010 remote-address=10.10.3.1 remote-as=65010
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65008
name=AS65008 out-filter=OUT-IPv6-65008 remote-address=2001:db9:80d0::b1:1 remote-
as=65008
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65010
name=AS65010 out-filter=OUT-IPv6-65010 remote-address=2001:dba:80d0::b1:0 remote-
as=65010
/routing filter add action=accept chain=IN-IPv4-65008 comment=Cliente prefix=10.8.0.0/22
prefix-length=22-24
/routing filter add action=discard chain=IN-IPv4-65008
/routing filter add action=discard chain=OUT-IPv4-65008 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=accept chain=OUT-IPv4-65008
/routing filter add action=accept chain=IN-IPv6-65008 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=IN-IPv6-65008
/routing filter add action=discard chain=OUT-IPv6-65008 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=accept chain=OUT-IPv6-65008
/routing filter add action=discard chain=IN-IPv4-65010 comment=Operadora
prefix=10.9.0.0/22 prefix-length=22-24
/routing filter add action=accept chain=IN-IPv4-65010 prefix=0.0.0.0/0
/routing filter add action=accept chain=IN-IPv4-65010
/routing filter add action=accept chain=OUT-IPv4-65010 prefix=10.9.0.0/22 prefix-
length=22-24
/routing filter add action=accept chain=OUT-IPv4-65010 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=discard chain=OUT-IPv4-65010
/routing filter add action=discard chain=IN-IPv6-65010 prefix=2001:db9::/32 prefix-
length=32-48
/routing filter add action=accept chain=IN-IPv6-65010 prefix=::/0
/routing filter add action=accept chain=IN-IPv6-65010
/routing filter add action=accept chain=OUT-IPv6-65010 prefix=2001:db9::/32 prefix-
length=32-48
/routing filter add action=accept chain=OUT-IPv6-65010 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=OUT-IPv6-65010
/system identity set name=Router-AS65009
/tool romon set enabled=yes
```

Apêndice 3

Configuração RouterOS do Router-AS65010:

```
/interface bridge add name=Loopback
/interface ethernet set [ find default-name=ether1 ] comment=Router-AS65011
/interface ethernet set [ find default-name=ether2 ] comment=Router-AS65009
/interface wireless security-profiles set [ find default=yes ] supplicant-
identity=MikroTik
/routing bgp instance set default as=65010 router-id=10.10.0.0
/ip address add address=10.10.0.0 comment=Loopback interface=Loopback network=10.10.0.0
/ip address add address=10.10.3.1/30 comment=Router-AS65009 interface=ether2
network=10.10.3.0
/ip address add address=10.10.3.129/30 comment=Router-AS65011 interface=ether1
network=10.10.3.128
/ip dhcp-client add disabled=no interface=ether1
/ipv6 address add address=2001:dba:80d0::b1:0/127 advertise=no comment=AS65009
interface=ether2
```

```
/ipv6 address add address=2001:dba:80d0::b1:2/127 advertise=no comment=AS65011
interface=ether1
/ipv6 address add address=2001:dba::/128 advertise=no comment=Loopback
interface=Loopback
/routing bgp network add network=10.10.0.0/22 synchronize=no
/routing bgp network add disabled=yes network=10.10.0.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.10.1.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.10.2.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.10.3.0/24 synchronize=no
/routing bgp network add network=2001:dba::/32 synchronize=no
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65009 name=AS65009 out-filter=OUT-
IPv4-65009 remote-address=10.10.3.2 remote-as=65009
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65009
name=AS65009 out-filter=OUT-IPv6-65009 remote-address=2001:dba:80d0::b1:1 remote-
as=65009
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65011 name=AS65011 out-filter=OUT-
IPv4-65011 remote-address=10.10.3.130 remote-as=65011
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65011
name=AS65011 out-filter=OUT-IPv6-65011 remote-address=2001:dba:80d0::b1:3 remote-
as=65011
/routing filter add action=accept chain=IN-IPv4-65009 comment=Cliente prefix=10.9.0.0/22
prefix-length=22-24
/routing filter add action=accept chain=IN-IPv4-65009 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=discard chain=IN-IPv4-65009
/routing filter add action=discard chain=OUT-IPv4-65009 prefix=10.9.0.0/22 prefix-
length=22-24
/routing filter add action=accept chain=OUT-IPv4-65009
/routing filter add action=accept chain=IN-IPv6-65009 prefix=2001:db9::/32 prefix-
length=32-48
/routing filter add action=accept chain=IN-IPv6-65009 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=IN-IPv6-65009
/routing filter add action=discard chain=OUT-IPv6-65009 prefix=2001:db9::/32 prefix-
length=32-48
/routing filter add action=accept chain=OUT-IPv6-65009
/routing filter add action=accept chain=IN-IPv4-65011 comment=Cliente
prefix=10.11.0.0/22 prefix-length=22-24
/routing filter add action=accept chain=IN-IPv4-65011 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=discard chain=IN-IPv4-65011
/routing filter add action=discard chain=OUT-IPv4-65011 prefix=10.11.0.0/22 prefix-
length=22-24
/routing filter add action=accept chain=OUT-IPv4-65011
/routing filter add action=accept chain=IN-IPv6-65011 prefix=2001:dbb::/32 prefix-
length=32-48
/routing filter add action=accept chain=IN-IPv6-65011 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=IN-IPv6-65011
/routing filter add action=discard chain=OUT-IPv6-65011 prefix=2001:dbb::/32 prefix-
length=32-48
/routing filter add action=accept chain=OUT-IPv6-65011
/system identity set name=Router-AS65010
/tool romon set enabled=yes
```

Apêndice 4

Configuração RouterOS do Router-AS65011:

```
/interface bridge add name=Loopback
/interface ethernet set [ find default-name=ether1 ] comment=Router-AS65010
/interface ethernet set [ find default-name=ether2 ] comment=Router-AS65008
/interface wireless security-profiles set [ find default=yes ] supplicant-
identity=MikroTik
/routing bgp instance set default as=65011 router-id=10.11.0.0
/ip address add address=10.11.0.0 comment=Loopback interface=Loopback network=10.11.0.0
/ip address add address=10.10.3.130/30 comment=Router-AS65010 interface=ether1
network=10.10.3.128
/ip address add address=10.11.3.1/30 comment=Router-AS65008 interface=ether2
network=10.11.3.0
/ip dhcp-client add disabled=no interface=ether1
```

```
/ipv6 address add address=2001:dbb:80d0::b1:0/127 advertise=no comment=AS65008
interface=ether2
/ipv6 address add address=2001:dba:80d0::b1:3/127 advertise=no comment=AS65010
interface=ether1
/ipv6 address add address=2001:dbb::/128 advertise=no comment=Loopback
interface=Loopback
/routing bgp network add network=10.11.0.0/22 synchronize=no
/routing bgp network add disabled=yes network=10.11.0.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.11.1.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.11.2.0/24 synchronize=no
/routing bgp network add disabled=yes network=10.11.3.0/24 synchronize=no
/routing bgp network add network=2001:dbb::/32 synchronize=no
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65008 name=AS65008 out-filter=OUT-
IPv4-65008 remote-address=10.11.3.2 remote-as=65008
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65008
name=AS65008 out-filter=OUT-IPv6-65008 remote-address=2001:dbb:80d0::b1:1 remote-
as=65008
/routing bgp peer add address-families=ipv6 hold-time=5s in-filter=IN-IPv6-65010
name=AS65010 out-filter=OUT-IPv6-65010 remote-address=2001:dba:80d0::b1:2 remote-
as=65010
/routing bgp peer add hold-time=5s in-filter=IN-IPv4-65010 name=AS65010 out-filter=OUT-
IPv4-65010 remote-address=10.10.3.129 remote-as=65010
/routing filter add action=accept chain=IN-IPv4-65008 comment=Cliente prefix=10.8.0.0/22
prefix-length=22-24
/routing filter add action=discard chain=IN-IPv4-65008
/routing filter add action=discard chain=OUT-IPv4-65008 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=accept chain=OUT-IPv4-65008
/routing filter add action=accept chain=IN-IPv6-65008 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=IN-IPv6-65008
/routing filter add action=discard chain=OUT-IPv6-65008 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=accept chain=OUT-IPv6-65008
/routing filter add action=discard chain=IN-IPv4-65010 comment=Operadora
prefix=10.11.0.0/22 prefix-length=22-24
/routing filter add action=accept chain=IN-IPv4-65010 prefix=0.0.0.0/0
/routing filter add action=accept chain=IN-IPv4-65010
/routing filter add action=accept chain=OUT-IPv4-65010 prefix=10.11.0.0/22 prefix-
length=22-24
/routing filter add action=accept chain=OUT-IPv4-65010 prefix=10.8.0.0/22 prefix-
length=22-24
/routing filter add action=discard chain=OUT-IPv4-65010
/routing filter add action=discard chain=IN-IPv6-65010 prefix=2001:dbb::/32 prefix-
length=32-48
/routing filter add action=accept chain=IN-IPv6-65010 prefix=::/0
/routing filter add action=accept chain=IN-IPv6-65010
/routing filter add action=accept chain=OUT-IPv6-65010 prefix=2001:dbb::/32 prefix-
length=32-48
/routing filter add action=accept chain=OUT-IPv6-65010 prefix=2001:db8::/32 prefix-
length=32-48
/routing filter add action=discard chain=OUT-IPv6-65010
/system identity set name=Router-AS65011
/tool romon set enabled=yes
```

Apêndice 5

Configuração RouterOS do Concentrador-Residencial:

```
/interface bridge add name=UltimaMilha
/interface ethernet set [ find default-name=ether1 ] comment=Router-AS65008
/interface ethernet set [ find default-name=ether2 ] comment=Router-Residencial
/interface wireless security-profiles set [ find default=yes ] supplicant-
identity=MikroTik
/ip pool add name=pool-pppoe-residencial ranges=100.64.0.0/22
/ipv6 pool add name=pool_WAN-Clientes-Residenciais prefix=2001:db8:80c0::/49 prefix-
length=64
/ipv6 pool add name=pool_LAN-Clientes-Residenciais prefix=2001:db8:8000::/41 prefix-
length=56
/ppp profile add dhcpv6-pd-pool=pool_LAN-Clientes-Residenciais dns-
server=8.8.8.8,1.1.1.1 local-address=100.127.255.255 name=profile-pppoe-residencial
```

```
remote-address=pool-pppoe-residencial remote-ipv6-prefix-pool=pool_WAN-Clientes-
Residenciais
/interface bridge port add bridge=UltimaMilha interface=ether2
/interface bridge port add bridge=UltimaMilha interface=ether3
/interface bridge port add bridge=UltimaMilha interface=ether4
/interface pppoe-server server add authentication=chap,mschap1,mschap2 default-
profile=profile-pppoe-residencial disabled=no interface=UltimaMilha one-session-per-
host=yes service-name=pppoe-server-residencial
/ip address add address=10.128.0.2/30 comment=Router-AS65008 interface=ether1
network=10.128.0.0
/ip dhcp-client add disabled=no interface=ether1
:global addNatRules do={
:global srcStart [:pick $NetworkIP 0 [:find $NetworkIP "/"]]
:global srcStart2 $srcStart
:global QtdRegras 0
:global QtdRegras2 0
:global portStop ($portStart + $portsPerAddr - 1)
  /ip firewall nat add chain=srcnat action=jump jump-target=$NewChain src-
address="$NetworkIP"
        :log info "O Network é $NetworkIP";
        :log info "Iniciando em $srcStart";
:put "Current IP: $srcStart\r\nTarget: $NetworkIP\r\n"
  :while ($srcStart in $NetworkIP) do={
        :log info "IP atual é $srcStart";
    /ip firewall nat add chain=$NewChain action=jump jump-target="$NewChain-
$($QtdRegras)" src-address="$srcStart-$($srcStart + ($IPsPerRule - 1 ))"
        :set QtdRegras ($QtdRegras + 1);
        :set srcStart ($srcStart + $IPsPerRule);
  }
        :log info "Qtd de Regras Jump criadas: $QtdRegras";
  :while ($srcStart2 in $NetworkIP) do={
        :for i from=1 to=$IPsPerRule do={
         /ip firewall nat add chain="$NewChain-$QtdRegras2" action=src-nat protocol=tcp
src-address=$srcStart2 to-address=$toPublicIP to-ports="$portStart-$portStop"
         /ip firewall nat add chain="$NewChain-$QtdRegras2" action=src-nat protocol=udp
src-address=$srcStart2 to-address=$toPublicIP to-ports="$portStart-$portStop"
        :set srcStart2 ($srcStart2 + 1);
        :set $portStart ($portStop + 1);
        :set $portStop ($portStart + $portsPerAddr - 1);
        :set i ($i + 1)
        }
        :set QtdRegras2 ($QtdRegras2 + 1);
  }
}
$addNatRules NewChain=cgnat NetworkIP=100.64.0.0/27 IPsPerRule=4 toPublicIP=10.8.1.0
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.32/27 IPsPerRule=4 toPublicIP=10.8.1.1
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.64/27 IPsPerRule=4 toPublicIP=10.8.1.2
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.96/27 IPsPerRule=4 toPublicIP=10.8.1.3
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.128/27 IPsPerRule=4 toPublicIP=10.8.1.4
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.160/27 IPsPerRule=4 toPublicIP=10.8.1.5
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.192/27 IPsPerRule=4 toPublicIP=10.8.1.6
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.0.224/27 IPsPerRule=4 toPublicIP=10.8.1.7
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.0/27 IPsPerRule=4 toPublicIP=10.8.1.8
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.32/27 IPsPerRule=4 toPublicIP=10.8.1.9
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.64/27 IPsPerRule=4 toPublicIP=10.8.1.10
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.96/27 IPsPerRule=4 toPublicIP=10.8.1.11
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.128/27 IPsPerRule=4 toPublicIP=10.8.1.12
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.160/27 IPsPerRule=4 toPublicIP=10.8.1.13
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.1.192/27 IPsPerRule=4 toPublicIP=10.8.1.14
portStart=1025 portsPerAddr=2000
```

```
$addNatRules NewChain=cgnat NetworkIP=100.64.1.224/27 IPsPerRule=4 toPublicIP=10.8.1.15
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.0/27 IPsPerRule=4 toPublicIP=10.8.1.16
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.32/27 IPsPerRule=4 toPublicIP=10.8.1.17
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.64/27 IPsPerRule=4 toPublicIP=10.8.1.18
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.96/27 IPsPerRule=4 toPublicIP=10.8.1.19
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.128/27 IPsPerRule=4 toPublicIP=10.8.1.20
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.160/27 IPsPerRule=4 toPublicIP=10.8.1.21
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.192/27 IPsPerRule=4 toPublicIP=10.8.1.22
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.2.224/27 IPsPerRule=4 toPublicIP=10.8.1.23
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.0/27 IPsPerRule=4 toPublicIP=10.8.1.24
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.32/27 IPsPerRule=4 toPublicIP=10.8.1.25
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.64/27 IPsPerRule=4 toPublicIP=10.8.1.26
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.96/27 IPsPerRule=4 toPublicIP=10.8.1.27
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.128/27 IPsPerRule=4 toPublicIP=10.8.1.28
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.160/27 IPsPerRule=4 toPublicIP=10.8.1.29
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.192/27 IPsPerRule=4 toPublicIP=10.8.1.30
portStart=1025 portsPerAddr=2000
$addNatRules NewChain=cgnat NetworkIP=100.64.3.224/27 IPsPerRule=4 toPublicIP=10.8.1.31
portStart=1025 portsPerAddr=2000
/ip firewall nat add chain=srcnat src-address=100.64.0.0/27 protocol=icmp action=src-nat
to-addresses=10.8.1.0 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.32/27 protocol=icmp action=src-
nat to-addresses=10.8.1.1 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.64/27 protocol=icmp action=src-
nat to-addresses=10.8.1.2 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.96/27 protocol=icmp action=src-
nat to-addresses=10.8.1.3 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.128/27 protocol=icmp action=src-
nat to-addresses=10.8.1.4 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.160/27 protocol=icmp action=src-
nat to-addresses=10.8.1.5 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.192/27 protocol=icmp action=src-
nat to-addresses=10.8.1.6 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.0.224/27 protocol=icmp action=src-
nat to-addresses=10.8.1.7 comment=ICMP-CGNAT-BLOCO-A
/ip firewall nat add chain=srcnat src-address=100.64.1.0/27 protocol=icmp action=src-nat
to-addresses=10.8.1.8 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.32/27 protocol=icmp action=src-
nat to-addresses=10.8.1.9 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.64/27 protocol=icmp action=src-
nat to-addresses=10.8.1.10 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.96/27 protocol=icmp action=src-
nat to-addresses=10.8.1.11 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.128/27 protocol=icmp action=src-
nat to-addresses=10.8.1.12 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.160/27 protocol=icmp action=src-
nat to-addresses=10.8.1.13 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.192/27 protocol=icmp action=src-
nat to-addresses=10.8.1.14 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.1.224/27 protocol=icmp action=src-
nat to-addresses=10.8.1.15 comment=ICMP-CGNAT-BLOCO-B
/ip firewall nat add chain=srcnat src-address=100.64.2.0/27 protocol=icmp action=src-nat
to-addresses=10.8.1.16 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.2.32/27 protocol=icmp action=src-
nat to-addresses=10.8.1.17 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.2.64/27 protocol=icmp action=src-
nat to-addresses=10.8.1.18 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.2.96/27 protocol=icmp action=src-
nat to-addresses=10.8.1.19 comment=ICMP-CGNAT-BLOCO-C
```

```
/ip firewall nat add chain=srcnat src-address=100.64.2.128/27 protocol=icmp action=src-
nat to-addresses=10.8.1.20 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.2.160/27 protocol=icmp action=src-
nat to-addresses=10.8.1.21 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.2.192/27 protocol=icmp action=src-
nat to-addresses=10.8.1.22 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.2.224/27 protocol=icmp action=src-
nat to-addresses=10.8.1.23 comment=ICMP-CGNAT-BLOCO-C
/ip firewall nat add chain=srcnat src-address=100.64.3.0/27 protocol=icmp action=src-nat
to-addresses=10.8.1.24 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.32/27 protocol=icmp action=src-
nat to-addresses=10.8.1.25 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.64/27 protocol=icmp action=src-
nat to-addresses=10.8.1.26 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.96/27 protocol=icmp action=src-
nat to-addresses=10.8.1.27 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.128/27 protocol=icmp action=src-
nat to-addresses=10.8.1.28 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.160/27 protocol=icmp action=src-
nat to-addresses=10.8.1.29 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.192/27 protocol=icmp action=src-
nat to-addresses=10.8.1.30 comment=ICMP-CGNAT-BLOCO-D
/ip firewall nat add chain=srcnat src-address=100.64.3.224/27 protocol=icmp action=src-
nat to-addresses=10.8.1.31 comment=ICMP-CGNAT-BLOCO-D
/ip route add comment=RotaDefault distance=1 gateway=10.128.0.1
/ipv6 address add address=fc00:2001:db8::2/126 advertise=no comment=Router-AS65008
interface=ether1
/ipv6 route add comment=RotaDefault-IPv6 distance=1 gateway=fc00:2001:db8::1
/ppp secret add name=residencial1 password=residencial1 profile=profile-pppoe-
residencial service=pppoe
/ppp secret add name=residencial2 password=residencial2 profile=profile-pppoe-
residencial service=pppoe
/system identity set name=Concentrador-Residencial
/tool romon set enabled=yes
```

Apêndice 6

Configuração RouterOS do Concentrador-Corporativo:

```
/interface bridge add name=UltimaMilha
/interface ethernet set [ find default-name=ether1 ] comment=Router-AS65008
/interface ethernet set [ find default-name=ether2 ] comment=Router-Corporativo
/interface wireless security-profiles set [ find default=yes ] supplicant-
identity=MikroTik
/ipv6 dhcp-server add address-pool=pool_LAN-Clientes-Corporativos interface=UltimaMilha
name=serverDHCPv6-Corporativo
/ipv6 pool add name=pool_LAN-Clientes-Corporativos prefix=2001:db8:8080::/42 prefix-
length=56
/ipv6 pool add name=pool_WAN-Clientes-Corporativos prefix=2001:db8:80c8::/50 prefix-
length=64
/routing ospf instance set [ find default=yes ] redistribute-connected=as-type-1
redistribute-static=as-type-1 router-id=100.128.0.130
/interface bridge port add bridge=UltimaMilha interface=ether2
/interface bridge port add bridge=UltimaMilha interface=ether3
/interface bridge port add bridge=UltimaMilha interface=ether4
/ip address add address=10.128.0.130/30 comment=Router-AS65008 interface=ether1
network=10.128.0.128
/ip address add address=100.0.0.1/30 comment=Router-Corporativo interface=ether2
network=100.0.0.0
/ip dhcp-client add disabled=no interface=ether1
/ip firewall nat add action=src-nat chain=srcnat comment="src nat - Router-Corporativo"
src-address=100.0.0.2 to-addresses=10.8.2.0
/ip firewall nat add action=dst-nat chain=dstnat comment="dst nat - Router-Corporativo"
dst-address=10.8.2.0 to-addresses=100.0.0.2
/ip route add comment="ROTA - Router-Corporativo" distance=1 dst-address=10.8.2.0/32
gateway=100.0.0.2
/ipv6 address add address=fc00:2001:db8::6/126 advertise=no comment=Router-AS65008
interface=ether1
/ipv6 address add address=::5242:4eff:fe00:9b01 advertise=no eui-64=yes from-
pool=pool_WAN-Clientes-Corporativos interface=UltimaMilha
/ipv6 route add distance=1 gateway=fc00:2001:db8::5
/routing filter add action=discard chain=ospf-in prefix=!0.0.0.0/0
```

```
/routing filter add action=accept chain=ospf-out prefix=10.8.0.0/22 prefix-length=22-32
/routing filter add action=accept chain=ospf-out prefix=100.0.0.0/10 prefix-length=10-30
/routing filter add action=discard chain=ospf-out
/routing ospf network add area=backbone network=10.128.0.128/30
/system identity set name=Concentrador-Corporativo
/tool romon set enabled=yes
```

Apêndice 7

Prefixos IPv4 e IPv6 e número de ASN utilizados no cenário:

Roteador	Número de ASN	Prefixo IPv4	Prefixo IPv6
Router-AS65008	65008	10.8.0.0/22	2001:db8::/32
Router-AS65009	65009	10.9.0.0/22	2001:db9::/32
Router-AS65010	65010	10.10.0.0/22	2001:dba::/32
Router-AS65011	65011	10.11.0.0/22	2001:dbb::/32

Apêndice 8

Divisão em sub-redes IPv4 do prefixo 10.8.0.0/22 do Router-AS65008:

Rede	Sub-rede	Finalidade
10.8.0.0/24		Infraestrutura, Serviços e CDNs
	10.8.0.0	Endereço de Loopback IPv4 do Router-AS65008
10.8.1.0/24		Atendimento de clientes residenciais
	10.8.1.0/27	CGNAT configurado no Concentrador-Residencial
10.8.2.0/24		Atendimento de clientes corporativos
	10.8.2.0/32	Delegado ao Router-Corporativo
10.8.3.0/24		Sessões eBGP e conectividades diversas na borda

Apêndice 9

Divisão em sub-redes dos prefixos privados IPv4:

Rede	Sub-rede	Finalidade
10.128.0.0/24		Rede para comunicação ponto a ponto interna do ISP
	10.128.0.0/30	Comunicação Router-AS65008 – Concentrador-Residencial
	10.128.0.128/30	Comunicação Router-AS65008 – Concentrador-Corporativo
100.0.0.0/10		Atendimento de clientes corporativos
	100.0.0.0/30	Atendimento ao Router-Corporativo
100.64.0.0/10		Atendimento de clientes residenciais
	100.64.0.0/22	CGNAT configurado no Concentrador-Residencial
	100.127.255.255/32	Gateway PPPoE Server do Concentrador-Residencial
172.16.0.0/12		Rede LAN corporativa
192.168.0.0/16		Rede LAN residencial