Universidade Tecnológica Federal do Paraná

Departamento Acadêmico de Informática

Curso de Bacharelado em Sistemas de Informação

Eduardo Follador

Análise e Implementação do protocolo IPV6 em infraestruturas de redes de computadores

Trabalho de Conclusão de Curso

CURITIBA
2015

Eduardo Follador

Análise e Implementação do protocolo IPV6 em infraestruturas de redes de computadores

Plano do Projeto da Disciplina de Trabalho de Conclusão do Curso de Bacharelado em Sistemas de Informação, apresentado à Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de bacharel em Sistemas de Informação.

Orientador: Fabiano Scriptore de Carvalho, MSc.

Curitiba
2015

RESUMO

O Protocolo de Internet versão 4 (IPV4) não é capaz de lidar com o massivo crescimento da necessidade de endereços IP ao redor do mundo, fazendo do IPV6 uma solução a ser utilizada. Apesar do benefício de poder se comunicar através de redes IPV6 com endereços IP reais, o processo de transição de IPV4 não é simples de ser executado, atrasando a adoção do IPV6. Para amenizar estes problemas, existem técnicas de transição como Pilha Dupla, Tunelamento, Tradução, entre outras, que permitem a utilização de IPV6 mesmo em um ambiente de redes onde haja predominância de IPV4. Após estruturar uma topologia de redes com equipamentos reais, algumas destas técnicas de transição foram colocadas em teste buscando avaliar o desempenho da rede com cada uma delas, através de comparações entre os valores de tempo de resposta do envio de um pacote através da rede. Após a execução e análise dos testes, foi constatado que a técnica de Pilha Dupla permite utilizar os recursos do protocolo IPV6 sem causar impacto na rede já existente, fazendo com que a dificuldade do processo de transição permaneça atrelada diretamente à complexidade da rede.

Palavras-chave: IPV6. IPV4. Redes de Computadores. Técnicas de Transição.

ABSTRACT

The Internet Protocol version 4 (IPV4) isn’t capable of dealing with the massive growth of the need of IP adresses around the world, making IPV6 a solution to be used. Besides the benefits of being able to communicate trought IPV6 networks using real IP adresses, the IPV4 transition process isn’t simple to be executed, delaying the adoption of IPV6. To ease these problems, there is several transition techniques such as Dual Stack, Tunneling, Translation, among others, that allow the use of IPV6 even on a network enviroment where IPV4 is the main protocol. After structuring a network topology with real equipments, some of these techniques were put to the test in order to evaluate the network performance using each one, thought comparissons between the delay of a packet being sent trought the network. After executing and analysing these tests results, it was found that the Dual Stack technique allows the use os IPV6 resources without impacting on the existing network, making the dificulty of the transition process to be linked directly to the network complexity.

Keywords: IPV6. IPV4. Computer Networks. Transition Techniques

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

CIDR: Classless Inter-domain Routing

DNS: Domain Name System

DSTM: Dual Stack Transition Mechanism

EIGRP: Extended IGRP

IETF: Internet Engineering Task Force

IGRP: Interior Gateway Routing Protocol

IPSec: IP Security Protocol

IPV4: Internet Protocol version 4

IPV6: Internet Protocol version 6

NAPT-PT: Network Address Port Translator - Protocol Translator

NAT: Network Address Translation

NAT-PT: Network Address Translation - Protocol Translation

NCP: Network Control Protocol

OSPF: Open Shortest Path First

QoS: Quality of Service

RIP: Routing Information Protocol

SIIT: Stateless IP/ICMP Translation

SIPP: Simple Internet Protocol Plus

TAAT: Teste de Atraso em Alto Tráfego

TAS: Teste de Atraso Simples

TCP: Transmission Control Protocol

TRT: Transport Relay Translation

TSP: Tunel Setup protocol

TUBA: TCP and UDP with Bigger Addresses

UDP: User Datagram Protocol

SUMÁRIO

1. INDRODUÇÃO

Ao longo dos anos, a Internet tem se tornado essencial na vida das pessoas. Com o surgimento do Protocolo de Internet versão 4 (IPV4), ou *Internet Protocol version 4* (DOMINGOS, 2015), a mais de 20 anos atrás, foi possível a interconexão de uma rede que se transformou em uma rede mundial, fazendo com que cada vez mais pessoas tivessem acesso à Internet (SMETANA, 2015). A Figura 1 representa o crescimento da Internet de 2000 a 2010 nas diversas regiões do mundo.

Regiões	*População (em 2010)*	*Usuários de Internet (em 2000)*	*Usuários de Internet (atualmente)*	*% por Região*	*Crescimento 2000-2010*
África	1.013.779.050	4.514.400	110.931.700	10,9 %	2.357,3 %
Ásia	3.834.792.852	114.304.000	825.094.396	21,5 %	621,8 %
Europa	813.319.511	105.096.093	475.069.448	58,4 %	352,0 %
Oriente Médio	212.336.924	3.284.800	63.240.946	29,8 %	1.825,3 %
América Norte	344.124.450	108.096.800	266.224.500	77,4 %	146,3 %
America Latina /Caribe	592.556.972	18.068.919	204.689.836	34,5 %	1.032,8 %
Oceania	34.700.201	7.620.480	21.263.990	61,3 %	179,0 %
TOTAL	**6.845.609.960**	**360.985.492**	**1.966.514.816**	**28,7 %**	**444,8 %**

Tabela 1: *Crescimento da internet em cada região do Mundo*
Fonte*: Adaptado de (MEDEIROS, SILVA, 2010)*

Apesar de seu grande sucesso, o IPV4 não foi capaz de suportar a tão exigente demanda de endereços IP e apesar de diversas técnicas para suprimir este problema, como o NAT (*Network Address Translation*), sua sucessão se tornou inevitável. Para tal finalidade, foi apresentado no IETF (*Internet EngineerTask Force*) o Protocolo de Internet versão 6 (IPV6), ou *Internet Protocol version 6* (DOMINGOS, 2015), que utiliza um endereço de 128 bits (HIROMI, YOSHIFUJI, 2005).

Apesar das inúmeras vantagens que o IPV6 aparentemente traz, em relação ao IPV4, sua implantação ainda é algo que causa bastante receio devido aos diversos problemas do processo de transição de um protocolo para outro (HIROMI, YOSHIFUJI, 2005). Em decorrência disso, o IPV6 está sendo

implantado gradualmente no lugar do IPV4, exigindo que, em muitas das vezes, ambos protocolos funcionem concorrentemente.

Neste trabalho são estudadas algumas destas técnicas para verificar como funciona a transição da infraestrutura IPV4 para uma em IPV6 e por fim, implantar uma topologia de redes IPV6 utilizando equipamentos reais no laboratório de redes da UTFPR.

1.1. Justificativa

Devido ao fato do IPV4 não ser suficiente para lidar com a proporção que a Internet está tomando, faz-se necessário buscar meios para realizar a transição de IPV4 para IPV6 nas redes ao redor do mundo. Porém, durante o processo de transição de uma estrutura de rede em IPV4 para uma que trabalhe com o protocolo IPV6, podem ser encontrados problemas que atrasem a execução deste processo.

Testes podem ser realizados com diferentes técnicas de transição de forma a identificar características importantes da topologia como compatibilidade de tecnologias, escalabilidade, segurança, configuração e administração de rede, suporte a QoS (*Quality of Service)*, mobilidade, políticas de roteamento e transição (IPV6.BR, 2015). Estas informações auxiliam na identificação da melhor técnica de transição a ser utilizada no ambiente analisado. Em vista disso, este trabalho se propõe a estudar técnicas de transição e testá-las em um laboratório de redes, de forma a identificar quais apresentam os melhores resultados em uma mesma topologia simples.

1.2. Objetivos

Toda pesquisa que procure apresentar um bom nível de credibilidade apresenta os objetivos que impulsionaram sua execução. Os objetivos desta pesquisa estão indicados a seguir.

1.2.1. Objetivo Geral

Estudar o funcionamento do protocolo IPV6 e avaliar técnicas de transição de uma arquitetura IPV4 para IPV6, realizando testes de implementação em um ambiente real utilizando equipamentos que se comuniquem adequadamente com o novo protocolo.

1.2.2. Objetivos Específicos

- Estudar os protocolos de rede IPV4 e IPV6, analisando suas características e diferenças;
- Estudar as técnicas de transição entre os protocolos IPV4 e IPV6;
- Implementar cenários reais de topologias de redes utilizando os protocolos IPV4 e IPV6;
- Implementar cenários reais de topologias de redes que utilizam as técnicas de transição entre os protocolos estudados;
- Realizar testes com as técnicas implantadas.

1.3. Estrutura/Organização

Este trabalho está organizado da seguinte forma. No capítulo 1 é apresentado o projeto, juntamente com sua justificativa e seus objetivos.

No capítulo 2, é realizado um levantamento conceitual da tecnologia a ser utilizada buscando contextualizar historicamente a evolução de algumas tecnologias de rede de computadores, bem como seu estado atual.

No capítulo 3 é apresentado o desenvolvimento do projeto, bem como seus resultados e considerações após a execução dos testes propostos.

Por fim, no capítulo 4 é apresentado o ponto de vista a respeito deste trabalho, levantando tópicos que obtiveram destaque durante o desenvolvimento da pesquisa do tema.

2. LEVANTAMENTO BIBLIOGRÁFICO E ESTADO DA ARTE

Para descrever os conceitos, técnicas e diferenças que serão abordadas e estudadas no decorrer deste trabalho, foi realizada uma revisão de literatura relacionada à área de Redes de Computadores, mais precisamente aos protocolos de comunicação, no intuito de adquirir a fundamentação necessária no contexto histórico dos protocolos de comunicação, técnicas de implementação e transição existentes, bem como seus resultados após testes em um laboratório de redes.

2.1. Redes de Computadores

A expressão "Rede de Computadores" é muito abrangente, porém segundo Tanenbaum (TANENBAUM, 2003), ela pode ser caracterizada como um conjunto de computadores autônomos interconectados por uma única tecnologia, ou seja, máquinas capazes de trocar informações entre si.

Um modelo bastante difundido para ilustrar a estrutura da Rede de Computadores é o Modelo de Referência OSI (*Open System Interconnection*), baseado em uma proposta desenvolvida pela ISO (*Internation Standard Organization*) como tentativa inicial de buscar a padronização internacional dos protocolos em camadas.

Cada uma das sete camadas do modelo OSI possui funções bem definidas e foram criadas devido a necessidade de um outro grau de abstração para categorizar a rede. Suas camadas são: Física, Enlace de Dados, Rede, Transporte, Sessão, Apresentação e Aplicação.

A camada Física é responsável por garantir que os bits sejam entregues aos seus destinos, dentro do canal de comunicação. A camada de Enlace de Dados fragmenta os dados de entrada em pequenos quadros que são enviados sequencialmente, buscando transformar uma linha bruta em uma linha livre de erros de transmissão. A camada de Rede busca controlar o roteamento dos pacotes de dados durante o processo de transmissão. A camada de Transporte cuida do processo de envio e recebimento de

pacotes oriundos de camadas superiores, preparando-os para serem enviados à camada de Rede. A camada de Enlace é responsável por coordenar o fluxo de dados entre os usuários da rede, com regras para sincronização e procedimentos a serem tomados em caso de falhas. A camada de Apresentação está relacionada à sintaxe e à semântica das informações transmitidas. Por último, a camada de Aplicação é responsável por prover serviços para algumas aplicações buscando isolar os processos de comunicação de rede que acontecem em todas as máquinas conectadas e que fazem requisições. (TANENBAUM, 2003)

***Figura 1**: Modelo OSI*
***Fonte**: (DLTEC do Brasil)*

2.2. Protocolos de Rede

Em 1966, foi criado um projeto para interligação de computadores em centros militares de Pesquisa, o ARPANET, que tinha por principal objetivo, manter uma conexão estável entre as estações, mesmo após a queda de uma delas.

De início, o ARPANET trabalhava com diversos protocolos diferentes, como o NCP (*Network Control Protocol*), porém quando a rede aumentou, todas as máquinas passaram a utilizar o protocolo TCP/IP. A partir deste

ponto deu-se início ao enorme crescimento da Internet culminando algum tempo depois na elaboração do protocolo IPV4 (IPV6.BR, 2015).

2.2.1. IPV4

O IPV4 (DOMINGOS, 2015), é um protocolo que permite que dispositivos que tenham suporte a este protocolo se conectem à Internet. Quando um dispositivo se conecta à rede, ele recebe um endereço IP único, como 121.123.125.127 por exemplo, e utiliza-o para se comunicar por meio da rede.

O IPV4 reserva 32 bits para endereçamento, possibilitando gerar mais de 4 bilhões de endereços diferentes. No começo era classificado em classes: A, B e C, onde a classe A era destinada a atender os endereços na faixa de 7 bits de rede (128 redes, 16.77.216 hosts), a classe B destinada aos endereços na faixa de 14 bits (16.384 redes, 66536 hosts) e da classe C aos endereços na faixa de 21 bits (2.097.152 redes, 256 hosts) (IPV6.BR, 2015).

Embora esta divisão tivesse o propósito de distribuir de forma mais organizada as faixas de endereços, a classe A atendia a uma faixa muito pequena de endereços de redes, porém ocupava metade de todos os endereços disponíveis. Além disso, grandes massas de endereços eram disponibilizadas para grandes empresas, que dificilmente utilizariam todos estes recursos, sendo esse um dos problemas que levou à escassez de endereços IPV4. Esta classificação não é mais utilizada nos dias de hoje.

Diante deste cenário preocupante, em meados de 1991 a IETF começou a pesquisar formas de solucionar este problema, criando o CIDR (*Classless Inter-domain Routing*), o NAT, entre outros (IPV6.BR, 2015).

2.2.2. IPV6

O IPV6 (DOMINGOS, 2015) foi efetivamente publicado como a composição de outras tentativas de protocolos, como o SIPP (*Simple Internet Protocol Plus*) e o TUBA (*TCP and UDP with Bigger Addresses*). O SIPP**,** uma evolução do IPV4, era focado em aumentar o espaço de endereçamento e já apresentava cabeçalhos de extensão e um campo "*flow"* para identificar o tipo de fluxo de cada pacote. O TUBA, também uma evolução do IPV4, é focado em aumentar a capacidade de endereçamento, porém voltado à transição de longo prazo baseada na atualização dos host e servidores DNS (*Domain Name System)* (IPV6.BR, 2015).

2.2.2.1. Melhorias

Dentre os diversos recursos e melhorias do IPV6 em relação ao IPV4, destacam-se:

- **Maior capacidade de armazenamento:** o IPV6 possui várias diferenças de especificações de armazenamento em relação ao IPV4. Entre elas se destaca o aumento de 32 para 128 bits no espaço de endereçamento possibilitando um aumento considerável na quantidade de endereços que podem ser distribuídos de pouco mais de 4 bilhões (IPV4) para um número inexprimível de 2^{128}. (MEDEIROS, SILVA, 2010)

- **Simplificação do cabeçalho:** o IPV6 traz um formato de cabeçalho mais visual e de mais fácil entendimento. Dentre as várias modificações de exclusão e reformulação de campos, as mudanças de maior destaque foram a alocação de um tamanho fixo para todos os cabeçalhos, ou seja, o cabeçalho tem o tamanho fixo de 40 bytes, diferentemente do cabeçalho IPV4 que possui tamanho variável, e também a remoção do *checksum*, validador que protege os pacotes de dados contra dados corrompidos, já que o IPV6 considera confiáveis as

camadas inferiores (MEDEIROS, SILVA, 2010) (MESONPI, 2015).

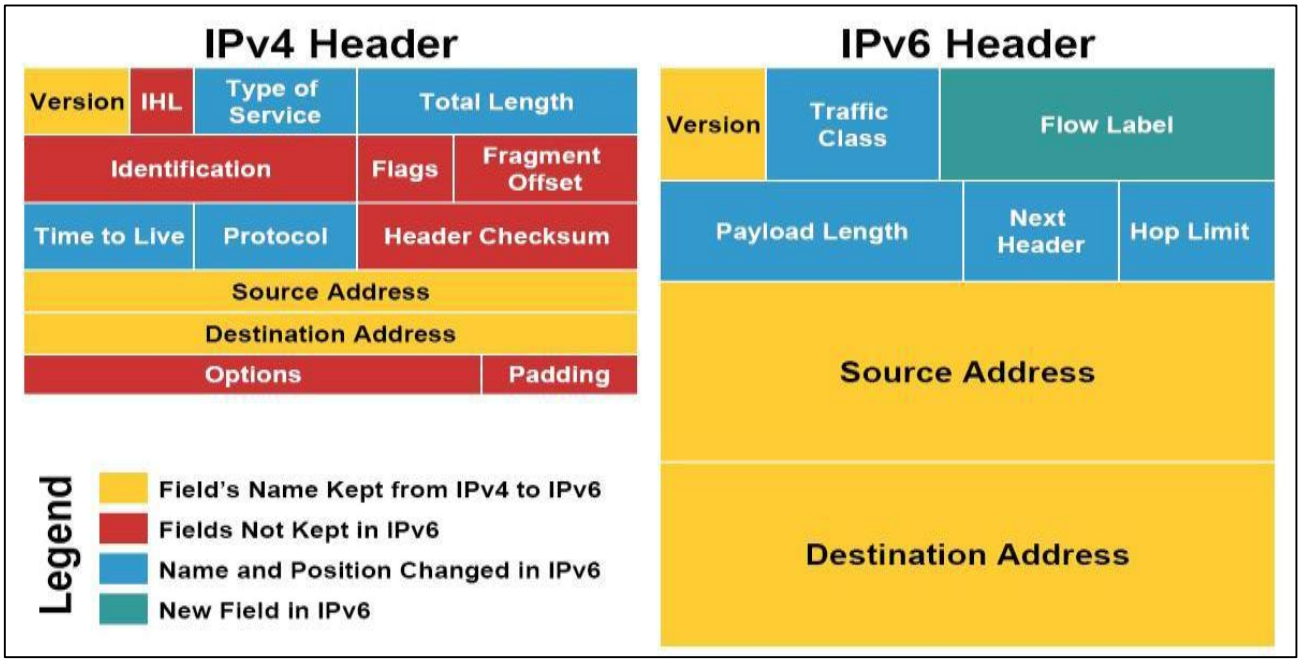


***Figura 2**: Modelo dos Cabeçalhos IPV4 e IPV6*
***Fonte**: Adaptado de (MEDEIROS, SILVA, 2010)*

- **Suporte a cabeçalhos de extensão:** o diferencial aqui é que o IPV6 consegue separar os campos básicos dos customizáveis, possibilitando um melhor gerenciamento de seu tamanho como um todo. Diferente dos cabeçalhos base, os de extensão não possuem tamanho fixo e podem variar de acordo com o tipo de cabeçalho. Para isso, os cabeçalhos de extensão possuem campos específicos como o EXTENSION HEADER LENGHT que indica seu tamanho (MEDEIROS, SILVA, 2010) (MESONPI, 2015).

- **Suporte à autenticação e privacidade:** foram especificados cabeçalhos de extensão capazes de fornecer mecanismos de autenticação e garantir a integridade e a confidencialidade dos

dados transmitidos. (MEDEIROS, SILVA, 2010) (MESONPI, 2015)

2.2.2.2. Roteamento

Roteamento é o processo de encaminhar os pacotes entre os segmentos de rede. Nas redes IPV6, cada roteador IPV6 fornece os recursos necessários para transmitir os pacotes pela rede.

O roteamento é a principal função do IPV6, pois com ele os pacotes são trocados entre cada roteador usando IPV6 na camada de Internet. Cada roteador mantém uma tabela de roteamento própria, ou seja, um mapa de caminhos para onde é possível enviar um pacote, e quando há necessidade de realizar um envio, esta tabela é utilizada para definir para onde este pacote deve ser enviado. (TECHNET, 2015)

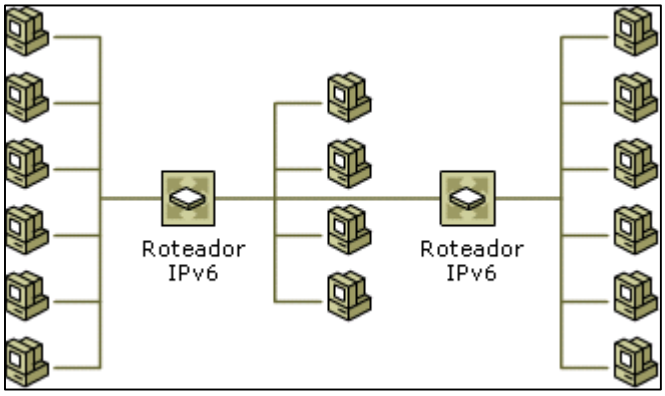


Figura 3: *Representação do Roteamento IPV6*
Fonte*: Adaptado de (TECHNET, 2015)*

Antes de enviar um pacote IPV6, o computador insere seu endereço IPV6 como origem e o endereço do destinatário como destino no cabeçalho IPV6 do pacote. Feito isso, o endereço de destino é comparado com a tabela de roteamento IPV6 mantida localmente e então é enviado o pacote para o segmento de rede encontrado na tabela. O pacote pode ter três destinos: pode ser enviado para uma camada acima da camada IPV6 no roteador, encaminhado para uma das redes contidas

na tabela de roteamento, ou simplesmente ser descartado caso não encontre nenhum destino cabível.

O IPV6 segue alguns critérios para a seleção da rota correta do pacote. Primeiramente, uma rota que corresponda ao endereço de destino do pacote (prefixo de 128 bits). Em seguida, uma rota cujo endereço de destino possua o maior prefixo. E por último, a rota padrão. Caso uma rota correspondente não seja encontrada, o destino será considerado como destino sem conexão (TECHNET, 2015).

2.2.2.3. Segurança

Um dos fatores mais importantes em segurança no IPV6 é o IPSec (*IP Security Protocol*). O termo IPSec se refere a um conjunto de protocolos do IETF que fornecem criptografia da camada de redes e autenticação para redes baseadas em IP (RADWAN, 2005). A principal função do IPSec é estabelecer redes virtuais privadas que estabeleçam a conexão entre usuários através da rede pública. Diferentemente do IPV4, o IPV6 não precisa utilizar NAT para privatizar a conexão devido ao alto número de endereços que possui.

A utilização do IPSec, diferentemente do IPV4, é mandatória no IPV6 devido à segurança que ele traz a conexões ponto a ponto e aos diversos tipos de ataques de rede que o IPV6 pode sofrer (RADWAN, 2005). Entre estes tipos de ataque destacam-se:

- ***The sniffing attacks:*** bastante comum tanto no IPV4 quanto no IPV6. Consiste em capturar dados que estejam trafegando na rede. Busca dados não criptografados que sejam de fácil identificação. (DURDAGI, BULDU, 2010)

- ***Application layer attacks:*** utiliza vírus e *worms* para comprometer as aplicações dos computadores e servidores. É o tipo mais comum de ataque devido ao fato de ele atuar na camada de aplicação, e não na camada de rede onde os

protocolos IPV4 e IPV6 atuam. Em decorrência disso, ambos os protocolos não são capazes de conter este tipo de ataque. (DURDAGI, BULDU, 2010)

- ***Flooding attacks:*** um dos ataques mais comuns no IPV4, consiste em inundar o roteador ou servidor com grandes quantidades de tráfego de dados, impossibilitando-o de realizar qualquer tipo de processamento. (DURDAGI, BULDU, 2010)

2.3. Métodos e técnicas de transição

Diversas técnicas de transição foram definidas para auxiliar no processo de implantação do protocolo IPV6 em redes de computadores. Segue uma breve descrição de algumas delas.

2.3.1. Pilha Dupla

Cada ponto da rede mantém um endereço IPV4 e IPV6 ao mesmo tempo, possibilitando a comunicação tanto em uma rede IPV4 quanto em uma IPV6. (ALJA'AFREH, MELLOR, et.al, 2009)

2.3.1.1. Pilha Dupla por IP

Nodos com *Dual IP Stack,* são nodos que mantém referências IPV4 e IPV6 ao mesmo tempo. Dessa forma, pode ser realizada tanto comunicação com nodos IPV6 quanto com nodos IPV4, bastando apenas fazer a transcrição para IPV4. Estes nodos são conhecidos como endereços IPV6 compatíveis com IPV4 e, com uma abordagem como

essa, é possível converter qualquer endereço IPV4 em IPV6, e vice-versa (NGNET.IT, 2015).

O problema desta técnica é que ela não elimina o problema inicial de realizar a transição de IPV4 para IPV6, que é a eliminação da necessidade de endereços IPV4, pois para que a transformação aconteça, os nodos também precisam armazenar um endereço IPV4.

2.3.1.2. Pilha Dupla em nível de Aplicação (*Dual Stack ALG*)

Esta técnica, assim como o NAT-PT (*Network Address Translation - Protocol Translation*) e o NAPT-PT (*Network Address Port Translator - Protocol Translator*), visam suprimir as deficiências da Pilha Dupla por IP e normalmente é utilizado em redes que já possuem IPV6 implantado, porém ainda necessitam se comunicar externamente através de IPV4. (NGNET.IT, 2015)

2.3.2. Tunelamento

O termo Tunelamento é utilizado para definir o processo de encapsulamento de um pacote IP dentro de outro com diferente estrutura, de forma a permitir a conexão entre redes configuradas com diferentes protocolos IP.

Alguns dos tipos de tunelamento existente são conhecidos como 6in4 e 4to6. No 6in4, um pacote IPV6 é encapsulado em um pacote IPV4 e enviado em um segmento de rede IPV4. Ao final do processo, o pacote é transformado ao seu estado original para então ser consumido pelo ponto de rede, sendo o oposto no 4to6. (ALJA'AFREH, MELLOR, et.al, 2009)

2.3.2.1. Teredo

Existem outras formas de se utilizar o 6in4. O Teredo, por exemplo, é um serviço de rede que utiliza o 6in4 em seu processo para permitir que até mesmo servidores mascarados por uma tabela NAT IPV4, obtenham conexões IPV6 através de envio de pacotes numa rede IPV4, sem possuir uma conexão IPV6 nativa (HUANG, 2005).

Um fator importante a se considerar no Teredo, é de que ele aumenta a possibilidade de ataques e invasões externas por permitir que quaisquer redes IPV6 roteáveis se conectem com redes protegidas pelo NAT, não se importando com a procedência dessa conexão, o que acaba por desconsiderar a função do NAT e expor a rede externamente (HOAGLAND, 2007).

Apesar de cumprir o objetivo pelo qual foi criado, o Teredo é uma medida provisória visto que, à longo prazo, todos os servidores deverão possuir uma conexão IPV6 nativa.

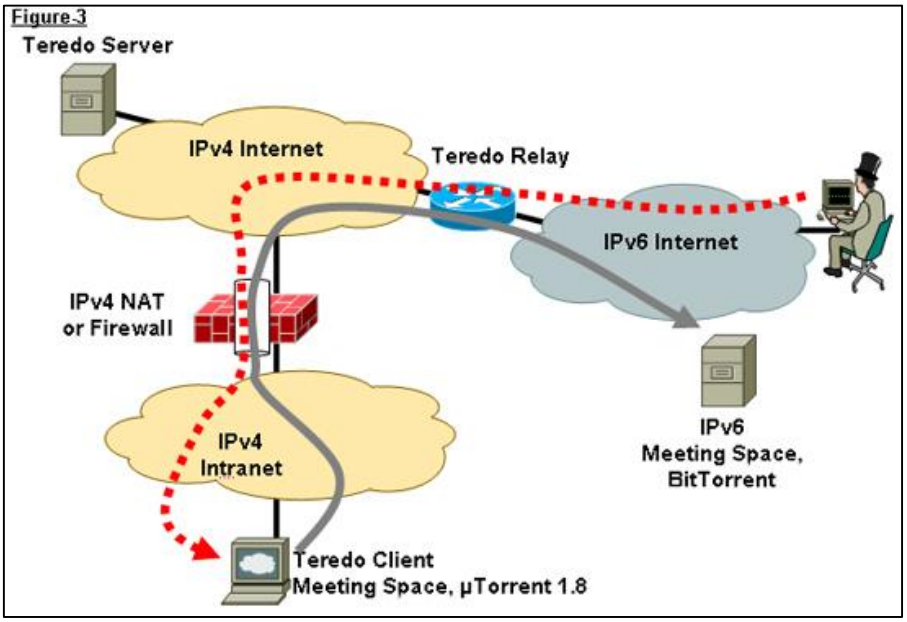


Figura 4: *Utilização de Teredo para obtenção de conexão IPV6*
Fonte: *http://www.snipview.com/q/IP_address*

2.3.2.2. Tunel-Broker

Semelhante ao Teredo, o Tunel-Broker também utiliza o 6in4 para seu funcionamento. A grande diferença entre eles é que o Tunel-Broker é em relação a segurança, visto que no Tunnel-Broker, o servidor ao qual são feitas as requisições é um servidor dedicado e credenciado, que analisa todas as requisições e libera os endereços IPV6 para que os usuários finais façam uso e conectem-se com redes IPV6 (IETF, 2015).

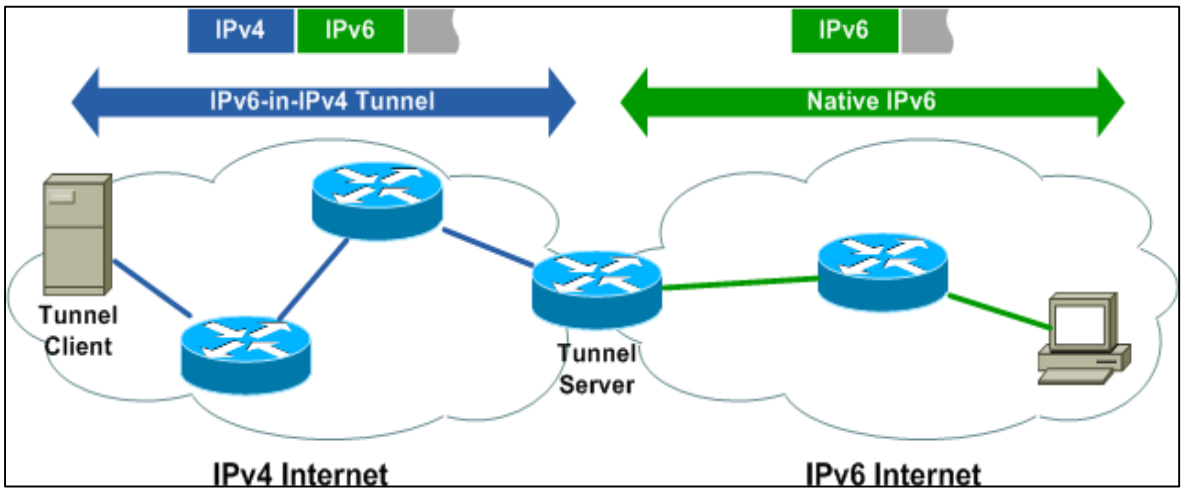


Figura 5: *Topologia de Tunelamento*
Fonte: *http://packetlife.net/blog/2008/dec/17/creating-IPV6-tunnel-packetlifenet/*

2.3.3. Tradução

É necessário um equipamento de tradução que atue entre dois endereços IP de redes diferentes, permitindo que um servidor IPV6 se comunique diretamente com um servidor IPV4 e vice-versa, ou seja, um protocolo é convertido para o outro. (ALJA'AFREH, MELLOR, et.al, 2009)

2.4. Protocolos de Roteamento

Os protocolos de rede são utilizados para a construção de tabelas de roteamento em redes comutadas por pacotes. São algoritmos estabelecidos com o intuito de reconhecer e mapear a topologia de rede. Estes protocolos armazenam as informações da rede através de tabelas de roteamento, que podem ser preenchidas manual ou dinamicamente. O processo de atualização e manutenção destas tabelas variam de acordo com o método de roteamento escolhido. (BIRKNER, 2008) (IMASTERS, 2015)

Uma forma de utilizar este recurso de roteamento, é inserindo manualmente os destinos para o qual um dado pacote deve ser enviado, dependendo de seu endereço de origem. O problema deste tipo de abordagem é que caso um enlace de rede se perca, ou seja desativado, o pacote que utilizaria este enlace nunca será enviado, mesmo que haja outros meios para se chegar ao destino final. (BIRKNER, 2008) (IMASTERS, 2015)

Para solucionar este problema existem os protocolos de roteamento dinâmicos, que buscam atualizar sua tabela de roteamento automaticamente dadas certas circunstâncias. Entre eles destacam-se o RIP, EIGRP e o OSPF, sendo que todos eles utilizam métricas (tipo de valor considerado para seleção do melhor destino) e processo de convergência (tempo que se passa entre o processo de atualização de rotas) tanto para IPV4 quanto para IPV6, o que muda é a forma de configuração. (BIRKNER, 2008) (IMASTERS, 2015)

2.4.1. RIP

O RIP (*Routing Information Protocol*), desenvolvido por volta dos anos 80, é atualmente um dos protocolos de roteamento mais utilizados ao redor do mundo, pois além do fato do protocol ser suportado pela maioria dos fabricantes de equipamentos de rede, ele também apresenta um processo de configuração muito mais fácil em comparação com os demais protocolos, seja IPV4 ou IPV6. (IMASTERS, 2015)

O RIP identifica qual o melhor enlace de rede a ser escolhido para mapear sua tabela de roteamento baseado na métrica de saltos (*hops*), sendo estes o número de enlaces necessários a serem percorridos para chegar ao destino.

Utilizado mais comumente em pequenas redes de computadores, o RIP possui algumas limitações que impedem que sua utilização seja viável em redes de grande escala. Um destes problemas é o fato do protocolo possuir uma limitação para o número de saltos analisados na hora de definir qual o melhor enlace de rede para se chegar a um dado ponto da rede, considerando infinito, ou seja, o pior caso possível, todo caminho que superar o valor de 15 saltos para chegar ao destino. Outro problema deste protocolo é o fato de que ele envia atualizações periodicamente, por meio de *broadcasts* através da rede para poder mapear novamente sua tabela de roteamento, o que acaba consumindo largura de banda da rede. (BIRKNER, 2008) (IMASTERS, 2015)

2.4.2. OSPF

Criado pelo IETF para suprir as carências de escalabilidade limitada, convergência lenta e suscetibilidade de loops de roteamento do RIP, o OSPF (Open Shortest Path First) é um protocolo não proprietário de Estado de Enlace (*link-state*) que se baseia no algoritmo de Djikstra para construção de suas tabelas de roteamento. Em um protocolo de Estado de Enlace, cada roteador calcula sua própria tabela de roteamento baseado nos custos dos estados de enlace, para cada destino diferente presente na rede. (BIRKNER, 2008) (IMASTERS, 2015)

A métrica utilizada para selecionar o melhor enlace no OSPF é chamada de Custo, sendo este o valor acumulado de um roteador para a rede de destino. Quanto menor o custo, mais provável será o uso da interface para encaminhar o tráfego de dados. (BIRKNER, 2008) (IMASTERS, 2015)

Um fator bastante importante do OSPF é que ele é um protocolo em constante desenvolvimento, e a cada nova necessidade identificada para este protocolo, novas funcionalidade são desenvolvidas e implementadas, mantendo

sempre a compatibilidade com versões anteriores. (BIRKNER, 2008) (IMASTERS, 2015)

2.4.3. EIGRP

Diferentemente do OSPF, o EIGRP (Extended IGRP) é o protocolo proprietário da Cisco Systems para roteamento de tráfego de redes. Aprimoramento do IGRP (Interior Gateway Routing Protocol), o EIGRP combina os protocolos de roteamento baseados em distância com os de Enlace Estático. (BIRKNER, 2008) (IMASTERS, 2015)

Apesar de ser a extensão de seu predecessor, o EIGRP se diferencia bastante do IGRP, principalmente no que diz respeito à criação de interconexões de redes escaláveis, já que apresenta diversas características que favorecem este processo como uma maior facilidade de instalação, aceite de múltiplos protocolos, aceitando VDSL entre outros. (BIRKNER, 2008) (IMASTERS, 2015)

A convergência do EIGRP é rápida e tranquila, já que as informações de roteamento modificadas são transmitidas imediatamente para os nós afetados pela mudança. A métrica utilizada pelo EIGRP contém cinco componentes que podem influenciar no resultado, porém por padrão, são avaliados apenas os valores de *bandwidth* e de *delay* para selecionar o melhor caminho para transmitir os pacotes de dados. (BIRKNER, 2008) (IMASTERS, 2015)

A Tabela 2 representa um quadro comparativo entre os protocolos analisados.

Características	RIP	OSPF	EIGRP
Tipo	Vetor de Distância	Estado de Enlace	Vetor de Distância
Convergência	Lento	Rápido	Rápido
Métrica	Saltos	Custo	Bandswitch/Delay
Uso Proprietário	Não	Não	Sim

Tabela 2: *Comparativo Protocolos de Roteamento*
Fonte: *Autoria própria*

3. METODOLOGIA

O método a ser aplicado no desenvolvimento deste projeto consiste em três etapas, pesquisa e análise da tecnologia e estruturação do laboratório, definição e planejamento dos testes e preparação do trabalho escrito, e realização dos testes com apuração dos resultados e conclusões.

A primeira etapa consiste na pesquisa e análise da situação atual da tecnologia e também na estruturação e planejamento do laboratório de informática. Nesta etapa, foram verificadas as características do IPV6 de forma a compreender qual a melhor maneira de implanta-lo na rede, bem como as técnicas de transição existentes. Durante este processo, foi realizada a estruturação os equipamentos com capacidade de comunicação IPV6 no laboratório onde seriam realizados os testes de análise das técnicas.

A segunda etapa do projeto diz respeito à aplicação das técnicas de transição estudadas e realização dos testes para coleta de dados. Primeiramente, foram definidos quais cenários seriam aplicados na topologia, permitindo assim a realização dos testes.

Na terceira etapa foram aplicados os testes propostos na etapa anterior, possibilitando a análise de dados para a obtenção das conclusões. Para isso foram comparados os resultados e realizado um levantamento sobre os diferenciais entre os cenários simulados com técnicas de transição diferentes. A partir destes resultados foi possível obter dados concretos para avaliar e classificar a viabilidade de cada técnica aplicada.

4. DESENVOLVIMENTO

Com o fim de avaliar o desempenho de cada um dos protocolos em uma topologia de redes, foram realizados testes em diferentes cenários. Com isso, foi possível levantar dados comparativos para fundamentar a análise de cada situação. Os critérios de avaliação consistem em Teste de Atraso Simples (TAS) e Teste de Atraso em Alto Tráfego (TAAT).

Para realizar a avaliação de TAAT e testes de carga, foi utilizado um software para teste de largura de banda, o IPerf, em conjunto com o JPerf. O JPerf é uma aplicação na plataforma Java que estende o IPerf, seu antecessor, possibilitando a utilização de uma interface gráfica para monitoramento. Esta ferramenta gera tráfego em uma infraestrutura de redes e foi utilizada para simular os testes de carga. Para os testes com o JPerf, a aplicação foi instalada nas duas máquinas localizadas nas extremidades da topologia, utilizando a função Cliente em um ponto e Servidor no outro, permitindo assim o monitoramento do envio de mensagens ponto a ponto da topologia. O objetivo deste teste é buscar dados de cada técnica de transição em um ambiente mais próximo à realidade de tráfego que as redes ao redor do mundo precisam administrar.

4.1. Topologia

A topologia utilizada é composta de 4 roteadores Cisco 1841, 4 switches Cisco 2960. Foi utilizado um padrão para todos os testes, onde todos os roteadores e switches são do mesmo modelo e marca. A taxa de transmissão utilizada entre os enlaces seriais foi de 2 Mbps. A conexão dos roteadores foi implementada conforme ilustrado na Figura 6.

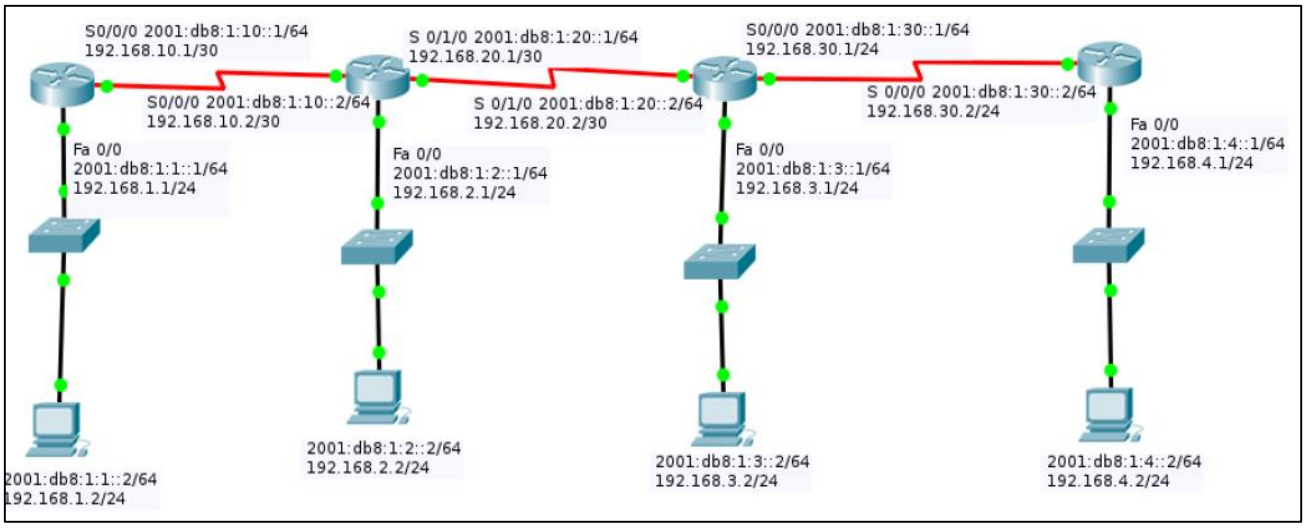


***Figura 6**: Topologia de Rede De Testes*
***Fonte**: Autoria Própria*

As configurações de cada equipamento foram todas aplicadas com base nesta topologia, com o fim de garantir a homogeneidade dos testes, pois ao aplicar diferentes cenários em topologias específicas, não é possível assumir com clareza que os dados apresentados de fato representam apenas a diferença de desempenho de cada técnica de transição.

4.2. Cenários

Para ser capaz de avaliar cada uma das técnicas independentemente, foram definidos alguns cenários específicos onde seria realizada a configuração necessária para o funcionamento do protocolo a ser testado juntamente com a técnica de transição a ser implementada. Os cenários são IPV4 Puro, IPV6 Pur, Pilha Dupla, Tunelamento 6in4 e Tunelamento 4to6.

4.2.1. Cenário 1: IPV4 Puro

Configurando cada um dos roteadores com endereços IPV4 em suas conexões Serial e FastEthernet, foi simulado um ambiente onde os usuários da rede, utilizando IPV4 em sua infraestrutura, trocam informações com a rede externa que também utiliza IPV4. A Figura 7

mostra as configurações realizadas para este teste, apresentando apenas endereços IPV4 configurados nos pontos da rede.

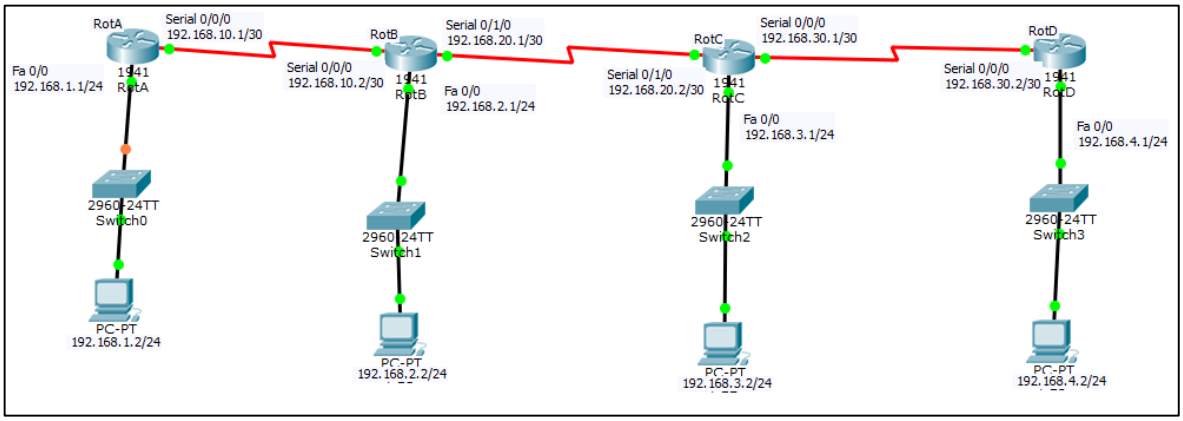


***Figura 7**: Configuração IPV4*
***Fonte:** Autoria Própria*

Com esta abordagem, foram realizados testes de comunicação via linha de comando do RotA para os demais roteadores. O Gráfico 1 registra a média da captura de dados feita após testar a comunicação entre o RotA e o RotB. Já o Gráfico 2 representa a diferença das médias de valores que a mensagem precisa percorrer roteadores mais distantes do RotA, com um intervalo de confiança de 95%.

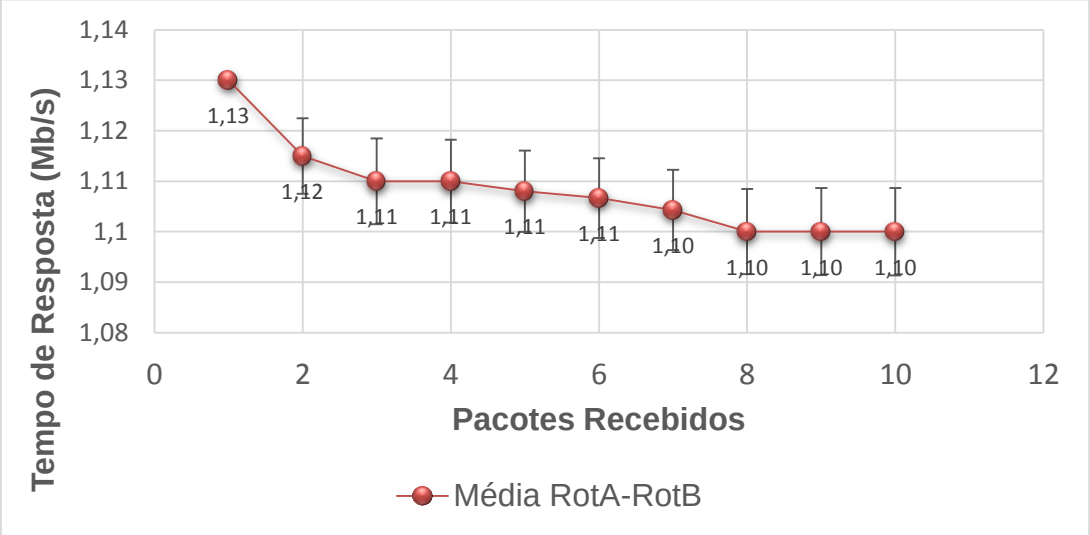


***Gráfico 1**: Gráfico de Tempo de Resposta IPV4 Puro RotA-RotB*
***Fonte**: Autoria Própria*

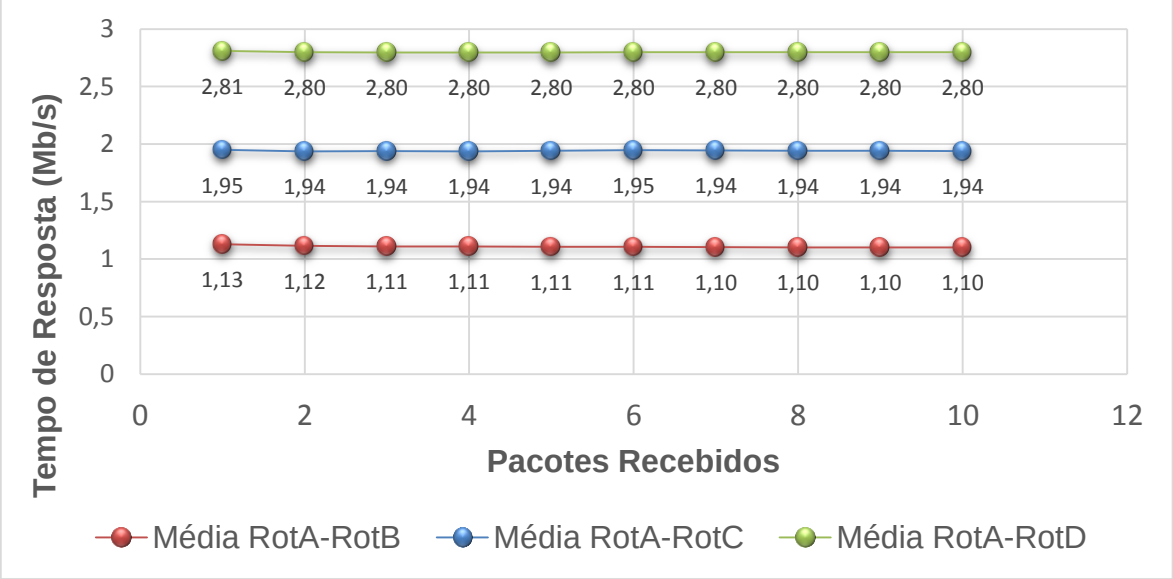


***Gráfico 2**: Gráfico diferença de tempo de resposta IPV4*
***Fonte**: Autoria Própria*

Com uma média de tempo de resposta de 1,1 milissegundos, a conexão RotA-RotB apresentou o melhor valor comparado com as conexões RotA-RotC e RotA-RotD, que trouxeram os valores de aproximadamente 1,9 e 2,8 milissegundos, respectivamente. Os resultados se apresentaram coerentes, de acordo com a topologia utilizada pois quanto mais distante o caminho de rede a ser percorrido, maior foi o tempo de resposta.

Os resultados apresentados no parágrafo anterior foram obtidos utilizando o OSPF como protocolo de roteamento, configurado em uma área única (0 -> *backbone*). Utilizando a mesma topologia, com a aplicação de roteamento estático (sem OSPF), os resultados não apresentaram mudanças significativas. Pôde-se verificar com isto, que a aplicação de um protocolo de roteamento dinâmico como o OSPF não causa mudanças significativas no tempo de resposta apresentado nos testes, em comparação com a uma topologia configurada com roteamento estático.

4.2.2. Cenário 2: IPV6 Puro

Foram aplicados endereços IPV6 a todos os roteadores e máquinas de forma a simular um ambiente em que tanto a rede interna do usuário quando a rede externa à que ele se conecta fossem completamente IPV6.

Assim como no cenário de IPV4 puro, foram realizados testes de comunicações entre as máquinas iniciando no RotA sendo que a média calculada do RotA para o RotB está representada no Gráfico 3 e a comparação as médias dos valores entre os demais roteadores está ilustrada no Gráfico 4, com um intervalo de confiança de 95%.

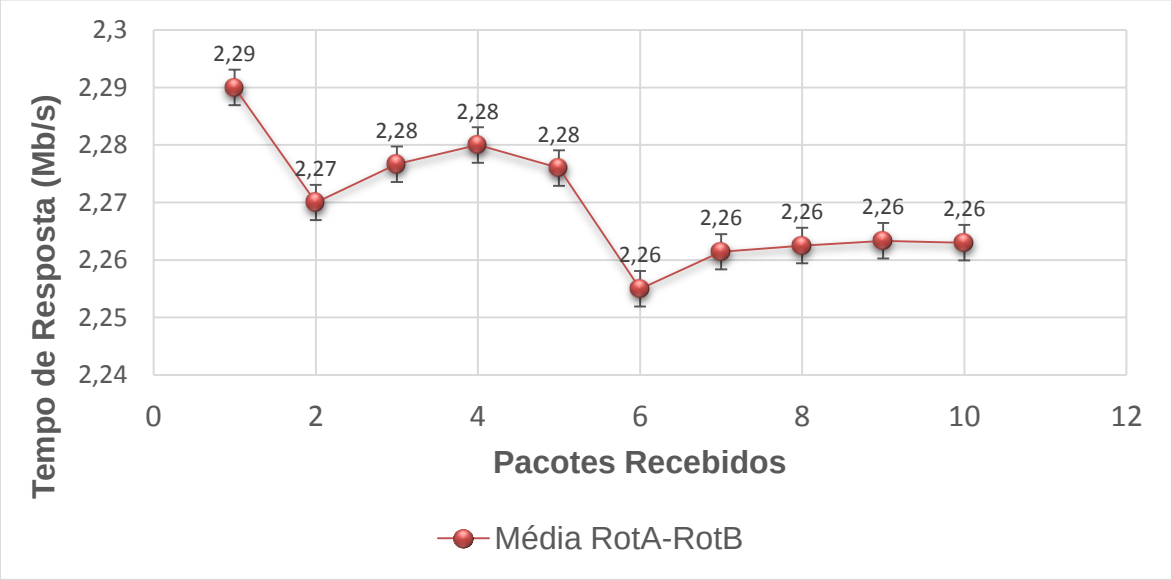


***Gráfico 3**:Gráfico de Tempo de Resposta IPV6 puro RotA-RotB*
***Fonte**: Autoria Própria*

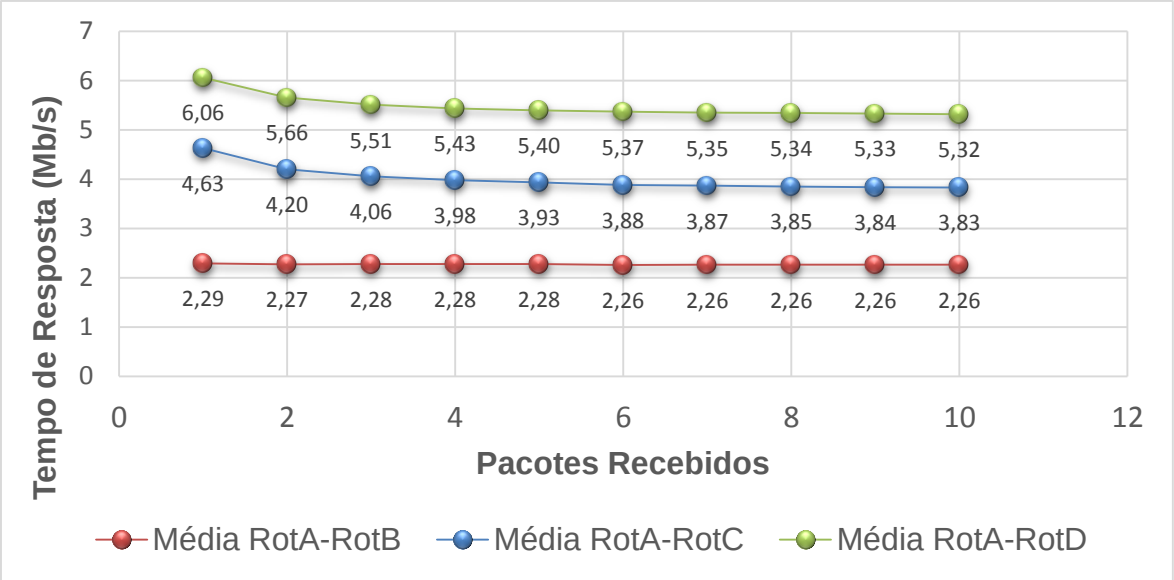


Gráfico 4: *Gráfico com diferença de tempo de resposta IPV6 medido por roteador*
***Fonte**: Autoria Própria*

Os testes IPV6 apresentaram aumento no tempo de resposta, quando comparados com um ambiente IPV4 puro, porém mantendo o crescimento do valor médio, conforme vai aumentando o caminho de rede a ser percorrido. A média de tempo de resposta de RotA-RotB foi igual a 2,26 ms, RotA-RotC igual a 3,81 ms e RotA-RotD igual a 5,26 ms.

Para avaliar o motivo desta diferença de valores, foram também realizados testes utilizando roteamento estático, sem OSPF, porém os valores medidos não sofreram alteração considerável.

Segundo (ZHOU, JACOBSSON, 2008), a razão deste aumento do tempo de resposta, em comparação com o IPV4, ainda não possui uma explicação concreta, porém, devido à prioridade mais lenta do IPV6 em relação ao IPV4, esta pequena diferença de valores acontece durante a transporte de uma mensagem num ambiente IPV6.

4.2.3. Cenário 3: Pilha Dupla

Avaliando um ambiente onde ambos protocolos estão configurados em toda a rede, os resultados se mantiveram os mesmos dos testes em ambientes com um único protocolo, demonstrando que ambos

conseguem se comunicar sem causar impacto nas demais configurações da topologia.

4.2.3.1. TAS IPV4

Realizados testes em um ambiente livre de tráfego de dados, foram também coletadas as medições para todos os roteadores da rede. O Gráfico 5 mostra a média do tempo de resposta de rede utilizando o caminho RotA-RotB, aproximadamente 1,11 ms quando utilizados endereços IPV4 e o Gráfico 6 a comparação entre todos os roteadores, com um intervalo de confiança de 95%.

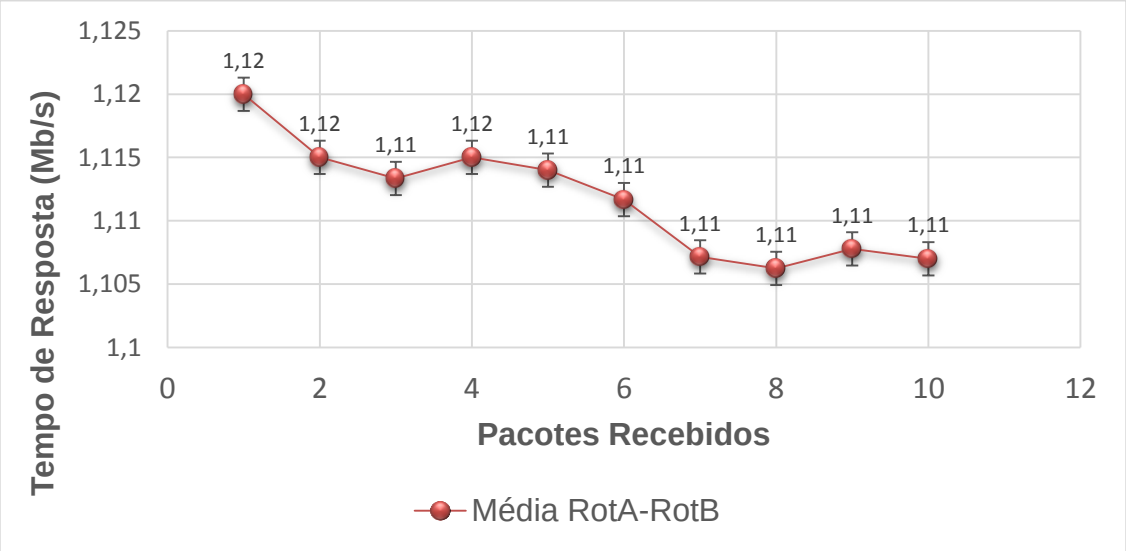


***Gráfico 5**: Gráfico de Tempo de Resposta Pilha Dupla IPV4*
***Fonte:** Autoria Própria*

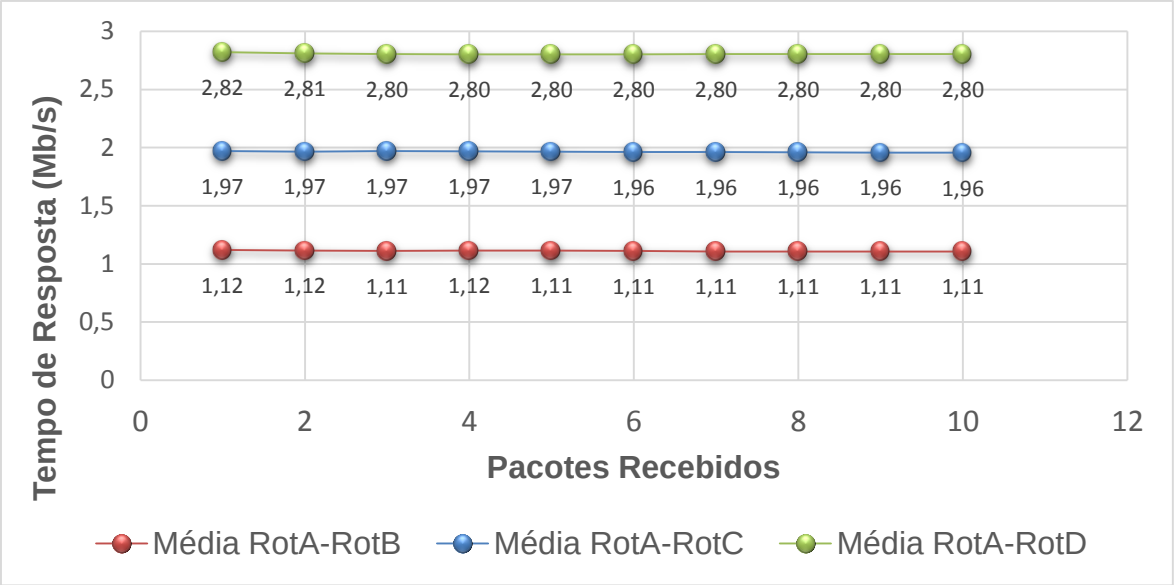


***Gráfico 6**: Gráfico de Tempo de Resposta Pilha Dupla IPV4 todos Roteadores*
***Fonte:** Autoria Própria*

Através dos valores medidos é possível perceber que não houve alterações significativas dos valores medidos em um ambiente IPV4 puro, quando enviadas mensagens IPV4. O Gráfico 7 faz uma comparação entre as médias de valores medidas do RotA ao RotD em ambos os cenários.

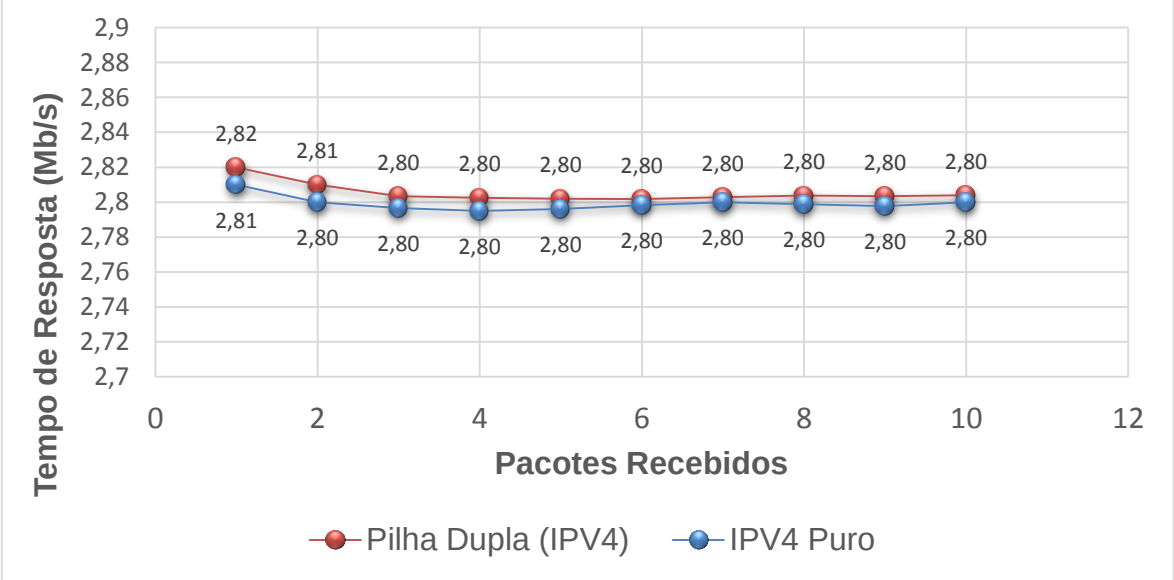


***Gráfico 7**: Comparação IPV4 Puro e Pilha Dupla (IPV4)*
***Fonte:** Autoria Própria*

4.2.3.2. TAS IPV6

Utilizando a mesma configuração realizada para o teste enviando uma mensagem para um endereço IPV4 utilizando a Técnica de Transição de Pilha Dupla, foi agora enviado uma nova mensagem do RotA para o RotB, porém agora para o endereço IPV6 conectado ao RotB.

Os resultados obtidos com este teste também não apresentaram grande diferença em relação com os testes com IPV6 Puro. Assim como no tópico anterior, o Gráfico 8 representa o tempo médio de resposta para a mensagem enviada e o Gráfico 9 a relação dos tempos medidos com mensagens para os demais roteadores, também utilizando um endereço IPV6, com um intervalo de confiança de 95%.

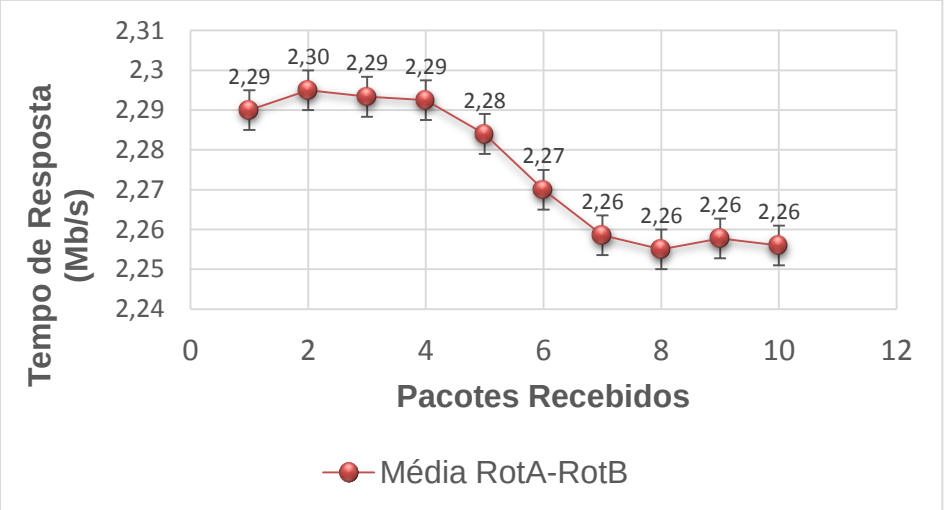


Gráfico 8: *Gráfico de Tempo de Resposta Pilha Dupla IPV6*
Fonte: *Autoria Própria*

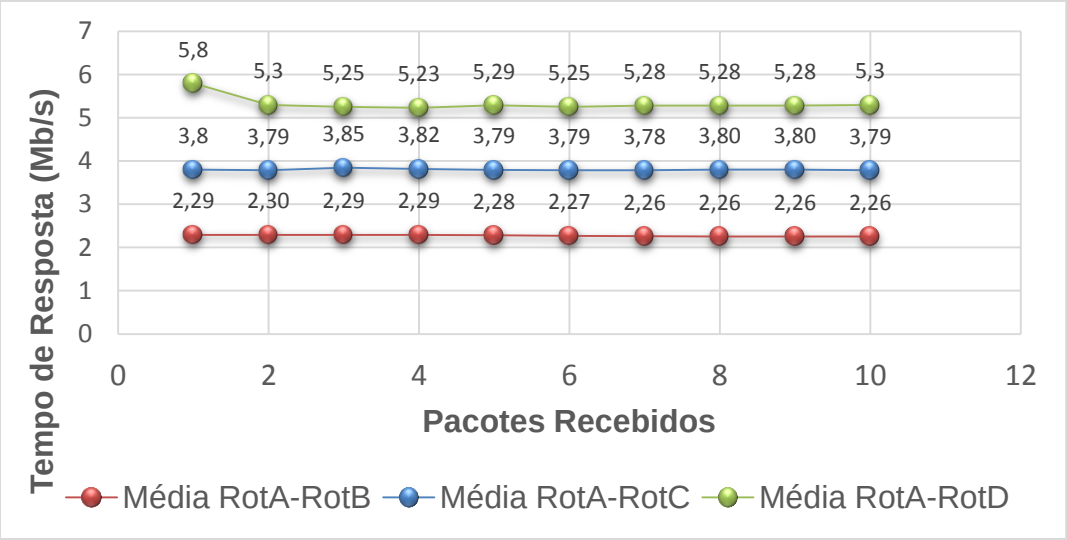


Gráfico 9: *Gráfico de Tempo de Resposta Pilha Dupla IPV6 todos Roteadores*
Fonte: *Autoria Própria*

Traçando um comparativo entre os testes realizados com IPV6 puro e Pilha Dupla, também não houve grande diferença entre os valores medidos do RotA para o RotD. O Gráfico 10 representa esta comparação.

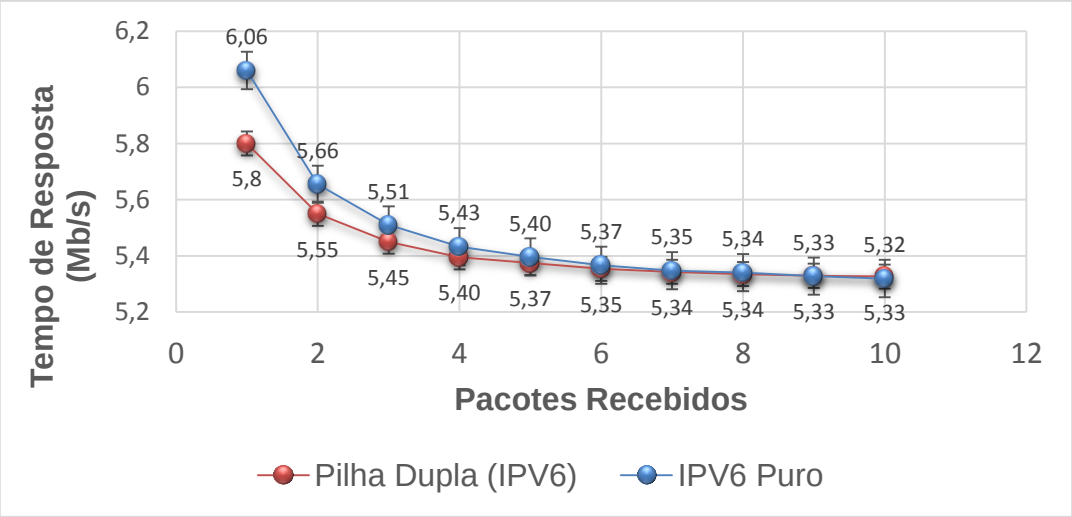


Gráfico 10: *Comparação IPV6 Puro e pilha Dupla (IPV6)*
Fonte: *Autoria Própria*

4.2.3.3. TAAT IPV4

Partindo do princípio de que os testes utilizando protocolo de roteamento dinâmico e estático não apresentaram mudanças significativas nos tempos de resposta, foi optado por utilizar o OSPF no TAAT para IPV4.

Utilizando o JPerf para simular um alto tráfego na rede configurada de aproximadamente 3 Mb, 50% maior que o tráfego máximo configurado nas interfaces seriais dos roteadores, foi verificado um considerável aumento no tempo de resposta medido. O Gráfico 11 registra a média dos valores medidos do RotA para o RotD e a Figura 8 ilustra o tráfego medido na interface do JPerf.

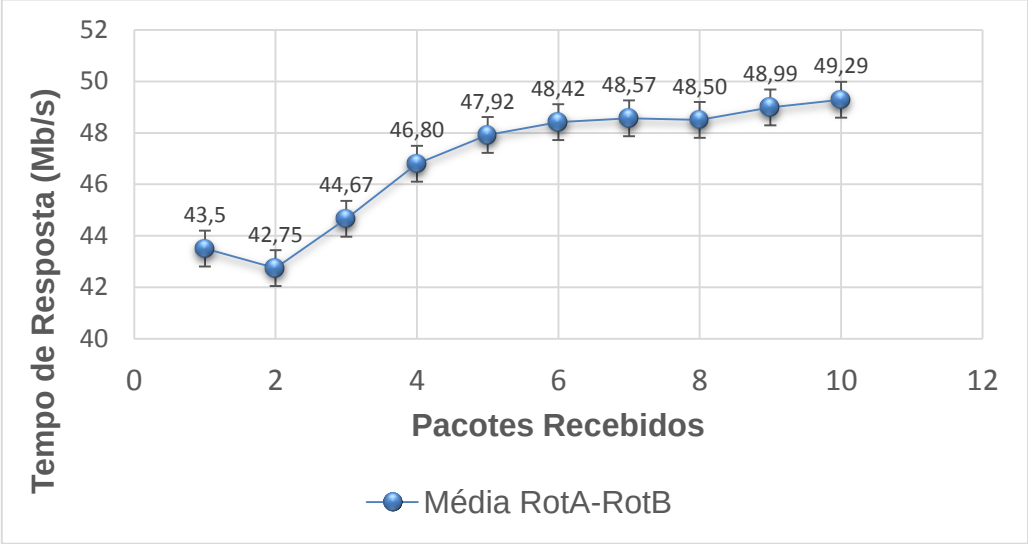


***Gráfico 11**: Tempo de Reposta com Alto Tráfego IPV4*
***Fonte:** Autoria Própria*

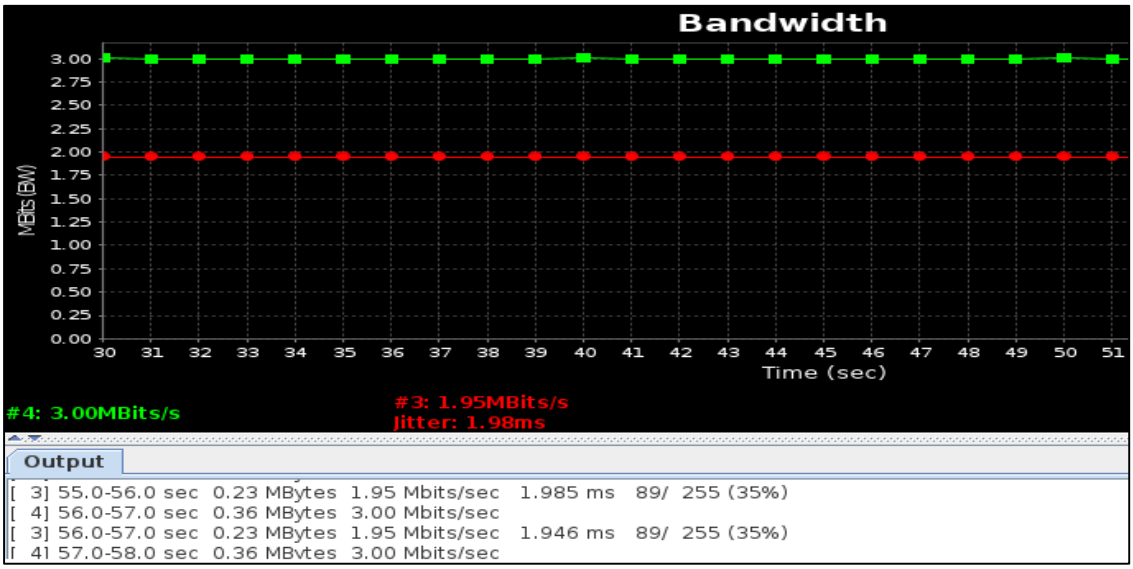


Figura 8: *Medição de Tráfego de Rede com JPerf em IPV4*
Fonte: *Autoria Própria*

Percebe-se que com um tráfego de redes consideravelmente superior ao limitado pela interface do roteador, o tempo de resposta médio calculado chega a ser quase cinquenta vezes maior do que o medido em uma rede sem tráfego algum. Apesar de haver um tráfego de 3mb percorrendo a rede, em uma configuração IPV4 simples, é possível notar o uso médio de 1,95 Mb de taxa de transmissão, praticamente o mesmo do valor máximo configurado na interface do roteador.

4.2.3.4. TAAT IPV6

Também utilizando o OSPF como protocolo de roteamento dinâmico, os testes com alto tráfego de dados utilizando um endereço IPV6 como destino apresentam, assim como no IPV4, um grande aumento do tempo de resposta medido do RotA para o RotD, conforme ilustrado no Gráfico 12.

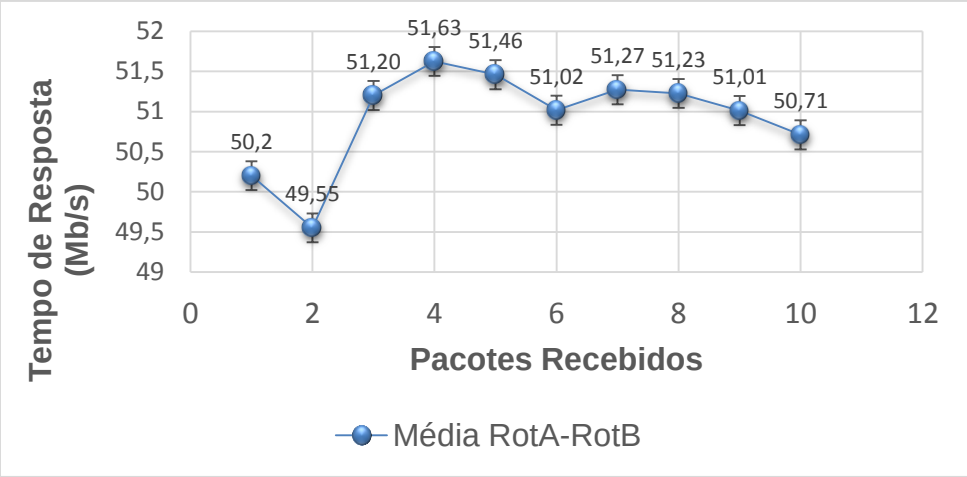


Gráfico 12: *Tempo de Reposta com Alto Tráfego IPV6*
Fonte: *Autoria Própria*

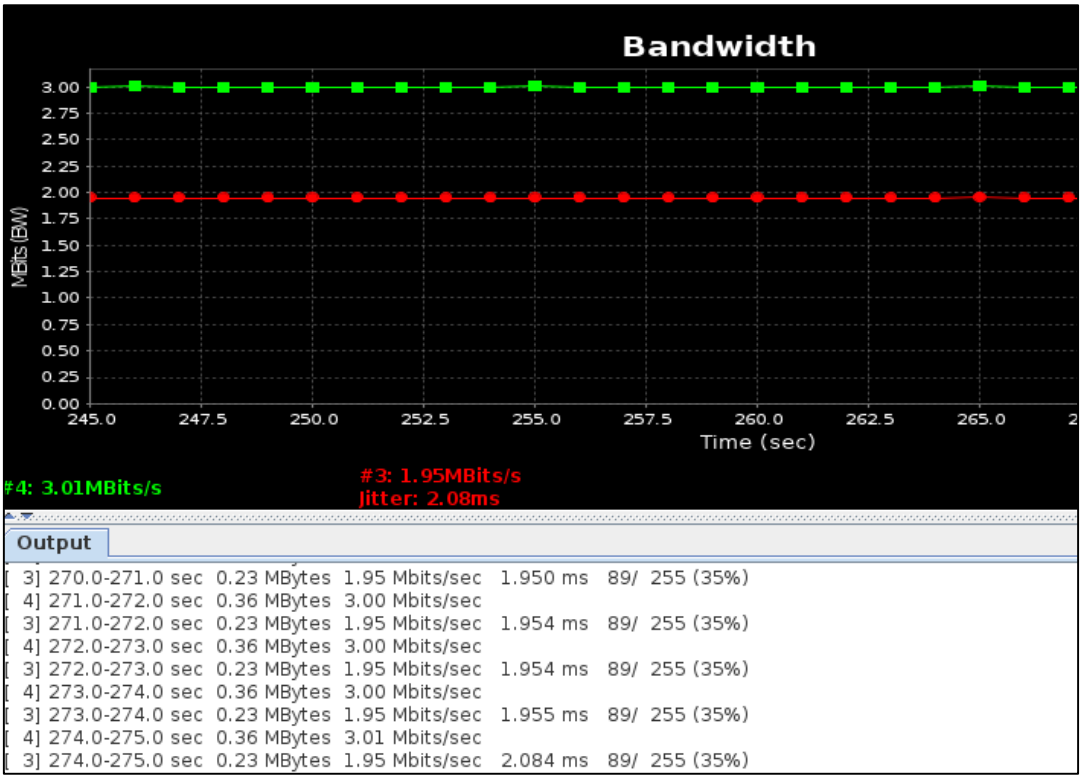


Figura 9*: Medição de Tráfego de Rede com JPerf em IPV6*
Fonte: *Autoria Própria*

Analisando os valores coletados e as informações contidas na Figura 9 é possível perceber um comportamento parecido com o apresentado no TAAT IPV4. O que apresenta destaque nos dados coletados é que a diferença entre a aumento da média de tempo de resposta de ambos protocolos não manteve a mesma proporção da diferença da média

calculada nos testes em ambiente puro. Com um aumento de quase 17% nos testes com IPV4 e de 9,5% nos testes com IPV6 aproximadamente.

4.2.4. Cenário 5: Tunelamento 6 in 4 (IPV6 - IPV4 - IPV6)

Por causa da incompatibilidade entre os protocolos IPV4 e IPV6, surgiram diversas técnicas de transição. Uma destas abordagens é fazer um tunelamento de um protocolo encapsulado em outro, para assim poder encaminha-lo na rede de backbone. Foram realizados testes de desempenho para analisar o comportamento da infraestrutura de rede com a implementação de túneis.

Padrão da internet nos dias de hoje, algumas instituições utilizam protocolo IPV6 em instalações locais e se comunicam através da internet utilizando um túnel IPV4.

4.2.4.1. TAS 6In4

Utilizando uma rede configurada em IPV4 na rede interna e passando por um túnel IPV6 foi realizado um teste de tempo de resposta com média de 5,8 ms, conforme ilustrado no Gráfico 13.

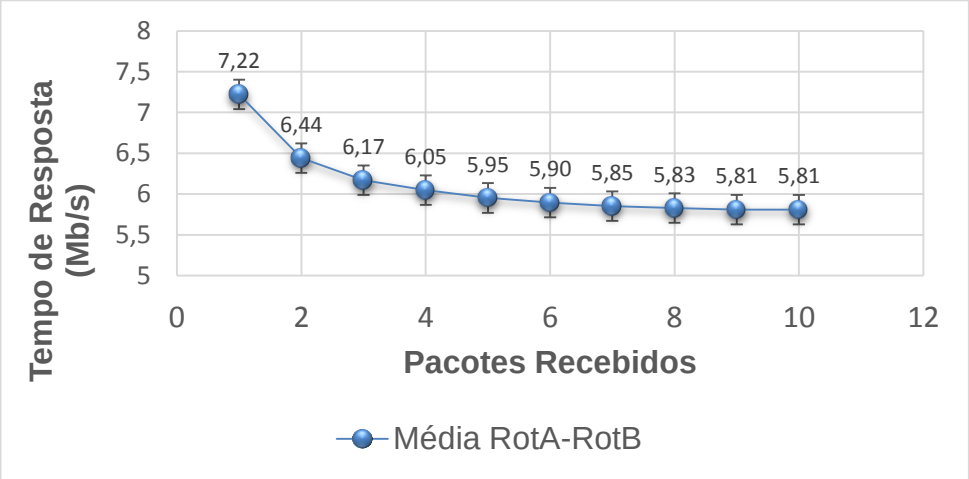


Gráfico 13: *Gráfico de Tempo de Resposta 6in4 RotA-RotD*
Fonte: *Autoria Própria*

Fazendo uma comparação com os cenários analisados anteriormente, com IPV4 puro, IPV6 puro e Pilha Dupla, pode-se constatar que o processo de tunelamento demanda mais tempo de roteamento, visto que é necessário fazer a transcrição dos pacotes diversas vezes na rede.

4.2.4.2. TAAT 6In4

Trazendo agora uma situação mais próxima ao que pode ser encontrado por uma instituição que opte por usar tunelamento 6in4 como Técnica de Transição para IPV6, os testes realizados apresentaram dados muito diferentes dos encontrados até o momento, sendo estes os únicos a registrarem perda de pacotes durante o teste, com perda de até 20 pacotes seguidos até o recebimento da próxima resposta.

O Gráfico 14 ilustra a média do tempo de resposta durante o teste de uma mensagem do RotA para o RotD, com um intervalo de confiança de 95%.

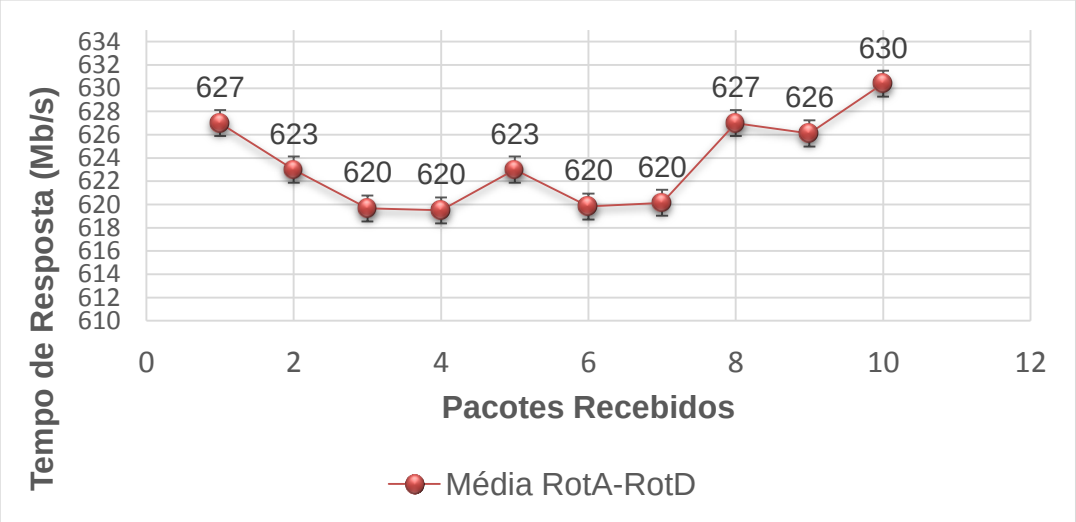


Gráfico 14: *Tempo de Reposta com Alto Tráfego 6in4*
Fonte: *Autoria Própria*

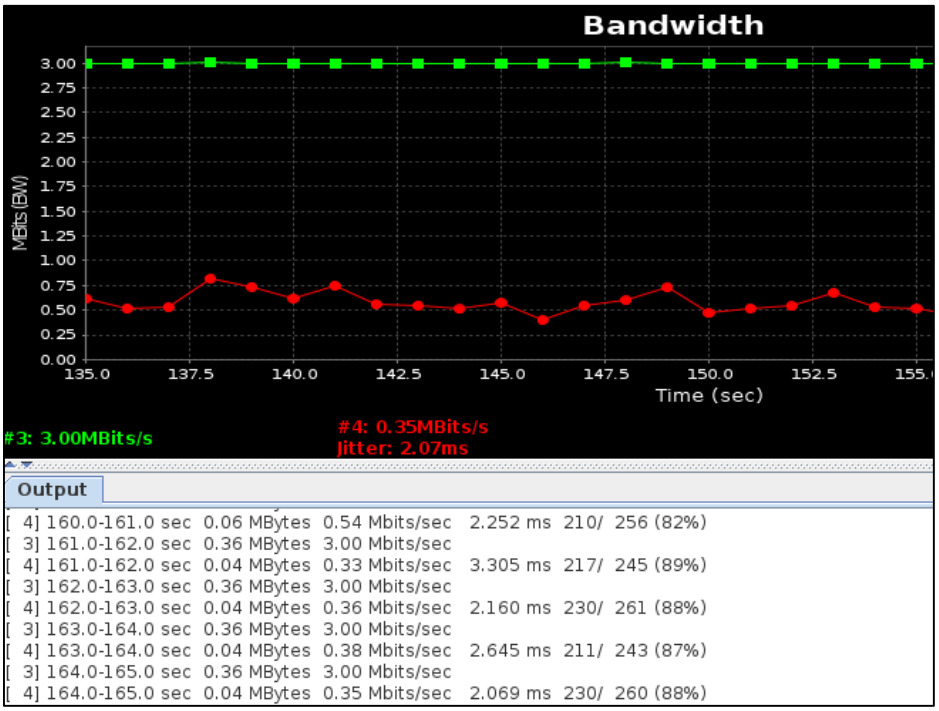


Figura 10: *Medição de Tráfego de Rede com JPerf em IPV6*
Fonte: *Autoria Própria*

Percebe-se através da Figura 10 que a quantidade de rede sendo utilizada durante o processo de comunicação do RotA e do RotD é de cerca de 0,35 Mb/s, aproximadamente 18% da quantidade de disponível nas interfaces seriais dos roteadores. Com valores medidos cerca de 10 vezes o valor medido para os testes com a Técnica de Pilha Dupla, é possível verificar que a comunicação entre os pontos da rede se torna problemática caso exista um pico de tráfego muito alto na rede, fazendo do tunelamento uma opção não muito interessante caso uma intermitência na comunicação seja algo crítico.

4.2.5. Cenário 4: Tunelamento 4 to 6 (IPV4 - IPV6 - IPV4)

Configurando agora um túnel capaz de receber mensagens IPV4, encapsula-las com endereços IPV6 através da rede e depois retorna-las à configuração IPV4 inicial, foi possível realizar testes simulando um tunelamento denominado 4to6.

O resultado apresentou um aumento no tempo de resposta, visto que as mensagens precisavam ser convertidas várias vezes antes de retornar ao ponto de origem. O tempo médio de resposta de mensagens que percorriam o caminho RotA-RotD foi de 6,98 milissegundos, conforme mostra o Gráfico 15. Houve um aumento de aproximadamente 30% em relação ao mesmo teste realizado em um ambiente IPV6 puro.

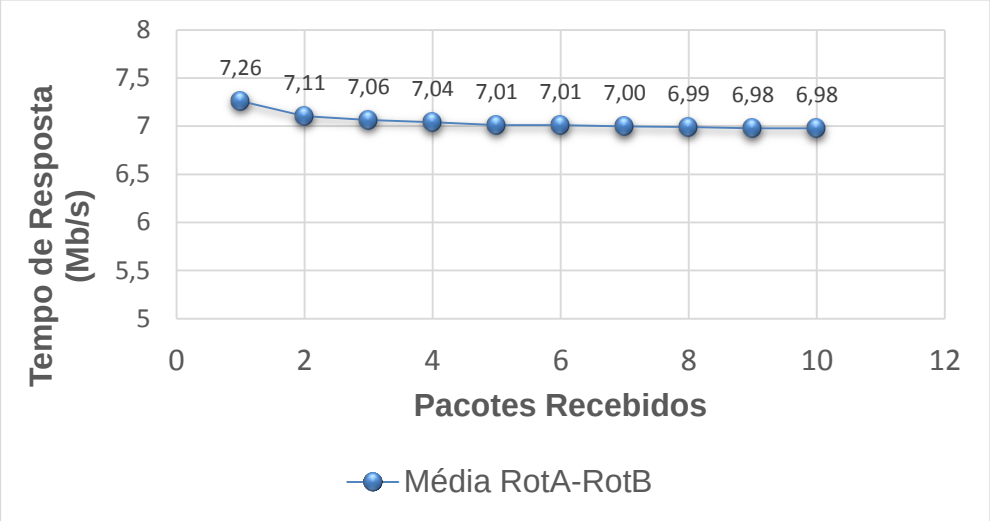


Gráfico 15: *Gráfico de Tempo de Resposta 4to6 RotA-RotD*
Fonte: *Autoria Própria*

Percebe-se também um aumento no tempo médio de resposta em comparação com os cenários sem tunelamento, porém o fator mais interessante é a diferença de tempo em relação a um tunelamento 6in4, um aumento de cerca de 20%.

4.3. Apuração de Resultados

Após realizar os testes com os vários tipos de cenários apresentados, verificou-que o método de Transição de Pilha Dupla se adequa melhor como alternativa para utilização de IPV6 em uma rede com topologia simples, pois não causa impacto no protocolo IPV4 e torna o ambiente capaz de receber requisições IPV6. O Gráfico 16 representa uma comparação das médias de

valores medidos para cada um dos diferentes cenários, com comunicação do RotA para o RotD em um ambiente livre de tráfego de dados.

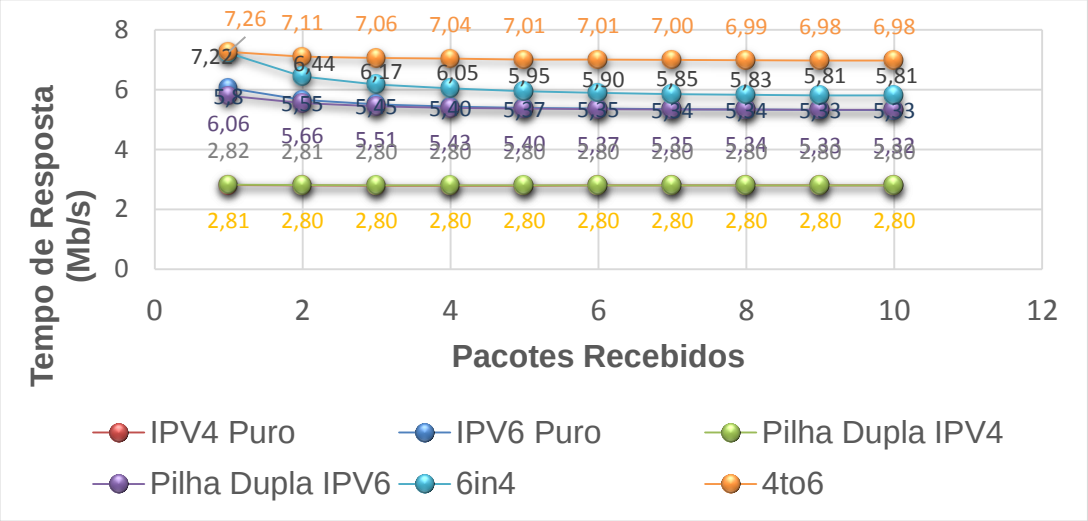


Gráfico 16: *Comparativo de Tempo de Reposta nos cenários testados do RotA ao RotD*
Fonte: *Autoria Própria*

Avaliando os dados acima, é possível perceber que a técnica de transição de Pilha Dupla não onera um maior custo para transportar as mensagens dos protocolos IPV4 e IPV6, em comparação com os ambientes configurados apenas com um protocolo. Apesar dos valores medidos com tunelamento 6in4 não apresentarem grande diferença do protocolo IPV6 puro, quando colocado em um ambiente onde existe grande tráfego de dados a comunicação se tornou inviável, levando cerca de 0,5 segundo para se obter o retorno de um pacote de dados enviado.

Em relação aos testes realizados com o protocolo de roteamento dinâmico OSPF, vale ressaltar que tanto no IPV4 quanto no IPV6, o OSPF se comporta da mesma forma, utilizando os mesmos critérios e métricas para escolha de roteamento de pacotes. O interessante aqui é perceber a diferença no processo de configuração de ambos, sendo esta mais simples em IPV6, visto que no IPV6 não é necessário especificar todas as redes às quais o roteador deve ser capaz de utilizar para o roteamento dinâmico, mas apenas identificar quais as interfaces do roteador que deverão realizar o roteamento. A Figura 11 ilustra a diferença de configuração entre ambos.

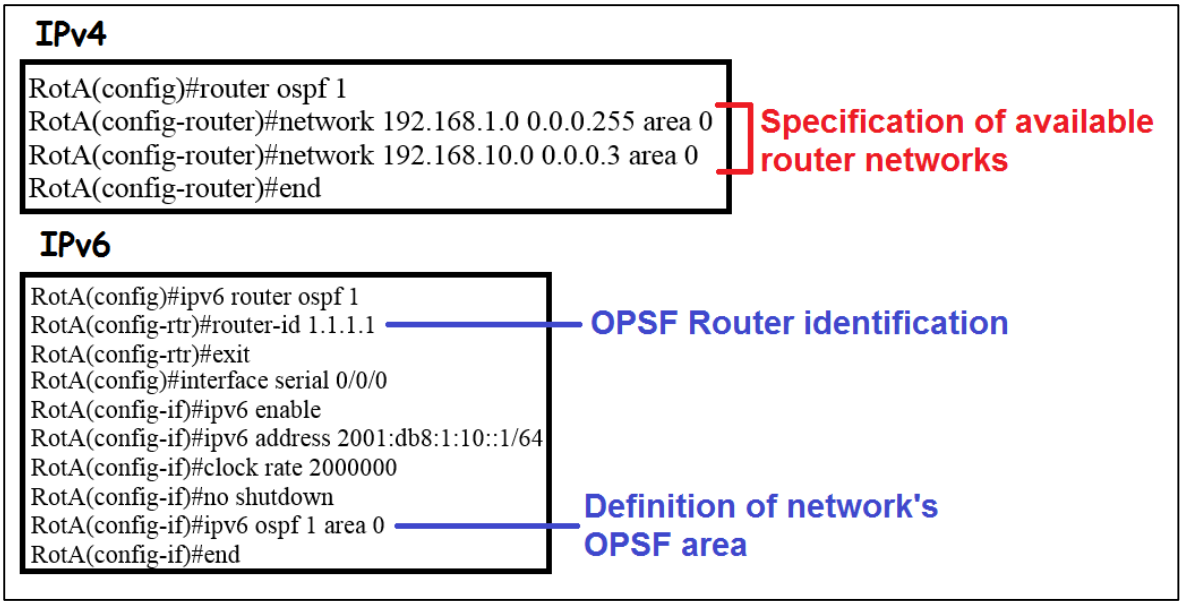


Figura 11: *Comparação de configuração de OSPF*
Fonte: *Autoria Própria*

5. CONCLUSÕES

Levando em consideração a situação atual do IPV4 no mundo, se torna inevitável pensar em utilizar o IPV6 como protocolo de redes, e dentro de alguns anos, o IPV6 acabará se tornando o protocolo mais utilizado nas redes de computadores ao redor do mundo. Por causa disso, faz-se imprescindível o conhecimento de qual técnica de transição existente pode ser utilizada para atingir este objetivo.

Fazendo use de técnicas de transição como a de Pilha Dupla, Tunelamento, entre outras, é possível aplicar o protocolo IPV6 em um ambiente de redes configurado apenas para IPV4. O que difere uma da outra são critérios como custos envolvidos, configuração necessária, necessidades de infraestrutura e tempo de resposta.

Considerando estes critérios, foi possível concluir através deste trabalho que a Pilha Dupla é a técnica que permitiu a melhor adequação do IPV6 em uma infraestrutura de rede IPV4 existente, e que mesmo em um ambiente que apresenta alto tráfego de dados, esta é capaz de administrar o roteamento de ambos os protocolos, sem causar perda de pacotes e com tempo de resposta de aproximadamente 50 ms para os testes realizados em um laboratório de redes. Além do fato de que não é preciso remover as configurações antigas, mas apenas adicionar o roteamento para os endereços IPV6.

O Tunnel Broker e o Teredo utilizam tunelamento 6in4 e, baseado nos testes realizados no cenário 6in4, foi verificado que a tendência para estas técnicas é de que haja um aumento considerável no tempo de resposta da conexão da infraestrutura de redes, fazendo com que sua utilização não seja a mais recomendada, principalmente para ambientes onde não possa haver interrupções na comunicação. Aliado a isso, ainda existe o problema de segurança para o Teredo, onde é possível estabelecer uma conexão não confiável e ter as portas de comunicação abertas para uma possível invasão.

Concluímos também que a aplicação do protocolo de roteamento dinâmico OSPF não apresenta impacto no tempo de resposta de comunicação, porém apenas permite que o roteador gerencie o roteamento dos pacotes de rede de

forma dinâmica, sendo que, uma configuração diferente deve ser realizada para cada um dos protocolos utilizados na rede.

6. REFERECIAS BIBLIOGRÁFICAS

ALJA'AFREH, R. MELLOR, J. et.al. **A Comparison between the Tunneling process and Mapping schemes for IPV4/IPV6 Transition.** International Conference on Advanced Information Networking and Applications Workshops, 2009.

BIRKNER, M. **Projeto de Interconexão de Redes. Cisco Internetwork Design – CID.** Pág 108-177, 2003
Constraints and Various Transition Mechanisms. IEEE Computer Society, 2008.

DLTEC do Brasil. http://dltec.com.br/blog/cisco/entendendo-o-modelo-osi-para-melhorar-sua-capacidade-de-resolver-problemas-em-uma-rede-cisco/ Acessado em 13-11-15 às 23:13.

DOMINGOS, F. http://alessandrobianchini.com.br/artigos/ipv6.pdf Acessado em 12-12-15 às 19:21.

DURDAGI, E. BULDU, A. **IPV4/IPV6 security and threat comparisons,** Elsevier, Science Redirect. Janeiro, 2010.

GALLO, M. A; HANCOCK, W. M. **Comunicação entre Computadores e Tecnologias de Rede**. 2004. Pioneira Thomson Learning.

GOVIL, J. KAUR, N et al. **An Examination of IPV4 and IPV6 Networks: Constraints and Various Transition Mechanisms.** IEEE Southeastcon, 2008.

HIROMI, R. YOSHIFUJI, H. **Problems on IPV4-IPV6 network Transition.** IEEE Computer Society, 2005.

HOAGLAND, J. **The Teredo Protocol: Tunneling Past Network Security and Other Security Implications.** Symantec Corporation. Symantec Advanced Threat Research, 2007.

HUANG, S. **Tunneling IPV6 through NAT with Teredo mechanism.** Advanced Information Networking and Application. AINA 2005.

IETF. https://tools.ietf.org/html/rfc3053. Acessado em 17-11-15 às 00:36

IMASTERS. http://imasters.com.br/artigo/8826/redes-e-servidores/tipos-de-roteamento. Acessado em 15-11-15 às 15:00.

IPV6.BR. http://IPV6.br/entenda/introducao/. Acessado em 11-05-15 às 23:47.

K. K., ETTIKAN, et al. **Application Performance Analysis in Transition**

Mechanism from IPV4 to IPV6, Multimedia University (MMU), 2001.

MEDEIROS, A. SILVA, M. **Evolução do Protocolo da Internet (IP): do IPV4 ao IPV6.** EPOCA, 2010.

MESONPI. http://mesonpi.cat.cbpf.br/IPV6/textos/sobre_%20IPV6/. Acessado em 26-06-15 às 12:50.

NGNET.IT. **Interoperability between IPV4 and IPV6**. http:/ntrg.cs.tcd.ie/undergrad/4ba2.02/IPV6/interop.html. Acessado em 11-05-15 às 16:00.

RADWAN, A.M. **Using IPSec in IPV6 Security**, Community College of Applied Science & Technology, 2005.

SMETANA, G. **IPV4 e IPV6**. http://www.abusar.org.br/ftp/pitanga/Redes/ArtigoIP.pdf Acessado em: 12-06-15 às 23:02.

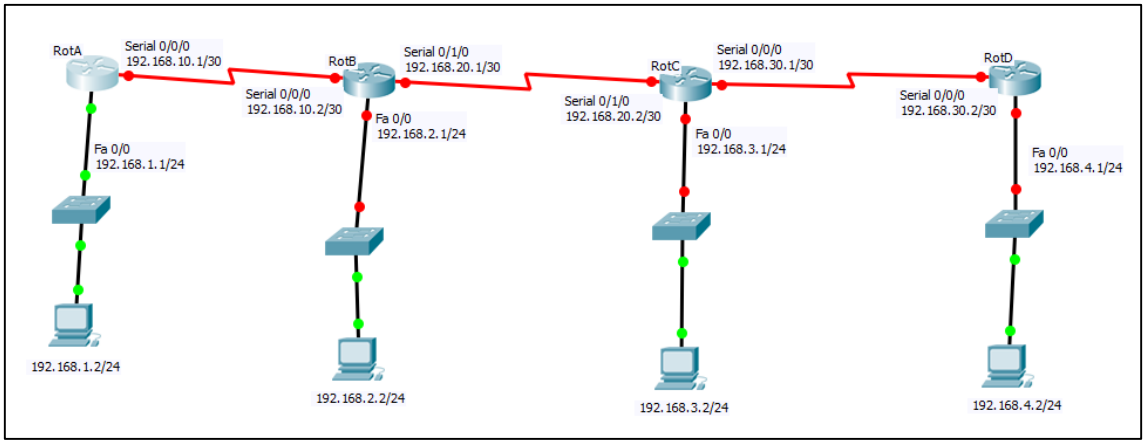
TANENBAUM, A. **Redes de Computadores. Quarta Edição**, 2003

TECHNET. https://technet.microsoft.com/pt-br/library/cc758763%28v=ws.10%29.aspx. Acessado em 26-06-15 às 20:13.

ZHOU, X. JACOBSSON, M. et.al. **IPV6 delay and loss performance evolution.** International Journal of Communication Systems, 2008.

APÊNDICE I – CONFIGURAÇÃO DE ROTEADORES

1. Cenário IPV4 Puro – Roteamento Estático



Configuração do RotA
Router>enable
Router#config terminal
Router(config)#hostname RotA
RotA(config)#interface fastethernet 0/0
RotA(config-if)#ip address 192.168.1.1 255.255.255.0
RotA(config-if)#no shutdown
RotA(config-if)#
RotA(config-if)#exit
RotA(config)#interface serial 0/0/0
RotA(config-if)#ip address 192.168.10.1 255.255.255.252
RotA(config-if)#clock rate 2000000
RotA(config-if)#no shutdown
RotA(config-if)#exit
RotA(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
RotA(config)#end
RotA#
RotA#wr
Building configuration...
[OK]

Configuração do RoteadorB
Router>enable
Router#config terminal
Router(config)#hostname RotB
RotB(config)#interface serial 0/0/0

```
RotB(config-if)#ip address 192.168.10.2 255.255.255.252
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#interface serial 0/1/0
RotB(config-if)#ip address 192.168.20.1 255.255.255.252
RotB(config-if)#clock rate 2000000
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#interface fastethernet  0/0
RotB(config-if)#ip address 192.168.2.1 255.255.255.0
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
RotB(config)#ip route 192.168.3.0 255.255.255.0 serial 0/1/0
RotB(config)#ip route 192.168.4.0 255.255.255.0 serial 0/1/0
RotB(config)#end
RotB#
RotB#wr
Building configuration...
[OK]
```

Configuração do roteador C

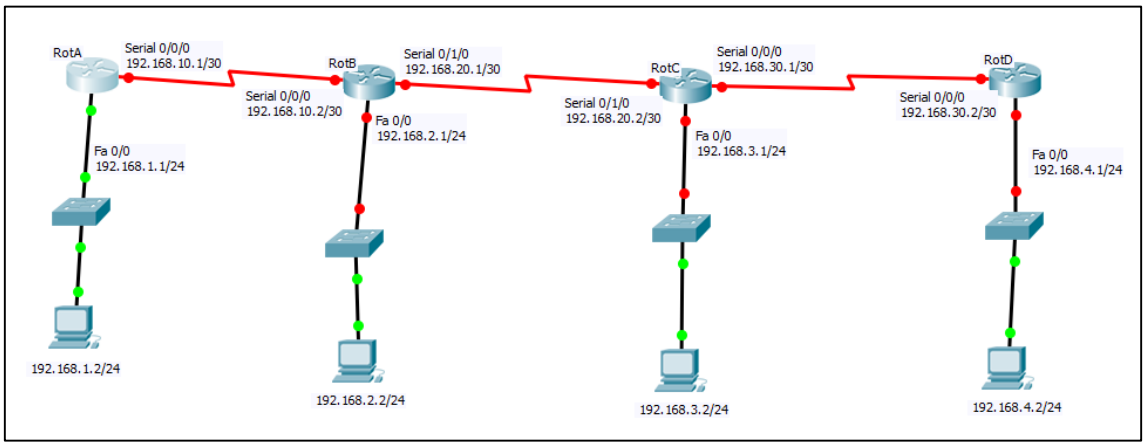
```
Router>enable
Router#config terminal
Router(config)#hostname RotC
RotC(config)#interface serial 0/1/0
RotC(config-if)#ip address 192.168.20.2 255.255.255.252
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#interface serial 0/0/0
RotC(config-if)#ip address 192.168.30.1 255.255.255.252
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#interface fastethernet 0/0
RotC(config-if)#ip address 192.168.3.1 255.255.255.0
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#ip route 192.168.1.0 255.255.255.0 serial 0/1/0
RotC(config)#ip route 192.168.2.0 255.255.255.0 serial 0/1/0
RotC(config)#ip route 192.168.4.0 255.255.255.0 serial 0/0/0
RotC(config)#end
RotC#
RotC#wr
Building configuration...
[OK]
```

Configuração do Roteador D

```
Router>enable
```

```
Router#config terminal
Router(config)#hostname RotD
RotD(config)#interface serial 0/0/0
RotD(config-if)#ip address 192.168.30.2 255.255.255.252
RotD(config-if)#no shutdown
RotD(config-if)#exit
RotD(config)#interface fastethernet 0/0
RotD(config-if)#ip address 192.168.4.1 255.255.255.0
RotD(config-if)#no shutdown
RotD(config-if)#exit
RotD(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
RotD(config)#end
RotD#
RotD#wr
Building configuration...
[OK]
RotD#
```

2. Cenário IPV4 puro – roteamento dinâmico com OSPF de área única



Configuração do RotA

```
Router>enable
Router#config terminal
Router(config)#hostname RotA
RotA(config)#interface fastethernet 0/0
RotA(config-if)#ip address 192.168.1.1 255.255.255.0
RotA(config-if)#no shutdown
RotA(config-if)#
RotA(config-if)#exit
RotA(config)#interface serial 0/0/0
RotA(config-if)#ip address 192.168.10.1 255.255.255.252
RotA(config-if)#clock rate 2000000
RotA(config-if)#no shutdown
RotA(config-if)#exit
```

```
RotA(config)#router ospf 1
RotA(config-router)#network 192.168.1.0 0.0.0.255 area 0
RotA(config-router)#network 192.168.10.0 0.0.0.3 area 0
RotA(config-router)#end
RotA#
RotA#wr
Building configuration...
[OK]
```

Configuração do RoteadorB

```
Router>enable
Router#config terminal
Router(config)#hostname RotB
RotB(config)#interface serial 0/0/0
RotB(config-if)#ip address 192.168.10.2 255.255.255.252
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#interface serial 0/1/0
RotB(config-if)#ip address 192.168.20.1 255.255.255.252
RotB(config-if)#clock rate 2000000
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#interface fastethernet  0/0
RotB(config-if)#ip address 192.168.2.1 255.255.255.0
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#router ospf 1
RotB(config-router)#network 192.168.10.0 0.0.0.3 area 0
RotB(config-router)#network 192.168.2.0 0.0.0.255 area 0
RotB(config-router)#network 192.168.20.0 0.0.0.3 area 0
RotB(config-router)#end
RotB#
RotB#wr
Building configuration...
[OK]
```

Configuração do roteador C

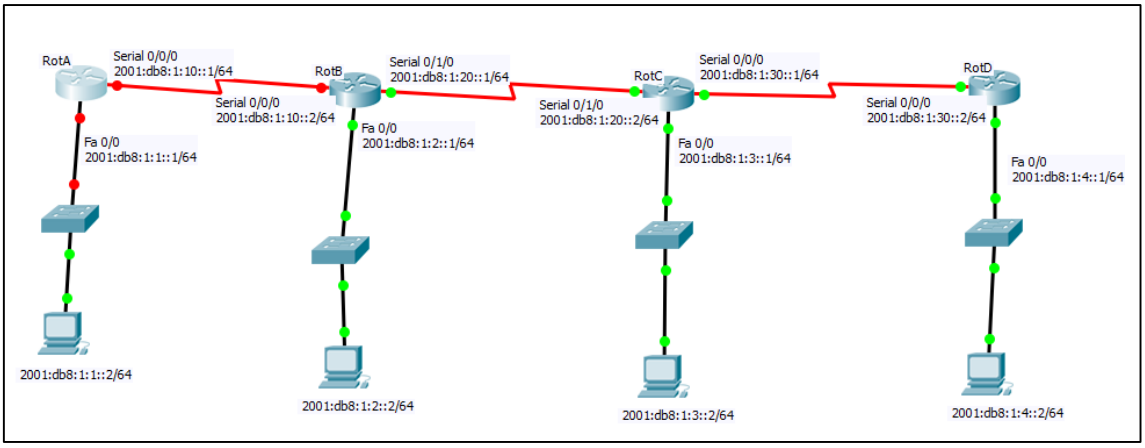
```
Router>enable
Router#config terminal
Router(config)#hostname RotC
RotC(config)#interface serial 0/1/0
RotC(config-if)#ip address 192.168.20.2 255.255.255.252
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#interface serial 0/0/0
RotC(config-if)#ip address 192.168.30.1 255.255.255.252
RotC(config-if)#no shutdown
RotC(config-if)#exit
```

```
RotC(config)#interface fastethernet 0/0
RotC(config-if)#ip address 192.168.3.1 255.255.255.0
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#router ospf 1
RotC(config-router)#network 192.168.20.0 0.0.0.3 area 0
RotC(config-router)#network 192.168.3.0 0.0.0.255 area 0
RotC(config-router)#network 192.168.30.0 0.0.0.3 area 0
RotC(config-router)#end
RotC#wr
Building configuration...
[OK]
```

Configuração do Roteador D

```
Router>enable
Router#config terminal
Router(config)#hostname RotD
RotD(config)#interface serial 0/0/0
RotD(config-if)#ip address 192.168.30.2 255.255.255.252
RotD(config-if)#no shutdown
RotD(config-if)#exit
RotD(config)#interface fastethernet 0/0
RotD(config-if)#ip address 192.168.4.1 255.255.255.0
RotD(config-if)#no shutdown
RotD(config-if)#exit
RotD(config)#router ospf 1
RotD(config-router)#network 192.168.30.0 0.0.0.3 area 0
RotD(config-router)#network 192.168.4.0 0.0.0.255 area 0
RotD(config-router)#end
RotD#wr
Building configuration...
[OK]
RotD#
```

3. Cenário IPV6 Puro – Roteamento Estático



Configuração do RotA
Router>enable
Router#config terminal
Router(config)#hostname RotA
RotA(config)#IPV6 unicast-routing
RotA(config)#interface fa 0/0
RotA(config-if)#IPV6 enable
RotA(config-if)#IPV6 address 2001:db8:1:1::1/64
RotA(config-if)#no shutdown
RotA(config-if)#exit
RotA(config)#interface serial 0/0/0
RotA(config-if)#IPV6 enable
RotA(config-if)#IPV6 address 2001:db8:1:10::1/64
RotA(config-if)#clock rate 2000000
RotA(config-if)#no shutdown
RotA(config-if)#exit
RotA(config)#IPV6 route ::/0 serial 0/0/0
RotB(config)#exit
RotA#wr
Building configuration...
[OK]

Configuração do RotB
Router>enable
Router#config terminal
Router(config)#hostname RotB
RotB(config)#IPV6 unicast-routing
RotB(config)#interface fastethernet 0/0
RotB(config-if)#IPV6 enable
RotB(config-if)#IPV6 address 2001:db8:1:2::1/64
RotB(config-if)#no shutdown
RotB(config-if)#exit

```
RotB(config)#interface serial 0/0/0
RotB(config-if)#IPV6 enable
RotB(config-if)#IPV6 address 2001:db8:1:10::2/64
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#interface serial 0/1/0
RotB(config-if)#IPV6 enable
RotB(config-if)#IPV6 address 2001:db8:1:20::1/64
RotB(config-if)#clock rate 2000000
RotB(config-if)#no shutdown
RotB(config-if)#exit
RotB(config)#IPV6 route 2001:db8:1:1::/64 serial 0/0/0
RotB(config)#IPV6 route 2001:db8:1:3::/64 serial 0/1/0
RotB(config)#IPV6 route 2001:db8:1:4::/64 serial 0/1/0
RotB(config)#exit
RotB#
RotB#wr
Building configuration...
[OK]
```

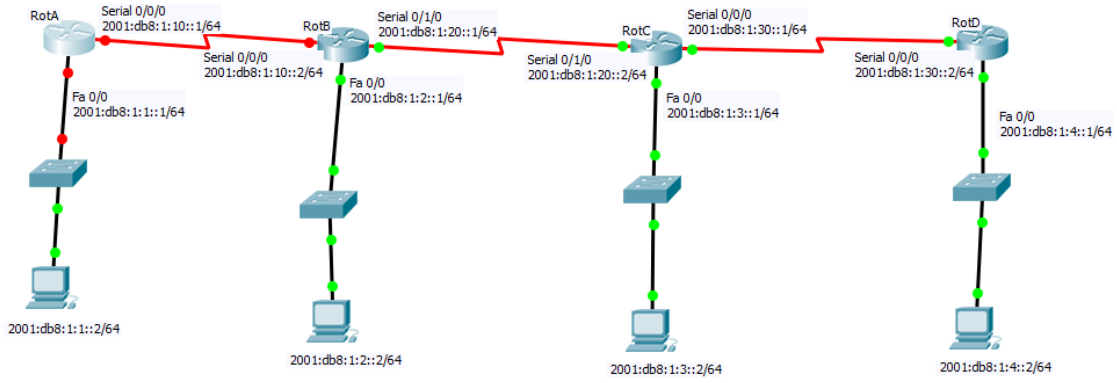
Configuração do RotC

```
Router>enable
Router#config terminal
Router(config)#hostname RotC
RotC(config)#IPV6 unicast-routing
RotC(config)#interface fastethernet 0/0
RotC(config-if)#IPV6 enable
RotC(config-if)#IPV6 address 2001:db8:1:3::1/64
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#interface serial 0/1/0
RotC(config-if)#IPV6 enable
RotC(config-if)#IPV6 address 2001:db8:1:20::2/64
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#interface serial 0/0/0
RotC(config-if)#IPV6 enable
RotC(config-if)#IPV6 address 2001:db8:1:30::1/64
RotC(config-if)#clock rate 2000000
RotC(config-if)#no shutdown
RotC(config-if)#exit
RotC(config)#IPV6 route 2001:db8:1:1::/64 serial 0/1/0
RotC(config)#IPV6 route 2001:db8:1:2::/64 serial 0/1/0
RotC(config)#IPV6 route 2001:db8:1:4::/64 serial 0/0/0
RotC(config)#exit
RotC#wr
Building configuration...
[OK]
```

Configuração do RotD

```
Router>enable
Router#config terminal
Router(config)#hostname RotD
RotD(config)#IPV6 unicast-routing
RotD(config)#interface fastethernet 0/0
RotD(config-if)#IPV6 enable
RotD(config-if)#IPV6 address 2001:db8:1:4::1/64
RotD(config-if)#no shutdown
RotD(config-if)#exit
RotD(config)#interface serial 0/0/0
RotD(config-if)#IPV6 enable
RotD(config-if)#IPV6 address 2001:db8:1:30::2/64
RotD(config-if)#no shutdown
RotD(config-if)#
RotD(config-if)#exit
RotD(config)#IPV6 route ::/0 serial 0/0/0
RotD#
RotD#wr
Building configuration...
[OK]
```

4. Cenário IPV6 Puro – roteamento dinâmico com OSPF de área única



Configuração do RotA

```
Router>enable
Router#config terminal
Router(config)#hostname RotA
```

```
RotA(config)#IPV6 unicast-routing
RotA(config)#IPV6 router ospf 1
RotA(config-rtr)#router-id 1.1.1.1
RotA(config-rtr)#exit
RotA(config)#interface fa 0/0
RotA(config-if)#IPV6 enable
RotA(config-if)#IPV6 address 2001:db8:1:1::1/64
RotA(config-if)#no shutdown
RotA(config-if)#IPV6 ospf 1 area 0
RotA(config-if)#exit
RotA(config)#interface serial 0/0/0
RotA(config-if)#IPV6 enable
RotA(config-if)#IPV6 address 2001:db8:1:10::1/64
RotA(config-if)#clock rate 2000000
RotA(config-if)#no shutdown
RotA(config-if)#IPV6 ospf 1 area 0
RotA(config-if)#end
RotA#wr
Building configuration...
[OK]
```

Configuração do RotB

```
Router>enable
Router#config terminal
Router(config)#hostname RotB
RotB(config)#IPV6 unicast-routing
RotB(config)#IPV6 router ospf 1
RotB(config-rtr)#router-id 2.2.2.2
RotB(config-rtr)#exit
RotB(config)#interface fastethernet 0/0
RotB(config-if)#IPV6 enable
RotB(config-if)#IPV6 address 2001:db8:1:2::1/64
RotB(config-if)#no shutdown
RotB(config-if)#IPV6 ospf 1 area 0
RotB(config-if)#exit
RotB(config)#interface serial 0/0/0
RotB(config-if)#IPV6 enable
RotB(config-if)#IPV6 address 2001:db8:1:10::2/64
RotB(config-if)#no shutdown
RotB(config-if)#IPV6 ospf 1 area 0
RotB(config-if)#exit
RotB(config)#interface serial 0/1/0
RotB(config-if)#IPV6 enable
RotB(config-if)#IPV6 address 2001:db8:1:20::1/64
RotB(config-if)#clock rate 2000000
RotB(config-if)#no shutdown
RotB(config-if)#IPV6 ospf 1 area 0
RotB(config-if)#end
```

```
RotB#
RotB#wr
Building configuration...
[OK]
```

Configuração do RotC

```
Router>enable
Router#config terminal
Router(config)#hostname RotC
RotC(config)#IPV6 unicast-routing
RotC(config)#IPV6 router ospf 1
RotC(config-rtr)#router-id 3.3.3.3
RotC(config-rtr)#exit
RotC(config)#interface fastethernet 0/0
RotC(config-if)#IPV6 enable
RotC(config-if)#IPV6 address 2001:db8:1:3::1/64
RotC(config-if)#no shutdown
RotC(config-if)#IPV6 ospf 1 area 0
RotC(config-if)#exit
RotC(config)#interface serial 0/1/0
RotC(config-if)#IPV6 enable
RotC(config-if)#IPV6 address 2001:db8:1:20::2/64
RotC(config-if)#no shutdown
RotC(config-if)#IPV6 ospf 1 area 0
RotC(config-if)#exit
RotC(config)#interface serial 0/0/0
RotC(config-if)#IPV6 enable
RotC(config-if)#IPV6 address 2001:db8:1:30::1/64
RotC(config-if)#clock rate 2000000
RotC(config-if)#no shutdown
RotC(config-if)#IPV6 ospf 1 area 0
RotC(config-if)#end
RotC#wr
Building configuration...
[OK]
```

Configuração do RotD

```
Router>enable
Router#config terminal
Router(config)#hostname RotD
RotD(config)#IPV6 unicast-routing
RotD(config)#IPV6 router ospf 1
RotD(config-rtr)#router-id 4.4.4.4
RotD(config-rtr)#exit
RotD(config)#interface fastethernet 0/0
RotD(config-if)#IPV6 enable
RotD(config-if)#IPV6 address 2001:db8:1:4::1/64
RotD(config-if)#no shutdown
```

```
RotD(config-if)#IPV6 ospf 1 area 0
RotD(config-if)#exit
RotD(config)#interface serial 0/0/0
RotD(config-if)#IPV6 enable
RotD(config-if)#IPV6 address 2001:db8:1:30::2/64
RotD(config-if)#no shutdown
RotD(config-if)#
RotD(config-if)#IPV6 ospf 1 area 0
RotD(config-if)#
RotD(config-if)#end
RotD#
RotD#wr
Building configuration...
[OK]
```