UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
PÓS-GRADUAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

EVALDO FORTUNATO JUNIOR

ESTRATÉGIA DE MIGRAÇÃO PARA IPV6: ANÁLISE DE IMPLANTAÇÃO DO *DUAL STACK*

MONOGRAFIA

CURITIBA

2014

EVALDO FORTUNATO JUNIOR

ESTRATÉGIA DE MIGRAÇÃO PARA IPV6: ANÁLISE DE IMPLANTAÇÃO DO *DUAL STACK*

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Teleinformática e Redes de Computadores, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Armando Rech Filho.

CURITIBA
2014

Dedico esse trabalho

À minha mãe, Julia, que se fez presente em quase todos os momentos da minha vida até agora, me ajudando direta ou indiretamente a conquistar os objetivos que planejei desde criança e possibilitando que os meus sonhos se tornassem realidade.

Aos meus padrinhos José Hamilton e Hilma, que me deram todo o amor e apoio que puderam, e ajudaram nos momentos complicados na parte emocional e até financeiramente.

À minha namorada, Caroline, que me apoia nas decisões profissionais e acadêmicas, visando sempre a minha evolução profissional e humana.

AGRADECIMENTOS

Agradeço

Ao meu orientador, Prof. Dr. Armando Rech Filho, pela orientação do trabalho, dicas, sugestões e revisões minuciosas.

Aos meus colegas profissionais, colegas de curso, colegas de futebol, colegas de churrasco, e amigos pessoais, Jean Manganelli e Felipe Rechia, pela ajuda prestada e paciência que tiveram comigo durante o curso.

Ao meu gestor durante o período de DATACOM, Alexandre Ceruti, por ajudar a tornar possível a realização desse curso.

Ao colega de DATACOM, Edson Leme, pelas empolgadas conversas e discussões sobre a transição do IPv4 para o IPv6.

À Deus, por me dar a oportunidade de tentar fazer cada dia melhor que o anterior.

“Dual stack where you can – Tunnel where you must – Translate only when you have a gun to your head”

(Tomáš Ondovčík – Cisco)

RESUMO

FORTUNATO JUNIOR, Evaldo. **Estratégia de Migração para IPv6: Análise de Implantação do *Dual Stack*.** 53f. Monografia (Especialização em Teleinformática e Redes de Computadores) – Programa de Pós Graduação em Teleinformática e Redes de Computadores. Universidade Tecnológica Federal do Paraná. Curitiba 2014.

A transição para o IPv6 se tornou um problema para a Internet devido à passividade das empresas em fazer a troca de protocolos. O atraso dessa transição tem preocupado as entidades reguladoras, visto que os blocos de endereços IPv4 disponíveis estão esgotados. O presente trabalho apresenta uma estratégia de migração para o IPv6 por meio do método *dual stack*. Para demonstrar que o *dual stack* pode ser aceito e reconhecido como o melhor método para a migração, foram executados testes comparando com outro método de transição, o tunelamento, representado pelo *6over4*. Os testes envolvem medidas de *jitter*, latência e recursos de *hardware*, além de três testes de falhas de sistema, que são *flap* de protocolo de roteamento, *reboot* de equipamento e falha de *link*. Os resultados apontaram desempenho semelhante entre os métodos, porém com vantagem para o *dual stack* considerando a facilidade de implantação, desempenho do processador do roteador e baixo impacto na rede. A desvantagem ficou por conta da utilização de memória RAM em relação ao *6over4* nos roteadores utilizados durante os testes.

Palavras-chave: IPv6. Pilha dupla. Migração. Transição. 6over4.

ABSTRACT

FORTUNATO JUNIOR, Evaldo. **Migration Strategy to IPv6: Analysis of Dual Stack Deployment.** 53 lf. Monografia (Especialização em Teleinformática e Redes de Computadores) – Programa de Pós Graduação em Teleinformática e Redes de Computadores. Universidade Tecnológica Federal do Paraná. Curitiba 2014.

The transition to IPv6 has become a problem to the Internet due to the passivity of companies to make the protocols switching. The delay of this transition has worried the regulatory authorities since the available IPv4 address blocks are exhausted. The present paper presents a migration strategy to IPv6 through the dual stack method. To demonstrate that dual stack can be acceptable and recognized as the best migration method some tests were executed comparing with another transition method, the tunneling, represented by 6over4. The tests involve measures of jitter, latency and hardware resources, and there are also three failure tests which are protocol flap, reboot and link failure. The results indicate similar performance between both methods, but with an advantage to the dual stack considering the ease of deployment, performance of router processor and the low impact on the network. The major disadvantage was because of RAM memory utilization compared to 6over4 on the used routers during the tests.

Keywords: IPv6. Dual Stack. Migration. Transition. 6over4

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

6over4	IPv6 over IPv4
6rd	IPv6 Rapid Deployment
6to4	IPv6 to IPv4
ARPANET	Advanced Research Projects Agency Network
BGP	Border Gateway Protocol
CANTIP	Common Architecture for the Internet
CIDR	Classless Inter-Domain Routing
CGN	Carrier Grade NAT
CPU	Central Processing Unit
DARPA	Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DSTM	Dual Stack Transition Mechanism
EGP	External Gateway Protocol
EUI-64	Extended Unique Identifier 64 bit
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICCC	International Computer Communication Conference
ID	Identification Document
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Internal Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IPng	Internet Protocol next generation
IPv4	Internet Protocol version 4
IPv5	Internet Protocol version 5
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LSA	Link State Advertisement
MAC	Media Access Control
MIT	Massachusetts Institute of Technology

NAT	Network Address Translation
NPL	National Physical Laboratories
OSPF	Open Shortest Path First
OSPFv3	Open Shortest Path First version 3
P2P	Peer-to-Peer
QoS	Quality of Service
RAM	Random Access Memory
RAND	Research And Development
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RFC	Request For Comments
SIPP	Simple Internet Protocol Plus
ST2	internet STream protocol version 2
TCP	Transmission Control Protocol
TUBA	TCP and UDP with Bigger Addresses
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

SUMÁRIO

1. INTRODUÇÃO

O protocolo IP (*Internet Protocol*), também conhecido por IPv4 (*Internet Protocol version 4*), foi criado para identificar computadores na Internet. Como as redes eram apenas acadêmicas no início da Internet, não houve um projeto para larga escala de utilização, mas a aplicação do IPv4 se mostrou tão eficiente que o mesmo passou a ser aproveitado para fins comerciais. A partir disso os endereços começaram a ser distribuídos pelo IANA (*Internet Assigned Numbers Authority*), que é o órgão gestor responsável.

O rápido crescimento da Internet e a política de distribuição de endereços adotada gerou a preocupação de que o IPv4 se esgotasse em questão de dois ou três anos (EQUIPE IPv6.br, 2012). Alguns métodos foram criados para "atrasar" o esgotamento do IPv4, como o CIDR (*Classless Inter-Domain Routing*) e o NAT (*Network Address Translation*), porém esses métodos não resolveriam a situação, apenas dariam sobrevida ao IPv4 e garantiriam melhor distribuição e utilização dos endereços até que uma solução definitiva fosse tomada. Para resolver esse problema, e alguns outros, o IETF (*Internet Engineering Task Force*) padronizou o IPv6 (*Internet Protocol version 6*), cuja capacidade de endereçamento é extremamente superior à de seu antecessor, e possui ainda algumas características de melhoria do protocolo.

Este trabalho visa compor um estudo, com base em análises teóricas e práticas, sobre a substituição do IPv4 pelo IPv6 utilizando o método *dual stack* (ou pilha dupla), que é tido por Berenger (S.D.) como melhor método para compor o cenário transitivo.

O método *dual stack* trata-se de IPv4 e IPv6 funcionando paralelamente em um mesmo equipamento, mas em pilhas diferentes, ou seja, um independente do outro. Desse modo, o IPv4 pode continuar sendo utilizado normalmente até que não seja mais desejado, e posteriormente possa ser desabilitado para então o IPv6 assumir todo o trabalho.

É aqui abordado o funcionamento dos protocolos de endereçamento, o esgotamento do IPv4, a criação do IPv6 e seus avanços e como está ocorrendo o processo de implantação do protocolo IPv6. Analisa-se neste trabalho o processo *dual stack*, seus prós e contras, e sua importância no processo de migração do IPv4, além de uma comparação de desempenho contra o método *6over4* (IPv6 *over* IPv4), pois é outro processo utilizado para auxiliar na transição e de fácil implantação, utilizando configurações básicas em um roteador capacitado.

Para o correto entendimento sobre os protocolos e métodos de migração, este trabalho contempla uma pesquisa sobre o papel do IPv4 na história da *Internet*, os motivos do esgotamento de endereços e sua substituição pelo IPv6 e como está ocorrendo o processo de implantação do IPv6 nos últimos anos. Além disso, é feito um comparativo entre o método *dual stack* e o *6over4*, citando os motivos do comparativo e os prós e contras dos dois métodos de transição. Para finalizar, é feita uma comparação básica de desempenho entre os dois métodos escolhidos visando identificar a viabilidade de implantação do *dual stack*, a qual envolve testes de convergência, *reboot* de requipamento, medidas de *jitter* e latência.

O objetivo geral desse trabalho é avaliar o desempenho do método de transição do IP para o IPv6 conhecido como *dual stack*, e confirmar se este método é o mais adequado e efetivo para realizar a migração para o IPv6.

Os objetivos específicos desse trabalho são:

- Discutir a atual situação do IP, mostrando brevemente como e porque foi criado. Quais são os atuais problemas, como se chegou ao esgotamento dos endereços;
- Mostrar como o IPv6 foi criado, o que foi pensado, quem são os responsáveis, como são distribuídos os endereços;
- Demonstrar e exemplificar os avanços do IPv6 em relação ao IPv4, uma vez que a vantagem da utilização do IPv6 não se limita em maior quantidade de endereços disponíveis;
- Pesquisar sobre como está ocorrendo a adoção do IPv6;
- Comprovar as vantagens e desvantagens do método *dual stack*, além de comparações básicas de desempenho em relação ao método 6over4.

A elaboração desse trabalho se faz pertinente para demonstrar que a implantação do IPv6 pode acontecer de maneira simples e de preferência sem causar problemas na rede. O método *dual stack* é um dos possíveis para a rede se adequar rapidamente ao IPv6, e causando pouco impacto na implantação.

Os resultados dos testes presentes nesse trabalho indicam de maneira simples se o *dual stack* é reconhecidamente um diferencial na implantação, e se a rede se comporta bem com os protocolos IPv4 e IPv6 trabalhando paralelamente.

As conclusões são formadas com base em análise de latência, *jitter*, tempo de convergência, utilização de memória RAM (*Random Access Memory*) e consumo de CPU (*Central Processing Unit*). São comparadas as medidas feitas com a aplicação do *dual stack* e do *6over4*.

A pesquisa foi desenvolvida, primeiramente, com a busca por informações que pudessem comprovar o atrasado na implantação do IPv6, através de sites, artigos e normas, e indicando porque o *dual stack* tem potencial para ser o melhor método de transição dos protocolos.

Posteriormente, para comprovar a afirmação sobre o *dual stack*, um método de transição com base em tunelamento foi escolhido para a execução de um comparativo com o objetivo de demonstrar que na prática isso realmente ocorre. O resultado final é registrado de acordo com medidas coletadas através de testes em uma topologia que compõe um cenário para ambos os métodos de transição.

O primeiro capítulo trata de apresentar o trabalho e seus objetivos, além de situar o leitor resumidamente sobre o problema que há na transição do IPv4 para o IPv6.

No segundo capítulo é feito um estudo contendo um resumo sobre a história da Internet, características do IPv4 e IPv6, a necessidade de transição do endereço e como está ocorrendo a adoção do IPv6.

O terceiro capítulo trata de uma atividade prática envolvendo testes e medidas dos métodos de transição *dual stack* e *6over4*, e comparando os resultados dos dois métodos em questão.

Por fim são apresentadas as conclusões e referências bibliográficas do trabalho nos capítulos 4 e 5, respectivamente.

2. REVISÃO BIBLIOGRÁFICA

2.1. RESUMO SOBRE A HISTÓRIA DA INTERNET

A Internet se tornou uma ferramenta largamente utilizada desde sua criação. Estima-se que mais de um terço da população mundial já utilizava a Internet até junho de 2012, sendo que a maioria desses usuários estão presentes na Ásia (ARGAEZ, 2012).

As primeiras ideias sobre a Internet surgiram no início da década de sessenta. O Doutor Joseph Carl Robnett Licklider, do MIT (*Massachu*setts *Institute of Technology*), formulou uma série de memorandos sobre uma rede "intergalática" de computadores. Os conceitos básicos imaginados por Licklider são praticamente os mesmos disponibilizados na Internet atualmente, acesso à dados como *e-commerce*, *online banking*, bibliotecas *online,* dentre outros (LEINER, S.D.).

Licklider encabeçou o programa de pesquisa de computadores no DARPA (*Defense Advanced Research Projects Agency*), e convenceu seus sucessores, Lawrense G. Roberts, Ivan Sutherland e Bob Taylor, sobre a importância desse conceito de redes.

Durante a década de sessenta, três grupos diferentes trabalharam paralelamente sobre projetos semelhantes, mas sem que um soubesse do outro. Enquanto Roberts publicava, em 1967, um plano sobre a ARPANET (*Advanced Research Projects Agency Network*), Donald Davies e Roger Scantlebury trabalhavam em um conceito de redes com pacotes no NPL (*National Physical Laboratories*) e, por fim, um grupo do RAND (*Research And Development*) publicou um trabalho sobre redes de roteamento de pacotes para segurança de voz. A palavra "pacote" foi adotada a partir do trabalho do NPL.

Em Outubro de 1972 Robert Kahn fez uma grande, e bem sucedida, demonstração da ARPANET no ICCC (*International Computer Communication Conference*). Essa foi a primeira demonstração pública dessa rede. Ainda nesse mesmo ano ocorreu a aplicação do correio eletrônico (*e-mail*).

A ARPANET trabalhava principalmente com o protocolo NCP (*Network Control Protocol*). O problema é que o NCP não tinha a capacidade de endereçar redes e máquinas, por isso Kahn decidiu desenvolver uma nova versão de protocolo, o qual deveria controlar erros e transmitir dados de maneira confiável. Esse protocolo seria então chamado TCP (*Transmission Control Protocol*). Em conjunto com o IPv4, o TCP proporcionou o cresimento ordenado da Internet. Para casos em que não fosse necessário confiabilidade de entrega dos pacotes, foi criado o UDP (*User Datagam Protocol*).

Conforme o desenvolvimento das LANs (*Local Area Network*), PCs (*Personal Computer*) e *workstations* na década de oitenta, foi necessáriao fazer uma separação de classes de redes, as quais são abordadas no capítulo 2.3.

O crescimento da Internet provocou mudanças também por parte dos roteadores. Originalmente havia um algoritmo único implementado por todos os roteadores na Internet. Com o grande aumento da quantidade de redes na Internet, se fez necessária a criação de modelo hierárquico de roteamento, o qual inclui o uso de um IGP (*Internal Gateway Protocol*) para executar o roteamento interno de uma região, e um EGP (*External Gateway Protocol*) para "unir" todas as regiões.

O protocolo IGP mais utilizado é o OSPF (*Open Shortest Path First*), porém existem outros IGPs comumente utilizados como o RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), que é um protocolo priprietário da empresa Cisco Systems, e o IS-IS (*Intermediate System to Intermediate System*). O protocolo EGP

mais utilizado é o BGP (*Border Gateway Protocol*).

Assim que a ARPANET foi desativada, por volta de 1990, o TCP/IP passou a dominar a Internet. Com o crescimento da Internet e o sucesso do TCP/IP, houve a necessidade da distribuição de endereços IPv4 por todo o mundo, fato que gerou a preocupação de que os endereços se esgotariam em breve. Por conta disso, alguns métodos, como NAT e CIDR, foram criados para manter o IPv4 funcionando por mais algum tempo, porém a solução para resolver completamente a questão de esgotamento foi a criação do IPv6.

2.2. O IPV4 E SUAS CARACTERÍSTICAS

O IPv4 foi desenvolvido para interconectar sistemas de redes de comutação de pacotes. Seu objetivo é proporcionar a transmissão de dados em blocos chamados datagramas, onde fontes e destinos são *hosts* identificados por endereços fixos. O IPv4 proporciona ainda a fragmentação e remontagem de datagramas de tamanho elevado, para que possam ser transmitidos em forma de pequenos pacotes, caso necessário. Na sequência destacam-se algumas características do protocolo, o qual é especificado na RFC 791 (POSTEL, 1981).

2.2.1. Endereçamento do IPv4

O protocolo IPv4 é definido pela RFC 791, a qual contempla todos os aspectos que devem ser considerados para a utilização desse protocolo. O objetivo dessa RFC (*Request For Comments*) é prover as funções necessárias para entregar um combinado de *bits* de uma fonte para um destino.

Um importante mecanismo do IPv4 é sua capacidade de endereçamento. Um endereço é basicamente formado por quatro octetos (32 *bits*), o que possibilita mais de quatro bilhões de endereços disponíveis para utilização.

A representação do endereço IPv4 normalmente é feita através de 4 números decimais de 0 à 255. A figura 2.1 mostra um exemplo da associação de um endereço com representação decimal em conjunto com seus respectivos octetos binários.

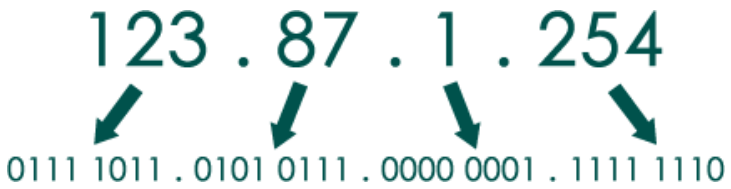

Figura 2.1 – Exemplo de endereço IPv4 e seus respectivos *bits*.

Fonte: Autoria própria.

2.3. A NECESSIDADE DE UM NOVO TIPO DE ENDEREÇO

Quando definido, o IPv4 foi divido em três classes de tamanhos fixos. A classe A proporciona a utilização de 128 redes e 16.777.216 *hosts* para cada rede. A classe B pode proporcionar 16.384 redes com 66.536 *hosts* em cada. Por fim, a classe C deixa 2.097.152 endereços para rede, com capacidade de 256 *hosts* para cada rede.

Segundo o Núcleo de Informação e Coordenação do ponto BR, essa divisão se mostrou ineficiente, pois a classe A atenderia um número pequeno de redes, mas ocupava metade dos endereços disponíveis, e para endereçar 300 dispositivos em uma rede, por exemplo, seria necessário obter um bloco da Classe B, fazendo com que mais de 65 mil endereços fossem desperdiçados, porque um bloco da classe C não atenderia esse número. Além disso, dezenas de faixas da classe A foram atribuídas a grandes empresas, como por exemplo IBM, HP, Apple, dentre outras (SANTOS, 2010).

A partir da década de 1990 a quantidade de *hosts* conectados só aumentou, principalmente após a criação do protocolo HTTP (*HyperText Transfer Protocol*), fato que logo gerou preocupação em relação ao esgotamento da quantidade de endereços.

Para solucionar a questão do esgotamento de IPv4, o IETF definiu algumas estratégias mitigadoras, como a extinção do uso de classes e agregação de rotas. Além disso duas outras técnicas foram apresentadas, o DHCP (*Dynamic Host Configuration Protocol*) e o NAT.

A grande vantagem do DHCP é permitir que um *host* utilize um IPv4 temporariamente, assim, caso esse *host* se desconecte, seu IPv4 ficará novamente disponível para que outro *host* possa utilizá-lo quando necessário.

Já o NAT permite que um único IPv4 seja utilizado para a saída na Internet, gerando grande economia de IPs em uma rede. Porém essa técnica possui algumas desvantagens, como quebra do modelo fim-a-fim, fazendo com que haja queda de desempenho em aplicações como VoIP (*Voice over Internet Protocol*) e conexões P2P (*Peer-to-Peer*).

Embora as ações de mitigação tenham atrasado o esgotamento do IPv4, era necessário a criação de um novo protocolo que desse conta da alta demanda de endereços.

Em 1993 o IETF solicitou ideias para projetar o novo protocolo, chamado inicialmente de IPng (*Internet Protocol next generation*). Tal processo é descrito na RFC 1550, a qual aborda alguns aspectos a serem considerados na entrega das sugestões, como escalabilidade, transição e implantação, segurança, configuração e robustez, dentre outros.

Vários projetos foram estudados para a confecção do novo protocolo, entretando três deles se destacaram, CANTIP (*Common Architecture for the Internet*), TUBA (*TCP and UDP with Bigger Addresses*) e SIPP (*Simple Internet Protocol Plus*). Todos os projetos apresentavam problemas, porém algumas características interessantes do SIPP, e do TUBA foram adotadas para o novo protocolo. O CANTIP acabou não sendo utilizado.

O novo protocolo foi então conhecido por IPv6.

Apesar de pouco conhecido existe um protocolo IP versão 5, o IPv5 (*Internet Protocol version 5*), e por isso o IPng precisou utilizar o “6” para explicar sua versão. O IPv5 na verdade é mais conhecido como ST2 (*internet STream protocol version 2*). Definido pela RFC 1190, e posteriormente revisado na RFC 1819, o ST2 é um protocolo experimental orientado a conexão e criado especificamente para o tráfego multimídia, como *streaming* de áudio e vídeo, além de jogos (EQUIPE IPv6.br, 2012).

2.4. O IPV6 E SEUS AVANÇOS

O IPv6 está definido na RFC 2460, a qual substitui a obsoleta RFC 1883 de 1995.

Suas principais diferenças em relação ao IPv4 podem ser vistas abaixo (DEERING; HINDEN, 1998).

- Maior capacidade de endereçamento

  Enquanto o IPv4 possui 32 *bits*, o tamanho do IPv6 é de 128 *bits*. Esses 128 *bits* permitem o suporte a mais níveis de hierarquia de endereçamento, um número muito maior de nós endereçáveis e a autoconfiguração de endereços simplificada. A escalabilidade do roteamento *multicast* foi melhorada adicionando um campo *scope* para os endereços *multicast*. Além disso, um novo tipo de endereço, chamado *anycast* foi definido, utilizado para enviar pacotes para qualquer nó de um grupo definido.

- Simplificação do formato do cabeçalho

  Alguns campos do cabeçalho IPv4 foram removidos ou considerados opcionais, para reduzir o custo de processamento para manipular um pacote e para limitar o custo da largura de banda do cabeçalho IPv6.

- Suporte melhorado para cabeçalhos de extensão

  A mudança na maneira como o cabeçalho é codificado permite maior eficiência no encaminhamento de pacotes, menor rigor nos limites para a quantidade de opções e maior flexibilidade para possíveis futuras opções.

- Capacidade de classificação de fluxos

  Uma nova funcionalidade foi inserida para possibilitar a marcação de pacotes pertencentes à um determinado fluxo de tráfego, para o qual a fonte dos dados solicita tratamento especial, algo como QoS (*Quality of Service*) ou serviços em tempo real.

- Suporte à autenticação e privacidade

  Foram especificados cabeçalhos de extensão para suportar autenticação, integridade dos dados e opcionalmente confidencialidade de dados.

2.4.1. Mudanças no Cabeçalho

As diferenças básicas do cabeçalho podem ser visualizadas mais facilmente na figura 2.2, a qual possui dois quadros que representam IPv4 e IPv6, respectivamente, e campos coloridos para informar as diferenças.

Em laranja estão os campos cujos nomes foram mantidos do IPv4 para o IPv6. Em vermelho campos removidos, ou seja, que não se encontram mais na versão 6 do protocolo. Em azul os nomes e posições que mudaram de uma versão para a outra. E por fim um novo campo adicionado, em marrom.

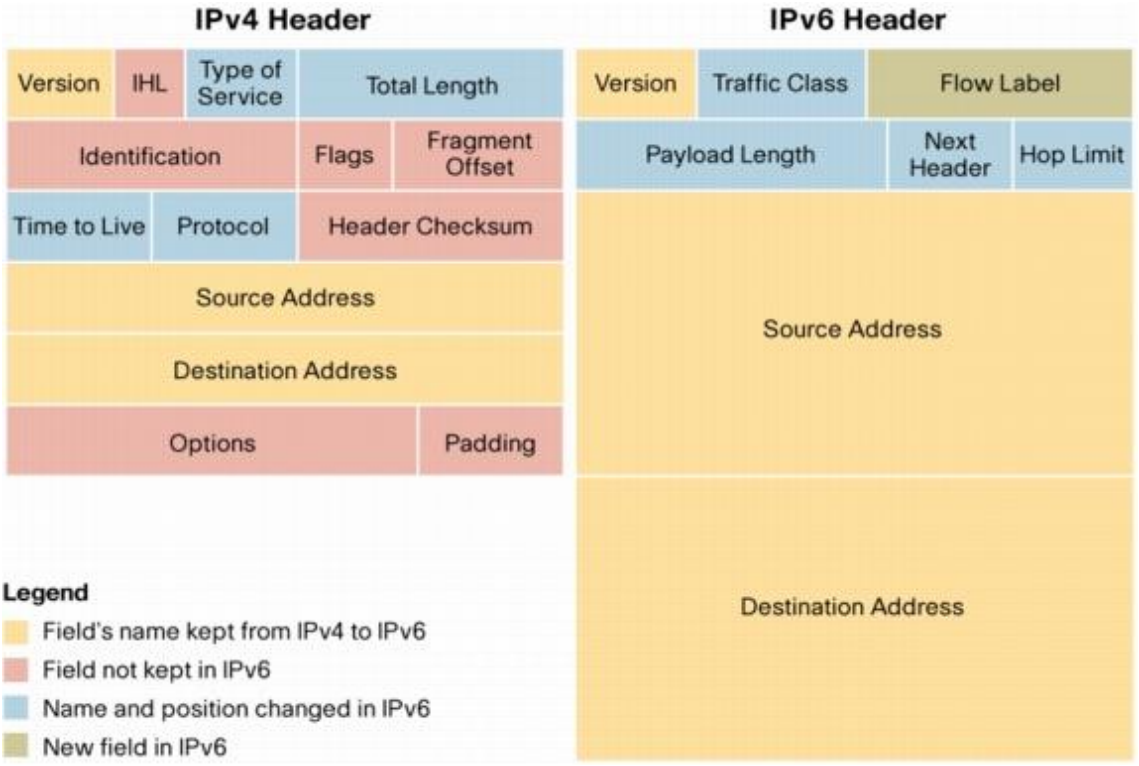

Figura 2.2 – Diferenças entre os cabeçalhos de IPv4 e de IPv6.

Fonte: Cisco (2006).

2.4.2. Endereçamento do IPv6

O endereçamento IPv6 é composto por 32 símbolos hexadecimais (ou 128 *bits*) separados por uma coluna, cujo símbolo utilizado é o "dois pontos" (:). A figura 2.3 mostra a representação de um endereço IPv6 qualquer e a relação com os respectivos *bits*.

Figura 2.3 – Exemplo de endereço IPv6 e seus relativos *bits*.

Fonte: Autoria própria.

Os endereços podem ser utilizados na seguinte faixa:

- de 0000:0000:0000:0000:0000:0000:0000:0000
- até FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

As máscaras, utilizadas no IPv4, por definição agora são chamadas de *prefix-length*. E sua capacidade, antes de 0 à 32, agora acompanha a quantidade de *bits* do novo endereço, de 0 à 128.

Tal quantidade de *bits* permite que o IPv6 possa endereçar 340 undecilhões de endereços.

O IPv6 possui a possibilidade de omitir zeros do endereço, o que facilita no momento de tratar um endereço. Tal característica serve tanto para zeros em um único segmento quanto para a abrangência de vários segmentos. Para simbolizar essa ação utiliza-se a "coluna dupla" (::).

Exemplos de omissão de zeros:

- 2001:0ba0:0000:0000:0000:0000:0000:0000
  - 2001:ba0:: → (com coluna dupla)
- 2001:0ba0:0000:0000:0000:0000:0000:1234
  - 2001:ba0:0:0:0:0: → 0:1234 (sem coluna dupla)
  - 2001:ba0::1234 → (com coluna dupla)

Entretanto, a omissão de zeros possui algumas restrições. Em cada um dos 8 segmentos apenas os zeros à esquerda podem ser omitidos, pois se os da direita também tivessem essa capacidade poderia ocorrer ambiguidade no endereço.

O usuário deve ficar atento para não omitir os zeros à direita, caso contrário o endereço será interpretado de maneira errada.

Exemplo de possível ambiguidade com omissão zeros:

- 2001:ba::
  - → 2001:0ba0::
  - → 2001:00ba::
  - → 2001:ba00::

Outra relação de ambiguidade possível ocorreria caso a coluna dupla fosse inserida mais de uma vez no meio do endereço. Portanto, permite-se que ela seja usada apenas uma vez.

Exemplo de possível ambiguidade de dupla coluna:

- 2001:0d02::0014::0095
  - → 2001:0d02:0000:0000:0014:0000:0000:0095
  - → 2001:0d02:0000:0000:0000:0014:0000:0095
  - → 2001:0d02:0000:0014:0000:0000:0000:0095

Os endereços reservados para documentações são os da rede 2001:db8::/32 (HUSTON; LORD; SMITH, 2004). As informações completas sobre endereços reservados podem ser encontradas na RFC 5156 (BLANCHET, 2008).

Para o IPv6 não há utilização de *broadcast*, portanto não há endereço reservado para esta funcionalidade.

2.4.3. Endereço Link-local

O endereço *link-local* é usado no endereçamento de um *link* único como modo automático de configuração de endereço. Os roteadores não devem encaminhar pacotes com *link-local* como origem ou destino para outros *links*.

Esses endereços são compostos pelo prefixo fe80::/64 somado com o endereço MAC (*Media Access Control*) do equipamento, porém sua parte final também pode ser gerada através de uma sequência aleatória.

Esse processo é derivado do modo de configuração EUI-64 (*Extended Unique*

Identifier 64 bit) formalizado pelo IEEE (*Institute of Electrical and Electronics Engineers*). Além disso, o endereço recebe a sequência "fffe" inserida entre o terceiro e o quarto *bytes* do endereço MAC.

Exemplo de formação automática de endereço *link-local*:

- Endereço MAC: 00:04:df:32:0e:79
    - Endereço *link-local* → fe80::204:dfff:fe32:e79/64

No exemplo acima, no primeiro *byte* do endereço MAC (00) o sétimo *bit* recebe um complemento. No caso, o primeiro *byte* é 0x00 (0000 0000), e com o complemento torna-se 0x02 (0000 0010). Por esse motivo, o endereço que aparece no *link-local* contém os valores "02:04:df:32:0e:79".

2.4.4. Boas Práticas

O IPv6 proporciona a utilização do ID (*Identification Document*) da VLAN (*Virtual Local Area Network*) no meio do endereço, o que pode ser muito útil para acompanhar e documentar a rede em questão. Por exemplo, usando a VLAN 201, pode-se ter o endereço de rede: 2001:DB8:201::/64.

Outra boa prática é adicionar o endereço *loopback* IPv4 à *loopback* IPv6. Por exemplo, considerando o endereço 2001:DB8::/64 para *loopbacks*, supondo que a *loopback* IPv4 de um roteador R1 seja 1.1.1.1/32, poderia ser usado o endereço 2001:DB8:0:0:1:1:1:1/128 como *loopback* IPv6. Isso torna as coisas mais consistentes e visíveis na tabela de roteamento.

Alguns prefixos são utilizados nas redes IPv6 de acordo com a necessidade do cliente. Porém quando é feita uma solicitação de endereços, é entregue um bloco apropriado. Por exemplo, se solicitada uma faixa de endereços IPv6 ao órgão brasileiro responsável pela distribuição, no mínimo o solicitante receberá uma faixa /64. Se houver necessidade, uma faixa maior de endereços pode ser fornecida, estando sujeito a um custo maior e contanto que a necessidade seja justificada (MOREIRAS, 2011).

Prefixos comumente utilizados:

- /64 – Para servidores, clientes, etc.
- /127 – Para *links point-to-point* (deve-se atentar para um possível conflito com *anycast*).
- /128 – Para endereços *loopback*.

2.5. TRANSIÇÃO DO IPV4 PARA O IPV6

Para entendimento sobre o melhor método de transição do IPv4 para o IPv6, é necessário conhecer as técnicas existentes para essa troca de protocolo.

Com a situação que a Internet se encontra, não é possível trocar um protocolo pelo outro de maneira rápida e eficiente, pois a dependência do IPv4 ainda é grande e parte considerável dos equipamentos ativos na atualidade não está preparada para receber o IPv6. Por isso foi definido um período de transição, assim as empresas que dependem do serviço teriam tempo para adaptar seus produtos, possibilitando a utilização do IPv6.

O problema é que esse período de transição não foi seguido seriamente,

acarretando um enorme atraso na implantação do IPv6 em todo o mundo.

Segundo Huston (2008), a transição deveria estar em vias de conclusão no período entre 2006 e 2009, conforme ilustra a figura 2.4.

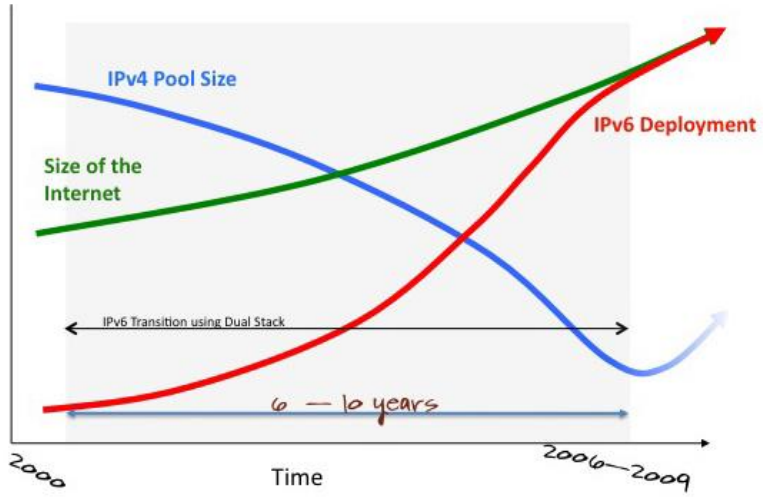

Figura 2.4 – Transição planejada.

Fonte: Huston (2008).

Através da figura 2.4 pode-se notar que a implantação do IPv6 deveria atingir sua plenitude no ano de 2009, quando estaria completamente compatível com a Internet. Enquanto isso a utilização do IPv4 cairia, permitindo que vários endereços fossem então liberados para uso, quando necessário.

Porém a realidade do IPv6 no ano corrente da publicação de Huston era completamente diferente. A implantação não foi desenvolvida conforme a previsão. Tal estado pode ser observado na figura 2.5.

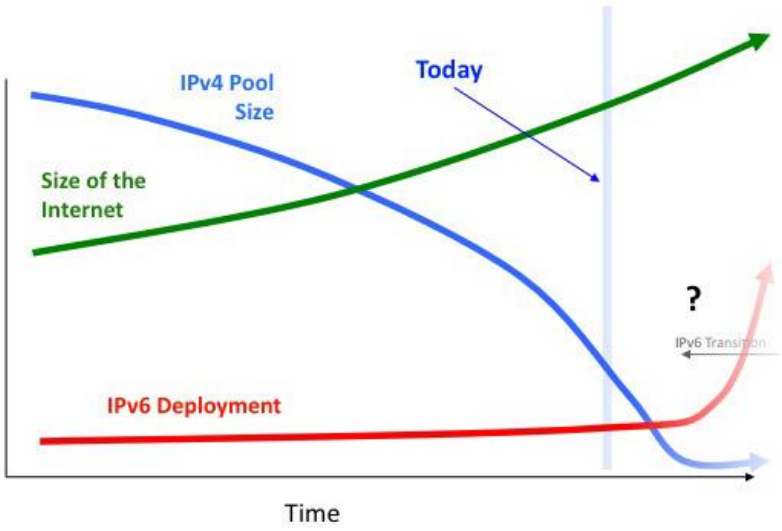

Figura 2.5 – Transição real.

Fonte: Huston (2008).

Através da figura 2.5 o atraso da transição é facilmente percebido. A implantação do IPv6 estava longe do que deveria ocorrer, além disso mostrava um índice preocupante, afinal o protocolo não dava mostras de que seria utilizado nos próximos anos, e em contrapartida a quantidade disponível de endereços IPv4 reduzia e se aproximava do esgotamento total.

Quatro anos mais tarde, Huston publicou outro artigo que trata do mesmo tema (HUSTON, 2012), e o resultado não foi muito diferente, a implantação continuava atrasada. Porém a figura 2.6 mostra que houve uma sensível melhora na utilização do IPv6. Mesmo assim Huston reconhecia que a implantação não acontecera da maneira prevista, e que na época era extremamente difícil prever o andamento da implantação em larga escala.

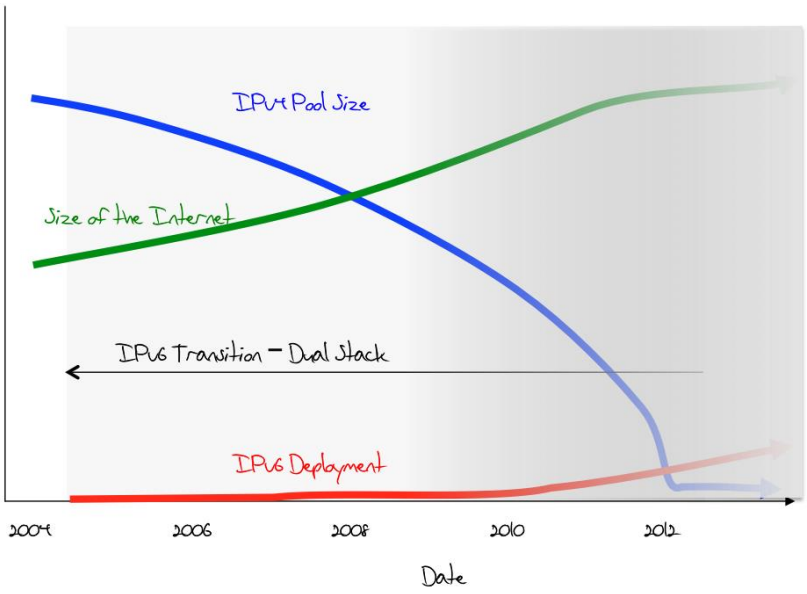

Figura 2.6 – Implantação em 2012.

Fonte: Huston (2012).

Existem várias técnicas para realizar a transição dos protocolos. Cada uma delas pode ser indicada para um determinado caso, e todas com o mesmo objetivo. Basicamente existem três categorias de técnicas de transição:

1. *Dual Stack* – Garante o suporte para IPv4 e IPv6 no mesmo dispositivo;
2. Túneis – Possibilita trafegar IPv6 em uma rede puramente IPv4.
3. Tradução – Permite a comunicação entre dispositivos que utilizam o IPv4 com dispositivos que utilizam o IPv6.

A seguir, algumas das principais técnicas são explicadas, com ênfase nos dois métodos escolhidos para este trabalho, 6over4 e *dual stack*. A tradução não está descrita em detalhes porque não é um método recomendado para transição (FRANKEL et al, 2010).

2.5.1. *Dual Stack*

O *dual stack* é, talvez, o principal método de transição entre todos os existentes. Esta técnica permite que a transição seja mais suave para a rede, pois garante que os serviços com suporte IPv4 continuem funcionando até a migração total para o IPv6, ao mesmo passo que os *hosts* que suportam IPv6 já possam utilizá-lo na rede (SANTOS, 2010).

Para o usuário comum, o serviço deve ser transparente, visto que o IPv4 continuará rodando normalmente para aplicações que dependam dele ou para usuários que não possuem infraestrutura adequada para a nova geração de IPs.

Conforme a necessidade de utilização do IPv4 diminuir, o protocolo pode ser desabilitado nos nós que o utilizam.

Uma das principais vantagens do *dual stack* é que o IPv4 e o IPv6 rodam em pilhas separadas. Sendo assim, as falhas de uma pilha não devem interferir diretamente na outra. A figura 2.7 ilustra uma situação com as duas pilhas rodando paralelamente no mesmo equipamento.

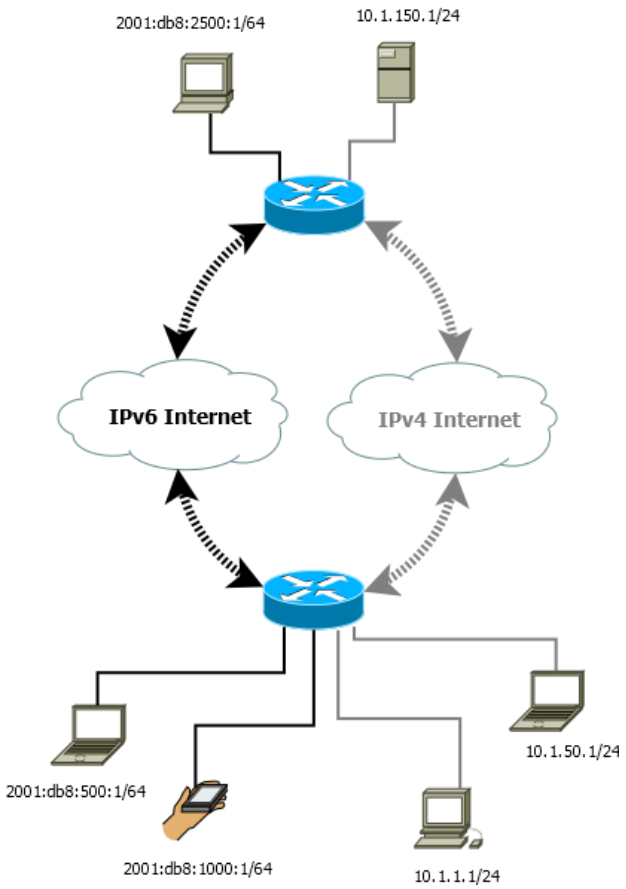

Figura 2.7 – Exemplo visual do *dual stack*.

Fonte: Autoria própria.

Assim como qualquer técnica de transição, o *dual stack* possui também desvantagens. Com o fato de habilitar as duas pilhas em um equipamento, é fácil imaginar

uma desvantagem desse método em relação ao consumo de recursos de hardware. O *dual stack* consome mais memória e processamento de um equipamento. Esse problema pode causar impacto em alguns casos específicos, por exemplo, supondo que um roteador, que trabalha com toda a tabela BGP IPv4 existente, algo perto de 500.000 rotas (BATES; SMITH; HUSTON, 2014), ou instâncias de OSPF com muitos LSAs (*Link State Advertisements*) e rotas, ou ainda serviços MPLS, todos rodando unicamente sobre IPv4, e então os mesmos serviços para IPv6 são habilitados em um determinado momento. Nesse caso é provável que haja aumento considerável do consumo de recursos no equipamento em questão, que por sua vez pode sofrer por conta de problemas como *overload* de CPU ou falta de memória no sistema.

Além do consumo de recursos, o operador terá que arcar com possíveis custos de novos equipamentos que suportem a pilha dupla, e também executar a análise de outros recursos que também deverão se adaptar à nova rede, como servidores, sistemas operacionais, e *firewalls*.

Para equipamentos mais próximos do *core* metropolitano podem ser necessários roteadores com protocolos específicos para IPv6, como o OSPFv3 (*Open Shortest Path First version 3*), ou que suportem a pilha dupla, como é o caso de BGP e IS-IS. Para utilização em pequenas redes o RIPng (*Routing Information Protocol next generation*) pode ser interessante.

Como o *dual stack* é considerado o método mais direto para a transição, possíveis ataques podem se tornar motivo de grande preocupação para os próximos anos. Inclusive, existe um *worm* chamado “IPv4-IPv6 dual stack worm”, o qual pode detectar vítimas em redes IPv4 e IPv6 (LIU et al, 2009).

2.5.2. *6over4*

O *6over4* é um dos métodos de transição que representa o tunelamento. O protocolo é responsável por transitar IPv6 em uma rede IPv4. A nomenclatura utilizada para o túnel propriamente dito é *6in4*, portanto o nome *6over4* está restrito para referenciar ao método de transição (PALET, 2005).

Para a implantação do *6over4* é necessário que os roteadores de borda possuam a capacidade de tunelamento para encapsular e desencapsular pacotes da rede. Esses roteadores fazem uma “ponte” entre redes IPv6 por redes IPv4, como ilustrado na figura 2.8.

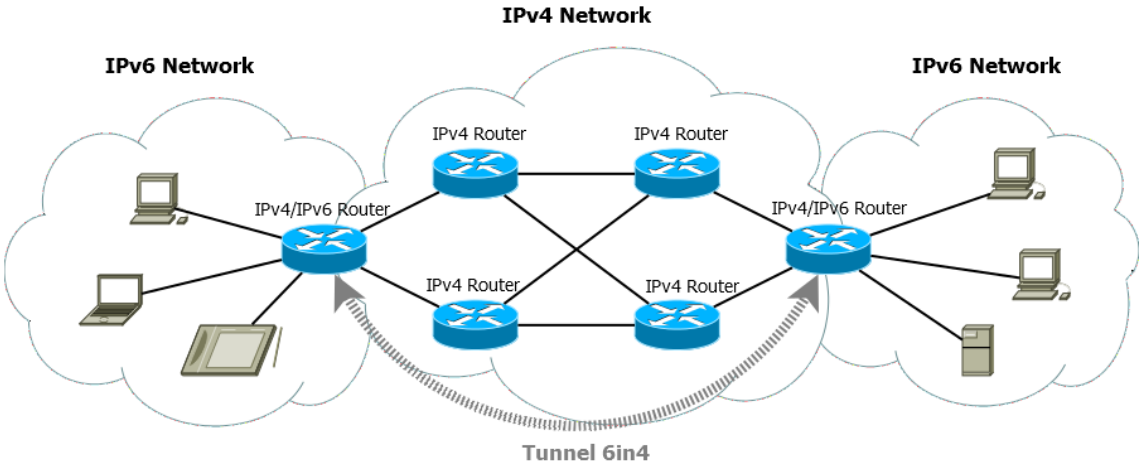

Figura 2.8 – Exemplo de representação do tunelamento *6over4*.

Fonte: Autoria própria.

Os roteadores que fazem o encapsulamento são chamados de *end-points*. Os *end-points* adicionam ao pacote original IPv6 um cabeçalho IPv4 para que o conteúdo possa chegar ao seu destino através de uma rede puramente IPv4. Para identificar o tipo do pacote, o mecanismo utiliza o protocolo do tipo 41 (CARPENTER; MOORE, 2001).

O *6over4* não é largamente implantando devido à sua dependência do *multicast* do IPv4. Entretando pode ser uma boa alternativa para pequenas redes que possuam *core* puramente IPv4 até que uma solução completa IPv6 seja implantada.

Algumas medidas de segurança devem ser consideradas para a implantação e utilização do *6over4* (FRANKEL et al, 2010):

- É necessário padronizar os controles de defesa tanto de IPv6 quanto de IPv4;
- Os roteadores que fazem a fronteira entre as redes IPv4 e IPv6 necessitam de regras de filtros para o protocolo 41, bloqueando os pacotes de fontes não confiáveis. É necessário também filtros para pacotes *multicast*;
- Pacotes IPv6 com *hop limit* no valor 255 não devem ser tratados como pacotes gerados localmente;
- Caso seja desejável a utilização do IPsec, é melhor que este rode no domínio IPv6.

2.5.3. Demais Métodos de Tunelamento

Os demais métodos de tunelamento estão dispostos abaixo (FRANKEL et al, 2010). As vantagens e desvantagens de cada método não são explicadas nesse trabalho visto que estas podem variar de acordo com a necessidade do cenário. Além disso, os equipamentos utilizados para os testes práticos possuem exclusivamente as funcionalidades *dual stack* e *6over4*.

- *6to4* e *6rd*

  O *6to4* (*IPv6 to IPv4*) é utilizado para conectar *sites* IPv6 por meio de redes IPv4, porém não deve ser confundido com o *6over4*. O *6to4* é um endereço IPv4 mapeado no endereço IPv6. O prefixo IPv6 utilizado deve estar na faixa 2002::/16, a qual é uma faixa reservada apenas para esse tipo de endereço. A representação

do endereço, entretanto, deve ser aplicada da seguinte forma (definida pela RFC 3056) 2002:A.B.C.D::/48, sendo "A.B.C.D" um endereço IPv4 público. A ideia do *6rd* (IPv6 *rapid deployment*) é a mesma do *6to4*, porém com endereços de provedores.

- ISATAP

  O ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*), ao contrário do *6over4*, não necessita de IPv4 *multicast*, porém precisa que os *hosts* sejam *dual stack*. O ISATAP permite que o tráfego percorra uma rede apenas com IPv4. Os túneis são construídos de maneira automática.

- Teredo

  Este protocolo foi desenvolvido pela Microsoft como solução para o problema de *hosts* que ficam atrás de NATs. O protocolo ISATAP resolve a questão da necessidade de *multicast* para o *6over4*, bem como o caso de endereços públicos para o *6to4*, porém não atravessa NATs. Essa tecnologia deve ser utilizada apenas em último caso, pois gera maior *overhead* que os demais protocolos.

- *Tunnel Brokers*

  Esta técnica proporciona o *dual stack* para nós em redes IPv4. O método requer a implantação de um servidor *tunnel broker*. O *tunnel broker* gerencia túneis entre clientes e *tunnel servers*. O método não funciona para clientes atrás de NATs. A conexão com o cliente normalmente é feita via HTTP.

- DSTM

  O DSTM (*Dual Stack Transition Mechanism*) tem por objetivo possibilitar que uma rede utilize o IPv6 no *core*, e que o IPv4 rode em túneis sobre o IPv6, ou seja, o contrário dos métodos citados anteriormente. Sua importância se dá considerando que o IPv6 se torne globalmente predominante, e quando fosse necessário transitar IPv4 sobre essas redes o DSTM auxiliaria.

- CGN e *Dual Stack Lite*

  O CGN (*Carrier Grade NAT*) é uma estratégia com objetivo de ajudar provedores para uma situação na qual não haja mais endereços IPv4 roteáveis disponíveis para os *sites* dos usuários. O CGN permite algumas possibilidades, como um "NAT duplo" (IPv4 → IPv4 → IPv4), que constitui mais uma camada de NAT, deixando para o cliente uma rede não roteável, por exemplo 10.0.0.0/8. A segunda estratégia seria alterando o tipo de IP duas vezes (IPv4 → IPv6 → IPv4). É ainda possível um método que consiste em rodar um túnel IPv4 sobre IPv6 entre o CGN e o *gateway* do cliente, chamado de *dual stack lite*. E, por fim, uma quarta opção é trabalhar a melhoria do *dual stack lite* tratando porções de portas como extensões dos endereços IPv4.

3. COMPARATIVO ENTRE *DUAL STACK* E *6OVER4*

Neste capítulo é feita uma comparação da implantação do IPv6 através dos métodos *6over4* e *dual stack*, do ponto de vista prático, através de medidas de *jitter*, latência, tempo de convergência de tráfego e medidas de memória RAM e utilização de CPU.

Os dois métodos em questão foram escolhidos porque aplicam as duas principais técnicas de transição, o próprio *dual stack*, e o tunelamento, este representado pelo *6over4*, e estão disponíveis nos equipamentos utilizados no comparativo.

O *6over4*, por depender de *multicast* é indicado basicamente para redes internas e dificilmente será utilizado abertamente na Internet. Já o *dual stack* pode trabalhar nas redes da Internet, porém sua escolha se fez para exemplificar sua aplicação também em ambiente fechado, visando à utilização de um mesmo cenário representativo para ambos os métodos.

O objetivo do comparativo é mostrar que a implantação do *dual stack* é pertinente para o andamento da transição de IPv4 para IPv6. A motivação para aplicação dessa atividade é o atraso da transição, conforme explicado no capítulo 2.5.

3.1. TOPOLOGIA DE TESTES

A topologia de testes foi escolhida para atender um cenário que pudesse abranger medidas de convergência de tráfego, *jitter* e latência, além de consumo de memória RAM e utilização de CPU.

Para garantir a convergência natural do tráfego, foi escolhido o protocolo de roteamento dinâmico OSPF, que envolve um anel com 4 elementos, possibilitando convergência através de teste de queda de *link*. O cenário OSPF é mostrado na figura 3.1.

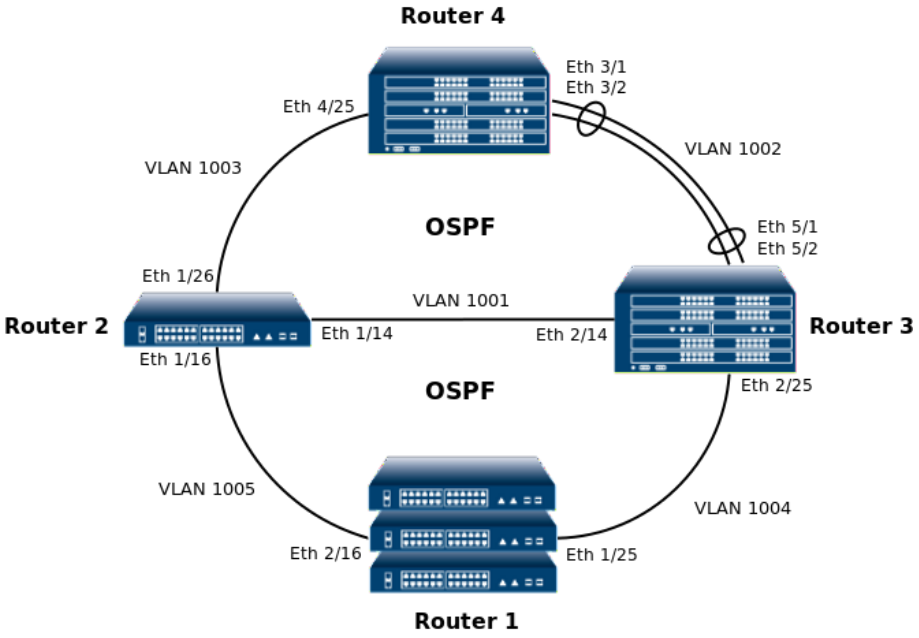

Figura 3.1 – Equipamentos em anel com protocolo OSPF.

Fonte: Autoria própria.

Além disso, há no cenário também uma linha com 3 elementos (sendo que um deles também faz parte do anel OSPF) rodando o protocolo de borda BGP, conforme ilustrado na figura 3.2.

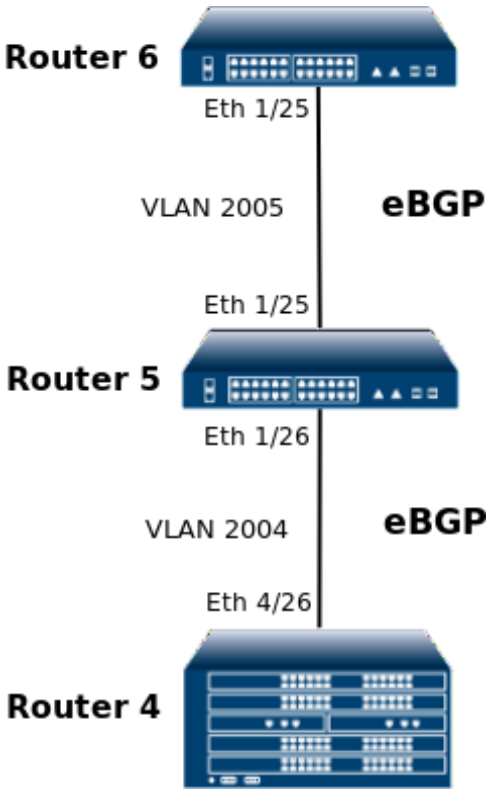

Figura 3.2 – Equipamentos em linha com protocolo BGP.

Fonte: Autoria própria.

O cenário completo, figura 3.3, vale integralmente para os testes de *6over4* e *dual stack*.

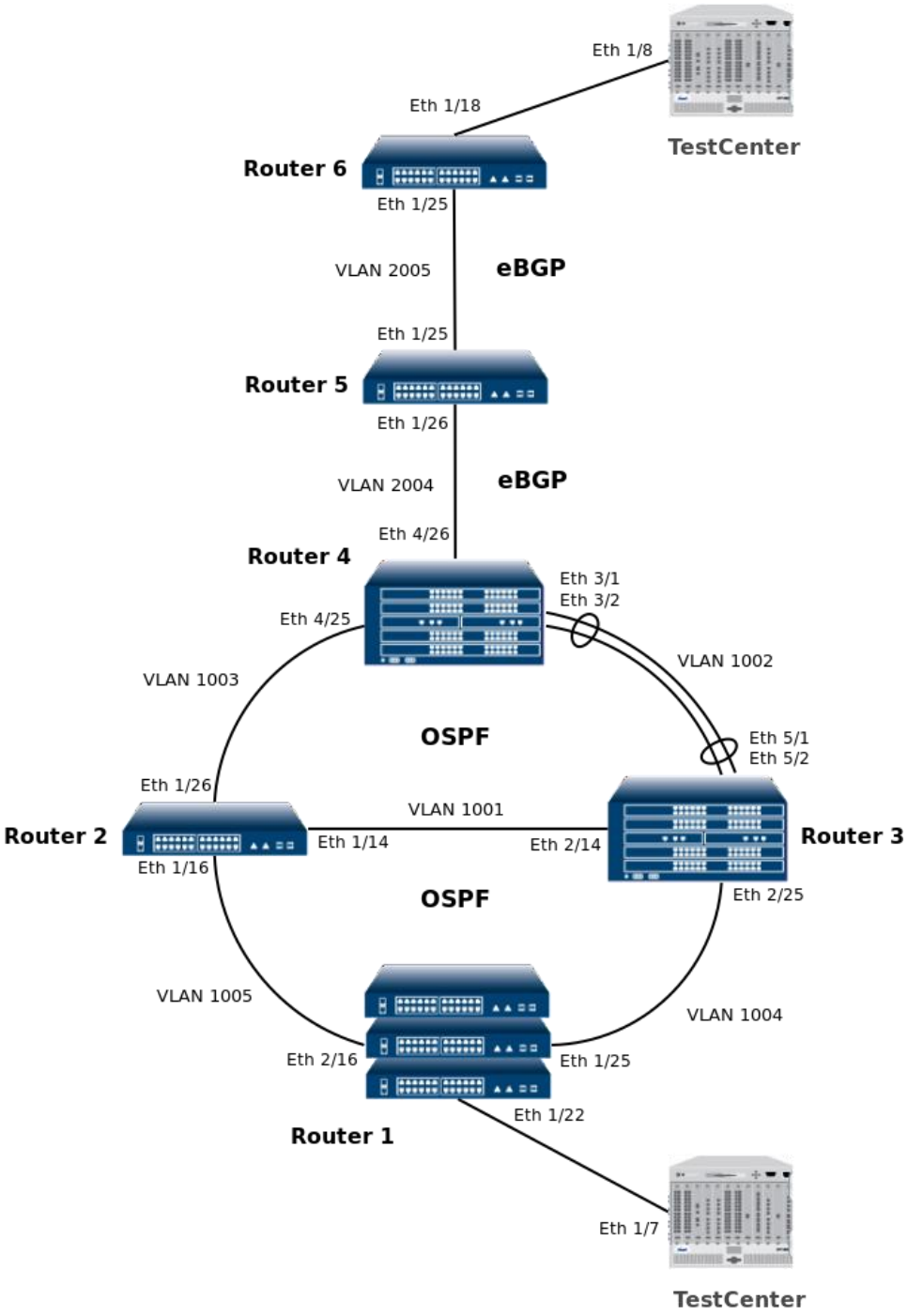

Figura 3.3 – Cenário completo com protocolos OSPF e BGP

Fonte: Autoria própria.

3.1.1. Equipamentos Utilizados

Os equipamentos utilizados no cenário descrito na figura 3.3 foram todos fornecidos pela empresa brasileira Datacom, a qual produz os roteadores utilizados nos testes. Já o *test center* é fabricado pela americana Spirent. Abaixo segue a lista de equipamentos, de acordo com a nomenclatura utilizada nas figuras 3.1, 3.2 e 3.3.

- Router 1: *Stacking* composto de três roteadores da linha 4100, nas seguintes configurações:

    - Unidade 1: ETH20GT+4GC+2XX;
    - Unidade 2: ETH24GX+2XX;
    - Unidade 3: ETH24GX+2XX.

- Router 2: Roteador *standalone*, linha 4100, ETH24GX+2XX;

- Router 3: Roteador da linha 4000, modelo 4004, nas seguintes configurações:
    - Unidade 1: MPU384;
    - Unidade 2: ETH24GX+2x10GX H Series;
    - Unidade 4: ETH24GX+2x10GX H Series;
    - Unidade 5: ETH2x10GX H Series.

- Router 4: Roteador da linha 4000, modelo 4004, nas seguintes configurações:
    - Unidade 1-A: MPU384;
    - Unidade 1-B: MPU384;
    - Unidade 3: ETH2x10GX H Series.
    - Unidade 4: ETH24GX+2x10GX H Series.

- Router 5: Roteador *standalone*, linha 4000, modelo 4001 ETH24GX+2x10GX H Series.

- Router 6: Roteador *standalone*, linha 4000, modelo 4001 ETH24GX+2x10GX H Series.

- TestCenter: *Test center* Spirent, modelo N11U, placa CM1G D12 de 12 portas.

3.2. APLICAÇÃO DO *6OVER4*

A aplicação do cenário *6over4* foi feita com a configuração de oito túneis *6in4*, sendo cada um deles responsável por transmitir *streams* de dez redes diferentes, o que dá um total de oitenta *streams* de tráfego gerados pelo equipamento *test center*.

Cada *stream* de tráfego foi gerado com 10 Mbps, com origem e destino para as duas portas do *test center*, no caso as portas Eth 1/7 e Eth 1/8 do cenário representado pela figura 3.3, totalizando 800 Mbps de tráfego bidirecional no cenário. Como cada porta possui no mínimo 1 Gbps *full duplex* de velocidade nos *links*, não houve sobrecarga ou descarte de pacotes durante o período de estabilidade do cenário.

3.2.1. Configurações do *6over4*

Este item traz os comandos necessários apenas para entender a ativação do *6over4*. É aqui abordado o mínimo possível de configuração considerável para que o tráfego vá de sua origem ao seu destino. Para que isso seja possível, são ilustradas em quadro as configurações do equipamento Router 1.

O quadro 3.1 retrata a lista de comandos para a configuração de Router 1. A representação de duas barras (“//”) diz respeito aos comentários nas configurações.

```
// Configuração 1
router ospf
 router-id 10.100.1.1
 network 10.10.5.0/24 area 0
 network 10.10.4.0/24 area 0
 redistribute connected
 log-adjacency-changes
!
interface vlan 1004
 ip address 10.10.4.2/24
 ip ospf network point-to-point
 set-member tagged ethernet 1/25
!
interface vlan 1005
 ip address 10.10.5.2/24
 ip ospf network point-to-point
 set-member tagged port-channel 3
!
// Configuração 2
interface vlan 3100
 ipv6 enable
 ipv6 address 2001:db8:0:3100::1/64
 set-member tagged ethernet 1/22
!
// Configuração 3
interface ip-tunnel 1
 ipv6 address 2001:db8::10.99.1.0/128
 tunnel source interface loopback 0
 tunnel destination ip-address 10.99.2.0
 tunnel type ipv6ip
!
// Configuração 4
interface loopback 0
 ip address 10.99.1.0/32
!
// Configuração 5
ipv6 route 2001:db8:0:100::/64 ip-tunnel 1
ipv6 route 2001:db8:7:179::/64 ip-tunnel 8
```

Quadro 3.1 – Configurações de Router 1 no cenário *6over4*.

Fonte: Autoria própria.

- Configuração 1: É a configuração necessária para estabelecer as vizinhanças OSPF com Router 2 e Router 3. Através dessa configuração é possível ensinar e aprender rotas das redes de todo o cenário, inclusive os endereços *loopbacks*, os quais serão utilizados como destinos e origens na configuração dos túneis *6in4*;

- Configuração 2: É a configuração da primeira VLAN de Router 1, dentre as oitenta, que fazem parte dos *streams* do cenário. Em Router 1 as VLANs estão na faixa 3100-3179, já em Router 6 na faixa 100-179. O endereço IPv6 é composto pelo prefixo 2001:db8, seguido de um número entre zero e sete, os quais estão dispostos de maneira que cada um desses números seja relativo à um túnel, em seguida vem o valor do ID da VLAN e por último a identificação do *host*, sendo que nos roteadores todos os *hosts* possuem final 1. Por exemplo, o endereço "2001:db8:0:3100::1/64" pertence ao Roteador 1, túnel 1 e VLAN 3100;

- Configuração 3: É a composição das configurações do primeiro túnel, de um total de oito. É necessário configurar um endereço IPv6 para identificação no túnel, um endereço de origem, um endereço de destino e o tipo de túnel. Os endereços de origem e destino são *loopbacks* IPv4;

- Configuração 4: Configuração das *loopbacks*. São ao todo oito (0 à 7) em cada roteador, sendo que as origens e destinos dos túneis estão configuradas em ordem entre os roteadores, por exemplo, a *loopback* 0 de Router 1 é a origem do túnel, e o destino é a *loopback* 0 de Router 6, e assim sucessivamente até a *loopback* 7.

- Configuração 5: Retrata a configuração das rotas estáticas. Em Router 1 existem oitenta rotas estáticas para as redes de Router 6, considerando o critério citado no início do capítulo: dez redes para cada túnel. O quadro 3.1 possui duas rotas, a primeira e a última criadas para atingir as redes IPv6 de Router 6.

3.2.2. Testes e Medidas Com o *6over4*

Este item aborda algumas medições feitas no cenário, são elas: medidas de *jitter*, latência e tempo de convergência de tráfego, além de utilização de memória RAM e consumo de CPU. As medidas de convergência de trafégo são referentes à testes de *reboot* de equipamento, *flap* de protocolo de roteamento e queda de *link.*

O equipamento *test center* consegue fazer por conta própria as medidas de *jitter* e latência durante a passagem de tráfego pela rede. O *throughput* do tráfego durante os testes foi de 800 Mbps em ambos os sentidos (Router 1 ↔ Router 6).

A figura 3.4 ilustra as seguintes medidas de *jitter*: *jitter* médio a curto prazo (medido em janela), *jitter* médio, *jitter* médio absoluto, o qual é a diferença de tempo de chegada de dois pacotes enviados consecutivamente e pertencentes ao mesmo *stream* (PERSER et al, 2006), *jitter* mínimo e *jitter* máximo, respectivamente. A imagem em questão possui informações de tráfego dos dois sentidos do cenário, a primeira parte (de cima) representa o tráfego no sentido Router 1→Router 6, e a segunda parte o sentido inverso.

Short Term Avg Jitter (us)	Avg Jitter (us)	RFC4689 Absolute Avg Jitter (us)	Min Jitter (us)	Max Jitter (us)
0.29	0.29	0.29	0.01	1.24
0.3	0.29	0.29	0.01	1.21
0.3	0.29	0.29	0.03	1.83
0.3	0.29	0.29	0.01	1.33
0.3	0.29	0.29	0.01	1.29
0.3	0.29	0.29	0.01	1.29
0.31	0.29	0.29	0.02	1.27
0.31	0.29	0.29	0.02	1.29
0.31	0.29	0.29	0.02	1.8
0.3	0.29	0.29	0.02	1.34

Short Term Avg Jitter (us)	Avg Jitter (us)	RFC4689 Absolute Avg Jitter (us)	Min Jitter (us)	Max Jitter (us)
0.3	0.3	0.3	0	1.39
0.3	0.3	0.3	0.02	1.36
0.3	0.3	0.3	0.03	1.36
0.3	0.3	0.3	0.03	1.38
0.3	0.3	0.3	0.03	1.44
0.3	0.3	0.3	0.03	1.43
0.3	0.3	0.3	0.02	1.84
0.3	0.3	0.3	0.03	1.43
0.3	0.3	0.3	0.03	1.39
0.3	0.3	0.3	0.03	0.96

Figura 3.4 – Medidas de *jitter* no cenário *6over4*.

Fonte: Autoria própria.

A figura 3.5 mostra as medidas de latência do tráfego, em sua transmissão constante. As medidas são as seguintes: latência média a curto prazo, latência média, latência mínima e latência máxima, respectivamente. A imagem em questão está divida em duas partes, a primeira delas, a metade de cima, mostra dez *streams* de tráfego no sentido Router 1→Router 6, já a segunda metade mostra dez *streams* de tráfego no sentido inverso.

Short Term Avg Latency (us)	Avg Latency (us)	Min Latency (us)	Max Latency (us)
18.22	17.22	15.66	154.75
18.22	17.22	15.76	154.96
18.22	17.22	15.74	154.72
18.22	17.22	15.8	154.91
18.22	17.22	15.79	154.77
18.22	17.22	15.75	154.81
18.22	17.22	15.78	154.72
18.22	17.22	15.75	154.59
18.22	17.22	15.77	154.63
18.21	17.22	15.74	154.84

Short Term Avg Latency (us)	Avg Latency (us)	Min Latency (us)	Max Latency (us)
17.75	17.36	15.75	16.357.04
17.75	17.38	15.78	15.695.89
17.75	17.13	15.81	31.35
17.75	17.33	15.71	14.276.05
17.75	17.3	15.8	12.831.25
17.75	17.23	15.74	9.856.37
17.75	17.13	15.81	31.35
17.75	17.13	15.78	563.17
17.75	17.13	15.8	560.62
17.75	17.13	15.77	561.43

Figura 3.5 – Medidas de latência no cenário *6over4*.

Fonte: Autoria própria.

O quadro 3.2 mostra a média entre as 20 medidas dos os *streams* do cenário. As medidas foram realizadas na porta Eth 1/7 do *test center*. O objetivo de registrar essas marcas é ter informações sobre as medições feitas no cenário como um todo.

***Streams* Medidos**	20
Média de Latência média a curto prazo	17,985 µs
Média de Latência Média	17,223 µs
Média de Latência Mínima	15,765µs
Média de Latência Máxima	3615,661µs
Média de *Jitter* médio a curto prazo	0,301 µs
Média de *Jitter* Médio	0.295 µs
Média de *Jitter* médio absoluto (RFC 4689)	0.295 µs
Média de *Jitter* Mínimo	0,0205 µs
Média de *Jitter* Máximo	1,3255 µs

Quadro 3.2 – Médias de *jitter* e latência no cenário *6over4*.

Fonte: Autoria própria.

Alguns testes de falha de cenário foram realizados com o intuito de perceber o tempo de recuperação do sistema. Tais testes foram validados considerando queda de *link*, oscilação do protocolo de roteamento e *reboot* de um equipamento.

A queda de *link* foi simulada executando o comando *shutdown* na interface 1/26 de Router 2, pois esse *link* faz parte do caminho principal do tráfego, e sua queda obriga a convergência para outro caminho. O caminho pelo qual o tráfego foi retomado passou a ser pelo próprio Router 2, porém através da VLAN 1001, via interface 1/14.

A oscilação do protocolo de roteamento foi simulada executando um *flap* no protocolo OSPF em Router 4. Este equipamento foi escolhido para execução do *flap* para garantir que a convergência não ocorresse, forçando a queda total de tráfego. Assim foi possível medir o tempo que o equipamento demora para subir novamente o protocolo e voltar a passar tráfego.

O mesmo ocorre para o teste de *reboot*, também executado em Router 4, para garantir que não houvesse convergência de tráfego, pois o objetivo deste teste foi verificar quanto tempo o roteador demora para subir, aplicar todas as configurações e voltar a transmitir tráfego corretamente.

Todos os testes foram realizados com três medidas, e então um tempo médio foi registrado, para garantir integridade no modo de medição.

A tabela 3.1 demonstra os testes e tempos de retomada de tráfego após cada execução.

Tabela 3.1 – Medidas de tempo de recuperação no cenário *6over4*.

Ação	Equipamento	Tempo 1	Tempo 2	Tempo 3	Tempo Médio
Shutdown	Router 2 Porta 1/26	00:05,584	00:05,804	00:06,324	00:05,904
No Shutdown	Router 2 Porta 1/26	00:03,041	00:02,921	00:03,063	00:03,008
Flap do OSPF	Router 4	00:25,492	00:25,083	00:25,008	00:25,194
Reboot de Eqto. Intermediário	Router 5	02:26,889	02:29,414	02:28,332	02:28,212

Fonte: Autoria própria.

3.2.3. Utilização de Recursos do *6over4*

A utilização de recursos de hardware considerou, assim como para os testes do *dual stack*, a medida de utilização de CPU e memória RAM durante um período de cinco minutos de estabilidade do sistema, com o volume de tráfego de 800 Mbps.

A tabela 3.2 mostra informações sobre os recursos utilizados. Nela é possível notar os equipamentos e suas medidas médias na seguinte ordem: utilização total da CPU, utilização da CPU pelo processo gerenciador de IPv6 (RADVD), consumo total de memória RAM e consumo de memória pelo processo gerenciador de IPv6.

Tabela 3.2 – Utilização de recursos no cenário *6over4*.

Equipamento	CPU (%)	RADVD CPU (%)	RAM (MB)	RADVD RAM (MB)
Router 1	19.5	1.5	579	0,836
Router 2	14.3	-	565	-
Router 3	7.6	-	693	-
Router 4	7.3	-	690	-
Router 5	10.8	-	589	-
Router 6	11.8	0.8	593	0,832

Fonte: Autoria própria.

3.3. APLICAÇÃO DO *DUAL STACK*

Para a aplicação do *dual stack*, o mesmo cenário do *6over4* foi mantido, não houve mudanças de *hardware* ou *links*.

Apenas alterações pontuais de configuração foram executadas. São elas:

- Remoção de todos os oito túneis presentes em Router 1 e Router 6;
- Remoção de todas as rotas estáticas IPv6 para as redes de Router 1 e Router 6;
- Adição de infra-estrutura IPv6 em todos os roteadores (endereços IPv6 nas VLANs);
- Adição do protocolo OSPFv3 em todos os roteadores que possuíam previamente o OSPFv2;
- Adição de vizinhança IPv6 nos roteadores que previamente possuiam o BGP.

Foram mantidas as oitenta VLANs conectadas ao *test center* (tanto em Router 1 quanto em Router 6), bem como seus respectivos endereços IPv6. Os *streams* de tráfego também se mantiveram os mesmos, de 800 Mbps no total.

3.3.1. Configurações do *Dual Dtack*

Este item é responsável por exibir o mínimo de comandos necessários para ativação do *dual stack* nos equipamentos. Ao contrário do método *6over4*, o qual é configurado apenas nos roteadores de borda, pois a infraesturura IPv4 é utilizada para transporte de dados, todos os roteadores do cenário precisam ter IPv6 e algum sistema para rotear as redes (nesse caso, o protocolo OSPF é utilizado).

Para o correto entendimento das configurações, os quadros 3.3 e 3.4 mostram as configurações principais de Router 1 e Router 4, respectivamente. Novamente, a representação de duas barras (“//”) diz respeito aos comentários nas configurações.

```
// Configuração 1
router ospf
 router-id 10.100.1.1
 network 10.10.5.0/24 area 0
 network 10.10.4.0/24 area 0
 redistribute connected
 log-adjacency-changes
!
```

```
router ospfv3
 router-id 10.100.1.1
 log-adjacency-changes
 redistribute connected
!
interface vlan 1004
 ip address 10.10.4.2/24
 ipv6 enable
 ipv6 address 2001:db8:1004::1/64
 ipv6 ospfv3 instance-id 0 area 0
 ipv6 ospfv3 network point-to-point
 ip ospf network point-to-point
 set-member tagged ethernet 1/25
!
interface vlan 1005
 ip address 10.10.5.2/24
 ipv6 enable
 ipv6 address 2001:db8:1005::1/64
 ipv6 ospfv3 instance-id 0 area 0
 ipv6 ospfv3 network point-to-point
 ip ospf network point-to-point
 set-member tagged port-channel 3
!
// Configuração 2
interface vlan 3100
 ipv6 enable
 ipv6 address 2001:db8:0:3100::1/64
 set-member tagged ethernet 1/22
!
```

Quadro 3.3 – Configurações de Router 1 no cenário *dual stack*.

Fonte: Autoria própria.

- Configuração 1: É a configuração necessária para estabelecer as vizinhanças OSPFv3 (versão exclusiva para IPv6). Diferente do OSPFv2, o protocolo roda por enlace, e não por redes, por isso não é necessário configuração da rede na árvore do OSPFv3. Basta que este seja ativado, de preferência com configuração de "router-id" para mais fácil identificação de vizinhos. A ativação do protocolo para um enlace específico é feita nas VLANs. Pelo quadro 3.2 é possível notar ainda que a configuração IPv4 e IPv6 são feitas paralelamente nas interfaces. Para o IPv6, é necessário configurar o ID da instância nas VLANs, bem como a área para divulgação das redes.

- Configuração 2: É um exemplo de configuração de VLAN com IPv6, na qual a interface está conectada ao *test center*. Essa configuração está presente também no quadro 3.1, pois VLAN de acesso foi um ponto que não sofreu alteração durante a configuração do *dual stack*.

O quadro 3.4 refere-se às configurações de Router 4. A escolha desse equipamento para contemplar o quadro abaixo foi devido ao fato de que este roteador faz a ponte entre o anel OSPF (versões 2 e 3) e BGP. Abaixo do quadro, há a explicação das configurações.

```
// Configuração 1
router ospf
 router-id 10.100.1.4
 network 10.10.3.0/24 area 0
 network 10.10.2.0/24 area 0
 network 10.20.4.0/24 area 0
 redistribute bgp
 log-adjacency-changes
!
router ospfv3
 router-id 10.100.1.4
 log-adjacency-changes
 redistribute connected
 redistribute bgp
!
router bgp 65531
 bgp log-neighbor-changes
 neighbor 10.20.4.2 remote-as 65532
 neighbor 2001:db8:2004::2 remote-as 65532
 redistribute ospf
!
interface vlan 1002
 ip address 10.10.2.2/24
 ipv6 enable
 ipv6 address 2001:db8:1002::2/64
 ipv6 ospfv3 instance-id 0 area 0
 ipv6 ospfv3 network point-to-point
 ip ospf network point-to-point
 set-member tagged port-channel 2
!
interface vlan 1003
 ip address 10.10.3.2/24
 ipv6 enable
 ipv6 address 2001:db8:1003::2/64
 ipv6 ospfv3 instance-id 0 area 0
 ipv6 ospfv3 network point-to-point
 ip ospf network point-to-point
 set-member tagged ethernet 4/25
!
interface vlan 2004
 ip address 10.20.4.1/24
 ipv6 enable
 ipv6 address 2001:db8:2004::1/64
 ip ospf network point-to-point
 set-member tagged ethernet 4/26
!
```

Quadro 3.4 – Configurações de Router 4 no cenário *dual stack*.

Fonte: Autoria própria.

- Configuração 1: A configuração OSPF é a mesma utilizada para os testes do *6over4*, possui as redes divulgadas na área 0, e configuração para redistribuição no OSPF das redes aprendidas via BGP; O OSPFv3 foi configurado para cumprir as mesmas funções de sua versão v2, divulgando para os vizinhos as rotas aprendidas via BGP; Em seguida aparece a configuração BGP IPv4 e IPv6, ambas com vizinhança para Router 5, além disso o BGP também redistribui para seu vizinho as rotas aprendidas via OSPF (versões 2 e 3). As VLANs 1002 e 1003 estão associadas aos OSPFs e a 2004 ao BGP.

3.3.2. Testes e Medidas Com o *Dual Stack*

São aqui abordados os mesmos testes e medições feitos com o *6over4*: *jitter*, latência, tempo de convergência de tráfego, utilização de memória RAM e consumo de CPU.

O *throughput* de tráfego de 800 Mbps nos dois os sentidos (Router 1↔Router 6) foi mantido para os testes e medidas com o *dual stack*.

A figura 3.6 ilustra uma lista com os mesmos tipos de medida exibidos na figura 3.4, porém as medições foram feitas com tráfego no cenário *dual stack*. As informações de *jitter* presentes na figura 3.6 estão divididas em duas partes, a primeira parte (de cima) representa o tráfego no sentido Router 1→Router 6, e a segunda parte o sentido inverso.

Short Term Avg Jitter (us)	Avg Jitter (us)	RFC4689 Absolute Avg Jitter (us)	Min Jitter (us)	Max Jitter (us)
0.31	0.29	0.29	0	1.3
0.31	0.29	0.29	0	1.5
0.31	0.29	0.29	0.01	1.5
0.3	0.29	0.29	0	1.29
0.29	0.29	0.29	0	1.55
0.29	0.29	0.29	0	1.75
0.29	0.29	0.29	0	1.49
0.29	0.29	0.29	0	1.75
0.28	0.29	0.29	0	1.78
0.28	0.29	0.29	0.01	1.85

Short Term Avg Jitter (us)	Avg Jitter (us)	RFC4689 Absolute Avg Jitter (us)	Min Jitter (us)	Max Jitter (us)
0.3	0.31	0.31	0.01	1.97
0.31	0.31	0.31	0.01	1.85
0.31	0.31	0.31	0.01	1.51
0.31	0.31	0.31	0.01	1.45
0.3	0.31	0.31	0.01	1.44
0.3	0.31	0.31	0.01	1.36
0.31	0.31	0.31	0.01	2.02
0.3	0.31	0.31	0.01	1.49
0.3	0.31	0.31	0.01	1.49
0.31	0.31	0.31	0.01	1.85

Figura 3.6 – Medidas de *jitter* no cenário *dual stack*.

Fonte: Autoria própria.

A figura 3.7 demonstra informações sobre as medidas de latência feitas durante testes com o cenário *dual stack*. Assim como na figura 3.6, a primeira lista (metade de cima) refere-se ao tráfego no sentido Router 1→Router 6, e a segunda parte (metade de baixo) sentido Router 6→Router 1.

Short Term Avg Latency (us)	Avg Latency (us)	Min Latency (us)	Max Latency (us)
16.86	16.86	15.78	18.04
16.86	16.86	15.81	18.09
16.86	16.86	15.8	18.29
16.86	16.86	15.76	18.26
16.86	16.86	15.78	17.97
16.86	16.86	15.78	18.09
16.86	16.86	15.8	18.37
16.86	16.86	15.8	18.32
16.86	16.86	15.77	18.57
16.85	16.86	15.77	18.28

Short Term Avg Latency (us)	Avg Latency (us)	Min Latency (us)	Max Latency (us)
16.87	16.87	15.83	18.68
16.87	16.87	15.81	18.47
16.87	16.87	15.8	18.29
16.87	16.87	15.82	18.04
16.86	16.87	15.81	18
16.87	16.87	15.81	18.53
16.87	16.87	15.82	18.62
16.87	16.87	15.8	18.33
16.87	16.87	15.8	18.44
16.87	16.87	15.82	18.73

Figura 3.7 – Medidas de latência no cenário *dual stack*.

Fonte: Autoria própria.

O quadro 3.5 demonstra a média entre as medidas dos 20 *streams* de tráfego. As medidas foram realizadas na porta Eth 1/7 do *test center*.

***Streams* Medidos**	20
Média de Latência média a curto prazo	16.864 µs
Média de Latência Média	16.865 µs
Média de Latência Mínima	15.7985 µs
Média de Latência Máxima	18,3205 µs
Média de *Jitter* médio a curto prazo	0,3 µs
Média de *Jitter* Médio	0.3 µs
Média de *Jitter* médio absoluto (RFC 4689)	0.3 µs
Média de *Jitter* Mínimo	0,006 µs
Média de *Jitter* Máximo	1,61 µs

Quadro 3.5 – Médias de *jitter* e latência no cério *dual stack*.

Fonte: Autoria própria.

Foram realizados os mesmos testes de falha do *6over4*, com o intuito de comparar os tempos de recuperação do sistema. Tais testes foram validados considerando queda de *link*, oscilação do protocolo de roteamento e *reboot* de um equipamento.

Seguindo a exatamente a mesma linha dos testes com *6over4*, os resultados dos testes de falha executados com o *dual stack* estão dispostos na tabela 3.3

O teste de queda de *link* consistiu em derrubar a porta 1/26, via comando *shutdown*, em Router 2, forçando a convergência para a VLAN 1001, interface 1/14, passando também por Router 3.

Foi simulada a queda do OSPFv3 executando um *flap* no protocolo em Router 4. Com isso, não houve convergência, forçando a queda total de tráfego.

O teste de *reboot* ocorreu em Router 5, garantindo que não houvesse convergência de tráfego.

Foram realizadas três medidas e calculado o tempo médio de perda de tráfego do cenário.

Tabela 3.3 – Medidas de tempo de recuperação no cenário *dual stack*.

Ação	Equipamento	Tempo 1	Tempo 2	Tempo 3	Tempo Médio
Shutdown	Router 2 Porta 1/26	00:06,033	00:06,000	00:05,944	00:05,992
No Shutdown	Router 2 Porta 1/26	00:06,951	00:06,997	00:06,998	00:06,982
Flap OSPF	Router 4	00:33,011	00:32,099	00:33,023	00:32,711
Reboot de Eqto. Intermediário	Router 5	02:32,985	02:33,282	02:33,024	02:33,097

Fonte: Autoria própria.

3.3.3. Utilização de Recursos do *Dual Stack*

Assim como para o *6over4*, a utilização de recursos de hardware leva em conta uso de CPU e memória RAM. Além disso foram realizadas medidas de *jitter*, latência e tempo de convergência de tráfego. As medições foram realizadas considerando um tempo de cinco minutos de estabilidade do sistema, ao passo que havia tráfego de 800 Mbps percorrendo o cenário nos dois sentidos.

A tabela 3.4 demonstra informações sobre os recursos utilizados. Os tipos de dados exibidos são os mesmos da tabela 3.2 porém com informações coletadas durante os testes de *dual stack*, e todos medidos em um intervalo de cinco minutos durante um período de estabilidade do sistema.

Tabela 3.4 – Utilização de recursos no cenário *dual stack*.

Equipamento	CPU (%)	RADVD CPU (%)	RAM (MB)	RADVD RAM (MB)
Router 1	17.3	1.4	581	0,840
Router 2	13.7	0.0	570	0,784
Router 3	7.4	0.0	708	0,784
Router 4	6.8	0.0	705	0,804
Router 5	10.7	0.0	601	0,804
Router 6	11.6	0.9	605	0,832

Fonte: Autoria própria.

3.4. ANÁLISE DOS RESULTADOS

A análise dos dados é feita para cada tipo de medição realizada durante os testes. A comparação entre as medidas feitas com *6over4* e com *dual stack* durante os testes no cenário proposto é feita individualmente, por exemplo, a comparação das medidas de *jitter* será independente das medidas dos outros parâmetros.

3.4.1. Análise dos Dados Coletados Com Medidas de *Jitter*

As medidas de *jitter* demonstram o atraso na entrega entre os pacotes, algo que afeta principalmente a tecnologia VoIP.

O quadro 3.6, possui informações sobre *jitter* retiradas dos quadros 3.2 e 3.5. As medidas estão classificadas de acordo com seus respectivos tipos de dados paralelamente aos métodos de transições dos quais foram extraídas.

Tipo de dados	**Método *6over4***	**Método *dual stack***
***Streams* Medidos**	20	20
Média de *Jitter* médio a curto prazo	0,301 µs	0,3 µs
Média de *Jitter* Médio	0.295 µs	0.3 µs
Média de *Jitter* médio absoluto (RFC 4689)	0.295 µs	0.3 µs
Média de *Jitter* Mínimo	0,0205 µs	0,006 µs
Média de *Jitter* Máximo	1,3255 µs	1,61 µs

Quadro 3.6 – Médias de *jitter* dos cenários *6over4* e *dual stack*.

Fonte: Autoria própria.

Através do quadro 3.6 pode-se notar que as medidas foram relativamente parecidas, com diferenças na casa dos nanosegundos.

O quadro 3.7 mostra a diferença, em porcentagem, entre o *jitter* medido com o *dual stack* em comparação ao *6over4*. Em caso de resultado negativo, deve ser interpretado que o *dual stack* se saiu melhor.

Tipo de dados	Diferença
Média de *Jitter* médio a curto prazo	-0,33 %
Média de *Jitter* Médio	1,69 %
Média de *Jitter* médio absoluto (RFC 4689)	1,69 %
Média de *Jitter* Mínimo	-97,07 %
Média de *Jitter* Máximo	21,46 %

Quadro 3.7 – Diferença entre medidas de *jitter* dos cenários *6over4* e *dual stack*.

Fonte: Autoria própria.

O quadro 3.7 demonstra que o *dual stack* se saiu melhor na medida de *jitter* médio a curto prazo, porém a diferença foi pouco significativa. Para as medidas de *jitter* médio e *jitter* médio absoluto, o *6over4* se mostrou superior.

As grandes diferenças se concentraram nas medidas de *jitter* mínimo e máximo, situação em que o *dual stack* teve resultados muito melhores se tratando do mínimo, mostrando que possui maior capacidade para minimizar o atraso de *jitter*. Em contrapartida, o *dual stack* mostra que o *6over4* pode ser superior se o *jitter* máximo for um problema considerável para a rede.

3.4.2. Análise dos Dados Coletados Com Medidas de Latência

A medida de *latência* trata-se do tempo que um dado demora para chegar ao seu destino.

O quadro 3.8, possui informações sobre latência retiradas dos quadros 3.2 e 3.5. As medidas estão classificadas de acordo com seus respectivos tipos de dados paralelamente aos métodos de transições dos quais foram extraídas.

Tipo de dados	Método *6over4*	Método *dual stack*
***Streams* Medidos**	20	20
Média de Latência média a curto prazo	17,985 µs	16.864 µs
Média de Latência Média	17,223 µs	16.865 µs
Média de Latência Mínima	15,765µs	15.7985 µs
Média de Latência Máxima	3615,661µs	18,3205 µs

Quadro 3.8 – Médias de latência dos cenários *6over4* e *dual stack*.

Fonte: Autoria própria.

O quadro 3.9 mostra a diferença, em porcentagem, entre a latência medida com o *dual stack* em comparação ao *6over4*. Assim como com as comparações de *jitter*, em caso de resultado negativo, deve ser interpretado que o *dual stack* se saiu melhor.

Tipo de dados	Diferença
Média de Latência média a curto prazo	-6,23 %
Média de Latência Média	-2,08 %
Média de Latência Mínima	0,21 %
Média de Latência Máxima	-99,49 %

Quadro 3.9 – Diferença entre medidas de latência dos cenários *6over4* e *dual stack*.

Fonte: Autoria própria.

O quadro 3.9 mostra que o *dual stack* se saiu melhor em três, das quatro, medidas. Apenas para a latência mínima se mostrou inferior em relação ao *6over4*.

Vale ressaltar a grande diferença para a média de latência máxima, a qual mostrou valores bastante altos por parte do método *6over4*, e por isso tamanha discrepância.

3.4.3. Análise dos Dados Coletados Com Testes de *Reboot*

Os testes com *reboot* de um equipamento intermediário incluíam basicamente o tempo que este demorava para subir novamente, aplicar todas as configurações, trocar mensagens com os vizinhos para estabelecimento de conexão para os protocolos e então retransmissão do tráfego.

Tanto para os testes com *dual stack* como com *6over4* foram coletadas três medidas de tempo e calculada uma média entre elas, para garantir maior confiabilidade da análise.

Para o *6over4* o tempo médio que o equipamento levou para concluir todos os procedimentos e voltar a transmitir tráfego foi de 02:28,212. Enquanto que a média das medidas para o mesmo teste, porém com cenário rodando *dual stack*, foi de 2:33,097.

Considerando o tempo apenas em segundos, para facilitar a análise, foram 148,212 segundos para o *6over4* contra 153,097 segundos para o *dual stack*. A razão entre as duas medidas médias gera um resultado que mostra vantagem de aproximadamente 3,3% do *6over4* sobre o método *dual stack*.

3.4.4. Análise dos Dados Coletados Com *Flap* do OSPF

O teste relacionado ao *flap* do protocolo OSPF é composto por medidas de tempo de recuperação do tráfego. Através de um *clear* no protocolo é possível perceber o tempo que o OSPF precisa para ser reaplicado no equipamento, estabelecer as vizinhanças para a troca de rotas e por fim voltar a transmitir o tráfego.

Assim como nos testes de *reboot*, foram coletadas três amostras de tempo, para cada método de transição, e com elas se foi calculado o valor médio.

Para o *6over4*, o tempo foi de 25,194 segundos, enquanto que para o *dual stack* este tempo foi em média de 32,711 segundos. Vale ressaltar que o *clear* executado para o *6over4* foi em cima do OSPFv2 e para o *dual stack* em cima apenas do OSPFv3 (mesmo tendo a versão 2 também habilitada e em funcionamento). De qualquer maneira, o *6over4* se mostrou aproximadamente 29,84% mais eficiente na retomada do protocolo de

roteamento.

3.4.5. Análise dos Dados Coletados Com *Shutdown* no *Link*

Para os testes de *shutdown*, o fator em análise é o tempo de convergência de tráfego. Assim como nas análises anteriores, foram feitas três medidas de tempo e calculada a média entre as três para os dois métodos de transição.

Os resultados dos testes com o *6over4* chegaram à uma media de 5,904 segundos, contra 5,992 segundos de média para o *dual stack*. Novamente o *6over4* se saiu melhor em rendimento, porém dessa vez com a menor diferença entre os testes relacionados à perda de tráfego, com aproximadamente 1,49% mais eficiente que o *dual stack*.

3.4.6. Análise dos Dados Coletados Sobre a Utilização de Recursos

A análise de utilização de recursos é feita através do comparativo de utilização de consumo geral de CPU no equipamento e no processo específico de gerenciamento do IPv6, chamado RADVD. O mesmo ocorre para memória RAM, com utilização total de memória e no processo específico RADVD.

A tabela 3.5 demonstra que em questão de utilização da CPU considerando o uso geral no equipamento. O método *dual stack* se mostrou mais eficiente em todos os roteadores de acordo com o cenário proposto.

Tabela 3.5 – Comparativo de consumo geral de CPU.

Equipamento	***6over4***	***Dual Stack***	**Diferença**
Router 1	19.5	17.3	-11,28%
Router 2	14.3	13.7	-4,19 %
Router 3	7.6	7.4	-2,63 %
Router 4	7.3	6.8	-6,84 %
Router 5	10.8	10.7	-0,93 %
Router 6	11.8	11.6	-1,69 %

Fonte: Autoria própria.

A tabela 3.6 mostra o comparativo apenas em Router 1 e Router 6 em relação ao consumo de CPU pelo processo RADVD, visto que com o método *6over4* não há aplicação de IPv6 nos outros roteadores do cenário. Em Router 1 o processo *dual stack* se mostrou mais eficiente, e o inverso ocorreu em Router 6. É importante ressaltar que os outros equipamentos que possuem pilha dupla apresentaram consumo muito baixo, ficando abaixo da casa dos décimos, situação que resultou resposta de 0.0% exibida pelo equipamento sobre o consumo de CPU pelo RADVD.

Tabela 3.6 – Comparativo do consumo de CPU pelo processo RADVD.

Equipamento	*6over4*	*Dual Stack*	Diferença
Router 1	1.5	1.4	-6,67 %
Router 2	-	0.0	-
Router 3	-	0.0	-
Router 4	-	0.0	-
Router 5	-	0.0	-
Router 6	0.8	0.9	12,5 %

Fonte: Autoria própria.

O consumo de memória, ao contrário do que ocorreu com a parte de CPU, foi toda favorável ao método *6over4*. Os dados em detalhes estão dispostos na tabela 3.7.

Tabela 3.7 – Comparativo de utilização geral de memória RAM.

Equipamento	*6over4*	*Dual Stack*	Diferença
Router 1	579	581	0,34 %
Router 2	565	570	0,88 %
Router 3	693	708	2,16 %
Router 4	690	705	2,17 %
Router 5	589	601	2,04 %
Router 6	593	605	2,02 %

Fonte: Autoria própria.

Considerando apenas o consumo de memória do processo RADVD, em Router 6 não houve diferença, enquanto que para Router 1 a vantagem foi do *6over4*. Nos demais roteadores, apenas o método *dual stack* consumiu recursos de memória, visto que para o *6over4* não há aplicação de IPv6. As medidas estão dispostas na tabela 3.8

Tabela 3.8 – Comparativo de utilização de memória RAM pelo processo RADVD.

Equipamento	*6over4*	*Dual Stack*	Diferença
Router 1	0,836	0,840	0,48
Router 2	-	0,784	-
Router 3	-	0,784	-
Router 4	-	0,804	-
Router 5	-	0,804	-
Router 6	0,832	0,832	0

Fonte: Autoria própria.

4. CONCLUSÕES

Os objetivos propostos no início do trabalho se basearam na hipótese de que o método de transição *dual stack* seria o mais recomendado para a implantação do IPv6 e substituição completa do IPv4.

Durante a pesquisa, considerando que a tradução não é um método recomendado, a transição foi analisada de maneira básica comparando os outros dois métodos possíveis, *dual stack* e tunelamento, sendo o tunelamento representado pelo método *6over4*.

Os testes comparativos foram executados em um cenário único, porém em duas etapas, cada uma envolvendo um dos dois métodos participantes da análise. Os parâmetros analisados, dentre eles medidas de *jitter*, latência e utilização de recursos, além de verificações de perda de tráfego, através de *reboot* de equipamento, queda de *link* e também *flap* de protocolo, foram medidos através de um equipamento de testes.

As maiores dificuldades encontradas durante a elaboração do trabalho foram em relação aos dados disponíveis sobre o atual estado do IPv6. Além disso, a complexidade da implantação do *6over4* resultaram em grande tempo gasto.

Foi possível perceber que sobre o consumo de recursos de CPU, o *dual stack* se mostrou superior em relação ao *6over4*, dados que podem ajudar na opção pelo *dual stack*. Porém a utilização de memória RAM ocorreu o contrário, motivo que pode influenciar negativamente pela escolha do método cujas pilhas IPv4 e IPv6 rodam em paralelo, ainda mais se considerar que a quantidade de rotas para redes IPv6 implicará em mais consumo de memória.

As medidas de latência se mostraram melhores, em geral, no método *dual stack*, enquanto que no caso do *jitter* a vantagem é levemente superior para o *6over4*, porém nada justifique fortemente a sua utilização em relação ao método com as duas pilhas paralelas.

Entre os testes de falha de tráfego, o que mais chama atenção é o de *flap* do OSPF, que ficou quase 30% superior em performance em favor do *6over4*, entretanto talvez seja, dos três, o mais improvável em questão de ocorrência. Nos casos de queda de *link* e *reboot* ambos tiveram leve desempenho superior em favor do *6over4*, porém dessa vez com pouca diferença, 1,49% e 3,3%, respectivamente. Novamente, nada que justifique fortemente a implantação do *6over4*.

Portanto, com os resultados analisados, considerando que o desempenho do *dual stack* foi próximo ao do *6over4* nos resultados dos testes executados, considerando a facilidade de implantação e o baixo impacto na rede concluiu-se que o *dual stack* é sim o melhor método para transição. Porém é necessário esforço por parte do gerente da rede para atualizar toda a planta, além de investimento financeiro para trocar equipamentos, caso os correntes não possuam IPv6.

Com mais tempo e recursos talvez várias topologias ilustrativas pudessem ser abordadas para detalhes da implantação em variados tipos de cenários, de acordo com a necessidade das redes. O importante é que o trabalho criou um método que permite ao gestor de uma determinada rede realizar os testes conforme a sua topologia particular e para ela determinar a melhor alternativa para transição.

Para futuros estudos a cerca do tema, além de um leque mais amplo de topologias, recomenda-se desenvolver pesquisas para avaliar a evolução da transição com o passar do tempo, de acordo com os métodos migratórios, correlacionando com o *hardware*

necessário para suportar a quantidade de rotas que a farão parte da Internet, visto que o IPv6 proporciona a utilização de muitas redes para a tabela global de roteamento, talvez até mais que a tabela global de IPv4, mesmo com um crescimento estruturado.

5. REFERÊNCIAS

ARGAEZ, E. **World Internet usage and population statistics**. Internet World Stats. 2012. Disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em 18 nov. 2013.

BATES, T.; SMITH, P.; HUSTON, G. **CIDR REPORT**. 2014. Disponível em <http://www.cidr-report.org/as2.0/>. Acesso em 03 abr. 2014.

BERENGUER, S. S. **IPv4 Exhaustion And IPv6 Deployment**. Lacnic.net. S.D. Disponível em <http://www.labs.lacnic.net/site/sites/default/files/IXP%20Workshop%20-%20IPv4%20Exhaustion%20and%20IPv6%20Deployment.pptx>. Acesso em 22 out. 2013

BLANCHET, M. **Special Use IPv6 Addresses**. IETF. 2008. Disponível em < http://tools.ietf.org/html/rfc5156>. Acesso em 07 jun. 2014.

CISCO. **IPv6 Extension Headers Review and Considerations**. Cisco. 2006. Disponível em < http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html>. Acesso em 07 jun. 2014

CARPENTER B. E.; MOORE, K. **Connection of Ipv6 Domains via IPv4 Clouds**. The Internet Society. 2001.

DEERING S. E.; HINDEN, R. M. **Internet Protocol, Version 6 Specification**. The Internet Society. 1998.

EQUIPE IPv6.br. **Questões Frequêntes**. Núcleo de Informação e Coordenação do ponto BR. 2012. Disponível em <http://ipv6.br/faq/>. Acesso em 22 out. 2013.

FRANKEL, S. et al. **Guidelines for the Secure Deployment of IPv6**. National Institude of Standards and Technology. Gaithersburg, USA. 2010.

HUSTON, G. **The Changing Foundation of the Internet: Confronting IPv4 Address Exhaustion**. 2008. Disponível em <http://www.potaroo.net/ispcol/2008-10/v4depletion.html>. Acesso em 27 mar. 2014.

HUSTON, G. **The End of Ipv4, Part2**. 2012. Disponível em <http://www.potaroo.net/ispcol/2012-08/EndPt2.html>. Acesso em 27 mar. 2014.

HUSTON, G.; LORD, A.; SMITH, P. **IPv6 Address Prefix Reserved for Documentarion**. The Internet Society. 2004.

LEINER, B. et al. **A Brief History of the Internet**. [S.D.]. Disponível em <http://www.internethalloffame.org/brief-history-internet>. Acesso em 31 jan. 2014.

LIU T. et al. **A new Worm Exploiting IPv6 and IPV4-IPv6 Dual-Stack Networks: Experiment, Modeling, Simulation, and Defense**. Xian, China. 2009.

MOREIRAS A. M. **Qual é o tamanho de bloco apropriado?**. Ipv6.br. 2011. Disponível em < http://ipv6.br/qual-e-o-tamanho-de-bloco-apropriado/>. Acesso em 31 mai. 2014.

PALET, J. **6in4 versus 6over4 terminology**. IETF. 2005. Disponível em <http://tools.ietf.org/html/draft-palet-v6ops-6in4-vs-6over4-01>. Acesso em 20 jun 2014.

PERSER, J. et al. **Terminology for Benchmarking Network-layer Traffic Controle Mechanisms**. IETF. 2006. Disponível em <http://tools.ietf.org/html/rfc4689>. Acesso em 13 jul 2014.

POSTEL, J. B. **RFC 791**. **Internet Protocol**. IETF. Arlington, USA. 1981.

SANTOS, R. R. dos et al. **Curso IPv6 Básico**. São Paulo. Núcleo de Informação e Coordenação do ponto BR. 2010.