V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

UNIBALSAS
Faculdade de Balsas

COMPARATIVO ENTRE AS TÉCNICAS DE TRANSIÇÃO DO IPV4 PARA IPV6: TRADUÇÃO, TUNELAMENTO E PILHA DUPLA.

SOUZA, Nelton Rodrigues Souza[1]
SILVA, Edilmárcio Reis Costa[2]
SOUSA, Jakson Ferreira de Sousa[3]

Resumo: Este trabalho apresenta uma comparação entre as três principais técnicas de transição do IPv4 para o IPv6: Pilha Dupla, Tradução e Tunelamento, demonstrando a necessidade de implementações diante do esgotamento do IPv4 e da incompatibilidade entre as versões dos protocolos, para que a mudança para o IPv6 possa ocorrer gradativamente sem provocar interrupção na comunicação das redes, demonstrando as diferenças técnicas entre as versões do protocolo IP, as melhorias técnicas propostas pelo IPv6 que não se restringem somente ao aumento de endereçamento. Para o cumprimento dos objetos propostos se fez necessário pesquisas bibliográficas de caráter analítica e descritiva, com o intuito de embasar as atividades desenvolvidas ao longo deste trabalho. A implementação de uma variante de cada técnica foi realizada em um ambiente virtualizado através de um simulador de redes, o Core. Foram realizados testes de latência, de Jitter, throughput, bandwidth e percentual de perda de pacotes, através dos quais foram gerados gráficos que demonstram que as técnicas de Tunelamento e Pilha Dupla obtiveram os melhores resultados, sendo que a técnica de Tradução não obteve resultados satisfatórios para uma eventual escolha em um processo de migração.

Palavras-chave: IPv4, IPv6, Pilha Dupla, Tradução, Tunelamento.

Abstract: This assignment shows the comparison between the three main transition techniques from IPv4 to IPv6: Dual Stack, Translation and Tunneling, showing the need of implementation facing the IPv4 depletion and icompability between the protocol versions, in order that the IPv6 changes can happen gradually without causing interruption on the network communication, demonstrating the technical differences between the IP protocol versions, the improvements offered by IPv6 that don't limit only to the IP addressing increase. To the proposed objects fulfillment it became necessary bibliographies researchs of analytical and descriptive feature, with the intuit to cover the developed activities during this work. The implementation of a variant from each technique was done on a virtual environment through a network simulator, the Core. There were made latency tests, Jitter's, , throughput, bandwidth and package loss percentage, and through them were generated graphics wich demonstrated that the Dual Stack and Tunneling techniques acquired the best results, being that the Translation technique did not acquire satisfactory results for an eventual choice on a migration process.

Keywords: IPv4, IPv6, Dual Stack, Translation, Tunneling.

[1]Acadêmico do Curso de Sistemas de Informação – Unibalsas
[2]Professor da Faculdade de Balsas - Unibalsas
[3]Professor da Faculdade de Balsas - Unibalsas

1. INTRODUÇÃO

A popularização do uso dos computadores e a sua utilização na internet, bem como outros dispositivos que também tem acesso a rede como celulares e *tablets*, por exemplo, impulsionaram o uso da internet e diante do esgotamento de endereçamentos IPv4 a necessidade de desenvolvimento de uma nova versão do protocolo IP (*Internet Protocol*) Protocolo de Internet, o IPv6, objetivando primariamente disponibilizar uma quantidade bem mais ampla de endereçamentos, 128 bits ao invés dos 32 bits do seu antecessor.

O IPv6 não possui retrocompatibilidade com o IPv4, sendo necessária a criação de técnicas de transição para permitir a interoperabilidade das versões e que essa migração possa ser realizada de forma gradual, minimizando o impacto no funcionamento das redes.

Segundo IANA[4] (2017) o iminente esgotamento da alocação de novos endereços de IPv4 disponíveis no mundo, é necessário à realização de um planejamento de migração para IPv6 devido a demanda crescente de uso de internet, como a utilização da IoT[5]. A implementação do IPv6 proporcionará uma alocação dos blocos de endereçamentos IP de forma hierárquica, geográfica e sistematizada, onde a IR[6] distribuem os blocos de endereços as autoridades regionais RIR[7] e estas distribuem as autoridades locais NIR[8] ou LIR[9] que redistribuem aos ISP[10] e estes ao consumidor final. (BRITO, 2013).

Este trabalho se propõe a analisar as características das três principais técnicas de transição como: funcionamento e aplicabilidade, expor as principais características do protocolo IPv6, demonstrar a principais diferenças do IPv4, funcionalidades, melhorias propostas como: sanar o esgotamento de endereçamentos IP's, resgate do princípio de conexão fim-a-fim, implementação de segurança como IPsec (*IP Security Protocol*) nativamente, bem como alocação de endereçamento hierarquicamente.

Foi realizado pesquisa bibliográfica em livros sobre redes de computadores, protocolo IP, técnicas de transição do IPv4 para IPv6, consultas ao site do NIC.BR[11], IPV6.BR[12], IANA, LACNIC[13] e as RFC's[14].

Foi utilizado um ambiente virtualizado para simulação de funcionamento das redes, reproduzindo três cenários, um para cada tipo de técnicas de transição, para mensurar percentual de perdas de pacotes, latência, Jitter, throughput e bandwidth.

Para entender a importância do assunto é preciso conhecer um pouco sobre a origem, o propósito para o qual as redes foram construídas e consequentemente os protocolos que foram criados, entender a sua evolução e aplicabilidade.

2. HISTÓRICO DA INTERNET

A internet já se tornou parte do nosso cotidiano para as mais diversificadas atividades, desde pesquisas, acesso bancário, vídeo conferência, navegação em sites, assistir TV, ouvir músicas, interagir em redes sociais, mas o propósito inicial da sua criação foi militar e acadêmico.

---

[4]IANA - Autoridade para Atribuição de Números da Internet - é a autoridade global que supervisiona a atribuição dos endereçamentos IP na Internet
[5]IoT - Internet das Coisas - é uma tecnologia que conecta dispositivos eletrônicos do dia-a-dia à internet
[6]IR - Registro de Internet - Autoridade Global
[7]RIR - Registro Regional de Internet – Autoridade Regional
[8]NIR - Registros Nacionais de Internet – é uma Autoridade Nacional
[9]LIR - Registros Locais de Internet – é uma Autoridade Local
[10]ISP - Provedor de Serviço Internet
[11]NIC.BR - Núcleo de Informação e Coordenação do Ponto BR - Autoridade Nacional do Brasil
[12]IPV6.BR – Serviço do NIC.BR com informações, documentação, vídeos informativos e palestras sobre IPv6
[13]LACNIN - Registro de Endereçamento da Internet para a América Latina e o Caribe é a Autoridade Regional
[14]RFC - Requisição de Comentários - Documentos que contém notas técnicas e organizacionais sobre a Internet e cobrem muitos aspectos das redes de computadores, protocolos, procedimentos, programas e conceitos.

V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

A criação da internet teve inicio com um projeto do DoD[15] que é um Departamento de Defesa do governo americano na década de 60 para interligação de computadores das bases militares e centro de pesquisas e foi desenvolvido pela ARPA (*Advanced Research Projects Agency*), Agência de Pesquisas e Projetos Avançados, recebendo o nome de ARPANET (*Advanced Research Projects Agency Network*), Rede de Agência para Projetos de Pesquisa Avançada, e que tinha como objetivo principal manter a estrutura de comunicação em funcionamento. (TANENBAUM, 2011).

A ARPANET trabalhava com diversos protocolos de comunicação, mas seu enfoque era no NCP (*Network Control Protocol*) Protocolo de Controle de Rede, mas já em meados de 1983 quando a rede alcançou 562 hosts[16] e por conta de restrições do NCP, foi adotado o protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) Protocolo de Controle de Transmissão IP, que dentre outras melhorias proporcionou o crescimento ordenado da rede. (IPV6.BR, 2012).

Nesse contexto de desenvolvimento de protocolos de comunicação e equipamentos de fabricantes diferentes que seriam utilizados nesse processo, bem como sistemas operacionais distintos que precisariam estar conectados surgiu à necessidade de padronização de Modelos de Referência, como o OSI[17], desenvolvido pela ISO[18], e o TCP/IP.

3. PROTOCOLOS DE COMUNICAÇÃO DE REDE

O modelo TCP/IP é um modelo de referência mais simplificado, com apenas quatro camadas, que surgiu como alternativa ao modelo OSI, diferenciando-se do mesmo pela mesclagem de algumas funções que estavam em camadas distintas do OSI em uma única camada, como a 4 do TCP/IP, que acumula funções da 5, 6 e 7 do OSI. (BRITO, 2013).

A arquitetura TCP/IP é um modelo que vem sendo amplamente utilizada devida a grande utilização do protocolo TCP/IP tanto por fabricantes quanto desenvolvedores de sistema operacionais, por esse protocolo possuir uma arquitetura aberta além da grande popularização da internet e uso de redes de computadores, praticamente se tornou um protocolo universal. O TCP/IP é na verdade um conjunto de protocolos, sendo os principais os que dão nome a ele, o TCP[19] e o IP[20]. (TANEBAUM, 2011).

Dentre os vários protocolos utilizados neste modelo de referência, este trabalho de pesquisa visa analisar as principais caraterísticas técnicas do protocolo IP, que atua na camada três do modelo TCP/IP, bem como identificar funcionalidades.

4. O PROTOCOLO IP

O protocolo IP (*Internet Protocol*) foi projetado para utilização em sistemas interligados em redes cuja transmissão é realizada em blocos chamados datagramas, provendo duas funções básicas: fragmentação de pacotes, que permite o envio de pacotes maiores que os limites de tráfego em um enlace de rede quebrando-o em pacotes menores para posterior reenvio; e o endereçamento que são dados armazenados no cabeçalho do protocolo que dentre outras informações estão o remetente, o destinatário, a versão do protocolo, a informação e a sequência dos pacotes para a remontagem quando o mesmo é fragmentado em cada nó da rede. (TORRES, 2016).

O protocolo de Internet IP é um conjunto de regras que permite a comunicação entre equipamentos interligados em rede e

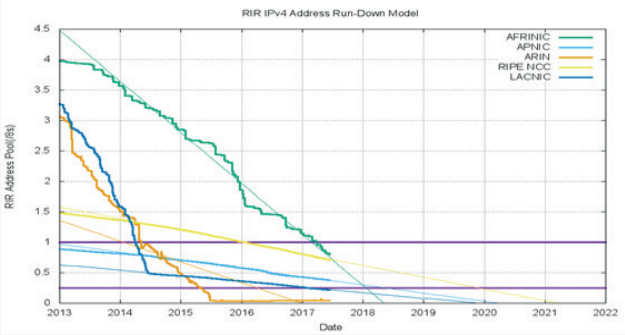
[15]DOD Departamento de Defesa – órgão do governo americano responsável pela coordenação e supervisão de todas as agências e funções do governo ligado diretamente com a segurança nacional e com as suas forças armadas.
[16]Host – é um termo técnico utilizado para definir um computador ou qualquer dispositivo conectado em uma rede com um endereço de IP.
[17]OSI - é um modelo de referência desenvolvido pela ISSO em sete camadas de funções
[18]ISO - Organização Internacional para a Normatização
[19]TCP - Protocolo de controle de transmissão – é um protocolo de transporte fim-a-fim, orientado a conexão com controle de erros.
[20]IP – Protocolo de Internet - é um protocolo de comunicação usado entre as máquinas em rede para encaminhamento dos dados através de endereçamento.

que foi inicialmente projetado para que cada dispositivo tivesse uma identificação única através de um endereço numérico, sendo de fácil implementação e não dependente de sistemas ou equipamentos desde quando foi projetado.

4.1 O PROTOCOLO IPv4

O IPv4 é um protocolo de 32 *bits*, divido em quatro blocos de oito *bits* chamados de octetos sendo possível ter 4.294.967.296 de endereços IP's distintos que foram projetados inicialmente em três classes de tamanhos fixos para dar maior flexibilidade na alocação de endereços contemplando redes de diferentes tipos e tamanhos, mas em pouco tempo, tornou-se ineficiente com o crescimento das redes. (IPV6.BR, 2012).

Figura 01: Estatística de esgotamento IPv4 – 2017.



Fonte: HUSTON, G[21]. (2017).

De acordo com a Figura 01, o esgotamento dos endereços IPv4 não deve ser visto como algo que ainda irá acontecer, visto que o esgotamento de IPv4 e previsão ainda para 2017 o fim da reserva técnica, conforme transcrição das informações na tabela abaixo:

Tabela 01: Esgotamento e reserva técnica das RIR's.

AUTORIDADE	PREVISÃO ESGOTAMENTO	% DE RESERVA TÉCNICA
APINIC[22]	04/2011	0,37 %
RIPE NCC[23]	09/2012	0,71 %
LACNIC[24]	06/2014	0,21%
ARIN[25]	09/2015	0%
AFRINIC[26]	06/2018	0,79%

Fonte: o autor (2017)

Segundo a RFC 4632 (2006) o CIDR possibilitou a alocação de endereçamentos IP's mais flexível, pois as máscaras poderiam ser ajustadas em conformidade ao tamanho de cada rede, não havendo mais a obrigatoriedade de utilização com os três tamanhos fixos estipulados por cada tipo de classe A, B, ou C com suas respectivas máscaras como era descrito na RFC 1519, que se tornou obsoleta após a adoção do CIDR, os endereços são especificados com o sufixo / XX que poderiam ir até /32 para representar quantos bits a máscara possuiria para redes (1) e para hosts (0) numa representação binária como o /24 = 255.255.250.0, trazendo maior flexibilidade e adequação de uso.

Segundo a RFC 3022 (2001), o NAT é uma técnica paliativa que foi desenvolvida para solucionar temporariamente o problema do esgotamento dos endereços de IPv4, visto que um computador da rede teria um IP público, e os demais hosts da rede teriam os chamados IP's privados, que são utilizados somente para tráfego interno. Quando algum desses hosts necessitarem de comunicação externa a rede a qual ele pertence, como a internet, o tráfego é direcionado para o *gateway*[27] da rede, que possui comunicação com as redes internas e externas, para que o mesmo faça uma intermediação traduzindo o tráfego.

O mascaramento utilizado no NAT

V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

quebrou o princípio fim-a-fim proposto na concepção da internet, a conexão direta entre dois *hosts*, dentre os principais problemas é possível citar a limitação do número de conexões simultâneas, restrições a aplicações que necessitam de conexão host-a-host para um bom funcionamento como P2P[28], VPN[29] e VoIP[30], exigindo maior poder computacional do *gateway da rede*. (BRITO, 2013).

As técnicas utilizadas para contornar o esgotamento de IPv4 tinham como principal objetivo oferecer soluções paliativas para dar uma sobrevida ao protocolo em uso, evitar que houvesse estagnação da rede e para que pudesse ser aprimorado e implementado um novo protocolo que já estava em desenvolvimento, o IPv6.

4.2 O PROTOCOLO IPv6

As soluções desenvolvidas para contornar a limitação de endereçamentos possíveis em IPv4, embora tenham conseguido certo êxito na redução de solicitações de IP's junto a IANA, não foram suficientes para solucionar a demanda de crescimento da rede.

O IPv6 foi projetado inicialmente para suprir o esgotamento de endereços IPv4, trazendo mudanças na estrutura do cabeçalho IP, mais simplificado e de tamanho fixo, acoplamento de funcionalidades no ICMP, uso do PMTUD e IPsec nativo. (BRITO, 2013).

De acordo com a RFC 1550 (1993) as pesquisas desenvolvidas para o sucessor do IPv4, que foi chamado IPng[31], que dentre as suas principais características além da escalabilidade e políticas de roteamento, deveriam prover transição, segurança, mobilidade e suporte a QoS[32].

O IPv6 foi inicialmente projetado para sanar definitivamente a escassez de endereços IP's na internet, possuindo 128 bits de endereços possíveis: 340.282.366.920.938. 463.463.374.607.431.768.211.456 (340 Undecilhões) de endereçamento, é equivalente a 79 octilhões de vezes a quantidade de IPv4. (IPV6.BR, 2012).

O IPv6 não utiliza *broadcast*[33], essa função foi acoplada ao *multicast*[34] onde a informação é enviada para um grupo de interfaces, com relação ao funcionamento do *unycast*[35] e *anycast*[36] o funcionamento segue similar ao seu antecessor, o IPv4.

O endereçamento IPv6 é distinto do IPv4 não só pela capacidade de endereçamento, mas também pela forma, os endereços são compostos por oito grupos de 16 *bits* chamados hexadecatetos (hexadecimais), separados por dois pontos. (LACNIC, 2015).

Os endereços IPv6 não são case-sensitives, ou seja, não levam em consideração maiúsculo ou minúsculo, suportam sistema de abreviação do endereço omitindo os zeros a esquerda a cada hexadecateto, podendo suprimir longas sequências de zeros por " :: ". Em URL o número do IP passa a vir entre colchetes para evitar ambiguidade quando for necessário especificar a porta no acesso. (IPV. BR, 2012).

O IPv6 trouxe algumas modificações na forma de funcionamento de algumas funções do seu antecessor como por exemplo: ICMP[37], ARP[38], RARP[39], IGMP[40], NDP[41], novas implementações como PMTUD[42] (*Path MTU Discovery*) para diferença de MTU[43] dos nós, sendo todas acopladas no ICM-

[31]IPng - Protocolo de Internet próxima geração - é um protocolo de 16 bits
[32]QoS - Qualidade de Serviço é utilizando para garantir largura de banda ou priorização de tráfego
[33]Broadcast - tipo de comunicação em que um quadro é enviado para todos os endereços da rede mesmo havendo somente um destinatário
[34]Multicast – tipo de comunicação em que um quadro é enviado para um grupo no qual há diversas interfaces associadas
[35]Unicast – tipo de comunicação em que um quadro é enviado para um único endereço da rede
[36]Anycast - tipo de comunicação em que um quadro é enviado a uma interface pertencente a um grupo
[37]ICMP - Protocolo utilizado para fornecer relatórios de erros de comunicação
[38]ARP - Protocolo de Resolução de Endereços - faz resolução de endereço lógico para endereço físico
[39]RARP - Protocolo de Resolução Reversa de Endereços faz resolução de endereço físico para endereço lógico
[40]IGMP Protocolo - protocolo de controle de grupo de multicast
[41]NPD Protocolo de descoberta de vizinho protocolo de descoberta de vizinhança dos nós
[42]PMTUD Protocolo utilizado para determinar dinamicamente o menor valor limite no trajeto
[43]MTU - Unidade Máxima de Transmissão de um nó da rede

Pv6. (BRITO, 2013).

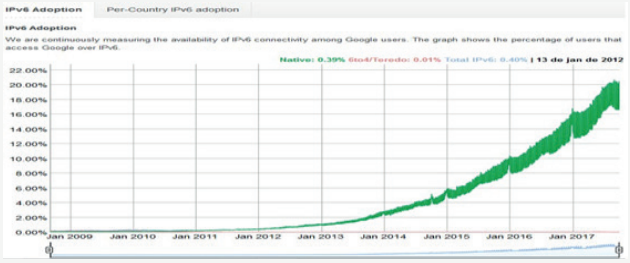
O cabeçalho do IPv6 trouxe algumas mudanças estruturais referentes ao seu antecessor como, por exemplo o tamanho, no IPv4 poderia variar de 20 a 60 bytes, no IPv6 ele é de tamanho fixo com 40 bytes, além da redução da quantidade de campos no cabeçalho de 12 para 8, removendo campos que se tornaram obsoletos para o IPv6, optando-se por manter o cabeçalho básico para otimizar o desempenho, além de novas funcionalidades que trouxeram aprimoramentos através de cabeçalhos de extensões que proporcionaram maior flexibilidade para futuras implementações com encadeamento de cabeçalhos. (IPV.BR, 2012).

De acordo com a RFC 4443 (2006) o ICMPv6 é obrigatória para todos os nós da rede, mantendo a mesma funcionalidade de reportar erros no tráfego e processamento de pacotes além de ganhar novas funcionalidades, que eram realizadas por outros protocolos como ARP e RARP, sendo acoplado diretamente no ICMPv6, proporcionando melhorias em *firewall*[44] por possibilitar bloquear descoberta de vizinhança e autoconfiguração.

Em conformidade com a RFC 1981 (1996) o PMTUD é um protocolo que foi desenvolvido com o intuito de se evitar fragmentação dos pacotes entre dois pontos, os pacotes não são montados e remontados nos roteadores[45], no meio da conexão, em caso de divergências de MTU na rota, o roteador descarta o pacote, envia um retorno PMTUD no ICMPv6 informando que rejeitou o pacote e também o tamanho do seu MTU (*Packet Too Big*), assim o emissor faz os devidos ajustes para adequação da rota, havendo fragmentação somente na origem, por isso é imprescindível o não bloqueio de pacotes ICMP no IPv6.

O IPSec[46] é um protocolo de segurança que possibilita a troca de informações entre hosts na internet de forma segura através de criptografia, possuindo suporte para criptografias simétricas, assimétricas e combinação entre elas, suporte aos cabeçalhos AH (*Authentication Header*), que provê criptografia do *payload* (dados) e do cabeçalho, e do ESP (*Encapsuled Security Payload*) que provê criptografia somente para o *payload* (dados), sendo possível uma combinação de técnicas com AH e ESP. (RFC 4301, 2005).

Figura 02: Estatística da adoção do IPv6 no Mundo.



Fonte: Google[47] (2017).

De acordo com a Figura 02, houve um aumento significativo no uso de IPv6 a partir de 2014, coincidentemente com o esgotamento do IPv4 em muitas regiões, saindo de aproximadamente 3% em janeiro de 2014 para pouco mais de 20% em outubro de 2017.

Diante das diferenças técnicas e estruturais do IPv6 em relação ao IPv4, por decisão de projeto não foi contemplado uma retrocompatibilidade com a antiga versão do protocolo, sendo necessário o desenvolvimento de técnicas de transição para que essa migração ocorresse de forma progressiva, até a completa mudança para o IPv6.

5. TÉCNICAS DE TRANSIÇÃO DO IPv4 PARA O IPv6

Este trabalho visa demonstrar as principais técnicas de transição que foram desenvolvidas para contornar problemas de interoperabilidade das versões dos protocolos IPv4 e IPv6, e que pudessem coexistir em um ambiente heterogêneo de forma que redes funcionando com protocolos distintos pudessem se comunicar até que a migração pudesse ocorrer de forma gradativa, sendo

[44]Firewall - dispositivo de rede responsável por aplicar políticas de segurança de tráfego de dados e acesso a rede
[45]Roteador – dispositivo de rede capaz de realizar e intermediar comunicação entre duas redes distintas
[46]IPSec - Protocolo de extensão que provê segurança em nível de camada IP
[47]Imagem disponível em: https://www.google.com/intl/en/ipv6/statistics.html

V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

as principais: Pilha Dupla, Tradução e Tunelamento.

Segundo APINIC (2017), atualmente há uma predominância de redes em IPv4, por isso as principais técnicas são para prover conexões às redes IPv6, mas com o decorrer gradual da migração e quando as redes IPv6 forem majoritárias, será necessário o aprimoramento das técnicas para prover a comunicação das futuras redes legadas em IPv4.

5.1 PILHA DUPLA

A técnica de Pilha Dupla foi desenvolvida para prover conexões em IPv6 sem a necessidade de desativação imediata da pilha de protocolo IPv4, visando uma migração gradual reduzindo o impacto no processo de migração.

A técnica de Pilha Dupla apresenta certa facilidade de implementação ao tornar possível a utilização das duas pilhas de protocolos, nos host e roteadores de rede, permitindo que a rede funcione em ambas as versões, mas exigindo que se façam configurações das duas redes lógicas em cada dispositivo, até completar o processo de migração. (RFC 6333, 2011).

A estruturação dos servidores DNS (Domain Name System) deverá suportar registro AAAA (*quad-A*) que faz o mapeamento de nomes de registro IPv6 conforme a RFC 3596, deverá ser capaz de resolver os nomes de domínio independente da versão do protocolo que originou a consulta ou que está sendo utilizado no domínio solicitado. (RFC 4213, 2003).

A Pilha Dupla pode ser implementada mesmo em redes que utilizam NAT com um único IP público IPv4, onde os equipamentos deverão ter suporte as duas pilhas de protocolos sendo capaz de acessar qualquer dispositivo da rede independente de versão.

Paralelamente ao desenvolvimento e utilização da técnica de Pilha Dupla surgiu outra técnica, a de Tunelamento, que tinha como proposta oferecer conexões IPv6 sem a necessidade de implementação da nova pilha de protocolo em todos os *hosts* da rede.

5.2 TUNELAMENTO

Essa técnica foi desenvolvimento visando além de prover conexões IPv6 para redes com IPv4, proporcionar facilidade de implementação por necessitar das duas pilhas de protocolos e configurações somente nos roteadores ou firewall de borda.

As técnicas de tunelamento consistem em realizar o encapsulamento do pacote IPv6 dentro de um pacote IPv4, quando o pacote IPv4 ao chegar ao destino deve ser descapsulado, para então receber a informação contida no pacote IPv6, a situação inversa também pode ocorrer em casos onde as redes envolvidas na troca de informação estão com IPv4 e o meio pelo qual as informações serão transmitidas está com IPv6, sendo uma técnica de boa aceitação no processo de transição para soluções de curto prazo. (BRITO, 2013).

O 6in4 é uma variante da técnica de tunelamento que é utilizado quando o meio envolvido nos enlaces não possui suporte nativo a IPv6 e para contornar essa situação é criado um túnel estático em IPv4 e dentro desse túnel passa o tráfego IPv6, é também conhecida como protocolo 41 e comporta encapsulamento somente do IPv6. (RFC 4213, 2005).

A Técnica de Tunelamento GRE (*Generic Routing Encapsulation*), originalmente desenvolvido pela Cisco, é um tipo de tunelamento estático para tráfego de dados em IPv6 dentro de túneis em IPv4, que se difere do *6in4* por exemplo, por suportar dentro do seu *payload* (dado do pacote) outros tipos de protocolos além do IPv6 que é encapsulado dentro do pacote GRE, que é novamente encapsulado dentro do pacote IPv4 exigindo dos *firewalls* e roteadores de bor-

da um tratamento específico para realizar a filtragem desse múltiplo encapsulamento. (RFC 2784, 2000).

A técnica de Tunelamento *Tunnel Broker* permite que um host ou rede com IPv4 possa ter conexões IPv6 através de um provedor que disponibiliza um túnel, a semelhança do funcionamento de um servidor VPN, através de um provedor de serviço que utiliza software ou scripts provêem conexões IPv6 com blocos /64 à /48. (RFC 3053, 2001).

Esse tipo de tunelamento é de fácil implementação inclusive para usuários domésticos que queiram testar o uso do IPv6, mas seu provedor de internet não oferece suporte ao protocolo, e não possuem conhecimento técnico para implementação.

A técnica de Tunelamento *6to4* foi uma das primeiras técnicas de transição desenvolvidas, cujo princípio de funcionamento baseava-se na utilização de relays públicos com pilha dupla para disponibilização dos túneis, que oferecessem conectividade IPv6 do tipo stateless[48] mesclando a técnica *6in4* automaticamente, tornando possível a comunicação de redes IPv4 com hosts ou sites na internet com IPv6 e isso de forma dinâmica, são mantidos de forma colaborativa, apresentaram diversos problemas de segurança. (RFC 3056, 2001).

O tunelamento Teredo foi desenvolvido pela Microsoft e é uma técnica dinâmica, tendo como diferencial a possiblidade dos hosts que estão com acesso à internet através de NAT, fornecendo um túnel IPv4 com UDP no qual se provê conectividade IPv6 através de servidores públicos com pilha dupla, cuja utilização atualmente não é recomendada por questões de falhas de segurança, sendo recomendada sua desativação, já que vem instalado e ativado nativamente em sistemas como Windows Vista e 7, sendo recomendado o bloqueio no firewall de borda da porta UDP 3544 para esse tipo de túnel. (RFC 438, 2006).

De acordo com a RFC 4214 (2005), os túneis do tipo ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) possuem aplicabilidade inversa do 6in4, realizando o encapsulamento do pacote IPv4 dentro de um pacote IPv6, sendo uma técnica de tunelamento dinâmica, sem necessidade de relays públicos, com aplicação somente para redes internas.

Uma terceira opção de técnica de transição foi a de Tradução, cuja proposta era prover interconexão entres redes distintas através de dispositivos de borda que pudessem realizar a conversão de uma pilha de protocolo para a outra e possibilitar a comunicação.

5.3 TRADUÇÃO

A Tradução é um tipo de técnica de transição que propôs a interconexão das redes sem a necessidade delas estarem utilizando as mesmas versões de protocolo, permitindo que uma determinada rede com IPv4 possa se comunicar com outras redes tenha IPv6, necessitando que seja feita uma tradução de um tipo para outro.

O funcionamento dessa técnica é semelhante ao que ocorre de IP público para IP privado e pode ser aplicada também a versionamento diferentes do protocolo IP, necessitando de Pilha Dupla somente nas bordas das redes. (IPV6.BR. 2012) .

A técnica de Tradução NAT444 também conhecida por CGNAT (Carrier Grade NAT), ou simplesmente NAT, que faz dupla aplicação de NAT44 com traduções de portas IPv4 para IPv4, uma na rede do usuário, e outra no ISP, onde há três blocos de IP's envolvido, os Públicos na internet, os endereços privados na rede do usuário, e os endereços de um bloco privado especial criado na rede do provedor chamado de endereços compartilhados (*Shared Adrress Space*) especificado na RFC 6598, comprometendo a flexibilidade e escalabilidade da rede, sua administração é complexa, quebrando um dos princípios de funcionamento da internet

[48]Stateless – sem estado – é um tipo de protocolo que não guarda o estado da conexão estabelecida, tratando novas conexões de forma independente.

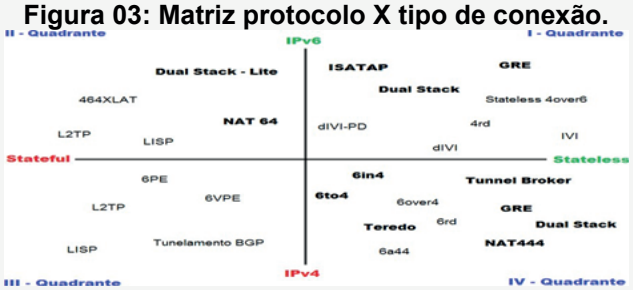
V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

que é a simplicidade do núcleo, não é uma técnica recomenda pelos órgãos gestores de internet, sendo NAT sobre NAT. (RFC 1918, 1996).

A técnica de Tradução NAT64 e DNS64 é útil em ambientes de predominância IPv6 onde há a necessidade de se realizar acesso a redes com IPv4, sendo necessária à tradução das requisições IPv6 em IPv4 que ao obter resposta realizam a tradução inversa, do IPv4 para o IPv6, é uma tradução do tipo *stateful*[49], ou seja, as consultas IPv4 são armazenadas na tabela de roteamento de forma estática para um prefixo IPv6 pré-definido do ISP, ou para um bloco exclusivo reservado para essa finalidade. (RFC 6146, 2011).

Para a implementação do NAT64 é obrigatório à utilização de outra técnica auxiliar, o DNS64, para realizar a tradução de nomes de domínios no caso do destino ser ainda em IPv4 é realizado um encaminhamento para o DNS64, que ao detectar que o nome consultado não possua registro AAAA (*quad-A*) será acrescentado o registro de mapeamento pré-definido para tradução NAT64 mais os 32 bits de endereçamento IPV4, e então os pacotes são encaminhados para o equipamento responsável por fazer a tradução *stateful*, substituindo o IPv6 do usuário por um IPv4 público. (RFC 6147, 2011).

Figura 03: Matriz protocolo X tipo de conexão.



Fonte: o autor (2017)

De acordo com a Figura 03, as técnicas estão dividas pelos tipos de conexão stateless e stateful e por predominância do protocolo de rede IPv4 e IPv6, sendo que as técnicas que estão em negrito foram abordadas neste artigo, salientando que é recomendável a utilização de técnicas do tipo stateless, neste caso as que estão nos quadrantes I e IV.

As técnicas de transição como o próprio nome sugerem, não devem ser consideradas como soluções definitivas, mas como auxílio até que o processo de migração para o IPv6 seja completado. Esses mecanismos de transição são importantes para manter a interoperabilidade da rede enquanto se faz a migração de forma.

6. DESENVOLVIMENTO DA PESQUISA

Em virtude da impossibilidade de realizar testes com redes que estejam utilizando IPv6, foi proposto a simulação em um ambiente virtualizado, no qual foram utilizados: o VirtualBox para criar e gerir as VM's (*Virtual Machine*), o sistema operacional Linux Xubuntu, o Core (*Common Open Research Emulator*) como simulador de redes, o Iperf para geração de tráfego TCP e UDP, o *Wireshark* para a analise de tráfego e uma adaptação dos cenários propostos no livro Laboratório IPv6 da Equipe IPV6.BR.

O VirtualBox é um programa multiplataforma para virtualização de sistemas operacionais baseado em software, sendo possível criar e gerenciar máquinas virtuais de vários sistemas em um único host, sendo capaz de instanciar várias VM's, está disponível em: https://www.virtualbox.org/wiki/Downloads.

O Xubuntu é uma distribuição Linux que tem com base o Ubuntu, cuja mantenedora é a Canonical, utiliza o XFCE (*Xform Common Environment*), mantendo a solidez da base Ubuntu com a leveza e versatilidade da interface XFCE, está disponível em: https://xubuntu.org/getxubuntu/#lts.

O Core é um simulador de rede versátil que possibilita a interligação com outras instâncias do mesmo na rede, ou com rede física, tem suporte para criação de cenário

[49]Statefull – tipo de conexão que armazena o estado da conexão de forma permanente
[50]Drag-and-drop - nomenclatura usual em interfaces gráficas onde os objetos podem ser arrastados para posições diferentes
[51]*Throughput* – taxa de transferência de dados de um ponto a outro da rede

no estilo *drag-and-drop*[50]. Disponível em: https://www.nrl.navy.mil/itd/ncs/products/core.

O Iperf é um aplicativo multiplatarforma desenvolvido em C++ utilizado para geração de tráfego TCP/UDP, teste de *throughput*[51], desenvolvido pela NLANR (*National Laboratory for Applied Network*) disponível em: https://iperf.fr/iperf-download.php.

O Wireshark, é um sniffer[52] amplamente utilizando para análise de tráfego de redes, possui suporte para IPv4 e IPv6, GUI (*Graphical User Interface*) intuitiva e recurso de geração de gráficos. Disponível em: https://www.wireshark.org/download.html.

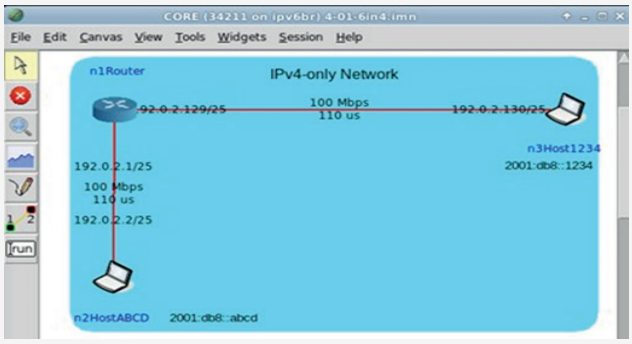
A utilização desse conjunto de ferramentas proporcionou recursos para viabilizar a implementação de cenários virtuais onde foi simulado o funcionamento dos três tipos de técnicas de transição, sendo possível mensurar o desempenho da rede.

A implementação utilizou três cenários distintos para simular no Core o uso de cada um dos três tipos de técnica de transição, onde foi utilizado o Iperf para gerar tráfego de rede, o Wireshark para analisar o tráfego, e também a construção de planilhas para realizar comparativo de desempenho com geração de gráficos.

Foram utilizadas as mesmas métricas para mensurar o desempenho das redes com uso de IPv4 e de um tipo de cada técnica de transição, foram realizados 20 entradas de cada tipo de teste para se obter uma média, cada entrada foi submetida por um intervalo de 60 segundos e os enlaces de redes foram definidos com velocidade de 100 Mb.

Na primeira análise foi utilizado um cenário para simular o funcionamento da técnica de transição Tunelamento, onde foram aplicadas as variações: 6in4 e GER, onde todos os nós da rede possuem a pilha IPv4 e IPv6 com exceção do roteador.

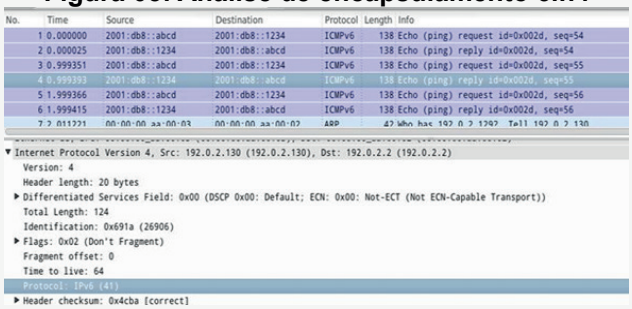
Figura 04 – Cenário para utilização da técnica de tunelamento



Fonte: Adaptado de Moreiras, A. et al. (2012)

De acordo com a Figura 04, o host n2HostABCD e o host n3Host1234 possuem as duas pilhas de protocolos, sendo que o roteador n1Router possui somente IPv4, todos os enlaces possuem velocidade de 100 Mb gerado tráfego com entre esses dois hosts.

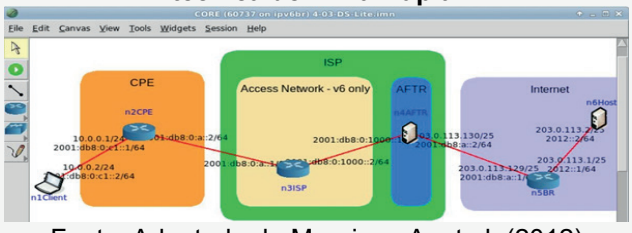
Figura 05: Análise de encapsulamento 6in4



Fonte: o Autor (2017)

De acordo com a Figura 05, o tráfego capturado pelo analisador de tráfego Wireshark, é possível observar no protocolo IPv4 a origem e o destino, a flag 41 que identifica a técnica 6in4, a origem e destino no protocolo IPv6 encapsulado dentro do IPv4.

Figura 06: Cenário utilizado para utilização da técnica de Pilha Dupla.



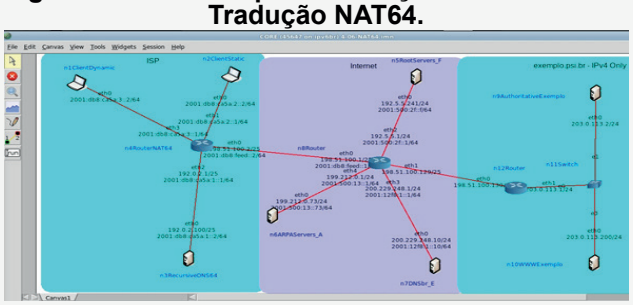
Fonte: Adaptado de Moreiras, A. et al. (2012)

[52]Snnifer – um farejador que intercepta e analisa tráfego de rede

V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

De acordo com a Figura 06, o cenário utilizado para teste com a técnica de Pilha Dupla têm a rede do ISP, a rede do cliente e a rede de destino que trabalham com as duas pilhas de protocolos. Foi gerado tráfego de rede entre os hosts n1Client e n6Host utilizando os protocolos IPv4 e IPv6 segundo as métricas pré-estabelecidas para mensurar o desempenho da técnica de transição.

Figura 07: Cenário para utilização da técnica de Tradução NAT64.



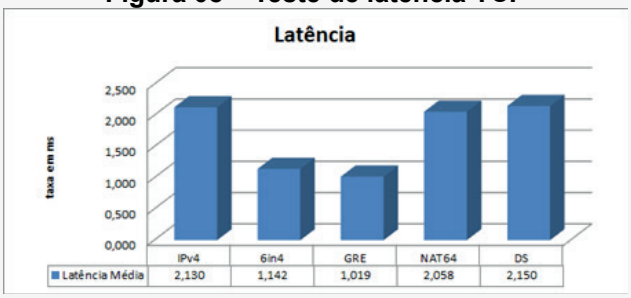
Fonte: Adaptado de Moreiras, A. et al. (2012)

De acordo com a Figura 07, o cenário utilizado para testes com a técnica de Tradução NAT64, onde temos a rede do ISP a internet, e o roteador de borda do ISP com as duas pilhas de protocolos, e um site utilizando somente IPv4. Foi gerado tráfego de rede do host n1ClientDynamic que utiliza somente IPv6 para o host n10WWWExemplo que utiliza somente IPv4, passando pela processo de tradução para depois mensurar o tráfego de rede.

7. RESULTADOS

Após implementar um tipo de cada técnica de transição do IPv4 para o IPv6, foram realizados alguns testes como: medição de latência, variação de latência, teste de Jitter para mensurar variação de atrasos na entrega de dados em rede, bandwidth[53] e throughput[54], variação de throughput, através da geração de tráfego de rede com o Iperf para os protocolos TCP com tráfego simples, full-duplex[55] e com cinco acessos simultâneos, e com UDP com pacotes de tamanho de 100 kb, 500 kb, 1.000 kb, 10 Mb e 50 Mb para analisar o Jitter[56] e com 100 Mb, para analisar o percentual de perda de pacotes nas redes utilizando as técnicas de transição.

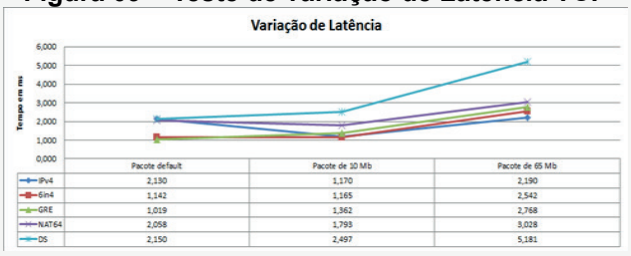
Figura 08 – Teste de latência TCP



Fonte: o autor (2017)

De acordo com a Figura 08, os testes de latência com o protocolo TCP com o tamanho de pacote padrão, as técnicas de tunelamento obtiveram um melhor desempenho com uma ligeira vantagem do GRE sobre o 6in4, sendo que as técnicas de Tradução e Tunelamento obtiveram desempenho semelhante ao IPv4.

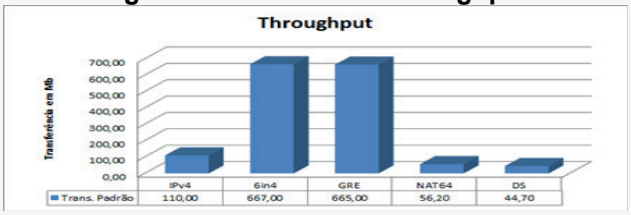
Figura 09 – Teste de variação de Latência TCP



Fonte: o Autor (2017)

De acordo com a Figura 09, nos testes com variação de latência com três tamanhos de pacotes diferentes, as técnicas de tunelamento não só obtiveram o melhor tempo, como também apresentaram a menor variação com ligeira vantagem do 6in4 para o GRE, sendo que as técnicas de Tradução e Pilha Dupla tiveram desempenho inferior ao IPv4 nativo e apresentaram também uma maior variação, com a técnica de Pilha Dupla apresentou o pior resultado.

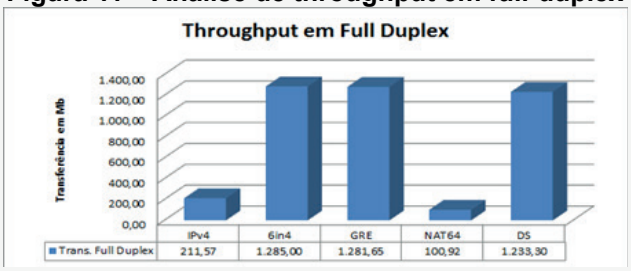
Figura 10 – Análise de throughput



Fonte: o Autor (2017)

De acordo com a Figura 10, o throughput que é a capacidade de transferência de dados da rede, a técnicas de Tunelamento obtiveram um desempenho bem superior às demais analisadas, com uma ligeira vantagem do 6in4 sobre o GRE, sendo que a técnica de Pilha Dupla obteve o pior resultado, inferior inclusive ao IPv4 nativo.

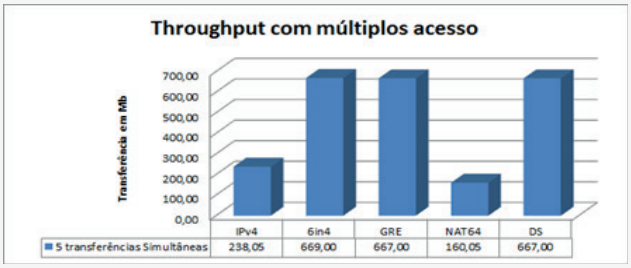
Figura 11 – Análise de throughput em full-duplex



Fonte: o Autor (2017).

De acordo com a Figura 11, a capacidade da rede operando em modo *full- duplex*, capacidade de enviar e receber dados simultaneamente, as técnicas de Tunelamento obtiveram pequena vantagem sobre a Pilha Dupla com o 6in4 obtendo o melhor desempenho e a técnica de Tradução obteve o pior desempenho, inferior inclusive ao IPv4 nativo.

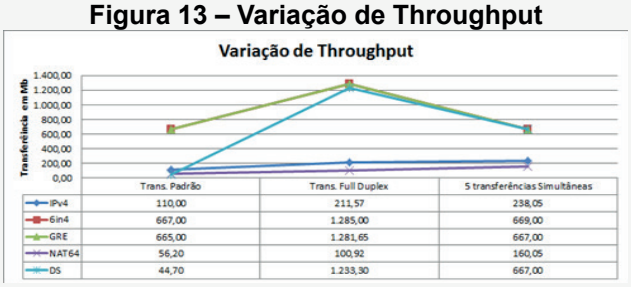
Figura 12 – Análise de throughput com múltiplos acessos simultâneos



Fonte: o Autor (2017).

De acordo com a Figura 12, a capacidade da rede operando com cinco acessos simultâneos com um host da rede que simulou um servidor, a técnica de Tunelamento 6in4 obteve o melhor desempenho com uma pequena diferença para o GRE e a Pilha Dupla, a técnicas de Tradução obteve o pior desempenho, inferior ao alcançado com IPv4 nativo.

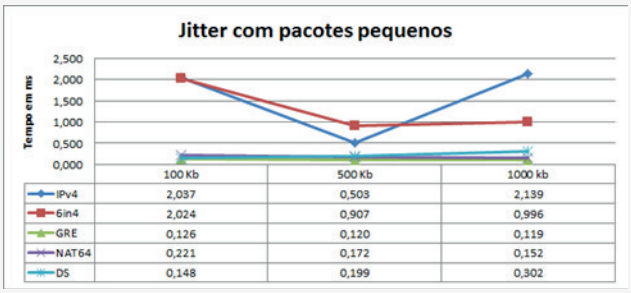
Figura 13 – Variação de Throughput



Fonte: o Autor (2017).

De acordo com a Figura 13, a variação de throughput entre os modos de operação simples, full-duplex e com cinco acessos simultâneos, o IPv4 obteve a menor variação, mas sempre com as piores taxas, dentre as técnicas de transição as de Tunelamento obtiveram o melhor desempenho neste quesito, seguido pela Pilha Dupla.

Figura 14 – Análise de Jitter com pacotes pequenos



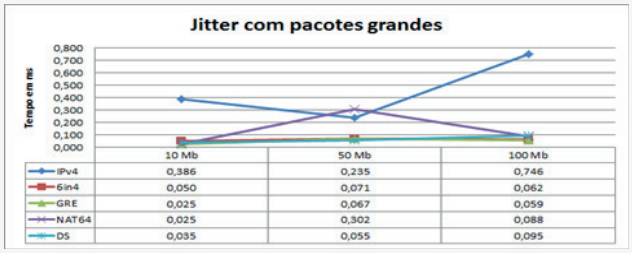
Fonte: o Autor (2017).

De acordo com a Figura 14, nos teste com UDP com pacotes de 100 Kb, 500 Kb e 1.000 Kb a taxa do Jitter, a técnica de Tunelamento GRE obteve o melhor desempenho com uma pequena vantagem sobre a Pilha Dupla, seguido pela técnica de Tradução, sendo que o 6in4 obteve o pior desempenho comparado com outras técnicas sendo

V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

melhor somente IPv4 além de apresentar a maior variação com pacotes de tamanhos diferentes.

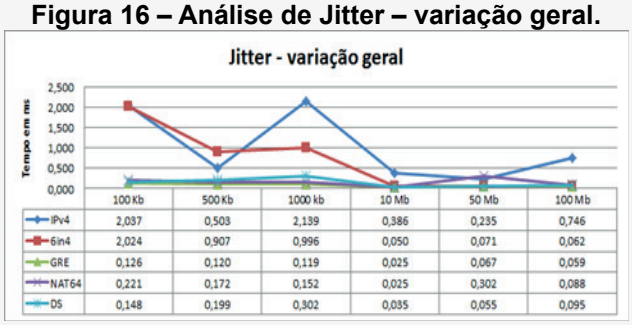
Figura 15 – Análise de Jitter com pacotes grandes.



Fonte: o Autor (2017).

De acordo com a Figura 15, nos teste com UDP com pacotes de 10 Mb, 50 Mb e 100 Mb a taxa do Jitter apresentou o melhor desempenho com a técnica de Tunelamento GRE com pequena vantagem para Pilha Dupla e 6in4, onde o IPv4 apresentou o pior desempenho e também a maior taxa de variação, sendo que das técnicas de transição a de Tradução teve o pior desempenho na variação do Jitter.

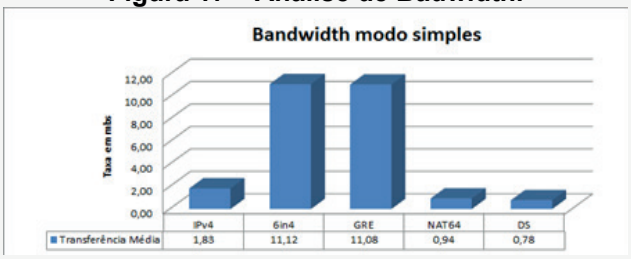
Figura 16 – Análise de Jitter – variação geral.



Fonte: o Autor (2017).

De acordo com a Figura 16, a variação geral do Jitter com todos os tamanhos de pacotes realizados nos testes de simulação, a técnica de Tunelamento GRE obteve o melhor desempenho, com uma diferença mínima para Pilha Dupla e Tradução, sendo que a técnica 6in4 obteve o pior desempenho das técnicas de transição.

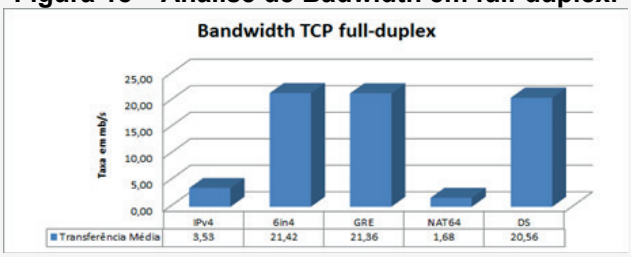
Figura 17 – Análise de Badwidth.



Fonte: o Autor (2017).

De acordo com a Figura 17, a largura de banda utilizada em modo TCP com a técnicas de Tunelamento foram muito superiores as demais, com as técnicas de Pilha Dupla e tradução sendo inferiores ao IPv4.

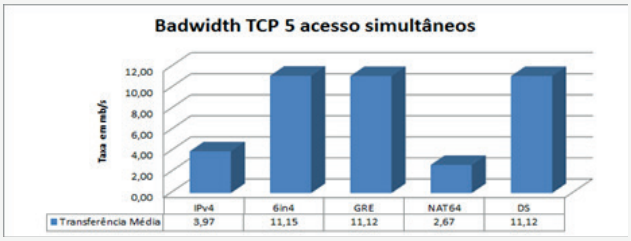
Figura 18 – Análise de Badwidth em full-duplex.



Fonte: o Autor (2017)

De acordo com a Figura 18, a largura de banda em TCP em modo full-duplex as técnicas de Tunelamento obtiveram os melhores resultados, com uma ligeira vantagem para a Pilha dupla, sendo que a técnica de Tradução obteve desempenho inferior ao obtido com IPv4.

Figura 19 – Análise de Badwidth múltiplos acesso.

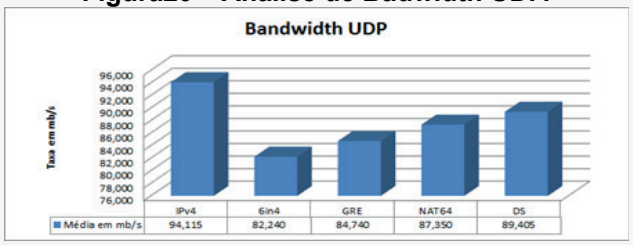


Fonte: o Autor (2017).

De acordo com a Figura 19, a largura de banda em TCP com múltiplos acessos simultâneos as Técnicas de Tunelamento obtiveram o melhor desempenho com ligeira vantagem para a Pilha Dupla, a técnica de

Tradução obteve o pior resultado, inferior ao IPv4.

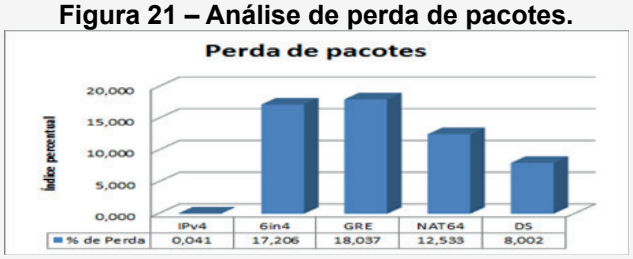
Figura20 – Análise de Badwidth UDP.



Fonte: o Autor (2017).

De acordo com a Figura 20, a largura de banda em modo UDP todas as técnicas de transição foram inferiores ao IPv4, sendo que a Pilha Dupla foi a que obteve o melhor desempenho, seguida pela Tradução e o pior resultado ficou com Tunelamento.

Figura 21 – Análise de perda de pacotes.



Fonte: o Autor (2017).

De acordo com a Figura 21, nos testes UDP utilizando a capacidade máxima da rede de 100 Mb, o IPv4 teve uma perda de pacotes insignificante, com relação as técnicas de transição a Pilha Dupla obteve o melhor desempenho, seguida pela técnica de Tradução, a técnicas de Tunelamento obteve o pior resultado, sendo que o GRE foi inferior ao 6in4.

Os resultados obtidos através dos testes realizados, as técnicas de Tunelamento e Pilha Duplas obtiveram resultados satisfatórios, a técnica de Tradução obteve resultados inferiores de desempenho na maioria dos quesitos comparados com as outras técnicas.

8. CONSIDERAÇÕES FINAIS

A necessidade de migração para IPv6 vai muito além da realidade do esgotamento de endereçamentos IPv4, pois há muitas novas tecnologias, como as relacionadas à IoT, VoIP, IPTV, streaming de áudio e vídeo por exemplo, em que é difícil imaginar sua implementação e o bom funcionamento sem utilização de IPv6.

Baseado nas características descritas sobre as técnicas analisadas e nos resultados obtidos, o objetivo de realizar uma comparação de funcionamento mensurando o uso das técnicas em ambiente virtualizado foi obtido êxito, e cuja pesquisa pode contribuir para um projeto de migração de redes IPv4 para IPv6.

A escolha de uma técnica de transição deve levar em consideração as características de cada técnica, a sua aplicabilidade, a estrutura da rede, os tipos de serviços utilizados, a escalabilidade da rede, o tempo estimado no processo de migração e os resultados obtidos com os testes realizados em ambiente simulado.

Em uma escala de prioridades para definição de uma técnica de transição a primeira opção deve ser a Pilha Dupla por ser uma solução viável em curto e médio prazo, por priorizar a utilização imediata do IPv6 em todos os hosts da rede, possuir facilidade de implementação por não requerer a realização de grandes mudanças na rede, pois o protocolo em uso continua em funcionamento podendo implantar o IPv6 para realizar a transição de forma gradativa, ser de rápida implementação, além de obter resultados satisfatórios nos testes em ambiente simulado. É importante salientar que o fato de existirem duas redes lógicas em uma mesma rede física, por causa das duas pilhas de protocolos, demanda maior organização e manutenção podendo comprometer a escalabilidade em um processo de migração em longo prazo.

A segunda opção deve ser da técnica

V. 9, n. 2, p. 24-39, 2018
http://www.unibalsas.edu.br/revista

de Tunelamento, por ser uma solução viável em curto, médio e longo prazo, pela simplicidade de implementação, não havendo a necessidade de utilização de IPv6 em todos os *hosts* da rede, requerendo implementação de Pilha Dupla somente nas bordas das redes, como firewall e roteadores, possui baixa complexidade de implementação e manutenção, não comprometendo a escalabilidade da rede em virtudes das regras se concentrarem somente bordas, além de obter bons resultados nos testes simulados, devendo atentar para o cuidado de adequação de hardware ao crescimento da rede para não comprometê-la, por demandar maior capacidade computacional em um eventual crescimento das redes.

E por último a técnica de Tradução deve ser preterida em detrimento das demais por não priorizar a migração da rede para Ipv6, possuir maior complexidade de implementação e manutenção, podendo ter a escalalidade comprometida além de não obter resultados satisfatórios comparada com outras técnicas de transição nos testes simulados.

9. REFERÊNCIAS

APINIC. **IPv6 Capable Rate by country (%)**. 2017. Disponível em: < https://stats.labs.apnic.net/ipv6 >. Acesso em 30.05.2017.

BRITO, Samuel Henrique Bucker. **IPv6 - O Novo Protocolo da Internet**. São Paulo--SP: Novatec Editora, 2013.

IANA. **IPv4 Address Space Registry**. 2017. Disponível em: <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml >. Acesso em: 01.06.2017.

IANA. **Number Resources.** 2017. Disponível em:<https://www.iana.org/numbers>. Acesso em: 01.06.2017.

IPv6.br. **Funcionalidades Básicas**. 2012. Disponível em: <http://www.IPv6.br/post/funcionalidades-basicas>. Acesso em: 16.03.2017.

IPv6.br. **Introdução**. 2012. Disponível em: <http://IPv6.br/post/introducao>. Acesso em: 06.03.2017.

IPv6.br. **Transição**. 2012. Disponível em: <http://www.IPv6.br/post/transicao>. Acesso em: 16.03.2017.

HUSTON, G. **IPv4 Address Report.** 2017. Disponível em: <http://www.potaroo.net/tools/ipv4/>. Acesso em 01.06.2017.

LACNIC. **Política de Designação e Alocação de endereços IPv6**. Disponível em: <http://www2.lacnic.net/documentos/politicas/chapter-4-pt.pdf>. Acesso em: 01.06.2017.

MOREIRAS, A. et al. **Laboratório de IPv6** – Aprenda na prática usando um emulador de redes. São Paulo: Novatec Editora, 2015.

RFC 1550. **Next Generation (IPng) White Paper Solicitation**. 1993. Disponível em: <https://tools.ietf.org/html/rfc1550 >. Acesso em: 15.05.2017.

RFC 1918. **Address Allocation for Private Internets**. 1996. Disponível em: < https://tools.ietf.org/html/rfc1918>. Acesso em: 09.03.2017.

RFC 1981. **Path MTU Discovery for IP version 6**. 1996. Disponível em: <https://tools.ietf.org/html/rfc1981>. Acesso em: 15.05.2017.

RFC 2784. **Generic Routing Encapsulation (GRE)**. 2000. Disponível em: <https://tools.ietf.org/html/rfc2784>. Acesso em: 15.04.2017.

RFC 3022. **Traditional IP Network Address**

Translator (Traditional NAT). 2001. Disponível em: <https://www.ietf.org/rfc/rfc3022.txt>. Acesso em: 11:03.2017.

RFC 3053. **IPv6 Tunnel Broker**. 2001. Disponível em: <https://tools.ietf.org/html/rfc3053>. Acesso em: 05.05.2017.

RFC 3056. **Connection of IPv6 Domains via IPv4 Clouds**. 2001. Disponível em: < https://tools.ietf.org/html/rfc3056>. Acesso em 29.04.2017.

RFC 3596. **DNS Extensions to Support IP Version 6**. 2003. Disponível em: <https://tools.ietf.org/html/rfc3596>. Acesso em: 15.05.2017.

RFC 4213. **Basic Transition Mechanisms for IPv6 Hosts and Routers**. 2005. Disponível em: < https://tools.ietf.org/html/rfc4213 >. Acesso em: 20.05.2017.

RFC 4214. **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)**. 2005. Disponível em <https://tools.ietf.org/html/rfc4214 >. Acesso em 30.09.2017.

RFC 4301. **Security Architecture for the Internet Protocol**. 2005. Disponível em: < https://tools.ietf.org/html/rfc4301>. Acesso em: 25.05.2017.

RCF 4443. **Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification**. 2006. Disponível em: <https://tools.ietf.org/html/rfc4443>. Acesso em: 15.05.2017.

RFC 4632. **Classless Inter-domain Routing (CIDR):** The Internet Address Assignment and Aggregation Plan. 2006. Disponível em: <https://www.ietf.org/rfc/rfc4632.txt>. Acesso em: 18.05.2017.

RFC 6146. **Stateful NAT64**: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. 2011. Disponível em: <https://tools.ietf.org/html/rfc6146>. Acesso em: 12.04.2017.

RFC 6147. **DNS64**: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. 2011. Disponível em: <https://tools.ietf.org/html/rfc6147>. Acesso em: 12.04.2017.

RFC 6333. **Dual Stack Lite (DS-Lite)** - Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. 2011. Disponível em: < https://tools.ietf.org/html/rfc6333> Acesso em: 15.05.2017.

TANENBAUM, Andrew S. WETHERALL, David. **Redes de Computadores**. 5ª ed. Rio de Janeiro: Pearson, 2003.

TORRES, Gabriel. **Redes de Computadores – Versão Revisada e Atualizada**. 2ª Edição Limitada. Rio de Janeiro, 2016.