IMPLANTAÇÃO DO PROTOCOLO IPV6 EM UM LABORATÓTIO DE INFORMÁTICA NA FAI FACULDADES

Alexandre Hentges Kaspary[1], Aléssio Inácio Cagliari[2]

RESUMO

Com o aumento considerável da utilização de internet no mundo inteiro, precisou-se buscar um protocolo que pudesse satisfazer esta demanda. Após anos de estudo e testes, foi lançado a sexta versão do protocolo IP, ou IPv6. Atualmente a migração do IPv4 para IPv6 está sendo feita de modo gradativo, permitindo uma melhor adaptação tanto por parte de provedores de internet e usuários finais, e após a migração completa, o protocolo anterior será desabilitado e, portanto, tornando-se obrigatório essa migração. A partir dessa obrigatoriedade, buscou-se antecipar a migração em um laboratório de informática da FAI Faculdades de Itapiranga-SC, podendo determinar as dificuldades e pontos fracos que podem surgir em uma migração de porte maior.

Palavras chave: IPv6. Laboratório. Internet.

ABSTRACT

With the considerable worldwide increase in the use of Internet, a protocol that could meet this demand had to be sought. After years of study and testing the sixth version of the IP protocol was released, or IPv6. Currently the migration from IPv4 to IPv6 is being made in a gradual way, allowing better adaptation by both Internet service providers and end users, and after complete migration, the previous protocol will be disabled and therefore, making this migration mandatory. From this obligation, we sought to anticipate the migration in a computer lab of FAI Faculdades de Itapiranga-SC, thus being able to determine the difficulties and weaknesses that can arise in a larger migration.

Key words: IPv6. Lab. Internet.

1 INTRODUÇÃO

O aumento do uso da internet causou o esgotamento do protocolo IPV4, e tornou-se necessário o desenvolvimento de um protocolo que satisfizesse essa necessidade. Nesse projeto, busca-se mostrar a história da internet, desde seu desenvolvimento até os dias atuais, bem como, descrever as principais diferenças entre os protocolos, seu funcionamento, tipos de endereços de cada protocolo, problemas de segurança que cada um possui e outras características.

[1] Acadêmico do curso de Gestão da Tecnologia da Informação da FAI Faculdades. E-mail: alexandre.kaspary@hotmail.com.

[2] Mestrando em Ensino Cientifico e Tecnológico pela Universidade Regional Integrada do Alto Uruguai e das Missões – URI e professor do curso de Gestão da Tecnologia da Informação da FAI Faculdades. E-mail: alessio.gti@seifai.edu.br.

Com a chegada do IPV6, foram constatados vários problemas de segurança que não existiam na versão anterior, sendo necessário o desenvolvimento de métodos de resolver os mesmos, que também serão citados no projeto.

Com o esgotamento do IPV4, torna-se obrigatório a migração para o novo protocolo, serão aqui mencionadas as principais técnicas de migração, como funcionam e em que casos devem ser utilizados. Após a produção da parte teórica, será feita a implantação do IPV6 em um laboratório de informática na FAI Faculdades de Itapiranga – SC, e também, serão desenvolvidos testes que poderão dar informações mais precisos quanto ao seu funcionamento.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, discorre a fundamentação teórica, sendo tratados os seguintes assuntos: história da internet, protocolos e serviços de rede e segurança em redes informatizadas.

2.1 EVOLUÇÃO DA INTERNET

A história da evolução da internet envolve muitos fatores: políticos, sociais e tecnológicos. Durante essa evolução, a internet sofreu inúmeras alterações, sempre se adaptando às necessidades de cada época. Desde fins militares até um simples meio de comunicação, com certeza a internet é algo que revolucionou a forma que vivesse.

2.1.1 História

No ano de 1958, o governo dos Estados Unidos criou um novo setor, chamado de ARPA (*Advanced Research Project Agency*) ou então Agência de projetos de pesquisa avançada. Este setor tinha como objetivo, fazer com que os EUA mantivessem a superioridade tecnológica e alertar eventuais avanços tecnológicos de outras nações. (GOETHALS, 2000)

A ARPA era diretamente associada ao Departamento de Defesa Norte-Americano, e possuía como projeto principal, construir uma rede de comunicação que interligasse os pontos críticos do sistema de defesa dos EUA, permitindo troca de informações mais rápidas e seguras.

Entre as principais características exigidas pelos Norte-Americanos, era a descentralização da rede, possibilitando que em casos de ataque, apenas a região que sofreu a ofensiva seria prejudicada com problemas de comunicação através dessa rede. Outra

característica era que todo nó (qualquer equipamento que pode ser conectado à rede) pudesse enviar, receber e repassar as informações da rede. (CARVALHO, 2006)

Alguns fatos fundamentais para que a evolução da internet acontecesse, e entre os principais estão: Em 1969 foi desenvolvida a ARPANET para satisfazer as necessidades do governo, uma conexão entre computadores que dividia as informações em pacotes e os enviava instantaneamente, e assim, juntava os pacotes no destino formando as informações enviadas. O envio poderia ser feito através de inúmeras rotas, permitindo o funcionamento do restante da rede em casos de ataques. Em 1971, a ARPANET já contava com aproximadamente 20 máquinas da própria ARPA interligadas. Em 1972 começou a ser pensado no conceito *interworking*, uma forma de interligar várias redes da ARPA, e posteriormente, em 1973, surgiu o nome INTERNET. Foram criadas mais duas redes, a BitNET para universidades e a CSNET para a área científica, e no começo da década de 80, conseguiram interligar as três redes e formar uma só rede aumentando a aplicabilidade da mesma. Após a junção das redes, em 1982 foi definido um padrão de protocolo para a comunicação entres as máquinas da rede, o TCP-IP. Esse protocolo identifica cada nó da rede com um endereço único, podendo assim qualquer nó se comunicar com qualquer outro. Em 1990 os Norte-americanos abriram o primeiro *Internet Service Provider* que disponibilizava a *internet* comercialmente no país, e assim dando fim a ARPANET. Em 1989, o físico britânico Tim Berners-Lee começou o projeto de desenvolvimento de um novo sistema de informação, no qual foi chamado de *World Wide Web* abreviado como WWW, e sendo apresentado em 1991. Antes era apenas possível efetuar troca de mensagens e transmissão de arquivos em tempo real, e com o WWW formou-se a possibilidade de criação de servidores de dados, podendo conter arquivos diversos, como texto, imagens e vídeos, tornando-os disponíveis a qualquer momento. (GOETHALS, 2000)

Outra característica do WWW envolvia o desenvolvimento de interfaces gráficas que poderiam ser utilizadas pelos usuários independentemente da plataforma que utilizavam, podendo ser Windows, Macintosh ou Unix. A internet começou disponibilizando poucos serviços, como o e-mail sendo o mais usado, o FTP para transferência de arquivos e o *Telnet* para poder acessar sessões de outros hosts da rede. No começo da implantação da internet o protocolo TCP-IP, então chamado de IPV4, contava com cerca de 4 bilhões de endereços diferentes disponíveis. Essa quantidade de endereços disponíveis era exagerada até os primeiros anos da década de 90, mas com a popularização da internet, mostrou-se que em pouco tempo surgiriam problemas com a falta de endereços disponíveis, tendo como necessidade buscar formas de resolver ou ao menos amenizar esse problema. (FLORENTINO, 2012)

2.1.2 Distribuição de endereços

O protocolo TCP-IP não permite a duplicação de endereços, ou seja, cada endereço é único no mundo inteiro. Para que se possa fazer esse controle, existe desde a ARPANET uma competência que gerencia a distribuição de IPs, sendo denominada de *Internet Assigned Numbers Authority*, ou então simplesmente IANA.

Atualmente, a ICANN (*Internet Corporation for Assigned Names and Numbers*) é responsável por realizar a função da IANA. Para facilitar o gerenciamento dos endereços ao redor do mundo, existe um sistema hierárquico do IANA, tendo órgãos regionais e alguns nacionais que auxiliam nessa função.

Figura 01: Hierarquia de distribuição de endereços

Fonte: http://caída.org (2015)

Como demonstra a Figura 01, existem cinco RIRs (*Regional Internet Registries*), o APNIC que faz o gerenciamento na Oceania e Ásia, o AFRINIC na África, o ARIN na América do Norte, o RIPE na Europa e uma certa parte da Ásia e o LACNIC que fica responsável pelo Carine e América Latina. Cada uma dessas entidades pode ter regras diferentes sobre a distribuição de endereços, podendo variar conforme disponibilidade e necessidade dos mesmos.

No caso do Brasil, quem faz esse gerenciamento é uma organização nacional, o NIC.br, o principal motivo disso, é que no Brasil, a internet chegou bem antes da criação do LACNIC, gerando a necessidade de criação de um órgão responsável. Posteriormente o NIC.br contribuiu com a fundação do LACNIC. (FLORENTINO, 2012)

Quando necessário, provedores de internet brasileiros entram em contato com o NIC.br fazendo a solicitação de blocos de endereços. Quando existem blocos disponíveis, o NIC.br fornece os mesmos sob determinados requisitos que o provedor deve atender. No caso de falta de blocos, o NIC.br faz a solicitação diretamente a LACNIC. Contudo, o IANA decretou o fim de seu estoque no dia 03 de fevereiro de 2011. O LACNIC conseguiu, com sua política de

distribuição, mantendo disponibilidade de endereços por mais três anos, acabando no dia 10 de junho de 2014. (IPV6.BR, 2015).

2.1.3 Esgotamento do IPV4

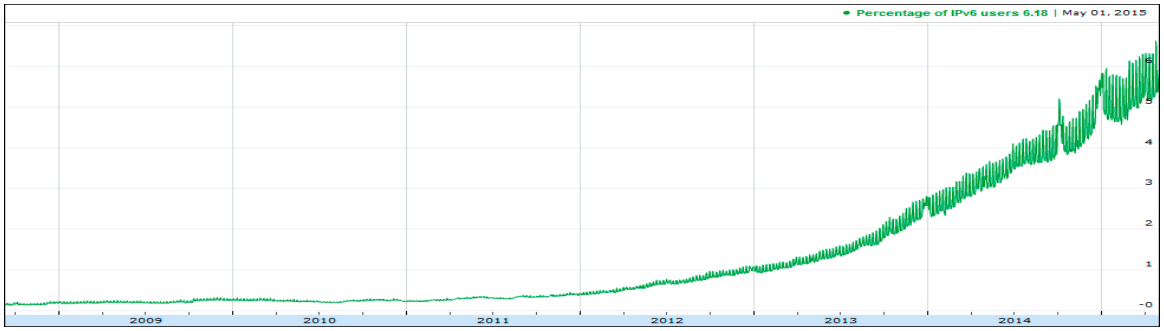
Com a quantidade exagerada de endereços IPV4 disponíveis (4 bilhões) antes da popularização da internet, não existia a preocupação com a possibilidade de esgotamento dos mesmos, fazendo assim a venda de grandes blocos para empresas privadas como HP, IBM, Apple, MIT, Ford e Xerox, disponibilizando algo próximo de 16 milhões de endereços para cada empresa, gerando assim um grande desperdício de IPs. Atualmente, o governo dos EUA possui 12 faixas de endereços IP, correspondente a mais do que a totalidade de endereços da América latina (IPV6.BR, 2015). Então chega-se a conclusão que a maior culpada com esse rápido término dos endereços IPV4 é a falta de preocupação que houve na distribuição dos blocos. Porém, ainda assim a falta de endereços não estaria resolvida.

2.1.4 Progresso de migração

O IPV6 foi desenvolvido de tal forma que não possui compatibilidade com o IPV4, porém ambos podem ser usados simultaneamente no mesmo equipamento sem qualquer problema. A princípio, o plano era fazer uma transição gradativa, mantendo os dois protocolos ativos, e assim desligar o IPV4 quando a implantação do IPV6 estivesse concluída.

O IPV6 não traz grandes melhorias se comparado à versão anterior, a única característica que se sobressai é o aumento da quantidade de endereços disponíveis. Os gestores de TI já estavam conscientes do IPV6 na década passada, porém, teriam que fazer investimentos sem benefícios a curto prazo, e assim o processo de migração ficou deixado de lado (BRITO, 2013).

Figura 02: Uso do IPV6 no mundo



Fonte: http://6lab.cisco.com/stats (2015)

Como demonstra o gráfico da Figura 02, a quantidade de usuários que já estão utilizando o IPV6 no mundo ainda é pequena. O gráfico demonstra que no dia 01 de maio de 2015, apenas 6,18% dos usuários mundiais possuem o protocolo ativado e operando. A porcentagem de usuários dobrou se comparado ao mesmo período do ano passado, e se a implantação continuar nesse ritmo, estima-se que em 4 anos todos devem ter o IPV6 funcionando.

No Brasil o processo também está atrasado. Desde o começo de 2015 houve aumento de usuários que já vem usando o novo protocolo e esse índice vem aumentado frequentemente.

Figura 03: Uso do IPV6 no Brasil

Fonte: http://6lab.cisco.com/stats (2015)

No caso do Brasil, apenas 1,45% dos usuários já estão utilizando o IPV6, o que pode parecer pouco, mas se compararmos o mês de janeiro de 2015 com maio de 2015, teve aumento de 14 vezes na quantidade usuários de IPV6, como demostrado no gráfico da Figura 03.

2.2 ESTRUTURA DO IPV6

2.2.1 Diferenças do IPV4 e IPV6

Com a chegada do novo protocolo, houve algumas mudanças na estrutura de um pacote IPV6 e principalmente mudanças na forma que o mesmo é escrito, permitindo assim resolver o problema da falta de endereços disponíveis que é enfrentado atualmente com IPV4 e melhorar a qualidade e agilidade no transporte de informações.

2.2.1.1 Estrutura do IPV4

O protocolo IPV4 tem como característica principal o comprimento de seus endereços, sendo definido em 32bits e separado em quarto octetos de 8 bits cada, que pode gerar algo

entorno de 4,3 bilhões de combinações diferentes. Para facilitar, os endereços são apresentados em forma decimal ao invés de forma binária. Um exemplo de endereço IPV4 é 192.168.1.1, que escrito em binário é 11000000. 10101000. 00000001. 00000001. (BRITO, 2013)

Todos os endereços, tanto IPV4 quanto o IPV6, possuem uma máscara de rede. Esta máscara de rede é responsável por separar a parte da internet pública, subrede e hosts.

No caso da subrede por exemplo, existe o IP 192.168.1.1, se usada uma máscara 255.255.255.0, os 24 primeiros bits identificam a rede com 192.168.1, e os 8 bits finais identificam os hosts da subrede. 8 bits representam um total de 256 números possíveis, podendo assim uma rede /24 (255.255.255.0) poder contar com 255 IPs diferentes. Usando o exemplo acima, na subrede funcionarão apenas os hosts que possuem seu IP entre os números 192.168.1.0 e 192.168.1.255.

No IPV4 existem três faixas de endereços destinados a uso exclusivo em redes privadas. A RFC1918 determina que as faixas 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16 podem ser usadas em subredes.

Os endereços IPV4 foram separados em classes, a classe A corresponde a endereços de 1.0.0.1 até 126.255.255.253, a classe B 128.0.0.1 até 191.255.255.254 e a classe C de 192.0.0.1 à 223.255.255.254. Os demais endereços foram denominados em outras classes para ser usadas em outras necessidades específicas.

2.2.1.2 Estrutura do IPV6

Com e chegada do IPV6, foram várias as mudanças feitas no protocolo, porém a diferença mais notável foi o tamanho de um endereço, passando de 32 para 128 bits.

A primeira confusão que não pode existir é que uma cadeia de 128 bits não representa apenas quatro vezes mais endereços do que uma cadeia de 32 bits, afinal, o crescimento de combinações possíveis duplica a cada novo bit adicionado na cadeia. Com o aumento do tamanho do endereço, a cada bit adicionado, a possibilidade de endereços dobra, passando assim de 4,3 bilhões de endereços no IPV4 para cerca de 340 undecilhões no IPV6. (BRITO, 2013)

Como mencionado, o endereço IPV4 é escrito de forma decimal, ou seja, contem números de 0 a 9, já o IPV6 contém caracteres hexadecimais, isto é, além dos números de 0 a 9, também poderão ser encontrados em sua notação as letras de A até F.

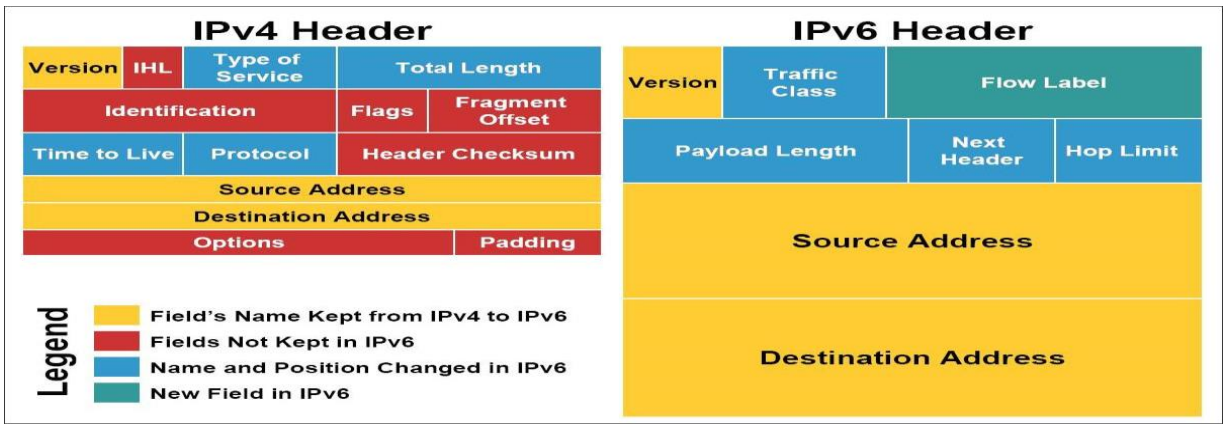
Os 128 bits do IPV6 foram divididos em oito partes iguais de 16 bits cada, sendo que a separação de cada parte é feita por dois pontos. Cada parte do endereço é denominado de

hexadecatetos ou duplo-octetos. O exemplo a seguir mostra a notação de um endereço IPV6: 2001:0DB8:AD1F:22E2:C3DE:CAEE:F0CA:84C1. Nos grupos de 4 caracteres, os zeros (0) à esquerda podem ser ocultados como forma de abreviação. Outro caso em que se pode usar a abreviação de endereço é quando está presente um conjunto de quatro zeros (0000), podendo ser substituídos por apenas por 1 zero ou então dois pontos (:), porém essa última técnica pode ser usada apenas uma vez dentro de um endereço para evitar ambiguidade. A seguir, uma forma de como se pode abreviar um endereço utilizando a técnica acima citada: 2001:0DB8:0000:0000:057A:1200:0000:0000 pode ser reescrito da seguinte forma 2001:DB8::57A:1200:0:0. Nota-se que o uso de dois pontos seguidos (::) só pode ser usado uma vez na abreviação de um endereço, mesmo contendo mais zeros. (MOREIRAS, 2012)

2.2.1.3 Cabeçalho do IPV6

Para que as informações possam trafegar na rede com um melhor funcionamento, todas as informações são divididas em partes denominados de pacotes de IP. Esses pacotes possuem uma estrutura com partes de tamanhos variados em que cada uma possui uma função específica no transporte de informações. Essa estrutura dos pacotes é chamada de cabeçalho, e entre os principais campos do cabeçalho IPV4 estão: A versão do pacote, que informa se o pacote corresponde a um pacote IPV4 ou IPV6; O comprimento do cabeçalho, que identifica onde as informações que o pacote transporta começam; Tipo de Serviço, identificando o tipo de pacote para poder definir sua prioridade; IPs de origem e destino; Dados; TTL, que é o tempo de vida do pacote, impedindo assim o trafego infinito do pacote em caso de falha de entrega, evitando congestionamento da rede; Entre outros campos menos importantes ou menos usados.

Figura 04: Diferenças de cabeçalhos



Fonte: http://www.datacentertalk.com (2015)

No IPV6, o protocolo mantém seus principais campos, porém alguns foram removidos, como o IHL, que guardava o tamanho total do cabeçalho, que foi removido e definido um valor fixo de 40 bits para o mesmo, assim como outros que foram vistos como desnecessários no funcionamento da internet atual. Apenas um campo foi adicionado no IPV6, o Flow Label, permitindo identificar pacotes que precisam de tratamento especial por roteadores e demais equipamentos de rede. Outros foram removidos, adicionados ou alterados, conforme Figura 04.

2.4 MÉTODOS DE MIGRAÇÃO

Quando o IPV6 foi lançado, já era esperado que a migração seria um processo que poderia levar anos até que esteja concluída. Sendo assim, foram desenvolvidas diversas opções de migração, cada uma se adaptando a cada tipo de rede, provedor e cliente. Cada uma deve ser analisada e escolhida a que melhor se adequa as necessidades. Todos os métodos de migração podem ser classificados em três tipos, a pilha dupla, o túnel e a tradução. (BRITO, 2013)

2.4.1 Pilha dupla

A pilha dupla consiste em instalar e ativar o IPV4 e o IPV6 nas mesmas máquinas, fazendo com que duas redes se criem naquele espaço. Este processo de migração é o mais recomendado, pois permite que o IPV4 possa ser simplesmente desativado quando o IPV6 já estiver difundo no mundo inteiro. Porém esse método traz uma certa dificuldade na gestão da rede, já que de certa forma serão duas redes, com firewalls de regras diferentes, dois protocolos diferentes, necessidades e problemas diferentes. (BRITO, 2013)

Porém um problema que existe é a falta de provedores que fornecem faixas de endereços IPV6 para os seus clientes, impossibilitando que a pilha dupla seja executada. Vendo essa necessidade foram criadas outras formas de transição, como o tunelamento e a transição, que resolvem o problema do fornecimento de IPV6 pelos provedores.

2.4.2 Tunelamentos

Quando o uso da pilha dupla não se torna possível, torna-se necessário a busca de novas formas de conseguir fazer a migração para o IPV6. O tunelamento faz o encapsulamento de pacotes IPV6 em pacotes IPV4, podendo assim trafegar em redes de protocolo IP da quarta versão. Essa técnica pode de 6in4 e determinada pela RFC4213. (MOREIRAS, 2012)

2.4.2.1 Túneis 6over4

Os túneis 6over4 (definido pela RFC2529) são criados manualmente e tem como objetivo principal permitir que uma conexão IPV6 passe por uma rede IPV4. Essa técnica usa o encapsulamento do 6in4 que também pode ser usado por outras técnicas de migração. (MOREIRAS, 2012)

A criação do túnel consiste em configurar os endereços IP de quarta versão que serão a origem e o destino destes pacotes. Após o recebimento do pacote, o mesmo será descapsulado e enviado para ser tratado adequadamente.

2.4.2.2 Túneis GRE

Definido pela RFC2784, o GRE é um túnel criado pela Cisco com o intuito de realizar o encapsulamento de diferentes tipos de protocolos. Esse sistema de túnel é suportado pela grande maioria dos sistemas operacionais modernos e outros equipamentos de redes encontrados atualmente. A forma e funcionamento do GRE é simples, parecido com 6over4. Ele pega os pacotes IPV6 e adiciona um cabeçalho IPV4 e um de GRE e o envia ao IP destinatário. Na chegado do pacote GRE, faz-se a remoção dos cabeçalhos IPV4 e GRE, restando apenas o pacote original que pode ser tratado adequadamente. Porém assim como o 6over4, a configuração desse túnel deverá ser feita de forma manual (MOREIRAS, 2012)

2.4.2.3 Tunnel Broker

O *tunnel broker* (RFC3053) é um serviço oferecido geralmente por grandes provedores de acesso. Ele é recomendado para os usuários que querem usar o IPV6 sem ter muito serviço de configurá-lo e sem ter altos custos. Para usufruir deste serviço, o usuário deve realizar um cadastro junto a empresa fornecedora, e toda a criação do túnel se dará de forma automática. (BRITO, 2013) O único serviço de *tunnel broker* no Brasil é o SixXS, que é oferecido de forma gratuita e está presenta em todo o mundo.

2.4.2.4 ISATAP

O ISATAP é uma técnica de migração que liga roteadores e outros dispositivos. Sua utilização se dá principalmente dentro de organizações onde já existe o fornecimento de IPV6

numa extremidade, porém os dispositivos não estão preparados para suportar o mesmo. Essa técnica é determinada pela RFC5214, e para a sua criação é utilizada a RFC4213, que define o protocolo 41 ou 6in4. (BRITO, 2013)

2.4.2.5 6to4

Por meio do 6to4 qualquer computador com um IPV4 válido poderia funcionar como uma extremidade de um conjunto de túneis automáticos e prover todos um bloco IPV6 /48 para ser distribuído e usado em uma rede. O 6to4 é definido pela RFC3056 e é uma das formas de transição mais antigas usadas atualmente. A função de cliente e roteador podem estar presentes num mesmo dispositivo, desde que tenha um endereço IP válido. (MOREIRAS, 2012)

2.4.3 Traduções

Durante a fase de esgotamento surgiram, além dos túneis, outros métodos que facilitam a implantação do IPV6 nas redes, e entre esses métodos estão as traduções.

2.4.3.1 AFT

O AFT (*Address Family Translation*) é um método que possui a capacidade de converter um endereço IPV4 para IPV6 (NAT46) ou vice-versa (NAT64). Comumente esta técnica está diretamente interligada com a tradução de DNS (*Domain Name Server*), que também possui as técnicas DNS64 e DNS46. (BRITO,2013)

3 PROCESSOS METODOLÓGICOS

Este capítulo abrange os procedimentos metodológicos utilizados para o desenvolvimento da pesquisa. Dessa forma, subdivide-se em tópicos específicos que tratam sobre caracterização da pesquisa, seleção da população e amostra, instrumentos de coleta de dados e análise e interpretação dos dados.

A pesquisa caracterizou-se quanto à natureza como teórica-empírico havendo coleta de dados através de atividades práticas desenvolvidas no laboratório de informática. Quanto ao tratamento de dados, caracteriza-se como uma pesquisa qualitativa.

Aos fins propostos, mostra como uma pesquisa exploratória, uma vez que busca proporcionar uma maior familiaridade com o problema e torná-lo explícito. Conforme sua conduta em relação aos dados, apresenta-se como uma pesquisa experimental, ou seja, busca-se através de experiências resolver o problema da pesquisa. O corpo de análise será diretamente voltado a FAI Faculdades, tendo como objetivo mostrar a importância do planejamento de migração para o IPV6. A pesquisa será baseada em dados primários e secundários. Será feito um levantamento de informações sobre o laboratório de informática, e será coletado material bibliográfico. Partindo da abordagem do problema e em relação ao tratamento dos dados levantados na empresa FAI Faculdades, pode-se especificar a pesquisa como caráter qualitativa, através de um contato com a empresa pesquisada, podendo vivenciar a realidade na mesma.

Os dados secundários adquiridos foram obtidos através de leituras e interpretação de publicação científica, livros, sites de internet entre outros dados disponíveis. Nesse estudo, foram analisadas informações necessárias para que pudesse fazer a elaboração do projeto.

4 DESENVOLVIMENTO

4.1 MIKROTIK

A Mikrotik é uma empresa de Letônia, fundada em 1995 com o objetivo de criar sistemas ISP (fornecedores de internet) sem fio e Routers. Atualmente, fornece tanto o software e hardware para conectividade à internet na maioria dos países do mundo. (MIKROTIK, 2015)

4.1.1 RouterOS

O Mikrotik RouterOs é um sistema operacional que tem ganho uma boa participação no mercado de Tecnologia da Informação, e isso acontece principalmente devido a sua robustez, estabilidade, facilidade de uso e as inúmeras funcionalidades que oferece. (BRASIL, 2015)

Alguns aspectos e funcionalidade do RouterOS são: Alta disponibilidade; Possibilidade de agregar interfaces; Pouco consumo de recursos de hardware; Suporte a RIP, OSPF e BGP; Acesso remoto por terminal ou sistema Windows e Web; Monitoramento em tempo real;Firewall; Hotspot;Filtro P2P; Otimizada para Wifi 802.11 a/b/g;Túneis; Gerência de banda;

4.1.2 RouterBoard

Em 1997 quando o RouterOS nasceu, o mesmo havia sido criado para ser instalado em hardware de computador convencional, mas em 2002 a Mikrotik decidiu criar seu próprio hardware para seu sistema operacional, e assim nasceu a marca RouterBoard. A RouterBoard basicamente é um minicomputador de baixo custo, que foi otimizado para tirar proveito de toda a capacidade do sistema operacional da Mikrotik. (MIKROTIK,2015)

O equipamento utilizado para realizar a implantação do IPv6 no laboratório de informática, trata-se de uma Mikrotik RouterBoard 2011iL, ou simplesmente RB2011iL.

Figura 05: RB2011iL

Fonte: http://routerboard.com/RB2011iL-IN (2015)

A RB2011iL foi desenvolvida para ser usada em ambientes internos e em diversos casos com grande quantidade de opções. Essa RB é um modelo básico que conta com 5 portas Fast Ethernet e 5 portas Gigabit. Como hardware essa RB conta com um processado Atheros MIPS de 600MHz e 64 MB de RAM.

4.2 SIXXS

Quando o provedor de internet não dispõe de conectividade IPv6, é necessário criar um túnel que faça a quebra dessa barreira, possibilitando a conectividade com o sexto protocolo e esses túneis são chamados de *tunnel brokers*. Este, permitem que uma rede isolada do IPv6 possa usar o mesmo, estimulando o crescimento do novo protocolo.

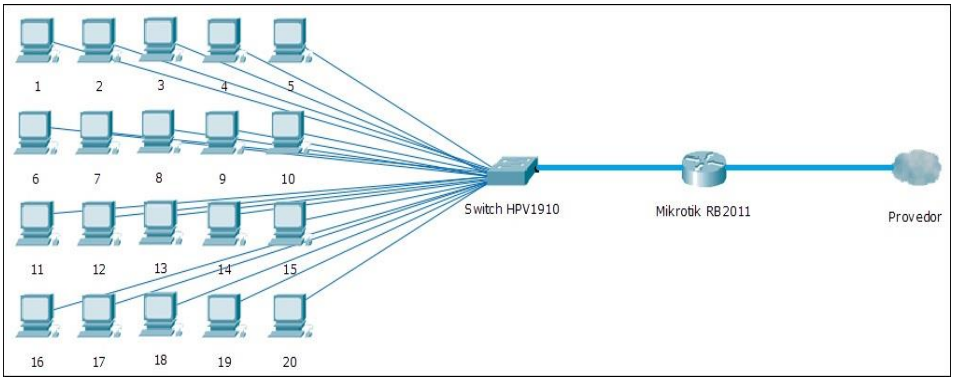
Quando é falado em *tunnel brokers* dois serviços são conhecidos mundialmente por fornecer esta opção, o Sixxs e o Huricanne Electric. Ambos podem ser usados de forma gratuita para realizar o encapsulamento e desencapsulamento do IPv6, porém no Brasil o Sixxs leva vantagem por ser o único a possuir servidor nesse país, aumentando a velocidade do túnel a ser feito com o serviço. O Sixxs é livre e sem fins lucrativos. Tem o objetivo de ajudar engenheiros

e administradores de redes encontrar um caminho para obter a conectividade IPv6 de forma rápida (SIXXS, 2015). Tanto o Sixxs[3] e o Huricanne[4] podem ser encontrados em seus sites.

4.3 LAYOUT DA REDE

Para realizar o processo de migração da rede para IPv6 foi necessário realizar uma adaptação na mesma. Tornou-se necessário a presença de um equipamento que pudesse realizar a encapsulamento dos pacotes IPv6, e como já mencionado, o equipamento escolhido foi a Mikrotik RB2011.

Figura 06: Layout da rede



Fonte: Dados do autor (2015)

A rede do laboratório conta com 20 computadores e todos estão conectados em um switch D-Link DES-1024D de 24 portas. Antes da migração o switch estava conectado diretamente com o servidor que provê a internet para a rede, mas para a migração foi necessário colocar a Mikrotik RB2011 entre eles e realizar as configurações de IPv4, e, portanto, a rede ficou com o layout apresentado na imagem acima.

A Mikrotik utilizada foi configurada com um endereço IPv4 válido em que os servidores da SixXS pudessem acessá-la sem qualquer tipo de problema, permitindo o funcionamento do túnel sem qualquer tipo de redirecionamento e abertura de portas no firewall da instituição.

[3] https://www.sixxs.net/
[4] http://he.net/

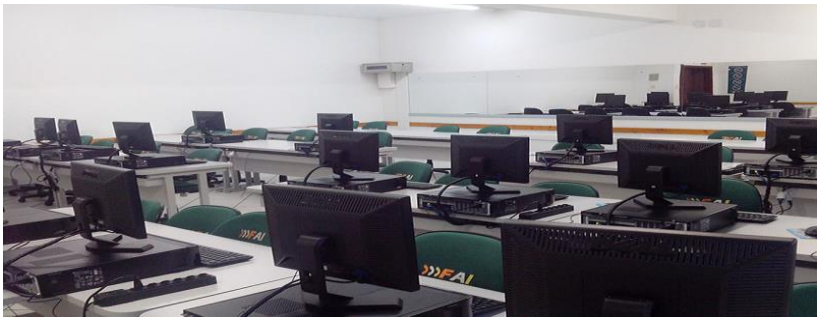
Figura 07: Mikrotik RB2011 instalada

Fonte: Dados do autor (2015)

Figura 08: Switch D-Link

Fonte: Dados do autor (2015)

Figura 09: Laboratório de informática

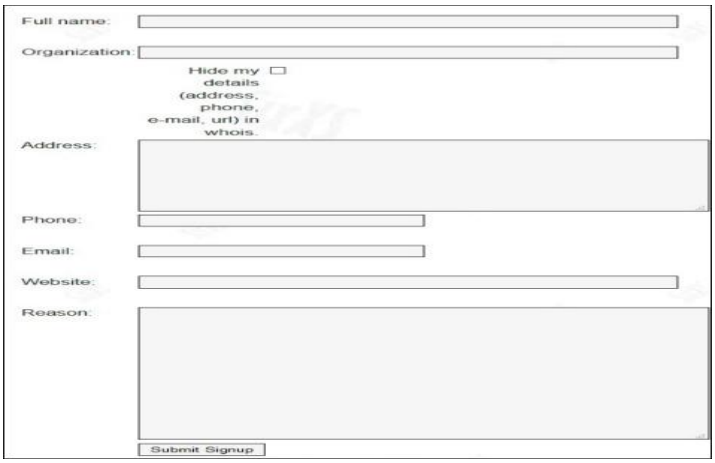


Fonte: Dados do autor (2015)

4.4 CADASTRO NO SIXXS

Para obter a conectividade IPv6 é necessário realizar um cadastro no Sixxs fornecendo informações como o nome, telefone, endereço, e-mail e motivo para a requisição do túnel IPv6.

Figura 10: Formulário de Cadastro



Fonte: https://www.sixxs.net/signup/ (2015)

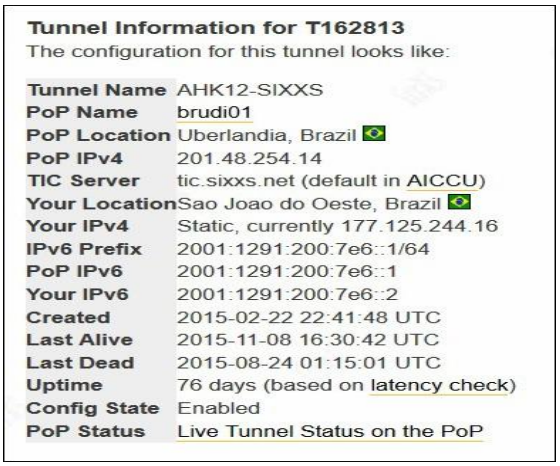
Após o término do cadastro, as informações de login foram enviadas ao e-mail cadastrado. Realizado o login, o próximo passo foi a requisição do túnel, repassando os dados da Mikrotik (Endereço IP).

Figura 11: Menu do sistema Sixxs

Fonte: https://www.sixxs.net (2015)

Após realizar a requisição do túnel demorou aproximadamente 24 horas para ser aprovado, e somente então as informações necessárias para a criação do túnel na Mikrotik foram fornecidas.

Figura 12: Informações para criação do túnel



Tunnel Information for T162813

The configuration for this tunnel looks like:

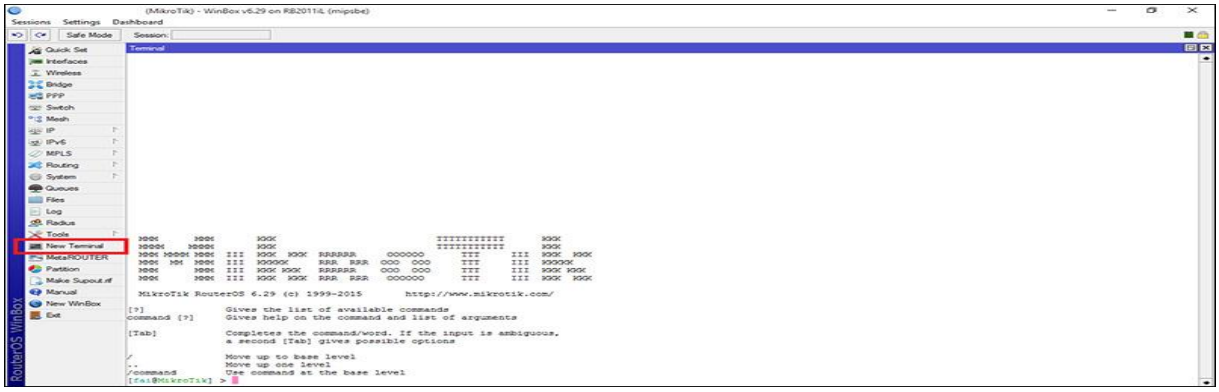
Tunnel Name	AHK12-SIXXS
PoP Name	brudi01
PoP Location	Uberlandia, Brazil
PoP IPv4	201.48.254.14
TIC Server	tic.sixxs.net (default in AICCU)
Your Location	Sao Joao do Oeste, Brazil
Your IPv4	Static, currently 177.125.244.16
IPv6 Prefix	2001:1291:200:7e6::1/64
PoP IPv6	2001:1291:200:7e6::1
Your IPv6	2001:1291:200:7e6::2
Created	2015-02-22 22:41:48 UTC
Last Alive	2015-11-08 16:30:42 UTC
Last Dead	2015-08-24 01:15:01 UTC
Uptime	76 days (based on latency check)
Config State	Enabled
PoP Status	Live Tunnel Status on the PoP

Fonte: https://www.sixxs.net (2015)

4.5 CONFIGURAÇÃO DA MIKROTIK

Para a configuração do túnel na Mikrotik a própria Sixxs disponibiliza um manual contendo todos os scripts necessários para criação do mesmo, sendo preciso apenas alterar para os dados repassados pelo Sixxs, como o bloco de endereços, gateway e outros dados. Para executar os scripts na Mikrotik basta acessá-la e procurar em seu menu esquerdo a opção “New Terminal” e na janela que se abre digitar os comandos e a cada linha executar dando “Enter”.

Figura 13: Terminal da Mikrotik



Fonte: Dados do autor (2015)

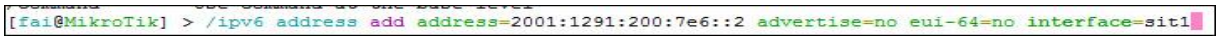
O primeiro comando repassado pelo Sixxs que foi executado tem a função de realizar a criação do túnel entre a Mikrotik e o servidor do Sixxs em Uberlândia, e para isto bastou apenas digitar no terminal o seguinte script:

Figura 14: Script para criação do túnel

Fonte: Dados do autor (2015)

Após a criação do túnel foi necessário adicionar uma faixa de endereços IPv6 referentes ao túnel criado, e isso foi possível executando o seguinte comando:

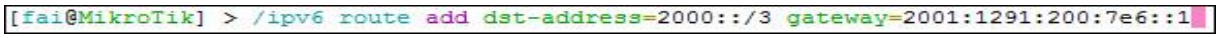
Figura 15: Comando para definir endereço IPv6



Fonte: Dados do autor (2015)

O terceiro comando é referente ao tipo de IPv6 que esses endereços pertencem. Ao criar o túnel, é necessário dizer que os endereços que farão parte dessa rede fazem parte do grupo dos endereços roteáveis, os 2000::/3, e necessário definir o gateway do túnel, e para isso foi preciso executar o seguinte comando:

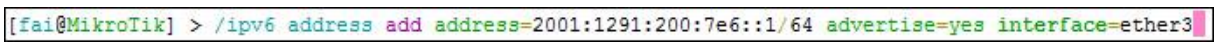
Figura 16: Definição da rota e gateway



Fonte: Dados do autor (2015)

O último passo necessário para que a configuração do IPv6 esteja completa, é definir o bloco de endereços para a rede, permitindo que os computadores da rede se autoconfigurem através da opção *stateless* do IPv6. Além de informar o bloco de endereços IPv6, é preciso também especificar a porta que está ligada ao switch.

Figura 17: Definição do bloco de endereços



Fonte: Dados do autor (2015)

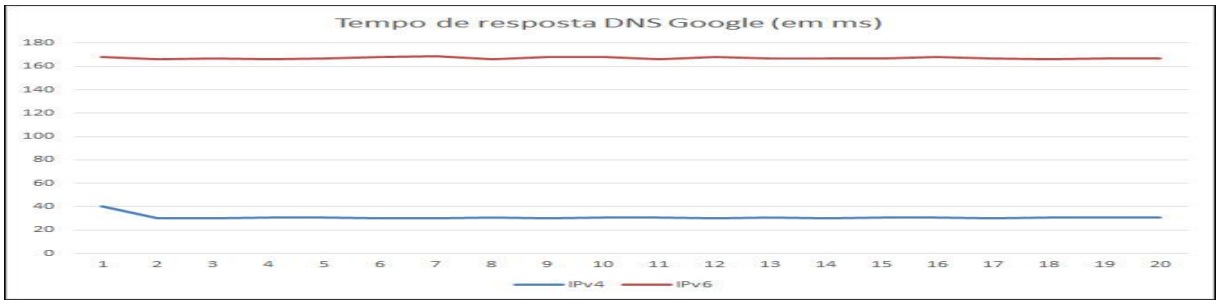
Alguns segundos após a execução de todos os scripts, os computadores começaram a receber os seus endereços IPv6 e já era possível usá-lo sem qualquer tipo de problema.

4.6 TESTES

Após a implantação do IPv6 no laboratório foi necessário realizar testes como o mesmo com fins de verificar sua estabilidade e se há algum tipo de perda com esse túnel. O primeiro

teste realizado foi para verificar se há alguma perda de pacote e se há um aumento no tempo de resposta de sites.

Figura 18: Gráfico de teste ping



Fonte: Dados do autor (2015)

Como mostra a Figura 18, no teste realizado com o servidor DNS do Google com o IP 2001:4860:4860::8888, houve um aumento médio de aproximadamente de 140 milissegundos, totalizando um aumento de 466% em relação ao IPv4. Quanto à sua estabilidade, durante os testes não houve perda de pacotes, mostrando-se bastante estável. O teste foi realizado utilizando o prompt de comando do Windows e foram realizados 5 testes seguidos com total de 20 pacotes cada e assim formando a média do gráfico acima utilizando o Microsoft Excel.

Outro teste realizado diz respeito a velocidade de download, se existe alguma perda de velocidade utilizando o túnel da Sixxs. Para a realização do teste foi um site[5] que fornece um link de um arquivo de 100MB.

Utilizando o IPv4 para realizar o download do arquivo, foi necessário um tempo de 7 minutos e 21 segundos para completar o download, mantendo uma média de 235 KB/s e com o IPv6 demorou 8 minutos e 28 segundos com uma média de 207 KB/s. Conclui-se então que existe uma pequena perda de velocidade, mas isso se deve principalmente ao túnel, já que em uma instalação nativa do IPv6 isso não deve acontecer.

Em teste de navegação cotidiana não houve uma perda de velocidade perceptível, mostrando que o serviço da Sixxs é uma boa alternativa par quem quer utilizar o IPv6 em casa ou na empresa que trabalha.

4.7 CUSTOS

Como qualquer outro projeto, um fator importante é o custo para realizá-lo. Abaixo uma tabela (Figura 19) informando os custos do projeto.

[5] https://code.google.com/p/jquery-speedtest/downloads/detail?name=100MB.txt

Figura 19: Tabela de custos

Custos			
Descrição	Quantidade	Valor Unitário	Valor Total
Mikrotik RB2011	1	R$ 750,00	R$ 750,00
Mão de Obra(horas)	4	R$ 40,00	R$ 160,00
Total			R$ 910,00

Fonte: Dados do autor (2015)

Para realizar a migração para o IPv6 foi necessário a obtenção de equipamento que conseguisse fazer o túnel que encapsula o protocolo de sexta versão no IPv4 e o envia para um servidor pré-determinado. O equipamento escolhido foi uma Mikrotik RB2011, cedida por um colega, tornando-se desnecessária a aquisição do mesmo. Caso fosse essa aquisição, o custo aproximado do equipamento ou um equivalente é de R$ 750,00.

Toda a parte de configuração e testes da implantação levaram aproximadamente 4 horas, e caso fosse necessário a contratação de um profissional para realizar essas tarefas, totalizaria um valor de R$ 160,00 usando como base o valor de R$ 40,00 por hora de serviço.

Totalizando os valores, o custo total de uma implantação é de R$ 910,00, lembrando que a implantação foi realizada em apenas um laboratório e, portanto, o valor com mão de obra não foi muito elevado. Em um projeto maior, consequentemente os custos também são maiores.

5 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Ciente da grande importância da migração para o novo protocolo, é com grande satisfação que foi concluído. Além de ter uma grande importância para a FAI Faculdades, muito conhecimento foi agregado com esse trabalho de conclusão. Através deste trabalho, oportunizou-se conhecer melhor os protocolos utilizados na rede mundial, os equipamentos utilizados e a rede da instituição. Com propósito de implantação gradativa do protocolo IPv6, o projeto contemplou a migração apenas em um laboratório de informática.

Recomenda-se realizar a implantação nos demais laboratórios e futuramente na rede completa da instituição, permitindo que a mesma continue operacional quando a versão 4 do protocolo IP seja desligada.

REFERÊNCIAS

BRASIL, Md. **Mikrotik RouterOS.** Disponível em: <http://mdbrasil.com.br/solucoesemhardware/mikrotik-routeros/>. Acesso em: 27 set. 2015.

BRITO, Samuel H. Bucke. **IPv6**: O novo protocolo da internet. São Paulo: Novatec, 2013.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil:** do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação (Mestrado) - Curso de Pós-graduação de Engenharia, UFRJ, Rio de Janeiro, 2006.

FLORENTINO, Adilson Aparecido. **IPv6 na prática.** São Paulo: Linux New Media do Brasil, 2012.

GOETHALS, Karen; AGUIAR, Antónia; ALMEIDA, Eugenia. **História da internet.** 1999. 41 f. Dissertação (Mestrado) - Curso de Gestão da Informação, Faculdade de Engenharia da Universidade do Porto, 2000.

IPV6.BR. **O IPv6.** 2012. Disponível em: <http://ipv6.br/entenda/>. Acesso em: 12 maio 2015.

MIKROTIK. About Mikrotik. Disponível em: <http://www.mikrotik.com/aboutus>. Acesso em: 27 set. 2015.

MOREIRAS, Antonio Marcos et al. **IPv6 Básico**. São Paulo: Ipv6.br, 2012.