

ANÁLISE DE IMPLEMENTAÇÃO DO PROTOCOLO DE REDE IPV6 EM UM PROVEDOR DE ACESSO À INTERNET

Leonardo Luis Christ Wuaden¹

Maxlan Maximiliano Roa²

RESUMO

O trabalho aborda, o processo de migração de uma rede IPv4 para IPv6, motivado por necessidades técnicas. Com o esgotamento de endereços IPv4 e a constante evolução das tecnologias, será necessária uma grande quantidade de endereços IP para suprir as necessidades das novas tecnologias. Neste contexto um dos problemas que se apresentam está relacionado a implementação do protocolo IPv6 sem interromper o funcionamento do provedor. O objetivo principal é implementar o protocolo de rede IPv6 em um provedor de acesso à internet, no Noroeste do Rio Grande do Sul, Brasil, utilizando a técnicas de implementação, utilizado em paralelo com o IPv4, assim é possível efetuar a implementação sem afetar o funcionamento do provedor. Com a implementação o provedor estará preparado para utilizar novas tecnologias. A falta de profissionais capacitados, alto custo de implementação e equipamentos são alguns fatores que dificultam a implementação do IPv6 em nossa região. A falta de provedores que trabalhem com esta tecnologia abre novo nicho de mercado para as empresas preparadas e que disponibilizem a tecnologia IPv6. O método de abordagem que foi utilizado neste estudo é o hipotético-dedutivo, porque partimos de um problema para construir as possíveis respostas. Além do método de abordagem, possui também os métodos de procedimentos. Neste estudo foram utilizados o comparativo e o monográfico.

O método de procedimento comparativo foi utilizado para realizar a comparação entre teoria e prática. Por fim, foi empregado o método de procedimento monográfico que foi utilizado por se tratar de um estudo de caso aplicado à Empresa Br Master Provedor de Internet.

Palavras chave: Tecnologia- IPv6- Implementação- Provedor.

ABSTRACT

The paper deals with the process of migration from an IPv4 to IPv6 network,

¹ Acadêmico do Curso de Gestão da Tecnologia da Informação- 6º Semestre. Faculdades Integradas Machado de Assis. leo_wuaden@hotmail.com

² Especialista em Sistemas de informação. Orientador. Professor do curso de Gestão da Tecnologia da Informação. Faculdades Integradas Machado de Assis. maxlan.roa@gmail.com

motivated by technical needs. With IPv4 address depletion and ever-evolving technologies, a large number of IP addresses will be needed to meet the needs of new technologies. In this context one of the problems that arise is related to the implementation of the IPv6 protocol without interrupting the provider's operation. The main objective is to implement the IPv6 network protocol in an internet access provider, in the northwest of Rio Grande do Sul, Brazil, using the implementation techniques, used in parallel with IPv4, so that it is possible to implement without affecting the provider's operation. With the implementation the provider will be prepared to use new technologies. The lack of trained professionals, high implementation costs and equipment are some of the factors that make IPv6 deployment difficult in our region. The lack of providers working with this technology opens a new market niche for companies that are ready to deploy IPv6 technology. The approach method that was used in this study is the hypothetical-deductive, because we start from a problem to build the possible answers. In addition to the approach method, it also has the procedure methods. In this study the comparative and the monographic were used.

The comparative procedure method was used to compare theory and practice. Finally, the monographic procedure method was used and was used because it is a case study applied to Br Master Internet Provider Company

Keywords: Technology- IPv6- Implementation- Provider.

INTRODUÇÃO

A implantação do protocolo IPv6 nos provedores de acesso à Internet no Brasil tem ocorrido de forma lenta, os provedores que estão se preocupando com esse assunto tendem a oferecer um serviço melhor aos seus clientes, além de contribuir com o crescimento de futuras tecnologias. (ABRANET, 2016).

A delimitação temática estudará a mudança do protocolo de rede IPv4 para o novo protocolo de rede IPv6 em um provedor de acesso à internet. A pequena quantidade de endereços IPv4 disponíveis, além da constante evolução das tecnologias, fazem com que a migração para o IPv6 seja necessária, uma vez que esta tecnologia permite uma grande quantidade de endereços IP além de possibilitar vantagens relacionadas à segurança e velocidade.

A importância desta pesquisa surgiu, pois, o protocolo de rede IPv6 é de suma importância para o futuro das tecnologias. Com a implementação deste protocolo seremos capazes de usufruirmos das tecnologias e serviços dependentes de internet.

A implementação do IPv6 já está acontecendo no Brasil, mas de forma muito lenta, as tecnologias estão sendo apresentadas para os usuários com uma velocidade muito grande, o IPv6 deveria estar funcionando em todo Brasil principalmente nos provedores de acesso à internet, para que quando as tecnologias sejam lançadas a rede já esteja pronta para recebê-las. Com essa preocupação a BR Master provedor de internet busca o conhecimento e a experiência para atender de forma eficaz e eficiente seus clientes com o uso do protocolo IPv6.

Este trabalho visa estudar como ocorreu a implementação do protocolo IPv6 em um provedor de acesso à internet, a BR Master Telecom, localizada na cidade de Campina das Missões, no estado do Rio Grande do Sul. Com o esgotamento de endereços IPv4 e a constante evolução das tecnologias como a IOT (internet das coisas), será necessária uma grande quantidade de endereços IP para suprir as necessidades das novas tecnologias. Este estudo busca responder à questão problema: Com o esgotamento dos endereços IPv4 qual a importância da implementação do protocolo de rede IPv6 em um provedor de acesso à internet, sem interromper o funcionamento do mesmo?

Tem-se como objetivo geral do trabalho, implementar o protocolo de rede IPv6 em um provedor de acesso à internet utilizando a técnica de pilha dupla, com esta técnica o IPv6 estará em funcionamento em paralelo ao IPv4, sendo assim possível efetuar a implementação sem interromper o funcionamento do provedor.

Os objetivos gerais do trabalho são:

- a) Obter uma consultoria externa para auxiliar no processo de implementação do IPv6.
- b) Obter um bloco de endereços IPv6 público junto a Nic.br.
- c) Providenciar a documentação necessária para a implementação.
- d) Verificar os equipamentos conectados à rede e sua compatibilidade com o protocolo IPv6, caso necessário fazer a atualização do parque de máquinas pra ter um perfeito funcionamento.

A metodologia utilizada na realização deste trabalho, quanto a natureza, trata-se de uma pesquisa aplicada e com relação ao tratamento dos dados, esta pesquisa é considerada qualitativa e quantitativa. Considerando os objetivos define-se que foram utilizadas as pesquisas exploratórias e descritivas. Com relação à forma de pesquisa técnica, foram realizadas pesquisas bibliográficas e estudo de campo.

Os dados obtidos foram comparados com o embasamento teórico de modo a estabelecer um melhor entendimento e enriquecimento da discussão do problema proposto. Como primeira etapa fez-se uma breve introdução ao tema, foi desenvolvido o referencial teórico, abordando assuntos relacionados a Protocolo IP, Protocolo IPv4, Protocolo IPv6 e Transição. Na segunda etapa deste trabalho, estão os métodos e técnicas, categorização da pesquisa, coleta e tratamento de dados. Na terceira etapa, as informações para a análise dos resultados foram obtidas através de uma análise com o gestor e com a equipe de implementação. Por fim, apresenta-se a conclusão, contendo os resultados e discussões.

1 REFERENCIAL TEÓRICO

O referencial teórico é a definição dos conceitos empregados durante o trabalho. No referencial teórico é onde se discutem os diferentes pontos de vista de autores sobre o mesmo assunto. Ele consiste em expor as idéias e com o intuito de fazer com que os leigos absorvam o máximo de conteúdo possível (LOPES, 2006).

Para realização deste trabalho científico foram abordados os temas: Protocolo IP, Protocolo IPv4, Protocolo IPv6, Transição e IOT.

1.1 PROTOCOLO IP

O protocolo IP possui a responsabilidade de endereçar e encaminhar os pacotes de dados que trafegam pela Internet. Para fazê-lo, ele divide os pacotes em duas partes, o cabeçalho, que carrega as informações de endereçamento e

os dados, a mensagem a ser transmitida. O TCP/IP forma uma pilha de protocolos de comunicação entre computadores em rede, a origem do seu nome vem de dois protocolos, TCP e IP. Cada camada desta pilha é responsável por um grupo de tarefas. (TANENBAUM, 2003)

Dessa forma quando ocorre o tráfego de dados através da rede, essa mensagem é dividida em unidades menores, assim se for necessário cada uma dessas unidades pode seguir uma rota diferente através da Internet. Devido a isso, as unidades podem chegar em uma ordem diferente no destino da ordem em que foram enviados na origem, como a tarefa do IP é somente a entrega dos pacotes cabe a outro protocolo reordená-los corretamente, nesse caso o TCP.

1.1.1 PROTOCOLO IPV4

O IPv4 é a versão mais utilizada do protocolo IP nas redes atualmente, sendo composto por 32 bits para endereçamento representado em 4 segmentos de números decimais variando de 0 a 255, em que parte do endereço identifica à rede e outra parte identifica a estação (MEDEIROS, 2008).

Sendo constituído por 32 bits de endereçamento, possibilita gerar mais de 4 bilhões de endereços diferentes. Embora seja um número consideravelmente grande se for levado em conta o crescimento exponencial do número de usuários de Internet esse número torna-se insuficiente.

Cada máquina de uma rede TCP/IP possui um endereço IP, tal como 200.252.155.9. O endereço IP, às vezes chamado de dotted quad, é composto por quatro números separados por ponto, cada qual na faixa de 0 a 255. (KUROSE; ROSS, 2006).

Estes endereços podem ser utilizados para indicar uma rede ou apenas um host individual. Para identificar a rede é necessário utilizar a máscara de rede após o IP.

Os números endereços de IPs disponíveis na versão quatro não são suficientes para atender a demanda atual da Internet. Por esse motivo estão sendo utilizados alguns mecanismos como citados abaixo para adiar o

esgotamento dos endereços IPv4. Alguns desses mecanismos são:

- A. *Network Address Translation (NAT)*: O NAT permite que com apenas um endereço válido na Internet, os computadores da rede interna tenham conexão com a Internet. Ele faz um mapeamento baseado no IP interno e na porta local do computador, gerando um número de 16 bits usando a tabela hash, posteriormente este número é utilizado no campo da porta de origem. O pacote que vai para a rede externa leva o IP do roteador e na porta de origem o número gerado pelo NAT, com isso o computador externo que receber o pacote sabe de onde ele veio, e envia a resposta novamente para o emissor;
- B. *Classless Inter Domain Routing (CIDR)*: Permite atribuir faixas de endereços de tamanhos variáveis, abolindo as classes de IP;
- C. *Variable Length Subnet Mask (VLSM)*: É um método que permite calcular sub-redes, alocando somente os bits necessários da sub-rede 22 utilizando máscaras de tamanho variáveis.

Mesmo utilizando todos esses mecanismos o esgotamento de endereços IP públicos o seu fim está previsto para o início do ano de 2020. No entanto só conseguem adquirir IPv4 novos entrantes.

Hoje distribuição de IPv4 se dá apenas para novos entrantes na América Latina e no Caribe. As fases de esgotamento foram feitas com base nos endereços livres e, atualmente, existem mais ou menos 2,8 milhões de endereços desocupados. No ritmo que está hoje, os endereços IPv4 se esgotam em janeiro de 2020, não sendo mais possível obter endereço IPv4 após disto. (PRESCOTT, 2018)

1.1.2 CABEÇALHO IPV4

Nesta versão do protocolo IP são treze campos fixos compõe o cabeçalho ou estrutura, seu tamanho pode variar de 20 a 60 bytes dependendo de opções que podem ou não ocorrer.

Versão	Comprimento do Cabeçalho	Tipo de Serviço	Comprimento do Datagrama	
Identificador			Flags	Deslocamento de Fragmentação
Tempo de Vida	Protocolo		Bits para verificação da Integridade do Cabeçalho	
Endereço IP da Fonte				
Endereço IP do Destino				
Opções				

Ilustração 1 - Cabeçalho IPv4.

Fonte: TANENBAUM, 2003.

De acordo com a *RFC 791*, os campos que formam o cabeçalho do IPv4 são:

Versão: Possui 4 bits e define a versão do protocolo IP do datagrama. Através desta informação o roteador poderá saber como tratar o restante do datagrama.

Comprimento do cabeçalho: Possui 4 bits, como o no IPv4 possui um número variado de opções este campo permite saber onde realmente começam os dados.

Tipo de Serviço: Possui 8 bits e é utilizado para diferenciar os datagramas. **Comprimento do Datagrama:** Possui 16 bits é o comprimento total do datagrama, o tamanho máximo teórico do datagrama IP é 65.535 bytes.

Comprimento do Pacote - Este campo fornece o tamanho total do pacote em bytes, incluindo o cabeçalho e os dados.

Identificador, flags, deslocamento de fragmentação: Estes três campos têm a ver com a fragmentação IP.

Flag Mais Fragmentos - A flag Mais Fragmentos (MF) é um único bit no campo Flag usado com o Deslocamento de Fragmentos na fragmentação e reconstrução de pacotes. O bit da flag Mais Fragmentos é configurado, o que significa que ele não é o último fragmento de um pacote. Quando um host de destino vê um pacote chegar com MF = 1, ele examina o Deslocamento de

Fragmentos para ver onde este fragmento deve ser colocado no pacote reconstruído. Quando um host de destino recebe um quadro com MF = 0 e um valor diferente de zero no Deslocamento de Fragmentos, ele designa este fragmento como a última parte do pacote reconstruído. Um pacote não fragmentado possui todas as informações de fragmentação iguais a zero (MF = 0, deslocamento de fragmentos = 0).

Flag Não Fragmentar - A flag Não Fragmentar (DF) é um único bit no campo Flag que indica que a fragmentação do pacote não é permitida. Se o bit da flag Não Fragmentar for configurado, a fragmentação do pacote NÃO será permitida. Se um roteador precisar fragmentar um pacote para permitir que ele passe para a camada de enlace de dados e o bit DF estiver definido como 1, o roteador descartará o pacote.

Deslocamento de Fragmento - Um roteador pode precisar fragmentar um pacote ao encaminhá-lo de um meio físico para outro que tenha uma MTU menor. Quando ocorre a fragmentação, o pacote IPv4 usa o campo Deslocamento de Fragmento e a flag MF no cabeçalho IP para reconstruir o pacote quando ele chega ao host de destino. O campo deslocamento de fragmento identifica a ordem na qual o fragmento do pacote deve ser colocado na reconstrução.

Tempo de Vida: Este campo serve para que o datagrama não fique circulando eternamente na rede, cada vez que passa por um roteador ele é decrementado e quando chegar a zero ele é descartado.

Protocolo: Este campo é utilizado somente quando chega em seu destino, ele serve para identificar qual protocolo da camada de transporte ele será encaminhado.

Soma de verificação de Cabeçalho: Ela ajuda o roteador na detecção de erros do datagrama. A soma é tratada a cada 2 bytes e funciona da mesma forma da soma de verificação do protocolo UDP. Cada vez que o datagrama passa por um roteador a soma de verificação é calculada novamente devida a mudança de alguns campos como o Tempo de vida. Quando é detectado algum erro o datagrama é descartado pelo roteador.

Endereço IP de 32 bit da Fonte: Este campo armazena o endereço IP do hospedeiro que gerou o datagrama.

Endereço IP de 32 bit do Destino: Este campo armazena o endereço IP do hospedeiro de destino do datagrama.

Opções: O campo opções permite que o cabeçalho IP seja ampliado, ele é raramente utilizado e nem é recomendada a sua utilização.

1.2 PROTOCOLO IPV6

É a versão mais atual do IP, ou seja, a versão 6. Sua criação foi iniciada em 1994, por Scott Bradner e Allison Marken, após isto este protocolo já sofreu muitas mudanças e melhorias até os dias de hoje (IPv6.BR, 2011).

A versão IPv6 mantém a compatibilidade com a versão IPv4, quando a transição é feita gradativamente. A intenção do IPv6 é substituir o IPv4, que tem apenas 4 bilhões de endereços (4×10^9) o IPv6 ($3,4 \times 10^{38}$) conta com cerca de 79 octilhões de vezes a quantidade de endereços IPv4. Além disso, o endereçamento é de 128 bits, com um total de 340.282.366.920.938.463.463.374.607.431.768.211.456 de endereços. Para se colocar em escala o que isso representa, seria o equivalente (estimado) a uma rede com 32 endereços para cada molécula de água do oceano (TANENBAUM, 2011).

Desde a criação do IPv6 foram feitas muitas modificações no protocolo, primeiramente foi testado em redes experimentais e após estar mais refinado, começou a ser utilizado em provedores de serviço, que passaram a utilizar o IPv6 em parte de suas redes. Empresas como Google, Facebook, Yahoo!, Terra, IG já estão testando a utilização do IPv6 (NETWORK WORLD, 2011). Provedores como a Global Crossing, da CTBC, e da Telefônica já fornecem trânsito IPv6 comercialmente no Brasil. Devido à importância de implantação desta nova versão do IP os governos têm começado a apoiar esta implantação. (IPv6.BR, 2011)

1.2.1 CABEÇALHO IPV6

Os cabeçalhos do IPv6 possuem 40 bytes, duas vezes maior que o do IPv4, é mais flexível e tem a possibilidade de ser estendido através de cabeçalhos adicionais. É mais eficiente que o cabeçalho da antiga versão, pois minimiza o overhead e reduz o custo do processamento dos pacotes (SANTOS et al., 2010).

O novo cabeçalho IPv6 é composta por 8 campos fixos, os campos do Cabeçalho IPv6 são:

- A. **Versão:** Este campo possui 4 bits e identifica a versão do protocolo IP utilizado, sendo valorizado com 6, se estiver na versão IPv6;
- B. **Classe de Tráfego:** Este campo possui 8 bits onde os pacotes são identificados através da prioridade ou classe de serviços;
- C. **Identificador de Fluxo:** Este campo possui 20 bits e faz a diferenciação dos pacotes do mesmo fluxo de rede, permitindo que o roteador identifique o tipo de fluxo de cada pacote, sem verificar sua aplicação;
- D. **Tamanho dos Dados:** Este campo possui 16 bits, identifica o tamanho dos dados em bytes, enviados junto ao cabeçalho IPv6. Os cabeçalhos de extensão estão incluídos também neste cálculo;
- E. **Próximo Cabeçalho:** Este campo possui 8 bits e identifica o cabeçalho que segue ao cabeçalho IPv6, este campo não contém apenas valores referentes a outros protocolos, mas também indica os valores dos cabeçalhos de extensão;
- F. **Limite de Encaminhamento:** Este campo possui 8 bits onde sua função é indicar o número máximo de roteadores que o pacote IPv6 pode passar antes de ser descartado;
- G. **Endereço de Origem:** Este campo possui 128 bits e indica o endereço de origem do pacote.
- H. **Endereço de Destino:** Este campo possui 128 bits e indica o endereço de destino do pacote.

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)	
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)
Endereço de Origem (Source Address)			
Endereço de Destino (Destination Address)			

Ilustração 2 - Cabeçalho IPv6.

Fonte: Nic.br, 2009.

1.2.2 IPSEC

Com a utilização cada vez maior da Internet para meios comerciais e transações que envolvem compras, vendas, transferências de informações importantes ou valores em dinheiro é cada vez mais necessário que a rede tenha segurança. Para isto utilizam-se métodos para ajudar nesta proteção, tais como, firewalls, antivírus, segurança no acesso à web com *Secure Socket Layer (SSL)* - 35 RFC 2246 (DIERKS; ALLEN, 1999)).

Desde o início da criação do IPv6 a questão da segurança foi bastante analisada, mecanismos de segurança passam a fazer parte do protocolo IPv6, sendo que qualquer par de dispositivos de uma conexão fim-a-fim possam usufruir desta segurança, com métodos que visam garantir a segurança dos dados que trafegam pela rede.

No IPv6 o seu suporte é obrigatório, já com seus principais elementos integrados, facilitando sua utilização. No IPv4 ele foi adaptado para funcionar, sendo opcional a sua utilização.

A melhor alternativa para a segurança em nível de aplicação é

fornecida na camada de rede, onde todo o conteúdo dos pacotes IP, e mesmo os próprios cabeçalhos IP, são protegidos. Essa solução apresenta muitas vantagens. Ela está disponível para todo o tráfego IP entre qualquer par de lados e, portanto, é útil para proteger dados de aplicações e também pode ser usada para proteger trocas de roteamento e sinalização. O IPSEC é a base da segurança em nível de rede. Ele é usado para autenticar o emissor das mensagens, para verificar se os dados da mensagem não foram adulterados e para ocultar informações de olhos não autorizados. (FARREL, 2005 p.484).

No IPv6 o seu suporte é obrigatório, já com seus principais elementos integrados, facilitando sua utilização. No IPv4 ele foi adaptado para funcionar, sendo opcional a sua utilização.

No IPSEC a criptografia e autenticação de pacotes são feitas na camada de rede, fornecendo assim uma solução de segurança fim-a-fim, garantindo a integridade, confidencialidade e autenticidade dos dados, como pode ser observado na ilustração 3.

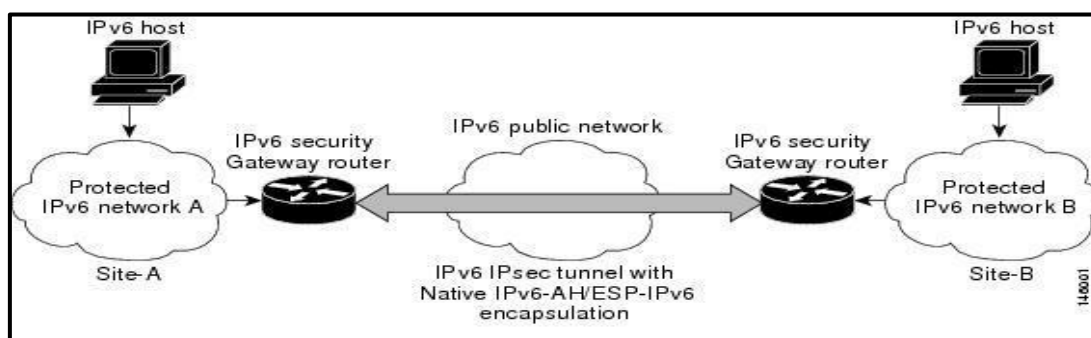


Ilustração 3 – IPSEC

Fonte: Cisco.br, 2012.

1.3 TRANSIÇÃO

Devido as mudanças introduzidas pelo IPv6, ele é incompatível com IPv4, por isso é necessário migrar para o novo protocolo. Durante um período de tempo eles deverão coexistir. As técnicas de transição foram criadas para que a migração do protocolo IPv4 para o IPv6 ocorra gradualmente. Essa implementação deve ocorrer de forma gradativa pois esse processo deve demorar alguns meses ou em alguns casos até anos, assim devem ser utilizadas técnicas para utilizar IPv4 E IPv6 em paralelo. Existe uma grande diversidade de

mecanismos capazes de efetuar essa transição, no entanto, de maneira geral, todos podem ser classificados em três grandes categorias: pilha dupla, tunelamento e tradução (BRITO, 2013).

O IPv6 foi criado com o intuito de substituir o IPv4, para suportar o crescimento da rede e assim resolver o problema de esgotamento de endereços, devido à dimensão da rede esse processo deveria ser realizado gradualmente, até alcançar toda a rede, as técnicas mais comuns utilizadas são (SANTOS, 2010):

- A. **Pilha dupla:** consiste na convivência do IPv4 e do IPv6 nos mesmos equipamentos, de forma nativa, simultaneamente. Essa técnica é a técnica padrão escolhida para a transição para IPv6 na Internet e deve ser usada sempre que possível.
- B. **Túneis:** Permitem que diferentes redes IPv4 comuniquem-se através de uma rede IPv6, ou vice-versa.
- C. **Tradução:** Permitem que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes.

TÉCNICAS	VANTAGEM	DESVANTAGEM
<i>Pilha Dupla</i>	<i>Utiliza técnicas stateless baseadas em uma dupla tradução de pacotes</i>	<i>Cada Host precisa ter as duas pilhas rodando separadamente, o que demanda o poder de processamento adicional e memória.</i>
<i>Tunnel Brokers</i>	<i>Baixa complexidade de funcionamento</i>	<i>Alta latência</i>
<i>6to4</i>	<i>Cria túneis automaticamente para outros endereços 6to4.</i>	<i>Segurança, sendo vulneráveis a ataques do tipo Man-in-the-Middle e DoS.</i>
<i>6rd</i>	<i>Rápida adoção do IPv6 para usuários domésticos</i>	<i>Deve sempre existir um protocolo IPv4 público operando em paralelo para seu funcionamento</i>
<i>NAT444</i>	<i>Não é necessário conhecimento em IPv6</i>	<i>Quebra do modelo fim-a-fim da Internet</i>

<i>ISATAP</i>	<i>Suporta a maior parte dos sistemas operacionais e roteadores e de fácil implantação</i>	<i>Não provê nenhuma economia de endereços IPv4, pois todos os hosts envolvidos na comunicação precisam de um endereço IPv4 público.</i>
<i>Teredo</i>	<i>Fácil implementação para usuários domésticos, devido a configuração automática.</i>	<i>Segurança por utilizar o protocolo UDP</i>
<i>NAT-PT</i>	<i>Tem uma eficiência mais elevada do que as técnicas utilizadas na camada de aplicação.</i>	<i>É muito complicado para criar entradas estáticas para múltiplas fontes de comunicação com vários destinos.</i>
<i>NAT64/DNS64</i>	<i>Infraestrutura de IPv4 permanece inalterado</i>	<i>Incompatibilidade com balanceamento de carga em servidores ou algo do gênero.</i>

Tabela 1: Vantagem e Desvantagem das técnicas de transição.

Fonte: Canno (2013)

1.3.1 PILHA DUPLA

Os dois protocolos funcionam paralelamente, assim aos poucos o IPv6 é implementado. Para o IPv6 na Internet essa é a técnica padrão e mais indicada para a alteração. Esse método consiste em implementar e utilizar ambos os protocolos, IPv4 e IPv6 na rede em geral, de maneira gradativa, implicando na coexistência de duas redes em paralelo. Este método de transição permitindo uma implantação gradual, com a configuração de pequenas seções do ambiente de rede de cada vez. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 em cada nó. (IPv6.br,2012).

Dessa forma, essa estratégia facilita o processo de transição para um ambiente totalmente baseado em IPv6, abaixo uma figura ilustra o método pilha dupla.

Esta técnica consiste em IPv4 e IPv6 coexistindo no mesmo equipamento, ou seja, os dispositivos e roteadores são equipados com pilhas de ambos protocolos, tendo capacidade de enviar e receber os dois tipos de pacotes. Com isso, um nó Pilha Dupla, se comportará

como um nó IPv6 na comunicação com outro nó IPv6 e se comportará como um nó IPv4 na comunicação com outro nó IPv4. (IPV6.BR,2012)

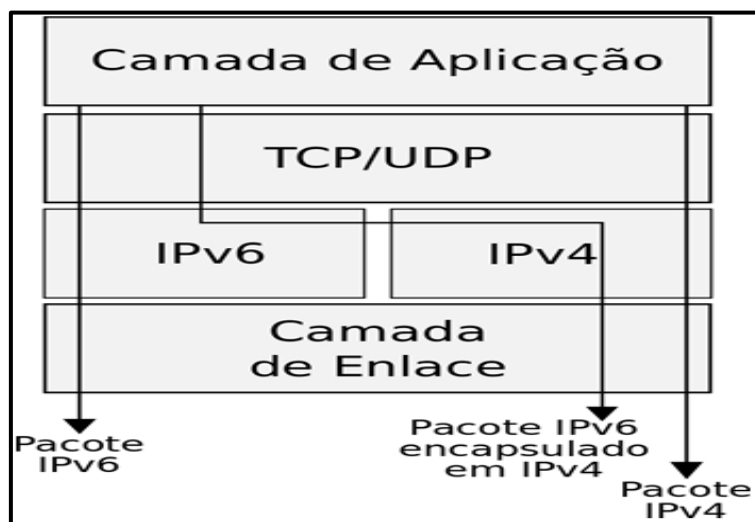


Ilustração 4: Funcionamento da técnica de pilha dupla.

Fonte: ipv6.br,2012

Na técnica de pilha dupla o IPv6 será sendo inserido na rede de forma progressiva, oferecendo aos usuários um maior aprendizado sobre o processo de operação do protocolo IPv6, trazendo assim, uma maior confiança no desligamento definitivo do protocolo antigo, o IPv4.

1.3.2 TÚNEIS IPV6-OVER-IPV4

O tunelamento IPv6-over-IPv4, é uma técnica utilizada para estabelecer túneis ponto-a-ponto através do encapsulamento de pacotes IPv6 dentro de cabeçalhos IPv4 para carregá-los sobre as infraestruturas de roteamento IPv4. A ilustração 5 ilustra como ocorre o encapsulamento. (RFC 4213,2015). Ao encapsular o pacote IPv6 dentro de um pacote IPv4, seus endereços de origem e destino são adequados para o IPv4 e no cabeçalho é colocado o tipo 41, por isto este encapsulamento também pode ser chamado de “protocolo 41”. Quando o destino recebe o pacote com o tipo 41 ele irá remover o cabeçalho IPv4 e tratar o pacote como IPv6.

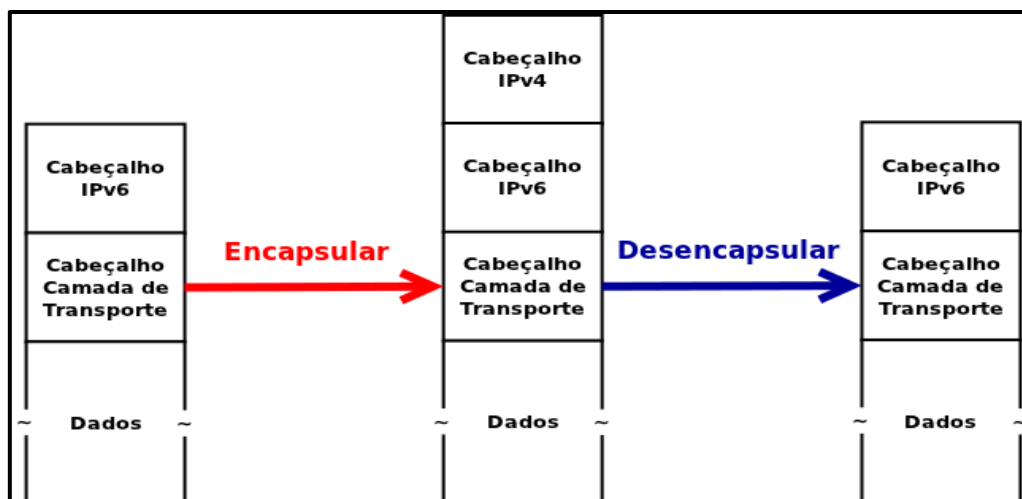


Ilustração 5: Encapsulamento 6in4.

Fonte: ipv6.br,2012

Ao encapsular o pacote IPv6 dentro de um pacote IPv4, seus endereços de origem e destino são adequados para o IPv4 e no cabeçalho é colocado o tipo 41, por isto este encapsulamento também pode ser chamado de “protocolo 41”. Quando o destino recebe o pacote com o tipo 41 ele irá remover o cabeçalho IPv4 e tratar o pacote como IPv6.

1.3.3 TRADUÇÃO NAT64/DNS64

A técnica de transição NAT64, que utiliza unicamente endereços IPv6 nos hosts clientes e possibilita a comunicação com destinos em IPv6 e IPv4, tem-se mostrado bastante popular em listas de discussões e RFCs. Um sub-protocolo crucial neste processo é o DNS64, que integra a solução, possibilitando a descoberta de endereços remotos IPv4.

O NAT64, definido na RFC6146, é uma técnica de tradução de pacotes que permite a nós somente IPv6 acessarem a Internet IPv4. Ele necessita de uma técnica auxiliar para a conversão do DNS, chamada de DNS64, definida pela RFC6147. São sistemas distintos, mas que trabalham em conjunto para permitir a comunicação entre as redes IPv6 e IPv4. O NAT64 realiza a tradução de endereços IPv4 em IPv6, de acordo com as definições da RFC6052, utilizando um prefixo IPv6 escolhido pelo provedor, ou o prefixo 64:FF9B::/96, recomendado por esta RFC (exemplo, o IPv4 203.0.113.1 seria convertido para o endereço IPv6 64:FF9B::203.0.113.1). Já a tradução do cabeçalho IPv6 em cabeçalho IPv4 e vice-versa é baseada na especificação da RFC6145. (IPv6.br, 2012).

O funcionamento do NAT64 é ilustrado no diagrama de sequência e na topologia das ilustrações 6 e 7, a seguir:

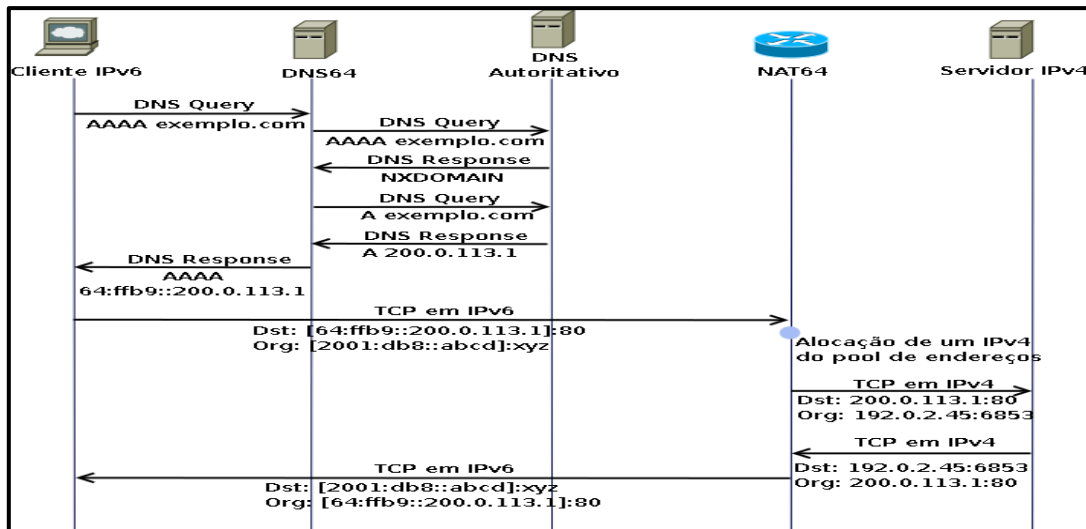


Ilustração 6:Diagrama de sequência do NAT64/DNS64.

Fonte: ipv6.br,2012

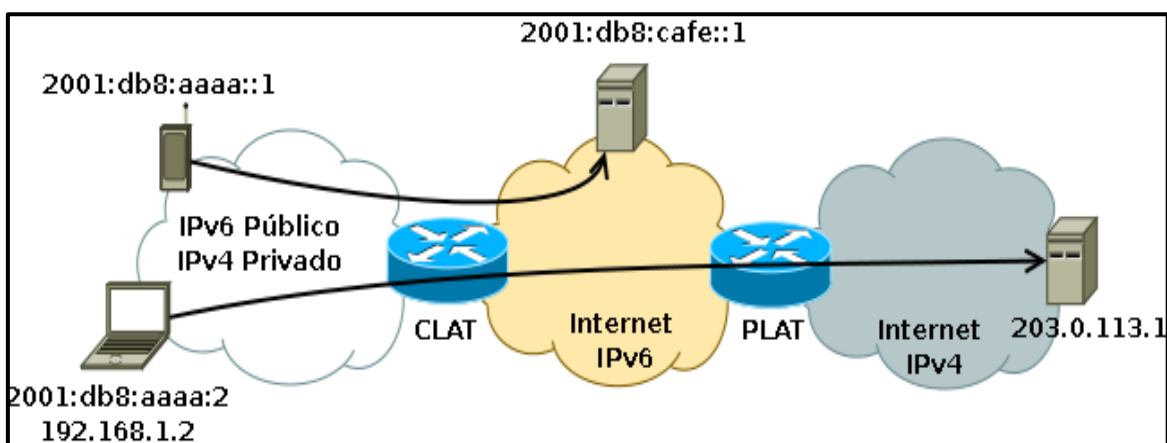


Ilustração 7:Topologia de rede do NAT64/DNS64.

Fonte: ipv6.br,2012

1.3 IOT

Um novo conceito de utilização da Internet, é denominada como Internet das Coisas (IOT). Esse termo foi empregado pela primeira vez no ano de 1999, por Kevin Ashton. A expressão ganhou vida quando o autor realizou

uma apresentação para Procter & Gamble (P & G) integrando o uso de tecnologias de endereçamento de dados e sinais com a Internet. O objetivo de sua proposta era melhorar o fluxo dos produtos e informações sem a interferência direta do homem.” Atualmente sabemos que a Internet é totalmente dependente do ser humano para obter dados, porém é também uma ferramenta facilitadora, gravando e recuperando quantias significativas de dados do mundo físico” (ASHTON, 2009).

De uma forma geral compreende-se por IOT a maneira com que objetos físicos do nosso cotidiano se interconectam na web, muitos destes equipamentos estão incorporados com computação ubíqua “O conceito mais abrangente de Computação ubíqua é o que a define como invisível ao olho nu do ser humano, mas sabe-se que ela está presente no espaço (Zhao, & Whang, 2011)”, são controlados pela Internet. “Os avanços em tecnologias subjacentes permitiram que “coisas” possam ser identificadas, detectadas e controladas remotamente usando sensores e atuadores” (FENG; LAURENCE; LIZHE, 2012). A IOT conecta em tempo real, pessoas e objetos com a tecnologia operando invisivelmente nas tomadas de decisões que antes eram do ser humano (ATZORI; IERA; MORABITO, 2010).

Alguns dados preliminares estimam que atualmente o mundo implementou 5 bilhões de dispositivos inteligentes e a previsão para o ano de 2020 é que haverá 50 bilhões de objetos conectados (CHASE, 2013). Para que a IOT se desenvolva é necessário o suporte de algumas tecnologias como sensores, atuadores, smartphones, arquitetura de redes, protocolos, interoperabilidade e conexão sem fio.” Entre as aplicações visíveis na atualidade essa tecnologia está, no monitoramento remoto de pacientes, automação e fabricação industrial, logística, gerenciamento de negócios e processos e transporte inteligente de pessoas e bens (RITZ; KNAACK, 2017).

Alguns exemplos de dispositivos IOT conectados são: Webcams e câmeras de segurança, termostatos programáveis baseados na web, tomadas de energia controladas remotamente, fechaduras eletrônicas, sistemas de alarme, sensores de ocupação, interfonos e sistemas de alto-falantes baseados na web, dispositivos de monitoramento ambiental, iluminação LED inteligente, pontos de

acesso sem fio, geladeiras, freezers máquinas de lavar, smartphones e smart tvs dentre muitos outros.

2 METODOLOGIA

Nesta seção, descreve-se formalmente a opção pelos métodos e pelas técnicas a serem utilizados na investigação, bem como se apresentam as conexões e a leitura operacional que o pesquisador fará do quadro teórico e de seus objetivos de estudo (DESLANDES, 2009).

O objetivo do trabalho é implementar o protocolo de rede IPv6 em um provedor de acesso à internet no noroeste do Rio Grande do Sul. Foram aplicados questionários com o gestor da empresa, com as principais questões a serem abordadas, relacionados com a implementação do IPv6 no provedor de internet, a pesquisa caracteriza-se como teórica prática.

2.1 CATEGORIZAÇÃO DA PESQUISA

Quanto à natureza do estudo, caracteriza-se como uma pesquisa teórico-empírica, pois foram utilizadas pesquisas bibliográficas e também a observação do ambiente e coleta de dados na empresa Br Master Provedor de Internet. Gil classifica o estudo teórico- empírica como “pesquisa aplicada voltada à aquisição de conhecimentos com vistas à aplicação numa situação específica.” (GIL, 2010, p.27)

Quanto à abordagem e tratamento de dados, a pesquisa é classificada como qualitativa e quantitativa, descritiva. Conforme Gil, as pesquisas classificadas como descritivas têm como objetivo descrever as características de determinada população ou fenômeno e podem estabelecer as relações entre as variáveis. (GIL, 2010).

Quanto aos fins e objetivos propostos, foram utilizados os métodos exploratórios e descritivos uma vez que há a necessidade de buscar o conhecimento das melhores formas de se implementar o IPv6 na empresa em estudo e nos seus respectivos clientes, utilizando o método descritivo. De acordo

com Gil, a pesquisa exploratória objetiva maior familiarização com o problema, tornando-o assim explícito. Já a pesquisa descritiva é definida pelo autor como aquela que tem como objetivo a descrição das características de determinada população ou fenômeno, sendo que se caracteriza pela utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática (GIL, 2010).

Quanto aos procedimentos técnicos, pode-se identificar essa pesquisa como estudo de caso e estudo de campo. No estudo de caso desenvolveu-se um estudo focado na empresa em questão. Essa pesquisa buscou através do estudo detalhado desta organização e suas particularidades. No estudo de campo foi elaborado um questionário/entrevista para o gestor de empresa em estudo. Para Vianna, o estudo de caso e de campo objetivam um estudo detalhado de um objeto ou situação, de forma a permitir o entendimento da sua totalidade (VIANNA, 2001).

Foram ainda realizadas pesquisas bibliográficas, utilizando-se livros, artigos publicados em revistas e na internet, e documental. Para Gil a pesquisa bibliográfica é “com propósito de fornecer fundamentação teórica ao trabalho bem como a identificação do estágio atual do conhecimento referente ao tema” (GIL, 2010).

2.2 GERAÇÃO DE DADOS

Tendo em vista a necessidade de identificar a importância e as dificuldades da implementação do IPv6, tem a necessidade de coletar dados a analisá-los posteriormente.

Para coletar dados foi necessário a pesquisa direta, pois foi realizado questionário e/ou entrevista com o gestor, também foi utilizada documentação indireta, pois foram efetuadas pesquisas bibliográficas sobre o tema, já incluídas no referencial teórico. Os dados foram coletados através de um questionário aplicado ao gestor do provedor, levando em conta que o estudo está relacionado ao nível gerencial da organização. Cerro, Bervian e Silva afirmam que o questionário “é a forma mais usada para coletar dados, pois possibilita medir

com mais exatidão o que se deseja” (CERVO; BERVIAN; SILVA, 2007, p. 53).

2.3 ANÁLISE E INTERPRETAÇÃO DOS DADOS

O método de abordagem que foi utilizado neste estudo é o hipotético-dedutivo, porque partimos de um problema para construir as possíveis respostas, que foi definido como sendo: Com o esgotamento dos endereços IPv4 qual a importância da implementação do protocolo de rede IPv6 em um provedor de acesso à internet sem interromper o funcionamento do mesmo?

Além do método de abordagem, possui também os métodos de procedimentos. Neste estudo foram utilizados o comparativo e o monográfico.

O método de procedimento comparativo foi utilizado para realizar a comparação entre teoria e prática. Segundo Vianna o método comparativo “consiste no confronto entre elementos, levando em consideração seus atributos” (VIANNA, 2001, p.152).

Por fim, foi empregado o método de procedimento monográfico que conforme Marconi e Lakatos “consiste na observação de determinados indivíduos, profissões, condições, instituições, grupos ou comunidades, com a finalidade de se obter generalizações” (MARCONI; LAKATOS, 2010, p.173). O método de procedimento monográfico foi utilizado por se tratar de um estudo de caso aplicado à Empresa Br Master Provedor de Internet.

Neste artigo foi utilizado o procedimento técnico de questionário aplicado, no qual visou conhecer a importância da implementação e as suas dificuldades, tendo em vista que a implementação deve ser feita sem interferir no funcionamento do provedor. Os dados coletados através do questionário geram resultados que foram comparados com a teoria pesquisada a respeito do tema permitindo fazer a análise dos resultados.

3 ANÁLISE DOS RESULTADOS

3.1 APRESENTAÇÃO DA ORGANIZAÇÃO

A BR Master provedor de acesso à internet localiza-se no centro do município de Campina das Missões-RS, iniciou os seus trabalhos no ano de 2001 sendo pioneira no ramo de atuação no município, inicialmente com internet discada. Desde então o provedor passou a investir em produtos e serviços buscando trazer internet de alta qualidade para Campina das Missões e para os municípios da região, através da internet via rádio e fibra óptica.

Atualmente o provedor conta com 7 colaboradores: sendo 4 técnicos instaladores/reparadores, 2 técnicos responsáveis pela infra-estrutura, uma secretária e 2 gestores/sócios fundadores. O provedor tem área de atuação em 3 municípios, Campina Das Missões, Salvador Das Missões e Vila Dona Otília (Roque Gonzales), atendendo essas localidades com internet via rádio e principalmente com fibra óptica, o provedor conta atualmente com aproximadamente 1.200 clientes nos 3 municípios de atendimento.

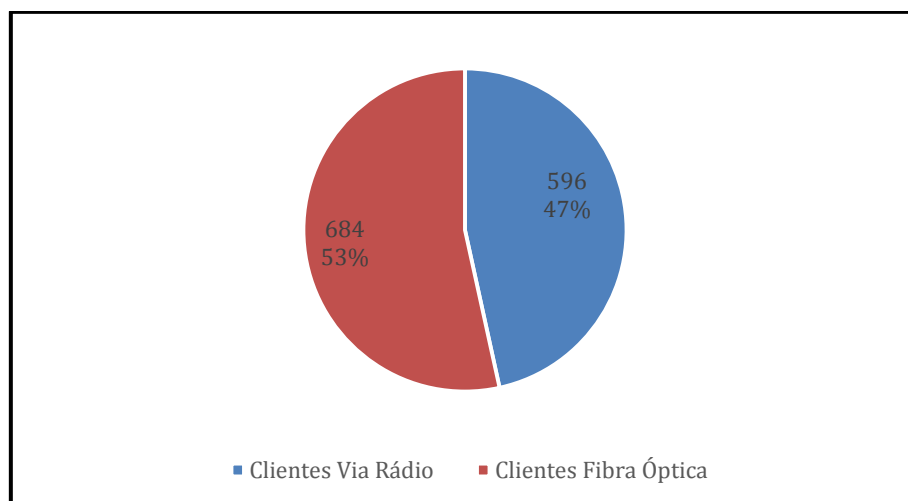


Ilustração 8: Cliente com conexões Via Rádio e Fibra Óptica.

Fonte: produção do pesquisador

3.2 ANÁLISE DOS RESULTADOS DA PESQUISA COM O GESTOR.

Para conhecer o contexto do provedor e buscando informações sobre a implementação do IPv6, no dia 18 de outubro de 2019 aplicou-se uma pesquisa para o gestor e socio fundador Lecir Haas. A técnica de pesquisa utilizada foi uma entrevista aonde foi aplicado um questionário criado no editor de textos *Word*. O questionário contém 14 questões discursivas envolvendo diversos

assuntos relacionados à implementação do IPv6.

Durante a entrevista o gestor comunicou que todo o processo de implementação foi realizado pela *FB Consultoria* localizada na cidade de Porto Belo-SC, e por esta razão algumas questões técnicas não poderiam ser respondidas com detalhes, pois o gestor não estava ciente do detalhamento da implementação.

O tempo total de implementação foi de aproximadamente 03 meses, que envolveu etapas de planejamento, troca de equipamentos, transição, documentação e testes. Todas as etapas da implementação foram realizadas pela *FB Consultoria*, por esta razão para o provedor a maior dificuldade foi a troca do sistema ERP *RouterBox*, que era responsável por integrar todos os setores do provedor em um único sistema, pois o mesmo era incompatível com o IPv6, para isso foi necessário adquirir um novo sistema, após pesquisas e orçamentos foi adquirido o ERP *IXC Soft* a principal diferença para o sistema anterior é a compatibilidade com IPv6, monitoramento da frota de veículos, integração com equipamentos ativos na infra-estrutura do provedor como roteadores, olt e onu.

O gestor do provedor participou de 3 treinamentos sobre o protocolo de rede IPv6, o primeiro realizado pela instituição nic.br no município de Santa Maria- RS com duração de 3 dias, que abordou os temas endereçamento e planejamento IPv6, serviços, segurança em redes IPv6 e técnicas de transição. O segundo em Porto Alegre- RS oferecido pela empresa *Voz e Dados* sobre *mikrotik* no IPv6 com duração de 5 dias. E terceiro no município de Foz do Iguaçu- PR pela empresa *Alive Solutions* também sobre *mikrotik* no IPv6 com 3 dias de duração. Os 3 cursos totalizam aproximadamente R\$ 8.000,00, nesse valor está incluso os treinamentos, estadias e deslocamentos.

A maioria dos equipamentos utilizados na infra-estrutura do provedor já eram compatíveis, tendo que substituir apenas o equipamento de borda, era utilizado uma Mikrotik RouterBoard modelo RB4011 com 1GB de RAM, processador ARM 32bit 1,4GHz de 4 núcleos, por uma Mikrotik Cloud Core Router modelo CCR1036 com 4 GB de RAM, processador ARM de 1,2Ghz e 36

núcleos. A principal vantagem proporcionada pela troca do equipamento foi a diminuição de uso do processamento do equipamento, pois o novo equipamento possui um processador de última geração, com mais núcleos de processamento e também maior quantidade de memória RAM. Também foi necessário a substituição de equipamentos de clientes produzidos a mais de 5 anos sem compatibilidade com o IPv6. A partir de então foi instalado principalmente roteadores *tp-link* de 2 antenas modelo WR840N 300mbps, *tp-link* de 3 antenas modelo WR940N 450 mbps, *tp-link* de 4 antenas modelo C50 ou C5 1200mbps, a escolha do equipamento instalado fica de acordo com a necessidade do cliente.

O principal equipamento substituído foi roteadores wireless de clientes de diversas marcas, com fabricação inferior a 2014 devido a sua incompatibilidade ao IPv6. Atualmente ainda restam alguns modelos de roteadores de clientes sem suporte a IPv6, porém apresentam instabilidades e necessitam de atualizações de firmware, sendo assim os clientes novos são ativados com IPv6 e os migrados conforme solicitação do cliente. Atualmente o provedor possui em torno de 40% dos clientes utilizando de IPV6, ou seja aproximadamente 480 dos 1.200 clientes já utilizam IPv6.

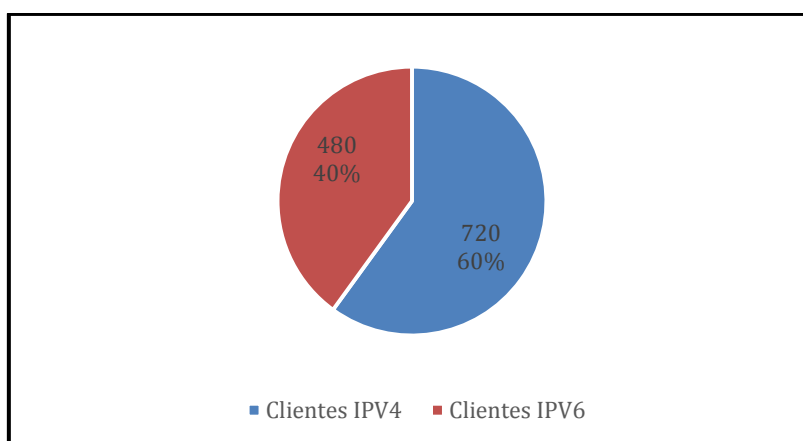


Ilustração 9: Utilização dos protocolos IP.

Fonte: produção do pesquisador

O custo total da implementação do IPv6 foi aproximadamente R\$ 26.000,00, a maior parte desse valor foi com a consultoria aproximadamente R\$

12.000,00, a troca do equipamento de infraestrutura CCR 1036 teve custo por volta de R\$ 6.000,00, os R\$ 8.000,00 restantes foram gastos em cursos e treinamentos.

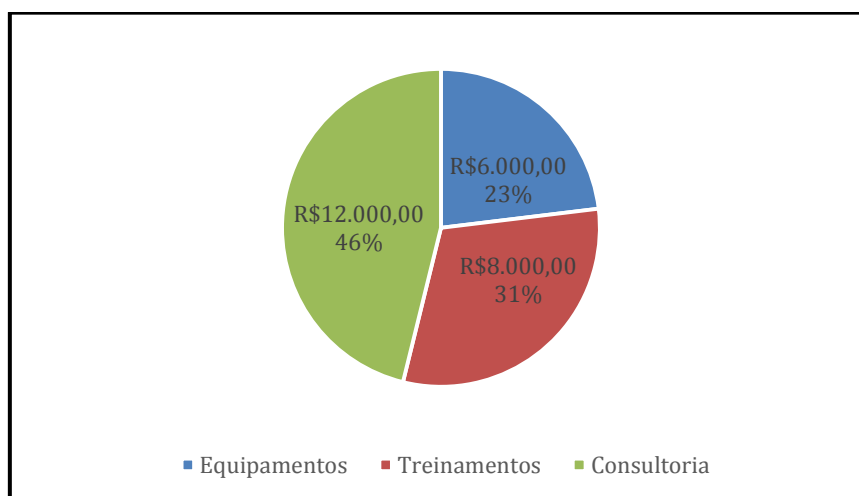


Ilustração 10: Custos de implementação IPv6.

Fonte: produção do pesquisador

Conforme informações repassadas pelo gestor, o investimento financeiro, é indispensável e de custo baixo, inferior a tantos outros investimentos tanto de hardware como de software que fazem parte do cotidiano do provedor.

Durante o processo de implementação alguns clientes tiveram interesse em participar em alguns testes de funcionamento do IPv6, sabedores de que poderiam ocorrer erros de navegação e da responsabilidade de comunicar o provedor se houver qualquer instabilidade.

Os motivadores para a implementação do IPv6 foram basicamente a escassez do IPv4 com a solidez que o IPv6 traz para a rede. Com o término da numeração IPv4, se faz necessário a utilização de CGNAT, recurso tradutor utilizado atualmente no IPv4 que utiliza um único IP público como base para vários outros endereços IP de uma rede privada, mas que tem algumas desvantagens: sem conexão fim a fim e alguns problemas de segurança e confiabilidade. Como a numeração de IPV6 é abundante, todos os dispositivos na casa do cliente terão IP público, ou seja, estão “visíveis” de qualquer ponto da internet. O uso do IPV6 também traz mais segurança, confiabilidade e

escalabilidade para toda a rede.

CONCLUSÃO

O trabalho descreve a implementação do protocolo de rede IPv6 na BR Master provedor de acesso à internet, utilizando as técnicas de transição, para que o provedor estivesse em pleno funcionamento durante os aproximadamente 03 meses de implementação, visando manter o provedor sempre atualizado com as tecnologias existentes no mercado. Com o IPv6 implementado o provedor aumenta a segurança, confiabilidade e escalabilidade tanto para a sua rede quanto para seus clientes, com o grande número de endereços IPv6 todos os dispositivos dos clientes terão IP público, ou seja, estão visíveis de qualquer lugar da internet.

Na seqüência buscou-se atingir o objetivo específico, que era obter uma consultoria externa para auxiliar na implementação, à FB Consultoria foi contratada gerando um custo de aproximadamente R\$ 12.000,00 para o provedor, a consultoria fez todos os processos de implementação de acordo com a estrutura do provedor. A consultoria também verificou a compatibilidade dos equipamentos de infra-estrutura com o IPv6, após a verificação dos equipamentos foi necessário a substituição do roteador de borda e teve custo por volta de R\$ 6.000,00. A documentação da implementação foi providenciada pelo provedor com auxílio da FB Consultoria, a documentação e o formulário de aprovação foi enviada para a nic.br, o provedor adquiriu um bloco de IPv6 / 32 ou seja 79,228 nonilhões de endereços IPv6.

Durante a implementação foi substituído também um roteador de borda, devido ao esgotamento do poder de processamento do mesmo, um roteador novo com processador mais potente foi instalado, com custo de R\$ 6.000,00.

A questão problema: Com o esgotamento dos endereços IPv4 qual a importância da implementação do protocolo de rede IPv6 em um provedor de acesso à internet sem interromper o funcionamento do mesmo? E foi

solucionado, em entrevista a aplicada ao gestor do provedor o mesmo confirmou que durante a implementação do IPv6, não tiveram problemas que afetavam o funcionamento dos clientes que utilizavam IPv4, algumas interrupções inevitáveis, mas planejadas ocorreram, como por exemplo a troca do roteador de bora, que foi substituído durante a madrugada quando a maioria dos clientes estão inativos. Sobre a importância da implementação o gestor destacou: 'Como a numeração de IPV6 é abundante, todos os dispositivos na casa do cliente terão IP público, ou seja, estão "visíveis" de qualquer ponto da internet. O uso do IPV6 também traz mais segurança, confiabilidade e escalabilidade para toda a rede.'

O estudo traz como resultado para a empresa em análise toda a evolução tecnológica embarcada no IPv6, a fim de se destacar no mercado de atuação, levando internet de última geração até a casa de seus clientes deixando-os com mais segurança e confiabilidade no uso da internet.

REFERÊNCIA

ABRANET. **Associação Brasileira de Internet**. Disponível em <http://www.abranet.org.br/Noticias/Clientes-residenciais-da-Copel-Telecom-recebem-o-IPv6-808.html?UserActiveTemplate=site#.XfQeWOhKjIV> . Acesso em: 05 set. 2019.

ASHTON, K. **That "Internet of Things" Thing**. *RFID Journal*, p. 4986, 2009.

ATZORI, L.; IERA, A.; MORABITO, G. **The Internet of Things: A survey**. *Computer Networks*, v. 54, n. 15, p. 2787–2805, 2010.

BRITO, S. H. B. **A Internet das Coisas (IoT)**. LabCiscoA 2014. Disponível em: <<http://labcisco.blogspot.com.br/2014/07/a-internet-das-coisas.html>>. Acessado em 12 de outubro de 2019.

BRITO, Samuel Henrique Bucke. **IPv6 - O Novo Protocolo da Internet**. Novatec Editora. 2013. Acesso em: 30 mar.2019.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia Científica**. 6 ed. São Paulo: Person Prentice Hall, 2007.

CHASE, J. **The Evolution of the Internet of Things**. Texas Instruments, v. 1, n. February, p. 7, 2013.

DESLANDES, S. F. **A Construção do Projeto de Pesquisa**. In: MINAYO, Maria Cecília de Souza (Org.). *Pesquisa Social: Teoria, método e criatividade*. Petrópolis: Vozes, 2009.

DIERKS, T; ALLEN, C. **The TLS Protocol**. RFC 2246, IETF. 1999. Disponível <https://www.ietf.org/rfc/rfc2246.txt>em: Acesso em: 10 jun 2019.

FARREL, Adrian. **A Internet e seus Protocolos: Uma análise Comparativa**. Rio de Janeiro: Elsevier, 2005.

FENG, X.; LAURENCE, T. Y.; LIZHE, W. **Internet of Things**. *International Journal of Communication Systems*, v. 25, n. 9, p. 1101–1102, 2012.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5 ed. São Paulo: Atlas, 2010.

IPV6.BR. **Transição**. Disponível em: <http://ipv6.br/post/transicao/> Acesso em: 10 mai. 2019.

KUROSE, James F.; ROSS, Keith W. (Autor). **Redes de computadores e a Internet: uma abordagem top-down**. 5. ed. São Paulo: Pearson Addison-Wesley, 2010.

LOPES, J. **O fazer do trabalho científico em ciências sociais aplicadas**. Recife: UFPE, 2006.

MARCONI, M. LAKATOS, E. de A. **Fundamentos de metodologia científica**. 6. ed. 5. reimp. São Paulo: Atlas, 2007.

MEDEIROS, Aparecida Lopes de. **Evolução do Protocolo da Internet (IP): do IPv4 ao IPv6**. Universidade do Estado do Rio Grande do Norte, 2008

MOREIRAS, SANTOS, HARANO, CORDEIRO, NAKARAMURA, MORALES, GANZELI, CARNIER, LUGOBONI. **Laboratório de IPv6**. Disponível em: <http://ipv6.br/pagina/livro-ipv6/> Acesso em: 26 abr.2019. Acesso em: 18

mai.2019.

PRESCOTT, Roberta, **Endereços IPv4 acabam em janeiro de 2020 na América Latina**, Disponível em:

<https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&%25252525253buser=&UserActiveTemplate=site%252Csite&infoid=49168&sid=4>. Acesso em: 09 jul 2019.

RFC 6146.**Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers**. Disponível em:

<https://tools.ietf.org/html/rfc6146>> Acesso em: 1 jun. 2019.

RITZ, J.; KNAACK, Z. **Internet of Things. Technology and engineering teacher**, v. 76, p. 6, 2017.

SANTOS, R. R. dos. et al. **Apostila - IPv6 Básico**. São Paulo: Núcleo de Informação e Coordenação do ponto BR, 2012. Disponível em:<http://ipv6.br/media/arquivo/ipv6/file/60/ApostilaIPv62012.zip>. Acessado em: 7 mai 2019.

SILVEIRA, A. M. **Redes IPv6 com Integração IPv4**. 2003

TANENBAUM, A. S. **Redes de Computadores**. 5. ed. Rio de Janeiro: Elsevier, 2003.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de Computadores**. 5. ed. Rio de Janeiro: Elsevier, 2011.

VIANNA, Ilca Oliveira de Almeida. **Metodologia do trabalho científico: um enfoque didático da produção científica**. 1ed. São Paulo: E.P.U, 2001.

ZHAO R., WHANG J. **Visualizing the research on pervasive and ubiquitous computing**. *Scientometri9+cs*. n. 86, p. 593-612, 2011.