UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

JONES MAIKON MARCONSSONI

CONVERGÊNCIA ENTRE IPv4 e IPv6 COM A UTILIZAÇÃO DA TÉCNICA DE PILHA DUPLA: ESTUDO DE CASO NA PREFEITURA MUNICIPAL DE CORONEL MARTINS - SC

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO
2015

JONES MAIKON MARCONSSONI

CONVERGÊNCIA ENTRE IPv4 e IPv6 COM A UTILIZAÇÃO DA TÉCNICA DE PILHA DUPLA: ESTUDO DE CASO NA PREFEITURA MUNICIPAL DE CORONEL MARTINS - SC

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Adriano Serckumecka

PATO BRANCO
2015

TERMO DE APROVAÇÃO

Convergência entre IPV4 e IPV6 com a Utilização da Técnica de Pilha Dupla: Estudo de Caso na Prefeitura Municipal de Coronel Martins – SC

por

Jones Maikon Marconssoni

Esta monografia foi apresentada às 17h00min do dia 26 de outubro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Banca Examinadora

Prof. M.Sc. Adriano Serckumecka
Orientador / UTFPR-PB

Prof. Dr. Fábio Favarim
UTFPR-PB

Prof. Dr. Éden Ricardo Dosciatti
UTFPR-PB

Prof. Dr. Fábio Favarim
Coordenador do II Curso de Especialização
em Redes de Computadores

AGRADECIMENTOS

Em primeiro lugar a Deus pela oportunidade de sempre estar progredindo e aperfeiçoando o conhecimento adquirido.

A minha família, meu pai Doloir, minha mãe Zoleide e minha irmã Bruna, que sempre me deram forças e incentivos para a conclusão desse trabalho.

A minha esposa Rafaela, pelo incentivo, apoio e pelas conversas estimulantes sobre a importância de cada item de um projeto de pesquisa.

A minha filha Alice, que apesar de ainda não estar presente, motivou imensamente o seu pai a cumprir mais essa etapa na vida.

Ao meu Professor Orientador Adriano Serckumecka, que não poupou esforços e tempo para que conseguíssemos alcançar nosso objetivo.

RESUMO

MARCONSSONI, Jones Maikon. CONVERGÊNCIA ENTRE IPv4 e IPv6 COM A UTILIZAÇÃO DA TÉCNICA DE PILHA DUPLA: ESTUDO DE CASO NA PREFEITURA MUNICIPAL DE CORONEL MARTINS - SC. 2015. 43 f. Monografia II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

A Internet tornou-se uma parcela considerável do dia a dia da população mundial. Atualmente existe uma variedade imensa de dispositivos de rede que permitem a conexão a ela. Dessa forma, eles devem ser endereçados de alguma maneira, e durante as últimas décadas, o protocolo responsável por executar essa função foi o IPv4. No momento atual existe uma nova versão do protocolo IP, o IPv6, que também possibilita o endereçamento dos dispositivos, de maneira que há a possibilidade de ambos coexistirem simultaneamente nos equipamentos. Em virtude disso, este trabalho visa explorar técnicas, que proporcionem a transição entre as versões desse protocolo. A partir da criação de um cenário de simulação, a técnica de migração de pilha dupla será implementada visando a total convergência entre as duas versões do protocolo IP.

Palavras-chave: IPv4. IPv6. Transição. Pilha dupla.

ABSTRACT

MARCONSSONI, Jones Maikon. CONVERGENCE BETWEEN IPv4 and IPv6 WITH TECHNICAL USE DOUBLE STACK: CASE STUDY IN THE TOWN HALL CORONEL MARTINS - SC. 2015. 43 f. Monografia (II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

The Internet has become a considerable part of the day to day of the world's population. Currently there is a wide variety of network devices that let you connect to it. Thus, they should be addressed in some way, and during the last decades, the protocol responsible for performing this function was IPv4. At the moment, there is a new version of the Internet protocol, IPv6, which also allows the addressing of the devices so that there is the possibility of both coexists simultaneously in the equipment. As a result, this paper aims to explore techniques that provide the transition between versions of this protocol. From the creation of a simulation scenario, the dual stack migration technique will be implemented with a view to full convergence between the two versions of IP protocol.

Keywords: IPv4. IPv6. Transition. Dual stack

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS, ABREVIATURAS E ACRÔNIMOS

ARPANET - *Advanced Research Projects Agency Network*

MILNET - *Military Network*

ISO - *International Organization for Standardization*

DoD - *Departament of Defense*

TCP/IP - *Transmission Control Protocol / Internet Protocol*

MAC - *Media Access Control*

ARP - *Address Resolution Protocol*

HTTP - *Hypertext Transfer Protocol*

SMTP - *Simple Mail Transfer Protocol*

FTP - *File Transfer Protocol*

DNS - *Domain Name System*

ICMP - *Internet Control Message Protocol*

RFC - *Request for Comments*

CIDR - *Classless Inter-Domain Routing*

NAT - *Network Address Translation*

SSH - *Secure Shell*

NDP - *Neighbor Discovery Interface*

SLAAC - *Stateless Addres Autoconfiguration*

SUMÁRIO

1 INTRODUÇÃO

O protocolo IPv6, vem se tornando uma realidade a cada dia, assim como a necessidade de domínio e conhecimento para sua implementação. O IPv6 apresenta diversas melhorias em relação ao seu antecessor, tornando essa evolução obrigatória para todos os segmentos que utilizam redes de computadores em sua estrutura lógica de funcionamento.

Em sua grande maioria, as empresas utilizam em sua estrutura de rede o IPv4, porém como o esgotamento de endereços IPv4 presente, essas empresas precisam migrar para a nova versão do protocolo, obtendo no IPv6 a única solução para esse problema.

O intuito desse trabalho é expor técnicas de convergência entre essas duas versões de protocolo, IPv4 e IPv6, levando em conta que a implementação desse novo protocolo, não poderá será feita de imediato e de uma só vez. Assim esse trabalho, possui o desafio apresentar cenários onde ambos os protocolos podem coexistir.

1.1 Objetivo Geral

Este trabalho tem o objetivo de fornecer para a Prefeitura Municipal de Coronel Martins um ambiente de transição para IPv6 com total interoperabilidade, garantindo conexão interna ou externa independente da versão do protocolo utilizado, através da técnica de pilha dupla.

1.2 Objetivos Específicos

Esse trabalho possui os seguintes objetivo específicos:

- ✓ Analisar a viabilidade da técnica de transição de pilha dupla no cenário proposto;
- ✓ Elaborar um projeto lógico da rede da Prefeitura Municipal de Coronel Martins - SC;

- ✓ Propor a segmentação de rede através da utilização de VLANs em um ambiente real;
- ✓ Desenvolver e implementar um endereçamento IP hierárquico, com base na segmentação de rede;
- ✓ Elaborar um cenário de protótipo no simulador Packet Tracer, com utilização da técnica de transição de pilha dupla.

1.3 Justificativa

Com base na solução de transição apresentada, o trabalho irá expor que as duas versões do protocolo IPv4 e IPv6 podem coexistir. Apesar de ser conhecido o real esgotamento IPv4 e com isso a necessidade de transição para o novo protocolo, muitas dessas instituições públicas, como a Prefeitura Municipal de Coronel Martins – SC, não se preocupam com a urgência da situação.

Entretanto, essas instituições podem e devem aplicar essas técnicas, sendo possível aplicá-las de forma gradual sem que haja necessidade de parada de serviços.

Dessa forma o conhecimento das técnicas de transição, como tunelamento, tradução e pilha dupla, e novos protocolos se torna imprescindível para profissionais de redes e demais interessados da área. Atingir todos os objetivos propostos servirá como base para a implementação da solução mediante o problema apresentado.

1.4 Estrutura do Trabalho

O presenta trabalho esta organizado em 5 (cinco) capítulos, da seguinte maneira:

Capitulo 1: apresenta a introdução ao trabalho, expõe ao leitor o contexto do problema, objetivos e uma breve justificativa do propósito da pesquisa feita.

Capitulo 2: neste capitulo é apresentado a base teórica que foi necessária para o desenvolvimento dessa atividade.

Capitulo 3: Neste capitulo são apresentados os materiais utilizados no desenvolvimento desde trabalho, assim como a metodologia utilizada.

Capitulo 4: Serão apresentados nesse capítulo, os detalhes da nova infraestrutura proposta pelo projeto, do mesmo modo as vantagens de sua implementação e os benefícios futuros ao cliente.

Capitulo 5: Finalizando no Capitulo 5, apresenta a conclusão do trabalho com uma pequena avaliação e algumas considerações técnicas com relação ao conteúdo.

2 REFERENCIAL TEÓRICO

2.1 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 a transmitida.

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 reordena-los corretamente, nesse caso o *TCP*.

2.1.1 IPv4

O IPv4 é a versão mais utilizada do protocolo IP nas redes atualmente, sendo composto por 32 bits para endereçamento representados 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.

2.1.1.1 Cabeçalho IPv4

Nesta versão do protocolo IP doze campos fixos compõe o cabeçalho ou estrutura, seu tamanho pode variar de 20 a 60 bytes dependendo de opções que podem ou não ocorrer, a figura 1 demonstra o cabeçalho do protocolo IPv4.

Figura 1 - Cabeçalho protocolo 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 permita 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.
- ✓ **Identificador, flags, deslocamento de fragmentação**: Estes três campos têm a ver com a fragmentação IP.
- ✓ **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 de ume 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. Casa 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.

2.1.1.2 Endereçamento

Como citado anteriormente, em uma rede baseada no protocolo IP, cada computador ou host é identificado através de um endereço IP, permitindo através disso, identificar o host e também a rede a qual ele pertence. O roteamento desses endereços na rede fica a cargo do roteador, um dispositivo que serve como saída dos pacotes desta rede em direção ao seu destino.

O endereço IP é um número de 32 bits, representado em decimal em forma de quatro números de oito bits separados por um ponto, no formato a.b.c.d, sendo assim, o menor endereço IP possível é o 0.0.0.0 e o maior 255.255.255.255 (TORRES, 2001). Com isso, teoricamente poderíamos ter mais de quatro milhões de endereços IP ou de dispositivos em uma rede.

Abaixo, a figura 2 apresenta algumas classes de endereçamento IPv4, com suas respectivas máscaras de subrede e demais especificações.

Classes IPv4 - Redes Privadas

Classe	Faixa de endereços de IP	Máscara de Subrede padrão	Notação CIDR	Número de Redes	Número de IPs	IPs por rede
A	10.0.0.0 – 10.255.255.255	255.0.0.0	/8	126	16.777.215	16.777.216
B	172.16.0.1 – 172.31.255.254	255.255.0.0	/16	16.382	1.048.576	65 534
C	192.168.0.0 – 192.168.255.255	255.255.255.0	/24	2.091.150	65.535	256

Figura 2 - Divisão de classes IPv4
Fonte (WIKIPEDIA, 2015)

Atualmente todos os endereços IP válidos na Internet possuem proprietário, logo não podemos utilizá-los precipitadamente. Assim quando nos conectamos

a Internet, recebemos um IP emprestado ou alugado pelo provedor de acesso e através dele que outros hosts da Internet nos enviam informações.

2.1.1.3 CIDR

A divisão de endereços IP em classes trouxe um enorme desperdício de endereços, visto que as classes não poderiam ser particionadas, somente conseguia-se os endereços necessários com a obtenção da classe inteira.

A solução para o problema foi a implantação do sistema CIDR (*Classless Inter-Domain Routing*), pronunciada como “cider”, a partir de 1993 (KUROSE, 2011).

Com o CIDR ao invés de se utilizar máscaras de rede estáticas, foram implementadas máscaras de tamanho variável permitindo flexibilidade maior na criação das faixas de endereços. Abaixo a tabela 1 apresenta alguns exemplos de máscaras variáveis e quantidades de redes e hosts permitidos.

Máscara	Bits da rede	Bits do Host	Número de redes	Número de hosts
255.255.255.0(/24)	Nenhum	00000000	Nenhuma	254 endereços (1 ao 254)
255.255.255.192 (/26)	11	000000	2 endereços (2 e 3)	62 endereços (1 a 62)
255.255.255.240 (/28)	1111	0000	14 endereços (1 a 14)	14 endereços (1 a 14)

Tabela 1 - Máscaras variáveis IPv4
Fonte: Autoria própria

2.1.1.4 Máscaras de Rede

Com essa definição de classes tradicionalmente utilizada, o endereço IPv4 tem o acompanhamento obrigatório de uma máscara de rede. Como exemplo, um endereço IP de classe A, possui uma máscara de rede igual a 255.0.0.0, onde o primeiro octeto refere-se a rede a qual o endereço pertence e os outros três identificam o host.

2.1.1.5 Prefixo de rede

Como citado anteriormente, o endereçamento IP possui 32 bits, sendo dividido em duas partes, com decimais separado por pontos a.b.c.d/x, onde x indica o número de bits existentes na primeira parte do endereço (KUROSE, 2011).

Esses bits constituem a parcela mais significativa de um endereço IP, representam a parcela do endereçamento de rede e normalmente são denominados prefixos de rede.

2.1.1.6 Subredes

As subredes são pequenas divisões que ocorrem dentro de uma mesma rede, segmentando a rede, tornando menor o número de hosts disponíveis, assim um maior aproveitamento dos endereços.

Com sua utilização, é possível interligar várias interfaces de rede, dividindo e organizando-as em redes menores, sem a necessidade da aplicação de um roteador para efetuar esse serviço.

2.1.1.7 NAT

O NAT (*Network Address Translation*) é uma técnica avançada de roteamento que permite que vários *hosts* acessem a Internet usando um único endereço de IP válido (MORIMOTO, 2010).

Deste modo, quando um pacote da rede local for direcionado para a Internet, o NAT mascara esse endereço, possibilitando assim a todos os hosts locais o acesso à Internet através de um único IP válido. Esse processo de tradução ocorre em tempo real, sem adição de latência ou redução de velocidade de conexão.

2.1.1.8 DHCP

O protocolo de configuração dinâmica de endereços de rede ou DHCP (*Dynamic Host Configuration Protocol*) permite através de um servidor ou roteador, o recebimento de uma configuração automática por todos os hosts da rede (KUROSE, 2011).

Essa configuração é obtida através de uma forma bem interessante, pois inicialmente o host não sabe que é, não possui endereço IP e não sabe qual é o endereço do servidor DHCP da rede. Assim, o host envia para a rede um pacote de broadcast ao IP 255.255.255.255, que é transmitido para toda a rede. Ao receber esse pacote o servidor DHCP responde com outro pacote de broadcast com endereço IP 0.0.0.0, transmitindo-o a toda rede.

Contudo, somente o host que enviou a solicitação lerá o pacote, pois este, é associado ao endereço MAC da placa de rede da estação. Neste pacote enviado pelo servidor, estão especificados o endereço IP, máscara de rede, gateway e servidor DNS que serão utilizados pelo host.

2.1.2 Limitações do IPv4 e Esgotamento de IPs

Como foi apresentado anteriormente com crescimento exponencial da Internet o protocolo IP versão 4 tornou-se obsoleto, por não ter disponibilidade suficiente de IPs a todos os seus usuários. A versão propriamente dita não é pequena, porém a política de divisão em classes de endereçamento, causou um grande desperdício de recursos no início do projeto, disponibilizando somente classes cheias de endereços IP as instituições interessadas.

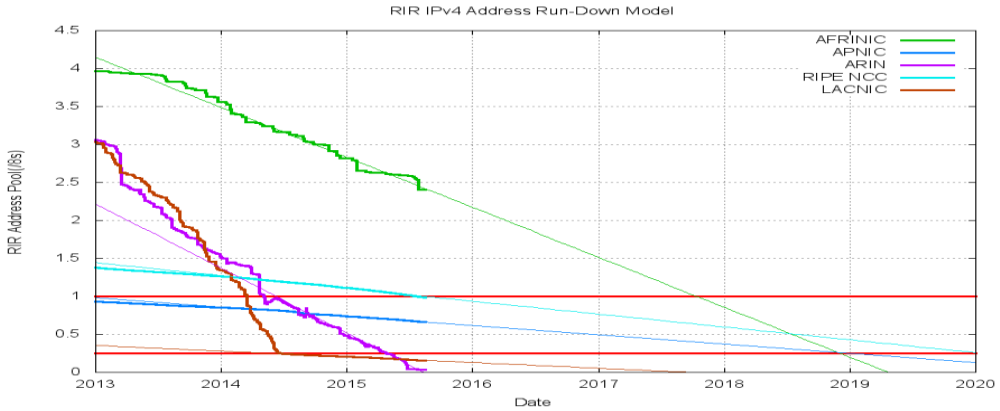

Figura 3 - Alocação de endereços IPv4, cálculo aproximado
Fonte (IPV6, 2015)

Diante disso, várias ferramentas ou soluções temporárias foram implementadas, na tentativa de retardar o esgotamento de IPs. Dentre essas, pode-se citar algumas, as quais foram apresentadas nos itens anteriores deste trabalho, como o CIDR, NAT e o DHCP.

Além do esgotamento de endereços, o IPv4 possui uma falha de desenvolvimento grave, pois não possui camadas de autenticação e encriptação, tanto que essas tarefas são adicionadas através de protocolos implantados sobre o TCP/IP, como por exemplo, o SSH.

2.1.3 IPv6

Conforme foi falado anteriormente, a Internet foi projetada para conectar máquinas e redes estáticas, fixadas e instaladas em edifícios ou bases militares, não tendo suporte algum a mobilidade. A partir do início do século XXI, houve uma grande difusão comercial em torno da Internet que em grande parte foi impulsionada pela intensa disseminação de dispositivos móveis para seu acesso.

Através desses fatores deu-se início a uma nova era, em que o elemento mais importante de uma rede deixa de ser a máquina e passa a ser o próprio usuário. Nessa era, as pessoas estão conectadas a Internet em qualquer lugar, por meio de diversos dispositivos, sejam eles móveis ou tradicionalmente fixos (BRITO, 2013).

Essa "era das pessoas" futuramente dará lugar a "era das coisas" em que qualquer coisa em qualquer lugar estará conectada a Internet para os mais variados fins. Contudo, para que esse grande avanço de conectividade se torne realmente viável, necessitamos muito mais que os 4.3 bilhões de endereços disponibilizados pelo IPv4, além de uma estrutura de segurança e mobilidade melhoradas.

O IPv6 atende a todos esses objetivos e necessidades propostas, além disso preserva os bons recursos do IP, descartando ou reduzindo a importância das características ruins e criando outras quando necessário. Genericamente, o IPv6 não é compatível com o IPv4, porém oferece compatibilidade a todos os outros protocolos auxiliares utilizados na Internet como TCP, UDP, ICMP, IGMP, entre outros (TANENBAUM, 2003).

Dentre as vantagens do IPv6 que pode-se destacar algumas, como um espaço de endereçamento quase ilimitado, processamento simplificado nos roteadores, dispensa a adoção de técnicas como o NAT, maior e melhor segurança com o IPSec embutido nele, além de um suporte à mobilidade com o MIPv6. Nos próximos capítulos será descrito cada uma das vantagens apontadas acima bem como algumas correções que possivelmente serão efetuadas em sua estrutura.

2.1.3.1 Cabeçalho do protocolo IPv6

Talvez a maior evolução do IPv6 em relação ao seu antecessor o IPv4 foi exatamente da estruturação dos campos presentes nos cabeçalhos. No protocolo IPv4 o cabeçalho possui 12 campos fixos, e um tamanho variável que pode ficar entre 20 e 60 bytes, já no protocolo IPv6 com seu formato otimizado, possui apenas 8 campos e um tamanho fixo de 40 bytes, conforme mostra a Figura 3, simplificando assim a eletrônica dos equipamentos, com tamanho fixo os roteadores não precisam analisar previamente um campo para determinar o tamanho do cabeçalho, melhorando assim consideravelmente seu desempenho.

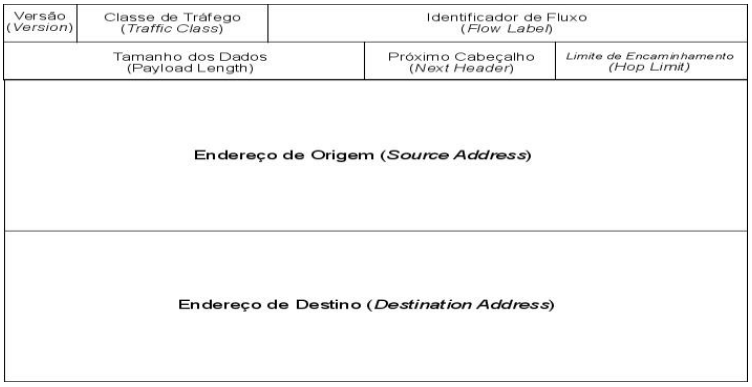

Figura 4 - Cabeçalho IPv6
Fonte (IPV6, 2015)

A seguir será apresentado uma breve descrição de cada campo do cabeçalho do protocolo IPv6:

- ✓ **Version:** Esse campo indica a versão do protocolo, no caso do IPv6, possuirá um valor 6.
- ✓ **Traffic class**: É utilizado para fazer distinção entre pacotes com diferentes requisitos de entrega em tempo real;

- ✓ **Flow label**: Esse campo tem uma funcionalidade que consiste em associar vários pacotes de uma mesma natureza em um único fluxo para fins de classificação e filtragem do tráfego, muito útil para aplicações multimídia.
- ✓ **Payload lenght**: Determina o número de bytes que seguem o cabeçalho de 40 bytes.
- ✓ **Next header**: Existe a possibilidade de haver outros cabeçalhos de extensão. Esse campo informa quais dos cinco cabeçalhos de extensão seguem esse cabeçalho.
- ✓ **Hop limit**: Sua função é impedir que os pacotes tenham duração eterna, na prática é igual ao campo TTL do IPv4.
- ✓ **Source address** e **Destination address**: Armazenam respectivamente o endereço fonte de onde partiu o pacote e o endereço para onde o pacote se destina.

2.1.3.2 Endereçamento IPv6

Como foi abordado anteriormente, a versão 6 do protocolo IP traz inúmeras mudanças em relação ao seu antecessor, no entanto, as duas mais marcantes dizem respeito a sua notação, ou seja seu formato de escrita e a sua estrutura que passa a ter 128 bits ao invés de 32.

O endereçamento IPv6 é escrito em formato hexadecimal, dividindo-o em 8 grupos de 16 bits cada um e separando-os pelo caractere ":", a seguir um exemplo: 2001:0db8:cafe:0000:8e70:5aff:feee:10ac (BRITO, 2013). Não havendo diferenciação de maiúsculas e minúsculas em uma representação alfanumérica escrita do IPv6.

A adoção do formato hexadecimal aconteceu em virtude desse sistema de numeração viabilizar a diminuição do tamanho dos endereços, levando em consideração e comparação aos sistemas binário e decimal.

Como esse sistema nos fornece endereços extensos, técnicas de abreviação podem ser aplicadas, ajudando a simplificar suas representações. Uma das regras consiste em omitir todos os zeros a esquerda do quarteto e uma segunda regra permite a representação de uma sequência continua de zeros por meio do

caractere ":". Na tabela a seguir podemos visualizar exemplos das duas regras de abreviação.

2001:0db8:0000:0000:0000:0000:0000:00b1
Primeira regra:
2001:db8:0:0:0:0:0:b1
Segunda Regra:
2001:db8::b1

Tabela 2 - Regra de abreviação IPv6
Fonte: Autoria própria

2.1.3.3 Redes IPv6 (prefixos/cidr)

Como foi visto anteriormente no IPv4 uma primeira parte do endereço identificava a rede ou prefixo e uma segunda parte do endereço identificava o host ou sufixo, o limite entre prefixo e sufixo era determinado pela máscara de rede. Também foi abordado uma outra forma de notação da máscara de rede, o CIDR, que permite que uma máscara no formato 255.0.0.0 seja apresentada de forma simplificada no formato /8.

No IPv6 a estrutura inicial foi mantida, prefixos e sufixos, porem a máscara de rede deixa de existir, sendo obrigatório a utilização da notação CIDR em sua representação. Essa mudança ocorreu em função do tamanho dos endereços, que trariam consigo mascaras muito extensas no formato hexadecimal do IPv6.

No protocolo IPv4 era comum o planejamento de endereçamento ou determinação do prefixo da rede, com base na quantidade de hosts necessários, visando a economia de endereços IP, já no IPv6 todas a redes locais devem ter necessariamente o prefixo /64, o que torna a quantidade de hosts nas subredes irrelevante (BRITO, 2013).

2.1.3.4 Tipos de endereços IPv6

Quando falamos em comunicação em redes de computadores, coerentemente temos que falar sobre os diferentes tipos de endereços que são associados a ela. Como em seu antecessor, o IPv6 também possui diferentes tipos de comunicação, mais especificamente três: *unicast*, *multicast* e *anycast*.

Apesar de possuir a mesma quantidade de variações que o IPv4, várias mudanças na estrutura dos tipos de endereços IPv6 serão apresentadas. Uma das mais importantes, sem dúvida, foi a remoção dos endereços broadcast, que consistiam no IPv4 no ultimo endereço válido de cada subrede podendo, a mensagem, ser enviada a todos os hosts da rede.

No IPv6 também há essa possibilidade, porém com um grupo de endereços *multicast* nativos, a seguir apresentaremos detalhes e uma breve descrição de cada tipo.

2.1.3.5 Endereços Unicast

Os endereços u*nicast* são responsáveis por identificar um host de maneira homogênea por meio de uma interface específica, de modo que o envio do pacote será entregue a uma única interface. Esses endereços ainda podem ser *link-local*, *unique-local* ou *global unicast*.

2.1.3.6 Endereços Multicast

O *multicast* é crucial para o funcionamento do IPv6 fazendo parte da essência de sua operacionalização por meio da criação/associação de vários grupos padronizados em que as interfaces passam a integrar no momento em que são ativadas (BRITO, 2013).

Foi através de um grupo do *multicast*, o *multicast-all-nodes*, que o endereço de broadcast pode ser eliminado no IPv6. Esse grupo permite a comunicação de um host para com os demais hosts da rede, por meio de um novo endereço distintamente padronizado para isso.

2.1.3.7 Endereços Anycast

Os endereços *anycast* são uma novidade trazida pelo IPv6 no que diz respeito a modelos de comunicação. Consiste em uma comunicação destinada ao nó mais próximo de nosso grupo, assim torna possível a atribuição de um mesmo endereço "*unicast*" para vários hosts, desde que seja informada a palavra *anycast* em sua configuração.

2.1.3.8 Protocolo NDP

O NDP (*Neighbor Discovery Interface*) ou simplesmente Protocolo de Descoberta de Vizinhança, tem a responsabilidade das mais diversas funcionalidades dentro do IPv6, tornando-se essencial para operação de redes baseadas nessa versão do protocolo IP. Entre as várias tarefas que o NDP pode executar, podemos citar algumas, como a descoberta de parâmetros, redirecionamento de roteadores, detecção de vizinhança ou mesmo a resolução dos endereços MAC.

2.1.3.9 SLAAC

Inegavelmente uma das mais interessantes novidades do IPv6, é a possibilidade da rede se autoconfigurar sem a necessidade de um servidor DHCP ativo na mesma. Essa forma de autoconfiguração denomina-se SLAAC (*Stateless Addres Autoconfiguration*), ela não mantém nenhum registro da atribuição dos endereços, pois ocorre diretamente nos hosts.

2.1.3.10 DHCPv6

No IPv4 como vimos anteriormente, o DHCP era responsável por manter uma tabela onde associava endereços físicos dos hosts (MAC) aos endereços lógicos atribuídos (IP), disponibilizando e distribuindo aos hosts configurações como gateway e servidor DNS.

No IPv6 o panorama alterou-se consideravelmente, pois as redes IPv6 possuem suporte ao processo de autoconfiguração, SLAAC, como comentamos anteriormente, tornando um servidor DHCP um item dispensável em uma rede desse tipo.

Contudo, a possibilidade de utilização do um servidor DHCP para fins de gerencia ou para prover algumas informações ainda pode ser aplicado. Nesses casos o DHCP se torna uma reprodução tradicional do DHCPv4, provendo informações de endereçamento a todos os hosts da rede, sendo assim, uma modalidade *statefull*.

2.2 Mecanismos de transição

Todos concordamos que a evolução natural da Internet será o IPv6, porem mesmo tendo essa consciência, temos que levar em conta o alto grau de disseminação do IPv4, que aliado a falta de profissionais preparados para trabalhar com IPv6 e o alto custo dos equipamentos para implementação do mesmo, causam uma lentidão a esse processo de transição.

Assim o prazo para que essa transição ocorra por completo não é exato, podendo levar alguns anos ou até mesmo décadas. Nesse período teremos duas tecnologias operando em paralelo, tecnologias não compatíveis diretamente entre si e com muitas diferenças de caracterização entre elas.

Dessa forma será fundamental a adoção de mecanismos de transição que proporcionem a comunicação entre essas tecnologias, não causando prejuízos e tornando-se imperceptíveis aos usuários essa transformação. 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).

2.2.1 Pilha dupla

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

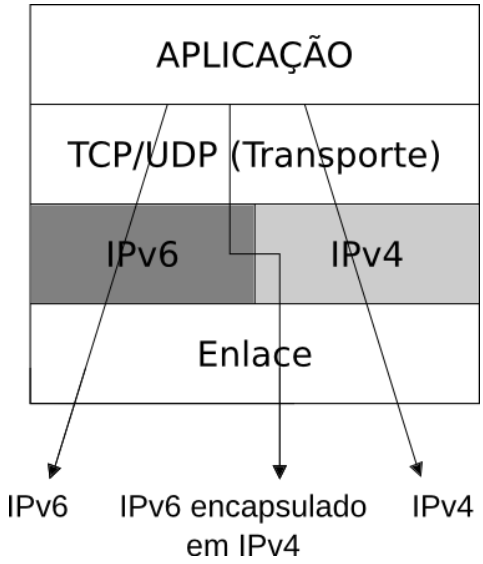

Figura 5 - Funcionamento da técnica de pilha dupla
Fonte (IPV6, 2015)

Essa técnica de pilha dupla, é vista com bons olhos para o bom desenvolvimento do protocolo, pois como o IPv6 estará sendo inserido na rede de forma progressiva, oferecerá 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.

2.2.2 Tunelamento

Quando não há a possibilidade de adoção da pilha dupla nos dispositivos, uma das alternativas viáveis é o tunelamento, que consiste no encapsulamento de pacotes IPv6 dentro de pacotes IPv4, de uma outra maneira, viabilizam que o trafego baseado em uma tecnologia, IPv4 ou IPv6, possa ser transportado por um meio transferência baseado em outra tecnologia. Abaixo uma figura demonstra a técnica de tunelamento.

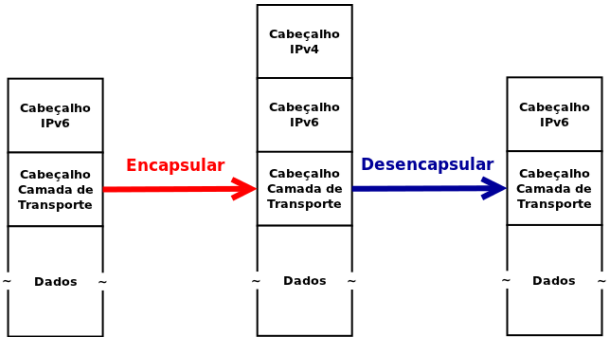

Figura 6 - Técnica de tunelamento
Fonte (IPV6, 2015)

Ainda que as técnicas de tunelamento sejam interessantes por viabilizar uma rápida facilitação operacional na comunicação entre essas tecnologias, causam preocupação, pois além de possuírem um pior desempenho comparado as outras técnicas de transição, elas não contribuem para a concretização completa da transição para o IPv6, trazendo consigo um efeito negativo, a manutenção do IPv4 ativo por mais tempo que o desejado.

Atualmente existem inúmeras técnicas de tunelamento publicadas em RFCs, dessa forma ficaria impossível abordarmos todas elas, levando em conta isso trabalharemos com as mais tradicionais, comumente mais utilizadas.

2.2.2.1 Túnel Manual 6over4 (6in4)

Nessa técnica um túnel manual é estabelecido entre dois nós IPv4, trabalhando com trafego IPv6. Esse trafego é permitido através do encapsulamento 6in4, que consiste em colocar os pacotes IPv6 dentro dos pacotes IPv4, adequando os cabeçalhos e colocando uma marcação tipo 41 nos mesmos, assim quando o destino receber um pacote com tipo 41, ele removerá o cabeçalho IPv4 tratando-o como pacote IPv6.

Nesse ponto é importante entendermos a diferença entre 6over4 e 6in4. O primeiro, ou 6over4, é propriamente um túnel estabelecido manualmente que permite conexão IPv6 entre nós IPv4, já o 6in4 é a técnica de encapsulamento utilizada por esse túnel em questão, técnica essa que também pode ser utilizada em outros mecanismos de transição.

2.2.2.2 Túnel 6to4

A técnica de tunelamento 6to4 consiste na formação de túneis automaticamente configurados entre hosts ou sites que possuem transito IPv4, ou seja, necessitam de acesso à Internet IPv6. Esse método somente é possível com ajuda de *relays* de pilha dupla públicos distribuídos pela Internet, estes executam a pilha dupla tornando-se responsáveis pela intermediação da comunicação IPv4 e IPv6.

Essa técnica de tunelamento é tradicionalmente muito utilizada, porém, traz consigo alguns problemas que tem causado seu abandono. Um problema que atinge o 6to4, diz respeito à segurança, afinal, os *relays* são públicos e bem conhecidos tornando-se alvos fáceis de ataques que gerem negação de serviço ou mesmo a falsificação por meio de *spoofing*, um *relay* intermediário falso.

2.2.3 Tradução

A tradução é um mecanismo de transição utilizado na comunicação de hosts que operam somente com uma versão do protocolo IP, ou que utilizem pilha dupla, possibilitando um roteamento transparente no trafego de pacotes entre eles. Pode realizar tanto a conversão de endereços como a troca de trafego TCP ou UDP (BRITO, 2013).

2.3 Limitações do IPv6

Quando abordamos as limitações do IPv6, nos atemos a poucos itens, pois como sucessor de um protocolo com diversos problemas estruturais e de planejamento, o IPv6 surge com a responsabilidade corrigir as falhas existentes em seu antecessor e suportar o crescimento exponencial do uso da Internet dos dias atuais.

Dessa forma, as maiores dificuldades encontradas serão sem dúvida na longa demora para a transição completa de uma versão do protocolo para outra. Por isso, como apresentamos anteriormente, existem diversas ferramentas para auxilio a essa transição, cabendo ao usuário escolher qual se adapte melhor a sua realidade.

3 MATERIAIS E MÉTODO

Este capítulo apresenta os materiais e o método utilizados no desenvolvimento deste trabalho.

3.1 MATERIAIS

Para o desenvolvimento do cenário que será apresentado nesse trabalho, foi utilizado um notebook básico, com as seguintes configurações:

- Processador Inter Core i5;
- 8gb de memória RAM;
- HD 750gb;

Foram utilizados também os seguintes softwares:

- Sistema Operacional Microsoft Windows 10 Pro 64bits;
- Microsoft Office 2010;
- Cisco Packet Tracer 6.2 (6.2.0.0052);

3.1.1 Cisco Packet Tracer

O Cisco Packet Tracer é um software simulador de rede, que permite aos seus usuários criar, praticar e solucionar problemas de rede através de uma interface gráfica simples. É um programa gratuito e esta disponível para download no próprio site da CISCO.

3.2 MÉTODO

Neste capitulo é demonstrado o desenvolvimento do trabalho e o método de aplicação das técnicas de rede para construção do modelo base da topologia de rede da Prefeitura Municipal de Coronel Martins.

A elaboração desse trabalho ocorreu em duas etapas: inicialmente foi desenvolvido uma pesquisa bibliográfica das soluções atualmente disponíveis para transição IPv4/IPv6, bem como seus funcionamentos e métodos de implementação. Posteriormente foi criado um cenário de simulação para testes,

para assim testar e comprovar funcionalidade da técnica escolhida e da configuração utilizada.

Primeiramente para obter uma plataforma de testes viável, foi necessário o estabelecimento de um cenário com uma comunicação simples IPv4. Após isso, deu-se a implementação do IPv6, juntamente com a inserção de outros elementos de rede necessários para testarmos o roteamento e a transição IPv4/Ipv6.

Diante disso foi desenvolvido um projeto lógico em Packet Tracer, para visualização da estrutura como um todo e também para proporcionar um ambiente aceitável onde fosse possível efetuar testes confiáveis, tanto na infraestrutura quanto nas conexões sugeridas.

Com base nesse projeto também foi possível elaborar uma segmentação da rede em VLANs, tendo como base a estrutura interna de funcionamento desse órgão público, isolando e separando a rede por setores e locais, melhorando o gerenciamento dos recursos, manutenção e segurança da rede de um modo geral.

Com a segmentação de rede se tornou viável a elaboração de um esquema hierárquico de endereçamento IPv4 e IPv6, possibilitando a cada VLAN, um endereçamento particular. Oferecendo assim, um melhor gerenciamento de rede, através de um roteamento mais enxuto e organizado, além de um melhor aproveitamento dos recursos dos setores internos desse órgão público, por meio do acesso interligado entre as VLANs internas.

4 RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados os detalhes das melhorias propostas a infraestrutura de rede presente na Prefeitura Municipal de Coronel Martins e também os testes realizados no ambiente de simulação Packet Tracer.

4.1 Apresentação do cenário

Com o intuito de atingir os objetivos propostos por esse trabalho, foi criado o seguinte modelo de simulação no Packet Tracer, conforme apresenta a Figura 12.

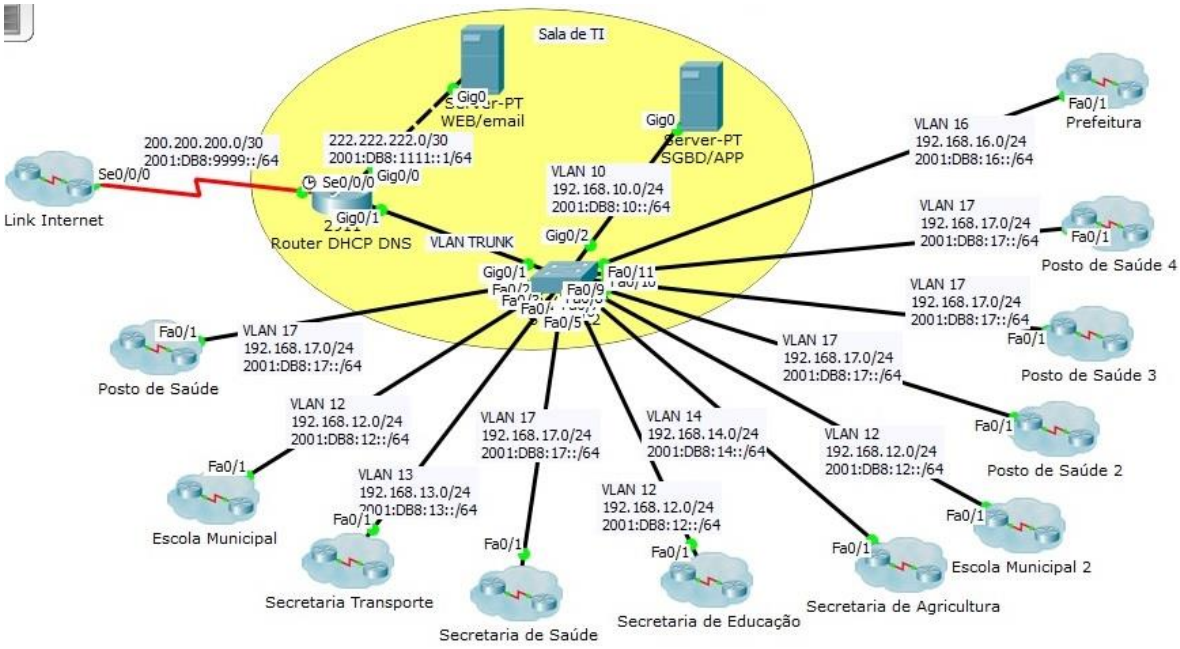

Figura 7 - Topologia de rede proposta para implementação
Fonte: Autoria Própria

Nesse cenário foi construído um protótipo, utilizando como base de rede IPv4 existente na Prefeitura Municipal de Coronel Martins, com a implementação de algumas melhorias. Abaixo segue a Figura 9, uma ilustração da sala de TI, seus servidores e link externo.

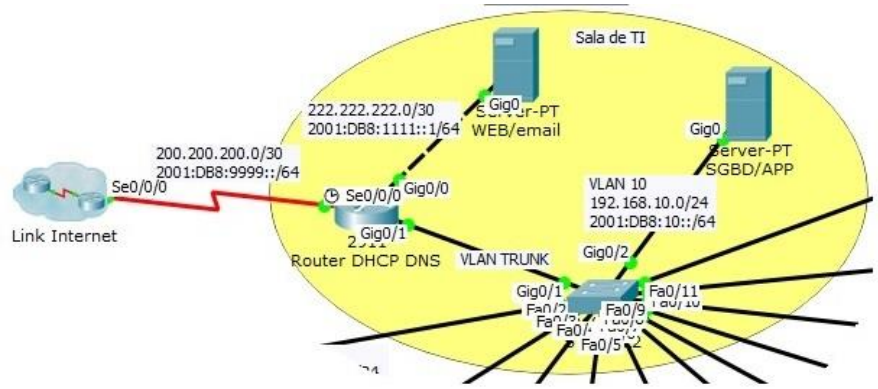

Figura 8 - Sala de TI, servidores e link externo
Fonte: Autoria Própria

A Prefeitura Municipal de Coronel Martins terá conexão com seu Router Web IPv4 através de uma pilha dupla. Assim quando a rede tenta trafegar sob um endereço IPv4 externo ela irá trafegar pela pilha IPv4 e sem divulgar o endereço de sua rede interna através do NAT. Quando o processo ocorrer com trafego IPv6, os endereços serão atribuídos através de um servidor DHCPv6 sem necessidade da utilização do NAT.

4.2 Descrição da proposta

A estrutura atual de rede da Prefeitura Municipal de Coronel Martins está totalmente ultrapassada, não possui nenhuma gerência de recursos ou de usuários, os setores estão desconexos e os servidores locais localizados em salas sem condições alguma de abriga-los.

Com a implementação desse projeto, iremos proporcionar uma melhoria considerável na estrutura de rede e organizacional dos setores que compõe esse órgão. Através dele, poderemos efetuar a segmentação dos departamentos em VLANS, interconexão de seus setores, melhoria na gerencia, na manutenção, no roteamento e na segurança de rede como um todo.

Dessa forma, esse projeto trará para esse órgão público inúmeras vantagens. Proporcionará um melhor controle interno no tráfego de dados e de usuários, com uma maior velocidade e confiabilidade no acesso as informações desejadas.

Também devemos falar da redução de gastos com reparos e manutenções na rede, pois como falamos anteriormente, essas mudanças oferecerão uma organização mais centralizada, isolando o problema e propiciando uma identificação e localização do defeito com maior rapidez, assim gerando menos custos.

Outro ponto que temos a obrigação de salientar, com relação as vantagens da implantação desse projeto, é a transição inevitável IPv4 para IPv6. Com o esgotamento da versão 4 do protocolo IP, todos deverão migrar para a versão 6 desse protocolo, tornando assim, sua versão anterior obsoleta e futuramente sem suporte.

Assim, com a técnica de transição de pilha dupla que é proposta pelo projeto, a rede continuará em funcionamento até sua migração total, pois ambas versões do protocolo trabalharão em cada terminal. Cada host, terá um endereço IPv4 e um IPv6, tornando assim, uma transição possivelmente complicada, simples a visão do usuário.

4.3 Ambiente de simulação

Tendo como base a estrutura atual de setores da Prefeitura Municipal de Coronel Martins, o ambiente de simulação foi proposto tendo em vista o agrupamento das subdivisões desses setores em VLANs. Criando assim, subredes privadas menores (escolas, unidades de saúde) dentro de uma rede privada maior (centro administrativo).

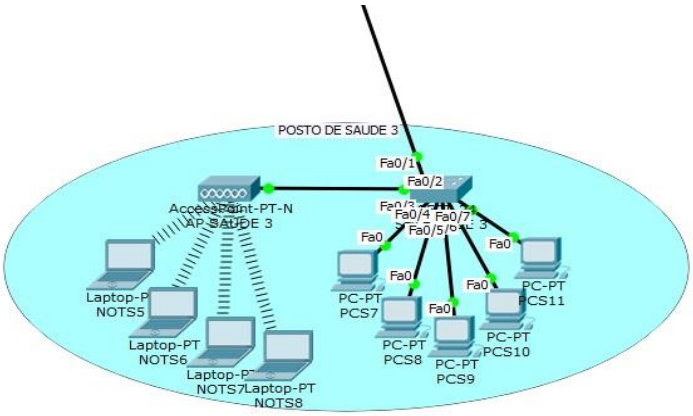

Figura 9 - Unidade de Saúde 3, pertencente a VLAN Saúde
Fonte: Autoria Própria

Abaixo segue uma tabela de endereçamento IPs e suas respectivas VLANs utilizadas no ambiente de simulação proposto.

Departamento/Setor	**VLAN**	**End. IPv4**	**End. IPv6**
Secretaria de Saúde	17	192.168.17.0/24	2001:db8:17::/64
Secretaria de Transportes	13	192.168.13.0/24	2001:db8:13::/64
Secretaria de Educação	12	192.168.12.0/24	2001:db8:12::/64
Secretaria de Agricultura	14	192.168.14.0/24	2001:db8:14::/64
Secretaria de Administração	16	192.168.16.0/24	2001:db8:16::/64
Servidor de Dados	10	192.168.10.0/24	2001:db8:10::/64

Tabela 3 - Endereçamento IP, VLANs e departamentos
Fonte: Autoria própria

4.4 Dados de testes

Para comprovar o real funcionamento da rede utilizando a técnica de transição de pilha dupla, foram implementados alguns testes, os quais algumas telas estarão ilustradas nos apêndices desse trabalho, constando aqui apenas a descrição, para acompanhamento e entendimento de como foram desenvolvidos.

4.4.1 Testes internos entre VLANs

Neste item apresentaremos uma descrição dos testes internos efetuados entre VLANs, demonstrando a segmentação da rede e endereçamento.

Utilizando como exemplo, a sub rede da escola municipal, selecionamos o PCE21 que possui o endereço 192.168.12.13/24 pertencente a VLAN educação, efetuamos o comando ping para o PCE3 com endereço 192.168.12.7/24 localizado na sub rede da secretaria de educação, pertencente a mesma VLAN.

Efetuamos agora o mesmo teste, porem selecionamos um PC não pertencente a VLAN educação, PCS25 com endereço 192.168.17.9/24, pertencente a VLAN saúde. Ambos testes, também foram efetuados nas mesmas condições, porém com endereçamento IPv6.

4.4.2 Testes internos Servidores

Após efetuarmos testes entre VLANs, realizaremos testes no acesso aos servidores localizados na sala de TI.

Para isso utilizaremos como exemplo a sub rede agricultura, pertencente a VLAN agricultura, através do PCA1 com endereço de ipv4 192.168.14.5/24, em seu web browser acessaremos o Servidor Web/Mail que possui endereço 222.222.222.2/30, assim será apresentado uma tela de boas-vindas da Cisco ao Packet Tracer.

Continuando com PCA1, agora testaremos o IPv6, efetuando o comando ping para o Servidor SGBD/APP.

4.4.3 Teste interno para externo IPv4 (NAT)

Primeiramente testaremos o NAT do IPv4. Utilizando como exemplo a sub rede de transporte, através do PCT1 que possui IPv4 192.168.13.2/24, efetuaremos o comando de ping para o servidor web ipv4 com endereço 189.126.222.2/30.

Após ativar o modo Debug NAT no Router DNS, podemos verificar a troca de endereço de IP efetuada pelo router, que internamente trata desse PCT1 pelo endereço 192.168.13.2, porém para acesso externo atribui um endereço IPv4 válido a esse host, no caso o 200.200.200.1, localizado em sua interface s0/0/0.

4.4.4 Teste interno para externo IPv6

Finalizamos com o teste IPv6 da rede interna para rede externa. Para tal, utilizamos a sub rede Prefeitura, pertencente a VLAN adm, com endereço IPv6 2001:db8:16:0:2d0:97ff:cec4, efetuamos um comando de ping para o Server Web IPv6 com endereço 2001:db8:8888::2.

5 CONCLUSÃO

No estudo realizado foi demonstrado uma técnica de transição e convergência entre as versões 4 (IPv4) e 6 (IPv6) do protocolo IP. Visto que o IPv4 já não possui mais endereços disponíveis a novos componentes de rede. Levando em conta o crescimento exponencial de dispositivos e equipamentos que utilizam a Internet, há uma necessidade de maior de disponibilidade de endereços por parte do protocolo utilizado.

Dessa forma, como foi apresentado nesse trabalho o IPv6 não vem somente para disponibilizar uma maior capacidade de endereçamento, traz também diversas funcionalidades e atualizações, como novas versões de protocolos de auxílio e facilidades em sua configuração.

Diante disso, podemos afirmar que a migração é um passo inevitável e indispensável para grandes empresas e órgãos públicos, contudo os mesmos não demonstram preocupação com o fato. Embora ainda utilizem o IPv4, não estão preparados para suportar comunicações em IPv6, tornando assim imprescindível o aprimoramento das técnicas de transição antes de sua plena implantação em IPv6, buscando dessa forma o melhor entendimento das soluções que o novo protocolo fornece.

No modelo proposto de simulação, foi realizada e implementada a técnica de pilha dupla, onde os equipamentos de rede são configurados para operar com as duas versões do protocolo IP. Permitindo assim aos usuários acessarem redes IPv4 e IPv6, conforme sua necessidade, tornando assim a transição menos impactante, mostrando ser um serviço promissor.

Concluindo, a viabilidade para realização da transição entre as versões do protocolo IP utilizando a técnica de pilha dupla, não requer altos custos de investimento na infraestrutura de rede, necessita de um projeto para implementação da transição de forma gradual, não deixando a escassez IPv4 atingir níveis críticos, e assim forçar uma mudança de forma brusca e desorganizada.

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR, Márcio Aurélio dos Santos. **Fundamentos de Redes de Computadores**. Universidade Federal do Amazonas, 2010

AMARAL, Allan Francisco Forzza. **Redes de Computadores**. Instituto Federal do Espírito Santo, 2012

BRITO, Samuel Henrique Bucke. **IPv6 - O Novo Protocolo da Internet**. Novatec Editora. 2013

IPV6, Alocação de endereços. Disponível em: < http://ipv6.br/post/alocacao-de-enderecos>. Acessado em 12/08/2015.

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.

MIRANDA, Anibal D. A. **Introdução as Redes de Computadores**. ESAB - Escola Superior Aberta do Brasil, 2008

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

MORIMOTO, Carlos E. **Hardware: o guia definitivo II**. Editora Meridional LTDA, 2010

PINHEIRO, José Mauricio Santos. **Artigo: Por falar em roteadores.** http://www.projetoderedes.com.br, 2005.

TANENBAUM, Andrew S. **Redes de Computadores: Quarta Edição**. Editora Campos, 2003

TORRES, Gabriel. **Redes de Computadores - Curso Completo**. Axcel Books de Brasil Editora, 2001

WIKIPEDIA, Endereço IP, Máscara de Rede e Sub-rede (IPv4). Disponível em: http://pt-br.wiki.brazilfw.com.br/Ipv4/pt-br. Acessado em 26/07/2015.

APÊNDICES – TELAS DE TESTES EFETUADOS EM AMBIENTE DE SIMULAÇÃO

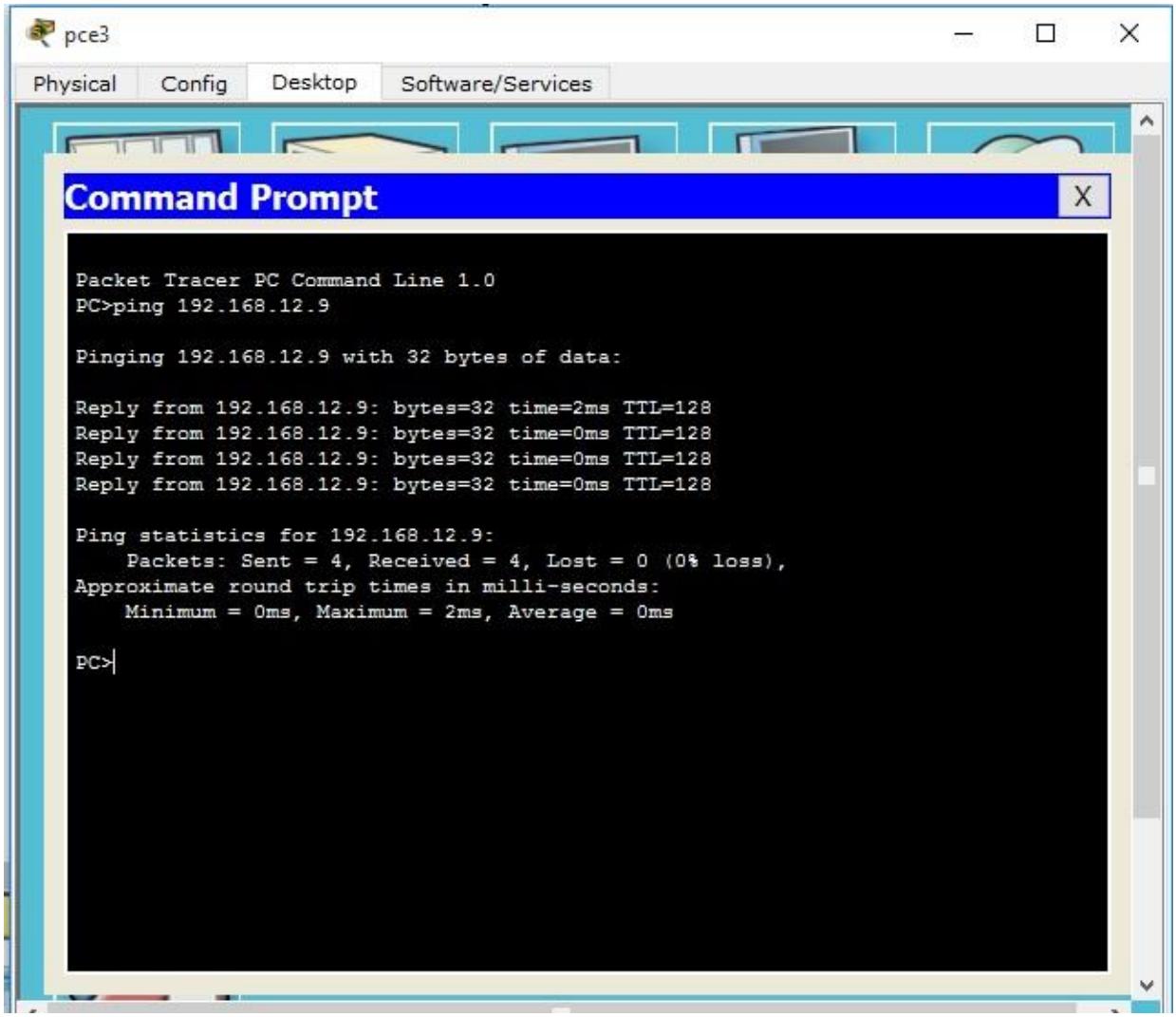

Figura 10 - Teste de conectividade interno entre PCs de mesma VLAN
Fonte: Autoria Própria

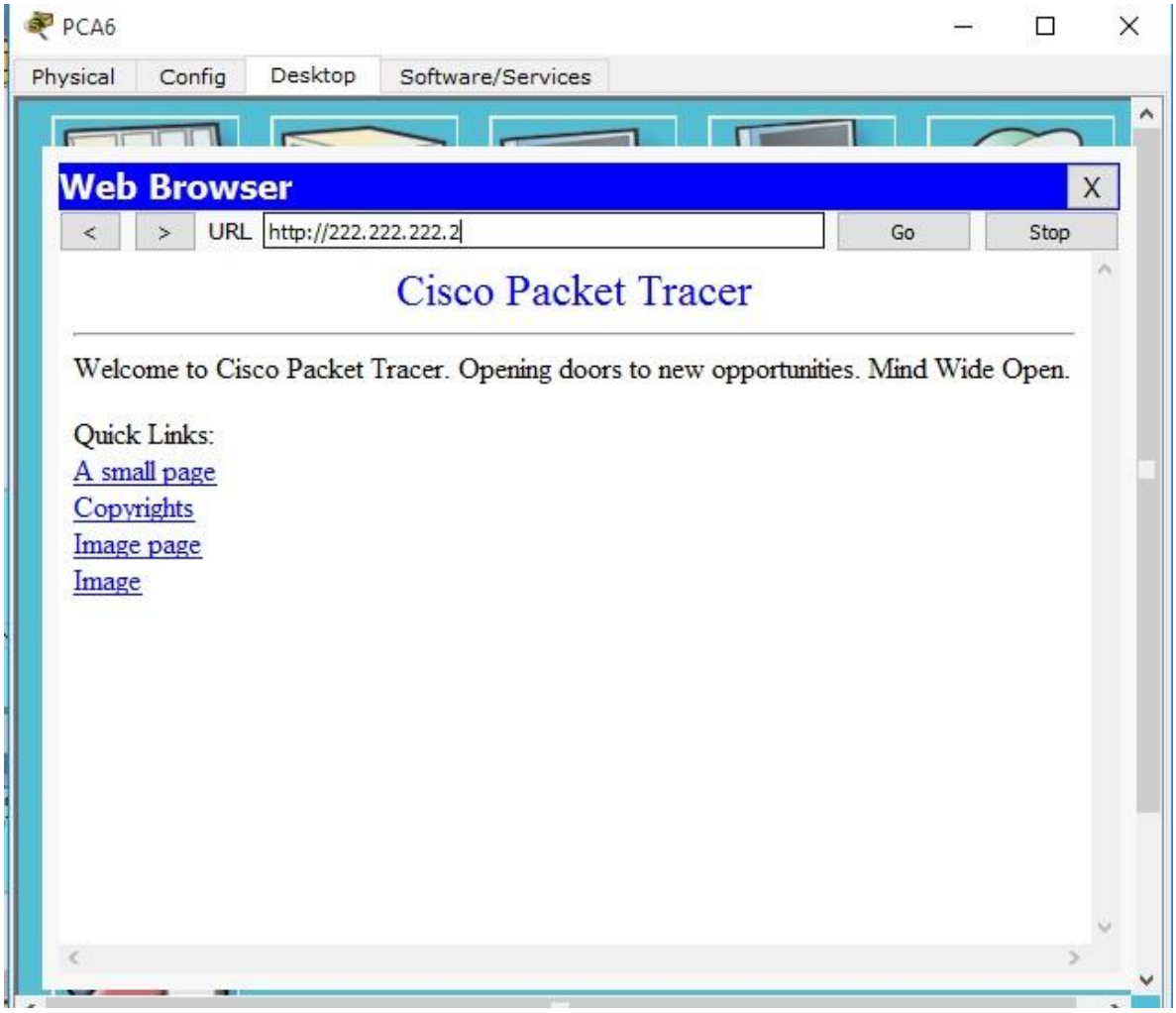

Figura 11 - Teste de acesso ao server web interno IPv4
Fonte: Autoria Própria

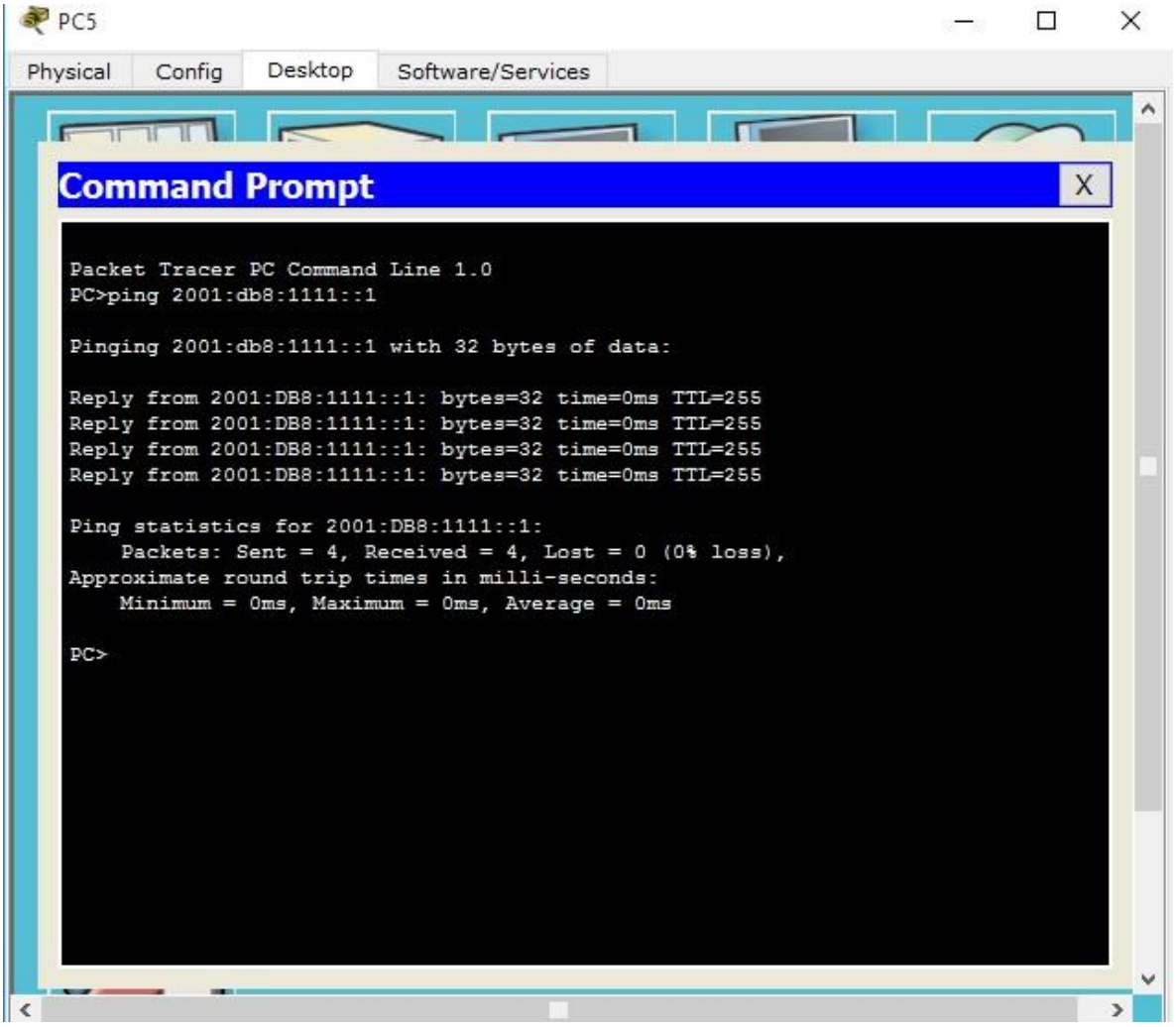

Figura 12 - Teste de acesso ao server web interno IPv6
Fonte: Autoria Própria

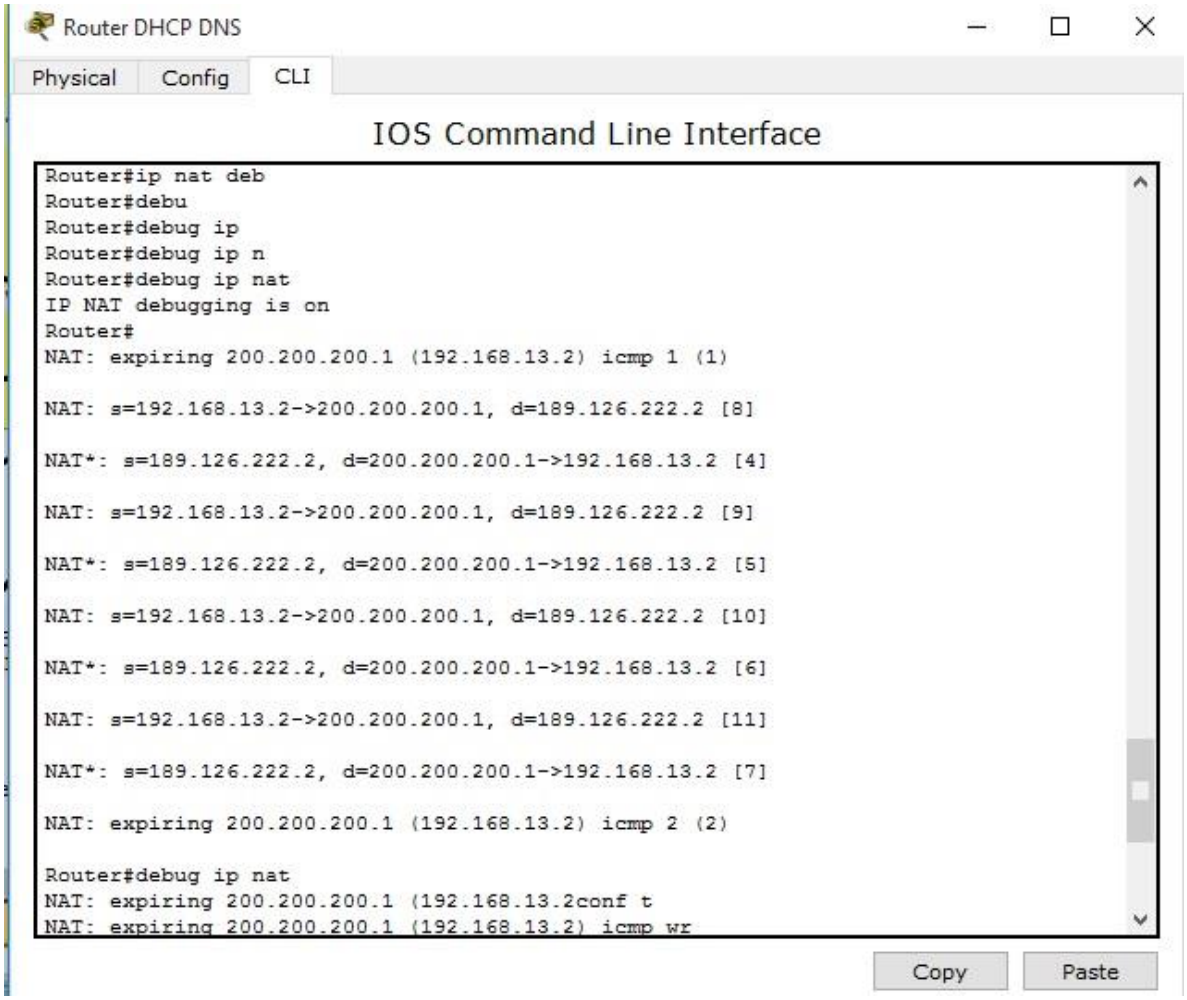

Figura 13 - Acesso server web externo IPv4, atraves do funcionamento do NAT
Fonte: Autoria Própria

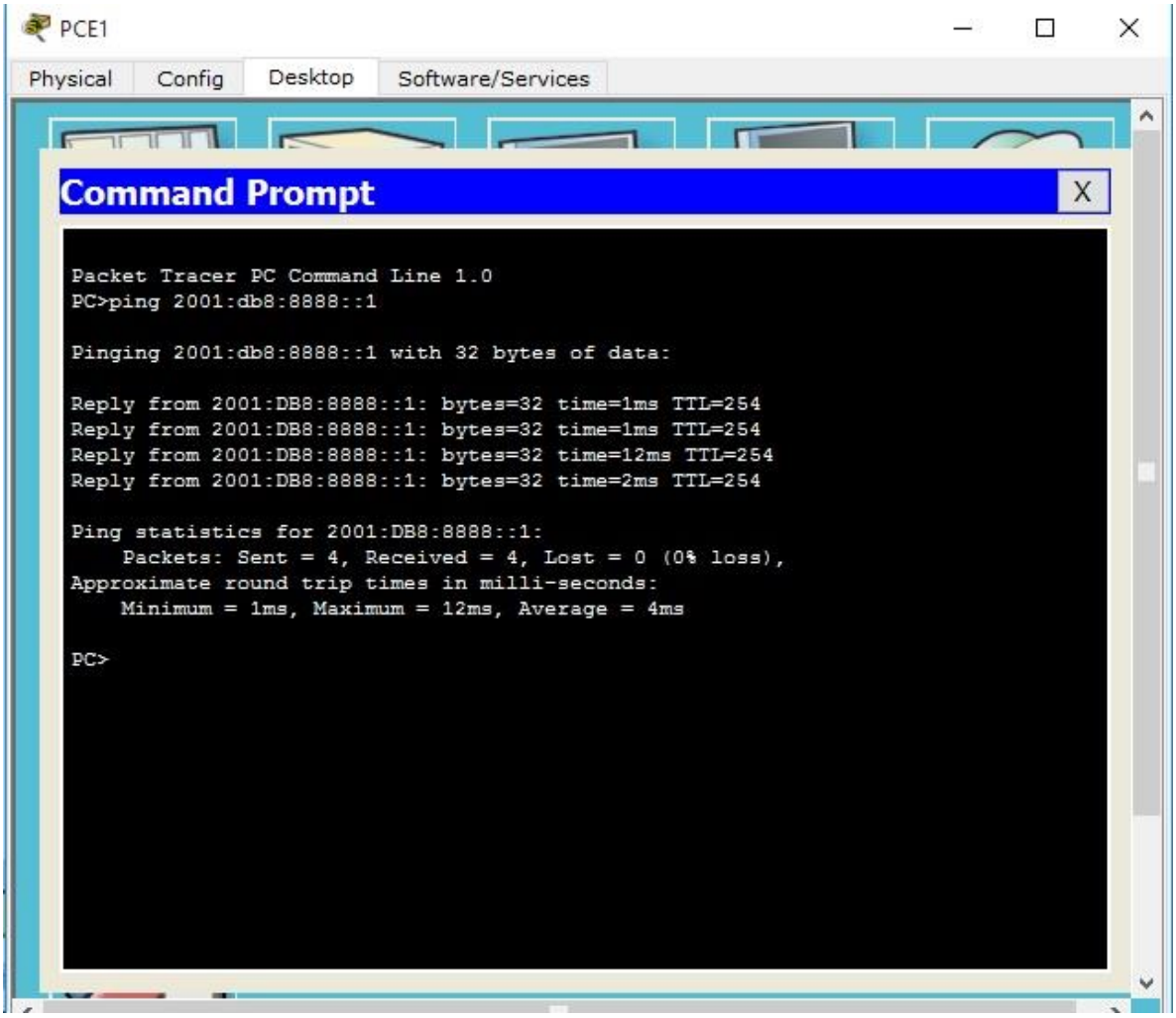

Figura 14 - Teste de acesso ao server web IPv6 externo
Fonte: Autoria Própria