

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

EDNO GUSTAVO PAMPLONA
RICARDO KIYOSHI TOKUNAGA

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

TRANSIÇÃO IPV4/IPV6: Técnica de Tunelamento

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2014

EDNO GUSTAVO PAMPLONA
RICARDO KIYOSHI TOKUNAGA

TRANSIÇÃO IPV4/IPV6: Técnica de Tunelamento

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Diplomação, do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Departamento Acadêmico de Eletrônica – DAELN – da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2014

TERMO DE APROVAÇÃO

EDNO GUSTAVO PAMPLONA
RICARDO KIYOSHI TOKUNAGA

TRANSIÇÃO IPV4/IPV6: Técnica de Tunelamento

Este trabalho de conclusão de curso foi apresentado no dia 11 de setembro 2014, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. PhD. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

Prof. MsC. Lincoln Herbert Teixeira
UTFPR

Prof. Dr. Kleber Kendy Horikawa Nabas
UTFPR

Prof. Dr. Augusto Foronda
Orientador - UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

RESUMO

PAMPLONA, Edno Gustavo; TOKUNAGA, Ricardo Kiyoshi. **Transição IPv4/IPv6: Técnica de Tunelamento**. 2014. 41 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior de Tecnologia em Sistemas de Telecomunicações, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Diante do esgotamento de endereços do protocolo IPv4, este trabalho tem como propósito abordar a implantação do protocolo IPv6 através da técnica de transição de tunelamento. Esta técnica tem o objetivo de conectar redes IPv6 através de redes IPv4, já que eles não são diretamente compatíveis entre si. Esta pesquisa apresenta conceitos teóricos juntamente com uma aplicação prática simulada da técnica de tunelamento manual com roteadores Cisco pelo programa Packet Tracer 6.0.1 e para seu roteamento são utilizados os protocolos OSPF e EIGRP.

Palavras-chave: IPv4. IPv6. Tunelamento.

ABSTRACT

PAMPLONA, Edno Gustavo; TOKUNAGA, Ricardo Kiyoshi. **Transition IPv4/IPv6: Tunneling Technique**. 2014. 41 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior de Tecnologia em Sistemas de Telecomunicações, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Faced with the exhaustion of IPv4 addresses, this work aims to address the deployment of IPv6 by tunneling transition technique. This technique aims to connect IPv6 networks across IPv4 networks, since they are not directly compatible. This research presents theoretical concepts along with a simulated practical application of the technique of manual tunneling with Cisco routers by Packet Tracer 6.0.1 program and its OSPF and EIGRP routing protocols are used.

Keywords: IPv4. IPv6. Tunneling.

LISTA DE FIGURAS

Figura 1 – Cabeçalho IPv4 e IPv6.....	17
Figura 2 – Túnel manual 6over4 entre dois dispositivos	23
Figura 3 – Tipos de pacote OSPF	24
Figura 4 – Tipos de pacote EIGRP.....	26
Figura 5 – Topologia utilizada na simulação túnel manual com OSPF	28
Figura 6 – <i>Ping</i> realizado do PC1 para o PC2.....	33
Figura 7 – Topologia utilizada na simulação túnel manual com EIGRP	34
Figura 8 – <i>Ping</i> realizado do PC1 para o PC0.....	39

LISTA DE TABELAS

Tabela 1 - Renomeação e Reposicionamento dos campos no IPv4 e IPv6.....	18
Tabela 2 - Tabela IP dos dispositivos e suas interfaces no modelo OSPF	29
Tabela 3 - Tabela IP dos dispositivos e suas interfaces no modelo EIGRP.....	34

SUMÁRIO

1 INTRODUÇÃO	8
1.1 PROBLEMA	9
1.2 OBJETIVOS	10
1.2.1 Objetivo Geral	10
1.2.2 Objetivos Específicos	10
1.3 JUSTIFICATIVA	11
1.4 PROCEDIMENTOS METODOLÓGICOS	12
2 REFERENCIAL TEÓRICO	13
2.1 IP	13
2.2 IPv6	13
2.2.1 Motivação	14
2.2.2 Desenvolvimento da Internet	15
2.2.3 Cabeçalho	16
2.3 ENDEREÇAMENTO	19
2.4 TUNELAMENTO	22
2.5 OSPF	23
2.6 EIGRP	25
3 SIMULAÇÃO	28
3.1 MODELO COM OSPF	28
3.2 MODELO COM EIGRP	33
4 CONCLUSÃO	40
REFERÊNCIAS	41

1 INTRODUÇÃO

A grande evolução da Internet trouxe grande ganho para as empresas e muita facilidade para a vida das pessoas. Em contrapartida a isso, veio o esgotamento de endereços IP (*Internet Protocol*) com o grande número de computadores conectados a rede da Internet.

Sendo a rede mais conhecida, a Internet é o modelo ideal para o estudo das redes de computadores. A Internet, na verdade, é um conjunto de redes diferentes que utilizam diversos meios e tecnologias, conectadas entre si através de protocolos em comum (TANENBAUM, 2003, p. 53).

O IP é um protocolo que foi projetado para criar ligações entre diferentes redes, possibilitando a intercomunicação entre dispositivos nelas presentes. Cada computador na Internet possui um número único, que o identifica dentre da mesma, chamado endereço IP.

O protocolo *Internet*, na verdade, faz parte de um conjunto maior de protocolos, conhecidos por TCP/IP suíte, que inclui outros protocolos como *Transmission Control Protocol* – Protocolo de Controle de Transmissão (TCP), *User Datagram Protocol* – Protocolo de Datagrama do Usuário (UDP), *Domain Name System* – Sistemas de Nomes de Domínios (DNS), *Address Resolution Protocol* – Protocolo de Resolução de Endereços (ARP), *Reverse Address Resolution Protocol* – Protocolo de Resolução Reversa de Endereços (RARP), *Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de Host (DHCP), *File Transfer Protocol* – Protocolo de Transferência de Arquivos (FTP), *Hypertext Transfer Protocol* – Protocolo de Transferência de Hipertexto (HTTP), *Border Gateway Protocol* – Protocolo de Roteamento de Borda (BGP), entre outros. Esse conjunto é hoje utilizado também nas redes locais. É, na verdade, o padrão de fato utilizado como protocolo de comunicação para diversas aplicações, a começar pela Internet (DOMINGOS, 2013).

Algumas das principais características desse protocolo são (Soares, 1995):

- Serviço sem conexão/não confiável;
- Endereçamento hierárquico;
- Fragmentação e remontagem de datagramas;

- Identificação da importância e confiabilidade exigida do datagrama;
- Roteamento adaptativo;
- Checagem da integridade dos dados do cabeçalho (*checksum*);
- Controle do tempo de vida (*time to live*) dos pacotes.

Atualmente os computadores se comunicam na Internet através do protocolo IPv4 (*Internet Protocol Version 4*). Este protocolo foi desenvolvido a mais de 20 anos e está ficando ultrapassado. O problema mais relevante dessa versão refere-se à crescente falta de endereços IPv4, que são usados por todas as máquinas novas conectadas à Internet.

O IPv6 (*Internet Protocol Version 6*) veio para resolver vários problemas do IPv4, entre eles, o número limitado de endereços disponíveis. Apresenta também melhorias com relação ao IPv4 em áreas tais como a auto configuração de roteamento e de rede.

1.1 PROBLEMA

A Internet não foi projetada inicialmente para uso comercial. Desde os anos 70 utiliza-se o protocolo IP para a comunicação em rede e a partir do início dos anos 80 a IPv4, versão atual do protocolo, passou a ser um dos protocolos mais utilizados no mundo.

O IPv4 é bastante estável e robusto e é baseado em 32 bits, logo são possíveis 2^{32} endereços IP únicos na Internet, ou seja, 4.294.967.296 endereços IPv4. Porém, a estrutura de endereços do IPv4 não é linear, sendo agregados em blocos de classes e domínios de redes (BARROS JÚNIOR. 2013).

Embora o intuito dessa agregação tenha sido tornar a distribuição de endereços mais flexível, abrangendo redes de tamanhos variados, esse tipo de classificação mostrou-se ineficiente, pois o bloco denominado classe A atenderia a um número muito pequeno de redes que alocaria a metade de todos os endereços disponíveis.

No entanto, esse esgotamento não se concretizou devido ao desenvolvimento de uma série de tecnologias que funcionaram como uma solução paliativa para o problema, adiando assim o esgotamento do IPv4.

O IPv4 e o IPv6 não são diretamente compatíveis entre si. O IPv6 não foi projetado para ser uma extensão, ou complemento, do IPv4, mas sim, um substituto que resolve o problema do esgotamento de endereços. Embora não interoperem, ambos os protocolos podem funcionar simultaneamente nos mesmos equipamentos e com base nisto a transição foi pensada para ser feita de forma gradual.

Nesse contexto, vamos apresentar uma das técnicas de transição do IPv4 para o IPv6, a técnica de tunelamento. Esta técnica tem o objetivo de conectar redes IPv6 através de redes IPv4 e quando uma empresa quer migrar para IPv6, deve ser usada esta técnica. Ou seja, qualquer empresa que precisa migrar para IPv6 deve usar esta técnica e este trabalho vai mostrar como fazer isto.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Nossa pesquisa baseia-se em descrever os conceitos e características dos protocolos IPv4 e IPv6 e demonstrar a importância e a necessidade destes protocolos trabalharem simultaneamente nas redes de computador, usando uma das técnicas de transição criadas para esta interoperação: Técnica de tunelamento. Será apresentada uma topologia e como deve ser feito este tunelamento.

1.2.2 OBJETIVOS ESPECÍFICOS

- Descrever os conceitos do método de tunelamento;
- Apresentar os fatos históricos que demonstram a necessidade da transição do IPv4 para o IPv6;
- Descrever as características e a importância da transição, usando o método escolhido;

- Descrever as configurações de *Tunneling*;
- Demonstrar a importância e a necessidade da interoperação dos protocolos IPv4 e IPv6;
- Simular um ambiente de transição do IPv4 para o IPv6, usando a técnica de tunelamento.

1.3 JUSTIFICATIVA

A palavra chave na transição entre as duas versões do protocolo IP é interoperação. As duas versões devem poder permanecer na rede simultaneamente, se comunicando e endereçando. A segunda palavra chave é facilidade. Deve ser fácil fazer um *upgrade* nos *softwares* da versão 4 para a 6, tanto para administradores de rede, técnicos, como para o usuário final

As justificativas da interoperação na transição são:

- Roteadores e máquinas devem ter seus programas de rede trocados sem que todos os outros no mundo tenham que trocar ao mesmo tempo;
- Pré-requisitos mínimos. O único pré-requisito é que os servidores de DNS devem ter a sua versão trocada antes. Para os roteadores não existem pré-requisitos;
- Quando as máquinas sofrerem o *upgrade* devem poder manter seus endereços IPv4, sem a necessidade de muitos planos de um reendereçamento, usando inicialmente um dos prefixos vistos anteriormente;
- Custos baixos;
- Os nós IPv6 devem poder se comunicar com outros nós IPv6, mesmo que a infraestrutura entre eles seja IPv4.

Para esta ultima justificativa, dois mecanismos foram criados: Transição de pilha dupla (*Dual-stack*) e transição de tunelamento (*Tunneling*). Escolhemos a técnica de tunelamento para apresentarmos neste trabalho.

1.4 PROCEDIMENTOS METODOLÓGICOS

A pesquisa do nosso trabalho será orientada por manuais, normas, tutoriais e as bibliografias de referência que tratam o escopo do projeto, incluindo o compartilhamento de informações com especialistas da área.

A primeira etapa do trabalho será baseada em conceituar o termos de Internet, protocolos IPv4 e IPv6, IP, entre outros, que serão necessários para o melhor entendimento do projeto.

Na segunda etapa será descrita a importância das redes de computadores nos dias de hoje, o porquê do esgotamento de endereços IPv4 e a necessidade da transição dos protocolos. Nesta fase também apresentaremos fatos históricos da Internet e uma visão técnica do método de tunelamento.

Na terceira etapa, demonstraremos todos os cenários possíveis da transição de protocolos, como: rede IPv6 para Internet IPv4, rede IPv4 para Internet IPv6, Internet IPv6 para rede IPv4, Internet IPv4 para rede IPv6, rede IPv4 para rede IPv6, rede IPv6 para rede IPv4, Internet IPv4 para Internet IPv6, Internet IPv6 para Internet IPv4, rede IPv6 para rede IPv6 bidirecional via Internet IPv4 e rede IPv4 para rede IPv4 bidirecional via Internet IPv6.

Posteriormente, serão apresentados a configuração, conceito e arquitetura da técnica de tunelamento.

Na última parte do trabalho, demonstraremos na prática o funcionamento do *Tunneling*, em todas as suas etapas.

2 REFERENCIAL TEÓRICO

2.1 IP

O protocolo IP teve origem no ano de 1970 no desenvolvimento da *ARPANET* (*Advanced Research Projects Agency Network*), a primeira rede operacional de computadores à base de comutação de pacotes. Esta rede foi depois interligada a outras formando em 1980 um vasto conjunto que passou a ser conhecido por Internet. Com a inclusão do protocolo IP no UNIX, no ano de 1982, um grande número de universidades passou a formar as suas redes que por sua vez também foram ligadas à Internet (ZAKON, 2013).

Na Internet, e nas redes particulares que vemos hoje nas empresas ou mesmo nas residências, o protocolo de comunicação usado pelos computadores chama-se IP. O protocolo IP fornece um serviço de datagramas que é depois usado por outros protocolos de nível superior, tais como o TCP e o UDP.

O TCP é um protocolo *full-duplex*, orientado à conexão e altamente confiável. A arquitetura TCP é bastante complexa, o que acarreta em um grande custo em termos de cabeçalhos (*overhead*). Já o protocolo UDP não oferece todo o requinte do TCP, mas realiza eficientemente o trabalho de transporte de dados que não requeiram confiabilidade na entrega (FILIPPETTI, 2007).

2.2 IPV6

O IP versão 6 começou a ser desenvolvido no início da década de 1990, com o objetivo de ser a solução definitiva para o esgotamento de endereços IPs na Internet. Tendo esse, como o principal objetivo.

As principais modificações foram o aumento de endereços, a simplificação do cabeçalho, melhor suporte para as opções oferecidas e o avanço na questão de segurança. O IPv6 atende a todos os objetivos propostos, preservando os bons recursos do IP, descartando ou reduzindo a importância das características ruins e criando outras quando necessário (TANENBAUM, 2003).

Algumas novidades do IPv6 (DEERING, 1996) :

- Endereço de 128 bits;
- Suporte a aplicações multimídia em tempo real;
- Suporte a *multicast* e *anycast*;
- Arquitetura de endereçamentos melhor estruturada;
- Mecanismos de segurança, incluindo encriptação e autenticação;
- Mobilidade;
- Suporte para datagramas “Jumbo”.

2.2.1 MOTIVAÇÃO

O crescimento da demanda por endereços IP foi o motivo básico que levou à definição de uma nova geração de IP. Uma lição que pode ser tirada da experiência com IPv4 é a de que o endereçamento e o roteamento devem suportar o crescimento futuro. É importante que tenhamos compreensão do crescimento passado e como será o crescimento futuro.

O IPv6 é a versão mais recente do protocolo IP. Ela tem de ser implantada rapidamente na Internet, porque a versão anterior, o IPv4, não é mais capaz de suportar o crescimento da rede: não há mais endereços livres.

Apesar de, num futuro próximo, ser possível ter redes totalmente IPv6, o mais comum será ter IPv4 e IPv6 na mesma infraestrutura. E, para permitir isto, são necessários ferramentas e mecanismos de coexistência e integração (HAGEN, 2002).

2.2.2 DESENVOLVIMENTO DA INTERNET

O Departamento de Defesa (DoD - *Department of Defense*) do governo estadunidense iniciou em 1966, através de sua Agência de Pesquisas e de Projetos Avançados (ARPA - *Advanced Research Projects Agency*), um projeto para a interligação de computadores em centros militares e de pesquisa. Este sistema de comunicação e controle distribuído com fins militares recebeu o nome de ARPANET,

tendo como principal objetivo criar uma arquitetura de rede sólida e robusta, baseada na comutação de pacotes, e que pudesse lidar com a indisponibilidade de alguns de seus nós, funcionando com os computadores e ligações de comunicação restantes.

No início, a ARPANET trabalhava com diversos protocolos de comunicação, sendo o principal o NCP (*Network Control Protocol*). No entanto, em 1o. de Janeiro de 1983, quando a rede já possuía 562 hosts, todas as máquinas da ARPANET passaram a adotar como padrão o conjunto de protocolos conhecido por TCP/IP, permitindo o crescimento ordenado da rede e eliminando restrições dos protocolos anteriores. Nesse mesmo ano, a ARPANET foi dividida em duas, uma rede fechada para os militares chamada MILNET, e uma rede aberta, com então 45 hosts, que evoluiu para a rede que hoje conhecemos como a Internet.

O IP versão 4, definido na RFC 791, e, como visto, uma das principais bases tecnológicas, sobre as quais se sustentam a Internet. Esse protocolo mostrou-se bastante robusto, de fácil implantação e interoperabilidade. No entanto, seu projeto remonta a década de 1970 e não previu alguns aspectos hoje importantes como:

- O crescimento das redes e um possível esgotamento dos endereços IP;
- O aumento da tabela de roteamento, que é a tabela onde estão relacionadas todas as interconexões entre as redes que compõem a Internet, permitindo identificar os possíveis caminhos para os pacotes, até seus destinos;
- Problemas relacionados a segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes.

Em 1990, existiam cerca de 313.000 hosts conectados a rede e estudos já apontavam para um colapso devido à falta de endereços. Outros problemas também tornavam-se aparentes, conforme a Internet evoluía, como o aumento da tabela de roteamento.

No encontro *Internet Engineering Task Force* (IETF) de Vancouver, em 1990, Frank Solensky, Phill Gross e Sue Hares afirmaram que à taxa de atribuição do espaço de endereçamento IPv4, existente à época, as classes do tipo B estariam esgotadas, possivelmente por volta de março de 1994 (BRANDER & MANKIN, 1995).

Em 1993, com a criação da *Web* e com a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior em sua taxa de crescimento.

As especificações da IPv6 foram apresentadas inicialmente na RFC 1883 de dezembro de 1995, no entanto, em dezembro de 1998, esta RFC foi substituída pela RFC 2460.

A primeira conexão com o protocolo IPv6 foi estabelecida em março de 1998 com a *Cisco System*, nos EUA (BRANDER & MANKIN, 1995).

2.2.3 CABEÇALHO

O cabeçalho IPv4 é composto por 12 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho varie de 20 a 60 *Bytes*. Estes campos são destinados transmitir informações sobre:

- a versão do protocolo;
- o tamanho do cabeçalho e dos dados;
- a fragmentação dos pacotes;
- o tipo dos dados sendo enviados;
- o tempo de vida do pacote;
- o protocolo da camada seguinte (TCP, UDP, ICMP);
- a integridade dos dados;
- a origem e destino do pacote.

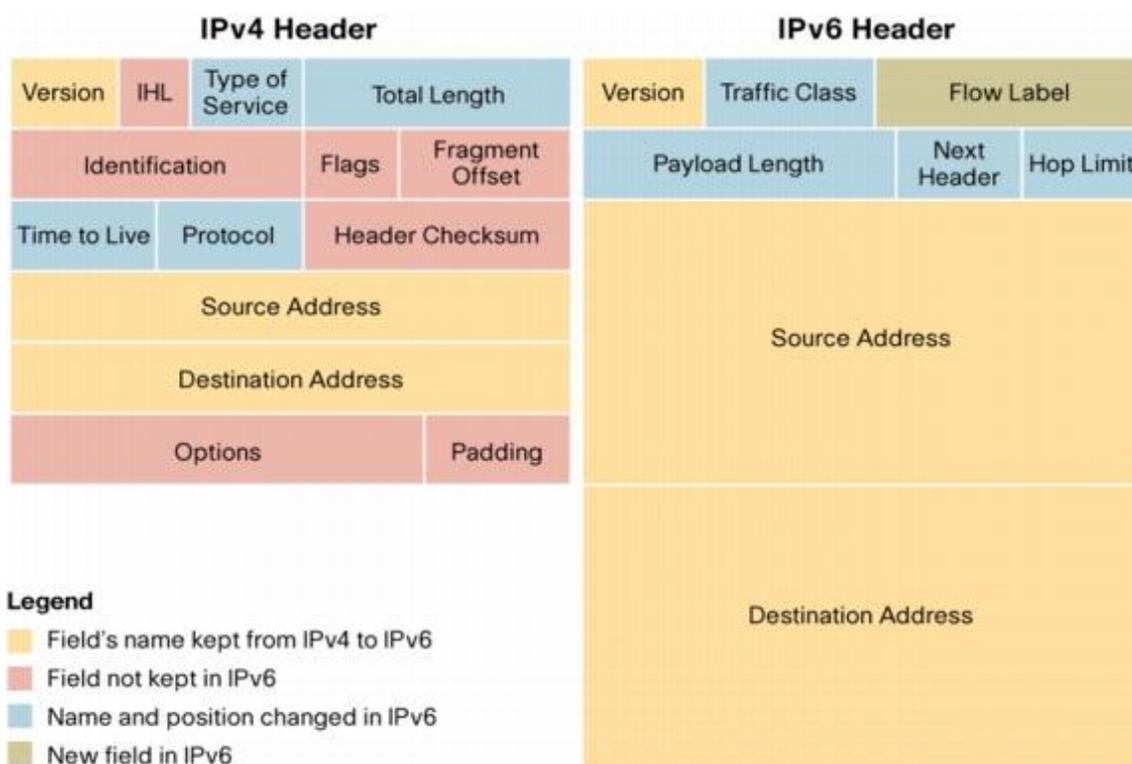


Figura 1 – Cabeçalho IPv4 e IPv6

Fonte: CISCO, 2006

Já no IPv6 foram realizadas algumas mudanças no formato do cabeçalho de modo a torna-lo mais simples. O número de campos foi reduzido para apenas oito e o tamanho foi fixado de 40 Bytes. Além disso, ele ficou mais flexível e eficiente com a adição de cabeçalhos de extensão que não precisam ser processados por roteadores intermediários. Tais alterações permitiram que, mesmo com um espaço de endereçamento quatro vezes maior que o do IPv4, o tamanho total do cabeçalho IPv6 fosse apenas duas vezes.

Dentre essas mudanças, na qual podemos observar na figura 1, destaca-se a remoção de seis dos campos existentes no cabeçalho IPv4, como resultado tanto da inutilização de suas funções quanto de sua reimplementação com o uso de cabeçalhos de extensão.

A primeira remoção foi a do campo “Tamanho do Cabeçalho” que tornou-se desnecessário uma vez que seu valor foi fixado. A seguir, os campos “Identificação”, “Flags”, “Deslocamento do Fragmento” e “Opções e Complementos” passaram a ter suas informações indicadas em cabeçalhos de extensão apropriados. Por fim, o campo “Soma de Verificação” foi descartado com o objetivo de deixar o protocolo

mais eficiente já que outras validações são realizadas pelos protocolos das camadas superiores da rede.

Outra alteração realizada com o intuito de agilizar o processamento foi a renomeação e reposicionamento de quatro campos conforme a tabela 1:

Tabela 1 - Renomeação e Reposicionamento dos campos no IPv4 e IPv6

IPv4	IPv6
Tipo de Serviço	Classe de Serviço
Tamanho Total	Tamanho dos Dados
Tempo de Vida (TTL)	Limite de Encaminhamento
Protocolo Próximo	Cabeçalho

Fonte: Autoria própria

Além disso, o campo “Identificador de Fluxo” foi adicionado para possibilitar o funcionamento de um mecanismo extra de suporte a QoS (*Quality of Service*).

Por fim, os campos “Versão”, “Endereço de Origem” e “Endereço de Destino” foram mantidos e apenas tiveram seus tamanhos alterados.

Conforme a observado na figura 1, o cabeçalho do IPv6 esta dividido nos seguintes campos:

- Versão (4 bits) - Identifica a versão do protocolo utilizado. No caso, o valor desse campo e 6;
- Classe de Tráfego (8 bits) – Identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço do IPv4”;
- Identificador de Fluxo (20 bits) – Identifica pacotes do mesmo fluxo de comunicação. Idealmente esse campo e configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nos intermediários de rede podem utiliza-lo de forma agregada com os endereços de origem e destino para realização de tratamento especifico dos pacotes;
- Tamanho do Dados (16 bits) – Indica o tamanho, em *Bytes*, apenas dos dados enviados junto ao cabeçalho IPv6. Substituiu o campo Tamanho Total do IPv4, que indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Contudo, o tamanho dos cabeçalhos de extensão também são somado nesse novo campo;

- Próximo Cabeçalho (8 *bits*) – Identifica o cabeçalho de extensão que segue o atual. Ele foi renomeado (no IPv4 chamava-se Protocolo) para refletir a nova organização dos pacotes IPv6, uma vez que ele deixou de conter os valores referentes a outros protocolos, para indicar os tipos dos cabeçalhos de extensão;
- Limite de Encaminhamento (8 *bits*) – Esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado. Ele padronizou o modo como o campo Tempo de Vida (TTL) do IPv4 vinha sendo utilizado, o qual diferia significativamente da descrição original que o definia como o tempo, em segundos, para o pacote ser descartado caso não chegasse a seu destino;
- Endereço de origem (128 *bits*) – Indica o endereço de origem do pacote;
- Endereço de Destino (128 *bits*) – Indica o endereço de destino do pacote.

O cabeçalho simplificado de IPv6 oferece várias vantagens com relação ao IPv4:

- Melhor eficiência de roteamento para desempenho e escalabilidade;
- Ausência de *broadcasts* e, desse modo, ausência de ameaças de *broadcast storms*;
- Sem necessidade de processar *checksums*;
- Mecanismos de cabeçalho de extensão simplificados e mais eficientes;
- Rótulos de fluxo para processamento sem a necessidade de abrir o pacote.

2.3 ENDEREÇAMENTO

O protocolo IPv6 apresenta como principal característica e justificativa maior para o seu desenvolvimento, o aumento no espaço para endereçamento. Por isso, é importante conhecermos as diferenças entre os endereços IPv4 e IPv6, saber reconhecer a sintaxe dos endereços IPv6 e conhecer os tipos de endereços IPv6 existentes e suas principais características.

No IPv4, o campo do cabeçalho reservado para o endereçamento possui 32 bits. Este tamanho possibilita um máximo de 4.294.967.296 (2³²) endereços

distintos. A época de seu desenvolvimento, esta quantidade era considerada suficiente para identificar todos os computadores na rede e suportar o surgimento de novas sub-redes. No entanto, com o rápido crescimento da Internet, surgiu o problema da escassez dos endereços IPv4, motivando a criação de uma nova geração do protocolo IP.

As especificações do IPv4 reservam 32 bits para endereçamento, possibilitando gerar mais de 4 bilhões de endereços distintos. Inicialmente, estes endereços foram divididos em três classes principais de tamanhos fixos, da seguinte forma:

- Classe A: definia o bit mais significativo como 0, utilizava os 7 bits restantes do primeiro octeto para identificar a rede, e os 24 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 1.0.0.0 até 126.0.0.0;
- Classe B: definia os 2 bits mais significativo como 10, utilizava os 14 bits seguintes para identificar a rede, e os 16 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 128.1.0.0 até 191.254.0.0;
- Classe C: definia os 3 bits mais significativo como 110, utilizava os 21 bits seguintes para identificar a rede, e os 8 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0;

O intuito dessa divisão tinha era tornar a distribuição de endereços flexível, abrangendo redes de tamanhos variados, mas essa classificação mostrou-se na verdade rígida e muito ineficiente, levando a um grande desperdício de endereços.

O IPv6 possui um espaço para endereçamento de 128 bits, sendo possível obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços (2¹²⁸). Este valor representa aproximadamente 79 octilhões (7,9×10²⁸) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões (5,6×10²⁸) de endereços por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

Os 32 bits dos endereços IPv4 são divididos em quatro grupos de 8 bits cada, separados por ".", escritos com dígitos decimais. Por exemplo: 192.168.0.10.

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por ":", escritos com dígitos hexadecimais (0-F). Por exemplo:

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos.

Além disso, regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequencia longa de zeros por "::".

Por exemplo, o endereço

2001:0DB8:0000:0000:130F:0000:0000:140B

pode ser escrito como

2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B.

Neste exemplo é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrario poderá haver ambiguidades na representação do endereço. Se o endereço acima fosse escrito como:

2001:DB8::130F::140B,

não seria possível determinar se ele corresponde a

2001:DB8:0:0:130F:0:0:140B,

a

2001:DB8:0:0:0:130F:0:140B

ou

2001:DB8:0:130F:0:0:0:140B.

Esta abreviação pode ser feita também no fim ou no inicio do endereço, como ocorre em

2001:DB8:0:54:0:0:0:0

que pode ser escrito da forma

2001:DB8:0:54::.

Existem três tipos de endereços IPv6:

- Unicast - Endereço que identifica uma única interface. Existem dois tipos de endereço *Unicast*: *Global IPv6 Address* e *Link-Local Address*.
- Anycast - Identifica um bloco de interfaces, de tal forma que um pacote enviado a um endereço de *anycast* será entregue a um elemento do bloco.
- Multicast - Identifica um grupo de interfaces, tal que um pacote enviado a um endereço de *multicast* é entregue a todos elementos do grupo. Não existe endereço de *broadcast* no IPv6, esta função foi substituída pelo endereço de *multicast*.

2.4 TUNELAMENTO

O tunelamento é um método de integração onde um pacote de IPv6 é encapsulado dentro de outro protocolo, como o IPv4. Esse método permite a conexão das ilhas de IPv6 sem que haja a necessidade de converter as redes intermediárias para o IPv6. Quando o IPv4 for usado para encapsular o pacote de IPv6, o pacote incluirá um cabeçalho de IPv4 de 20 bytes sem opções, um cabeçalho de IPv6 e a *payload*.

A técnica de criação de túneis, ou tunelamento, permite transmitir pacotes IPv6 através da infra-estrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4.

Existem várias técnicas de tunelamento disponíveis, incluindo:

- Tunelamento manual de IPv6 sobre IPv4 – Um túnel manual é estabelecido entre dois nós IPv4 para enviar o tráfego IPv6, os pacotes de IPv6 são encapsulados dentro do protocolo IPv4. Na figura 2 apresenta um exemplo de topologia em que é utilizado o túnel manual 6over4.
- Tunelamento dinâmico *6to4*, de acordo com CARPENTER e MOORE (2001) na RFC 3056, estabelece a conexão das ilhas de IPv6 automaticamente através de uma rede IPv4, normalmente a Internet. Ele aplica automaticamente um prefixo de IPv6 válido e exclusivo a cada ilha de IPv6, permitindo a rápida implantação do IPv6 em uma rede corporativa sem que ocorra a recuperação de endereço dos ISPs ou dos registros.
- Protocolo de endereçamento automático de túnel intra-site (ISATAP, *Intra-Site Automatic Tunnel Addressing Protocol*) – Mecanismo de tunelamento de sobreposição automática que usa a rede de IPv4 subjacente como uma camada de enlace para o IPv6, é tratado por TEMPLIN, GLEESON e THALER (2008) na RFC 5214. Os túneis do ISATAP permitem que os *hosts* de pilha dupla individuais de IPv4 ou IPv6 dentro de um local se comuniquem com outros *hosts* em um link virtual, criando uma rede de IPv6 que utiliza a infraestrutura de IPv4.

- Tunelamento Teredo - Uma tecnologia de transição de IPv6 que fornece o tunelamento automático de *host* para *host* em vez de um tunelamento de *gateway*, é descrito na RFC 4380(2006). Essa abordagem transmite o tráfego *unicast* de IPv6 quando os *hosts* de pilha dupla (*hosts* que executam tanto o IPv6 quanto o IPv4) estão localizados atrás de um ou de vários NATs de IPv4.

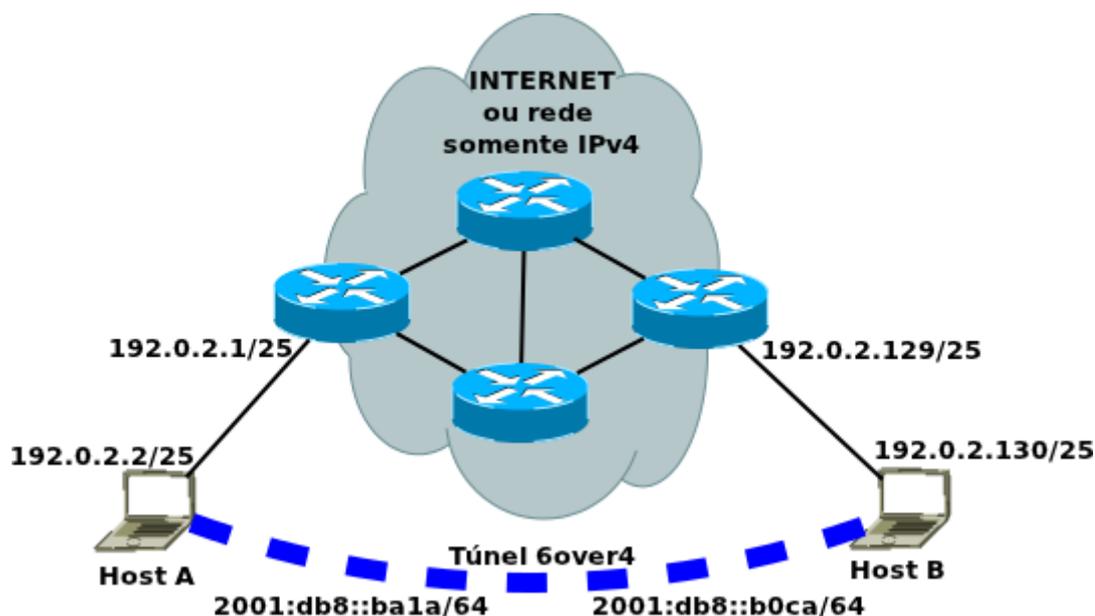


Figura 2 – Túnel manual 6over4 entre dois dispositivos

Fonte: IPv6.br, 2012

Neste trabalho será utilizada a técnica de tunelamento manual e para seu roteamento serão utilizados os protocolos OSPF (*Open Shortest Path First*) e EIGRP (*Enhanced Interior Gateway Routing Protocol*) que serão descritos a seguir.

2.5 OSPF

O OSPF, a exemplo do RIP, é um protocolo aberto, disponível ao público, sendo que pode ser desenvolvido e aperfeiçoado por vários fabricantes. É um dos mais importantes protocolos que utilizam algoritmos de roteamento estado de enlace, também conhecidos como algoritmos SPF e é comumente utilizado

(juntamente com o seu “primo”, o IS-IS) em ISPs de níveis mais altos, já que sua implementação é mais complexa.

Os roteadores de uma rede que utilizam o OSPF identificam os roteadores vizinhos e, então, se comunicam com eles. As informações recebidas dos roteadores vizinhos possibilitam a criação de um banco de dados *link-state*. O roteador então constrói um mapa topológico completo de toda a rede, utilizando um algoritmo de Dijkstra para determinar os caminhos mais curtos para todas as sub-redes, utilizando uma métrica baseada na largura de banda do caminho (KUROSE, 2006).

Outra característica do OSPF é a capacidade de designação de um roteador, em um determinado segmento, que fará a comunicação, ou seja, o envio das informações de *link-state* para os demais roteadores. Em um segmento de rede multiacesso com *broadcast*, a troca de informações entre todos os roteadores vizinhos pode gerar uma grande sobrecarga. Com o roteador designado, chamado de DR (*Designed Router*), todos os roteadores de um segmento enviam suas informações de *link-state* para este que age como um porta-voz do segmento, repassando estas informações para os demais roteadores do segmento.

Tipo	Nome do pacote	Descrição
1	Hello	Detecta vizinhos e cria adjacências entre eles
2	Descrição de banco de dados (DBD)	Verifica se há sincronização de banco de dados entre roteadores
3	Requisição Link-State (LSR)	Solicita registros de link-state específicos de roteador para roteador
4	Atualização Link-State (LSU)	Envia registros de link-state especificamente solicitados
5	Link-State Acknowledgement (LSAck)	Reconhece os outros tipos de pacote

Figura 3 – Tipos de pacote OSPF

Fonte: Cisco, 2007

A figura 3 mostra os cinco diferentes tipos de pacotes link-state OSPF. Cada pacote serve a um propósito específico no processo de roteamento OSPF:

- *Hello* – Os pacotes *Hello* são utilizados para estabelecer e manter a adjacência com outros roteadores OSPF.

- DBD - O pacote de Descrição de Bancos de Dados (DBD) contém uma lista abreviada do banco de dados *link-state* do roteador que o está enviando, os roteadores que o recebem comparam com o banco de dados *link-state* local.
- LSR - Os roteadores que recebem podem solicitar mais informações sobre qualquer entrada no DBD enviando uma Requisição *Link-State* (LSR).
- LSU - Os pacotes de Atualização *Link-State* (LSU) são utilizados para responder às LSRs, bem como anunciar novas informações. Os LSUs contêm sete tipos diferentes de Anúncios *Link-State* (LSAs). Os LSUs e os LSAs são brevemente discutidos em um tópico posterior.
- LSAck - Quando um LSU é recebido, o roteador envia um *Link-State Acknowledgement* (LSAck) para confirmar o recebimento do LSU.

2.6 EIGRP

O EIGRP é um protocolo híbrido, que utiliza técnicas de algoritmos vetor de distância e estado de enlace, combinadas de forma a reduzir as dificuldades, principalmente em termos de convergência para o caso de mudanças na rede.

Como o próprio nome já diz (*enhanced* = reforçado) é uma versão melhorada do IGRP, sendo um protocolo *classless*, possibilitando a prática do VLSM, CIDR e sumarização de rotas além de melhorar a segurança da rede, através de autenticação (FILIPETTI, 2007). Por ser muito semelhante ao IGRP, o EIGRP é compatível como o seu “irmão”, proporcionando interoperabilidade entre os protocolos, fazendo um compartilhamento de rotas automático, sem a necessidade de configurações avançadas.

O EIGRP inclui diversos recursos que geralmente não são encontrados em outros protocolos de roteamento de vetor de distância como o RIP (*Routing Information Protocol*) e IGRP. Estes recursos incluem:

- O Protocolo confiável de transporte (RTP, *Reliable Transport Protocol*);
- Atualizações associadas;
- Algoritmo de atualização por difusão (DUAL, *Diffusing Update Algorithm*);
- Estabelecimento de adjacências;
- Tabelas de vizinho e topologia.

A tabela de vizinhos é a mais importante do EIGRP. Ela contém a lista de roteadores adjacentes. Para trocar informações entre os vizinhos os roteadores utilizam pacotes do tipo *hello*, como podemos observar na figura 4. Pacotes *hello* são utilizados para descobrir e manter adjacências e para a eleição de um DR em redes multiacesso. Quando um roteador envia ao seu vizinho um pacote *hello*, este marca o seu endereço e a interface a qual está conectado. O pacote anuncia um *hold time* (tempo de retenção), que é o período de tempo no qual um roteador considera um vizinho como alcançável e operacional. Após este período se o roteador não receber outro pacote *hello* do vizinho, este será considerado inalcançável e a rota deverá ser recalculada (Cisco Systems, 2003).

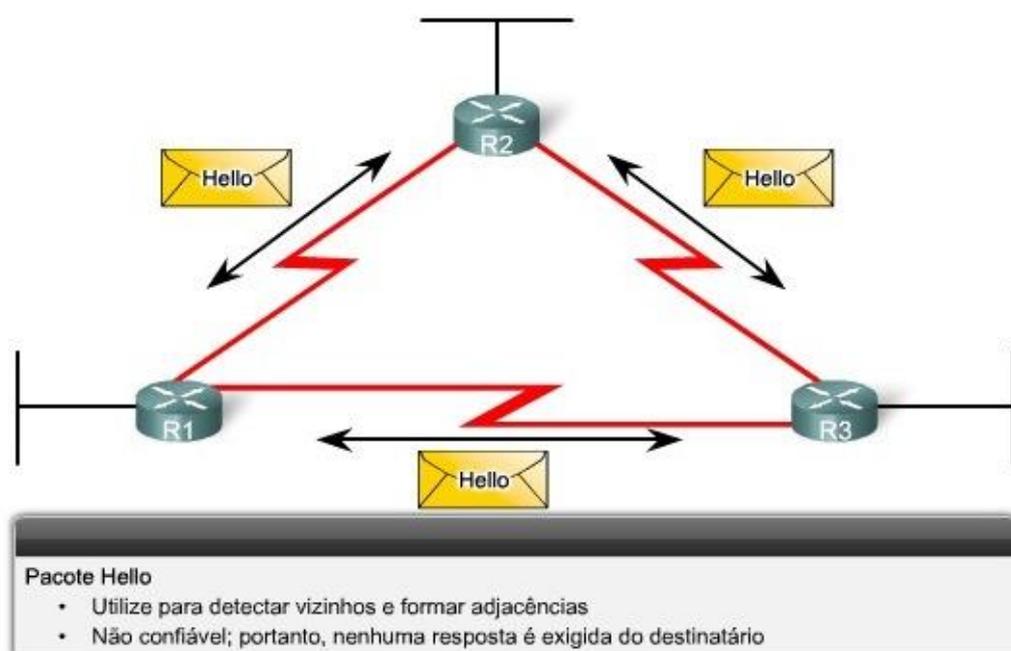


Figura 4 – Tipos de pacote EIGRP

Fonte: Cisco, 2007

A tabela de topologia contém todos os destinos informados pelos roteadores vizinhos. Para cada destino é associado um endereço IP e uma lista de vizinhos que anunciaram este destino, juntamente com a métrica anunciada. É importante

destacar que os roteadores irão anunciar apenas rotas que estejam utilizando, sendo esta uma regra básica de protocolos que utilizam vetor distância.

Com estas informações é possível montar a tabela de roteamento, que irá conter apenas as melhores rotas para cada destino. Para este estudo é importante entender mais a fundo quais as métricas utilizadas pelo EIGRP e como elas são combinadas para a determinação das melhores rotas.

Para cada rota o EIGRP associa 5 (cinco) diferentes métricas, que são praticamente as mesmas utilizadas pela IGRP. São elas:

- *Delay* – atraso (10s de micro-segundos)
- *Bandwidth* – largura de banda ou taxa de transferência (*kilobits* por segundo)
- *Reliability* – confiabilidade (número entre 1 e 255; sendo 255 o mais confiável)
- *Load* – carga (número entre 1 e 255; sendo 255 o mais saturado)
- MTU (*Minimum path Maximum Transmission Unit*)

Por padrão, apenas *Delay* e *Bandwidth* são habilitados em um roteador usando EIGRP, sendo que as métricas podem ser habilitadas ou desabilitadas pelo administrador conforme necessário.

3 SIMULAÇÃO

A seguir serão mostrados exemplos de como fazer a implementação do túnel manual com roteadores Cisco pelo programa Packet Tracer 6.0.1. A configuração manual consiste em definir quais serão os IPv4 de origem e destino que serão utilizados em cada ponta do túnel. Ao ser recebido pelo nó destino, o pacote IPv6 é desencapsulado e tratado adequadamente.

Esse tipo de túnel pode ser utilizado para contornar um equipamento ou enlace sem suporte a IPv6 numa rede, ou para criar túneis estáticos entre duas redes IPv6 através da *Internet* IPv4.

3.1 MODELO COM OSPF

A figura 5 mostra a topologia utilizada na simulação do túnel manual com o protocolo OSPF.

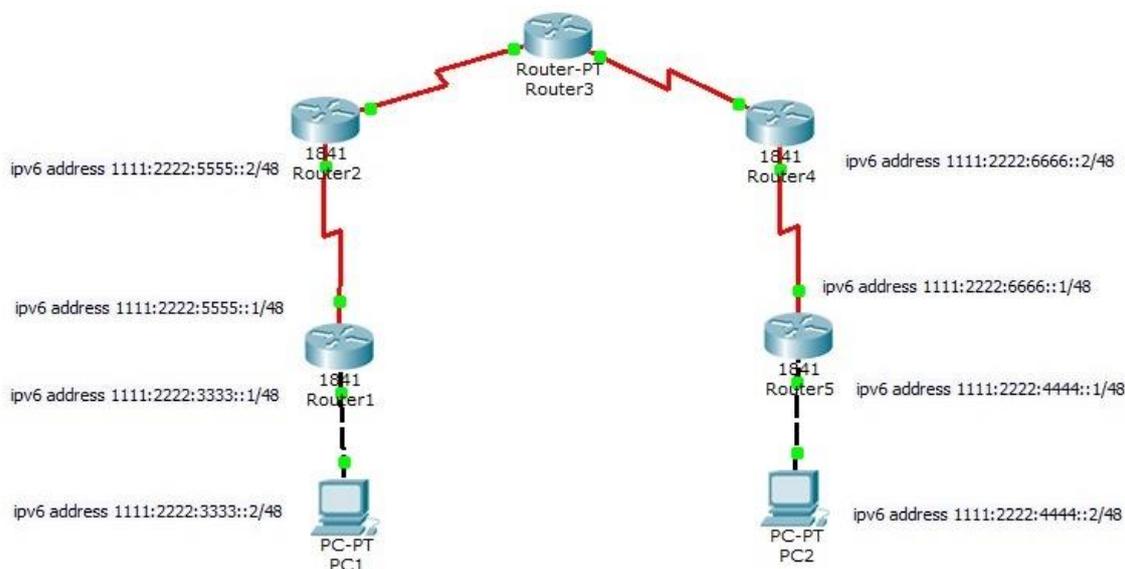


Figura 5 – Topologia utilizada na simulação túnel manual com OSPF

Fonte: Autoria Própria

A tabela 2 demonstra os IPs utilizados com seus respectivos dispositivos e interfaces.

Tabela 2 - Tabela IP dos dispositivos e suas interfaces no modelo OSPF

Dispositivo	Interface	Endereço IP	Máscara
Router 1	FastEthernet 0/0	1111:2222:3333::1/48	
Router 1	Serial 0/1/0	1111:2222:5555::1/48	
Router 2	Serial 0/0/0	1111:2222:5555::2/48	
Router 2	Serial 0/1/0	192.23.1.2	255.255.255.0
Router 3	Serial 2/0	192.23.1.3	255.255.255.0
Router 3	Serial 3/0	192.34.1.3	255.255.255.0
Router 4	Serial 0/0/0	192.34.1.4	255.255.255.0
Router 4	Serial 0/1/0	1111:2222:6666::2/48	
Router 5	FastEthernet 0/0	1111:2222:4444::1/48	
Router 5	Serial 0/1/0	1111:2222:6666::1/48	
PC1	FastEthernet 0	1111:2222:3333::2/48	
PC2	FastEthernet 0	1111:2222:4444::2/48	

Fonte: Autoria própria

A seguir será demonstrado as configurações utilizadas em cada roteador para o seu funcionamento. Podemos observar que o túnel foi estabelecido no Router2 e Router4.

Configurações no Router1

```
interface FastEthernet0/0
ipv6 address 1111:2222:3333::1/48
ipv6 ospf 1 area 0
```

```
interface Serial0/1/0
ipv6 address 1111:2222:5555::1/48
ipv6 ospf 1 area 0
```

```
ipv6 router ospf 1
router-id 1.1.1.1
log-adjacency-changes
```

```
ip classless
```

Configurações no Router2

```
interface Tunnel0
mtu 1476
ipv6 address 3000::1/112
ipv6 ospf 1 area 0
tunnel source Serial0/1/0
tunnel destination 192.34.1.4
tunnel mode ipv6ip
```

```
interface Serial0/0/0
ipv6 address 1111:2222:5555::2/48
ipv6 ospf 1 area 0
clock rate 1000000
```

```
interface Serial0/1/0
ip address 192.23.1.2 255.255.255.0
clock rate 1000000
```

```
router ospf 100
log-adjacency-changes
network 192.23.1.0 0.0.0.255 area 0
```

```
ipv6 router ospf 1
router-id 3.3.3.3
log-adjacency-changes
```

```
ip classless
no cdp run
```

Configurações no Router3

```
interface Serial2/0  
ip address 192.23.1.3 255.255.255.0
```

```
interface Serial3/0  
ip address 192.34.1.3 255.255.255.0  
clock rate 1000000
```

```
router ospf 100  
log-adjacency-changes  
network 192.23.1.0 0.0.0.255 area 0  
network 192.34.1.0 0.0.0.255 area 0
```

```
ip classless
```

Configurações no Router4

```
interface Tunnel0  
mtu 1476  
ipv6 address 3000::2/112  
ipv6 ospf 1 area 0  
tunnel source Serial0/0/0  
tunnel destination 192.23.1.2  
tunnel mode ipv6ip
```

```
interface Serial0/0/0  
ip address 192.34.1.4 255.255.255.0
```

```
interface Serial0/1/0  
ipv6 address 1111:2222:6666::2/48  
ipv6 ospf 1 area 0
```

```
router ospf 100  
log-adjacency-changes
```

```
network 192.34.1.0 0.0.0.255 area 0
```

```
ipv6 router ospf 1  
router-id 4.4.4.4  
log-adjacency-changes
```

```
ip classless  
no cdp run
```

Configurações no Router5

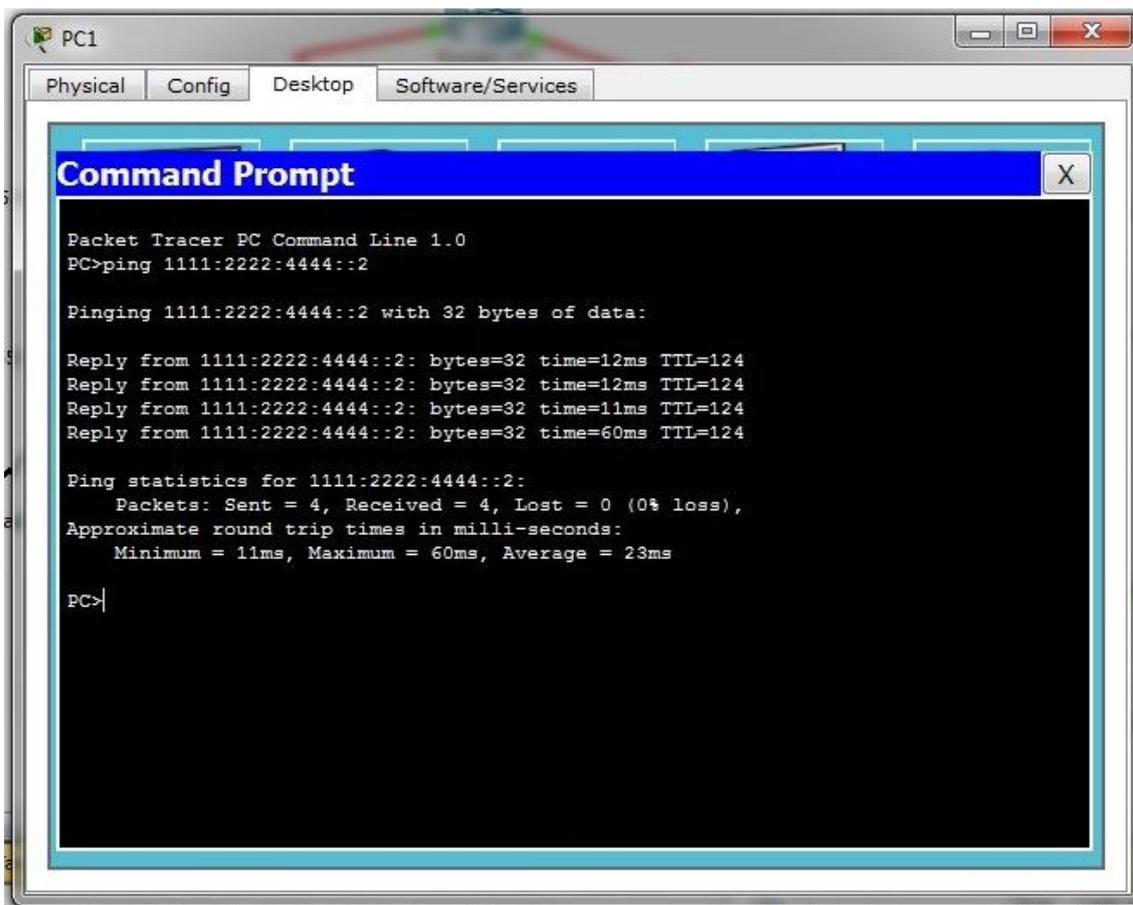
```
interface FastEthernet0/0  
ipv6 address 1111:2222:4444::1/48  
ipv6 ospf 1 area 0
```

```
interface Serial0/1/0  
ipv6 address 1111:2222:6666::1/48  
ipv6 ospf 1 area 0
```

```
ipv6 router ospf 1  
router-id 2.2.2.2  
log-adjacency-changes
```

```
ip classless  
no cdp run
```

Para realizar o teste de conectividade foi utilizado o comando *ping*, como podemos observar na figura 6. O *ping* foi realizado do PC1 para o PC2, ou seja, foi possível trafegar via *Internet* IPv4, comprovando assim que o túnel está funcionando perfeitamente.



The image shows a screenshot of a Packet Tracer PC Command Prompt window. The window title is "PC1" and it has tabs for "Physical", "Config", "Desktop", and "Software/Services". The Command Prompt window is titled "Command Prompt" and contains the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 1111:2222:4444::2

Pinging 1111:2222:4444::2 with 32 bytes of data:

Reply from 1111:2222:4444::2: bytes=32 time=12ms TTL=124
Reply from 1111:2222:4444::2: bytes=32 time=12ms TTL=124
Reply from 1111:2222:4444::2: bytes=32 time=11ms TTL=124
Reply from 1111:2222:4444::2: bytes=32 time=60ms TTL=124

Ping statistics for 1111:2222:4444::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 60ms, Average = 23ms

PC>
```

Figura 6 – Ping realizado do PC1 para o PC2

Fonte: Autoria própria

3.2 MODELO COM EIGRP

A figura 7 mostra a topologia utilizada na simulação do túnel manual com o protocolo EIGRP.

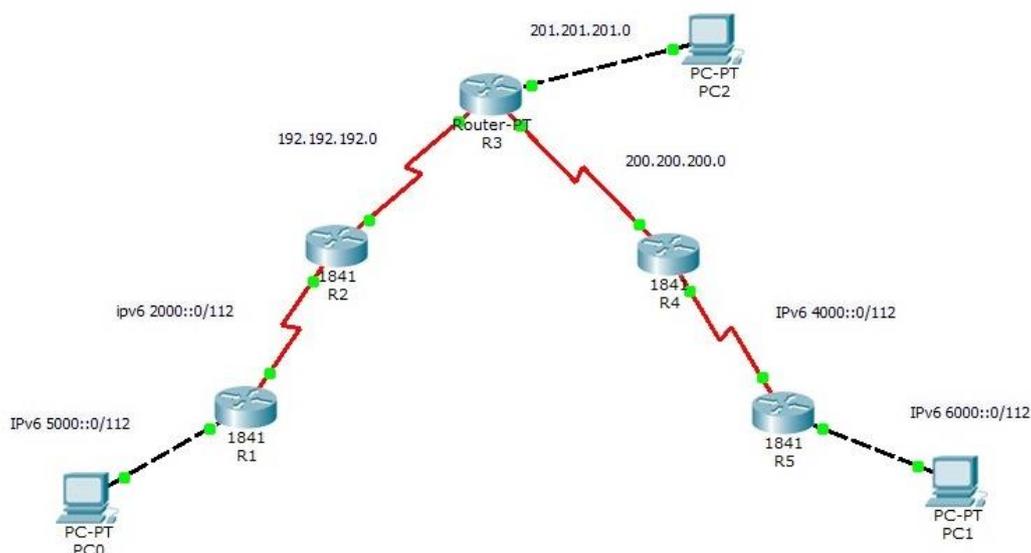


Figura 7 – Topologia utilizada na simulação túnel manual com EIGRP

Fonte: Autoria Própria

A tabela 3 demonstra os IPs utilizados com seus respectivos dispositivos e interfaces.

Tabela 3 - Tabela IP dos dispositivos e suas interfaces no modelo EIGRP

Dispositivo	Interface	Endereço IP	Máscara
R1	FastEthernet0/0	5000::2/112	
R1	Serial0/1/0	2000::2/112	
R2	Serial0/0/0	192.192.192.2	255.255.255.0
R2	Serial0/1/0	2000::1/112	
R3	FastEthernet0/0	201.201.201.1	255.255.255.0
R3	Serial2/0	192.192.192.3	255.255.255.0
R3	Serial3/0	200.200.200.3	255.255.255.0
R4	Serial0/0/0	200.200.200.4	255.255.255.0
R4	Serial0/1/0	4000::1/112	
R5	FastEthernet0/0	6000::1/112	
R5	Serial0/1/0	4000::2/112	
PC0	FastEthernet 0	5000::2/112	
PC1	FastEthernet 0	6000::2/112	
PC2	FastEthernet 0	201.201.201.2	255.255.255.0

Fonte: Autoria própria

A seguir será demonstrado as configurações utilizadas em cada roteador para o seu funcionamento. Podemos observar que o túnel foi estabelecido no R2 e R4.

Configurações no R1

```
interface FastEthernet0/0
ipv6 address 5000::2/112
ipv6 eigrp 222
```

```
interface Serial0/1/0
ipv6 address 2000::2/112
ipv6 eigrp 222
clock rate 1000000
```

```
router eigrp 100
network 192.192.192.0
network 200.200.200.0
network 201.201.201.0
auto-summary
```

```
ipv6 router eigrp 222
router-id 3.3.3.3
no shutdown
```

Configurações no R2

```
interface Tunnel0
mtu 1476
ipv6 address 3000::1/112
ipv6 eigrp 222
tunnel source Serial0/0/0
tunnel destination 200.200.200.4
tunnel mode ipv6ip
```

```
interface Serial0/0/0
```

```
ip address 192.192.192.2 255.255.255.0
ipv6 eigrp 222
clock rate 1000000
```

```
interface Serial0/1/0
ipv6 address 2000::1/112
ipv6 eigrp 222
```

```
router eigrp 100
network 192.192.192.0
network 200.200.200.0
network 201.201.201.0
auto-summary
```

```
ipv6 router eigrp 222
no shutdown
```

```
ipv6 router eigrp 2222
router-id 4.4.4.4
shutdown
```

Configurações no R3

```
interface FastEthernet0/0
ip address 201.201.201.1 255.255.255.0
```

```
interface Serial2/0
ip address 192.192.192.3 255.255.255.0
```

```
interface Serial3/0
ip address 200.200.200.3 255.255.255.0
clock rate 1000000
```

```
router eigrp 100
network 192.192.192.0
network 200.200.200.0
network 201.201.201.0
auto-summary
```

```
router rip
```

Configurações no R4

```
interface Tunnel0
mtu 1476
ipv6 address 3000::2/112
ipv6 eigrp 222
tunnel source Serial0/0/0
tunnel destination 192.192.192.2
tunnel mode ipv6ip
```

```
interface Serial0/0/0
ip address 200.200.200.4 255.255.255.0
ipv6 eigrp 222
```

```
interface Serial0/1/0
ipv6 address 4000::1/112
ipv6 eigrp 222
```

```
router eigrp 100
network 192.192.192.0
network 200.200.200.0
network 201.201.201.0
auto-summary
```

```
ipv6 router eigrp 222
```

```
no shutdown
```

```
ipv6 router eigrp 2222  
router-id 2.2.2.2  
shutdown
```

Configurações no R5

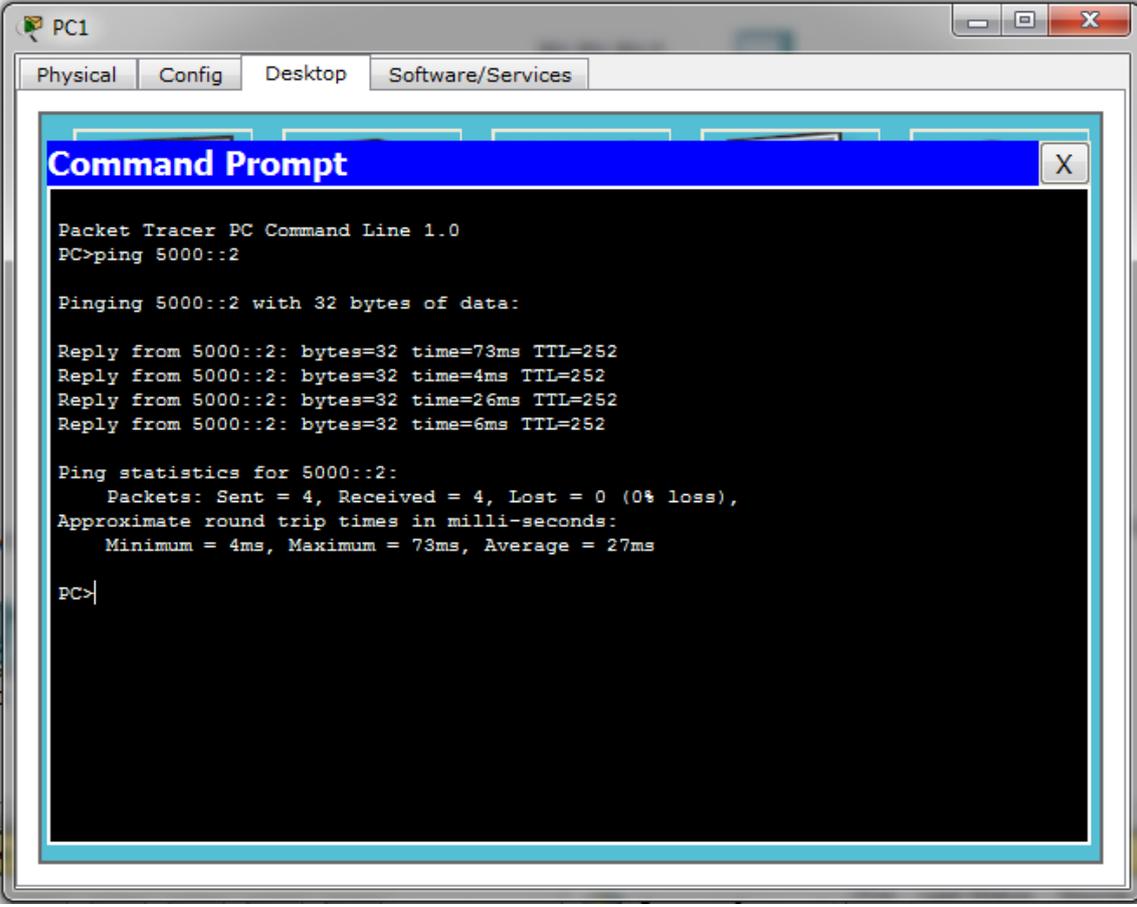
```
interface FastEthernet0/0  
ipv6 address 6000::1/112  
ipv6 eigrp 222
```

```
interface Serial0/1/0  
ipv6 address 4000::2/112  
ipv6 eigrp 222  
clock rate 1000000
```

```
router eigrp 222  
auto-summary
```

```
ipv6 router eigrp 222  
router-id 1.1.1.1  
no shutdown
```

Para realizar o teste de conectividade foi utilizado o comando *ping*, como podemos observar na figura 8. O *ping* foi realizado do PC1 para o PC0, ou seja, foi possível trafegar via *Internet* IPv4, comprovando assim que o túnel está funcionando perfeitamente.



The image shows a Packet Tracer PC Command Prompt window for PC1. The window title is "Command Prompt" and it has a blue header bar. The main content area is black with white text. The text shows the command "PC>ping 5000::2" being executed. The output indicates that the ping was successful, with four replies received from 5000::2. The ping statistics show that all four packets were received, with a 0% loss rate. The approximate round trip times in milliseconds are: Minimum = 4ms, Maximum = 73ms, and Average = 27ms. The prompt "PC>" is visible at the bottom of the window.

```
Packet Tracer PC Command Line 1.0
PC>ping 5000::2

Pinging 5000::2 with 32 bytes of data:

Reply from 5000::2: bytes=32 time=73ms TTL=252
Reply from 5000::2: bytes=32 time=4ms TTL=252
Reply from 5000::2: bytes=32 time=26ms TTL=252
Reply from 5000::2: bytes=32 time=6ms TTL=252

Ping statistics for 5000::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 73ms, Average = 27ms

PC>
```

Figura 8 – Ping realizado do PC1 para o PC0

Fonte: Autoria própria

4 CONCLUSÃO

O esgotamento de endereços do protocolo IPv4 já é realidade reforçando ainda mais a importância da migração para o IPv6 por apresentar um aumento significativo de endereços disponíveis. Durante esse período de migração é preciso que redes IPv6 se comuniquem com outras redes IPv6 mesmo que a infraestrutura entre eles seja IPv4, por isso a importância de técnicas de transição.

Entre estas técnicas temos o túnel manual na qual foi abordado neste trabalho e se demonstrou eficiente, estabelecendo o túnel entre redes IPv6 através de redes IPv4 e funcionando perfeitamente. Demonstrando ser uma fácil e boa opção para empresas que estão migrando para o IPv6.

REFERÊNCIAS

BARROS JÚNIOR, José Carlos. **Estratégia de implementação IPv6**. Disponível em: <<http://www.saude.mt.gov.br/upload/documento/104/estrategias-de-implementacao-ipv6-autor-jose-carlos-barros-junior-%5B104-070212-SES-MT%5D.pdf>> Acesso em: 07 de Junho de 2013.

BRADNER, S; MANKIN, A. **RFC 1752 – The Recommendation for the IP Next Generation Protocol**. January 1995.

CARPENTER, B.; MOORE, K. **RFC 3056 Connection of IPv6 Domains via IPv4 Clouds**, 2001.

Cisco. **IPv6 Extension Headers Review and Considerations**, 2006. Disponível em: <http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html> Acesso em: 23 de Julho de 2013.

Cisco Systems. **CCNA 2: Conceitos Básicos de Roteadores**, v. 3.1.1, 2003.

_____. **CCNA Exploration 4.0**, 2007.

DEERING, S.; HINDEN, R. **Internet Protocol, Version 6 (IPv6) Specifications**, RFC 1883, Abril 1996.

DOMINGOS, Fabiano Donisete. **Técnica de transição entre redes IPv4/IPv6**. Disponível em: <<http://www.alessandrobianchini.com.br/artigos/ipv6.pdf>> Acesso em: 03 de Junho de 2013.

FILIPPETTI, M. A. **CCNA 4.0: Guia Completo de Estudos**. Florianópolis: Visual Books, 2007.

HAGEN, Sílvia. **IPv6 Essentials**. O'Reilly, 2002.

IPv6.br. **Transição**. Disponível em: <<http://ipv6.br/entenda/transicao/>> Acesso 04 de Agosto de 2014.

KUROSE, James F. **Redes de Computadores e a Internet: uma abordagem top-down**. São Paulo: Pearson Addison Wesley, 2006.

TANENBAUM, Andrew. S. **Redes de Computadores**. 4. ed. São Paulo: Campus, 2003.

TEMPLIN, F.; GLEESON, T.; THALER, D. **RFC 5214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)**, 2008

ZAKON, Robert Hobbes. **Hobbes' Internet Timeline 10.2**. Disponível em: <<http://www.zakon.org/robert/internet/timeline>> Acesso em: 11 de Junho de 2013