UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
CURSO SUPERIOR DE TECNOLOGIA EM DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO

EDIVANIA CARDOSO REGHINI

TÉCNICAS DE TUNELAMENTO PARA REDES HIBRIDAS IP & IPv6

TRABALHO DE DIPLOMAÇÃO

MEDIANEIRA – PR
2013

EDIVANIA CARDOSO REGHINI

TÉCNICAS DE TUNELAMENTO PARA REDES HIBRIDAS- IP &IPv6

Trabalho de conclusão de curso, da disciplina de Trabalho de Diplomação do curso de Tecnologia em Desenvolvimento de Sistemas –UTFPR – Universidade Tecnológica Federal do Paraná, Câmpus Medianeira.
Tendo como requisito parcial para obtenção do curso de tecnólogo.

Orientador: Neylor Michel, Dr.

MEDIANEIRA – PR
2013

Ministério da Educação

Universidade Tecnológica Federal do Paraná

Diretoria de Graduação e Educação Profissional

Curso Superior de Tecnologia Desenvolvimento de Sistemas de Informação

TERMO DE APROVAÇÃO

TÉCNICAS DE TUNELAMENTO PARA REDES HIBRIDAS. IPv4-IPv6

Por

EDIVANIA CARDOSO REGHINI

Este Trabalho de Diplomação (TD) foi apresentado às 09:10 h do dia 27 de março de 2013 como requisito parcial para a obtenção do título de Tecnólogo no Curso Superior de Tecnologia em Desenvolvimento de Sistemas de Informação, da Universidade Tecnológica Federal do Paraná, Câmpus Medianeira. A acadêmica foi arguida pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com louvor e mérito.

Prof. Dr. Neylor Michel
UTFPR – *Campus* Medianeira
(Orientador)

Prof. Me. Paulo Lopes de Menezes
UTFPR – *Campus* Medianeira
(Convidado)

Prof. Me.Cesar Angonese
UTFPR – *Campus* Medianeira
(Convidado)

Prof. Me. Juliano R. Lamb
UTFPR – *Campus* Medianeira
(Responsável pelas atividades de TCC)

"Há um tempo em que é preciso abandonar as roupas usadas, que já tem a forma do nosso corpo, e esquecer os nossos caminhos, que nos levam sempre aos mesmos lugares". É o tempo da travessia: e, se não ousarmos fazê-la, teremos ficado, para sempre, à margem de nós mesmos.

Fernando Pessoa

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, por ter me dado uma família tão especial que sempre me apoiou em vários momentos difíceis durante minha estadia na Universidade, pela compreensão e dedicação sempre.

Dedico também aos meus amigos parceiros em todas as horas.

AGRADECIMENTOS

Agradeço primeiramente a Deus.

A minha família que batalhou para me manter em uma Universidade publica.

Aos amigos e colegas de turma que contribuíram para meu crescimento pessoal e intelectual.

Ao Professor Neylor Michel por ter me orientado e auxiliado no desenvolvimento deste trabalho de diplomação.

As minhas amigas em especial a Salaia, Aline, Daiane, Bruna, Poliana e a minha irmã Edilaine por me aturarem nos momentos de stress, sempre dando aquele apoio moral e torcendo pelo meu sucesso.

A todos aqueles que, direta ou indiretamente, colaboraram para que este trabalho atingisse os objetivos propostos.

RESUMO

O *Internet Protocol version* 6 (IPv6) é o protocolo de rede que surgiu para suprir a necessidade do protocolo IPv4 que esta em uso desde 1980. Existem inúmeras mudanças no IPv6 em relação ao Protocolo versão 4 (IPv4), onde a mais significante delas foi o aumento do seu tamanho de endereços de rede de 32 para 128 bits. Isso proporciona um numero maior de endereços suficientes para satisfazer a demanda mundial por um único endereço IP. A demanda atual de uso da Internet, páginas da web, e-mail, serviços *peer-to-peer*, bem como a utilização de dispositivos móveis, cresceu muito além das expectativas de seus autores. Aplicações em grande escala e o desenvolvimento de novas tecnologias e redes móveis têm superado a capacidade do IPv4 para oferecer serviços adequados e endereços exclusivo na grande rede. O IPv6 veio para resolver as limitações endereçamento, bem como fornecer mais funcionalidade. O IETF iniciou o projeto Internet *Protocol Next Generation* (IPng), em 1993, para investigar diferentes propostas e formular recomendações para ações futuras. Paralelamente com o desenvolvimento do novo protocolo era desenvolvido um conjunto de mecanismos chama SIT (*Simple Internet Transition*) onde é especificado regras de gerenciamento e protocolos para simplificar a migração. Uma das principais características do SIT era que a transição deve ser realizada de uma forma progressiva evitando a troca e a atualização mínima dos equipamentos já existente na rede. O tunelamento, possibilita a transmissão de pacotes IPv6 através da infraestrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4.

Palavras – chave : tunelamento, cabeçalho e configuração.

ABSTRACT

The Internet Protocol version 6 (IPv6) is a network protocol that has emerged to meet the need of the IPv4 protocol that is in use since 1980. There are numerous changes over the IPv6 Protocol version 4 (IPv4), where the most significant of these was the increase of size of network address bits from 32 to 128. This provides a larger number of addresses sufficient to meet global demand for a single IP address. The current demand for using the Internet, web pages, email services, peer-to-peer, and the use of mobile devices has grown far beyond the expectations of the authors. Large-scale applications and development of new technologies and mobile networks have surpassed the ability of IPv4 to provide adequate services and exclusive addresses in the network .. The large IPv6 address came to addressing the limitations and provide additional functionality. The project started the IETF Internet Protocol Next Generation (IPng) in 1993 to investigate various proposals and make recommendations for future action. In parallel with the development of the new protocol was developed a set of mechanisms called SIT (Simple Internet Transition) which is specified management rules and protocols to simplify migration. One of the main features of the SIT was that the transition should be done in a progressive manner avoiding the exchange and minimal upgrade of equipment already on the network. The tunneling enables the transmission of IPv6 packets through IPv4 existing infrastructure without the need for any change in routing mechanisms, encapsulating the contents of the IPv6 packet in an IPv4 packet.

Keywords: tunneling, header and configuration.

SIGLAS

APNIC - The Asia Pacific Network Information Centre

ARPA - Advanced Research Projects Agency

CDIR - Classless Inter Domain Routing.

CPU - Central Processing Unit

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DOD - Departament of Defense

HTTP- Hypertext Transfer Protocol

IANA - Internet Assigned Numbers Authority

ICMP - Internet Control Message Protocol

IETF - Internet Engineering Task Force

IP - Internet Protocol

IPSEC - IP Security Protocol

IPv4 - Internet protocolo versão 4

IPv6 - Internet protocolo versão 6

IPX - Internetwork Packet Exchange

ISP - Internet Service Provider

MAC - Media Access Control address

MPLS- Multi Protocol Label Switching

MTU - Maximum Trasmit Unit

NAT - Network Address Translation.

NCP - Network Control Protocol

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First.

P2P - Peer-to-Peer

PAT – Port Address Translation

PPP - Point-to-Point Protocol

QoS - Quality of Service

RFC - Request for Comments

RIP - Routing Information Protocol.

ROAD - Routing and Addressing

SIT - Simple Internet Transition

TCP/IP - Transmition Control Protocol / Internet Protocol

TTL - Time To Live

UDP - User Datagram Protocol

VOIP- Voice Over Internet Protocol.

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

O IPv4 (RFC 791) foi concebido há 30 anos para um número relativamente pequeno de usuários. Naquela época, parecia improvável que a tecnologia de computação pessoal iria se tornar tão difundida como é hoje no mundo. Em 1981 a Internet era utilizada quase que exclusivamente por acadêmicos e pesquisadores, e os 4,3 bilhões de endereços IPv4 disponíveis teoricamente foram considerados mais do que suficiente. Atualmente o conjunto de endereços de IPv4 que é de responsabilidade da IANA (Internet Assigned Numbers Authority) esta se reduzindo de maneira significativa e seu fim se aproxima rapidamente.

Devido a este grande crescimento, surgiram inúmeras aplicações, estas por sua vez começaram a variar e a apresentar novas necessidades as quais o IPV4 mostrou-se deficiente pois foi projetado inicialmente para ser utilizado em uma rede acadêmica com poucos requisitos. A Internet esta muito difundida nos dias atuais e a partir da mesma criou-se novos nichos de mercados e negócios onde podemos destacar o e-commerce e o vídeo conferência.

O IETF (Internet Task Engineering Force) resolveu especificar uma nova versão para o protocolo IP, o IPv6. O projeto IPv6 vai muito além de uma versão do antigo protocolo IPv4 com endereçamento de 128 bits, funções desnecessárias foram removidas, serviços e funções que trabalhavam bem foram mantidas, novas funcionalidades foram acrescentadas além do aumento do espaço de endereçamento de 32 para 128 bits, suportando mais níveis de hierarquias e endereçamento.

Um dos principais desafios encontrados pelo IETF foi desenvolver um protocolo que atendesse as novas demandas do mercado e a interoperabilidade com o protocolo IPv4, além de sua implantação ser flexível. Espera-se que a transição ocorra antes que a capacidade de endereçamento e roteamento IPv4 atinja o seu limite máximo. Os mecanismos de transição asseguram que dispositivos rodando IPv6 ou IPv4, ou com ambos, possam colaborar mutuamente, permitindo que tanto ambientes que tenham os protocolos de mesma versão, quanto os que possuam versões distintas, possam interoperar durante a fase de transição. Esta característica protege os investimentos realizados em tecnologia IPv4 e garante que o mesmo não ficará obsoleto, até a migração de todas as máquinas que compõem a Internet.

O objetivo deste trabalho é apresentar as principais características do protocolo IPv6, incluindo arquitetura de endereçamento e as novas funcionalidades incluídas,

analisando seus principais mecanismos utilizados para a transição do IPv4 para o IPv6, definindo quais os métodos mais indicados para efetuar a migração da tecnologia atualmente em uso (IPv4) para a sua sucessora (IPv6).

O fator que mais encoraja o desenvolvimento sobre o protocolo IPv6 é o tamanho de seu endereçamento de 128 bits, contra 32 bits do atual IPv4, o endereçamento maior permite uma hierarquia mais flexível e o roteamento de grandes blocos. Além do endereçamento, novos serviços são oferecidos pelo IPV6, como stateless auto configuration, renumeração facilitada, serviço anycasting e segurança padronizada para a camada de rede.

Tendo o endereçamento do protocolo aumentado para 16 bytes, adaptações e até mesmo modificações estão sendo feitas, em protocolos de controle, de roteamento, em estruturas de registros de endereços e outros.

1.1 OBJETIVO GERAL

Apresentar um estudo do protocolo IPv6 e os mecanismos de transição sendo esse protocolos de tunelamento, que poderão ser utilizados para assegurar uma implantação bem-sucedida e segura do protocolo IPv6 tento como principal objetivo manter a comunicação entre o protocolo já existente o IPv4. Para realizar os testes será o simulador GNS3.

1.2 OBJETIVOS ESPECÍFICOS

- Desenvolver um referencial teórico sobre o protocolo e cabeçalho IPv6.
- Apresentar os materiais e métodos de transição entre IPv6 e IPv4.
- Apresentar e configurar os principais protocolos de tunelamento para IPv6.
- Apresentar um protocolo de tunelamento suportável pelo software de simulação GNS3.

1.3 JUSTIFICATIVA

O esgotamento de endereços IP já é uma realidade, no inicio da década de 80 pesquisadores já previram que haveria um crescimento significativo do numero de computadores e dispositivos na grande rede. O que não se esperava é que houvesse um grande crescimento das aplicações e dispositivos acelerando assim o esgotamento dos endereços IP.

Na prática, a fornecimento de endereços IPv4 disponíveis tem sido limitado desde o início de 1990. Anteriormente, uma organização podia solicitar uma faixa de endereços IP muito maior do que poderia realmente justificar, por esse motivo muitos blocos IPv4 que contam como utilizados não estão sendo utilizados por muitas razões.

Apresentaram-se estudos para se otimizar o uso dos endereços, foram implementados tecnologias do tipo do NAT (Network Address Translation), visando reduzir a necessidade de se fornecer endereços IP a todos os hosts da rede, e o CIDR (Classless Inter-Domain Routing) introduzindo em 1993 pelo RFC 1517 que utiliza mascaras de comprimento variável, amenizando a necessidade do desenvolvimento de um novo protocolo.

A implantação do IPv6, apesar do assunto ser muito comentado, ainda anda a passos curtos, mas vem aumentando gradativamente. A não implantação deste novo protocolo pode prejudicar o desenvolvimento da Internet, e o desenvolvimento de muitas empresas e serviços.

Tendo em vista este cenário, o presente trabalho tem como objetivo disponibilizar um estudo sobre o novo protocolo IPv6 e seus principais mecanismos de transição, auxiliando assim nas estratégias de migração das redes existentes.

2 REVISAO BIBLIOGRÁFICA

2.1 ESGOTAMENTO DE ENDEREÇOS

A Internet surgiu através do Departamento de Defesa (DOD – Departament of Defense) do governo dos Estados unidos em 1966 através de sua Agência de pesquisa e Projetos Avançados (ARPA – Advanced Research Projects Agency) que desenvolvia um projeto de interligação de computadores em centros militares e de pesquisas e tinha como principal objetivo formar uma arquitetura de rede sólida e robusta.

No inicio eram utilizados diversos protocolos sendo o principal deles o NCP (Network Control Protocol), mas com o crescimento da rede passou-se a adotar o protocolo TCP/IP, pois o mesmo permitia um crescimento ordenado da rede e eliminava as restrições dos protocolos anteriores.

> Definido na RFC 791, o protocolo IP possui duas funções básicas: a fragmentação, que permite o envio de pacotes maiores que o limite de tráfego estabelecido de um enlace, dividindo-os em partes menores; e o endereçamento, que permite identificar o destino e a origem dos pacotes a partir do endereço armazenado no cabeçalho do protocolo. (SANTOS et al. 2010, p.09)

A versão utilizada o IPv4, versão esta de fácil configuração e interoperabilidade que se mostrou muito robusta com o passar dos anos, mas seu projeto inicial não previu alguns aspectos importantes como o seu possível crescimento e esgotamento dos endereços IP, o aumento da tabela de roteamento, a segurança dos dados transmitidos e a prioridade de entrega de determinados pacotes. O protocolo IPv4 reserva 32 bits para o endereçamento possibilitando gerar mais de 4 bilhões de endereços distintos.

A cada ano que passa a Internet evoluí e o número de pessoas conectadas a grande rede esta cada dia maior, no ano de 1990 estudos já apontavam para o colapso de esgotamento de endereços. A Figura 1 mostra o crescimento do número de usuários na Internet a partir da sua utilização comercial.

> Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de hosts em 1993 para mais de 26.000.000 de hosts em 1997.(SANTOS et al. 2010, p.09)

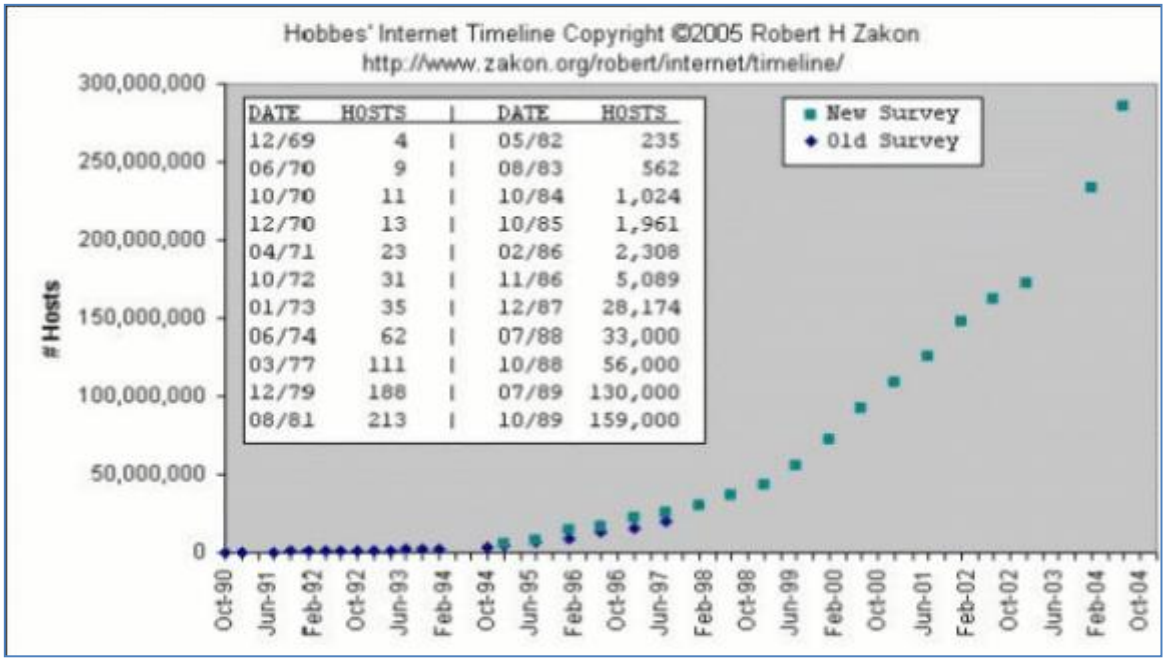

Figura 1- O crescimento da internet

Fonte: MOREIRAS (2009).

Em 1991, membros da IETF (Internet Engineering Task Force) chegaram a conclusão de que o crescimento exponencial da Internet levaria ao esgotamento dos endereços até o final de 1994 isto se as tabelas de roteamento não esgotassem a capacidade dos hardwares de roteamento da época. A figura 2 mostra o Estoque de IANA.

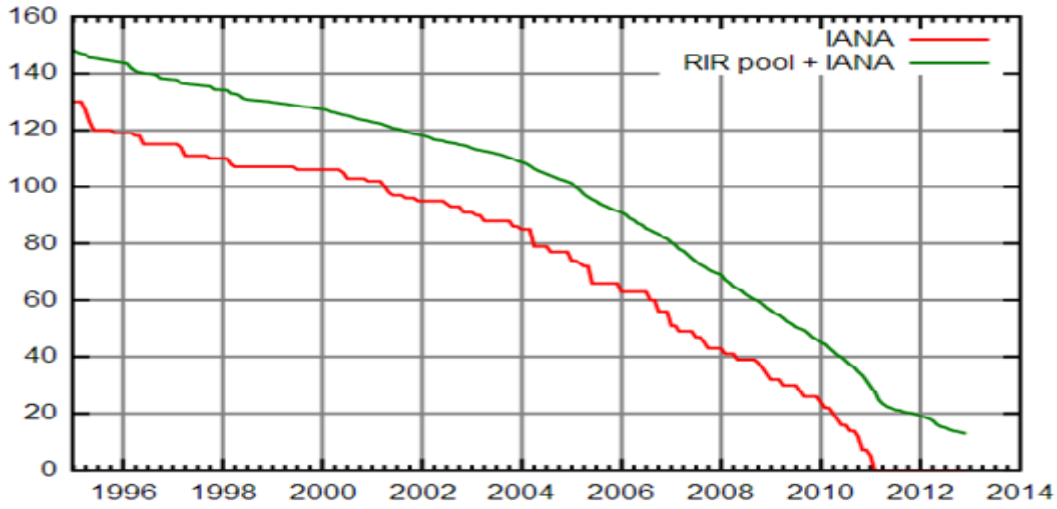

Figura 2- Estoque de IANA

Fonte: WIKIPEDIA (2013)

Diante destes fatos passou-se a discutir nova técnicas e estratégias para solucionar o problema do esgotamento dos endereços IP e o aumento das tabelas de roteamento. Ainda em 1991, é formado um grupo de trabalho, ROAD (Routing and Addressing) que apresenta soluções para o problema. Entre as soluções apresentadas podemos destacar a utilização do CIDR (Classless Interdomain Routing) que tem como principal objetivo terminar com uso de classes permitindo assim a alocação de um tamanho apropriado para a real necessidade da rede além de permitir a agregação de rotas reduzindo assim a tabela de roteamento. Ainda neste ano foram apresentas novas soluções como o DHCP (Dynamic Host Configuration Protocol), a NAT (Network Address Translation).

2.2 O IPV6

Em 1990 a Engineering Task Force (IETF) iniciou as pesquisas para o desenvolvimento de um novo protocolo para a Internet. Foram iniciadas várias pesquisas paralelas na tentativa de resolver o esgotamento dos endereços IP. Em 1993 foi criada pela IETF o grupo IPng (Next Generation Internet Protocol), responsável por analisar todas as pesquisas referentes a criação do novo protocolo, em 1994 houve a recomendação por parte do grupo de pesquisas IPng para a criação de um novo protocolo chamado IPv6, recomendação esta que está especificada na RFC 1752.

O Protocolo IPv6 pode ser considerado como uma das maiores atualizações tecnológica e de infraestrutura da história, criado não só para resolver o problema de esgotamento de endereços IP, mas também para oferecer serviços e benefícios que não existiam no IPv4, muitos desses serviços já existiam e foram melhorados e otimizados.

O novo protocolo foi desenvolvido para atuar em redes de alto desempenho como Gigabit Ethernet, ATM e outros, bem como atuar em redes de baixo desempenho que possuem uma baixa largura de banda, a exemplo das redes sem fio.

2.2.1 Funcionalidades

Dentre muitos os benefícios que foram implementados nesta nova versão podemos destacar:

- O aumento da capacidade de endereçamento;
- Cabeçalhos flexíveis;

- Classes de Serviços (QoS);
- Autoconfiguração;
- Suporte a criptografia (Ipsec);

2.2.2 Endereçamento

O aumento do espaço de endereçamento foi uma das principais razões para a criação do novo protocolo, seguido da otimização das tabelas de roteamento. A grande disponibilidade de endereços permite um grande alcance global, pois o novo protocolo é capaz de endereçar todos os hosts do planeta. Esta alta disponibilidade de endereços é um dos maiores benefícios agregados a esta nova versão de protocolo, pois atenderá a demanda de crescimento da grande rede.

> A disponibilidade de um espaço de endereços e prefixos de rede muito grande fornece uma flexibilidade na arquitetura de redes que permite uma organização hierárquica e possivelmente geográfica, onde um prefixo de rede pode ser usado para endereçar um país ou um continente inteiro subdividido em seus diversos níveis.(SILVA, 2005).

A grande disponibilidade de endereços possibilita o desenvolvimento de novas aplicações para celulares, televisores digitais, telefones IP onde cada um destes dispositivos possuirá um endereço único e global, possibilitando uma conexão fim a fim de tais equipamentos.A arquitetura de endereçamento do novo protocolo inicialmente foi definida através da RFC 1884, mas a mesma se tornou obsoleta em Julho de 1998 com a publicação da RFC2373. O formato dos novos endereços não se difere muito aos que já vinham sendo utilizados, assim como o IPv4 o novo protocolo possui o Prefixo de Rede e o Sufixo de Host.

(FILIPPETI, 2011) comenta sobre as classes de endereços que deixam de existir. A separação entre o Prefixo de Rede e os Sufixos de host pode ser realizada em qualquer parte do endereço utilizando a notação “prefixal” (/xx), da mesma forma que vem sendo utilizado no protocolo IPv4 quando utilizamos a notação CIDR. No endereçamento, dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede.

O endereço IPv6 possui um formato hexadecimal dividido em oito blocos cada bloco possui 04 dígitos hexadecimais (16 bits) separados por dois pontos (":"), o

endereço padrão IPV6 é dividido em três seções: Global Routing Prefix, Subnet e Interface ID, conforme ilustrado na figura 3.

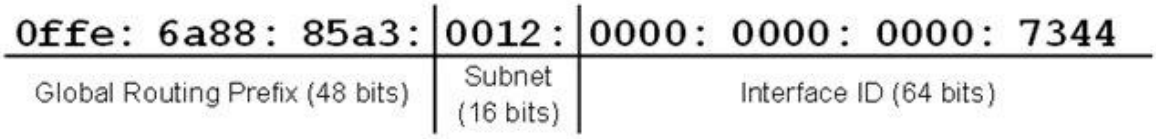

Figura 3 - Endereço padrão IPv6

Fonte: FILIPPETTI (2011)

A partir do prefixo global de roteamento é possível identificar um endereço especial, tais como multicast, ou um intervalo de endereços atribuído a uma rede.

São permitidas abreviações de endereços, onde podem ser omitidos os zeros a esquerda de um bloco, exemplo:

0ffe:6a88:85a3:12:0:0:0:7344

É permitido ainda a utilização de dois pontos, apenas uma única vez, para representar uma sequência consecutivas de zeros, exemplo:

0ffe:6a88:85a3:12::7344

Em ambientes que possuem os dois protocolos é possível encontrar dispositivos com um endereço formado pelos dois protocolos, os valores do endereçamento IPV4 ocupam as 04 ultimas posições, o endereço 192.168.0.2 pode ser representado das seguintes formas: 0:0:0:0:0:0:192.168.0.2, ::192.168.0.2 ou ainda ::C0A8:2. (HAGEN, 2002).

2.3 TIPOS DE ENDEREÇOS

No protocolo IPv4 são conhecidos os endereços unicast, broadcast e multicast, no novo protocolo o endereço broadcast deixa de existir e passa-se utilizar mais os endereços multicast e através da RFC 1546 é apresentado o novo tipo de endereçamento utilizado pelo novo protocolo o anycast.

Endereços unicast identificam uma única interface e pode ser dividido em Global Unicast, Link Local e Unique Local. Link Local-Address (endereços de enlace

local), são endereços locais, este endereço pode ser gerado automaticamente para cada interface, equivale ao IPV4 aos endereços privados não roteáveis, é caracterizado pelo prefixo FE80::/64. Global Unicast (Endereço Unicast Global), corresponde aos endereços válidos atualmente, são endereços únicos que são obtidos através dos provedores. Unique Local (Endereços únicos de escopo local), endereços não roteáveis na Internet, porem podem ser roteados dentro de uma intranet.

Os endereços Multicast possuem os mesmos conceitos dos que são utilizados no IPv4, é um endereço que identifica um grupo de interfaces , um pacote quando enviado a um endereço multicast é processado por todos os membros do grupo.

Anycast, nada mais é que uma modificação dos endereços multicast, onde um endereço Anycast pode ser atribuído a várias interfaces. Um pacote quando enviado a um endereço anycast é entregue a apenas a uma interface, normalmente a mais próxima.

O novo protocolo permite ainda realizar a atribuição de múltiplos endereços IPv6 de qualquer tipo (unicast, multicast anycast) a uma única interface.

De acordo com (NED, 1998) o anycast identifica um bloco de interfaces, de tal forma que um datagrama enviado para o endereço, que é roteado ao longo de um caminho mais curto e entregue a um host de um determinado grupo.

Segundo (COMER, 2001), o endereçamento anycast permite a replicação de serviços, onde uma corporação que fornece serviços através da rede, atribui endereços anycast a vários hosts, e quando um usuário envia um datagrama para um endereço anycast, o IPv6 roteia o datagrama para um dos hosts do grupo.

O endereço anycast não pode ser utilizado como endereço de origem (source address) de qualquer pacote IPv6 e nem pode ser configurado num host IPv6, ou seja, ele só pode ser associado a roteadores, pois existem algumas complicações no uso generalizado desse endereço. (SILVA, 2001).

Para (COMER, 2001), o endereço multicast corresponde a um grupo de hosts, possivelmente em muitas localidades diferentes e a composição do grupo pode mudar a qualquer momento. Quando um datagrama é enviado para um endereço multicast, o IPV6 entrega uma cópia do datagrama para cada membro do grupo.

2.4 CABEÇALHO

O cabeçalho IPv6 é muito mais simples que o cabeçalho IPv4, possui um tamanho fixo de 40 bytes e é definido pela RFC 2460. O cabeçalho IPv6 foi projetado para ser simples e flexível, reduzindo assim a carga de processamento dos roteadores intermediários. Isto é possível, pois transformou os campos não essenciais e campos de opção em cabeçalhos de extensão que não precisam ser processados por todos os roteadores intermediários. Os cabeçalhos flexíveis permitem a adição de novas funcionalidades, dispensando assim a necessidade criação de um novo protocolo para novas aplicações.

A base do cabeçalho é muito parecida com a base do cabeçalho IPv4, embora possua um formato diferente. No cabeçalho do novo protocolo, cinco campos do cabeçalho IPv4 foram removidos: Header Length, Identification, Flags, Fragment Offset, Header Checksum.

O comprimento do cabeçalho (Header Length) foi removido porque agora o seu comprimento é fixo, no IPv4 o comprimento do cabeçalho possui no mínimo 20 bytes, mas se for adicionado os campos opcionais ele pode ser estendido 60 bytes. O campo de identificação (Identification), o campo Flags, e campo de fragmentação (Fragment Offset) eram responsáveis pela “quebra” dos pacotes maiores no cabeçalho do IPV4. A fragmentação acontece quando um grande pacote é enviado através de uma rede que suporta apenas pacotes menores, neste tipo de cenário o roteador IPv4 divide o pacote em fatias menores e encaminhando assim esses pacotes. O host de destino recolhe os pacotes e os remonta novamente, se faltar um pacote ocorre um erro e a transmissão deverá ser refeita.

No protocolo IPv6, um host descobre o caminho e o tamanho da unidade máxima de transmissão (MTU), através de um procedimento chamado Path MTU Discovery. Se houver a necessidade de fragmentação do pacote, será adicionado cabeçalho de extensão, os pacotes por sua vez não são verificados por todos os roteadores intermediários. O Header Checksum, foi removido com a finalidade de melhorar a velocidade de processamento, já que não há a necessidade do pacote ser verificados por todos os roteadores. Existe um campo de Checksum na camada de transporte (UDP e TCP). O campo Tipo de Serviço foi substituído pelo campo Traffic

Class. O IPv6 tem um mecanismo diferente para lidar com preferências. O campo Flow Label (etiqueta de fluxo) foi adicionado, para realizar o tratamento dos pacotes.

Os campos do cabeçalho IPv6 são os seguintes: versão (IP versão 6), classe de tráfego (substitui o campo tipo de serviço do IPv4), etiqueta de fluxo (novo campo para a Qualidade de Serviço (QoS)), comprimento de carga (comprimento dos dados após a parte fixa do cabeçalho IPv6), o próximo cabeçalho (substitui o campo protocolo do IPv4), o limite de saltos (substitui o tempo de vida do IPv4), e endereços de origem e destino. O formato do cabeçalho IPv6 é ilustrado na Figura 4.

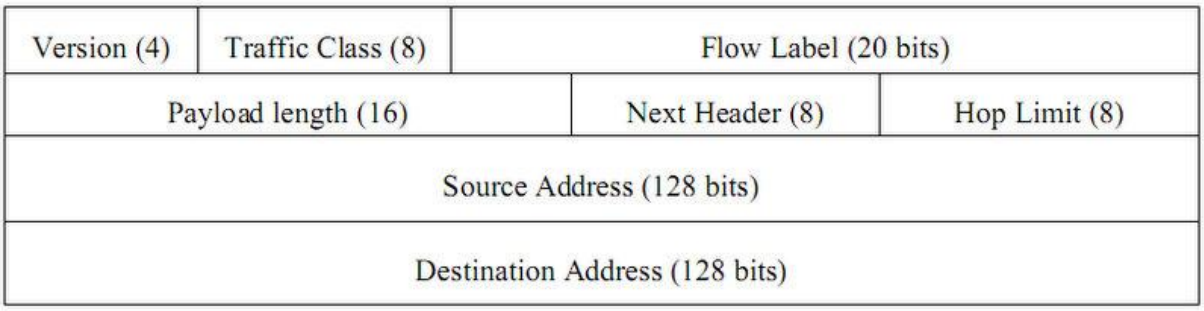

Figura 4 - formato do Cabeçalho IPv6

Fonte: (PEARCE et. al. 2010)

O tamanho do cabeçalho base pode ser de até 64KB, ou maior, quando utilizado a opção jumbo de carga.

2.4.1 Cabeçalho de extensão

Um cabeçalho IPv4 pode se estender de 20 bits a 60 bits, mas esta opção é raramente utilizada devido sua baixa performance de processamento e por gerar alguns problemas de segurança. A maneira utilizada pelo protocolo IPv6 para o tratamento dos campos opcionais do cabeçalho foi utilizar os cabeçalhos de extensão.

De acordo com URTADO (2008), um datagrama IPv6, além de seu cabeçalho Base, pode possuir um cabeçalho de extensão. Não existe um número fixo de cabeçalhos de extensão que um datagrama IPv6 pode possuir. Diferentemente do cabeçalho base, os de extensão não tem tamanho fixo, podendo variar de acordo com o tipo de cabeçalho de extensão, por este motivo os cabeçalhos de extensão possuem um campo chamado EXTENSION HEADER LENGTH, usado para indicar seu tamanho. A sequência dos cabeçalhos de extensão é definida pelo campo Next header.

A RFC 2460 define seis cabeçalhos de extensão: hop-by-hop option header, utilizado para transportar uma informação opcional que deve ser processada por todos os nós no caminho do pacote. Quando presente este cabeçalho deverá vir sempre após o cabeçalho base. Routing header, utilizado pela origem para listar um ou mais nós intermediários que devem ser visitados até o pacote chegar ao destino muito utilizado quando possui mais de uma opção de caminho. Fragment header, utilizado quando o pacote a ser enviado é maior que o MTU do caminho até o destino. O pacote é fragmentado na origem, pois diferentemente do IPv4, nessa versão os roteadores não suportam fragmentação. Destination options header, utilizado para transportar informação opcional ou adicional que deve ser analisada somente pelo destino do pacote. Authentication header (AH) e encapsulating security payload (ESP) header, utilizado pelo serviço IPSec (IP Security Protocol) para prover autenticação e garantia de integridade aos pacotes IPv6, esse cabeçalho é idêntico ao utilizado no cabeçalho IPv4.

2.5 AUTO-CONFIGURAÇÃO

O novo protocolo conta com a possibilidade de auto-configuração dos endereços, criando assim endereços link-local para cada uma das interfaces do cliente, possibilitando a comunicação com os hosts vizinhos, isto é, hosts pertencentes ao mesmo segmento lógico sem a necessidade de se configurar manualmente os dispositivos.

Os mecanismos de auto-configuração existentes no protocolo IPv6 são o Stateful definido pela RFC 3315, conhecido como DHCP no protocolo IPv4, e o Stateless, definido pela RFC 2462. Com a presença de um servidor DHCP os roteadores enviam mensagens a rede que identificam a sub-rede associada ao segmento. Os hosts geram seus endereços baseados na combinação de seu endereço físico, juntamente com as mensagens recebidas do servidor. Para gerar os seus endereços o host utiliza uma combinação de informações tais como seu endereço MAC e as informações recebidas do servidor. Na ausência de um servidor é possível realizar a configuração automática onde os hosts geram apenas um endereço Link-local com o prefixo FE80, endereço este suficiente para a comunicação com os demais dispositivos do segmento.

Em uma rede pode ser utilizado os dois tipos de autoconfiguração ao mesmo tempo. Por exemplo, um host poderá utilizar Stateless para gerar o seu próprio endereço e em seguida através do Stateful requisitar o complemento do seu endereço, este tipo de endereçamento possui um tempo de "vida", após o tempo o endereço torna-se inválido.

2.5.1 Segurança IPsec

A arquitetura do protocolo IPSec é baseada nos primeiros protocolos de segurança IP que compreendiam IP seguro, autenticação e cifragem dos datagramas e foram publicados em 1995 nas RFC 1825 e RFC 1829. O IP Security é um conjunto de protocolos de segurança utilizado na comunicação do protocolo IP para autenticar o remetente e prover a integridade e a confiabilidade dos dados transmitidos.

O IPSec utiliza dois cabeçalhos de extensão, Authentication header (AH) e encapsulating security payload (ESP) header.

2.5.2 QoS

O protocolo IP, na sua maior parte, não há a distinção dos pacotes e nem a garantia de entrega dos mesmos. O protocolo TCP, acrescenta a confirmação de entregas, mas não controla determinados parâmetros essências como atraso e alocação de banda. Aplicações utilizadas nos dias de hoje necessitam que haja a distinção dos conteúdos para as diferentes classes de serviço, exemplo dados de multimídia.

Implementações IPv6 utilizam recursos compatíveis com o QoS para identificar e priorizar os pacotes quando a rede se encontra congestionada. No cabeçalho IPv6 existem dois campos destinados ao QoS, Classe de tráfego (Traffic Class) e etiqueta de fluxo (Flow Label), os novos campos permitem realizar a distinção dos pacotes nos diferenciados tipos de tráfegos. O campo Flow label é responsável por "etiquetar" ou priorizar determinados fluxo de pacotes como voz sobre IP (VoIP) ou videoconferência, ambos os serviços dependem do tempo de entrega. Os novos campos do cabeçalho definem como o trafego é gerenciado e identificado, permitindo assim que os roteadores realizem um gerenciamento especial para cada tipo de pacote. Com a identificação do trafego no cabeçalho é possível dar suporte a QoS mesmo quando os pacotes estiverem utilizando IPSec.

2.6 TRANSIÇÃO PARA IPV6

Embora todos os estudos já realizados confirmem que existe a necessidade de se obter mais endereços IP para que a Internet continue crescendo e que esse problema poderá ser facilmente resolvido com a adoção do IPv6, o ritmo de implantação da nova versão do protocolo IP não está ocorrendo da forma que foi prevista no início de seu desenvolvimento, que apontava o IPv6 como protocolo padrão da Internet aproximadamente treze anos após sua definição.

2.6.1 Técnicas de transição

O SIT (Simple Internet Transition Mechanisms) definido pela RFC (Request For Comments) 1933 é um conjunto de mecanismos criados para permitir a transição IPv4-IPv6. Os mecanismos introduzidos pelo SIT asseguram que hosts IPv6 possam interoperar com hosts IPv4 até o momento em que os endereços IPv4 se esgotem.

> Como o período de coexistência entre os dois protocolos podem durar indefinidamente, a implementação de métodos que possibilitem a interoperabilidade entre o IPv4 e o IPv6, poderá garantir uma migração segura para o novo protocolo, através da realização de testes que permitam conhecer as opções que estes mecanismos oferecem, além de evitar, no futuro, o surgimento de “ilhas” isoladas de comunicação.(SANTOS et al. 2010)

Os mecanismos de transição podem ser classificados nas seguintes categorias:

- Pilha Dupla: que provê o suporte a ambos os protocolos no mesmo dispositivo;
- Tunelamento: que permite o tráfego de pacotes IPv6 sobre estruturas de rede IPv4;
- Tradução: que permite a comunicação entre nós com suporte apenas a IPv6 com nós que suportam apenas IPv4.

Estas técnicas podem ser utilizadas em combinação, a migração para IPv6 pode ser realizada passo a passo, começando com apenas um único host ou sub-rede. Há a possibilidade de migrar a rede de uma empresa, ou parte da mesma, e quando o

provedor ISP utilize ainda o protocolo IPv4, ou o provedor já utilize o novo protocolo e a rede da empresa ainda utilize o protocolo IPv4.

Segundo PEARCE et al. (2010), um exemplo típico de transição entre os dois protocolos, ocorre quando uma organização que possui a sua rede em um ambiente IPv4 deseja realizar a migração de parte da mesma, formando assim ilhas com hosts IPv4 e hosts IPv6. Inicialmente a empresa poderá utilizar túneis IPv4 para conectar nas ilhas IPv6. A tradução e a pilha dupla permitiram que os hosts IPv6 utilizem recursos IPv4. Sempre que for possível, evitar a utilização de métodos de tradução, pois é um método muito complexo por envolver a tradução de inúmeros protocolos, possuindo assim muitas incompatibilidades.

No final da migração a maioria dos equipamentos da rede estarão utilizando o novo protocolo, existirão ilhas de IPv4 isoladas que ficaram com serviços legados, o trafego IPv4 ocorrerá sobre túneis IPv6 e o mecanismo de tradução permitirá que os hosts IPv6 acessem os serviços.

2.6.2 Implantação

Muitos fatores têm atrasado a implantação do novo protocolo, técnicas como o NAT e o DHCP que no inicio ajudou no desenvolvimento aumentando a vida útil do atual protocolo, agora estão colaborando para a demora da adoção. Aliado a isso há o fato de que o Protocolo IPv4 ainda não apresentou graves problemas de funcionamento.

> A utilização do IPv6 está ligada principalmente a área acadêmica, e para que a Internet passe a utilizar IPv6 em grande escala, é necessário que a infraestrutura dos principais ISPs seja capaz de transmitir tráfego IPv6 de forma nativa. No entanto, sua implantação em redes maiores tem encontrado dificuldades devido, entre outras coisas, ao receio de grandes mudanças na forma de se gerenciá-las, na existência de gastos devido a necessidade de troca de equipamentos como roteadores e switches, e gastos com o aprendizado e treinamento para a área técnica. (SANTOS et al. 2010, p.29)

Várias redes IPv6 de grande porte estão atualmente em operação, a mais conhecida é a “6bone” que esta operando desde 1996, a rede é utilizada para interligar laboratórios de IPv6 da França, Dinamarca e Japão, é uma rede IPv4 que foi sobreposta através da utilização de túneis.

Vários países demonstraram interesse na adoção do novo protocolo, principalmente os que possuem uma alta densidade populacional e um alto desenvolvimento tecnológico.

O principal obstáculo para a implantação do novo protocolo é a migração da grande base das redes que estão em IPv4, por esse motivo o IPv6 deverá implementado gradativamente, de modo que ambas as versões do IP poderão coexistir por alguns anos, até que o período de transição seja completado e todos os hosts do planeta sejam IPv6.

Os mecanismos de transição possuem um conjunto de ferramentas que devem ser aplicados em hosts e/ou em roteadores onde o seu principal objetivo é minimizar os impactos causados nesta transição de protocolos.

> Os mecanismos de transição asseguram que dispositivos rodando IPv6 ou IPv4, ou com ambos, possam colaborar mutuamente, permitindo que tanto ambientes que tenham os protocolos de mesma versão, quanto os que possuam versões distintas, possam interoperar durante a fase de transição. Esta característica protege os investimentos realizados em tecnologia IPv4 e garante que o mesmo não ficará obsoleto, até a migração de todas as máquinas que compõem a Internet.(FERREIRA et al. 2010).

2.7 PILHA DUPLA

Na fase inicial de implementação do novo protocolo é recomendado que os nós possuíssem suporte as duas versões dos protocolos IP, pois muitos serviços e dispositivos de rede ainda trabalham somente sobre IPv4. Deste modo, uma possibilidade é a de se introduzir o método conhecido como pilha dupla (Dual-Stack). Este método permite que hosts e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois pacotes, IPv4 e IPv6.

> Este método de transição pode facilitar o gerenciamento da implantação do IPv6, por permitir que este seja feito de forma gradual, configurando pequenas seções do ambiente de rede de cada vez. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 de cada nó. (SANTOS et. al. 2010)

O método de pilha dupla deve ser implantado em todos os roteadores da rede, deverão ser atribuídos os dois tipos de endereços paralelamente, pois não há

comunicação entre os dois protocolos IPv4 e IPv6. O uso desse método requer que todos os recursos de rede tenham capacidade de memória e processamento suficientes para suportar as duas pilhas de endereçamento IP, pois exige um gerenciamento duplo.

A finalidade deste método de transição é diminuir o número de túneis utilizado durante o processo de transição, as organizações utilizam o método de pilha dupla quando a maioria dos seus equipamentos são capazes de realizar a implementação de pilha dupla e quando desejam que a transição ocorra rapidamente.

Este tipo de implementação requer a configuração do Switch para ativar ou desativar uma das pilhas, por esse motivo esse método possui três tipos operação:

Quando a pilha IPv4 é habilitada, a pilha IPv6 é desabilitada, o nó se comporta como IPv4. Quando a pilha IPv6 é ativada, a pilha IPv4 é desativada, comportando-se como um nó IPv6. Quando os dois protocolos estão habilitados, o nó pode usar os dois protocolos. Um nó IPv6/IPv4 tem pelo menos um endereço para cada versão do protocolo, ele utiliza mecanismos de IPv4 para configurar um endereço IPv4 (configuração estática ou DHCP) e utiliza mecanismos de IPv6 para configurar endereço IPv6 (autoconfiguração ou DHCPv6).

O DNS é utilizado com as duas versões do protocolo para resolver nomes e endereços IP. Em um nó IPv6/IPv4 precisa de um servidor DNS capaz de resolver ambos os tipos de registros de endereços.

O método de pilha dupla como os demais métodos de transição possui algumas vulnerabilidades que necessitam ser tratadas em ambos os protocolos. A RFC 4942 apresenta os riscos que os dispositivos que operam nos sistemas estão sujeitos. Para que não aconteçam problemas durante a migração as empresas deverão implantar uma política e segurança consistente tanto para IPv4 quanto para IPv6, incluindo a instalação de firewalls e filtros de pacotes. A empresa, o administrador de rede, deverá estar ciente de todas as novas funcionalidades incluídas neste novo protocolo, como por exemplo, a mobilidade a configuração automática dos endereços sem a necessidade de servidor DHCP, descoberta de outros hosts vizinhos, endereços de privacidade e ao final a utilização do IPsec, este protocolo por sua vez será o responsável por encriptar todos os dados do pacote

Como ambos os protocolos estão sendo utilizados, acessos inesperados e não autorizados podem ocorrer entre os hosts, violando assim as políticas de segurança. Por esse motivo as empresas deverão atualizar os seus sistemas de detecção de intrusão (firewalls), além de manter constantes monitoramentos.

O IPv6 permite a autoconfiguração dinâmica, este termo implica que um host é capaz de estabelecer um endereço sem a presença de um servidor estático, o único requisito é um roteador devidamente configurado, mas nenhum servidor é necessário na conexão.

A configuração automática e renumeração do IPv6 são definidos no RFC 2462. A palavra "apátridas" é derivada do fato de que este método não requer o acolhimento de estar ciente de seu estado atual, de modo a ser atribuído um endereço IP pelo servidor DHCP. O processo de configuração automática sem estado compreende as seguintes etapas realizadas por um dispositivo de rede:

- Link-Local Geração Endereço - O dispositivo é atribuído um endereço link-local. É composto de '1111111010 'como os primeiros dez bits seguidos por 54 zeros e um identificador de interface 64 bit.

- Link-Local de teste único Endereço - Nesta etapa, o dispositivo em rede garante que o endereço link-local gerado por ele não é já utilizado por qualquer outro dispositivo, ou seja, o endereço é testado para sua singularidade.

- Link-Local de Atribuição de endereços - Uma vez que o teste de singularidade é limpo, a interface IP é atribuído o endereço do link local. O endereço se torna utilizável na rede local, mas não através da Internet.

- Contato Router - O dispositivo de rede faz o contato com um roteador local para determinar o seu próximo curso de ação no processo de configuração automática.

- Direção Router - O nó recebe instruções específicas do roteador em seu próximo curso de ação no processo de configuração automática.

- Configuração de Endereços Global - O host configura-se com o seu endereço de Internet exclusivo. O endereço é composto por um prefixo de rede fornecido pelo roteador junto com o identificador do dispositivo.

3 TUNELAMENTO

A técnica de criação de túneis, ou tunelamento, permite transmitir pacotes IPv6 através da infraestrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4, conforme ilustrado na figura 6 . Por exemplo, se um provedor tem ainda um Infraestrutura IPv4, a técnica de tunelamento permite que você tenha uma rede IPv6 corporativa e se comunique com outros hosts IPv6 através de um túnel sobre a rede IPv4 .

A figura 5 apresenta a seguinte infraestrutura. Os Routes A e C estão conectados por uma rede IPv6 assim como os Routes B e D. Porem o link entre Router A e B é realizada por um enlace IPv4. Nesta topologia faz-se necessário a implementação de um túnel para trafegar os dados IPv6.

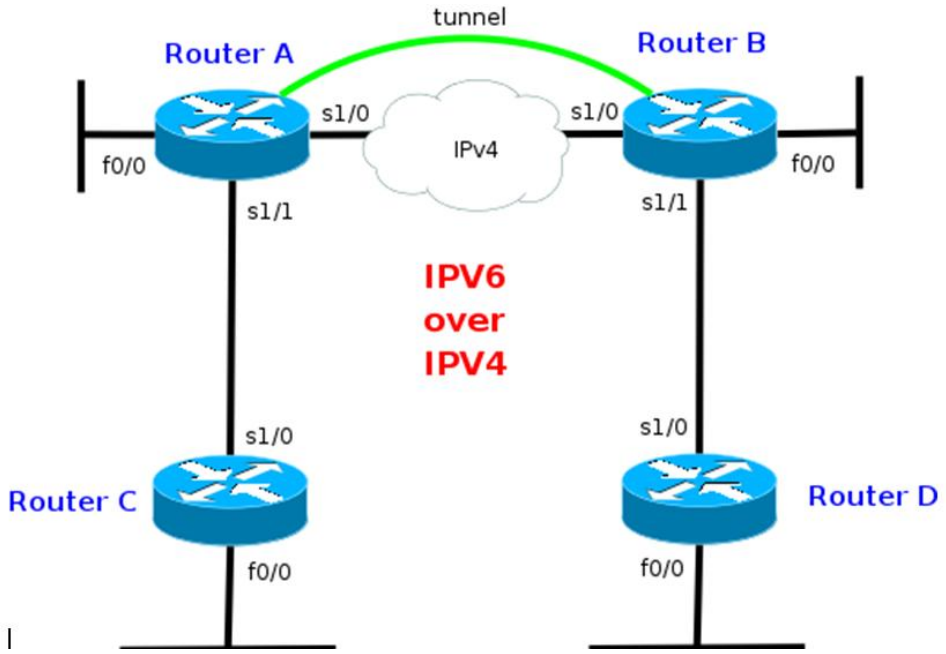

Figura 5 - Topologia do estudo com aplicação do túnel 6to4

A seguir observam-se os script´s resumidos da configuração global apresentada na figura 6 e 7, exportada através do comando running-config.

```
RA
!
 interface Tunnel0
  no ip address
  IPv6 address 3333::1/16
  IPv6 enable
  IPv6 rip utfpr enable
  tunnel source Serial1/0
  tunnel destination 192.168.1.2
  tunnel mode ipv6ip
  !
  !
 interface Serial1/0
  ip address 192.168.1.1 255.255.255.252
  serial restart-delay 0
  !
 interface Serial1/1
  no ip address
  IPv6 address AC:AC::A/32
  IPv6 enable
  IPv6 rip utfpr enable
  serial restart-delay 0
```

Figura 6- script de configuração RA.

```
RB
 interface Tunnel0
  no ip address
  IPv6 address 3333::2/16
  IPv6 enable
  IPv6 rip utfpr enable
  tunnel source Serial1/0
  tunnel destination 192.168.1.1
  tunnel mode ipv6ip
  !
 interface Serial1/0
  ip address 192.168.1.2
255.255.255.252
  serial restart-delay 0
  !
 interface Serial1/1
  no ip address
  IPv6 address BD:BD::B/32
  IPv6 enable
  IPv6 rip utfpr enable
  serial restart-delay 0
```

```
RC
!
interface Serial1/0
 no ip address
 IPv6 address AC:AC::C/32
 IPv6 enable
 IPv6 rip utfpr enable
 serial restart-delay 0
```

```
RD
!
interface Serial1/0
 no ip address
 IPv6 address BD:BD::D/32
 IPv6 enable
 IPv6 rip utfpr enable
 serial restart-delay 0
```

Figure 7- Script de configuração, RB, RC, RD.

As técnicas de tunelamento e encapsulamento de pacotes IPv6 em pacotes IPv4 são definidas por diversas RFCs, como na RFC 4213, têm sido as mais utilizadas na fase inicial de implantação do IPv6, por serem facilmente aplicadas em teste, onde há redes não estruturadas para oferecer tráfego IPv6 nativo. Varias formas de layouts de túneis podem ser implementadas, entre elas podemos destacar:

Host-a-Host, permite que os host dual-stack conversem entre si em uma rede IPv4, utilizando pacotes IPv6 encapsulados em pacotes IPv4, utilizam uma comunicação direta do tipo P2P e é muito utilizada na maioria dos tipos de tunelamentos, conforme ilustrado na figura 8.

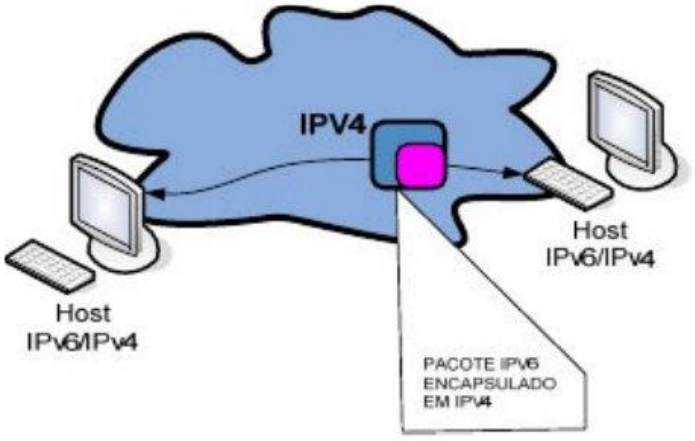

Figura 8 - Host-a-Host

Fonte: GOMES (2009)

Host-a-Roteador, hosts IPv6/IPv4 enviam pacotes IPv6 a um roteador IPv6/IPv4 intermediário utilizando uma rede IPv4. Esse método permite que seja realizada a ligação do primeiro segmento da rede que está localizado entre os dois hosts, permitindo assim que ocorra a comunicação entre os dois hosts IPv6. A figura 9 exemplifica o modelo Host-a-Roteador.

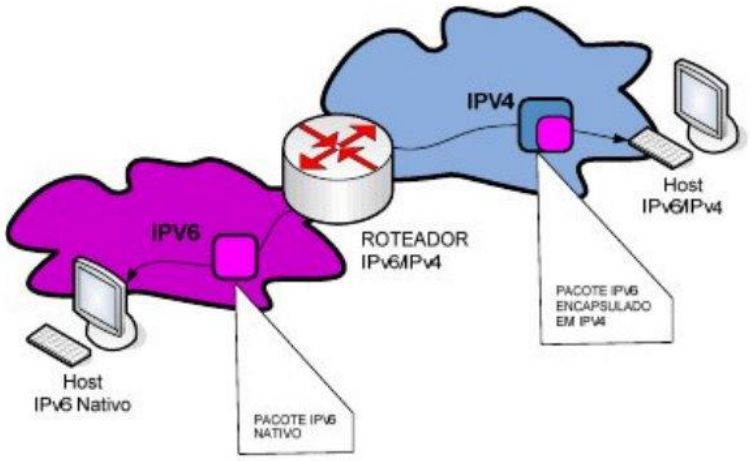

Figura 9- Host-a-Roteador

Fonte: GOMES (2009)

Roteador-a-Roteador, definidos com gateways dual-stack IPv6/IPv4, possuem uma conexão IPv4 entre si e são configurados para realizar a troca de pacotes IPv6 de redes IPv6 através de uma rede IPv4, permitindo assim a comunicação entre os dois segmentos IPv6, conforme ilustra a figura 10.

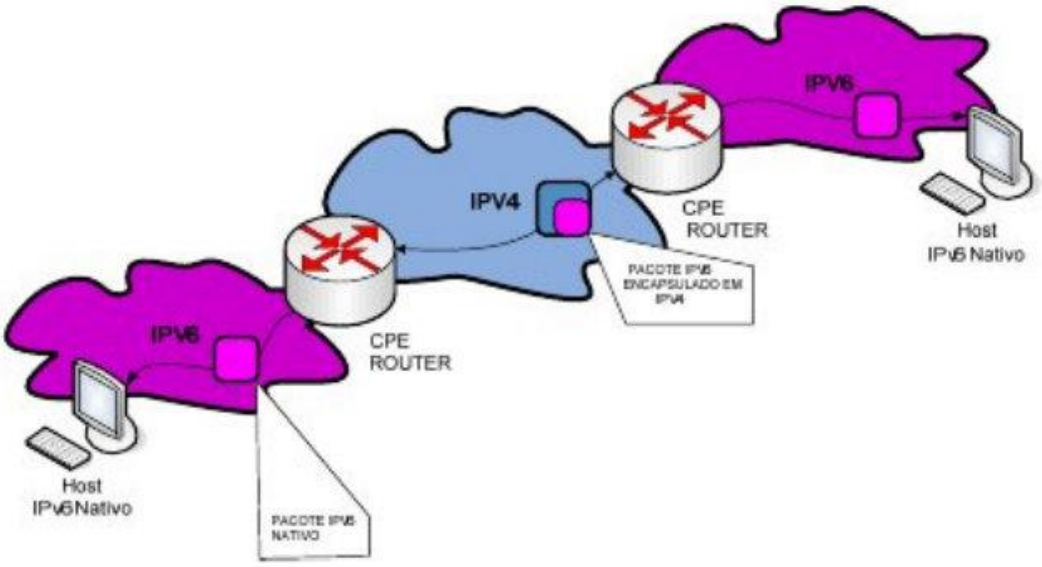

Figura 10 - Roteador-a- Roteador

Fonte: GOMES (2009)

As principais técnicas de tunelamento são os pacotes IPv6 encasulado em pacotes IPv4 (Protocolo 41, 6to4, ISATAP e Tunnel Brokers), pacotes IPv6 encapsulado em pacotes GRE (Protocolo GRE) e pacotes IPv6 encapsulados em pacotes UDP (TEREDO.)

Os túneis podem ser configurados manualmente utilizando os mecanismos genéricos de encapsulamento ou ainda utilizar mecanismos de criação semi-automáticas de túneis. Os túneis criados manualmente necessitam de configuração de endereço de origem e destino do túnel enquanto os criados automaticamente somente necessitam apenas ser ativados e os seus respectivos protocolos se encarregam da criação e manutenção dos túneis.

3.1.1 Tunnel Isatap

Este mecanismo de transição é projetado para fornecer a conectividade IPv6 entre nós IPv6 dentro de uma rede baseada no protocolo IPv4 que não tenha um roteador IPv6. Definida pela RFC 5214 é baseada em túneis IPv6 criados automaticamente dentro de uma rede IPv4, permitindo assim implantar IPv6 na sua rede corporativa, por trás do firewall, mesmo se você não tem um roteador IPv6.

O tipo de tunelamento ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) ainda permite que você utilize um mecanismo de tunelamento automático se você estiver usando endereços IPV4 privados e NAT. Endereços IPV4 e os prefixos definidos no roteador ISTAP são utilizados em clientes e roteadores como parte dos endereços, permitindo assim que um nó identifique facilmente os pontos de entrada e saída de um túnel IPV6, sem utilizar nenhum protocolo ou recurso auxiliar. A comunicação entre clientes de uma rede ISATAP é realizada diretamente, após a autoconfiguração não há a necessidade de se utilizar o roteador ISATAP. O trafego da rede sempre será o IPV4, os pacotes IPV6 serão encapsulados e desencapsulados localmente nos clientes.

Um exemplo de endereço ISATAP de um endereço IPV4 público 200.134.81.51 seria 2001:10fe:0:8003:134:5efe:200.134.81.51. Na composição do novo endereço o prefixo da rede 2001:10fe:0:8003 mais o 134 , ID IPV4 publico , mais o prefixo ISATAP :5efe são adicionados ao endereço IPV4 para a composição do endereço ISATAP.

3.1.2 Tunnel Broker

Segundo SANTOS (et al. 2010, p.181), descrita na RFC 3053, essa técnica permite que hosts IPV6/IPV4 isolados em uma rede IPV4 acessem redes IPV6. Seu

funcionamento é bastante simples, primeiramente é necessário cadastrar-se em um provedor de acesso Tunnel Broker e realizar o download de um software ou script de configuração. A conexão do túnel é estabelecida através da solicitação do serviço ao Servidor Web do provedor, que após autenticação, verifica qual tipo de conexão o cliente está utilizado (IPV4 público ou NAT) e lhe atribui um endereço IPV6. A partir desse ponto, o cliente pode acessar qualquer host na Internet.

3.1.3 Tunelamento 6to4

Definido pela RFC 3056, a "Conexão de domínios IPv6 via IPv4 Nuvens", especifica um mecanismo que permite endereços IPv6 locais se comunicarem outros endereços IPv6 através de uma rede IPv4 sem uma configuração de um túnel. A rede implementada sobre o protocolo IPv4 é tratada como uma camada de ligação ponto-a-ponto unicast, e os domínios com endereços nativos IPv6 irão se comunicar com os demais endereços do mesmo protocolo através de roteadores 6to4, também conhecido como 6to4 gateways. Estes roteadores apenas serão utilizados durante o período de coexistência dos dois protocolos, não devem ser utilizados como uma solução permanente.

O protocolo associa dois endereços IPv6 por interface, um endereço unicast e um endereço link-local. O host utiliza um prefixo IPv6 de 64 bits para o seu endereço unicast e define a identificação da interface nos 32 bits restantes. Exemplo FE80::A.B.C.D em cada interface 6over4.

> Os endereços IPv6 são formados através de um prefixo “2002::/10”, reservados pela IANA, que será utilizado único e exclusivamente para endereços 6to4, e seguido do endereço IPv4 convertido em hexadecimal como no exemplo 2002:aabb:ccdd::/48, onde aabb:ccdd é o endereço IPv5 público do cliente já convertido para o formato hexadecimal de dois dígitos. (GOMES et. al 2009).

Segundo PERACE (2010), por utilizar endereços e serviços do protocolo IPv4, é recomendável que se aplique um controle de segurança, pois utilizando o protocolo 6over4, o usuário estará sujeito a ataques IPv6 e ataques IPv4. As questões de segurança para o protocolo 6over4 incluem a aplicação de regras nos roteadores de borda, onde deverá ser analisado o tráfego de entrada e saída de pacotes Unicast IPv4 quando o

protocolo for do tipo 41 e suas fontes forem desconhecidas. Os roteadores de borda somente deverão aceitar conexão de túneis IPv6-IPv4 de fontes confiáveis.

Na topologia da figura 5 a implementação foi realizada utilizando o tunnel 6over4. A figura 11 ilustra que o tunnel está operacional.

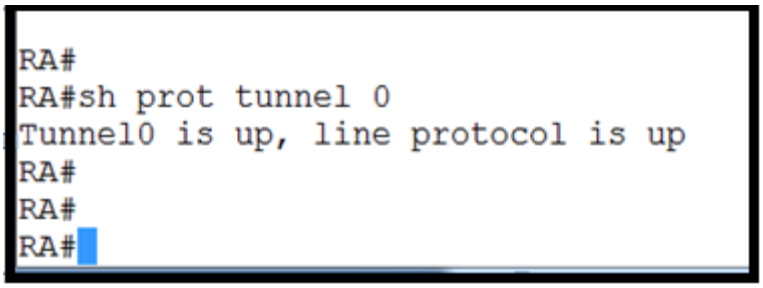

Figura 11 - Roteador A Tunnel Up

A configuração do tunnel para o Router A está ilustrada na figura 12. Onde observa-se a implementação do mode IPv6ip.

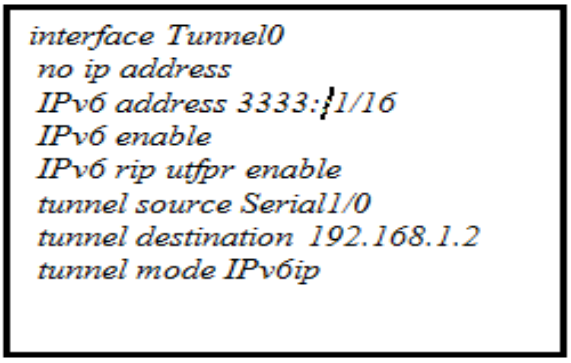

Figura 12 - Configuração do Tunnel 0 em Router A

Através da figura 13 é possível identificar o sucesso do protocolo ICMP disparando contra o IPv6 BD:BD::D, sendo esta o IPv6 configurado no Router D.

Este resultado exibe e confirma que o tunelamento IPv6ip é completamente funcional para o qual se propõe.

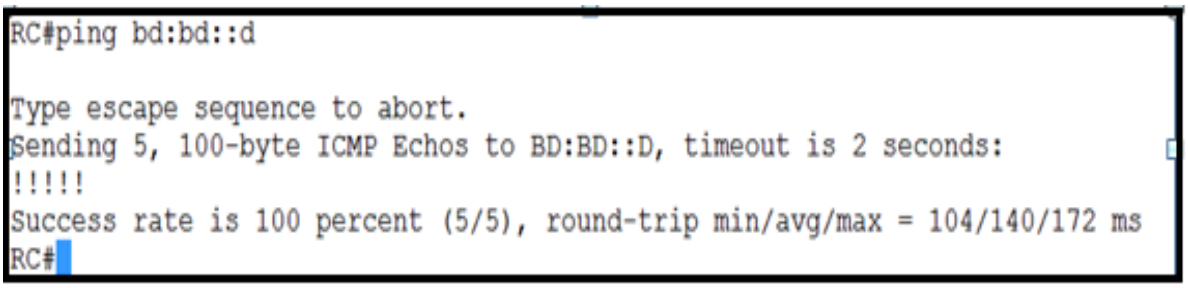

Figura 13 - Teste de conectividade entre Router C e Router D

3.1.4 Tunnel Teredo

Tecnologia criada para suprir as deficiências deixadas pelo tunelamento 6to4 e Túnel Broker, esta tecnologia de tunelamento funciona através do protocolo UDP e permite que o seu funcionamento através do NAT e sem autenticação. Esta técnica de tunelamento não é considerada eficiente, pois a sua complexibilidade exige muito processamento, mas é uma das únicas formas de conexão para clientes que estão atrás de NAT e desejam se conectar a Internet utilizando o protocolo IPV6. O Túnel Teredo não funciona através do NAT simétrico e apesar de sua complexidade tem uma grande importância na migração IPV4/IPV6 doméstica.

3.1.5 Tunnel GRE

O GRE (Generic Routing Encapsulation) é um túnel estático entre dois hosts originalmente desenvolvido pela Cisco com a finalidade de encapsular vários tipos diferentes de protocolos, como por exemplo IPV6 e IS-IS.

Segundo (SANTOS et al. 2010, p.202), este tipo de encapsulamento é suportado na maioria do sistemas operacionais e roteadores e consiste em um link ponto a ponto. A principal desvantagem do túnel GRE é a configuração manual, que de acordo com a quantidade de túneis, gerará um grande esforço na sua manutenção e gerenciamento. O funcionamento deste tipo de túnel é muito simples, e consiste em pegar os pacotes originas, adicionar o cabeçalho GRE, e enviar ao IP de destino (o endereço do destino é especificado no cabeçalho GRE), quando o pacote encapsulado chega à outra ponta do túnel (IP de destino) é removido dele o cabeçalho GRE, sobrando apenas o pacote original, o qual é encaminhado normalmente ao destinatário.

A configuração dos túneis GRE é muito semelhante àquela feita para o 6over4. Conforme ilustra a figura 14. Em seguida pode-se verificar configuração nos script´s ilutrados nas figuras 15 e 16, substituindo o comando tunnel mode ipv6ip por tunnel mode gre.

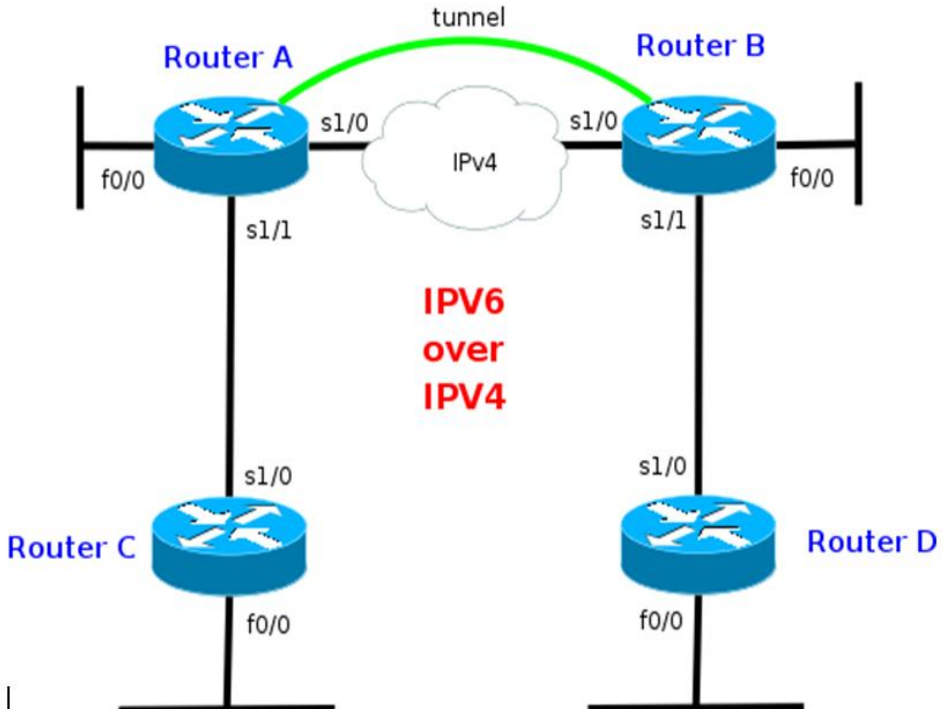

Figura 14 - Topologia do estudo com aplicação do túnel GRE

```
RA
!
 interface Tunnel0
  no ip address
  IPv6 address 3333::1/16
  IPv6 enable
  IPv6 rip utfpr enable
  tunnel source Serial1/0
  tunnel destination 192.168.1.2
  tunnel mode gre
 !
 !
 interface Serial1/0
  ip address 192.168.1.1 255.255.255.252
  serial restart-delay 0
 !
 interface Serial1/1
  no ip address
  IPv6 address AC:AC::A/32
  IPv6 enable
  IPv6 rip utfpr enable
  serial restart-delay 0
```

Figura 15 - script do Roteador A

```
RB
 interface Tunnel0
  no ip address
  IPv6 address 3333::2/16
  IPv6 enable
  IPv6 rip utfpr enable
  tunnel source Serial1/0
  tunnel destination 192.168.1.1
  tunnel mode gre
 !
 interface Serial1/0
  ip address 192.168.1.2
255.255.255.252
  serial restart-delay 0
 !
 interface Serial1/1
  no ip address
  IPv6 address BD:BD::B/32
  IPv6 enable
  IPv6 rip utfpr enable
  serial restart-delay 0
```

```
RC
!
interface Serial1/0
 no ip address
 IPv6 address AC:AC::C/32
 IPv6 enable
 IPv6 rip utfpr enable
 serial restart-delay 0
```

```
RD
!
interface Serial1/0
 no ip address
 IPv6 address BD:BD::D/32
 IPv6 enable
 IPv6 rip utfpr enable
 serial restart-delay 0
```

Figura 16 - Script do roteador B, C e D

4 CONCLUSÕES

Devido o crescimento exponencial da Internet e o surgimento de novas aplicações, o uso do protocolo IPv6 torna-se indispensável, uma vez que o protocolo IPv4 passou a apresentar limitações.

As companhias começaram a preparar para a implantação do novo protocolo, criando uma estratégia eficaz de migração. Embora o protocolo IPv6 ainda não esteja sendo usado em grande escala, a transição para o mesmo é inevitável. Certamente grande parte das organizações operem em dual-stack para que acomode os dois protocolos IPv4 e IPv6.

As conclusões submetem para a importância do protocolo IPv6, apresentando as suas principais características e alterações em comparação com o protocolo IP juntamente com seus mecanismos de transição. A transição para o novo protocolo se faz necessária devido o protocolo atual não suportar mais o crescimento das grandes redes, pois somente o IPv6 permitirá o crescimento permitirá o crescimento continuo da rede.

Os testes realizados trazem que o protocolo GRE RFC (2784) apresentou-se bastante estável e de fácil configuração com facilidade de encapsular vários tipos diferentes de protocolos de roteamento, sendo suportado na maioria dos IOS e possibilita links ponto a ponto e multiponto

O 6to4 (RFC 3056) é umas das técnicas de transição mais antigas em uso, é a técnica que inspirou a criação do 6rd. Sua concepção foi simples e muito interessante: com ajuda de relays pilha dupla distribuídos na Internet, abertos, instalado de forma colaborativa por diversas redes, qualquer rede IPv4 poderia obter conectividade IPv6, através de túneis 6in4 automáticos. Por meio do 6to4 qualquer computador com um IPv4 válido pode funcionar como uma extremidade de um conjunto de túneis automáticos e prover todo um bloco IPv6 /48 para ser distribuído e usado em uma rede. Sua configuração é muito simples porem exige um experiência e conhecimento avançado de configuração de roteadores. Outro fato dos sistemas operacionais ativarem os túneis 6to4 sem intervenção ou conhecimento dos usuários traz algumas consequências sérias. Uma delas é que firewalls ou outras medidas de segurança em redes corporativas podem ser inadvertidamente contornados.

O 6to4 é, então, um protocolo com histórico importante, mas cujo uso deve ser evitado atualmente. Deve-se desativá-lo em redes corporativas e bloqueá-lo nos firewalls. Contudo, para redes pilha dupla que têm serviços IPv6 públicos na Internet, principalmente servidores

Web, é recomendada a instalação de um relay 6to4 para responder a solicitações de usuários externos usando essa tecnologia, mitigando parte dos problemas trazidos pela mesma.

5 REFERÊNCIAS BIBLIOGRÁFICAS

BARATA, Bruno. IPv6-NAT-PT. CCIE SERVICE PROVIDER, Rio de Janeiro, Jun. 2010. Disponível em: < http://babarata.blogspot.com/2010/06/IPv6-nat-pt.html>Acesso em 15 de fevereiro de 2013;

COMER, D; **"**Redes de Computadores e Internet. Abrange Transmissão de Dados, Ligações Inter-redes e Web"; 2ª Edição; Editora Campus, 2003.

FILIPPETTI, Marco Aurélio. CCNA 4.1 Guia de estudos completo. 1ª ED – Visual Books.(Capitulo 5 – TCP/IP).

FERREIRA D.O., SILVA E., BRITO R., MOREIRA S.R. **IPv6**, Brasília, UNIVERSIDADE CATÓLICA DE BRASÍLIA, 2010. Disponível em: <http://www.ucb.br/prg/professores/maurot/ra/RA_arqs/conteudo_web/IPv6/index.html > . Acesso em 22 de fevereiro de 2013;

FILIPPETTI, Marco. IPv6 para o CCNA**.** São Paulo: Blog CCNA, 2011. Vídeo Aula de (28 Min.). Disponível em< ttp://www.ccna.com.br/VA/VA_IPv6/player.html>. Acesso em 09 março. 2013.

FRAZÃO, A; "Novidades IPv6". NewsGeneration 30 de junho de 1997. Disponível no site http://www.rnp.br/newsgen/ascii/n2.txt; Acesso em 12 de fevereiro de 2013;

GOMES, Alexandre José Camilo; TRINDADE, Carlos Botelho da. Melhores práticas de migração de uma rede IPv4/IPv6. 2009. 168 f. Trabalho de Graduação de Curso – Engenharia Elétrica com ênfase em telecomunicações. Instituto de Educação Superior de Brasília, Brasília, 2009.

HAGEN, Silvia. IPv6 Essentials**.** O'Reilly Media, Sebastopol-USA, Julh. 2002.

MOREIRAS, Antonio.M. Entenda o esgotamento do IPv4. **IPV6.br**, Rio de Janeiro, Mar. 2009. Disponível em: < http://www.IPv6.br/IPV6/ArtigoEsgotamentoIPv4> . Acesso em 09 de março de 2013.

MORIMOTO, Carlos E.. IPV4 – Definição de IPV4. Disponível em: <http://www.hardware.com.br/termos/IPv4>. Acesso em 03 de fevereiro de 2012.

MURPHY, Niall Richard. IPv6 Network Administration. 1ª ED - Oreilly & Assoc.(Capitulo 6 - Operations).

NED, F**.** A Nova Geração de Protocolos IP. Rio de Janeiro, Rede Nacional de Ensino e Pesquisa (RNP), Nov. 1998. Disponível em: < Http://www.rnp.br/newsgen/9811/intr-IPv6.html > Acesso em 09 de março de 2013.

NED, F; "A Nova Geração de Protocolos IP"; NewsGenaration, vol.2 no.8, 1998; Disponível em <http://www.rnp.br/newsgen/9811/intr-IPv6.html>Acesso em 12 de fevereiro de 2013;

PEARCE, John; ROOKS,Mark; GRAVEMAN, Richard; FRANKEL, Sheila. Guidelines for the Secure Deployment of IPv6**.** Gaithersburg. 2010.

RFC 791: Internet Protocol Darpa Internet Program Protocol Specification Set 1981. Disponivel em: < www.ietf.org/rfc/rfc791.txt>. Acesso em 09 de março de 2013.

RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. Network Working Group, Dez. 1998. Disponível em: < http://www.ietf.org/rfc/rfc2460.txt >. Acesso em 09 de março de 2013.

RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers. Network Working Group, Out. 2005. Disponível em: < http://www.ietf.org/rfc/rfc4213.txt > . Acesso em 09 de março de 2013.

SANTOS, Rodrigo Regis dos; MOREIRAS, Antônio M.;REIS Eduardo Ascenço; ROCHA, Ailton Soares CURSO IPV6 BÁSICO**.** São Paulo.2010.

SILVA, Sérgio Carneiro da. O Protocolo IPv6 e sua Transição. 2005. 59 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior Sistemas de Informação. Faculdade De Ciências Aplicadas De Minas, Uberlândia, 2005.

URTADO, Alexandre, ALVES Nilto Jr. Implementação do protocolo IPv6 na RedeRio. IPV6.br, Rio de Janeiro, Out. 2008. Disponível em: <http://www.IPv6.br/IPV6/ArtigoImplementacaoRedeRioParte03>Acesso em 10 de março de 2013.

IPv4 address exhaustion jan, 2013. Disponível em: <http://en.wikipedia.org/wiki/File:Ipv4-exhaust.svg>. Acesso em 29 de março de 2013.