UNIVERSIDADE ESTADUAL DE LONDRINA

Fábio Engel de Camargo

Transição do IPv4 para o IPv6

LONDRINA - PARANÁ
2010

UNIVERSIDADE ESTADUAL DE LONDRINA

Fábio Engel de Camargo

Transição do IPv4 para o IPv6

Trabalho de Conclusão de Curso apresentado ao Curso de Ciência da Computação, Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Dr. Mario Lemes Proença Jr.

LONDRINA - PARANÁ

2010

Camargo, Fábio Engel

Transição do IPv4 para o IPv6 / Camargo, Fábio Engel. -- Londrina: UEL / Universidade Estadual de Londrina, 45 f. 2010.

Orientador: Mario Lemes Proença Jr.

Monografia (Graduação) – UEL / Universidade Estadual de Londrina, 2010.

Referências bibliográfica: f.58-60

1. IPv6. 2. Técnicas de Transição IPv6. 3. IP.

Fábio Engel de Camargo

Transição do IPv4 para o IPv6

Esta monografia foi julgada adequada para obtenção do título de Bacharel em Ciência da Computação, e aprovada em sua forma final pela Coordenação do Curso de Ciência da Computação, do Departamento de Computação da Universidade Estadual de Londrina.

Banca Examinadora:

_____

Prof. Dr. Mario Lemes Proença Jr. - Orientador
Universidade Estadual de Londrina

_____

Prof. Dr. Rodolfo Miranda de Barros
Universidade Estadual de Londrina

_____

Prof. Msc. Elieser Botelho Manhas Jr.
Universidade Estadual de Londrina

Londrina, 29 de novembro de 2010

Dedico este trabalho à minha família, principalmente a meus pais, Valdemir e Célia, por todo apoio, dedicação, carinho e compreensão em todos os momentos da minha vida.

À minha namorada Bruna, por seu companheirismo, paciência e auxílio durante as revisões deste trabalho.

A meu primo Marcio, que considero um irmão, que muito contribuiu para que eu conquistasse este objetivo de me formar em Ciência da Computação.

AGRADECIMENTOS

Agradeço à Universidade Estadual de Londrina por permitir que eu me qualificasse em uma importante instituição pública de ensino.

Agradeço ao prof. Dr. Mario Lemes Proença Jr. por aceitar me orientar durante a graduação.

Agradeço aos docentes do Departamento de Computação pelo incentivo e ensino prestados durante minha formação.

Por fim, agradeço aos meus colegas de curso, especialmente ao Álvaro, Gilson, Humberto, José André e Sérgio, pelas incontáveis histórias e recordações destes quatro anos de curso.

RESUMO

O *Internet Protocol Version 6* (IPv6) foi desenvolvido durante a década de 90, em resposta as previsões do imediato esgotamento dos endereços IP, necessários para identificação dos diversos dispositivos que compõe a Internet, que comprometeu o ritmo de crescimento ao impossibilitar a adesão de novos aparelhos à grande rede. A substituição da antiga versão do protocolo pelo IPv6 ocorre de forma gradual, sendo que por um período indeterminado de tempo as duas versões coexistirão. Este trabalho apresenta os aspectos referentes à implantação IPv6, principalmente por meio das técnicas que garantem esta interoperabilidade, essenciais durante todo o período de transição. O trabalho também abrange as características que formam o novo protocolo além de fornecer uma visão sobre o atual estágio de implantação em diversos cenários por meio de uma pesquisa de campo.

Palavras-chave: IPv6; Técnicas de Transição IPv6; IP.

ABSTRACT

The Internet Protocol Version 6 (IPv6) was developed in the 90', in response to predictions of immediate exhaustion of IP addresses, it necessaty to identify many devices that comprise the Internet, thus compromised its pace of growth by impeding the entry of new devices in the net. The replacement of the old version to IPv6 occurs gradually, for an indefinite period of time the two versions will coexist. This work presents aspects related to IPv6 deployment primarily by the techniques that ensure such interoperability, essential during the transition period. The work also covers the features that make the new protocol, besides it provids an insight into the current stage of deployment in various scenarios through a survey.

Key-words: IPv6, IPv6 Transition Technologies; IP.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

AH - *Authentication Header*
ALG - *Application Level Gateway*
AS - *Autonomous System*
BGP4 - *Border Gateway Protocol version* 4
BIA - *Bump-in-the-*API
BIS - *Bump in the Stack*
CGI.BR - Comitê gestor da Internet no Brasil
CIDR - *Classless Inter Domain Routing*
DDoS - *Distributed Denial of Service*
DHCP - *Dynamic Host Configuration Protocol*
DNS - *Domain Name System*
DoS - *Denial of Service*
ESP - *Encapsulating Security Payload*
IANA - *Internet Assigned Numbers Authority*
ICMP - *Internet Control Message Protocol*
IETF - *Internet Engineering Task Force*
IKE - *Internet Key Exchange*
IPng - *Internet Protocol Next Generation*
IPSec - *Internet Protocol Security*
IPv4 - *Internet Protocol Version* 4
IPv6 - *Internet Protocol Version* 6
ISATAP - *Intra-Site Automatic Tunnel Addressing Protocol*
IS-IS - *Intermediate System-to-Intermediate System*
MTU - *Maximum Transmission Unit*
NAPT-PT - *Network Address Port Translation – Packet Translation*
NAT - *Network Translation Address*
NAT-PT - *Network Address Translation – Protocol Translation*
NGTrans - *Next Generation Transition*
NRO - *Number Resource Organization*
OSPFv3 - *Open Shortest Path First version 3*
QoS - *Quality of Service*
RFC - *Request for Comments*
RIPng - *Routing Information Protocol next-generation*
RIR - *Regional Internet Registry*
SIIT - *Stateless* IP/ICMP *Translation Algorithm*
TCP - *Transmission Control Protocol*
TRT - *Transport Relay Translator*
UEL - Universidade Estadual de Londrina

1. Introdução

Durante quase duas décadas, a Internet permaneceu restrita ao ambiente militar e científico. A sua popularização ocorreu somente por volta dos anos 80, em razão da queda no custo dos computadores e dos atrativos recursos oferecidos pela recém desenvolvida *World Wide Web* (ou apenas Web) [1].

Desde então, a grande rede tem crescido exponencialmente, já que se tornou um centro em serviços como os de entretenimento, educação e comunicação, e que progressivamente, atinge os mais diversos meios sociais, políticos e econômicos.

Entretanto, esta expansão é colocada em risco devido às limitações existentes no protocolo que lhe serve de base, o IP. Isto porque, o protocolo foi projetado com a capacidade de gerar pouco mais de 4 bilhões de endereços distintos, necessários para identificar os dispositivos na rede. Apesar de ser suficiente para a época, este número mostra-se pequeno, comparado as perspectivas futuras de crescimento da Internet [2].

Atenta às crescentes demandas por endereços IP, a IETF (*Internet Engineering Task Force*), desenvolveu no final de 1995, uma nova versão do protocolo IP, o IPv6, que além de estabelecer um espaço de endereçamento grande o suficiente, fornece melhorias na camada de rede [3].

Dentre estas melhorias destaca-se a arquitetura IPSec, responsável pela implementação dos mecanismos de segurança da nova versão do protocolo IP. A incorporação do IPSec à sua especificação demonstra a preocupação do IPv6 em solucionar os diversos problemas e deficiências de segurança existentes.

O IPSec, de fato, garante a integridade e a confidencialidade do tráfego. No entanto, isto não implica que a arquitetura não possui vulnerabilidades. Além de que, para que o IPSec realmente seja eficiente, a total substituição pelo IPv6 deve ser realizada pelas estruturas que formam a Internet. Mas isto não acontece de forma tão simples.

Discussões sobre as políticas de implantação IPv6, determinaram que a substituição do protocolo somente poderia ocorrer de forma gradual, no qual por um período indeterminado de tempo as duas versões coexistiriam, até que por fim, todos dispositivos respondam somente pelo novo protocolo.

O processo de implantação existe há mais de uma década, no entanto com a iminente exaustão dos endereços, ele deve ser acelerado. Daí, a preocupação em compreender o atual estágio e esclarecer as tecnologias utilizadas durante transição.

Portanto, esta monografia busca elucidar os aspectos referentes ao período de transição do IPv4 para o IPv6, a partir dos mecanismos definidos pela IETF para prover a interoperabilidade dos protocolos.

Para isto, é realizado: Especificação das características do IPv6; Analise das técnicas de transição elaboradas pela IETF; Apontamento do atual estado de implantação no mundo, no Brasil e na Universidade Estadual de Londrina, como pesquisa de campo.

Deste modo, o trabalho esta dividido da seguinte forma: No capítulo 2 serão apresentados os conceitos sobre o IPv6; No capítulo 3, serão abordadas as Técnicas de Transição IPv6; No capítulo 4 serão descritos os estágios de implantação em diferentes cenários e finalmente no capítulo 5 serão apresentadas as conclusões deste trabalho.

2. IPv6

O protocolo IP (*Internet Protocol*) foi projetado na década de 70 e formalizado no ano de 1981 com o propósito de fornecer as bases para a interligação de redes diversas, como as conectadas por linhas telefônicas, rádio, satélite e as tecnologias futuras. Junto com o protocolo TCP, foi responsável pela expansão da ARPANET, rede militar do departamento de defesa americano que originou a Internet [4].

Sem pretensões globais, o IP, conhecido por IPv4, foi esquematizado para suportar um sistema de endereçamento de 32 bits, o que na época era mais do que suficiente, já que o número de bits garantia a possibilidades de 4.294.967.296 endereços distintos. No entanto, a rápida propagação da Internet, mostrou que este número poderia ser insuficiente frente ao grande número de dispositivos com acesso a web.

Este problema tem a atenção da IETF desde 1990, quando a entidade iniciou os preparativos para a criação do modelo sucessor do protocolo IP. Para isto foi instituído o IPng (*Internet Protocol Next Generation*), grupo cuja responsabilidade era detalhar os requisitos necessários da nova versão.

O novo protocolo deveria conter um cabeçalho simplificado, de estrutura hierárquica de endereços que permitisse a agregação de rotas, grande o suficiente para satisfazer as necessidades da internet no futuro, além da criação de mecanismos de autenticação e criptografia com configuração *plug and play* [5].

Após a avaliação de várias propostas, em dezembro de 1995 foi publicada a RFC 1883, documento oficial contendo o formato do novo protocolo, o IPv6. Três anos mais tarde, o documento foi substituído pela RFC 2460 [6], contendo a atual especificação ao qual servirá de base para o trabalho.

As principais diferenças do IPv6 em relação ao IPv4 podem ser organizadas, segundo [6], nas seguinte categorias:

- Ampliação da capacidade de endereçamento – O novo protocolo aumenta o espaço de endereçamento de 32 bits para 128 bits, o que leva a suportar mais níveis na hierarquia de endereços, um número maior de *hosts* endereçáveis e a possibilidade de auto-configuração de endereços. A escalabilidade do roteamento *multicast* é melhorada através da adição de um campo próprio para endereços *multicast,* este campo é definido para o envio de pacotes a todos os membros do grupo.

- Simplificação do formato do cabeçalho – Alguns campos do cabeçalho do IPv4 foram retirados a fim de reduzir o custo de processamento no seu manuseio.
- Suporte aprimorado para as extensões e opções – Ao contrário do IPv4 onde as opções eram integradas na própria base do cabeçalho, o IPv6 trata as opções como cabeçalhos de extensão, estes não são obrigatórios e são inseridos entre o cabeçalho IPv6 e o *payload,* possibilitando os pacotes serem construídos muito mais flexíveis e simples.
- Capacidade de fluxo rotulado – Consiste em rotular um conjunto de pacotes enviado por uma fonte a um mesmo destino, exigindo um tratamento especial ou qualidade de serviço.
- Recursos de autenticação e privacidade – Prevê suporte a autenticação, integridade de dados e opcionalmente a confidencialidade dos dados.

Com isto, o IPv6 resolveu a principal limitação do seu antecessor, estabelecendo novos recursos julgados necessários para a camada de rede. Para compreende-lo melhor, apresento as características que formam o IPv6 nos 7 sub-capítulos seguintes.

2.1. Formato de Cabeçalho

O IPv6 introduz um novo formato de cabeçalho, mais simplificado que sua versão anterior por possuir menos campos e um tamanho fixo de 40 bytes. Esta facilidade implica em menos processamento dos roteadores, contribuindo com o aumento de velocidade da comunicação. A figura abaixo ilustra o cabeçalho [6]:

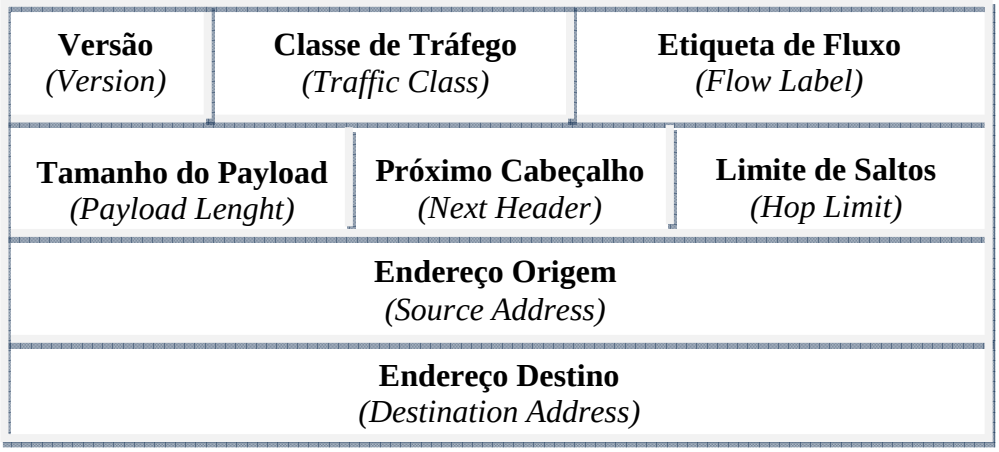

Figura 2.1 – Cabeçalho IPv6

Onde os campos possuem as seguintes funcionalidades:

- Versão/ *Version* - 4 bits - Informa a versão do Protocolo utilizada, sendo 4 para o IPv4 e 6 para o IPv6. Este campo somente possui serventia durante a fase de transição do novo protocolo que já leva alguns anos, devendo cair em desuso quando a implantação for completa.
- Classe de Tráfego/ *Traffic Class* - 8 bits - Utilizado para distinguir entre as diferentes classes ou prioridades dos pacotes.
- Etiqueta de Fluxo/ *Flow Label* - 20 bits - Permite rotular uma sequência de pacotes, criando uma pseudo-conexão entre origem e destino. É utilizada também para obtenção de QoS.
- Tamanho do *Payload/ Payload Lenght* - 16 bits - Comprimento do *payload*, ou seja, o tamanho dos dados reais transmitidos. No IPv6 qualquer extensão do cabeçalho é considerada parte do *payload*.
- Próximo Cabeçalho/ *Next Header* - 8 bits - Identifica o tipo de cabeçalho de extensão seguinte ao cabeçalho IPv6. Este campo permite a transformação de alguns campos do cabeçalho do IPv6 em campos opcionais.
- Limite de Saltos/ *Hop Limit* - 8 bits - Campo destinado a evitar que pacotes tenham duração de vida alta ou infinita. Para isso o seu valor é decrementado a cada salto entre roteadores. Quando se verifica que o valor é zero, o pacote é descartado.
- Endereço Origem/ *Source Address* - 128 bits - Endereço do *host* de origem do pacote.
- Endereço Destino/ *Destination Address* - 128 bits - Endereço do receptor do pacote. Caso uma extensão de cabeçalho de roteamento exista, este pode não ser o último destino.

2.2. Cabeçalhos de Extensão

A fim de se obter um cabeçalho simples e compacto, o IPv6 insere o conceito de cabeçalhos de extensão. O cabeçalho principal do IPv6 visa atender as generalidades encontradas na comunicação, no entanto, não fornece mecanismos as vezes necessários como autenticação, fragmentação, criptografia entre outros. Os vários

cabeçalhos de extensão possibilitam a existência destes mecanismos, mas apenas quando necessários, não sobrecarregando o tamanho do cabeçalho principal e causando ineficiência a rede [6].

Os cabeçalhos de extensão são colocados entre o cabeçalho IPv6 principal e o cabeçalho do protocolo da camada de transporte, de forma que estejam ligados entre si pelo campo Próximo Cabeçalho, numa estrutura semelhante a uma lista encadeada de dados, como mostrado a seguir:

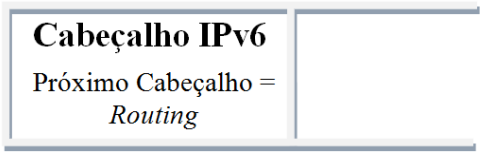

Figura 2.2 – Exemplo Sem Cabeçalho de Extensão

Figura 2.3 – Exemplo com 1 Cabeçalho de Extensão

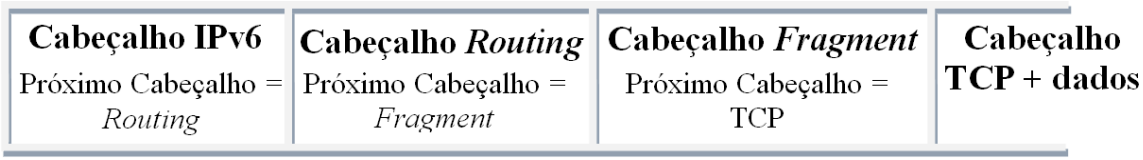

Figura 2.4 – Exemplo com 2 Cabeçalhos de Extensão

Uma implementação completa inclue os seguintes cabeçalhos [6]:

- *Hop-by-Hop Options* – Campo que contém opções a serem processadas por todos os nós dos quais o pacote percorre.
- *Routing* – Cabeçalho utilizado pelo nó de origem para indicar uma lista de nós a serem visitados pelo pacote.
- *Fragment* – Cabeçalho utilizado para o envio de um pacote de forma que se ajuste ao MTU das camadas inferiores das ligações por onde percorre.
- *Authentication Header* – Cabeçalho utilizado para verificação da identidade do transmissor do pacote.
- *Encapsulating Security Payload* – Cabeçalho que possui informações sobre criptografia

- *Destination Options* – Cabeçalho de extensão para transporte de informação opcional que somente será analisa pelo *host* destino.

2.3. Endereçamento

A mais expressiva mudança do IPv6 em relação a seu modelo anterior está no espaço de endereçamento. Com a mudança do espaço dedicado de 32 bits do IPv4, para 128 bits do IPv6, é possível a combinação de 340,282,366,920,938,463,463,374,607,431,768,211,456 ou (ou 3.4 x 10^{38}) endereços distintos. Para melhor compreensão de tamanha magnitude, se esta quantidade de endereços fosse atribuída à superfície da Terra, tal relação significaria aproximadamente 6,65 x 10^{23} endereços por metro quadrado [2].

2.3.1. Tipos de Endereçamento

Segundo [7], os endereços do IPv6 são classificados em 3 categorias de formatos básicos:

Unicast – Endereço que tem por objetivo identificar apenas uma interface ou *host*. Sendo assim, um pacote enviando a um endereço *unicast* possuirá um único destinatário.

Anycast – Tipo de endereço atribuído a mais de um *host* ao qual compartilham um único prefixo de endereço, por exemplo, uma pequena rede interligada fisicamente. Um pacote enviado a um destino *anycast* encontrará seu destino ao encontrar um único *host* pertencente ao grupo ao qual identifica, geralmente, o *host* mais próximo deste grupo segundo o protocolo de roteamento.

Multicast – Este endereço identifica um grupo de *hosts*. Um pacote enviado a um endereço *multicast* é recebido por todos os membros do grupo ao qual define.

No Ipv6 não são mais definidos endereços de *broadcast*, a função destes pode ser substituída pelos endereços *multicast*.

2.3.2. Notação

Com um número maior de bits para denotar um endereço, o IPv6 define um novo tipo de notação. Esta consiste em um conjunto de 8 grupos de 4 números

hexadecimais separados por um símbolo dois-pontos. Sendo permitido o uso de caracteres maiuscúlos ou minúsculos [7].

Como por exemplo:

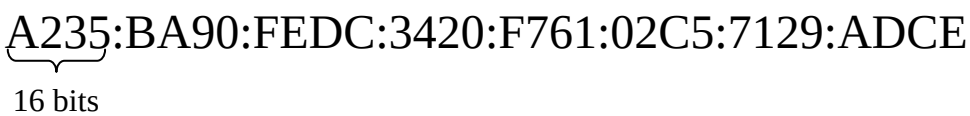

Figura 2.5 – Exemplo de endereço IPv6

Entretanto, este formato prevê a existência de uma longa cadeia de zeros. Para facilitar a escrita destes casos, dois modos foram definidos. O primeiro visa omitir os zeros à esquerda, deixando pelo menos um digito no grupo de bits. Exemplo:

- 3020:0:0:0:0:0:5DA:327C

Como este modo ainda prevê a existência de uma sequência de zeros encadeados, a segunda forma sugere então a substituição da cadeia de zeros por dois símbolos seguidos do tipo dois-pontos. Esta substituição pode ocorrer somente uma vez, caso contrário ocasionará ambiguidade, o exemplo anterior ficaria desta maneira:

- 3020::5DA:327C

Outra notação importante é a dos prefixos de rede. Seu formato de escrita segue o mesmo utilizado pelo IPv4, sendo representado da seguinte forma: EndereçoIPv6/Tamanho do prefixo, onde o tamanho do prefixo especifica a quantidade de bits mais a esquerda do endereço destinados a representar o prefixo da rede. Por exemplo:

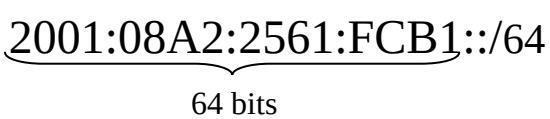

Figura 2.6 – Exemplo de prefixo IPv6

O prefixo acima indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede. Esta representação possibilita a agregação dos endereços de forma hierárquica, tornando possível identificar a topologia da rede por

meio de parâmetros como localização geográfica, provedor de acesso, sub-rede, etc. Com isto, o tamanho das tabelas de roteamento é minimizado, acelerando o encaminhamento do tráfego.

2.3.3. Alocação de Endereços

Assim como sua versão anterior, o IPv6 realiza uma divisão do seu espaço de endereçamento. A divisão ocorre de acordo com o valor dos bits superiores do endereço. Os bits superiores e seus valores fixos são conhecidos como prefixo de formato. A tabela a seguir lista a alocação, de acordo com a RFC 3513, informando o formato de prefixo e a fração que ocupa em relação a todo espaço existente [7]:

Tabela 2.1 – Alocação de Endereços IPv6

Alocação	Prefixo (binário)	Fração do Espaço
Não Atribuído	0000 0000	1/256
Não Atribuído	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Não Atribuído	0000 01	1/64
Não Atribuído	0000 1	1/32
Não Atribuído	0001	1/16
Global Unicast	001	1/8
Não Atribuído	010	1/8
Não Atribuído	011	1/8
Não Atribuído	100	1/8
Não Atribuído	101	1/8
Não Atribuído	110	1/8
Não Atribuído	1111 0	1/32
Não Atribuído	1111 10	1/64
Não Atribuído	1111 110	1/128
Não Atribuído	1111 1110 0	1/512
Link-Local Unicast Addresses	1111 1110 10	1/1024
Site-Local Unicast Addresses	1111 1110 11	1/1024
Endereços *Multicast*	1111 1111	1/256

2.4. Auto-Configuração

O IPv6 foi projetado de modo que a configuração de endereços seja do tipo *plug-and-play*, ou seja, basta o *host* estar ligado que um endereço lhe será associado automaticamente. Assim, não é necessária a configuração manual de cada *host* para que obtenha acesso a rede. A auto-configuração se dá através de duas formas [3]:

- Configuração *Stateful*: Implica na existência de um servidor de configuração de endereços, que no mundo IPv4 é conhecido por DNS.
- Configuração *Stateless*: O próprio *host* constrói seu endereço IP baseado no seu endereço MAC de interface de rede. Cada interface de rede possui este endereço que o identifica univocamente, este número é combinado com o prefixo da rede local, ou com o prefixo informado por um roteador.

2.5. Roteamento

De forma similar ao IPv4, os nós IPv6 utilizam uma tabela de roteamento local para determinar como encaminhar os pacotes. A tabela de roteamento é preenchida por entradas padrões durante sua inicialização e entradas adicionais a partir da comunicação entre roteadores ou mesmo por meio do *Dynamic Host Configuration Protocol for* IPv6 (DHCPv6) [2].

No que diz respeito ao modelo de roteamento, o IPv6 fez poucas inovações. Os vários protocolos de roteamento IPv4, que garantem a comunicação entre os roteadores, possuem versão correspondente ou uma extensão para o IPv6, como é o caso dos protocolos de roteamento interno OSPFv3 e externo BGP.

A estrutura dos *Autonomous System* (AS), conjunto de redes controladas por uma entidade administrativa comum, mantém-se inalterada com a utilização dos protocolos de roteamento IPv6, mesmo com a possibilidade de agora rotear pacotes de ambas as versões. Sendo que para o tráfego interno serão utilizados os protocolos RIPng, OSPFV3 e IS-IS. Enquanto somente o protocolo BGP4 está disponível para troca de rotas IPv6 entre os *Autonomous System* [2].

2.6. Qualidade de Serviço

O termo Qualidade de Serviço, comumente apresentado por seu acrônimo QoS (*Quality of Service*), designa a capacidade de oferecer maior garantia na entrega dos pacotes e segurança para as aplicações [3]. No IPv6, QoS é um conceito intrínseco e de grande importância, por isso foi desenvolvido de forma a oferecer flexibilidade suficiente para suportar diversos mecanismos de QoS.

O próprio cabeçalho principal designa dois campos para obtenção de qualidade de serviço, são eles: Etiqueta de Fluxo e Classe de Tráfego. O primeiro é utilizado para rotular um fluxo de pacotes (pacotes que possuem mesmo origem e destino), a fim de receber um tratamento diferenciado pelos roteadores. O segundo campo define a prioridade dos pacotes com a qual o roteador terá de lidar. Ambos possibilitam a implementação de aplicações multimídia, com integração de serviços de dados, voz e vídeo em tempo real com alta performance [3].

2.7. Segurança

Os serviços de segurança do IPv6 são conferidos por conta da arquitetura IPSec (IP *Security Protocol*). O IPSec foi concebido para prover diversos serviços de segurança na camada de rede, tanto para o IPv4 quanto o IPv6, sendo que na antiga versão seu uso é opcional e na nova se trata de um serviço nativo.

No IPv6, o IPSec utiliza dois cabeçalhos de extensão para prover segurança de tráfego, o *Authentication Header* (AH) e o *Encapsulating Security Payload* (ESP).

O *Authentication Header* provê integridade e autenticação das entidades envolvidas na comunicação. Nem todas as aplicações foram desenvolvidas de forma a necessitar de autenticação, como é o caso do roteamento e da descoberta de vizinhos (*neighbor discovery*), no entanto, com os múltiplos ataques ao sistema de roteamento, a integridade e autenticação dos pacotes IP passou a ser altamente desejável. Da mesma forma ocorre com a necessidade de autenticação sobre os pacotes que trafegam pela internet, alvos de ataques como *spoofing*, técnica que consiste em mascarar os pacotes utilizando endereços de remetentes falsos [3]. Para fornecer autenticação fim-a-fim dos dados transportados, o AH define o seguinte cabeçalho de extensão:

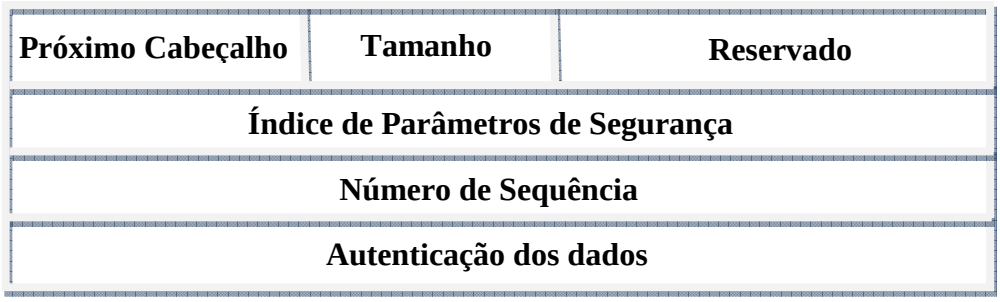

Figura 2.7 – Cabeçalho de Extensão *Authentication Header*

Aos quais os elementos da estrutura do cabeçalho denotam:

- Próximo Cabeçalho - 8 bits - Indica o próximo cabeçalho a ser analisado.
- Tamanho - 8 bits - Tamanho do cabeçalho AH.
- Reservado - 16 bits - Não utilizado, possui valor zero.
- Índice de Parâmetros de Segurança - 32 bits - Indica qual algoritmo de *checksum* é utilizado.
- Número de Sequência - 32 bits - Contador utilizado na marcação das mensagens, com o propósito de evitar *replay attacks*.
- Autenticação dos dados - Tamanho Variável - Contém o *integrity check value* (ICV), valor baseado no cálculo de alguns campos do endereço, cabeçalho AH e dados. Utilizado como mensagem de código de autenticação.

O *Encapsulating Security Payload* é responsável pela integridade do interior do pacote e confidencialidade dos dados. Sendo utilizado quando se deseja proteção contra modificações ou mesmo acesso indevido aos dados enviados pela rede. O seu cabeçalho possui o seguinte formato:

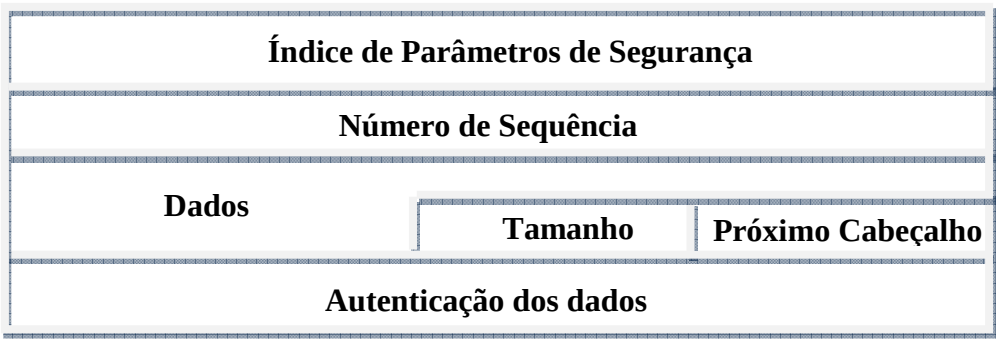

Figura 2.8 – Cabeçalho de Extensão *Encapsulating Security Payload*

Aos quais os campos do cabeçalho representam:

- Índice de Parâmetros de Segurança - 32 bits - Indica qual algoritmo de criptografia esta sendo utilizado.
- Número de Sequência - 32 bits - Contador utilizado na marcação das mensagens, com o propósito de evitar *replay attacks*.
- Dados - Tamanho Variável - Dados a serem enviados.
- Tamanho - 8 bits -Tamanho do cabeçalho ESP.
- Próximo Cabeçalho - 8 bits - Indica o próximo cabeçalho a ser analisado.
- Autenticação dos dados - Tamanho Variável - Contém o ICV calculado sobre o pacote ESP menos o autenticação dos dados.

Além destes mecanismos, o IPSec necessita de um método de gestão de chaves. Para isto, define como norma de gestão o protocolo *Internet Key Exchange* (IKE) responsável pela criação, eliminação e alteração das chaves [8].

Em geral, o uso do IPSec melhora a segurança da rede, mas não resolve todos os problemas conhecidos, como as técnicas de ataque de DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*) [9].

O fornecimento de autenticação e criptografia para cada pacote na camada de rede representa significativa melhoria e preocupação em resolver as vulnerabilidades existentes, mas isto não impede que novas formas de ataque sejam desenvolvidas, principalmente durante o período de transição entre IPv4 e IPv6 [9].

3. Técnicas de Transição

A adoção do novo protocolo implica uma série de mudanças e atualizações, tanto em questões de hardware quanto de software. Embora a maioria dos sistemas operacionais, como Windows (desde a versão 2000), Linux (desde a versão do *kernel* 2.18) e Mac Os (desde a versão 10.2 Jaguar) [10], já estejam preparados para receber o IPv6, diversos softwares e elementos estruturais de rede, como roteadores e modems de acesso ADSL, não se encontram aptos a utilizar o novo protocolo.

Considerando estas restrições, o IPv6 passa por um período de transição, no qual a implantação ocorre de forma gradual, de modo que as duas versões coexistam por alguns anos até que por fim todos dispositivos façam uso da nova versão. Para que este período seja tranquilo e sem grandes complicações, a IETF determinou a criação do grupo de trabalho NGTrans (*Next Generation Transition*), responsável pela criação de técnicas e mecanismos que assegurem a interoperabilidade dos dispositivos IPv4 e IPv6.

O trabalho do NGTrans resultou na criação de uma série de mecanismos, que podem ser aplicados individualmente ou em conjunto, de forma que venham à atender as necessidades das mais diversas topologias de rede. Os mecanismos se dividem em três classes de técnicas: Pilha Dupla, Tunelamento e Tradução.

3.1. Pilha Dupla

Durante o período de transição, a técnica mais simples utilizada para que dispositivos de versões distintas do protocolo se comuniquem é a chamada Pilha Dupla. Esta técnica baseia-se no uso de ambas as pilhas de protocolos por parte dos *hosts* e roteadores. Desta forma, o dispositivo pilha dupla pode enviar e receber pacotes com endereços IPV4 e IPv6, decidindo qual utilizar baseado no dispositivo com quem troca tráfego [11]. A figura a seguir ilustra a técnica:

Figura 3.1 – Pilha Dupla

O dispositivo configurado como pilha dupla utiliza dois endereços, um IPv4 (seja por DHCP ou configuração automática) e outro IPv6 (por mecanismos do protocolo como auto-configuração, DHCPv6 ou mesmo configuração automática). A vantagem desta técnica é que ela permite gradual implantação, o que possiblita atualização por pequenos setores. Após toda a rede estar atualizada, basta apenas desabilitar a pilha do protocolo antigo [12].

Outras vertentes devem ser analisadas perante seu uso, como a necessidade de readequação de elementos da infra-estrutura da rede, por exemplo, a configuração do serviço DNS (*Domain Naming System*) [12].

O serviço DNS é responsável pela resolução (tradução) de nomes de domínios em endereços IP, para isto ele mantém um registro interno relacionando os nomes dos dispositivos aos seus respectivos IPs. Como os espaços de endereçamento das duas versões se diferem, 32 e 128 bits, um novo formato de registro foi definido para armazenar endereços IPv6, o AAAA[13]. Desta forma, o serviço DNS atua respondendo com endereços IPv6 às consultas do tipo AAAA e endereços IPv4 às consultas do tipo A.

Para casos em que um único nome de domínio possua endereços dos dois tipos, o DNS pode ser configurado de modo a responder utilizando uma ordem pré-definida. Este artifício força a ocorrência de maior tráfego do protocolo escolhido como primeira opção. Ajustes podem ser feitos em nível de aplicação, a fim de priorizar o tráfego de uma versão [11].

3.2. Tunelamento

A técnica de Tunelamento providencia uma maneira de se utilizar o IPv6 sobre uma infra-estrutura IPv4 já existente, sem a necessidade de mudanças nos mecanismo de roteamento. Isto ocorre através da criação de túneis em que o conteúdo do pacote IPv6 é encapsulado em um pacote IPv4 e transmitido pela própria rede IPv4.

Um túnel possui dois pontos finais, um de entrada e outro de saída, operando da seguinte maneira: O ponto de entrada configura o campo *Hop Limit* (limite de salto) do cabeçalho IPv6 para 1, encapsula o pacote em um cabeçalho IPv4 e transmite o pacote encapsulado pelo túnel, se necessário fragmentando o pacote. O ponto de saída recebe o pacote e verifica a existência de fragmentação, remontando-o se necessário. O cabeçalho IPv4 é removido e o pacote remetido a seu destino [3].

O tunelamento permite o envio de pacotes sobre diversas topologias de roteamento IPv4, podendo ocorrer nos seguintes cenários [11]:

- Roteador-a-Roteador – Roteadores do tipo IPv4/IPv6 (pilha dupla) interconectados por uma estrutura IPv4 podem trocar tráfego IPv6 entre si, como exemplifica a figura:

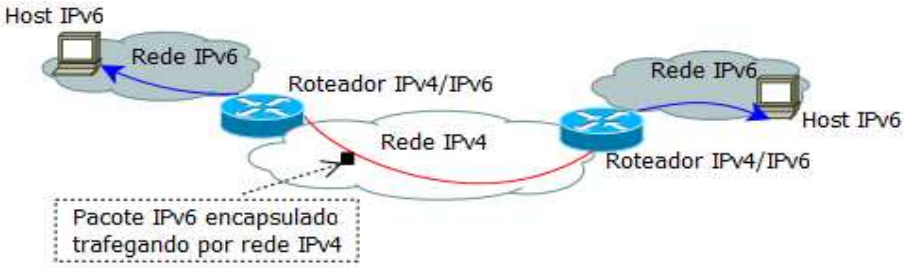

Figura 3.2 – Topologia Roteador-a-Roteador

- *Host*-a-Roteador – *Host* IPv4/Ipv6 estabelece túnel com roteador IPv4/Ipv6 intermediário, acessível por uma infra-estrutura IPv4.
- Roteador-a-*Host* – Roteador pilha dupla envia pacotes IPv6 ao destino final, seja através de túnel ou IPv6 nativo. A figura a seguir exemplifica os dois últimos modos apresentados:

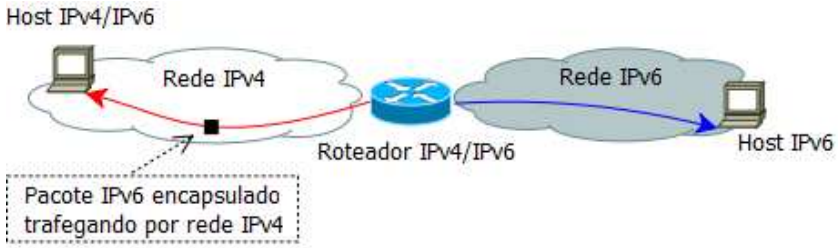

Figura 3.3 – Topologia *Host*/Roteador-a-*Host*/Roteador

- *Host*-a-*Host* – *Hosts* IPv4/IPv6 interligados por uma rede IPv4 trocam pacotes IPv6 entre si, como mostra a figura a seguir:

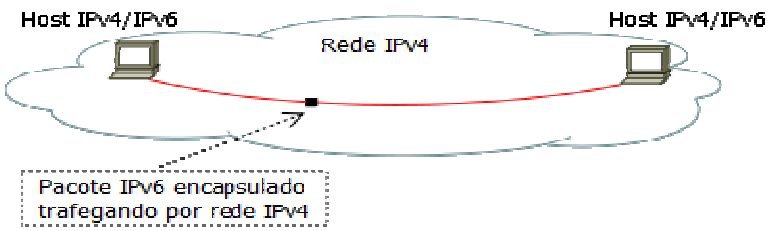

Figura 3.4 – Topologia *Host* -a-*Host*

3.2.1. Encapsulamento

O encapsulamento de um pacote IPv6 em um IPv4 acontece da seguinte forma [11]:

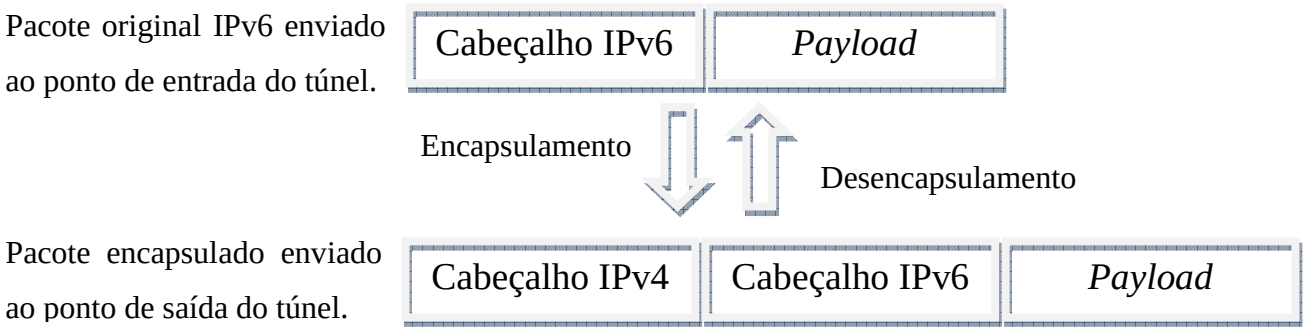

Figura 3.5 – Encapsulamento/Desencapsulamento

Alguns campos do cabeçalho IPv4 requerem atenção especial [11]:

- *Version*: O valor 4 será utilizado, como um pacote IPv4 comum.
- IHL (*Internet Header Length*): Este campo mensura o tamanho do cabeçalho IP em palavras de 32 bits, como não existem opções para o cabeçalho encapsulado o valor mínimo 5 é adotado.
- *Total Lenght:* Campo destinado a conter o tamanho do pacote. Deverá somar o tamanho do *payload* com os cabeçalhos IPv4, IPv6 e qualquer cabeçalho de extensão existente.
- *Identification:* Gerado de forma única, como qualquer outro pacote IPv4 transmitido.
- *Flags:* Indica se mais pacotes fragmentados devem chegar.
- *Fragment Offset:* Indica se é realizada a fragmentação.
- *Time to live:* Seu valor depende da aplicação utilizada.
- *Protocol:* O valor 41 é inserido como indicação de encapsulamento. Este critério facilita a análise de tráfego IPv6, pois basta ao *sniffer* de rede aplicar um filtro sobre este campo para obter todos pacotes tunelados que passam por ele.
- *Header Checksum:* Calcula normalmente o valor de soma para verificação de integridade.
- *Source Address:* Endereço do ponto de entrada do túnel, entidade que realiza o encapsulamento.

- *Destination Address:* Endereço do ponto de saída do túnel.
- *Hop Limit:* Os túneis são modelados como um único salto, isto esconde a existência do túnel por parte da entidade final e impossibilita a detecção por ferramentas comuns.

Além de adicionar um cabeçalho IPv4, o encapsulador deve tratar de outras questões complexas como [11]:

- Determinar quando se deve realizar a fragmentação ou o envio de um pacote ICMPv6 avisando a fonte de origem que o pacote é grande demais.
- Redirecionar avisos de erros ICMPv4 recebidos no caminho do túnel, em avisos ICMPv6 para a fonte de origem.

A primeira questão aborda a forma com que o encapsulador deve proceder quando se depara com um pacote cujo tamanho excede o MTU. O MTU (*Maximum Transmission Unit*) refere-se ao tamanho máximo que um pacote pode possuir para ser transmitido. Sendo o pacote encapsulado uma junção dos cabeçalhos IPv4 e IPv6, esse limite pode ser extrapolado, restando para o encapsulador a tarefa de enviar à fonte emissora uma mensagem ICMPv6, reportando que o pacote excedeu o limite. No entanto, este esquema se mostra ineficiente e não operável por três razões, e portanto não deverá ser utilizado [11]:

- Isto resultaria em mais fragmentação. Fragmentações nesta camada devem ser evitadas devido a problemas de desempenho.
- Gasto de memória e processamento dos roteadores, situados nos limites do túnel, ao remontar os pacotes.
- O encapsulador não tem conhecimento sobre a capacidade do desencapsulador em desfragmentar os pacotes, ou mesmo conhece o limite máximo de tamanho de pacote que o dispositivo pode receber.

Desta forma, o encapsulador não deve tratar o túnel como uma interface comum, com um MTU de 64 kilobytes, mas sim utilizar um MTU estático ou dinâmico, baseado no ponto final do túnel. A escolha do MTU estático utiliza por padrão o valor fixo de 1280 bytes como limite. Este valor ainda pode variar de 1280 bytes a 1480 bytes desde que seja implementada uma opção que altere o valor de MTU e que seja garantida, por parte do receptor, a capacidade de desencapsular pacotes deste tamanho. O modo dinâmico faz uso do *IPv4 Path MTU Discovery Protocol*, uma técnica que determina

o valor máximo de MTU entre dois *host*. Se ambos os casos forem implementados, a decisão de qual modo utilizar deverá ser previamente configurada nos pontos finais [11].

3.2.2. Desencapsulamento

O dispositivo ao receber um pacote cujo valor do campo *Protocol* seja igual a 41, logo identifica de que se trata de um pacote encapsulado. Em seguida, através dos campos de origem e destino, realiza a verificação do tipo de túnel a que o pacote pertence. O pacote é remontando, caso esteja fragmentado, e por fim o cabeçalho IPv4 é removido para que o pacote IPv6 possa ser enviado ao seu destino.

A verificação da fonte emissora é realizada antes do processamento do pacote, a fim de atenuar técnicas de *spoofing*. Outro efeito positivo desta verificação, é que os pacotes com endereços falsos de origem ou cujo destino direto não é o desencapsulador, como pacotes enviados por broadcast, são discretamente descartados [11].

3.2.3. Túneis

Como mostrado anteriormente, os túneis podem ser construídos através de dois pontos, *hosts* ou roteadores, seguindo as topologias apresentadas. Independente dos pontos de entrada e saída, o funcionamento é o mesmo: Encapsulamento, configuração do cabeçalho, transmissão e desencapsulamento. Diferenciando-se pelo modo de configuração, manual ou automático.

Os manualmente configurados apresentam uma forma simples e eficaz de túnel, utilizada quando se busca conectividade permanente e configuração exclusiva. Neste modo, os endereços IPv4 e IPv6 dos pontos de entrada e saída são configurados manualmente [14], exigindo grande mobilização e conhecimento da topologia por parte dos administradores, no entanto, garantindo uma segurança bastante robusta ao tráfego. Esta configuração também possui desvantagens, problemas de escalabilidade são encontrados com o aumento do número de interfaces na rede, já que cada ponto necessita de atenção especial e configuração manual.

Na configuração automática, os túneis são projetados de modo que possam estabelecer o endereço IPv6 a partir do endereço já IPv4 existente. Diversos

mecanismos de transição fazem uso deste tipo de configuração, sendo que cada um possui um cenário no qual sua aplicação é recomendada e características distintas a serem relevadas em um projeto de implantação. Os principais mecanismos são apresentados a seguir.

3.2.4. 6to4

Definido na RFC 3056, o 6to4 tem como principal objetivo prover conexão a domínios IPv6 isolados sobre uma rede IPv4, sem a necessidade de configuração dos túneis nos roteadores situados nos limites destes domínios. Desta maneira, os túneis são construídos com a capacidade de obtenção automática de endereço IPv4 da outra extremidade do túnel [15]. Representação do acesso através de túneis 6to4:

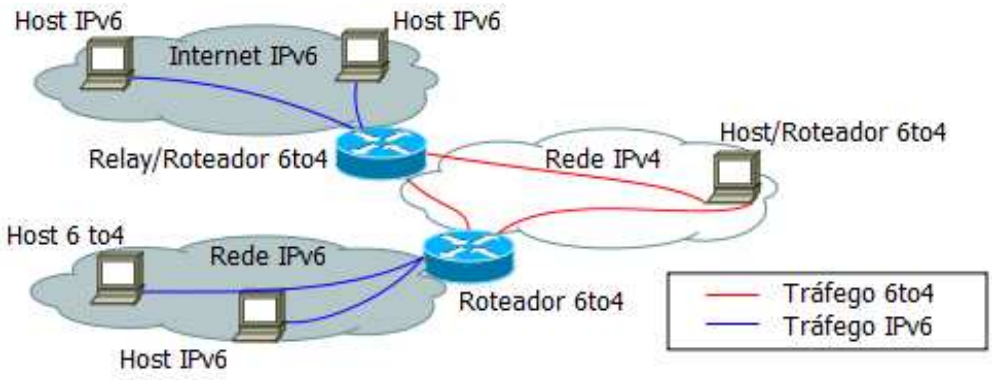

Figura 3.6 – Tunelamento 6to4

Descrição dos elementos presentes na figura:

- *Host*/Roteador 6to4: Dispositivo que possui um endereço IPv4 público e conectividade 6to4 através de um roteador 6to4. O acesso a uma rede IPv6 nativa só é possível utilizando um *relay* 6to4.
- Roteador 6to4: Fornece aos *hosts* IPv6 a possibilidade de acesso aos *hosts* 6to4. Para o acesso às redes IPv6 nativas, realiza o direcionamento do tráfego até o *relay router* mais próximo, que por sua vez encaminha os pacotes à rede IPv6.
- *Relay* 6to4: Roteador com conexão IPv6 nativa e suporte ao 6to4, permite a comunicação com as redes IPv6, IPv4 e 6to4.
- *Host* 6to4: Host IPv6 comum, que tem pelo menos um endereço no formato 6to4, necessitando de um roteador 6to4 para comunicar com outras redes do mesmo tipo.

O endereço IPv6 é estabelecido através do prefixo global **2002:wwxx:yyzz::/48:[ID Sub Rede]:[ID Interface]**, onde wwxx:yyzz é o endereço IPv4 público do dispositivo convertido para hexadecimal. A estrutura do endereço 6to4 é representada na seguinte forma [15]:

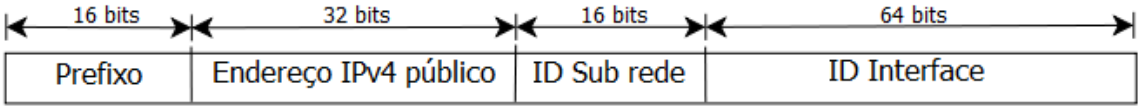

Figura 3.7 – Endereço 6to4

Onde os campos da figura anterior representam:

- Prefixo: O prefixo 2002::/16 é reservado pela IANA (*Internet Assigned Numbers Authority)* para uso exclusivo do 6to4.
- Endereço IPv4 público: O endereço IPv4 é convertido para hexadecimal. Por exemplo, o endereço local 192.168.1.13 resultará: C0A8:010D.
- ID Sub rede: Usado para segmentação da rede 6to4 em várias sub redes, 2^{16} sub redes são possíveis.
- ID Interface: Identifica a interface, com 2^{64} combinações possíveis.

Diversos cenários baseados em túneis 6to4 podem ser construídos para transporte de tráfego IPv6, no entanto, uma rede 6to4 somente consegue se comunicar com outra rede se esta faz uso do mesmo modelo de atribuição de endereço, ou seja, redes nativas IPv6 ficam fora do escopo de comunicação. Para resolver esta limitação roteadores *relays*, definidos anteriormente, executam a função de ponte entre as redes 6to4 e as demais.

Para que um dispositivo 6to4 possa utilizar desses roteadores *relays*, ele precisa localizar o que está mais próximo de si, criando um túnel 6to4 associado a sua rota. Existem muitas instituições que fornecem roteadores *relays* para o acesso gratuito, tal como: Microsoft (6to4.ipv6.org) e Cisco (ipv6-lab-gw.cisco.com). Para encontrar o mais próximo, a RFC 3038 define o uso do prefixo *anycast* 192.88.99.0/24 para o anuncio de rotas disponíveis até um roteador *relay*. O endereço correspondente ao *host* 1 deste prefixo 192.88.99.1 (2002:c058:6301:: quando convertido) é utilizado para o envio dos pacotes para o descobrimento de *relays* [16].

3.2.5. ISATAP

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*), definido na RFC 5214, especifica um túnel automático capaz de conectar dispositivos pilha dupla sobre redes IPv4 [17]. Útil, por exemplo, em casos que a rede já possui numeração IPv6 válida, mas que no entanto, só os utiliza na borda da rede para acesso externo, mantendo a infra-estrutura IPv4 [12].

A obtenção de endereço IPv6, faz uso do endereço IPv4 do próprio *host* e do prefixo especificado no roteador ISATAP, ao qual se encontra conectado. Isto faz com que qualquer dispositivo ISATAP possa determinar os pontos de entrada e saída dos túneis IPv6, sem fazer uso de qualquer tipo de protocolo ou recurso auxiliar [17]. A criação do endereço ISATAP ocorre através do seguinte formato:

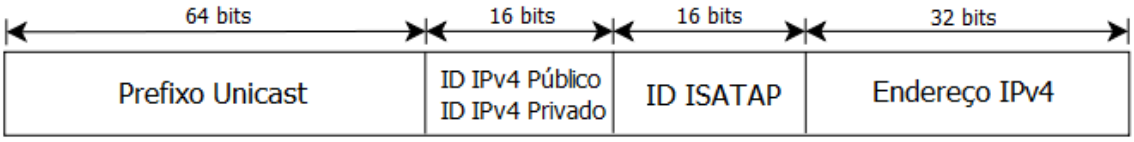

Figura 3.8 – Endereço ISATAP

Onde os campos representam [12]:

- Prefixo Unicast: É utilizado qualquer prefixo *unicast* IPv6. Inclui endereços locais de ligação (FE80::/64) ou globais.
- ID IPv4 Público ou Privado: Valor depende da natureza do endereço IPv4, se o endereço for privado, o campo recebe o valor “0”, caso seja público o valor “200”.
- ID ISATAP: O valor “5EFE” é utilizado como forma de identificação.
- Endereço IPv4: Endereço IPv4 do dispositivo em formato IPv4.

A comunicação entre dispositivos ISATAP pode ocorrer em uma mesma rede, ou através de redes separadas por domínios IPv6. *Hosts* ISATAP estabelecidos em uma mesma rede comunicam-se sem a interferência do roteador ISATAP, já que precisam apenas de uma auto-configuração inicial do roteador, para que os endereços IPv6/ISATAP possam ser estabelecidos. Desta forma, o tráfego IPv4 encapsulado pode trafegar pela rede.

Entre *hosts* separados, a troca de pacotes depende do roteador ISATAP, como por exemplo, na topologia mostrada a seguir:

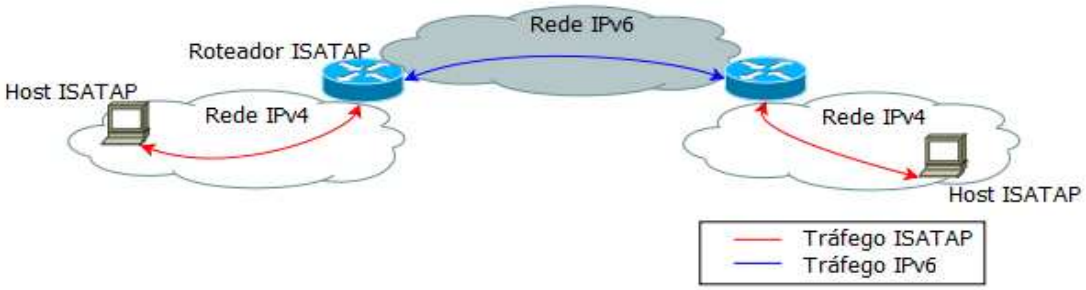

Figura 3.9 – Exemplo Tunelamento ISATAP

Neste caso, através da tabela de roteamento, os *hosts* descobrem que precisam utilizar a interface ISATAP para estabelecer a comunicação. Assim, todo tráfego entre *host* ISATAP e roteador ISATAP, ocorre de modo encapsulado. A troca de tráfego entre roteadores ISATAP ocorre de maneira convencional, sendo que para isto, o roteador, ao receber um pacote cujo campo protocolo consta o valor 41, realiza o desencapsulamento antes de transmiti-lo [12].

3.2.6. *Tunnel Broker*

A idéia desta técnica consiste no uso de servidores dedicados, denominados T*unnel brokers*, que gerenciam automaticamente a criação de túneis a partir de requisições de usuários. É uma das técnicas mais simples para obtenção de tráfego IPv6, onde um simples *script* executável pode ser utilizado para o estabelecimento do túnel. Suas especificações são encontradas na RFC 3053 [18]. A figura a seguir mostra os passos necessários para a criação do túnel:

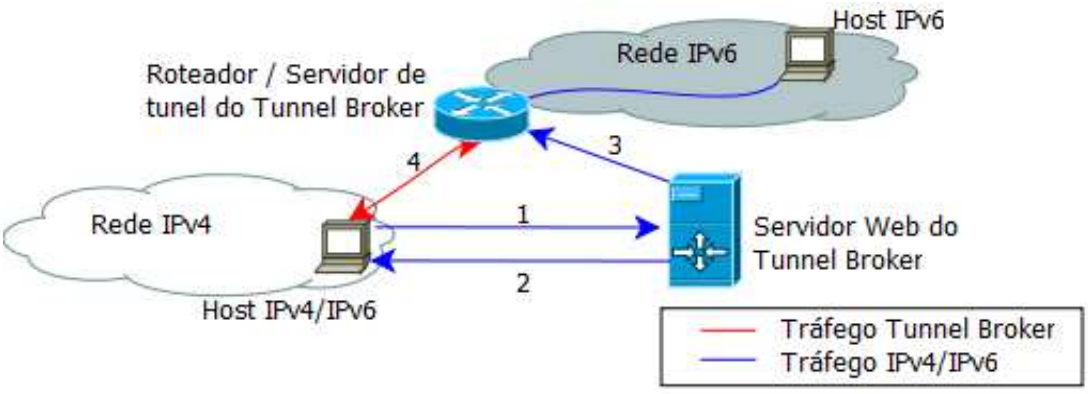

Figura 3.10 – Tunelamento *Tunnel Brokers*

Onde os números indicam a ordem dos passos:

- 1 – *Host* pilha dupla realiza requisição de criação de túnel ao Servidor Web de *Tunnel Broker*.
- 2 – Servidor Web de *Tunnel Broker* retorna script para que o *host* possa criar túnel com o Roteador/Servidor de túnel.
- 3 – Servidor Web de *Tunnel Broker* informa ao Roteador/Servidor de túnel a existência do novo túnel criado.
- 4 – O script é executado pelo *host* IPv4/IPv6 e o acesso a rede IPv4 é obtido através do Roteador/Servidor de *Tunnel Broker*.

3.2.7. Teredo

Um problema em comum dos métodos vistos até então, é o de que eles não funcionam quando o dispositivo IPv6 encontra-se atrás de um ou mais NATs (*Network Address Translations*). Com a escassez dos endereços IPv4, a técnica de NAT passou a fazer parte do cenário de diversas organizações ao proporcionar às redes privadas acesso à internet através de um único endereço IP público. Para isto, o NAT mapeia o endereço privado, junto com a porta utilizada pela aplicação, de modo que os pacotes ao serem enviados para Internet utilizem o endereço público do roteador como endereço de origem e o número gerado pelo NAT como porta [19]. Apesar de ser eficaz, a técnica possui o inconveniente de traduzir apenas os protocolos TCP e UDP, desta forma, quando um pacote tunelado atinge o NAT, ele é descartado, visto que os pacotes deste tipo definem o campo *Protocol* como 41.

O mecanismo de transição 6to4 funciona com o NAT, desde que o mesmo dispositivo faça as funções de NAT e roteador 6to4. Para os demais casos, onde o NAT não pode ser facilmente atualizado, a RFC 4380 fornece o mecanismo de tunelamento automático Teredo [20].

A RFC de definição especifica a existência de dispositivos Teredo, como *host*, servidor e *relay*, para seu funcionamento. Para melhor entendimento dos aspectos que envolvem o mecanismo, uma figura contendo tais dispositivos será exibida, seguida pelas funções de cada aparelho:

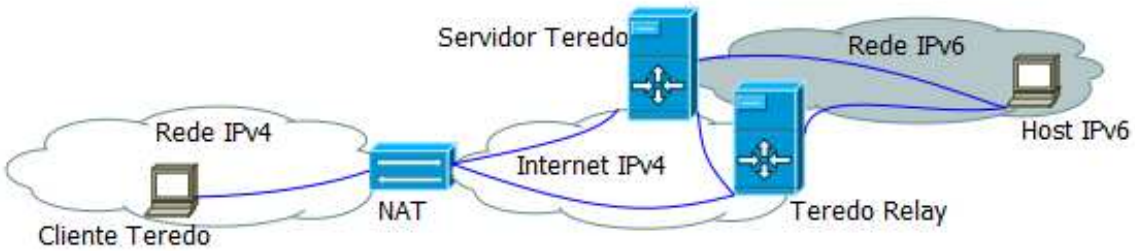

Figura 3.11 – Tunelamento Teredo

- Cliente Teredo: Representa um dispositivo que possui acesso a Internet IPv4 através de um NAT e que busca conectividade IPv6.
- Servidor Teredo: Dispositivo situado na Internet IPv4 cujo objetivo é auxiliar a criação do túnel entre o Cliente Teredo e seu destino IPv6. Por não realizar encaminhamento de tráfego a largura de banda gasta é mínima, sendo assim, possui a capacidade de suportar um grande número de requisições. O portal IPv6 [21], disponibiliza uma lista de Servidores Teredo localizados por todo o mundo, alguns destes servidores: teredo.remlab.net - França, teredo.autotrans.consulintel.com - Espanha, teredo.ipv6.microsoft.com - Estados Unidos, debian-miredo.progsoc.or - Austrália.
- Teredo *Relay*: Dispositivo que encaminha o tráfego IPv6, situado na outra extremidade do túnel (a primeira ocupada pelo Cliente Teredo). Por sua função, necessita de muita largura de banda, e possui um número limitado no atendimento de requisições.

A imagem anterior demonstra um Cliente Teredo, atrás de um NAT, buscando acesso ao *host* IPv6, o qual pode representar um site, um serviço e etc. Para que isto aconteça, o Cliente Teredo inicia a operação interagindo com o Servidor Teredo. Neste processo, o servidor descobre o tipo de NAT ao qual o cliente se encontra e configura seu endereço Teredo. O endereço Teredo possui o seguinte formato [20]:

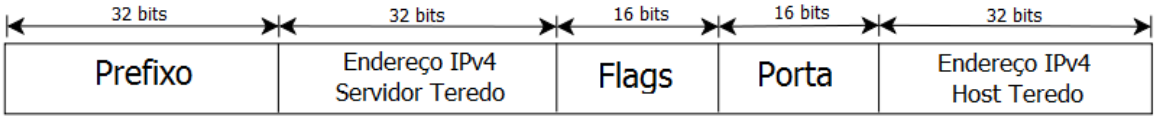

Figura 3.12 – Endereço Teredo

Onde os campos significam:

- Prefixo: É utilizado o identificador do serviço Teredo 3FFE:831F::/32.

- Endereço IPv4 Servidor Teredo: IP do Servidor Teredo.
- Flags: Contém número relativo ao tipo de NAT utilizado (Cone, Cone Restrito, Cone Restrito por porta e Simétrico).
- Porta: Indica a porta UDP de saída do NAT, sendo que cada bit da porta é invertido, o que pode ser feito através de uma operação de OU exclusivo (XOR) com 0xFFFF. Por exemplo, o valor 7250 (0x1C52) aplicado a operação XOR sobre 0xFFFF gera o valor 0xE3AD.
- Endereço IPv4 Cliente Teredo: O endereço do cliente também é mascarado através da operação XOR, no entanto como o campo é de 32 bits a operação é realizada sobre o valor 0xFFFFFFFF. Por exemplo, o IP 192.168.1.13 (C0A8:010D) aplicado a operação XOR sobre 0xFFFFFFFF resulta 3F57FEF2.

O endereço Teredo incorpora o endereço e a porta, ambos mapeados, através do qual o cliente irá receber os pacotes encapsulados. Tendo esta etapa concluída, o cliente precisa descobrir o Teredo *Relay* que se encontra mais perto do seu destino, para isto, envia uma mensagem ICMPv6 *echo request* via Servidor Teredo. A mensagem é então encaminhada ao host IPv6 destino. O host IPv6, responde a mensagem para o cliente através de um ICMPv6 *echo request*, roteado pelo Teredo *Relay* mais perto de si. Antes de rotear o pacote, o *relay* encapsula a mensagem e a envia diretamente ao cliente, desta forma o cliente obtém o endereço IPv4 e a porta utilizada por ele. Tendo descoberto o *relay* mais próximo, o túnel pode ser criado. Os pacotes provenientes do cliente são então encapsulados e enviados até o *relay* Teredo, que então remove os cabeçalhos IPv4 e UDP e os encaminha até o host IPv6 [20].

Apesar de se mostrar eficiente, a utilização de túneis Teredo somente é encorajada em último caso, quando a aplicação dos mecanismos apresentados anteriormente for inviável. Isto ocorre pela quantidade razoável de sobrecarga causada durante o encapsulamento UDP [20].

3.3. Tradução

A técnica de Tradução consiste no uso de um dispositivo intermediário, que atua em diversas formas e camadas, realizando a tradução dos cabeçalhos e conversões de endereços e APIs de programação, garantindo a troca de tráfego entre dispositivos nativos IPv6 e IPv4, ou mesmo dispositivos pilha dupla. Embora

eficaz, a técnica de tradução não suporta algumas características avançadas do IPv6, tal como os serviços de segurança, controle de acesso, confidencialidade e integridade de dados. Além de impor algumas limitações a estrutura topológica da rede, pois qualquer mensagem enviada pelo dispositivo tradutor deverá retornar pelo mesmo dispositivo [22].

Os mecanismos baseados em Tradução podem ser classificados de acordo com a camada em agem:

- Camada de Rede – Integram esta classe: SIIT, NAT-PT e NAPT-PT.
- Camada de Transporte – Mecanismos cuja tradução ocorre nesta camada: SOCKS e TRT.
- Camada de Aplicação – Atua nesta camada: ALG.
- Camada Adicional – Alguns mecanismos inserem camadas adicionais na pilha de protocolo. Fazem parte deste grupo: BIS e BIA.

Na continuação do capitulo, os mecanismos classificados serão expostos.

3.3.1. SIIT

O mecanismo de Tradução SIIT (*Stateless* IP/ICMP *Translation Algorithm*) permite a comunicação entre *hosts* com suporte apenas ao IPv4 e *hosts* que possuem apenas suporte ao IPv6 através de um algoritmo proposto na RFC 2765. Ele utiliza um tradutor, situado na camada de rede, que realiza a conversão de campos dos cabeçalhos IPv6 para IPv4 e vice-versa. O funcionamento da técnica pode ser acompanhado na figura a seguir [23]:

Figura 3.13 – Tradução SIIT

O mecanismo determina que o Roteador SIIT contenha um *pool* de endereços IPv4 públicos alocados. Para que ocorra comunicação entre um *host* IPv6 e

outro IPv4, como os da figura, o roteador mapeia um endereço IPv4 para IPv6 ao *host* IPv4, no formato 0::FFFF:a.b.c.d, e define um endereço IPv4 traduzido no formato 0::FFFF:0:a.b.c.d ao *host* IPv6. Estes endereços são utilizados para o envio de pacotes por parte do *host* IPv6, sendo o endereço traduzido utilizado como origem e o mapeado para destino.

Quando o pacote chega ao SIIT, o cabeçalho é traduzido em IPv4. Os campos do cabeçalho IPv4 possuem valores correspondentes IPv6, ou podem ser obtidos automaticamente, como por exemplo o campo de atribuição de versão.

A tradução de cabeçalho IPv4 para IPv6 ocorre de forma similar, no entanto, ocasiona a perda de algumas funcionalidades do novo protocolo, como o cabeçalho de extensão *Authentication Header* [23].

3.3.2. NAT-PT

O NAT-PT (Network *Address Translation – Protocol Translation*) é mais um tradutor IPv6/IPv4. Descrito na RFC 2766, ele permite à dispositivos IPv6 nativos o acesso à dispositivos IPv4, e vice-versa.

Um dispositivo NAT-PT, como um *gateway*, reside na fronteira entre uma rede IPv4 e IPv6, mantendo um conjunto de endereços IPv4 públicos que serão utilizados na atribuição de dispositivos IPv6 de forma dinâmica. O processo de tradução de endereço e cabeçalho segue os mecanismos definidos anteriormente no SIIT, diferenciando por este tradutor manter o estado do mapeamento dos endereços enquanto dura a sessão [24].

Um acesso de um *host* IPv6 à outro IPv4 é obtido conforme mostra a figura:

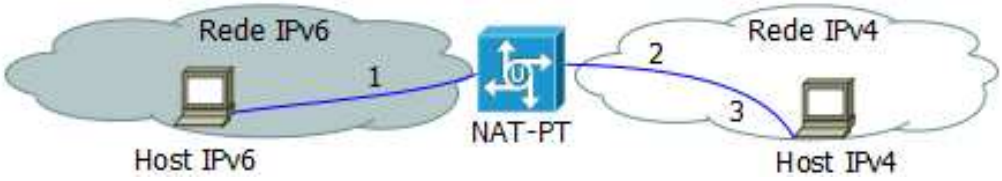

Figura 3.14 – Tradução NAT-PT

- 1 - O *host* IPv6 envia um pacote ao gateway NAT-PT com o prefixo ::/96 adicionado ao endereço IPv4 de destino, isto é necessário para que o roteador reconheça o tipo de comunicação realizada.
- 2 - O roteador ao receber o pacote mapeia o endereço do *host* IPv6 para um endereço IPv4 público, traduz o cabeçalho para IPv4 e o envia à seu destino.
- 3 – Para que o *host* IPv4 possa transmitir uma resposta, o NAT-PT deve manter informações sobre a sessão, incluindo endereço IPv4 público e outros parâmetros para tradução. Caso este estado não exista, o pacote é silenciosamente descartado pelo NAT-PT.

A configuração padrão do NAT-PT garante apenas acesso unidirecional, isto implica que apenas *hosts* IPv6 podem iniciar a sessão. Para que a comunicação se torne bidirecional é incentivado o uso de *gateway* DNS-*Application Level Gateway* (DNS-ALG). Estes são capazes de traduzir endereços IPv6 em *DNS Queries* e responder ao seus endereços IPv4 vinculados, e vice-versa [24].

3.3.3. NAPT-PT

Também definido na RFC 2766, o *Network Address Port Translation – Packet Translation* diferencia-se por prover comunicação entre nós nativos IPv6 e IPv4 de uma forma transparente utilizando apenas um único endereço IPv4 público. Para isto, realiza a tradução de portas TCP/UDP dos *hosts* em portas TCP/UDP do endereço IPv4 registrado [24].

Enquanto o NAT-PT possui um número limitado de sessões, dependente do número de endereços IPv4 públicos disponíveis, o NAPT-PT é capaz de realizar 63.000 sessões TCP e 63.000 UDP por endereço IPv4 [24].

Um exemplo similar ao apresentado na RFC de definição será utilizado para demonstrar o funcionamento deste tradutor. Supondo que o endereço público IPv4 utilizado para mapear os endereços IPv6 seja 187.0.84.217, temos o seguinte cenário, em que o *host* IPv6 possui uma aplicação que deseja estabelecer uma conexão TCP com o *host* IPv4:

Figura 3.15 – Tradução NAPT-PT

- A comunicação tem inicio com o *host* IPv6 criando um pacote com endereço de origem FEDC:0:4137::44FF:AB26 (seu endereço IPv6 privado) e porta TCP 3850. O endereço de destino é configurado como PREFIXO::200.192.6.13 e porta TCP 30, sendo que PREFIXO é qualquer prefixo /32 pré determinado e anunciado pelo NAPT-PT à rede.
- Quando o gateway NAPT-PT recebe o pacote, inicia uma sessão atribuindo uma das portas do endereço público para a tradução do pacote. O pacote traduzido conterá como endereço de origem o endereço público 187.0.84.217 e porta TCP reservada 1200. Desta forma, o pacote é encaminhado ao *host* IPv4.
- O tráfego de retorno, oriundo do *host* Ipv4 e porta 30, será reconhecido pela sessão já iniciada. O pacote é então traduzido novamente e encaminhado para o *host* IPv6 com os seguintes endereços: Origem PREFIXO::200.192.6.13 e porta 30. Destino FEDC:0:4137::44FF:AB26 e porta 3850.

As sessões NAPT-PT são restritas a um serviço por servidor, através de um mapeamento estático TCP/UDP. Outra limitação esta no fato de que a abertura de conexão do NAPT-PT é unidirecional, assim como o NAT-PT padrão, impondo que os *hosts* IPv6 iniciem as sessões com os *hosts* IPv4..

3.3.4. BIS

Definido na RFC 2767, o BIS (*Bump in the Stack*) é um mecanismo de tradução baseado em pilha dupla, funcionando entre a camada de aplicação e a de rede com a adição de três módulos. A figura a seguir ilustra este mecanismo [25]:

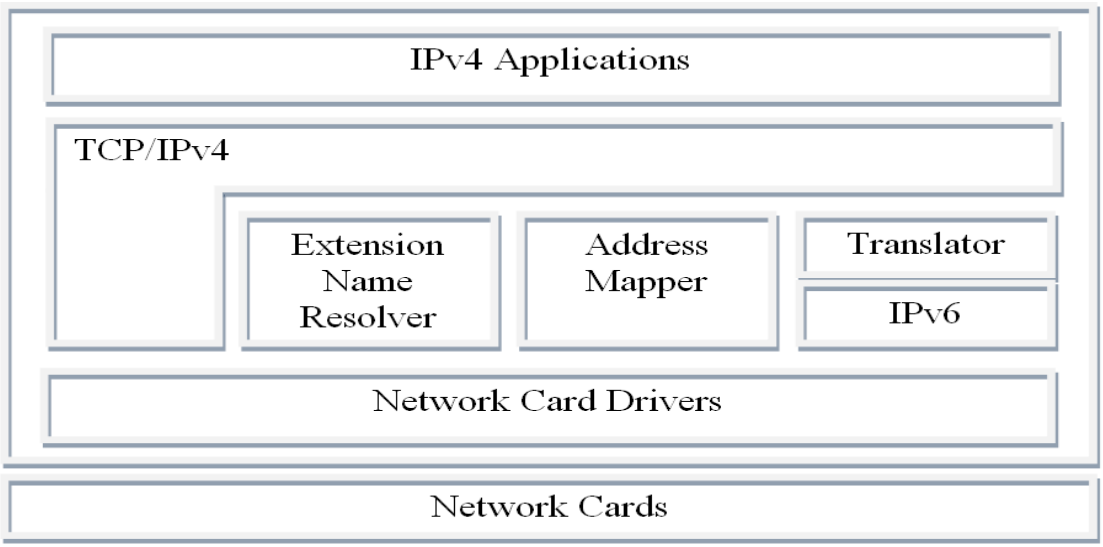

Figura 3.16 – Tradução BIS

Os três módulos inseridos possuem as seguintes funções:

- *Translator*: Utiliza o mecanismo de SIIT para realizar a tradução IPv4 em IPv6 e vice-versa.
- *Extension Name Resolver*: Atua nas *queries* DNS, de forma que se o DNS retorna um registro do tipo AAAA, o *Resolver* requisita ao *address mapper* um endereço IPv4 correspondente ao IPv6.
- *Address Mapper:* Mantém uma porção de endereços IPv4 privados à serem associados à endereços IPv6, conforme necessidade do *Resolver*.

O BIS possibilita aos softwares não adaptados ao IPv6, conseguir conectividade sobre o novo protocolo. Tal tarefa é desempenhada da seguinte forma: O software ao realizar uma consulta DNS sobre um dispositivo IPv6, recebe do BIS um endereço IPv4 privado para representar tal dispositivo. Deste modo, o software pode utilizar o endereço normalmente. Os pacotes destinados a este endereço IPv4 são interceptados pelo BIS, que utiliza o mecanismo de SIIT para traduzi-los e enviá-los à seu destino IPv6. A ação de volta acontece de forma similar, com o BIS traduzindo os pacotes para IPv4.

O mecanismo BIS pode ser útil na fase inicial de implantação, onde as aplicações não foram modificadas para operar com o IPv6 ou não podem ser atualizadas por algum motivo. O BIS, no entanto, apresenta algumas limitações. A comunicação é restringida a um sentido único, partindo de um *host* IPv4 à outro IPv6. Mesmo para comunicação entre *hosts* IPv4, a utilização de mecanismos adicionais de tradução em

algum ponto das aplicações envolvidas é necessária. Além de não funcionar em comunicações *multicast* [25].

3.3.5. BIA

O *Bump-in-the-*API possui o mesmo propósito do BIS, fazer com que aplicações IPv4 comuniquem-se com dispositivos IPv6, sem qualquer modificação na aplicação. No entanto, enquanto o BIS funciona em dispositivos apenas IPv4, o BIA requer que o dispositivo possua as duas versões do protocolo IP.

O BIA age inserindo uma API de tradução entre o *socket* API e os módulos TCP/IP da pilha do dispositivo, com a intenção de traduzir as funções do *socket* IPv4 em funções do *socket* IPv6, e vice-versa, garantindo a comunicação entre aplicações IPv4 e IPv6. De acordo com a RFC 3338 de definição, a API de tradução consiste em três módulos, conforme mostra a figura a seguir [26]:

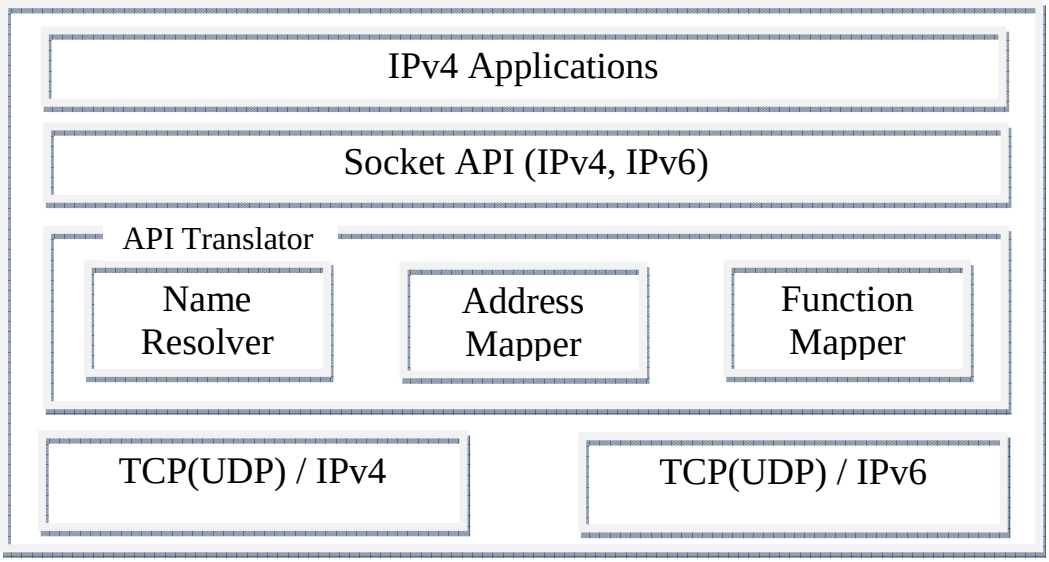

Figura 3.17 – Tradução BIA

Os módulos *Name Resolver* e *Address Mapper* funcionam da mesma maneira do BIS, o módulo *Function Mapper* intercepta as chamadas de funções *socket* IPv4 e invoca as chamadas correspondentes de funções *socket* IPv6, e vice-versa.

Apesar de atuar de forma semelhante ao BIS, este mecanismo se difere por suas funções da livraria terem conhecimento dos falsos endereços utilizados,

traduzindo-os para endereços IPv6. E sobressai sobre o mesmo por suas aplicações não introduzirem um *overhead* na tradução dos cabeçalhos dos pacotes. [26].

3.3.6. *SOCKS*

Socks é uma técnica de tradução baseada em seu protocolo homônimo definido em [27], cujo objetivo deste protocolo é assegurar que aplicações do tipo cliente-servidor, tanto TCP quanto UDP, funcionem via um servidor de *proxy*.

A técnica de tradução é composta por um *gateway Socks*, que utiliza pilha-dupla, e um *host* cliente que faz uso do software *SOCKS* LIB entre as camadas de aplicação e transporte. A esquematização, baseada na RFC 3089, pode ser vista a seguir:

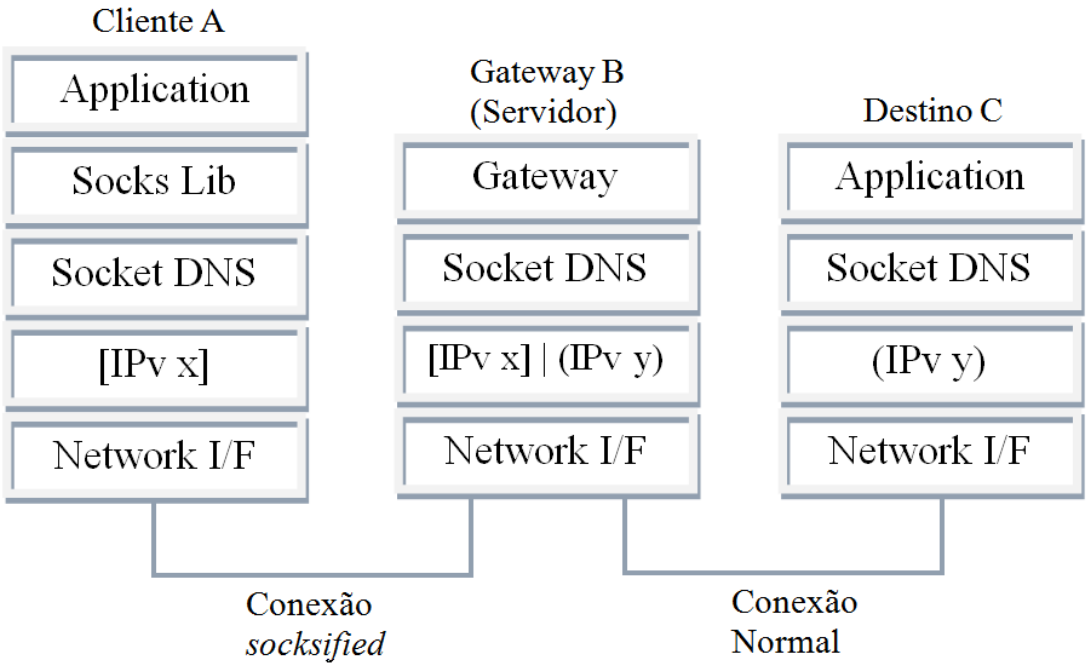

Figura 3.18 – Tradução *SOCKS*

O *SOCKS* LIB, presente no cliente A, monitora todas as requisições DNS oriundas do próprio cliente, interceptando-as e respondendo com endereços IPv4 falsos, estes endereços são então mapeados em uma tabela de resolução de nomes. Quando o cliente realiza uma chamada a API de conexão, o SOCKS LIB substitui o endereço falso usado pelo original, envia um pacote denominado *socksified* ao Gateway B, que atua como *Proxy* e realiza então a pesquisa DNS original. De acordo com o tipo de registro obtido,

AAAA para IPv6 e A para Ipv4, o Gateway B abre um *socket* para comunicação com o Destino C [28].

A técnica de SOCKS possui comunicação bidirecional nativa, ou seja, permite que *host* IPv4 e IPv6 iniciem sessões. Entretanto, possui o incômodo de se utilizar endereços IPv4 públicos.

3.3.7. ALG

Application Level Gateway, ou ALG, permite a aplicações de dispositivos atuando por de trás de um NAT ou firewall acesso externo a rede. Em redes IPv6, um dispositivo ALG habilitado com pilha dupla, pode ser utilizado para estabelecer conexões com redes IPv4 [24].

O uso da técnica, exibido na imagem a seguir, é bastante simples. Um dispositivo que busca comunicação com outro de versão diferente, necessita apenas iniciar a conexão com o ALG, que então realiza uma conexão com o dispositivo destino, retransmitindo todas as requisições de entrada e saída de dados:

Figura 3.19 – Tradução ALG

3.3.8. TRT

O *Transport Relay Translator* é proposto na RFC 3142, como um tradutor atuante na camada de transporte, permitindo que dispositivos nativos IPv6 troquem tráfego (TCP ou UDP) com dispositivos nativos IPv4. Este mecanismo possui a vantagem de poder ser implantando sem modificações extras tantos nos *hosts* IPv6 quanto nos IPv4. Ele apenas necessita de um dispositivo pilha dupla inserido em um ponto intermediário da rede [29].

Para que um dispositivo IPv6 se comunique com outro IPv4 ele deve inserir um prefixo falso ao endereço IPv4 no qual deseja se comunicar. O pacote contendo

tal prefixo é interceptado quando passa pelo TRT, em seguida traduzido e remetido ao seu destino em um pacote TCP ou UDP. Este mecanismo é apresentado na figura abaixo, onde o *host* IPv6 insere o Prefixo FEC:0:0:1::/64 ao endereço IPv4 10.1.1.1 de destino [29]:

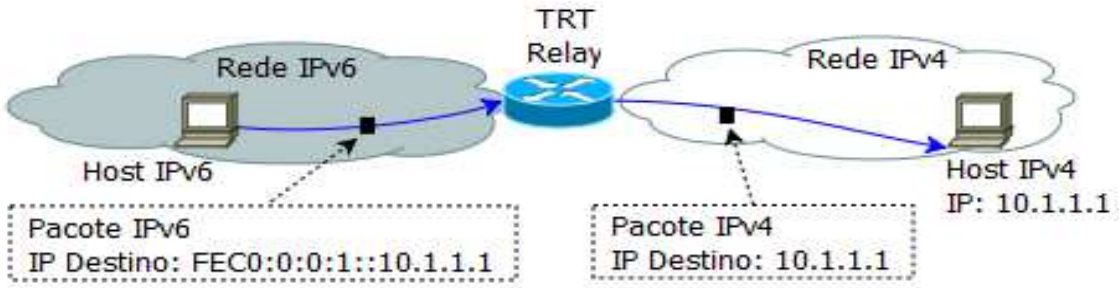

Figura 3.20 – Tradução TRT

Apesar da simplicidade, o mecanismo de TRT cobre a maioria das aplicações utilizadas (HTTP, SMTP, SSH e outros), e possui alta escalabilidade. Múltiplos sistemas TRTs podem ser utilizados em conjuntos através da configuração de diferentes prefixo falsos, onde cada TRT fica responsável por interceptar um prefixo pré-definido [29].

3.4. Síntese das Técnicas de Transição

As técnicas apresentadas possibilitam inúmeras combinações e formas de se garantir conectividade meio ao novo protocolo IP. A escolha de uma delas esta diretamente relacionada ao seu domínio de aplicabilidade e as suas características, ou seja, ao fazer uso de uma técnica de transição, ela deve ser capaz de prover a interoperabilidade entre os protocolos e atender as eventuais necessidades da rede, como: manutenção da topologia, escalabilidade, configurações de segurança, etc.

A mais simples delas, Pilha Dupla, é a solução de transição de maior uso, como afirma [30]. Isolada é bastante limitada, no entanto, unida à outras técnicas pode criar uma solução completa. A tabela a seguir sintetiza esta técnica:

Tabela 3.1 – Síntese da Técnica de Pilha Dupla

	Pilha Dupla
Aplicabilidade	• Dispositivos que necessitam interagir com outros de ambas as versões.
Vantagens	• Permite implantação gradual por setores. • Após o período de transição, basta desabilitar a pilha IPv4. • Permite que o dispositivo envie e receba pacotes IPv4 e IPv6
Desvantagens	• Exige readequação de elementos da infra-estrutura da rede, como serviço DNS. • A dupla camada de protocolo demanda maior poder de processamento e uso de memória, assim como espaço para alocação de tabelas de roteamento.

Os mecanismos baseados em Tunelamento tem sido amplamente utilizados em testes durante a fase inicial de implantação, como afirma [12]. Dentre todos, o 6to4 é o que possui maior nível de performance e adaptabilidade, por isto, é tido normalmente como a primeira escolha dentre os elementos desta categoria [30][31]. Mesmo sendo o mais eficiente, o 6to4 não abrange todas as exigências que uma rede pode ter, por exemplo, a existência de um NAT. Entre os mecanismos de tunelamento o único que consegue ultrapassar um NAT, desde que utilizado de forma isolada, é o Teredo, no entanto, seu uso somente é encorajado neste caso, por despender de mais processamento na conversão dos pacotes em UDP.

A técnica Tunelamento, de forma geral, possui as seguintes características:

Tabela 3.2 – Síntese da Técnica de Tunelamento

	Tunelamento
Aplicabilidade	• Casos em que se deseja obter tráfego IPv6, mas no entanto, a infra-estrutura de roteamento utilizada é a IPv4.
Vantagens	• Não há necessidade de mudança nos mecanismo de roteamento • Permite a utilização em diversas topologias.
Desvantagens	• Acrescenta carga adicional ao roteador. Cada ponto de entrada ou saída do túnel exige tempo e poder de processamento para realizar o encapsulamento e o desencapsulamento dos pacotes.

Sendo que os mecanismo de tunelamento herdam estas caracteristicas e definem as próprias:

Tabela 3.3 – Sínteses dos mecanismo de Tunelamento

Túnel Manual	Aplicabilidade	• *Hosts*/Domínio IPv6 que buscam comunicar entre si ou com uma rede nativa IPv6 através de uma rede IPv4.
	Vantagens	• Possui forma simples e eficaz. • Estabelece um link seguro como uma comunicação comum.
	Desvantagens	• Problemas de escalabilidade. • Não atravessa NAT
6to4	Aplicabilidade	• *Host*/Domínio isolados sobre uma rede IPv4 buscando comunicação com *hosts* Ipv4 ou rede nativa Ipv6.
	Vantagens	• Possui configuração simples do lado do cliente. • Túnel existe somente durante sessão
	Desvantagens	• Necessita de um *Relay* 6to4 para acesso à redes IPv6 nativas. • Não atravessa NAT
ISATAP	Aplicabilidade	• *Host* dentro de domínio IPv4 buscando comunicação com *hosts* do mesmo domínio, domínios separados ou então *hosts* em rede nativa IPv6.
	Vantagens	• Garante Conectividade IPv6 entre dispositivos em uma mesma rede IPv4.
	Desvantagens	• Necessita de um roteador ISATAP configurado em cada domínio. • Não atravessa NAT
Tunnel Broker	Aplicabilidade	• *Hosts*/Domínio IPv6 que buscam comunicar entre si ou com uma rede nativa IPv6 através de uma rede IPv4.
	Vantagens	• Possui forma simples e eficaz. • Execução através de um script.
	Desvantagens	• Depende de servidor web para criação de túneis. • Não atravessa NAT.
Teredo	Aplicabilidade	• *Host* Ipv6 localizado atrás de um NAT, buscando conectividade IPv6 por tunelamento de pacotes sobre UDP.
	Vantagens	• Tráfego passa pelo NAT de forma transparente.
	Desvantagens	• Necessita de muitos roteadores *relay* para garantia de eficiência. • Sobrecarga no controle e gestão da rede.

As soluções de transição baseadas na técnica de Tradução proporcionam mecanismos que asseguram a comunicação entre dispositivos que ostentam versões distintas do protocolo de internet com o custo de restringir as propriedades do IPv6 durante a tradução. Os dois principais representantes desta categoria, os mecanismo de NAT-PT e NAPT-PT, exigem alterações significativas em sua especificação para aplicação em redes genéricas, como afirma [32]. Ainda assim, apresentam um conjunto importante de soluções, assegurando que algumas redes não se tornem verdadeiras ilhas durante a transição. A síntese destes mecanismos é mostrada a seguir, na tabela 3.4.

O estudo das três classes de técnicas de transição permite concluir que o conhecimento sobre as mesmas será de grande importância durante todo o período de transição. A técnica de pilha dupla aparenta ser a mais vantajosa, no entanto, exige a readequação de elementos estruturais. Para os caso em que esta atualização não seja possível, os mecanismos de tunelamento apresentam uma solução eficiente. Restanto então, como uma última opção, os mecanismos baseado em tradução.

	Aplicabilidade	Vantagens	Desvantagens
SIIT	• *Host* somente IPv6 que busca comunicar com *host* somente Ipv4, e vice-versa.	• Independe da aplicação utilizada.	• Integridade Ponto a ponto não é mantida. • Não fornece tráfego transparente.
NAT-PT	• *Host* somente IPv6 que busca comunicar com *host* somente Ipv4, e vice-versa.	• Fornece tradutor transparente para o destino final.	• Configuração Básica permite abertura de conexão apenas no sentido unidirecional. • Número limitado de sessões, relativos ao *pool* de endereços IPv4.
NAPT-PT	• *Host* somente IPv6 que busca comunicar com *host* somente Ipv4, e vice-versa.	• É capaz de realizar 63.000 sessões TCP e 63.000 UDP por endereço IPv4.	• As sessões são restritas a serviço por servidor. • Não atravessa NAT.
BIS	• *Hosts* com software IPv4 buscando conectividade com *host* IPv6.	• Possibilita software não adaptados ao IPv6 conexão sobre o novo protocolo.	• Utiliza apenas comunicação *unicast*. • Não atravessa NAT
BIA	• *Hosts* com software IPv4 buscando conectividade com *host* IPv6.	• Possibilita software não adaptados ao IPv6 conexão sobre o novo protocolo. • Não depende da interface de rede. • Não introduz *overhead* na tradução dos cabeçalhos.	• Utiliza apenas comunicação *unicast*. • Não atravessa NAT.
SOCKS	• *Host* somente IPv6 que busca comunicar com *host* somente Ipv4, e vice-versa.	• Não necessita de modificações no sistema DNS • A segurança fim-a-fim é mantida, alguns itens do IPSEc podem ser utilizados.	• Não transpassa um NAT • Faz uso de endereços Ipv4 públicos.
ALG	• *Host* IPv6 ou IPv4 atrás de um NAT buscando conectividade.	• Atravessa NAT. • Pode trabalhar em conjunto com o NAT-PT.	• Sujeito a limitações pela falta de comunicação fim a fim.
TRT	• *Host* somente IPv6 que busca comunicar com *host* somente Ipv4, e vice-versa.	• Não necessita modificações extras nos *hosts* IPv4 e IPv6.	• Precisa de um TRT *stateful*. • Utiliza endereços IPv4 públicos.

Tabela 3.4 – Síntese dos Mecanismo de Transição

4. Implantação IPv6

Embora as especificações do IPv6 tenham sido lançadas em 1995, a delegação dos novos endereços somente iniciaram no dia 14 de julho de 1999, por meio de um anúncio oficial da IANA, organização que atua como autoridade máxima sobre a distribuição de endereços IP, autorizando a distribuição dos blocos às entidades regionais [33].

A delegação dos endereços é realizada de acordo as necessidades dos cinco órgãos regionais, denominados Regional Internet Registry (RIR), responsáveis pela alocação e administração dos endereços e demais recursos relacionados. Os cinco RIRs são identificados de acordo com a área de atuação:

- AfriNIC – África.
- APNIC – Ásia/Pacifico.
- ARIN – América do Norte.
- LACNIC – América Latina e algumas ilhas do Caribe.
- RIPE NCC – Europa, Oriente Médio e Ásia Central.

Apesar de o novo protocolo estar em execução há mais de uma década, a sua implantação ainda se encontra no estágio inicial na maioria das regiões. As previsões referentes ao esgotamento dos endereços IPv4 variaram ao passar do tempo, como afirma [34], no entanto, os últimos números disponibilizados pelos órgãos de registro confirmam a iminente exaustão dos endereços, colocando em risco o atual crescimento da Internet.

4.1. Escassez de Endereços IPv4

De acordo com anúncio oficial da *The Number Resource Organization* (NRO), entidade formada pelos cinco órgãos regionais, em 18 de outubro de 2010 o APNIC requisitou dois blocos de endereços IPv4 à IANA. Com esta alocação, a quantidade de endereços ainda disponíveis passou de 10% em Janeiro para menos de 5% após nove meses, representando mais de 200 milhões de endereços IPv4 atribuídos aos registros regionais de Internet neste curto período de tempo [35].

A quantidade de endereços reservados pode ser acompanhada através de documentos disponibilizados diariamente pelos registros regionais, destinados a

fornecer informações instantâneas sobre os recursos de numeração da Internet. O APNIC, coleta todos estes números, os seus e dos demais registros, e os disponibiliza graficamente através de uma ferramenta encontrada em [36]. Através desta ferramenta, obtivemos os números necessários para relacionar a quantidade de endereços IPv4 alocados pelos RIRs ao longo dos anos. A relação é apresentada por meio do gráfico abaixo:

Figura 4.1 – Alocação Cumulativa de Endereços IPv4 (25/10/2010)

Como se pode observar, no período de 1987 a 1993 a alocação de endereços obteve um crescimento acelerado, induzindo a criação de diversos prognósticos de exaustão dos recursos já nos primeiros anos da nova década. As previsões não se concretizaram devido ao desenvolvimento de algumas tecnologias que possibilitam uma sobrevida ao IPv4. São elas: CIDR(1993), DHCP (1997), NAT (1999). O *Classless Inter Domain Routing* aboliu o esquema de classes antes utilizado, permitindo definir tamanhos de blocos arbitrários, garantido melhor uso do espaço. A técnica de *Dynamic Host Configuration Protocol* possibilitou aos provedores de Internet reutilizarem endereços para conexões não permanentes. E por fim, a técnica de NAT garantiu que diversos dispositivos possam fazer uso da Internet utilizando apenas um endereço IPv4 público [4].

O efetivo uso destas técnicas é observado no gráfico com a notável desaceleração no período de 1993 a 2000. No entanto, a partir de 2001 a alocação volta a ter alta taxa de crescimento, fazendo com que no ano de 2010 ultrapasse os quatro bilhões de endereços, exigindo que a implantação do IPv6 seja acelerada.

4.2. IPv6 no Cenário Mundial

Os primeiros anos de execução do IPv6 se caracterizaram por seu baixo consumo. Fatores como custo de formação qualificada e aquisição de novos equipamentos contribuíram para o baixo índice de aceitação do novo protocolo. A adoção do IPv6 somente atingiu melhores níveis a partir do ano de 2003, é o que se pode observar a partir dos números de blocos de endereços IPv6/32 delegados aos cinco registradores regionais. A delegação cumulativa destes endereços, compreendida entre 1999 e agosto de 2010, é mostrada no seguinte gráfico:

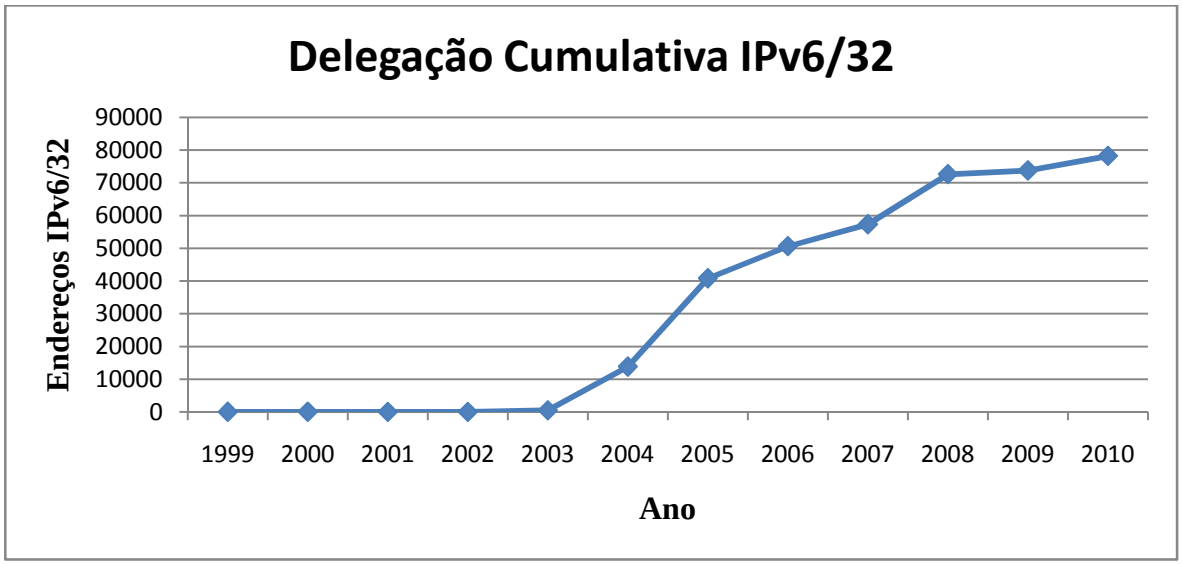

Figura 4.2 – Delegação Cumulativa de endereços IPv6/32 (25/10/2010)

Deste total de mais de 78 mil blocos, a maioria é distribuída entre os três registros regionais RIPE NCC, APNIC e ARIN, como demonstra o gráfico abaixo:

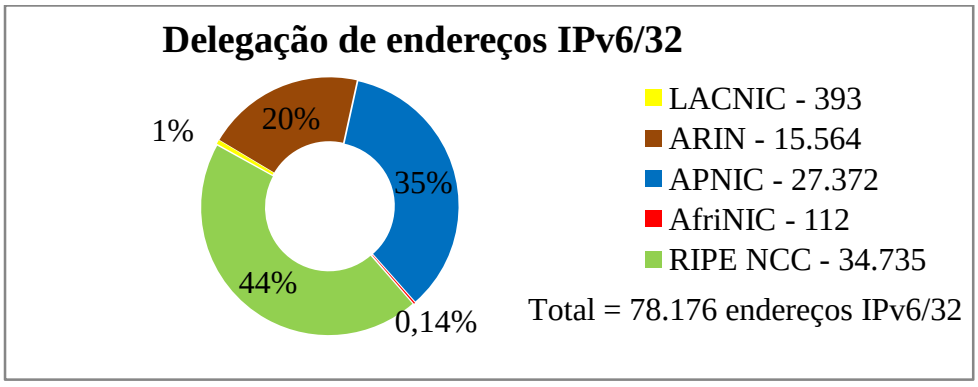

Figura 4.3 – Delegação IPv6 aos RIRs (25/10/2010)

O alto número de alocações do RIPE NCC pode ser atribuído as políticas de implantação IPv6 européias, sobretudo ao plano de ação previsto pela *Commission Of The European Communities*, descrito em [37]. Que consiste em tarefas a serem executadas por um período de três anos, como implementações testes para verificar o grau de funcionalidade e disponibilidade do IPv6. De modo que todas as tarefas sejam acompanhadas por uma comissão, responsável por disponibilizar contínuos relatórios sobre o progresso.

Segundo os dados provenientes da APNIC, 38.6% dos blocos de endereços IPv6/32 pertencentes a região estão alocados a domínios japoneses. O Governo japonês investe em ações pró-IPv6 desde o ano 2000, através de investimentos financeiros, redução de impostos sobre produtos com a nova versão do protocolo habilitada, estabelecendo parcerias e disponibilizando os resultados de pesquisas. As ações do governo, aliadas a iniciativas privadas fizeram do Japão a nação líder na adoção do IPv6, como afirma a análise realizada em [38].

O órgão de registro norte americano ARIN, ocupa apenas a terceira posição em relação à administração de blocos de endereço IPv6. Fato contrastante quando comparado a quantidade de endereços IPv4 que o bloco detém, superior a 50 % [36]. A grande quantidade de endereços da versão antiga do protocolo é atribuída a razões históricas, como o excesso de endereços destinados às instituições norte americanas. A terceira posição, no entanto, é atribuída à lenta adoção do novo protocolo no país, maior do grupo. Ainda que pouco se tenha feito nos Estados Unidos sobre a implantação IPv6, como afirma [39], o governo americano compreende a urgência do assunto e determina a utilização de IPv6 nativo em todos os servidores externos (web, e-mail, DNS, ISP e etc) até outubro de 2012 e estabelece para as redes internas o prazo até 2014.

Apesar de contarem com baixos números de alocações IPv6, comparado aos demais, os órgãos de registros AfriNIC e LACNIC vem se preparando há anos para a implantação, através de programas e cursos de capacitação da nova tecnologia. Os números apenas refletem o atraso tecnológico das regiões que formam estes grupos. Segundo [40], pouco menos de 11% da população africana possui acesso à Internet. Os países latino-americanos apresentam uma posição um pouco mais confortável, comparada a África, tendo mais de 34% da população acesso à grande rede, tendo o Brasil como o maior expoente da região.

4.3. IPv6 no Cenário Brasileiro

As iniciativas pró IPv6 no Brasil ainda são muito recentes. As alocações dos novos endereços passaram somente a ser feitas pelo Registro.br (responsável pelo registro de nomes e domínios brasileiros desde 1995) em dezembro de 2007, até então as alocações ocorriam diretamente com o LACNIC, implicando em uma série de tarefas burocráticas extras, como a assinatura de contratos em espanhol com uma empresa estrangeira. Com o órgão local intermediando, houve um aumento imediato pela requisição dos endereços [41]. Atualmente o Brasil é o principal "consumidor" de endereços IPv6 da região, como demonstra a figura a seguir:

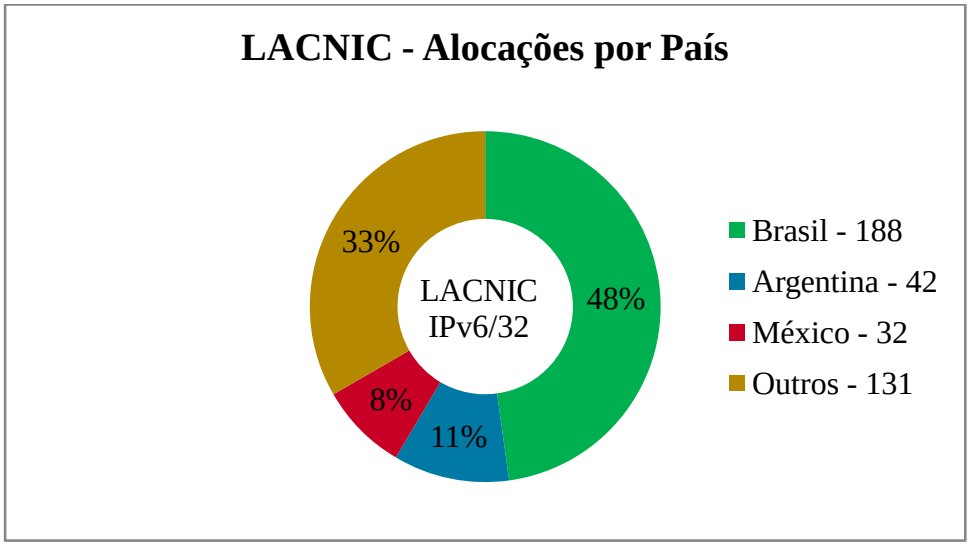

Figura 4.4 – Alocação de Endereços IPv6/32 – LACNIC (25/10/2010)

A quantidade de endereços alocados não implica necessariamente em uso destes recursos, no entanto sugere interesse dos brasileiros pela adoção da nova versão do protocolo IP. Isto se comprova também por meio de ações desempenhadas por órgãos civis, como realiza o CGI.br (Comitê gestor da Internet no Brasil). O CGI.br através do seu Centro de Estudos e Pesquisas Tecnológicas em Redes e Operações (CEPTRO.br), criou em 2008 o projeto IPv6.br, com o objetivo de disseminar o IPv6 pelo Brasil. Além de um site (www.ipv6.br) com informações e artigos, o projeto fornece cursos presenciais e a distância, buscando capacitar o maior contingente possível [41].

O governo brasileiro desde 2004, por meio do documento de referência da e-PING (conjunto de políticas que regulamentam a utilização de TI no governo federal), demonstra preocupação sobre o iminente fim de endereços IPv4 ao

determinar que todos os órgãos da administração pública devem planejar a imigração IPv6, limitando as novas contratações e atualizações de dispositivos de rede que ofereçam suporte as duas versões do protocolo IP [42].

4.4. IPv6 na Universidade Estadual de Londrina

A Universidade Estadual de Londrina (UEL) encontra-se no estágio inicial de implantação IPv6. Segundo Fernando Favero, Diretor de Suporte a Redes e Sistemas, a Universidade requisitou um bloco de endereços IPv6 no início deste ano. De acordo com a política de distribuição de endereços do Registro.br, os recursos são partilhados baseados no tipo de organização solicitante. O conjunto de redes da UEL constitui um sistema autônomo (AS), com o propósito de utilizar os endereços somente em sua própria infra-estrutura, desta forma ela é classificada na categoria de usuário final, recebendo um bloco /48.

A instituição ainda não utiliza estes endereços em seu tráfego interno, no entanto, um de seus *links* externos possui conexão IPv6 nativa com a Rede Nacional de Pesquisa (RNP). O *link* de 100 Mbps é mantido entre o Ponto de Presença Paranaense (PoP-PR), situado em Curitiba, e um roteador pilha dupla localizado na Universidade, garantindo acesso a Internet à dispositivos IPv4 e IPv6.

Apesar de não estarem previstas maiores ações de implantação IPv6 a curto prazo, a Universidade conta com membros do setor de TI aptos a trabalhar com a nova tecnologia, inclusive capacitados por cursos oferecidos pelo IPv6.br.

5. Conclusão

No que tange o IPv6, o novo protocolo foi elaborado de forma a suprir as necessidade de seu antecessor e atender as expectativas futuras da Internet. O seu espaço de endereçamento de 128 bits aliado aos mecanismos de QoS e segurança o tornam capaz de acomodar a atual estrutura da Internet e permitir seu crescimento.

O seu processo de implantação envolve diversos fatores, como capacitação de pessoal, aquisição ou atualização de equipamentos de infra-estrutura, que tornam a tarefa dispendiosa, contribuindo para que ocorra de forma gradual. Durante este processo é de extrema importância que as redes continuem compatíveis. Para isto, as técnicas de transição compõem-se de ferramentas fundamentais para o sucesso da transição.

A utilização dos mecanismos de transição ocorre desde o primeiro momento da implantação, no qual pequenas redes IPv6 encontram-se envolta a uma infra-estrutura predominantemente IPv4, até posteriormente, quando o quadro se inverterá e a maioria dos serviços e praticamente toda internet utilizará o novo protocolo e apenas poucas redes permanecerão utilizando o IPv4.

Para apontar o atual estágio global de implantação IPv6, foi utilizado como base o número de blocos de endereços IPv6/32 delegados para cada registro regional. A atribuição dos endereços não implica em uso, entretanto, fornece um parâmetro de indicação de interesse na adoção do novo protocolo.

A partir da análise destes números, pode-se observar o alto interesse da região asiática e européia em receber os novos endereços. O Japão concentra a maior parte dos blocos designados à região asiática, isto se deve as imediatas ações realizadas pelo governo, como os incentivos concedidos em produtos com a nova versão. De forma similar, acontece na Europa, através do contínuo incentivo da Comunidade Européia. Em ambos os casos ficou clara a importância do governo em fomentar as iniciativas para implantação do IPv6.

No Brasil, o governo reconhece a necessidade do novo protocolo, no entanto, pouco investe em ações efetivas. O Comitê Gestor da Internet no Brasil, um órgão civil, lidera os projetos em favor ao IPv6.

Exceto em alguns casos particulares, nota-se que a maioria das organizações e países, encontra-se no estágio inicial de implantação, como é o caso da

Universidade Estadual de Londrina, apresentado no capítulo quatro. Existe o consenso sobre a urgente necessidade de implantação IPv6, ainda mais com o fato de restarem menos de 5% de endereços IPv4 disponíveis, porém a maioria das ações consistem até o momento em treinamento de pessoal. Diversos fatores contribuem para isto, como o custo da troca de elementos estruturais da rede, ou mesmo o *upgrade* ou adaptação dos softwares, além da inexistência de serviços que funcionem exclusivamente com o novo protocolo.

O atual cenário de implantação permite concluir que a maioria das redes não estará apta a receber o novo protocolo quando o número de endereços IPv4 esgotar. Ainda por um tempo indeterminado, as duas versões continuarão existindo, de forma que os mecanismos de transição garantirão a interoperabilidade entre elas.

Sendo assim, espera-se que este trabalho possa servir de incentivo a discussões sobre a adoção do IPv6, sendo também útil à quem deseja obter informações a respeito da transição.

6. Bibliografia

[1] Barry M. Leiner *et al*, **A Brief History of the Internet**, SIGCOMM Comput. Commun. Rev. 39, 5, pp.22-31, Out. de 2009.

[2] Joseph Davies, **Understanding IPv6**, Editora Microsoft Press, 2ª Edição, 2008.

[3] Silvia Hagen, **IPv6 Essentials**, Editora O'Reilly 2ª Edição, 2006.

[4] Andrew S. Tanenbaum**, Redes de Computadores,** Editora Campus, 4ª edição, 2003.

[5] S. Bradner, A. Mankin, **The Recommendation for the IP Next Generation Protocol**, RFC 1752, Jan. de 1995.

[6] S. Deering, R. Hinden, **Internet Protocol, Version 6 (IPv6) Specification**, RFC 2460, Dez. de 1998.

[7] S. Deering, R. Hinden, **Internet Protocol Version 6 (IPv6) Addressing Architecture**, RFC 3513, Abr. de 2003.

[8] S. Kent, R. Atkinson, **Security Architecture for the Internet Protocol**, RFC 2401, Nov. de 1998.

[9] Dequan Yang, Xu Song, Qiao Guo, **Security on IPv6**, Advanced Computer Control (ICACC), 2010 2nd International Conference on, vol.3, no., pp.323-326, 27-29 de Mar. de 2010.

[10] Rodrigo Regis dos Santos; **Habilitando IPv6 em Sistemas Operacionais**. Disponível em: <http://www.ipv6.br/IPV6/ArtigoHabilitandoIPv6SO>. Acesso em: 06 Set. de 2010.

[11] E. Nordmark, R. Gilligan, **Basic Transition Mechanisms for IPv6 *Hosts* and Routers**, RFC 4213, Out. de 2005.

[12] Rodrigo Regis dos Santos, Antonio M. Moreiras, Ailton Soares da Rocha, **Curso IPv6 Básico**, Núcleo de Informação e Coordenação do ponto BR, 2010.

[13] S. Thomson, C. Huitema, V. Ksinant, M. Souissi, **DNS Extensions to Support IP Version 6,** RFC 3596, Out. de 2003.

[14] Cisco Systems, **Cisco IOS IPv6 Configuration Guide**, Release 12.4. Ultima atualização 30 de julho de 2010. Capitulo: Implementing Tunneling for IPv6.

[15] B. Carpenter, K. Moore, **Connection of IPv6 Domains via IPv4 Clounds**, RFC 3056, Fev. de 2001.

[16] C. Huitema, **An Anycast Prefix for 6to4 Relay Routers**, RFC 3068, Jun. de 2001.

[17] F. Templin, T. Gleeson, D. Thaler, **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)**, RFC 5214, Mar. de 2008.

[18] A. Durand, P. Fasano, I. Guardini, D. Lento, **IPv6 Tunnel Broker**, RFC 3053, Jan. de 2001.

[19] P. Srisuresh, M. Holdrege, **IP Network Address Translator (NAT) Terminology and Considerations**, RFC 2663, Agos. de 1999.

[20] C. Huitema, Teredo: **Tunneling IPv6 over UDP through Network Address Translation (NATs)**, RFC 4380, Fev. de 2006.

[21] The IPv6 Portal, **Teredo**, Disponível em: <http://www.ipv6tf.org/index.php?page=using/connectivity/teredo> Acesso em: 01 Out. de 2010.

[22] Masaki Nakajima, Nobumasu Kobayashi, **IPv4/IPv6 Translation Technology**, Fujitsu scientific and technical journal, vol. 40 no 1, pp. 159-169, 2004.

[23] E. Nordmark, **Stateless IP/ICMP Translation Algorithm (SIIT)**, RFC 2765, Fev. de 2000.

[24] G. Tsirtsis, P. Srisuresh, **Network Address Translation – Protocol Translation (NAT-PT)**, RFC 2766, Fev. de 2000.

[25] K. Tsuchiya, H. Higuchi, Y. Atarashi, **Dual Stack *Hosts* using the "Bump-In-the-Stack" Technique (BIS)**, RFC 2767, Fev. de 2000.

[26] S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, A. Durand, **Dual Stack *Hosts* Using "Bump-in-the-API" (BIA)**, RFC 3338, Out. de 2002.

[27] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones, **SOCKS Protocol Version 5**, RFC 1928, Mar. de 1996.

[28] H. Kitamura, **A SOCKS-based IPv6/IPv4 Gateway Mechanism**, RFC 3089, Abr. 2001.

[29] J. Hagino, K. Yamamoto, **An IPv6-to-IPv4 Transport Relay Translator**, RFC 3142, Jun. de 2001.

[30] D. Shalini Punithavathani, K. Sankaranarayanan, **IPv4/IPv6 Transition Mechanisms**, European Journal of Scientific Research, vol.34 no.1, pp.110-124, 2009

[31] Steinar H. Gunderson, **Global IPv6 statistics – Measuring the current state of IPv6 for ordinary users**, Google White Paper, Out. de 2008.

[32] C. Aoun, E. Davies, **Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status**, RFC 4966, Jul. de 2007.

[33] IANA, **Delegation of IPv6 address space**, Disponível em: <http://www.iana.org/reports/1999/ipv6-announcement.html> Acesso em: Jul. de 1999.

[34] Peter H. Salus, **One Byte at a Time: Internet Addressing**, The Internet Protocol Journal, vol 2, no 4, Dez. de 2009.

[35] NRO, **Remaining IPv4 Address Space Drops Below 5%**, Disponível em: <http://www.nro.net/media/remaining-ipv4-address-below-5.html> Acesso em: 19 Out. de 2010.

[36] APNIC, **Apstats**, Disponível em: <http://www.apnic.net/apstats> Acesso em: 23 Out. de 2010.

[37] Commission Of The European Communities, **Advancing The Internet: Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe**, Mai. de 2008.

[38] Patrick Grossetete, Ciprian Popoviciu, Fred Wettling, **Global IPv6 Strategies: From Business analysis to operational planning**, Editora Cisco Press, 2008.

[39] William Jackson, **Government takes the lead on IPv6 adoption**, Disponível em: <http://fcw.com/articles/2010/10/18/cybereye-gov-leads-on-ipv6.aspx> Acesso em: 26 Out. de 2010.

[40] Internet World Stats, **World Internet Usage and Populations Statistics**, Disponível em: <http://www.internetworldstats.com/stats.htm> Acesso em: 26 Out. de 2010.

[41] Ceptro.br, **IPv6.br – Projeto para a disseminação do IPv6 no Brasil**, Disponível em: <http://www.ceptro.br/CEPTRO/MenuCEPTROSPIPv6> Acesso em: 26 Out. de 2010.

[42] CGI.br, NIC.br, **Dimensões e características da Web brasileira: um estudo do gov.br**, 2010.