Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Leandro Bomfim Taranto

Técnicas de Transição para IPv6

Rio de Janeiro

2013

Leandro Bomfim Taranto

Técnicas de Transição para IPv6

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

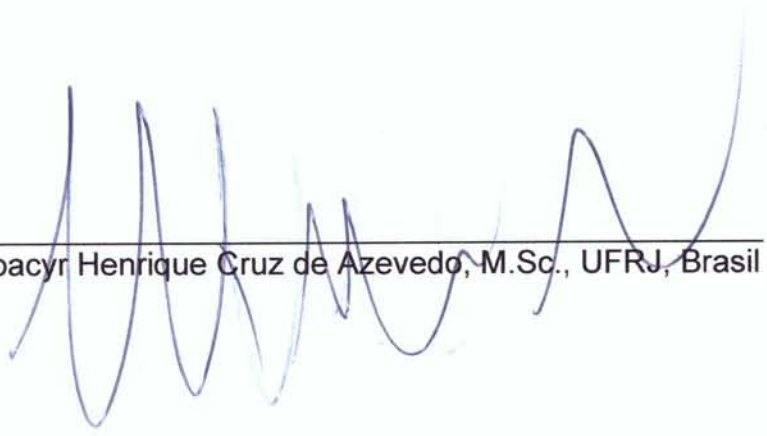
2013

Leandro Bomfim Taranto

Técnicas de Transição para IPv6

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Por ser uma tarefa muito árdua, dedico este trabalho a Deus, a meus Pais e a minha Esposa por ajudar-me a conseguir toda estrutura física e piscicológica para a elaboração desta monografia.

AGRADECIMENTOS

Gostaria de agradecer a minha esposa que contribuiu para as horas dedicadas ao meu estudo para elaboração desta monografia.

RESUMO

TARANTO, Leandro Bomfim. **Técnicas de Transição para IPv6**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

Para a comunicação dos computadores através da Internet é necessária a utilização do endereçamento IP (*Internet Protocol*). Atualmente está em uso na Internet o IPv4 (*Internet Protocol Version 4*). Com o esgotamento de endereços IPv4 no mundo desde fevereiro de 2011, onde os últimos blocos de endereçamento foram entregues para os órgãos regionais, segundo dados do IANA (*Internet Assined Number Authority*), e com crescimento exponecial da Internet e dos mais variados tipos de dispositivos conectados a ela, está fazendo com que ocorra um rápido esgotamento dos endereços ainda disponíveis. Com o objetivo de prover uma alternativa ao iminente fim dos endereços IPv4, foi criado o IPv6 (*Internet Protocol Version 6)*, que permite a criação de um número infinitamente maior de endereços públicos de Internet. Este trabalho tem como objetivo descrever as características e funcionalidades do protocolo IPv6 assim como as técnicas de transição do protocolo IPv4 para IPv6 que serão de extrema importância para empresas, instituições de ensino e para provedores de Internet. Este trabalho ainda destina-se a técnicos, engenheiros, analistas de sistemas que possam utilizar este documento como base para estudos e nos projetos que serão necessários para a utilização do IPv6 em suas áreas de atuação. Será mostrado também o cenário atual do IPv4 e IPv6 no Brasil e no mundo e um estudo de caso.

ABSTRACT

TARANTO, Leandro Bomfim. **Técnicas de Transição para IPv6**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

For computers communication in the Internet is needed to use IP address (Internet Protocol). Currently the Internet use IPv4 (Internet Protocol Version 4). IPv4 address exhaustion in the world happened since February 2011, when the distribution of the last remaining of IPv4 address blocks to each regional organization assignments, informed by IANA (Internet Assined Number Authority), and exponential growth of the Internet and all kinds of devices connected to it, happens the rapid depletion of the last remaining IPv4 addresses. In order to propose an alternative to the impending end of IPv4, IPv6 (Internet Protocol Version 6) was developed, that allows the creation of an infinitely larger number of public Internet addresses. This paper aims to describe the features and functionality of the IPv6 protocol as well as techniques for the transition from IPv4 to IPv6 will be extremely important to businesses, educational institutions and Internet service providers. This work also aims to technicians, engineers, systems analysts who will use this document as a basis for studies and projects that will be needed for the use of IPv6 in their fields. It is shown also the current scenario of IPv4 and IPv6 in Brazil and the world and a case of study.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AFTR	Address Family Transition Router
ALG	Application Layer Gateway
API	Application Programming Interface
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
AS	Autonomous System
BIA	Bump in the API
BIS	Bump in the Stack
CGN	Carrier Grade NAT
CIDR	Classless Inter-Domain Routing
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DNS	Domain Name System
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
IANA	Internet Asined Number Authority
ICMPv4	Internet Control Message Protocol Version 4
ICMPv6	Internet Control Message Protocol Version 6
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IID	Identificador da Interface
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
LACNIC	Latin American and Caribbean Internet Addresses Registry
LSN	Large Scale NAT
LSP	Label Switch Path
MBGP	Multiprotocol BGP
MIPv6	Mobile IPv6
MLD	Multicast Listener Discovery
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmit Unit
NAT	Network Address Translation
NTP	Network Time Protocol
P2P	Peer to Peer
PMTUD	Path MTU Discovery

QoS	Quality of Service
RA	Router Advertisement
RIR	Regional Internet Registry
ROAD	ROuting and Addressing
SIIT	Stateless IP/ICMP Translation Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
STUN	Simple Traversal of UDP through NATs
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol Internet Protocol
TRT	Transport Relay Translator
UDP	User Datagram Protocol
ULA	Unique Local Address
uPnP	Universal Plug and Play

SUMÁRIO

1 INTRODUÇÃO

Não há dúvida de que, em um futuro próximo, não serão somente as pessoas que estarão on-line. Dispositivos como carros, sensores residenciais, eletrodomésticos, enfim, qualquer aparelho estará de alguma forma conectado à Internet. Em poucos anos, conforme pesquisa divulgada pela empresa Cisco Systems, serão mais de 15 bilhões de dispositivos conectados à Internet acessando remotamente aplicações e grandes bancos de dados [7].

Acessaremos a Internet a partir de qualquer lugar, das formas mais variadas: tablets, computadores, smartphones cada vez mais poderosos, computadores de bordo e até óculos ou relógios com visores especiais. Além disso, surgirão novas demandas, geradas por aplicações industriais e residenciais, sistemas de transporte conectados à grande nuvem, serviços de telefonia integrados, rede de sensores, computação distribuída e jogos on-line.

Para a comunicação dos computadores através da Internet é necessária a utilização do endereçamento IP *(Internet Protocol)*. Atualmente está em uso na Internet o IPv4 (*Internet Protocol Version 4)*.

Desde fevereiro de 2011 os últimos blocos de endereços IPv4 foram entregues para os órgãos regionais, segundo dados do IANA *(Internet Assined Number Authority)* [8]. Com isto a Internet não poderá ser expandida e a adição de novos usuários e serviços não poderão ser comercializados por provedores de serviços, trazendo grandes impactos financeiros para grandes empresas e limitando as suas expansões no mercado de telecomunicações.

Com o objetivo de prover uma alternativa ao iminente fim dos endereços IPv4, foi criado o IPv6 (*Internet Protocol Version 6)*, que permite a criação de um número infinitamente maior de endereços públicos de Internet.

As diversas metodologias de implantação do IPv6 estabelecidas pelo IETF *(Internet Engineering Task Force)* e as suas técnicas existem a algum tempo, porém com o fim dos endereços IPv4 e com o avanço da Internet está sendo necessário colocar em prática esses recursos.

O IETF recomenda que seja realizada a migração do IPv4 para o IPv6 de forma gradual e que os dois protocolos coexistam por um determinado período até que não existam mais serviços ou dispositivos utilizando o IPv4.

Porém como os endereços IPv4 já se esgotaram será necessário acelerar este processo de implantação e utilizar novas técnicas de transição para IPv6, que serão descritas nesta monografia, para que os atuais serviços e dispositivos continuem a funcionar na Internet.

Este trabalho tem como objetivo descrever as limitações do protocolo IPv4 e detalhar as características e funcionalidades do protocolo IPv6 assim como as diferentes formas e técnicas de transição, discutindo alternativas, motivações e estatísticas de uso.

Neste trabalho será descrito o cenário atual do IPv4 e IPv6 no Brasil e no mundo, o funcionamento e arquitetura do IPv6, as técnicas de transição para o IPv6 disponíveis e um estudo de caso de implantação de uma destas técnicas que os provedores de serviços, principalmente no Brasil, deverão utilizar para que os serviços de Internet possam continuar a serem ofertados.

Este trabalho ainda destina-se para orientação de técnicos, engenheiros e analistas de sistemas que possam utilizar este documento como base para seus estudos e projetos em suas áreas de atuação que envolvam este tema.

2 O PROTOCOLO IPV4

Uma rede pode ser definida como um conjunto de computadores e outros equipamentos interligados e capazes de comunicarem-se utilizando um conjunto pré determinado de regras, ou “linguagem”, chamada de protocolo. O IPv4 é um protocolo que foi projetado para criar ligações entre diferentes redes, possibilitando a intercomunicação entre dispositivos nelas presentes. Uma interligação entre diversas redes é normalmente chamada de Internet [1]. Cada computador numa determinada Internet possui um número único, que o identifica dentre da mesma, chamado endereço IP.

O Protocolo Internet, na verdade, faz parte de um conjunto maior de protocolos, conhecidos por TCP/IP *(Transmission Control Protocol Internet Protocol)*. Esse conjunto é hoje utilizado também nas redes locais. É, na verdade, o padrão de fato utilizado como protocolo de comunicação para diversas aplicações, a começar pela Internet.

Atualmente os computadores se comunicam na Internet através do protocolo IPv4 que foi desenvolvido a mais de 20 anos e que, apesar de ser robusto, está ficando ultrapassado. O problema mais relevante dessa versão refere-se à crescente falta de endereços IPv4, que são usados por todas as máquinas conectadas à Internet.

2.1 O ESGOTAMENTO DE ENDEREÇOS IPV4

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

Tabela 1 – Classes de Endereçamento IPv4

Classe	Formato	Rede	Hosts
A	7 Bits Rede, 24 Bits Host	128	16.777.216
B	14 Bits Rede, 16 Bits Host	16.384	65.536
C	21 Bits Rede, 8 Bits Host	2.562.097.152	256

Embora o intuito dessa divisão tenha sido tornar a distribuição de endereços mais flexível, abrangendo redes de tamanhos variados, esse tipo de classificação mostrou-se ineficiente. Desta forma, a classe A atenderia um número muito pequeno de redes, mas ocupava metade de todos os endereços disponíveis; para endereçar 300 dispositivos em uma rede, seria necessário obter um bloco de endereços da classe B, desperdiçando assim quase o total dos 65 mil endereços; e os 256 endereços da classe C não supriam as necessidades da grande maioria das redes[1].

Outro fator que colaborava com o desperdício de endereços era o fato de que dezenas de faixas classe A foram atribuídas integralmente a grandes instituições como IBM, AT&T, Xerox, HP, Apple, MIT, Ford, Departamento de Defesa Americano, entre muitas outras, disponibilizando para cada uma 16.777.216 milhões de endereços. Além disso, 35 faixas de endereços classe A foram reservadas para usos específicos como *multicast, loopback* e uso futuro.

Em 1990, já existiam 313.000 *hosts* conectados à rede e estudos já apontavam para um colapso devido à falta de endereços. Outros problemas

também tornavam-se mais efetivos conforme a Internet evoluía, como o aumento da tabela de roteamento.

Devido ao ritmo de crescimento da Internet e da política de distribuição de endereços, em maio de 1992 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C já estavam alocados. Nesta época a rede já possuía 1.136.000 *hosts* conectados.

Em 1993, com a criação do protocolo HTTP *(Hypertext Transfer Protocol)* e a liberação por parte do Governo Americano para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de *hosts* em 1993 para mais de 26.000.000 de *hosts* em 1997.

2.1.1 **CIDR**

O IETF *(Internet Engineering Task Force)* passa a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e o problema do aumento da tabela de roteamento. Para isso, em novembro de 1991, é formado o grupo de trabalho ROAD *(ROuting and Addressing),* que apresenta como solução a estes problemas a utilização do CIDR *(Classless Inter-domain Routing),* definido na RFC 4632.

O CIDR tem como idéia básica o fim do uso de classes de endereços, permitindo a alocação de blocos de tamanho apropriado a real necessidade de cada rede; e a agregação de rotas, reduzindo o tamanho da tabela de roteamento.

Com o CIDR os blocos são referenciados como prefixo de redes. Por exemplo, no endereço a.b.c.d/x, os x bits mais significativos indicam o prefixo da

rede. Outra forma de indicar o prefixo é através de máscaras, onde a máscara 255.0.0.0 indica um prefixo /8, 255.255.0.0 indica um /16, e assim sucessivamente.

2.1.2 **NAT**

A NAT *(Network Address Translation),* foi outra técnica paliativa desenvolvida para resolver o problema do esgotamento dos endereços IPv4. Definida na RFC 3022, tem como idéia básica permitir que, com um único endereço IP, ou um pequeno número deles, vários hosts possam trafegar na Internet. Dentro de uma rede cada computador recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno. No entanto, quando um pacote precisa ser roteado para fora da rede, uma tradução de endereço é realizada, convertendo endereços IP privados em endereços IP públicos globalmente únicos.

Para tornar possível este esquema utilizam-se os três intervalos de endereços IP declarados como privados na RFC 1918, sendo que a única regra de utilização é que nenhum pacote contendo estes endereços pode trafegar na Internet pública.

A utilização da NAT mostrou-se eficiente no que diz respeito a economia de endereços IP, além de apresentar alguns outros aspectos positivos, como facilitar a numeração interna das redes, ocultar a topologia das redes e só permitir a entrada de pacotes gerados em resposta a um pedido da rede. No entanto, o uso da NAT apresenta inconvenientes que não compensam as vantagens oferecidas.

A NAT quebra o modelo fim-a-fim da Internet, não permitindo conexões diretas entre dois hosts, o que dificulta o funcionamento de uma série de

aplicações, como P2P *(peer-to-peer),* VoIP *(Voice over Internet Protocol) e* VPNs *(Virtual Private Network).*

Outro problema é a baixa escalabilidade, pois o número de conexões simultâneas é limitado, além de exigir um grande poder de processamento do dispositivo tradutor. O uso da NAT também impossibilita rastrear o caminho do pacote, através de ferramentas como *traceroute*, por exemplo, e dificulta a utilização de algumas técnicas de segurança como IPSec (*Internet Protocol Security*).

Além disso, seu uso passa uma falsa sensação de segurança, pois, apesar de não permitir a entrada de pacotes não autorizados, a NAT não realiza nenhum tipo de filtragem ou verificação nos pacotes que passa por ela.

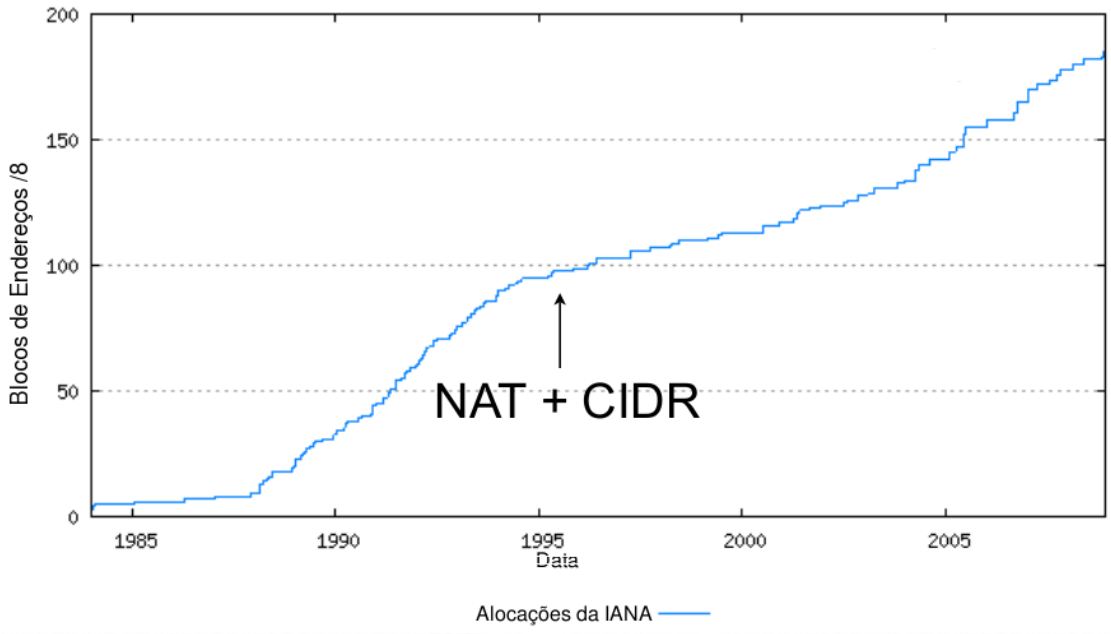


Figura 1 - Alocações da IANA

Embora estas soluções tenham diminuído a demanda por IPs, elas não foram suficientes para resolver os problemas decorrentes do crescimento da Internet. A adoção dessas técnicas reduziu em apenas 14% a quantidade de

blocos de endereços solicitados à IANA e a curva de crescimento da Internet continuava apresentando um aumento exponencial (figura 1).

Essas medidas, na verdade, serviram para que houvesse mais tempo para se desenvolver uma nova versão do IP, que fosse baseada nos princípios que fizeram o sucesso do IPv4, porém que fosse capaz de suprir as falhas apresentadas por ele [1].

2.1.3 **DHCP**

Outra solução, apresentada na RFC 2131 foi o protocolo DHCP *(Dynamic Host Configuration Protocol).* Através do DHCP um host é capaz de obter um endereço IP automaticamente e adquirir informações adicionais como máscara de sub-rede, endereço do roteador padrão e o endereço do servidor DNS (*Domain Name System*) local.

O DHCP tem sido muito utilizado por parte dos ISPs *(Internet Service Provider)* por permitir a atribuição de endereços IP temporários a seus clientes conectados. Desta forma, torna-se desnecessário obter um endereço para cada cliente, devendo-se apenas designar endereços dinamicamente através de seu servidor DHCP. Este servidor terá uma lista de endereços IP disponíveis, e toda vez que um novo cliente se conectar à rede lhe será designado um desses endereço de forma arbitrária e, no momento que o cliente se desconecta, o endereço é liberado e pode ser alocado a outro cliente.

2.2 O CENÁRIO NACIONAL E MUNDIAL

O estoque de endereços IPv4 central está esgotado depois da IANA ceder o último dos seus chamados blocos “/8” (cada um com cerca de 16 milhões de endereços). Assim os RIRs (*Regional Internet Registry*) não terão qualquer fornecimento adicional após terem cumprido as solicitações dos seus clientes.

No Brasil, o orgão que administra os endereços do Brasil é o NIC.br que é integrante do RIR LACNIC (*Latin American and Caribbean Internet Addresses Registry*), onde podemos observar na figura 2 que a quantidade de endereços IPv4 está reduzindo drasticamente, e o próprio NIC.br está incentivando o uso do IPv6 e restringindo o pedido de alocações de endereços IPv4, já que os mesmos estão com a previsão de término em meados de 2013.

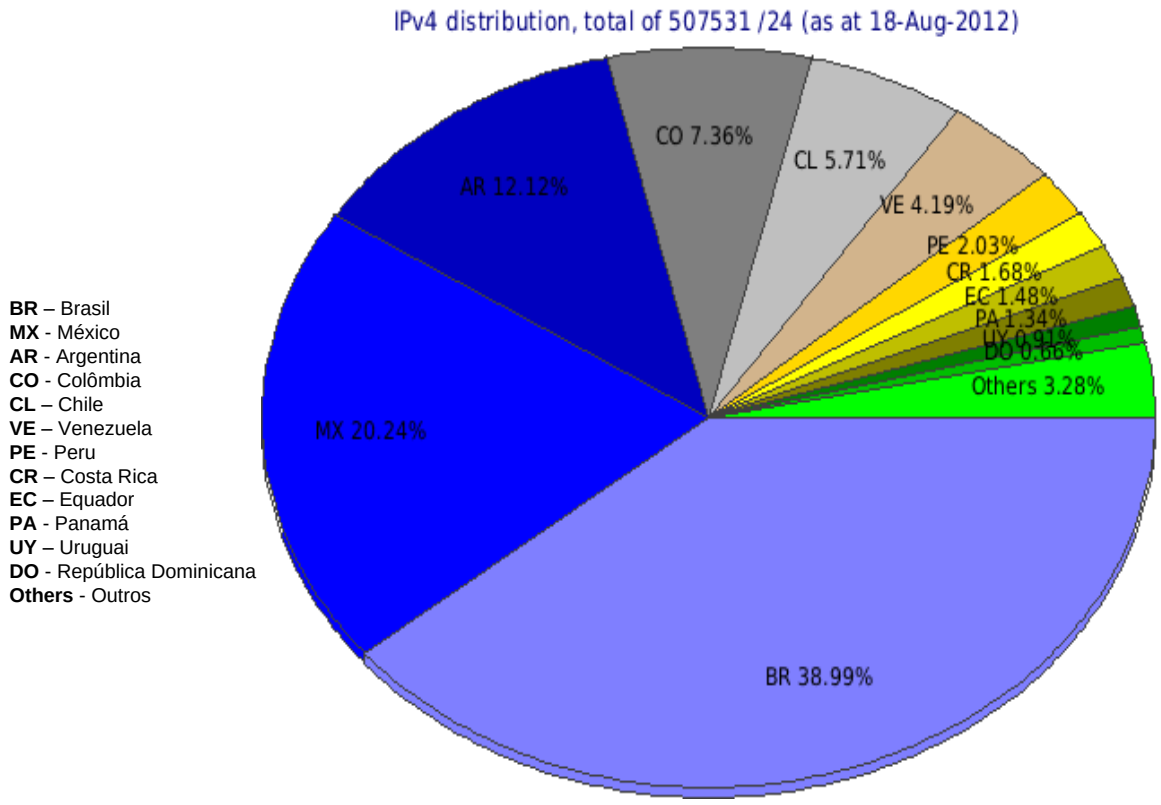


Figura 2 - Alocação IPv4 no Brasil

A previsão dos últimos endereços IPv4 que estarão disponíveis, podem ser vistos na figura 3 [5] , onde podemos observar que até 2015, caso o rítmo de alocação não aumente, ainda teremos endereços IPv4 disponíveis em alguns RIRs.

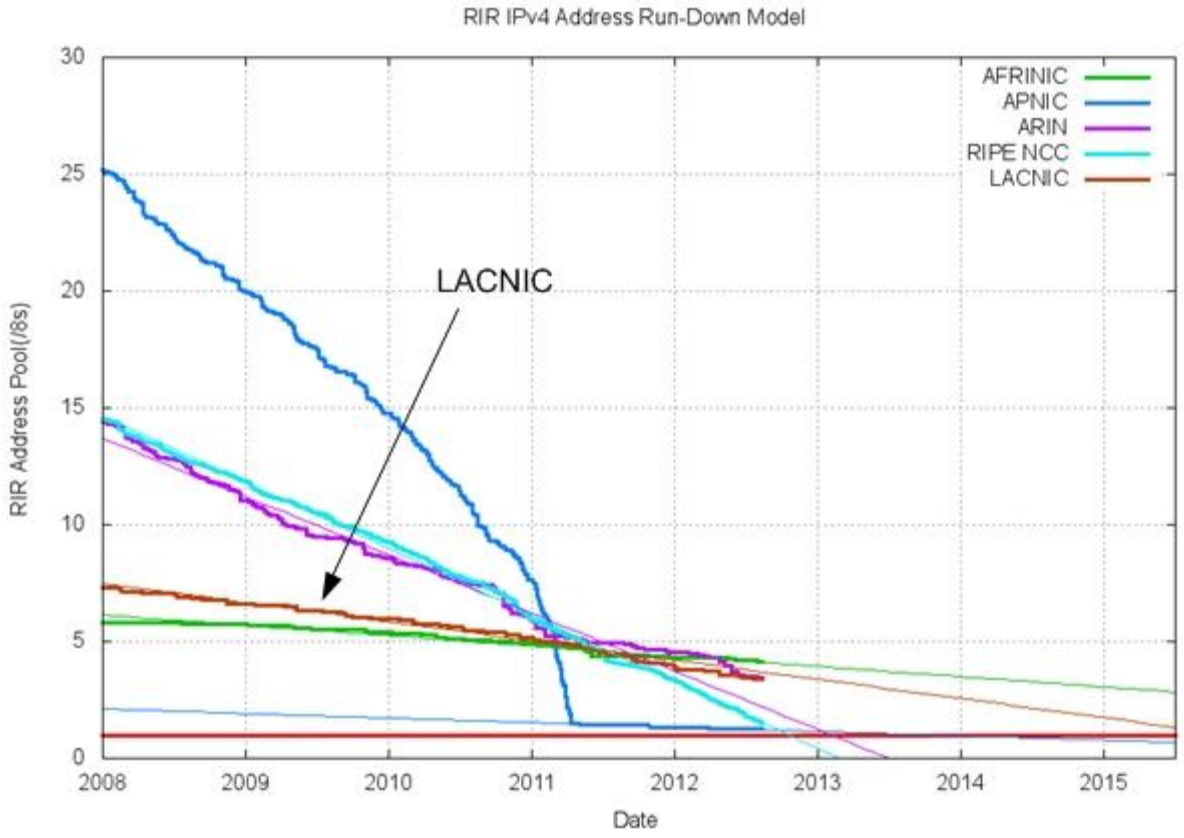


Figura 3 - Alocação de Endereços IPv4 no Mundo

3 O PROTOCOLO IPV6

O IPv6 foi desenvolvido para ser um passo evolutivo sobre o IPv4, sendo mesmo um requisito de projeto que a nova versão não fosse radicalmente igual a versão anterior. As funções que tivessem bom desempenho no IPv4 seriam mantidas, e as funções que não funcionassem bem seriam removidas.

O protocolo IPv6 foi criado não só para resolver problemas da quantidade de endereços, mas também para oferecer novos serviços e benefícios que não existiam o IPv4 ou que não eram utilizados de forma otimizada.

3.1 CABEÇALHO IPV6

Conforme a observado na figura 4, o cabeçalho do IPv6 está dividido nos seguintes campos:

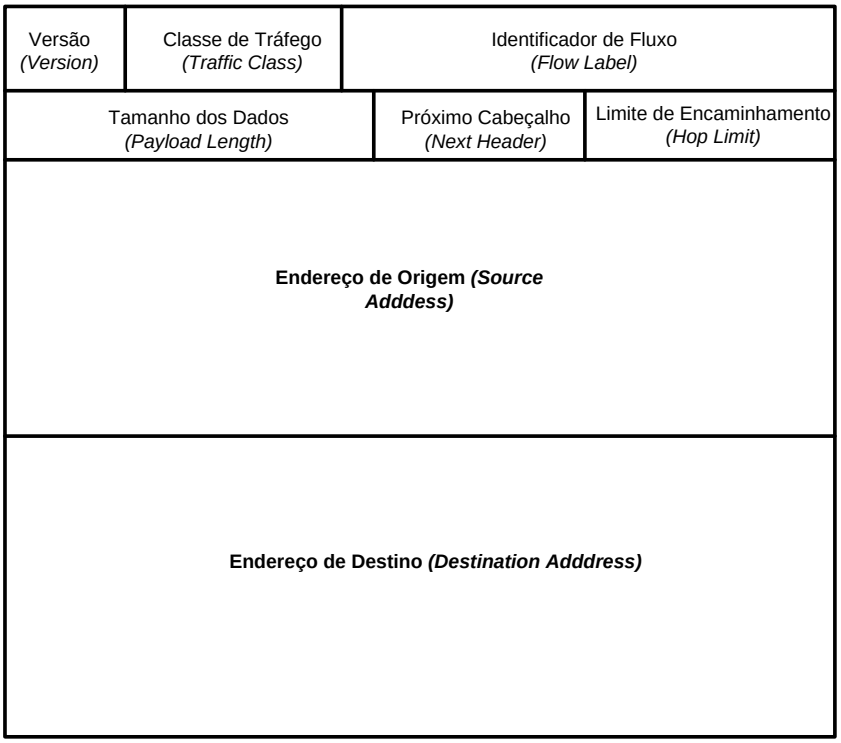


Figura 4 - Cabeçalho IPv6

Versão (4 bits) – Identifica a versão do protocolo utilizado. No caso, o valor desse campo é 6.

Classe de Tráfego (8 bits) – Identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço” do IPv4.

Identificador de Fluxo (20 bits) – Identifica pacotes do mesmo fluxo de comunicação. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.

Tamanho dos Dados (16 bits) – Indica o tamanho, em Bytes, apenas dos dados enviados junto ao cabeçalho IPv6. Substituiu o campo “Tamanho Total” do IPv4, que indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Contudo, o tamanho dos cabeçalhos de extensão também são somado nesse novo campo.

Próximo Cabeçalho (8 bits) – Identifica o cabeçalho de extensão que segue o atual. Ele foi renomeado (no IPv4 chamava-se “Protocolo”) para refletir a nova organização dos pacotes IPv6, uma vez que ele deixou de conter os valores referentes a outros protocolos, para indicar os tipos dos cabeçalhos de extensão.

Limite de Encaminhamento (8 bits) – Esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado. Ele padronizou o modo como o campo “Tempo de Vida” (TTL) do IPv4 vinha sendo utilizado, o qual diferia significativamente da descrição original que o definia como o tempo, em segundos, para o pacote ser descartado caso não chegasse à seu destino.

Endereço de origem (128 bits) – Indica o endereço de origem do pacote.

Endereço de Destino (128 bits) – Indica o endereço de destino do pacote.

Os cabeçalhos de extensão são opcionais e inseridos apenas entre o cabeçalho base IPv6 e a carga útil de dados (*payload*), se necessário, conforme pode-se observar na figura 5.

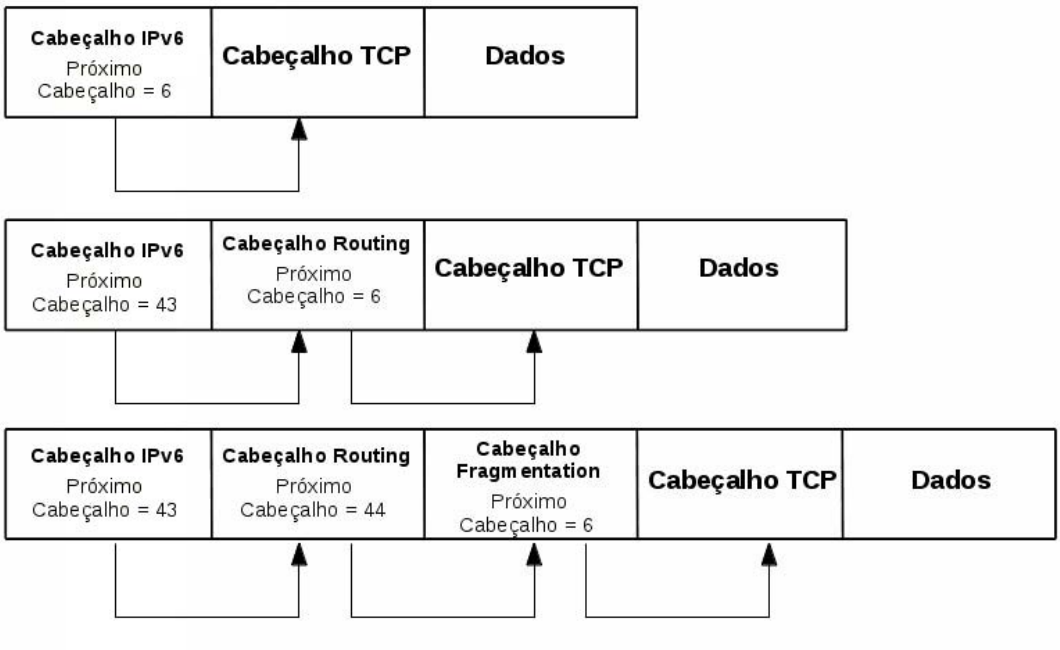


Figura 5 - Cabeçalhos de Extensão

As especificações do IPv6 definem seis cabeçalhos de extensão: *Hop-by-Hop Options, Destination Options, Routing, Fragmentation, Authentication Header e Encapsulating Security Payload.*

Hop-by-Hop options - informações gerais para os roteadores. Deve vir logo após o cabeçalho base IPv6, já que ele é o único cabeçalho a ser examinado por cada nó intermediário.

Routing - rota completa ou parcial a ser seguida.

Fragmentation - gerenciamento de fragmentos de datagrama.

Authentication - verificação da identidade do remetente e autenticação de datagrama IP (Algoritmo MD5 - *Message Digest number 5*).

Encrypted security payload - informação sobre a criptografia, integridade e confidencialidade de datagramas IP (Algoritmo DES - *Data Encryption Standard*).

Destination options - informação adicional sobre o destinatário.

3.2 ENDEREÇAMENTO IPV6

A disponibilidade de um número quase ilimitado de endereços IP é um dos maiores benefícios da implementação de redes IPv6. O IPv6 aumenta o número de bits do endereço por um fator 4, desta forma passa a ter 128 bits, possibilitando no futuro que outros dispositivos também possuam endereços IP. Assim, esses 128 bits fornecem aproximadamente 3,4 $x10^{38}$ possíveis endereços, o que seria suficiente para alocar nos dias de hoje cerca de 1.030 endereços por pessoas existentes na terra.

Existem três tipos de endereços IPv6: *anycast, unicast e multicast* conforme descritos abaixo:

Unicast – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface.

Anycast – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue à interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de

roteamento). Um endereço *anycast* é utilizado em comunicações de um para um de muitos.

Multicast – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Um endereço *multicast* é utilizado em comunicações de um para muitos.

Diferente do IPv4, no IPv6 não existe endereço *broadcast*, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6 essa função foi atribuída à tipos específicos de endereços *multicast*.

A representação dos endereços IPv6 divide o endereço em oito grupos de 16 bits, separando-os por " **:** " e escritos com dígitos hexadecimais:

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

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

Além disso, regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequência longa de zeros por "**::**". Por exemplo, o endereço **2001:0DB8:0000:0000:130F:0000:0000:140B** pode ser escrito como **2001:DB8:0:0:130F::140B** ou **2001:DB8::130F:0:0:140B**. Neste exemplo é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidades na representação do endereço. Se o endereço acima fosse escrito como **2001:DB8::130F::140B**, não seria possível determinar se ele corresponde a **2001:DB8:0:0:130F:0:0:140B**, a **2001:DB8:0:0:0:130F:0:140B** ou **2001:DB8:0:130F:0:0:0:140B**.

Esta abreviação pode ser feita também no fim ou no início do endereço, como ocorre em **2001:DB8:0:54:0:0:0:0** que pode ser escrito da **forma 2001:DB8:0:54::** [1].

Outra representação importante é a dos prefixos de rede. Em endereços IPv6 ela continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR. Esta notação é representada da forma "endereço-IPv6/tamanho do prefixo", onde "tamanho do prefixo" é um valor decimal que especifica a quantidade de bits contíguos à esquerda do endereço que compreendem o prefixo. O exemplo de prefixo de sub-rede apresentado a seguir indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede.

Prefixo 2001:db8:3003:2::/64

Prefixo global 2001:db8::/32

ID da sub-rede 3003:2

Esta representação também possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

Com relação a representação dos endereços IPv6 em URLs *(Uniform Resource Locators*), estes agora passam a ser representados entre colchetes. Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL. Observe os exemplos a seguir [1]:

http:///[2001:12ff:0:4::22]/index.html

http:///[2001:12ff:0:4::22]:8080

3.2.1 **Tipos de Endereços IPV6**

Como descrito anterirmente o endereço IPv6 possui três classificações de endereçamento, *Unicast, Anycast e Multicast*, que serão detalhados os tipos a seguir.

Global Unicast – equivalente aos endereços públicos IPv4, o endereço *global unicast* é globalmente roteável e acessível na Internet IPv6. Ele é constituído por três partes: o prefixo de roteamento global, utilizado para identificar o tamanho do bloco atribuído a uma rede; a identificação da sub-rede, utilizada para identificar um enlace em uma rede; e a identificação da interface, que deve identificar de forma única uma interface dentro de um enlace.

Link Local – podendo ser usado apenas no enlace específico onde a interface está conectada, o endereço *link local* é atribuído automaticamente utilizando o prefixo **FE80::/64**. Os 64 bits reservados para a identificação da interface são configurados utilizando o formato *IEEE EUI-64* [1]. Vale ressaltar que os roteadores não devem encaminhar para outros enlaces, pacotes que possuam como origem ou destino um endereço link-local.

ULA (Unique Local Address) – endereço com grande probabilidade de ser globalmente único, utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces. Um endereço ULA não deve ser roteável na Internet global.

Um endereço ULA, criado utiliza um ID global alocado pseudo-randomicamente, sendo composto das seguintes partes:

- **Prefixo: FC00::/7.**

• **Flag Local (L):** se o valor for 1 **(FD)** o prefixo é atribuído localmente. Se o valor for 0 **(FC)** o prefixo deve ser atribuído por uma organização central (ainda a definir).

• **Identificador global:** identificador de 40 bits usado para criar um prefixo globalmente único.

• **IID** (**Identificador da Interface):** identificador da interface de 64 bits.

Deste modo a estrutura de um endereço ULA é **FDUU:UUUU:UUUU:<ID da sub-rede>:<Id da interface>** onde "U" são os bits do identificador único, gerado aleatoriamente por um algoritmo específico.

Os **IID**, utilizados para distinguir as interfaces dentro de um enlace, devem ser únicos dentro do mesmo prefixo de sub-rede. O mesmo IID pode ser usado em múltiplas interfaces em um único nó, porém, elas dever estar associadas a diferentes sub-redes [1].

Normalmente utiliza-se um IID de 64 bits, que pode ser obtido de diversas formas. Ele pode ser configurado manualmente, a partir do mecanismo de autoconfiguração *stateless* do IPv6, a partir de servidores DHCPv6 (*Dynamic Host Configuration Protocol Version 6) stateful*, ou formados a partir de uma chave pública.

Endereço Não-Especificado (*Unspecified*): - é representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (equivalente ao endereço IPv4 *unspecified* 0.0.0.0). Ele nunca deve ser atribuído a nenhum nó, indicando apenas a ausência de um endereço. Ele pode, por exemplo, ser utilizado no campo Endereço de Origem de um pacote IPv6 enviado por um host durante o processo de inicialização, antes que este tenha seu endereço exclusivo determinado. O endereço *unspecified* não deve ser utilizado como endereço de destino de pacotes IPv6;

Endereço *Loopback*: representado pelo endereço *unicast* 0:0:0:0:0:0:0:1 ou ::1 (equivalente ao endereço IPv4 *loopback* 127.0.0.1). Este endereço é utilizado para referenciar a própria máquina, sendo muito utilizado para teste internos. Este tipo de endereço não deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 enviados para outros nós. Além disso, um pacote IPv6 com um endereço *loopback* como destino não pode ser enviado por um roteador IPv6, e caso um pacote recebido em uma interface possua um endereço *loopback* como destino, este deve ser descartado;

Endereços IPv4-mapeado: representado por 0:0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz, é usado para mapear um endereço IPv4 em um endereço IPv6 de 128-bit, onde wxyz representa os 32 bits do endereço IPv4, utilizando dígitos decimais. É aplicado em técnicas de transição para que nós IPv6 e IPv4 se comuniquem. Exemplo **::FFFF:192.168.100.1** .

IPv6 *anycast* - é utilizado para identificar um grupo de interfaces, porém, com a propriedade de que um pacote enviado a um endereço *anycast* é encaminhado apenas à interface do grupo mais próxima da origem do pacote.

Os endereços *anycast* são atribuídos a partir da faixa de endereços *unicast* e não há diferenças sintáticas entre eles. Portanto, um endereço *unicast* atribuído a mais de uma interface transforma-se em um endereço *anycast*, devendo-se, neste caso, configurar explicitamente os nós para que saibam que lhes foi atribuído um endereço *anycast*. Além disso, este endereço deve ser configurado nos roteadores como uma entrada separada (prefixo /128 – *host route*).

Este esquema de endereçamento pode ser utilizado para descobrir serviços na rede, como servidores DNS e proxies HTTP, garantindo a redundância desses serviços. Também pode ser utilizado para fazer balanceamento de

carga em situações onde múltiplos hosts ou roteadores provêem o mesmo serviço, para localizar roteadores que forneçam acesso a uma determinada sub-rede ou para localizar os Agentes de Origem em redes com suporte a mobilidade IPv6.

Todos os roteadores devem ter suporte ao endereço *anycast Subnet-Router*. Este tipo de endereço é formado pelo prefixo da sub-rede e pelo IID preenchido com zeros (ex.: 2001:db8:cafe:dad0::/64). Um pacote enviado para o endereço *Subnet-Router* será entregue para o roteador mais próximo da origem dentro da mesma sub-rede.

IPv6 *multicast* - são utilizados para identificar grupos de interfaces, sendo que cada interface pode pertencer a mais de um grupo. Os pacotes enviados para esses endereço são entregues a todas as interfaces que compõe o grupo. Os endereços *multicast* não devem ser utilizados como endereço de origem de um pacote.

Esses endereços derivam do bloco **FF00::/8**, onde o prefixo FF, que identifica um endereço *multicast*, é seguido por quatro bits que representam quatro flags e um valor de quatro bits que define o escopo do grupo *multicast*. Os 112 bits restantes são utilizados para identificar o grupo multicast.

Os *flags* são definidos da seguinte forma:

- O primeiro bit mais a esquerda é reservado e deve ser marcado com 0;
- ***Flag* R**: Se o valor for 1 indica que o endereço *multicast* .carrega. o endereço de um Ponto de Encontro (*Rendezvous Point*). Se o valor for 0, indica que não há um endereço de Ponto de Encontro embutido;

- ***Flag* P**: Se o valor for 1 indica que o endereço *multicast* é baseado em um prefixo de rede. Se o valor for 0 indica que o endereço não é baseado em um prefixo de rede;
- ***Flag* T**: Se o valor for 0 indica que o endereço *multicast* é permanente, ou seja, é atribuído pela IANA. Se o valor for 1 indica que o endereço *multicast* não é permanente, ou seja, é atribuído dinamicamente.

Os quatro bits que representam o escopo do endereço *multicast* são utilizados para delimitar a área de abrangência de um grupo *multicast.* Os valores atribuídos a esse campo são:

1 - abrange apenas a interface local;

2 - abrange os nós de um enlace;

3 - abrange os nós de uma sub-rede

4 - abrange a menor área que pode ser configurada manualmente;

5 - abrange os nós de um site;

8 - abrange vários sites de uma mesma organização;

E - abrange toda a Internet;

0, F - reservados;

6, 7, 9, A, B, C, D - não estão alocados.

Deste modo, um roteador ligado ao *backbone* da Internet não encaminhará pacotes com escopo menor do que 14 (E em hexa), por exemplo. No IPv4 o escopo de um grupo *multicast* é especificado através do campo TTL do cabeçalho.

Na tabela 2 podemos observar endereços *Multicast* definidos que são permanentes e utilizados por outros protocolos.

Tabela 2 - Endereços Multicast Permanentes

Endereço	Escopo	Descrição
FF01::1	Interface	Todas as interfaces em um nó (*all-nodes*)
FF01::2	Interface	Todos os roteadores em um nó (*all-routers*)
FF02::1	Enlace	Todos os nós do enlace (*all-nodes*)
FF02::2	Enlace	Todos os roteadores do enlace (*all-routers*)
FF02::5	Enlace	Roteadores OSFP
FF02::6	Enlace	Roteadores OSPF designados
FF02::9	Enlace	Roteadores RIP
FF02::D	Enlace	Roteadores PIM
FF02::1:2	Enlace	Agentes DHCP
FF02::FFXX:XXXX	Enlace	*Solicited-node*
FF05::2	Site	Todos os roteadores em um site
FF05::1:3	Site	Servidores DHCP em um site
FF05::1:4	Site	Agentes DHCPem um site
FF0X::101	Variado	NTP (Network Time Protocol)
FF0X::101	Variado	NTP (Network Time Protocol)

3.3 FUNCIONALIDADES

O protocolo IPv6 apresenta uma série de novas funcionalidades e outras aprimoradas em relação ao IPv4. A seguir serão descritas estas funcionalidades e suas características que tornam o IPv6 um protocolo de nova geração, não só pela sua quase infinita quantidade de endereços, mas como pelos seus novos atributos.

3.3.1 **ICMPV6**

Definido na RFC 4443 para ser utilizado com o IPv6, o ICMPv6 (*Internet Control Message Protocol Version 6*) é uma versão atualizada do ICMP (*Internet Control Message Protocol Version 4*) utilizado com IPv4.

Esta nova versão no ICMPv6, embora apresente as mesma funções que no ICMPv4, como reportar erros no processamento de pacotes e enviar mensagens sobre o *status* a as características da rede, é compatível com seu antecessor, apresentando agora um número maior de mensagens e funcionalidades.

O ICMPv6 é agora o responsável por realizar as funções dos protocolos ARP (*Address Resolution Protocol*), que mapeia os endereços da camada dois para IPs e vice-versa no IPv4, e do IGMP (*Internet Group Management Protocol*), que gerencia os membros dos grupos *multicast* no IPv4.

O valor no campo Próximo Cabeçalho, que indica a presença do protocolo ICMPv6, é 58, e o suporte a este protocolo deve ser implementado em todos os nós.

O ICMPv6 é um protocolo chave na arquitetura IPv6, visto que, além do gerenciamento dos grupos *multicast*, através do protocolo MLD (*Multicast Listener Discovery*), e da resolução de endereços da camada dois, suas mensagens são essenciais para o funcionamento do protocolo de Descoberta de Vizinhança (*Neighbor Discovery*), responsável por localizar roteadores vizinhos na rede, detectar mudanças de endereço no enlace, detectar endereços duplicados, etc.; no suporte à mobilidade, gerenciando Endereços de Origem dos *hosts* dinamicamente; e no processo de descoberta do menor MTU (*Maximum Transmit Unit*) no caminho de uma pacote até o destino.

3.3.2 **Descoberta de vizinhança**

Definido pela RFC4861, o protocolo de Descoberta de Vizinhança torna mais dinâmicos alguns processos de configuração de rede em relação ao IPv4, combinando as funções de protocolos como ARP, ICMP *Router Discovery* e ICMP *Redirect*, além de adicionar novos métodos não existentes.

O protocolo de Descoberta de Vizinhança do IPv6 é utilizado por *hosts* e roteadores para os seguintes propósitos:

- determinar o endereço MAC dos nós da rede;
- encontrar roteadores vizinhos;
- determinar prefixos e outras informações de configuração da rede;
- detectar endereços duplicados;
- determinar a acessibilidades dos roteadores;
- redirecionamento de pacotes;
- autoconfiguração de endereços.

3.3.3 **DHCPv6**

Definido na RFC 3315, o DHCPv6 é uma opção ao mecanismo de autoconfiguração *stateless* do IPv6, podendo ser utilizado quando não há roteadores na rede, ou quando seu uso for indicado nas *mensagens RA (Router Advertisement)*, sendo capaz de fornecer endereços IPv6 e diversos parâmetros de rede, como endereços de servidores DNS, NTP (*Network Time Protocol*), SIP (*Session Initiation Protocol*), etc.

No DHCPv6 a troca de mensagens entre cliente e servidor é realizada utilizando-se o protocolo UDP. Os clientes utilizam um endereço *link-local* para transmitir ou receber mensagens DHCPv6, enquanto que os servidores utilizam um endereço *multicast* reservado (**FF02::1:2** ou **FF05::1:3**) para receber mensagens dos clientes. Caso o cliente necessite enviar uma mensagem a um servidor que esteja fora de sua sub-rede é utilizado um *Relay* DHCPv6.

3.3.4 **Path MTU Discovery**

No IPv6 a fragmentação dos pacotes é realizada apenas na origem, não sendo permitida em roteadores intermediários. Este processo tem o intuito de reduzir o overhead do cálculo dos cabeçalhos alterados nos roteadores intermediários.

Para isso, é utilizado, no início do processo de fragmentação, o protocolo *Path MTU Discovery*, descrito na RFC 1981, que descobre de forma dinâmica qual o tamanho máximo permitido ao pacote, identificando previamente os MTUs de cada enlace no caminho até o destino. O protocolo PMTUD (*Path MTU Discovery*) deve ser suportado por todos os nós IPv6. No entanto, implementações mínimas de IPv6 podem omitir esse suporte, utilizando 1280 Bytes como tamanho máximo de pacote.

3.3.5 ***Jumbograms***

A RFC 2675 define uma opção do cabeçalho de extensão *Hop-By-Hop* chamada *Jumbo Payload*. Esta opção permitir envio de pacotes IPv6 com cargas úteis entre 65.536 e 4.294.967.295 Bytes de comprimento, conhecidos como *jumbograms*.

Ao enviar *jumbograms* o cabeçalho IPv6 trará os campos “Tamanho dos Dados” e “Próximo Cabeçalho” com o valor zero. Este último indicará que as opções do cabeçalho de extensão *Hop-By-Hop* devem ser processadas pelos nós, onde são indicados os tamanhos dos pacotes *jumbograms.*

3.3.6 **Gerenciamento de Grupos Multicast**

O gerenciamento dos grupos *multicast* no IPv6 é realizado pelo MLD, definido na RFC 2710. Este protocolo é o responsável por informar aos roteadores *multicast* locais o interesse de nós em fazer parte ou sair de um determinado grupo *multicast*. No IPv4 este trabalho é realizado pelo protocolo IGMP.

3.3.7 **DNS**

A base de dados de um servidor DNS pode armazenar tanto registros IPv6 quanto IPv4.

Um novo registro foi criado para armazenar os endereços IPv6 de 128 bits, o AAAA ou *quad-A* no serviço DNS. Sua função é traduzir nomes para endereços IPv6, equivalente ao registro A utilizado com o IPv4. Caso um *host*

possua mais de um endereço IPv6 ele terá um registro *quad-A* para cada endereço. Os registros são representados como segue:

Exemplo: **www.ipv6.br. IN A 200.160.4.22**

IN AAAA 2001:12ff:0:4::22

Para resolução de reverso foi adicionado o registro PTR ip6.arpa, responsável por traduzir endereços IPv6 em nomes. Em sua representação, omitir sequência de zeros não é permitido e o bit menos significativo é colocado mais a esquerda, como é possível observar no exemplo a seguir:

Exemplo:

22.4.160.200.in-addr.arpa PTR www.ipv6.br.

2.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2. ip6.arpa

PTR www.ipv6.br.

Os outros tipos de registro DNS não sofreram alterações, apenas foram adaptados para suportar o novo tamanho dos endereços.

3.3.8 **QoS**

O serviço QoS (*Quality of Service*) é tratado em IPv6 da mesma maneira que é tratado em IPv4, possuindo suporte por classe de serviço através do campo de tráfego e do modelo DiffServ (*Differentiated Services*). Entretanto, o cabeçalho IPv6 tem um novo campo chamado *flow label*, que pode conter um rótulo identificando um fluxo específico de dados. Desta forma, o nó fonte gera uma rota de fluxo com rótulo disponibilizando QoS nesse caminho, onde cada roteador do caminho toma ações baseadas por esse rótulo.

No cabeçalho, os campos "Traffic Class" e "Flow Label" foram criados especialmente para facilitar o desenvolvimento de protocolos para controle em tempo real, de forma a permitir a implementação de aplicações multimídia e com a integração de serviços de dados, voz e vídeo em tempo real.

3.3.9 **Mobilidade**

O suporte à mobilidade permite que um dispositivo móvel se desloque de uma rede para outra sem necessidade de alterar seu endereço IP de origem, tornando a movimentação entre redes invisível para os protocolos das camadas superiores. Com isso, todos os pacotes enviados para este nó móvel continuarão sendo encaminhados a ele usando o endereço de origem.

No suporte à mobilidade IPv6 existem alguns componentes chave para o seu funcionamento:

Nó Móvel – dispositivo que pode mudar de uma rede para outra enquanto continua recebendo pacotes através de seu Endereço de Origem;

Rede de Origem – rede que atribui o Endereço de Origem ao Nó Móvel;

Agente de Origem – roteador localizado na Rede de Origem que mantém a associação entre o Endereço de Origem e o Endereço Remoto do Nó Móvel;

Endereço de Origem – endereço global unicast atribuído pela Rede de Origem ao Nó Móvel. É utilizado como endereço permanente para o qual os pacotes são encaminhados;

Rede Remota – qualquer rede, diferente da origem, onde o Nó Móvel se encontra;

Endereço Remoto – endereço global *unicast* atribuído ao Nó Móvel pela Rede Remota;

Nó Correspondente – nó que se comunica com o Nó Móvel. Este pode ser móvel ou estacionário.

O Nó Móvel possui um Endereço de Origem fixo, que lhe é atribuído pela sua Rede de Origem. Mesmo quando o nó se desloca de sua Rede de Origem, este endereço é mantido.

Ao ingressar em uma Rede Remota, o Nó Móvel recebe um ou mais Endereços Remotos através dos mecanismos de autoconfiguração, constituídos de um prefixo válido na Rede Remota.

Para assegurar que os pacotes IPv6 destinados ao seu Endereço de Origem sejam recebidos, o nó realiza uma associação entre o Endereço de Origem e o Endereço Remoto, registrando seu novo endereço no Agente de Origem através do envio de uma mensagem *Binding Update*. Como resposta a essa mensagem o roteador da Rede de Origem envia uma mensagem *Binding Acknowledgement*.

Essa associação de endereços também pode ser feita diretamente com o Nó Correspondente, com o intuito de otimizar a comunicação.

Para o Nó Móvel detectar que retornou a sua rede, ele utiliza o processo de Descoberta de Vizinhos Inacessíveis, para detectar se o seu roteador padrão está ativo. Caso localize um novo roteador padrão, ele irá gerar um novo endereço baseado no prefixo anunciado na mensagem RA.

No entanto, encontrar um novo roteador padrão não significa necessariamente que ele esteja em uma nova rede, podendo ser apenas uma renumeração em sua rede ou a adição de um novo roteador.

Com isso, antes de realizar a associação de endereços com o Agente de Origem e com os Nós Correspondentes, o Nó Móvel tenta localizar novamente seu roteador padrão e irá comparar se o intervalo entre o envio de mensagens RA não solicitadas é o mesmo que o configurado em sua Rede Original.

Quando o Nó Móvel retorna a sua Rede de Origem, ele envia uma mensagem *Binding Update* informando ao Agente de Origem o seu retorno e que este não precisa mais lhe encaminhar os pacotes [9]. A figura 6 ilustra a topologia com mobilidade IPv6.

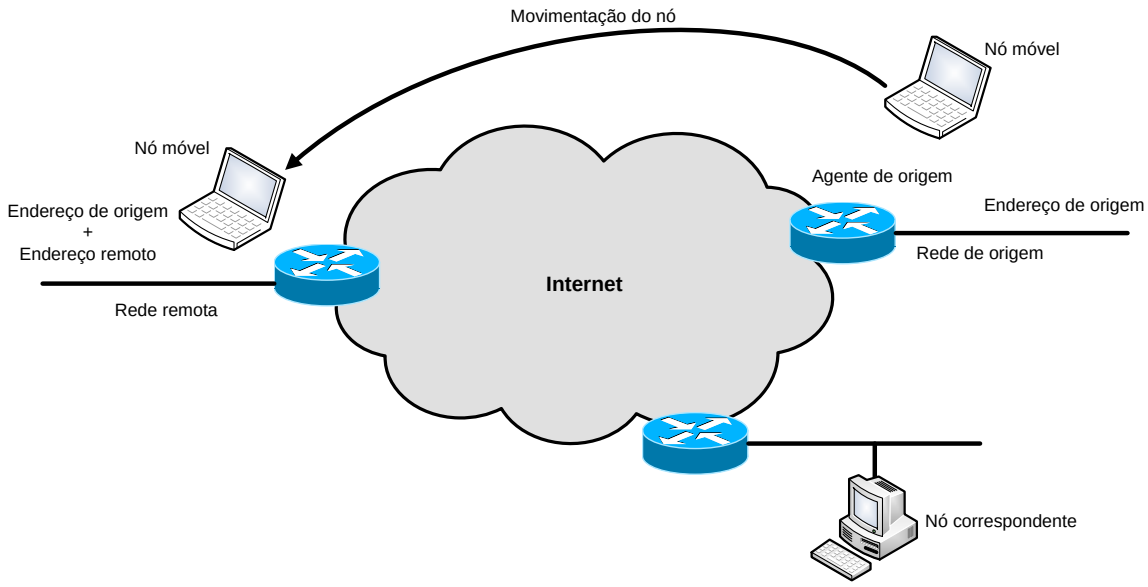


Figura 6 - Mobilidade IPv6

As comunicações entre nós móveis e nós correspondentes podem acontecer de dois modos: tunelamento bidirecional e otimização de rota.

No tunelamento bidirecional, os pacotes enviados pelo nó correspondente para o endereço original do nó móvel são interceptados pelo angente de origem que os encaminhará, através de um túnel, para o nó móvel utilizando o endereço remoto. Em seguida o nó móvel responde ao agente de origem, através do túnel, que

reeenvia o pacote ao nó correspondente. Neste caso o nó correspondente não necessita ter suporte à mobilidade IPv6 e o nó móvel não precisa se registrar no nó correspondente.

No modo otimização de rota, a comunicação entre o nó móvel e o nó correspondente ocorre diretamente, sem a necessidade da utilização do agente de origem. Para que esta comunicação ocorra, o nó móvel registra seu endereço no nó correspondente, que associa os endereços de origem e remoto do nó móvel.

4 TÉCNICAS DE TRANSIÇÃO

Com o intuito de facilitar o processo de transição entre as duas versões do Protocolo Internet, algumas técnicas foram desenvolvidas para que toda a base das redes instaladas sobre IPv4 mantenha-se compatível com o protocolo IPv6, sendo no primeiro momento de coexistência entre os dois protocolos, essa compatibilidade torna-se essencial para o sucesso da transição para o IPv6.

Cada uma dessa técnicas apresenta uma característica específica, podendo ser utilizada individualmente ou em conjunto com outras técnicas, de modo a atender as necessidades de cada situação, seja a migração para o IPv6 feita passo-a-passo, iniciando por um único host ou sub-rede, ou até de toda uma rede corporativa.

Estes mecanismos de transição podem ser classificados nas seguintes categorias:

Pilha Dupla: que provê o suporte a ambos os protocolos no mesmo dispositivo;

Tunelamento: que permite o tráfego de pacotes IPv6 sobre estruturas de rede IPv4;

Tradução: que permite a comunicação entre nós com suporte apenas a IPv6 com nós que suportam apenas IPv4.

Como o período de coexistência entre os dois protocolos pode durar indefinidamente, a implementação de métodos que possibilitem a interoperabilidade entre o IPv4 e o IPv6 poderá garantir uma migração segura para o novo protocolo, através da realização de testes que permitam conhecer as

opções que estes mecanismos oferecem, além de evitar, no futuro, o surgimento de ilhas isoladas de comunicação [10].

4.1 PILHA DUPLA

A utilização deste método permite que hosts e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois pacotes, IPv4 e IPv6.

Com isso, um nó Pilha Dupla, ou nó IPv6/IPv4, na comunicação com um nó IPv6 se comportará apenas como um nó IPv6, e na comunicação com um nó IPv4 se comportará apenas como um nó IPv4.

Cada nó IPv6/IPv4 é configurado com ambos endereços, utilizando mecanismos IPv4 (ex. DHCP) para adquirir seu endereço IPv4, e mecanismos do protocolo IPv6 (ex. autoconfiguração e/ou DHCPv6) para adquirir seu endereço IPv6.

Este método de transição pode facilitar o gerenciamento da implantação do IPv6, por permitir que este seja feito de forma gradual, configurando pequenas seções do ambiente de rede de cada vez. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 de cada nó [10].

A figura 7 ilustra a técnica.

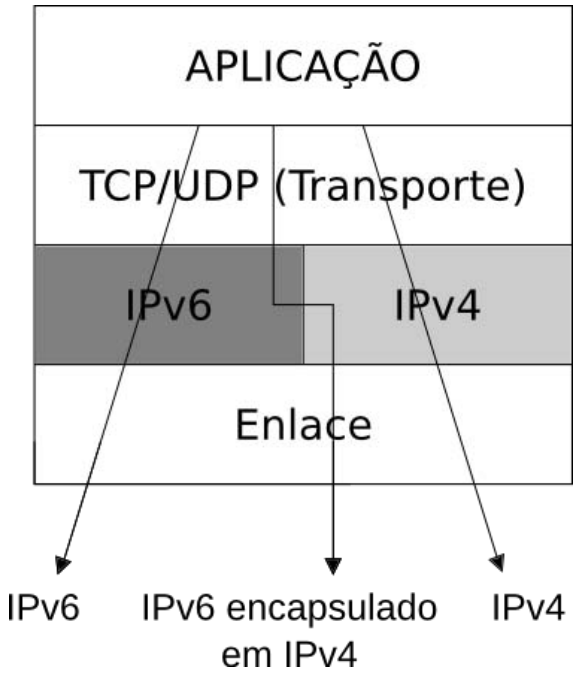


Figura 7 - Pilha Dupla

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[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 prédefinida. 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 [12].

4.2 TUNELAMENTO

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

Essas técnicas, tratadas na RFC 4213, têm sido as mais utilizadas na fase inicial de implantação do IPv6, por serem facilmente aplicadas em testes, onde há redes não estruturadas para oferecer tráfego IPv6 nativo.

Existem diversas técnicas de tunelamento disponíveis. Os cenários onde podem ser aplicados, as dificuldades de implementação e a diferença de performance variam significativamente entre os modelos, necessitando uma análise detalhada de cada um. As principais técnicas de tunelamento usutilizadas serão detalhadas nós próximos tópicos.

4.2.1 **Tunel 6over4**

As técnicas de tunelamento fazem o encapsulamento de pacotes IPv6 em pacotes IPv4. Este encapsulamento é conhecido como 6in4 ou IPv6-in-IPv4 (RFC 4213). Ele consiste em colocar o pacote IPv6 dentro de um pacote IPv4, adequar os endereços de origem e destino para o IPv4 e colocar no cabeçalho o tipo 41 (29 em

hexadecimal). Esse tipo de encapsulamento é conhecido por 6in4, ou como “protocolo 41”. Quando o destino receber o pacote com tipo 41 ele irá remover o cabeçalho IPv4 e tratar o pacote como IPv6. A figura 8 ilustra esse comportamento.

Também é possível, de forma análoga, encapsular pacotes IPv4 em pacotes IPv6, técnica conhecida como 4in6.

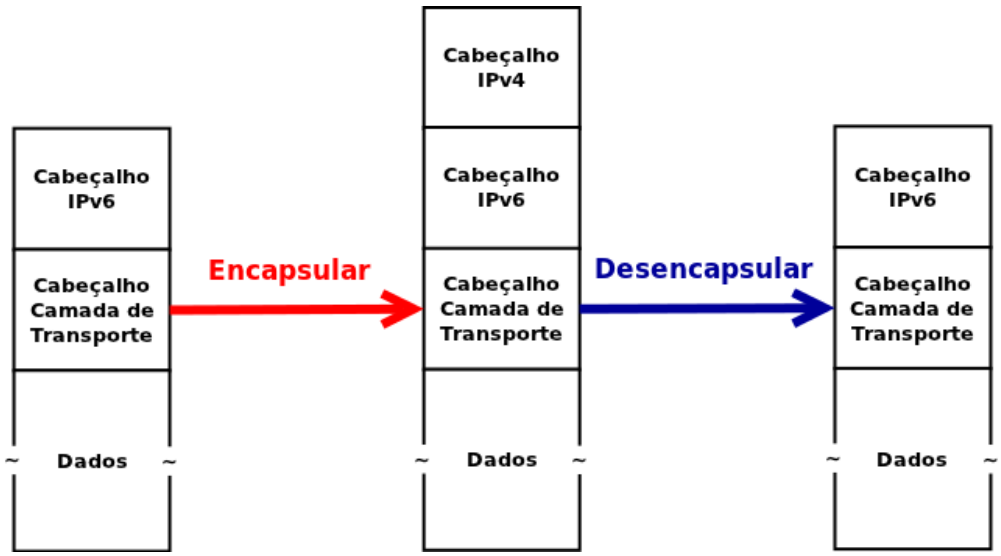


Figura 8 - Funcionamento 6in4

Uma das formas de utilizar túneis é criando-os manualmente. A técnica 6over4 (RFC 4213) utiliza um túnel manual estabelecido entre dois nós IPv4 para enviar o tráfego IPv6. Todo o tráfego IPv6 a ser enviado é encapsulado em IPv4 usando 6in4, explicado anteriormente. A configuração manual consiste em definir quais serão os IPs versão 4 de origem e destino que serão utilizados em cada ponta do túnel. Ao ser recebido pelo nó destino, o pacote IPv6 é desencapsulado e tratado adequadamente.

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

É importante entender a diferença entre 6over4 e 6in4. O túnel 6over4 é um túnel estabelecido manualmente que tem o objetivo de permitir conexão IPv6 entre dois nós de rede conectados por uma rede via IPv4. Ele usa o encapsulamento 6in4. Já o encapsulamento 6in4, com a utilização do tipo 41, pode ser utilizado também em outras técnicas de transição que transportam pacotes IPv6 em redes IPv4.

As figura 9 e 10 ilustram exemplos de implementação da técnica 6over4 em computadores ou em roteadores, onde devem ser criados tuneis de forma estática e o roteamento IPv6 em ambos deve ser habilitado.

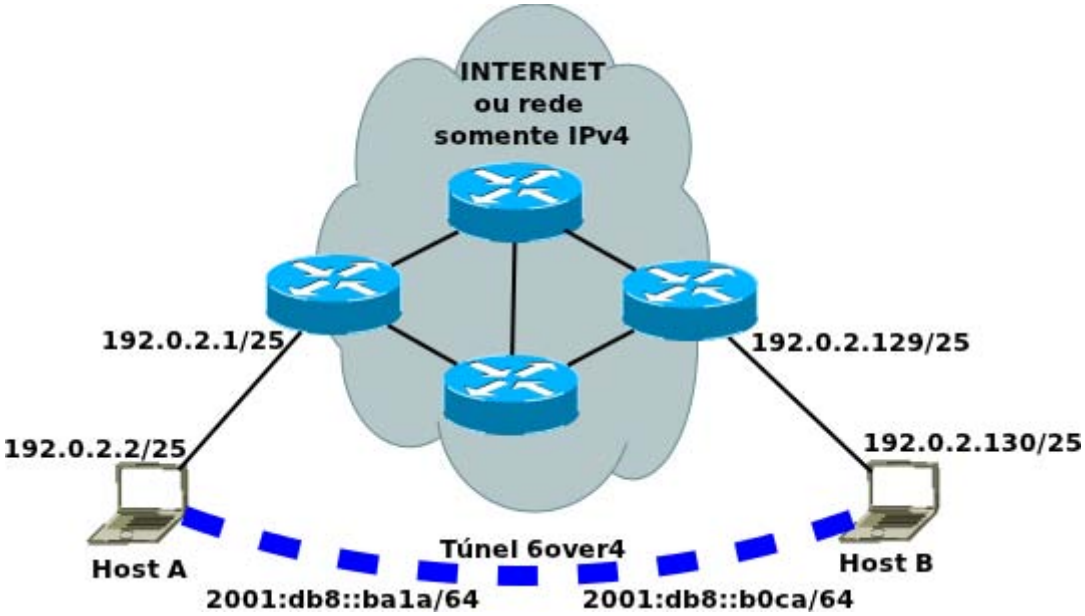


Figura 9 - Implementação 6over4 entre computadores

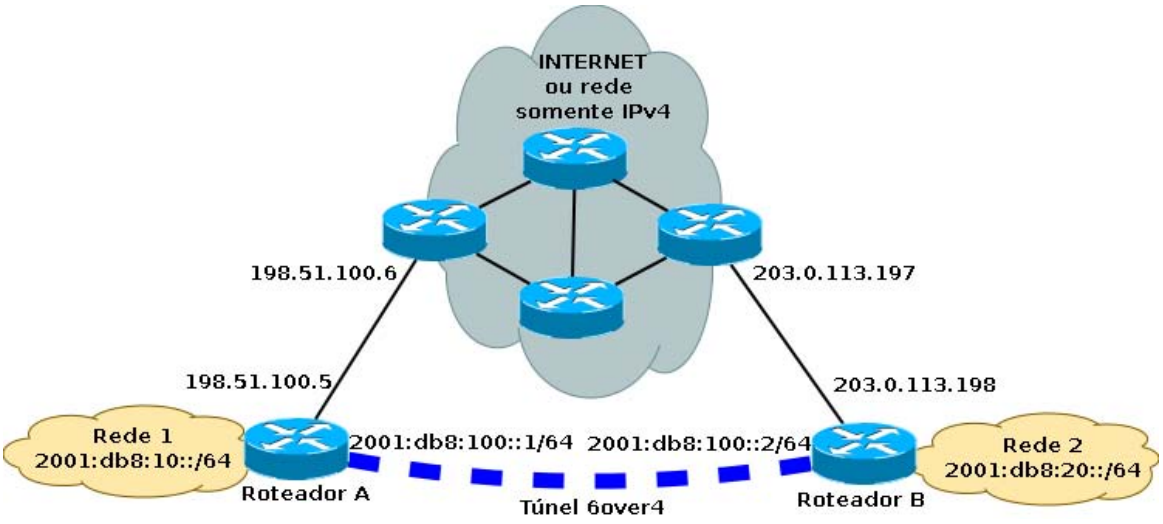


Figura 10 - Implementação 6over4 entre roteadores

4.2.2 **Tunel Broker**

A idéia desta técnica consiste no uso de servidores dedicados, denominados *Tunnel Brokers*, que gerenciam automaticamente a criação de túneis a partir de requisições de usuários. É uma das técnicas mais simples para obtenção IPv6, onde um simples *script* executável pode ser utilizado para o estabelecimento do túnel. Suas especificações são encontradas na RFC 3053 [14].

A figura 11 mostra os passos necessários para a criação do túnel:

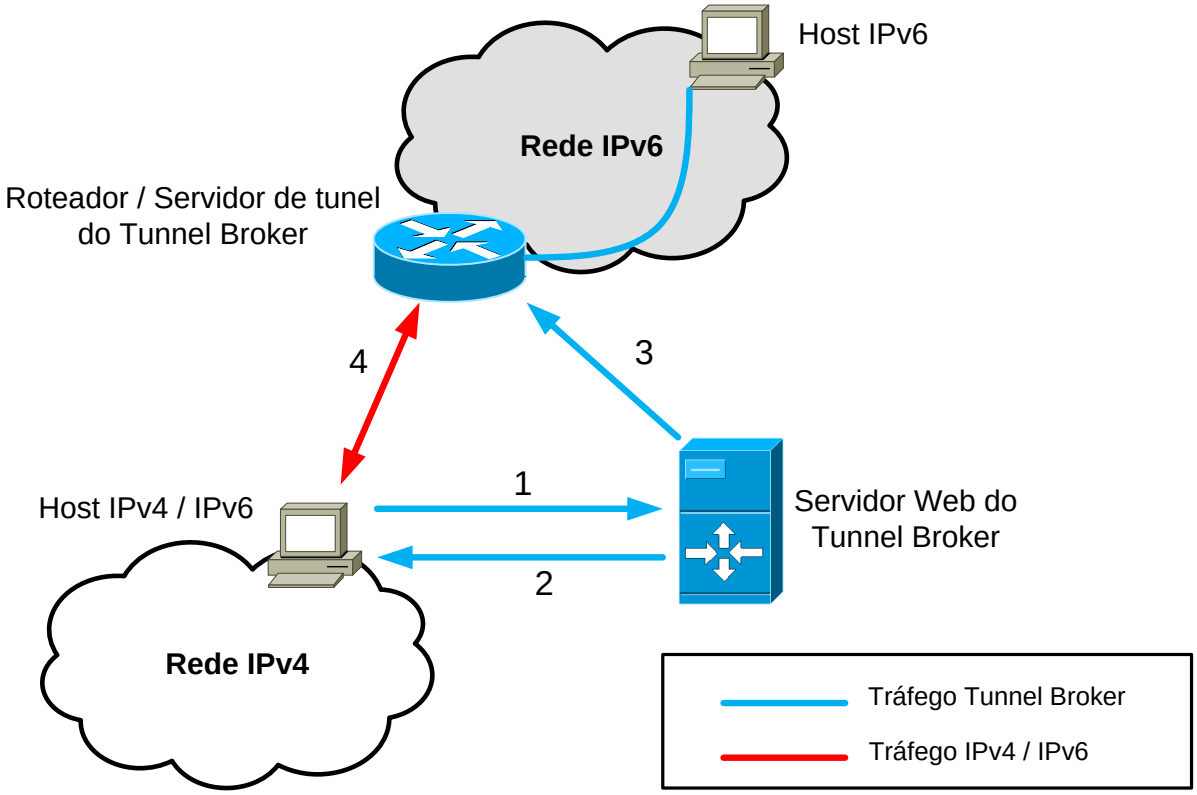


Figura 11 - Funcionamento Tunnel Broker

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 túnel criado.
4. – O *script* é executado pelo host IPv4/IPv6 e o acesso à rede IPv4 é obtido através do Roteador/Servidor de *Tunnel Broker*.

4.2.3 **Tunel GRE**

Outra opção de túnel estático para o tranporte de IPv6 em redes IPv4 é o GRE (*Generic Routing Encapsulation*) RFC 2784. Ele é um túnel estático entre dois nós, desenvolvido orinalmente pela Cisco, com a finalidade de encapsular vários tipos diferentes de protocolos, como por exemplo IPv6.

Este tipo de encapsulamento é suportado na maioria do sistemas operacionais e roteadores e possibilita a criação de um *link* ponto-a-ponto. Assim como o 6over4 sua configuração é manual, de modo que pode gerar um esforço na sua manutenção e gerenciamento proporcional à quantidade de túneis.

O pacote com cabeçalho é explicado na figura 12.

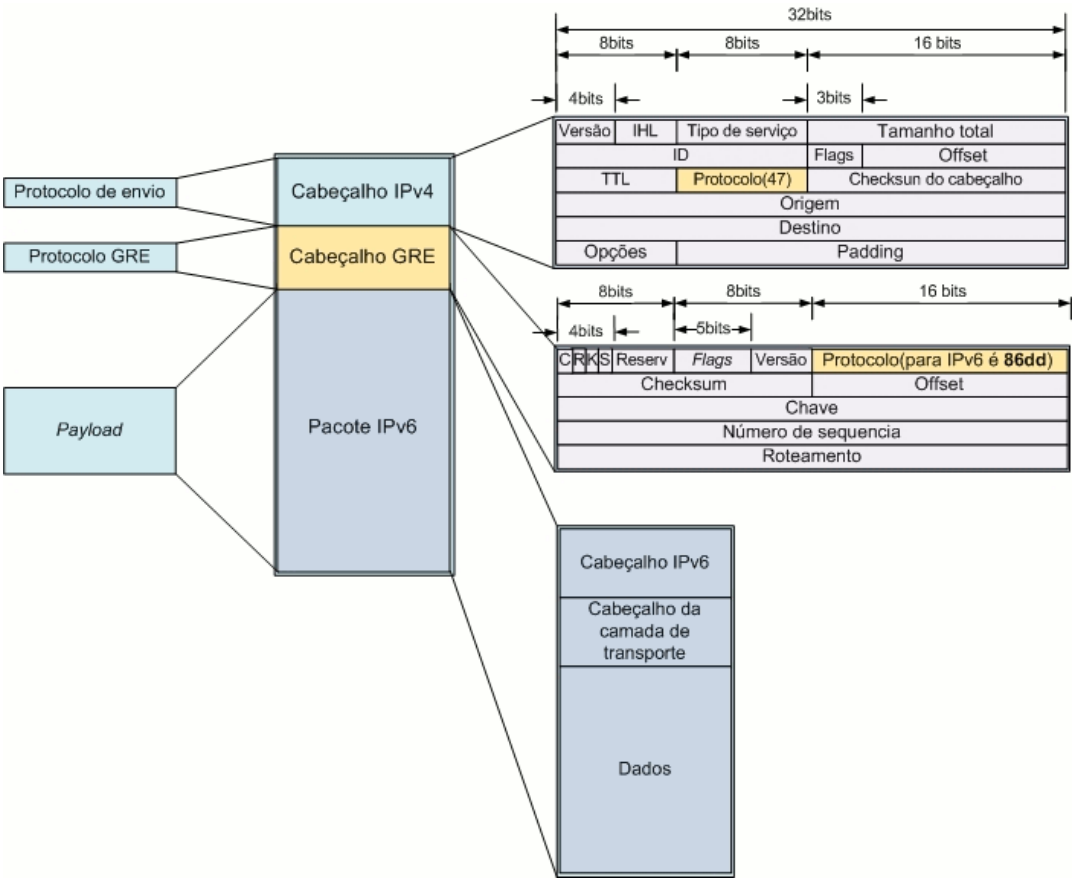


Figura 12 - Pacote com cabeçalho GRE

O funcionamento deste tipo de túnel é muito simples: consiste em pegar os pacotes originais, adicionar o cabeçalho GRE e o cabeçalho IPv4, e enviar ao IP de destino. Quando o pacote encapsulado chegar na outra ponta do túnel (IP de destino), remove-se dele os cabeçalhos IPv4 e GRE, restando apenas o pacote original, que é encaminhado normalmente ao destinatário.

4.2.4 **6to4**

O 6to4 (RFC 3056) é umas das técnicas de transição mais antigas em uso e é a técnica que inspirou a criação do 6rd (Item 4.4.2). Sua concepção era simples e muito interessante: com ajuda de *relays* pilha dupla distribuídos na Internet, abertos, instalados de forma colaborativa por diversas redes, qualquer rede IPv4 poderia obter conectividade IPv6 através de túneis 6in4 automáticos.

Por meio do 6to4 qualquer computador com um IPv4 válido poderia funcionar como uma extremidade de um conjunto de túneis automáticos e prover todo um bloco IPv6 /48 para ser distribuído e usado em uma rede.

A técnica funcionou parcialmente e ainda é usada na Internet, mas apresenta diversos problemas. De fato, talvez tenha trazido mais problemas para a implantação do IPv6 de forma geral, do que ajudado.

O 6to4 é composto dos seguintes elementos:

***Relay* 6to4:** roteador com suporte ao 6to4 e que possui conexão nativa IPv4 e IPv6. Ele funciona como a extremidade dos túneis automáticos para os Roteadores 6to4 que precisam se comunicar com a Internet IPv6. Os *relays* 6to4 usam o endereço *anycast* IPv4 192.88.99.1 e anunciam rotas para 2002::/16 através deles para a Internet.

Roteador 6to4: roteador que suporta 6to4 que fica na extremidade de uma rede IPv4 e é responsável por trazer conectividade IPv6 para esta rede, por meio dos túneis 6to4. No caso dos acessos à Internet IPv6, ele direcionará o tráfego até o *Relay Router* mais próximo, que encaminhará o pacote ao seu destino. Para acesso a outras redes 6to4, os túneis são fechados diretamente com outros Roteadores 6to4.

Cliente 6to4: equipamento de rede ou computador que usa endereços IPv6 fornecidos pelo túnel 6to4. O cliente 6to4 é um cliente pilha dupla convencional, normalmente numa rede doméstica ou corporativa, que pode usar IPv4 nativo ou compartilhado. O cliente não diferencia um endereço IPv6 obtido via 6to4 de um endereço IPv6 nativo.

As funções de Roteador e Cliente 6to4 podem estar presentes no mesmo equipamento. Um *desktop* convencional, por exemplo, usando Windows Vista, atua de forma automática como Roteador 6to4 desde que tenha um endereço IPv4 válido disponível.

O endereçamento 6to4, conforme definição da IANA, utiliza o prefixo de endereço global 2002:wwxx:yyzz::/48, onde wwxx:yyzz é o endereço IPv4 público do cliente convertido para hexadecimal. O exemplo a seguir mostra como fazer a conversão de endereços:

Endereço IPv4: 200.192.180.002.

200=C8

192=C0

180=B4

002=02

Com isso, o bloco IPv6 correspondente, via 6to4, é 2002:C8C0:B402::/48.

As figuras 13 e 14 demonstram o fluxo dos pacotes em uma rede 6to4. É importante notar que não existe a necessidade de os pacotes irem e voltarem pelo mesmo relay 6to4. As etapas 1, 3, 4 e 6 utilizam pacotes IPv6 e as etapas 2 e 5 utilizam pacotes IPv6 encapsulados em IPv4 através do protocolo 41.

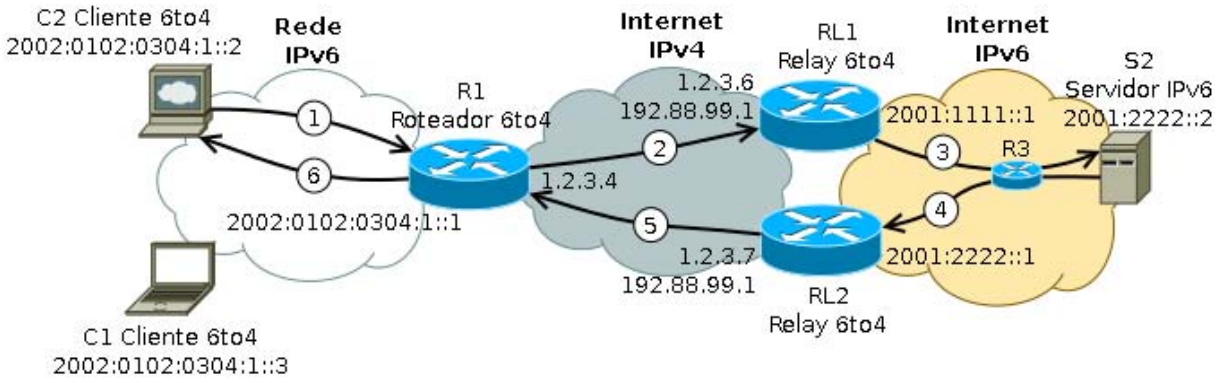


Figura 13 - Rede 6to4

Equipamento	Rota
RL1	::/0 rede IPv6 através da interface LAN / 2002::/16 através da interface virtual 6to4
RL2	::/0 rede IPv6 através da interface LAN / 2002::/16 através da interface virtual 6to4
S2	Rota padrão através de R3
R3	2002::/16 através do Relay RL2 (rota descoberta através da divulgação via BGP)
R1	::/0 através do Relay 6to4 RL1 ou RL2 utilizando a interface virtual 6to4 2002::/16 através da interface virtual 6to4 2002:0102:0304:1/64 para a rede local através da interface LAN
C1	::/0 através de R1 / 2002:0102:0304:1::/64 através da interface LAN
C2	::/0 através de R1 / 2002:0102:0304:1::/64 através da interface LAN

Figura 14 - Roteamento da rede 6to4

4.2.5 **Teredo**

Um problema em comum dos métodos vistos até então é que eles não funcionam quando o dispositivo IPv6 encontra-se atrás de um ou mais NATs. 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 [15]. Apesar de ser eficaz, a técnica possui o inconveniente de traduzir apenas os protocolos TCP *(Transmission Control Protocol)* e UDP *(User Datagram Protocol)* , 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 [16].

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, a figura 15 exibe tais dispositivos, seguida pelas funções de cada aparelho.

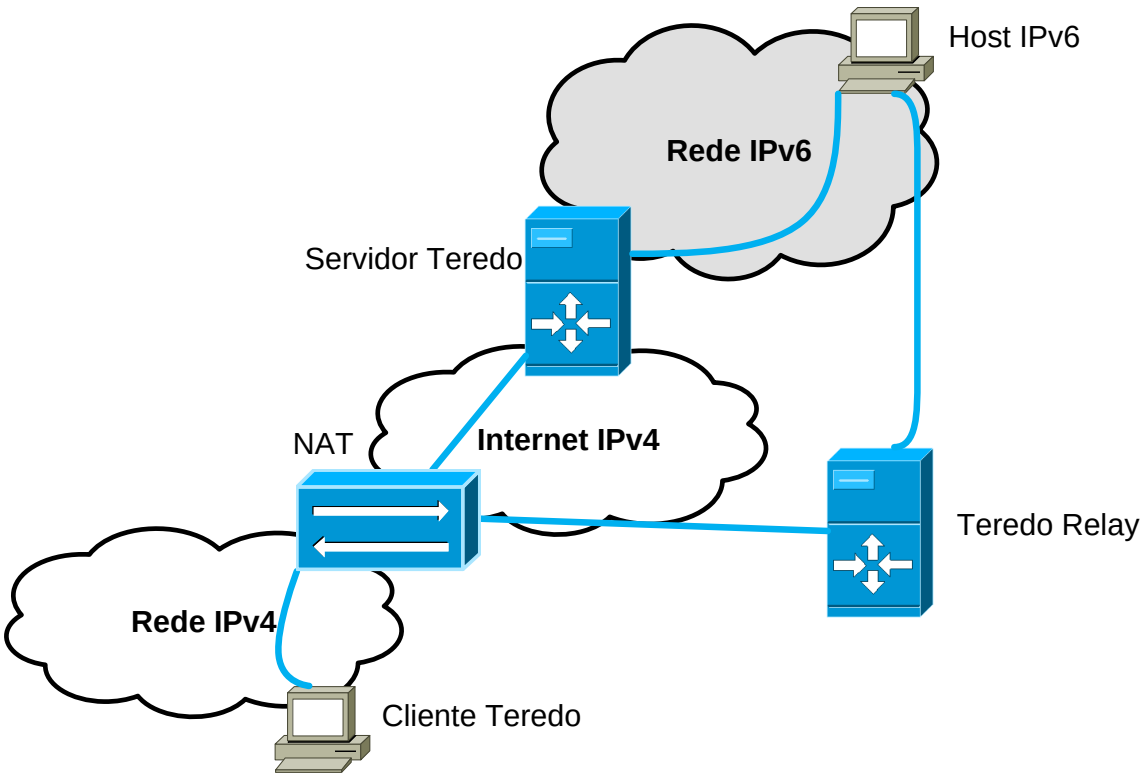


Figura 15 - Tunelamento Teredo

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 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 é mínima, sendo assim possui a capacidade de suportar um grande número de requisições. O portal IPv6 [17], disponibiliza uma lista de Servidores Teredo localizados por todo o mundo. Alguns destes servidores são: 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 figura 15 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 formato da figura 16 [16].

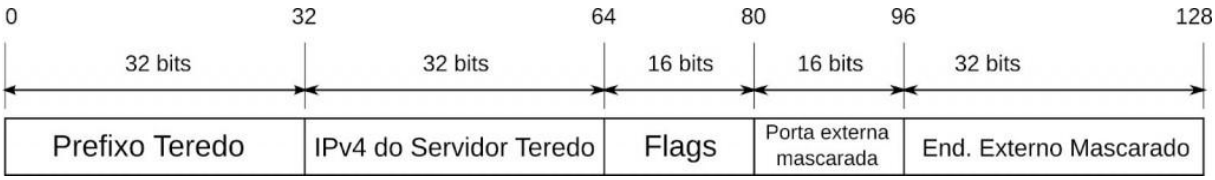


Figura 16 - Endereço Teredo

Assim como o 6to4, o Teredo possui questões de segurança. Através do encapsulamento ele pode permitir que tráfego que seria bloqueado em IPv4 consiga chegar ao destino. Ele vem instalado e habilitado por padrão no Windows. Recomenda-se que seja desabilitado em redes corporativas.

4.2.6 **ISATAP**

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) é uma técnica de tunelamento que liga dispositivos a roteadores. Sua utilização ocorre dentro das organizações, pois não há um serviço público de ISATAP. É possível utilizar a técnica quando a organização tem IPv6 na extremidade de sua rede, fornecido por seu provedor, mas sua infraestrutura interna, ou parte dela, não suporta o protocolo.

A figura 17 demonstra o conceito do ISATAP.

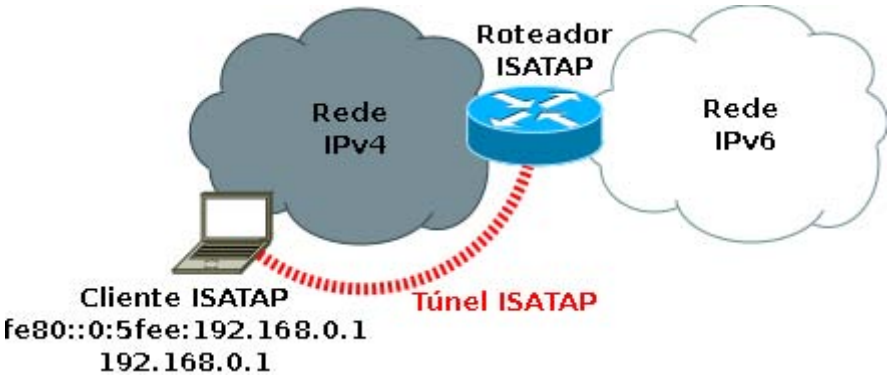


Figura 17 - Topologia ISATAP

Esta técnica, definida na RFC 5214, é baseada em túneis IPv6 criados automaticamente dentro da rede IPv4 e em endereços IPv6 associados aos clientes de acordo com o prefixo especificado no roteador ISATAP e no IPv4 do cliente. Para a criação destes túneis são utilizadas as especificações da seção 3 da RFC 4213, que trata do tunelamento através do protocolo IPv4 tipo 41 ou 6in4.

Os endereços IPv4 dos clientes e roteadores são utilizados como parte dos endereços ISATAP, permitindo a um nó determinar facilmente os pontos de entrada e saída dos túneis IPv6, sem utilizar nenhum protocolo ou recurso auxiliar [18].

O formato do endereço ISATAP segue o seguinte padrão:

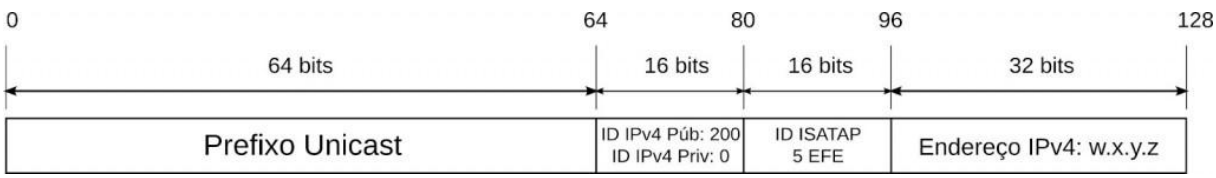


Figura 18 - Tradução de Endereço ISATAP

- **Prefixo unicast :** É qualquer prefixo unicast válido em IPv6, que pode ser link-local (FE80::/64) ou global. Normalmente utiliza-se uma rede /64 obtida a partir do prefixo global fornecido pelo provedor Internet para uso na rede.
- **ID IPv4 público ou privado:** Se o endereço IPv4 for público, este campo deve ter o valor "200". Se for privado (192.168.0.0/16, 172.16.0.0/12 e 10.0.0.0/8), o valor do campo será zero;
- **ID ISATAP:** Sempre tem o valor 5EFE;
- **Endereço IPv4**: É o IPv4 do cliente ou roteador em formato IPv4;

O ISATAP é suportado pela maior parte dos sistemas operacionais e roteadores e é de fácil implantação.

4.3 TRADUÇÃO

As técnicas de tradução possibilitam um roteamento transparente na comunicação entre nós que apresentem suporte apenas a uma versão do protocolo IP, ou utilizem pilha dupla. Estes mecanismos podem atuar de diversas formas e em camadas distintas, traduzindo cabeçalhos IPv4 em cabeçalhos IPv6 e vice-versa, realizando conversões de endereços ou atuando na troca de tráfego TCP ou UDP.

4.3.1 **SIIT**

SIIT *(Stateless IP/ICMP Translation Algorithm)* - definido na RFC 2765, o SIIT é um mecanismo de tradução *stateless* de cabeçalhos IP/ICMP, permitindo a comunicação entre nós com suporte apenas ao IPv6 com nós

que apresentam suporte apenas ao IPv4. Ele utiliza um tradutor localizado na camada de rede da pilha, que converte campos específicos dos cabeçalhos de pacotes IPv6 em cabeçalhos de pacotes IPv4 e vice-versa. Para realizar este processo, o tradutor necessita de um endereço IPv4-mapeado em IPv6, no formato 0::FFFF:a.b.c.d, que identifica o destino IPv4, e um endereço IPv4-traduzido, no formato 0::FFFF:0:a.b.c.d, para identificar o nó IPv6. Quando o pacote chega ao SIIT, o cabeçalho é traduzido, convertendo o endereço para IPv4 e encaminhado ao nó de destino [19]. O funcionamento desta técnica pode ser acompanhado na figura 19.

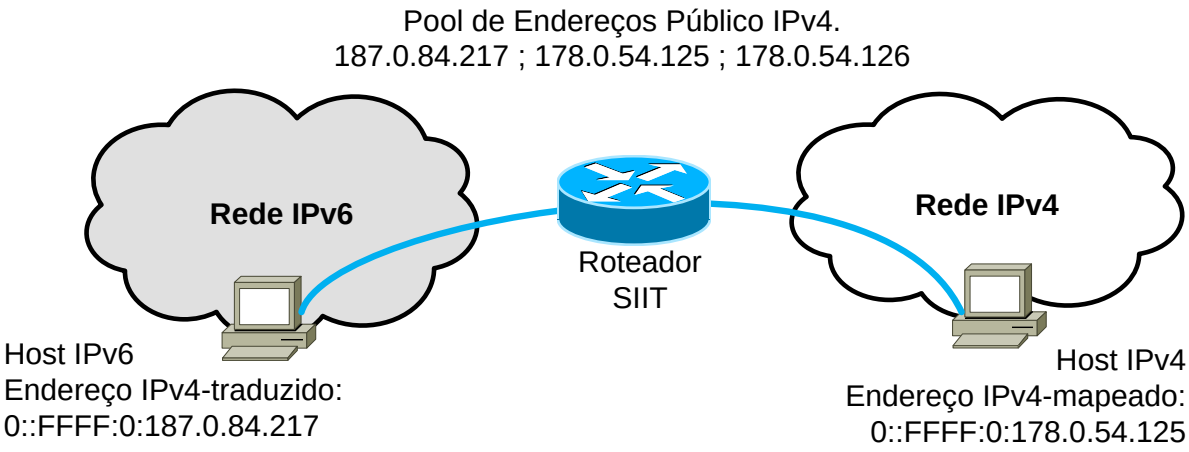


Figura 19 - Tradução SIIT

4.3.2 **BIS**

BIS *(Bump in the Stack)* possibilita a comunicação de aplicações IPv4 com nós IPv6. Definida na RFC 2767, o BIS funciona entre a camada de aplicação e a de rede, adicionando à pilha IPv4 três módulos: *translator*, que traduz os cabeçalhos IPv4 enviados em cabeçalhos IPv6 e os cabeçalhos IPv6 recebidos em cabeçalhos IPv4; *extension name resolver*, que atua nas DNS

queries realizadas pelo IPv4, de modo que, se o servidor DNS retorna um registro AAAA, o *resolver* pede ao *address mapper* para atribuir um endereço IPv4 correspondente ao endereço IPv6; e *address mapper*, que possui uma certa quantidade de endereços IPv4 para associar a endereços IPv6 quando o *translator* receber um pacote IPv6.

Como os endereços IPv4 não são transmitidos na rede, eles podem ser endereços privados [21].

Esse método permite apenas a comunicação de aplicações IPv4 com hosts IPv6, e não o contrário, além de não funcionar em comunicações *multicast*.

4.3.3 **BIA**

BIA *(Bump in the API)*, similar ao BIS, esse mecanismo adiciona uma API (*Application Programming Interface)* de tradução entre o *socket* API e os módulos TPC/IP dos *hosts* de pilha dupla, permitindo a comunicação de aplicações IPv4 com hosts IPv6, traduzindo as funções do *socket* IPv4 em funções do *socket* IPv6 e vice-versa. Conforme descrito na RFC 3338, três módulos são adicionados: *extension name resolver* e *address mapper*, que funcionam da mesma forma que no BIS; e o *function mapper*, que detecta as chamadas das funções do *socket* IPv4 e invoca as funções correspondentes do socket IPv6 e vice-versa [20]. O BIA apresenta duas vantagens em relação ao BIS: não depende do driver da interface de rede e não introduz *overhead* na tradução dos cabeçalhos dos pacotes. No entanto, também não suporta comunicações *multicast*.

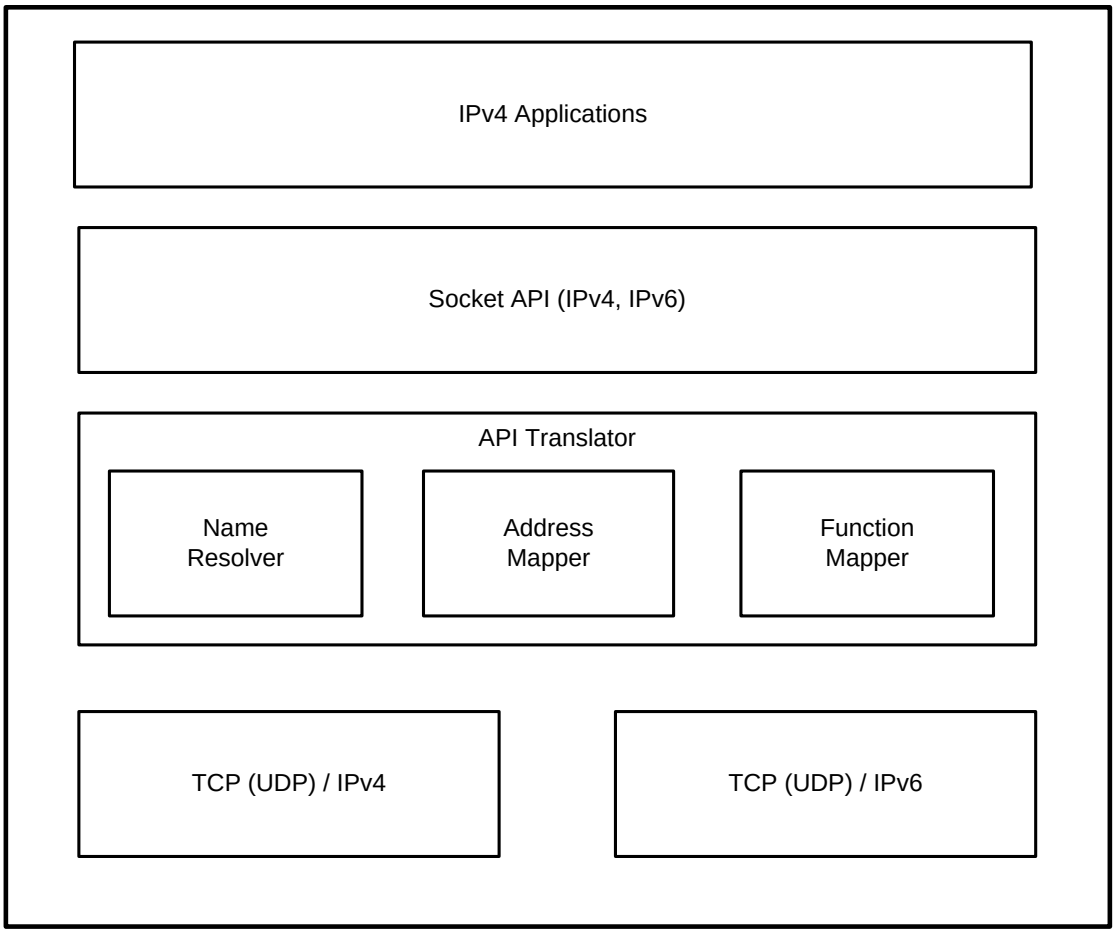


Figura 20 - Tradução BIA

4.3.4 **TRT**

O TRT *(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 tanto nos *hosts* IPv6 quanto nos IPv4. Ele apenas necessita de um dispositivo pilha dupla inserido em um ponto intermediário da rede [22].

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, onde é traduzido e remetido ao seu destino em um pacote TCP ou UDP. Este mecanismo é apresentado na figura 21, onde o hot IPv6 insere o Prefixo FEC:0:0:1/64 ao endereço IPv4 10.1.1.1 de destino.

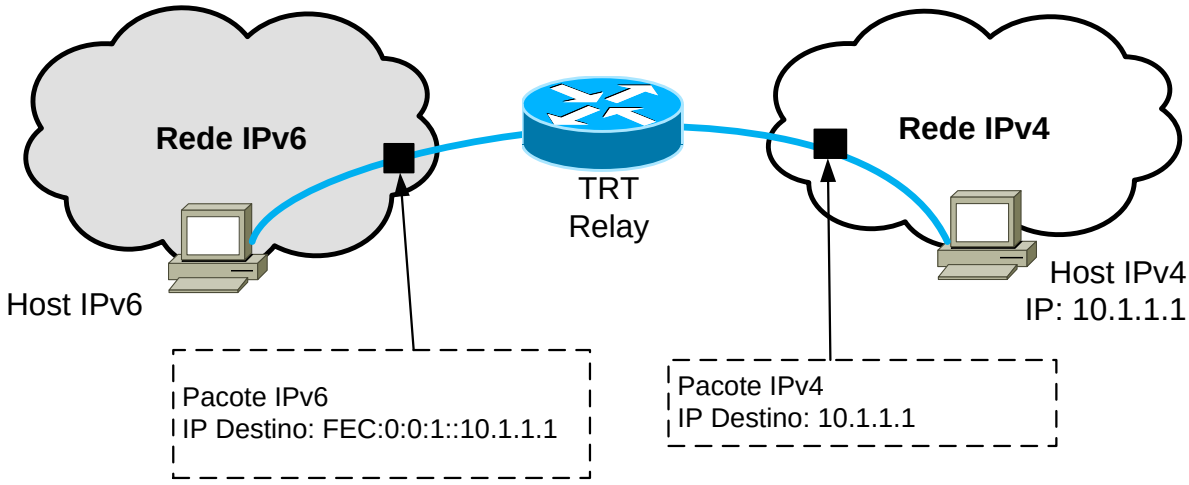


Figura 21 - Tradução TRT

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 conjunto através da configuração de diferentes prefixos falsos, onde cada TRT fica responsável por interceptar um prefixo pré-definido.

4.3.5 **ALG**

A técnica ALG (Application Layer Gateway) permite a aplicações de dispositivos atuando por trás de um NAT ou firewall tenham acesso externo à rede.

Em redes IPv6 um dispositivo ALG habilitado com pilha dupla pode ser utilizado para estabelecer conexões com redes IPv4 [23].

O uso desta técnica, exibindo na figura 22, 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.

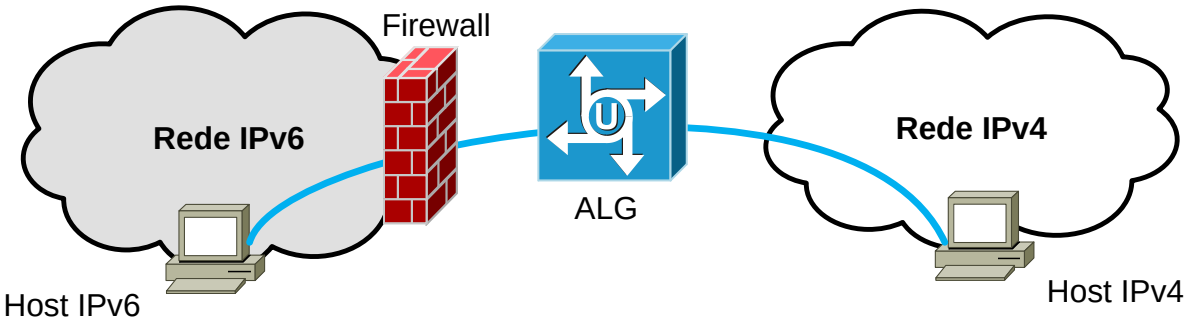


Figura 22 - Tradução ALG

4.4 TÉCNICAS UTILIZADAS PELOS PROVEDORES

Como podemos observar até este momento, foram descritas diversas técnicas para a utilização do IPv6, porém entre tantas existem técnicas que foram desenvolvidas e destinadas a provedores de serviços. Com estas técnicas os provedores poderão continuar a oferecer serviços de Internet e garantir a expansão destes serviços que atualmente são fundamentais para o mundo. Nós próximos tópicos serão descritos umas das principais técnicas que estão sendo utilizadas.

4.4.1 **6PE e 6VPE**

Roteamento através de MPLS *(Multiprotocol Label Switching)* tem sido largamente utilizado nas redes dos grandes provedores de conectividade Internet. Entretanto, grande parte destes equipamentos já instalados não possuem suporte a IPv6. Dado o alto custo destes equipamentos, pode existir a necessidade de mantê-los em operação. No intuito de resolver este problema pode-se utilizar as técnicas apresentadas neste tópico.

As técnicas em questão são o 6PE e o 6VPE, definidas, respectivamente, nas RFCs 4798 e 4659, que permitem que redes IPv6 estabeleçam a comunicação por meio de um *core* MPLS IPv4, usando LSPs *(Label Switch Paths)*. Sua implementação utiliza MBGP *(Multiprotocol BGP)* sobre IPv4 para se trocar rotas IPv6 e necessita que os PEs (Rototeadores de Borda) sejam Pilha Dupla. Através do MBGP os roteadores de borda recebem as rotas IPv6 mas aplicam MPLS IPv4 sobre os pacotes para realizar o roteamento. Quando o pacote chegar à rede IPv6 de destino o cabeçalho MPLS é removido e o pacote é encaminhado normalmente através do IPv6.

A diferença entre o 6PE e o 6VPE é que no primeiro caso os roteadores mantêm apenas uma tabela global de roteamento, de forma que o 6PE é mais indicado para provimento de conectividade Internet. Já os roteadores 6VPE são capazes de manter várias tabelas de roteamento separadas logicamente, de forma que a técnica é apropriada para prover serviços de VPNs. A figura 23 ilustra o funcionamento do 6PE [24].

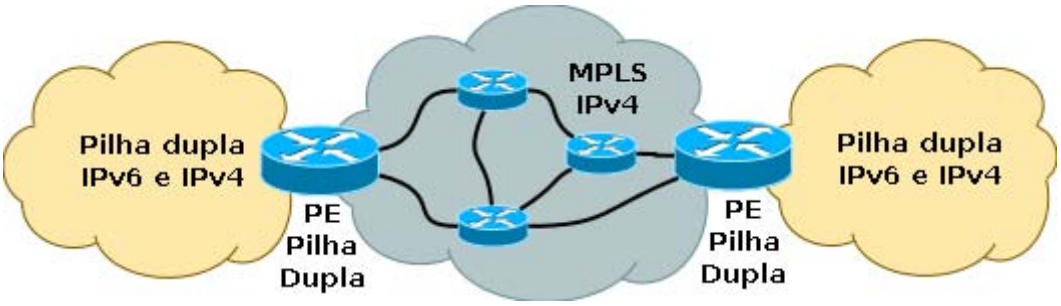


Figura 23 - Topologia de rede 6PE

4.4.2 **6rd**

O 6rd tem o objetivo de permitir ao usuário final ter conexão com as redes IPv6 apesar da rede da operadora continuar funcionando em IPv4. Este tipo de técnica, assim como o 6PE/6VPE, permite que os provedores utilizem a infraestrutura IPv4 já existente para fazer uma implantação rápida do IPv6.

O 6rd (RFC5569) é uma extensão da técnica 6to4, que está em desuso conforme explicado anteriormente. O 6rd resolve algumas das limitações técnicas do 6to4, como por exemplo sua assimetria e a falta de controle sobre os *relays* utilizados, permitindo sua utilização em larga escala.

Para entender o funcionamento do 6rd pode-se observar a figura 24, que ilustra a topologia típica de uso.

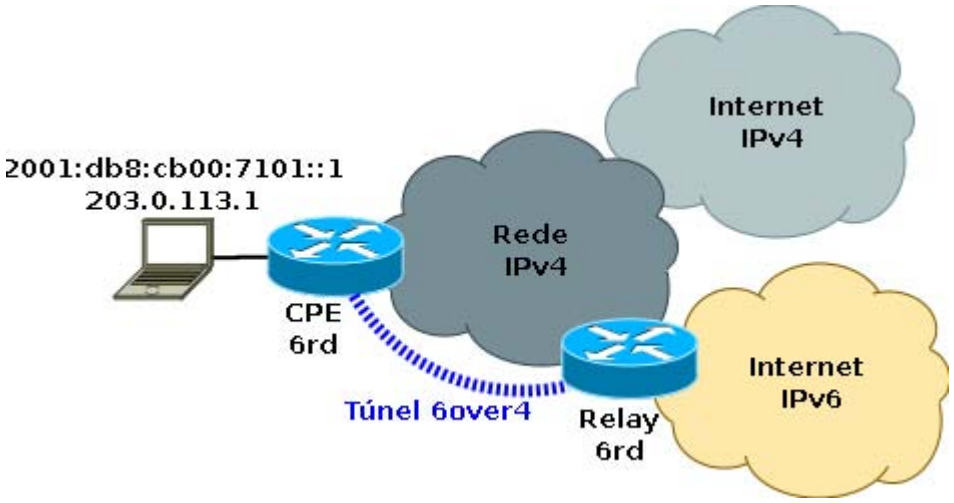


Figura 24 - Topologia da rede 6rd

Analisando a figura 24, é possível notar que o 6rd depende basicamente de dois componentes:

CPE (*Customer Premises Equipment*) 6rd: instalado como interface entre a rede da operadora e do usuário;

***Relay* 6rd:** instalado na interface entre a rede IPv4 da operadora e a Internet IPv6.

O CPE 6rd é um CPE tradicional (xDSL modem, cable modem, 3G modem etc), cujo software foi modificado para permitir o uso do 6rd. A necessidade dessa modificação dificulta a implementação da técnica, uma vez que requer a substituição, lógica ou física, de equipamentos em campo. Tal modificação nos CPEs normalmente é viável nos casos em que o provedor gerencia remotamente o equipamento, sendo capaz de fazer *upgrades* em seu *firmware*.

O 6rd *relay* é um equipamento que vai encapsular e desencapsular pacotes para trafegarem corretamente nas redes IPv4 e IPv6.

O CPE 6rd atribui ao usuário um endereço IPv4, como um CPE normal. Entretanto um endereço IPv6 também é atribuído ao usuário. Este endereço IPv6 é

um endereço IPv6 público válido, mas é construído de maneira específica para que o *relay* 6rd identifique-o como um endereço 6rd. O endereço IPv6 atribuído é constituído da seguinte forma:

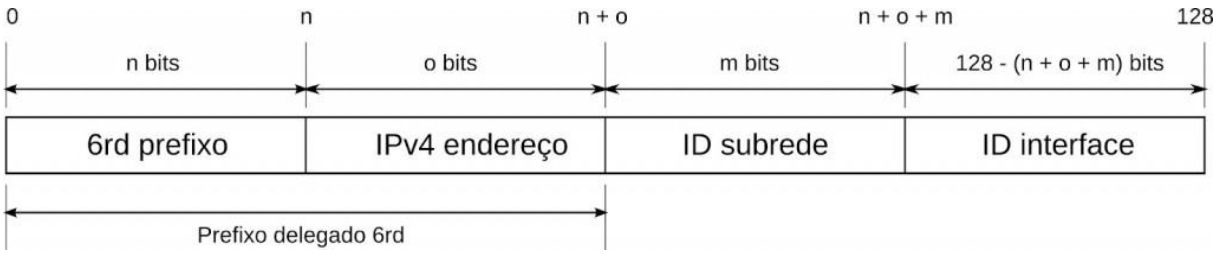


Figura 25 - Tradução de endereço IPv4 para IPv6 no 6rd

No 6rd o tamanho *"n"* do prefixo e o tamanho *"o"* do endereço IPv4, que formam o prefixo delegado 6rd, são escolhas do provedor de acesso. Para permitir que a autoconfiguração de endereço *stateless* funcione é necessário que o tamanho deste prefixo *"n + o"* seja menor que 64 bits. O ID subrede de tamanho *"m"* pode ser definido pela operadora, mas é mais provável que a operadora deixe a definição do valor e tamanho do campo para o usuário final adequar a necessidade de sua rede.

Normalmente utiliza-se *n*=32, *o*=32 e *m*=0. Pode-se, contudo, aumentar o número de bits utilizados por *"n"* para além de 32, forçando o endereço IPv4 a utilizar parte dos 64 bits menos significativos, o que impede o funcionamento da autoconfiguração *stateless*. Para evitar que isto ocorra, o endereço IPv4 pode ocupar menos de 32 bits. Tal configuração é possível se os endereços IPv4 fizerem parte de uma mesma rede, pois pode-se omitir o prefixo da mesma. Por exemplo, se todos os endereços IPv4 forem da rede 198.51.0.0/16, os 16 bits que representam os números 198 e 51 podem ser omitidos e a representação do endereço IPv4

necessitará somente de 16 bits, ao invés dos 32 bits necessários para representar o endereço completo.

O 6rd é uma técnica funcional cuja implementação em massa foi testada com sucesso no provedor francês Free. Entretanto, a técnica não tem sido adotada por outros, principalmente pela necessidade de atualização do software ou de substituição dos CPEs.

É importante deixar claro que o 6rd não é uma técnica para ser usada em novos usuários Internet, mas sim para os usuários já existentes, de forma a conseguir uma implantação muito rápida do IPv6. O 6rd funciona com base numa rede IPv4 e não resolve o problema da escassez de endereços. Técnicas escolhidas para novos usuários Internet devem preferencialmente basear-se em redes IPv6 e, quando necessário, preservar endereços IPv4, compartilhando-os.

4.4.3 **NAT444**

O NAT444 tem sido usado na tentativa de prolongar a vida útil do IPv4 na Internet. Este mecanismo fere o princípio de comunicação fim-a-fim da Internet e seu uso deve ser evitado. Alternativas que levem as redes IPv4 na direção de redes somente IPv6 são preferíveis, assim como alternativas que usem métodos *stateless* e que mantenham a complexidade nas extremidades da rede.

Se usado, o NAT444 deve acompanhar a implantação do IPv6 nativo para os usuários. Não deve ser usado isoladamente.

O NAT444 é descrito no em draft-shirasaki-nat444-05 e também é conhecido como LSN *(Large Scale NAT)* ou CGN *(Carrier Grade NAT).* Este mecanismo atribui um IPv4 privado para cada um dos usuários de um Provedor de Serviços, de forma

semelhante ao que já é normalmente feito em redes domésticas e em diversas redes corporativas. Ou seja, os usuários conviverão, nesse caso, com duas camadas de NAT.

A utilização desta técnica resolveria, de forma provisória, o problema da falta de endereços IPv4, já que eles seriam largamente reutilizados, mas o custo seria comprometer as conexões fim-a-fim e, possivelmente, a "quebra" de diversas aplicações hoje existentes.

Pode-se argumentar que o NAT já é usado normalmente e que não há prejuízo na utilização da Internet por conta disso. Isso não é verdade. O NAT, na rede dos usuários, por si só, já é prejudicial, embora tenha desempenhado um importante papel nos últimos anos para a conservação dos endereços IPv4 na Internet. Técnicas como servidores STUN *(Simple Traversal of UDP through NATs),* uPnP *(Universal Plug and Play)* e outras foram desenvolvidas para restaurar, parcialmente, a comunicação fim a fim perdida com uma camada apenas de NAT. Com o uso de NAT444 elas deixarão de funcionar.

Outro ponto a considerar é que essa técnica é cara, exigindo equipamentos com grande poder de processamento. Investimentos altos tendem a ser politicamente ignorados dentro de grandes corporações, o que pode levar a um atraso na adoção do IPv6.

Um ponto a considerar, do ponto de vista estritamente técnico, é a escolha do bloco de IPs a ser usado no NAT. Como o uso dos blocos da RFC1918 é comum nas redes dos usuários, qualquer bloco escolhido dentre os disponíveis pelo provedor fatalmente colidirá com o bloco de algum de seus clientes. Existe uma proposta em estudo para a reserva de um novo bloco, exclusivo para a utilização em situações onde houver duplo NAT. O ARIN *(American Registry for Internet Numbers)*

prontificou-se a ceder o bloco em questão e a proposta está sendo analisada pelo IETF: draft-weil-shared-transition-space-request-15.

Devido ao rápido esgotamento do IPv4, podem existir situações em que essa técnica terá de ser utilizada. Seu uso muitas vezes é incentivado por fabricantes de equipamentos, talvez devido ao alto custo dos equipamentos necessários para sua implementação [1].

A figura 26 exemplifica o funcionamento das redes hoje e como ficará o funcionamento da rede com a utilização do NAT444.

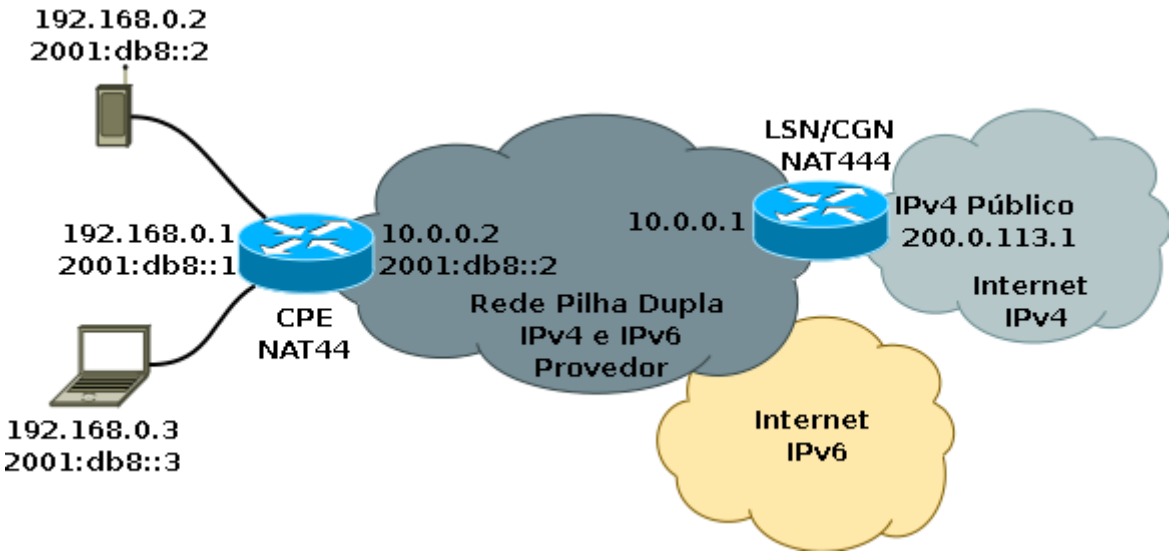


Figura 26 - Topologia de rede NAT444

4.4.4 **Dual Stack Lite (DS-Lite)**

Em um cenário em que não há mais IPv4 disponíveis, mas a base de usuários do provedor continua a crescer e ainda há muitos serviços exclusivamente disponíveis em IPv4 na Internet, o provedor não pode oferecer exclusivamente

conectividade IPv6 ao usuário final, sendo forçado a oferecer também conectividade IPv4, mas com IPs de alguma forma compartilhados.

A técnica *Dual Stack Lite* (Pilha dupla simplificada), padronizada na RFC 6333, pode ser aplicada em situações em que o provedor já oferece IPv6 nativo para seus usuários. Sua implementação necessita de um equipamento denominado AFTR *(Address Family Transition Router),* que implementa um CGN, que é um NAT de grande porte, na rede do provedor. Entre o AFTR e o CPE do usuário utiliza-se um túnel IPv4 sobre IPv6 para transportar o tráfego IPv4. No contexto do DS-Lite, o CPE do usuário é chamado de B4, abreviação para *DS-Lite Basic Bridging BroadBand*. Nas extremidades desses túneis são usados endereços da faixa 192.0.0.0/29, especialmente reservada para este fim. Para o CPE do usuário e os demais equipamentos da rede do usuário são utilizados IPs da RFC 1918 não havendo problema se diferentes usuários utilizarem faixas de IPs repetidas, dado que o AFTR identifica os diferentes túneis com base no IPv6 de origem dos pacotes encapsulados.

Na CPE do usuário deve existir um DHCPv4 para a distribuição dos endereços na rede interna. Deve existir também um *proxy* DNS, que permita consultas via IPv4, mas faça essas consultas ao DNS recursivo do provedor via IPv6, evitando traduções desnecessárias no AFTR.

É importante frisar alguns pontos:

- O AFTR usa CGN, mas não força o usuário a utilizar duplo NAT. Ou seja, AFTR realiza a função de NAT, de forma concentrada, para cada um dos dispositivos de cada usuário [1].

- O DS-Lite utiliza endereços privados na faixa 192.0.0.0/29 para as extremidades dos túneis v4 sobre v6, evitando a utilização desnecessária de endereços IPv4 na infraestrutura do provedor.

A figura 27 mostra um exemplo de topologia.

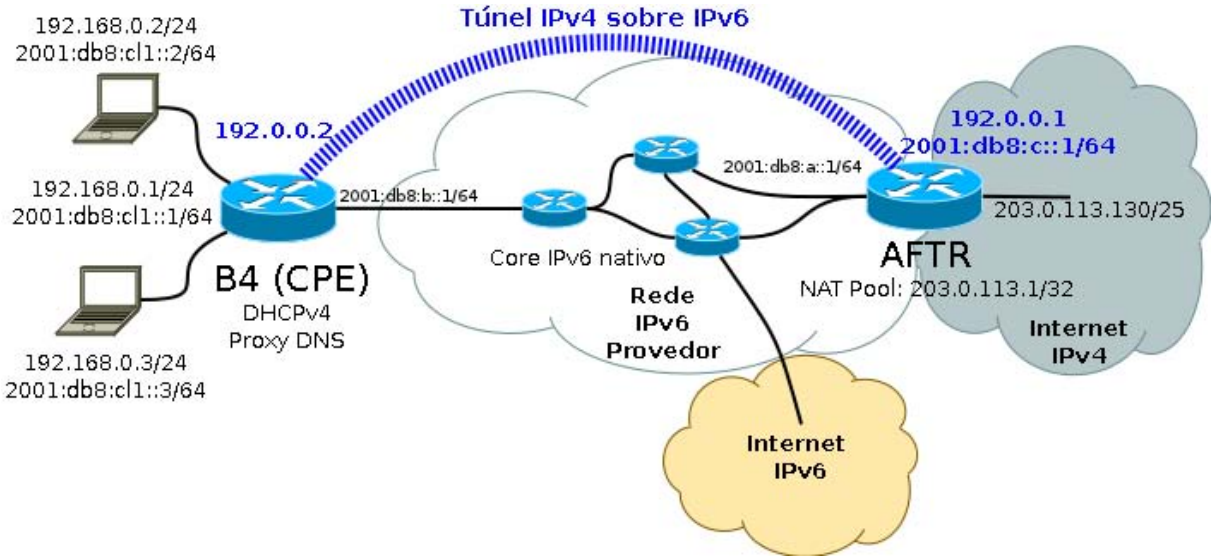


Figura 27 - Exemplo de Topologia DS-Lite

5 ESTUDO DE CASO

Para estudo de caso será apresentado um cenário de implantação do IPv6 em um provedor de serviço que atualmente possui um backbone MPLS com IPv4 e necessita implementar o IPv6 para continuar oferecendo serviços de Internet para seus clientes. Este cenário foi configurado e homologado com o software GNS3 [33].

A técnica de transição utilizada por este provedor de serviços será o 6PE, onde as configurações dos roteadores serão baseados no sistema operacional da Cisco Systems. A figura 28 ilustra a topologia do provedor de serviços.

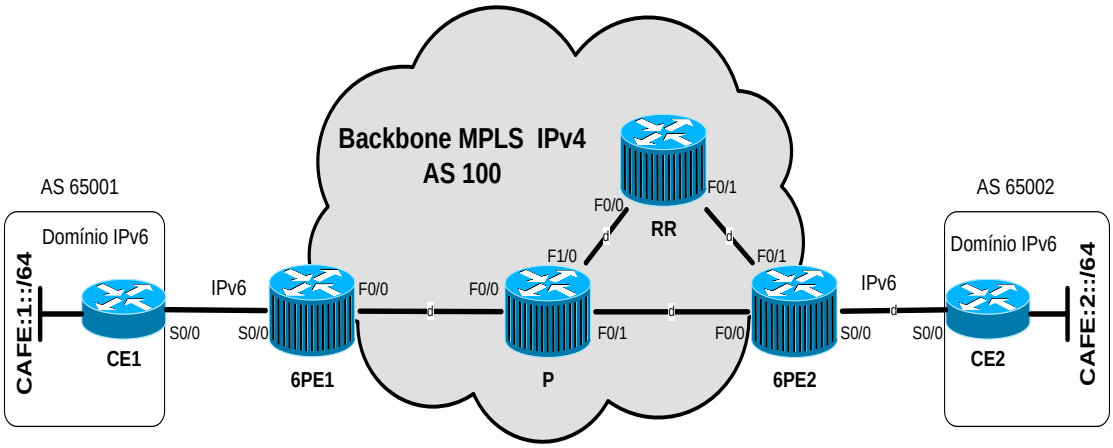


Figura 28 - Topologia Estudo de Caso

A solução 6PE permite a comunicação entre os domínios IPv6 do CE1 com CE2 através do Backbone MPLS IPv4 do provedor de serviços. O protocolo MBGP no backbone IPv4 é usado para alocação de Labels que serão atribuídos para cada prefixo IPv6 que será anunciado pelo 6PE1 e 6PE2. Os roteadores 6PE são considerados *dual-stack*, pois estão utilizando IPv6 para comunicação com os CEs e IPv4 com os roteadores do Backbone.

Configuração CE1:

```
!
hostname CE1
!
ipv6 unicast-routing
ipv6 cef
!
!
interface Loopback0
 no ip address
 ipv6 address CAFE:1::1/64
!
interface Serial0/0
 description To 6PE1 Router
 no ip address
 ipv6 address 2001:1::1/124
 clock rate 2000000
!
router bgp 65001
 no synchronization
 bgp router-id 10.210.0.1
 bgp log-neighbor-changes
 neighbor 2001:1::2 remote-as 100
 neighbor 2001:1::2 description 6PE1 neighbor
 no auto-summary
 !
 address-family ipv6
  neighbor 2001:1::2 activate
  network CAFE:1::/64
 exit-address-family
!
```

Configuração CE2:

```
!
hostname CE2
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
 no ip address
 ipv6 address CAFE:2::1/64
!
interface Serial0/0
 description To 6PE2 Router
 no ip address
 ipv6 address 2001:2::1/124
 clock rate 2000000
!
router bgp 65002
 no synchronization
 bgp router-id 10.210.0.2
 bgp log-neighbor-changes
```

```
 neighbor 2001:2::2 remote-as 100
 neighbor 2001:2::2 description 6PE2 neighbor
 no auto-summary
 !
 address-family ipv6
  neighbor 2001:2::2 activate
  network CAFE:2::/64
  no synchronization
 exit-address-family
!
```

Configuração 6PE1:

```
!
hostname 6PE1
!
ipv6 unicast-routing
ipv6 cef
!
mpls label protocol ldp
mpls ipv6 source-interface Loopback0
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ipv6 address ABCD:1::1/128
!
interface FastEthernet0/0
 description To P2 Router
 ip address 10.1.1.1 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
interface Serial0/0
 description To CE1 Router
 no ip address
 ipv6 address 2001:1::2/124
 mpls ip
 clock rate 2000000
!
router ospf 100
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.3 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 description RR iBGP neighbor
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 2001:1::1 remote-as 65001
 neighbor 2001:1::1 description CE1 eBGP neighbor
 no auto-summary
 !
```

```
 address-family ipv6
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-label
  neighbor 2001:1::1 activate
  redistribute connected
  no synchronization
 exit-address-family
!
mpls ldp router-id Loopback0 force
!
```

Configuração 6PE2:

```
!
hostname 6PE2
!
ipv6 unicast-routing
ipv6 cef
!
mpls label protocol ldp
mpls ipv6 source-interface Loopback0
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ipv6 address ABCD:1::2/128
!
interface FastEthernet0/0
 ip address 10.1.1.10 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
interface Serial0/0
 description To CE2 Router
 no ip address
 ipv6 address 2001:2::2/64
 mpls ip
 clock rate 2000000
!
interface FastEthernet0/1
 ip address 10.1.1.14 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.1.8 0.0.0.3 area 0
 network 10.1.1.12 0.0.0.3 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 description RR iBGP neighbor
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 2001:2::1 remote-as 65002
```

```
 neighbor 2001:2::1 description CE2 eBGP neighbor
 no auto-summary
 !
 address-family ipv6
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-label
  neighbor 2001:2::1 activate
  redistribute connected
  no synchronization
 exit-address-family
!
mpls ldp router-id Loopback0 force
!
```

Configuração P:

```
!
hostname P
!
mpls label protocol ldp
!
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet0/1
 ip address 10.1.1.9 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet1/0
 ip address 10.1.1.5 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.4 0.0.0.3 area 0
 network 10.1.1.8 0.0.0.3 area 0
!
```

Configuração RR:

```
!
hostname RR
!
ipv6 unicast-routing
ipv6 cef
!
mpls label protocol ldp
mpls ipv6 source-interface Loopback0
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 ipv6 address ABCD:1::3/128
!
interface FastEthernet0/0
 ip address 10.1.1.6 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
interface FastEthernet0/1
 ip address 10.1.1.13 255.255.255.252
 speed 100
 full-duplex
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 10.1.1.4 0.0.0.3 area 0
 network 10.1.1.12 0.0.0.3 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 no auto-summary
 !
 address-family ipv6
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 route-reflector-client
  neighbor 1.1.1.1 send-label
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 send-label
 exit-address-family
!
mpls ldp router-id Loopback0 force
!
```

5.1 VERIFICAÇÃO DO FUNCIONAMENTO DO ESTUDO DE CASO

O comando **show bgp ipv6 unicast** mostra os prefixos IPv6 aprendidos via MBGP.

```
6PE1#show bgp ipv6 unicast
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:1::/124     ::                       0         32768 ?
*>i2001:2::/64      ::FFFF:2.2.2.2           0    100      0 ?
*> ABCD:1::1/128    ::                       0         32768 ?
*>iABCD:1::2/128    ::FFFF:2.2.2.2           0    100      0 ?
*> CAFE:1::/64      2001:1::1                0             0 65001 i
*>iCAFE:2::/64      ::FFFF:2.2.2.2           0    100      0 65002 i
6PE1#
```

Nos resultados dos comandos abaixo podemos observar a imposição dos labels para o prefixo CAFE:2::/64. O label 20 é advertido pelo roteador 6PE2 via MBGP. O Label 17 refere-se a imposição de Label para o IGP next-hop 2.2.2.2 (6PE2).

```
6PE1#show bgp ipv6 unicast CAFE:2::/64
BGP routing table entry for CAFE:2::/64, version 9
Paths: (1 available, best #1, table Global-IPv6-Table)
  Advertised to update-groups:
        2
  65002
    ::FFFF:2.2.2.2 (metric 3) from 3.3.3.3 (3.3.3.3)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Originator: 2.2.2.2, Cluster list: 3.3.3.3
      mpls labels in/out nolabel/20
6PE1#show ip cef 2.2.2.2
2.2.2.2/32, version 12, epoch 0, cached adjacency 10.1.1.2
0 packets, 0 bytes
  tag information set
    local tag: 17
    fast tag rewrite with Fa0/0, 10.1.1.2, tags imposed: {17}
  via 10.1.1.2, FastEthernet0/0, 0 dependencies
    next hop 10.1.1.2, FastEthernet0/0
    valid cached adjacency
    tag rewrite with Fa0/0, 10.1.1.2, tags imposed: {17}
6PE1#show ipv6 cef CAFE:2::/64
CAFE:2::/64
     nexthop ::FFFF:2.2.2.2
    fast tag rewrite with Fa0/0, 10.1.1.2, tags imposed: {17 20}
6PE1#
```

Rota IPv6 do CE2 aprendida via encapculamento MPLS:

```
6PE1#show ipv6 route CAFE:2::/64
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
B   CAFE:2::/64 [200/0]
     via ::FFFF:2.2.2.2, IPv6-mpls
6PE1#
```

Roteamento IPv6 no CE1 e ping para o endereço IPv6 do CE2:

```
CE1#ping ipv6 CAFE:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to CAFE:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/52 ms
CE1#sh ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:1::/124 [0/0]
     via ::, Serial0/0
L   2001:1::1/128 [0/0]
     via ::, Serial0/0
B   2001:2::/64 [20/0]
     via FE80::C00B:BFF:FEFA:0, Serial0/0
B   ABCD:1::1/128 [20/0]
     via FE80::C00B:BFF:FEFA:0, Serial0/0
B   ABCD:1::2/128 [20/0]
     via FE80::C00B:BFF:FEFA:0, Serial0/0
C   CAFE:1::/64 [0/0]
     via ::, Loopback0
L   CAFE:1::1/128 [0/0]
     via ::, Loopback0
B   CAFE:2::/64 [20/0]
     via FE80::C00B:BFF:FEFA:0, Serial0/0
L   FF00::/8 [0/0]
     via ::, Null0
CE1#
```

De acordo com as saídas dos comandos apresentados, pode-se observar o funcionamento correto da solução 6PE em um cenário que o Backbone do provedor de serviços possui apenas MPLS e IPv4 habilitados.

6 IMPLANTAÇÃO DO IPV6

Os endereços, IPv6 assim como os endereços IPv4, são delegados de acordo com as necessidades dos órgãos regionais, denominados RIRs, responsáveis pela alocação e administração dos endereços e demais recursos relacionados. Os cinco RIRs são identificados de acordo com a sua área de atuação listado abaixo:

- 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.

De acordo com os dados dos RIRs e com o crescimento exponencial da Internet, os endereços IPv4 estimam esgotar em 2013 para a maioria dos RIRs colocando em risco o atual crescimento da Internet. Diante destas ameaças diversos RIRs e orgãos relacionados aos RIRs que são localidados nos países onde os RIRs são responsáveis, vêem realizando um trabalho contínuo de estudo e disseminação do IPv6 não só para provedores de serviços mas também para órgãos do Governo, Universidades e empresas.

O NIC.br é o orgão gestor da Internet no Brasil que administra a alocação de endereços IPv4 e IPv6 e está diretamente ligado ao LACNIC. O mesmo vem realizando as atividades de coordenação de esforços para implantar o IPv6 no Brasil [25].

6.1 NO BRASIL

Atualmente o Brasil é um dos principais consumidores de endereços IPv6 da região LACNIC, sendo que em primeiro lugar temos a Argentina como demonstra a figura 29.

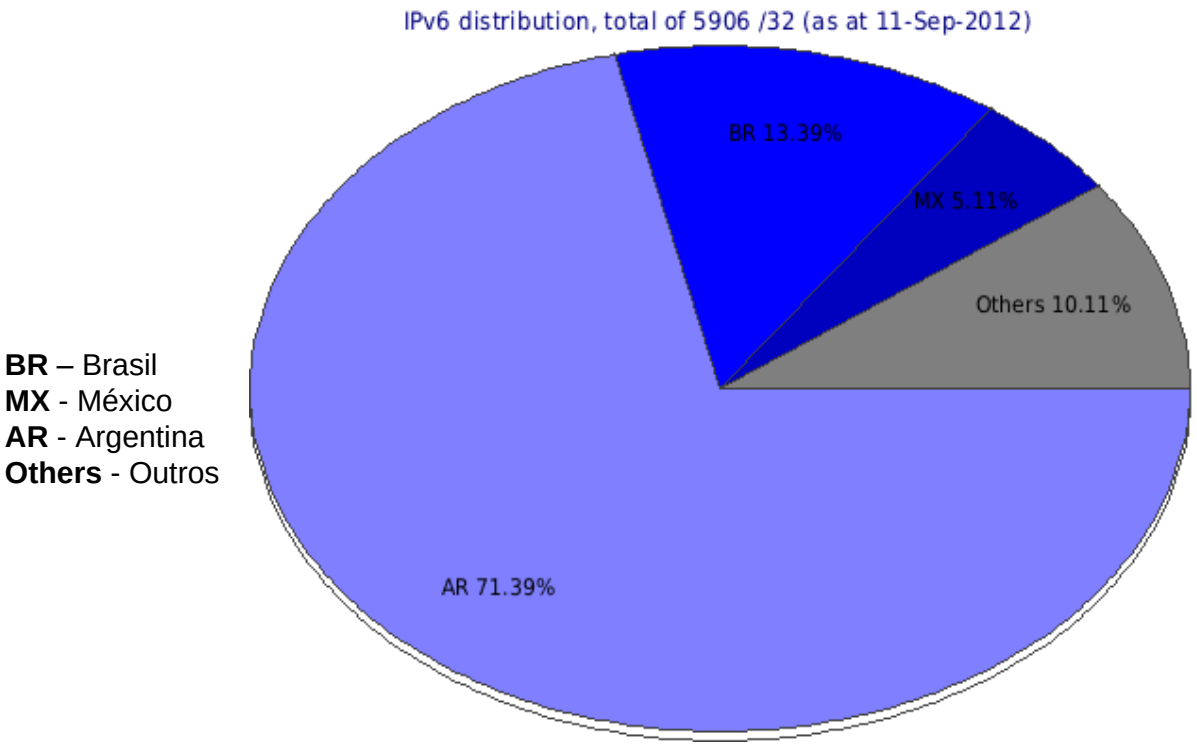


Figura 29 - IPv6 no LACNIC

Este constante crescimento por IPv6 é reflexo do trabalho realizado pelo NIC.br, porém pode-se observar que será necessário um aumento deste crescimento por IPv6, pois os endereços IPv4 ainda dispónveis no NIC.br estão em eminência de esgotar.

Um cronograma foi desenvolvido pelo NIC.br, com base no diálogo com provedores Internet, operadoras de telecom e provedores de conteúdo.

O cronograma pode ser considerado uma recomendação técnica do NIC.br e um guia, mas não é um documento estático, pode evoluir com o tempo. É baseado numa lógica bastante simples [25]:

- As operadoras de telecom devem oferecer trânsito IPv6 primeiro, para que os demais sejam capazes de implantar o protocolo.
- O conteúdo deve migrar rápido para IPv6: todos os sites, governo, comércio eletrônico, corporativos, etc, para que não corram risco de perda de audiência, e porque isso evitará que provedores de acesso tenham de implantar técnicas de transição complexas, caras e nocivas à Internet, como o NAT444 ou *Carrier Grade* NAT.
- Usuários domésticos e redes corporativas devem realizar a migração de forma planejada, começando tão logo quanto possível.

A figura 30 descreve os marcos para que as operadoras e provedores de conteúdo disponibilizem os serviços de IPv6 para seus usuários.

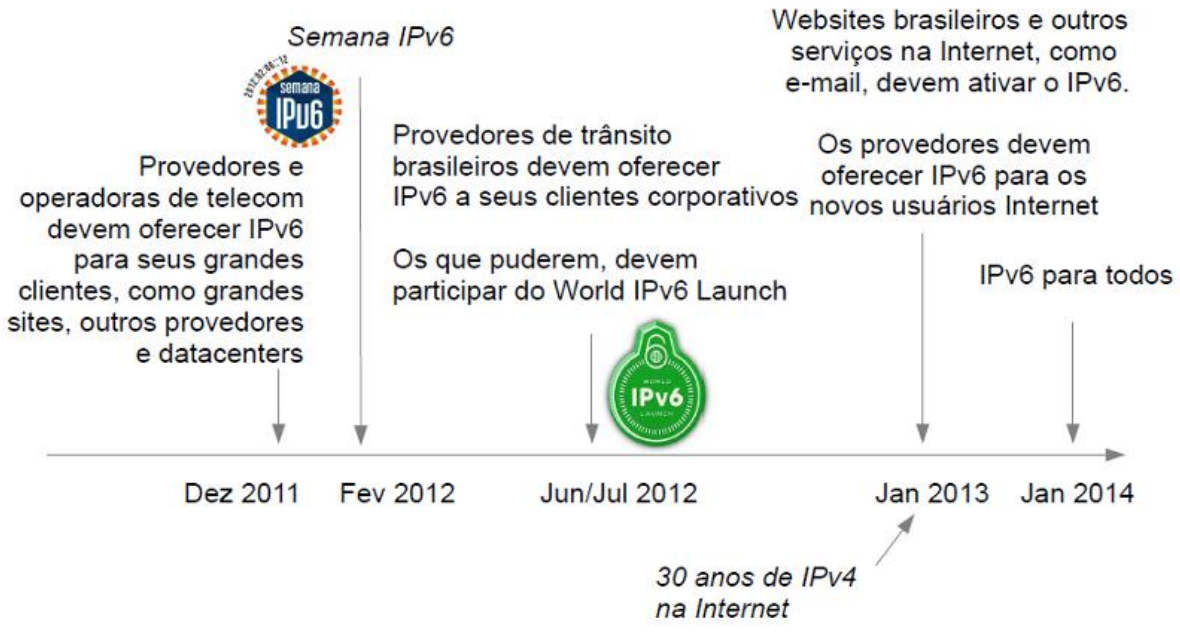


Figura 30 - Cronograma NIC.br – (NIC.br 05/06/2012)

6.2 NO MUNDO

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 2004, 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 2004 e 2011, é mostrada na figura 31.

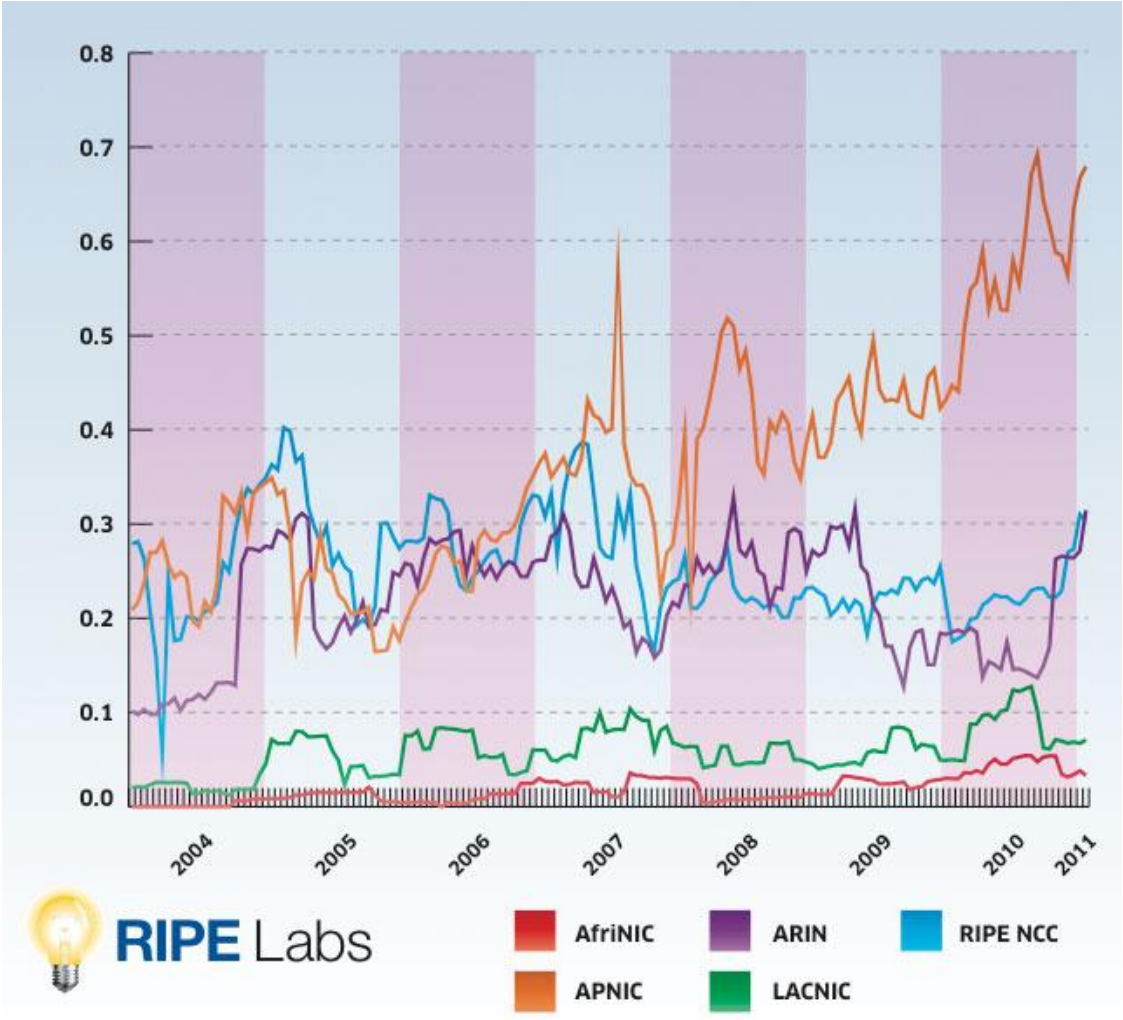


Figura 31 - Alocação Global de IPv6

O alto número de alocações do AfriNIC pode ser atribuído às políticas de implantação IPv6 que foram realizadas na África [26].

No RIPE NCC pode ser atribuído às políticas de implantação IPv6 européias, sobretudo ao plano de ação previsto pela *Commission Of The European Communities* [27], que consiste em tarefas a serem executadas por um período de três anos, como implementações e 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 relatórios contínuos 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 [28].

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 % [29]. A grande quantidade de endereços da versão antiga do protocolo é atribuída à 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 [30], 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 vêem 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. Pouco menos de 11% da população africana possui acesso à Internet [31]. Os países latino-americanos apresentam uma posição um pouco mais confortável, comparada à África, tendo mais de 34% da população acesso à grande rede, tendo o Brasil como o maior expoente da região.

7 CONCLUSÃO

A implantação do IPv6 é importante para a saúde futura da Internet. A oferta cada vez menor de endereços IPv4 disponíveis tem sido amplamente documentada, assim como os desafios enfrentados por aqueles que desejam migrar para o IPv6. Em termos de dados concretos, no entanto, indústria e as universidades têm tido pouca visibilidade da taxa de implantação do IPv6 na Internet.

Um desses estudos, realizado pela Arbor Networks [32], buscou medir a quantidade de tráfego IPv6 na Internet analisando durante um ano dados de mais de 90 ISPs, coletando informações de 2.393 roteadores de *peering* e *backbone*, juntamente com 278.797 interfaces de clientes e *peering*, totalizando 4 Tbps de tráfego interdomínio na Internet. Arbor Networks analisou tanto o tráfego IPv6 nativo quanto encapsulado, em ISPs da Europa, da Ásia e principalmente dos EUA. Dos 4 Tbps medidos em todo o período, apenas 600 Mbps de tráfego IPv6 foi coletado, o que representa 0,0026% do total do tráfego IPv4. No entanto, é possível observar um crescimento no volume de tráfego IPv6 desde o começo do estudo, iniciando em 50 Mbps e até atingir 150 Mbps em julho de 2008. A proporção de IPv6 contra o tráfego IPv4 permaneceu praticamente o mesmo em relação a 2007.

Este último ponto é particularmente interessante, pois parecem indicar que não há atualmente nenhuma migração significativa de usuários de IPv4 para IPv6. No entanto, desde que o tráfego IPv4 em geral cresceu significativamente, implica também que o uso do IPv6 está crescendo aproximadamente a mesma taxa do IPv4 (ou talvez um pouco mais lento). Tal como acontece com IPv4, este crescimento do tráfego IPv6 pode resultar de novos usuários migrando para o IPv6 e usuários existentes aumentando a sua utilização IPv6 para atender à sua demanda por aplicações de alta largura de banda, como *streaming* de vídeo.

No que tange o IPv6, o novo protocolo foi elaborado de forma a suprir as necessidade de seu antecessor e atender às 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 infraestrutura 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.

A partir da análises destes números, podemos observar que a os Estados Unidos estão à frente da implantação do IPv6 seguido do Japão que concentra o maior número de endereços na região da Ásia. De forma similar, acontece na Europa, através do contínuo incentivo da Comunidade Européia. Em ambos os casos ficou clara a importância do govervo em fomentar as iniciativas para implantação do IPv6.

No Brasil, um orgão que tem orientado e difundido o conhecimento do IPv6 é o NIC.br, porém não é o suficiente para que instituições, principalmente os Proverodres de Serviço, realizem a implantação do IPv6 em suas redes. O Governo

Brasileiro pouco tem investido em ações para o estímulo do uso do IPv6 e pode contribuir para um problema futuro da Internet no Brasil.

Pode-se concluir que a implantação do IPv6, principalmente no Brasil, ainda está lento e não apto para atender à demanda atual e futura da Internet. Por algum tempo ainda teremos a coexistência dos protocolocos IPv4 e IPv6, de forma que os mecanismos de transição garantirão a interoperabilidade entre elas.

Diante disto, espera-se que este trabalho tenha ajudado a demostrar de uma forma simples e direta a necessidade de implantar a transição do IPv4 para o IPv6 através de diversas técnicas e serve de incentivo para a migração para o IPv6.

8 REFERÊNCIAS

[1] Ceptro.br, IPv6.br – Projeto para a disseminação do IPv6 no Brasil. http://www.ceptro.br/CEPTRO/MenuCEPTROSPIPv6 Acesso em: 30 Jul. de 2012

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

[3] Loshin Pete, IPv6:Theory,Protocol,andPractice, Editora Morgan Kaufiman, 2ª edição. 2003

[4] http://www.lacnic.net – Acessado em: 12 Ago. de 2012.

[5] http://www.potaroo.net/tools/ipv4 – Acessado em: 12 Ago. de 2012.

[6] James F. Kurose, **Redes de Computadores e a Internet** - 3ª Edição.

[7] http://www.cisco.com - Acessado em: 13 Ago. de 2012

[8] http://www.iana.org - Acessado em: 13 Ago. de 2012

[9] http://www.gta.ufrj.br/ensino/eel879/trabalhos_v1_2010_2/joimilte/3MobilidadesuporteemredeIPv6..html - Acessado em: 19 Ago. 2012.

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

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

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

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

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

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

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

[17] **The IPv6 Portal, Teredo**, Disponível em:

<http://www.ipv6tf.org/index.php?page=using/connectivity/teredo> Acesso em: 25 Ago. de 2012.

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

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

[20] 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.

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

[22] J. Hagino, K. Yamamoto, **An IPv6-to-IPv4 Transport Relay Translator**, RFC3142, Jun. de 2001.

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

[24] http://www.lacnic.net/documentos/seminarios/6PE_6VPE_LACNIC.pdf - Acessado em 30 Ago. de 2012.

[25] www.ipv6.br – Acessado em 11 Set. de 2012.

[26] http://www.ipv6news.info/2011/01/31/global-patterns-in-ipv4-allocation-statistics/ - Acessado em 11 Set. de 2012.

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

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

[29] APNIC, Apstats, Disponível em: <http://www.apnic.net/apstats> Acesso em: 16 Set. de 2012.

[30] 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: 16 Set. de 2012.

[31] Internet World Stats, World Internet Usage and Populations Statistics, Disponível em: <http://www.internetworldstats.com/stats.htm> Acesso em: 16 Set.de 2012.

[32] http://www.arbornetworks.com/IPv6research - Acesso em: 16 Set.de 2012.

[33] http://www.gns3.net – Acesso em: 05 Jan. de 2013.