SALVADOR GIAQUINTO

TRANSIÇÃO DE UM AMBIENTE CORPORATIVO OPERANDO COM OS PROTOCOLOS IPv4/NAT PARA O PROTOCOLO IPv6, COLOCANDO A IPTNET RUMO ÀS NOVAS REDES DE PRÓXIMA GERAÇÃO

Trabalho apresentado ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo, para a obtenção do título de Mestre em Engenharia de Computação

ÁREA DE ATUAÇÃO: REDES DE COMPUTADORES

ORIENTADOR: PROF. DR. ANTONIO LUIZ RIGO

SÃO PAULO

2003

Dedicatória

Aos meus pais e família, que me ensinaram desde cedo a importância da leitura e do saber, e, em especial, a minha esposa Marlene, grávida de dois meses, pelo apoio e compreensão.

Agradecimentos

À pesquisadora Marina Michiyo Sugaya, pela sua sabedoria de vida e pela oportunidade de meu ingresso nesta Instituição.

Aos meus amigos do departamento de redes do IPT, especialmente ao Rui e à Fátima da CGP, pelo apoio e compreensão na execução do trabalho.

A todos do Cenatec (Centro de Aperfeiçoamento Tecnológico), por toda a orientação e infra-estrutura necessária para a realização do trabalho.

Ao meu orientador professor Antonio Luiz Rigo, pela confiança depositada em mim e pelos valiosos períodos dedicados para a conclusão deste trabalho.

A Deus, pela saúde e por proporcionar esse passo importante na minha vida.

Sumário

Anexos

Lista de Figuras

Lista de Tabelas

Resumo

O protocolo IPv4 pode ser visto como um dos maiores inventos da história da Tecnologia da Informação das últimas décadas, sendo a base da rede mundial Internet conectando pessoas e organizações em qualquer lugar a qualquer hora em todo o planeta. Porém, a comunidade acadêmica e as empresas perceberam que o IPv4 não está apto às exigências das tecnologias atuais e das novas aplicações com características diferenciadas das existentes, exigindo reformulação na sua atual estrutura. Além disto, o aumento da popularidade da Internet reforça ainda mais esta idéia, uma vez que não suportará a grande demanda de equipamentos e usuários que ainda irão se conectar à Internet, como celulares, PDAs, *home appliances* etc.

O novo protocolo IPv6 provoca mudanças importantes, tais como: a ampliação do esquema de endereçamento, suporte a aplicações em tempo real, segurança, mobilidade e cabeçalhos mais simplificados, tornando a rede Internet com uma maior escalabilidade e eficiência conforme exigência das novas aplicações que estão sendo desenvolvidas.

O IPv6 tem a incumbência de substituir o IPv4, mantendo suas melhores características e oferecendo soluções para várias restrições da atual versão. Existem diversos mecanismos de transição em desenvolvimento que manterão a convivência harmoniosa entre as duas versões, até a migração total da rede para IPv6.

Este trabalho busca abordar as possibilidades oferecidas pelo protocolo IPv6 e os serviços associados. Pretende-se enfatizar também vários problemas decorrentes do uso do NAT na rede do IPT, denominada IPTNet, as novas características do protocolo IPv6 e o impacto dos principais métodos de transição existentes.

Como parte do trabalho, montou-se uma rede de testes piloto IPv6, realizando várias comparações com os protocolos IPv4, NAT e IPv6 e posteriormente interligando esse ambiente ao *backbone* mundial IPv6, denominado *6Bone*, através da RNP (Rede Nacional de Pesquisa).

Abstract

The IPv4 protocol can be seen as one of the largest inventions of history of the Technology of Information on these last decades, being the base of the world the Internet connecting people and organizations anywhere to any hour in the whole planet. Even so, the academic community and the companies noticed that the IPv4 is not capable of the demands of current technologies and new applications with differentiated characteristics of the existent ones, demanding an improvement in its current structure. Besides this the increase of Internet popularity still reinforces more this idea, once it won't support the great demand of equipments and users that will still connect to the Internet, as celular, PDAs, home appliances etc.

The changes associated with the option of the new IPv6 protocol are of the highest importance such as: the increase of address outline, support for real time applications, safety, mobility and simplified headers, turning the Internet with a large escalability and with large acting according to demand of the new applications that are being developed.

The IPv6 protocol has the great incumbency today of substitute the IPv4, maintaining its best characteristics and offering solutions for several restrictions of the current version. There are several transition mechanisms in development that will maintain a harmonious coexistence among the two versions, until the total migration of the net for IPv6 protocol.

This work intends to approach the possibilities offered by the IPv6 protocol and the associated services. It intends to emphasize the several current problems with the use of NAT in the IPT net, denominated IPTNet, the new characteristics of the protocol IPv6 and the impact of the main existent transition methods.

As part of the this work it will be setting up a net for pilot test with the IPv6 protocol, accomplishing several acting tests with the IPv4, NAT and IPv6 protocols and later on interconnecting that sets to the world backbone IPv6, denominated *6Bone*, through RNP (National Research Net).

Estrutura da dissertação

O primeiro capítulo expõe os objetivos e a motivação do trabalho relatando os principais problemas apresentados pelo atual protocolo IPv4 e o cenário da atual Rede IPTNet, descrevendo a estrutura física/lógica e principais dados estatísticos.

O segundo capítulo traz um histórico sobre a criação do protocolo IPv4, estrutura do cabeçalho, esquema de endereçamento de classe TCP/IP e características gerais.

O terceiro capítulo apresenta o desenvolvimento do protocolo IPv6, mudança de representação do endereçamento IPv6, tipos de endereços, formato do cabeçalho IPv6, os cabeçalhos de extensão suportados pelo IPv6 e características gerais.

O quarto capítulo faz uma abordagem geral sobre o NAT, técnicas de conversão de endereços estáticos e dinâmicos, descrevendo as principais vantagens e desvantagens da sua implementação, relatando os problemas em potencial que estão sendo visualizados nas novas aplicações pelo Comitê Gestor da Internet no Brasil.

O quinto capítulo descreve os principais métodos e mecanismos de transição existentes do protocolo IPv4 para o IPv6, e vice-versa, que estão sendo desenvolvidos basicamente em três grupos: protocolo de pilha dupla, tunelamento e a translação de pacotes IPv4-IPv6.

O sexto capítulo explana como está o posicionamento do IPv6 em nível mundial, citando os principais projetos e enfatizando a rede de testes denominada *6Bone*. Será descrito também o atual estágio e como aderir ao *backbone* da rede IPv6 no Brasil chamada de *Br6Bone*, gerenciada pela Rede Nacional de Pesquisa – RNP com vários pontos interligados.

O sétimo capítulo apresenta a montagem da rede de testes implementada no ambiente da rede IPTNet, composto de sistemas operacionais Linux (RedHat) e Windows (2000 Server e XP), descrevendo a interligação da rede com o *backbone* mundial IPv6, metodologia utilizada e os resultados dos experimentos realizados.

No oitavo capítulo, a conclusão do trabalho e perspectivas de trabalhos futuros.

Capítulo 1 - INTRODUÇÃO

1.1. Objetivo e motivação do trabalho

Este trabalho pretende abordar e explorar as possibilidades oferecidas pelo protocolo IPv6, disseminando a sua utilização à rede IPTNet, centros de pesquisa e também ao mestrado profissional do IPT.

O IPv4, amplamente utilizado nas últimas duas décadas, é um protocolo não-orientado à conexão, não-confiável e trabalha com o principio da entrega dos pacotes seguindo a regra do melhor esforço, rodando nas mais variadas arquiteturas de redes e sistemas operacionais.

Com o crescimento exponencial da Internet, o IPv4 deve ser remodelado, provocando o desenvolvimento de um novo protocolo IPv6 provido de características como: maior espaço de endereçamento, menor número de entradas nas tabelas de roteamento, maior escalabilidade, segurança nativa, suporte à mobilidade, *multicast* mais eficiente, facilidade de configuração e qualidade de serviço exigido pelas novas aplicações.

Os protocolos IPv4 e IPv6 não são diretamente compatíveis, exigindo que programas sejam reescritos. Dessa forma, é necessário desenvolver mecanismos de transição eficientes, visando habilitar aplicações para continuarem a trabalhar, enquanto a infra-estrutura de rede com o novo protocolo seja atualizada de modo gradativo.

O desenvolvimento e as implementações dos mecanismos de transição devem ser transparentes para serviços e aplicações já existentes, que utilizam os protocolos TCP (orientado à conexão) e UDP (não-orientado à conexão), também chamado de serviço datagrama, alterando os cabeçalhos IPv4 para IPv6, e vice-versa, dos pacotes que trafegam através da rede.

A configuração, administração e operação do IPv6 são mais fáceis do que o IPv4, e aspectos como, segurança e proteção, foram introduzidos, devido a uma forte exigência das novas aplicações, principalmente relacionadas à transação e comércio eletrônicos de dados.

Além disso, o IPv6 possui o espaço de endereçamento muito maior, e uma das metas é utilizar cada endereço IP uma única vez. Amplia o suporte a *multicast* presente no IPv4, para sustentar a transmissão de videoconferências ou realizando a comunicação de um *site* para um grupo selecionado de usuários, por meio da Internet.

Os cabeçalhos dos pacotes IPv6 são extensíveis e concatenados permitindo a transporte de informações adicionais exigidas para uma determinada transmissão, sendo possível criar novos tipos de pacotes e serviços de rede, como requisitos de qualidade de serviço, associadas à determinada aplicação em trânsito pela rede.

A atual implementação do protocolo IPv4 está baseada no fato de que os dispositivos e as redes são fixos. Cada vez mais equipamentos móveis estão sendo conectados à Internet, aparelhos celulares, carros equipados com computadores, jogos e, até mesmo, redes completas estão se tornando móveis.

Por meio da mobilidade e da facilidade de configuração, os equipamentos de rede necessitam conectar-se a diferentes dispositivos em diferentes redes, sendo requisito fundamental que essas conexões sejam dinâmicas e transparentes para o

usuário final. A idéia de estar conectado em qualquer lugar a qualquer hora é essencial no mundo globalizado.

Dessa forma, entre os vários objetivos desse trabalho, podem-se destacar:

a) estudar as vantagens de utilização do protocolo IPv6 na Rede IPTNet em substituição do endereçamento IPv4 e do protocolo NAT utilizando endereço IP privativo;

b) promover a evolução dos novos protocolos, participando do processo de avaliação e depuração liderado pela RNP e conduzido por um seleto grupo de colaboradores da Internet e projetos afins;

c) disponibilizar serviços IPv6 à comunidade acadêmica e parcerias com institutos e empresas do setor público e privativo;

d) analisar os diversos mecanismos e procedimentos que ajudem a transição IPv4-IPv6.

e) comparar o protocolo IPv4 em relação ao IPv6 em ambientes de rede utilizando a infra-estrutura do *backbone Gigabit Ethernet* da rede IPTNet;

f) instalar uma rede piloto IPv6 no mestrado profissional do IPT para que os alunos tenham um ambiente ideal para realizar novos estudos e desenvolvimento de aplicações para o IPv6.

1.2. Instituição

O IPT é uma instituição centenária ligada à Secretaria de Ciência, Tecnologia e Desenvolvimento Econômico do Estado de São Paulo, situado numa área construída de 87.000 m² no campus da Cidade Universitária, no qual trabalham cerca de 1.500 funcionários, desse total, 400 são pesquisadores.

O IPT cumpre seu objetivo atuando em três grandes áreas: inovação, pesquisa e desenvolvimento. Desenvolve, ainda, programas específicos de apoio a micro e pequenas empresas, apoio às exportações, garantia da qualidade de produtos e serviços e a diretrizes de políticas públicas. Contando com os seus 72 laboratórios e equipes de pesquisa, são elaborados relatórios técnicos sobre diagnósticos, estudos e análises teórico-experimentais, entre outros serviços.

Outras atividades de relevo do Instituto dizem respeito à difusão do conhecimento científico e tecnológico. São atendidas, anualmente, cerca de 20 mil consultas a sistemas de informação tecnológica, tais como normas, informações referenciadas, relatórios técnicos e pesquisas bibliográficas especializadas.

1.3. Cenário da rede IPTNet

Iniciado em 1990, o projeto de implantação da Rede de Comunicação de Dados do IPT, denominada IPTNet, vem sendo continuamente adequado às tendências do mercado mundial, adotando sempre soluções de arquiteturas abertas.

A estrutura central da rede IPTNet está implementada em topologia estrela baseada em um *backbone* de tecnologia *Gigabit Ehernet*, conforme figura 1. Cada prédio interligado recebe um *link Gigabit*, ramificado internamente em *Fast-Ethernet* e/ou *Ethernet* dependendo do porte do prédio, quantidade de *hosts* e tipo de aplicações existentes.

A rede é composta basicamente de equipamentos da marca 3Com com *swicthes* nível 3 no núcleo central, contendo VLANs associadas à sub-redes IP por divisão/projetos.

O Instituto conta com aproximadamente 1.500 contas de usuários e 1.400 *hosts* instalados (entre servidores e *desktops*), a grande maioria composta por *hardware* com processadores Intel e com sistemas operacionais Solaris, Linux, Windows 9x/ME/NT/2000 e Netware 4.x.

Nas estatísticas dos principais serviços corporativos oferecidos pela rede IPTNet no ano de 2001 teve-se: 1 milhão de e-mails enviados e 600 mil recebidos; computando as listas de discussão interna e do mestrado, 7 mil acessos via linha discada e 460 mil consultas aos servidores Web.

A seguir, apresentam-se os principais dados a respeito da rede IPTNet.

a) *link* de acesso - 100 Mbps via CCE-USP, para acesso à rede mundial Internet;

b) cabeamento - fibra óptica: 25 km de fibra óptica multímodo (62,5/125 μm) e 15 km de fibra monomodo (10/125 μm) interligando 36 prédios. Cabo metálico: 150 km de cabo UTP categoria 5/5e para o cabeamento interno das redes locais dos prédios;

c) pontos de telecomunicações – o IPT possui aproximadamente 4.000 pontos de telecomunicações (dados e voz);

d) equipamentos de rede - um *switch* nível 3 marca Foundry modelo FastIron 4802, um *switch* marca 3Com modelo 4060, um *switch* nível 3 marca 3Com modelo 4007, um roteador marca 3Com modelo Netbuilder II, 33 *switches* marca 3Com modelo 3300, 3 *switches* marca 3Com modelo 4400, 45 *hubs* conectados aos *switches* , um servidor de linha discada marca USR Total Control modelo Enterprise 1000, contendo um canal E1 com 30 modems padrão V.90 (56K);

e) servidores centrais - 2 *workstations* marca Sun modelos Sparc 20 e Sparc 4, 12 servidores marca Itautec modelos InfoServer e InfoWay, 3 servidor marca Compaq modelos Prosigna 500 e Prosigna 300;

e) sistemas operacionais servidores - Solaris, Linux (distribuições Conectiva, Debian e Red Hat) e Microsoft (NT/2000);

f) serviços disponíveis - DNS (BIND), SMTP (POSTFIX), POP3 (QPOPPER), autenticação (RADIUS), listas (PETIDOMO), Web (APACHE), Web Intranet (IIS), Webmail, FTP (PROFPD), proxy (SQUID), sistema de LOG (Syslogd), WINS , gerenciamento da rede IPTNet (CA, SUNNET MANAGER e Transcend), analisador de tráfego (MRTG);

g) *hosts* – 1.484 *hosts* (servidores, estações de trabalho e microcomputadores) e 1.560 contas de usuários cadastrados;

h) contas de e-mail – 2.061 usuários cadastrados e com acesso ao correio eletrônico;

i) endereçamento TCP/IP - A Rede IPTNet conta com cinco endereços classe "C" públicos, adquiridos via FAPESP, e a adoção de uma rede privativa classe "A" para a rede interna, utilizando o protocolo NAT (*Network Address Translation*) para a conversão de endereços privativo para público e vice-versa implementado diretamente no roteador.

O esquema de endereçamento privativo adotado na rede IPTNet foi o seguinte:

Endereço IP	10.VLAN.PREDIO.HOST
Mascara rede	255.255.0.0
Gateway	10.VLAN.0.1

Tabela 1 – Esquema de endereçamento privativo adotado IPTNet.

j) VLANs (LANsVirtuais) – Existem 25 VLANs configuradas por divisão/projetos do IPT, e o roteamento IP é realizado no *switch* de camada 3 central localizado no prédio 39;

Divisão	**Rede (IP)**	**Número (VLAN)**
IPTNET	10.0.0.0	100
CEF	10.1.0.0	18
DEC	10.2.0.0	2
DIMET	10.3.0.0	3
DQ	10.4.0.0	4
DME	10.5.0.0	5
DE/AJ/ASO/CCT/GQ	10.6.0.0	6
DITT	10.7.0.0	7
CENATEC	10.8.0.0	8
DITEL	10.9.0.0	9
DEES	10.10.0.0	10
CITEC	10.11.0.0	11
CRH	10.12.0.0	12
DPF	10.13.0.0	13
DIGEO	10.14.0.0	14
CS	10.15.0.0	15
CGP	10.16.0.0	16
SAC	10.17.0.0	17
Default (Gerenciamento)	10.100.0.0	1
PROGEX	10.200.0.0	200
SPDESIGN	10.201.0.0	201
IPv6	10.206.0.0	206
DMZ	200.18.53.0	202
BIDIRECIONAL	200.18.106.0	106
PEDAGOGICA	200.18.109.0	203

Tabela 2 – Configuração de sub-redes IP associadas a VLANs da rede IPTNet.

Figura 1 - Projeto físico da rede IPTNet

Capítulo 2 - PROTOCOLO INTERNET VERSÃO 4 - IPv4

2.1. Introdução

O protocolo IPv4 com endereço de 32 bits poderia suportar aproximadamente 4 bilhões de computadores, número esse muito maior que qualquer expectativa por parte dos projetistas que organizaram este espaço de endereçamento em classes (grandes e pequenas), atribuindo grandes classes para grandes empresas e instituições.

Com a virada do milênio, percebeu-se que devido à natureza hierárquica da Internet, o número de endereços IPv4 apresentou a sua saturação em termos práticos. O crescimento exponencial de *hosts* conectados à rede exauriu o espaço de endereçamento tornando o IP um recurso escasso.

Em janeiro de 2002, as estatísticas do *Internet Software Consortium* (www.isc.org) mostram existir cerca de 147 milhões de endereços distribuídos para *hosts* conectados diretamente na Internet. A Tabela 3 ilustra o motivo desta preocupação, com respectiva taxa de crescimento anual.

Ano:	Número de *hosts*	Crescimento ao ano
1994	2.217.000	59,22%
1995	4.852.000	118,85%
1996	9.472.000	95,21%
1997	16.146.000	70,46%
1998	36.739.000	27,94%
1999	43.230.000	17,66%
2000	72.398.092	67,47%
2001	109.574.429	51,34%
2002	147.344.723	34,46%

Tabela 3 – Taxa de crescimento da Internet.

A utilização em massa da Internet estimulou a criação e o desenvolvimento de uma grande quantidade de aplicações para o protocolo TCP/IP, com suporte a serviços que não podem ser providos de maneira eficaz pelo IP atual. Um exemplo deste tipo de serviço é a multimídia, que necessita de transmissões de vídeo e som pela rede.

Com as aplicações de transações eletrônicas, surge a necessidade de que os dados transmitidos tenham autenticação, privacidade e integridade. A definição atual do protocolo em questão não implementa esquemas de segurança, tornando o ambiente da Internet inseguro para tráfego de dados não-criptografados, aliado à incerteza de que o *host* em contato seja mesmo aquele que diz ser.

2.2. Histórico

O protocolo IPv4, descrito na RFC 1166, teve a sua origem nas redes de computadores do Departamento de Defesa norte-americano no final dos anos 70, tendo sido formalmente definido em 1981. A rede designada por ARPANET (*Advanced Research Projects Agency Network*) foi a primeira a ter este protocolo implementado.

O objetivo era permitir a interconexão de redes de computadores, transferindo blocos de dados denominados datagramas de um endereço IPv4 origem para um de destino. O protocolo fornece também serviço de fragmentação e remontagem de datagramas, quando necessário, para que estes possam ser transmitidos através de redes onde o tamanho máximo permitido para os pacotes é pequeno [TAN97].

O sucesso do protocolo TCP/IP tem ultrapassado as expectativas mais otimistas dos seus proponentes, devido aos seguintes aspectos:

- arquitetura aberta e simplificada;
- facilidade e disponibilidade das especificações técnicas RFC (*Request for Comments*);
- endereçamento hierárquico dividido em classes;
- facilidade de fragmentação e remontagem de pacotes;
- roteamento adaptativo distribuído nos roteadores;
- protocolo embasado no modelo cooperativo e de interoperabilidade;
- suporte a diversos meios de comunicação.

2.3. Arquitetura de protocolos TCP/IP

O termo TCP/IP, acrônimo de *Transmission Control Protocol/Internet Protocol*, é um conjunto de protocolos, em que dois dos mais importantes protocolos (IP e TCP) deram seus nomes à arquitetura. O protocolo IP, base da estrutura de comunicação da Internet, é um protocolo baseado na tecnologia de comutação de pacotes.

O protocolo TCP/IP pode ser utilizado sobre qualquer estrutura de rede, seja ela simples, como uma ligação ponto-a-ponto, ou uma rede de pacotes complexa. Como exemplo, podem-se empregar estruturas de rede, como *Ethernet*, FDDI, PPP, ATM, Frame-Relay, Fibre Channel, enlaces de satélite, e várias outras, como meio de comunicação do protocolo TCP/IP.

A arquitetura TCP/IP possui uma série de diferenças em relação à arquitetura OSI, que se resumem principalmente nos níveis de aplicação e inter-rede da arquitetura TCP/IP.

A Figura 2 ilustra a comparação entre TCP/IP e OSI. Notar que a camada inter-rede de TCP/IP apresenta altura menor que o correspondente nível de rede OSI. Isto representa o fato de que uma das funções do nível de rede OSI é realizada pelo nível de rede TCP/IP, para a entrega local de mensagens dentro da mesma rede. A decisão de roteamento é tratada quando a origem e o destino da mensagem estão situados em redes distintas.

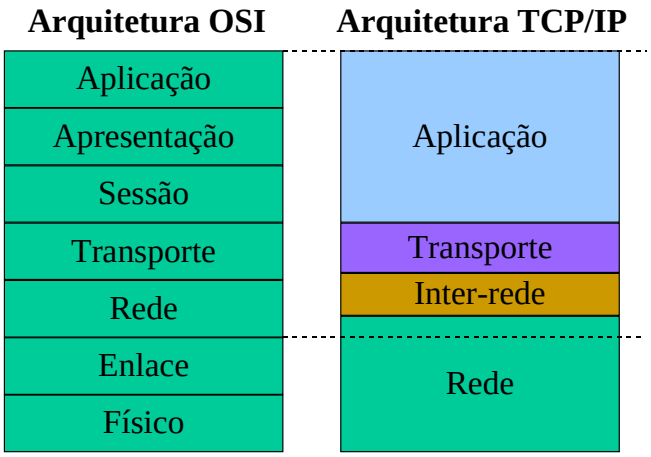


Figura 2 – Comparação OSI x TCP/IP.

2.4. Protocolo IPv4

O Protocolo IPv4 é responsável pela comunicação entre máquinas em uma estrutura de rede TCP/IP. Ele provê a capacidade de comunicação entre cada elemento componente da rede para permitir o transporte de uma mensagem de uma origem até o destino. O protocolo IP provê um serviço sem conexão e não-confiável entre máquinas em uma estrutura de rede [SOA95].

As funções mais importantes realizadas pelo protocolo IPv4 são a atribuição de um esquema de endereçamento da rede utilizada, além da capacidade de tomar decisões de roteamento para o transporte das mensagens entre os roteadores.

2.4.1. Formato do datagrama IPv4

O cabeçalho IPv4 tem uma parte fixa de 20 bytes (tamanho mínimo) e uma parte de opcionais de tamanho variável podendo atingir 40 bytes, limitando o cabeçalho total a 60 bytes, conforme Figura 4.

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				Padding

Figura 3 - Campos do datagrama IPv4.

2.4.2. Campos do cabeçalho IPv4

Campo: *Version.*
Tamanho: 4 bits.
Descrição: Mostra a versão do protocolo IP usada no datagrama, possuindo o valor 4.

Campo*: Identification Header Length* (IHL).
Tamanho: 4 bits.
Descrição: O comprimento do cabeçalho IP pode ser variável, e esse campo indica o tamanho em palavras de 32 bits, para o uso de campos opcionais.

Campo**:** *Type of Service*.
Tamanho: 8 bits.
Descrição: A função desse campo é armazenar parâmetros de qualidade de serviço (QoS) por onde trafega um datagrama, devendo ser utilizado para priorizar aplicações do tipo multimídia e sensíveis a atraso. Na versão IPv4, é ignorado na maioria das implementações.

Campo: *Total Length*.
Tamanho**:** 16 bits.
Descrição**:** Indica o tamanho total do datagrama, incluindo a parte do cabeçalho e dados, especificado em bytes.

Campo: *Identification*.
Tamanho: 16 bits.
Descrição: Usado na fragmentação de datagramas, possui um número único atribuído pelo *host* de origem, para o reagrupamento do datagrama fragmentado pelos roteadores durante o percurso realizado e do MTU de cada rede física percorrida pelo datagrama.

Campo: *Flags.*
Tamanho: 3 bits.
Descrição: Usado na fragmentação de datagramas. Possui controles de DF (não-fragmentar) e MF (mais fragmentos).

Campo**:** *Fragment Offset*.
Tamanho: 13 bits.
Descrição: Usado com datagramas fragmentados, para ajudar no reagrupamento completo do datagrama. O seu valor é composto com valor múltiplo de 64 bits (parte de dados) que estão contidos nos fragmentos anteriores. No primeiro fragmento este valor é sempre zero.

Campo**:** *Time to Live*.
Tamanho: 8 bits.
Descrição: Usado para limitar o tempo de vida (em segundos) de um datagrama na rede. Esse campo recebe um valor inicial quando o datagrama é criado e, para cada roteador por onde o datagrama passa, deve-se subtrair deste campo o tempo usado para o seu processamento. Para cada passagem pelo roteador, esse campo é decrementado de uma unidade. Como o roteador é capaz de processar um datagrama em menos de um segundo, o campo TTL tornou-se uma métrica de número de saltos, em vez de métrica de tempo subtraindo o valor 1 desse campo a cada salto. Quando o valor atingir zero, o datagrama é descartado, e uma mensagem enviada ao emissor, através do protocolo ICMP [SOA95].

Campo*: Protocol.*
Tamanho: 8 bits.
Descrição: Indica o protocolo de nível superior para quem o datagrama deve entregar os dados. Os mais usados na internet são ICMP (valor 1), TCP (valor 6) e UDP (valor 17).

Campo: *Header Checksum*.
Tamanho: 16 bits.
Descrição: Verifica e garante a integridade do cabeçalho IP. Caso exista algum erro, o datagrama deve ser ignorado. Esse campo não garante a integridade dos dados contidos no datagrama, função dos níveis superiores de protocolos.

Campo: *Source Address*.
Tamanho: 32 bits.
Descrição: Endereço de *host* origem do datagrama.

Campo: *Destination Address*.
Tamanho: 32 bits.
Descrição: Endereço de *host* destino do datagrama.

Campo: *Options.*
Tamanho: variável.
Descrição: Este campo pode ser usado para serviços extras, como informações de segurança, roteamento na origem, depuração etc. Uma implementação IP não necessita ser capaz de gerar opções nos datagramas criados, porém todas as implementações de IP precisam ser capazes de processar e suportar todas as opções [MUR00].
Alguns exemplos de opções válidas:
a) *Security*: especifica o nível de segurança do datagrama.
b) *Strict Source Routing*: especifica no datagrama qual a rota a ser seguida, retirando esta liberdade do roteador. Em geral é usado para testes de rede.
c) *Record Route*: anota a rota de cada roteador por onde o datagrama trafegou.

Campo*: Padding*.
Tamanho: variável.
Descrição: No caso da utilização do campo anterior, o datagrama é preenchido até o próximo byte, garantindo que o cabeçalho tenha um tamanho múltiplo de 32 bits.

2.4.3. Endereçamento IPv4

Os endereços IPv4 consistem em números de 32 bits, compostos de quatro octetos, como por exemplo, 200.18.109.44. A primeira parte do endereço identifica uma rede específica e a segunda, um *host* dentro dessa rede. Uma interface de rede pode ser associada a vários endereços IP.

Foram definidas três classes principais de endereços, que fornecem alguma flexibilidade no endereçamento de redes de várias dimensões. A Tabela 4 mostra a capacidade máxima de endereçamento do atual protocolo IPv4.

A existência de classes de endereços fixas é um fator limitante e que leva à utilização ineficiente do espaço de endereçamento disponível, dependendo do porte das redes.

Classe	Formato	Prefixo	Redes	*Hosts*
A	7 Bits Rede, 24 Bits Host	0	128	16.777.216
B	14 Bits Rede, 16 Bits Host	10	16.384	65.536
C	21 Bits Rede, 8 Bits Host	110	2.562.097.152	256
D	*Multicast*	1110		
E	Uso futuro	11110		

Tabela 4 - Classes de endereços IPv4.

Na primeira classe de endereços, classe “A”, o bit mais significativo é 0, os outros sete bits do primeiro octeto identificam a rede, e os 24 bits restantes definem o endereço de *host*. Essa classe de endereços é usada para redes de grande porte, os endereços de rede variam de 1.0.0.0 a 126.0.0.0, e cada rede tem capacidade de endereçar cerca de 16 milhões de *hosts*. O endereço 127.0.0.1 é utilizado como *loopback* na interface local.

Os endereços de classe “B” usam dois bytes para o número da rede e dois para o endereço de *host*. Os endereços de rede da classe B situam-se na faixa de 128.1.0.0 até 191.254.0.0, e cada rede pode interligar cerca de 65 mil *hosts*.

Os endereços de classe “C” utilizam três bytes para identificar a rede e um para o *host*. Os endereços de rede situam-se na faixa de 192.0.1.0 até 223.255.254.0 e cada rede pode endereçar 254 *hosts*.

A ineficiência desse esquema de endereçamento mostrou ao longo do tempo que o IPv4 capaz de suportar as exigências atuais relacionadas às novas tecnologias e às diversas áreas de negócio.

A criação do CIDR (*Classless Inter-Domain Routing*) descrito na RFC 1519, foi a solução adotada para adiar, por mais algum tempo, o problema de exaustão do espaço de endereçamento durante a fase de desenvolvimento e transição para o novo protocolo IPv6, possuindo um esquema de endereçamento mais eficiente de alocação de IPs. Conforme estatísticas do grupo de trabalho do IETF *Lifetime Expectations* (www.ietf.org), a previsão é que seja para meados do ano 2008.

2.4.4. Classless Inter-Domain Routing (CIDR)

Nas classes de endereços existentes na Internet, existem milhões de endereços IPv4 desperdiçados, principalmente em classes “A” e “B”, e como o custo da concessão de um espaço de endereçamento é associado com a classe da rede, as organizações deveriam optar pela dimensão que satisfaça suas necessidades a um custo mínimo.

Entre as três classes, a mais procurada foi a classe “B”, por balancear a quantidade de redes e *hosts*, já que a classe “A”, com 16 milhões de endereços IPv4, é muito grande para a maioria dos casos; e uma rede da classe “C”, com 256 endereços, é muito pequena.

Para evitar o desperdício de endereços, o ideal seria que fossem alocadas redes de classe “C”. Dessa forma, caso uma organização necessitasse de 1.000 endereços IPv4, receberia um bloco de 1.024 endereços na forma de quatro redes classe “C” com 256 *hosts* em cada uma.

No caso do *backbone* da Internet, os principais roteadores devem conter informações de todas as redes interligadas, para poder encaminhar os pacotes aos respectivos destinos. O ideal para a alocação de endereços não é o mesmo para o roteamento, gerando um enorme crescimento das tabelas de roteamento, sendo amenizado com a criação do CDIR.

As regras de alocação foram alteradas pela RFC 1519, que dividiu o mundo em quatro zonas e atribuiu uma parte do espaço de endereçamento da classe “C” para cada uma delas. A alocação foi feita da seguinte forma:

Região	Endereços alocados
Europa	194.0.0.0 a 195.255.255.255
América do Norte	198.0.0.0 a 199.255.255.255
América Central e do Sul	200.0.0.0 a 201.255.255.255
Ásia e região do Pacífico	202.0.0.0 a 203.255.255.255

Tabela 5 - Alocação das redes classe “C” por região para CIDR.

No CIDR, os blocos são referenciados como redes de prefixo. Por exemplo, uma rede classe “A” passou a ser referenciada com uma rede de prefixo /8, significando que os 8 bits do endereço definem a porção de rede. Uma forma alternativa de descrevê-lo é através da máscara 255.0.0.0 (da mesma forma, o prefixo /16 pode ser descrito por 255.255.0.0). Por meio de um método denominado *supernetting*, é possível criar e agrupar um número maior de redes com máxima eficiência devido à diminuição das tabelas de roteamento.

O objetivo prático desse método é a utilização de regras de prefixos, delegando espaços de endereçamento mais realistas; ao invés do uso das tradicionais classes “A”, “B” e “C”, que são de tamanhos impróprios para a grande maioria dos casos.

Na Tabela 6, são relacionados alguns exemplos de prefixos para identificação de redes pelo CIDR.

Prefixo CIDR	Equivalente na classe “C”
/8	65.536
/9	32.768
/10	16.384
/11	8.192
/12	4.096
/13	2.048
/14	1.024
/15	512
/16	256 (ou 1 classe B)
/17	128
/18	64
/19	32
/20	16
/21	8
/22	4
/23	2
/24	1

Tabela 6 - Equivalência entre prefixos CIDR e redes classe “C”.

Parte do espaço de endereçamento regional é atribuído a provedores que operem dentro dessa zona geográfica. Paralelamente foram desenvolvidos novos protocolos de roteamento, com capacidade para utilizar agregação de informação de roteamento segundo a norma CIDR.

2.4.5. Serviço sem conexão

O serviço oferecido pelo protocolo IP é sem conexão. Portanto, cada datagrama IP é tratado como uma entidade independente que não possui relação com qualquer outro datagrama. Não é usado qualquer mecanismo de controle de erros nos dados, exceto o *checksum*, para garantir que as informações contidas no cabeçalho estão corretas e íntegras.

O IPv4 é um protocolo não-orientado à conexão (não-confiável), pois não garante que o datagrama venha a ser entregue corretamente ao destino. O IP define também o caminho que cada pacote deve percorrer e o modo como as diversas máquinas e roteadores devem processar os pacotes, como e quando gerar as mensagens de erros e em que condições os pacotes devem ser descartados [TAN97].

O TCP é um protocolo de camada transporte, situado logo acima da camada de rede. Oferece um serviço orientado à conexão, com confiabilidade de comunicação fim a fim, de modo a fornecer qualidade de serviço às aplicações criadas sobre este protocolo. O TCP faz a retransmissão de pacotes perdidos, descarta pacotes duplicados, reordena pacotes recebidos fora de ordem, fragmenta dados em pacotes de 64K (tamanho máximo de um pacote IPv4) e faz o controle de fluxo.

Por outro lado, o protocolo UDP, que também é um protocolo de camada de transporte, possui a função de multiplexador para o envio e recebimento de datagramas utilizando portas para direcionar os datagramas para as aplicações. O protocolo UDP é similar ao IP, no aspecto de não ser orientado à conexão, e as funções de retransmissões,

pacotes duplicados, ordenação de pacotes devem ser implementados pelas aplicações que utilizam o UDP.

2.4.6. Fragmentação e remontagem de datagramas

O IP foi concebido para uma ampla variedade de tipos de *hardware* de redes. Diferentes tipos de redes têm restrições diferentes quanto ao tamanho máximo de dados que pode ser transmitido pela camada de enlace. Um exemplo muito conhecido é o caso do IP sobre *Ethernet*, cujo quadro tem um tamanho máximo MTU (*Maximum Transmission Unit*) de 1.518 bytes.

A seguir, exemplos de tamanhos máximos de pacotes de algumas tecnologias [OPP99].

Tecnologia	**Tamanho máximo (bytes)**
Ethernet e *Fast-Ethernet* 10/100 Mbps	1.518
Token Ring 4 Mbps	4.500
Token Ring 16 Mbps	18.000
FDDI	4.500
ATM com AAL5	65.535
ISDN usando PPP	1.500
T1	4.500 (não especificado), valor utilizado na prática.

Tabela 7 – Tamanhos máximos de pacotes em diversas tecnologias.

O datagrama IP pode ter no máximo 65.535 bytes, porém a camada IP do lado da origem limita o tamanho do datagrama de modo a não exceder o tamanho do MTU da rede local. Quando um datagrama tem de passar por outras redes com MTUs inferiores, os roteadores ficam encarregados de fragmentar o datagrama de modo a não exceder o MTU da rede seguinte.

A função do roteador nesse processo é negociar com os *hosts* da rede e com o próximo roteador o tamanho máximo que pode ser usado naquela sub-rede, onde datagramas com tamanhos maiores que o permitido deverão ser fragmentados. A remontagem é realizada pelo *host* destino e nunca por um roteador, por motivos de desempenho.

O cabeçalho IP contém informações suficientes para identificar cada fragmento e remontá-lo por completo no destino. Este processo tem a desvantagem de, na perda de um fragmento, perde-se o datagrama inteiro.

2.4.7. Roteamento

Na arquitetura TCP/IP, roteadores são os elementos responsáveis por interligar duas ou mais redes distintas. Redes interligadas podem ser: redes locais, redes de longa distância com comutação de pacotes ou ligações ponto-a-ponto seriais.

O roteamento entre redes é a principal função do protocolo IP, podendo ser realizada por um roteador, um *switch* nível 3 ou mesmo um *host* com mais de uma placa de rede instalada. A função do roteador é transmitir datagramas a destinatários ligados em outras redes, baseado no identificador de rede do endereço IP de destino.

As tabelas de rotas encontradas em um roteador/*host* são compostas por uma lista de interfaces locais com os endereços IP atribuídos (rotas diretas) e com a lista de redes e dos endereços IP dos *gateways* associados (rotas indiretas). Essas tabelas podem ser configuradas manualmente (estáticas) ou dinamicamente através de diversos protocolos de roteamento existentes.

Quando um roteador necessita encaminhar um datagrama, inicialmente verifica se o destino do datagrama é um *host* conectado a mesma rede. Se for, o datagrama é entregue à interface da rede, que se encarrega de mapear o endereço IP no endereço físico do *host*, encapsulando o datagrama em um quadro de rede, e finalmente transmití-lo ao destinatário.

Se o datagrama da rede de destino for diferente daquela onde se encontra o *host* IP, procura-se na tabela de roteamento uma entrada com o endereço correspondente, recuperando-se o endereço do roteador que deve ser usado para alcançar a rede de destino. Uma desvantagem deste esquema é que o tamanho das tabelas de roteamento aumenta consideravelmente, quando se liga um número grande de redes individuais, como o caso da Internet.

Para contornar esse problema, são utilizadas rotas denominadas *default*, que consistem em caminhos alternativos, quando não é encontrada uma rota específica para uma determinada rede. Através de um protocolo específico ICMP *(Internet Control Message Protocol*), o roteador informará ao módulo IP se ele é ou não a melhor escolha para alcançar uma determinada rede. Essa mensagem, chamada *redirect* no ICMP, carrega como parâmetro o endereço do roteador que é a escolha correta. O módulo IP, ao receber tal mensagem, adiciona uma entrada em sua tabela de roteamento associando a rede de destino ao endereço do roteador recebido na mensagem [OPP99].

Uma redefinição do procedimento de atribuição de endereços permitiria melhor utilização do espaço de endereçamento, como também a realização de roteamento hierárquico de redes e sub-redes, diminuindo o número de entradas nas tabelas de roteamento, conforme descrito no próximo capítulo.

Capitulo 3 - PROTOCOLO INTERNET VERSÃO 6 - IPv6

3.1. Introdução

O protocolo IPv4 sofreu poucas alterações desde sua criação, visando principalmente manter a compatibilidade com sistemas antigos, também chamados de sistemas “legados”. No decorrer deste trabalho, observar-se-á que a massificação da utilização da Internet gerou problemas que o atual IPv4 não está conseguindo atender. Tornou-se evidente a necessidade da criação e desenvolvimento de uma nova geração de protocolos denominado IPng (*IP next generation*) para suprir e expandir as atuais capacidades.

O *Internet Protocol version 6* (IPv6) foi projetado considerando-se aspectos relevantes como: redes com arquiteturas mais escaláveis, maior segurança e integridade dos dados, extensões de suporte a qualidade de serviço (QoS), autoconfiguração, maior agregação no nível do *backbone* global e, ao mesmo tempo, manter a eficiência em redes de baixos desempenho como as redes sem fio.

Dessa forma, várias funções foram alteradas e novas funcionalidades foram acrescentadas, sendo que a migração do IPv4 para o IPv6 poderá ser feita em etapas, aproveitando a atual estrutura já implementada.

Apesar de existirem vários *backbones* com IPv6 em caráter experimental, a previsão para o início de operação comercial do IPv6 é por volta de 2010. Por alguns anos, os equipamentos deverão oferecer interoperabilidade entre IPv4 e IPv6, através dos diversos mecanismos de transição (descrito no capítulo 5).

3.1.1. Visão geral

A maioria dos negócios da Internet está baseada no protocolo IPv4, contendo servidores e serviços via Web. Segundo uma pesquisa realizada pelo Garther Group, a globalização e as constantes evoluções causadas pelas novas tecnologias estão criando novos ambientes de negócios, no qual esses serviços serão integrados em todos os tipos de dispositivos e equipamentos fixos ou móveis, realizando virtualmente qualquer tarefa ou transação eletrônica.

Dentro desse contexto, a questão da mobilidade constitui um dos componentes mais importantes quanto a assuntos relacionados à revolução tecnológica a que se assiste. O protocolo IPv6 será um item extremamente relevante no enfoque aqui tratado: o IPv4 tem problemas em gerir esta facilidade, que vão além da necessidade do aumento do número de endereços IP oficiais para todos os dispositivos móveis, sendo praticamente impossível com o IPv4, por diversas razões a serem discutidas durante o trabalho.

Vislumbram também novos mercados promissores e com excelentes perspectivas de gerar negócios, podendo destacar o mercado do entretenimento através da rede, com o surgimento da tecnologia de TV digital interagindo com a Internet, a nova geração de telefones celulares de terceira geração (3G), com a Nokia lançando o seu primeiro aparelho no mercado europeu, e os aparelhos eletrônicos inteligentes baseados em microprocessadores, como os da família Nitron da Motorola com tecnologia desenvolvida no Brasil.

O futuro da Tecnologia da Informação mudará a forma de se viver em um mundo conectado, dando oportunidade de fazer mais atividades em um tempo menor, com mais objetividade e com a devida confiabilidade e segurança. A questão da comunicação sem fio se tornará um aspecto essencial, tornando o indivíduo menos dependente de certa localização geográfica.

Seguindo a tendência da evolução tecnológica nas últimas décadas o custo de acesso à Internet tende a cair, enquanto a largura de banda oferecida tende a crescer na esteira do desenvolvimento e avanço das tecnologias de fibras óticas, fazendo com que a qualidade de serviço torne-se um padrão na Internet, permitindo que clientes e/ou usuários negociem certos acordos de nível de serviço de seus provedores de acesso.

Com a convergência das aplicações para o protocolo IP, a evolução do atual protocolo IPv4 para o IPv6 e aliada à nova visão de negócios, deverá estimular a geração de aplicações, permitindo que os serviços se adaptem ao ambiente do cliente, oferecendo a qualidade de serviço esperada e o melhor desempenho final.

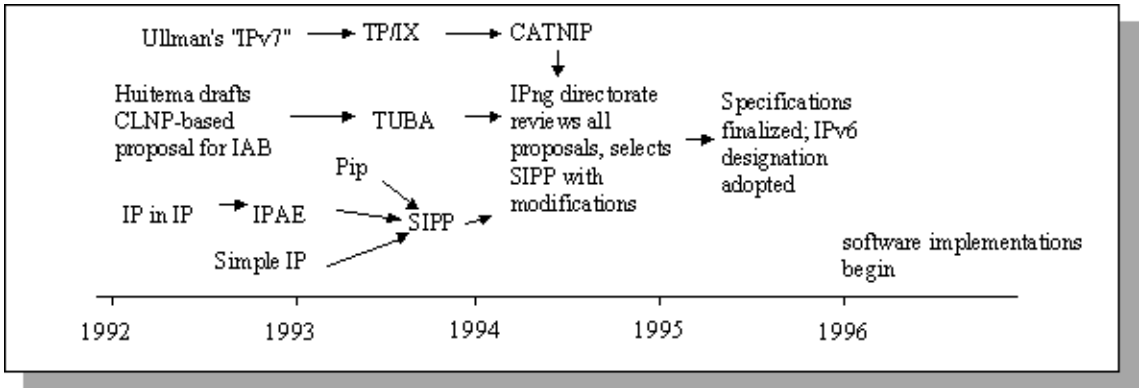
A iniciativa IPv6 não significa que as tecnologias associadas ao IPv4 estejam esgotadas, porém, quanto mais cedo forem efetivadas as implementações para o IPv6, menores serão os custos das organizações com a transição.

3.2. Histórico do IPv6

Em 1992, começaram os primeiros encontros para o desenvolvimento de um novo protocolo, denominado de IPng (nova geração) ou IPv6 (versão 6), como resultado de um longo processo de discussão que durou até 1994, com a criação pelo IETF do IPngWG (*IP Next Generation Working Group*), com base em alguns objetivos que deveriam ser alcançados para resolver os problemas do IPv4. Desde 1994, foram publicados mais de 30 RFCs relacionadas com o IPv6.

Em janeiro de 1995 foi emitido a RFC 1752, com as recomendações para o novo protocolo e, em junho de 1996, concretiza-se a idéia da construção de uma rede de testes IPv6 chamada de *6Bone*, descrita no capítulo 6, semelhantes a já existentes para testes de *multicast* (*MBone*) e para testes de qualidade de serviço (*QBone*).

Para maiores informações a respeito do histórico do IPv6, consultar o *site* (www.ipv6.org) [4] [6].



3.3. Objetivos

Os principais objetivos a serem alcançados com a nova versão do protocolo IPv6 são:

- escalabilidade;
- arquitetura simplificada e alinhada em 64 bits;
- redução da tabela de roteamento;
- expansão da capacidade de endereçamento e redução das tabelas de roteamento;
- simplificação do cabeçalho;
- suporte a cabeçalhos de extensão e opções;
- suporte à autenticação e privacidade;
- suporte á autoconfiguração (*Plug and Play*);
- suporte para seleção de rota pelo originador;
- capacidades de qualidade de serviço (QoS);
- suporte para *Jumbograms;*
- mapeamento de endereços e Nomes;
- fragmentação mais eficiente;
- melhoria em redes *multicast* através da especificação de escopos;
- reendereçamento automática de *sites* e roteadores;
- suporte à mobilidade IP com otimização de roteamento e outras melhorias;
- transição simples e flexível.

3.4. Protocolo IPv6

Um aspecto importante a salientar é que o IPv6 utiliza o termo pacote mais do que o datagrama, sendo que o significado é o mesmo, porém com formatos diferentes e utiliza o termo nó para qualquer sistema que esteja executando o protocolo IPv6, podendo ser um *host* ou um roteador [MUR00].

O protocolo IPv6 muda em grande parte o formato do seu pacote. Como é mostrado na figura 4, o cabeçalho IPv6 consiste em duas partes, o cabeçalho IP básico de tamanho fixo e os cabeçalhos de extensão podendo ser de tamanho variável.

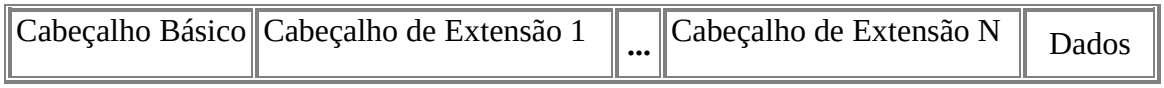


Figura 4 - Formato geral do pacote IPv6.

O cabeçalho básico possui 40 bytes com a possibilidade de zero ou mais cabeçalhos de extensão, seguidos de dados.

O formato do cabeçalho básico do IPv6 é simplificado, possuindo apenas oito campos, enquanto o IPv4 possui 14 campos, sendo os campos alinhados e múltiplos de oito bits, facilitando a sua implementação diretamente em *hardware*. Isso torna o custo de processamento dos cabeçalhos IPv6 menor, pois existem menos campos a serem processados pelos nós da rede, gastando menos largura de banda. Apesar do tamanho do endereço IPv6 ter aumentado quatro vezes, o tamanho do cabeçalho IPv6 é apenas duas vezes maior que o cabeçalho IPv4.

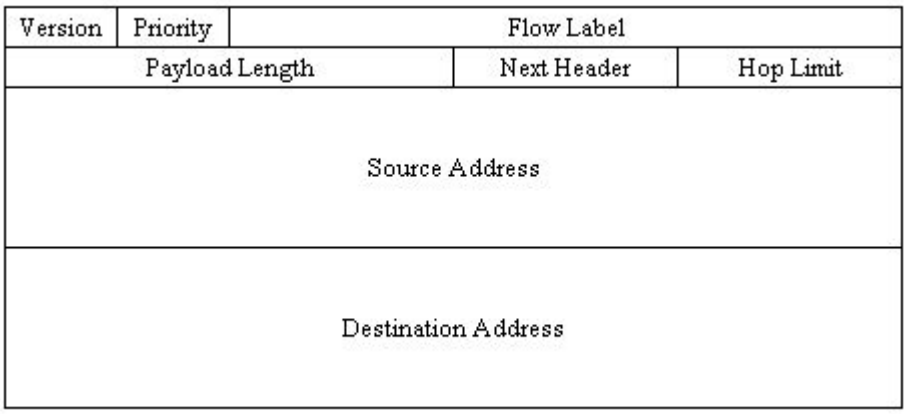


Figura 5 - Cabeçalho básico do pacote IPv6.

O tamanho do cabeçalho básico é fixo no IPv6, não havendo necessidade do campo de tamanho de cabeçalho. O campo de opcionais do IPv4 são tratados como pacotes especiais e expressos após o cabeçalho fixo principal, nos cabeçalhos de extensão, conforme RFC 2460.

O primeiro campo do cabeçalho básico foi o único que permaneceu com o mesmo significado de representar o número da versão. Os campos de tamanho do cabeçalho, tipo do serviço, identificação, *flags*, deslocamento do fragmento, e o campo de verificação de soma do cabeçalho IPv4 foram retirados. Os campos de tamanho total, tipo do protocolo e o tempo de vida foram renomeados. O mecanismo de opções foi revisado, e dois novos campos foram adicionados: o de prioridade e o de rótulo de fluxos.

O campo de tamanho total do IPv4 é colocado no campo de tamanho de carga do IPv6. O campo de vida (TTL) recebe o nome de limite de salto no IPv6, sendo que ambos são decrementados do valor 1 em cada passagem pelos roteadores. A função do campo ToS no IPv4 foi transferida para os novos campos no IPv6 denominados classe de serviço (prioridade) e rótulo de fluxo.

Dentre os campos da versão IPv4 que foram eliminados, dois merecem destaque: o de *checksum* e o de fragmentação. A função do campo de *checksum* era detectar erros que afetassem o cabeçalho IP, sem detectar, no entanto, erros no restante do pacote. Devido ao enorme desenvolvimento dos meios físicos e das fibras óticas, a maioria dos erros não é de transmissão, visto que os mecanismos de checagem de erros nos quadros *Ethernet* e PPP são bastante eficientes. Como os roteadores só alteram o campo *Hop Limit (Time-to-live)* no IPv4, estes então terminam por recalcular o *checksum*, antes de retransmitir o pacote, o que pode causar a não detecção de possíveis erros. Além disso, vários roteadores, visando aumento de desempenho, não verificavam mais este campo, terminando assim por torná-lo totalmente supérfluo.

O campo fragmentação foi excluído e os pacotes não são mais fragmentados por roteadores. O IPv4 inclui um procedimento de fragmentação de forma que os emissores possam enviar pacotes sem se preocupar com a capacidade dos retransmissores. Já no IPv6, os *hosts* devem aprender o tamanho máximo do pacote aceitável, através de uma chamada de procedimento *path MTU discovery*, descrito no item 3.4.10. Caso tentem enviar pacotes maiores, tais pacotes serão rejeitados pela rede. Dessa forma não há

necessidade dos campos de identificação do pacote, *flags* de controle da segmentação e deslocamento do fragmento.

O campo de tamanho total do IPv4 foi substituído pelo tamanho da carga útil do pacote (*payload*). Com relação ao campo tipo do protocolo, foi renomeado para tipo do próximo cabeçalho para refletir a nova organização dos pacotes IP.

O campo tipo do próximo cabeçalho será configurado para conter o tipo do primeiro cabeçalho de extensão. Enquanto que o campo tempo de vida foi renomeado para limite de saltos. No IPv4, o tempo de vida foi expresso como o número de segundos, indicando quanto tempo os pacotes permaneceriam na rede antes de serem destruídos. Já no IPv6 esse campo é decrementado a cada retransmissão, contando o número de saltos e não o número de segundos que um pacote fica na rede.

3.4.1. Cabeçalho básico

Ter um cabeçalho básico fixo e outros de extensão atende às necessidades de se possuir generalidade e eficiência na nova versão. Os mecanismos de fragmentação, autenticação, e outros que se fizerem necessários, serão tratados somente quando presentes no pacote. Para tanto, são incluídos em cabeçalhos de extensão, pois se estivessem sempre presentes, o cabeçalho básico principal do protocolo seria tão grande que o tempo de processá-lo levaria à ineficiência da rede.

A seguir, os campos que compõem o cabeçalho básico do pacote IPv6 [CHO02].

Campo: *Version*.
Tamanho: 4 bits.
Descrição: Indica qual a versão do protocolo que está sendo utilizado, neste caso o valor é igual a 6.

Campo: *Traffic Class (Priority)*.
Tamanho: 8 bits.
Descrição: O uso deste campo permite que *hosts* ou roteadores identifiquem os diferentes tipos de prioridades e classes de tráfego para pacotes IPv6. Os valores de prioridade estão divididos para dois tipos de tráfego: tráfego controlado por congestionamento e não-controlado por congestionamento. Esse campo ainda está em fase de sua total definição. O valor *default* é zero. Os nós que suportam a implementação de classe de trafego IPv6 devem ter permissão para alterar o valor desse campo para uso do serviço.

Campo: *Flow Label*.
Tamanho: 20bits.
Descrição: Usado pelo roteador para solicitar serviços de tratamento especiais. Assim como o campo anterior está em estado experimental. Os nós que não suportem funções de controle de fluxo devem definir esse campo como zero para os pacotes de origem, ignorar quando recebido ou simplesmente encaminhar o pacote.

Campo: *Payload Length*.
Tamanho: 16 bits.
Descrição: Identifica o tamanho da carga útil do pacote em bytes, excluído o cabeçalho fixo do IPv6. Se um cabeçalho de extensão for utilizado, é computado como parte da carga útil do pacote. Um *link* IPv6 pode suportar pacotes até 64 Kbytes. Para pacotes

maiores, utiliza-se a opção *Jumbo Payload*, localizada no cabeçalho de extensão *Hop-by-Hop* e o tamanho do pacote será zero.

Campo: *Next Header*.
Tamanho: 8 bits.
Descrição: Indica o tipo de próximo cabeçalho imediatamente após o cabeçalho principal do IPv6. Os valores desse campo estão descritos no item 3.4.2.

Campo: *Hop Limits*.
Tamanho: 8 bits.
Descrição: É utilizado para determinar o número máximo de equipamentos roteadores pelos quais o pacote pode trafegar. A cada nó que passa o pacote, este campo é decrementado do valor 1. O pacote será descartado quando o valor for zero.

Campo: *Source Address*.
Tamanho: 128 bits.
Descrição: É o endereço do *host* de origem do pacote.

Campo: *Destination Address*.
Tamanho: 128 bits.
Descrição: É o endereço do *host* de destino. Caso exista o cabeçalho de roteamento, este campo indica o endereço do próximo destino, e não do destino final. Este valor pode ser alterado durante o percurso.

3.4.2. Cabeçalhos de Extensão

Com a nova concepção do IPv6, cada pacote inicia com um cabeçalho básico, sendo que em vários casos será o único cabeçalho necessário para a entrega do pacote. Porém, em outros casos, é necessário que informações adicionais sejam colocadas após o cabeçalho fixo, para serem tratadas pelo destino ou pelos sistemas intermediários.

Com a simplificação do cabeçalho IPv4, alguns campos foram retirados ou passaram a ser opcionais de forma a simplificar o tratamento de um pacote comum, tornando o IPv6 mais eficiente, principalmente nos mecanismos de fragmentação e autenticação, devendo ser suportados somente quando necessários, fazendo com que o cabeçalho não carregue dados desnecessários. No protocolo IPv4 essas informações são transportadas no campo opções.

Com base na RFC 2460, todos os cabeçalhos de extensão são identificados por um valor específico e carregam no campo n*ext header* a informação do tipo do cabeçalho, sendo computados como parte de extensão do conteúdo, conforme figura 6.

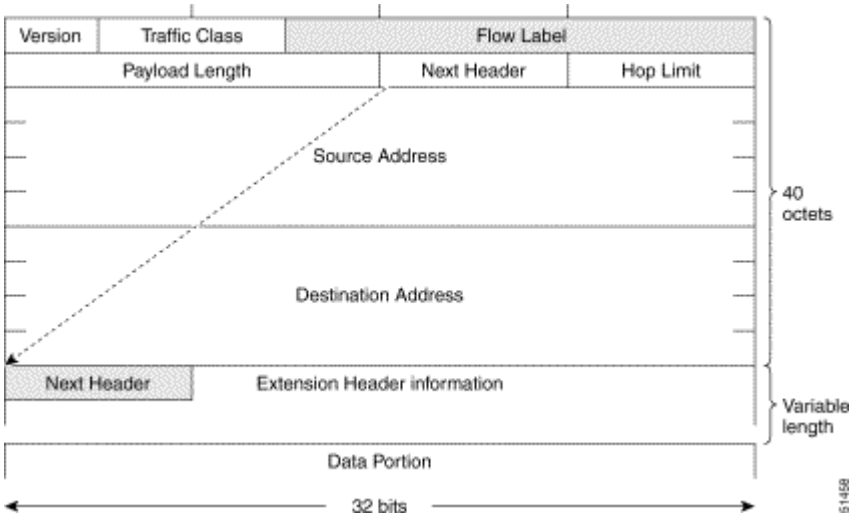


Figura 6 – Campo *Next Header*.

A seguir, a disposição dos principais cabeçalhos de extensão e respectivos valores:

a) *Hop-by-hop options* (00);
b) *Destination options* (60);
c) *Routing* (43);
d) *Fragment* (44);
e) *Authentication* (51);
f) *Encapsulating security payload* (50).

Cada cabeçalho de extensão pode aparecer no máximo uma vez em um pacote, exceto o cabeçalho de destino, que pode ocorrer uma vez antes do cabeçalho de roteamento e outra antes do cabeçalho da camada superior. A seguir, outros valores possíveis e respectivos protocolos: IP (4), TCP (6), UDP (17), ICMP (58), IDRP (45), RSVP (46), e caso não haja necessidade de nenhum cabeçalho de extensão, é associado o valor 59 (*next header* inexistente).

A implementação do IPv6 recomenda que os nós, que originam os pacotes, coloquem os cabeçalhos de extensão em uma ordem especifica, conforme visto acima. Apesar da ordem recomendada, os nós IPv6 que recebem os pacotes devem estar preparados para tratar os cabeçalhos de extensão mesmo que venham em qualquer ordem, exceto para o cabeçalho *hop-by-hop* que deve ser sempre o primeiro após o cabeçalho principal IPv6, caso exista.

No caso dos roteadores, eles estão interessados apenas nos campos de *hop-by-hop* e *routing*. Uma vez que o roteador tenha verificado esses campos, ele não precisa tratar o restante das opções e deve encaminhar o pacote imediatamente [MUR00].

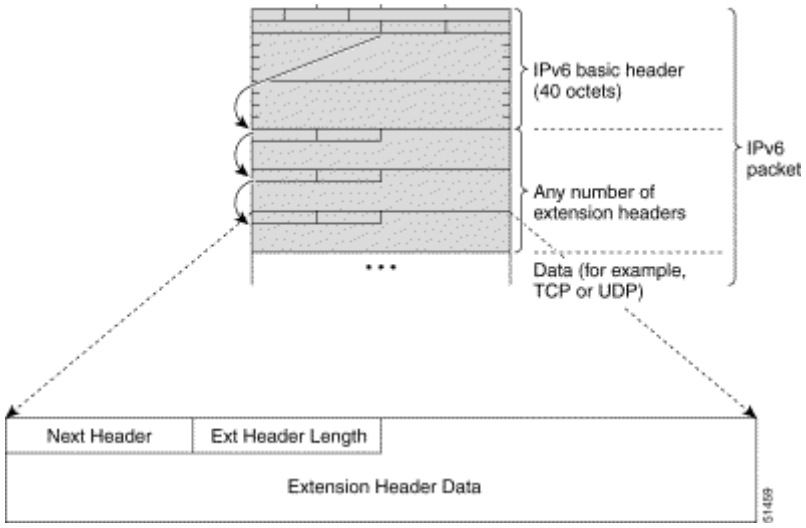


Figura 7 - Formato do cabeçalho de extensão.

3.4.2.1. Cabeçalho – *Hop byHop*

Esse cabeçalho contém opções que devem ser tratadas por todos os nós durante o percurso de um pacote IPv6 e, quando presente em um pacote, esse cabeçalho é utilizado para transportar informações opcionais, sendo o primeiro cabeçalho após o principal, conforme abaixo descrito. Quando presente em um pacote IPv6, é identificado pelo valor zero no campo próximo cabeçalho do cabeçalho básico do IPv6 e contém opções de extensão variável conhecido como TLV (*Type Lengtht Value*), a fim de manter o alinhamento de 8 bytes para os cabeçalhos subsequentes.

Uma opção muito interessante é o tamanho de conteúdo *Jumbogram*, usada para indicar um pacote com tamanho superior a 64 Kbytes.

Campo: *Next Header*.
Tamanho: 8 bits.
Descrição: Indica o próximo cabeçalho, utiliza os mesmos valores que o campo no protocolo IPv4.

Campo: *Header Extention Length*.
Tamanho: 8 bits.
Descrição: Identifica o tamanho do campo *options* logo em seguida, em unidades de 64 bits.

3.4.2.2. Cabeçalho - *Destination options*

Este cabeçalho possui o mesmo formato do cabeçalho *hop by hop*, sendo examinado apenas pelo nó destino. O cabeçalho de extensão possui duas variações:

a) *Destination Options Header-1*: Carrega informações do primeiro destino listado no campo endereço do IPv6.

b) *Destination Options Header-2*: Leva informações opcionais que serão analisadas somente no destino final.

3.4.2.3. Cabeçalho – *Routing*

O cabeçalho de *routing* possui a função de permitir que um caminho através da rede seja previamente definido, e é identificado pelo valor 43 no campo próximo cabeçalho do cabeçalho *hop-by-hop*. A função desse campo é semelhante à opção de liberar origem e registrar rota no IPv4.

O caminho que um pacote percorre através da rede é normalmente determinado pelos roteadores que compõem a rede. Em algumas situações, o nó origem deseja um maior controle da rota que o pacote irá transitar, fazendo com que tome decisões de uma rota mais lenta, porém mais segura que normalmente tomaria.

Também armazena uma lista de endereços dos roteadores por onde o pacote deverá obrigatoriamente passar até chegar a seu destino final. Ao passar pelo roteador, o campo *destination address* é modificado, recebendo o endereço do próximo campo do cabeçalho de roteamento.

Campo: *Next Header*.
Tamanho: 8 bits.
Descrição: Indica o tipo de cabeçalho imediatamente após o cabeçalho de roteamento.

Campo: *Header Extension Length.*
Tamanho: 8 bits.
Descrição: Tamanho do cabeçalho em palavras de 64 bits, excluindo os primeiros 64 bits do próprio cabeçalho.

Campo: *Routing Type*.
Tamanho: 8 bits.
Descrição: Tipo do cabeçalho de roteamento. Se ele não for compreensível por algum equipamento roteador no caminho, o datagrama será descartado. Geralmente é setado em zero, sendo a única opção disponível no momento.

Campo: *Segments Left*.
Tamanho: 8 bits.
Descrição: Indica o número de rotas, ou nós intermediários, que serão visitados para que o pacote chegue ao seu destino final; sendo o valor máximo permitido de 23.

Campo: *Reserved*.
Tamanho: Indefinido.
Descrição: Colocado como zero na transmissão e ignorado na recepção.

O segmento que reconhecer seu endereço no campo *destination address* do cabeçalho principal do IPv6 poderá analisar o cabeçalho de roteamento. Após isto, será analisado o campo *segments left*, caso seu valor for igual a zero, então não há mais segmentos para percorrer e o pacote chegou a seu destino final. Caso este segmento não seja o destino final, então continua a verificação do cabeçalho de roteamento analisando o campo *routing type*, caso este valor seja inválido, o pacote é rejeitado e enviada uma mensagem ICMP para o *host* de origem. Se este for o segmento final, este aceita o pacote. Caso o *segments left* for maior que zero, então este pacote deve continuar a procurar o seu destino, o roteador irá atualizar o *destination address* do cabeçalho principal e enviará o pacote, e assim por diante.

3.4.2.4. Cabeçalho – *Fragment*

No IPv6, esse cabeçalho é usado pela origem para a fragmentação e remontagem de pacotes e só pode ser feita pelo nó de origem ou de destino, não mais pelos nós intermediários, fazendo com que isso melhore o desempenho da rede. É identificado pelo valor 44 no campo próximo cabeçalho.

O nó de origem é quem determina o tamanho máximo de unidade de transmissão (MTU), dos *links* em que o pacote irá percorrer até chegar a seu destino. Para determinar este tamanho, o nó de origem envia um pacote com o maior MTU possível para o destino desejado, caso algum nó intermediário não suporte este pacote, envia uma mensagem ICMP do tipo pacote muito grande para a origem, juntamente com o valor do tamanho suportado pelo nó que gerou o impedimento do pacote. O nó de origem ajusta novamente o novo tamanho do MTU do pacote para o valor recebido e transmite, repetindo a operação até que o pacote seja aceito no destino.

O cabeçalho de Fragmentação carrega informações necessárias para que o destino possa remontar estes pacotes.

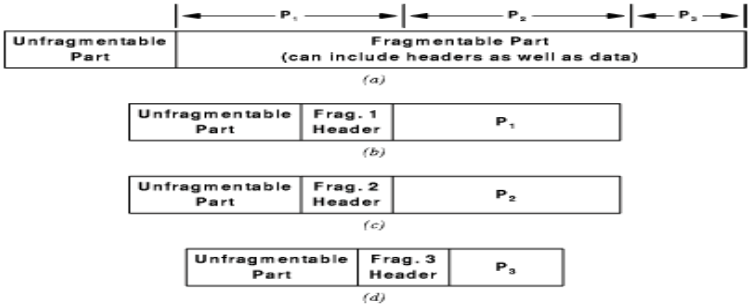


Figura 8 - Cabeçalho de Fragmentação.

A seguir a descrição de cada campo do cabeçalho IPv6 [MUR00]:

Campo: *Next Header*.
Tamanho: 8 bits.
Descrição: Indica o tipo do próximo cabeçalho.

Campo: *Reserved*.
Tamanho: Indefinido.
Descrição: Colocado como zero na transmissão e ignorado na recepção.

Campo: *Fragment OffSet*.
Tamanho: 13 bits.
Descrição: Indica a posição do fragmento no pacote.

Campo: *M (More Fragments).*
Tamanho: 1 bit.
Descrição: Caso esta opção esteja com o valor 1, indica que ainda restam fragmentos e 0 indica que é o último pacote do fragmento.

Campo: *Identification*.
Tamanho: 32 bits.
Descrição: Esse campo é usado para identificar os fragmentos pertencentes a um mesmo pacote.

3.4.2.5. Cabeçalho – *Authentication*.

O cabeçalho de autenticação (AH – *Autenthication Header*), descrito na RFC 2402, é usado para garantir a integridade de um pacote na rede e que não foi alterado durante o seu percurso. O cabeçalho de autenticação oferece um mecanismo que permite que o nó de destino saiba se o pacote enviado é mesmo de quem diz ser. Neste tipo de serviço, a privacidade da comunicação é garantida, mas sem confidencialidade, isto é, os dados não são criptografados.

Um dos objetivos da autenticação de pacotes é evitar ataque de máquina conhecido como IP *spoof*. O IP *spoof* consiste em utilizar o endereço de uma máquina em outra. Além de IP *spoofing*, um outro aspecto na segurança da Internet é a implantação de analisadores de tráfego (*sniffers),* que podem verificar o tráfego pela rede em dados não-criptografados.

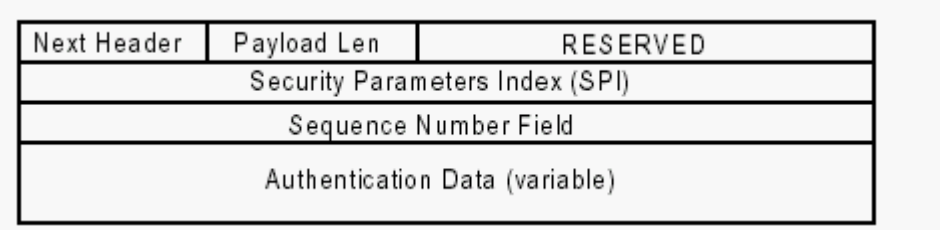


Figura 9 – Cabeçalho AH.

A seguir os campos do cabeçalho AH [CHO02]:

Campo: *Next Header*.
Tamanho: 8 bits.
Descrição: Identifica o tipo do próximo cabeçalho após o cabeçalho de autenticação.

Campo: *Length*.
Tamanho: 8 bits.
Descrição: Indica o tamanho do cabeçalho em palavras de 32 bits.O valor zero indica que é usado para fins de depuração. No IPv4 o seu valor é 1, e no IPv6, é 2.

Campo: *Security Parameter Index*.
Tamanho: 32 bits.
Descrição: Utilizado para identificar diferentes SA (*Security Association*), sendo uma conexão lógica unidirecional *simplex* entre dois sistemas IPSec, contendo os mesmos endereços de destino e protocolo de segurança (AH ou ESP descrito no próximo item). O valor desse campo tem significado apenas local, conforme definido pelo criador da SA, sendo que os valores de 1 a 255 são reservados pelo IANA,e o valor zero deve ser usado para propósitos específicos de implementação local.

Campo: *Sequence Number*.
Tamanho: 32 bits.
Descrição: Possui um contador que é incrementado a cada transmissão. O transmissor e o receptor possuem o valor zero quando uma associação segura é iniciada. Ele sempre

está presente no pacote e é enviado pela origem, embora o receptor possa ou não tratá-lo. Esse campo também é utilizado para evitar um *replay* de pacotes. Um *replay* consiste em capturar o pacote e enviar um outro montado com informações modificadas.

Campo: *Authentication Data*.
Tamanho: variável.
Descrição: Inclui o chamado ICV (*Integrity Check Value*), calculado com o algoritmo selecionado na iniciação do SA, para que o receptor verifique a integridade do pacote.

3.4.2.6. Cabeçalho - *Encapsulating Security Payload*

O cabeçalho *Encapsulating Security Payload* (ESP), descrito na RFC 2406, provê a checagem da integridade, autenticação e criptografia aos pacotes. Como visto anteriormente, o cabeçalho de autenticação do IPv6 não fornece privacidade ou confidencialidade dos dados no nível de rede.

Antes de ser iniciada uma comunicação, é necessário que o transmissor e o receptor defina uma ou mais chaves secretas, conhecidas somente por eles, criando uma associação. Os parâmetros desta associação são os algoritmos de autenticação e suas chaves de criptografia. Como algoritmo padrão do IPv6, foi definido o MD5 (*Message Digest 5*), podendo ser utilizados vários outros métodos.

O ESP pode ser utilizado de dois modos [FOR01].

3.4.2.6.1. Modo de transporte

O cabeçalho IP original não é alterado, sendo colocado um cabeçalho ESP logo após o cabeçalho original. Nesse método, a desvantagem é que não existe autenticação nem criptografia para o cabeçalho IP e a vantagem é que requer menos processamento comparado ao modo túnel. Assim como o AH, o modo transporte do ESP é utilizado principalmente por *hosts*.

3.4.2.6.2. Modo de Túnel

Utiliza o método de tunelamento, encapsulando o pacote inteiro dentro de um novo cabeçalho IP, proporcionando grande proteção ao pacote IP, haja vista que o pacote original se tornou a carga útil para o novo pacote ESP. Porém, o novo cabeçalho continua desprotegido. A sua utilização é recomendada sempre que qualquer dos pontos de uma SA (associação de segurança) entre sistemas for necessária, podendo ser roteadores ou *firewalls*.

O processamento de um cabeçalho ESP deverá aumentar o tempo de processamento nos roteadores das pontas dos túneis. Isto acontecerá devido ao tempo necessário para processar os complexos algoritmos de criptografia existentes, e o uso de ESP não deverá impactar nos roteadores intermediários que não participarão desta associação de segurança.

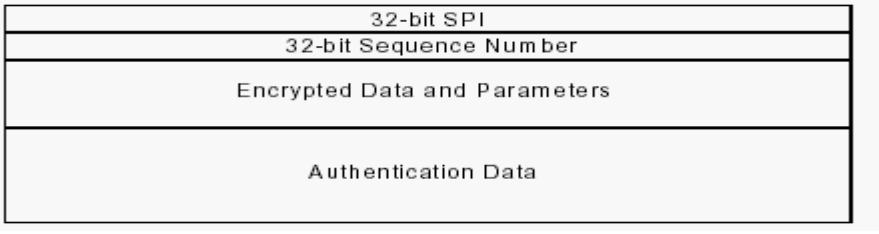


Figura 10 – Cabeçalho ESP.

A seguir, os campos do cabeçalho ESP:

Campo: *Security Parameters Index*.
Tamanho: 32 bits.
Descrição: Identifica juntamente com os endereços de destino uma SA (associação segura) para o pacote, conforme visto no item 3.4.2.5.

Campo: *Sequence Number*.
Tamanho: 32 bits.
Descrição: Possui um contador que é incrementado a cada transmissão. O transmissor e o receptor possuem o valor zero quando uma associação segura é iniciada.

Campo: *Payload Data*.
Tamanho: variável.
Descrição: Este campo consiste em um número múltiplo de 8 bytes, descritos pelo campo próximo campo, contendo a carga útil criptografada a ser transmitida, com o algoritmo escolhido durante o estabelecimento da SA.

Campo: *Padding*.
Tamanho: variável.
Descrição: é utilizado para incluir valores ao campo anterior caso o algoritmo necessite que este seja múltiplo de um número específico.

Campo: *Pad Length*.
Tamanho: variável.
Descrição: indica o número de bytes utilizados no campo anterior. O intervalo válido é de 0 a 255, em que o valor zero indica que nenhum byte de preenchimento foi incluído.

Campo: *Next Header*.
Tamanho: 8 bits.
Descrição: mostra o tipo de dado contido no campo *payload data*, por exemplo, se neste campo contém TCP, indica que a carga útil é o dado vindo da camada de transporte.

Campo: *Authentication Data*.
Tamanho: variável.
Descrição: Este campo é opcional, e análogo ao do cabeçalho visto no item 3.4.2.5. Usado apenas se o serviço de autenticação for selecionado para a associação de segurança.

Como o cabeçalho AH, o ESP é parte integrante do protocolo IPv6, sendo colocado após os cabeçalhos de extensão de *hop-by-hop*, roteamento e de fragmentação. Os cabeçalhos de opções de destino podem aparecer tanto antes quanto depois do cabeçalho AH.

3.4.3. Segurança

Os protocolos AH e ESP podem ser aplicados isoladamente ou em conjunto formando uma arquitetura denominada IPSec (*IP Security*), sendo que a especificação do protocolo IPv6 inclui essa segurança na sua camada de rede. Essa arquitetura é bastante flexível, de modo a evitar problemas relacionados com restrições de exportação de criptografia e não impede a utilização de outros mecanismos de segurança por parte das aplicações.

No protocolo IPv4 nativo não foi implementado nenhum tipo de segurança no nível de rede. Para corrigir este problema, o IPv6 fornece naturalmente capacidades de segurança, que são baseadas nos flexíveis cabeçalhos de extensão, como visto no início deste capítulo.

Tendo em vista que a utilização generalizada do IPv6 não é um processo imediato, o IPSec foi desenvolvido de modo a poder ser utilizada com o protocolo IPv4. Com a crescente utilização da Internet para fins financeiros, a preocupação com segurança é cada vez maior. Bancos disponibilizam serviços de *home banking*, empresas vendem seus produtos *online*, e usuários querem ter privacidade ao utilizar a Internet.

O protocolo IPv6 em conjunto com o IPSec propicia a implementação de VPN (*Virtual Private Network*), que cuida basicamente da criação de redes lógicas, utilizando infra-estruturas de redes físicas já existentes [STR00]. Uma vez que os dados acima da camada IP são criptografados e autenticados, praticamente todo o problema de privacidade de dados que uma VPN exige estará resolvido.

3.4.4. Autoconfiguração

A nova versão do protocolo possui mecanismos destinados a facilitar a gestão e configuração de ambientes de redes IP através da utilização de mecanismos de autoconfiguração. Desta forma, não é necessário configurar cada estação da rede manualmente como ocorre hoje, permitindo que o nó obtenha um endereço assim que for ligado.

Uma das principais características do IPv6 é facilitar a criação de novas redes. Atualmente com o IPv4, no modo manual é necessário que o administrador de rede configure um endereço a cada dispositivo novo ou configure um servidor de DHCPv4 (*Dynamic Host Configuration Protocol*) contendo um *pool* de endereços da rede na qual está conectado.

A diminuição do trabalho de administração de redes é um dos principais objetivos a ser alcançado no gerenciamento de redes de computadores atuais, envolvendo a definição dos parâmetros de *hosts*, roteadores e enlaces. Informações de configuração do IPv4, como número IP, DNS, *gateway e netmask* são fundamentais para estabelecer a conectividade.

O serviço de DHCPv4 facilita de certa forma esse processo, mas este provoca outros problemas operacionais, como por exemplo, no caso de uma empresa mudar de provedor, todos os seus endereços IPs devem ser alterados para outra rede, de forma a respeitar o sistema hierárquico de IPs atribuído pelo provedor.

Com o protocolo IPv6, esse tipo de problema não ocorre, permitindo que os dispositivos de rede procurem e configurem os seus próprios endereços, assim que forem ligados à rede.

Espera-se, por exemplo, que ao comprar um computador, o usuário possa simplesmente conectá-lo a uma rede e acessá-la, sem necessidade de lidar com a configuração de interfaces, protocolos, endereços etc.

Outro objetivo da autoconfiguração é permitir a mobilidade, ou seja, a utilização de um mesmo computador em vários locais e em redes distintas, sem a necessidade de configuração manual de endereços IP, permitindo o ajuste automático e transparente para o usuário a todas as situações.

3.4.4.1. Obtenção de Endereço Local

Uma das principais características do IPv6 é a facilidade de obtenção do seu endereço de rede. Um nó IPv6, ao iniciar suas interfaces, obtém um endereço de *link-local*, automaticamente para cada interface IPv6 composto do prefixo FE80::/64. Porém, para compor o endereço completo, necessita-se também do número da interface com valor único de 64 bits para compor um endereço completo de 128 bits.

O IEEE (*Institute of Eletrical and Eletronics Engineering*) criou o padrão EUI-64, descrito na RFC 2373, onde esse valor pode ser obtido através dos 48 bits do padrão de endereçamento IEEE 802, que forma o endereço MAC da interface de rede. Nos primeiros 24 bits existem os bits de controle “U/L" (*Universal/Local*) indicando se o endereço é administrado localmente (valor 0) ou globalmente (valor 1) e “I/G” (*Individual/Group*) indicando se o endereço é *unicast* (valor 0) ou *multicast* (valor 1).

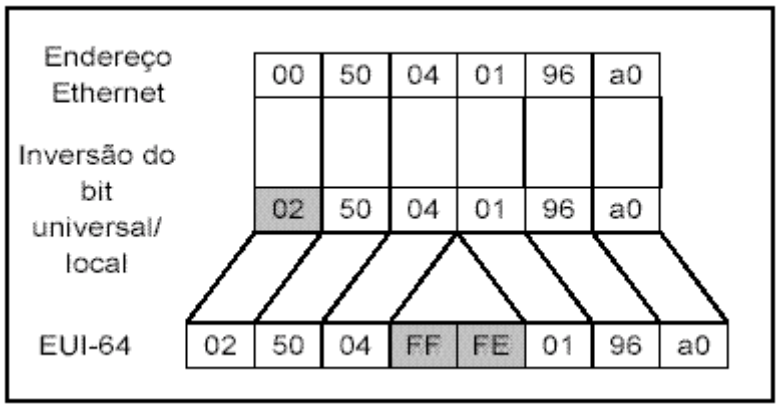


Figura 11 – Exemplo de conversão do endereço IEEE 802 para o EUI-64.

Conforme figura 11, duas modificações foram efetivadas para compor o endereço com o padrão EUI-64. A primeira modificação é colocar o bit “U/L” com o valor 1 e a segunda, acrescentar o valor FF:FE no meio do endereço [AND01]. No exemplo acima, o endereço IPv6 formado (FE80::250:04FF:FE01:96A0) é a junção do prefixo de *link local* FE80::/16 com o endereço MAC de 48 bits, composto pelo EUI-64.

A autoconfiguração de endereços permitirá que o próprio nó defina os parâmetros necessários para a conexão na Internet. Essa autoconfiguração é implementada utilizando o protocolo ND (Neighbor Discovery) descrito no item 3.4.12, que faz uma combinação do protocolo ARP e o ICMP. Quando a máquina for ligada, deve automaticamente associar um endereço IPv6 a sua interface de rede. São definidos mecanismos de autoconfiguração com manutenção de estado (dependentes de uma entidade que realiza a atribuição de endereços) e sem manutenção de estado [MUR00]. Esta funcionalidade é bastante útil para o estabelecimento de ligações móveis.

3.4.4.2. Configuração *Statefull*

A configuração é determinada pela rede, ou seja, existe um servidor de DHCP, com o qual o *host* se comunica e recebe um endereço IP completo. Caso não haja roteadores no link, essa configuração deve ser adotada. Neste método o tempo de vida associado ao endereço é determinado pelo servidor de endereços.

A seguir algumas vantagens de utilizar esse método:

- atribuição de endereços IPv6 ao nó;
- entrega de informação de configuração específica de cada nó da rede;
- garantia de maior controle de configuração de cada nó.

3.4.4.3. Configuração *Stateless*

A configuração é determinada pelo gestor da rede. O nó gera o seu próprio endereço combinando a informação local (endereço MAC da placa de rede) e o prefixo da rede publicada pelo roteador do segmento que está ligado, através do protocolo ND (a ser visto no item 3.4.12). O tempo de vida é definido a partir do tempo de vida do prefixo proveniente da resposta do roteador.

Na ausência do roteador, o nó cria apenas o endereço de *link local*, sendo suficiente para a comunicação no mesmo segmento de rede.

A seguir algumas vantagens de utilizar esse método:

- nenhuma informação manual é requerida;
- configuração mínima dos roteadores;
- inexistência de servidores adicionais.

3.4.5. Reendereçamento (*Renumbering*)

De modo a possibilitar o reendereçamento dos endereços IP numa rede, bastará que um novo prefixo com tempo de vida fixado seja anunciado pelo roteador a todos os *hosts* do seu *link*. Durante o período de reendereçamento, o prefixo antigo será removido das mensagens de propagação dos roteadores.

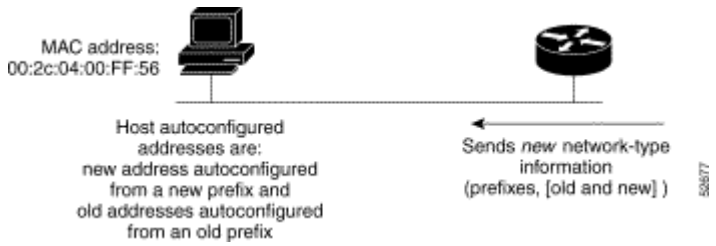


Figura 12 – Reendereçamento básico.

Existe também uma solicitação *multicast* chamada "*ND Router Solicitation multicast*" que é enviada para descobrir se um roteador é capaz de informar o valor do SLA (*Site Level Aggregation Identifier*, conforme item 3.4.14.1), para a sub-rede em questão e o seu prefixo. O roteador do *site* responderá a solicitação informando o prefixo da rede.

Como o endereçamento IPv6 pode ser baseado no prefixo atribuído pelo provedor, é essencial que um *site* seja facilmente reendereçado, na mudança um provedor para outro. Em conjunto com os protocolos de autoconfiguração, o protocolo RR (*Router Renumbering*), descrito na RFC 2894, é utilizado, fazendo com que o novo prefixo seja utilizado.

Os *hosts* aprendem seu novo prefixo de roteamento automaticamente quando são reiniciados, ou durante as atualizações periódicas usando o protocolo ND, sendo informados pelo roteador local que um novo prefixo deverá ser usado.

O reendereçamento é uma tarefa trabalhosa para as redes baseadas em IPv4, onde os *hosts* da rede são geralmente configurados manualmente. Com o protocolo IPv6, essa tarefa se tornará mais fácil.

3.4.6. IP Móvel

O mercado de transmissão de dados sem fio explodiu depois de um período inicial que se prolongou pelos últimos dez anos. As redes sem fio passaram de ferramentas de finalidade específica para alguns usuários móveis de elite para a iminência de ser amplamente adotados por usuários de nível de poder aquisitivo mais baixo.

A natureza do acesso à informação está sofrendo uma revolução silenciosa. Enquanto a Internet torna-se disponível aos consumidores em todo o mundo, por meio dos computadores domésticos, está surgindo um tipo semelhante de rede que elimina a necessidade de um computador ou de cabeamento para acessar à Internet.

Essa nova rede sem fio consiste em milhões de dispositivos pequenos e portáteis prontamente disponíveis sempre e onde quer que um usuário necessite de informações. Computadores de mão, telefones inteligentes e dispositivos similares estão se tornando cada vez mais disponíveis com opções de conectividade sem fio.

Há um grande número de redes que suportam mobilidade de *hosts*: WWLAN (*Wireless Wide Área Network*), WLAN (*Wireless Local Área Network*) e WPAN (*Wireless Personal Área Network*) envolvendo redes locais, celulares, satélites etc.

À medida que cada vez mais empresas empregam a Web para integrar os sistemas de informação de seus parceiros e clientes, o valor da Web como ferramenta de referência aumenta exponencialmente. Com a atual infra-estrutura das comunicações sem fio em rápido crescimento, está sendo cada vez mais fácil acessar as informações via Web a partir de qualquer fonte a qualquer hora.

O crescimento do acesso a Web sem fio pode ser sentido pelo grande número de companhias que investem nessa tecnologia emergente, esperando conseguir uma fatia das receitas desse mercado em crescimento. Essas empresas fornecem a infra-estrutura, o *hardware* e o *software* necessários para viabilizar o acesso a Web sem fio. Elas reconhecem o potencial comercial dos milhões de assinantes de serviços de comunicação de dados sem fio durante os próximos anos.

O telefone celular é um exemplo perfeito desse desenvolvimento comercial. A crescente demanda pública de telefones celulares durante os últimos 15 anos resultou em uma das indústrias mais bem-sucedidas deste século. Centenas de milhões de telefones sem fio foram vendidos até agora. Muitos desses aparelhos sem fio serão equipados para funcionar tanto com voz quanto com dados.

A maioria dos dispositivos de comunicação, tais como PDAs e celulares, que usam serviços de tempo real, precisarão estar ligados à Internet de modo mais efetivo. A presença do protocolo IPv6 em um estágio operacional avançado será fundamental, sendo que alguns especialistas acreditam que o futuro do comércio eletrônico está na mobilidade.

3.4.6.1. Aspectos do IP Móvel

A mobilidade IP, especificada na RFC 2002 (*IP Mobility Support*), tem como principal função manter os *hosts* conectados independente da sua localização física, ou para os *hosts* que necessitam transitar de uma rede para outra, de maneira que a comunicação e a conectividade IP permaneçam transparentes para os níveis de camada superior como TCP e para as aplicações.

Um aspecto relevante é a necessidade de protocolos auxiliares para suportar a mobilidade. O IPv6 móvel compartilha algumas características do atual IPv4 móvel, em que a questão da mobilidade na nova versão é totalmente integrada com o protocolo IPv6, provendo melhorias importantes e eliminando alguns problemas atuais, descritos na RFC 3024.

A utilização de um serviço em tempo real como VoIP e vídeo, dentro de um ambiente móvel, depende de aspectos como: minimização do impacto do redirecionamento do tráfico, dos atrasos envolvidos, otimização do roteamento, reendereçamento automático, bom suporte à autenticação e segurança e do desempenho final.

3.4.6.2. Entidades envolvidas com o IP Móvel

A Figura 13 [10] mostra as entidades envolvidas na configuração de uma rede com IP móvel:

a) *Mobile Agent* (agente móvel) – um nó ou *host* que faz parte de uma rede, e que em determinado momento pode mudar de rede, sem perder sua identidade com a rede original;

b) *Home Agent* (agente local) – um nó que representa a rede original do agente móvel. Este agente redireciona todos os datagramas endereçados ao agente móvel;

c) *Foreing Agent* (agente estrangeiro) – um nó ou *host* que representa a rede onde o agente móvel está temporariamente alocado. Ele é o intermediador entre o agente móvel e o agente de origem;

d) *Home Address* – é o seu endereço original e permanente que o identifica diante da rede de origem;

e) *Local-link Address* – é um endereço com o qual os *hosts* da rede de origem podem se comunicar com o agente móvel sem o intermédio de roteadores;

f) *Carrier-of Address* – é o endereço que é associado ao agente móvel, quando ele não se encontra em sua rede de origem;

g) *Túnel* – é um caminho pelo qual os pacotes endereçados ao *host* móvel devem trafegar.

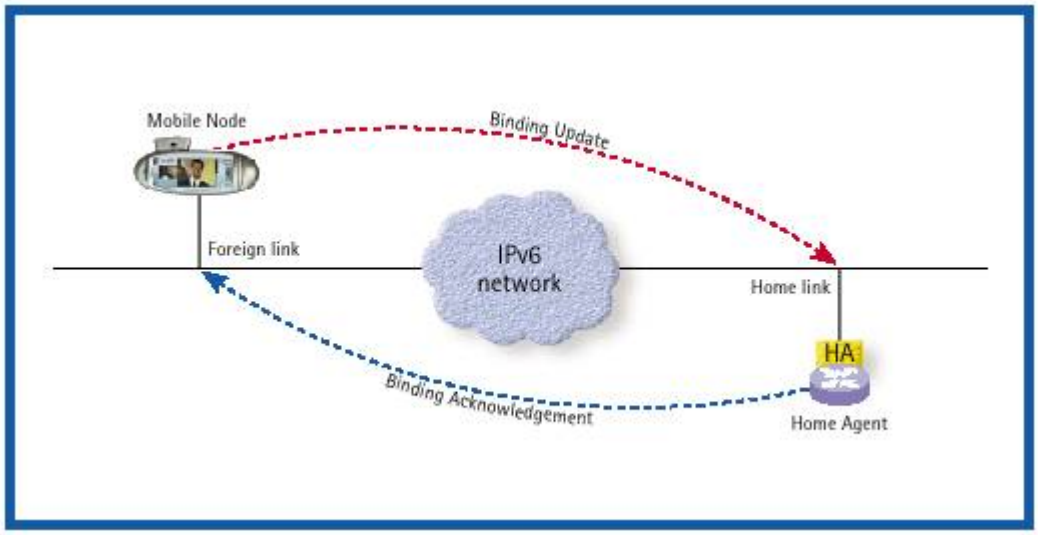


Figura 13 – Entidades do IPv6 móvel.

3.4.7. Suporte para tráfego com garantia de qualidade de serviço.

No protocolo IPv6, os campos *flow label* e *traffic class* oferecem métodos para a entrega diferencial de classes de serviço (CoS), criados especialmente para facilitar o desenvolvimento de protocolos para controle de tráfego em tempo real, como o RSVP (*Resource Reservation Protocol*), de forma a permitir a implementação, na Internet, de aplicações multimídia com a integração de serviços de dados, voz e vídeo em tempo real e com qualidade de serviço garantida.

Na especificação do IPv6, o termo fluxo pode ser definido como uma seqüência de pacotes de uma determinada origem para um determinado destino (*unicast* ou *multicast*), na qual a origem requer um tratamento especial aos equipamentos de rede, por informações contidas nos próprios pacotes do fluxo, por exemplo, no cabeçalho *hop-by-hop options*.

O campo classe de tráfego pode ser usado por nós de origem para identificar e distinguir entre classes ou prioridades dos pacotes IPv6.

3.4.8. Suporte para *Jumbograms*

Com essa opção habilitada é possível enviar pacotes com tamanho superior a 64Kb. O limite de um pacote *Jumbogram* é de 4Gb (tamanho registrado nos primeiros 32 bits do *payload*). O valor zero no campo *Payload Length* do cabeçalho indica um pacote *Jumbogram*. Esta propriedade é útil para as redes com grande largura de banda, reduz a utilização da CPU e aumenta a eficiência da rede.

Para habilitar pacotes “Jumbogram” no Linux, deve-se compilar o *kernel* com a opção "LARGE_LOMTU". Um aspecto importante a ressaltar é que os protocolos TCP/UDP e IPSec não possuem suporte para *Jumbogram* até o momento.

3.4.9. Domain Name System version 6 (DNSv6)

O serviço de DNS (*Domain Name System*) é de extrema utilidade para o protocolo IPv6. Com o desenvolvimento do IPv6, surge a necessidade de prover um serviço de nomes que suporte esse novo protocolo. O documento DNS *Extensions to*

Support IP version 6, descrito na RFC 2874, especifica um novo tipo de campo DNS de 128 bits denominado “AAAA”, que permite mapear nomes de domínios em endereços IPv6.

Estão em fase de desenvolvimento novos tipos de registros que facilitarão a manutenção desse serviço. Além disso, um novo domínio foi criado para a resolução de reverso, o “ip6.int”. Esse domínio está em fase de transição para um outro domínio de reverso, o “ip6.arpa”, seguindo as orientações da RFC 3152. A forma de atribuição e delegação de reverso permanece a mesma. Para efeitos de compatibilidade, o serviço de DNS deve suportar ambos.

Segundo a RFC 2874, foram introduzidos novos registros para a manutenção das zonas de DNS tipo “A6”, visando à substituição do tipo “AAAA”. Esses novos tipos de campos estão em desenvolvimento verificando-se a sua real eficiência e utilidade. Um novo formato para a representação de registros reversos foi também introduzido, tomando o lugar do *nibble format*, denominado *bitstring label*.

Essas novas funções já estão implementas, só que hoje existe uma grande discussão em torno do custo/benefício que essas propostas podem trazer. Até o momento, a versão mais estável do software BIND (*Berkeley Internet Name Domain*) se encontrava na 9.2.0. Versões mais recentes podem ser utilizadas.

O serviço de DNS adaptado para o IPv6 permaneceu o mesmo em suas características essenciais em relação ao IPv4. As modificações ocorreram no recurso *resource record* que passou a suportar endereços IPv6 e a criação de um novo domínio para suportar buscas de endereços IPv6.

3.4.10. Fragmentação/remontagem de pacotes

No IPv4, para enviar um pacote maior que o tamanho máximo permitido pelas diversas tecnologias utilizadas na rede, é necessário o ajuste do MTU do pacote durante todo o percurso, fazendo com que os roteadores quebrem o pacote em fragmentos menores e enviem os pacotes separados. O *host* destino deve remontá-los.

Numa rede *Ethernet* o tamanho mínimo de um frame é de 64 bytes e o máximo de 1518 bytes (18 de cabeçalho e 1500 de *payload*). Em redes como *Token Ring* ou FDDI os valores são maiores. Nesse caso, um pacote que percorre várias tecnologias de rede diferentes, o valor do MTU deve ser ajustado pelo menor valor.

A fragmentação é um dos itens responsáveis pela ineficiência por parte dos roteadores e estações destino, pois a perda de um fragmento faz com que todo o segmento da camada superior TCP seja retransmitido, comprometendo a largura de banda, alocação de recursos de memória e processamento.

No protocolo IPv6, a tarefa da fragmentação foi transferida para o nó de origem, liberando os roteadores desse trabalho. Com a implementação do protocolo *MTU Discovery,* conforme RFC 1191, o nó origem descobre de forma dinâmica o tamanho máximo do pacote em seu percurso até o nó destino, onde são previamente identificados os tamanhos máximos permitidos em cada *link* do caminho a percorrer. Dessa forma, o protocolo *MTU Discovery* tende a ser um método mais eficiente do que a fragmentação.

3.4.11. *Internet Control Message Protocol version 6* (ICMPv6)

O ICMPv6 (*Internet Control Message Protocol*), especificado na RFC 2463, não é compatível com o ICMP do IPv4, devido ao aumento de tamanho dos campos. É utilizado em conjunto com o protocolo ND, conforme item 3.4.12, tendo como principal função reportar erros encontrados no processamento dos pacotes, servindo como um protocolo de diagnósticos da camada de rede [NAU01].

O ICMPv6 pode ser utilizado por roteadores para descobrir os membros de um grupo *multicast* específico chamado MLD (*Multicast Listener Discovery*), fornecendo funções equivalente ao IGMP (*Internet Group Multicast Protocol*), cujas informações são fornecidas aos roteadores para qualquer protocolo de roteamento *multicast* que estiver sendo utilizado. Assim, os pacotes *multicast* são entregues a todos os nós que estiverem tratando e escutando pelo endereço *multicast* apropriado.

Mensagens ICMPv6 não podem ser enviadas em respostas a mensagens de *multicast*, pois podem ocasionar um congestionamento na rede. Outro aspecto é que mensagens de erro ICMP não podem ser enviadas em resposta de outras mensagens ICMP, pois poderiam ocorrer *loops* destas mensagens.

Cada mensagem ICMPv6 é precedida por um cabeçalho IPv6 e/ou cabeçalhos de extensões IPv6, identificado pelo campo próximo cabeçalho com o valor 58, sendo que todas as mensagens ICMPv6 têm o mesmo formato geral, composto por tipo, código, checksun e a variável do corpo.

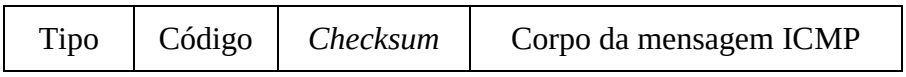


Figura 14 - Formato de mensagem ICMPv6 genérica.

Campo: Tipo.
Tamanho: 8 bits.
Descrição: O valor zero na posição mais significativa do byte indica mensagem de erro e o valor 1 indica mensagem informativa.

Campo: Código.
Tamanho: 8 bits.
Descrição: Varia de acordo com o tipo de mensagem.

Campo: *Checksum*.
Tamanho: 16 bits.
Descrição: Campo de checagem da integridade das mensagens do protocolo ICMPv6 e parte do cabeçalho do IPv6.

Campo: Corpo da mensagem.
Tamanho: Variável em múltiplos de 32 bits.
Descrição: Uso geral.

As mensagens IPv6 são agrupadas em duas classes [CHO02]:

a) Mensagens de Erro - apresentam erros de nós destino ou roteadores intermediários. As mensagens de erro possuem os valores de 0 a 127, sendo que os tipos de mensagens podem ser:

- *Destination Unreachable*: mensagem de destino inacessível, enviada por um nó origem ou um roteador, indicando que um pacote não pôde ser entregue ao destino por qualquer motivo, exceto em caso de congestionamento;

- *Packet Too Big*: mensagem de pacote muito grande, enviada quando o pacote não puder ser enviado devido ao MTU do *link* ser menor que o tamanho do pacote. Esse é um dos mecanismos de descoberta de MTU do percurso;

- *Time Exceeded*: mensagem enviada pelo roteador indicando limite de salto igual a zero. Pode indicar um *loop* de roteamento ou um valor de salto inicial muito pequeno;

- *Parameter problem*: mensagem enviada por um nó destino ou roteador indicando um erro no cabeçalho fixo ou em um cabeçalho de extensão.

b) Mensagens de Informação - tratam funções de diagnóstico gerais e específicos. As mensagens possuem os valores de 128 a 255, e seus tipos podem ser:

- *Echo Request*: mensagem enviada por um nó destino, visando a uma solicitação de eco. Utilizado para verificar se um nó está ativo na rede e identificar problemas de roteamento;

- *Echo Replay*: mensagem de resposta de uma solicitação de eco, contendo número de seqüência de cada solicitação por parte do nó que enviou a mensagem;

- Tipos ND, MLD: conjunto de mensagens e processos que determinam o relacionamento entre nós vizinhos de um determinado *link*.

3.4.12. *Protocol Neighbor Discovery* (ND)

Um problema apresentado pelo protocolo ARP é que ele trabalha com *broadcast* para realizar o mapeamento entre endereço físico e IP ajudando a criar o chamado *broadcast storm*.

A principal função do protocolo IP é mover dados de um nó para outro da rede. Para que isso ocorra, são necessárias outras funções como: indicar mensagens de erros, descobrir rotas, apresentar diagnósticos etc. O protocolo ND, descrito na RFC 2461, pode ser visto como uma combinação dos protocolos ARP e ICMP, realizando as tarefas de determinar os endereços da camada de enlace dos vizinhos interligados no mesmo segmento e limpar valores armazenados em cachê que se tornem inválidos.

Para que o protocolo ND possa ser iniciado, deve ser utilizado um endereço de *multicast* especial na camada MAC, composto pelo número 3333 e os últimos 32 bits do endereço IPv6 a serem ouvidos por todas as placas de rede do mesmo *link*. Caso corresponda a seu endereço *multicast*, o pacote será repassado para a camada superior [NAU01].

Este processo de descoberta utiliza ICMPv6 e endereços *Solicited Node Multicast* para determinar o endereço da camada de rede de um elemento vizinho nessa mesma rede e verificar a sua acessibilidade, conforme figura 15.

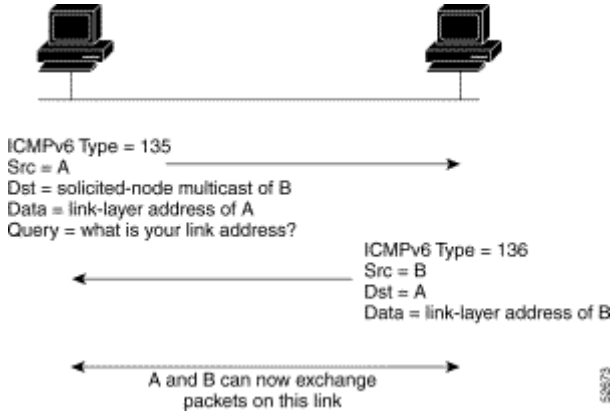


Figura 15 – Descoberta de vizinhança com o protocolo ND.

Outras funções importantes do protocolo ND relacionadas à interação entre nós conectados no mesmo *link* são: autoconfiguração de endereço local na interface conectada, descoberta de roteador vizinho para encaminhar pacotes, descoberta de *host* vizinho que possibilita um nó identificar outros *host*s em seus enlaces, resolução de endereços, redirecionamento de anúncio por onde um roteador garante que o nó estará habilitado a conectar-se a dispositivos fora de seu enlace local, detecção de endereços duplicados e detecção de inacessibilidade de vizinhos [MUR00].

A seguir, os tipos de protocolo que compõem o ND:

- *Router Discovery*: utilizado para localização e identificação de roteadores no seu *link local*;
- *Prefix Discovey*: utilizado para que os nós descubram os prefixos de rede para os destinos no mesmo *link local*;
- *Parameter Discovery*: usado para que os nós descubram parâmetros adicionais, como o MTU do *link* e o *default hop limit* para os pacotes de saída;
- *Address Autoconfiguration*: processo de configuração automática de um endereço IPv6 para uma determinada interface, na ausência de um servidor de DHCPv6;
- *Address Resolution*: processo de resolução de endereços IPv6 para um endereço de camada *link*;
- *Next-Hop Determination*: algoritmo de mapeamento que visa determinar o endereço IPv6 do vizinho ao qual deve ser enviado o tráfego, baseado no endereço destino ou no endereço de um roteador *default*;
- *Neighbor Unreachbility Detection*: maneira pela qual um nó determina que o vizinho não está mais acessível;
- *Duplicate Address Detection*: maneira pela qual o nó verifica a existência de um endereço duplicado no seu *link*;
- *Redirect*: maneira pela qual um nó informa o melhor endereço do primeiro salto (*hop*) para alcançar um destino específico.

O protocolo IPv6 possui quatro entradas de *cache*, através do protocolo ND, sendo que o IPv4 possui apenas uma chamada *cache ARP* [NAU01].

- *Destination Cache*: mantém informações sobre os nós destinos, na qual foi enviado trafego recente, incluindo os endereços dos nós destino e origem e associando um endereço IPv6 de um destino ao vizinho na direção em que os pacotes são enviados. As entradas são criadas pelo procedimento de determinação do próximo salto;

- *Neighbor Cache*: contém um conjunto de informações sobre os nós vizinhos, para os quais houve tráfego recente;

- *Prefix List Cache*: possui informações recebidas pelas mensagens de *Router Advertisements*, contendo uma relação dos prefixos locais e um temporizador de expiração individual que define um conjunto de endereços que estão no *link*. Os nós recebem e armazenam essas informações que são transmitidas de um roteador nesse *cache*, permitindo que um nó determine um destino remoto;

- *Router List Cache*: contém informações sobre os roteadores, para as quais podem ser enviados pacotes. As entradas da lista de roteadores apontam para entradas no *cache* vizinho. Para cada entrada, existe um valor de temporizador de expiração associado retirado do *Router Advertisements* usado para excluir entradas das quais o nó recebe anúncios.

O protocolo IPv6 necessita das entradas de cache relacionadas para auxiliar no roteamento de um pacote.

3.4.13. *Dynamic Host Configuration Protocol version 6* (DHCPv6)

Conforme visto anteriormente, o IPv6 implementa a autoconfiguração para estabelecer endereços em *hosts*, não havendo a necessidade de configuração manual. Quando se instala um nó numa determinada rede, automaticamente será atribuído pelo protocolo IPv6 um endereço completo. Esta característica de autoconfiguração, denominada *stateless autoconfiguration*, estará presente no IPv6 eliminando a necessidade de se configurar manualmente cada nó da rede.

Para obter maior controle sobre o esquema de endereçamento IP da organização, o administrador pode optar por outra forma de autoconfiguração, conhecida como *statefull autoconfiguration*, havendo a necessidade de um servidor de DHCPv6 instalado na rede.

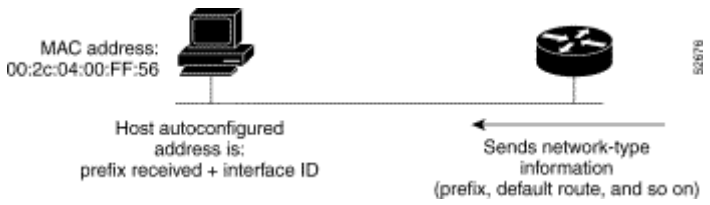


Figura 16 – Autoconfiguração com DHCPv6.

3.4.14. Endereçamento IPv6

Para evitar a atual sobrecarga das tabelas de roteamento (atualmente diminuída pela utilização do protocolo CIDR), o IPv6 introduz uma nova hierarquia de endereçamento, apresentada na figura 17.

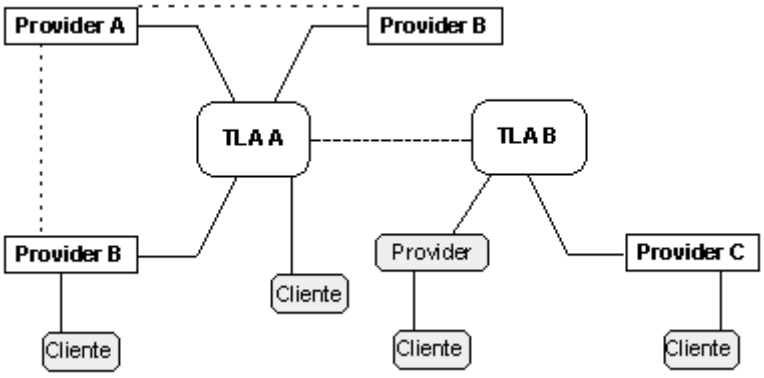


Figura 17 - Hierarquia de endereçamento IPv6.

3.4.14.1. Níveis de hierarquia

Conforme RFC 2374, apresentam-se os níveis de hierarquia presentes no IPv6.

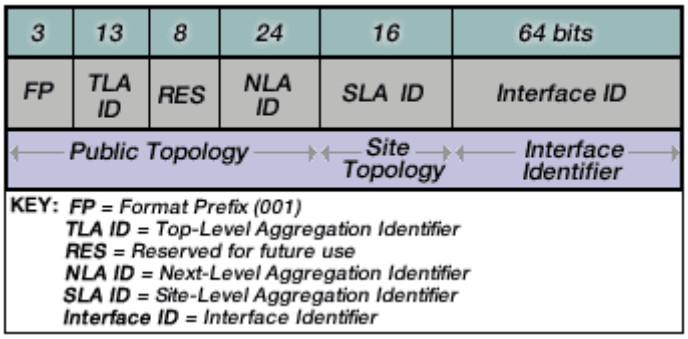


Figura 18 – Níveis de hierarquia de endereçamento.

a) *Public Topology*.
Conjunto de provedores que fornecem serviços públicos de acesso à Internet.

b) *Site Topology*.
Refere-se a um *site* local específico de uma organização que provê serviço público de acesso.

c) *Interface Identifier*.
Numero único, situado no segmento local da rede, composto de 64 bits, identificando a interface do enlace.

3.4.14.2 Formato do endereçamento IPv6.

a) FP (*Format Prefix*).
Valor atual binário é 001. Esse valor é utilizado para identificar endereços *unicast* globais agregáveis.

b) Identificador TLA (*Top-Level Aggregation Identifier*).
O valor desse campo é 0x1FFE e foi designado pela IANA para uso temporário pelo *6Bone* da IETF. Os roteadores situados nesse nível possuem entradas na tabela para cada TLA ativo. Esse campo pode suportar ate 8.192 entradas (2^13) para o identificador TLA.

c) Identificador NLA (*Next-Level Aggregation Identifier*).
Esse número será designado pelo administrador do NLA, em uma hierarquia de endereços suficiente para identificar redes corporativas e *sites* de usuários finais, de forma consistente com a topologia e arquitetura do *6Bone*.

n	24-n bits	16	64 bits
NLA1	Site ID	SLA ID	Interface ID

Tabela 8 – Divisão do campo NLA.

As organizações que recebem um identificador TLA possuem 24 bits para uso no NLA, permitindo que essas organizações possam prover serviços a outras organizações dependendo do esquema de endereçamento adotado. As organizações que tiverem um TLA podem suportar vários NLA para uso no Site ID.

n bits	(24-n) bits			16 bits	64 bits
NLA1	Site ID			SLA ID	Interface ID
	m bits	(24-n-m) bits		16 bits	64 bits
	NLA2	Site ID		SLA ID	Interface ID
		o	24-n-m-o	16 bits	64 bits
		NLA3	Site ID	SLA ID	Interface ID

Tabela 9 – Sub-divisões campo NLA.

d) Identificador SLA ID (*Site-Level Aggregation Identifier*).
Esse número deve ser utilizado pela organização para criar sua própria hierarquia de endereços e identificar suas sub-redes, podendo suportar até 65.355 sub-redes diferentes. É análogo ao conceito de sub-redes do IPv4.

N bits	(16-n) bits		64 bits
SLA1	Subrede		Interface ID
	M bits	(16-n-m) bits	64 bits
	SLA2	Subrede	Interface ID

Tabela 10 – Divisão do campo SLA.

Os endereços IPv6 apresentam muitas variantes, que podem ser distinguidos pelos primeiros bits do prefixo do endereço. Alguns exemplos comuns são:

Prefixo	Tipo do endereço
0000 0000	Reserved
001	Aggregatable Unicast Global
1111 1110 10	Site Local
1111 1110 11	Link Local
1111 1111	Multicast

Tabela 11 – Prefixos associados a determinados tipos de endereços IPv6.

Para cada tipo de endereço, existem ainda divisões quanto à visibilidade:

- *Link-local*, endereços únicos na ligação física do mesmo segmento de rede;
- *Site-local*, endereços únicos num *site*;
- *Link-global*, endereços únicos globais.

O endereço *link-local* (FE80::) deve ser único no segmento de rede ligado, sendo configurado automaticamente baseado em seu endereço MAC. É utilizado nas seguintes situações: autoconfiguração, descoberta de nós vizinhos através do protocolo ND (*Neighboor Discovery*) ou quando o roteador não está presente.

Os endereços *link-local* e *site-local* (FEC0::) só têm significado local. Os endereços *site-local* são similares aos endereços privativos do IPv4, e não podem ser propagados fora da organização. Pode ser utilizado como endereçamento de uma intranet e não possui acesso à Internet.

3.4.14.3. Endereçamento global

Antes de conectar um *host* IPv6 na rede, precisa-se entender a estrutura de endereçamento denominado de *aggregatable unicast global* e quais tipos de endereços são alocados para realizar a interconexão de rede. Notar que somente 1/8 do espaço de endereço total é reservado para este formato, deixando um range para o desenvolvimento futuro de esquemas de endereçamento global.

Um problema que os projetistas levaram em conta foi o crescimento das tabelas de roteamento. Dessa forma, sem algum tipo de estrutura de topologia, haveria necessidade de uma rota para todo o *host* destino, gerando problemas de escalabilidade.

O endereço *unicast global*, especificado na RFC 2374, tende a ser o formato predominante usado por *hosts* IPv6 conectados à Internet. Com a estrutura do endereçamento global, esse endereço foi tratado do mesmo modo que o mecanismo de CIDR, possuindo uma estrutura bem definida.

Prefixo de formato	TLA ID	Reservado	NLA ID	SLA ID	Interface ID
001	13 bits	8 bits	24 bits	16 bits	64 bits

Tabela 12 – Esquema de endereçamento global IPv6.

Foram definidas três atribuições do TLA, cada um para uma finalidade diferente:

Prefixo	Uso
3FFE::/16	Alocação experimental de teste para o *6Bone*
2001::/16	Alocação regional de produção do Internet Registry
2002::/16	Espaço de endereço de transição *6to4*

Tabela 13 – Prefixos de endereços TLA.

Na prática, cada uma dessas estruturas TLAs possuem sua estrutura de espaço de endereçamento diferente:

3.4.14.3.1. Endereço *6Bone*

A rede de testes *6Bone* (www.6bone.net) foi criada para o desenvolvimento e experiências envolvendo o IPv6. Cada organização interligada ao *backbone* é associada a um identificador chamado de *pseudo TLA ID*, que pode delegar sub-redes para outras organizações, de acordo com sua própria política de endereçamento, conforme abaixo.

Prefix and TLA ID	PTLA ID	pNLA ID	SLA ID	Interface ID
3FFE	<12 bits>	<20 bits>	<16 bits>	<64 bits>

Tabela 14 – Formato de endereço do *6Bone*.

3.4.14.3.2. Endereço de Produção

Atualmente, já estão sendo oferecidos blocos de endereços *unicast* IPv6 de produção por três entidades com a supervisão do RIR (*Regional Internet Registries)*: INTERNIC (*Internet Network Information Center*), RIPE-NCC (*Reseaux IP Européens Coordination Center*) e APNIC (*Asian and Pacific Network Information Center*).

Como o espaço de endereçamento alocado para o *6Bone* é limitado, foi organizado um bloco de endereços de produção para missão de propósitos específicos.

Os endereços de produção são organizados de maneira similar ao espaço de endereçamento do *6Bone*. Sob esse prefixo, são alocados os identificadores para *backbones*, utilizando para isso o campo de subTLA, similar ao conceito de pseudo TLA.

Prefix and TLA ID	**subTLA ID**	**Reserved**	**NLA ID**	**SLA ID**	**Interface ID**
2001	<13 bits>	<6 bits>	<13 bits>	<16 bits>	<64 bits>

Tabela 15 – Formato de endereço de produção.

3.4.14.3.3. Endereço de transição 6to4

Qualquer *host* que tenha um endereço IPv4 global pode se mapeado e atribuído a um endereço IPv6 usando o mecanismo de *6to4*, descrito no 5.4.2.

No esquema de *6to4*, quando se envia um pacote com o prefixo 2002::/16 , está-se encapsulando o endereço do IPv4 do *host* solicitante via endereço IPv6. Evidente que isso requer um software de encapsulamento apropriado e roteamento em todos os *sites*

6to4, para que os dispositivos possam realizar o encaminhamento entre *sites* que suportam ou não o esquema *6to4*, a ser visto com maiores detalhes no capitulo 5.

Prefix and TLA ID	IPv4 address	SLA ID	Interface ID
2002	<32 bits>	<16 bits>	<64 bits>

Tabela 16 – Formato de endereço de transição 6to4.

3.4.14.4. Notação de endereços

Os endereços IPv6 são endereços de 128 bits. Eles são escritos em oito grupos de quatro dígitos hexadecimais, separados por dois-pontos (:) entre os grupos, conforme exemplo abaixo:

1000:0000:0000:0000:0123:4567:89AB:CDEF

Como estes endereços podem possuir muitos zeros, adotam-se três tipos de otimizações para facilitar sua manipulação:

- zeros podem ser omitidos no início do grupo. Assim, o numero 0123 pode ser escrito como 123;
- um ou mais grupos com 4 bytes com valor 0 podem ser omitidos, substituindo-os por um par de dois pontos. Desta forma, o número do exemplo acima ficará assim:

  1000::123:4567:89AB:CDEF;

- por fim, os endereços IPv4 podem ser escritos por um par de dois pontos seguido da notação da versão 4, da seguinte forma:

  ::200.18.53.133

O endereço IPv6 é representado de modo similar à representação do IPv4 na notação CIDR da seguinte forma (Endereço-IPv6/Tamanho-do-prefixo), onde o Tamanho-do-prefixo é um número decimal que indica quantos bits de mais alta ordem representam o prefixo do endereço.

Por exemplo, o endereço FE80:1122:33::1234:5678:9ABC/64 indica que os primeiros 64 bits (FE80:1122:0033:0000) representam o prefixo do endereço.

3.4.14.5. Tipos de endereços IPv6

A capacidade total de endereçamento do novo protocolo é de dois elevado a 128 bits, sendo possível atribuir muitos endereços IP por m2 ao redor do planeta.

Os endereços IPv6 não identificam nós de rede, mas sim interface ou conjuntos de interfaces. Como cada interface pertence a um único nó, qualquer endereço unicast de uma interface pode ser usado para identificar o nó.

Ao contrário da Internet atual, que usa hierarquia de dois níveis (prefixo de rede + sufixo de *host*), o grande espaço de endereço do IPv6 permite uma hierarquia de vários níveis ou várias hierarquias.

Essa nova hierarquia está organizada de forma que um único endereço é atribuído a cada provedor de acesso à rede pela autoridade da Internet, o provedor, por

sua vez, atribui a cada assinante um único identificador, e o assinante atribui um único identificador a cada sub-rede e a cada nó da interface.

O IPv6 abandona a idéia de classes de endereços, mas baseia-se em prefixos como o IPv4, mudando a função desses prefixos. Eles não mais identificam as diferentes classes de endereços, mas diferentes usos de endereços.

Dois endereços são reservados para encapsulamento de protocolos que não sejam IP, como OSI NSPA e Novell IPX. O prefixo de endereço baseado no provedor permite que organizações provedoras de acesso à Internet ganhem uma grande parcela do espaço de endereçamento, e a dividam hierarquicamente, como o CIDR.

A tabela 17 apresenta a proposta de alocação de endereços do IPv6, descrito na RFC 2373.

Alocação de Espaço	Prefixo (binário)	Fração de endereços
Reservado (compatível com IPv4)	0000 0000	1/256
Reservado	0000 0001	1/256
Endereços NSAP	0000 001	1/128
Endereços IPX	0000 010	1/128
Reservado	0000 011	1/128
Reservado	0000 100	1/128
Reservado	0000 101	1/128
Reservado	0000 110	1/128
Reservado	0000 111	1/128
Reservado	0001	1/16
Reservado	001	1/8
Provedor – *Unicast* atribuído	010	1/8
Reservado	011	1/8
Reservado para Geográfico	100	1/8
Reservado	101	1/8
Reservado	110	1/8
Reservado	1110	1/16
Reservado	1111 0	1/32
Reservado	1111 10	1/64
Reservado	1111 110	1/128
Disponível para uso local	1111 1110	1/256
Usado para *multicast*	1111 1111	1/256

Tabela 17 – Alocação de endereços IPv6.

3.4.14.5.1. Endereço *unicast*

Há várias formas de atribuição de endereços *unicast* no IPv6. Os dois principais tipos de endereços *unicast* IPv6 são: baseados em provedor ou baseados geograficamente. Nos endereços baseados em provedor, cada provedor de *backbone* recebe um bloco de endereços e fica responsável por distribuir estes endereços a seus usuários. A diferença para os endereços baseados geograficamente é que, neste caso, o prefixo é determinado de acordo com a localização geográfica da rede, e não de acordo com o provedor.

Existem ainda os endereços *unicast* NSAP, endereços hierárquicos IPX, endereços de uso local, os endereços de *hosts* IPv4 e há ainda a possibilidade de definições futuras de endereços. Um endereço de uso local é um endereço *unicast* que tem apenas escopo de roteamento local.

3.4.14.5.2. Endereço *unicast* de *site-local e link-local*

Nos endereços de *site-local* há um identificador que deve ser único no domínio em que está sendo usado. A combinação de identificador de rede e de interface permite que uma rede privativa seja construída, sem qualquer outra alocação de endereços.

Endereços de uso local permitem ainda que organizações que não estão conectadas à Internet operem sem a necessidade de requisitar um prefixo do espaço de endereço global da Internet.

Esses endereços têm apenas significado local, e podem ser associados a uma rede tipo Intranet, possuindo o prefixo FEC0::/10.

Para os usuários que utilizam um *link* simples, quando não existe a presença de roteador envolvido, o prefixo delegado é FE80::/10, chamado de *link local*, conforme visto no item 3.4.14.2.

3.4.14.5.3. Endereço IPv4 compatível

O mecanismo de transição IPv6 inclui uma técnica para *hosts* e roteadores processarem dinamicamente pacotes IPv6 sobre a infra-estrutura de roteamento IPv4. Os nós IPv6 que utilizam esta técnica têm um endereço IPv6 *unicast* especial que leva um endereço IPv4 nos 32 bits de mais baixa ordem.

Esses endereços IPv6 são conhecidos como “IPv4 compatível”, utilizados para realizar o tunelamento de pacotes IPv6 sobre IPv4, possuindo o seguinte formato ::<endereço_IPv4>. Por exemplo, o endereço 1.2.3.4 (hexadecimal 01.02.03.04) torna-se ::0102:0304.

3.4.14.5.4. Endereço IPv4 mapeado

Existe um segundo tipo de endereços IPv6 que armazena um endereço IPv4 embutido, conhecido como “IPv4-mapeado”, possuindo o seguinte formato ::FFFF:<endereço_IPv4>. Este endereço é usado quando um nó IPv6 precisa se comunicar com um *host* IPv4. Isto requer um *host* ou roteador de pilha dupla para a devida tradução. Por exemplo, se um nó IPv6 deseja enviar dados a um *host* com endereço IPv4 1.2.3.4, ele usa o seguinte endereço de destino ::FFFF:0102:0304.

3.4.14.5.5. Endereço não especificado e de *loopback*

Existem dois endereços especiais que não podem ser utilizados para endereçamento. O endereço 0:0:0:0:0:0:0:0 (::), que indica a ausência de um endereço para a interface e o endereço 0:0:0:0:0:0:0:1 (::1) , que é o endereço de *loopback*, que faz com que a interface envie datagramas para si mesmo, similar ao endereço IPv4 127.0.0.1.

3.4.14.5.6. Endereço *anycast*

Um endereço IPv6 *anycast* é atribuído para mais de uma interface (tipicamente pertencentes a diferentes nós), com a propriedade de que um pacote enviado para um endereço *anycast* é roteado para a interface mais próxima que tem aquele endereço, de acordo com a medida de distância do protocolo de roteamento.

Endereços *anycast*, quando usados como parte de uma seqüência de rotas, permitem que os nós selecionem por quais, dos vários provedores de serviço, eles querem mandar seu tráfego. Isto pode ser implementado e configurado com endereços *anycast* para identificar o conjunto de roteadores pertencentes a um determinado provedor de serviço.

Estes endereços podem ser usados como endereços intermediários no cabeçalho de roteamento IPv6, para que um pacote seja entregue via um provedor especifico ou seqüência de provedores. Outra possibilidade de uso de endereços *anycast* é para identificar um conjunto de roteadores ligados a uma particular sub-rede, ou um conjunto de roteadores que provêem entrada num domínio de roteamento particular.

Os endereços *anycast* são alocados do espaço de endereços *unicast*, usando qualquer uma das formas de endereços *unicast* definidas. Portanto, endereços *anycast* são sintaticamente idênticos aos endereços *unicast*. Quando um endereço *unicast* é atribuído a mais de uma interface, ele torna-se um endereço *anycast*, os nós aos quais ele é atribuído devem ser explicitamente configurados, para saber que ele é um endereço *anycast*.

Cabe ressaltar que por ser um serviço novo, oferecido apenas para os nós que implementam IPv6, suas aplicações ainda não foram completamente previstas. Inicialmente, é recomendado que endereços *anycast* estejam limitados aos nós intermediários.

Um conjunto de *hosts* que oferecem o mesmo serviço (*cluster* de servidores Web ou bancos de dados) pode compartilhar o mesmo endereço *anycast.* Na requisição de um determinado serviço, o servidor mais próximo atende de acordo com as métricas usadas de roteamento. Os endereços *anycast* servem, desta forma, como um mecanismo simples de balanceamento de carga, uma vez que vários algoritmos de roteamento consideram o caminho mais curto aquele que tiver com menor carga.

Ao configurar vários servidores de nome com o mesmo endereço *anycast* uma forma de redundância é estabelecida, uma vez que, se um dos servidores falhar outro será contatado (o segundo mais próximo de acordo com o algoritmo de roteamento).

3.4.14.5.7. Endereço *multicast*

Um endereço IPv6 *multicast* é um identificador para um grupo de interfaces. Uma interface pode pertencer a qualquer número de grupos *multicast.* Quando se envia uma mensagem a um endereço *multicast*, ela será entregue a todos os membros do grupo por ele identificado, como mostrado a seguir.

A tabela abaixo representa alguns endereços *multicast* pré-definidos, conforme RFC 2375:

FF01:0:0:0:0:0:0:1	*All nodes (node-local scope)*
FF02:0:0:0:0:0:0:1	*All nodes (link-local scope)*
FF01:0:0:0:0:0:0:2	*All routers (node-local scope)*
FF02:0:0:0:0:0:0:2	*All routers (link-local scope)*
FF01:0:0:0:0:0:0:3	*All hosts (node-local scope)*
FF02:0:0:0:0:0:0:3	*All hosts (link-local scope)*
…	…
FF02:0:0:0:0:0:0:B	*Mobile-Agents*
FF05:0:0:0:0:0:0:2	*All Routers (site-local scope)*
FF05:0:0:0:0:0:1:3	*All-dhcp-servers (site-local scope)*

Tabela 19 – Endereços *multicast*.

No IPv6, não existe endereço *broadcast*, sendo substituído com a utilização dos diferentes tipos de endereços *multicast*.

3.4.14.6. Roteamento

Os protocolos de roteamento são utilizados para a disseminação de informações de rotas, podendo ser de dois tipos. O roteamento interior, que ocorre dentro de um sistema autônomo denominado IGP (*Interior Group Protocol*), caracteriza-se por possuir os elementos básicos de roteamento que são a rede ou o prefixo CDIR para protocolos mais recentes. O outro é o protocolo de roteamento exterior que ocorre entre sistemas autônomos denominado EGP (*Exterior Group Protocol*) onde o elemento de roteamento básico é uma coleção de prefixos CIDR identificados por um número de sistema autônomo [CHO02].

No IPv4 geralmente são utilizados no IGP os protocolos RIP (*Routing Information Protocol)*, OSPF (*Open Shortest path First*) e no EGP o protocolo BGP4 (*Border Gateway Protocol* versão 4) podendo ser utilizado também o roteamento estático. Os protocolos de roteamento para o IPv6 estão sendo adaptados. No caso dos IGP estão sendo utilizados os protocolos RIPng (RFC2080 e RFC2081) e OSPFv3 (RFC2740). Para o EGP é utilizado o BGP4+ (RFC2772), sendo o seu uso mandatário no núcleo da rede *6Bone*.

Para trabalhar com protocolos de roteamento de uso gratuito, utilizando o sistema operacional Unix/Linux, existe um pacote chamado GNU ZEBRA, disponível em (www.zebra.org), contendo os principais protocolos de roteamento baseados em TCP/IP como RIPng, OSPFv3 e BGP4+.

Dessa forma, para resolver o problema da expansão das tabelas de roteamento, onde a alternativa para a redução destas tabelas está na agregação de várias entradas na tabela em uma única entrada, o IPv6 propõe a utilização de endereços de provedores, por ter uma boa relação com as topologias das redes.

As redes são identificadas por prefixos de tamanho variável, por exemplo, todas as redes do Brasil têm o mesmo prefixo, ou seja, possuem os primeiros bits em comum.

Mas somente esta divisão não se torna suficiente, pois existem vários provedores de acesso no mesmo país.

Todos os clientes conectados a seus provedores serão roteados através da rede deste provedor. Fora desta rede, é suficiente manter uma entrada para cada provedor na tabela de rotas, ocasionando com isto a redução considerável das tabelas.

O IPv6 também inclui extensões de roteamento simples, mas que suportam novas funcionalidades.

a) seleção de provedor (baseado em políticas, performance, custo, etc.);
b) computação móvel (roteamento para a localização corrente);
c) reendereçamento automático (rotear para novos endereços).

Para adicionar funcionalidade, uma opção de roteamento é usada pela origem IPv6 para listar um ou mais nós intermediários para serem acessados no caminho até o destino do pacote.

O IPv6 permitirá que os projetistas do *backbone* da Internet criem uma hierarquia aberta e muito flexível de roteamento global. No nível do *backbone* Internet, onde as redes da maioria das organizações e ISPs se agregam, é necessário manter um sistema de hierarquia de endereçamento que se assemelhe com a hierarquia do sistema telefônico, conforme mencionado a seguir.

Os endereços de 128 bits IPv6 permitirão um roteamento similar ao que ocorre com as chamadas telefônicas. O prefixo atribuído aos roteadores do *backbone* envolverá apenas a identificação do TLA (*Top Level Agregator*). Cada TLA deverá saber encaminhar pacotes para os seus descendentes diretos de acordo com a sua árvore hierárquica de endereçamento.

O IPv4 usa uma hierarquia de endereçamento pouco flexível e com poucos níveis de profundidade para mover o tráfego entre redes interconectadas ao *backbone* Internet. Sem uma hierarquia de endereços, os roteadores do *backbone* são forçados a armazenar muitas entradas na sua tabela de roteamento com informações relativas a cada uma das redes, para que estas possam ser alcançadas. Dado o número enorme de redes já conectadas e o crescimento exponencial desse número, o armazenamento de informações para cada uma destas redes em uma mesma tabela de rotas seria totalmente impraticável.

3.4.14.7. Comparação entre os protocolos IPv4 e IPv6

A tabela a seguir mostra as principais diferenças significativas entre os protocolos IPv4 e IPv6, contendo informações de caráter global, endereçamento e de formato de cabeçalho [HOL02].

IPv4	**IPv6**
Informações gerais	
Os endereços de origem e de destino possuem tamanho de 32 bits (4 bytes)	Os endereços de origem e de destino possuem tamanho de 128 bits (16 bytes)
Suporte a IPsec é opcional	Suporte a IPsec é nativo
Não existe identificação de fluxo de pacote para QoS presente no cabeçalho do IPv4	Possui a identificação de fluxo de pacote para QoS, incluso no cabeçalho do IPv6 através do campo *Flow Label*, podendo ser tratado pelos roteadores
A fragmentação pode ser realizada tanto por roteador quanto pelo *host* de origem	A fragmentação não pode ser realizada por roteador, somente pelo *host* de origem
Realizado *checksum* de cabeçalho	Não é realizado *checksum* de cabeçalho
O cabeçalho inclui campo de opções	Todos os campos de opções foram movidos para os cabeçalhos de extensão do IPv6
Utiliza o *ARP Request* através de *broadcast* para resolver endereços MAC da camada de enlace e manter a associação entre endereço IPv4 e MAC	*ARP Request* foi substituído por mensagem de *Multicast Neighbor Solicitation*
ICMP *Router Discovery* é utilizado para determinar o endereço IPv4 a ser utilizado como *default gateway* e se é opcional	ICMP *Router Discovery* foi substituído pelo ICMPv6 *Router Solicitation* e o *Router Advertisement* sendo mandatários
Endereços de *broadcast* são utilizados para enviar mensagens para todos os *hosts* pertencentes a mesma rede	Não existem endereços de *broadcast* no IPv6. São utilizados endereços de *multicast* para enviar mensagem a todos os nós pertencentes ao *link-local*
A configuração pode ser manual ou via DHCP	A configuração é *plug and play*, mas pode ser manual ou via DHCPv6
Suporta datagrama até 64Kbytes	Suporta pacotes até 4 Gbytes (*Jumbogram*)
Espaço de endereçamento	
Endereços divididos em classes	Não é aplicável no IPv6
Endereços de *multicast* (224.0.0.0/4)	Endereços *multicast* IPv6 (FF00::/8)
Endereços *broadcast*	Não é aplicável no IPv6
Endereço não especificado (0.0.0.0)	Endereço não especificado (::)
Endereço de *loopback* (127.0.0.1)	Endereço de *loopback* (::1)
Endereço IP público válido na Internet	Endereço *unicast aggregatable global*
Endereços IP privados (Ex: 10.0.0.0/8)	Endereço *site-local* (FEC0::/48)
Não aplicável a IPv4	Endereço autoconfigurável *link-local* (FE80::/64)
A representação dos endereços é feita em decimal separado por pontos normais	A representação é feita em hexadecimal separado por dois pontos (:). Os endereços IPV4 compatíveis são expressos em decimal separados por ponto normal

continua

continuação

A representação da máscara de rede é feita em notação decimal ou através do tamanho de prefixo da rede (notação CDIR)	A notação do prefixo da rede é feita somente pelo tamanho do prefixo (notação CDIR)
A resolução de nomes DNS: endereços IPv4 é feita através de *resource record* (A)	Endereços IPv6 a resolução é feita através de *resource record* (AAAA ou A6)
Resolução reversa DNS utiliza o domínio IN-ADDR.ARPA	Utiliza o domínio IP6.INT
Informações de campos dos cabeçalhos	
Versão (atual possui o valor 4)	Mesmo campo com valor 6
Internet Header Length	Removido no IPv6, já que o cabeçalho básico do IPv6 é fixo com o tamanho de 40 bytes. Os cabeçalhos de extensão podem ser fixos ou possuírem tamanho variável, neste caso, indicando o seu próprio tamanho
Type of Service	Substituído pelo campo *Traffic Class*
Total Length	Substituído pelo campo *Payload Length* indicando apenas o tamanho do payload
Identification, *Fragmentation Flags e* *Fragment Offset*	Removidos no IPv6. As informações de fragmentação não são inclusas no cabeçalho básico do IPv6, mas, sim, no cabeçalho de extensão especifico chamado *Fragment*
Time to Live	Substituído pelo campo *Hop Limit*
Protocol	Substituído pelo campo *Next Header*
Header Checksum	Removido no IPv6. Os erros de nível de bit são realizados pela camada de *link layer*
Source Address	O campo permaneceu o mesmo, somente com endereços de 128 bits
Destination Address	O campo permaneceu o mesmo, somente com endereços de 128 bits
Options	Removido no IPv6. O campo IPv4 options foi substituído por cabeçalho de *extension*

Tabela 20 – Resumo comparativo entre os protocolos IPv4 e IPv6.

3.4.14.8. Novas aplicações e tecnologias para o IPv6

Conforme visto ao longo do capítulo, as vantagens do IPv6 em relação ao IPv4 são basicamente o aumento do espaço de endereçamento, a facilidade de configuração (*plug and play*), redução de custos de administração da rede, segurança nativa e a questão da melhoria na mobilidade IP, em relação ao IPv4.

Os problemas a serem resolvidos são eminentes; o IPv6 deverá acrescentar capacidades e maior flexibilidade, robustez e escalabilidade, podendo suportar de forma eficaz aplicações de tempo real.

A convergência entre a TV digital interativa, equipamentos móveis e o PC, acessando a Internet é somente uma questão de tempo. Para essas aplicações, é necessário maior largura de banda, exigindo maior tráfego e, para isso, é necessário também que os roteadores tratem de maneira mais eficaz os pacotes que transitam pela Internet, uma característica fundamental, disponível no novo protocolo IPv6,cujo cabeçalho básico e cabeçalhos de extensão estão descrito nos itens 3.4.1 e 3.4.2.

Para os milhões de dispositivos móveis que atualmente não possuem acesso à Internet, o novo protocolo IPv6 será de extrema importância, pois cada um desses dispositivos deverá possuir um endereço IP global para acesso à rede mundial. Com a Internet móvel, espera-se que mais de um bilhão de celulares estejam usando endereços IP em 2005, segundo dados do IDC.

Alguns organismos de telefonia, como o 3GPP (*Third Generation Partnership Project*), já adotaram o IPv6 como base para os serviços IP. Em recente artigo, a British Telecom mostrou que, em aproximadamente 15 anos o telefone celular deverá ser parte integrante da vida de uma pessoa, acordando-a durante o café da manhã, com uma música baixada diretamente de um servidor MP3, lendo seus *e-mails*, fazendo transações financeiras no percurso até a garagem, mostrando-lhe o melhor caminho para enfrentar problemas de trânsito naquele dia e conectando-o com outras pessoas em videoconferências. Ele não será apenas mais um simples celular, mas um equipamento multifuncional conectado ao mundo IP [TAU02].

O outro exemplo prático dessa aplicação seria que, numa solução convencional de Internet móvel, o vendedor precisaria se conectar antes de começar a tirar o pedido e teria de baixar da rede cada tela de informação que fosse preencher. Com os celulares que executam programas, o vendedor poderia preencher todo o pedido e conectar-se somente no momento da transmissão, o que reduziria o tráfego gerado e custos com a transação. Esse tipo de aplicação pode ser comparado a dispositivos de mão com sistemas operacionais, como o Windows CE da Microsoft.

A Microsoft está trabalhando também em um projeto chamado Stinger, que é uma plataforma para o telefone móvel inteligente, combinando facilidades de celulares e PDAs, mantendo o usuário permanentemente conectado por voz ou dados.

Os protocolos WAP (*Wireless Access Protocol*) e WTP (*Wireless Transaction Protocol*) e a sua linguagem básica WML (*Wireless Markup Protocol*) foram desenvolvidos exclusivamente para a Internet móvel, pois as tecnologias existentes da Web como HTML se mostraram inadequadas para esse ambiente. Outra tendência é o uso de dispositivos móveis que permitam rodar programas como a tecnologia BREW (*Binary Runtime Enviroment for Wireless*), acrescentando funcionalidades e serviços que vão além da voz. Dessa forma, os avanços dessas aplicações certamente irão incentivar, e muito, o crescimento do mundo sem fio.

Em recente artigo publicado, Ethevaldo Siqueira, secretário executivo do Ministério das Comunicações, disse que “a quarta geração de celulares (4G) deverá unificar as diferentes redes sem fio, incluindo as redes locais (LANs), *wireless* nas diferentes tecnologias existentes (IEEE 802.11, HiperLAN/2, HomeRF e *Bluetooth*). Sob a tecnologia de 4G, serão integrados não apenas as redes públicas fixas e celulares,

mas especialmente uma ampla rede de equipamentos móveis que, por seu intermédio, farão o *roaming*, nas diversas áreas geográficas e de concessionárias de operadoras. Em breve a empresa DOCOMO, do Japão, estará realizando testes com esse aparelho".

3.4.14.9. Negócios na Internet para o IPv6

Pesquisas dos principais organismos, como *IDC, Garther Group e Yankee Group*, apontam que os responsáveis pelas áreas de TI das grandes corporações esperam da Internet melhorias como: maior confiabilidade, melhor escalabilidade e capacidades de qualidade de serviço nas aplicações.

Para atender aos requisitos acima mencionados, não basta apenas investir em novos protocolos, mas também nas aplicações, que são o motor para a geração de negócios na Internet. Um exemplo desse processo é o caso das empresas de telecomunicações que investiram muito na parte de infra-estrutura, acarretando problema de capacidade de ociosidade dos seus *links* de fibra óptica, deixando para segundo plano as aplicações para esse tipo de negócio.

Segundo o professor Jerry Hausman do MIT, as empresas de telecomunicações necessitam de novas tecnologias e aplicações que demandem por fibra ótica recuperando os altos investimentos feitos até agora. Foi o que ocorreu com os computadores nos anos 80: com o aparecimento dos programas de planilha eletrônica, as empresas começaram a comprar os chamados PCs.

Capítulo 4 – NETWORK ADDRESS TRANSLATION (NAT)

4.1. Introdução

Na última década, depois do desenvolvimento no meio acadêmico, presenciou-se o crescimento da Internet principalmente em empresas chamadas de "pontocom", implementando sistemas de *e-Bussiness*, utilizando aplicações Web. Um elemento chave desse processo foi a acessibilidade dos computadores através das comunicações realizadas via Internet, envolvendo o protocolo IPv4, conforme visto no capítulo 2.

Para atender à enorme demanda por endereços IPs conectados à rede todos os dias, várias tecnologias e protocolos foram desenvolvidos para estender a vida útil do IPv4, promovendo melhor aproveitamento do estoque residual. Dentre esses desenvolvimentos, encontra-se o NAT (*Network Address Translation*).

Como qualquer solução paliativa, o NAT também introduziu problemas para as tecnologias e aplicações emergentes passíveis de utilização no ambiente corporativo como: aplicações P2P (*Peer-to-Peer*), videoconferência, *real-time data streaming*, VoIP (Voz sobre IP), VPN (*Virtual Private Network*), serviços de SAN (*Storage Área Network*), as quais requerem uma complexidade maior na arquitetura do que as aplicações tradicionais.

O desenvolvimento dessas novas aplicações e as restrições impostas pelo NAT, como se verá adiante, faz com que o IPv6 se torne uma das melhores alternativas para a otimização do uso do protocolo IPv4 e para contornar a escassez imposta pela demanda de números IPs. Ter-se-á que superar as limitações do IPv4 por algum tempo ainda e conviver com soluções de curto prazo, pois o estoque de IPs está praticamente esgotado.

Há muitas maneiras de economizar endereços IPs em ambiente privativo, consumindo um único IP público ou global. Além do NAT, que será abordado nesse capítulo, pode-se utilizar um servidor *proxy*, que faz o papel de interface de acesso entre a rede interna e a Internet, ambos visíveis para a Internet, através de um único IP global na interface do servidor e contribuindo com o nível de segurança das máquinas internas, escondidas para a Internet.

4.2. Definição de NAT

O NAT converte endereços IPs privados da rede interna em endereços IPs públicos globalmente únicos para o uso na Internet. O NAT atua basicamente nas camadas de rede e transporte, alterando os endereços IPs e portas TCP/UDP durante a tradução. As modificações nos pacotes devem ser suficientes para que o serviço NAT individualize o pacote de cada cliente e, então, retornem qualquer tráfego correspondente ao solicitante [BIL01].

O NAT pode atuar também na camada de aplicação, e qualquer tradução além da citada anteriormente requer um esforço adicional dos componentes de *software*, conforme item 4.5.4.

A principal utilização do NAT é para redes que possuem intervalos de endereços privativos e queiram se comunicar com *hosts* da Internet. Isto também pode ser obtido ao implementar uma solução com *firewall*, utilizando um servidor *proxy* ou *socks*, e não ficam expostos a Internet. No entanto, caso esses serviços não atendam às necessidades específicas do cliente, o NAT pode ser usado para gerenciar o tráfego entre a rede interna e a externa, e ser utilizado como um elemento de segurança ocultando os endereços de *hosts* da rede interna.

4.3. Endereçamento privativo.

Atualmente a convergência em torno do protocolo IP é inevitável, sendo que outros protocolos de camada de rede, como o IPX da Novell, NetBiui e NBT (NetBios over TCP/IP) da Microsoft, estão sendo descontinuados por seus fabricantes. Com o surgimento da técnica de NAT, muitas organizações, inclusive o IPT, que possuíam sérias limitações de endereços de rede principalmente com endereços classe "C" oficiais, montaram a sua infra-estrutura de rede da Intranet, composta de endereços privativos de rede classe "A", conforme descrito abaixo.

Para as redes privadas, o IANA (*Internet Assigned Numbers Authority*) reservou três espaços de endereçamento IP, conforme consta na tabela 21. As recomendações constantes na RFC 1918 visam conservar o espaço de endereços IP global, orientando que este seja utilizado quando não houver necessidade que o endereço IP seja único.

Endereço inicial	Endereço final	Máscara de rede
10.0.0.0	10.255.255.255	Prefixo 10/8
172.16.0.0	172.31.255.255	Prefixo 172.16/12
192.168.0.0	192.168.255.255	Prefixo 192.168/16

Tabela 21 – Classes IP para redes privativas.

A função do endereçamento privativo é permitir a conectividade entre todos os *hosts* que fazem parte da rede interna ou Intranet. Um ponto fundamental é que esses endereços, quando devidamente configurados, não podem ser roteáveis, ou seja, não podem ser repassados pelos roteadores da Internet, possuindo validade apenas no ambiente interno da organização a que está associado, especificado na RFC 1917.

Sempre que um *host* da rede interna com endereços privativos tiver a necessidade de acessar qualquer *host* da Internet, o NAT entra em ação, fazendo a devida conversão dos endereços no datagrama IP. Essa tarefa pode ser realizada por um roteador central ou numa máquina dedicada nos seguintes sistemas operacionais: Linux, Windows2000, Solaris etc.

4.4. Planejamento

Para a devida implantação do NAT, os gerentes de TI devem montar um plano contendo todo o planejamento da sua nova estrutura, verificando com detalhes as conseqüências de tal implementação, principalmente porque é um erro muito comum pensar em NAT apenas para resolver o problema relativo ao esgotamento de endereços IPv4.

Deve-se levar em consideração questões como aumento na carga administrativa de rede com a resolução de nomes de duas redes independentes (internet com IP públicos e Intranet com IPs privativos), posicionamento do NAT em conjunto com a DMZ (*Demilitarized Zone*) e o seu *firewall*, novos serviços e aplicações de *e-Bussiness* via Web, acesso remoto à rede Intranet via linha discada, conexão de diferentes redes privativas através da Internet denominadas de Extranets, redundância com alta disponibilidade de *links* ligados a provedores externos e a questão de novas tecnologias como VPN, VoIP, SAN e mobilidade de *hosts* [BIL01].

Outro fator importante é que muitas vezes, dependendo da política de segurança implantada pela corporação, não é possível colocar todos os servidores e serviços

existentes na área denominada de DMZ, protegida pelo *firewall*, na qual esses servidores devem possuir acesso externo da Internet.

Pode-se recorrer a servidores virtuais, *hosts* que possuem endereço privativo, porém visíveis para a Internet: um IP público representa o servidor virtual e várias máquinas com IPs privativos associados aos servidores reais, utilizando o NAT para a traduzir o endereço de destino dentro da organização, e realizando-se o balanceamento de servidores para agregar alta disponibilidade em serviços críticos, caso algum desses servidores fique fora do ar.

Cabe ressaltar que existem diversas implementações de NAT atualmente, e há diversas técnicas de implementação disponíveis dependendo da necessidade de cada organização, inclusive com soluções proprietárias de vários fornecedores.

4.5. Técnicas de NAT

Quando se fala de NAT, a tradução dos endereços pode ser feita essencialmente de duas maneiras: estática e dinâmica [MAC00] [5].

A seguir, serão utilizados com freqüência os termos “m” e “n” significando:

- m: a quantidade de endereços IP privados que precisam ser traduzidos.
- n: a quantidade de endereços IP públicos que estão disponíveis para serem utilizados nas traduções.

4.5.1. NAT – Estático

O NAT estático utiliza o esquema de tradução (m:n onde m,n>=1 e m=n), também conhecido como encaminhamento de pacotes, onde um ou mais endereços privados da rede interna são sempre traduzidos (mapeados) para os mesmos endereços públicos na rede externa, conforme figura 19.

Com esse método, não é necessário que a informação sobre a manutenção do estado das conexões seja mantida, permanecendo na tabela até que sejam apagados ou esgote seu tempo limite via *time out*. Tanto para o acesso *outbound* (direção da rede interna para a pública) quanto ao acesso *inbound* (direção da rede pública para a rede interna), o NAT faz a conversão fixa de endereços que nunca muda e não há economia de endereços IP, sendo a tradução realizada na base de um para um (1:1).

Os pacotes originários da rede pública que se destinam a *hosts* constantes na tabela de tradução de endereços são aceitos, mas os demais são descartados. Ainda assim, podem ser utilizados recursos de *firewall* para limitar o acesso externo para apenas alguns tipos de serviços, por exemplo, permitir tráfego *inbound* pela porta TCP 80 para o servidor Web.

A principal vantagem desse método é permitir um controle sobre os *hosts* que podem ou não usar os serviços do NAT. A desvantagem é o aumento do trabalho dos administradores de rede, referente à configuração e manutenção das tabelas dos roteadores.

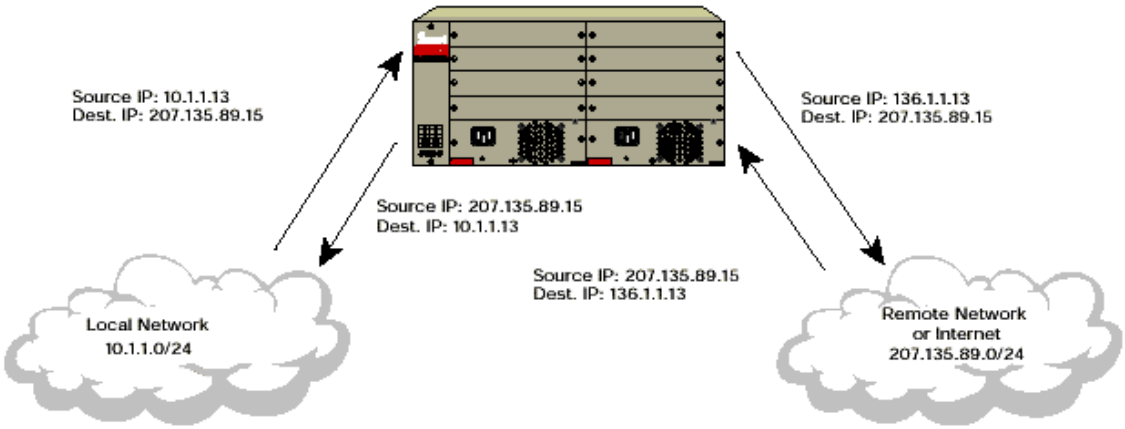


Figura 19 - Exemplo de NAT estático.

4.5.2. NAT – Dinâmico

O NAT dinâmico utiliza o esquema de tradução (m:n onde m>=1 e m>=n), onde as traduções de endereços IP privativos são criados a partir de um único endereço (caso especial de NAT dinâmico, item 4.5.3) ou um *pool* de endereços IP públicos disponíveis. Nesse caso, em cada conexão, o endereço IP privado é traduzido para um endereço IP público diferente, conforme figura 20 [3].

Quando todos os endereços IP alocados ao NAT estão ocupados, as traduções e os pedidos de novas conexões serão recusados. No NAT dinâmico existe a necessidade de manter o controle sobre o estado dos *hosts* em comunicação e, em alguns casos, até mesmo das conexões (códigos de porta TCP ou UDP) desses mesmos *hosts*.

Para cada conexão, os pacotes provenientes da rede interna serão traduzidos para um endereço IP público diferente, fazendo com que os *hosts* da rede interna não sejam acessíveis externamente. As tentativas de conexões partindo de *hosts* da rede externa somente serão aceitos caso haja uma entrada correspondente na tabela de tradução de endereços. É responsabilidade do NAT manter informações sobre o estado de cada mapeamento existente entre endereços IP públicos e privados.

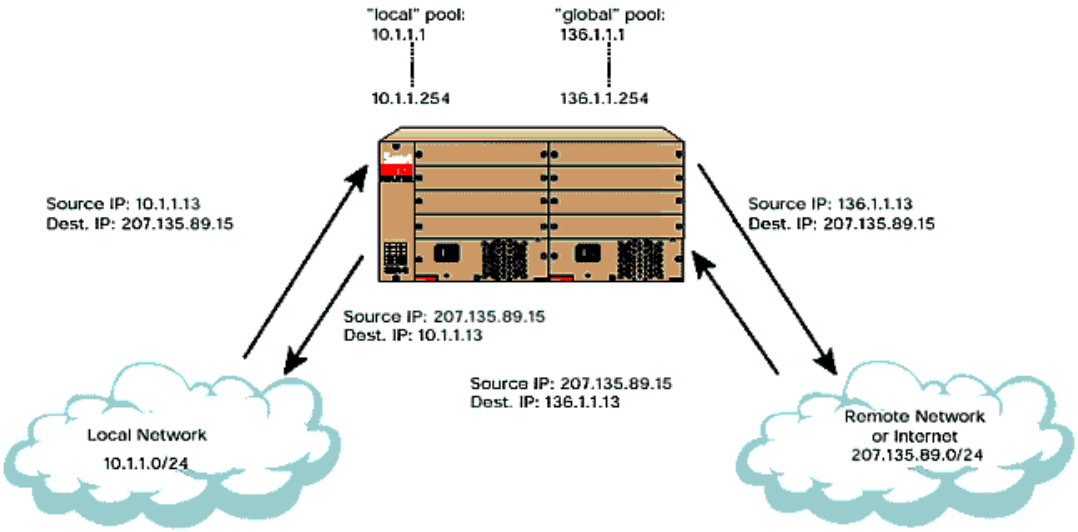


Figura 20 - Exemplo de NAT dinâmico.

4.5.3. Network Address Transation - Port Transation (NAT-PT)

Um caso especial do NAT dinâmico é a tradução m:1 do NAT-PT, utilizando o esquema (m:n onde m>=1 e n=1). Provavelmente essa é a técnica de NAT mais utilizada atualmente, pelo qual vários endereços IP da rede interna podem ser representados externamente por apenas um endereço IP público.

O serviço de NAT-PT é um caso especial de NAT dinâmico, com a função de converter diversos IPs privativos em apenas um IP público. Neste caso, toda a rede interna é mapeada em um IP público externo. A principal diferença com o NAT dinâmico visto no item anterior é que, neste caso, não existe a limitação de uma conexão a cada instante, ou seja, não há correspondência entre um *host* trocando dados com a Internet e um NAT IP ocupado.

Muito conhecido em ambientes Linux como mascaramento de IP [RAN00], pelo fato de ser capaz de funcionar em níveis de protocolo mais complexos e de fazer modificações mais complicadas que simples alterações de endereços.

O mascaramento no Linux também é capaz de lidar com outros protocolos como: FTP e o RealAudio, que podem exigir conexões TCP inversas ou portas UDP adicionais. O suporte para esses protocolos pode ser adicionado através da carga dinâmica de novos módulos no núcleo do *kernel*.

Em contraste ao NAT dinâmico, no mascaramento IP, um endereço IP público pode estar associado a mais de uma conexão com a rede interna ao mesmo tempo. Um número arbitrário de conexões é multiplexada em torno de um mesmo endereço IP público por meio dos códigos referentes às portas TCP e UDP. Na implementação padrão, a quantidade de portas alocadas foi de 4.096 para TCP e UDP.

Um problema dessa técnica é que alguns serviços em certos *hosts* somente aceitam conexões provenientes de portas privilegiadas, visando garantir que não se originam de usuários comuns. Na implementação de vários sistemas Unix e Linux, o uso de portas TCP e UDP privilegiadas (portas com número inferior a 1.024) é reservado aos administradores.

No modo NAT-PT é impossível que exista tráfego do tipo *inbound* com origem na rede externa pelo mascaramento IP. Isso ocorre porque o NAT utiliza as associações já existentes entre endereço IP público e número de porta para as traduções. Com isso, apenas o tráfego *inbound* das sessões ativas é aceito, ou seja, *hosts* que iniciaram conexões da rede interna.

Quando houver a necessidade de acesso a servidores ou mesmo *hosts* à rede interna, existem duas possibilidades: configurar o *host* no modo estático, permitindo acesso bidirecional, ou atribuir endereços públicos a esses *hosts.*

A grande vantagem do mascaramento IP é que este exige apenas um único endereço IP público para que uma rede inteira consiga acesso à Internet. Isso é importante, pois os endereços IP públicos podem custar muito caro. Com isso, é possível compartilhar conexões via linha discada ou linha ADSL (*Asymmetric Digital Subscriber Line*).

No ambiente Windows2000 existe o serviço que permite múltiplos clientes usarem uma única conexão a uma rede externa, chamada de ICS (*Internet Connection Sharing*), podendo ser uma conexão utilizando uma interface de rede ou mesmo via linha discada utilizando o serviço de RRAS (*Remote Routing Access Service*).

Como visto anteriormente, o NAT modifica o endereço IP e os números de portas TCP e UDP dos pacotes durante a tradução, e essas informações são suficientes para que os serviços NAT modifiquem o pacote e, então, retornem o tráfego correspondente ao cliente original.

Qualquer tradução, além desses três itens citados, requer uma carga adicional dos componentes de *software* chamados de editores NAT, fazendo modificações no pacote IP além da tradução básica. Para isso, o Windows2000 inclui editores NAT para os seguintes protocolos: FTP, ICMP, e NBT (NetBios over TCP) [FOR01].

A figura 21 mostra um exemplo do funcionamento para um cliente que se conecta a um servidor Web da Internet, mostrando o endereço IP e as portas de cada conexão (do cliente para o NAT e do NAT para o servidor Web). O mascaramento continuará a repassar pacotes de volta ao cliente, desde que o cliente mantenha a sua conexão TCP ativa. No caso do protocolo UDP, que é sem conexão, o mascaramento repassará os pacotes de volta ao cliente, dependendo do tempo de configuração de *time-out*.

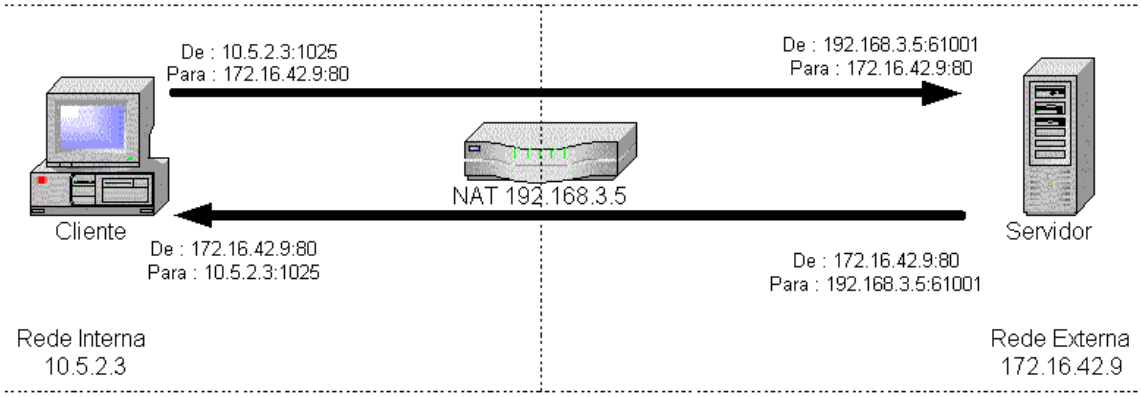


Figura 21- Mascaramento para protocolos de saída.

O mascaramento pode ser utilizado para encaminhar portas de entrada a serviços internos da rede. A capacidade de mapear portas de entrada deve ser configurada de forma estática para cada porta que deve ser encaminhada [ZWI00]. A figura 22 mostra o mascaramento configurado para encaminhar o serviço de SSH a um servidor interno e inclui os endereços de IP e números de portas correspondentes a cada conexão (interna e externa).

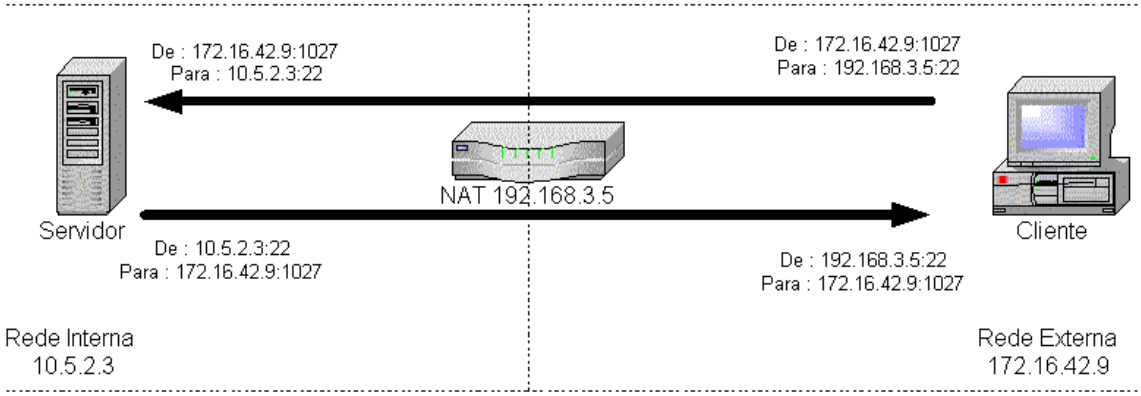


Figura 22 - Encaminhamento de serviços de entrada com mascaramento.

No caso de protocolos mais complexos, o mascaramento pode configurar portas TCP e UDP adicionais de escuta com base no conteúdo do pacote que tenham sido vistos. Assim o mascaramento pode até reescrever o conteúdo de pacotes de dados, a fim de substituir endereços IP e número de portas, como por exemplo, no caso do serviço de FTP que utiliza as portas 20 (dados) e 21 (comandos).

4.5.4. *Application Level Gateway* (ALG)

As técnicas de NAT são importantes mecanismos para a resolução de problemas como o limite de números IPs. Existem outros usos de NAT, que são independentes da solução destes problemas, e que estão sendo usados por várias empresas.

Um ALG é um agente tradutor específico, utilizado nas aplicações em que o NAT apresenta dificuldades para tradução. Em especial, aquelas que incluem endereços IP ou números de porta na parte denominada de *payload* de um datagrama IP, como por exemplo, do protocolo FTP.

Certas aplicações executadas em *hosts* da rede interna podem comunicar-se com *hosts* na rede externa, somente com o uso de ALG.

Um das vantagens é que ALGs não precisam saber informações de estado do NAT, já que podem alterar a parte de *payload* e simplesmente avisar o NAT para que inclua informações adicionais de estado. São semelhantes a *proxies*, no sentido de que funcionam baseados no conhecimento da aplicação. Eles podem ser transparentes ou não [BIL01].

4.6. Limitações do NAT

O NAT funciona bem para endereços IP no seu cabeçalho. Alguns protocolos de aplicação trocam informações de endereços IP na parte de dados do aplicativo, chamado de *payload*, na qual o NAT geralmente não estará apto a trabalhar com a tradução de endereços IP no protocolo de aplicação. Deve-se ressaltar que a implementação do NAT, para aplicativos específicos que possuam informação IP nos dados do aplicativo, é mais complexa que as implementações de NAT comum.

Outra limitação preponderante do NAT é que este altera várias informações em um datagarama IP. Quando uma autenticação IPSec ponta a ponta é utilizada, o datagrama, no qual o endereço foi alterado, falhará na verificação de integridade deste, uma vez que a mudança de qualquer bit no datagrama IP invalidará o valor de verificação de integridade que foi gerado pela origem.

A seguir, uma lista das principais limitações do NAT, apresentadas na RFC 3027:

- necessidade de manter informações baseadas em estados.

  À exceção do NAT estático, é necessário armazenar e gerenciar dinamicamente informações, não apenas sobre os clientes usando um NAT em um dado momento, mas também as suas conexões. Adicionalmente, essas informações poderão expirar devido à inatividade dos *hosts* envolvidos e isso deve ser controlado para disponibilizar novas conexões aos demais *hosts* da rede interna.

- aplicações que embutem endereço IP.

  As aplicações que utilizam informações de endereçamento IP na parte de *payload* não podem ser traduzidas facilmente pelo NAT, é necessário que algum

tipo de ALG seja utilizado para trabalhar nos pacotes pertencentes às camadas de aplicação.

- aplicações com interdependência entre sessões de dados e controles.

  O NAT opera com a premissa de que cada sessão é independente. Características de cada sessão como: orientação, endereços IP fonte e destino, protocolo e identificadores do nível de transporte, são determinadas independentemente no início de cada sessão.

  Entretanto, aplicações como H.323 usam uma ou mais sessões de controle para ajustar características das sessões seguintes. Essas aplicações exigem o uso de ALG que possa interpretar e traduzir a parte de *payload* sempre que necessário.

- problemas de depuração e log.

  Como um endereço IP da rede privada pode ser associado a um ou mais endereços IP públicos, ou mesmo a diversas portas ao longo do tempo no caso de mascaramento IP; é muito difícil fazer qualquer estudo de controle do fluxo baseado puramente em endereços públicos e portas. Isso dificulta a análise de logs de sistema e pode até mesmo dificultar o uso associado a outras soluções de segurança.

- tradução de pacotes fragmentados.

  O NAT pode apresentar problemas no gerenciamento de pacotes fragmentados, nos casos em que o primeiro fragmento não é o primeiro a ser processado. No modo dinâmico, se os pacotes chegarem em ordem aleatória e o primeiro fragmento chegar antes, não há problema independente da ordem dos demais. Basicamente o NAT armazena o primeiro fragmento por causa das informações do cabeçalho de transporte de tal forma que ele procura pelos outros fragmentos.

A RFC 2993 apresenta as vantagens e desvantagens do uso do protocolo NAT.

4.7. Vantagens do NAT

- no modo dinâmico, permite acesso à Internet sem a necessidade de obter e associar endereços IP públicos com a rede privada. Um grande número de *hosts* pode acessar a Internet por um endereço público porque um número diferente de porta é utilizado para cada conexão;

- o NAT fornece a funcionalidade de um servidor *proxy*;

- o mascaramento de endereços IP minimiza o impacto de alterações de endereçamento de configurações de *hosts* clientes, nas trocas de provedores de acesso;

- evita a necessidade de justificativas freqüentes às autoridades da Internet acerca de novos pedidos de alocação de endereços públicos;

- para aplicações que não se baseiam na autenticidade do cabeçalho do pacote, o emprego de NAT é transparente, e os *hosts* não necessitam de alterações.

4.8. Desvantagens do NAT

- quebra a estrutura do modelo fim-a-fim da Internet (RFC 2775);
- cria um caminho crítico de falha no dispositivo que mantém o estado da comunicação e informação sobre mapeamentos realizados dinamicamente;
- não permite a implementação de certos serviços, como IPSec, RPC e DNSSec, pois os pacotes são criptografados;
- gera a confusão entre espaço de endereçamento IP público e privativo;
- o NAT dinâmico aumenta a complexidade operacional quando serviços públicos residem no lado privado. Isso implica a restrição de que apenas um *host* privado pode ser acessado através de porta bem conhecida.

4.9. Recomendação uso do NAT

A seguir apresentam-se algumas recomendações feitas pelo Comitê Gestor da Internet no Brasil – Grupo de trabalho de Engenharia e Operações de redes (www.cg.org.br), realizado em meados de 2000.

Existem várias implementações do NAT baseada na RFC1631, dependendo do fabricante ou do sistema operacional utilizado, conforme as necessidades específicas de cada organização. São mencionadas várias recomendações para a não-utilização do NAT, onde pode-se destacar:

- consultas inversas a servidores DNS não funcionam apropriadamente;
- usuários não poderão utilizar clientes IPSec em seus PCs, pois a tradução de endereços, por definição, é vista pelo protocolo IPSec como um ataque de interceptação. Isso significa que usuários que utilizam esses clientes para se conectar a sua corporação e estabelecer uma rede virtual privada não poderão fazer isso através da rede do seu provedor;
- aplicativos baseados no protocolo H.323 (Internetphone, Netmeeting, etc) não funcionarão aproriadamente. O H.323 é um protocolo complexo, que utiliza portas dinâmicas e inclui vários fluxos UDP. Os endereços e portas negociados entre os participantes de uma sessão multimídia são transmitidos dentro do fluxo de dados (*payload*) da conexão de mais alto nível;
- o uso de NAT necessita de um poder de processamento maior mesmo com a ajuda de um algoritmo de ajuste de *checksum* otimizado, pois cada pacote de dados está sujeito a procura na tabela de tradução e modificações;
- além dos problemas mencionados acima, existem outros relacionados a QoS, troca de tabelas de roteamento, Secure DNS da RFC2535, e outros diversos aplicativos populares.

4.9.1. Outras recomendações do uso do NAT

Conforme RFC 2993, são feitas várias recomendações a serem avaliadas antes da opção pelo uso de NAT.

- o mecanismo utilizado para resolução de nomes deve garantir resposta correta para cada administração de endereços. Incluir servidor DNS ou DNS ALG no dispositivo NAT, em vez de tentar sincronizar sistemas DNS independentes;

- se o NAT é dinâmico, o TTL deve ser ajustado em zero para os clientes não colocá-los em *cache;*

- se o NAT for único, considerar as possibilidades de um único ponto de falha (sem redundância);

- examinar as aplicações que necessitam passar pelo NAT e, se for o caso, providenciar os ALGs apropriados;

- se existirem campos com a parte de *payload* criptografados, seus conteúdos não podem ser alterados, a menos que o NAT seja um ponto terminal de algum tipo de sistema de segurança;

- determinar o caminho da resolução de nomes, para o caso de *hosts* do lado externo do NAT-PT exigirem visibilidade;

- garantir que as aplicações usadas interna e externamente não usem nomes de *hosts* embutidos nos pacotes.

A seguir, apresenta-se uma lista com os principais serviços utilizados na Internet e compatibilidade com o NAT [SHI00].

Protocolos	**NAT**	**Razão para falha**	**Solução ALG**
Camada de Rede e Transporte			
PPTP / L2TP	SIM	N/A	N/A
VPN (IKE / IPSec)	NÃO	IP encriptado	NÃO
SSL / TLS	SIM	N/A	N/A
Camada de Aplicação			
RPC	NÃO	1.IP e Portas dinâmicas 2.IP e Portas encriptados	SIM NÃO
KERBEROS	SIM	N/A	N/A
RADIUS	SIM	N/A	N/A
VoIP (H.323 / SIP / MGCP)	NÃO	IP e Portas dinâmicas	SIM
SET	SIM	N/A	N/A
FTP	NÃO	IP e Portas no *payload*	FTP-ALG
DNS DNSSec	NÃO NÃO	IP e Portas no *payload* IP e Portas encriptados	DNS-ALG NÃO
STMP/POP3/IMPA4/SSH	SIM	N/A	N/A
HTTP.	SIM	N/A	N/A
SNMP	NÃO	IP no *payload*	SNMP-ALG

Tabela 22 - Compatibilidade de protocolos em ambiente NAT.

A tabela 22, mostra que o NAT não consegue operar com serviços que trabalham com portas dinâmicas necessitando de um ALG, e no caso de endereços IP ou portas encriptados no seu payload o serviço de NAT não é possível.

No caso da rede IPTNet, o serviço de NAT está implementado diretamente no roteador de saída (marca Foundry modelo FastIron 4802) e possui suporte de ALG para os seguintes serviços: ICMP, UDP e TCP (Genérico), FTP, VDOLive, StreamWorks, CU-SeeMe, RealAudio, RealVideo, RealMedia, QuickTime, Microsoft Media Services, Web Theater (Vxtreme).

Muitas corporações, incluindo o IPT, adotaram o NAT e o esquema de endereçamento privativo para garantir acessibilidade de todos os seus usuários à rede Internet, e para isso, adotou tecnologias que mudaram os requerimentos de gerenciamento da sua infra-estrutura IP.

4.10. Futuro do NAT

Um dos principais projetistas do protocolo TCP/IP, o Dr. Vint Cerf, afirmou, durante uma conferência em 1977, que 32 bits de endereçamento eram o bastante para o crescimento da Internet por um longo período de tempo. Após quase 25 anos em outra recente conferência o próprio Dr. Vint declara que estava enganado, apoiando e participando do desenvolvimento do protocolo IPv6.

A crise gerada pela falta de endereços IP reforça a necessidade de um grande aumento de endereços IP nos próximos anos. Porém, o problema de esgotamento de endereços é apenas um dos itens dos vários problemas do atual protocolo IPv4 e não como item mandatário para a migração para o IPv6, visto que o NAT possibilitou a muitas empresas o acesso à Internet, e, dependendo das reais necessidades, vão continuar com esse método por muito tempo.

Conforme visto ao longo do capítulo, a criação do NAT permite trabalhar com endereços privativos e com aplicações básicas da Internet (Web, FTP, E-mail etc). No contexto atual, onde o IPv6 está sendo utilizado apenas pela comunidade acadêmica, as empresas comerciais, que necessitam de conectividade imediata com IPs fixos, vão utilizar o NAT como ferramenta de interconexão, combinado com um sistema de *firewall* para a segurança da sua rede interna.

O NAT terá o seu lugar não somente como conversor de endereços IPv4 públicos e privativos para sistemas legados, mas também como tradutor de protocolos IPv4 e IPv6, devendo ser um sistema importante durante a fase de transição e migração dos protocolos.

Contudo a grande alavanca para o IPv6 está associada as aplicações de tempo real, segurança com IPSec, Voz sobre IP, qualidade de serviço e principalmente a questão da mobilidade em conjunto com tecnologias *wireless*, onde milhões de dispositivos móveis estão sendo utilizados atualmente sem conectividade com a Internet como: celulares, *laptops*, PDAs, *player* MP3, câmeras digitais, equipamentos móveis existentes em carros, barcos, aeronaves e em equipamentos de entretenimento como: PCs domésticos, TV digital e *home appliances*.

Com as novas aplicações para o mundo dos negócios voltados a B2B (*business-to-business*), as corporações necessitam da conectividade fim-a-fim global, segurança, desempenho, e escalabilidade para atender às fortes exigências dessas novas aplicações emergentes da Internet, sendo caraterísticas intrínsecas do novo protocolo IPv6.

Capítulo 5 – MECANISMOS DE TRANSIÇÃO IPv4-IPv6

5.1. Introdução

Os protocolos IPv6 e IPv4 não são compatíveis diretamente entre si, fazendo com que *hosts* e roteadores IPv4 não possam tratar diretamente pacotes do tráfego IPv6 e vice- versa. Com isso, haverá certas dificuldades iniciais como ocorrem em qualquer mudança de plataforma e/ou paradigma a se implantar nas organizações.

Pensando nessa situação, o IETF criou um grupo de trabalho denominado NGTrans (*NgTran Working Group*), para avaliar e propor soluções específicas com o propósito de garantir a transição de maneira gradual, não causando impacto na funcionalidade da Internet, durante o período do tempo de migração.

A RFC 28893 (*Transtion Mechanisms for IPv6 Hosts and Routers*) e a RFC 2185 (*Routing Aspects of IPv6 Transition*) definem os principais aspectos dos mecanismos de transição, também conhecidos como SIT (*Simple Internet Transition*) tendo como principais objetivos:

a) permitir a atualização progressiva e individual de *hosts* e roteadores;
b) evitar as dependências de atualização;
c) completar a transição antes do esgotamento do espaço de endereçamento IPv4.

5.2. Componentes da transição

5.2.1. *Hosts*

Na prática, o conceito da transição gradativa significa que muitos *hosts* ficarão restritos à operação com o IPv4 e os demais *hosts* farão a migração para IPv6. Para permitir e manter a interoperabilidade entre os dois protocolos, é necessário que todos os *hosts* que estiverem com o IPv6 possam se comunicar com o protocolo IPv4, da mesma forma deverá ocorrer com as APIs (*Aplication Program Interface*) das aplicações.

5.2.2. Roteadores e protocolos de roteamento

Os roteadores possuem papel fundamental de sustentação da infra-estrutura geral da rede Internet, devendo seguir as mesmas regras aplicadas aos *hosts*, acima mencionado.

Os novos dispositivos com suporte ao IPv6 devem partir do princípio que todos sistemas restantes estejam interagindo com o protocolo IPv4, inclusive com os protocolos de roteamento Quando as versões comerciais começarem a ganhar mais interesse dentro da infra-estrutura da Internet, as regras de roteamento de IPv6 devem permitir o roteamento, baseadas na origem e no destino.

5.2.3. *Domain Name System* (DNS)

Durante a fase da transição, os nós com suporte IPv6 devem ser capazes de conviver com endereços IPv4 e endereços IPv6. Os sistemas antigos, que não forem realizados a atualização, terão naturalmente ainda um endereço IPv4. Entretanto, um endereço IPv6 pode já ter sido atribuído também. O DNS tem que responder com ambos os endereços, se disponível, para perguntas dos *hosts* IPv6. Fica a cargo do *host* a decisão de qual protocolo deseja utilizar.

Os servidores de DNS deverão ser os primeiros a serem atualizados, após a alocação de um endereço de IPv6 em uma organização, devendo realizar o mapeamento de endereços para disponibilizar na Internet. Isto permite que os novos nós IPv6 executem o serviço de localização e resolução de nomes, via comando *"nslookup"*.

O conceito de dualismo do protocolo permite que os sistemas IPv4 continuem a sua operação sem nenhuma modificação. A atualização nos protocolos de roteamento pode também ser executada de forma gradativa, na qual o número de roteadores capazes de suportar IPv6 também aumentará.

Maiores informações a respeito do DNS verificar o item 3.4.9.

5.3. Métodos de Transição

Durante a fase de transição, poder-se-á ter três tipos diferentes de nós IP:

- nó IPv4: roteador ou *host* com suporte apenas para IPv4;
- nó IPv6: roteador ou *host* com suporte apenas para IPv6;
- nó IPv4/IPv6: roteador ou *host* com suporte para os protocolos IPv4 e IPv6.

Os nós podem usar a autoconfiguração sem estado *(stateless*) ou com estado (*statefull*) para obter seu endereço IPv6, conforme visto nos itens 3.4.4.2 e 3.4.4.3.

Os mecanismos introduzidos pelo SIT asseguram que *hosts* IPv6 possam interoperar com *hosts* IPv4, até o momento em que os endereços IPv4 se esgotem. Com a utilização do SIT, existe a garantia de que a nova versão do protocolo IP não vai tornar obsoleta a versão atual, protegendo assim o enorme investimento já realizado no IPv4. Os nós que necessitam apenas de visibilidade limitada (por exemplo, impressoras), a atualização para o protocolo IPv6 será ser em ultima instância.

Os principais métodos de transição utilizados, conforme figura 23 [6] são os seguintes:

- **Pilha dupla** - implementação de pilha dupla para *hosts* e roteadores que devem interoperar com o IPv4 e o IPv6;
- **Tunelamento** - mecanismos de tunelamento IPv6 sobre IPv4 para o transporte de pacotes IPv6 através de redes com roteadores IPv4;
- **Translação** - tradução de cabeçalho IPv4/IPv6.

A seguir, apresenta-se o detalhamento dos métodos acima mencionado, avaliando –se os principais mecanismos existentes associados a cada método.

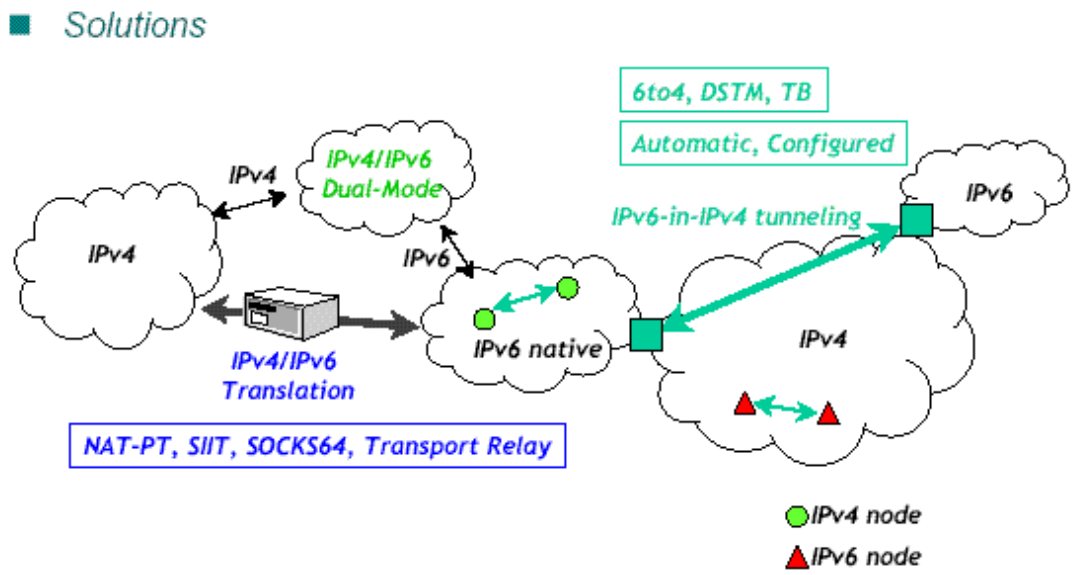


Figura 23 – Métodos de transição IPv4-IPv6.

5.3.1. Pilha dupla (*Dual stack*)

A maneira mais simples de resolver a questão da interoperabilidade entre as duas versões foi introduzir a idéia de duplicação dos protocolos IPv4 e IPv6 na camada de rede, rodando as duas pilhas de protocolos no mesmo nó, permitindo que se possa manipular os dois tipos de tráfego [MUR00].

O protocolo IPv6 pode incorporar endereços IPv4, utilizando os endereços IPv6 compatíveis com IPv4, conforme descrito no item 3.4.14.5.3. Cabe lembrar, que os endereços não precisam necessariamente estar relacionados.

Esse método será utilizado no início do processo de transição, onde todos os nós de pilha dupla deverão possuir um endereço IPv4 configurado. A figura 24, mostra um nó de pilha dupla podendo se comunicar tanto com um sistema IPv4 e/ou IPv6 na mesma conexão. A questão chave desse processo é o DNS, pois o nó de pilha dupla deve tomar a decisão de qual protocolo deverá utilizar, conforme informação retornada pelo DNS. Assim, a configuração dos endereços IPv6 com registros tipo “AAAA” é requisito fundamental para a interoperabilidade dos dois protocolos.

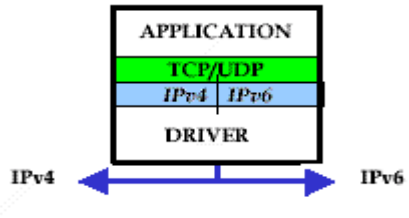


Figura 24 – Pilha dupla.

Fica claro que mudanças nos protocolos de transporte e novas APIs serão necessários para explorar todas as potencialidades do novo protocolo com as novas aplicações que deverão surgir, como veremos adiante.

5.3.1.1. *Dual Stack Transition Mechanism* (DSTM)

Os *hosts* com pilha dupla configurada possuem endereços permanentes. Com o problema de escassez de endereços IPv4, esse endereço público deveria ser utilizado somente quando requisitado, evitando o desperdício de endereços.

Para resolver esse problema, foi criado um mecanismo chamado de DSTM, permitindo que nós, com a implementação de pilha dupla, possam ser configurados para realizar conexões em IPv4, alocando-se endereços IPv4 temporários e dinamicamente, ou seja, somente quando necessário.

O mecanismo de DSTM é resultado da combinação de AIIH (*Assignment of IPv4 global addresses to IPv6 Hosts*) e DTI (*Dynamic Tunnelling Interface*).O DSTM permite a comunicação bidirecional de um *host* IPv4 com um nó com pilha dupla configurada dentro de uma rede IPv6 nativa, sendo necessários um servidor DHCPv6 integrado com DNS e um roteador de borda com suporte a DSTM, conforme figura 25. Os pacotes IPv4 são encapsulados em IPv6 através de um túnel DTI [9].

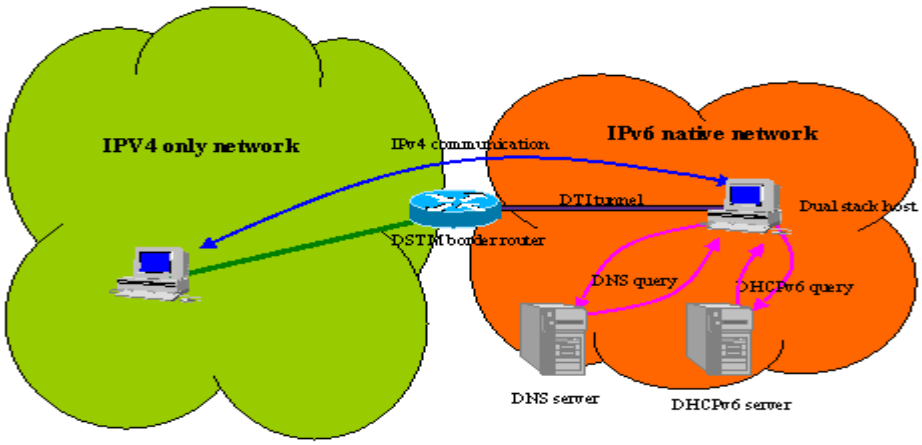


Figura 25 - Arquitetura de DSTM.

5.3.2. Tunelamento

O método do tunelamento permite o encaminhamento de tráfego IPv6, através da infra-estrutura IPv4 existente da Internet. Dessa forma, um roteador ou *host* que implemente a pilha dupla, situado no extremo de uma topologia IPv6, tem apenas a função de encapsular pacotes IPv6 em IPv4 (adicionar um cabeçalho especial IPv4 a um pacote IPv6), enviando-o em seguida através de infra-estrutura IPv4, como se fossem dados IPv4 normais. Os roteadores IPv4 efetuam o reencaminhamento destes dados sem envolvimento do protocolo IPv6. Na outra extremidade do túnel, encontra-se outro roteador ou *host* que tem a função de desencapsular o pacote IPv6 (retirar o cabeçalho IPv4) e encaminhar o pacote para o seu destino, usando as funções do protocolo IPv6.

Assim, o nó de entrada do túnel faz o encapsulamento do pacote IPv6 num cabeçalho IPv4, e o nó de saída do túnel recebe o pacote encapsulado, retirando o cabeçalho IPv4, atualizando o cabeçalho IPv6 e processando o pacote IPv6 resultante.

Conforme figura 26, em vez de enviar um pacote IPv6 diretamente ao seu destino, os pacotes IPv6 são encapsulados dentro de pacotes IPv4, usando a infra-estrutura IPv4. Portanto, na fase de transição, o mecanismo de tunelamento deverá ser muito utilizado.

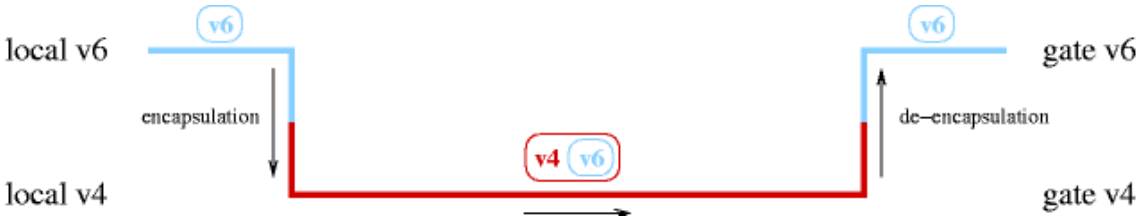


Figura 26 – Tunelamento de pacotes IPv6 dentro do IPv4.

A RFC 1933 definiu duas técnicas de tunelamento, com a diferença no modo como identificam o endereço da extremidade do túnel.

5.3.2.1. Túnel sobre IPv4 configurado ou estático

Esse método se caracteriza por encaminhar qualquer pacote IPv6 através de uma rede IPv4. Em túneis configurados, o endereço do nó de saída do túnel é determinado com base em informação de configuração do nó, onde se faz o encapsulamento. Este nó necessita armazenar o endereço do final de cada túnel que nele se inicia. Quando um pacote IPv6 é transmitido através de um túnel, o endereço final configurado para esse túnel é usado como endereço destino do cabeçalho IPv4 que encapsula o pacote. A determinação de quais pacotes a enviar por cada túnel é feita através de informação de roteamento do nó que vai encapsular esses pacotes.

O túnel configurado caracteriza-se pelo fato de requerer uma preparação de ambos os lados do próprio túnel, geralmente sujeita a alguma forma de registro, a fim de intercambiar os dados de configuração. Um exemplo desse túnel é o encapsulamento *6over4* descrito no item 5.3.2.3.

5.3.2.2. Túnel sobre IPv4 automático

Esse método é utilizado para encaminhar um pacote IPv6 *unicast* com o formato de endereço compatível IPv4, conforme descrito no item 3.4.14.5.3. Em túneis automáticos, o endereço do nó de saída do túnel é determinado a partir do pacote que vai ser encapsulado. O endereço destino do pacote original tem de ser um endereço IPv6 compatível com IPv4, sendo o endereço do final do túnel a componente IPv4 do primeiro, os 32 bits menos significativos do endereço IPv6 compatível com IPv4 [MUR00].

Um túnel automático requer um servidor público com suporte à conectividade IPv6, por exemplo, via *6Bone*. Este servidor torna públicos os próprios dados de conectividade e ativa o protocolo de tunelamento, que não requer um registro explícito dos *sites* que o utilizam para se conectar.

5.3.2.3. Túnel *6over4*

O método denominado 6over4, documentado na RFC 2529, é um mecanismo que não requer registro de informações IPv6, e implementa o transporte do IPv6 em uma rede IPv4 habilitada para o *multicast*. Nesse caso, existe a necessidade de registro em um *gateway* como o *6Bone*. A sua principal desvantagem é a necessidade de uma infra-estrutura *multicast* existente. Se não existir uma estrutura desse tipo, a sua criação e configuração requerem esforço comparável à configuração de túnel IPv6 direto. Portanto, trata-se de uma hipótese que não vale a pena considerar.

5.3.2.4. Túnel *6to4*

Este mecanismo permite a interligação de ilhas IPv6 através da infra-estrutura IPv4 existente, conforme RFC 3068. A Figura 27 mostra a construção de endereços IPv6 a partir do IPv4. Os pacotes são encapsulados usando o prefixo 2002, sendo transmitidos via rede IPv4. O prefixo 2002 (conforme item 3.4.14.3.3) é reservado aos endereços de tipo *6to4*, isto é, aos endereços IPv6 derivados do IPv4.

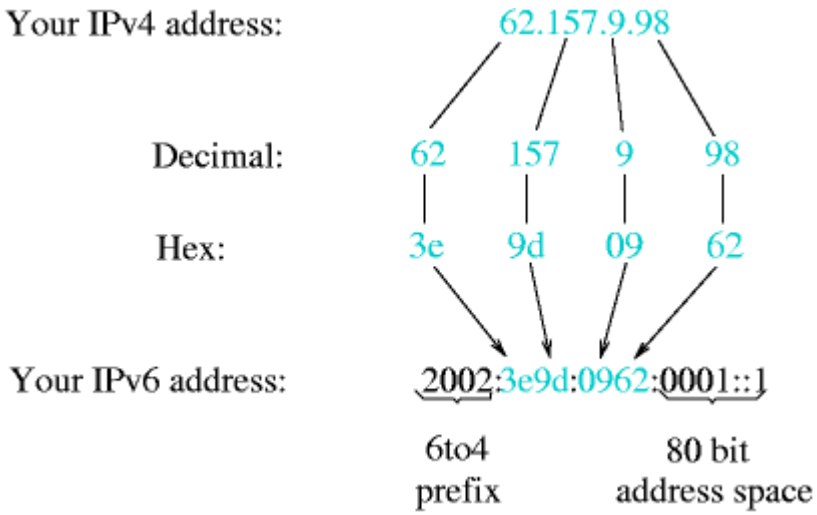


Figura 27 –Montagem de endereço IPv6 no método *6to4*.

A junção do prefixo *6to4* e do endereço IPv4 público, é montado o endereço IPv6 único e atribuído à máquina que tinha o endereço IPv4 de iniciação. Nesse método não há necessidade da utilização de endereços IPv4 compatíveis ou um túnel configurado, e são implementados tipicamente em roteadores de borda.

Diferentemente da configuração do túnel 6over4, não é necessário registrar-se em um *gateway 6Bone* que encaminhe o tráfico IPv6, pois as respostas são enviadas ao usuário do *gateway 6to4* mais próximo. O encapsulamento dos pacotes é realizado por uma interface de rede habilitada para 6to4, que depois providencia seu encaminhamento de acordo com o roteador instalado localmente.

No que diz respeito ao envio de pacotes IPv6 (tráfego de saída), a interface de rede habilitada para *6to4* trata o pacote IPv6 e o encapsula em um pacote IPv4. É necessária uma conexão no *gateway 6to4*, por sua vez conectado ao *6Bone*, que elimine o encapsulamento dos pacotes e os encaminhe ao *6Bone*.

5.3.2.5. *Tunnel Broker*

Descrito na RFC 3053, a principal aplicação dessa técnica consiste em que *hosts* IPv4 isolados possam acessar redes e serviços IPv6, via túnel IPv6 em IPv4. Baseado em interface Web, é estabelecido um túnel entre o nó IPv6 e o *host* requisitante, através de vários scripts que são rodados pelo cliente.

Essa técnica é bastante útil para usuário *dial-up*, que não precisa reconfigurar seu túnel manualmente todas as vezes que se conectam a um provedor. Assim, o cliente não necessita estar em uma rede *multicast* via *6over4* e a informação é enviada via http em IPv4.

O *Tunnel Broker* é muito simples, do ponto de vista do usuário, e ideal para usuários isolados que querem conexões com nós IPv6.

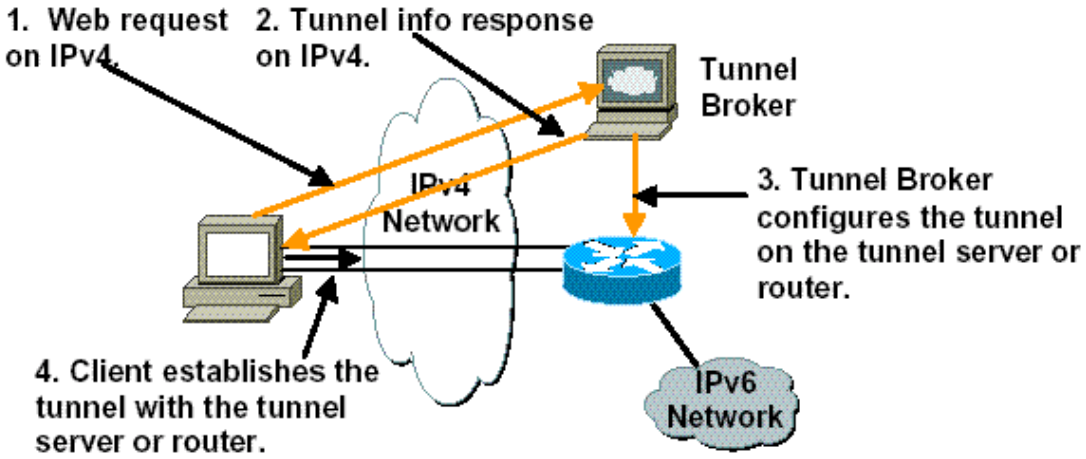


Figura 28 – *Tunnel Broker*.

5.3.3. Translação NAT-PT (*Network Address Translation – Port Translation*)

Através dos diversos mecanismos de transição descritos acima, a instalação de *hosts* e roteadores com pilha dupla fornece a compatibilidade com sistemas IPv4 existentes [8].

Assim, quando a transição do *backbone* atingir um estágio avançado, os novos nós a serem conectados terão apenas endereços IPv6. Dessa forma a tradução de cabeçalho será exigida apenas quando os nós IPv6 quiserem conversar com *hosts* IPv4.

O papel dos roteadores será de fundamental importância, os quais, além do mapeamento entre campos nos dois cabeçalhos, deverão converter os endereços de origem e destino dos endereços mapeados para endereços IPv4 puros, ao tirar os 32 bits de ordem inferior do seu endereço. Na direção contrária, o roteador adiciona o prefixo ::FFFF/96 ao endereço IPv4 para formar o endereço IPv4 mapeado (item 3.4.14.5.4) [1].

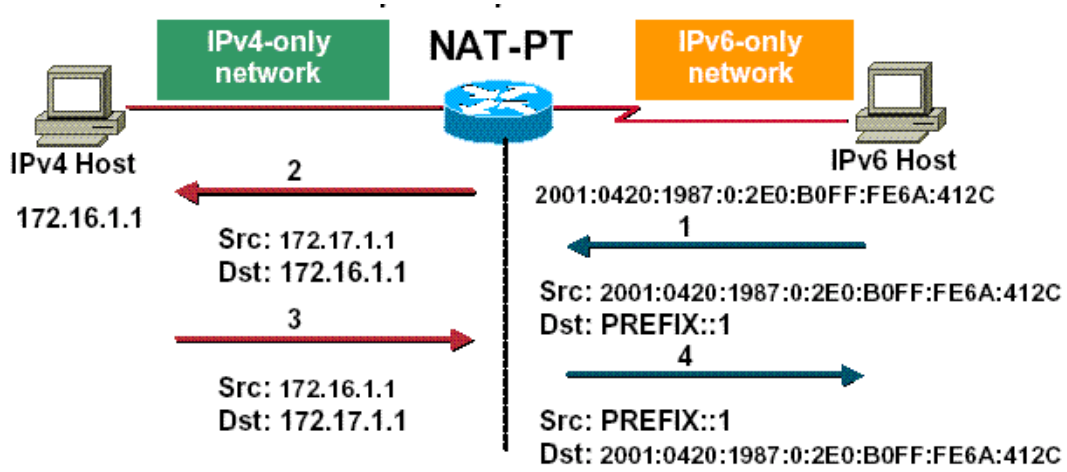


Figura 29 – Método NAT-PT.

O método NAT-PT, definido na RFC 2766, permite a comunicação entre nós IPv6 e *hosts* IPv4. A comunicação é realizada por um dispositivo dedicado que faz a tradução entre endereços IPv4 e IPv6 e mantém o estado das conexões durante o tempo da sessão. O dispositivo de NAT-PT também inclui um ALG (*Aplication Level Gateway*) para tornar a tradução possível entre IPv4 e requisições e respostas de IPv6 DNS (DNS_ALG). As extensões de DNS para NAT estão descritas na RFC 2694.

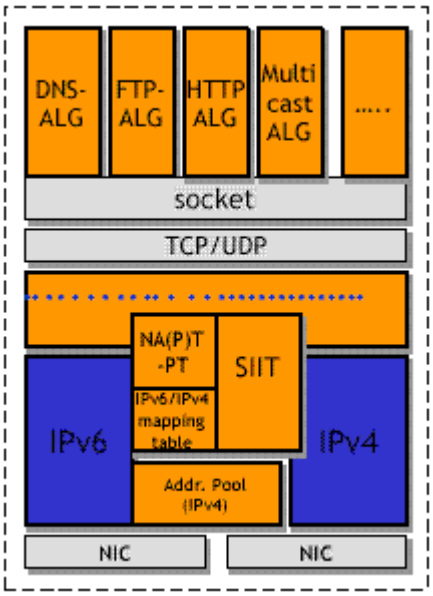


Figura 30 – ALG de Aplicações.

5.3.3.1. *Stateless IP/ICMP Translation* (SIIT)

O SIIT descreve um método de translação entre os protocolos IPv4 e IPv6. A translação é limitada a certos campos do cabeçalho IP, convertendo os campos específicos de cada protocolo, operando no modo *stateless*, no qual se devem verificar todos os pacotes que passam pelo sistema tradutor. O método SIIT está descrito na RFC 2765.

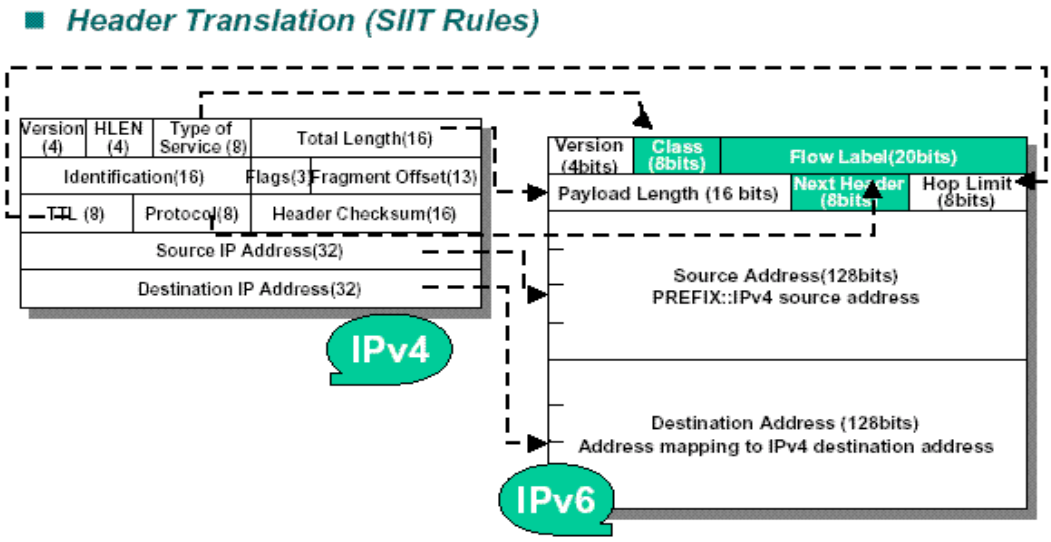


Figura 31 – Translação de cabeçalho IPv4-IPv6 com SIIT.

5.3.3.2. Migração de aplicações

As APIs de programação para IPv6 não são as mesmas para IPv4, necessitando que os programadores empreguem, em novas aplicações, as funcionalidades adicionadas ao IPv6, nas áreas de segurança, qualidade de serviço, mobilidade, multimídia etc. Os programas IPv4 atuais simplesmente não poderão conversar diretamente com *hosts* IPv6 sem modificação.

Grande parte dos *softwares* atuais deverá ser modificada para suportar o IPv6, podendo ser uma simples tarefa de recompilar o programa usando novas APIs, ou tão complexo como ter que reescrever uma grande parte de código de linhas do programa, dependendo completamente de como a aplicação original foi escrita.

A lista das principais aplicações com suporte ao IPv6 está disponível em (www.ipv6.org/v6-apps.html).

5.3.3.3. *SOCKS-64*

O método de *gateway* via *SOCKS* é uma ferramenta que possui características avançadas denominadas *SOCKS-EXT*, conforme RFC 1928, atuando como um *relay* de conexões TCP/UDP entre *hosts* com forte esquema de autenticação e provendo uma maneira fácil de conectar *hosts* IPv4 para nós IPv6 e vice-versa.

Como o *SOCKS* trabalha na camada de aplicação, não existem as desvantagens de outros mecanismos, como vulnerabilidade com fragmentação de pacotes, segurança fim a fim ou limites de salto entre redes. Outro aspecto importante é que não há necessidade de modificação de DNS, porém a aplicação do cliente deve possuir capacidade de configurar *SOCKS*. Aplicações escritas para IPv4 não necessitam de grandes mudanças ou modificações.

5.3.3.4. *Bump In the Stack* (BIS)

O método *Bump In The Stack*, descrito na RFC 2767, permite o uso de aplicações rodando em ambientes IPv4 a se comunicar com nós IPv6. São adicionados três módulos na pilha IPv4, que intervêm entre a aplicação e a rede, possuindo as seguintes funcionalidades: uma extensão para resolver nomes, um mapeador de

endereço e um tradutor. A idéia principal é que, quando uma aplicação IPv4 precisa comunicar-se com nós IPv6, o endereço IPv6 daquele nó é mapeado em um endereço IPv4 de um range de *hosts* de pilha dupla. O pacote IPv4 gerado para a comunicação é traduzido em um pacote IPv6 de acordo com o método SIIT.

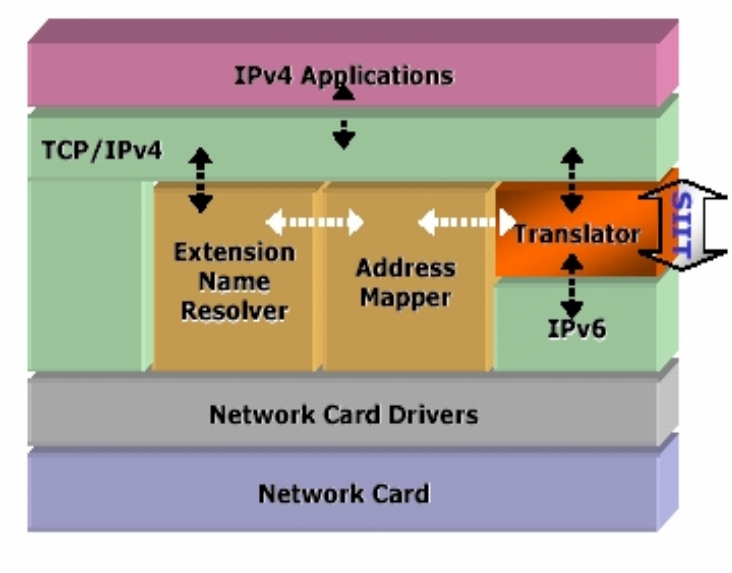


Figura 32 – *Bump In the Stack* (BIS)

5.3.3.5. *Bump-In-the-API* (BIA)

O método chamado de *Bump-in-the-API* consiste na tradução entre APIs de IPv4 e APIs de IPv6 em *hosts* de pilha dupla, de modo que possa ser efetivada sem a tradução e dependência do cabeçalho IP em protocolos de mais baixo nível, permitindo que *hosts* se comuniquem com outros nós IPv6 usando as aplicações IPv4, conforme RFC 3338.

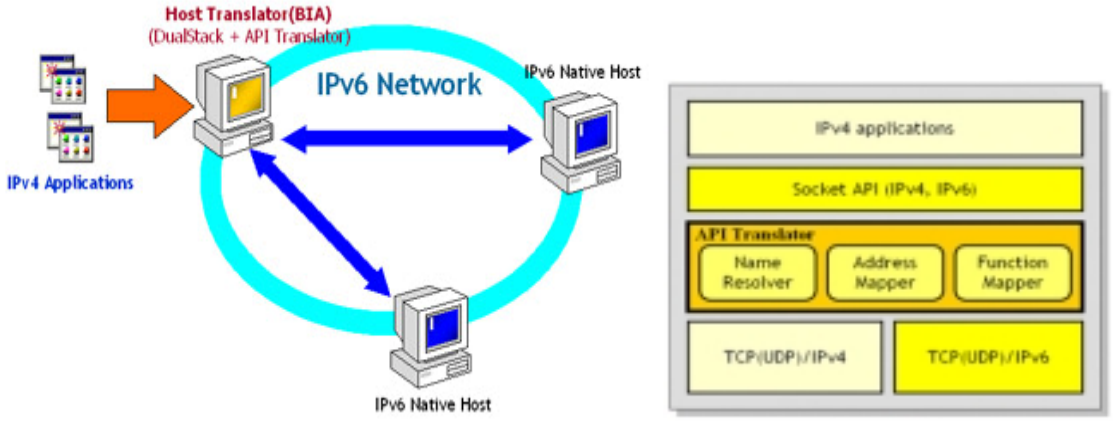


Figura 33 - *Bump-in-the-API* (BIA).

A técnica de BIA introduz um tradutor de API entre o módulo do *socket* do API e o módulo de TCP/IP no *host* de pilha dupla e traduz a função do *socket* API de IPv4 na função do *socket* API do IPv6 e vice-versa.

Quando as aplicações IPv4 no *host* de pilha dupla se comunicam com outros nós IPv6, o tradutor do API detecta as funções do *socket* API das aplicações IPv4 e invoca

as funções do API do *socket* IPv6 para se comunicar com os nós IPv6 e o vice-versa. A fim de comunicar-se entre as aplicações IPv4 e os nós IPv6, os endereços do range IPv4 serão atribuídos através do resolvedor, conhecido no tradutor de API [7].

A seguir, a tabela comparativa entre os vários mecanismos de transição descritos e sua devida aplicabilidade entre os protocolos IPv4 e IPv6 [11]:

Mecanismos de transição	**Implicações com as aplicações**	**Requerimentos de endereços IPv4 públicos**	**Utilização em *Hosts/Site***	**Escalabilidade**	**Comentários**	**Comunicação fim-a-fim**			
						IPv4-IPv4	**IPv6-IPv6**	**IPv4-IPv6**	**IPv6-IPv4**
Dual Stack	Não	Endereços permanentes ou *pool* de endereços IPv4 alocados via servidor DHCP	*Site/Host*	Não	Implementação simples e disponível em qualquer nó com suporte a IPv6	X			
DSTM	Não	*Pool* de endereços IPv4 são requeridos por um servidor AIIH.	*Site/Host*	Limitado ao número de conexões DTI que o roteador DSTM suporta	Permite que *host* rodem aplicações fim-a-fim com rede somente IPv6. Permite *hosts* IPv4/IPv6 com aplicação somente IPv6 a comunicação com *hosts* IPv4 ou IPv6 sem a necessidade de ALG	X			
6to4	Aplicações necessitam ser “portadas” para a comunicação com IPv6	O roteador de borda deve possuir um endereço IPv4.	*Site*	Limitado ao número de túneis suportado pelo roteador *6to4*	Permite a comunicação entre redes IPv6 separada por uma rede somente IPv4 Cada rede IPv6 necessita possuir o roteador de borda *6to4* configurado		X		
Tunnel Broker	Aplicações necessitam ser “portadas” para a comunicação com IPv6	Pelo menos um endereço IPv4 para a implementação do túnel.	*Site/Host*	Limitado ao número de túneis e endereços IPv6 suportado pelo servidor de *tunel broker*	Permite um *host* IPv4 isolado dentro de uma rede totalmente IPv4, a comunicação com rede IPv6 *Host* necessita suporte a IPv4 e IPv6		X		

continua

continuação

Meca-nismos de transição	**Implicações com as aplicações**	**Requerimentos de endereços IPv4 públicos**	**Utilização em *Hosts*/*Site***	**Escalabilidade**	**Comentários**	**Comunicação fim-a-fim**			
						IPv4-IPv4	**IPv6-IPv6**	**IPv4-IPv6**	**IPv6-IPv4**
6over4	Aplicações necessitam ser "portadas" para a comunicação com IPv6	Um endereço IPv4 por *host*	*Host*	Limitado ao número de túneis suportado pelo roteador *6over4*	Permite conectar rede IPv6 separada por uma rede somente IPv4 Necessita de uma rede multicast IPv4 Cada rede IPv6 necessita de roteador de borda *6over4*		X		
NAT-PT	Aplicações que incluem endereço IP na camada superior necessitam de um ALG	*Pool* de endereços IPv4	*Site*	Limitado ao número de translações simultâneas que podem ser feitas	Necessita de ALG para diversos protocolos FTP, DNS etc Mecanismo localizado em um único ponto			X	X
SIIT	Não compatível com aplicações que utilizam o endereço IP nas camadas superiores.	*Pool* de endereços IPv4.	*Site*	Não	Permite a comunicação de aplicações IPv4 com *host* somente IPv6			X	X
BIS	Não	Não (*pool* de endereços IPv4 privativos podem ser utilizados)	*Host*	Não	Permite a comunicação de aplicações IPv4 com *host* somente IPv6			X	X
SOCKS64	Não	Não	*Site*	Não	Permite aplicações IPv4 a comunicação com nós apenas IPv6		X	X	X

Tabela 23 – Comparação entre os diversos mecanismos de transição.

Capítulo 6 - POSICIONAMENTO DO IPv6 NO CENÁRIO MUNDIAL

6.1. Introdução

Pode-se dizer, com certeza, que o protocolo IPv6 não é apenas algo teórico, mas, sim, uma tecnologia em estágio bastante avançado e com enorme potencial comercial para o futuro da Internet.

A razão disso é que muitas empresas se juntaram e montaram um fórum, sem fins lucrativos, denominada IPv6 Fórum (www.ipv6forum.com), com a missão de disseminar as vantagens do protocolo IPv6 e as suas potencialidades, incentivando o seu desenvolvimento ao redor do mundo. A lista dessas corporações envolvem fabricantes de equipamentos de rede, institutos de pesquisas, universidades, operadoras de telecomunicações, consultorias, ISPs etc.

As metas impostas pelo IPv6 Fórum exigem esforços da comunidade acadêmica e empresas do setor de tecnologia, pressionando as organizações de normalização para acelerar o processo de definição e padronização por completo do protocolo IPv6.

6.2. IPv6 Fórum

O IPv6 Fórum não é responsável pelo desenvolvimento do padrão IPv6, tarefa esta de responsabilidade do IETF. Entre os principais objetivos do IPv6 Fórum podem-se destacar:

- estabelecer metas de arquitetura aberta para o IPv6 através do fórum internacional;
- compartilhar o conhecimento a respeito do IPv6 entre os seus membros;
- desenvolver novas aplicações baseadas em IPv6 e soluções globais;
- promover a interoperabilidade entre as diversas implementações do IPv6;
- alcançar a qualidade de serviço fim-a-fim exigida pelas novas aplicações;
- minimizar e resolver assuntos relativos que criam barreiras para o desenvolvimento do IPv6.

Atualmente, podem-se identificar cinco grandes regiões no que se refere a como está o desenvolvimento do IPv6 em nível mundial.

a) Região da Ásia

Nesta área, devido ao grande número de usuários, o impacto da falta de endereços foi mais sentido. Dessa forma, a pressão para encontrar soluções alternativas foi muito grande, principalmente por parte do governo japonês com os projetos WIDE (www.v6.wide.ad.jp), KAME (www.kame.org) e TAHI (www.tahi.org).

b) Região da Europa

A questão da mobilidade e do desenvolvimento de novos padrões de *wirelles* pelas operadoras de telecomunicações é uma das prioridades da industria desta região. O ETSI (*European Telecommunications Standards Institute*) e o IPv6 Fórum estabeleceram um acordo de cooperação para promover o IPv6.

c) Região da América do Norte

Muitas atividades referentes à padronização, ao desenvolvimento e a testes do IPv6 tiveram origem nessa região. Muitas dessas atividades foram criadas pelo *backbone* de testes IPv6, podendo ser vistas em *6Bone* (www.6bone.net). Outras entidades têm forte presença nessa área, como a participação do 6REN (www.6ren.net) coordenando a iniciativa do IPv6 em institutos de pesquisa e redes educacionais, e do Freenet/Viagénie (www.freenet6.net) e (viagenie.qc.ca), estabelecendo túneis automáticos com vários centros de pesquisa e empresas.

O *backbone* da rede *6Bone* foi criado pelo grupo de trabalho IPng da IETF, com o objetivo de alavancar uma série de testes de implementação do protocolo IPv6 nas diversas plataformas e sistemas operacionais, à semelhança do que acontece com a rede internacional *MBone* para testes *multicast* e *QBone* para teste de qualidade de serviço.

Além de realizar testes, a rede *6Bone* pretende servir de ponto de partida para a implementação do protocolo na rede mundial. Cabe ressaltar que o *6Bone* não pretende impor quaisquer políticas relacionadas com o fornecimento de acesso à Internet com ISPs (*Internet Service Providers*) ou com a sua hierarquia.

Atualmente, a rede *6Bone* consiste numa rede virtual que permite o transporte de pacotes IPv6, funcionando sobre a rede física da Internet baseada no IPv4. A rede é composta por ilhas IPv6 que suportam diretamente o protocolo e que se comunicam entre si através de ligações virtuais ponto a ponto (túneis). As máquinas que realizam estas ligações ponto a ponto executam um sistema operacional com suporte para IPv6, utilizam protocolos de roteamento adequados à nova versão e suportam a realização de túneis IPv6 em IPv4.

Essa rede é independente da organização IETF, sendo um projeto informal de colaboração entre instituições situadas por todo o mundo. As atividades do *6Bone* fazem, no entanto, parte dos esforços realizados pelo grupo de transição para IPv6 da IETF (Ngtrans).

Desde então, tem havido crescimento linear, englobando aproximadamente 51 instituições no seu *backbone*, aos quais se encontram ligadas cerca de 320 ilhas IPv6 situadas em 39 países.

6.3. *6Bone*

O *6Bone* (www.6bone.net) é estruturado como uma rede hierárquica de três níveis conforme mostrado a seguir [6].

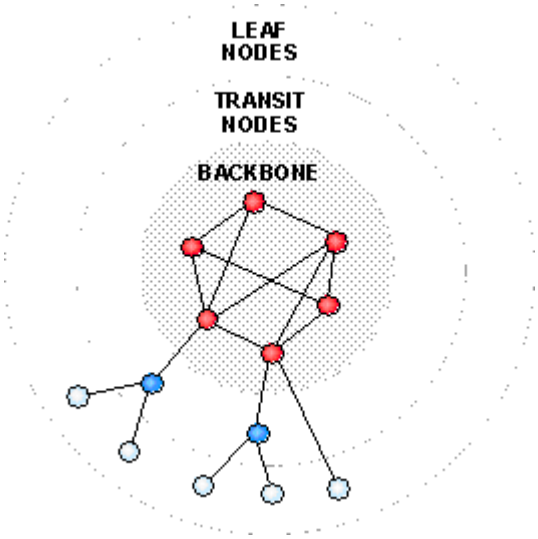


Figura 34 – Estrutura hierárquica do *6Bone*.

O *backbone* central é composto de uma série de redes IPv6 sobre os túneis IPv4 (e algumas ligações diretas) que interconectam os nós do *backbone*, delegando o endereçamento IPv6, de forma hierárquica para os nós intermediários (*transit nodes*) e para os nós das pontas (*leaf nodes*).

Abaixo, a taxa de crescimento do *6Bone* e número de nós interligados [6].

Ano	Número de nós 6Bone
Julho 1997	150
Dezembro 1997	203
Março 1998	240
Agosto 1998	302
Dezembro 1998	332
Março 1999	361
Julho 1999	412
Janeiro 2000	505
Novembro 2001	1015

Tabela 24 - Taxa de crescimento do *6Bone*.

Todas as instituições pertencentes ao *6Bone* possuem o prefixo 3ffe::/16, utilizado para testes e com a atribuição de um prefixo com 24 bits de comprimento para as instituições interligadas diretamente no *6Bone*.

Instituição	Prefixo de teste	Instituição	Prefixo de teste
CSELT/IT	3FFE:1000::/24	SWITCH/CH	3FFE:2000::/24
DIGITAL-CA/US	3FFE:1200::/24	STUBA/SK	3FFE:2200::/24
UNI-C/DK	3FFE:1400::/24	INR/RU	3FFE:2400::/24
UO/US-OR	3FFE:1500::/24	NLNET/NL	3FFE:2500::/24
NUS-IRDU/SG	3FFE:1600::/24	SMS/FI	3FFE:2600::/24
MREN/US-IL	3FFE:1700::/24	ERA/SE	3FFE:2700::/24
NTT-ECL/JP	3FFE:1800::/24	VBNS/US	3FFE:2800::/24
3COM/US-CA	3FFE:1900::/24	SPRINT/US	3FFE:2900::/24
CAIRN/US	3FFE:1A00::/24	UIO/NO	3FFE:2A00::/24
UL/PT	3FFE:1B00::/24	RNP/BR	3FFE:2B00::/24
MERIT/US-MI	3FFE:1C00::/24	BT-LABS/UK	3FFE:2C00::/24

Tabela 25 -Instituições que fazem parte do *6Bone*.

A rede *6Bone* é atualmente um dos pilares mais importantes no desenvolvimento do protocolo IPv6, contando com grande número de participantes, e será certamente o ponto de partida de transição do protocolo para a atual Internet.

d) Região da Rússia

Foi desenvolvido o *FREEnet (Rússia-wide academic and research network*), com forte relacionamento com o IPv6 Fórum, com o objetivo de estabelecer a comunidade russa de usuários de IPv6 e prover soluções de serviço para o novo protocolo.

e) Resto do mundo

Nessa área, os países que possuem alguma projeção internacional em trabalhos com o IPv6 são Coréia, Índia, Austrália, Singapura e México.

6.4. *Br6Bone* da RNP

O Brasil está participando destas pesquisas através da iniciativa da RNP (Rede Nacional de Pesquisa) com o projeto chamado *Br6Bone* (www.6bone.rnp.br), empreendido pelo LCT - Laboratório de Configuração e Testes da RNP. Esse projeto foi iniciado em janeiro de 1998 com a alocação do prefixo 3FFE:2B00::/24**,** conforme tabela 24, por parte do *6Bone*. A primeira conexão foi estabelecida por um túnel e efetivada em março de 1998 com a Cisco System, nos EUA, e logo em seguida, no mesmo ano, com a NTT (*Nippon Telephone and Telegraph*) do Japão.

Hoje a RNP conta com cinco túneis internacionais e 25 pontos de presença nacionais instalados em universidades e institutos de pesquisa, relacionados a seguir.

Sigla	Instituição
ATENTO	Atento Brasil S/A
CPQD	CPqD - Centro de Pesq. e Desenvolvimento Telecom
CEFET	Centro Federal de Educação Tecnológica da Bahia
CCE-USP	Universidade do Estado de São Paulo
DIVEO	Diveo Brazil
FIPP	Faculdade de Informática de Presidente Prudente
IPT	Instituto Pesquisas Tecnológicas
LNCC	Laboratório Nacional de Computação Científica
POP-MG	Ponto de presença - Minas Gerais
POP-RN	Ponto de presença – Rio Grande do Norte
PoP-CE	Ponto de presença – Ceara
PoP-RS	Ponto de presença – Rio Grande do Sul
PoP-PA	Ponto de presença – Pará
POP-SE	Ponto de presença – Sergipe
PEGASUS	Rede Pegasus, Pegasus Network Brazil
RNP	Rede Nacional de Pesquisa
TECPAR	Instituto de Tecnologia do Paraná
UCB	Universidade Católica de Brasília
UNICAMP	Universidade Estadual de Campinas
UNB	Universidade de Brasília
UCPEL	Universidade Católica de Pelotas
UFBA	Universidade Federal da Bahia
UFMA	Universidade Federal do Maranhão
UFRJ	Universidade Federal do Rio de Janeiro
UNISINOS	Universidade do Vale do Rio dos Sinos

Tabela 26 – Instituições ligadas com IPv6 ao *Br6Bone.*

A RNP está preparada para aceitar o estabelecimento de túneis e a atribuição de prefixos a instituições que pretendam participar do projeto IPv6, respeitando as atuais regras de atribuição propostas e contidas em (www.6bone.rnp.br).

6.5. Posicionamento do IPT no contexto do *Br6Bone*

O IPT, ao longo desse trabalho, está participando e fazendo parte do *Br6Bone* com a rede 3ffe:2b00:103::/48, endereço este solicitado e cedido oficialmente, em maio de 2002, pela RNP, conforme apresentado no Anexo 7.

Capítulo 7 – MODELO PROPOSTO

7.1. Ambiente piloto

Os objetivos práticos a serem alcançados, a partir da montagem do ambiente piloto para testes, são:

- estudar as vantagens do protocolo IPv6 na Rede IPTNet, visando à substituição do endereçamento IPv4 e do protocolo NAT utilizando endereços privativos;
- acompanhar a evolução dos novos protocolos da Internet e projetos afins;
- Implantar uma rede piloto IPv6 e promover a sua devida ligação com o *Br6Bone*;
- avaliar novas aplicações em IPv6;
- disponibilizar serviços IPv6 à comunidade e parcerias com institutos e empresas;
- colaborar com o desenvolvimento de mecanismos e procedimentos de transição IPv4-IPv6;
- comparar o protocolo IPv4 juntamente com o NAT em relação ao IPv6 em ambientes de rede utilizando o infra-estrutura do *backbone Gigabit Ethernet* da rede IPTNet.

Para a realização dos testes com o protocolo IPv6, foram montados basicamente dois ambientes. O primeiro, de laboratório sem conexão com a Internet, conforme Figura 35, teve como objetivo a capacitação em relação aos diversos sistemas operacionais utilizados. O segundo, de produção, utilizando a infra-estrutura da rede IPTNet, visou à implantação de uma rede piloto IPv6 através de um túnel IPv6-IPv4 com a RNP, conforme Figura 39.

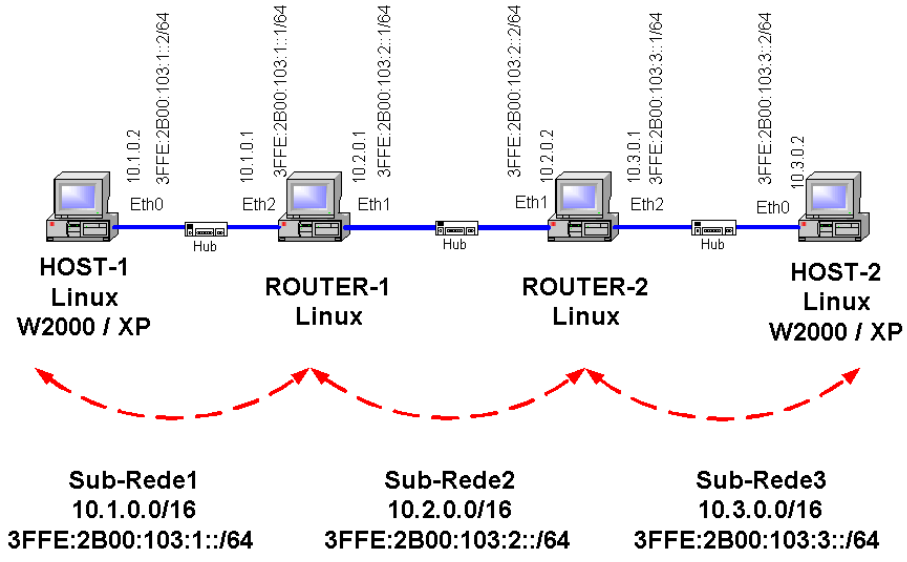


Figura 35 – Ambiente de laboratório sem conexão externa.

7.2. Componentes do Ambiente de Testes

7.2.1. *Hardware*

a) *Host*-1 (Compaq Proliant 7000).
Pentium II Xeon 450 MHz.
256 MB RAM.
Controladora Smart Array 3100ES.
2 discos SCSI de 2GB.
1 placa de rede Compaq NC 3131 *Fast Ethernet* PCI 64 bits.

b) *Router*-1 (Compaq Proliant 500).
Pentium 120 MHz.
64 MB RAM.
Controladora SCSI integrada.
1 disco SCSI de 4 GB.
2 placas de rede 3Com Etherlink XL 10/100 PCI.

c) *Router*-2 (Compaq Proliant 300).
Pentium 120 MHz.
64 MB RAM.
Controladora SCSI integrada.
1 disco SCSI de 4 GB.
2 placas de rede 3Com Etherlink XL 10/100 PCI.

d) *Host*-2 (Compaq Proliant 1600).
Pentium III 800 MHz.
132 MB RAM.
Controladora Smart 2SL.
2 discos SCSI de 2 GB.
1 placa de rede Netelligent 10/100 TX UTP PCI.

e) Hubs Synoptics 2813 *Ethernet*.

7.2.2. Sistemas Operacionais

- Windows 2000 com SP1.
- Windows XP Professional.
- Linux (RedHat 7.2) com kernel 2.4.

7.2.3. Ferramentas de monitoração

- Baseadas em Windows – Ethereal, Analyser version 2.2 1997/2002 NetGroup Politécnico di Torino e Network Monitor /System Monitor.
- Baseadas em Linux – Ethereal.

7.3. Comparativo entre os protocolos IPv4 e IPv6

Para a comparação dos protocolos, inclusive com o NAT, foram utilizados o ambiente piloto e a infra-estrutura do *backbone* da rede IPTNet, avaliando-se as seguintes métricas:

- tempo de *Round Trip Time* (RTT): o intervalo de tempo entre a solicitação de algum serviço de rede e uma resposta ao pedido, medido através dos comandos “ping” e “ping6”. Ao analisar o tempo de RTT, estar-se-ão medindo também as medidas de variação de retardo (latência) e podem-se verificar eventuais perdas de pacotes.
- taxa de transferência efetiva (Kb/s), medido com o programa de FTP.

O tempo de RTT é composto dos seguintes itens:

- tempo de transmissão: basicamente depende da velocidade do *link* entre as duas máquinas;
- tempo de processamento: depende da velocidade do processador da máquina e do tamanho dos cabeçalhos a serem processados. Esse tempo é maior no IPv6 (40 bytes) quando comparado com o IPv4 (20 bytes), ambos sem opções;
- tempo de propagação: tempo necessário para que o sinal possa se propagar pelo meio físico através da rede. No caso de testes em laboratório, onde a distância dos cabos é curta, esse tempo é desprezível.

Os usuários de aplicativos de multimídia exigem variação mínima no retardo nos pacotes, onde o retardo deve ser constante para vídeo e voz. As variações de retardo, denominadas *jitter*, causam interrupções na qualidade de voz e vídeo e saltos nos fluxos de vídeo.

A variação do tamanho dos pacotes é um requisito fundamental no desempenho de uma rede, haja vista que pacotes pequenos são menos eficientes quando comparados a pacotes com *payload* maiores, maximizando a quantidade de dados úteis de aplicativos enviados em comparação com o cabeçalho.

A análise dos tamanhos dos pacotes auxilia na verificação do desempenho de um segmento de rede. Por exemplo, um número excessivo de pacotes *Ethernet* com tamanho muito pequenos (menores que 64 bytes) pode indicar um número excessivo de colisões em andamento, causado por uma porta ou placa de rede com problemas.

Nos testes realizados nesse trabalho, somente os serviços estritamente necessários foram carregados, sendo que em cada experimento foram enviados 10 (dez) pacotes, com tamanhos de 64 bytes (mínimo) e 65.500 bytes (máximo), analisando-se os tempos médios em cada teste.

Os sistemas operacionais utilizados foram o Windows 2000 Server, Windows XP e o Linux com a distribuição RedHat 7.2 com kernel 2.4. Os sistemas possuem suporte aos dois protocolos IPv4 e IPv6, analisando-se aspectos relacionados à integração que foi efetivada de maneira fácil e gradual, sem apresentar maiores problemas.

No ambiente de laboratório, para os experimentos de comparação, as máquinas possuem suporte aos protocolos IPv4 e IPv6, separados por *hubs* com segmentos *Ethernet*, com a finalidade de poder colocar o analisador em cada segmento. Foi alocada uma máquina para a captura dos pacotes, analisando-se o protocolo IPv4, IPv6 encapsulado no IPv4 e finalizando o IPv6.

A seguir, uma tabela com valores teóricos do *overhead* gerado pelo encapsulamento dos protocolos IPv4 e IPv6 no *frame Ethernet*, verificando aspectos de capacidade de carga do *payload* x cabeçalho, em cada situação analisada do trabalho.

Protocolo	**IPv4**	**IPv6**	**IPv6 encapsulado no IPv4**
Ethernet header (sem TAG)	14	14	14
Ethernet payload	1500	1500	1500
IP header (sem opções)	20	40	20
IP payload	1480	1460	1480
Header			40
Payload			1440
Overhead	1,35%	2,74%	4,16%

Tabela 27 – *Overhead* dos protocolos IPv4 e IPv6 no *frame Ethernet*.

As máquinas com função de roteamento IPv6 podem ser configuradas para realizar a autoconfiguração de endereços IPv6 através de solicitações e anúncio de prefixos, através do serviço chamado RADVD (*Router Advertisement Daemon*), configurado em etc/radvd.conf. Esta possibilidade vem trazer benefícios para as novas tecnologias de redes móveis, sendo possível a uma máquina configurar o seu prefixo de rede automaticamente sempre que for ligada à rede.

Numa máquina com o sistema operacional Linux foi instalado o serviço de DNS com suporte para endereços IPv6, sendo realizada a resolução de nomes do domínio "ip6.ipt.br". A raiz para os domínios invertidos do IPv6 é "ip6.int", em substituição do "in-addr.arpa" do IPv4. A parte restante é o prefixo invertido, à semelhança do que ocorre no IPv4.

Foram alocadas também duas máquinas para estabelecer túneis com a Freenet6 em ambiente Windows 2000, e outra para estabelecer um túnel com a RNP em ambiente Linux, utilizando o roteamento manual em detrimento ao protocolo de encaminhamento BGP4+, recomendado pelo *6Bone*. Não está disponível um roteador dedicado com suporte ao IPv6, prevendo-se para uma próxima fase juntamente com outros serviços básicos de rede, a saber: colocar em operação um servidor Web, FTP e correio eletrônico com IPv6, informações sobre o protocolo IPv6, ajudas de instalação para algumas plataformas, resultados da evolução do grupo de trabalho IPng da IETF, etc. Isso pode ser um complemento importante da bancada de testes e contribuir para a divulgação do protocolo IPv6.

7.4. Configuração dos Sistemas Operacionais

7.4.1. Configuração do IPv6 - Linux

O Linux é um sistema operacional, multiusuário e multitarefa, de livre distribuição, disponível para equipamentos Intel e compatíveis, Motorola, Digital Alpha, Sparc, Mips e PowerPC, entre outros. É uma implementação aderente ao POSIX (*Portable Operating System Interface*), ou seja, segue as indicações do IEEE para sistemas abertos e portabilidade.

O núcleo do Linux não utiliza código proprietário de qualquer espécie, e a maior parte de seu desenvolvimento feita sob o projeto GNU da *Free Software Foundation*, o que torna obrigatório que binários e fontes sejam distribuídos conjuntamente.

Muito mais do que isso, o Linux vem se consolidando cada dia mais como um sistema para plataforma Intel, que veio realmente para ficar e que conquista mais e mais adeptos, ao contrário de outros como o Solaris versão Intel ou MacOS da Apple. Talvez o principal fator que tenha levado a esse crescimento e conquistado tantas pessoas seja o fato de que ele cresceu juntamente com a Internet.

Em meados dos anos 90, por volta de 92, um estudante finlandês de computação, chamado Linus Torvalds começou a criar um sistema operacional chamado Linux. O grande mérito de Linus foi disponibilizar o código fonte do kernel para toda a comunidade acadêmica. Atualmente, o Linux não é apenas um sistema operacional de uso acadêmico, mas que tende a ganhar uma grande fatia do espaço no mundo comercial.

A escolha da distribuição RedHat deve-se ao fato de ser uma distribuição homologada pelos principais fabricantes, incluindo a Compaq/HP, por apresentar total compatibilidade de *hardware* nos equipamentos de testes e incluir o suporte nativo para a pilha IPv6.

Na instalação do Linux com o RedHat, o módulo pode ser carregado manualmente ou recompilado no kernel, de maneira que as interfaces de rede sejam configuradas automaticamente com o endereço IPv6 *link-local*. Para a comunicação entre nós IPv6 através de um túnel IPv4, são necessários os seguintes arquivos de comandos do Linux, conforme abaixo descrito.

7.4.1.1. Configuração das interfaces.

Host-1
#insmod ipv6
#ifconfig eth0 add 3ffe:2b00:103:1::2/64

Router-1
#insmod ipv6
#ifconfig eth1 add 3ffe:2b00:103:2::1/64 (configurado no roteamento IPv6)
#ifconfig eth2 add 3ffe:2b00:103:1::1/64
#ifconfig sit0 up
#ifconfig sit0 tunnel ::10.2.0.2
#ifconfig sit1 up
#ifconfig sit1 inet6 add 3ffe:2b00:103:2::1/126

Router-2
#insmod ipv6
#ifconfig eth1 add 3ffe:2b00:103:2::2/64 (configurado no roteamento IPv6)
#ifconfig eth2 add 3ffe:2b00:103:3::1/64
#ifconfig sit0 up
#ifconfig sit0 tunnel ::10.2.0.1
#ifconfig sit1 up
#ifconfig sit1 inet6 add 3ffe:2b00:103:2::2/126

Host-2
#insmod ipv6
#ifconfig eth0 add 3ffe:2b00:103:3::2/64

Em *Host-1* a primeira linha carrega o módulo IPv6 e a segunda linha mostra como associar um endereço IPv6 na interface eth0.

Em *Router-1* as quarta e quinta linhas criam uma interface virtual denominada "sit0" para a criação do túnel da ponta remota associando o endereço IPv4 da extremidade do túnel. As sexta e sétima linhas criam outra interface virtual "sit1" para a configuração local do túnel com os dados IPv6 passados pela outra ponta do túnel.

As configurações de *Router-2* e *Host-2* são similares às anteriores.

7.4.1.2. Configuração de Roteamento

Host-1
#route –A inet6 add 3ffe::/16 gw 3ffe:2b00:103:1::1 dev eth0

Router-1
#echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
#route -A inet6 add 3ffe::/16 gw 3ffe:2b00:103:2::2 dev sit1

Router-2
#echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
#route -A inet6 add 3ffe::/16 gw 3ffe:2b00:103:2::1 dev sit1

Host-2
#route –A inet6 add 3ffe::/16 gw 3ffe:2b00:103:3::1 dev eth0

Em *Host-1*, é apresentado o comando para o roteamento padrão no Linux, utilizando o backbone de testes com o prefixo (3ffe::/16).

Em *Router*-1 a primeira linha habilita o repasse dos pacotes entre as interfaces e a segunda linha, a rota padrão apontando para a outra extremidade do túnel.

As configurações de *Router*-2 e *Host*-2 são similares às anteriores.

7.4.2. Configuração IPv6 - Microsoft

7.4.2.1 Configuração IPv6 no Windows 2000 Server

O Windows, sistema operacional criado e desenvolvido pela Microsoft, é um sistema fechado e proprietário, ou seja, não é possível modificá-lo. Em compensação, é largamente utilizado e, no IPT, cerca de 70% dos computadores utilizam o Windows.

Existe um projeto chamado Microsoft Research IPv6, desenvolvido pela Microsoft em conjunto com a USC (*University of Southern California*). Como o projeto ainda está em fase de desenvolvimento, a Microsoft optou por disponibilizar os códigos fonte da implementação do IPv6 no Windows, permitindo a colaboração de interessados no desenvolvimento do IPv6 para Windows.

Para obter esses códigos, basta acessar a página (http://research.microsoft.com/msripv6) preencher um formulário e baixar os arquivos. A implementação do IPv6 no Windows possui suporte a Windows NT, 2000, XP e na plataforma .NET [2].

Para o suporte ao Windows 95/98/ME/NT, existem versões pagas, como o Trumpet (http://www.trumpet.com.au/ipv6.htm), e versões gratuitas como pacote Toolnet6 da empresa Hitachi (http://www.hitachi.co.jp/Prod/comp/network/pexv6-e.htm), homologado apenas para algumas placas de rede.

O Windows possui suporte ao IPv6 para os seguintes serviços: Internet Explorer, Telnet, FTP e Microsoft Network Monitor. No final de 2002, a Microsoft estará disponibilizando suporte ao IIS, Microsoft Media Server e RPC.

A seguir, descreve-se a seqüência para o processo de instalação do IPv6 para o Windows 2000:
- instalar o S*ervice Pack* SP1;
- criar um diretório C:>\IPv6Kit;
- fazer o download do arquivo tpipv6.exe para o diretório C:>\IPv6Kit;
- em C:>\IPv6Kit, executar o arquivo setup.exe;
- adicionar o protocolo IPv6;
- reiniciar o sistema.

Host-1
C:\>ipv6 adu 4/3ffe:2b00:103:1::2
C:\>ipv6 rtu 3ffe::/16 4/3ffe:2b00:103:1::1 (gateway)

Host-2
C:\>ipv6 adu 4/3ffe:2b00:103:3::2
C:\>ipv6 rtu 3ffe::/16 4/3ffe:2b00:103:3::1 (gateway)

A primeira linha mostra como associar um endereço IPv6. Observar que o número 4, que aparece antes do endereço IPv6, é o da interface alocado pelo Windows, podendo variar de acordo com o número de interfaces instaladas na máquina, da mesma forma que ocorre no Linux com eth0, eth1 etc. A segunda linha configura a rota padrão.

7.4.2.2 Configuração do Windows XP

Para a configuração da interface no Windows XP, devem-se executar os mesmos comandos do Windows 2000, conforme item acima, exceto no carregamento do protocolo IPv6, devendo ser executados os seguintes comandos:
- entrar no prompt do DOS;
- digitar C:>ipv6 install.

7.4.3. Configuração do túnel com a RNP em ambiente Linux

Para estabelecer um túnel com a RNP, é necessário o preenchimento do formulário, conforme Anexo 7, e obter a autorização do comitê gestor. A seguir, a configuração do túnel do IPT com a RNP, em detalhes na Figura 39.

```
#ifconfig eth0 add 200.18.53.133 net 255.255.255.244 gw 200.18.53.129
#ifconfig eth1 add 3ffe:2b00:103:1::133/64
#echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
#ifconfig sit0 up
#ifconfig sit0 tunnel ::200.136.100.141
#ifconfig sit1 up
#ifconfig sit1 inet6 add 3ffe:2b00:500:2F::2/126
#route -A inet6 add 3ffe:://16 gw 3ffe:2b00:500:2F::1 dev sit1
```

7.4.4. Configuração do túnel com o Freenet6 em ambiente Windows 2000

Para criar um túnel com a rede Freenet6, deve-se acessar o seguinte *site* http://www.freenet6.net, possuindo suporte para os seguintes sistemas operacionais: FreeBSD, Windows, Linux, Solaris 8, NetBSD e OpenBSD.

Para realizar o tunelamento com o Freenet6, foi utilizado o programa TSPC (*Tunnel Server Protocol Client*), através dos seguintes passos:

- instalar o Windows 2000 com o Service Pack 1;
- instalar a pilha IPv6;
- fazer o download do arquivo (freenet6-0.7a.zip) no *site* Freenet6;
- instalar o módulo cliente do Freenet6;
- criar a conta de usuário para o túnel autenticado no *site* Freenet6;
- configurar o arquivo tspc.conf com o usuário e número IP;
- executar o comando C:\>ctspc –vf tspc.conf;
- testar a conectividade com o IPv6;

7.4.5. Configuração do túnel com o Freenet6 em ambiente Linux.

- instalar o RedHat 7.2 com kernel 2.4;
- instalar o modulo de IPv6 com o comando insmod IPv6;
- fazer o download do arquivo (tar xfvz freenet6-0.xx.tgz) no *site* Frrenet6;
- instalar o módulo cliente do Freenet6 com o comando make install target=linux installdir=/opt/tspc;
- criar o usuário para o túnel autenticado;
- configurar o arquivo tspc.conf;
- executar o comando #./tspc –vf tspc.conf no diretório /opt/tspc/bin;
- testar a conectividade com o IPv6.

7.5. Experimentos

7.5.1. Ambiente de Laboratório

Com base na Figura 35, a primeira etapa dos testes, os experimentos foram realizados utilizando apenas o protocolo IPv4, verificando-se os tempos de RTT dos pacotes originados pelo *Host*-1, passando por todas as interfaces até o destino *Host*-2.

Na segunda etapa, foi configurado o túnel IPv6-IPv4 entre as máquinas *Router*-1 e *Router*-2, sendo que as máquinas das extremidades *Host*-1 e *Host*-2 possuem o protocolo IPv6 configurado.

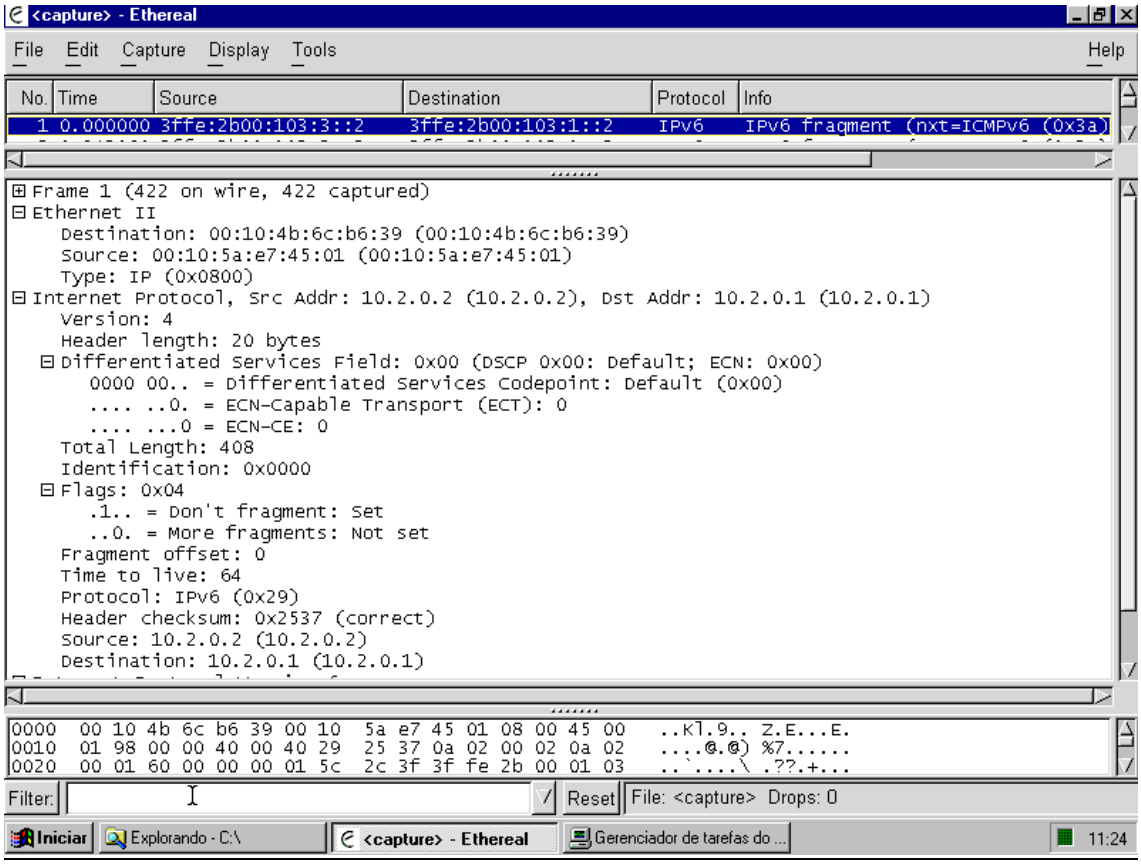
Na última fase, foi retirado o túnel IPv4-IPv6 e configurado o IPv6 em todas as máquinas, inclusive com função de roteamento, verificando-se os tempos de RTT do protocolo IPv6 fim-a-fim.

A seguir, a tabela com os resultados obtidos em cada etapa.

Tamanho dos pacotes (bytes)	**64 (mínimo)**	**65.500 (máximo)**
IPv4		
H1 → H1 (*loopback* Linux)	0.050	0.966
H1 → H2 (Linux para Windows)	0.964	109.660
IPv6 com túnel IPv4 configurado		
H1 → H2 (Linux para Windows)	1.223	119.903
IPv6		
H1 → H1 (*loopback* Linux)	0.056	0.874
H1 → H2 (Linux para Windows)	0.902	107.959

Tabela 28 – Tempos de RTT de pacotes (ms).

A seguir, um exemplo do pacote IPv6 encapsulado em IPv4.



Continua

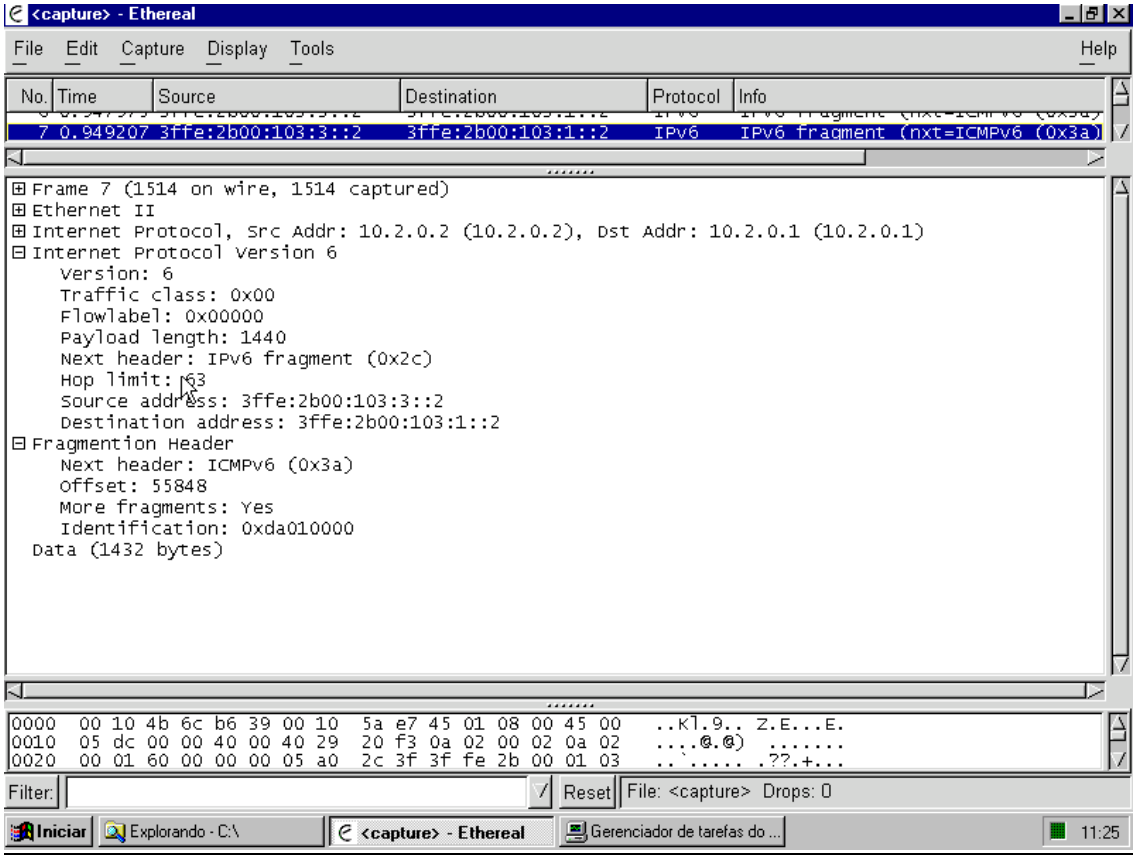


Figura 36 – Exemplo de pacote IPv6 encapsulado em IPv4.

A seguir, um exemplo do pacote IPv6.

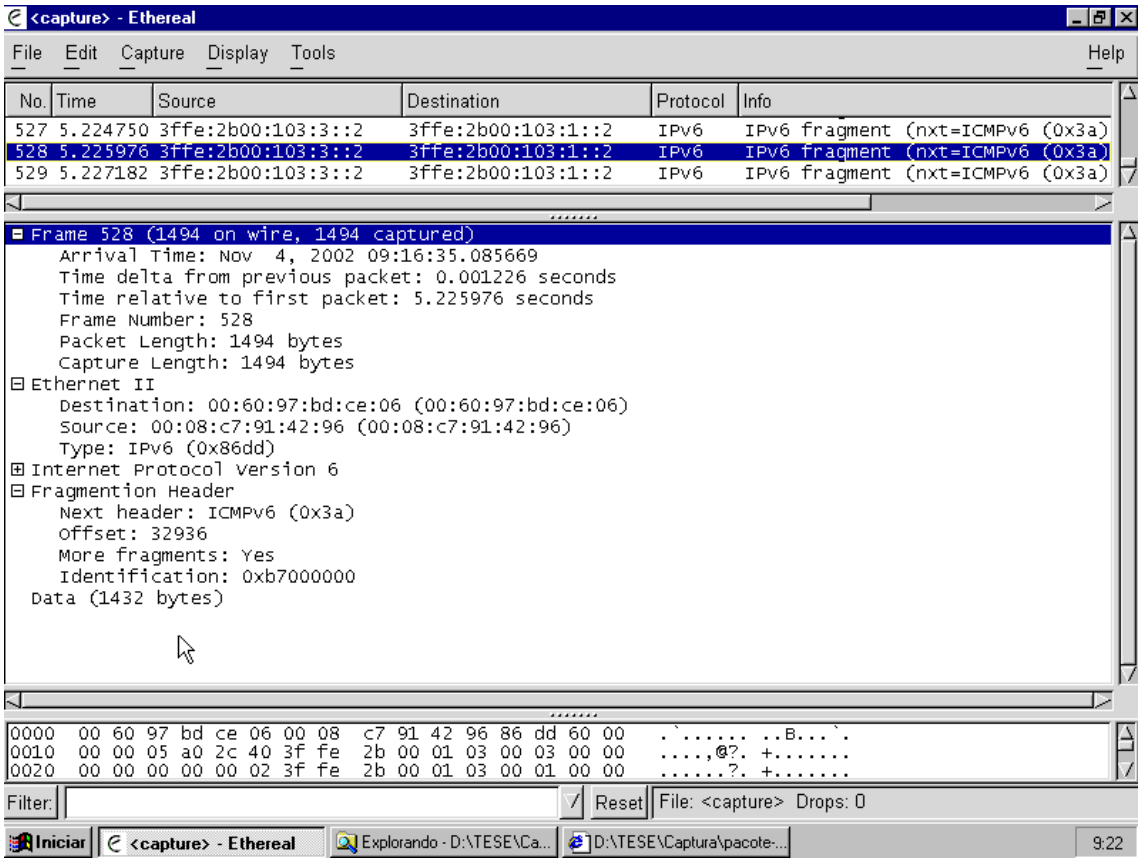


Figura 37 – Exemplo de pacote IPv6.

7.5.2. Ambiente da Rede IPTNet

7.5.2.1. Comparativo do protocolo IPv4 com endereços públicos e privativos NAT.

Para verificar a diferença de taxa de transferência gerado pelo protocolo IPv4, com endereços públicos e privativos usando NAT, foi utilizado o ambiente de produção da rede IPTNet, através do roteador de saída (Foundry 4802), realizado em final de semana com o tráfego da rede praticamente estável.

No experimento, foi usada a mesma máquina com o endereço público da DMZ (200.18.53.140) e outro com IP privativo configurado com o NAT dinâmico (10.0.1.22), verificando-se a taxa de transferência de arquivos, utilizando o serviço de FTP conectado ao servidor externo (200.9.66.90), conforme Figura 38.

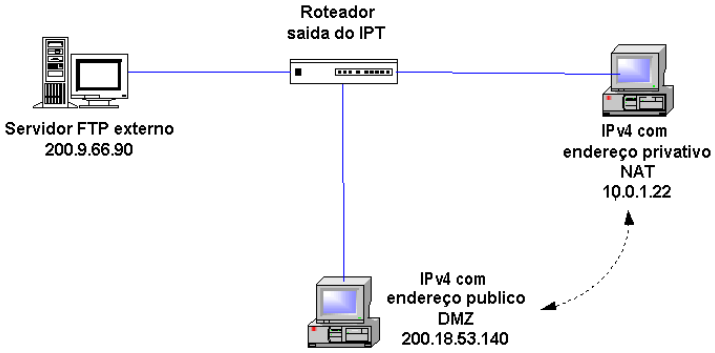


Figura 38 – Ambiente de produção com IPv4 público e privativo com NAT.

Arquivo (Kbytes)	IPv4 público (DMZ) → IPv4 público	IPv4 privativo (NAT) → IPv4 público
2.293	4,7	4,3
4.287	4,3	4,1

Tabela 29 – Taxa de transferência de arquivos com IPv4 públicos e privativos (Kbytes/s).

7.5.2.2. Túnel em produção com a RNP e com o Freenet6

A seguir, a topologia da configuração dos túneis configurados no ambiente da rede IPTNet, com os respectivos endereços em cada interface.

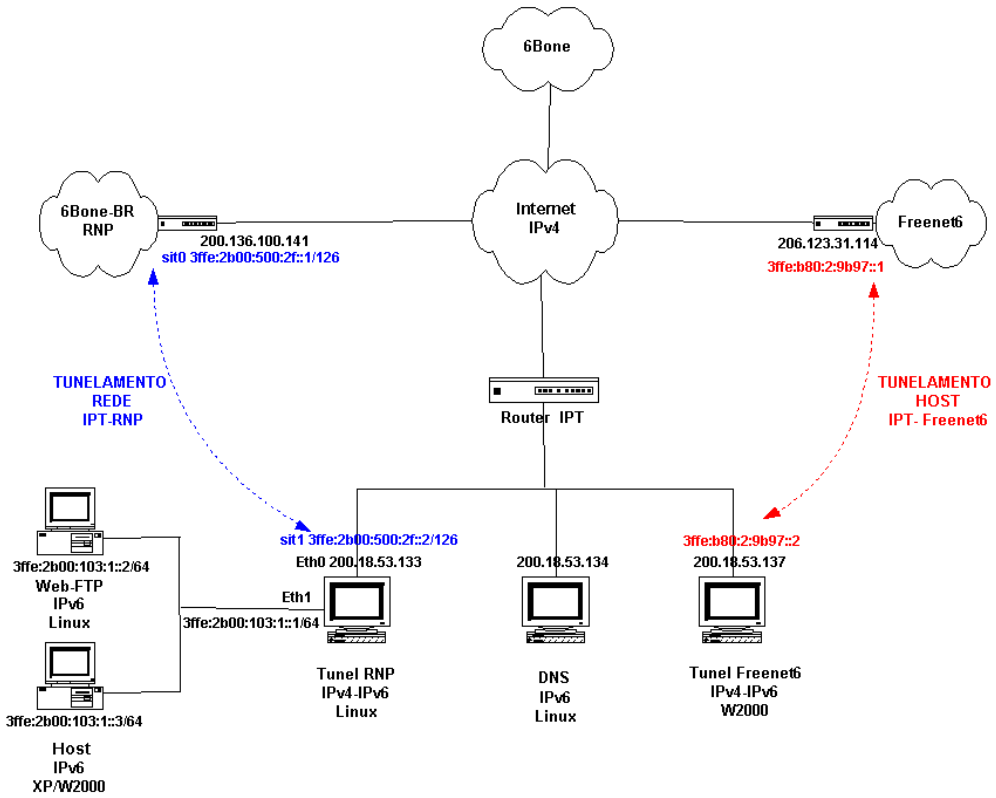


Figura 39 – Ambiente dos túneis com a RNP e a Freenet6.

7.6. Proposta de Endereçamento IPv6 na Rede IPTNet

Apresenta-se uma proposta de alocação para o endereçamento IPv6 a ser utilizado no IPT, contendo o prefixo 3FFE:2B00:0103::/48, alocado pela RNP. Com esse esquema, poder-se-iam endereçar 65.536 sub-redes diferentes com prefixo de tamanho /64 disponível, ou dividir a topologia do *site* em (SLA1 e SLA2), com a possibilidade de endereçar 256 sub-redes com o prefixo /56, tendo cada uma 256 nós, conforme a seguir descrito.

Topologia pública		Topologia *site*		Local interface
16 bits	32 bits	16 bits		64 bits
TLA	NLA	SLA		Interface (EUI-64)
		SLA1	SLA2	

Divisão	**Sub-Redes**
IPTNET	3FFE:2B00:0103:0101::/56
CEF	3FFE:2B00:0103:0200::/56
DEC	3FFE:2B00:0103:0300::/56
DIMET	3FFE:2B00:0103:0400::/56
DQ	3FFE:2B00:0103:0500::/56
DME	3FFE:2B00:0103:0600::/56
DE/AJ/ASO/CCT/GQ	3FFE:2B00:0103:0700::/56
DITT	3FFE:2B00:0103:0800::/56
CENATEC	3FFE:2B00:0103:0900::/56
DITEL	3FFE:2B00:0103:0A00::/56
DEES	3FFE:2B00:0103:0B00::/56
CITEC	3FFE:2B00:0103:0C00::/56
CRH	3FFE:2B00:0103:0D00::/56
DPF	3FFE:2B00:0103:0E00::/56
DIGEO	3FFE:2B00:0103:0F00::/56
CS	3FFE:2B00:0103:1000::/56
CGP	3FFE:2B00:0103:1100::/56
SAC	3FFE:2B00:0103:1200::/56
PROGEX	3FFE:2B00:0103:1300::/56
SPDESIGN	3FFE:2B00:0103:1400::/56
PEDAGOGICA	3FFE:2B00:0103:1500::/56
	...
Reservado	3FFE:2B00:0103:FF00::/56

Tabela 30 – Proposta de endereçamento IPv6 para rede IPTNet.

Com base na delegação do endereçamento das sub-redes acima, mostra-se um exemplo de como ficaria a distribuição dos endereços da sub-rede da divisão DME, com o prefixo 3FFE:2B00:103:7::/56 (lembrar que no IPv6 cada nó da interface recebe o prefixo /64).

Endereços DME	**Departamento**
3FFE:2B00:0103:0700::/64	Térmica
3FFE:2B00:0103:0701::/64	Vazão
3FFE:2B00:0103:0702::/64	Sistemas e Controle
3FFE:2B00:0103:0703::/64	Plasma
3FFE:2B00:0103:0704::/64	Óptica
…	...
3FFE:2B00:0103:07FF::/64	Reservado

Tabela 31 – Exemplo de endereçamento IPv6 para a sub-rede DME.

7.7. Resultados dos testes comparativos

A seguir alguns resultados extraídos durante o trabalho:

a) avaliação do NAT, no ambiente de produção da rede IPTNet operando com o protocolo IPv4, comparando-se endereços privativos e endereços públicos, conforme figura 38.

Verificou-se na média o *overhead* de 7% gerado pelo NAT, na taxa de transferência de arquivos medidos com o serviço de FTP, descritos na Tabela 29.

b) avaliação inicial do protocolo IPv4, seguido do tunelamento IPv6-IPv4 e finalizando com o IPv6, conforme Figura 35 e resultados na Tabela 28.

Nos testes de *loopack,* realizados com o sistema operacional Linux, fica implícito que os resultados são relacionados somente a aspectos que envolvem a pilha de protocolos, não levando em consideração aspectos de roteamento, fragmentação ou protocolos auxiliares. Dessa forma, verificou-se que a média dos tempos de resposta do IPv6 foi 9,2% melhor do que o IPv4, mostrando que a implementação da pilha de protocolo IPv6 foi melhorada em relação ao seu antecessor IPv4.

Nos experimentos com as máquinas das duas extremidades *Host-1 e Host-2*, com o protocolo IPv4 e, em seguida, o IPv6, foi levada em consideração a questão do roteamento e da fragmentação de pacotes, e a média dos tempos de resposta foi de 1,6% a favor do IPv6.

A comunicação das duas máquinas IPv6 nas extremidades, com o túnel IPv4 configurado entre os roteadores, mostrou que a diferença das médias dos tempos de resposta foi de 9,5% mais lento em comparação ao IPv4 fim-a-fim, e 11,3% mais lento em comparação ao IPv6 fim-a-fim, devido principalmente aos tempos de processamento de encapsulamento dos pacotes.

CAPÍTULO 8 – PERSPECTIVAS E CONCLUSÃO

8.1. Perspectivas

O IPv6 apesar de apresentar conceitos do IPv4, é um protocolo totalmente remodelado, contendo novas características e funcionalidades, conforme visto no capítulo 3. Durante o trabalho, verificou-se que o IPv6 é um protocolo que se encontra num estágio avançado de padronização e presente nos principais sistemas operacionais do mercado, possuindo a grande missão de substituir o IPv4, devido ao fato deste protocolo não oferecer suporte às exigências das aplicações e tecnologias atuais.

Os principais fabricantes estão mobilizados para essa transição, pois perceberam a viabilidade e o potencial para a geração de novos negócios. A partir do momento que, as ilhas IPv6, começarem a se expandir com a implantação de *Intranets* nas corporações e estiverem operando em conjunto com os roteadores configurados com o IPv6, pode-se afirmar que o ciclo de vida do IPv4 tenderá a diminuir, como aconteceu com várias outras tecnologias relacionadas à Tecnologia da Informação ao longo do tempo.

Com a massificação do protocolo IPv6 estarão conectados dispositivos fixos e móveis, com conexões *wireless*, transmissão de voz e dados via celular, comunicação em banda larga e conectividade global, tornando a Internet o meio mais importante para o comércio, para as comunicações, e para a sociedade da informação digital.

Além disto, o aumento da popularidade da Internet reforça ainda mais esta idéia, uma vez que não suportará a grande demanda de equipamentos e usuários que ainda irão conectar-se, como é o caso dos dispositivos móveis e redes domésticas com o uso de *home apliances*. Os provedores de acesso (ISP) terão um papel fundamental nesse processo de disseminação do IPv6, oferecendo um melhor nível de serviço para os usuários que, de posse de um ou mais endereços IPv6 globais, poderão disponibilizar seus próprios servidores contendo suas páginas pessoais, compartilhar os dados pessoais com os PCs domésticos e obter uma maior interação com novos serviços.

No médio prazo, com o crescimento da infra-estrutura oferecida pelo *6bone*, um número significativo de redes IPv6 deverá integrar-se a seu *backbone*, como o caso do IPT, consolidando a fusão das tecnologias de computação e comunicação através da Internet. Em 2002, aproximadamente 35 países participavam oficialmente do *6Bone*/NGTrans/IETF, incluindo o Brasil, demonstrando forte interesse por parte dos países e instituições participantes.

8.2. Conclusão

Durante a fase de implantação e testes do IPv6 no IPT, realizados com os sistemas operacionais Linux e Windows, verificou-se o crescente número de *sites*, contendo os serviços básicos de Web, FTP e E-mail com suporte IPv6, demonstrando a real visibilidade e integração dos dois protocolos, presentes nos sistemas avaliados.

A implementação do piloto IPv6 na rede IPTNet ocorreu de forma transparente, com a criação de uma VLAN exclusiva para o IPv6, efetivada numa máquina dedicada, realizando o tunelamento direto com a RNP. A próxima etapa é a configuração do túnel diretamente no roteador de saída do IPT, realizando o roteamento IPv6 das sub-redes conforme proposto na Figura 35, sem alterar a configuração IPv4 atual, devendo apenas compatibilizar a configuração dos *hosts* clientes com suporte ao IPv6.

A utilização do NAT na rede IPTNet propiciou, ao longo de vários anos, uma solução para o problema de escassez de endereços e de acessibilidade dos 1.500 *hosts* existentes, porém introduziu algumas limitações, que comprometem o funcionamento de protocolos/aplicações visto na Tabela 22, e gerando um maior custo de administração e gerenciamento. Com o IPv6 as soluções de NAT devem ser repensadas, avaliando-se os recursos e aplicações que serão usados na rede e o nível de segurança desejado.

Com o IPv6, o papel do NAT deverá ser substituído de um tradutor de endereços públicos e privativos, para um agente conversor de protocolo de IPv4 para IPv6, sendo um elemento importante durante a fase de transição, realizando a comunicação de aplicações IPv4 nativas com aplicações IPv6 nativas.

Dessa forma, a transição no IPT estará ocorrendo em paralelo com os principais serviços de rede atuais, oferecendo aos usuários as duas opções de acessibilidade com suporte de pilha dupla. O real sucesso do IPv6 e a motivação da migração da rede IPTNet para este novo protocolo, dependem também do esforço da instituição e da comunidade em geral no desenvolvimento das novas aplicações com características diferenciadas das existentes, e que, tendem a ser “portadas” para este novo protocolo, explorando todas as potencialidades que o IPv6 tem para oferecer.

Os testes comparativos de tempo de RTT do protocolo IPv6 em relação ao IPv4 não foram significativos em ambiente de laboratório. Os experimentos foram realizados em máquinas com sistemas operacionais configurados com pilha dupla e com tunelamento, fazendo com que os roteadores diminuam o desempenho final. Dessa forma, acredita-se que as redes IPv6 nativas implementadas com roteadores dedicados, no ambiente da Internet, devam melhorar os valores obtidos, utilizando-se o esquema de endereçamento totalmente hierárquico, fragmentação dos seus pacotes somente pela origem e pelo uso do *flow label* oferecendo parâmetros de qualidade de serviço, otimizando a performance global.

Cabe ressaltar que o roteador IPv6 analisa apenas o cabeçalho fixo e, caso exista a necessidade de alguma informação adicional, este será tratado e ajustado via cabeçalhos de extensão, gerando maior flexibilidade dependendo da necessidade das aplicações e, conseqüentemente, melhor eficiência na rede, transportando no cabeçalho as informações estritamente necessárias.

Um fator crítico a ser resolvido é a questão das aplicações proprietárias, que devem gerar um esforço maior por parte das corporações, pois nesses casos, a comunidade Internet não pode ajudar diretamente, ficando a cargo exclusivamente da empresa realizar os investimentos necessários para a migração.

Analisando-se o aspecto da transição, o principal fator a ser superado é a questão da compatibilidade de aplicações IPv4 acessando aplicações IPv6 e vice-versa, já que o serviço de resolução de nomes DNS para o IPv6 funciona muito bem. Encontram-se disponíveis diversos mecanismos de transição padronizados pelo IETF, e que merecem maiores estudos por parte da comunidade IPv6, a fim de avaliar as mais diversas aplicações, focando aspectos de compatibilidade, eficiência e desempenho final.

Com a capacitação adquirida durante o trabalho podemos ajudar a disseminar o conhecimento de redes IPv6, inicialmente dentro do programa de mestrado profissional do IPT e numa segunda etapa apoiando a RNP e o conjunto de pontos de presença a nível nacional, fundamental para o sucesso da nova tecnologia.

A capacitação e assimilação para o protocolo IPv6 deve ser fácil, principalmente para os profissionais que possuem familiariedade com o IPv4 e pelo fato de possuir muitas RFCs publicadas e material disponível na Internet a respeito do novo protocolo.

8.3. Trabalhos Futuros

Durante esse trabalho, verificaram-se aspectos gerais de implantação do protocolo IPv6, aumento de funcionalidades e comparação entre os dois protocolos. Essa área de tecnologia exige constante aprimoramento, como em qualquer outra área em pleno desenvolvimento.

Diversos assuntos merecem estudo mais detalhado e que podem ser temas para futuros trabalhos de mestrado, como:

- mobilidade associada ao IPv6, verificando aspectos de reendereçamento e autenticação;
- implementação do protocolo MPLS (*Multiprotocol Label Switching*) com IPv6;
- comparativo entre os protocolos de roteamento para IPv6 com o pacote Zebra para Linux;
- questões de segurança utilizando IPSec nativo do IPv6;
- sistemas de *firewall* para IPv6;
- voz sobre IPv6;
- utilização e melhorias do *multicast* no IPv6;
- aspectos relacionados à migração de aplicações com API para IPv6.

Acredita-se que a transição de IPv4 para IPv6 irá mudar significativamente a forma de trabalhar, pesquisar e administrar novas redes nos próximos anos e, dentro desse contexto global, espera-se que o ambiente IPv6, montado no IPT, possa dar substancial contribuição para a Instituição e para futuros trabalhos de mestrado.

O IPT está aberto a parcerias com a finalidade de trocar experiências e integrar o maior número de instituições ligadas a RNP via IPv6. Para isso, conta com uma massa crítica de pesquisadores, professores e alunos de mestrado com disposição de realizar novos trabalhos relacionados ao protocolo IPv6, colocando o IPT como um ponto de presença forte no contexto nacional, incentivando a participação de outras instituições de pesquisa, de modo a promover um trabalho cooperativo de desenvolvimento, teste e implantação deste protocolo rumo à nova geração de redes denominadas NGN (*Next Generation Networks*).

Anexos

1. Arquivo de roteamento do *Host*-1 (Linux)

#route –A inet6
Kernel IPv6 routing table

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
::1/128	::	U	0	0	0	lo
3ffe:2b00:103:1::2/128	::	U	0	749	0	lo
3ffe:2b00:103:1::/64	::	UA	256	1	0	eth0
fe80::208:c7ff:fe09:c40c/128	::	U	0	3	0	lo
fe80::/10	::	UA	256	0	0	eth0
ff00::/8	::	UA	256	0	0	eth0
3ffe::/16	3ffe:2b00:103:1::1	UG	1	753	1	eth0
3ffe::/16	::	UDA	256	0	0	eth0

2. Arquivo de roteamento do *Host*-2 (Windows 2000)

C:\>ipv6 -v rt

::/0 -> 6/3ffe:2b00:103:3::1	pref 0 (lifetime infinite, publish, no aging)
3ffe:2b00:103:3::/64 -> 6	pref 0 (lifetime infinite, publish, no aging)
3ffe:2b00:103:3::2/128 -> 1/::1	pref 0 (lifetime infinite)
fe80::/10 -> 6	pref 1 (lifetime infinite)
fe80::208:c7ff:fe91:4296/128 -> 1/::1	pref 0 (lifetime infinite)
fe80::/10 -> 5	pref 1 (lifetime infinite)
fe80::a03:2/128 -> 1/::1	pref 0 (lifetime infinite)
::10.3.0.2/128 -> 1/::1	pref 0 (lifetime infinite)
fe80::/10 -> 3	pref 1 (lifetime infinite)
fe80::208:c7ff:fe91:4297/128 -> 1/::1	pref 0 (lifetime infinite)
::/96 -> 2	pref 0 (lifetime infinite)

3. Arquivo de configuração tspc.conf

```
# tsp client version
tsp_version=1.0.0
tsp_dir=/ipv6/freenet6

# auth_method=any|supported mechanism
# if any is specified, the first mechanism that is supported by both the
# server and the client will be picked. The order of precedence is the
# mechnism list shown by the output of -h. supprted mechanism is one of
# the token shown by th output of -h (case sensitive).
auth_method=any
#
# client_v4=auto 1.1.1.1 (valid ip address)
# if auto is specified, if_source or -s cmd line option must be specified.
client_v4=200.18.53.137

# userid=anonymous
# the userid can be anonymous or any alphanumeric value that is dns legal.
# userid=anonymous
userid=salvador
```

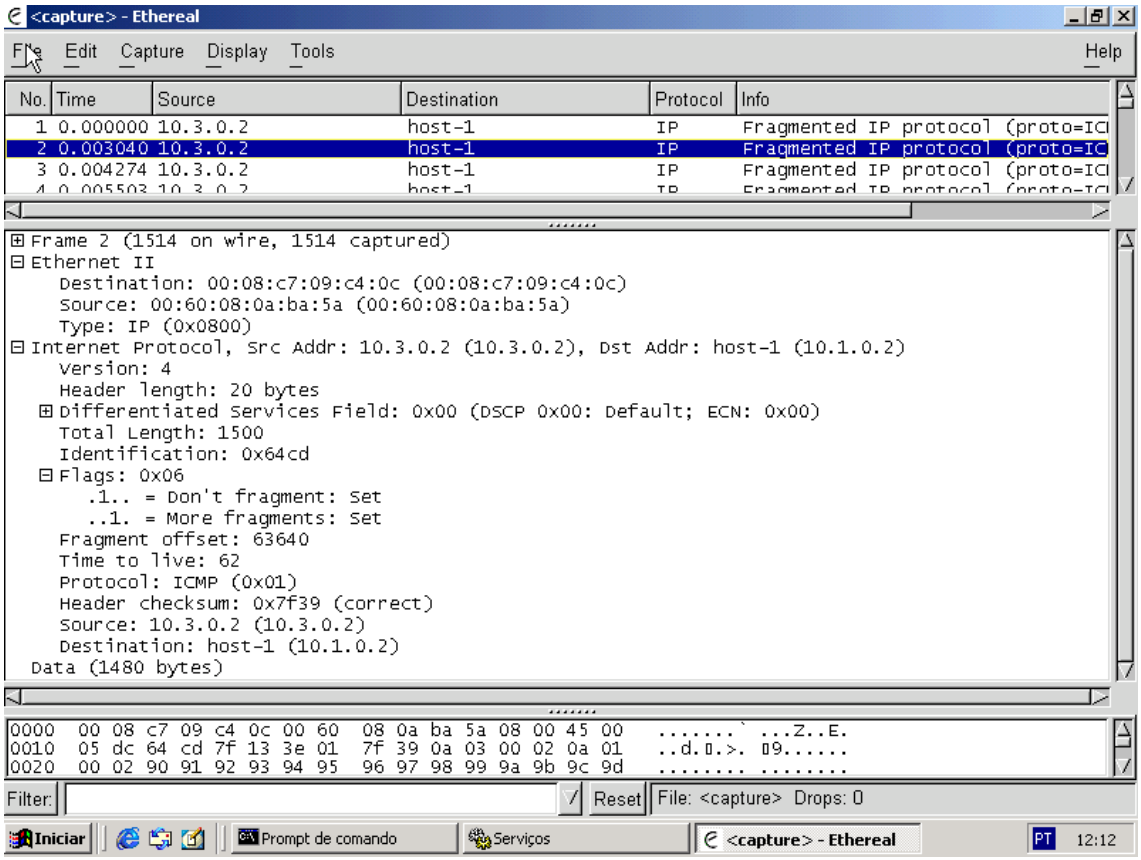
```
# passwd=
# The passwd must be empty if userid is anonymous or an alphanumeric string
# if userid is not anonymous.
passwd=*******

# template=target
# template tells which configuration script needs to be run for interface
# setup.
# Normally you only need to put your osname in the value.
# You can also use "checktunnel" if you only want the tunnel info print out.
#template=checktunnel
template=WindowsNT-2K

server=tsps1.freenet6.net
#server=local*host*

if_tunnel=2

# end of tspc.conf
```

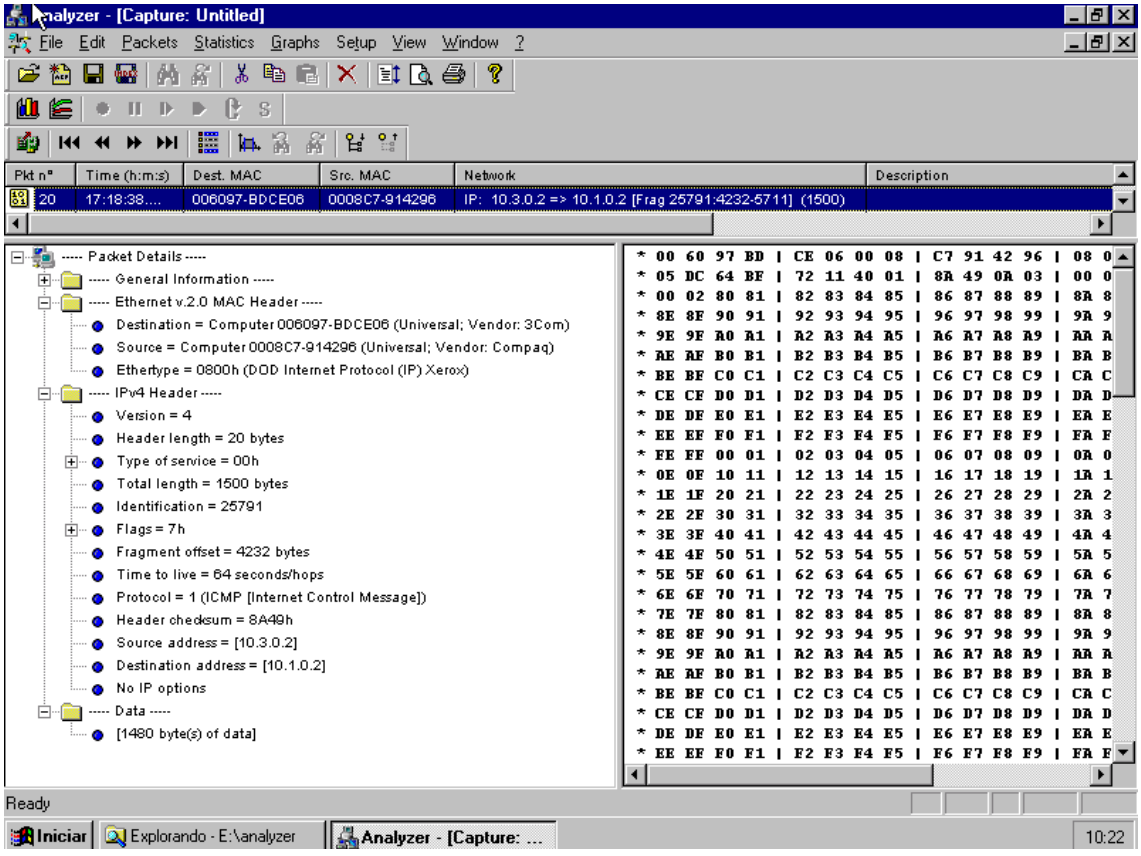
4. Arquivo de log da conexão com o TSP

```
C:\IPv6\freenet6>tspc -vf tspc.conf
tspc - Tunnel Server Protocol Client
Loading configuration file
Connecting to server
Send request
Process response from server
TSP_HOST_TYPE                   host
TSP_TUNNEL_INTERFACE            2
TSP_HOME_INTERFACE
TSP_CLIENT_ADDRESS_IPV4         200.18.53.137
TSP_CLIENT_ADDRESS_IPV6         3ffe:0b80:0002:9b97:0000:0000:0000:0002
TSP_SERVER_ADDRESS_IPV4         206.123.31.114
TSP_SERVER_ADDRESS_IPV6         3ffe:0b80:0002:9b97:0000:0000:0000:0001
TSP_TUNNEL_PREFIXLEN            64
TSP_VERBOSE                     1
TSP_HOME_DIR                    /ipv6/freenet6
IPv4 tunnel server address configured : 206.123.31.114
IPv6 host address configured :          3ffe:0b80:0002:9b97:0000:0000:0000:0002
Success ! Now, you're ready to use IPv6 connectivity to Internet IPv6
Your host is configured to use this IPv6 address :
3ffe:0b80:0002:9b97:0000:0000:0000:0002
End of the script
Closing, exit status: 0
Exiting with return code : 0 (0 = no error)
```

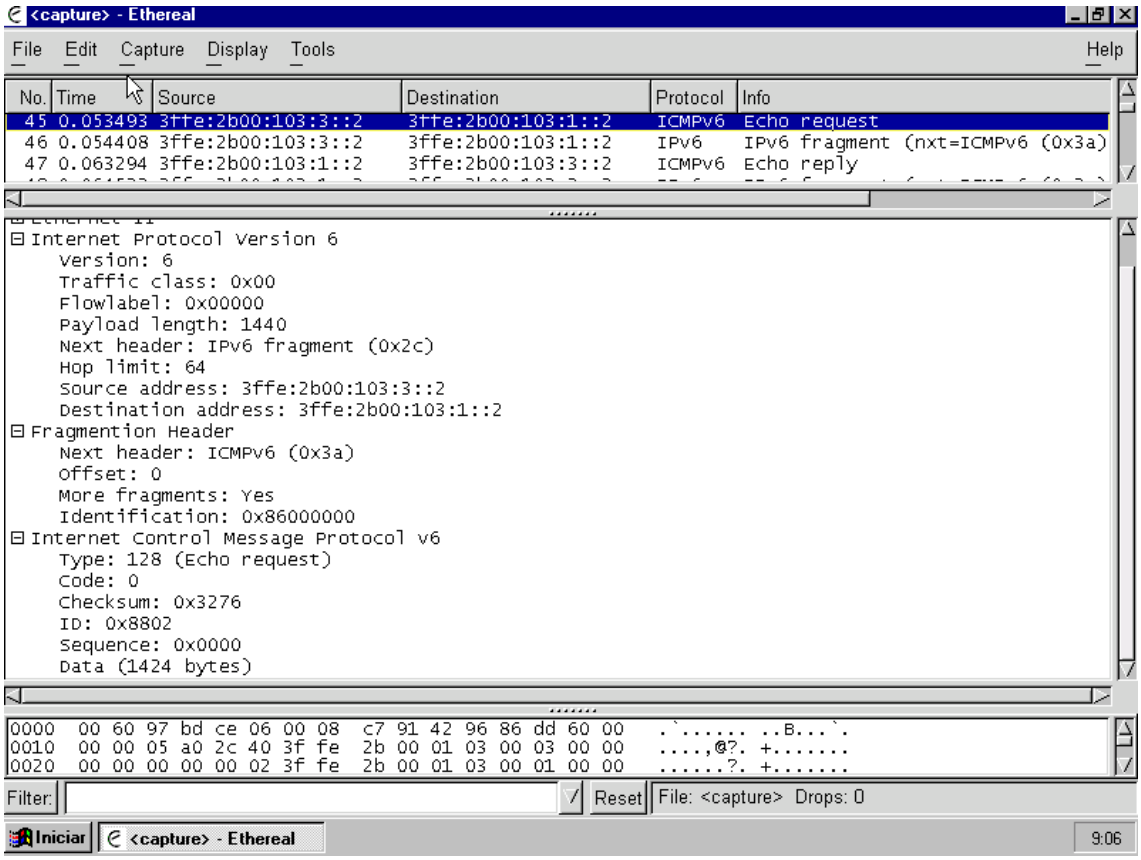
5. Pacotes capturados durante os experimentos

5.1. Pacote IPv4

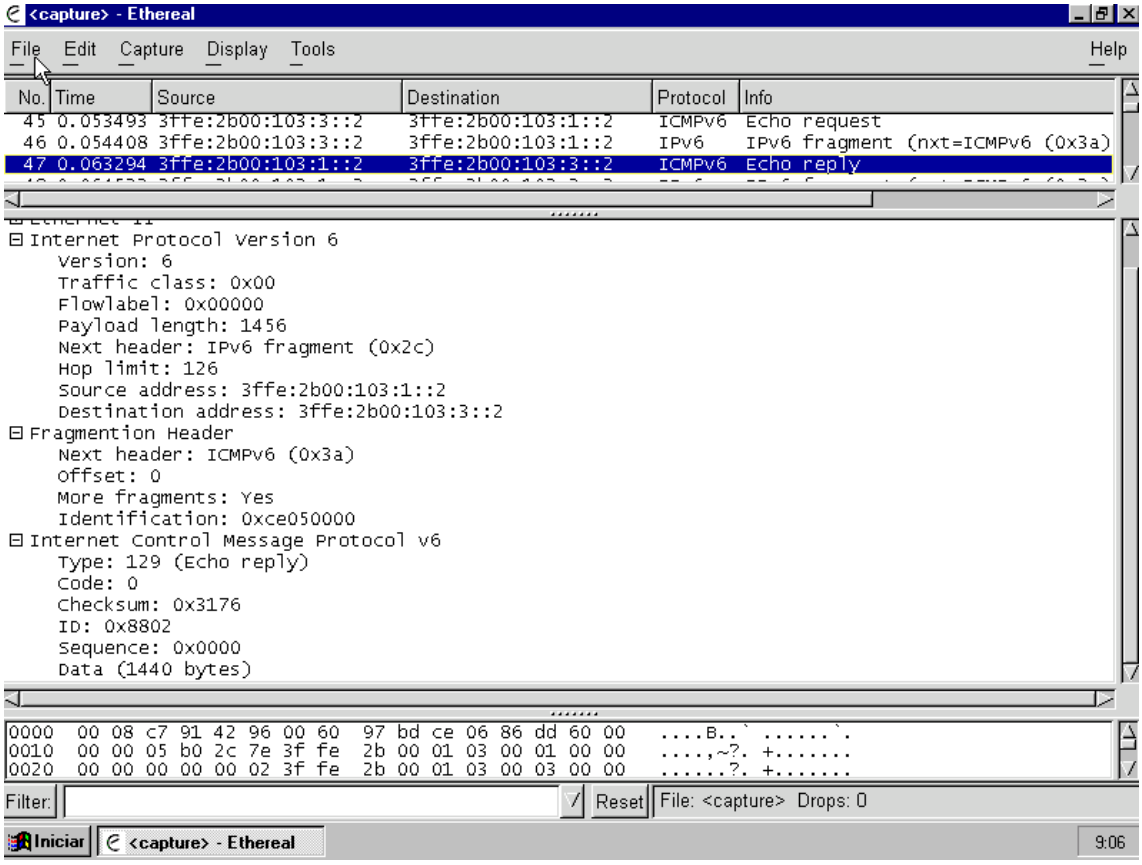




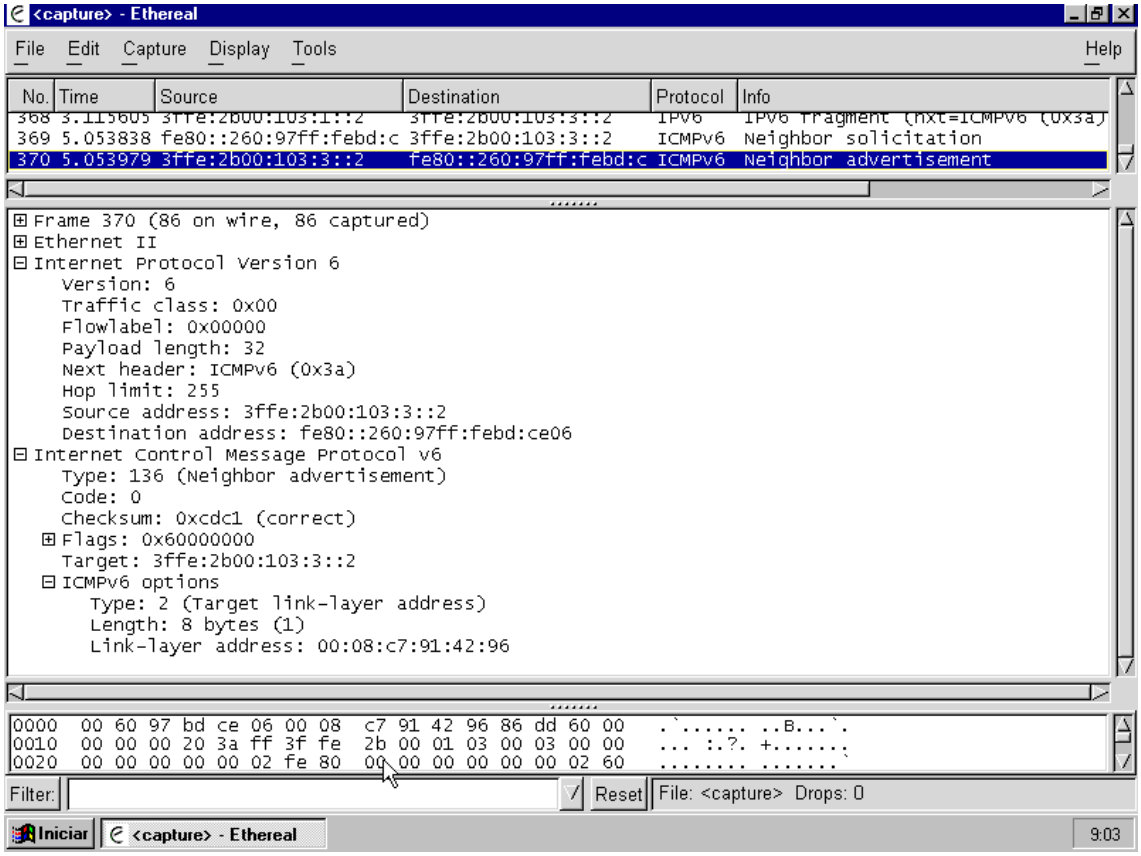
5.2. Pacote ICMPv6 (echo request)



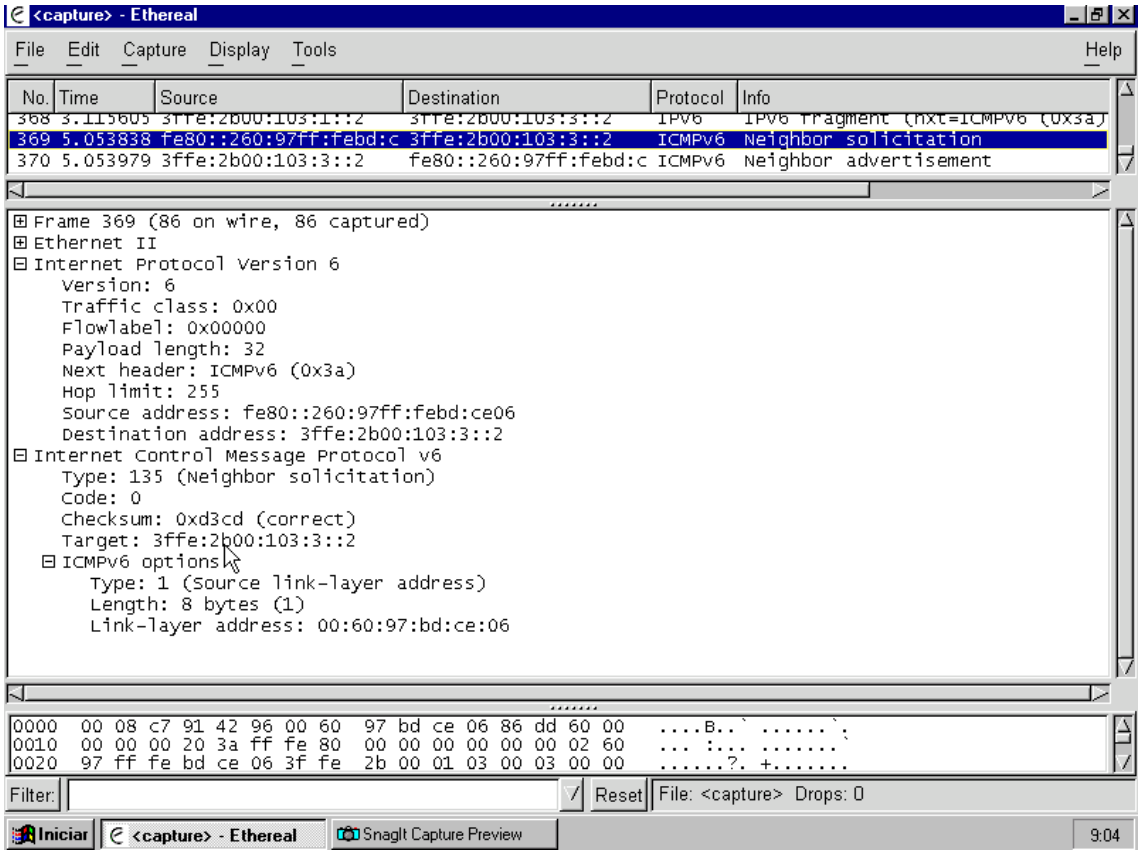
5.3.Pacote ICMP (echo replay)



5.4. Pacote Neighbor Advertisement



5.5. Pacote Neigboor Solicitation



6. Estatísticas de NAT do roteador do IPT

telnet@IPTNet#sh ip nat trans
Total translations: 585 (133 static, 452 dynamic)
Hits: 3192740 Misses: 81881
Expired translations: 3274045
Dynamic mappings:
 pool INTRANET: mask = 255.255.255.224
start 200.18.53.193 end 200.18.53.214
total addresses 22 overloaded
IP Fragments: saved 507, restored 10, timed out 497
ACL IP Fragments: out of seq frag 0, frag head 19, frag count 0
Sess: Total 32768, Avail 29699, NAT 1300
Stream media=1, RTSP=(1:197), MMS=(1:4466), PNM=(1:16)
SMedia LB max CSeq=3, adjust=0, NAT SMedia max CSeq=5, adjust=1

Inside global	Last Inside Local	xmit pkts	xmit bytes	rx pkts	rx bytes	cnt
200.18.53.193	10.4.36.9	4611452	3058484484	4464648	3334429260	18
200.18.53.194	10.5.55.69	2559785	744945914	3146968	3037005137	17
200.18.53.195	10.4.36.2	3018746	904355677	3583710	3206609422	10
200.18.53.196	10.8.1.94	2706878	821941689	3212937	3132320982	27
10.5.55.211	200.18.106.21	2084	2568879	1671	107203	0
10.0.1.42	200.18.53.215	3980	452749	6659	540851	0
200.18.53.197	10.3.5.4	2453344	886756232	2868376	2640427466	21
10.9.56.16	200.18.106.31	0	0	246	15610	0
200.18.53.198	10.200.65.9	3228098	1232612190	3718500	3484988342	8

telnet@IPTNet#sh ip nat trans

Pro	Inside global	Inside local	Outside local	Outside global
tcp	200.18.53.209:61864	10.3.3.5:1794	216.35.213.254:80	216.35.213.254:80
tcp	200.18.53.211:62248	10.3.2.15:1039	200.168.206.90:443	200.168.206.90:443
tcp	200.18.53.201:25235	10.5.55.69:1574	143.108.13.105:80	143.108.13.105:80
udp	200.18.53.205:6263	10.2.54.43:1224	64.202.98.45:4844	64.202.98.45:4844
tcp	200.18.53.214:50782	10.7.46.8:1841	66.159.183.182:2232	66.159.183.182:2232
tcp	200.18.53.202:65197	10.5.39.101:2939	128.220.39.180:1214	128.220.39.180:1214
tcp	200.18.53.193:45892	10.6.53.104:1269	200.246.179.118:80	200.246.179.118:80
tcp	200.18.53.205:10088	10.4.31.51:3923	2.211.41.253:1214	12.211.41.253:1214
tcp	200.18.53.209:57526	10.3.3.5:1795	216.35.213.254:80	216.35.213.254:80
tcp	200.18.53.211:58884	10.2.54.87:1539	64.201.101.2:80	64.201.101.2:80
tcp	200.18.53.211:32746	10.3.2.15:1040	200.168.206.90:443	200.168.206.90:443
tcp	200.18.53.209:35029	10.3.3.5:1796	216.35.213.254:80	216.35.213.254:80
	200.18.53.215	10.0.1.42	200.182.98.157	200.182.98.157
tcp	200.18.53.211:50930	10.2.54.87:1473	200.63.164.102:1081	200.63.164.102:1081
tcp	200.18.53.214:11374	10.7.46.8:1840	24.29.151.242:1214	24.29.151.242:1214

7. Modelo para Solicitação de Endereço IPv6 para a RNP

(Cidade/ Estado, DD/ MM/ AA).
À Rede Nacional de Pesquisa A/ C Adailton Silva.
Coord. Adjunto do LCT/ RNP adailton@ lct. rnp. Br.
Fax: (19) 788-2094.
De: Sr(a). Nome do Solicitante Instituição/ Instituto.
Endereço Completo E-mail Telefone.

Prezado Senhor,
Solicitamos da Rede Nacional de Pesquisa a alocação de um endereço IPv6 para uso em projeto de pesquisa e participação no Backbone IPv6 Brasileiro.
Desde já nos comprometemos a seguir as recomendações e exigências do Grupo de Trabalho NGTRANS (*Next Generation Transition*) da IETF (http:// www. ietf. org/ html. charters/ ngtrans-charter. html), do *6Bone* (http:// www. 6bone. net), inclusive no que se refere às especificações da Internet Draft "*6Bone Routing Practice*" (http:// www. ietf. org/ internet-drafts/ draft-ietf-ngtrans-6bone-routing-01. txt), e outras recomendações que porventura sejam definidas pela Rede Nacional de Pesquisa ou pela IETF. Também nos comprometermos a disponibilizar informações técnicas de pesquisas e testes relevantes para os projetos envolvidos.

Atenciosamente,
Nome do Solicitante Cargo do Solicitante.

8. Formulário enviado pelo IPT para solicitação de endereço IPv6

. Instruções gerais:
. Enviar o formulário preenchido para ipv6-adm@rnp.br
. Não utilize caracteres acentuados ou cedilha.
. Todas as linhas iniciadas com um "#", como a presente, são
comentários e podem ser removidas antes do envio do
formulário.

8.1. Nome da organização que solicita a rede
Identificar a organização, indicando, quando julgar adequado,
subordinação organizacional (campo "Departament/Unit"), como.
no exemplo abaixo.
organization.....: Instituto Pesquisas Tecnológicas do Estado de São Paulo.
departament/unit.....: Departamento de Serviços e Telecomunicações.
address.....: Av Prof Almeida Prado 532.
address.....: Cidade Universitária.
city.....: São Paulo.
state/province.....: SP.
postal Code.....: 05508-901.
country.....: BR.

8.2. Características da Organização e da Utilização da Rede

Preencher com o código de suas letras, dentre as opções abaixo,
a que melhor descreva a organização ou a rede
EB - ensino 1o e 2o graus, ou profissionalizante
ES - ensino superior, graduação ou pós-graduação
GO - órgãos de governo, execut., legisl., judiciário ou militar
IP - instituto de pesquisa, cultural ou científico, museus
CO - organ. comercial, visando lucro, ISPs, indústria, comércio
OR - ONGs, associações, sindicatos, organ. sem fins lucrativos
NE - NET - redes de serviço ou outros usos que não os acima
type1: GO

Caso tenha selecionado EB, ES, GO ou IP, escolha também uma das
opções abaixo. Caso contrário, deixe em branco ou remova a linha
"type2".
PR - entidade privada
FE - subordinada ao governo federal
ET - subordinada a governo estadual
MU - subordinada a governo municipal
type2: ET

8.3. Contato Administrativo
IMPORTANTE: o contato administrativo deve necessariamente ser uma
pessoa vinculada à organização que solicita a rede. O endereço postal
e telefone dessa pessoa serão interpretados como os da própria
organização que solicita a rede.
Caso a pessoa já esteja cadastrada na base de dados da RNP, coloque
aqui apenas o seu "*nic-handle*" e deixe os outros campos dessa
seção em branco.
nic-hdl:

Caso não haja cadastramento prévio, forneça as informações abaixo.
Como parte do processo de registro, lhe será devolvido um *nic-handle*
(identificador único) para a pessoa especificada.
person: Salvador Giaquinto.
address: IPT - Instituto Pesquisas Tecnológicas.
address: Departamento Serviços e Telecomunicações.
address: Av. Prof Almeida Prado 532.
address: 05508-901.
phone: +55 11 3767-4663.
fax-no: +55 11 3767-4101.
e-mail: salvador@ipt.br.
notify: salvador@ipt.br.

8.4. Contato Técnico
Caso o contato técnico e o administrativo sejam a mesma pessoa,
deixar os campos abaixo em branco.
A pessoa de contato técnico pode não ser formalmente vinculada
a organização que solicita a rede, podendo ter endereço, telefone e
fax diferentes, e mesmo trabalhar regularmente em outra organização.
#
Caso a pessoa já esteja cadastrada na base de dados da RNP, coloque
aqui apenas o seu "*nic-handle*" e deixe os outros campos dessa
seção em branco.
nic-hdl:
Caso contrário, forneça as informações abaixo.
Como parte do processo de registro, lhe será devolvido um *nic-handle*
para a pessoa especificada. Veja exemplo:
address:
phone:
fax-no:
e-mail:
notify:
organization:

8.5. Nome da Rede
Nome da rede. Ano deve conter, no máximo, 14 caracteres.
alfanuméricos. Veja exemplo:
netname: IPT.

8.6. Breve Descrição da Rede IPv6
Campo obrigatório. Necessário para avaliação do pedido. Formato livre.

Solicitação de um endereço IPv6, para iniciar os testes com uma rede piloto no IPT verificando os principais métodos de transição existentes e montar um plano de endereçamento definitivo visando à migração de todos os *hosts* de IPv4 para IPv6 para todo o campus do IPT.

Além disso, tem-se também o mestrado profissional em engenharia de computação recentemente autorizado pelo MEC, contando com 457 alunos que, na sua maioria, estarão desenvolvendo suas dissertações em temas associados a redes de computadores utilizando a infra-estrutura instalada no Instituto.

8.7. Espaço Solicitado
Informar o tamanho do prefixo IPv6 solicitado:
NLA (/48), SLA (/56) ou Leaf Site (/64).
Alocações inicias.
Length of IPv6 prefix. /48.

Justifique, em formato livre, a quantidade de espaço de endereçamento solicitado. O correto preenchimento desse item é fundamental no julgamento da solicitação.

O IPT, instituição centenária, ligada à Secretaria de Ciência, Tecnologia e Desenvolvimento Econômico do Estado de São Paulo, situa-se numa área construída de 87.000 m no campus da Cidade Universitária, em São Paulo, onde trabalham cerca de 1.300 funcionários, desse total, 400 são pesquisadores.

O IPT cumpre seu objetivo atuando basicamente em três grandes áreas: inovação, pesquisa e desenvolvimento; serviços tecnológicos e desenvolvimento e apoio metrológico.

Com o apoio de seus 72 laboratórios e equipes de pesquisa, são elaborados relatórios técnicos sobre diagnósticos, estudos e análises teórico-experimentais, entre outros serviços. O IPT desenvolve, ainda, programas específicos de apoio a micro e pequenas empresas, apoio às exportações, a garantia da qualidade e a políticas publicas.

Outras atividades de relevo do IPT dizem respeito à difusão do conhecimento científico e tecnológico. São atendidas, anualmente, cerca de 20 mil consultas aos sistemas de informação tecnológica, tais como normas, informações referenciadas e pesquisas bibliográficas especializadas.

Atualmente a rede IPTNet possui tecnologia *Gigabit Ethernet* no backbone central, possuindo mais de 1.400 *hosts* e mais de 1.500 contas de usuários. Utiliza cerca de 30 km de fibras ópticas, interligando 27 prédios no campus e 53 km de cabo UTP categoria 5 para o cabeamento interno das redes locais dos prédios. Opera com os sistemas operacionais Solaris, Linux (Distribuições Conectiva, Debian e Redhat) e Microsoft Windows NT/2000 e possui um link de acesso de 100 Mbps com a USP para acesso a rede mundial INTERNET.

8.8. Dados do Servidor de Nomes
Primary IP6.INT Server Hostname: volta.ipt.br.
Secondary IP6.INT Server Hostname

8.9. IP da Interface de Túnel
Endereço IP da interface de túnel.
tunnel endpoint: 200.18.53.133/27.

8.10. Outras informações:
Coloque aqui informações que lhe pareçam importantes a respeito da organização ou #experimentos que deseje conduzir.
Este campo é opcional e em formato livre.

* Dúvidas, críticas ou sugestões, relativas a esse formulário, favor endereça-lás a
* ipv6-adm@rnp.br Serão bem-vindas.

Os campos telefone e e-mail são indispensáveis.

O CONTATO ADMINISTRATIVO TEM QUE SER OBRIGATORIAMENTE UMA PESSOA VINCULADA À ORGANIZACAO QUE SOLICITA A REDE, PESSOA ESSA QUE SEJA RESPONSÁVEL PELA CONECTIVIDADE À INTERNET DE SUA ORGANIZACAO.OS DADOS DE ENDERECO E TELEFONE DO ADMIN-C SERAO CONSIDERADOS COMO SENDO OS DA ORGANIZACAO.

Tipicamente, o contato-admin será o gerente de processamento de dados ou de redes, ou o chefe do CPD da organização solicitante.

Tipicamente, o contato-técnico será o técnico diretamente envolvido com o gerenciamento da rede da organização e sua conexão á Internet. Essa pessoa será procurada sempre que ocorram problemas ou dúvidas relacionadas ao funcionamento adequado da rede. Por imediato, entende-se um período de até 60 dias após a entrada em operação de rede.

9. Localização dos prédios do IPT e dutos de fibra óptica

A seguir a disposição dos prédios com os respectivos números associados e a interligação dos dutos de fibra óptica ao longo da avenida principal:

Glossário

ALG – *Aplication Level Gateway* - agente tradutor específico, utilizado nas aplicações em que o NAT apresenta dificuldades para tradução endereços IP contidos na carga útil do pacote.

API – *Aplication Program Interface* – também conhecido como *socket*, que permite que uma aplicação tenha acesso aos protocolos TCP/IP, através de chamadas do sistema operacional. Planejada para ser uma interface de comunicação genérica sendo apresentada primeiramente pelo sistema Unix BSD 4.2, tornou-se padrão de indústria.

ARP - *Address Resolution Protocol*. Protocolo usado para vincular dinamicamente um endereço IP a um endereço físico de *hardware* (MAC).

ARPA - *Advanced Research Projects Agency*. Órgão do governo norte-americano que fundou a Arpanet e mais tarde a Internet.

Backbone – Núcleo central de uma determinada rede e atua como principal caminho para o trafego entre as redes interligadas.

Bps - bits por segundo. Medida da taxa de transmissão de dados.

Broadcast - Referência a um endereço de difusão, onde o sistema de entrega de pacotes fornece uma cópia de determinado pacote para todos os *hosts* ligados à rede.

CIDR - Abreviatura de *Classless Inter-Domain Routing*. Esquema de endereçamento que usa um grupo de endereços contíguos de classe "C". O CIDR foi adotado como uma solução temporária para o problema de consumo de espaço no endereço de classe B.

Circuito virtual - Abstração básica fornecida por um protocolo baseado em conexões, como o TCP. Uma vez criado, o circuito virtual permanece em vigor até que o seu encerramento seja explicitamente solicitado.

Controle de fluxo - Controle da taxa com que (*host*s ou roteadores) transmitem pacotes numa rede ou interligação em redes, normalmente para evitar congestionamentos.

Datagrama - Unidade de informação básica passada através de uma interligação em redes TCP. Um datagrama IP está para uma interligação em redes, assim como um pacote de hardware está para uma rede física. Contém um endereço de origem e um endereço de destino, juntamente com os dados.

DHCP - *Dynamic Host Configuration Protocol*. Protocolo que o *host* usa para obter todas as informações necessárias de configuração, inclusive um endereço IP.

DMZ – abreviatura de *Demilitarized Zone*. Consiste em uma rede protegida situada entre a rede pública e a rede interna, composta de servidores como DNS, WWW, correio eletrônico etc.

DNS - *Domain Name System*. Sistema de base de dados distribuído, usado para converter endereços IP em nomes de máquinas. Os servidores DNS de toda a rede Internet conectada implementam um espaço de nome hierárquico, que dá liberdade aos *sites* para atribuírem nomes e endereços às suas máquinas.
Endereço - Identificação IPv4 ou IPv6, para uma interface ou conjunto de interfaces.

Endereço de hardware - Endereços de baixo nível usados por placas de rede ou equipamentos de redes com tecnologia *Ethernet* composto de 48 bits. Também conhecido como endereço MAC.

Firewall – Geralmente equipamento dedicado, colocado entre uma ligação em redes interna de uma organização e uma conexão a uma interligação em redes externa, de modo a oferecer segurança.

FTP - *File Transfer Protocol*. Protocolo de alto nível, padrão TCP/IP, para transferir arquivos de uma máquina para outra.

H.323 – Protocolo que permite videoconferência sobre LANs e outras redes de comutação de pacotes.

Host - qualquer nó da rede que não é um roteador.

IAB - *Internet Architecture Board*. Entidade responsável por estabelecer as políticas e diretrizes para o TCP/IP e a Internet global.

IANA - *Internet Assigned Number Authority*. Entidade responsável pela atribuição de endereços usados nos protocolos TCP/IP.

ICMP - *Internet Control Message Protocol.* Parte integrante do protocolo da Internet (IP) que lida com mensagens de erro e de controle. Especificamente, roteadores e *hosts* usam o ICMP para enviar mensagens de problemas relativos aos datagramas ao ponto inicial que os enviou. O ICMP também inclui solicitação e resposta de eco usada para verificar se um destino é alcançável.

IETF - *Internet Engineering Task Force*. Entidade responsável pelo projeto do TCP/IP e da Internet global. A IETF está dividida em áreas, cada qual com um administrador independente. As áreas estão subdivididas em grupos de trabalho.

Internet - Conjunto de redes interligadas através do protocolo TCP/IP, formando uma única rede virtual. A Internet conecta hoje milhões de computadores.

IPv4 - *Internet Protocol* versão 4, composto de 32 bits. Protocolo da camada de rede do TCP/IP que define o datagrama IP como a unidade de informação passada através de uma interligação em redes e fornece as bases para o serviço sem conexão de entrega de pacotes.

IPv6 - Nome oficial da próxima versão do IP, sucessor do IPv4, composto de 128 bits de endereçamento.

ISO - *International Standard Organization*. Instituição internacional que define, discute, propõe e especifica padrões para protocolos de rede. A ISO é conhecida melhor pelo modelo de referência de sete camadas que descreve a organização conceitual de protocolos.

ISP - *Internet Service Provider*. Empresas responsáveis pelo acesso à Internet através de canal de alta velocidade.

Link - facilidade de comunicação através do qual os nós podem se comunicar na camada de enlace, a camada imediatamente inferior ao IPv6, tais como *Ethernet*, ATM , FDDI etc.

MBONE - *Multicast Backbone*. Acordo entre *sites* para enviar datagramas em *multicast* através da Internet.

MTU - *Maximum Transfer Unit*. O maior tamanho de um pacote que pode ser transferido em determinada rede física. A MTU é determinada pelo *hardware* da rede.

Multicast - técnica que permite que cópias de um único pacote sejam passadas a um subconjunto selecionado de todos os destinos possíveis. Por exemplo, as redes *Ethernet* suportam *multicast*, permitindo que uma interface de rede pertença a um ou mais grupos *multicast*.

NAT - *Network Address Translator*. Mecanismo para reduzir a necessidade de endereços públicos válidos na Internet. O NAT permite que uma organização com endereços privativos possam se conectar à Internet traduzindo esses endereços em endereços globalmente roteáveis.

NGN – *Next Generation Networks*. Redes de próxima geração com recursos de comutação de pacotes que permitirão oferecer, em uma única infra-estrutura IP, diversos serviços como som, imagem, texto, dados e voz.

Nó - um dispositivo que implementa a pilha IPv6.

OSI - *Open System Interconnection*. Modelo de referência usado para protocolos, padrões ISO, para a conexão de sistemas de computadores.

Pacote - Termo usado para fazer referência a qualquer bloco pequeno de dados enviado numa rede de comunicação de pacotes, composto de um cabeçalho mais o *payload* (carga útil + dados).

Ping - Nome de um programa utilizado na interligação de redes TCP/IP para testar a conectividade e possibilidade de alcançar o destino, através do envio ao destino de um pedido de eco ICMP e da espera por uma resposta.

RFC - *Request For Comments*. Nome de um conjunto de normas que contêm levantamentos, avaliações, idéias, técnicas e comentários, bem como padrões de protocolos TCP/IP sugeridos e aceites. As RFC's estão disponíveis *on-line*.

SIT - *Simple Internet Transition*. É um conjunto de mecanismos criados para permitir a transição IPv4-IPv6.

SOCKS – É um padrão para *gateway* em nível de circuito, não requerendo o uso de um servidor *proxy* mais convencional, onde o usuário primeiramente tem que conectar a *firewall* antes de solicitar a segunda conexão ao destino. O cliente necessita que a sua aplicação tenha suporte a SOCKS.

TCP - *Transmission Control Protocol*. Protocolo do nível de transporte padrão que fornece um serviço *full-duplex*, confiável, de comunicação fim-a-fim. O TCP é orientado à conexão porque, antes de transmitir os dados, os participantes necessitam de

estabelecer uma conexão. Todos os dados são enviados em segmentos TCP e cada um deles é enviado na Internet através de um datagrama IP.

TTL - *Time To Live*. Técnica usada pelo TCP-IP para evitar que pacotes permaneçam em *loops* intermináveis na rede.

UDP - *User Datagram Protocol*. Protocolo de transporte TCP/IP, não-orientado à conexão, que permite uma aplicação de uma máquina envie um datagrama a uma aplicação de outra máquina. O protocolo UDP utiliza o protocolo IP para entregar datagramas. A diferença mais importante entre os protocolos IP e UDP é que este último inclui o número da porta do protocolo, permitindo que o emissor faça a distinção entre várias aplicações numa determinada máquina remota.

Unicast - Método com o qual um pacote é enviado para um único destino. A maioria dos datagramas IP é enviado através de *unicast*.

Vizinhos - nós ligados pelo mesmo *link.*

VoIP – Voz sobre IP. Protocolos e produtos que permitem a transmissão de chamadas telefônicas sobre redes IP.

VPN – *Virtual Private Network.* Interligação de redes particulares virtuais, caracterizada pelo conjunto de protocolos e processos que permitem a uma determinada empresa interconectar com segurança *sites* que fazem parte de uma rede particular por meio de rede pública (Internet).

WEB – Abreviatura de *Word Wide Web*, sendo uma rede de servidores da Internet que oferece serviços de hipertexto e outros serviços a terminais que executam aplicativos clientes, como os navegadores.

Referências Bibliográficas

[AND01] ANDRADE, Maiko, Proposta de Implementação do protocolo IpngLS, Universidade do Rio dos Sinos – Novembro de 2001.

[BIL 01] DUTCHER, Bill. The NAT Handbook Implementing and Managing Network Address Translation, Wiley, 2001.

[CHO02] CHOWDHURY, DHIMAN DEB, Projetos Avançados de rede IP: Roteamento, Qualidade de Serviço e Voz sobre IP, Tradução, Editora Campus, 2002.

[FOR01] FORTENBERRY, Thaddeus Windows 2000, Virtual Private Networking, tradução Melissa Kassner, editora Berleley, 2001.

[HOL02] HOLLENBECK Rion, GROOM Frank, JONES Steve, The Next Generation Protocol, ICS 621 – 2002.

[MUR00] MURHAMMER, Martin W. TCP/IP Tutorial e Técnico Tradução, Editora Makron Books, 2000.

[NAU01] NAUGLE, MATTHEW, Guia Ilustrada do TCP-IP, Tradução Ana Beatriz Tavares e Ana Beatriz de Castro, Editora Berkley, 2001.

[OPP99] OPPENHEIMER, Priscilla Projeto de Redes TOP-DOWN, CISCO Systems , Editora Campus, 1999.

[PER20] Solving NAT and Private IP problems – Permeo Technologies, Inc, July 2001.

[RAN00] RANCH, David. Linux IP Masquerade HOWTO -versão 1.81. Janeiro de 2000. http://metalab.unc.edu/pub/Linux/docs/HOWTO/IP-Masquerade-HOWTO.

[SHI00] Shieh, Shiuh-Pyng, Ho Fu-Shen, Huang Yu-Lun and Luo Jia-Ning. "Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP stack." IEEE Internet Computing. vol. 4, no. 6 (November/December 2000).

[SOA95] SOARES, Luiz Fernando G, LEMOS Guido e COLCHER Sergio, Redes de Computadores LAN, MAN, WAN as Redes ATM Segundo Edição, editora Campus, 1995.

[STR00] STREBE, Matthew & PERKINS Charles Firewalls, editora Makron Books, 2000.

[TAN 97] TANEMBAUM, Andrew S. Redes de Computadores. Editora Campus, 3a Edição, 1997.

[TAU02] TAURION, CESAR Internet Móvel, Tecnologia e modelos, Editora Campus, 2002.

[ZWI 00] ZWICKY, Elizabeth D. Construindo Firewalls para Internet Editora Campus 2 edição 2000.

RFC 1166 - Internet numbers S. Kirkpatrick, M.K. Stahl, M. Recker, Jul-01-1990. Informational (Obsoletes RFC1117 RFC1062 RFC1020).

RFC 1191 - Path MTU discovery J.C. Mogul, S.E. Deering, Nov-01-1990. Draft (Obsoletes RFC1063).

RFC 1519 - Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy V. Fuller, T. Li, J. Yu, K. Varadhan, September 1993. Proposed (Obsoletes RFC1338).

RFC 1631 - The IP Network Address Translator (NAT) K. Egevang, P. Francis, May 1994. Informational (Obsoleted by RFC3022).

RFC 1752 - The Recommendation for the IP Next Generation Protocol S. Bradner, A. Mankin, January 1995. Proposed.

RFC 1917 - An Appeal to the Internet Community to Return Unused IP Networks (Prefixes) to the IANA P. Nesser II, February 1996. IETF BCP #4 Best Current Practice.

RFC 1918 - Address Allocation for Private Internets Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, February 1996. IETF BCP #5 Best Current Practice (Obsoletes RFC1627 RFC1597).

RFC 1928 - SOCKS Protocol Version 5 M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones, March 1996. Proposed.

RFC 2002 - IP Mobility Support C. Perkins, Ed., October 1996. Proposed (Obsoleted by RFC3220) (Updated by RFC2290).

RFC 2080 - RIPng for IPv6 G. Malkin, R. Minnear, January 1997. Proposed.

RFC 2081 - RIPng Protocol Applicability Statement G. Malkin, January 1997. Informational.

RFC 2185 - Routing Aspects of IPv6 Transition R. Callon, D. Haskin, September 1997. Informational.

RFC 2373 - IP Version 6 Addressing Architecture. R. Hinden, S. Deering. July 1998. (Obsoletes RFC1884) (Status: Proposed Standard).

RFC 2374 - An IPv6 Aggregatable Global Unicast Address Format R. Hinden, M. O'Dell, S. Deering, July 1998. Proposed (Obsoletes RFC2073).

RFC 2375 - IPv6 Multicast Address Assignments. R. Hinden, S. Deering. July 1998. (Status: Informational).

RFC 2402 - IP Authentication Header. S. Kent, R. Atkinson. November 1998. (Obsoletes RFC1826) (Status: Proposed Standard).

RFC 2406 - IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998. (Obsoletes RFC1827) (Status: Proposed Standard).

RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden, December 1998. Draft (Obsoletes RFC1883).

RFC 2461 - Neighbor Discovery for IP Version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson. December 1998. (Obsoletes RFC1970) (Status: Draft Standard).

RFC 2463 -Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. A. Conta, S. Deering.December 1998. (Obsoletes RFC1885) (Status: Draft Standard).

RFC 2529 - Transmission of IPv6 over IPv4 Domains without Explicit Tunnels B. Carpenter, C. Jung, March 1999. Proposed.

RFC 2535 - Domain Name System Security Extensions. D. Eastlake 3rd. March 1999.) (Obsoletes RFC2065) (UpdatesRFC2181, RFC1035, RFC1034) (Updated by RFC2931, RFC3007, RFC3008, RFC3090, RFC3226) (Status: Proposed Standard).

RFC 2694 - DNS extensions to Network Address Translators (DNS_ALG) P. Srisuresh, G. Tsirtsis, P. Akkiraju, A. Heffernan, September 1999. Informational.

RFC 2740 - OSPF for IPv6 R. Coltun, D. Ferguson, J. Moy, December 1999. Proposed.

RFC 2765 - Stateless IP/ICMP Translation Algorithm (SIIT) E. Nordmark, February 2000. Proposed.

RFC 2766 - Network Address Translation - Protocol Translation (NAT-PT) G. Tsirtsis, P. Srisuresh, February 2000. Proposed (Updated by RFC3152).

RFC 2767 - Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS) K. Tsuchiya, H. Higuchi, Y. Atarashi, February 2000. Informational.

RFC 2772 - Bone Backbone Routing Guidelines R. Rockell, R. Fink, February 2000. Informational (Obsoletes RFC2546) (Updated by RFC3152).

RFC 2775 - Internet Transparency. B. Carpenter. February 2000. Status: Informational).

RFC 2874 - DNS Extensions to Support IPv6 Address Aggregation and Renumbering M. Crawford, C. Huitema, July 2000. Proposed (Updates RFC1886) (Updated by RFC3152 RFC3226).

RFC 2893 - Transition Mechanisms for IPv6 Hosts and Routers. R. Gilligan, E. Nordmark. August 2000. (Obsoletes RFC1933) (Status: Proposed Standard).

RFC 2894 - Router Renumbering for IPv6. M. Crawford. August 2000. (Status: Proposed Standard).

RFC 2993 - Architectural Implications of NAT. T. Hain. November 2000. (Status: Informational).

RFC 3024 - Reverse Tunneling for Mobile IP, revised. G. Montenegro, Ed.. January 2001. (Obsoletes RFC2344) (Status: Proposed Standard).

RFC 3027 - Protocol Complications with the IP Network Address Translator M. Holdrege, P. Srisuresh, January 2001. Informational.

RFC 3053 - IPv6 Tunnel Broker A. Durand, P. Fasano, I. Guardini, D. Lento, January 2001. Informational.

RFC 3068 - An Anycast Prefix for 6to4 Relay Routers. C. Huitema. June 2001. (Status: Proposed Standard).

RFC 3152 - Delegation of IP6.ARPA R. Bush, August 2001. IETF BCP #49 Best Current Practice (Updates RFC2874 RFC2772 RFC2766 RFC2553 RFC1886).

RFC 3338 - Dual Stack Hosts Using "Bump-in-the-API" (BIA). S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, A. Durand. October 2002. (Status: Experimental).

[1] http://www.cisco.com
[2] http://www.microsoft.com
[3] http://www.enterasys.com/products/whitepapers/ssr/network-trans/
[4] http://playground.sun.com/pub/ipng/html/
[5] http://www.suse.de/~mha/linux-ip-nat/diplom/node1.html
[6] http://ntrg.cs.tcd.ie/undergrad/4ba2.02/ipv6
[7] http://www.krv6.net/bia/
[8] http://www.6talk.net/6talk_natpt.htm
[9] http://www.ipv6.rennes.enst-bretagne.fr/dstm/index.html
[10] http://sites.uol.com.br/wirelessbr/
[11] http://www.eurescom.de/~public-webspace/P1000-series/P1009/index.html