UNIVERSIDADE DO EXTREMO SUL CATARINENSE
CURSO DE CIÊNCIA DA COMPUTAÇÃO

ADILSON MIOTELLI

ESTUDO DA TRANSIÇÃO ENTRE PROTOCOLOS DE COMUNICAÇÃO IPv4 E IPv6

CRICIÚMA, JUNHO DE 2006.

ADILSON MIOTELLI

ESTUDO DA TRANSIÇÃO ENTRE PROTOCOLOS DE COMUNICAÇÃO IPv4 E IPv6

Trabalho de Conclusão de Curso para a Obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. M.Sc. Rogério Antônio Casagrande

CRICIÚMA, JUNHO DE 2006.

ADILSON MIOTELLI

ESTUDO DA TRANSIÇÃO ENTRE PROTOCOLOS DE COMUNICAÇÃO IPv4 E IPv6

Submetido ao corpo docente do Departamento de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

_____

Profª. M.Sc. Ana Cláudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

_____

Profº. M.Sc. Rogério Antônio Casagrande (UNESC)
Orientador

_____

Prof. M.Sc. Paulo João Martins (UNESC)

_____

Profº. Esp. Vilson Gruber (SATC)

Aos meus pais, Rubens e Neide, meus irmãos Luciano, Luiz e Aldir e a todos os meus amigos, em especial ao Jhonas, pelo apoio concedido até aqui.

AGRADECIMENTOS

Agradeço muito a Deus por me guiar e iluminar ao longo da vida, pois em vários momentos de tristeza e angústia me manteve com a calma e a determinação para seguir em frente.

Agradeço também:

A minha família que é minha mão direita nesta vida, me proporcionando amor, educação e afeto, além de estarem sempre me incentivando e me dando força nos momentos que preciso.

A todos meus amigos que me deram apoio e ajudaram nos momentos que precisei.

A todos os professores que ministraram durante o curso, que foram a base do meu conhecimento para despertar o interesse na busca de novos horizontes.

Em especial ao meu orientador Rogério Antônio Casagrande que sempre esteve ao meu lado, tranqüilizando, orientando e incentivando para o desenvolvimento deste trabalho.

A todos os meus colegas de trabalho da Diretoria de Informática e Monitores dos Laboratórios que sempre me deram incentivos para ser perseverante em meus trabalhos.

A todos meus colegas de profissão da Seara Alimentos S/A que foram bastante flexíveis em me ajudar e incentivar nesta caminhada.

E por fim, a todos os meus grandes amigos e companheiros que vivenciaram esta caminhada durante quatro anos e meio, todos os dias.

“I am enough of an artist to
draw freely upon my imagination.
Imagination is more important than knowledge.
Knowledge is limited.
Imagination encircles the world.”

(Albert Einstein)

RESUMO

Com o uso do protocolo de comunicação atual (IPv4), muitas vezes a falta de segurança, restrição à comunicação em tempo real e a possível falta de endereçamento IP, pelo crescimento exponencial de *hosts* ligados a rede de computadores, têm despertado a pesquisa e o desenvolvimento do novo protocolo IP (IPv6). Este com capacidade de endereçamento enorme, por usar 128 bits de endereçamento, e correções de deficiências do IPv4 vêm crescendo continuadamente dia-a-dia conforme a implantação de novas redes de comunicação e sua absorção através da transição do protocolo anterior ao atual. Na realização desta pesquisa buscou-se a abordagem dos dois protocolos IP com suas características, novas funções e principalmente nas formas de transição e convivência dos protocolos nas redes em diversos cenários que são encontrados. Os protocolos precisam funcionar em conjunto por muito tempo já que não existe a possibilidade de realizar uma migração imediata para o novo protocolo. Esta convivência deve ser bastante sutil de forma a manter o funcionamento regular da rede durante a transição. Além disto, este trabalho de pesquisa consiste no desenvolvimento de uma interface de apoio ao estudo dos protocolos de comunicação IPv4, IPv6 e mecanismo de transição e convivência dos mesmos.

Palavras-chaves: Redes de Computadores, Arquitetura TCP/IP, Protocolos de Comunicação, Mecanismos de Transição.

ABSTRACT

With the use of the current protocol communication (IPv4), sometimes the lack of security, restriction to the communication in real time and the possible lack of addressing IP, have to propitiate the research and the development of new protocol IP (IPv6) for on the exponential growth of hosts existing in computer networks. The IPv6 have capacity of enormous addressing, for using 128 bits of addressing, and corrections of deficiencies of the IPv4 come continued growing day-by-day as the implantation of new communication networks and its absorption through the transition of the previous protocol to the current one. In the accomplishment of this research it searched boarding of two protocols IP with its features, new functions and mainly in the forms of transition and co-existebce of the protocols in netwoks in diverse scenes that are found. The protocols need to function in set for much time since the possibility does not exist to carry through an immediate migration for the new protocol. This co-existence must be sufficiently subtle for the regular functioning of the network during the transition. Moreover, this work of research consists of the development of an interface of support to the study of the communication protocols IPv4 and IPv6 and mechanism of transition and co-existence of the same ones.

Keywords: Computer networks, Architecture TCP/IP, Communication Protocols, Transition Mechanisms..

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ALG	*Application Layer Gateway*
API	*Application Programmation Interface*
ARP	*Address Resolution Protocol*
ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
BBN	*Bolt Beranek e Newman*
BIA	*Bump in the API*
BIS	*Bump in the Stack*
BOOTP	*BOOTstrap Protocol*
CAN	*Controller Area Network*
CPU	*Central Processing Unit*
DARPA	*Department of Defense Advanced Research Projects Agency*
DEC	*Digital Equipment Corporation*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name Service*
DQDB	*Distributed Queue Dual Bus*
DSTM	*Dual Stack Transition Mechanism*
EUA	Estados Unidos da América
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
IBM	*International Business Machines*
ICMP	*Internet Control Message Protocol*
ICMPv4	*Internet Control Message Protocol version 4*

ICMPv6	*Internet Control Message Protocol version 6*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
IPng	*Internet Protocol The Next Generation*
IPSec	*Internet Protocol Security Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISATAP	*Intra-Site Automatic Tunnel Addressing Protocol*
ISO	*International Standards Organization*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
Mbps	Megabits por Segundo
MIT	*Massachussets Institute of Technology*
MLD	*Multicast Listener Discovery*
MTU	*Maximum Transfer Unit*
NAPT-PT	*Network Address Port Translation and Packet Translation*
NAT-PT	*Network Address Translation with Protocol Translation*
NCP	*Network-Control Protocol*
NDP	*Neighbor Discovery Protocol*
NGTRANS	*Next Generation Transition*
NNTP	*Network News Transfer Protocol*
OSI	*Open Systems Interconnection*
PAN	*Personal Area Network*

PPP	*Point-to-Point Protocol*
QoS	Qualidade de Serviços
RARP	*Reverse Address Resolution Protocol*
RFC	*Request For Comments*
RTP	*Real Time Protocol*
SIIT	*Stateless IP/ICMP Translation Algorithm*
SLIP	*Serial Line Internet Protocol*
SMTP	*Simple Mail Transfer Protocol*
SNA	*System Network Architecture*
SNMP	*Simple Network Management Protocol*
SNMPv3	*Simple Network Management Protocol version 3*
ST2	*Straems 2*
TCP	*Transmission Control Protocol*
TELNET	*Telecomunications Network*
TEP	*Tunnel End Point*
TRT	*Transport Relay Translator*
UDP	*User Datagram Protocol*
UML	*Unified Modeling Language*
UNESC	Universidade do Extremo Sul Catarinense
WAN	*Wide Area Network*
WWW	*World Wide Web*
XNS	*Xerox Network System*

SUMÁRIO

1 INTRODUÇÃO

No mundo globalizado em que se vive hoje, a cada dia se acelera a corrida por novas tecnologias e formas de inovar os serviços utilizados atualmente. É também cada vez menor o grupo de indivíduos que não tem acesso a algum meio de informação. O que mais tem se desenvolvido entre eles, e que se difunde cada vez mais em proporções enormes, tanto em infra-estrutura quanto em número de usuários, é a rede mundial de computadores (Internet).

A indústria de Redes percebe cada dia mais claramente a necessidade de substituição do atual protocolo de Internet, o IPv4, pois, com o crescimento que a Internet atingiu atualmente, surgiu a necessidade de um protocolo que mantenha a estrutura global do IPv4, mas solucionando suas deficiências. As exigências por mais espaço de endereçamento, o controle e o desígnio de um endereço mais simples na camada IP, melhor suporte a QoS, maior segurança, e um número crescente de tipos de mídia e dispositivos com acesso a Internet, por exemplo, foram fatores que contribuíram e têm contribuído para o desenvolvimento do IPv6.

Roteadores atuais possuem implementado mecanismos que permitem que os dois protocolos co-existam entre si e se comuniquem. Este trabalho visa a realização de um estudo sobre os protocolos IPv4 e IPv6, bem como um estudo sobre os mecanismos de transição possíveis e desenvolvidos até o momento.

Deste modo com o intuito de aplicar os conceitos de IPv4, IPv6 e mecanismos de transição e convivência dos protocolos de comunicação desenvolveu-se uma interface de apoio ao estudo dos mecanismos de transição, para facilitar o entendimento dos mesmos, já que é um assunto bastante complexo.

1.1 OBJETIVO GERAL

Realizar o estudo da transição entre os protocolos de comunicação IPv4 e IPv6, e desenvolver uma interface de apoio ao estudo destes mecanismos de transição e convivência.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos abordados para contemplar o objetivo geral são:

a) compreender os protocolos de comunicação;
b) definir as características e benefícios do IPv6 com relação ao IPv4;
c) compreender a arquitetura de endereçamento dos protocolos, descrevendo suas hierarquias e estruturas;
d) entender os mecanismos de transição e seus métodos;
e) realizar um estudo dos três mecanismos de transição dos protocolos existentes;
f) desenvolver uma interface de apoio ao estudo dos protocolos de comunicação IPv4 e IPv6, além de seus mecanismos de transição.

1.3 JUSTIFICATIVA

Tem-se observado no mundo o crescimento exponencial da rede de computadores, com isso originou uma enorme requisição de novos serviços.

As exigências por mais espaço de endereçamento, o controle e o desenvolvimento de um endereço mais simples na camada IP, para um melhor suporte a Qualidade de Serviços (QoS), maior segurança, um número crescente de tipos de mídia e dispositivos com acesso a Internet têm contribuído para o desenvolvimento do IPv6. Portanto, cada vez mais será necessário o entendimento das funcionalidades, bem como, conhecer como estão acontecendo as transições, comunicações e uso do novo protocolo que promete se expandir cada vez mais nas redes futuras (COMER, 2001).

Estas comunicações e manipulações de pacotes de informação engloba vários requisitos e detalhamentos na rede. Por esse motivo sentiu-se a necessidade de desenvolver uma interface de apoio ao estudo, para facilitar o aprendizado e entendimento da comunicação entre protocolos usando mecanismos de transição.

Esta interface, num primeiro momento, possuirá implementados os módulos de informações sobre o IPv4, IPv6 e os mecanismos de transição com seus métodos correspondentes, além de um breve resumo e informações sobre a ferramenta e o estudo no ícone “ajuda.”.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por 7 capítulos. No capítulo 1 encontra-se uma contextualização ao tema proposto, bem como os objetivos e justificativas para realização deste trabalho.

Nos capítulos 2 e 3, são abordados os conceitos fundamentais de redes de computadores e modelos de referência, indispensáveis para o entendimento do trabalho.

Os capítulos 4 e 5 descrevem respectivamente as características dos protocolos IPv4 e IPv6, seus endereçamentos, cabeçalhos, datagramas, mensagens ICMP e diferenças entre os protocolos.

No capítulo 6 são apresentados os mecanismos de transição disponível que podem ser usados para possibilitar a transição e convivência dos protocolos IPv4 e IPv6.

Enquanto no capítulo 7 apresenta o trabalho desenvolvido, sendo descrito os passos de todo o processo de desenvolvimento desta pesquisa, bem como apresenta as funções da interface implementada, dificuldades na construção e resultados obtidos.

E por fim, tem-se a conclusão, onde encontra-se também algumas sugestões para trabalhos futuros e as referências bibliográficas citadas e consultadas para o desenvolvimento de toda esta pesquisa.

2 REDES DE COMPUTADORES

Uma rede de computadores é formada por um conjunto de dispositivos capazes de se comunicar através do sistema de comunicação por troca de informações e compartilhar recursos, interligados por um sistema de comunicação, ou seja, segundo Tanenbaum (1997), uma rede de computadores é um conjunto de computadores autônomos interconectados. Dois ou mais computadores são ditos “interconectados” quando podem trocar informações.

Existem características que diferenciam os sistemas distribuídos e redes de computadores, que geralmente vários autores fazem confusão com estes dois termos.

Segundo Tanenbaum (1997), a principal diferença é que nos sistemas distribuídos, o usuário não tem conhecimento da existência de diversos computadores autônomos ligados uns aos outros, ou seja, em um sistema distribuído o usuário não tem consciência de que há diversos processadores. Portanto, neste caso, nada é visível, tudo é feito automaticamente pelo sistema, sem o conhecimento do usuário.

Numa rede, os usuários precisam conectar-se por si próprios com uma máquina, submeter-se às tarefas remotas e movimentar os arquivos. Entretanto, os dois assuntos possuem uma série de pontos em comum, pois os dois precisam movimentar arquivos. Sua diferença está em quem faz a movimentação, se é o sistema ou o usuário.

Segundo Soares, Lemos e Colcher (1995), o sistema de comunicação constitui-se de um arranjo topológico interligando os vários módulos processadores, que se referem à dispositivos capazes de comunicar através do sistema de comunicação por troca de mensagens, através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).

Segundo Tanenbaum (2003), existem algumas razões econômicas e tecnológicas para a instalação de redes de computadores, como:

a) **compartilhamento de recursos:** disponibilizar todos os programas, recursos e dados a todos os usuários da rede, independentemente da localização física dos recursos e dos usuários. Em outras palavras, o fato dos usuários estarem distantes dos dados não impede de usá-los e manipula-los como se estivessem armazenados no próprio computador;

b) **aumento de confiabilidade:** viabilizar fontes alternativas de fornecimento de recursos. Por exemplo, arquivos podem ser salvos em três computadores diferentes e assim, se um deles falhar (por problemas de hardware), o arquivo poderá ser obtido de um dos outros dois computadores, além de que se uma das CPU falhar as outras podem assumir as funções mesmo que tenha uma queda de desempenho;

c) **economia de dinheiro:** a relação custo/desempenho dos computadores de pequeno porte é muito melhor do que a dos computadores de grande porte, considerando que computadores de grande porte são dezenas de vezes mais rápidos, porém, são milhares de vezes mais caros;

d) **escalabilidade:** possibilitar o aumento gradual do desempenho do sistema à medida que cresce o volume de carga, bastando para tal, que se adicionem mais processadores;

e) **meio de comunicação:** uma rede de computadores representa um meio de comunicação altamente eficaz e rápida para funcionários que trabalham em locais muito distantes uns dos outros, aumentando assim, o espírito de equipe entre grandes grupos de pessoas.

Estas características têm impulsionado buscas de tecnologias constantes na área de redes e cada vez mais a comunicação entre as pessoas deve ganhar importância em relação ao aumento da confiabilidade.

Além destas razões citadas acima, pode-se citar outros motivos para a interconexão como (TANENBAUM, 2003):

a) **acesso às informações remotamente:** realização de transações financeiras e comércio eletrônico;
b) **comunicação pessoa a pessoa:** uso de correio eletrônico permite usuários remotos se comunicarem instantaneamente, vendo e ouvindo uns aos outros;
c) **entreterimento:** possibilidade de vídeo sob demanda e jogos interativos.

A partir deste momento será desviada a atenção das aplicações e dos aspectos sociais das redes para tratar das questões técnicas relacionadas à rede. Estas questões técnicas serão divididas em duas etapas: hardware de rede e software de rede.

2.1 HARDWARE DE REDE

Segundo Tanenbaum (2003), em redes de computadores não há uma classificação definida que poderíamos utilizar, porém, existem duas dimensões gerais nas quais pode-se classificá-las: a tecnologia de transmissão e a escala.

A tecnologia de transmissão se divide em dois tipos (TANENBAUM, 2003):

a) **redes de difusão (*broadcasting*):** possuem apenas um canal de comunicação que é compartilhado por todas as máquinas. Entretanto,

existe um campo de endereço dentro do pacote que especifica o destino da mensagem. Alguns sistemas de difusão também aceitam transmissão para um conjunto de máquinas que é conhecido como uma multidifusão (*multicasting*);

b) **redes ponto a ponto (*unicasting*):** consistem em várias conexões entre pares individuais de máquinas, sendo que um pacote para ir da origem para o destino, tenha de visitar uma ou mais máquinas intermediárias.

As redes de computadores podem ser divididas em locais, metropolitanas, geograficamente distribuídas, controle e pessoais. A seguir será feita uma breve abordagem da dimensão relacionada à escala.

2.1.1 *Local Area Network* (LAN)

Conhecidas também como redes locais caracterizam-se como sendo redes que permitem a interconexão de equipamentos de comunicação de dados numa pequena região. São bastante usadas para conectar computadores pessoais, escritórios e instalações industriais, tornando possível o compartilhamento de recursos de hardwares e trocas de informações (SOARES; LEMOS; COLCHER, 1995).

As LAN comuns, geralmente, são executadas a velocidades que pode variar de 10, 100, 1000 e 10000 Mbps, com baixo retardo, altas taxas de transmissão e cometem poucos erros, sendo que em LAN’s mais modernas, estas velocidades podem ser maiores. Geralmente são de propriedade privada (SOARES; LEMOS; COLCHER, 1995).

2.1.2 *Metropolitan Area Network* (MAN)

São redes também conhecidas como redes metropolitanas. Este termo surge com o aparecimento do padrão IEEE 802.6, ou *Distibuted Queue Dual Bus* (DQDB)[1], que nada mais é do que um padrão especial. Apresenta características semelhantes às das redes locais, sendo que as MAN's, em geral, cobrem distâncias maiores do que as LAN's operando em velocidades maiores (SOARES; LEMOS; COLCHER, 1995).

Este tipo de rede possui a capacidade de transformar dados em voz. Uma MAN não contém elementos de comutação capazes de transmitir pacotes através de uma série de linhas de saídas e tem apenas um ou dois cabos. Podem ser públicas ou privadas.

2.1.3 *Wide Area Network* (WAN)

Estas redes conhecidas como redes geograficamente distribuídas, surgiram das necessidades de se compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos (SOARES; LEMOS; COLCHER, 1995).

São redes que contém um grupo de máquinas que tem a finalidade de executar os programas do usuário. Por exemplo, define-se essa máquina de ***host***. Os ***hosts*** são conectados por uma **sub-rede**, que por sua vez possui a tarefa de transportar mensagens de um ***host*** para outro. Esta estrutura de rede é bastante simplificada, pois separa os aspectos de aplicação (os *hosts*) dos aspectos pertencentes à rede (a sub-rede) (TANENBAUM, 2003). Tais redes são em geral públicas.

[1] DQDB proporciona duas formas de comunicação integrada: a comutação de circuitos e comutação de pacotes.

2.1.4 *Controller Area Network* (CAN)

São redes de controle de área que abrangem um espaço proporcional as LAN dependendo do uso. Por ser uma rede baseada em sistemas em que a informação é transmitida em tempo real, exige um controle rígido de erros e garantia de recebimento de mensagens (KRISHNAMURTHY; REXFORD, 2001)

As CAN's possuem características como prioridade de mensagens, consistência dos dados, flexibilidade de configuração, detecção e sinalização de erros dentre outras. Com isso as CAN's vêm sendo utilizadas em aplicações industriais apresentando autos índices de sucesso (KRISHNAMURTHY; REXFORD, 2001).

2.1.5 *Personal Area Network* (PAN)

As redes de área pessoal é uma rede de computadores pessoais, formadas por dispositivos conectados próximos ao usuário. Estes dispositivos podem ser pertencentes ao usuário ou não (KRISHNAMURTHY; REXFORD, 2001).

Por exemplo, imagina-se um computador portátil conectando-se a um outro e este a uma impressora. Esta tecnologia é o mesmo que uma as redes locais, porem a diferença é que as PAN apresentam pouca possibilidade de crescimento pois é destinada à utilização doméstica.

2.2 SOFTWARE DE REDE

Segundo Tanenbaum (2003), para que a estrutura das redes ficasse mais simples, a maioria das redes foi organizada como uma série de camadas ou níveis que

são colocados um em cima do outro. O objetivo de cada camada é oferecer determinados serviços para as camadas superiores, ocultando detalhes de implementação desses recursos.

Um protocolo se define como sendo um conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas (TANENBAUM, 2003).

Portanto, um protocolo é basicamente um conjunto de regras que controla o formato e o significado dos quadros, pacotes, ou mensagens trocadas pelas entidades pares contidas em uma camada.

Segundo Tanenbaum (2003), um serviço é um conjunto de primitivas (operações) que uma camada oferece para a camada imediatamente acima dela. Os serviços podem ser de dois tipos:

a) **serviço orientado à conexão:** o usuário estabelece uma conexão, usa a conexão e em seguida libera a conexão;
b) **serviço sem conexão:** cada mensagem possui o endereço destino completo e cada um deles é roteado através do sistema independente de todos os outros.

Os serviços são classificados também pela sua Qualidade de Serviço (QoS) que é a garantia de que uma mensagem chegue com o mesmo formato original ao seu destino.

Já as operações podem ser: *Request*, *Indication*, *Response* e *Confirm*. Os elementos ativos em cada camada são freqüentemente chamados de entidades. As entidades de um mesmo nível/camada que se encontra em diferentes máquinas são chamadas de pares (*peers*) e a comunicação entre os pares é feita usando o protocolo da camada (SOARES; LEMOS; COLCHER, 1995).

Entre cada par há uma interface que define as operações e os serviços que a camada inferior tem a oferecer a camada superior. Para compreender melhor este processo analise a Figura 01.

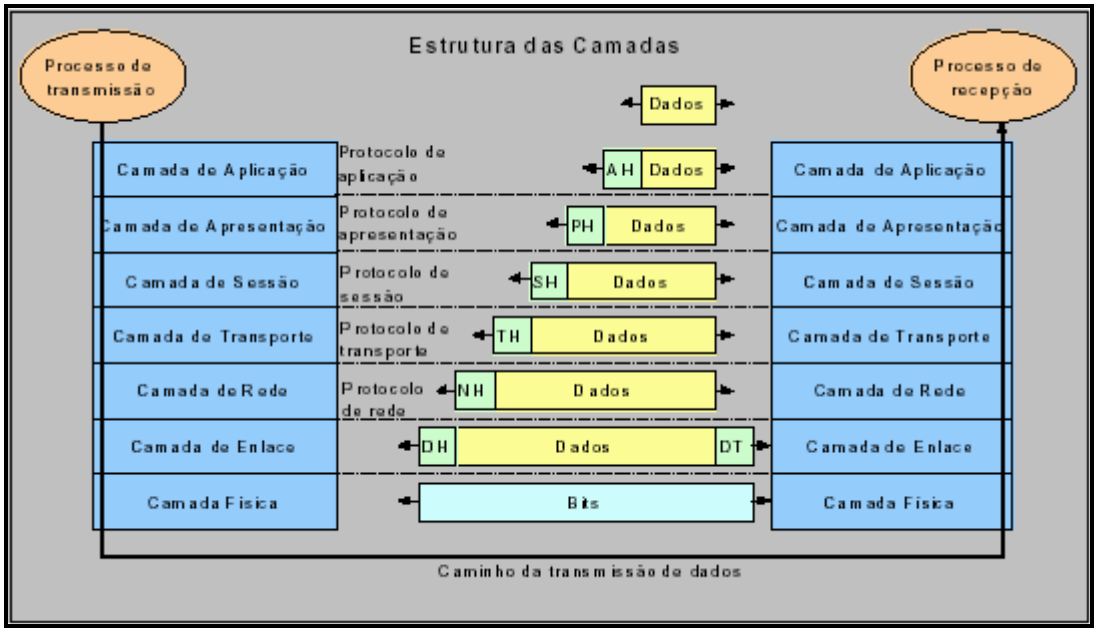

Figura 01. Estrutura das camadas
Fonte: Adaptado de TANENBAUM, A. (2003).

Na verdade os dados não são transmitidos da camada *n* do emissor para a camada *n* do receptor. Cada camada transfere os dados e informações de controle para a camada logo abaixo dela até chegar à última camada, sendo que abaixo desta camada está o meio físico onde acontece a comunicação propriamente dita. Quando chega ao receptor realiza-se o processo inverso.

Portanto, um conjunto de camadas de protocolos é chamado de arquitetura de rede, e uma lista de protocolos usados por um determinado sistema, um protocolo por camada, é chamado de pilha de protocolos.

O uso das redes de computadores é muito comum e necessário quando se trata de manipulação de informações e principalmente no que diz respeito à comunicação com trocas de arquivos entre organizações e pessoas.

A seguir será feita uma abordagem das arquiteturas de redes com destaque os modelos de referência muito conhecidos: o modelo de referência OSI e o modelo de referência TCP/IP.

3 MODELOS DE REFERÊNCIA

Após ter feito uma breve descrição de conceitos de redes divididas em camadas, é importante conhecer duas importantes arquiteturas de redes: o modelo de referência OSI e o modelo de referência TCP/IP.

Segundo Amentt, Dulaney e Harper (1997), um modelo de referência define-se sendo uma arquitetura estabelecida de modo a possibilitar uma maior compatibilidade entre diferentes plataformas.

3.1 MODELO DE REFERÊNCIA OSI

Segundo Pinheiro (2004), para atender o objetivo de facilitar o processo de padronização e obter interconectividade entre máquinas de diferentes fabricantes, a *International Standards Organization* (ISO), no início da década de 1980, aprovou um modelo de arquitetura para sistemas abertos, visando permitir a comunicação entre máquinas e definindo padronizações para a construção de redes de computadores independente da tecnologia de implementação.

Desde então, esse modelo foi denominado *Open Systems Interconnection* (OSI), servindo de base para a implementação de qualquer tipo de rede. Veja na Figura 02, as camadas do modelo OSI.

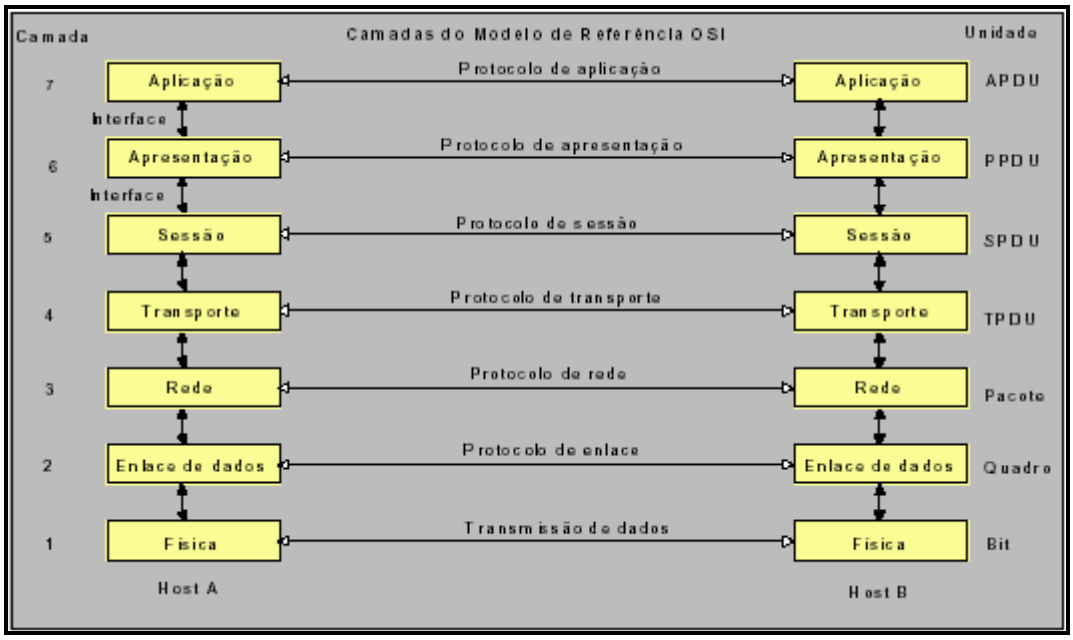

Figura 02. Modelo de Referência OSI
Fonte: Adaptado de TANENBAUM, A. (2003).

Veja a seguir as funções específicas que cada camada é responsável (PINHEIRO, 2004):

a) **física:** trata da transmissão de bits brutos através de um canal de comunicação. As funções dos protocolos deste nível são fazer com que um bit "1" transmitido seja entendido pelo receptor como bit "1" e não como bit "0";

b) **enlace:** transforma um canal de transmissão de dados brutos em uma linha que pareça livre dos erros de transmissão não detectados na camada de rede;

c) **rede:** especifica o modo como os pacotes são roteados da origem para o destino e possui as funções de rotear pacotes entre fonte e destino, controlar congestionamento e contar o número de pacotes ou *bytes* utilizados pelo usuário, para fins de tarifação;

d) **transporte:** sua principal função é realizar a divisão dos dados em pacotes de tamanhos compatíveis com a camada de rede a ser utilizada e, reagrupá-los sem erros na outra extremidade. Esta é a verdadeira

camada fim-a-fim que liga a origem ao destino através da resolução de seus endereços e nomes. É também a camada responsável pelo estabelecimento das conexões e pelo controle de fluxos;

e) **sessão:** permite que usuários de diferentes máquinas estabeleçam sessões entre si. Suas funções são administrar e sincronizar diálogos entre dois processos de aplicação;

f) **apresentação:** preocupa-se com a sintaxe e a semântica das informações transmitidas, como por exemplo, a codificação dos dados de acordo com o padrão estabelecido. Suas funções são de assegurar que a informação seja transmitida de tal forma que seja entendida e usada pelo receptor, representação da criptografia e compressão dos dados;

g) **aplicação:** possui o maior número de protocolos por estar mais perto do usuário e os mesmo possuírem necessidades diferentes. Possui aplicações específicas para o protocolo, tais como transferência de arquivos, gerência de rede, dentre outras.

3.2 MODELO DE REFERÊNCIA TCP/IP

Segundo Kurose e Ross (2005), com o projeto ARPANET[2], da *Department of Defense Advanced Research Projects Agency* dos EUA (DARPA), em 1969 começou-se o desenvolvimento do protocolo TCP/IP, com o objetivo de desenvolver uma rede que interligasse os computadores do governo americano, de diferentes fabricantes e utilizando diferentes sistemas operacionais. Essa rede era usada para fins militares, sendo que era descentralizada e se um dos computadores dessa rede fosse

[2] ARPANET foi a primeira rede operacional de computadores à base de comutação de pacotes e o precursor da internet.

destruído num ataque, os demais continuariam funcionando graças a um mecanismo de rotas alternativas.

Algum tempo depois desse início com finalidade militar, a *National Science Foundation* criou uma rede semelhante para interconectar instituições de pesquisa e universidade, utilizando os mesmos protocolos da rede ARPANET.

Desses projetos surgiu o protocolo TCP/IP que serviu como base para a construção da rede que hoje se conhece como Internet.

A partir de 1993 a Internet ficou disponível para uso comercial e se popularizou de tal forma que hoje a maioria das pessoas a utiliza com familiaridade (KUROSE; ROSS, 2005).

Segundo Kurose e Ross (2005), a arquitetura Internet TCP/IP é organizada em quatro camadas conceituais, conforme Figura 03. TCP/IP é uma nomenclatura para o termo *Transmission Control Protocol/Internet Protocol*, ou seja, é um conjunto de protocolos, onde dois dos mais importantes (o TCP e o IP) deram seus nomes à arquitetura.

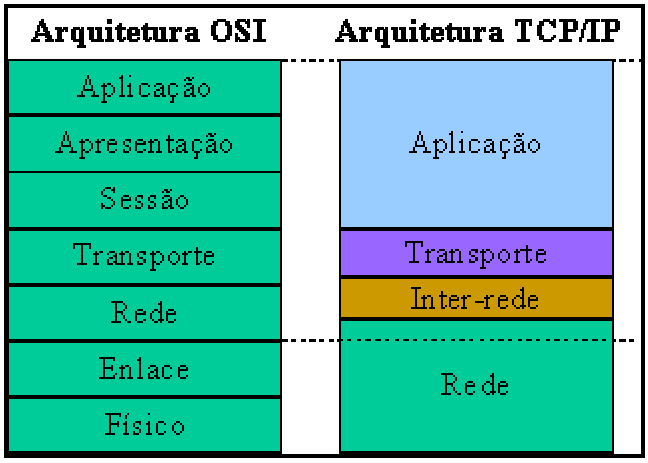

Figura 03. O modelo de referência TCP/IP
Fonte: Adaptado de TANENBAUM, A. (2003).

A Figura 03 ilustra as camadas OSI e as Camadas TCP/IP lado a lado para facilitar a visualização e comparação entre as duas arquiteturas.

A seguir, serão descritas as funções de cada camada TCP/IP, seus protocolos em específico e seu funcionamento.

3.2.1 Camada de Aplicação

Segundo Krishnamurthy e Rexford (2001), a Camada de Aplicação descreve os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário, além de administrar detalhes de uma aplicação em particular.

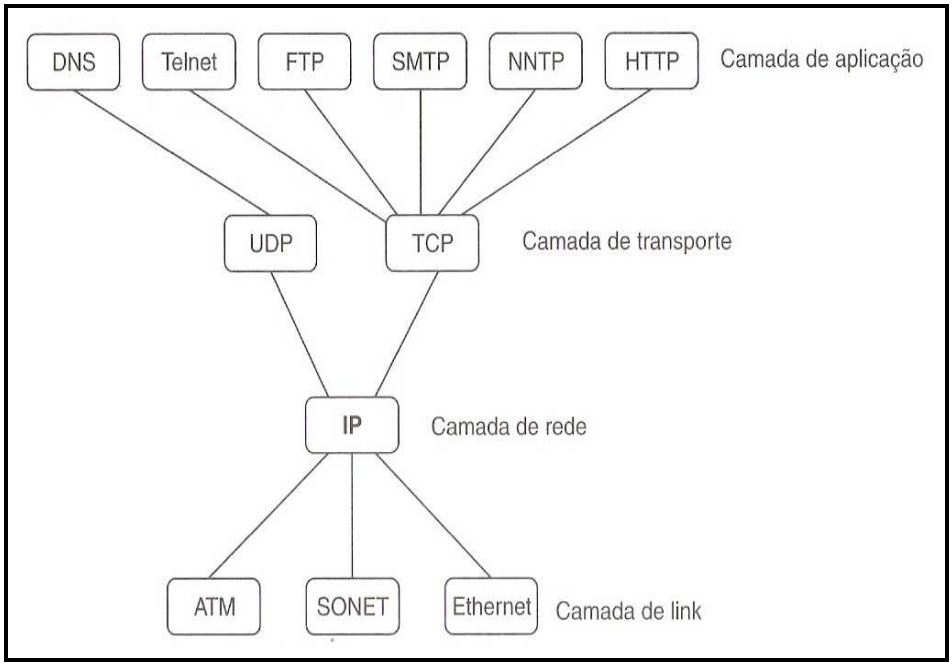

Figura 04. Disposição de protocolos em camadas
Fonte: Adaptado KRISHNAMURTHY, B.; REXFORD, J. (2001).

Conforme a Figura 04, existem muitos serviços TCP/IP disponibilizados na camada de aplicação, sendo que os mais importantes são (MOURA ET AL, 1999):

a) ***Simple Mail Transfer Protocol*** **(SMTP):** fornece serviço de correio eletrônico global que tenha suporte a diferentes tipos de sistemas localizados em diferentes estações;

b) ***Domain Name Service*** **(DNS):** fornece serviços de tradução de nomes e diretórios. Este protocolo será mencionado com maior ênfase nos

capítulos 4 e 5 onde serão descritos os protocolos IPv4, IPv6 e os mecanismos de transição ;

c) ***File Transfer Protocol* (FTP):** fornece serviço de trocas de arquivos entre computadores;

d) ***Telecomunications Network* (TELNET):** fornece serviços de terminais virtuais;

Segundo Comer (1999), pode-se separar os protocolos de aplicação em protocolos de serviços básicos ou protocolos de serviços para o usuário:

a) **protocolos de serviços básicos:** que fornecem serviços para atender as próprias necessidades do sistema de comunicação TCP/IP: DNS, BOOTP, DHCP;

b) **protocolos de serviços para o usuário:** TELNET, FTP, SMTP, SNMP, NNTP, HTTP, RTP.

3.2.2 Camada de Transporte

Segundo Moura et al (1999), a Camada de Transporte permite o estabelecimento de conexões fim-a-fim, além de suportar o fluxo de dados entre dois computadores, garantindo a qualidade de serviço para a camada de aplicação.

Na camada de transporte existem dois protocolos fim-a-fim definidos (MOURA ET AL, 1999):

a) ***Transmission Control Protocol* (TCP):** protocolo orientado a conexão, fornece fluxo de dados confiável, retransmite pacotes perdidos, elimina pacotes duplicados, fornece avisos de recebimento. Além destas características, o protocolo TCP fornece a confiabilidade necessária para

os mecanismos de comunicação em meios pouco confiáveis, onde podem ocorrer, perdas, destruição, duplicação ou a desordenação de pacotes;

b) ***User Datagram Protocol*** **(UDP):** fornece uma interação sem conexão, não confiável por não se preocupa com perdas de pacotes e confirmação de recebimento. Servidores que utilizam serviços de transporte UDP são do tipo interativo, existindo poucas exceções, além de fornecer um serviço com baixa taxa de *overhead* para transações sem conexão e não confiável.

3.2.3 Camada de Inter-rede

Segundo Tanenbaum (2003) a Camada de Rede integra toda a arquitetura. Sua função é permitir que qualquer *host* lance pacotes pela rede e garantir que eles sejam transmitidos independentes do local de destino. A comunicação é realizada através do protocolo IP. Para identificar cada máquina e a rede onde estão situadas, é definido um identificador, chamado endereço IP. Os protocolos existentes nesta camada são definidos da seguinte forma (MOURA ET AL, 1999):

a) ***Internet Protocol*** **(IP):** principal protocolo desta camada, usado tanto pelo TCP como pelo UDP. Sua função é fornecer serviço de identificação e de transporte de dados. Atualmente é usado na maioria das redes o IPv4, mas já está em uso e em fase de transição o novo protocolo IP (o IPv6), que serão abordados no capítulo 4 e 5;

b) ***Internet Control Message Protocol* (ICMP):** sua função é tratar erros e controlar erros. Também pode ser usado para informar ao remetente sobre rotas preferidas ou sobre congestionamento na rede;

c) ***Internet Group Message Protocol* (IGMP):** protocolo de controle de grupos de endereços.

Para que os pacotes possam ser passados de um *hos*t a outro são utilizados roteadores que se baseiam nos endereços IP em cada pacote.

3.2.4 Camada de Rede

A Camada de Rede é responsável pela transmissão de dados por um meio físico chamado meio de comunicação. Os principais protocolos desta camada são (MOURA ET AL, 1999):

a) ***Address Resolution Protocol* (ARP):** fornece a tradução automática de endereços IP para endereços físicos;

b) ***Reverse Address Resolution Protocol* (RARP):** utilizado para permitir que estações de trabalho aprendam o seu endereço IP quando são ligadas;

c) ***Serial Line Internet Protocol* (SLIP):** constitui uma maneira simples de encapsulamento de pacotes IP por meio de interfaces seriais;

d) ***Point-to-Point Protocol* (PPP):** corrige as deficiências de compartilhamento de linha, correção de pacotes corrompidos e conhecer com antecedência o endereço IP de seu par, que existem no SLIP.

Os protocolos ARP e RARP são usados somente com alguns tipos de interface e convertem os endereços da camada IP em endereços usados fisicamente pela interface de rede.

Estes modelos são a referência para a configuração e implantação de um sistema de redes capaz de facilitar a troca de informações usando protocolos de comunicação que serão abordados logo a seguir nos capítulos 4 e 5.

Até esta etapa da pesquisa foi abordada a estrutura geral das redes de computadores como: tipos de redes, modelos de referência, além de vários protocolos e funções que atuam diretamente no funcionamento operacional desta grande “teia” que é a rede mundial de computadores (Internet).

No capítulo a seguir, será feita uma abordagem mais detalhada do protocolo que identifica cada *host* nesta grande rede. A rede de computadores (Internet) funciona que nem o tradicional correio. Para que o carteiro entregue as correspondências para as pessoas corretas é necessário que cada pessoa tenha um endereço, o que não é diferente na Internet, onde cada *host* que quiser comunicar-se com outras máquinas precisam ter um endereço e este é o endereço IP. O IPv4 é o atual protocolo em maior uso na Internet.

4 O PROTOCOLO IPv4

A partir deste capítulo será dada uma atenção especial aos protocolos IP, exemplificando e comentando sobre seu funcionamento, características próprias, formas de endereçamento, entre outros.

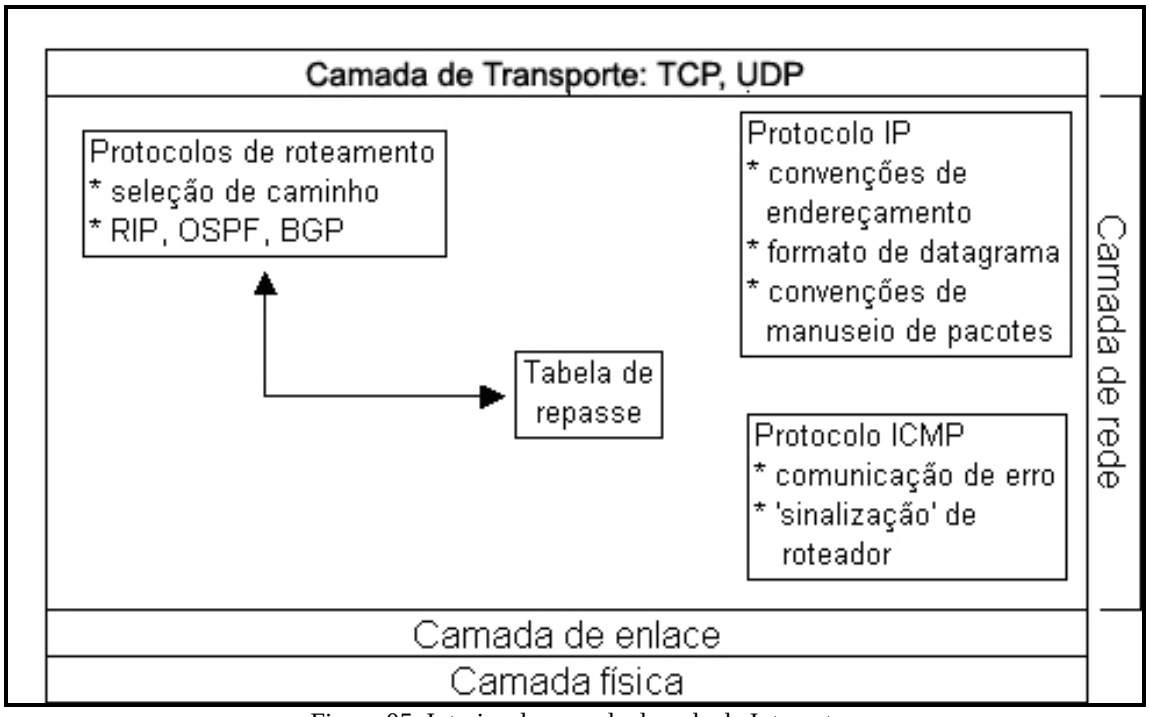

Figura 05. Interior da camada de rede da Internet
Fonte: Adaptado de KUROSE, J.; ROSS, K. (2005).

Conforme a Figura 05, a camada de rede possui três componentes importantes: o protocolo IP, o componente de roteamento (que determina o caminho que um datagrama segue desde sua origem até seu destino) e o terceiro componente é o *Internet Control Message Protocol* (ICMP), que realiza a comunicação de erros em datagramas e atende requisições de certas informações da camada de rede.

Conceitualmente, IP é um protocolo de entrega de pacote não confiável, sendo que sua tarefa é fornecer a melhor forma de transportar datagramas de uma origem para um destino, que pode estar em outras redes. A questão de o protocolo ser considerado de entrega de pacotes não confiável é porque os pacotes enviados pelo IP podem ser perdidos, ficar fora de ordem ou serem duplicados (TANENBAUM, 2003).

4.1 O FORMATO DO DATAGRAMA DO IPv4

Segundo Tanenbaum (2003), cada versão do protocolo IP possui seu datagrama, sendo que o mesmo consiste em duas partes: cabeçalho e texto. O cabeçalho possui uma parte fixa de 20 *bytes* e uma parte opcional de tamanho variável. Na Figura 06 pode-se observar que o cabeçalho é transmitido na ordem da esquerda para a direita, sendo que o primeiro é o bit do campo versão.

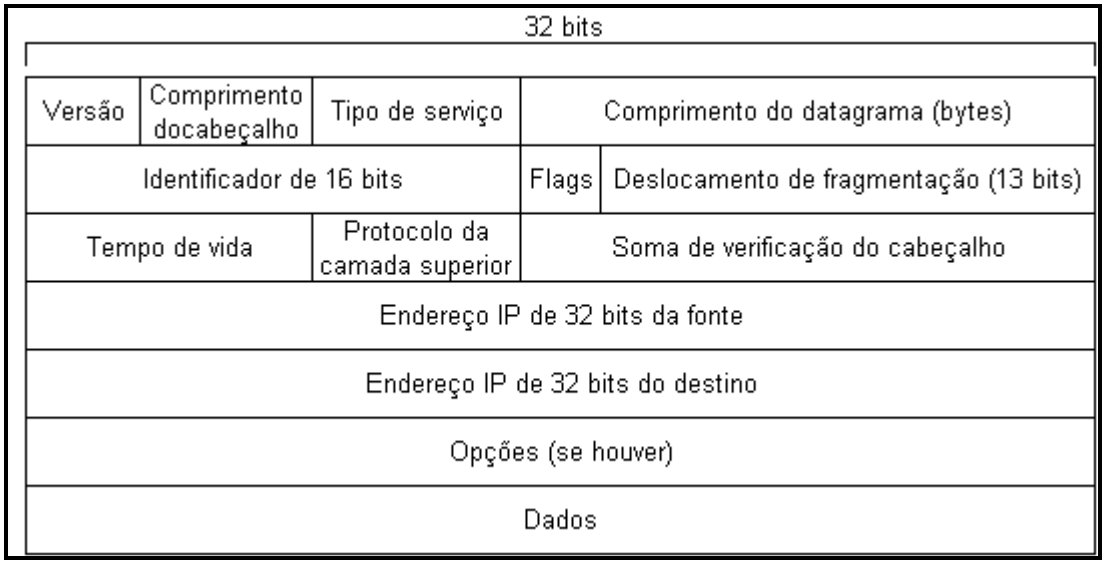

Figura 06. Formato do datagrama IPv4
Fonte: Adaptado de Kurose, J.; Ross, K. (2005).

Portanto, cada campo composto na Figura 06 possui suas características e funções próprias. São elas (DARPA 1981):

a) **versão:** é composto de quatro *bits*, sendo que estes especificam a versão do protocolo IP do datagrama;

b) **comprimento do cabeçalho:** são quatro *bits* que tem a responsabilidade de determinar onde os dados realmente começam. A maior parte dos datagramas IP não possui opções, no entanto, o datagrama IP comum tem um cabeçalho de 20 *bytes*;

c) **tipo de serviço:** servem para diferenciar os diferentes tipos de datagramas IP, sendo necessário diferenciá-los uns dos outros. Por exemplo, diferenciar datagramas de tempo real dos outros serviços;

d) **comprimento do datagrama:** tamanho total do datagrama, incluindo cabeçalho e dados;

e) **identificador:** permite que o *host* de destino determine a qual datagrama pertence um fragmento recém chegado;

f) ***flags*:** permite que o *host* especifique se no conjunto é mais importante o retardo, taxa de transferência ou a confiabilidade. Na teoria este campo permite que os roteadores escolha entre uma ligação de satélite, onde possui alta taxa de transferência mas com grandes retardos ou uma linha privada, com pequeno retardo e baixa taxa de transferência;

g) **deslocamento de fragmentação:** informa a que ponto do datagrama atual o fragmento pertence. Com exceção do último, todos os fragmentos de um datagrama devem ser múltiplos de 8 *bytes*;

h) **tempo de vida:** serve para garantir que os datagramas não fiquem circulando pela rede para sempre, ou seja, cada salto que o datagrama realiza de uma rede a outra é decrementado uma unidade, se este campo chegar a 0, o datagrama é descartado;

i) **protocolo:** informa o processo de transporte a ser aplicado ao datagrama, que pode ser o TCP, também o UDP e alguns outros;

j) **soma de verificação do cabeçalho:** é útil para auxiliar o roteador na detecção de erros gerados por palavras de memória danificada no mesmo;

k) **endereços IP de fonte e de destino:** indica o número da rede e o número do *host*;

l) **opções:** permite que um cabeçalho IP seja ampliado, ou seja, permitir que versões posteriores do protocolo incluam informações, possibilitando experiências de novas idéias, evitando a alocação de bits de cabeçalho para informações raramente necessárias;

m) **dados:** esta é a razão da existência do datagrama. Muitas vezes este campo contém o segmento da camada de transporte (TCP ou UDP) a ser entregue ao destino. Portanto este campo pode carregar outros tipos de dados com mensagens ICMP, assunto que será tratado adiante.

Para o IPv4 um datagrama pode possuir de um único octeto de dados até octetos de 64 K, incluindo cabeçalho. Resumidamente, um pacote enviado através de uma rede TCP/IP é chamado de datagrama IP, sendo que cada datagrama consiste em um cabeçalho seguido de dados. Os endereços de origem e destino no cabeçalho do datagrama são IP.

Mas nem sempre os pacotes possuem um tamanho certo e pronto para ser transportados. Veja a seguir o que acontece neste caso.

4.1.1 A fragmentação e remontagem do datagrama

Cada tecnologia de rede, geralmente, possui sua própria restrição quanto ao tamanho que um pacote pode ter para transporte. Esta situação leva a existir duas opções para o modelo de serviço IP: ter certeza que os datagramas possuem tamanhos pequenos e que cabem dentro de um pacote em qualquer tecnologia de rede, ou oferecer um meio em que quando os pacotes forem muito grandes para determinada tecnologia,

os pacotes possam ser fragmentados e posteriormente remontados (PETERSON; DAVIE, 2004).

Para por em prática a segunda opção, a idéia é que cada rede tenha uma Unidade Máxima de Transferência (MTU), que é o maior datagrama que o IP pode transportar em um quadro. Porém, quando um *host* envia um datagrama, ele pode escolher o tamanho que desejar. Sendo assim a fragmentação só será necessária se o caminho até o destino for uma MTU menor, ou seja, se o protocolo de transporte der ao IP um pacote maior que a MTU local, a opção do *host* é realizar a fragmentação.

Segundo Peterson e Davie (2004), normalmente a fragmentação ocorre em um roteador que identifica um datagrama que possui uma MTU menor que o datagrama recebido. Para que os datagramas possam ser remontados no destino, todos eles recebem uma identificação no campo identificador que é escolhido pelo *host* de envio, sendo que eles são exclusivos entre todos os datagramas. O IP não recupera fragmentos faltantes, então se nem todos os fragmentos chegarem ao destino, o *host* abandonará o processo de remontagem e ignora os fragmentos que chegarem.

Para que o *host* destino saiba que recebeu o último fragmento do datagrama original, o último datagrama tem um bit de *flag* ajustado para o valor 0, sendo que todos os outros fragmentos possuem um bit de *flag* ajustado para 1.

4.2 OS ENDEREÇOS IP

Para ser capaz de identificar um *host* na Internet, cada computador da rede precisa de um endereço, conhecido como endereço IP.

Conseqüentemente, os endereços IP são usados para identificar de maneira única um *host* na Internet, sendo que ele identifica uma interface que é capaz de enviar e

receber datagramas IP. Segundo Kurose e Ross (2005), este endereço (IPv4) é formado por 32 bits (4 bytes), sendo possível um total de 2^{32} endereços. O endereço IP é representado pelos 4 *bytes* separados por . (ponto) e representados por números decimais. Desta forma o endereço IP: 11000001 00100000 11011000 00001001 é representado por 193.32.216.9.

O endereço IP identifica tanto uma rede que a estação está conectada, quanto a estação a que se refere.

Segundo Comer (2001), como o endereço IP possui tamanho fixo, uma solução que os projetistas de redes encontraram foi dividí-lo em duas metades: dois *bytes* para identificar a rede e dois para a estação.

Para dividir o endereçamento IP em redes e estações, foram definidas algumas classes. Logo a seguir, na Figura 07, será mostrada a divisão das classes e um breve comentário sobre cada uma delas.

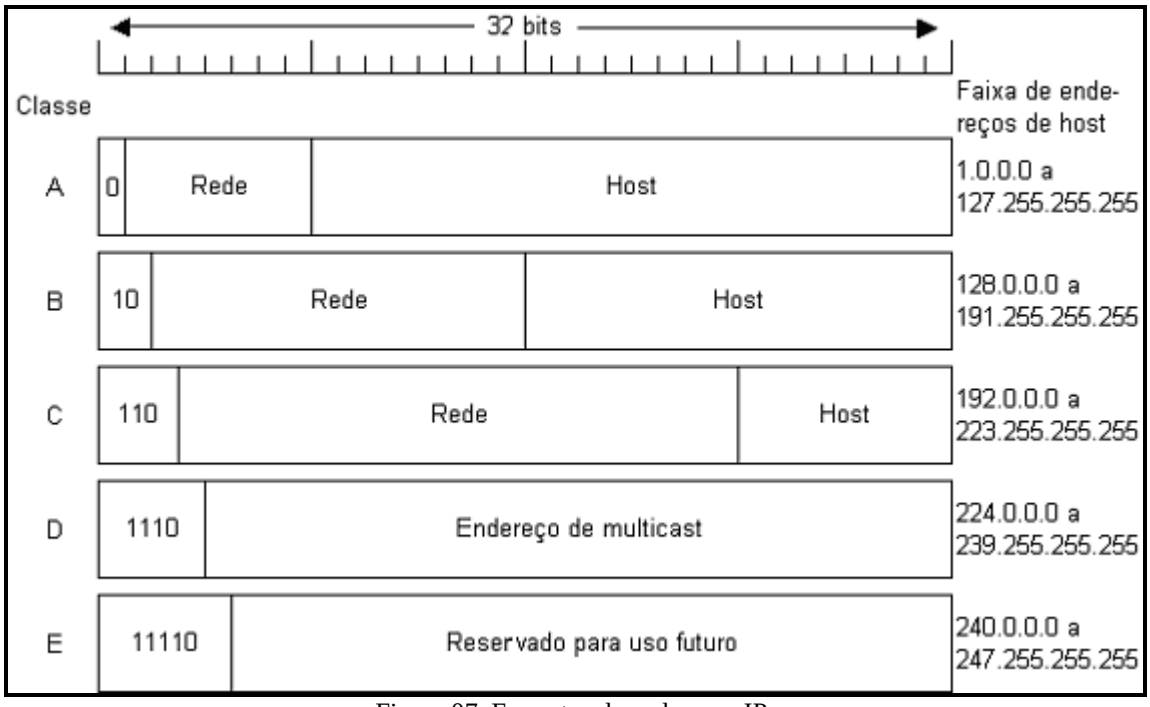

Figura 07. Formatos de endereços IP
Fonte: Adaptado de TANENBAUM, A. (2003).

O endereçamento da classe A, possui uma identificação de rede de 1 *byte* e de máquina com 3 *bytes*. Com isso é possível endereçar até 256 redes com 2^{24} estações.

Já na classe B utiliza-se 2 *bytes* para rede e 2 *bytes* para estação, enquanto um endereço de classe C utiliza 3 *bytes* para rede e 1 byte para estação. Conforme a Figura 7, para permitir a distinção de uma classe de endereço para outra, utiliza-se os primeiros bits do primeiro *byte* (TANENBAUM, 1997).

Os endereços de classe D são reservados para *multicasting*, ou seja, um tipo de transmissão com área limitada, e usada apenas para *hosts* que estejam usando o mesmo endereço classe D. E os endereços E são reservados para uso futuro.

4.3 O PROTOCOLO DE CONTROLE ICMP

Quando um roteador não consegue passar adiante um datagrama recebido, por estar congestionado demais ou por ter zerado o campo tempo de vida, ele precisa informar o transmissor do datagrama que ocorreu um erro. Para informar este tipo de erro é usado o protocolo ICMP. É importante ressaltar que protocolo ICMP é somente um mecanismo para tratamento do erro, sendo assim ele não se preocupa em corrigir o erro e nem em verificar a integridade dos datagramas que circulam pela rede (TORRES, 2001).

A mensagem ICMP é transmitida usando um datagrama IP, e como ele não verifica se um datagrama chegou ou não ao destino, pode ocorrer a perda da própria mensagem ICMP no meio do caminho.

Para poder ter uma idéia concreta, a seguir, será descritas algumas das mensagens ICMP existentes. São elas:

a) **eco:** serve para verificar se o caminho entre o transmissor e o receptor está bom;

b) **destino inalcançável:** mensagem enviada pelo roteador em casos que não consiga entregar um determinado datagrama;

c) **congestionamento:** quando um roteador recebe um número maior de datagramas do que lhe é capaz de processar, ele pode inclusive descartar datagramas por não estar sendo capaz de recebê-los. Então o roteador envia uma mensagem de redução da velocidade de transmissão ao transmissor do datagrama descartado;

d) **redirecionamento:** as vezes o roteador verifica que na rede local existe uma rota melhor a ser usada para enviar um datagrama recebido, então ele envia uma mensagem ICMP solicitando o redirecionamento ao transmissor, enviando também o datagrama ao destino;

e) **tempo de vida excedido:** quando o campo tempo de vida é zerado, o roteador envia para a máquina transmissora uma mensagem ICMP de tempo de vida excedido.

Dentre estes existem outras mensagens ICMP, mas consideram-se estas as mais utilizadas.

Este protocolo tem mostrado-se muito eficiente no processo de comunicação até o momento, porém com o surgimento de novas tecnologias mais exigentes em segurança, comunicação em tempo real dentre outras e ao aumento de endereçamento despertou a necessidade para o desenvolvimento de uma nova versão do IP.

A partir destas requisições foi desenvolvido o IPv6 que já está sendo usado em instituições de ensino e instituto de pesquisa nacional, porém ele não é compatível com o IPv4 necessitando mecanismos de transição e convivência que permita a troca de informações em arquiteturas diferentes. Veja a seguir as especificações do IPv6 que será o provável futuro da Internet.

5 O PROTOCOLO IPv6

Atualmente, utilizamos o IP versão 4, existe uma explicação do porque do desenvolvimento da versão 6, e não da versão 5. A explicação é porque já existe a versão 5, e é conhecida como protocolo *Straems 2* (ST2). O ST2 é um protocolo utilizado em projetos experimentais de tempo real na Internet, mais especificamente para aplicações multimídia (COMER, 2001).

A base do IPv6 é o IPv4, isto é, foi criado sobre uma plataforma comprovada eficaz, o que é importante tanto para a transição entre a versão 4 e a 6, quanto para a excelência do IPv6. Porém a transição para o IPv6 não ocorrerá rapidamente, sendo que essa é uma estratégia da nova versão do protocolo, para que haja a co-existência das duas versões por muitos anos.

A atual versão do IP (IPv4), não sofreu significativas alterações desde a publicação da RFC[3]791 em 1981. Apesar de esta versão provar ser bastante robusta, fácil de implementar e suportar testes de escalabilidade, não foi previstos alguns requisitos que com o crescimento exponencial da rede (Internet) na última década sentiu-se a necessidade de serem atendidos, como:

a) **ameaça de esgotar o espaço de endereçamento IPv4:** com a escassez dos endereços IPv4, algumas organizações começaram a usar o *Network Addresss Translator* (NAT) para realizar o mapeamento de múltiplos endereços privados em um único endereço IP público;
b) **grandes tabelas de roteamento:** na versão atual do protocolo IP (o IPv4), a forma que os identificadores de redes são alocados, faz com que

[3] Request for Comments (RFC) é um documento que descreve os padrões de uma tecnologia desenvolvida pela Internet Engineering Task Force (IETF).

existam mais de 85.000 rotas nas tabelas de roteamento para roteadores de backbone, tornando uma tabela muita extensa;

c) **necessidade de configuração simplificada:** com o crescimento no número de computadores e no uso de dispositivos usando o IP, há uma grande necessidade de simplificar e automatizar o processo de configuração de endereços e outras características, vistos que muitas implementações atuais precisam ser configuradas manualmente ou usar um protocolo de configuração de endereço *stateful* como o *Dynamic Host Configuration Protocol* (DHCP);

d) **segurança no nível de rede IP:** atualmente, existe o padrão IPSec para a segurança de pacotes IPv4, porém sua implementação é opcional e prevalece as soluções proprietárias. Portanto, a privacidade em comunicações exige serviços de criptografia para protegerem os dados para não serem vistos ou alterados em trânsito;

e) **suporte melhorado para entrega de dados em tempo real:** também chamado de Qualidade de Serviço (QoS), o campo “Tipo de Serviço” do IPv4 possui funcionalidade limitada.

Com a necessidade de resolver estes e outros problemas, a *Internet Engeneering Task Force* (IETF), desenvolveu um conjunto de protocolos e padrões conhecidos como IPv6 (que anteriormente era chamada de *IP – The Next Generation* (IPng).

5.1.1 Características encontradas no IPv6

O protocolo IPv6 foi criado não só para resolver problemas da quantidade de endereços disponíveis, mas também para oferecer novos serviços e benefícios que não existiam no IPv4 ou que não eram utilizados de forma otimizada. Dentre muitos benefícios, podemos caracterizá-las em (COMER, 2001):

a) **formato do cabeçalho:** o novo cabeçalho possui um formato para manter o mínimo de *overhead* possível, isso foi alcançado com a remoção de alguns campos opcionais e não essenciais para os cabeçalhos de extensão que vem após o cabeçalho do IPv6. Assim os pacotes são processados de forma mais eficiente pelos roteadores;

b) **melhor suporte para extensões e opções:** no IPv6 as opções são consideradas cabeçalhos de extensão, enquanto que no IPv4 as opções eram integradas no cabeçalho base. Estes cabeçalhos de extensão são opcionais e são inseridos entre o cabeçalho base e a carga de dados;

c) **configuração de endereço *stateless* e *stateful*:** as formas encontradas para simplificar a configuração de máquinas foi através de endereços *stateful*, que precisa de um servidor DHCP, ou configuração de endereços *stateless*, onde as máquinas que estão no mesmo enlace se auto-configuram com endereços IPv6 do enlace (chamados de *link-local*), e com endereços originados dos prefixos anunciados pelos roteadores locais. No caso de não ter um roteador, as máquinas do enlace se auto-configuram automaticamente com endereços *link-local* e se comunicam sem configuração manual da mesma forma;

d) **tamanho de endereço:** cada endereço IP passou de 32 bits para 128 bits ou 16 *bytes*, espaço suficiente para garantir endereçamento para a Internet por um longo período de tempo. Embora isso expressa $3,4x10^{38}$ possíveis combinações, o IPv6 foi projetado para permitir níveis de sub-redes, porém técnicas como o NAT não são mais necessárias;

e) **cabeçalho de extensão:** o IPv6 tem a capacidade de incrementar cabeçalhos de extensão após o cabeçalho base. No IPv4 a opção no cabeçalho pode suportar somente 40 *bytes*, já os cabeçalhos de extensão são limitados somente pelo tamanho do pacote IPv6;

f) **suporte a IP móvel:** o IPv6 móvel permite roteamento de pacotes IPv6 para nós móvel de forma transparente. Cada nó móvel é identificado pelo seu endereço *home*, e enquanto o nó estiver distante de sua sub-rede que deu origem, ele está associado a um endereço *care-of*, que indica sua localização. Assim, o IPv6 móvel permite que qualquer nó IPv6 aprenda e armazene o endereço *care-of* associado com o endereço *home* do nó móvel e então envia pacotes destinados ao nó móvel para o endereço *care-of* usando o cabeçalho de roteamento do IPv6;

g) **suporte a segurança:** o IPv6 possui exigência ao IPSec através das extensões de autenticação e confidencialidade;

h) **melhor suporte para QoS:** com a identificação de tráfego usando o campo *Flow Label* do cabeçalho base do IPv6, roteadores recebem a permissão de identificar e providenciar manipulação especial para pacotes de um fluxo (série de pacotes entre uma origem e um destino);

i) **possui um novo protocolo para comunicação entre nós do mesmo enlace:** o novo protocolo *Neighbor Discovery* é uma lista de mensagens

Internet Control Protocol para IPv6 (IMCPv6), que gerencia a comunicação entre nós do mesmo enlace. Este novo protocolo substitui as mensagens do protocolo *Address Resolution Protocol* (ARP), *Router Discovery, ICMPv4* e *ICMPv4 Redirect* com suas mensagens *unicast* e *multicast Neighbor Discovery*;

j) **suporte para áudio e vídeo:** nesta versão do IP, foi incluído um mecanismo que permite estabelecer um caminho de alta qualidade e associar datagramas com este caminho.

A disponibilidade de um número de endereços IP é um dos maiores benefícios da implementação de redes IPv6. Comparado ao IPv4, o endereço que na versão 4 era de 32 bits, passa a ter 128 bits. Assim, esses 128 bits fornecem aproximadamente $3{,}4 \times 10^{38}$ possíveis endereços. É claro que esses números são apenas informativos, porque com o IPv6 os equipamentos possuem não mais um só endereço, mas vários endereços destinados a serviços diferenciados.

5.2 O FORMATO DO DATAGRAMA IPv6

O cabeçalho do IPv6 foi criado com o objetivo de melhorar a eficiência da rede. O formato novo introduz o conceito de um cabeçalho de extensão, permitindo uma maior flexibilidade para suportar características opcionais (Comer, 2001).

O protocolo IPv6 muda em grande parte o formato do seu pacote. Como mostrado na Figura 08, o cabeçalho IPv6 consiste em duas partes, o cabeçalho IP básico de tamanho fixo e os cabeçalhos de extensão podendo ser de tamanho variável.

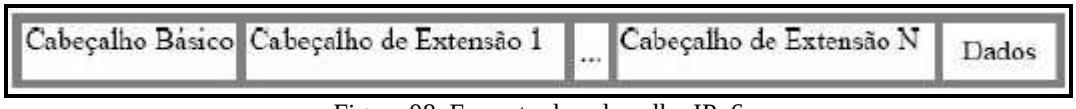

Figura 08. Formato do cabeçalho IPv6
Fonte: Adaptado de COMER, D. (2001).

5.2.1 Formato do pacote IPv6

Na Figura 09, observa-se que o cabeçalho IPv6 está sempre presente e tem comprimento fixo de 40 *bytes*, sendo que o endereço origem e destino usam 16 *bytes* cada, onde resta somente 8 *bytes* para a informação no cabeçalho.

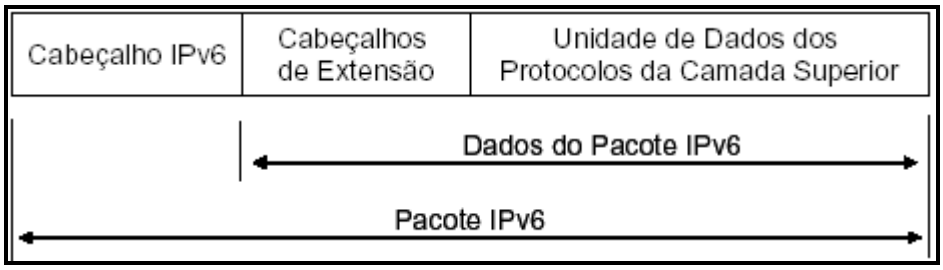

Figura 09. Estrutura de um pacote IPv6
Fonte: Adaptado de COMER, D. (2001).

O cabeçalho de extensão é opcional no pacote IPv6, podendo estar ou não, além de possuírem tamanhos variáveis. Esta forma de implementação dos cabeçalhos de extensão permite que o IPv6 tenha suporte a novas funções no futuro.

Como se observa na Figura 09, os dados do pacote IPv6 é uma combinação dos cabeçalhos de extensão com a unidade de dados dos protocolos da camada superior. O campo identificado como a unidade de dados dos protocolos da camada superior consiste do cabeçalho do protocolo da camada superior e sua carga de dados útil, exemplo, mensagem ICMPv6 ou mensagem UDP ou segmento TCP.

5.2.2 Formato do cabeçalho básico do IPv6

O cabeçalho do IPv6 é bem maior que o do IPv4, porém contém bem menos informações. Conforme na a Figura 09, a maioria do espaço no cabeçalho é dedicado aos dois campos que identificam o remetente e o receptor.

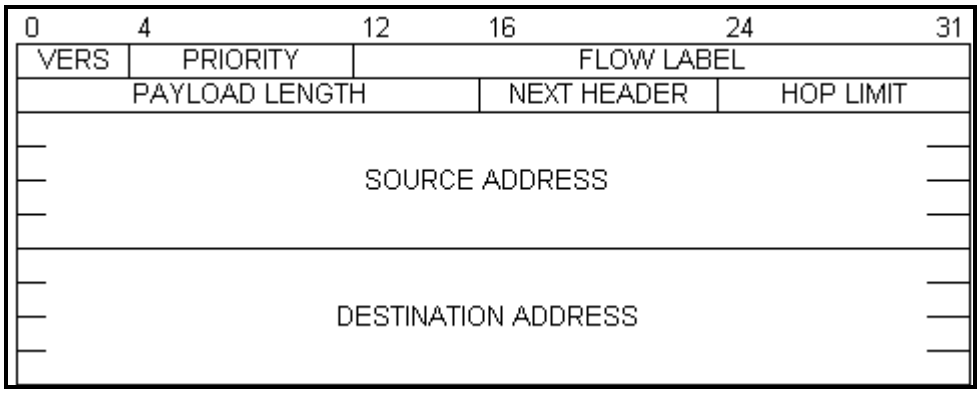

Figura 10. Formato do cabeçalho base do IPv6
Fonte: Adaptado de COMER, D. (2001).

O primeiro campo do cabeçalho básico segue a idéia do IPv4: representa 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, que faziam parte 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.

Os campos do cabeçalho básico de um pacote IPv6 são:

a) ***version*:** composto por 4 bits, identifica o número da versão do protocolo IP, neste caso 6;

b) ***priority (Traffic Class)*:** composto por 8 bits, o campo de classe de tráfego é semelhante ao tipo de serviço do IPv4. O uso deste campo permite que *hosts* ou roteadores, identifiquem os diferentes tipos de prioridades e classes de tráfego para pacotes IPv6;

c) ***flow Label*:** contêm 20 bits, o rótulo de fluxo é usado para identificar o fluxo de tráfego para controle adicional em *QoS*, ou seja, indica que este pacote pertence a uma seqüência de pacotes entre uma origem e um destino, por isso exige tratamento especial pelos roteadores;

d) ***payload Length*****:** com 16 bits, define o comprimento da carga útil da mensagem IPv6. Este comprimento inclui os cabeçalhos de extensão e a unidade da camada superior;

e) ***next header*****:** possui 8 bits e é usado para identificar o tipo de cabeçalho imediatamente seguinte ao cabeçalho IPv6, podendo ser tanto os cabeçalhos de extensão como os protocolos da camada superior como o TCP, UDP ou ICMPv6;

f) ***hop limit*****:** também com 8 bits, contém o número inteiro que é decrementado em uma unidade em cada nó que remete o pacote. O pacote será descartado se o *Hop Limit* for decrementado e chegar a zero, ou seja, é utilizado para determinar o número máximo de equipamentos roteadores pelos quais o pacote pode trafegar;

g) ***source address*****:** com 128 bits, armazena o endereço IPv6 da máquina origem do pacote;

h) ***destination address*****:** com 128 bits, armazena o endereço IPv6 da máquina destino do pacote. 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.

5.2.3 Os cabeçalhos de extensão do IPv6

Segundo Deering e Hinden definiram na RFC2460 (1998) e Kent e Atkinson definiram na RFC2406 (1998), a especificação de IPv6 define seis cabeçalhos de extensão:

a) ***hop-by-hop options*:** como o nome já diz, ele carrega informações opcionais que precisam ser examinadas por todos os nós que o pacote passar até chegar ao destino. Por isso, ele deve vir logo após o cabeçalho base IPv6, pois é o único cabeçalho que é examinado por todos os nós intermediários;

b) ***routing*:** é usado para fornecer uma lista de nós que ele deve ser roteado no caminho até o pacote chegar ao destino, ou seja, traçar um caminho específico;

c) ***fragment*:** quando um pacote a ser enviado é maior que o *Maximum Transmission Unit* (MTU) suportado, então o nó de origem fragmenta o pacote, já que no IPv6, só podem fragmentar pacotes nos nós de origem. Portanto este cabeçalho é usado para serviços de fragmentação e remontagem de pacotes;

d) ***destination options*:** usado para especificar parâmetros opcionais que são examinados por nós a serem percorridos ou pelo destino final, o que depende em que posição ele estiver na ordem dos cabeçalhos de extensão;

e) ***authentication*:** usado para oferecer segurança ao pacote que está sendo transportado. Este cabeçalho possui dois modos de operação. Um é transporte, que é utilizado para autenticação fim-a-fim entre duas máquinas e outro através de um túnel que é usado quando *gateways* de segurança possui proteção para diversas máquinas na rede. No modo de túnel, um cabeçalho adicional externo é colocado no início do pacote com o endereço origem do *gateway* de segurança, enquanto que o

cabeçalho interno original tem o endereço origem da máquina interna da rede;

f) ***encapsulating security playload (ESP)*:** este cabeçalho pode ser usado também tanto em modo de transporte como em modo de túnel. No modo transporte, o cabeçalho IP, os cabeçalhos de extensão, até o cabeçalho ESP, não são cifrados, portanto não são protegidos, pois se cifrar estes cabeçalhos todo o mecanismo de roteamento se torna inútil, já que roteadores podem precisar ver, processar e até mesmo modificar estes cabeçalhos enquanto o pacote está transitando na rede. Sendo assim, se for necessário cifrar todo o pacote, deve ser criado um túnel e empacotar todo o pacote original em um pacote IP externo, onde o conteúdo não é protegido pela cifragem.

No IPv6 também existe a limitação de tamanho de pacotes, portanto veja a seguir como ocorre a fragmentação e remontagem dos pacotes IPv6.

5.3 A FRAGMENTAÇÃO E REMONTAGEM DO DATAGRAMA NO IPV6

A fragmentação no IPv6 é semelhante com o IPv4, porém, o IPv6 não inclui campos para informações de fragmentação no cabeçalho base. Ao invés de fazer isso, o IPv6 os coloca em um cabeçalho de extensão de fragmento separado, sendo que a presença do cabeçalho identifica o datagrama como um fragmento.

Sendo assim, cada fragmento é menor do que o datagrama original, o tamanho do fragmento é escolhido como sendo o tamanho da unidade de transmissão máxima (MTU) da rede subjacente que os fragmentos devem ser enviados (COMER, 2001).

Segundo Comer (2001), no IPv4 o roteador é que executa a fragmentação, quando recebe um datagrama grande demais para a rede através da qual o datagrama deve ser enviado. Já no IPv6, o responsável pela fragmentação é o *host* remetente, assim os roteadores ao longo do caminho que recebem um datagrama grande não fragmentarão o datagrama.

5.4 ENDEREÇAMENTO NO IPv6

O IPv6 atribui um endereço único a cada conexão entre um computador e uma rede física, além de separar cada um desses endereços em um prefixo que identifica a rede e um sufixo que identifica um computador particular da rede.

O IPv6 não possui classes definidas, sendo assim o limite entre o prefixo e o sufixo pode cair em qualquer lugar dentro do endereço e não pode ser determinado a partir do endereço apenas.

5.4.1 Formato do endereço IPv6

O endereço de 128 bits do IPv6 é separado em conjuntos de oito números hexadecimais de 16 bits cada, divididos por dois pontos (“:”). O formato padrão do endereço IPv6 é:

XXXX : XXXX : XXXX : XXXX : XXXX : XXXX : XXXX : XXXX,

por exemplo:

2031 : 0000 : 1F1F : 0000 : 0000 : 0100 : 11A0 : ADDF

As seguintes convenções também são usadas para representar os endereços IPv6, incluindo modos para encurtá-los e representá-los mais facilmente (COMER, 2001):

a) os principais zeros podem ser removidos;

b) 0000 = 0 (forma comprimida);

c) "::" representa um ou mais grupos de 16 bits zeros, e só pode aparecer uma vez em um endereço. Por exemplo, 2001:0:13FF:09FF:0:0:0:0001 = 2001:0:13FF:09FF::1.

OBS.: O dois pontos pode ocorrer somente uma vez no endereço porque o computador sempre usa a representação binária completa do endereço com 128 *bits*, mesmo quando o endereço é mostrado simplificado. Quando o computador encontra um dois pontos duplo, ele o expande com quantos zeros são necessários para chegar a 128 *bits*, e se for encontrado mais que um dois ponto duplo, o computador não saberá quantos zeros adicionar a cada um dos dois pontos.

Os quatro últimos octetos podem usar representação decimal de endereços IPv4. Para exemplo, um endereço de IPv6 *IPv4-compatible* é 0:0:0:0:0:0.192.168.0.1. Ao contrário de um nó IPv4, um nó IPv6 permite mais de um tipo de endereço de IP: *unicast*, *anycast* e *multicast*.

5.4.2 Tipos de endereço do IPv6

Segundo Hinder e Deering (2003) definem na RFC3513, Comer (2001), a arquitetura dos endereços IPv6 pertencem a um destes três tipos de endereços:

a) ***Unicast*:** Endereço usado para identificar uma única interface. Um pacote destinado para um endereço *unicast* é entregue à interface identificada por aquele endereço;

b) ***Anycast*:** O endereço anycast é um endereço global que é relacionado a um conjunto de interfaces que pertencem a nós diferentes. Um pacote destinado a um endereço de *anycast* é roteado para a mais próxima interface. Este endereço é usado para comunicações *one-to-one-of-many*;

c) ***Multicast*:** como no IPv4, um endereço *multicast* é referenciado a um conjunto de interfaces que pertencem a nós diferentes. Um pacote destinado a um endereço *multicast* é roteado a todas as interfaces identificadas por aquele endereço. O endereço *broadcast* foi substituído pelo *multicast* do IPv6.

Todos os bits zero e um são permitidos para qualquer campo em um endereço IPv6. Um *host* ou um roteador, podem ter muitas interfaces e conseqüentemente, múltiplos endereços *unicast*, pois os endereços IPv6 são designados para interfaces. Portanto uma interface pode ter múltiplos endereços de qualquer tipo ou escopo.

Basicamente, um endereço IPv6 possui 3 partes: o prefixo de roteamento global, o identificador de sub-rede e o de interface, conforme mostrado na Figura 11.

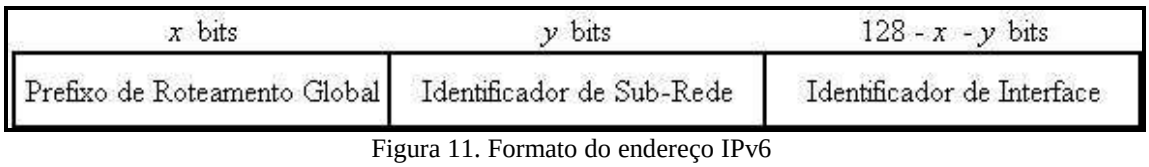

Figura 11. Formato do endereço IPv6
Fonte: Adaptado de HINDER e DEERING (2003).

5.5 O ICMPv6

Com as diversas modificações implementadas no protocolo IP, o protocolo de controle de mensagens também sofreu alterações. O ICMPv6 faz parte das especificações IPv6 e atua junto com o IP na camada de rede oferecendo serviços de controle de erros, diagnóstico e funções de controle diversas ao IPv6.

No ICMPv4, para suporte a serviços relacionados ao uso do *multicast* era usado o protocolo IGMP desenvolvido para este fim. No ICMPv6 estes serviços foram incorporados ao protocolo.

Segundo Conta e Deering (1998) descrevem na RFC2463, o ICMPv6 possui suporte ao IPv6 móvel e um *framework*[4] para:

a) ***Multicast Listener Discovery* (MLD):** segundo Haberman (2003) descrito na RFC3590, são três mensagens ICMPv6 que substituem a versão 2 do IGMP, que é o protocolo usado para gerenciar o roteamento dos pacotes destinados para grupos *multicast* de forma eficiente;

b) ***Neighbor Discovery Protocol* (NDP):** segundo Narten, Nordmark e Simpson descrevem na RFC2461, são cinco mensagens ICMPv6 que gerenciam a comunicação *host-and-host* no enlace. As mensagens de *Address Resolution Protocol* (ARP), de *ICMPv4 Router Discovery* e de *ICMPv4 Redirect* são substituídas por este protocolo.

Existem, basicamente, dois tipos de mensagens ICMPv6:

a) **mensagens de erro:** são usadas para identificar erros na entrega e roteamento de pacotes IPv6 tanto no destino como em roteadores percorridos pelo pacote;

[4] *Framework* é uma estrutura de suporte definida em que um outro projeto do software pode ser organizado e desenvolvido.

b) **mensagens de informação:** são usadas para identificar funções de diagnóstico e funcionalidades adicionais, como MLD e NDP.

5.5.1 Formato das mensagens ICMPv6

Basicamente, todas as mensagens ICMPv6 possuem a mesma estrutura de cabeçalho. Conforme podemos observar na figura 12, os campos são:

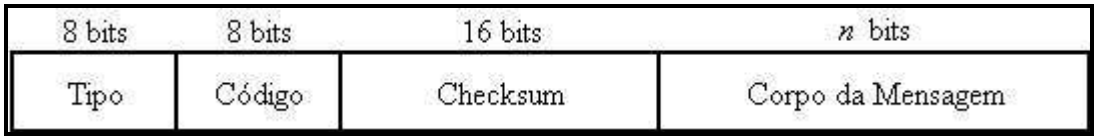

Figura 12. Formato das mensagens ICMPv6
Fonte: Adaptado da CONTA A.; DEERING S. (1998).

a) **tipo:** especifica o tipo da mensagem que consequentemente, determina o formato do restante da mensagem;

b) **código:** depende do tipo da mensagem existe um e serve para diferenciar as inúmeras mensagens dentro de um determinado tipo;

c) **checksum:** é usado para identificar se existem dados corrompidos no cabeçalho ICMPv6 e em partes do cabeçalho IPv6, sendo que para calcular o *checksum*, um *host* precisa determinar o endereço origem e destino no cabeçalho IPv6;

d) **corpo da mensagem:** conforme o tipo e código da mensagem, o corpo dela possui informações diferentes e seu tamanho é variável.

5.5.2 Neighbor Discovery

Narten, Nordmark e Simpson descrevem na RFC2461 que o protocolo *Neighbor Discovery* é uma lista de mensagens ICMP para IPv6 que têm a função de

gerenciar a interação dos *hosts* do mesmo enlace, ou seja, resolve os problemas de interação dos *hosts* do mesmo enlace. As funções deste protocolo podem ser divididas em:

a) ***Router Discovery*:** possui o objetivo de encontrar roteadores vizinhos (no mesmo enlace) que está sendo encaminhandos pacotes;

b) ***Prefix Discovery*:** realiza a descoberta do prefixo da rede para identificar se o destino está no mesmo enlace. Isto é necessário para saber se o pacote deve ser encaminhado para um roteador ou direcionado diretamente para o *host* destino;

c) ***Parameter Discovery*:** permite realizar o controle e roteamento de parâmetros de rede como o *Maximum Transfer Unit* (MTU) e o *hop limit*;

d) ***Address Autoconfiguration*:** permite designar endereços IP automaticamente, sendo que as máquinas usam uma informação de prefixo qualquer para criar seus endereços e a partir disso testar se este endereço gerado não está em uso em outra máquina. O mecanismo padrão de auto-configuração é o *stateless*;

e) ***Address Resolution*:** dentro do mesmo enlace, usando somente o endereço IP de destino, as máquinas resolvem o endereço IPv6 de uma máquina;

f) ***Next-hop determination*:** determina o tráfego que o endereço IP deve seguir até chegar ao destino sendo que o próximo salto pode ser um roteador ou o próprio destino;

g) ***Neighbor Unreachability Detection*:** usado para verificar a capacidade de acesso dos roteadores e das máquinas, ou seja, rastrear a

acessibilidade e se a máquina não está mais disponível executa o *address resolution*;

h) ***Duplicate Address Detection*:** quando uma máquina desejar usar um novo endereço em suas interfaces, este procedimento é executado para verificar se não existe outra máquina que esteja usando o mesmo endereço para prevenir colisões de endereços no momento da auto-configuração;

i) ***Redirection*:** usado para direcionar um *host* para o melhor roteamento ou para sinalizar que o destino está no mesmo enlace;

As mensagens *Neighbor Discovery* possuem o formato das mensagens ICMPv6. O pacote ICMPv6 é um cabeçalho de extensão do IPv6. Observe na Figura 13 que no primeiro campo foi atribuído o valor 58 ao próximo cabeçalho, isto indica que o próximo cabeçalho de extensão será o pacote ICMPv6.

Figura 13. Formato da mensagem Neighbor Discovery
Fonte: Adaptado de NARTEN, T.; NORDMARK, E.; SIMPSON, W. (1998).

Todas as mensagens *Neighbor Discovery* são configuradas com *hop limit* de 255 para garantir que elas se originaram de um *host* no enlace local. Desta forma, quando receber uma mensagem com valor diferente deste, será descartada para evitar ataques de redes baseados em *Neighbor Discovery* externos.

5.5.3 Auto-configuração

A execução da auto-configuração permite que máquinas configurem-se automaticamente sem a necessidade de realizar este processo manual antes de conectá-la à rede. Um endereço *link* local pode ser configurado automaticamente por uma máquina IPv6, pois usando *router discovery* é possível determinar o endereço do roteador, parâmetros de configuração, prefixos de enlace e endereços adicionais. Os roteadores podem distribuir vários prefixos e as máquinas determinam a informação do prefixo distribuído.

Thomson e Narten (1998) descrevem na RFC2462 que um endereço IPv6 é alocado à uma máquina por um determinado tempo, desta forma ele possui os seguintes estados:

a) ***tentative*:** é um endereço que está no estágio de ser designado, identificado no momento da verificação da unicidade do endereço;
b) ***valid*:** este já é um endereço que passou pelo estágio de verificação e pode receber e enviar mensagens *unicast*;
c) ***preferred*:** endereço que já foi designado para alguma interface e pode ser usado sem restrição;
d) ***deprecated*:** seu tempo de vida está próximo de acabar, portanto não se usa para novas comunicações mas continua sendo um endereço válido podendo ser usado por comunicações em andamento;
e) ***invalid*:** quando o tempo de vida do endereço acaba, assim não pode mais usar para enviar ou receber informações.

Neste capítulo, foram apresentadas as características do IPv6, as modificações e melhorias em realação ao IPv4, o novo cabeçalho com a inserção de

cabeçalhos de extensão, novo formato de mensagens ICMP dentre outras. Porém para que os dois protocolos comuniquem-se e convivam entre si, é necessário o uso de mecanismos de transição.

Existem basicamente três tipos de mecanismos de transição e convivência: dual-stack, tunelamento e tradução de cabeçalhos, sendo que os mecanismos de tunelamento e tradução possuem vários métodos disponíveis. Todos estes mecanismos citados, além de seus métodos, serão abordados no capítulo a seguir.

6 MECANISMOS DE TRANSIÇÃO DO IPv4 PARA O IPv6

Segundo Kurose e Ross (2005) o IPv6 não é compatível com o IPv4, então máquinas que utilizam IPv4 e estão conectadas em redes IPv4 não se comunicam com máquinas IPv6 em redes IPv6. Para que as duas redes conversem entre si é necessário algum mecanismo de transição.

Desta forma, os *hosts* e redes baseadas em IPv6, precisam coexistir com IPv4 e usar a infra-estrutura de roteamento IPv4 existente, pois é impossível fazer esta migração imediatamente. Sistemas baseados em IPv6 precisarão trabalhar juntos com o IPv4 conforme ocorra a migração gradual dos protocolos.

Pensando em tudo isso, a IETF criou o grupo de trabalho *Next Generation Transition* (NGTRANS), com o objetivo de desenvolver ferramentas e mecanismos que permitam a mudança gradual do IPv4 para IPv6. Durante dois anos este grupo disponibilizou muitos esboços que estabeleceram vários mecanismos para a integração com o IPv6, sendo que variam de um simples tunelamento até complexos como o Teredo (que será tratado no item 6.2.7).

Em fevereiro de 2003, o grupo NGTRANS foi fechado deixando mais de doze ferramentas desenvolvidas que foram transferidas para o grupo de trabalho *v6ops*. A seguir, uma abordagem mais detalhada destes mecanismos de transição.

Os mecanismos de transição podem ser classificados em três principais categorias:

a) **pilha dupla:** conhecida também por *Dual Stack*;

b) **tunelamento:** conhecida como *encapsulation* ou *tunel*;

c) **tradução:** conhecida por *translation*.

6.1 PILHA DUPLA (*DUAL-STACK*)

Esta é a técnica mais fácil para integrar IPv6 em uma rede IPv4, sendo que as duas pilhas[5] são colocadas dentro do mesmo ambiente e na mesma interface. Dependendo com quem queira se comunicar, utiliza-se uma das duas pilhas para processar o pacote a ser enviado. Esse mecanismo permite que nós IPv6 se comuniquem com nós IPv4 e realizem roteamento de pacotes IPv4 (KUROSE; ROSS, 2005). Para suportar as duas pilhas os roteadores e as máquinas de trabalho precisam ser atualizadas. Esta técnica exige duas tabelas de roteamento com funções de administração e gerenciamento parecidas. Num *host* com pilha dupla, existem os dois endereços configurados em sua interface, sendo que o endereço IPv6 é configurado estaticamente ou dinamicamente por meio de configurações *stateless* ou *stateful*.

Além destas configurações, as rotas IPv4 e IPv6 precisam ser configuradas separadas, possuindo registros para IPv4 (A) e registros para IPv6 (AAAA ou A6) criados na configuração do DNS. Outro detalhe é que muitas das novas redes IPv6 não podem obter endereços IPv4 válidos para os seus *hosts*, sendo assim o uso de *hosts* com pilha dupla é útil para os mecanismos de transição por meio de estabelecimento de túneis ou por tradução de endereços.

Veja na Figura 14 a relação dos dois protocolos IP implementados juntos em uma pilha.

[5] Pilhas: implementação da arquitetura IPv4 e IPv6 juntas no mesmo ambiente para identificarem pacotes de ambas tecnologias.

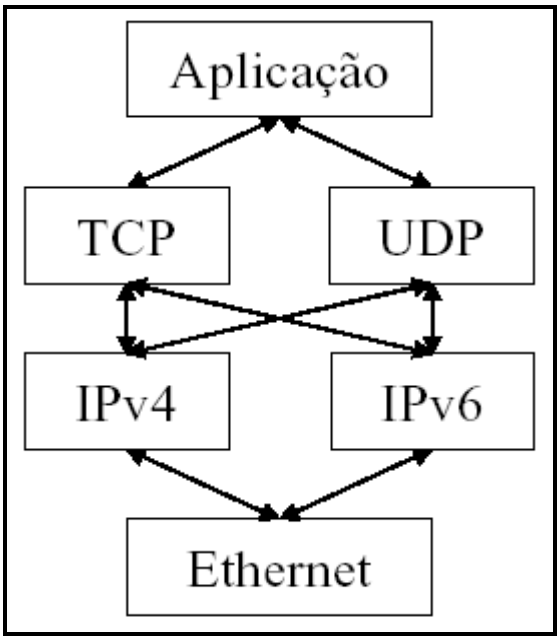

Figura 14. Pilha Dupla IPv4 e IPv6
Fonte: Adaptado KRISHNAMUETHY, B.; REXFORD, J. (2001).

6.2 TUNELAMENTO (*ENCAPSULATION* ou *TUNEL*)

Utilizando o conceito de tunelamento esse mecanismo consiste em transmitir um datagrama IPv6 como parte de dados de um datagrama IPv4, a fim de que dois nós IPv6 possam se comunicar através de uma rede que só suporte IPv4. A rede IPv4 é vista como um túnel e o endereço IPv4 do nó da outra extremidade deste túnel consta como destino do datagrama IPv4. Neste nó, o cabeçalho IPv4 é retirado e o pacote IPv6 volta a trafegar normalmente a seu destino (conforme a figura 15). Os nós das duas extremidades do túnel devem ser capazes de falar IPv4 e IPv6 já que têm uma interface ligada a uma rede IPv4 e outra ligada a uma rede IPv6 (KUROSE; ROSS, 2005).

Figura 15. Túnel estabelecido para a comunicação entre ilhas IPv6
Fonte: Adaptado KUROSE; ROSS, (2001).

Este mecanismo é muito utilizado em casos que a infra-estrutura de rede não possui a capacidade de ter conectividade IPv6, sendo assim, usando o tunelamento é possível que o tráfego IPv6 seja carregado sobre a infra-estrutura de rede IPv4. Consiste em encapsular um pacote de um protocolo dentro de outro permitindo que a informação seja transportada sobre o segundo protocolo. Conforme a Figura 15, o pacote IPv6 é encapsulado em um pacote IPv4 usando o "protocolo 41"[6] do IP, desta forma é tunelado até o destino onde é desencapsulado e encaminhado o pacote IPv6 original.

Existem alguns métodos de tunelamento disponíveis, a seguir serão citados e comentados cada um deles.

6.2.1 Túnel configurado

Gilligan e Nordmark (2000) descrevem na RFC2893, este método é definido como tunelamento IPv6 sobre IPv4, sendo que o endereço IPv4 final do túnel é determinado pela configuração da máquina responsável pelo encapsulamento. Assim o *host* encapsulado precisa manter informação sobre todos os endereços finais dos túneis. Este túnel precisa ser configurado manualmente e é do tipo ponto-a-ponto.

6.2.2 Tunnel Broker

Durand et al (2001) descrevem na RFC3053 que é possível usar *scripts* executáveis para configurar cada ponto final de túnel. Esta forma automática recebe o nome de *tunnel broker*, sendo útil também quando um usuário possui uma máquina pilha dupla em uma rede IPv4-*only* e quer obter conexão IPv6.

[6] Protocolo 41: é o protocolo que identifica a encapsulação de IPv6 sobre IPv4.

A principal função do *tunnel broker* é permitir que um usuário entre em contato com o servidor *web*, caso deseje, entrar com detalhes de autenticação e receber de volta um *script* para estabelecer um túnel *IPv6-in-IPv4* até o servidor *tunnel broker*. O provedor de um serviço *tunnel broker* precisa ter um servidor de *web* disponível sobre o IPv4 e um roteador pilha dupla capaz de aceitar comandos de *setup* para criar novos túneis para clientes finais, conforme Figura 16.

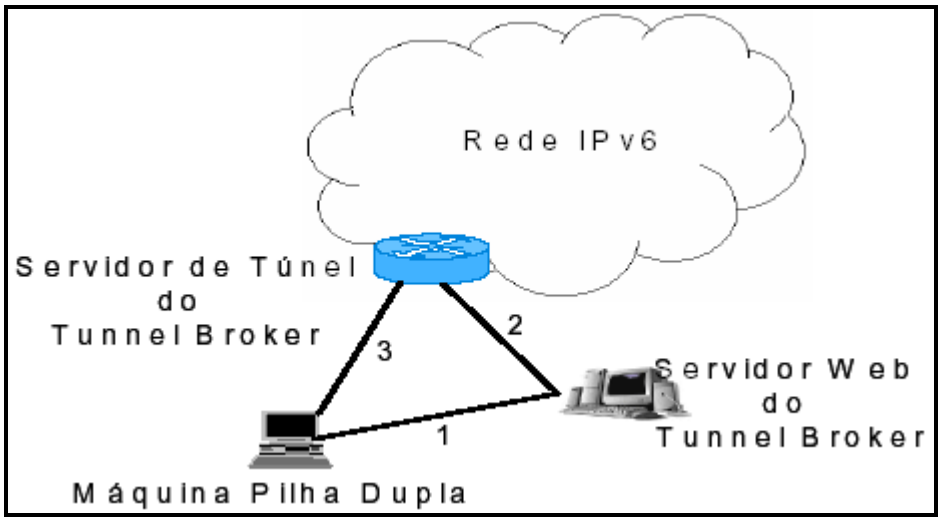

Figura 16. Exemplo prático de um Tunnel Broker
Fonte: Adaptado de DURAND, A; et al (2001).

A Figura 16 mostra uma especificação da operação típica de um servidor *tunnel broker*. No primeiro passo (1), o usuário realiza a conexão ao servidor de *web* solicitando um túnel, já no segundo passo (2), este servidor retorna um *script* para que o usuário crie um túnel com o servidor de túnel e informa ao servidor sobre o novo cliente. No terceiro passo (3), o usuário ativa o *script* e adquire acesso a rede IPv6 por meio do servidor de túnel.

6.2.3 Túnel Automático

Este mecanismo pode ser usado somente em comunicações *router-to-host* e *host-to-host*, pois são esquemas onde qualquer ponto final do túnel são receptores dos

pacotes. Este túnel funciona só em tunelamento IPv6-over-IPv4 não podendo ser ao contrário porque usa endereços privados. Outra característica deste mecanismo é que este tipo de túnel usa IPv6 *IPv4-compatible* nas extremidades do túnel.

Segundo Gilligan e Nordmark (RFC2893 de 2000), técnicas de túnel configurado e de túnel automático podem ser combinadas. Um *host* IPv4/IPv6 que possuir um endereço *IPv4-compatible* e esteja conectado só a rede IPv4, deve usar túneis automáticos para comunicar-se com outros *hosts* IPv6 que utilizam endereços *IPv4-compatible*, portanto precisaria de pelo menos um túnel configurado para conseguir chegar aos demais *hosts* IPv6, mesmo podendo utilizar um túnel configurado em um sentido combinado com um túnel automático no outro sentido para realizar a mesma comunicação.

6.2.4 Mecanismo IPv6-to-IPv4

Este mecanismo é uma forma de tunelamento automático *router-to-router*, que usa o prefixo IPv6 2002::/16 para endereçar uma rede que participa do 6to4. Usando pouca configuração, permite que domínios IPv6 isolados se comuniquem.

Carpenter e Moore (2001) relatam na RFC3056 que, se domínios IPv6 isolados desejarem se comunicar, é necessário estabelecer um prefixo de 2002:V4ADDR[7]::/48. Este prefixo possui o mesmo formato dos prefixos normais /48, assim permitindo que um domínio IPv6 possa usá-lo como qualquer outro prefixo /48 válido.

Quando domínios 6to4 desejarem comunicar-se entre si não é necessário configurar o túnel. Conforme a Figura 17, pontos finais dos túneis são determinados

[7] V4ADDR é o endereço IPv4 global configurado na interface apropriada de saída do roteador.

pelo valor NLA (V4ADDR) do endereço IPv6 de destino presente no pacote IPv6 transmitido.

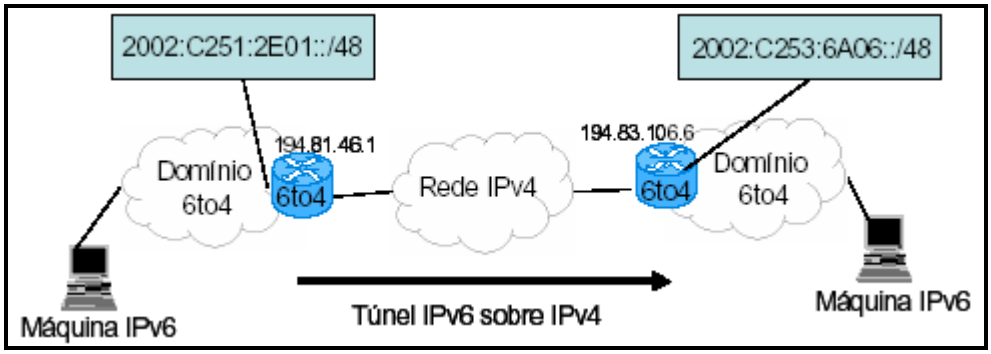

Figura 17. Esquema do mecanismo 6to4
Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

Portanto, no caso de domínios 6to4 terem a necessidade de se comunicar com domínios *IPv6-only*, esta conexão pode ocorrer através de um roteador *relay* que tenha pelo menos uma interface lógica 6to4 e uma interface nativa IPv6.

6.2.5 Mecanismo IPv6-over-IPv4

Carpenter e Jung (1999) relatam na RFC2529 que este método não está em uso por várias razões sendo uma delas a ausência de suporte *multicast* IPv4 em várias redes. O princípio de funcionamento deste método é permitir que máquinas IPv6 isoladas que não possuem conexão direta com roteador IPv6 localizadas num *link* físico, torne-se máquinas IPv6 funcionais usando um domínio IPv4 que suporte *multicast* IPv4 como seu enlace local. Neste caso, endereços *multicast* IPv6 são transformados em endereços *multicast* IPv4 para permitir *Neighbor Discovery* (descoberta do vizinho).

6.2.6 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Pelo fato de conectar máquinas e roteadores IPv6 dentro de redes IPv4 sem causar impactos no tamanho da tabela de roteamento e exigir serviços especiais IPv4, esta é uma alternativa ao *6over4*. Neste caso, cada máquina precisa de um roteador ISATAP no enlace para adquirir endereço e informação de endereçamento.

Templin et al (2005) descreveram na RFC4214, os pacotes enviados para a Internet IPv6 são roteados por um roteador ISATAP e os pacotes destinados a outras máquinas na mesma rede são tunelados direto para o destino. Normalmente, clientes ISATAP usam auto-configuração *stateless* de endereços IPv6 com descoberta de roteador ISATAP automática, mas pode-se usar endereços definidos estaticamente.

6.2.7 Teredo

Huitema (2006) descreve na RFC4380 que este mecanismo permite que usuários em um ambiente IPv4 com endereçamento privado (NAT) consiga obter conexão IPv6. Sua funcionalidade básica é um *host* encapsular pacotes IPv6 em UDP IPv4 e formar um túnel para um servidor Teredo na Internet IPv4, ficando a critério deste servidor a função de desencapsular e entregar o pacote IPv6.

A criação do endereço ocorre através da comunicação do servidor e o *host* Teredo. A partir disso, o cliente Teredo busca encontrar uma porta UDP aberta no *gateway* NAT existente com a finalidade de alcançar o servidor Teredo e quando for encontrado o cliente pode se comunicar usando IPv6 via servidor.

6.2.8 Dual Stack Transition Mechanism (DSTM)

Este mecanismo é usado para redes *IPv6-only*, de forma que as aplicações IPv4 ainda necessitam de máquinas pilha dupla na infra-estrutura IPv6. São usados túneis para permitir que o tráfego IPv4 seja tunelado sobre o domínio *IPv6-only* até encontar um *gateway* IPv6/IPv4. Este *gateway* possui a função de encapsular, desencapsular e encaminhar o pacote entre os domínios *IPv6-only* e IPv4.

Segundo BOUND, J. et al (2001), esta solução é bastante transparente para as aplicações IPv4 além de permitir o uso de segurança da camada 3. Porém, da maneira que é usado o tunelamento é necessário um endereço IPv4 para a máquina que queira conectar-se a Internet IPv4. Outra característica do DSTM é a redução de endereçamento, pois é alocado o endereço apenas durante a comunicação possibilitando o compartilhamento de um endereço por várias máquinas.

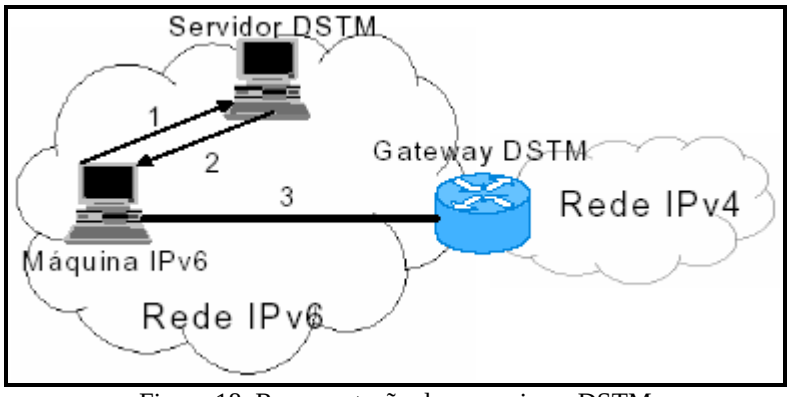

Figura 18. Representação do mecanismo DSTM
Fonte: Adaptado de BOUND, J. et al (2001).

Conforme representado na Figura 18, o DSTM possui três componentes: o próprio servidor de endereços DSTM, um *gateway* DSTM ou *Tunnel End Point* (TEP) e um *host* pilha dupla que deseja comunicar-se usando IPv4 chamado de *host* DSTM. Para que ocorra uma comunicação neste método são necessários alguns passos, como:

(1) Na necessidade do envio de um pacote IPv4 é solicitado pelo cliente DSTM (ao servidor) um endereço IPv4;

(2) O servidor solicita ao *gateway* DSTM para adicionar um TEP para o *host* que fez a requisição, pois é ele que controla o mapeamento de endereço IPv4/IPv6 efetuado pelo *gateway* DSTM. Se for criado com sucesso o ponto final do túnel, o servidor DSTM responde para a máquina com as seguintes informações: endereço IPv4 alocado, duração da alocação e os endereços IPv4 e IPv6 do TEP;

(3) Todas estas informações são usadas pelo cliente DSTM para configurar um túnel IPv4 sobre IPv6 até o *gateway* DSTM. Assim, como o cliente DSTM possui conexão IPv4 válido ele é capaz de conectar-se a qualquer máquina externa.

Todos estes oito mecanismos abordados pertencem a uma mesma técnica que é o tunelamento, onde cada uma técnica possui características próprias que as diferenciam umas das outras. Desta forma é possível classificar estes mecanismos em sub-classes unindo os que possuem alguma semelhança.

A seguir, a distribuição desta classificação:

a) **tunelamento via servidor de origem IPv4:** são os métodos que formam túneis *IPv6-in-IPv4* entre servidores de túneis e clientes. Caracterizam-se pelos mecanismos *Tunnel Broker* e Teredo;

b) **tunelamento via servidor de origem IPv6:** são aqueles que estabelecem túneis *IPv4-in-IPv6* entre túneis e clientes. Pode-se citar o mecanismo DSTM com esta característica;

c) **tunelamento *IPv6-over-IPv4*:** este método usa endereços IPv4 para configura e gerar o túnel IPv6 sobre redes IPv4 automaticamente. Dentre os quais caracteriza os mecanismos túnel configurado e túnel automático;

d) **tunelamento interno:** este usa a infra-estrutura da rede IPv4 como um *link* virtual. Caracterizam-se pelos mecanismos ISATAP e *6over4*;

e) **tunelamento *6to4*:** realiza tunelamento automático *router-to-router* e usa o prefixo IPv6 2002::/16 na designação de uma rede que participa do *6to4*. Nesta classe o *6to4* é o único mecanismo;

f) **tunelamento *4to6*:** este estabelece túneis *IPv4-in-IPv6* entre clientes e servidores e entre clientes e clientes.

6.3 TRADUÇÃO (*TRANSLATION*)

Normalmente, os mecanismos de tradução são usados quando dispositivos *IPv6-only* precisam comunicar-se com dispositivos *IPv4-only* ou vice-versa. A seguir será feita uma breve descrição dos mecanismos de tradução disponível.

6.3.1 Stateless IP/ICMP Translation Algorithm (SIIT)

Nordmark (2000) descreve na RFC2765 que este mecanismo usa um tradutor na camada de rede da pilha de protocolos. Também chamado de tradutor de cabeçalhos, funciona fazendo a tradução de cabeçalhos de datagramas IPv6 em cabeçalhos de datagramas IPv4 e vice-versa.

Para entender melhor este mecanismo pode-se usar um exemplo da seguinte forma: considera-se que o *host IPv4-only* tenha o endereço 200.254.245.1, para que o *host IPv6-only* se comunique ele precisa enviar pacotes para ::FFFF:200.254.245.1, além de possuir uma rota correspondente a rede ::FFFF/96 no *host IPv6-only*, que por sua vez distribuirá todos os pacotes destinados para *hosts IPv4-only* para o *host*

intermediário que execute o SIIT. A partir deste *host* intermediário os pacotes IPv6 originais serão convertidos em pacotes IPv4 com endereço de destino. Estes pacotes IPv4 convertidos devem chegar no *host IPv4-only* e este responder enviando pacotes IPv4 ao endereço 200.254.245.1 onde deve ser roteado ao *host* intermediário para executar o SIIT, que realiza a tradução convertendo pacotes IPv4 originais em pacotes IPv6 com endereço de origem ::FFFF:200.254.245.1.

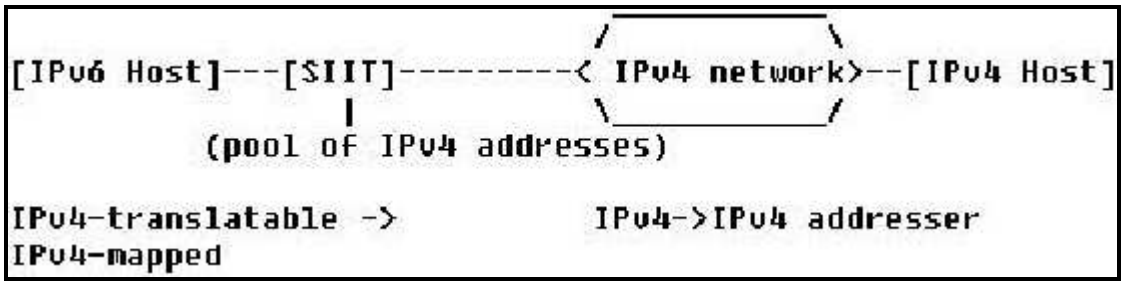

Figura 19. Comunicação entre *host IPv4-only* e *host IPv6-only*
Fonte: Adaptado de NORDMARK, E. (2000).

Conforme a Figura 19, mostra o uso do SIIT para um *host IPv6-only* se comunicar com um *host IPv4-only*. Veja que o *host* intermediário possui endereços IPv4 para fazer alocação temporária para os *host* IPv6 que fizerem comunicação com *hosts* IPv4.

6.3.2 Network Address Translation with Protocol Translation (NAT-PT)

Srisuresh e Egevang (2001) descrevem na RFC3022 que este é um serviço que da permissão à máquinas IPv6 e IPv4 com suas aplicações se comunicarem. Este método usa a tradução de cabeçalhos e conversão de endereços, desta forma, a tradução de cabeçalhos é usada para converter cabeçalhos IPv4 em formato de cabeçalho IPv6 e vice-versa, que resulta num novo cabeçalho parecido com o cabeçalho original mas não igual. Já a conversão é utilizada para que máquinas IPv4 saibam identificar máquinas IPv6 (ou vice-versa) através de endereços de sua própria rede.

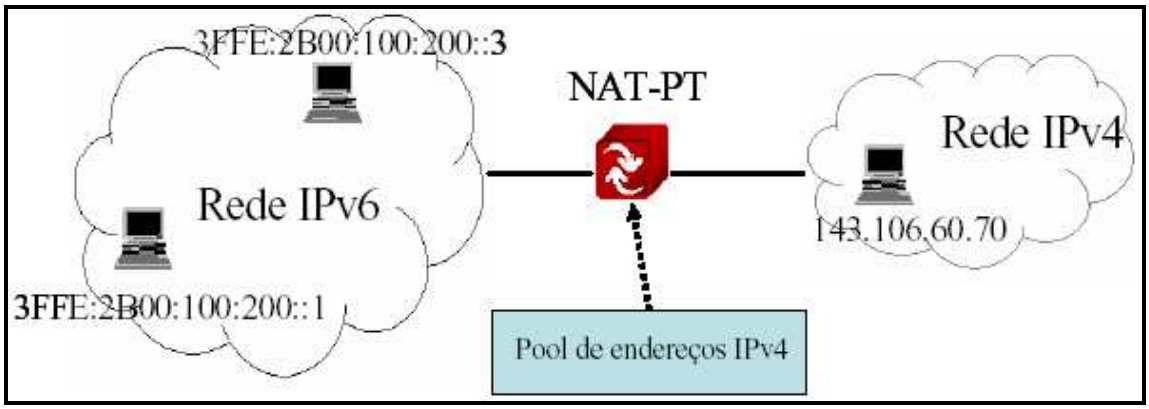

Figura 20. Esquema do mecanismo NAT-PT
Fonte: Adaptado de TSIRTSIS, G.; SRISURESH, P. (2000).

Conforme pode-se observar na Figura 20, o NAT-PT utiliza endereços dinamicamente alocados para datagramas traduzidos.

6.3.3 Network Address Port Translation and Packet Translation (NAPT-PT)

Tsirtsis e Srisuresh (2000) descrevem na RFC2766 que este mecanismo permite que haja comunicação entre máquinas IPv6 e IPv4 usando um único endereço IPv4. As portas TCP/UDP das máquinas IPv6 são traduzidas em porta TCP/UDP de endereços registrados IPv4.

Este mecanismo possui vantagem sobre o NAT-PT, pois permite um número máximo de 64 K de seções de TCP e 63 K para o UDP por endereço IPv4, antes que esgote as portas a serem designadas, já no NAT-PT possui um conjunto de endereços IPv4 que pode ser eliminado impedindo que outras máquinas IPv6 possam estabelecer conexões com a Internet enquanto este conjunto de endereços estiver alocado para outras máquinas.

6.3.4 Bump in the Stack (BIS)

Segundo descrito na RFC2767 por Tsuchiya, Higuchi e Atarashi (2000), este mecanismo se assemelha ao NAT-PT combinado com o SIIT, onde é implementado na pilha de protocolos do sistema operacional dentro de cada máquina. O SIIT caracteriza-se como sendo uma interface de tradução entre redes IPv6 e IPv4, já o BIS é uma interface de tradução entre aplicações IPv4 e redes IPv6.

Este mecanismo possui algumas limitações como a de permitir comunicação de IPv4 para IPv6, mas não ao contrário, pois não envia e nem recebe pacotes IPv4 na rede, se algumas aplicações IPv4 tentarem se comunicar usando o BIS não será possível sem que haja introdução de mecanismos de tradução entre as aplicações e também não funciona para comunicações *multicast*.

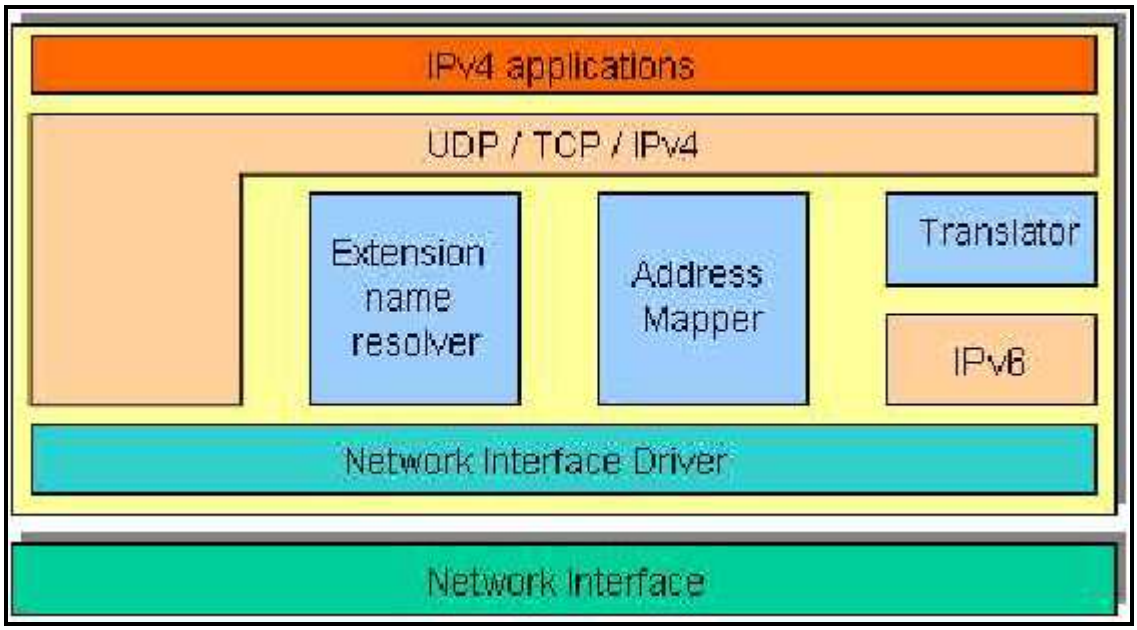

Figura 21. Esquema do mecanismo BIS.
Fonte: Adaptado de TSUCHIYA, K.; HIGUCHI, H; ATARASHI, Y.

Conforme observa-se na Figura 21, este mecanismo é baseado em pilha dupla onde são adicionados três módulos:

a) **o *translator*:** que sua única função é traduzir cabeçalhos IPv4 que estejam saindo, em cabeçalhos IPv6 e cabeçalhos IPv6 que estejam entrando, em cabeçalhos IPv4;

b) **módulo *address mapper*:** constitui numa lista de endereços IPv4 além das associações entre endereços IPv4 e IPv6. Ao receber um pacote IPv6 da rede e ser identificado que não existe entrada mapeada para ele, este módulo fornecerá um endereço para o *translator* reconhecer. É importante destacar que os endereços IPv4 jamais são transmitidos na rede, sendo assim não há a necessidade de serem endereços válidos, podendo-se usar uma lista de endereços privados;

c) **o módulo *extension name resolver*:** sua função é monitorar as perguntas IPv4 de DNS visando criar novas perguntas para resolver registros A e AAAA que após é retornado para a aplicação IPv4. Se retornar somente o registro AAAA, este módulo pede ao *address mapper* para estabelecer um endereço IPv4 que corresponda ao endereço IPv6;

6.3.5 Bump in the API (BIA)

Segundo descrito na RFC3338 de Lee et al (2002), este é um mecanismo parecido ao BIS, sendo que a diferença é que o BIA insere um tradutor API entre o socket API e os módulos TCP/IP da pilha da máquina IPv6, ao invés de traduzir cabeçalho entre IPv4 e IPv6. Sendo assim, as funções do socket API IPv4 são traduzidas em funções do socket API IPv6 e vice-versa. O mecanismo BIA é usado em sistemas que possui uma pilha IPv6, mas não possui aplicações para IPv6.

Suas vantagens em relação ao mecanismo BIS são a de possuir independência ao driver da interface de rede e não causa *overhead* na tradução dos cabeçalhos dos pacotes.

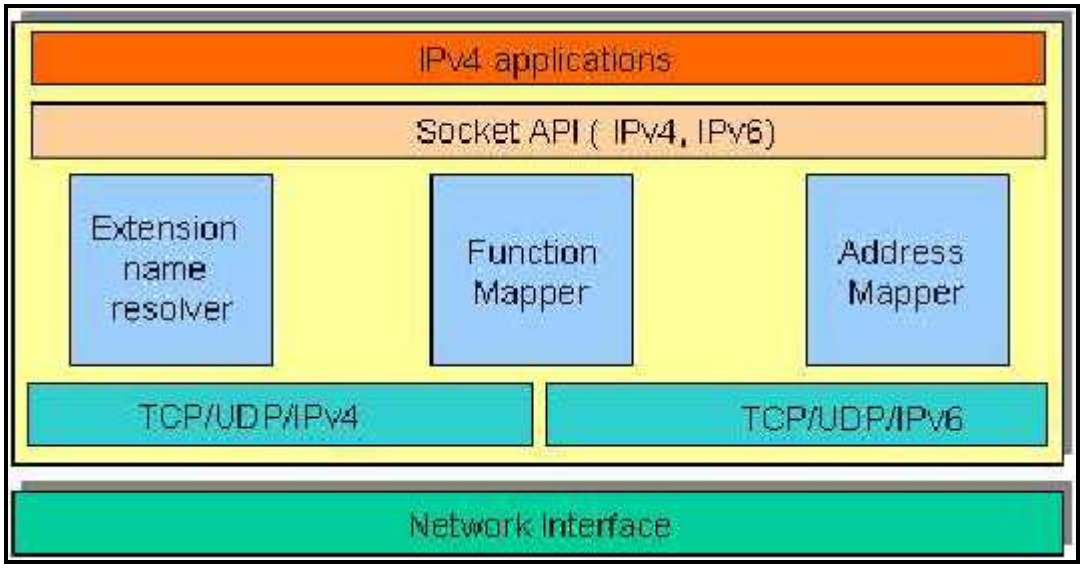

Figura 22. Esquema do mecanismo BIA
Fonte: Adaptado de LEE, G. et al (2002).

Conforme a Figura 22, o mecanismo BIA é baseado também na introdução de três módulos:

a) **módulo *extension name resolver*:** sua função é monitorar as perguntas IPv4 de DNS visando criar novas perguntas para resolver registros A e AAAA que após é retornado para a aplicação IPv4. Se retornar somente o registro AAAA, este módulo pede ao *address mapper* para estabelecer um endereço IPv4 que corresponda ao endereço IPv6;

b) **módulo *function mapper*:** caracteriza por mapear chamadas de *socket* IPv4 em chamadas de *socket* IPv6 e vice-versa. Após mapear, as chamadas de funções *socket* API IPv4 são interpretadas e realiza-se a solicitação de chamadas de funções *socket* API IPv6 correspondentes;

c) **módulo *address mapper*:** constitui numa lista de endereços IPv4 além das associações entre endereços IPv4 e IPv6. Ao receber um pacote IPv6 da rede e ser identificado que não existe entrada mapeada para ele, este

módulo fornecerá um endereço IPv4 para o *translator* reconhecer. É importante destacar que os endereços IPv4 jamais são transmitidos na rede, sendo assim não há a necessidade de serem endereços válidos, pode-se usar uma lista de endereços privados;

6.3.6 Transport Relay Translator (TRT)

Segundo Hagino e Yamamoto (2001) descrevem na RFC3142, este tradutor encontra-se na camada de transporte e permite que máquinas *IPv6-only* troque informações (TCP ou UDP) com máquinas *IPv4-only*. Neste caso não há necessidade de modificações nas máquinas, além de que um TRT rodando em uma máquina pilha dupla, pode usar um protocolo ao comunicar-se com o cliente e outro ao comunicar-se com o servidor de aplicação.

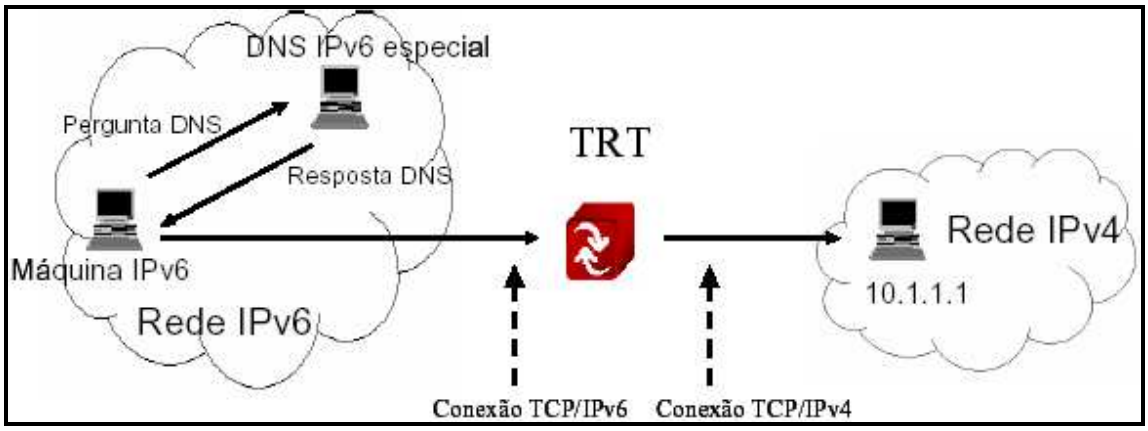

Figura 23. Esquema do mecanismo TRT
Fonte: Adaptado de HAGINO, J.; YAMAMOTO, K. (2001).

A Figura 23 ilustra este mecanismo. Quando é feita a tradução em TCP é recalculado o *checksum*, mantido estado necessário sobre qual cliente está conectado com qual *socket* do servidor e quando o cliente finalizar a comunicação deve-se remover este estado. Já na tradução em UDP, deve-se recalcular o *checksum* também, que é obrigatório em IPv6 e opcional em IPv4.

6.3.7 Socks

Segundo Kitamura (2001) descreve na RFC3089, este mecanismo pode ser considerado também como um *transport relay*, mas é usado referenciado como um protocolo *proxy* para ambiente cliente/servidor. Este mecanismo permite que duas máquinas cliente e servidor realizem conexões TCP e UDP por meio de um *proxy* conhecido como *Socks Server*. Este *proxy* atua como um *relay* de conexões TCP e UDP.

No momento que um cliente quiser conectar-se a um servidor de aplicação, ele configura uma conexão com um servidor *proxy* conhecido e pré-configurado usando um *proxy* especial. Então o cliente informa para o *proxy* o endereço IP e o número da porta do servidor com quem deseja se comunicar, e a partir disso o servidor *proxy* se responsabiliza em configurar uma conexão com o servidor de aplicação.

6.3.8 Application Layer Gateway (ALG)

Este mecanismo permite que usuários que estão por trás de *firewalls* ou de *gateway* NAT, usem aplicações de redes que não seria possível sem o uso dele. Para que isso ocorra o cliente deve abrir uma conexão com o ALG que estabelece uma conexão com o servidor, funcionando como um transmissor de requisições que saem e de dados que entram.

Pode-se citar um exemplo bastante usado que é o DNS-ALG. O DNS trata de resolução de nomes de *hosts* em endereços IP, por este motivo ele manipula endereços IPs em suas mensagens. Desta forma, é possível que haja a interoperabilidade pois podem ter *hosts IPv4-only, hosts IPv6-only* e *hosts* IPv4/IPv6, assim no serviço DNS *hosts IPv4-only* possuirão resolução de seus nomes no DNS para endereços IPv4

(registros A), nós *IPv6-only* possuirão resolverão de seus nomes no DNS para endereços IPv6 (registros AAAA) e nós IPv4/IPv6 possuirão resolução para ambos tipos de endereços (registros A e AAAA).

No caso de um *host IPv6-only* tentar iniciar uma comunicação com um *host IPv4-only*, sendo que os dois estão conectados a um NAT-PT, esta comunicação deve iniciar pela caracterização do nome do *host* e no momento que o *host IPv6-only* tentar obter o endereço IPv6 do *host IPv4-only* comunicando com o servidor DNS. Este deverá retornar o endereço IPv6 do tipo IPv4 mapeado que corresponde ao endereço IPv4 que está relacionado ao *host IPv4-only*. Para ser mais prático será usado a representação do endereço da seguinte forma: supondo que este *host* (*IPv4-only*) tivesse o endereço 200.254.245.1 deveria retornar o endereço ::FFFF:200.254.245.1, pois esta consulta está esperando por endereços IPv6 que é feito com o uso do DNS-ALG.

Da mesma forma, que foram classificados os mecanismo em sub-classes no tunelamento, os mecanismos de tradução podem ser classificados como:

a) **mecanismos de tradução da camada de rede:** os mecanismos com estas características são o SIIT, NAT-PT e NAPT-PT;
b) **mecanismos de tradução da camada de transporte:** neste classifica-se o TRT e Socks;
c) **mecanismos de tradução da camada de aplicação:** nesta camada encontra-se o ALG;
d) **mecanismos de tradução da camada adicional:** este se caracteriza pelos métodos que adicionam uma camada na pilha de protocolos. Dentre eles encontra-se o BIS e BIA.

Estes são os mecanismos e métodos disponíveis que podem ser implementados numa rede para possibilitar a comunicação entre protocolos IP e aplicações diferentes.

Para facilitar a compreensão do novo protocolo de endereçamento IP (IPv6) e os mecanismos de transição e convivência possíveis, surge a necessidade de desenvolver uma interface de apoio ao estudo com estas informações.

Pensando nisso, a seguir, será feita a descrição da interface desenvolvida. Com a explosão da era da informação, instituições estão direcionando cada vez mais o enfoque a interfaces de apoio ao ensino, por dois motivos: a inclusão digital e pela rapidez de aprendizado que interfaces computacionais proporcionam.

7 ESTUDO DA TRANSIÇÃO ENTRE PROTOCOLOS DE COMUNICAÇÃO IPv4 E IPv6

O presente trabalho consiste no estudo dos mecanismos de transição entre os protocolos IPv4 e IPv6 além do desenvolvimento de uma interface de apoio ao ensino, que mostre ao usuário as informações sobre os mecanismos de transição com seus métodos o funcionamento para o entendimento do mesmo.

A metodologia para a realização do trabalho foi iniciada com o levantamento bibliográfico a respeito dos temas da pesquisa. Em seguida, para o cumprimento dos objetivos, foram realizadas as seguintes etapas:

a) estudo sobre os protocolos IPv4 e IPv6;
b) estudo dos mecanismos de transição de protocolos IPv4 e IPv6;
c) modelagem da interface;
d) desenvolvimento da interface de apoio ao ensino;
e) descrição dos resultados obtidos.

7.1 ESTUDO DOS PROTOCOLOS IPV4 E IPV6

Consistiu no levantamento bibliográfico dos temas envolvidos na pesquisa, com o intuito de compreender e descrever o funcionamento das redes de computadores. Toda a pesquisa foi realizada com base em *Request for* Comments (RFC), que é um documento que descreve os padrões de uma tecnologia desenvolvida pela *Internet Engineering Task Force* (IETF). Nesta etapa foram encontradas algumas dificuldades por ser uma pesquisa direcionada a documentos bastante técnicos e toda literatura inglesa.

No levantamento bibliográfico sobre IPv4 e IPv6, foram comentadas as características de cada protocolo, as mudanças de cabeçalho e endereçamento, novas funcionalidades foram adicionadas, dentre muitos outros fatores.

7.2 ESTUDO DOS MECANISMOS DE TRANSIÇÃO DE PROTOCOLOS IPv4 e IPv6

Na comunicação entre os protocolos, vários cenários de comunicação podem ser encontrados, ou seja, pode ocorrer comunicação entre redes IPv4, redes IPv6 e redes IPv4 e IPv6 juntas. A seguir será feita uma abordagem destes cenários, bem como uma representação gráfica do funcionamento das mesmas.

Será demonstrado as formas de comunicação e a relação de cada um mecanismo com determinada arquitetura, onde será levado em consideração a aplicação de origem e destino, o pacote de origem e destino bem como a rede de trânsito destas informações.

7.2.1 Forma de comunicação entre redes IPv4

Na Figura 24, observa-se, duas redes IPv4 comunicando-se por redes de trânsito diferentes (IPv4 e IPv6). Observa-se que no primeiro caso (1), o fluxo de ida não apresenta necessidade de mecanismo de transição porque as redes e a rede de trânsito usam o IPv4. O mesmo acontece no segundo caso (2) com o fluxo de volta, onde também estão comunicando-se sobre arquiteturas IPv4. Porém, no terceiro (3) e quarto (4) caso é necessário o uso de algum mecanismo de transição, pois a rede de

trânsito está usando um protocolo diferente do protocolo das redes que estão envolvidas na comunicação.

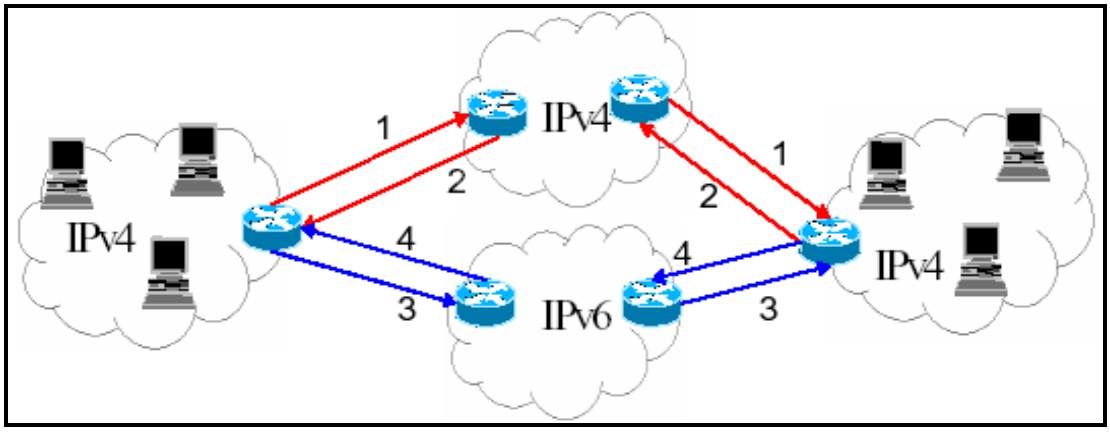

Figura 24. Esquema de comunicação entre redes IPv4
Fonte: Adaptado de GILLIGAN, R.; NORDMARK E. (2000).

Na Tabela 1 é mostrada esta comunicação de forma mais prática além da especificação dos mecanismos que são usados neste tipo de comunicação.

Tabela 1. Mecanismos usados na comunicação entre redes IPv4

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv4	IPv4	Caso (1): não tem necessidade de mecanismo de transição.	Caso (2): não tem necessidade de mecanismo de transição.
IPv4	IPv4	IPv6	IPv4	IPv4	Caso (3): Usa-se Tradução (nas camadas de rede, transporte ou aplicação) ou tunelamento 4to6.	Caso (3): Usa-se Tradução (nas camadas de rede, transporte ou aplicação) ou tunelamento 4to6.

Fonte: Adaptado de GILLIGAN, R.; NORDMARK E. (2000).

7.2.2 Forma de comunicação entre redes IPv6

Na Figura 25, pode-se observar a comunicação entre duas redes IPv6 usando redes de trânsito IPv4 e IPv6. Neste caso, tem-se o inverso do tipo anterior, onde o terceiro (3) e quarto (4) caso, por serem redes que usam o mesmo protocolo de rede IPv6, não há necessidade de mecanismos de transição. Já no primeiro (1) e segundo (2)

caso, a comunicação é entre protocolo IPv6, mas a rede de trânsito é IPv4, então há necessidade do uso de mecanismo de transição.

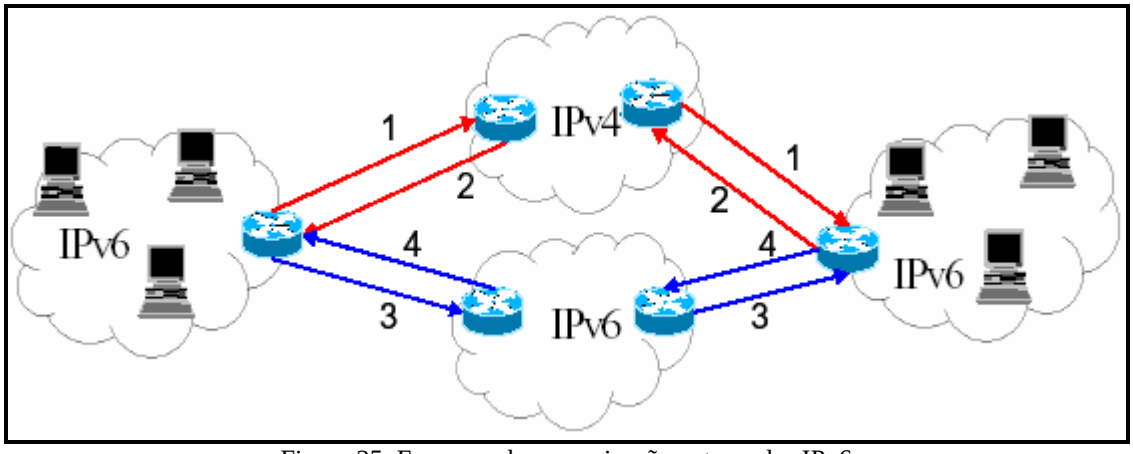

Figura 25. Esquema de comunicação entre redes IPv6
Fonte: Adaptado de GILLIGAN, R.; NORDMARK E. (2000).

Na Tabela 2, observa-se esta comunicação de forma mais prática além da especificação dos mecanismos que são usados neste tipo de comunicação.

Tabela 2. Mecanismos usados na comunicação entre redes IPv6

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv6	IPv6	IPv4	IPv6	IPv6	Caso (1): Usa-se Tradução (nas camadas de rede, transporte ou aplicação) ou tunelamento (do tipo 4to6, interno ou IPv6-over-IPv4).	Caso (2): Usa-se Tradução (nas camadas de rede, transporte ou aplicação) ou tunelamento (do tipo 4to6, interno ou IPv6-over-IPv4).
IPv6	IPv6	IPv6	IPv6	IPv6	Caso (3): não tem necessidade de mecanismo de transição.	Caso (3): não tem necessidade de mecanismo de transição.

Fonte: Adaptado de GILLIGAN, R.; NORDMARK E. (2000).

7.2.3 Forma de comunicação entre redes IPv4 e IPv6

Conforme a Figura 26 observa-se que existe uma rede IPv4 realizando comunicação com uma rede IPv6 por redes de trânsito diferentes (IPv4 e IPv6). Em todos os casos (1, 2, 3 e 4), existe necessidade do uso de mecanismos de transição por se

comunicarem entre redes que usam protocolos diferentes, conforme mostrado na Tabela 3.

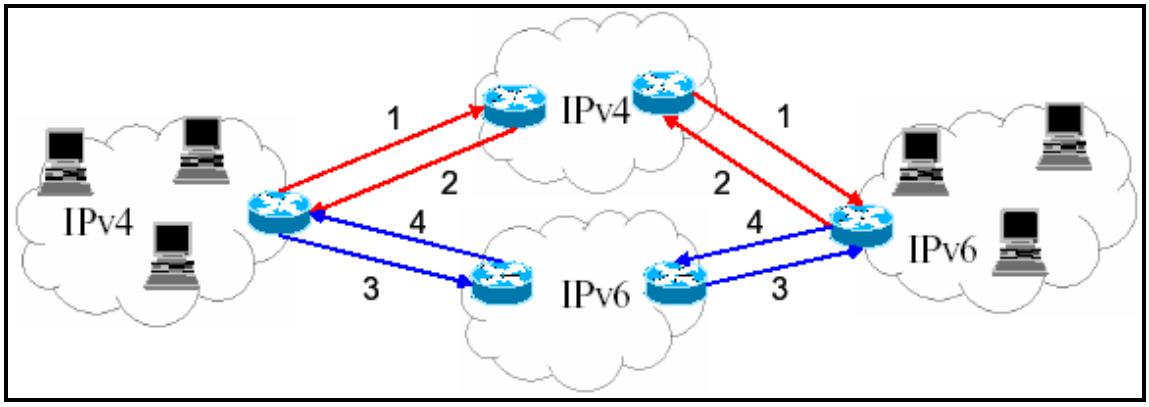

Figura 26. Esquema de comunicação entre redes IPv4 e IPv6
Fonte: Adaptado de GILLIGAN, R.; NORDMARK E. (2000).

Tabela 3. Mecanismos usados na comunicação entre redes IPv4 e IPv6

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv6	IPv6	Caso (1): Usa-se Tradução (nas camadas de rede, transporte ou aplicação) ou tunelamento no servidor (origem IPv4).	Caso (2): Usa-se Tradução (nas camadas de rede, transporte ou aplicação).
IPv4	IPv4	IPv6	IPv6	IPv6	Caso (3): Usa-se Tradução (nas camadas de rede, transporte ou aplicação) ou tunelamento no servidor (origem IPv4).	Caso (3): Usa-se Tradução (nas camadas de rede, transporte ou aplicação).

Fonte: Adaptado de GILLIGAN, R.; NORDMARK E. (2000).

7.2.4 Forma de comunicação entre redes IPv4 e IPv6 com aplicação IPv4

Neste tipo, aparentemente não existe diferença do citado anteriormente, mas na Figura 27 existe uma comunicação de uma rede IPv4 com IPv6 usando redes de trânsito IPv4 ou IPv6, onde a aplicação IPv4 que está rodando dentro da rede IPv6 não foi migrada ainda, exigindo o uso de mecanismos de transição específicos. Logo abaixo, observa-se na Tabela 4 os mecanismos utilizados para esta transição.

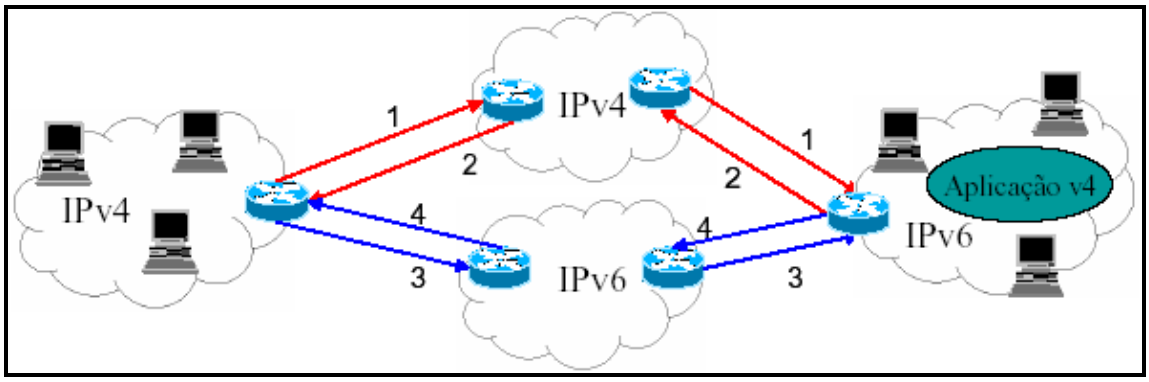

Figura 27. Esquema de comunicação entre redes IPv4 e IPv6 com aplicação IPv4
Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

Tabela 4. Mecanismos usados na comunicação entre redes IPv4 e IPv6 com aplicação IPv4

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv6	IPv4	Caso (1): Usa-se Tradução combinada com tunelamento via servidor (origem IPv4) ou tradução (nas camadas de rede, transporte ou aplicação).	Caso (2): Usa-se tunelamento via servidor (origem IPv6).
IPv4	IPv4	IPv6	IPv6	IPv4	Caso (3): Usa-se Tradução combinada com tunelamento via servidor (origem IPv4) ou tradução (nas camadas de rede, transporte ou aplicação).	Caso (3): Usa-se tunelamento via servidor (origem IPv6).

Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

7.2.5 Forma de comunicação entre redes IPv6 com aplicação de origem IPv4

Neste caso existe a comunicação entre duas redes IPv6 por redes de trânsito IPv4 ou IPv6 conforme a Figura 28. Porém neste caso existe uma aplicação IPv4 dentro de uma rede IPv6 origem. No entanto, a aplicação está executando na máquina em IPv4 mas quando sai o pacote, este é IPv6. Conforme a Tabela 5 é possível usar certos mecanismos para realizar a transição destes pacotes.

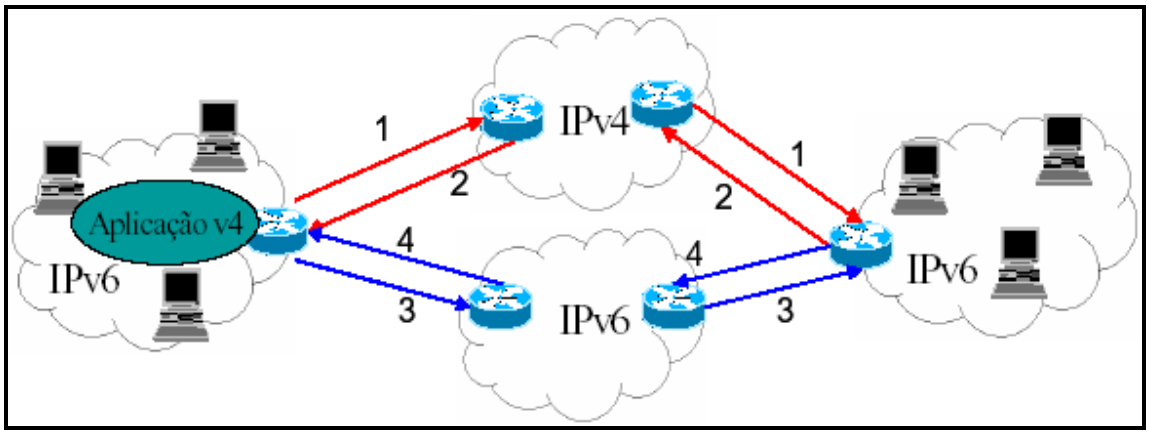

Figura 28. Esquema de comunicação entre redes IPv6 com aplicação de origem IPv4
Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

Tabela 5. Mecanismos usados na comunicação entre redes IPv6 com aplicação de origem IPv4.

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv6	IPv4	IPv6	IPv6	Caso (1): Usa-se Tradução combinada com tunelamento (do tipo 6to4 ou IPv6-over-IPv4) ou tradução (nas camadas de rede, transporte ou aplicação).	Caso (2): Usa-se Tradução combinada com tunelamento (do tipo 6to4 ou IPv6-over-IPv4) ou tradução (nas camadas de rede, transporte ou aplicação).
IPv4	IPv6	IPv6	IPv6	IPv6	Caso (3): Usa-se Tradução.	Caso (3): Usa-se Tradução.

Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

7.2.6 Forma de comunicação entre aplicações IPv4 em redes IPv6

Conforme visualiza-se na Figura 29, existe a comunicação entre duas redes IPv6, por redes de trânsito IPv4 ou IPv6, mas dentro das duas redes existem aplicações IPv4 que não foi feita a migração ainda para IPv6. Na Tabela 6, verifica-se também os mecanismos que são possíveis ser aplicados neste caso.

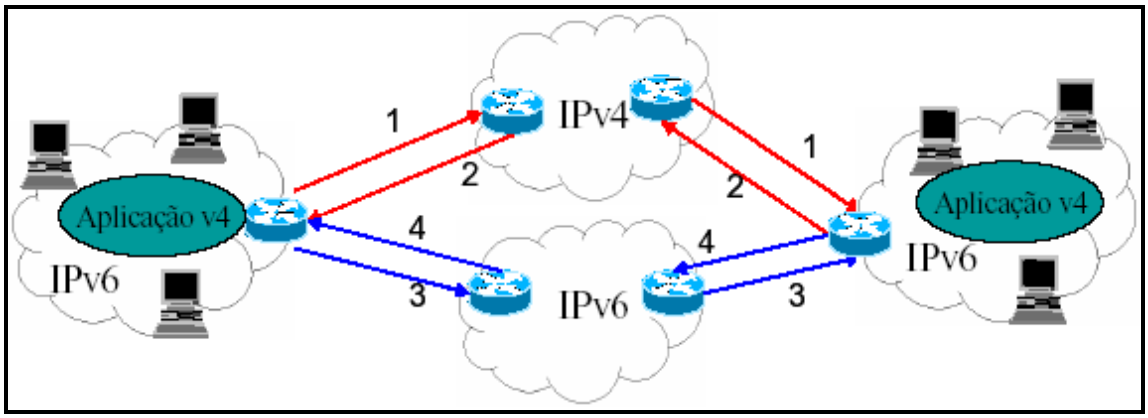

Figura 29. Esquema de comunicação entre aplicações IPv4 em redes IPv6
Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

Tabela 6. Mecanismos usados na comunicação entre aplicações IPv4 em redes IPv6

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv6	IPv4	Caso (1): Usa-se Tradução combinada com tunelamento via servidor (origem IPv4) ou tradução (nas camadas de rede, transporte ou aplicação).	Caso (2): Usa-se tunelamento via servidor (origem IPv6).
IPv4	IPv4	IPv6	IPv6	IPv4	Caso (3): Usa-se Tradução combinada com tunelamento via servidor (origem IPv4) ou tradução (nas camadas de rede, transporte ou aplicação).	Caso (3): Usa-se tunelamento via servidor (origem IPv6).

Fonte: Adaptado de CARPENTER, B.; MOORE, K. (2001).

7.3 MODELAGEM DA INTERFACE GRÁFICA

A modelagem do *InterativeIP* (nome dado a interface de apoio ao ensino implementada) foi elaborada visando principalmente facilitar o desenvolvimento da interface, como também a interação do usuário com a mesma, deixando-a simples e padronizada em relação aos seus módulos.

Na modelagem do *InterativeIP*, utilizou-se a *Unified Modeling Language* (UML), realizando-se o diagramas de atividades.

O diagrama de atividades do *InterativeIP*, que demonstra o aspecto dinâmico do sistema, pode ser visualizado na Figura 30. Essas ações consistem em:

a) **entrada do sistema:** no momento que o usuário executar o sistema, a interface entrará direto ao sistema no menu principal;
b) **estudo IPs:** abre uma aba com duas opções: IPv4 e IPv6;
c) **IPv4:** abre uma nova janela com o estudo sobre este protocolo onde tem os botões: home, sobre o IPv4, características, datagrama, endereçamento, ICMPv6, referências e retornar;
d) **IPv6:** abre uma nova janela com o estudo sobre este protocolo onde tem os botões: home, sobre o IPv4, características, datagrama, endereçamento, ICMPv6, IPv6 no mundo referências e retornar;
e) **transição:** mostra a aba com as opções: Dual Stack, Tunelamento e Tradução;
f) **dual stack:** mostra o conteúdo sobre o mecanismo de transição *dual stack*;
g) **tunelamento:** no momento que o mouse passar por cima da aba tunelamento vai mostrar os seguintes ícones: Túnel Configurado, Tunnel Broker, Túnel Automático, IPv6-to-IPv4, IPv6-over-IPv4, ISATAP, Teredo e DSTM que se clicar em cada um deles, mostra o conteúdo do método clicado;
h) **transição:** no momento que o mouse passar por cima da aba transição vai mostrar os seguintes ícones: SIIT, NAT-PT, NAPT-PT, BIS, BIA, TRT, Socks e ALG que se clicar em cada um deles, mostra o conteúdo do método clicado;

i) **simulação:** ao clicar nesta opção no menu, abrirá uma aba com o nome de Simulação Gráfica;

j) **simula gráfica:** esta opção ao clicar deveria mostrar uma simulação gráfica mostrando a troca de um pacote entre redes IPv4 e IPv6 usando os mecanismos de transição Dual-Stack e Tunelamento. Esta simulação foi desenvolvida a parte de ações e o código fonte construída em forma de Applet mas não foi adicionado os objetos para a visualização da simulação;

k) **ajuda:** ao clicar neste menu, abrirá uma aba com o nome de Sobre a Ferramenta;

l) **sobre a ferramenta:** ao clicar nesta aba, abrirá uma nova janela com os botões menu, resumo e retornar. Esta tela mostrará um breve resumo do desenvolvimento, além do desenvolvedor, orientador entre outras informações.

m) **Sair:** ao clicar em sair vai encerar o sistema.

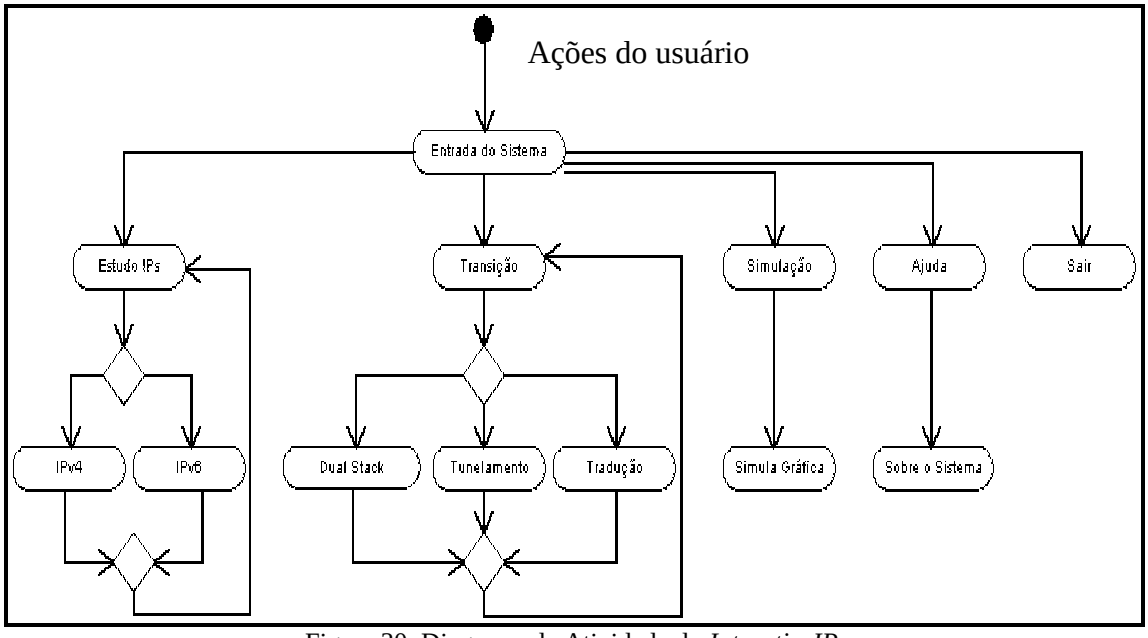

Figura 30. Diagrama de Atividade do *InterativeIP*

7.4 DESENVOLVIMENTO DA INTERFACE DE APOIO AO ENSINO

A interface foi implementada na Linguagem Java devido a algumas de suas várias características, como: permite reutilização de código, as aplicações em Java rodam em qualquer sistema operacional (multiplataforma) e suas ferramentas de programação são gratuitas. O ambiente de programação Java utilizado para esta interface foi o NetBeans 5.0. Os textos adicionados no visualizador é sincronizado com programação html e o código fonte da Simulação foi desenvolvido em *Applet* conforme anexo no CD que acompanha este trabalho.

7.5 DESCRIÇÃO DOS RESULTADOS OBTIDOS

Com relação aos resultados obtidos foram abordados os mecanismos de transição disponíveis e classificados seus usos conforme o cenário de rede existente. Em paralelo a este estudo foi desenvolvido uma interface visual usando o NetBenas 5.0 e HTML para que leigos possam conhecer as características de mecanismo e seus respectivos métodos.

Conforma e Figura 31 veja como ficou a interface gráfica do usuário.

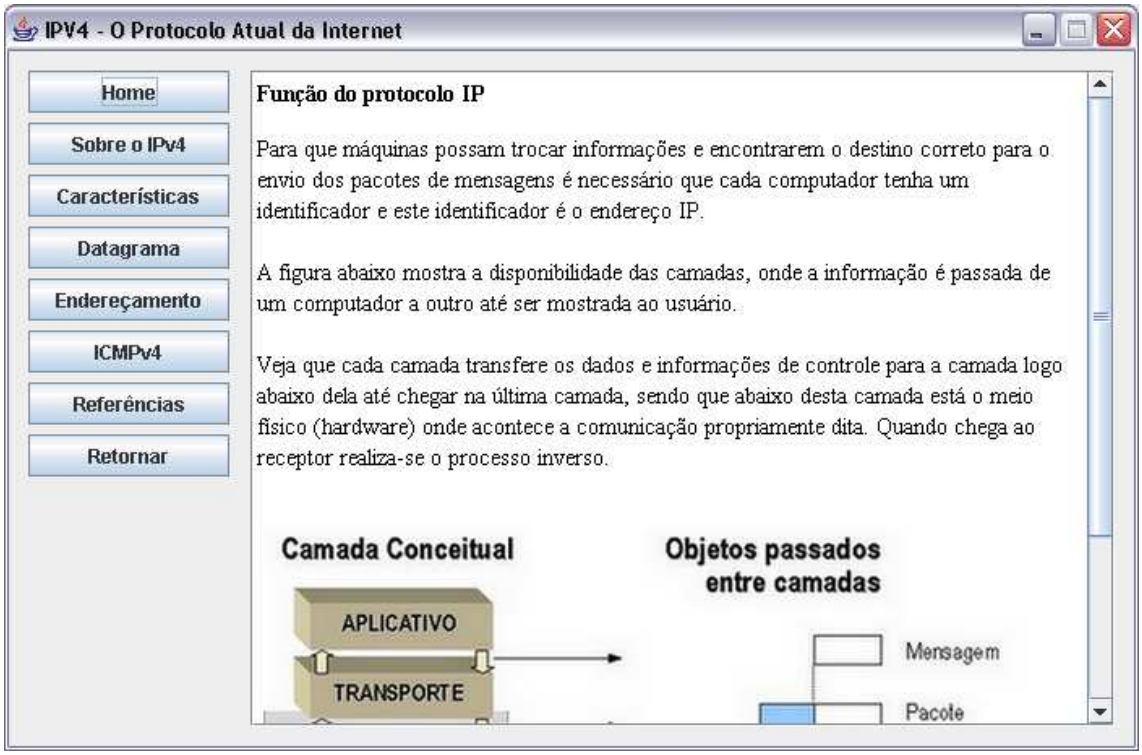

Figura 31. Tela do estudo do protocolo IPv4

Esta é a tela de visualização de informações sobre o protocolo IPv4, conforme for clicando nos botões a esquerda vai mostrar a informação correspondente ao título do botão. A tela do estudo de protocolos IPv6 possui o mesmo formato, a única diferença é que aquela possui um botão a mais que é sobre o IPv6 no mundo e as informações contidas nela.

A Figura 32 mostra a disponibilidade dos Menus da tela principal.

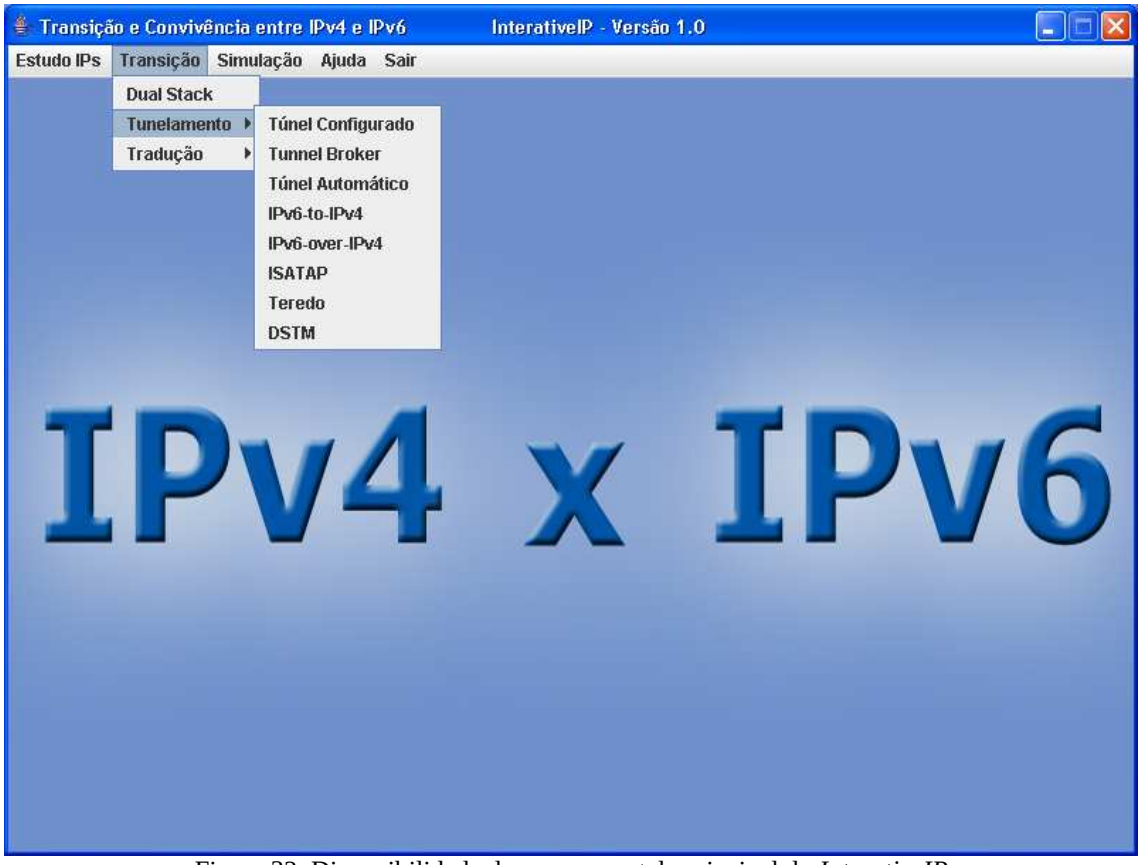

Figura 32. Disponibilidade dos menus na tela principal do *InterativeIP*

A Figura 33 ilustra a disposição da tela sobre o estudo de mecanismos de transição mostrada ao usuário.

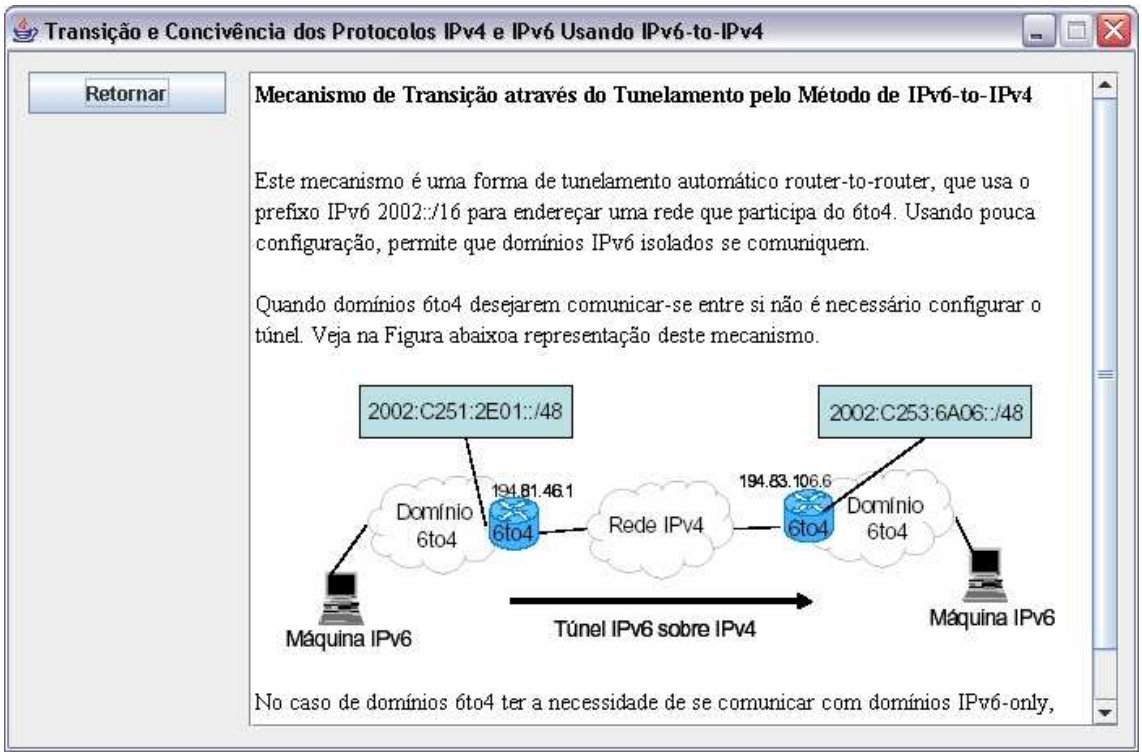

Figura 33. Tela de estudo dos mecanismos de transição.

CONCLUSÃO

Esta pesquisa demonstrou a importância do conhecimento dos mecanismos de transição e convivência entre os protocolos IPv4 e IPv6, bem como os tipos de mecanismos que deveremos utilizar dependendo do cenário de redes existente.

Com este intuito, foi realizado um estudo sobre os mecanismos de transição disponível e que podem ser implementados para que máquinas de arquiteturas IP diferentes possam traçar informações regularmente. Além do estudo destes mecanismos foi desenvolvido uma interface de apoio ao estudo para facilitar o entendimento do leitor, já que é um assunto bastante complexo.

Conforme a metodologia proposta, foi realizado o estudo dos protocolos IPv4 e IPv6, especificando seus datagramas, endereçamento, formato dos pacotes, origem e a necessidade para que os mesmo trabalhem juntos durante algum tempo enquanto que sejam migradas as redes gradualmente para o IPv6.

Também realizou-se a descrição dos mecanismos de transição entre os protocolos. Foram definidas as características de cada um e o funcionamento.

Usaram-se os diagramas de use case e de atividades para realizar a modelagem da interface gráfica para facilitar o desenvolvimento da interface, como também a interação do usuário com a interface.

A simulação gráfica não foi totalmente concluída pela dificuldade que tive em aprender a programar *applet* que foi a única forma em java que eu encontrei para implementar esta simulação, mas o código fonte parcial da mesma está pronta conforme está em anexo no CD que acompanha este trabalho.

Sugere-se como trabalhos futuros:

a) Implementar a comunicação entre os protocolos IPv4 e IPv6 usando pacotes de mensagem real, para obter uma simulação eficiente;
b) Melhorar as interfaces gráficas com o usuário e abordar mais informações sobre a tecnologia IPv6 e os mecanismo de transição;
c) Concluir o desenvolvimento da simulação gráfica de uma comunicação entre os protocolos IPv4 e IPv6 em redes com arquiteturas diferentes;
d) Implementar uma ferramenta de apoio ao ensino, abordando os conceitos do uso do computador no ensino aprendizagem e que ofereça maior interatividade com o usuário;
e) Realizar uma aplicação experimental configurando o protocolo IPv6 em algumas máquinas e fazendo a mesma comunicar-se com outras máquinas que estejam usando redes e aplicações IPv4.

REFERÊNCIAS

AMENTT, Matthew F.; DULANEY, Emmett; HARPER, Eric. **Desvendando o TCP/IP.** Tradução: ARX Publicações. Rio de Janeiro: Campus, 1997.

BOUND, J. et al. NGTRANS Working Group. **DRAFT:** Dual Stack Transition Mechanism (DSTM). July 2001. Disponível em: <http http://www.rennes.enst-retagne.fr/~toutain/draft-ietf-ngtrans-dstm-04.txt >. Acesso em: 29 mai. 2006.

CARPENTER, B.; JUNG, C. Network Working Group. **Request for Comments 2529:** Transmission of IPv6 over IPv4 Domains without Explicit Tunnels. March 1999. Disponível em: <http://www.ietf.org/rfc/rfc2529.txt>. Acesso em: 02 abr. 2006.

CARPENTER, B.; MOORE, K. Network Working Group. **Request for Comments 3056:** Connection of IPv6 Domains via IPv4 Clouds. February 2001. Disponível em: <http://www.ietf.org/rfc/rfc3056.txt>. Acesso em: 06 abr. 2006.

COMER, Douglas E.; STEVENS, David L. **Interligação em redes com TCP/IP.** Tradução: Ana Maria Neto Guz. Vol. II. Rio de Janeiro: Campus, 1999.

COMER, Douglas E. **Redes de Computadores e Internet.** Tradução: Marinho Barcellos. 2. ed. Porto Alegre: Bookman, 2001.

CONTA, A.; DEERING, S. Network Working Group. **Request for Comments 2463:** Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. December 1998. Disponível em: <http://www.ietf.org/rfc/rfc2463.txt>. Acesso em: 16 abr. 2006.

DARPA. DARPA Internet Program. **Request for Comments 791:** Internet Protocol. September 1981. Disponível em: <http://www.ietf.org/rfc/rfc0791.txt>. Acesso em: 23 out. 2005.

DEERING, S.; HINDEN, R. Network Working Group. **Request for Comments 2460:** Internet Protocol Version 6 (IPv6) Specification. December 1998. Disponível em: <http://www.ietf.org/rfc/rfc2460.txt>. Acesso em: 11 nov. 2005.

DURAND, A. et al. Network Working Group. **Request for Comments 3053:** IPv6 Tunnel Broker. January 2001. Disponível em: <http://www.ietf.org/rfc/rfc3053.txt>. Acesso em: 27 abr. 2006.

GILLIGAN, R.; NORDMARK E. Network Working Group. **Request for Comments 2893:** Transition Mechanisms for IPv6 Hosts and Routers. August 2000. Disponível em: <http://www.ietf.org/rfc/rfc2893.txt>. Acesso em: 02 mai. 2006.

HABERMAN, B.; Network Working Group. **Request for Comments 3590:** Source Address Selection for the Multicast Listener Discovery (MLD) Protocol. September 2003. Disponível em: <http://www.ietf.org/rfc/rfc3590.txt>. Acesso em: 19 abr. 2006.

HAGINO, J.; YAMAMOTO, K. Network Working Group. **Request for Comments 3142:** An IPv6-to-IPv4 Transport Relay Translator. June 2001. Disponível em: <http://www.ietf.org/rfc/rfc3142.txt>. Acesso em: 15 mai. 2006.

HINDER, R.; DEERING, S. Network Working Group. **Request for Comments 3513:** Internet Protocol Version 6 (IPv6) Addressing Architecture. April 2003. Disponível em: http://www.ietf.org/rfc/rfc3513.txt>. Acesso em: 23 nov. 2005.

HUITEMA, C. Network Working Group. **Request for Comments 4380:** Teredo - Tunneling IPv6 over UDP through Network Address Translations (NATs). February 2006. Disponível em: <http://www.ietf.org/rfc/rfc4380.txt>. Acesso em: 18 mai. 2006.

KENT, S.; ATKINSON, R. Working Group. **Request for Comments 2406:** IP Encapsulating Security Payload (ESP). November 1998. Disponível em: <http://www.ietf.org/rfc/rfc2406.txt>. Acesso em: 13 mai. 2006.

KITAMURA, H. Network Working Group. **Request for Comments 3089:** A SOCKS-based IPv6/IPv4 Gateway Mechanism. April 2001. Disponível em: <http://www.ietf.org/rfc/rfc3089.txt>. Acesso em: 13 mai. 2006.

KRISHNAMURTHY, Balachander; REXFORD, Jennifer. **Redes para a Web.** Tradução: Daniel Vieira. Rio de Janeiro: Campus, 2001.

KUROSE, James F.; ROSS, Keith W. **Computer networking:** a top-down approach featurig the internet. Boston: Addison Wesley, 2001.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem to-down. Tradução: Arlete Simille Marques. 3. ed. São Paulo: Pearson Addison Wesley, 2005.

LEE, S. et al. Network Working Group. **Request for Comments 3338:** Dual Stack Hosts using “Bump-In-the-API” (BIA). October 2002. Disponível em: <http://www.ietf.org/rfc/rfc3338.txt>. Acesso em: 14 mai. 2006.

MOURA, José A. B. et al. **Redes de Computadores:** Serviços, Administração e Segurança. São Paulo: Makron Books, 1999.

NARTEN, T.; NORDMARK, E.; SIMPSON, W. Network Working Group. **Request for Comments 2461:** Neighbor Discovery for IP Version 6 (IPv6). December 1998. Disponível em: <http://www.ietf.org/rfc/rfc2461.txt>. Acesso em: 14 mai. 2006.

NORDMARK, E. Network Working Group. **Request for Comments 2765:** Stateless IP/ICMP Translation Algorithm (SIIT). February 2000. Disponível em: <http://www.ietf.org/rfc/rfc2765.txt>. Acesso em: 13 mai. 2006.

PETERSON, Larry L.; DAVIE, Bruce S. **Redes de Computadores:** uma abordagem de sistemas. Tradução: Daniel Vieira. Rio de Janeiro: Elsevier, 2004.

PINHEIRO, José M. S. **O Modelo OSI.** Projeto de Redes. 22 nov. 2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php>. Acesso em: 24 out. 2005.

SOARES, Luiz F. G.; LEMOS, Guido; COLCHER, Sérgio. **Redes de cumputadores das LANs, MANs e WANs às Redes ATM.** 2. ed. Rio de Janeiro: Campus, 1995.

SRISURESH, P.; EGEVANG, K. Network Working Group. **Request for Comments 3022:** Tradicional IP Network Address Translator (Traditional NAT). January 2001. Disponível em: <http://www.ietf.org/rfc/rfc3022.txt>. Acesso em: 17 mai 2006.

TANENBAUM, Andrew S. **Redes de Computadores.** Tradução: Insight serviços de informática. 3. ed. Rio de Janeiro: Campus, 1997.

TANENBAUM, Andrew S. **Redes de computadores.** Tradução: Vandenberg D. de Souza. 4. ed. Rio de Janeiro: Campus, 2003.

TEMPLIN, F. et al. Network Working Group. **Request for Comments 4214:** Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). October 2005. Disponível em: <http://www.ietf.org/rfc/rfc4214.txt>. Acesso em: 15 mai. 2006.

THOMSON, S.; NARTEN, T. Network Working Group. **Request for Comments 2462:** IPv6 Stateless Address Autoconfiguration. December 1998. Disponível em: <http://www.ietf.org/rfc/rfc2462.txt>. Acesso em: 19 mai. 2006.

TORRES, Gabriel. **Redes de Computadores:** curso completo. Rio de Janeiro: Axcel Books, 2001.

TSIRTSIS, G.; SRISURESH, P. Network Working Group. **Request for Comments 2766:** Network Address Translation - Protocol Translation (NAT-PT). February 2000. Disponível em: <http://www.ietf.org/rfc/rfc2766.txt>. Acesso em: 17 mai. 2006.

TSUCHIYA, K.; HIGUCHI, H.; ATARASHI, Y. Network Working Group. **Request for Comments 2767:** Dual Stack Hosts using the “Bump-In-the-Stack” Technique (BIS). February 2000. Disponível em: <http://www.ietf.org/rfc/rfc2767.txt>. Acesso em: 17 mai. 2006.

BIBLIOGRAFIA RECOMENDADA

6BONE*:* testbed for deployment of IPv6. Disponível em: <http://www.6bone.net>. Acesso em: 22 mai. 2006.

ARIN - American Registry for Internet Numbers. Disponível em: <http://www.arin.net>. Acesso em: 13 mai. 2006.

CALLON, R.; HASKIN, D. Network Working Group. **Request for Comments 2185:** Routing Aspects Of IPv6 Transition. September 1997. Disponível em: <http://www.ietf.org/rfc/rfc2185.txt>. Acesso em: 26 fev. 2006.

IANA - Internet Assigned Numbers Authority. Disponível em: <http://www.iana.org>. Acesso em: 09 mai. 2006.

IETF - Internet Engineering Task Force. Disponível em: <http://www.ietf.org>. Acesso em: 14 mai. 2006.

HILGENSTIELER, Fernando. **Protótipo de software para monitoração do cabeçalho do protocolo HTTP em uma rede TCP/IP.** 2003. 51 f. Monografia (Bacharel em Ciência da Computação) – Universidade Regional de Blumenau, Blumenau, 2003.

KARING, Anderson. **Protótipo de um sistema de monitoramento de desempenho de redes de computadores baseado no protocolo SNMPv3.** 2002. 117 f. Monografia (Bacharel em Ciência da Computação) – Universidade Regional de Blumenau, Blumenau, 2002.

LACNIC - Latin American and Caribbean Internet Addresses Registry. Disponível em: <http://www.lacnic.net>. Acesso em: 18 mai. 2006.

MURHAMMER, Martin W. et al. **TCP/IP:** Tutorial e Técnico. Tradução: Jussara Licinia Souza Gaertner. São Paulo: Makron Books, 2000.

PARTRIDGE, C.; MILLIKEN, W. Network Working Group. **Request for Comments 1546:** Host Anycasting Service. November 1993. Disponível em: <http://www.ietf.org/rfc/rfc1546.txt>. Acesso em: 23 mai. 2006.

RNP - Rede Nacional de Ensino e Pesquisa (RNP). Disponível em: <http://www.rnp.br>. Acesso em: 12 mai. 2006.

TEMPLIN, F. et al. **Draft IETF NGTRANS ESATAP:** Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). January 2002. Disponível em: <http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-ngtrans-isatap-03.txt>. Acesso em: 29 mai. 2006.

ULLMANN, R. Network Working Group. **Request for Comments 1475:** TP/IX: The Next Internet. June 1993. Disponível em: <http://www.ietf.org/rfc/rfc1475.txt>. Acesso em: 12 abr. 2006.