UNIVERSIDADE FEDERAL DE SANTA CATARINA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

EDSON ALEXANDRE DOMINGUES MORENO

ASPECTOS DE TRANSIÇÃO DO PROTOCOLO IPv4 PARA O IPv6

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Orientador: MAURO ROISENBERG

Florianópolis, Março de 2002

ASPECTOS DE TRANSIÇÃO DO PROTOCOLO IPv4 PARA O IPv6

Edson Alexandre Domingues Moreno

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação (Área de Concentração Sistemas de Computação) e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Fernando A. Ostune Galthier, Dr. Eng.

Banca Examinadora

Mauro Roisenberg, Dr.

Jorge Muniz Barreto, Dr.

Vitório Bruno Bazzola, Dr.

"Não basta ensinar ao homem uma especialidade, porque o tornará assim uma máquina utilizável, mas não uma personalidade. É necessário que adquira um sentimento, um senso prático daquilo que vale a pena ser empreendido, daquilo que é belo, do que é moralmente correto A não ser assim, ele se assemelhará, com seus conhecimentos profissionais, mais a um cão ensinado do que a uma criatura harmoniosamente desenvolvida. Deve aprender a compreender as motivações dos homens, suas quimeras e suas angústias, para determinar com exatidão seu lugar preciso em relação a seus próximos e a comunidade."

Albert Einstein

AGRADECIMENTOS

A DEUS pela oportunidade oferecida a este simples mortal.

À família, pelo apoio, consideração e compreensão, especialmente Karina, minha amada esposa.

Ao professor Mauro Roisenberg pela paciência e orientação durante todo o trabalho.

Aos professores da UFSC com quem convivi e muito aprendi.

Aos amigos aqui conquistados.

À todas as pessoas que contribuíram direta e indiretamente para a conclusão deste trabalho.

SUMÁRIO

	Lista de Figuras	viii
	Lista de Tabelas	ix
	Abreviatura e Siglas	x
	Resumo	xii
	Absctract	xiii
1.	**INTRODUÇÃO**	14
1.1.	Motivação	16
1.2.	Objetivo	17
1.2.1.	Objetivos Gerais	17
1.2.2.	Objetivos Específicos	17
1.3.	Organização do Texto	18
2.	**INTERNET**	19
2.1.	Introdução	19
2.2.	Histórico	20
2.3.	Internet 2	25
2.4.	Órgãos Regulamentadores	26
2.4.1.	IETF – *Internet Engineering Task Force*	27
2.4.2.	ISOC – *Internet Society*	28
2.4.3.	IAB - *Internet Archetcture Board*	29
2.4.4.	IRTF – *Internet Research Task Force*	30
2.4.5.	IANA – *Internet Assigned Number Authority*	30
2.4.6.	Comitê Gestor Internet no Brasil	31
3.	**A ARQUITETURA DA REDE INTERNET**	32
3.1.	Introdução	32
3.2.	Os Protocolos da Internet	32
3.2.1.	Os Protocolos TCP/IP	33
3.2.1.1	Comparação entre as arquiteturas TCP/IP e OSI	34

4.	**O PROTOCOLO INTERNET IP VERSÃO 4 (IPv4)**	40
4.1.	Introdução	40
4.2.	Endereçamento IPv4	46
4.2.1.	Endereços Especiais	51
4.2.1.1.	Broadcast e Multicast	52
5.	**O PROTOCOLO INTERNET IP VERSÃO 6 (IPv6)**	54
5.1.	Introdução	54
5.2.	Cabeçalho de Extensão IPv6	60
5.2.1.	Formato das Opções	62
5.2.2.	Opções de enchimento: Pad 1 e PadN	63
5.2.3.	Cabeçalho de extensão "*Hop-by-Hop Options*"	64
5.2.4.	Cabeçalho de extensão "*Routing*"	65
5.2.5.	Cabeçalho de extensão "*Fragment*"	66
5.2.6.	Cabeçalhos de extensão "*Destination Options*"	68
5.2.7.	Ausência de Cabeçalho de Extensão Seguinte	68
5.3.	Propósito do Projeto IPv6	69
5.3.1.	Endereçamento	69
5.3.1.1.	Endereçamento *Multicasting*	73
5.3.1.2.	Endereçamento *Unicasting*	75
5.3.1.3.	Endereçamento *Anycasting*	76
5.3.2.	Segurança	77
5.3.3.	Desempenho	78
6.	**TRANSIÇÃO IPv4 PARA IPv6**	80
6.1.	Introdução	80
6.2.	Exigências Para Transição	81
6.2.1.	Minimizando a Resistência	82
6.3.	Componentes de Transição	82
6.3.1.	Hosts	82
6.3.2.	DNS	83
6.4.	Técnicas de Transição	84
6.4.1.	Camada Dupla (*Dual Stack*)	85
6.4.2	Túneis IPv6 em IPv4	86

6.5. Migrando Aplicações 88
6.6 Considerações Finais 88

7. **CONCLUSÃO** 90
7.1. Considerações Iniciais 90
7.2. Resultados Alcançados 91

REFERÊNCIAS BIBLIOGRÁFICAS 93

Lista de Figuras

Figura nº	Identificação da figura	Página
1	Camadas da Arquitetura de Rede Internet	33
2	Comparação entre as arquiteturas OSI e TCP/IP	35
3	Funcionamento do TCP/IP	39
4	A Estrutura do Datagrama Protocolo IPv4	41
5	Formato Original do Campo Tipo de Serviço	42
6	Formato dos Endereços IP	46
7	Estrutura do Datagrama Protocolo IPv6	57
8	Prioridade Para Tráfego com Controle de Congestionamento	59
9	Datagrama Protocolo IPv6 com Cabeçalhos de Extensão	60
10	Formato das Opções Individuais dos Cabeçalhos de Extensão	62
11	Formato do Cabeçalho de Extensão *Hop-By-Hop*	64
12	Formato do Cabeçalho de Extensão *Routing*	65
13	Formato do Cabeçalho de Extensão *Fragmentation*	66
14	Formato do Cabeçalho de Extensão *Destination Options*	68
15	Exemplo de Um Endereço IPv6	70
16	O Mesmo Endereço da Fig. 15 em Outra Notação	70
17	Lista de Caracteres para Representação Alternativa IPv6	70
18	Serviço *Multicast*	74
19	Serviço *Unicast*	75
20	Serviço *Anycast*	77
21	Camada dupla (dual)	85
22	Túnel IPv6 em IPv4	86

Lista de Tabelas

Tabela nº	Identificação da tabela	Página
1	Tipos de Cabeçalhos de Extensão	61
2	Tratamento das opções que não forem compreendidas pelo roteador	63
3	Faixas de Endereços IPv6	72
4	Escopo para um endereço *Multicasting*	73

Abreviatura e Siglas

Símbolo	Descrição do Símbolo
ARP	*Address Resolution Protocol*
ATM	Rede de comunicação criada pela DARPA
CIDR	*Classless InterDomain Routing*
DARPA	*U.S. Defense Advanced Research Projects Agency*
DNS	*Domain Name System*
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
IAB	*Internet Architecture Board*
IANA	*Internet Assigned Number Authority*
ICMP	*Internet Control Mesage Protocol*
IEEE	*Institute of Eletrical and Eletronics Engineers*
IHL	*Internet Header Length*
IMP	*Interface Message Processors*
IP	*Internet Protocol*
IPng	*Internet Protocol Next Generation*
IPSec	*Internet Protocol Security*
IPv4	Protocolo da Internet versão 4
IPv6	Protocolo da Internet versão 6
ISP	*Internet Service Providers*
Nc	Número de campos de um datagrama
NGI	*Next Generation Internet*
OSI	*Open Systems Interconection*
QoS	*Quality of Service*
RFC	*Request For Comments*
RNP	Rede Nacional de Pesquisa
RSVP	*Resource Reservation Protocol*
SIPP	*Simple Internet Protocol Plus*

SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple network Management Protocol*
TCP	*Transmission Control Protocol*
TCP/IP	Conjunto de protocolos da arquitetura de rede da Internet
Telnet	Serviço de acesso remoto
UDP	*User Datagram Protocol*
UFSC	*Universidade Federal de Santa Catarina*
UTP	*Unshield Twist Pair*
URL	*Uniform Resource Location*
WWW	*World Wide Web*

RESUMO

Uma nova versão e implementação do Internet Protocolo (IP), denominado IPv6, foi recomendada pelo IETF *(Internet Engineering Task Force)*. Esta nova versão, irá substituir aos poucos a versão corrente, o IPv4. Mas antes desta troca ocorrer, alguns protocolos deverão passar por análises referente as possíveis modificações e/ou implementações derivadas desta migração.

A arquitetura da rede da Internet é divida em níveis, os quais os protocolos são distribuídos conforme suas características e funções. Alguns destes protocolos levam em seus datagramas informações referentes ao endereço IP das máquinas origem e destino, e uma modificação na estrutura de endereçamento poderá trazer a necessidade de ajustes destes protocolos.

Este trabalho propõe um estudo das técnicas existentes e necessárias para que possa ocorrer a migração do IPv4 para o IPv6.

O protocolo IPv6 foi desenvolvido para atender novas necessidades na Internet e apresenta soluções para problemas de endereçamento, tabelas de roteamento e questões de segurança. Este novo protocolo não é, ainda, muito utilizado, o que justifica a análise das formas de transição, uma vez que IPv4 e IPv6 coexistirão ainda por muitos anos.

ABSTRACT

The Internet Protocol (IP) new version and implement, called Ipv6, was recommended by the IETF (Internet Engineering Task Force). This new version will replace the present version, the Ipv4. But before occur this change, some protocols must pass for analyses about the changes and/or implements possible from this migration.

The Internet Architecture is divided into levels, the ones the protocols are distributed according to its characteristics and functions. Some of these protocols carry in its datagrams information about the IP address of the origin machines, and a change in the addressing structure can bring these protocols fit need.

This paperwork proposes a study of the present and necessary techniques to occur the migration from the Ipv4 to the Ipv6.

The Ipv6 protocols was developed to answer the Internet new needs and show solutions to the addressing problem, routing table and secure questions. This new protocol isn't used yet, what justifies the analyses of the change's form. The Ipv4 and the Ipv6 will exist for many years.

1. INTRODUÇÃO

A disseminação e o crescimento desenfreado da Internet tem originado uma mudança comportamental em todo o mundo. Muito embora este crescimento seja incentivado por empresas e instituições de ensino para a propagação velocíssima de informações, há uma pesada crítica sob os protocolos de comunicação utilizada para o tráfego dos dados. Insegurança e lentidão de comunicação tem sido alvo de crítica e preocupação devido a má gerência da qualidade de serviços e ao fraco desempenho na propagação de datagramas (COMER, 1994).

O protocolo IP, responsável pela entrega do datagrama no destino da comunicação, atualmente trabalha em sua versão 4.0 (IPv4) e tem sofrido atualizações em seu código com incorporação de recursos como protocolo de segurança e protocolo de gerência de banda passante, porém provavelmente estas modificações não suportarão o crescimento esperado em tráfego multimídia no futuro.

Órgãos regulamentadores da Internet sugerem a atualização total do protocolo de rede através da aplicação do IP versão 6.0 (IPv6), um protocolo moderno ao qual implementa conceitos e técnicas não previstas em seu antecessor, visando uma comunicação mais veloz e segura.

Além de segurança e desempenho, a implementação do IPv6 endereçará muito mais interfaces de rede, pois o campo de endereçamento possui 128 bits contra apenas 32 do IPv4.

Apesar do protocolo IPv6 ser assunto amplamente comentado e difundido no meio da rede WWW, grande parte de suas implementações ainda se encontram em fase de experimento, documentação e padronização.

Douglas Comer (COMER, 1994), presidente da *Internet Society Vinton Cerf* descreve em seu livrou:

"Os protocolos TCP/IP mostram um importante desafio arquitetônico com a contínua e fenomenal expansão da Internet. Com o crescimento anual de 100% no número de redes ligadas à Internet coloca em xeque o sistema de roteamento. As classes B estão paulatinamente sendo esgotadas e o uso das técnicas de CIDR (Classless InterDomain Routing) representam uma solução paliativa a este problema. Uma nova versão do IP faz-se necessária para suportar um endereçamento muito maior e prover suporte ao problema de escalabilidade.

Ao mesmo tempo, novas e bastante ambiciosas aplicações já sugerem que a Internet precisa suportar pacotes de voz e vídeo em proporções cada vez maiores.

Segurança é também um dos fatores mais importantes, especialmente com a expansão de redes aplicadas ao mundo dos negócios. Procurar uma maneira uniforme de suportar a Internet e ainda lidar com a variedade de tecnologias pelo mundo, algumas das quais sujeitas a restrições de exportação, é um desafio de enormes proporções".

1.1. Motivação

Notoriamente, os meios de comunicação apresentam como solução para o problema de esgotamento dos endereços de *hosts*, a implementação do protocolo IPv6 sem entanto apresentar aos leitores os traumas desta migração, de compatibilidade, roteamento e outros mais.

O próprio IPv4 possui mecanismos para melhorar problemas referentes aos endereços e também modificações na estrutura que não se restringe apenas em ganhar alguns bits para endereçamento (HINDEN, 1998_1).

Desta forma, novas questões são levantadas com o surgimento deste novo protocolo, pois também diversas empresas como a *SUN Microsystems* e a própria *Microsoft* possuem sessões voltadas para o IPv6 com informações de endereçamento e configuração (LEE, 2000).

1.2. Objetivo

Este trabalho propõe o estudo do Aspecto de Transição do protocolo IP em sua versão 4 (IPv4) para a versão 6 (IPv6), em consideração as conseqüências diretas e indiretas que esta transição possam vir a sofrer.

A consolidação do aprendizado adquirido durante o curso de mestrado em Ciência da Computação na Universidade Federal de Santa Catarina em parceria com a UNIPAR, Universidade Paranaense, também é objetivo desta proposta de pesquisa.

1.2.1. Objetivos Gerais

- Conhecer o protocolo IPv4;
- Conhecer o protocolo IPv6;
- Estudar e apresentar as atuais técnicas de transição destes protocolos.

1.2.2. Objetivos Específicos

Analisar a real situação do protocolo IPv6 junto à comunidade de pesquisa e junto às corporações;

Avaliar os detalhes da migração do protocolo IP sobre os produtos e serviços.

1.3. Organização do Texto

Na próxima seção serão apresentados uma breve introdução sobre a Internet e Internet 2, seus órgãos regulamentadores, arquitetura da rede Internet, protocolos e a comparação do modelo OSI com o utilizado atualmente pelo TCP/IP. Em uma seção seguinte, são apresentados os protocolos IP, nas versões 4 e 6 (IPv4 e IPv6), focando principalmente a diferença e o propósito da versão em discussão quanto ao endereçamento, segurança e desempenho. Finalmente é então apresentado um epílogo do trabalho.

2. INTERNET

Neste capítulo será apresentado um comentário sobre o histórico da Internet breve conhecimento a respeito da Internet e o surgimento da Internet 2, bem como suas características.

2.1. Introdução

O objetivo deste capítulo é apresentar um histórico a respeito da Internet, iniciando das primeiras idéias lançadas no *Massachusetts Institute of Technology* até o seu último grande marco significativo que foi a criação da *World Wide Web*. Posteriormente será apresentado um breve comentário a respeito da Internet 2, que é um projeto de redes de altíssima velocidade com objetivo de atender aplicações voltadas para aplicações de tempo real envolvendo multimídia. Para finalizar, será abordado um tópico referente aos órgãos regulamentadores da Internet, onde estes interagem entre si com objetivo de organizar e regulamentar, tornando desta forma a Internet um organismo com possibilidade de constante evolução.

2.2. Histórico

Não poderíamos iniciar este trabalho, cujo assunto principal é Internet, sem mencionarmos, mesmo que em breves linhas, um histórico da Computação, mesmo porque a Internet deriva deste avanço.

Poderíamos escrever um livro inteiro ou quem sabe até uma coleção deles para relatar as descobertas e acontecimentos da Computação, apresentando desde a manipulação de ossos, utilizada por John Napier, para executar operações de multiplicação, divisão e extração de raiz quadrada ou cúbica através da descoberta do algoritmo, até o destaque do primeiro computador do mundo, o ENIAC, construído em 1.946 nos Estados Unidos, com propósito de montar tabelas para calcula de trajetória de projéteis. Porém, ficaremos restritos a um breve comentário.

Os primeiros computadores eram constituídos de válvulas eletrônicas, grandes e caras que queimavam com grande facilidade. Os computadores tinham apenas uso científico e estavam instalados nos grandes centros de pesquisa. Isso caracterizou a primeira geração de computadores (1.945 a 1952). Estas válvulas eram ligadas por quilômetros de fios ligados manualmente, explicando assim as enormes dimensões fisicas dos computadores.

A segunda geração, marcada entre 1.954 a 1.964, teve como principal característica a revolução dos transistores que substituíram as volumosas válvulas e diminuindo a quantidade de cabos e fios necessários para composição dos computadores de geração anterior. Conseqüentemente, o tamanho dos computadores foi consideravelmente reduzido.

A linguagem de programação foi simplificada e denominada ASSEMBLER, e já se podia programar através de comandos abreviados (comandos mnemônicos).

A terceira geração dos computadores, entre 1.964 a 1.970, surgiu com a utilização dos circuitos integrados, que proporcionavam a possibilidade do computador executar vários processamentos simultâneos. A programação dos computadores desta geração foi facilitada pelo aparecimento de linguagens orientadas para o problema específico. As linguagens eram de naturezas universais e muito próximas a linguagem do homem.

Entre 1.970 e 1988 caracterizou-se a quarta geração com o aparecimento e utilização da Tecnologia Biploar MOS-LSI (*Large Scale Integrate)* – CHIPS. Esta geração foi marcada pelo aparecimento dos microcomputadores e conseqüentemente pelo seu uso em escritórios e lares. A linguagem foi ainda mais melhorada, tornando-se interpretada e voltada definitivamente para o usuário final.

A quinta e até o momento última geração (1.988 até os dias de hoje) é marcada pela tendência de imitar a natureza, tanto nos circuitos integrados BIOCHIPS (Circuitos Integrados com moléculas orgânicas) como na programação com desenvolvimento das técnicas de inteligência artificial, processamento simbólico, linguagens naturais e reconhecimento de voz.

A Internet teve seu início entre o final da década de 1960 e o início da década de 1970, na Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa (DARPA – *U. S. Defense Advanced Research Projects Agency*) do governo dos Estados Unidos, com um programa de pesquisa que objetivava investigar novas técnicas e

tecnologias para a viabilização da troca de pacotes de dados entre várias redes de computadores de diferentes arquiteturas (CERF, 1998). O objetivo principal era desenvolver protocolos de comunicação que permitissem a comunicação de forma transparente de computadores em uma rede com computadores de outra rede (TANENBAUM, 1996). Desse projeto originou-se a rede ARPANET.

Um documento expedido pelo órgão regulamentador da Internet, *Internet Society*, (LEINER, 1998), aponta o pesquisador da MIT ***J. C. R. Licklider***, com o seu conceito "*Galactic Network*" apresentado em 1962, como o precursor das idéias da Internet. Em 1995, o *Federal Networking Council* dos Estados Unidos reconheceu e aprovou uma resolução definindo o termo Internet. Esta definição realizada por membros da Internet e comunidades de direitos da propriedade intelectual, apresentando o seguinte: (FNC, 1995):

*"Internet se refere ao sistema de informação global que – (i) é logicamente ligado por um endereço único global baseado no Internet Protocol (IP) ou suas subseqüentes extensões; (ii) é capaz de suportar comunicações usando o Transmission Control Protocol /Internet Protocol (*TCP/IP*) ou suas subseqüentes extensões e/ou outros protocolos compatíveis ao IP; e (iii) provê, usa ou torna acessível, tanto publicamente como privadamente, serviços de mais alto nível produzidos na infra-estrutura descrita".*

O protocolo original da Internet foi o protocolo IMP-IMP, ao qual permitia a conexão entre minicomputadores conhecidos como IMP *(Interface Message Processors*). Este protocolo sem conexão transformava as mensagens em pequenos pacotes que eram enviados pela rede de forma independente (TANENBAUM, 1996). No ano de 1974 *Vinton*

Cerf e *Robert Kahn* propuseram um modelo de protocolos dividido em camadas para a arquitetura de redes de Internet, chamado de TCP/IP, que foi atualizado em 1978 tornando-se a versão aceita pela comunidade científica internacional. A partir de 1983 todas as máquinas da ARPANET foram obrigadas a utilizar o TCP/IP que fora, então, reconhecido como o padrão da comunicação na Internet.

A Internet disponibilizava basicamente três tipos de serviços baseados em troca de arquivos e mensagens entre usuários, como:

- Telnet - serviço de acesso remoto;
- FTP – serviço de troca de arquivos;
- *E-mail* – serviço de correio eletrônico.

Com o surgimento da WWW *(World Wide Web)* em 1991, fez-se então que o número de computadores ligados a Internet saltasse de 313.000 no final de 1990 para 2.056.000 em 1993 (BOZZANO, 1998), chegando a mais de 50.000.000 no ano de 1997 (IDGNOW, 1997).

A Internet surgiu no Brasil em 1992 durante um evento organizado pelas Nações Unidas, a ECO 92, como um requisito de infra-estrutura do evento. Em 1993 a Rede Nacional de Pesquisa (RNP) dá início a sua estrutura e cria a sua rede, com finalidade acadêmica, unindo onze estados no país. Paralelo a essa rede, denominada *backbone*, foi montado o primeiro repositório de dados para a Internet do país. Em 1995 a estatal Embratel – Empresa Brasileira de Telecomunicações -, passou a fornecer acesso a Internet a partir de seu *backbone* já instalado.

Abaixo, segue um demonstrativo referente alguns eventos significativos da evolução do protocolo TCP/IP e da Internet (PALMA, 2000):

1969 ARPANET autorizada pelo DOD

1970 ARPANET adota o *Network Control Protocol* (NCP)

1971 23 hosts na ARPANET

1972 Especificação do Telnet

1973 Especificação do *File Transfer Protocol* (FTP)

1974 Especificação do *Transmission Control Protocol* (TCP)

1975 Primeiro *mailing list* da ARPANET (MsGroup)

1978 TCP subdivido em TCP e IP

1981 Publicação do Standart *Internet Protocol* (IP)

1982 TCP e IP definidos como *suite* pela ARPA e DCA

1983 Substituição do NCT pelo TCP/IP (flag day)

1984 Surgimento do DNS1986: Criação da NFSNet

1986 Criação da IETF e da IRTF pela IAB

1987 10.000 *hosts* na NFSNet

1989 100.000 *hosts* na NFSNet

1990 ARPANET deixa de existir e Brasil se conecta à NFSNet

1992 Criação da ISOC

1993 Criação do InterNIC

1994 Início do uso comercial da Internet no Brasil

1996 Guerra dos browsers: Microsoft x Netscape

1999 60.000.000 de hosts na Internet

2.3. Internet 2

A Internet 2 surgiu de iniciativa norte-americana, que objetiva o desenvolvimento de tecnologias e aplicações avançadas de redes Internet para a comunidade acadêmica, pesquisa e comercial.

O objetivo deste projeto é oferecer o desenvolvimento de novas aplicações que não são atualmente viáveis com a tecnologia atual, tais como telemedicina, bibliotecas digitais, laboratórios virtuais, dentre outras.

Há muito ainda a ser pesquisado sobre a necessidade dos usuários e a possibilidade de tecnologias para redes de alto desempenho, principalmente por não existir uma linha de trabalho ao qual oriente pesquisas de novas possibilidades de aplicações da Internet 2.

A arquitetura física da rede eletrônica que dá suporte ao Internet 2 inclui a implantação de GigaPOPs – pontos de presença com velocidade de tráfego da ordem de Gigabits. A função principal do GigaPOP é o gerenciamento da troca do tráfego Internet 2 de acordo com especificações de velocidade e qualidade de serviços previamente estabelecidos através da rede.

A Internet 2 é parte de um projeto maior que está diretamente relacionado à Presidência da República do governo norte-americano, o NGI – *Next Generation Internet* – cujo objetivo é o desenvolvimento de tecnologias de rede de última geração, focando inicialmente a pesquisa, a formação de recursos humanos, o experimento de tecnologias necessárias para o desenvolvimento de novos tipos de serviços que garantam transações altamente seguras e de qualidade.

No Brasil existe um projeto viabilizado pela RNP – Rede Nacional de Pesquisa – conhecido por ReMAV - Redes Metropolitanas de Alta Velocidade, que objetiva promover, em diversas partes regiões do país, a criação de infra-estrutura e serviços de redes de alta velocidade.

O projeto ReMAV viabilizará a integração nacional das redes metropolitanas de alto desempenho, formando o primeiro estágio do backbone nacional de alta velocidade, o RNP2. A partir deste, almeja-se oferecer conexões de alta velocidade para a Internet2, nos Estados Unidos, permitindo desta forma que instituições de ensino e pesquisa do Brasil passem a integrar aquela iniciativa, formando parcerias com universidades americanas para o desenvolvimento de novas aplicações e serviços.

2.4. Órgãos Regulamentadores

Esta seção apresenta alguns órgãos responsáveis pela discussão, especificação, regulamentação da arquitetura utilizada pela Internet.

2.4.1. IETF - Internet Engineering Task Force

O IETF é o órgão responsável pela especificação de novos padrões na Internet sendo composto por projetistas de redes, operadores, vendedores e pesquisadores preocupados com a evolução da arquitetura da Internet. É um órgão, aberto a toda comunidade, que publica e gerencia as *RFC (Request For Comments)* que, por sua vez, são documentos que regulamentam as tecnologias da Internet. Os principais objetivos da IETF são (MALKING, 1994):

- Identificar e propor soluções a problemas técnicos e operacionais da Internet;
- Especificar o desenvolvimento ou uso de protocolos e novas arquiteturas que venham a solucionar algum problema na Internet;
- Fazer recomendações ao IESG *(Internet Engineering Steering Group)* considerando a padronização dos protocolos em uso na Internet;
- Facilitar a transferência tecnológica do IRTF *(Internet Research Task Force)* para toda a comunidade Internet;
- Providenciar um fórum para a troca de informações entre a comunidade Internet, vendedores, usuários, pesquisadores, agências contratantes e gerentes de rede.

2.4.2. ISOC – Internet Society

A ISOC é uma organização comprometida com o crescimento e evolução da Internet e com as questões sociais, políticas e técnicas que surgem a partir do seu uso. Ela é composta por membros individuais e organizacionais, sendo seu corpo diretor eleito com a participação de todos os associados (HOVEY, 1996). O principal propósito da ISOC, segundo (HOVEY, 1996) é:

"Manter e estender o desenvolvimento e disponibilidade da Internet e suas tecnologias e aplicações associadas – ambas como um fim por si mesma e como um meio de habilitar organizações, profissionais e indivíduos do mundo todo para colaborar, cooperar e inovar em seus respectivos campos e interesses".

Entre seus objetivos gerais e propostas incluem:

- Desenvolvimento, manutenção, evolução e disseminação de padrões para a Internet e suas tecnologias e aplicações;
- Crescimento e evolução da arquitetura da Internet;
- Manutenção e evolução dos processos administrativos necessários para a Internet global e Intranets;
- Educação e pesquisas relacionadas com a Internet e *internetworking*;
- Harmonização das ações e atividades em nível internacional para facilitar o desenvolvimento e disponibilidade da Internet;

- Coletar e disseminar todas as informações relacionadas com Internet e *internetworking* incluindo históricos e arquivos.

2.4.3. IAB – Internet Architecture Board

O IAB tem como principal função a discussão e o estudo da arquitetura da Internet e seus protocolos, auxiliando a IETF a aprovar os projetos enviados a ela. É um órgão de controle do IETF. É composto por um grupo de notáveis não necessariamente técnicos em computação. Alguns assuntos em discussão na IAB (HOVEY, 1996):

- Futuro do endereçamento Internet;
- Princípios arquiteturais da Internet;
- Objetivos futuros e direcionamentos para o IETF;
- Gerenciamento dos domínios de alto nível no DNS *(Domain Name Syste*m);
- Registro de arquivos do tipo MIME;
- Conjunto internacional de caracteres.

2.4.4. IRTF – Internet Research Task Force

A IRTF investiga assuntos avançados e considerados ainda incertos de serem acrescentados junto à Internet. Suas atividades são organizadas em grupos de estudos e quando estes tem alguma aplicabilidade eles são repassados para o IETF que irá adequá-los e disponibilizá-los para a comunidade Internet mundial (HOVEY, 1996).

Alguns grupos atualmente formados:

- Descoberta de novos recursos na Internet;
- Gerenciamento de Redes;
- *Multicast* confiável;
- Segurança em *multicast*;
- Gerenciamento de serviços;
- Segurança e privacidade.

2.4.5. IANA – Internet Assigned Number Authority

A IANA é a autoridade habilitada a atribuir registro dos vários parâmetros de protocolos na Internet, como números de portas, números de protocolos, códigos e

numeração de MIBs *(Management Information Base)*. Funciona como o domínio de mais alta instância para o DNS. Todos números assinalados pela IANA são referenciados em RFCs com o título *"Assigned Numbers"*.

2.4.6. Comitê Gestor Internet no Brasil

Em Maio de 1995, o Ministério de Comunicações (MC) e o Ministério da Ciência e Tecnologia (MCT) firmaram um convênio para tornar efetiva a participação da sociedade brasileira nas decisões envolvendo a implantação, administração e uso da Internet. Dessa forma foi constituído o Comitê Gestor Internet, que conta com a participação do MC e MCT, de entidades operadoras e gestoras de *backbones*, de representantes de provedores de acesso ou de informações, de representantes de usuários, e da comunidade acadêmica. O Comitê Gestor tem como atribuições principais (COMITÊ, 1999):

- Fomentar o desenvolvimento de serviços Internet no Brasil;
- Recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil;
- Coordenar a atribuição de endereços Internet, o registro de nomes de domínios, e a interconexão de *backbones*;
- Coletar, organizar e disseminar informações sobre os serviços Internet.

3. A ARQUITETURA DE REDE DA INTERNET

Neste capítulo será apresentado um comentário sobre os principais protocolos de comunicação da Internet.

3.1. Introdução

O objetivo deste capítulo é apresentar informações a respeito da arquitetura de rede da Internet, através da identificação das camadas de atuação do protocolo IP (*Internet Protocol)*. Este protocolo é o centro do estudo realizado, sendo abordado inicialmente as características de sua versão atualmente em uso, a versão 4.0, e posteriormente um estudo especial sobre o protocolo IP em sua mais nova versão (o IPv6), focando sua transição que é um dos principais objetos de concentração desta pesquisa.

3.2. Os Protocolos da Internet

A Internet possui uma arquitetura composta por um conjunto de protocolos desenvolvidos que permitem que computadores comuniquem entre si em uma rede. Padrões que especificam detalhes desta comunicação estão embutidos neste conjunto de protocolos assim como convenções e normas para rotear o tráfego gerado por essa comunicação. A

nomenclatura TCP/IP é também utilizada para descrever esta arquitetura devido a seus dois protocolos mais importantes o TCP *(Transmission Control Protocol)* e o IP *(Internet Protocol)*, muito embora existam outros protocolos que constituem essa família, como o IP *(Internet Protocol)*, ARP *(Address resolution protocol)*, ICMP *(Internet control Message Protocol)*, UDP *(User Datagram Protocol)*, TCP *(Transport Control Protocol)*, RIP (R*outing Information Protocol)*, Telnet, SMTP (*Simple Mail Transfer Protocol)*, DNS *(Domain Name System)* e outros mais.

Quatro camadas que interagem entre si compõem esta arquitetura, tornando-se flexível e adaptável à mudanças. As quatro camadas são: camada de aplicação, camada de transporte, camada de rede ou internet e a camada de interface, conforme podemos ver na Fig. 1 que apresenta cada camada da arquitetura com seus respectivos protocolos. Apesar de ser comparado ao modelo de referência OSI, a arquitetura de rede da Internet segue normas próprias definidas pelos órgãos normativos.

Aplicação	Telnet, FTP, SMTP
Transporte	TCP, UDP
Rede	IP, ICMP, ARP
Interface	Ethernet, ATM, X.25

FIGURA 1: Camadas da Arquitetura de Rede Internet

3.2.1 Protocolos TCP/IP

Atualmente, o protocolo TCP/IP é o mais utilizado em redes locais devido à popularização da Internet, motivo ao qual o mesmo foi criado. Mesmo em sistemas

operacionais que utilizam o seu protocolo próprio (como Windows NT com seu NetBEUI e o NetWare com seu IPX/SPX), hoje suportam o protocolo TCP/IP.

A grande vantagem do TCP/IP em relação a outros protocolos existentes é o fato dele ser roteável, isto é, foi concebido para redes de muitos hots e de longa distancia, podendo haver vários caminhos para se atingir o computador receptor.

O fato de possuir uma arquitetura aberta permitindo que qualquer fabricante possa adotar sua própria versão TCP/IP em seu sistema operacional, sem haver necessidade de pagamento de direitos autorais a ninguém. Desta forma, fabricantes de sistemas operacionais adotaram o TCP/IP, transformando-o em um protocolo universal fazendo com que sistemas diferentes possam comunicar-se entre si.

3.2.1.1 Comparação entre as arquiteturas TCP/IP e OSI

A principal diferença entre os dois, é que o modelo OSI evoluiu de uma definição formal elaborada por comissões da ISO para o desenvolvimento de produtos, enquanto que o TCP/IP nasceu da necessidade do mercado e da demanda de produtos para resolver o problema de comunicação e a partir daí passou por uma série de implementações onde muitos produtos foram desenvolvidos fora da arquitetura internet, passando a ser incorporados a ela.

Vale então dizer que a arquitetura OSI é considerado um modelo de jure, enquanto que arquitetura internet é considerada um modelo "de facto".

Analisando-se comparativamente a estrutura dos dois modelos (Fig. 2), pode-se observar que a parte referente às sub-redes de acesso da arquitetura internet corresponde à camada física, à de enlace e, parcialmente, à de rede do modelo OSI, sem que haja nenhuma padronização neste sentido.

O IP corresponde à camada de rede, enquanto o TCP e o UDP oferecem serviços semelhantes aos prestados, respectivamente, pelos protocolos de transporte orientados e não-orientados à conexão do modelo OSI. Nas camadas superiores, a arquitetura Internet coloca sob responsabilidade da aplicação os serviços fornecidos pelas camadas de sessão, apresentação e aplicação do modelo OSI.

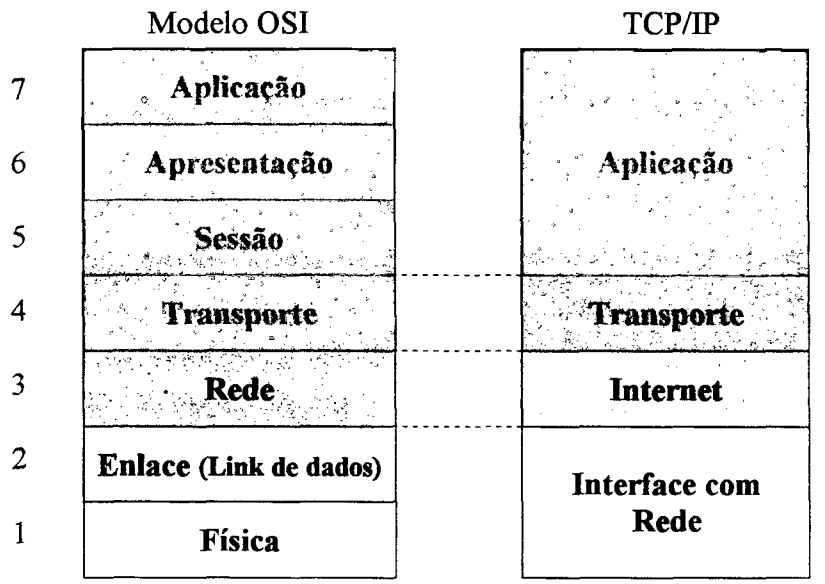

FIGURA 2: Comparação entre as arquiteturas OSI e TCP/IP

O fato da arquitetura TCP/IP possuir menos camadas que o modelo OSI implica na sobrecarga de algumas camadas com funções que não lhe são específicas. Por exemplo, podemos citar a transferência de arquivos: no ambiente TCP/IP, as funções correspondentes

à camada de apresentação OSI são desempenhadas pelo próprio protocolo de transferência de arquivos FTP. Por outro lado, o TCP/IP nos fornece aplicações simples, eficiente e de fácil implementação a nível de produtos. Uma das maiores limitações da arquitetura TCP/IP é quanto a sua capacidade de endereçamento, que já está se tornando limitada, devido ao crescimento da Internet.

Já a arquitetura OSI sofre críticas por apresentar "modelos e soluções acadêmicas" e objetivar atendimento a requisitos de propósito geral em detrimento de soluções imediatas, compatíveis com as exigências atuais dos usuários. É também criticada por não apresentar meios de migração entre as arquiteturas atualmente em funcionamento e suas soluções.

Diante desta situação, observa-se atualmente um emergente esforço de aproximação entre as duas arquiteturas, objetivando-se aproveitar o que cada uma tem de melhor a oferecer, de forma a se encontrar soluções mistas. Abaixo, segue um breve comentário sobre as camadas conforme os padrões TCP/IP:

- Camada de Aplicação: Corresponde às camadas de 5 a 7 no modelo OSI e faz a comunicação entre os aplicativos e o protoclo de transporte. Muitos protocolos operam nesta camada, tais como o HTTP (*HiperText Transfer Protocol*), SMTP (*Simple Mail Transfer Preotocol*), o FTP (*File Transfer Protocol*), O SNMP (*Simple Network Mangement Protocol*), o DNS (*Domain Name System*) e o Telnet.

  A comunicação entre a camada de aplicação e a camada de transporte é efetuada através de uma porta. Estas portas são numeradas e as aplicações padrões sempre utilizam uma mesma porta. O protocolo SMTP utiliza sempre a porta 25, o

protocolo HTTP utiliza sempre a porta 80 e o FTP portas 20 e 21 (transmissão de dados e transmissão de controle respectivamente).

- Camada de Transporte: Esta camada é responsável por pegar os dados enviados pela camada de aplicação e transformá-los em pacotes, a serem repassados para a camada de Internet. O modelo TCP/IP permite a utilização de multiplexação, ou seja, transmissão "simultânea" de dados de diversas aplicações, utilizando o conceito de intercalação de pacotes; vários programas poderão estar comunicando-se com a rede ao mesmo tempo, sendo que os pacotes gerados serão enviados à rede de forma intercalada, não sendo preciso o término de uma aplicação para então começar outra. Essa possibilidade é devido à utilização de portas, já que dentro do pacote há informação da porta de origem e de destino do dado. Como exemplo, podemos citar o recebimento de três pacotes, sendo o primeiro de e-mail, o segundo de www e o terceiro de FTP.

  Nesta camada operam o TCP e o UDP(*User Datagram Protocol)*. Ao contrário do TCP, este segundo protocolo não verifica se o dado chegou ou não ao destino. Diante disso, o protocolo mais utilizado na transmissão de dados é o 5TCP, enquanto o UDP é tipicamente usado na transmissão de informações de controle. Quando recebido os dados, a camada de transporte pega os pacotes passados pela camada Internet e os coloca em ordem, verificando se todos chegaram corretamente.

- Camada de Internet: Equivalente à camada 3 (rede) do modelo OSI. Há vários protocolos que operam nesta camada, tais como IP (*Internet Protocol*), ICM

(*Internet Control Message Protocol*), ARP (*Address Resolution Protocol*) e RARP (*Reverse Address Resolution Protocol*). Na transmissão de um dado de programa, o pacote de dados recebido da camada TCP é dividido em pacotes chamados *datagramas*. Os datagramas são enviados para a camada de interface com a rede, onde são transmitidos pelo cabeamento da rede através de pacotes. Esta camada não verifica se os datagramas chegaram ao destino pois este serviço é feito pelo TCP.

Esta camada é respondável pelo roteamento de pacotes, ou seja, adiciona ao datagrama informações sobre o caminho que ele deverá percorrer.

- Camada de Interface com a Rede: Esta camada, que equivale às camadas 1 e 2 do modelo OSI, é responsável por enviar o datagrama recebido pela camada de internet em forma de um bloco através da rede. A Fig. 3 apresenta o esquema completo de um computador operando com o protocolo TCP/IP:

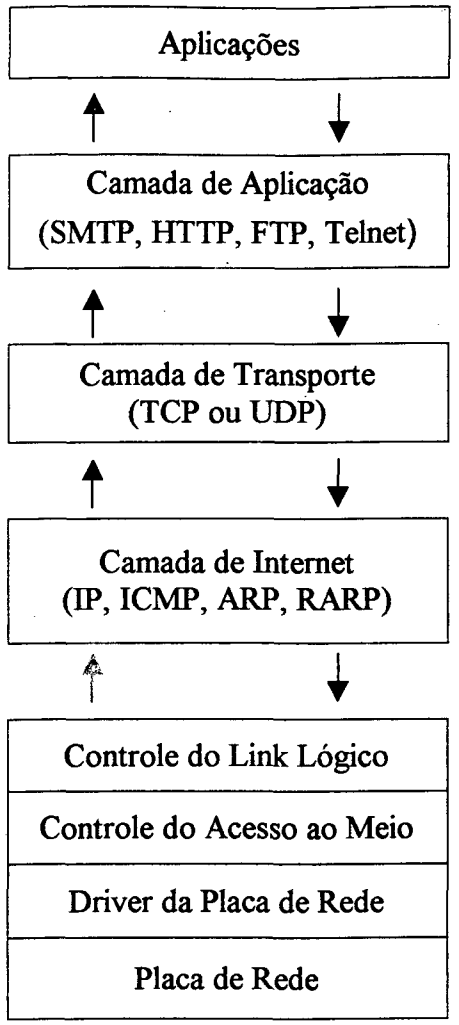

FIGURA 3: Funcionamento do TCP/IP

4. O PROTOCOLO IP VERSÃO 4 (IPv4)

Neste capítulo será apresentado um esboço sobre o protocolo IP bem com suas características e formas de endereçamento.

4.1. Introdução

O protocolo IP atua na camada de rede da arquitetura de rede da Internet e sua unidade de informação chama-se datagrama. Este protocolo não é orientado à conexão, desta forma não há garantia da entrega do datagrama ao destino, podendo os blocos de dados chegarem em ordem diversas, passando por caminhos diferentes um dos outros. Caso um datagrama se perca ou sofra alterações por interferência durante percurso percorrido, não há um mecanismo de retransmissão para os mesmos. O descarte do datagrama também pode ocorrer caso o mesmo não encontre o seu destino ou fique muito tempo à sua procura (BOZZANO, 1998).

O funcionamento da comunicação do protocolo IP é efetuada da seguinte forma: a camada de transporte trata as unidades de dados vinda da camada de aplicação e os entrega à camada de rede na forma de datagrama. Estes são transmitidos através da rede interna em forma de bits, de acordo com a interface utilizada na camada de interfaces. Se o destino não for a rede interna, os bits são direcionados para o equipamento roteador que irá recompor o datagrama e buscar as informações de cabeçalho do mesmo para enviá-lo ao seu destino por

um caminho definido pelas tabelas de caminhos do roteador. No momento em que o datagrama é lido pelo equipamento roteador ele pode ser fragmentado em mais datagramas devido a requisições do próprio equipamento ou do meio de comunicação.

O Protocolo IPv4 é a versão atualmente em uso na Internet. Ele foi especificado em 1978 e sofreu algumas atualizações até chegar à versão 4. A Fig. 4 apresenta a estrutura do datagrama do protocolo IPv4.

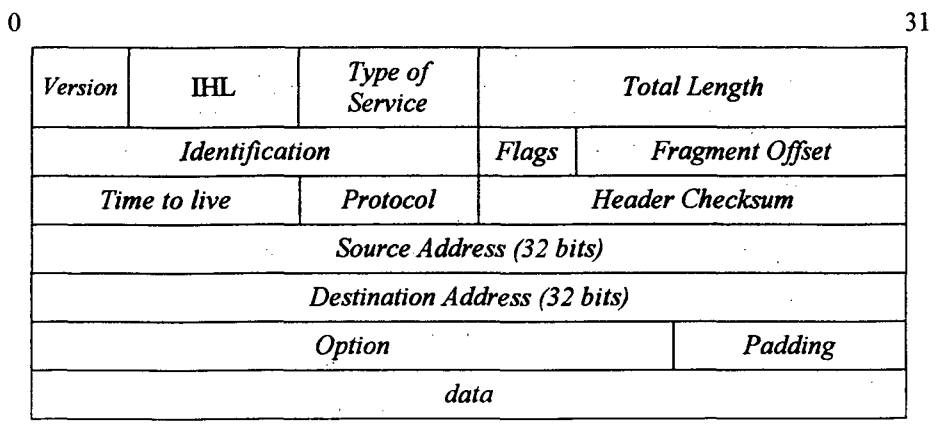

FIGURA 4: A Estrutura do Datagrama Protocolo IPv4

No datagrama IP encontramos os seguintes campos:

- *Version* (Versão): identifica a versão do protocolo que montou o bloco, neste caso o valor 4.
- *IHL - Internet Header Length* (Tamanho do cabeçalho): Indica o comprimento do cabeçalho do datagrama, dado em número de palavras de 32 bits, isto é, o número de linhas existentes, que em outras palavras é o número de bits existentes no cabeçalho dividido por 32. Seu tamanho mínimo é de 5 palavras

de 32 bits (20 bytes), sendo esse o valor mais comum, já que normalmente os campos *Options e Padding* não são utilizados.

- *Type of Service* (T*ipo* de Serviço): Este campo indica às sub-redes o tipo de serviço que deve ser oferecido ao datagrama (por exemplo, para transmissão de voz digitalizada necessita-se mais de uma entrega rápida do que um controle rigoroso de erros, ao passo que para um serviço de transferência de arquivos, o tempo de entrega pode ser sacrificado para se obter um maior controle de erro), ou seja, informa a qualidade desejada para a entrega do datagrama. Desta forma, três bits de precedência informa a prioridade do datagrama, dependendo do tipo de dado que ele carrega conforme descrito acima. A Fig. 5 ilustra o formato do campo serviço.

Precedência (3 bits)	D (1 bit)	T (1 bit)	R (1 bit)	Nao usado (2 bits)

Figura 5: Formato original do campo *Type of Service*

Os bits D, T e R significam, respectivamente, *Delay* (atraso), *Througthput* (velocidade) e *Realiability* (Confiabilidade). O transmissor poderia ativar cada um desses bits (colocando-s em 1) quando necessitasse de baixo atraso, alta velocidade e/ou alta confiabilidade, dependendo é claro da situação. Muito embora não há como garantir essas características em uma grande rede, podemos desta forma facilitar o trabalho do roteador. Por exemplo: se houvesse mais de uma rota para atingir o destino, a escolha poderia ser feita

baseada na configuração dos bits D, T e R do campo Tipo de Serviço. Assim,k um roteador poderia enviar o datagrama para um caminho lento, porém de alta confiabilidade caso o bit R estivesse habilitado, liberando uma outra rota para o mesmo destino para os datagramas que necessitassem de alto desempenho.

- *Total Length (*Tamanho Tota)l: Indica o número total de bytes que compõem o datagrama. Como esse campo poussui 16 bits, o datagrama só pode ter, no máximo, 65535 bytes (2^{16}). Obviamente, quanto maior o tamanho do datagrama, mais uma estação ocupa a rede, deixando-a mais lenta. Por esta razão, os datagramas usam tamanhos bem menores que 65535 bytes, como por exemplo 576 bytes.

- *Identification* (Identificação): Utilizado para identificar o datagrama, ou seja, possibilita ao *host* determinar a que datagrama pertence um fragmento recém-chegado (todos os fragmentos de um datagrama possuem o mesmo valor).

- *Flags*: É responsável para controlar a fragmentaçao de datagramas e é composto de um bit não utilizado seguido por dois bits, DF e MF. O DF (*Don't Fragment*) indica que os *gateways* não devem fragmentar este datagrama (por incapacidade do destino juntar novamente os fragmentos). MF (*More Fragments*), é utilizado como dupla verificação do campo Tamanho Total, sendo que todos os fragmentos (exceto o último) possuem este bit setado.

- *Fragment Offset (*Deslocamento do Fragmento): Campo responsável por informar a que posição no datagrama atual pertence o fragmento.

- *Time to Live* (Tempo de Vida): Indica o tempo máximo de vida do datagrama. Cada vez que o datagrama passa por um *gateway* (roteador por exemplo) esse número é decrementado. Quando chega a zero, o datagrama é descartado, não atingindo o destino. No receptor, o protocolo TCP irá perceber que está faltando um datagrama e pedirá uma retransmissão do datagrama que está faltando. O objetivo é eliminar os datagramas que demorem tempo demais para chegar ao destino, o que pode ocorrer caso a rota escolhida seja muito longa ou mesmo errada, caso exista um roteador mal-configurado no meio do caminho. Assim, elimina-se datagramas que poderiam ficar vagando eternamente pela Internet à procura de seu destino caso eles encontrem problemas de rota, o que congestionaria toda a rede.

- *Protocol* (Protocolo): Esse campo indica o protocolo que pediu o envio do datagrama, através de um código numérico. Por exemplo, o número seis indica o TCP, o número 17 indica o UDP, o número um indica o ICMP e assim por diante. Dessa maneira, no dispositivo receptor, a camada IP sabe para qual protocolo superior ela deverá entregar os dados presentes dentro do datagrama.

- *Header Checksum (Checksum* de Cabeçalho): é utilizado pelos *gateways* para se fazer uma verificação do cabeçalho (apenas do cabeçalho, não dos dados),

para que o *gateway* não roteie um datagrama que chegou com o endereço errado. Além disso, o fato de se usar somente o cabeçalho, é que a conta fica menor e mais rápida de ser feita (já que o cabeçalho tem tipicamente 20 bytes).

- *Source Address* (Endereço de Origem): Como o próprio nome diz, neste campo há o endereço de IP de onde está partindo o datagrama.
- *Destination Address* (Endereço de Destino): Como o anterior, neste campo há o endereço IP de destino do datagrama.
- *Option* (Opções): Usado para o transporte de informações de segurança, roteamento na origem, relatório de erros, depuração, fixação da hora e outras. Caso este campo não seja utilizado, ele é preenchido com zeros até ter 32 bits de comprimento. Estes zeros adicionados serão conhecidos como *Padding.*
- *Padding:* Este campo possui tamanho variável e é utilizado para se garantir que o comprimento do cabeçalho do datagrama seja sempre um múltiplo inteiro de 32 bits. Se os campos *Options* e *Padding* não forem utilizados, o cabeçalho possuirá 20 bytes, caso contrário o cabeçalho passa a ter 24 bytes.
- *Data* (Dados): São os dados que o datagrama está carregando. Apesar de o tamanho máximo do datagrama ser 65.535 bytes (o que deixa 65.515 ou 65.511 bytes disponíveis para os dados, dependendo do tamanho do cabeçalho), esse tamanho é muito grande, pois dificulta a transmissão e

congestiona a rede. Por isso, na maioria das vezes o tamanho utilizado é de 566 bytes.

4.2 Endereçamento IPv4

O roteamento dos datagramas através das sub-redes é executado baseado no seu endereço IP, números de 32 bits normalmente escritos como quatro octetos (em decimal), por exemplo 200.250.45.8. Devido ao fato de existirem redes dos mais variados tamanhos compondo a inter-rede, utiliza-se o conceito de classes de endereçamento:

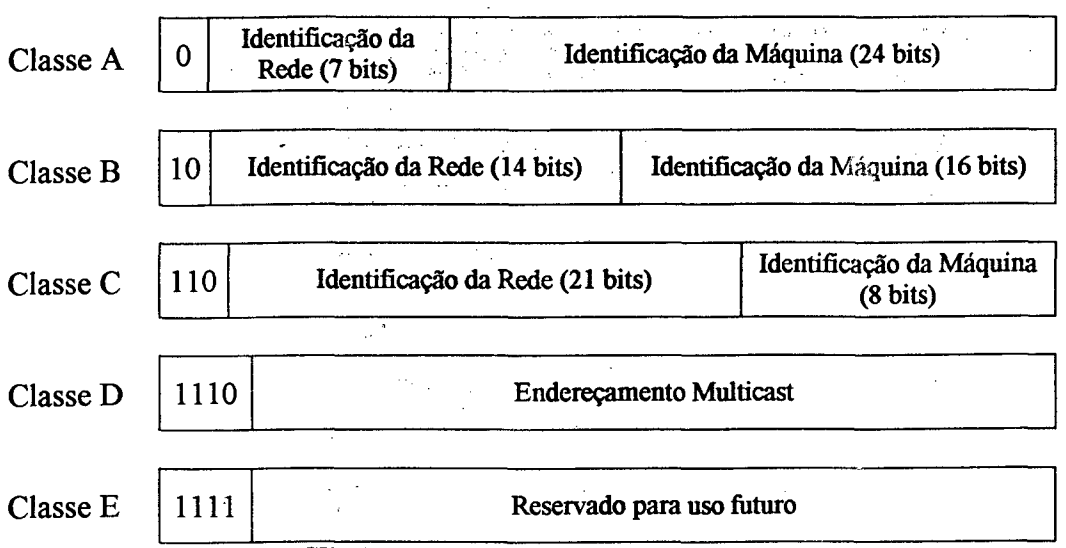

FIGURA 6: Formato dos Endereços IP

Podemos identificar um IP com relação a sua classe, da seguinte forma:

Classe A:

- Identificada pelo primeiro bit igual a 0. Valor do primeiro octeto contido na faixa entre 0 e 127;
- Possui um campo *Net ID* (identificação da rede) de 7 bits;
- Podem existir no máximo 128 redes classe A;
- Cada rede pode endereçar até 224 (16 M) *hosts*;
- Destinada a redes com grande número de estações.

Classe B:

- Identificada pelos dois primeiros bits do endereço colocados em 1 e 0 respectivamente. Valor do primeiro octeto contido na faixa entre 128 e 191;
- Possui um campo Net ID de 14 bits;
- Podem existir no máximo 16384 redes classe B;
- Cada rede pode endereçar até 216 (64 K) *hosts*;
- Destinada a redes consideradas de médio porte;
- Exemplo: UFSC - endereço de rede=150.162.

Classe C:

- Identificada pelos três primeiros bits do endereço colocados em 1, 1 e 0 respectivamente. Possui um campo *Net ID* de 21 bits. Valor do primeiro octeto contido na faixa entre 192 e 223;
- Podem existir no máximo 2.097.152 redes classe C;
- Cada rede pode endereçar até 28-2 (254) *hosts*;
- Os endereços de *Host* ID = 00000000 e 11111111 são destinados a *broadcasting*;

- Destinada a redes consideradas de pequeno porte.

  Exemplo: teracom - endereço de rede=200.250.45

O gerenciamento destes endereços de IP é de responsabilidade da IANA - *Internet Assigned Numbers Authority* (http://www.iana.org), cujo órgão é encarregado de entregar endereços IP aos países do mundo. Em cada país há um representante designado pelo órgão. No Brasil, é a FAPESP - Federação de Auxílio a Pesquisa do Estado de São Paulo.

Desde sua origem, o protocolo IP foi desenvolvido e implementado como um protocolo de comunicação com controle de tráfego utilizando a regra do melhor esforço (*Best-effort Service* ou *Lack of* QoS), que não provê nenhum mecanismo de qualidade de serviços e, conseqüentemente nenhuma garantia de alocação de recursos da rede. Na época ninguém imaginava que a Internet se tornaria a grande rede mundial que é atualmente, surgindo assim alguns problemas com o tempo. Um dos problemas foi a diminuição da quantidade de endereços IP disponíveis para as interfaces conectadas. A atual implementação está com sua capacidade de oferta de endereços muito diminuída, com previsão de esgotamento total em pouco tempo.

Para tentar minimizar esse problema, alguns mecanismos foram criados como por exemplo o CIDR *(Classless InterDomain Routing*), que propõe o fim das classes de endereçamento IP e a distribuição de endereços a partir de regiões geográficas, ou domínios.

Outro grande problema relacionado também com o endereçamento, é o aumento do tamanho das tabelas geradas pelo serviço de DNS (*Domain Name System)* devido ao aumento de sites e servidores conectados na Internet.

Outros problemas dizem respeito ao desempenho em redes de alta velocidade e baixa velocidade, bem como a capacidade de gerenciar requisitos de medição e manutenção da qualidade do serviço *(Qo*S) prestado pela rede. Além do mais o IPv4 não fornece um mecanismo próprio para tratamento da segurança dos dados, sendo necessário obter uma ferramenta extra de terceiros, nem sempre compatível com os demais protocolos que existem na rede.

O protocolo IP em sua versão 4.0 faz seu endereçamento com 32 bits conforme Postel descreve na (RFC 791), onde se percebe que é um recurso com limite relativamente baixo. Mesmo assim, a alocação dos IPs em boa parte das vezes é mal feita. Um bom exemplo é a UFSC ter uma classe B 150.162.0.0/16. Existem no mundo 16382 (14 bits do endereço IP já que os dois primeiros bits são necessariamente 10) redes Classe B possíveis. Uma classe B é capaz de endereçar com até 65535 *hosts* (16 bits menos significativos do endereço IP). Certamente a Universidade tem hoje bem menos de 20 mil computadores.

Muitos sites, particularmente os provedores de acesso a Internet, utilizam-se de um recurso chamado NAT (*Network Address Resolution*) para contornar o problema de falta de endereços IPs. O NAT permite que IPs reservados a redes privadas (RFC 1918) sejam usados e quando alcançarem a Internet o roteador deve converter este IP para um endereço válido. Assim, os IPs privados não deveriam ser roteados pelas redes públicas (Internet).

Infelizmente isso muitas vezes não ocorre, sendo difícil descobrir se é má configuração ou má fé.

O problema do tamanho excessivo das tabelas de roteamento foi parcialmente contornado com a adoção do CIDR (*Classless InterDomain Routing*) descrito pela (RFC 1519). A idéia básica por trás do CIDR é alocar as redes classe C restantes (cerca de 2 milhões) em blocos de tamanho variável. Se um site precisa de por exemplo 2000 endereços, receberia 8 classes C contínuas que representam 2048 endereços. Conforme sugerido pela (RFC 1519), novas regras para alocação para redes classe C baseada em localização geográfica. O mundo foi dividido em 4 grandes zonas: Europa, América do Norte, América do Central e do Sul, Ásia e Pacífico3. Dessa maneira, cada uma destas zonas teria 32 milhões de endereços para serem alocados e outras 320 milhões de endereços classe C de 204.0.0.0 a 223.255.255.255. Com a solução CIDR, as antigas classes A, B e C não são mais usadas para roteamento. Por este motivo CIDR é *classless routing* ou roteamento sem classes.

A compreensão de como se comportou o crescimento passado pode contribuir em muito na projeção de um protocolo que tenha uma vida útil maior.

Devido a estes e outros problemas o *IETF* iniciou estudos para criar um novo protocolo que substituísse o IPv4. A esse projeto foi dado o nome de IPng (*Internet Protocol Next Generation)* que posteriormente foi regulamentado com o nome de IPv6.

4.2.1. Endereços Especiais

Alguns endereços IP são reservados, não podendo ser usados para identificar as placas de interface com a rede nas máquinas. São reservados os endreços na rede 127.0.0.0, os endereços com números 0 e os endereços com números 255.

Os endereços na rede 127.0.0.0 identificam a própria máquina. Normalmente é usado o endereço 127.0.0.1 para identificar a própria máquina, quando uma aplicação envia mensagens para esse endereço. As mensagens são entregues na própria maquina em que se encontra a aplicação.

Um endereço com 0 nos bytes usados para identificar a placa, identifica uma ree. Por exemplo, o endereço 184.51.0.0 identifica a rede 184.51.0.0. Um endereço com 0 nos bytes para identificar a rede, identifica uma placa na rede. Por exemplo, o endereço 0.0.14.1 na rede 184.51.0.0 identifica a placa 184.51.14.1

Os endereços 255 são usados quando é necessário enviar uma mensagem para mais de um destino simultaneamente. Isto se chama broadcast. Por exemplo, uma mensagem enviada para o endereço 184.51.255.255 é entregue em todas as placas na rede 184.51.0.0.

4.2.1.1 Broadcast e Multicast

Os endereços para *broadcast* e *multicast* são usados quando há a necessidade de envio de um mesmo datagrama para mais de uma máquina. Quando um datagrama é enviado para o endereço de *broadcast*, é entregue a todas as máquinas da rede. O tratamento dado pelos roteadores aos datagramas pode ser bloquear ou propagar.

Por não saberem para que segmentos da rede devem propagar os datagramas para o endereço de *broadcast*, os roteadores são normalmente configurados para bloqueá-los. Isso evita uma degradação na performance da rede decorrente de transmissão desnecessária dos datagramas nos segmentos. O bloqueio por parte dos roteadores faz com que os datagramas sejam propagados apenas nos segmentos em que foram originados.

No *multicast*, o datagrama é enviado apenas para um grupo de máquinas de rede. Podem existir vários grupos de máquinas, cada um identificado por um endereço da classe D que pode variar entre 224.0.0.0 e 239.255.255.255. Por exemplo, os endereços para multicast 224.0.0.5 e 224.0.0.6 são usados pelo protocolo de roteamento OSPF (*Open Shortest Path First*) para troca de informações entre os roteadores.

Na utilização de um endereço *multicast* de uma mensagem, apenas as máquinas configuradas como membros do grupo recebem uma cópia da mensagem. As máquinas podem se tornar membros de um grupo, ou abandona-lo a qualquer momento, podendo também ser membros de mais de um grupo. Para terem acesso às mensagens enviadas para

endereços *multicast*, as máquinas devem suportar o IGMP (*Internet Group Management Protocol*), que faz parte da maior parte das implementações dos protocolos TCP/IP.

Os datagramas para os endereços de *multicast* são propagados nos segmentos onde existam máquinas que façam parte dos grupos para os quais os datagramas se destinam. Uma técnica para propagação adotada por alguns roteadores denomina-se *flooding*. Nessa técnica, o roteador verifica se é a primeira vez que o datagrama está sendo recebido. Em caso afirmativo, propaga o datagrama em todos os segumentos, exceto naquele pelo qual o datagrama foi recebido. Os roteadores podem também criar estruturas de dados que descrevam os caminhos mais eficientes para a entrega dos datagramas às máquinas nos grupos.

5. O PROTOCOLO INTERNET IP VERSÃO 6 (IPv6)

Este capítulo apresentará as características do protocolo de Internet em sua versa 6 (IPv6), abordando um breve histórico, características, formas de endereçamento e principais objetivos.

5.1. Introdução

O IPv6, é a nova versão do protocolo IP que foi projetado como uma evolução do IPv4, para ser executado em redes de alto desempenho como a ATM *(Assinchronous transfer Mode*) e ao mesmo tempo se manter eficiente em redes de baixo desempenho como as redes sem fio.

Os primeiros passos concretos do novo IP começaram em 1990, quando a IETF começou a trabalhar na nova versão do IP, uma versão que nunca tivesse problema de exaustão de endereços, resolveria uma variedade de problemas relacionados às novas tecnologias, mais flexível e eficiente. Para isso foi formado o grupo de trabalho IPng. Os principais objetivos a serem alcançados com o protocolo IPv6 são (BRADNER, 1995):

- Suportar bilhões de *hosts*, mesmo que os endereços fossem alocados de forma ineficiente;
- Reduzir o tamanho da tabela de rotas;

- Simplificar o protocolo para permitir que os roteadores processem os pacotes mais rapidamente;
- Prover melhor segurança (autenticação e privacidade) que o atual IP, versão 4.0;
- Dar maior atenção ao tipo de serviço trafegado, particularmente para dados de Tempo Real;
- Permitir o escopo do alcance de um pacote (*Multicasting*);
- Fazer o possível para que um *host* tenha mobilidade sem mudar seu endereço;
- Permitir que o protocolo evolua no futuro;
- Permitir que protocolos antigos e novos coexistam por anos.

Para encontrar um protocolo que alcançasse todos estes objetivos, a IETF lançou uma chamada através da (RFC 1550). Vinte e uma propostas foram recebidas, nem todas completas. Em 1992 foram avaliadas mais profundamente. Algumas propostas faziam pequenos remendos ao atual IP e outras planejavam um protocolo completamente diferente. As três melhores propostas foram publicadas na IEEE Network em 1993. Depois de muita discussão e revisão, uma versão modificada e combinada das propostas de Deering e Francis, chamada SIPP (*Simple Internet Protocol Plus*) foi selecionada e designada IPv6. O atual IP vigente encontra-se na versão 4 (IPv4) e a versão 5 já havia sido atribuída a um protocolo experimental de Tempo Real.

As Recomendações para o protocolo IPv6 foram aprovadas pelo grupo diretor da IETF como um Padrão Proposto na (RFC 1752). Atualmente, o editor do grupo de trabalho

IPng é Robert M. Hinden, membro da IETF desde 1985 e pesquisador na área de interconexão de redes de alta performance e ATM. Hinden auxiliou no grupo de trabalho do SIPP.

O processo de padronização da IETF exige que para se tornar um Proposed Standard, uma idéia precisa ser completamente explicada em uma RFC (Request For Comments) e ter interesse da comunidade científica. Para avançar para o estágio de Draft Standard, é preciso existir uma implementação que tenha sido testada por pelo menos dois sites durante 4 meses. (TANENBAUM, 1996), Atualmente, uma grande parcela dos resultados do grupo de trabalho IPng já foi discutido e implementado por diversos sites em todo o mundo, portanto o IPv6 encontra-se em estágio avançado de padronização. Grandes fabricantes de roteadores como a Cisco e a IBM já tem produtos que suportam a nova versão do IP. A maior parte do trabalho do IPng encontra-se na categoria Padrão Proposto (*Proposed Standard*) e apenas um relatório técnico relacionado ao *path MTU discovery* ainda é um Padrão Rascunho (*Draft Standard*).

A Fig. 7 apresenta o cabeçalho principal do IPv6. Esse cabeçalho é fixo e deve estar associado a toda unidade de informação emitida pela camada de rede. A inovação está no fato de outras informações poderem ser colocadas junto a esse cabeçalho, sempre que necessário, através de cabeçalhos de extensão.

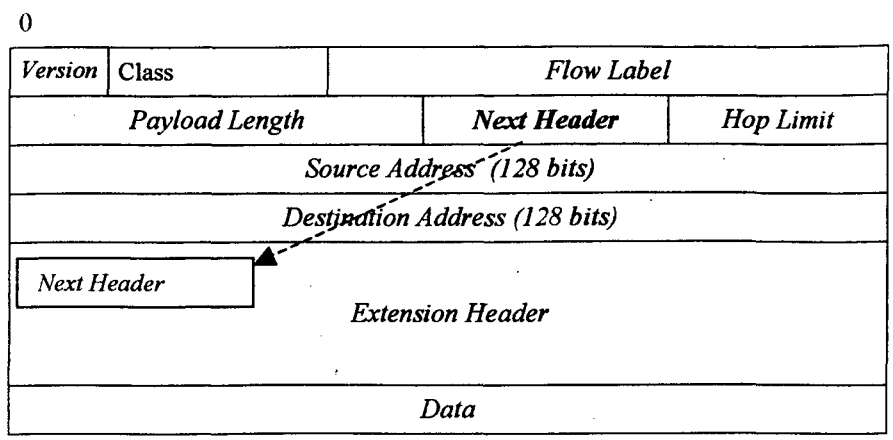

FIGURA 7: A Estrutura do Datagrama Protocolo IPv6

Os campos que compõem este cabeçalho são descritos em:

- *Version* (Versão): Neste campo de 4 bits possui a mesma função do IPv4, ou seja, determinar a versão correspondente do datagrama, que neste caso será sempre 6 (0110).

- *Class* (Classe de Tráfego): É definido com tamanho de 4 bits. Os valores das prioridades para tráfegos com controle de congestionamento estão descritos na Fig. 8. Nela estão protocolos capazes de diminuir o fluxo de envio caso ocorra congestionamento. Para pacotes de aplicações em tempo real que são enviadas em taxa constante existe outra tabela com valores de prioridade de 8 a 15. Para este tráfego, a prioridade mais baixa deve ser usada para datagramas que serão descartados caso exista um congestionamento (e.g. vídeo de alta fidelidade). O valor mais alto (15) deve ser usado para datagramas que serão descartados com menor

facilidade (e.g. tráfego de áudio de baixa qualidade). Não existe relação entre os valores das prioridades dos dois grupos.

- *Flow Label* (Rótulo de Fluxo): Campo que possui 20 bits em seu tamanho, onde o mesmo é uma sucessão de pacotes enviados onde a origem define que os roteadores devem tratar o pacote de maneira especial. Este campo é capaz de reservar recurso para uma aplicação que exija, por exemplo, uma alta qualidade de serviço (QoS). Neste campo está apenas a informação que o datagrama deve ou não ser tratado de maneira especial. A maneira pela qual deve ser tratado é informada em um cabeçalho estendido *Hop-by-Hop* que será visto mais adiante. Pode haver diversos fluxos de uma fonte para um destino, bem como tráfego que não é associado a qualquer fluxo. Este campo permite a distinção

- *Payload Length* (Tamanho da Carga): Ao contrário do IPv4, é um campo que descreve apenas o tamanho do datagrama sem contar com o cabeçalho.

- *Next Header* (Próximo Cabeçalho): Identifica o tipo de cabeçalho que se segue (depois do cabeçalho IPv6), são usados os identificadores de protocolo IPv4, adcionalmente são definidos cabeçalhos de extensão do IPv6 que permitem transportar opções. Este campo possui um tamanho de 8 bits.

- *Hop Limit* (Limite de *Hops):* Campo com tamanho de 8 bits, é idêntico ao campo *Time to Live* (Tempo de Vida) do IPv4, o nó de origem inicializa-o e cada *router* por onde o datagrama passa decrementa-lhe uma unidade, se atingir zero antes de chegar ao destino o datagrama é descartado.onde o é um campo de 8 bits que

decrementado em 1 em cada nó que repassa o pacote. O pacote é descartado caso o limite alcance 0.

- *Source Addres* e *Destination Address:*: Identificam os endereços de IP origem e destino respectivamente, conforme o próprio nome diz.

Prioridade	Tráfego
0	Sem tráfico
1	Nao detalhado
2	Sem tratamento especial (email)
3	Reservado
4	Com tratamento especial (ftp, NFS, http)
5	Reservado
6	Interativo (telnet, X)
7	controle (protocolos de roteamento, SNMP, ICMP)

FIGURA 8: Prioridade Para Tráfego com controle de Congestionamento

Os grupos de padronização sugerem que os cabeçalhos sejam criados em tamanhos múltiplos de 8 bits, devido a questões de performance, conforme a Fig. 9. Os cabeçalhos de extensão já definidos são (BRADNER, 1995):

- *Authentication* – determina a necessidade de autenticação do destino;
- *Destination Options – 2* – trafega informações do destino da mensagem;
- *Destination Options –1* – trafega informações do destino da mensagem;
- *Encryption* - possibilita a encriptação da mensagem;
- *Fragmentation* – transmite informações de fragmentação da mensagem;
- *Hop by Hop Options* – transmite informações adicionais para roteadores;
- *Routing* - determina rotas fixas para a mensagem.

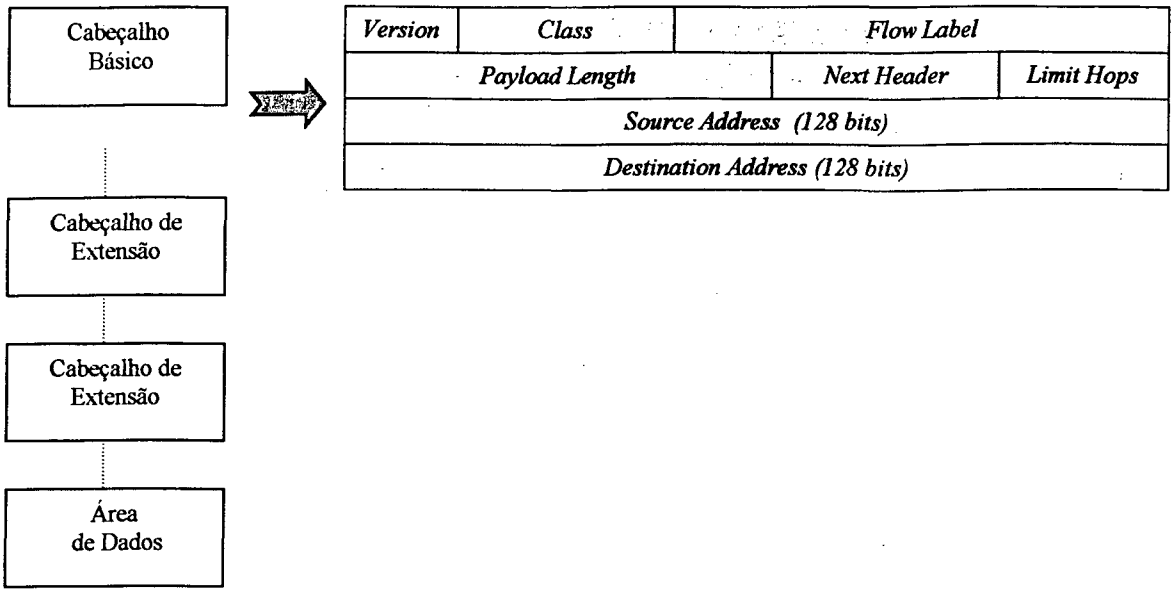

FIGURA 9: Datagrama Protocolo IPv6 com os Cabeçalhos de Extensão

5.2. Cabeçalhos de extensão do IPv6

Os cabeçalhos de extensão foram definidos com a finalidade de fornecer informações adicionais relativas as facilidades utilizadas por um determinado datagrama. A Tab. 1 apresenta os seis cabeçalhos atualmente definidos.

Os campos do cabeçalho IPv6 são significativamente em menor número do que os do IPv4, ao qual nota-se a ausência de qualquer tipo de informação relativamente a fragmentação. O que acontece é que muitos campos passaram a ser opcionais sob a forma de cabeçalhos de extensão. Trata-se de cabeçalhos adicionais que circulam encapsulados no datagrama IPv6.

Um datagrama IPv6 pode transportar vários cabeçalhos, onde cada cabeçalho contém um identificador que indica o tipo do cabeçalho seguinte, depois dos cabeçalhos de

extensão encontra-se a informação (cabeçalho + dados) relativa ao protocolo de nível superior (ICMP, TCP, UDP, etc). Neste último caso são usados os mesmos identificadores de protocolo do IPv4, e para os cabeçalhos de extensão do IPv6 são definidos novos identificadores.

Cabeçalho de Extensão	Valor	Descrição
Hop-by-hop	0	Informações diversas para roteadores
Routing	43	Rota parcial ou integral a ser seguida
Fragmentation	44	Fragmentação de IP
Authentication	50 e 51	Verificação da Identidade do datagrama
Encryped Security Payload	6 e 17	Informações sobre o conteúdo encriptado
Destination Options	60	Informações adicionais par ao destino

TABELA 1: Tipos de cabeçalhos de extensão.

Todos os cabeçalhos de extensão são opcionais, porém caso existam todos, a ordem deve ser a seguinte:

- Cabeçalho IPv6;
- Cabeçalhos de extensão do IPv6;
    - *Hop-by-Hop Options;*
    - *Destination Options;*
    - *Routing;*
    - *Fragment;*
    - *Authentication;*
    - *Encapsulating Security Payload;*

- *Destination Options;*

- Protocolo de Nível Superior.

O cabeçalho de extensão *Destination Options* no final da lista, destina-se a opções dirigidas apenas ao nó final. O outro cabeçalho *Destination Options* será processado em todos os nós indicados no cabeçalho *Routing* (*Source Routing*).

5.2.1. Formato das Opções

Os cabeçalhos de extensão que contêm opções (*Hop-by-Hop Options* e *Destination Options*) utilizam uma estrutura semelhante para armazenar as opções, as estruturas dos cabeçalhos diferem entre si.

A estrutura usada para guardar opções é definida na Fig. 10.

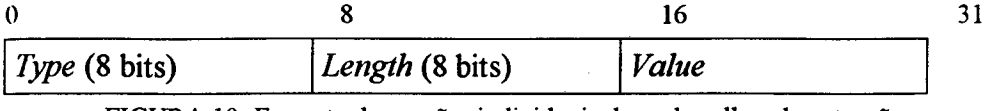

FIGURA 10: Formato das opções individuais dos cabeçalhos de extensão

Os dois bits mais significativos do campo *Type* indicam a ação a tomar quando um nó não reconhece a opção, conforme apresentado na Tab. 2.

Dois bits de mais alta ordem	Ação
00	Desconsidere esta opção
01	Descarte o datagrama e não envie uma mensagem ICMP
10	Descarte o datagrama e envie uma mensagem ICMP
11	Descarte o datagrama e envie uma mensagem ICMP para endereços não *Multicast*

TABELA 2: Tratamento das opções que não forem compreendidas pelo roteador

Os 5 bits de mais baixa ordem do campo *Type* indicam a opção propriamente dita. O terceiro bit de mais alta ordem indica se os dados desta opção poderão mudar ou não durante o percurso do pacote.

5.2.2. Opções de enchimento: Pad 1 e PadN

As opções devem ficar alinhadas a 32 bits com o cabeçalho. Nos casos em que basta um octeto para garantir o alinhamento usa-se a opção Pad 1 (tipo=0), correspondendo a um enchimento com o 8 bits zero. A opção Pad1 é o único caso particular que não respeita a estrutura geral das opções.

Quando são necessários mais do que um octeto, utiliza-se a opção PadN (tipo=1), com o comprimento necessário para o enchimento (o campo *Data Length* pode conter o valor zero, correspondendo a dois octetos de enchimento).

5.2.3. Cabeçalho de extensão "Hop-by-Hop Options"

Este cabeçalho de extensão contém opções a serem processadas em todos os nós percorridos pelo datagrama, a sua presença é identificada pelo valor zero no campo Próximo Cabeçalho do cabeçalho IPv6, o formato deste cabeçalho pode ser verificado na Fig. 11.

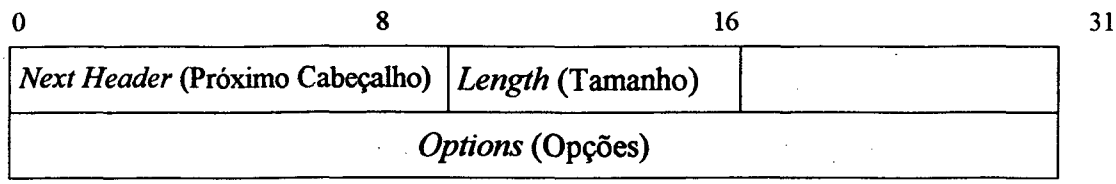

FIGURA 11: Formato do Cabeçalho de extensão *Hop-By-Hop*

Esta especificação do protocolo define a opção chamada *Jumbo Payload,* cuja identificação é 194, servindo para transportar pacotes com mais de 65.535 bytes. Se esta opção for ativada, a opção Tamanho da Carga do cabeçalho principal do IPv6 é indicada com o valor zero "0"

A opção *Jumbo Payload* pretende tirar partido de implementações de camadas inferiores que suportam um MTU superior a 65.575 (dados + 40 octetos do cabeçalho IPv6), por esta razão estes datagramas nunca são fragmentados. A coexistência da opção *Jumbo Payload* com um cabeçalho de extensão *Fragment* leva o nó receptor a enviar uma mensagem ICMP "*Parameter Problem*" com código igual a zero, apontando para o referido cabeçalho.

5.2.4. Cabeçalho de extensão "Routing"

Este cabeçalho é usado pelo nó de origem para indicar uma lista de nós a visitar no percurso do datagrama (*source routing*), é identificado pelo valor 43 no campo Próximo Cabeçalho do cabeçalho anterior. A Fig. 12 indica seu formato.

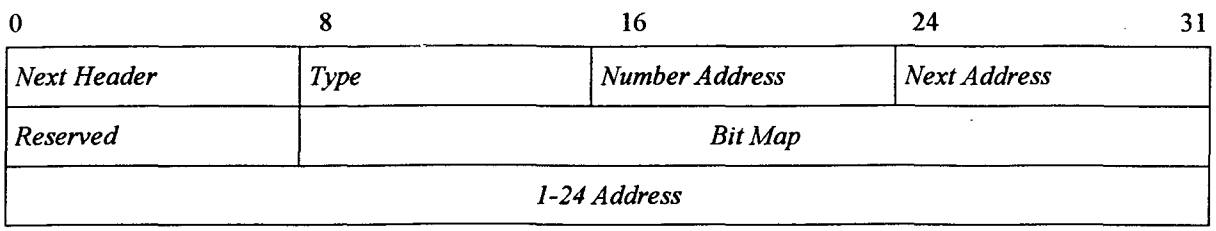

FIGURA 12: Formato do cabeçalho de extensão *Routing*

O campo *Next Header* (Próximo cabeçalho) possui a mesma função de todos os outros cabeçalhos, ou seja, identificar o próximo tipo de cabeçalho. O campo de maior importância é o *Type* (Tipo), que permite identificar as variantes deste cabeçalho, sendo que a constituição do último campo depende do valor deste campo, ou seja, indica o tipo de roteamento. Atualmente este campo é definido em zero. *Number Address* (Número do Endereço) indica o número de endereços presentes neste cabeçalho (de 1 a 24). O Campo *Next Address* indica o próximo endereço para o qual o datagrama poderia ser enviado. Este campo inicia com o zero (0) e é incrementado cada vez que um endereço é visitado. Já o campo *Bit Map* (Mapa de Bits) é um mapa de bits que serve para indicar qual dos tipos de tratamento deve ser tomada a cada um dos roteadores. O endereço pode ser visitado

diretamente depois que o antecede (*strict*) ou faze-lo indiretamente, podendo existir *loose*, ou seja, roteadores intermediários.

5.2.5. Cabeçalho de extensão "Fragment"

Tal como o IPv4, o IPv6 suporta fragmentação de datagramas de modo a que estes se ajustem ao MTU (*Maximum Transmission Unit)* das camadas inferiores das ligações por onde passa.

Ao contrário do que acontecia com o IPv4, a fragmentação no IPv6 não é implementada entre nós intermédios. O nó de origem é obrigado a determinar o valor mínimo do MTU no caminho que o datagrama vai seguir, o nó de destino final procede ao reagrupamento.

O IPv6 exige que todas as ligações suportem um MTU de no mínimo de 576 octetos. Os nós devem implementar o mecanismo *Path* MTU *Discovery* (RFC 1191), que permite a determinação do MTU máximo para um dado caminho.

O cabeçalho de extensão Fragment é identificado pelo valor 44 no campo *Next Header* do cabeçalho anterior, é apresentado na Fig. 13.

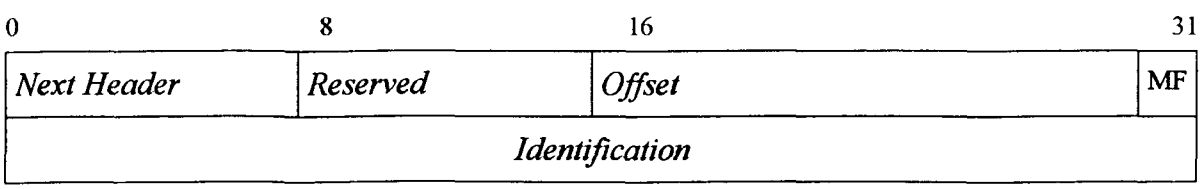

FIGURA 13: Formato do cabeçalho de extensão *Fragmentation*

Next Header (Próximo Cabeçalho) indica obviamente, o próximo cabeçalho de extensão. O campo *Offset* indica a que ponto do datagrama original o fragmento pertence. Já o campo MF refere-se a existência de mais fragmentos ou se este trata-se do último. Finalmente, o campo *Identification* (Identificação) simboliza unicamente o fragmento assim como no IPv4. O número de bits deste campo foi ampliado devido as redes de alta velocidade.

Para efeitos de fragmentação, um datagrama IPv6 divide-se em duas partes:

- Parte Não Fragmentável: Constituída pelo cabeçalho IP e cabeçalhos de extensão com processamento em nós intermédios, ou seja, até ao cabeçalho de extensão *Routing*, inclusive.
- Parte Fragmentável: Outros cabeçalhos de extensão e dados.

Cada fragmento contém uma cópia da parte não fragmentável do datagrama original, seguida do cabeçalho de extensão *Fragment* e finalmente o fragmento propriamente dito (da parte fragmentável). O campo *Payload Length* dos cabeçalhos IPv6 de cada fragmento são alterados de modo a conterem o tamanho do fragmento.

5.2.6. Cabeçalhos de extensão "Destination Options"

Este cabeçalho possui a mesma estrutura do cabeçalho de extensão *Hop-by-Hop* e destinam-se a transportar opções adicionais, identificado pelo valor 60 no campo *Next Header* do cabeçalho anterior.

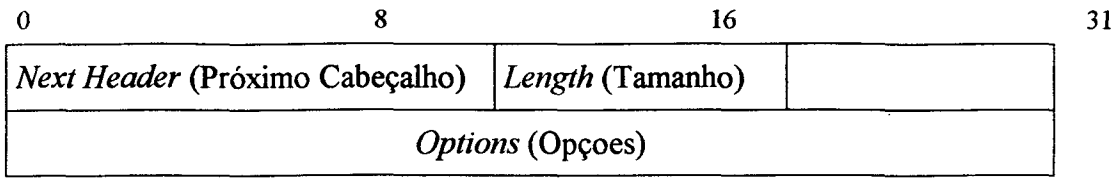

FIGURA 14: Formato do Cabeçalho de extensão *Destination Options*

A diferença entre *Hop-by-Hop* e *Destination Options*, é que o primeiro (*Hop-by-Hop)* deve ser processado por todos os roteadores, enquanto *Destination Options* somente pelo seu destino. Como os campos já foram definidos anteriormente, não se faz necessário à redefinição dos mesmos.

5.2.7. Ausência de Cabeçalho de Extensão Seguinte

O valor 59 no campo Próximo Cabeçalho de um cabeçalho indica que nada se lhe segue.

5.3. Propósitos do projeto do IPv6

O IPv6 mantém as principais características que fizeram do IPv4 um sucesso mundial. Assim como o IPv4, é um protocolo sem conexão, ou seja, cada datagrama contém um endereço de destino e é roteado de forma independente. O IPv6 também possui um número máximo de roteadores por onde pode passar (*Hop Limit*). Com objetivo de simplificar a principal função do IP, rotear pacotes, vários campos foram suprimidos e outros tornaram-se opcionais.

Visando a atualização e a melhora deste protocolo em relação ao IPv4, o projeto do protocolo IPv6 determina o foco de atuação e estudos em três principais áreas:

- Endereçamento;
- Segurança e;
- Desempenho.

5.3.1. Endereçamento

A estrutura de endereçamento do IPv6 de 128 bits (RFC 1884) permite mais de 340 x 10^{34} endereços para interfaces na rede contra os apenas (256^4) possíveis com o IPv4. Desta forma podemos imaginar, na pior das hipóteses, um endereçamento que resultaria em 1564 endereços / m^2 da superfície terrestre.

Os 128 bits ou 16 bytes de um endereço IPv6 pode ser descrito por oito grupos de 4 dígitos hexadecimais (base 16: de 0 a F), com o símbolo de dois pontos ":" separando cada grupo conforme descrito na Fig. 15.

8000:0000:0000:0000:0123:4567:89AB:CDEF

FIGURA 15: Exemplo de um Endereço IPv6

Para facilitar a escrita, um ou mais grupo de 0000 pode ser substituído por ":", assim como um zero à esquerda pode ser suprimido, conforme a Fig. 16.

8000::123:4567:89AB:CDEF

FIGURA 16: O Mesmo Endereço da Fig. 15 em Outra Notação

A (RFC 1924) sugere outra forma de representação usando base 85, permitindo qualquer endereço IPv6 com exatamente 20 caracteres. Para isto, foram escolhidos os seguintes 85 caracteres em ordem crescente, conforme apresentado na Fig. 17.

'0'..'9', 'A'..'Z', 'a'..'z', '!', '#', '$', '%', '&', '(', ')', '*', '+', '-', ';', '<', '=', '>', '?', '@', '^', '_', '`', '{', '|', '}', '~'.

FIGURA 17: Lista de caracteres para representação alternativa do IPv6

Independente da notação utilizada, muito embora a aconselhada seja a hexadecimal em blocos de 16 bits, esta grande mudança é possível devido a alteração de tamanho, em bits, do endereço IP que passou a ser representado por 128 bits contra os 32 da versão anterior e sem o uso de classes como no IPv4. Além do mais o IPv6 é auto-configurável, ou

seja, permite que uma interface obtenha o seu endereço IP e informações a respeito da rede a que ele pertence no momento de sua conexão à rede de forma transparente, sem o risco de alocação de um endereço duplicado.

O endereçamento do IPv6 é organizado de forma hierárquica, de modo que exista uma instância superior para distribuir os endereços a uma instância inferior, que por sua vez os distribuem para outras instâncias. A intenção é diminuir o tamanho das tabelas de roteamento, uma vez que a distribuição das instâncias se dará de uma forma estruturada e lógica a partir de prefixos do endereço IP.

O modo de comunicação na rede também foi modificado, se com o IPv4 a comunicação se dá através do envio de datagramas para todos os endereços de interfaces dentro de uma mesma sub-rede, modo de comunicação chamado de *broadcasting*, no IPv6 a comunicação é sempre direcionada à interface ou ao grupo de interfaces a que se deseja comunicar. O IPv6 apresenta três tipos de endereçamentos: *multicasting*, onde o datagrama é enviado a uma ou mais interfaces diretamente sem que as outras que não foram indicadas recebam o datagrama; *unicasting*, onde o datagrama é enviado a uma interface unicamente sendo este o modo padrão nas implementações do protocolo IPv6; e , por fim, o modo *anycasting*, onde o datagrama é enviado a um conjunto de interfaces e apenas uma desse conjunto recebe o datagrama. Assim a rede passa a fazer um melhor uso da largura de banda disponível para comunicação, aprimorando a qualidade do serviço de rede por ela oferecida (DEERING, 1998).

O IPv6, ao contrário do IPv4, não utiliza a idéia de classes de endereços. Porém utiliza o mesmo tipo de prefixação que passam a indicar os diferentes usos dos endereços. A Tab. 3 mostra estas faixas.

Prefixo Binário	**Utilização**	**Fração**
0000:0000	Reservado (incluindo IPv4)0	1/256
0000:0001	Não definido	1/256
0000:001	Endereço OSI NSAP	1/128
0000:010	Endereço Novell Netware IPX	1/128
0000:011	Não definido	1/128
0000:1	Não definido	1/32
0001	Não definido	1/16
001	Não definido	1/8
010	Endereço baseado no provedor	1/8
011	Não definido	1/8
100	Endereço baseado na localização geográfica	1/8
101	Não definido	1/8
110	Não definido	1/8
1110	Não definido	1/16
1111:0	Não definido	1/32
1111:10	Não definido	1/64
1111:110	Não definido	1/128
1111:1110:0	Não definido	1/512
1111:1110:10	Endereços para uso local do enlace	1/1024
1111:1110:11	Endereços para uso loção do site	1/1024
1111:1111	Multicast	1/256

TABELA 3: Faixas de Endereços IPv6

5.3.1.1. Endereçamento *Multicasting*

Um endereço *multicast* identifica um grupo de interfaces pertencentes a diferentes nós, mas um pacote destinado a um endereço *multicast* é enviado para todas as interfaces do grupo, conforme representado na Fig. 18. O segundo octeto que se segue ao prefixo define o tempo de vida (TTL) e o contexto do endereço *multicast.*

Um endereço permanente *multicast* tem um parâmetro de tempo de vida igual a zero "0" enquanto um endereço temporário tem o mesmo parâmetro igual a um "1".

O contexto para este tipo de endereço apresenta os valores conforme descrita na Tab. 4.

Valor	**Escopo**
2	*Link-local*
5	*Site-local*
8	*Organization-local*
E	*Global*

TABELA 4: Escopo para um endereço *Multicasting*

A definição da zona de atuação não afeta os identificadores de grupo de *multicast*, apenas define as máquinas do grupo que devem receber os dados.

Relativamente ao emissor de um datagrama, os valores definem uma hierarquia de destinos com dimensão crescente.

Estão definidos alguns *well known multicast addresses* (endereços multicast bem-conhecidos), cuja sua principal utilização é identificar conjuntos de máquinas que implementam determinados tipos de serviço:

- O identificador zero está reservado FF0?:0:0:0:0:0:0:0
- Todos os nós FF01:0:0:0:0:0:0:1

  FF02:0:0:0:0:0:0:1
- Todos os *routers* FF01:0:0:0:0:0:0:2

  FF02:0:0:0:0:0:0:2
- Servidores DHCP IPv6 FF02:0:0:0:0:0:0:C

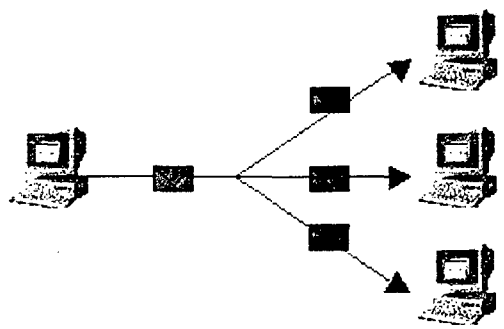

FIGURA 18: Serviço Multicast.

5.3.1.2. Endereçamento *Unicasting*

Este tipo de endereçamento identifica uma única interface específica. O pacote enviado para um endereço *Unicast* é entregue a interface especificada pelo endereço, ou seja, o endereço de destino é associado somente um computador, conforme descrito na Fig. 19.

Tal como acontece para o IPv4, existem alguns endereços com utilizações reservadas:

- Endereços desconhecidos – 0:0:0:0:0:0:0:0
- Endereços de *Loopback* - 0:0:0:0:0:0:0:1

Os endereços *unicast* são identificados por um início diferente de 1111:1111. Os endereços *unicast* possuem formato idêntico ao *anycast*, porém sua estrutura interna de um endereço *unicast* pode ser definida conforme as necessidade. Numa rede local IEE 802 propõe-se a utilização de 48 bits menos significativos para armazenar MAC da interface. Este procedimento torna desnecessário o ARP. Os bits seguintes poderão ser utilizados pela organização para definir sub-redes internas, onde a parte mais significativa contém um identificador da organização (*subscriber prefix*).

FIGURA 19: Serviço *Unicast*

5.3.1.3. Endereçamento *Anycasting*

Este tipo de endereçamento é utilizado para identificar um grupo de interfaces pertencentes a nós distintos. Um pacote destinado a um endereço *anycast* é enviado para uma das interfaces identificada pelo endereço, conforme ilustra a Fig. 20. Especialmente, o pacote é enviado para a interface mais próxima de acordo com o protocolo de *routing.*

Um endereço *anycast* não pode ser utilizado como endereço de origem (*source address)* de um pacote IPv6.

Este tipo de endereçamento é útil para detecção rápida de um determinado servidor ou serviço. Pode-se (por exemplo) definir um grupo de servidores de DNS configurados com endereçamentos *anycast*, assim um *host* irá aceder ao serviço mais próximo utilizando este endereço. Para cada endereço *anycast* atribuído, existe um prefixo mais longo desse mesmo endereço que identifica a região ao qual todas as interfaces pertencem.

Os endereços *anycast* são na realidade endereços únicos, com a particularidade de um mesmo endereço estar atribuído a vários nós. Pretende-se que ao usar um endereço *anycast* para destino de um datagrama, seja atingido o nó mais próximo (menor métrica) que possui esse endereço.

Para efeitos de *routing,* está definido um tipo particular de endereço *anycast* (*Subnet-Router anycast address*), onde todos os *routers* de uma dada sub-rede possuem o endereço *anycast* correspondente à sub-rede, com o valor zero para o identificador de interface.

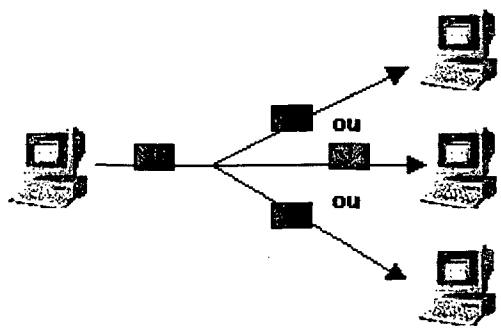

FIGURA 20: Serviço *Anycast*

5.3.2. Segurança

O *IETF (Internet Engineering Task Force)* organizou um grupo de trabalho denominado *IPSec (IP Security Protocol).* O objetivo é desenvolver mecanismos que ofereçam proteção ao datagrama IP e às aplicações que rodam sobre o protocolo IP, estabelecendo níveis de segurança para as comunicações *host-a-host, subrede-a-subrede* e *host-a-subrede*. A esse protocolo foi dado o nome de *IPSec* (ATKINSON, 1998).

O *IPSec* é uma plataforma aberta formada por um conjunto de protocolos que provêm serviços de autenticação, integridade, controle de acesso e confidencialidade na camada de rede IP, tanto em redes com o protocolo IPv4 como em redes com o protocolo IPv6. Ele foi desenvolvido para oferecer serviços de segurança com alta qualidade de serviço, baseados em controle de acesso, integridade não orientada à conexão, autenticação na origem dos dados e confidencialidade.

O IPv6 utiliza os cabeçalhos de extensão para prover autenticação e criptografia. A segurança é fornecida através da encriptação dos dados e da inclusão de mecanismos de autenticação do datagrama conforme (ATKINSON, 1998). Desta forma é possível ter segurança contra duplicação de dados na rede e contra ataques de *hackers* que utilizam a técnica de desviar o tráfego de uma máquina para outra de sua posse, por exemplo. O objetivo maior do *IPSec* é garantir ao IP mecanismos de criptografia e autenticação sem causar um impacto adverso no desempenho da Internet como um todo.

5.3.3. Desempenho

O desempenho de uma rede IPv6 está relacionado diretamente ao desempenho do roteamento de seus datagramas. O tráfego de datagramas IP que deixam uma rede e conseqüentemente têm de passar pelo roteador é crescente devido à incorporação de novos serviços na Internet. Além do mais a velocidade dos meios de transporte também se eleva à medida que as tecnologias se aperfeiçoam, assim os roteadores têm de ser capazes de receber, processar, desfragmentar e enviar datagramas sempre com mais rapidez, para não comprometer o funcionamento de toda a Internet.

Apesar do cabeçalho do datagrama do IPv6 necessitar do dobro da quantidade de bits de um cabeçalho do IPv4 ele possui menos campos que este, o que diminui o tempo de processamento dos datagramas no roteador, além disso, os cabeçalhos de extensão que não importam ao roteamento não são processados nos roteadores, o que melhora

significativamente o desempenho do roteamento. É interessante observar, também, que o IPv6 fragmenta os datagramas com mais eficiência de modo que a fragmentação e a remontagem destes somente ocorra nos equipamentos de origem e destino dos mesmos, diminuindo a sobrecarga de trabalho nos roteadores (GONCALVES, 1998).

É possível a otimização do desempenho do IPv6 através do campo *Rótulo de Fluxo* do cabeçalho do datagrama. Nesse campo é possível controlar serviços nos roteadores ao longo do caminho, como prioridade de envio do datagrama, atrasos, requerimentos de largura de banda, tratamento de congestionamentos e outros requisitos de qualidade desses serviços. As otimizações realizadas pelo cabeçalho IPv6 valem para todos os outros datagramas da seqüência, não sendo necessário a reavaliação desse campo em cada datagrama.

Esta dissertação visa aprofundar mais nos aspectos de desempenho do protocolo IPv6, envolvendo avaliações analíticas em ambientes simulados, focalizando o tráfego entre uma interface e o caminho percorrido pelos datagramas.

6. TRANSIÇÃO IPv4 PARA IPv6

Este capítulo apresenta os aspectos referente à transição do protocolo de Internet em sua atual versão 4 (IPv4) para um novo protocolo denominado IPv6, apresentando as exigências, componentes e técnicas atualmente em pesquisa e atuação.

6.1. Introdução

Devido a problemas de limitações de endereços e a falta de segurança entre outros, a vida do IPv4 deve ter seus dias contados.

O IPv6 será implementado gradativamente, de modo que ambas as versões IP deverão coexistir por alguns anos, até que o período de transição seja completado e todos os *hosts* do planeta sejam IPv6. Assim, este deverá apresentar uma total compatibilidade com versão anterior, gerando desta forma uma interoperabilidade e a transição seja conduzida de forma transparente para a sociedade.

O fato do IPv6 ter em sua faixa de endereços as do IPv4, não garante a total compatibilidade entre eles, pois os datagramas destas versões são incompatíveis.

A transição definitivamente é um assunto caro para as grandes organizações e a tentação para ficar com a tecnologia velha é forte.

As especificações do IETF referentes ao IPv6 contém muita informação relativo aos assuntos de transição. A maioria dos documentos são apresentados em forma de RFCs, e algum material está disponível como desenhos de Internet e publicações. Esta pesquisa está em constante evolução, e as informações aqui contidas refletem os assuntos mais significantes atualmente da transição IPv4 para IPv6.

6.2. Exigências para Transição

O processo de transição do atual IPv4 para IPv6 pode ser comparado aos processos de migração de menor escala que acontece em todo o tempo. Versões de sistemas operacionais, softwares de aplicação e banco de dados são exemplos bons de tal migração. Porém, as dificuldades e investimentos necessários para tal transição podem ser comparadas as efetuadas em sistemas e equipamentos ocorrido na década passada, a fim de solucionar o problema do "bug do milênio".

Os desagrados fixados para a transição de IPng deveriam ser iguais as que ocorrem em migrações de menor escala. Porém, para a comunidade de Internet global é a transição de maior importância para a história da Internet, devendo esta ficar atenta a todos os detalhes.

A transição exige de forma direta definições de especificações, desenvolvimento de produtos e por fim o serviço a ser provido.

6.2.1. Minimizando a Resistência

É assumido o desconforto geral de grandes organizações para IPng. Os pontos de vista do IETF e indústrias são diferentes e podem conduzir a significante resistência para a adoção da nova tecnologia. As Indústrias vêem o mundo do ponto de vista empresarial. Computação como um todo é uma ferramenta de negócio, onde as técnicas utilizadas nunca são mais importantes.

A total migração para o IPv6 poderá provavelmente levar mais que uma década, entretanto nunca estará completa a menos que as técnicas de transição sejam aceitas pela maioria dos usuários da Internet e tendo conhecimento da necessidade de flexibilidade da transição, compatibilidade com sistemas antigos e principalmente custo previsto.

6.3. Componentes de Transição

6.3.1. Hosts

Na prática a transição não poderá restringir o uso de *hosts* IPv4, mas sim ter a capacidade operacional de operar simultanemanete com IPv6. Para permitir interoperabilidade sem retalhos, todos os *Hosts* IPng correntes devem poder ainda comunicar-se com a tecnologia mais velha. No software de nível de aplicação projetado para IPv4 deverá ser utilizado o API mais antigo, enquanto aplicações de IPng novas usam

o API recompilado. Assim a aplicação deverá reconhecer qual protocolo estará sendo utilizado. O API IPv4 e aplicações de padrão deveriam estar bem disponíveis em *Hosts* IPv6 como se interagissem com ferramentas comuns (g.e. FTP, Telnet).

6.3.2. DNS

A concepção do DNS (*Domain Name Service)* está definida nas RFCs 974, 1034 e 1035, havendo várias implementações comerciais feitas a partir destes documentos, podendo conter pequenas diferenças em cada implementação.

O funcionamento do DNS é importante conceituá-lo como um grande banco de dados abstrato que é formado a partir de milhares de máquinas denominadas servidores de nomes, que se encontram distribuídas na Internet. Assim, ao submetermos uma pesquisa de nome ao DNS, para obter o endereço IP, teoricamente seria equivalente a submetê-la a um grande banco de dados que contém todos os registros de nomes de todos os *"host"* da rede, enquanto na prática este banco de dados encontra-se distribuído em milhares de máquinas, e a pesquisa de nomes vai transitando de um servidor para outro, até que seja resolvida.

Um novo DNS denominado "AAAA" foi definida para o IPv6 (RFC 1886). Uma vez que nodos IPv6/IPv4 tem de interoperar diretamente com protocolos Ipv4 e Ipv6, este novo DNS deverá fornecer endereços de resolução de nomes capaz de tratar pacotes do tipo "A" (IPv4) e do tipo "AAAA" (Ipv6).

6.4. Técnicas de Transição

O SIT (*Simple Internet Transition Mechanisms)* é um conjunto de mecanismos criados para permitir a transição IPv4-IPv6. Este projeto foi desenvolvido de modo a facilitar aos utilizadores, administradores de sistemas e operadores a instalação e integração do IPv6. Seus objetivos são:

- permitir a atualização progressiva e individual de *hosts* e *routers;*
- evitar as dependências de atualização;
- completar a transição antes do esgotamento do espaço de endereçamento IPv4;
- Os mecanismos introduzidos pelo SIT asseguram que *hosts* IPv6 possam interoperar com *hosts* IPv4 até o momento em que os endereços IPv4 se esgotem. Com a utilização do SIT há a garantia de que a nova versão do protocolo IP não vai tornar obsoleta a versal atual, protegendo assim o enorme investimento já realizado no Ipv4. Os *hosts* que necessitam apenas de uma ligação limitada (g.e. impressora) não precisarão nunca ser atualizadas para IPv6. As técnicas introduzidas pelo SIT são: camada IP dupla *(dual stack),* endereços IPv6 compatíveis com IPv4 e túneis IPv6 em IPv4 (com encapsulamento de cabeçalhos).

6.4.1. Camada Dupla *(dual stack)*

Para permitir a comunicação entre nodos apenas IPv6 e nodos apenas IPv4, criou-se uma pilha dupla, que implementa as duas versões de protocolo IP. Nodos que implementam esta pilha tem a designação de nodos IPv6/IPv4 e conseguem comunicar com as duas versões do IP.

Com esse mecanismo, nodos IPv6 devem ter as duas pilhas TCP/IP internamente, a pilha da versão 6 e a da versão 4. Através da versão do protocolo, se decide qual pilha processará o datagrama. Esse mecanismo permite que nodos já atualizados com IPv6 se comuniquem com nodos IPv4, e realizem roteamento de pacotes de nodos que usem somente IPv4.

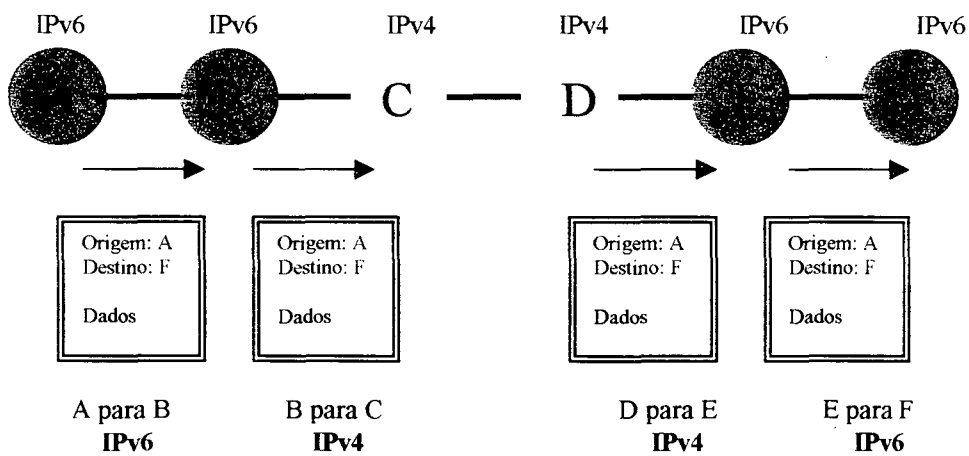

FIGURA 21: Camada dupla *(dual)*

6.4.2. Túneis IPv6 em IPv4

Na medida em que o desenvolvimento e a instalação das infraestruturas de *routing* IPv6 não são concluídas, pode-se encaminhar tráfego IPv6 através de infraestruturas IPv4 utilizando túneis IPv6 em IPv4. Um *router* ou *host* que implemente a pilha dupla TCP/IP situado no extremo de uma topologia IPv6 tem apenas a função de encapsular datagramas IPv6 em IPv4 - adicionar um cabeçalho especial IPv4 a um datagrama IPv6, enviando-o de seguida através de infraestruturas IPv4, como se fossem dados IPv4 normais. Os *routers* IPv4 efetuam o reencaminhamento destes dados sem envolvimento do protocolo IPv6. Na outra extremidade do túnel encontra-se outro *router* ou *host* que tem a função de desencapsular o pacote IPv6, retirar-lhe o cabeçalho IPv4, e encaminhar o pacote para o seu destino, usando as funções do protocolo IPv6.

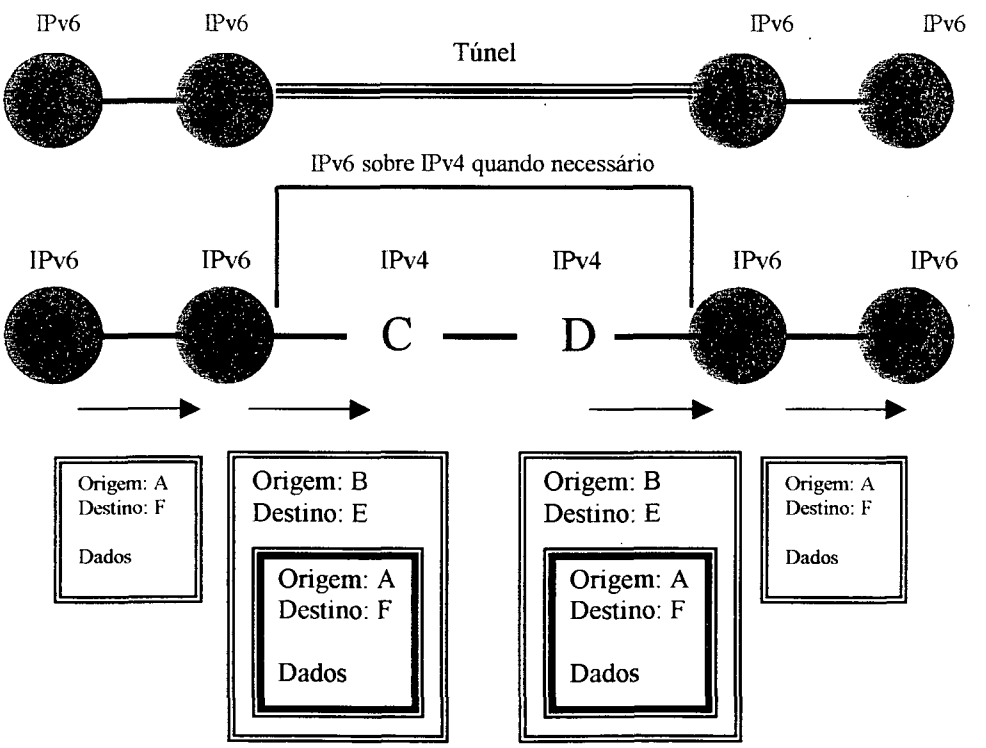

FIGURA 22: Túnel IPv6 em IPv4

Existem dois tipos de túneis IPv6 em IPv4: configurado e automático. Estes que diferem principalmente no modo como é determinado o endereço do final do túnel. A maior parte dos mecanismos de base é comum aos dois tipos:

- o nodo entrada do túnel faz o encapsulamento do pacote IPv6 num cabeçalho IPv4;
- o nodo saída do túnel recebe o pacote encapsulado, retira o cabeçalho IPv4, atualiza o cabeçalho IPv6 e processa o pacote IPv6 resultante;
- os nodos que fazem encapsulamento podem necessitar de manter informação respeitante a cada túnel, como por exemplo a MTU dos túneis que servem.

Em **túneis configurados**, o endereço do nodo de saída do túnel é determinado com base em informação de configuração no nodo onde se faz o encapsulamento. Este nodo necessita de armazenar o endereço do final de cada túnel que nele se inicia. Quando um pacote IPv6 é transmitido através de um túnel, o endereço final configurado para esse túnel é usado como endereço destino do cabeçalho IPv4 que encapsula o pacote.

A determinação de quais os pacotes a enviar por cada túnel é feita através de informação de *routing* do nodo que vai encapsular esses pacotes.

Em **túneis automáticos**, o endereço do nodo de saída do túnel é determinado a partir do pacote que vai ser encapsulado. O endereço destino do pacote original deve ser um endereço IPv6 compatível com IPv4, sendo o endereço do final do túnel a componente IPv4 do primeiro, onde os 32 bits menos significativos do endereço IPv6 compatível com IPv4 serão completados com zero.

6.5. Migrando Aplicações

Um grande número de aplicações existentes que usam e estrutura TCP/IP foram implementadas durante anos. A principal preocupação com relação a estes softwares é justamente o endereçamento. Em prática, o *host* assume o IP interno de 32 bits, e as aplicações provavelmente migrarão gradativamente para o Ipng.

Assim a conclusão imediata é que uma aplicação de TCP/IP existente não pode enviar exclusivamente IPv6 ao *host*, ou seja, deve haver uma configuração opcional.

Sistemas Operacionais como Windows 2000, Windows NT e Windows XP já possuem suporte à IPv6, porém é claro e explícito que estes suportes são experimentais.

6.6. Considerações Finais

Este capítulo apresentou as possíveis formas de transição do atual protocolo de comunicação de Internet (IP) em sua versão 4 (IPv4), para um novo na versão 6 (IPv6), obedecendo regras de integração definidas em RFCs e descritas pelo IETF.

Tal transição não consiste somente na redefinição e especificação de um novo protocolo, mas também nos produtos e serviços providos.

Pelo estudo realizado, é impossível prever o tempo que será gasto para que total migração seja efetuada, mesmo porque o protocolo IPv4 não poderia deixar de existir

rapidamente devido a grande utilização e propagação do mesmo. Além disso, pode haver definições a serem efetuadas, além de que há uma resistência a tal mudança por grande parte da grande comunidade comercial de Internet.

Um novo protocolo, como o IPv6 aqui estudado, funciona muito bem na teoria, porém qualquer que seja a estratégia de migração será altamente árdua. Apresentar uma solução ideal para tal transição é sem dúvida um desafio que onera uma profunda pesquisa onde resultados práticos são absolutamente necessários para uma correta análise do assunto. Mesmo assim, haverá inúmeras situações que provavelmente não serão previamente observadas, exigindo desta forma uma necessidade de administração momentânea do problema.

Teoricamente, o tunelamento (Túneis IPv6 em IPv4) seria mais fácil de ser implementado, devido a possibilidade trafegar datagramas IPv6 utilizando a velha, conhecida e até o momento utilizada estrutura IPv4, interligando assim duas redes IPv6 em redes IPv4.

Desta forma, *router* ou *host* situados no extremo de uma topologia IPv6 ficariam apenas encarregados de encapsular datagramas IPv6 em IPv4 enviando-os conseqüentemente por infraestruturas IPv4. Este processo descarta a necessidade de criação das estruturas específicas IPv6 e também exija que todos migrem para a nova estrutura.

7. CONCLUSÃO

7.1. Considerações Iniciais

Este trabalho apresentou os protocolos IPv4 e IPv6 em seus aspectos teóricos, comparando-o com o IPv4, que é a versão atualmente em uso.

Devido a pouca publicação a respeito de transição destes protocolos, este trabalho passa a obter sua relevância, pois é realizado um profundo estudo a respeito destes protocolos.

É claramente um desafio lançar IPng na comunidade de Internet, não tanto para os usuários domésticos e educacionais, mais sim para as grandes organizações de Internet.

As técnicas de transição especificadas pelo IETF satisfazem bastante as exigências gerais, O esquema representado é de fácil adoção. As principais áreas de melhorias estão na configuração e administração, mas podem ocorrer complexidades maiores durante a fase de transição onde deverão funcionar as duas versões simultaneamente.

Obviamente, toda e qualquer transição deste porte exige um enorme empenho da comunidade, seja ela científica ou comercial. É notável também que devida a alta complexidade envolvida nesta transição, as partes interessadas prorroguem ao máximo este processo, aguardando resultados de estudos e projetos em andamento, sejam eles resultados positivos ou negativos, mas que sirvam de base para futuras implementações.

Enquanto não houver um *backbone* que ofereça serviços de tráfego em IPv4 e IPv6, simultaneamente ou não, não haverá o verdadeiro interesse de implementação e/ou transição para este novo protocolo. A Própria *Microsoft* informa em seu mais recente produto, o *Windows Xp*, que as implementações IPv6 contidas no mesmo são restritas para estudos e testes científicos e não há nenhuma responsabilidade e formalização sobre o serviço. Desta forma, enquanto houver mecanismos e possibilidades de mantermos o IPv4 em funcionamento, certamente será mantido este protocolo até que seja realmente necessário, seja por questões de endereçamento, segurança ou desempenho.

Uma pergunta interessante que permanecerá provavelmente anos é: "Será que haverá um dia em que não nenhuma função de apoio ao IPv4 será necessária?".

7.2. Resultados Alcançados

Os objetivos propostos neste trabalho foram alcançados com sucesso, tanto os objetivos gerais quanto os objetivos específicos. Dos objetivos gerais o estudo dos protocolos IPv4 e IPv6 merecem destaque. A mídia em geral concentra-se a mudança focando apenas a questão do endereçamento, que passa de 32 bits para 128 bits. De fato, esta alteração resolve um problema espacial de endereçamento, mas não só este. O estudo mais profundo do IPv6 mostra que as mudanças propostas pela comunidade internacional não se limitam a tão pouco. De forma geral pode-se dizer que o IPv6 não é compatível com

o IPv4, mesmo existindo mecanismos para que as duas versões possam estabelecer comunicação.

Quanto aos objetivos específicos propostos, os resultados obtidos deste estudo referente as atuais formas de transição foram satisfatórios, podendo-se neste material ter a noção exata da dificuldade em se consolidar por completo esta migração, mesmo porque há pouco material publicado sobre o assunto.

Por este trabalho não apresentar resultados sobre estudos práticos desta transição, fica indicada a possível continuidade de estudo sobre o assunto, implementando as situações de transição citadas no capítulo anterior, mostrando desta forma resultados práticos, tornando mais clara a real problemática do assunto.

8. REFERÊNCIAS BIBLIOGRÁFICAS

(COMER, 1994) COMER, Douglas E. *Internetworking with TCP/IP Vol.II: Design, Implementation, and Internals, 2rd ed.* Prentice Hall, 1994. http://www.cs.purdue.edu/comer

(ATKINSON, 1998) ATKINSON, R; KENT S. *Security Architecture for the Internet Protocol.* Request for Comments : 2401. IETF, Novembro, 1998.

(BRADNER, 1995) BRADNER, S.; MANKIN, A.*The Recommendation for the IP Next Generation Protocol.* Request for Comments : 1752. IETF, Janeiro, 1995.

(BOZZANO, 1998) BOZZANO, Jussara Maria. *Gerenciamento de Autoconfiguração em Redes com IPv6.* Dissertação de mestrado do CPGCC-UFSC. Florianópolis, Brasil. Setembro, 1998.

(CERF, 1998) CERF., Vinton G. A Brief. *History of the Internet and Related Networks.* Internet Society (ISOC). Fevereiro, 1998. Site: http://www.isoc.org

(COMITÊ, 1999) COMITÊ GESTOR DA INTERNET NO BRASIL. *Sobre o Comitê Gestor.* Brasil, Maio, 1999.

(DEERING, 1998) DEERING, S. HINDEN, R. *Internet Protocol, Version 6 (IPv6) Specification.* Request for Comments : 2460. IETF. Dezembro, 1998.

(FNC, 1995) FNC, Federal Networking Council. *Definition of Internet.* FNC Resolution. EUA. 1995. Site http://www.fnc.gov/Internet_res.html

(GONCALVES, 1998) GONCALVES, Marcus; KITTY Niles. *IPv6 Networks.* McGraw-Hill Companies, INC. EUA, 1998.

(HINDEN, 1998_1) HINDEN, R. DEERING, S. *IP Version 6 Addressing Architecture.* Request for Comments : 2373. IETF, Julho.

1998.

(HOVEY, 1996) HOVEY, R; BRADNER, S. *The Organizations Involved in the IETF Standards Process*. Request For Comments : 2028. IETF,Outubro, 1996.

(IDGNOW, 1997) IDG NOW!. *Desempenho da Internet no Brasil*. IDG Computerworld do Brasil. Universo On-Line. Brasi. Setembro 1997. Site http://www.uol.com.br/idgnow/

(LEE, 2000) LEE, Thomas; DAVIES, Joseph. *Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference*. Microsoft Press. EUA. Março, 2000.

(LEINER, 1998) LEINER, Barry M; CERF. Vinton G.; POSTEL, Jon; et al. *A Brief History of the Internet. Internet Society* (ISOC). Fevereiro, 1998. Site http://www.isoc.org

(MALKING, 1994) MALKIN, G. The Tao of IETF - *A Guide for New Attendees of the Internet Enigneering Task Force*. Request For Comments : 1718. IETF, Novembro, 1994.

(TANENBAUM, 1996) TANENBAUM, Andrew S. *Computer Networks*, 3rd Edition. Upper Saddle River, New Jersey, EUA. 1996.