UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MAURÍLIO ALVES MARTINS DA COSTA

AVALIAÇÃO ANALÍTICA DE DESEMPENHO DO USO DO IPV6

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

Prof. Dr. Carlos Becker Westphall

Florianópolis, Maio de 2000

AVALIAÇÃO ANALÍTICA DE DESEMPENHO DO USO DO IPV6

Maurílio Alves Martins da Costa

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.

Carlos Becker Westphall, Dr.

Fernando A. O. Gauthier, Dr.

Banca Examinadora

Carlos Becker Westphall, Dr., Orientador

Ricardo Felipe Custodio, Dr., Co-Orientador

João Bosco Mangueira Sobral, Dr.

Vitório Bruno Mazzola, Dr.

" Jamais a natureza
Reuniu tanta beleza
Jamais algum poeta
Teve tanto, pra cantar!...
Num pedacinho de terra
Belezas sem par ! "

Hino de Florianópolis
Zininho

AGRADECIMENTOS

A Deus pela oportunidade oferecida a este simples mortal.

À família pelo apoio, pela consideração e pelos exemplos oferecidos.

Ao professor Westphall pela paciência e pela orientação durante todo o trabalho.

Ao professor Custódio que também dedicou seu tempo me co-orientando.

Aos professores da UFSC com quem convivi e muito aprendi.

Aos novos amigos aqui conquistados que, com certeza, fazem parte de um rico e vasto capítulo da história de minha vida.

A todos que de forma direta ou indireta torceram por mim.

Por fim agradeço a você que está lendo este trabalho.

Obrigado !

SUMÁR

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

ABREVIATURAS E SIGLAS

ARP	:	*Address Resolution Protocol.*
ARPANET	:	Rede de comunicação criada pela DARPA.
ATM	:	*Assynchronus Transfer Mode.*
B	:	Largura de banda do meio de transmissão.
BA	:	Bahia.
Br	:	Largura de banda do roteador.
CAT	:	Categoria de cabeamento.
CEFET	:	Centro Federal de Educação Tecnológica.
CIDR	:	*Classless InterDomain Routing.*
CSMA/CD	:	*Carrier-sense multiple access with collision detection.*
DARPA	:	*U.S. Defense Advanced Research Projects Agency.*
D	:	Tamanho em bytes de um datagrama.
DNS	:	*Domain Name System.*
Embratel	:	Empresa Brasileira de Telecomunicações.
FTP	:	*File Transfer Protocol.*
HTTP	:	*HyperText Transfer Protocol.*
IAB	:	*Internet Architecture Board.*
IANA	:	*Internet Assigned Number Authority.*
ICMP	:	*Internet Control Message Protocol.*
IEEE	:	*Institute of Eletrical and Eletronics Engineers.*
IESG	:	*Internet Engineering Steering Group.*
IETF	:	*Internet Engineering Task Force.*
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.*
L	:	Latência do meio de transmissão.
Lr	:	Latência do roteador.
MC	:	Ministério de Comunicações.
MCT	:	Ministério de Ciência e Tecnologia.
MIB	:	*Management Information Base.*
MIME	:	*Multipurpose Internet Mail Extensions.*
MIT	:	*Massachusetts Institute of Technology.*
MIME	:	*Multipurpose Internet Mail Extensions.*
Nc	:	Número de campos de um datagrama.
NGI	:	*Next Generation Internet.*
OSI	:	*Open Systems Interconection.*
POP	:	Ponto de Operação e Presença.
QoS	:	*Quality of Service.*
ReMAV	:	Redes Metropolitanas de Alta Velocidade.
RFC	:	*Request For Comments.*
RNP	:	Rede Nacional de Pesquisa.
RSVP	:	*Resource Reservation Protocol.*
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.
Tfe	:	Tempo do datagrama na fila de entrada do roteador.
Tfs	:	Tempo do datagrama na fila de saída do roteador.
Tp	:	Tempo de processamento de um datagrama no roteador.
Tpc	:	Tempo de processamento de cada campo do datagrama no roteador.
Tprop	:	Tempo de propagação do datagrama durante a sua transmissão.

UDP	:	*User Datagram Protocol.*
UFRJ	:	Universidade Federal do Rio de Janeiro.
UFSC	:	Universidade Federal de Santa Catarina.
UNICAMP	:	Universidade Estadual de Campinas.
UTP	:	*Unshield Twist Pair* (Par trançado não blindado).
URL	:	*Uniform Resource Locator.*
WWW	:	*World Wide Web.*

RESUMO

Uma nova implementação do Internet Protocolo (IP) foi recomendada pelo IETF (*Internet Engineering Task Force*). Esta nova versão, o IPv6, irá substituir aos poucos a versão corrente, o IPv4. Mas antes desta troca ocorrer, o IPv6 deve apresentar um desempenho de transmissão de dados pelo menos igual ao seu predecessor. Este trabalho apresenta uma avaliação analítica de desempenho do IPv6, comparando-o com o desempenho do IPv4.

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 de desempenho relativa à comunicação de datagramas num meio físico com roteadores no caminho.

O objetivo deste trabalho é realizar uma avaliação analítica de desempenho do uso do IPv6 levando em consideração a comunicação entre duas interfaces através de uma estrutura com vários meios físicos de transmissão, interligados através de equipamentos roteadores. Para tal foi implementada uma rede IPv6 no Laboratório do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, com três estações, onde cada estação pode comunicar com uma outra através de uma estação roteadora de datagramas.

ABSTRACT

A new implementation of the Internet Protocol (IP) was recommended by IETF (*Internet Engineering Task Force*). This new version of the Internet Protocol, the IPv6, will eventually replace the current version. Before that change can take place, the IPv6 must be able to show a data transmission performance at least as well as their predecessors. Within this context, this work presents a analytical valuation of the IPv6 performance making comparative concerning the performance of IPv4.

The Internet Protocol version 6 was developed to attend the Internet necessities and presents the solutions to the missing address, routing tables expansion problems and security issues. It is a new protocol that is not widely used, what justifies the performance analysis related to datagram communications in a physical middle with routers presences.

The objective of this work is to carry through an analytical evaluation of performance of the IPv6 use in the communication among two interfaces through a structure with some physical layer elements of transmission, linked through routers-equipments. Within this context a IPv6 network was implemented in the Laboratório do Curso de Pós-Graduação em Ciência da Computação of the Universidade Federal de Santa Catarina.

1. INTRODUÇÃO

A Internet está causando uma mudança de comportamento no mundo. Apesar de seu uso crescente e estratégico, os protocolos de comunicação que ela utiliza para trafegar os dados ainda são objetos de críticas. Essas críticas vão desde a lentidão nos *backbones* à insegurança da transmissão dos dados, passando por questões de baixo desempenho na propagação de datagramas e da falta de mecanismos de gerência da qualidade de serviço.

Segundo ***Latif Ladid***, presidente do *IPv6 Forum* em [MCG99] *"o sucesso do desenvolvimento da Internet como uma plataforma de negócios depende de torná-la um ambiente seguro e robusto"*.

Muitos destes problemas estão sendo resolvidos com a atualização do código do protocolo de rede responsável pela entrega do datagrama no destino da comunicação, o protocolo IP em sua versão 4.0. Essa atualização passa pela incorporação de recursos não planejados na versão original, como o protocolo de segurança *IPSec* [ATK98] ou o protocolo de gerência de banda passante RSVP [GON98].

Uma solução sugerida pelos órgãos regulamentares da Internet é a atualização completa do protocolo de rede da arquitetura utilizada pela Internet através da implementação do IPv6, um protocolo moderno capaz de superar os problemas existentes na atual versão, trazer novos conceitos e novas técnicas que visem um melhor desempenho da Internet como um todo.

O protocolo IPv6 já é uma realidade, ainda que muitas das implementações se encontrem em fase experimental. Com ele é possível endereçar muito mais interfaces de

redes, já que o campo de endereçamento possui 128 bits, contra os 32 do IPv4. Também é possível associar criptografia e autenticação aos dados, sem que para isso se tenha que encapsular todo o datagrama ou utilizar um protocolo extra, sem nenhuma integração com o IP, dentre outras possibilidades. Em um artigo para a *Network World Fusion*, ***Carolyn Marsan***, *[MAR99],* descreve as características do IPv6 da seguinte forma :

> *" IPv6 supports 128-bit addresses, while IPv4 supports 32-bit addresses. IPv6 can support a virtually unlimited number of Internet addresses, while IPv4 only supports a few billion. The extra addresses offered by IPv6 are important for the development of Internet devices, such as phones and television set-top boxes, which will each require a unique address in order to be accessed over the 'Net."*

Além de novas capacidades, o IPv6 possui mecanismos que permite a sua integração como o IPv4, possibilitando uma transição sem muitos traumas para o usuário a um custo baixo, já que ela pode ser feita por partes, sem a necessidade de parar toda a rede. E uma vez convertida a rede corporativa, ainda assim, é possível integra-la com a rede IPv4 através de técnicas que transportam o datagrama IPv6 via IPv4 ou permitindo a existência de uma camada dupla com ambos os protocolos ativos [BOZ98].

O projeto inicial de desenvolvimento do protocolo determina um foco de atuação visando três principais áreas : **endereçamento**, **segurança** e **desempenho**. Porém o protocolo IPv6 ainda não tem sido muito explorado no que diz respeito à avaliação de seu desempenho quando comparado com as outras áreas. Isto se deve, em parte, a uma política de primeiro desenvolver e colocar em funcionamento uma tecnologia para depois, então, começar a fazer refinamentos visando otimizar o seu funcionamento [GON98].

1.1. Objetivo

Este trabalho apresenta uma avaliação analítica de desempenho do IPv6 levando em consideração a comunicação entre duas interfaces através de uma estrutura com vários meios físicos de tecnologias diferentes e com um número indeterminado de caminhos possíveis. Essa avaliação se dará de forma analítica e utilizará medidas coletadas em um ambiente real.

É também objetivo deste trabalho, consolidar o aprendizado desenvolvido durante o curso de mestrado em Ciência da Computação na Universidade Federal de Santa Catarina.

1.1.1. Objetivos Gerais

- Avaliar os protocolos da camada de rede da arquitetura Internet;
- Conhecer o protocolo IPv6;
- Desenvolver a habilidade de configuração de protocolos de rede em diferentes sistemas operacionais;
- Desenvolver uma aplicação prática envolvendo protocolos de rede;
- Estudar novas tecnologias no contexto de redes de computadores.

1.1.2. Objetivos Específicos

- Analisar a real situação do protocolo IPv6 junto à comunidade de pesquisa e junto às corporações;
- Avaliar analiticamente a comunicação entre duas estações através de um meio de transmissão com roteamento de datagramas;
- Avaliar o uso do IPv6 numa rede real, comparando com o IPv4;
- Configurar uma rede IPv6.

1.2. Motivação

O protocolo IPv6 vem sendo explorado no noticiário público com sendo a solução para o problema da escassez de endereços a que está destinado a comunidade Internet devido a pouca quantidade de endereço disponibilizado pelo IPv4. Nenhuma outra característica do IPv6 é explorada, levando aos leitores a falsa impressão de que atualizando o protocolo IP da rede, passando de IPv4 para IPv6, ele não terá nenhum problema a mais e de que os protocolos são compatíveis entre si.

Uma melhor pesquisa mostra que não é bem assim. Primeiro que já existem mecanismos para utilizar melhor os endereços IPv4 [BAR93] e depois pode-se ver que as mudanças são mais profundas envolvendo uma modificação na estrutura de endereço que vai além de apenas aumentar o número de bits representativos para endereçamento [HIN98].

Assim novos questionamentos a respeito da arquitetura do protocolo foram surgindo, incluindo a curiosidade de saber como seria o desempenho do IPv6 em uma rede real. A aquisição de um conhecimento mais profundo a respeito deste novo protocolo serviu como a principal motivação para o desenvolvimento deste trabalho.

Existe, também, uma grande movimentação dentro das grandes empresas que trabalham com equipamentos de rede e sistemas operacionais indicando a implementação de soluções que atendam a esse novo protocolo. Alguns sistemas operacionais como o *AIX* da *IBM* e o *Solaris* da *SUN Microsystems*, possuem a pilha de protocolos TCP/IPv6 implementada já na versão pré-instalada, devendo ao usuário apenas ativá-la, se assim desejar. A *Microsoft Co.* já disponibilizou sua versão experimental para o público e já expressou seu interesse em disponibilizar uma versão para funcionar com o seu novo sistema operacional o *Windows 2000* [MAR00]. Vale aqui observar que o material de estudos do *Microsoft Windows 2000* possui uma sessão voltada para o IPv6, trazendo informações sobre sua configuração e endereçamento [LEE00].

Outra fonte de motivação foi o fato de que não existe um guia sistemático de instalação do protocolo IPv6 que explicasse todos os passos para se conseguir instalar e imediatamente utilizar os recursos deste protocolo. Existem alguns como o apresentado em [BIE00] mas que exigem um grau de conhecimento do sistema operacional utilizado, no caso o *Linux*, que pode inviabilizar a instalação para usuários inexperientes na sua utilização.

1.3. Trabalhos Correlatos

Nesta sessão são apresentados os trabalhos já publicados que foram relevantes na composição desta dissertação. Todos os trabalhos são referenciados no capítulo de referências bibliográficas e durante toda a dissertação.

- [BOZ98]
  Este é o primeiro trabalho voltado para o protocolo de rede IPv6 realizado dentro da Universidade Federal de Santa Catarina. Aqui foi realizado um trabalho de fundamentação de todo o protocolo IPv6.

  Ele se constituiu na primeira fonte de consulta para a realização deste trabalho e como ponto de partida para buscar outros trabalhos a respeito do IPv6.

- [BJO98]
  Neste trabalho, o autor apresenta uma metodologia para implementação de uma rede IPv6 no *Linux*, a partir desta rede ele realiza medidas do desempenho do IPv6 para alguns serviços disponíveis na época, enfatizando a ligação ao *backbone* IPv6 mundial *6Bone*.

- [COS99]
  Dissertação de mestrado defendida na Universidade Federal de Santa Catarina, envolvendo avaliação analítica que é utilizada como a referência para a avaliação analítica utilizada neste trabalho.

- [GUR99]
  Este artigo refere-se a um trabalho de comparação de desempenho do IPv4 e o IPv6 realizado no âmbito do Núcleo de Processamento de Dados da Universidade Federal de Santa Catarina.

- [OLI99]
  Apesar de seu tópico principal não se constituir em objeto de estudo nesta dissertação, o referido trabalho foi de grande valia para o entendimento de alguns aspectos referentes ao IPv6, principalmente no que diz respeito a segurança e mobilidade.

1.4. Estado da Arte

O protocolo IPv6 está sendo utilizado na maioria das vezes para testes em redes experimentais, mas já existem algumas iniciativas de utilização deste protocolo em aplicações e serviços para usuários finais.

No Japão, a *NTT Communications*, empresa do ramo de telecomunicações, está oferecendo desde o dia 20 de Março do ano 2000, serviços de Internet para o usuário final em IPv6 através de *backbone* próprio [MAR00_2]. No início de 2000 foi anunciada a utilização do IPv6 como o protocolo utilizado em vídeo conferência entre os EUA e o Japão.

O protocolo IPv6 já começa a ser anunciado em congressos como o "The 2nd Annual Global IP Summit 2000" a ser realizado em Maio na Itália e que conta com o apoio de grandes empresas de telecomunicações e organizações como o ATM Forum, IPv6 Forum e IETF. Neste congresso está programado uma sessão para apresentação e

discussão do IPv6, apresentando conceitos iniciais, técnicas de migração do IPv4 para o IPv6 e discussões sobre o impacto deste protocolo.

No Brasil existem vários estudos ocorrendo dentro de universidades onde se destacam a UNICAMP, a UFRJ, o CEFET-BA e a UFSC.

1.5. Estrutura da Dissertação

Esta dissertação está estruturada da seguinte forma :

No capítulo 2 é apresentado uma contextualização histórica da Internet, desde sua criação até os dias atuais, com ênfase na apresentação de seus órgãos regulamentadores, inclusive o que atua no Brasil. Neste capítulo é realizado um apanhado geral a respeito da Internet, com uma introdução histórica que vai das primeiras idéias lançadas no *Massachusetts Institute of Technology* até o seu último grande marco significativo que foi a criação da *World Wide Web*. Também é apresentada a Internet 2, um projeto de redes de alta velocidade voltada para aplicações em tempo real envolvendo multimídia.

O capítulo 3 apresenta a arquitetura de rede da Internet, também chamada de protocolo TCP/IP. Neste capítulo é mostrada a estrutura em camadas deste protocolo e, posteriormente, é feito um estudo mais específico da camada Internet, onde são, então, estudos os protocolos IPv4 e o IPv6.

No capítulo 4 é apresentada a configuração da rede local IPv6 criada no Laboratório do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina com os dados coletados nela que serão utilizados para a avaliação analítica proposta.

No capítulo 5 é feito o estudo dos aspectos de desempenho do IPv6, envolvendo a avaliação analítica do desempenho deste protocolo, focalizando o tráfego no meio físico de transmissão e o caminho percorrido pelo datagrama através dos

roteadores, apresentando avaliação específica para o IPv6. Por fim, é apresentada a avaliação de desempenho do uso do IPv6 baseada em um ambiente real.

O capítulo 6 apresenta a conclusão final da dissertação, onde são vistos : um estudo sobre as dificuldades apresentadas durante a realização de todo o trabalho, um cenário de perspectivas futuras e sugestões de tópicos para trabalhos futuros, seguindo a mesma linha de pesquisa.

O Anexo 1 apresenta a metodologia utilizada na configuração do ambiente de rede IPv6 implementado no Laboratório do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina. São apresentadas metodologias para dois sistemas operacionais, o *Linux RedHat 6.1* e o *Microsoft Windows NT 4.0 WorkStation*.

O Anexo 2 apresenta os dados coletados nos testes realizados na rede IPv6. São listados todos os dados coletados por tipo de datagrama e por carga utilizada.

2. A INTERNET

2.1. Considerações Iniciais

Neste capítulo é realizado um apanhado geral a respeito da Internet, com uma introdução histórica indo das primeiras idéias lançadas no *Massachusetts Institute of Technology* até o seu último grande marco significativo que foi a criação da *World Wide Web*. Então é apresentado, a título de ilustração, sem devidos aprofundamentos tecnológicos, a Internet 2 . A Internet 2 é um projeto de redes de alta velocidades voltadas para aplicações de tempo real envolvendo multimídia.

Por fim existe um tópico em que são apresentados os órgãos regulamentadores da Internet. Esses órgãos interagem entre si de modo a organizar e fazer da Internet um organismo sempre em evolução.

Este capítulo tem como função trazer informações que quase sempre são omitidas nos documentos e artigos publicados a respeito da Internet, visando, assim, um público que está ainda iniciando os primeiros contatos com esta tecnologia, informando de onde ela veio, qual a sua situação atual, quem estipula o que pode ou não ser suportado e por fim quem a regulamenta.

2.2. Histórico

O projeto da Internet teve o 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 para investigar novas técnicas e tecnologias para a viabilização da troca de pacotes de dados entre várias redes de computadores de diferentes arquiteturas [CER98]. O objetivo era desenvolver protocolos de comunicação para permitir que computadores em uma rede se comuniquem de forma transparente com qualquer outro computador de uma outra rede [TAN96]. Desse projeto originou-se a rede ARPANET.

Um documento da *Internet Society*, órgão de regulamentação da Internet, [LEI98], indica ***J. C. R. Licklider***, um pesquisador do MIT, 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 aprovou uma resolução definindo o termo Internet. Esta definição foi desenvolvida em consulta com membros da Internet e comunidades de direitos da propriedade intelectual e diz o seguinte [FNC95] :

> *" 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 subsequentes extensões; (ii) é capaz de suportar comunicações usando o Transmission Control Protocol/Internet Protocol (TCP/IP) ou suas subsequentes 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, que permitia a conexão entre minicomputadores chamados de IMP (*Interface Message Processors*). Este protocolo era sem conexão e transformava as mensagens em pequenos pacotes para serem enviados pela rede de forma independente [TAN96]. Em 1974 ***Vinton Cerf*** e ***Robert Kahn*** propuseram um modelo de protocolos 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 1983 todas as máquinas da ARPANET foram obrigadas a utilizar o TCP/IP que fora, então, reconhecido como o padrão da comunicação na Internet.

O principal uso da Internet era a troca de arquivos e mensagens entre seus usuários sendo o Telnet – serviço de acesso remoto -, o FTP – serviço de troca de arquivos e o *e-mail* – serviço de correio eletrônico- os serviços mais comuns. O ponto culminante para o seu sucesso foi o surgimento da WWW (*World Wide Web*) em 1991, fazendo com que o número de computadores ligados a Internet saltasse de 313.000 no final de 1990 para 2.056.000 em 1993 [BOZ98], chegando a mais de 50.000.000 no ano de 1997 [IDG97].

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

2.3. A Internet 2

A Internet 2 é uma iniciativa norte-americana, voltada para o desenvolvimento de tecnologias e aplicações avançadas de redes Internet para a comunidade acadêmica, de pesquisa e comercial. Esta iniciativa visa o desenvolvimento de novas aplicações como telemedicina, bibliotecas digitais, laboratórios virtuais, dentre outras que não são viáveis com a tecnologia Internet atual.

Não há uma linha de trabalho única e pré-determinada que oriente as pesquisas das novas possibilidades de aplicações que estão sendo desenvolvidas no projeto da Internet 2. Ainda há muito a ser pesquisado sobre a necessidade dos usuários e o potencial das tecnologias para redes de alto desempenho. De uma forma geral, não se

conhece ainda o limite do que é tecnicamente possível. Pode-se dizer, então, que o foco principal do Internet 2 reside no desenvolvimento de aplicações avançadas com uso intensivo de tecnologias multimídia em tempo real.

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 faz parte de um projeto maior, patrocinado pelo governo norte-americano e diretamente ligado à Presidência da República, o NGI – *Next Generation Internet* – cujo objetivo é o desenvolvimento de tecnologias de rede de última geração, tendo como foco inicial a pesquisa, o desenvolvimento, a formação de recursos humanos, bem como a experimentação das tecnologias necessárias para o desenvolvimento de novos tipos de serviços de rede que garantam transações seguras e alto nível de qualidade.

No Brasil existe um projeto viabilizado pela RNP – Rede Nacional de Pesquisa – chamado "Projetos de Redes Metropolitanas de Alta Velocidade", mais conhecido pela sigla ReMAV, que tem o objetivo de promover, em diversas regiões do país, a criação de infra-estrutura e serviços de redes de alta velocidade.

O projeto ReMAV deverá promover a integração, em nível nacional, de todas as redes metropolitanas de alto desempenho, formando o primeiro estágio do backbone nacional de alta velocidade, o RNP2. Neste mesmo momento, planeja-se disponibilizar conexões de alta velocidade para a Internet2, nos Estados Unidos, permitindo que as 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.

Maiores informações sobre a Internet 2 e o projeto ReMAV podem ser conseguidos no site da RNP, http://www.rnp.br .

2.4. Órgãos Regulamentadores

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 à 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 [MAL94] :

- 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 [HOV96]. O principal propósito da ISOC, segundo [HOV96] 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 [HOV96] :

- 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 System*);
- 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 seus estudos tem alguma aplicabilidade eles são repassados para o IETF que irá adequá-los e disponibilizá-los para a comunidade Internet mundial [HOV96].

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 é referenciado em RFCs com o título "*Assigned Numbers*".

2.4.6. Comitê Gestor Internet / 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 [COM99] :

- 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.

2.5. Conclusão

De origem militar, inspirada nos conflitos internacionais da chamada era da "Gerra-Fria", a Internet foi evoluindo com o auxilio das instituições acadêmicas até possuir a estrutura dos dias atuais. Atualmente ela deixou de ser uma tecnologia de uso

específico para passar a ser uma das principais tecnologia de transmissão de sinais de dados, tanto dados simples quanto multimídia, sendo utilizada, inclusive, como tecnologia de comunicação em massa.

Neste capítulo foi apresentada a evolução da Internet desde sua concepção teórica em 1962, com *J. C. R. Licklider*, até os dias atuais onde verificamos a evolução do Brasil e sua rede de pesquisa neste campo. A Internet 2 foi introduzida sem muito detalhamento, mas indicando o caminho para o qual a Internet poderá se migrar.

3. A ARQUITETURA DE REDE DA INTERNET

3.1. Considerações Iniciais

Neste capítulo é explorado informações a respeito da arquitetura de rede da Internet. Uma visão geral é apresentada, tendo como objetivo mostrar a camada de atuação do protocolo IP. O protocolo IP é o foco do estudo, sendo apresentado com características da versão atualmente em uso, a versão 4.0.

Em um tópico especial é feito o estudo do protocolo IPv6, este sim, objeto de estudo da dissertação. O estudo é introdutório e não abrange todos os pontos do protocolo, o que pode ser feito através das referências citadas no próprio texto.

3.2. A Arquitetura de Protocolos da Internet

A arquitetura de rede Internet é um conjunto de protocolos desenvolvidos para permitir que os computadores comuniquem entre si em uma rede. Nesse conjunto de protocolos estão inclusos padrões que especificam os detalhes de como ocorre a comunicação entre os computadores, assim como convenções e normas para rotear o tráfego gerado por essa comunicação. O nome TCP/IP é também utilizado para descrever esta arquitetura devido a seus dois protocolos mais importantes o TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*), porém existem mais protocolos que constituem essa família.

Esta arquitetura é constituída de quatro camadas que interagem entre si tornando-se flexível e adaptável à mudanças. As quatros 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.

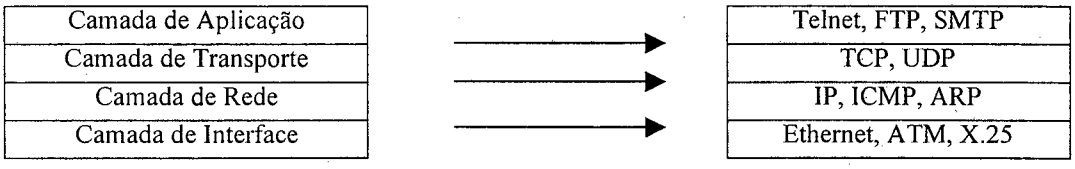

FIGURA 1 : CAMADAS DA ARQUITETURA DE REDE INTERNET

A camada de aplicação contém os protocolos de alto nível que são diretamente utilizados pelos programas que interagem com os usuários.

A camada de transporte é a camada que controla a conversação entre as aplicações envolvidas em uma comunicação inter-redes. Nessa camada são definidos os protocolos para estruturação e entrega de mensagens, além da verificação de erros de transmissão de dados. A comunicação pode ser feita de forma confiável ou não, dependendo do protocolo a ser utilizado.

A camada de rede determina a interconexão entre as redes da Internet. Ela é a responsável pelo roteamento dos datagramas – unidades de dados da camada – entre os *hosts*, com a função de encontrar o caminho mais curto e confiável entres os computadores envolvidos na comunicação. Essa camada não é orientada a conexão, não oferece tratamento de erros para os dados e nem controle de fluxo.

A camada de interface, também camada de abstração de hardware, tem como função principal a interface da camada de rede da arquitetura Internet com os diversos tipos de padrões para redes (X.25, ATM, Ethernet, Token Ring, Frame Relay, entre outras).

3.3. O Protocolo Internet (IP)

O protocolo IP atua na camada de rede da arquitetura de rede da Internet e sua unidade de informação chama-se datagrama. Ele não é orientado à conexão, assim 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. Se um datagrama se perder ou for alterado por alguma interferência em seu caminho não há um mecanismo de retransmissão para os mesmos. Além do mais, se um datagrama não encontrar o seu destino ou ficar muito tempo à sua procura ele é simplesmente descartado [BOZ98].

A comunicação com IP funciona assim : 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 envia-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. 2 apresenta a estrutura do datagrama do protocolo IPv4.

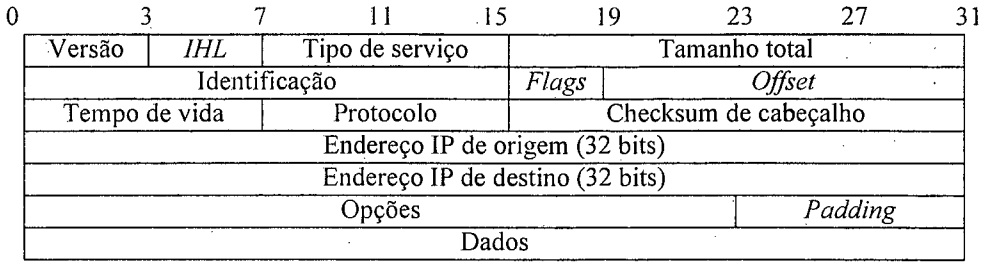

FIGURA 2 : A ESTRUTURA DO DATAGRAMA PROTOCOLO IPV4

Este protocolo foi projetado em 1978, sem levar em consideração os avanços conquistados pela Internet no seu atual estágio, assim alguns problemas surgiram 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 minimizar esse problema foram criados mecanismos como por exemplo o CIDR (*Classless InterDomain Routing*), [BAR93], que tem como proposta o fim das classes de endereçamento IP e a distribuição de endereços a partir de regiões geográficas – domínios.

Um outro problema, ainda relacionado com o endereçamento, é o aumento do tamanho das tabelas geradas pelo serviço de DNS devido ao aumento de sites e servidores conectados na Internet.

Outros problemas dizem respeito ao desempenho em redes de alta velocidade, como as redes ATM, e em redes de baixa velocidade, bem como a capacidade de gerenciar requisitos de medição e manutenção da qualidade do serviço (*QoS*) 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.

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 que posteriormente foi regulamentado com o nome de IPv6.

3.4. O Protocolo Internet versão 6

O IPv6, também conhecido como IPng (*Internet Protocol Next Generation*), é a nova versão do protocolo IP que foi projetado como uma evolução do IPv4, para ser executado em redes de altas performances como a ATM (*Assinchronous Transfer Mode*) e ao mesmo tempo se manter eficiente em redes de baixas performance como as redes sem fio.

Em Janeiro de 1995 foi emitida a RFC 1752 que apresentava as recomendações para o IPv6. Os principais objetivos a serem alcançados com o protocolo IPv6 são [BRA95] :

- Aceitar bilhões de *hosts* – através da expansão do espaço de endereçamento e uma hierarquia mais versátil, reduzindo a tabela de roteamento;
- criar um protocolo simples e passível de expansão;
- oferecer segurança incluindo autenticação e privacidade;
- oferecer suporte a mecanismos de controle de qualidade de serviço;
- permitir *multicast*, através da especificação de escopos;
- permitir auto configuração e auto reconhecimento de hosts;
- oferecer suporte a comunicação sem fio;
- oferecer suporte à versão anterior do protocolo IP.

A Fig. 3 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.

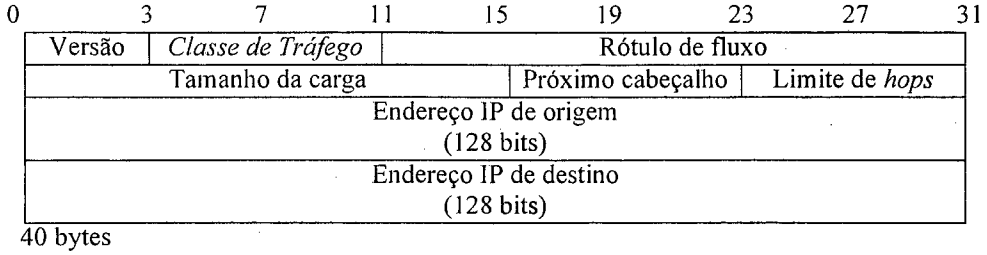

FIGURA 3 : A ESTRUTURA DO DATAGRAMA PROTOCOLO IPV6

Ter um cabeçalho básico fixo e outros extras aprimora o desempenho do IPv6 reduzindo o tráfego junto ao datagrama uma vez que devido ao aumento do tamanho dos endereços IP um datagrama básico, sem dados e cabeçalhos de extensão, tem 40 bytes.

Os grupos de padronização sugerem que os cabeçalhos sejam criados em tamanhos múltiplos de 8 bits, devido a questões de performance, conforme a Fig. 4. Os cabeçalhos de extensão já definidos são [BRA95] :

- *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.

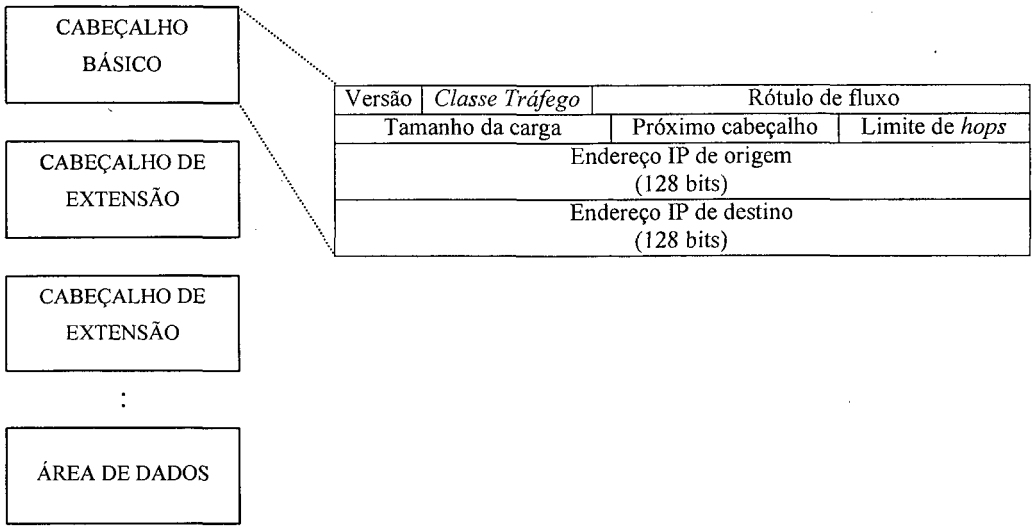

FIGURA 4 : DATAGRAMA PROTOCOLO IPV6 COM OS CABEÇALHOS DE EXTENSÃO

3.5. Propósitos do projeto do IPv6

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.

3.5.1. Aspectos do endereçamento IPv6

A estrutura de endereçamento do IPv6 permite mais de $340x10^{34}$ endereços para interfaces na rede contra os apenas 4×10^9 possíveis com o IPv4. Isto é possível devido a mudança de tamanho, em bits, do endereço IP que passou a ser representado por 128 bits distribuídos seqüencialmente, sem o uso de classes como no IPv4. Além do mais o IPv6 é auto-configurável, permitindo 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 subrede, 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 [DEE98].

3.5.2. Aspectos de segurança

O *IETF* organizou um grupo de trabalho de nome *IP Security* com o objetivo de desenvolver mecanismos que forneçam 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* [ATK98].

O *IPSec* provê 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 [ATK98]. 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.

3.5.3. Aspectos de 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 consequentemente 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 [GON98].

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 interfaces e o caminho percorrido pelos datagramas.

3.6. Conclusão

A arquitetura de redes da Internet é uma estrutura de protocolos dividida em camadas, onde cada camada tem sua função específica e elas comunicam entre si através de unidades de dados que é passada de uma camada superior à camada imediatamente inferior ou vice-versa.

Dentre os protocolos correspondentes de cada camada, o protocolo IP é que desempenha as atividades mais importantes de toda a arquitetura. O IP tem como função a fragmentação/desfragmentação e o roteamento de unidades de dados através dos equipamentos roteadores existentes no caminho a ser seguido até o destino da comunicação.

O IP atualmente se encontra na versão 4.0 que foi apresentada em 1978 e possui problemas para ser utilizado nos dias atuais, dentre os quais destacam-se a baixa quantidade de endereços de interfaces oferecido, a não hierarquização dos endereços e a falta de recursos de segurança e de controle de qualidade de serviço para a transmissão dos dados. Devido a esses e outros problemas, além da necessidade de inclusão de novos requisitos tecnológicos a esses protocolo, está sendo criado uma nova versão do IP, o IPv6.

Informações mais detalhadas a respeito do protocolo IPv6 podem ser obtidas em [HUI97], [DEE98], [BRA95], [BOZ98], [GON98] e [HIN98]

4. A REDE LOCAL IPV6 UTILIZADA NA COLETA DOS DADOS

4.1. Considerações Iniciais

Para avaliar o desempenho do uso do protocolo IPv6 é necessário que haja um ambiente para realizar a coleta do dados a serem analisados. Neste capítulo é apresentada a configuração da rede local IPv6 criada no Laboratório do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina. Esta rede é experimental e utilizou-se de equipamentos e recursos disponíveis no próprio laboratório.

Também são apresentados, neste capítulo, os dados coletados na rede configurada e que serão utilizados para a avaliação analítica proposta. Os dados se referem ao tempo de propagação de um datagrama em diversas situações e com variações no tamanho do mesmo.

4.2. Características da Rede Local IPv6

A rede utilizada para coletar os dados utilizados na avaliação analítica do desempenho do uso do IPv6 consiste em três computadores interligados entre si através cabos de par trançado categoria 5 (*UTP CAT 5*) com vazão máxima de 10 Mbits/segundo através do protocolo de transmissão *Ethernet*, conforme norma *IEEE 802.3*.

Na fase de testes os microcomputadores da rede estavam interligados através de um hub, que por sua vez servia a todos os outros elementos de rede disponíveis no laboratório. Para a coleta dos dados o equipamento de interligação foi substituído, sendo utilizado um tipo especial configuração do cabeamento chamado configuração de pinagem cruzada, ou "*cross over*", como é mais comumente referido.

A razão de utilizar o cabo com pinagem cruzada se deve à necessidade de garantir um tráfego mais homogêneo entre os microcomputadores e eliminar o atraso no tempo de propagação do datagrama ocasionado pelo *hub* e/ou por colisões com outros datagramas de outras estações.

Cada microcomputador utilizado é considerado uma estação de trabalho específica da rede. Para efeitos da coleta de dados as estações receberam denominações referentes à função desempenhada, conforme ilustra a Figura 5. A Estação 1 é a estação emissora do datagrama a ser avaliado. A Estação 2 por conseguinte é a estação receptora.

Cada uma das estações está configurada em sub-redes distintas. Desta forma é necessário uma estação para desempenhar a função de ligação entre essas duas sub-redes. Esta estação é a Estação *Router* que ser caracteriza por possuir duas interfaces de rede. Cada interface de rede está em uma sub-rede distinta, de forma que possa haver o roteamento do datagrama de uma sub-rede a outra.

Vale ressaltar que a cada estação está associada uma função específica apenas para fins didáticos e dentro do contexto da coleta de dados, uma vez que qualquer uma das estações pode ser tanto emissora quanto receptora de datagramas. Quanto a função de roteamento, somente a estação Router pode executá-la.

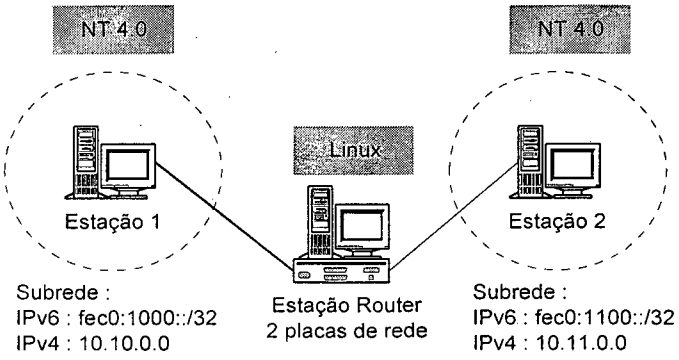

FIGURA 5 : TOPOLOGIA DA REDE

A Fig. 5 apresenta além da topologia de rede adota, informações a respeito de cada sistema operacional utilizado nas estações. A Estação 1 e a Estação 2 utilizam o sistema operacional *Microsoft Windows NT 4.0 WorkStation* com a pilha TCP/IPv4 e TCP/IPv6 ativadas. O NT 4.0 é um sistema operacional bastante difundido para uso corporativo e de fácil manipulação, a sua escolha se deu devido à fácil configuração da pilha TCP/IPv6, além da disponibilização de vários aplicativos de rede como *ping*, *traceroute* e *ttcp*.

A Estação *Router* está configurada com o sistema operacional *Linux* da distribuidora *RedHat* em sua versão 6.1. Esta versão vem com o *kernel* 2.2.12-20, que possui suporte ao IPv6. A escolha deste sistema operacional ocorreu devido à necessidade de se configurar um roteador para datagramas enviados pelo protocolo IPv6. Como o *Windows NT* ainda não possui esse suporte, era necessária uma outra alternativa. Além do mais era desejado um sistema operacional mais robusto para poder controlar a rede e gerenciar a coleta de dados para a avaliação.

Uma observação importante para o *Linux* é que a versão do *kernel*, o núcleo do sistema onde estão colocado os códigos principais ao funcionamento do sistema operacional, deve ser superior a 2.2.10, pois somente a partir desta versão é que o suporte ao IPv6 foi implementada.

Para maiores detalhes a respeito da configuração do protocolo IPv6 em cada um desses sistema operacional, consulte o Anexo 1. Nesta seção é apresentada uma

metodologia para a instalação da pilha TCP/IPv6 tanto no *Linux* quanto no *Windows NT 4.0*.

Na Fig. 5 há uma indicação das sub-redes criadas. Cada sub-rede possui duas interfaces de redes associadas, uma para cada estação inclusa na sub-rede e duas paraa Estação *Router*. Para cada interface de rede é associado um único endereço IPv6. Lembrando que no IPv6 é possível associar mais de um endereço a uma interface de rede, criando assim as pseudo-interfaces.

Uma sub-rede é caracterizada por seu prefixo. Na rede criada uma sub-rede possui o prefixo **fec0:1000::/32** e a outra possui o prefixo **fec0:1100::/32**. Como indicado em [HIN98] o prefixo é seguido pela indicação do número de bits válidos para a determinação da sub-rede. Uma confusão pode ser feita em relação aos prefixos devido à falta de experiência no seu manuseio.

Quando uma interface de rede é configurada, o sistema de auto-configuração sugere um endereço no formato **fe80::/10**. Esse prefixo caracteriza a criação de um endereço *link-local* [HIN98]. Ser um endereço *link-local*, significa que ele é válido apenas dentro da sub-rede na qual ele foi criado. Este endereço não pode ser roteado e alcançar uma outra rede. Quando se deseja obter o roteamento de datagramas é necessário associar um outro endereço à interface de rede – não é preciso retirar o endereço *link-local*. O novo endereço associado à interface de rede deve seguir à política exposta em [HIN98] onde alguns prefixos são reservados a determinados propósitos. Um desses prefixos é o **fec0::** que é um endereço reservado para uso em intranets.

Ao endereço com o prefixo **fec0::** é permitido ser roteado dentro do ambiente de alcance da rede local, mas os endereços com esse prefixo não devem ser entendidos no *backbone* da Internet.

A Fig. 6 apresenta a topologia de endereços IPv6 adotada na rede aqui estudada.

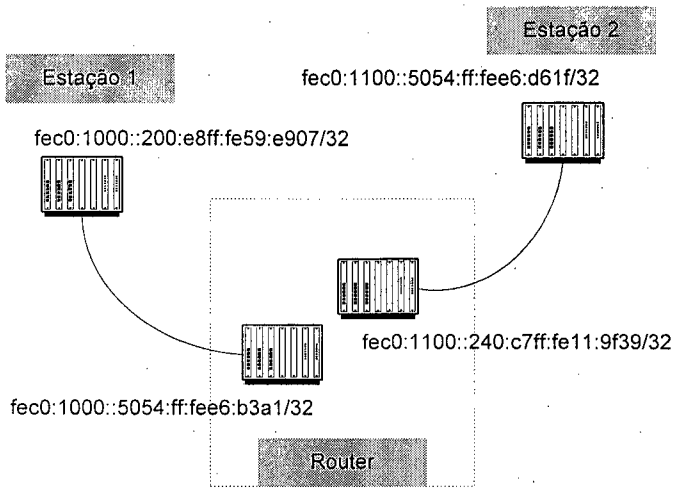

FIGURA 6 : TOPOLOGIA DE ENDEREÇOS IPV6

Com apresentado na Fig. 6, no caso da Estação 1 foi associado o endereço **fec0:1000::200:e8ff:fe59:e907/32**, para a Estação 2 foi associado o endereço **fec0:1100::5054:ff:fee6:d61f/32**. À Estação Router foram associados o endereço **fec0:1000::5054:ff:fee6:b3a1/32** para a interface de rede pertencente à sub-rede **fec0:1000::/32** e o endereço **fec0:1100::240:c7ff:fe11:9f39/32** para a interface pertencente à sub-rede **fec0::1100::/32**. Após o prefixo de identificação da sub-rede, pode ser colocado um número qualquer de acordo com a política de endereçamento própria, no caso da rede em questão foi colocado o endereço *ethernet* de cada interface de rede.

Ainda a respeito da pilha TCP/IPv6, nenhum cabeçalho de extensão foi associado ao protocolo IPv6 nesta implementação. Assim não foi feita nenhuma configuração referente à inclusão do *IPSec*, o protocolo de segurança e autenticação proposto pelo *IETF*, e nem configuração referente a inclusão do tunelamento de IPv6 sobre o IPv4.

4.3. Coletando os dados na Rede Local IPv6

Para a avaliação do desempenho do uso do IPv6 está sendo levado em conta o tempo de propagação apenas do datagrama IPv6, sem nenhum cabeçalho de extensão,

entre a Estação 1 e a Estação 2, através da Estação *Router*. Porém para fazer a avaliação é necessário haver um termo de comparação, para o qual seja utilizado o mesmo parâmetro tempo de propagação do datagrama entre a Estação 1 e a Estação 2, através da Estação *Router*. Este termo é o datagrama do protocolo IPv4.

Foram coletados os tempos em milissegundos da transmissão de datagramas entre a Estação 1 e a Estação *Router*, entre as duas interfaces da Estação *Router* e entre a Estação *Router* e a Estação 2. Para a coleta foi utilizado o aplicativo de rede ***ping*** que envia um datagrama com um tamanho predefinido através da rede e retorna o tempo gasto para o datagrama sair do emissor e retornar a ele.

Nas medidas aqui realizadas forma utilizados pacotes com tamanhos de 64 bytes, 750 bytes e 1500 bytes, de forma que possa avaliar o tempo de propagação para diferentes cargas. A escolha desse valores se deu baseado no valor máximo de quadro possível no meio físico. Como o meio é o Ethernet, o quadro máximo é de 1500 bytes, acima disso o quadro é fragmentado, o que acarreta um aumento do tempo de propagação de todo a informação, que desta vez estará em mais de um datagrama. O valor 750 bytes corresponde ao meio termo no tamanho do datagrama e o valor 64 bytes é o valor padrão sugerido pelo aplicativo de rede *ping*.

O ideal para a medida de desempenho é utilizar um aplicativo de rede implementado para essa função como ***ttcp***. Porém ao tentar fazer as medidas com esse aplicativo o sistema operacional ficava instável e paralisava, sendo necessário reinicializa-lo. Isso ocorreu para os testes com a opção IPv6 ativada, ou seja quando se desejava fazer medidas de desempenho para datagramas IPv6.

Devido a esse problemas foi escolhido fazer a medida com o aplicativo de rede ***ping***, que não tem a função de medir o desempenho de um datagrama, mas como ele retorna o tempo gasto para o datagrama ir e voltar a um endereço válido, esse valor seria suficiente para a avaliação proposta neste trabalho. Deve-se ressaltar que o problema de paralisação do sistema operacional também ocorreu com esse aplicativo, quando foram feitas medidas para os datagramas IPv6, a mensagem enviada pelo sistema operacional

indicava uma inconsistência de pilha de execução do mesmo. Com o aplicativo ***ping*** é mais fácil contornar esse problema, tomando apenas algumas medições por vez, ao invés de todo o conjunto total de medições desejadas. Assim foram feitas 15 medições por vez para os datagramas IPv6, até alcançar um total de 100 medições. Os dados coletados são apresentados no Anexo 2.

A Fig. 7 representa graficamente os dados recolhidos nas medidas realizadas entre a Estação 1 e a Estação *Router*, dentro da mesma sub-rede, para o protocolo IPv4.

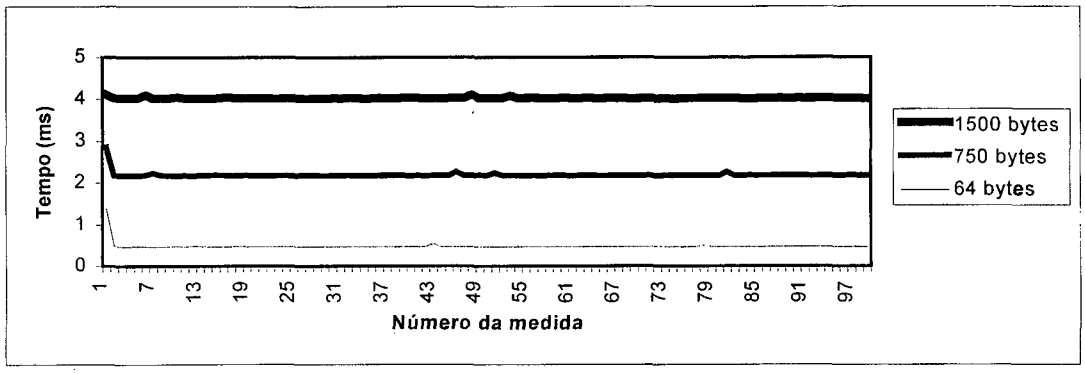

FIGURA 7 : MEDIDAS REALIZADAS ENTRE A ESTAÇÃO 1 E A ESTAÇÃO *ROUTER* PARA IPV4

A Fig. 8 representa graficamente os dados recolhidos nas medidas realizadas entre a Estação 1 e a Estação *Router*, dentro da mesma sub-rede, para o protocolo IPv6.

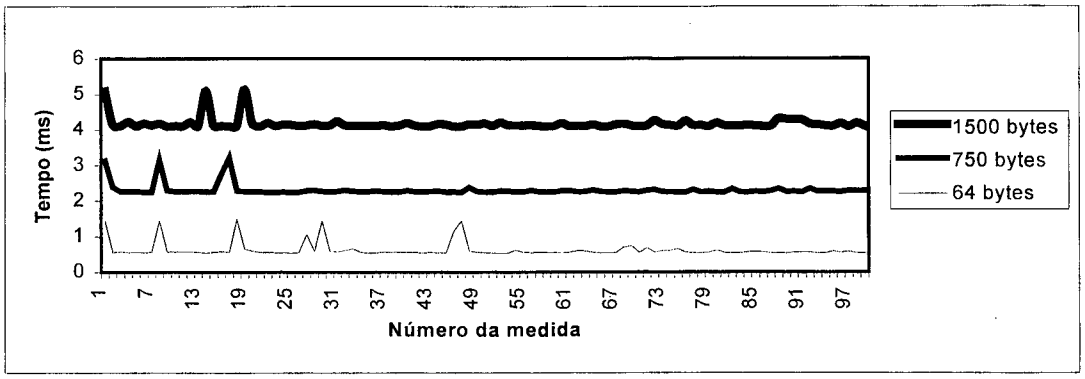

FIGURA 8 : MEDIDAS REALIZADAS ENTRE A ESTAÇÃO 1 E A ESTAÇÃO *ROUTER* PARA IPV6

Alguns valores se destacam na observação do gráfico apresentado. Não foi realizado um estudo aprofundado para a determinação do motivo destes picos. Um dos motivos do aparecimento desses valores pode ser relativo à rede de testes, uma vez que existe uma certa uniformidade de suas ocorrências. O primeiro pico ocorre devido à contabilização do tempo de carga do aplicativo na memória primária do computador.

A Fig. 9 representa graficamente os dados recolhidos nas medidas realizadas na Estação *Router*, para o protocolo IPv4.

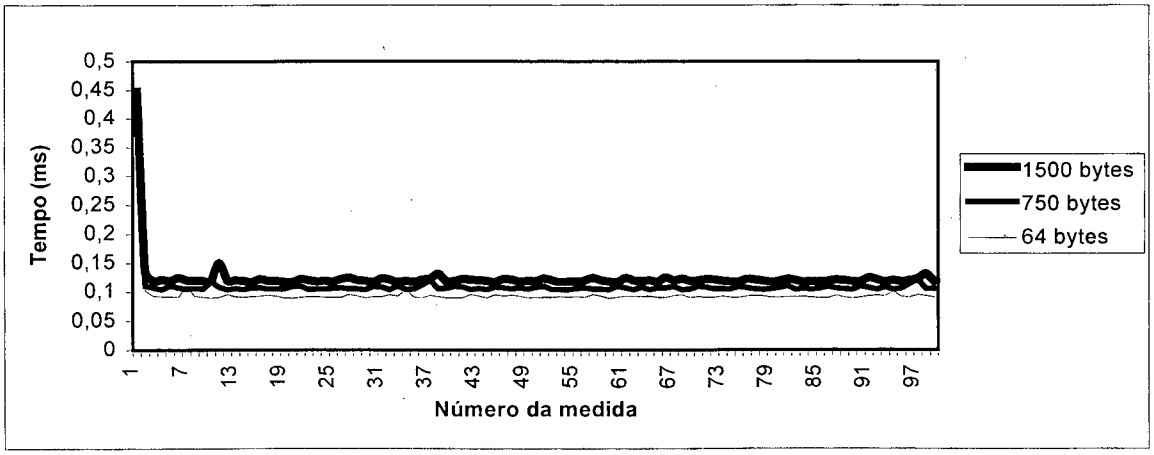

FIGURA 9 : MEDIDAS REALIZADAS NA ESTAÇÃO *ROUTER* PARA IPV4

A Fig. 10 representa graficamente os dados recolhidos nas medidas realizadas na Estação *Router*, para o protocolo IPv6.

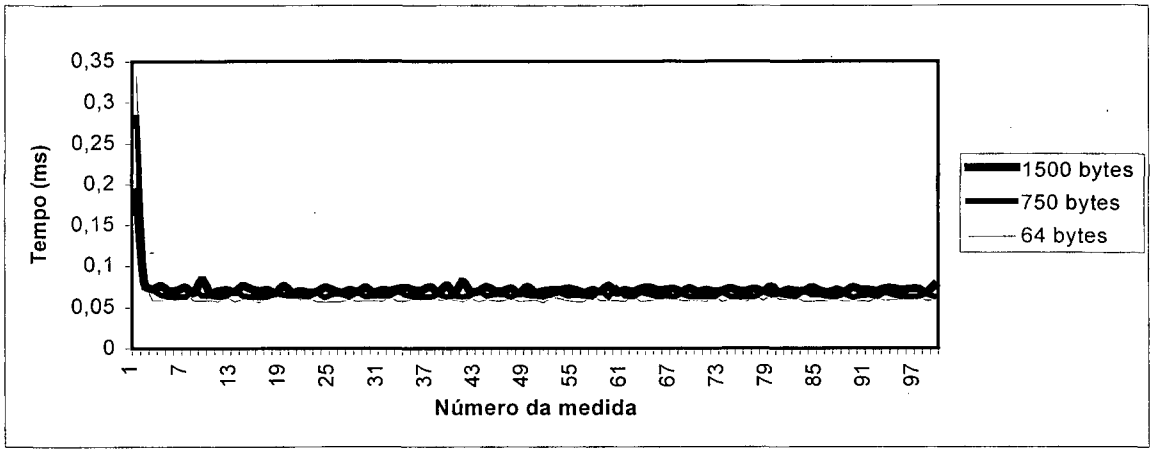

FIGURA 10 : MEDIDAS REALIZADAS NA ESTAÇÃO *ROUTER* PARA IPV6

A Fig. 11 representa graficamente os dados recolhidos nas medidas realizadas entre a Estação *Router* e a Estação 2, dentro da mesma sub-rede, para o protocolo IPv4.

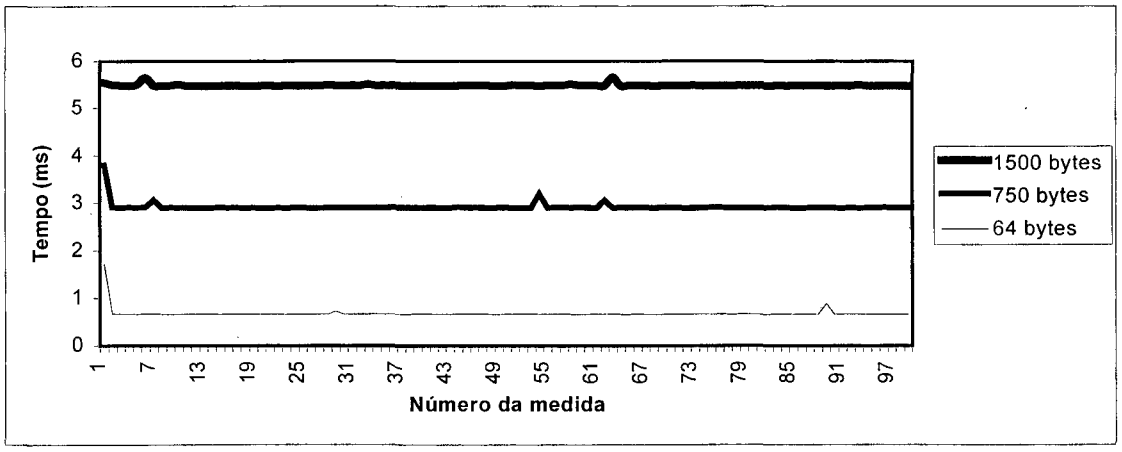

FIGURA 11 : MEDIDAS REALIZADAS ENTRE A ESTAÇÃO *ROUTER* E A ESTAÇÃO 2 PARA IPV4

A Fig. 12 representa graficamente os dados recolhidos nas medidas realizadas entre a Estação *Router* e a Estação 2, dentro da mesma sub-rede, para o protocolo IPv6.

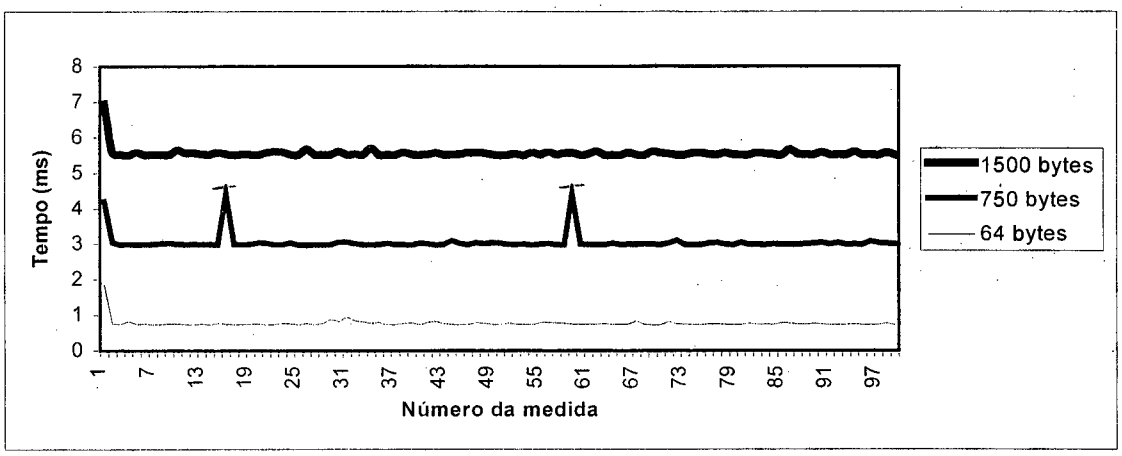

FIGURA 12 : MEDIDAS REALIZADAS ENTRE A ESTAÇÃO *ROUTER* E A ESTAÇÃO 2 PARA IPV6

4.4. Conclusão

A implementação de uma rede que suporte o protocolo IPv6 ainda é uma tarefa árdua. O principal motivo dessa dificuldade é o fato de que as pilhas TCP/IPv6 estão em fase experimental de implementação, pelo menos as pilhas aqui implementadas, assim são necessárias modificações em arquivos de comandos poucos explorados.

Para estações clientes o novo protocolo tem se demonstrado bastante estável. Estas estações apenas ativam a pilha TCP/IPv6 e configuram um endereço, se o endereço for *link-local*, pode-se até mesmo aceitar o endereço oferecido pela serviço de auto-configuração. Se for utilizado um endereço *site-local*, ou outro válido na Internet, tem-se que criar um *script* para configurar esse endereço toda vez que a pilha for acionada, além de indicar o computador *gateway* para a sub-rede ao qual a estação pertence.

Já as estações servidoras, como a Estação *Router* aqui configurada, estas sim apresentam bastante instabilidade no funcionamento. Nesta implementação existiram problemas de várias naturezas que dificultaram o trabalho de tomada de valores.

A expectativa é que novas versões das pilhas TCP/IPv6 sejam colocada à disposição da comunidade com correções e com a apresentação de novas funcionalidades. Sendo a expectativa maior para que implementem as pilhas já com uma total integração com o sistema operacional utilizado, de forma a facilitar a configuração, retirando, por exemplo, a necessidade de se recompilar todo o *kernel* do produto. Essa tendência já pode ser verificada nas novas versões do sistema operacional **AIX** da *IBM* e no **Solaris** da *SUN Microsystem*.

Os valores aqui apresentados serão avaliados numa sessão a parte, portanto eles foram utilizados apenas para ilustração dos resultados obtidos ao final da implementação da rede IPv6.

5. AVALIAÇÃO ANALÍTICA DE DESEMPENHO DO USO DO IPV6

5.1. Considerações Iniciais

Neste capítulo é feito o estudo dos aspectos de desempenho do IPv6, envolvendo avaliações analíticas do desempenho deste protocolo, focalizando o tráfego no meio físico de transmissão e o caminho percorrido pelo datagrama através dos roteadores. Para tanto é realizada uma descrição matemática do tempo de propagação do datagrama durante a transmissão entre duas interfaces de comunicação.

Também é feita uma avaliação específica para o IPv6, considerando características particulares deste protocolo que irão influenciar no desempenho final da propagação do datagrama. Esta avaliação é baseada na descrição matemática apresentada no item anterior sendo indicado apenas o comportamento das variáveis envolvidas na avaliação para o caso específico do protocolo IPv6.

Por fim é apresentada a avaliação de desempenho do uso do IPv6 baseada em um ambiente real. Essa avaliação é realizada a partir dos dados coletados na rede IPv6 implementada no Laboratório do Curso de Pós-Graduação de Ciências da Computação da Universidade Federal de Santa Catarina. Estes dados estão apresentados no Anexo 2.

Neste último tópico é utilizada a comparação entre os resultados coletados para o datagrama IPv4 e os resultados coletados para o datagrama IPv6, apresentados em forma de gráficos.

5.2. Avaliação Analítica de Desempenho do Tempo de Propagação

Na análise de desempenho proposta são levadas em consideração as influências exercidas pelo meio de transmissão de dados e pelo roteador. As influências exercidas pela fonte geradora e receptoras finais do datagrama na Internet, as interfaces de rede no caso da rede IPv6 utilizada neste trabalho, são desconsideradas.

Como parâmetro de desempenho, esta análise visa o estudo do tempo de propagação do datagrama durante a sua transmissão (**Tprop**) que é o tempo em segundos requerido pelo datagrama para trafegar entre o equipamento emissor e o equipamento receptor de dados através do meio de transmissão utilizado. Os parâmetros considerados foram os seguintes :

Ao que diz respeito ao datagrama:

1 - Tamanho do datagrama (**D**) : Tamanho do datagrama em bits.
2 - Número de campos (**Nc**) : Número de campos do datagrama.

Em relação ao meio de transmissão:

1 - Largura de banda da rede (**B**) : Capacidade de transmissão do meio em bits/segundo.
2 - Latência do meio (**L**) : Tempo, em segundos, de atraso característico do meio.

Quanto ao roteador :

1 - Largura de banda do roteador (**Br**) : Capacidade de transmissão do meio em bits/segundo.
2 - Latência do roteador (**Lr**) : Tempo, em segundos, de atraso característico do roteador.

3 - Tempo na fila de entrada (**Tfe**) : Tempo, em segundos, que o datagrama fica na fila de entrada do roteador.

4 - Tempo na fila de saída (**Tfs**) : Tempo, em segundos, que o datagrama fica na fila de saída do roteador.

5 - Tempo de processamento (**Tp**) : Tempo, em segundos, necessário para processar as informações de cabeçalho do datagrama.

6 - Tempo de processamento de cada campo do datagrama (**Tpc**) : Tempo, em segundos, necessário para processar cada campo do datagrama.

O cenário para a determinação do tempo de propagação do datagrama (**Tprop**) durante a sua transmissão pode ser avaliado por partes, onde é determinado o tempo de propagação no meio de transmissão e o tempo de propagação no roteador.

Assim, de acordo com os parâmetros levantados, tem-se para o meio de transmissão que tempo de propagação do datagrama consiste no tempo característico do meio de transmissão adicionado do *throughput* da rede. O *throughput* é razão entre a quantidade de dados trafegando em um meio pela capacidade de transmissão desse meio.

Analiticamente temos :

$$\mathbf{Tprop(meio) = L + D/B} \qquad (1)$$

Onde :

(D/B) : é "*throughput*" do meio de transmissão, para cada datagrama.

Para o roteador temos que o tempo de propagação do datagrama corresponde a uma soma de tempos que envolve a latência característica do elemento roteador, o tempo que o datagrama fica na fila de espera para processamento, o tempo que o roteador leva processando o datagrama, além do throughput do roteador, já que o

datagrama transita internamente ao roteador, utilizando seu hardware como meio de transmissão. Analiticamente podemos escrever o tempo de propagação do datagrama em um roteador como sendo:

$$\mathbf{Tprop(roteador) = Lr + Tfe + Tfs + Tp + D/Br} \qquad (2)$$

Onde :

(D/Br) : é "*throughput*" do roteador, para cada datagrama.

O tempo de processamento do datagrama (**Tp**) pode ser refinando levando em consideração o tempo gasto no processamento de cada cabeçalho separadamente, já que algumas das informações do cabeçalho são para configuração de valores no próprio roteador.

O tempo de processamento do roteador (**Tp**) também é influenciado pela quantidade de campos a serem processados. De forma que quanto menos campos houverem, menor será o tempo de processamento para um datagrama. Portanto deve-se considerar esse fator com bastante cuidado, pois na análise deste tempo é que se encontra o ponto de otimização do tempo final de propagação do sinal, já que, normalmente, o tamanho de um datagrama (**D**) é constante, levando em consideração o preenchimento do campo de dados e a inexistência de cabeçalhos de extensões.

Assim temos o tempo de processamento do cabeçalho do datagrama (**Tp**) descrito da seguinte forma :

$$\mathbf{Tp = Nc * Tpc} \qquad (3)$$

O tempo de propagação do datagrama no roteador (**Tprop(roteador)**) é, então descrito analiticamente por :

$$\mathbf{Tprop(roteador) = Lr + Tfe + Tfs + (Nc * Tpc) + D/Br} \qquad (4)$$

Como conseqüência do levantamento analítico apresentado acima, temos então que o tempo de propagação do datagrama durante sua transmissão entre um equipamento emissor até um equipamento receptor, passando por um único equipamento roteador é dado por :

$$\mathbf{Tprop = 2*Tprop\ (meio) + Tprop\ (roteador)} \qquad (5)$$

Ou, ainda :

$$\mathbf{Tprop = 2*[L + (D/B)] + Lr + Tfe + Tfs + (Nc * Tpc) + D/Br} \qquad (6)$$

O fator de multiplicação da parcela de medida do tempo de propagação do datagrama no meio físico se justifica devido ao fato que serão necessários dois segmentos do meio físico para unir o equipamento emissor ao equipamento receptor através do roteador, como podemos ver na Fig. 13.

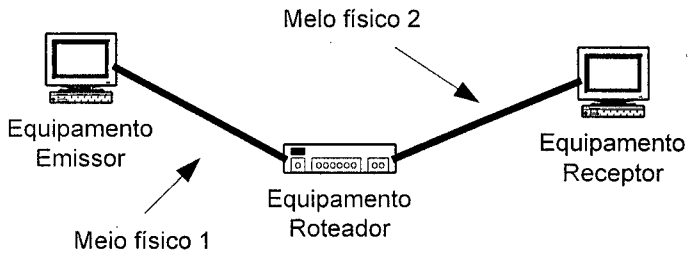

FIGURA 13 : TOPOLOGIA DA REDE DE TRANSMISSÃO DO DATAGRAMA

Se houver uma expansão do caminho percorrido pelo datagrama sugerido na Fig. 13, ocorrerá um modelo com vários segmentos de transmissão e outros vários roteadores, como mostrado na Fig. 14.

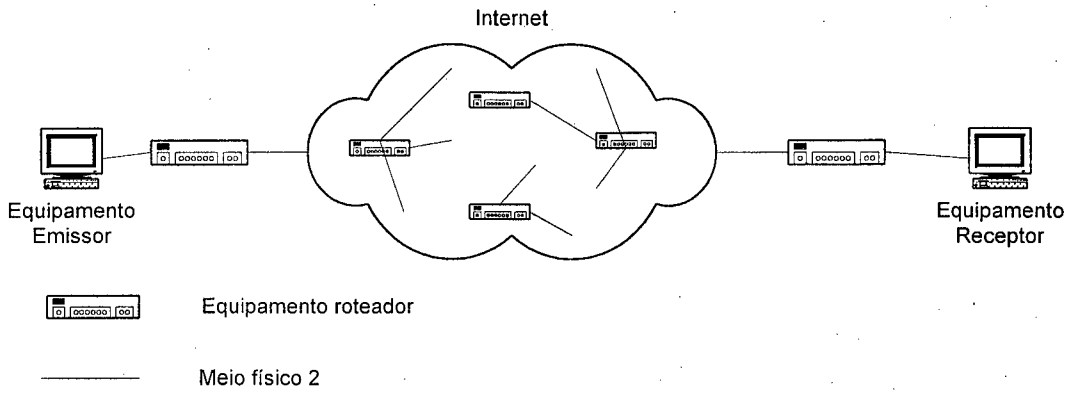

FIGURA 14 : TOPOLOGIA DA REDE DE TRANSMISSÃO DO DATAGRAMA NA INTERNET

Então o tempo de propagação final do datagrama durante a transmissão entre o equipamento emissor e o equipamento receptor do datagrama poderá ser descrito como :

$$\mathbf{Tprop} = \sum_{0}^{n} \mathbf{Tprop(meio)} + \sum_{0}^{m} \mathbf{Tprop(roteador)} \qquad (7)$$

Onde **n** corresponde ao número de segmentos físicos existentes no caminho e **m** corresponde ao número de equipamentos roteadores, sendo que **n** e **m** são valores inteiros positivos.

ou, ainda :

$$\mathbf{Tprop} = \sum_{0}^{n} \mathbf{L} + (\mathbf{D}/\mathbf{B}) + \sum_{0}^{m} [\mathbf{Lr} + \mathbf{Tfe} + \mathbf{Tfs} + (\mathbf{Nc} * \mathbf{Tpc}) + \mathbf{D}/\mathbf{Br}] \qquad (8)$$

5.3. Avaliação Analítica de Desempenho do Uso do IPv6

Utilizando-se das fórmulas apresentadas no tópico anterior vê-se que o desempenho do protocolo IPv6 pode ser otimizado apenas no roteador, já que para o meio de transmissão o desempenho depende apenas do tamanho do datagrama emitido e esse, no caso do IPv6, é maior que o datagrama IPv4, no que diz respeito ao cabeçalho básico. Como já fora apresentado anteriormente no capítulo 3, a estrutura do cabeçalho é comum a qualquer datagrama IPv6 independente da função que ele irá exercer. Essa estrutura tem o tamanho de 40 bytes.

De forma a melhorar o tempo de propagação do datagrama através do roteador, os projetistas do IPv6 otimizaram o seu mecanismo de fragmentação [GON98]. Antes de iniciar a transmissão o IPv6 envia um datagrama via ICMP (*Internet Control Message Protocol*) para coletar informações sobre a possível rota a ser feita até o destino. A partir destas informações é calculado o tamanho do fragmento que irá poder passar por toda a rede, assim, o datagrama já sai fragmentado em função do menor tamanho possível no caminho.

Esta otimização tem conseqüência direta no tempo de fila de espera, tanto de entrada (**Tfe**) quanto no de saída (**Tfs**). Também gera impacto no tempo de processamento do datagrama no roteador (**Tp**), já que haverá menos tarefas para serem realizadas, uma vez que a análise do tamanho do datagrama foi eliminada. Como conseqüência dessa diminuição no tempo de processamento devido ao mecanismo de fragmentação, temos uma redução no tempo de propagação do datagrama no roteador (**Tprop(roteador)**).

O IPv6 possui uma outra forma de incrementar o seu desempenho que é através do campo *Rótulo de Fluxo*. Este campo possui uma seqüência de 24 bits passíveis de combinações para informar uma ação ao processador de suas informações. Esse campo pode ser utilizado para gerenciar critérios de qualidade nos serviços oferecidos pelo IPv6. Através deste campo é possível realizar o controle do tráfego, permitindo a

melhor alocação da banda disponível pelo meio físico, acarretando numa melhor do tempo de propagação do datagrama no roteador (**Tprop(roteador)**). O meio de transmissão também pode ter seu tempo de propagação, (**Tprop(meio)**), otimizado, uma vez que a alocação de banda passante exerce influência no seu desempenho.

Outro aspecto que contribui para a melhoria do desempenho do protocolo IPv6 no que diz respeito ao tempo de propagação de datagramas através de roteadores é a estrutura de endereçamento como citado em [CRA98], [HIN98_2] e [EUI00]. O IPv6 utiliza-se dos endereços físicos das interfaces de rede [EUI00], quanto das conexões lógicas, como no caso do ATM [ARM99]. Como o endereçamento IPv6 permite 128 bits para identificação de uma conexão lógica à rede, então, é feito um arranjo neste campo de modo que o endereço receba o prefixo da rede e o seu complemento seja correspondente ao endereçamento físico da interface.

Este artifício permite uma maior interação do protocolo com a camada física da rede, diminuindo o tempo necessário na resolução de um caminho para o datagrama, o que acarreta um ganho no tempo de propagação do datagrama no roteador (**Tprop(roteador)**).

A inclusão das estruturas de cabeçalhos de extensão, como já vistos no capítulo 3, também contribui para um melhor desempenho do IPv6 no tempo de propagação de datagramas.

Quando o datagrama estiver levando consigo algum dado para ser entregue a uma interface destino, o que é mais comum, ele pode associar os cabeçalhos de extensão que se fizerem necessários de acordo com a funcionalidade de cada um desses cabeçalhos. Por exemplo, se houver a necessidade de criptografar os dados de modo a fornecer um grau maior de segurança a eles, então o campo com informações de criptografia é associado ao datagrama, mas somente este cabeçalho. Se além da segurança através de criptografia, houver necessidade de informar uma rota fixa para o datagrama seguir, associa-se outro campo do cabeçalho de extensão a ele, e assim tal informação é repassada ao roteador assim que o datagrama for processado. Se novos

requisitos forem necessários basta associar o cabeçalho de extensão desejado ao datagrama e este requisito será ativado.

Desta forma, o IPv6 faz com que o datagrama tenha apenas campos úteis para si, não penalizando a transmissão com campos extras que apenas fariam a passagem pelo roteador ficar mais lenta devido a necessidade de processa-los. Como conseqüência desse mecanismo, ocorre um ganho no tempo de processamento do datagrama gerando, assim, nova redução no tempo de propagação do datagrama no roteador (**Tprop(roteador)**).

5.4. Avaliando o Desempenho do IPv6 em um Ambiente Real

Para esta análise são considerados o tempo de propagação do datagrama nos meios físicos de transmissão e no roteador utilizado na transmissão de um datagrama entre uma estação emissora até uma estação receptora, conforme ilustra a Fig. 15, o tamanho do datagrama utilizado em cada transmissão e, logicamente, a natureza do datagrama, se ele é um datagrama IPv4 ou um datagrama IPv6.

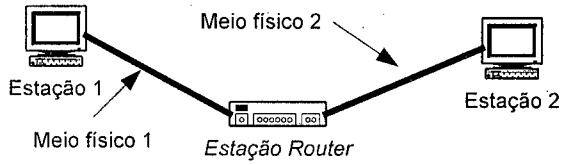

FIGURA 15 : TOPOLOGIA DA REDE AVALIADA

5.4.1. Análise de Desempenho do IPv6 no Meio de Transmissão

Para analisar o desempenho do IPv6 junto ao meio de transmissão é necessário conhecer um pouco a respeito do meio utilizado.

Na rede implementada fora utilizado o protocolo de transmissão *Ethernet* com CSMA/CD (*Carrier-sense multiple access with collision detection*), segundo o padrão

IEEE 802.3. *Ethernet* é uma especificação de cabeamento e sinalização para de redes de computadores que tem entre suas características a capacidade de envio máximo de 1500 octetos por quadro entre dois equipamentos de rede, através de cabeamento de par trançado, podendo para isso utilizar um equipamento difusor de datagramas, como o *hub*. Maiores informações a respeito do protocolo *Ethernet* deve-se consultar [MET76] que é o artigo original escrito por ***Robert Metcalfe*** apresentando este protocolo. Em [BOG88] é feito uma análise do desempenho do *Ethernet*, buscando desvendar o que é mito e o que é realidade a respeito deste protocolo. Por fim, uma leitura obrigatória se faz necessária da RFC2464 [CRA98] em que é discutida a transmissão de pacotes IPv6 sobre redes *Ethernet*.

Foram realizadas medidas tanto entre a Estação 1 e a Estação *Router* quanto entre a Estação *Router* e a Estação 2. De forma a verificar se o comportamento é o mesmo nos dois caminhos, como seria de se esperar. O comportamento de cada protocolo com as variadas cargas, 64, 750 e 1500 bytes, foram apresentadas no capítulo anterior.

Observando as figuras, Fig. 7, Fig. 8, Fig. 11, Fig. 12, apresentadas no capítulo anterior pode-se concluir que o IPv6 é mais lento que o IPv4 para qualquer quantidade de carga testada. Essa conclusão era esperada, uma vez que na transmissão no cabeamento o datagrama não sofre nenhum processamento, sendo apenas encapsulado pela unidade de dados correspondente ao protocolo de meio de transmissão utilizado. O datagrama IPv6 é maior que o datagrama básico IPv4, o IPv6 é de 40 byte e o de IPv4 de apenas 20 bytes.

A Fig. 16 apresenta um gráfico com o comparativo do tempo de propagação de um datagrama entre a Estação 1 e a Estação *Router*. Valores negativos na escala de tempo, significam que o protocolo IPv6 está tendo um desempenho inferior ao do protocolo IPv4. Os valores apresentados foram obtidos subtraindo o tempo de propagação do datagrama IPv6 do tempo de propagação do datagrama IPv4 no meio de transmissão, conforme dados listados no Anexo 2.

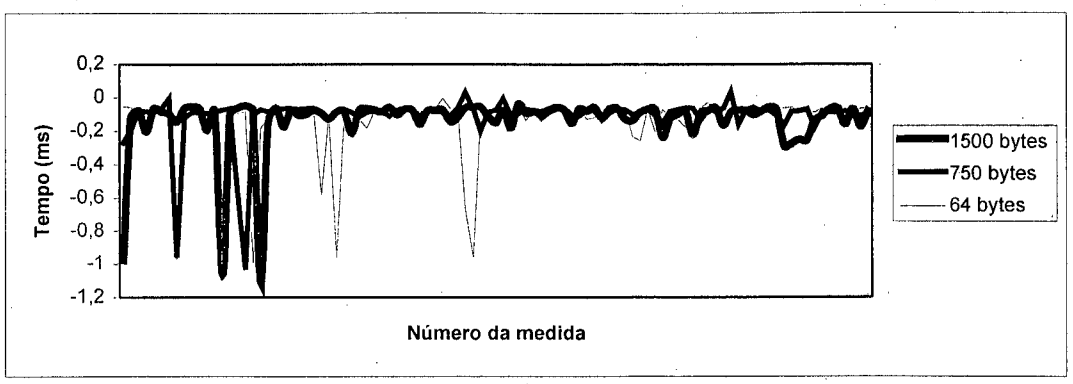

FIGURA 16 : IPV6 X IPV4 ENTRE ESTAÇÃO 1 – ESTAÇÃO *ROUTER*

Vale ressaltar que o fato de nem todos os datagramas medidos terem tido um desempenho uniforme é importante para essa análise, uma vez que o resultado apresentado mostrou que o desempenho foi negativo, o que quer dizer que o IPv6 é mais lento, para essas medidas, que o IPv4.

A Fig. 17 apresenta a mesma comparação para o tempo de propagação de um datagrama entre a Estação *Router* e a Estação 2.

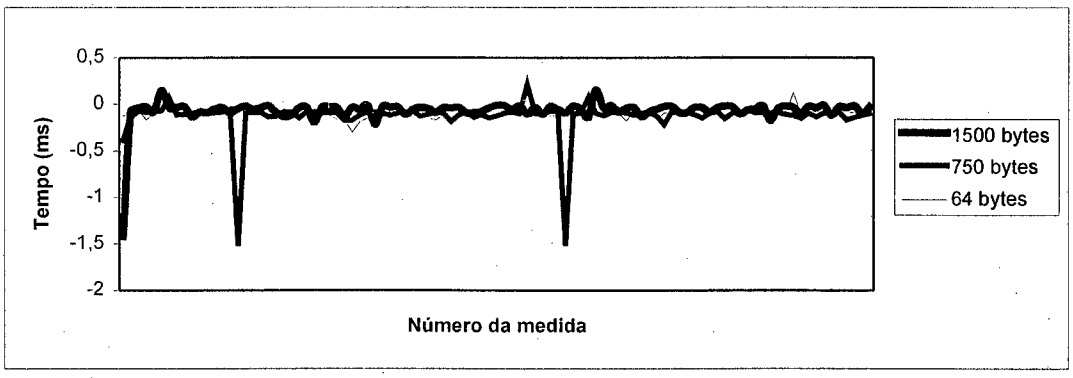

FIGURA 17 : IPV6 X IPV4 ENTRE ESTAÇÃO *ROUTER* - ESTAÇÃO 2

5.4.2. Análise de Desempenho do IPv6 no roteador

A Fig. 18 apresenta um gráfico com o comparativo do tempo de propagação de um datagrama na Estação *Router*. Valores positivos na escala de tempo, significam que

o protocolo IPv6 está tendo um desempenho superior ao do protocolo IPv4. Os valores apresentados foram obtidos subtraindo o tempo de propagação do datagrama IPv6 do tempo de propagação do datagrama IPv4 no roteador, conforme dados listados no Anexo 2.

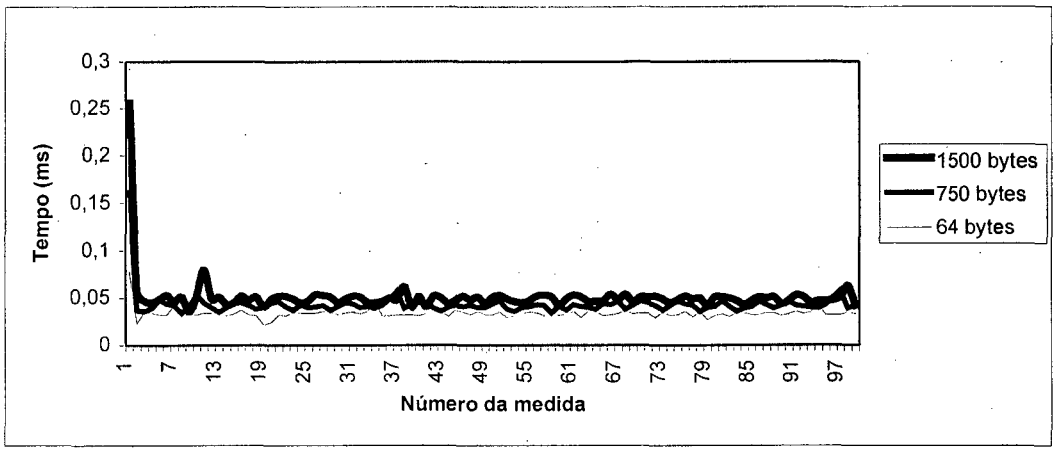

FIGURA 18 : IPV6 X IPV4 NA ESTAÇÃO *ROUTER*

Observando as figuras, Fig. 9, Fig. 10, apresentadas no capítulo anterior pode-se concluir que o IPv6 é mais rápido que o IPv4 para qualquer quantidade de carga testada, no que se trata a propagação do datagrama em um roteador.

A Fig. 18 confirma que no roteador o desempenho do tempo de propagação do datagrama IPv6 é superior ao desempenho do protocolo IPv4. Isto se deve a estrutura de endereçamento utilizado no IPv6 que adiciona a si o endereço *Ethernet* de identificação física de uma interface de rede ao endereço IPv6 da estação. Essa estrutura é a ***EUI-64***, que é definida pelo *IEEE* como um identificador global de 64 bits.

A utilização do endereçamento no formato ***EUI-64*** é informado no momento da seleção dos parâmetros do *kernel*, para posterior compilação, como indicado no Anexo 1. Maiores informações sobre o EUI-64 pode ser encontrado em [EUI00]. O mecanismo de roteamento de endereços IPv6 sobre redes Ethernet é explicado em [CRA98] e, por fim, em [HID98_2] é feita uma discussão a respeito de endereçamento *Unicast* envolvendo o ***EUI-64***.

5.4.3. Análise de Desempenho do IPv6 em Toda o Percurso da Transmissão

Uma vez analisado o desempenho do IPv6 para cada parte da transmissão tem-se então o desempenho final, somando-se todos os desempenhos encontrados, obtendo um gráfico como o apresentado na Fig. 19, quer caracteriza o desempenho total do tempo de propagação de datagramas IPv6 entre uma estação emissora e uma estação receptora, passando por uma estação roteadora.

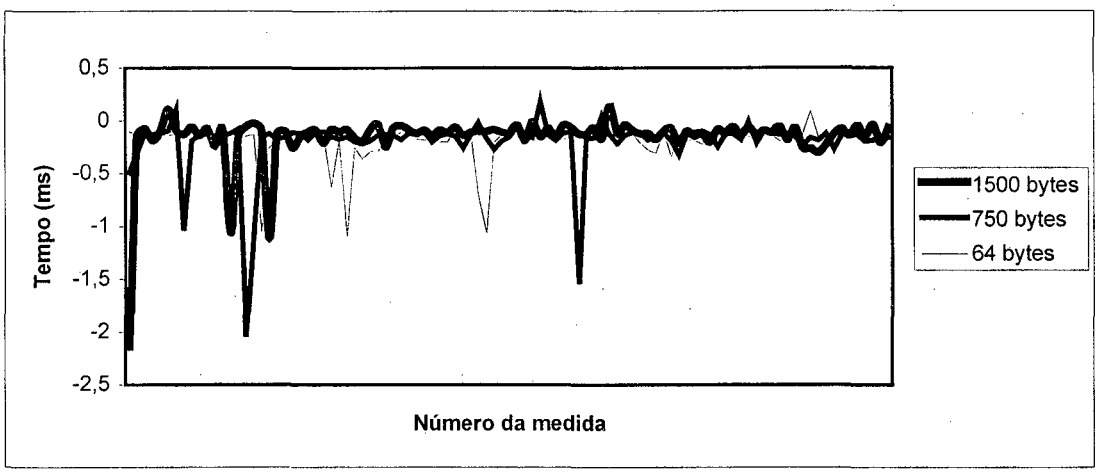

FIGURA 19 : IPV6 X IPV4 EM TODO PERCURSO

A Fig. 19 apresenta um gráfico com o comparativo do tempo de propagação de um datagrama na Estação *Router*. Valores negativos na escala de tempo, significam que o protocolo IPv6 está tendo um desempenho inferior ao do protocolo IPv4. Os valores apresentados foram obtidos subtraindo o tempo de propagação do datagrama IPv6 do tempo de propagação do datagrama IPv4 para todo o percurso percorrido, conforme dados listados no Anexo 2.

Como pode ser visualizado, o IPv6 apresentou um desempenho final inferior ao desempenho apresentado pelo protocolo IPv4. Esse desempenho inferior se deve ao desempenho no meio de transmissão.

Vale observar que, excluindo alguns valores que tiveram um desempenho muito ruins, a grande maioria dos valores medidos, tiveram um desempenho próximo a zero.

5.5. Conclusão

Neste capítulo foi apresentada a avaliação analítica de desempenho do uso do protocolo IPv6. Junto a essa avaliação analítica foi apresentada a avaliação de desempenho em um ambiente real, que veio a comprovar a validade da avaliação analítica.

As descrições matemáticas sugeridas no item 5.2 servem tanto para uma rede com o protocolo IPv6 quanto para uma rede com o protocolo IPv4. Por isso no tópico 5.3 é feita uma análise a respeito dos fatores de melhoria do desempenho no IPv6, tendo como termo de comparação o IPv4.

Estas descrições, também, não limitam o tamanho da rede ou o número de roteadores que podem existir no caminho percorrido. Essa limitação fica por conta da capacidade dos equipamentos, sendo portanto uma limitação inerente à tecnologia de fabricação desses componentes.

No item 5.4 foi realizada a análise de desempenho em um ambiente real, ambiente esse apresentado no capítulo anterior e cujos dados estão apresentados no Anexo 2. Nesta análise foi enfocado apenas o desempenho do datagrama, tanto IPv4 quanto IPv6, no que diz respeito ao tempo sua propagação na rede. O comportamento deste datagrama no que diz respeito a valores não uniformes apresentados, não fazem parte do escopo deste trabalho.

6. CONCLUSÃO FINAL

6.1. Considerações Iniciais

Este trabalho apresentou o protocolo IPv6 em seus aspectos teóricos e práticos, sempre comparando-o com o IPv4, que é a versão atualmente em uso. Devido a pouca publicação a respeito de medidas de seu desempenho, este trabalho passa a obter sua relevância, pois nele é realizada a avaliação do desempenho do uso do IPv6 em uma rede local implementada no Laboratório do Cursos de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, utilizando valores reais, medidos diretamente no sistema, através da transmissão de datagramas entre duas estações, uma emissora e outra receptora, passando por uma estação roteadora destes datagramas. Um outro aspecto de relevância aqui apresentado é a avaliação analítica, onde o comportamento do tempo de propagação do datagrama é descrito matematicamente.

Neste trabalho, como já citado acima, é proposto um modelo matemático que descreve o tempo de propagação do datagrama durante a transmissão entre uma estação emissora e uma receptora, levando em consideração aspectos de roteamento e o meio físico presente na comunicação. Este modelo não é restritivo de forma a unir um sistema com duas estações e um roteador. Ele pode ser expandido para um sistema mais amplo com diferentes meios físicos de transmissão envolvidos e vários roteadores no caminho uma vez que os parâmetros avaliados são fundamentais e existentes em qualquer implementação utilizada. Assim ele pode ser utilizado não apenas para o problema aqui analisado, mas também para outras análises, como por exemplo a de congestionamentos

e comportamento de aplicativos numa transmissão. Além disso o modelo é aplicável tanto ao IPv6 quanto ao IPv4.

6.2. Resultados Alcançados

Os objetivos propostos neste trabalho foram alcançados com sucesso, tanto os objetivos gerais quanto os objetivos específicos. Dos objetivos gerais merece destaque o estudo do protocolo IPv6. Algumas revistas e jornais falam a respeito deste protocolo com o destaque único para a mudança do número de bits de endereçamento, que passou de 32 bits para 128 bits, como se essa fosse a mudança mais relevante e importe ocorrida. O estudo mais atento e aprofundado do IPv6 mostra que as mudanças propostas pela comunidade internacional não se limitam a tão pouco. Como exemplo vale citar que toda a estrutura de endereçamento foi modificada, modificando o modo de comunicação entre as entidades envolvidas na comunicação e até mesmo a forma de roteamento dos datagramas. De forma geral pode-se dizer que o IPv6 não é compatível com o IPv4, ainda que existam mecanismos para que as duas versões possam estabelecer comunicação.

Quanto aos objetivos específicos propostos, os dados obtidos a partir da avaliação analítica e da comparação real de valores medidos na rede implementada são compatíveis, de forma que as descrições matemáticas apresentadas foram comprovadas através dos resultados alcançados no ambiente real. Estes dados indicam que o desempenho do IPv6 em uma rede local é pior que o desempenho alcançado pelo IPv4, ainda que a diferença seja pouca, como pode ser vista nos gráficos apresentados.

O maior problema da comunicação na Internet em se tratando de tempo de propagação de dados está no roteador, pois é ai que processamento de informações referentes ao IP. Neste aspecto o IPv6 se mostrou bastante eficiente, apresentando resultados de desempenho melhor que os apresentados pelo IPv4. Uma possível expansão da rede utilizada para testes, envolvendo mais estações e um roteador dedicado podem resultar num desempenho final melhor para o IPv6, uma vez que os problemas que ocorrem no roteamento serão mais explicitados.

6.3. Dificuldades Encontradas

Durante a realização dos trabalhos várias dificuldades foram encontradas. A maior dificuldade foi em conseguir um ambiente para fazer os testes. A princípio a intenção era utilizar os recursos existentes no Núcleo de Processamento de Dados da UFSC. Lá existe uma conexão com o *6Bone* e já foi configurada uma rede IPv6 utilizando duas estações *NT* e uma *AIX*. Nesse ambiente existe, também, um roteador IPv6.

Devido a dificuldades internas para a alocação de equipamentos os testes foram inviabilizados. Como uma das estações NT apresentou defeitos durante os testes foi sugerido conseguir uma outra estação, porém todas as outras estações estavam em ambiente de produção e necessitaria modificar o cabeamento no *switch*.

Devido a esses percalços optou-se por criar um ambiente dentro do próprio laboratório do Curso de Pós-Graduação em Ciência da Computação. Esse laboratório também possui poucas máquinas disponíveis para uso e elas são utilizadas por todos os alunos do curso. A saída foi configurar as máquinas num fim de semana, particionando o disco rígido de forma que pudesse colocar os sistemas operacionais.

O fato dos sistemas operacionais possuírem implementações experimentais acabou resultando em dificuldades, pois, no caso da Estação *Router*, foi necessário recompilar todo o sistema operacional e devido a um erro ocorrido, foi preciso reinstalá-lo novamente.

A busca de trabalhos correlatos também apresentou dificuldade. Não existem muitas publicações a respeito do protocolo IPv6. Muito do que se encontra ainda explica o que é o IPv6 e traz informações já encontradas em *RFCs* e livros regulares.

6.4. Perspectivas Futuras

Dentre as perspectivas esperadas para o futuro, espera-se obter uma implementação mais estável da pilha de protocolos IPv6. Uma nova versão do *kernel* do *Linux* está para ser disponibilizada, assim, tem-se a expectativa de que haja alguma mudança de forma a já incorporar os recursos do IPv6 nativos, como já ocorre com o *AIX* da IBM.

Ainda em relação a uma nova versão, espera-se uma padronização dos comandos e dos arquivos de configuração do IPv6 nos vários sistemas operacionais existentes, assim como já ocorre com o IPv4.

A demonstração pública do interesse de grandes empresas em relação ao protocolo IPv6, deve fazer com que avance as pesquisas e surjam novas aplicações. Empresas como *Microsoft Co.*, *Sun Microsystem*, *IBM*, *Cisco*, *3Com* e *Oracle*, já demonstraram interesse em desenvolver soluções para o IPv6.

A exploração dos serviços de comunicação tanto móveis quanto fixos estão aprimorando cada vez mais o tráfego de voz e dados através do IP. Com a criação de backbones particulares e a necessidade de controle do tráfego existe um campo para a aplicação do IPv6, como já foi feito pela NTT no Japão.

Outra expectativa ocorre em relação do IP móvel, o aumento do consumo de tecnologia móvel está abrindo um campo tecnológico sem precedentes. Não existe padrões para a transmissão de informações e o IPv6 é um forte candidato a ser o protocolo para a transferência dos dados.

6.5. Propostas para Novos Trabalhos

- Expandir os testes para uma rede local, utilizando um roteador dedicado ao invés de um micro roteando através de cabo *cross over*;
- Realizar os testes de avaliação do desempenho em pilhas mais estáveis;
- Incrementar os testes verificando as conseqüências do uso de cabeçalhos de extensão;
- Pesquisar mais a respeito do IPv6 móvel e sua integração com as tecnologias já existentes;
- Realizar avaliações de desempenho utilizando a rede de alta velocidade da UFSC, incluindo aspectos de segurança e de qualidade de serviço;
- Pesquisar sobre as possibilidades de gerenciamento de uma rede IPv6 através do SNMP e outras ferramentas.

7. REFERÊNCIAS BIBLIOGRÁFICAS :

[ARM99] ARMITAGE, G.; SCHULTER P.; JORK M. IPv6 over ATM Networks. Request for Comments : 2492. IETF, Janeiro, 1999.

[ATK98] ATKINSON, R; KENT S. Security Architecture for the Internet Protocol. Request for Comments : 2401. IETF, Novembro, 1998.

[BIE00] BIERINGER Peter. IPv6 & Linux How-To, version 3.13. Munich, Alemanha. Fevereiro, 2000. Site : http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

[BOG88] BOGGS, David R.; MOGUL, Jeffrey C.; KENT, Christopher A. Measured Capacity of an Ethernet : Myths and Reality. WRL Research Report 88/4. Western Research Laboratory, Digital Corp. Palo Alto, California, EUA. Setembro, 1988.

[BRA95] BRADNER, S.; MANKIN, A.The Recommendation for the IP Next Generation Protocol. Request for Comments : 1752. IETF, Janeiro, 1995.

[BJO98] BJÖRKLUND, Ulf. Understanding the Performance of the Linux IPv6 Implementation. Tese de mestrado. Kungl Tekniska Högskolan, Estocolmo, Suécia. Novembro, 1998.

[BOZ98] BOZZANO, Jussara Maria. Gerenciamento de Autoconfiguração em Redes com Ipv6. Dissertação de mestrado do CPGCC-UFSC. Florianópolis, Brasil. Setembro, 1998.

[CER98] CERF., Vinton G. A Brief History of the Internet and Related Networks. Internet Society (ISOC). Fevereiro, 1998. Site http://www.isoc.org

[COM99] COMITÊ GESTOR DA INTERNET NO BRASIL. Sobre o Comitê Gestor. Brasil, Maio, 1999.

[COS99] COSTA, Taís Freire da Silva. Avaliação Analítica do Uso de Agentes Móveis na Gerência de Redes. Dissertação de mestrado do CPGCC-UFSC. Florianópolis, outubro, 1999.

[CRA98] CRAWFORD, M. Transmission of IPv6 Packets over Ethernet Networks. Request for Comments : 2464. IETF, Dezembro, 1998.

[DEE98] DEERING, S. HINDEN, R. Internet Protocol, Version 6 (IPv6) Specification. Request for Comments : 2460. IETF, Dezembro, 1998.

[EUI00] IEEE. Guidelines for 64-bits Global Identifier (EUI-64). IEEE Standards. EUA. Fevereiro, 2000. Site http://standards.ieee.org/regauth/oui/tutorials/EUI64.html

[FNC95] FNC, Federal Networking Council. Definition of Internet. FNC Resolution. EUA. 1995. Site http://www.fnc.gov/Internet_res.html

[FRE99] FREITAS, Allan Edgard Silva; et all. Procedimentos de instalação e configuração de IPv6 em Linux. RNP, Centro de Informações, Rio de Janeiro, RJ, Brasil. 1999. http://www.rnp.br/ipv6/ipv6-proc-linux.html

[FUL93] FULLER, V.; MERIT, J. Yu; VARADHAN K. Classless Iner-Domain Routing (CIDR) : an Address Assignment and Aggregation Strategy. Request for Comments : 1519. IETF, Setembro, 1993.

[GON98] GONCALVES, Marcus; KITTY Niles. IPv6 Networks. McGraw-Hill Companies, INC. EUA, 1998.

[GUR99] GURGACZ, Carla Verônica; BOZZANO, Jussara Maria. Analysis of Security Performance for IPv6 and IPv4. Núcleo de Processamento de Dados, Universidade Federal de Santa Catarina. Florianópolis, SC, Brasil. Agosto, 1999.

[HIN98] HINDEN, R. DEERING, S. IP Version 6 Addressing Architecture. Request for Comments : 2373. IETF, Julho, 1998.

[HIN98_2] HINDEN, R. DEERING, S. An IPv6 Aggregatable Global Unicast Address Format. Request for Comments : 2374. IETF, Julho, 1998.

[HOV96] HOVEY, R; BRADNER, S. The Organizations Involved in the IETF Standards Process. Request For Comments : 2028. IETF, Outubro, 1996.

[HUI98] HUITEMA, CHRISTIAN. IPv6 : The New Internet Protocol, 2ª Edition. Prentice Hall. EUA, 1998.

[IDG97] IDG NOW !. Desempenho da Internet no Brasil. IDG Computerworld do Brasil. Universo On-Line. Brasi. Setembro 1997. Site http://www.uol.com.br/idgnow/

[INF81] ISI; Information Sciences Institute. Internet Protocol - DARPA Internet Program - Protocol Specification. Request for Comments : 791. IETF. September, 1981.

[JAI91] JAIN, Raj. The art of computer systems performance analysis : techniques for experimental design, measurement, simulation, and modeling. John Wiley & Sons, Inc. EUA, 1991.

[LEE00] LEE, Thomas; DAVIES, Joseph. Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference. Microsoft Press. EUA. Março, 2000.

[LEI98] 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

[MAL94] MALKIN, G. The Tao of IETF - A Guide for New Attendees of the Internet Enigneering Task Force. Request For Comments : 1718. IETF, Novembro, 1994.

[MAR99] MARSAN, Carolyn Duffy. Internet Protocol Version 6. Network World Fusion. August, 1999. Site http://www.nwfusion.com/archive/1999/73836_08-30-1999.html

[MAR00] MARSAN, Carolyn Duffy. Cisco, Microsoft give IPv6 shot in the arm. Network World Fusion. March, 2000. Site http://www.nwfusion.com/news/2000/0320ipv6.html

[MAR00_2] MARSAN, Carolyn Duffy. Japan´s NTT to be first ISP to offer IPv6. Network World Fusion. March, 2000. Site http://www.nwfusion.com/news/2000/0320carrier.html

[MCG99] MCGARVEY, Joe. IPv6 Forum Holds First Meeting. Inter@ctive Week. September, 1999.

[MET76] METCALFE, Robert M.; BOGGS, David R. Ethernet : Ditributed Packet Switching for Local Computers Networks. Communications of the ACM, Vol. 19, No 5. Julio 1976. pp.395-404.

[MIC00] MICROSOFT RESEARCH TEAM. Internet Protocol Version 6. Microsoft Co. EUA. Fevereiro, 2000. Site http://www.research.microsoft.com/msripv6/

[OLI99] OLIVEIRA, Frederico S. G.; PEDROZA, Aloysio de Castro P.; Uma arquitetura para suporte a segurança e mobilidade sobre IPv6. XVI Simpósio Brasileiro de Redes de Computadores. Rio de Janeiro, Brasil. 1999.

[TAN96] TANENBAUM, Andrew S. Computer Networks, 3rd Edition. Upper Saddle River, New Jersey, EUA. 1996.

ANEXO 1 : CONFIGURAÇÃO DA REDE IPV6

1.1. Considerações Iniciais

Para a coleta dos dados utilizados na avaliação analítica de desempenho do uso do IPv6 apresentado neste trabalho, configurou-se uma rede IPv6 experimental no Laboratório de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

A rede consiste em três computadores interligados entre si através cabos de par trançado categoria 5. Cada computador é considerado uma estação de trabalho específica. Os micros estão dispostos em duas sub-redes distintas de modo que uma das estações, a Estação Router, é a responsável pelo roteamento dos datagramas entre as outras duas estações. A Fig. 20 ilustra a atual topologia da rede.

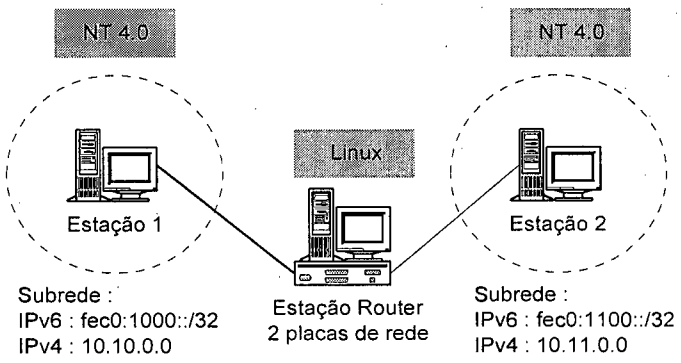

FIGURA 20 : TOPOLOGIA DA REDE

A Estação 1 e a Estação 2 possuem o sistema operacional Windows NT 4.0 WorkStation com as pilhas IPv4 e IPv6 ativadas. A Estação Router possui o sistema operacional Linux RedHat 6.1, kernel 2.2.12-20, com duas placas de redes para servir como elo de ligação entre as duas sub-redes. A ligação entre as placas de rede é feita com cabo UTP CAT 5 com pinagem cruzada (também conhecido como "*cross-over*"), que permite a comunicação direta entre interfaces de rede sem a necessidade de um elemento de ligação entre eles, com por exemplo um *hub*.

A razão de utilizar o cabo com pinagem cruzada se deu apenas para garantir um tráfego mais homogêneo entre as estações e eliminar o atraso no tempo de propagação do datagrama ocasionado pelo *hub* ou por colisões com outros datagramas de outras estações, já que o *hub*, por construção e definição, apenas repassa os datagramas que chegam a ele para todas as estações conectadas.

Nos próximos tópicos será apresentada a metodologia empregada para configuração da pilha TCP/IPv6 em cada estação. A configuração da pilha TCP/IPv4 não é necessária para o funcionamento do IPv6, mas para esse trabalho foi considerado que cada estação já possuía a pilha TCP/IPv4 ativada e configurada.

1.2. Instalando a Pilha TCP/IPv6 no Microsoft Windows NT

A configuração do IPv6 no Microsoft Windows NT é simples. Devendo-se apenas instalar a pilha de protocolos TCP/IPv6 e configurar a interface de rede com o endereço IPv6 desejado. Várias aplicações, como o *ping6*, *tracert6* e *ttcp*, também já são disponibilizadas, facilitando os testes e o uso do protocolo.

A atual versão da pilha de protocolos é uma versão ainda em pesquisa, logo, o usuário terá de realizar algumas tarefas através de um conjunto de comandos ou fazendo arquivos de comandos, os chamados *scripts*, para executá-los em conjunto e conseguir configurar a rede a contento.

Já existe suporte ao *IPSec*, mas sem criptografia, ao tunelamento de datagramas IPv6 sobre o IPv6 e a roteamento de datagramas IPv6, o que faz desta implementação uma boa escolha para ambientes corporativos já habituado ao uso de softwares da *Microsoft Co*. Ainda não há suporte à redes móveis, uma característica importante do IPv6. A *Microsoft* em seu site adverte que o uso deste protocolo não tem fins comerciais, não fazendo parte de seus produtos oficialmente. A atual implementação é de fins de pesquisa e apenas para testes [MIC00].

Não há uma implementação similar para os sistemas operacionais da linha Windows 9X, mas a atual implementação é compatível com o Windows 2000.

Passos para instalação da pilha TCP/IPv6 :

1. Buscar no *site* da *Microsoft Co.*, através do endereço *http://www.research.microsoft.com/msripv6/* o arquivo ***msripv6-bin-1_4.exe***. Esta é a última versão disponibilizada até a escrita deste documento, ela corresponde à *release* 1.4 de 13 de janeiro de 2000. Todos os passos necessários para conseguir esse arquivo é detalhado na página acessada.

2. Executar o arquivo ***msripv6-bin-1_4.exe***. Assim será criado um diretório de nome ***IPv6Kit*** na raiz da unidade de disco atual, conforme a Fig. 21. Este diretório contém todos os aplicativos e arquivos de configuração necessários para o funcionamento do IPv6, do protocolo *IPSec* e da implementação do tunelamento de IP.

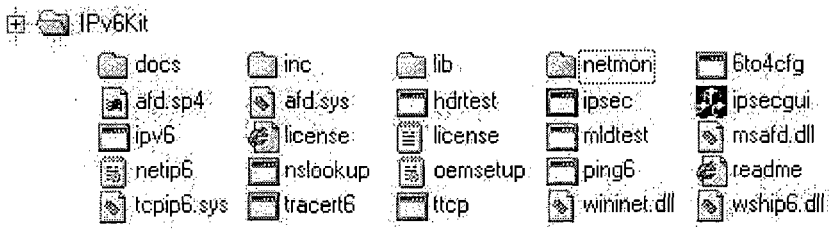

FIGURA 21 : CONTEÚDO DO DIRETÓRIO ***IPV6KIT***

3. Uma vez instalado o diretório ***IPv6Kit*** o próximo passo é acionar a pilha junto ao Windows NT. Isto é feito no Painel de Controle através da opção de configuração de Rede, da mesma forma como é feito para o IPv4. Dentro da opção de configuração de Rede basta escolher Protocolos e então o botão Adicionar. O caminho do novo protocolo será sugerido através do botão de comandos Com Discos na tela Selecione Protocolo de Rede. Ao ser pedido o caminho do arquivo de configuração, na tela Insira o Disco, deve-se indicar o diretório ***IPv6Kit***, como indicado na Fig. 22. A nova pilha de protocolos deverá aparecer listada na tela. Feche a aplicação e reinicialize o sistema operacional.

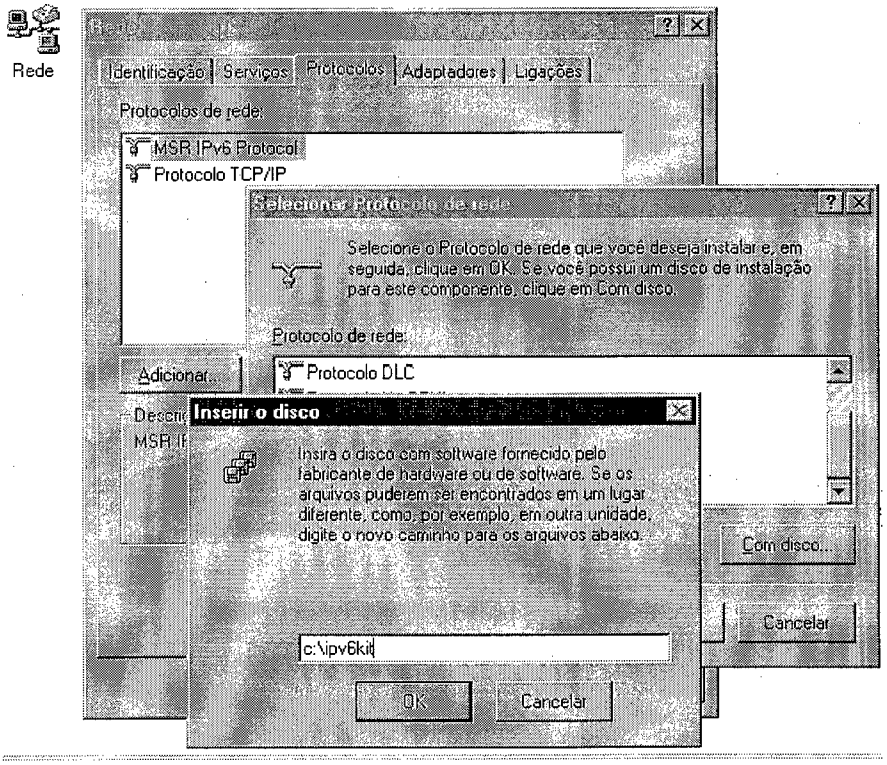

FIGURA 22 : INSTALANDO A PILHA DE PROTOCOLOS IPV6

4. A pilha IPv6 não possui uma interface gráfica de configuração através das propriedades do protocolo de rede no Painel de Controle, como no IPv4, onde poderia ser informado o número IPv6 da máquina, o endereço do servidor de nomes e/ou o endereço do *gateway* da rede. Toda essa operação

deve ser feita manualmente através de linhas de comandos próprios para tal fim, que também são diferentes dos utilizados no IPv4. Para saber se o protocolo IPv6 está funcionando abra uma sessão no DOS e digite o seguinte comando :

```
C:\> ipv6 if
```

As informações mostrada no Quadro 1 serão apresentadas na tela :

```
Interface 4 (site 1):
  uses Neighbor Discovery
  link-level address: 00-00-e8-59-e9-07
    preferred address fe80::200:e8ff:fe59:e907, infinite/infinite
    multicast address ff02::1, 1 refs, not reportable
    multicast address ff02::1:ff59:e907, 1 refs, last reporter
  link MTU 1500 (true link MTU 1500)
  current hop limit 128
  reachable time 40500ms (base 30000ms)
  retransmission interval 1000ms  DAD transmits 1

Interface 3 (site 1):
  uses Neighbor Discovery
  link-level address: 10.10.10.11
    preferred address fe80::a0a:a0b, infinite/infinite
    multicast address ff02::1, 1 refs, not reportable
    multicast address ff02::1:ff0a:a0b, 1 refs, last reporter
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 21500ms (base 30000ms)
  retransmission interval 1000ms  DAD transmits 1

Interface 2 (site 0):
  does not use Neighbor Discovery
  link-level address: 0.0.0.0
    preferred address ::10.10.10.11, infinite/infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 0ms (base 0ms)
  retransmission interval 0ms  DAD transmits 0

Interface 1 (site 0):
  does not use Neighbor Discovery
  link-level address:
    preferred address ::1, infinite/infinite
  link MTU 1500 (true link MTU 1500)
  current hop limit 1
  reachable time 0ms (base 0ms)
  retransmission interval 0ms  DAD transmits 0
```

QUADRO 1 : SAÍDA DA EXECUÇÃO DO COMANDO IPV6 IF

Apesar da configuração ser relativa a apenas uma única placa de rede física, são apresentadas informações sobre quatro interfaces de rede. Na verdade são criadas interfaces virtuais, ou pseudos-interfaces, com propósitos especificos como uma pseudo-interface para *loopback*, que é a *Interface 1* e outra para tunelamento de IP que é a pseudo-interface *Interface 2*. Por construção essas duas pseudos-interfaces não podem ser excluídas. Outras duas pseudos-interfaces são sugeridas, podendo uma delas ser apagada ou novas criadas, dependendo da necessidade do gerente da rede. Vale lembrar que o IPv6 permite que uma interface de rede tenha mais de um único endereço associado a ela.

Como o serviço de auto-configuração (*Neighbor Discovery*) está ativado por *default*, um endereço IP de *link-local* já será sugerido para a interface de rede. Este endereço caracteriza-se pelo prefixo de *link-local* (fe80::) mais um sufixo relativo ao endereço *ethernet* próprio da placa de rede [DEE98].

5. Uma vez que as informações contida no Quadro 1 apareçam e que, principalmete, uma das interfaces tenha um endereço IPv6 associado a si, alguns programas aplicativos podem ser executado para testar o funcionamento da rede, como por exemplo o aplicativo ping que deve ser executado como o exemplo :

```
C:\> ping6 < endereço ipv6 >
```

1.2.1 Configurando subredes IPv6

Para a coleta de dados relativos à propagação de um datagrama no IPv6 é necessário configurar as estações em sub-redes distintas. Para tal deve-se utilizar o endereçamento de *site-local* que se caracteriza pela ocorrência do prefixo fec0::.

A configuração de uma rede *site-local* tem de ser feita a partir de *scripts*, como o apresentado na Quadro 2, uma vez que as modificações numa pseudo-interface são

descartadas assim que a pilha é descarregada da memória. O Quadro 2 exibe o *script* utilizado em uma das máquinas NT da rede, a explicação mais completa da utilização de cada comando é encontrada no arquivo ***config.htm*** que está no diretório ***ipv6kit/doc***, criado na descompactação do arquivo ***msripv6-bin-1_4.exe***.

```
@echo off
rem
rem                Arquivo de configuracao da rede IPv6
rem
rem Autor : Maurilio Alves (alves@inf.ufsc.br)
rem Data  : 31/03/2000
rem Ultima modificacao : 02/04/2000
rem
rem Os comentarios com # nao sao validos. Estao sendo utilizados apenas
rem para carater ilustrativos, devendo ser suprimidos ao ser executado.

rem Levantando a pilha IPv6
net stop  tcpip6        # Se houver uma pilha ativa, desativa-a
net start tcpip6        # Ativa a pilha tcpip6, apagando todas as
                        # configuracoes anteriores.

rem Limpando a tabela de rotas
ipv6 rcf
ipv6 ncf

rem Retirando o endereco LinkLocal oferecido pelo Neighbor Discovery
ipv6 adu 4/fe80::200:e8ff:fe59:e907 life 0
                                    # Endereco link-local sugerido

rem Adicona prefixo de rede
ipv6 spu fec0:1000::/32 4      # Prefixo que determina a sub-rede

rem Adicionando o endereco SiteLocal desejado
ipv6 adu 4/fec0:1000::200:e8ff:fe59:e907

rem Adicionando rota para visualizar o roteador IPv6
ipv6 rtu fec0:1000::/32 4
ipv6 rtu fec0:1100::/32 4
```

QUADRO 2 : *SCRIPT* DE CONFIGURAÇÃO DE UM ENDEREÇO *SITE-LOCAL*

Esta configuração deve ser feita em cada máquina da rede. Os endereços utilizados neste exemplo correspondem a uma única interface de rede e mais especificamente à pseudo-interface 4. Como em cada máquina estes endereços serão diferentes, o script deve ser modificado utilizando o endereço *link-local* sugerido pela auto-configuração da pseudo-interface desejada.

1.3. Instalando a Pilha TCP/IPv6 no Linux Red Hat 6.1

O *Linux* é um sistema operacional de código aberto, que não precisa de licença ou registro especial para ser utilizado tanto na computação pessoal quanto na computação corporativa. Ele é desenvolvido por técnicos e acadêmicos através de um esforço conjunto através da Internet, onde cada inovação ou correção é disponibilizada gratuitamente e com livre acesso ao código fonte.

Existe uma organização que gerencia a criação de versões do *kernel* do *Linux*, a Kernel.org [KER00]. Uma de suas funções é padronizar o núcleo do sistema operacional de modo a patrocinar a maior compatibilidade entre as várias distribuições existentes. *Linux*, em qualquer uma de suas distribuições, é fornecido com uma série de programas e com o *kernel*, onde se encontram os códigos para gerenciar os processos e a memória, controlar dispositivos e sistema de arquivos etc. O *kernel* é identificado sempre por um número de versão, na forma: X.Y.Z onde X é a versão principal; Y identifica o estado do mesmo, sendo que números ímpares indicam *kernel* em desenvolvimento e pares, *kernels* estáveis, próprios para um ambiente de produção e Z identifica a versão corrente [FRE99].

A versão mais atual de *kernel* estável inicia-se com 2.2 e a versão mais atual em desenvolvimento inicia-se com 2.1. O suporte para IPv6 está presente em ambas as versões a título de "em desenvolvimento". É recomendado que se trabalhe com o *kernel* superior à versão 2.2.10 [BIE00].

Antes de detalhar os passos para configurar o protocolo IPv6, leia com atenção a seguinte citação de *Craig Metz*, um dos projetista do IPv6 para *Linux*, em [BIE00] :

> *"IPv6 é, antes de tudo, algo ainda experimental e a sua implementação ainda tem muito a desejar. Eu não acho que muitas pessoas entendam realmente isso e então eles esperam muito mais do que atualmente existe."*

Para fazer com que o *Linux* suporte o IPv6 é necessário um conhecimento avançado no sistema operacional envolvendo tarefas que vão desde a re-compilação do *kernel*, à configuração de rede através de *scripts*.

1.3.1. Passos para a instalação da pilha TCP/IPv6 :

Os passos aqui descritos dizem respeito ao *RedHat Linux* 6.1, *kernel* 2.2.12-20, com instalação completa (mas sem jogos e aplicativos que não dizem respeito ao funcionamento básico do sistema operacional). Eles se basearam no documento [BIE00] e [FRE99] com algumas mudanças devido a incompatibilidades encontradas no processo de instalação.

1. Configurando o *kernel* para suporte ao IPv6

   Para informar ao *kernel* para ativar o suporte ao IPv6 é necessário executar arquivo ***config*** que possui as entradas de parâmetros dos módulos implementados pelo sistema operacional. Uma forma mais amigável de realizar esta tarefa é utilizar o aplicativo *menuconfig*.

   Uma vez executado o aplicativo basta selecionar as opções desejadas e então seguir para o passo seguinte de compilação do *kernel*. A listagem de comandos abaixo ilustram como fazer a configuração dos parâmetros dos módulos do kernal para suportar o IPv6. O texto que se segue ao simbolo # é apenas um comentário, não sendo necessário a sua digitação.

   ```
   %cd /usr/src/linux        # Diretório dos arquivos fontes do Linux
   %make menuconfig          # Comando para executar o aplicativo menuconfig
   ```

A Fig. 23 apresenta a tela padrão do *menuconfig*.

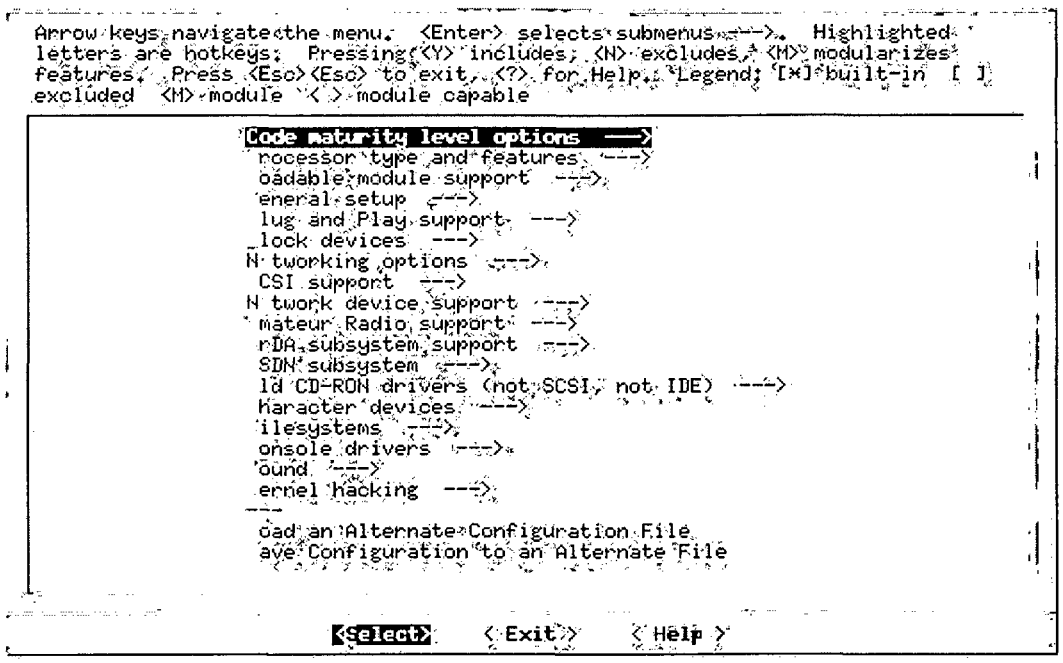

FIGURA 23 : TELA PADRÃO DO MENUCONFIG

Um menu em cascata é apresentado. Como o código de suporte ainda está em desenvolvimento selecione o menu :

Code Maturity Level Options

Neste menu marque a opção :

[*] Prompt for development and/or incomplete code/drivers

Esta opção deve ser selecionada com o simbolo [*] assim como todas as outras que forem indicadas.

As próximas entradas estão sob o menu :

Networking Options

Selecione a opção :

<*> The IPv6 Protocol

Para indicar o uso do protocolo IPv6.

Para habilitar o padrão de endereçamento utilizado no 6Bone selecione a opção seguinte :

[*] enable EUI-64 token format

Como a máquina com o sistema operacional *Linux* foi escolhida para ser o roteador entre as sub-redes, é necessário informar ao *kernel* as entradas para roteamento :

[*] IP : optimize as router not host
[*] IP : advanced router
[*] IP : policy routing

Para informações mais detalhadas a respeito de cada opção selecionada ou para outras opções apresentadas nos menus deve-se fazer uma consulta aos manuais *on-line* disponíveis no site da *RedHat* (http://www.redhat.com).

2. Compilando o *kernel* com as entradas de módulos modificadas.

Para compilar o *kernel* execute a seqüência de comandos, um após o outro :

```
%make dep
%make clean
%make zlilo     # caso ocorra erro utilize make bzImage ou consulte manual
%make modules
%make modules_install
```

Deve-se reiniciar sistema operacional :

```
%shutdown –r 0
```

Se o sistema reiniciar sem nenhum problema, as mudanças realizadas podem ser efetivadas :

```
%cd /usr/src/linux
%make install
```

O sistema operacional deve, novamente ser reinicializado :

```
%shutdown –r 0
```

3. Modificando os arquivos de configuração de protocolos e *hosts* para o suporte a IPv6.

Deve-se fazer algumas inclusões nos arquivos ***/etc/hosts*** e ***/etc/protocols*** para que o IPv6 funcione corretamente.

No arquivo ***/etc/hosts*** inclua as seguintes linhas :

```
::1             ip6-localhost ip6-loopback
fe00::0         ip6-localnet
ff00::0         ip6-mcastprefix
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
ff02::3         ip6-allhosts
```

No arquivo ***/etc/protocols*** inclua as seguintes linhas :

```
ipv6            41      IPv6            # IPv6
ipv6-route      43      IPv6-Route      # Routing Header for IPv6
ipv6-frag       44      IPv6-Frag       # Fragment Header for IPv6
ipv6-crypt      50      IPv6-Crypt      # Encryption Header for IPv6
ipv6-auth       51      IPv6-Auth       # Authentcation Header for IPv6
icmpv6          58      IPv6-ICMP       # ICMP for IPv6
ipv6-nonxt      59      IPv6-NoNxt      # No Next Header for IPv6
ipv6-opts       60      IPv6-Opts       # Destination Options for IPv6
```

4. Instalando as aplicações clientes da rede com suporte ao IPv6.

A partir deste momento, é necessário instalar as aplicações clientes de rede com suporte ao IPv6, em [BIE00] são listados alguns pacotes com os respectivos aplicativos. Na configuração desta rede foi utilizado um pacote conseguido junto ao NPD (Núcleo de Processamento de Dados) da Universidade Federal de Santa Catarina, o ***ipv6pkg.tgz***, o mesmo sugerido por [FRE99].

Por questões de segurança é recomendável fazer uma cópia de cada aplicativo que será substituído, já que as aplicações terão o mesmo nome que

tinham as que suportavam apenas o IPv4. Para fazer a cópia dos aplicativos execute os comandos:

```
% cp /sbin/ifconfig /sbin/ifconfig.old
% cp /sbin/route /sbin/route.old
% cp /bin/ping /bin/ping.old
% cp /usr/bin/ftp /usr/bin/ftp.old
% cp /usr/bin/telnet /usr/bin/telnet.old
% cp /bin/hostname /bin/hostname.old
% cp /bin/netstat /bin/netstat.old
% cp /usr/bin/finger /usr/bin/finger.old
% cp /usr/bin/tftp /usr/bin/tftp.old
% cp /sbin/arp /sbin/arp.old
% cp /usr/sbin/traceroute /usr/sbin/traceroute.old
% cp /sbin/rarp /sbin/rarp.old
```

O pacote já pode ser instalado :

```
%cd /
%tar –zxvpf /apps/ipv6pkg.tgz
```

Assim, todo um conjunto completo de aplicativos e utilitários portados para o IPv6 foi descompactado no diretório ***/usr/inet6***, a maior parte deles usa a biblioteca libinet6.a (incluída no *package*), portando o próximo passo é disponibilizá-la para qualquer aplicação, através da criação de um *link* :

```
% ln -sf /usr/inet6/lib/libinet6.a /usr/lib/libinet6.a
```

Agora basta criar os links simbólicos para todos os aplicativos clientes portados no sistema :

```
# ln -sf /usr/inet6/sbin/ifconfig /sbin/ifconfig
# ln -sf /usr/inet6/sbin/route /sbin/route
# ln -sf /usr/inet6/bin/ping /bin/ping
# ln -sf /usr/inet6/bin/ftp /usr/bin/ftp
# ln -sf /usr/inet6/bin/telnet /usr/bin/telnet
# ln -sf /usr/inet6/bin/hostname /bin/hostname
# ln -sf /usr/inet6/bin/netstat /bin/netstat
# ln -sf /usr/inet6/bin/finger /usr/bin/finger
# ln -sf /usr/inet6/bin/tftp /usr/bin/tftp
# ln -sf /usr/inet6/sbin/arp /sbin/arp
# ln -sf /usr/inet6/sbin/traceroute /usr/sbin/traceroute
# ln -sf /usr/inet6/sbin/rarp /sbin/rarp
```

A pilha TCP/IPv6 está configurada já podendo ser manipulada. O comando *ifconfig* deve apresentar a configuração de cada interface de rede configurada, que no caso específico do computador com o *Linux* são duas interfaces físicas.

```
% ifconfig
```

A resposta a este comando é apresentada no Quadro 3 abaixo :

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

eth0      Link encap:Ethernet  HWaddr 52:54:00:E6:B3:A1
          inet addr:10.10.10.10
          Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::5054:ff:fee6:b3a1/10 Scope:Link
          inet6 addr: fe80::5254:e6:b3a1/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0xde00

eth1      Link encap:Ethernet  HWaddr 00:40:C7:11:9F:39
          inet addr:10.11.10.10
          Bcast:10.11.255.255  Mask:255.255.0.0
          inet6 addr: fe80::40:c711:9f39/10 Scope:Link
          inet6 addr: fe80::240:c7ff:fe11:9f39/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:5 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:3 Base address:0x300
```

QUADRO 3 : COMANDO *IFCONFIG*

Se o endereço no formato do IPv6 não aparecer, então deve-se reiniciar sistema operacional e novamente executar o comando *ifconfig*:

%shutdown –r 0

Configurando o Roteamento Entre as Subredes IPv6

1.3.2. Configurando o Roteamento Entre as Subredes IPv6

A rede IPv6 utilizada na coleta dos dados é constituída por duas sub-redes que tem como roteador a estação configurada com o sistema operacional *Linux* com duas interfaces de redes, que são responsáveis pela interligação das subredes. Cada interface de rede desta estação está configurada com um endereço *site-local*.

É necessário criar alguns *scripts* para que o endereço *site-local* e as regras de roteamento entre as sub-redes sejam configurados sempre que a rede for inicializada. Não há uma interface gráfica que auxilie nesta tarefa, assim, comandos devem ser colocados em um arquivo e este por sua vez executado quando se desejar utilizar a rede IPv6.

Para a rede em questão estão sendo utilizados alguns *scripts* propostos em [BIE00] mais atualizações em alguns arquivos de configuração da rede. Como o ambiente é experimental, toda a configuração do roteador é executada através da chamada manual do *script*, o processo não foi automatizado através dos arquivos de inicialização do *Linux*.

Os *scripts* propostos por [BIE00] são : ***functions-ip6***, ***ifup-routes***, ***network-ip6***, ***network-ip6.conf***, ***network-ip6.init***, ***radvd.init***, ***static-routes*** e ***tunnels-ip6.init***. Eles estão disponíveis no próprio documento. Destes ***ifup-routes***, ***radvd.init***, ***static-routes e tunnels-ip6.init*** não foram explorados, por não serem importantes no escopo da coleta de dados realizada. O arquivo ***network-ip6.init*** é o arquivo de inicialização principal. A partir dele todos os outros *scripts* são executados e os arquivos de configuração lidos. Ele deve ser colocado no diretório ***/etc/rc.d/init.d*** e nenhuma modificação é necessária nele. Para executa-lo, digite o seguinte comando :

```
% cd /etc/rc.d/init.d
% ./network-ip6.init start      # Eh necessaria a opção start para ativar o script
```

Outro arquivo que fica no diretório ***/etc/rc.d/init.d*** e também é um *script* para configuração dos parâmetros de configuração do protocolo IPv6 é o ***functions-ip6***. Ele também deve ser copiado como sugerido em [BIE00].

Para terminar a configuração estão faltando apenas os arquivos com as entradas para configuração dos serviços oferecidos pelo IPv6. São os arquivos ***network-ip6 e network-ip6.conf*** que devem ser armazenados no diretório ***/etc/sysconfig***.

No arquivo ***network-ip6.conf*** são especificados os endereços para as interfaces de rede. Aqui mais de um endereço pode ser especificado para cada interface, criando as pseudo-interfaces. Também são especificadas as rotas possíveis para o serviço de envio de datagramas entre as sub-redes. Mais de uma rota pode ser especificada, desde que haja necessidade. O Quadro 4 mostra a configuração utilizada na estação *Linux* da rede IPv6 utilizada para a coleta de dados.

```
#!F:network-ip6.conf
#!P:/etc/sysconfig
#!O:root:root
#!M: 440
#!D:IPv6 configuration file
#!C:Copyright 1997-1999 Peter Bieringer <pb@bieringer.de>
#!V:Version 2.13 1999-06-26

# Changes to
#  2.11: nothing important
#  2.12: NBMA tunnel configuration ready
#  2.13: Review

# This file is needed by 'functions-ip6' version 2.xx

### The order in the file is only for a good overview, it is not
### really
### necessary. The important values are 'device' and 'key'!

################# Tunnel section

#####################################################################
# Configuracoes desprezadas, pois nao foi implementado tunel        #
#####################################################################

################# Interface section

## Here you can specify several addresses for your interfaces.
## More than one are possible!

#Device     Key   prefix            suffix            length
#eth0 iface fec0:0:0:1  0:0:0:1                  64
eth0  iface fec0:1000   0:0:5054:ff:fee6:b3a1   32
eth1  iface fec0:1100   0:0:240:c7ff:fe11:9f39  32

################ Gateway section

## Here you can specify several routes to your gateway.
## More than one are possible!

#Device     Key   Gateway address                    Network
#eth0 route fec0:0:0:1:0:0:0:20               fec0:0:0:2::/64
eth0  route fec0:1000::5054:ff:fee6:b3a1      fec0:1000::/32
eth1  route fec0:1100::240:c7ff:fe11:9f39     fec0:1100::/32
```

QUADRO 4 : ARQUIVO ***NETWORK-IP6.CONF***

No arquivo ***network-ip6***, listado no Quadro 5, pode-se informar se a rede Ipv6 será ou não habilitada, se a estação será um gateway para rede, se ela poderá realizar o serviço de envio de datagramas IPv6, o *IPv6Forwarding*, ou realizará tunelamento de

IPv4 sobre IPv6, entre outros serviços. Para habilitar ou desabilitar cada serviço basta colocar o respectivo parâmetro dentre os valores sugeridos.

```
#!F:network-ip6
#!P:/etc/sysconfig
#!D:IPv6 network configuration file
# Changes to:
#  1.11: add IP6FORWARDING switch (to differ between a host and a
#router)
## IPv6 configuration debugging
# Bit0: show all commands, bit1:don't execute anything
IP6DEBUG=0
## IPv6 network configuration? {yes|no}
IP6NETWORKING=yes

# Take information from the file
IP6INTERFACEFILE=/etc/sysconfig/network-ip6.conf

## Gateway network configuration
# for i.e. routing IPv6 packages over local IPv6 routers
# similar to the default gateway in IPv4)
# Allow gateway configurations {yes|no}
IP6GATEWAYCONFIG=yes

# Take information from the file
IP6ROUTEFILE=/etc/sysconfig/network-ip6.conf

# Allow forwarding option, host is a router {yes|no}
IP6FORWARDING=yes

## IPv6 tunnels
# for tunneling IPv6 packages over IPv4 routers to a IPv6 tunnel
#endpoint
# i.e. 6bone connection, ask a 6bone partner near your location for
#set up
# tunnel to you
# Allow IPv6 tunnel interface configuration {yes|no}
# modifiquei para no em 31/03/2000
IP6TUNNELCONFIG=no

# Take information from the file
#IP6TUNNELFILE=/etc/sysconfig/network-ip6.conf

## Router Advertisement Daemon
# Start Daemon {yes|no}
IP6RADVD=no

# Sepcify configuration file
#IP6RADVDFILE="/usr/inet6/etc/radvd.conf"
#IP6RADVDFILE="/etc/sysconfig/radvd.conf"
# Specify options
#IP6RADVDOPTIONS=""
#IP6RADVDOPTIONS="-d 9"
```

QUADRO 5 : ARQUIVO ***NETWORK-IP6.***

Por algum motivo o serviço de *IPv6Forwarding* não foi acionado. Como sugestão de solução optou-se por utilizar os mesmos parâmetros para ativação deste serviço no IPv6, junto ao arquivo ***network***, utilizado pelo IPv4. Esta solução mostrou-se satisfatória, permitindo o bom funcionamento do serviço de roteamento. O arquivo ***network*** fica no diretório ***/etc/sysconfig*** e tem a mesma função que o ***network-ip6***, porém para redes IPv4. O Quadro 6 apresenta o arquivo com as alterações.

```
#/etc/sysconfig/network

NETWORKING=yes
IP6NETWORKING=yes
FORWARD_IPV4=yes
IP6FORWARDING=yes
HOSTNAME=pluck
IP6HOSTNAME=pluck6
GATEWAY=
GATEWAYDEV=
IP6GATEWAYCONFIG=yes
```

QUADRO 6 : ARQUIVO ***NETWORK***

Devido a essa mudança a estação de ser reiniciada :

%shutdown –r 0

Uma vez configurado todos os arquivos é necessário, então, executar um pequena seqüência de comandos que podem, inclusive serem adicionados a um novo *script*. Nesta seqüência, primeiro, são eliminados os endereços *link-local* sugeridos pelo serviço de configuração automática do IPv6, chamado de *Neighbor Discovery*. Então o arquivo ***network-ip6.init*** deve ser executado. Os comandos se seguem :

```
%ifconfig eth0 del fe80::5054:ff:fee6:b3a1/10     # Apaga o endereco 1 da eth0
%ifconfig eth0 del fe80::5254:e6:b3a1/10          # Apaga o endereco 2 da eth0
%ifconfig eth1 del fe80::240:c7ff:fe11:9f39/10    # Apaga o endereco 1 da eth1
%ifconfig eth1 del fe80::40:c711:9f39/10          # Apaga o endereco  2 da eth1
% cd /etc/rc.d/inet.d
%./network-ip6.init start          # Iniciando a configuração das interfaces
```

Como teste para confirmar a configuração das interfaces de rede o seguinte comando pode ser passado na linha de comando :

%ifconfig

Uma listagem parecida com o do Quadro 7 deverá ser mostrada. O novo endereço *site-local* configurado em ***network-ip6.conf*** deve aparecer.

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

eth0      Link encap:Ethernet  HWaddr 52:54:00:E6:B3:A1
          inet addr:10.10.10.10  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fec0:1000::5054:ff:fee6:b3a1/32 Scope:Site
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2098 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0xde00

eth1      Link encap:Ethernet  HWaddr 00:40:C7:11:9F:39
          inet addr:10.11.10.10  Bcast:10.11.255.255  Mask:255.255.0.0
          inet6 addr: fec0:1100::240:c7ff:fe11:9f39/32 Scope:Site
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:6 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:3 Base address:0x300
```

QUADRO 7 : LISTAGEM DO COMANDO ***IFCONFIG***

O comando ***route*** mostrará a nova configuração da tabela de roteamento. O Quadro 8 apresenta a tabela de roteamento para a estação *Linux* utilizada na rede em que foi feita a coleta de dados.

%route –A inet6

```
Kernel IPv6 routing table
Destination                    Next Hop                   Flags Metric Ref Use Iface
::1/128                        ::0                        U     0      0     0 lo
fe80::0/10                     ::0                        UA    256    0     0 eth0
fe80::0/10                     ::0                        UA    256    0     0 eth1
fec0:1000::5054:ff:fee6:b3a1/128 ::0                      U     0      0     0 lo
fec0:1000::0/32                ::0                        U     1      1     0 eth0
fec0:1000::0/32                fec0:1000::5054:ff:fee6:b3a1 UG    1      0     0 eth0
fec0:1000::0/32                ::0                        UA    256    0     0 eth0
fec0:1100::240:c7ff:fe11:9f39/128::0                      U     0      0     0 lo
fec0:1100::0/32                ::0                        U     1      1     0 eth1
fec0:1100::0/32                fec0:1100::240:c7ff:fe11:9f39 UG    1      0     0 eth1
fec0:1100::0/32                ::0                        UA    256    0     0 eth1
ff00::0/8                      ::0                        UA    256    0     0 eth0
ff00::0/8                      ::0                        UA    256    0     0 eth1
```

QUADRO 8 : LISTAGEM DO COMANDO ***ROUTE***

A configuração da rede utilizada para esta dissertação levou seis dias para ser concluída, mais outros seis para ser considerada apta para os testes. Essa demora ocorreu devido a pouca documentação existente e às constantes mudanças de estruturas nos arquivos de configuração de rede existentes no *Linux*. Até mesmo para instalar uma segunda placa de rede no *Linux* houve dificuldades, pois o software gráfico utilizado, o *linuxconf*, não estava gravando a configuração passada a ele no arquivo de inicialização correspondente, assim a cada reinicialização do sistema operacional as configurações da segunda placa de rede eram descartadas e ela não funcionava.

Apesar de que outras redes IPv6 já foram configuradas no âmbito da Universidade Federal de Santa Catarina, principalmente no Núcleo de Processamento de Dados (NPD), em nenhuma delas tinham a documentação da existência de um *script* de roteamento, sendo que na documentação existente, nem ao menos fora citado o uso de roteamento para a rede.

As aplicações dos clientes de rede ainda não estão integradas para funcionar tanto para IPv4 quanto para IPv6, mas já existem alguns pacotes disponibilizados na Internet que indicam a possibilidade desta integração, como o ***IPv6pkg.tgz*** utilizado nesta implementação. Assim possibilitará uma maior facilidade na configuração do

IPv6, pois os conhecimentos acumulados com o IPv4, no que diz respeito a sintaxe e semântica de comandos, poderão auxiliar na resolução de problemas.

A expectativa é que este documento auxilie na implementação de novas redes, minimizando o tempo despendido na montagem e configuração dos elementos de rede para o IPv6.

ANEXO 2 : DADOS COLETADOS NA REDE IPV6

2.1. Considerações Iniciais

Neste anexo estão listados os valores de tempo de propagação do datagrama na rede IPv6 utilizada para a avaliação analítica. Todos os gráficos e análises realizadas neste trabalho referenciam-se a esses dados.

2.2. Dados Recolhidos entre a Estação 1 e a Estação *Router*

As tabelas Tab. 1, Tab. 2 e Tab. 3, apresentam os dados recolhidos durante medidas realizadas entre a Estação 1 e a Estação *Router*, dentro da mesma sub-rede, para o protocolo IPv4 com cargas de 64 bytes, 750 bytes e 1500 bytes respectivamente. Como as medidas foram feitas com diferentes cargas, cada tabela informa em seu cabeçalho o protocolo e a carga correspondente à medição.

As tabelas Tab. 4, Tab. 5 e Tab. 6, apresentam os dados recolhidos nas medidas realizadas entre a Estação 1 e a Estação *Router*, dentro da mesma sub-rede, para o protocolo IPv6 com cargas de 64 bytes, 750 bytes e 1500 bytes respectivamente.

IPv4 – 64 bytes

TABELA 1 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 64 BYTES

1,391	0,473	0,475	0,471	0,471	0,475	0,472	0,473	0,484	0,473
0,494	0,489	0,471	0,47	0,471	0,471	0,471	0,475	0,473	0,473
0,474	0,481	0,476	0,473	0,544	0,472	0,47	0,476	0,474	0,474
0,469	0,472	0,472	0,473	0,473	0,471	0,472	0,472	0,505	0,471
0,482	0,476	0,473	0,476	0,478	0,475	0,476	0,471	0,477	0,477
0,475	0,474	0,471	0,473	0,471	0,478	0,475	0,474	0,477	0,475
0,471	0,473	0,473	0,472	0,471	0,47	0,474	0,473	0,471	0,471
0,473	0,486	0,471	0,471	0,471	0,472	0,476	0,475	0,474	0,473
0,472	0,47	0,471	0,471	0,475	0,471	0,471	0,475	0,476	0,477
0,481	0,473	0,471	0,471	0,476	0,474	0,476	0,473	0,473	

IPv4 – 750 bytes

TABELA 2 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 750 BYTES

2,856	2,185	2,178	2,18	2,174	2,183	2,243	2,181	2,174	2,171
2,176	2,172	2,177	2,174	2,191	2,187	2,173	2,177	2,182	2,173
2,173	2,173	2,178	2,175	2,173	2,174	2,178	2,174	2,173	2,176
2,175	2,181	2,176	2,177	2,172	2,174	2,176	2,18	2,175	2,173
2,175	2,173	2,174	2,174	2,18	2,273	2,177	2,179	2,182	2,175
2,238	2,174	2,179	2,18	2,173	2,174	2,172	2,18	2,179	2,174
2,173	2,175	2,174	2,175	2,173	2,175	2,176	2,18	2,175	2,175
2,182	2,17	2,176	2,175	2,179	2,177	2,174	2,177	2,178	2,176
2,269	2,174	2,174	2,183	2,178	2,174	2,175	2,176	2,175	2,18
2,182	2,172	2,179	2,176	2,175	2,176	2,188	2,176	2,176	

IPv4 – 1500 bytes

TABELA 3 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 1500 BYTES

4,109	4,029	4,025	4,02	4,026	4,09	4,018	4,031	4,022	4,044
4,023	4,019	4,021	4,024	4,019	4,04	4,04	4,025	4,023	4,029
4,028	4,018	4,017	4,027	4,025	4,022	4,017	4,022	4,016	4,029
4,023	4,033	4,027	4,017	4,018	4,034	4,018	4,018	4,035	4,033
4,026	4,017	4,019	4,015	4,023	4,025	4,031	4,091	4,019	4,026
4,029	4,026	4,078	4,018	4,031	4,028	4,022	4,024	4,018	4,025
4,02	4,018	4,033	4,021	4,019	4,025	4,018	4,022	4,016	4,022
4,031	4,016	4,028	4,016	4,022	4,029	4,028	4,034	4,025	4,028
4,02	4,018	4,017	4,016	4,02	4,031	4,024	4,028	4,017	4,029
4,02	4,023	4,025	4,029	4,03	4,023	4,018	4,02	4,017	

IPv6 – 64 bytes

TABELA 4 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 64 BYTES

1,445	0,552	0,57	0,542	0,553	0,546	0,562	1,444	0,571	0,56
0,568	0,574	0,551	0,535	0,549	0,568	0,555	1,477	0,653	0,585
0,553	0,551	0,546	0,546	0,539	0,547	1,053	0,576	1,432	0,588
0,572	0,602	0,654	0,554	0,533	0,535	0,558	0,556	0,558	0,553
0,556	0,539	0,549	0,54	0,543	1,146	1,431	0,594	0,557	0,542
0,538	0,538	0,537	0,609	0,55	0,541	0,551	0,553	0,556	0,539
0,549	0,599	0,591	0,551	0,533	0,546	0,541	0,707	0,73	0,546
0,68	0,555	0,599	0,602	0,654	0,554	0,533	0,535	0,546	0,61
0,542	0,538	0,532	0,558	0,571	0,564	0,535	0,539	0,531	0,56
0,564	0,563	0,539	0,54	0,588	0,554	0,581	0,535	0,539	

IPv6 – 750 bytes

TABELA 5 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 750 BYTES

3,125	2,382	2,261	2,262	2,261	2,247	2,249	3,139	2,293	2,26
2,261	2,266	2,262	2,247	2,254	2,758	3,206	2,284	2,253	2,257
2,246	2,24	2,241	2,246	2,24	2,235	2,279	2,291	2,265	2,246
2,265	2,296	2,266	2,257	2,254	2,285	2,252	2,243	2,251	2,286
2,253	2,254	2,263	2,285	2,243	2,246	2,242	2,378	2,268	2,25
2,244	2,281	2,275	2,248	2,251	2,295	2,258	2,248	2,244	2,28
2,282	2,248	2,252	2,306	2,265	2,243	2,249	2,281	2,266	2,247
2,288	2,319	2,259	2,246	2,24	2,241	2,312	2,251	2,261	2,239
2,235	2,333	2,248	2,24	2,266	2,248	2,282	2,342	2,259	2,26
2,251	2,349	2,261	2,264	2,266	2,256	2,291	2,282	2,278	

IPv6 – 1500 bytes

TABELA 6 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 1500 BYTES

5,086	4,148	4,102	4,221	4,093	4,176	4,115	4,176	4,087	4,098
4,09	4,211	4,103	5,086	4,123	4,101	4,089	4,1	5,134	4,18
4,088	4,191	4,097	4,132	4,125	4,096	4,111	4,149	4,103	4,109
4,234	4,107	4,092	4,09	4,104	4,091	4,121	4,087	4,112	4,191
4,107	4,093	4,093	4,158	4,142	4,086	4,088	4,146	4,132	4,176
4,105	4,204	4,116	4,111	4,113	4,119	4,093	4,081	4,091	4,176
4,087	4,098	4,09	4,142	4,086	4,088	4,146	4,16	4,105	4,091
4,099	4,253	4,155	4,115	4,106	4,247	4,121	4,115	4,086	4,191
4,107	4,093	4,093	4,117	4,103	4,089	4,098	4,316	4,289	4,278
4,274	4,162	4,133	4,099	4,092	4,18	4,088	4,191	4,097	

2.3. Dados Recolhidos na Estação *Router*

As tabelas Tab. 7, Tab. 8 e Tab. 9, apresentam os dados recolhidos durante medidas realizadas na Estação *Router*, responsável por permitir a comunicação entre as sub-redes, para o protocolo IPv4 com cargas de 64 bytes, 750 bytes e 1500 bytes respectivamente. Como as medidas foram feitas com diferentes cargas, cada tabela informa em seu cabeçalho o protocolo e a carga correspondente à medição.

As tabelas Tab. 10, Tab. 11 e Tab. 12, apresentam os dados recolhidos nas medidas realizadas na Estação *Router* para o protocolo IPv6 com cargas de 64 bytes, 750 bytes e 1500 bytes respectivamente.

IPv4 – 64 bytes

TABELA 7 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 64 BYTES

0,41	0,102	0,093	0,092	0,092	0,091	0,109	0,093	0,091	0,09
0,091	0,096	0,092	0,091	0,092	0,093	0,094	0,093	0,09	0,089
0,091	0,092	0,092	0,091	0,091	0,091	0,096	0,093	0,09	0,092
0,092	0,095	0,093	0,104	0,091	0,09	0,094	0,092	0,09	0,09
0,09	0,096	0,093	0,09	0,095	0,093	0,094	0,093	0,09	0,091
0,091	0,091	0,092	0,091	0,092	0,091	0,096	0,093	0,089	0,091
0,093	0,093	0,093	0,093	0,091	0,091	0,094	0,095	0,091	0,092
0,091	0,091	0,093	0,091	0,091	0,093	0,094	0,093	0,091	0,091
0,092	0,092	0,092	0,091	0,09	0,09	0,094	0,091	0,089	0,091
0,093	0,094	0,093	0,101	0,092	0,091	0,095	0,093	0,091	

IPv4 – 750 bytes

TABELA 8 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 750 BYTES

0,444	0,111	0,107	0,104	0,111	0,107	0,105	0,106	0,105	0,118
0,108	0,104	0,106	0,104	0,107	0,107	0,105	0,105	0,105	0,109
0,11	0,104	0,105	0,105	0,106	0,107	0,105	0,105	0,104	0,109
0,108	0,104	0,11	0,104	0,105	0,112	0,12	0,105	0,106	0,109
0,108	0,104	0,106	0,104	0,108	0,107	0,105	0,107	0,105	0,108
0,11	0,104	0,104	0,104	0,106	0,107	0,105	0,105	0,104	0,11
0,107	0,104	0,108	0,104	0,107	0,107	0,109	0,104	0,105	0,11
0,108	0,105	0,105	0,105	0,109	0,107	0,105	0,104	0,105	0,107
0,111	0,104	0,106	0,104	0,106	0,109	0,106	0,105	0,104	0,11
0,107	0,104	0,108	0,104	0,106	0,114	0,121	0,105	0,105	

IPv4 – 1500 bytes

TABELA 9 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 1500 BYTES

0,447	0,136	0,119	0,121	0,119	0,124	0,12	0,119	0,119	0,12
0,15	0,12	0,12	0,119	0,117	0,122	0,119	0,119	0,117	0,117
0,122	0,12	0,118	0,119	0,118	0,122	0,124	0,12	0,119	0,117
0,123	0,121	0,117	0,119	0,117	0,121	0,123	0,131	0,118	0,119
0,122	0,121	0,12	0,119	0,117	0,122	0,121	0,118	0,119	0,119
0,123	0,12	0,117	0,118	0,118	0,12	0,124	0,12	0,118	0,117
0,124	0,12	0,119	0,12	0,118	0,125	0,12	0,123	0,119	0,12
0,122	0,121	0,119	0,118	0,118	0,122	0,121	0,119	0,117	0,119
0,122	0,12	0,117	0,117	0,117	0,119	0,121	0,12	0,118	0,118
0,124	0,121	0,118	0,12	0,118	0,12	0,123	0,131	0,118	

IPv6 – 64 bytes

TABELA 10 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 64 BYTES

0,332	0,079	0,058	0,058	0,06	0,059	0,067	0,058	0,058	0,058
0,057	0,062	0,057	0,06	0,059	0,056	0,062	0,062	0,069	0,065
0,059	0,061	0,057	0,057	0,057	0,057	0,06	0,057	0,058	0,058
0,057	0,062	0,057	0,058	0,06	0,059	0,062	0,06	0,058	0,059
0,057	0,061	0,057	0,06	0,058	0,058	0,062	0,057	0,058	0,059
0,056	0,062	0,061	0,058	0,057	0,057	0,065	0,058	0,058	0,058
0,057	0,064	0,057	0,058	0,06	0,059	0,061	0,058	0,058	0,058
0,057	0,062	0,057	0,06	0,059	0,057	0,064	0,058	0,064	0,06
0,059	0,062	0,057	0,057	0,058	0,058	0,06	0,057	0,058	0,058
0,057	0,061	0,058	0,059	0,06	0,059	0,063	0,058	0,058	

IPv6 – 750 bytes

TABELA 11 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 750 BYTES

0,282	0,074	0,071	0,065	0,063	0,063	0,063	0,072	0,064	0,064
0,063	0,064	0,071	0,064	0,063	0,062	0,063	0,067	0,065	0,064
0,064	0,063	0,068	0,062	0,066	0,066	0,063	0,068	0,063	0,064
0,064	0,064	0,069	0,065	0,063	0,063	0,063	0,066	0,063	0,064
0,063	0,065	0,07	0,064	0,066	0,066	0,063	0,067	0,065	0,064
0,063	0,066	0,068	0,064	0,065	0,064	0,063	0,071	0,063	0,073
0,064	0,063	0,068	0,066	0,063	0,064	0,063	0,066	0,063	0,063
0,063	0,063	0,068	0,063	0,062	0,063	0,063	0,068	0,065	0,066
0,064	0,063	0,07	0,065	0,065	0,063	0,063	0,066	0,062	0,064
0,065	0,063	0,068	0,065	0,063	0,063	0,063	0,066	0,063	

IPv6 – 1500 bytes

TABELA 12 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 1500 BYTES

0,191	0,079	0,072	0,076	0,07	0,071	0,074	0,068	0,083	0,068
0,07	0,071	0,069	0,076	0,072	0,07	0,071	0,068	0,076	0,068
0,07	0,068	0,069	0,074	0,071	0,068	0,071	0,069	0,074	0,068
0,071	0,07	0,072	0,074	0,071	0,071	0,075	0,069	0,077	0,068
0,081	0,069	0,07	0,075	0,07	0,07	0,073	0,067	0,075	0,068
0,07	0,071	0,071	0,073	0,071	0,068	0,071	0,069	0,076	0,068
0,071	0,069	0,073	0,074	0,071	0,071	0,072	0,069	0,073	0,069
0,071	0,069	0,07	0,073	0,07	0,07	0,072	0,069	0,075	0,068
0,071	0,07	0,07	0,074	0,07	0,068	0,071	0,069	0,074	0,071
0,071	0,07	0,073	0,073	0,071	0,072	0,072	0,068	0,076	

2.4. Dados Recolhidos entre a Estação *Router* e a Estação 2

As tabelas Tabela 13, Tabela 14 e Tabela 15, apresentam os dados recolhidos durante medidas realizadas entre a Estação *Router* e Estação 2, dentro da mesma sub-rede, para o protocolo IPv4 com cargas de 64 bytes, 750 bytes e 1500 bytes respectivamente. Como as medidas foram feitas com diferentes cargas, cada tabela informa em seu cabeçalho o protocolo e a carga correspondente à medição.

As tabelas Tabela 16, Tabela 17 e Tabela 18, apresentam os dados recolhidos nas medidas realizadas entre a Estação *Router* e Estação 2, dentro da mesma sub-rede, para o protocolo IPv6 com cargas de 64 bytes, 750 bytes e 1500 bytes respectivamente.

IPv4 – 64 bytes

TABELA 13 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 64 BYTES

1,719	0,664	0,669	0,66	0,655	0,66	0,66	0,653	0,656	0,656
0,665	0,662	0,665	0,657	0,656	0,66	0,658	0,66	0,658	0,655
0,657	0,658	0,655	0,659	0,657	0,66	0,658	0,655	0,724	0,656
0,657	0,657	0,667	0,659	0,656	0,659	0,655	0,656	0,657	0,663
0,655	0,658	0,654	0,657	0,657	0,661	0,662	0,655	0,656	0,659
0,657	0,657	0,663	0,656	0,657	0,661	0,657	0,654	0,655	0,656
0,66	0,657	0,671	0,653	0,655	0,658	0,655	0,655	0,654	0,657
0,658	0,664	0,661	0,657	0,655	0,66	0,656	0,655	0,659	0,653
0,656	0,656	0,658	0,659	0,655	0,659	0,657	0,656	0,887	0,654
0,658	0,658	0,666	0,655	0,655	0,655	0,656	0,656	0,656	

IPv4 – 750 bytes

TABELA 14 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 750 BYTES

3,812	2,907	2,897	2,907	2,897	2,917	3,062	2,893	2,905	2,898
2,898	2,893	2,894	2,899	2,919	2,898	2,896	2,894	2,901	2,894
2,893	2,901	2,894	2,896	2,896	2,895	2,893	2,896	2,898	2,896
2,894	2,899	2,894	2,897	2,895	2,909	2,896	2,896	2,899	2,896
2,896	2,894	2,895	2,914	2,899	2,896	2,898	2,892	2,897	2,897
2,895	2,897	2,895	3,189	2,899	2,908	2,908	2,901	2,902	2,899
2,893	3,057	2,892	2,905	2,898	2,908	2,898	2,893	2,897	2,897
2,901	2,894	2,894	2,896	2,902	2,91	2,897	2,894	2,895	2,895
2,893	2,898	2,917	2,903	2,895	2,895	2,897	2,896	2,897	2,896
2,893	2,902	2,895	2,896	2,897	2,914	2,903	2,899	2,9	

IPv4 – 1500 bytes

TABELA 15 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV4 DE 1500 BYTES

5,542	5,494	5,482	5,476	5,499	5,649	5,479	5,475	5,482	5,504
5,475	5,476	5,47	5,476	5,478	5,482	5,481	5,472	5,474	5,477
5,48	5,47	5,481	5,477	5,474	5,478	5,477	5,486	5,48	5,477
5,484	5,473	5,506	5,477	5,484	5,482	5,475	5,476	5,474	5,474
5,478	5,478	5,478	5,473	5,487	5,479	5,484	5,476	5,475	5,477
5,494	5,479	5,481	5,473	5,483	5,481	5,488	5,504	5,479	5,483
5,481	5,476	5,655	5,472	5,483	5,488	5,476	5,471	5,473	5,473
5,479	5,477	5,487	5,472	5,482	5,485	5,475	5,476	5,481	5,485
5,481	5,472	5,481	5,473	5,48	5,482	5,485	5,491	5,474	5,476
5,482	5,475	5,493	5,477	5,477	5,475	5,478	5,476	5,475	

IPv6 – 64 bytes

TABELA 16 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 64 BYTES

1,846	0,756	0,74	0,827	0,744	0,758	0,734	0,741	0,756	0,754
0,741	0,734	0,754	0,734	0,781	0,75	0,74	0,748	0,752	0,753
0,734	0,742	0,78	0,764	0,742	0,77	0,744	0,772	0,889	0,827
0,954	0,849	0,819	0,772	0,802	0,734	0,737	0,776	0,787	0,738
0,805	0,827	0,764	0,742	0,742	0,734	0,796	0,775	0,743	0,735
0,781	0,75	0,74	0,734	0,786	0,806	0,785	0,77	0,75	0,748
0,75	0,747	0,763	0,74	0,748	0,749	0,837	0,739	0,735	0,73
0,827	0,756	0,754	0,741	0,734	0,755	0,755	0,739	0,74	0,741
0,772	0,746	0,752	0,741	0,785	0,77	0,75	0,748	0,767	0,759
0,732	0,74	0,744	0,758	0,734	0,741	0,741	0,771	0,734	

IPv6 – 750 bytes

TABELA 17 : TEMPO DE PROPAGAÇÃO DO DATAGRAMA IPV6 DE 750 BYTES

4,2	3,048	2,975	2,993	2,973	2,988	2,996	3,009	3,016	2,997
2,984	2,989	2,985	2,983	2,978	4,419	2,991	2,983	2,99	3,031
3,022	2,985	2,982	3,047	2,979	2,977	2,984	2,988	2,996	3,07
3,066	3,016	2,983	2,983	2,996	3,026	2,996	2,983	2,974	3,028
3,007	2,976	2,991	3,103	3,016	2,983	3,041	3,007	3,045	3,022
2,992	2,982	2,998	2,979	2,998	3,016	2,983	2,978	4,419	3,002
2,992	2,982	2,987	3,029	2,988	2,996	2,989	3,012	2,996	2,985
3,027	3,111	2,982	2,976	2,987	3,025	3,047	2,989	2,974	3,051
2,986	2,989	2,977	2,997	2,984	2,989	2,985	3,006	3,019	3,05
2,992	3,036	2,988	2,992	2,983	3,084	3,045	3,017	3,003	