UNIVERSIDADE DO EXTREMO SUL CATARINENSE
CURSO DE CIÊNCIA DA COMPUTAÇÃO

DIORDGENES TROMBIM

DIAGNÓSTICO DO TRÁFEGO DE REDE DE LABORATÓRIOS DE INFORMÁTICA.

ESTUDO DE CASO: UNIVERSIDADE DO EXTREMO SUL CATARINENSE

CRICIÚMA, JULHO DE 2006

DIORDGENES TROMBIM

DIAGNÓSTICO DO TRÁFEGO DE REDE DE LABORATÓRIOS DE INFORMATÍCA.

ESTUDO DE CASO: UNIVERSIDADE DO EXTREMO SUL CATARINENSE

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

Orientador: Prof. M.Sc. Rogério Antônio Casagrande

CRICIÚMA, JULHO DE 2006

DIORDGENES TROMBIM

DIAGNÓSTICO DO TRÁFEGO DE REDE DE LABORATÓRIOS DE INFORMÁTICA.

ESTUDO DE CASO: UNIVERSIDADE DO EXTREMO SUL CATARINENSE

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

_____
Profª M.Sc. Ana Claudia Garcia Barbosa
Coordenador(a) do Curso de Ciência da Computação

Banca Examinadora:

_____
Prof. M.Sc. Rogério Antônio Casagrande
Orientador

_____
Prof. M.Sc. Giovani Cascaes (SATC)

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

Dedico este trabalho à Deus que me proporcionou fé, força e persistência na busca por todos os objetivos para a conclusão deste curso.

AGRADECIMENTOS

A minha mãe, Sueli, por toda a ajuda prestada, pela educação, honra, honestidade e por mostrar que é enfrentando os maiores obstáculos que nos tornamos dignos e principalmente por fazer acreditar que sou capaz;

aos meus irmãos Alexandre e Renan pela compreensão por tantas vezes que estive ausente física e mentalmente;

aos funcionários do setor de informática da UNESC, por toda colaboração fornecida, possibilitando que a pesquisa pudesse ser realizada;

aos professores do curso, em especial ao meu orientador Rogério Antônio Casagrande, que além de fornecer a idéia do assunto deste trabalho, proporcionou todo o auxílio necessário para que as dificuldades encontradas, gradativamente fossem vencidas;

a todas as pessoas, principalmente amigos e parentes que de uma forma ou outra colaboraram para que este trabalho pudesse ser concluído;

e principalmente a Deus que a cada dia me proporciona mais felicidade diante das realizações e conquistas.

O valor das coisas não está no tempo que elas duram, mas na intensidade com que acontecem. Por isso existem momentos inesquecíveis, coisas inexplicáveis e pessoas incomparáveis.

Fernando Pessoa

RESUMO

Grande parte da utilização da Internet está envolvida diretamente com o dia-a-dia da população mundial, onde estabelecimentos corporativos são movimentados e mantidos essencialmente por meio de comunicação entre redes interligadas e informações são trocadas instantaneamente, independente da localização geográfica. Estas redes de computadores comportam a troca de informações e dados diversos, onde o controle sobre o fluxo destes dados muitas vezes torna-se impercebível. Este trabalho mostrou pela aplicação de uma técnica de amostragem estatística como foi possível analisar o conteúdo de tráfego da rede dos laboratórios da Universidade do Extremo Sul Catarinense. Foi aplicada a técnica de amostragem estratificada, possibilitando desta forma que amostras do tráfego de rede pudessem ser coletadas. O software Ethereal foi instalado no *proxy* dos laboratórios, que possui como sistema operacional o *LINUX*. Pela realização das coletas os dados foram armazenados em arquivos gerados pela própria ferramenta, onde posteriormente foi possível realizar a análise sobre estes arquivos. Nas demonstrações realizadas enfatizou-se principalmente o comportamento dos principais protocolos, aplicações e serviços encontrados, na sua maioria identificados por pertencerem à arquitetura *TCP/IP*, assim como a identificação da quantidade de pacotes que trafegaram sobre cada um deles.

Palavras-chave: Sniffer, Tráfego, Protocolos e Pacotes.

ABSTRACT

The great majority in the use of the Internet is involved directly with day-by-day of the worldwide population, where corporative establishments are put into motion and essentially kept by means of communication between linked networks and information they are changed very fast, independent of the geographic localization. These computer networks hold the diverse exchange of information and some else data, where the control on the flow of these data many times becomes imperceptible. This work showed for the application of one technique of statistics sampling, as it was possible to analyze the content of traffic of the network of the laboratories of the University of Extreme South Catarinense. The technique of extracting sampling was applied, making possible of this form that samples of the network traffic could be collected. The Ethereal software was installed in proxy of the laboratories, it has as operational system, the LINUX. By the accomplishment of the collections the data had been stored in archives generated for the proper tool, where later it was possible to carry through the analysis on these archives. In the demonstrations realized it was emphasized the main protocols, joined applications and services, in its majority identified by belonging to architecture TCP/IP, as well as the identification of the amount of packages that had passed through on each one of them.

Keywords: Sniffer, Traffic, Protocols and Packages.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ARP	*Address Resolution Protocol*
CEP	*Controle Estatístico de Processos*
DARPA	*Defense Advanced Research Projects Agency*
DNS	*Domain Name Service*
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
LAN	*Local Area Networks*
MAC	*Media Access Control*
NIC	*Network Interface Card*
RARP	*Reverse Address Resolution Protocol*
SMTP	*Simple Mail Transfer Protocol*
TCP	*Transmission Control Protocol*
TTL	*Time To Live*
UDP	*User Datagram Protocol*
WWW	*Word Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Atualmente, o acesso à informação e a agilidade em adquirir o conhecimento fazem a diferença nos negócios e na vida pessoal. Diferença essa, importante tanto para a parte de conhecimento pessoal, como também para o conhecimento dentro das organizações e empresas diversas.

Este trabalho visa mostrar de forma específica e centralizada, o tipo de informação e dados diversos que trafegam em redes corporativas.

Por meio de ferramentas de análise de tráfego de rede, os *Sniffers*, são mostradas informações e dados coletados por estes, onde de forma estatística estes dados serão expostos explicitamente, esclarecendo assim que tipo de dado trafega por tal rede. A rede analisada foi a dos laboratórios de informática da Universidade do Extremo Sul Catarinense. Foram definidos pontos estratégicos para análise, além de horários pré-definidos para coleta de dados.

Por meio de um software de análise de tráfego, o *Ethereal*, detalha-se a forma como a realização das coletas foi proporcionada, e como esta possibilitou a identificação do conteúdo coletado, permitindo a análise detalhada por meio dos arquivos armazenados. Esta ferramenta foi instalada no *proxy* dos laboratórios, onde por meio do monitoramento da interface de rede estes arquivos puderam ser gerados pela própria ferramenta.

Todo o conteúdo de dados coletados é mostrado de forma estatística e comparativa, especificando os tipos de dados que trafegam na rede.

1.1 OBJETIVO GERAL

Realizar um diagnóstico sobre o tráfego de rede dos Laboratórios de Informática da Universidade do Extremo Sul Catarinense.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos do trabalho consistem em:

a) estudar e aplicar o conhecimento sobre protocolos de comunicação em rede.
b) estudar e aplicar o conhecimento sobre ferramentas para análise de tráfego de rede.
c) realizar a amostragem dos dados;
d) demonstrar explicitamente o tipo de dados coletados por meio de amostras estatísticas.

1.3 JUSTIFICATIVA

Uma rede pode conter um enorme tráfego de dados e informações que provêm das estações e servidores. Dados estes que para trafegarem, sofrem um processo de

codificação, passando de informações alfanuméricas para bits. Esses bits ficam agrupados em forma de pacotes e então são transmitidos pela rede.

Sendo assim, não se tem mais um efetivo controle administrativo de quais pacotes estão trafegando, o destino destes pacotes, a sua origem, que dado está trafegando e principalmente o propósito de distribuição.

A utilização de ferramentas Sniffers visa identificar e mostrar a origem dos dados e as possíveis aplicações de onde estes são provenientes.

O propósito deste trabalho é o de mostrar o tipo de tráfego da rede, especificando e diagnosticando o conteúdo dos dados, gerando pesquisa, onde pela realização de amostragens estatísticas se possa ter noção e conhecimento do que se passa na rede, identificando, esclarecendo e possivelmente criando métodos para o controle deste tráfego. Não diferente de outras redes organizacionais, a da Universidade do Extremo Sul Catarinense possui um fluxo de dados intenso, onde muitos destes não possuem um propósito válido ou finalidade específica.

Este trabalho proporcionou um conhecimento claro diante de tais situações ou de até conceituados problemas, onde pela aplicação da ferramenta de análise de tráfego e demonstrações estatísticas realizadas dispôs à sociedade acadêmica um esclarecimento prático e facilitado diante das eventuais situações encontradas durante a pesquisa.

1.4 ESTRUTURA DO TRABALHO

A seguir é demonstrado de forma resumida o conteúdo de cada um dos capítulos existentes neste trabalho.

O primeiro capítulo demonstra uma visão geral deste trabalho, expondo os objetivos a serem alcançados.

O segundo capítulo descreve brevemente o histórico do surgimento da Internet, explica o funcionamento das redes de computadores e a comunicação de dispositivos por meio de protocolos de comunicação e também demonstra os principais protocolos pertencentes à arquitetura TCP/IP.

No terceiro capítulo pode ser visto o conceito atribuído aos sniffers, a funcionamento destes programas e a utilização destes nos diferentes segmentos de rede.

O capítulo quatro descreve alguns trabalhos correlatos a este.

O quinto capítulo descreve como foi realizada a análise do tráfego de rede dos laboratórios da Universidade do Extremo Sul Catarinense. É descrita a técnica de amostragem estatística utilizada para a definição dos horários e tempo de cada amostra, além de serem expostos as informações sobre os dados coletados e a forma como foi aplicada a ferramenta de análise de tráfego de rede a fim de possibilitar a identificação dos dados. Neste mesmo capítulo são descritas as dificuldades encontradas na realização da pesquisa e as conclusões obtidas pela realização de todas as etapas realizadas para a finalização deste trabalho.

2 REDES E PROTOCOLOS

De acordo com Comer (2001) as redes de computadores obtiveram um crescimento explosivo nos últimos anos. Esta forma de comunicação e interligação entre pontos diversos tornou-se indispensável em muitos aspectos de negócios, como propaganda, produção, transporte, planejamento, faturamento e contabilidade. Instituições de ensino, do elementar até a pós-graduação, estão usufruindo das redes de computadores com o objetivo de proporcionar aos seus professores e alunos a facilidade de acesso as informações contidas em bibliotecas *on-line* em todo o mundo.

Comer (2001) afirma ainda que o crescimento contínuo da Internet global é dos fenômenos mais observados e interessantes na área de redes. Atualmente a Internet tornou-se um sistema de comunicação de alto grau de produtividade que incorpora milhões de pessoas em todo o globo terrestre.

Portanto, neste contexto de crescimento e importância das redes de computadores, nos próximos capítulos pode-se observar como surgiu esta necessidade de criação, seus conceitos básicos e a linguagem utilizada para realizar a comunicação entre os pontos interligados, linguagem esta chamada de *Protocolos*.

2.1 A INTERNET

Grande parte da Internet resultou da "evolução" de um sistema criado em 1969. Nesta época, os oficiais do Departamento de Defesa dos Estados Unidos começaram a notar

que os militares estavam adquirindo uma coleção grande e diversificada de computadores, onde alguns destes computadores não estavam em rede e outros estavam agrupados em redes menores. Uma das divisões deste Departamento - a Agência de Projetos de Pesquisa Avançada em Defesa (DARPA) – concluiu que o país precisava criar um modo fácil de trocar informações militares entre cientistas e pesquisadores localizados em diferentes regiões geográficas.

O objetivo, segundo Stang (1994), era desenvolver um conjunto de protocolos de comunicação, os quais permitiriam computadores ligados em rede comunicar-se de forma transparente entre várias redes diferentes. O sistema de protocolos que foi criado chamou-se *Transmission Control Protocol* e *Internet Protocol*, o popular TCP/IP. Este protocolo tinha duas vantagens principais sobre os outros disponíveis: era o mais leve e podia ser implementado por um custo bem mais baixo. Pode ver mais sobre o *Transmission Control Protocol (TCP/IP)* na sub-seção 2.3.1.1.

Uma rede simples de quatro computadores, conhecida como DARPANET, foi desenvolvida. Algum tempo depois foi rebatizada de ARPANET e, em 1972, cresceu a ponto de incluir 37 computadores e, ao mesmo tempo, o modo de utilização da rede começou a mudar.

Além de ser empregada para trocar informações importantes, sobre atividades militares, os usuários da ARPANET, começaram a enviar mensagens eletrônicas por meio de caixas de correio pessoais.

A seguir será possível ter acesso aos conceitos e assuntos envolvendo Redes de Computadores. Todo o processo de transmissão de dados entre estações e a forma de comunicação entre elas.

2.2 REDES

Comer (2001), descreve que uma *rede* é um conjunto de computadores ou dispositivos semelhantes ao computador interligados entre si por algum meio de transmissão de dados. Poderá ser visto mais sobre transmissão de dados na sub-seção 2.2.1.

Na rede, estes dispositivos podem se comunicar por meios de transmissão, como, uma impressora conectada à rede onde vários computadores podem realizar trabalhos de impressão.

Na Figura 1 observa-se a representação da situação descrita acima.

Figura 1. Rede de computadores e dispositivos

Segundo Casad (1999), por um meio de transmissão em uma rede, passam dados de um computador para outro. Para a interação com o mundo na Internet, um computador utiliza aplicações que realizam tarefas específicas e gerenciam a entrada e saída de dados. Portanto, se um computador é integrante de uma rede, algumas de suas aplicações devem ser capazes de se comunicar com aplicações de outros computadores desta rede.

Casad (1999) afirma que um conjunto de protocolos de rede é um sistema de regras que ajuda a definir o processo complexo de transferência de dados. De uma

aplicação em um computador, os dados trafegam pelo *hardware* de rede deste computador, pelo meio de transmissão até o destino correto e depois pelo *hardware* de rede do computador de destino até uma aplicação receptora.

2.2.1 Transmissão de Dados

De acordo com Comer (2001), a comunicação entre computadores em uma rede envolve codificar dados em uma forma de energia e enviar esta energia por um meio de transmissão. Como exemplo disto, a corrente elétrica pode ser utilizada para transferir dados por meio de um fio, ou ondas de rádio podem ser utilizadas para carregar dados por meio do ar.

Estando os dispositivos de *hardware* conectados a um computador executando a codificação e decodificação dos dados, programadores e usuários não necessitam adquirir conhecimento sobre os detalhes de transmissão de dados. Porém, já que uma das funções do software de comunicação é tratar de falhas e erros que surgem no *hardware*, torna-se necessário compreender alguns conhecimentos básicos sobre a transmissão de dados, para poder estar manipulando estes *softwares*.

Comer (2001) afirma que existem várias formas de efetuar a transmissão de dados entre dispositivos. Entre elas estão:

a) ***Fios de cobre:*** redes convencionais usam fios como meio de transmissão para conectar computadores porque o fio é mais barato e fácil de instalar. Dos vários materiais que estes fios podem ser fabricados, o fio de cobre é o

mais utilizado, pois possue uma baixa resistência a corrente elétrica, significando que os sinais podem viajar por distâncias maiores. O mais popular destes fios é chamado de *cabo coaxial*, que poderá ser visualizado na figura 3.

b) ***Fibras de vidro:*** também chamada de *fibra óptica*, este meio utiliza a luz para transmitir dados. Esta fibra de vidro é revestida de plástico, o que permite que o cabo possa ser "dobrado" sem que haja o rompimento da fibra de vidro. Dentre as várias vantagens que este meio de transmissão de dados possui sobre os outros, estão: a maior distância de propagação dos sinais, a não interferência elétrica sobre outros cabos de transmissão, o maior fluxo de informações em um determinado intervalo de tempo, entre outros. Embora todas estas vantagens caracterizem este meio de transmissão, tudo isso custa mais caro, sendo esse um dos motivos pela não implementação deste recurso em muitos locais.

c) ***Rádio:*** Além da forma convencional da transmissão de programas de rádio e de televisão e para uma comunicação privada com dispositivos como telefones portáteis, a radiação eletromagnética pode ser utilizada para transmitir dados de computador. Esta forma de transmissão de dados, ao contrário das redes que utilizam fios ou fibras ópticas, não necessita de uma conexão física direta entre os dispositivos. Os computadores ou outro dispositivo qualquer que utiliza este meio de transmissão possui uma antena, que pode transmitir como também receber sinais.

Muitos outros meios podem ser utilizados para a transmissão de dados entre dispositivos, como infravermelho, luz de laser, microonda, satélites, entre outros. Cada meio, caracteriza-se por vantagens, desvantagens e custos diante uns dos outros.

Na sub-seção abaixo é possível observar como a transmissão de dados é feita pelo uso de pacotes.

2.2.1.1 Pacotes

Segundo Comer (2001) a maioria das redes de computadores não transfere dados como uma seqüência arbitrária de bits contínuos. Ao contrário disso, o sistema de rede divide os dados em blocos pequenos chamados de *pacotes,* que ele envia um a um. Daí o porquê das redes de computadores serem chamadas de *redes de pacotes* ou *redes de comutação de pacotes.*

Comer (2001) afirma ainda que dois fatos contribuem fortemente para o uso de pacotes em redes de computadores. O primeiro designa o fato de um receptor e um remetente precisarem coordenar a transmissão para assegurar que os dados chegam corretamente. Isto porque na ocorrência de erros durante a transmissão dos dados, estes podem ser perdidos. Esta divisão dos dados em blocos ajuda o receptor e o remetente a identificarem quais blocos chegaram ou não ao destino. O segundo fato pelo uso de pacotes incorpora a questão de assegurar que todos os computadores recebam acesso justo e imediato à uma instalação de comunicação compartilhada. Um sistema de rede não pode

impedir que um computador tire a permissão de acesso de outro computador perante os recursos disponibilizados na rede.

Para resumir todo este contexto de uso de pacotes, esta utilização significou o fim da espera de um computador ligado a rede para emitir dados diante do meio de comunicação. Nos primórdios das redes de computadores não existia o acesso justo às informações. Estas redes permitiam que um programa aplicativo mantivesse um recurso de comunicação compartilhada, pois permitia-se que este aplicativo fosse até o fim da transmissão até que outro aplicativo pudesse começar a usar o recurso.

Para se entender o funcionamento da utilização de pacotes na rede, pode-se observar a Figura 2.

Figura 2. Uma das razões por que as redes de computadores fazem o uso de pacotes. Enquanto um par de computadores se comunica, os outros devem esperar.
Fonte: Comer, D. (2001)

Suponha que uma rede tenha concedido a um programa aplicativo o uso exclusivo de uma rede até que o aplicativo termine. Por exemplo, imagine que os computadores A, B, C e D indicados na Figura 2, compartilhem um canal de comunicação e que eles usem este canal para efetuar a transferência de arquivos. Desta forma, sem a utilização de pacotes na transmissão, enquanto o computador *A* envia um arquivo para o computador *D*, os computadores *B* e *C* devem esperar para poder ter acesso também ao meio de transmissão.

Demonstrada a forma de comunicação em rede por meio da utilização de pacotes, na sub-seção abaixo é mostrada a forma que as interfaces de redes fazem o filtro de pacotes para que estes possam ou não serem aceitos por uma máquina na rede.

2.2.1.1.1 Filtro de Pacotes

Segundo NORTHCUTT et al (2002), a filtragem de pacotes é um dos métodos mais acessíveis e antigos de se controlar os acessos à rede. O conceito de filtragem de pacotes é simples: um pacote tem ou não permissão para entrar no dispositivo de rede (placa-de-rede, por exemplo). Esta permissão é atribuída a ele conforme a comparação que é feita nas informações contidas no cabeçalho do pacote.

Para que haja a facilidade na comunicação entre computadores na rede, as informações enviadas de um computador a outro precisam ser divididas em partes manipuláveis, chamadas de *pacotes*. Estes pacotes possuem os chamados *cabeçalhos de pacotes*, que são segmentos de informações que se fixam no início de cada pacote para identificá-lo.

NORTHCUTT et al (2002) afirmam ainda que por meio dos valores localizados nos cabeçalhos de pacotes, estes identificadores transportam informações como o endereço de origem e destino do pacote, além da *porta do protocolo*[1] com qual eles estão se comunicando. Por exemplo, quando um pacote do protocolo *TCP/IP* chega a um roteador,

[1] Portas de Protocolos são utilizadas para identificar qual é a porta de origem ou de destino do pacote.

este verifica seu destino para ver se este pacote poderá chegar no local desejado. Caso puder, este roteador passa o pacote para o segmento de rede apropriado.

Ainda de acordo com NORTHCUTT et al (2002), para se ter uma idéia mais clara de como funciona a filtragem de pacotes é indispensável saber que os protocolos utilizam portas de comunicação. O TCP e o UDP – que podem ser vistos detalhadamente nas sub-seções 2.3.1.1 e 2.3.1.2 - por exemplo, usam portas para controlar as seções de comunicação. Quando uma máquina cliente contata um servidor, aleatoriamente o cliente especifica uma porta com número superior a 1023 para utilizar na transmissão de dados. Depois disso, o cliente contata o servidor em uma porta definitiva. Quando a resposta é enviada do servidor para o cliente, esta informação sai da porta definida (porta 80 para HTTP, por exemplo) e são deixadas no cliente por uma porta aleatória com numeração maior que 1023. Como cada protocolo utiliza uma porta de comunicação diferenciada e alternativa, uma forma de filtragem de pacotes e serviços na rede pode ser pela porta de comunicação.

Ainda no contexto da utilização de pacotes para a comunicação em redes de computadores, a partir do próximo capítulo pode-se adquirir conhecimento sobre a forma de funcionamento das redes locais e o tráfego de dados.

2.2.2 Redes Locais e Tráfego de Dados

As *Local Area Networks (LAN's)*também chamadas de Redes Locais, são pequenas redes conectadas entre si via *Ethernet*. São redes privadas contidas em um prédio

ou em um campus universitário que têm alguns quilômetros. De acordo com Comer (1999), *Ethernet* é o nome dado a uma tecnologia de rede local popular, de *comutação de pacotes,* criada na década de 1970. Aos poucos, esta tecnologia tornou-se popular nestas redes locais. O termo *Ethernet* foi chamado assim por ser uma rede tipicamente interligada por cabos. A Ethernet é bem adequada a aplicativos em que um meio de comunicação local deva transportar tráfego diverso, ocasionalmente intenso, a altas taxas de dados.

> Ethernet é uma rede de barramento em que múltiplos computadores compartilham um meio de transmissão único. Enquanto um computador transmite um quadro para outro, todos os demais computadores devem esperar. (COMER, 2001. p. 87).

Estes cabos, chamados de *ether,* são totalmente passivos, ou seja, todos os componentes eletrônicos ativos que fazem a rede funcionar são associados aos computadores conectados à rede. A Figura 3 mostra detalhadamente o corte transversal do cabo original deste tipo de rede.

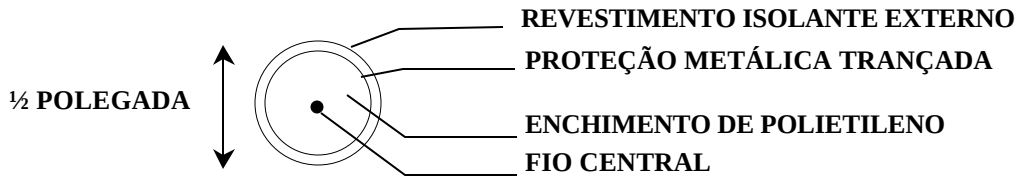


Figura 3. Corte transversal no cabo coaxial usado na Ethernet original.
Fonte: Comer (1999)

Os dados, na maioria das vezes, trafegam de uma rede para outra por meio de cabos. E por estes cabos, este tráfego é feito em pequenas unidades chamadas *frames.* Os frames são construídos em seções e cada seção desta carrega consigo informações especializadas. Os 12 primeiros bytes de um frame Ethernet contêm informações dos

endereços do destino e da origem. Desta forma, esses valores fornecem dados onde é facilmente identificado o local de onde vieram tais dados e para onde estão indo.

Tanenbaum (1997) afirma que as redes locais são utilizadas para conectar computadores pessoais e estações de trabalho localizadas em instalações industriais e em escritórios, permitindo que recursos sejam compartilhados (por exemplo, impressoras) e informações sejam trocadas entre as máquinas.

Tanenbaum (1997) afirma ainda que as redes locais podem adquirir várias topologias. Em uma rede de barramento, que pode ser visualizada na Figura 4, em um instante qualquer uma máquina pode desempenhar o papel de mestre e possivelmente realizará uma transmissão de dados para outras máquinas por meio deste barramento. No momento em que a mensagem é enviada, as outras máquinas serão impedidas de enviar algum tipo de mensagem. Para entender mais esta forma de transmissão de dados e a comunicação de máquinas com a topologia de barramento pode ser observada a Figura 4.

A Ethernet constitui numa tecnologia de Redes Locais, dotada de padrões, onde um deles, o *IEEE 802.3*[2], constitui uma topologia de barramento. Esta topologia permite uma operação de controle descentralizada à velocidade de 10 ou 100 Mbps. Em uma rede Ethernet os computadores podem estabelecer uma transmissão no momento que quiserem. Caso haja uma colisão de dois ou mais pacotes, cada computador aguardará um tempo aleatório e fará uma nova tentativa de transmissão.

[2] O Padrão IEEE 802 é um conjunto de padrões para ligação, manutenção e segurança de redes locais e também em grandes redes.

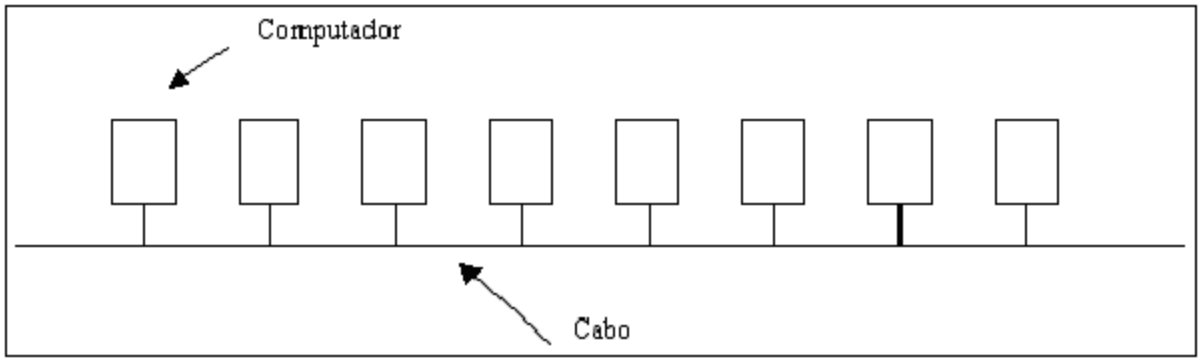


Figura 4. Topologia de barramento.
Fonte: Tanenbaum, A. (1997)

Não somente as redes locais, mas também toda a rede mundial de computadores adota padrões de comunicação entre estações e dispositivos diversos. Estes padrões ou linguagens são chamados de *protocolos*.

2.3 PROTOCOLOS DE COMUNICAÇÃO

Comer (1999) afirma que um protocolo de comunicação nada mais é do que um conjunto de convenções que regem o tratamento e, especialmente, a formatação de dados num sistema de comunicação. Seria a "gramática" de uma "linguagem" de comunicação padronizada.

Comer (1999) descreve ainda que os sistemas de comunicação de dados não usam somente um único protocolo para gerenciar todas as tarefas de transmissão. Ao contrário disso, estes sistemas requerem uma pilha de protocolos cooperativos, que podem ser chamados de *família de protocolos*. Dentre os problemas que surgem quando as máquinas se comunicam por meio de uma rede de dados, estão:

a) *Falha de hardware:* um host ou um roteador qualquer pode falhar tanto pela falha no hardware como também pelo fato de ter ocorrido um colapso no sistema operacional. Uma transmissão ativa em uma rede pode ser interrompida acidentalmente a qualquer momento, por motivos diversos. Portanto o *software* de protocolo necessita detectar estas falhas e recuperar-se delas, caso possível.

b) *Congestionamento de redes:* mesmo que *hardware* e *software* operem corretamente, as redes possuem capacidades finitas que podem ser vencidas. Desta forma, os protocolos precisam encontrar maneiras para que uma máquina que esteja congestionada possa suprimir o excesso de tráfego.

c) *Demora ou perda de pacotes:* Algumas vezes, os pacotes demoram muito ou são perdidos. Sendo assim, os protocolos precisam aprender sobre as falhas ou adaptar-se a longas demoras.

d) *Danificação de dados:* Interferências elétricas ou magnéticas ou falhas de hardware podem causar a transmissão de erros ou danificam os conteúdos dos dados transmitidos. O protocolo precisa detectar e corrigir tais erros.

e) *Duplicação de dados ou erros seqüenciais:* Em redes em que podem existir rotas múltiplas para a transmissão de dados, pode ocorrer de dados serem transmitidos fora da seqüência ou podem inclusive transmitir duplicatas de pacotes. Os protocolos precisam portanto, reorganizar e remover estes pacotes duplicados.

Conforme descrito nos parágrafos anteriores, para que haja a comunicação entre computadores, vários protocolos podem ser utilizados. De acordo com Pompermayer Jr (2002), dentre os protocolos mais utilizados estão os pertencentes à Arquitetura *Transmission Control Protocol/Internet Protocol (TCP/IP).* Outros protocolos que juntamente com o TCP/IP são utilizados também para esta comunicação.

Desta forma, a partir da sub-seção 2.3.1 são descritos alguns destes protocolos, principalmente os pertencentes à arquitetura *TCP/IP*, que compõe um conjunto dos protocolos mais utilizados atualmente para a comunicação de redes de computadores.

2.3.1 Arquitetura TCP/IP

Nesta sub-seção foi feita uma breve revisão teórica sobre a tecnologia da arquitetura TCP/IP, pois denomina-se como um assunto fundamental para o entendimento do funcionamento de ferramentas de análise de tráfego (*Sniffers*).

É mostrada a pilha de protocolos desta arquitetura, descrevendo brevemente cada camada e seus respectivos protocolos, bem como algumas aplicações dentre as várias que merecem atenção.

Segundo Comer (1999), a arquitetura TCP/IP, apresentada na Figura 5, trata-se de um conjunto de protocolos divididos em quatro camadas conceituais. Estas quatro camadas desta arquitetura são construídas sobre uma quinta camada (Comer, 2000) que corresponde ao nível físico ou nível de hardware, como pode ser visto na Figura 5 cada

camada desta possui funções bem definidas. São elas: aplicação, transporte, Internet e a de acesso à rede.

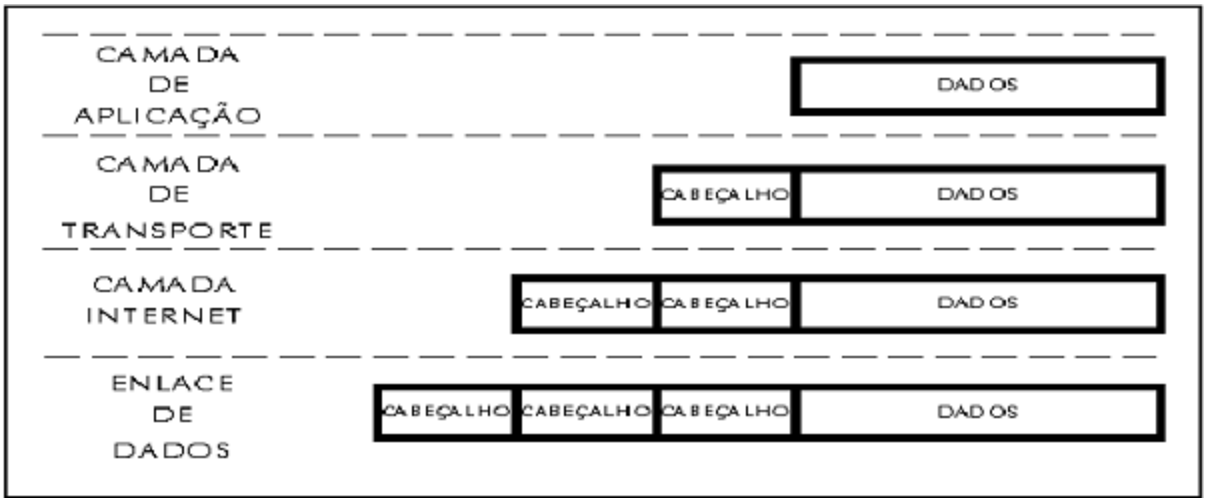


Figura 5. Camadas da arquitetura TCP/IP
Fonte: Comer, D. (1999)

Já na Figura 6, pode ser vista a forma de transmissão de dados entre estas camadas desta arquitetura.

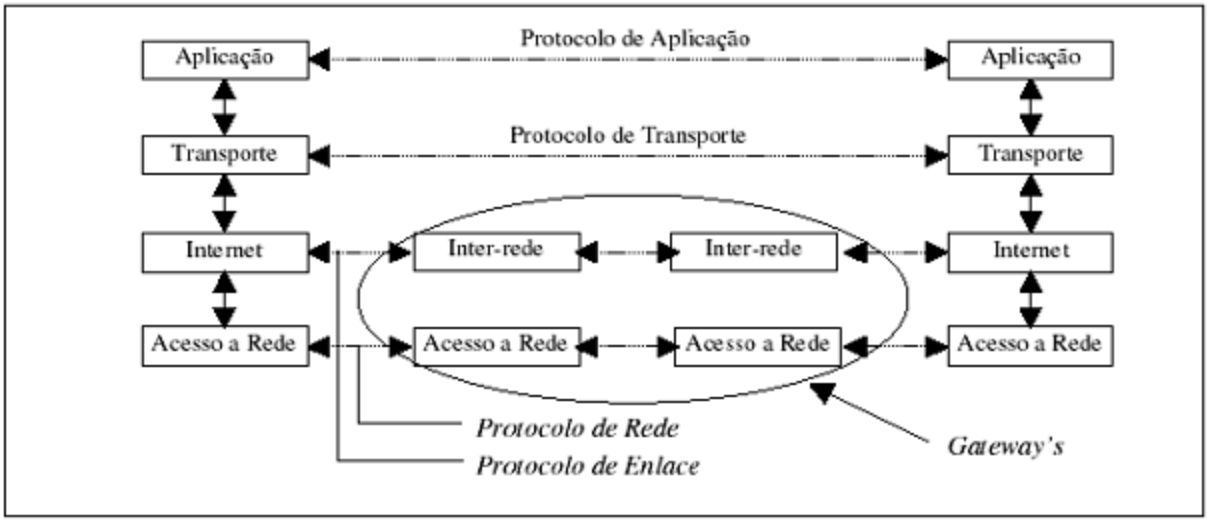


Figura 6. Camadas e forma de transmissão de dados no modelo TCP/IP
Fonte: De Souza, A. (2004)

Na Figura 7 são mostrados alguns dos tipos de dados que são transmitidos de uma camada para a outra.

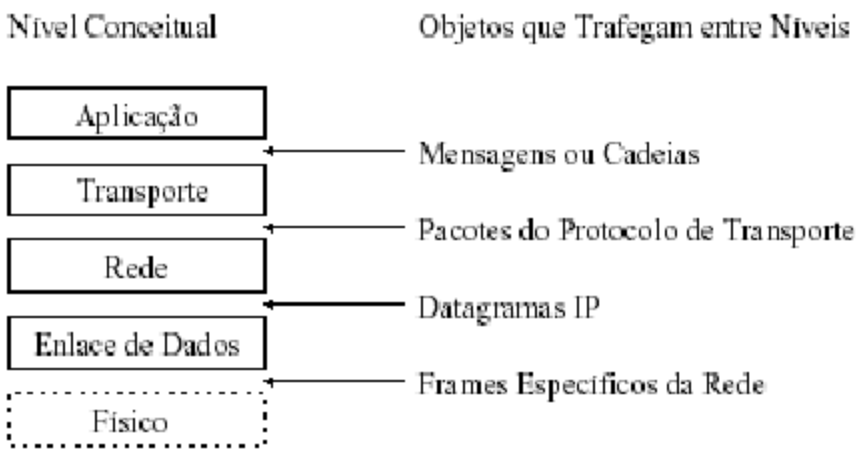


Figura 7. Demonstração de alguns dos objetos que são repassados de uma camada para a outra.
Fonte: Chaves, M. (2003)

a) **Camada de aplicação:** segundo Tanenbaum (1997) é nesta camada que estão os protocolos de alto nível como terminal virtual (*TELNET*), protocolo de transferência de arquivos (FTP), protocolo de envio de correio eletrônico (SMTP) entre outros. É nesta camada que estão os programas dos usuários. O TCP/IP combina todas as questões relacionadas a aplicações em uma camada e garante que esses dados estejam empacotados corretamente para a próxima camada.

b) **Camada de transporte:** responsável por uma comunicação entre dois *hosts* fim-a-fim, podendo oferecer comunicações orientadas ou não orientadas à conexão. Fazem parte desta camada os protocolos *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP). Esta camada é responsável por questões de qualidade de serviços de confiabilidade, controle de fluxo e correção de erros. O TCP mantém um "diálogo" entre a

origem e o destino enquanto empacota informações da camada de aplicação em unidades chamadas segmentos. Orientado para conexões não significa que exista um circuito entre os computadores que se comunicam. Significa que segmentos da camada de transporte trafegam entre dois hosts para confirmar que a conexão existe logicamente durante um certo período.

c) **Camada inter-redes ou Internet:** é onde está implementado o protocolo *Internet Protocol (IP)*. Nesta camada é feito o roteamento e a entrega dos pacotes IP. A finalidade da camada de Internet é enviar pacotes da origem de qualquer rede na *Internetwork* e fazê-los chegar ao destino, independentemente do caminho e das redes que tomem para chegar lá. O protocolo que especificamente age nesta camada é chamado Internet Protocol (IP). A determinação do melhor caminho e a comutação de pacotes acontecem nessa camada. Como exemplo disso, pegue o sistema postal. Quando você envia uma carta, você não sabe como ela vai chegar ao seu destino (existem várias rotas possíveis), mas, o que realmente importa, é que ela chegue.

d) **Camada de enlace:** de acordo com Tanenbaum (1997), esta camada é responsável por encapsular os pacotes da camada inter-redes no formato específico da rede associada e extrair os pacotes dos quadros vindos da rede e encaminhá-los à camada Inter-redes.

e) **Camada Física:** esta camada é correspondente ao nível de hardware, ou meio físico, pois trata dos sinais eletrônicos. Os *frames,* originados da camada de enlace, são convertidos em sinais eletrônicos compatíveis com o

meio físico. Posteriormente estes sinais são conduzidos até a próxima interface de rede, que pode ser um *host* destino ou *gateway* da rede.

De acordo com Comer (1999), o *TCP/IP* é utilizado para vários propósitos, não somente para a Internet, pois a maioria das redes *intranets*[3] utilizam este protocolo para comunicação entre máquinas. Dentre as vantagens oferecidas sobre os outros protocolos, está a facilidade e mobilidade diante de muitos Sistemas Operacionais e dispositivos de hardware.

Comer (1999) afirma ainda que o software TCP/IP geralmente é residente no sistema operacional, onde desta forma poderá ser compartilhado por todos os programas aplicativos executados na máquina. Ou seja, o sistema operacional possui uma única cópia de um protocolo, neste caso o TCP/IP, e vários programas utilizam este código de forma compartilhada. As camadas desta arquitetura tendem a funcionar de forma independente umas das outras, onde os dados transferidos de um programa não afetem os transferidos por outro.

O TCP e o IP na verdade são apenas dois protocolos pertencentes à uma coleção maior de protocolos chamada família de protocolos TCP/IP. Hoje, os protocolos inseridos à arquitetura TCP/IP fornecem transporte de dados a todos os serviços disponíveis na Internet.

Alguns destes serviços são:

a) Transferência de arquivo (FTP)

b) Acesso à *Word Wide Web (WWW)*

[3] São redes locais de acesso restrito, implantadas internamente em empresas para o uso de um grupo de pessoas de forma privada.

c) Transmissão de correio eletrônico *(SMTP)*

Comer (2000) afirma que para cada camada da arquitetura TCP/IP existem protocolos que desempenham funções específicas dentro destas camadas, ou seja, cada protocolo pertence a uma camada da arquitetura.

A Figura 8 demonstra o que foi descrito no parágrafo acima.

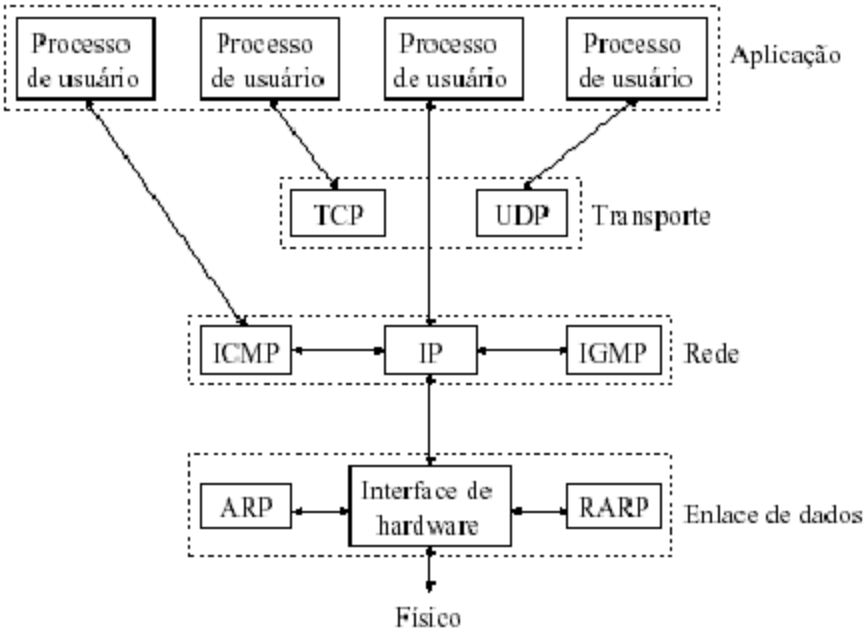


Figura 8: Vários protocolos dentro das diferentes camadas da arquitetura TCP/IP.
Fonte: Chaves, M. (2003).

Dentre os vários protocolos pertencentes à arquitetura TCP/IP, a seguir serão vistos alguns destes, começando por um dos principais, o TCP (*Transmission Control Protocol*).

2.3.1.1 O Protocolo TCP (Transmission Control Protocol)

O Transmission Control Protocol (TCP) caracteriza-se por ser um protocolo que garante a entrega confiável dos dados ao destino. Segundo Dimarzio (2001), no momento da transmissão, o TCP recebe os dados e os desmembra em segmentos. Em seguida esses segmentos são numerados pelo TCP antes da entrega pela rede.

Comer (1999) afirma que este protocolo caracteriza-se por garantir a entrega dos pacotes porque exige que um receptor comunique-se com a origem, do qual retornará uma mensagem de confirmação, à medida que recebe os dados. O transmissor dos pacotes também mantém um registro de cada pacote que envia e espera uma confirmação antes de enviar o próximo pacote.

A Figura 9 mostra detalhadamente como funciona o procedimento de envio e recebimento dos pacotes entre a origem e o destino em uma transmissão de dados pelo protocolo *TCP*.

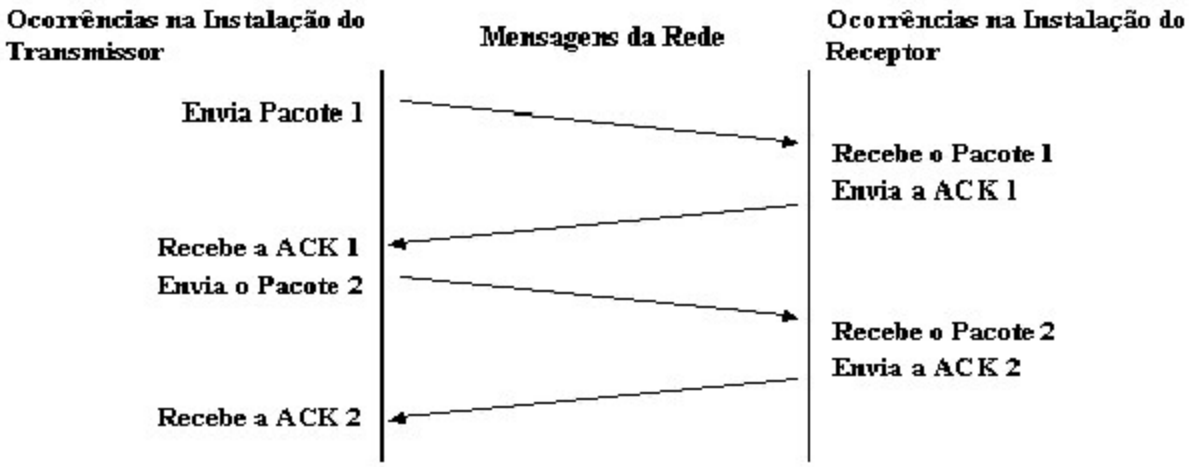


Figura 9: O TCP utiliza a confirmação positiva com retransmissão, em que o transmissor aguarda uma confirmação para cada pacote enviado.

Fonte: Comer, D. (1999).

Assim que todos os segmentos estiverem prontos para a entrega, o TCP solicita uma seção com a camada de transporte do destinatário. É papel do IP conhecer o destino. Assim que a conexão é feita, o TCP inicia a transmissão dos segmentos.

A cada pacote recebido o destino envia uma confirmação. Após isso, o dispositivo de destino inicia uma montagem dos segmentos em dados do usuário, baseado na numeração dos segmentos. Caso esteja faltando algum dos segmentos, o destino torna solicitar o segmento específico do remetente. Portanto, se um segmento se perder em trânsito, o TCP simplesmente o enviará de novo.

O TCP é considerado um protocolo orientado à conexões, isto porque ele abre uma conexão com o destino antes de enviar segmentos. Desta forma, o remetente (origem) pode ter a certeza de que o destino está ativo e pronto para receber quaisquer segmentos que este deseja enviar.

Na numeração feita pelo TCP para a entrega no destino, os segmentos são inseridos em uma fila para a transmissão pela rede. Em seguida, o TCP constrói um circuito virtual até os dispositivos de destino. Desta forma os segmentos chegarão ao destino na ordem correta.

As principais funções desempenhadas pelo TCP são:

a) **transferência de dados:** os dados da aplicação são adicionados em mensagens de tamanho variável;

b) **transferência de dados urgentes:** os dados urgentes, como por exemplo, as informações de controle, são transferidos com indicativo de urgência, tendo prioridade sobre os dados normais;

c) **estabelecimento e liberação de conexão:** antes de iniciar qualquer tipo de transferência de dados é estabelecida uma conexão e esta por sua vez é liberada somente após o término da transferência dos dados;

d) **segmentação:** as mensagens entregues ao TCP podem ser segmentadas. Cada segmento deve compor um datagrama IP e possuir um número de identificação, que possibilita a posterior recomposição da mensagem original no destino;

e) **controle de fluxo:** o TCP envia muitos segmentos ao destino, mesmo antes de receber um reconhecimento positivo ou negativo. Ele adapta-se à diferentes velocidades entre os dois dispositivos envolvidos;

f) **controle de erros:** a numeração dos segmentos permite que estes sejam ordenados e entregues ao destino na seqüência correta.

Um outro protocolo pertencente a esta arquitetura é o *User Datagram Protocol (UDP)*, caracterizado por desempenhar transmissão de dados sem confirmação de recebimento, diferentemente do protocolo TCP. O protocolo UDP é descrito na seção abaixo.

2.3.1.2 O Protocolo UDP (User Datagram Protocol)

Existem situações em que o dispositivo de origem não precisa ter a garantia de chegada dos dados no dispositivo destino, como exemplo podem ser citados alguns tipos de transmissão de áudio e vídeo. Nestas situações, o protocolo TCP é substituído pelo *User*

Datagram Protocol (UDP) que é um protocolo que não é orientado a conexão, ou seja, não necessita estabelecer uma conexão entre origem e destino antes de enviar os dados.

Este protocolo não verifica se o dispositivo destino está conectado. Na realidade o protocolo UDP empacota os dados e os envia para camada inferior para que o protocolo IP dê prosseguimento ao envio dos dados. Estes pacotes, segmentos, apesar de serem numerados antes de serem enviados, não sofrem nenhuma verificação de chegada ao destino. O UDP pode ser comparado ao sistema tradicional de entrega de cartas. Prepara-se uma carta, em seguida ela é posta em um envelope, depois selada e posteriormente esta é colocada no correio na esperança de que chegue ao seu destino, embora não se tenha esta garantia.

Na Figura 10 pode ser visto a ilustração de como é composto um datagrama UDP.

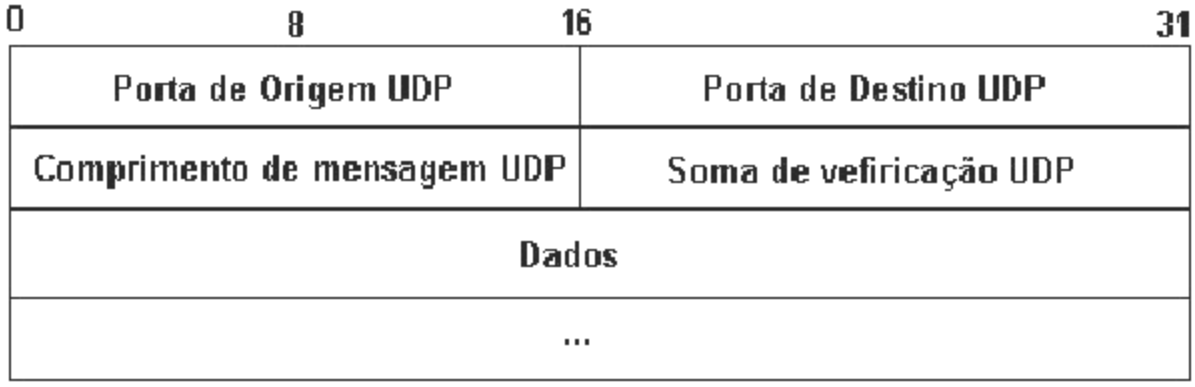


Figura 10. Formato do datagrama UDP
Fonte: Pompermayer Jr, L. (2002)

Os protocolos TCP e UDP descritos nas duas últimas seções são protocolos que exercem funções na camada de transporte da arquitetura TCP/IP. Interligado a todos estes funcionamentos, na seção 2.3.1.3 é descrito o protocolo IP, pertencente a camada de rede desta arquitetura e responsável por garantir o endereçamento dos pacotes pela rede.

2.3.1.3 O Protocolo IP

O protocolo *Internet Protocol (IP)* teve origem em 1970 juntamente com o desenvolvimento da ARPANET, a qual posteriormente sofreu interligação com outras redes, formando em 1980 um enorme conjunto de redes que começou a ser chamado de Internet.

O IP é utilizado em computadores interligados em rede, onde há a troca de pacotes entre eles. Este protocolo fornece a transmissão de blocos de dados, chamados de datagramas, entre a origem e o destino dos dados. O IP serve de base ou suporte para os outros protocolos da arquitetura TCP/IP, tais como ICMP, UDP e TCP, que são transmitidos em datagramas IP.

De acordo com Torres (2001), o protocolo IP é um protocolo não orientado à conexão, ou seja, este protocolo não verifica se o datagrama chegou ou não ao seu destino. A tarefa de verificação de chegada ao destino é feita pelo protocolo TCP, que recebe os datagramas que chegam e os coloca em ordem, solicitando a retransmissão dos datagramas que estiverem faltando.

A principal função do *Internet Protocol* (IP) é o roteamento. Esta operação consiste em adicionar mecanismos para que o datagrama chegue o mais rápido possível ao seu destino. Em grandes redes (por exemplo, a Internet), há um número exorbitante de caminhos em que um pacote pode percorrer para ir da origem ao destino, por isso a função de roteamento é feita com o auxílio de roteadores da rede.

Para entendermos melhor o funcionamento do protocolo IP, veremos na sub-seção seguinte a estrutura do datagrama IP, conforme ilustrado na Figura 11.

2.3.1.3.1 Estrutura do Datagrama IP

Um datagrama IP é constituído resumidamente em cabeçalho e dados. A área de dados não tem tamanho fixo, portanto, o tamanho de uma datagrama IP é variável. O tamanho máximo do datagrama IP é de 65.535 bytes, incluindo o cabeçalho.

A estrutura do datagrama IP é mostrada abaixo pela Figura 11:

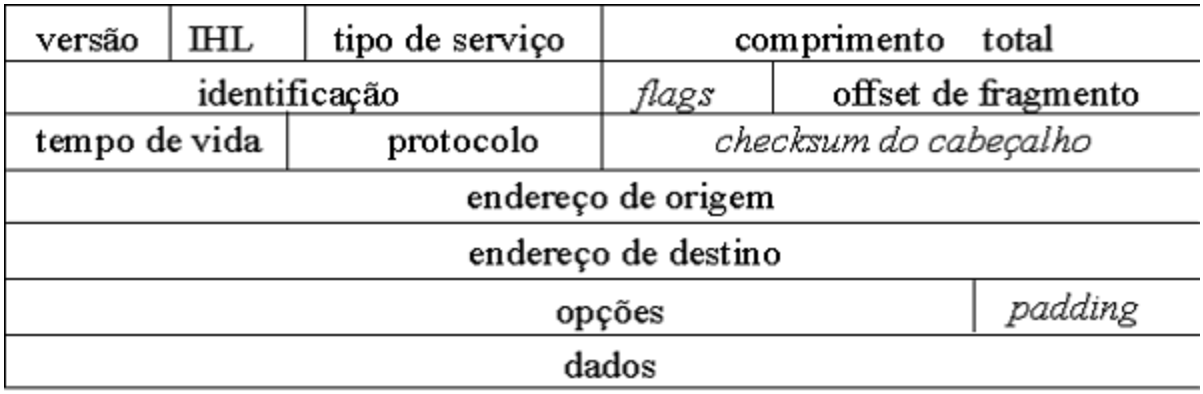


Figura 11. Estrutura do datagrama IP
Fonte: Comer, D. (2001)

Conforme Figura 11, no diagrama IP podem ser encontrados os seguintes campos:

a) **Vers (versão):** 4 bits. Segundo Torres (2001), este campo indica a versão do protocolo IP que está sendo usado. O protocolo IP que está sendo descrito é o IPv4.

b) **Hilen (tamanho):** Campo de 4 bits. contém o comprimento do cabeçalho IP em palavras de 32 *bits*.

c) **Service Type (Tipo de Serviço):** 8 bits. A qualidade desejada para a entrega do datagrama é incorporada a este campo. Este campo é subdividido em:

    1) precedence: campo de 3 bits, indica a precedência de datagramas com valores desde 0 (precedência normal) até 7 (controle de rede), com estes *bits* permite-se ao transmissor indicar a importância de cada datagrama que ele está enviando;
    2) bits *D, T, R*: indicam o tipo de transporte que o datagrama deseja: baixo retardo (D), alta capacidade de processamento (T) e alta confiabilidade (R);

d) **Total Length (tamanho total):** 16 bits. Neste campo está contido o comprimento do datagrama medido em bytes, incluindo cabeçalho e dados. Segundo Torres (2001), quanto maior o tamanho do datagrama, mais uma estação ocupa a rede, deixando-a mais lenta. Por esse motivo, os datagramas usam tamanhos bem menores que 65.535 bytes (tamanho máximo de um datagrama IP), como, por exemplo, 576 bytes.

e) **Identification (Identificação):** 16 bits. Usado para identificar o datagrama. Quando o datagrama é criado e enviado na rede pelo transmissor, é atribuído à ele um número de identificação. Este número será usado para identificar o datagrama caso ele sofra fragmentação no caminho até o destino.

f) **Flags:** 3 bits. Controla a fragmentação de datagramas.

g) **Fragment Offset (Offset do Fragmento):** 13 bits. Especifica o início do datagrama original dos dados que estão sendo transportados no fragmento. É medido em unidades de 8 bytes;

h) **TTL, Time to live (Tempo de Vida):** campo de 8 bits. Indica o tempo máximo de vida do datagrama. Cada vez que o datagrama passar por um gateway (roteador) esse número é decrementado. Quando o valor deste campo é igual a zero, o datagrama é descartado, não chegando ao destino.

i) **Protocol (Protocolo):** 8 bits. Este campo contém um código numérico que indica o protocolo que solicitou o envio do datagrama. Por exemplo, o número 6 indica o TCP, número 17 indica o UDP e número 1 identifica o ICMP. Desta forma, quando o datagrama for passado à um protocolo superior, a camada IP já sabe para qual protocolo passar.

j) **Header-checksum (Checksum do Cabeçalho):** 16 bits. Assegura integridade dos valores do cabeçalho. O protocolo IP adiciona um campo de checksum para os valores presentes no cabeçalho. Esse campo calcula somente o checksum do cabeçalho, portanto não usa o campo de dados no cálculo. Os roteadores analisam esse campo e refazem o checksum para verificar se o cabeçalho está ou não corrompido.

k) **Source IP Address (Endereço IP de origem)**: 32 bits. Indica o endereço IP de onde está partindo o datagrama.

l) **Destination IP Address (Endereço IP de Destino):** 32 bits. Indica o endereço IP de destino do datagrama.

m) **Options (Opções + Pad):** campo opcional. Se este campo for utilizado no datagrama, o cabeçalho terá o tamanho de 24 bytes. Este campo possui tamanho variável, portanto ele é preenchido com zeros até ter 32 bits de comprimento. Estes zeros adicionados a este campo são conhecidos como *pad* ou *padding*. Este campo é utilizado para testes e verificação da existência de erros na rede.

n) **Data (Dados):** são os dados que o datagrama está levando.

Na sub-seção a seguir será visto o protocolo *Internet Control Message Protocol (ICMP)*, que é um protocolo que funciona na camada de rede da arquitetura TCP/IP, juntamente com o *IP*.

2.3.1.4 O Protocolo ICMP (Internet Control Message Protocol)

De acordo com Carvalho (1997), o protocolo ICMP é um protocolo usado para transferências de mensagens de gateways e estações para uma estação de rede Internet. Estas mensagens, em sua maioria, indicam a ocorrência de problemas no transporte de algum datagrama ou ainda servem a operações de controle. Resumidamente, este protocolo tem como finalidade relatar os erros que ocorrem com os datagramas IP.

O ICMP não garante a entrega das mensagens ao destinatário, pois utiliza o IP para transporte de mensagens. As mensagens ICMP são geradas na verdade por gateways na rota de transporte de um datagrama ou pela estação de destino.

Quando algum problema previsto pelo ICMP realmente ocorre, a mensagem ICMP com a descrição do erro é preparada e entregue à camada IP, que irá adicionar à mensagem ICMP o cabeçalho IP e a envia ao emissor do datagrama com o qual ocorreu o problema.

Na Figura 12 pode ser visualizado o formato da mensagem do protocolo ICMP.

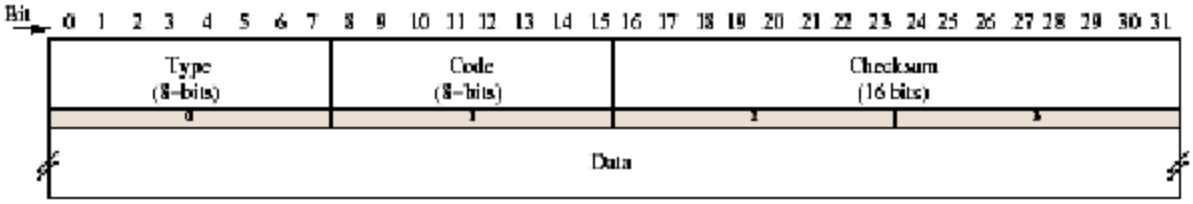


Figura 12. Formato da mensagem do ICMP.
Fonte: Chaves, M. (2003).

Já na Figura 13 então pode-se visualizar a forma de encapsulamento de uma mensagem ICMP.

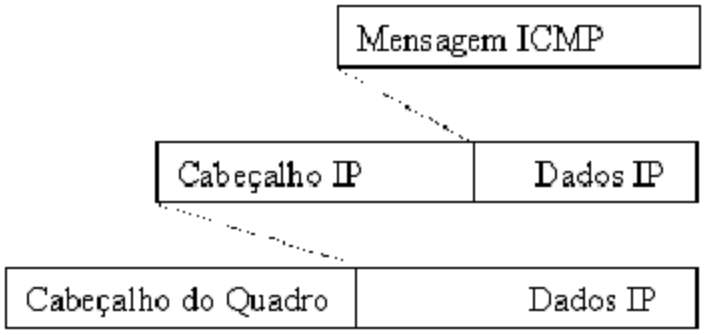


Figura 13. Encapsulamento da mensagem ICMP em um datagrama IP
Fonte: Carvalho, T. (1997)

Em casos em que a mensagem ICMP tratar de um datagrama anteriormente enviado, a mensagem também transporta o cabeçalho completo daquele datagrama IP e mais os 64 bits iniciais do seu campo de dados.

Assim, a estação que o emitiu pode identificar exatamente o datagrama a que se refere o problema, assim como distinguir qual é o protocolo de nível superior envolvido.

2.3.1.5 O Protocolo Address Resolution Protocol (ARP)

Comer (2001) afirma que o protocolo *Address Resolution Protocol (ARP)* permite que um determinado computador se comunique com outro computador em rede quando somente o endereço de IP é conhecido pelo destinatário. Para se obter o endereço *Media Access Control* (*MAC*) do computador do destinatário, o protocolo ARP envia um *broadcast* com o IP do destinatário requisitando o endereço do MAC do mesmo. No padrão ARP é especificado claramente a forma que devem ser enviadas as mensagens de requisição de ARP por meio de uma rede.

O protocolo especifica que uma mensagem de requisição de ARP deve ser inserida em um quadro de hardware e distribuído por meio de *broadcast* para todos os computadores da rede. Na rede, cada computador recebe e examina o endereço de IP. O computador que possui o endereço de IP recebido envia uma resposta ao remetente, enquanto todos os demais computadores processam e descartam a requisição sem enviar uma resposta.

Quando um computador envia uma mensagem de resposta, esta transmissão não é feita por *broadcast*, pois a resposta é inserida em um quadro e enviada diretamente de volta ao computador que fez a requisição.

Segundo Comer (2001), uma mensagem ARP tem o formato definido conforme Figura 14.

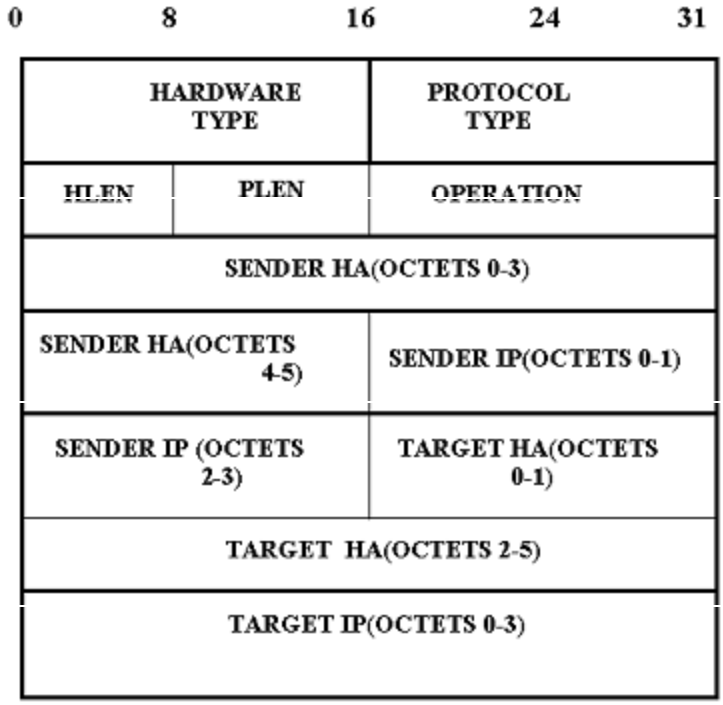


Figura 14. Formato de uma mensagem ARP
Fonte: Comer, D. (2001)

As linhas da Figura 14 possuem os seguintes campos:

a) **Hardware Type** *(tipo do hardware)*: composto de dois octetos, especifica o tipo de hardware utilizado na rede física.

b) **Protocol Type** *(tipo do protocolo)*: composto de dois octetos, especifica o endereço do protocolo utilizado no nível superior do emissor.

c) **Operation** *(operação)*: especifica se o datagrama é um pedido ARP (request 1) ou uma resposta ARP (reply 2), ou ainda um *RARP* (request 3, reply 4).

d) **HLEN e PLEN**: habilitam o ARP para ser usado com redes arbitrárias porque eles especificam o comprimento dos endereços do hardware e dos protocolos do nível superior. O *HLEN (Hardware Lenght)* é utilizado para identificar o tamanho dos campos *SENDER HA* e *TARGET HA*. O campo

PLEN (Protocol Lenght) especifica o tamanho dos campos *SENDER IP* e *TARGET IP.*

e) **SENDER HA** *(Sender Hardware Address)*: endereço físico de quem envia o pacote.

f) **SENDER IP** *(Sender Protocol Address):* endereço lógico (IP) de quem envia o pacote.

g) **TARGET HA** *(Target Hardware Address)* : Endereço físico desejado. Na operação de request vai em branco, e, quem responder preenche este campo.

h) **TARGET IP** *(Target Protocol Address)*: Endereço lógico da máquina desejada.

2.3.1.6 O Protocolo Reverse Address Resolution Protocol (RARP)

De acordo com Comer (2001), as aplicações utilizam o endereço IP quando especificam o destino. Os *hosts* e *gateways* utilizam os endereços físicos para transmitir datagramas na rede. Para realizar o mapeamento de endereços, ou seja, de endereço físico para IP, eles dependem do protocolo de resolução de endereços (ARP). O endereço IP de uma máquina é gravado em uma área de armazenamento secundário, por exemplo, no disco rígido. Ao contrário disto, quando uma máquina sem disco necessitar seu endereço IP ela utiliza o RARP.

De forma resumida, o protocolo RARP funciona respectivamente da seguinte forma:

a) máquinas sem disco precisam saber seu IP.

b) Servidores RARP possuem um banco de dados com mapeamento IP X MAC.

c) Estas máquinas então enviam uma requisição broadcast ao servidor RARP.

d) A máquina recebe o endereço IP fornecido por um servidor RARP e armazena em memória até ser reiniciada.

2.3.1.7 O Protocolo Internet Group Management Protocol (IGMP)

Leal (2004) descreve que o protocolo IGMP é uma extensão do protocolo IP que possibilita o *multicasting* para IP. Este protocolo opera em roteadores e estações de trabalho, permitindo que os roteadores determinem os endereços *multicast* que existem em seus segmentos. Por meio deste conhecimento, roteadores podem criar ramificações de multicast, permitindo que os dados de *multicast* possam ser recebidos e propagados para as suas respectivas estações de trabalho de multicast.

2.3.1.8 Aplicações

Chaves (2003) afirma que vários outros protocolos constituem as chamadas aplicações ou serviços, que correspondem ao mais alto nível da pilha de protocolos TCP/IP. Estas aplicações estão associadas a uma série de parâmetros, como número do protocolo,

número da porta e outros. Estes parâmetros são nomeados por um coordenador central, conhecido como *Internet Assigned Numbers Authority (IANA)*, responsável por atribuir valores únicos a estes parâmetros e também pela atualização destes valores catalogados no registro.

O número das portas (um dos parâmetros utilizados pelas aplicações) são divididos normalmente em três categorias (Stevens, 1998):

a) *Portas privilegiadas (0 - 1023):* a numeração atribuída a estas portas é definida pela IANA e na maioria dos sistemas só podem ser utilizadas exclusivamente por processos do sistema ou por aplicação que sejam executadas por usuários privilegiados.

b) *Portas registradas (1024 - 49151):* estas numerações são catalogadas e listadas pela IANA e na maioria dos sistemas, podem ser utilizadas por processos usuários não privilegiados ou por aplicações de usuários não privilegiados.

c) *Portas privadas (49152 - 65535):* estas portas não são controlas pela IANA.

A partir de dados coletados na IANA (2006), na Tabela 1 são relacionadas as portas que são utilizadas normalmente por estas aplicações na Internet.

Tabela 1. Algumas aplicações de rede e suas respectivas portas

Aplicação/Serviço	Porta
FTP (File Transfer) [data]	20/tcp
FTP (File Transfer) [control]	21/tcp
SSH (Secure Shell)	22/tcp
TELNET (Remote Login)	23/tcp
SMTP (Eletronic Mail)	25/tcp
DNS (Domain Name System)	53/udp

FINGER (User Information)	79/tcp
HTTP (The World Wide Web)	80/tcp
POP3 (Post Office Protocol - version 3)	110/tcp
Sun RPC (Remote Procedure Call)	111/tcp
NTP (Network Time Protocol)	123/udp
IMAP (Internet Message Access Protocol)	143/tcp
SNMP (Simple Network Management Protocol)	161/udp
NFS (Network File System)	2049/udp

Fonte: Chaves (2003)

Algumas destas aplicações são descritas abaixo:

Simple Mail Transfer Protocol – SMTP: este protocolo é utilizado nos serviços básicos de envio de mensagens. Funciona de forma independente de um sistema particular de transmissão e necessita apenas um canal confiável para enviar e/ou receber dados ordenados.

File Transfer Protocol – FTP: é uma aplicação com características de promover o compartilhamento de arquivos, de proteção ao usuário referente às variações nos sistemas de armazenamento de arquivos entre estações e também de transferir os arquivos de forma confiável. Diferente da maioria das outras aplicações, o FTP usa duas conexões de rede separadas, onde a maioria de suas implementações contém dois modos de operação: o ativo e o passivo. No modo ativo, ao ser realizada a conexão com o servidor, o cliente abre, a partir de uma porta acima de 1023/tcp, um canal de controle na porta 21/tcp do servidor. Para que exista a transferência de arquivos e informações diversas, o servidor remoto abre um canal de dados a partir da porta 20/tcp para uma porta acima de 1023/tcp no cliente. Já no modo passivo, tanto a conexão de controle, quanto à conexão para a transferir os dados são iniciadas do cliente para o servidor.

Domain Name System – DNS: também chamada de Name Service, esta aplicação relaciona endereços IP com os seus respectivos nomes atribuídos a dispositivos da rede.

Network File System – NFS: este sistema foi desenvolvido pela Sun Microsystems e permite que computadores possam "montar" discos ou parte deles (diretórios) de dispositivos remotos e operá-los como se fossem locais.

HyperText Transfer Protocol – HTTP: este protocolo é a base do ambiente *World Wide Web* (WWW) que basicamente permite a leitura dinâmica e interativa de documentos constituídos de texto, imagens e som.

Post Office Protocol – POP: esta aplicação tem como função permitir que um certo usuário acesse e obtenha mensagens de correio eletrônico que estão armazenadas em certo servidor. Normalmente as mensagens adquiridas pelo cliente são deletadas do servidor.

Simple Network Management Protocol - SNMP: este protocolo é utilizado para o gerenciamento de redes TCP/IP. Seus processos atuam como gerentes ou agentes e objetos são gerenciados para a coleta de informações úteis para o gerenciamento da rede. Estes objetos representam recursos, tais como sistema (estação de trabalho), gateway ou equipamentos de transmissão (*modem, bridge, concentrador*). Para cada objeto gerenciado é feito um mapeamento do mesmo como uma coleção de variáveis, onde os valores podem ser lidos e alterados. Os agentes recolhem a informação e os gerentes processam estas informações coletadas, com o objetivo de detectar falhas no funcionamento dos componentes da rede (*gateways, hosts*), de forma que possam ser tomadas providências para contornar os problemas gerados por estas falhas (CASE et al., 2002).

TELNET: esta aplicação tem como finalidade proporcionar a facilidade na comunicação bidirecional, com o objetivo de oferecer um método padronizado para a utilização de uma interface de dispositivos de terminais e/ou processos orientados a terminal (Chaves, 2003).

Internet Message Access Protocol – IMAP: também incorporado à camada de aplicação da arquitetura TCP/IP, este protocolo tem como objetivo permitir que um cliente acesse e manipule mensagens de correio de eletrônico dos servidores. Alguns mecanismos podem ser destacados nesta aplicação, como: manipulação remota de pastas contendo mensagens, efetuação de operações de criação, troca e exclusão de pastas; exclusão permanente de mensagens.

3 SNIFFERS

Conforme afirma Furmankiewicz (2000), sniffers são dispositivos que podem monitorar processos de transportes de dados em rede. Um sniffer é um dispositivo – seja hardware ou software – que pode ler todo pacote enviado por uma rede.

Sniffers geralmente são utilizados para identificar problemas de rede que, embora invisíveis para o usuário, degradam o desempenho da rede.

Portanto, *sniffer* é um programa que captura os pacotes que estão trafegando na rede e os exibe na tela ou armazena em disco para uma análise posterior. Apesar desta aparente mal intencionada função, as primeiras ferramentas de *sniffing* foram criadas com o objetivo de ajudar na administração de redes.

Na expressão "aparente mal intencionada função", é dada referência ao conceito e visão que muitas vezes um *sniffer* é tratado. Este tipo de ferramenta, para muitos, significa uma forma de "bisbilhotar" e investigar maldosamente o que está sendo feito nas outras máquinas, por outros usuários, no entanto pode servir como ferramenta de administração de redes.

Estes dispositivos podem ler e identificar toda e qualquer atividade que ocorra no nível de rede entre dois ou mais dispositivos nesta rede. Júnior e Filho (2002) afirmam que embora um *sniffer* possa ser utilizado de diversas maneiras e com diversos propósitos, o seu princípio de funcionamento continua sendo o mesmo: capturar e analisar tráfego de rede sem interferir no funcionamento desta. Na Figura 15 pode ser observada a arquitetura de um *sniffer,* mostrando detalhadamente o modo como interage com a rede e as etapas de captura de pacotes.

Na Figura 15 pode ser vista a arquitetura de uma *Sniffer*.

Figura 15. Arquitetura de um Sniffer
Fonte: Júnior e Filho (2002)

Segundo Furmankiewicz (2000), o termo "sniffer" éderivado de um produto, chamado *Sniffer* da Network General Corporation. Pelo fato da Network General Corporation ter dominado o mercado, este termo tornou-se popular e desde então os analisadores de protocolo passaram a ser chamados assim.

Para que seja possível capturar todos os pacotes trafegando na rede, é necessário colocar a placa de rede em *modo promíscuo*, ou seja, independente do endereço de destino do frame ser igual ou não ao da placa da máquina onde o sniffer está instalado, ele é lido como se fosse dele. Será visto mais detalhadamente o funcionamento de um *Sniffer* no próximo tópico. É o equivalente ao grampo telefônico, só que em escala muito maior pois, dependendo da forma como a rede foi montada, todos que estão ligados nela vão estar vulneráveis. Uma vez a placa de rede estando em modo promíscuo, o sniffer poderá

capturar e analisar qualquer tráfego que passe no segmento em que se encontra instalado. Na figura 16, é visto como uma placa de rede em modo promíscuo fica apta a capturar todos os pacotes que por ela passam.

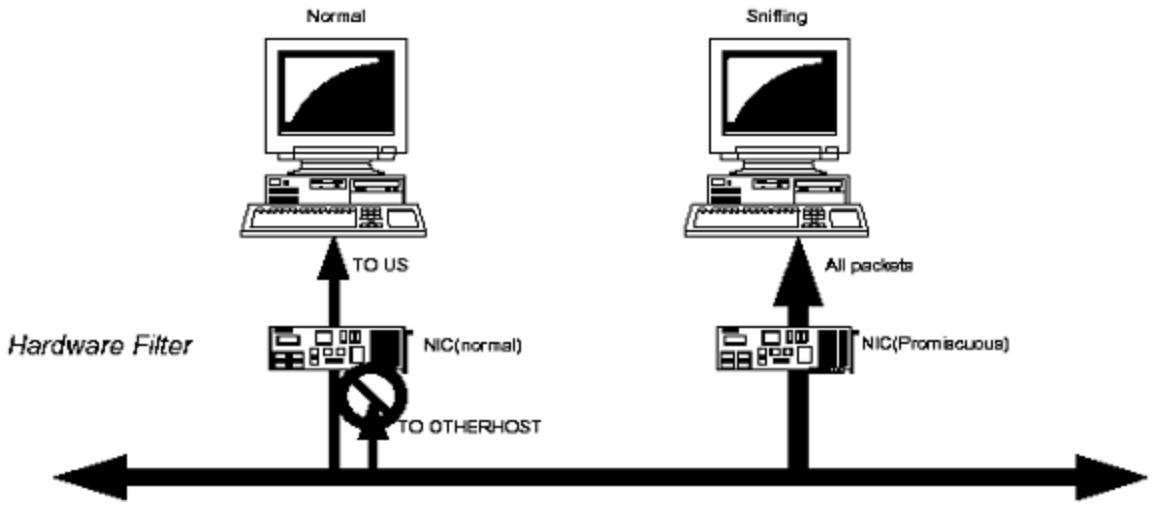


Figura 16: Demonstração de uma máquina com a placa de rede em modo promíscuo.
Fonte: SANAI (2001)

3.1 FUNCIONAMENTO DE UM *SNIFFER*

De acordo com Casagrande (2003), em uma rede *Ethernet* cada estação pertencente a ela possui uma interface que é chamada de NIC (*network interface card*). Esta interface possui um endereço físico (*MAC – media access control*) de 6 bytes atribuído pelo fabricante que a identifica na rede. Na Ethernet toda comunicação é baseada neste endereço de *hardware*. Esta interface pode ser configurada com vários filtros, podendo rejeitar ou receber determinados tipos de pacotes, como *unicast, broadcast* e *multicast*, por exemplo.

Casagrande (2003) descreve ainda que as estações da rede normalmente estão aptas a "escutar" e responder somente a pacotes endereçados a ela, pois a interface*Ethernet* que esteja funcionando normalmente deverá ignorar todo tráfego de rede que não seja direcionado a ela. Desta forma os pacotes que possuem os endereços MAC não direcionados a esta estação serão descartados por ela. Na rede *Ethernet* como estão em um mesmo meio compartilhado, é possível configurar esta interface para que capture todos os pacotes, independentes para qual endereço o mesmo tenha sido direcionado. Este tipo de funcionamento é definido como "modo promíscuo", e sob estas condições as estações de rede podem monitorar e capturar o tráfego de rede, mesmo que o endereço de destino não seja o seu.

Normalmente, *Sniffers* capturam os pacotes na rede, possibilitando ao administrador ter detalhes sobre os endereços de origem e destino, formação de pacotes, além dos dados e outras informações em nível dos protocolos utilizados na comunicação.

Uma das principais razões do aumento na utilização destes softwares surgiu devido à existência de protocolos inseguros como FTP, Telnet, POP entre outros. Estes protocolos são atribuídos como inseguros pelo fato de enviarem senhas em formato texto comum que são facilmente capturadas. A descoberta destas informações poderia fazer com que um usuário mal intencionado viesse a atacar sistemas e redes interconectadas e até mesmo outros dispositivos alocados nesta rede. A topologia da rede, a interface de comunicação e sua operação, os protocolos utilizados e o comportamento dos usuários são fatores importantes ao analisar-se o potencial de uso de um *sniffer*, principalmente quando o objetivo é a captura de informações alheias. A seguir é descrita a forma como os sniffers

são utilizados nos dois mais comuns segmentos de rede, comutada (o *switch*) e rede por difusão (*o hub*).

3.2 UTILIZAÇÃO DE SNIFFERS EM UM SEGMENTO DE REDE

Sniffers possuem a fama de serem programas ofensivos nas redes de computadores. De acordo com Casagrande (2003), muitos autores afirmam que para controlar estes problemas com sniffers na rede, basta substituir os *hubs* por *switches*. Hubs transmitem dados às estações por meio de barramento, onde todos os pacotes são distribuídos em um segmento único de rede e poderão ser lidos por todas as máquinas, caso a placa de rede esteja em modo promíscuo. Casagrande (2003) afirma que um segmento de rede é uma arquitetura que reside por detrás de um roteador, ponte, *hub* ou *switch*, onde cada nodo é endereçado por qualquer outro conectado ao segmento. Utilizando *hubs* para efetuar-se a conexão entre as máquinas, a distribuição do sinal se dará por todas as portas deste dispositivo, fazendo que todos os nodos de um segmento de rede tenham acesso aos pacotes transmitidos. Sendo assim, com a instalação de um *sniffer* em qualquer nodo deste segmento, existe a possibilidade de se capturar os dados que por ele trafegarem.

Na figura 17, pode-se comparar o funcionamento de um *hub* e um *switch*, onde as informações estão sendo enviadas do nodo A ao nodo D.

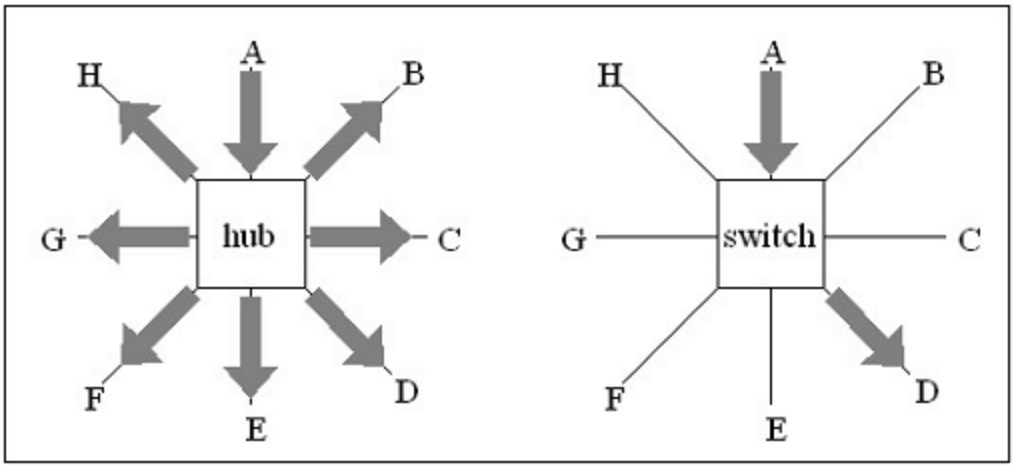


Figura 17. Funcionamento de um HUB e de um SWITCH
Fonte: Casagrande, R. (2003)

Apesar disto tudo e do direcionamento direto ao destino, os switches não foram desenvolvidos com o propósito de segurança e sim para a segmentação de tráfego, pois durante o tráfego existe o isolamento dos dados em cada uma de suas portas.

3.2.1 Redes de Difusão (Meio Compartilhado)

De acordo com Junior e Filho (2002) Redes de Difusão caracterizam-se pelo compartilhamento do meio de transmissão de dados, que nada mais é do que a camada de enlace da rede. É mais comum ser utilizada em configurações de pequeno porte, como redes domésticas e redes de pequenos laboratórios, isto porque seu custo de implementação é baixo.

Na Figura 18 pode ser vista a forma de inserção de uma ferramenta *sniffer* em uma rede de difusão. O *sniffer* é instalado em uma máquina qualquer, de forma que o meio

físico é compartilhado entre todas as estações, onde a captura dos dados que nesta rede torna-se de fácil execução para esta ferramenta.

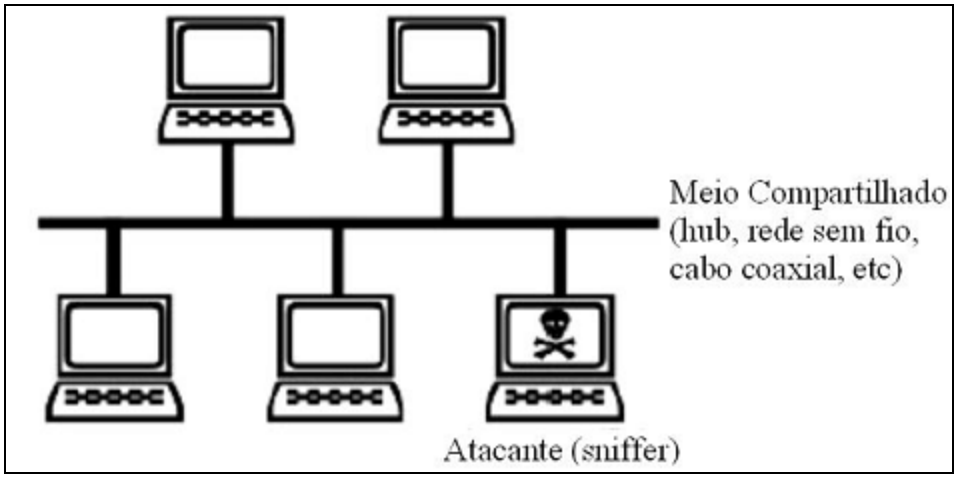


Figura 18. Sniffers em uma rede de meio compartilhado.
Fonte: Junior e Filho (2002)

3.2.2 Redes Comutadas

Junior e Filho (2002) afirmam que redes comutadas efetuam a transmissão e enlace de dados dedicado para cada máquina da rede. Um comutador é que realiza a distribuição do tráfego de dados pelo endereço de destino que cada pacote possui. O desempenho deste tipo de rede é considerado superior ao de redes de difusão, porém seu custo é bem mais alto, dada a necessidade de hardwares especializados.

A Figura 19 demonstra a forma de instalação de um *sniffer* em uma rede comutada.

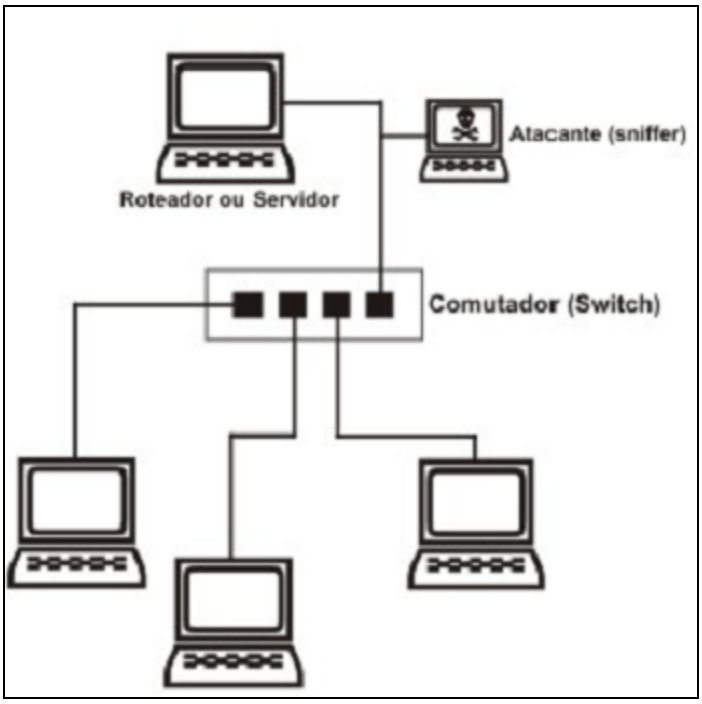


Figura 19. Instalação de um *sniffer* em uma rede comutada
Fonte: Junior e Filho (2002)

De acordo com Junior e Filho (2002) neste tipo de rede, com uma técnica que visa "enganar" diversos protocolos, é possível a um atacante capturar praticamente todo o tráfego da rede, mesmo tendo acesso apenas a uma máquina. Neste cenário, o atacante tenta enganar as máquinas da rede de forma que o tráfego seja redirecionado para um local onde possa ser capturado.

3.3 SNIFFERS MAIS UTILIZADOS

Atualmente existem dezenas de softwares *sniffers* desenvolvidos, com diversas finalidades e para vários sistemas operacionais. De acordo com Casagrande (2003) os

sniffers mais utilizados para os sistemas operacionais *Windows*, *Linux* e alguns também para *Unix* são:

a) ***Ethereal:*** é um analisador gráfico de protocolos de rede para ambientes Unix e Windows. Com ele é possível examinar o tráfego de dados na rede ou de registros de monitoração armazenados em disco. Neste último caso, possibilita percorrer os dados, visualizando informações de vários níveis para cada pacote. Esta ferramenta pode ser obtida em: http://www.ethereal.com

b) ***Ntop:*** O NTop é um aplicativo utilizado para Windows e Linux. Este Sniffer permite o monitoramento da atividade da rede de forma parecida à ferramenta *Top* do Unix, que informa quais são os processos que a CPU utiliza e o desempenho dela. Possui também uma interface HTML com uma série de estatísticas e gráficos.

c) **IPTraf:** O *IPTraf* é um utilitário de monitoramento de rede, com o modo texto para levantamento de estatísticas de rede para Linux. Este aplicativo agrupa uma série de informações como o total de pacotes e bytes trafegados pela rede, indicadores de atividade, detalhamento do tráfego TCP e UDP e total de pacotes e bytes trafegados pela estação de trabalho local.

d) **EtherApe:** é um monitor de rede gráfico para Unix. Com os modos Ethernet, IP e TCP, ele mostra a atividade da rede graficamente. As estações são representadas por pontos e o enlace entre eles por linhas que variam de espessura de acordo com o protocolo.

e) **TCPDump:** O TCPDump é um programa original do Linux que coloca a interface de rede em modo promíscuo, ou seja, aceitando todos os pacotes que trafegam pela rede. O *TCPDump* possui um mecanismo poderoso de filtragem de pacotes, de modo que pode armazenar apenas os dados que sejam de interesse.

f) ***Network Monitor:*** ferramenta que já vem inserida na instalação do Windows® NT/2000/ME.

g) ***Network Associates Sniffer:*** Produto de direitos comerciais da *Network Associates* e pode ser encontrado em http://www.nai.com

h) ***LanExplorer:*** Ferramenta bem conhecida neste meio. Pode ser obtido em http://www.intellimax.com/.

i) ***Sniffit:*** Este sniffer é muito utilizado para a análise de dados em nível de aplicação. Poderá ser obtido de forma gratuita em http://www.symbolic.it/Prodotti/sniffit.html

j) ***Analyzer:*** analisador de protocolo de domínio público. Pode ser obtido em http://netgroup-serv.polito.it/analyzer/

4 TRABALHOS CORRELATOS

A análise de rede e a implementação de ferramentas para estas análises têm sido desenvolvidas em muitos trabalhos científicos:

a) A Universidade Regional de Blumenau realizou pesquisas sobre a implementação de um protótipo para monitoração de pacotes em uma TCP/IP em ambiente Linux. O trabalho apresentou ainda um estudo sobre a segurança em redes de computadores. O protótipo foi desenvolvido para ambientes Linux. (Pompermayer Jr, 2002).

b) A Universidade Federal do Rio Grande do Sul apresentou um trabalho sobre formas de detecção de sniffers. Este trabalho visou descrever a forma de detecção de *sniffers* na rede, além dos cenários destas detecções e a efetuar a avaliação destas técnicas em uma rede local. As técnicas foram testadas em sistemas operacionais diferentes, como *linux* e *windows*. (Casagrande, 2003).

c) A Unesp - Universidade Estadual Paulista estudou o desenvolvimento de um sistema de captura de pacotes TCP/IP utilizado para a obtenção de assinaturas de ataque na determinação de comportamento anômalo para detecção de intrusos em redes de computadores. (De Souza, 2004).

d) A Universidade de São Paulo, André Franceschi de Angelis, autor do trabalho “Um modelo de tráfego de rede para aplicação de técnicas de Controle Estatístico de Processos”, utilizando a técnica de Controle Estatístico de Processos (CEP), trabalhou com a hipótese de que é possível

determinar estatisticamente o comportamento de uma determinada rede de um dado número de variáveis de interesse. Ao final, o modelo é representado por um conjunto de variáveis que descrevem o tráfego modelado. Este modelo foi construído através da observação da rede local do Instituto de Física de São Carlos (IFSC). (Franceschi, 2003).

5 ANÁLISE DO TRÁFEGO DA REDE DOS LABORATÓRIOS

Neste capítulo são apresentadas as formas como foram realizadas as coletas de dados, a maneira como foram definidas as estatísticas de amostragem, cenário das coletas e os resultados obtidos pela realização da análise das coletas. Dentre estas descrições apresentadas, é exposta ainda a descrição da ferramenta utilizada e a interface de rede analisada.

5.1 METODOLOGIA

Os resultados apresentados a seguir foram analisados e expostos resumidamente, já que a exposição completa dos diversos dados torna-se impraticável e de pouco benefício. Endereços de IP e outras informações privadas do tráfego de rede da universidade foram omitidas, garantindo a privacidade e restrição de acesso a estes dados.

Na primeira seção é descrita a técnica utilizada para a aplicação dos métodos estatísticos que conseqüentemente possibilitaram a realização das coletas. Posteriormente, ao decorrer do texto é descrito o cenário existente utilizado para a aplicação da ferramenta sobre a interface analisada, tipo de armazenamento realizado sobre os dados de cada coleta e por fim os resultados obtidos.

A seguir é descrita a técnica de amostragem estatística aplicada para a realização das definições dos horários, tempo de coleta e tamanho das amostras.

5.1.1 Técnicas de Amostragem Estatística

Esta etapa do trabalho constituiu na decisão e implementação do método de amostragem estatística que foi aplicado para a realização das coletas dos dados. Dentre os métodos existentes, a técnica de Amostragem Estratificada foi a escolhida para realização deste trabalho. O objetivo principal em aplicar esta técnica consistiu em estimar algumas propriedades do tráfego original a partir da amostras de pacotes. Barbetta (2005) descreve que em pesquisas científicas, quando se quer conhecer características de uma população, é comum observar-se apenas uma amostra dos elementos totais. Na aplicação de amostragem estatística por levantamento de amostras, a escolha pelos elementos que serão observados consiste em aplicar uma metodologia adequada, onde os resultados da amostra sejam informativos, caracterizando toda a população.

A técnica de amostragem estratificada consiste em retirar amostras por meio de *estratos* de uma certa população, como pode ser visto na sub-seção seguinte.

5.1.1.1 Amostragem Estratificada

Nesta seção descreve-se a técnica de Amostragem Estratificada que foi utilizada na análise de tráfego de rede e a forma de utilização desta técnica para a redução do volume de dados da amostra.

Kamienski (2005) descreve que numa amostragem estratificada, uma população de N unidades primeiramente é dividida em subpopulações ou estratos de N_1, N_2, N_3 ,..N_x. A

soma das subpopulações deve resultar no total da população, onde $N_1 + N_2 + N_3 + ... + N_x = N$. Para que todos os benefícios da estratificação sejam adquiridos os valores de cada um dos estratos (N_j) devem ser conhecidos. Assim que os estratos estiverem definidos, seleciona-se uma amostra de cada um deles, sendo as seleções feitas diferentemente para cada um dos estratos. Os valores das amostras dentro de cada estrato são denominados n_1, $n_2 ... n_L$.

A estratificação é uma técnica comum que pode proporcionar o aumento de precisão nas estimativas das características da totalidade da população (Cocharan, 1997). De um modo geral, é possível dividir uma população heterogênea em várias subpopulações que separadamente sejam homogêneas. Se todas as subpopulações são homogêneas, considerando que os valores das medidas de cada uma das unidades variem pouco entre si, pode-se obter uma estimativa precisa do valor médio de um estrato qualquer mediante a análise de uma pequena amostra deste estrato (Kamienski, 2005). Por fim, as estimativas de cada uma das subpopulações podem ser combinadas para constituírem uma estimativa precisa do conjunto da população.

Barbetta (2005) afirma que a técnica de amostragem estratificada pode ser dividida de duas formas: *proporcional* e *uniforme*.

Na amostragem estratificada proporcional, a proporcionalidade do tamanho de cada estrato de uma população é mantida na amostra, ou seja, o número de elementos de cada estrato é proporcional ao tamanho do estrato. Por exemplo, se um determinado estrato corresponde a 30% do total de uma população, então ele deve corresponder a 30% da amostra.

Na amostragem uniforme a seleção do número de elementos de cada estrato é feita de forma idêntica. A amostragem estratificada uniforme costuma ser utilizada em que o maior interesse é obter valores de estimativas separadas para cada estrato.

Para a realização deste trabalho foi utilizada a técnica de Amostragem Estratificada Proporcional. Nas seções abaixo pode ser vista a forma que esta técnica foi aplicada sobre os dados obtidos pela amostra total de um dia[1].

5.2 DEFINIÇÃO DOS HORÁRIOS E TEMPO DE CADA COLETA

Para a definição dos horários das coletas foram feitas algumas entrevistas com funcionários responsáveis pela administração e gerenciamento da rede da UNESC. O objetivo principal destas entrevistas foi o de obter informações necessárias para início das coletas dos dados. Conforme informações obtidas, foi definido que o período de maior tráfego na rede e utilização dos laboratórios está entre 08 e 22 horas.

Com base nestas informações, a definição dos horários das coletas foi feita por meio da realização de uma coleta de dados do tráfego de um dia, que posteriormente serviu de base para o cálculo de algumas variáveis, como por exemplo, população total, estratos e tamanho das amostras de cada estrato. Esta coleta foi feita no período de um dia, das 08 às 22 horas.

[4] Neste trabalho entende-se um dia como sendo o período em que foram feitas as coletas, ou seja, das 08 às 22h.

Após a realização desta *coleta base*[2], algumas variáveis foram definidas, possibilitando o cálculo do tempo e tamanho de cada amostra. As variáveis necessárias para esta etapa foram:

a) ***População:*** definiu-se como população o tamanho total em megabytes do volume de dados coletados por meio da *coleta base*. Total em megabytes das 14 horas da coleta.

b) ***Estratos ou subpopulações***: para a realização das coletas, os estratos foram definidos como sendo o total em megabytes do volume de tráfego de dados durante o período de uma hora. Representou o total do tráfego atribuído a cada hora diante do total de horas que foram coletadas.

Com os valores definidos para cada uma das variáveis citadas, o cálculo do tamanho e tempo de cada amostra pôde ser realizado. Baseado na técnica de amostragem estratificada, primeiramente foi realizado o cálculo da porcentagem de cada estrato perante o valor total da população. Este cálculo foi feito por meio da aplicação da seguinte fórmula:

$$p = (E/P)$$

onde,

p= porcentagem representativa do valor do estrato diante do valor da população.
E= estrato
P= população

Com o valor da porcentagem representativa do estrato diante da população, o tamanho de cada amostra foi atribuído pela seguinte fórmula:

[5] Coleta Base foi o nome atribuído a coleta realizada inicialmente para que os valores de cada variável fossem definidos.

$$t = p * E$$

onde:

t= tamanho da amostra para cada hora.

Após a definição dos valores do tamanho de cada amostra, por fim o tempo de cada amostra foi definido então pela fórmula abaixo:

$$f = t / E$$

onde:

f= tempo (em horas) de coleta a cada hora

Para facilitar a identificação do tempo de cada amostra, os valores resultantes da fórmula acima foram convertidos para minutos e segundos.

Todos os cálculos realizados para definição dos horários, tempo de cada amostra, tamanho dos estratos e tamanho de cada amostra foram realizados sobre os valores adquiridos pela realização da *coleta base*. Nas Tabelas 2 e 3 podem ser visualizados os valores (em megabytes) do volume de tráfego de cada hora encontrados pela realização desta coleta.

Tabela 2. Volume de tráfego por hora – Período: Das 08 às 15h.

Períodos	**08 às 9h**	**09 às 10h**	**10 às 11h**	**11 às 12h**	**12 às 13h**	**13 às 14h**	**14 às 15h**
Volume em MB	3.672	5.364	4.320	1.296	2.988	3.060	3.168

Tabela 3. Volume de tráfego por hora – Período: Das 15 às 22h.

Períodos	**15 às 16h**	**16 às 17h**	**17 às 18h**	**18 às 19h**	**19 às 20h**	**20 às 21h**	**21às 22h**
Volume em MB	4.140	3.384	1.764	4.032	18.072	19.296	7.812

Os valores demonstrados nas Tabelas 2 e 3 acima foram coletados pelo programa *Multi Router Traffic Grapher (MRTG)*[1]. Este programa foi instalado no *proxy* dos laboratórios. Com esta ferramenta foi possível realizar e visualizar por meio de gráficos o comportamento do tráfego referente ao volume de dados na rede durante certo intervalo de tempo. O gráfico gerado pelo *MRTG* identificou no eixo *Y* escalas de tráfego de dados em megabytes por segundo (MBps) e no eixo *X* apresentou o intervalo de tempo dividido em horas. Posteriormente, na análise realizada sobre o gráfico, foi feito um mapeamento do mesmo, onde cada hora identificada foi dividida em escalas menores de 12 minutos, ou seja, cada hora foi dividida em 5 partes iguais. Para cada ponto de divisão, foi feita uma marcação de identificação do valor em MBps correspondente ao eixo *Y*. Ao final, os valores de cada ponto identificado foram somados, representando desta forma o volume total de dados trafegados na hora analisada.

O gráfico citado no parágrafo acima pode ser visto na Figura 20.

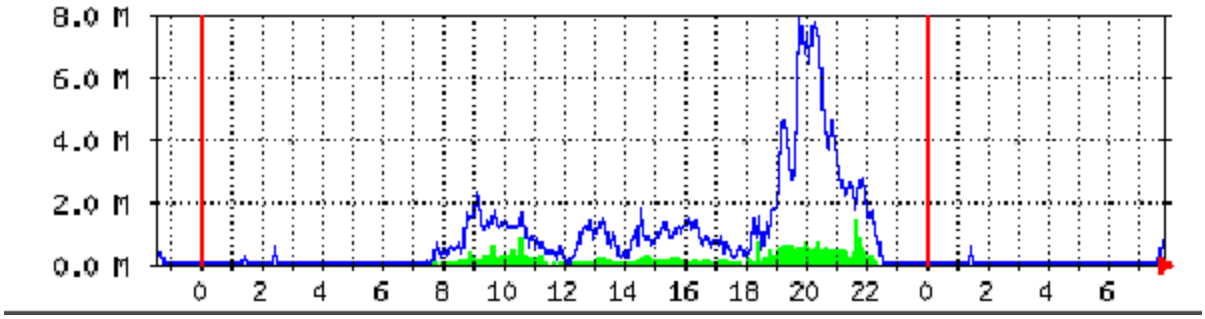


Figura 20. Gráfico do tráfego da UNESC gerado pelo *MRTG*.

[6] O Multi Router Traffic (MRTG) é uma ferramenta que utiliza o protocolo *SNMP* para obtenção dos dados da rede e gera gráficos indicativos do consumo de banda em redes.

O mapeamento dos valores foi feito sobre os pontos gerados pela linha azul do gráfico anterior, identificando o tráfego gerado pela interface *Eth1*. Os detalhes das informações das capturas dos dados são descritos na seção 5.3.

Com a identificação dos valores do tráfego da rede, os horários e tempo de cada coleta foram definidos conforme descrito na seção abaixo.

5.2.1 Horários e Amostras Definidas

Os dados foram coletados no período de 15 a 19 de maio de 2006. Pela técnica de amostragem estratificada foi possível executar o cálculo do tamanho das amostras de cada hora durante o dia, onde posteriormente, baseado no tamanho da amostra foi possível formular o cálculo do tempo de cada amostra nas horas determinadas.

O total das amostras coletadas durante a semana representou um dia de tráfego, ou seja, as quatorze horas estabelecidas para a realização das coletas foram divididas durante a semana da coleta, onde para cada dia foram realizadas amostras de horários pré-determinados. Na Tabela 4 podem ser vistos os horários pré-definidos, assim como também a identificação do número da coleta conforme dia e horário.

Tabela 4. Horários e tempo de duração de cada coleta.

Dias da semana	Coleta	Horários	Dur. da coleta
4ª FEIRA	1	08h às 09h	2 min e 41 seg
3ª FEIRA	2	09h às 10h	3 min e 55 seg.
	3	10h às 11h	3 min e 9 seg.
	4	11h às 12h	57 seg.
5ª FEIRA	5	12h às 13h	2 min e 11 seg.
	6	13h às 14h	2 min e 14 seg.
	7	14h às 15h	2 min e 19 seg.
4ª FEIRA	8	15h às 16h	3 min e 01 seg.
	9	16h às 17h	2 min e 28 seg.
	10	17h às 18h	1 min e 18 seg.
	11	18h às 19h	2 min e 57 seg.
6ª FEIRA	12	19h às 20h	6 min e 35 seg.
	13	20h às 21h	7 min e 02 seg.
	14	21h às 22h	5 min e 42 seg.

Para os horários de sexta-feira, no período das 19 às 20h e das 20 às 21h o tempo de coleta foi reduzido, pois pelo cálculo inicial, para cada uma destas amostras seria necessário manter a ferramenta de coleta capturando dados por mais de 12 minutos, o que possivelmente poderia causar algum dano ao *proxy* dos laboratórios devido à sobrecarga de processamento e armazenamento dos dados.

5.3 CENÁRIO

Nesta seção do trabalho estão descritos os itens necessários para a realização da coleta, como: software utilizado, local de instalação, armazenamento de dados, escopo da rede definido para a análise, entre outros.

A ferramenta utilizada para a realização deste trabalho foi o software *Ethereal*. Este software foi instalado no servidor *proxy* dos laboratórios no sistema operacional Linux. Para a realização das capturas de dados, foi monitorada a interface de rede *ETH1*. Esta interface incorpora todo o tráfego interno proveniente dos laboratórios e também recebe o tráfego originado de requisições internas feitas à rede externa e direciona estes dados novamente aos laboratórios.

5.3.1 Escopo da Rede

Dentre as áreas possíveis para a realização deste trabalho, decidiu-se por executar a análise nos laboratórios da UNESC. A escolha foi motivada pelo fato que nesta área da rede o tráfego é variado devido às várias finalidades de uso a que se destina às estações pertencentes aos laboratórios.

Empiricamente, idealizou-se por identificar o tráfego dos laboratórios visando a exposição de dados mais diversificados, originados pela variedade e diferenciação da forma de uso com que cada usuário desempenha sobre as estações.

Atualmente, dentre os 20 laboratórios existentes, cerca de 480 estações estão inseridas e são utilizadas diariamente por acadêmicos de cursos diversos. Cada uma destas estações possui softwares específicos, que significativamente podem ser ditos como responsáveis pela variedade do tráfego.

5.3.2 Utilização da Ferramenta *Ethereal* nas Coletas dos Dados

Para a realização das coletas de dados e análise do tráfego da rede foi utilizado o software *Ethereal*. Esta ferramenta é um analisador de redes que permite examinar dados em tempo real ou de um segmento de rede específico informado e possibilita que os dados coletados possam ser armazenados em disco (CAMY, 2003). Neste trabalho foi utilizada a versão 0.10.14. Dentre as suas vantagens de utilização, destaca-se a sua interface gráfica, caracterizando-se por proporcionar praticidade na manipulação e análise dos dados coletados. Também caracteriza-se pela vantagem oferecida na navegação entre os quadros capturados e pelo grande número de protocolos que podem ser identificados. Esta ferramenta permite a visualização gráfica dos pacotes, identificando os protocolos campo a campo e mostrando o valor correspondente a cada campo.

O *Ethereal* caracteriza-se ainda por possibilitar a leitura e escrita de arquivos que possuem formato compatível com outros programas, como por exemplo, o *TCPDUMP*.

Dentre as características já mencionadas, destacam-se ainda:

a) Podem ser feitas capturas em vários tipos de interfaces física de rede, como: *Ethernet*, *PPP*, *Token-Ring*, entre outras.

b) Permite a criação de filtros no canal de comunicação. Esta funcionalidade proporciona a organização do material recolhido, onde apenas os protocolos caracterizados são mostrados.

c) Possibilita a criação de filtros para a captura na rede, onde serão aceitos somente protocolos pré-determinados, permitindo a restrição do número de

protocolos que serão mostrados ao usuário. Esta utilidade disponível no software permite enfocar a análise em certos protocolos e não em todo o tráfego da rede.

A forma como o tráfego é demonstrado pelo *Ethereal* segue a seguinte ordem: listagem dos pacotes capturados (1), detalhe sobre os protocolos pertencentes a cada um dos pacotes (2) e conteúdo hexadecimal de um pacote (3). Estes campos descritos podem ser visualizados na Figura 21.

Para visualizar os detalhes de um certo pacote, este deverá ser ativado e em seguida poderão ser observados os diferentes níveis de protocolos presentes, como o Ethernet, IP, TCP e HTTP.

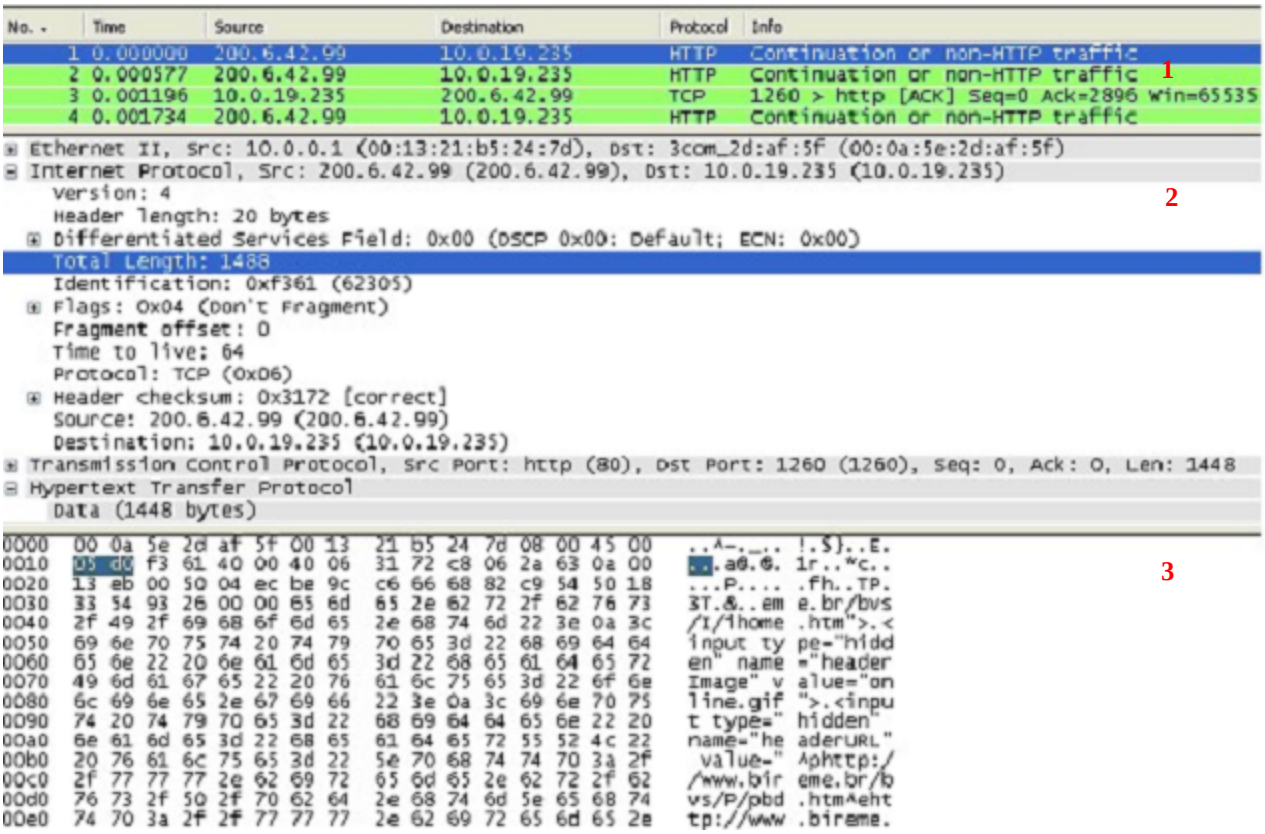


Figura 21. Forma de tráfego demonstrada pelo *Ethereal*.

5.3.2.1 Aplicação de Filtros Sobre os Arquivos Coletados

Das facilidades disponibilizadas pela ferramenta utilizada, a aplicação de filtros foi de suma importância, cuja aplicação proporcionou a manipulação dos dados de cada uma das coletas, onde o acesso às informações dos pacotes coletados foi facilitado e permitiu que desta forma estatísticas e comprovações de números fossem feitas seguramente.

A utilização dos filtros foi aplicada principalmente para possibilitar a identificação dos protocolos e aplicações que estiveram presentes nas coletas realizadas. Na Figura 22 pode ser vista a área do software utilizada para este fim e na tabela 5 são mostradas algumas das expressões utilizadas para a filtragem dos dados de determinada coleta, bem como o resultado da aplicação de cada uma das expressões.

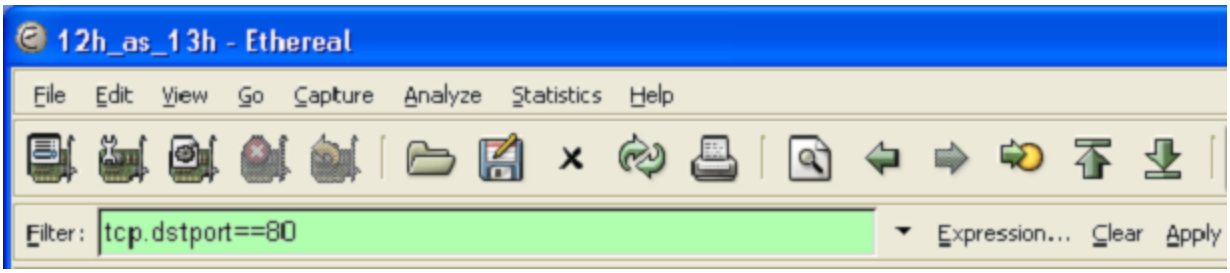


Figura 22. Área do software para aplicação de filtros sobre a coleta analisada

Na figura acima a aplicação do filtro exposto retorna todos os pacotes que tenham no campo “Destination port”, localizado no cabeçalho do protocolo TCP, o valor 80. Como objetivo principal da aplicação deste filtro, destina-se a identificação de pacotes do protocolo de transporte *Transmission Control Protocol (TCP)* direcionados à porta número 80 (http).

Tabela 5. Alguns dos principais filtros utilizados para a identificação do tráfego das coletas.

EXPRESSÃO	DESCRIÇÃO
ip.proto == 0x11	Mostra somente o tráfego referente ao protocolo UDP
ip.proto == 0x06	Mostra somente o tráfego referente ao protocolo TCP
tcp.dstport == 80 || tcp.srcport == 80	Porta de destino ou origem sejam igual a 80.
eth.type == 0x0800	Mostra apenas os pacotes que utilizaram o protocolo IP
Tpc || udp	Mostra apenas pacotes dos protocolos TCP ou UDP
Nbns	Mostra apenas os pacotes do serviço NetBios Name Service
eth.type != 0x0800	Trafego de pacotes Não-IP
not(tcp) && udp	Não traz os pacotes do protocolo ‘ TCP’ . Somente pacotes ‘ UDP’

5.3.3 Armazenamento e Dados Coletados

Os dados observados diretamente sobre a rede em análise foram coletados e gerados em arquivos pela própria ferramenta de coleta, o *Ethereal*. Estes arquivos foram armazenados em disco e posteriormente puderam ser visualizados e analisados novamente por meio desta ferramenta.

Esta forma de manipulação dos arquivos proporcionou grande facilidade na identificação dos dados coletados, onde a qualquer momento pôde ser feita a visualização dos dados coletados de determinado horário. A Figura 23 mostra as linhas e identificações proporcionadas pelo *Ethereal* sobre os pacotes coletados. Podem ser visualizadas informações detalhadas pelas camadas de divisão do pacote e cabeçalhos de cada um dos protocolos.

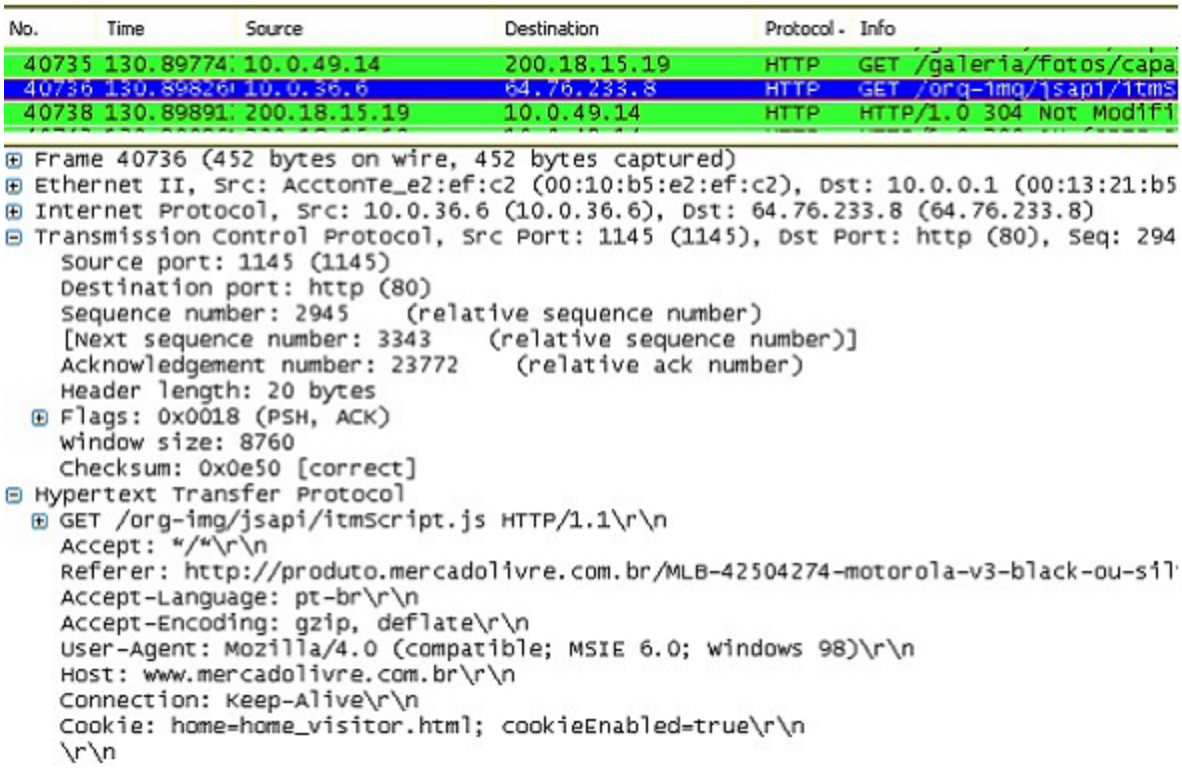


Figura 23. Janela principal do Ethereal com as identificações do pacote selecionado.

Para cada coleta realizada foi criado um arquivo de armazenamento contendo as informações da respectiva coleta. Estes arquivos foram identificados de forma que cada um deles recebeu o nome do período da realização em que a coleta foi feita, como por exemplo *"8h_as_9h"*.

5.4 DIFICULDADES ENCONTRADAS

Do mesmo modo que a maioria das atividades que envolvem desenvolvimento de opinião e conhecimento, para a realização deste trabalho muitas foram às dificuldades encontradas.

Indiferentemente, pelo surgimento das situações encontradas para o desenvolvimento do trabalho, inicialmente encontrou-se grande dificuldade relacionada à escolha da ferramenta a ser utilizada para a realização da coletas de dados. A primeira delas a ser estudada e fortemente cogitada para esta etapa, foi o software *Network Top (NTOP).* Grandes estudos foram realizados sobre este software e a escolha para a utilização deste foi quase que concretizada. A decisão pela não utilização do software, que por sinal já se encontrava instalado no servidor *proxy* dos laboratórios, surgiu devido não se ter encontrado uma forma de se armazenar em arquivos as coletas a serem realizadas, onde surgiu a idéia de armazenar as informações em arquivos de extensão "*.htm*", porém esta possibilidade foi descartada, evidenciando-se que as informações não seriam precisas.

Posteriormente, uma outra etapa do trabalho que expôs grande dificuldade foi a decisão pela implantação de um método de amostragem estatística que garantisse a realização de amostras precisas e que a coleta de pequenas quantidades de dados pudesse expôr precisamente as informações contidas nestes arquivos. Vários encontros foram feitos com professores da área estatística, e muitas situações foram criadas e analisadas para esta decisão. Dentre todas as possibilidades abordadas, baseando-se em explicações de bibliografias conceituadas e conhecimento profissional destes professores, mais esta etapa foi concretizada com sucesso.

Após a decisão da ferramenta a ser utilizada para a realização das coletas, necessitou-se a prestação de serviços dos profissionais encarregados pelo gerenciamento e controle da rede da UNESC. Devido ao fato de que a ferramenta *NTOP* foi descartada para a realização das coletas, foi necessário contar com a ajuda destes profissionais para a instalação do novo software no servidor dos laboratórios, o *Ethereal*, cuja liberdade de

instalação não pode ser direcionada a qualquer usuário ou até mesmo qualquer profissional da UNESC.

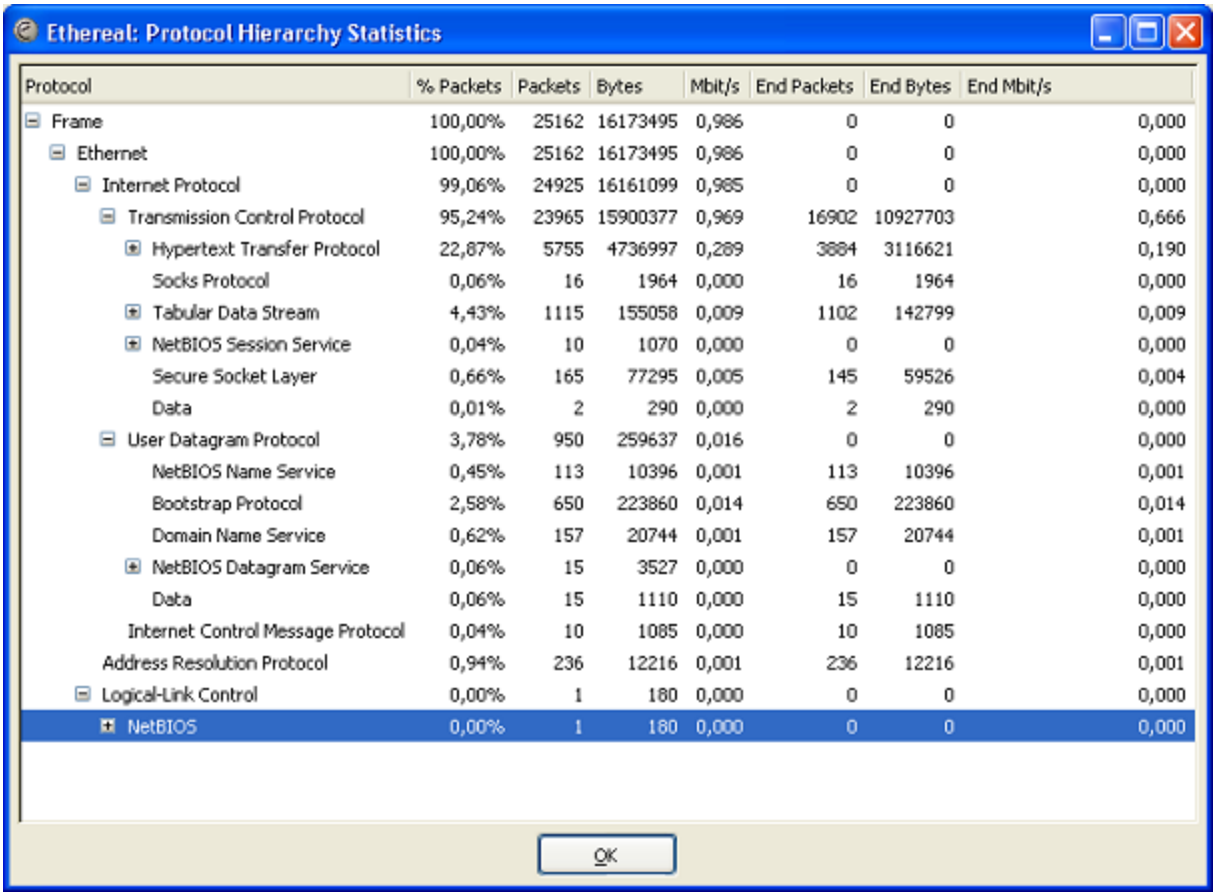
Por fim, com os dados coletados, foi necessário criar métodos claros e objetivos de se mostrar informações coletadas, objetivando o entendimento facilitado do conteúdo da pesquisa.

5.5 RESULTADOS OBTIDOS

Nesta etapa do trabalho são apresentadas ferramentas de auxílio a amostragens estatísticas, como gráficos e tabelas, mostrando os resultados obtidos neste trabalho, convenientemente agrupados e resumidos.

A realização da análise sobre os dados coletados foi proporcionada e facilitada pela ferramenta utilizada, o *Ethereal*. Os dados coletados puderam ser identificados de forma explicita e objetiva, proporcionada pela disposição de ferramentas auxiliares encontradas neste software, como por exemplo, a janela de *hierarquia de protocolos*, onde puderam ser demonstrados os protocolos, aplicações e serviços existentes na rede. Por esta tela, o número de pacotes e bytes encontrados em cada coleta pôde ser identificado de acordo com o seu protocolo de origem e obteve-se acesso a informações sobre os campos de cada camada de protocolo, podendo-se identificar o nível de tráfego de cada pacote sobre a arquitetura *TCP/IP* e também dos pacotes dos protocolos que não utilizam o *IP* como protocolo de rede.

Na Figura 24 pode ser visualizada a janela de *Hierarquia de Protocolos*, onde foi possível o acesso a diversas informações sobre os pacotes. Nesta mesma figura pode-se observar os níveis dos protocolos existentes nos pacotes originados do tráfego da rede analisada. São mostrados o número de pacotes e a quantidade em bytes do tráfego de rede identificado separadamente por protocolo ou aplicação.



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	25162	16173495	0,986	0	0	0,000
Ethernet	100,00%	25162	16173495	0,986	0	0	0,000
Internet Protocol	99,06%	24925	16161099	0,985	0	0	0,000
Transmission Control Protocol	95,24%	23965	15900377	0,969	16902	10927703	0,666
Hypertext Transfer Protocol	22,87%	5755	4736997	0,289	3884	3116621	0,190
Socks Protocol	0,06%	16	1964	0,000	16	1964	0,000
Tabular Data Stream	4,43%	1115	155058	0,009	1102	142799	0,009
NetBIOS Session Service	0,04%	10	1070	0,000	0	0	0,000
Secure Socket Layer	0,66%	165	77295	0,005	145	59526	0,004
Data	0,01%	2	290	0,000	2	290	0,000
User Datagram Protocol	3,78%	950	259637	0,016	0	0	0,000
NetBIOS Name Service	0,45%	113	10396	0,001	113	10396	0,001
Bootstrap Protocol	2,58%	650	223860	0,014	650	223860	0,014
Domain Name Service	0,62%	157	20744	0,001	157	20744	0,001
NetBIOS Datagram Service	0,06%	15	3527	0,000	0	0	0,000
Data	0,06%	15	1110	0,000	15	1110	0,000
Internet Control Message Protocol	0,04%	10	1085	0,000	10	1085	0,000
Address Resolution Protocol	0,94%	236	12216	0,001	236	12216	0,001
Logical-Link Control	0,00%	1	180	0,000	0	0	0,000
NetBIOS	0,00%	1	180	0,000	0	0	0,000

Figura 24. Tela de Hierarquia de protocolos

Baseado nas Figuras 25 e 26, constatou-se que o período de maior tráfego nos laboratórios da UNESC está compreendido entre 19 e 21 horas. Na Figura 25 que compreende os horários das 8 às 15 horas, o maior tráfego está entre 9 e 10 horas. Constata-se desta maneira que a causa deste aumento de tráfego neste horário, justifica-se por acadêmicos deslocarem-se aos laboratórios para a utilização das máquinas. Já no período

das 11 às 12h compreende o menor tráfego, justificado pelo motivo do término das aulas às 11:35h.

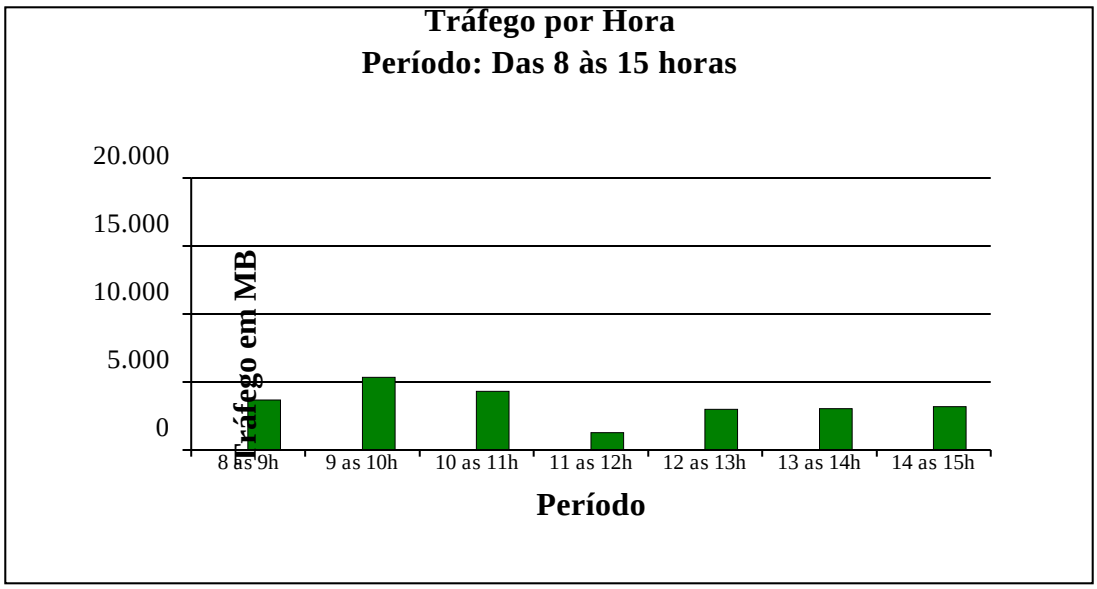


Figura 25. Tráfego por hora – Período: Das 8 às 15 horas.

Conforme pode ser observado na Figura 26, o horário de maior tráfego está compreendido no intervalo entre 20 e 21 horas. Da mesma forma que constatado na análise do tráfego do período demonstrado na Figura 25, este volume de tráfego é ocasionado devido ao acesso feito pelos acadêmicos às estações destes laboratórios no intervalo das aulas no período noturno.

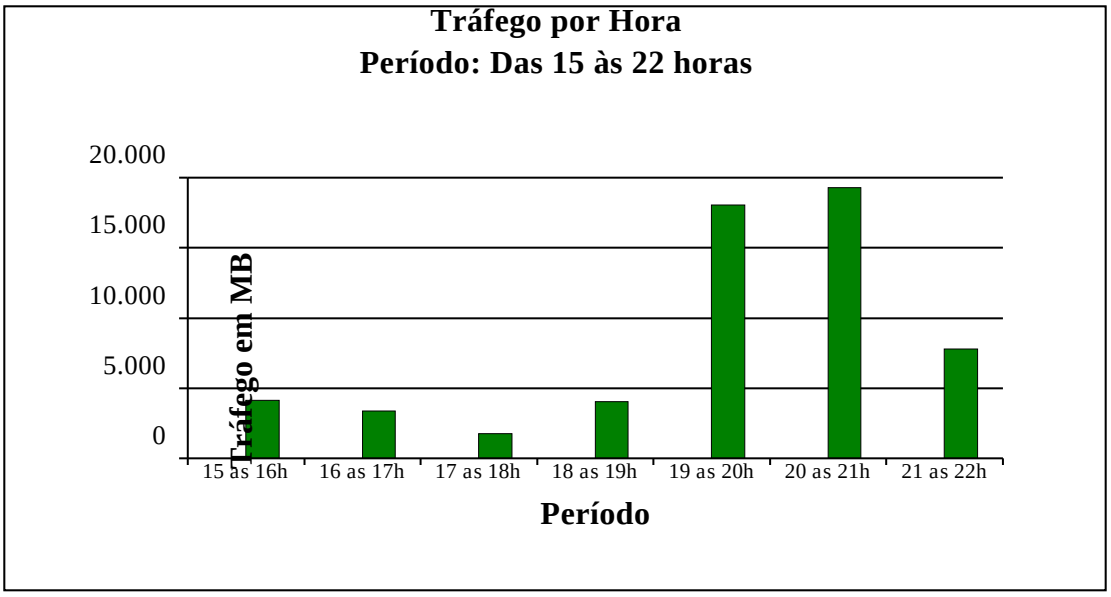


Figura 26. Tráfego por hora – Período: Das 15 às 22 horas.

O acesso às estações dos laboratórios e utilização dos recursos da rede incorpora principalmente a pesquisa na Internet, acesso a e-mails por páginas de provedores deste serviço e acesso a páginas diversas. Estes resultados são firmados perante a visualização da Figura 27, onde foi constatado que 78% dos pacotes de aplicações e serviços encontrados na rede contiveram o *HTTP* e o *DNS* como protocolos deste nível.

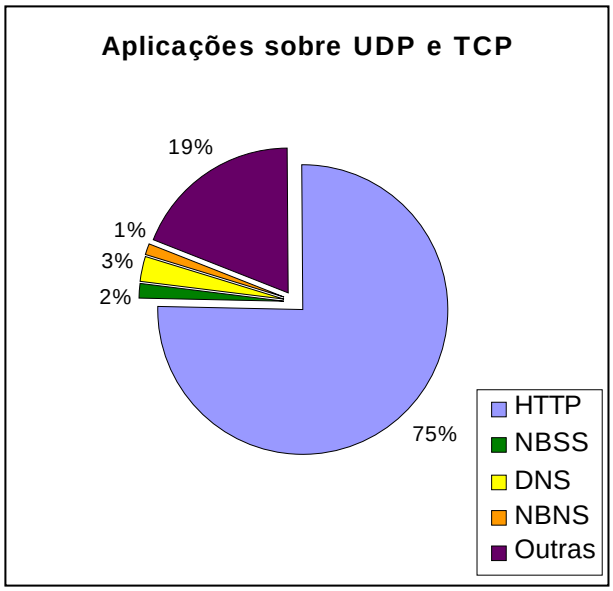


Figura 27. Relação do tráfego de aplicações sobre os protocolos *TCP* e *UDP*

Numa visão geral, cerca de 45% do tráfego total diário dos laboratórios da UNESC está compreendido nos horários das 19 às 21 horas. Esta estatística é justificada pela utilização de todos os laboratórios no período noturno. Na Figura 28 pode-se ter uma visão completa do volume de tráfego em pacotes de cada hora perante o tráfego diário total.

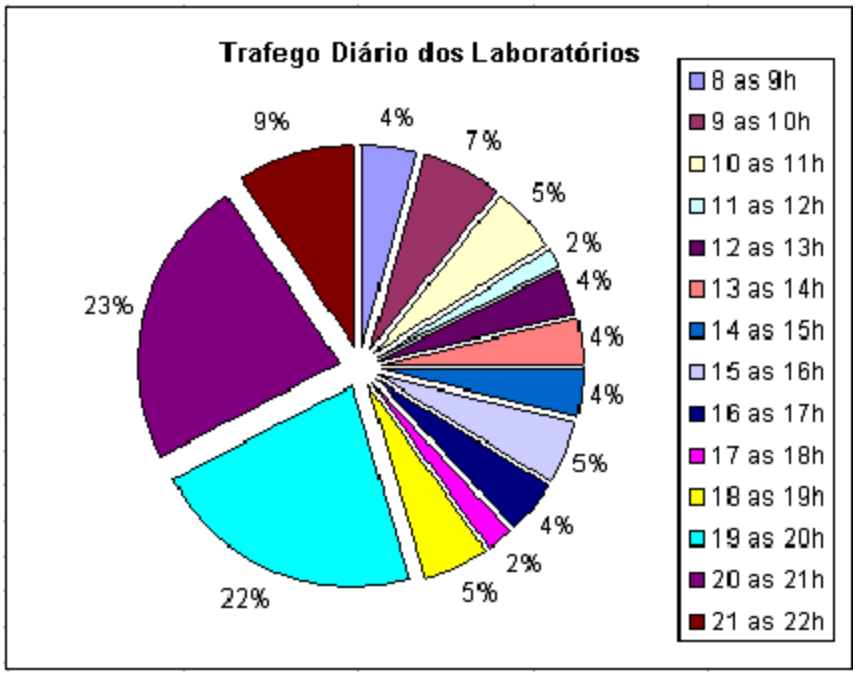


Figura 28. Tráfego Diário dos Laboratórios.

Perante a realização das 14 coletas na semana, pela verificação no número de pacotes, constatou-se que 99% de todo tráfego da rede dos laboratórios da UNESC é realizado sobre o protocolo de rede *Internet Protocol (IP).*

Os valores demonstrados na Figura 29 consistem a soma de todos os pacotes das 14 coletas realizadas, onde se obteve que dos *1.011.249* pacotes coletados, *1.004.651* corresponderam a pacotes que trafegaram sobre o protocolo IP. O restante dos *6.598* pacotes corresponderam ao tráfego de pacotes sobre protocolos Não IP, identificados principalmente pelos protocolos *Address Resolution Protocol (ARP)*, *Netbios* e *Internet Packet eXchange (IPX).*

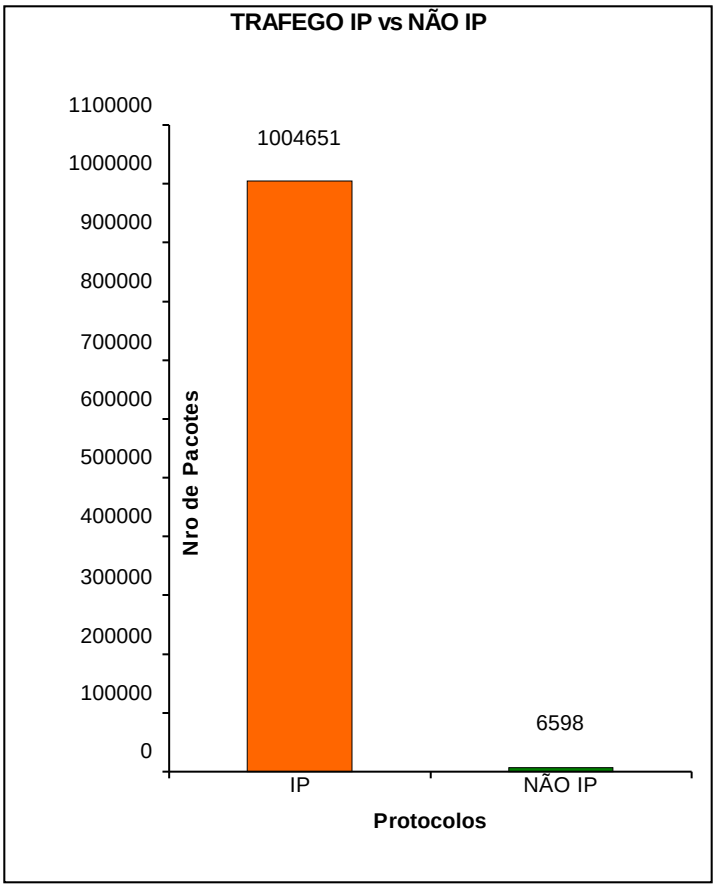


Figura 29. Demonstração em número de pacotes do tráfego IP versus Não IP.

Conforme pode ser observado na Figura 30, de todo o tráfego sobre o protocolo de rede *IP*, pouco menos de 98% dos pacotes pertenceram ao protocolo de transporte *Transmission Control Protocol (TCP)*, sendo o restante dos pacotes identificados com os protocolos *UDP*, *ICMP*, *IGMP*.

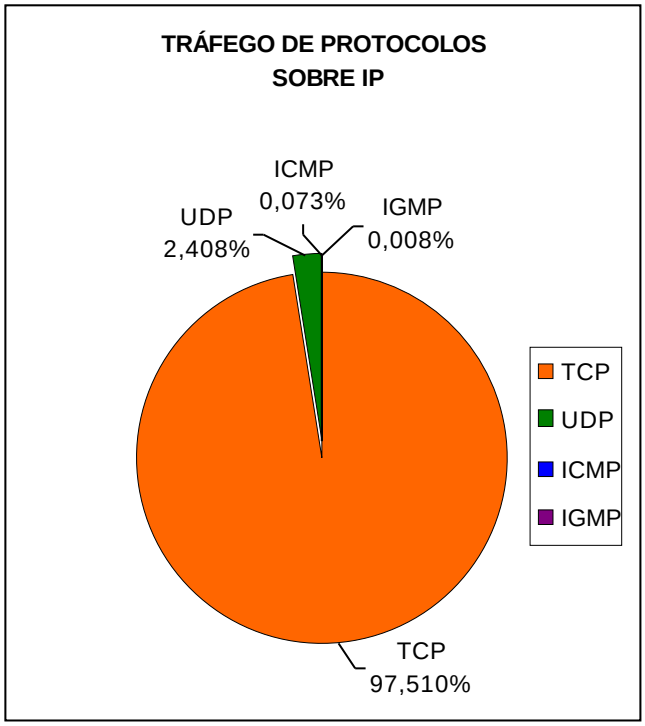


Figura 30. Relação de pacotes que trafegaram sobre o protocolo IP.

Pela visualização da Tabela 6, pode ser constatada a amostragem feita na Figura 30, analisando detalhadamente o número de pacotes identificados para cada protocolo.

Tabela 6. Relação do número de pacotes trafegados sobre o protocolo IP

COLETA	PROTOCOLO			
	TCP	UDP	ICMP	IGMP
1	45.400	583	32	4
2	73.999	1.084	55	0
3	62.422	1.013	42	6
4	9.516	299	22	0
5	23.965	950	10	0
6	28.640	3.483	32	0
7	24.067	5.464	11	2
8	34.813	1.225	38	0
9	64.389	644	30	0
10	20.550	376	18	2
11	34.177	584	44	2
12	217.637	3.616	237	43
13	210.989	2.592	80	4
14	129.076	2.278	86	20
Total	**979.640**	**24.191**	**737**	**83**

Das estatísticas resultantes do tráfego de pacotes que não utilizaram o IP como protocolo de rede, pode-se afirmar que a significância de menos de 2% do tráfego resultou na identificação dos protocolos *ARP*, *Netbios*, *IPX* e outros.

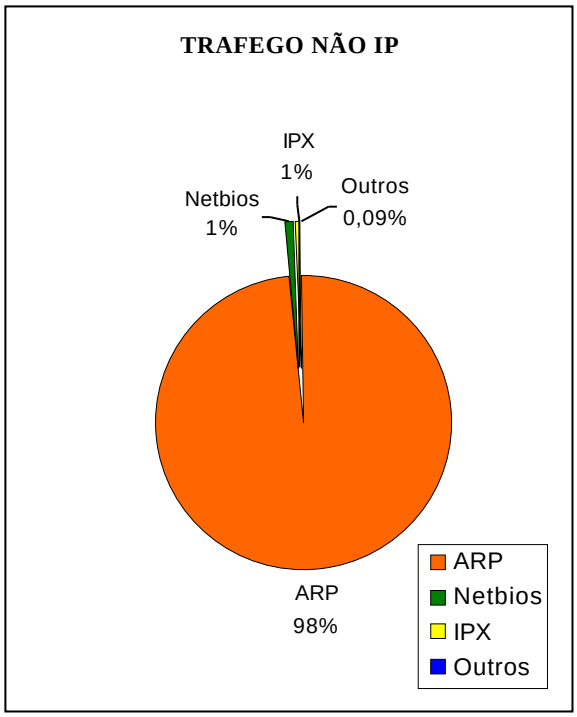


Figura 31. Relação de pacotes que não trafegaram sobre o protocolo IP.

A comprovação dos valores utilizados para a criação do gráfico da Figura 31 pode ser visualizada pela Tabela 7, onde demonstra-se claramente o número de pacotes que trafegaram com estes protocolos que não utilizam o IP como protocolo de rede.

Tabela 7. Relação do número de pacotes trafegados sobre o protocolo Não IP

COLETA	PROTOCOLO			
	ARP	***Netbios***	***IPX***	***Outros***
1	293	1	4	0
2	224	8	4	0
3	223	8	3	0
4	116	0	1	0
5	236	1	0	0
6	347	7	0	1
7	498	0	0	0
8	797	10	7	2
9	272	1	0	1
10	107	1	0	0
11	202	0	5	1
12	1.322	15	0	1
13	1.024	7	7	0
14	837	2	2	0
Total	***6.498***	***61***	***33***	***6***

Pela realização das coletas foram identificadas as 10 portas *TCP* e *UDP* mais utilizadas no tráfego de cada um dos horários analisados. Para esta amostragem foi selecionada aleatoriamente uma coleta de cada dia da semana. Esta relação de tráfego pode ser vista nas Tabelas 8, 9, 10 e 11. Muitas das portas utilizadas estão identificadas com suas aplicações correspondentes, como, por exemplo, pela porta 80 tem-se a identificação da utilização da aplicação *HTTP*.

Tabela 8. Volume de dados pelas principais portas TCP e UDP encontradas. Quarta-feira, 17 de maio de 2006 – Período: Das 8 às 9 horas

PORTA	APLICAÇÃO/ SERVIÇO	Nº PACOTES
53	*DNS*	95
80	*HTTP*	16.530
137	*Netbios Name Service*	263
139	*NetBios Session Service*	516
443	*HTTPS*	777
1068		13.569
1143		67
1245		23
1246		154
5000		1.150

Tabela 9. Volume de dados pelas principais portas TCP e UDP encontradas. Terça-feira, 16 de maio de 2006 – Período: Das 11 às 12 horas

PORTA	APLICAÇÃO/ SERVIÇO	Nº PACOTES
53	*DNS*	53
80	*HTTP*	3.431
137	*Netbios Name Service*	181
139	*NetBios Session Service*	37
443	*HTTPS*	285
1050		257
1504		604
2020		98
2854		50
3963		5

Tabela 10. Volume de dados pelas principais portas TCP e UDP encontradas. Quinta-feira, 18 de maio de 2006 – Período: Das 13 às 14 horas.

PORTA	APLICAÇÃO/ SERVIÇO	Nº PACOTES
53	*DNS*	411
80	*HTTP*	10.264
137	*Netbios Name Service*	797
139	*NetBios Session Service*	578
443	*HTTPS*	213
1031		34
1089		60
2532		1398
2993		2.552
5000		1.111

Tabela 11. Volume de dados pelas principais portas TCP e UDP encontradas. Sexta-feira, 19 de maio de 2006 – Período: Das 19 às 20 horas.

PORTA	APLICAÇÃO/ SERVIÇO	Nº PACOTES
53	*DNS*	1.112
80	*HTTP*	83.537
137	*Netbios Name Service*	760
139	*NetBios Session Service*	1934
443	*HTTPS*	1.827
1063		176
1104		284
1227		647
1426		45
1516		35

Em síntese aos resultados obtidos, pode-se afirmar que na rede analisada, grande parte do tráfego diário é constituída nos horários noturnos, devido ao fato de neste período todos ou grande parte dos laboratórios estarem em atividades, onde o acesso à rede é evidente.

Dos protocolos, aplicações e serviços identificados na rede, o *Internet Protocol* (nível de rede) e o *Transmission Control Protocol* (*TCP)* (nível de transporte) foram os que prevaleceram fortemente sobre o tráfego dos pacotes sobre a rede. Fica comprovada e evidente a utilização destes protocolos por ser uma rede estruturada sobre a arquitetura *TCP/IP*.

CONCLUSÃO

Em todas tarefas realizadas por seres humanos é comum e de extremo interesse íntimo que muitas de suas atividades sejam monitoradas e possivelmente aprimoradas, visando um melhor desempenho no que diz respeito a forma como estas atividades são executadas, proporcionando o bem-estar social e individual.

Incorporado a este contexto este trabalho mostrou a forma como a rede interna dos laboratórios da Universidade do Extremo Sul Catarinense comportou-se e constitui-se diante perspectivas de funções a que está exposta.

Este trabalho explorou a utilização de ferramentas de monitoramento de tráfego de redes, capaz de identificar e expôr informações úteis para que estatísticas e levantamentos de informações de tráfego de rede pudessem ser mostradas. Aprimorou-se uma técnica de amostragem estatística que pudesse garantir a integridade das informações, onde pequenas amostras de dados comportaram informações necessárias para uma análise e afirmação de situações referente ao tráfego total. Os dados coletados conforme a aplicação das técnicas de amostragem estatística, foram estudados e analisados de forma que a apresentação dos resultados obtidos pudesse ser objetiva.

Chegou-se à conclusão também que pela realização da *coleta base*, o tamanho das amostras de cada horário foi maior que o volume real coletado conforme os tempos definidos. A explicação para esta situação está voltada ao fato de que o cálculo do tamanho do volume de tráfego de cada hora foi efetuado sobre o mapeamento de um gráfico gerado pelo programa *Multi Router Traffic Grapher (MRTG),* onde os valores em megabytes foram representados fixamente pelo pico identificado a cada 12 minutos, ou seja, foi

considerado como valor constante a cada 12 minutos do horário coletado, onde obviamente estes valores tiveram variação entre estes intervalos.

Os objetivos propostos à realização deste trabalho foram alcançados, pois conhecimentos foram adquiridos conforme pesquisas realizadas sobre fundamentos teóricos, comportando aprimoramento do aprendizado sobre protocolos de comunicação em rede, ferramentas para monitoramento de tráfego, técnicas estatísticas para realização das coletas e meios de análise que possibilitaram a demonstração dos dados coletados.

Pela realização das coletas constatou-se que 99% do tráfego de pacotes na rede ocorre sobre o protocolo de rede *Internet Protocol*. De todo este tráfego sobre o protocolo *IP*, cerca de 98% dos pacotes contiveram o TCP como protocolo do nível de rede. Apenas pouco mais de 2% do tráfego sobre *IP* foram direcionados a funções realizadas pelos protocolos *ICMP*, *IGMP* e *UDP*. O restante do 1% do tráfego, que não utilizou o *IP* como protocolo de rede, foi constituído pelos protocolos *ARP*, *IPX*, *Netbios* e outros.

Constata-se que pelo surgimento do protocolo IPX, pelo fato de que este protocolo é proveniente da rede *Novell*, pode ser feita uma verificação das configurações da rede dos laboratórios, visto que este protocolo não é utilizado na arquitetura da rede atual.

Diante deste cenário, é justo argumentar que a realização deste trabalho visou mostrar informações referenciadas a uma parte da rede da universidade. Como sugestão poderiam ser realizados outros trabalhos incorporando análises para exposição de informações de outras áreas da rede da universidade, criando uma visão sobre o todo, ou ainda a realização de análises sobre outras redes corporativas. Poderiam ser estudadas outras ferramentas de monitoramento, gratuitas ou não. Enfim, sugere-se a realização de

outras análises de rede com a utilização de técnicas de amostragem diferentes da utilizada neste trabalho, envolvendo outros meios de expôr informações seguras e resumidas.

REFERÊNCIAS

ALBUQUERQUE, Marcio Portes de; RONCERO, Valeriana Gomes; ALBUQUERQUE, Marcelo Portes de. **Monitoramento do Protocolo RTSP (Real Time Streaming Protocol) utilizando NTop (Network Top)**. Rio de Janeiro: Editora do CBPF - NT004/02, 2002.

ALMEIDA, João Paulo; RAMLIE, Yohannes Albertino**. NTop – Network Top**. Disponivel em:. <http://www.ntop.org/ntop.html>. Acesso em: 04 mai. 2006

BARBETTA, Pedro Alberto. **Estatística aplicada às ciências sociais**. 5. ed. rev Florianópolis: UFSC - Fapeu Editora da UFSC, 2005. 340 p.

CAMY, Alexandre R.; SILVA, Evandro R. N.; RIGHI, Rafael. **Relatório da Análise do Protocolo HTTP**. Santa Catarina – Florianópolis, 2003.

CARVALHO, Tereza Cristina Melo De Brito, **Arquiteturas de redes de computadores OSI e TCP/IP**. 2 ed. rev. e ampl. São Paulo: Makron Books, 1997. 695 p.

CASAD, Joe; WILLSEY, Bob. **Aprenda em 24 horas TCP/IP**. Rio de Janeiro: Campus, 1999. 347 p.

CASAGRANDE, Rogério A. **Técnicas de Detecção de Sniffers.** Dissertação (Mestrado em Ciência da Computação). Programa de Pós-Graduação em Computação, Instituto de Informática, Universidade Federal do Rio Grande do Sul. Porto Alegre, 2003.

CASE, J.; Fedor, M.; Schoffstall, M.; Davin, J. **A simple network management protocol SNMP)**. Request for Comments RFC 1157.

CHAVES, Marcelo H. P. C. **Análise de Estado de Tráfego de Redes TCP/IP Para Aplicação em Detecção de Intrusão.** Ministério da Ciência e Tecnologia: Instituto Nacional de Pesquisas Espaciais. Mestrado em Computação Aplicada. São Paulo. 2003.

COCHARAN, William G., **Sampling Techniques**, 3ª ed. New York: John Willey, 1977.

COMER, Douglas; STEVENS, David L. **Interligação em rede com TCP/IP**. Rio de janeiro: Ed. Campus, 1999. 2.v

_____, Douglas. E. **Internetworking with TCP/IP.** 4. ed. New Jersey: Prentice Hall, 2000. v.1: principles, protocols, and architectures. 750 p.

_____, Douglas E. **Redes de Computadores e Internet**. Porto Alegre: Ed. Bookman, 2001.

DE SOUSA, Aleck Zander Tomé; FILHO, Sérgio Antônio Leugi . **Um Sistema de Captura de Pacotes para Uso em Segurança de Redes.** São Paulo: 2004. Unesp - Universidade Estadual Paulista - Instituto de Biociências, Letras e Ciências Exatas, São Paulo, 2004.

DERI, L., Suin, S. and Carbone, R. **Ntop - Network Top**.
Disponivel em:. < http://www.ntop.org/>. Acesso em: 05 mai. 2006.

DIMARZIO, J. F. **Projeto e arquitetura de redes**. Rio de Janeiro: Campus, 2001. 370 p.

ETHEREAL: A Network Protocol Analyzer. Disponível em: <www.ethereal.com>. Acesso em: 25 mai. 2006.

FRANCESCHI, André de A.**Um modelo de tráfego de rede para aplicação de técnicas de Controle Estatístico de Processos.** Tese (Doutorado em Física). Instituto de Física de São Carlos, Universidade de São Paulo. São Paulo, 2003.

FURMANKIEWICZ, Edson. **Segurança máxima: o guia de um hacker para proteger seu site na Internet e sua rede**. Rio de Janeiro: Ed. Campus, 2000. 826 p.

HAYDEN, Matt. **Aprenda em 24 Horas Redes**. 2.ed. Rio de Janeiro: Campus, 1999.

IANA. **Protocol numbers and assignment services**.
Disponível em <http://www.iana.org/numbers.htm>. Acesso em 29 de Abril de 2006.

JUNIOR, Ademar de Souza Reis; FILHO, Milton Soares. **Um sistema de testes para a detecção remota de Sniffers em redes tcp/ip.** 2002. 68f. Monografia (Graduação em Ciência da Computação) – Curso de Ciência da Computação, Universidade Federal do Paraná, Paraná, 2002.

KAMIENSKI, C., (...[et al.])., **Caracterizando Propriedades Essenciais do Tráfego deRedes através de Técnicas de Amostragem Estratificada**. SBRC 2005, Recife – PE, 2005, Maio 2005.

LEAL, Marco A. de Araújo. **Qos – Qualidade de Serviço em TCP/IP**. Universidade Federal de Lavras. Minas Gerais, 2004. Disponível em: <http://www.ginux.ufla.br/documentacao/ monografias/mono-marco-aurelio.pdf>. Acesso em: 15 mai. 2006.

MOURA, José Antão Beltrão. **Redes locais de computadores: protocolos de alto nível e avaliação de desempenho**. Rio de Janeiro: Makron Books, 1986. 454 p.

NORTHCUTT, Stephen (...[et al.]). **Desvendando** : **segurança em redes**. Rio de Janeiro: Campus, 2002. 650 p.

POMPERMAYER JR, Jorge Luiz. **Protótipo de Software Para a Monitoração de Pacotes em uma Rede TCP/IP em Ambientes Linux**. Blumenau: Universidade Regional de Blumenau - Centro de Ciências Exatas e Naturais - Curso de Ciências da Computação, 2002.

SANAI, D. **Detection of Promiscuous Nodes Using ARP Packets.** Securityfriday, 2001. Disponível em <http://www.unesc.net/~rac/mestrado/>. Acesso em: 09 nov. 2005.

STANG, David J; MONN, Sylvia. **Segredos de segurança em rede.** Rio de Janeiro:Berkeley, 1994.

STEVENS, W. R. **UNIX network programming**. 2. ed. Upper Saddle River: Prentice Hall, 1998. v. 1.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Campus, 1997.

TORRES, Gabriel. **Redes** de computadores: **curso** completo. Rio de Janeiro: Axcel Books do Brasil, 2001. 664 p

BIBLIOGRAFIA RECOMENDADA

BARBETTA, Pedro Alberto. **Estatística aplicada às ciências sociais**. 5. ed. rev Florianópolis: UFSC - Fapeu Editora da UFSC, 2004. 340 p.

CASAD, Joe; WILLSEY, Bob. **Aprenda em 24 horas TCP/IP**. Rio de Janeiro: Campus, 1999. 347 p.

CASAGRANDE, Rogério A. **Técnicas de Detecção de Sniffers.** Dissertação (Mestrado em Ciência da Computação). Programa de Pós-Graduação em Computação, Instituto de Informática, Universidade Federal do Rio Grande do Sul. Porto Alegre, 2003.

COMER, Douglas; STEVENS, David L. **Interligação em rede com TCP/IP**. Rio de janeiro: Ed. Campus, 1999. 2.v

DIMARZIO, J. F. **Projeto e arquitetura de redes**. Rio de Janeiro: Campus, 2001. 370 p.

MOURA, José Antão Beltrão. **Redes locais de computadores: protocolos de alto nível e avaliação de desempenho**. Rio de Janeiro: Makron Books, 1986. 454 p.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Campus, 1997.

APÊNDICE A – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 8 ÀS 9 HORAS DO DIA 17 DE MAIO DE 2006

Tabela 12. Volume dos dados coletados em pacotes e bytes. Dia 17, das 8 às 9h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	45.400	34.582.301
Hipertext Transfer Protocol (http)	7.316	7.028.822
NetBIOS Session Service (NBSS)	516	73.518
Outras aplicações que utilizam TCP	1.901	339.740
User Datagram Protocol (UDP)	583	79.646
Domain Name Service (DNS)	190	29.639
NetBIOS Name Service (NBNS)	263	24.700
Hipertext Transfer Protocol (http)	9	1.467
Outras aplicações que utilizam UDP	121	23.740
Internet Control Message Protocol (ICMP)	32	4.906
Internet Group Management Protocol (IGMP)	4	240
Subtotal (IP)	**46019**	**34.667.093**
Trafego não IP		
Address Resolution Protocol (ARP)	293	15.348
NetBios	1	180
Internetwork Packet eXclange (IPX)	4	536
Subtotal	***298***	***16064***
Total geral	**46317**	**34.683.157**

APÊNDICE B – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 9 ÀS 10 HORAS DO DIA 16 DE MAIO DE 2006

Tabela 13. Volume dos dados coletados em pacotes e bytes. Dia 16, das 9 às 10h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	73.999	50.011.623
Hipertext Transfer Protocol (HTTP)	19.996	19.319.376
NetBIOS Session Service (NBSS)	350	48.658
Outras aplicações que utilizam TCP	1.881	322.824
User Datagram Protocol (UDP)	1.084	152.249
Domain Name Service (DNS)	619	96.092
NetBIOS Name Service (NBNS)	341	32.308
Outras aplicações que utilizam UDP	124	23.849
Internet Control Message Protocol (ICMP)	55	5795
Subtotal (IP)	***75.138***	***50.169.667***
Trafego não IP		
Address Resolution Protocol (ARP)	224	11.622
NetBios	8	1.713
Internetwork Packet eXclange (IPX)	4	240
Subtotal	***236***	***13.575***
Total geral	**75.374**	**50.183.242**

APÊNDICE C – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 10 ÀS 11 HORAS DO DIA 16 DE MAIO DE 2006

Tabela 14. Volume dos dados coletados em pacotes e bytes. Dia 16, das 10 às 11h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	62.422	43.421.124
Hipertext Transfer Protocol (http)	12.554	10.863.889
Real Time Streaming Protocol (RTSP)	214	288.810
NetBIOS Session Service (NBSS)	66	9948
Outras aplicações que utilizam TCP	1.554	280.975
User Datagram Protocol (UDP)	1.013	155.272
Domain Name Service (DNS)	666	110.042
NetBIOS Name Service (NBNS)	229	22.820
Outras aplicações que utilizam UDP	118	22.410
Internet Control Message Protocol (ICMP)	42	4.492
Internet Group Management Protocol (IGMP)	6	360
Subtotal (IP)	***63.483***	***43.581.248***
Trafego não IP		
Address Resolution Protocol (ARP)	223	11.760
NetBios	8	1.713
Internetwork Packet eXclange (IPX)	3	180
Subtotal	***234***	***13.653***
Total geral	**63.717**	**43.594.901**

APÊNDICE D – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 11 ÀS 12 HORAS DO DIA 16 DE MAIO DE 2006

Tabela 15. Volume dos dados coletados em pacotes e bytes. Dia 16, das 11 às 12h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	9.516	6.347.392
Hipertext Transfer Protocol (HTTP)	3.257	3.621.233
NetBIOS Session Service (NBSS)	20	2.998
Outras aplicações que utilizam TCP	588	98.904
User Datagram Protocol (UDP)	299	35.304
Domain Name Service (DNS)	106	16.438
NetBIOS Name Service (NBNS)	5	1.246
Outras aplicações que utilizam UDP	13	1.838
Internet Control Message Protocol (ICMP)	22	1.563
Subtotal (IP)	***9.837***	***6.384.259***
Trafego não IP		
Address Resolution Protocol (ARP)	116	5.934
Internetwork Packet eXclange (IPX)	1	60
Subtotal	***117***	***5.994***
Total geral	**9.954**	**6.390.253**

APÊNDICE E – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 12 ÀS 13 HORAS DO DIA 18 DE MAIO DE 2006

Tabela 16. Volume dos dados coletados em pacotes e bytes. Dia 18, das 12 às 13h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	23.965	15.900.377
Hipertext Transfer Protocol (HTTP)	5.755	4.736.997
NetBios Session Service (NBSS)	10	1.070
Outras aplicações que utilizam TCP	1.298	234.607
User Datagram Protocol (UDP)	950	259.637
Domain Name Service (DNS)	157	20.744
NetBIOS Name Service (NBNS)	113	10.396
Outras aplicações que utilizam UDP	680	228.497
Internet Control Message Protocol (ICMP)	10	1.085
Subtotal (IP)	***24.925***	***16.161.099***
Trafego Não IP		
Address Resolution Protocol (ARP)	236	12.216
NetBios	1	180
Subtotal	***237***	***12.396***
Total geral	**25.162**	**16.173.495**

APÊNDICE F – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 13 ÀS 14 HORAS DO DIA 18 DE MAIO DE 2006

Tabela 17. Volume dos dados coletados em pacotes e bytes. Dia 18, das 13 às 14h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	28.640	18.751.971
Hipertext Transfer Protocol (HTTP)	10.942	12.256.283
NetBIOS Session Service (NBSS)	424	56.936
File Transfer Protocol (FTP)	42	3.719
Outras aplicações que utilizam TCP	1.819	318.510
User Datagram Protocol (UDP)	3.483	882.697
Domain Name Service (DNS)	823	112.840
NetBIOS Name Service (NBNS)	540	49.824
Outras aplicações que utilizam UDP	2.120	720.033
Internet Control Message Protocol (ICMP)	32	4.220
Subtotal (IP)	***32.155***	***19.638.868***
Trafego Não IP		
Address Resolution Protocol (ARP)	347	17.760
NetBios	7	1.533
Outros Protocolos Não IP	1	78
Subtotal	***355***	***19.371***
Total geral	**32.510**	**19.658.239**

APÊNDICE G – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 14 ÀS 15 HORAS DO DIA 18 DE MAIO DE 2006

Tabela 18. Volume dos dados coletados em pacotes e bytes. Dia 18, das 14 às 15h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	24.067	13.386.746
Hipertext Transfer Protocol (http)	8.143	6.847.186
NetBIOS Session Service (NBSS)	10	1.070
Outras aplicações que utilizam TCP	2.226	342.441
User Datagram Protocol (UDP)	5.464	1.799.287
Domain Name Service (DNS)	172	28.263
NetBIOS Name Service (NBNS)	163	15.284
Bootstrap Protocol	5038	1.736.112
Outras aplicações que utilizam UDP	91	19.628
Internet Control Message Protocol (ICMP)	11	1.151
Internet Group Management Protocol (IGMP)	2	120
Subtotal (IP)	***29.544***	***15.187.304***
Trafego Não IP		
Address Resolution Protocol (ARP)	498	25.614
Subtotal	***498***	***25.614***
Total geral	**30.042**	**15.212.918**

APÊNDICE H – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 15 ÀS 16 HORAS DO DIA 17 DE MAIO DE 2006

Tabela 19. Volume dos dados coletados em pacotes e bytes. Dia 17, das 15 às 16h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	34.813	18.095.978
Hipertext Transfer Protocol (HTTP)	9.054	6.761.718
NetBIOS Session Service (NBSS)	180	26.184
Outras aplicações que utilizam TCP	2.761	422.977
User Datagram Protocol (UDP)	1.225	147.961
Domain Name Service (DNS)	441	65.480
NetBIOS Name Service (NBNS)	687	63.312
Outras aplicações que utilizam UDP	97	19.169
Internet Control Message Protocol (ICMP)	38	4.164
Subtotal (IP)	***36.076***	***18.248.103***
Trafego não IP		
Address Resolution Protocol (ARP)	797	43.302
Internetwork Packet eXclange (IPX)	10	1.378
NetBios	7	1.533
Outros Protocolos Não IP	2	120
Subtotal (Não IP)	***816***	***46.333***
Total geral	**36.892**	**18.294.436**

APÊNDICE I – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 16 ÀS 17 HORAS DO DIA 17 DE MAIO DE 2006

Tabela 20. Volume dos dados coletados em pacotes e bytes. Dia 17, das 16 às 17h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	64.389	37.040.495
Hipertext Transfer Protocol (http)	18.605	18.400.488
NetBIOS Session Service (NBSS)	318	47.558
Simple Mail Transfer Protocol (SMTP)	3.891	596.114
Real Time Streaming Protocol (RTSP)	83	111.414
Telnet	1	90
Outras aplicações que utilizam TCP	2.462	403.692
User Datagram Protocol (UDP)	644	94.062
Domain Name Service (DNS)	398	66.964
NetBIOS Name Service (NBNS)	191	17.572
Outras aplicações que utilizam UDP	55	9.526
Internet Control Message Protocol (ICMP)	30	3.839
Subtotal (IP)	***65.063***	***37.138.396***
Trafego não IP		
Address Resolution Protocol (ARP)	272	14.088
NetBios	1	180
Outros Protocolos Não IP	1	60
Subtotal (Não IP)	***274***	***14.328***
Total geral	**65.337**	**37.152.724**

APÊNDICE J – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 17 ÀS 18 HORAS DO DIA 17 DE MAIO DE 2006

Tabela 21. Volume dos dados coletados em pacotes e bytes. Dia 17, das 17 às 18h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	20.550	11.405.282
Hipertext Transfer Protocol (http)	5.882	5.667.931
NetBIOS Session Service (NBSS)	1.242	165.592
Outras aplicações que utilizam TCP	2.012	285.812
User Datagram Protocol (UDP)	376	62.265
Domain Name Service (DNS)	333	56.490
NetBIOS Name Service (NBNS)	20	1.840
Outras aplicações que utilizam UDP	23	3.935
Internet Control Message Protocol (ICMP)	18	2.825
Internet Group Management Protocol (IGMP)	2	120
Subtotal (IP)	***20.946***	***11.470.492***
Trafego não IP		
Address Resolution Protocol (ARP)	107	5.538
NetBios	1	180
Subtotal (Não IP)	***108***	***5.718***
Total geral	**21.054**	**11.476.210**

APÊNDICE K – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 18 ÀS 19 HORAS DO DIA 19 DE MAIO DE 2006

Tabela 22. Volume dos dados coletados em pacotes e bytes. Dia 19, das 18 às 19h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	34.177	26.036.853
Hipertext Transfer Protocol (http)	10.857	13.272.878
NetBIOS Session Service (NBSS)	406	58.086
Outras aplicações que utilizam TCP	1.838	351.535
User Datagram Protocol (UDP)	584	71.857
Domain Name Service (DNS)	209	29.118
NetBIOS Name Service (NBNS)	300	27.924
Hipertext Transfer Protocol (http)	3	525
Network Time Protocol (NTP)	4	360
Outras aplicações que utilizam UDP	68	13.930
Internet Control Message Protocol (ICMP)	44	5.338
Internet Group Management Protocol (IGMP)	2	120
Subtotal (IP)	***34.807***	***26.114.168***
Trafego não IP		
Address Resolution Protocol (ARP)	202	10.392
Internetwork Packet eXchange (IPX)	5	744
Outros Protocolos Não IP	1	60
Subtotal (Não IP)	***208***	***11.196***
Total geral	**35.015**	**26.125.364**

APÊNDICE L – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 19 ÀS 20 HORAS DO DIA 19 DE MAIO DE 2006

Tabela 23. Volume dos dados coletados em pacotes e bytes. Dia 18, das 19 às 20h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	217.637	150.834.724
Hipertext Transfer Protocol (http)	65.475	67.491.620
NetBIOS Session Service (NBSS)	1.248	177.992
Tabular Data Stream (TDS)	5.187	605.576
Post Office Protocol (POP)	39	4.452
Telnet	492	335.491
Secure Socket Layer (SSL)	1.090	585.701
Outras aplicações que utilizam TCP	1.412	955.623
User Datagram Protocol (UDP)	3.616	561.840
Domain Name Service (DNS)	2.225	343.677
NetBIOS Name Service (NBNS)	680	68.092
Hipertext Transfer Protocol (http)	35	6.017
Network Time Protocol (NTP)	28	2.520
Outras aplicações que utilizam UDP	648	141.534
Internet Control Message Protocol (ICMP)	237	25.055
Internet Group Management Protocol (IGMP)	43	2.580
Subtotal (IP)	***221.533***	***151.424.199***
Trafego não IP		
Address Resolution Protocol (ARP)	1.322	68.880
NetBios	15	3.256
Outros Protocolos Não IP	1	60
Subtotal (Não IP)	***1.338***	***72.196***
Total geral	**222.871**	**151.496.395**

APÊNDICE M – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 20 ÀS 21 HORAS DO DIA 19 DE MAIO DE 2006

Tabela 24. Volume dos dados coletados em pacotes e bytes. Dia 19, das 20 às 21h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	210.989	150.091.858
Hipertext Transfer Protocol (http)	37.668	30.149.063
NetBIOS Session Service (NBSS)	88	12.240
Tabular Data Stream (TDS)	5.570	706.204
Post Office Protocol (POP)	14	3.051
File Transfer Protocol (FTP)	13	1.255
Secure Socket Layer (SSL)	1.638	1.097.874
Outras aplicações que utilizam TCP	5.146	4.577.412
User Datagram Protocol (UDP)	2.592	387.884
Domain Name Service (DNS)	1.512	239.006
NetBIOS Name Service (NBNS)	589	55.052
Outras aplicações que utilizam UDP	491	93.826
Internet Control Message Protocol (ICMP)	80	8.291
Internet Group Management Protocol (IGMP)	4	240
Subtotal (IP)	***213.665***	***150.488.273***
Trafego não IP		
Address Resolution Protocol (ARP)	1.024	53.088
NetBios	7	1.533
Internetwork Packet eXchange (IPX)	7	830
Subtotal (Não IP)	***1.038***	***55.451***
Total geral	**214.703**	**150.543.724**

APÊNDICE N – DETALHAMENTO DO TRÁFEGO DO PERÍODO DAS 21 ÀS 22 HORAS DO DIA 19 DE MAIO DE 2006

Tabela 25. Volume dos dados coletados em pacotes e bytes. Dia 19, das 21 às 22h.

Protocolo	Número de Pacotes	Bytes
Trafego IP		
Transmission Control Protocol (TCP)	129.076	82.545.190
Hipertext Transfer Protocol (http)	40.523	42.596.414
NetBIOS Session Service (NBSS)	370	49.476
Domain Name Service (DNS)	2	674
Real Time Streaming Protocol (RTSP)	67	75.918
Post Office Protocol (POP)	48	5.830
Tabular Data Stream (TDS)	3.708	419.237
Outras aplicações que utilizam TCP	1.842	1.812.795
User Datagram Protocol (UDP)	2.278	370.899
Domain Name Service (DNS)	1.817	296.819
NetBIOS Name Service (NBNS)	170	16.288
Hipertext Transfer Protocol (http)	21	8.286
Network Time Protocol (NTP)	8	720
Outras aplicações que utilizam UDP	262	48.786
Internet Control Message Protocol (ICMP)	86	7.684
Internet Group Management Protocol (IGMP)	20	1.200
Subtotal (IP)	***131.460***	***82.924.973***
Trafego não IP		
Address Resolution Protocol (ARP)	837	42.750
NetBios	2	370
Outros Protocolos Não IP	2	120
Subtotal (Não IP)	***841***	***43.240***
Total geral	**132.301**	**82.968.213**