UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

FABRICIO CARDOSO DE JESUS

ANÁLISE DA REDE SOB O PONTO DE VISTA DO CONTROLE DE INFORMAÇÕES E TRÁFEGO

ESTUDO DE CASO: TSA QUÍMICA DO BRASIL

CRICIÚMA, NOVEMBRO DE 2008

FABRICIO CARDOSO DE JESUS

ANÁLISE DA REDE SOB O PONTO DE VISTA DO CONTROLE DE INFORMAÇÕES E TRÁFEGO

ESTUDO DE CASO: TSA QUÍMICA DO BRASIL

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. MSc. Rogério Antônio Casagrande

CRICIÚMA, NOVEMBRO DE 2008

FABRICIO CARDODO DE JESUS

ANÁLISE DA REDE SOB O PONTO DE VISTA DO CONTROLE DE INFORMAÇÕES E TRÁFEGO
ESTUDO DE CASO: TSA QUÍMICA DO BRASIL

Submetido ao corpo docente do Curso 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. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Rogério Antônio Casagrande (UNESC)
Orientador

Prof. Esp. Arildo Sônego (UNESC)

Prof. MSc. Paulo Martins (UNESC)

AGRADECIMENTOS

Agradeço profundamente à Deus, por estar sempre presente, dando força e coragem para enfrentar todas as dificuldades até aqui encontradas e também por toda felicidade e conquistas de minha vida.

À minha família, pela ajuda, amor e compreensão durante este período de faculdade, principalmente nesta etapa de TCC, onde muitas vezes não pude estar tão presente como deveria.

Aos meus pais e irmãos, pelo convívio durante toda minha vida, pela formação do meu caráter, amor e auxílio em todos os momentos difíceis.

Ao meu orientador Rogério Antônio Casagrande, por aceitar este desafio comigo, mesmo sabendo das muitas dificuldades, principalmente devido ao curto espaço de tempo disponível para a conclusão do trabalho.

À empresa TSA Química do Brasil LTDA, que disponibilizou seus recursos e o ambiente para podermos efetuar as pesquisas e estudos, e de uma forma geral a todos os amigos e colegas, que de uma forma ou de outra me ajudaram na conclusão deste trabalho.

O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis.

José de Alencar

RESUMO

A importância das redes de computadores e os benefícios que a mesma proporciona às organizações é muito grande. Contudo, se trata de um recurso finito e sendo assim possui suas limitações. As redes de computadores possibilitam a troca de informações de dados diversos, o fluxo destas informações muitas vezes fica imperceptível. A falta de um controle adequado sobre o mesmo pode gerar condições adversas, como utilização imprópria dos recursos da rede, seja esta de forma ingênua, principalmente por meio das mais variadas ferramentas disponíveis atualmente, ou mesmo com más intenções. Este tráfego indevido além de aumentar o tempo de resposta de outras aplicações dependentes da rede, coloca em risco a segurança das informações da organização. Este trabalho, vem por meio de análises do tráfego da rede, diagnosticar a mesma com intuito de poder informar à organização que tipo de informação está trafegando na rede, se possui informações desnecessárias e o que poderia estar sendo feito para otimizar o tráfego. Para a coleta dos dados foi aplicada a técnica de amostragem estratificada proporcional e para à análise foi utilizada a ferramenta Wireshark, que possibilitou o estudo do tráfego, separando os protocolos utilizados pela rede e gerando estatísticas sobre os mesmos e possibilitando a elaboração de um parecer a respeito do tráfego de rede da organização.

Palavras-Chave: Sniffer; Redes; Tráfego; Análise do Tráfego; Wireshark.

ABSTRACT

The importance and benefits that computers networks brings to the organizations is so huge. However, it is a finite resource, so it has its limitation. Computer networks makes possible the change of a variety of data information, the flowing of such information is, many times, unperceivable. The lack of a suitable control over it can cause inappropriate situations, such as inopportune utilization of the networks resource in an innocent (ingenuous) way, mainly through the many available tools that are found nowadays or even with evil intentions. This inconvenient traffic makes slower the time of answers from other dependent uses of networks and besides endangers the organization information safety. This work, through the analysis of the networks traffic, has the objective to diagnose it, in order to notice the organization what king of information has been transiting at networks, if there is useless information and what could be done to optimize its traffic. For data collection has used the technique of sampling and stratified proportional to the analysis tool was used to Wireshark, and made possible the traffic study, separating the protocols used by networks and developing statistics over them and allowing the elaboration of a report regarding to organizations networks traffic.

Keywords: Sniffer; Networking, Traffic, Traffic Analysis; Wireshark.

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*
ERP	*Enterprise Resource Planning*
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
ICMP	*Internet Control Message Protocol*
ISO	*International Organization for Standardization*
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*
WTS	*Windows Terminal Server*
SGBD	*Sistema de Gerenciamento de Banco de Dados*

SUMÁRIO

1 INTRODUÇÃO

Com o passar do tempo é notória a disseminação da informática em todos os segmentos da sociedade, e juntamente com essa disseminação surge a necessidade da transmissão eficiente da informação gerada (COMER, 2006).

Segundo Kurose e Ross (2006) nos dias atuais, a velocidade na transmissão e a agilidade em adquirir conhecimento tornam-se um diferencial importante, tanto no meio empresarial quanto no pessoal, fazendo com que a grande parte da população mundial esteja diretamente ligada à Internet. Esta por sua vez, permite a ligação de empresas com suas redes locais e pessoas, independente do local onde estejam.

Ainda segundo Kurose e Ross (2006) com toda a infra-estrutura existente, o que acaba acontecendo é a falta de monitoramento e controle dos dados transitados pelas redes, ou seja, em muitos casos as organizações acabam por desconhecer o que trafega pela sua própria rede. Desta forma, o que pode ocorrer é a aplicação equivocada de recursos no momento em que se faz necessário melhorar o desempenho da mesma.

Sendo assim, a idéia principal da pesquisa é analisar e constatar se a rede da empresa TSA Química está ou não sendo prejudicada por fatores que se refiram à transmissão dos dados em rede local.

A análise deverá ser feita com a aplicação de técnicas estatísticas juntamente com ferramentas de monitoramento de tráfego, que permitam a geração de estatísticas da rede da empresa em questão, separando os tipos de dados que estão sendo trafegados, a fim de determinar se a rede está operando de forma otimizada no que se refere à qualidade do tráfego encontrado.

1.1 OBJETIVO GERAL

Analisar a rede da empresa TSA Química do Brasil de modo a poder caracterizar a mesma como uma rede otimizada sob o ponto de vista do tráfego de dados.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos do trabalho consistem em:

a) Compreender a estrutura de uma rede de computadores;

b) Compreender os protocolos utilizados para transmissão dos dados;

c) Pesquisar e utilizar uma ferramenta no processo de monitoria do fluxo de dados da rede;

d) Analisar os dados obtidos a fim de diagnosticar a rede de acordo com seu tráfego;

e) Documentar os procedimentos sugeridos para otimização do tráfego da rede.

1.3 JUSTIFICATIVA

O objetivo de toda e qualquer rede de computador é transmitir e compartilhar informações. Para que esta transmissão seja possível, é necessário que seja feita um encapsulamento nos dados de forma com que tanto o remetente quanto o destinatário

consigam entender a informação depois do envio. Neste processo de encapsulamento os dados são separados em bits e re-agrupados em pacotes desta forma são colocados na rede (KUROSE; ROSS, 2006).

A partir daí não se tem mais um controle efetivo sobre estes dados, como tipo de informação, origem, destino dos pacotes e principalmente o objetivo do mesmo.

A aplicação de ferramentas *sniffers* neste caso ajudam na separação destes pacotes e identificação destas informações.

Este trabalho visa por meio de amostras estatísticas, analisar as informações transmitidas na rede da empresa, estudar e analisar estas informações a ponto de definir se estas possuem um propósito adequado com a política da empresa[1], também se algo poderia ser feito no intuito de ter um melhor controle deste tráfego, garantindo assim uma melhor vazão das informações e uma rede otimizada sobre este ponto de vista.

1.4 ESTRUTURA DO TRABALHO

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

O primeiro capítulo demonstra uma visão geral desta pesquisa, expondo os objetivos a serem alcançados.

[1] De acordo com a política da TSA Química do Brasil LTDA, todos os bens da mesma devem ser utilizados única e exclusivamente para fins e objetivos da empresa.

O segundo capítulo visa demonstrar o funcionamento de uma rede no que diz respeito às regras de comunicação, ou seja, explica o que são e quais os principais protocolos utilizados por uma rede com arquitetura TCP/IP.

No terceiro capítulo é demonstrado o que são *sniffers*, seu funcionamento e as principais características deste tipo de ferramenta.

No quarto capítulo é mostrado alguns trabalhos correlatos a este.

O quinto capítulo mostra todas as etapas da análise do tráfego da rede da empresa TSA Química LTDA, desde o processo de coleta das amostras, os parâmetros que foram utilizados e a forma como foram realizadas as análises das mesmas. Neste capítulo também são citadas as principais dificuldades encontradas durante a realização deste trabalho e abrange também as sugestões para melhoria da rede da empresa sob o ponto de vista do tráfego da mesma.

2 REDES DE COMPUTADORES

O ponto chave da tecnologia dominante neste século tem sido a aquisição, o processamento e a distribuição da informação (KUROSE; ROSS, 2006). A alta necessidade de transmissão da informação tem impulsionado os meios que fazem essa transmissão possível.

Comer (2006) descreve que uma rede é um conjunto de computadores ou dispositivos semelhantes ao computador interligados entre si por algum meio de transmissão de dados.

Segundo ele, o principal objetivo das redes de computadores é realizar a transmissão de informações. Nos últimos anos as redes obtiveram um crescimento explosivo e isso se deve ao fato da comunicação e interligação entre pontos diversos, que se tornou indispensável para muitos ramos de negócios. As redes, que há algum tempo atrás eram utilizadas apenas por empresas, para o compartilhamento de informações relacionadas ao seu segmento, agora também são utilizadas até mesmo por usuários visando principalmente o entretenimento. Para as instituições de ensino, esse compartilhamento de informações também é de grande valia, pois permite que professores e alunos usufruam informações em todo o mundo, como exemplo pode ser citado as bibliotecas on-line.

Ainda de acordo com Comer (2006), o crescimento da Internet é dos fatos mais observados e interessantes na área de redes, sendo esta considerada um sistema de comunicação de alto grau de produtividade que incorpora milhões de pessoas em todo o mundo.

A seguir serão demonstrados alguns aspectos da Internet e as regras que possibilitam a comunicação por meio da mesma.

2.1 INTERNET

Segundo Kurose e Ross (2006) a Internet pública é uma rede mundial de computadores que permite a conexão de milhões de equipamentos de computação em todo o mundo. Com o passar do tempo o termo, rede de computadores, está ficando meio obsoleto, pois são vários os equipamentos, além de computadores, que são criados com os recursos de comunicação por meio da rede.

Para que esta comunicação seja possível, todos os equipamentos devem disponibilizar a funcionalidade dos protocolos, ou ainda em outras palavras, todos os equipamentos devem se comunicar utilizando uma linguagem comum. Estas regras que possibilitam a comunicação entre as máquinas são chamadas de protocolos (Kurose e Ross, 2006). A seguir será visto de forma mais detalhada quais suas principais funcionalidades.

2.2 PROTOCOLOS DE COMUNICAÇÃO

Segundo Comer (2006) durante as últimas duas décadas, houve um grande aumento na quantidade e no tamanho das redes. Várias redes, no entanto, foram criadas por meio de implementações diferentes de hardware e de software. Como resultado, muitas redes eram incompatíveis, e como conseqüência impossibilitava a comunicação entre elas.

Na metade da década de 80, as empresas começaram a ter problemas gerados pelas expansões realizadas. A comunicação entre redes que usavam especificações e implementações diferentes se tornou mais difícil. As empresas perceberam que precisavam abandonar os sistemas de redes proprietários.

De acordo com Carvalho (1997) os sistemas proprietários têm desenvolvimento, posse e controle privados. Proprietário significa que uma empresa ou um pequeno grupo de empresas controla todos os usos da tecnologia. "Aberto" quer dizer que o livre uso da tecnologia está disponível para o público. Para tratar do problema da incompatibilidade entre as redes e da impossibilidade delas se comunicarem entre si, a *International Organization for Standardization* (***ISO***) pesquisou esquemas de redes como, por exemplo, DECNET, SNA e TCP/IP, para descobrir um conjunto de regras. Como resultado dessa pesquisa, a ISO criou um modelo de rede que ajudaria os fabricantes a criar redes que poderiam ser compatíveis e operar junto com outras redes.

Ainda de acordo com Carvalho (1997) o processo de decompor comunicações complexas em discretas tarefas menores pode ser comparado ao processo de montagem de um automóvel. Se tomado como um todo, o processo de projetar, industrializar e montar um automóvel é altamente complexo. É improvável que uma só pessoa saiba como executar todas as tarefas necessárias para construir um carro partindo do zero. Por isso, os engenheiros mecânicos projetam o carro, os engenheiros industriais projetam os moldes para as peças e os técnicos de montagem específicos montam cada parte do carro.

Segundo Comer (2006) o modelo de referência OSI, lançado em 1984, foi o esquema descritivo criado. Ele ofereceu aos fabricantes um conjunto de padrões que

garantiram maior compatibilidade e interoperabilidade entre os vários tipos de tecnologias de rede, criados por várias empresas de todo o mundo.

Ainda segundo Comer (2006) apesar do modelo de referência OSI seja universalmente reconhecido, o padrão aberto técnico e histórico da Internet é o *Transmission Control Protocol/Internet Protocol* (TCP/IP). O modelo de referência TCP/IP e a pilha de protocolos deste modelo tornam possível a comunicação de dados entre dois computadores quaisquer, em qualquer parte do mundo de forma extremamente rápida.

De acordo com Kurose e Ross (2006) para explicar melhor a funcionalidade dos protocolos de comunicação, pode ser feita uma analogia com a comunicação humana. Explicando melhor: Em uma simples conversação são utilizados protocolos de comunicação, pois ao dirigir a palavra a alguém, com um “Oi” por exemplo, espera-se que a pessoa em questão entenda e nos dê um retorno, assim fica subentendido que a pessoa entendeu a mensagem e se pode prosseguir. Protocolos de comunicação nada mais é que padrões de linguagens que permitem que duas ou mais entidades possam compartilhar informações.

Comer (2006) afirma que um protocolo de comunicação nada mais é do que um conjunto de regras que regem o tratamento e, especialmente, a formatação de dados em um sistema de comunicação. Seria a "gramática" de uma "linguagem" de comunicação padronizada.

Protocolos de redes são como protocolos da linguagem humana, a única diferença é que nos protocolos de rede as entidades que trocam mensagens e realizam as ações são componentes de software e hardware. É importante ressaltar que toda e qualquer

atividade, na Internet, que envolva duas ou mais entidades remotas comunicantes, estarão utilizando algum protocolo (KUROSE; ROSS, 2006).

Segundo Comer (2006) no sistema de comunicação de dados são utilizados vários protocolos para que seja possível compartilhar dados de todas as aplicações existentes, ou seja, para determinada aplicação ou tipo de informação, precisará de um determinado protocolo.

Antes de serem demonstradas as características dos principais protocolos utilizados na transmissão de dados, serão demonstradas outras questões referentes à transmissão de informações.

2.3 TRANSMISSÃO DE DADOS E PACOTES

Segundo Kurose e Ross (2006) a comunicação e transmissão de dados entre sistemas finais, ou seja, equipamentos conectados a alguma rede, são realizados por enlaces de comunicação, sendo que estes enlaces se referem aos meios físicos pelos quais as informações serão conduzidas. Entre os principais meios físicos estão cabos coaxiais, fibra óptica, fios de cobre, ondas de rádio, etc, sendo que para cada um deles a velocidade na transmissão irá variar.

Na comunicação de sistemas finais são utilizados equipamentos intermediários de comutação, mais conhecidos como comutadores de pacotes, cuja função é encaminhar a informação que está chegando em um de seus enlaces de comunicação de entrada para um de seus enlaces de comunicação de saída, sendo que atualmente os dois

comutadores mais conhecidos e utilizados são os roteadores e switches (TANENBAUM, 2003).

A seqüência de enlaces de comunicação que o pacote percorre desde sua origem ao seu destino é chamado de caminho ou rota (TANENBAUM, 2003).

2.3.1 Pacotes

De acordo com Comer (2006) no processo de transferência dos dados por meio da rede, estes são divididos em pequenos blocos, chamados pacotes, por isso os termos redes de pacotes ou ainda redes de comutação de pacotes.

A utilização de pacotes em uma rede evita que uma única estação monopolize a rede por muito tempo e torna mais fácil a correção de erros. Se por acaso um pacote chegar corrompido, apenas este terá de ser retransmitido.

Segundo Comer (2006) as principais vantagens da utilização de pacotes na transmissão de dados em redes de computadores são:

a) a necessidade do receptor e o remetente precisarem coordenar a transmissão para assegurar que os dados cheguem 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;

b) O fato de que o 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.

Neste processo de segmentação em pacotes, outra técnica que é aplicada é a filtragem de pacotes. Segundo Northcutt et al (2002) este é um dos métodos mais antigos e acessíveis de se controlar os acessos à rede. É um método bem simples, onde pelo cabeçalho do pacote, é verificado se este pode ou não trafegar pelo dispositivo de rede.

É importante destacar que no cabeçalho do pacote são encontradas informações como endereço de origem e destino do pacote, além da porta do protocolo com qual eles estão se comunicando.

Um exemplo citado por Northcutt et al (2002) sobre a filtragem de pacotes, é que quando uma máquina cliente faz uma requisição a um servidor ela utiliza uma porta (aleatória) superior a 1023 para utilizar na transmissão de dados, o servidor recebe a requisição em uma porta definida (porta 80 para HTTP, por exemplo), e no momento da resposta utiliza esta mesma porta para o envio, e o cliente vai receber novamente uma porta aleatória superior a 1023. Sendo assim conclui-se que cada protocolo utiliza uma porta de comunicação específica e uma alternativa e desta forma permiti-se trabalhar com os filtros de pacotes.

2.3.2 Transmissão de dados

A comunicação entre computadores em uma rede envolve codificar dados em uma forma de energia e enviar esta energia por um meio de transmissão (COMER, 2006). Como exemplo disto, a corrente elétrica pode ser utilizada para transferir dados por meio de um fio, ou ondas de rádio que podem ser utilizadas para carregar dados por meio do ar.

Segundo Kurose e Ross (2006) sistemas finais utilizam a Internet para se comunicarem, sendo que os enlaces, roteadores e outros componentes da Internet fornecem os meios necessários para a transmissão destes dados.

Ainda segundo Kurose e Ross (2006) redes TCP/IP, mais especificamente na Internet, oferecem dois tipos de serviços para comunicação de sistemas finais: serviços orientados para conexão e serviços não orientados para conexão. Será visto de forma mais detalhadamente a seguir.

2.3.2.1 Serviços orientados para conexão

Em uma comunicação orientada a conexão, para realizar uma transfeência entre um programa cliente e um programa servidor, são enviados pacotes de controles de um para o outro antes de serem enviados os dados da aplicação. Segundo Kurose e Ross (2006) este procedimento é conhecido como apresentação, ou ainda conexão de sistemas finais, e faz com que, tanto o cliente quanto o servidor se preparem para a transmissão dos dados que serão feitas posteriormente.

De acordo com Kurose e Ross (2006) serviços orientados para conexão fornecidos pela Internet vêm conjugados com diversos outros serviços, dentre eles transferência de dados confiável, controle de fluxo e controle de congestionamento.

a) **transferência de dados confiável**: significa que a conexão fará a transmissão de todos os dados para a aplicação e na devida ordem, mesmo que para isso precisem ser retransmitidas quantas vezes forem necessárias.

b) **controle de fluxo:** é o serviço que garante que nenhum dos lados de uma conexão sobrecarregue o outro, enviando em uma velocidade que não se consiga processar as informações. Este serviço é implementado pelos sistemas finais por meio de *buffers* de envio e recebimento;

c) **controle de congestionamento**: este serviço ajuda a evitar que a Internet pare. Isso ocorre quando os comutadores de pacotes ficam sobrecarregados e mesmo assim, sistemas finais continuam a enviar pacotes. Nesta situação os buffers começarão a "transbordar" e perder pacotes. Para solucionar este problema os sistemas finais são avisados do tráfego intenso e diminuem a velocidade com que enviam os seus pacotes durante o período de congestionamento.

2.3.2.2 Serviços não orientados para conexão

Neste tipo de serviço, segundo Kurose e Ross (2006) não existe a etapa de apresentação, neste caso o remetente não espera nenhum tipo de retorno de confirmação,

sendo assim os dados são entregues de forma mais rápida. Com estas características, o serviço não orientado para conexões se torna o ideal para aplicações simples orientadas a transação. Este serviço é denominado *Protocolo de Datagrama do Usuário* (UDP). Pelo fato de ser um serviço mais simples, o mesmo não realiza as funções de controle de fluxo e controle de congestionamento. É considerado um serviço de transferência não confiável, pois não se pode ter a certeza se todos os pacotes chegaram corretamente ao seu destino.

Segundo Kurose e Ross (2006) a maioria das aplicações da Internet utiliza o serviço orientado para conexão (TCP). Como exemplos podem ser citados: Telnet, SMTP, FTP, HTTP, mas o UDP tem também grande importância, principalmente em tecnologias novas relacionadas à multimídia, como a comunicação pela Internet e vídeo conferência.

2.4 REDES LOCAIS E REDES DE LONGA DISTÂNCIA

Segundo Comer (2006) as redes de comutação de pacotes são separadas em duas categorias, sendo elas LAN's e WAN's. O principal motivo desta divisão segundo ele, diz respeito as suas características de cada uma delas.

Comer (2006) afirma ainda que as WAN's, também chamadas de *long haul networks* (redes de longa distância), possibilita a comunicação entre longas distâncias, desprezando na maioria das situações a posição geográfica entre as extremidades da comunicação. Em contrapartida, este tipo de tecnologia se prende no quesito velocidade, pois como normalmente opera a longas distâncias, não consegue trabalhar com altas taxas

de conexão. As WAN's trabalham em uma velocidade que pode variar entre 1,5 Mbps (milhões de *bits*/segundo) até 2,4 Gbps (bilhões de *bits*/segundo).

Já nas *Local Area Networks* (LAN's), também conhecidas como redes locais, os computadores ficam localizados geralmente em um único prédio, sacrificando assim a possibilidade de comunicar-se a longas distâncias Com isso a taxa de velocidade é muito maior, operando entre 100 Mbps e 10 Gbps e os atrasos na comunicação da rede são bem menores (COMER, 2006).

A partir do próximo capítulo será abordado de forma mais detalhada os protocolos e suas camadas, sendo estes os grandes responsáveis pela comunicação da rede independente da categoria em que as mesmas se enquadrem.

2.5 ARQUITETURA EM CAMADAS

A principal vantagem de se trabalhar com uma arquitetura de camadas é a possibilidade de dividir o processo complicado de fazer comunicação de dados, em tarefas menores, possibilitando modularizar e tratar de forma separada cada um dos serviços oferecidos pela camada em questão (KUROSE; ROSS, 2006).

O que acaba acontecendo é que para fornecer uma estrutura para o projeto de protocolos de redes, os projetistas de rede, organizam seus trabalhos e pesquisas sempre se baseando em camadas, sendo que neste caso, todos os protocolos estarão sempre associados a uma determinada camada.

Segundo Comer (2006) trabalhar com camadas facilita muito para o projetista, pois pode focar-se em uma camada de cada vez, não se importando como as demais funcionam, em outras palavras, divide-se um grande problema em problemas menores, simplificando assim a busca pela solução do mesmo.

Segundo Kurose e Ross (2006) alguns pesquisadores se opõem ao uso de camadas, pois alegam que na utilização das mesmas, o que acaba ocorrendo é a duplicidade de funções. Um exemplo que pode ser descrito é o serviço de recuperação de erros, que é oferecido pela camada de enlace e também fim-a-fim. Outra desvantagem seria o fato de em certos casos uma camada precisar de uma informação que esteja somente em uma outra camada.

A arquitetura TCP/IP trabalha com um conjunto de protocolos divididos em quatro camadas, que são: Aplicação, transporte, Internet e rede (enlace), sendo estas construídas sobre uma quinta camada, que se refere ao nível físico ou de hardware (COMER, 2006). Na Figura 1 pode-se ver mais claramente como fica esta estrutura.

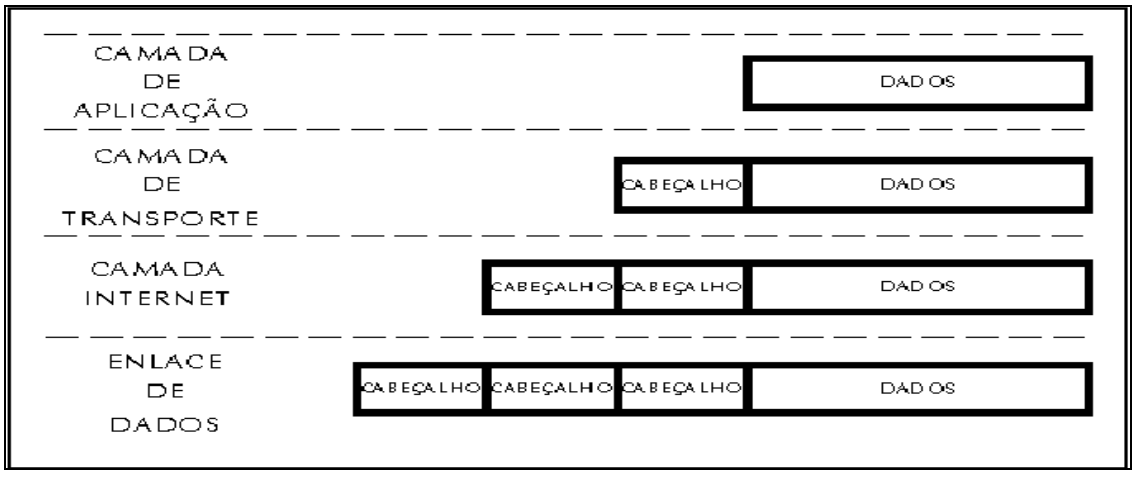

Figura 1. Camadas da arquitetura TCP/IP
Fonte: COMER, D. (2006)

Onde:

a) **camada de aplicação:** de acordo com Kurose e Ross (2006) é na camada de aplicação onde se encontram 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 à 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, é responsável pela qualidade de serviços de confiabilidade, controle de fluxo e correção de erros. O TCP mantém um "diálogo" entre a origem e o destino enquanto empacotam 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 percorram 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 acontece 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:** 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 (SILVA, 2001);

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.

A seguir serão demonstrados os principais protocolos que atuam na camada de aplicação, onde estão os principais aplicativos utilizados por usuários, que consomem a maioria dos recursos de rede.

2.6 PROTOCOLOS E SUAS FUNCIONALIDADES

Segundo Kurose e Ross (2006) novos programas e aplicativos surgem todos os dias, tanto públicos como proprietários. Esta pesquisa procurou focar os principais e mais utilizados na empresa em questão e seus respectivos protocolos de comunicação.

2.6.1 Telnet/SSH

De acordo com Comer (2006) o protocolo Telnet é um aplicativo que permite que se faça um acesso a uma máquina pela rede remotamente. Este aplicativo realiza uma conexão TCP, e por meio dela envia toques do teclado do usuário cliente remotamente para outra máquina, e também mostra o retorno na tela do usuário, dando a impressão de que se esta trabalhando diretamente na máquina remota. Esta característica, segundo ele, faz com que este serviço seja caracterizado como transparente.

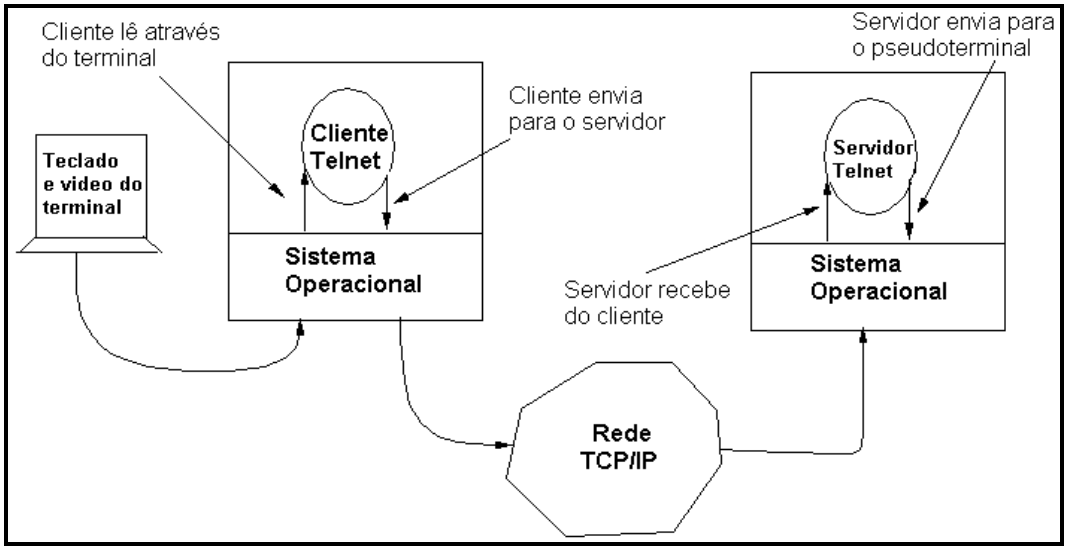

Figura 2. Caminho dos dados em uma sessão de terminal remoto Telnet.
Fonte: Adaptado de Comer, D. (2006)

Ainda segundo Comer (2006) ao utilizar este protocolo no nível de aplicação tem suas vantagens e desvantagens. A vantagem é a facilidade de se operar o servidor remotamente ao invés de se ter o código diretamente embutido no sistema operacional. A desvantagem seria o longo caminho a ser percorrido pelos dados até se concluir determinada operação, pois o mesmo sai do teclado do usuário, passa pelo sistema operacional do mesmo, pelo programa, viaja pela rede ate a máquina servidora, pelo sistema operacional desta, depois precisa viajar até o programa aplicativo do servidor. O aplicativo irá processar a informação e a resposta terá de fazer todo o caminho de volta ate chegar à tela do usuário.

O protocolo *Secure Shell* (SSH), tem a mesma funcionalidade do Telnet, porém com dois recursos diferenciados. Um deles é a conexão segura e o outro e a capacidade de realizar as transferências de dados adicionais e independentes pela mesma conexão usada para o login remoto.

Segundo Comer (2006) a base do SSH possui três principais funções, conforme a seguir:

a) Protocolo de camada de transporte: fornece a confiabilidade e integridade dos dados, com total privacidade;

b) Protocolo de autenticação de usuário: realiza a autenticação do usuário com o servidor;

c) Protocolo de conexão: faz a segmentação de uma única conexão SSH em diversos canais de comunicação.

Além destes aplicativos também foram criados outros com a mesma característica de conexão por TCP/IP para login remoto, tais como VNC, RDP, só que estes interagem diretamente com o desktop e não somente em modo texto dos aplicativos vistos anteriormente.

2.6.2 FTP/TFTP

O *File Transfer Protocol*, mais conhecido como FTP, segundo Comer (2006) é o principal protocolo para transferência de arquivos e grande responsável pelo tráfego de rede/Internet.

De acordo com Kurose e Ross (2006) em uma conexão FTP típica, um usuário precisa disponibilizar ou capturar arquivos de um determinado hospedeiro. Para isso o usuário deve realizar a autenticação no hospedeiro, e uma vez logado, o FTP utilizará duas conexões para a realização da transferência ou cópia do arquivo. Uma delas para

informações de controle e a outra para transferências dos dados que estão sendo transferidos.

Pela conexão de controle trafegam informações como identificação de usuário, senha, comandos de troca de diretório remoto e comandos para inserir e pegar arquivos. Na conexão de dados, os arquivos são efetivamente transferidos.

Ainda segundo Kurose e Ross (2006) estas duas conexões utilizam portas distintas, ou seja, a conexão de controle é realizada pela porta 21(tanto no cliente como no servidor) e a conexão dos dados é feita na porta 20 (também no cliente e no servidor), conforme Figura 3.

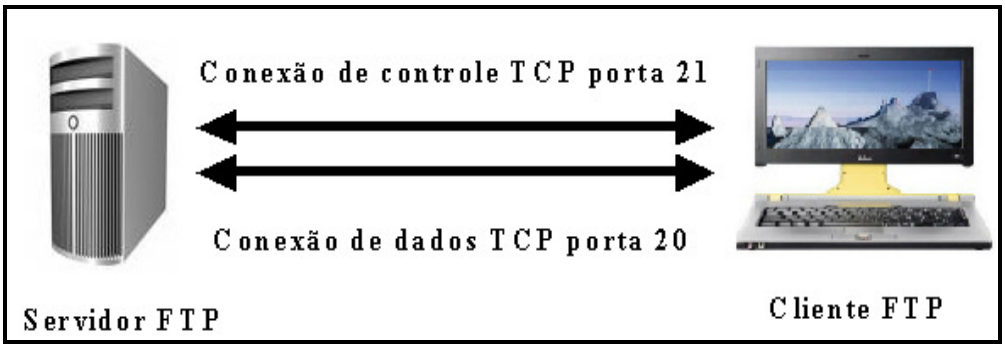

Figura 3. Conexão cliente/servidor via FTP
Fonte: Adaptado de Kurose e Ross (2006)

Segundo Comer (2006) apesar da exigência de autenticação do protocolo FTP, este ainda é muito carente no quesito segurança, pois para a transferência tanto a senha como os dados, não é utilizada criptografia. E devido a essa carência, é que foram criados outros mecanismos, ou extensões do FTP para fornecer segurança adicional para o processo de transferência de arquivos, como:

a) *Secure Sockets Layer* FTP (SSL-FTP): Utiliza a tecnologia Secure Sockets Layer, sendo que nestas transferências, inclusive senhas, são criptografadas;

b) *Secure File Transfer Program* (SFTP): Outro programa criado como alternativa para o FTP. Utiliza transferências multiplexadas de uma única conexão SSH, utilizada para fornecer segurança a outras aplicações;

c) *Secure Copy* (SCP): Utiliza criptografia para fornecer transferência segura. Como o SFTP, também utiliza um canal SSH, porém este pode ser utilizado via linhas de comando.

Segundo Comer (2006) o FTP além de ser o protocolo mais conhecido e utilizado para transferência de arquivos é também o mais complexo e difícil de programar, além de que exige que clientes e servidores gerenciem várias conexões TCP concorrentes. Em razão disto, na família de protocolos TCP/IP, existe um segundo protocolo para transferências de arquivos, que é o TFTP (*Trivial File Transfer Protocol*), destinado a aplicações que dispensam interações complexas entre cliente e servidor, sendo utilizado em transferências simples de arquivos sem autenticação.

O protocolo TFTP, por não necessitar de um serviço de dados confiável, trabalha sobre o UDP. O seu funcionamento é bem simples, ele realiza toda a sua transmissão, com pacotes fixos de 512 bytes, sendo que se for enviado algum pacote de menor tamanho, indica o fim do arquivo. Este protocolo trabalha baseado em retransmissão por *timeout,* ou seja, se depois de determinado tempo o receptor não receber o pacote, o emissor realizará a retransmissão do mesmo.

2.6.3 Principais Protocolos de Correio Eletrônico

Nos dias atuais, a busca por ferramentas que facilitem a comunicação entre as organizações é constante. Uma das ferramentas já bem conhecidas e utilizadas pelas empresas é o correio eletrônico, e como conseqüência, a necessidade de se controlar as informações que trafegam por esta ferramenta é indiscutível.

2.6.3.1 SMTP

Segundo Kurose e Ross (2006) o sistema de correio é composto por três componentes, sendo eles: agentes de usuário, servidores de correio e SMTP. Cada um deles tem uma função específica no processo de transmissão da informação. Os agentes de usuários também denominados leitores de correio, é o componente que permite aos usuários lerem e enviarem suas mensagens, ou ainda de forma mais clara, seria o aplicativo. Uma vez enviada a mensagem, o seu próximo destino é o servidor de e-mail. O servidor de correio é o centro da infra-estrutura, sendo este responsável por organizar as mensagens e retransmiti-las caso necessário. O SMTP, segundo Kurose e Ross (2006), é o principal protocolo de camada de aplicação do correio eletrônico, sendo que o mesmo utiliza o serviço de transferência confiável do TCP.

O SMTP é um protocolo muito antigo e até por isso possui algumas características arcaicas, como por exemplo, a necessidade de codificar todas as mensagens para o formato ASCII. Essa característica, no caso de mensagens pequenas, não chega a

influenciar muito, porém para mensagens com grandes anexos acaba se tornando bem trabalhoso.

Outra característica do SMTP é a transmissão direta das mensagens entre os servidores do remetente e destinatário, sem a necessidade de servidores intermediários.

Segundo Comer (2006) a comunicação entre cliente e servidor é feita por meio de comandos abreviados e números com três dígitos.

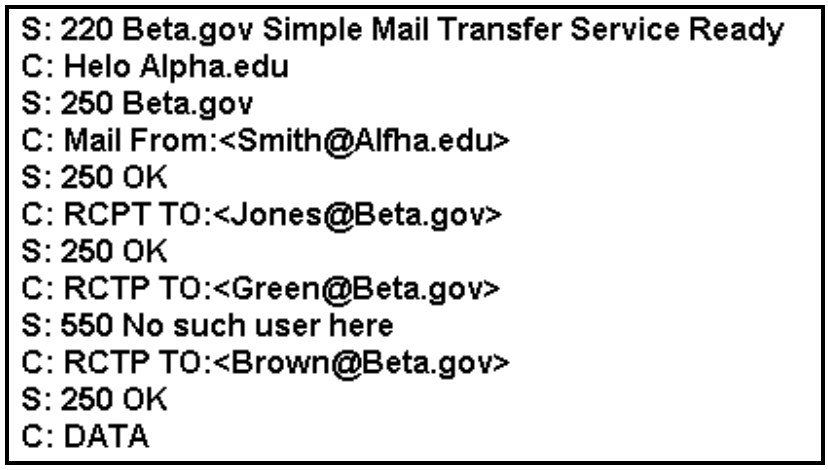

Figura 4. Exemplo de transferência SMTP
Fonte: COMER, D. (2006)

Na Figura 4 pode-se ver um exemplo de comunicação entre cliente e servidor. Primeiramente o cliente se comunica com o servidor e espera o comando 220 READY FOR MAIL, ao receber esta mensagem o cliente sabe que pode começar o envio da mensagem. Caso o servidor estiver sobrecarregado, ele espera diminuir o fluxo de seus processos e somente após envia o comando para dar prosseguimento com o envio da mensagem.

No processo SMTP, de um modo geral, o que acaba acontecendo é o servidor sempre permanecer a disposição para aceitar novas mensagens, sendo que este precisa estar conectado à Internet a todo tempo.

A seguir serão demonstrados dois protocolos que permitem que um usuário remoto, acesse seus e-mails em uma caixa de correio permanente. Estes protocolos dispensam que um servidor SMTP estabeleça uma conexão permanente com a Internet, ou seja, não há a necessidade do servidor estar conectado na Internet a todo o tempo.

2.6.3.2 POP3

De acordo com Comer (2006) no protocolo *Post Office Protocol* (POP3) as mensagens são transferidas fisicamente para a máquina do usuário. Este protocolo é extremamente simples. O cliente solicita uma autenticação no servidor, e uma vez realizada, as mensagens são transferidas para a máquina do usuário e logo após estas são apagadas do servidor.

É importante informar que geralmente o que ocorre nestas situações é a máquina trabalhar com dois protocolos, o SMTP para o envio das mensagens e o POP3 para o recebimento do servidor para a estação local, sendo este sempre em formato de texto no padrão 2822.

Segundo Kurose (2006) a conexão TCP que é utilizada para comunicação cliente/servidor é feita pela porta 110, e possui três etapas distintas: a 1ª é a de autenticação do cliente no servidor, conforme Figura 5, sendo necessário para isso o envio de usuário e senha. Na 2ª etapa as mensagens são marcadas, copiadas para a máquina do usuário e finalmente na última etapa é feita a exclusão das mensagens marcadas no servidor.

Figura 5. Autenticação de usuário no protocolo POP3
Fonte: KUROSE, J.; ROSS, K. (2006)

2.6.3.3 IMAP4

Segundo Comer (2006) o IMAP4, versão quatro do *Internet Message Access Protocol*, serve como uma boa alternativa ao POP3, sendo que este permite que o usuário possa acessar suas mensagens de qualquer lugar, pois ao contrário do POP3, este não transfira as mensagens para a máquina do usuário.

De acordo com Kurose (2006) as características do IMAP que merecem destaques são a associação das mensagens a uma pasta INBOX no momento do recebimento da mesma pelo servidor, sendo que o usuário pode estar transferindo a mensagem posteriormente e também a capacidade que o protocolo de capturar componentes da mensagem por meio de um agente de usuário. Por meio desta característica o usuário pode estar optando por fazer a verificação do cabeçalho da mensagem e somente após estar transferindo o restante da mesma. Esta característica se faz muito útil em conexões de banda estreita como uma conexão de modem sem fio ou de baixa velocidade.

2.6.4 HTTP

O protocolo *HyperText Transfer Protocol* (HTTP), segundo Kurose e Ross (2006), foi desenvolvido baseado em dois programas, sendo um cliente e um servidor.

Estes programas são executados em sistemas finais diferentes e se comunicam trocando mensagens HTTP. Quando um usuário requisita uma página WEB, o browser (navegador) envia ao servidor uma requisição para os objetos das páginas. O servidor ao receber a requisição também responde com mensagens HTTP contendo os objetos solicitados.

Ainda de acordo com Kurose e Ross (2006) o HTTP utiliza como protocolo adjacente o TCP, ou seja, primeiro é estabelecido uma conexão entre cliente e servidor e somente após é realizada a troca de mensagens HTTP por meio das interfaces sockets do protocolo TCP.

Segundo Comer (2006) as páginas WEB no servidor recebem um identificador único conhecido como URL (*Uniform Resource Locator*), que fazem com que o servidor identifique as requisições e devolva as páginas solicitadas, sendo que na URL é especificado o servidor, a porta, o caminho onde o arquivo se encontra no servidor e dependendo da situação, na URL também são passados parâmetros pelo cliente.

Uma alteração importante no protocolo HTTP, desde que o mesmo foi criado, se refere ao modo como são estabelecidas as conexões entre servidor/cliente. Inicialmente o cliente requisitava determinado item, o servidor atendia a solicitação e logo após fechava a

conexão. Na versão 1.1 do HTTP, foi adotada a técnica de conexão persistente, que mantém a mesma aberta e nesta são requisitadas e atendidas várias solicitações (Comer, 2006).

A principal vantagem da conexão persistente é a diminuição do tempo de resposta para as requisições, visto que se tem menos conexões TCP. Como conseqüência será utilizada menos memória para os *buffers* e menos tempo de utilização de processamento da máquina.

A desvantagem desta técnica está na necessidade de identificação do início e fim de cada item enviado pela conexão TCP.

Outras características que merecem destaque no que se refere a HTTP são as funcionalidades de controles como *proxy* e cache para as páginas acessadas, sendo que ambos possibilitam uma maior velocidade na entrega das requisições, uma diminuição considerável no tráfego de rede, pois reduzem transferências desnecessárias da rede.

Todos os protocolos vistos até o momento se baseiam em endereços IP's para fazer a transmissão dos dados. Será visto agora os protocolos que realizam o mapeamento do hardware das máquinas da rede de forma dinâmica e permitem que este endereço fique transparente aos usuários, sendo os mesmos já não relacionados à camada de aplicação.

2.6.5 ARP

O protocolo *Address Resolution Protocol* (ARP), segundo Comer (2006), é um protocolo que trata os endereços em um nível mais baixo da rede, permitindo que se possa

atribuir um endereço IP a uma determinada máquina e ele cria um vínculo dinâmico ao endereço físico da mesma.

Comer (2006) afirma ainda que o protocolo *Address Resolution Protocol (ARP)* possibilita que uma determinada máquina se comunique com outra por meio da rede quando somente o endereço de IP é conhecido pelo destinatário. Para se obter o endereço *Media Access Control* (*MAC*) da máquina do destinatário, o protocolo ARP envia um *broadcast* com o IP do destinatário requisitando o endereço MAC da mesma. Todas as máquinas irão receber a mensagem e analisar a mesma, mas somente a máquina com o IP destinatário responderá com o seu endereço MAC.

De acordo com Comer as mensagens ARP têm o seguinte formato:

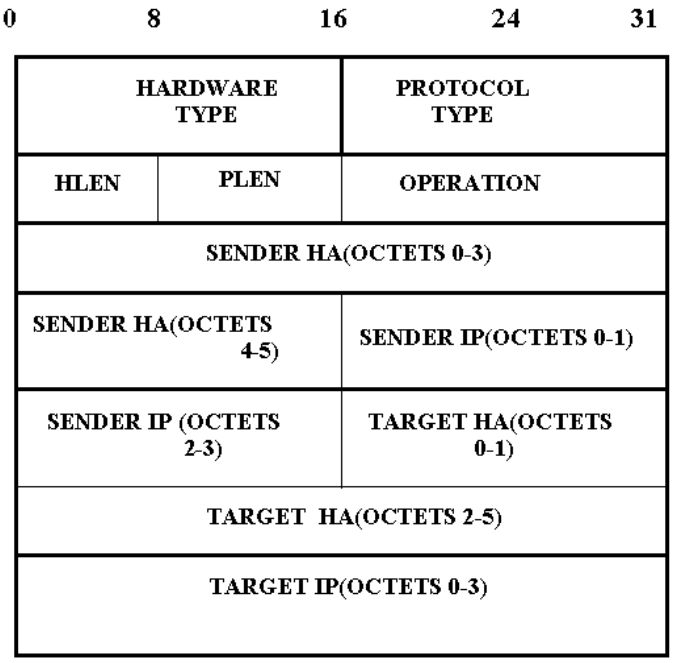

Figura 6. Formato de uma mensagem ARP
Fonte: COMER, D. (2006)

Onde:

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.

2.6.6 RARP

O *Reverse Address Resolution* (RARP) permite que um sistema obtenha um endereço IP no início da comunicação. Este protocolo segue o mesmo formato do ARP, sendo diferenciado pelo campo operação, onde para o protocolo RARP deve aparecer "3" para o caso de uma requisição e "4" para a resposta (COMER, 2006).

O funcionamento deste protocolo é bem simples. Segundo Comer (2006) o sistema (máquina), faz a requisição RARP se identificando, neste caso utilizando o endereço MAC do sistema para que o remetente saiba para quem responder, e recebe como resposta o IP na resposta RARP, IP este que será utilizado para toda a comunicação.

2.6.7 ICMP

O protocolo *Internet Control Message Protocol* (ICMP) tem como principal objetivo relatar os erros que ocorrem com os datagramas IP (CARVALHO, 1997).

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.

Segundo Carvalho (1997) 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.

Na Figura 6 se pode visualizar de que forma é feito o encapsulamento de uma mensagem ICMP em um datagrama IP.

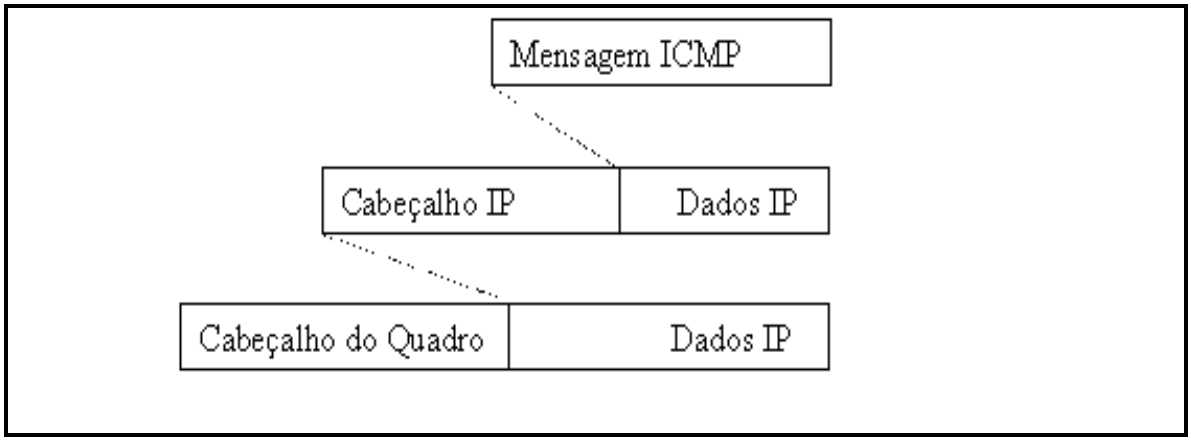

Figura 7. Encapsulamento da mensagem ICMP em um datagrama IP
Fonte: CARVALHO, T. (1997)

Segundo Ulbrich e Valle (2006) o protocolo ICMP possui o mesmo cabeçalho do protocolo IP, mas no campo de dados é inserido mais um campo de controle, denominado ICMP Type Field, que vai identificar o tipo de mensagem que o ICMP vai transportar.

No Capítulo 3 serão demonstradas algumas ferramentas *sniffers*, que são programas capazes de capturar os dados que trafegam pela rede, separando até mesmo por protocolos e com isso permitindo a análise sobre estes dados.

3 SNIFFERS

O TCP/IP, que foi o protocolo base para o tráfego de redes, desde sua origem até os dias atuais, mostrou muita qualidade na questão de flexibilidade, porém, deixa a desejar no que diz respeito à segurança, mesmo porque a característica mais visada na sua criação foi a flexibilidade (CARMONA, 2006).

Segundo Carmona (2006) todas as informações que trafegam na rede, são apenas separadas em pacotes, que são reagrupados na estação de destino. Mas estas informações trafegam por toda a rede de forma limpa, sendo que este protocolo não fornece um nível de segurança adequado para as informações que são transitadas.

As informações transitadas em modo texto ou limpo, facilitam a utilização de ferramentas *sniffers*, que são capazes de remontar os bits de texto e traduzir estas mensagens (FURMANKIEWICZ, 2000).

3.1 O QUE É SNIFFER?

O termo *sniffer* é derivado de um produto, chamado *Sniffers* 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 (FURMANKIEWICZ, 2000).

Os *sniffer*s geralmente são utilizados pelos administradores de rede para identificação de problemas na mesma, pois ao capturar pacotes, fornecem ao administrador,

informações sobre endereço de origem e destino, formação dos pacotes, além de outras informações ao nível de protocolo úteis da resolução de problemas (CASAGRANDE, 2003).

Segundo Furmankiewicz (2000) *sniffers* 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, sendo que dependendo do programa utilizado, dispõe-se de vários recursos para estudar o tráfego da rede em questão.

Apesar de seu ótimo propósito, ou seja, auxiliar os administradores de rede, os *sniffer's* também podem ser utilizados para fins de espionagem, principalmente por hacker's, pois como estas ferramentas podem ler e identificar toda e qualquer atividade que ocorra no nível de rede entre dois ou mais dispositivos na mesma (Júnior e Filho, 2002). Esta característica faz com que os *sniffers's* sejam muito relacionados com ferramentas espiãs ou de espionagem.

Na Figura 8 pode ser verificado a arquitetura de um *sniffer*.

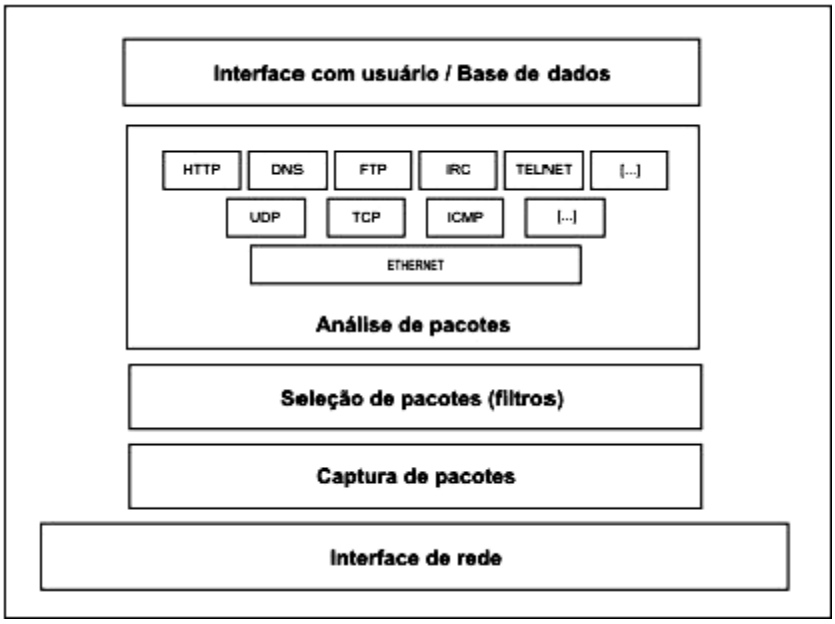

Figura 8. Arquitetura de um Sniffer
Fonte: REIS, JÚNIOR; SOARES, FILHO (2002)

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 caracterizados como inseguros pelo fato de enviarem senhas em formato texto comum que são facilmente capturadas (CASAGRANDE, 2003).

3.2 FUNCIONAMENTO DE UM SNIFFER

De acordo com Ulbrich e Valle (2006) para que uma ferramenta *sniffer* consiga detectar e capturar os pacotes de uma rede, o mesmo deve também estar diretamente conectado a mesma, assim como as demais máquinas.

Conforme já mencionado anteriormente, em uma rede Ethernet, a comunicação é baseada no MAC das máquinas, que é o número que identifica esta máquina na rede. Segundo Comer (2006) este MAC é definido um uma interface chamada NIC (network *interface card*). Nesta interface podem ser definidos parâmetros, que podem restringir tipo de pacotes irão ser aceitos e quais serão recusados, como por exemplo, *unicast, broadcast* e *multicast.*

Segundo Ulbrich e Valle (2006) quando um *sniffer* é instalado em uma rede, a primeira ação executada é colocar alguma interface de rede em modo promíscuo. Uma vez feito isso à interface passará a "escutar e receptar" todos os pacotes que estão trafegando pela rede, e não apenas os destinados a ela, que é o modo padrão.

Uma vez em modo promíscuo, a ferramenta *sniffer* passa a capturar todos os pacotes que passam pela rede. A maioria das ferramentas possui diversas funcionalidades, que facilitam os administradores de rede, ou hackers separarem o tráfego por protocolo, analisar o tráfego, emitir gráficos estatísticos do fluxo de dados (ULBRICH; VALLE, 2006).

Segundo Casagrande (2003) alguns fatores podem estar influenciando na execução destas ferramentas em uma rede como a topologia da mesma, os protocolos utilizados, o comportamento dos usuários, entre outros.

De acordo com Ulbrich e Valle (2006), o equipamento utilizado para conexão das máquinas na rede interfere diretamente na forma como vai ser instalada e configurada a ferramenta *sniffer*. Alguns autores mencionam ainda que para controlar problemas com *sniffers* na rede basta substituir os *hubs* por *switches*.

Na Figura 9 se pode observar o funcionamento do *sniffer* em uma rede comutada, com a utilização de *switch* e também em uma rede de difusão, com *hubs.*

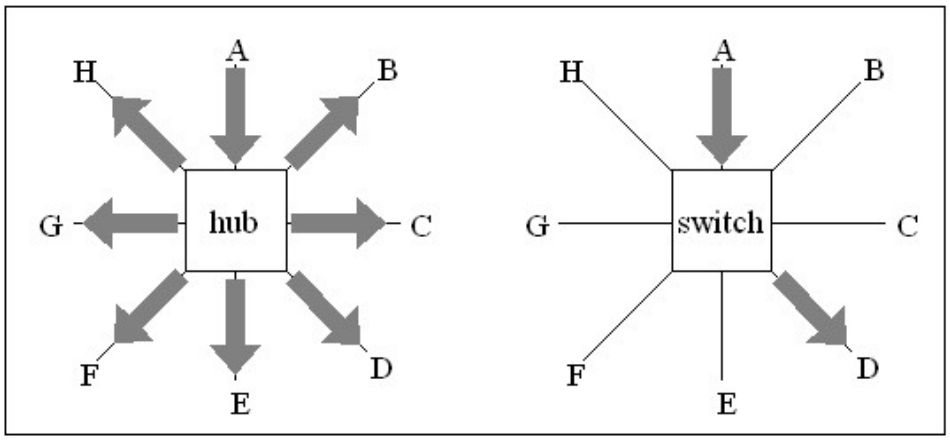

Figura 9. Funcionamento de um HUB e de um SWITCH
Fonte: Casagrande, R. (2003)

Na Figura 9 apesar do *hub* ser representado por uma estrela, na realidade as máquinas são ligadas na rede por meio de barramento, desta maneira, quando uma máquina envia um pacote pela rede para uma outra máquina qualquer em modo promíscuo, todas as demais máquinas da rede estarão "ouvindo".

Segundo Casagrande (2003) em redes comutadas, o switch realiza a distribuição do tráfego de dados pelo endereço de destino que cada pacote possui, ou seja, os pacotes são direcionados apenas para a máquina de destino, sem que as interfaces das demais máquinas da rede fiquem sabendo de sua existência.

O desempenho deste tipo de rede é considerado superior ao de redes de difusão, porém seu custo é mais alto, dada à necessidade de hardwares especializados.

Apesar da eficiência quanto ao direcionamento dos pacotes, as redes comutadas não ficam isentas da utilização dos *sniffers*, no que se refere ao uso mal intencionado da

ferramenta, até mesmo porque os switches não foram criados com o propósito de segurança (JUNIOR; FILHO, 2002).

Conforme Junior e Filho (2002) existem técnicas que permitem "driblar" diversos protocolos, possibilitando assim 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, conforme pode ser visualizado na Figura 10 abaixo.

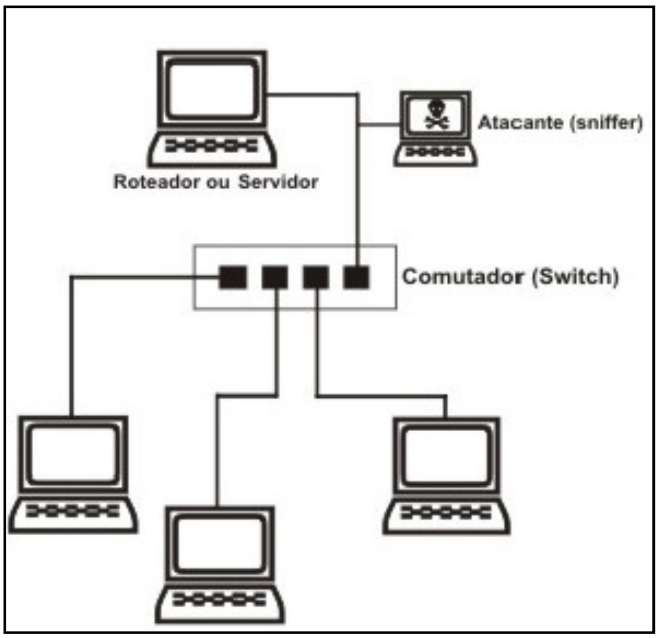

Figura 10. Instalação de um *sniffers* em uma rede comutada
Fonte: REIS, JÚNIOR; SOARES, FILHO (2002)

Segundo Casagrande (2003) outra técnica capaz de driblar os comutadores é a *MAC Flooding*, que consiste em inundar o switch com endereços MAC falsos, obtendo assim o estado *fail open*, sendo que com isso o switch passe a trabalhar como um *hub*, permitindo assim que o *sniffer* obtenha as informações de todas as máquinas conectadas. O

que possibilita a utilização desta técnica é o modo de trabalho do switch, que utiliza uma tabela de endereços MAC para poder estabelecer circuitos virtuais entre as estações conectadas em suas portas.

3.3 PRINCIPAIS SNIFFERS E SUAS FINALIDADES

Existem atualmente muitas ferramentas do tipo *sniffer*, com diversas aplicações e funcionalidades, sendo estas disponíveis para os sistemas Linux e Windows.

De acordo com Casagrande (2003) algumas das principais ferramentas disponíveis no mercado são:

a) **Win Sniffer**: ferramenta para monitoramento de rede, cujo principal objetivo é controlar os principais protocolos de rede, como FTP, Telnet, HTTP, POP2/POP3, IMAP, NNTP, ICQ e outros. Ao contrário dos demais, *sniffers*, que apresentam "lixo" na leitura dos pacotes, este captura as informações de maneira clara, organizada, e muito fácil de usar;

b) ***Ntop:*** este *sniffer* permite o monitoramento da atividade da rede de forma parecida à ferramenta *Top* do Unix, que informa os processos que a CPU utiliza e o desempenho dela. Pode ser utilizado para Windows e Linux e dá suporte aos seguintes protocolos: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, TCP/UDP;

c) **IPTraf:** é uma ferramenta de monitoramento de rede, com o modo texto para levantamento de estatísticas de rede. Trabalha no sistema operacional

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) ***Wireshark:*** antigo e muito conhecido Ethreal. É um analisador gráfico de protocolos de rede para ambientes Unix e Windows. Tem como objetivo dar ao administrador da rede o controle sobre o trafega pela rede, possibilitando a detecção de forma rápida de qualquer tipo de *trojan*, *spyware* ou acesso não autorizado;

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

h) ***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

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

No próximo capítulo serão demonstrados alguns trabalhos correlatos a este.

4 TRABALHOS CORRELATOS

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

a) A UNESC – Universidade do Extremo Sul Catarinense apresentou um trabalho onde foram realizadas pesquisas e análises sobre o tráfego de redes dos laboratórios da universidade, onde foi utilizada a técnica de amostragem estratificada para a definição das amostras e a ferramenta Ethreal em um ambiente Linux para a coleta e estudo do tráfego da rede (TROMBIM, 2006).

b) 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 também um estudo sobre a segurança em redes de computadores (POMPERMAYER JR, 2002).

c) A Universidade Federal do Rio Grande do Sul apresentou um trabalho sobre formas de detecção de *sniffers*. Este trabalho teve como principal objetivo 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).

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 por meio da observação da rede local do Instituto de Física de São Carlos (IFSC). (FRANCESCHI, 2003).

e) 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. (SOUZA; FILHO, 2004).

5 ANÁLISE DO TRÁFEGO DA REDE DA TSA QUÍMICA DO BRASIL

Neste capítulo serão demonstradas as técnicas estudadas e também a forma que foi realizada a coleta e análise dos dados da empresa. Será apresentada a técnica de amostragem, a ferramenta utilizada e todos os demais procedimentos utilizados para obtenção das amostras posteriormente analisadas.

Será visto também, com base na análise das informações coletadas, o diagnóstico da rede sob o ponto de vista de tráfego de dados na mesma.

5.1 MÉTODO DE COLETA APLICADO NA PESQUISA

Segundo Barbetta (2005) em pesquisas científicas, quando se deseja conhecer características de uma população, é comum analisar apenas uma amostra dos elementos totais, e no sucesso deste tipo de aplicação em trabalhos já realizados[2], para realização da análise da rede da TSA Química, dentre as técnicas de amostragem estatística existentes, foi aplicada a técnica de Amostragem Estratificada.

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 (BARBETTA; 2005).

[2] Em trabalho de graduação realizado na UNESC, em 2006, a técnica em questão foi aplicada com sucesso para definição das amostras para posterior coleta de informações referentes a um segmento de rede da UNESC (ver trabalhos correlatos).

Este tipo de amostragem, viabilizou a coleta e análise dos dados da rede da TSA Química, pois em um cenário empresarial é imensa à quantidade de informações que trafegam pela rede e a análise acaba por dificultar o processo.

5.1.1 Método de Amostragem Estratificada

Segundo Cocharan (1997) a estratificação é uma técnica comum que pode proporcionar o aumento de precisão nas estimativas das características da totalidade da população.

De acordo Kamienski (2005) para a aplicação de uma amostragem estratificada, uma população total N, é dividida em subpopulações ou estratos menores, N1, N2, N3, N4,...NX, sendo que a soma destes estratos deve resultar no total da população.

Este método, segundo Barbetta (2005), pode ser aplicado de duas formas, sendo elas, proporcional e uniforme.

Esta pesquisa seguiu o mesmo raciocínio de trabalhos feitos anteriormente (TROMBIM, 2006), sendo que os mesmos tiveram êxito da obtenção dos resultados, sendo que para isso foi utilizado o método de amostragem estratificada proporcional.

Com todos os estratos, seleciona-se para cada um deles uma amostra, podendo ser diferentes seus valores para cada estrato, sendo estas amostras n1,n2,n3,...nx.

Este método leva em consideração que o tamanho de cada estrato é proporcional ao tamanho correspondente de cada amostra, ou seja, se um determinado

estrato equivale a 20% do total da população, neste caso ele deve corresponder a 20% da amostra. As fórmulas a serem aplicadas podem ser verificadas a seguir.

$$p = (E/P)$$

Onde:

a) p = porcentagem representativa do valor do estrato diante do valor da população;
b) E = estrato;
c) P = população total.

Para os cálculos deste trabalho foi definido que o extrato seria representado pelo volume em megabytes do tráfego da rede referente à uma hora de coleta.

5.1.2 Aplicação do método definido no cenário da empresa

Para aplicação do método de amostragem estratificada o 1º passo realizado foi a realização de uma coleta base. Baseando-se nesta coleta foi calculado o percentual de importância de cada horário e posteriormente o tamanho de cada amostra, sendo este calculado por meio da fórmula a seguir:

$$t = p * E$$

Onde,

t= tamanho da amostra para cada hora.

Para realização desta coleta base observou-se o período de maior tráfego na rede da empresa. Isto foi possível por meio da ferramenta PRTG, instalada no proxy da empresa, conforme Figura 11.

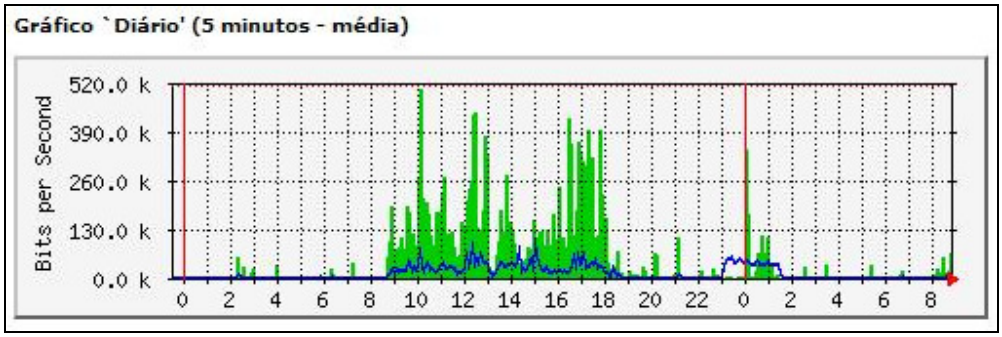

Figura 11. Gráfico do tráfego da TSA Química gerado pelo P*RTG*

Com o tamanho da amostra definido foi aplicada a fórmula abaixo para chegar ao valor em tempo de cada amostra.

$$f = t / E$$

Onde:

f= tamanho da amostra para cada hora.

Esta coleta foi realizada no dia 08/10/2008, por meio da ferramenta PRTG Traffic Grapher, onde foram obtidos os dados conforme Figura 12.

	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum	
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second
8/10/2008 17:00 - 18:00	725.614,366	1.652,029	551.766,530	1.256,224	1.277.380,896	2.908,254
8/10/2008 16:00 - 17:00	711.692,080	1.620,427	412.380,321	938,934	1.124.072,401	2.559,361
8/10/2008 15:00 - 16:00	608.938,573	1.386,455	398.863,374	908,148	1.007.801,947	2.294,603
8/10/2008 14:00 - 15:00	755.431,386	1.727,549	463.094,259	1.059,021	1.218.525,645	2.786,570
8/10/2008 13:00 - 14:00	562.143,518	1.750,229	296.174,846	922,138	858.318,363	2.672,367
8/10/2008 12:00 - 13:00	389.310,780	1.247,139	153.710,710	492,405	543.021,490	1.739,544
8/10/2008 11:00 - 12:00	842.418,117	1.917,880	453.020,687	1.031,364	1.295.438,804	2.949,244
8/10/2008 10:00 - 11:00	725.455,762	1.651,677	911.263,729	2.074,715	1.636.719,491	3.726,392
8/10/2008 09:00 - 10:00	769.271,350	1.759,955	438.073,086	1.002,233	1.207.344,436	2.762,188
8/10/2008 08:00 - 09:00	807.710,854	1.847,232	420.440,551	961,546	1.228.151,404	2.808,778
8/10/2008 07:00 - 08:00	363.784,565	2.209,790	130.743,950	794,197	494.528,516	3.003,988

Figura 12. Coleta base via ferramenta PRTG Traffic Grapher

Conforme já mencionado a ferramenta utilizada foi o PRTG Traffic Grapher, que apresentou uma boa interface e fácil de ser utilizada. A mesma foi instalada em um ambiente Windows e proporcionou a geração das informações necessárias para o processo de cálculo.

Com a aplicação das fórmulas citadas anteriormente se obteve os resultados conforme Tabela 1.

Tabela 1. Horários e tempo de duração de cada coleta.

Dias da semana	Coleta	Horários	Dur. da coleta
2 ª FEIRA	1	07h às 08h	2 min e 40 seg.
3 ª FEIRA	2	08h às 09h	6 min.
	3	09h às 10h	6 min.
	4	10h às 11h	8 min e 20 seg.
4 ª FEIRA	5	11h às 12h	6 min.
	6	12h às 13h	2 min e 40 seg.
	7	13h às 14h	4 min e 20 seg.
5 ª FEIRA	8	14h às 15h	6 min.
	9	15h às 16h	5 min e 20 seg.
	10	16h às 17h	5 min e 40 seg.
	11	17h às 18h	6 min.

Para formação da tabela acima foram realizados os seguintes cálculos, conforme aplicação das fórmulas já citadas:

p = 494528 / 11891297 = 4%

t = 494528 * 4% = 19781,12

f = 19781,12 / 494528 = 2,40 (convertido para minutos/segundos)

O cálculo acima condiz com o horário das 7h às 8h, sendo que para os demais horários foram aplicadas as mesmas fórmulas.

Após a definição dos tempos a serem coletados, o próximo passo seria realizar as coletas e analisar os dados em questão.

5.2 APLICAÇÃO DA FERRAMENTA SNIFFER NA REDE DA EMPRESA

Com os tempos das amostras definidos o passo seguinte seria realizar as coletas para posterior análise dos dados.

Para o início desta fase de coletas, um dos pontos chaves foi buscar o entendimento do ambiente a ser coletado, ou seja, conhecer a estrutura de rede da TSA Química LTDA.

5.2.1 Estrutura da rede da TSA Química

A rede da TSA Química atualmente é composta por 69 computadores, onde destes 69, 6 são servidores e 63 são estações de usuários.

A conexão entre os computadores e máquinas é feita por 3 *switches* e 4 *hubs*, sendo estes distribuídos da seguinte forma: Na sala dos servidores fica um switch principal, e este distribui o sinal para o restante da rede. Deste *switch* o sinal é distribuído para outro switch que também fica na sala dos servidores e outro que fica no setor de Expedição da empresa. O *switch* principal também faz a ligação para os *hubs*, localizados nos seguintes setores: RH, Almoxarifado, Produção Solvente, Unidade Água.

Para os *hubs* dos setores Produção Solvente, Almoxarifado e Expedição, a conexão é feita por fibra óptica, devido à distância que a comunicação é realizada.

Para a conexão com o *hub* da Unidade Água, por estar a alguns kilometros da matriz e por conseqüência do *switch* principal, a comunicação é feita por wireless.

Conforme mencionado, a empresa dispõe de 6 servidores, sendo eles relacionados:

a) 4 Linux (rede, e-mail, *firewall* e banco de dados);

b) 2 Windows (servidor WTS e servidor de aplicações virtualizado).

Para realização das coletas, dentre as possibilidades estudadas a mais viável foi a substituição do *switch* principal da empresa por um *hub* devido ao fato do *switch* não trabalhar em modo de difusão, conforme abordado na sessão 3.2. Com isso se conseguiria capturar toda a comunicação das estações da empresa com os servidores da mesma.

Aplicando a substituição citada, foi desconsiderada a comunicação feita entre as estações dos demais *switches* da empresa, mas como no ambiente da mesma, não se tem à prática de utilizar compartilhamento entre máquinas, exceto pastas nos próprios servidores, impressoras, capturando o tráfego das estações com os servidores, estaria sendo capturado a maioria do tráfego real da empresa.

Esta técnica de aplicação do *sniffer* foi ilustrada na Figura 10 na sessão 3.2.

A seguir será demonstrado como foram realizadas as coletas dos dados e a aplicação da ferramenta da análise do tráfego da rede.

5.2.2 Aplicação da Ferramenta Wireshark

A opção pelo Wireshark[3] aconteceu depois de várias pesquisas e referências encontradas na Internet, onde se pode verificar as características da ferramenta (destacadas na seqüência) e constatar que a mesma atenderia as necessidades do trabalho, além de se tratar de um software gratuito.

A instalação foi feita em minha estação de trabalho, onde se pôde estudar melhor a ferramenta antes da coleta e análise efetiva dos dados.

Na Figura 13 pode ser visualizado a tela principal da ferramenta.

---

[3] A ferramenta Wireshark encontra-se disponível para download no site http://www.wireshark.org/download.html

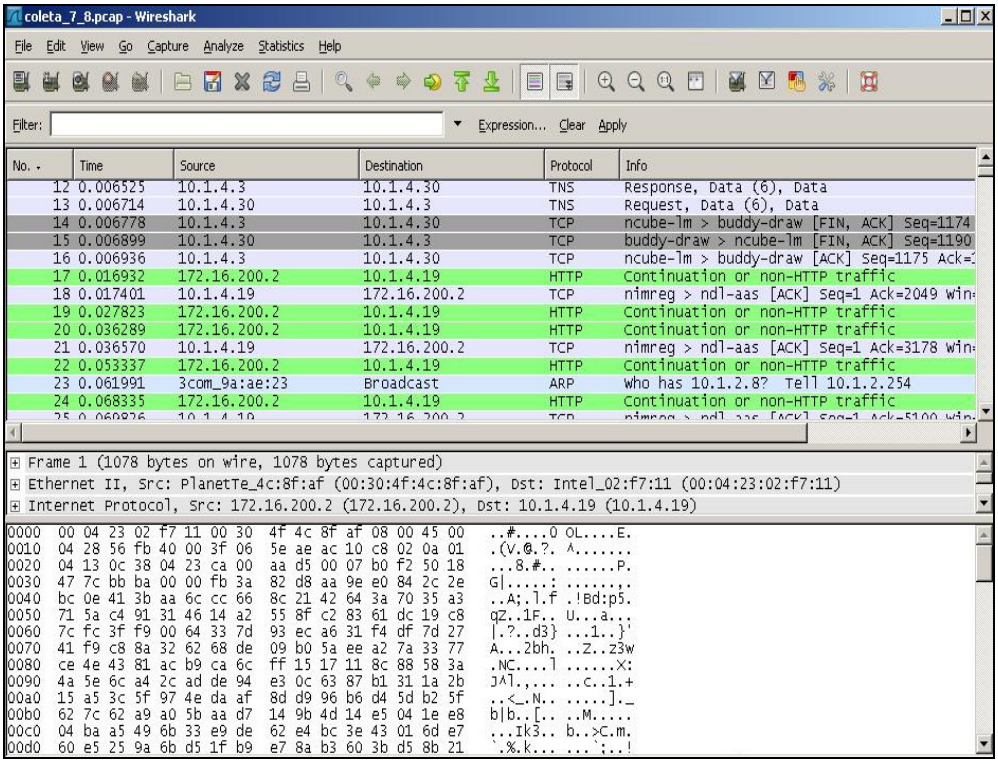

Figura 13. Demonstração da ferramenta Wireshark

A forma como o tráfego é demonstrado pelo Wireshark segue a seguinte ordem: listagem dos pacotes capturados no 1º quadro, detalhes sobre os protocolos pertencentes a cada um dos pacotes no 2º quadro e conteúdo hexadecimal de um pacote no 3º.

A ferramenta dispõe de várias funcionalidades, dentre ela pode-se destacar:

a) possibilidade de realizar vários filtros sobre os dados coletados, permitindo desta forma organizar e analisar somente o tráfego de interesse;

b) possibilidade de desmembramento e visualização de cada parte do pacote, ou seja, possibilita identificar o que cada camada adiciona ao pacote.

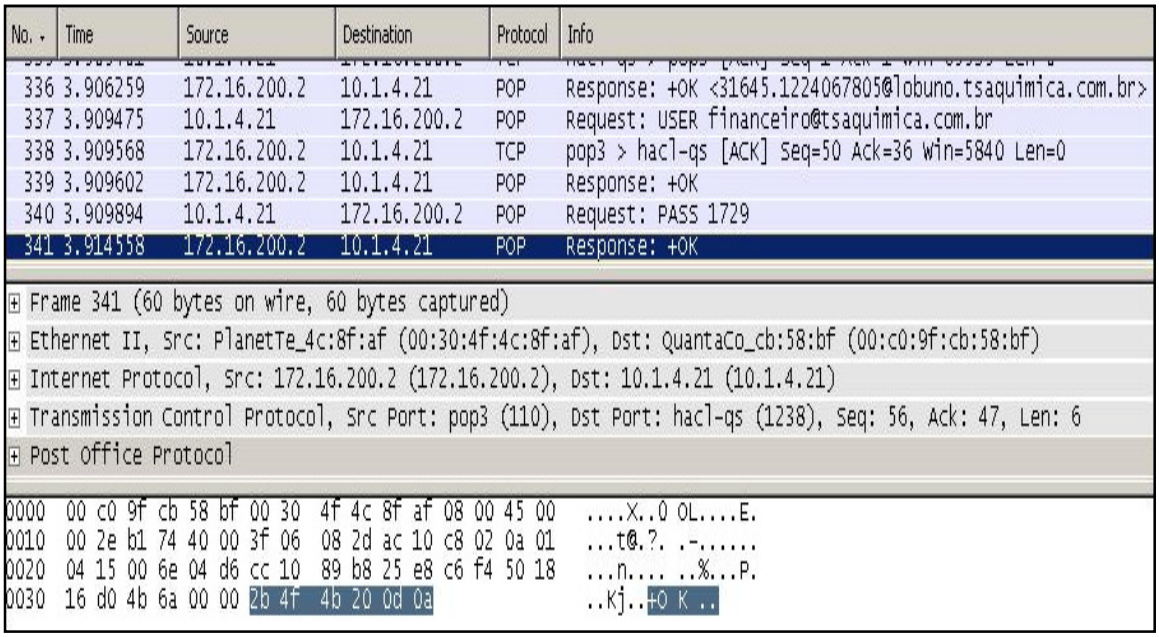

Figura 14. Visualização de autenticação de usuário de correio com Wireshark

O quadro superior da Figura 14 mostra a lista ordenada dos pacotes capturados. Nos quadros inferiores são mostradas informações deste pacote.

No quadro do meio pode ser verificado como foi formado o pacote que efetivamente transita pela rede. Na prática, o que ocorre é o seguinte: Para a formação do pacote, o aplicativo de correio do usuário fornece informações para o protocolo POP3 montar seu pacote. Este pacote é passado para o protocolo TCP que adiciona seu cabeçalho e posteriormente passa o pacote para o protocolo IP, responsável por definir a rota do pacote. Feito isso o pacote é passado para a placa Ethernet, que por sua vez adiciona os endereços MAC de origem e destino no pacote, conhecido como frame Ethernet está pronto para ser lançado na rede.

No terceiro quadro podem ser visualizadas além das informações em um formato compreensível as suas equivalências em hexadecimal.

5.2.3 Aplicação de filtros sobre as coletas

Depois de realizadas as devidas coletas sobre a rede da TSA Química, o próximo passo seria a análise dos dados. Porém, devido à grande quantidade de dados transitados pela rede da empresa, esta análise seria praticamente impossível sem a aplicação de filtros sobre estes dados.

Conforme já citado como uma das principais vantagens da ferramenta Wireshark, os filtros realmente foram de suma importância no momento da análise dos dados coletados. Proporcionaram 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 de forma segura.

A utilização dos filtros foi aplicada principalmente para possibilitar a identificação dos protocolos e aplicações que estiveram presentes nas coletas realizadas.

Um exemplo de filtro que pode ser citado e que foi utilizado para buscar todo o tráfego destinado para o servidor de banco de dados, “ip.src == 10.1.4.3 || ip.dst==10.1.4.3”.

A ferramenta disponibiliza no seu help várias formas e exemplos de como pode estar sendo utilizados os filtros de forma a auxiliar no processo de manipulação dos dados coletados.

5.2.4 Dificuldades Encontradas

Principalmente por se estar atuando em um ambiente de produção, várias foram as dificuldades encontradas.

Uma das primeiras situações com a qual se foi deparado, foi à forma como deveria ser feita a coleta dos dados, que por estar em um ambiente corporativo, estaria representando uma grande quantidade de dados, não possibilitando o estudo sobre o montante absoluto dos mesmos.

Para a realização efetiva das coletas também foi muito estudado a forma de como as mesmas seriam executadas, de modo que mesmo sendo amostras, representassem de forma eficiente o ambiente geral da rede da empresa. Era conhecido que pelo fato da empresa utilizar *switch* como principal distribuidor de sinal, deveria ser realizado alguma modificação ou tratamento para possibilitar a captura do tráfego para o estudo.

Com a opção pela troca do *switch*, foi encontrada outra situação adversa. Esta troca teria que ser feita com toda a empresa em funcionamento, pois o *hub* utilizado para a captação não seria capaz de suportar a demanda por muito tempo. Então era feita a troca, depois de capturados os dados, a troca era desfeita, voltando para o *switch* titular.

Para as máquinas com Windows XP, não chegava a representar um problema, pois a mesma somente perdia conexão por poucos segundos, porém estações com Windows 98 o reinicio da máquina era necessário para a conexão com o banco de dados/rede.

No momento da análise das informações coletadas, já na ferramenta *sniffer*, foi encontrada outra situação que acabou prejudicando o estudo das coletas de uma forma

geral. Foi detectada uma limitação de memória da ferramenta, não suportando mais que 1,0 Gb, sendo que esta limitação impossibilitou a junção de todos os arquivos coletados, necessitando a análise e estudo individualmente.

Superadas as adversidades citadas, foi tentado demonstrar da forma mais clara possível o tráfego da rede da empresa, bem como os principais protocolos utilizados no ambiente da mesma.

5.2.5 Resultados Obtidos conforme Coletas Realizadas

Nesta seção do trabalho buscou-se por meio de tratamentos e filtros, definir de forma clara e distinta a utilização da rede da empresa com base nas amostras coletadas.

O primeiro passo realizado foi a verificação da demanda e consumo da rede da empresa, separado por horas. Na Figura 15 pode-se observar os picos de consumo na rede e perceber claramente a diminuição de utilização durante o período das 12:00 hs às 13:00 hs, que corresponde ao horário de almoço da maioria dos funcionários.

Conforme verificado na Figura 15, uma das situações que foi detectada foi uma grande utilização da rede durante o horário de almoço. Mesmo com a diminuição significativa, o consumo permaneceu muito alto para um horário onde a maioria dos colaboradores da empresa estaria almoçando.

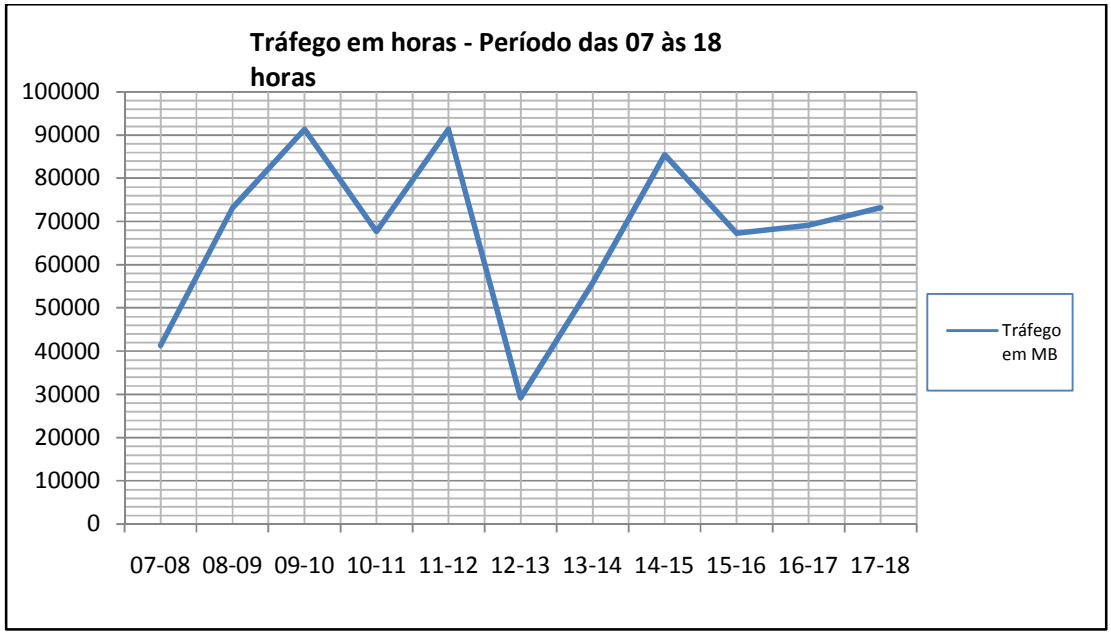

Figura 15. Tráfego por hora – Período: Das 8 às 15 horas.

Com uma visão do tráfego em geral da rede da empresa, conforme Figura 15, foi comparado o mesmo com o tráfego em separado dos servidores da empresa a fim de ter uma noção da forma como estava sendo feita a distribuição da banda de rede.

Para as coletas deste trabalho foram desconsiderados pela ferramenta os protocolos ARP e RARP, por serem protocolos nativos da rede, e pouco poderia ser feito no intuito de otimizar ou diminuir a utilização deste tipo de protocolo.

Na Figura 16 é demonstrado o tráfego total da rede, já demonstrado na figura acima, porém agora visualizado em pacotes, e o tráfego do servidor de banco de dados da empresa, sendo este considerado um tráfego totalmente produtivo para a empresa.

Pode ser observado que o tráfego da rede, na maior parte do dia segue uma relação com o tráfego do banco de dados. Outro ponto detectado foi que mesmo com uma

diminuição do tráfego ao meio dia devido ao intervalo de almoço, principalmente para o banco de dados, continuou havendo um grande volume na rede.

Outro ponto importante observado foi que de todo o tráfego da rede com o servidor de banco de dados, foi-se utilizado praticamente um único protocolo, sendo ele o TNS, protocolo utilizado para comunicação com o banco de dados Oracle, salvo de algumas poucas exceções.

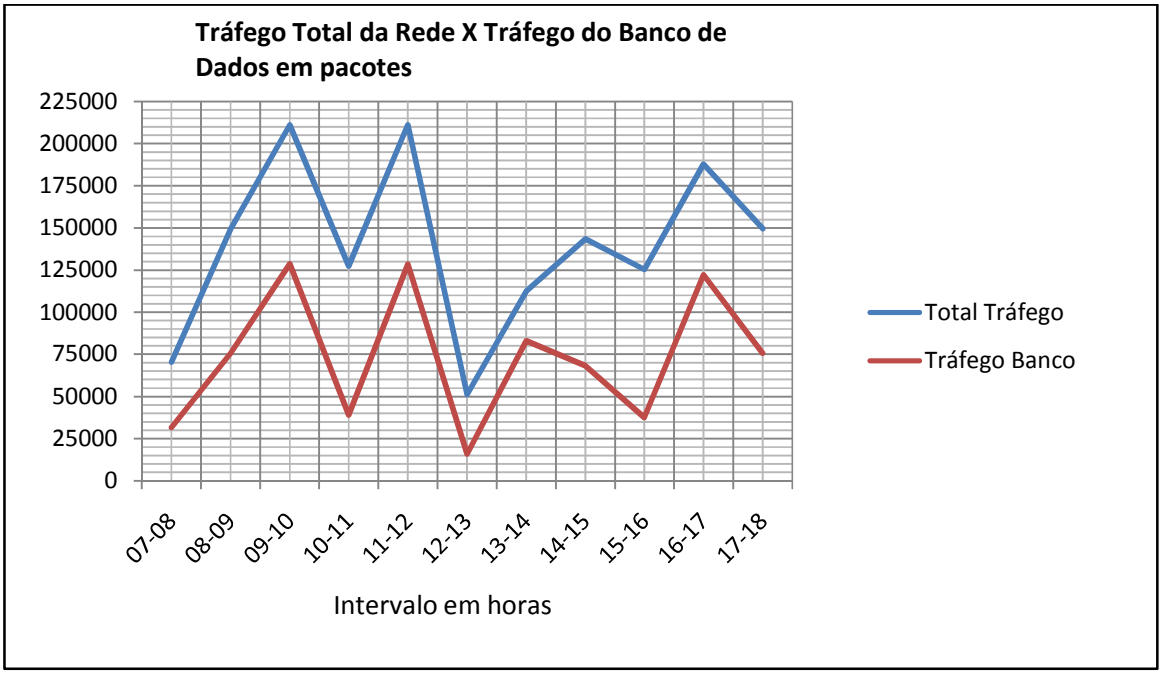

Figura 16. Comparação do Tráfego total da rede com o tráfego para o banco de dados

Na Figura 17, assim como na Figura 16, foi comparado o tráfego total da rede, só que desta vez com o servidor de arquivos da rede. Este servidor utiliza ambiente Linux e possui um servidor Samba para armazenamento de arquivos, inclusive fonte e executáveis dos principais programas da empresa.

Na análise do tráfego deste servidor foi detectado que o principal protocolo utilizado foi o SMB (*Server Message Block*), que se refere a um protocolo de compartilhamento de arquivos, criado pela Microsoft e utilizado em redes Windows (ROSS, 2008).

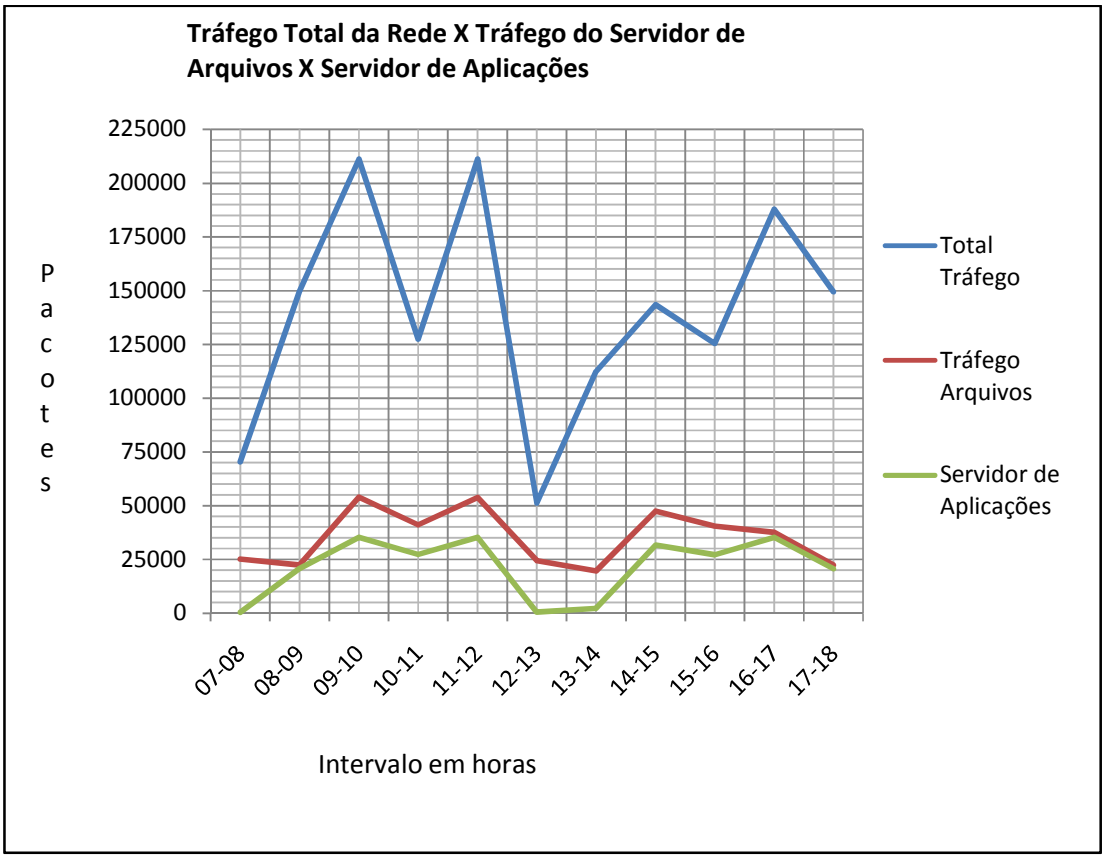

Figura 17. Comparação do Tráfego total da rede com o tráfego do servidor de arquivos

O tráfego da linha vermelha na Figura 17 se refere a todo acesso que é feito ao servidor de arquivos Samba, bem como cópia, transferências e modificações nos arquivos deste servidor.

A linha verde na Figura 17 se refere ao tráfego referente a uma máquina virtual, instalada no servidor de arquivos, mas para efeito de tráfego de rede, deve ser considerada como uma máquina independente. Neste servidor estão instalados vários serviços referentes a aplicativos da Senior Sistemas LTDA, empresa esta que fornece o sistema ERP, folha e ponto dos funcionários da TSA Química LTDA.

Até o momento foi visto a latência da rede para utilização interna, ou seja, os pacotes estavam sempre trafegando na rede interna da empresa. A seguir será mostrado um dos pontos mais importantes da análise, que se refere ao uso da rede para acesso externo, que além de poder prejudicar o fluxo da rede, consome também o *link* de Internet da empresa para fins não produtivos atrapalhando assim o trabalho de usuários que dependem deste recurso.

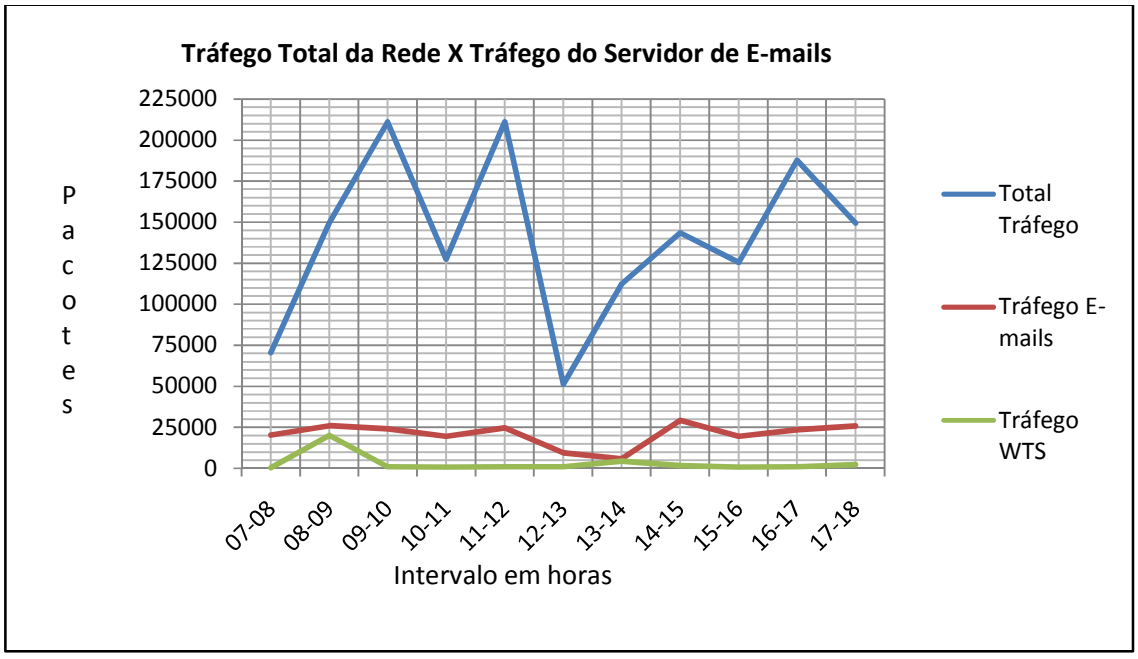

Figura 18. Comparação do Tráfego total da rede, tráfego do servidor de e-mails, tráfego do servidor WTS

Na Figura 18 pode-se verificar o tráfego de e-mails e também do servidor WTS, que se comparado ao fluxo total da rede parece não ter tanta relevância, porém, conforme já

foi citado, este tráfego não se refere apenas ao consumo da rede interna da empresa, mas sim ao consumo da banda de Internet.

Todo tráfego da empresa referente ao acesso externo precisa ser dada uma atenção especial, pois é este tipo de acesso que expõe a empresa aos riscos provenientes da Internet, como vírus, espionagens, invasões, *spans*, *trojans*, além de desviar a atenção dos funcionários da empresa de suas responsabilidades e rotinas produtivas de trabalho.

Na Figura 19 pode ser visualizado como está a divisão do tráfego da empresa entre seus servidores.

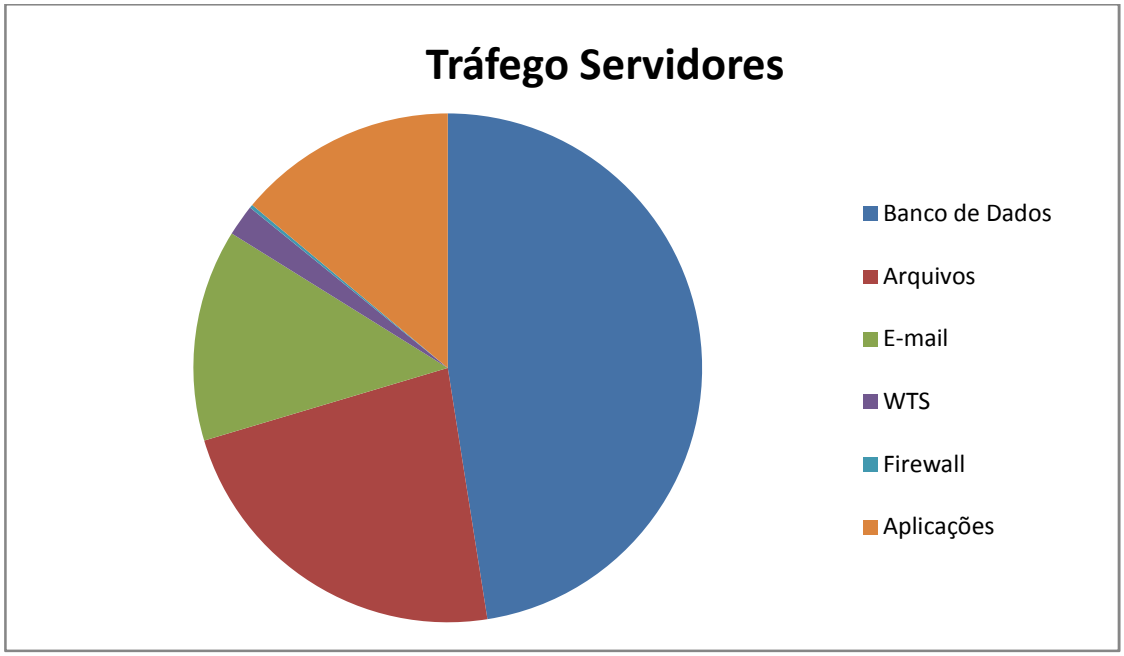

Figura 19. Tráfego de rede dos servidores da empresa

Para poder visualizar o tráfego da rede de uma forma geral, foi utilizada a opção “Merge” da ferramenta Wireshark, o qual possibilita a junção dos arquivos coletados, porém conforme já mencionado na sessão 5.2.4, devido a limitação de memória

da ferramenta, foi retirado desta junção todo o tráfego referente ao servidor de banco de dados.

Após a junção dos arquivos podê-se identificar algumas aplicações e serviços que tiveram uma utilização maior, conforme verificado na Tabela 2 a seguir.

Tabela 2. Volume de pacotes das principais aplicações e serviços

APLICAÇÃO/ SERVIÇO	Nº PACOTES
DNS	1655
HTTP	42411
Netbios Name Service	1770
NetBios Session Service	211513
HTTPS	203
POP	20107
SMTP	9264
TNS	806475

Na da Tabela 2, se pode confirmar que o maior tráfego de rede é formato pelo protocolo TNS, para o tráfego das informações do banco de dados entre servidor e estações de usuários.

Outro ponto observado com a união dos arquivos é que o tráfego que predomina da rede da empresa roda na estrutura TCP/IP, sendo que 99,48% utilizado o protocolo TCP e apenas 0,52% roda sobre o UDP como protocolo de nível de rede.

Na Tabela 2 se pode observar um número muito alto de pacotes utilizando o protocolo Netbios Session Service (no nível de rede), isto se refere à utilização de um protocolo de rede de alto nível, chamado SMB, que é um protocolo de compartilhamento de arquivos na rede. Este protocolo permite que um cliente manipule um determinado arquivo

como se estivesse em sua própria máquina. É um protocolo que pode ser utilizado tanto em redes Windows quanto em Linux.

Na rede da empresa foram detectados alguns outros protocolos, porém apresentando um grau de utilização insignificante perante o contexto, sendo assim não foram detalhados neste trabalho.

5.3 SUGESTÕES DE MELHORIA PARA O CENÁRIO DA EMPRESA

Na rede da empresa TSA Química do Brasil, conforme foi verificado trafegam vários tipos de dados, e por conseqüência, são utilizados muitos protocolos.

Para melhorar uma rede, de uma forma geral, existem várias possibilidades, como melhorar os equipamentos da estrutura, realizar tratamentos nas aplicações utilizadas para diminuir a quantidade do tráfego utilizado e também conscientizar as pessoas quanto à utilização e mau uso dos serviços e aplicações disponíveis.

Referente a estrutura física da TSA Química, um ponto considerado negativo e que tem influência direta na velocidade e desempenho da rede é a utilização de *hubs* para a comunicação de alguns pontos da rede. Seria muito importante a substituição dos mesmos por *switches*, evitando o tráfego por difusão e por conseqüência melhorando o desempenho da rede.

Em se tratando de tráfego de dados na rede, alguns controles são sugeridos para a empresa diminuir o tráfego da rede, aumentando assim a vazão, segurança e a produtividade da rede da TSA Química do Brasil.

Na empresa em questão, o maior responsável pelo consumo da banda de rede é o SGBD (Sistema de Gerenciamento de Bando de Dados) utilizado, que usa muito da banda da rede por meio do protocolo TNS, sendo este um tráfego produtivo, pois diz respeito aos principais programas utilizados pela empresa. Contudo, como o mesmo apresenta uma utilização muito grande, seria importante pesquisar se as últimas versões deste software poderiam estar trazendo benefícios à empresa, pois normalmente novas tecnologias otimizam recursos tanto de software quanto de hardware. Atualmente a empresa está trabalhando com a versão 9 e já está disponível a 11 do Oracle, que é o SGBD utilizado pela empresa. Talvez com uma atualização da versão do banco de dados utilizado, já se reduzisse significativamente o tráfego referente ao protocolo TNS.

Com base na análise das coletas da rede, observou-se em vários momentos a má utilização de alguns recursos, principalmente por meio dos protocolos HTTP e POP3, ou seja, utilização de acesso a Internet e e-mails sem fins produtivos para a empresa.

Na Tabela 3 são relacionados alguns sites que não condizem com o caráter produtivo da empresa.

Conforme se pode observar na Tabela 3, nas amostras coletadas, se pôde observar que alguns usuários estão utilizando a rede/internet para fins de entretenimento ou consultas pessoais. Uma situação evidente encontrada na rede foi a utilização de várias rádios on-line. Este tipo de acesso pode acabar prejudicando toda a rede da empresa, além de comprometer outros serviços, como o de e-mail por exemplo, que está totalmente ligado ao link de Internet da empresa, além de desviar o funcionário de seus devidos afazeres.

O que ocorre na TSA Química vem a ser o que ocorre em muitas organizações, onde não se realiza o controle adequado dos recursos que são disponibilizados aos seus colaboradores.

Tabela 3. Algumas páginas acessadas no ambiente TSA

PAGINAS	IP Origem
www.terra.com.br	10.1.4.24
www.atribunanet.com.br	10.1.4.10
www.guarani.com.br	10.1.4.24
www.sommaiorpremium.com.br	10.1.4.24
www.globo.com	10.1.4.23
web.infomoney.com.br	10.1.4.49
www.89fm.com.br	10.1.4.24
www.americanas.com.br	10.1.4.24
www.morenafm.com.br	10.1.4.24
www.jovempanfm.com.br	10.1.4.24
www.antena1criciuma.com.br	10.1.4.24
www.97fm.com.br	10.1.4.24
www.radio.usp.br	10.1.4.24
afavorita.com.br	10.1.4.228
www.style.com	10.1.4.49
www.superfm.com.br	10.1.4.24
www.opovo.com.br	10.1.4.26
www.recifefm.com.br	10.1.4.26
www.pedradailha.com.br	10.1.4.53
www.verdinha.com.br	10.1.4.26
www.concursos.correioweb.com.br	10.1.4.26
www.fm93.com.br	10.1.4.26
www.submarino.com.br	10.1.4.24
www.tvdiario.tv.com.br	10.1.4.26
terratv.terra.com.br	10.1.4.22
www.jornaldepiracicaba.com.br	10.1.4.26
www.livrariasaraiva.com.br	10.1.4.22

Sugere-se a empresa que crie filtros capazes de refinar o acesso, bloqueando as páginas mais acessadas. Seria interessante a implantação de um sistema de possibilitasse a criação de níveis de acesso, pois desta forma poderia ser definida uma política de acesso, por setor ou usuário.

A forma atual permite que usuários acessem várias páginas com conteúdo impróprio contrariando a política da empresa. Outra opção seria criar processo que enviasse aos coordenadores da empresa relatórios com os acessos dos seus subordinados, pois inibiria o acesso indevido e aumentaria o controle sobre os mesmos.

Quanto aos e-mails foi observado que alguns possuem em sua estrutura vários pacotes, referentes a grandes anexos, que muitas vezes são arquivos que não contribuem em nada para a empresa.

Para a questão dos e-mails também seria interessante aumentar o controle sobre os mesmos, criando filtros para os anexos, tratando suas extensões e também o tamanho total do e-mail.

O tráfego de e-mails e de Internet indevidamente além de prejudicar a rede pelo consumo de banda de rede e link de Internet, influencia na produtividade do funcionário que gasta seu tempo em algo sem agregação nenhuma para a organização e abre lacunas para entrada de vírus e outras ameaças provenientes da Internet, fazendo com que investimentos para essa questão sejam tratados com extrema importância.

Independente da implantação de ferramentas para controle de acessos, conforme mencionado é de extrema importância que todos os usuários da empresa sejam

conscientizados da má utilização dos recursos de que dispõem, pois este com certeza é quem vai ter o maior peso no que se refere à utilização e tráfego de rede da empresa.

CONCLUSÃO

Em ambientes organizacionais e corporativos, a busca pelo aprimoramento dos recursos utilizados e o aumento na qualidade dos bens e serviços oferecidos deve ser constante.

Um dos fatores que pode facilitar a busca pelo aprimoramento vem a ser o domínio e controle dos recursos já utilizados.

A temática deste trabalho surgiu com o intuito estudar e diagnosticar a rede da empresa TSA Química do Brasil LTDA, sob o ponto de vista do tráfego de dados. Para tal realização foi utilizada a ferramenta Wireshark, que juntamente com a técnica de amostragem estratificada para definição das coletas, proporcionou a geração de estatísticas da rede.

A análise destas coletas possibilitou o estudo do tráfego da rede da empresa e a identificação de algumas situações até então desconhecidas. Pode-se observar que na rede da empresa o responsável pela utilização da maior banda da rede é o banco de dados da mesma da empresa, porém outros recursos também têm demonstrado um consumo bastante elevado.

Observou-se vários casos onde tráfego gerado na rede por parte dos usuários não condiz com a política de trabalho da organização, ou seja, em algumas situações a rede é utilizada para fins de entretenimento e outros fins particulares, o que além de desviar a atenção dos colaboradores, influência de forma negativa na segurança e performance da rede da empresa.

Com base nas situações encontradas, sugestões foram elaboradas e documentadas, visando melhorar o desempenho da rede da empresa e aumentar o nível de segurança deste recurso para a organização.

A empresa TSA Química LTDA, pode verificar a importância deste trabalho por meio do diagnóstico gerado, sendo que o departamento de TI (Tecnologia da Informação) da empresa prontamente afirmou que a maioria das sugestões apontadas seriam verificadas e possivelmente aplicadas.

De forma geral, os objetivos propostos à realização deste trabalho foram alcançados, pois conhecimentos foram adquiridos conforme pesquisas realizadas sobre fundamentos teóricos, proporcionando o aprimoramento e 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.

Como sugestão para trabalhos futuros poderiam ser realizados estudos verificando a rede da empresa sob outros aspectos, como infra-estrutura, segurança, como também a verificação e análise do impacto da substituição dos hubs por switches, estudos de outros técnicas e procedimentos visando otimizar uma rede de computadores ou mesmo estudo e realização das coletas com a aplicação de outra técnica de amostragem.

REFERÊNCIAS

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

CARMONA, Tadeu. **Segredos da Espionagem Digital.** Diregati/ Universo dos Livros, 2006. 123p.

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. 695p.

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.

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

COMER, Douglas E. **Interligação em rede com TCP/IP**. Volume1: Princípios, Protocolos e Arquitetura. 5ª ed. Rio de Janeiro: Campus, 2006. 435p.

DIGERATI, Equipe. **Universo Hacker**. **Conheça os segredos do submundo hacker.** 2ª ed. Digerati Editorial, 2003. 96p.

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: Campus, 2000. 826 p.

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 de Redes através de Técnicas de Amostragem Estratificada**. SBRC 2005, Recife – PE, 2005, Maio 2005.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down.** 3 ed. **-** São Paulo: Editora Pearson Education do Brasil, 2006. 659p.

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.

ROSS, Julio. **Redes de Computadores.** 1 Ed. – Editora Antenna Edições Técnicas, 2008. 148 p.

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.

TANENBAUM, Andrew S. **Redes de computadores**. 4ª ed. Rio de Janeiro: Campus, 2003.

TROMBIN, Diordgenes. **Diagnóstico do Tráfego de Rede de Laboratórios de Informática. Estudo de caso: Universidade do Extremo Sul Catarinense.** Trabalho de Conclusão de Curso. Graduação, Universidade do Extremo Sul Catarinense. Criciúma, 2006.

ULBRICH, Henrique César; VALLE, James Della. **Universidade Hacker: Desvende todos os segredos do submundo dos hackers.** 5 ed. – São Paulo: Editora Digerati, 2004. 348p.

BIBLIOGRAFIA RECOMENDADA

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

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

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