

# Uma Metodologia Pragmática para Análise e Aplicação de Ferramentas de Gerência

Anilton Garcia, Edson Gimenez, Marconi Marques, Rafael Andrade

Instituto Nacional de Telecomunicações (INATEL) CEP 37540-000 - Santa Rita do Sapucaí - MG - Brasil

**Resumo:** Devido ao crescimento em dimensão e complexidade das redes de computadores, juntamente com a integração de serviços como voz, vídeo e dados, a gerência de desempenho aparece como sendo de vital importância para garantia de qualidade dos serviços prestados. Assim, torna-se necessário lançar mão de recursos computacionais que proporcionem um gerenciamento mais eficaz e preciso. A construção de uma metodologia pró-ativa de gerência de desempenho pressupõe a utilização de um conjunto de ferramentas capazes de possibilitar a monitoração, o controle e o planejamento de capacidade em ambientes de comunicação de dados. Buscando contribuir com este processo é proposta neste artigo uma metodologia pragmática para análise e aplicação de ferramentas de gerência de modo a auxiliar a tomada de decisão no tocante a que ferramentas devem ser adotadas tomando-se por base os serviços e aplicações suportados pela rede. Como forma de validação da metodologia proposta foi feito um estudo de caso que teve como foco a análise de tráfego do enlace Rede INATEL - Provedor de acesso Impsat.

**Palavras Chave:** Gerência de Desempenho, Qualidade dos Serviços, Ferramentas de Gerência, Análise de Tráfego.

## I. INTRODUÇÃO

As atuais redes de comunicação de dados são compostas de uma variedade de dispositivos que devem se intercomunicar e compartilhar recursos. Na maioria dos casos, a eficiência de diversos serviços prestados está associada ao bom desempenho da rede.

A prática da Gerência de Desempenho compreende três atividades básicas: monitoramento, controle e planejamento de capacidade. O monitoramento tem como função rastrear as atividades na rede, o controle tem como função fazer ajustes necessários para melhorar o desempenho da mesma e o planejamento de capacidade tem como função identificar os pontos de estrangulamento do sistema e apontar alternativas quanto a capacidade necessária para manter o bom funcionamento das aplicações/serviços suportados pela rede. Então, são algumas preocupações da Gerência de Desempenho:

- Qual o nível de utilização da capacidade total?
- Existe tráfego tratado de forma não eficiente?
- A vazão de tráfego tem alcançado níveis inaceitáveis?
- Existe algum "gargalo"?

- O tempo de resposta está aumentando?

Para tratar estas questões, o gerente de rede deve focar seu trabalho em um conjunto de recursos a serem monitorados para então fazer a estimativa de desempenho. Isso inclui associar métricas e valores que constituirão a formação de um cenário de referência (*baseline*), onde serão feitas análises que possibilitarão a caracterização do desempenho atual do ambiente. Contudo, para uma melhor eficiência do gerenciamento, é imprescindível a utilização de recursos computacionais que proporcionem um maior dinamismo e precisão no levantamento dos dados necessários à formatação dos diagnósticos que descrevem o estado atual da rede, bem como medidas a serem tomadas para melhoria do desempenho.

No intuito de contribuir para a implantação de uma gerência de desempenho pró-ativa é apresentada a análise de alguns *softwares* de gerência, onde são destacadas suas características e modo de operação. Indiretamente faz-se um comparativo entre *softwares free* e aqueles que necessitam de licença, confrontando seus pontos fortes e fracos.

O ambiente de testes foi o Laboratório de Comunicações Digitais do INATEL (LabII-1), que proporcionou a simulação de diferentes tipos de tráfego (dados, vídeo, áudio) para se ter uma visão mais consistente dos recursos de cada ferramenta. Foram analisados alguns parâmetros como eficiência de operação, características básicas e utilização da rede. Finalizando, realizou-se um estudo de caso baseado em uma metodologia pró-ativa de gerência de redes.

## II. PROCEDIMENTO PROPOSTO

Abaixo estão descritos os passos que compõem o procedimento proposto e que foram utilizados para análise das ferramentas. A principal preocupação é explorar ao máximo os recursos disponibilizados pelos *softwares*.

### 1. Obtenção do Produto

Cita a fonte de aquisição do *software*.

### 2. Configuração Mínima

Descrição de hardware e sistema operacional necessários.

### 3. Instalação

Este parâmetro apresenta o procedimento para instalação do programa, configurações necessárias e o grau de dificuldade apresentado na instalação.

#### 4. Eficiência de Operação

Descreve o *software* quanto as suas principais funcionalidades, ausência de um dado recurso e nível de dificuldade de operação.

#### 5. Consumo de Memória

Quantidade de memória consumida pelo programa na sua execução. Este parâmetro foi medido a partir do Gerenciador de Tarefas do Windows.

#### 6. Consumo de CPU

Consumo de processamento da CPU, medido a partir do programa em processo de captura de dados. Parâmetro também medido a partir do Gerenciador de Tarefas do Windows.

#### 7. Seleção da Interface de Captura

Descreve o procedimento de seleção da interface de rede a ser utilizada no processo de captura.

#### 8. Configuração de Agentes Remotos

Verificar a possibilidade de instalação de agentes remotos para coleta dos dados.

#### 9. Utilização da Rede

Este item tem como objetivo analisar a influência de utilização da rede pelo programa, caso utilize, pois o *overhead* gerado é um fator que pode levar a rejeição do mesmo. No caso específico de redes que possuem enlaces de baixa velocidade, este fator é de extrema importância. Esta influência vai ocorrer em programas que utilizem agentes externos, ou quando existir uma central de gerenciamento e for necessário fornecer informações dos agentes para esta central.

#### 10. Características Básicas

Descreve as características que proporcionam uma visão prévia da capacidade de operação do *software*.

#### 11. Captura de Dados

Descreve os procedimentos a serem seguidos no processo de captura de dados, bem como dificuldades encontradas durante a configuração desta tarefa.

#### 12. Configuração do Buffer no Processo de Captura

Descreve como configurar o tamanho do *buffer* a ser utilizado no processo de captura, caso exista esta opção.

### III. AMBIENTE DE TESTE

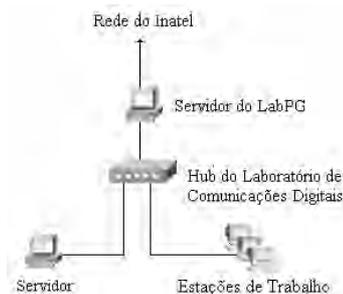


Figura 1 - Ambiente de Teste

O ambiente de teste foi o Laboratório de Comunicações Digitais que possui uma rede padrão Ethernet com velocidade de 10 Mbps. Esta consiste de 1 servidor, 16 estações de trabalho e 1 *hub*, conectado a um servidor do Laboratório de Pós Graduação (LabPG) que está atuando como roteador. As máquinas utilizadas para execução dos *softwares* possuem processadores Intel Pentium IV de 1,8 GHz, com 256 MB de RAM e HD de 20 GB. O sistema operacional utilizado é o Microsoft Windows 2000.

### IV. DESCRIÇÃO DA METODOLOGIA DE TESTE

A idéia básica utilizada para definir os testes consiste em estabelecer uma seqüência de passos a serem seguidos para se obter os resultados necessários a avaliação dos *softwares* de gerenciamento. A metodologia proposta é constituída de dois procedimentos básicos, que são descritos a seguir:

#### 1º Procedimento - Instalação e Operacionalidade

1. Obtenção do produto;
2. Analisar os requisitos de hardware que o fabricante diz como mínimo necessário;
3. Tempo de instalação;
4. Ocupação de disco;
5. Verificar se o mesmo encontra-se funcionando de maneira satisfatória.

#### 2º Procedimento - Análise das Características

Análise dos parâmetros descritos no item II (“*Procedimento Proposto*”)

### V. SOFTWARES ANALISADOS

Os programas analisados mostraram funções avançadas, embora algumas estivessem desativadas nas versões avaliadas. De uma maneira geral apresentaram características comuns, sendo semelhantes na forma de captura e visualização dos gráficos. A seguir serão apresentadas as características dos programas selecionados.

#### V.1 SNIFFER PRO 3.0

Se trata de uma ferramenta paga, produzida pela Network Associates Technology.

#### 1. Obtenção do Produto

Contato no Brasil: rua Geraldo Flausino Gomez 78, Cj. - 51 Brooklin Novo - São Paulo, SP - 04575-060, fone: (55 11) 5505 1009.

#### 2. Configuração Mínima

Sistema Operacional	Microsoft Windows 98, NT com Service Pack 3, 4, 5 e 6a, ou 2000 (apenas laptop). Microsoft Internet Explorer 5.01 com Microsoft Virtual Machine.
Acesso Internet	Acesso Internet Requerido
CPU	Pentium II 400MHz
Memória	128 MB RAM
Ocupação em Disco	32 MB.
Adaptador de Rede	Placa configurada com endereço IP e conectada à rede.

Tabela 1 - Configuração Mínima do Sniffer Pro

### 3. Instalação

O *software* não traz nenhuma complicação durante a instalação, bastando executar o arquivo de instalação e seguir as instruções. Uma das etapas será o registro do produto. O tempo médio de instalação é de 4 minutos.

### 4. Eficiência de Operação

Inicialmente o *software* apresenta-se com fácil entendimento das aplicações nele disponíveis. No entanto, no aprofundamento dos recursos oferecidos, há uma certa dificuldade para se ter uma interpretação precisa do que será executado, levando-se em consideração o primeiro contato com a ferramenta.

Detectou-se em certas funções a escassez de recursos que facilitam a atividade do administrador na rede. Como exemplo, tem-se a função de geração de pacotes onde a especificação dos endereços de origem e destino é feita diretamente no pacote, em base hexadecimal, o que poderia ser feito por meio de um recurso onde entraríamos com o endereço IP e a conversão seria automática. Foi identificado também a impossibilidade de agendamento simultâneo de *jobs*, ou seja, monitoramentos automáticos com início e término pré-configurados só podem ser realizados um por vez.

De um modo geral, o *software* se mostrou eficiente na monitoração e na coleta de informações do ambiente em que foram feitos os testes. Há uma disponibilidade de recursos que facilitam a geração de relatórios em diferentes formatos. Assim, o *Sniffer Pro* se mostrou uma ferramenta com grau satisfatório no levantamento de informações necessárias à administração de um ambiente de rede.

### 5. Consumo de Memória

A execução do programa consome aproximadamente 15 MB de memória RAM.

### 6. Consumo de CPU

Observa-se um consumo entre 1% e 3% com o programa em processo de captura.

### 7. Seleção da Interface de Captura

O *Sniffer Pro* possibilita a abertura de sessões independentes do programa, cada qual relacionada a uma placa de rede diferente. O processo de configuração para tal não impõe nenhuma dificuldade.

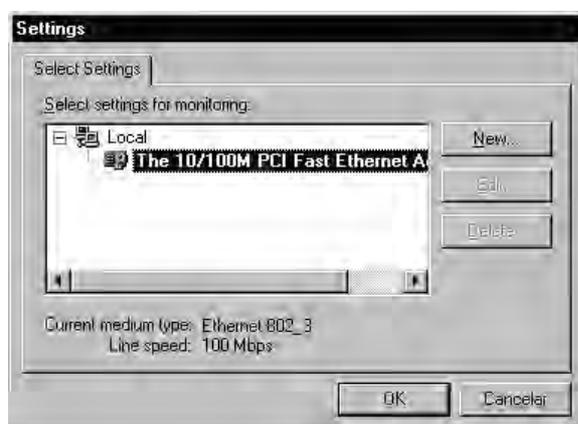


Figura 2 - Tela de Seleção da Interface de Captura

### 8. Configuração de Agentes Remotos

É possível ativar a captura de pacotes utilizando a placa de rede de um *host* remoto.

### 9. Utilização da Rede

Em se tratando de um *sniffer* não há utilização de recursos da rede monitorada, levando-se em consideração a não utilização de agentes remotos (ensaio não realizado devido a versão analisada não disponibilizar tal recurso).

### 10. Características Básicas

O *Sniffer Pro* se trata de uma ferramenta de gerência que possui as seguintes características básicas:

- Monitora as atividades da rede em tempo real;
- Coleta dados de utilização e estatística de erros para uma estação em particular ou conjunto de estações;
- Possibilita a montagem de um histórico contendo os dados até então analisados;
- Gera alarmes visíveis e audíveis (alarme configurado de acordo com a necessidade imposta);
- Notifica o administrador da rede quando problemas são detectados;
- Possibilita a captura de pacotes para uma análise mais detalhada;
- É dotado de funções como simulação de tráfego, medida de tempo de resposta, contagem de saltos e pesquisa de erros;
- É aplicável às tecnologias de rede *Ethernet*, *Fast Ethernet* (100BaseT), *Gigabit Ethernet*, *Token Ring* e *ATM*. São mais de 200 protocolos decodificados.

### 11. Captura dos Dados

A captura de pacotes é uma tarefa simples, melhor especificada na Figura 3. Esta possibilita o levantamento de medidas e realização de cálculos sobre o tráfego para uma análise mais minuciosa do desempenho atual da rede.

Depois de feita a captura é possível decodificar o pacote, obtendo-se assim, informações mais detalhadas sobre as transações que estão ocorrendo. Pode-se optar por configurar filtros para realização de uma captura mais específica, onde se seleciona quais estações de trabalho serão analisadas, bem como o tamanho e o tipo de pacote a ser capturado.

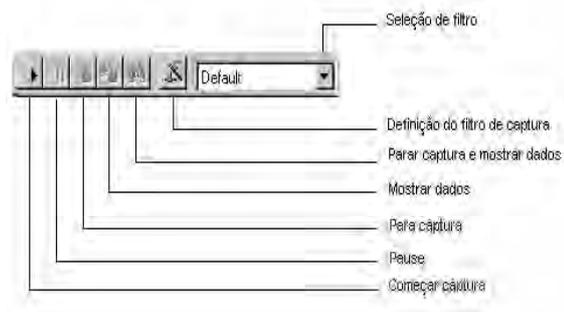


Figura 3 - Controles de captura de Pacotes

O *status* do processo é mostrado pelo painel de captura que possibilita a visualização da quantidade de pacotes capturados e a porcentagem preenchida do *buffer* de captura. Uma amostra mais detalhada dos dados pode ser obtida na opção *Detail*. Por fim, podemos configurar intervalos (disparos de captura) em horários e dias previamente definidos, porém não é possível configurar diferentes intervalos em um mesmo dia.

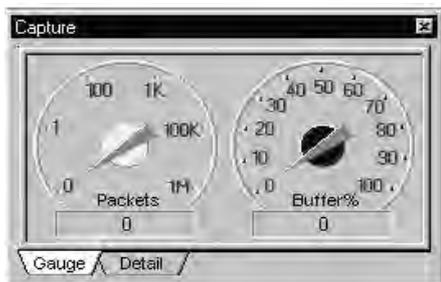


Figura 4 - Painel de Captura

12. Configuração do *Buffer* no Processo de Captura

O tamanho do *buffer* no processo de captura pode ser configurado de 256 KB a 192 MB, para o *Windows 98/2000*, e até 64 MB para o *Windows NT*. No entanto, para o *Windows NT*, apesar do *Sniffer Pro* ter a especificação de 192 MB, o tamanho máximo do *buffer* é de 64 MB. Assim, criando-se um filtro de 192 MB o processo de captura acarretará em falha.

V.2 ETHEREAL 0.9.4

1. Obtenção do Produto

O *Ethereal* é um *software free* disponível para *download* no endereço <http://www.ethereal.com/download.html>.

2. Configuração Mínima

Sistema Operacional	AIX, BeOS, Caldera (SCO), Debian GNU/Linux, FreeBSD, Gentoo, HP, Tru64 Unix, HP-UX, Irix, LinuxPPC, Linux Mandrake, MacOS X, NetBSD, OpenBSD, Red Hat Linux, s/390 (Linux), Solaris/Intel, Solaris/SPARC, Slackware Linux, SuSE Linux, Microsoft Windows 95/98/ME ou Windows NT 4/2000/XP.
CPU	Informação não disponibilizada na página do <i>software</i> .
Memória	Informação não disponibilizada na página do <i>software</i> .
Ocupação em Disco	Aproximadamente 20 MB.
Adaptador de Rede	Placa configurada com endereço IP e conectada à rede.

Tabela 2 - Configuração Mínima do Ethereal 0.9.4

3. Instalação

O *Software* não traz nenhuma complicação durante a instalação, bastando executar o arquivo de instalação e seguir as instruções. No *Windows 95/98/ME/NT/2000/XP* para efetuar a captura de pacotes será necessário instalar o driver de captura

Winpcap disponível para *download* na página: <http://winpcap.polito.it/install/default.htm>.

O tempo total de instalação é de aproximadamente 1 minuto.

4. Eficiência de Operação

O programa apresentado possibilita a prática de *sniffing* através de comandos e configurações de fácil entendimento. No entanto, existem algumas exceções que exigem maior conhecimento por parte do administrador de rede. Observa-se uma deficiência no que se diz respeito a interface gráfica do *software*. Há gráficos, como por exemplo o de *throughput* do segmento, onde se tem uma difícil interpretação dos pontos plotados. Um detalhe importante é que o *Ethereal* possui o código fonte aberto, permitindo sua implementação e adaptação de acordo com a necessidade do ambiente.

De maneira geral, o *Ethereal* é uma ferramenta simples, mas que possui funcionalidades bem aplicáveis à coleta de dados em uma rede.

5. Consumo de Memória

A execução do programa consome aproximadamente 6 MB de memória RAM.

6. Consumo de CPU

Observa-se um consumo entre 4% e 8% com o programa em processo de captura, o que pode ser considerado razoavelmente baixo.

7. Seleção da Interface de Captura

O *Ethereal* possibilita a abertura de sessões independentes do programa, cada qual relacionada a uma placa de rede diferente. O processo de configuração para tal não impõe nenhuma dificuldade.

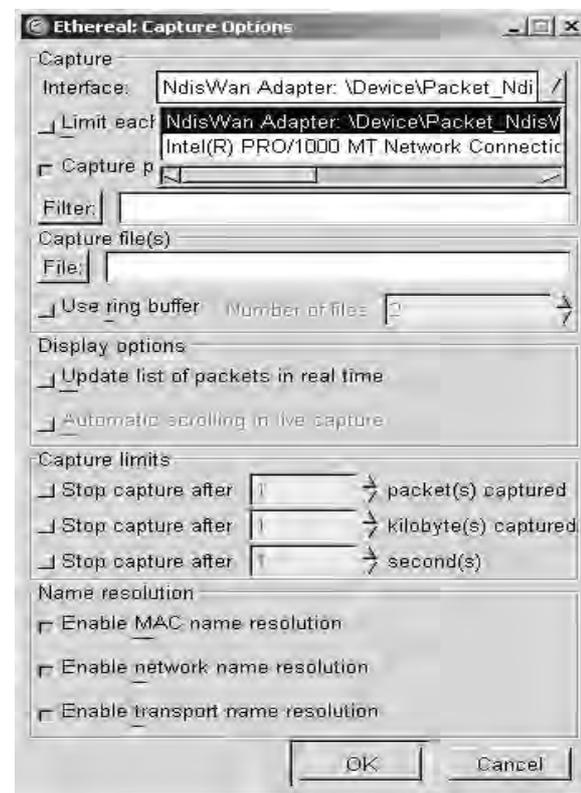


Figura 5 - Opções de Captura de Pacotes

### 8. Configuração de Agentes Remotos

O *Ethereal* não possibilita a captura de pacotes utilizando agente remotos.

### 9. Utilização da Rede

Por ser um *sniffer* e não possuir suporte a agentes remotos, não gera nenhum tráfego adicional ao segmento de rede.

### 10. Características Básicas

O *Ethereal* se trata de um *sniffer* onde se encontram presentes as seguintes características:

- Possibilita a captura de pacotes em um dado ambiente com atividades em tempo real;
- Possui o recurso de filtro de captura, onde se particulariza o dado (tipo de protocolo, tamanho de pacote, etc) que se deseja capturar para posterior análise;
- Possui recursos estatísticos onde pode ser levantando, por exemplo, porcentagem de utilização de um certo protocolo, média de pacotes por segundo no segmento analisado, intervalo entre o primeiro pacote e o último pacote capturado, tráfego em bytes e média de bytes por segundo.
- É possível visualizar o conteúdo de um pacote em particular fazendo uso da ferramenta *Follow TCP Stream* no menu *Tools*, onde se seleciona a formatação dos dados (ASCII, EBCDIC, Hexa) e assim tem-se a decodificação do conteúdo;
- Possui suporte para uma grande variedade de protocolos, o que amplia sua capacidade de aplicação em diferentes tecnologias de rede.

### 11. Captura dos Dados

O processo de captura de pacotes no *Ethereal* baseia-se em configurações como seleção da interface de rede, seleção do filtro e do arquivo onde serão gravados os dados coletados, além das opções de exibição, limite de captura e resolução de nomes. Tais operações podem ser efetuadas de maneira simples e clara através da tela de captura já apresentada anteriormente na Figura 5.

### 12. Configuração do *Buffer* no Processo de Captura

O *software* não possui nenhuma configuração específica para determinação do tamanho do *buffer*.

## V.3 ANALYZER 2.2

### 1. Obtenção do Produto

O *Analyzer* é um *software free* disponível para *download* no endereço <http://analyzer.polito.it/install/default.htm>.

### 2. Configuração Mínima

Sistema Operacional	Ambientes Windows 32 Bits
CPU	Não disponível.
Memória	Não disponível.
Ocupação em Disco	4 MB.
Adaptador de Rede	Placa configurada com endereço IP e conectada à rede.

Tabela 3 - Configuração Mínima do Analyzer 2.2

### 3. Instalação

O *Software* não necessita ser instalado. O arquivo adquirido na página informada é de auto-extração, bastando executá-lo e em seguida informar o local onde o mesmo será descomprimido. Neste local será criada uma pasta que se encontra o arquivo "*Analyzer.exe*". No *Windows*, para efetuar a captura de pacotes, será necessário instalar o driver de captura *Winpcap* disponível para *download* na página: <http://winpcap.polito.it/install/default.htm>. O tempo total de instalação é de aproximadamente 1 minuto.

### 4. Eficiência de Operação

O *software Analyzer* se trata de um *sniffer* que possui uma diversidade de aplicações bastante funcionais à prática da gerência de redes no que se diz respeito a recursos de coleta de dados e monitoramento de aplicações em tempo real. Uma interface gráfica de fácil interação contribui para uma rápida aprendizagem de utilização do *software*, bem como para um tratamento mais dinâmico dos dados coletados.

Um recurso que chama a atenção é a possibilidade do monitoramento em tempo real, onde se pode avaliar o tráfego das camadas de enlace, rede, transporte e aplicação, selecionando-se um número de amostras e intervalo de atualização do gráfico que oferece as opções de visualização em bits, bytes e pacotes versus o tempo de monitoração. Um detalhe importante é que em um mesmo gráfico podemos habilitar a análise de diferentes dados, como exemplo, desde o tráfego total gerado pelos dispositivos de rede e aplicativos ao tráfego gerado por gerenciamento SNMP (*Simple Network Management Protocol*).

O processo de captura de pacotes possui funcionalidades que vai da configuração do *buffer* de captura, número de pacotes a serem coletados e horário a se realizar a captura, às definições de filtros de captura mais complexas. Na configuração de filtros são definidas as expressões com operações lógicas e aritméticas, parâmetros de um dado protocolo que se deseja analisar, o que exige um maior conhecimento do administrador da rede em relação aos protocolos das camadas monitoradas. Por fim, tem-se a opção por salvar os arquivos de captura em formato html ou txt.

Neste contexto, o *software* se mostra bastante versátil, visto que muitas aplicações que enriquecem o processo de captura e análise dos dados coletados ainda se encontram em fase de implementação.

### 5. Consumo de Memória

A carga do programa consome aproximadamente 2 MB de memória RAM.

### 6. Consumo de CPU

Observa-se um consumo de 2% a 5% com o programa em processo de captura, o que pode ser considerado razoavelmente baixo.

### 7. Seleção da Interface de Captura

Assim como os *softwares* anteriormente apresentados, o *Analyzer* também permite que mais de uma sessão do programa seja aberta possibilitando que a captura seja feita através de diferentes interfaces de

rede. A seleção da interface é simples e pode ser feita como mostra a Figura 6.

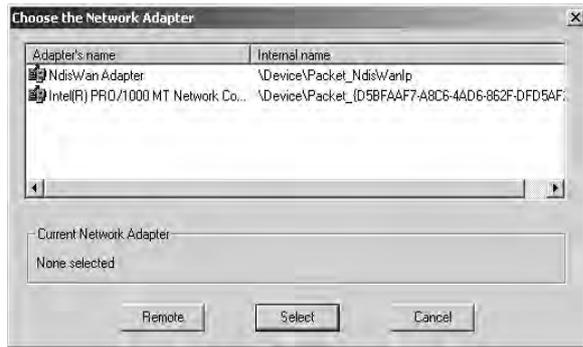


Figura 6 - Tela de Seleção de Interface de Captura

8. Configuração de Agentes Remotos

O *Analyzer* não possibilita a captura de pacotes utilizando agentes remotos.

9. Utilização da Rede

Por ser um *sniffer* e não possuir suporte a agentes remotos, não gera nenhum tráfego adicional ao segmento de rede.

10. Características Básicas

O *Analyzer* possui as seguintes características:

- Captura de pacotes e análise gráfica das atividades do ambiente gerenciado em tempo real;
- Dado um processo de captura, pode-se isolar de todos os pacotes capturados referentes a um dado protocolo, tamanho em bytes e outros parâmetros definidos por expressões aritméticas e lógicas;
- Levantamento de estatísticas MAC (*Medium Access Control*) como os quadros perdidos no *buffer*, quadros não transmitidos por excesso de colisão, número de quadros recebidos com erros e sem erros, velocidade do enlace, quadros transmitidos com sucesso após uma colisão, dentre outras;
- Pode-se analisar com bastante detalhe um dado pacote, tendo em vista o tamanho do quadro, *host* fonte e *host* destino, cabeçalho IP (*Internet Protocol*) e TCP (*Transmission Control Protocol*) e serviços NetBios.

11. Captura dos Dados

O processo de captura consiste em configurações que vão desde a seleção da interface de rede a ser usada na coleta dos dados à definição do filtro de captura. A seleção da interface de rede é um procedimento muito simples, bastando somente abrir a caixa de diálogo correspondente e selecionar o respectivo NIC (*Network Interface Card*), como ilustrado na Figura 7. Já a configuração do filtro em alguns pontos se torna um tanto complexo, já que dependendo da necessidade. Faz-se necessário a edição no bloco de notas. No entanto, para se analisar algum parâmetro das camadas de enlace, rede, transporte e aplicação é necessário somente selecionar a respectiva camada e o parâmetro de análise desejado.

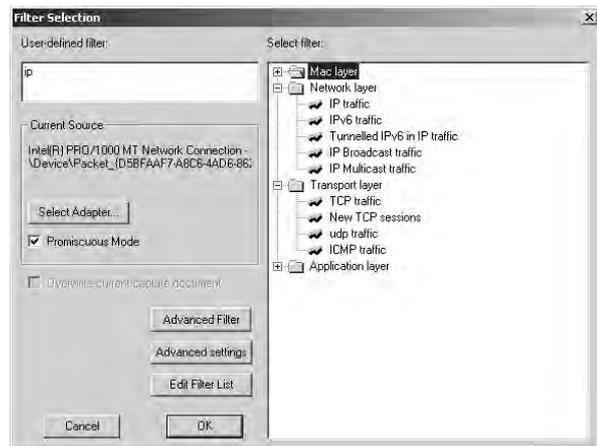


Figura 7 - Tela de Captura de Dados

12. Configuração do *Buffer* no Processo de Captura

Ao configurar o processo de captura, temos a opção de tamanho de *buffer* que pode ser definido entre os valores de 256 KB a 128 MB, como segue na figura a seguir.

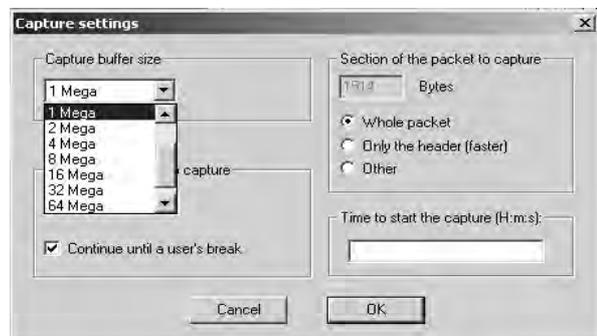


Figura 8 - Configuração do *Buffer*

V.4 NETBOY SUITE 2.0

O *NetBoy Suite 2.0* é um pacote de ferramentas de gerência pago, formado por três módulos: o *EtherBoy* que é um monitor da rede, o *PacketBoy* que desempenha o papel de um *sniffer* e o *WebBoy* otimizado para monitoramento de tráfego de Internet. A versão analisada é demonstrativa, mas fornece uma boa visão do que vem a ser realmente o programa completo.

1. Obtenção do Produto

O produto pode ser comprado através da página <http://www.ndgsoftware.com>.

2. Configuração Mínima

Sistema Operacional	Microsoft Windows 9x/Me/NT/2000.
Acesso Internet	Acesso Internet Requerido
CPU	Intel Pentium II 400MHz
Memória	128 MB RAM
Ocupação em Disco	Aproximadamente 15 MB.
Adaptador de Rede	Placa configurada com endereço IP e conectada à rede.

Tabela 4 - Configuração Mínima do *NetBoy Suite 2.0*

### 3. Instalação

Basta executar o arquivo de instalação e seguir as instruções. Uma destas será informar o número serial do produto. O tempo médio de instalação é de 1 minuto.

### 4. Eficiência de Operação

O *NetBoy Suite 2.0* é um pacote de *softwares* dotados de recursos gráficos interessantes que facilitam a visualização e entendimento dos recursos disponibilizados. Pelo fato da versão analisada ser demonstrativa, algumas funções possuem limitações de recursos. Como exemplo, citamos a limitação de 50 pacotes que o *PacketBoy* impõe na sua captura finalizando o processo quando essa quantidade é alcançada. Identificou-se também o problema de não haver possibilidade de agendamento de *jobs*.

Uma outra ferramenta do pacote, o *EtherBoy*, monitora a rede de maneira satisfatória e gera estatísticas e relatórios com dados importantes para a avaliação do ambiente. Podemos obter informações como o *hanking* dos *hosts* que geram e recebem mais tráfego, enlaces mais sobrecarregados, alarmes com maior ocorrência, etc.

Por fim temos o *WebBoy*, uma ferramenta otimizada para monitoramento do tráfego de Internet. Gera também estatísticas importantes, tais como: URLs (*Universal Resource Locator*) mais acessadas, computadores que mais acessam a *Web*, servidores de *Web* mais acessados, dentre outras.

O *NetBoy Suite 2.0* é um pacote cujos módulos proporcionam uma visão eficiente do ambiente em estudo possibilitando ao administrador, através dos dados coletados e estatísticas disponibilizadas, identificar possíveis problemas em seu ambiente de rede.

### 5. Consumo de Memória

*EtherBoy*: consumo de aproximadamente 5 MB com o programa em execução.

*PacketBoy*: consumo de aproximadamente 3 MB com o programa em execução.

*WebBoy*: consumo de aproximadamente 11 MB com o programa em execução.

### 6. Consumo de CPU

*EtherBoy*: consumo de aproximadamente 3%.

*PacketBoy*: consumo de aproximadamente 2%.

*WebBoy*: consumo de aproximadamente 4%.

### 7. Seleção da Interface de Captura

A seleção da interface de captura é feita da mesma forma nas três ferramentas do pacote, assim como mostrado na Figura 9.

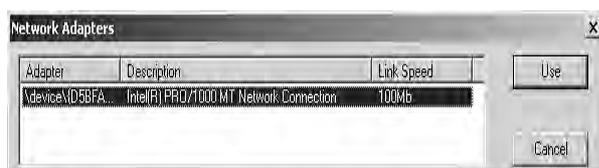


Figura 9 - Seleção da Interface nos Módulos do *NetBoySuite 2.0*

### 8. Configuração de Agentes Remotos

A NDG Software possui um agente remoto, o

*NetBoy Agent*, disponibilizado na versão *NetBoy Suite 3.0* que pode ser instalado e configurado para coleta de dados e monitoramento remoto. A versão analisada não possui tal módulo.

### 9. Utilização da Rede

Por ser um *sniffer* e não possuir suporte a agentes remotos, não gera nenhum tráfego adicional ao segmento de rede.

### 10. Características Básicas

O *NetBoy Suite* é formado por três ferramentas que possuem as seguintes características:

- Captura pacotes e monitora o tráfego da rede/Internet em tempo real;
- Gera alarmes audíveis ou com execução de um arquivo de extensão .exe.
- Possibilita a criação de filtros para captura de pacotes;
- Disponibiliza estatísticas como citadas anteriormente e criação de relatórios em formatos html e txt;
- Suporta grande quantidade de protocolos;
- As três ferramentas do pacote trabalham independentemente, mas possuem funcionalidades que podem ser agregadas a fim de tornar o trabalho do administrador mais eficiente.

### 11. Captura dos dados

A captura dos dados é feita pelo *PacketBoy* e consiste na seleção da *interface* a ser usada na coleta dos dados e definição do filtro a ser utilizado para tal. É possível também através da ferramenta *Trigger Builder* criar uma regra para disparar o início do processo de captura. A Figura 10 exibe a tela de configuração desta atividade.

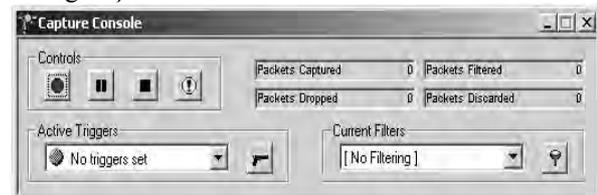


Figura 10 - Tela de Configuração do Processo de Captura no *PacketBoy*

### 12. Configuração do Buffer no Processo de Captura

O *software* não possui nenhuma configuração específica para determinação do tamanho do *buffer* para o processo de captura.

## V.5 MRTG (MULTI ROUTER TRAFFIC GRAPHER) 2.9.27

### 1. Obtenção do Produto

O MRTG é um *software free* para monitorar indicadores de desempenho de uma rede, podendo ser encontrado para *download* na página <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/pub>.

Para o seu funcionamento também é necessário a instalação do compilador ActivePerl, disponível para *download* na página <http://www.activestate.com>.

2. Configuração Mínima

Sistema Operacional	UNIX, Windows 95/98/ME/NT/2000, Linux, Mac OS X 10.1
CPU	Não disponível.
Memória	Não disponível.
Ocupação em Disco	MRTG 2.9.27: 3,86 MB. ActivePerl 5.8.0: 46,9 MB.
Adaptador de Rede	Placa configurada com endereço IP e conectada à rede.

Tabela 5 - Configuração Mínima do MRTG 2.9.27

3. Instalação

O *Software* MRTG não necessita ser instalado. O arquivo adquirido na página informada é de auto-extração, bastando executá-lo e em seguida informar o local onde o mesmo será descomprimido.

Apenas será necessário a criação de uma pasta para publicação das páginas com os gráficos gerados pelo programa. Para a instalação do ActivePerl basta executar o arquivo ActivePerl-5.8.0.805-MSWin32-x86 adquirido na página informada acima. O tempo total de instalação é de aproximadamente 2 minutos.

Após a instalação, deve-se relacionar os dispositivos a serem monitorados através da criação de um ou mais arquivos de configuração. Isto pode ser feito manualmente ou através da ferramenta *cfgmaker* pertencente ao pacote do MRTG. O tempo de configuração pode variar de acordo com a complexidade do monitoramento a ser realizado. A seguir é mostrado, como exemplo, uma parte de um arquivo de configuração responsável pelo monitoramento de tráfego do enlace INATEL - IMPSAT.

```
-----
Target[impsat]: 2:SnMp31971@200.186.136.129:
Options[impsat]:growright,bits
SetEnv[impsat]:MRTG_INT_IP="200.186.136.129"
MRTG_INT_DESCR="Serial0"
MaxBytes[impsat]: 128000
Title[impsat]: Análise de tráfego Inatel <-> Impsat
PageTop[impsat]: <H1>Análise de tráfego Inatel <-> Impsat</H1>
<TABLE>
<TR><TD>System:</TD>      <TD>Link      Inatel      <->
Impsat</TD></TR>
<TR><TD>Maintainer:</TD><TD>Seção de Redes e Internet</TD><
/TR>
<TR><TD>Description:</TD><TD>Serial0 </TD></TR>
<TR><TD>Max Speed:</TD> <TD>1 Mbps</TD></TR>
<TR><TD>Ip:</TD><TD>200.186.136.129</TD></TR></TABLE>
#-----
```

4. Eficiência de Operação

O MRTG é um Gerente SNMP (*Simple Network Management Protocol*) que permite a construção de páginas *Web* para a monitoração de sistemas. Acionado em intervalos regulares o *software* consulta as MIBs (*Management Information Base*) dos dispositivos monitorados para buscar os valores das variáveis de interesse, conforme especificados nos arquivos de configuração. De posse desses valores, ele gera gráficos contendo as curvas de evolução das

variáveis monitoradas. Quatro tipos de gráficos podem ser gerados para a mesma medida: diário, semanal, mensal e anual. Na Figura 11 é apresentado, como exemplo, um gráfico diário do tráfego no enlace INATEL - IMPSAT [<http://www.inatel.br/conexoes/trafejo/impsat.html>].

Análise de tráfego Inatel <-> Impsat

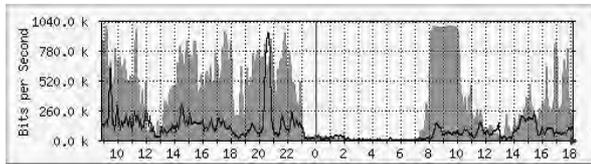


Gráfico 'Diário' (5 minutos - média)

Máx 1003.7 kb/s Média 368.5 kb/s Atual 159.6 kb/s  
 Ent: (98.0%) Ent: (36.0%) Ent: (15.6%)  
 Máx 941.5 kb/s Média 98.7 kb/s Atual 73.1 kb/s  
 Sai: (91.9%) Sai: (9.6%) Sai: (7.1%)

Figura 11 - Gráfico Diário do Tráfego no Enlace INATEL - IMPSAT

Esta ferramenta tem um uso bastante difundido para a Análise de Tráfego principalmente no meio acadêmico, por ser *free* e possuir funcionalidades importantes ao processo de monitoramento do ambiente.

A maior desvantagem observada, em comparação às ferramentas com interface gráfica, é que o processo de configuração e operação do *software* é feito através de linhas de comando, dificultando o manuseio para usuários com pouca experiência no MRTG.

5. Consumo de Memória

A carga do programa consome aproximadamente 100 KB de memória RAM.

6. Consumo de CPU

Observa-se um consumo médio baixo, próximo de 0, com picos entre 13% e 18% no processo de atualização.

7. Seleção da Interface de Captura

O MRTG, como mencionado anteriormente, atua como um Gerente SNMP, não realizando assim a captura de pacotes na rede.

8. Configuração de Agentes Remotos

A ferramenta em questão não possui agentes remotos próprios, bastando que os dispositivos que se deseja monitorar estejam com os respectivos Agentes SNMP ativos.

9. Utilização da Rede

A carga gerada com a utilização do *software* é relativamente baixa acarretando pequena utilização da rede. Este parâmetro dependerá diretamente da quantidade de variáveis monitoradas (respostas dos agentes) e do intervalo de *pooling* (requisições do gerente).

10. Características Básicas

O MRTG possui as seguintes características:

- Geração de resultados gráficos no formato html;
- Permite o monitoramento da utilização da CPU e do disco, estado do enlace físico de uma interface, utilização de memória, quantidade de pacotes e bits que entram e saem de uma interface;
- Gerenciamento baseado em método de *pooling* e utilizando o protocolo SNMP.

#### 11. Captura dos Dados

Por não ser uma ferramenta de prática de *sniffing*, o MRTG não realiza a captura dos dados na rede.

#### 12. Configuração do *Buffer* no Processo de Captura

Pelo mesmo motivo descrito no item anterior, não há configuração de *buffer* no *software*.

### VI. ANÁLISE COMPARATIVA

Dentre os parâmetros analisados, segue-se na tabela abaixo uma síntese do comparativo entre os *softwares* estudados. É importante ressaltar que todos os testes foram feitos em um ambiente de laboratório, onde se procurou, na medida do possível, retratar o comportamento de um ambiente real. Tal preocupação justifica-se pelo objetivo de extrair dos processos de avaliação resultados bem próximos da realidade e, também, uma melhor validação dos dados que foram levantados.

Observou-se nos *softwares* analisados recursos que são de grande valia na atividade de gerenciamento de redes de computadores. Em se tratando de um paralelo

entre as ferramentas gratuitas e as que possuem custo, percebe-se que é bastante relevante a caracterização do ambiente que será monitorado (quanto a complexidade), visto que podemos ser atendidos com satisfação pelos recursos de uma ferramenta gratuita.

Assim, para a tarefa de coleta de dados o *Analyzer* apresentou bastante eficiência e qualidade na interface gráfica, gerando arquivos em formato html ou txt. Além de oferecer a possibilidade de monitoramento em tempo real, onde podemos, no mesmo gráfico, monitorar diferentes tipos de tráfego (o que facilita comparações). Quanto ao *Ethereal*, há um destaque para a decodificação de pacotes capturados e o fato de possuir seu código aberto, o que favorece implementações de acordo com as necessidades que surgirem no gerenciamento de diferentes ambientes.

O *Sniffer Pro* apresenta-se como uma ferramenta de grande eficácia, pois além de destacar-se pela interface bastante amigável, possui a possibilidade de se montar um histórico contendo diversos parâmetros que são de grande importância na análise e levantamento de uma linha de base (dados de referência) do ambiente monitorado. Em relação aos *sniffers* descritos anteriormente, este se destaca pelos recursos de simulação de tráfego e integração com base de dados, o que evita trabalho adicional ao tratamento dos dados.

O *NetBoy Suite 2.0*, por se tratar de um pacote de *softwares*, possibilita um gerenciamento bastante amplo em recursos ao administrador, no entanto a coleta de dados mostra-se semelhante aos *sniffers* estudados.

Parâmetros	Sniffer Pro 3.0	Ethereal 0.9.4	Analyzer 2.2	NetBoySuite 2.0	MRTG 2.9.27
<b>Produto</b>	Pago	Gratuito	Gratuito	Pago	Gratuito
<b>Configuração mínima</b>	P-II 400 MHz, 128 MB RAM	Não disponível em manual	Não disponível em manual	P-II 400 MHz, 128 MB RAM	Não disponível em manual
<b>Instalação</b>	Simple	Simple	Simple	Simple	Complexa
<b>Eficiência de operação</b>	Satisfatório na coleta de dados	Satisfatório na coleta de dados	Satisfatório na coleta de dados	Satisfatório no monitoramento	Satisfatório na coleta das variáveis.
<b>Consumo de memória</b>	Médio	Baixo	Baixo	Médio	Baixo
<b>Consumo de CPU</b>	Baixo	Baixo	Baixo	Baixo	Baixo
<b>Seleção da interface de captura</b>	Simple	Simple	Simple	Simple	-
<b>Configuração de agentes remotos</b>	Recurso disponível	Recurso não disponível	Recurso não disponível	Recurso disponível (versão 3.0)	Recurso não disponível
<b>Utilização da rede</b>	Utiliza recursos c/ agente remoto	Não utiliza recursos da rede	Não utiliza recursos da rede	Utiliza recursos c/ agente remoto	Baixa
<b>Características básicas</b>	Eficaz conjunto de recursos	Eficaz conjunto de recursos	Eficaz conjunto de recursos	Eficaz conjunto de recursos	Eficaz conjunto de recursos
<b>Captura de dados</b>	Simple	Simple	Simple, exceto config. De filtros	Simple	-
<b>Configuração do buffer</b>	De 256 KB a 192 MB	Não disponível	De 256 KB a 128 MB	Não disponível	-

Tabela 6 - Análise Comparativa

Já o monitoramento apresenta recursos que enriquecem bastante o conjunto de dados coletados, pode se obter informações onde temos colocado em ordem crescente *hosts* que geram e recebem mais tráfego e enlaces mais sobrecarregados. Além da possibilidade de monitoramento do tráfego de *Internet*, recurso não disponível nas outras ferramentas.

Contudo, a questão de custo torna-se um parâmetro de grande importância, fazendo-se necessária uma análise cuidadosa dos indicadores de desempenho que serão monitoradas para assim, ser feita a escolha da ferramenta mais adequada à realidade do ambiente. Tomando-se por base as necessidades de gerência para os objetivos da rede, pode-se adotar uma solução baseada em ferramentas gratuitas eficazes, assim como pode ser necessário a combinação com ferramentas que dependem de licença para sua execução.

**VII. ESTUDO DE CASO**

Como estudo de caso foi monitorado o enlace de dados Rede INATEL - Provedor de Acesso Impsat, que caracteriza-se por possuir velocidade de transmissão de 1 MBps, modo full-duplex.

O critério adotado para a análise partiu de uma metodologia de gerência pró-ativa de desempenho [6]. Tal metodologia consiste em classificar os elementos que compõe um sistema distribuído em:

- Clientes;
- Facilidades de Comunicação;
- Provedores de Serviço.

Considerando a classificação acima, o presente trabalho foca-se ao grupo de facilidades de comunicação referenciando entre os indicadores de desempenho como erros físicos, tempo de resposta, colisões, dentre outros, a utilização da banda passante. Tais indicadores foram baseados nas obras de Jain [5], Bochanan [2] e Stallings [10], onde o padrão de qualidade definido para a utilização de banda passante consiste em:

- Menor do que 65% em redes sem disputa por meio físico;
- Menor do que 20% em redes com disputa pelo meio físico.

No instante em que se inicia a fase de coleta de dados, é importante definir a frequência de monitoramento e o período ou duração do monitoramento. Para efeitos práticos, recomenda-se usar uma frequência maior ou igual a 5 segundos e fazer o monitoramento nos períodos significativos do funcionamento dos sistema [6].

Baseado na Análise das Ferramentas acima se optou pelo uso do *software* MRTG, tendo em vista o estudo proposto. As variáveis coletadas no dispositivo gerenciado (roteador/interface serial) foram *ifInOctets* e *ifOutOctets*, fornecendo informações referentes ao tráfego de entrada e saída respectivamente.

Quanto ao período de coleta, foi feito um monitoramento durante uma semana ininterruptamente. Na Figura 12, é mostrado um exemplo de arquivo gerado pelo MRTG.

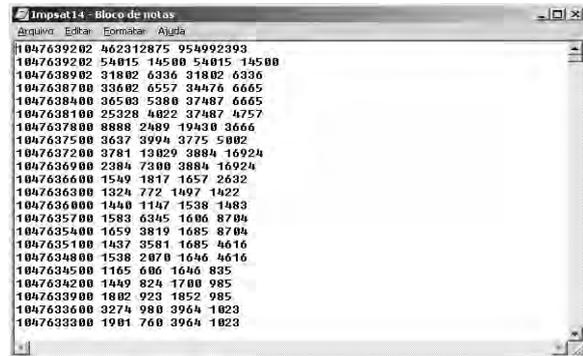


Figura 12 - Arquivo Gerado pelo MRTG

Observa-se que os dados coletados pela ferramenta não trazem informações prontas para análise, havendo assim a necessidade de um tratamento dos mesmos para que se possa obter informações úteis para o gerenciamento da rede. As Figuras 13 e 14 apresentam a visualização dos dados coletados após manipulação utilizando a Planilha Eletrônica EXCEL da *Microsoft Corporation*.

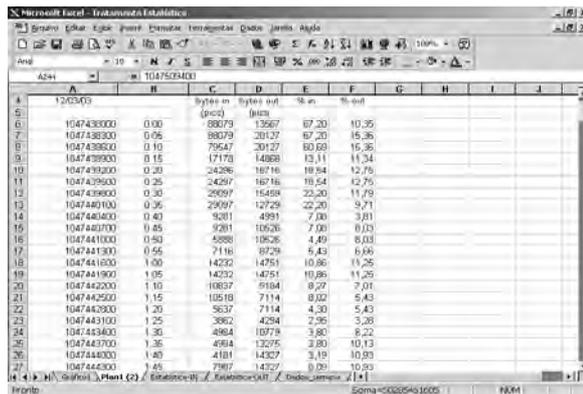


Figura 13 - Tratamento Estatístico dos Dados

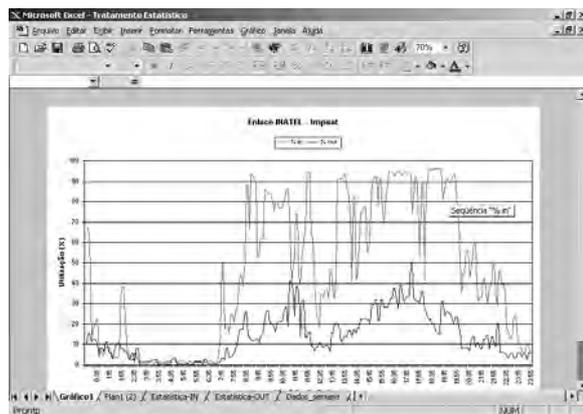


Figura 14 - Visualização Gráfica dos Dados

Para uma melhor interpretação das informações obtidas, foram calculados além da Média, o Desvio Padrão, que é uma medida do grau de dispersão dos valores em relação ao valor médio, e o Coeficiente de Variação, que indica quão grande é a variação dos

valores em relação à Média [1] a fim de se obter um resultado consistente de tal análise.

A seguir tem-se as estatísticas referentes ao período de coleta no enlace em estudo.

Enlace INATEL – Impsat Entrada			
Data	Média	DP	CV
07/mar	46,22933	35,68957	77,20114
08/mar	33,18685	32,11656	96,77496
09/mar	18,11061	19,38362	107,0291
10/mar	54,8206	40,877	74,56503
11/mar	54,06453	37,54872	69,45168
12/mar	54,41052	36,20466	66,53981
13/mar	64,51	36,55725	56,67245

Tabela 7 - Estatísticas de Entrada/Rede INATEL

Enlace INATEL - Impsat Saída			
Data	Média	DP	CV
07/mar	17,32821	18,98861	109,582
08/mar	11,24506	13,40402	119,1992
09/mar	7,273149	5,504341	75,68029
10/mar	15,83695	10,72667	67,73188
11/mar	16,37996	10,29511	62,85188
12/mar	17,88314	12,78698	71,50297
13/mar	19,77191	15,22978	77,02738

Tabela 8 - Estatísticas de Saída/Rede INATEL

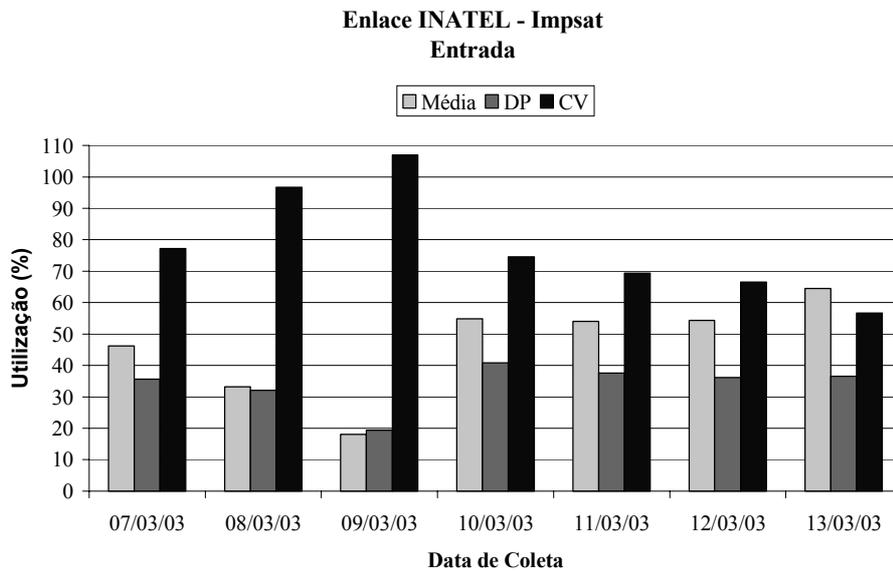


Figura 15 - Estatísticas de Entrada/Rede INATEL

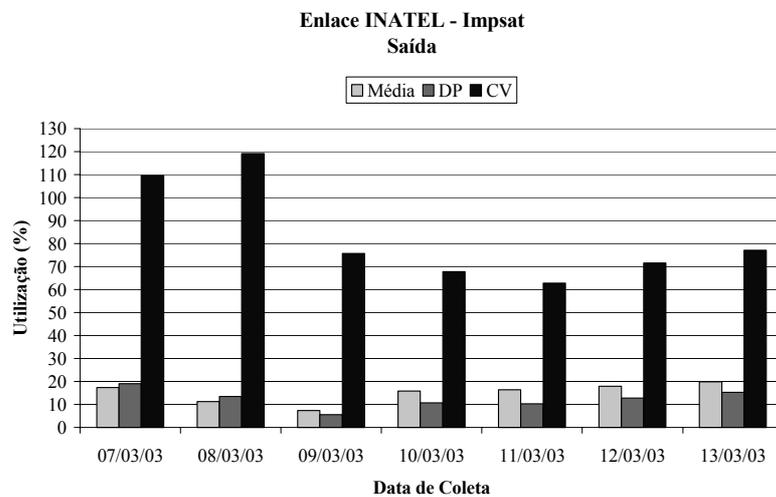


Figura 16 - Estatísticas de Saída/Rede INATEL

Para a medida de tráfego, coeficiente de variação com valor baixo indica uma utilização constate e com valor igual ao da média ao contrário de um coeficiente de variação com valor alto, que indica um tráfego em rajadas.

De acordo com o padrão de qualidade definido para o estudo da utilização do enlace de dados Rede INATEL - Provedor de Acesso Impsat, conclui-se através dos resultados:

- A utilização média encontra-se dentro do limite aceitável (< 65%);
- O tráfego não apresenta grandes variações entre os dias do período analisado caracterizando um comportamento uniforme;
- Os elevados valores do Coeficiente de Variação denunciam um mau comportamento da utilização média diária;
- Pela análise dos gráfico diários de utilização (ex.: Figura 14), observa-se que há uma concentração de altas taxas de utilização em determinados períodos do dia.

### VIII. CONCLUSÃO

Procurou-se com este trabalho retratar a cautela que o gerenciamento de redes de comunicação de dados exige quanto às funções que serão monitoradas e à escolha da ferramenta que melhor atende as necessidades do ambiente monitorado. Para tanto, foi utilizado o processo de análise dos *softwares* em questão para validar tal preocupação.

Notou-se que os recursos disponíveis nas ferramentas gratuitas podem atender com eficácia a execução das tarefas de monitoramento. Além de possibilitar, no caso do produto com código fonte aberto, implementações que proporcionam um melhor dinamismo na gerência de um ambiente em particular. Quanto às ferramentas que necessitam de licença notou-se características comuns às gratuitas, todavia a presença de recursos que facilitam, em muito, a atividade de um gerente de redes.

Com isso, fazendo-se uma análise consistente das reais necessidades do monitoramento de um dado ambiente, há a possibilidade de escolha de uma ferramenta que proporcionará a melhor relação custo x benefício. O que conseqüentemente favorece a uma gerência que evite gastos desnecessários e ao mesmo tempo possua um dinamismo satisfatório na atividade de gerenciar uma rede de comunicação de dados.

### IX. REFERÊNCIAS BIBLIOGRÁFICAS

- [1] DRAGO, Ádrian. **Uma Ferramenta Computacional para Auxílio na Prática da Gerência de Desempenho de Redes de Computadores**. Pós-graduação em Redes de Computadores, Vitória: UFES, junho 2001.
- [2] BOCHANAN, Robert W. **The Art of Testing Network Systems**. New York: John Wiley, 1996.
- [3] CARLESSO, Rogério. **Análise e Desempenho de Redes, o Estudo da Rede UFES**. Projeto de Graduação, Vitória: UFES, janeiro de 2000.
- [4] **EtherBoy, PacketBoy, and WebBoy User Manuals**. 1999 NDG Software, Inc. <http://ns3.ndgsoftware.com/Support/faqs/index.html>
- [5] JAIN, R. **The Art of Computer Systems Performance Analysis**. New York: Jhon Wiley, 1991.
- [6] MONTEIRO, Maxell E. **Metodologia para Gerência Proativa de Desempenho em Redes de Comunicação de Dados**. Dissertação Mestrado em Informática – Programa de Pós-graduação em Informática, Vitória: UFES, abril 2000.
- [7] PICCOLI, Rostan. **Uma Proposta de Metodologia para Avaliação de Desempenho em Redes de Computadores e Estudo de Caso no Redimensionamento da Rede UFES**. Pós-graduação em Redes de Computadores, Vitória: UFES, dezembro 1999.
- [8] SHARPE, Richard, Ed Warnicke. **Ethereal User's Guide V1.1 for Ethereal 0.8.19**. DocBook/SGML, <http://www.ethereal.com/download.html>.
- [9] **Sniffer Basic Getting Started Guide Release 4.5**. Manual provided by Network Associates.
- [10] STALLINGS, William. **SNMPv1, SNMPv2, SNMPv3 e RMON 1e 2**. 3<sup>a</sup> ed. Massachusetts: Addison Wesley, 1999.

**Prof. Dr. Anilton Salles Garcia** é Engenheiro pela Universidade Federal do Espírito Santo (UFES), graduado em 1976. É Mestre em Otimização e Pesquisa Operacional pela Universidade Estadual de Campinas (UNICAMP) em 1978 e Doutor em Engenharia Elétrica: Automação pela UNICAMP em 1987. Foi pesquisador por cinco anos do Projeto UNICAMP/CPqD – Redes Digitais e Engenheiro de Projeto Sênior por quatro anos da ELEBRA TELECOM Ltda, onde desenvolveu atividades de pesquisa, desenvolvimento e consultoria técnica especializada para empresas operadoras, nas áreas de Engenharia de Tráfego, Avaliação e Projeto de Sistemas de Comutação e Planejamento de Redes Telefônicas. Foi Consultor do Contrato UNICAMP/TELESP – Metodologia de Planejamento da Transmissão no desenvolvimento de modelos e ferramentas computacionais para o planejamento do enfeixamento (bundling) em redes SDH. É Professor Adjunto (Licenciado) da UFES e Professor do Mestrado em Telecomunicações do INATEL. As principais áreas de atuação incluem Modelagem, Otimização e Projeto de Redes SDH, Modelagem de tráfego e Avaliação de Desempenho de Redes, Análise e Projeto de Redes, Redes Multicamadas, Sistemas Distribuídos (CORBA), Redes Inteligentes e Arquiteturas de Gerência de Redes.  
E-mail: anilton@inatel.br

**Prof. Edson Josias Cruz Gimenez** é Engenheiro Eletricista pelo Instituto Nacional de Telecomunicações (INATEL), graduado em 1987. É Especialista em Informática Gerencial pela Faculdade de Administração e Informática em 1994 e Especialista em Educação Matemática pela Pontifícia Universidade Católica de Campinas (PUCCAMP) em 1997. Encontra-se em fase de conclusão de mestrado na área de Análise de Desempenho e Planejamento de Redes de Dados no INATEL. É Professor Titular do Departamento de Métodos Quantitativos, FAI, e Professor Adjunto do Departamento de Telecomunicações, INATEL.

E-mail: edsonjcg@inatel.br

**Rafael Carvalho Faria Andrade** é aluno do oitavo período de Engenharia Elétrica opção Eletrônica com ênfase em Telecomunicações pelo INATEL. É Técnico em Processamento de Dados formado pela

Fundação Educacional Montes Claros em dezembro de 1998. É integrante do Grupo de Pesquisa “Análise de Desempenho em Redes de Computadores e Avaliação de Ferramentas de Gerência”. Atualmente está desenvolvendo o projeto de Iniciação Científica “Sistema Multiagente para Gerência de Desempenho em Redes de Telecomunicações”.

E-mail: rafael-faria@inatel.br

**Marconi Dias Marques** é aluno do nono período de Engenharia Elétrica opção Eletrônica com ênfase em Telecomunicações pelo INATEL. É integrante do Grupo de Pesquisa “Análise de Desempenho em Redes de Computadores e Avaliação de Ferramentas de Gerência”. Atualmente está desenvolvendo o projeto de Iniciação Científica “Ferramenta Computacional para Auxílio na Prática da Gerência de Desempenho de Redes de Computadores”.

E-mail: marconi\_dias@inatel.br