**TIAGO MACIEL MELO**

# MONITORAMENTO DE REDES DE MÉDIO PORTE UTILIZANDO SOFTWARE LIVRE

**Estudo de caso na Prefeitura Municipal de São João do Sul/SC**

Palhoça
2007

**TIAGO MACIEL MELO**

# MONITORAMENTO DE REDES DE MÉDIO PORTE UTILIZANDO SOFTWARE LIVRE

**Estudo de caso na Prefeitura Municipal de São João do Sul/SC**

Monografia apresentada ao Curso de Especialização em Implantação de Software Livre como requisito à obtenção de Especialista em implantação de software livre.

Universidade do Sul de Santa Catarina

Orientador Prof º Luiz Otavio Botelho Lento

Palhoça
2007

## RESUMO

Esta monografia objetiva estudar a implantação de ferramentas livres para o gerenciamento de redes de computadores em redes de médio e pequeno porte. Este tipo de ferramenta é utilizado há vários anos em grandes redes de computadores para minimizar ao máximo falhas e maximizar desempenho. O impulso para a realização deste projeto foi a observação do contexto atual onde as ferramentas de gerenciamento de redes livres são amplamente utilizadas e consideradas essenciais em muitas organizações, mas por outro lado são desconhecidas por tantas outras. Para a realização da pesquisa, é analisado um estudo de caso na Prefeitura Municipal de São João do Sul/SC que possui uma rede de pequeno porte e que utiliza um servidor central de onde são enviados quantidade de dados considerável para várias estações de trabalho. Os primeiros capítulos mostram fundamentos teóricos sobre gerenciamento de redes, como, protocolo SNMP, MIBS e Agente e Gerente, em seguida são estudados ferramentas livres com a finalidade de gerenciar redes mostrando suas vantagens e desvantagens. Nesta etapa é selecionada uma ferramenta para teste no ambiente físico para por fim, mostrar resultados que justifiquem ou não a implantação deste tipo de ferramenta em pequenas redes.



Palavras-chave**:** Viabilidade, Gerência.

## ABSTRACT

This objective monograph to study to implant free tools for the management of computer networks in medium nets and small transport. This type of tool is used has some years in great computer networks to minimize to the maximum imperfections and to maximize performance. The impulse for the accomplishment of this project was the comment of the current context where the tools of management of free nets widely are used and considered essential in many organizations, but on the other hand is unknown for as much others. For the accomplishment of the research, a study of case in the Municipal City hall is analyzed of São João do Sul/SC that possesss a net of small transport and that it uses a central server of where considerable amount of data for some stations of work is sent. The first chapters show theoretical beddings on management of nets, as, protocol SNMP, MIBS and Agent and Manager, after that its advantages and disadvantages are studied free tools with the purpose to manage nets showing. In this stage a tool for test in the physical environment for finally is selected, to show resulted that they justify or not it implantation of this type of tool in small nets.



Keywords: Viability, Management


.

## LISTA DE ILUSTRAÇÕES

**SUMÁRIO**

# 1 INTRODUÇÃO

As redes de computadores estão presentes nos mais diversos setores. Nos dias de hoje, fica difícil imaginar uma empresa ou organização operando sem o compartilhamento de recursos e informações. Há alguns anos, os computadores eram utilizados isoladamente, operando de tal forma que um dispositivo não tivesse comunicação nenhuma com outro terminal.

Com a introdução da internet, as redes de computadores foram sendo implantadas rapidamente em vários setores, como comércio, indústria, ensino e ambientes de administração pública.

Muitas pessoas começaram a descobrir as vantagens de ter computadores interligados, como, por exemplo, o compartilhamento de arquivos e de alguns periféricos.

Com este crescimento, as redes ficaram cada vez mais importantes, sendo em alguns casos indispensáveis para o funcionamento de uma organização. Para controlar tudo isso, surgiu o conceito de gerencia de redes, que visa maximizar sua eficiência e produtividade.

Segundo Soares (1995, p. 434), a monitoração do tráfego, do estado e do desempenho de uma estação da rede, assim como a monitoração do meio de transmissão e de outros sinais, é necessária para o gerenciamento da rede, de forma a possibilitar a detecção de erros, diagnoses e resoluções de problemas, tais como, falhas, diminuição do desempenho etc.

A pesquisa vai abranger então o funcionamento e o comportamento do gerenciamento de redes de pequeno a médio porte com a utilização de ferramentas livres. Os maiores focos da pesquisa são observar como um ambiente de trabalho absorve uma ferramenta livre e se ferramentas de gerência de redes podem contribuir em pequenas redes ou se não traz nenhuma utilidade na organização.

Vai ser utilizado o protocolo de gerenciamento SNMP (Simple Network Management Protocol), mostrando pesquisa e resultados em um ambiente de trabalho.

## 1.1 Delimitação do tema

A viabilidade de implantação de ferramentas para o monitoramento de tráfego de redes baseadas em software livre na prefeitura municipal de São João do Sul/SC.

### 1.1.1 Tema

Ferramentas livres para o monitoramento de redes de computadores.

## 1.2 Problematização

É viável e vantajosa a implantação de ferramentas livres para o monitoramento de tráfego em redes de médio porte?

## 1.3 Objetivos

### 1.3.1 Objetivo geral

Analisar o comportamento de uma organização ao gerenciar uma rede de computadores de médio porte utilizado software livre.

### 1.3.2 Objetivos específicos

- Analisar ferramentas de gerenciamento de redes que melhor se enquadram para sua utilização em redes de médio porte.
- Analisar a viabilidade do uso de ferramentas de gerenciamento de redes em organizações pequenas.
- Identificar vantagens do uso de ferramentas de gerenciamento de redes.
- Identificar dificuldades encontradas por organizações de pequeno e médio porte na implantação de ferramentas de gerenciamento de redes tendo como estudo de caso a prefeitura municipal de São João do Sul.

## 1.4 Justificativa

As organizações públicas ou privadas detêm muitas vezes de redes de computadores de médio porte. Muitas dessas organizações sequer conhecem os mecanismos para gerenciar o tráfego em suas redes de computadores. A grande utilização dessas redes, onde dados importantes trafegam por seus mais variados dispositivos muitas vezes não recebem as atenções que poderiam ser tomadas. Uma dessas atenções diz respeito ao gerenciamento do tráfego de dados. Encontramos a necessidade então de uma análise mais aprofundada sobre as possibilidades de implantação destas ferramentas livres de monitoramento de tráfego nessas redes de médio porte.

Os resultados dessa análise servirão como parâmetro para verificáramos se existem vantagens ou não da implantação de ferramentas livres para o gerenciamento de redes de médio porte, representada aqui como estudo de caso pela prefeitura municipal de São João do Sul/SC.

## 1.5 Relevância da Gerência de Redes

O gerenciamento de redes foi no inicio de sua idealização, estimulada pela obrigação de monitorar e controlar o mundo de dispositivos que fazem parte das redes de comunicação.

Conforme a RNP (1997), atualmente as redes de computadores e os seus recursos associados, alem das aplicações distribuídas, tem se tornado fundamental e de tal importância para uma organização, que elas basicamente "não podem falhar".

Isto significa que o grau de erros e de degradação de desempenho considerados admissíveis esta cada vez menor, sendo este grau igual ate a zero, dependendo do valor da rede para uma organização.

# 2 GERENCIAMENTO DE REDES

O administrador de rede é a pessoa responsável pelo monitoramento da rede. Este monitoramento tem que ser feito ao nível de software e hardware, os quais fazem parte de uma rede. O trabalho do administrador é encontrar e corrigir falhas que impeçam que a rede funcione corretamente. Estas falhas podem ser de comunicação ineficiente ou inexistente.

Conforme Humberto (2004), os objetivos do gerenciamento são:

- Identificação e registro de problemas (Até antes de o usuário perceber);
- Determinação da causa (Quem são os culpados?);
- Registrar a ocorrência de eventos (Possíveis problemas?);
- Prevenir a ocorrência de falhas (Correlação de eventos);
- Controlar a utilização dos recursos da rede. Administrar a configuração da rede;
- Monitorar o desempenho da rede (Planejar seu crescimento);
- Gerenciar a segurança da rede;
- Definir pontos, elementos e parâmetros críticos para alarmes.

Pode-se dizer que a administração de rede é um pouco difícil por ser na maioria das vezes heterogênea, ou seja, na maior parte dos casos, os dispositivos ligados a ela são feitos por fabricantes diferentes.

As falhas que causam os maiores problemas, segundo Comer (1999, p. 435), são as mais fáceis de identificar. Um cabo de rede rompido ou um dispositivo sem alimentação, por exemplo, simplesmente pararão de enviar e receber pacotes. Estes exemplos são dados ao nível de hardware, mas podem ocorrer também falhas ao nível de software, por exemplo, rotas inválidas que, por conseqüência, podem causar perda de pacotes.

Desafios mais difíceis são falhas intermitentes ou parciais, por exemplo, roteadores que mandam pacotes erroneamente e em seguida outros corretamente. Para problemas dos mais variados tipos, existem algumas “armas” para detê-los, como o Checksun e o CRC, que são valores usados para ver se dados são alterados durante a transmissão. Mesmo assim, esta não é uma estratégia muito boa, pois as falhas escondidas prejudicam o desempenho da rede. O desempenho da rede cai, porque a retransmissão de pacotes é feita e isso usa largura de banda, que poderia ser usada para mandar outros dados.

Conforme Soares (1995, p. 419), para o administrador descobrir falhas e gerenciar a rede, estão a sua disposição os softwares de gerenciamento de redes. Estes softwares

permitem monitorar os dispositivos da rede através de interrogações e comandos feitos em uma linguagem especial.

Este sistema de gerenciamento é como um cliente-servidor, no qual a máquina do gerente é o cliente e os dispositivos são servidores. Para não haver confusão com aplicativos cliente-servidor que são usados por usuários, denota-se como cliente a máquina do administrador, sendo o gerente e o aplicativo da máquina gerenciada como agente.

Para a administração usam-se protocolos padrões de gerenciamento de redes, estes protocolos são usados para troca de mensagens entre o gerente e os agentes. O maior exemplo é o SNMP.

## 2.1 Gerência de Redes SNMP

Como explica o autor Harnedy (1997), *o Simple Network Management Protocol* (SNMP) é um protocolo da camada de aplicação lançado em 1988 e projetado para facilitar a troca de informação de gerência entre dispositivos da rede. Através do SNMP, são transportados dados informativos (tais como pacotes por taxas de segundo e de erro da rede).

Utiliza os serviços do protocolo de transporte UDP (User Datagram Protocol) para enviar suas mensagens através da rede. Com esse protocolo, os administradores controlam facilmente o desempenho da rede, encontram e resolvem problemas. Sua especificação está contida no RFC-1155 (Structure Of Management Information), RFC-1156 (Management Information Base) e RFC-1157 (Simples Network Management Protocol). Este protocolo é o centro do desenvolvimento do gerenciamento SNMP

Como *o Transmission Control Protocol* (TCP), o SNMP é um Internet Protocol.

Atualmente, existem três versões do SNMP: versão 1, versão 2 e versão 3. Na versão 2 do SNMP, procurou-se a correção de algumas deficiências da versão 1, melhorando a comunicação através da chamada Manager to Manager MIB. Já a versão 3 do SNMP tem como vantagens aspectos ligados à segurança.

Hoje, o SNMP é o protocolo mais utilizado para controlar redes comerciais de diversos tipos. O SNMP é um protocolo relativamente simples, contudo seu poder de gerenciamento é bastante poderoso, podendo controlar difíceis problemas apresentados em variados tipos de redes TCP/IP.

O SNMP, segundo Harnedy (1997), parte do esquema de gerenciamento OSI, onde os processos que implementam as funções de gerenciamento de Internet atuam como agentes ou gerentes. Esses agentes têm por função descobrir falhas ou problemas nos componentes da rede (Hosts, roteadores, gateways, etc...). Dessa forma, podem ser tomadas providências antes mesmo que o problema venha a acontecer, ou até mesmo saber como ou de onde surgiu o problema. Cada componente gerenciado é visto como uma coleção de variáveis, onde os valores podem ser lidos ou alterados. O gerente, então, envia comandos aos agentes, solicitando uma leitura no valor das variáveis dos componentes gerenciados, ou modificando seu valor. Na troca de informações entre o gerente e o agente, são aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede. Essa troca de mensagem entre gerente e agente é definida pelo protocolo SNMP, onde ele define o formato e a ordem que deve ser seguida à seqüência das informações de gerenciamento.

Para armazenar tais informações, são utilizados MIB (Management Information Base), onde são armazenadas as informações sobre o funcionamento dos Hosts, Roteadores e dos processos que executem os protocolos de comunicação (TCP. IP, ARP, etc...). Com o SNMP os gerentes de rede têm também a capacidade de modificar valores de uma variável de um objeto na MIB.

### 2.1.1 Agente e gerente

Comer (1999, p. 437) cita que o Agente é um processo executado em uma máquina gerenciada, sendo responsável pela manutenção das informações de gerência da máquina. Ele tem duas funções principais: atender as requisições enviadas pelo gerente e enviar automaticamente informações de gerenciamento ao gerente quando previamente programado.

Comer (1999, p. 437) diz ainda que o Gerente é um programa executado trabalhando em uma estação servidora, permitindo a obtenção e envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes. Ele é responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas, enquanto que o agente fica responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos específicos ao gerente.

“Resumindo, a gerência de redes que utiliza o protocolo SNMP consiste em quatro componentes principais: nós gerenciados, estações de gerenciamento, informações de gerenciamento e um protocolo de gerenciamento”. (SOARES, 1997, p. 419)

Estes componentes são vistos na figura 1:

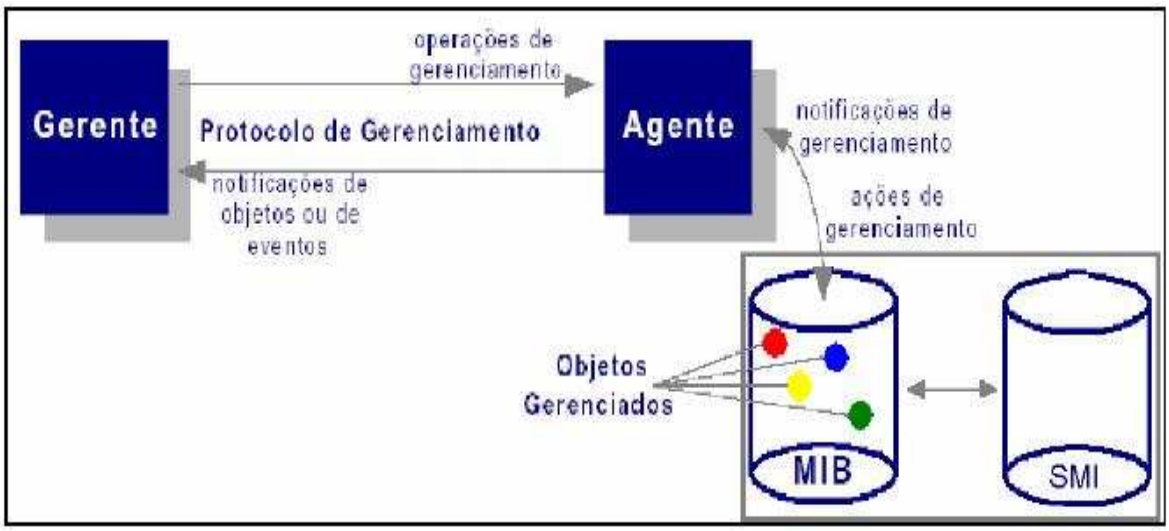



Figura 1 – Componentes do SNMP (Harnedy, 1997)

### 2.1.2 Management information base – MIB

Para Harnedy (1997), as MIBs, ou bases de informações de gerência, são compostas pelas informações de gerenciamento e pelos objetos gerenciados. Um objeto gerenciado é definido como a unidade da informação de gerenciamento. A comunicação e o processamento de dados são os recursos que podem ser gerenciáveis através da utilização de um protocolo. As informações de gerenciamento referentes aos objetos gerenciados residem na MIB. Ela define o conteúdo da informação que é transportada através do protocolo de gerenciamento.

Tradicionalmente, define-se uma MIB como um conjunto de objetos gerenciados. Estes objetos e suas instâncias são representados por variáveis. Às variáveis são atribuídas definições que informam exatamente quais serão seus atributos.

A *Management Information Base* do Agente é uma coleção de variáveis de interesse. Os grupos de variáveis da MIB que compreendem um particular módulo de informação de gerenciamento controlado pelo Agente são dependentes das funcionalidades do dispositivo e de quais recursos ou serviços o Agente deverá gerenciar. (HARNEDY, 1997)

### 2.1.3 Estrutura da MIB

A estrutura da informação de gerenciamento (SMI – Structure of Management Information) define as regras para a descrição da informação de gerenciamento. (SOARES, 1997).

O SMI atende às necessidades para que as variáveis que representam os objetos gerenciados da rede sejam adequadamente definidas. Sua estrutura é em forma de árvore, cuja função primária é definir os nomes das variáveis da MIB. Segundo Comer (1999, p. 438), cada objeto ao qual o SNMP tem acesso deve ser definido e determinado com um único nome. O SMI é definido utilizando a linguagem ASN.1 (Abstract Syntax Notation 1), permitindo que a MIB possa ser definida e categorizada de acordo com a estrutura hierárquica definida.

O ASN.1 atribui a cada objeto um prefixo longo que garante que o nome será único. Por exemplo, um inteiro que conta o número de datagramas IP que um dispositivo recebe tem o nome: iso.org.dod.internet.mgmt.mib.ip.ipInReceives. Quando o nome do objeto for representado em uma mensagem SNMP, em cada parte do nome é atribuído um inteiro. Deste modo cada variável tem sua identificação única ou OID (ObjectID). Por exemplo, em uma mensagem SNMP o nome ipInReceives é: 1.3.6.1.2.1.4.3.

A MIB foi definida primeiramente em oito grupos de objetos, logo depois, com o lançamento da MIBII, foram incorporados mais dois grupos. Os grupos que constituem a MIB são: System, Interfaces, Adrdress translation, IP, ICPM, TCP, UDP, EGP, Transmission, SNMP.

Cada um destes grupos define operações e novos grupos. Por exemplo: o grupo System descreve o hardware e o sistema operacional da máquina gerenciada.

A estrutura de árvore da MIB pode ser visualizada na figura 2.

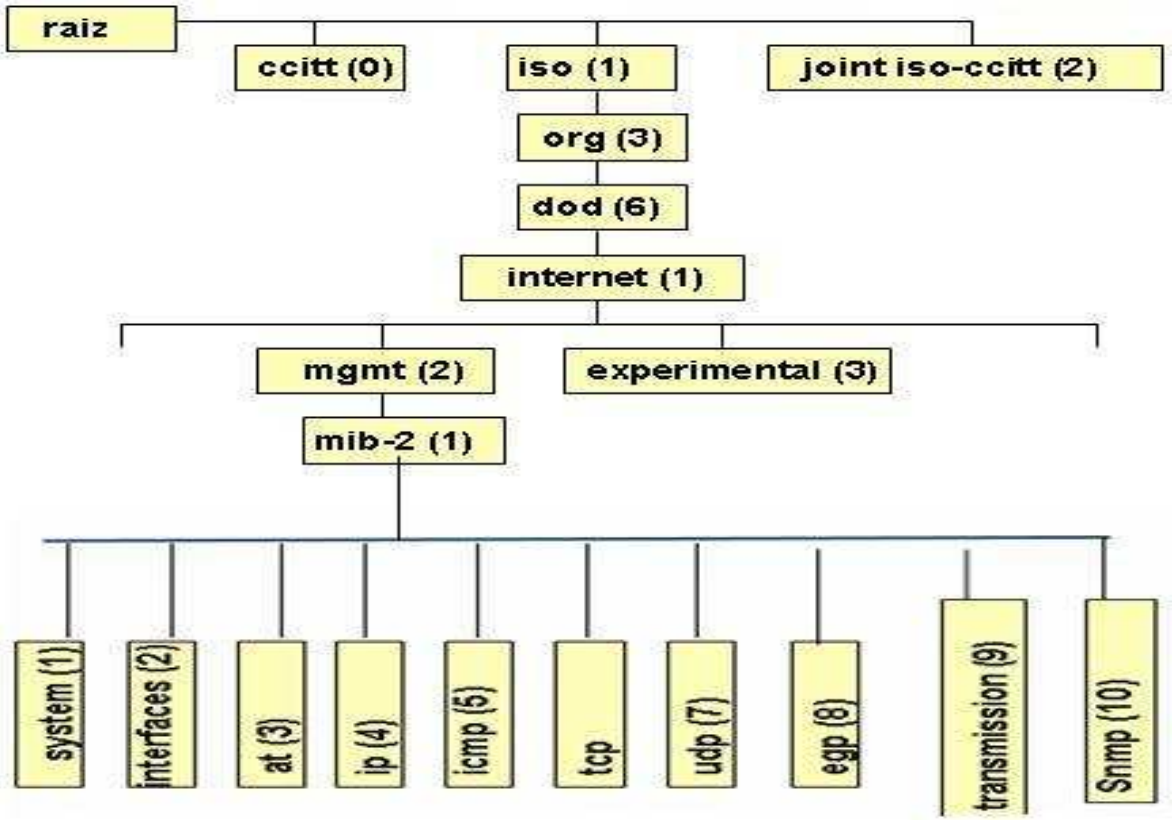



Figura 2 – Estrutura da MIB (Fonte: Soares, 1995)

### 2.1.4 Mibs disponíveis

Existem muitas MIBs disponíveis, algumas são padrões e outras criadas por fabricantes de determinados dispositivos. Por exemplo, encontra-se disponível a HOST-RESOURCES-MIB, que é a mib padrão para o gerenciamento de sistema em ambiente Windows. Neste caso, para ambiente Linux é empregada UCD-SNMP-MIB.

### 2.1.5 Operações do SNMP

Para obter informações de gerenciamento, o protocolo SNMP utiliza a troca de mensagens (fig. 2). Estas mensagens são compostas por um cabeçalho padrão e uma PDU (Protocol data Unit). O cabeçalho especifica a versão do SNMP e o nome da comunidade. O primeiro serve para que a troca de mensagens entre agentes e gerentes seja compatível, o nome da comunidade serve como um dispositivo de segurança, ou uma senha de acesso.

Quando um agente recebe uma solicitação do gerente, imediatamente será feita uma solicitação da comunidade. Se a comunidade for igual à definida pelo agente, o gerente terá o acesso, caso contrário, uma mensagem será retornada pelo agente iniciando falha na autenticação.

| Versão | Comunidade | PDU |
|---|---|---|

Figura 3 – Mensagem SNMP (Fonte: Soares, 1995)

As PDUs definidas pelo SNMP, segundo Comer (1999, p. 410), são as seguintes:

- Get: Utilizada para requisitar um ou mais valores da MIB do sistema;
- Get-next: Recupera os valores seqüencialmente;
- Get-bulk (SNMPv2 e SNMPv3);
- Set: Atualiza valores de variáveis;
- Get-response: Retorna os resultados das PDUs get, get-next e set;
- Trap: Informação do agente sobre eventos e problemas;
- Notification (SNMPv2 e SNMPv3);
- Inform (SNMPv2 e SNMPv3);
- Report (SNMPv2 e SNMPv3).

## 2.2 Áreas da Gerência

A gerência de rede possui cinco áreas que segundo Muniz (1996), em ordem de importância são mostradas abaixo.

### 2.2.1 Gerência de configuração

O alvo da gerência de configuração é o de aceitar a elaboração, a introdução, a partida, a operação contínua, e a posterior suspensão dos serviços de interconexão entre os sistemas abertos, tendo então, o emprego de manutenção e monitoração da estrutura física e

lógica de uma rede, abrangendo a averiguação da existência dos elementos, e a verificação da interconectividade entre estes elementos.

A gerência de configuração, logo, é correspondente a um conjunto de facilidades que permitem controlar os objetos gerenciados, identificá-los, coletar e disponibilizar dados sobre estes objetos para as funções de atribuir valores iniciais e fazer alterações aos parâmetros de um sistema aberto e iniciar e encerrar as operações dos objetos gerenciados.

### 2.2.2 Gerência de falhas

A gerência de falhas é responsável pela detecção, isolamento e conserto de falhas na rede. As informações que são coletadas sobre os vários recursos da rede podem ser usadas em conjunto com um mapa desta rede, para indicar quais elementos estão funcionando, quais estão em mau funcionamento, e quais não estão funcionando.

O ideal é que as falhas que possam vir a ocorrer em um sistema sejam detectadas antes que os efeitos significativos decorrentes desta falha sejam percebidos.

### 2.2.3 Gerência de desempenho

A gerência de desempenho faz o papel da monitoração de desempenho, da análise desse desempenho e planejamento de capacidade da rede.

O gerenciamento de desempenho é um conjunto de funções responsáveis pela manutenção e exame dos registros que contém o histórico dos estados de um sistema, com o objetivo de serem usados na análise das tendências do uso dos componentes, e para definir um planejamento do sistema através do dimensionamento dos recursos que devem ser alocados para o sistema, com o objetivo de atender aos requisitos dos usuários deste sistema, para satisfazer a demanda de seus usuários, ou seja, garantir que não ocorram insuficiências de recursos quando sua utilização se aproximar da capacidade total do sistema.

### 2.2.4 Gerência de segurança

Na gerência de segurança, a atenção está voltada pela proteção dos elementos da rede, monitorando e detectando violações da política de segurança estabelecida.

O objetivo do gerenciamento de segurança é o de dar subsídios à aplicação de políticas de segurança, que são os aspectos essências para que uma rede seja operada corretamente, protegendo os objetos gerenciados e o sistema de acessos indevidos de intrusos.

Deve providenciar um alarme ao gerente da rede sempre que se detectarem eventos relativos a segurança do sistema. Os mecanismos a serem adotados dependem do uso de uma política de segurança, que é feita pelo uso das funções de segurança do gerenciamento de redes.

### 2.2.5 Gerência de contabilidade

Responsável pela contabilização e verificação de limites da utilização de recursos da rede, com a divisão de contas feita por usuários ou grupos de usuários.

A gerência de contabilidade provê meios para se medir e coletar informações a respeito da utilização dos recursos e serviços de uma rede, para podermos saber qual a taxa de uso destes recursos, para garantir que os dados estejam sempre disponíveis quando forem necessários ao sistema de gerenciamento, ou durante a fase de coleta, ou em qualquer outra fase posterior a esta. Deve existir um padrão para obtenção e para a representação das informações de contabilização, e para permitir a interoperabilidade entre os serviços da rede.

# 3 FERRAMENTAS DE GERENCIAMENTO

Existe uma grande quantidade de ferramentas de gerenciamento, muitas são distribuídas gratuitamente e têm versões disponíveis para os mais variados sistemas operacionais. Algumas delas são descritas abaixo.

## 3.1 MRTG

Conforme as citações de Biasoto (2004), o Multi Router Traffic Grapher (MRTG) é uma ferramenta para monitorar a carga do tráfego nas ligações da rede. MRTG gera páginas em HTML que contêm as imagens do PNG que fornecem uma representação visual deste tráfego, seja ela na rede ou até mesmo em algum recurso de equipamentos ligada a rede. O MRTG trabalha na maioria dos casos em plataformas de Windows NT ou UNIX, sendo que a configuração e a instalação são muito simples, devido ao grupo de ferramentas de configuração.

Biasoto (2004) ainda diz que o MRTG mostra um gráfico diário detalhado do que está sendo analisado, criando assim representações visuais do tráfego visto durante os últimos sete dias, das últimas cinco semanas e dos últimos doze meses. Isto é possível porque o MRTG mantém um registro de todos os dados que pega na rede. Este registro é adquirido automaticamente, de modo que não cresça o tempo excedente, mas contem ainda todos os dados relevantes para todo o tráfego visto sobre os últimos dois anos. Ele é executado de maneira eficiente, podendo monitorar duzentas ou mais ligações da rede.

O MRTG não se limita a monitorar apenas o tráfego de uma rede. É possível monitorar toda a variável do SNMP. E possível mesmo usar um programa externo, recolhendo os dados que devem ser monitorados através do MRTG. Hoje, o MRTG está sendo muito usado para monitorar variáveis, tais como a carga de sistema, disponibilidade de sessões do início de uma sessão, modem, bridges e etc. No MRTG também é possível analisar mais de um tipo de dado no mesmo gráfico.

A figura 4 mostra um gráfico gerado pelo MRTG. O gráfico mostra o tráfego em uma porta de um switch. O intervalo em azul mostra o tráfego de entrada e o verde, o tráfego de saída.

Esta pesquisa utiliza este software para monitorar uma pequena rede no seu estudo de caso. A escolha do MRTG se deu por motivos de fácil instalação e configuração e por ser extremamente compatível com a proposta da pesquisa.

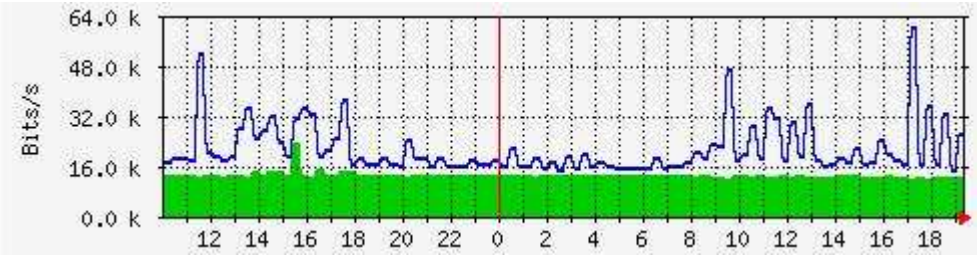



Figura 4 – Gráfico do MRTG (MRTG, 2004)

### 3.2 Whatsupgold

O WhatsUpGold é uma ferramenta de gerenciamento de rede muito eficaz. Monitora dispositivos e aplicações e mostra seus monitoramentos através de um browser, onde o administrador de rede pode corrigir e até mesmo prever algum problema possível na rede. (WHATSUPGOLD, 2004)

O WhatsUpGold monitora a rede e fornece notificações em tempo real de qualquer problema ou falha encontrada, podendo também reiniciar automaticamente todo o serviço com falha sem nenhum esforço manual do gerente de rede. Um e-mail ou até mesmo uma notificação por telefone podem ser emitidos pelo WhatsUpGold quando um dispositivo, uma aplicação ou um serviço não está respondendo. Ele tem a capacidade de descobrir dispositivos em uma rede e após a descoberta passar a monitorar também esses dispositivos.

No momento ele está na sua versão 11 e reúne características fundamentais de uma aplicação sólida em ambiente Windows e um gerenciamento de rede fácil de utilizar.

### 3.3 Nagios

Nagios é uma ferramenta com rica característica de monitoramento de pacotes, com poder de fornecer informações atuais sobre o sistema ou do recurso utilizado por uma

rede inteira. Além disso, segundo a empresa 4LINUX (2004) o Nagios pode também ser configurado para emitir alerta e executar outras ações quando forem detectados problemas na rede. Sua versão atual estável é a 2.9.

### 3.4 Ethereal

Ethereal é uma ferramenta muito utilizada por profissionais de rede em todo mundo. Ela analisa protocolos de rede descobrindo possíveis problemas.

> É um analisador/monitor de rede para Unix (gráfico) (...). Permite examinar dados de uma rede em tempo real ou de um segmento específico captado e gravado em disco. Pode-se interativamente "navegar" pelos dados da captação, obter um sumário de observação e detalhes de cada pacote recebido/gravado. (...) Excelente para análise de problemas e diagnóstico. (ETHERREAL, 2004)

### 3.5 RRDTOOL

RRD é a sigla para Round Robin Database. O RRD é um sistema para armazenar e mostrar dados em série obtidos em um determinado período de tempo (banda de rede, temperatura da máquina, etc). Os dados são armazenados de maneira bastante compacta e não aumentam com o tempo (por isso que o banco é dito "circular"). O RRDTOOL também é capaz de gerar gráfico a partir desses dados. (RRDTOOL, 2004)

### 3.6 AdventNet Mib-Browser e Mg-Soft Mib-Browser

Estas ferramentas possibilitam realizar operações SNMP visualmente com uma interface amigável e de fácil compreensão. Primeiramente, carrega-se a MIB que contém a variável a ser gerenciada e depois se pode realizar as operações de que o SNMP dispõe.

Além disso, a MIB é mostrada no formato de árvore, o que facilita a navegação entre as variáveis desejadas.

A figura 5 mostra a interface do AdventNet Mib-Browser.

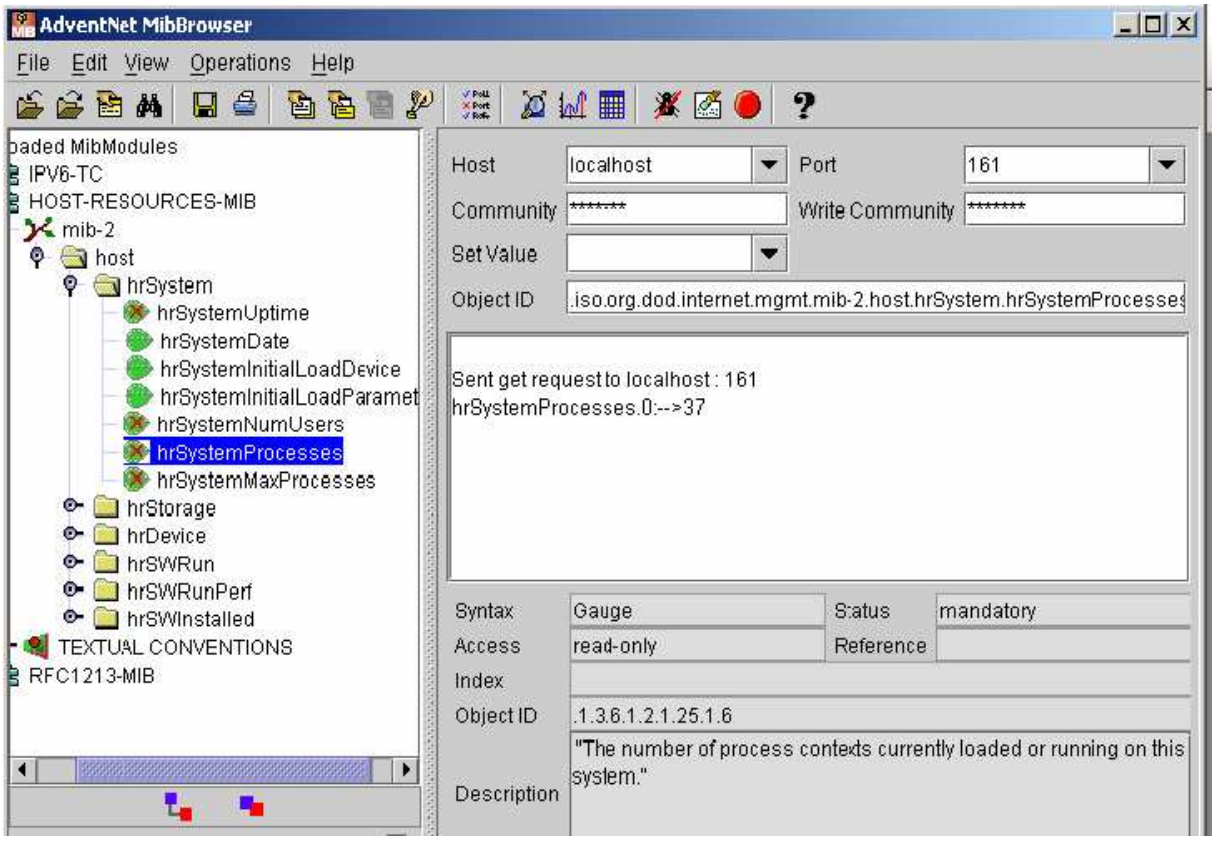



Figura 5 – Interface do AdventNet Mib-Browser (ADVENTENET, 2004)

# 4 AMBIENTE DE GERÊNCIA DE REDES

## 4.1 Origem e Objetivos

O modelo estrutural da rede analisada que segue a pesquisa "monitoramento de redes de médio porte utilizando software livre" é mostrado na figura 6. O projeto objetiva aprofundar conhecer o comportamento de organizações quando recebem a implantação de um software livre para a finalidade de gerenciar suas redes de computadores de pequeno ou médio porte.

Compõe o projeto: um estudo teórico, escolha de um software livre para implantação e testes, análise do comportamento de uma instituição no que diz respeito a área tecnológica e humana no ato da implantação do software livre, dando uma resposta para os objetivos do projeto.

A rede utilizada na Prefeitura Municipal de são João do Sul é composta por uma rede local com equipamentos em ambiente Windows. O principal alvo do gerenciamento é analisar o tráfego de informações enviadas e recebidas pelo servidor de banco de dados. O gerenciamento da rede utilizará o modelo de gerenciamento Internet, adotando a abordagem gerente/agente, onde os agentes mantêm informações sobre recursos e os gerentes requisitam essas informações aos agentes. Tem-se, então, o padrão Internet SMI (*Structure of Management Information*), que especifica uma metodologia para definição da informação de gerenciamento contida na MIB. A MIB define os elementos de gerenciamento de informação como variáveis e tabelas de variáveis.

O protocolo de gerenciamento utilizado é o SNMP. Esse protocolo de gerenciamento tem a função de garantir a comunicação entre os recursos ou dispositivos de redes homogêneas (dispositivos do mesmo fabricante) ou não. O SNMP é um mecanismo de gerenciamento de redes baseadas em TCP/IP e se associa ao esquema de MIB. Está sendo incluído no projeto por ter vantagens como simplicidade e facilidade de implementação.

Para se ter um gerenciamento ainda mais completo e detalhado, foi utilizado a ferramenta de gerenciamento de redes MRTG.

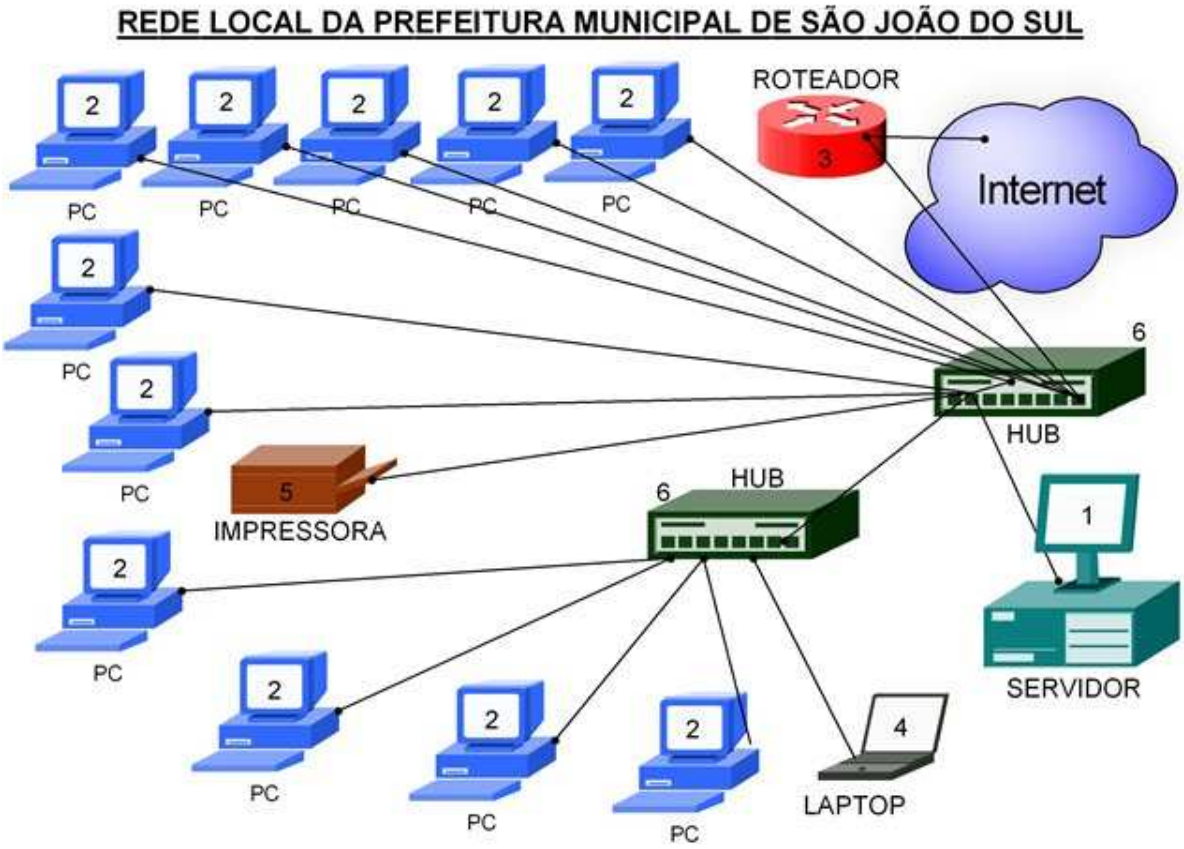



Figura 6 – Modelo Estrutural da rede

### 4.2 Enumeração dos Dispositivos

[1] Servidor Windows

[2] Clientes Windows

[3] Modem Roteador ADSL

[4] Cliente Windows (Laptop)

[5] Impressora Laser

[6] HUB

### 4.3 Ambiente Proposto Para Avaliação

A rede utilizada para a realização da pesquisa pode ser visualizada na figura 6. Como se pode ver, a rede foi composta por doze computadores desktops incluindo um laptop, impressora diretamente ligada a rede, um servidor de banco de dados, 2 hubs e 1 roteador de

internet ADSL. Destes desktops, sete se comunicam com mais assiduidade com o servidor, neles estão instalados sistemas de administração pública que operam com dados mantidos no computador principal (servidor). Neste estudo de caso, o servidor foi utilizado como gerente e configurado com o Sistema Operacional Microsoft Windows XP Professional. Este mesmo computador serviu também como agente e nele foi gerenciado o seu trafego de dados que entravam e saiam pela sua interface de rede.

Como no servidor, o sistema operacional utilizado pelos desktops também é o Microsof Windows XP Professional. Este Sistema Operacional tem suporte SNMP, bastando apenas instala-lo no painel de controle do SO.

## 4.4 Configurações e Resultados

Na máquina gerente, foi instalada a ferramenta de gerenciamento MRTG (Multi Router Traffic Grapher) versão 2.15.2. Os procedimentos para a instalação do MRTG no ambiente Windows, podem ser visualizados no Anexo A.

O MRTG é baseado na linguagem de programação Perl, sendo imprescindível sua instalação, neste projeto a versão do Perl utilizado foi a 5.8.8.820. Esta ferramenta é capaz de gerar gráficos das estatísticas da rede e publicá-los em formato html, sendo possível sua visualização por qualquer computador da rede, bastando apenas ter um navegador web. Para que isto ocorra, é necessário que o servidor web da máquina gerente esteja habilitado e configurado.

O servidor da rede, buscou informações de sua variável referente a entrada e saída de dados da sua interface de rede.

O Anexo B mostra como foi feito o gerenciamento deste computador e alguns gráficos gerados com o MRTG.

Depois disso, foi usado o MRTG para criar os gráficos em html. Para que ele gerasse o html, primeiramente criou-se um arquivo *.cfg, onde encontram-se as configurações das variáveis que seriam gerenciadas. Com um simples comando, o MRTG criou os arquivos html partindo do que estava no arquivo *.cfg.

Depois da pesquisa de softwares  que tem por finalidade de gerenciar redes e realizada a implantação de um destes na monitoração de um pequena rede de computadores, ficou constatado que a utilização de softwares livres nesta área de trabalho é muito ampla e

atualmente existe uma quantidade muito grande de softwares para gerencia de redes, sendo muitos deles livres.

Não restam dúvidas que a utilização de um software livre nesta área de trabalho é uma boa opção, já que a maioria tem suas versões estáveis e bem difundidas.

# 5 CONCLUSÃO

A conclusão tirada após a realização desse trabalho é que o gerenciamento de redes ainda não foi muito difundido em redes de pequeno porte. Logicamente, isto se da pela falta de conhecimento por parte responsáveis destas redes quanto à utilidade que a gerência pode lhes oferecer.

Mesmo assim, o trabalho foi de grande valia por ter aberto em discussão a utilização de software livre principalmente por se tratar dentro de um centro de administração publica, um dos focos dessa pesquisa.

A fase inicial da implantação do software para gerenciamento de redes, foi aceito muito bem e gerou desejos para a continuação da utilização do mesmo. Depois de algumas discussões, opiniões foram dadas para a utilização do MRTG na geração de gráficos sobre gerenciamento de todos os hosts da rede, gerenciamento de memória, disco, CPU, enfim, tudo para dar informações detalhadas e centralizadas com o objetivo de maior desempenho no funcionamento geral do ambiente de trabalho computacional da organização.

A escolha do MRTG se deu por satisfazer com suas características os propósitos do projeto, facilidade de implantação, configuração e por ser bem conceituado no ambiente de gerencia de redes.

Enfim, a pesquisa proposta teve muito valor e, como já foi citado, para que o software de licença pública e suas funcionalidades entrem de vez no mercado, o mesmo precisará de esforços dos mais variados campos de atividades, principalmente do meio acadêmico.

## 5.1 Dificuldades Encontradas

Durante a realização da pesquisa, algumas dificuldades foram encontradas. Dentre as mais destacadas, seguem ao fato do curso ser realizado a distancia. Portanto, a indisponibilidade de estar dentro de uma biblioteca frequentemente, o não acompanhamento pessoal quase que diário de orientador, colegas e professores e a falta do ambiente acadêmico foram os maiores empecilhos.

## 5.2 Pesquisas Futuras

A utilização de software livre nas mais variadas áreas de trabalho cresce a cada dia. Interesse em experimentos de software com licença publica são grandiosos e algumas vezes faltam apenas um pequeno auxílio para concretizá-los. Para que essas novas tecnologias entrem no mercado, muitas pesquisas têm que ser feitas. Isso está acontecendo neste momento com muitos softwares livres com enorme potencial para serem utilizados nas mais diversas tarefas.

Focando a implantação de softwares livres, estudos mais detalhados com programas utilizados por grande quantidade de usuários em uma única organização ainda é uma grande área a ser estudada e observada com atenção.

Outras interessantes pesquisas que podem ser feitas em prefeituras municipais giram em torno da implantação de alguns softwares livres com a finalidade administração pública, tendo em vista que estas organizações sofrem muito por terem que pagar altos valores relativos a licenças.

# REFERÊNCIAS

- ADVENTNET. **Ferramenta**. Disponível em: <www.adventnet.com>. Acesso em 06/2007.

- 4LINUX. **Nagios**. Disponível em: <http://www.4linux.com.br/consultoria/nagios>. Acesso em 06/2007.

- BIASOTO, Gilberto. **MRTG**. Disponível em: <http://www.networkdesigners.com.br/Colunas/mrtg/mrtg.html>. Acesso em 05/2007.

- COMER, Douglas E. **Redes de Computadores e Internet**. Volume II. Ed. Campus, 1999.

- COMER, Douglas E. **Interligação em rede com TCP/IP**. 3. ed. Rio de janeiro. Ed. Campus, 1999.

- ETHERREAL. **Ferramenta**. Disponível em: <http://www.linuxsecurity.com.br>. Acesso em 06/2007.

- HARNEDY, Sean. Total SNMP: **Exploring the Simple Netowrk Management Protocol**. 2 ed. Prentice Hall PTR, 1997.

- HUMBERTO. **Gerência**. Disponível em: <http://www.univale.br/servicos/downloads/detalhes/default.asp?idarquivador=3588>. Acesso em 06/2007.

- MRTG**. Multi Router Traffic Grapher**. Disponível em: <www.mrt.org>. acesso em 05/2007.

-RRDTOOL. **Ferramenta**. Disponível em: http://lyra.soueu.com.br/index.php/CursosPalestras/MedidaTrafegoRedeRRDTOOL>. Acesso em 06/07.

- SOARES, Luiz F. G. **Redes de computadores**, 2. ed. Rio de Janeiro. Ed. Campus, 1995.

- WHATSUPGOLD. **Whatsupgold**. Disponível em: <http://www.ipswitch.nl/international/portuguese/whatsupgold.html>. Acesso em 05/2007.

# ANEXOS

# ANEXO A – INSTALAÇÃO DO MRTG

A instalação do MRTG é consideravelmente simples. O pacote de instalação, tanto para o ambiente Linux como pra Windows, pode ser encontrado no site www.mrtg.org. Para o MRTG funcionar, é preciso também instalar o pacote de compilação da linguagem de programação Perl. Esta instalação pode ser adquirida do site www.activestate.com.

Na versão para Windows, para o MRTG funcionar, basta apenas descompactar o arquivo para uma pasta qualquer e depois disso instalar o Perl.

Para gerar os gráficos das estatísticas da rede, os comandos são iguais tanto para a versão Windows como para Linux.

Os comandos básicos para gerenciar a entrada e saída de bytes da interface de rede são os seguintes:

cfgmaker --global 'WorkDir: /home/httpd/mrtg'--global 'Options[_]: bits,growright' --output /home/mrtg/cfg/mrtg.cfg community@router.abc.xyz

Onde workdir informa o local onde o arquivo html ficará hospedado. A opção output informa o nome do arquivo de configuração *.cfg e em community deve-se colocar o nome da comunidade SNMP e logo após o  IP host da máquina gerenciada.

Para gerar o html a partir do arquivo *.cfg o comando utilizado é o seguinte:

perl mrtg mrtg.cfg

Maiores informações estão disponíveis no site www.mrtg.org.

# ANEXO B – GERÊNCIA SNMP COM MRTG

Para fazer o gerenciamento da rede e gerar os gráficos com o MRTG utiliza-se os comandos padrões do MRTG.

Ex: perl cfgmaker public@10.1.1.2 --global "WorkDir: c:\www\mrtg" --output mrtg.cfg

O comando acima gerou o arquivo de configuração do servidor, mrtg.cfg. Assim já é possível gerenciar a entrada e saída de bytes da interface de rede. Agora com o comando "**perl mrtg mrtg.cfg**" é gerado o gráfico em html.

Para conferir se realmente o arquivo .html foi gerado, basta olhar na pasta onde foi desejado hospedar o arquivo html. Esta opção está na seção Workdir do *.cfg.

O arquivo mrtg.cfg é descrito abaixo:

mrtg.cfg

```
# Created by
# cfgmaker public@192.168.0.36 --global "WorkDir: c:\www\mrtg" --output
mrtg.cfg
### Global Config Options
#  for UNIX
# WorkDir: /home/http/mrtg
#  or for NT
# WorkDir: c:\mrtgdata
### Global Defaults
#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits
EnableIPv6: no
RunAsDaemon: yes
######################################################################
# System: SCI
# Description: Hardware: x86 Family 15 Model 6 Stepping 4 AT/AT COMPATIBLE
- Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)
# Contact:
# Location:
######################################################################
### Interface 1 >> Descr: 'MS-TCP-Loopback-interface' | Name: '' | Ip:
'127.0.0.1' | Eth: '' ###
### The following interface is commented out because:
### * it is a Software Loopback interface
#
# Target[192.168.0.36_1]: 1:public@192.168.0.36:
# SetEnv[192.168.0.36_1]: MRTG_INT_IP="127.0.0.1" MRTG_INT_DESCR="MS-TCP-
Loopback-interface"
# MaxBytes[192.168.0.36_1]: 1250000
# Title[192.168.0.36_1]: Traffic Analysis for 1 -- SCI
# PageTop[192.168.0.36_1]: <h1>Traffic Analysis for 1 -- SCI</h1>
#           <div id="sysdetails">
#                <table>
#                     <tr>
#                          <td>System:</td>
#                          <td>SCI in </td>
```

```
#                         </tr>
#                         <tr>
#                               <td>Maintainer:</td>
#                               <td></td>
#                         </tr>
#                         <tr>
#                               <td>Description:</td>
#                               <td>MS-TCP-Loopback-interface  </td>
#                         </tr>
#                         <tr>
#                               <td>ifType:</td>
#                               <td>softwareLoopback (24)</td>
#                         </tr>
#                         <tr>
#                               <td>ifName:</td>
#                               <td></td>
#                         </tr>
#                         <tr>
#                               <td>Max Speed:</td>
#                               <td>1250.0 kBytes/s</td>
#                         </tr>
#                         <tr>
#                               <td>Ip:</td>
#                               <td>127.0.0.1 (localhost)</td>
#                         </tr>
#                   </table>
#             </div>


### Interface 2 >> Descr: 'Intel(R)-PRO/100-VE-Network-Connection---
Miniporta-do-agendador-de-pacotes' | Name: '' | Ip: '192.168.0.36' | Eth:
'00-16-76-4d-b6-ef' ###

Target[192.168.0.36_2]: 2:public@192.168.0.36:
SetEnv[192.168.0.36_2]: MRTG_INT_IP="192.168.0.36"
MRTG_INT_DESCR="Intel(R)-PRO/100-VE-Network-Connection---Miniporta-do-
agendador-de-pacotes"
MaxBytes[192.168.0.36_2]: 12500000
Title[192.168.0.36_2]: Traffic Analysis for 2 -- SCI
PageTop[192.168.0.36_2]: <h1>Traffic Analysis for 2 -- SCI</h1>
            <div id="sysdetails">
                  <table>
                        <tr>
                              <td>System:</td>
                              <td>SCI in </td>
                        </tr>
                        <tr>
                              <td>Maintainer:</td>
                              <td></td>
                        </tr>
                        <tr>
                              <td>Description:</td>
                              <td>Intel(R)-PRO/100-VE-Network-Connection---
Miniporta-do-agendador-de-pacotes  </td>
                        </tr>
                        <tr>
                              <td>ifType:</td>
                              <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                              <td>ifName:</td>
```

```
                              <td></td>
                        </tr>
                        <tr>
                              <td>Max Speed:</td>
                              <td>12.5 MBytes/s</td>
                        </tr>
                        <tr>
                              <td>Ip:</td>
                              <td>192.168.0.36 (SCI)</td>
                        </tr>
                  </table>
            </div>


WorkDir: c:\www\mrtg                        <tr>
                              <td>Maintainer:</td>
                              <td></td>
                        </tr>
                        <tr>
                              <td>Description:</td>
                              <td>Intel(R)-PRO/100-VE-Network-Connection---
Miniporta-do-agendador-de-pacotes  </td>
                        </tr>
                        <tr>
                              <td>ifType:</td>
                              <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                              <td>ifName:</td>
                              <td></td>
                        </tr>
                        <tr>
                              <td>Max Speed:</td>
                              <td>12.5 MBytes/s</td>
                        </tr>
                        <tr>
                              <td>Ip:</td>
                              <td>10.1.1.2 (tiagosjs)</td>
                        </tr>
                  </table>
            </div>
workdir: c:\www\mrtg
```

Para poder gerenciar também outras variáveis do dispositivo é preciso criar um arquivo com a estrutura que contenha as opções destas variáveis.

OBS. Para fazer a atualização dos dados dos gráficos de tempos em tempos basta adicionar o comando "RunAsDaemon: yes" dentro do arquivo *.mrtg gerado.

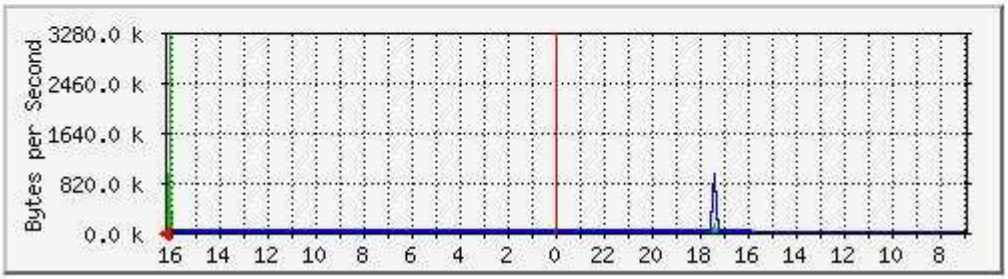
Abaixo, gráficos gerados mostrando taxa de transferência máxima, mínima e média da entrada e saída de dados da interface de rede do servidor de dados da Prefeitura Municipal de São João do Sul/SC durante dois dias de trabalho.

Max Speed: 12.5 MBytes/s
Ip: 192.168.0.36 (SCI)

---

The statistics were last updated **Friday, 29 June 2007 at 16:19**,
at which time **'SCI'** had been up for **8:21:28**.

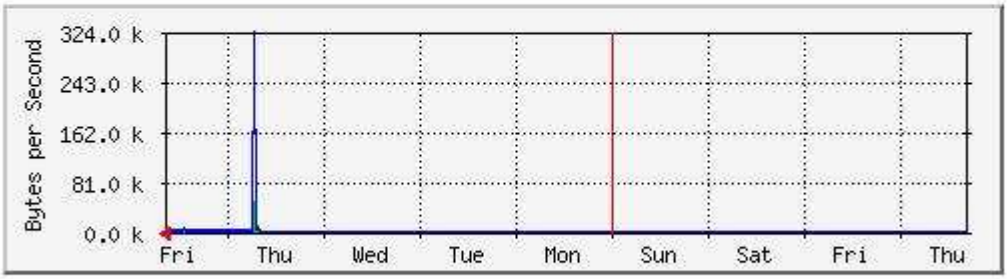
## `Daily' Graph (5 Minute Average)




| | Max | Average | Current |
|---|---|---|---|
| In | 3260.7 kB/s (26.1%) | 17.6 kB/s (0.1%) | 4621.0 B/s (0.0%) |
| Out | 949.5 kB/s (7.6%) | 7606.0 B/s (0.1%) | 5729.0 B/s (0.0%) |

---

## `Weekly' Graph (30 Minute Average)




| | Max | Average | Current |
|---|---|---|---|
| In | 50.5 kB/s (0.4%) | 2041.0 B/s (0.0%) | 6044.0 B/s (0.0%) |
| Out | 321.4 kB/s (2.6%) | 7353.0 B/s (0.1%) | 4755.0 B/s (0.0%) |

Figura 7 – Gráficos gerados com o MRTG na Pref. Mun. São João do Sul