# MONITORAMENTO DE REDES WAN COM MRTG

Cláudio Leones Bazzi[1], Juliano Rodrigo Lamb[1], Neylor Michel[1],Marcos Teixeira Junior[2], Leandro Scalabrin[3]
{bazzi, lamb, neylor, scalabrin}@utfpr.edu.br, the_ments@hotmail.com

*RESUMO. As redes de computadores consistem em uma realidade praticamente indispensável atualmente. Voz, vídeo, dados convencionais, dados em tempo real (dados expressos) são transmitidos por estas redes, tornando os usuários cada vez mais dependentes da disponibilidade destes recursos. No entanto, existem dificuldades quanto a parâmetros para medição de qualidade e desempenho de uma rede. O conhecimento de métodos de medição e monitoramento do desempenho da rede faz com que se consiga argumentar em face destas perguntas e afirmações. Neste sentido buscou-se realizar uma análise prática do monitoramento de redes de computadores*

*PALAVRAS-CHAVE: Voz, Medição de Qualidade, Monitoramento*

*ABSTRACT: The indispensable computer networks are a reality and currently. Conventional voice, video, data, data in real time (given express) are transmitted by these nets, becoming the users each time more dependents of the availability of these resources. All professional of computer networks certainly it questions regarding the quality of its net. The knowledge of methods of measurement and monitoramento of the performance of the net makes with that all obtain to argue in face of these questions and affirmations. In this direction one searched to carry through a practical analysis of the monitor of computer networks*

*KEYWORDS:Voice, Regarding the Quality, Monitor .*

## 1 INTRODUÇÃO

O protocolo SNMP é um protocolo de gerência típica de redes TCP/IP, da camada de aplicação que facilita o intercâmbio de informações, entre os dispositivos de rede. Possibilita aos administradores de rede gerenciar o desempenho da rede e encontrar e resolver problemas de rede. O software de gerência de rede segue o modelo cliente-servidor convencional: uma aplicação servidora na máquina do gerente e uma aplicação cliente no dispositivo de rede a ser analisado ou monitorado. Para evitar confusão com outras aplicações de rede, os sistemas

[1] Mestre. Docente junto ao Colegiado de Informática da Universidade Tecnológica Federal do Paraná – UTFPR

[2] Graduando. Curso de Tecnologia em Gerenciamento de Redes – Centro de Ensino Superior de Foz do Iguaçu – CESUFOZ

[3] Especialista. Docente junto ao Centro de Ensino Superior de Realeza – CESREAL – PR

de gerência de redes evitam os termos *cliente* e *servidor*. Em vez disso, usam "Gerente" para a aplicação *cliente* e "Agente" para a aplicação servidora que corre no dispositivo de rede.

Uma rede gerenciada pelo protocolo SNMP é formada por três componentes chaves:

1. Dispositivos Gerenciados
2. Agentes
3. Sistemas de Gerenciamento de Redes (NMS-*Network-Management Systems*)

Um d*ispositivo gerenciado* é um nó de rede que possui um agente SNMP instalado e se encontra em uma rede gerenciada. Estes dispositivos coletam e armazenam informações de gerenciamento e mantém estas informações disponíveis para sistemas NMS através do protocolo SNMP. Dispositivos gerenciados, também às vezes denominados de dispositivos de rede, podem ser roteadores, servidores de acesso, impressoras, computadores, servidores de rede, *switches*, dispositivos de armazenamento, dentre outros.

Um *agente* é um módulo de software de gerenciamento de rede que fica armazenado em um dispositivo gerenciado. Um agente tem o conhecimento das informações de gerenciamento locais e traduzem estas informações para um formato compatível com o protocolo SNMP.

Todos os objetos acessados pelo SNMP devem ter nomes únicos definidos e atribuídos. Além disso, o Gerente e o Agente devem acordar os nomes e significados das operações *fetch* e *store*. O conjunto de todos os objetos SNMP é coletivamente conhecido como MIB (do inglês: *Management Information Base*). O *Standard* SNMP não define o MIB, mas apenas o formato e o tipo de codificação das mensagens. A especificação das variáveis MIB, assim como o significado das operações *fetch* e *store* em cada variável, é determinado por um padrão próprio. A definição dos objetos do MIB é feita com o esquema de nomes do ASN.1 (*Abstract Syntax Notation*), o qual atribui a cada objeto um prefixo longo que garante a unicidade do nome, a cada nome é atribuído um número inteiro. Também, o SNMP não especifica um conjunto de variáveis, e que a definição de objetos é independente do protocolo de comunicação, permite criar novos conjuntos de variáveis MIB, definidos como *Standards*, para novos dispositivos ou novos protocolos. Por isso, foram criados muitos conjuntos de variáveis MIB que correspondem a protocolos como UDP, IP, ARP, assim como variáveis MIB para *hardware* de rede como Ethernet ou FDDI, ou para dispositivos tais como *bridges, switches* ou impressoras.

O MRTG (*Multi Router Traffic Grapher)* é uma ferramenta de monitoramento que gera páginas *html* com gráficos de dados coletados a partir de SNMP. É conhecido principalmente

pelo seu uso no monitoramento de tráfego de rede, mas pode monitorar qualquer coisa desde que o *host* forneça os dados via SNMP ou *scripts*.

Algumas características do MRTG são:

- Medição de dois valores, no caso de tráfego, podem ser entrada e saída.
- Leitura via SNMP ou através de *script* que retorne um formato padrão.
- Coleta de dados a cada 5 minutos por padrão, mas o tempo pode ser aumentado.
- Criação de uma página *html* com quatro gráficos (diário, mensal, semanal e anual).
- O MRTG pode avisar caso o gráfico atinja um valor pré-estabelecido. Por exemplo: se determinado servidor atinge 95% do espaço do disco, o MRTG pode encaminhar um e-mail para o administrador informando o ocorrido.
- Presença de uma ferramenta para gerar os arquivos de configuração: o CFGMAKER.
- Presença de uma ferramenta para gerar uma página de índice para os casos em que muitos itens são monitorados: o INDEXMAKER.
- O MRTG é software livre. Distribuído nos termos GNU *General Public License*.

Os roteadores podem realizar comunicação entre si diretamente utilizando protocolos específicos, tais como (RIP, OSPF, PPP, IGRP) para definir as rotas de tráfego dos pacotes. Quando utilizados em para a comunicação de redes a longa distâncias, utilizam um link de alguma empresa Telecom, caracteriza-se por redes WAN (Figura 1).

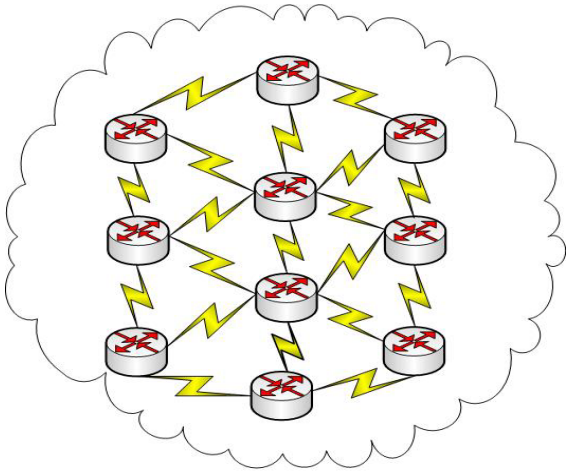


**Figura 1 –** Topologia de roteadores em um ambiente WAN

## 2 MATERIAL E MÉTODOS

Utilizou-se no desenvolvimento deste trabalho o roteamento de uma rede com protocolo RIP (*Routing Information Protocol*). Escolheu-se uma configuração simples que pudesse simular com pequeno ambiente WAN para interligar uma matriz a sua filial (Tabela 1).

**Tabela 1** - Configuração de equipamentos utilizados

| • Servidor (matriz) | • Ambiente WAN | • Cliente (filial); |
|---|---|---|
| ○ Processador AMD Duron 1100MHz;<br>○ Memória Kingston 512Mb DDR400;<br>○ Placa mãe ECS;<br>○ HD Maxtor 10Gb;<br>○ Placa de rede PCI Realtek 8139c;<br>○ Gabinete *Full* ATX; | ○ Roteadores cisco série 1601 (Figura 2a);<br>○ Cabos seriais db60 DCE-DTE (Figura 2b);<br>○ *Switch fast ethernet*;<br>○ Cabos rede categoria 5e; | ○ Laptop Sony Vaio; |

O protocolo RIP é baseado no algoritmo vetor-distância, que utiliza a contagem de *hops* como métrica. "Uma contagem de *hops* é o número de roteadores por onde um pacote tem que passar para atingir o seu destino."

(a) (b)

**Figura 2.** Roteador série 1600 (a) e cabos de interligação (b)

Quando um roteador recebe um *update*, ele compara essa informação com a existente na sua própria tabela. Se essa atualização inclui uma rota ainda não existente, ela é adicionada. Se ela já existir, é feita uma comparação entre a métrica das duas, sendo que opta pela menor.

Em uma rede desta natureza, cada roteador envia sua tabela inteira para todos os roteadores adjacentes em intervalos predefinidos de tempo (geralmente 30 segundos). Essa tabela também é enviada quando a topologia da rede é alterada (mais alguma rede é anunciada). A esse procedimento damos o nome de anúncio.

Estas mensagens fazem com que todos os roteadores adjacentes atualizem suas tabelas, que por sua vez serão enviadas aos seus respectivos vizinhos. É importante lembrar que esses anúncios são feitos por *broadcast*. Se as tabelas forem grandes, podem ser necessários vários *broadcasts*, cada um com uma parte da tabela.

Outra característica do RIP é que ele é um protocolo *classful*, isto é, não repassa informação de máscara em seus *updates*. Protocolos *classless* possuem a vantagem de trazer em seus anúncios a máscara, possibilitando que uma *subnet* seja anunciada sem que toda a sua classe também seja.

A topologia da rede proposta no corrente estudo, corresponde a Figura 3.

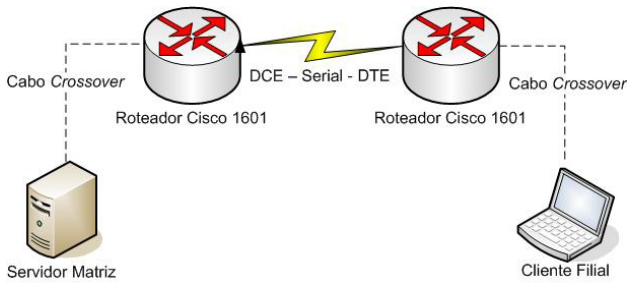


**Figura 3 -** Estrutura topológica da rede

Para instalação do servidor, utilizou-se a distribuição de Sistema Operacional linux Debian 4.0, última versão estável, instalada a partir de um CD. Como o ambiente instalado é puramente em modo texto, para visualização dos gráficos gerados pelo MRTG foram também instaladas a versão enxuta do *desktop* GNOME e o navegador FIREFOX, ambos instalados com a ferramenta *aptitude*.

Para a configuração do *MRTG* para o monitoramento de tráfego foi utilizado um bloco de notas vazio onde se começaram as definições das regras. Algumas considerações:

a. Precisa-se conhecer o "*IP address*" ou "*host name*" do dispositivo a ser monitorado;
b. Necessário conhecer a comunidade de leitura do dispositivo a ser monitorado.

Com estas informações básicas pode-se iniciar o monitoramento do dispositivo, tratando-se do tráfego de entrada e saída das interfaces.

Criou-se uma pasta para armazenar as imagens e arquivos gerados pelo MRTG: /var/www/html/mrtg. Para este exemplo estamos monitorando um roteador CISCO 1600, sendo o seu endereço IP 192.168.1.1 e a comunidade (senha) "public".

As regras que foram escrito dentro do arquivo `cfg` são descitas no Quadro 1.

```
WorkDir: /var/www/html/mrtg      // Diretório onde será armazenado todos os dados coletados
Language: brazilian  // Língua que aparecerá na tela depois que abrir o relatorio no browser ou apache.
Options[_]: bits,growright  // bits = velocidade em bits , growright = gráfico sai do lado direito pro esquerdo
RunAsDaemon: yes  // rodar em modo Daemon
Target[lan]: 1:public@192.168.1.1  // teu alvo ou interface que será monitorado com seu community (que nosso caso colocamos public ).
MaxBytes[lan]:6matriz  // link da tua banda
AbsMax[lan]: 6matriz  // link da tua banda
Unscaled[lan]: dwmy  // os quatro gráfico serão redimensionados de acordo com o uso do link.
```

**Quadro 1:** Regras que foram escrito dentro do arquivo *cfg*.

Pode-se notar que o MRTG irá fazer apenas uma coleta e terminará, para fazer com que ele fique coletando os dados e atualizando automaticamente os gráficos, precisaremos editar o arquivo `mrtg.cfg` incluindo a seguinte linha: `RunAsDaemon: Yes`

Para executar o MRTG utilizou-se o comando `root@user:/#mrtg /root/mrtg.cfg`. A configuração dos roteadores foi desenvolvida em duas partes distintas, [1] configuração do roteador da matriz (Tabela 2 e Tabela 3) e [2] roteador da filial.

**Tabela 2:** Configuração do roteamento IP e interfaces (Matriz)

| **Habilitando o roteamento IP** | **Configuração da interface** | |
|---|---|---|
| | **Serial** | **Ethernet** |
| <matriz>#<br><matriz>#**conf t**<br><matriz>(config)#**ip routing**<br><matriz>(config)# | <matriz>#<br><matriz>#**conf t**<br><matriz>(config)#**int s0**<br><matriz>(config-if)#**ip address 100.1.1.1 255.0.0.0**<br><matriz>(config-if)#**clock rate 800000**<br><matriz>(config-if)# **encapsulation ppp**<br><matriz>(config-if)#**no shut** | <matriz>#<br><matriz>#**conf t**<br><matriz>(config)#**int e0**<br><matriz>(config-if)#**ip address 192.168.1.1 255.255.255.0**<br><matriz>(config-if)#**no shut** |

**Tabela 3:** Configuração RIP e SNMP (Matriz)

| **Habilitação do protocolo RIP** | **Anúncio das redes pelo RIP** | **Configuração do SNMP** |
|---|---|---|
| <matriz>#**conf t**<br><matriz>(config)#**router rip**<br><matriz>(config-router)# | <matriz>#**conf t**<br><matriz>(config)#**router rip**<br><matriz>(config-router)#**network 192.168.1.0**<br><matriz>(config-router)# | <matriz>#**conf t**<br><matriz>(config)# **snmp-server community public ro**<br><matriz>(config)# **snmp-server location matriz** |

As configurações foram salvas através da linha de comando `<matriz>#copy running-config startup-config`. Para o roteador da filial as configurações são especificadas conforme a Tabela 4 e Tabela 5.

**Tabela 4:** Configuração do roteamento IP e interfaces (Filial)

| **Habilitando o protocolo IP** | **Configuração da interface** | |
|---|---|---|
| | **Serial** | **Ethernet** |
| <filial >#**conf t**<br><filial >(config)#**router rip**<br><filial >(config-router)# | <filial>#<br><filial >#**conf t**<br><filial >(config)#**int s0**<br><filial >(config-if)#**ip address 100.1.1.2 255.0.0.0**<br><filial >(config-if)#**encapsulation ppp**<br><filial >(config-if)#**no shut** | <filial >#<br><filial >#**conf t**<br><filial >(config)#**int e0**<br><filial >(config-if)#**ip address 192.168.2.1 255.255.255.0**<br><filial >(config-if)#**no shut** |

**Tabela 5:** Configuração RIP e SNMP (Filial)

| **Anúncio das redes pelo RIP** | **Configuração do SNMP** |
|---|---|
| <filial >#**conf t** | <matriz>#**conf t** |
| <filial >(config)#**router rip** | <matriz>(config)# **snmp-server community public ro** |
| <filial >(config-router)#**network 192.168.2.0** | <matriz>(config)# **snmp-server location filial** |
| <filial >(config-router)# | |

# 3 RESULTADOS E DISCUSSÃO

Realizadas as configurações, realizou-se a busca pelo monitoramento apresentado, visando avaliar o trafego da rede em função da geração de pacotes gerados, tanto pela comunicação do protocolo RIP como troca de informações entre computadores. Foram gerados gráficos referentes ao tráfego diário (Figura 4 e Tabela 6).

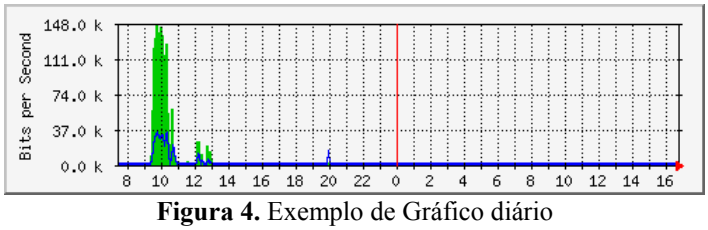


**Figura 4.** Exemplo de Gráfico diário

Os dados observados correspondem a observações de aproximadamente 5 minutos em ambiente operacional.

**Tabela 6.** Dados trafegados (Diário)

| | | Máx | Média | Atual |
|---|---|---|---|---|
| **a** | **Entrada** | 145.2 kb/s (1.3%) | 4632.0 b/s (0.0%) | 688.0 b/s (0.0%) |
| | **Saída** | 33.3 kb/s (0.3%) | 1104.0 b/s (0.0%) | 16.0 b/s (0.0%) |

- Gráfico "Semanal" (30 minutos Média) – Figura 5 e Tabela 7.

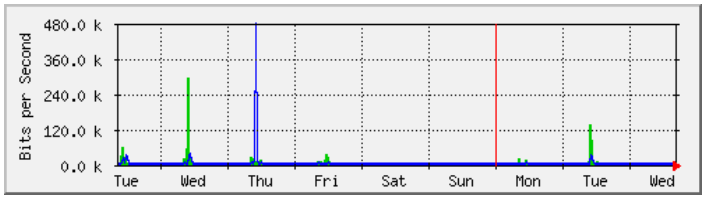


**Figura 5.** Exemplo de gráfico semanal

**Tabela 7.** Dados trafegados (Semanal)

| | | Máx | Média | Atual |
|---|---|---|---|---|
| **a** | **Entrada** | 295.6 kb/s (2.6%) | 3528.0 b/s (0.0%) | 624.0 b/s (0.0%) |
| | **Saída** | 479.1 kb/s (4.3%) | 2136.0 b/s (0.0%) | 16.0 b/s (0.0%) |

- Gráfico "Mensal" (2 horas Média) – Figura 6 e Tabela 8

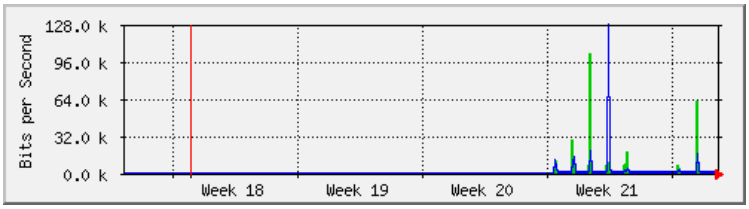


**Figura 6.** Exemplo de gráfico mensal

**Tabela 8.** Dados trafegados (Mensal)

| | | Máx | Média | Atual |
|---|---|---|---|---|
| | **Entrada** | 103.1 kb/s (0.9%) | 3368.0 b/s (0.0%) | 384.0 b/s (0.0%) |
| | **Saída** | 127.6 kb/s (1.1%) | 2064.0 b/s (0.0%) | 16.0 b/s (0.0%) |

- Gráfico "Anual" (1 dia Média) – Figura 7 e Tabela 9

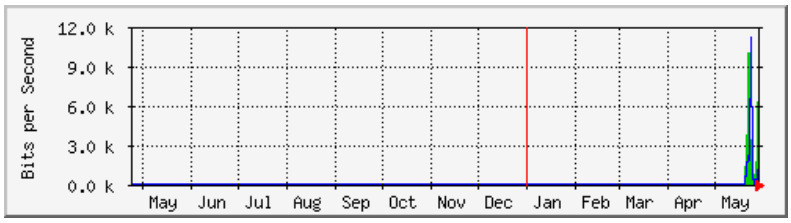


**Figura 8** - Exemplo de gráfico anual**.**

**Tabela 8.** Dados trafegados (Anual)

| | | Máx | Média | Atual |
|---|---|---|---|---|
| | **Entrada** | 10.0 kb/s (0.1%) | 3408.0 b/s (0.0%) | 6280.0 b/s (0.1%) |
| | **Saída** | 11.1 kb/s (0.1%) | 2120.0 b/s (0.0%) | 1648.0 b/s (0.0%) |

## 4 CONCLUSÃO

O acompanhamento de uma rede local com posse destas ferramentas permite um acompanhamento de como anda a rede gerenciada fornecendo elementos sobre como podemos resolver problemas ou eventuais falhas que ocorrem no decorrer do uso, até mesmo futuros problemas que possam trazer sérias conseqüências dentro da empresa.

## 5 REFERENCIAS BIBLIOGRÁFICA


Bruscato, Alexandre Carlos; Hattmann, Amilton Carlos; Pinho, Antonio Carlos; Muncinelli, Gian Franco**; Simple Network Management Protocol.** Publicado em 11/07/2005 **Disponível em:** http://pt.wikipedia.org/wiki/SNMP, acessado em 15/05/2007.

**Download Do Cd De Instalação Do Debian 4**. Disponível em: ftp://ftp.br.debian.org/debian-cd/4.0_r0/i386/iso-cd/debian-40r0-i386-netinst.iso, acessado em 18/05/2007.

Filho, Huber Bernal**. Simple Network Management Protocol (SNMP)**. Publicado em 25/04/2005. **Disponível em:** http://www.teleco.com.br/tutoriais, acessado em 15/05/2007.

**Gerando gráficos para interfaces de rede com MRTG.** Disponível em http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=5784, acessado em 20/05/2007.

**Instalando e configurando SNMP e MRTG no linux**. Disponível em http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=2552, acessado em 21/05/2007.

**Medição de desempenho de redes WAN - conceitos e técnicas**. Disponível em: http://www.teleco.com.br/tutoriais, acessado em 15/05/2007.

**Monitoração de tráfego com MRTG**. Disponível em http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=1139, acessado em 19/05/2007.

**ROTEADOR.** Disponível em: http://pt.wikipedia.org/wiki/roteador, acessado em 18/05/2007.