

A Estatística em Gerência de Redes (de Computadores)

Fabiane Almeida Oliveira², Gilvan de Souza Santos^{1,2}, Herman Ricardo J. F. Telles^{1,2},
Líbni Pires O. Melo²

¹Universidade do Estado da Bahia, (UNEB CAMPUS VIII)

²Faculdade Sete de Setembro, (FASETE)
48600-000, Paulo Afonso, BA

fabianealmeida16@hotmail.com, gilvangat@hotmail.com, hermantelles@yahoo.com.br, libnisistemas@hotmail.com

Ryan Ribeiro de Azevedo^{2,3}

³Centro de Informática – Universidade Federal de Pernambuco (CIN-UFPE)

Av. Prof. Luiz Freire, s/n Cidade Universitária 50740-540 - Recife, PE - Brasil

rra2@cin.ufpe.br

Resumo: Para garantir a qualidade dos serviços de redes foi necessário ampliar as ferramentas de gerenciamento, favorecendo a agilidade, produtividade, segurança e portabilidade nas operações [7], usando a estatística para avaliar e diagnosticar problemas existentes. Este trabalho apresenta um estudo sobre o uso da estatística para a tomada de decisões na Gerência de Redes. Além disso, discuti-se alguns softwares que utilizam dados estatísticos como auxílio para as tomadas de decisões.

Palavras-chave: Gerência de redes, estatística, desempenho, *software*.

1. Introdução

A monitoração de uma rede (de computadores) implica entre outras, em coletar informações sobre os objetos gerenciados de forma que se possa chegar a uma série de diagnósticos, tais como detecção de falhas, localização de sobrecargas, alerta de problemas, gráficos de utilização dos recursos, demonstração de tendências, entre outros, permitindo a ampla utilização dos recursos fisicamente distribuídos [18].

A gerência de redes exige medições dos objetos gerenciados, essas medições precisam ser tratadas. Nesse ponto a Estatística entra como peça fundamental para o gerenciamento de redes, pois produz resultados a partir dos dados coletados. As informações estatísticas são geradas pelos recursos de rede e os *softwares* de gerenciamento produzem relatórios baseados nessas informações [15].

O objetivo deste trabalho é mostrar que os *softwares* gerenciadores de redes, largamente utilizados, emitem relatórios estatísticos que englobam informações, tais como: tráfego médio gerado ou recebido pelos *hosts* na rede, média da utilização de banda, quantidade média do tráfego *multicast* gerado ou recebido pelo *host*, estatísticas de tráfego de conexões TCP ativas, estatísticas de tempo de

utilização de recursos, dados de atividades de processadores, dados de uso de memória, tempo de resposta e taxa de erros, estatísticas de desempenho de equipamentos, estatísticas de tráfego para fluxos definidos pelo usuário, velocidade média de *download* e *upload* de pacotes, entre outros.

Este trabalho está organizado da seguinte forma: na Seção 2 é abordada a gerência de redes, os seus objetivos e os tipos de gerenciamento que existem. Na Seção 3 será feita uma análise de quatro *softwares* para o gerenciamento de redes: *NTOP* [1], *Vert-it*, *Nagios* [5] e *MRTG* [4]. E na Seção 4 são apresentadas as conclusões e os trabalhos futuros.

2. Gerência de Redes

Um sistema de gerenciamento de redes de computadores detecta e corrige falhas, em um tempo mínimo, além de estabelecer procedimentos [9] para a previsão de problemas futuros analisando um conjunto de conceitos básicos que são:

- O objeto gerenciado: qualquer objeto passível de ser monitorado numa rede para verificar certos parâmetros de funcionamento que podem ser dispositivos lógicos (*software*) ou físicos (*hardware*);
- O agente: elemento responsável pela coleta de informações dos objetos gerenciados, enviando-as ao gerente e executando comandos determinados por ele, baseados em tais informações;
- O gerente: é quem concentra as informações passadas pelo agente e envia comandos de gerenciamento a este para serem executados sobre os objetos gerenciados;
- A MIB (*Management Information Base*): é a estrutura básica de um sistema de gerenciamento.

Na Figura 1 é apresentado um sistema de gerenciamento e os seus componentes.

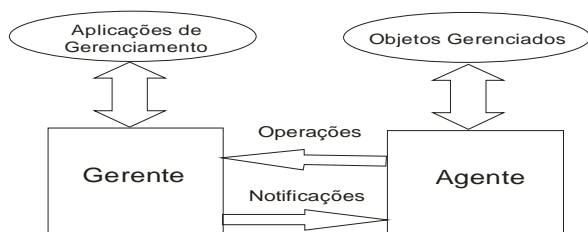


Figura 1: Exemplo de sistema de gerenciamento.

O gerenciamento de redes de computadores inclui analisar os recursos de computação distribuídos e seu controle efetivo, o contínuo crescimento da rede em termos de componentes, usuários, interfaces, protocolos e fornecedores [20].

2.1 Objetivos do Gerenciamento de Redes

O gerenciamento de redes consiste em monitorar, detectar falhas e tomar determinadas medidas corretivas [9], para isso são utilizados protocolos de gerenciamento baseados em outros tipos de protocolos como: TCP/IP e o SNMP.

O RMON (*Remote Network Monitoring*) é um padrão IETF de gerenciamento de redes, segundo a RFC 1757, o RMON não é uma pilha de protocolos, nem mesmo um protocolo por si só. Trata-se de uma extensão de MIB (*Management Information Base*), para ser utilizada com protocolos de gerenciamento de redes em aplicações para a internet, baseadas no TCP/IP. Os avanços introduzidos pelo padrão RMON foram: o controle de monitoramento remoto, múltiplos gerentes e o gerenciamento de tabelas. As suas principais características são: interoperabilidade independente de fabricante; capacidade de fornecer informações precisas sobre as causas de falha no funcionamento normal da rede, assim como da severidade dessa falha; e oferecer ferramentas adequadas para diagnóstico da rede.

Além dos sistemas de gerenciamento, os protocolos auxiliam a fazer a parte do funcionamento da gerência. Abaixo na Figura 2 é apresentado o funcionamento de um protocolo de gerenciamento.

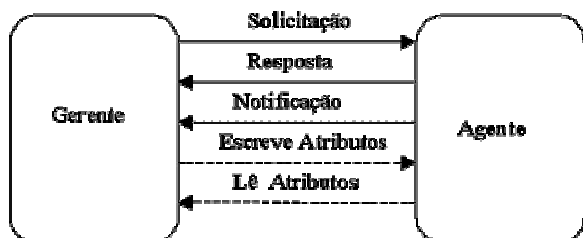


Figura 2: Funcionamento de um protocolo de gerenciamento.

2.2 Tipos de Gerenciamento de Redes

A utilização dos tipos de gerenciamento de redes se destaca por seguir os padrões OSI e TCP/IP [15]. Eles são divididos pelas suas características para melhorar o gerenciamento por partes determinadas, seguindo uma ordem por suas funções.

Gerenciamento de Falhas. Tem o objetivo de garantir um funcionamento contínuo da rede e seus serviços. Este tipo de gerenciamento faz a distinção entre falha e erro, analisa uma falha como uma condição anormal que requer uma ação para correção, enquanto que o erro é um evento simples, como um grampeamento no cabo pode causar distorções que induzem a uma alta taxa de erros.

Gerenciamento de Desempenho. O gerenciamento de desempenho garante a eficiência da rede, é a monitoração das atividades da rede e o controle dos recursos através de ajustes e trocas analisando questões relativas à: nível de capacidade de utilização, tráfego excessivo e aumento do tempo de resposta.

Gerenciamento de Configuração. O gerenciamento de configuração se preocupa com a interconexão dos dispositivos gerenciados, ele está relacionado com as tarefas de manutenção, adição e atualização dos componentes e do estado dos componentes durante a operação da rede.

Gerenciamento de Contabilização. Trabalha o custo de utilização da rede e seus recursos, permite ao administrador determinar se um usuário ou grupo de usuários estão abusando de seus privilégios de acesso, e se usuários estão usando a rede de forma ineficiente.

Gerenciamento de Segurança. Busca garantir a segurança de informações sigilosas em tráfego na rede e requer permitir que políticas de segurança sejam tomadas para garantir a monitoração e o controle de acesso à rede ou parte da rede; usando a estatística como prova de suas análises.

3. Softwares de Gerenciamento de Redes

O crescimento do número de *softwares* de gerenciamento tem proporcionado enormes benefícios para os administradores de rede, devido à variedade de serviços oferecidos pelos seus fabricantes. Mas em contrapartida, o gerenciamento torna-se uma tarefa complexa em consequência do crescimento acelerado das redes de computadores e do suporte a um grande conjunto de serviços.

O principal objetivo dos *softwares* de gerenciamento é auxiliar o gerente de uma rede no monitoramento e detecção de problemas [10]. Existem quatro tipos de ferramentas: ferramentas a nível físico, que detectam problemas em nível de cabos e conexões de *hardware*; monitores de rede, que se conectam as redes, monitorando o tráfego; analisadores de rede, que

auxiliam no rastreamento e correção de problemas encontrados nas redes; sistemas de gerenciamento de redes integrados (SGRI), os quais permitem o monitoramento e controle de uma rede inteira a partir de um ponto central.

As informações que circulam em uma rede de computadores devem ser transportadas de modo confiável e rápido. Para que isso aconteça é importante que os dados sejam monitorados de maneira que os problemas que porventura possam existir sejam resolvidos na medida do possível, é aí que entra os softwares de gerenciamento. Uma rede sem mecanismos de gerência pode apresentar problemas como congestionamento do tráfego, recursos mal utilizados, recursos sobrecarregados, problemas com segurança e outros.

A gerência está associada ao controle de atividades e ao monitoramento do uso de recursos da rede [15]. As tarefas básicas da gerência em redes são: obter informações da rede, tratar essas informações, possibilitando um diagnóstico, e encaminhar as soluções dos problemas. É isso que os *softwares* de gerenciamento tentam manipular nos diversos componentes de uma rede, possibilitando descobrir, prever e reagir a problemas.

Devido a grande variedade de ferramentas destinadas ao gerenciamento de redes, algumas incluem monitoramento, análise do tráfego da rede, segurança de redes, configuração, entre outras.

Nesta seção será realizada uma análise de quatro *softwares* para administração de redes, mostrando o uso da estatística como auxílio na tomada de decisão no gerenciamento de redes, são eles: *NTOP* [1], *Vert-it*, *Nagios* [5] e *MRTG* [4].

3.1 Ntop – Network Top

O Ntop [1] é um aplicativo com o código fonte livre, desenvolvido na linguagem C, com API PERL e PHP, baseado em uma biblioteca de captura de pacotes na rede chamada libpcap, suportando qualquer tipo de banco de dados [18]. Ferramenta simples, portátil e rápida, pois está baseada em interface web, que possui como finalidade monitorar e analisar o tráfego de rede, como também gerenciar a rede de computadores, permitindo ao usuário localizar atividades pertinentes na rede.

Através de atividades como detecção de erros, violação de segurança e otimização da rede dentre outras, integradas a métodos e cálculos estatísticos, disponibiliza informações referentes à rede e ao computador, como, o tráfego total gerado ou recebido por um determinado *host*; valor total, porcentagem, média ou os picos de utilização da banda; desempenho da rede local; espaço utilizado em disco rígido; quantidade de memória alocada e o consumo de cada processo no processador.

Na arquitetura do Ntop [1], apresentada na Figura 3, pode-se ver o funcionamento e a composição geral da ferramenta.

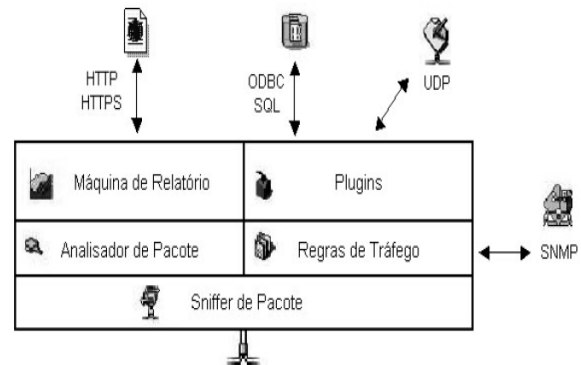


Figura 3: Arquitetura do Ntop.

Seu funcionamento acontece da seguinte forma: o *sniffer* de pacote coleta todos os pacotes da rede, é ele quem monitora e analisa o tráfego, detectando a sobrecarga da rede e possíveis problemas. Após colher os pacotes, eles são transmitidos para o analisador de pacote, onde os pacotes são processados um de cada vez. As informações sobre as estações são armazenadas em uma tabela *hash*, e esse armazenamento é feito de duas formas, baseado em GNU que é um conjunto de rotinas de acesso ao banco de dados ou utilizando o banco de dados SQL. Toda vez que as informações de tráfego tiverem que ser exibidas, a máquina de relatório mostrará os dados solicitados.

O *software* Ntop [1], tem como principais funções:

- Medição do tráfego da rede;
- Monitoramento do tráfego da rede;
- Otimização e Planejamento da rede;
- Detecção de Violações de Segurança da rede.

A partir dessas funções que o gerente da rede vai obter informações estatísticas essenciais, permitindo que administradores possam identificar o uso improdutivo da largura de banda da rede, fazendo uma revisão das políticas para que obtenha um uso mais inteligente e eficaz da largura de banda disponível, como também a utilização de protocolos desnecessários.

Outro método estatístico utilizado pelo Ntop [1], são as medidas de tráfego apresentadas através de gráficos que consiste em medir a utilização de atividades relevantes, gerando uma série de estatísticas. É a partir daí que o gerente da rede vai obter informações identificando o uso improdutivo da largura de banda, como também a utilização de protocolos desnecessários. Abaixo na Figura 4 pode-se ver um exemplo de gráfico gerado pelo Ntop.

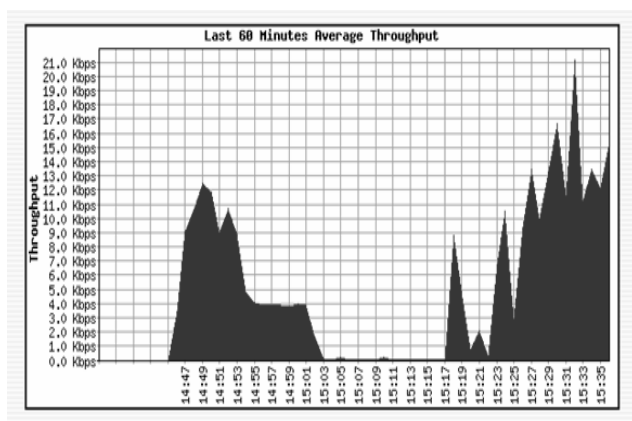


Figura 4 - Ntop: Modo web.

Portanto o Ntop [1] pode ser utilizado para medidas de monitoramento de tráfego, tendo como principais características, um servidor HTTP embutido, suporte a vários tipos de enlaces de rede, pouca utilização da CPU, portabilidade para várias plataformas, armazenamento das informações de tráfego em um banco de dados SQL, e integração com várias ferramentas de rede, tornando o Ntop [1] adequado para usuários que desejam analisar o tráfego da rede.

3.2 Vert-it: Network Administrator

Assim como o Ntop [1], o Vert-it é um software que surgiu com a finalidade de oferecer recursos avançados que possibilitem ao administrador de rede, formas de realizar suas atividades de gerenciamento da rede de uma maneira simples, segura e prática, de modo a proporcionar uma varredura em toda a rede, permitindo o controle de qualquer máquina da rede local ou WAN [12]. Pode-se observar na Figura 5, um dos recursos que o Vert oferece que é um mapa de localização da rede.

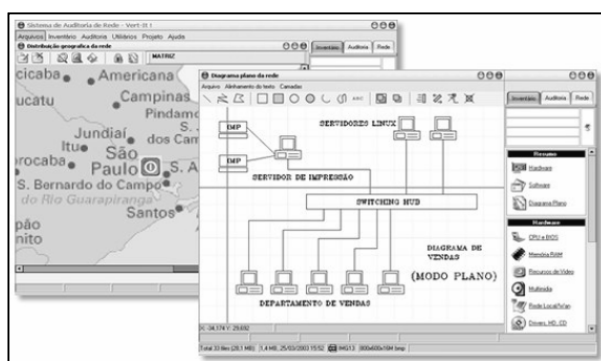


Figura 5: Mapa de localização da rede no Vert-it.

Alguns dos vários recursos que o *software* oferece são:

- Auditoria: permite fazer um acompanhamento das transformações de ambiente de hardware e software de cada uma das máquinas da rede;

- Atualização centralizada: atualiza programas do sistema operacional e aplicativos;
- Perfil ativo: relata mudanças feitas na instalação tanto de *softwares* como de *hardware*;
- Comunicação: permite comunicação através de um caixa de diálogo com uma estação de rede local ou WAN;
- Inventário – disponibiliza todos os bens de *hardware* e *software* da instituição, através de consultas e relatórios;
- Suporte: proporciona recursos para a verificação do ambiente de rede e soluções para atualização e correção de problemas;
- Servidor de notificação: recebe automaticamente cadastros e auditorias feitas em máquinas dos clientes, informando também alterações no perfil;
- Controle remoto: proporciona o controle de equipamentos Linux e Windows conectados à rede;
- Recursos Gráficos: disponibiliza recursos gráficos para a construção de projetos de redes e *lay-outs*;
- Gerador de relatórios: permite construir impressões personalizadas;
- Gráficos e estatísticas: mostra o desempenho de todos os equipamentos, assim como estatísticas de tempo de utilização, Figura 6 e 7;
- Banco de dados SQL: armazena informações em um banco de dados SQL *Interbase/Firebird*;
- Mapas geográficos: suporta a transferência de mapas geográficos para sua rede, Figura 5.

Percebe-se através dos recursos listados acima, que esse *software* dispõe de recursos gráficos estatísticos, onde a partir deles poderão ser observados as atividades do processador da estação, a memória da estação, a melhor rota de acesso ao computador, proporcionando ao gerente de rede, avaliar os momentos de sobre carga no processamento, avaliar a estação que necessita de mais memória, os recursos de rede que estão sendo mal utilizados, desempenho e outros, para assim poder fazer as alterações necessárias e também prevenir futuras falhas na rede.

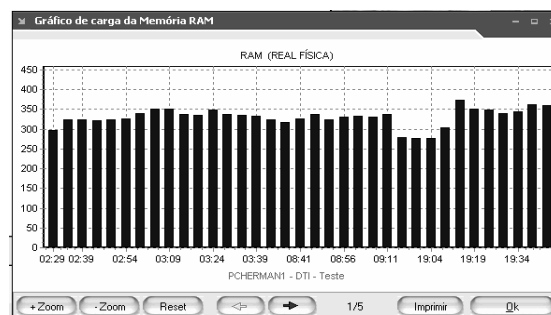


Figura 6: Gráfico de carga da Memória RAM.

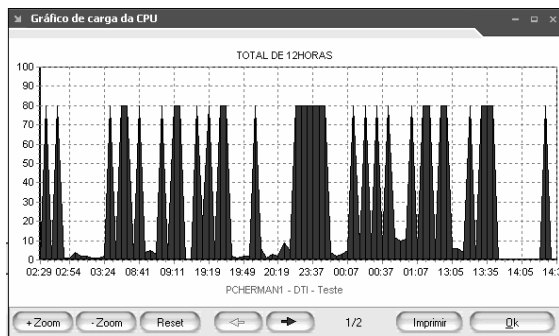


Figura 7: Gráfico de carga da CPU.

O *software* Vert-it, como outros *softwares* de gerenciamento de redes, integra cálculos estatísticos, ajuda a detectar erros ou falhas que ocorrem na rede e também auxilia na prevenção de futuros danos, tornando-se uma ferramenta essencial para a execução de atividades de gerência.

3.3 Nagios

Nagios é uma poderosa ferramenta *Open Source* de monitoramento de redes, que verifica constantemente a disponibilidade do serviço, local ou remoto [6]. Com ele é possível monitorar *hosts*, micros, *switchs*, impressoras e tudo o que estiver ligado à rede. O Nagios pode ser configurado para mandar tipos de avisos por meio de e-mail ou celular para grupos de usuários cadastrados. Assim, é possível obter relatórios de disponibilidade e configurar ações corretivas para os problemas ocorridos na rede [3]. Ele tem uma interface que permite monitoramento via WAP e *browser* e possui configuração de alertas, para avisar quando ocorrerem problemas e quando os problemas forem resolvidos. Na Figura 8 abaixo podemos ver na tela via *browser* [11] o state do Nagios.

State	Time	% Total Time	% Known Time
UP	7d 23h 26m 29s	53.18%	100.00%
DOWN	0d 0h 0m 0s	0.00%	0.00%
UNREACHABLE	0d 0h 0m 0s	0.00%	0.00%
Undetermined	7d 0h 33m 31s	46.82%	
All	15d 0h 0m 0s	100.0%	100.0%

Figura 8: *Host State Breakdowns* do Nagios.

O seu funcionamento é bem mais aproveitado com um servidor WEB, também baseado em teoria *Open Source*. A compilação irá gerar arquivos CGIs que serão utilizados em conjunto com o Apache. É apresentado na Figura 9 o *Service State Statistics* do Nagios [11].

State	Time	% Time
OK	0d 0h 9m 25s	0.2%
WARNING	4d 3h 43m 15s	99.8%
UNKNOWN	0d 0h 0m 0s	0.0%
CRITICAL	0d 0h 0m 0s	0.0%
All States	4d 3h 52m 40s	100.0%

Figura 9: *Service State Statistics*.

Essa ferramenta explora a facilidade de criação de novos plugins, o que permite a customização do sistema ao máximo se adequando às necessidades dos administradores de redes. Ela é considerada muito dinâmica pela vasta geração de gráficos e inúmeras possibilidades de monitoramento da rede. Foi criada primeiramente para o sistema operacional Linux, mas pode rodar em outros Unixes também.

O Nagios oferece diversos recursos [21] [13], dentre eles estão:

- Monitoração de serviços de rede (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Monitoração de recursos de computadores ou equipamentos de rede na maioria dos sistemas operacionais com suporte a rede;
- Plataforma flexível por sua eficaz lista de plugins que permite aos usuários facilmente criar seus próprios modos de monitoração dependendo de suas necessidades, usando a ferramenta de desenvolvimento da sua escolha;
- Checagem dos serviços paralelizados;
- Capacidade de definir a rede hierarquicamente;
- Capacidade de notificar quando um serviço ou equipamento apresenta problemas e quando o problema é resolvido (via email, pager, celular);
- Capacidade de definir tratadores de eventos que executam tarefas em situações pré-determinadas ou para a resolução pró-ativas de problemas;
- Rotação automática de log;
- Suporte para implementação de monitoração redundante;
- Excelente interface baseada na web para visualização do atual status da rede, notificações, histórico de problemas, arquivos de log, entre outras.

Com todos esses recursos disponíveis pode-se perceber a grande utilidade dessa ferramenta para o gerenciamento de redes.

3.4 MRTG

O *Multi Router Traffic Graphey* (MRTG) [4] é uma ferramenta desenvolvida por Tobias Oetiker e Dave Rand com o objetivo de monitorar o tráfego na rede, *links* de redes, a utilização de interfaces e de CPU ou

qualquer coisa desde que forneça dados SNMP ou *scripts* para ler os dados dos roteadores [15], podendo gerar alertas a partir de "*thresholds*", facilitando assim o gerenciamento da rede.

O MRTG é um programa desenvolvido em *Perl*, mas utiliza um módulo em C para gerar gráficos, que são mostrados automaticamente em páginas HTML com imagens *GIF* atualizadas em um determinado período de tempo [18]. Esses gráficos mostram dados estatísticos em relação ao uso da banda em termos de velocidade.

Geralmente é utilizado juntamente com um servidor *Web* como o Apache, por exemplo, para fazer consultas aos gráficos de monitoramento, podendo ser consultadas de qualquer computador que tenha um *browser* instalado [19]. Além de ser uma ferramenta livre, é relativamente fácil de instalar e configurar, tanto em ambiente *Linux* como em ambiente Windows, isso dependendo do caso. Um exemplo de gráfico é apresentado na Figura 10.

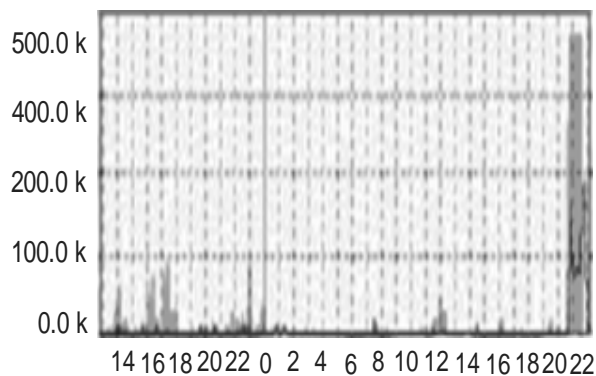


Figura 10: Tráfego de dados.

É retratado na Figura 10 acima um dos gráficos *default* gerado para uma interface de rede local mostrando a quantidade de *bytes* transmitida e recebida nas últimas 24 horas, na última semana, no último mês e no último ano, isto é possível por que o MRTG armazena os *logs* das informações dos equipamentos contendo as datas, dessa forma tornando a coleta de dados pontual, possibilitando a visualização diária, semanal, mensal ou anual das estatísticas geradas nos gráficos [7].

Para gerar um gráfico é preciso conhecer o identificador de objetos (*OID*) da variável que o agente responde. O MRTG não possui limite de equipamentos para se gerenciar, podendo monitorar qualquer variável *SNMP* como, por exemplo, a taxa de utilização do canal, média de utilização de modems e carga de CPU. Suas principais características são:

- Mede sempre dois valores, no caso de tráfego, pode ser entrada e saída;

- Faz as leituras via SNMP ou através de *script* que retorne um formato padrão;
- Coleta dados a cada 5 minutos por padrão, mas este tempo pode ser aumentado;
- Cria uma página HTML com quatro gráficos (diário, semanal, mensal e anual). Se algum deles não for necessário pode ser suprimido;
- O MRTG pode avisar caso o valor do gráfico atinja um valor pré-estabelecido. Por exemplo: se determinado servidor atinge 95% do espaço do disco, o MRTG pode mandar um e-mail para o administrador informando o ocorrido;
- Possui uma ferramenta para gerar os arquivos de configuração;
- Possui uma ferramenta para gerar um página de índice para os casos em que muitos itens são monitorados: o INDEXMAKER.

O MRTG é um *software* que oferece facilidade nas tarefas de monitoramento do funcionamento de um determinado sistema. Embora o seu foco seja o acompanhamento de componentes de rede através do protocolo SNMP, pode ser utilizado para verificar o funcionamento do seu PC ou estação de trabalho mesmo sem instalar o suporte a SNMP - basta usar a sua interface com *scripts* Shell [18].

É apresentado na Figura 11 um quadro comparativo das principais características dos quatro *softwares* abordados nesta seção.

Características	Vert-it	NTop	Nagios	MRTG
Auditoria	X	-	-	-
Gráficos	X	X	X	X
Relatórios	X		X	-
Inventário	X	-	-	-
Web browser	-	X	X	X
Multiplataforma	X	X	X	X
Software Livre	-	X	X	X
Deteção de erros	X	X	X	X
Banco de dados SQL	X	X	-	-

Figura 11: Quadro comparativo dos *softwares*.

4. Conclusões e Trabalhos Futuros

Analisando os pontos abordados sobre a Gerência de Redes, o uso de *softwares* para gerenciamento e a utilidade deles na tomada de decisão dentro das organizações, verifica-se a importância desses componentes para a solução de diversos problemas. Através do levantamento dos dados estatísticos fornecidos pelos *softwares* é possível perceber a necessidade dessas informações para o controle e monitoramento das redes de computadores.

Como trabalhos futuros sugere-se um estudo sobre os *softwares* de gerenciamento, focando

principalmente nos gráficos e dados estatísticos gerados no decorrer do monitoramento de cada *software*.

Agradecimentos

Os autores agradecem à professora Dra. Marcília Andrade Campos do CIN-UFPE – Centro de Informática da Universidade Federal de Pernambuco pela revisão e sugestões de melhoria deste trabalho.

Referências

- [1] A. Márcio Portes de, A. Marcelo Portes, R. Valeriana Gomes. Monitoramento do Protocolo RTSP (Real Time Streaming Protocol) utilizando NTop (Network Top).
- [2] A. F. Clayton. A. M. João Wesley. (Goiânia 2004). “Análise de protocolos na área de Gerência de Redes (SNMP/RMON). UFGO, Escola de Engenharia Elétrica e de Computação.
- [3] B. Wanderson. (2004). Nagios - Um poderoso programa de monitoramento de rede. Disponível em: <http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=595>.
- [4] C. Augusto C. (2004). MRTG sem SNMP: monitoramento simplificado. BR-Linux.org.
- [5] C. S. Victor, “Nagios: Gerenciamento de Redes”. 2007. Disponível em: <http://vicouto.wordpress.com/2007/07/01/nagios-gerenciamento-de-redes/>.
- [6] D. César A. Nagios – Configuração Básica e Monitoramento. Disponível em: <http://under-linux.org/wiki/index.php/Tutoriais/Monitoramento/nagios-basic>.
- [7] F. Cleyton Araújo e M. João W. Alves. Análise de Protocolos na área de gerência de redes (SNMP/RMON). Universidade de Goiás. Goiânia, 2004.
- [8] “Gerência de Redes”, Esmilda Saez Artola. Disponível em: http://penta.ufrgs.br/gr952/e_capa.html.
- [9] “Gerenciamento de Redes”, Lisandro Zambenedetti Granville. Disponível em: http://www.inf.ufrgs.br/granville/Gerencia/Programa/Mod1/Mod1_4.pdf.
- [10] iEvolution Fóruns. Conceitos Básicos de Gerenciamento de Redes. Disponível em: <http://forum.ievolutionweb.com/index.php?showtopic=4271>.
- [11] Interface Web do Nagios. Disponível em: <http://www.nagios.org/about/screenshots.php>.
- [12] Manual do Vert-It Administrator. Aprimorando a forma de administrar sua rede. Disponível em <http://www.vertsyst.com.br>.
- [13] Nagios – Visão Geral. Disponível em: <http://pt.wikipedia.org/wiki/Nagios>.
- [14] Ntop.org: <http://www.ntop.org/news.html>.
- [15] P. Mateus Casanova. Administração e Gerência de Redes de Computadores. (Florianópolis, 2001). Universidade Federal de Santa Catarina.
- [16] P. Eriko. (2005). “Gerência de Redes SNMP”. Redes de Computadores.
- [17] Projeto Software Livre (2004). Monitoramento e Segurança de Redes com Software Livre.
- [18] R. Vinícius de Miranda. Um Estudo sobre Ferramentas de Gerência de Redes IPv6. Centro Universitário Luterano de Palmas- ULBRA, 2005.
- [19] S. Madson da Silva, Estudo de Gerenciamento da Rede de Distribuição com o protocolo SNMP e Tutorial para implantação de ferramentas de gerência, Teresina –PI, 2006.
- [20] T. Andrew. Redes de Computadores. Quarta Edição. Editora Campus, 2003.
- [21] V. B. Tiago, (2004) “Monitoramento e Segurança de Redes com Software Livre”. UFBA. Disponível em: http://twiki.dcc.ufba.br/bin/view/PSL/SlidesCursoRedesEnecomp#Slide_4_Gerência_de_recursos_Nag.