SNMP

IGOR THIAGO MARQUES MENDONÇA

Curso de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Catarina
Campus Universitário – Trindade
88040-900 – Florianópolis – SC
Tel.: (48) 331.9738 Fax.: (48) 331.9566

RESUMO

O *Simple Network Management Protocol* (SNMP) é o protocolo mais utilizado para o gerenciamento de redes IP e internets. Em sua primeira versão, conhecida como SNMPv1, é largamente utilizada [1]. A versão dois (SNMPv2) implementou novas funcionalidades mas somente na três (SNMPv3) foram implementadas as questões de segurança. Este artigo apresenta inicialmente as necessidades do gerenciamento de redes. Apresenta também o modelo de gerência de redes SNMP descrevendo suas versões e implementações bem como as ferramentas utilizadas nessa tarefa que se tornou extremamente necessária devido ao crescimento das redes e do número de dispositivos de diversos fabricantes ao fim dos anos 80. Finalmente mostraremos o custo que esse gerenciamento acarreta para as redes de computadores.

1. INTRODUÇÃO

Devido ao crescimento e as expansões das redes de computadores, novas tecnologias e produtos foram implantadas. Assim muitas empresas sofreram as "dores" deste desdobrar de tecnologias diferentes e às vezes até incompatíveis. Estava criada a necessidade de gerenciar este emaranhado de cabos, computadores e dispositivos.

Poderíamos entender gerenciamento de redes como um "serviço" que emprega uma variedade de ferramentas, aplicações e dispositivos para manter e monitorar o funcionamento de redes de computadores cada vez mais heterogêneas.

O *Simple Network Management Protocol* (SNMP), proposto em 1988, foi concebido para fornecer fácil implantação e baixo custo para ser implantado nos diversos dispositivos de gerenciamento de redes como roteadores, HUBs, servidores, estações de trabalho, e outros dispositivos de rede. A especificação do SNMP define:

- Um protocolo para troca de informações entre um ou mais gerenciadores de sistema (gerentes) e um número de agentes.
- Um mecanismo para formatar e armazenar as informações de gerenciamento (MIB).
- Um número de objetos ou variáveis para manipular as informações.

A primeira versão do SNMP (conhecida como SNMPv1) transformou-se rapidamente no esquema de gerenciamento de redes e foi largamente utilizada [1], principalmente pela não existência de um modelo já bem definido. Entretanto, a sua larga utilização mostrou suas deficiências. Entre elas a impossibilidade de comunicação entre estações de gerenciamento, a inabilidade de transferência de dados complexos e os aspectos de segurança. As deficiências foram corrigidas nas versões dois e três em 1993 e 1997 respectivamente, conhecidas como SNMPv2 e SNMPv3.

O SNMPv2 na verdade não obteve aceitação, pois apesar de implantar algumas correções do SNMPv1, falhou em não implantar as deficiências nas questões de segurança. Então em 1997 foram trabalhadas as questões de segurança do protocolo SNMP, definindo-se a versão três (SNMPv3).

Este artigo examina o gerenciamento de redes, com ênfase no gerenciamento pelo protocolo SNMP. O artigo começa com uma introdução sobre as necessidades do gerenciamento de redes e apresenta o SNMP como um modelo de gerência de redes. A seguir apresenta as três versões do SNMP, conhecidas como SNMPv1, SNMPv2 e SNMPv3 e mostrar as definições deste modelo de gerência. Apresentarei algumas ferramentas comerciais, de domínio público e uma plataforma de desenvolvimento que utilizam SNMP para o propósito de gerenciamento e por fim, expor os custos para a rede gerados pelo protocolo SNMP.

2. GERENCIAMENTO DE REDES E O MODELO DE GERÊNCIA SNMP

Para facilitar o gerenciamento de redes a ISO (Internacional Organization for Standardization) definiu inicialmente as áreas de gerenciamento de redes e são elas: [11]

- Gerência de falhas: O objetivo principal da área funcional de gerência de falhas é detectar, isolar e corrigir falhas ou funcionamento anormal dos diversos dispositivos componentes do sistema de comunicação.
- Gerência de contabilização: Que provê meios para se medir e coletar informações a respeito da utilização dos recursos e serviços de uma rede, para saber qual a taxa de uso destes recursos garantindo que os dados estejam sempre disponíveis quando forem necessários.
- Gerência de configuração: Define o conjunto de funções que permitem a configuração remota através de um console gerente.
- Gerência de segurança: Oferece suporte ao monitoramento e controle de acesso, autorização e autenticação de máquinas e usuários e geração e análise de registros de segurança.
- Gerência de desempenho: Compreende duas categorias principais, monitoramento e controle. Monitoramento é a função que analisa a atividade na rede. A função de controle permite ao gerenciamento de desempenho fazer ajustes permitindo aumentar o desempenho da rede.

O modelo de gerência SNMP foi proposto para suprir as necessidades de gerenciamento do que seria futuramente a rede internet, ou seja, para funcionar sobre o conjunto de protocolo TCP/IP.

O SNMP é um protocolo de gerência utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP. [4]

O protocolo SNMP está situado na camada de aplicação, e como é um serviço, precisa caminhar pela pilha TCP/IP, este processo está ilustrado na Figura 1, então quando há uma mensagem na camada de aplicação do lado do cliente esta mensagem é repassada camada de transporte que estabelece a comunicação via protocolo UDP (User Datagram Protocol), depois repassada para a camada de rede, que irá endereçar e rotear esta mensagem, e por fim será repassada a camada física que é o meio por onde a mensagem será transmitida até o servidor.

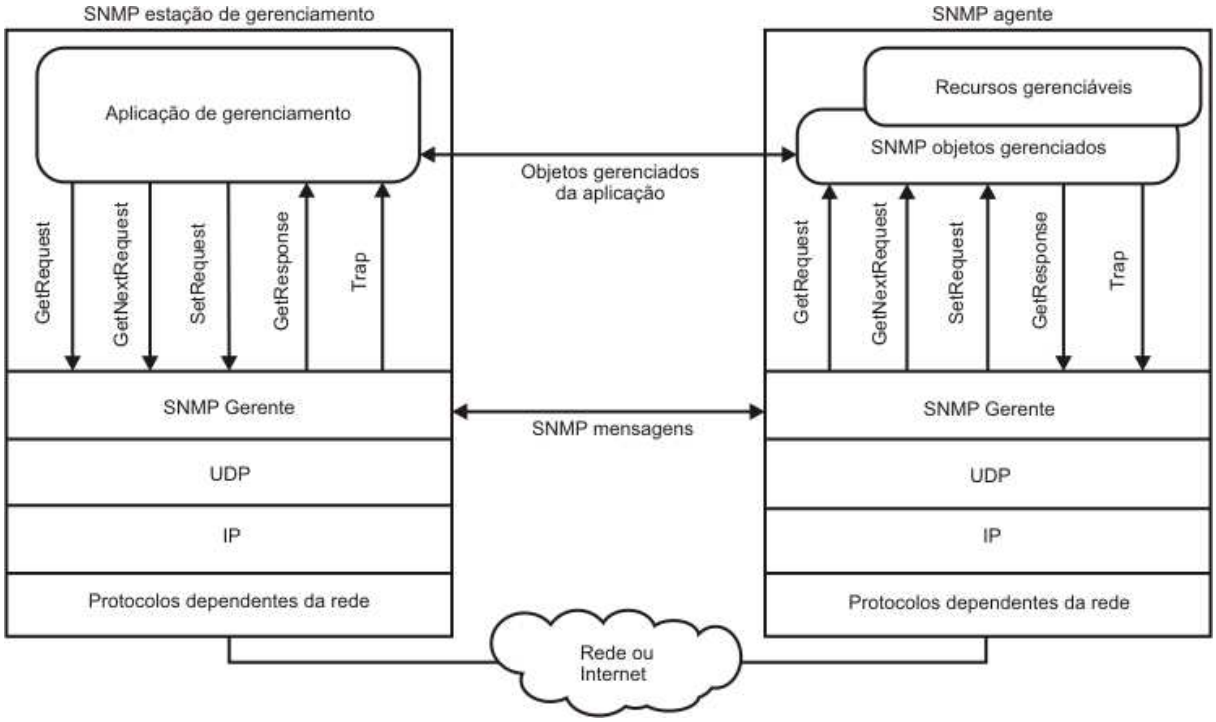

Figura 1 - SNMP na pilha TCP/IP.

O modelo de gerenciamento SNMP para redes TCP/IP, é composto pelos seguintes elementos [1], exibidos no diagrama de fluxo na Fig. 2:

- Gerente ou estação de gerenciamento: É onde está centralizada a interface de controle com os demais dispositivos da rede; nele devem estar às aplicações de gerenciamento e analise dos dados obtidos do agente remoto, deve também fornecer ferramentas de monitoramento e controle de tais dispositivos.
- Agente: processo responsável pela manutenção das informações de gerencia do dispositivo gerenciado; estes dispositivos gerenciados são comumente HUBs, roteadores, impressoras; são dispositivos equipados com um agente SNMP; eles estão aptos a responder requisições dos gerentes e podem conter um mecanismo de alarme (TRAP) para avisar ao gerente de algum evento ocorrido nele.
- MIB: Onde estão armazenadas as informações de estado do dispositivo, estes estados podem ser: configurações do dispositivo, informações de status do dispositivo ou dados estatísticos gerados no dispositivo; estes estados são representados como objetos e cada objeto é uma variável da MIB, que está identificado por sua localização. Pela complexidade da MIB, um capítulo foi escrito sobre ela.

O gerente faz o monitoramento requisitando dos agentes contidos nos dispositivos de rede as variáveis da MIB. Faz também configurações nos dispositivos através do envio de mensagens específicas. Os tipos de mensagens deste modelo de gerência são:

- Get: habilita o gerente buscar informações contidas nas MIBs dos agentes
- Set: habilita o gerente alterar variáveis das MIBs dos gerentes quando as mesmas têm permissão para tal operação.
- Trap: habilita o agente a notificação de eventos específicos ocorridos nele.

No modelo de gerenciamento SNMP, mesmo tendo os elementos bem definidos, e o SNMP estar na camada de aplicação da pilha TCP/IP, temos a ausência de uma interface para interação com o usuário final.

Figura 2 - Modelo de gerência SNMP

RFC		Data
1155	Structure and identification of management information for TCP/IP-based internets	Maio 1990
1157	Simple Network Management Protocol (SNMP)	Maio 1990
1212	Concise MIB definitions	Março 1991
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	Março 1991

Tabela 1 - RFCs que definem o SNMPv1.

3. VERSÕES DO SNMP

3.1. SNMPv1

O SNMPv1 é definido pelas RFCs mostradas na Tabela 1. O SNMP surgiu juntamente com o crescimento das redes TCP/IP no final dos anos 80.

No SNMP a informação é trocada entre a estação de gerenciamento e o agente no formato de mensagens. Cada mensagem SNMP tem em sua composição o número de sua versão, neste modelo de gerenciamento as versões diferentes não se comunicam, tem também o nome da comunidade usada para a troca de mensagens, que habilita uma mesma rede utilizarem o mesmo padrão de gerenciamento com dispositivos distintos e uma área de dados, onde está dividida dentro do PDU (Protocol Data Units). Existem cinto tipos de PDUs e são eles: get-request, get-next-request, get-response, set-request e trap.

Diferentemente de outros protocolos do TCP/IP, as mensagens SNMP não têm um tamanho fixo [3], elas são codificadas usando o padrão ANS.1. A Fig. 3 é um exemplo de uma mensagem SNMP.

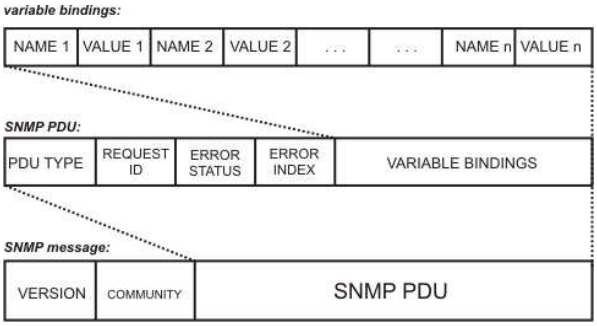

Figura 3 – Mensagem SNMP

Os tipos get-request e get-next-request são comandos onde o gerente solicita ao agente alguma informação contida em sua MIB. A diferença entre os dois comandos é que no primeiro, get-request, o gerente obtém diretamente o valor de uma variável, enquanto no segundo, get-next-request, é utilizado para navegar dentro de uma estrutura de arvore a qual é composta a MIB como veremos mais adiante. Para os dois tipos de mensagens enviadas, o retorno do agente será uma mensagem do tipo get-response. O tipo de mensagem set-request é utilizado pelo gerente para atualizar algum parâmetro na MIB do agente e por último o tipo de mensagem trap é utilizada pelo agente para notificar o gerente de algum evento ocorrido nele. Por questões de economia e simplicidade, existem somente dois formatos para mensagens [1] [4]. Um onde entra a mensagem de trap e outro onde entram os outros tipos de mensagens.

3.1.1 Transmissão de mensagens SNMP

As ações que uma entidade SNMP desenvolve para transmitir um dos cinco tipos de mensagem para outra entidade SNMP são:

- Construção do PDU;
- Este PDU é passado para o serviço de autenticação juntamente com o endereço do remetente e do destinatário; este serviço faz todos os ajustes para que seja feita a troca de mensagens;
- O protocolo então constrói uma mensagem contendo a versão do SNMP o nome da comunidade e os dados gerados no passo anterior.
- A mensagem então é passada para a camada de transporte do TCP/IP.

3.1.2 Recepção de mensagens SNMP

As ações que uma entidade desenvolve quando recebe uma mensagem SNMP são:

- Checar a sintaxe básica da mensagem e caso encontre falha a mesma é descartada.
- Verifica a versão do SNMP, caso seja incompatível também descarta a mensagem.
- O protocolo passa então a mensagem para o serviço de autenticação que poderá fazer proceder das seguintes maneiras:
    - Se a autenticação falha, um trap é gerado e enviado ao remetente e a mensagem é discartada.
    - Em caso de autenticação com sucesso é repassada a PDU.
- O protocolo faz uma checagem se sintaxe e caso ocorra falha descarta a mensagem. Caso contrário se a comunidade está correta ele dá continuidade no processamento da mensagem.

3.2. SNMPv2

O SNMPv1 proliferou-se rapidamente, pois surgiu como uma ferramenta simples para gerenciamento de redes. A primeira versão ofereceu funções de fácil implementação, fácil uso e sua simplicidade não prejudica o desempenho da rede. Após o início dessa utilização pelos administradores de redes, notaram-se algumas falhas e a necessidade de novas funcionalidades. Entre elas a necessidade da transferência de dados complexos, a comunicação entre gerentes e questões de segurança. As duas primeiras necessidades foram implementadas na SNMPv2, como mostradas na Tabela 2.

RFC		Data
1901	Introduction to Community-based SNMPv2.	Janeiro 1996
1902	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	Janeiro 1996
1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework.	Janeiro 1996

Tabela 2 - RFCs que definem as mudanças para o SNMPv2

3.2.1 Transmissão de dados complexos

A implementação da transmissão de dados complexos no SNMPv2, obteve um impacto positivo no quesito de consumo de recursos da rede, pois na versão anterior, caso fosse necessário a transferência de uma tabela de dados, a transferência se daria mensagem a mensagem até que todos os elementos fossem transferidos, o que na implementação do SNMPv2 não é mais necessário, o comando get-bulk foi implementado para suprir essa necessidade. Um exemplo da utilização desse novo comando seria um gerente solicitado a um agente alocado em um roteador a sua tabela de roteamento.

3.2.2 Gerenciamento descentralizado de redes

Quando uma rede cresce enormemente tanto em dispositivos conectados a ela e quanto ao trafego que por ela passa, o gerenciamento centralizado já não é o mais ideal, pois só um gerente teria que lidar com todos os dispositivos e tanto o tráfego por ele gerado seria alto como também este gerente precisaria realizar muitas tarefas. No SNMPv2, com a adição do suporte a comunicação manager-to-manager, ou seja, comunicação entre estações de gerenciamento, uma abordagem de gerenciamento descentralizado poderia ser adotado.

3.3. SNMPv3

O SNMPv2 supriu várias deficiências da sua versão antecessora, mas não uma muito importante: segurança. As questões de segurança foram implementadas somente no SNMPv3. Esta versão consiste em três módulos: processamento e controle das mensagens, o processamento local e o módulo de segurança.

O primeiro módulo, processamento e controle das mensagens é responsável pelas funções de criação e análise gramatical das mensagens, o segundo módulo, processamento local é responsável pelo controle de acesso às variáveis da mensagem, faz o processamento desses dados e é responsável pelas processamento das traps e por último o módulo de segurança tem as função de criptografia e autenticação das mensagens.

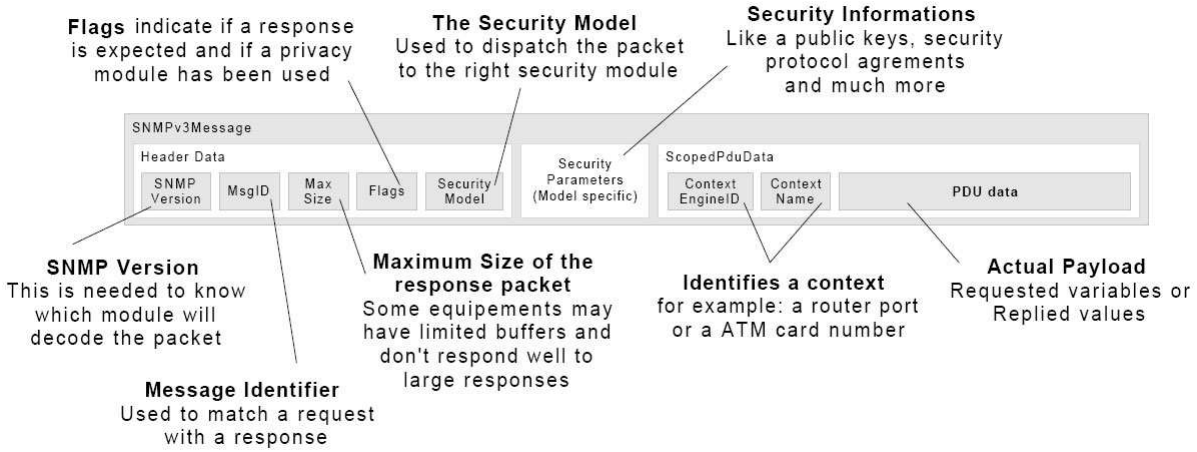

Figura 4 – Modelo de mensagem SNMPv3

As características de segurança implementadas pelo SNMPv3 são: autenticação, criptografia e controle de acesso [1]. Para esta nova versão, um formato de mensagem diferente foi adotado como visto na Figura 4.

4. MIB (MANAGEMENT INFORMATION BASE)

A MIB é um dos principais componentes da arquitetura do SNMP. Ela é uma base de dados, cuja estrutura é especificada pelo padrão SMI (Structure of Management Information), trabalha com objetos gerenciáveis que são visões abstratas de um recurso real do sistema. Estes objetos são os recursos da rede que devem ser monitorados, por exemplo: consumo de banda, status de operação do dispositivo, colisão de pacotes, ...

São permitidas operações de leitura e escrita nestas bases de informações.

A estrutura deste componente foi definida pela RFC 1066, em forma de árvore hierárquica, mostrada na Figura 5, onde cada objeto tem seu identificador conforme sua posição na árvore. A RFC 1213 introduziu com a MIB-II as funcionalidades para o gerenciamento de redes TCP/IP e foi nela que parâmetros como número de pacotes transmitidos, estados da interface entre outras foram implementados, a Tabela 3 mostra as implementações da MIB-II por grupos e o que eles contêm.

Alguns nós dessa árvore foram reservados para o uso, por exemplo, da IAB (International Activities Board) [4]. Os nós que acho importante destacar são o experimental, que é utilizado pela IAB para testes e novas implementações da tecnologia SNMP, o private que está disponível para que os fabricantes dos dispositivos possam implementar funcionalidades que não estão definidas na MIB-II ou que sejam característicos somente do dispositivo e é claro a MIB-II que é responsável pelo gerenciamento de redes TCP/IP.

Grupo	Informação
system(1)	informações básicas do sistema
Interfaces(2)	informações da rede
at(3)	tradução de endereço
ip(4)	protocolo ip
icmp(5)	protocolo icmp
tcp(6)	protocolo tcp
udp(7)	protocolo udp
egp(8)	protocolo egp
transmission(10)	meios de transmissão de dados
snmp(11)	protocolo snmp

Tabela 3 – Grupos da MIB-II

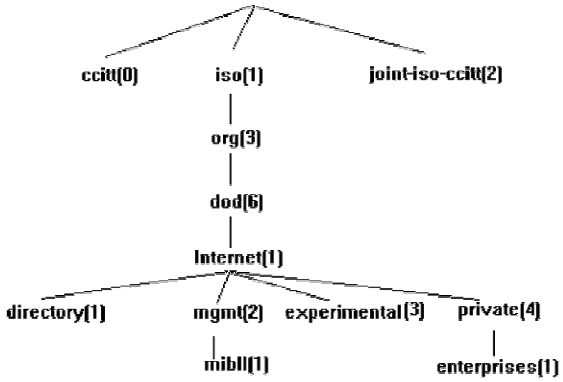

Figura 5 – Estrutura de árvore hierárquica da MIB

5. INTERFACES PARA O ADMINISTRADOR

Como dito anteriormente, o SNMP não define a interface de comunicação entre o administrador e a estação de gerenciamento. Existem várias ferramentas desenvolvidas e em desenvolvimento. Abordarei neste capítulo, divido em três sub-capítulos, ferramentas de interface comerciais, open source e uma plataforma de desenvolvimento de comunicação para uma estação de gerenciamento.

5.1. Ferramentas comerciais

As ferramentas comerciais são normalmente, de fácil instalação e utilização. A ferramenta que vou comentar leva o codinome de PRTG Traffic Grapher e é desenvolvida pela empresa alemã PAESSLER [7]. A versão avaliada é de idioma inglês, é distribuída como freeware para monitoramento de somente um objeto SNMP, ou comercialmente para o monitoramento de toda uma rede. É um programa para instalação em sistemas operacionais Windows. Ele denomina os objetos gerenciáveis como sensores, onde o administrador pode adicionar os sensores que deseja monitorar e qual o período entre cada requisição. Gera gráfico em tempo real, como mostrado na Figura 6. Assim como o PRTG, cito o HP Open View e o What'up Gold como ferramentas comerciais.

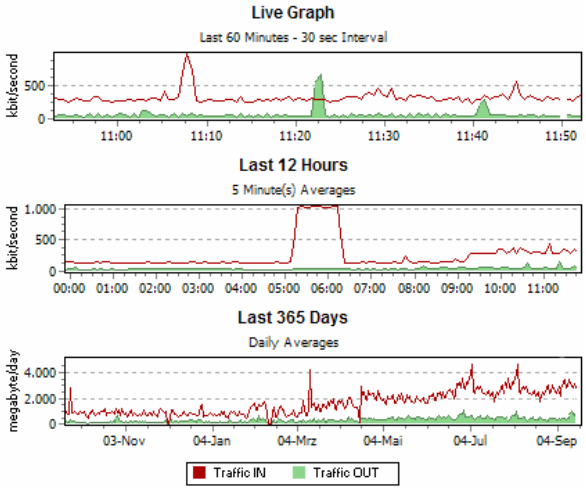

Figura 6 – Gráficos gerados pelo PRTG

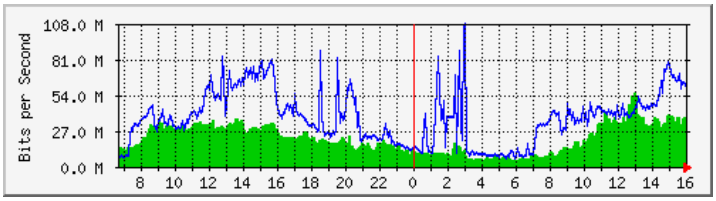

Figura 7 – Gráfico gerado pelo MRTG

5.2. Ferramentas Open Source

A ferramenta avaliada, MRTG (Multi Router Trafig Grapher), foi desenvolvida em C e Perl para acessar as variáveis de tráfego nos dispositivos gerenciáveis. Com os dados obtidos ele constrói gráfico, mostrado na Figura 7, e disponibiliza no formato de páginas para a internet. Assim como a maioria dos programas, faz gráficos diários, semanais, mensais e anuais. A distribuição deste programa é feito sobre os termos da GNU (General Public License) e existem distribuições para sistemas operacionais baseados em Unix e Windows. A instalação desse software não é muito simples, pois tem várias dependências tanto de bibliotecas e compiladores para instalar ele, quanto à configuração do sistema para que ele funcione adequadamente. O seu site tem toda a documentação necessária para fazer as instalações seja no ambiente Unix ou Windows [6]. Outra ferramenta open source existente é o cacti, que é na verdade um front-end para o RRDTool, e utiliza o MySQL para guardar as informações e PHP para manipulação dos dados.

5.3. Ambiente de desenvolvimento

O ambiente avaliado foi o PHP. Esta linguagem apresenta comandos para a implementação das estações de gerenciamento, mas têm como pré-requisito a instalação do NET-SNMP que é um conjunto de aplicações que implementam as três versões do SNMP [8]. Através destes comandos implementei, como mostrado na Figura 8, a requisição de dados do agente SNMP mostrando o nome do dispositivo e fazendo alguns cálculos a partir de objetos gerenciáveis desse dispositivo.

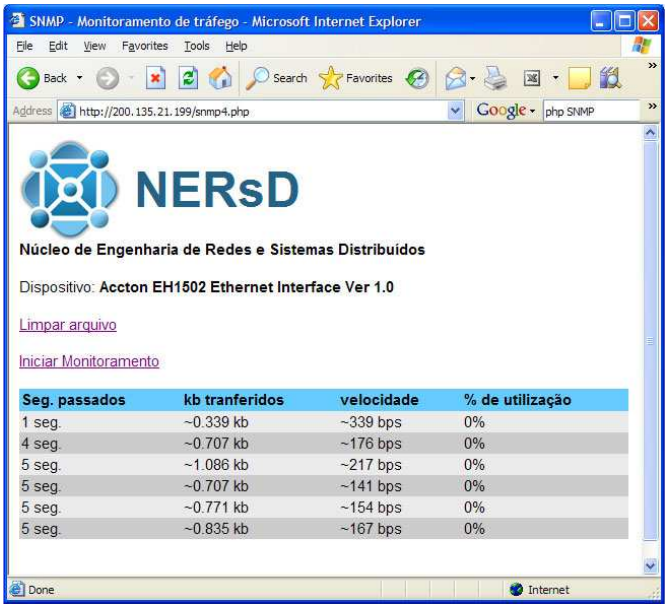

Figura 8 – Implementação usando PHP

4. CONCLUSÕES

O modelo de gerenciamento SNMP para redes é a maneira mais eficaz e produtiva de se fazer o gerenciamento de uma rede TPC/IP, proporcionando a centralização das informações agregou imensa facilidade para os gerentes de rede, fazendo com que, somente em um local, ele pudesse gerenciar toda uma rede fisicamente separada. Desde a primeira versão, este modelo foi adotado pelos fabricantes de dispositivos e utilizado pelos gerentes de rede. As versões posteriores a primeira versão vieram para corrigir e melhorar as funcionalidades desse modelo de gerenciamento.

O consumo de recursos da própria rede que o SNMP gerencia é pequeno já em sua primeira versão e nas versões posteriores são ainda menores devido as novas implementações que visaram tal requisito.

Dentre as vantagens do protocolo estão [9]: simplicidade, visto nos poucos modos de operações, extensibilidade, pois as MIBs podem ser alteradas para adequação de novas realidades, centralização de informações onde o gerente tem domínio de todos os dispositivos da rede de um único ponto, interoperabilidade entre equipamentos de fabricantes diferentes e por ser relativamente simples um agente pode ser implementado em diversos dispositivos. Das desvantagens: O protocolo não define programas de interface com o gerente, insegurança na troca de mensagens, pois ao mesmo tempo em que a utilização do protocolo UDP o torna mais leve também o torna inconfiável, MIBs proprietárias dificultam o desenvolvimento das aplicações de interface, pois para cada equipamento o fabricante pode definir a sua.

Vislumbrei também que esse modelo de gerenciamento é facilmente portável para outras aplicações que não o gerenciamento de redes TCP/IP como, por exemplo, o gerenciamento de dispositivos de medição de energia elétrica, devido ao baixo custo para a criação de agentes para outros dispositivos. Existem também outras aplicações baseadas nesse modelo como a do Seti@Home [10], onde dentre outros é monitorado a quantidade de processadores que no momento estão trabalhando em prol deste projeto.

5. BIBLIOGRAFIA

[1] W. Stallings, SNMP and SNMPv2: The Infrastructure for Network Management, IEEE Communications Magazine, março de 1998.

[2] A. Pras, T. Drevers, R. v.d. Meent, D. Quartel, Comparing the Performance of SNMP and Web Services-Based Management, IEEE eTNSM (Transactions on Network and Service Management), Vol.1 No.2 December 2004, 11 pages.

[3] D. Commer, Internetworking with TCP/IP – Chapther 26 Internet Management, 3rd ed., Editora Pratience-Hall do Brasil, Ltda. Rio de Janeiro, 1995, pp 447-463.

[4] B. Z. Dias, N. Alves Jr., Protocolo de Gerenciamento de Redes, Centro Brasileiro de Pesquisas Físicas, Julho 1992, 17 páginas.

[5] O. Cherkaoui, Y. S. Hillaire, H. Mili, A. Obaid, The modularity of SNMPv3, Computers and Communications, 1998. ISCC '98. Proceedings. Third IEEE Symposium on 30 June-2 July 1998 Page(s):120 - 124

[6] http://www.mrtg.org

[7] http://www.paessler.com/prtg

[8] http://www.net-snmp.org

[9] K. Amirthalingam, R. J. Moorhead, SNMP-an overview of its merits and demerits, System Theory, 1995., Proceedings of the Twenty-Seventh Southeastern Symposium on 12-14 March 1995 Page(s): 180 - 183

[10] http://home.lordrich.com/mrtg

[11] M. A. Schults, Protótipo de Software de Gerência de Desempenho de um Access Point de Rede Sem Fio Utilizando o Protocolo SNMP: Capítulo 4 – Gerenciamento de Rede, Trabalho de Conclusão de Curso Submetido à Universidade Regional de Blumenau.