Caracterização de Padrões de Uso do Protocolo SNMP*

Ewerton Monteiro Salvador[1], Jussara M. Almeida[1], José Marcos Silva Nogueira[1], Lisandro Zambenedetti Granville[2], Paulo Eduardo Barbosa[2]

[1] Departamento de Ciência da Computação
Universidade Federal de Minas Gerais (UFMG)
Av. Antônio Carlos, 6627 – ICEx – Belo Horizonte, MG

{ewerton, jussara, jmarcos}@dcc.ufmg.br

[2]Instituto de Informática
Universidade Federal do Rio Grande do Sul (UFRGS)
Av. Bento Gonçalves, 9500 – Porto Alegre, RS

{granville, pauloctb}@inf.ufrgs.br

Abstract. *The Simple Network Management Protocol (SNMP), proposed almost 20 years ago, still remains as the de facto standard for managing of TCP/IP networks. However, there are few studies that present the real use of SNMP in production networks. This work aims at contributing with the efforts carried out by the network management community in order to improve the knowledge about the use of SNMP by presenting the characterization results of a sample of the management traffic from the Brazilian RNP network. The presented results may guide the development of new technologies for managing networks, in order to better meet the needs of the production networks users.*

Resumo. *O Simple Network Management Protocol (SNMP), proposto há quase 20 anos, continua sendo o padrão de facto para gerenciamento de redes TCP/IP. Contudo, ainda são poucos os estudos que descrevem a real utilização do SNMP em redes em produção. Visando contribuir com os esforços da comunidade de gerenciamento de redes para melhorar a compreensão da utilização do protocolo, este trabalho apresenta os resultados da caracterização de uma amostra do tráfego de gerenciamento da RNP, no Brasil. Os resultados apresentados podem direcionar o desenvolvimento de novas tecnologias para o gerenciamento de redes, a fim de melhor atender as necessidades dos usuários das redes em produção.*

1. Introdução

Na última década, um conjunto de novos estudos estão sendo conduzidos na área de gerenciamento de redes a fim de investigar o quão adequadas são as técnicas de gerenciamento existentes frente às características atuais das redes de computadores. Dentre os resultados que vêm sendo alcançados a partir desses estudos, destacam-se aqueles que buscam descentralizar a tarefa de gerenciamento de redes, seja utilizando tecnologias alternativas, como Web Services [Curbera et al. 2002] ou redes P2P

*Os autores deste artigo agradecem o apoio fundamental do CNPq, da FAPEMIG e da CAPES para a realização deste trabalho, assim como a disponibilidade da RNP para o fornecimento da amostra de tráfego SNMP aqui estudada.

[Androutsellis-Theotokis and Spinellis 2004], ou criando novos modelos, como o modelo de gerenciamento por delegação [Goldszmidt and Yemini 1995] ou o modelo de gerenciamento baseado em políticas [Westerinen et al. 2001]. Contudo, o padrão *de facto* para gerenciamento de redes TCP/IP continua sendo o *Simple Network Management Protocol* (SNMP) [Case et al. 1990], o qual foi proposto há quase 20 anos e permanece sendo amplamente utilizado.

Diversas publicações recentes têm por objetivo principal a identificação de padrões de utilização do SNMP por meio de medições de tráfegos de gerenciamento de redes em produção. A principal motivação por trás desses estudos é o fato de que ainda hoje pouco se conhece sobre a forma como o SNMP é efetivamente utilizado em redes reais. Este fato é prejudicial para a comunidade de gerenciamento de redes como um todo, pois a falta desse conhecimento leva os pesquisadores e desenvolvedores a fazerem pressuposições sobre o comportamento do protocolo, o que enfraquece a base sobre a qual novas tecnologias estão sendo propostas e desenvolvidas. Atualmente, já existe uma metodologia bem definida para a realização desse tipo de estudo [Schoenwaelder 2008], e alguns interessantes resultados preliminares já foram publicados em veículos relevantes [Schönwälder et al. 2007] [Salvador and Granville 2008a] [Salvador and Granville 2008b]. Exemplos de questões que estão sendo investigadas são: quais recursos do SNMP (ex.: versões, operações, MIBs - *Management Information Bases*) estão sendo utilizados; como o uso do SNMP difere nos vários tipos existentes de redes das organizações; quais informações são mais frequentemente requisitadas e quais são as interações mais típicas que estão sendo empregadas? Contudo, os resultados conhecidos até o presente momento não são exaustivos, e uma série de características acerca da utilização do SNMP demandam investigações mais profundas a fim de se alcançar resultados mais concretos, tais como: identificação de componentes periódicos e aperiódicos nos tráfegos, correlações existentes entre tipos de mensagens distintos com possíveis relações causa-efeito, potencial para otimização do consumo de banda e do balanceamento de carga do tráfego de gerenciamento, aplicações reais para o uso de *traps*, entre outras.

Neste contexto, este trabalho objetiva contribuir com novos resultados acerca da utilização do SNMP nas redes em produção. Para tanto, foi estudado um tráfego de gerenciamento SNMP da Rede Nacional de Ensino e Pesquisa (RNP). Uma série de técnicas de análises quantitativas foram empregadas sobre uma amostra do tráfego, a fim de se caracterizar a utilização do SNMP quanto a aspectos tais como periodicidade de diversos componentes do tráfego, correlações entre tipos de mensagens encontradas nos diversos dias de tráfego monitorado, relação entre o uso de traps e os eventos ocorridos na rede dentro da amostra de tráfego coletada e níveis de centralização do tráfego de gerenciamento da RNP.

O restante deste artigo está organizado da seguinte maneira. A Seção 2 apresenta os trabalhos que estão relacionados a este artigo. Já a Seção 3 destaca o conjunto de técnicas que compuseram a metodologia empregada para as medições sobre o tráfego da RNP estudado, enquanto que a Seção 4 detalha os resultados que foram obtidos a partir do estudo realizado. Por fim, a Seção 5 apresenta conclusões e trabalhos futuros.

2. Trabalhos relacionados

Devido ao fato da metodologia proposta pelo IRTF (*Internet Research Task Force*) para medições de tráfegos SNMP ser relativamente nova, atualmente existem poucos trabalhos contendo resultados acerca dos padrões de utilização do protocolo de gerenciamento nas redes em produção. O primeiro artigo relacionado a este tema foi publicado em 2007, pelo próprio autor da metodologia do IRTF, em parceria com outros pesquisadores [Schönwälder et al. 2007] e consistiu numa coletânea de resultados preliminares de medições realizadas sobre oito tráfegos SNMP coletados. Dentre as principais conclusões do trabalho, encontram-se os fatos de que o SNMP é utilizado primeiramente para monitoramento e não para configuração e que, apesar de o SNMPv3 ser o padrão atual para gerenciamento de redes TCP/IP, o mesmo foi pouco visto nos tráfegos estudados.

Já em 2008, foi publicado o trabalho de Salvador e Granville [Salvador and Granville 2008a], no qual foram realizadas algumas medições sobre uma amostra do tráfego de gerenciamento do Ponto-de-Presença (POP) da Rede Nacional de Ensino e Pesquisa (RNP) no Rio Grande do Sul. No mesmo ano, um novo trabalho [Salvador and Granville 2008b] foi publicado por esses mesmos autores, onde a amostra de tráfego estudada foi a da Rede Nacional de Pesquisa (RNP) como um todo, ao invés de apenas um POP (caso da publicação anterior). Uma característica comum desses dois trabalhos é que os mesmos tinham como foco principal um conjunto de propostas de técnicas de visualização para serem utilizadas em conjunto com a metodologia proposta pelo IRTF, a fim de facilitar o processo de interpretação dos resultados obtidos a partir das medições realizadas sobre um tráfego SNMP. Nesse contexto, as análises realizadas sobre os tráfegos do POP da RNP no Rio Grande do Sul e da própria rede da RNP como um todo tiveram por objetivo principal validar as técnicas de visualização proposta. Devido a isso, os tráfegos estudados nos trabalhos anteriores ainda não foram extensivamente analisados, fato este que consiste numa interessante oportunidade de pesquisa que está sendo explorada no presente artigo.

Em 2009 os pesquisadores Dobrev e Stancu-Mara [Dobrev et al. 2009], em colaboração com o autor da metodologia do IRTF, Schoenwaelder, passaram a investigar técnicas de visualização que melhor representassem a interação entre nós presentes num determinado tráfego de gerenciamento SNMP. Nesse trabalho, foram avaliadas a utilização de duas ferramentas de visualização (*network animator* - nam, e NetViz/JUNG) em conjunto com tráfegos SNMP representados nos formatos definidos pela metodologia do IRTF para medições de tráfegos SNMP. Esse trabalho se relaciona com o presente artigo no que diz respeito à constante busca pela identificação de padrões de utilização através de análises sobre tráfegos de gerenciamento de redes.

3. Metodologia utilizada nas medições sobre o tráfego SNMP

Para a realização das medições sobre o tráfego SNMP da Rede Nacional de Ensino e Pesquisa (RNP), foram utilizadas a metodologia do IRTF para medições de tráfegos SNMP [Schoenwaelder 2008] e um conjunto de técnicas de análise quantitativa. Os quatro primeiros passos citados na metodologia do IRTF já foram previamente realizados, sendo eles: captura do tráfego de gerenciamento, conversão dos arquivos PCAP para o formato CSV (*Comma Separated Values*), filtragem dos arquivos CSV para remoção de dados sensíveis (ex.: *strings* de comunidade e endereços IP de gerentes e agentes) e armazenamento dos arquivos PCAP e CSV em um repositório estável para os casos em que um

retorno aos dados originais seja necessário. Os esforços dos quais este artigo é resultante foram concentrados no quinto passo da metodologia do IRTF, que consiste na realização de análises sobre o arquivo de tráfego no formato CSV, através da execução de programas e *scripts*, a fim de se caracterizar a utilização do protocolo SNMP nas redes em produção.

Objetivando-se compreender os padrões de utilização do SNMP na rede de gerenciamento da RNP, as seguintes métricas foram selecionadas: distribuição dos diversos tipos de mensagens de gerenciamento trocadas entre gerentes e agentes da rede, distribuição de acessos a objetos e MIBs utilizados e periodicidade do tráfego de gerenciamento. A escolha das mesmas se deu pela grande quantidade de informações acerca do uso do SNMP no tráfego estudado que pode ser obtida a partir desse conjunto de métricas. Como exemplo citam-se: pontos de concentração de tráfego de gerenciamento na rede, justificativas para o uso das diversas operações encontradas no tráfego identificadas a partir das informações acessadas nos agentes da rede, componentes periódicos e aperiódicos na distribuição das operações realizadas pelo SNMP na rede da RNP, entre outros.

Com relação às técnicas de análise quantitativa empregadas no estudo do SNMP na RNP, foi feita uma caracterização do tráfego estudado, apresentando as distribuições dos números dos diversos tipos de mensagens SNMP presentes no tráfego, tais como *get-request*, *response*, *get-next-request*, *trap*, entre outras. Foram ainda analisadas as correlações entre os números de mensagens de cada tipo e o número de mensagens de mesmo tipo em diferentes dias em que houve monitoramento de tráfego na rede da RNP.

Conforme já mencionado anteriormente, a carga de trabalho escolhida para a execução das análises foi o tráfego de gerenciamento SNMP da RNP. Esse tráfego é o produto de 14 dias de monitoramento no núcleo da rede da instituição, ocorrido entre os dias 22 de junho e 5 de julho de 2007. Uma vez que os autores deste trabalho já tinham a disposição essa amostra de tráfego, a mesma foi selecionada, também, devido à sua disponibilidade, além do fato da mesma ser representativa no cenário brasileiro de redes de computadores. As características gerais do tráfego SNMP são apresentadas na Tabela 1.

Tabela 1. Características gerais da amostra de tráfego estudada

Início da amostra:	2007-06-22T22:10:03+0000
Fim da amostra:	2007-07-06T22:10:56+0000
Duração do trace:	14 dias 0 horas 0 minutos
Quantidade de mensagens:	30.674.350
Quantidade de gerentes:	6
Quantidade de agentes	100

Uma particularidade a ser mencionada nesse tráfego é a pequena quantidade de mensagens capturadas no segundo dia do monitoramento (23 de junho de 2007). Isso ocorreu devido a um problema durante o processo de captura dos pacotes SNMP, ocasionando o corrompimento do arquivo PCAP (resultante da captura de pacotes pelo *sniffer* de rede). Contudo, esse estudo considera todas as mensagens SNMP capturadas neste dia e que não foram corrompidas por esta falha, a fim de se extrair o máximo da amostra obtida.

4. Resultados

Os resultados obtidos a partir da presente pesquisa serão detalhados nas próximas subseções da seguinte forma: primeiramente serão apresentados dados sobre o uso do SNMP na rede da RNP de um modo geral. Em seguida, serão caracterizadas as diversas operações do SNMP que foram observadas na amostra estudada. Por fim, serão discutidas as correlações percebidas entre as diversas operações do protocolo.

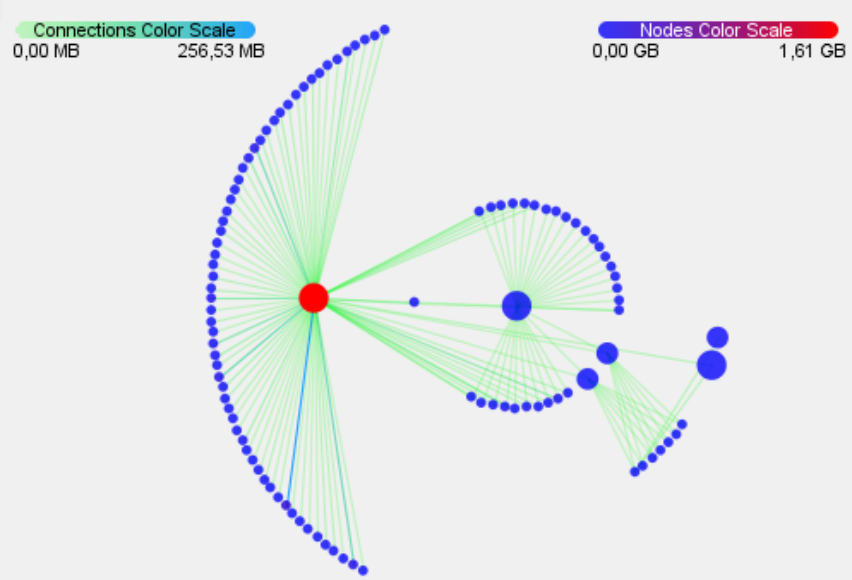

Figura 1. Topologia de gerenciamento SNMP da rede da RNP

Na Figura 1, onde é apresentada a topologia de gerenciamento percebida na RNP, pode-se notar que a maior parte do tráfego de gerenciamento está concentrado em torno de um único gerente, o qual encontra-se colorido de vermelho por concentrar a maior quantidade de tráfego. Todo o tráfego desse gerente principal consiste exclusivamente de mensagens de polling do protocolo SNMP (`get-request`, `get-next-request`, `get-bulk-request` e `response`). As mensagens do tipo `trap` estão todas concentradas no segundo maior gerente da rede, que está representado na figura como o círculo grande azul imediatamente à direita do gerente principal. Esse gerente também é exclusivamente utilizado para lidar com mensagens do tipo `trap`. Os demais fluxos de mensagens são menos representativos, muito provavelmente porque os mesmos tiveram uma participação esporádica no processo de gerenciamento da rede da RNP ao longo dos dias em que houve monitoramento. Assim, a caracterização do tráfego é focada principalmente no tráfego concentrado nesses 2 principais gerentes da rede e os agentes interconectados a esses nós.

4.1. Distribuição da quantidade de mensagens no tráfego

Um dos *scripts* de análise que acompanham a ferramenta SNMPDUMP [Schoenwaelder 2008], utilizada na conversão de formatos de tráfego na metodologia do IRTF, gera um relatório apresentando a distribuição do número dos vários tipos de mensagens e também as versões utilizadas do protocolo SNMP. Esse *script* foi executado sobre todo o tráfego da RNP monitorado, a fim de se obter uma visão geral da distribuição das mensagens de gerenciamento. O resultado obtido está representado na Tabela 2.

Tabela 2. Tipos e versões das mensagens no tráfego da RNP

Tipo de mensagem	Versão do SNMP	Quantidade
get-request	SNMPv1	940.491
get-request	SNMPv2c	11.574.343
get-next-request	SNMPv1	2.154.137
get-next-request	SNMPv2c	7.032
get-bulk-request	SNMPv2c	774.570
trap	SNMPv1	6.614
trap	SNMPv2c	107.977
response	SNMPv1	2.777.042
response	SNMPv2c	12.332.123

Nota-se que não foram observadas mensagens SNMPv3 no tráfego analisado. A explicação mais provável para isso é a ausência de implementação desta versão do SNMP na maioria dos dispositivos de rede disponíveis na rede da RNP. Outro fato interessante é o baixo uso de *traps* no tráfego estudado, em comparação com as outras operações observadas. Isso mostra uma subutilização de um recurso com potencial para reduzir substancialmente a sobrecarga causada pelo tráfego de gerenciamento, através da substituição da técnica de *polling*, com requisições e respostas constantes, pela técnica de notificação. Por fim, é fácil identificar que a versão predominante do SNMP no tráfego estudado é a SNMPv2c, que por sua vez está presente na maioria dos atuais dispositivos de redes com capacidade de gerenciamento disponíveis no mercado. Apesar da versão 2 do protocolo SNMP já disponibilizar formas de reduzir a quantidade de mensagens de *polling* na rede, com a introdução da operação `get-bulk-request`, existe o lado negativo de uma grande deficiência na segurança das operações realizadas através do protocolo, que só foram sanadas na versão 3 do mesmo.

4.2. MIBs e sub-árvores mais acessadas no tráfego

Através da execução de um *script* específico, observou-se também a distribuição de acessos a objetos de gerenciamento e MIBs SNMP ao longo de todo o tráfego monitorado. Na Tabela 3 estão listadas as 10 MIBs e suas respectivas sub-árvores de objetos mais acessadas no tráfego estudado. O objetivo desta análise também foi permitir uma melhor compreensão das características básicas do tráfego, a fim de se adequar melhor as técnicas empregadas.

A partir dos dados da Tabela 3 pode-se observar que a maior parte dos acessos são a objetos da `MIB-2`, que é uma MIB padronizada pelo IETF. Nesta MIB, a sub-árvore mais acessada é a `interfaces`, que fornece informações sobre o estado da interface de rede do dispositivo monitorado, o que indica que provavelmente está se realizando *polling* sobre esses dispositivos para se saber o estado de funcionamento dos mesmos. Nota-se também que algumas MIBs não padronizadas também estão sendo utilizadas, como a `enterprises/cisco` e a `enterprises/ucd-snmp`, o que demonstra que nem sempre administradores optam por utilizar MIBs padronizadas em detrimento das MIBs fornecidas pelos fabricantes dos dispositivos utilizados.

Tabela 3. MIBs mais acessadas no tráfego da RNP

MIB/Sub-árvore	Número de Acessos
mib-2/interfaces	28.478.953
mib-2/ifMIB	8.427.996
mib-2/system	2.943.137
mib-2/ip	2.740.604
enterprises/cisco	902.246
enterprises/ucd-snmp	856.915
enterprises/2636	721.492
mib-2/bgp	331.264
snmpModules/snmpMIB	168.933
mib-2/ospf	149.936

4.3. Caracterização das operações do SNMP na rede da RNP

A partir desta subseção serão detalhadas algumas características do uso das operações do SNMP na rede da RNP, a partir da análise das distribuições das mensagens ao longo da amostra de tráfego estudada. As distribuições foram organizadas de duas formas distintas: uma leva em consideração a quantidade de mensagens por operações amostradas a cada 15 minutos (ex.; o ponto 0 representa a quantidade de mensagens observadas entre 00h:00m:00s e 00h:14m:59s, enquanto que o ponto 15 representa a quantidade de mensagens entre 00h:15m:00s e 00h:29m:59s, e assim por diante), enquanto que a outra considera a quantidade de mensagens de cada operação amostrada a cada 1 minuto. A primeira visa oferecer uma visão de mais alto nível da utilização agregada das operações do SNMP, enquanto a segunda é utilizada sempre que se faz necessária a visualização de partes do tráfego num maior nível de detalhamento, a fim de se encontrar explicações para observações que não são evidentes a partir da distribuição amostrada a cada 15 minutos.

`Mensagens get-request`

A distribuição do número de mensagens da operação `get-request` no tráfego é relativamente constante ao longo de todos os dias presentes na amostra de tráfego. Nas medições realizadas no dia 26 de junho de 2007, ilustrada na Figura 2, a média da ocorrência de mensagens `get-request` em intervalos de 15 minutos é 10.337,67, o desvio padrão é 55,87, e o coeficiente de variação é apenas 0,0054. Uma vez que esses valores são representativos para todo o tráfego, conclui-se que, de um modo geral, a variação no tráfego de mensagens `get-request` é muito pequena. Contudo, observa-se um aumento na variação da quantidade de mensagens `get-request` a partir das 12:00h de todos os dias em que houve monitoramento do tráfego neste horário. Este comportamento está ilustrado na Figura 2, que mostra a variação do número de mensagens `get-request` em intervalos de 15 minutos em um dia específico da carga analisada. Note que o valor 0 não foi incluído no eixo y, uma vez que a ordem de grandeza desses valores para a operação `get-request` é muito superior à das demais operações observadas na rede da RNP. Além disso, o uso de uma escala muito grande esconderia a variação que ocorre a partir do ponto 720 (12:00h). Apesar dessa variação ser pequena, é clara a mudança de padrão da curva a partir das 12:00h.

A possível razão para a pequena variação que ocorre a partir das 12:00h é o aci-

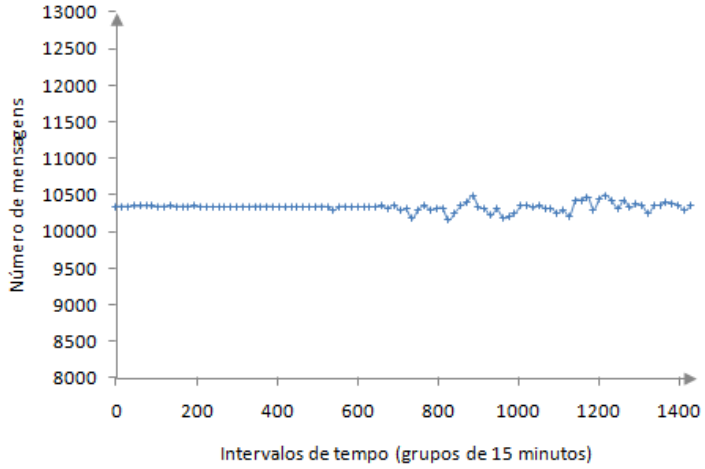

Figura 2. Distribuição do número de mensagens `get-request` amostrada em intervalos de 15 minutos, observada no dia 26 de junho de 2007

onamento de rotinas de *polling* por parte dos sistemas de gerenciamento a partir deste horário. Contudo, esperava-se uma maior periodicidade das solicitações, fato que não ocorre no tráfego estudado, uma vez que não é possível se estabelecer um padrão claro na distribuição da quantidade de mensagens a partir das 12h. Uma investigação mais profunda, em conjunto com os administradores da rede da RNP, se faz necessária, afim de se esclarecer a razão por trás desse comportamento.

Uma investigação mais detalhada foi realizada na parte mais constante do tráfego de mensagens `get-request`. A distribuição do número de mensagens amostradas em intervalos de 1 minuto no período das 03h até as 04:30h está representada na Figura 3. A partir da análise desta figura observa-se que, de fato, no período que antecede às 12h, o tráfego de mensagens `get-request` é bastante periódico, o que pode ser explicado pelo fato de que a RNP utiliza ferramentas de gerenciamento que realizam *polling* nos dispositivos e serviços gerenciados em intervalos de tempo pré-fixados, de forma periódica.

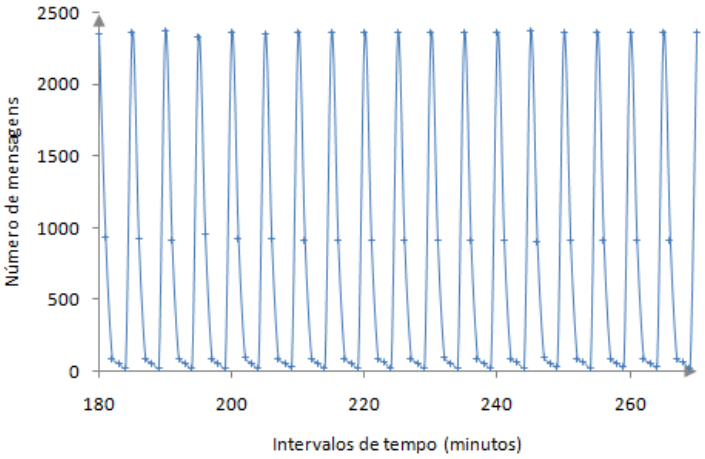

Figura 3. Distribuição do número de mensagens `get-request` amostrada em intervalos de 1 minuto, observada entre as 3h e 4:30h do dia 26 de junho de 2007

Mensagens get-next-request

Mensagens `get-next-request` são utilizadas para serem realizados caminhamentos em árvores MIB, e a utilização deste tipo de caminhamento é bastante comum em softwares de gerenciamento que realizam *polling* sobre os objetos gerenciados. Devido a essas características, é esperado que o tráfego de mensagens `get-next-request` seja mais periódico. Observou-se que a amostra de tráfego da rede da RNP também segue essa tendência em todos os dias em que houve monitoramento, conforme demonstrado na Figura 4.

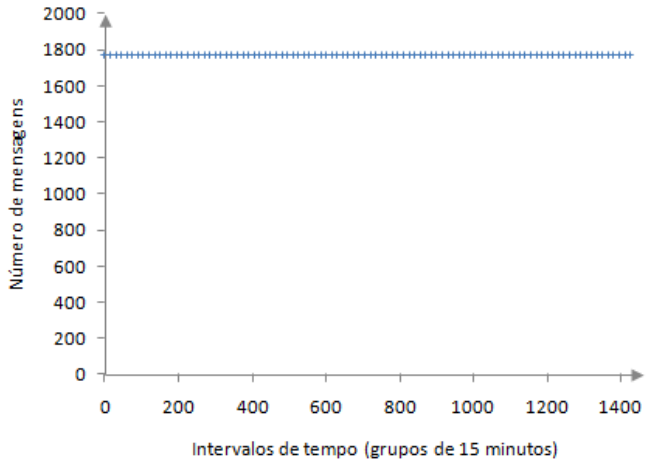

Figura 4. Distribuição do número de mensagens `get-next-request` amostrada em intervalos de 15 minutos, observada no dia 04 de julho de 2007

No dia retratado na Figura 4, observou-se que a média da distribuição da quantidade de mensagens em intervalos de 15 minutos foi de 1.770,16 mensagens, o desvio padrão foi de 0,79 e o coeficiente de variação de variação foi 0,0004. Com isso, ressalta-se ainda mais a periodicidade do tráfego de mensagens `get-next-request` observada na rede da RNP, uma vez que valores bastantes próximos desses que foram apresentados se repetem ao longo de todos os dias em que houve monitoramento de tráfego.

get-bulk-request

A operação `get-bulk-request` foi definida na versão 2 do SNMP, e tem função semelhante à da operação `get-next-request`. Basicamente, esse tipo de mensagem solicita a um agente a recuperação de valores de vários objetos simultaneamente. A diferença entre o `get-bulk-request` e o `get-next-request` é que no `get-bulk-request` é possível o transporte de valores de várias instâncias de um mesmo objeto, diminuindo assim a sobrecarga do SNMP sobre a rede. Por conta desse comportamento, esta operação também é muito utilizada na função de `polling` pelos sistemas de gerenciamento, o que resulta na expectativa da distribuição de mensagens desse tipo ter um comportamento periódico. Mais uma vez esse comportamento pôde ser observado ao longo de todo o tráfego da RNP estudado, conforme mostra a Figura 5.

No dia 29 de junho, retratado na Figura 5, registrou-se uma média de distribuição de mensagens em intervalos de 15 minutos de 589,82 mensagens, desvio padrão de 12,80 e coeficiente de variação de 0,02171. Mais uma vez, isso demonstra um comporta-

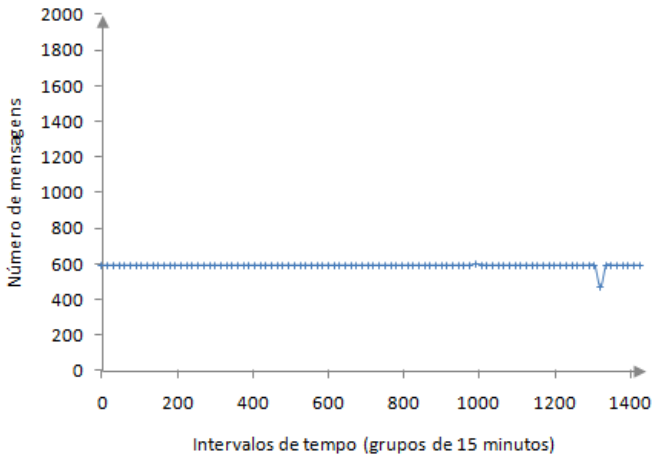

Figura 5. Distribuição do número de mensagens `get-bulk-request` amostrada em intervalos de 15 minutos, observada no dia 29 de junho de 2007

mento bastante constante nessa distribuição, a qual se repete em todos os dias do tráfego monitorado, porém em proporção bem menor em relação às operações `get-request` e `get-next-request`. A utilização de mensagens do tipo `get-bulk-request` é mais econômica do que os tipos `get-request` e `get-next-request` pelo fato de ser necessário, na maioria dos casos, apenas um único cabeçalho de mensagem para a recuperação de valores de vários objetos, ao contrário do que ocorre nos dois outros tipos de mensagem (um cabeçalho para um valor recuperado). Este fato mostra que existe um potencial de diminuição da sobrecarga do tráfego de gerenciamento na rede estudada.

Um ponto que chama atenção no gráfico da Figura 5 ocorre nas proximidades do ponto 1.320 (correspondente ao período entre as 22h:00m:00s e 22h:14m:59s), onde percebe-se um valor anormalmente baixo, em comparação com os outros valores do gráfico. Este declive é uma constante em todos os dias onde o tráfego de gerenciamento da RNP foi monitorado, sempre no mesmo horário, o que indica que muito provavelmente se trata de um comportamento pré-programado no sistema de gerenciamento da rede. Outras investigações se fazem necessárias para melhor explicar o fenômeno observado.

`trap`

Na amostra de tráfego estudada puderam ser observadas mensagens do tipo `trap` das versões 1 e 2 do protocolo SNMP. Uma vez que o mecanismo de traps é assíncrono, espera-se que a distribuição da quantidade dessas mensagens tenha um caráter mais aperiódico, uma vez que elas só são enviadas na rede mediante a ocorrência de algum evento específico. Essa expectativa foi concretizada no estudo realizado sobre o tráfego SNMP da rede da RNP. Um exemplo típico do comportamento das mensagens do tipo `trap` desse tráfego encontra-se representado na Figura 6.

Uma das coisas que se percebe ao se analisar a Figura 6 é a existência de picos que se destacam em relação a um patamar inferior de quantidade de mensagens do tipo `trap`. A existência desses picos indicam possíveis problemas que ocorreriam no instante em que os mesmos aparecem, uma vez que mensagens do tipo `trap` são enviadas na ocorrência de um evento relevante para o gerenciamento da rede. Dentre os principais problemas

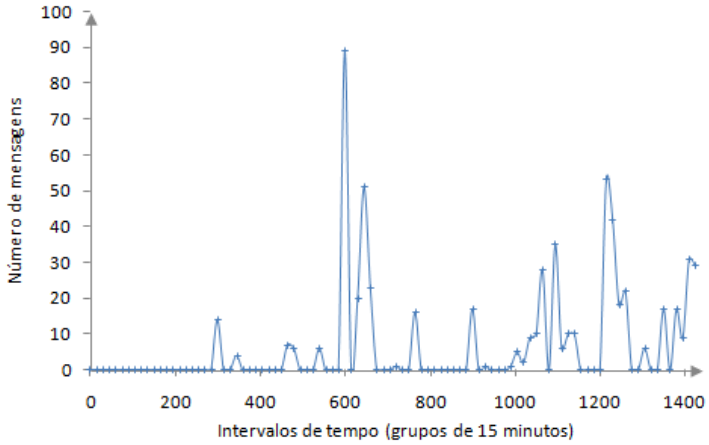

Figura 6. Distribuição do número de mensagens `trap` amostrada em intervalos de 15 minutos, observada no dia 26 de junho de 2007

reportados nas mensagens de `trap`, encontram-se falhas de autenticação e problemas com o protocolo de roteamento BGP.

A variação na distribuição de mensagens do tipo `trap` é sempre muito alta em todos os dias onde houve monitoramento do tráfego de gerenciamento da RNP. No caso do dia 26 de junho de 2007, registrou-se uma média de 141,1354 mensagens a cada 15 minutos, com desvio-padrão de 152,3156 e coeficiente de variação de 1,0792. Esse comportamento é típico ao longo de todo o tráfego estudado, onde o menor coeficiente de variação registrado foi 0,5399. Esse comportamento também não é surpreendente, uma vez que o número de eventos que ocorrem na rede e que causam emissão de `traps` pode perfeitamente variar bastante ao longo de um dia na rede.

`response`

As mensagens `response` são observadas na rede gerenciada sempre em resposta a mensagens `get-request`, `get-next-request` e `get-bulk-request`, contendo as informações dos objetos requisitados pelo gerente. Devido a essa característica, é esperado que as mensagens `response` possuam comportamento bastante semelhante ao da união das mensagens `get-request`, `get-next-request` e `get-bulk-request`. De fato, observou-se, no caso específico da rede da RNP, que, conforme esperado, a distribuição da quantidade de mensagens `response` apresentava componentes periódicos e aperiódicos. Esse comportamento pode ser observado na Figura 7 abaixo.

Na distribuição representada na Figura 7, a média registrada foi de 12.398,66 mensagens a cada 15 minutos, com desvio padrão de 55,33 e coeficiente de variação de 0,0045. Esse dado nos mostra que, apesar da existência de componentes aperiódicos, a quantidade de mensagens do tipo `response` tem uma distribuição bastante constante e periódica no geral (conforme observa-se na maioria absoluta da representação da distribuição das mensagens), de modo similar àquela representada na Figura 2 referente à distribuição de mensagens `get-request`. Esse comportamento também se repete em todos os dias onde houve monitoramento do tráfego SNMP da RNP.

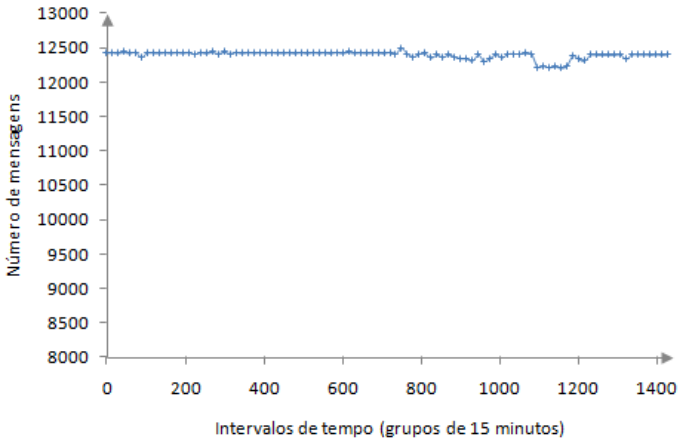

Figura 7. Distribuição do número de mensagens response amostrada em intervalos de 15 minutos, observada no dia 3 de julho de 2007

4.4. Correlações verificadas no tráfego SNMP da rede da RNP

Uma vez que a maioria das mensagens do SNMP atendem a eventos específicos e independentes entre si, espera-se que existam poucas correlações entre as distribuições dos diversos tipos de mensagens que compõem o protocolo. As mensagens com maior potencial de correlação são as do tipo `get` (i.e., `get-request`, `get-next-request` e `get-bulk-request`) com as suas respectivas mensagens de `response`.

Na análise de cada um dos dias do tráfego de gerenciamento da RNP em que houve monitoramento, percebeu-se que os maiores coeficientes de correlação encontravam-se entre as mensagens `get-request` e `response` (correlação tipicamente variando entre 0,80 e 0,90 para cada um dos dias observados). Esse fato se explica porque a maior parte do *polling* realizado na rede é feito com o uso de mensagens `get-request`,e para cada uma dessas mensagens uma mensagem `response` é gerada. Além disso, a operação `get-request`, juntamente com seus respectivos `responses`, praticamente dominam o tráfego periódico na rede gerenciamento da RNP, o que contribui para que a correlação entre eles seja alta.

As demais mensagens observadas ao longo do tráfego monitorado possuem baixa correlação. Tipicamente, o coeficiente de correlação entre essas mensagens varia de 0 a 0,25.

5. Conclusões e trabalhos futuros

A partir das análises realizadas sobre o tráfego fornecido pela Rede Nacional de Ensino e Pesquisa (RNP), foi possível se chegar a um conjunto de resultados interessantes acerca do protocolo SNMP. Atualmente, existe um grande esforço por parte da comunidade de pesquisa em gerenciamento e operação de redes de computadores para se determinar os padrões de uso do protocolo SNMP nas redes em produção. O presente estudo contribui com esse esforço, através de dados que ora confirmam vários dos aspectos que eram apenas pressupostos sobre o uso do SNMP, ora trazem a tona novas características ainda desconhecidas pela comunidade de gerenciamento de redes. Muitas das análises que foram empregadas neste trabalho não haviam sido utilizadas anteriormente em outros trabalhos inseridos no contexto da caracterização do uso do protocolo SNMP. Em

especial, as análises das distribuições dos números de mensagens em perspectiva com a dimensão temporal do tráfego monitorado demonstrou ser capaz de fornecer *insights* bastante interessantes acerca do comportamento do protocolo SNMP na rede da RNP, tais como: identificação de componentes aperiódicos em momentos específicos do tráfego monitorado, níveis de variação tipicamente relacionados com cada operação do protocolo SNMP, potencial para otimização do tráfego de *polling* a partir de modificações nas operações utilizadas para recuperação de valores dos agentes da rede, entre outros.

O tráfego SNMP estudado se mostrou, predominantemente, constante e periódico. Esse comportamento já era esperado, uma vez que a maior parte das ferramentas de gerenciamento de redes conhecidas faz uso extenso de *polling* para determinar o estado dos vários agentes que estão sendo gerenciados. Seria desejável o estudo do comportamento da geração de mensagens feita pelas ferramentas de gerenciamento da rede, a fim de melhor explicar os fenômenos aqui estudados. Contudo, esse tipo de análise não é factível, uma vez que os dados das mensagens contidas na amostra de tráfego SNMP não são suficientes para que "porções" de tráfego provenientes de ferramentas de gerenciamento distintas sejam isoladas.

Foi possível também se identificar um componente aperiódico nesse mesmo tráfego, inclusive criado a partir de mensagens que são tipicamente usadas para a execução do *polling* na rede, como é o caso do `get-request`. Esse componente é significativo o suficiente para justificar um estudo mais aprofundado do mesmo, sendo necessário isolá-lo da parte periódica do tráfego, a fim de ser melhor analisado. Os autores do presente artigo planejam a realização de um estudo desse tipo para o futuro.

Os recursos do SNMP para notificação (`traps`) se mostraram pouco utilizados na rede estudada, em detrimento do extenso uso de *polling*. Ressalta-se que o uso de traps é recomendado no SNMP a fim de diminuir a sobrecarga de mensagens de gerenciamento sobre a rede. Os coeficientes de variação do número de mensagens do tipo `trap` foram os maiores dentre os analisados no tráfego SNMP da RNP, fato este que não representou uma surpresa para os autores deste trabalho.

Conforme esperado, observou-se que o SNMP é utilizado na rede da RNP exclusivamente para monitoramento dos dispositivos e serviços, e nunca para configuração dos mesmos. Isso provavelmente se deve aos problemas de segurança que o SNMP pode apresentar para configuração de recursos na rede, uma vez que as *strings* de comunidade, que funcionam como uma espécie de senha nesse tipo de operação, trafegariam em claro na rede. A possibilidade de criptografar esse tipo de informação só surgiu a partir da versão 3 do SNMP; este, porém, ainda não é suportado por vários dos dispositivos de rede atuais. Também por esse motivo não foram registradas no tráfego da RNP mensagens da versão 3 do SNMP.

Referências

Androutsellis-Theotokis, S. and Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Comput. Surv.*, 36(4):335–371.

Case, J. D., Fedor, M. L., and Schoffstal, J. D. (1990). Simple Network Management Protocol (SNMP). RFC 1157. [S.l.]: Internet Engineering Task Force, Network Working Group.

Curbera, F., Duftler, M., Khalaf, R., Nagy, W., Mukhi, N., and Weerawarana, S. (2002). Unraveling the web services web - an introdution to soap, wsdl,and uddi. *IEEE Internet Computing*, 6(2):86–93.

Dobrev, P., Stancu-Mara, S., and Schönwälder, J. (2009). Visualization of node interaction dynamics in network traces. In *AIMS '09: Proceedings of the 3rd International Conference on Autonomous Infrastructure, Management and Security*, pages 147–160, Berlin, Heidelberg. Springer-Verlag.

Goldszmidt, G. and Yemini, Y. (1995). Distributed management by delegation. In *Proceedings of the 15th International Conference on Distributed Computing Systems, 1995*, pages 333–340, Vancouver, BC, Canada.

Salvador, E. M. and Granville, L. Z. (2008a). Arquitetura de uma ferramenta e técnicas de visualização para medições sobre tráfego snmp. In *Simpósio Brasileiro de Redes de Computadores, SBRC, 26.*, Rio de Janeiro, Brasil.

Salvador, E. M. and Granville, L. Z. (2008b). Using visualization techniques for snmp traffic analyses. In *IEEE Symposium on Computers and Communications, ISCC*, Marrakesh, Marrocos.

Schönwälder, J., Pras, A., Harvan, M., Schippers, J., and van de Meent, R. (2007). SNMP Traffic Analysis: Approaches, Tools, and First Results. *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management*.

Schoenwaelder, J. (2008). Simple Network Management Protocol (SNMP) Measurements and Trace Exchange Formats. *Internet Research Task Force (IRTF), RFC 5345*.

Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J., and Waldbusser, S. (2001). Rfc 3198 - terminology for policy-based management. Disponível em `ftp://ftp.rfc-editor.org/in-notes/rfc3198.txt`. Acesso em maio de 2006.