

Introdução

O gerenciamento de dispositivos em uma rede local se mostra como uma tarefa de importância cada vez maior dentro das organizações. Além disso, a quantidade de equipamentos que podem ser gerenciados tende a aumentar continuamente e, aliada a isto, está a necessidade de simplificar o processo de gerência. Assim, o protocolo SNMP (*Simple Network Management Protocol*) pode ser usado para o gerenciamento dos dispositivos conectados a uma rede local de forma simples e direta. Por sua vez, os equipamentos tendem a oferecer cada vez mais possibilidades de gerenciamento, de modo a facilitar tarefas como a detecção de falhas, a visualização de grandezas e as notificações de condições de exceção ou eventos. Portanto, cada vez mais equipamentos oferecem funcionalidades de gerenciamento por SNMP, o que os torna compatíveis com as redes locais e mais facilmente gerenciáveis.

Protocolo SNMP

O SNMP é o protocolo de gerência de redes padrão do IETF (*Internet Engineering Task Force*) [3] e se tornou padrão de fato para o gerenciamento de redes IP. Ele é um protocolo pertencente à camada de aplicação da arquitetura OSI [11] e utiliza na camada de transporte os serviços do protocolo UDP para enviar suas mensagens através da rede IP. Cada dispositivo gerenciado é chamado de nó gerenciado.

Funcionamento Geral

O protocolo SNMP define duas entidades para o gerenciamento, as quais trocam informações entre si através de requisições do tipo cliente-servidor. O gerente SNMP (cliente) realiza basicamente duas operações: a leitura de valores (GET) para o monitoramento do dispositivo gerenciado e a escrita (SET) onde for possível efetuar a alteração de valores deste dispositivo. O agente SNMP (servidor) fica então responsável por responder às solicitações do gerente e alterar as informações quando solicitada tal operação, além de notificar o gerente (TRAP) no caso de ocorrer alguma exceção. Toda a inteligência do processo fica na estação de gerência permitindo que o agente seja uma aplicação muito simples e com o mínimo de interferência no dispositivo em que está sendo executado. As decisões tomadas na ocorrência de problemas e as funções de relatórios ficam sob responsabilidade do gerente.

Agente SNMP

O agente é um processo executando no nó gerenciado (ou próximo a ele), responsável pela manutenção de um banco de dados local com as informações de gerência desse nó. Cada nó gerenciado pelo SNMP deve possuir um agente e uma base de informações de gerência. Sendo assim, o nó gerenciado é visto como um conjunto de variáveis que representam informações referentes ao seu estado atual. Essas variáveis ficam disponíveis ao gerente através de consultas e podem ser alteradas por ele – se assim as variáveis foram definidas. Ao disponibilizar essas variáveis à leitura, o nó permite seu monitoramento e, ao receber novos valores do gerente, o nó estará sendo controlado. O agente também é responsável por notificar o gerente no caso da ocorrência de alguma exceção no nó gerenciado. Os nós gerenciados podem apresentar falhas ou comportamentos inadequados e quando o agente identifica que ocorreu um evento significativo ele envia pacotes informativos sobre o ocorrido a todas as estações de gerência de sua lista de distribuição de alarmes. Esta operação é efetuada através de interrupções (*traps*) e essas *traps* podem ou não informar exatamente os detalhes sobre o que ocorreu inesperadamente, podendo ser necessário que a estação de gerenciamento realize consultas para essa investigação e obtenção de mais detalhes.

Tipos de Agentes SNMP

Os agentes SNMP podem ser classificados em dois tipos distintos, que diferem entre si pela forma como são implementadas as funcionalidades do protocolo SNMP e pelo modo como são feitas as interações com os dispositivos gerenciados [2]. O primeiro tipo de agente SNMP é o *agente extensível*. Este tipo de agente em geral oferece suporte à MIB-II, e utiliza o SNMP diretamente (mais detalhes sobre MIBs podem ser encontrados no capítulo 3 deste artigo). Isto significa que possui a implementação de todas as funcionalidades do protocolo SNMP. Para que ele se comunique com o dispositivo gerenciado, é necessária a implementação de agentes estendidos. Um exemplo de agente extensível é o agente SNMP do sistema operacional Microsoft Windows®. Ele não possui suporte a nenhuma MIB, e para que ele responda às requisições de objetos de uma determinada MIB deve haver uma biblioteca adicional que implemente o suporte à MIB. Para a plataforma Linux/Unix pode-se citar o agente Net-SNMP (anteriormente chamado de UCD-SNMP) [7]. Este agente é usado como base para a implementação de uma grande variedade de agentes estendidos e é um dos mais difundidos para o ambiente. Por sua vez, o agente estendido possui somente funções básicas de comunicação com o dispositivo gerenciado para busca de informações. Este tipo de agente é baseado em um agente principal (extensível), o qual implementa as funções do protocolo SNMP. Dessa forma, o trabalho de resposta às requisições do protocolo SNMP é feito

somente pelo agente extensível, ficando para o agente SNMP estendido o trabalho de comunicação com o dispositivo gerenciado e disponibilização das informações de monitoração ao agente extensível.

Gerente SNMP

O gerente é uma aplicação em execução em uma estação de gerenciamento. É possível que exista um ou mais gerentes em execução em uma mesma estação – colaborando entre si para o gerenciamento – e todos eles utilizam o protocolo de gerência disponibilizado por essa estação. Essas aplicações são capazes de monitorar os agentes através de requisições de informações contidas na base de informações de gerenciamento e de alterar as características dos nodos gerenciados, informando novos valores ao agente. Os gerentes são os responsáveis pela implementação da política que será adotada na gerência e eles são acessíveis à pessoa ou entidade responsável pelo gerenciamento do nodo. O envio de alarmes por e-mail, chamadas telefônicas, mensagens para telefones celulares ou outras formas de comunicação com o administrador são comuns nestes aplicativos. Além disso, a visualização das grandezas e estados dos equipamentos é fundamental neste tipo de aplicação. Outra forma de visualização interessante é a apresentação de gráficos que mostrem a evolução de valores ou condições do equipamento ao longo do tempo, fornecendo informações sobre tendência de comportamento dos equipamentos.

Operações do Protocolo

O protocolo SNMP define as operações de leitura de valores, escrita de valores e notificação de condições de exceção (*traps*). Para que ocorra a troca de mensagens no protocolo SNMP são utilizadas cinco PDUs (*Protocol Data Unit*): *GetRequest*, *GetNextRequest*, *GetResponse*, *SetRequest* e *Trap* (considerando a versão 1 do SNMP – SNMPv1). Cada PDU corresponde à definição dos formatos empregados pelas entidades do protocolo na troca de informações. As PDUs *GetRequest* e *GetNextRequest* serão utilizadas pelo gerente quando este desejar realizar uma leitura de dados, enquanto que a PDU *SetRequest* é utilizada pelo gerente para solicitar uma alteração do dado referente a algum objeto. Por sua vez, o agente responderá a uma solicitação do gerente utilizando a PDU *GetResponse* e tomará a iniciativa de enviar interrupções ao gerente através da PDU *Trap*, quando ocorrer uma condição de exceção que justifique essa notificação. A definição do SNMP prevê uma autenticação que deve ser feita ao trocar informações utilizando o protocolo. Essa autenticação é realizada através da *string de comunidade* (informada por quem está tomando a iniciativa no envio de informações). A comunidade pode ser diferente para leitura, escrita e envio de *traps*. Se a comunidade for informada incorretamente, o agente não responderá a solicitação do gerente. Com a definição da versão 2 do SNMP (SNMPv2) surgiram duas novas PDUs (*InformRequest* e *GetBulkRequest*) e a possibilidade de se realizar um gerenciamento distribuído, através da comunicação gerente-gerente. No SNMPv3, um dos objetivos na definição foi de aumentar a segurança já que a forma como é feita a autenticação pela comunidade nas versões anteriores sempre foi considerada muito fraca para garantir alguma forma de segurança.

Management Information Base (MIB)

A MIB (*Management Information Base*) é a base de informações de gerenciamento. O agente é capaz de responder ao gerente consultas SNMP sobre o conjunto de informações contido na MIB. De fato, em geral é codificado um arquivo – chamado *arquivo de MIB* – no qual são relacionadas essas informações para que o gerente saiba quais são as informações que podem ser solicitadas a um agente e também as informações de alerta (*traps*) que poderão ser enviadas do agente para o gerente. Constituída por uma estrutura em árvore contendo as variáveis de gerência de um determinado equipamento, a MIB define para cada variável um identificador único denominado OID (*Object Identifier*), formado por um inteiro não negativo. Em princípio, todos os objetos definidos em todos os padrões oficiais podem ser exclusivamente identificados. Para localizar uma determinada informação, o identificador da variável que será acessada pelo SNMP é representado com o IP do equipamento em conjunto com o identificador do objeto na árvore MIB (OID). O OID de um nodo da árvore descrita por uma MIB é composto pelo OID do seu pai mais seu próprio identificador relativo. Entretanto, o uso de números nos OIDs dificulta a compreensão dos nodos da MIB e por isso o OID pode ser substituído por um nome (*OID Name*), que pode ser usado em conjunto com o OID “numérico”. Por exemplo, o OID 1.3.6.1.2.1.1 pode ser representado pelo *OID Name* “system”. Por sua vez, *sysUpTime* é o OID 1.3.6.1.2.1.1.3 ou *system.3*. Para cada objeto são definidos o nome, um identificador, uma sintaxe, uma descrição e um controle de acesso. As instâncias dos objetos são chamadas de variáveis. O nome do objeto (*Object Name*) é composto por uma string de texto curto. O identificador do objeto (OID) é formado por números separados por pontos. A sintaxe (*syntax*) descreve o formato ou valor e define o tipo do objeto. A descrição é uma string que informa o que a variável representa. O acesso é o tipo de controle que se pode ter sobre o objeto (somente leitura, leitura e escrita ou não acessível). Os nodos em uma árvore de MIB podem ser de diferentes tipos de dados (inteiros, strings ou contadores, por exemplo). Também é possível a definição de tabelas, juntamente com a definição do que consta em cada

linha da tabela. Por fim, é possível inserir na árvore da MIB informação sobre as *traps* que podem ser enviadas pelo agente ao gerente, de modo que o gerente possa interpretar as notificações que ele recebe.

MIBs Padronizadas e Proprietárias Muitas MIBs definidas se tornam padrão no gerenciamento a que se propõem. A RFC1066 [4] apresentou a primeira versão da MIB, a MIB I, que definiu a base de informações necessárias para gerenciar redes baseadas na pilha de protocolos TCP/IP. A RFC1213 [5] propôs uma segunda MIB, a MIB II. Ela também foi feita para gerenciar redes baseadas na pilha de protocolos TCP/IP e implementa novos objetos em relação a MIB I. É o padrão utilizado atualmente e tornou obsoleta a MIB I. Além destas, há uma grande gama de MIBs para o gerenciamento de redes, dos computadores conectados a uma rede e para dispositivos e equipamentos em geral. Além das MIBs padronizadas, cada fabricante pode definir uma MIB para descrição de seus equipamentos (MIB proprietária). Estas bases de informações de gerenciamento podem ser baseadas em MIBs padrão ou totalmente personalizadas de acordo com as características do equipamento ou dispositivo gerenciado. Com isso, o que se obtém é um gerenciamento bastante específico, o que pode acarretar uma melhoria na qualidade e quantidade das informações gerenciadas e nas notificações (*traps*) enviadas ao gerente. Um exemplo claro de existência de MIB padronizada ocorre no gerenciamento de No-Breaks – UPS (*Uninterruptible Power Supply*). A RFC 1628 [1] define a UPSMIB, uma MIB genérica para utilização na monitoração de equipamentos do tipo UPS. Com isso, apesar de muitos fabricantes de equipamentos definirem suas próprias MIBs proprietárias ajustadas a seus equipamentos, muitas delas são parecidas ou fortemente baseadas na UPS-MIB [9].

Conclusões

Cada vez mais equipamentos oferecem a possibilidade de serem gerenciados por SNMP, o que torna necessário o conhecimento a respeito do funcionamento do protocolo e de como pode-se aproveitá-lo para o gerenciamento dos equipamentos em uma rede local. Este artigo pretende ser um ponto de partida para este entendimento e, embora não esgote o assunto, oferece uma introdução a respeito do que se pode obter ao utilizar o SNMP para a monitoração de equipamentos. O uso do SNMP mostra-se bastante interessante na medida em que permite que se utilize ferramentas diversas para a gerência.

Referências

- [1] CASE, J.; *UPS Management Information Base*. Request For Comments 1628 – Internet Engineering Task Force, (May, 1994).
- [2] GRANVILLE, L. Z.; *Construção de Agentes SNMP em ambiente Linux*. Instituto de Informática, Universidade Federal do Rio Grande do Sul. Disponível em <http://www.inf.ufrgs.br/granville/AgentesSNMP/download/apostila_parte_I.pdf>. Acesso em agosto, 2006.
- [3] INTERNET ENGINEERING TASK FORCE. Disponível em: <<http://www.ietf.org>>. Acesso em julho, 2006.
- [4] MCCLOGHRIE, K.; ROSE, M.; *Management Information Base for Network Management of TCP/IP-based internets*. Request For Comments 1066 – Internet Engineering Task Force, (August, 1988).
- [5] MCCLOGHRIE, K.; ROSE, M.; *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. Request For Comments 1213 – Internet Engineering Task Force, (March, 1991).
- [6] MULTI ROUTER TRAFFIC GRAPHER. Disponível em <<http://oss.oetiker.ch/mrtg/>>. Acesso em agosto, 2006.
- [7] NET-SNMP. Disponível em <<http://www.net-snmp.org/>>. Acesso em agosto, 2006.
- [8] POLINA, E.R.; *Desenvolvimento de um Agente SNMP para Gerência de No-Breaks em uma Plataforma não Convencional*. Projeto de Diplomaciação. Instituto de Informática, Universidade Federal do Rio Grande do Sul, (Ago, 2003).
- [9] POLINA, E.R.; *Um estudo sobre gerenciamento de no-breaks*. Trabalho Individual. Instituto de Informática, Universidade Federal do Rio Grande do Sul, (Mar, 2005).
- [10] ROUND ROBIN DATABASE TOOL. Disponível em <<http://oss.oetiker.ch/rrdtool/>>. Acesso em agosto, 2006.
- [11] TANENBAUM, A.; *Computer Networks*. 3rd edition, Prentice Hall, 1996.