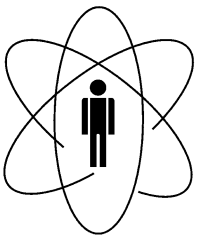
ISSN 0101-9201



CBPF - CENTRO BRASILEIRO DE PESQUISAS FÍSICAS

Rio de Janeiro

Notas Técnicas

CBPF-NT-001/13

junho 2013

O Protocolo SNMP

Antonio Matheus Benaion Esteves & Nilton Alves Jr.

Ministério da
Ciência, Tecnologia e Inovação

dx.doi.org/10.7437/NT2236-7640/2013.01.001
Notas Técnicas, v. 3, n. 1, p. 1–14, 2013

O Protocolo SNMP

Antonio Matheus Benaion Esteves e Nilton Alves Jr.
Centro Brasileiro de Pesquisas Físicas - CBPF
Rua Dr. Xavier Sigaud,
150 – Urca – Rio de Janeiro – RJ – Brasil

Esta nota técnica tem como objetivo apresentar as principais características e funcionalidades do protocolo de gerenciamento SNMP - Simple Network Managment Protocol.

Inicialmente, foram abordados o contexto histórico da atividade de gerência de redes e as motivações que levaram à criação deste protocolo; posteriormente, foram apresentados os conceitos básicos relacionados ao mesmo e à sua utilização, bem como os principais aplicativos do protocolo SNMP para a atividade de gerência de redes. Paralelamente a isto, foi apresentada a base de dados MIB - Management Information Base, responsável pela geração da árvore de estrutura hierárquica das interfaces e suas respectivas estatísticas de interesse dentro de um equipamento de rede, ressaltando que esta árvore é acessada por intermédio do protocolo SNMP. Também foram apresentadas algumas vantagens e desvantagens do protocolo, bem como foram propostas soluções para contornar as limitações apresentadas.

Após isto, foram propostos alguns exemplos práticos de implementação, para ilustrar o uso do protocolo SNMP na gerência de redes. Finalizando esta nota, seguiram-se algumas considerações finais sobre o protocolo.

1. INTRODUÇÃO

Uma série de fatores ocasionou o aumento da complexidade das ações de gerência de redes, juntamente com o aumento da importância destas, para assegurar o funcionamento adequado de todos os elementos de rede. Isto gerou a necessidade de se criar uma solução com a qual estas atividades pudessem ser realizadas de forma padronizada e satisfatória, independente da distância física entre os equipamentos monitorados e quem os gerencia. Em particular, podemos destacar os seguintes fatores [1][2][3]:

- A drástica evolução, em termos de topologia, das redes de computadores, partindo de pequenas redes locais (LAN's) para grandes redes espalhadas por países, continentes e até mesmo por todo o planeta (Internet e Intranets).
- A criação de diversos protocolos de rede, para variadas finalidades (comunicação entre dois ou mais pontos de rede, estabelecimento de conexões de rede, troca de mensagens de um ponto a outro, etc.).
- A evolução e diversificação dos equipamentos de rede (comutadores, concentradores, roteadores, etc.), onde cada fabricante desenvolve seus próprios equipamentos, possivelmente com aspectos específicos não existentes em equipamentos similares de outros fabricantes.
- O aumento cada vez mais expressivo do número de usuários conectados às redes.

No início da década de 80, iniciou-se o desenvolvimento do protocolo de gerência de redes SNMP - Simple Network Management Protocol, por parte da organização IETF - Internet Engineering Task Force, para disponibilizar uma forma simples de gerenciar equipamentos de uma dada rede de computadores [1]. Este protocolo começou a ser empregado efetivamente na década de 90, com o advento da RFC1157 [4].

Antes do protocolo SNMP, o protocolo utilizado para a gerência de rede era o SGMP - Simple Gateway Management Protocol. A principal limitação deste protocolo residia no fato dele ter sido desenvolvido apenas para a gerência de roteadores de Internet, restringindo sua utilização em gerência de redes. Por sua vez, o protocolo SNMP é capaz de gerenciar sistemas operacionais, periféricos como impressoras e fontes de energia, por exemplo, dentre outros dispositivos de rede [2]. A especificação do protocolo SGMP se encontra na RFC1028, publicada em 1987 [5].

Atualmente, existem 3 versões do protocolo SNMP disponíveis para utilização. A versão SNMPv1 é a versão corrente do protocolo, como padrão completo da organização IETF. Sua segurança está pautada no conceito de comunidades (*communities*). *Communities* funcionam de forma similar a senhas, sendo dados do tipo *string* utilizados para:

- Estabelecer conexões seguras entre equipamentos monitorados e as máquinas que os gerenciam [2].

- Acessar estatísticas de um dado equipamento de rede, desde que a *community* em questão tenha permissão para acessar tais estatísticas [4].

Conforme exposto anteriormente, esta versão foi disponibilizada para uso em 1990, quando da publicação da RFC1157 [4].

A versão SNMPv2, também conhecida em algumas literaturas como SNMPv2c, utilizada na implementação do protocolo descrita nesta nota, também possui status IETF, contudo, em nível Experimental[1][6], embora alguns fornecedores já a utilizem na prática [2]. Especificações desta versão podem ser encontradas nas RFC's1902 [7], 1903 [8], 1904 [9], 1905 [10], 1906 [11], 1907 [12], 1908 [13] e 1909 [14], todas publicadas em 1996. As principais mudanças que esta versão traz em relação à versão SNMPv1 são:

- Correção de falhas de segurança na autenticação das *communities*, quando algum aplicativo do protocolo SNMP tenta estabelecer conexão, ou acessar uma estatística qualquer de um equipamento monitorado. Desta mudança vem a razão para o nome SNMPv2c, onde o protocolo tem sua segurança mais fortemente baseada no conceito de *communities*, justificando o "c" ao final do nome desta versão [2][14].

- Criação do tipo de dado Counter64, como versão estendida do tipo Counter, criado na versão SNMPv1. Este tópico será abordado mais adiante, no capítulo 2 [7].

- Criação do tipo de mensagem InformRequest, onde dois ou mais gerentes podem se comunicar, possibilitando assim um gerenciamento descentralizado de uma rede [10].

- Criação do tipo de mensagem GetBulkRequest, para otimizar a recuperação de dados de equipamentos monitorados [10].

A versão SNMPv3 ainda não possui status IETF, o qual será alcançado posteriormente [6]. Especificações desta versão podem ser encontradas nas RFC's2570 [15], 2571 [16], 2572 [17], 2573 [18], 2574 [19] e 2575 [20], todas publicadas em 1999, e a principal mudança que esta versão apresenta em relação às suas predecessoras reside na ênfase que a mesma apresenta no aspecto da segurança fornecida às atividades do protocolo. Dentre outros aspectos de segurança, pode-se destacar [2][15]:

- Suporte para autenticação rigorosa junto a cada equipamento monitorado pelo protocolo.

- Comunicação privativa entre os equipamentos monitorados.

[1] O status IETF Experimental é concedido às RFC's que fazem parte de alguma pesquisa em determinado assunto, mas ainda sem serem largamente utilizadas pelos fabricantes de equipamentos de redes. As RFC's largamente utilizadas por diversos fabricantes recebem status Informacional; e as RFC's consideradas obsoletas recebem status Histórico.

Atualmente, o principal objetivo das pesquisas em gerenciamento de redes consiste na obtenção da máxima performance da rede, otimizando-se assim os elementos de gerência e monitoramento de redes. Conforme explicado nos parágrafos anteriores sobre as versões do protocolo SNMP, este também tem sido o principal enfoque de melhorias e correções deste protocolo [1].

Após esta introdução sobre o contexto histórico e as motivações que levaram ao surgimento do protocolo SNMP, o próximo capítulo abordará os conceitos relacionados à base de dados MIB, a qual contém os dados acessados pelo protocolo SNMP. No capítulo posterior ao capítulo sobre a base MIB, será analisado o protocolo SNMP propriamente dito, juntamente com suas vantagens e limitações técnicas. Por fim, seguirão mais dois capítulos: um com exemplos de como o protocolo SNMP pode ser implementado em atividades de gerência de redes; e o outro, com as considerações finais desta nota.

2. A BASE DE DADOS MIB

Antes de se falar sobre o protocolo SNMP propriamente dito, é preciso entender a base de dados acessada por este protocolo, para obter todas as estatísticas de interesse dos equipamentos de rede monitorados. Esta base de dados em questão é a base MIB.

A base MIB - Management Information Base é o conjunto de objetos de um dado equipamento de rede, organizados de modo a contemplar todas as estatísticas deste equipamento para sua respectiva gerência da rede. Pode ser considerada ainda como um banco de dados, responsável por armazenar todas estas estatísticas dos equipamentos de rede [1][2].

Objetos são a abstração dos recursos de um sistema. Todos os recursos a serem gerenciados via SNMP são modelados, e as estruturas dos dados resultantes desta modelagem são então denominados objetos, os quais contém as estatísticas de um equipamento de rede. Os objetos podem ser configurados para leitura/escrita, ou somente leitura, dependendo do nível de permissão a ser concedido ao gerente da rede. Cada leitura representa o estado atual do equipamento de rede, enquanto que as escritas automaticamente modificarão tal estado, sendo refletidas em tempo real para o(s) gerente(s) que estiver(em) visualizando o objeto naquele momento.

Atualmente, são definidos três tipos de bases de dados MIB: MIB II, MIB experimental e MIB privada. A base MIB II surgiu na RFC1213 [21], como uma evolução da base MIB I, apresentada originalmente na RFC1066 [22]. Esta evolução consistiu no uso da base MIB baseado na pilha de protocolos TCP/IP, o qual teve explicado, na base MIB I, o conjunto de informações necessárias para a implementação de práticas de monitoramento e controle de redes baseadas nos protocolos TCP/IP [1].

Além disso, a base MIB II também fornece informações de gerenciamento sobre um dado equipamento. Através disto, podemos obter estatísticas como, por exemplo, número de pacotes, ou bytes (também chamados de octetos) transmitidos por cada uma das interfaces do equipamento, totais de envios bem-sucedidos e com falha de pacotes, estado da(s) interface(s), etc.

Na base MIB experimental, os objetos que a integram estão em fase de desenvolvimento e/ou teste, possuindo normalmente características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados na mesma [1].

Por fim, a base MIB privada é a modalidade da MIB onde seus componentes fornecem estatísticas específicas dos equipamentos gerenciados por elas, tais como configuração e colisões; e também é possível reinicializar e/ou desabilitar uma ou mais portas de um roteador gerenciado pela base MIB em questão [1].

Como as bases MIB experiental e privada são bases MIB I ou II customizadas para fins específicos dos fabricantes que as utilizam, não existem RFC's publicadas para estas bases em especial.

2.1. Construção

As regras de construção da base MIB são descritas na SMI - Structure of Management Information. A SMI é um conjunto de documentos que definem [1][2]:

- Forma de identificação e agrupamento das estatísticas;
- Sintaxes permitidas para estas estatísticas;
- Tipos de dados permitidos para estas estatísticas;
- Lista de equipamentos gerenciados e os objetos que integram cada um deles;
- Objetos gerenciados e seus respectivos comportamentos.

Desta forma, cabe ao conjunto de documentos SMI construir a estrutura de gerenciamento de objetos e equipamentos, enquanto que cabe à MIB apresentar esta estrutura construída [2].

Os objetos constituintes de uma base MIB são especificados pelo documento ASN.1 - Abstract Syntax Notation One, encarregado de fornecer uma descrição abstrata destes objetos, descrição esta que desconsidera a estrutura e as restrições do equipamento no qual a base MIB está sendo implementada. Para cada objeto são definidas as seguintes instâncias:

- **Object Name**: Nome do objeto, composto por uma string de texto curto.
- **Object Identifier - OID**: Identificador do objeto, formado por números que são separados por pontos. *Exemplo: .1.3.6.1.2.1.2.2.1.10*
- **Syntax**: sintaxe do objeto, descreve o formato, ou o valor, da informação. Pode ser de um tipo simples (inteiro, uma string de octetos (bytes), um Object Identifier (OID) ou nulo; ou uma sintaxe de aplicação (endereço de rede (IP), um contador, uma medida específica, um intervalo de tempo ou incompreensível ao usuário).
- **Definição**: Descrição textual do que é o objeto em questão.
- **Acesso**: Tipo de permissão que se pode ser definida, em relação à manipulação de conteúdo do objeto, podendo ser: somente leitura, leitura e escrita ou não acessível.

2.2. Estrutura

A figura 1 abaixo apresenta a estrutura definida pela organização ISO para representar a estrutura lógica da base MIB, com os identificadores e os nomes de cada um dos objetos componentes da mesma.

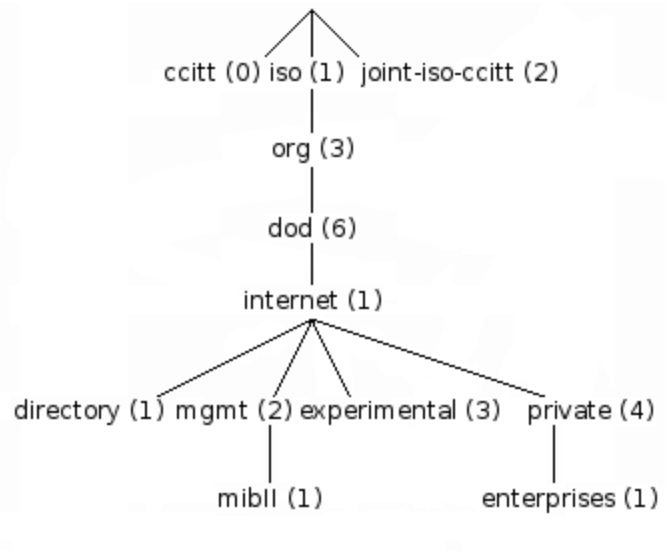


Figura 1: Estrutura lógica de uma base MIB

O nó raiz da base MIB não possui nenhuma denominação, mas possui pelo menos três subníveis:

- **Nó .0**: Administrado pela organização Consultative Committee for International Telegraph and Telephone - CCITT;
- **Nó .1**: Administrado pela organização International Organization for Standartization - ISO;
- **Nó .2**: Administrado em conjunto pelas organizações CCITT e ISO.

Sob o nó .1 fica o nó .1.3, chamado *org*, que pode ser utilizado por outras instituições. Abaixo dele fica o *dod* (nó .1.3.6), pertencente ao departamento de defesa dos EUA. O departamento de defesa dos EUA alocou um nó para a comunidade *internet* (.1.3.6.1), que é administrado pela organização International Activities Board - IAB e abaixo deste nó temos os nós *directory* (.1.3.6.1.1), *management* (.1.3.6.1.2), *experimental* (.1.3.6.1.3) e *private* (.1.3.6.1.4).

Sob o nó *directory* estão as informações sobre o serviço de diretórios OSI [23].

Sob o nó *management* estão as informações de gerenciamento, é sob este nó que está o nó responsável pela MIB II (.1.3.6.1.2.1).

Sob o nó *experimental* estão os nós das MIBs experimentais.

Sob o nó *private* fica o nó *enterprises* (.1.3.6.1.4.1) e sob este nó ficam os nós das indústrias de equipamentos gerenciados na MIB, como o nó da IBM (.1.3.6.1.4.1.2) e o da Cisco (.1.3.6.1.4.1.9), dentre outros [1][24].

2.3. MIB II

1. **Organização**

   Abaixo da sub-árvore *MIB II* estão os objetos usados para obter informações específicas dos dispositivos da rede. Os principais objetos estão divididos em 10 grupos, que estão presentes na tabela I.

2. **Tipos de dados**

   Na sub-árvore *MIB II*, cada objeto contém um determinado tipo de dado, especificado antes do valor nominal do mesmo, quando da verificação do nó em questão . Os tipos de dados considerados pelo documento SMI são [2]:

   - **Integer**: Normalmente é um número inteiro, utilizando 32 bits, para especificar informações numéricas de um objeto gerenciado qualquer. De acordo com a RFC1155 [25], o valor numérico zero (0) não deve ser utilizado para este tipo de dado; caso tal valor seja utilizado, o objeto em questão não será listado na base MIB. Na versão SMIv2 do documento SMI, também existe o dado do tipo Integer32, equivalente ao Integer convencional [2].
   - **String**: É uma string contendo zero ou mais octetos (bytes). Utilizada para especificar strings de texto, ou ainda endereços físicos de um ou mais objetos.
   - **Counter**: Número de 32 bits, o qual é sempre definido como zero, a cada vez em que ocorre overflow no contador, ou seja, o valor máximo de $2^{32} - 1$ é excedido. É um valor que nunca sofre decréscimo, exceto para os casos de overflow, ou de reinicialização do equipamento, quando todos os objetos deste tipo são zerados; sendo então utilizado para contabilizar quaisquer informações de totais de um equipamento, como, por exemplo, totais de pacotes recebidos e enviados. Na versão SMIv2, também existe o dado do tipo Counter32, equivalente ao Counter convencional.
   - **Object Identifier**: String composta por sequências de números e pontos, utilizada como representação do caminho até um dado objeto qualquer em uma base MIB.
   - **Null**: Representa um objeto que não esteja sendo utilizado pelo protocolo SNMP.
   - **Sequence**: Define listas de dados diferentes existentes no documento ASN.1. Pode conter zero ou mais tipos.

Tabela I: Grupos de informações da sub-árvore *MIB II*

Grupo	Informação
system (1)	informações básicas do sistema
interfaces (2)	interfaces de rede
at (3)	tradução de endereços
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
snmp (11)	protocolo SNMP

   - **Sequence Of**: Define objetos gerenciados formados por dados do tipo Sequence.
   - **IpAddress**: Utilizado para representar endereços de rede (IP's), conforme o padrão IPv4 (32 bits). As versões existentes do documento SMI (SMIv1 e SMIv2) não processam endereços IP segundo o futuro padrão de endereços IPv6 (128 bits), problema este a ser resolvido pela próxima versão do documento SMI (SMI Next Generation - SMING).
   - **NetworkAddress**: Idem ao IpAddress, mas sendo capaz de representar tipos de endereços de rede diferentes do IPv4.
   - **Gauge**: Mesmo tipo de dado que o tipo Counter, com a diferença de poder aumentar e diminuir seu valor, independente da ocorrência ou não de overflow ou reinicialização do equipamento. Na versão SMIv2 do documento SMI, também existe o dado do tipo Gauge32, equivalente ao Gauge convencional.
   - **TimeTicks**: Dado numérico de tamanho igual aos dados Counter e Gauge, normalmente utilizado para medir tempo corrente a partir de algum evento específico do equipamento, como, por exemplo, a última reinicialização do mesmo.
   - **Opaque**: Habilita o armazenamento de codificações do documento ASN.1 em um objeto do tipo String.
   - **Unsigned32 - exclusivo da versão SMIv2**: Utilizado para representar valores numéricos de 0 até 231.
   - **Counter64 - exclusivo da versão SMIv2**: Apresenta o mesmo princípio de funcionamento que o Counter32, mas com 64 bits de tamanho, variando assim de 0 até $2^{64} - 1$. Utilizado quando números de 32 bits se mostram ineficazes como contadores, ou seja, o estado de overflow é alcançado muito rapidamente pela estatística em questão.

- **Bits - exclusivo da versão SMIv2**: Listagem de bits não negativos do objeto gerenciado.

3. **Exemplos**

   Alguns exemplos de nós existentes nos principais grupos da sub-árvore MIB II são:

   - **Nó System (.1.3.6.1.2.1.1)**: Faz a listagem de objetos existentes no sistema operacional do equipamento gerenciado.
     - **sysDescr (.1.3.6.1.2.1.1.1)**: Descrição textual do equipamento gerenciado. Pode incluir o nome e a versão do hardware do equipamento e o sistema operacional do mesmo. Variável do tipo String.
     - **sysObjectID (.1.3.6.1.2.1.1.2)**: Caminho dentro da base MIB especificado para o gerenciamento do subsistema de uma determinada instituição. Variável do tipo OID.
     - **sysUpTime (.1.3.6.1.2.1.1.3)**: Tempo transcorrido (em milhares de segundos) desde a última vez em que o gerenciamento do sistema na rede foi reinicializado. Variável do tipo TimeTicks.
     - **sysContact (.1.3.6.1.2.1.1.4)**: Descrição da identificação do gerente da máquina gerenciada e informações de contato. Variável do tipo String.
     - **sysORLastChange (.1.3.6.1.2.1.1.8)**: Tempo transcorrido (em milhares de segundos) desde a última modificação ocorrida em alguma instância do equipamento. Variável do tipo TimeTicks.
   - **Nó Interfaces (.1.3.6.1.2.1.2)**: Lista as informações relativas às interfaces do equipamento.
     - **ifNumber (.1.3.6.1.2.1.2.1)**: Total de interfaces de rede existentes no equipamento (independente do estado atual delas). Variável do tipo Integer.
     - **ifAdminStatus (.1.3.6.1.2.1.2.2.1.7)**: Estado esperado para a interface. Variável do tipo Integer, tendo como possíveis valores *up(1)* ou *down(2)*.
     - **ifOperStatus (.1.3.6.1.2.1.2.2.1.8)**: Estado atual da interface. Variável do tipo Integer, tendo como possíveis valores *up(1)* ou *down(2)*.
     - **ifInOctets (.1.3.6.1.2.1.2.2.1.10)**: Número total de bytes recebidos pela interface. Variável do tipo Counter.
     - **ifOutOctets (.1.3.6.1.2.1.2.2.1.16)**: Número total de bytes enviados pela interface. Variável do tipo Counter.
   - **Nó AT (.1.3.6.1.2.1.3)**: Responsável pela tradução de endereços das interfaces do equipamento, mantido somente por questões de compatibilidade com outras versões da base MIB, sendo que não existirá na próxima versão da mesma (MIB-III).
     - **atIfIndex (.1.3.6.1.2.1.3.1.1.1)**: Identificador da interface do equipamento. Variável do tipo Integer.
     - **atPhysAddress (.1.3.6.1.2.1.3.1.1.2)**: Endereço físico da interface do equipamento. Variável do tipo String.
     - **atNetAddress (.1.3.6.1.2.1.3.1.1.3)**: Endereço de rede (IP) da interface do equipamento. Variável do tipo NetworkAddress.
   - **Nó IP (.1.3.6.1.2.1.4)**: Faz o mapeamento dos atributos do protocolo IP para o equipamento.
     - **ipForwarding (.1.3.6.1.2.1.4.1)**: Indica se o equipamento é um gateway. Variável do tipo Integer, podendo assumir os valores 1 (forwarding - equipamento é um gateway); ou 2 (notForwarding - equipamento não é um gateway).
     - **ipDefaultTTL (.1.3.6.1.2.1.4.2)**: Indica o valor default da variável TTL, responsável pelo número máximo de saltos que um datagrama IP pode realizar de um ponto a outro, dentro de uma rede. Variável do tipo Integer.
     - **ipInReceives (.1.3.6.1.2.1.4.3)**: Total de datagramas recebidos pelas interfaces, independente de terem ou não sido recebidos com sucesso. Variável do tipo Counter32.
     - **ipInHdrErrors (.1.3.6.1.2.1.4.4)**: Total de datagramas recebidos e descartados com erros em seus respectivos cabeçalhos. Variável do tipo Counter32.
   - **Nó ICMP (.1.3.6.1.2.1.5)**: Faz o mapeamento dos atributos do protocolo ICMP para o equipamento.
     - **icmpInMsgs (.1.3.6.1.2.1.5.1)**: Total de mensagens ICMP recebidas pelo equipamento, com ou sem erros no envio. Variável do tipo Counter32.
     - **icmpInErrors (.1.3.6.1.2.1.5.2)**: Total de mensagens ICMP recebidas pelo equipamento com algum erro especificado pelo protocolo ICMP. Variável do tipo Counter32.
     - **icmpInDestUnreachs (.1.3.6.1.2.1.5.3)**: Total de mensagens ICMP recebidas pelo equipamento com erro de destino não encontrado (Destination Unreachable). Variável do tipo Counter32.
     - **icmpOutMsgs (.1.3.6.1.2.1.5.14)**: Total de mensagens ICMP enviadas pelo equipamento, com ou sem erros no envio. Variável do tipo Counter32.
     - **icmpOutErrors (.1.3.6.1.2.1.5.15)**: Total de mensagens ICMP enviadas pelo equipamento com algum erro especificado pelo protocolo ICMP. Variável do tipo Counter32.

- **Nó TCP (.1.3.6.1.2.1.6)**: Faz o mapeamento dos atributos do protocolo TCP para o equipamento.
  - **tcpRtoMin(.1.3.6.2.1.6.2)**: Tempo mínimo permitido, em milisegundos, para a retransmissão de pacotes com erro de timeout para implementações TCP. Variável do tipo Integer.
  - **tcpMaxConn(.1.3.6.2.1.6.4)**: Número máximo de conexões TCP suportadas pelo equipamento. Variável do tipo Integer.
  - **tcpCurrentEstab (.1.3.6.2.1.6.9)**: Número de conexões TCP abertas no equipamento (estabelecidas ou à espera de fechamento). Variável do tipo Gauge.
  - **tcpInSegs (.1.3.6.2.1.6.11)**: Total de segmentos recebidos pelo equipamento, via protocolo TCP, com ou sem erro na transmissão. Variável do tipo Counter.
  - **tcpRetransSegs (.1.3.6.2.1.6.12)**: Número total de segmentos retransmitidos pelo equipamento, via protocolo TCP, após erro na transmissão anterior. Variável do tipo Counter.
- **Nó UDP (.1.3.6.1.2.1.7)**: Faz o mapeamento dos atributos do protocolo UDP para o equipamento.
  - **udpInDatagrams (.1.3.6.1.2.1.7.1)**: Total de datagramas UDP entregues aos usuários deste protocolo. Variável do tipo Counter.
  - **udpNoPorts (.1.3.6.1.2.1.7.2)**: Total de datagramas UDP recebidos para os quais não existia aplicação na porta especificada pelo datagrama. Variável do tipo Counter.
  - **udpInErrors (.1.3.6.1.2.1.7.3)**: Total de datagramas UDP recebidos com quaisquer erros, exceto erro de inexistência de aplicação na porta especificada pelo datagrama. Variável do tipo Counter.
  - **udpLocalAddress (.1.3.6.1.2.1.7.5.1.1)**: Endereço IP do usuário UDP do equipamento gerenciado. Variável do tipo IpAddress.
  - **udpLocalPort (.1.3.6.1.2.1.7.5.1.2)**: Número da porta do usuário UDP do equipamento gerenciado. Variável do tipo Integer.
- **Nó EGP (.1.3.6.1.2.1.8)**: Faz o mapeamento dos atributos do protocolo EGP, responsável por detectar equipamentos de rede e/ou redes que estejam conectados ao equipamento monitorado [26].
  - **egpInMsgs (.1.3.6.1.2.1.8.1)**: Total de mensagens EGP recebidas sem erro. Variável do tipo Counter.
  - **egpOutErrors (.1.3.6.1.2.1.8.4)**: Total de mensagens EGP que não puderam ser enviadas com sucesso. Variável do tipo Counter.
  - **egpNeighState (.1.3.6.1.2.1.8.5.1.1)**: Estado atual do sistema EGP em relação ao acesso a seu vizinho mais imediato. Variável do tipo Integer, podendo assumir os valores 1 (idle - inativo); 2 (acquisition - depois de solicitado o acesso); 3 (down - após confirmação de acesso); 4 (up - após o acesso, estabelecimento de conexão); ou 5 (cease - fim de utilização).
  - **egpNeighAddr (.1.3.6.1.2.1.8.5.1.2)**: Endereço IP do vizinho EGP do equipamento de rede monitorado. Variável do tipo IpAddress.
  - **egpAs (.1.3.6.1.2.1.8.6)**: Número identificador do Sistema Autônomo (AS) da entidade EGP. Sistema Autônomo pode ser entendido como por todo conjunto de redes e/ou equipamentos de rede que sejam administrados por uma entidade (empresa, administrador de redes, etc.) específica [26]. Variável do tipo Integer.
- **Nó Transmission (.1.3.6.1.2.1.10)**: Configurações de transmissão do elemento de rede.
- **Nó SNMP (.1.3.6.1.2.1.11)**: Faz o mapeamento dos atributos do protocolo SNMP para o equipamento.
  - **snmpInPkts (.1.3.6.1.2.1.11.1)**: Total de mensagens recebidas pelo equipamento monitorado pelo protocolo SNMP. Variável do tipo Counter.
  - **snmpOutPkts (.1.3.6.1.2.1.11.2)**: Total de mensagens enviadas pelo equipamento monitorado pelo protocolo SNMP. Variável do tipo Counter.
  - **snmpInTotalReqVars (.1.3.6.1.2.1.11.13)**: Total de objetos da base MIB resgatados pelo equipamento monitorado pelo protocolo SNMP. Variável do tipo Counter.

3. O PROTOCOLO SNMP

O protocolo SNMP é largamente utilizado para monitoramento de desempenho e funcionamento de diversos equipamentos de rede, tais como roteadores, switches, servidores, etc [27].

Este protocolo tem como objetivos a flexibilidade e a facilidade de sua implementação, sua especificação pode ser encontrada na RFC1157, publicada em 1990 [4].

Para entender o funcionamento do protocolo SNMP, é preciso compreender os conceitos que lhe servem como base. O funcionamento do protocolo SNMP se baseia em dois dispositivos: o agente e o gerente. Cada máquina é vista como um conjunto de dados e variáveis que representam estatísticas do estado atual do agente, estatísticas essas que ficam disponíveis ao gerente para consulta e/ou edição. Cada máquina gerenciada via protocolo SNMP deverá possuir um agente e uma base MIB associada a este agente, apresentando as estatísticas obtidas do mesmo.

A figura 2 apresenta a ideia básica da comunicação entre agentes e gerentes via protocolo SNMP.

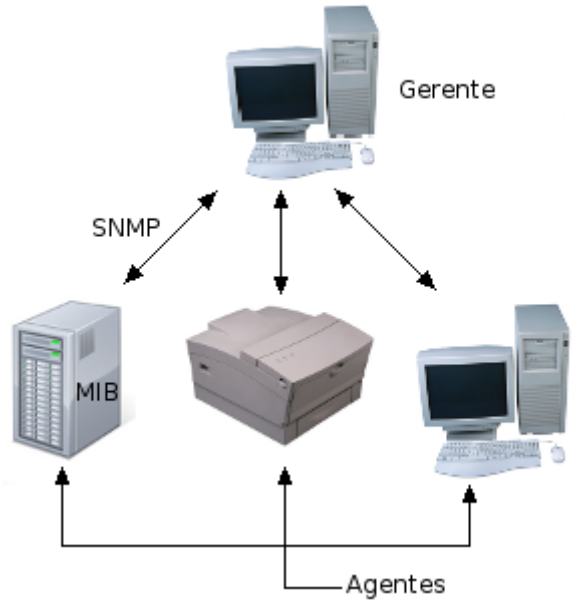


Figura 2: Funcionamento do protocolo SNMP

- **Agente**: Executado na máquina gerenciada pelo protocolo SNMP, guardando as estatísticas de gerência da máquina, estatísticas estas estruturadas em uma base de dados MIB. Suas funções principais são:
  - Atender às requisições enviadas pelo gerente (servidor).
  - Enviar informações de gerenciamento ao gerente (servidor), quando programado para tal.
- **Gerente**: Executado a partir de uma máquina atuando como um servidor, permitindo obtenção e envio de estatísticas do gerenciamento através da comunicação com o(s) agente(s).

O protocolo SNMP opera na camada de aplicação da rede, a qual é a última camada do modelo TCP/IP [3][4]. O protocolo SNMP é utilizado para obtenção de estatísticas de equipamentos conectados a determinados computadores operando como servidores, equipamentos estes operando em uma rede baseada nos protocolos do modelo de redes TCP/IP. Os dados são obtidos via requisições de um dado gerente a um ou mais agentes, para isto utilizando-se o protocolo de transporte UDP - User Datagram Protocol, responsável pelas atividades de envio e recebimento de mensagens através de uma rede qualquer. O tipo de informação mais significativo que pode ser obtido via protocolo SNMP consiste na base de dados MIB, que estrutura hierarquicamente os dados de todas as interfaces agregadas ao equipamento de rede pesquisado, organizando assim todas as estatísticas relacionadas a este equipamento em especial.

Os aplicativos do protocolo SNMP se baseiam no mecanismo de busca/alteração, ou seja, estão disponíveis as operações de alteração de um valor de uma estatística, de obtenção dos valores de uma estatística e suas variações. A quantidade de aplicativos disponibilizada pelo protocolo SNMP é reduzida, o que facilita sua implementação, tornando-a mais simples, estável e flexível. Esta limitação de aplicativos disponíveis ajuda a reduzir o tráfego de mensagens de gerenciamento através da rede. Já a simplicidade do protocolo SNMP permite que este seja utilizado em diversas aplicações de gerenciamento de redes; e sua estabilidade e flexibilidade permitem a possibilidade de se acrescentar estatísticas novas à base MIB do equipamento gerenciado [1].

Para se realizar o monitoramento de equipamentos de rede via protocolo SNMP, o equipamento gerente envia continuamente mensagens SNMP aos agentes gerenciados, a fim de obter suas respectivas estatísticas. Os campos de uma mensagem de gerenciamento do protocolo SNMP estão estruturados da seguinte forma:

1. **Mensagem SNMP**: Trata-se da mensagem SNMP na sua visão mais geral, baseada em três partes principais. São elas:
   - **version**: Versão do protocolo SNMP.
   - **community**: Uma senha criada para o controle de acesso e/ou edição às estatísticas de um agente via protocolo SNMP.
   - **SNMP PDU**: Espaço da mensagem SNMP onde ficam registradas as configurações da mensagem, de acordo com o tipo de mensagem SNMP enviada, tipo este que pode ser *GetRequest*, *GetNextRequest*, *SetRequest*, *GetResponse* e *Trap*.
2. **GetRequestPDU, GetNextRequestPDU e SetRequestPDU**: Mensagens de envio e recepção de requisições do protocolo SNMP, por parte de um dado gerente. A estrutura do espaço SNMP PDU para este tipo de mensagem possui os seguintes campos:
   - **PDU Type**: Tipo de mensagem SNMP (neste caso, podem ser *GetRequestPDU*, *GetNextRequestPDU* ou *SetRequestPDU*) enviada pelo gerente.
   - **request-id**: Identificador da requisição.
   - **error-status**: Indica se ocorreu erro no processamento da mensagem. Para mensagens do tipo *request* (*GetRequestPDU*, *GetNextRequestPDU* e *SetRequestPDU*), esta variável apresentará sempre valor 0.
   - **error-index**: Quando um *error-status* é diferente de 0, este campo fornece informações adicionais sobre a variável da mensagem SNMP que gerou erro em error-status. Para mensagens do tipo *request* (*GetRequestPDU*, *GetNextRequestPDU* e *SetRequestPDU*), esta variável apresentará sempre valor 0.
   - **variable-bindings**: Uma lista de nomes de variáveis e seus respectivos valores.
3. **GetResponsePDU**: Mensagens de obtenção de resposta a requisições SNMP, para um dado gerente. A estrutura do espaço SNMP PDU para este tipo de mensagem possui os mesmos campos que aparecem nas mensagens de envio e recepção de requisições, com a diferença de que os campos *error-status* e *error-index* podem apresentar valores diferentes de 0.

4. **TrapPDU**: Mensagens de notificações SNMP, enviadas para um gerente. A estrutura do espaço SNMP PDU para este tipo de mensagem possui os seguintes campos:

    - **PDU Type**: Tipo de mensagem SNMP (neste caso, *TrapPDU*) enviada pelo gerente.
    - **enterprise**: Tipo do objeto gerador da mensagem trap.
    - **generic-trap**: Mensagem trap genérica, ou mensagem padrão de notificação do protocolo SNMP.
    - **specific-trap**: Código da mensagem trap.
    - **time-stamp**: Intervalo de tempo entre a última (re)inicialização da entidade de rede(agente) e a geração da mensagem trap.

5. **variable-bindings**: Listagem de nomes de variáveis e seus valores. Esta listagem segue sempre o padrão de colocar primeiro o nome variável, imediatamente seguido pelo valor contido na mesma.

A figura 3 apresenta a estrutura de uma mensagem SNMP que é enviada, quando da requisição de estatísticas sobre um dado agente na rede [23]:

O gerenciamento de redes através do protocolo SNMP é conhecido como modelo de gerenciamento SNMP, ou gerenciamento SNMP, o qual permite o acompanhamento simples do estado atual da rede monitorada, em tempo real.

3.1. Funcionamento dos aplicativos mais utilizados do protocolo SNMP

Nesta seção, serão apresentados alguns dos aplicativos mais utilizados no protocolo SNMP, seu funcionamento e sua sintaxe básica.

Antes de iniciar a descrição propriamente dita sobre estes aplicativos, é pertinente esclarecer algumas nomenclaturas utilizadas na sintaxe básica das linhas de comando destes aplicativos.

O termo COMMON FLAGS representa os parâmetros de acesso mais utilizados pelos aplicativos do protocolo SNMP, como *version* (-v) e *community* (-c), parâmetros estes que normalmente são obrigatórios para o acesso a um equipamento de rede, mas havendo também casos em que os mesmos podem ser opcionais, caso não hajam restrições de acesso ao equipamento.

O termo OPTIONS representa os parâmetros diversos de configuração do aplicativo em questão, que podem ser utilizados para definir formas especifícas de acesso a dadas informações do equipamento monitorado.

O termo HOST representa o equipamento acessado pelo aplicativo. Este termo pode vir em forma textual, ou na forma do endereço IP do equipamento.

O termo OID representa a estatística a ser acessada pelo aplicativo, quando for o caso. Pode aparecer como nome textual da mesma, ou como o identificador OID desta.

Uma vez esclarecidas as nomenclaturas utilizadas, pode-se então descrever os aplicativos do protocolo SNMP propriamente ditos. São eles [27]:

1. **snmptranslate**:

    - **Descrição**: Este aplicativo traduz um ou mais identificadores de objetos SNMP de sua forma de string para o correspondente numérico da mesma, ou vice-versa.
    - **Sintaxe Básica**: *snmptranslate [OPTIONS] OID [OID] ...*

2. **snmpwalk**:

    - **Descricão**: Retorna uma sub-árvore de valores de gerenciamento, com seus respectivos dados, utilizando requisições SNMP do tipo GETNEXT, onde a requisição obtém o próximo identificador OID, a partir do identificador que foi passado como argumento de entrada no aplicativo *snmpwalk*. O identificador OID especifica a parte da estatística que será procurada na requisição, retornando assim todas as variáveis da sub-árvore com raiz no identificador OID especificado para o usuário.

      Caso não seja passado nenhum identificador OID na linha de comando do aplicativo, será utilizado como valor default o SNMPv2-SMI::mib-2, junto com todos os valores de objetos de outros módulos MIB que estejam incluídos na sub-árvore gerada a partir do identificador default.

      Ocorrendo erro na rede, durante o processamento da requisição, um pacote de ero será enviado, junto com uma mensagem discriminando o que está incorreto na requisição.

      Se a construção da sub-árvore causar uma busca que exceda o fim da base de estatísticas da rede, a mensagem "End of MIB" será mostrada ao usuário.
    - **Sintaxe básica**: *snmpwalk [COMMON FLAGS] [OPTIONS] HOST [OID]*

3. **snmpdelta**:

    - **Descricão**: Aplicativo utilizado para monitorar, ao longo do tempo, a variação de valores de uma determinada estatística do equipamento monitorado. Esta monitoração apresenta, a cada segundo, a diferença entre o valor atual da estatística e o valor que ela apresentava no segundo anterior.

      Este aplicativo pode ser utilizado também para apresentar variações de mais de uma estatística simultaneamente. Para isto, deverão ser passados na linha de comando os identificadores OID das estatísticas de interesse.
    - **Sintaxe básica**: *snmpdelta [COMMON FLAGS] [OPTIONS] HOST OID [OID] ...*

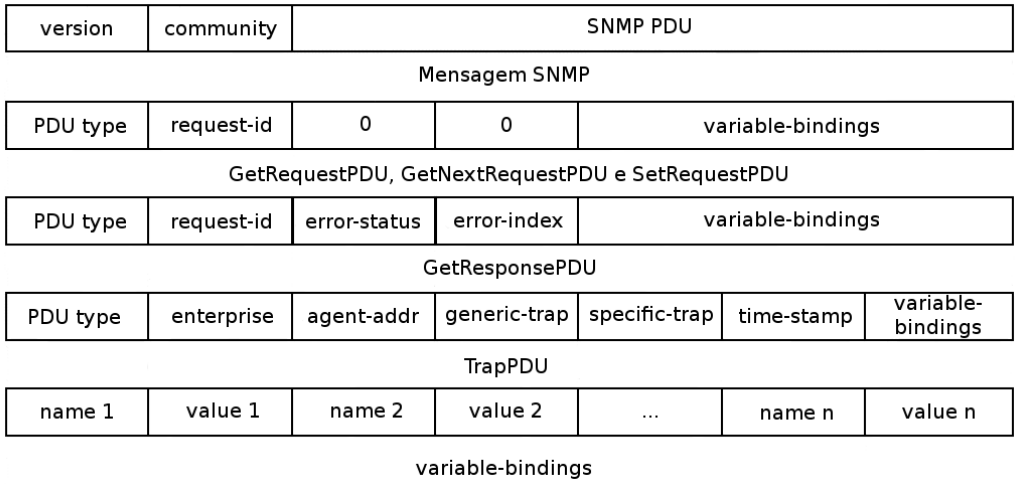


Figura 3: Formato de uma mensagem SNMP

4. **snmpget**:
   - **Descrição**: Enquanto o aplicativo *snmpwalk* retorna uma sub-árvore com raiz no HOST, o aplicativo snmpget retorna a string de um único identificador OID, juntamente com a estatística associada ao mesmo. É possível colocar mais de um identificador como parâmetro de entrada no aplicativo, de modo que, cada linha da saída retornada corresponderá a um identificador OID passado na entrada (funcionalidade disponível a partir da versão 2 do SNMP, na versão 1 só é possível se passar um identificador OID por entrada).
   - **Sintaxe básica**: *snmpget [COMMON FLAGS] HOST OID [OID] ...*
5. **snmpgetnext**:
   - **Descrição**: Opera de forma similar ao aplicativo *snmpget*, no entanto retorna a string do identificador OID imediatamente posterior - na base MIB do equipamento monitorado - ao identificador passado como argumento na linha de comando do aplicativo, juntamente com a estatística associada ao mesmo.
   - **Sintaxe básica**: *snmpgetnext [COMMON FLAGS] [OPTIONS] HOST OID [OID] ...*
6. **snmpset**:
   - **Descrição**: Aplicativo utilizado para escrever um determinado valor em alguma estatística do equipamento gerenciado. A linha de comando do aplicativo deve conter o tipo de variável da estatística - tipo este que deve ser compatível com o tipo de dado definido previamente para esta estatística - e o valor a ser escrito.
   - **Sintaxe básica**: *snmpset [COMMON FLAGS] [OPTIONS] HOST OID TYPE VALUE [OID TYPE VALUE] ...*
7. **snmpdf**:
   - **Descrição**: Aplicativo utilizado para obter a quantidade de espaço disponível em disco do equipamento monitorado, analisando o quanto de espaço está sendo ocupado pelos processos em operação no mesmo.
   - **Sintaxe básica**: *snmpdf [COMMON FLAGS] [OPTIONS] HOST*
8. **snmpnetstat**:
   - **Descrição**: Aplicativo utilizado para apresentar informações diversas de rede sobre o equipamento monitorado. Estas informações são organizadas no formato de tabela, e podem representar desde a relação de conexões estabelecidas por elementos integrantes do equipamento a outros pontos de rede; até estatísticas das interfaces do equipamento (por exemplo, pacotes recebidos e enviados).
   - **Sintaxe básica**: *snmpnetstat [COMMON FLAGS] [OPTIONS] HOST*
9. **snmpstatus**:
   - **Descrição**: Aplicativo utilizado para apresentar o status geral do equipamento monitorado. Este status mostra:
     - O endereço IP do equipamento.
     - Uma descrição geral do equipamento.
     - A última vez em que o gerenciamento do equipamento via protocolo SNMP foi inicializado.
     - O total de pacotes recebidos por todas as interfaces do equipamento.
     - O total de pacotes enviados por todas as interfaces do equipamento.
     - O total de datagramas IP recebidos pelas interfaces.

  - O total de datagramas IP enviados pelas interfaces.

- **Sintaxe básica**: *snmpstatus [COMMON FLAGS] [OPTIONS] HOST*

3.2. Vantagens e desvantagens na utilização do protocolo SNMP

Nesta seção, serão analisadas as vantagens e as limitações do protocolo SNMP, em termos de utilização. Além disto, serão propostas algumas práticas capazes de contornar as limitações apresentadas por este protocolo.

Diante dos aspectos apresentados ao longo desta nota técnica; especialmente no que diz respeito a este capítulo, a importância do protocolo SNMP para o desenvolvimento de sistemas de gerência e monitoração de redes de computadores e seus respectivos equipamentos pode ser verificada em aspectos como:

- A segurança que o protocolo SNMP oferece aos sistemas que o utilizam, em função da obrigatoriedade do emprego de senhas (*communities*), quando da busca por uma determinada estatística de interesse, ou para modificar valores de variáveis internas responsáveis por estatísticas do equipamento. Também é válido observar que o emprego de *communities* permite que o usuário acesse apenas algumas estatísticas do equipamento, estatísticas cujo acesso esteja habilitado pela *community* em questão. Com esta prática, é possível haver vários usuários acessando simultaneamente estatísticas distintas do equipamento, com *communities* diferentes.

- A simplicidade de instalação e implementação do protocolo, permitindo que o mesmo seja utilizado em diversas aplicações de gerência de equipamentos de rede, sem grandes dificuldades técnicas em sua utilização. Em princípio não é preciso se instalar nenhum outro software específico antes da instalação do protocolo SNMP propriamente dito, caso este seja utilizado apenas no formato de linhas do comando em terminais UNIX; por outro lado, para a utilização do protocolo SNMP em plataformas Web baseadas na linguagem de programação PHP, é preciso instalar um pacote de integração entre a linguagem PHP e o protocolo SNMP, para que os aplicativos do protocolo possam ser utilizados plenamente via Web, mas esta instalação também não demanda elevado grau de dificuldade. Conforme mencionado neste parágrafo, é possível se utilizar o protocolo SNMP em sistemas de gerenciamento de redes baseados em páginas Web, o que será ilustrado no capítulo 4.

- A possibilidade de se expandir a utilização do protocolo SNMP, onde, a partir de sua implementação básica, poderão ser criadas novas variáveis para armazenar novas estatísticas na base MIB do equipamento monitorado. Um exemplo disto são as bases de dados MIB dos tipos experimental e privada, onde, conforme visto no capítulo 2, é possível criar novas estatísticas na base MIB, de modo a contemplar demandas específicas do equipamento a ser monitorado.

- Dificilmente mensagens enviadas pelo protocolo SNMP de um ponto de rede a outro causam congestionamento na rede, graças à quantidade reduzida de aplicativos disponíveis para este protocolo; e graças também à possibilidade de se obter, através da base de dados MIB, todas as estatísticas de um dado equipamento de rede de forma simples, através da utilização do aplicativo *snmpwalk*, que retorna a estatística de forma imediata.

Como limitações na utilização do protocolo SNMP, foram observados os fatores a seguir:

- A simplicidade da implementação do protocolo, ao mesmo tempo em que facilita seu uso, pode se tornar um problema em equipamentos com muitos itens existentes em sua base de dados MIB, uma vez que tais itens podem se tornar de difícil obtenção, caso não se conheça a estrutura desta base MIB.

- Outro problema relacionado com a simplicidade de implementação do protocolo SNMP reside no fato de que equipamentos com quantidades elevadas de interfaces e/ou estatísticas associadas a ele podem retornar muitas estatísticas desnecessárias para o que o usuário necessita, tornando mais difícil a utilização do protocolo, no que diz respeito àquilo que é verdadeiramente necessário ao usuário, em termos de estatísticas de interesse para o gerenciamento de redes.

- Uma última limitação observada é que, caso não haja possibilidade de estabelecer comunicação entre o gerente e o equipamento de rede monitorado através do protocolo SNMP, não será mais possível se obter ou modificar quaisquer estatísticas deste equipamento via protocolo SNMP.

Ao mesmo tempo em que foram observadas limitações no uso do protocolo SNMP, algumas possíveis soluções foram observadas para contornar estas limitações. São elas:

- Mapear, de forma clara e bem definida, o conjunto de estatísticas do(s) equipamento(s) a ser(em) monitorado(s); e realizar um constante monitoramento de todas estas variáveis ao longo do tempo. Desta forma, será possível sempre se saber como a base MIB do equipamento está estruturada; o que é realmente necessário para o usuário, em termos de estatísticas a serem monitoradas; e ainda ter controle sobre eventuais perdas de comunicação com equipamentos monitorados.

- Outra medida proposta como solução consiste em restringir ao máximo os critérios de busca para de qualquer estatística de ineteresse em um dado equipamento, através do identificador OID vinculado à mesma. Desta maneira, caso a base MIB do equipamento possua uma quantidade elevada de objetos associados a ela, reduz-se o grau de dificuldade em se obter qualquer estatística de interesse.

4. AMBIENTES E FERRAMENTAS DE IMPLEMENTAÇÃO

4.1. Ambientes e ferramentas utilizadas

Nesta seção, serão apresentados os ambientes e ferramentas utilizados para a implementação prática do protocolo SNMP, bem como a forma como esta implementação foi realizada.

Para a implementação prática, foi montada uma plataforma LAMP, acrônimo para os aplicativos Linux, Apache, MySQL e PHP, as tecnologias empregadas nesta plataforma. A distribuição utilizada do Linux é a Ubuntu, versão 9.10; em conjunto com as versões 2.2.12 do Apache, 5.1.37 do MySQL, e 5 do PHP. Este projeto também utilizou o aplicativo PHPMyAdmin, versão 3.2.2.1deb1, o qual oferece uma interface via browser para o usuário administrar o banco MySQL, sendo assim mais amigável e intuitivo para uso, quando comparado com aplicativos convencionais de gerência de bancos de dados.

4.2. Implementação

Para esta nota, a implementação do protocolo SNMP se deu sob duas abordagens distintas. Na primeira, executou-se a simulação simples do aplicativo *snmpwalk*, via prompt, retornando todas as estatísticas dos equipamentos de rede associados a um dado servidor, passado como parâmetro através de seu endereço IP; na outra abordagem, através de um aplicativo de gerência e monitoramento de redes, que utiliza o aplicativo *snmpwalk* para levantar todas as interfaces existentes de cada equipamento, bem como os dados técnicos e status das interfaces do equipamento monitorado.

4.2.1. Implementação via prompt

Um exemplo de implementação via prompt pode ser definido pela sintaxe básica do aplicativo *snmpwalk*:

snmpwalk [COMMON FLAGS] [OPTIONS] HOST [OID]

Conforme descrito no capítulo 3. Para ilustrar este trabalho, serão apresentados dois exemplos de execução do aplicativo *snmpwalk*: Uma execução simples, a partir de um dado endereço IP, retornando todos os elementos de rede conectados ao host associado a este endereço; e uma execução mais específica, onde, a partir de um dado host, busca-se um atributo específico de um dado elemento de rede conectado ao host.

Por medida de simplicidade, o exemplo com o aplicativo *snmpwalk* geral será rodado a partir de um host de um computador pessoal, com poucos elementos de rede conectados ao mesmo. O aplicativo *snmpwalk* executado terá a seguinte forma:

snmpwalk -v 2c -c public localhost

O qual apresentou o resultado abaixo:

root@antonio-desktop:~# snmpwalk -v 2c -c public localhost
SNMPv2-MIB::sysDescr.0 = STRING: Linux antonio-desktop 2.6.31-14-generic #48-Ubunt
u SMP Fri Oct 16 14:04:26 UTC 2009 i686
(...)
SNMPv2-MIB::sysName.0 = STRING: antonio-desktop
(...)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCom
pliance
(...)
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
(...)

Exemplificando alguns valores obtidos no caso acima:

- A variável *sysDescr* (.1.3.6.1.2.1.1.1) retornou a descrição do equipamento gerenciado, incluindo o sistema operacional e a data de início da operação do mesmo.
- A variável *sysName* (.1.3.6.1.2.1.1.5) retornou o nome admininstrativo dado ao sistema operacional do equipamento gerenciado.
- A variável *sysORLastChange* (.1.3.6.1.2.1.1.8) retornou o tempo transcorrido desde a última modificação ocorrida em alguma instância do equipamento.
- A variável *sysORID.1* (.1.3.6.1.2.1.1.9.1.2.1) retornou um dos identificadores de funcionalidades que o equipamento em questão é capaz de realizar. Neste caso, o identificador relativo à base de dados MIB.
- A variável *sysORDescr.1* (.1.3.6.1.2.1.1.9.1.3.1) retornou uma das descrições de funcionalidades que o equipamento em questão é capaz de realizar. Neste caso, uma referência à base de dados MIB.

No segundo exemplo, serão obtidas as interfaces conectadas a um dado equipamento - cujos endereço IP e *community* reais foram omitidos por questões de segurança - como exemplo do funcionamento do aplicativo *snmpwalk* para obtenção de dados específicos de um equipamento. A execução do aplicativo neste exemplo terá a seguinte forma:

snmpwalk -v 2c -c public 10.0.94.244 .1.3.6.1.2.1.2.2.1.2

O qual apresentou o resultado abaixo:

root@antonio-desktop:~# snmpwalk -v 2c -c public 10.0.94.244 .1.3.6.1.2.1.2.2.1.2
IF-MIB::ifDescr.1 = STRING: Serial3/0
(...)

IF-MIB::ifDescr.3 = STRING: FastEthernet0/0
(...)
IF-MIB::ifDescr.12 = STRING: Ethernet2/0
(...)
IF-MIB::ifDescr.24 = STRING: Null0
IF-MIB::ifDescr.25 = STRING: Loopback0
(...)
IF-MIB::ifDescr.27 = STRING: Multilink100

É interessante observar no exemplo acima que o aplicativo *snmpwalk*, ao listar as interfaces de um equipamento, consegue detectar tanto as interfaces reais, ou seja, as que possuem estrutura física, como as interfaces do tipo Serial, FastEthernet ou Ethernet; quanto as interfaces virtuais, que possuem somente estrutura lógica, como as interfaces do tipo Null, Loopback ou Multilink.

4.2.2. Implementação via aplicativo de gerência Web

Na implementação via aplicativo de gerência Web, podemos ver alguns exemplos práticos de como a utilização do protocolo SNMP viabiliza as atividades de monitoração e gerência de rede, com o uso de uma interface Web. Nisto, pode-se destacar a possibilidade de se monitorar estatísticas como o tráfego de rede que passa pela interface; ou ainda verificar o status das interfaces do equipamento monitorado, quanto a quantidades de pacotes recebidos/enviados, funcionamento da interface propriamente dita etc.

Na figura 4, pode-se observar a utilização do aplicativo *snmpwalk* para obter a listagem de interfaces de um dado equipamento, através de busca pela estatística *ifDescr* (.1.3.6.1.2.1.2.2.1.2), o qual retorna os nomes de todas as interfaces do equipamento; e o elemento MIB *locIfDescr*, ou *ifDescr2* (.1.3.6.1.4.1.9.2.2.1.1.28), que retorna o nome da instituição cadastrado diretamente a cada interface do equipamento, embora neste exemplo, o cadastro de equipamento também foi efetuado de forma manual, em um sistema específico desenvolvido para gerenciar equipamentos de rede. Já na figura 5, o aplicativo *snmpwalk* é empregado para obter as estatísticas, status, etc. de uma das interfaces propriamente ditas.

Exemplificando alguns valores obtidos na figura 5:

- A variável *ifSpeed* (.1.3.6.1.2.1.2.2.1.5.24) retornou a taxa estimada de velocidade de banda da interface 24 (FastEthernet0/24) do equipamento, em bits por segundo.
- A variável *ifPhysAddress* (.1.3.6.1.2.1.2.2.1.6.24) retornou o endereço físico (MAC Address) da interface 24 (FastEthernet0/24) do equipamento.
- A variável *ifAdminStatus* (.1.3.6.1.2.1.2.2.1.7.24) retornou o status operacional esperado para a interface 24 (FastEthernet0/24) do equipamento, neste caso, o status está com o valor 1 (up), ou seja, espera-se que a interface esteja operando normalmente.
- A variável *ifLastChange* (.1.3.6.1.2.1.2.2.1.9.24) retornou o intervalo de tempo em que a interface 24 (FastEthernet0/24) do equipamento está initerruptamente operacional, em milhares de segundos.
- A variável *ifInOctets* (.1.3.6.1.2.1.2.2.1.10.24) retornou o total de bytes (octetos) recebidos pela interface 24 (FastEthernet0/24) do equipamento.

Interfaces:

#	Nome	ifDescr2
1	FastEthernet0/1	
18	FastEthernet0/18	
20	FastEthernet0/20	
21	FastEthernet0/21	
23	FastEthernet0/23	
24	FastEthernet0/24	UP-Link 7600
25	GigabitEthernet0/1	
26	GigabitEthernet0/2	
27	Null0	
28	Vlan1	
29	Vlan94	VLAN 94

Figura 4: Lista de interfaces obtidas via aplicativo *snmpwalk*

Detalhes da interface: FastEthernet0/24

Estatística	Dado
ifIndex	24
ifDescr	FastEthernet0/24
ifType	ethernetCsmacd(6)
ifMtu	1500
ifSpeed	100000000
ifPhysAddress	0:d:bc:b4:3f:18
ifAdminStatus	up(1)
ifOperStatus	up(1)
ifLastChange	(9176) 0:01:31.76
ifInOctets	1180431405
ifInUcastPkts	899743584
ifInNUcastPkts	6318886
ifInDiscards	0
ifInErrors	0
ifInUnknownProtos	0
ifOutOctets	737597771
ifOutUcastPkts	240214956
ifOutNUcastPkts	3894405
ifOutDiscards	0
ifOutErrors	0
ifOutQLen	0
ifSpecific	SNMPv2-SMI::zeroDotZero

Figura 5: Dados de interface obtidos via aplicativo *snmpwalk*

Cabe observar que, em ambas as abordagens sob as quais o aplicativo *snmpwalk* foi utilizado; seja via linha de comando em terminal do sistema operacional Linux, ou via aplicação Web; o aplicativo em si sempre retornará os mesmos resultados, variando apenas a forma como os mesmos estarão dispostos na interface de saída.

5. CONCLUSÃO

Esta nota técnica apresentou o protocolo de gerenciamento de equipamentos de rede SNMP - Simple Network Management Protocol.

Após as apresentações do contexto histórico; das motivações para a criação do protocolo SNMP; e dos conceitos básicos pertinentes ao mesmo, foram apresentados alguns exemplos práticos de sua utilização, para obtenção de dados de interesse acerca de um dado equipamento: o primeiro, com a execução do aplicativo *snmpwalk* via linha de comando no Sistema Operacional Linux, buscando os elementos de rede relacionados a um PC comum, que pode ser encontrado em qualquer residência; e o segundo, onde o mesmo aplicativo *snmpwalk* é utilizado para se obter, primeiramente a listagem de interfaces de rede conectadas a um equipamento; e, em seguida, algumas estatísticas de uma interface deste mesmo equipamento, e estes resultados sendo então disponibilizados em um sistema Web de monitoramento e gerência de redes, ressaltando assim a utilidade do protocolo SNMP em gerenciamento Web de equipamentos de rede.

Diante dos aspectos apresentados nos parágrafos anteriores, e ao longo da nota, mostra-se então a importância do protocolo SNMP para o desenvolvimento de sistemas de gerência e monitoração de equipamentos diversos de redes de computadores. Esta importância pode ser verificada em aspectos como:

- A segurança oferecida pelo protocolo, devido à obrigatoriedade da utilização de senhas (communities), quando da busca por uma determinada estatística de interesse, ou para modificar valores de variáveis internas responsáveis por estatísticas do equipamento.
- A simplicidade de implementação do protocolo, a qual permite que o mesmo seja utilizado em diversas aplicações de gerência de equipamentos de rede, sem grandes dificuldades técnicas em sua utilização.
- A flexibilidade do protocolo SNMP, possibilitando que, a partir de sua implementação básica, sejam criadas novas variáveis para armazenamento de estatísticas do equipamento monitorado.
- O fato que dificilmente as mensagens do protocolo SNMP ocasionam congestionamento na rede, em função da quantidade reduzida de aplicativos disponíveis para este protocolo; e a possibilidade de se obter, através da base de dados MIB, todas as estatísticas de um dado equipamento de rede de forma simples.

Por outro lado, pode-se destacar também algumas desvantagens do protocolo SNMP, tais como:

- A simplicidade da implementação do protocolo pode se tornar um problema em equipamentos com muitos itens existentes em sua base de dados MIB, no sentido de que tais itens podem se tornar de difícil obtenção, caso não se conheça a estrutura da base MIB em questão
- Equipamentos com muitas interfaces e/ou estatísticas podem acabar retornando uma série de estatísticas desnecessárias para o usuário, diminuindo a eficiência do protocolo e dificultando ao usuário o acesso ao que é verdadeiramente necessário a este.
- Se por alguma razão não houver mais a possibilidade de se alcançar um equipamento de rede através do protocolo SNMP, não haverá mais como obter ou modificar as estatísticas deste equipamento via SNMP.

Como soluções para as desvantagens apresentadas, podem ser realizadas práticas como:

- Mapeamento bem definido e constante monitoração de todas as variáveis contidas em um dado equipamento.
- Sempre que for necessário se obter uma estatística qualquer via protocolo SNMP, buscar se restringir ao máximo os critérios de busca para a mesma, através do identificador OID vinculado à estatística em questão.

---

[1] Beethovem Z. Dias; Nilton A. Jr. "Protocolo de gerenciamento SNMP". *Nota Técnica CBPF-NT-006/01*, 2001.

[2] Douglas R. Mauro; Kevin J. Schmidt. *SNMP Essencial*. Editora Campus, 2001. ISBN 8535208828.

[3] James F. Kurose; Keith W. Ross. *Computer Networking: a Top-Down Approach Featuring the Internet*. Addison-Wesley, 2006. ISBN 8588639181.

[4] J. Case; M. Fedor; M. Schoffstal; J. Davin. A simple network management protocol(SNMP) - RFC1157. Technical report, 1990.

[5] M. Schoffstall J. Davin; J. Case, M. Fedor. A simple gateway monitoring protocol - RFC1028. Technical report, 1987.

[6] S. Bradner. The internet standards process – revision 3 - RFC2026. Technical report, 1996.

[7] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Strucuture of management information for version 2 of the simple network management protocol (SNMPv2) - RFC1902. Technical report, 1996.

[8] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Textual coventions for version 2 of the simple network management protocol (SNMPv2) - RFC1903. Technical report, 1996.

[9] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Conformance statements for version 2 of the simple network management protocol (SNMPv2) - RFC1904. Technical report, 1996.

[10] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Protocol operations for version 2 of the simple network management protocol (SNMPv2) - RFC1905. Technical report, 1996.

[11] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Transport mappings for version 2 of the simple network management protocol (SNMPv2) - RFC1906. Technical report, 1996.

[12] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Management information base for version 2 of the simple network management protocol (SNMPv2) - RFC1907. Technical report, 1996.

[13] J. Case; K. McCloghrie; M. Rose; S. Waldbusser. Coexistence between version 1 and version 2 of the internet-standard network management framework - RFC1908. Technical report, 1996.

[14] K. McCloghrie. An administrative infrastructure for SNMPv2 - RFC1909. Technical report, 1996.

[15] J. Case; R. Mundy; D. Partain; B. Stewart. Introduction to version 3 of the internet-standard network management framework - RFC2570. Technical report, 1999.

[16] D. Harrington; R. Presuhn; B. Wijnen. An architecture for describing snmp management frameworks - RFC2571. Technical report, 1999.

[17] J. Case; D. Harrington; R. Presuhn; B. Wijnen. Message processing and dispatching for the simple network management protocol (snmp) - RFC2572. Technical report, 1999.

[18] D. Levi; P. Meyer; B. Stewart. Snmp applications - RFC2573. Technical report, 1999.

[19] U. Blumenthal; B. Wijnen. User-based security model (usm) for the simple network management protocol (snmpv3) - RFC2574. Technical report, 1999.

[20] B. Wijnen; R. Presuhn; K. McCloghrie. View-based access control model (vacm) for the simple network management protocol (snmp) - RFC2575. Technical report, 1999.

[21] K. McCloghrie; M. Rose. Management information base for network management of TCP/IP-based internets: MIB II - RFC1213. Technical report, 1991.

[22] K. McCloghrie; M. Rose. Management information base for network management of TCP/IP-based internets - RFC1066. Technical report, 1988.

[23] Grupo de Redes da Universidade Federal do Rio Grande do Sul. Especificação do protocolo SNMP; `http://penta.ufrgs.br/gr952/trab1/snmp_especificacao.html/`, Dezembro de 1995; Acessado em 17 de Setembro de 2011.

[24] Cisco Systems Inc. SNMP Object Navigator; `http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en`, Maio de 2011; Acessado em 17 de Setembro de 2011.

[25] K. McCloghrie; M. Rose. Structure and identification of management information for TCP/IP-based internets - RFC1155. Technical report, 1990.

[26] Lisiane Hartmann. Protocolo de Roteamento EGP; `http://penta.ufrgs.br/rc952/Lisiane/lis220.html`, Setembro de 1995; Acessado em 3 de Dezembro de 2011.

[27] SourceForge.net. Tutorial para utilização do protocolo SNMP; `http://www.net-snmp.org/`, Março de 2007; Acessado em 17 de Setembro de 2011.

Notas Técnicas é uma publicação de trabalhos técnicos relevantes, das diferentes áreas da física e afins, e áreas interdisciplinares tais como: Química, Computação, Matemática Aplicada, Biblioteconomia, Eletrônica e Mecânica entre outras.

Cópias desta publicação podem ser obtidas diretamente na página web http://notastecnicas.cbpf.br ou por correspondência ao:

Centro Brasileiro de Pesquisas Físicas
Área de Publicações
Rua Dr. Xavier Sigaud, 150 – 4º andar
22290-180 – Rio de Janeiro, RJ
Brasil
E-mail: socorro@cbpf.br/valeria@cbpf.br
http://www.biblioteca.cbpf.br/index_2.html

Notas Técnicas is a publication of relevant technical papers, from different areas of physics and related fields, and interdisciplinary areas such as Chemistry, Computer Science, Applied Mathematics, Library Science, Electronics and Mechanical Engineering among others.

Copies of these reports can be downloaded directly from the website http://notastecnicas.cbpf.br or requested by regular mail to:

Centro Brasileiro de Pesquisas Físicas
Área de Publicações
Rua Dr. Xavier Sigaud, 150 – 4º andar
22290-180 – Rio de Janeiro, RJ
Brazil
E-mail: socorro@cbpf.br/valeria@cbpf.br
http://www.biblioteca.cbpf.br/index_2.html