Universidade Católica do Salvador
CURSO DE BACHARELADO EM INFORMÁTICA

O Protocolo SNMP

Por

Lécia de Souza Oliveira

Índice

Introdução

Devido ao crescimento das redes de computadores que têm se tornado grandes redes interconectadas (internet), fez-se necessário a criação de protocolos de gerenciamento que simplificasse o monitoramento dos equipamentos em uma rede de computadores. Além disso, tornou-se necessário haver integração e comunicação entre os equipamentos a serem gerenciados e o administrador da rede, fornecendo a este as informações necessárias para garantir que a integridade da rede seja mantida, bem como prevenir possíveis falhas.

Universidade Católica do Salvador
Disciplina: Redes de Computadores
Professor: Marco Antônio
Aluna: Lécia Oliveira

1- O que é SNMP?

O SNMP (Simple Network Management Protocol) é um protocolo de gerencia de redes cujo objetivo é disponibilizar uma forma simples e prática de realizar o controle dos equipamentos de uma rede de computadores. Definido em nível de aplicação, O SNMP utiliza os serviços do protocolo de transporte UDP (User Datagram Protocol) para enviar suas mensagens através da rede.

Nos últimos anos o SNMP tem dominado o mercado de sistemas de gerenciamento de redes devido, principalmente, a sua simplicidade de implementação, pois consome poucos recursos de redes e de processamento, o que permite a sua inclusão em equipamentos bastante simples.

O SNMP ajuda o administrador a localizar e corrigir erros ou problemas de uma rede. Através de agentes SNMP, o administrador da rede consegue visualizar estatísticas de tráfego da rede e após analisar esses dados o administrador pode atuar na rede, alterando a sua configuração.

2- Histórico do SNMP

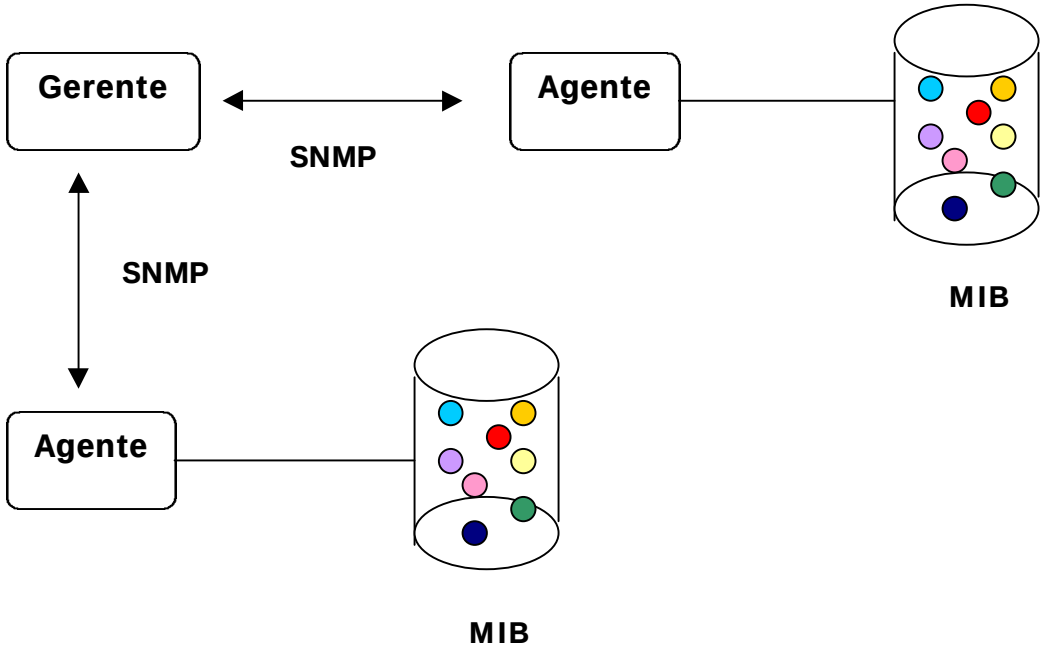
O SNMP foi desenvolvido no final dos anos 80 por um grupo da Internet Engineering Task Force (IETF) e teve sua origem em um protocolo para monitoração de gateways IP, o Simple Gateway Management Protocol (SGMP). O modelo SNMP possui uma abordagem genérica, podendo ser utilizado para gerenciar diferentes tipos de sistemas. Sua especificação está contida no RFC 1157.

- 1989: SNMP v1
- 1992: Remote Monitoring – RMON
- 1993: SNMP v2
- 1996: SNMP v2c (Community Security)
- 1996: MIB RMON v2
- 1998: SNMP v3 (User Security Model)

3- Estrutura Geral do Sistema e Funcionamento

O modelo de gerenciamento consiste em um esquema centralizado, isto é, uma estação (host) é configurada como gerente e os demais elementos da rede desempenham o papel de agentes. Um agente serve de procurador para aqueles equipamentos que não implementam o SNMP. Cada agente possui uma MIB que contém as variáveis relativas aos objetos gerenciados.O modelo genérico compreende três componentes:

- um conjunto de objetos gerenciados, correspondente a um agente e uma MIB associada;
- uma estação de gerenciamento de rede;
- um protocolo de gerenciamento de rede que é usado pela estação gerente e pelos agentes na troca de informações de gerenciamento



Legenda:

- **-** Objeto Gerenciado
MIB **-** Management Information Base
SNMP - Simple Network Management Protocol

Figura 1.0 Modelo de Gerenciamento SNMP

3.1- Protocolo de Gerenciamento

O protocolo de gerenciamento é visto sob o paradigma de **observação remota**, isto é, ele não transporta simplesmente operações de gerenciamento que devem ser executadas pelos objetos gerenciados; cada objeto é visto como uma coleção de variáveis (MIB), cujo valor pode ser lido ou alterado, possibilitando, assim, a monitoração e o controle de cada elemento da rede.

O agente, quando recebe a solicitação do gerente, encaminha as informações ou altera valores das variáveis que representam os objetos gerenciados. O agente pode, ainda, avisar o gerente da ocorrência de algum evento não-previsto, encaminhando esses avisos na forma de traps.

3.2- O Gerente

O gerente compreende um tipo de software que permite a obtenção e o envio de informações de gerenciamento junto aos mecanismos gerenciado mediante comunicação com um ou mais agentes.

As informações de gerenciamento podem ser obtidas com o uso de requisições efetuadas pelo gerente ao agente, como também, mediante envio automático disparado pelo agente a um determinado gerente. Tipicamente um gerente está presente em uma estação de gerenciamento de rede.

Devido à natureza de intensos recursos de processamento consumidos pelos componentes, a aplicação gerente é usualmente implementada em uma Workstation rodando sistema operacional multitarefa, tal como Unix ou Windows NT. Muitas vezes o dispositivo de rede (Workstation) destinado a abrigar a aplicação gerente deverá disponibilizar uma grande quantidade de memória RAM, um considerável espaço em disco, outros mecanismos de armazenamento secundário e dispositivo de backup.

3.3- O Agente

O agente utiliza as chamadas de sistema para realizar o monitoramento das informações do nodo e utiliza as chamadas de procedimento remoto (Remote Procedure Call- RPC) para o controle das informações do nodo. Caso ocorra alguma exceção no nodo gerenciado o agente fica responsável de notificar o gerente através de uma interrupção trap. Também compete ao agente efetuar a interface entre os diferentes mecanismos usados na instrumentação das funcionalidades de gerenciamento inseridos em um determinado dispositivo gerenciado.

3.4- MIB (Management Information Base)

As informações que se encontram nos nodos agentes ficam organizadas em bases de informações de gerência chamadas Management Information Base (MIB) que são definidas em uma estrutura chamada Structure of Management Information – SMI.A. SMI especifica como as informações de gerência serão agrupadas e denominadas, definindo os tipos de dados e sintaxe utilizada na MIB de forma a evitar a dependência dos detalhes de implementação dos equipamentos utilizados em rede.

A MIB pode ser definida como um conjunto gerenciável de recursos em determinado nodo. Ela é formada por uma estrutura de árvore dividida por tipos de informação e contém as características de cada recurso que possam interessar a gerência.

Na MIB, os objetos gerenciados são representados por variáveis que estão dispostas em uma estrutura hierárquica (árvore), onde as folhas definem a informação e os nós definem a estrutura. A MIB não contém os dados reais, apenas os organiza de forma adequada. Ela não guarda valores de instância, desta forma quando um gerente requisita uma instância, cabe ao agente realizar a consulta ao nodo e transmitir o valor correspondente.

A identificação e a forma de representação dos objetos contidos na MIB são definidos na linguagem abstrata Abstract Syntax Notation One – ASN.1, desenvolvida pelo órgão International Telecommunication Union (ITU) . Ela se caracteriza por representar as informações sem levar em consideração as estruturas e restrições dos equipamentos utilizados no sistema. Dessa maneira a linguagem ASN.1 tem como objetivo fornecer uma forma de representação genérica para a definição do formato das PDU trocadas pelo protocolo e dos objetos que são gerenciados. A identificação do objeto é

referida por Object Identifier - OID e uma vez que o objeto é registrado com um determinado OID ele não poderá ser eliminado nem sua definição alterada.

A MIB pode ter 3 classicações possíveis:

- **MIB Padrão:** Possui um conjunto de objetos bem definidos, conhecidos e aceitos pelos grupos e padrões Internet;
- **MIB Experimental:** Estas MIBs podem conter informações específicas sobre outros elementos da rede e gerenciamento de dispositivos que são considerados importantes. Este termo "experimental" é como se fosse um ensaio para a MIB se tornar padrão;
- **MIB Privada:** São projetadas por empresas individuais exclusivamente para seus dispositivos de rede.

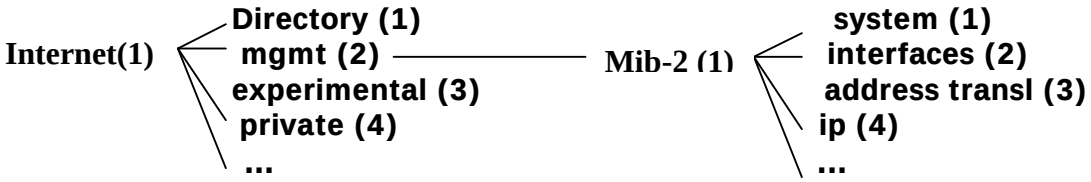


Figura 2.0 – Estrutura Hierárquica da MIB

4- Formato SNMP

No SNMP, as informações são trocadas entre uma estação de gerenciamento e um agente na forma de uma mensagem SNMP. Cada mensagem inclui o número da versão SNMP, o nome da comunidade para ser usado para esta troca e um de cinco tipos do Protocolo de Unidade de Dados (PDUs).

Campo	Descrição
Version	Versão SNMP; RFC 1157 é versão 1
Comunity	Uma PAIring de um agente SNMP com alguns conjuntos arbitrários de entidades de aplicação SNMP
Request-id	Usado para distinguir entre requests OUStanding para cada request com ID único
Error-status	Usado para indicar que uma exceção ocorreu quanto processava um request
Error-index	Quando um error-status é não 0, error-index pode prover informações adicionais indicando qual variável na lista causou a exceção
Varable-bindings	Uma lista de nomes de variáveis e valores correspondentes
Enterprise	Tipo do objeto gerador do Trap
Geric-trap	Tipo genérico do Trap
Specific-trap	Código específico do Trap
Time-stamp	Tempo ocorrido entre última (re) inicialização da rede e a geração do Trap

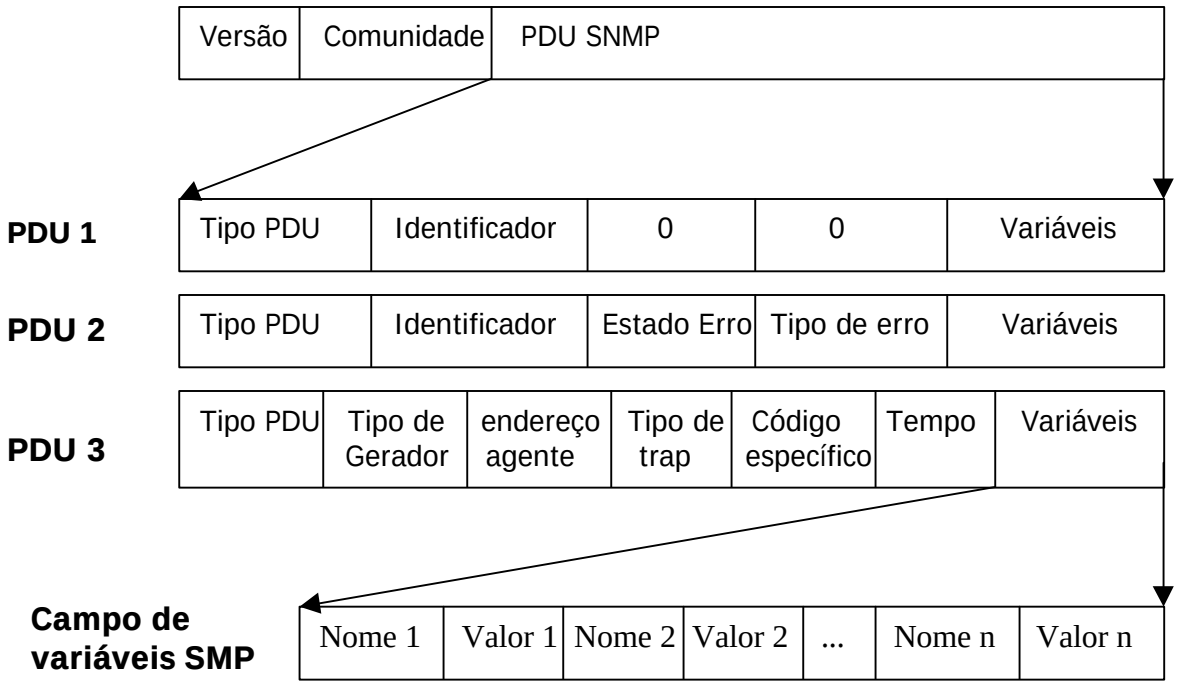


Figura 3.0 – Mensagem SNMP

PDU 1: GetRequest, GetNextRequest
PDU 2: GetResponse
PDU 3: Trap

4.1- Transmissão de uma Mensagem SNMP

Uma entidade SNMP realiza as seguintes ações para transmitir um de cinco tipos de PDU para outra entidade SNMP:

a) O PDU é construído usando a estrutura ANS.1, definida no RFC 1157
b) Este PDU é então passado para um serviço de autenticação, junto com o endereço de origem e destino e o nome da comunidade. O serviço de autenticação realiza qualquer transformação para esta troca, assim como criptografia ou a inclusão de um código de autenticação e retorna o resultado.
c) A entidade do protocolo então constrói a mensagem, consistindo de um campo versão, nome da comunidade, e o resultado do passo b.

A leitura é realizada através do transporte de variáveis informadas pelo agente tendo como resposta os respectivos valores destas variáveis. A escrita

envia uma lista de variáveis informando os novos valores a serem adotados por estas mesmas variáveis.

Dispositivos diferentes contém informações diferentes, além disso, o conjunto de variáveis (MIB) a ser adotado por um agente pode ser expandido ou alterado pelo administrador. Dessa forma é realizada uma operação transversal (get-next) implementada pelo protocolo SNMP para informar o próximo valor contido na base de informações, sendo que o gerente identifica o final da MIB através do retorno de um valor inválido. Para entender as regras da versão 1 do SNMP, as operações de gerenciamento deverão implementar processos para execução das requisições: GetRequest, SetRequest e GetNextRequest – PDUs (Protocolo de Unidade de Dados).

4.2- Recebimento de uma Mensagem SNMP

Em princípio, uma entidade SNMP realiza as seguintes ações assim que recebe uma mensagem SNMP:

- Faz uma supervisão na sintaxe básica na mensagem e descarta a mensagem se ela falhar na comunicação;
- Verifica o número da versão e descarta a mensagem se é incompatível;
- A entidade do protocolo então passa o nome do usuário, a parcela PDU da mensagem e a origem e destino do endereço de transporte para um serviço de autenticação:
    a) Se a autenticação falha, o serviço de autenticação avisa a entidade do protocolo SNMP, que descarta a mensagem;
    b) Se a autenticação tem sucesso, o serviço de autenticação retorna na forma de um objeto ANS.1.

- A entidade do protocolo faz uma supervisão na sintaxe básica do PDU. Por outro lado, usando o nome da comunidade, o plano de acesso SNMP apropriado é selecionado e o PDU é processado de acordo.

O SNMP possui um controle de limite de tempo (time-out) para o recebimento de uma mensagem que é executado em paralelo com as demais funções de gerência, permitindo que a aplicação de gerência não fique dependendo de uma mensagem de um nodo falho e detectando a falha de comunicação entre nodos.

4.3- Variáveis (Variable-bindings)

Toda operação envolve acesso a uma instância de objeto. Somente objetos folhas na árvore de instância de objetos podem ser acessados, isto é, somente objetos escalares. Entretanto, é possível em um grupo SNMP um número de operações do mesmo tipo (Get, Set, Trap) em uma mensagem simples. Assim, se uma estação de gerenciamento quer receber os valores de todos objetos escalares em um grupo particular para um agente particular, ele pode enviar uma mensagem simples requerendo todos os valores e recebendo uma resposta, listando os valores. Para implementar trocas de múltiplos objetos, todos os objetos da PDU SNMP incluem um campo de ligação de variáveis. Estes campos consistem de uma seqüência de referências a instâncias de objetos, junto com o valor destes objetos.

5- Operações do protocolo SNMP

As operações de gerenciamento são componentes da Aplicação Gerente que controlam e monitoram os agentes pertencentes à comunidade de um determinado domínio de gerenciamento. As operações de gerenciamento podem ler e escrever em variáveis da MIB da cada aplicação agente para gerenciar o dispositivo de rede. As operações de gerenciamento podem também armazenar informações de gerenciamento recuperadas junto as aplicações agentes em uma MIB própria e/ou em um Banco de Dados. O gerente SNMP realiza basicamente duas funções durante a gerência:

- leitura de valores (get): monitoramento das características do nodo
- escrita de valores (set): controle das características do nodo

A troca de mensagens no SNMP ocorre através das PDUs (Protocol Data Units) utilizadas pelo protocolo para a troca de informações entre os diversos elementos da gerência e a estrutura utilizada para o transporte de variáveis.

Os tipos de PDUs são:

- Get (recuperar o valor da variável)
- Set (alterar valor da variável)
- Get-next (recuperar o valor da próxima variável)
- Trap (notificação)

Para realizar as operações o protocolo SNMP utiliza cinco tipos de PDU:

- Get Request
- GetNextRequest
- SetRequest
- GetResponseTrap

O GetRequest PDU é emitido por uma entidade SNMP e é de interesse de uma estação de gerenciamento de rede de uma aplicação. A entidade de transmissão inclue os seguintes campos na PDU:

Tipo PDU: indicando que este é um GetRequest PDU;

Request-id: a entidade de transmissão determina números de tal maneira que cada request seja único para cada agente. O request-id habilita a aplicação SNMP para resposta de entrada correlativa com request (pedido).

Variable-bindings: Uma lista de instâncias de objetos cujos valores são requeridos

A entidade de recebimento SNMP responde ao GetRequest PDU com um GetResponse PDU contendo o mesmo Request-id. A operação GetRequest é atômica: todos os outros valores são recuperados ou nenhum é.

O GetNextRequest PDU é quase idêntico para todos GetRequest PDU. Ele tem o mesmo módulo de troca e o mesmo formato que o GetRequest PDU. A única diferença é que no GetRequest PDU, cada variável na lista de ligação de variáveis referencia à uma instância de objetos de quem o valor é retornado. No GetResponse PDU, para cada variável, a resposta retorna o valor da instância do objeto.

O SetRequest PDU é emitido por uma entidade SNMP sob interesse de uma aplicação da estação de gerenciamento. Tem o mesmo padrão de troca PDU e o mesmo formato que o GetRequest PDU. A diferença é que o SetRequest é usado para gravar um valor de objeto, mais propriamente para lê-lo. Assim, a lista de ligação de variáveis no SetRequest PDU inclui ambos identificadores da instância de objetos e um valor para ser definido para cada instância da lista.

A entidade SNMP de recebimento responde a um SetRequest PDU com um GetResponse PDU contendo o mesmo request-id. Se a entidade de resposta é capaz de estabelecer valores para todas as variáveis listadas na entrada da lista de variáveis, então o GetResponse PDU inclui o campo variáveis de ligação com um valor que é fornecido para cada variável.

A Trap (notificação) PDU é emitida por uma entidade SNMP como representante de uma aplicação do gerente. Ela é usada para prover a estação de gerenciamento com uma notificação assíncrona de alguns eventos

significantes. Seu formato é completamente diferente dos outors PDUs SNMP. Os campos são:

- Tipo da PDU: indica que este é um GetRequest PDU;
- Enterprise: identifica o subsistema de gerenciamento de rede que gerou a trap. O valor é pego do SysObjectID no grupo sistema;
- Agente addr: contém o endereço IP do objeto gerador da trap;
- Trap genérico: contém um dos tipos pré-definidos;
- Trap específico: contém um código que indica mais especificamente a origem da trap;
- Time-stamp: contém o tempo entre a última reinicialização da entidade da rede que emitiu o trap e geração do trap;
- Variable-bindings: contém informações adicionais a trap

6- Restrições das Operações

- Permitem somente inspeção e/ou alteração de variáveis
- A estrutura da MIB não pode ser alterada pelas operações
- Somente podem ser acessados valores escalares em cada operação

7- Segurança no Protocolo SNMP

O protocolo SNMP pode realizar operações de reconfiguração na rede alterando características de equipamentos ou até desligando máquinas, sendo que não existe qualquer mecanismo de segurança aplicado ao conteúdo das mensagens. O controle é feito através da verificação do conteúdo de um campo especial no pacote do SNMP denominada comunidade. A comunidade é definida como sendo o relacionamento entre duas entidades do SNMP. Ela é definida como um conjunto de bytes formando caracteres ASCII que serão utilizados para efetuar este relacionamento. Dessa forma, quando é realizada a comunicação entre duas entidades do SNMP, a entidade destinatária da mensagem realiza a verificação do conteúdo da comunidade para averiguar se esta informação é proveniente do remetente indicado.

SNMP Agent: Community Names

- **AIX: /etc/snmpd.conf**
  - **community name><address><mask><permissions><view>**
  - community public 146.84.47.160 255.255.255.255.0 read only 1.17.2
  - community private 146.84.47.160 255.255.255.255.255 readwrite
  - **view 1.17.2 system enterprises view**

Figura 4.0- Community

Através da comunidade é possível que o agente realize uma verificação da integridade do agente realizando autenticação e políticas de acesso (agente controla que diferentes gerentes podem obter diferentes variáveis da MIB) através deste campo. O mais importante no entendimento de comunidade, é que sem o conhecimento prévio da comunidade de um determinado equipamento gerenciável, será impossível a qualquer aplicação de gerência acessar as informações da MIB. Outra consideração importante é que um equipamento pode ter mais de uma comunidade configurada, como uma com direitos de leitura, escrita e trap. Portanto, um mesmo equipamento poderá contar com três strings de comunidade diferentes. Isto tem o objetivo de se aumentar a segurança no acesso aos equipamentos.

No exemplo, o arquivo **snmpd.conf** é onde se pode configurar o acesso que se quer fornecer às estações gerente quando realizam a requisição SNMP. Pode-se limitar o acesso com read-only e read-write.

Com esse tipo de autenticação, o acesso a MIB se torna pouco seguro, devido principalmente a:

- Identificação da origem: a comunidade é transmitida sem qualquer proteção
- Integridade da mensagem: ao ser interceptada a mensagem não garante qualquer proteção referente ao conteúdo
- Tempo-limite: período de tempo que a mensagem pode ficar presa por algum serviço
- Privacidade: qualquer serviço pode monitorar uma comunicação entre entidades SNMP
- Autorização: não há controle de autorização de acesso aos dados da MIB

8- Limitações de SNMP

- Falta de segurança
  - Esquema de autenticação trivial
  - Limitações no uso do método SET
- Ineficiência
  - Esquema de eventos limitado e fixo
  - Operação baseada em pooling
  - Comandos transportam poucos dados
- Falta de Funções Específicas
  - MIB com estrutura fixa
  - Falta de comandos de controle
  - Falta de comunicação entre gerenciadores
- Não Confiável
  - Baseado em UDP/IP
  - Trap sem reconhecimento

9- SNMPv2 e SNMPv3

Visando obter melhorias com relação aos aspectos de segurança foram desenvolvidas novas versões do SNMP. A segunda versão, o SNMPv2 contém mecanismos adicionais para resolver os problemas relativos á segurança como: privacidade de dados, autenticação e controle de acesso.

A terceira versão, o SNMPv3 tem como objetivo principal alcançar a segurança, sem esquecer-se da simplicidade do protocolo, através de novas funcionalidades como:

- Autenticação de privacidade
- Autorização e controle de acesso
- Nomes de entidades
- Pessoas e políticas
- Usernames e gerência de chaves
- Destinos de notificações
- Relacionamentos proxy
- Configuração remota

Conclusão

O protocolo SNMP é um modelo simples de gerenciamento de rede de fácil implementação, pois gera pouco tráfego de informações. Além disso, seu design simples facilita ao usuário programar as variáveis que ele gostaria de monitorar. Porém, por ser tão simples, a informação que o SNMP manipula através das variáveis não é nem detalhada nem tão organizada o suficiente para as necessidades das redes a partir de 1990 e, além disso, não garante muita segurança a rede.

Com o surgimento das novas versões o SNMPv2 e SNMPv3, foram realizadas alterações na especificação do protocolo, tais como a forma de representação das variáveis, e inclusão de novos tipos de PDUs e o retorno dos tipos de erros, que acabaram por tirar a simplicidade do protocolo .

Entretanto, o SNMP é amplamente usado sendo que a maioria dos fabricantes de hardware para internet (como bridges e roteadores) projetam seus produtos para suportar o SNMP.

Bibliografia

Sites:

http://pucmgmt.metropoa.tche.br/
http://www.ieee.org
http://homer.span.ch/~spaw2724/SNMP/Portugues/
http://ppgiapucpr.br/~mazieiro/

Livro:

Embratel, Empresa Brasileira de Telecomunicações- editora MARKRON Books- 2º edição Revisada e Ampliada