TRABALHO SOBRE SNMP

UNIVERSIDADE CATÓLICA DO SALVADOR
TELEPROCESSAMENTO E REDES
PROF: MARCO ANTÔNIO CÂMARA
ALUNO: ANDREI GALVÃO DO NASCIMENTO

Introdução ao SNMP

No final dos anos 70 as redes de computadores cresceram de simples redes separadas que não eram conectadas entre elas para grandes redes interconectadas. Estas grandes redes interconectadas chamou-se de internet e começou a crescer de modo a ficar cada vez mais difícil de gerenciá-la tornando-se necessário a criação de um protocolo de gerenciamento. O protocolo de gerência de redes Simple Network Management Protocol (SNMP) foi desenvolvido no final da década de 80 por um grupo da Internet Engineering Task Force (IETF) - Internet Architecture Board (IAB) com o objetivo de disponibilizar uma forma simples e prática de realizar o controle dos equipamentos em uma rede de computadores.Este protocolo tinha como premissa ser implementado facilmente nos produtos existentes e flexível para englobar produtos e especificações futuras. O SNMP é um protocolo de gerência definido à nível de aplicação, utilizando os serviços do protocolo de transporte UDP (User Datagram Protocol) para enviar suas mensagens através da rede. Sua especificação está contida no RFC 1157.

SNMP - Modelo de Gerenciamento ou Protocolo?

O Gerenciamento Internet, também chamado de abordagem SNMP ou modelo de gerenciamento SNMP, é padronizado pela IETF, uma organização aberta que define os padrões para a Internet. O modelo SNMP possui uma abordagem genérica, podendo ser utilizado para gerenciar diferentes tipos de sistemas. Com a popularização do protocolo SNMP, convencionou-se chamar de "Gerenciamento SNMP" o gerenciamento baseado no padrão de "gerência Internet". Então, o SNMP é o nome do protocolo no qual as informações trafegam entre a MIB (agente) e a Aplicação de Gerência e o nome deste modelo de gerência.

Funcionamento do SNMP

O SNMP possui duas classes de dispositivos: - Agente: é um processo executado no nodo gerenciado, responsável pela manutenção das informações de gerência deste nodo. Cada nodo gerenciado pelo SNMP deve possuir um agente e uma base de informações de gerência correspondendo a todas as características encontradas na base de informações MIB - Gerente: refere-se a uma estação servidora, executando o protocolo de gerência de redes e uma ou mais aplicações de gerência.Para realizar a troca de informações entre os componentes da rede a aplicação da gerência utiliza o protocolo SNMP Cada objeto gerenciado é visto como uma coleção de variáveis (MIB) cujo valor pode ser lido ou alterado. O gerente envia comandos aos agentes, solicitando uma leitura no valor das variáveis dos objetos gerenciados (get e response), ou modificando seu valor (put). Na troca de informações entre o gerente e o agente, sao aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede. A troca de mensagens entre o gerente e o agente é definida pelo protocolo SNMP. O SNMP define o formato e a ordem que deve ser seguida no intercambio de informações de gerenciamento.

Arquitetura do Modelo de Gerenciamento SNMP

O funcionamento do SNMP baseia-se na troca de operações que permitem que o gerente solicite que o agente lhe informe, ou modifique, o valor de uma variável de um objeto na MIB. O SNMP define também uma operação (trap), que permite que um agente informe ao gerente a ocorrência de um evento especifico, como, por exemplo, a queda de um link em um roteador

Agentes SNMP

Um nodo gerenciável é caracterizado como algum dispositivo enquadrável entre as seguintes categorias:

- um nodo que possui aplicações: o estação de trabalho, mainframe , terminal ou impressora
- um sistema de roteamento
- um dispositivo tal como bridge, repetidor hub ou analisador

Cada nodo gerenciável é formado:

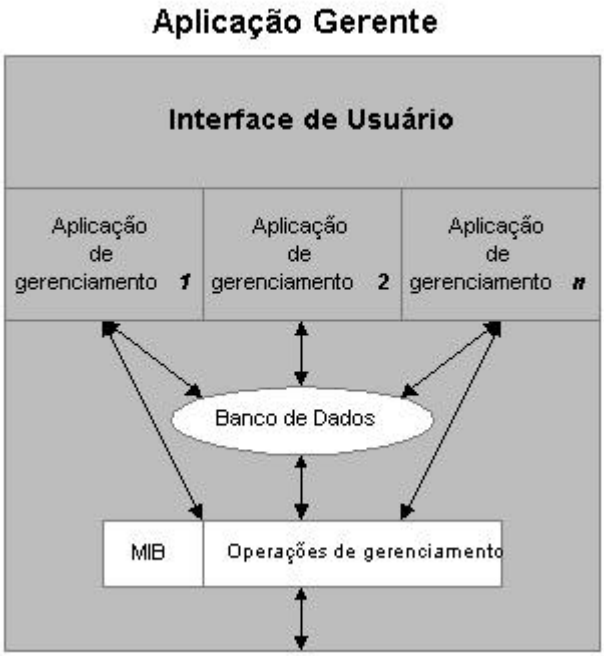
- pelo protocolo de comunicação de gerência: responsável por estabelecer a comunicação entre o agente e o gerente permitindo o monitoramento e controle do nodo gerenciado
- uma parte intermediária para instrumentação: permite que as estruturas de dados MIB usadas na representação da parte útil possam ser manipuladas por requisições do protocolo de gerência - e a parte útil do nodo.
- Responsável por realizar as funções para o qual o nodo foi construído sem levar em consideração a gerência

Dessa forma cada nodo gerenciável é visto como um conjunto de variáveis que representam informações referentes ao seu estado atual. Estas informações ficam disponíveis ao gerente através de consultas e podem ser alteradas por ele. O sistema de gerência fica habilitado a identificar na estrutura da rede os problemas relacionados aos nodos e modifica-los de acordo com a necessidade. 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 inseridas em um determinado dispositivo gerenciado.

Gerentes SNMP

O gerente compreende um tipo de software que permite a obtenção e o envio de informações de gerenciamento junto aos mecanismos gerenciados mediante comunicação com um ou mais agentes. As decisões na ocorrência de problemas, o monitoramento e as funções tipo relatórios fica a cargo do gerente enquanto ao agente fica a responsabilidade com relação as funções para o envio e alteração de informações e a notificação da ocorrência de alguma exceção ao gerente.Dessa forma, o gerente é responsável pela implementação da política que será adotada na gerência. O gerente está acessível à pessoa ou entidade responsável pela administração da rede cabendo à aplicação-gerente informar as condições da rede para esta pessoa ou entidade. 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.



Simple Network Management Protocol

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 de cada Agente para gerenciar o dispositivo de rede. As operações de gerenciamento podem, também, armazenar informações de gerenciamento recuperadas junto aos Agentes em uma MIB própria e/ou em um Banco de Dados próprio. É através das mensagens do SNMP que são enviadas e recebidas as informações de interrupção, controle e monitoramento entre os agentes e gerentes. 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

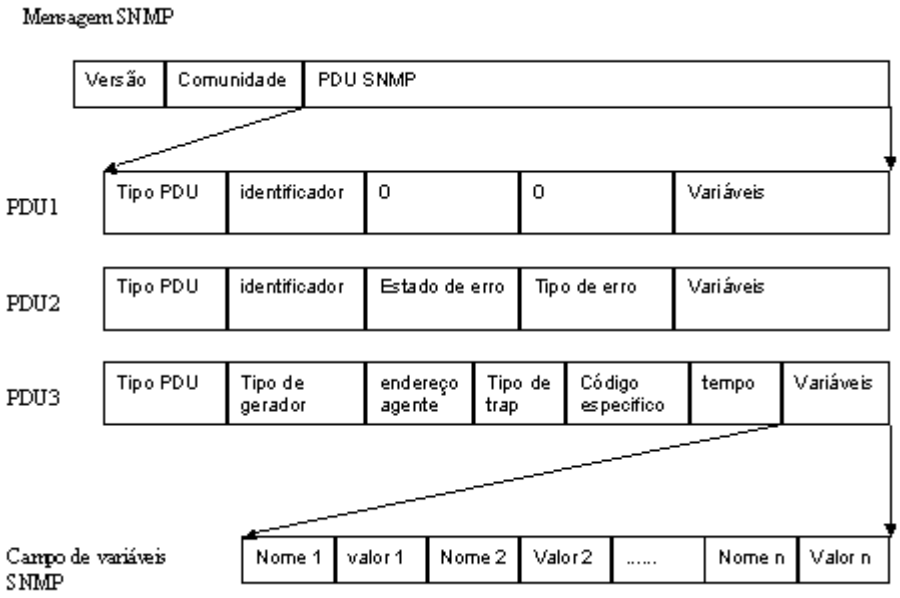
O protocolo SNMP possui quatro operações básicas:

- 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:

- GetRequest
- GetNextRequest
- SetRequest
- GetResponse
- Trap

Segue abaixo os tipos de PDUs.



- PDU1: GetRequest, GetNextRequest
- PDU2: GetResponse
- PDU3: Trap

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 adotadas 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 atender as regras da versão 1 do SNMP, as operações de gerenciamento deverão implementar processos para execução das requisições: GetRequest, SetRequest e GetNextRequest - PDUs (Protocol Data Units).

Para atender as regras da versão 2 do SNMP, as operações de gerenciamento deverão implementar processos adicionais para a requisição GetBulk-PDU, para o tratamento das alterações da mensagem Response-PDU, de um novo formato de Trap (termo inglês que significa "notificações; mensagem de alerta eventual" no vocabulário técnico do SNMP), e para a possibilidade de mensagens do tipo InformRequest-PDU. O envio de uma mensagem de interrupção (trap) é a forma de comunicação que o agente utiliza para obter a atenção do gerente e informa-lo sobre a ocorrência de uma situação excepcional no nodo gerenciado. Não existe garantia de chegada de uma trap nem resposta para a mesma.Ao receber uma trap o gerente deve decidir como deverá processa-la ficando responsável por acionar as iterações necessárias para o tratamento do nodo gerenciado, identificando a natureza e extensão do problema.

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. A comunicação com a MIB, visando reconhecer o próprio conjunto de objetos gerenciados, que podem ser controlados e monitorados, e uma interface para as funções de envio e recebimento de mensagens SNMP via camada de transporte (protocolo UDP e outros utilizados), são procedimentos que deverão ser incluídos nas operações de gerenciamento.

As operações de gerenciamento também deverão fornecer os serviços necessários para qualquer requisição de aplicações de gerenciamento que podem compor um Sistema de Gerenciamento de Rede (chamados de Plataformas de Gerenciamento, quando são utilizados produtos proprietários). A Application Programing Interface-API poderá ser proprietária, implementada por um fabricante de operações de gerenciamento, ou aberta, como, por exemplo, a que foi desenvolvida para Aplicações Gerente baseadas em ambiente Windows, denominada WinSNMP, ou ainda as API's, desenvolvida para plataformas Unix. As operações de gerenciamento podem ser encaradas como mecanismos de comunicação SNMP, utilizados na troca de mensagens entre Aplicações Gerente e Agente. Esses mecanismos estão disponíveis em uma implementação do SNMP, denominada UCD-SNMP, e portada para o sistema operacional Linux. As operações de gerenciamento estão implementadas no pacote de software desenvolvido na University California Davis-UCD, na forma de utilitários (operações de gerenciamento) que processam as requisições Get, GetNext, Walk, Set e Trap.

Informações de Gerência

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 na rede.. A MIB pode ser definida como um conjunto gerenciável de recursos em um 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.

A MIB não guarda valores de instância, dessa forma quando um gerente requisita uma instância cabe ao agente realizar a consulta ao nodo e transmitir o valor correspondente. Os objetos contidos na MIB são abstrações de recursos existentes no sistema. A identificação e a forma de representação dos objetos contidos na MIB são definidos na linguagem abstrata Abstract Syntax Notation One - ASN.1. que 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 de um 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.

Transporte

O protocolo de transporte não orientado à conexão User Datagram Protocol (UDP) fornece um meio de transporte que ocupe o mínimo de recursos da rede e possibilitando o controle necessário sobre a transmissão, tamanho e conteúdo dos pacotes.O protocolo não orientado à conexão tem qualidades tais como sua implementação ser realizada de maneira simples e permitir transferir à aplicação a responsabilidade de implementar a política que será adotada para confiabilidade do sistema. Além disso, os serviços não orientados fazem o estabelecimento da comunicação de maneira veloz e utilizam menos recursos do nodo a ser gerenciado. UDP prove protocolos de portas usadas para distinguir múltiplos programas executando em uma simples máquina. Dessa forma, UDP distingue múltiplos processos em uma máquina permitindo os computadores de origem e os receptores a inserirem 16 bits, chamado de protocol port numbers, em cada mensagem UDP. O número das portas identificam a fonte e o destino. UDP não usa técnicas para ter certeza que a mensagem chegou ao seu destino, então as mensagens UDP podem ser perdidas, duplicadas ou chegar fora de ordem.

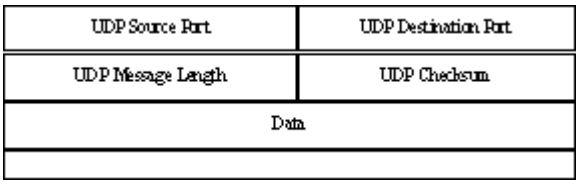
Os protocolos de transporte e de rede fornecem algumas facilidades de importância vital ao tráfego na rede:

- roteamento: controla a rota que será adotada pelos pacotes, utilizando rotas alternativas
- independência: permitem que diferentes equipamentos troquem informações
- controle de erros: controlam a integridade dos dados transportados
- multiplexação/demultiplexação: permite o melhor aproveitamento do meio de transporte
- controle de fragmentação: permite transporte de mensagens em diferentes tamanhos de pacotes

Formato das mensagens UDP

Cada mensagem UDP é chamada de user datagram e consiste em duas partes:

- cabeçalho UDP
- área de dados UDP



Source Port e Destination port -contém os 16 bits de identificação das portas de fonte e destino da mensagem

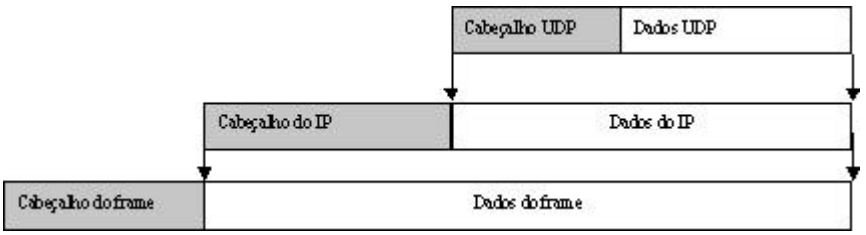
- Length - contém o tamanho da mensagem UDP

- UDP checksum - provê a única forma de garantia que os dados chegaram intactos e podem ser usados

O algoritmo checksum é o mesmo usado no IP, ou seja, ele divide os dados em quantidades de 16 bits e computa o complemento de um do somatório do complemento de um. Quando o algoritmo chega a um resultado igual a zero quer dizer que a mensagem está intacta. Para computar o algoritmo checksum o UDP usa um pseudo-cabeçalho para verificar se o datagrama UDP chegou ao seu destino correto.

Encapsulação UDP

As mensagens UDP são encapsuladas em um datagrama IP para a transmissão pela internet. O datagrama é encapsulado em um frame cada vez que viaja em uma rede simples , como mostra a figura abaixo:

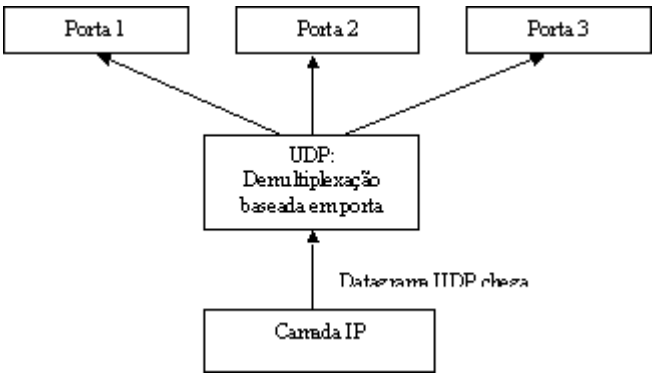


O Datagrama UDP é encapsulado em um datagrama Ip para transmissão pela internet que por sua vez é encapsulado em um frame toda vez que passar por uma rede simples.

Multiplexação e demultiplexação UDP

O software UDP aceita os datagramas UDP de vários programas de aplicação e passa-os para o IP para a transmissão dos mesmos e aceita os datagramas UDP que chegam do IP e passam para o programa de aplicação apropriado. Dessa forma cada programa de aplicação deve negociar com o sistema operacional para obter uma porta e associar-se a ela antes de mandar um datagrama UDP. Dessa forma a multiplexação e demultiplexação entre software UDP e programas de aplicação ocorre pelo mecanismo de portas.

Exemplo de demultiplexação:



UDP utiliza o número da porta de destino para selecionar a porta de destino apropriada para os datagramas que chegam.

Interação no SNMP

Transmitindo uma mensagem do SNMP

Tanto o gerente (no caso do get, get-next e set) como o agente (no caso das interrupções trap) realizam as seguintes operações para a transmissão de PDU's entre entidades:

- a PDU é construída utilizando a estrutura ASN.1.
- a PDU passa por um serviço de autenticação (endereços de origem, endereço de destino e nome da comunidade)
- a mensagem é construída sendo composta por um campo de versão, nome da comunidade e o resultado obtido no segundo passo
- o novo objeto ASN.1. é transmitido ao serviço de transporte

Recebendo a mensagem SNMP

Tanto o agente (no caso de set, get e get-next) quanto o gerente (no caso das interrupções) realizam as seguintes tarefas ao receberem uma mensagem:

- verificação da sintaxe da mensagem
- verificação do número de versão
- serviço de autenticação verifica o nome do usuário, a parte de PDU da mensagem e os endereços de origem e destino
- retorna uma PDU correspondente no caso de sucesso

Interação no SNMP

Transmitindo uma mensagem do SNMP

Tanto o gerente (no caso do get, get-next e set) como o agente (no caso das interrupções trap) realizam as seguintes operações para a transmissão de PDU's entre entidades:

- a PDU é construída utilizando a estrutura ASN.1.
- a PDU passa por um serviço de autenticação (endereços de origem, endereço

de destino e nome da comunidade)

- a mensagem é construída sendo composta por um campo de versão, nome da comunidade e o resultado obtido no segundo passo
- o novo objeto ASN.1. é transmitido ao serviço de transporte

Recebendo a mensagem SNMP

Tanto o agente (no caso de set, get e get-next) quanto o gerente (no caso das interrupções) realizam as seguintes tarefas ao receberem uma mensagem:

- verificação da sintaxe da mensagem
- verificação do número de versão
- serviço de autenticação verifica o nome do usuário, a parte de PDU da mensagem e os endereços de origem e destino
- retorna uma PDU correspondente no caso de sucesso

Segurança no protocolo SNMP

O protocolo de gerência SNMP pode realizar operações de reconfiguração na rede alterando características de equipamentos ou até desligando máquinas, sendo 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 denominado comunidade. A comunidade é definida como sendo o relacionamento entre duas entidades do SNMP.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.

Através da comunidade é possível que o agente realize uma verificação da integridade do gerente 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 somente de leitura, outra com direitos de leitura e escrita e finalmente outra 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.

Segue abaixo algumas características da MIB:

- identificação da origem: a comunidade é transmitida sem qualquer proteção sendo que a mensagem SNMP pode ser interceptada por algum intruso que poderá copiar o mesmo nome de comunidade e entrar na MIB
- 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

Management Informaton Base

Base de Informações MIB

MIB é a estrutura de dados, organizada em árvore, que contém as informações necessárias à gerência de um determinado nodo na rede.Cada nodo da rede que possui um agente mantém uma MIB própria que indica os recursos de gerência daquele nodo.A MIB é descrita através de uma representação abstrata de sua sintaxe chamada de Abstract Syntax Notation One - ASN.1. As regras de construção da estrutura da MIB são descritas através do Structure os Management Information - SMI.Os objetos gerenciáveis são abstrações dos recursos encontrados na rede. Dentro da MIB os objetos gerenciáveis são chamados de variáveis, sendo que para cada uma destas variáveis é atribuído um número, número este denominado Object id, ou Identificador de Objeto.

Resumindo, a MIB nada mais é do que um conjunto de variáveis. Algumas variáveis existem apenas a título de armazenarem informações de gerenciamento (como uma variável que guarda o número de bytes recebidos por uma porta do equipamento), outras servem para configuração do equipamento (como variáveis que armazenam o nome, localização e número IP do equipamento) e outras guardam informações básicas do equipamento (como variáveis que guardam informações sobre o modelo e características do equipamento). Finalmente, estas variáveis estão aptas a serem lidas ou, quando possível, modificadas pelo software de gerenciamento através da sua interface de software (o agente). Apenas para facilitar o entendimento, o agente é um elemento "transparente" no processo de gerenciamento. Simplesmente solicitamos informações a uma variável e ela responde. Não percebemos a existência do agente nesta transação.

A MIB pode ter 3 classificações 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.

Estrutura da MIB

Todos os objetos de uma MIB estão organizados de maneira lógica em uma estrutura de árvores onde suas folhas representam os objetos que identificam um recurso, atividade ou outra informação referente à gerência. Cada objeto da MIB possui um identificador único que contém o nome e a localização do objeto. O nó raiz da árvore MIB não tem nome ou número, mas tem três subárvores como mostra a figura:

SMI

A estrutura de informações de gerência SMI é um conjunto de documentos que definem:

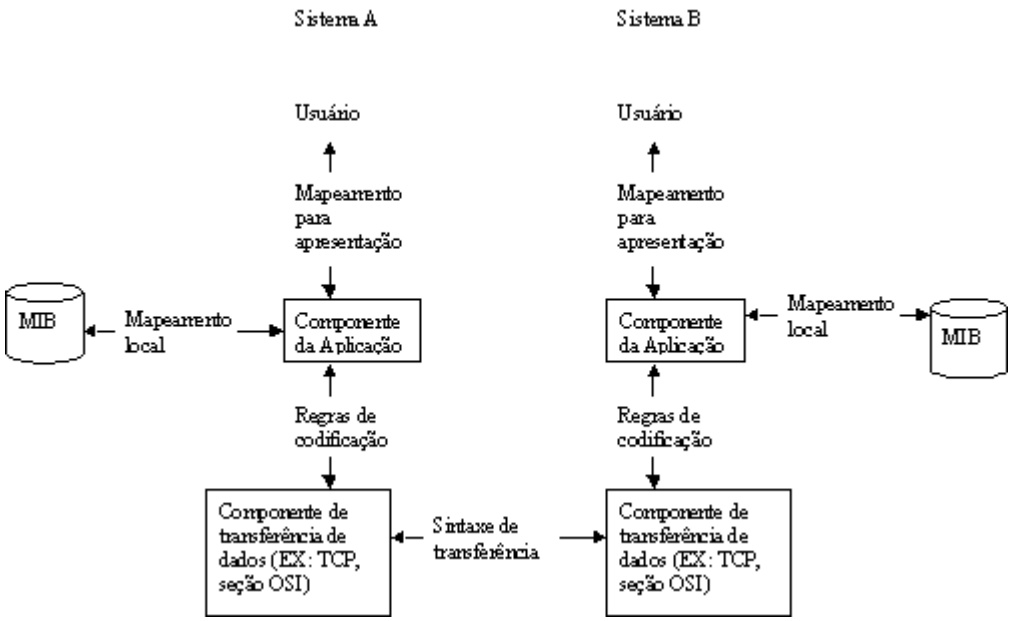
- forma de identificação e agrupamento das informações
- sintaxes permitidas
- tipos de dados permitidos

Cada classe de informação de gerência é chamado de objeto ou tipo de objeto e as instâncias deste objeto são chamadas de variáveis do SNMP. O SNMP representa as informações de gerência como variáveis, sendo as operações do SNMP responsáveis por requisitar ou modificar os valores destas variáveis. Um objeto pode possuir apenas uma instância (objeto escalar) ou múltiplas instâncias (objeto colunar).

1. ASN.

ASN.1. é uma linguagem formal desenvolvida pelos órgãos international Telecommunication Union ITU e pelo International Organization for Standardization ISO para a representação e identificação dos objetos na base de informações de gerência visando realizar transferência de informações entre aplicaçòes de diferentes sistemas. É uma forma de descrição abstrata dos dados com o objetivo de não se levar em consideração a estrutura e restrições do equipamento no qual está sendo implementada. Para a troca de informações é utilizado o conjunto de regras Basic Encoding Rules (BER). Dessa forma a sintaxe descrita em ASN.1. representa as informações do sistema e a sintaxe de transferência BER realiza a codificação destas informações em conjunto de bytes para realizar a comunicação entre os sistemas. Os dados representados em ASN.1. compõem a MIB e devem ser armazenados dentro da aplicação.

Segue abaixo o uso das sintaxes abstrata e de transferência:



Sintaxe da linguagem ASN.1. A forma básica para a construção do conjunto de descrições das informações em ASN.1. é realizada através de um módulo. Neste módulo são especificados:

- nome do módulo
- indicação de quais definições podem ser importadas por outros módulos
- referência de módulos que devem ser importados de outro local
- declarações contendo definições ASN.1.

Exemplo:

<<nome_módulo>> DEFINITIONS :: = BEGIN
<<exportados>>
<<módulos_importados>>
<<declarações>> --comentários
END

Os tipos de objetos definidos em ASN.1.:

- tipos (types) definem novas estruturas de dados
- valores (values): são variáveis (instâncias) de um tipo
- macros: utilizado para alterar a gramática da linguagem ASN.1.

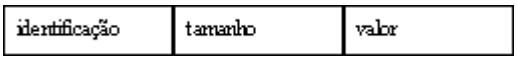
Sintaxe de transferência BER

A sintaxe de transferência BER é o método para a codificação dos valores de cada tipo ASN.1. em um conjunto de bytes. Segue abaixo como os valores ASN.1. podem ser codificados através da BER em um conjunto composto por:

- tag (identificação) : indica o tipo de dado, classe deste tipo e se o tipo é composto ou primitivo

- lenght(tamanho): tamanho ocupado pelo valo

- value(valor): valor que deve ser transportado



SNMPv2 e SNMPv3

Versões SNMPv2 e SNMPv3

Visando a melhoria com relação aos aspectos de segurança forma desenvolvidas novas versões do SNMP.O SNMPv1 permite que qualquer intruso tenha acesso a informações pois sua única proteção a verificação dos dados da comunidade contidos nas mensagens. A segunda versão, o SNMPv2 contém mecanismos adicionais para resolver os problemas relativos á segurança:

- privacidade de dados: impede que intrusos tenham acesso as informações que trafegam na rede
- autenticação: intrusos não conseguem enviar dados falsos (como desligar uma máquina) através da rede
- controle de acesso: prevê acesso restrito a alguns usuários para certas variáveis

Com as 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, acabaram por tirar a simplicidade do protocolo e por conseqüência não conseguiu substituir a primeira versão. A terceira versão do SNMP, o SNMPv3 surgiu a partir de dois subgupos (SNMPv2u e o SNMPv2*) que se formaram com a desativação do trabalho de desenvolvimento do SNMPv2.

O SNMPv3 que tem como objetivo principal alcançar a segurança, sem esquecer-se da simplicidade do protocolo, através de novas funcionalidades:

- autenticação e privacidade
- autorização e controle de acesso
- nomes de entidades
- pessoas e políticas
- usernames e gerência de chaves
- destinos de notificações
- relacionamentos proxy
- configuração remota

Remote Network Monitoring (RMON
Conceitos Básicos

Com a MIB-II o gerenciamento de redes pode obter informações locais de dispositivos individuais.Cada dispositivo contém um agente SNMP.Um gerente SNMP pode aprender sobre a quantidade de tráfego de entrada e saída sobre cada dispositivo mas tem dificuldades sobre o tráfego da LAN como um conjunto. Dessa forma os dispositivos que são empregados para o estudo do tráfego da rede como um conjunto são chamados de network monitors (monitores de redes). Estes monitores analisam cada pacote da rede e fornecem sumários da informação contendo estatísticas de erros, número de colisões, estatísticas de performance, número de pacotes transmitidos por segundo e o tamanho dos pacotes distribuídos.

O monitor pode manter pacotes ou pacotes parciais para analisar mais tarde.Filtros podem ser usado para limitar o número de pacotes contados ou capturados baseados no tipo de pacote ou outras características dos pacotes.Para os propósitos do gerenciamento de rede em um meio internet deve-se ter um monitor para cada subrede, chamados de remote monitors que devem se comunicar com uma estação de gerenciamento central da rede

Objetivos RMON

RMON provê um caminho efetivo e eficiente para monitorar sub-redes internet reduzindo a carga dos outros agentes e estações de gerenciamento. Segue abaixo alguns dos objetivos do RMON:

- Operação Off-line: o monitor pode pode acumular estatísticas que serão enviadas ao gerente mais tarde.Dessa forma o gerente pode aumentar o tempo de polling (gerente fica constantemente verificando status dos monitores). O monitor também pode notificar a estação de gerenciamento quando ocorrer eventos excepcionais
- Problema de detecção e reportagem: O monitor pode reconhecer algumas condições de erro e outras condições tipo congestionamento excessivo. O monitor pode ser configurado para verificar constantemente estas condições e notificar a estação de gerenciamento quando alguma delas ocorrer.
- O monitor pode analisar o tráfego da subrede para determinar quais hosts geram mais tráfego ou erros na subrede. Este tipo de informação não é acessível para a estação central de gerenciamento de rede pois ela não é diretamente conectada na subrede.
- Múltiplos gerentes: as razões para múltiplos monitores incluem o fato de aumentar a capacidade de realizar diferentes funções e fornecer capacidade de gerenciamento para diferentes unidades de uma organização

Controle do monitores remotos

Um monitor remoto pode ser implementado tanto como um dispositivo dedicado como uma função disponível a um sistema cujos recursos de processamento e memória são especificamente dedicados a função de monitoramento. Com estes recursos dedicados o monitor remoto pode ser capaz de executar tarefas mais complexas e uma maior escala de funções do que um agente pode suportar

Comparações entre os protocolos SNMP e CIMP

SNMP

O protocolo de gerência de redes Simple Network Management Protocol (SNMP) foi desenvolvido no final da década de 80 por um grupo da Internet Engineering Task Force (IETF) - Internet Architecture Board (IAB). O SNMP foi projetado para resolver os problemas de comunicação entre diferentes tipos de redes de forma simples. O protocolo SNMP possui quatro operações básicas:

- 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:

- GetRequest
- GetNextRequest
- SetRequest
- GetResponse
- Trap

Vantagens do SNMP

A maior vantagem do SNMP é seu design simples e fácil implementação em grandes redes e causa pouco stress na rede.Além disso seu design simples facilita ao usuário programar as variáveis que ele gostaria de monitorar, pois cada variável consistem as seguintes informações:

- O título da variável
- O tipo de dados da variável
- Permissões da variável (read-only e read-write)
- O valor da variável

O protocolo SNMP é amplamente usado sendo que a maioria dos vendedores de hardwares para internet (como bridges e roteadores) projetam seus produtos para suportar o SNMP. Devido ao seu design simples , tornou-se fácil para este protocolo ser atualizado para expandir e atender as necessidades dos usuários no futuro

Desvantagens do SNMP

Uma deficiência do SNMP é que ele não garante muita segurança à rede permitindo que intrusos entrem na rede,interceptem uma mensagem e leiam seu conteúdo, ou até mesmo desligar alguns equipamentos Para resolver este

problema a segunda versão do protocolo SNMPv2 adicionou alguns mecanismos para combater os maiores problemas de segurança:

- privacidade dos dados
- autenticação
- controle de acesso

O maior problema do protocolo SNMP é que ele foi considerado para ser tão simples que a informação que ele manipula através das variáveis não é nem tão detalhada como organizada suficiente para as necessidades das redes a partir de 1990.

CMIP

O grupo da Internet Engineering Task Force (IETF) , o Internet Management Working Group projetou o protocolo de gerência de redes adaptado ao modelo OSI, chamado de Common Management Information Protocol (CMIP). O CMIP possui duas formas básicas de implementação:

- CMIP: utiliza as camadas OSI para a gerência
- CMOT: representa o CMIP sobre os protocolos TCP/IP

CMIP foi desenvolvido para suprir as carências encontradas no SNMP de forma a ser um sistema de gerenciamento de redes maior e mais detalhado.No CMIP as variáveis são mais complexas e com sofisticadas estruturas de dados. O protocolo CMIT/CMOT possui seis operações básicas:

- Get (recuperar o valor da variável)
- Set (alterar valor da variável)
- Action (realiza comando imperativo no nodo)
- Create (manipulação de instâncias)
- Delete (remoção)
- event-report (notificação)

Para realizar as operações o protocolo CMIT/CMOT utiliza onze tipos de PDU:

- m-eventReport
- m-EventReport-Confirmed
- m-Get
- m-Linked-Reply
- m-Set
- m-Set-Confirmed
- m-Action
- m-Action-Confirmed
- m-Create

- m-Delete
- m-Cancel-Get-Confirmed

Vantagens do CMIP

Uma das maiores vantagens do CMIP é com relação a segurança. O CMIP pode prover um grande controle sobre a rede através de seus sofisticados serviços de notificação.

Outra vantagem é com relação ao fato que suas variáveis são mais complexas que as variáveis do SNMP fornecem uma maior quantidade de informaçõ

Desvantagens do CMIP

O protocolo CMIP requer mais dos recursos de rede do que o SNMP.Ou seja, poucos sistemas do planeta conseguem manipular a complexa implementação do CMIP sem grandes modificações. Outra desvantagem é que o CMIP é muito difícil de se programar, á tantos tipos de variáveis que somente programadores muito experientes são capazes de utiliza-las com seu potencial total.

BIBLIOGRAFIA

Sites:

http://pucmgmt.metropoa.tche.br/

http://www.ieee.org

http://homer.span.ch/~spaw2724/SNMP/Portugues/