1 A arquitetura SNMP

O modelo arquitetural SNMP consiste em uma coleção de estações de gerenciamento e elementos de rede. As estações de gerenciamento executam aplicações que monitoram e controlam os elementos de rede. Os elementos de rede são equipamentos tais como hospedeiros, gateways, servidores de terminais, e similares, que possuem agentes de gerenciamento, e que são responsáveis pela execução das funções de gerenciamento de rede, requisitadas pelas estações de gerenciamento. O protocolo SNMP é usado para transportar a informação de gerenciamento entre as estações de gerenciamento e os agentes existentes nos elementos de rede. A figura 1 mostra algumas das interações possíveis entre um Gerente e um Agente, através do protocolo SNMP.

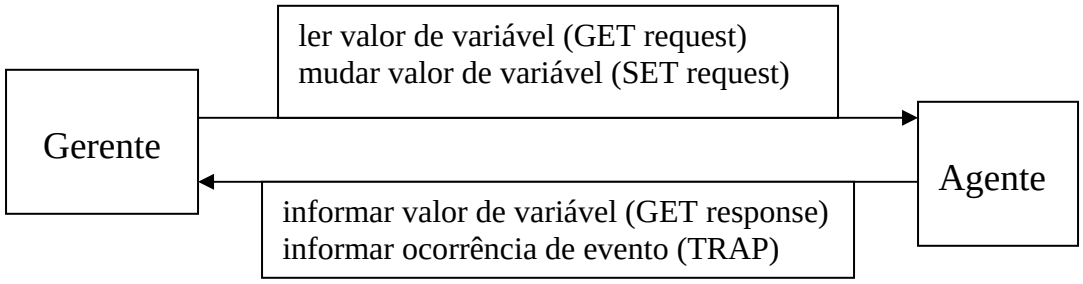

Figura 1. Troca de mensagens SNMP entre Gerente e Agente

O modelo proposto busca minimizar o número e a complexidade de funções de gerenciamento realizadas pelos agentes de gerenciamento. As razões que tornam este objetivo atrativo são:

- O custo de desenvolvimento do software de agente de gerenciamento, necessário para suportar o protocolo é significativamente reduzido;
- O grau de funcionalidade suportado remotamente é proporcionalmente aumentado, à medida que se aumenta a utilização dos recursos internet na tarefa de gerenciamento;
- A quantidade de funções de gerenciamento, que são suportadas remotamente, é gradativamente aumentada, através da imposição de algumas restrições sobre a forma e sofisticação das ferramentas de gerenciamento.
- Conjuntos simplificados de funções de gerenciamento são facilmente entendidos e utilizados pelos desenvolvedores de ferramentas de gerenciamento de redes.

O segundo objetivo do protocolo é que o paradigma funcional para monitoração e controle deve ser suficientemente extensível para acomodar aspectos adicionais, e possivelmente não previstos, da operação e gerenciamento de redes.

O terceiro objetivo é que a arquitetura deve ser, tanto quanto possível, independente da arquitetura e dos mecanismos de hospedeiros e gateways particulares.

1.1 Serviços e protocolos de gerência

O primeiro dos protocolos de gerência de rede foi o SGMP (*Simple Gateway*

Monitoring Protocol) que surgiu em novembro 1987. Entretanto, o SGMP era restrito à monitoração de gateways. A necessidade crescente de uma ferramenta de gerenciamento de rede mais genérica fez emergirem mais algumas abordagens:

High-Level Entity Management System – HEMS – generalização do HMP – Host Management Protocol;

SNMP – *Simple Network Management Protocol* – um melhoramento do SGMP;

CMOT – (CMIP over TCP/IP) uma tentativa de incorporar o máximo possível o protocolo (CMIP), serviços e estrutura de base de dados que estava sendo padronizada pela ISO para gerenciamento de redes.

No início de 1988 a IAB (*Internet Architecture Board*) revisou os protocolos e escolheu o SNMP como uma solução de curto prazo e o CMOT como solução de longo prazo para o gerenciamento de redes. O sentimento era que, em um período de tempo razoável, as instalações migrariam do TCP/IP para protocolos baseados em OSI. Entretanto, como a padronização do gerenciamento baseado no modelo OSI apresentava muita complexidade de implementação e o SNMP, devido à sua simplicidade, foi amplamente implementado nos produtos comerciais, o SNMP tornou-se um padrão de fato. Posteriormente, pela existência de lacunas funcionais (devido exatamente à simplicidade do SNMP), foram definidas novas versões do protocolo SNMP chamadas de SNMPv2 e SNMPv3, e o SNMP original ficou conhecido como SNMPv1.

A primeira versão da arquitetura de gerenciamento SNMP foi definida no RFC 1157 de maio de 1990.

O RFC 1157 define que a arquitetura SNMP consiste de uma solução para o problema de gerenciamento de redes, em termos de:

- O escopo da informação de gerenciamento comunicada pelo protocolo;
- A representação da informação de gerenciamento comunicada pelo protocolo;
- Operações sobre a informação de gerenciamento, suportadas pelo protocolo;
- A forma e o significado das trocas entre entidades de gerenciamento;
- A definição dos relacionamentos administrativos entre entidades de gerenciamento;
- A forma e o significado das referências às informações de gerenciamento.

O RFC 1157 define ainda três objetivos a serem alcançados pelo SNMP: minimizar o número e complexidade das funções de gerenciamento, ser flexível o suficiente para permitir expansões futuras e ser independente da arquitetura e mecanismo dos dispositivos gerenciados.

1.2 Elementos da Arquitetura

O SNMP foi projetado para ser um protocolo de camada de aplicação da família TCP/IP e trabalhar sobre UDP, que é um protocolo não orientado à conexão.

A comunicação de informações de gerenciamento é feita no SNMPv1 utilizando somente cinco mensagens de protocolo, conforme mostrado na figura 2. Três delas (get-request, get-next-request e set-request) são iniciadas pelo processo de aplicação gerente, as

outras duas (get-response e trap) são geradas pelo processo agente. A geração de mensagens é chamada de um evento. No esquema de gerenciamento SNMP, o gerente monitora a rede, indagando os agentes sobre seu estado e características. Entretanto a eficiência é aumentada quando agentes enviam mensagens não solicitadas chamadas de traps. Um trap ocorre quando o agente observa a ocorrência de um parâmetro pré-configurado no módulo agente.

Operação	Função
get-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis informados na solicitação
get-next-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis que sucedem lexicograficamente àquelas informadas na solicitação
set-request	Solicitação para atribuição de valor a uma ou um conjunto de variáveis
get-response	Resposta às operações get-request, get-next-request e set-request
Trap	Envio de um evento não solicitado para uma ou várias estações de gerenciamento. Tipos de traps definidos no RFC 1215: cold start, warm start, link down, link up, authentication failure, egp neighbor loss e enterprise specific.

Figura 2 – Operações Suportadas no SNMPv1

A mensagem SNMP é dividida em duas seções: uma identificação de versão e nome da comunidade e a PDU (protocol data unit). A versão e comunidade são às vezes chamadas de header de autenticação SNMP. Existem 5 tipos diferentes de PDU: get-request, get-next-request, get-response, set-request e trap. Todas as PDU´s, exceto o trap, têm o mesmo formato, conforme mostra a figura 3.

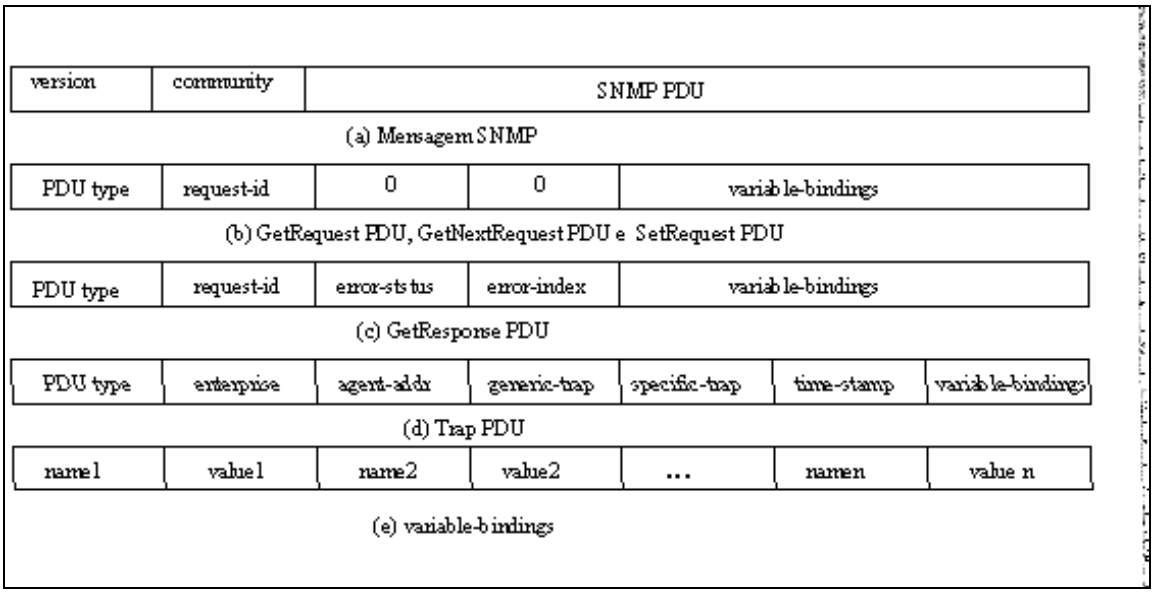

Figura 3 – Formato de Mensagens SNMPv1

O SNMPv1 tem um processo de autenticação fraca. Ele se baseia em um string de caracteres chamado *community* contido no cabeçalho do pacote SNMP e que trafega em modo legível pela rede. São definidas duas *communities*, uma para acesso somente de leitura e outra para acesso de leitura e gravação.

O SNMP não provê mecanismos específicos para que um gerente dê comandos para que um agente execute uma ação. Entretanto, é possível utilizar a operação set para contornar esta deficiência. Um objeto pode ser utilizado para representar um comando, então uma ação específica é executada se o valor do objeto é alterado para um valor específico (ex: objeto *reboot*).

Apesar de amplamente difundido e utilizado no gerenciamento de redes de computadores, o SNMPv1 possui as seguintes limitações:

- ✓ Não é apropriado para o gerenciamento de redes muito grandes, devido à limitação de performance de *polling*;
- ✓ *Traps* SNMP não são reconhecidos, pois são implementados sobre protocolos sem reconhecimento/conexão;
- ✓ O padrão SNMPv1 provê somente autenticação trivial;
- ✓ O modelo da MIB é limitado e não suporta aplicações que questionam o gerenciamento baseado em valores ou tipos de objetos;
- ✓ Não é possível ter uma idéia do tráfego existente nas redes onde os recursos gerenciados estão instalados, pois estas informações referem-se ao próprio recurso onde o agente está executando;
- ✓ Incapacidade de analisar seus próprios dados e enviarem notificações quando alguns limiares forem atingidos; e
- ✓ Não suporta a comunicação gerente-gerente.
- ✓ Não suporta a comunicação gerente-gerente.

1.3 Modelo de informação

Atualmente vários documentos definem a informação de gerenciamento no modelo SNMP, sendo que os principais são: o RFC 1155 - Estrutura da Informação de Gerenciamento (SMI), o RFC 1213 - Base de Informação de Gerenciamento (MIB) e o RFC 1157 – Protocolo Simples de Gerenciamento de Rede (SNMP).

A SMI (*Structure and Identification of Management Information* for TCP/IP-Based *Internets*) descreve como os objetos gerenciados contidos na MIB são definidos.

A MIB (*Management Information Base*) descreve quais são os objetos contidos na MIB.

O SNMP (*Simple Network Information Protocol*) define o protocolo usado para gerenciar estes objetos.

1.3.1 Estrutura da Informação de Gerenciamento (SMI)

A SMI especifica as estruturas que representam os recursos a serem gerenciados, usando um subconjunto da sintaxe denominada ASN.1 (*Abstract Syntax Notation One*) [ISO8824, 1987].

Também, para efeitos de simplicidade, é utilizado um subconjunto das regras básicas de codificação ASN.1. Todas as codificações utilizam a forma de tamanho definido. Além disso, quando permitido, são usadas codificações de não construtores, preferencialmente às

codificações de construtores. Esta restrição se aplica a todos os aspectos de codificação ASN.1, tanto para as unidades de dados do protocolo, quanto para os objetos de dados que elas contém.

Os nomes para todos os tipos de objetos contidos na MIB, são definidos explicitamente na MIB padrão Internet ou em outros documentos que seguem as convenções de nomeação definidas na SMI. A SMI requer que todos os protocolos de gerenciamento definam mecanismos para identificar instâncias individuais dos tipos de objetos de um elemento de rede particular.

Cada instância de tipo de objeto definido na MIB é identificada, nas operações SNMP, por um nome único chamado *nome de variável*. Geralmente, o nome de uma variável SNMP é um OBJECT IDENTIFIER da forma x.y, onde x é o nome de um tipo de objeto não agregado definido na MIB e y é um fragmento de OBJECT IDENTIFIER que, de uma forma específica para o tipo de objeto nomeado, identifica a instância desejada.

Esta estratégia de nomeação permite a exploração completa da semântica da PDU GetNextRequest, porque ela atribui nomes para variáveis relacionadas, em uma ordem lexicográfica contínua.

A nomeação de tipos específicos de algumas instâncias de objetos, para algumas classes de tipos de objetos, é definida a seguir. Instâncias de um tipo de objeto, para as quais nenhuma das seguintes convenções de nomeação são aplicáveis, são nomeadas por um OBJECT IDENTIFIER da forma x.0, onde x é o nome do tipo de objeto na definição da MIB.

Suponha-se, por exemplo, que se deseje identificar uma instância da variável sysDescr. A classe de objeto para sysDescr é:

iso	org	dod	internet	mgmt	mib	system	sysDescr
1	3	6	1	2	1	1	1

Neste caso, o tipo de objeto x deve ser 1.3.6.1.2.1.1.1, para o qual deve ser concatenado um sub-identificador 0, isto é, 1.3.6.1.2.1.1.1.0 identifica uma e somente uma instância de sysDescr.

A figura 4 mostra a árvore de registro utilizada para nomeação de objetos definidos na MIB.

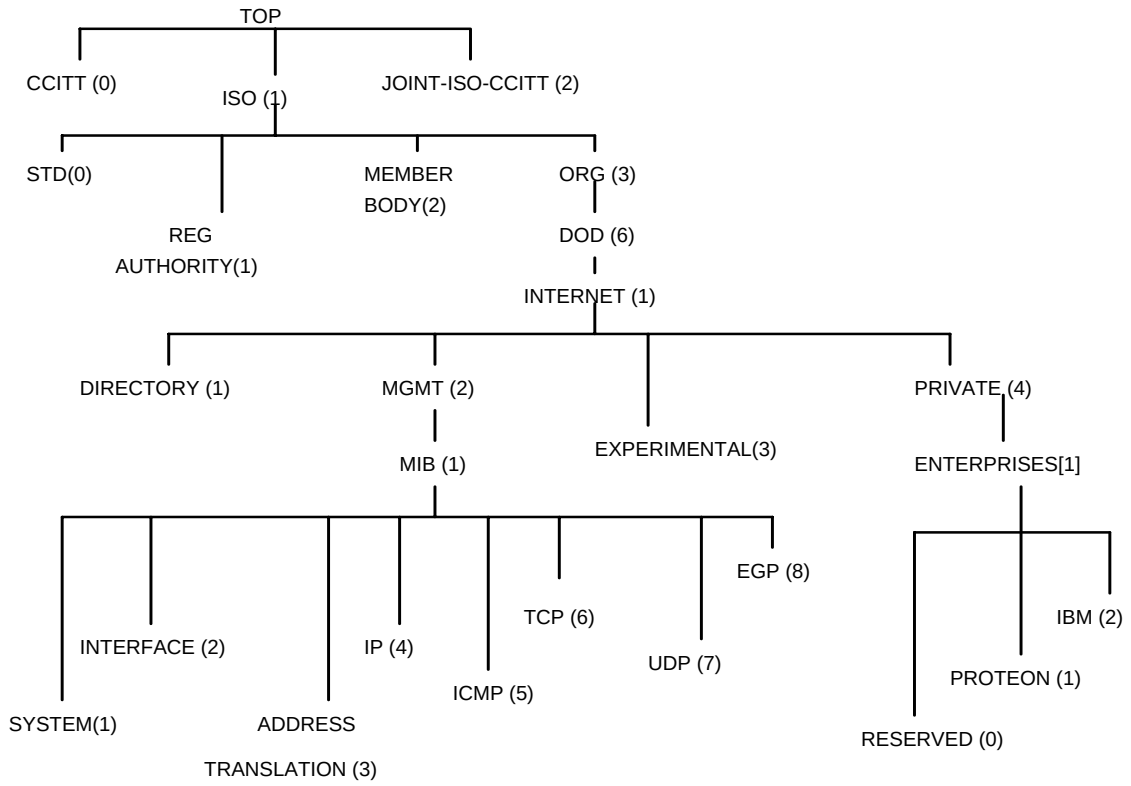

Figura 4 - Árvore de registro de tipos de objetos

A sub-árvore MGMT contém a definição das bases de informação de gerenciamento que foram aprovadas pelo IAB. Atualmente, existem duas versões da MIB: mib-1 e mib-2. A mib-2 é uma extensão da primeira. As duas possuem o mesmo identificador na sub-árvore porque apenas uma das duas estará presente em qualquer configuração.

A SMI identifica os tipos de dados que podem ser usados na construção de uma base de informação de gerenciamento e como os recursos dentro desta base podem ser representados e nomeados. São definidos apenas dois tipos de dados simples: escalar (variáveis simples) e array bidimensional de escalares (tabelas).

Os tipos de dados ASN.1 que podem ser utilizados na definição dos objetos da MIB são basicamente:

UNIVERSAL:

INTEGER, OCTET STRING, NULL, OBJECT IDENTIFIER, SEQUENCE e SEQUENCE OF.

APPLICATION:

NetworkAddress, IpAddress, Counter, Gauge, TimeTicks e Opaque.

Cada objeto na MIB possui um nome, um tipo, um valor, uma forma de acesso, um status e uma descrição, e sua definição, de acordo com a SMI, segue a seguinte estrutura:

nome do objeto OBJECT-TYPE
SYNTAX <nome de um tipo, ex.: INTEGER, IpAddress, etc.>

```
        ACCESS      <read-only, write-only, read-write, not-accessible >
        STATUS      <se é obrigatório ou não: mandatory ou optional>
        DESCRIPTION     <um texto explicativo escrito entre aspas>
        ::= {<nome usado para acessar o objeto via SNMP>}
```

Exemplos:

```
tcpConnTable  OBJECT-TYPE
        SYNTAX      SEQUENCE OF TcpConnEntry
        ACCESS      not-accessible
        STATUS      mandatory
        DESCRIPTION     "A table containing TCP connection-specific information."
        ::= {tcp 13}

tcpConnEntry  OBJECT-TYPE
        SYNTAX      TcpConnEntry
        ACCESS      not-accessible
        STATUS      mandatory
        DESCRIPTION
        "Information about a particular current TCP connection. An object of this type is
        transient, in that it ceases to exist when (or soon after) the connection makes the
        transition to the CLOSED state."
        ::= {tcpConnTable 1}

TcpConnEntry SEQUENCE       {tcpConnState       INTEGER,
                             tcpConnLocalAddress     IpAddress,
                             tcpConnLocalPort        INTEGER (0..65535),
                             tcpConnRemAddress       IpAddress,
                             tcpConnRemPort          INTEGER (0..65535)}

tcpConnState   OBJECT-TYPE
        SYNTAX      INTEGER    {closed (1),
                                listen (2),
                                synSent (3),
                                synReceived (4),
                                established (5),
                                finWait1 (6),
                                finWait2 (7),
                                closeWait (8),
                                lastAck (9),
                                closing (10),
                                timeWait (11),
                                deleteTCB (12) }
        ACCESS      read-write
        STATUS      mandatory
DESCRIPTION     "The state of this TCP connection.
```

```
        The only value which may be set by a management station is deleteTCB(12).
        Accordingly, it is appropriate for an agent to return a "bad value" response if a
        management station attempts to set this object to any other value.
        If a management station sets this object to the value deleteTCB(12), then this has
        the effect of deleting the TCB (as defined in RFC 793) of the corresponding
        connection on the managed node, resulting in immediate termination of the
        connection.
        As an implementation-specific option, a RST segment may be sent from the
        managed node to the other TCP end point (note however that RST segments are not
        sent reliably)."
::= {tcpConnEntry 1}

tcpConnRemPort  OBJECT-TYPE
        SYNTAX      INTEGER (0..65535)
        ACCESS      read-only
        STATUS      mandatory
        DESCRIPTION     "The remote port number for this TCP connection."
        ::= {tcpConnEntry 4}
```

1.3.2 A base de informações de gerenciamento - MIB

A MIB é uma coleção estruturada de objetos gerenciados. Objetos gerenciados representam os recursos sujeitos ao gerenciamento. Cada nodo do sistema de gerenciamento mantém uma MIB que reflete o estado dos recursos gerenciados naquele nodo. Uma entidade de gerenciamento pode monitorar os recursos de um nodo, lendo os valores dos objetos na MIB e pode controlar os recursos de um nodo, modificando estes valores.

Os objetos da mib-2 são subdivididos nos seguintes grupos:

- system: informações gerais sobre o sistema;
- interfaces: informações sobre cada uma das interfaces do sistema para a sub-rede;
- at(address translation; deprecated): descreve a tabela de translação de endereços para mapeamento de endereços internet para endereços de sub-rede;
- ip: informação relativa a experiências de implementação e execução do protocolo IP (internet protocol) no sistema;
- icmp: informação relativa a experiências de implementação e execução do protocolo ICMP (internet control message protocol) no sistema;
- tcp: informação relativa a experiências de implementação e execução do protocolo TCP (transmission control protocol) no sistema;
- udp: informação relativa a experiências de implementação e execução do protocolo UDP (user datagram protocol) no sistema;
- egp: informação relativa a experiências de implementação e execução do protocolo EGP (external gateway protocol) no sistema;
- cmot: informações para sistemas de gerência OSI;
- transmission: fornece informações sobre esquemas de transmissão e protocolos de acesso em cada interface do sistema;

- snmp: informação relativa a experiências de implementação e execução do protocolo SNMP (simple network management protocol) no sistema;

A organização em grupos é conveniente porque os objetos são organizados de acordo com as funções das entidades gerenciadas e também porque ela oferece um guia para os implementadores de agentes, no sentido de identificar quais objetos devem ser implementados. Se a semântica de um grupo for aplicável para uma determinada implementação, então todos os objetos do grupo devem ser implementados. Por exemplo, uma implementação deve incluir todos os objetos do grupo TCP se e somente se ela implementa o protocolo TCP; portanto, uma bridge ou um router não necessita implementar os objetos do grupo TCP. Uma exceção a esta regra é o grupo de translação de endereços (at). A figura 5 ilustra a estrutura do grupo system e a tabela 1 fornece a sintaxe do objeto, a forma de acesso permitida e uma descrição sucinta da semântica.

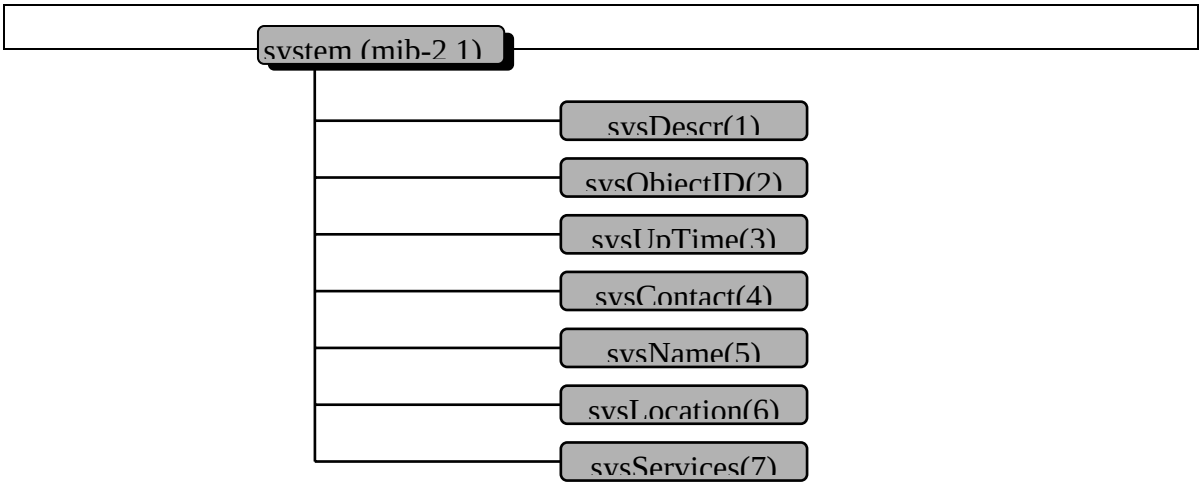

Figura 5. Grupo System da MIB-II

Tabela 1 - Objetos do grupo System da MIB-II

Objeto	Sintaxe	Acesso	Semântica
sysDescr	DisplayString (Size (0..255)	RO	Descrição de uma entidade (hardware, sistema operacional, etc.
sysObjectID	OBJECT IDENTIFIER	RO	Identificação do sub-sistema contido na entidade
sysUpTime	TimeTicks	RO	Tempo decorrido desde a última reinicialização
sysContact	DisplayString (Size (0..255)	RW	Identificação da pessoa de contato para este nodo

			gerenciado
sysName	DisplayString (Size (0..255)	RW	Nome atribuído administrativamente para este nodo
sysLocation	DisplayString (Size (0..255)	RW	Localização física do nodo
sysServices	INTEGER (0..127)	RO	Valor indicando o conjunto de serviços oferecidos pela entidade