UNIVERSIDADE FEDERAL DA PARAÍBA

Centro de Ciências e Tecnologia

Coordenação de Pós-Graduação em Informática

Mestrado em Informática

Base de Dados de Gerenciamento SNMP/MIB

Aluno: Washington Luiz Evangelista Teixeira

Professor: Joberto Sérgio Barbosa Martins

Campina Grande, PB

Setembro de 1993

INTRODUÇÃO

O poder de processamento dos computadores tem crescido cada vez mais nos últimos anos, enquanto seu custo segue em direção oposta, possibilitando seu acesso até mesmo ao cidadão comum. Conecta-los para troca de informação é uma tendência irreversível. Mesmo aquela faixa da população que não dispõe de computadores, tem acesso a serviços cada vez mais informatizados e normalmente interligado a uma rede de computadores, tornando-o também um usuário.

Esse contínuo crescimento de usuários de redes de computadores, coloca esse mercado consumidor como atrativo para um número cada vez maior de empresas fornecedoras. Nesse momento é conveniente lembrar que as necessidades insatisfeitas dos consumidores possui uma velocidade maior que os organismos internacionais conseguem padronizar. Esses dois fatores, aliados a outros de menor importância, provocam o aparecimento de produtos diversos com interoperabilidade difícil, mas que necessitam interagir devido a seus investimentos. Isso faz crescer a importância e a complexidade da gerência de redes de computadores.

A área de atuação do gerenciamento de rede é vasta, envolvendo principalmente as de: gerenciamento de falha; gerenciamento de configuração; gerenciamento de contabilização; gerenciamento de desempenho; e gerenciamento de segurança.

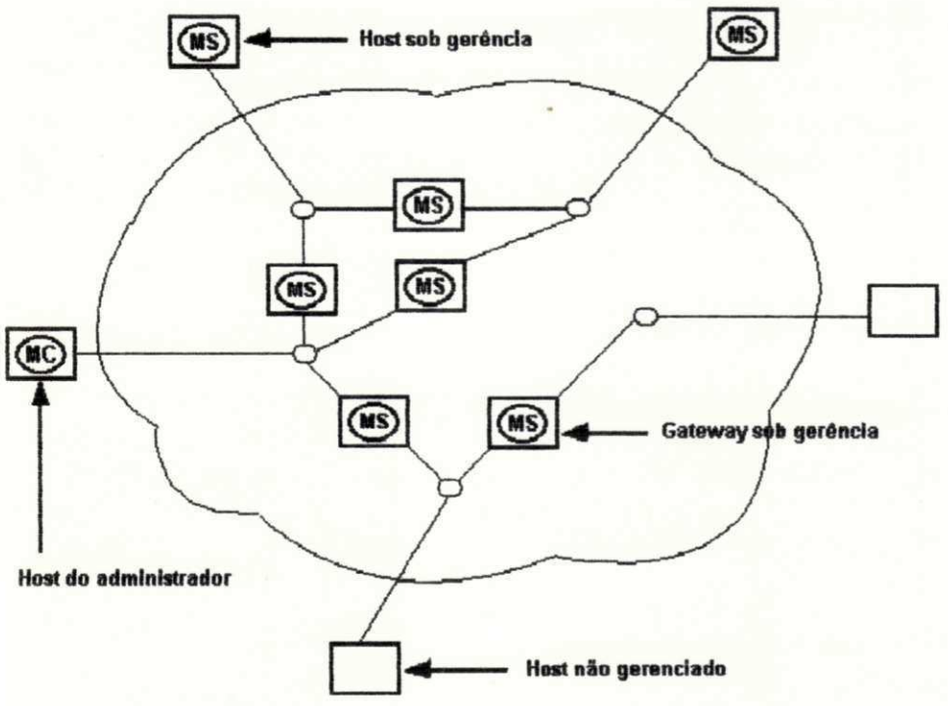
A família de protocolos TCP/IP é um padrão de fato para interconexão de sistemas abertos. É usado no mundo inteiro pelos mais variados setores da sociedade, por permitir um alto grau de interoperabilidade, aliados a um bom número de fornecedores e plataformas disponíveis.

Para gerenciar redes de computadores, o usuário possui uma gama de possibilidades, podendo ser padrão oficial, padrão de fato ou solução proprietária. A família de protocolos TCP/IP possui solução integrada para gerência de rede de computadores.

Esse trabalho visa descrever os princípios da base de dados utilizada pelo TCP/IP na função de gerência. Para que a leitura do trabalho não tenha como pré-requisito o conhecimento do mecanismo de gerência do TCP/IP, será descrito de forma geral esse mecanismo, citando os agentes envolvidos com suas responsabilidades. Também será desenvolvida uma associação destes agentes, da base de dados com a modelagem por objetos. O trabalho é concluído com considerações que visem sedimentar as informações apresentadas.

O MODELO DA ARQUITETURA DE GERENCIAMENTO DO TCP/IP

Dominar o conceito de gerência de rede TCP/IP, passa obrigatoriamente pela compreensão do seu modelo de gerenciamento, como também dos agentes envolvidos. A arquitetura escolhida é centralizada como pode ser percebido pela figura abaixo. Múltiplas gerências sobrepostas podem coexistir. Passando agora para os agentes temos que o administrador da rede é o primeiro deles, profissional especializado responsável pela tomada de decisões nas ações de gerências de uma rede ou parte dela (domínio do administrador); o segundo agente é denominado servidor, que é na pratica um processo em execução em uma máquina remota (tendo como referência a máquina do administrador), executando as ações de gerências sobre algum recurso de rede dentro do mesmo domínio; o gerente é o terceiro agente, tendo a responsabilidade proporcionar a comunicação entre administrador e servidor, na prática também um processo em execução na máquina do administrador. Adicionalmente há uma interface homem-máquina que permite a comunicação entre o administrador é o gerente. Essa interface pode conter ou não uma ferramenta de gerência.



Um administrador de rede utilizando seu equipamento (uma workstation por exemplo), através da interface homem-máquina invoca um processo gerente sendo executado localmente, informado-o para contactar um ou mais processos servidores. Após a conexão e reconhecimento do administrador como autorizado, este último pode, com o envio de mensagens, obter informações sobre recursos da rede localmente ao servidor,

como também alterar o comportamento de algum recurso. Estes são vistos pelo gerente como um conjunto de variáveis conceituais consultáveis, alteráveis ou ambas, ou seja uma abstração do recurso. Essas variáveis podem ser simples como um contador de datagrama que chegam num roteador, ou complexas como a tabela de roteamento. Podem ter sido definidas exclusivamente para gerência ou coincidam com uma estrutura de dados do TCP/IP. Portanto uma variável conceitual pode conter muitos itens de dados.

O formato e o significado das mensagens trocadas entre gerente e servidor, como também formato, significado e apresentação das variáveis conceituais são padronizadas e estão comentados logo a seguir.

O PROTOCOLO DE COMUNICAÇÃO DE INFORMAÇÕES DE GERÊNCIA

O TCP/IP não possui um protocolo oficial para comunicação de informações de gerência, no entanto possui duas propostas padrões recomendáveis. A primeira delas denominada de SNMP ("Simples Network Management Protocol") é a mais utilizada pelo mercado é será abordada neste trabalho. A segunda conhecida por CMIP sobre TCP (CMOT), especifica o padrão ISO ("International Organization for Standardization") correspondente ("Commom Management Information Services" / "Commom Management Information Protocol"), sobre uma conexão TCP ("Transmission Control Protocol"). As duas propostas operam no nível de aplicação, proporcionando uniformidade com o uso do mesmo conjunto de protocolos em toda a rede. É importante acrescentar o fato de que todos os componentes da rede respondem ao mesmo conjunto de comandos.

Ambas as propostas dividem a gerência em duas áreas, especificando padrões para cada uma delas. A primeira se preocupa com a comunicação entre cliente e servidor, definindo a forma e o significado das mensagens trocadas, bem como a representação dos itens de dados incluídos. A segunda área se preocupa com os dados sendo controlados, definindo que itens de dados (variável conceitual) o servidor deve manter, bem como suas denominações e a sintaxe que os expressam. Adicionalmente também está padronizado a autenticação de um administrador por parte de um servidor (proteção contra acesso indevido). Será visto mais a frente que a segunda área é uma extensão ao protocolo.

O protocolo SMNP opera com a filosofia do paradigma de busca e armazenamento (fetch-store), isso conceitualmente significa que um administrador interagem com um servidor, através do gerente, utilizando apenas dois comandos (busca e armazenamento). O primeiro permite ler e o segundo alterar o conteúdo de uma variável conceitual. Com esse mecanismo, a alteração do conteúdo de uma variável pode levar o servidor a executar ações como reconfigurar um recurso da rede, reinicializa-lo ou mesmo deixa-lo inoperante.

A figura abaixo resume as operações básicas que um servidor pode executar sobre suas variáveis conceituais a pedido do administrador da rede via gerente.

OPERAÇÕES	FUNÇÕES
Get-request	Obter o conteúdo de uma variável especifica
Get-next-request	Obter o valor da próxima variável, sem conhecer sua denominação
Get-response	Responder a uma operação de Get-request ou Get-next-request
Set-request	Armazenar um valor em uma variável específica
Trap	Resposta vinculada à ocorrência de um evento

Para cada uma das operações mencionadas é definido um tipo específico de mensagem de protocolo (PDU "Protocol Data Unit"), A filosofia de aquisição da informação do servidor em relação ao gerente pode ser passiva ou ativa. No primeiro caso o servidor aguarda indefinidamente uma consulta ("pooling") do gerente para alterar ou retornar o conteúdo de uma variável ou ainda executar alguma ação decorrente da alteração do conteúdo da variável. No segundo caso em decorrência de uma operação 'Trap', o servidor por iniciativa própria informa sobre a ocorrência de algum evento monitorado por ele, normalmente erros, falhas ou violação de algum protocolo.

Nesse momento é conveniente um parênteses para comentar ASN.1 ("Abstract Syntax Notation.1"). Um padrão internacional muito utilizado pela padronização de gerência do TCP/IP.

ASN.1 é uma linguagem formal especificada pela ISO e adequada para definir protocolos de comunicação, por garantir interoperabilidade e possuir duas codificações para a mesma informação. Uma textual adequada para a leitura humana e uma outra numérica e compacta adequada a computadores. Ambas as notações são isentas de ambigüidades tanto na representação quanto no significado. ASN.1 é especialmente importante quando a implementação do protocolo prevê o uso em plataformas heterogêneas que diferem na representação interna dos dados. Cada máquina traduz a codificação para sua representação interna. Outros usos de codificação ASN.1 será visto mais a frente.

Voltando ao protocolo de comunicação de informações de gerência SNMP, pode-se dizer que, ao contrário dos demais membros da família, suas mensagens não possuem campos fixos, no entanto são especificados na notação ASN.1. A codificação para esse caso consiste de três partes principais. A primeira é a versão do protocolo, a segunda corresponde ao identificador da comunidade SNMP (domínio), e a terceira contem os dados. Esta ultima pode conter uma ou mais PDUs. Abaixo o formato de uma mensagem em notação ASN.1 na forma textual.

```
SNMP-Message ::=
  SEQUENCE {
    version INTEGER {
      versao-1 (0)
  },
  community
    OCTETO STRING,
  data
    ANY
}
```

A representação de um item de dado numa mensagem codificada em ASN.1 é composta de duas partes, um cabeçalho e um corpo. O cabeçalho por sua vez contem duas informações, um código de tipo do item de dado e seu comprimento em octetos. O corpo contem o valor do item de dado. Para a perfeita compreensão de um exemplo falta ainda algumas considerações que estão mais adiante, por isso um exemplo de representação de item de dado num mensagem será apresentado no momento oportuno.

A BASE DE DADOS GERENCIAL

Foi dito anteriormente que o servidor mantinha um conjunto de variáveis conceituais, cujos conteúdos eram acessíveis pelo administrador, via gerente, podendo obter seus conteúdos ou modifica-los com o envio de mensagem. Foi dito também que as mensagens podiam transportar uma ou mais PDUs, cada uma correspondendo a uma operação básica que o servidor deverias realizar sobre uma variável. No entanto quase nada foi dito sobre as variáveis. É chegado o momento.

Relembrando que uma variável conceitual é uma abstração de um recurso real da rede, portanto um modelo computacional desse recurso. Como os recursos modelados são os mais heterogéneos possíveis, é obvio que a implementação de uma mesma operação básica varia em complexidade de acordo com a complexidade do recurso modelado. Também é aceitável que algumas podem ser idênticas, diferindo apenas nos endereços de acesso, seria o caso de variáveis simples tipo contadores de datagramas. Modelar um recurso simples pode exigir apenas um item de dado mas modelar recurso complexo complexo faz-se necessário vários itens de dados (atributos).

Nesse momento podemos ver claramente que é possível mapear uma variável conceitual como um objeto, ou seja cada tipo de recurso pertence a uma classe que modela aquele recurso. Cada recurso por sua vez é uma instância (objeto) de sua classe. Já o mecanismo de herança pode ser percebido no momento em que o servidor é visto como uma instância de uma superclasse. Nela estão todos os atributos (itens de dados) e métodos (operações básicas) comuns a todos os objetos (variáveis conceituais). As particularidades próprias de cada tipo de variável conceitual necessárias à modelagem do recurso correspondente é uma redefinição (especialização) do gerente ou de uma outra classe já especializada.

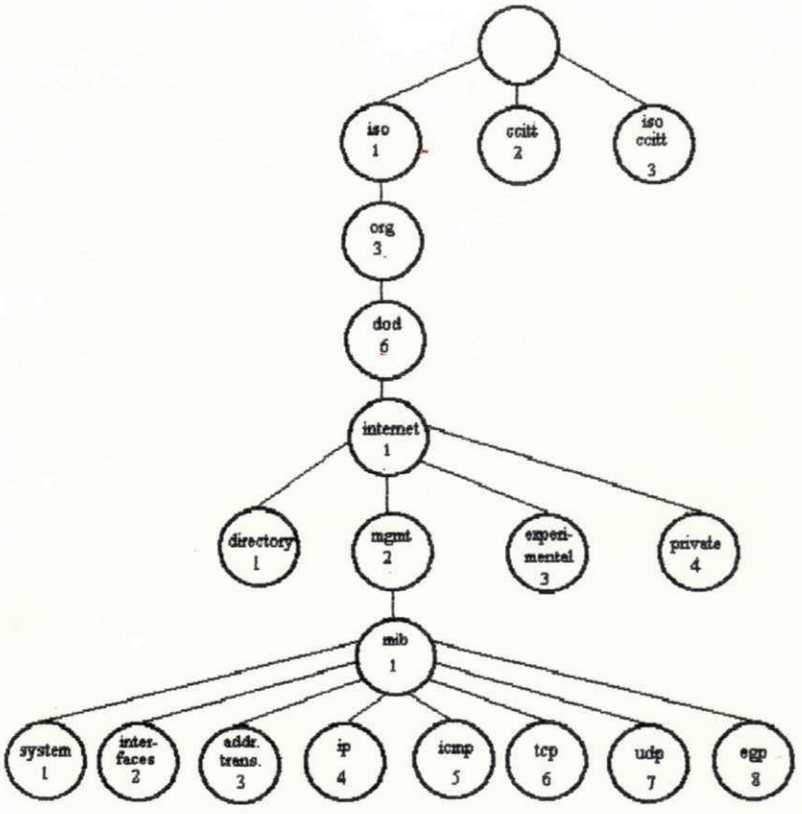
No caso de dois ou mais recursos de um mesmo tipo diferindo apenas em sofisticação, caso cada um é uma instância de classes especializadas a partar de uma classe base que contem atributos e operações comuns.

Em adição as propostas de protocolo de comunicação para gerência de rede (SNMP/CMOT), um padrão em separado foi definido para gerenciar os objetos. Esse padrão inicialmente denominado de MIB (Management Information Base) foi de comum acordo dos grupos. Uma extensão se fez necessária mas devido a falta de consenso em 1989 o grupo do SNMP apresentou o padrão MIB-II, enquanto o outro grupo definiu o padrão MIB-II-OIM.

A MIB é conceitual e define o conjunto de objetos gerenciáveis que o servidor deve manter bem como a semântica de cada um. Relembrando que um objeto MIB (variável conceitual) pode registrar por exemplo o estado de cada uma das conexões de rede (variável complexa), o numero de datagramas retransmitidos (variável simples) ou o conteúdo corrente da tabela de roteamento do protocolo IP. A MIB do TCP/IP não possui uma dimensão temporal, portanto não fornece a historia da gerência. Deve receber extensões para uma gerência pró-ativa.

Um segundo padrão adicional foi definido para especificar a MIB. Denominado de SMI (Structure of Management Information) que especifica dois conjuntos de regras: o primeiro define como nomear objetos MIB; e segundo como especificar tipos de objetos, as operações realizadas sobre eles, como também o comportamento destes mediante a execução destas operações.

O SMI define a codificação ASN.1 para nomear objetos MIB. Nesse caso a codificação define uma hierarquia de nomes onde o nome de um objeto MIB reflete sua posição na hierarquia. Esse padrão garante denominação única e absoluta (global). O SMI utiliza a hierarquia de identificadores de objetos administrada pela ISO e pelo CCITT ("Consultative Committee for International Telegraph and Telephone"). A figura abaixo expressa a sub-arvore dessa hierarquia que interessa a MIB. Com esse padrão não é só possível tratar os objetos mas também outros itens correlatos como por exemplo documentos de padrões internacional de protocolo. Cada identificador de objeto possue uma codificação com duas formas de apresentação, uma textual e outra numérica.



A definição de tipo contém cinco campos:

. nome textual (identificador de objeto);
. uma sintaxe ASN.1;
. a definição da semântica associada ao tipo do objeto;
. o tipo de acesso (read-only, read-write, write-only e protected); e
. status (obrigatório, opcional e absoluto)

A combinação de um protocolo de comunicação com a SMI é denominado de "framework". Um administrador interage com o servidor de acordo com as regras do "framework".

O identificador de objetos raiz não possui nomeação, mas seus descendentes diretos são ISO, CCITT e conjuntamente os dois. Como exemplo, seja o identificador 'internet', sua codificação na forma textual é grafada como iso.org.dod.internet e 1.3.6.1 na forma numérica. A MIB do TCP/IP possui codificação iso.org.dod.internet.mgmt.mib e 1.3.6.1.2.1 respectivamente. Observar que a codificação utiliza o ponto para separar os identificadores de objetos e a hierarquia é grafada da esquerda para a direita.

Observe que a MIB do TCP/IP possui oito categorias resumidas na tabela abaixo.

CATEGORIA DA VARIÁVEL	TIPO DA INFORMAÇÃO
system	Host ou gateway
interfaces	Interface de rede
Address translation	Endereço de translação
ip (Internet Protocol)	Software de protocolo IP
icmp (Internet Control Message Protocol)	Software de protocolo ICMP
tcp (Transmission Control Protocol)	Software de protocolo TCP
udp (User Datagram Protocol)	Software de protocolo UDP
egp (Exterior Gateway Protocol)	Software de protocolo UGP

Agora que foi apresentado o modo de identificar objetos MIB do TCP/IP, é conveniente colocar alguns exemplos da nomeação padronizada. A tabela abaixo traz estes exemplos.

VARIÁVEL MIB	CATEGORIA	SIGNIFICADO
sysUpTime	system	Tempo decorrido da ultima reinicialização
ifNumber	interfaces	Numero de interface de rede
ifMtu	interfaces	MTU para uma interface particular
ifDefaultTTL	ip	Valor do campo 'time-to-live'
ipInReceives	ip	Numero de datagramas recebidos
ipForwDatagrams	ip	Numero de datagramas enviados
ipOutNoRoutes	ip	Numero de rotas falhas
ipReasmOK	ip	Numero de datagramas remontados
ipFragOK	ip	Numero de datagramas fragmentados
ipRoutingTable	ip	Tabela de roteamento IP
icmpInEchos	icmp	Numero de ICMP echos recebidos
tcpRtoMin	tcp	Tempo mínimo de retransmissão no TCP
tcpMaxconn	tcp	Numero máximo de conexões
tcpInSegs	tcp	Numero de segmentos TCP recebidos
udpInDatagrams	udp	Numero de datagramas UDP recebidos
egpInMsgs	egp	Numero de mensagens EGP recebidas

Considere a variável MIB de prefixo iso.org.dod.internet.mgmt.mib.ip.ipAddrTable (1.3.6.1.2.1.4.20) que contem uma lista dos endereços IP para cada interface de rede. Esse objeto é uma tabela unidimensional onde cada elemento é uma estrutura de cinco itens. O objetivo de colocar tal consideração é a de mostrar uma variável complexa dispondo apenas de seu endereço de entrada e exemplificar o uso da operação básica Get-next-request, que obtém todos os elementos da tabela.

ipAddrTable possui a seguinte notação em ASN.1:

ipAddrTable ::= SEQUENCE OF IpAddrEntry, onde

```
IpAddrEntry ::=SEQUENCE {
        ipAdEntAddr
        IpAddress.
        ipAdEntIfindex
        INTEGER.
        ipAdEntNetMask
        IpAddress.
        ipAdEntBcastAddr
        IpAddress.
        ipAdEntReasmMaxSize
        INTEGER (0..65535).
}
```

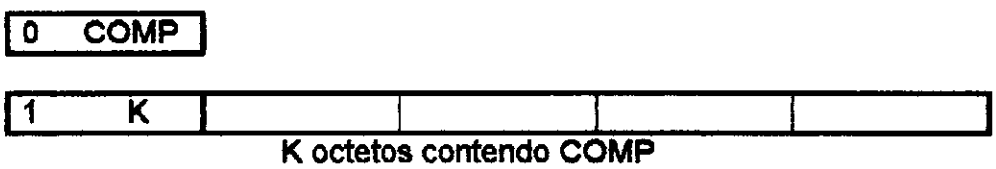
O exemplo pressupõe que IpAddress já foi definido anteriormente. Existem codificações adequadas para atribuir conteúdos a cada item de cada elemento, mas foge ao escopo do trabalho.

Quando foi comentado sobre o formato de uma mensagem trocada entre gerente e servidor faltou um exemplo elucidativo por falta de outras informações. Agora é um bom momento.

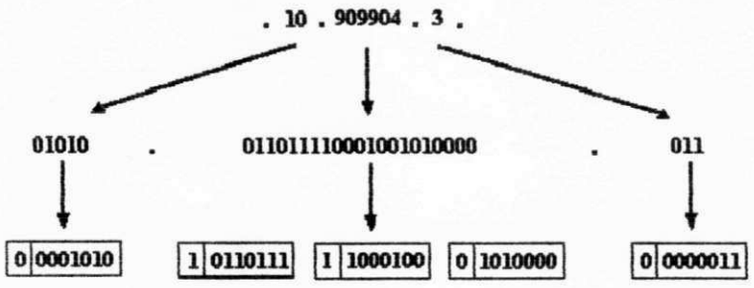
A figura abaixo exemplificar uma mensagem Get-request, onde os cinco primeiros octetos correspondem a versão, os próximos oito correspondem a community e os demais a PDU Get-request. Os octetos estão grafados em hexadecimal com seu significado logo abaixo. Os parênteses e os pontos são apenas para esclarecimento

30	29	02	01	00			
SEQUENCE	len=41	(INTEGER	len=1	vers=0)			
04	06	70	75	62	6C	69	63
(string	len=6	p	u	b	l	i	c)
A0	1C	02	04	05	AE	56	02
(get req.	len=28	(INTEGER	len=4		——— request id	———	)
02	01	00	02	01	00		
(INTEGER	len=1	status)	(INTEGER	len=1	error index)		
30	0E	30	0C	06	08		
(SEQUENCE	len=14	(SEQUENCE	len=12	(objectid	len=8		
2B	06	01	02	01	01	01	00
1.8	.6	.1	.2	.1	.1	.1	.0)
05	00						
null	len=0)))						

A codificação adotada para o comprimento de um item de dado obedece a codificação ASN.1. O SNMP especifica que se o comprimento do item de dado for menor que 128, a codificação é feita em um único octeto com o bit de mais alta ordem em zero e os demais bits contendo o valor. Caso o comprimento seja igual ou maior que 128, o primeiro octeto possui o bit de mais alta ordem com valor 1 e os demais sete bits indicando quantos octetos seguem contendo o valor do item de dado.



Codificação semelhante ainda segundo ASN.1, é utilizada para identificador de objeto. Caso o identificador seja menor que 128 segue o padrão do parágrafo anterior. Em caso contrario, são utilizados tantos quantos octetos sejam necessários, e em cada um deles são utilizados apenas os sete bits de mais baixa ordem, ficando o bit de mais alta ordem colocado em 0 no ultimo octeto e em 1 nos demais.



CONCLUSÕES

O modelo gerenciamento TCP/IP é centralizado mas de processamento distribuído modelado a objetos. Em termos de implementação significa dividir o "software" em módulos, cada um apresentado interfaces bem definidas para os outros módulos. Adicionalmente implementa aspectos próprios do domínio do problema. Uma aplicação de gerência que utilize algum dos módulos, só necessita conhecer a semântica da interface. Melhorias posteriores nos módulos na afeta a aplicação. Isso também é válido para inclusão de novos módulos.

A MIB é conceitual por ser abstrata, é distribuída por permitir que atributos seus sejam um item de dado de um "software" ou o registrador de um equipamento de comunicação. É instantânea por não registrar a história da gerência.

A MIB como definida não permite identificar instâncias de uma mesma classe de objetos mas apenas tipos de objetos.

A MIB não inclui informações de gerenciamento para aplicações tais como acesso a terminais remotos (TELNET), transferência de arquivo (FTP "File Transfer Protocol") e correio eletrônico.

BIBLIOGRAFIA

CARVALHO, T.C.M.Brito, et al. **Gerenciamento de redes - Uma abordagem de sistemas abertos**. 1.ed. São Paulo: Makron Books do Brasil, 1993. 364p.

COMER, Douglas E., STEVENS, David L. **Internetworking with TCP/IP**. 1.ed. New Jersey: Prentice-Hall, Inc., 1991. vol.1 e 2.

MARTINS, Joberto S.B. **Arquiteturas de redes de computadores e protocolos de comunicação**. Campina Grande:Pós-Graduação em Informática da UFPB, 1993. 400p. (Notas de aula).