Gerenciamento de Redes e Interconexões

Prof. Marcos Monteiro, MBA

http://www.marcosmonteiro.com.br

contato@marcosmonteiro.com.br

Porque gerenciar?

- Controlar a complexidade
  - Dimensao da rede
- Melhorar a qualidade de serviço
  - Detectar gargalos, aumentar estabilidade
- Balancear necessidades
  - Segurança, desempenho, recursos, serviços...
- Reduzir tempo de manutenção
  - Eliminar fragilidades, criar redundâncias
- Controlar custos
  - contabilização

O que gerenciar?

- Controle de acesso à rede
- Disponibilidade e desempenho
- Documentação de Configuração
- Gerencia de Mudanças
- Planejamento de capacidade
- Auxilio ao usuário
- Gerencia de Problemas
- Controle de Inventários

Gerência de redes

- Segundo Pujolle:

"a gerência de redes corresponde as ações que permitem gerenciar a configuração, a segurança, as panes, as medições da performance e da contabilização".

Quando nasceu

- A definição de um sistema de gerência para a industria do setor das telecomunicações foi iniciada em 1985 pelo CCITT (Consultative Committee for International Telegraph and Telephone).

- ISO (International Standards Organization) acrescentou em 1989 ao modelo de referencia OSI (Open Systems Interconnection) de sete camadas uma arquitetura de gerência de redes.

ISO-OSI/MN

- Modelo Organizacional – hierarquia de sistemas de gerencia de domínios de gerencia.
- Modelo Informacional – Define os objetos de gerencia e suas relações, é necessário para armazenar os objetos.
- Modelo Funcional – Descreve as funcionalidades de gerencia:
    - Gerencia de falhas;
    - Gerencia de configuração;
    - Gerencia de desempenho;
    - Gerencia de contabilização;
    - Gerencia de segurança.

Gerência OSI

- Gerencia de falhas
  - detectar, isolar e corrigir falhas ou funcionamento anormal dos diversos dispositivos componentes do sistema de comunicação (ou da rede).

As falhas devem ser detectadas antes que seus efeitos sejam percebidos.

Gerência de Falhas

- Os procedimentos característicos das aplicações para gerência de falhas são:
  - detecção e informação da ocorrência de falhas, utilizando um protocolo padrão para geração e comunicação de eventos;
  - manutenção de um registro de todos eventos reportados, processando e organizando estes eventos em diversos níveis de severidade;
  - Como resultado da análise do registro de eventos mantidos, realizar inferências sobre o sistema gerenciado, rastreando falhas e realizando ações para corrigi-las e tentar evitar novas ocorrências.

Gerência de Contabilização

A gerência de contabilização provê meios para se medir e coletar informações a respeito da utilização dos recursos e serviços de uma rede, para saber qual a taxa de uso destes recursos garantindo que os dados estejam sempre disponíveis quando forem necessários.

A função de contabilização é usada para finalidades como tarifas sobre serviços prestados, controle de consumo dos usuários, etc.

Gerência de Configuração

- definição, obtenção e alteração dos parâmetros de configuração dos dispositivos gerenciados;
- definição e alteração dos relacionamentos entre os diversos dispositivos da rede;
- distribuição e atualização de software;
- configuração local ou remota.

Gerência de segurança

- A área de gerência de segurança oferece suporte ao monitoramento e controle de acesso, autorização e autenticação de máquinas e usuários e geração e análise de registros de segurança.
- As principais funções desta área são:
  - Controle de acesso aos recursos;
  - Armazenamento e recuperação das informações de segurança;
  - Gerência e controle dos processos de segurança tais como senhas, criptografia, chaves públicas e privadas, etc.

Gerência de Desempenho

- Área funcional compreendendo o conjunto das funções associadas com a avaliação de desempenho dos diversos componentes da rede de comunicação.

- Seu objetivo principal é o monitoramento constante do sistema e de seus componentes, coletando dados para análise de comportamento.

Gerência de Desempenho

- As três principais fontes geradoras de baixo
- desempenho são:
  - falhas de componentes: neste caso o gerente humano deve utilizar ferramentas de gerência de falhas, a fim de detectar e corrigir os componentes de hardware ou software com problemas.
  - Elevadas cargas de utilização: os mecanismos de gerência de contabilização permitem ao gerente determinar qual dispositivo e usuário estão gerando a carga elevada;
  - erros de configuração: através de ferramentas de Gerência de Configuração é possível reconfigurar os dispositivos mal configurados, que estão prejudicando o desempenho do sistema.

Gerência de Desempenho

- Indicadores de Desempenho
  - Orientados a Serviço
    - Disponibilidade
      - A disponibilidade pode ser expressa pelo tempo que a rede, componente ou aplicação está disponível para o usuário. Dependendo da aplicação, alta disponibilidade pode ser significativa (em uma rede bancária, uma hora sem a rede pode produzir prejuízos de milhões).
      - A disponibilidade é baseada na confiabilidade doscomponentes individuais da rede.
      - Confiabilidade é a probabilidade que um componente irá cumprir sua função específica por um tempo específico. A falha de componentes é normalmente expressa pelo Mean Time Between Failures (MTBF), que é o tempo entre falhas.

- Tempo de Resposta
  - É o tempo que leva para um sistema reagir a uma determinada entrada.
  - Em um sistema interativo é o tempo que leva para o usuário digitar a tecla e esta aparecer no terminal.
  - É o tempo que leva para um sistema responder a uma requisição a fim de efetuar uma determinada tarefa.
- O tempo total de resposta é composto de quatro elementos principais:
  - tempo de processamento do nó: é o tempo que leva para que o nó analise o dado a ser enviado e defina o caminho a ser seguido;
  - tempo de enfileiramento: o tempo requerido para o processamento nas filas de espera. Quanto maior o número de mensagens colocadas na fila, maior é o tempo de enfileiramento, ou seja, depende do tráfego da rede;
  - tempo de transmissão: o tempo para que todos os bits de um pacote sejam transmitidos para o enlace de comunicação ;
  - tempo de propagação: é o tempo que leva para a transmissão no enlace de comunicação, dependendo exclusivamente da propagação do enlace.

- Exatidão
  - A exatidão não é normalmente uma preocupação do usuário, pois existem os mecanismos de correção de erros embutidos em protocolos como os de enlace e transporte.
  - Porem é útil monitorar os parâmetros da rede, tal como a taxa de erros. Isso pode dar uma indicação de uma linha de comunicação defeituosa ou a existência de uma fonte de ruído ou interferência que deve ser corrigida.

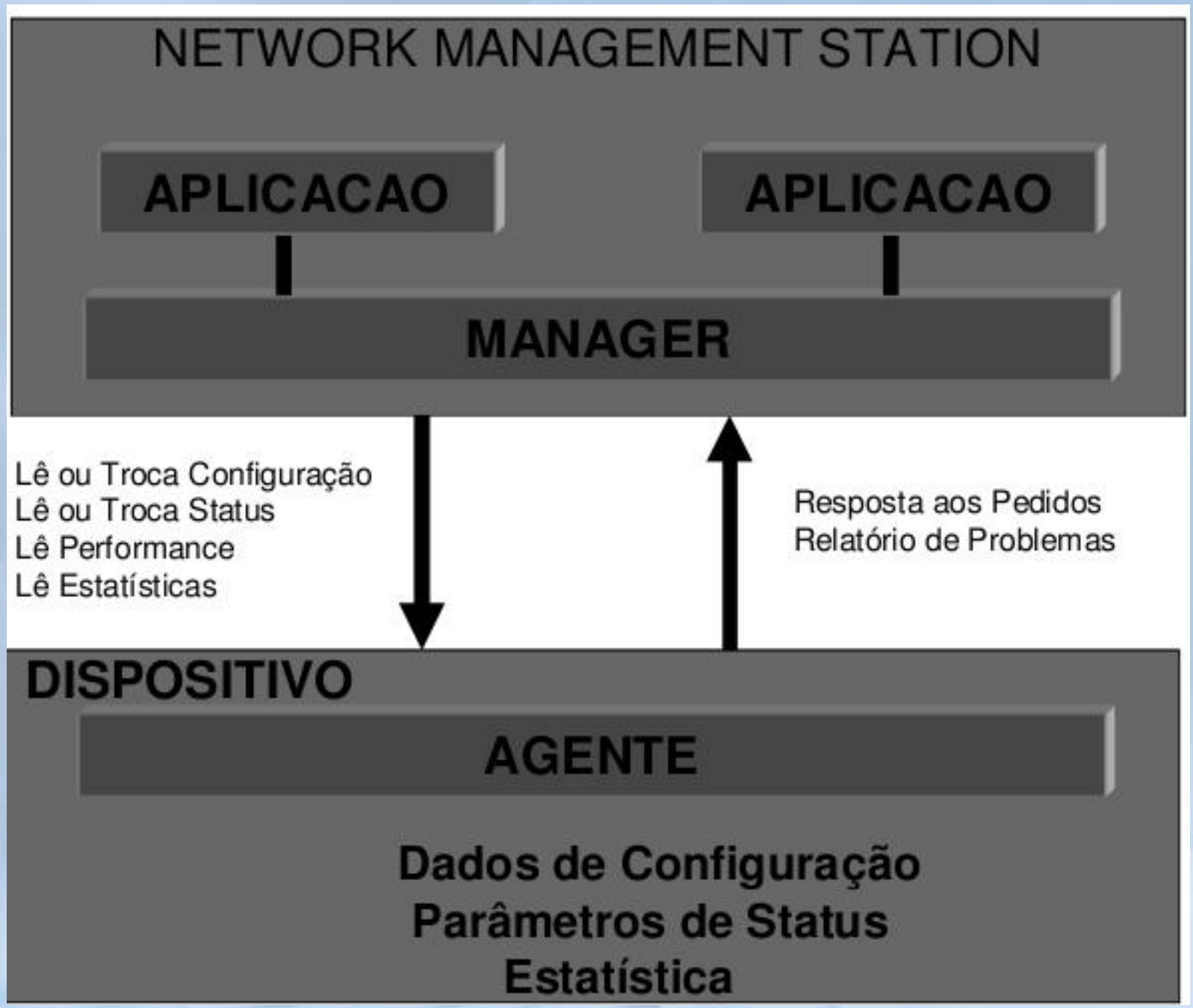
– Orientados a Eficiência

- Throughtput
  - A taxa efetiva na qual eventos orientados a aplicações ocorrem.
- Utilização
  - A utilização consiste na porcentagem de tempo que um recurso está em uso sobre um determinado período de tempo.

- Utilização
  - A utilização da rede é usada na determinação de potenciais “gargalos” e áreas de congestionamento.
  - Como o tempo de resposta aumenta exponencialmente conforme a utilização dos recursos aumenta, congestionamentos podem sair de controle se não forem visualizados cedo e tratados rapidamente.
  - Analisando a utilização da rede, um analista pode verificar recursos disponíveis a um determinado momento e ajustar a rede de acordo.

Modelo de Gerência

- Modelo composto de um “manager” e de um agente.
  - O manager (gerente) é SOFTWARE instalado em uma estação de gerência. Sua função e permitir a analise dos dispositivos da rede, atualizar configurações e informações de status.
  - O agente é um SOFTWARE instalado em cada dispositivo da rede. Ele recebe do gerente mensagens de escrita ou leitura de dados relacionados ao dispositivo. O agente recebe as mensagens e envia a resposta ao gerente.


NETWORK MANAGEMENT STATION
APLICACAO
APLICACAO
MANAGER
Lê ou Troca Configuração
Lê ou Troca Status
Lê Performance
Lê Estatísticas
Resposta aos Pedidos
Relatório de Problemas
DISPOSITIVO
AGENTE
Dados de Configuração
Parâmetros de Status
Estatística

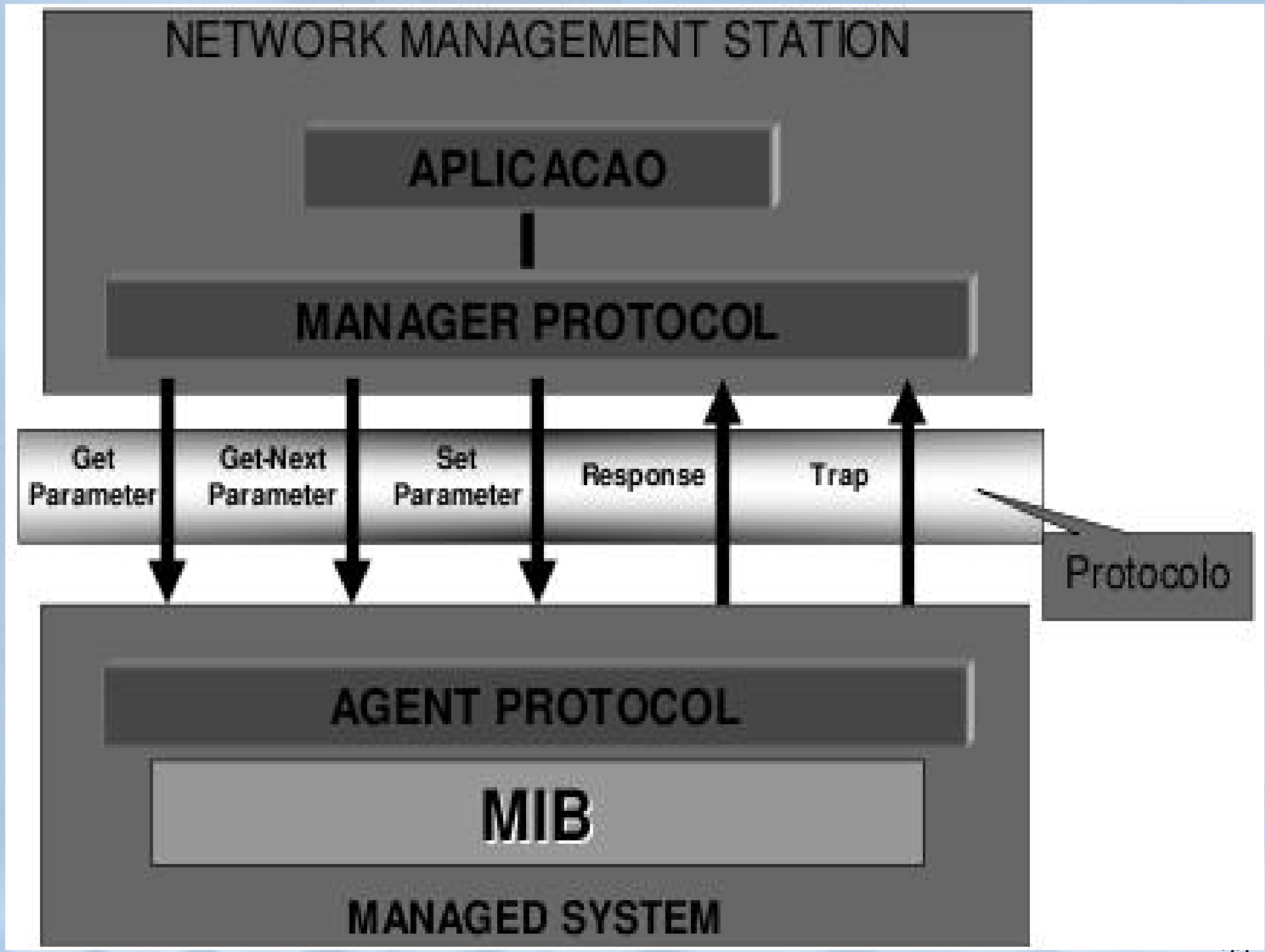
Network Management Application

- Aplicação não normalizada.
  - A cada fabricante de estações de gerencia compete a implementação da aplicação.
- Essas aplicações permitem ao gerente:
  - Obter o mapeamento da LAN (todos os dispositivos conectados)
  - Imprimir relatórios gráficos do trafico da rede.
  - Configurar seus próprios parâmetros tais como respostas a determinados eventos, relatórios específicos, mensagens de outras aplicações.

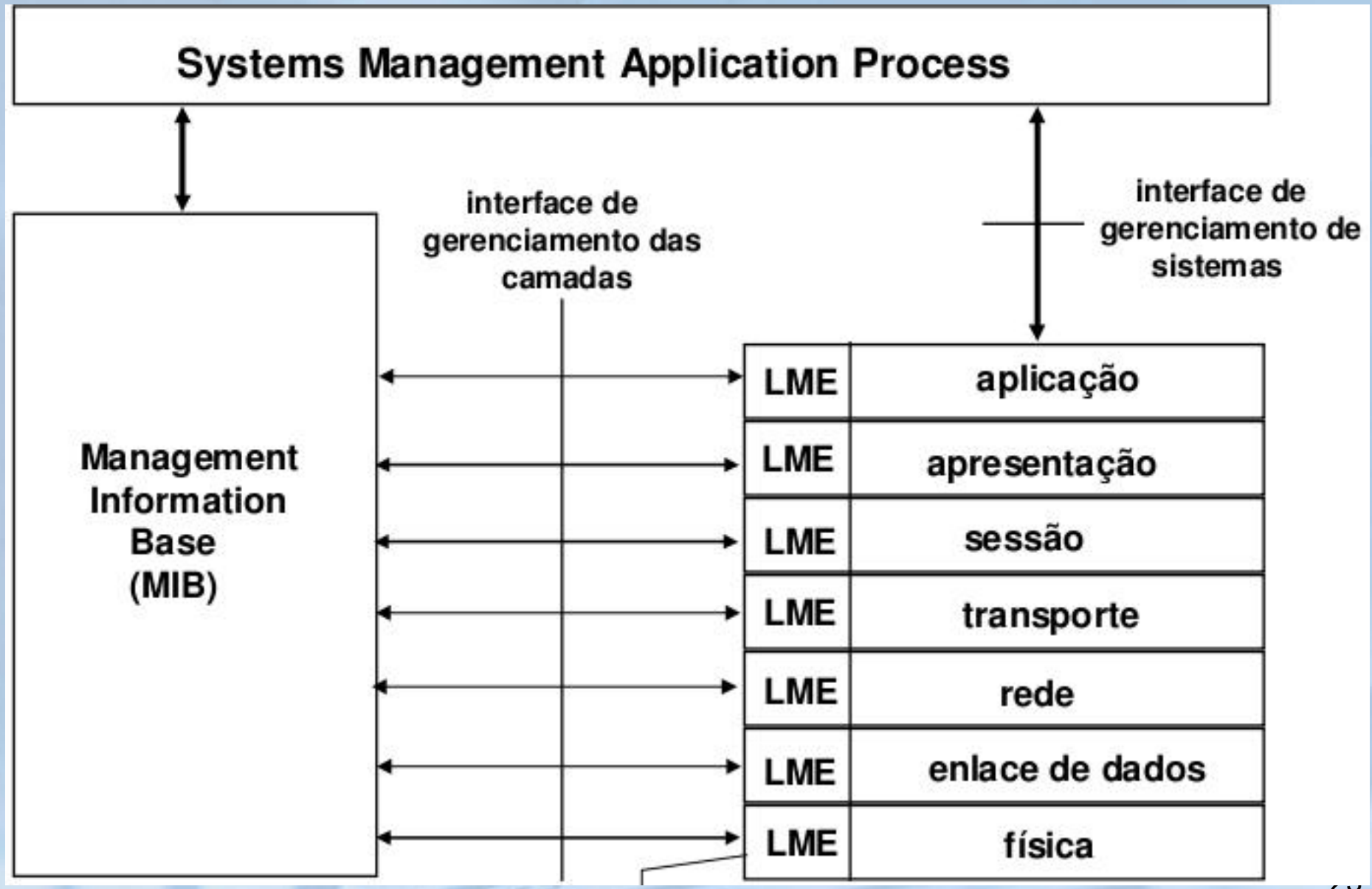
Protocolos de Gerência

- SNM Protocol
  - SNMP é o protocolo utilizado para permitir a troca de informações de gerência entre o gerente e o agente.
- SNM Informations
  - As informações a serem gerenciadas podem ser armazenadas num dispositivo como:
    - combinação de chaves,
    - Valores,
    - Contadores,
    - variáveis de memórias,
    - tabelas ou arquivos.

Isso pode ser considerado como uma database (base de dados) e é chamada MIB.


NETWORK MANAGEMENT STATION
APLICACAO
MANAGER PROTOCOL
Get Parameter
Get-Next Parameter
Set Parameter
Response
Trap
Protocolo
AGENT PROTOCOL
MIB
MANAGED SYSTEM

Arquitetura de Gerenciamento



MIB
Management Information Base

- Um sistema de gerenciamento necessita de uma base de dados sobre os recursos e elementos gerenciados. Em OSI esta base de dados se chama de MIB.
- Uma MIB é definida usando-se regras gerais sobre dados e recursos chamadas de SMI (Structure of Management Information).
- A SMI determina os tipos de dados que podem fazer parte da MIB e determina a representação e nomes de recursos.

MIB (Management Information Base)

- MIB I
- MIB II

informações gerais sobre o equipamento sem características especificas de cada: status da interface, numero de pacotes transmitidos e perdidos e informações dos protocolos de transmissão, etc.

- MIB Experimental
- MIB Privada

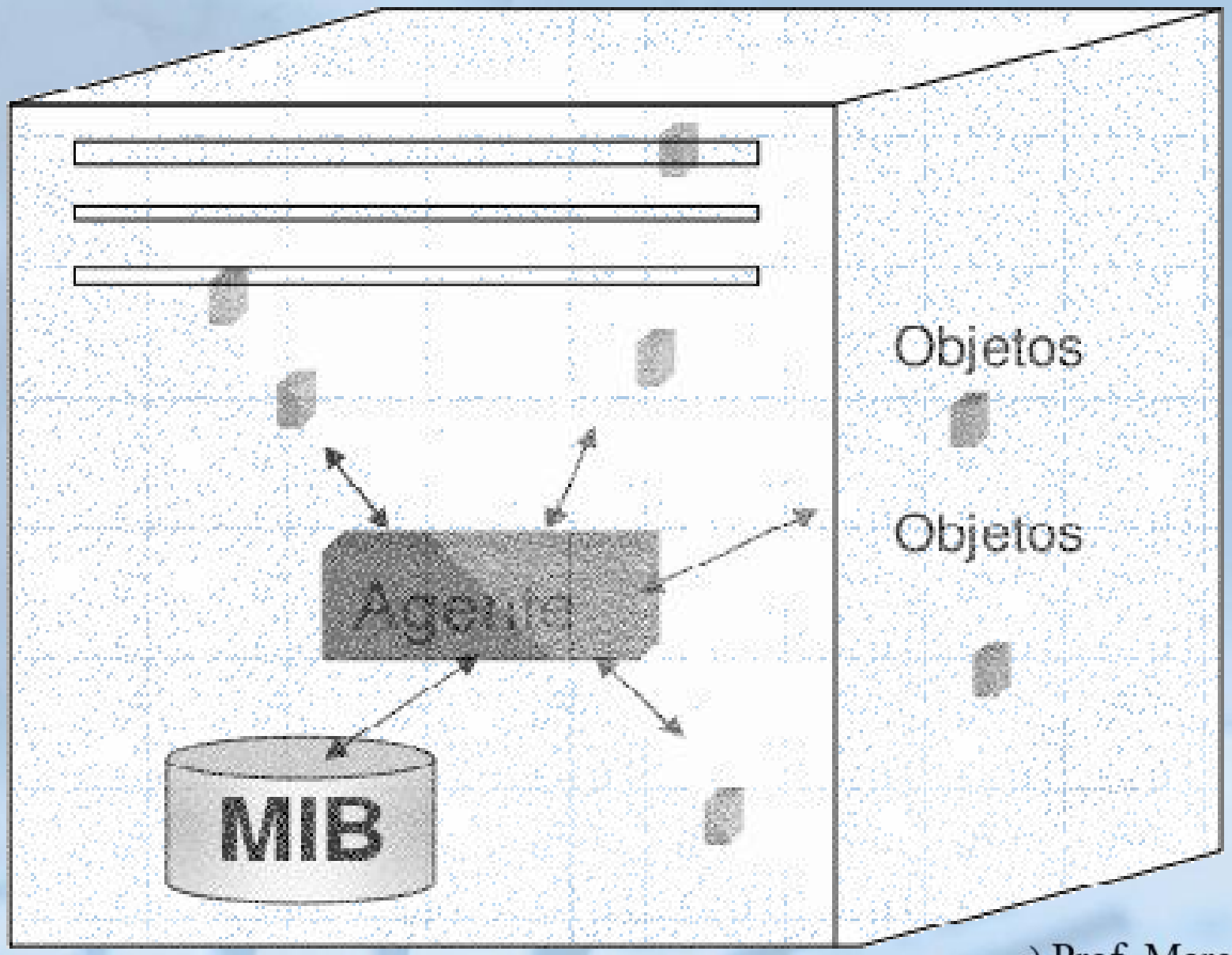
Especificas do equipamento- colisões, configurações, reboot, desabilitar porta de um hub por exemplo.

Permite uma gerencia maior

Managed Objects (Objetos)

- Cada recurso monitorado ou controlado é representado por um objeto gerenciado
- A MIB é uma coleção estruturada de objetos
  - exemplos de objetos:
    - hardware: comutadores, roteador
    - software: algoritmos de roteamento, filas
  - objetos são
    - específicos a uma camada: objetos da camada (N)
    - não-específicos a uma camada: objetos do sistema

Objetos



Estrutura dos Objetos

- Um objeto é definido por seus atributos, operações, atributos, operações, notificações e relações com outros objetos
- Cada objeto é uma instância de uma classe de objetos gerenciados.
- A comunidade de gerencia de redes usa o termo OBJECT para instanciar uma variável ou objeto de gerência.

Estrutura dos Objetos

- Um objeto é visto como:
  - Um nome único: OBJECT IDENTIFIER
  - Atributos:
    - tipo de dados,
    - descrição (incluindo detalhes para a implementação),
    - informações de status.
  - Operações validas que podem ser realizadas (read, write, set)

Denominação dos Objetos

- ISO e CCITT usam a idéia de uma arvore hierárquica para definir a estrutura lógica de uma MIB.
- O nome de cada objeto esta registrados na árvore de nomes OSI.
- Um identificador (inteiro) é associado a cada objeto.
- O nome de um objeto é uma seqüência de inteiros derivada do caminho da raiz da árvore até o nó correspondente à classe do objeto.

Object IDentifier (OID)

- Example .1.3.6.1.2.1.1
- iso(1)
- org(3)
- dod(6)
- internet(1)
- mgmt(2)
- mib-2(1)
- system(1)

Grupo de Informações MIB-2(RFC 1312)

• system (1)	inf. básicas do sistema
• interfaces (2)	interfaces de rede
• at (3)	tradução de endereços
• ip (4)	protocolo ip
• icmp (5)	protocolo icmp
• tcp (6)	protocolo tcp
• udp (7)	protocolo udp
• egp (8)	protocolo egp
• transmission (10)	meios de transmissão
• snmp (11)	protocolo snmp

Grupo System (1.3.6.1.2.1.1)

- sysDescr (1.3.6.1.2.1.1.1): Descrição textual da unidade. Pode incluir o nome e a versão do hardware, sistema operacional e o programa de rede.
- sysObjectID (1.3.6.1.2.1.1.2): Identificação do fabricante
- sysUpTime (1.3.6.1.2.1.1.3): Tempo decorrido (em milhares de segundos) desde a última reinicializarão do gerenciamento do sistema na rede.
- sysContact (1.3.6.1.2.1.1.4): Texto de identificação do gerente da máquina gerenciada e como contactá-lo.
- sysName (1.3.6.1.2.1.1.5): “fully-qualified domain name”
- sysLocation (1.3.6.1.2.1.1.6): Localização física da entidade
- sysServices (1.3.6.1.2.1.1.7): Valor indicando o conjunto de serviços oferecidos pela maquina.

Grupo Interfaces (1.3.6.1.2.1.2)

- ifNumber (1.3.6.1.2.1.2.1): Número de interfaces de rede presentes no sistema.
- ifDescr (1.3.6.1.2.1.2.2.1.2): Descrição da interface (nome, fabricante, ...)
- ifType (1.3.6.1.2.1.2.2.1.3): Informação sobre o tipo de interface
- ifMtu (1.3.6.1.2.1.2.2.1.4): Tamanho maximo do datagrama na interface.
- ifSpeed (1.3.6.1.2.1.2.2.1.5): Banda passante nominal da interface
- ifPhysAddress (1.3.6.1.2.1.2.2.1.6): Endereço da camada de enlace da interface.
- ifAdminStatus (1.3.6.1.2.1.2.2.1.7): Estado atual da administração da interface (“up” ou “down”).
- ifOperStatus (1.3.6.1.2.1.2.2.1.8): Estado atual da interface.

Grupo Interfaces (1.3.6.1.2.1.2)

- ifInOctets (1.3.6.1.2.1.2.2.1.10): Número total de Bytes recebidos pela interface.
- ifInDiscards (1.3.6.1.2.1.2.2.1.13): Número total de pacotes (recepção) descartados pela interface .
- ifInErrors (1.3.6.1.2.1.2.2.1.14): Número total de pacotes recebidos com erros pela interface.
- ifOutOctets (1.3.6.1.2.1.2.2.1.16): Número total de bytes transmitidos pela interface.
- ifOutDiscards (1.3.6.1.2.1.2.2.1.19): Número total de pacotes (transmissão) descartados pela interface.
- ifOutErrors (1.3.6.1.2.1.2.2.1.20): Número total de pacotes não transmitidos devido a erros.

Grupo IP (1.3.6.1.2.1.4)

- ipForwarding (1.3.6.1.2.1.4.1): Indica se esta entidade é um gateway.
- ipDefaultTTL (1.3.6.1.2.1.4.2): O valor default do campo Time-To-Live do cabeçalho do pacotes.
- ipInReceives (1.3.6.1.2.1.4.3): Número total de datagramas recebidos pelas interfaces, incluindo os recebidos com erro.
- ipInHdrErrors (1.3.6.1.2.1.4.4): Número de datagramas que foram recebidos e descartados devido a erros no cabeçalho IP.
- ipInDiscards (1.3.6.1.2.1.4.8): Numero de datagramas recebidos e descartados.

Grupo ICMP (1.3.6.1.2.1.5)

- icmpInMsgs (1.3.6.1.2.1.5.1): Número total de mensagens ICMP recebidas por esta entidade, incluindo aquelas com erros.

- icmpOutMsgs (1.3.6.1.2.1.5.14): Número total de me nsagens ICMP enviadas por esta entidade, incluindo aquelas com erros.

Grupo TCP (1.3.6.1.2.1.6)

- tcpMaxConn (1.3.6.2.1.6.4): Número máximo de conexões TCP que esta entidade pode suportar.
- tcpCurrentEstab (1.3.6.2.1.6.9): Número de conexões TCP que estão como estabelecidas ou a espera de fechamento.
- tcpRetransSegs (1.3.6.2.1.6.12): Número total de segmentos retransmitidos.

Grupo UDP (1.3.6.1.2.1.7)

- udpInDatagrams (1.3.6.1.2.1.7.1): Número total de datagramas UDP entregues aos usuários UDP.
- udpNoPorts (1.3.6.1.2.1.7.2): Número total de datagramas UDP recebidos para os quais não existia aplicação na referida porta.
- udpLocalPort (1.3.6.1.2.1.7.5.1.2): Número da porta do usuário UDP local

Grupo SNMP (1.3.6.1.2.1.11)

- snmpInPkts (1.3.6.1.2.1.11.1): Número total de mensagens recebidas pela entidade SNMP.
- snmpOutPkts (1.3.6.1.2.1.11.2): Número total de mensagens enviadas pela entidade SNMP.
- snmpInTotalReqVars (1.3.6.1.2.1.11.13): Número total de objetos da MIB que foram resgatados pela entidade SNMP.

RMON - Remote Network Monitoring

- Dispositivos para monitoramento remoto de redes são chamados de “monitor” ou “probe”.
- São usados no gerenciamento de redes.
- A MIB RMON defines objetos de gerencia para os dispositivos remotos de monitoramento de redes.

Grupos da RMON

- – Statistics OBJECT IDENTIFIER ::= { rmon 1 }
- – History OBJECT IDENTIFIER ::= { rmon 2 }
- – Alarm OBJECT IDENTIFIER ::= { rmon 3 }
- – Hosts OBJECT IDENTIFIER ::= { rmon 4 }
- – hostTopN OBJECT IDENTIFIER ::= { rmon 5 }
- – Matrix OBJECT IDENTIFIER ::= { rmon 6 }
- – Filter OBJECT IDENTIFIER ::= { rmon 7 }
- – Capture OBJECT IDENTIFIER ::= { rmon 8 }
- – Event OBJECT IDENTIFIER ::= { rmon 9 }

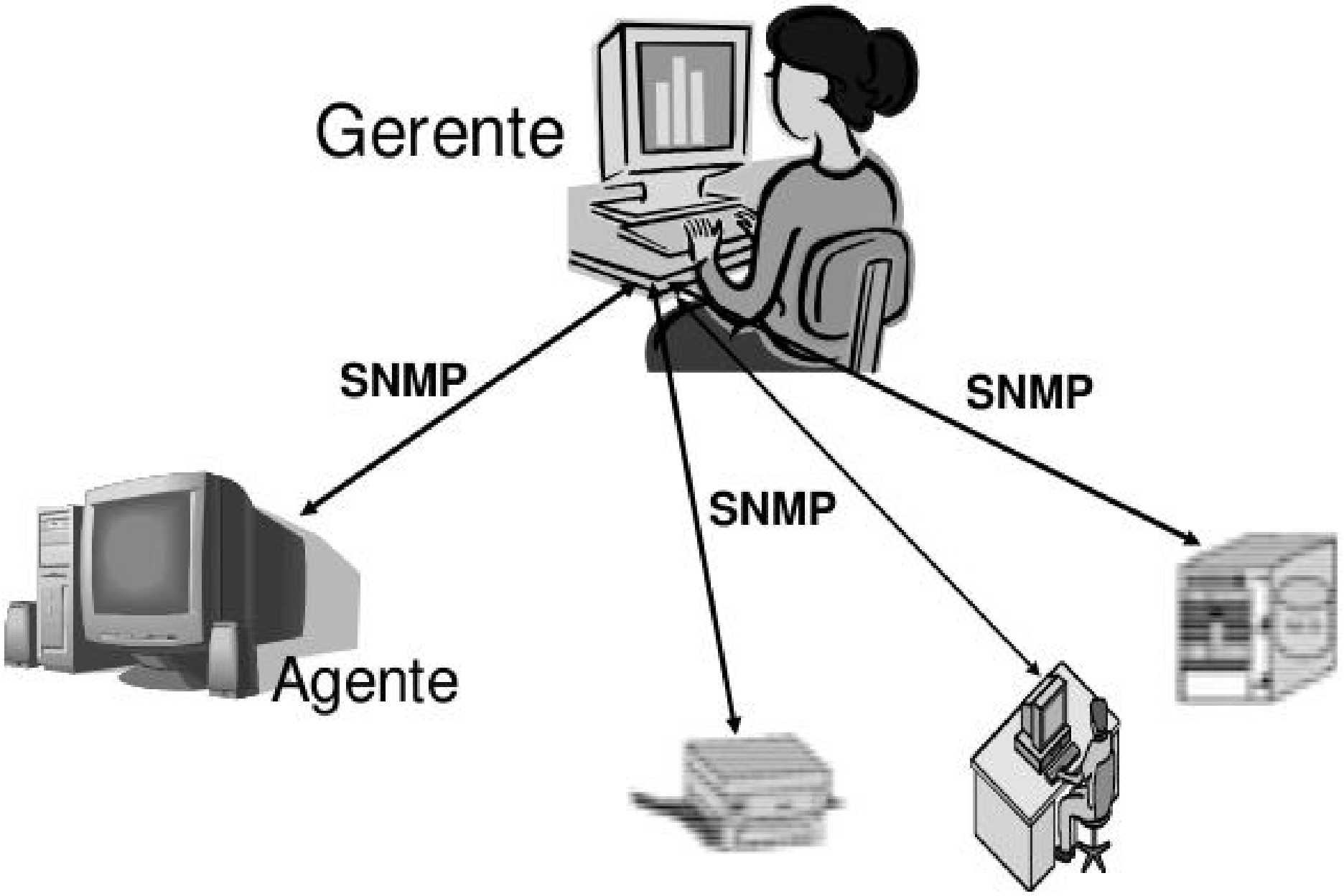
SNMP - Simple Network Management Protocol

- Especificado na RFC 1157.
- Protocolo de gerência, baseado na pilha de protocolos TCP/IP.
- Definido no nível de aplicação.
- Utiliza o protocolo de transporte UDP- User Datagram Protocol.
- Utilizado para troca de informações entre managers e clientes SNMP.

Protocolo SNMP

- O funcionamento do SNMP é baseado em dois dispositivos o agente e o gerente.
- Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual.
- Essas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele.
- Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

Modelo SNMP



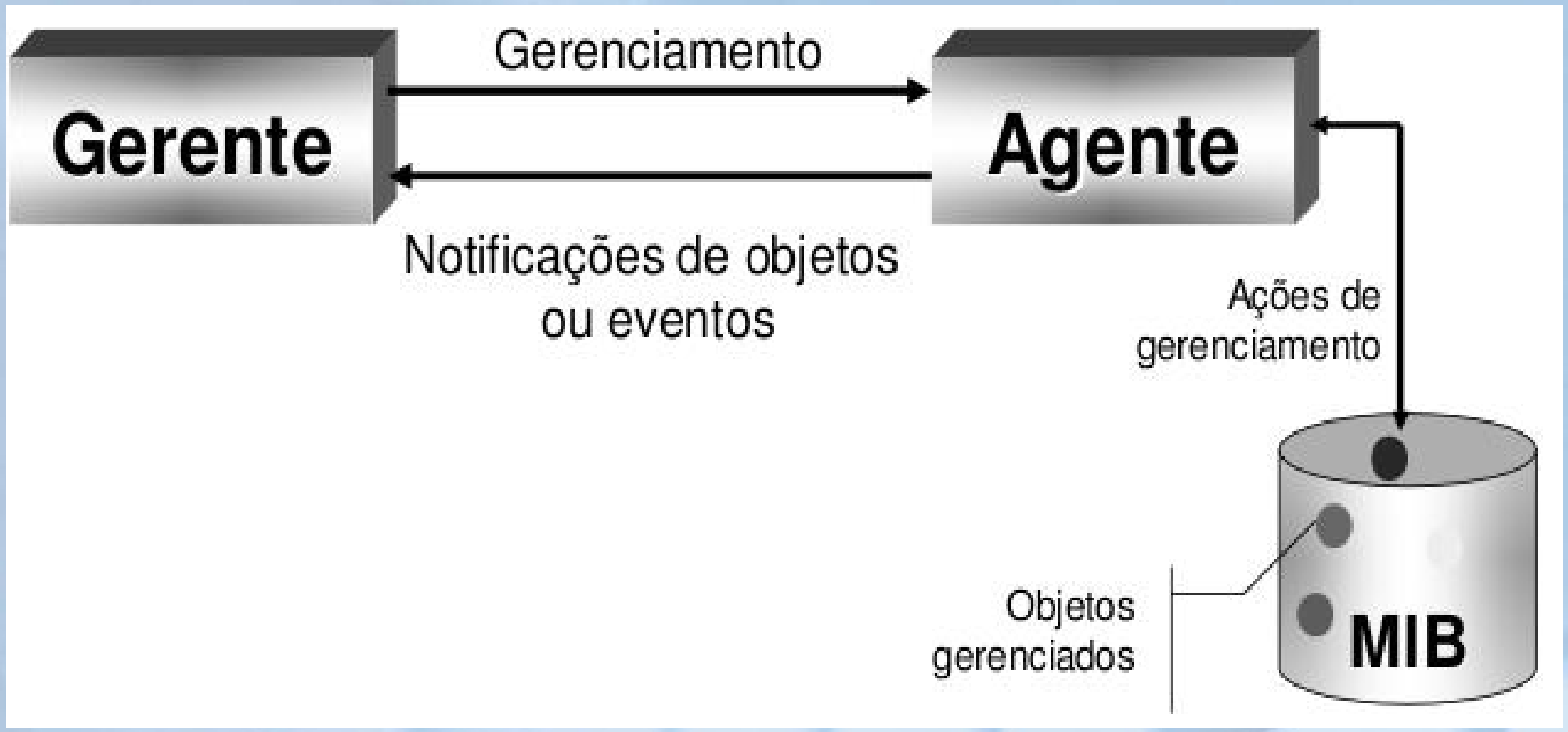
O Agente

- É um “software” executado na máquina gerenciada, responsável pela manutenção das informações de gerência da máquina. As funções principais de um agente são:
  - Atender as requisições enviadas pelo gerente;
  - Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado;
- O agente utiliza as chamadas de sistema para realizar o monitoramento das informações da máquina e utiliza as RPC (Remote Procedure Call) para o controle das informações da máquina.

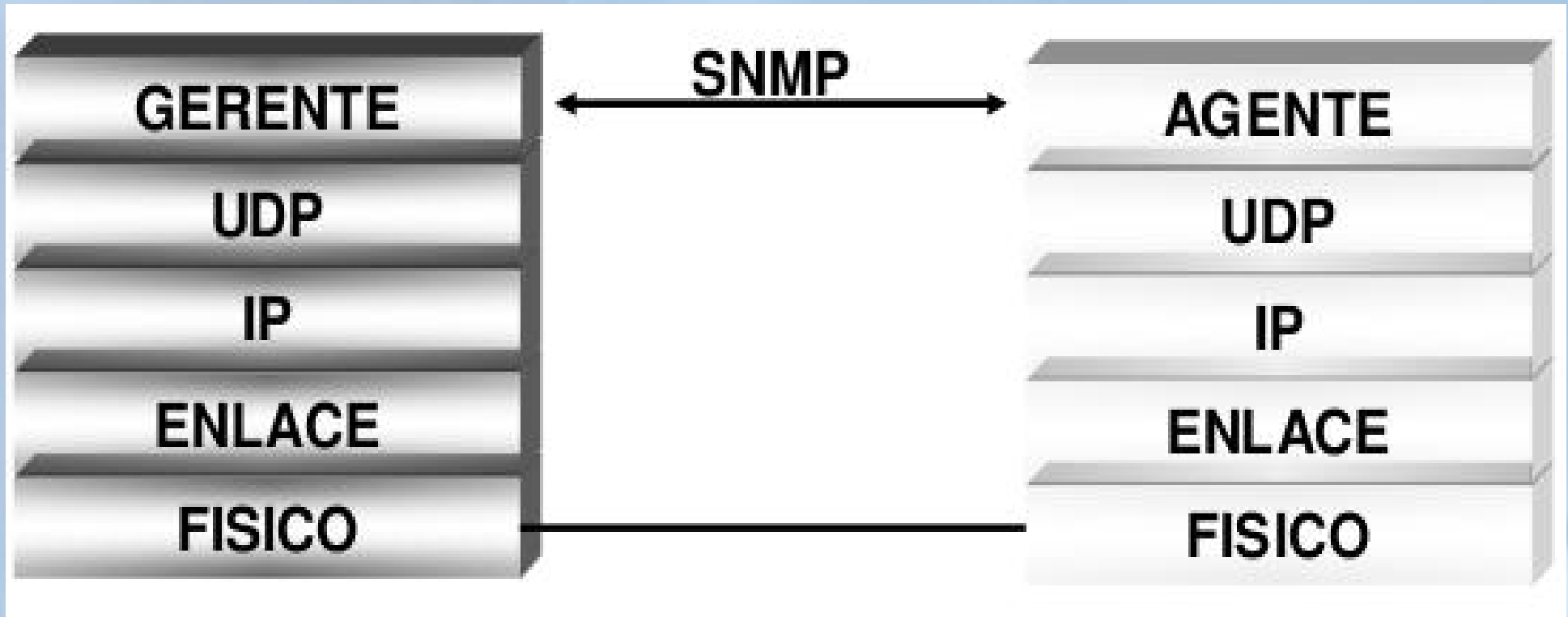
O Gerente

- É um “software” permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes.
- É executado em uma estação servidora.
- O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas.

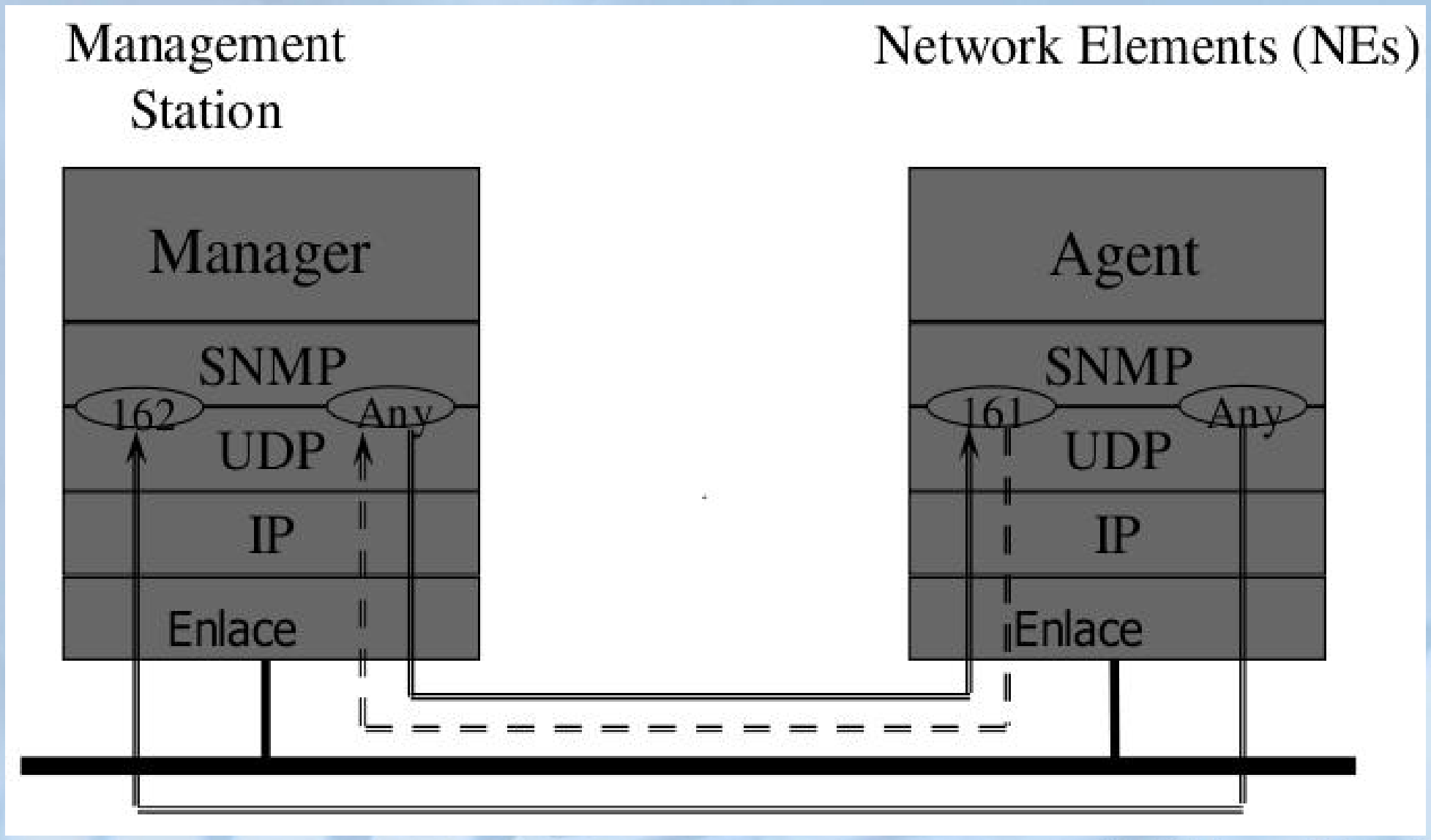
Relacionamento de um gerente com o objeto gerenciado.



Relacionamento entre gerente e agente baseado no modelo TCP/IP



Portas UDP



;) Prof. Marcos Monteiro

Comandos do SNMP

- GetRequest, ou Get
  - A operação mais comum.
  - Usada para interrogar o agente SNMP sobre o valor de uma determinada variável da MIB.
- GetNextRequest, ou GetNext
  - Utilizada para ler o valor da próxima variável; o gerente fornece o nome de uma variável e o cliente obtém o valor e o nome da próxima variável;
  - Também é utilizado para obter valores e nomes de variáveis de uma tabela de tamanho desconhecido.
- SetRequest [Set]
  - A operação SET é enviada pelo gerente para solicitar ao agente a alteração do valor de uma determinada variável da MIB

Comandos do SNMP

- GetResponse [Response]
  - Simples resposta a um Get, GetNext or Set.
- Trap
  - Notificação Assíncrona
  - O agente SNMP pode ser programado para enviar uma mensagem Trap quando um certo conjunto de circunstancia vierem a acontecer.
  - Circunstancias podem ser eventos, “thresholds”, etc.

Communities

- Publico (GET)
- Privada (SET)

Mensagem no Protocolo SNMP

- Uma mensagem possui três partes principais:
  - Version:
    - Contem a versão do SNMP.
    - Tanto o gerente como o agente devem utilizar a mesma versão.
  - Community :
    - Identifica a comunidade.
    - É utilizada para permitir acesso do gerente as MIBs.
  - SNMP PDU
    - O PDU (Protocol Data Units) contem os dados da mensagem, sendo constituído do pedido ou da resposta a um pedido.

Campos da PDU

- Type: O campo PDU Type indica o tipo de PDU utilizada.
- Request ID: é utilizado para identificar a requisição. O mesmo valor é utilizado como resposta a esta mensagem.
- Error Status: é utilizado para identificar uma situação inesperada ou erro que acontece durante o processamento da mensagem.
- Error Index: indica qual variável da lista causou o erro.
- Variable Bindings: possui uma lista de variáveis e seus respectivos valores.

Mensagem no Protocolo SNMP

Versio	Community	Type	Request ID	Error Status	Error Index	Variable Bindings

TCP/IP

- SNMP (Simple Network Management Protocol) 1990 – não proprietário, público e fácil, permite gerenciar um ambiente heterogêneo.

- O SNMPv2
  - Proposto para resolver certos pontos fracos do SNMPv1 (versão 1).
- O SNMPv3
  - foi proposto para introduzir mecanismos de segurança na versão 2.

SNMP Commands

- snmpget [options] node variable [...]
  - SNMP Get request
- snmpnext [options] node variable [...]
  - SNMP GetNext request
- snmpwalk [options] node variable
  - solicitação repetitiva usando SNMP GetNext/GetBulk
- snmptrap [-d] [-p port] [-c community] node enterprise agent-addr generic-trap specific-trap time-stamp variable type value [variable type value...]
  - SNMP Version 1 Trap

Integrador de sistemas de Gerenciamento

Soluções Proprietárias

- NetView – IBM
- Accumaster – AT&T
- Allink – Nynex
- SunNet Manager – Sun

Softwares Livres

MRTG

NAGIOS

CACTI

Algumas ferramentas e comandos

- Tcpdump ou Ethereal
- Ipscan e portscan
- Nbtstat
- Arp

Fontes:

- Livros:
  - Windows NT SNMP
    - James Murray, O'Reilly Eds, 1998.
  - Managing Networks with SNMP, 2nd
    - ed Mark Miller, MIS Press, 1997.
  - SNMPv1, v2, v3 and RMON I and II, STALLINGS,
    - Willian, Prentice-Hall, 1998.
  - Computer Networks,
    - TANEMBAUM, A., Prentice-Hall
- URLs:
  - http://smurfland.cit.buffalo.edu/NetMan
  - http://snmp.cs.twente.nl/General/snmp
  - http://www.nmf.org