Gerência de Redes de Computadores e de Telecomunicações

Profa. Elizabeth Sueli Specialski, Dra.

Elizabeth Sueli Specialski graduou-se em Matemática pela Pontifícia Universidade Católica do Rio Grande do Sul em 1978, obteve o título de Mestre em Ciências da Computação pela Universidade Federal do Rio Grande do Sul em 1981 e o título de Doutora em Engenharia pela Universidade Federal de Santa Catarina em março de 2000. É professora no nível Adjunto IV da Universidade Federal de Santa Catarina e vem atuando em pesquisa e formação na área de Redes de Computadores e de Gerência de Redes de Computadores e de Telecomunicações junto ao Departamento de Informática e de Estatística da UFSC nos cursos de Graduação em Computação e Pós-Graduação em Computação e em Engenharia de Produção. Seu desempenho é traduzido pela publicação de mais de 50 trabalhos em Congressos Nacionais e Internacionais, palestras convidadas e consultorias realizadas junto a empresas fornecedoras de produtos e serviços de telecomunicações.

Endereço para contato:

Prof. Elizabeth Sueli Specialski
Departamento de Informática e de Estatística
Universidade Federal de Santa Catarina
Campus Universitário — Trindade
88040-900 — Florianópolis — SC
Tel.: (048) 331-7513 / 331-9739 / 9972-4345
Fax: (048) 331-9566
E-mail: beth@inf.ufsc.br ou especialski@bol.com.br

Sumário

1 Necessidades de Gerenciamento

Por menor e mais simples que seja uma rede de computadores, precisa ser gerenciada, a fim de garantir, aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável.

À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle.

A adoção de um software de gerenciamento não resolve todos os problemas da pessoa responsável pela administração da rede. Geralmente o usuário de um software de gerenciamento espera muito dele e, conseqüentemente, fica frustrado quanto aos resultados que obtém. Por outro lado, esses mesmos softwares quase sempre são sub-utilizados, isto é, possuem inúmeras características inexploradas ou utilizadas de modo pouco eficiente. Para gerenciar um recurso, é necessário conhecê-lo muito bem e visualizar claramente o que este recurso representa no contexto da rede [Adams 97].

O investimento em um software de gerenciamento pode ser justificado pelos seguintes fatores [Harnedy 97]:

- As redes e recursos de computação distribuídos estão se tornando vitais para a maioria das organizações. Sem um controle efetivo, os recursos não proporcionam o retorno que a corporação requer.
- O contínuo crescimento da rede em termos de componentes, usuários, interfaces, protocolos e fornecedores ameaçam o gerenciamento com perda de controle sobre o que está conectado na rede e como os recursos estão sendo utilizados.
- Os usuários esperam uma melhoria dos serviços oferecidos (ou no mínimo, a mesma qualidade), quando novos recursos são adicionados ou quando são distribuídos.
- Os recursos computacionais e as informações da organização geram vários grupos de aplicações de usuários com diferentes necessidades de suporte nas áreas de desempenho, disponibilidade e segurança. O gerente da rede deve atribuir e controlar recursos para balancear estas várias necessidades.
- À medida que um recurso fica mais importante para a organização, maior fica a sua necessidade de disponibilidade. O sistema de gerenciamento deve garantir esta disponibilidade.
- A utilização dos recursos deve ser monitorada e controlada para garantir que as necessidades dos usuários sejam satisfeitas a um custo razoável.

1.1 Áreas Funcionais de Gerenciamento

Além desta visão qualitativa, uma separação funcional de necessidades no processo de gerenciamento foi apresentada pela ISO (International Organization for Standardization), como parte de sua especificação de Gerenciamento de Sistemas OSI. Esta divisão funcional foi adotada pela maioria dos fornecedores de sistemas de gerenciamento de redes para descrever as necessidades de gerenciamento: Falhas, Desempenho, Configuração, Contabilização e Segurança.

Gerenciamento de Falhas

Falhas não são o mesmo que erros. Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento. Uma falha normalmente é causada por operações incorretas ou um número excessivo de erros. Por exemplo, se uma linha de comunicação é cortada fisicamente, nenhum sinal pode passar através dela. Um grampeamento no cabo pode causar distorções que induzem à uma alta taxa de erros. Certos erros como por exemplo, um bit errado em uma linha de comunicação, podem ocorrer ocasionalmente e normalmente não são considerados falhas.

Para controlar o sistema como um todo, cada componente essencial deve ser monitorado individualmente para garantir o seu perfeito funcionamento. Quando ocorre uma falha, é importante que seja possível, rapidamente:

- Determinar o componente exato onde a falha ocorreu;
- Isolar o resto da rede da falha, de tal forma que ela continue a funcionar sem interferências;
- Reconfigurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou;
- Reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.

O impacto e a duração do estado de falha pode ser minimizado pelo uso de componentes redundantes e rotas de comunicação alternativas, para dar à rede um grau de "tolerância à falhas".

Gerenciamento de Contabilização

Mesmo que nenhuma cobrança interna seja feita pela utilização dos recursos da rede, o administrador da rede deve estar habilitado para controlar o uso dos recursos por usuário ou grupo de usuários, com o objetivo de:

- evitar que um usuário ou grupo de usuários abuse de seus privilégios de acesso e monopolize a rede, em detrimento de outros usuários;
- evitar que usuários façam uso ineficiente da rede, assistindo-os na troca de procedimentos e garantindo a desempenho da rede;
- conhecer as atividades dos usuários com detalhes suficientes para planejar o crescimento da rede.

O gerente da rede deve ser capaz de especificar os tipos de informações de contabilização que devem ser registrados em cada nodo, o intervalo de entrega de relatórios para nodos de gerenciamento de mais alto nível e os algoritmos usados no cálculo da utilização.

Gerenciamento de Configuração

O gerenciamento de configuração está relacionado com a inicialização da rede e com uma eventual desabilitação de parte ou de toda a rede. Também está relacionado com as tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e do status dos componentes durante a operação da rede.

Alguns recursos podem ser configurados para executar diferentes serviços como, por exemplo, um equipamento pode atuar como roteador, como estação de trabalho ou ambos.

Uma vez decidido como o equipamento deve ser usado, o gerente de configuração pode escolher o software apropriado e um conjunto de valores para os atributos daquele equipamento.

O gerente da rede deve ser capaz de, inicialmente, identificar os componentes da rede e definir a conectividade entre eles. Também deve ser capaz de modificar a configuração em resposta às avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou a fim de atender à necessidades dos usuários.

Relatórios de configuração podem ser gerados periodicamente ou em resposta às requisições de usuários.

Gerenciamento de Desempenho

O gerenciamento do desempenho de uma rede consiste na monitoração das atividades da rede e no controle dos recursos através de ajustes e trocas. Algumas das questões relativas ao gerenciamento do desempenho, são:

- qual é o nível de capacidade de utilização?
- o tráfego é excessivo?
- o throughput foi reduzido para níveis aceitáveis?
- existem gargalos?
- o tempo de resposta está aumentando?

Para tratar estas questões, o gerente deve focalizar um conjunto inicial de recursos a serem monitorados, a fim de estabelecer níveis de desempenho. Isto inclui associar métricas e valores apropriados aos recursos de rede que possam fornecer indicadores de diferentes níveis de desempenho. Muitos recursos devem ser monitorados para se obter informações sobre o nível de operação da rede. Colecionando e analisando estas informações, o gerente da rede pode ficar mais e mais capacitado no reconhecimento de situações indicativas de degradação de desempenho.

Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes. Estas informações podem ser utilizadas para reconhecer situações de gargalo antes que elas causem problemas para o usuário final. Ações corretivas podem ser executadas, tais como, trocar tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou ainda, a longo prazo, indicar a necessidade de expansão de linhas para uma determinada área.

Gerenciamento de Segurança

O gerenciamento da segurança provê facilidades para proteger recursos da rede e informações dos usuários. Estas facilidades devem estar disponíveis apenas para usuários autorizados. É necessário que a política de segurança seja robusta e efetiva e que o sistema de gerenciamento da segurança seja, ele próprio, seguro.

O gerenciamento de segurança trata de questões como:

- geração, distribuição e armazenamento de chaves de criptografia;
- manutenção e distribuição de senhas e informações de controle de acesso;
- monitoração e controle de acesso à rede ou parte da rede e às informações obtidas

dos nodos da rede;
- coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.

1.2 Monitoração e Controle da Rede

As funções de gerenciamento de rede podem ser agrupadas em duas categorias: monitoração de rede e controle de rede. A monitoração da rede está relacionada com a tarefa de observação e análise do estado e configuração de seus componentes; é uma função de "leitura". O controle da rede é uma função de "escrita" e está relacionada com a tarefa de alteração de valores de parâmetros e execução de determinadas ações.

Monitoração

A monitoração consiste na observação de informações relevantes ao gerenciamento. Estas informações podem ser classificadas em três categorias:

- Estática: caracteriza a configuração atual e os elementos na atual configuração, tais como o número e identificação de portas em um roteador.
- Dinâmica: relacionada com os eventos na rede, tais como a transmissão de um pacote na rede.
- Estatística: pode ser derivada de informações dinâmicas; ex. média de pacotes transmitidos por unidade de tempo em um determinado sistema.

A informação de gerenciamento é coletada e armazenada por agentes e repassada para um ou mais gerentes. Duas técnicas podem ser utilizadas na comunicação entre agentes e gerentes: *polling* e *event-reporting.*

A técnica de polling consiste em uma interação do tipo *request/response* entre um gerente e um agente. O gerente pode solicitar a um agente (para o qual ele tenha autorização), o envio de valores de diversos elementos de informação. O agente responde com os valores constantes em sua MIB.

Na técnica de *event-reporting,* a iniciativa é do agente. O gerente fica na escuta, esperando pela chegada de informações. Um agente pode gerar um relatório periodicamente para fornecer ao gerente o seu estado atual. A periodicidade do relatório pode ser configurada previamente pelo gerente. Um agente também pode enviar um relatório quando ocorre um evento significativo ou não usual.

Tanto o *polling* quanto o *event-reporting* são usados nos sistemas de gerenciamento, porém a ênfase dada a cada um dos métodos difere muito entre os sistemas. Em sistemas de gerenciamento de redes de telecomunicações, a ênfase maior é dada para o método de relatório de evento. Em contraste, o modelo SNMP dá pouca importância ao relatório de evento. O modelo OSI fica entre estes dois extremos.

A escolha da ênfase depende de um número de fatores, incluindo os seguintes:

- a quantidade de tráfego gerada por cada método;
- robustez em situações críticas;
- o tempo entre a ocorrência do evento e a notificação ao gerente;

- a quantidade de processamento nos equipamentos gerenciados;
- a problemática referente à transferência confiável versus transferência não confiável
- as aplicações de monitoração de rede suportadas;
- as considerações referentes ao caso em que um equipamento falhe antes de enviar um relatório.

Controle de Rede

Esta parte do gerenciamento de rede diz respeito à modificação de parâmetros e à execução de ações em um sistema remoto. Todas as cinco áreas funcionais de gerenciamento (falhas, desempenho, contabilização, configuração e segurança), envolvem monitoração e controle. Tradicionalmente, no entanto, a ênfase nas três primeiras destas áreas, tem sido na monitoração, enquanto que nas duas últimas, o controle tem sido mais enfatizado. Alguns aspectos de controle na gerência de configuração e de segurança são apresentados a seguir.

O controle de configuração inclui as seguintes funções:

- definição da informação de configuração - recursos e atributos dos recursos sujeitos ao gerenciamento;
- atribuição e modificação de valores de atributos;
- definição e modificação de relacionamentos entre recursos ou componentes da rede;
- inicialização e terminação de operações de rede;
- distribuição de software;
- exame de valores e relacionamentos;
- relatórios de status de configuração.

O controle de segurança é relativo à segurança dos recursos sob gerenciamento, incluindo o próprio sistema de gerenciamento. Os principais objetivos em termos de segurança, são relativos à confidencialidade, integridade e disponibilidade. As principais ameaças à segurança referem-se à interrupção, interceptação, modificação e mascaramento.

As funções de gerenciamento de segurança podem ser agrupadas em três categorias:

- manutenção da informação de segurança
- controle de acesso aos recursos
- controle do processo de criptografia

2 Modelos de Gerenciamento de Rede

Um sistema de gerenciamento de rede é uma coleção de ferramentas para monitorar e controlar a rede, integradas da seguinte forma:

- uma única interface de operador, com um poderoso mas amigável conjunto de comandos, para executar a maioria ou todas as tarefas de gerenciamento da rede;
- uma quantidade mínima de equipamentos separados, isto é, que a maioria do hardware e software necessário para o gerenciamento da rede seja incorporado nos equipamentos de usuários existentes.

O software usado para realizar as tarefas de gerenciamento, reside nos computadores hospedeiros (estações de trabalho) e nos processadores de comunicação (switches, routers, hubs,...).

Todos os equipamentos da rede, que fazem parte do sistema de gerenciamento, possuem um conjunto de software destinado às tarefas de coletar informações sobre as atividades relacionadas com a rede, armazenar estatísticas localmente e responder aos comandos do centro de controle da rede. Estes nodos são referenciados como AGENTES. No mínimo um hospedeiro da rede é designado para as tarefas de controlador da rede (GERENTE) e possui uma coleção de software chamada Aplicação de Gerenciamento da Rede. A aplicação de gerenciamento da rede possui uma interface que permite, a um usuário autorizado, gerenciar a rede. A figura 2.1 apresenta um cenário possível de um sistema de gerenciamento de rede.

Um software de gerenciamento genérico é composto por:

- Elementos gerenciados
- Agentes
- Gerentes
- Bancos de Dados de Informações
- Protocolos para troca de informações de gerenciamento
- Interfaces para programas aplicativos
- Interfaces com o usuário

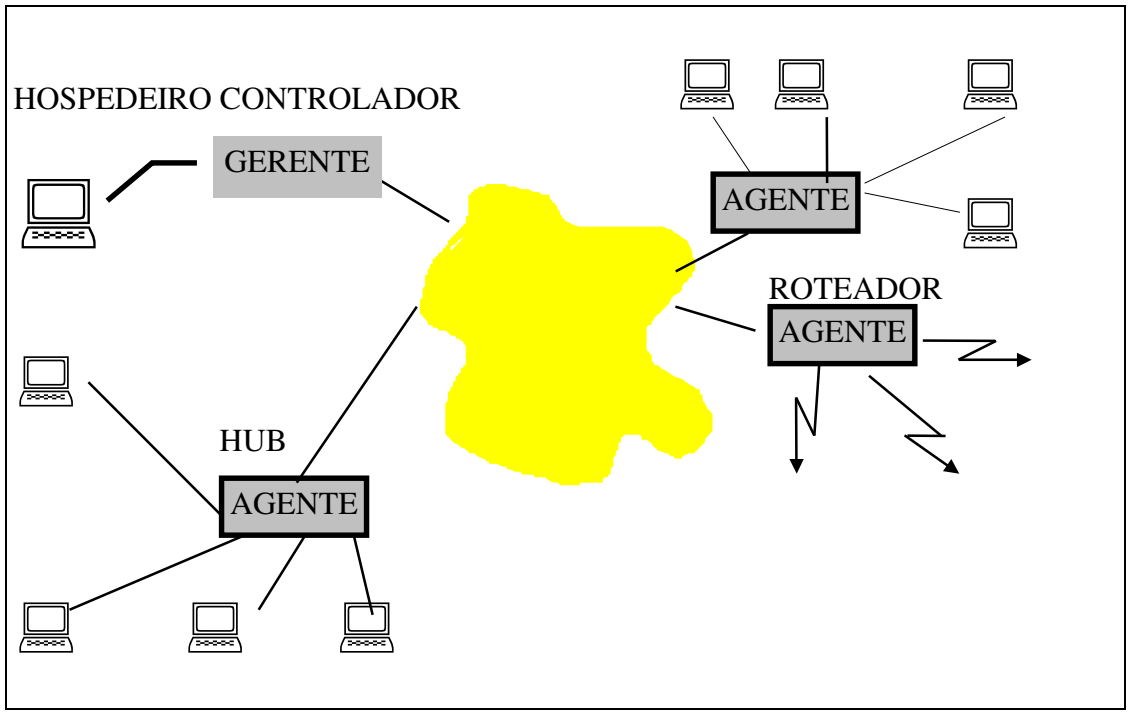


Figura 2.1. Configuração de um sistema de gerenciamento de rede.

A arquitetura do software de gerenciamento residente no gerente e nos agentes varia de acordo com a funcionalidade da plataforma adotada. Genericamente, o software pode ser dividido em três grandes categorias:

- software de apresentação (interface)
- software de gerenciamento (aplicação)
- software de suporte (base de dados e comunicação)

2.1 Software de apresentação

A interface de usuário, em um sistema de gerenciamento, permite que o usuário monitore e controle a rede. Normalmente ela está localizada no sistema hospedeiro gerente. Em alguns casos é comum existir uma interface em alguns agentes a fim de permitir a execução de testes e também a visualização ou alteração de alguns parâmetros localmente. A figura 2.2 (a) mostra os dois blocos que representam o software de apresentação das informações de gerência.

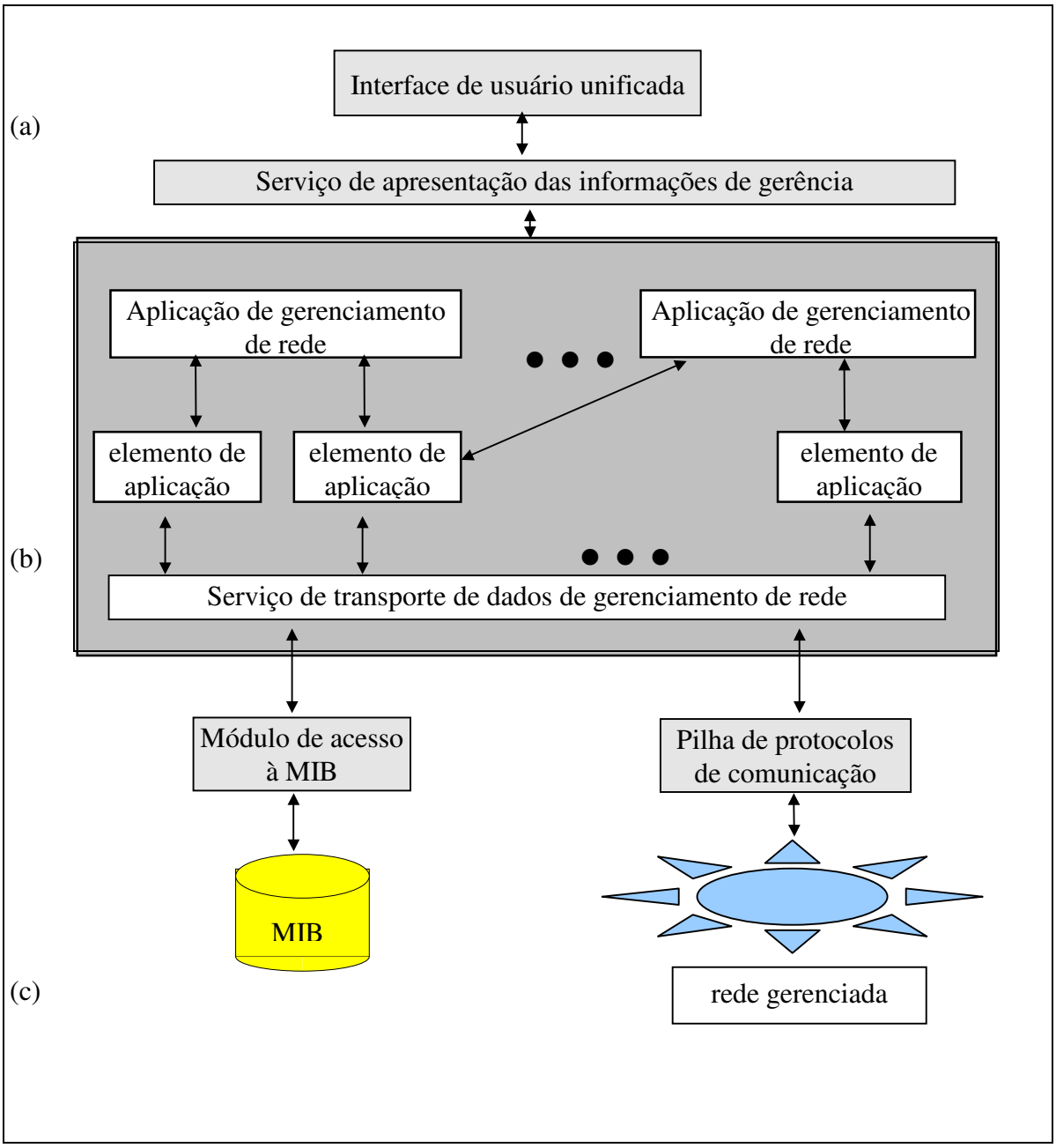


Figura 2.2. Arquitetura de um sistema de gerenciamento de rede.

O principal, em qualquer sistema de gerenciamento, é que a interface seja unificada, isto é, que ela seja a mesma em qualquer nodo, permitindo que o usuário gerencie uma rede heterogênea com um mínimo de treinamento.

Um dos perigos em qualquer sistema de gerenciamento é a sobrecarga de informações. Dependendo da configuração estabelecida, uma grande quantidade de informações pode ser disponibilizada para o usuário. As ferramentas da interface de apresentação devem organizar, sumarizar e simplificar, tanto quanto possível, estas informações. Na maioria dos

produtos existentes no mercado, são utilizados gráficos e tabelas para a apresentação das informações.

2.2 Software de Gerenciamento

O software que fornece a aplicação de gerenciamento pode ser muito simples, como é o caso do modelo SNMP, ou muito complexo, como o modelo OSI. A figura 2.2 (b) mostra uma estrutura genérica de um software de gerenciamento, organizado em três níveis: aplicação de gerenciamento de rede, elementos de serviço da aplicação e serviço de transporte de dados de gerenciamento da rede.

A aplicação de gerenciamento de rede provê os serviços de interesse do usuário como, por exemplo, gerenciamento de falhas, de configuração, de segurança, etc. Os elementos de serviço da aplicação implementam as funções com propósito geral, que servem de suporte às diversas aplicações, tais como, alarmes genéricos ou sumarização de dados. O serviço de transporte de dados de gerenciamento consiste de um protocolo usado para a troca de informações entre gerentes e agentes e de uma interface de serviço para os elementos de serviço de aplicação.

2.3 Software de Suporte ao Gerenciamento

Para executar suas tarefas, o software de gerenciamento necessita acessar uma base de informações de gerenciamento (MIB) e agentes e gerentes remotos.

A MIB localizada em um nodo agente contém informações de gerenciamento que refletem a configuração e o comportamento do nodo e parâmetros que podem ser usados para controlar a operação do nodo. A MIB localizada no gerente contém informações específicas do nodo onde está localizada e informações resumidas sobre os agentes sob o seu controle.

O módulo de acesso à MIB, mostrado na figura 2.2 (c), inclui software de gerenciamento de arquivos que habilitam o acesso à MIB. Adicionalmente, o módulo de acesso à MIB pode converter o formato local das informações para um formato padronizado do sistema de gerenciamento.

O modelo de informação de um sistema de gerenciamento fornece a estrutura para representação, armazenamento e transferência das informações de gerenciamento. Esta estrutura é denominada SMI (Structure Management Information) e, dependendo do sistema, poderá apresentar maior ou menor complexidade.

No modelo OSI, a SMI é baseada no paradigma de orientação a objetos, enfatizando as hierarquias de classe, de containment e de registro. Já o modelo SNMP, utiliza conceitos de Tipos de Dados, embora a sua nomenclatura refira-se a objetos.

A figura 2.3. mostra exemplos de definição de objeto em cada um dos modelos.

Modelo SNMP	Modelo OSI

abcObjectType OBJECT-TYPE
SYNTAX INTEGER {
choicelabel1 (1),
choicelabel2 (2)
}
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Description Text"
::= { pqr 3 }
	network MANAGED OBJECT CLASS
	DERIVED FROM top;
	BEHAVIOR network-behavior;
	CHARACTERIZED BY
	networkPackage PACKAGE
	ATTRIBUTES
	networkID GET,
	networkType GET;
	
	REGISTERED AS (exemplo MObjectClass 2);

Figura 2.3. Exemplos de especificação de objetos gerenciados

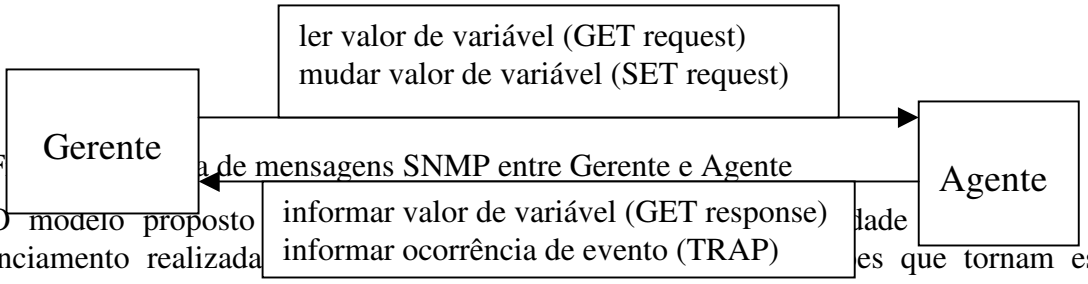
A comunicação entre gerentes e agentes é suportada por uma pilha de protocolos, tais como a pilha OSI ou a pilha TCP/IP. A arquitetura de comunicação suporta o protocolo de gerenciamento de rede que está localizado na camada de aplicação.

Os serviços básicos de um sistema de gerenciamento de rede são os serviços de monitoração e controle. Estes serviços são obtidos através de primitivas para a leitura e escrita nos valores dos objetos gerenciados. Outros serviços adicionais são: criação e destruição de objetos gerenciados, execução de ações sobre objetos gerenciados e emissão de relatórios de eventos.

A comunicação entre agentes e gerentes, a fim de alcançar estes serviços, deve seguir um conjunto de regras básicas, como em qualquer outra aplicação distribuída. Este conjunto de regras pode apresentar maior ou menor complexidade, dependendo do modelo adotado. O modelo OSI utiliza o protocolo CMIP (Common Management Information Protocol) que apresenta funcionalidades para emitir relatórios diversos sobre a ocorrência de eventos, criar e destruir instâncias de classes de objetos, executar ações sobre objetos, ler e modificar valores de atributos de objetos e para a execução de operações sobre vários objetos a partir da definição de um escopo e de um filtro para a seleção de objetos. O modelo Internet utiliza o protocolo SNMP (Simple Network Information Protocol), cuja funcionalidade reside basicamente na leitura e alteração de valores de variáveis e em alguns relatórios de evento para situações específicas.

3 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 3.1 mostra algumas das interações possíveis entre um Gerente e um Agente, através do protocolo SNMP.



F a de mensagens SNMP entre Gerente e Agente

O modelo proposto lade de gerenciamento realizada es 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.

3.1 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.

3.2 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 3.2. 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 3.2 – 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 3.3.

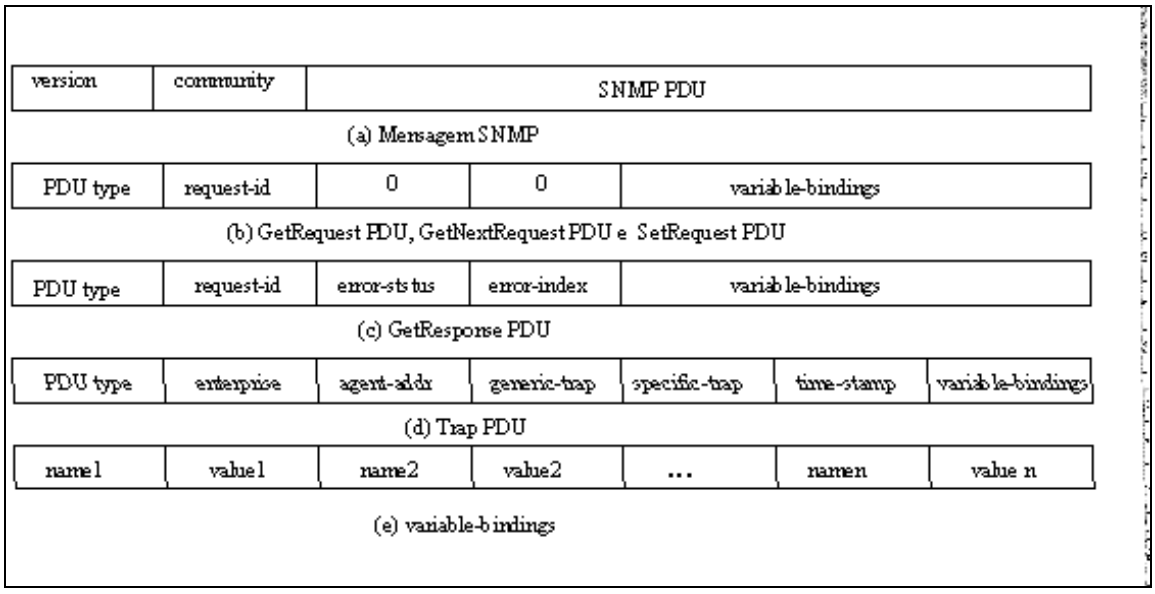


Figura 3.3 – Formato de Mensagens SNMPv1

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.

3.3 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.

3.3.1 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 3.4 mostra a árvore de registro utilizada para nomeação de objetos definidos na MIB.

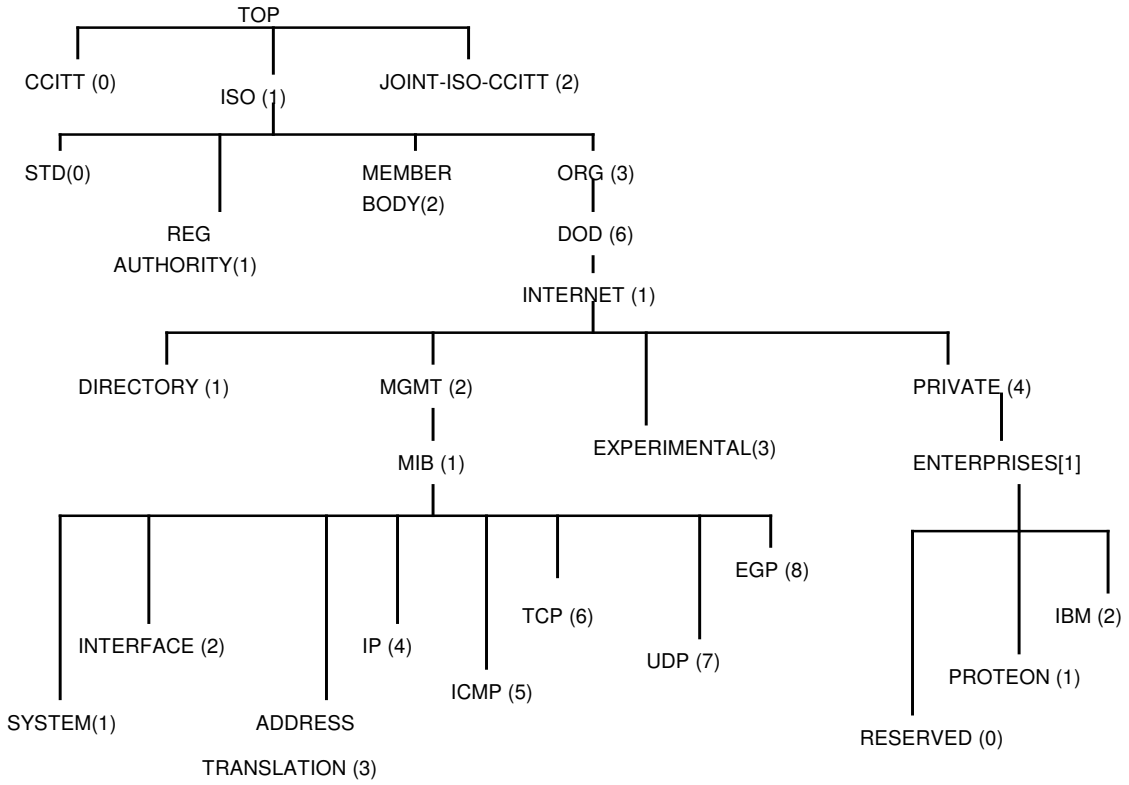


Figura 3.4 - Árvore de registro de tipos de objetos

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}
```

3.3.2 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 3.5 ilustra a estrutura do grupo system e a tabela 3.1 fornece a sintaxe do objeto, a forma de acesso permitida e uma descrição sucinta da semântica.

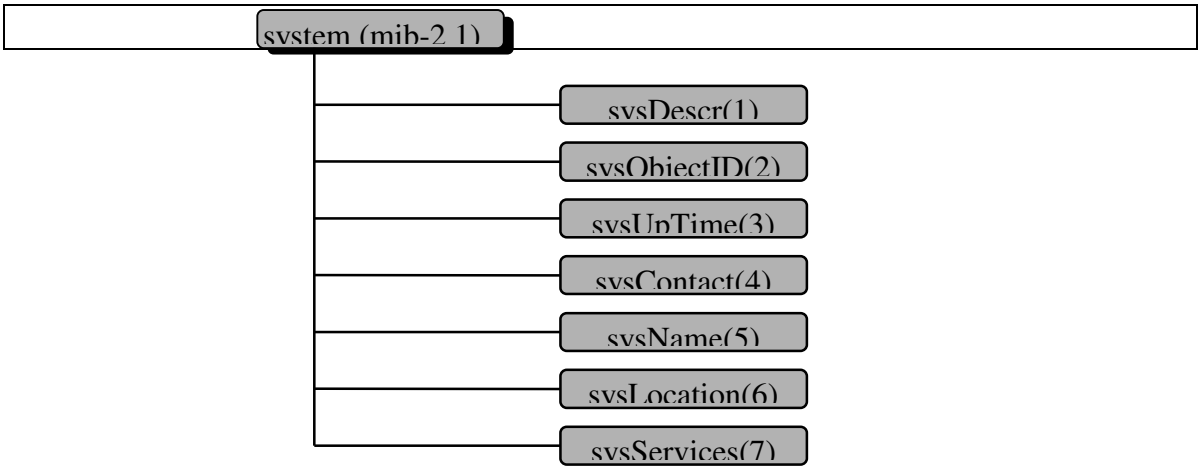


Fig. 3.5. Grupo System da MIB-II

Tabela 3.1 - 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	RO	Valor indicando o conjunto de

	(0..127)		serviços oferecidos pela entidade

3.4 Monitoração Remota - RMON MIB

A medida em que as redes foram crescendo e se tornando geográfica e logicamente distribuídas, o gerenciamento de redes tornou-se mais desafiador. Utilizando apenas informações da MIB-II, o gerente de redes não consegue ter uma idéia do tráfego existente nas redes onde os recursos gerenciados estão instalados porque estas informações referem-se apenas ao próprio recurso onde o agente está executando. Em uma grande rede, com vários nós gerenciados e não gerenciados, fica praticamente impossível inspecionar variáveis da MIB-II de todos os agentes da rede para se ter uma idéia do tráfego entre eles.

Uma solução encontrada foi a instalação de dispositivos remotos de gerenciamento, denominados probes, nos segmentos remotos. A mais importante adição ao conjunto de padrões SNMP foi a MIB RMON (Remote Network Monitoring MIB) que padronizou as informações de gerenciamento enviadas para e recebidas desses probes na RFC1757 [Wal 95].

Outro problema com os agentes SNMP tradicionais é que estes não são capazes de analisar seus próprios dados e, por exemplo, serem programados para enviarem notificações quando certos limiares nas variáveis forem atingidos. Isto força a estação de gerenciamento a ficar inspecionando (fazendo *polling*) as variáveis das diversas entidades de gerenciamento, causando um tráfego excessivo na rede.

A tecnologia de RMON consiste na presença de um monitor instalado na rede que se deseja estudar, coletando informações e, eventualmente, enviando notificações sobre a ocorrência de eventos. O monitor pode ser tanto um dispositivo dedicado à captura de dados e à sua análise, como também pode estar implementado em estações de trabalho, em servidores, roteadores, hubs, etc.

Essencialmente, a RMON é uma extensão da MIB Internet. Através da escrita em variáveis desta MIB, o gerente pode programar o monitor para coletar dados e armazená-los em tabelas para serem recuperados posteriormente.

O RMON divide o processo de captação de dados em duas partes. Os dados são coletados pelo agente RMON que pode estar em um segmento próximo ao dispositivo ou implementado no dispositivo. Uma ou mais estações de gerenciamento falam com o agente RMON (usando SNMP) em lugar de falar diretamente com o dispositivo gerenciado. Por terminologia, um sistema que implementa a MIB RMON é chamado de probe RMON. Mesmo que a estação de gerenciamento perca conexão ao probe a coleta de dados continua, uma vez que o probe está conectado diretamente à rede sendo monitorada.

A RMON foi projetada para atingir os seguintes objetivos:

operação off-line: o monitor coleta e armazena estatísticas que podem ser recuperadas pela estação gerente a qualquer momento;

monitoração preemptiva: o monitor está sempre ativo, continuamente rodando diagnósticos e armazenando dados;

detecção e alerta de problemas: o monitor pode verificar continuamente determinadas condições e comunicá-las quando ocorrerem;

resumo dos dados: o monitor é capaz de realizar algum processamento como, por exemplo, descobrir os 10 hosts mais ativos na rede;

múltiplos gerentes: o monitor deve suportar várias estações gerentes.

A figura 3.6 mostra o cenário de gerenciamento de uma rede utilizando RMON.

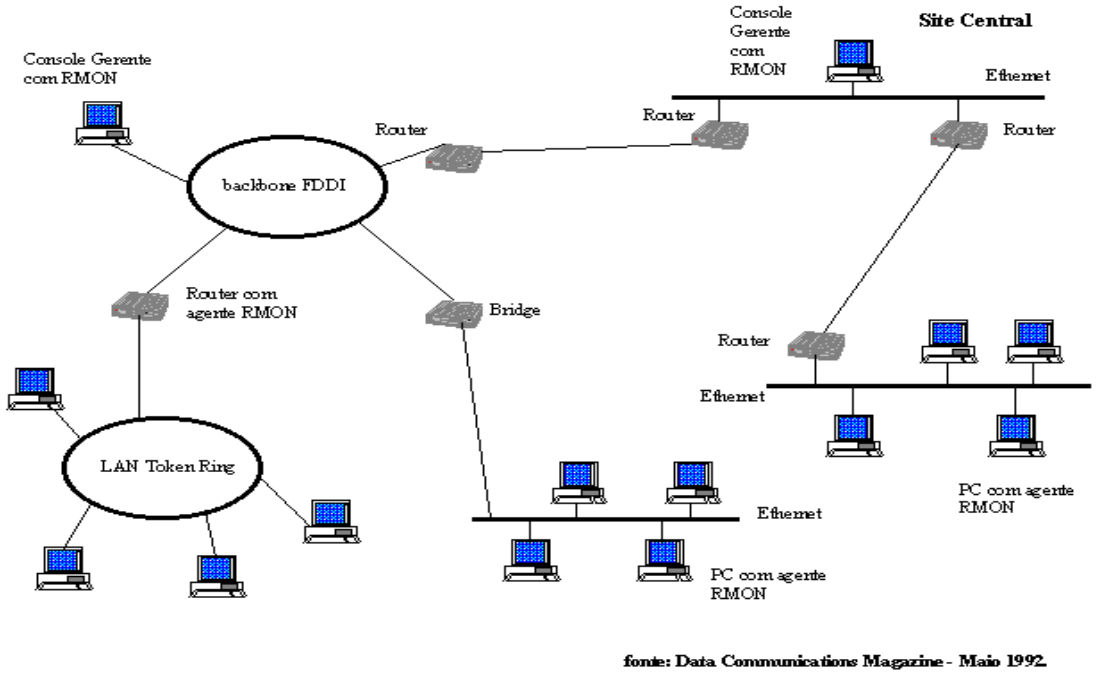


Figura 3.6 – Utilização do RMON na gerência de rede.

Para implementar um agente RMON em um dispositivo, ele deve ser capaz de operar no modo promíscuo, isto é, deverá poder aceitar dados não endereçados especificamente para ele.

As metas definidas pelo grupo de trabalho para a definição das MIBs RMON são definidas nos RFCs 1757 e 2021. São elas:

- ✓ **operação off-line** – o probe acumula estatísticas e executa diagnósticos continuamente, mesmo que a comunicação com a estação gerente não seja possível ou eficiente. As notificações podem ser enviadas para o gerente quando eventos excepcionais ocorrerem. Além disso o gerente pode recuperar informações do probe RMON quando melhor lhe aprouver, utilizando o protocolo SNMP;

- ✓ **monitoramento pró-ativo** - se o monitor tiver recursos suficientes, pode executar continuamente diagnósticos e logar performance da rede. Em uma falha na rede, pode notificar a estação gerente da falha e prover informações proveitosas no diagnóstico da falha;
- ✓ **detecção e registro de problemas** - O monitor pode passivamente reconhecer certas condições de erro e outros, como congestionamento, no tráfego observado. Quando uma condição configurada ocorrer, pode registrar e tentar notificar a estação gerente;
- ✓ **análise de dados** - o monitor pode executar análises específicas sobre os dados coletados na sub-rede. Por exemplo, pode determinar qual *host* gera a maior parte do tráfego ou dos erros na sub-rede;
- ✓ **múltiplos gerentes** - uma configuração de rede pode ter mais do que uma estação gerente como medida de redundância, que podem executar funções diferentes e prover capacidades de gerência para unidades diferentes na organização.

O RMON provê informações estatísticas e de diagnóstico, minimiza o tráfego de gerenciamento, reduz o impacto de perda de conectividade, serve várias estações de gerenciamento simultaneamente e fornece, ainda, um conjunto padrão de métricas que pode ser usado por vários dispositivos que suportam RMON.

A MIB RMON possui OID {1.3.6.1.2.1.16} e foi originalmente definida para redes ethernet em novembro de 1991 no RFC 1271, em 1995 foi substituída pelo RFC 1757, que foi, em maio de 2000, substituído pelo RFC 2819. Originalmente a MIB RMON só contemplava redes ethernet, mas em setembro de 1993 foi desenvolvido o RFC 1513, que trazia extensões para redes token ring. A MIB RMON contém 10 grupos. A figura 3.7 mostra a localização da MIB RMON com os grupos definidos:

- ✓ ***statistics*** **(rmon 1)** – provê estatísticas medidas pelo probe no segmento, tais como número e tamanho dos pacotes, broadcast, colisões, etc;
- ✓ ***history*** **(rmon 2)** - grava amostras estatísticas periódicas do tráfego para permitir análise posterior;
- ✓ ***alarm*** **(rmon 3)** - compara amostras estatísticas com limiares configurados gerando alarmes quando estes limiares forem ultrapassados;
- ✓ ***host*** **(rmon 4)** - mantém estatísticas dos hosts na rede, incluindo o MAC address dos hosts ativos;
- ✓ ***hostTopN*** **(rmon 5)** - provê relatórios indicando quais hosts estão no topo de uma categoria em particular;
- ✓ **matrix (rmon 6)** - armazena estatísticas de tráfego sobre conversações entre hosts;
- ✓ ***filter*** **(rmon 7)** - permite que pacotes sejam selecionados de acordo com um critério especificado;
- ✓ ***capture*** **(rmon 8)** - permite que pacotes sejam capturados depois de passarem pelo filtro;
- ✓ ***event*** **(rmon 9)** - controla a geração e notificação de eventos, o que pode incluir mensagens de trap SNMP;
- ✓ ***tokenRing (rmon 10) – provê parâmetros adicionais para redes token ring.***

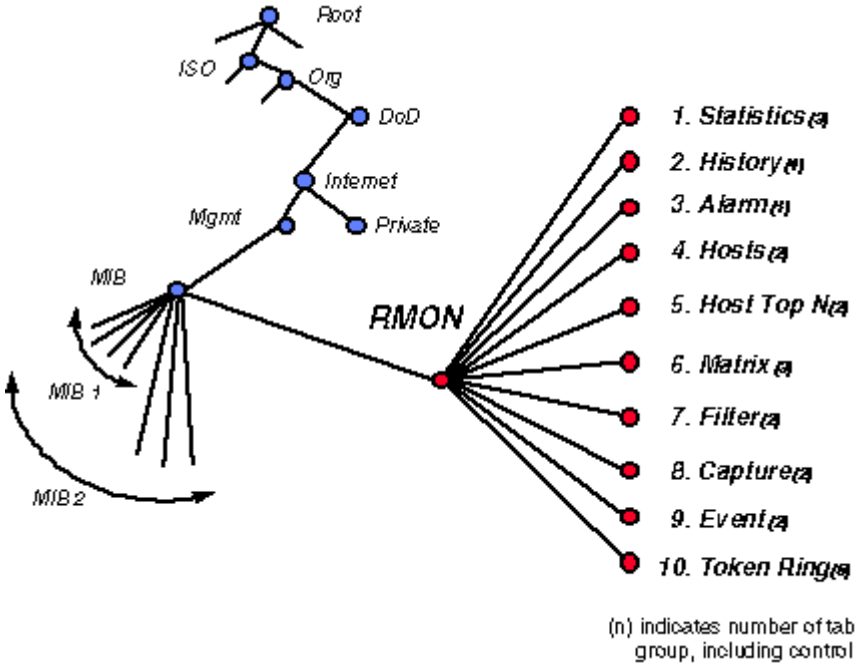


Figura 3.7 – Grupos RMON

Subramanian [Subramanian 2000] (p.327) enquadra os grupos RMON em três grandes categorias: a maior é a dos grupos que analisam as informações e geram estatísticas. Nesta categoria enquadram-se os grupos statistics, history, host e host top N. A segunda categoria trata de eventos da rede e funções de geração de relatórios. Estes são os grupos de alarm e event. A terceira categoria trata com filtragem e captura de pacotes. Nesta categoria enquadram-se os grupos filter e packet capture. A figura 3.8 ilustra esta classificação.

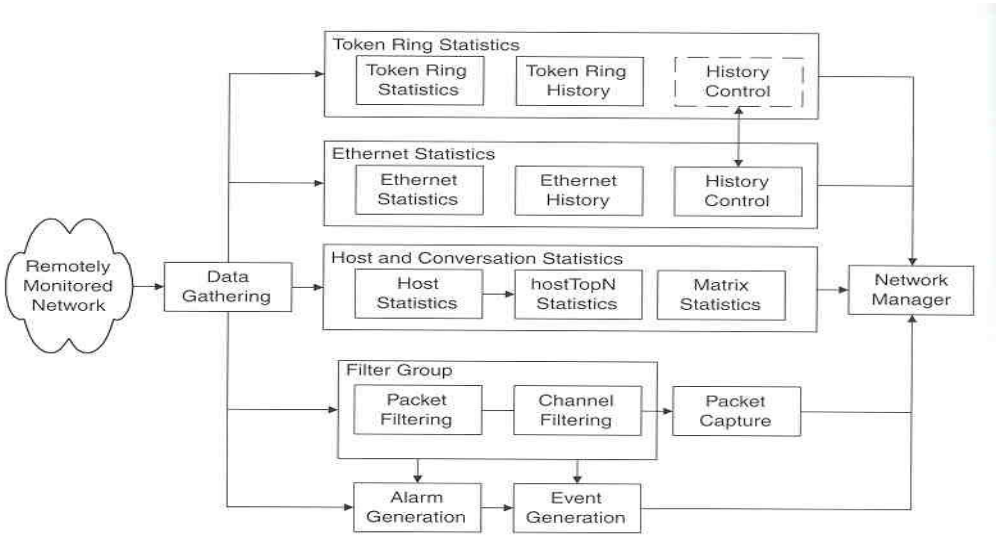


Figura 3.8 – Classificação dos grupos RMON

Todos os grupos são opcionais, mas a implementação de alguns grupos requer outros grupos. Existem as seguintes dependências:

- ✓ o grupo *alarm* requer a implementação do grupo *event*;
- ✓ o grupo *hostTopN* requer a implementação do grupo *host*;
- ✓ o grupo capture requer a implementação do grupo *filter*.

Tipicamente, um monitor remoto necessitará ser configurado para coletar dados. A configuração dita o tipo e forma de dados para serem coletados. A MIB é organizada em grupos funcionais. Cada grupo terá uma ou mais tabelas de controle e uma ou mais tabelas de dados. Uma tabela de Controle contém parâmetros que descrevem o dado na tabela de Dados, que é somente para leitura. Assim, a estação gerente seta os parâmetros apropriados para configurar o monitor remoto para coletar os dados desejados. Os parâmetros são setados pela adição de um novo registro na tabela, ou alterando uma existente. Desse modo, funções para serem executadas pelo monitor são definidas e implementadas na tabela. Por exemplo, uma tabela Controle pode conter objetos que especifiquem a origem dos dados coletados, tipos de dados, hora/data da coleta etc...

A RMON2

A MIB RMON original se preocupava basicamente com operação e gerenciamento das camadas física e de enlace, de uma rede remota. O RMON2 definido no RFC2021, estende as capacidades do RMON às camadas superiores, adicionando 10 novos grupos, conforme mostra a figura 3.9: (Miller 1997, Subramanian 2000)

- ✓ ***protocol directory*** **(rmon 11) -** identifica os protocolos que o probe pode monitorar. Os protocolos que podem ser monitorados foram definidos no RFC2074;
- ✓ ***protocol distribution*** **(rmon 12)** - provê informação relativa ao tráfego de diferentes protocolos, tanto em bytes quanto em pacotes. Ele coleta estatísticas que ajudam o administrador de rede a gerenciar a banda alocada para cada protocolo;
- ✓ ***address map*** **(rmon 13)** - correlaciona os endereços de rede com endereços MAC, armazenando-os em uma tabela. A tradução de endereços permite a geração de mapas topológicos aprimorados e a detecção de endereços ip duplicados;
- ✓ ***network-layer host*** **(rmon 14)** – coleciona estatísticas sobre o volume de tráfego de entrada e saídas das estações com base no endereço de nível de rede. Como conseqüência, o gerente pode observar além dos roteadores que interligam as sub-redes e identificar as reais estações que estão se comunicando;
- ✓ ***network-layer matrix*** **(rmon 15)** – provê estatísticas sobre o volume de tráfego entre pares de estações com base no endereço do nível de rede;
- ✓ ***application-layer host*** **(rmon 16)** – agrega estatísticas sobre o volume de tráfego por protocolo de nível superior gerado de ou para cada endereço de rede;
- ✓ ***application-layer matrix*** **(rmon 17)** – coleciona estatísticas sobre o volume de tráfego, por protocolo, trocados por pares de endereços de rede;

- ✓ ***user history collection*** **(rmon 18)** - combina mecanismos vistos nos grupos *alarm* e *history* para prover informações de coleção de dados históricos especificados pelo usuário;
- ✓ ***probe configuration*** **(rmon 19)** – define parâmetros de configuração padrões para probes RMON. Deste modo, a estação de gerenciamento com software de um fabricante é capaz de configurar, remotamente, um probe de outro fabricante;
- ✓ ***rmon conformance (rmon 20)*** **–** descreve os requisitos de conformidade para a MIB RMON2.

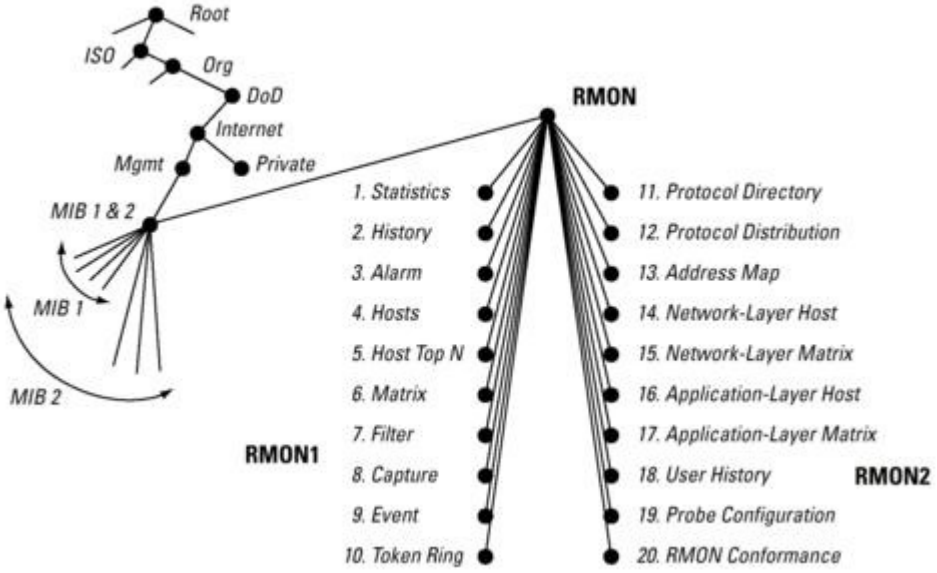


Figura 3.9 – Grupos RMON2

Stallings [Stallings 1999], (p.277) cita duas implicações importantes decorrentes do fato de que o RMON2 decodifica pacotes das camadas 3 a 7 do modelo OSI:

- ✓ o probe RMON2 pode monitorar o tráfego baseado nos endereços e protocolos de camada de rede, incluindo o IP. Isto possibilita que o probe veja acima da rede local ao qual está conectado;
- ✓ como o RMON2 pode decodificar e monitorar tráfego da camada de aplicação, o probe pode gravar tráfego para aplicações específicas.

A figura 3.10 mostra o nível de visibilidade que RMON e RMON2 provêem dentro de um segmento LAN ou de uma rede em cada uma das camadas do OSI.

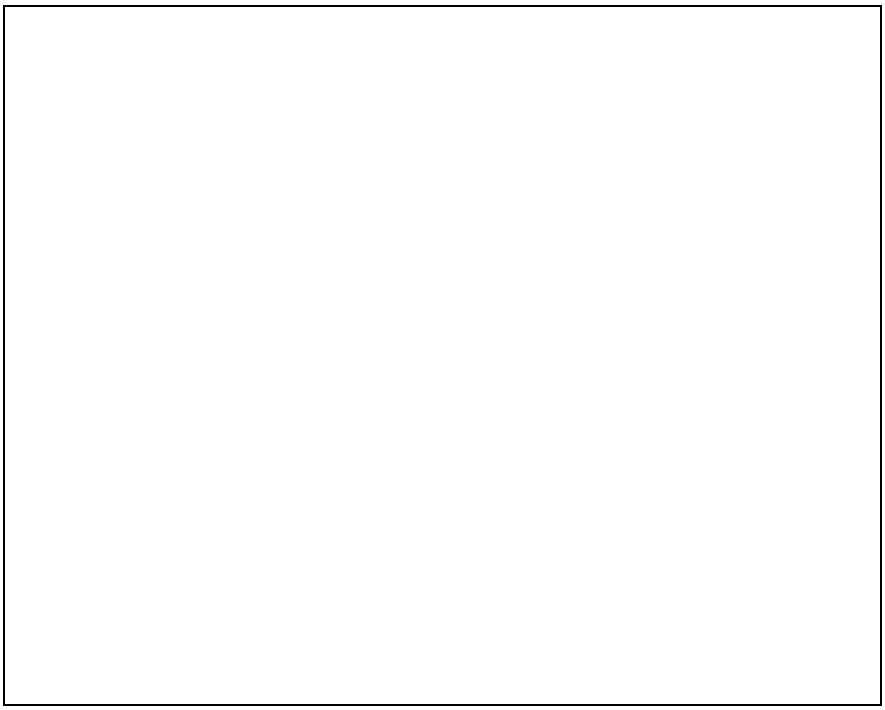


Figura 3.10 – Visibilidade RMON1 x RMON2

As restrições com relação à performance para implementação do RMON1 são ainda maiores no RMON2, pois ele necessita ainda de mais recursos de memória e processamento para ser implementado. Para atender a estas demandas, os fabricantes de dispositivos RMON2 estão oferecendo probes stand-alone que executam em plataformas de hardware de alta capacidade de memória e processamento. (Stallings 1999, p.326)

3.5 O SNMPv2

O SNMP foi desenvolvido como uma solução temporária para prover um gerenciamento mínimo da rede, a solução definitiva viria com o gerenciamento baseado no modelo OSI. Alguns motivos fizeram que esta transição não acontecesse da forma planejada, principalmente porque:

- ✓ o modelo OSI usava a abordagem orientada a objeto que era mais complexa do que o que se planejava implementar no SNMP que implementou um MIB escalar, o que tornava a transição mais complexa.
- ✓ o desenvolvimento de padrões OSI de gerenciamento e subseqüente disponibilização de sua implementação em dispositivos de rede demorou muito mais do que o esperado, abrindo uma janela de oportunidade que foi aproveitada pelo SNMP.

A versão 2 do SNMP (SNMPv2) foi desenvolvida quando se tornou óbvio que o padrão de gerenciamento OSI não seria implementado em um futuro próximo. Os maiores fabricantes de dispositivos de rede já haviam incorporado módulos SNMP em seus equipamentos e estava claro para todos que o SNMP necessitava de melhoramentos.

O primeiro projeto do SNMPv2 não foi amplamente aceito pelo mercado. As razões,

para esta falta de aceitação, são a complexidade dos melhoramentos de segurança e administração do framework. Várias tentativas de simplificação foram tentadas, entretanto não se chegou a nenhum consenso. Como resultado ocorreram três ações (Miller 1997, p.201):

- ✓ os documentos que tinham atingido consenso foram publicados em janeiro de 1996 como RFC´s 1902-1908;
- ✓ modificações menores no modelo de administração e segurança do SNMPv2, denominados comunit-based SNMPv2 (SNMPv2c), foram publicados em janeiro de 1996, documento RFC 1901;
- ✓ o trabalho continuou em outras áreas: segurança, framework administrativo, MIB de configuração remota e comunicação gerente-gerente.

Várias mudanças significativas deveriam ser introduzidas no SNMPv2. Uma das mais significativas seria a de prover funções de segurança, que inexistiam no SNMPv1. Infelizmente, depois de muito esforço, não houve consenso, então a feature de segurança foi retirada da especificação final.

Apesar do modelo organizacional permanecer praticamente inalterado e a despeito da falta de melhorias na parte de segurança, várias melhorias foram feitas na arquitetura SNMPv2: novos tipos de dados, novas macros, convenções textuais, operações que facilitam a transferência de grandes quantidades de dados (bulk), transferência de blocos de dados (bulk), códigos de erro mais detalhados, suporte a multiprotocolos na camada de transporte, inclusão de mensagem de gerente para gerente, definição de uma nova estrutura de informações de gerenciamento (SMIv2 definida nas RFCs 1902 a 1904), comandos de conformidade, melhorias em tabelas e inclusão de dois novos grupos na MIB , security e SNMPv2. [Subramanian 2000], [Miller 1997]

O SNMPv2 provê três tipos de acesso às informações de gerenciamento de redes. O primeiro tipo de interação chamado request-response, é quando o gerente SNMP envia uma solicitação a um agente SNMPv2 que responde. O segundo tipo de interação é um request-response onde ambas as entidades são gerentes SNMP. O terceiro tipo é uma interação não confirmada, onde um agente SNMPv2 envia uma mensagem não solicitada, ou trap, para o gerente e nenhuma resposta é retornada. Somente a segunda forma é nova no SNMPv2, as outras duas já existiam no SNMPv1. A figura 3.11 mostra a arquitetura de gerenciamento utilizando o SNMPv2.

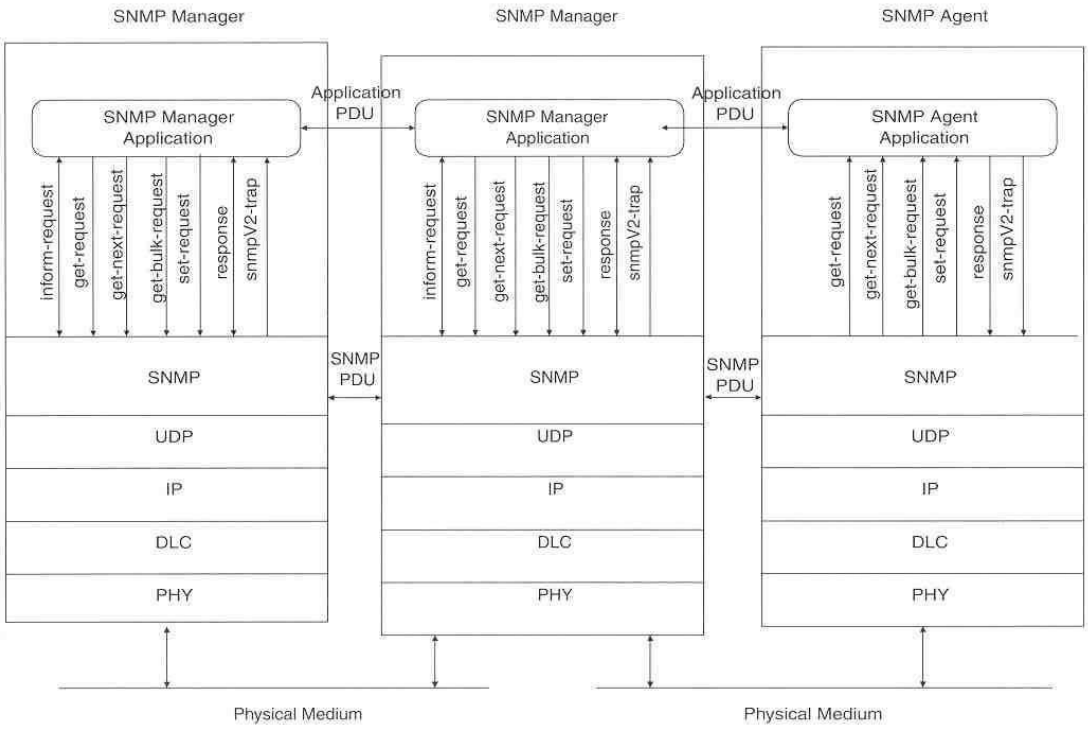


Figura 3.11 – Arquitetura de gerenciamento de rede SNMPv2

A alteração mais importante nas operações do SNMPv2 foi a inclusão de duas novas PDU´s. A GetBulkRequest que permite ao gerente recuperar grandes blocos de dados eficientemente, em particular várias linhas de tabelas. A PDU information-request é gerada por um gerente para informar a outro gerente informação contida em sua visão da MIB. Uma resposta é gerada pelo gerente que recebeu a mensagem para o gerente que a enviou.

A estrutura de dados PDU foi padronizada (figura 3.12) para que todas as mensagens possuam um formato comum, a informação nos traps na versão 2 do SNMP foi modificada para ficar com o mesmo padrão das outras PDU´s. Isto aumenta a eficiência e performance na troca de mensagens entre sistemas.

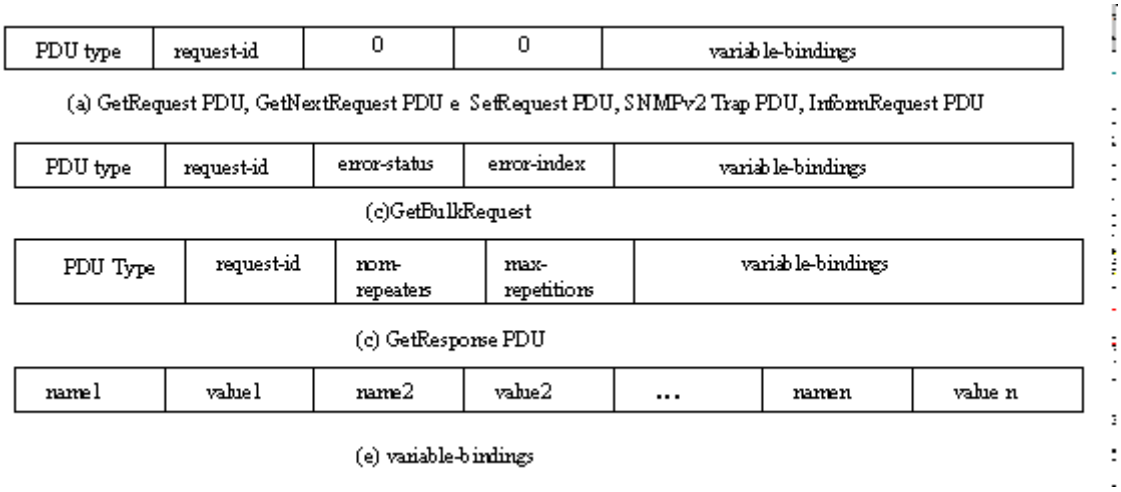


Figura 3.12 – Formato de PDUs do SNMPv2

As PDUs GetRequest e GetNextRequest são idênticas às do SNMPv1 em formato e semântica. A diferença é que no SNMPv1 as operações eram atômicas: ou todos os valores eram retornados ou nenhum valor retornava. No SNMPv2 a lista de variable-bindings é preparada, mesmo se valores não podem ser recuperados para todas as variáveis. Se uma condição de exceção é encontrada para uma variável então a variável é retornada com a indicação da exceção em lugar do valor.

A versão 1 do SNMP foi originalmente definida para transmissão sobre o UDP e IP. Pesquisas subseqüentes exploraram o uso do SNMP com outros protocolos de transporte, incluindo o OSI (RFC 1418), appletalk (RFC 1419) e IPX (RFC 1420). O SNMPv2 formalmente define implementações sobre outros protocolos de transporte no RFC 1906. apesar de definido para vários protocolos de transporte, o RFC 1906 sugere que agentes continuem ouvindo o UDP na porta 161 e gerem notificações na porta 162 do UDP.

O grupo de trabalho do IETF responsável pelo SNMPv2 propôs dois esquemas de migração (RFC 1908) do SNMPv1 para o SNMPv2: o gerente bilíngüe que falaria com o agente SNMP na versão que ele entendesse e o SNMP proxy server que receberia as mensagens SNMPv2 e, atuando como proxy, as transmitiria para o agente como SNMPv1.

Algumas modificações foram introduzidas na MIB internet, conforme ilustrado na figura 3.13: o grupo system do SNMPv2 é composto pelos mesmos objetos do SNMPv1 expandindo com a inclusão de novos objetos que permitem a uma entidade SNMPv2 agindo como agente descrever seus recursos dinamicamente. Além disso, o grupo SNMP na versão do SNMPv2 comparado com o originalmente definido da MIBII tem muito menos objetos. A razão é que as estatísticas detalhadas definidas na MIB II não auxiliam na solução de problemas e adicionam complexidade desnecessária aos agentes.

Apesar das vantagens apresentadas pelo SNMPv2 ele apresenta algumas limitações: pouquíssimo utilizado, sua complexidade implica em dificuldades de implementação e não foi bem recebido pela comunidade de gerência.

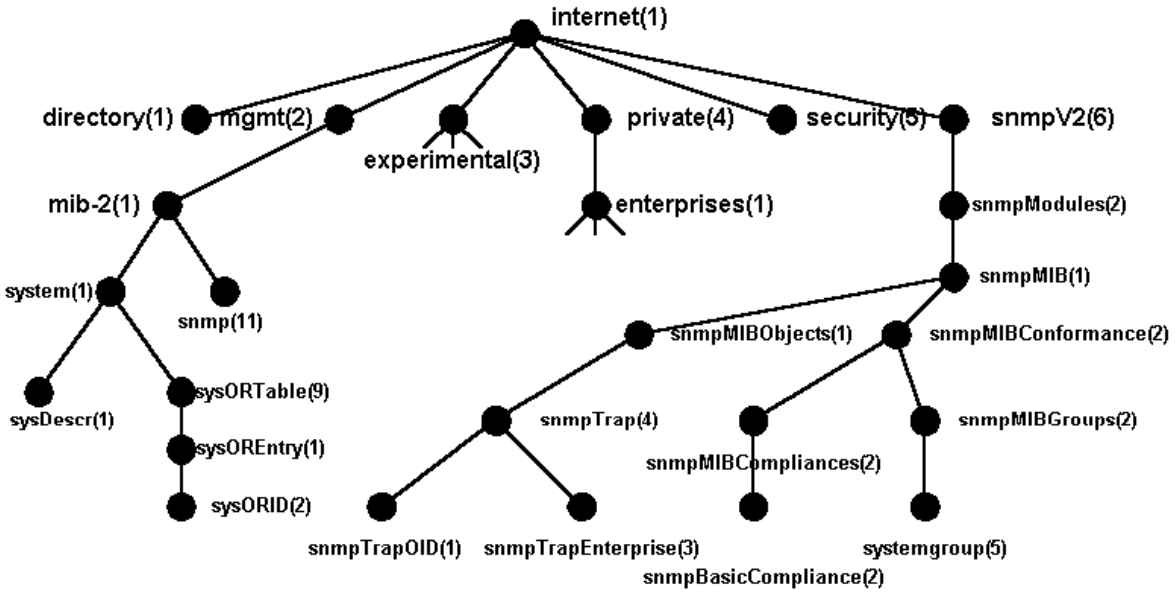


Figura 3.13 – Árvore do SNMPv2

3.6 **O SNMPv3**

Depois de muita controvérsia, o SNMv2 foi liberado como um framework SNMP, SNMPv2C, sem qualquer implementação adicional de segurança. Esta deficiência foi solucionada no SNMPv3. Os documentos do grupo de trabalho do SNMPv3 não são de fato especificações completas de um protocolo de gerenciamento de redes. Na verdade estes documentos definem um conjunto de características de segurança e um framework que poderia ser utilizado com as capacidades funcionais do SNMPv2 ou SNMPv1. (Stallings 1999, Subramanian 2000)

Uma das características chave do SNMPv3 é a modularidade da documentação e arquitetura. O projeto da arquitetura integrada das especificações SNMPv1 e SNMPv2 com as do SNMPv3. Esta integração permite a continuação de uso do legado de SNMP por agentes e gerentes SNMPv3.

O RFC 2571, documento que definiu a arquitetura do SNMPv3, define os seguintes objetivos que guiaram seu desenvolvimento:

- ✓ utilizar o trabalho existente. Os conceitos de segurança do SNMPv3 se baseiam fortemente no SNMPv2u e SNMPv2*;
- ✓ resolver o problema de segurança, principalmente para a operação *set-request*, considerada a deficiência mais importante no SNMPv1 e SNMPv2C;
- ✓ ser modular para possibilitar o desenvolvimento de parte da arquitetura, mesmo que o consenso não tenha sido atingido no todo;
- ✓ definir uma arquitetura que permita longevidade ao *framework* SNMP que já tenha sido definido e que venha a ser definido no futuro;

- ✓ manter o SNMP o mais simples possível;
- ✓ projetar uma arquitetura modular que permita a implementação sobre diversos ambientes operacionais; e
- ✓ acomodar modelos de segurança alternativos.

Um dos principais objetivos do SNMPv3 foi a área de segurança. Autenticação, privacidade, bem como a autorização e controle de acesso foram incorporados na especificação SNMPv3. O SNMPv3 é projetado para prover segurança conta as seguintes ameaças:

- ✓ modificação da informação – uma entidade poderia alterar uma mensagem em trânsito gerada por uma entidade autorizada;
- ✓ masquerade – uma entidade não autorizada assumir a identidade de uma entidade autorizada;
- ✓ modificação de stream de mensagem – como o SNMP é projetado para operar sobre um protocolo não orientado à conexão, existe a ameaça de que as mensagens SNMP possam ser reordenadas, atrasadas ou duplicadas;
- ✓ descoberta – uma entidade poderia observar trocas de mensagens entre gerentes e agentes e aprender o valor de objetos gerenciados e eventos notificados.

O SNMPv3 não contém mecanismos de segurança contra duas ameaças:

- ✓ denial of service – uma pessoa poderia impossibilitar trocas de mensagens entre gerente e agente;
- ✓ análise de tráfego – uma pessoa poderia observar o padrão de tráfego entre gerentes e agentes.

A arquitetura SNMP, conforme definida no RFC 2571, consiste de uma coleção de entidades SNMP distribuídas e interagindo. Cada entidade implementa uma parte das características do SNMP e pode atuar como um nó agente, um nó gerente ou uma combinação dos dois. Cada entidade SNMP consiste de uma coleção de módulos que interagem entre si para prover serviços.

A figura 3.14, definida no RFC 2571, mostra detalhes de uma entidade SNMP e seus componentes:

- ✓ dispatcher – permite o suporte concorrente a múltiplas versões de mensagens SNMP no engine SNMP;
- ✓ message processing subsystem – responsável por preparar mensagens para envio e extrair dados de mensagens recebidas;
- ✓ security subsystem – provê serviços de segurança tais como autenticação e privacidade de mensagens. Este subsistema pode conter múltiplos modelos de segurança;
- ✓ access control subsystem – provê um conjunto de serviços que uma aplicação pode usar para checagem de direitos de acesso;

- ✓ command generator – inicializa as PDUs SNMP (get, getnext; getbulk, setrequest) e processa a resposta gerada para uma requisição;
- ✓ command responder – recebe as PDUs SNMP destinadas para o sistema local. A aplicação command responder executará a operação apropriada do protocolo, usando o controle de acesso, e gera a mensagem de resposta a ser enviada;
- ✓ notification originator – monitora o sistema por eventos e condições particulares e gera mensagens (trap/inform) baseado nos eventos e condições. Devem existir mecanismos para determinar para onde enviar as mensagens, qual versão do SNMP utilizar e quais parâmetros de segurança devem ser utilizados;
- ✓ notification receiver – ouve as mensagens de notificação e gera mensagens de resposta quando uma mensagem contendo uma PDU inform é recebida;
- ✓ proxy forwarder – repassa mensagens SNMP. Sua implementação é opcional;

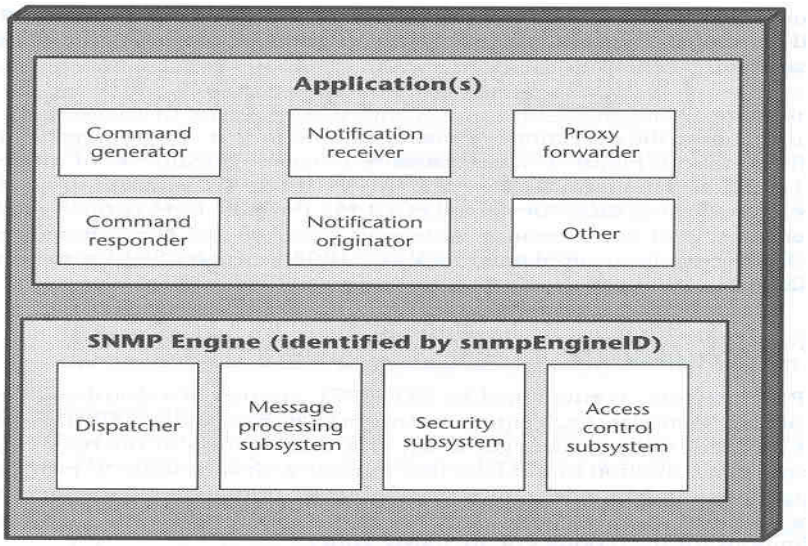


Figura 3.14 – Entidade SNMPv3 (RFC 2571)

O formato das mensagens SNMPv3 consiste de quatro grupos, mostrados na figura 4.15. O primeiro grupo é um campo simples, que é o número da versão e está na mesma posição que no SNMPv1 e SNMPv2, o subsistema dispatcher verifica o número da versão e encaminha para o modelo de processamento de mensagem apropriado. O segundo grupo, denominado global/header data, contém parâmetros administrativos da mensagem, incluindo o modelo de segurança utilizado, vários modelos são permitidos. O terceiro grupo contém parâmetros de segurança e é usado pelo modelo de segurança na comunicação entre entidades. O quarto grupo de dados contém os campos da PDU, conforme da versão do SNMP utilizada, podendo estar criptografado ou em texto claro.

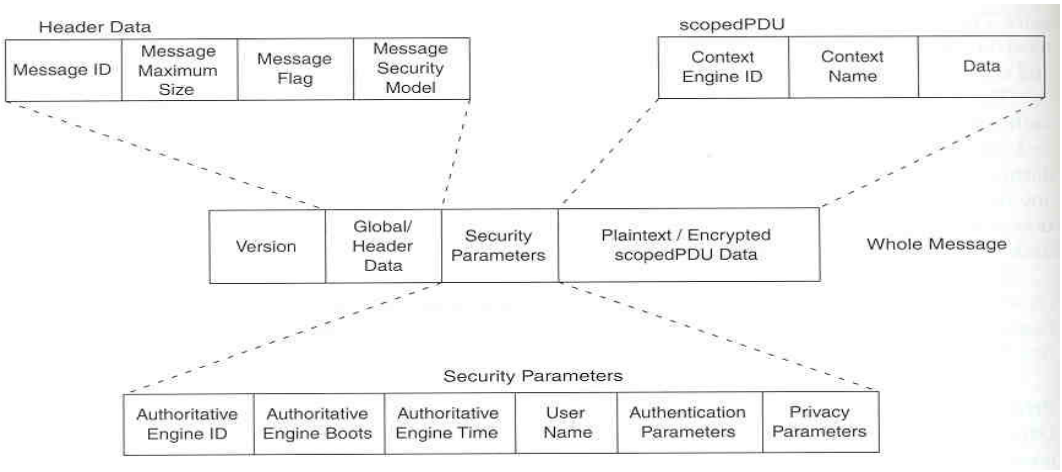


Figura 3.15 – Formato de mensagens SNMPv3

O modelo de segurança do SNMPv3 é um modelo de segurança baseado em usuários (USM – User-based Security Model) que reflete o conceito tradicional de nome de usuários e senhas. A base de segurança no uso de esquemas de autenticação e privacidades são chaves secretas. A chave secreta para autenticação é derivada de uma senha escolhida pelo usuário.

O controle de acesso trata de quem pode acessar os componentes de gerenciamento das redes e o que pode ser acessado. Nas versões anteriores do SNMP, este tópico era coberto pela política de acesso baseada em nomes de comunidade. No SNMPv3, o controle de acesso tornou-se muito mais seguro e flexível pela introdução do modelo de controle de acesso baseado em visão (VACM – View-based Access Control Model). O VCAM define um conjunto de serviços que uma aplicação em um agente podem usar para validar comandos de requisição e notificação.

3.7 O SMON

Um switch é um dispositivo de rede utilizado para reduzir a contenção e o congestionamento da rede, comumente verificados em redes compartilhadas. Os switches permitem também a comutação entre diferentes tecnologias (ethernet, token ring, fast ethernet, etc.). Além disso, é comum a implementação de VLANs (Virtual LAN ou Redes Locais Virtuais) em switches, de tal forma que diferentes redes locais possam coexistir em um mesmo equipamento e uma mesma rede local virtual possa ser implementada por vários equipamentos, desde que os mesmos obedeçam a um padrão. Neste sentido foi desenvolvido o padrão de identificação de VLAN IEE 802.1Q.

A principal diferença entre gerenciar uma rede local compartilhada e uma rede com switches é o nível de granularidade necessário. Em redes tradicionais, o monitoramento de desempenho, segurança e contabilização pode ser feito monitorando-se uns poucos pontos na rede, por onde flui o tráfego. Em redes que utilizam switches, aumenta enormemente o número de pontos, onde se faz necessário o monitoramento, porque cada switch pode conter vários segmentos de rede.

Para contornar os problemas gerados pela excessiva segmentação de redes baseadas em

switch, pela implementação de priorização de tráfego e também pela criação de VLANs, foi definido no RFC 2613 um padrão que estende o RMON para adequá-lo melhor ao gerenciamento de redes com switch. Este padrão foi inicialmente definido pela Lannet e denominado de SMON.

O SMON estende o conceito de fonte de dados, que na MIB II e RMON eram somente instâncias das interfaces, acrescentando VLANs e entidades físicas, conforme definido no RFC 2037, como a sub árvore 22 do RMON. Dessa forma, os grupos host e matrix do RMON e seus similares do RMON 2, devem ser estendidos para suportar as novas fontes de dados definidas no SMON.

4 Necessidades de Gerenciamento de Aplicações de Rede

Com a popularidade das redes de computadores hoje em dia, cada vez mais usuários utilizam diferentes aplicações de rede. O acesso à Internet hoje já não é mais considerado um privilégio de poucos, e há quem diga que no mundo moderno não se pode mais viver sem uma conexão à Internet.

Dentro das organizações, o uso mais intensivo de aplicações de rede mudou completamente o padrão de uso das redes de computadores. Se antigamente as pessoas utilizavam a rede para consultas esporádicas a bancos de dados ou para o uso compartilhado de um recurso caro, hoje as redes de computadores estão substituindo os meios de comunicação tradicionais, como o próprio telefone.

Basta tomar como exemplo o caso da Universidade Federal de Santa Catarina (UFSC). Hoje existem mais computadores na Universidade interligados em rede do que terminais telefônicos, e esta diferença tende a aumentar.

Com tanta utilização da rede de computadores nas mais diversas tarefas, é óbvio que o tráfego dentro da rede aumenta. Mas saber a quanto anda o tráfego não é suficiente para saber “o quê” os usuários estão fazendo.

É interessante conhecer quais são as aplicações que mais consomem largura de banda da rede, e que tipos de serviços de informações os usuários mais utilizam. Nos dias de hoje, é comum pensarmos que o maior tráfego dentro da rede seja gerado pelos serviços de informação disponíveis via WWW (World Wide Web). Entretanto, nada nos diz com certeza de que este serviço seja o maior devorador de largura de banda. Outros serviços essenciais como o terminal virtual (telnet), transferência de arquivos (ftp) e o correio eletrônico (e-mail) estão sendo utilizados a todo o momento.

Assim, para conhecer que aplicações são responsáveis por quais fatias de tráfego na rede, fazem-se necessários mecanismos que permitam ao gerente de rede obter estas informações. As aplicações de gerenciamento tradicionais somente são capazes de obter informações sobre o tráfego total de cada máquina, com detalhamento dos protocolos de transporte e de níveis inferiores.

Existem no mercado produtos que conseguem dar o tráfego recebido e enviado pelos serviços executados nas máquinas servidoras, mas isto não é suficiente. Nem sempre o

usuário está acessando máquinas servidoras da própria rede da organização. Portanto, medir tráfego nos servidores não mostra todo o tráfego das aplicações dos usuários pois, parte deste tráfego é direcionada para servidores em outras redes.

O gerenciamento de cada máquina cliente da rede poderia fornecer informações sobre o que o usuário está usando, e dentro de cada rede seria possível ter-se uma noção dos padrões de tráfegos das aplicações.

Dessa forma, o gerenciamento de aplicações de rede pode ter dois enfoques:

Gerenciamento das estações servidoras de aplicações, isto é, com enfoque nos serviços. Para esta situação já existe uma tentativa, proposta em janeiro de 1994 sob a forma da RFC 1565 [Kil 94] - Network Services Monitoring MIB. Esta proposta consiste de um módulo de MIB, em conformidade com a SMIv2, e que acrescenta 24 novos objetos para a monitoração de serviços de rede;

Gerenciamento das estações clientes, com enfoque nas atividades dos softwares clientes. Não existe ainda nenhuma proposta no IETF neste sentido, mas boa parte do trabalho pode ser aproveitada da RFC 1565 [Kil 94].

Segundo a RFC 1565 [Kil 94], o gerenciamento efetivo de serviços Internet deve satisfazer dois requisitos:

- Deve ser possível monitorar um grande número de componentes (tipicamente para uma grande organização); e
- O monitoramento de aplicações deve ser integrado ao gerenciamento de redes genérico.

Para satisfazer a estes dois requisitos, o módulo MIB proposto na RFC 1565 não inclui nenhum objeto que permita o controle dos serviços de rede em execução, para que a implementação seja facilitada. O monitoramento dos serviços de rede está integrado ao gerenciamento de redes genérico através do uso do modelo de gerenciamento SNMP.

Entretanto, o gerenciamento de aplicações nos clientes de rede pode exigir algumas situações onde sejam necessárias funções de controle. Assim, um agente construído para este fim deve ser capaz de:

- identificar as aplicações clientes de rede em execução;
- monitorar as conexões ativas das aplicações;
- coletar estatísticas de conexões e informações relacionadas;
- controlar o estado operacional das conexões;
- controlar o estado operacional de cada aplicação, sendo possível, por exemplo, suspender uma aplicação, restaurá-la ao estado normal, abortá-la, etc.;
- ser programado para reportar a ocorrência de eventos relativos a conexões de rede.

Um agente SNMP com estas características estaria envolvido em três áreas funcionais (segundo o modelo OSI) do gerenciamento de redes:

1. Performance: a coleta de estatísticas através das funções de monitoração permite o conhecimento do uso que os usuários fazem da rede;

2. Configuração: as funções de controle permitem que sejam configuradas nas máquinas clientes quais serviços de rede podem ou não ser utilizados. Tais configurações têm efeito no desempenho da rede;
3. Segurança: através das funções de controle e de reporte de eventos, a estação de gerenciamento pode ser notificada da tentativa de uma estação cliente conectar a hosts considerados não seguros, por exemplo.

4.1 Construção de novas MIBs

Criar novas definições de informação de gerenciamento é uma tarefa que deve tornar-se mais comum à medida que novas tecnologias surgem e à medida que a experiência com as tecnologias existentes é acumulada.

Definições de novos tipos de informação de gerenciamento podem ser criadas pelos engenheiros que criaram a nova tecnologia, pelos engenheiros que desenvolvem as aplicações para gerenciar a tecnologia, e pelos gerentes de marketing de produtos que representam as necessidades dos clientes (e usuários) do produto. Uma definição é bem sucedida se ela é largamente difundida e se agrega valor a sistemas de gerenciamento. O tempo tem mostrado que o sucesso inclui os seguintes ingredientes [Per 97]:

- A definição deve ser escrita e disponibilizada amplamente a um custo insignificante;
- Ela deve ser implementável por desenvolvedores de agentes;
- Ela deve ser implementável por desenvolvedores de aplicações de gerenciamento;
- As implementações de agentes e aplicações devem ser interoperáveis umas com as outras;
- Os resultados obtidos da aplicação devem possuir um valor maior do que o custo do sistema (e da rede) em termos de recursos necessários para executar a aplicação.

Para atingir estes objetivos, a pessoa ou grupo que esteja escrevendo as novas definições devem possuir uma certa experiência e habilidade com o assunto, incluindo [Per 97]:

- Conhecimento de como escrever definições válidas;
- Conhecimento da tecnologia a ser gerenciada;
- Compreensão de como a tecnologia precisa ser gerenciada;
- Compreensão dos custos de implementação de várias técnicas usadas para escrever definições tanto em agentes como em aplicações de gerenciamento;
- A habilidade de, concisa e precisamente, escrever as definições de forma que elas sejam interpretadas com o mesmo significado pela maioria dos leitores (pessoas) das definições;
- A habilidade de escrever as definições em um nível de abstração de forma que elas possam ser estendidas e aplicadas para áreas para as quais não se tinha pensado, e ainda em um nível de abstração que possa ser eficientemente entendido e aplicado à geração atual de tecnologia.

Novos objetos podem ser adicionados a uma MIB SNMP através de uma entre três maneiras diferentes [Sta 93]:

1. A sub-árvore mib-2 pode ser expandida ou completamente trocada por uma nova revisão (provavelmente seria chamada de mib-3). Um exemplo de expansão da MIB é a RMON MIB [Wal 95];
2. Uma MIB experimental pode ser construída para uma aplicação particular. Tais objetos podem ser subseqüentemente movidos para a sub-árvore mgmt. Exemplos disso são as várias MIBs específicas a tipos de enlaces que têm sido definidas, como a IEEE 802.5 token ring LAN (RFC 1231);
3. Extensões privadas podem ser adicionadas à sub-árvore private. Uma que está documentada em uma RFC é a MUX (multiplexer) MIB (RFC 1227).

5 Gerência de Redes de Telecomunicações

As operadoras de serviços de telecomunicações passam por uma fase de transição entre um ambiente de monopólio para um ambiente onde a desregulamentação do mercado incentiva a concorrência e a oferta de novos e sofisticados serviços. A sobrevivência neste mercado requer um conhecimento sólido das tecnologias emergentes e uma visão clara de como administrar os recursos existentes para aumentar a relação entre o custo do sistema implantado e a receita obtida junto aos usuários.

Caso o fator qualidade não estivesse envolvido, este relacionamento seria facilmente equacionado. No entanto, quando se deseja um relacionamento envolvendo os três fatores custo X qualidade X lucro, é fundamental que se tenha uma política de gerenciamento com objetivos bem definidos e com uma perfeita integração das informações vitais para o alcance de um resultado satisfatório.

O ambiente de telecomunicações é bastante complexo para que se tenha uma visão simplista de administração. Neste sentido, o ITU-T apresentou uma série de recomendações que visam organizar este ambiente e orientar as operadoras e fornecedores de equipamentos e serviços de telecomunicações através de um modelo de gerenciamento. No entanto, uma das tarefas mais difíceis consiste, exatamente, em organizar este conjunto de informações de forma a torná-lo aplicável em um ambiente real de uma rede de telecomunicações.

Em primeiro lugar, é importante ficar claro que o gerenciamento de um ambiente de telecomunicações foi estruturado segundo uma hierarquia composta de 5 níveis e ilustrada pela figura 5.1:

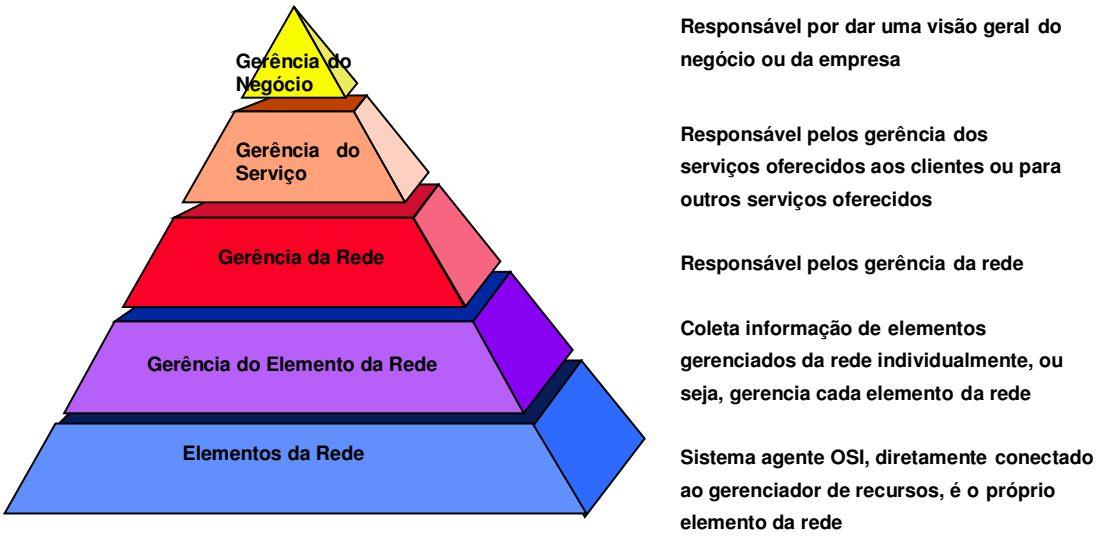


Figura 5.1 - Hierarquia de gerenciamento

Entender esta hierarquia é o primeiro passo para se chegar a um sistema de gerenciamento eficaz. Esta hierarquia é aplicável não só no ambiente de Telecomunicações mas, também, em qualquer ambiente que tenha uma rede como suporte às suas atividades.

Em primeiro lugar, deve ficar bem claro qual o negócio da empresa. No caso de uma empresa operadora de serviços de telecomunicações, fica óbvio que o negócio é o fornecimento de serviços de telecomunicações e que este fornecimento deve ser realizado de forma competitiva e que deve apresentar resultados satisfatórios em termos de receita. Gerenciar um negócio de telecomunicações implica em investimentos em novas tecnologias para o fornecimento de novos serviços antes mesmo que estes serviços sejam exigidos pelos usuários. É fundamental, portanto, que existam ferramentas para possibilitar o planejamento de novos serviços, amparadas por um eficiente estudo de tendências de mercado. Fica claro que, neste contexto, devem ser utilizadas as técnicas de marketing e administração como seriam utilizadas em qualquer outra empresa, independentemente do tipo de negócio a que ela se dedica.

Uma vez identificados os objetivos a serem alcançados pela empresa, deve-se focalizar o conjunto de serviços de telecomunicações que serão comercializados. Nesta etapa, é importante que se defina claramente quais os objetivos de cada um dos serviços em termos de funcionalidades, disponibilidade, custo, qualidade e, se possível, tempo de vida. De posse destas informações, é possível planejar a tarifação de cada serviço, considerando-se fatores tais como número de usuários, níveis de qualidade oferecidos e até mesmo a existência de serviços alternativos.

A oferta de um serviço de telecomunicação depende da existência de tecnologias que o suportem e do custo destas tecnologias. Muitas vezes um determinado serviço possui custos proibitivos e a empresa deve aguardar pelo surgimento de soluções alternativas ou mesmo, caso este seja um dos objetivos da empresa, investir em pesquisas por novas soluções.

Uma vez instalado, um serviço de telecomunicação deve ser constantemente observado para a identificação de fatores que possam influenciar em seu desempenho. A gerência de um serviço de telecomunicação implica, portanto, em uma contínua monitoração de parâmetros relacionados com taxa de utilização, disponibilidade, qualidade, custos associados e desempenho. Os desvios observados devem ser corrigidos o mais rapidamente possível, a fim de evitar perdas de receitas ou mesmo descontentamento de seus usuários. Para que a gerência de um serviço seja completa, é necessário que o sistema de gerência tenha acesso às informações relativas à infraestrutura de suporte ao serviço. Problemas relacionados com a infraestrutura de suporte devem ser reportados ao sistema de gerência do serviço para que ações corretivas ou alternativas sejam realizadas.

6 A arquitetura de gerenciamento OSI

A arquitetura de gerenciamento OSI define:

- ⇨ as estruturas de gerenciamento passíveis de serem empregadas
- ⇨ os componentes de um sistema de gerenciamento
- ⇨ a estrutura da informação de gerenciamento
- ⇨ os serviços e protocolos para troca de informações de gerenciamento

6.1 Estruturas de gerenciamento

A estrutura de gerenciamento refere-se aos três enfoques definidos pela ISO em seu "framework" [ISO 7498-4]: Gerenciamento de Sistemas, Gerenciamento de Camada e Operação de Camada.

O Gerenciamento de Sistemas, conforme apresentado na figura 5.1, foi idealizado para monitorar e controlar o sistema como um todo. Para tanto, prevê funções de gerenciamento em todas as camadas da pilha de protocolos e seu escopo de abrangência é o mais completo.

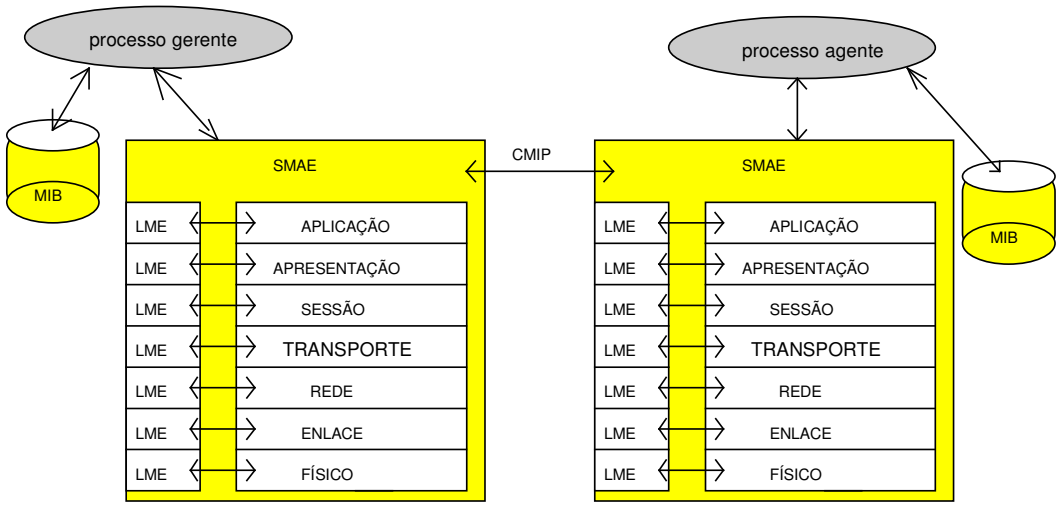


Figura 6.1 Gerenciamento de Sistemas

O Gerenciamento de Camada consiste na monitoração e controle dos recursos de uma camada de forma isolada e independente, conforme ilustrado na figura 5.2. Pode-se, por exemplo, enfocar aspectos da camada de transporte, analisando-se o número de conexões estabelecidas com sucesso e o número de tentativas, sem sucesso, de estabelecimento de conexões, para identificar situações de sobrecarga ou ociosidade nos sistemas. Esta abordagem, no entanto, não contempla um relacionamento com as atividades das outras camadas de protocolo; ela é útil para controlar recursos que, por sua natureza, não suportam uma arquitetura completa (todas as sete camadas do RM-OSI).

Figura 5.2 Gerenciamento de Camada

A estrutura de Operação de Camada, mostrada na figura 5.3, restringe-se à monitoração e controle de uma única instância de comunicação. Neste caso, as informações de gerenciamento são concernentes à uma conexão. Por exemplo, na camada de transporte, pode-se ter várias conexões ativas; a operação de camada trata da gerência de cada uma destas conexões, de forma independente. Esta estrutura se aplica quando é desejável que, por exemplo, o usuário fique encarregado de gerenciar a sua própria conexão.

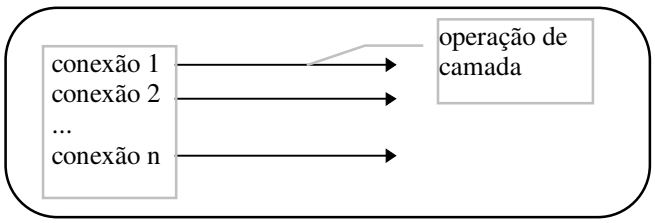


Figura 5.3 Operação de Camada

6.2 Componentes de gerência OSI

O ambiente de gerenciamento OSI é composto por elementos gerenciados, agentes e gerentes. Os elementos gerenciados são representados por objetos gerenciados, seguindo o paradigma da Abordagem de Orientação a Objetos. Os agentes e gerentes são entidades usuárias do serviço de gerenciamento OSI e são denominados de MIS-Users (Management Information Service - Users). Os papéis assumidos por estas entidades não são fixos, isto é, um MIS-User pode executar o papel de gerente em um contexto, definido por uma associação, e um papel de agente em outro contexto, definido por outra associação. A figura 2.4 ilustra um possível cenário de um ambiente de gerenciamento OSI.

No modelo de gerenciamento OSI, o número de associações estabelecidas entre os MIS-User é considerado uma questão local, dependente de implementação. Conforme mostra a figura 5.4, pode-se ter um gerente associado a vários agentes e um agente associado a vários gerentes. Estas associações são estabelecidas com a finalidade de trocar informações de gerenciamento.

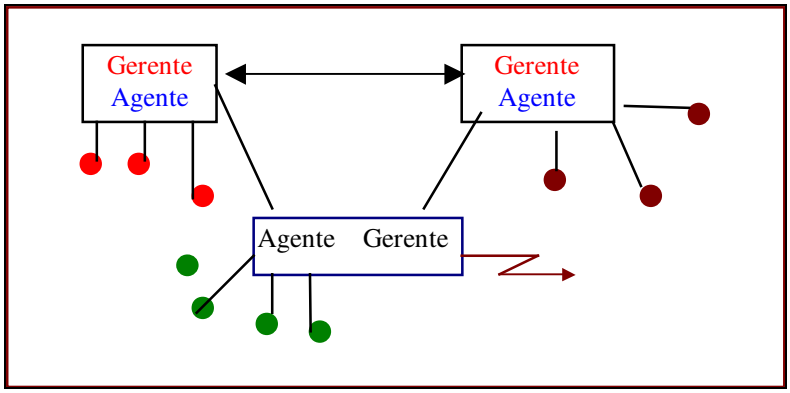


Figura 5.4 Componentes do Gerenciamento OSI

6.3 Estrutura da informação de gerenciamento

As informações de gerenciamento são organizadas em bases de dados. O conjunto das bases de dados de informações de gerenciamento é denominado MIB (Management Information Base), e a sua implementação não está sujeita à padronização. As informações são definidas segundo uma SMI (Structure Management Information). No modelo de

gerenciamento OSI, a SMI estabelece que a forma de representação das informações deve seguir o modelo de orientação a objetos, considerando três hierarquias: hierarquia de herança, hierarquia de nomeação ou de containment e hierarquia de registro.

6.4 Serviços e protocolos de comunicação

A comunicação entre as entidades de gerenciamento Gerente e Agente é realizada pelo protocolo CMIP (Common Management Information Protocol), definido em [ISO/IEC 9596].

No caso especial de gerenciamento de redes de telecomunicações, também é permitida a utilização do protocolo FTAM (File Transfer Access and Management) para a transferência de informações de gerenciamento entre agentes e gerentes. Esta facilidade tornou-se essencial devido à necessidade de transferência de grandes quantidades de dados neste ambiente.

Os serviços de gerenciamento disponíveis para as entidades gerentes e agentes são definidos pelo CMIS (Common Management Information Service), descrito em [ISO/IEC 9595]. Neste documento são definidos dois serviços de gerenciamento: o serviço de operações de gerenciamento e o serviço de notificações de gerenciamento. As operações de gerenciamento são emitidas pelos MIS-Users (Management Information Service - Users), que são entidades de gerenciamento no papel de gerente; as notificações são emitidas pelos MIS-Users (Management Information Service - Users) que assumem o papel de agente. A figura 5.5 mostra um cenário de comunicação onde são trocadas operações e notificações de gerenciamento.

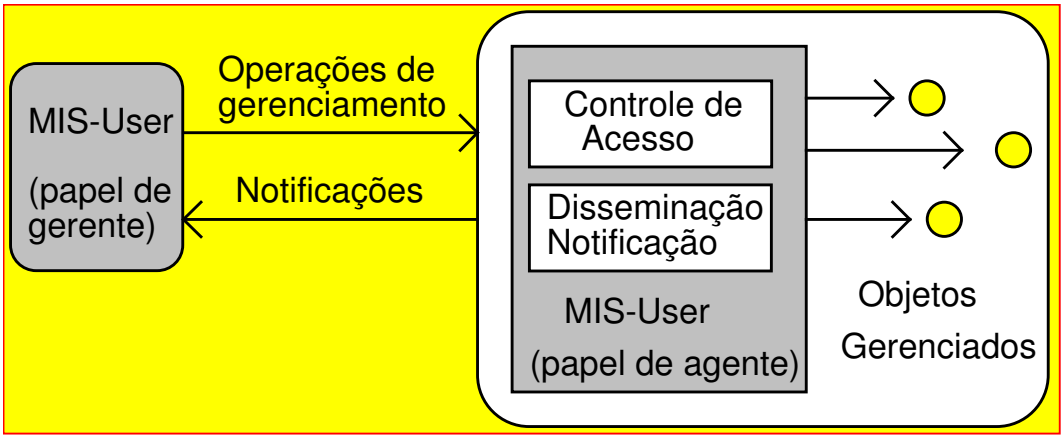


Figura 5.5 Serviços de Gerenciamento

As operações de gerenciamento podem sofrer um controle de acesso dependendo da especificação dos objetos gerenciados, isto é, dependendo da definição do objeto, a operação pode ter sucesso ou ser negada ao MIS-User solicitante. Na figura 5.5, observa-se que existe uma função de controle de acesso associada ao MIS-User agente. Esta função

tem como objetivo principal, autenticar o Gerente na solicitação de uma associação e verificar sua autoridade na execução de operações de gerenciamento. Mais detalhes desta função serão apresentados no capítulo 5 onde é descrita a Função de Controle de Acesso no Modelo Funcional de Gerenciamento OSI.

As notificações representam informações sobre eventos ocorridos no sistema gerenciado e são enviadas ao destinatário através da utilização do serviço M-EVENT-REPORT, definido no CMIS. Na figura 5.5, pode-se observar a função de disseminação de notificações que consiste em um suporte funcional ao MIS-User agente para a identificação dos destinatários para os quais devem ser repassadas as notificações geradas pelos objetos gerenciados. A tabela 5.1 mostra as primitivas de serviço de gerenciamento definidas pelo CMIS.

Embora uma notificação possa ser gerada como efeito colateral de uma operação de gerenciamento, ela não pode ser considerada como uma resposta a uma operação. As operações de gerenciamento são emitidas por iniciativa de um gerente. Se uma operação de gerenciamento for solicitada no modo confirmado, então ela será respondida através das primitivas response e confirm; caso contrário, nenhuma resposta será gerada. Uma notificação é emitida por iniciativa do MIS-User agente que, por sua vez, pode solicitar este serviço no modo confirmado ou não confirmado.

Tabela 5.1 Serviços de Gerenciamento

Tipo de serviço	Modo de requisição	Primitivas	Semântica
M-CANCEL-GET (operação)	confirmado	request/indication response/confirm	Cancelar uma operação de leitura realizada sobre vários objetos
M-GET (operação)	confirmado	request/indication response/confirm	Ler valores de atributos de objetos
M-SET (operação)	confirmado	request/indication response/confirm	Modificar valores de atributos de objetos
	não confirmado	request/indication	
M-CREATE (operação)	confirmado	request/indication response/confirm	Criar uma instância de objeto
M-ACTION (operação)	confirmado	request/indication response/confirm	Solicitar que uma ação pré-definida seja executada por um objeto
	não confirmado	request/indication	
M-DELETE (operação)	confirmado	request/indication response/confirm	Destruir uma instância de objeto
	não confirmado	request/indication	
M-EVENT-REPORT (notificação)	confirmado	request/indication response/confirm	Notificar a ocorrência de um evento a um sistema gerente
	não confirmado	request/indication	

		n	

Resumo

Pode-se resumir este conjunto de definições, da seguinte forma:

As estruturas de gerenciamento que podem ser empregadas no modelo de gerenciamento OSI são: Gerenciamento de Sistemas (abrange todas as camadas), Gerenciamento de Camada (abrange apenas uma camada) e Operação de Camada (abrange apenas uma instância de comunicação).

Os componentes de um sistema de gerenciamento OSI são: MIS-Users (que podem assumir o papel de Gerente ou de Agente), e os Objetos Gerenciados (que representam os recursos sujeitos ao gerenciamento).

Os Serviços de Gerenciamento disponíveis são as Operações e as Notificações. Dependendo de sua natureza, podem ser solicitados no modo confirmado ou não confirmado.

O Protocolo para transferência das informações de gerenciamento é o CMIP e, no caso de Sistemas de Telecomunicações, pode ser utilizado o protocolo FTAM em lugar do CMIP.

A Informação de Gerenciamento é definida seguindo a AOO-Abordagem de Orientação a Objetos e é armazenada em uma MIB.

7 Serviços de suporte à comunicação

A camada de aplicação OSI é definida para suportar diferentes aplicações. No modelo de referência OSI, é a camada que dá suporte para os aplicativos (ou aplicações) dos usuários. Os aplicativos é que fazem o verdadeiro trabalho para o qual os computadores foram adquiridos. Os aplicativos utilizam-se dos serviços da camada de aplicação para suas necessidades de comunicação.

Um Processo de Aplicação (AP - Application Process) é um processo que “roda” na camada de aplicação e uma Entidade de Aplicação (AE) representa os aspectos de comunicação dos processos de aplicação.

Vários agrupamentos de funcionalidades foram definidos para preencher as necessidades das aplicações. Um elemento de serviço de aplicação (ASE - *Application Service Element*) é um agrupamento que suporta um conjunto de necessidades de comunicação de uma aplicação. Cada AE é composta por um ou mais elementos de serviço de aplicação (ASEs). Alguns exemplos de ASEs são o ACSE - *Association Control Service Element* (usado para estabelecer e gerenciar uma associação entre entidades pares de aplicação), o ROSE - *Remote Operation Service Element* (usado para a execução de operações remotas), o RTSE - *Reliable Transfer Service Element* (oferecendo um serviço de transferência confiável), o CCR - Commitment Concurrency and Recovery (que possibilita a execução de várias operações de uma forma atômica).

Alguns processos de aplicação (APs), tais como o FTAM - *File Transfer Access Management* (usado para a transferência e manipulação remota de arquivos) e o MHS - Message Handling System (usado para a transferência e manipulação de mensagens) também são utilizados por outras aplicações devido às facilidades que eles oferecem.

7.1 Elementos de Serviço para aplicações de gerenciamento

Uma aplicação de gerenciamento, como qualquer outra aplicação no Modelo OSI, utiliza-se dos serviços oferecidos pelos elementos de serviço ASEs (*Application Service Element*) da camada 7 do RM-OSI (*Reference Model - Open System Interconnection*).

Para o caso especial da aplicação de gerenciamento, dois elementos de serviço genérico são necessários: o ACSE (*Association Control Service Element*), que oferece serviços para o estabelecimento e controle das associações de gerenciamento e o ROSE (*Remote Operations Service Element*) que fornece serviços para a execução de operações remotas.

Além destes elementos de serviço, dois outros são definidos para dar suporte às aplicações de gerenciamento: o CMISE (*Common Management Information Service Element*) e o SMASE (*System Management Application Service Element*).

O CMISE é constituído de uma descrição de serviços (CMIS) e da definição do protocolo de gerenciamento CMIP. Os serviços obrigatórios oferecidos por este elemento de serviço possibilitam a criação de um objeto (serviço M-CREATE), a destruição de um objeto (serviço M-DELETE), a execução de uma ação sobre um objeto (serviço M-ACTION), a leitura de valores de atributos de um objeto (serviço M- GET) e a modificação de valores dos atributos de um objeto (serviço M-SET). Embora o CMISE tenha sido desenvolvido para dar suporte ao gerenciamento de entidades de comunicação OSI, devido ao poder de suas facilidades, tem sido aplicado, também, no gerenciamento de redes de telecomunicações. Uma descrição mais detalhada deste elemento de serviço é realizada no capítulo 4.

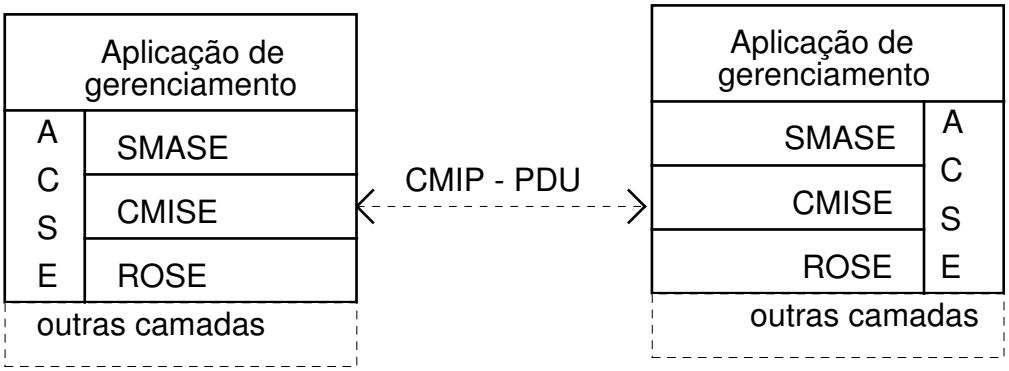
O SMASE é um elemento de serviço que apresenta facilidades relacionadas com a funcionalidade da aplicação de gerenciamento. Nele estão agrupados os serviços oferecidos pelas funções de gerenciamento definidas na série de recomendações ISO/IEC 10164 - X | ITU-T X.700. Existem várias funções de gerenciamento definidas e, entre elas, a função de gerenciamento de objetos OMF - *Object Management Function* assume um papel fundamental no cenário do gerenciamento por oferecer serviços de "*pass-throught"* para as demais funções de gerenciamento acessarem os serviços CMIS. Esta função e as demais funções que compõem o SMASE serão abordadas no capítulo 5. Para efeitos de clareza na descrição do fluxo da informação de gerenciamento, basta, por enquanto, observar a tabela 6.1 que mostra como os serviços de gerenciamento podem ser solicitados para o SMASE (através da OMF) e o seu respectivo mapeamento para as primitivas de serviço do CMISE.

Tabela 7.1 - Serviço de *Pass-throught*

Serviço solicitado	Serviço de "pass-throught" da OMF	Serviços do CMISE
Criação de objeto: Create	PT-CREATE	M-CREATE
Destruição de objeto: Delete	PT-DELETE	M-DELETE
Ação sobre um objeto: Action	PT-ACTION	M-ACTION
Modificação de valor de atributo: Replace	PT-SET	M-SET
Modificação de valor de atributo: Replace-with-default	PT-SET	M-SET
Modificação de valor de atributo: Add	PT-SET	M-SET
Modificação de valor de atributo: Remove	PT-SET	M-SET
Leitura de valor de atributo: Get	PT-GET	M-GET
Notificação	PT-EVENT-REPORT	M-EVENT-REPORT

Na figura 7.1 estão representados os elementos de serviço **ACSE**, **ROSE**, **SMASE** e **CMISE**, utilizados por uma aplicação de gerenciamento, com as respectivas primitivas de serviço.

Para garantir um perfeito entendimento do fluxo das informações de gerenciamento trocadas entre gerentes e agentes, é necessário conhecer, com detalhes, os elementos de serviço envolvidos. Com este objetivo, os ítens 7.1.1 e 7.1.2 apresentam aspectos importantes dos elementos de serviço ACSE e ROSE.



Primitivas oferecidas pelos elementos de serviço:

ACSE	**ROSE**	**SMASE (OMF)**	**CMISE**
A-ASSOCIATE	RO-INVOKE	PT-GET	M-GET
A-RELEASE	RO-RESULT	PT -SET	M-SET
A-ABORT	RO-ERROR	PT -CANCEL-GET	M-CANCEL-GET
	RO-REJECT	PT -ACTION	M-ACTION
		PT -CREATE	M-CREATE
		PT -DELETE	M-DELETE
		PT -EVENT-REPORT	M-EVENT-REPORT

Figura 7.1 Elementos de Serviço para o suporte às aplicações de gerenciamento

7.1.1. *Controle de Associação (ACSE)*

A função principal do ACSE é prover facilidades básicas para o controle de uma associação de aplicação entre duas entidades de aplicação, as quais se comunicam por meio de uma conexão realizada na camada de apresentação.

Os serviços ACSE são providos pelo uso do protocolo ACSE em conjunto com os serviços P-CONNECT, P-RELEASE, P-U-ABORT e P-P-ABORT da camada de apresentação.

A fim de efetuar o controle de uma associação de aplicação, o ACSE provê os seguintes serviços:

A-ASSOCIATE usado para prover o início do uso de uma associação. Este é um serviço confirmado e possui os seguintes parâmetros:

Modo;

Nome do Contexto de Aplicação;

Título do AP(Application Process) Chamador;

Qualificador da AE Chamadora;

Identificador de Invocação do AP Chamador;

Identificador de Invocação da AE Chamadora;

Título do AP Chamado;

Qualificador da AE Chamada;

Identificador de Invocação do AP Chamado;

Identificador de Invocação da AE Chamada;

Título do AP Respondente;

Qualificador da AE Respondente;

Identificador de Invocação do AP Respondente;

Identificador de Invocação da AE Respondente;

Informação do Usuário;

Resultado;

Fonte do Resultado;

Diagnóstico;

Endereço de Apresentação Chamador;

Endereço de Apresentação Chamado;

Endereço de Apresentação Respondente;

Lista de Definição do Contexto de Apresentação;

Lista do Resultado de Definição do Contexto de Apresentação;

Nome do Contexto de Apresentação Default;

Resultado do Contexto de Apresentação;

Default;

Qualidade do Serviço;

Requerimentos de Apresentação;

Requerimentos de Sessão;

Número Serial do Ponto de Sincronização Inicial;

Especificação Inicial de Tokens;

Identificador de Conexão de Sessão.

A-RELEASE: usado por um usuário de serviços ACSE para prover a finalização normal do uso de uma associação. Opcionalmente, o usuário receptor pode responder negativamente ao pedido de finalização da associação. Este é um serviço confirmado e possui os seguintes parâmetros:

Razão;

Informação do Usuário;

Resultado.

A-ABORT: um usuário de serviços ACSE se utiliza deste serviço para provocar a liberação anormal de uma associação, com possível perda de informação. Este é um serviço não confirmado e possui os seguintes parâmetros:

Fonte do Aborto;

Informação do Usuário.

A-P-ABORT: usado pelo provedor de serviços ACSE para indicar a liberação anormal de uma associação, a qual é provocada por problemas em serviços das camadas inferiores à camada de aplicação. Sua ocorrência indica uma possível perda de informação. Este é um serviço iniciado pelo provedor e possui o seguinte parâmetro:

Razão do Provedor.

A cada usuário ACSE está associada uma máquina de protocolo de controle de associação (ACPM) que irá prover os serviços ACSE através da camada de apresentação. Dados específicos das primitivas de serviço são passados através das unidades de dados do protocolo de aplicação (APDUs), conforme ilustrado na tabela 6.2.

Tabela 7.2 Mapeamento das primitivas de serviço do ACSE em APDUs

Primitiva	APDU
A-ASSOCIATE. Request	AARQ
A-ASSOCIATE. Response	AARE
A-RELEASE. Request	RLRQ
A-RELEASE.response	RLRE
A-ABORT. Request	ABRT

Essas APDUs são enviadas como dados de usuário nas primitivas dos serviços de apresentação.

Conforme descrito anteriormente, o ACSE é o elemento de serviço que gerencia associações entre processos de aplicação. Uma associação corresponde a uma conexão de apresentação com a adição de alguma semântica da camada de aplicação. Cada associação estabelecida é específica a uma dada aplicação. Todas as entidades de aplicação OSI contêm um ACSE, uma vez que, até a presente data, todas as aplicações definidas pelo RM-OSI são orientadas à conexão.

A entidade que solicita um pedido de associação de aplicação é chamada de entidade iniciadora e a entidade que aceita um pedido de associação de aplicação é chamada de entidade respondedora.

Uma vez que o conceito de embedding é empregado nas três camadas superiores, conexões de aplicação, apresentação e sessão ocorrem ao mesmo tempo.

Os serviços do ACSE são alcançados pela invocação de suas primitivas de serviço, relacionadas na tabela 7.3.

Tabela 7.3 Primitivas do ACSE

Primitiva	serviço oferecido	tipo de serviço
A-ASSOCIATE	Estabelece uma associação	confirmado
A-RELEASE	Libera uma conexão	confirmado
A-ABORT	Encerramento iniciado pelo usuário	não confirmado
A-P-ABORT	Encerramento iniciado pelo provedor	só indicação

7.1.2. *Operações Remotas (ROSE)*

O elemento de serviço ROSE oferece serviços de suporte às aplicações interativas. De uma forma geral, opera de maneira equivalente a uma chamada de procedimento remoto (RPC - Remote Procedure Call).

Este elemento de serviço é bastante útil no suporte às aplicações distribuídas.

Existe sempre uma aplicação que solicita a execução de uma operação a outra aplicação, que pode devolver ou não o resultado correspondente.

A entidade que solicita uma operação é chamada entidade invocadora e a que recebe a solicitação é chamada entidade executora.

É importante observar que as entidades de aplicação somente podem utilizar os serviços do ROSE se já houver uma associação de aplicação estabelecida. Neste caso, podem existir 3 classes de associação:

Classe 1: somente a entidade iniciadora da associação pode invocar operações.

Classe 2: somente a entidade respondedora da associação pode invocar operações.

Classe 3: ambas as entidades, iniciadora e respondedora da associação, podem invocar operações.

São definidas, também, cinco classes de operação, que são caracterizadas pelo tipo de interação (síncrona ou assíncrona) e pelo comportamento da entidade executora. O tipo de interação diz respeito à forma como a entidade iniciadora se comporta após a solicitação de uma operação, isto é, se fica bloqueada aguardando o resultado da operação (operação síncrona) ou se fica livre para executar outras operações (operação assíncrona). O comportamento da entidade executora é modelado em termos de emissão de uma resposta à operação (sucesso ou falha da operação) ou se nenhum resultado é emitido (operação não confirmada). A tabela 7.4 ilustra as possíveis classes de operações no ROSE.

Tabela 7.4 - Classes de operação definidas no ROSE

Classe de operação	Tipo de interação	Forma de resposta
Operação classe 1	síncrona	relatando sucesso ou falha
Operação classe 2	assíncrona	relatando sucesso ou falha
Operação classe 3	assíncrona	relatando somente falha
Operação classe 4	assíncrona	relatando somente sucesso
Operação classe 5	assíncrona	resultado não relatado

O ROSE geralmente é utilizado por aplicações envolvendo o serviço de mensagens MHS (*Message Handling Service*), o serviço de diretório DS (*Directory Service*) ou o serviço de informação de gerenciamento CMIS. O usuário do ROSE dispõe de um conjunto de primitivas de serviço descritas na tabela 6.5.

Tabela 7.5 - Primitivas de serviço do ROSE

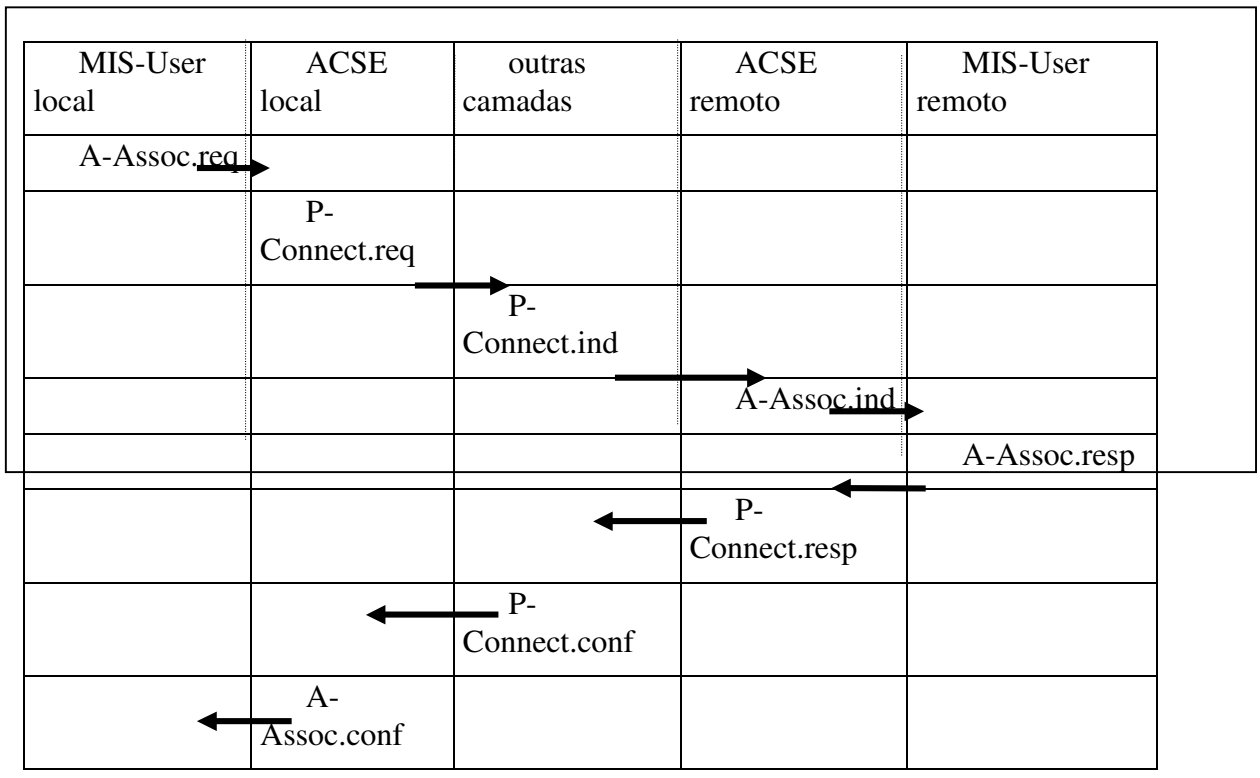
Primitiva	Significado	Tipo de serviço
RO-INVOKE	Invoca uma operação	não confirmada
RO-RESULT	Resultado de operação bem sucedida	não confirmada
RO-ERROR	Resultado de operação sem sucesso	não confirmada
RO-REJECT-U	Rejeição iniciada pelo usuário	não confirmada
RO-REJECT-P	Rejeição iniciada pelo provedor	só indicação

Protocolo ROSE

Para cada serviço iniciado pelo usuário do ROSE é criada uma APDU ROSE, que é mapeada para a primitiva RT-TRANSFER do RTSE ou para o serviço P-DATA de apresentação.

7.2 Fluxo da informação de gerenciamento

Uma aplicação de gerenciamento (exercendo o papel de gerente ou de agente), solicita uma associação com uma entidade par, através da primitiva de serviço de associação A-ASSOCIATE.request oferecida pelo ACSE, indicando as unidades funcionais que suporta e outras informações relevantes para a associação a ser estabelecida. A entidade par responde ao pedido através da primitiva A-ASSOCIATE.response, confirmando ou negando o estabelecimento da associação. A fase de troca de informações de gerenciamento só pode ser iniciada caso a associação tenha sido estabelecida com sucesso. Na resposta afirmativa para o estabelecimento da associação, a entidade respondedora confirma ou restringe o conjunto das funcionalidades que podem ser utilizadas nesta instância de associação. A figura 7.2 mostra um exemplo de fluxo de informações em uma associação entre duas entidades de aplicação de gerenciamento.



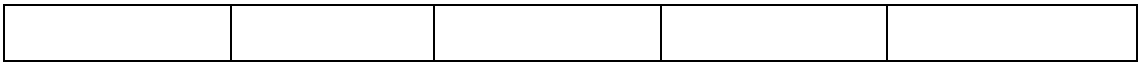
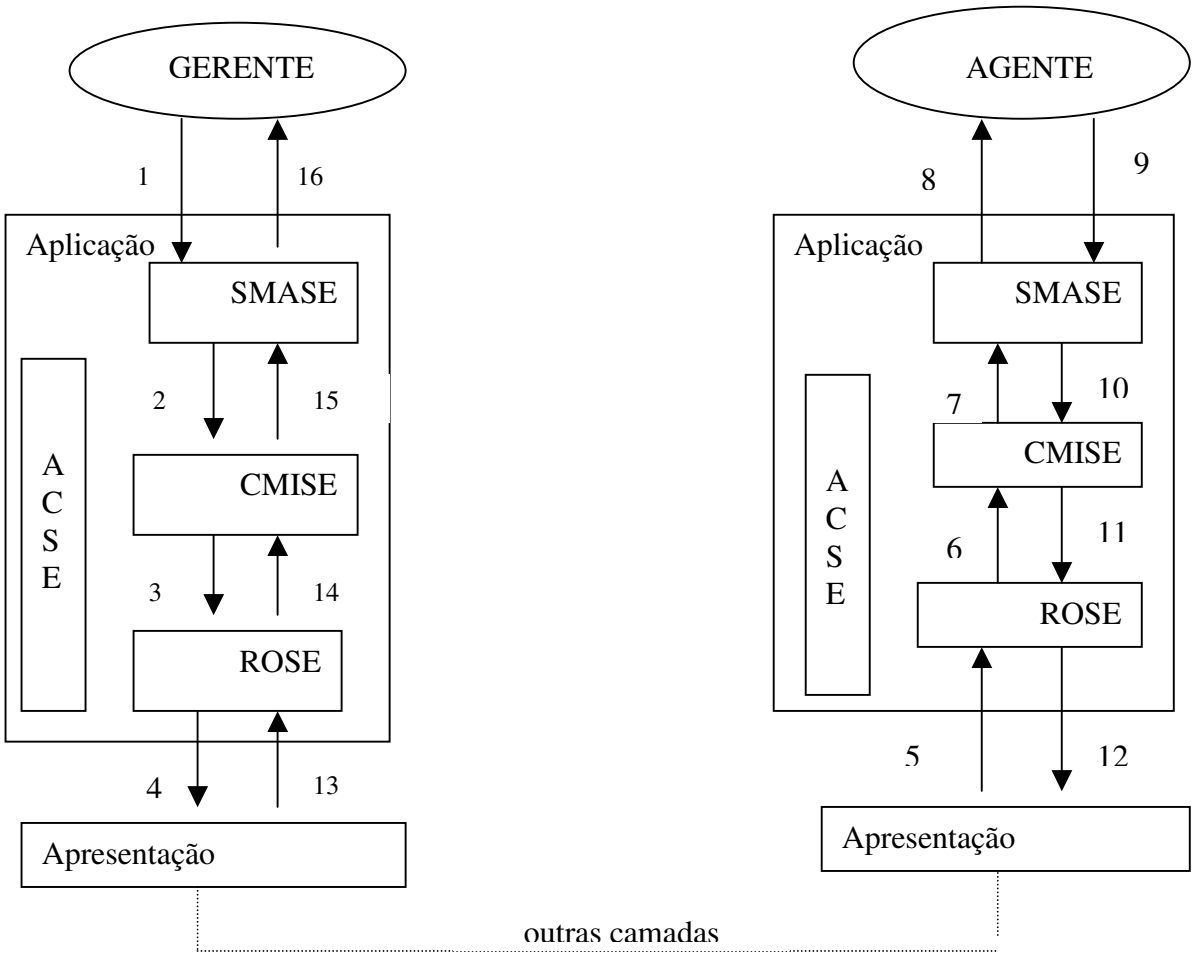


Figura 7.2 - Fase de Associação entre dois MIS-Users

O elemento de serviço CMISE é composto da especificação de um conjunto de serviços denominado CMIS (*Common Management Information Service*) e de um protocolo denominado CMIP (*Common Management Information Protocol*). O CMIS é composto de um conjunto de primitivas que oferecem serviços para a criação (*M-CREATE*) e destruição (*M-DELETE*) de objetos gerenciados, para a execução de ações (*M-ACTION*) sobre objetos gerenciados e, ainda, operações de leitura (*M-GET*) e modificação (*M-SET*) de valores de atributos de objetos gerenciados. Um serviço para o cancelamento de um pedido de leitura de valores de atributos de vários objetos (*M-CANCEL-GET*) é oferecido de modo opcional, isto é, o suporte a este serviço não é obrigatório.

As operações e notificações de gerenciamento são solicitadas diretamente ao CMISE (que utiliza os serviços oferecidos pelo ROSE) ou, em sistemas que apresentam alguma funcionalidade, ao SMASE. O CMISE utiliza os serviços oferecidos pelo ROSE para transferir as operações e notificações para o MIS-User remoto. No caso de serem solicitadas ao SMASE, estas são repassadas por um serviço de *Pass-Through* para o CMISE. O serviço de *Pass-Through* para as operações e notificações de gerenciamento é oferecido pela Função de Gerenciamento de Objetos, denominada OMF (*Object Management Function*). A figura 7.3 mostra o cenário de comunicação entre dois MIS-Users, na solicitação de uma leitura de valor de atributo.



Do Gerente para o Agente	Do Agente para o Gerente
PT-Get. request	PT-Get. response
M-GET. request	M-Get. response
RO-INVOKE. request	RO-RESULT. request
P-Data. request	P-Data. request
P-Data.indication	P-Data. indication
RO-INVOKE.indication	RO-RESULT. indication
M-Get. indication	M-Get.confirm
PT-Get. indication	PT-Get.confirm

Figura 7.3 – Cenário de comunicação para a operação de leitura de valor de atributo

7.3 Conhecimento de Gerenciamento Compartilhado

Quando duas entidades de aplicação de gerenciamento estabelecem uma associação para troca de informações de gerenciamento, é necessário que seja identificado um Conhecimento de Gerenciamento Compartilhado (SMK - *Shared Management Knowledge*) a fim de garantir uma compatibilidade entre os dois sistemas comunicantes. Um conhecimento de gerenciamento compartilhado inclui:

- informações sobre os objetos gerenciados que são visíveis para aquela aplicação;
- o protocolo a ser utilizado na troca de informações de gerenciamento;
- as funções e unidades funcionais suportadas;
- as restrições nas unidades funcionais.

Os objetos gerenciados visíveis para uma determinada aplicação, constituem uma visão da MIB e as informações sobre eles incluem as classes às quais eles pertencem, identificação das instâncias e restrições de acesso.

O protocolo de gerenciamento a ser utilizado pode ser o CMIP ou o FTAM ou ainda algum outro protocolo que possa vir a ser definido no futuro.

As unidades funcionais são, portanto, as unidades básicas de negociação entre MIS-Users e consistem em agrupamentos de serviços de funções de gerenciamento. Uma funcionalidade pode ser alcançada em uma ou mais unidades funcionais; neste caso, algumas restrições podem ser estabelecidas.

Unidades funcionais que atravessam os limites de uma função, podem suportar os seguintes conjuntos de capacidades:

- somente notificações;
- somente operações de gerenciamento;
- notificações e operações de gerenciamento.

As Unidades Funcionais definidas até o momento, são:

- Kernel (obrigatória) oferece os serviços de criação e destruição de objetos gerenciados, execução de uma ação sobre um objeto gerenciado, leitura e modificação de valores de atributos e emissão de notificações.
- *Cancel Get* (opcional) permite o cancelamento de uma operação de leitura quando esta for realizada sobre múltiplos objetos.
- *Scoping* (opcional) fornece a facilidade de seleção de um conjunto de objetos sobre os quais uma determinada operação de gerenciamento deve ser aplicada. Esta unidade funcional só pode ser utilizada se a unidade funcional *Multiple Objects Selection* também tiver sido selecionada para utilização. O escopo pode ser definido

considerando-se uma sub-árvore completa ou apenas um nível particular da sub-árvore. A raiz da sub-árvore é indicada pelo identificador de um objeto gerenciado (chamado, neste caso, de objeto gerenciado base).

- *Filter* (opcional) fornece a possibilidade de se estabelecer condições que devem ser satisfeitas por um objeto gerenciado a fim de que a operação de gerenciamento possa ser executada sobre ele.
- *Multiple Reply* (opcional) permite que várias respostas sejam emitidas a partir de uma única operação de gerenciamento. As várias respostas são relacionadas através de um parâmetro denominado *linked-id*. Um exemplo da utilização desta unidade funcional é o caso onde uma ação de teste é solicitada a um sistema gerenciado e deseja-se receber informações durante a execução do teste.
- *Multiple Objects Selection* (opcional) permite que uma única operação de gerenciamento seja executada sobre mais do que um objeto gerenciado. Deve ser utilizada em conjunto com a unidade funcional *Scoping*.

De acordo com a norma X.700, o conhecimento de gerenciamento pode ser estabelecido antes da associação, durante o estabelecimento da associação ou ainda, durante o tempo de vida da associação. A figura 6.4 apresenta uma visão do conhecimento de gerenciamento compartilhado entre duas entidades de aplicação de gerenciamento.

No exemplo da figura 7.4, três unidades funcionais foram negociadas para utilização: *Multiple Objects Selection*, *Scoping* e *Multiple Reply*.

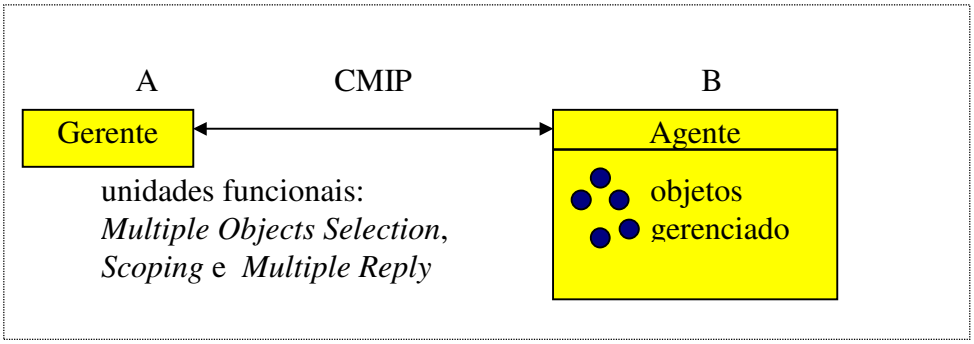


Figura 7.4 Conhecimento de Gerenciamento Compartilhado entre A e B.

A unidade funcional *Multiple Objects Selection* indica que as operações de gerenciamento podem ser executadas, não apenas sobre um único objeto mas sobre vários objetos e a unidade funcional *Multiple Reply* indica que uma única operação de gerenciamento pode ocasionar diversas respostas.

7.4 Domínios Gerenciais

O ambiente de gerenciamento OSI pode ser organizado em Domínios Gerenciais com o objetivo de diminuir a complexidade, estabelecer diferentes políticas de gerenciamento na organização ou até mesmo para atender às necessidades geográficas. Os domínios

gerenciais devem ser definidos, portanto, com base nos seguintes critérios:

a) o ambiente a ser gerenciado é dividido seguindo um propósito funcional (falhas, configuração, desempenho, segurança ou contabilização), ou seguindo um propósito de gerenciamento (diferentes tecnologias, estrutura organizacional ou estrutura geográfica).

b) para cada um dos propósitos anteriormente descritos, devem ser designados os papéis de gerentes e agentes em uma visão da MIB. Estes papéis não são fixos, podendo ser alterados dinamicamente.

c) formas de controle consistentes devem ser estabelecidas, isto é, o agrupamento de objetos gerenciados em um domínio de gerenciamento deve permitir, por exemplo, a aplicação de diferentes políticas de gerenciamento em diferentes grupos.

Um exemplo de utilização dos Domínios de Gerenciamento pode ser encontrado em uma empresa que possui uma política de segurança diferente para cada um de seus Departamentos; as informações do Departamento de Recursos Humanos certamente são informações mais sensíveis que as do Departamento de Engenharia e, portanto, necessitam de formas de controle diferenciadas. A organização em Domínios de Gerenciamento permite diminuir a complexidade de gerenciamento dos diferentes serviços e mecanismos utilizados nas diferentes políticas de segurança.

Em redes de telecomunicações, o ambiente de gerenciamento pode ser dividido, primeiramente, segundo uma estrutura geográfica (Estados, regiões dentro dos Estados, etc.), e depois segundo critérios funcionais e estruturais. Desta forma, pode-se pensar, por exemplo, em um Gerente de Falhas do Serviço de Telefonia Pública da cidade de Florianópolis, em Santa Catarina e também em um Gerente de Desempenho para o Serviço de Comutação de Pacotes no Estado de Santa Catarina. Na verdade, não existem regras fixas para a organização em Domínios Gerenciais; esta organização deve atender, antes de tudo, às necessidades do ambiente a ser gerenciado.

Uma vez estabelecidos os Domínios de Gerenciamento, é necessário ainda atender aos seguintes requisitos administrativos:

a) estabelecer e manter as respectivas autoridades em cada domínio de gerenciamento, aplicar modificações em seus limites e organizar a forma de sobreposição de domínios gerenciais;

b) gerenciar a transferência de controle de um domínio de gerenciamento para outro.

Um domínio administrativo de gerenciamento é um domínio de gerenciamento onde os objetos gerenciados estão sob a responsabilidade de uma e somente uma autoridade administrativa.

8 Funções e serviços CMISE

O CMISE consiste de uma definição de serviço (CMIS) e de uma especificação de protocolo (CMIP).

Os serviços e o protocolo são especificados pela definição de várias operações que podem ser invocadas pela aplicação de gerenciamento (no papel de gerente) sobre objetos gerenciados e pela definição de notificações que são emitidas pela aplicação de gerenciamento (no papel de agente) como resultado de algum evento ocorrido nos objetos gerenciados, para o gerente.

A definição do CMISE é especificada em termos do serviço que a máquina de protocolo proporciona a seus usuários e pela sintaxe e semântica das unidades de dados de protocolo (PDUs) trocadas entre entidades pares.

O protocolo é baseado no paradigma request-reply onde o invocador requisita a execução de uma operação sobre um ou mais objetos gerenciados. O sistema que invoca a operação atua no papel de gerente e, o sistema que recebe a operação atua no papel de agente. O executor da operação possui o processo agente que proporciona a interface de comunicação externa e uma visão dos objetos gerenciados em uma estrutura de árvore.

As operações de gerenciamento consistem em troca de unidades de protocolo para criar, destruir, ler e modificar a informação de gerenciamento, bem como executar ações específicas de objeto gerenciado. O termo informação de gerenciamento é usado, aqui, para referenciar objetos gerenciados e suas propriedades.

Além das operações já mencionadas, o protocolo suporta a transferência de relatórios que descrevem eventos ocorridos nos objetos gerenciados.

8.1 Serviços de gerenciamento

Os serviços definidos em ISO/IEC 9595 são:

M-GET: para ler o valor de um conjunto de atributos de um objeto.

M-SET: para substituir o valor de um conjunto de atributos de um objeto.

M-CREATE: para criar uma instância de objeto de uma determinada classe.

M-DELETE: para destruir uma instância de objeto.

M-ACTION: para solicitar que uma instância de objeto realize uma determinada ação.

M-EVENT-REPORT: para avisar a ocorrência de um evento em um objeto.

M-CANCEL-GET: para cancelar uma operação de leitura realizada sobre múltiplos objetos.

Os serviços M-SET, M-ACTION, M-DELETE e M-EVENT-REPORT podem ser requisitados tanto no modo confirmado quanto no modo não-confirmado, enquanto que os

serviços M-GET, M-CREATE e M-CANCEL-GET são sempre confirmados.

Alguns destes serviços podem ser requisitados de tal forma que a operação pode ser executada sobre um objeto individual ou sobre múltiplos objetos. O mecanismo para seleção de múltiplos objetos é descrito como uma combinação dos mecanismos de escopo (*scoping*) e filtro (*filtering*).

O mecanismo de scoping pode ser utilizado pelo usuário do serviço CMIS, para identificar os objetos gerenciados que são candidatos para a execução de uma operação particular, utilizando um dos métodos seguintes:

selecionar todos os objetos em uma sub-árvore;

selecionar objetos em um nível particular de uma sub-árvore.

A raíz da sub-árvore é indicada por um parâmetro cujo valor é o identificador de um objeto denominado objeto gerenciado base.

Filtering é um mecanismo de aplicação de critérios para selecionar objetos a fim de determinar se uma operação deve ou não ser executada sobre o objeto. O parâmetro filter é um conjunto de uma ou mais asserções sobre a presença ou valor de um atributo em um objeto gerenciado.

As asserções sobre o valor de um atributo são avaliadas usando regras de comparação associadas com o tipo do atributo. São definidas as seguintes regras de comparação:

equality: avaliado como TRUE se e somente se existe um valor de atributo que é igual ao declarado;

greater or equal: avaliado como TRUE se e somente se o valor do atributo fornecido na asserção de valor do atributo é maior ou igual ao valor do atributo;

less or equal: avaliado como TRUE se e somente se o valor do atributo fornecido na asserção de valor do atributo é menor ou igual ao valor do atributo;

present: avaliado como TRUE se e somente se tal atributo está presente no objeto gerenciado;

substring: avaliado como TRUE se e somente se existe um valor de atributo no qual o substring especificado aparece em uma determinada ordem.

subset of: avaliado como TRUE se e somente se todos os membros declarados estão presentes no atributo;

superset of: avaliado como TRUE se e somente se todos os membros do atributo estão presentes na asserção de valor de atributo;

non-null set intersection: avaliado como TRUE se e somente se no mínimo um dos membros declarados está presente no atributo.

Além dos mecanismos de scoping e filtering, também é definido um mecanismo de sincronização (*synchronization*) que indica a forma que uma operação de gerenciamento deve ser sincronizada sobre instâncias de objetos gerenciados, quando múltiplos objetos gerenciados foram selecionados através dos mecanismos de escopo e filtro. Duas técnicas de sincronização foram definidas: melhor esforço (*best effort*) e atômica (*atomic*). A

sincronização de melhor esforço, quando selecionada para a execução de uma operação, indica que a operação deve ser executada sobre todos os objetos selecionados pelo mecanismo de escopo, para os quais é possível a execução da operação. Para aqueles os quais a operação falha, deve ser retornada uma mensagem de erro. Para o caso onde a sincronização atômica é selecionada, se a operação falhar em pelo menos um dos objetos selecionados, ela não deve ser executada em nenhum dos outros, mesmo que seja possível. A sincronização atômica pode ser comparada ao mecanismo de operações atômicas oferecido pela camada de sessão do modelo de referência OSI. A ordem com que os objetos gerenciados são selecionados para a execução da operação é considerada uma questão local e, portanto, dependente da implementação. O CMIS não fornece um parâmetro para indicar sincronização de atributos de um objeto, isto é, não existe uma forma de se executar uma operação com sincronização atômica sobre vários atributos de um mesmo objeto.

Os próximos ítens são dedicados à apresentação dos serviços de gerenciamento oferecidos pelo CMISE, com mais detalhes.

8.1.1.M-EVENT-REPORT

Este serviço é usado para relatar a ocorrência de um evento, para outro sistema aberto. As ações que devem ser executadas quando um relatório de evento é recebido, não são especificadas na definição deste serviço.

Se o serviço for requisitado no modo confirmado, uma confirmação de recepção deve ser encaminhada pelo sistema receptor para o sistema que emitiu o relatório de evento.

Os parâmetros obrigatórios, associados com a requisição deste serviço, são: um número de sequência, o modo de serviço (confirmado ou não confirmado) e o tipo de evento relatado. Adicionalmente, o relatório de evento pode incluir o horário em que o evento ocorreu e informações específicas do evento. No modo confirmado, a resposta positiva deve conter o número de seqüência como parâmetro obrigatório. As informações como identificação do objeto, tipo de evento e horário de resposta, podem ser incluídas opcionalmente na resposta. Uma resposta de erro também pode ser gerada.

8.1.2. M-GET

Este serviço é confirmado e possibilita que o sistema aberto invocador recupere valor(es) de atributo(s) de um ou mais objetos gerenciados de um outro sistema aberto. Os parâmetros obrigatórios, na requisição do serviço, são: um número de seqüência e a identificação do objeto gerenciado (que pode ser usado de duas formas: como referência para os atributos que devem ser recuperados ou como referência para a seleção de outros objetos gerenciados que ele contenha). A requisição pode incluir, também, informações de segurança para validar a requisição e os identificadores dos atributos cujos valores devem ser recuperados. Se nenhum atributo é especificado, os valores de todos os atributos do objeto são requisitados.

Se a operação refere-se à seleção de múltiplos objetos, uma resposta é enviada para cada objeto individual. Neste caso, o número de seqüência da requisição original é usado para ligar as múltiplas respostas à requisição e é referenciado como o parâmetro *linked-ID*. O término das múltiplas respostas, se a operação teve sucesso, pode ser indicado tanto por um

resultado vazio quanto por uma informação na última resposta. No caso de sucesso parcial, a resposta contém tanto a informação de erro quanto os valores dos atributos recuperados com sucesso.

8.1.3. M-SET

Este serviço é utilizado pelo sistema invocador para requisitar a modificação de valor de atributo(s) de um ou mais objetos gerenciados em um outro sistema aberto. Os parâmetros obrigatórios são o número de seqüência, a identificação do MO (que é usado de uma ou duas formas, conforme descrito no serviço M-GET) e um operador de modificação. O operador de modificação serve para identificar se a operação mapeada é um Set-With-Default, um Replace, um Add ou um Remove. O conjunto de valores de um atributo multi-valorado é considerado como um conjunto matemático quando a operação Add é executada; se o valor já existe, ele não é adicionado e nenhum erro será gerado.

Quando o serviço requisitar a seleção de múltiplos objetos, os procedimentos são similares àqueles descritos no serviço M-GET. É importante observar que este serviço pode ser requisitado no modo confirmado ou no modo não confirmado e que, respostas múltiplas só podem ser obtidas no modo confirmado. No serviço não confirmado, o sistema invocador só poderá determinar o resultado da operação através da recuperação dos valores dos atributos modificados.

8.1.4. M-ACTION

Este serviço habilita a um sistema aberto invocador, requisitar para um outro sistema aberto, a execução de uma ação sobre um ou mais objetos gerenciados. O tipo de ação é definido como parte da descrição do MO. Os detalhes associados à execução da ação (como por exemplo, as pré e pós condições necessárias para manter a integridade do MO), não são definidas pelo CMIS, uma vez que as ações são específicas aos MOs e às funções de gerenciamento. Os parâmetros obrigatórios são: um número de seqüência, a identificação do MO (que é usado em uma das formas já descritas no serviço M_GET), e o tipo de ação. Os parâmetros opcionais incluem uma informação específica da ação (se definida) e informação de controle de segurança.

Os procedimentos associados a este serviço, quando requisitado para realização sobre múltiplos objetos, são os mesmos definidos para o serviço M_SET.

8.1.5. M-CREATE

Este serviço confirmado é utilizado para requisitar a criação de um novo MO em um outro sistema aberto. Apenas um único MO pode ser criado por requisição. Diferentes métodos podem ser utilizados na criação de um nome para o novo objeto e na atribuição de valores para seus atributos. Um MO pode ser criado como uma cópia de um outro MO já existente, com um nome diferente. Na criação da cópia, os valores dos atributos podem ser alterados explicitamente. A atribuição do nome para o novo MO pode ser feita de uma das seguintes maneiras:

indicação do nome explicitamente na criação;

atribuição de um identificador único relativo ao objeto superior especificado na

requisição;

atribuição do nome pelo sistema criador do MO, de acordo com as restrições impostas na definição do objeto.

A atribuição de valores para os atributos depende dos valores que são fornecidos com a requisição e da existência ou não de definição de valores iniciais ou de valores default. Se não existirem valores para todos os atributos requisitados, a operação de create irá falhar e uma resposta de erro será enviada.

Se a operação de criação for realizada com sucesso, a resposta irá incluir o nome do novo objeto, se ele não foi fornecido na requisição. Adicionalmente, os identificadores e valores de todos os atributos atribuídos para o MO, podem também serem incluídos na resposta.

8.1.6. M-DELETE

Este serviço é utilizado para solicitar que um outro sistema aberto delete um ou mais objetos gerenciados. Os parâmetros obrigatórios para a requisição deste serviço são: um número de seqüência e a identificação do MO (que pode ser usado de uma das formas descritas no serviço M-GET). Quando múltiplos objetos são deletados, respostas são geradas para cada um dos objetos deletados.

Existem duas opções de permissão para a destruição de objetos e elas se referem à forma de manter a integridade dos nomes dos MOs. Estas opções são descritas como parte da definição do MO e consistem em permitir ou não a destruição de um objeto quando existem outros objetos nele contidos. É importante ressaltar que a requisição de destruição deve manter a integridade dos relacionamentos entre os objetos, de forma que os apontadores de relacionamento de um MO não referenciem objetos que não existam mais.

8.1.7. M-CANCEL-GET

Este serviço confirmado é utilizado para solicitar o cancelamento de um serviço M_GET, solicitado previamente e, para o qual, nenhuma resposta tenha sido recebida. O cancelamento de uma operação de get pode ser necessário em alguns casos onde, por exemplo, múltiplos objetos foram selecionados e a aplicação invocadora não deseja mais receber as múltiplas respostas ou o tempo de execução da operação get é muito longo. Se a operação get já tiver sido completada antes da recepção do cancelamento, uma resposta de erro será emitida. Se o cancelamento tiver sucesso, uma resposta positiva é enviada para o serviço M-CANCEL-GET e uma resposta de erro é enviada para o serviço M-GET solicitado anteriormente. Os parâmetros obrigatórios na requisição deste serviço são: um número de seqüência para esta requisição e o número de seqüência da requisição a ser cancelada.

8.2 Protocolo de gerenciamento CMIP

O CMIP especifica os elementos de protocolo que devem ser utilizados para fornecer os serviços de operação e notificação do CMIS; As operações podem ser:

⇨classe 1 - confirmada síncrona

⇨classe 2 - confirmada assíncrona

⇨classe 5 - não confirmada assíncrona

O CMIP é especificado em termos das várias semânticas das operações, sintaxe das informações trocadas e procedimentos que devem ser suportados pela máquina de protocolo.

A máquina de protocolo CMIPM (Commom Management Information Protocol Machine) recebe as primitivas de serviço request e response do usuário do serviço CMIS (MIS-User) e emite PDUs (Protocol Data Unit) que serão transferidas através dos serviços oferecidos pelo elemento de serviço ROSE.

Por outro lado, a CMIPM remota recebe as PDUs do ROSE e as encaminha através de primitivas indication e confirm apropriadas, para o MIS-User correspondente.

Os procedimentos de protocolo somente indicam como interpretar cada um dos campos existentes na PDU mas não indicam como o usuário deve processar a informação recebida.

A sintaxe das unidades de dados do protocolo, é especificada usando uma sintaxe denominada ASN.1 (Abstract Syntax Notation One).

8.2.1. Formato das PDUs CMIP

Fase de Associação (mapeadas sobre PDUs do ACSE):

```
CMIPUserInfo ::=SEQUENCE {
protocolVersion    [0]      IMPLICIT ProtocolVersion
                            DEFAULT {version1},
funcional Units    [1]      IMPLICIT FuncionalUnits
                            DEFAULT { },
accessControl      [2]      EXTERNAL OPTIONAL,
userInfo           [3]      EXTERNAL OPTIONAL }
ProtocolVersion ::= BIT STRING { version1 (0), version2 (1) }
FuncionalUnits ::= BIT STRING {
                            multipleObjectSelection (0),
                            filter (1),
                            multipleReply (2),
                            extendedService (3),
                            cancelGet (4) }
```

Fase de Operação (mapeadas sobre PDUs do ROSE):

ROIVapdu ::=SEQUENCE {

invokeID InvokeIDType,

linked-ID [0] IMPLICIT InvokeIDType OPTIONAL,

operation-value OPERATION,

argument ANY DEFINED BY operation-value OPTIONAL }

InvokeIDType ::= INTEGER

Exemplo:

m-Get OPERATION ::= localValue 3

ROIV-m-Get ::= ROIVapdu (WITH COMPONENTS

{ invokeID PRESENT,

linked-ID ABSENT,

operation-value (m-Get),

argument (INCLUDES GetArgument) })

Operação M-GET

M-Get OPERATION

ARGUMENT GetArgument

RESULT GetResult

ERRORS (accessDenied, classInstanceConflict, complexityLimitation, operationCancelled, getListError, invalidFilter, invalidScope, noSuchObjectClass, noSuchObjectInstance, processingFailure, syncNotSupported)

LINKED (m-Linked-Reply)

::= localValue 3

GetArgument ::= SEQUENCE {

COMPONENTS OF BaseManagedObjectId,

accessControl [5] AccessControl OPTIONAL,

synchronization [6] IMPLICIT CMISSync DEFAULT bestEffort,

scope [7] Scope DEFAULT baseObject,

filter CMISFilter DEFAULT and { },

attributeIdList [12] IMPLICIT SET OF AttributeId OPTIONAL }

BaseManagedObjectId ::= SEQUENCE {

baseManagedObjectClass ObjectClass,

baseManagedObjectInstance ObjectInstance }

AccessControl ::= EXTERNAL

```
CMISSync ::= ENUMERATED { bestEffort (0), atomic (1) }
Scope ::= CHOICE {INTEGER {     baseObject (0),
                                firstLevelOnly (1),
                                wholeSubtree (2)  },
                    individualLevels [1] IMPLICIT INTEGER
                    baseToNthLevel  [2] IMPLICIT INTEGER }
CMISFilter ::= CHOICE {     item    [8] FilterItem,
                            and     [9] IMPLICIT SET OF CMISFilter,
                            or      [10] IMPLICIT SET OF CMISFilter,
                            not     [11] CMISFilter }
```

AttributeId ::= CHOICE { globalForm [0] IMPLICIT OBJECT IDENTIFIER, localForm [1] IMPLICIT INTEGER }

```
GetResult ::= SEQUENCE {
    managedObjectClass  ObjectClass OPTIONAL
    managedObjectInstance       ObjectInstance OPTIONAL
    currentTime  [5] IMPLICIT GeneralizedTime OPTIONAL
    attributeList [6] IMPLICIT SET OF Attribute OPTIONAL
ObjectClass ::= CHOICE {
    globalForm    [0] IMPLICIT OBJECT IDENTIFIER,
    localForm     [1] IMPLICIT INTEGER }
ObjectInstance ::= CHOICE {
    distinguishedName    [2] IMPLICIT DistinguishedName,
    nonSpecificForm      [3] IMPLICIT OCTET STRING,
    localDistinguishedName [4] IMPLICIT RDNSequence }
```

8.2.2. ERROS

Quando um serviço é requisitado no modo confirmado, uma resposta é enviada para indicar o sucesso ou a falha na execução do serviço. São definidos vários erros no padrão CMIS. Alguns destes erros são gerais e aplicáveis a todos os serviços (como por exemplo, *duplicate invocation*, *no such object instance*, *unrecognized operation* e *processing failure*). Alguns erros específicos, aplicáveis a serviços individuais, são, por exemplo:

No such event type para M-EVENT-REPORT

Access denied para M-GET, M-SET, M-ACTION, M-CREATE e M-DELETE

No such action para M-ACTION

No such attribute para M-GET e M-SET

9 Arquitetura Funcional do modelo OSI

Este capítulo é dedicado ao estudo mais aprofundado do elemento de serviço de aplicação de gerenciamento de sistemas SMASE (*System Management Application Service Element*).

O SMASE define a semântica e a sintaxe abstrata da informação transferida em MAPDUs (Management Application Protocol Data Unit), isto é, especifica a informação de gerenciamento a ser trocada entre as entidades de aplicação de gerenciamento de sistemas.

Os serviços providos pelo SMASE podem ser agrupados em unidades funcionais, com o objetivo de facilitar o processo de negociação entre as entidades comunicantes. A negociação de unidades funcionais de gerenciamento de sistemas SMFUs (*Systems Management Funtional Units*) é opcional. Um conjunto inicial de SMFUs agregadas pode ser determinado em tempo de estabelecimento de associação, através do uso do parâmetro smfuPackages. O parâmetro smfuPackages é definido como um conjunto de unidades funcionais e deve estar presente nas primitivas A-ASSOCIATE (request e indication) quando for realizada uma negociação das SMFUs e nas primitivas A-ASSOCIATE (response e confirm) se a negociação for aceita; nos demais casos, o parâmetro deve ser omitido.

A informação do usuário, a ser passada no parâmetro “user information” da primitiva A-ASSOCIATE, é definida em CCITT Rec.X.701 | ISO/IEC 10040, usando a syntaxe abstrata ASN.1:

```
SMASE-A-ASSOCIATE-Information {joint-iso-ccitt ms(9) smo(0) asn.1Modules(2)
negotiationDefinitions(0) version1(1)}
DEFINITIONS ::= BEGIN
SMASEUserData ::= SEQUENCE{
smfuPackages SET OF    FunctionalUnitPackage        OPTIONAL,
-- shall be present on request/indication if SMFU negotiation is proposed and
-- on response/confirm if SMFU negotiation is accepted, otherwise this
-- parameter shall be omited.
reason       Reason          OPTIONAL,
-- may only be present on A-ASSOCIATE response/confirm. When
-- SMFU negotiation fails, when SMFU negotiation results in a
-- reduction of the proposed set of SMFUs or when association request
-- is rejected, it may carry a specific reason for this.
systemManagementUserInformation      GraphicString    OPTIONAL
-- this parameter is provided solely for the convenience of
--implementations needing to distinguish between different
```

-- implementation environments, it shall not be subject of conformance

-- test

Após o estabelecimento do conjunto de SMFUs, a associação deve restringir-se ao conjunto de unidades funcionais agregadas até que um novo conjunto seja estabelecido, isto é, somente podem ser utilizadas operações e notificações pertencentes ao conjunto agregado. No entanto, a negociação das unidades funcionais é feita apenas na fase de estabelecimento de associação, uma vez que a definição dos mecanismos para modificar o conjunto agregado de SMFUs durante o tempo de vida da associação, ainda não foram definidos, sendo objeto de estudos posteriores.

Para identificar um conjunto de SMFUs, os bits correspondentes a cada SMFU, no parâmetro smfuPackages, devem ser marcados com o valor 1. O conjunto de todas as SMFUs cuja posição correspondente no parâmetro smfuPackages está setada com o valor 1, é o conjunto agregado de SMFUs a ser negociado durante a fase de estabelecimento de associação entre as entidades de aplicação de gerenciamento. A omissão de sequências de bits em um BITSTRING deve ser interpretada como setada para zero.

O serviço de comunicação usado pelo SMASE pode ser fornecido pelo CMISE ou por outros ASEs, tais como o FTAM (*File Transfer, Access and Management*) [ISO8571] ou TP (*Transaction Processing*) [ISO/IEC 10026]. Quando o CMISE é utilizado, a presença do ROSE [CCITT Rec. X.219 | ISO/IEC 9072] é requerida.

De uma forma geral, este elemento de serviço pode ser visto como sendo composto de um conjunto de funções que oferecem serviços de suporte para as aplicações de gerenciamento. Embora nem todas as funções sejam obrigatórias, é importante que se conheça cada uma delas no sentido de se ter parâmetros para selecionar produtos de gerenciamento no mercado.

9.1 SMASE - System Management Application Service Element Aspectos funcionais

O SMASE pode ser visto como um conjunto de funções de gerenciamento de sistemas que dão suporte às áreas funcionais de gerenciamento.

Uma função de gerenciamento define as atividades de gerenciamento e as informações necessárias para alcançar um determinado objetivo. As funções de gerenciamento podem ser combinadas para executar uma atividade de gerenciamento específica; este agrupamento é denominado de Unidade Funcional.

Unidades funcionais

- unidades básicas de negociação entre MIS-Users;
- serviços de funções de gerenciamento podem ser agrupados em uma ou mais unidades funcionais;
- unidades funcionais que atravessam os limites de uma função, podem suportar os seguintes conjuntos de capacidades:
    - somente notificações;

- somente operações de gerenciamento;
- notificações e operações de gerenciamento.

Existem diversas Funções de Gerenciamento definidas nos documentos de padronização mas, neste documento, iremos abordar apenas algumas delas. O objetivo é mostrar a funcionalidade que pode ser obtida no caso da sua inclusão em soluções de gerenciamento.

9.2 Função de Gerenciamento de Objeto

Uma operação de gerenciamento pode ser realizada sobre os atributos de um objeto ou sobre o objeto como um todo.

Sobre o objeto:
CREATE: criação de uma instância de classe de objeto
DELETE: destruição de uma instância de classe de objeto
ACTION: solicitação para a execução de uma ação sobre uma instância de classe de objeto

Sobre os atributos:
GET ATTRIBUTE VALUE: leitura do valor de um atributo
REPLACE ATTRIBUTE VALUE: modificação do valor de um atributo
REPLACE WITH DEFAULT VALUE: modificação do valor de um atributo pelo seu valor default
ADD MEMBER: adição de um elemento no conjunto de valores de um atributo
REMOVE MEMBER: remoção de um elemento do conjunto de valores de um atributo

Esta função oferece serviços de relatórios sobre a criação de objeto, remoção de objeto e mudança de valor de atributo.

Oferece, ainda, os serviços de PASS-THROUGH para as demais funções de gerenciamento acessarem os serviços do CMIS. O mapeamento das operações em serviços da OMF (Object Management Function) é apresentado na tabela 9.1.

Tabela 9.1 Mapeamento das operações nos serviços Pass-Through

Operações sobre o MO	Pass - Through
Create	PT-CREATE
Delete	PT-DELETE
Action	PT-ACTION
Replace	PT-SET
Add	PT-SET
Remove	PT-SET
Replace-with-Default	PT-SET
Get	PT-GET
Notification	PT-EVENT-REPORT

Serviços da OMF

⇒ **seis serviços de pass-through**
⇒ **relatório de Criação de Objeto**
⇒ **relatório de Remoção de Objeto**
⇒ **relatório de Mudança de Valor de Atributo**

9.3 Função de Gerenciamento de Estado

Um atributo de Estado representa as condições instantâneas de disponibilidade e operacionalidade do recurso correspondente, sob a visão do gerenciamento.

Esta função tem como objetivo prover definições genéricas que permitam obter informações, mudar o estado de gerenciamento de um objeto gerenciado e emitir notificações sobre estas mudanças de estado, quando elas forem decorrentes de alguma operação em um sistema aberto.

- **Estado operacional**: indica se o recurso está ou não fisicamente instalado e em operação;
- **Estado de utilização**: indica se o recurso está ou não em uso em um dado instante e, se está ou não apto a aceitar outros usuários adicionais;
- **Estado de administração**: indica a permissão ou proibição da utilização do recurso, imposta pelos serviços de gerenciamento.

O modelo da Função de Gerenciamento de Estado define atributos que podem ser utilizados na modelagem dos objetos que representam os recursos gerenciados. Os atributos e seus respectivos valores são apresentados na tabela 9.2 e os diagramas de estado representando a mudança de estado administrativo e de utilização de objetos gerenciados são apresentados nas figuras 9.1 e 9.2, respectivamente.

Tabela 9.2 Atributos de Estado

Atributo de Estado	**Valores possíveis**
Operacional	*Enable* *Disable*
Utilização	*Idle* *Active* *Busy* *Unknown*
Administrativo	*Locked* *Unlocked* *Shutting Down*

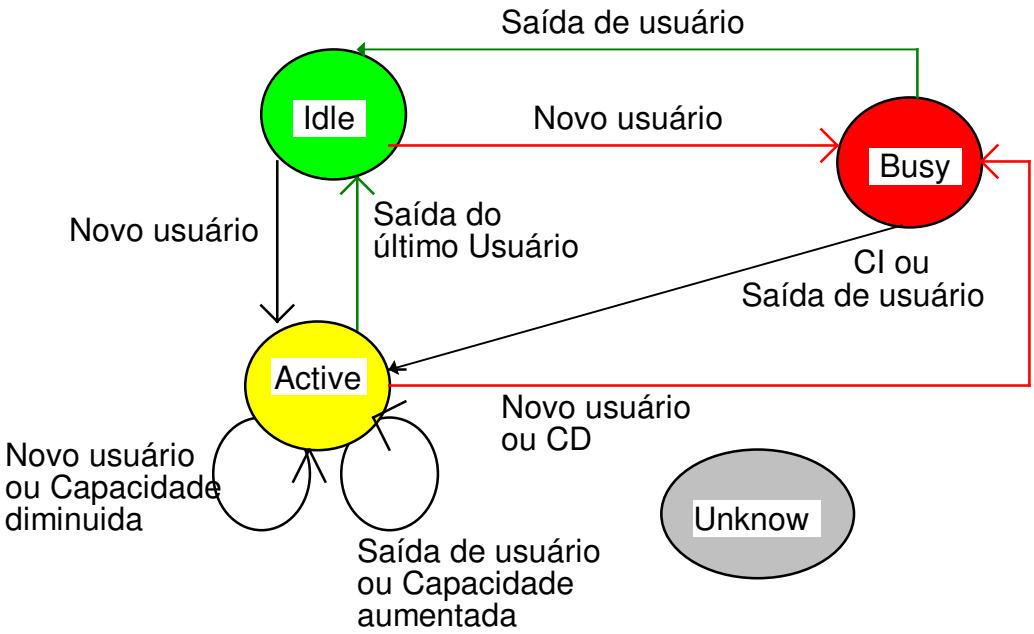


Figura 9.1 Diagrama de estados de utilização

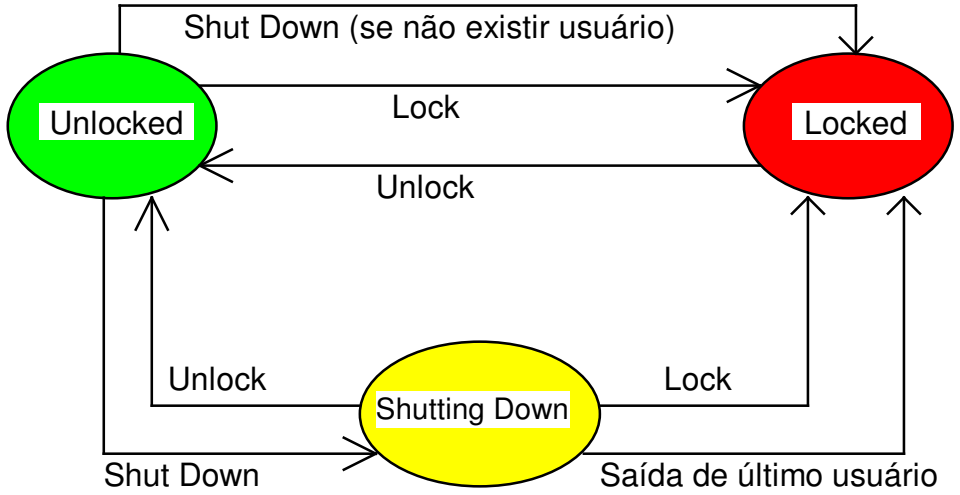


Figura 9.2 Diagrama de estados administrativo

9.4 Atributos de Status

Status de Reparo: Under Repair / Fault Report Outstanding
Status de Instalação: Not Installed / Initialization Incomplete / Initialization Required
Status de Disponibilidade: In Test / Failed / Power Off / Off Line / Off Duty / Dependency / Degraded
Status de Controle: Subject to Test / Read Only / Part of Services Locked / Reserved for Test / Suspended

9.5 Atributos para representação de relacionamento

O relacionamento entre objetos gerenciados é descrito por um conjunto de regras que determinam como a operação de uma parte do sistema aberto afeta a operação de outra parte deste mesmo sistema. Os tipos de relacionamentos, mostrados na figura 9.3, são:

- Direto e Indireto
- Simétrico e Assimétrico

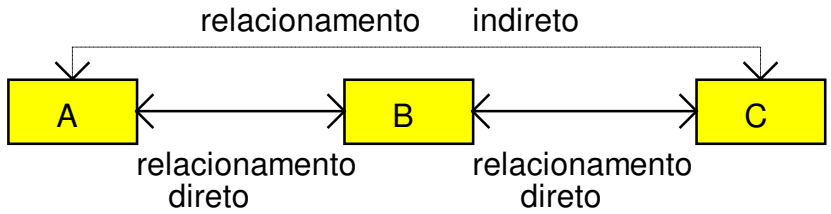


Figura 9.3 – Tipos de relacionamentos considerados

Categorias de Relacionamento

- Relacionamento de Inclusão
- Relacionamento de um Sentido
- Relacionamento Recíproco

Tipos de Relacionamento Recíproco	Atributos de Relacionamento
Relacionamento de Serviço: Servidor e Usuário	Objeto Provedor: GET, REPLACE Objeto Usuário: GET, REPLACE
Relacionamento Par: Par	Par: GET
Relacionamento Fallback: Primário e Secundário	Primário: GET, REPLACE Secundário: GET, REPLACE
Relacionamento Backup: Backup e Backed-up	Instância de Objeto Backup: GET Instância de Objeto Backed-up: GET
Relacionamento de Grupo: Proprietário e Membro	Membro: GET, REPLACE Proprietário: GET, REPLACE

Grupo de Atributos de Relacionamento: constituído de todos os atributos de relacionamento de um MO.

9.6 Função de Relatório de Alarme

Tem como objetivo prover informações sobre as condições operacionais e a qualidade de serviço do sistema gerenciado bem como definir critérios que permitam identificar o grau de mau funcionamento do sistema gerenciado e o nível de degradação da qualidade de serviço.
Um alarme consiste em uma mensagem enviada do sistema Agente para o sistema Gerente, contendo as seguintes informações:
Tipo de Alarme, Causas Prováveis, Nível de Severidade, Indicação de Tendências, Informação de Valor Limite, Sugestões de Ações de Reparo e Descrição do Problema.

Tipos de Alarme

Alarme de Comunicação
Alarme de Qualidade de Serviço
Alarme de Processamento
Alarme de Equipamento
Alarme Ambiental

Causas Prováveis(Ver anexo 1)

Níveis de Severidade

Cleared: o alarme ou conjunto de alarmes foi removido.
Indeterminado: não é possível identificar como as condições de funcionamento foram afetadas.
Crítico: exige ação corretiva imediata do sistema.
Maior: as condições de funcionamento de um sistema estão sendo afetadas exigindo uma ação corretiva urgente.
Menor: ações corretivas são necessárias para prevenir a ocorrência de falhas mais sérias.
Alerta: suspeita de ocorrência de falhas. Devem ser realizados diagnósticos sobre o recurso gerenciado.

Indicação de tendências

Indica se existem alarmes pendentes e quais as tendências demonstradas pelo alarme emitido, em relação aos anteriores.

☹ Mais Severo
😐 Nenhuma Mudança
☺ Menos Severo

Obs.: Esta informação só tem sentido se existirem alarmes pendentes.

Informação de Valor Limite

Definida através de quatro sub-campos:
Valor-Limite Pré-Fixado: identificador do atributo de valor-limite que causou a notificação;

Nível-Limite: valor-limite que, quando ultrapassado, provoca a notificação de um alarme;
Valor Observado: valor que ultrapassou o valor-limite pré-fixado;
Instante de Ultrapassagem: instante de ocorrência da ultrapassagem do valor-limite.

Registro de Alarme

Representa a informação armazenada em logs, como resultado do relatório de eventos recebido, quando o tipo de evento é um dos alarmes definidos.

Serviço de Relatório de Alarme

Possibilita que um usuário notifique outro usuário sobre a ocorrência de um alarme. Pode ser confirmado ou não-confirmado.

A classe de objeto **Registro de Alarme** é derivada da classe **Registro de Log de Evento** que, por sua vez, é derivada da classe **Registro de Log**.

9.7 Função de Gerenciamento de Relatório de Evento

Os principais objetivos desta função referem-se à:

- Selecionar os relatórios de eventos que devem ser enviados a um sistema de gerenciamento particular;
- Determinar os destinatários para os quais os relatórios de eventos devem ser enviados;
- Controlar (suspender e retomar) o repasse de relatórios de eventos;
- Possibilitar que um sistema de gerenciamento externo modifique as condições de emissão de relatórios de eventos;
- Designar endereços alternativos

O modelo para a função de Gerenciamento de Relatório de Evento é apresentado na figura 9.4.

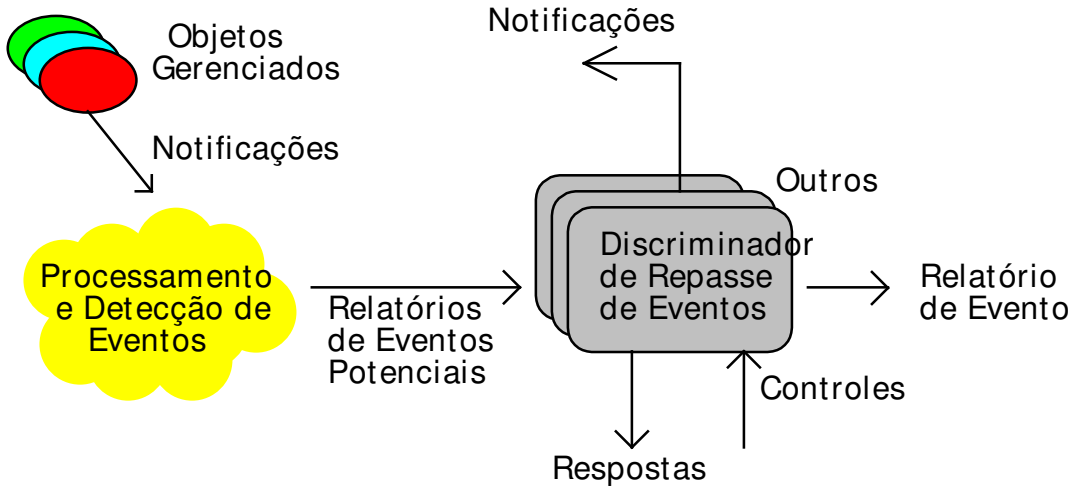


Figura 9.4. Modelo para a função de Gerenciamento de Relatório de Evento

O objeto Discriminador estabelece as condições que devem ser satisfeitas para que um objeto de entrada seja repassado e pode estar associado a um pacote de programação que determine quando a emissão do evento deve ocorrer.

Atributos do Discriminador de Repasse de Eventos

- Destination address: especifica um grupo de endereços primários;
- Backup address list: lista ordenada de endereços a serem usados no caso de falha do endereço primário;
- Active address: identifica o endereço da Entidade de Aplicação para a qual os eventos são repassados pelo discriminador;

Outros atributos definidos para o objeto Discriminador são os atributos de estado administrativo, operacional e de utilização e o atributo que define o critério de discriminação a ser empregado.

O atributo Construtor de Discriminador tem como valor um conjunto de uma ou mais asserções sobre a presença de valores de atributos. Estas asserções podem ser agrupadas usando operadores lógicos AND e OR.

A classe de objeto Discriminador também pode ser derivada para acomodar condições específicas em cada sub-classe particular.

Um objeto Discriminador pode ser especificado para testar condições específicas de igualdade ou desigualdade de atributos, a presença de atributos e a ausência de qualquer uma destas condições.

Pacotes de Programação

Permitem que os discriminadores troquem, automaticamente, suas condições de *reporting-on* e *reporting-off*. São definidos três tipos de Pacotes de Programação:

- Pacote de Programação Diária (*Daily Scheduling Package*) tem um único atributo: *Intvls*
- Pacote de Programação Semanal (*Weekly Scheduling Package*) tem os atributos: *StartTime StopTime* e *WeekMask (DaysOfWeek* e *IntvlsOfDay)*
- Pacote de Programação Externa (*External Schedular Scheduling Package*) tem um único atributo que especifica o nome do MO programador (*SchedularName*).

Serviços

Criação de Relatório de Repasse de Eventos;
Eliminação de Relatório de Repasse de Eventos;
Modificação de valores de atributos,
Suspensão e Retomada de atividade de discriminação

9.8 Função de Controle de Log

Define um objeto que tem como objetivo preservar informações sobre eventos ocorridos ou sobre operações efetuadas sobre objetos. A representação da função de Log é dada na figura 9.5.

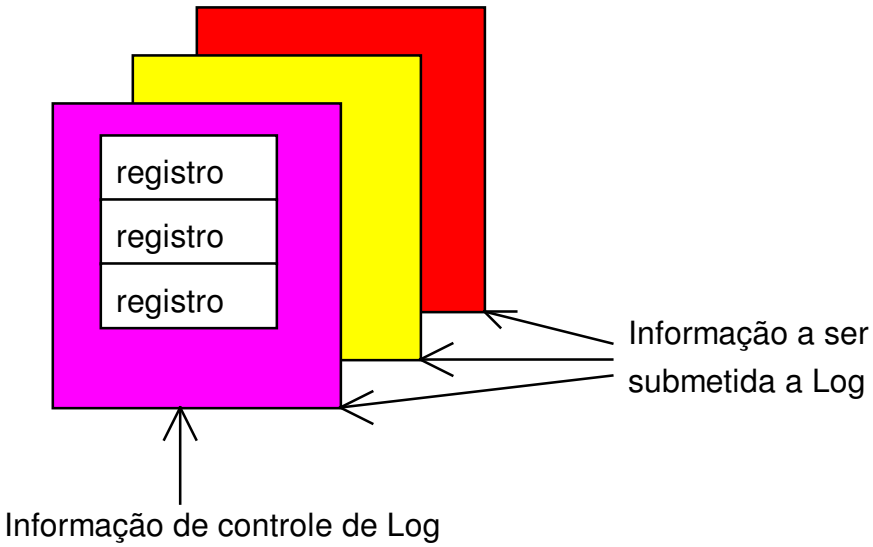


Figura 9.5 A Função de Log

Atributos do Log
Log Id (instância do log)
Discriminator Constructor
Administrative State (UNLOCKED e LOCKED)
Operational State (ENABLE e DISABLE)
Availability Status
Usage State (ACTIVE, IDLE, BUSY e UNKNOWN)
Max Log Size
Current Log Size
Number of Records
Capacity Alarm Threshold
Log Full Action (wrap ou halt)
Packages

Registros de Log

Representam a informação armazenada no Log. A classe Registro de Log é definida com dois atributos:

Log Record Id (Get)
Logging Time (Get)

Os Registros de Log não podem ser criados explicitamente por operações de gerenciamento e só podem ser recuperados ou eliminados.

Serviços de Controle de Log
Iniciação de Log;
Remoção de Log;
Modificação de valores de atributos de Log;
Suspensão da atividade de armazenamento;
Retomada da atividade de armazenamento;
Eliminação e recuperação de Registro de Log;

9.9 Funções de Gerenciamento de Segurança

O modelo de gerenciamento OSI define três funções de gerenciamento de segurança que têm como objetivos principais:

- Fornecer relatórios de eventos relativos à segurança;
- Fornecer informações estatísticas;
- Manter e analisar históricos de registros de segurança;
- Selecionar parâmetros do serviço de segurança;
- Ativar e desativar serviços de segurança.

Considerações gerais sobre a gerência de segurança

Diferentes políticas de segurança podem ser adotadas nos sistemas abertos. Grupos de entidades que obedecem a uma mesma política de segurança formam um Domínio de Segurança.

As informações de segurança devem ser distribuídas entre todas as entidades que têm relação com segurança e devem ser armazenadas em uma base específica (SMIB)

Categorias de atividades de gerenciamento de segurança: Segurança do Sistema, Serviços de Segurança e Mecanismos de Segurança.

Função de Relatório de Alarme de Segurança

Esta função define os tipos de relatórios que podem ser utilizados para informar sobre atentados e violações contra a segurança, detectados pelos mecanismos de segurança do sistema.

As informações contidas nestes relatórios possibilitam que o usuário seja notificado sobre a gravidade percebida em relação à operações errôneas, atentados e violação de segurança dos sistemas.

O modelo, apresentado na figura 9.6, segue aquele definido para a função de relatório de evento.

Informações sobre alarmes

⇨ **Tipos de alarmes:**

violação de integridade;
violação operacional;
violação física;
violação de serviço ou mecanismo de segurança;
violação no domínio do tempo.

⇨ **Causas de Alarme**

⇨ **Gravidade do Alarme:**

indeterminado, crítico, maior ou menor.

Modelo de Controle de Acesso

O modelo de controle de acesso é descrito pelas figuras 9.7 e 9.8 que mostram, respectivamente, o controle de acesso na fase de associação e na fase de operações de gerenciamento.

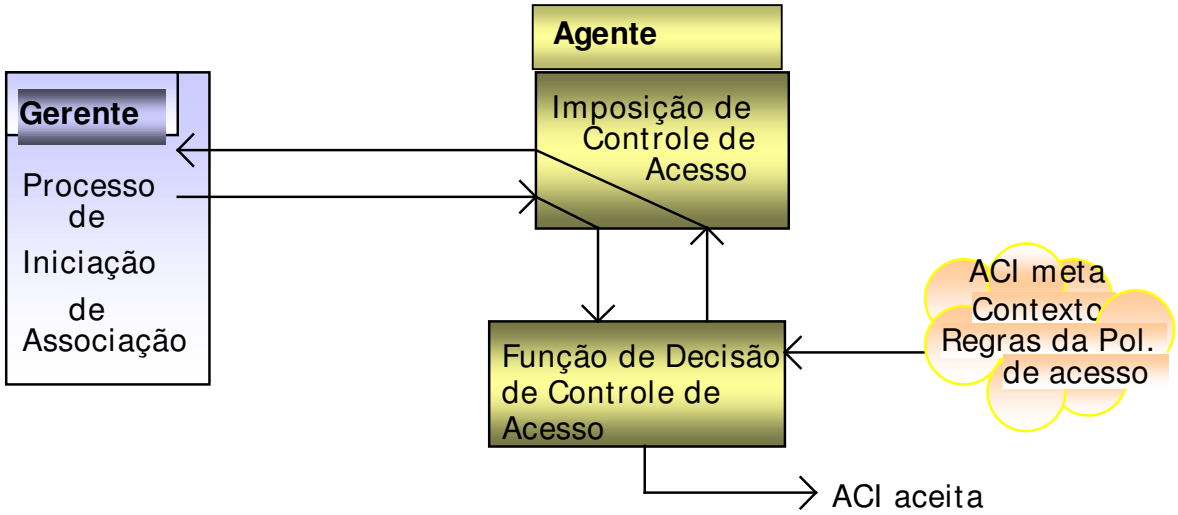


Figura 9.7. Modelo de controle de acesso para Associação de Gerenciamento

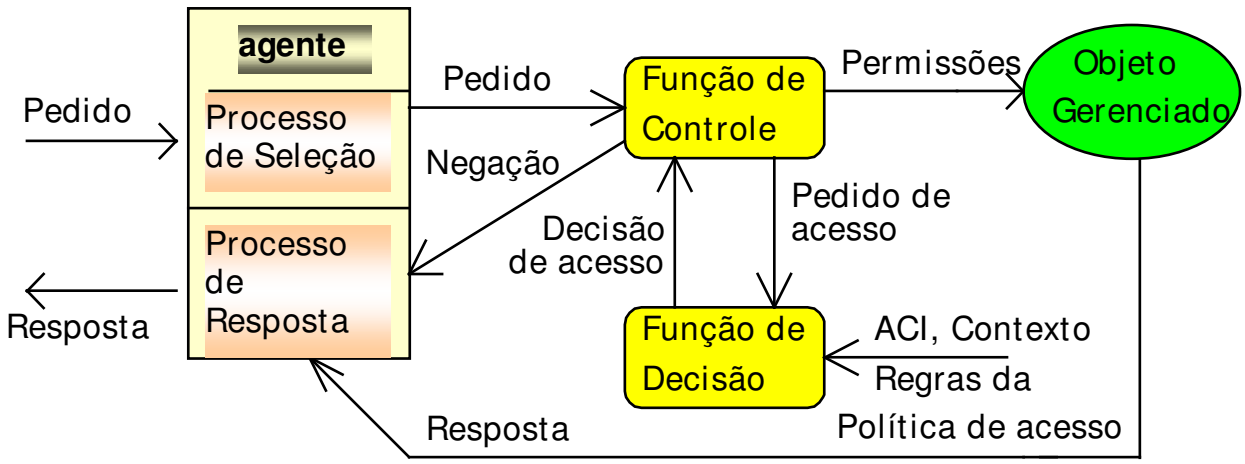


Figura 9.8. Modelo de controle de acesso para Operações de Gerenciamento

9.10 Função de Medida de Contabilização

O objetivo desta função é coletar e registrar informações sobre a utilização de recursos do ambiente OSI, associando tarifas às medidas de utilização.
A funcionalidade de medida de contabilização é definida através de dois objetos:

- **Objeto de controle de medida de contabilização** dedicado ao controle do gerenciamento de contabilização
- **Objeto de dados de medida de contabilização** - representa a utilização de um recurso por um determinado usuário

Atributos do Objeto de Controle de Medida de Contabilização

units of usage: unidade de medida da utilização de um recurso

recording triggers: eventos que causam a atualização dos dados de medida de contabilização;

reporting triggers: eventos que causam a emissão de notificação sobre informações de contabilização;

data object reference: dados de medida de contabilização sujeitos ao controle de medida de contabilização;

resource name: identifica o recurso a ser contabilizado.

Ações e Notificações de Controle de Medida de Contabilização

Ações:	Notificações:
Start metering	*Accounting Started*
Suspend metering	*Accounting Suspended*
Resume metering	*Accounting Resumed*

Atributos do Objeto de Dados de Medida de Contabilização

- requester id
- subscriber id
- service requested
- usage start time
- data object state
- resource name
- responder id
- meter info
- service provided
- usage meter time
- control object reference

Serviços da função de Medida de Contabilização

Gerenciamento de Medida de Contabilização:

- criação e remoção de instâncias de objetos de controle de medida de contabilização;
- leitura e modificação de atributos de objetos de controle de medida de contabilização.
- início, suspensão e retomada de medida de contabilização

Serviço de Dados de Medida de Contabilização:

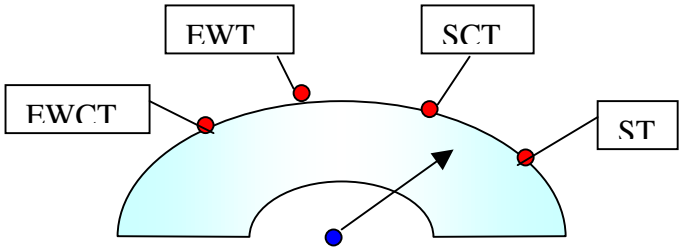
- criação e remoção de objetos de dados de medida de contabilização;
- recuperação de valores de atributos de objetos de dados de medida de contabilização.

9.11 Função de Monitoração de Carga de Trabalho

O objetivo desta função é avaliar a demanda e a utilização de recursos do ambiente OSI e a eficiência das atividades de comunicação.
A execução desta função deve possibilitar:

- obtenção de informações estatísticas;
- manutenção e análise dos registros de históricos do sistema;
- determinação do desempenho do sistema sob condições naturais e artificiais;
- alteração do modo de operação do sistema.

Modelos
Modelo de Utilização: monitoração do uso instantâneo de um recurso OSI.
Modelo de taxa de Rejeição: monitoração da rejeição de um pedido de serviço.
Modelo de Taxa de Pedido de Recursos: monitoração dos pedidos de uso de recursos OSI.
A figura 9.9 mostra o Modelo genérico para Monitoração de Carga.
Para cada um destes tipos de monitoração são definidos: o valor máximo aceitável (threshold), o valor de alerta e o valor em que a situação de alerta é removida.



EWCT - Early Warning Clear Threshold
EWT - Early Warning Threshold
SCT - Severe Clear Threshold
ST - Severe Threshold

Figura 9.9 - Modelo genérico para Monitoração de Carga

Objetos Métricos
Podem ter os seguintes atributos:

- identificação do objeto métrico;
- identificação do objeto gerenciado que está sendo observado e de seus atributos;
- identificação do algoritmo métrico usado nas observações;
- número de observações, frequência das observações e instante da última observação;
- programação das observações;
- indicação dos resultados das observações;
- valores para os quais são gerados alarmes;
- estado administrativo.

Serviços
Iniciação de Monitoração;
Finalização de Monitoração;
Suspensão da Monitoração;
Retomada da Monitoração;
Modificação dos atributos de um objeto métrico;
Leitura de atributos de objetos métricos.

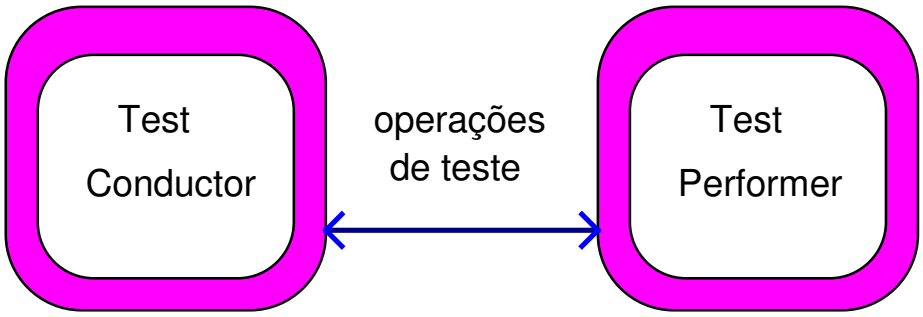
9.12 Função de Gerenciamento de Teste

Esta função tem como objetivo o controle remoto de testes e a especificação de testes a serem realizados sobre os recursos gerenciados. Considera que deva ser aplicável a diferentes metodologias de teste:

Testes de loopback
Testes de inserção de falhas
Autoteste

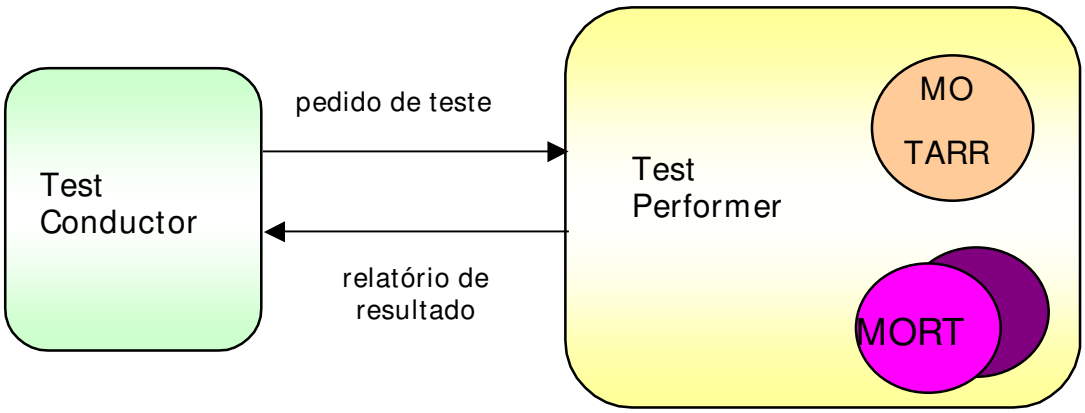
Ambiente de teste
Cada teste pode envolver a criação de um ambiente de teste, o controle e a monitoração das operações de teste e o retorno ao ambiente normal.
O controle de um teste consiste em suspender, retomar e finalizar o teste.
Os testes podem ser escalonados de forma periódica ou não periódica.

Modelo para a função de teste

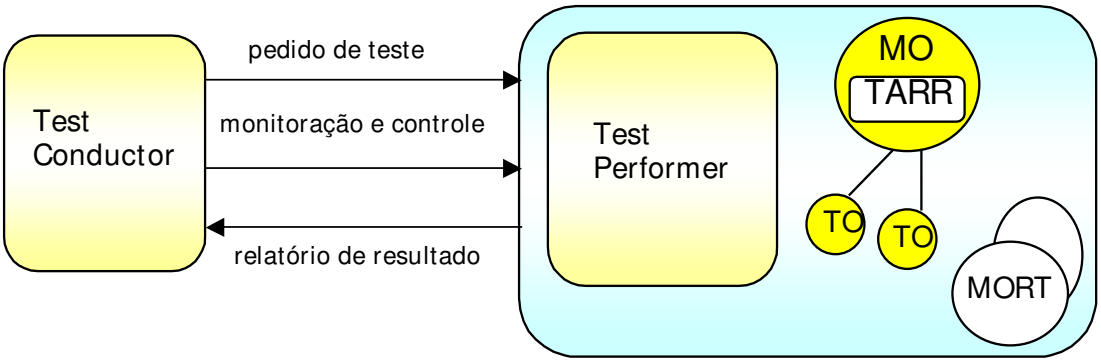


Funcionalidade TARR é capacidade que um objeto gerenciado possui para receber e responder a operações de teste.
MORT: objeto gerenciado usado como referência das funcionalidades que estão sendo testadas.
TO: objeto gerenciado que existe somente durante a execução de um teste controlado.

Testes não controlados



Teste controlável



TO - Test Object
MO - Managed Object
MORT - Managed Object Referring toTest
TARR - Test Action Request Receive

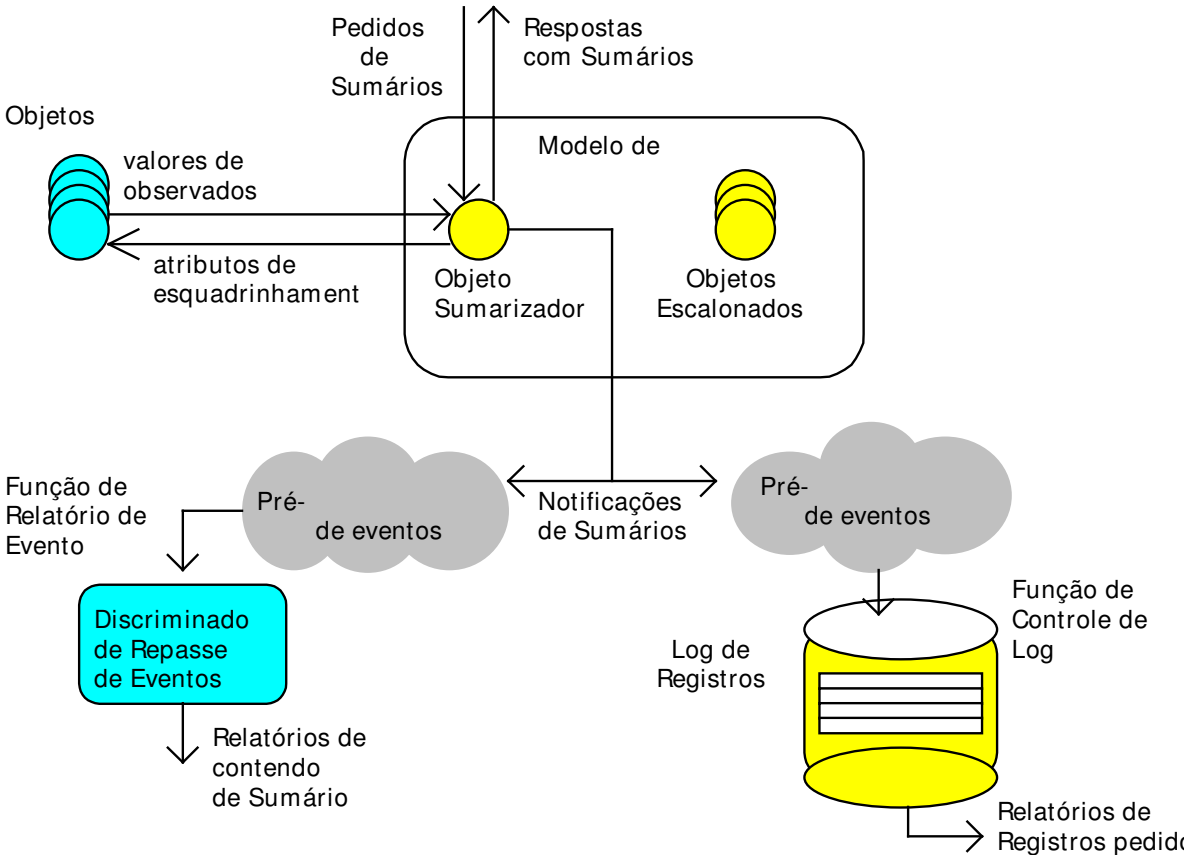
9.13 Função de Sumarização

O objetivo desta função é obter informações a partir de observações relativas a múltiplos objetos gerenciados e seus atributos, em um ou mais instantes distintos no tempo.

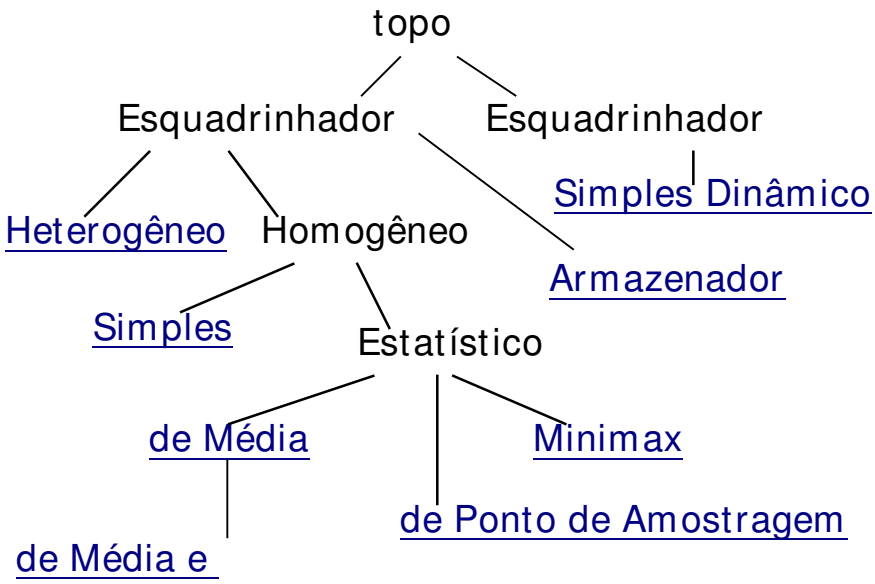
O processo de esquadrinhamento é especificado por meio de um atributo chamado esquadrinhador do objeto sumarizador.

É possível realizar o esquadrinhamento dos objetos e a emissão de relatórios de sumarização em base diária, semanal ou sob programação externa.

Modelo da Função de Sumarização



Classes de objetos de sumarização



10 Características das arquiteturas de gerenciamento

As arquiteturas de gerenciamento são classificadas em arquiteturas proprietárias e arquiteturas abertas. Esta classificação é realizada considerando-se aspectos relacionados à utilização de um modelo de informação padronizado bem como aos protocolos utilizados para a comunicação Gerente-Agente. Alguns exemplos de arquiteturas abertas são:

- Internet SNMP: Simple Network Management Protocol
- ISO/ITU-T CMIP: Common Management Information Protocol
- ODP/OMG CORBA: Common Object Request Broker Architecture

Uma arquitetura é dita fechada quando não se tem acesso às definições de seu modelo de informação ou aos protocolos utilizados na comunicação. A utilização de plataformas fechadas dificulta a interoperabilidade com outros sistemas, obrigando, muitas vezes, a uma dependência de soluções oferecidas por um único ou um número limitado de fornecedores.

As principais diferenças relacionadas com as arquiteturas abertas referem-se a:

- orientação a objetos ou a tipos de dados
- modelos de informação
- protocolo para comunicação
- funcionalidades

10.1 A utilização de plataformas de gerenciamento: mitos e fatos

Uma plataforma de gerenciamento é dita aberta quando apresenta uma arquitetura aberta e interfaces de programas aplicativos (API's) abertas.

Uma plataforma de software consolida e gerencia funções comuns que são usadas por aplicações independentes. É composta por comportamentos e serviços e provê um conjunto

comum de funções que são utilizadas por diferentes aplicações.

Uma plataforma de gerência de redes de propósito geral deverá prover serviços funcionais comuns aos domínios SNMP, CMISE, TL1 e ASCII

Uma plataforma inclui todos os módulos que são compartilhados entre diferentes aplicações de gerenciamento mas não inclui a funcionalidade de aplicações específicas. Portanto, a interface com a plataforma deve ser bem definida para permitir o desenvolvimento de aplicações, utilizando de forma transparente os serviços da plataforma;

Algumas plataformas são específicas para o gerenciamento da rede, limitando-se à oferta de serviços e protocolos de comunicação; outras podem oferecer serviços para outras aplicações que não são de gerência. Normalmente esta funcionalidade é obtida com um alto custo, através da integração de diferentes produtos. Se considerarmos a problemática existente no setor de telecomunicações, poderemos observar que os produtos ofertados estão longe de satisfazer às necessidades deste setor pois, na sua grande maioria, oferecem uma funcionalidade restrita a apenas uma porção de um nível funcional TMN (geralmente referem-se ao nível de gerencia de elemento de rede).

Atualmente, uma solução que vem sendo adotada é a utilização de plataformas integradoras. Estas plataformas geralmente contem serviços de comunicação que fornecem suporte para comunicação síncrona, assíncrona, transacional e interativa entre processos de aplicação de gerência e entre aplicações de gerência e os elementos de rede suportados. Podem oferecer, ainda, serviços de diretório, acesso de dados e funções de segurança. Os serviços de gerenciamento de dados podem fornecer suporte para a MIB, para a persistência de objetos e para sistemas de bases de dados. Os serviços de apresentação podem fornecer uma forma comum de observação entre processos de gerência divergentes.

10.2 A visão dos dados

O uso de plataformas de integração, permite a coleta de informações de vários sistemas e elementos da rede. O problema consiste em identificar quais dados são relevantes para serem recuperados

Muitos dados existem no sistema, mas estão armazenados em formatos incompatíveis para serem utilizados de forma integrada. Alguns dados precisam ser trabalhados e depois encaminhados para aplicações de níveis superiores na forma de porcentagens, médias, valores mínimo e máximo, etc...

Informações duplicadas, desconexas, incompatíveis proliferam em toda empresa devido às necessidades de desenvolvimento de aplicações específicas e urgentes;

A Engenharia de Informação é a disciplina utilizada para identificar necessidades de informação e para desenvolver sistemas de informação que produzem mensagens que fornecerão informação para atender algum objetivo. Ela é um processo de manufatura que utiliza dados como matéria prima, para construir e transmitir uma mensagem para um recipiente. Ela é também um processo de filtragem de grandes massas de dados para uma mensagem que provê informação.

O seu único objetivo é pegar o dado certo, para o pessoal certo, no lugar certo, no tempo

certo, na forma certa e com o custo certo, de tal forma que eles possam tomar decisões corretas e executar as ações corretas. Para isto, algumas técnicas têm sido apresentadas e as mais atuais referem-se ao Data Warehouse e ao Data mining.

10.3 Implantação de um sistema de gerência

A implantação de um sistema de gerência não é uma tarefa trivial e exige uma certa competência de seu coordenador e da equipe encarregada. A principal causa do descontentamento após a implantação de um sistema de gerência é devido ao fato desta tarefa ter sido subestimada e não ter sido dimensionada de forma adequada. Mesmo a implantação de sistemas simples possuem um custo razoável, seja este custo calculado em termos de aquisição ou em termos de tempo e de pessoal. Isto porque não existem soluções prontas. Qualquer solução exigirá um esforço de customização caso se deseje obter um sistema de gerência que seja útil. Para se alcançar os objetivos globais, muitas aplicações deverão ser desenvolvidas e integradas à plataforma adquirida.

A tarefa exige, portanto, um planejamento cuidadoso das metas a serem alcançadas e este planejamento exigirá uma equipe multidisciplinar com especialistas de vários departamentos da empresa e de fora da empresa.

De uma maneira simplificada, podemos estabelecer uma estratégia metodológica para a implantação de um sistema de gerência:

- Conhecimento do plano estratégico da empresa a fim de identificar seus objetivos e prioridades;
- Definição dos objetivos a serem alcançados com o sistema a ser implantado;
- Especificação dos serviços necessários para o alcance dos objetivos;
- Identificação das prioridades para identificar os serviços mais urgentes;
- Seleção da plataforma de integração considerando o atendimento aos serviços e/ou facilidades para o desenvolvimento de aplicações que proporcionem o seu atendimento;
- Modelagem das informações identificando aquelas que realmente serão úteis para o alcance dos objetivos;
- Desenvolvimento de novas aplicações para complementar o trabalho.

A equipe designada para o planejamento e implantação do sistema de gerência deve conter, pelo menos, um técnico especialista de cada área da empresa. Com isto procura-se assegurar uma abrangência da solução adotada evitando-se a perda de informações estratégicas para a empresa. Além destes componentes, será necessário integrar à equipe (caso esta participação ainda não tenha sido contemplada), pelo menos um especialista em projeto de bases de dados, um especialista em marketing, um especialista em modelagem de dados e um especialista no negócio da empresa.

O trabalho de implantação de um sistema de gerência passa primeiro por uma profunda conscientização do problema que se observa na empresa. A partir desta conscientização é necessária uma tomada de decisão que se constitui a parte mais difícil por envolver mudanças nos procedimentos e custos.

Uma vez tomada a decisão, o próximo passo consiste em selecionar a equipe

cuidadosamente, observando, inclusive, questões como relacionamentos pessoais. Esta equipe deverá, então, assumir a coordenação dos trabalhos estabelecendo o modelo do processo e selecionando as ferramentas que poderão auxiliar a tarefa do projeto.

Após cumprir as etapas da metodologia proposta anteriormente, a equipe poderá iniciar a especificação e implantação dos sistemas, sem esquecer de estabelecer um plano de contingência e de manutenção.

10.4 Considerações finais

A decisão de se implantar um sistema de gerenciamento deve estar embasada em diversos fatores. Muitas empresas desistem da idéia logo após tomarem conhecimento dos custos e dos riscos de desenvolvimento de um sistema deste porte. Outras optam por adquirir uma solução simplificada que, no futuro poderá deixar muito a desejar ocasionando geralmente, a desativação do sistema completamente.

Uma recomendação de política a ser seguida consiste em se analisar os riscos de não optar pelo desenvolvimento deste tipo de sistema. Caso a não adoção desta solução não afete a saúde da empresa (como, por exemplo, a sua perda de competitividade), então ela poderá adotar algumas soluções paliativas porém, o administrador da empresa deve sempre considerar que, caso a empresa apresente um crescimento, em muito pouco tempo este crescimento irá gerar a necessidade de implantação de um sistema de gerência que seja o mais abrangente possível.

Quando o sistema de gerência é implantado de forma consciente, o retorno de investimento é muito claro, isto é, a minimização ou mesmo a ausência de falhas, o aumento do desempenho, a integração e segurança das informações, a contabilização de utilização de recursos e o controle da configuração de sistemas e processos fornecem um ambiente extremamente saudável para a concretização de bons negócios.

11 Bibliografia

[Adams 97] Adams, E., Willetts, K. J., The Lean Communications Provider - Surviving the shakeout through Service Management Excellence. McGraw-Hill, 1997.

[Harnedy 97] Harnedy, S., Total SNMP - Exploring the Simple Network Management Protocol, Prentice Hall, Upper Saddle River, NJ, 1997.

LanTimes, diversos exemplares, 1998

[Perkins 97] Perkins, D., McGinnis, E., Understanding SNMP MIBs, Prentice Hall, Upper Saddle River, NJ, 1997.

[Spec-1 98] Specialski, E., Otimizando a integração de sistemas gerenciais em ambientes multifornecedor, Conferência sobre Tecnologia da Informação em Telecom, Institute for International Research, São Paulo, maio 1998.

[Spec-2 98] Specialski, E., A complexidade da tarefa de gerenciamento e sua automação, Workshop de Sistemas Inteligentes para o Gerenciamento de Redes, USP, São Paulo, junho 1998.

[Spec-3 98] Specialski, E., Aplicando Data Warehouse no ambiente de Telecomunicações. Seminário apresentado no Pós-Graduação em Engenharia de Produção, UFSC, julho, 1998.

[Tschichholz 95] Tschichholz, M., Hall,J., Abeck, S., Wies, R., Information Aspects and Future Directions in an Integrated Telecommunications and Enterprise Management Environment, Journal of Network and System Management, vol.3, Mar 1995.

[Wal 95] Waldbusser, S. Remote Network Monitoring Management Information Base, RFC 1757. Carnegie Mellon University, February 1995.

Alguns sites:

Tópicos iniciais sobre Gerência de Redes: http://www.hq.rnp.br/gerencia

IETF Home Page: http://www.ietf.org

IETF Structure and Internet Standards Proccess:

http://www.ietf.org/structure.html

Network Management Area

http://www.ietf.org/html.charters/wg-dir.html#Network_Management_Area

IETF MIB Modules: http://www.simple-times.org/pub/simple-times/html/

Enterprise specific MIBs (The SimpleWeb)

http://wwwsnmp.cs.utwente.nl/ietf/enterprise.html

RFC Editor: http://www.isi.edu/rfc-editor/overview.html

SunNet Manager:http://www.sun.com/sunsoft/solstice/net_mgt.html

SystemView

http://www.software.ibm.com/sysman/technology/

http://www.software.ibm.com/sysman/technology/snmpv2wp.html

IBM NetView for Windows Version 2
http://www.raleigh.ibm.com/nvm/nvmover.html

Hp-Openview

http://www.inotech.com/sample/index.html

http://hpcc998.external.hp.com:80/nsmd/ov/rpm/novntpr.htm

http:// hpcc998.external.hp.com:80/nsmd/ov/whatisov/wnm.html

POLYCENTER Manager on Netview (DEC)

http://www.networks.digital.com/npb/html/products_guide/polyntvw.html

Transcend (3COM)

http://www.3com.com/0files/products/dsheets/tnmunix.html

http://www.3com.com/0files/products/dsheets/400195.html

CiscoWorks (Cisco)

http://www.cisco.com/warp/public/734/cworks/index.html

Spectrum (Cabletron)

http://www.ctron.com/spectrum/

Patrol (BMC) - Gerencia aplicações HTTP, NFS, etc

http://www.bmc.com/products/pat/internet/index.html

What's UP (sistema monitor de redes -Win95)

http://www.ipswitch.com/pd_whatsup.html

HNMS (Sistema de Gerenciamento)

http://cognac.cosmic.uga.edu/pub/HNMS.html

Netscarf (ferramenta de monitoração de tráfego)

http://nic.merit.edu/~netscarf/proposal.html

12 Anexo: Informações sobre alarmes: Causa provável

This parameter defines further qualification as to the probable cause of the alarm. Probable cause values for notifications shall be indicated in the behaviour clause of the object class definition. This Recommendation | International Standard defines, for use within the Systems management application context defined in CCITT X.701 | ISO/IEC 10040, standard Probable causes that have wide applicability across managed object classes. These values are registered in CCITT X.721 | ISO/IEC 10165-2. The syntax of standard Probable causes shall be the ASN.1 type object identifier. Additional standard Probable causes, for use within the Systems management application context defined in CCITT X.701 | ISO/IEC 10040, may be added to this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Other Probable causes, for use within the Systems management application context defined in CCITT X.701 | ISO/IEC 10040, may be defined outside of this Recommendation | International Standard and registered using the procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Probable causes may be defined for use outside of the Systems management application context; the syntax of such Probable causes shall be either an ASN.1 object identifier or ASN.1 type integer.

The managed object class definer should choose the most specific Probable cause applicable.

This Recommendation | International Standard defines the following Probable causes

- adapter error;
- application subsystem failure: A failure in an application subsystem has occurred (an application subsystem may include software to support the Session, Presentation or Application layers);
- bandwidth reduced: The available transmission bandwidth has decreased;
- call establishment error: An error occurred while attempting to establish a connection;
- communications protocol error: A communication protocol has been violated;
- communications subsystem failure: A failure in a subsystem that supports communications over telecommunications links, these may be implemented via leased telephone lines, by X.25 networks, token-ring LAN, or otherwise;
- configuration or customization error: A system or device generation or customization parameter has been specified incorrectly, or is inconsistent with the actual configuration;
- congestion: A system or network component has reached its capacity or is approaching it;
- corrupt data: An error has caused data to be incorrect and thus unreliable;
- CPU cycles limit exceeded: A Central Processing Unit has issued an unacceptable number of instructions to accomplish a task;

- dataset or modem error: An internal error has occurred on a dataset or modem;
- degraded signal: The quality or reliability of transmitted data has decreased;
- DTE-DCE interface error: A problem in a DTE-DCE interface, which includes the interface between the DTE and DCE, any protocol used to communicate between the DTE and DCE and information provided by the DCE about the circuit;
- enclosure door open;
- equipment malfunction: An internal machine error has occurred for which no more specific Probable cause has been identified;
- excessive vibration: Vibratory or seismic limits have been exceeded;
- file error: The format of a file (or set of files) is incorrect and thus cannot be used reliably in processing;
- fire detected;
- flood detected;
- framing error: An error in the information that delimits the bit groups within a continuous stream of bits;
- heating/ventilation/cooling system problem;
- humidity unacceptable: The humidity is not within acceptable limits;
- I/O device error: An error has occurred on the I/O device;
- input device error: An error has occurred on the input device;
- LAN error: An error has been detected on a local area network;
- leak detected: A leakage of (non-toxic) fluid or gas has been detected;
- local node transmission error: An error occurred on a communications channel between the local node and an adjacent node;
- loss of frame: An inability to locate the information that delimits the bit grouping within a continuous stream of bits;
- loss of signal: An error condition in which no data is present on a communications circuit or channel;
- material supply exhausted: A supply of needed material has been exhausted;
- multiplexer problem: An error has occurred while multiplexing communications signals;
- out of memory: There is no program-addressable storage available;
- output device error: An error has occurred on the output device;
- performance degraded: Service agreements or service limits are outside of acceptable limits;
- power problem: There is a problem with the power supply for one or more resources;
- pressure unacceptable: A fluid or gas pressure is not within acceptable limits;

- processor problem: An internal machine error has occurred on a Central Processing Unit;
- pump failure: Failure of mechanism that transports a fluid by inducing pressure differentials within the fluid;
- queue size exceeded: The number of items to be processed (configurable or not) has exceeded the maximum allowable;
- receive failure;
- receiver failure;
- remote node transmission error: An error occurred on a communication channel beyond the adjacent node;
- resource at or nearing capacity: The usage of a resource is at or nearing the maximum allowable capacity;
- response time excessive: The elapsed time between the end of an inquiry and beginning of the answer to that inquiry is outside of acceptable limits;
- retransmission rate excessive: The number of repeat transmissions is outside of acceptable limits;
- software error: A software error has occurred for which no more specific Probable cause can be identified;
- software program abnormally terminated: A software program has abnormally terminated due to some unrecoverable error condition;
- software program error: An error has occurred within a software program that has caused incorrect results;
- storage capacity problem: A storage device has very little or no space available to store additional data;
- temperature unacceptable: A temperature is not within acceptable limits;
- threshold crossed: A limit (configurable or not) has been exceeded;
- timing problem: A process that requires timed execution and/or coordination cannot complete, or has completed but cannot be considered reliable;
- toxic leak detected: A leakage of toxic fluid or gas has been detected;
- transmit failure;
- transmitter failure;
- underlying resource unavailable: An entity upon which the reporting object depends has become unavailable;
- version mismatch: There is a conflict in the functionality of versions of two or more communicating entities which may affect any processing involving those entities.