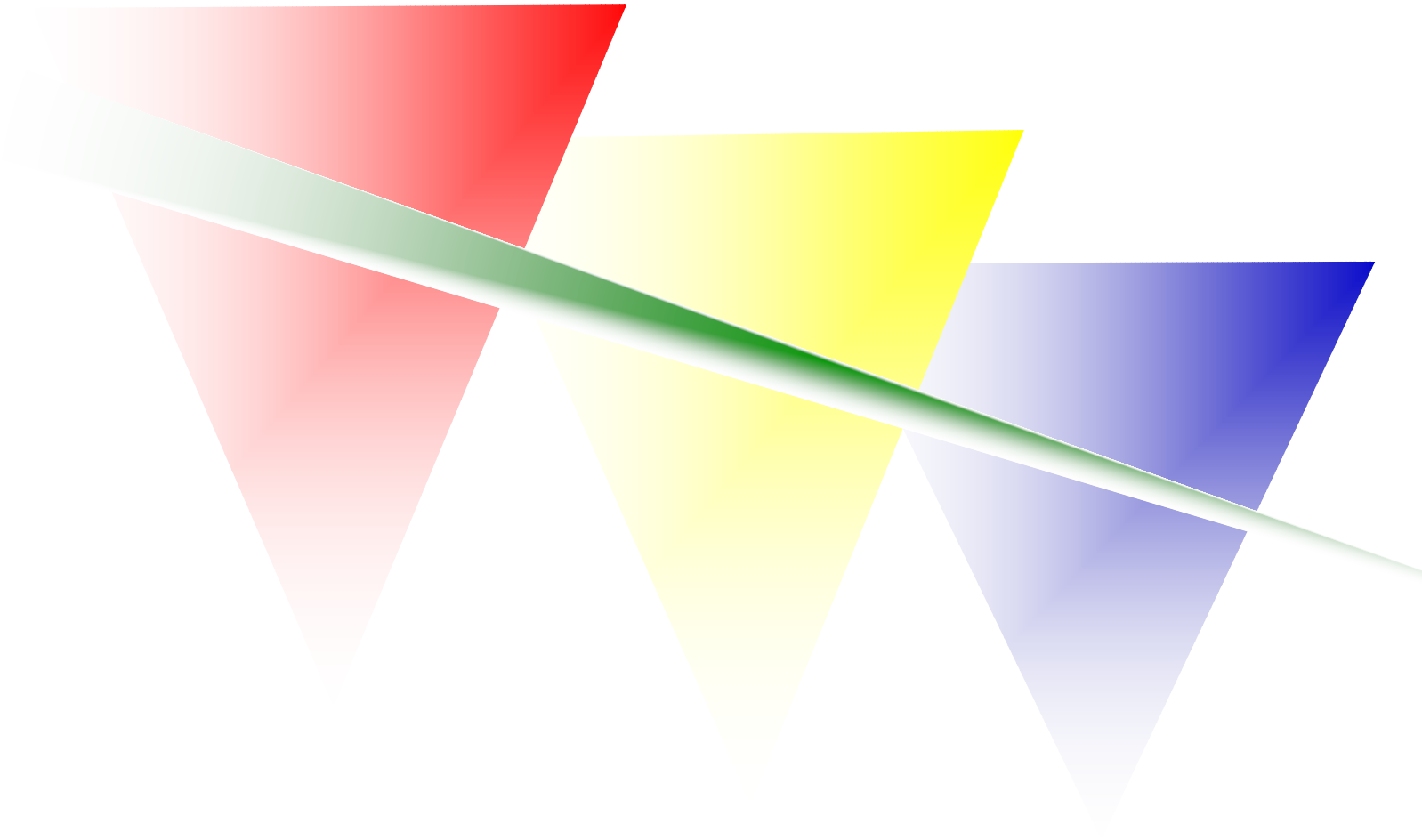
Gerenciamento de Redes de Computadores



José Maurício dos Santos Pinheiro
Versão 2.0 – Agosto 2002

ÍNDICE

Introdução

As redes de computadores foram concebidas, inicialmente, como um meio de compartilhar dispositivos periféricos tais como impressoras, modems de alta velocidade, dentre outros, existindo apenas em ambientes acadêmicos, governamentais e em empresas de grande porte. Entretanto, a rápida evolução das tecnologias de redes aliada à grande redução de custos dos recursos computacionais, motivou a proliferação das redes de computadores por todos os segmentos da sociedade.

À medida que essas redes foram crescendo e tornaram-se integradas às organizações, o compartilhamento dos dispositivos tomou aspecto secundário em comparação às outras vantagens oferecidas. As redes passaram então a fazer parte do cotidiano das pessoas como uma ferramenta que oferece recursos e serviços que permitem uma maior interação e um conseqüente aumento de produtividade.

Além disso, ocorreu uma grande mudança nos serviços oferecidos, pois além do compartilhamento de recursos, novos serviços, tais como correio eletrônico, transferência de arquivos, Internet, aplicações multimídia, dentre outras, foram acrescentadas, aumentando a complexidade das redes. Não bastassem esses fatos, o mundo da interconexão de sistemas de computadores ainda tem que conviver com a grande heterogeneidade dos padrões de redes, sistemas operacionais, equipamentos, etc.

Considerando este quadro, torna-se cada vez mais necessário o gerenciamento do ambiente de redes de computadores para mantê-lo funcionando corretamente. Surge a necessidade de buscar uma maneira consistente de realizar o gerenciamento de redes para, com isso, manter toda a estrutura da rede funcionando de forma a atender as necessidades de seus usuários e às expectativas de seus administradores.

O contínuo crescimento em número e diversidade de componentes das redes de computadores também tem contribuído para que a atividade de gerenciamento de rede se torne vez mais imprescindível. Os benefícios da integração dos sistemas computacionais de uma empresa, de natureza e portes diferentes, como forma de distribuir as tarefas e compartilhar os recursos disponíveis, são hoje uma realidade. As grandes redes corporativas, que são inter-redes formadas pela interconexão de pequenas redes locais, assumiram um papel fundamental para os negócios das empresas que delas se utilizam. Por este motivo, estas redes requerem um sistema de gerenciamento eficiente para que as informações da corporação estejam sempre disponíveis no local e no momento onde forem requisitadas.

Desde a década de 80 vários grupos têm trabalhado para definir arquiteturas padronizadas (e abertas) para o gerenciamento de redes heterogêneas, ou seja, redes compostas por equipamentos de diferentes fabricantes. As principais arquiteturas abertas de gerenciamento de redes são relacionadas às tecnologias TCP/IP e OSI da ISO e estas são conhecidas mais facilmente pelos nomes dos protocolos de gerenciamento utilizados: Simple Network Management Protocol - SNMP do TCP/IP e o Common Management Information Protocol - CMIP de OSI.

Muitos produtos de gerenciamento já foram desenvolvidos obedecendo estes padrões. Por razões históricas, os primeiros produtos seguiram o padrão SNMP e até

hoje este é o protocolo que possui o maior número de implementações. Embora atualmente existam algumas aplicações de gerenciamento muito sofisticadas, a maioria destas aplicações possibilita apenas o monitoramento dos nós de uma rede e não possui “inteligência” para auxiliar os administradores de rede na execução de sua tarefa.

A arquitetura de gerenciamento SNMP, adotada na tecnologia TCP/IP, supõe a existência de estações de gerenciamento, onde são executadas as aplicações de gerenciamento e os nós gerenciados, que são os elementos da rede (estações, roteadores e outros equipamentos de comunicação), que desempenham funções de comunicação na operação normal da rede, através dos chamados protocolos úteis. Estes protocolos são instrumentados para permitir o monitoramento e controle do seu funcionamento.

Uma parte significativa do processo de gerenciamento baseia-se na aquisição de informações sobre a rede, sendo as mais importantes àquelas relativas a erros, falhas e outras condições excepcionais. Tais dados devem ser armazenados em forma bruta, sendo importante definir os valores aceitáveis como limiares de tolerância que, quando ultrapassados, determinam uma sinalização para pedir intervenção de um operador, ou o início de uma operação corretiva. Tais limites não são necessariamente absolutos, tais como a taxa de erros num enlace de dados, sendo necessário dispor de estatísticas de erros em função do tráfego existente. Um determinado limiar pode ser aceitável numa situação de carga leve na rede, mas intolerável numa outra situação, de carga mais intensa, no qual o número de retransmissões faria com que o tráfego total excedesse a capacidade do enlace, afetando seriamente o tempo de resposta.

Capítulo 1 - Gerenciamento em Redes de Computadores

1.0 Gerência de Redes

A gerência em redes de computadores torna-se tarefa complexa em boa parte por conseqüência do crescimento acelerado das mesmas tanto em desempenho quanto em suporte a um grande conjunto de serviços. Além disso, os sistemas de telecomunicações, parte importante e componente das redes, também adicionam maior complexidade, estando cada vez mais presentes, mesmo em pequenas instalações.

Admitindo-se que as ferramentas para gerência de redes não abrangem toda a gama de problemas de uma rede e que estas nem sempre são usadas nas organizações que possuem redes, se faz necessário que outros mecanismos de gerência sejam utilizados para suprir suas carências mais evidentes.

As informações que circulam em uma rede de computadores devem ser transportadas de modo confiável e rápido. Para que isso aconteça é importante que os dados sejam monitorados de maneira que os problemas que porventura possam existir sejam detectados rapidamente e sejam solucionados eficientemente. Uma rede sem mecanismos de gerência pode apresentar problemas que irão afetar o tráfego dos dados, bem como sua integridade, como problemas de congestionamento do tráfego, recursos mal utilizados, recursos sobrecarregados, problemas com segurança entre outros.

O gerenciamento está associado ao controle de atividades e ao monitoramento do uso dos recursos da rede. A tarefa básica que uma gerência de rede deve executar envolve a obtenção de informações da rede, tratar estas informações possibilitando um diagnóstico seguro e encaminhar as soluções dos problemas. Para cumprir estes objetivos, funções de gerência devem ser embutidas nos diversos componentes da rede, possibilitando descobrir, prever e reagir a problemas.

Para resolver os problemas associados à gerência em redes a ISO através do OSI/MN propôs três modelos:

- **O Modelo Organizacional** que estabelece a hierarquia entre sistemas de gerência em um domínio de gerência, dividindo o ambiente a ser gerenciado em vários domínios.
- **O Modelo Informacional** que define os objetos de gerência, as relações e as operações sobre esses objetos. Uma MIB é necessária para armazenar os objetos gerenciados.
- **O Modelo Funcional** que descreve as funcionalidades de gerência: gerência de falhas, gerência de configuração, gerência de desempenho, gerência de contabilidade e gerência de segurança.

1.1 – Informação Gerencial

A base da informação gerencial (MIB - *Management Information Base*) é um banco de dados que armazena informações referentes a todos os objetos gerenciados (incluindo seus atributos, operações e notificações). Os objetos gerenciados dentro da MIB são definidos em termos de:

- **Atributos** - Propriedades dos objetos gerenciados.
- **Operações** - São as ações que os *Agentes* podem submeter ao *Gerente* para informar sobre a ocorrência de eventos nos objetos gerenciados;
- **Notificações** - São informações que os *Agentes* podem emitir ao *Gerente* para informar sobre a ocorrência de eventos nos objetos gerenciados;
- **Relações** - as formas de comunicação entre os objetos.

As definições dos objetos gerenciados na MIB dependem do padrão usado no sistema de gerência. No caso do modelo OSI, os objetos são definidos de acordo com os atributos, operações, notificações e relações:

- Os atributos são as propriedades dos objetos que podem ter valores simples ou complexos.
- As operações dizem respeito às operações a que estão submetidos os objetos.
- As notificações são informações que os agentes enviam ao gerente para informar sobre eventos nos objetos de sua base de informações local.
- A relação diz respeito à relação de um objeto com outros.

A MIB segue uma arquitetura do tipo árvore, onde as informações referentes a objetos da árvore estão nas suas folhas.

1.2 – Arquitetura em árvore da MIB

Basicamente são definidos quatro tipos de MIB's: MIBI, MIBII, MIB experimental e MIB privada. As MIB's do tipo I e II fornecem informações gerais sobre o equipamento gerenciado, sem levar em conta as características específicas deste equipamento. A MIBII, em verdade, é uma evolução da MIBI, que introduziu novas informações além daquelas encontradas na MIBI. Portanto, através das MIB's do tipo I e II é possível obter informações como tipo e status de interface (Ethernet, FDDI, Token-Ring), número de pacotes transmitidos, número de pacotes com erro, informações de protocolos de transmissão etc.

As MIB's experimentais são aquelas que estão em fase de testes, com a perspectiva de serem adicionadas ao padrão e que, em geral, fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.

As MIB's privadas são específicas dos equipamentos gerenciados, possibilitando que detalhes peculiares a um determinado equipamento possam ser obtidos. É desta forma que é possível se obter informação sobre colisões, configuração, swap de portas, e muitas outras, de um hub. Também é possível fazer um teste, reinicialização ou desabilitar uma ou mais portas do hub através de MIB's proprietárias.

Um objeto da MIB obtém seu nome da posição em uma estrutura hierárquica na forma de uma estrutura de dados do tipo árvore. Nesta estrutura as informações referentes a objetos da árvore estão nas suas folhas. A principal questão é: como identificar uma folha na árvore da MIB?

Deve-se observar que a estrutura da árvore contém um tronco principal e um conjunto de galhos. Dessa forma, para chegar a informação referente a um objeto folha, basta usar pontos para separar cada galho da árvore. Observar também que o nó principal da árvore (o tronco) é identificado por um ponto (**.**).

Assim para chegarmos acessar o objeto referente à Folha02 da figura seguinte, tem-se:

.Galho_T1_03.Galho_T2_02.Galho_T3_03.Folha02

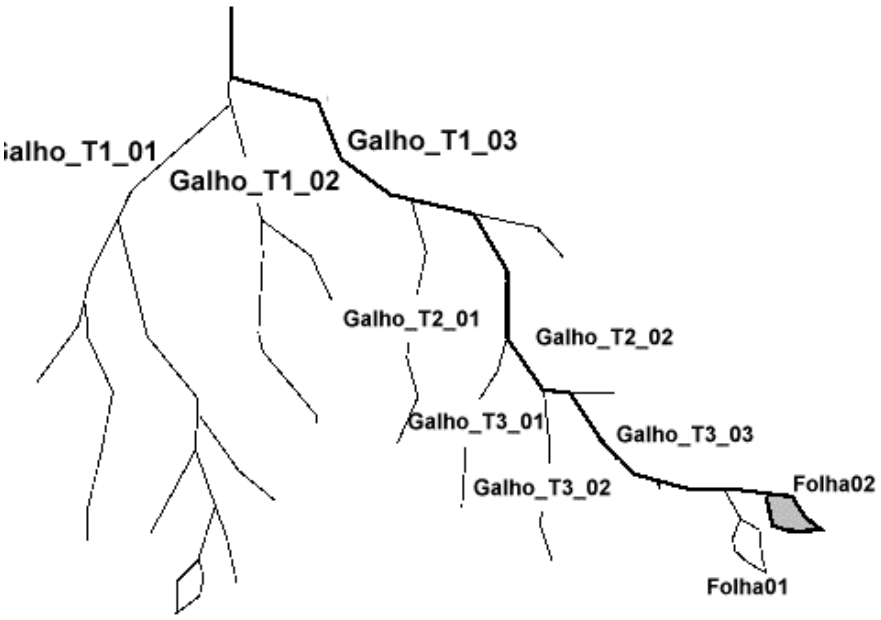


Figura 1 - Arquitetura Árvore da MIB

1.3 – Objeto gerenciado, Gerente e Agente

Um *objeto gerenciado* é um termo que pode ser definido como uma representação abstrata das características relativas ao gerenciamento de um recurso real da rede. O termo objeto tem sido utilizado devido à técnica de orientação a objetos que tem se estabelecido como um paradigma muito utilizado na modelagem de sistemas. Os processos de gerenciamento usados em atividades de gerenciamento podem ser classificados como *processo gerente* ou *processo agente*.

- Um processo gerente é parte de uma aplicação distribuída que tem a responsabilidade de uma ou mais atividades de gerenciamento, ou seja, ele transmite operações de gerenciamento (*actions*) aos agentes e recebe notificações (*events*) destes.

- Um processo é dito *agente* quando parte de uma aplicação distribuída irá executar as diretivas enviadas pelo processo *gerente*. Assim, ele passará para o Gerente uma visão dos objetos sendo gerenciados e refletirá o comportamento desses objetos, emitindo notificações sobre os mesmos.

O código de um agente é constituído por uma função de gerenciamento - contadores, rotinas de teste, temporizadores, etc, que permite o controle e gerenciamento do objeto gerenciado. Já a instrumentação de gerenciamento está tipicamente associada a uma estrutura particular de gerenciamento, que especifica as regras empregadas para definir a informação referente a um objeto referenciado, permitindo, assim, que este possa ser monitorado e gerenciado.

A **SMI (*Structure Management Information***), como é chamada esta instrumentação, é análoga à linguagem de programação usada para construir estruturas de dados e permitir operações que possam ser executadas sobre essas estruturas. A combinação de uma SMI com um protocolo particular é denominada framework.

1.4 - Definição do gerenciamento

O gerenciamento de redes de computadores pode ser definido como a coordenação (controle de atividades e monitoração de uso) de recursos materiais (modems, roteadores, etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações. O modelo clássico de gerenciamento pode ser sumarizado em três etapas:

- **Coleta de dados:** um processo, em geral automático, que consiste de monitoração sobre os recursos gerenciados.
- **Diagnóstico:** esta etapa consiste no tratamento e análise realizados a partir dos dados coletados. O computador de gerenciamento executa uma série de procedimentos (por intermédio de um operador ou não) com o intuito de determinar a causa do problema representado no recurso gerenciado.
- **Ação ou controle:** Uma vez diagnosticado o problema, cabe uma ação, ou controle, sobre o recurso, caso o evento não tenha sido passageiro (incidente operacional).

1.5 - O que gerenciar

Dependendo da ênfase atribuída aos investimentos realizados no ambiente de processamento de dados, as funções de gerência de rede podem ser centralizadas no processador central ou distribuídas em diversos ambientes locais. O gerenciamento de rede implica na utilização de várias ferramentas inseridas em uma estrutura, de certa forma complexa, com os limites de atuação definidos, se possível padronizado, entre os componentes envolvidos. Esta estrutura pode definir aspectos como: a estratégia empregada no atendimento/chamadas dos usuários, atuação do pessoal envolvido nas tarefas de gerenciamento de rede, supridores de serviços, etc.

O foco para as atividades de gerenciamento de rede é a organização e, aspectos como o atendimento do usuário, se caracterizam como primordial para o sucesso da estrutura. É desejável que o usuário dos serviços de rede tenha um único ponto de contato para reportar problemas e mudanças.

Os limites de atuação desta gerência devem levar em conta a amplitude desejada pelo modelo implantado na instalação que, além de operar a rede, deve envolver tarefas como:

- Controle de acesso à rede;
- Disponibilidade e desempenho;
- Documentação de configuração;
- Gerência de mudanças;
- Planejamento de capacidade
- Auxílio ao usuário;
- Gerência de problemas;
- Controle de inventário.

A ênfase relativa atribuída em cada uma dessas categorias por uma instalação depende do tamanho e complexidade da rede.

1.6 - A rede do ponto de vista do usuário

De um ponto de vista técnico, observa-se que as redes de computadores estão em constante expansão, tanto fisicamente como em de complexidade. Entretanto, para o usuário final a rede é vista como algo muito simples, ou seja, apenas um recurso que oferece ferramentas que facilitam suas atividades cotidianas. Desta forma, para o usuário, os sistemas de computação devem estar disponíveis o tempo todo para auxiliá-lo a atingir objetivos como vendas, qualidade, rapidez, eficiência etc.

Então, deve-se considerar qual seria o verdadeiro impacto de uma eventual parada nos servidores de redes, em uma paralisação parcial, em apenas uma linha ou estação de trabalho. Situações como estas devem ser levadas em conta antes da elaboração de qualquer modelo de gerência de redes, pois a partir de respostas a questões como estas é que se pode elaborar uma estrutura mínima.

Qualquer que seja a estrutura implantada, para se obter resultado dentro de padrões aceitáveis de serviços e informações, para o usuário final, além de ferramentas, é fundamental o bom nível técnico do pessoal envolvido com as atividades administrativas e de gerência da rede.

Capítulo 2 - Protocolos de gerenciamento

Os protocolos de gerenciamento têm a função de garantir a comunicação entre os recursos de redes homogêneas ou não. Com esse requisito satisfeito, operações de gerenciamento podem ser realizadas. Vários produtos têm surgido com a finalidade de gerenciar a rede, quase que em sua totalidade baseados no padrão SNMP e CMIP. Geralmente estes produtos de gerenciamento de redes incorporam funções gráficas para o operador de centro de controle.

Porém os dois protocolos que mais se desenvolveram foram o CMIP *(Common Management Information Protocol)* e o SNMP*(Simple Network Management Protocol)*, respectivamente, protocolos do modelo OSI *(Open System Interconnection)* e da arquitetura TCP/IP.

2.1 – Protocolo CMIP

O protocolo CMIP é o protocolo OSI do Nível de Aplicação, orientado a conexão e utiliza os serviços providos pelo ASCE (Association Control Service Element), ROSE (Remote Operations Service Element) e pelo serviço de apresentação. O CMIP trabalha em conjunto com o CMIS (*Common Management Information Service),* uma interface de serviço que descreve os serviços de gerenciamento OSI oferecidos às aplicações de gerenciamento. A utilização dos padrões da ISO para gerenciamento têm sido sustentadas pela OSF, que está comprometida, através do OSF/DME (Open Software Foundation/Distributed Management Environment), em suportar os padrões OSI de gerenciamento. A função do DME é fornecer facilidades que permitam integrar o gerenciamento de sistemas em ambientes heterogêneos, satisfazendo três requisitos básicos: interoperabilidade, consistência e flexibilidade.

A interface CMIS define as seguintes primitivas de gerenciamento para o modelo OSI:

- **M-EVENT-REPORT** – utilizada para envio de notificações a um gerente.
- **M-GET** – utilizada pelo gerente para requisitar informações de gerenciamento ao agente.
- **M-SET** – utilizada pelo gerente para requisitar modificações de informações de gerenciamento ao agente.
- **M-ACTION** – utilizada para invocar um procedimento pré-definido, especificado como parte de um objeto gerenciado.
- **M-CREATE** – utilizada para solicitar a criação de uma nova instância de uma classe de objetos.
- **M-DELETE** – utilizada para remover uma ou mais instâncias de objetos.
- **M-CANCEL-GET** – utilizada para terminar uma operação de GET muito demorada.

2.2 – Protocolo CMOT

Com o aparecimento da Internet e da arquitetura TCP/IP, surgiu a necessidade de desenvolver um protocolo de gerenciamento que interligasse essa arquitetura ao modelo de gerenciamento OSI, mas especificamente que a estrutura de gerenciamento OSI pudesse ser aplicada sobre os objetos gerenciados de uma rede TCP/IP. O CMOT (CMIP sobre TCP/IP) baseia-se na estrutura de gerenciamento do OSI e nos modelos, serviços e protocolos desenvolvidos pela ISO.

2.3 – Protocolo SNMP

A necessidade de mecanismos de gerenciamento nas redes baseadas em TCP/IP é atendida pelo SNMP em associação com o esquema de MIB, que também é suportado pelo padrão OSF/DME. Uma das vantagens do SNMP é a simplicidade e facilidade de implementação. Assim, isso a grande maioria dos problemas de gerenciamento podem ser contornados com o TCP/IP.

O SNMP *(Simple Network Management Protocol)* é um protocolo de gerenciamento da camada de aplicação da arquitetura TCP/IP sendo o mais utilizado por ser simples e fácil de implementar. Esse protocolo foi projetado nos anos 80 com um intuito de provisoriamente solucionar os problemas de comunicações entre redes heterogêneas.

O sucesso do SNMP reside no fato de ter sido ele o primeiro protocolo de gerenciamento não proprietário, público, fácil de ser implementado e que possibilita o gerenciamento efetivo de ambientes heterogêneos. Existem três versões desse protocolo. A segunda versão tenta dar suporte para a transferência eficiente de grandes blocos de dados e dar estratégias de gerenciamento de rede centralizado, problemas que não foram abordados na primeira versão. Outra questão que não foi implementada na versão SNMP1 foi a segurança, que é a principal meta da versão SNMP3.

No gerenciamento SNMP é adicionado um componente ao *hardware* (ou *software*) que estará sendo controlado recebendo o nome de agente. Este agente é encarregado de coletar os dados dos dispositivos e armazená-los em uma estrutura MIB - *Management Information Base*. Além desta base de dados, normalmente é desenvolvido um *software* aplicativo com a habilidade de sumarizar estas informações e exibi-las nas estações encarregadas das tarefas de monitorar a rede. Estas estações são chamadas de nó gerente e é onde processos gerentes são executados.

Os pioneiros na implantação dos protocolos SNMP foram os fornecedores de gateways, bridges e roteadores. Normalmente, o fornecedor desenvolve o agente SNMP e posteriormente desenvolve uma interface para a estação gerente da rede. Em geral, estes produtos funcionam para vários sistemas operacionais, como VMS, SUN-OS, DOS, AIX e outros, sendo muito comum que estes fornecedores incluam bibliotecas e utilitários que permitam a criação de aplicações de gerenciamento com características específicas para alguns componentes da rede. As implementações básicas do SNMP permitem monitorar e isolar falhas, já as aplicações mais sofisticadas permitem gerenciar o desempenho e a configuração da rede. Estas

aplicações, em geral, incorporam menus e alarmes para facilitar a interação com o profissional que está gerenciando a rede.

A utilização do SNMP para gerenciamento de rede na Internet é produto de vários mitos. Os dois mais críticos e de maior relevância são: o mito do colapso de rede e o mito do agente bobo.

A escolha da utilização de UDP como protocolo de transporte para o SNMP, aconteceu devido ao fato deste tipo de protocolo não orientado a conexão ter a habilidade de continuar funcionando quando a rede falha. O mito diz que se fosse utilizada uma conexão TCP, esta seria desfeita enquanto que o UDP continuaria funcionando para salvar o dia. Só que existe uma diferença básica entre gerenciamento de redes em termos de monitoração e gerenciamento de redes em termos de resolução de problemas. Hoje em dia, a totalidade do gerenciamento de redes que vem sendo feito é quando a rede não está falhando, e até porque hoje quando há uma pane de rede é devido a problemas físicos e assim nem o TCP nem tão pouco o UDP irão funcionar. Com este ponto de vista, nós podemos dizer que as vantagens da utilização do UDP como protocolo de transporte é realmente apenas um mito, e que o TCP pode ser utilizado como protocolo de transporte para o SNMP e com vantagens quando se está fazendo monitoração.

Outro ponto importante é que os algoritmos criados para prevenir congestionamento de TCP fizeram com que o uso de mensagens TCP se comportasse bem melhor para aliviar congestionamentos que mensagens UDP. Além disso, é esperado que se possa requisitar prioridade ao tráfego de gerenciamento de redes. Com isso, tendo um caminho já estabelecido, pode-se monitorar e controlar a rede, não importando quão congestionada ela esteja.

Para se fazer resolução de problema num caso de falha na rede, é necessário que sejam desenvolvidas ferramentas e técnicas diferentes das utilizadas hoje para monitoração e controle. Até porque o uso de SNMP para este tipo de tarefa é bem menos eficiente que utilizar ferramentas como *ping*, *nslookup*, *traceroute* e *mtrace*.

Um outro grande mito criado é o do agente bobo. Sempre se ouviu falar que alguns dispositivos de rede só possuem capacidade de processamento suficiente apenas para suportar um agente SNMP. Por este motivo, foi criado o conceito de agente *proxy* para que dispositivos com pouca capacidade de processamento pudessem ser gerenciados. Hoje os dispositivos de rede possuem mais capacidade de processamento e memória que as próprias estações de gerenciamento de antes. Com esta evolução nos dispositivos, alguns deles hoje são capazes de gerenciar a si próprios se assim se desejar. Com isso, derruba-se este mito de que os agentes têm que ser simples e bobos, e que só uma estação com maior capacidade de processamento teria a capacidade de ser gerente.

O esquema dos produtos desenvolvido com o protocolo SNMP é um pouco diferente dos produtos que utilizam o protocolo CMIP. Os fornecedores de produtos que utilizam o protocolo CMIP pressupõem que os fabricantes possuam algum tipo de gerenciamento em seus equipamentos, portanto estas informações podem ser disponibilizadas para um integrador via protocolo CMIP. O conceito de integrador foi definido em três níveis: o mais baixo, que contém os agentes e os elementos gerenciadores, o intermediário, que consiste em elementos do sistema de gerenciamento, e finalmente o nível mais alto, que consiste no integrador dos sistemas de gerenciamento. Produtos como o NetView da IBM, Accumaster da AT& T, Allink da

Nynex e o SunNet Manager da Sun Microsiytems, dentre outros, são exemplos deste tipo de implementação.

A dificuldade maior para uma aplicação integradora é que os fornecedores não têm as mesmas variáveis de gerenciamento e tampouco as mesmas operações em seus servidores de objetos. A escolha entre um ou outro protocolo de gerenciamento deve recair sobre o tipo de rede e dos produtos a ela agregados, sendo que podem ser mesclados os dois protocolos.

O SNMP e seu Internet Standard Network Management Framework são adequados a agentes simples e fáceis de implementar, enquanto o CMIP e o seu framework Network Management Forum Release 1.0 são adequados para agentes com um ou mais servidores de objetos dentro da modalidade cliente-servidor orientado para objeto, dentre os quais inclui-se o RPC.

O protocolo SNMP define também algumas primitivas de gerenciamento:

- **Primitiva Get -** O *Get* é uma primitiva usada pelo gerente para ler algum valor na MIB. O gerente inicialmente envia uma mensagem de *get-request* ao agente, tendo como parâmetro a identificação do objeto cujo valor é requerido. Essa identificação pode ser uma seqüência de nomes separados por pontos ou uma seqüência de números também separados por pontos. Essa seqüência de números ou nomes é um espelho da organização hierárquica da MIB. Em seguida, o agente consulta a MIB e responde à requisição do gerente com a primitiva *get-response*, levando o valor do objeto.

- **Primitiva Set -** O *Set* é uma primitiva usada pelo gerente para escrever algum valor na MIB. Inicialmente, o gerente envia a primitiva de requisição *set-request* ao agente, passando como parâmetros o identificador do objeto cujo valor será alterado e o novo valor que o objeto receberá. O identificador dos objetos tem as características especificadas na primitiva get. Em seguida, o agente modifica o valor do objeto na MIB e envia uma mensagem de resposta ao gerente, *get-response.*

- **Primitiva Get Next Request -** Esta primitiva tem as mesmas características e faz as mesmas funções da primitiva get, porém quando o gerente faz uma requisição ao agente passando como parâmetro o identificador de um determinado objeto, ele irá receber como resposta o valor do objeto sucessor a este. Essa leitura sucessiva segue o percurso da árvore de identificação da MIB.

- **Primitiva Trap -** Essa primitiva, ao contrário das anteriores, é utilizada pelo agente para informar ao gerente que algum evento anormal aconteceu. Essa primitiva pode ser usada a qualquer momento, não precisando de uma requisição do gerente pra ser usada. Outra diferença com relação as demais primitivas é que ela não necessita de uma resposta.

2.4 – Protocolo RMON

Enquanto o SNMP trabalha limitadamente, onde o gerente obtém apenas informações de um determinado equipamento, os monitores do RMON *(Remote MONitoring),* também chamados de *probes*, trabalham em modo promíscuo, capturando as informações do tráfego da rede como um todo. O RMON é a capacidade de gerenciamento remoto do SNMP, porém, tenta diminuir a quantidade de informações trocadas entre a rede local gerenciada e a estação gerente. Os agentes que implementam a RMON MIB possuem cinco funções:

1. **Operações *Off-line*:** operações que permitem ao agente continuar executando suas tarefas mesmo que a comunicação com a estação de gerenciamento não seja possível ou esteja com problemas.
2. **Monitoração pró-ativa:** permite executar continuamente diagnósticos e manter *logs* do desempenho das redes a fim de desenvolver a função de *baseline*, isto é, manter históricos das operações normais por um tempo estendido e em seguida fazer uma análise para identificar problemas potenciais na rede.
3. **Detecção e registro de problemas:** o monitor RMON pode reconhecer determinadas condições das redes fazendo constantes averiguações com o objetivo de informar ao gerente sobre eventos e situações de erros significativos para a rede.
4. **Valorização dos dados coletados:** o monitor RMON pode realizar análises específicas sobre os dados coletados em suas sub-redes.
5. **Múltiplos Gerentes:** oferece maior nível de disponibilidade, pois o diagnóstico poderá ser feito a partir de mais de uma estação gerente. O uso de múltiplos gerentes também permite a execução de diferentes funções ou o gerenciamento de diferentes departamentos em uma empresa.

Dois padrões do protocolo RMON são implementados:

2.4.1 – RMON1

Monitora em nível de camada MAC *(Media Access Control)* o tráfego e coleta informações e estatísticas do segmento de rede local. Faz ainda um diagnóstico remoto de erros e falhas contidas no segmento com a ajuda de um analisador de protocolos.

2.4.2 – RMON2

Com a utilização do padrão RMON original, um monitor RMON pode monitorar o tráfego de rede ao qual está conectado, mas não pode saber de onde está provindo originalmente este tráfego, nem tão pouco o destino final. Para tentar solucionar esta deficiência, foi criado um grupo de trabalho para desenvolver o padrão RMON2,

gerando dois internet drafts: *Remote Network Monitoring MIB Version 2* e *Remote Network Monitoring MIB Protocol Identifiers*.

Um monitor RMON2 não está limitado a monitorar e decodificar o tráfego da camada de rede. Ele também pode ver os protocolos de alto nível rodando acima da camada de rede, determinando, assim, que protocolos da camada de aplicação estão gerando este tráfego.

Um gerente necessita, periodicamente, consultar os monitores para obter informações. Seria interessante, para efeitos de eficiência, que apenas os dados que foram alterados desde a última consulta fossem retornados. Para possibilitar tal facilidade, o RMON2 criou o conceito de filtragem de tempo *(time filtering*), introduzindo um *time stamp* em cada linha, que armazena a última vez em que esta foi alterada.

O RMON2 opera no nível da camada de rede e camadas superiores, complementando o RMON1, possibilitando coletar informações estatísticas e monitorar a comunicação fim-a-fim e o tráfego gerado por diferentes tipos de aplicação.

A configuração do gerenciamento RMON2 é composta por uma probe que gerencia o tráfego da rede incluindo suas sub-redes. Em cada sub-rede existe uma máquina que gerencia localmente o tráfego desta, também funcionando do mesmo modo que a probe e independente de sua arquitetura. A figura seguinte mostra esta configuração.

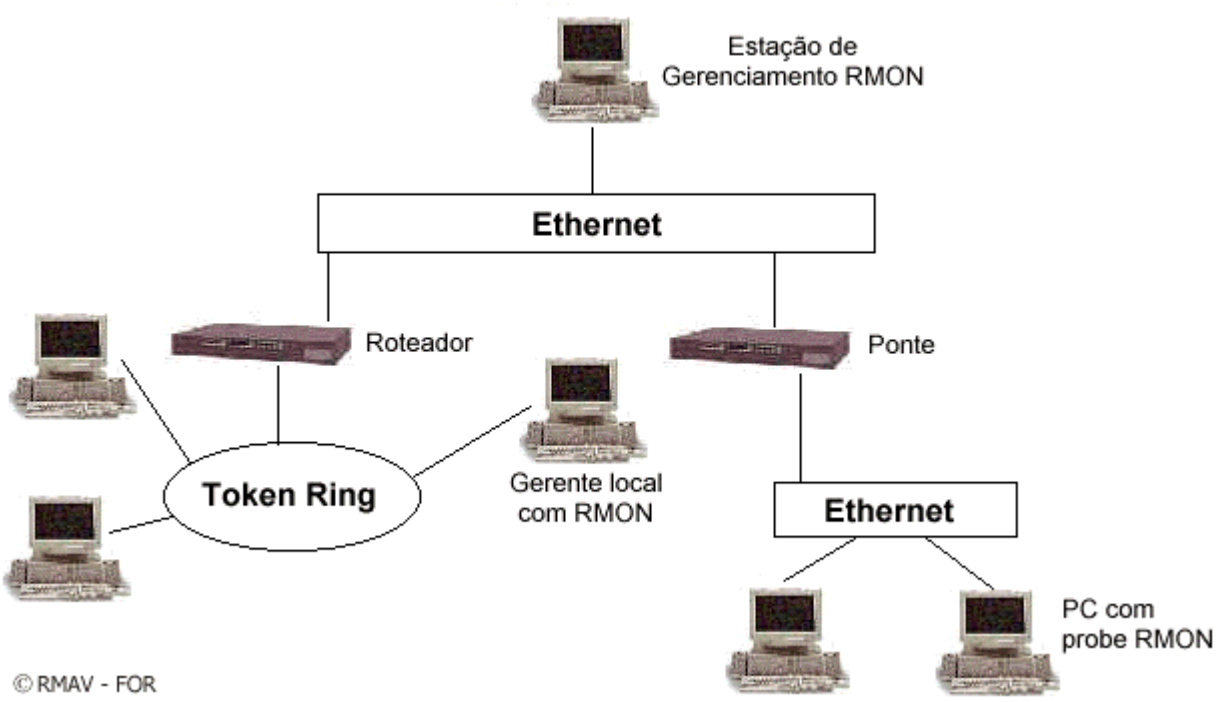


Figura 2 - Exemplo de configuração de uma rede utilizando o RMON

Capítulo 3 – Modelos de Gerenciamento

Os modelos de gerenciamento diferenciam-se nos aspectos organizacionais no que se refere à disposição dos gerentes na rede, bem como no grau da distribuição das funções de gerência. Existem dois modelos adotados para gerência de redes: o Modelo Internet e o Modelo OSI.

3.1 – Modelo Internet

O modelo de gerenciamento Internet adota uma abordagem gerente/agente onde os agentes mantêm informações sobre recursos e os gerentes requisitam essas informações aos agentes. O padrão Internet SMI (*Structure of Management Information*) especifica uma metodologia para definição da informação de gerenciamento contida na MIB. A MIB define os elementos de gerenciamento de informação como variáveis e tabelas de variáveis.

A RFC (*Request for Comments*) 1066 apresentou a primeira versão da MIB para uso com o protocolo TCP/IP, a MIB-I. Este padrão explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas no protocolo TCP/IP. O RFC 1066 foi aceito pela IAB (Internet Activities Board) como padrão no RFC 1156. O RFC 1158 propôs uma segunda MIB, a MIB-II, para uso com o protocolo TCP/IP, sendo aceita e formalizada como padrão no RFC 1213. A MIB-II expandiu a base de informações definidas na MIB-I.

3.1.1 – Estrutura e identificação da informação

Um dos componentes conceituais de importância nos sistemas de gerenciamento é a forma com que as informações sobre os elementos básicos que se quer monitorar/gerenciar/administrar são armazenados. Estas informações precisam estar disponíveis de forma padronizada, de forma que qualquer aplicação de gerenciamento possa resgatá-las e torná-las úteis de alguma forma.

Objetos gerenciados são acessados via uma informação virtual armazenada, denominada Base de Informação Gerencial ou MIB. Objetos de uma MIB são especificados usando a Notação Sintática Abstrata (Abstract Syntax Notation One - ASN.1). Cada tipo de objeto (denominado *Object Type*) tem um nome, uma sintaxe e uma codificação.

O nome é representado unicamente como um IDENTIFICADOR de OBJETO (*Object Identifier*). Um IDENTIFICADOR de OBJETO é um nome administrativo determinado. A sintaxe para um tipo de objeto define uma estrutura abstrata de dados correspondente para este tipo de objeto. Por exemplo, a estrutura de um dado tipo de objeto pode ser um Inteiro (INTEGER) ou uma String de Octetos (OCTET STRING) ou ainda qualquer construção ASN.1 a ser avaliada para uso na definição da sintaxe de um tipo de objeto.

Uma codificação de um tipo de objeto é simplesmente como instâncias daquele tipo de objeto e são representados usando a sintaxe deste tipo de objeto. Implicitamente ligado a notação de uma sintaxe de objeto e codificação é como o objeto está representado quando estamos transmitindo em uma rede. Nomes são usados para identificar objetos gerenciáveis e são especificados na sua hierarquia natural. O conceito de Identificador de Objeto é usado para reproduzir esta noção.

Um Identificador de Objeto pode ser usado com outras intenções além de nomear tipos de objetos gerenciáveis. Por exemplo, cada padrão internacional tem um identificador de objetos designados a eles com a intenção de identificação. Desta forma, os identificadores de objetos representam um significado para identificar algum objeto, sem considerar a semântica associada com este objeto (isto é, um objeto de rede, um documento padrão, etc).

No padrão Internet, os objetos gerenciados são definidos em uma árvore de registro, equivalente a hierarquia de registro do padrão OSI. A MIBII usa o modelo arquitetura de árvore para organizar todas as suas informações. Cada parte da informação da árvore é um nó rotulado que contém:

- Um identificador de objetos (OID): seqüência de números separados por pontos.
- Uma descrição textual: descrição o nó rotulado.

Um Identificador de Objetos é uma seqüência de Inteiros o qual atravessa uma árvore global. Esta árvore consiste de uma raiz conectada a um número de nós rotulados lado a lado. Cada nó pode, deste modo, ter seus próprios filhos os quais são rotulados. Neste caso, nós podemos assumir este nó como uma sub-árvore. Este processo pode continuar de um nível arbitrário ao mais profundo. O Identificador de Objetos é entendido como um controle administrativo de significados designados para os nós que podem ser delegados quando se atravessa pela árvore. Um rótulo é um par de uma breve descrição textual e um inteiro.

O nó raiz não é rotulado, mas tem pelo menos três filhos diretamente abaixo dele: Um deles é administrado pela International Organization for Standardization, cujo label é iso(1); o outro é administrado pela International Telegraph and Telephone Consultative Committee (agora denominado ITU-T), rotulado ccitt(0); e o terceiro é administrado em conjunto pela ISO e CCITT, denominada joint-iso-ccitt(2).

Abaixo do nó iso(1), a ISO designou uma sub-árvore para ser usada por outras organizações, denominado org(3). Destes nós filhos, dois foram designados para o National Institutes of Standards and Technology dos EUA. Uma destas sub-árvores foi transferida pelo NIST para o departamento de defesa dos EUA, denominado dod(6). O DoD não mostrou como ele gerencia sua própria sub-árvore de Identificadores de Objetos. Desta forma, assume-se que o DoD aloca um nó para a comunidade Internet, para ser administrada pela Internet Activities Board (IAB) como se segue:

- **internet OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 } -** Com isso, a sub-árvore da Internet de Identificadores de Objetos começa com o prefixo: **1.3.6.1.**

Agora, vamos especificar a política abaixo o qual esta sub-árvore de Identificadores de Objetos é administrada. Inicialmente, quatro nós são apresentados:

directory OBJECT IDENTIFIER ::= { internet 1 }
mgmt OBJECT IDENTIFIER ::= { internet 2 }
experimental OBJECT IDENTIFIER ::= { internet 3 }
private OBJECT IDENTIFIER ::= { internet 4 }

Directory - A sub-árvore Directory(1) é reservada para o uso do diretório OSI na Internet.

- **Mgmt -** A sub-árvore mgmt(2) é usada para identificar objetos que estão definidos em documentos aprovados pela IAB. A administração da sub-árvore mgmt(2) é delegado pela IAB para a *Internet Assigned Numbers Authority*. As RFCs que definem novas versões de modelos Internet de MIB's aprovadas é determinado um identificador de objetos pela *Internet Assigned Numbers Authority* para identificar os objetos definidos por aquela RFC.

Por exemplo, a RFC que define o modelo Internet inicial de MIB pode ser designado como um documento de gerenciamento de número 1. Esta RFC pode usar o identificador de objetos { mgmt 1 } ou 1.3.6.1.2.1 na definição do modelo Internet da MIB.

A geração de novas versões do modelo de Internet da MIB é um processo rigoroso, com regras que são usadas quando uma nova versão é definida.

- **Experimental -** A sub-árvore experimental(3) é usada para identificar objetos usados por experiências da Internet. A administração desta sub-árvore é delegada pela IAB para a *Internet Assigned Numbers Authority*.

Por exemplo, um experimento pode receber o número 17 e ter disponível o identificador de objetos { experimental 17 } ou 1.3.6.1.3.17 para uso.

- **Private -** A sub-árvore private(4) é usada para identificar objetos definidos unilateralmente. A administração desta sub-árvore é delegada pela IAB para a Internet Assigned Numbers Authority. Inicialmente, esta sub-árvore tem, no mínimo, um filho: **enterprises OBJECT IDENTIFIER ::= { private 1 }**
- A sub-árvore enterprises(1) é usada, entre outras coisas, para permitir que prováveis facções de subsistemas de redes registrem modelos de seus produtos. Recebendo uma sub-árvore, a empresa pode, por exemplo, definir novos objetos MIB na sua sub-árvore. Com isto, é fortemente recomendado que a empresa também registre seus subsistemas de rede abaixo desta sub-árvore, de modo a evitar uma ambigüidade no mecanismo de identificação para serem usados pelos protocolos de gerência.

Por exemplo, se a empresa "Flintstones, Inc." produz subsistemas de rede, então ela pode requisitar um nó abaixo da sub-árvore enterprises para a Internet Assigned Numbers Authority. Com isto, um nó pode ser numerado dessa forma: 1.3.6.1.4.1.42. A empresa "Flintstones, Inc." pode então registrar sua "Rota Fred" com o nome de: 1.3.6.1.4.1.42.1.1.

A figura seguinte mostra como é feita a alocação para redes baseadas nos protocolos TCP/IP, dentro da hierarquia global de árvore.

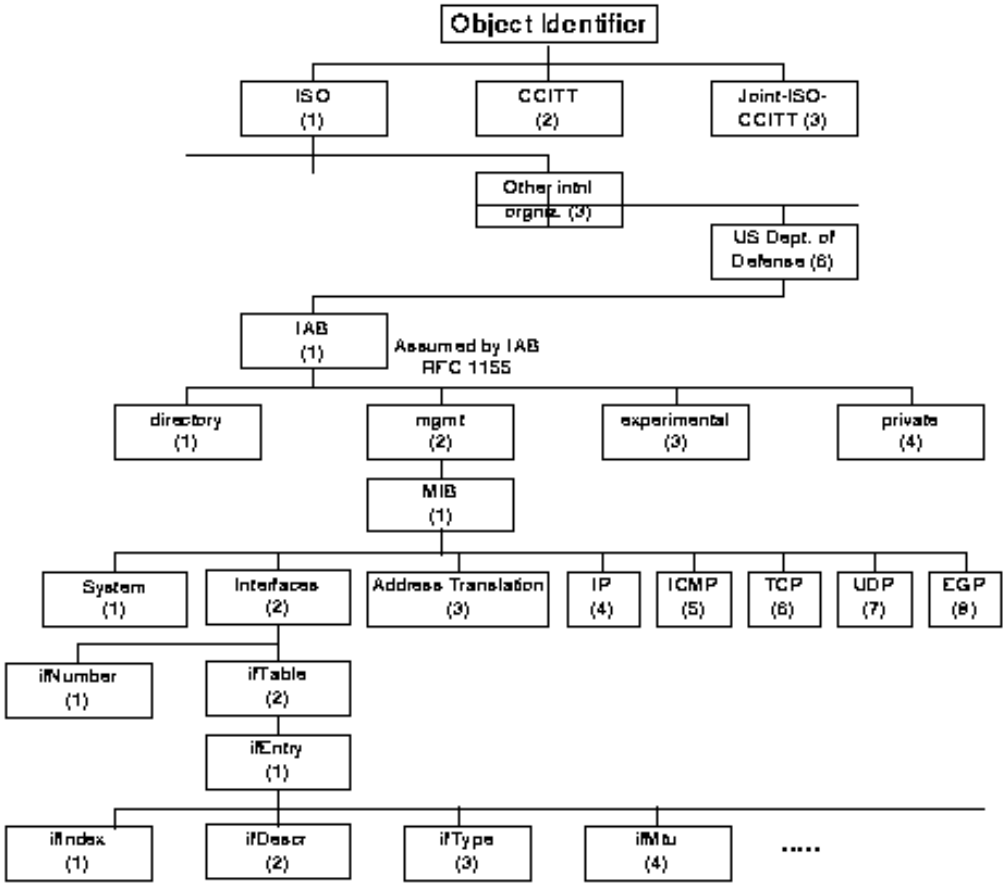


Figura 3 - Árvore de alocação para redes baseadas em TCP-IP

Observar que o nó raiz da árvore MIB na figura seguinte não tem nome ou número (é identificado por um ponto **(.)**), porém tem três sub-árvores:

1. **CCITT(0)**, administrada pelo CCITT;
2. **ISO(1)**, administrada pela ISO;
3. **joint-iso-ccitt(2)**, administrada pela ISO juntamente com o CCITT.

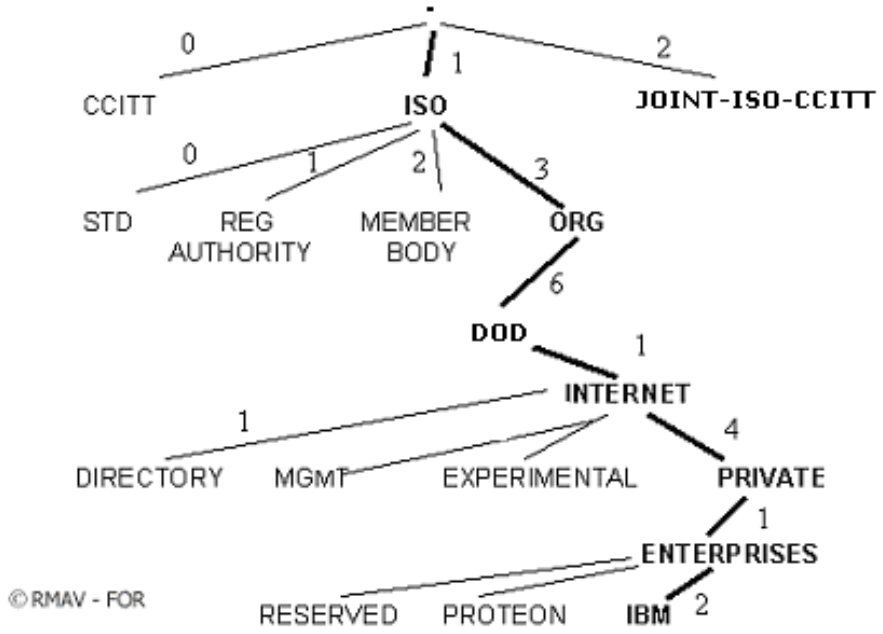


Figura 4 – Árvore MIB no modelo Internet

Abaixo da sub-árvore MIBII estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos são divididos em 11 grupos, que são apresentados na tabela seguinte.

Grupos	Informações
system(1)	**Sistema referente aos dispositivos da rede**
interfaces(2)	**Interface da rede com o meio físico**
address translation(3)	**Mapeamento de endereços IP em endereços físicos**
ip(4)	**Referente ao protocolo IP**
icmp(5)	**Referente ao protocolo ICMP**
tcp(6)	**Referente ao protocolo TCP**
udp(7)	**Referente ao protocolo UDP**
egp(8)	**Referente ao protocolo EGP**
cmot(9)	**Referente ao protocolo CMOT**
transmission(10)	**Trata dos meios de transmissão**
snmp(11)	**Referente ao protocolo SNMP**

Cada objeto contido nos grupos apresentados na tabela anterior é descrito no RFC1213. A descrição dos objetos é dividida em cinco partes: o nome do objeto, a sintaxe abstrata do objeto, a descrição textual do significado do objeto, o tipo de acesso permitido ao objeto (*read-only*, *read-write*, *write-only* ou *not-accessible*), e o estado do objeto (*mandatory* ou *deprecated*).

3.1.2 - Sintaxe

A Sintaxe é usada para definir a estrutura correspondente aos tipos de objetos, usando as construções da linguagem informal ASN.1. O tipo ObjectSyntax define as diferentes sintaxes que podem ser usadas na definição de um tipo de objeto.

Apenas os tipos primitivos da ASN.1 como INTEIRO, STRING de OCTETOS, IDENTIFICADOR de OBJETOS e NULO são permitidos. Estes são algumas vezes referidos como tipos não agregados.

O tipo construído SEQUENCE da ASN.1 é permitido, podendo este ser usado para gerar listas ou tabelas. Para listas, a sintaxe é da seguinte forma: **SEQUENCE { < type1> ,..., < typeN> }**, onde cada < type> está relacionado com algum dos tipos primitivos da linguagem ASN.1 listadas anteriormente. Para tabelas, a sintaxe é da seguinte forma: **SEQUENCE OF < entry>**, onde < entry> pode ser uma lista construída. Listas e tabelas são, algumas vezes, referidas como tipos agregados.

Em geral, novos tipos de aplicação podem ser definidos, sendo assim, podem estar relacionados dentro de um tipo primitivo, lista, tabela, ou alguma outra aplicação implicitamente definida pela ASN.1.

A seguir, alguns tipos de aplicação definidos:

- **NetworkAddress (Endereço de Rede) -** Esta "escolha" representa um endereço entre as várias possibilidades de famílias de protocolos. Até este exato momento, apenas uma família de protocolos, a família Internet, está presente nesta "escolha".
- **IpAddress (Endereço de IP) -** Este tipo de aplicação representa um endereço Internet de 32 bits. Ele é representado como uma STRING de 4 OCTETOS de tamanho, dentro da ordem de bytes da rede.
- **Counter (Contador) -** Este tipo de aplicação representa um inteiro não negativo o qual aumenta até atingir o valor máximo, quando então ele encerra e começa de novo a aumentar a partir do zero. O valor máximo para os contadores é de 2^{32-1} (4294967295 em decimal).
- **Gauge (Medida) -** Este tipo de aplicação representa um inteiro não negativo, que pode aumentar ou decrementar, mas encerra quando atinge o valor máximo. Este valor é de 2^{32-1} (4294967295 em decimal).
- **Time Ticks (Intervalos de Tempo)** - Este tipo de aplicação representa um inteiro não negativo que conta o tempo em centenas de segundos desde alguma época**.** Quando tipos de objetos estão definidos em uma MIB a qual usa este tipo de ASN.1, a descrição deste tipo de objeto identifica a época correspondente.

Opaque (Opaco) - Este tipo de aplicação sustenta a capacidade de passar arbitrariamente a sintaxe ASN.1. Um valor é codificado usando as regras básicas da ASN.1 dentro de uma string de octetos. Deste modo, é codificada como uma string de octetos, tendo o efeito de "ocultar duplamente" o valor ASN.1 original. Notar que esta implementação necessita apenas de ser capaz de acessar e reconhecer dados obscuramente codificados. Não é necessário ser capaz de desvendar o dado e então interpretar o seu conteúdo.

3.1.3 – Codificações

Uma vez que uma instância de um tipo de objeto tenha sido identificada, seu valor deve ser transmitido aplicando-se as regras básicas de codificação da linguagem ASN.1 na sintaxe deste tipo de objeto.

3.2 – Modelo OSI

O padrão OSI conforme mencionado anteriormente define três modelos para gerência de redes:

- **Modelo organizacional** - descreve a forma pela qual a gerência pode ser distribuída entre domínios e sistemas dentro de um domínio.
- **Modelo informacional** - apresenta as áreas funcionais e seus relacionamentos.
- **Modelo funcional** - provê a base para a definição de objetos gerenciados e suas relações, classes atributos, ações e nomes.

Para a definição dos objetos gerenciados deve-se considerar três hierarquias:

1. **Hierarquia de Herança** - também denominada hierarquia de classe - tem como objetivo facilitar a modelagem dos objetos, através da utilização do paradigma da orientação a objetos. Assim podem ser definidas classes, superclasses, subclasses. Trata-se de uma ferramenta para uma melhor definição de classes.
2. **Hierarquia de Nomeação** - identifica quando um objeto gerenciado faz parte de um e somente um objeto gerenciado. Um objeto gerenciado existe somente se o objeto que o contém existir, e dependendo da definição, um objeto só pode ser removido se aqueles que lhe pertencerem forem removidos primeiro.
3. **Hierarquia de Registro** - A hierarquia de registro é usada para identificar de maneira universal os objetos, independentemente das hierarquias de heranças e nomeação. Esta hierarquia é especificada segundo regras estabelecidas pela notação ASN.1 (Abstract Syntax Notation. One).

3.2.1 – Requisitos de gerenciamento

No modelo OSI os requisitos de gerenciamento de rede em geral se dividem em cinco áreas funcionais:

- **Gerenciamento de configuração**

As aplicações de gerenciamento de configuração lidam com a instalação, inicialização, partida, modificação e registro de parâmetros de configuração ou opções de hardware e software de rede. Além disso, a gerência de configuração é responsável por manter um inventário atualizado e produzir relatórios baseados nesse inventário.

- **Gerenciamento de falhas**

Os recursos do gerenciamento de falhas fazem rastreamento para auditoria, ou seja, mostram características de erros da rede. Sua responsabilidade é detectar, isolar e corrigir operações anormais na rede. Requer constante observação do funcionamento dos dispositivos que a compõem de forma que se possa identificar rapidamente o problema e resolvê-lo sem grandes prejuízos.

- **Gerenciamento de segurança**

A gerência de segurança controla o acesso aos recursos da rede através do uso de técnicas de autenticação e políticas de autorização. Necessita do registro dos atos dos usuários que venham a usufruir os recursos da rede. Identifica pontos críticos e pontos de acesso para tentar mantê-los seguros. Para isso usa-se autenticação, criptografia e outros recursos.

- **Gerenciamento de desempenho**

Os recursos de gerenciamento de desempenho produzem informações estatísticas em tempo real sobre a taxa de utilização da rede, bem como da taxa de erros. Envolve a certificação de que a rede permaneça descongestionada e acessível para que os usuários possam utilizá-la eficientemente. Para isso, é feito um monitoramento dos equipamentos da rede e seus enlaces associados para determinar sua utilização, taxas de erros e outros parâmetros.

- **Gerenciamento de contabilização**

A gerência de contabilização é responsável pela coleta e processamento dos dados, implementando mecanismos para que sejam registradas todas as ações de usuários que resultem em consumo de recursos, envolvendo a medição do uso dos recursos da rede de maneira a estabelecer métricas, verificar quotas, determinar custos e taxar usuários.

No modelo tradicional, as redes são compostas por múltiplos componentes. Além das máquinas em que as aplicações estão efetivamente rodando, roteadores, bridges, gateways e modems são componentes importantes. No que envolve os softwares, outros componentes estão envolvidos, especialmente em ambientes multifornecedores. A tarefa de gerenciamento deve, então, ser resolvida por uma combinação entre entidades chamados de gerentes e agentes.

Capítulo 4 - Objetos Gerenciáveis

4.1 – Definição de tipo de objeto

Uma definição de tipo de objeto usando TCP/IP possui cinco campos:

1. **Objeto -** É um nome textual para o tipo de objeto denominado DESCRITOR de OBJETO (Object Descriptor) o qual acompanha o seu correspondente IDENTIFICADOR de OBJETO.
2. **Sintaxe -** É uma sintaxe abstrata para um tipo de objeto. Ela pode ser uma escolha entre: uma Sintaxe Simples (SimpleSintax) que pode ser um tipo Inteiro (Integer), uma String de Octetos (Octet String), um Identificador de Objeto (Object Identifier) ou Nulo (Null). Pode ser também uma Sintaxe de Aplicação (ApplicationSintax) podendo esta ser um Endereço de Rede (NetworkAdddress), um Contador (Counter), uma Medida (Gauge), um Intervalo de Tempo (TimeTicks) ou Incompreensível (Opaque); e, além destes também pode ser um outro tipo de aplicação.
3. **Definição -** É uma descrição textual da semântica de um tipo de objeto. Implementações devem assegurar que as instâncias do objeto cumpram esta definição desde que esta MIB seja pretendida por uso em ambiente multi-vendedor. A definição é vital para que os objetos tenham significados consistentes através de todas as máquinas.
4. **Acesso -** Para leitura, leitura e escrita, escrita ou sem acesso.
5. **Status -** Obrigatório, opcional ou obsoleto.

O seguinte exemplo mostra a definição de um objeto contido em uma MIB. Seu nome é **sysDescr** e faz parte do grupo do System:

OBJETO

sysDescr { system 1 }

Sintaxe STRING de OCTETOS

Definição Este valor deve incluir todo o nome e identificação da
versão do tipo de hardware do sistema, software de
sistema operacional e software de rede. É obrigatório
que contenha apenas caracteres ASCII imprimíveis.

Acesso leitura

Status obrigatório

Um objeto gerenciador não tem apenas que estar definido, mas identificado também. Isto é feito usando o Identificador de Objetos como um número de telefone,

reservando um grupo de números para diferentes localizações. No caso do TCP/IP - baseado em gerenciamento de rede, o número alocado é 1.3.6.1.2 e a SMI usa isto como uma base para definir novos objetos.

Deste modo, é definido uma Estrutura de Informação de Gerenciamento *(SMI - Structure Management Information*) que especifica o modelo de informação a ser adotado. Este modelo deve incluir a definição da estrutura da informação de gerenciamento armazenada em bases de dados destinadas a esse fim, as operações que podem ser realizadas sobre a mesma e as notificações que podem ser emitidas em decorrência de alguma operação ou alteração destas informações. Assim sendo, pode-se garantir a interoperabilidade entre diferentes sistemas de gerenciamento de rede onde tais sistemas conseguem ter uma visão comum da informação de gerenciamento.

4.2 - Base de Informação Gerencial (MIB)

Todo sistema complexo necessita armazenar as informações manipuladas em algum tipo de base de dados. A Base de Informação é o nome conceitual para a informação de gerenciamento, incluindo os objetos gerenciados e seus atributos. Pode-se considerar as informações para a configuração do sistema como também pertencentes a MIB.

A SMI descreve o cenário no qual a Base de Informação Gerencial pode ser definida. A SMI, baseada na abordagem orientada a objetos, introduz os conceitos de hierarquia, herança, nomeação e registros usados na caracterização e identificação de objetos gerenciados. Além disso, ela define o conjunto de operações que pode ser realizado sobre os objetos gerenciados da MIB e o comportamento desses objetos mediante a execução destas operações.

Dentro deste contexto, a MIB é definida como um conjunto de objetos gerenciados dentro de um Sistema Aberto, na qual um objeto gerenciado é a visão abstrata de um recurso real dentro deste sistema.

4.2.1 - A MIB da Internet (TCP/IP)

A MIB da Internet define os objetos que podem ser gerenciados por cada camada do protocolo TCP/IP. Estes objetos estão sob a guarda de um agente de gerenciamento e a comunicação entre este agente e um gerente, localizado na estação de gerenciamento é feita utilizando o protocolo SNMP.

A MIB e o protocolo SNMP utilizam uma restrição do padrão ASN.1 do OSI para a definição dos objetos e dos Protocol Data Units (PDU's). Inicialmente, esta escolha foi feita para permitir uma compatibilidade com o protocolo CMIP do modelo OSI, mas este objetivo não existe mais.

Como todos os padrões da tecnologia TCP/IP, as definições usadas no gerenciamento SNMP foram publicadas na série RFC (Requests For Comments). As definições originais do protocolo SNMP, bem como dos objetos gerenciados foram publicados em 1989. Em 1990, foi feita uma revisão da MIB, que passou a se chamar

de MIB-II. Em 1993, foi publicado um conjunto de padrões novos, chamado SNMPv2, com alterações ao protocolo e extensões às definições dos objetos.

A MIB divide os objetos em vários grupos. A tabela a seguir mostra a MIB-I e os grupos nela definidos.

Grupo	Objetos para:	Número de objetos
System	Informações básicas do sistema	3
Interfaces	Interfaces de rede	22
At	Tradução de endereço	3
Ip	Software de protocolo IP	33
Icmp	Protocolo de estatística para controle interno de mensagens	26
Tcp	Software do Protocolo TCP	17
Udp	Software do Protocolo UDP	4
Egp	Software do Protocolo EGP	6

A tabela a seguir mostra a MIB-II e os grupos nela definidos.

Grupo	Objetos para:	Número de objetos
System	Informações básicas do sistema	7
Interfaces	Interfaces de rede	23
At	Tradução de endereço	3
Ip	Software de protocolo IP	38
Icmp	Protocolo de estatística para controle interno de mensagens	26
Tcp	Software do Protocolo TCP	19
Udp	Software do Protocolo UDP	7
Egp	Software do Protocolo EGP	18
Transmiss	Transmissão – média específica	0
SNMP	Aplicações SNMP	30

A lista definida de objetos gerenciáveis foi derivada daqueles elementos considerados essenciais. Esta implementação de se pegar apenas objetos essenciais não é restrita, uma vez que a SMI proporciona mecanismos de extensão como uma nova versão de uma MIB e uma definição de um objeto privado ou que não seja padrão.

4.2.2 - A MIB no modelo OSI

Existem três tipos de hierarquias de gerenciamento usadas pelos Sistemas de Gerenciamento OSI: Herança, Nomeação e Registro.

- **Hierarquia de Herança -** A hierarquia de herança, também denominada de hierarquia de classe, está relacionada às propriedades associadas aos objetos descritas através de seus atributos, comportamento, pacotes condicionais, operações e notificações. Dentro desta hierarquia, define-se, então, o conceito de classes de objeto hierarquizadas às quais pertencem objetos com propriedades similares. Existem, então, superclasses às quais estão subordinadas subclasses. Uma subclasse herda todas propriedades de sua superclasse, de maneira irrestrita, independentemente da necessidade ou não destas propriedades. A estas subclasses podem ser aglutinadas propriedades adicionais. A superclasse do topo desta hierarquia é chamada de TOPO *(Top)*, da qual todas as outras classes são derivadas. Dentro desta organização, as classes mais gerais são definidas próximas ao TOPO.
A figura abaixo apresenta um exemplo de árvore de Classes de Objetos Gerenciados.

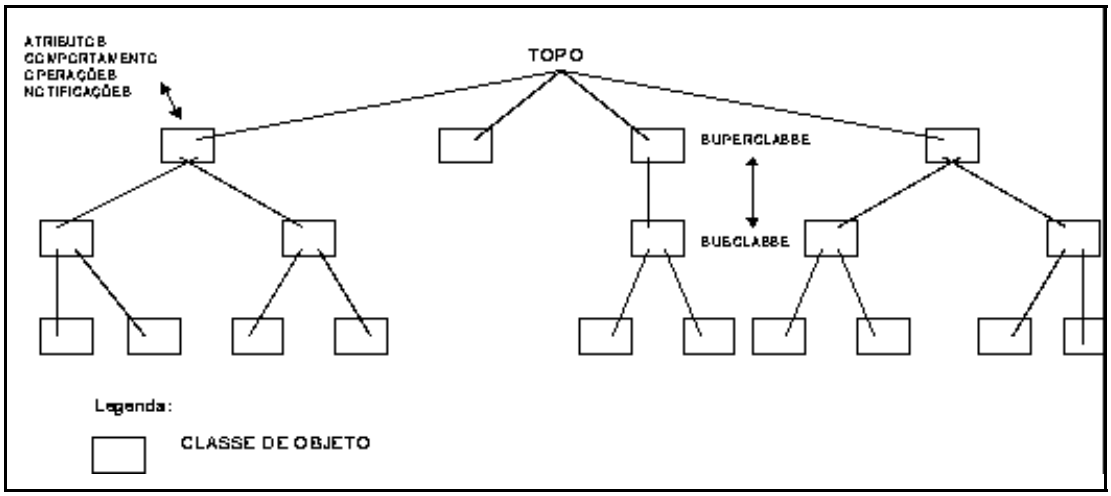


Figura 5 - Árvore de classes de objetos

Opcionalmente, utiliza-se o conceito de herança múltipla, ou seja, a habilidade de uma subclasse ser derivada de mais de uma superclasse, permitindo a maior reutilização possível de definições de classes. Isto também permite melhorar a capacidade de um sistema de gerenciamento reconhecer características familiares entre classes de objeto. Este conceito de herança múltipla assegura ainda que, quando uma classe herda a mesma característica de múltiplas superclasses, então, aquela classe é definida como se aquela característica fosse herdada de uma única superclasse.

Dentro desta hierarquia, conforme mencionado anteriormente, as propriedades dos objetos de uma classe são descritas através dos seus atributos, comportamento, pacotes condicionais, operações e notificações. Um atributo pode determinar ou refletir o comportamento de um objeto gerenciado. Os atributos de um objeto podem ser obrigatórios ou contidos em pacotes condicionais. Se um atributo é obrigatório, ele deve estar presente em todos as instâncias dos objetos gerenciados de uma dada classe. Todo atributo possui um valor ou conjunto de valores (set-valued) do mesmo tipo. A Asserção de Valor de Atributo (AVA - Atribute Value Assertion) é uma declaração de que um atributo particular possui um valor. O valor de um atributo pode ser lido e/ou modificado através de operações sobre objetos gerenciados.

Todos os objetos gerenciados de uma classe devem possuir o mesmo comportamento, que define: a semântica dos atributos, operações e notificações; a resposta às operações de gerenciamento; as circunstâncias em que as notificações devem ser emitidas; as dependências entre valores de atributos particulares e os efeitos dos relacionamentos entre objetos gerenciados. Um pacote condicional é uma coleção de atributos, notificações, operações e comportamentos opcionais, que está totalmente presente ou ausente num objeto gerenciado. Apenas uma instância de um pacote condicional pode existir em um objeto gerenciado e a mesma somente pode ser acessada como parte deste objeto. Deve-se ainda ressalvar o conceito de classes alomórficas. Uma subclasse é dita alomórfica de sua superclasse quando apresenta comportamento semelhante à sua superclasse. Para uma subclasse alomórfica, a faixa de valores de um atributo herdado deve ser a mesma ou um subconjunto da faixa de valores definida para o mesmo atributo da sua superclasse alomórfica.

- **Hierarquia de Nomeação -** A hierarquia de nomeação, também chamada de hierarquia de *containment*, descreve as relações entre instâncias de objetos com seus respectivos nomes. Dentro desta hierarquia, define-se um relacionamento "estar contido em" aplicado aos objetos. Objetos de uma classe podem conter objetos da mesma classe e de classes diferentes. Um objeto gerenciado que contém outro objeto é dito superior; o objeto contido é dito subordinado. Um objeto gerenciado está contido dentro de um e somente um objeto gerenciado superior.

Este relacionamento de *containment* pode ser usado para modelar hierarquias de partes do mundo real (por exemplo, módulos, sub-módulos e componentes eletrônicos) ou hierarquias organizacionais (por exemplo, diretório, arquivos, registros e campos). Isto implica que o objeto gerenciado existe somente se o seu objeto superior existir e que todo objeto gerenciado tem um nome que é derivado de um relacionamento de *containment.*

O nível mais alto desta hierarquia é chamado de RAIZ, que é um objeto nulo e sempre existe. Dentro de uma instância superior, todos os subordinados são unicamente identificados por um nome característico relativo (RDN - *Relative Distinguished Name*). Um RDN é formado por um atributo, chamado de atributo característico (*distinguished attribute*) e mais algum valor. A combinação do atributo e do valor deve ser única para cada instância do objeto tendo o mesmo superior. Um nome completo de uma instância, chamado de "nome característico" (DN - *Distinguished Name*), consiste em uma seqüência de RDNs começando pela RAIZ e inclui o RDN da própria instância. Assim, todos os DNs são únicos e cada instância de objeto tem um único nome.

Para cada classe de objeto, uma ou mais regras devem ser definidas para identificar a classe superior e o atributo característico. Estas regras são chamadas de *name bindings*. Uma vez que um *name bindings* foi definido para uma classe de objeto, este *name bindings* está disponível para uso em todas as classes derivadas daquela classe. Novos *name bindings* podem ser criados como resultado de especialização, entretanto, para todas as classes de objetos alomórficas, novos *name bindings* somente podem ser criados se eles forem também definidos para todas suas superclasses alomórficas.

- **Hierarquia de Registro -** A hierarquia de registro, por sua vez, é usada para identificar de maneira universal os objetos, independentemente das hierarquias de heranças e nomeação. Esta hierarquia é especificada segundo as regras estabelecidas pela notação ASN.1 para árvore de registros usada na atribuição de identificadores a objetos. Cada nó desta árvore está associado a uma autoridade de registro (por exemplo, ISO - *International Organization for Standardization* e CCITT - *Consultative Commitee for International Telegraph and Telephone*) que determina como são atribuídos os seus números. Desta maneira, cada objeto é identificado por uma seqüência de números, cada um correspondente a um nó.

4.3 - Operações de Gerenciamento

As operações de gerenciamento executadas na fronteira do objeto gerenciado (fronteira entre um recurso e o objeto gerenciado que o representa), são primitivas. Para que se obtenha sucesso na realização de uma operação, o sistema de gerenciamento invocador deve ter os direitos de acesso necessários e as restrições de consistência, associadas à classe do objeto gerenciado e não devem ser violadas. O sistema de gerenciamento pode ser requisitado para executar uma operação em vários objetos gerenciados com sincronização atômica, isto é, ou esta operação é efetivamente realizada sobre todos os objetos, ou não é realizada.

A definição da classe de objetos deve especificar, para cada operação sobre o objeto gerenciado, o critério para suportar pedidos de operações de gerenciamento com sincronização atômica com outros objetos gerenciados. A execução só está sujeita a restrições existentes na definição de classes relevantes.

Existem dois tipos básicos de operações de gerenciamento que podem ser realizados sobre os objetos gerenciados: Operações orientadas a atributos e operações sobre objetos gerenciados como um todo.

4.3.1 - Operações Orientadas a Atributos

O comportamento descrito a seguir é comum a todas as operações orientadas a atributos:

- Todos os atributos envolvidos como parte de uma única operação devem estar disponíveis para o objeto gerenciado;
- Todas as operações falham se e somente se o comportamento do objeto gerenciado é tal que a operação não é realizada em alguns dos atributos deste objeto;
- Quando uma operação de leitura ou modificação sobre uma lista de valores de atributos é solicitada através de um único pedido, a forma em que estas leituras ou modificações são sincronizadas entre os atributos depende da definição do comportamento da classe do objeto gerenciado e da lista de atributos especificados na operação;
- Quando uma sincronização atômica está em efeito, os estados intermediários resultantes da operação não são visíveis por outras operações de gerenciamento. A

utilização de sincronização atômica pode levar a resultados inesperados, se os atributos da lista não estiverem sincronizados entre si no objeto.

As seguintes informações devem estar disponíveis para execução de operações orientadas a atributos:

- Identificador de atributo;
- Filtros;
- Listas ordenadas das classes de objetos alomórficas;

Após a execução da operação, os seguintes resultados estão disponíveis na fronteira do objeto gerenciado:

- Identificador de atributo e valores dos atributos que sofreram operações;
- Indicação de erro para os atributos que não puderam ser submetidos à operação.

Os seguintes tipos de erros devem ser identificados:

- Identificadores de atributos desconhecidos, isto é, não encapsulado dentro do objeto gerenciado;
- Classe de objeto especificada que não é parte do conjunto alomórfico do objeto gerenciado;
- Falha geral no processamento da operação.

A operação de gerenciamento sobre um atributo de objeto gerenciado pode provocar efeitos diretos e/ou indiretos. Os efeitos diretos são definidos pela operação de gerenciamento Substituição do Valor do Atributo (*Replace Attribute Value*). Os efeitos indiretos são resultados de relações do objeto gerenciado em questão. Como exemplos de efeitos indiretos pode-se citar:

- Modificação de um atributo dentro do mesmo objeto;
- Mudança de comportamento do objeto gerenciado;
- Alteração de um atributo de um objeto gerenciado relacionado;
- Mudança no comportamento de um objeto gerenciado relacionado causado pela mudança de um ou mais atributos naquele objeto gerenciado.

As operações orientadas a atributos especificadas nas normas ISO/IEC 10165-1 são as seguintes:

a) ***GET ATTRIBUTE VALUE (Obtenção de Valor do Atributo)*** - Esta operação aplica-se a todos os tipos de atributos, exceto aqueles definidos como não acessíveis para leitura. Sua função é ler a lista de valores de atributos especificada, ou, se nenhuma lista é fornecida, ler todos os valores de atributos a retornar àqueles que puderem ser lidos. Para que uma operação de GET ATTRIBUTE VALUE seja realizada, devem estar disponíveis informações relativas aos identificadores de atributos ou de grupos de atributos usadas para determinar como ou se a operação em questão deve ser executada. Se os valores de tais atributos não puderem ser lidos, há indicação de erro, identificando-se os casos de erro devido à restrição de acesso para leitura.

b) ***REPLACE ATTRIBUTE VALUE (Substituição do Valor do Atributo)*** - Esta operação aplica-se somente a grupos de atributos ou a atributos que são acessíveis para escrita. Sua função é alterar os valores dos atributos especificados com os novos valores conhecidos. Para que uma operação de REPLACE ATTRIBUTE VALUE seja efetuada, é necessário que sejam fornecidas informações referentes aos

identificadores dos atributos a serem alterados e seus novos valores. Tais informações são usadas para determinar como e se tal operação deve ser executada. Há indicação de erro para os atributos cujos valores não puderem ser substituídos, identificando-se aqueles não substituídos por não serem acessíveis para escrita.

c) ***SET WITH DEFAULT VALUE (Substituição do Valor do Atributo pelo Valor Default)*** - Esta operação aplica-se a todo tipo de atributo, exceto àqueles definidos como não acessíveis para escrita. Sua função e fazer com que o objeto gerenciado substitua o valor de alguns de seus atributos pelo seu valor default, definido como parte da especificação da classe de objeto em questão. Esta operação não restaura as condições iniciais do objeto quando de sua criação. Para a realização de uma operação de SET WITH DEFAULT VALUE devem ser fornecidas informações referentes aos atributos e aos grupos de atributos usados para determinar como e se os seus valores devem ser substituídos por seus valores default. Há indicação de erro se esta operação não puder ser efetuada, identificando-se as situações em que os valores de atributos não são acessíveis para escrita em que não existem valores default definidos.

d) ***ADD MEMBER (Inclusão de Valores)*** - Esta operação aplica-se a atributos cujos valores são conjuntos (sets) acessíveis para escrita. Para cada conjunto especificado de valores de atributo, esta operação substitui os valores de atributos existentes pelo conjunto união do conjunto existente com o conjunto especificado nesta operação. Para que a operação ADD MEMBER seja realizada, devem estar disponíveis informações relativas aos identificadores dos atributos e aos seus valores a serem adicionados. Estas informações são utilizadas para determinar como e se esta operação deve ser executada. Há indicação de erro para aqueles atributos cujos novos valores não puderem ser adicionados, identificando-se os valores não adicionados por não serem acessíveis para escrita.

e) ***REMOVE MEMBER (Remoção de Valores)*** - Esta operação aplica-se a atributos cujos valores são conjuntos (sets) acessíveis para escrita. Para cada conjunto especificado de valores de atributo, esta operação substitui o conjunto existente de valores de atributo pelo conjunto diferença entre o conjunto já existente e o conjunto especificado nesta operação. Para determinar se e como esta operação deve ser executada, devem ser fornecidos informações referentes aos identificadores de atributos e seus valores a serem excluídos. Há indicação de erros para aqueles atributos dos quais não puderam ser excluídos valores, identificando-se aqueles valores não excluídos por não serem acessíveis para escrita.

4.3.2 - Operações sobre Objetos Gerenciados

Estas operações aplicam-se a objetos gerenciados como um todo e seus efeitos geralmente não se limitam a modificar os valores dos seus atributos. São definidas as seguintes operações: CREATE, DELETE e ACTION. Operações adicionais podem ser definidas por meio da operação ACTION. A semântica destas operações faz parte da

definição da classe de objeto gerenciado. Os objetos gerenciados são criados e removidos por meio de operações de gerenciamento ou como efeito colateral de uma outra operação.

a) *CREATE (Criação de Objeto)* - Esta operação aplica-se a todos os objetos especificados como passíveis de criação pela definição de sua respectiva classe de objeto. Sua função é requisitar a criação e iniciação de um objeto gerenciado. É uma operação única, desde que aplicada a um objeto gerenciado que ainda não exista. A operação CREATE cria um objeto gerenciado de uma classe específica ou pertencente a uma subclasse alomórfica, dentro da hierarquia de nomeação. Quando um objeto gerenciado é criado, são designados valores a todos seus atributos, encapsulados no objeto ou em algum de seus pacotes específicos. Estes valores são obtidos a partir de informações fornecidas na própria operação CREATE e da definição de sua classe de objeto.

Na operação CREATE podem ser especificados explícita ou implicitamente um ou mais pacotes condicionais por meio da especificação de um objeto gerenciado ou por default, como parte da especificação da classe de objeto. Esta operação falha se o sistema não puder fornecer um objeto gerenciado com pelo menos um dos pacotes condicionais requeridos. Uma definição de objeto gerenciado deve permitir a um objeto ser criado sem a especificação do nome de suas instâncias e sem a especificação de sua localização na hierarquia de nomeação.

A localização de um objeto gerenciado na hierarquia de nomeação pode ser especificada explicitamente, através da especificação do nome do objeto gerenciado que vai conter a instância que está sendo criada, ou implicitamente, através do nome da própria instância sendo criada. Quando é especificado somente o nome do objeto gerenciado, que vai conter a instância criada, o RDN do novo objeto gerenciado é atribuído pelo sistema gerenciado.

Para determinar como e se a operação de criação pode ser executada, devem ser fornecidas as seguintes informações:

- Identificador da classe de objeto;
- Atributo de pacotes;
- Identificadores dos atributos para os quais devem ser designados valores específicos como parte da iniciação da instância de objeto;
- Identificador da referência do objeto gerenciado, a partir do qual a informação de iniciação deste objeto está sendo obtida.

Como resultado da operação de criação, devem ser retornadas as informações referentes aos identificadores dos atributos para os quais tiverem sido atribuídos valores como parte da iniciação da instância do objeto. Além disso, no caso de o objeto gerenciado não poder ser criado, há indicação de erro, identificando-se as situações específicas, tais como: identificadores de atributos desconhecidos, identificador inválido da referência do objeto gerenciado e especificação do *name binding* inválido.

b) *DELETE (Remoção de Objeto)* - Esta operação aplica-se a todos os objetos gerenciados que podem ser removidos remotamente. Ela pode ser efetuada mesmo sobre objetos gerenciados que tiverem sido criados através de uma operação local. A

operação DELETE requisita que o objeto gerenciado remova a si mesmo. Esta operação remove o objeto gerenciado que representa um recurso e implica um efeito análogo sobre o próprio recurso.

Quando um objeto gerenciado recebe um pedido de remoção, ele verifica se outros objetos gerenciados estão contidos nesse objeto. Caso afirmativo, o comportamento do objeto gerenciado depende da especificação da classe do objeto gerenciado. O objeto gerenciado pode remover todos os objetos gerenciados nele contidos para assegurar a integridade do nome, ou pode recusar-se a executar esta operação de remoção até que todos os objetos gerenciados nele contidos tenham sido removidos.

Similarmente, quando um objeto gerenciado a ser removido tem relacionamento com outros objetos gerenciados, as remoções destes objetos podem comprometer a integridade dos relacionamentos e/ou dos objetos gerenciados relacionados. Geralmente, objetos gerenciados e seus relacionamentos devem ser removidos de maneira a assegurar a integridade do sistema gerenciado a cada remoção efetuada. Se a remoção de um objeto gerenciado resultar na perda da integridade do relacionamento, então, o objeto gerenciado pode rejeitar o pedido de remoção ou iniciar operações que assegurem que esta integridade seja mantida. A emissão ou não de uma notificação, como resultado da remoção de um objeto gerenciado, depende da definição do objeto gerenciado.

Para que seja possível determinar como e se a operação de DELETE deve ser executada, devem ser fornecidas informações referentes à lista ordenada das classes alomórficas e aos filtros associados. No caso de os objetos gerenciados não poderem ser removidos, é retornada uma indicação de erro identificando-se aqueles erros decorrentes de identificadores de atributos desconhecidos. Como resultado da operação de remoção de objetos gerenciados, pode ou não ser emitida uma notificação. Isto depende da definição do objeto gerenciado.

c) *ACTION* - Essa operação pode ser executada para todas as classes de objetos gerenciados. A operação ACTION requer que o objeto gerenciado execute a ação especificada e indique o seu resultado. A ação e a informação opcional associada são parte da definição de classe do objeto gerenciado.

As seguintes informações devem estar disponíveis para ser possível determinar como e se a operação ACTION deve ser executada sobre uma instância de classe de objetos gerenciados:

- Lista ordenada das classes alomórficas;
- Especificação da ação a ser executada;
- Identificador da classe de objeto para suportar comportamento alomórfico.

Após a execução da ação especificada, são obtidas informações sobre o seu resultado e eventuais erros. Neste caso, devem ser identificados erros relativos à ação desconhecida e à classe de objeto desconhecida.

4.4 - Compiladores de MIB's

Além da descrição dos objetos gerenciados e suas relações, uma MIB contém informações detalhadas sobre cada objeto, como por exemplo, o tipo de acesso a um objeto, um valor *default* razoável para um objeto e um conjunto de valores que um objeto pode assumir. Estas informações possuem um valor inestimável para os fornecedores de softwares para agentes e gerentes, pois elas permitem que vários fornecedores utilizem um mesmo conjunto de informações de gerenciamento, obedecendo a um conjunto de características padrão. Além disso, uma MIB pode ser compilada por um compilador de MIB's, de forma que as informações presentes na MIB estejam disponíveis para aplicações como MIB *browsers* e *graphers*. Estas aplicações são consideradas aplicações genéricas. São aplicações simples que obtém toda a sua capacidade de gerenciamento através da análise de uma MIB, sem qualquer intervenção humana.

Além de checar a sintaxe de uma MIB, um compilador de MIB's pode gerar automaticamente as estruturas de dados e o código necessário para que um agente implemente uma determinada MIB. Um compilador de MIB's também pode fazer com que as informações sobre os objetos gerenciados de MIB's proprietárias ou de novas MIB's que sejam padronizadas estejam disponíveis para uma aplicação de gerenciamento existente.

A entrada para um compilador de MIB's é uma coleção de módulos de MIB's escritos em um subconjunto de linguagem ASN.1. Estes módulos contêm definições de objetos gerenciados que correspondem às informações sobre os dispositivos da rede que podem ser manipulados através do protocolo SNMP. Os compiladores de MIB's podem gerar várias representações das definições dos objetos gerenciados contidos nas MIB's usadas como entrada. Estas representações podem ser processadas mais facilmente pelos agentes e aplicações de gerenciamento do que a representação ASN.1. Algumas destas representações são declarações de estruturas de dados em linguagens de programação de alto nível, como C, que podem ser compiladas e ligadas em uma aplicação de gerenciamento ou agente. Outras são arquivos de dados contendo representações das definições dos objetos gerenciados que podem ser lidas para a memória por uma aplicação de gerenciamento ou agente em tempo de execução. Em alguns casos, o compilador de MIB's gera um código de saída que auxilia na implementação das MIB's de entrada. Por exemplo, um compilador de MIB's pode gerar esqueletos de rotinas para a recuperação ou alteração do valor de um objeto gerenciado, ou rotinas para a geração de Trap-PDU's específicas.

A habilidade de reconhecer as descrições presentes em uma MIB mecanicamente é muito atraente, principalmente para os fabricantes de aplicações genéricas, pois estas podem cobrir uma grande variedade de agentes de MIB's. Com o grande número de MIB's padronizadas e MIB's proprietárias disponíveis atualmente, os compiladores de MIB's reduzem o esforço dos fornecedores para manterem suas aplicações atualizadas.

Assim, muitos esforços estão concentrados em facilitar a forma pela qual diversas MIB's possam ser compiladas em cada produto de gerenciamento. Tentativas

estão sendo feitas para que mais informações possam ser reconhecidas dinamicamente possibilitando que uma aplicação gerencie eficientemente um dispositivo completamente desconhecido para o fornecedor do produto de gerenciamento e para o usuário.

Embora os compiladores de MIB já tenham provado sua utilidade, o gerenciamento de redes inteligente não poderá ser alcançado pela simples utilização desta tecnologia. Infelizmente, a informação mais importante da MIB, ou seja, o texto que descreve detalhadamente um objeto, não pode ser compreendido por um compilador de MIB (com a tecnologia disponível atualmente). Por exemplo, um compilador pode ler a descrição de um objeto da MIB-II e aprender que este objeto é um inteiro que pode assumir os valores um e dois, o valor deste objeto pode ser lido e alterado e a implementação deste objeto é obrigatória. Mas somente um ser humano pode compreender a partir da descrição em linguagem natural do objeto *ipForwarding*, que se o valor deste objeto for igual a um então o sistema descrito por este objeto está atuando como um gateway, senão o sistema é apenas um nó da rede. Além disso, existem informações conhecidas por um administrador de rede experiente que não são descritas em nenhuma MIB, como por exemplo, o fato de que em algumas circunstâncias, pode ser perigoso para um sistema atuar como um gateway.

Para a construção de um sistema de gerenciamento de redes inteligente, as aplicações devem conter todo este conhecimento. Como este conhecimento não pode ser fornecido no formato da MIB, os fornecedores de aplicações de gerenciamento devem desenvolver outras formas de incluir estes conhecimentos em suas aplicações. Sem esta inteligência, muitas aplicações genéricas ficam limitadas à coleta, formatação e exibição das informações de gerenciamento. Estas informações são apresentadas para o usuário, que aplica sua inteligência humana para analisá-las. Esta carga só poderá ser retirada das mãos do administrador de rede se as aplicações se tornarem mais inteligentes.

Sem esta inteligência será muito difícil que uma aplicação possa coletar informações suficientes de uma MIB desconhecida para gerenciar eficientemente um dispositivo desconhecido.

4.5 - Interface com o Usuário

A indústria de gerenciamento de redes reconhece que, embora os protocolos e MIB's de gerenciamento tenham progredido muito, as aplicações de gerenciamento ainda deixa muito a desejar. Alguns membros da comunidade de padronização acreditam que a solução é a inclusão de novos tipos de informação ao formato da MIB padrão. As informações orientadas para a aplicação deveriam ser adicionadas às definições dos objetos da MIB. Além das informações existentes, como tipo e descrição, as informações orientadas para a aplicação consistem de labels para tabelas ou gráficos, informações para formatação, valores-limiares (*thresholds*), texto de ajuda (*help*), e outras. Estas informações seriam lidas pela estação de gerenciamento, que as utilizaria para produzir uma melhor interface com o usuário para os objetos de gerenciamento SNMP.

As informações orientadas para a aplicação são lidas pela estação de gerenciamento. Algumas destas informações podem controlar como a aplicação vai exibir os dados coletados através do protocolo SNMP, enquanto outras informações podem ser exibidas para ajudar o usuário a entender o significado destes dados. No entanto, as aplicações que utilizam estas novas facilidades não podem ser consideradas “inteligentes”, pois não são capazes de fazer recomendações para o usuário com base nos dados recebidos através do protocolo SNMP. Esta inteligência, tão desejada pelos gerentes de rede, só poderá ser fornecida adequadamente pelas aplicações desenvolvidas para uma MIB particular.

Como as MIB’s proprietárias multiplicam o número de MIB’s padrão por um fator de dez, é muito difícil para os fabricantes de aplicações de gerenciamento de rede suportar todas as MIB’s proprietárias. Para estas MIB’s, as informações adicionadas orientadas para a aplicação são muito importantes.

4.5.1 - Divulgando as informações

Foi sugerido que as informações orientadas para a aplicação fossem adicionadas ao formato padrão das MIB’s, pela extensão da macro OBJECT-TYPE. Por várias razões, este não é o lugar ideal para definir estas informações. Uma MIB é um contrato entre os projetistas de agentes e os projetistas de aplicações de gerenciamento, realizado por uma entidade de padronização ou por um fabricante.

Uma MIB descreve os objetos de gerenciamento para garantir que a implementação dos agentes e gerentes utilizem as mesmas definições. Os autores de MIB’s em geral e as entidades de padronização em particular não podem assumir a responsabilidade adicional de projetar a interface para os usuários. Os grupos que trabalham na definição de novas MIB’s possuem muitos outros detalhes para se preocupar. Além disso, os grupos de padronização são internacionais.

A forma correta de adicionar estas informações nas aplicações seria a criação de uma nova macro, ligada ao objeto da MIB ao qual se refere. Arquivos de macros APPLICATION-INFO poderiam ser fornecidos pelos vendedores de agentes para definir partes da interface para o usuário das estações de gerenciamento. Esta estratégia seria mais apropriada para MIB’s proprietárias, que, de outra forma não poderia esperar suporte à aplicação de todas as estações de gerenciamento de redes. É importante que as aplicações de gerenciamento se tornem mais eficientes. Porém, a adição de novas funções a estas aplicações deve se concentrar nas áreas corretas. As informações sobre a interface com o usuário não pertencem as MIB’s padrão, mas serão muito úteis se estiverem disponíveis a partir de outras fontes.

As MIB’s da ISO e da Internet são modeladas através das técnicas de programação por objeto. Dentro deste contexto, os recursos a serem gerenciados são representados através de objetos gerenciados. A grande diferença entre estas MIB’s reside nas hierarquias usadas para representar tais objetos. A hierarquia de registros é usada para identificar de maneira universal os objetos tanto nos casos da ISO como no caso da Internet. Em ambos, esta hierarquia é especificada seguindo as regras definidas pela notação ASN.1 usada na atribuição de identificadores de objetos.

Embora a arquitetura de gerenciamento SNMP tenha possibilitado o monitoramento dos nós gerenciadores, ela não provocou a produção de aplicações de gerenciamento “inteligentes”. A principal causa desta situação é que as informações de gerenciamento foram definidas em um nível muito baixo. Foram produzidas diversas MIB’s contendo vários objetos gerenciados, mas não foram produzidos documentos descrevendo como estes objetos podem ser usados no gerenciamento eficiente de uma rede. O resultado disto é que a maioria das aplicações de gerenciamento é de *browsers*, que não possuem nenhuma inteligência. Por outro lado, alguns dos produtos desenvolvidos nos últimos anos possuem características mais inteligentes e, portanto úteis do que estas ferramentas mais simples.

Capítulo 5 - O protocolo SNMP

O protocolo SNMP (*Simple Network Management Protocol*) é a solução adotada na Internet para permitir que gerentes de redes possam localizar e corrigir problemas. Geralmente, é utilizado um processo na máquina do administrador chamado de cliente (uma *workstation* ou um *gateway*, por exemplo) que se conecta a um ou mais servidores SNMP localizados em máquinas remotas, para executar operações sobre os objetos gerenciados (por exemplo, para obter informações sobre estes objetos).

5.1 – Descrição do protocolo

O SNMP utiliza o protocolo UDP na comunicação entre cliente e servidor. Para o cliente da rede, o SNMP executa as operações sobre os objetos de forma transparente, o que permite a interface do software de gerenciamento da rede criar comandos imperativos para executar operações sobre os objetos gerenciados. Esta é a grande diferença entre gerenciar uma rede usando o protocolo SNMP e gerenciar a mesma rede usando outros protocolos.

No protocolo SNMP são definidas tanto a sintaxe (forma e a representação dos nomes e dos valores) como o significado das mensagens trocadas entre os clientes e os servidores. O formato das mensagens e dos objetos gerenciados de uma MIB são especificados com a linguagem ASN.1 e ao contrário de outros protocolos usados nas redes TCP/IP, suas mensagens não apresentam campos fixos, e portanto, não pode-se representar as mensagens simplesmente com o uso de estruturas fixas. O SNMP também define as relações administrativas entre os vários *gateways* que estão sendo gerenciados, determinando a autenticação necessária para os clientes acessarem os objetos gerenciados.

Ao contrário dos outros protocolos de gerenciamento que apresentam muitos comandos (operações), o SNMP apresenta somente um conjunto limitado de comandos, baseado num simples mecanismo de busca/alteração. Portanto, é muito mais simples de ser implementado do que um protocolo com muitas operações, em que cada operação sobre um objeto necessita de um comando diferente para implementá-la.

O mecanismo de busca/alteração conceitualmente só apresenta duas operações: uma que permite ao cliente alterar atributos de um objeto de uma MIB (**SET**), e outra para obter os valores dos atributos de um objeto (**GET**). Somente estão disponíveis estas operações (e suas variações) para o gerenciamento da rede, que serão aplicadas sobre os objetos de uma MIB. A principal vantagem de um mecanismo como este é a simplicidade e flexibilidade que este mecanismo dá ao protocolo, o que permite ao SNMP ser um protocolo bem estável porque a sua estrutura básica continuará fixa, mesmo que novos objetos sejam adicionados na MIB, ou que novas operações sejam definidas sobre estes objetos (elas serão constituídas por estas operações básicas).

A MIB define o conjunto e a semântica dos objetos que os servidores SNMP devem controlar, ou seja, define o conjunto conceitual de objetos que um servidor SNMP controla. A MIB é usada para armazenar em seus objetos os estados internos

das entidades de uma rede. Na maioria dos casos, usamos as variáveis convencionais para o armazenamento dos objetos de uma MIB, mas em alguns casos, em que a estrutura interna do TCP/IP não é exatamente compatível com a estrutura de um objeto de uma MIB, é necessário que o SNMP seja capaz de computar os objetos de uma MIB a partir das estruturas de dados disponíveis (simulação deste conjunto conceitual de objetos).

Ao receber e enviar mensagens no protocolo SNMP, os nomes dos objetos não devem ser armazenados na forma textual, e sim na forma numérica definida pela sintaxe ASN.1, que representa o objeto univocamente, com o objetivo de tornar o pacote SNMP mais compacto. Quando a forma numérica que representa um objeto terminar com um zero (como em 1.3.6.1.2.1.4.3.0), representa que o objeto é a única instância existente. Por exemplo, o objeto gerenciável iso.org.dod.internet.mgmt.mib.ip.ipInReceives será representado na mensagem SNMP como 1.3.6.1.2.1.4.3.

Para minimizar o espaço interno necessário para representar um objeto, e considerando que todos os objetos em uma MIB apresentam o mesmo prefixo no seu nome, podemos retirar o prefixo após a mensagem chegar na máquina, e recolocá-lo imediatamente antes de enviar a mensagem para outra máquina. Resumidamente os principais objetivos do protocolo SNMP são:

- Reduzir o custo da construção de um agente que suporte o protocolo;
- Reduzir o tráfego de mensagens de gerenciamento necessárias para gerenciar os recursos da rede;
- Reduzir o número de restrições impostas as ferramentas de gerenciamento da rede, devido ao uso de operações complexas e pouco flexíveis;
- Apresentar operações simples de serem entendidas, sendo facilmente usadas pelos desenvolvedores de ferramentas de gerenciamento;
- Permitir facilmente a introdução de novas características e novos objetos não previstos ao se definir o protocolo;
- Construir uma arquitetura que seja independente de detalhes relevantes somente a algumas implementações particulares.

A versão atual do protocolo SNMP é a 2.0 (SNMPv2). A principal diferença entre esta versão e a anterior é a existência de um mecanismo de comunidade melhorado, que apresenta uma identificação não ambígua tanto da origem, como do formato da mensagem SNMPv2, permitindo utilizar métodos de acesso mais convencionais aos objetos gerenciados, além de permitir o uso futuro de protocolos assimétricos de segurança, com o uso de chaves públicas.

O SNMP tem como base a técnica “fetch-store”, ou seja, todas as suas operações previstas são derivadas de operações básicas de busca e armazenamento. Estas operações são:

- get-request - leitura de uma variável
- get-next-request - leitura da próxima variável
- get response - resposta a uma operação de leitura
- set request - gravação de um campo variável
- trap - notificação da ocorrência de um evento

Um gerente interage com um agente de acordo com as regras estabelecidas pelo framework de gerenciamento. Em geral, o gerenciamento da rede impõe

overheads significativos, pois cada nó apenas produz algumas variáveis que serão lidas e usadas para sua monitoração.

5.2 - Operações disponíveis no protocolo SNMP

Após a definição de como são armazenadas as informações em uma MIB pelas entidades do protocolo SNMP, é importante saber o que deve ser feito com estas informações. O que deve ser feito com os objetos num ambiente de gerenciamento é definido através das operações aplicadas nos objetos, que são enviadas ao servidor pelo cliente. Duas operações (comandos) básicas no protocolo SNMP são:

- **SET** - é usada por um cliente para alterar um ou mais atributos de um objeto gerenciado (*set-request*);
- **GET** - é usada por um cliente para obter o valor(es) de um ou mais atributos de um objeto gerenciado (*get-request* para o pedido e *get-response* para obter o retorno deste pedido).

Uma operação GET ou SET somente se refere a uma única instância de um objeto representada através de seu nome. No protocolo SNMP, as operações são atômicas, isto é, todas as operações de um pedido devem ser executadas. Não existem execuções parciais de um pedido (no caso, operações aplicadas a múltiplos objetos). Se ocorrer algum erro durante a execução de uma operação, os resultados produzidos por esta operação devem ser ignorados. Antes de executar um pedido, o servidor deve mapear apropriadamente os nomes dos objetos codificados em ASN.1 nos objetos internos que armazenam as características das entidades da rede (através dos atributos do objeto).

Além das operações padrões, existem mais outras duas operações:

- **GET-NEXT** - o nome do objeto não só especifica o objeto a acessar (para obter seus atributos, como na operação GET normal), como também é usado para descobrir qual o próximo objeto na seqüência léxica. Como retorno, a operação informa o nome do próximo objeto na hierarquia da MIB, e os valores dos seus atributos.
- **TRAP** - é usada para informar a ocorrência de eventos, permitindo aos servidores SNMP enviarem informações aos clientes sempre que ocorrer algum evento que informa a ocorrência de alterações nos objetos (no protocolo, foram definidas somente algumas *traps*).

A operação GET-NEXT é útil para obter os atributos dos objetos de uma tabela de tamanho desconhecido, pois um cliente pode enviar continuamente requisições GET-NEXT a um servidor que se encarregará de enviar os atributos do objeto e o nome do próximo objeto. Cada novo pedido deve especificar o nome do objeto retornado pelo pedido anterior, o que permite varrer a tabela sem saber qual o próximo objeto desta tabela. Este processo é chamado de caminhamento na tabela. Devido ao ASN.1 não apresentar nenhum mecanismo para implementar tabelas ou para indexá-las, denotamos os elementos individuais (objetos) de uma tabela através de um sufixo.

Para facilitar o uso do comando GET-NEXT em tabelas, alguns nomes de objetos na MIB correspondem tabelas completas ao invés de objetos individuais, não podendo ser usados em uma operação GET (pois esta falhará), mas podem ser usados como parâmetro para a operação GET-NEXT, indicando o primeiro objeto da

tabela. Não será necessário conhecer o nome do próximo objeto, pois cada comando GET-NEXT retornará o nome do próximo item da tabela. Executando este processo sucessivamente até que todos os itens da tabela tenham sido acessados, teremos varrido toda a tabela.

A implementação de uma estrutura de dados que suporte o comando GET-NEXT pode ser complicada devido a esta operação poder pular o próximo objeto simples (na ordem lexicográfica) devido a existência de objetos vazios. Como conseqüência, não se pode usar simplesmente a ordem lexicográfica presente na árvore para determinar quais objetos satisfazem a um comando GET-NEXT, devendo também existir um programa que examine os objetos, pule aqueles objetos que estejam vazios e descubra o primeiro objeto simples pertencente a um objeto não vazio.

Para o suporte das funções GET, SET e GET-NEXT sobre tabelas, ao contrário do que acontece com objetos simples mapeados em memória, é necessário um software adicional para mapear a tabela numa estrutura interna de dados. No caso das tabelas MIB, o servidor SNMP deve providenciar algum mecanismo que permita a cada tabela ter três funções para implementar as operações GET, SET e GET-NEXT.

Para o servidor descobrir qual função deve ser usada, o software que implementa o servidor deve usar a tabela para escolher a função correta, através do uso de um ponteiro para uma tabela que conterá ponteiros para cada uma das operações. As entradas em uma tabela apontam para outras tabelas que não contém o identificador completo do objeto, mas somente o prefixo deste identificador, porque o identificador completo do objeto para um item da tabela é formado pelo prefixo que identifica a tabela, mais um sufixo que identifica uma entrada particular na tabela em que o objeto está armazenado. Uma vez determinado o prefixo correspondente ao objeto e formado o nome do objeto, a função de acesso correspondente à operação pedida é invocada. No caso das tabelas, a função de acesso obtém o sufixo do identificador do objeto, e o usa para selecionar uma das entradas da tabela. Para a maioria das tabelas, é usado o endereço IP para selecionar uma entrada. O endereço IP é codificado no identificador do objeto usando-se a representação decimal com pontos.

5.3 - Mensagens no protocolo SNMP

Ao contrário de muitos outros protocolos TCP/IP, as mensagens no protocolo SNMP além de não apresentarem campos fixos, são codificadas usando a sintaxe ASN.1 (tanto a mensagem de pedido, como a de resposta) o que dificulta o entendimento e a decodificação das mensagens.

As partes mais importantes de uma mensagem são: as operações (GET, SET e GET-NEXT) e a identificação, no formato ASN.1, dos objetos em que as operações devem ser aplicadas.

Deve existir um cabeçalho que informe o tamanho da mensagem, que só será conhecido após a representação de cada campo ter sido computada. Na verdade, o tamanho da mensagem depende do tamanho de sua parte remanescente (que contém os dados), portanto o tamanho só poderá ser computado após a construção da

mensagem. Uma maneira de evitar este problema é construir a mensagem de trás para frente.

Uma mensagem SNMP deve definir o servidor do qual obtemos ou alteramos os atributos dos objetos, e que será responsável por converter as operações requisitadas em operações sobre as estruturas de dados locais. Após verificar os campos de uma mensagem, o servidor deve usar as estruturas internas disponíveis para interpretar a mensagem e enviar a resposta da operação ao cliente que requisitou o pedido. Uma mensagem é constituída por três partes principais:

- A versão do protocolo;
- A identificação da comunidade, usada para permitir que um cliente acesse os objetos gerenciados através de um servidor SNMP;
- A área de dados, que é dividida em unidades de dados de protocolo *(Protocol Data Units - PDU's*). Cada PDU é constituída ou por um pedido do cliente, ou por uma resposta de um pedido (enviada pelo servidor).

O primeiro campo de uma mensagem SNMP é um operador seqüencial, seguido por um campo com o tamanho total da mensagem (se este tamanho não for igual ao do datagrama, será retornado um código de erro). O próximo campo é um número inteiro que identifica a versão do protocolo SNMP, seguido por um campo usado para a autenticação, indicando a comunidade que o cliente pertence (a comunidade public permite a qualquer cliente acessar os objetos, não precisando o servidor verificar se o cliente pode ou não acessar o objeto). O quarto campo contém a operação que será executada, devendo ser um GET, SET ou GET- NEXT pois a operação de TRAP só é gerada pelo servidor. O quinto campo é usado para o servidor ter certeza de que o valor deste campo é igual ao tamanho da parte da mensagem que contém os dados. O sexto campo é uma identificação para o pedido, e o sétimo e o oitavo campo são flags que indicam erros quando estão setadas (campos de *status* e de índice de erro).

Na definição de uma mensagem, cada uma das PDU's é constituída ou por um dos cinco tipos de PDU's para as operações ou por uma PDU para a resposta. Na definição da mensagem SNMP, deve-se ter uma sintaxe individual para cada um das cinco operações da PDU. Alguns termos encontrados nas sintaxes das PDU's das operações são:

- O campo RequestID é um inteiro de 4 bytes (usado para identificar as respostas);
- Os campos ErrorStatus e ErrorLevel são inteiros de um byte (sendo nulos em um pedido de um cliente);
- O campo VarBindList é uma lista de identificadores de objetos na qual o servidor procura os nomes dos objetos, sendo definida como uma seqüência de pares contendo os nomes dos objetos (em ASN.1 este par é representado como uma seqüência de dois itens). Na sua forma mais simples (com um objeto) apresenta dois itens: o nome do objeto e um ponteiro nulo.

5.4 - Servidores e Clientes SNMP

Um servidor SNMP deve ser capaz de aceitar pedidos de operações sobre os objetos gerenciados, executá-los e retornar o resultado das operações após sua execução. A figura seguinte ilustra como uma mensagem percorre um servidor SNMP, mostrando que primeiramente a mensagem é interpretada, indicando qual objeto da MIB deve ser mapeado num item de dados local sobre o qual a operação será aplicada.

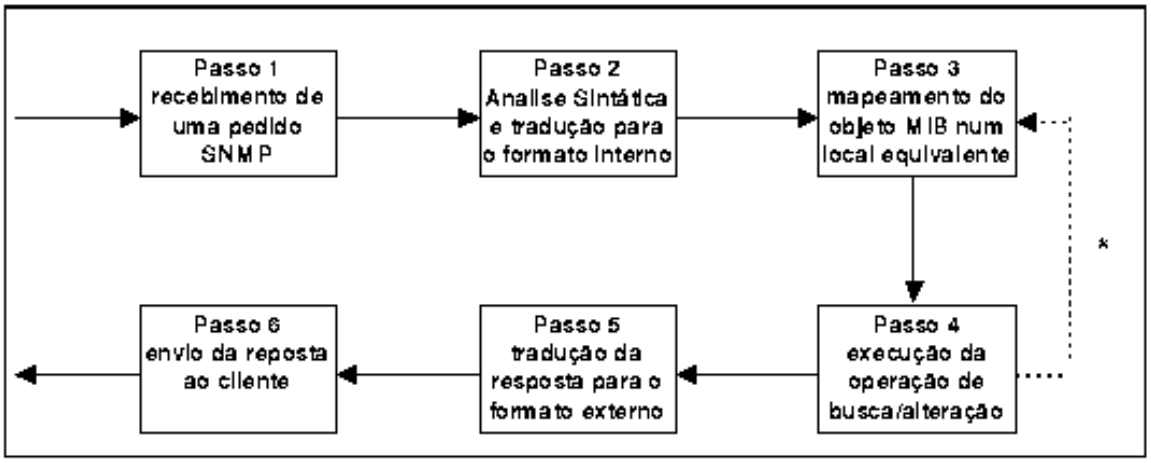


Figura 6 - Fluxo de uma mensagem SNMP dentro de um servidor. Os passos 3 e 4 são repetidos para cada objeto especificado na mensagem (passo com *)

Numa operação de busca, as informações sobre o(s) objetos(s) são retornadas na mensagem SNMP de resposta ao pedido, que depois de ser convertida para o formato de uma mensagem SNMP, será enviada ao cliente que solicitou a operação. Se forem solicitadas operações sobre múltiplos objetos (representados na mensagem por seus identificadores), a operação será aplicada a cada um dos objetos presentes na mensagem (passos 3 e 4 na figura).

Um servidor SNMP deve ter um eficiente mapeamento de nomes, pois quando um nome de um objeto na sintaxe ASN.1 chegar ao servidor num pedido, o servidor deverá ser capaz de reconhecer o nome, para chamar o procedimento correto para executar a operação solicitada no pedido. Ao invés de manter todas as informações necessárias para atender ao pedido, podemos chamar um procedimento que irá mapear o nome do objeto para a sua representação interna correspondente. A maioria destes procedimentos é rápida e direta, pois simplesmente convertem o formato de uma mensagem SNMP (no formato ASN.1) para a representação interna, mas se não existir uma representação para algum objeto no servidor, os pedidos que executem operações sobre este objeto irão requerer mais computação por parte do servidor, e não somente a computação necessária para uma simples tradução de um nome de um objeto MIB para a estrutura de dados local usada para armazenar os dados.

Após a conversão dos campos da mensagem para a forma interna usada pelo servidor, o pedido será armazenado numa estrutura descritora que contem um

ponteiro para uma lista ligada com os nomes de todos os objetos sobre os quais a operação deve ser aplicada. Após serem geradas as respostas, estas devem ser convertidas para que possam ser adicionadas na mensagem de resposta, que será enviada ao cliente que solicitou o pedido. As operações presentes nos pedidos geralmente são executadas por funções no processo servidor. Na prática, existem vários detalhes que complicam o código do servidor, como o fato de a mensagem SNMP usar a representação ASN.1 em seus campos. Por isso, o servidor não pode usar uma estrutura fixa para descrever o formato da mensagem, mas ao invés de usar uma estrutura não fixa (variável), o servidor pode percorrer a mensagem, analisar cada campo como pode, traduzindo cada um dos campos do formato ASN.1 para o seu formato interno, e traduzindo a resposta para o formato ASN.1 antes de enviá-la ao cliente.

Um cliente SNMP deve construir e enviar o seu pedido ao servidor, esperar pela resposta de seu pedido, e verificar se a resposta concorda com a resposta do que foi pedido. Devido ao protocolo UDP não garantir a entrega dos pacotes, o cliente deve implementar estratégias para *time out* e retransmissão das mensagens que contém os pedidos. Um cliente só pode obter ou alterar os atributos de um objeto gerenciado somente se tiver permissão para acessar o objeto. Esta permissão é definida através de uma política de acesso. Esta política usa o mecanismo de comunidades (community), em que definimos para cada comunidade, um grupo de objetos e de operações que podem ser realizadas sobre estes objetos. Se um cliente não pertencer a comunidade autorizada para acessar o objeto, ou se não tiver autoridade para executar a operação sobre o objeto presente em seu pedido, o pedido será recusado, e será retornada uma mensagem de erro ao cliente, informando que ele não tem direito de acesso ao objeto, ou que ele não pode executar a operação pedida sobre os atributos do objeto. Este mecanismo permite a definição de relações administrativas entre os servidores e os clientes SNMP de uma rede.

5.5 – SNMPv2

Apesar do alto índice de aceitação, a implementação de protocolos e aplicações SNMP apresentaram deficiências, principalmente, com relação à segurança e a transferência eficiente de um grande número de informações do agente para o gerente. Além disso, o SNMP não se adequa ao gerenciamento de grandes redes de computadores, devido ao fato de apresentar limitações de desempenho para obtenção de requisições explícitas, e não dar suporte à comunicação gerente-gerente. Apenas durante o ano de 1993, foram publicadas 11 RFC's definindo revisões para o SNMP e dando início ao padrão SNMPv2. Esta série de revisões trouxe consigo grandes avanços que foram incorporados ao protocolo original. Tais avanços podem ser classificados de acordo com as seguintes categorias:

- Estrutura de informação;
- Primitivas de comunicação (PDU's);
- Comunicação gerente-gerente e gerenciamento hierárquico;
- Segurança.

A estrutura de informação de gerenciamento (SMIv2) para o SNMPv2 é mais elaborada, e eliminou ambigüidades nas definições dos objetos encontrados nas especificações anteriores. Em relação às primitivas foram acrescentados dois novos PDU's:

- **get-bulk-request-PDU**, que permite que uma grande quantidade de informações possa ser transferida do agente para o gerente eficientemente;
- **inform-request-PDU**, que permite a um gerente enviar ou eventualmente solicitar informações a outro gerente.

As comunicações gerente-gerente, como também o gerenciamento hierárquico, foram incorporados ao protocolo com a introdução do novo tipo de mensagem, *inform-request;* e com a SNMPv2-M2M MIB, que é constituída por dois grupos: um grupo de alerta e um grupo de eventos.

No aspecto segurança, o SNMPv2 acrescentou ao protocolo novos conceitos e serviços que trouxeram mais segurança ao protocolo. Os conceitos incluídos foram: o conceito de visão de MIB definido em termos de sub-árvores, restringindo o acesso a porções predefinidas da MIB; e o conceito de contexto, que é uma coleção de objetos e seus respectivos agentes, e a especificação dos privilégios envolvidos. Os serviços incluídos são de integridade, autenticação e confiabilidade dos dados.

Capítulo 6 - Gerenciamento no modelo OSI

Assim como o protocolo SNMP, a ISO propõe como solução para gerenciamento de redes o protocolo CMIP (Common Management Information Protocol), que também define em seu escopo os papéis de gerente e agente que trocam informações sobre os recursos gerenciados e que são armazenados em MIB's.

6.1 – O protocolo CMIP e os serviços do CMIS

O protocolo CMIP engloba vários tipos de PDU's, que são mapeadas em operações análogas ao SNMP. São elas:

- **M-Action -** execução de alguma ação sobre um objeto gerenciado
- **M-Create -** criação de uma instância de um objeto gerenciado
- **M-Delete -** remoção de uma instância de um objeto gerenciado
- **M-Get -** leitura de atributos dos objetos gerenciados
- **M-Set -** modificação de atributos de objetos gerenciados
- **MEVENT-REPORT -** notificação de um evento associado a um objeto gerenciado.

Também são definidos recursos adicionais que permitem selecionar o grupo de objetos sobre os quais se aplica uma determinada operação. O scopping, como é chamado este recurso, permite selecionar um grupo instância de objeto sobre os quais se realizará uma única operação.

Por meio dos recursos de filtro, outra facilidade do CMIP, é possível definir um conjunto de testes aplicáveis a um grupo de instâncias de objetos, que fora anteriormente selecionado através do scopping. Assim sendo, é possível reduzir significativamente a extração sobre a qual se desenrolará uma operação de gerenciamento. Além destes, existe o recurso de sincronização, que permite sincronizar diversas operações de gerenciamento realizadas sobre instâncias de objetos selecionados através de recursos de scopping e filtro.

Existe uma terceira proposta chamada de CMOT (*CMIP Over TCP/IP*) cujo objetivo é permitir o uso do CMIP em redes com o protocolo TCP/IP.

Uma comparação entre o SNMP e o CMIP demonstra que o SNMP é excessivamente simples quando usado em aplicações que não foram previstas quando foi definido, e que apresenta deficiências em relação a segurança ao ser usado em aplicações mais críticas. Já o CMIP é um protocolo poderoso e abrangente, que já foi concebido com o objetivo de adequar-se à complexidade das redes. Mas apesar desta característica, ainda não alcançou um grau de estável de aceitação pela comunidade. As projeções de mercado demonstram que o SNMP continuará sendo muito usado em pequenas redes, enquanto que o CMIP deve dominar o mercado composto pelas grandes redes corporativas e redes públicas de telecomunicações.

Os serviços do CMIS e o protocolo CMIP são oferecidos na camada de aplicação, sendo usados para implementar sistemas desenvolvidos para vários propósitos, como gerenciamento de desempenho, do nível de falhas, de segurança, de

configuração e de contabilidade, usando os recursos de uma rede baseada no modelo de comunicação OSI.

CMIS - Common Management Information Service, são os serviços prestados na camada de aplicação. São orientados a conexão, necessitando de um canal virtual para troca de informações. Permite definir os objetos através da seleção de sub-árvores (*scopping*), ou através do uso de predicados (filtragem). O CMIS apresenta os seguintes serviços às aplicações de gerenciamento:

- GET - Para obter informações (atributos) de um objeto gerenciado;
- SET - Para alterar os atributos de um objeto gerenciado;
- ACTION - Para executar um comando sobre um objeto gerenciado;
- CREATE - Para criar uma nova instância de um objeto;
- DELETE - Para descartar uma instância de um objeto (removê-la);
- EVENT-REPORT - Para o relato de ocorrências excepcionais (notificações sobre um evento associado a um objeto gerenciado).

Alem das funções apresentadas no protocolo CMIP, o CMIS apresenta facilidades adicionais que permitem selecionar um conjunto de objetos sobre o qual pode-se aplicar a mesma operação, e também a existência de respostas múltiplas para cada requisição (uma para cada objeto gerenciado). São três facilidades adicionais:

1. **Scopping** - permite selecionar um grupo de instâncias de objetos gerenciados sobre o qual será aplicada uma única operação;
2. **Filtro -** dá a possibilidade de definir um conjunto de testes que serão aplicados a um grupo de instâncias de um objeto, selecionado por uma operação de *scopping* anterior, permitindo formar um grupo menor a partir deste, sobre o qual as operações de gerenciamento devem ser aplicadas;
3. **Sincronização** permite sincronizar várias operações de gerenciamento a serem aplicadas a instâncias de objetos gerenciados, obtidos através do uso das operações de scopping e de filtragem.

O CMISE (Common Management Information Service Element) implementa os serviços definidos pelo CMIS, executando o protocolo CMIP. É correspondente ao mecanismo SASE (*Special Application Service Element*) da camada de aplicação, e utiliza os elementos ACSE (*Association Control Service Element*) e ROSE (*Remote Operations Service Element*) que juntos correspondem ao mecanismo de CASE (*Common Application Service Element*) também da camada de aplicação.

O protocolo CMIP apresenta uma forma inteligível comum utilizada para transferir as informações de gerenciamento entre as entidades pares na comunicação de gerenciamento, sendo que uma destas atua como um gerente, enquanto a outra atua como agente, sendo que as informações são armazenadas em MIB's descritas através da linguagem ASN.1.

Um *framework* que utilize o protocolo CMIP tende a usar a modelagem da orientação a objetos, que encapsula as operações associadas a uma estrutura de dados na própria estrutura. Aqui um agente tem um servidor de objetos gerenciados que pode executar operações de gerenciamento nas variáveis relacionadas a um nó gerenciado. Se este agente for executado em outra máquina (separadamente ao resto do código de gerência), tem-se então o gerenciamento distribuído de rede.

Os serviços oferecidos pelo CMISE ao protocolo CMIP podem ser confirmados ou não confirmados. Os serviços oferecidos pelo CMISE e usados pelas aplicações de gerenciamento e para o informe de notificações, são:

- M-EVENT-REPORT - Reporta um evento de um objeto gerenciado;
- M-GET - Solicita a busca de informações de gerenciamento;
- M-CANCEL-GET - Solicita o cancelamento de um serviço M-GET previamente requisitado e ainda pendente;
- M-SET - Solicita a modificação da informação de gerenciamento;
- M-ACTION - Solicita a execução de uma ou mais ações sobre os objetos gerenciados;
- M-CREATE - Solicita a criação de uma instância de um objeto gerenciado;

M-DELETE - Solicita a remoção de uma ou mais instâncias de objetos gerenciados.

6.2 - Conceitos básicos

O gerenciamento no modelo OSI da ISO baseia-se na teoria da orientação a objetos. O sistema representa os recursos gerenciados através de entidades lógicas chamadas de objetos gerenciados. Ao desenvolver uma aplicação de gerenciamento, usamos processos distribuídos conhecidos como gerentes (os quais gerenciam) e agentes (os que realizam as ações).

Além de definir um modelo informacional, define-se também um modelo funcional em que para cada área é definido um conjunto de funções, que ao serem implementadas, serão usadas para gerenciar a rede. Existem cinco áreas funcionais no gerenciamento num ambiente OSI:

- Gerência de configuração (estado da rede);
- Gerência de desempenho (vazão e taxa de erros);
- Gerência de falhas (comportamento anormal);
- Gerência de contabilidade (consumo de recursos);
- Gerência de segurança (acesso).

6.2.1 - Gerentes, agentes e objetos gerenciados

A função de um processo gerente é a da coordenação das atividades a serem realizadas, através do envio de solicitações aos processos agentes. Cabe aos processos agentes a execução das operações sobre os objetos gerenciados, o envio das respostas as solicitações feitas pelos gerentes, e a emissão de notificações aos gerentes que relatem qualquer alteração ocorrida no estado dos objetos gerenciados. Ao estabelecer uma associação com os processos de aplicação, é possível que o gerente realize operações sobre o objeto ou sobre seus atributos. Este relacionamento entre gerente, agente e objeto gerenciado pode ser visto na figura seguinte.

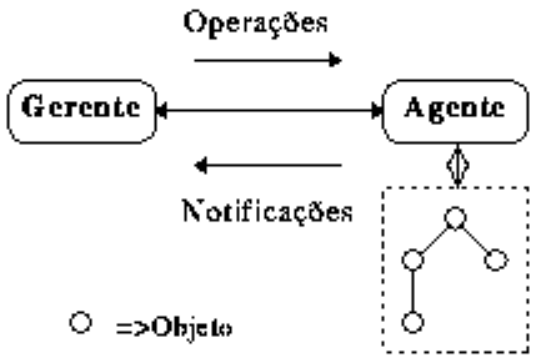


Figura 7 - Relacionamento Gerente - Agente

Um objeto gerenciado é uma representação lógica de um ou mais recursos de comunicação ou de processamento de dados. Pode-se ter objetos específicos para uma camada, chamados de objetos gerenciados da camada N, e objetos usados por mais de uma camada, chamados de objetos gerenciados do sistema. Uma MIB é composta por um conjunto contendo estes objetos e seus atributos (contendo informações de gerência). Definimos um objeto gerenciado através de:

- Seus atributos ou propriedades, que contém informações importantes para representar o recurso que este se relaciona;
- Sua reação às operações que recebe;
- Através de uma notificação, que indica a ocorrência de algum evento;
- As ações (operações) que podemos executar sobre este objeto;
- Seu relacionamento com outros objetos gerenciados.

Para se definir um objeto, é usada a linguagem ASN.1, que descreve os princípios necessários para se especificar os objetos (GDMO - Guidelines for the Definition of Managed Objects).

Num ambiente de gerenciamento OSI, usa-se o protocolo CMIP para definir as regras de comunicação entre os processos gerente e agente. O protocolo CMIP implementa as primitivas oferecidas pelo serviço de informação de gerenciamento CMIS. Este ambiente também propõe uma estrutura de gerenciamento para permitir a definição dos conceitos necessários à construção de classes de objetos gerenciados, os princípios necessários à nomeação dos objetos e dos seus componentes, e como é definido o inter-relacionamento entre os objetos. Para descrever a estrutura, são usadas a Hierarquia de Herança, a Hierarquia de Nomeação e a Hierarquia de Registro.

1. Na **Hierarquia de Herança** a modelagem é realizada com base nas classes de objetos. Para se obter sub-classes com um comportamento mais particular, deve-se detalhar uma superclasse, gerando a partir destas subclasses para um propósito mais particular do que esta classe.
2. Na **Hierarquia de Nomeação** é descrita a relação de composição entre os objetos, ou seja, a relação subordinado-superior entre estes objetos, além de serem definidas as regras usadas para nomear os objetos (*name binding*), de forma que este seja univocamente determinado.

3. Na **Hierarquia de Registro** são registradas as definições das classes dos objetos, os atributos dos objetos, as ações que podem ser aplicadas, as notificações geradas e os pacotes, seguindo as regras definidas pela notação ASN.1.

Um problema que este modelo apresenta é a existência de mais complexidade ao se construir os agentes, mas apesar desta desvantagem, e de os agentes consumirem mais recursos da rede, o uso da rede é otimizado, devido a minimização dos pedidos de informação (*polling*) necessários para obter dados sobre o objeto gerenciado, além de deixar que o gerente realize as tarefas mais específicas.

Devido à hierarquia introduzida por este modelo, é possível que um mesmo processo tenha ao mesmo tempo, a função de gerente e de agente, sendo chamado de gerente intermediário. Assim pode-se distribuir as tarefas entre os gerentes intermediários, de forma que cada um seja responsável por gerenciar um certo domínio da rede.

6.2.2 - Modelo de Gerenciamento OSI

O modelo de gerenciamento OSI é definido com base em dois conceitos principais: Estrutura de gerenciamento e MIB's. Usando-se alem destes, outros conceitos.

Na estrutura de gerenciamento, temos três tipos de gerenciamento:

1. **Gerenciamento de sistemas**: É um protocolo executado na camada de aplicação, que é responsável pelo gerenciamento dos sistemas. Pode-se gerenciar aqui quaisquer objetos associados a um sistema aberto. Este gerenciamento necessita do apoio das funções de todas as sete camadas do modelo OSI para poder realizar o gerenciamento;
2. **Gerenciamento de camada**: Este gerenciamento é realizado sobre os objetos gerenciados relacionados às atividades de uma camada particular, e usa os protocolos de gerenciamento específicos para a camada, e as funções de apoio internas desta camada. Os protocolos de gerenciamento de propósito especial não prestam serviços a camadas superiores, e são independentes dos protocolos de gerenciamento das outras camadas.
3. **Operação de camada**: É usada no gerenciamento de uma única instância de comunicação em uma camada. É um tipo de gerência que exige menores requisitos das funções de apoio, por não ser necessário um protocolo particular para a troca de informações de gerenciamento, pois se utiliza o protocolo normal da camada para trocar estas informações.

Uma MIB é usada para armazenar as informações transferidas ou modificadas quando são usados os protocolos de gerenciamento OSI. As informações podem ou ser fornecidas ou por agentes administrativos locais ou por sistemas abertos remotos. É disponibilizada uma interface MIB para cada uma das sete camadas, que oferece as operações necessárias ao gerenciamento da rede em cada uma das camadas.

Uma interface específica para cada camada é obtida através das Entidades de Gerenciamento de Camadas (*LME - Layer Management Entities*). Cada LME contém a funcionalidade da camada a que está relacionada. A integração destas entidades e a execução da função de interfaceamento com o gerente são executadas pela Entidade

de Aplicação de Gerenciamento de Sistema (*SMAE - System Management Application Entity*). Esta entidade também providencia a interface entre as LME's de um nó da rede com as suas correspondentes no outro nó, usando o Protocolo de Informação de Gerenciamento (*CMIP)*, como pode ser visto na figura seguinte.

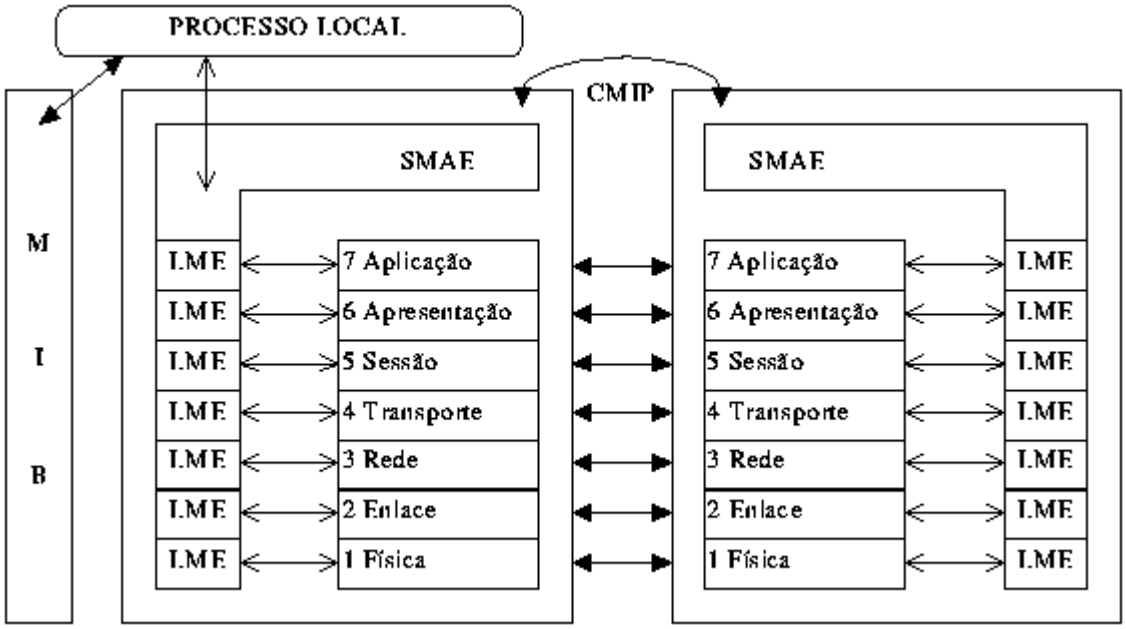


Figura 8 - Modelo de gerenciamento OSI

Os serviços fornecidos por alguma função de gerenciamento de sistema são agrupados em unidades funcionais. Estas unidades são básicas para a negociação entre os Usuários do Serviço de Informação de Gerenciamento (*MIS-Users - Management Information Service-Users*), que são aplicações que utilizam os serviços de gerenciamento, e que podem desempenhar tanto a função de um agente, como a de um gerente. Quando tem a função de agente, o MIS-User é parte de alguma aplicação distribuída que controla os objetos gerenciados no seu domínio (ambiente local), e realiza operações sobre os objetos gerenciados em função dos comandos enviados pelo gerente, podendo também enviar notificações dos objetos gerenciados aos gerentes. Os papéis designados ao MIS-Users não são permanentes, podendo este, dependendo do contexto, ter a função de um agente, de um gerente, ou ambas (o papel que o processo tem será definido com base no processo com o qual este processo interage).

6.3 - Componentes do Modelo de Gerenciamento OSI

Como o ambiente a ser gerenciado é distribuído, as atividades de gerência também devem ser distribuídas. Uma instância de uma aplicação distribuída pode ser formada por uma associação de duas ou mais aplicações de gerenciamento do sistema. As interações entre os sistemas são feitas através das operações de

gerenciamento e das notificações, sendo que uma entidade tem a função de um gerente, solicitando ações de gerenciamento a outra entidade que tem a função de agente, executando as operações e enviando as notificações emitidas pelos objetos gerenciados.

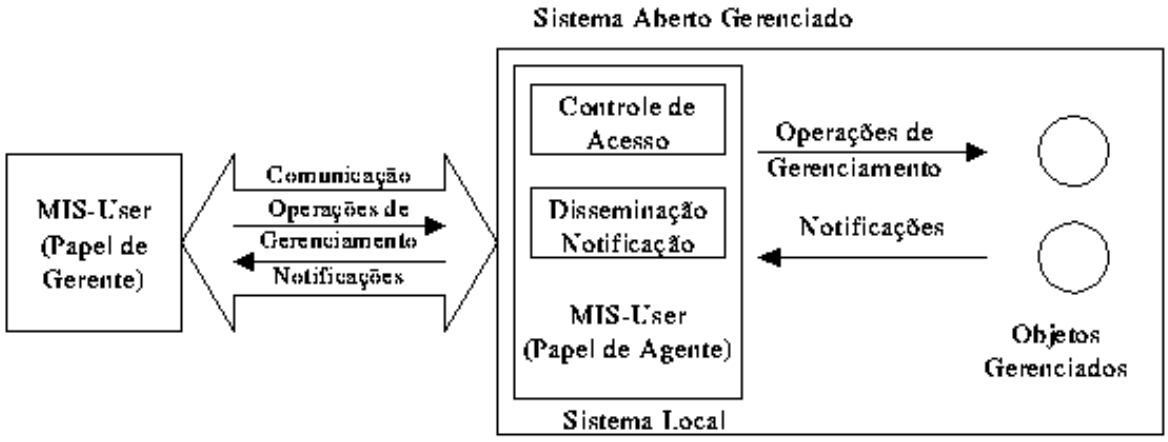


Figura 9 - Suporte de comunicação para notificações e operações de gerenciamento

Um pedido de operação que chega a um agente é rejeitado, a menos que os mecanismos que controlam os acessos aos objetos gerenciados permitam ao gerente realizar as operações solicitadas sobre estes objetos. Sempre que existirem notificações enviadas pelos objetos gerenciados, o sistema gerenciado (agente) envia as notificações aos gerentes. Para a execução das atividades acima, dois aspectos são necessários na comunicação: Suporte para a transferência dos pedidos de operações de gerenciamento e para o envio de notificações entre MIS-Users e suporte para controlar o acesso aos objetos gerenciados para a distribuição das informações de notificação.

6.4 - Aspectos das Comunicações

Os sistemas abertos gerenciados utilizam o protocolo OSI para se comunicarem. O modelo OSI apresenta serviços gerais para gerenciamento chamados de CMIS Além disso, os MIS-Users podem utilizar outros serviços além dos fornecidos pelo modelo OSI. Uma associação entre dois SMAE's é realizada através de um contexto de aplicação que define o conhecimento inicial de gerenciamento compartilhado, e os vários ASEs (*Applicaton Service Elements*) que podem ser usados. Uma SMAE é formada por:

- Elemento de Serviço de Aplicação de Gerenciamento de Sistema (*SMASE - Systems Management Application Service Element*), que especifica a semântica e a sintaxe abstrata da informação que é transferida pelas Unidades de Dados do Protocolo de Aplicação de Gerenciamento (*MAPDU's - Management Application Protocol Data Units*), além de especificar as informações de gerenciamento que devem ser trocadas entre duas SMAE's.

- Elemento de Serviço de Controle de Associação (*ACSE - Association Control Service Element*);
- Elementos de Serviço de Aplicação (*ASEs - Application Service Elements*).

Os serviços de comunicação necessários a uma SMASE podem ser prestados por um Elemento de Serviço de Informação de Gerenciamento Comum (*CMISE)* ou por vários ASEs, como o de Transferência, Acesso e Gerenciamento de Arquivos (*FTAM - File Transfer, Access and Management*), ou pelo Processamento de Transações (*TP - Transaction Processing*). O CMISE define os serviços e procedimentos necessários para transferir as Unidades de Dados do Protocolo Comum de Informação de Gerenciamento (*CMIPDU's - Commom Management Information Protocol Data Units*) e fornece um meio para a troca de informações usadas pelas operações de gerenciamento. Para usá-lo é necessário um Elemento de Serviço de Operações Remotas (*ROSE - Remote Operations Service Element*).

6.4.1 - Conhecimentos de Gerenciamento

As Informações de gerenciamento que são compartilhadas entre os SMAE's são chamadas genericamente de conhecimento de gerenciamento compartilhado (*SMK - Shared Management Knowledge*). Este conhecimento pode ser estabelecido em qualquer momento, em especial, antes de se estabelecer uma associação, durante o seu estabelecimento, ou durante o seu tempo de vida. Pode-se também definir ou alterar o conhecimento de gerenciamento ao se estabelecer a associação. Esta visão de compartilhamento de informações pode ser vista na figura seguinte.

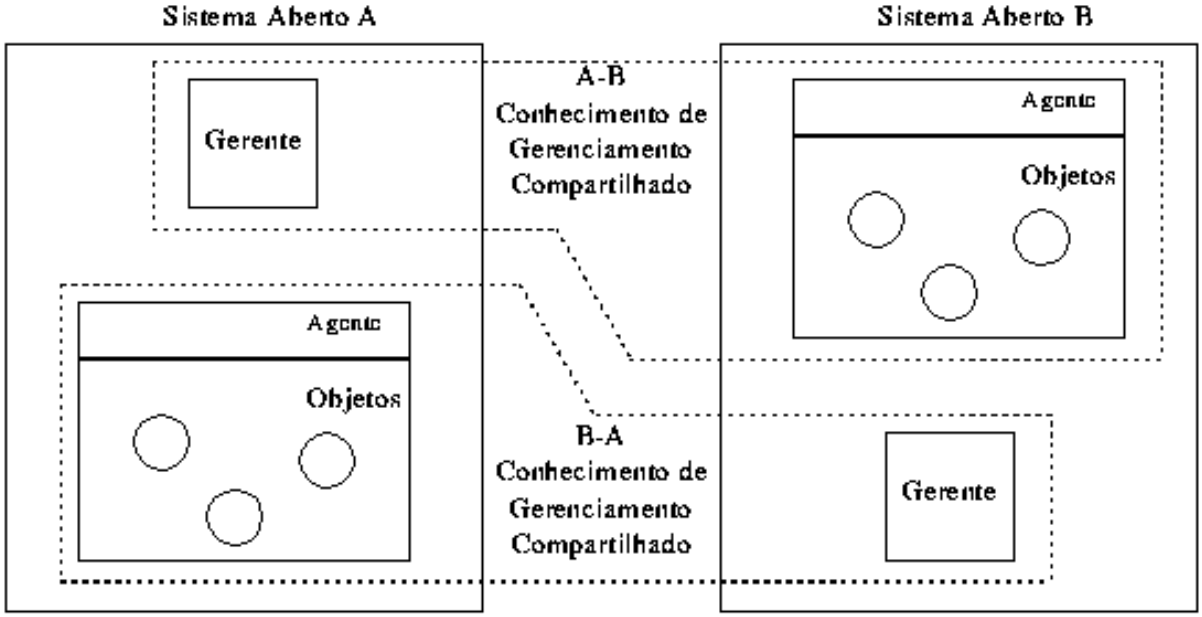


Figura 10 - Gerenciamento compartilhado

O conhecimento de gerenciamento compartilhado deve conter, dentre outras coisas, os seguintes elementos:

- O protocolo utilizado;
- As funções e unidades funcionais suportadas;
- As informações sobre os objetos gerenciados;
- As restrições nas funções suportadas, e as relações entre as funções e os objetos gerenciados.

6.4.2 - Domínios Gerenciais

Um Domínio Gerencial é uma forma de organizar o ambiente de gerenciamento OSI e ocorre quando organizamos os objetos em conjuntos, de forma que o ambiente seja divido de acordo com regras. Divide-se o ambiente de gerenciamento OSI em partes que tenham um mesmo propósito funcional (como falha, segurança, contabilização, desempenho ou configuração), ou o mesmo propósito de gerenciamento (estruturas geográficas, tecnológicas ou organizacionais). Definir temporariamente e alterar os papéis dos gerentes e agentes para cada um dos propósitos definidos, dentro de cada um dos conjuntos de objetos gerenciados definidos e executar as regras de controle de tal forma que estas sejam consistentes (por exemplo, política de segurança).

6.5 - Áreas Funcionais no Gerenciamento OSI

O objetivo do gerenciamento OSI é o de resolver os problemas relativos a configuração de uma rede, as falhas que possam ocorrer nos componentes, aos níveis de desempenho que a rede apresenta, a segurança que esta apresenta e a contabilização de sua utilização. Estas diferentes partes que ocorrem num problema de gerenciamento de redes são chamadas de Áreas Funcionais de Gerência.

Estas áreas funcionais são constituídas por processos de aplicação de gerenciamento residentes na camada OSI de aplicação. Os dados necessários para o funcionamento das diversas áreas funcionais estão em uma MIB que inclui os objetos gerenciados, seus atributos, as operações que podem ser executadas e as notificações que estes podem enviar.

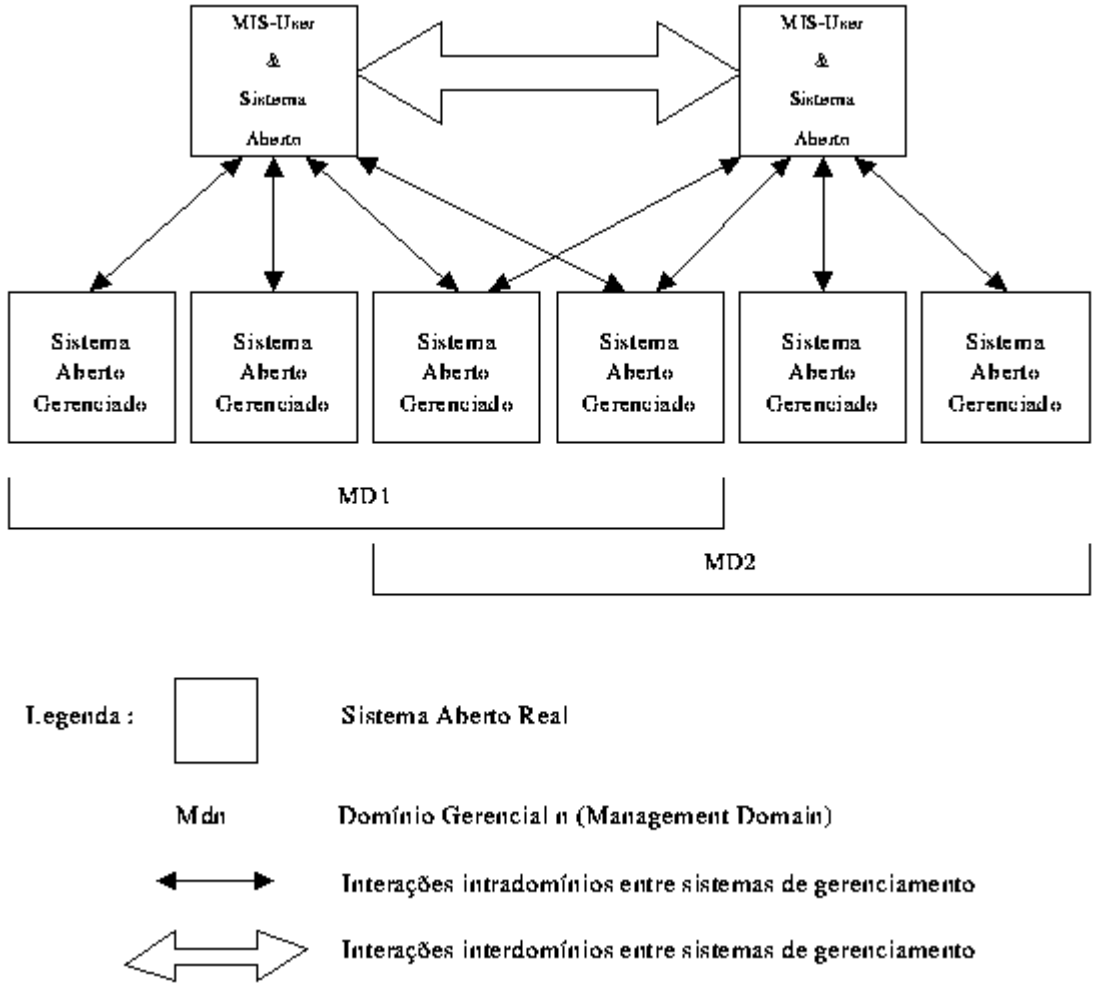


Figura 11 - Domínios gerenciais

A ISO define como deve ser o formato para se representar as informações de gerenciamento, e as ferramentas para coletar as informações e controlar os objetos gerenciados (que são definidos como estruturas de dados especificadas com a linguagem ASN.1), mas como os dados são tratados, e como os resultados devem ser apresentados não são padronizados pela ISO. Para serem atendidos os requisitos necessários as áreas funcionais, foram definidas as seguintes funções de gerenciamento:

- Função de Gerenciamento de Objeto (*OMF - Object Management Function*) - ISO10164-1 - Objetivo gerenciar a criação e a remoção de um objeto gerenciado, e o exame ou alterações nos atributos de um objeto gerenciado. Apresenta funções para gerar relatórios de criação/remoção de objetos, e relatórios de mudanças nos nomes e valores dos atributos dos objetos gerenciados. Aqui é descrito como devemos usar o serviço PASS-THROUGH para mapear uma operação de gerenciamento para o serviço correspondente do CMISE.
- Função de Gerenciamento de Estado (*STMF - State Management Function*) - ISO10164-2 - Esta função é usada para representar as condições instantâneas que se

referem à disponibilidade e operacionalidade de um recurso sob a visão do gerenciamento. Cada classe de objetos gerenciados tem o seu próprio conjunto de atributos de estado, que são usados para expressar e controlar os aspectos de operação dos recursos associados a cada classe. A função de gerenciamento de estado deve ser padronizada, pois deve ser comum a um grande número de recursos gerenciados, e expressa os aspectos essenciais que se referem a operacionalidade de um recurso num dado intervalo de tempo. Tem como objetivo o controle da disponibilidade geral deste recurso, tornando as informações sobre esta disponibilidade visíveis, e no caso do recurso estar inoperante, a função define quais ações devem ser tomadas para colocá-lo operante.

Devem fornecer definições genéricas para permitir a obtenção de informações, a mudança do estado de um dos objetos, e a emissão de notificações sobre as mudanças no estado de um objeto, sempre que decorrerem de alguma operação realizada no sistema aberto. São definidos dentro do escopo de gerenciamento de estado, três fatores que afetam o estado de gerenciamento de um objeto em relação a disponibilidade do recurso associado a este objeto:

- **Operacionalidade:** Se um dado recurso está ou não instalado, e no caso de estar instalado, se está ou não em operação;
- **Utilização:** Se um dado recurso está ou não em uso em um dado instante de tempo, e se este é ou não capaz de aceitar mais outros usuários adicionais;
- **Administração:** Através dos serviços de gerenciamento, impõe-se a permissão ou proibição do uso de um dado recurso.

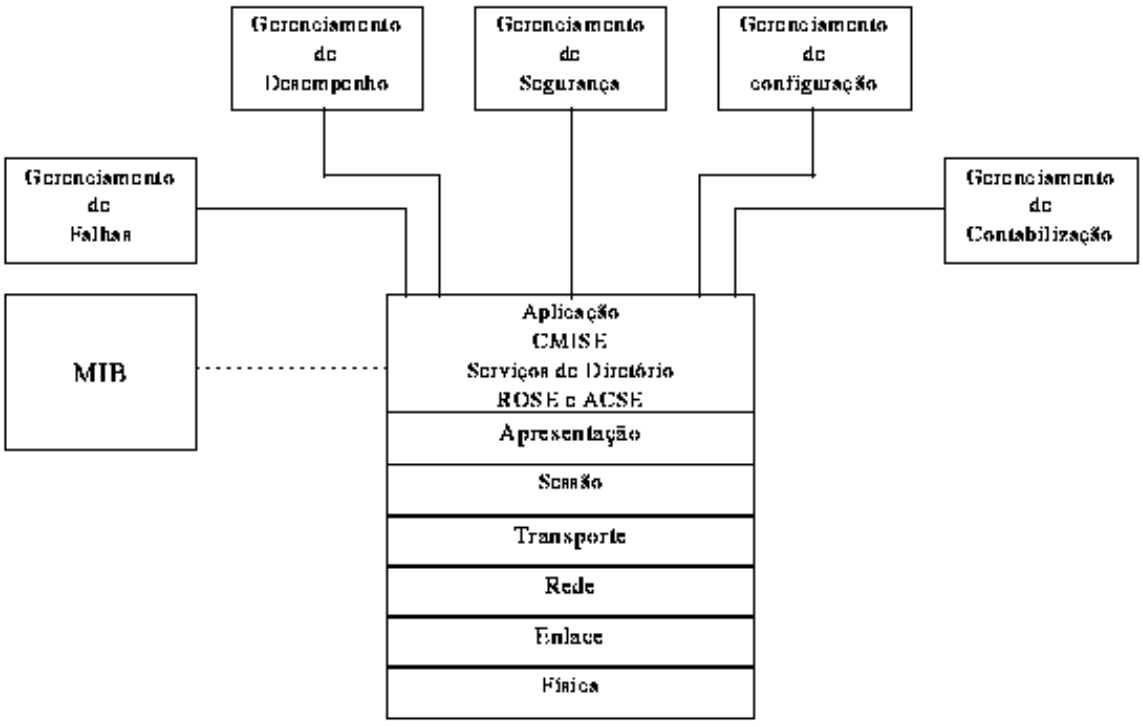


Figura 12 - Áreas funcionais do gerenciamento OSI

- Atributos para Representação de Relacionamento (*ARR - Attributes for Representing Relationship*) - ISO10164-3 - Um relacionamento é um conjunto de regras que são usadas para descrever como uma operação realizada numa parte de um sistema aberto poderá afetar alguma outra parte deste sistema. Um relacionamento existe entre dois objetos gerenciados quando uma operação executada em um deles afeta uma operação executada no outro. Para que este relacionamento seja reconhecido no modelo OSI, devem ser conhecidas informações suficientes de gerenciamento, que permitam ao Usuário do Serviço de Informação de Gerenciamento identificar quais são os objetos gerenciados envolvidos, e quais as regras que governam as suas interações.

A partir de modelos e conceitos definidos no padrão da ISO, foram definidos os seguintes atributos de relacionamento: objeto provedor, objeto usuário, atributo par, primário, secundário, identificação da instância de objeto Backup, identificação da instância de objeto Backed-up, membro, proprietário e grupo de atributos de relacionamento.

- Função de relatório de alarme (*ARF - Alarm Report Function*) - ISO10164-4 - Tem como objetivo fornecer informações que permitam ao gerente atuar sobre as condições operacionais e a qualidade do serviço de um sistema gerenciado. Devem ser definidos critérios para identificar um mal funcionamento no sistema gerenciado, em função da ocorrência de falhas, que permitam avaliar qual o grau de mal funcionamento do recurso. O nível de severidade do alarme é avaliado em função do nível de degradação que este irá provocar na qualidade do serviço oferecido ao usuário deste sistema, ou pelo estado da capacidade de uso de um determinado objeto gerenciado.

Podemos ter diversos níveis de severidade de alarme, deste um nível de alerta que não provoca nenhuma degradação sobre o serviço prestado ao usuário, até um alarme crítico que diz que o serviço não pode mais ser fornecido ao usuário.

- Função de Gerenciamento de Relatório de Evento (*ERMF - Event Report Management Function*) - ISO10164-5 - A função de gerenciamento de Relatório de Evento tem como objetivos:
    - Definir um serviço para o controle de relatórios de eventos que permita selecionar quais relatórios devem ser enviados para um sistema de gerenciamento particular;
    - Definir quais devem ser os destinos dos relatórios de eventos gerados;
    - Definir um mecanismo de transmissão de relatórios que permita o controle sobre o repasse destes relatórios;
    - Possibilitar que um sistema de gerenciamento externo altere as condições usadas para emitir os relatórios;
    - Definir endereços secundários (usados para *back-up*) aos quais enviamos os relatórios de eventos, caso o endereço primário não esteja disponível.
- Função para o controle de Log (*LCF - Log Control Function*) - ISO10164-6 - O objetivo de função de controle de log (um repositório de dados que contém registros com informações que devem ser preservadas) é o de permitir as demais funções de gerenciamento, preservar informações sobre os eventos que ocorreram, ou sobre as operações executadas nos objetos gerenciados. Uma vez que estas informações

podem mudar, a função de controle de log deve satisfazer as seguintes características:

- O Controle de Log deve ser flexível para permitir a seleção de quais registros do log devem ser preservados pelo sistema de gerenciamento;
- Deve permitir que um sistema externo altere os critérios usados na preservação dos registros;
- Deve permitir a um sistema externo saber se foi alterada alguma característica de preservação, ou se um registro foi perdido;
- Definir mecanismos para controlar o tempo durante o qual devem ser realizadas as atividades de preservação das informações;
- Deve permitir que um sistema externo recupere e elimine os registros em um log, como também criar e eliminar logs.

- Função de Relatório de Alarme de Segurança (*SARF - Security Alarm Reporting Function*) - ISO10164-7- É a função de gerenciamento do sistema pela qual um usuário do gerenciamento de segurança recebe as notificações sobre os eventos relacionados a segurança da rede. Este usuário deve saber quais as operações que falharam (*miss operations*) nos serviços e mecanismos de segurança, os atentados (*attacks*), e as violações (*breaches*) a esta segurança, quando estes atentados foram detectadas pelos mecanismos de segurança, além de outros processamentos relacionados com a segurança do sistema. Deve-se também notificar ao usuário a gravidade das operações erradas, dos atentados e violações na segurança do sistema.
- Função de Registro para Auditoria de Segurança (*SATF - Security Audit Trail Function)* - ISO10164-8 - O usuário do gerenciamento de segurança usa esta função para gravar todos os eventos potenciais relacionados à segurança no seu domínio de gerenciamento. Estas informações são gravadas num objeto de log de auditoria de segurança (*security audit log*). Através de uma comparação com utilização planejada do sistema de gerenciamento e a utilização real gravada neste log, o usuário pode saber qual é o grau de atendimento dos requisitos definidos pela política de segurança.

Uma análise ou auditoria dos relatórios de alarmes de segurança possibilita que o usuário detecte desvios no uso das normas da política de segurança, e correlacione estes desvios com os alarmes de segurança de menor severidade, ou com qualquer outro evento normal, para descobrir quais são os pontos vulneráveis ou quais partes do mecanismo de segurança que estão funcionando precariamente.

Para a execução desta auditoria, é necessário que estejam no log todos os eventos relativos à segurança como: as conexões, as desconexões, todos os eventos relativos à utilização dos mecanismos de segurança, as próprias operações para gerenciamento da rede, e a contabilização da utilização de cada recurso gerenciado. O log pode ser local, em que os registros podem ser recuperados por um gerente, ou remoto, em que enviamos os registros ao gerente sempre que eventos relativos à segurança ocorrem.

Resumidamente, o usuário do gerenciamento de segurança, precisa ter a capacidade de controle dos mecanismos de auditoria de segurança em relação a sua operação, e na escolha dos eventos de interesse do sistema que devem ser auditados, para que seja possível perceber atentados contra a segurança, ou problemas ao se concretizar qual deve ser a política de segurança a ser adotada.

- Função de Registro para Controle de Acesso ou Função de Controle de Acesso (*OAAC - Objects and Attributes for Access Control*) - ISO10164-9 - O modelo de controle de acesso faz parte do gerenciamento dos mecanismos de segurança descritos na arquitetura de segurança do modelo OSI. Este controle de acesso aos objetos envolvidos na gerência da arquitetura OSI, é uma interpretação do modelo básico usado pelas aplicações de gerenciamento. No contexto do gerenciamento da segurança do sistema, pode permitir ao administrador de um domínio prevenir-se de acessos não autorizados aos recursos. Para isso, são disponibilizados mecanismos para controle do acesso, para que somente usuários autorizados possam ter acesso a um recurso de gerenciamento específico. Deve-se também evitar o envio das notificações a destinatários não-autorizados, impedir o acesso às operações de gerenciamento por entidades que não sejam autorizadas, e proteger as informações de gerenciamento contra sua divulgação indesejável.
- Função de Medida de Contabilização (*AMF - Accounting Metering Function*) - ISO10164-10 - Define os mecanismos necessários para a coleta de informações sobre a utilização dos recursos no ambiente OSIE (*Open System Interconnection Environment*), uma representação para que estas informações sejam armazenadas de maneira adequada, e associar tarifas as medidas de utilização de cada um dos recursos gerenciados. Definem-se objetos de dados e de controle de medida de contabilização. Podem-se realizar operações sobre as instâncias destes objetos para se obter informações sobre a utilização de um recurso, iniciar, retomar e suspender as medidas de contabilização do uso do recurso, e também manter um registro dessa medida.
- Função de Monitoração de Carga de Trabalho (*WMF - Workload Monitoring Function*) - ISO10164-11 - O seu objetivo é a avaliação da demanda necessária de um recurso e a real utilização de um dado recurso do OSIE, além da avaliação da eficiência das atividades de comunicação. Deve incluir as seguintes funções:
    - Obtenção de informações estatísticas;
    - Manutenção e análise dos registros do histórico do sistema;
    - Determinação do desempenho do sistema sob condições naturais e artificiais;
    - Alteração do modo de operação do sistema, com objetivo de realizar atividades referentes ao gerenciamento do seu desempenho.
- Função de Gerenciamento de Teste (*TMF - Test Management Function*) - ISO10164-12 - Objetiva satisfazer o controle remoto de testes, além de estabelecer a estrutura básica dos testes a serem realizados sobre os recursos gerenciados. A necessidade de execução de operações de teste pode ser necessária em diferentes áreas funcionais.

▶ Um teste é uma operação de monitoração de um sistema aberto (ou parte deste sistema aberto), num ambiente de gerenciamento que permita obter informações sobre a funcionalidade e/ou desempenho dos sistemas que são sujeitos aos testes.

▶ O teste necessita da criação de um ambiente de teste, de uma operação de teste, e finalmente, o retorno ao ambiente normal após a execução do teste.

O objetivo de uma operação de teste é o de monitorar e controlar um sistema. O controle inclui atividades como a suspensão, a reinicialização ou o término do teste. Deve-se identificar cada um dos testes univocamente. Pode-se realizar os testes de

acordo com uma programação que pode ter tanto testes periódicos, quanto esporádicos. Podem-se combinar testes simples para criarem-se testes complexos. Em alguns casos, pode ser necessária a execução de um conjunto de testes particulares para alguma necessidade específica, e logo após o término do teste, devem-se correlacionar os resultados de cada teste, para a formulação do resultado final.

- Função de Sumarização (*SF - Summarization Function*) - ISO10164-13 - Este função é usada para obter informações a partir de observações relativas a múltiplos objetos gerenciados. Para isso, deve-se incluir os relatórios de eventos, e o escalonamento das observações ao se especificar as funções. São definidos métodos para a observação e o relato de valores dos atributos dos objetos gerenciados, determinados métodos para o relato de estatísticas com base em diversos valores de atributos, sendo que cada um destes foi observado em um mesmo instante. Os valores dos atributos e as estatísticas fornecem uma informação sumarizada do conjunto de objetos gerenciados e seus atributos, em um ou mais intervalos de tempo distintos. Como conseqüência, as estatísticas são calculadas em função do conjunto de objetos gerenciados e não em relação ao tempo.

Em resumo, ela suporta a habilidade para agregar os valores de atributos observados e/ou disponibilizar informações estatísticas sobre estes valores de atributo.

6.5.1 - Gerência de Configuração

O objetivo da gerência de configuração é o de permitir a preparação, iniciação, partida, a operação contínua, e a posterior suspensão dos serviços de interconexão entre os sistemas abertos, tendo então, a função de manutenção e monitoração da estrutura física e lógica de uma rede, incluindo a verificação da existência dos componentes, e a verificação da interconectividade entre estes componentes.

A gerência de configuração, portanto, é correspondente a um conjunto de facilidades que permitem controlar os objetos gerenciados, identificá-los, coletar e disponibilizar dados sobre estes objetos para as seguintes funções:

- Atribuição de valores iniciais aos parâmetros de um sistema aberto;
- Início e encerramento das operações sobre objetos gerenciados;
- Alteração da configuração do sistema aberto;
- Associação de nomes a conjuntos de objetos gerenciados.

6.5.2 - Gerência de Desempenho

Na gerência de desempenho, temos a possibilidade de avaliar o comportamento dos recursos num ambiente de gerenciamento OSI para verificar se este comportamento é eficiente, ou seja, preocupa-se com o desempenho corrente da rede, através de parâmetros estatísticos como atrasos, vazão, disponibilidade, e o número de retransmissões realizadas.

O gerenciamento de desempenho é um conjunto de funções responsáveis pela manutenção e exame dos registros que contém o histórico dos estados de um sistema, com o objetivo de serem usados na análise das tendências do uso dos componentes, e para definir um planejamento do sistema através do dimensionamento dos recursos que devem ser alocados para o sistema, com o objetivo de atender aos requisitos dos usuários deste sistema, para satisfazer a demanda de seus usuários, ou seja, garantir que não ocorram insuficiências de recursos quando sua utilização se aproximar da capacidade total do sistema.

Para atingir estes objetivos, deve-se monitorar taxa de utilização dos recursos, a taxa em que estes recursos são pedidos, e a taxa em que os pedidos a um recurso são rejeitados. Para cada tipo de monitoração, definimos um valor máximo aceitável (*threshold*), um valor de alerta, e um valor em que se remove a situação de alerta. Definem-se três modelos para atender aos requisitos de monitoração do uso dos recursos do sistema:

- Modelo de Utilização: Provê a monitoração do uso instantâneo de um recurso;
- Modelo de Taxa de Rejeição: Provê a monitoração da rejeição de um pedido de um serviço;
- Modelo de Taxa de Pedido de Recursos: Provê a monitoração dos pedidos do uso de recursos.

6.5.3 - Gerência de Falhas

A gerência de falhas tem a responsabilidade de monitorar os estados dos recursos, da manutenção de cada um dos objetos gerenciados, e pelas decisões que devem ser tomadas para restabelecer as unidades do sistema que venham a dar problemas. As informações que são coletadas sobre os vários recursos da rede podem ser usadas em conjunto com um mapa desta rede, para indicar quais elementos estão funcionando, quais estão em mau funcionamento, e quais não estão funcionando. Opcionalmente, pode-se aqui gerar um registro das ocorrências na rede, um diagnóstico das falhas ocorridas, e uma relação dos resultados deste diagnóstico com as ações posteriores a serem tomadas para o reparo dos objetos que geraram as falhas.

O ideal é que as falhas que possam vir a ocorrer em um sistema sejam detectadas antes que os efeitos significativos decorrentes desta falha sejam percebidos. Pode-se conseguir este ideal através da monitoração das taxas de erro do sistema, e da evolução do nível de severidade gerado pelos alarmes (função de relatório de alarme), que permite emitirmos as notificações de alarme ao gerente, que pode definir as ações necessárias para corrigir o problema e evitar as situações mais críticas.

6.5.4 - Gerência de Contabilidade

A gerência de Contabilidade provê meios para se medir e coletar informações a respeito da utilização dos recursos e serviços de uma rede, para podermos saber qual

a taxa de uso destes recursos, para garantir que os dados estejam sempre disponíveis quando forem necessários ao sistema de gerenciamento, ou durante a fase de coleta, ou em qualquer outra fase posterior a esta. Deve existir um padrão para obtenção e para a representação das informações de contabilização, e para permitir a interoperabilidade entre os serviços do protocolo OSI.

A função de contabilização deve ser genérica para que cada aplicação trate os dados coerentemente de acordo com as suas necessidades. Estas funções podem ser usadas para várias finalidades como tarifas sobre serviços prestados, controle de consumo dos usuários, etc. É implementada através de objetos gerenciados especiais associados à contabilização (a utilização dos recursos ligados a estes objetos que representam as características de um dado recurso monitorado) chamados de "Objetos Contabilizados". Existem dois tipos de objetos:

- Objetos de Controle de Medida de Contabilização;
- Objetos de Dados de Medida de Contabilização.

Os **Objetos de Controle de Medida de Contabilização** permitem que o sistema ao coletar as informações sobre o uso de um determinado recurso, selecione quais dados são relevantes, além de permitir que este sistema defina sobre quais circunstâncias deve ser realizada a coleta. Este controle irá definir quais eventos são gerados ao se atualizar e notificar as informações sobre o uso de um recurso. Apresenta uma visão genérica de gerenciamento, para ser particularizada para a contabilização de recursos específicos, além de usar os pacotes especificados num controle de medida, para incorporar as funcionalidades necessárias a contabilização. Alguns tipos de eventos que podem ocorrer são:

- Escalonamento por períodos de tempo;
- Ações de controle do próprio sistema de gerenciamento;
- Estímulos provenientes da mudança de valores dos atributos.

Os **Objetos de Dados de Medida de Contabilização** são usados para representar um recurso usado por um usuário, contendo informações como: qual é o usuário do recurso, qual a unidade de medida usada na contabilização, qual a quantidade consumida, etc. Estas informações podem ser obtidas através de um GET para a obter os valores dos atributos dos dados de medida, ou através do uso de parâmetros nas notificações enviadas pela gerência de contabilização. Novamente são definidas apenas propriedades genéricas que podem ser especializadas conforme a necessidade.

Os objetos de dados de medida só podem ser criados se existir uma instância de um objeto de controle de medida para controlá-lo. Um objeto de controle de medida só pode ser destruído quando todos os objetos de dados de medida controlados por este objeto forem também destruídos. Uma instância de um objeto de controle de medida pode controlar várias instâncias de objetos de dados de medida. Deve-se sempre ter pelo menos uma instância do objeto de dados na memória que seja responsável por monitorar um objeto contabilizado, para que possamos enviar solicitações sobre seu uso.

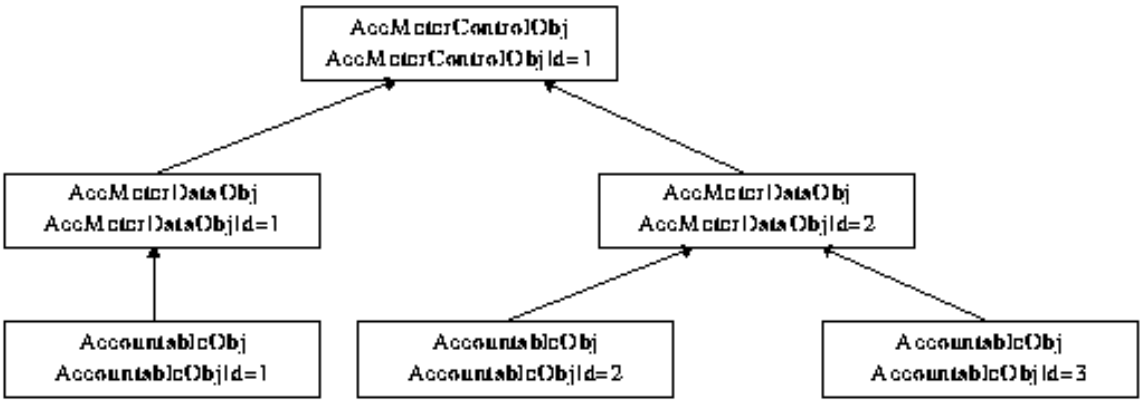


Figura 13 - Relacionamento entre objetos gerenciados

A figura anterior mostra o relacionamento entre os objetos de controle de medida, os objetos de dados de medida e os objetos contabilizados. Nela, pode-se notar que os objetos de controle de medida (AccMeterControlObj) referenciam os objetos de dados de medida que controlam (AccMeterDataObj). Cada um dos objetos de dados de medida contém uma referência a uma instância do objeto contabilizado, em que realizamos as coletas das informações de contabilização.

Ao implementar-se a função de gerência de contabilização, devem-se considerar os seguintes aspectos:

- Controlar o registro e a emissão dos dados relacionados a contabilização através dos objetos de controle de medida de contabilização;
- Coletar os dados de contabilização, usando os objetos de dados de medida de contabilização para representar os recursos contabilizados;
- Armazenar os resultados da contabilização para criar históricos de contabilização dos recursos através do uso de registros de contabilização.

6.5.5 - Gerência de Segurança

O objetivo do gerenciamento de segurança é o de dar subsídios à aplicação de políticas de segurança, que são os aspectos essências para que uma rede baseada no modelo OSI seja operada corretamente, protegendo os objetos gerenciados e o sistema de acessos indevidos de intrusos. Deve providenciar um alarme ao gerente da rede sempre que se detectarem eventos relativos à segurança do sistema. São distinguidos dois conceitos no modelo OSI em relação a segurança: Arquitetura de Segurança do Modelo OSI e funções de Gerenciamento de Segurança, estas compondo a área funcional de gerência de segurança.

O objetivo da Arquitetura de Segurança do modelo OSI é o de dar uma descrição geral dos serviços de segurança e dos mecanismos associados a este, e de definir em que posição do modelo de referência situa-se os serviços de segurança e os seus mecanismos associados. A norma de referência da Arquitetura de Segurança trata exclusivamente da segurança dos canais de comunicação, através de mecanismos como a criptografia, a assinatura numérica, e a notarização, que permite

aos sistemas que usam este canal se comunicarem de forma segura. Para isso, definem-se os seguintes serviços:

1. Autenticação tanto de entidades pares quanto da origem dos dados (*authentication*);
2. Controle de acesso aos recursos da rede (*access control*);
3. Confidencialidade dos dados (*confidenciality*);
4. Integridade dos dados (*integrity*);
5. A não-rejeição ou não-repudiação (*non-repudiation*);

Os mecanismos a serem adotados dependem do uso de uma política de segurança, que é feita pelo uso das Funções de Segurança do Gerenciamento de Redes OSI. Estas funções tratam do controle dos serviços de segurança do modelo OSI, e dos mecanismos e informações necessárias para se prestar estes serviços. Então, os objetivos do gerenciamento de segurança são:

- O fornecimento de relatórios de eventos relativos à segurança e o fornecimento de informações estatísticas;
- A manutenção e análise dos registros de histórico relativos à segurança;
- A seleção dos parâmetros dos serviços de segurança;
- A alteração, em relação a segurança, do modo de operação do sistema aberto, pela ativação e desativação dos serviços de segurança.

Para que estes objetivos sejam atingidos, devem-se olhar as diferentes políticas de segurança a serem adotadas no sistema aberto. Todas as entidades que seguem uma mesma política de segurança pertencem ao mesmo domínio de segurança. Devido ao gerenciamento necessitar distribuir as informações de gerenciamento de segurança entre todas as atividades que se relacionam com a segurança, os protocolos de gerenciamento assim como os canais de comunicação devem ser protegidos, usando os mecanismos previstos na arquitetura de segurança.

As informações de gerenciamento de segurança são armazenadas numa MIB especial que deve dar apoio as três categorias de atividades de gerenciamento de segurança existentes. Esta MIB é chamada de SMIB (*Security Management Information Base*).

6.6 - A Plataforma OSIMIS

OSIMIS é uma plataforma de gerência orientada a objetos e desenvolvida principalmente na linguagem C++. Através do encapsulamento dos detalhes existentes no acesso aos serviços de gerenciamento, ela fornece um ambiente para o desenvolvimento de aplicações com uma interface orientada a objetos, o que permite aos desenvolvedores se preocuparem com a construção da aplicação, ao invés dos detalhes necessários para se acessar um serviço/protocolo de gerência. Usa o modelo OSI gerente-agente e os objetos gerenciados para abstrair os recursos reais. Não há nenhuma restrição para que aplicação desempenhe os dois papéis ao mesmo tempo (de agente e gerente).

A plataforma OSIMIS originou-se dos resultados obtidos das pesquisas voltadas para a área de gerenciamento de sistemas de comunicações e de sistemas distribuídos. Novos recursos vêm sendo acrescentados à arquitetura, para que seja

mais genérica possível na implementação das facilidades oferecidas pelo modelo OSI de gerência. A versão 4.0 permite a fácil integração entre sistemas (inclusive os proprietários) devido aos diferentes modelos e facilidades de gerência que apresenta. Nesta versão existe uma aplicação que permite a coexistência entre os modelos OSIMIS (CMIS/P) e *Internet* (SNMPv1). Originalmente, a plataforma foi designada para usar o ISODE (ISO Development Environment), mas já existem trabalhos para migrá-la para outras interfaces como a XOpen. Os serviços e aplicações que esta plataforma disponibiliza são:

- Implementação completa dos serviços CMIS e do protocolo CMIP;
- Agente OSI que realiza todas as funções especificadas no modelo de gerência;
- Objetos padrões;
- Bibliotecas de classes C++ para determinados tipos de atributos, com os respectivos codificadores e decodificadores para as suas sintaxes;
- Uso de um objeto coordenador (*coordinator*) que gerência todo o processo de comunicação do sistema;
- Métodos genéricos de interação entre o objeto coordenador e os objetos gerenciados, através dos objetos chamados de fontes de conhecimento (*knowledge sources*);
- Compilador para a linguagem formal de especificação dos objetos de gerência OSI (*GDMO - Guidelines for the Definition of Management Objects*);
- Interface de alto nível para os desenvolvedores de aplicações gerentes (RMIB e SMIB);
- Mecanismo de transparência à localização de agentes, utilizando a implementação ISODE do serviço de diretório OSI;
- Aplicação genérica de passarela (*gateways*) entre os modelos de gerência OSI (CMIS/P) e *Internet* (SNMPv1).

Este modelo fornece uma implementação completa dos serviços e protocolos comuns do modelo OSI, permitindo ou usar a especificação completa do protocolo, ou uma versão mais leve deste. Fornece um suporte suplementar para o ISODE, que permite codificar, decodificar e analisar as cadeias de caracteres na especificação ASN.1. O OSIMIS oferece uma interface de alto nível chamada RMIB, que oferece os seguintes serviços aos desenvolvedores:

- Estabelecimento e liberação de associações;
- Uso de nomes mais informais ao invés dos identificadores de objetos;
- Manipulação transparente de estruturas ASN.1;
- Listas de respostas (*linked lists*);
- Interface de alto nível para os relatórios de eventos;
- Tratamento de erros em diferentes níveis.

Na plataforma OSIMIS é oferecido suporte para organizar os processos dirigidos por eventos, para facilitar a integração com outros mecanismos de coordenação, como as interfaces gráficas dos usuários, que devem tratar dos eventos que ocorrem. As aplicações que realizam o papel de gerenciadoras interagem com os agentes que cuidam de determinados objetos gerenciados, utilizando apenas o título e as classes dos objetos gerenciados. Isso é possível através da transparência de localização que neste caso, tem a função de identificar para a aplicação, quais são os agentes que possuem os objetos gerenciados associados a determinados recursos,

assim como deve localizar este agente para a aplicação. A transparência de localização é realizada através do serviço de diretório OSI que armazena as informações de forma hierárquica e distribuída, sendo ideal para o armazenamento das informações necessárias as aplicações gerentes, e para a localização dos agentes. Para armazenarmos as informações necessárias as aplicações gerentes, usamos o mecanismo DSA/DUA (*Directory Service Agent/Directory User Agent*) que permite as aplicações informarem a sua existência e os serviços que a aplicação disponibiliza aos seus usuários. Essas aplicações devem notificar ao DSA/DUA quando terminarem. Esse mecanismo funciona da seguinte forma: Ao iniciar a operação, cada agente e cada aplicação gerenciadora se cadastra na árvore de informação de diretório (*DIT-Directory Information Tree*), como mostra o passo S na figura. Quando a aplicação de gerência deseja acessar um recurso, ela executa os seguintes passos: Obter o nome do agente que gerencia a MIB que tem os objetos que representam o recurso requerido (passo 1); Obter o endereço de apresentação em que o agente está em execução (passo 2); Associação com o agente que esta identificou (passo 3).

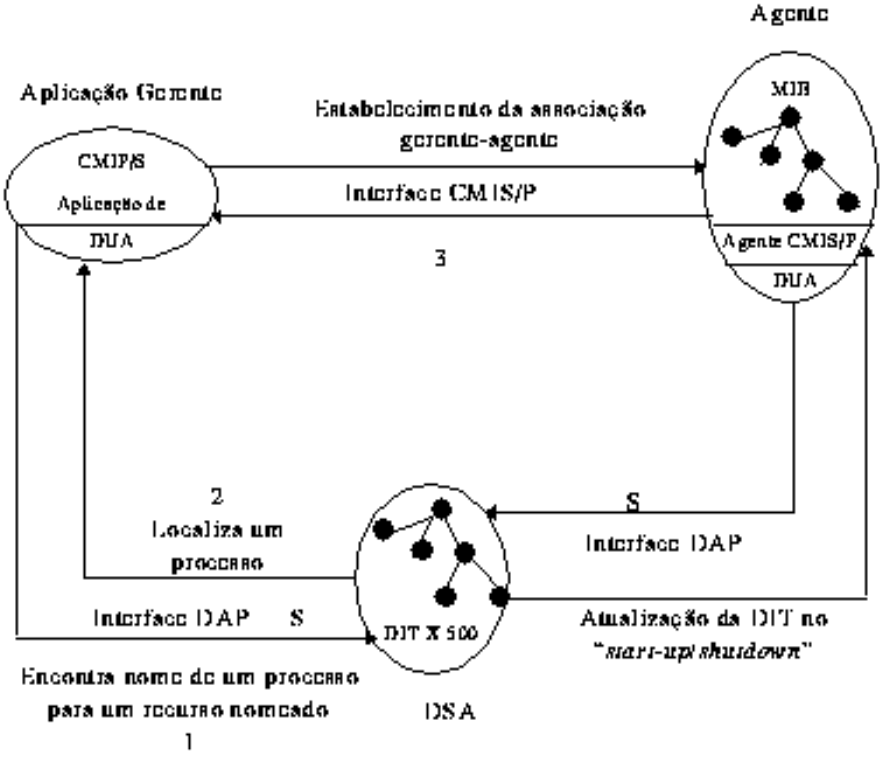


Figura 14 - Mecanismo de transparência de localização

Além destas facilidades, a OSIMIS apresenta algumas outras, como um compilador GDMO para construção de classes de objetos gerenciados, mecanismo de transparência na localização de objetos gerenciados, através do uso do serviço de diretório X.500, implementação do protocolo SNMP ao nível de aplicação através do uso da coexistência entre os dois protocolos, conjunto de aplicações genéricas e

agentes específicos para a camada de transporte OSI e para a versão OSI da MIB da camada TCP/IP.

6.6.1 – A plataforma OSIMIS e os protocolos CMIP e SNMP

Devido ao protocolo padrão de gerência de rede mais utilizado ser o SNMP, a plataforma OSIMIS apresenta um modelo de conversão entre as duas plataformas, que deve prover mecanismos capazes de permitir a existência mútua destas duas plataformas em um ambiente de gerenciamento de redes. As principais restrições funcionais necessárias a esta coexistência são:

- Tradução da MIB SNMP em GDMO;
- Conversão das operações SNMP em operações CMIP;
- Redução do tráfego de informações de gerência decorrente do processo de "*polling*" do SNMP através do modelo OSI de notificações.

A coexistência é realizada através de uma aplicação de passarela, que tem a função de um agente OSI na camada superior e gerente SNMP na camada inferior. Usa as facilidades apresentadas pelo GMS (*Generic Management System*) para suportar todas as funções realizadas por um agente OSI, e usa os objetos especializados do GMS e os gerentes SNMP para realizarem juntos a conversão das informações de gerenciamento. A técnica adotada para a coexistência nada mais é do que a definição de um conjunto genérico de regras de conversão entre os dois modelos, e o uso de um processo de aplicação capaz de operar sobre qualquer MIB. Para isso, é necessário um conversor de objetos SMI SNMP para objetos GDMO OSI, além de um compilador GDMO para compilar os objetos convertidos.

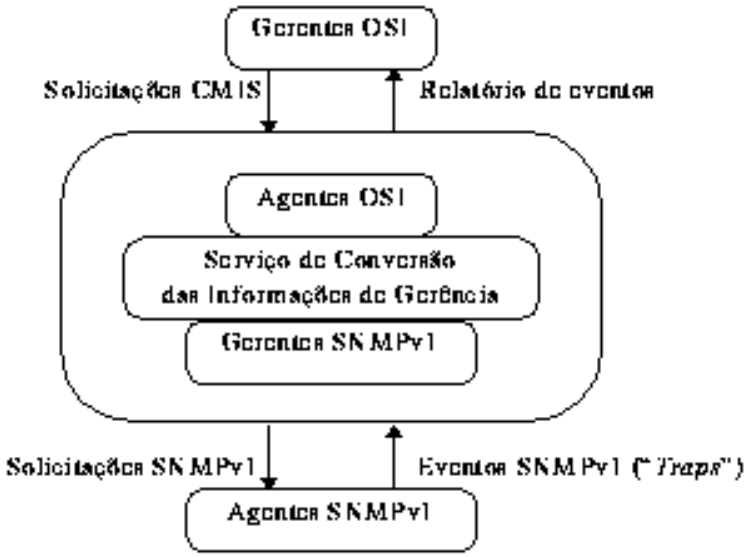


Figura 15 - Arquitetura de passarela entre protocolos CMIP e SNMPv1

6.6.2 - Plataforma OSIMIS e orientação a eventos

Para implementar o mecanismo assíncrono da orientação a eventos, a plataforma OSIMIS apresenta dois objetos especiais: o Coordenador (*coordinator*) e as Fontes de Conhecimento (*Knowledge Sources*), que fornecem abstrações especiais na implementação deste mecanismo.

O Objeto Coordenador é um centralizador dos eventos externos, além de tratar das chamadas dos temporizadores. Só existe uma instância deste objeto no sistema. Também é usado para implementar os mecanismos de iteração entre os objetos gerenciados e os recursos que representam, através de um comando CMIS GET. São possíveis três mecanismos:

1. Acesso por demanda de aplicações gerentes;
2. Acesso por *polling*;
3. Acesso por eventos assíncronos.

Os Objetos Fontes de Conhecimento são usados para ativar, em tempo real, os objetos gerenciados quando ocorrerem eventos externos. São os pontos de comunicação externos onde ocorrem os eventos. Nas aplicações gerentes, obtêm-se com estes as informações sobre os recursos gerenciados. Também podem gerenciar o *polling* para acessar os objetos gerenciados. Ao contrário do objeto anterior, podemos ter várias instâncias deste objeto.

6.6.3 - Sistema Genérico para gerenciamento

É implementado através de uma interface para o desenvolvimento de aplicações, que oculta totalmente os detalhes necessários para se usar os serviços oferecidos pelo CMIS para endereçar objetos, o escopo dos níveis de hierarquia, a filtragem dos atributos dos objetos, e as correções de erro. A facilidade para o desenvolvimento de aplicações apresentadas pela interface é devido ao uso de duas classes de objetos: MO e MOClassInfo.

A classe MO é a classe raiz da hierarquia das classes de objetos gerenciados, e possui métodos e atributos que automatizam os acessos as informações usando o protocolo CMIP, além de conter informações sobre as posições dos objetos gerenciados na árvore de informação de gerenciamento (MIT).

A classe MOClassInfo apresenta informações comuns a todos os objetos pertencentes a uma classe, permitindo criar uma instância deste objeto através da alocação dinâmica, além de poder definirmos valores default para alguns dos atributos deste objeto.

6.6.4 - Interfaces para construção de processos gerentes

São API's (*Aplication Programs Interfaces*), amigáveis para o acesso eficiente a objetos MIB remotos, o que facilita a construção de processos gerentes. São interfaces implementadas em OSIMIS, portanto orientadas a objetos, para acesso aos serviços CMIS. Usam-se dois enfoques distintos:

- ***Remote MIB (RMIB)*** apresenta uma abstração no acesso a MIB's Remotas, através do uso da noção de um objeto de associação, que é usado para encapsular uma operação de gerenciamento com um objeto remoto, obscurecendo então, os serviços usados do protocolo CMIP assim como o acesso a MIT remota.
- ***Shadow MIB (SMIB)*** abstrai os objetos gerenciados num espaço de endereçamento local, possibilitando a total transparência do uso do protocolo de gerenciamento. Parâmetros de gerenciamento podem ser substituídos por ponteiros.

Capítulo 7 - Distribuição da Gerência na Rede

Com o crescimento das redes de computadores, em tamanho e complexidade, sistemas de gerência baseados em um único gerente responsáveis por todas as funções de gerenciamento são inapropriados, devido ao volume das informações que devem ser tratadas e que podem pertencer a localizações geograficamente distantes do gerente.

Desta forma, evidencia-se a necessidade da distribuição da gerência na rede, através da divisão das responsabilidades gerenciais entre gerentes locais que controlem domínios distintos e da expansão das funcionalidades dos agentes.

7.1 – Centros de operação de rede

Cada gerente local de um domínio pode prover acesso a um gerente responsável (pessoa que interage com o sistema de gerenciamento) local e/ou ser automatizado para executar funções delegadas por um gerente de mais alto nível, geralmente denominado de Centro de Operações da Rede (*NOC - Network Operation Center*). O NOC é responsável por gerenciar os aspectos interdomínios, tal como um enlace que envolva vários domínios, ou aspectos específicos de um domínio, devido à inexistência de gerente local. Os tipos mais básicos de tarefas de gerenciamento de uma rede são as funções de monitoramento e controle.

A monitoração consiste na observação periódica de objetos gerenciados importantes para a política de gerenciamento. A partir da monitoração, o gerente tem conhecimento do estado da rede e, desta forma, pode efetuar operações de controle sobre a mesma. A distribuição das funções de monitoração é mais premente em relação às funções de controle, pois a monitoração consome mais recursos da rede, bem como a atenção do gerente, pois através dela é que se obtém o estado da rede em relação ao tempo, enquanto que as funções de controle são invocadas em menor número, geralmente com objetivos de alteração de configuração e erradicação de problemas.

Os modelos de gerência diferenciam-se nos aspectos organizacionais envolvendo a disposição dos gerentes na rede, bem como no grau da distribuição das funções de gerência.

7.2 - Modelo Internet

O modelo inicial de gerência Internet concentra as funções de controle e monitoração em um único gerente responsável pelo acesso aos diversos agentes da rede. Os agentes são simples fornecedores das variáveis da MIB, enquanto que o gerente, através do mecanismo de *polling*, monitora a rede, efetuando, quando necessário, operações de controle. Não é definido nenhum mecanismo para a comunicação entre gerentes. Tal abordagem objetiva a simplificação dos agentes, permitindo o rápido desenvolvimento destes e a minimização dos recursos usados nos

elementos de rede. Contudo o gerente é sobrecarregado com todas as funções, gerando grande tráfego na rede e degradando o tempo de resposta aos eventos da rede.

Com intuito de prover a monitoração remota em um ambiente de gerenciamento Internet, foi definida a MIB RMON (*Remote Network Monitoring*). Tal MIB permite que as funções de monitoração sejam realizadas através da captura dos pacotes que transitam por uma sub-rede sem a interferência constante do gerente. A RMON é composta por nove grupos: Statistics, History, Alarm, Host, HostTopN, Matrix, Filter, Packet Capture e Event.

1. O grupo Statistics mantém estatísticas das interfaces do agente, por exemplo, o número de colisões.
2. History armazena amostras de informações colhidas no grupo Statistics.
3. O grupo Alarm fornece mecanismos usados para a monitoração de variáveis de gerenciamento do tipo Integer, com valores-limites configurados que podem disparar eventos ao serem atingidos pelo valor monitorado.
4. O Host contêm informações referentes aos nodos da sub-rede, como o número de pacotes enviados por cada nodo.
5. O grupo HostTopN classifica as informações obtidas pelo grupo Host, gerando, por exemplo, os nodos que mais transmitiram pacotes.
6. O Matrix possui informações referente a comunicação entre dois nodos da sub-rede.
7. O Filter provê mecanismos de filtros para os pacotes recebidos da sub-rede, que podem disparar um evento ou um processo de armazenamento de pacotes.
8. Packet Capture armazena informações dos pacotes recebidos na sub-rede;
9. O Event controla a geração e notificação dos eventos definidos, por exemplo, um relativo a um alarme especificado no grupo Alarm.

Com o crescimento da rede Internet, foi proposta uma adaptação do modelo de gerência original baseado no protocolo SNMP. Tal proposta, denominada de SNMP 2.0, aumenta as funcionalidades dos agentes, através da flexibilização na geração de notificações assíncronas e da capacidade de um processo assumir ambas as funcionalidades de gerente e agente, permitindo a comunicação entre gerentes de níveis diferentes. O SNMP 2.0 adiciona dois tipos novos de operações no protocolo, *GetBulkRequest* e *InformRequest*, que permitem um aumento das funcionalidades dos agentes e gerentes intermediários. A GetBulkRequest otimiza a recuperação de um volume considerável de variáveis, principalmente em relação à recuperação de entradas de tabelas. Por exemplo, para a recuperação de 10 entradas de uma tabela é necessário o envio de 10 operações GetNextRequest no SNMP original, e com a versão 2.0, somente um GetBulkRequest é suficiente. A InformRequest permite um gerente enviar de forma assíncrona uma notificação de algum evento, sendo análogo ao TRAP, contudo é um serviço confirmado.

Dentro do contexto do SNMP 2.0 foi definida uma MIB, denominada de M2M, que suporta a distribuição de funções de monitoração entre os gerentes da rede. Tal monitoração é baseada em amostras realizadas em variáveis do tipo COUNTER, GAUGE e TIMETICKS de agentes. Os valores de tais atributos são comparados com valores-limites configurados, e caso sejam atingidos, um InformRequest ou um TRAP é enviado pelo gerente que implementa a MIB M2M a outro gerente.

A MIB é especificada a partir dos conceitos de alarme, evento e notificação. O alarme é uma condição configurada que é verificada periodicamente. Se um alarme for detectado, é disparado o evento associado, que por sua vez, pode gerar uma notificação para um gerente especificado. Tal MIB é análoga aos grupos Alarm e Event da RMON.

7.3 - Modelo OSI

O modelo OSI possibilita a delegação das funções de monitoração aos agentes, através da definição de um ambiente orientado a objetos que incorpora tais procedimentos e da abordagem orientada a notificações assíncronas do modelo. Contudo as funções de controle ainda ficam relegadas ao gerente, pois o conhecimento relativo à tomada de decisões gerenciais não se adapta para ser codificado em classes de objeto, ao contrário do conhecimento referente à monitoração, que é mais simples, geralmente estático e periódico.

Tal modelo gera agentes mais complexos de serem desenvolvidos, consumindo mais recursos dos elementos de rede, enquanto que economiza o uso da rede, devido a minimização dos pedidos de informações (*pollings*) necessários para obter dados sobre os objetos gerenciados, livrando o gerente para tarefas mais “inteligentes”.

Além da definição de um agente mais funcional, o modelo OSI introduz o conceito de hierarquia de gerentes, através da possibilidade de um mesmo processo de aplicação funcionar como gerente e agente, sendo denominado de gerente intermediário. Desta forma é possível ao NOC delegar tarefas para gerentes intermediários responsáveis por certos domínios da rede. A comunicação entre gerentes é realizada pelo acesso a objetos da MIB que possuem as informações que devem ser compartilhadas ou funcionalidades que devem ser delegadas entre os gerentes.

As funcionalidades que podem ser delegadas a um agente ou a um gerente intermediário são exemplificadas nas funções de gerenciamento definidas pelo ISO, que fornecem serviços padronizados para as cinco áreas funcionais de gerenciamento OSI: configuração da rede, falhas dos componentes, níveis de desempenho, segurança de acesso e contabilização do uso dos recursos. Tais funções são relativas, principalmente, à monitoração remota, como a monitoração de um atributo de um objeto que representa a utilização de um recurso, ou ao controle de algum mecanismo necessário para o gerenciamento, como o registro de logs. A seguir são exemplificadas algumas das funções de gerenciamento:

- **Função de gerenciamento de objeto**: especifica três tipos de notificações relativas à criação de objeto, remoção de objeto e mudança de valor de atributo. Nesse caso o gerente não precisaria ficar realizando *polings* para a verificação de tais condições, e sim, o objeto emitiria as notificações. Para tal, a classe do objeto monitorado deve importar as definições das notificações. Em tempo de execução, se o gerente quiser receber somente determinados tipos de notificações, por exemplo, relativa à criação de objetos, pode usar o objeto *eventForwardingDiscriminator* definido

na função de controle de relatórios, que repassa somente tipos de notificações configurados no objeto;

- **Função de relatório de alarmes**: define notificações genéricas de alarme referentes à falhas, fornecendo informações tais como o tipo da falha, causa provável e índice de gravidade. Os tipos de falhas variam desde problemas de comunicação, como perda de sinal, até alarmes cobrindo problemas ambientais, como umidade alta. Tal função possibilita grande autonomia aos elementos gerenciados, que notificarão de forma assíncrona o gerente na ocorrência de uma falha. Nesse caso, o gerente somente precisará verificar periodicamente a conectividade com o agente, e iniciar procedimentos de recuperação de falhas no recebimento de uma notificação. As classes de objetos que necessitam se autogerenciar devem importar a definição padrão da notificação de alarme. Também é definida uma estrutura de registro relativo ao gerenciamento. O mecanismo de registro de informações em um log é definido na função de controle de log, que define um objeto que seleciona as notificações que devem ser armazenadas localmente sobre forma de um objeto que representa um registro de log.

- **Função de monitoração de carga de trabalho**: define objetos métricos que realizam a monitoração de atributos de outros objetos dos tipos COUTER e GAUGE, que podem representar a utilização de um recurso, a taxa de requisição de um recurso ou a taxa de rejeição de acesso a um recurso. O objeto métrico pode enviar notificações quando o atributo monitorado atinge valores-limite pré-determinados. Além da análise pura do valor amostrado, são definidos também objetos que usam a média e a variância dos valores do atributo monitorado para a comparação com os valores-limite. Tal função permite a análise de desempenho de recursos gerenciados, sem a necessidade de consultas periódicas por parte do gerente.

7.4 - Gerência via Servidores Elásticos

A abordagem de gerência via servidores elásticos é realizada através da distribuição de programas independentes que encapsulam funções de controle e monitoração de objetos gerenciados. O termo elástico se refere à capacidade do servidor de alterar dinamicamente a sua funcionalidade, através da execução e remoção dos programas delegados. Um servidor elástico pode atuar como um agente ou como um gerente intermediário, sendo que cada programa delegado pode ser armazenado até que o gerente responsável invoque um comando de execução. As instâncias dos programas podem ser suspensas, reiniciadas ou finalizadas. Tais funções são realizadas através do protocolo de delegação.

Uma instância de um programa de gerenciamento pode se comunicar com o gerente criador, com outros programas, invocar funções de bibliotecas disponíveis no ambiente e acessar os objetos gerenciados. O acesso aos objetos gerenciados é realizado pelos Pontos de Controle de Observação, que representam uma interface genérica de acesso, desta forma escondendo os detalhes de implementação. Tal interface pode acessar diretamente os recursos gerenciados, possibilitar uma

conversão de protocolo, por exemplo, para o acesso a redes CMIP ou SNMP, e ainda possibilitar o acesso a outros servidores elásticos, através do protocolo de delegação. No último caso, evidencia-se a capacidade da definição de um gerenciamento composto por vários gerentes.

A abordagem via servidor elástico minimiza o tráfego na rede, bem como toma ações de forma mais rápida em relação aos eventos da rede. O servidor elástico é configurado somente para as funções realmente necessárias para cada momento dentro da política de gerenciamento da rede, ao contrário de agentes OSI ou Internet que podem permanecer atualizando objetos da MIB que não estão sendo usados.

Capítulo 8 - Segurança para Gerência de Redes

Neste capítulo é apresentado um levantamento dos riscos de segurança associados a Sistemas de Gerência de Redes e descreve uma Arquitetura de Segurança aplicável a tais sistemas, garantindo a autenticação, integridade e confiabilidade nas comunicações entre as entidades de gerência.

Os Protocolos de Gerência de Redes e os canais de comunicação que transportam informação de gerência são potencialmente vulneráveis a atentados contra a segurança. Cuidados particulares devem, portanto, ser tomados para assegurar que tais protocolos e informações estejam protegidos. A definição de vulnerabilidade e dos riscos de segurança dos Sistemas de Gerência e a criação de ferramentas para tratar estes problemas fazem parte do conjunto de ações fundamentais para o funcionamento confiável das redes. A especificação de ferramentas, seu comportamento e seus inter-relacionamentos compõem uma arquitetura de segurança.

8.1 - Segurança em Redes de Computadores

Existem diversos elementos sobre os quais podem incidir ameaças contra a segurança em um ambiente informatizado e, em especial, em um ambiente interligado por redes de computadores. Segurança em informática pode ser compreendido como a garantia ou confiança que os usuários tem em determinado sistema. Segurança aplicada no domínio das Redes de Computadores, então, deve garantir que o sistema não seja comprometido por ameaças cuja origem não esteja localizada, necessariamente, no computador local, mas remotamente. Existem muitas formas de comprometer sistemas porque normalmente existem muitos pontos expostos. Estes pontos de exposição podem ser classificados conforme estas seis categorias: hardware, software, informação/dados, pessoal, documentação e suprimentos.

No jargão de segurança, os itens que se enquadram nas categorias acima são chamados ativos. São os ativos de uma instalação que devem ser protegidos de ameaças porque é o comportamento apropriado destes ativos que vai permitir o funcionamento dos sistemas. Uma alteração, destruição, erro ou indisponibilidade de algum destes ativos pode gerar um comprometimento do sistema. Analisando os ativos apresentados no escopo de segurança em redes de computadores, apenas Hardware, Software e Informação/Dados são passíveis de serem protegidos por meios do que se convenciona chamar de Segurança Lógica, em contraposição à Segurança Física, onde esta última é a segurança tradicional de informática, centrada em restrições de acesso físico às instalações e equipamentos, prevenção de acidentes de trabalho e planos de recuperação de desastres como incêndios e inundações. Já a Segurança Lógica lança mão de software para garantir quatro princípios básicos: autenticação de usuário, disponibilidade de recursos, integridade das informações e confidencialidade das informações.

8.1.1 - Agressões e Falhas

Outra forma de analisar os problemas de segurança é fazer uma classificação das ameaças entre agressões e falhas. Falhas são acontecimentos acidentais que, de uma forma ou de outra, põem em risco a segurança das instalações e dos sistemas porque atentam contra a confiabilidade e/ou disponibilidade de um sistema. Exemplos de falhas são: inundações, incêndios, terremotos, roedores que atacam a fiação e provocam curtos-circuitos, acidentes ou erros humanos (derramamento de líquidos sobre equipamento, manipulação incorreta de equipamento, digitação de dados incorretos, etc) e falhas de hardware, de software e de comunicação. As agressões, por outro lado, são intencionais e hostis. São exemplos de agressões as ameaças de bombas, roubo, operação inadequada proposital de equipamentos, software propositadamente incorreto, vírus, invasões através de redes, (tentativas de) acesso a informações confidencias, etc. Não é possível abordar todos os problemas a partir do enfoque de Segurança Lógica. Os problemas relacionados às falhas dizem respeito a outros aspectos que não seja Segurança Lógica (manutenção e segurança física, por exemplo). Na lista de agressões também se encontram diversas ameaças que não são tratáveis por medidas de Segurança Lógica, como ameaças de bomba e roubo.

Então, sob esta ótica, as ameaças que dizem respeito à segurança em redes de computadores são agressões efetuadas por pessoas não autorizadas (as quais serão chamadas de *invasores*) que objetivam obter benefícios indevidos ou prejudicar o funcionamento dos sistemas.

8.1.2 - Acesso à Informação e à Capacidade de Processamento

O que está em “disputa” neste contexto de proteção de Sistemas em Rede pode ser resumido em dois itens: A informação em si: o acesso, a destruição e a modificação de informação e o acesso a serviços; e o acesso à capacidade de processamento de informação e ao equipamento: roubo de ciclos de máquina, acesso a serviços, redes e software, e uso da capacidade de armazenamento.

Por informação deseja-se representar muitas coisas: dados para processamento, tecnologia, know-how, conhecimento científico, informações econômico-financeiras, estratégicas e políticas, projetos, etc. Computadores podem manter informações confidenciais sobre pessoas, sobre objetivos militares, informações vitais para empresas ou governos, saldos bancários, e assim por diante. O valor destas e de outras informações é alto, apesar de ser muito difícil, na maioria dos casos estabelecer o valor intrínseco de determinada informação.

Desta forma, a capacidade de acesso à informação, bem como a capacidade de alterá-la ou destruí-la, representa então poder, que é protegido pelos legítimos detentores da mesma e que é buscado (de forma ilegítima) pelos invasores. O acesso ao hardware e ao software (e o decorrente acesso à capacidade de processamento) também representa poder, já que a utilização dos mesmos permite o processamento de informações. O acesso ilegítimo à capacidade de processamento pode ser apenas roubo de tempo de processamento, mas esse tipo de ato pode levar a conseqüências

sérias, como o aumento de custo para usuários legítimos ou, em caso extremo, a negação de serviço para os usuários legítimos, uma vez que a cpu e/ou memória estão ocupadas realizando tarefas estranhas à instalação. Um exemplo típico de roubo de tempo de cpu é a utilização de máquinas para decifrar informações criptografadas (como arquivos de senhas) para ter acesso a novas informações: uma agressão (roubo de ciclos) que alimentará outra agressão (a invasão de outros sistemas).

As agressões referentes à informação e à capacidade de processamento podem ser executadas basicamente de três formas: por escuta ou monitoração da rede, por invasão ao sistema e por mascaramento. A escuta/monitoração do canal é tarefa simples e mesmo com recursos pouco sofisticados é possível alcançar tal feito. Exemplos de formas de se conseguir monitoração de redes vão desde o uso de analisadores de protocolos (recurso caro) até a modificação do software de um computador comum para atuar como escuta. Existem ainda equipamentos próprios para escuta (passiva) que se valem de emanações eletromagnéticas dos cabos e conectores. O comprometimento da segurança de um nó intermediário em redes store-and-forward ou de gateways e roteadores leva à exposição de informações a terceiros. Então, toda informação que circula pelas redes pode ser interceptada e, se medidas de segurança não tiverem sido adotadas, esta informação se torna não confidencial. Pouco se pode fazer ao nível de software para impedir este tipo de agressão. O uso de criptografia deve ser considerado, pois, apesar de não impedir o ataque, é uma forma de reforçar o sigilo das comunicações.

A invasão de sistemas com o objetivo de ganhar acesso a informações e a recursos computacionais é uma das agressões mais comuns. As vulnerabilidades relativas à invasão de sistemas podem ser geradas de muitas formas. Por exemplo, pela não instalação de senhas por parte de usuários ou por falhas de implementação de softwares. Os riscos associados são os mesmos relacionados para a escuta do canal e mais a possibilidade de negação de serviços para usuários legítimos em função dos invasores estarem usufruindo serviços de forma não autorizada. Grande parte desta vulnerabilidade é responsabilidade do sistema operacional hospedeiro, reduzindo a responsabilidade dos mecanismos de segurança das redes. Na verdade, esta forma de agressão normalmente se transforma ou em escuta ou em mascaramento depois de concretizada a invasão.

O terceiro item, mascaramento, consiste na tentativa de personificação de uma terceira entidade em uma comunicação. O objetivo é o mesmo que os anteriores: acesso a informações ou a recursos computacionais. O mascaramento pode ser conseguido por invasão simples (como visto acima) ou por meios muito mais sofisticados como a alteração de pacotes que fluem na rede ou ainda forjando pacotes. Estando mascarado de uma entidade comunicante legítima da rede, o software “clandestino” pode ter acesso às informações sensíveis ou a recursos importantes e até provocar eventos anonimamente. Fica claro que este tipo de agressão é complexo o que pressupõe a necessidade do invasor ser conhecedor profundo dos protocolos de comunicação utilizados.

8.2 Gerência de Redes e Segurança

Gerência de Redes é uma aplicação distribuída onde processos de gerência (agentes e gerentes) trocam informações com o objetivo de monitorar e controlar a rede. O processo gerente envia solicitação ao processo agente que por sua vez responde às solicitações e também transmite notificações referentes aos objetos gerenciados que residem em uma base de informação de gerenciamento (MIB).

Toda e qualquer informação produzida pelo Sistema de Gerência, em um determinado instante, está ou em uma MIB ou trafegando pela rede (em uma comunicação típica entre um agente e um gerente ou entre dois gerentes) ou ainda poderá ser deduzida (reproduzida) com informações parciais oriundas destas duas fontes. Toda informação produzida pelo Sistema de gerência é útil para a manutenção da rede em operação com confiabilidade. Sem dúvida, os Sistemas de Gerência facilitam a administração das redes seja pela automatização de algumas atividades, seja por permitir maior controle sobre os recursos da rede ou ainda por fornecer informações (estatísticas, por exemplo) que permitirão ajustes, correções ou adaptações às necessidades dos usuários.

Entretanto, neste ponto também é possível observar que o próprio Sistema de Gerência e as informações por ele geradas são de extrema valia para indicar pontos vulneráveis a ataques, ter acesso e controlar indevidamente recursos da rede, manipular informações, em suma, realizar atividades prejudiciais à rede, aos sistemas e/ou aos usuários. Sob certa ótica, é possível até afirmar que uma rede com Sistema de Gerência formal implantado é menos segura do que a mesma rede sem o Sistema de Gerência. Os exemplos a seguir explicam esta afirmação:

- Se um agente emite um alarme acerca de uma falha em um mecanismo de segurança e este alarme é interceptado por um invasor; então se está fornecendo uma informação valiosa para que um intruso possa realizar outras agressões.
- Uma notificação de alarme forjada por um intruso pode levar a alguma ação (por parte do gerente “iludido”) que libera informações ou serviços a usuários que não teriam autorização em situações normais.
- Uma entidade infiltrada que se mascara de gerente pode ter acesso a informações sensíveis mantidas na MIB, inclusive com poder de alteração (como desativação de serviços de segurança ou alteração de registros de contabilização).
- Um agente mascarado pode fornecer acesso a recursos da rede para usuários não autorizados e/ou indisponibilizar tais recursos para usuários legítimos; ou ainda forjar informações com o intuito de forçar o gerente para a alocação de mais ou melhores recursos.

Com estas e muitas outras vulnerabilidades é que se pode concluir que um Sistema de Gerência de Redes torna a rede mais insegura por um lado, ao mesmo tempo em que cria mecanismos de controle que serão úteis também na manutenção da segurança da rede.

8.2.1 Ameaças sobre Sistemas de Gerência

As ameaças abordadas dizem respeito às agressões que podem ser executadas por intrusos na rede ou por usuários que tentam obter mais recursos ou informações do que são autorizados. Podem ser classificadas em: Mascaramento, Monitoração ou Escuta Passiva e Escuta Ativa.

- **Mascaramento -** É a pretensão de uma entidade de se fazer passar por outra de modo a ter acesso a informações, ganhar novos privilégios, afetar os sistemas, etc. Para criar uma entidade mascarada, o agressor deve ter acesso à rede, podendo ser um acesso autorizado (lícito) ou não. Então, uma primeira barreira contra este tipo de agressão é um Sistema de Controle de Acesso à rede o mais confiável possível. Controle de Acesso envolve identificação, autenticação e autorização, além de uma política de segurança e consciência por parte dos usuários da importância da segurança para a rede e seus sistemas.
    - Por **identificação** - entende-se uma estrutura de nomes que garanta a identificação única para cada entidade da rede. Mas não basta identificação porque as entidades podem não ser confiáveis ao se identificar, sendo necessário então a confirmação da entidade:
        - **Autenticação**, ou seja, a validação de que uma entidade é quem ou aquilo que diz ser.
        - **Autorização** permite indicar se determinada entidade (identificada e autenticada) possui acesso legítimo (autorizado) a determinado recurso ou operação e deve evitar acesso caso contrário.

Mas não se pode pensar em Controle de Acesso somente no momento do primeiro acesso em uma sessão (login) mas também em outras atividades durante a sessão, de forma continuada, sob pena de abordar o problema de maneira muito pobre. É então importante para a segurança em um Sistema de Gerência que cada entidade componente do mesmo esteja devidamente identificada e autenticada e tenha os direitos de acesso definidos e controlados. Para tanto, faz-se necessária a especificação e implantação de serviços de Identificação/Autenticação específicos para entidades comunicantes, e de Confidencialidade de Acesso aos recursos (no caso, o acesso à MIB).

- **Monitoração ou Escuta Passiva -** Neste caso, há apenas coleta de informações que transitam na rede. Apesar de, em um primeiro momento, os riscos que representa a escuta passiva parecerem pequenos, é possível recolher muitas informações úteis para o comprometimento de uma rede. Alguns exemplos são as informações que dizem respeito à segurança da rede ou sobre falhas, que fluem entre agentes e gerentes da rede. Estas informações podem ser senhas de usuários, informações trocadas entre entidades para autenticação, informações sobre configuração, informações sobre falha de algum mecanismo de segurança, etc. Quando informações sensíveis como as citadas devem transitar pela rede, é fundamental que sejam adotadas medidas para evitar que tais informações sejam acessadas indevidamente. Para tanto é necessário definir um Serviço de Confidencialidade de Comunicação.

- **Escuta Ativa -** A escuta ativa difere da escuta passiva por não apenas coletar informações que fluem pela rede, mas também por alterá-las de alguma forma, seja no conteúdo, na seqüência, no tempo ou pela destruição ou criação de mensagens; de forma a realizar ou induzir ações não autorizadas ou criar condições para ações não autorizadas ou ainda encobrir atos ilícitos praticados. Duas medidas de proteção se tornam então necessárias: autenticação da origem das mensagens e garantia da integridade das mensagens. Sem estes dois serviços a rede continuará aberta a ataques.

Os Sistemas de Gerência de Redes estão sujeitos a todas estas ameaças porque estão baseadas na separação das funções de gerência com distribuição das informações, sendo necessária a comunicação entre entidades de gerência. Deve-se então acrescentar ao Serviço de Identificação/Autenticação de entidades a tarefa de autenticar a origem, a forma e o momento do envio das mensagens. Além disso, um Serviço de Integridade de mensagens deve ser estabelecido e será o responsável pela garantia de que uma mensagem não sofreu alterações em seu caminho desde a origem até o destinatário, envolvendo as tarefas de evitar alteração de informações, re-seqüenciamento e a simples destruição.

A autenticação, por sua vez, também depende da integridade das mensagens para algumas tarefas. Por exemplo, de nada adianta validar a origem de uma mensagem que foi alterada por uma escuta ativa ou se durante uma autenticação de entidade as mensagens podem ser afetadas de modo a validar uma entidade mascarada.

8.2.2 Requisitos de Proteção

No contexto de um Sistema de Gerência, as ameaças que cabem ser analisadas, dentre todas as ameaças à segurança em uma rede de computadores, são as seguintes:

- Acesso não autorizado à informação de gerência que flui pela rede;
- Acesso não autorizado à informação de gerência mantida na MIB;
- Alteração e re-sequenciamento de mensagem de gerenciamento;
- Geração de mensagens de gerenciamento por terceiros (entidades que não fazem parte da arquitetura de segurança).

Os Serviços de Segurança que precisam estar disponíveis para contrapor estas ameaças, conforme visto anteriormente são:

- Confidencialidade contra acessos não autorizados à informação de gerência;
- Integridade contra alterações e re-sequenciamento;
- Autenticação contra geração de mensagens por terceiros.

Para suportar o Serviço de Confidencialidade (ou privacidade) é necessário o uso de criptografia. Há dois tipos básicos de criptografia em uso nos dias atuais: por chave secreta e por chave pública. A segunda alternativa - chave pública - é a mais usada devido à eficiência do processo da distribuição das chaves. Um sistema de chaves públicas prevê a existência de duas chaves simétricas: o que uma chave cifra e seu par decifra e vice-versa. Uma das chaves é mantida em segredo (chave privada) e a outra é divulgada (chave pública - daí o nome do sistema) através de um serviço

de diretório, por exemplo. O uso de criptografia é a única forma de garantir que uma mensagem que esteja trafegando pela rede e seja interceptada não forneça informações valiosas para o agressor. A mensagem poderá ser interceptada, mas dificilmente será decodificada.

Da mesma forma o acesso a MIB pode ser aberto, pois, se as informações lá contidas estiverem cifradas, elas não serão úteis para invasores, uma vez que estes não terão tempo hábil para decifrá-las antes que ocorram alterações nas mesmas. Assim, um grau de segurança adicional é conseguido com o uso de criptografia sobre a MIB. Empregando o conceito de que a MIB somente poderá ser acessada por um único agente, toda a informação poderá ser guardada criptografada com a chave pública deste agente. Desta forma, só o mesmo agente pode ter acesso às informações geradas ou manipuladas por ele próprio. Para suportar o Serviço de Integridade, duas providências se fazem necessárias:

- Para evitar que uma mensagem alterada seja considerada válida, a ação a ser tomada é a cifragem de um campo que contenha o checksum de toda a mensagem. A chave que deve ser utilizada para isto é a chave privada do remetente da mensagem (a chave privada do esquema de chave pública). Com isto se garante a integridade da mensagem, pois um agressor não terá como alterar a mensagem, gerar um novo checksum e criptografá-lo, pois não possuirá a chave correta. Já o destinatário pode verificar a integridade simplesmente usando a chave pública do remetente para conferir o checksum calculado com o decifrado. Qualquer alteração da mensagem é imediatamente detectada.
- Para evitar o re-sequenciamento, o que deve ser feito é a inclusão de um campo que indicará a ordem da seqüência da mensagem. Este campo deverá conter um valor dentro de uma seqüência determinada a cada comunicação entre cada par de entidades (ou seja, a cada mensagem, o remetente incluirá o valor da seqüência e indicará qual valor deverá ser usado na próxima comunicação entre estas duas entidades). Estes dois campos também devem ser criptografados com a chave privada do remetente.

O Serviço de Autenticação deve garantir que a origem das mensagens de gerenciamento são entidades legítimas para evitar a execuções de ações indevidas ou o acesso a informações por terceiros. Uma observação à providência referente à alteração de mensagens citada acima pode levar a conclusão de que a própria integridade oferece meios de aferir a autenticidade das mensagens, uma vez que somente o interlocutor autêntico conhecerá sua chave privada e com isto poderá gerar os campos criptografados de acordo com o esperado. A autenticação, então, está automaticamente incluída no Serviço de Integridade.

8.3 Arquitetura de Segurança para Gerência de Redes

Cada agente e gerente do Sistema de Gerência devem possuir uma Interface de segurança que deve garantir que as mensagens recebidas pelos agentes e gerentes são realmente internas ao Sistema (autênticas) e que não foram alteradas (íntegras). Além disso, pode ser desejável a confidencialidade da comunicação entre as entidades do Sistema e esta característica também deve ser garantida pela

Interface de Segurança. Esta interface atuará como uma “clearing house” entre cada par comunicante, impedindo que informações de gerência sejam acessadas, alteradas ao forjadas por entidades não autorizadas.
Os serviços diretamente implementados pela Interface de Segurança são:

- **Serviço de Autenticação:** garantindo a origem autêntica das mensagens;
- **Serviço de Integridade:** que impede o processamento de mensagens adulteradas ou forjadas;
- **Serviço de Confidencialidade de Comunicação:** tornando as mensagens não acessíveis por terceiros, enquanto úteis;
- **Serviço de Confidencialidade de Acesso:** que garante a proteção às informações de gerência mantidas na MIB.

Todos os Serviços acima devem estar presentes nas Interfaces de Segurança dos agentes e dos gerentes componentes do Sistema de Gerência, à exceção do último, cuja presença somente é necessária nas entidades agente, pois diz respeito apenas a atividades destes. Acessoriamente, são facilmente conseguidos como “efeito-colateral” da implantação dos serviços acima os seguintes:

- **Serviço de Controle de Acesso:** em função da Confidencialidade de Acesso. Se apenas o proprietário da MIB pode “compreender” os dados lá mantidos, o problema de acesso está resolvido;
- **Serviço de Não-Repudio:** resultante da implantação do Serviço de Autenticação. Uma vez garantida a origem da mensagem, também não há como o remetente negar a autoria da mesma, pois somente ele poderia gerar uma mensagem com campos criptografados pela chave privada dele.

Além dos serviços citados, é de grande importância que as Interfaces de Segurança mantenham registros de ocorrências em logs para que seja possível a realização de auditorias, como atividade de gerenciamento de segurança.

Interface de Segurança é, portanto, uma redoma que encapsula totalmente cada agente e cada gerente do Sistema de Gerência, de forma que toda comunicação entre estas entidades se dê somente através da Interface. Esta abordagem permite que a instalação da Interface seja transparente para os agentes e gerentes, ou seja, nada é alterado nos agentes e gerentes para que a Arquitetura de Segurança seja implantada. As comunicações entre entidades sempre passarão por filtros (as Interfaces de Segurança) em cada um dos lados desta comunicação, para verificação de integridade e autoria e para garantir privacidade. A figura seguinte mostra a Interface de Segurança.

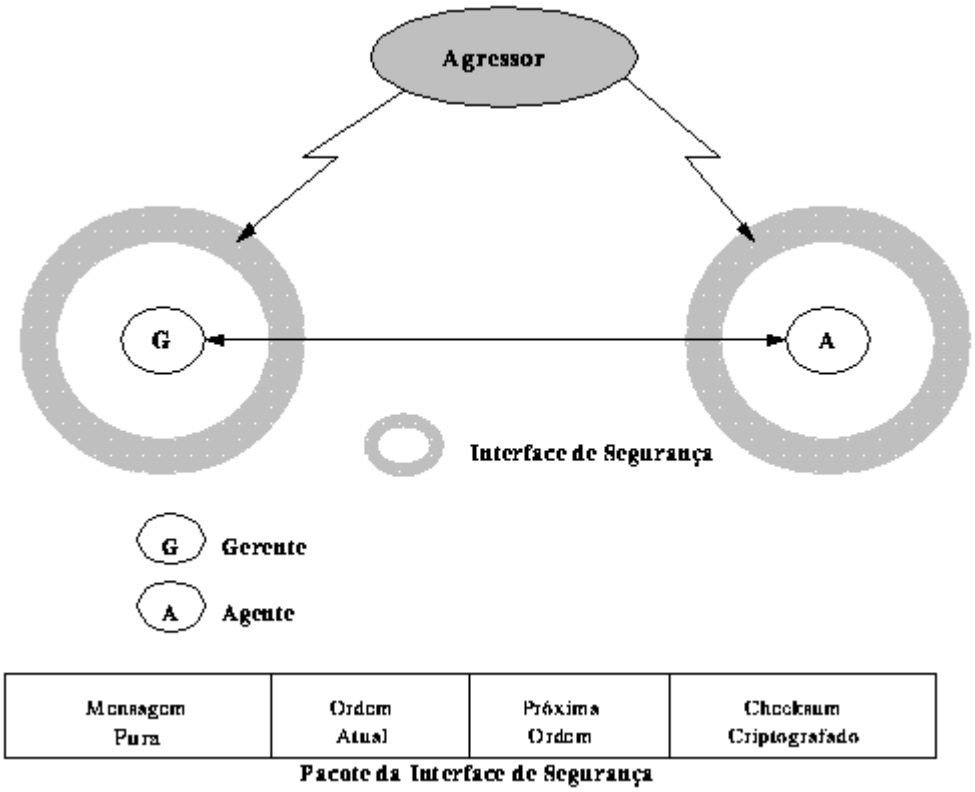


Figura 16 - Interface de Segurança

Somente trafegarão na rede (no escopo de Sistemas de Gerência) pacotes de comunicação entre Interfaces de Segurança que encapsulam pacotes de agentes e gerentes, com todos os mecanismos de segurança para evitar possíveis agressões. A interface de segurança emissora é responsável pela incorporação dos mecanismos no pacote original e a interface do lado receptor é responsável pelas verificações e liberação ou não de pacotes.

O acesso às informações de gerência guardadas na MIB também deve ser restrito. Existem duas formas de prover tal restrição: pela instalação de um mecanismo de controle de acesso próprio ou a criação de um mecanismo de confidencialidade, onde as informações armazenadas na MIB estariam cifradas. A estratégia de estabelecer um Serviço de Confidencialidade no acesso a MIB, garantindo que um e somente um agente (o seu criador e mantenedor) terá acesso direto às informações lá contidas, se apresenta como a mais interessante. Três itens motivam esta escolha:

1. O mecanismo de confidencialidade já está disponível para outros serviços de segurança (Confidencialidade de Comunicação), eliminando a necessidade de construção de um novo mecanismo de segurança, o controle de acesso;
2. Elimina a necessidade de criação de uma Interface de Segurança também para a MIB, centralizando nos agentes a implementação dos mecanismos de segurança;
3. Não possui certas vulnerabilidades presentes nos mecanismos de controle de acesso, como a abertura para o mascaramento.

A forma de implantar o Serviço de Confidencialidade no acesso a MIB é o uso de criptografia em todos os acessos à mesma. O agente responsável pela MIB possui

uma chave que é utilizada para cifrar todas as informações antes de armazená-las e decifrar as informações quando do acesso. A cifragem das informações contidas na MIB pode ser feita com a mesma chave que o agente utiliza para garantir a privacidade das comunicações ou com uma chave própria para a tarefa, podendo ser inclusive com o uso de uma técnica de chave secreta, mais eficiente em termos de tempo para criptografar e decriptografar. Isto porque o acesso a MIB é completamente independente de todo o processo de comunicação entre entidades. Tal mecanismo permite inclusive que o acesso em si possa ser realizado sem restrições, mas uma vez que as informações estão criptografadas, não há liberação efetiva das mesmas para aqueles que não possuírem as chaves.

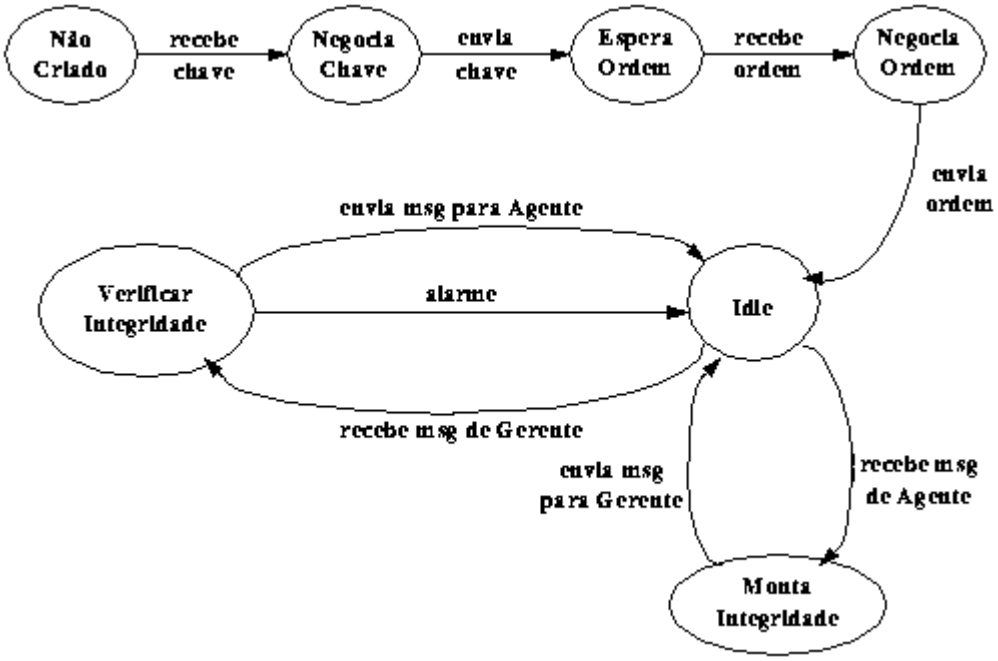


Figura 17 - Integridade e autenticação no agente

8.3.1 - Algoritmos

Os algoritmos utilizados para a implementação das Interfaces de Segurança são divididos em Algoritmos para Autenticação e Integridade e Algoritmos para Confidencialidade. Estes dois algoritmos são apresentados a seguir:

- Algoritmo para Autenticação e Integridade - Para se conseguir a garantia de autenticidade e integridade das mensagens que são trocadas entre as entidades componentes do Sistema de Gerência, cada Interface de Segurança deve implementar (indistintamente para agentes e gerentes) os algoritmos para o envio e o recebimento de mensagens a seguir, além de uma negociação preliminar para a troca de informações que serão necessárias para o desenrolar das comunicações, como as chaves públicas das duas interfaces e a determinação do primeiro valor que será utilizado para garantir a ordem das mensagens.

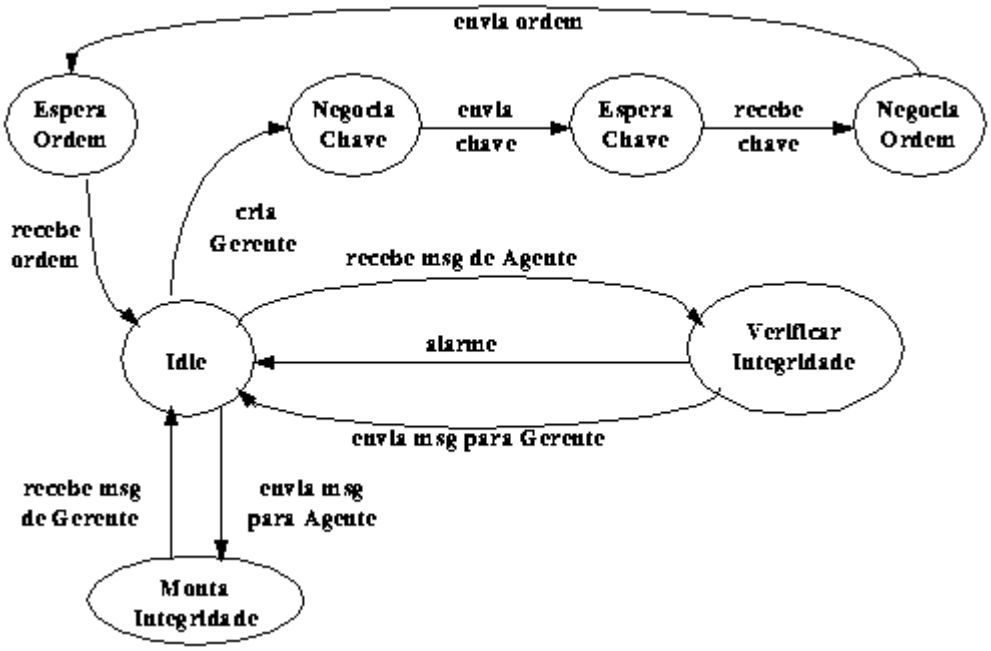


Figura 18 - Integridade e autenticação no gerente

- Algoritmos para Confidencialidade - Conforme apresentado, há dois momentos onde é necessária a confidencialidade: na comunicação e no acesso à MIB.
    - **Confidencialidade na Comunicação** - A confidencialidade na comunicação deve ser garantida quando requisitada. As atividades relativas a confidencialidade devem ser realizadas sobre uma mensagem já preparada pelos mecanismos de integridade e Autenticação, sendo realizada, portanto, um nível abaixo.
    - **Confidencialidade no Acesso à MIB** - Para a confidencialidade das informações contidas na MIB.

Uma Arquitetura de Segurança genérica para aplicação em Sistemas de Gerência de Redes é extremamente flexível uma vez que permite sua aplicação em todos os Sistemas de Gerência baseados em entidades agentes e gerentes, ao mesmo tempo, não exige que tais entidades sofram alterações para suportá-la, tornando transparente a sua instalação.

A ampliação do conceito de assinatura digital permite não só validar a origem, mas também a integridade das mensagens e ao controle de acesso à MIB ser feito através do serviço de confidencialidade, que não impede o acesso mas não revela as informações senão para o legítimo proprietário.

Embora a Arquitetura de Segurança apresentada seja genérica, ela já é implementada nos sistemas de gerência que estão baseados no modelo OSI. Isto ocorre porque a camada de Apresentação deste modelo já implementa serviços de criptografia das mensagens.

Capítulo 9 - Ferramentas de Gerenciamento de Redes

Muitos fabricantes de produtos de redes oferecem também produtos específicos de gerenciamento de redes que se dirigem a necessidades mais detalhadas. Dentre estes, vale salientar:

9.1 - AT&T - UNMA

Unified Network Management Architeture (UNMA) um produto desenvolvido pela AT&T propõe um gerenciamento integrado de redes, em ambientes heterogêneos, utilizando as interfaces definidas segundo o padrão OSI (*Open Systems Interconnection*) . O componente principal desta estratégia é o integrador *Accumaster*, o qual permite obter uma visão global dos elementos físicos e lógicos de rede a partir de uma interface centralizada. A arquitetura UNMA é dividida em três níveis que seguem as especificações da ISO/ITU-T:

Nível 1 - fornece uma visão global do sistema através de comunicações entre os *Element Management System* (EMS) e o integrador *Accumaster*;

Nível 2 - composto pelos EMS, que são programas que fornecem facilidades locais de gerenciamento assim como realizam funções que permitem gerenciar um grupo particular de elementos de rede;

Nível 3 - composto pelos elementos de rede (modem, multiplexadores, LANs, etc.)

9.2 - DEC - EMA

Enterprise Management Architecture (EMA) é o sistema de gerenciamento da arquitetura de rede DEC chamada DNA (*Digital Network Architecture*). Define como ponto de partida a relação gerente-agente, o que a DEC denomina diretor-entidade (*Director-Entity*). EMA fornece meios para o gerenciamento de redes de forma hierárquica centralizada ou distribuída, ou outra forma qualquer de organização entre estas duas. Possui também uma implementação proprietária do protocolo CMIP (*Common Management Information Protocol*) para facilitar comunicações com outros sistemas proprietários.

A função principal de EMA é fornecer um gerenciamento integrado, traduzido por uma interface usuário coerente, uma base de informações comum e um acesso integrado às funções de gerenciamento e às entidades gerenciadas. A EMA suporta três tipos de módulos de gerenciamento: de acesso, que estabelece interface para sistemas de gerenciamento e elementos de outros fornecedores; de funções, que implementa as aplicações de gerenciamento, tais como administração de configuração e alarmes; de apresentação, que implementa serviço de interface de usuário.

A DEC elaborou seu gerente de rede de maneira flexível, modular e extensível servindo de base para operação em ambientes complexos e heterogêneos, criando o que pode ser chamado de "sistema operacional de gerenciamento de redes".

9.3 - HP Open View

A arquitetura *Network Management Architecture* (NMA) do HP OpenView é um refinamento do modelo de gerenciamento OSI. A infra-estrutura de comunicação fornece uma interface baseada no *Common Management Information Service* (CMIS) e suporta várias pilhas de protocolos. Os serviços de gerenciamento como métodos de acesso a objetos são tratados com uma visão orientada a objeto adotado pela arquitetura NMA. Estes objetos podem ser equipamentos físicos ou qualquer função de gerenciamento no interior dos processos gerentes. A arquitetura NMA refina o processo gerente em três possíveis componentes: a interface usuário, a aplicação de gerenciamento e o serviço de gerenciamento.

9.4 – SunNet Manager (Sun Microsystems)

O *SunNet Manager* baseia-se no modelo Gerente-Agente, onde o gerente é um processo iniciado pelo usuário e o agente é um processo que tem acesso ao objeto gerenciado e coleta os dados de comportamento do gerente. A figura a seguir ilustra o seu esquema de funcionamento.

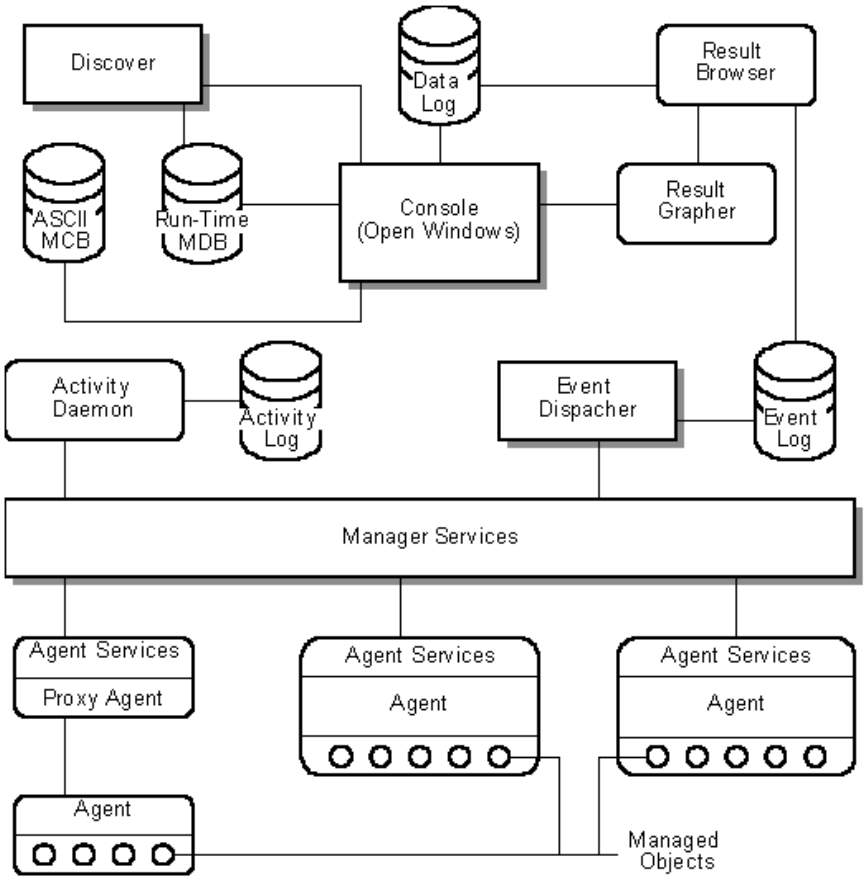


Figura 19 – Arquitetura em blocos do SunNet Manager

A aplicação de gerenciamento central no pacote *SunNet Manager* (lugar onde um usuário inicia tarefas de gerenciamento e informações de gerenciamento são retornadas) é denominada Console. Esta apresenta uma interface gráfica suportada por X-terminais, que permitem múltiplas instâncias do Console executarem em uma única máquina ao mesmo tempo. Cada instância do Console é reconhecida pelo nome do usuário que a invoca. O nome do usuário é mostrado entre parênteses numa região da Console e das janelas de ferramentas do SunNet Manager. Cada instância da Console poderá trabalhar somente com outras ferramentas que usa o mesmo nome do usuário. A Console oferece mecanismos para iniciar pedidos de relatórios de dados e relatórios de eventos**.**

- **Relatórios de Dados** permitem direcionar Agentes para enviar relatórios de dados brutos de gerenciamento em uma base periódica.
- **Relatórios de Eventos** mostram como direcionar Agentes para relatar apenas quando condições específicas são encontradas (isto é, quando um evento ocorre).

No SunNet Manager, os atributos de um objeto gerenciado são descritos em uma porção da MDB chamada o Esquema-Agente. O Agente é capaz de responder aos pedidos do Gerente porque ambos usam a mesma definição de dados para o objeto gerenciado. Os dados da MDB e qualquer atualização realizada usando o editor gráfico possibilita constituir uma base de dados dinâmica em tempo de execução, a qual pode ser salva para a MDB a qualquer momento.

9.4.1 - Ferramentas

O SunNet Manager inclui várias ferramentas que podem ser invocadas a partir da Console:

- ***Discover*** - realiza a busca de elementos de rede e automaticamente cria uma representação gráfica da rede. À medida que os elementos de rede vão sendo encontrados, eles são adicionados à base de dados (run-time database).
- ***Result Browser*** - permite ao usuário examinar e organizar os arquivos de log;
- ***Result Grapher*** - permite visualizar relatórios de dados e informações do arquivo de log.

Existem dois tipos de Agentes no SunNet Manager: aqueles que têm acesso aos objetos gerenciados e aqueles que acessam os dados indiretamente**.** A maioria dos Agentes acompanha esta versão de gerenciamento de objetos a partir das Sun Workstations onde estão instalados. O segundo tipo de Agente proporciona a habilidade para gerenciar objetos que não são diretamente acessados. Tais Agentes são chamados agentes proxy. Agentes proxy são executados em estações Sun, chamadas proxy systems, e utilizam protocolo de tradução de mecanismos dependendo da necessidade de acesso para os objetos gerenciados. O proxy system pode ser uma estação de trabalho na qual a console do SunNet está sendo executado em uma outra estação na rede. Por exemplo: o PING Agente proxy tem a função de testar o alcance de dispositivos (IP) *Internet Protocol* traduzindo os pedidos do Gerente através do *Echo Requests Internet Control Message Protocol* (ICMP). Agentes proxy permitem ao SunNet Manager estender-se virtualmente dentro de

qualquer domínio. O Agente proxy *Simple Network Management Protocol* (SNMP) pode gerenciar qualquer dispositivo que suporta SNMP, o protocolo de gerenciamento padrão para o mundo TCP/IP.

O Gerente e Agente comunicam-se através da biblioteca Serviços Gerente/Agente, a qual proporciona a infra-estrutura de gerenciamento e trata dos serviços de comunicação. Os processos Gerente e Agente usam a biblioteca Serviços através de *Application Programming Interfaces* (API's), a qual por sua vez usa o Remote Procedure *Call/External Data Representation* (RPC/XDR) capacidade do SunOS. O Agente e o Gerente não precisam se preocupar com os níveis mais baixos da rede envolvidos na comunicação entre eles. O processo Agente precisa preocupar-se apenas com a coleta de dados do objeto gerenciado.

A tabela seguinte descreve os tipos de agentes do SunNet Manager.

Agente	Dados
diskinfo	informações so bre o disco
etherif	estatísticas da interface Ethernet
hostif	estatísticas da interface
hostmem	utilização do memória.
hostperf	performance do host
ippath	informações da rota do pacote IP
iproutes	tabela e estatísticas da rota IP.
layers	estatísticas da camada de protocolo.
lpstat	status da impressora.
ping	informações da conexão IP.
rpcnfs	estatísticas RPC e NFS.
snmp	SNMP (proxy)
sync	estatísticas de sincronismo.
traffic	analisador do tráfego Ethernet.
X25	informação do circuito virtual X.25

O despachante de eventos é um processo que usa os Serviços Gerente/Agente para direcionar relatórios de eventos para o destino apropriado, tal como a Console do SunNet Manager. Qualquer outra aplicação de gerenciamento pode usar o despachante de eventos, registrando o recebimento de alguns ou todos os relatórios de eventos baseado em uma variedade de critérios de seleção.

9.5 - Tivoli

O Tivoli é uma plataforma de gerenciamento distribuído desenvolvida pela IBM. Um sistema que gerencia os nodos e serviços da rede, garantindo informações atualizadas e com segurança. O seu gerenciamento compreensivo de processos e tecnologias permite a organização identificar, medir e administrar todos aspectos de serviços oferecidos para maximizar a produtividade, a efetividade operacional, e rentabilidade dos negócios.

O Tivoli trabalha com o conceito de regiões de policiamento (*Policy Region)* ou TMR – *Tivoli Management Region*. Uma região de policiamento abrange um conjunto de recursos gerenciados, como contas de usuários, estações de trabalho, roteadores. Em uma rede podem ser definidas mais de uma região de policiamento. Cada região possui suas próprias políticas de controle de acesso e gerenciamento.

Em uma região de policiamento existem alguns elementos que ajudam no gerenciamento como:

- **TMR server** - responsável por controlar toda região de policiamento e define as políticas utilizadas nessa região;
- **Managed Node -** trabalha como um intermediário entre as funções do Endpoint e do Endpoint Gateway. Executa algumas tarefas a pedido do TMR server;
- **Endpoint Gateway -** controla as comunicações e operações entre os Endpoints. Responsável por enviar aos Endpoints métodos que permitem aos Endpoints realizarem as funções de gerenciamento;
- **Endpoint -** agente que executa as operações de gerenciamento nos recursos finais.

A figura a seguir mostra a tela principal com os elementos do Tivoli.

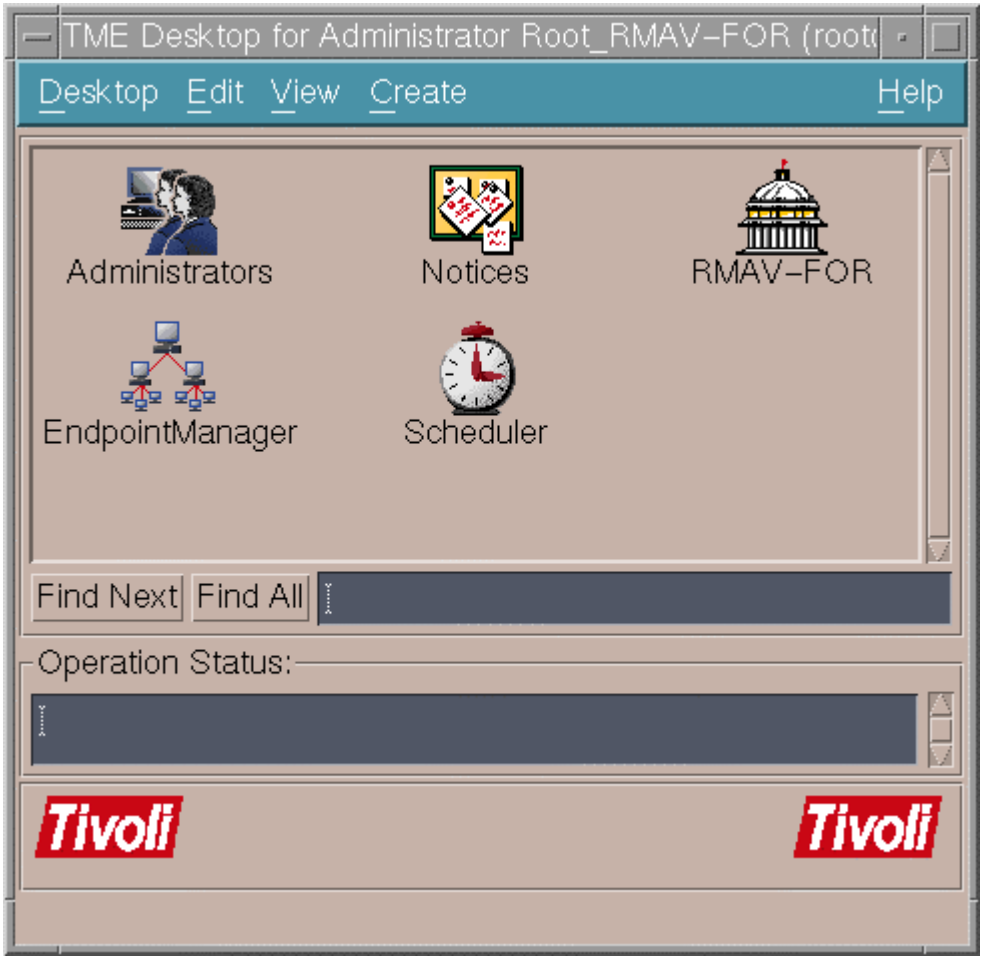


Figura 20 - Tela principal do Tivoli

O ambiente de gerenciamento do Tivoli ou TME (Tivoli Management Environment) é dividido em vários módulos, os principais são:

- **Framework -** Módulo principal do Tivoli. Tem funções básicas de administração e serviços de gerenciamento. Facilita no restante das funções de gerenciamento, como no gerenciamento de sistemas e em notificações, e na integração com os outros módulos;
- **User Administration -** Permite o gerenciamento de grupos e contas de usuários em vários sistemas operacionais que fazem integração com a plataforma como Windows, Netware e Unix;
- **Distributed Monitoring** - monitora o status de vários recursos da rede como sistemas, aplicações e processos. Monitora recursos locais ou remotos, além de apresentar eventos e alarmes de rede;
- **Inventory -** Tem as funções de manter e procurar informações sobre o inventário do ambiente e sobre *hardware* e *software;* monitorar e registrar mudanças de configuração; disponibilizar as informações de inventário para funções de auditoria na empresa;
- **Software Distribution -** permite a distribuição e instalação de software em máquinas de uma rede heterogênea;
- **Enterprise Console** - aplicação que gerencia eventos baseados em regras. Podem-se programar eventos a serem alarmados.

Além desses módulos de gerenciamento o Tivoli utiliza-se do Netview, ferramenta também desenvolvida pela IBM, para o diagnóstico e controle de redes de comunicação. Seu objetivo era substituir uma gama variada de produtos similares já existentes. O mais conhecido desses produtos é o Network Communication Control Facility (NCCF) que funciona como uma aplicação Virtual Telecommunication Access Method (VTAM), fornecendo uma visão do estado da rede através de um monitor de controle e uma base de dados. Outros produtos de controle são o Network Problem Determination Application (NPDA), que opera na detecção de problemas e o Network Logical Data Manager (NLDM), que gerencia dados lógicos.

O principal objetivo do NetView foi então reunir as funcionalidades destes produtos em um só, melhorando o desempenho e introduzindo novos conceitos no gerenciamento de redes. Três componentes são definidos na arquitetura do NetView: Pontos Focais (focal points), gerentes que realizam as funções de controle integrado; Pontos de Entrada (entry points), agentes tratados como recursos gerenciados, que reportam seus dados de gerenciamento via SNA(System Network Protocol) aos pontos focais; e pontos de serviço (services points), destinados a prover gateways traduzindo protocolos não padrões SNA no protocolo (NMVT), o que permite a integração de dispositivos não-SNA ao esquema de gerenciamento NetView.

9.6 – Unicenter TNG

Uma plataforma que controla todos os recursos na rede de uma organização desde *laptop*s até *mainframes* e desde Intranet até Extranets. O Unicenter TNG gerencia cada dispositivo, servidor, estação de trabalho, sistema operacional, banco de dados e aplicações que estão sendo executados na rede, proporcionando uma

visão única de todos os ambientes. As funções da plataforma Unicenter TNG são desenvolvidas em uma arquitetura multilinear e orientada a objetos. Infra-estrutura com repositório de objetos, escalável e com tecnologia gerente/agente, opera em redes heterogêneas e distribuídas permitindo a integração de qualquer tipo de sistema operacional ou serviço a um gerenciamento modular, sem limitações arbitrárias.

A tecnologia de objetos é a base para todos os aspectos do CA-Unicenter TNG. Os repositórios distribuídos de objetos são utilizados por todas as suas funções de gerenciamento, para armazenar informações sobre os objetos gerenciados, suas propriedades e seus relacionamentos. Essa ferramenta possui uma interface, chamada "Interface de Mundo Real 3-D", que exibe uma situação real dos objetos e capacita o controle e a gerência de todos os recursos disponíveis na rede. Qualquer subsistema pode definir classes e objetos no repositório. E todo objeto criado também é gerenciado pelo repositório de objetos o qual constitui um poderoso mecanismo de abertura para integração entre funções de gerenciamento em todos os níveis.

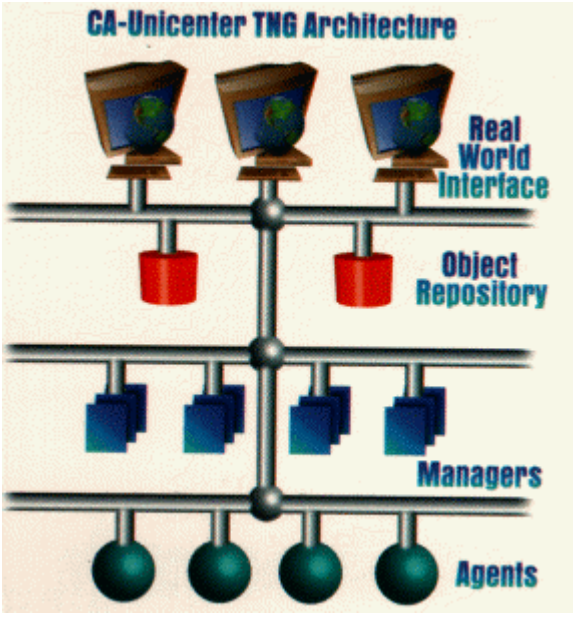


Figura 21 - Arquitetura do Unicenter TNG

O Unicenter TNG baseia-se em uma arquitetura para gerenciamento em múltiplos níveis gerente/agente. Gerentes e Agentes podem ser explorados em qualquer configuração, dependendo da necessidade das funções de gerenciamento do ambiente gerenciado. Os agentes são ativos e inteligentes, capazes de implementar policiamentos e coordenar juntamente com outros agentes ativos as seguintes funções:

- Monitorar eventos e *status;*
- Executar o gerenciamento da configuração de ambientes distribuídos;
- Executar o armazenamento através de redes heterogêneas.

A função de descobrimento automático não detecta somente a topologia e periféricos da rede, mas também os computadores, suas configurações de *hardware* e *software,* bancos de dados, aplicações e usuários.

Capítulo 10 – Novos conceitos e abordagens

Como tudo evolui, gerenciamento de redes também está evoluindo e muitas coisas que alguns anos atrás eram "verdades" hoje já não são mais. Pontos que eram considerados importantes e de relevância já não possuem a mesma importância de antes. Assim, antigos conceitos estão sendo revistos, e novos estão surgindo, levando todos a reavaliar a forma que está sendo feito gerenciamento de redes hoje, e levantando perspectivas para o futuro.

Durante os anos de vida do SNMP, surgiram várias e várias MIB's. Elas formam uma coleção de dados e valores necessários para monitorar e controlar dispositivos de rede que foram levantados por especialistas durante todos estes anos. As MIB's e a especificação SMI são o mais importante legado do SNMP.

Através da utilização das MIB's, aprendeu-se o valor de definições claras e concisas, formando o veículo fundamental pelo qual uma estação de gerenciamento pode aprender sobre os dispositivos que estão sob o seu controle. Apesar desta importância, alguns aprimoramentos ainda podem ser feitos às definições das MIB's. Serão apresentadas duas novas funcionalidades a seguir.

10.1 - Meta Variáveis

Meta-variáveis são variáveis que existem apenas na definição da MIB. Cada meta-variável é definida em função de variáveis reais da MIB. Além de ser simples de se fazer, não requer que nenhuma alteração seja feita nos protocolos existentes ou na implementação dos agentes. Por exemplo, poderia existir uma meta-variável chamada "taxa de erro" que seria calculada utilizando como base variáveis reais.

A idéia básica é utilizar-se dos conhecimentos dos gerentes de rede espalhados pelo mundo, para que estes, com a sua experiência, informem que informações acham relevantes para se chegar a um consenso de que meta-variáveis precisariam ser definidas. Para obter o valor destas meta-variáveis, a estação de gerenciamento tem que executar a função ela mesma. Isto implica que esta função deve ser expressa em alguns procedimentos que devem ser mapeados em *get*'s e *set*'s. Alguns acham que estas funções seriam mais bem expressas em forma de simples *scripts.*

Extensões podem ser feitas ao conceito de meta-variáveis. Uma delas seria incluir dispositivos dedicados para gerar os valores destas meta-variáveis e exportá-las como variáveis reais SNMP através de uma MIB própria deste dispositivo. Uma outra possível extensão deste conceito, seria os próprios agentes calcularem os valores das meta-variáveis, tornando-as assim variáveis reais.

10.2 - Scripting MIB's

Como já foi dito anteriormente, RMON adicionou a facilidade de invocação de uma ação através da utilização de um objeto para representar um comando. Com esta facilidade, pode-se inserir um script a um dispositivo, iniciar sua execução, requisitar ou esperar que lhe seja informado o resultado. Um script poderia, por exemplo, monitorar as variáveis de um dispositivo observando sinais de erro. Depois ele poderia reportar o problema, fazer mais testes para se fazer um diagnóstico, ou tomar atitudes com o intuito de se fazer uma correção. Um script completo pode ser expresso como uma linguagem interpretativa, onde cada linha do mesmo seria uma linha da tabela. Assim, cada linha seria executada mediante a alteração dos objetos correspondentes.

Uma outra possibilidade seria tratar um script inteiro como uma variável, e a sua invocação pelo gerente se daria através de uma mensagem *get*. O agente, mediante o recebimento desta mensagem, espera que o script termine a execução e retorna o resultado para o gerente, como se fosse uma variável comum. As dificuldades para a utilização de scripts não estão neles mesmos ou na linguagem que eles são implementados. As dificuldades são:

- **Segurança dos Scripts:** esta segurança se refere aos limites que se devem impor aos scripts, ou seja, fazer com que o mesmo faça apenas o que ele tem que fazer e que não possa ser usado para causar danos;
- **Integridade dos Scripts:** garantir que o script que está executando é realmente aquele que se espera;
- **Controle de Scripts:** uma estação de gerenciamento deve estar apta a controlar a execução do script e até de abortá-lo;
- **Controle de Recursos:** como os scripts são programas, limites devem poder ser impostos em termos de consumo de CPU, de memória e de outros recursos;
- **Recuperação de um Script:** é importante que uma estação possa saber da existência de scripts que ela criou, no caso, por exemplo, de uma reinicialização após uma pane;
- **Poder Expressivo:** existe uma discussão sobre quais as ações que um script pode invocar. Há um consenso de que as primitivas a serem invocadas sejam de alto nível:
    - Ping ICMP;
    - Traceroute;
    - Descoberta do caminho MTU;
    - Ferramentas de consultas a DNS;
    - Operações SNMP, incluindo o acesso às MIB's;
    - Ferramentas de consultas às bases de dados locais de redes;
    - Ferramenta ou serviço que regule intervalos de tempo;
    - Ferramentas para enviar mensagens aos usuários em situações adversas.
- **Migração dos Scripts:** este não é um problema sério desde que a estação que criou o script o controle, e desde que o mesmo tenha autorização de executar em outra máquina;

- **Debug dos Scripts:** como scripts também são programas, eles também podem apresentar problemas. Espera-se que um script seja simples o suficiente para que não se precise de uma ferramenta de depuração.

10.3 - Gerenciamento por Delegação

A utilização de scripts traz consigo a possibilidade de se criar um sistema onde as tarefas de monitoração e de controle de um gerente de mais alto nível podem ser repassadas para subgerentes, responsáveis por uma área específica, determinada pela proximidade com os dispositivos gerenciados.

A idéia básica é "gerenciamento por delegação", onde o gerente do nível superior cria um script que é carregado nos gerentes de área para execução. Este gerente de área ou subgerente é um dispositivo *multi-threadead* e pode executar vários scripts simultaneamente, permitindo, assim, que um único subgerente possa ser invocado por vários gerentes superiores. Um dos benefícios da proximidade dos subgerentes com os dispositivos sendo gerenciados é que, com a grande banda e presumidamente uma baixa taxa de perda e de erros de pacote, permite-se que mensagens SNMP sejam trocadas de forma rápida e confiável.

10.4 - Vermes - Agentes Migratórios

O termo "verme" em redes de computadores foi utilizado por John Brunner para denominar um programa que se move através da rede, indo de computador a computador e com a capacidade ainda de se reproduzir. Em termos de gerenciamento de redes, vermes são scripts que se replicam e migram. Eles, como também o gerenciamento por delegação, são derivados do conceito de *scripting* MIB's.

Os agentes migratórios possuem uma gama de aplicações muito vasta. Eles podem ser utilizados para gerenciamento de configuração e de desempenho. Também podem ser utilizados para o transporte de dados não disponíveis no ambiente SNMP, e para manter tais informações confidenciais.

Podem-se utilizar tais agentes para aprimorar a detecção de falhas e a sua correção nas aplicações de gerenciamento SNMP. No caso, por exemplo, de um dispositivo estar mandando notificação de um problema interno, um agente pode ser disparado especificamente para aquele dispositivo e para aquele problema. Uma outra utilização bastante interessante seria a utilização destes agentes migratórios como agentes *proxy*.

Uma outra utilização para agentes migratórios, seria a combinação deste conceito com o de gerenciamento por delegação. Nesta proposta, os subgerentes monitorariam os dispositivos sob sua responsabilidade através de agentes migratórios. O gerente central poderia determinar que cada subgerente utilizasse um plano de viagem distinto para se fazer o gerenciamento dos dispositivos sob seu controle.

10.5 - MÉTODOS DE ACESSO - PROTOCOLOS

Anteriormente, foi falado sobre o mito de se poder continuar a fazer gerenciamento, no caso de uma pane, se o SNMP fosse baseado em um protocolo de transporte não orientado a conexões.

10.5.1 - Associações de Longa Duração

Existe uma relação bem estabelecida entre a estação gerente e os dispositivos gerenciados. Mas, no SNMP, este relacionamento é de certa forma vago e indireto. Uma estação não mantém uma comunicação direta com o dispositivo. A medida em que se precisa de informações, uma comunicação é estabelecida e logo depois é desfeita, tornando cada comunicação única. Seria interessante que se tivesse uma associação explícita entre a estação gerente e o agente, partindo-se do pressuposto de que não vai haver apenas uma única troca de informações entre eles, e além de que, possivelmente, depois de uma troca de mensagem, uma outra será feita.

Esta associação seria composta de informações de segurança e outras informações de estado, e deveria existir, quando possível, uma conexão de transporte aberta entre o gerente e o agente. Esta abordagem simplifica muito as questões relacionadas com segurança, já que a autenticação e a privacidade seriam estabelecidas com o início da associação e só seria necessário uma outra troca de informações de segurança em pontos importantes da associação.

Uma outra vantagem desta abordagem seria uma grande melhoria de desempenho na transmissão de grandes quantidades de dados. Como também já foi apresentado, o SNMP poderia utilizar o TCP como protocolo de transporte, já que as razões apresentadas no início para a utilização de UDP não são mais tão vantajosas.

10.5.2 - Uso de HTTP como Método de Acesso

Na Internet está-se fazendo com grande sucesso uma enorme carga de transações www http, que é baseado em conexões TCP. Na área de gerenciamento de rede, também está crescendo, cada vez mais, a utilização de W*eb*. Muitas empresas estão utilizando *sites* internos para exibir o *status* da rede e informações de desempenho. Tendo este tipo de abordagem menor custo e provendo mais fácil acesso às informações do que as plataformas de gerenciamento de redes usadas até então.

A utilização do HTTP como protocolo de comunicação para gerenciamento traz grandes vantagens. Em primeiro lugar não seria mais necessário software especializado de gerenciamento para monitorar e configurar um dispositivo. Em segundo lugar, poderiam se utilizar conexões do HTTP com maior eficiência no transporte de grande quantidade de dados. Em terceiro lugar, problemas de versões que ocorrem quando um antigo agente ou gerente não mais suportam o novo seriam diminuídos. Outra grande vantagem é a independência de plataforma e de localização

da aplicação. E, finalmente, a integração com documentação on-line, que pode ser facilmente produzida.

Como desvantagem temos que uma conexão TCP para se trazer apenas uma variável não vale a pena. Outra questão é o problema da padronização das informações que devem ser exportadas pelos agentes. O problema é que a carga de como mostrar as informações ficaria com o agente. Mas, isto seria um problema apenas para dispositivos mais simples.

Um outro problema apontado é que a utilização do TCP para grandes transportes de dados não traz tantos ganhos em comparação com a mensagem *get-bulk*.

10.6 - APLICAÇÕES DE GERENCIAMENTO

Os padrões SNMP vêm sendo utilizados com muito sucesso já há algum tempo devido a sua grande capacidade de se adequar a aplicações específicas de dispositivos, bastando para isto o fabricante construir uma MIB e um agente que saiba tratar os dados representados nesta MIB. Apesar do SNMP em si ser relativamente "simples", há um certo trabalho para dar suporte a uma MIB no agente. Há ainda mais trabalho para construir o suporte de gerenciamento para utilizar os dados da MIB, e ainda um pouco mais quando se fala em desenvolver o gerenciamento nas várias plataformas existentes para gerenciamento de redes.

Alguns dispositivos hoje podem ser comparados às estações de gerenciamento de alguns anos atrás em termos de capacidade de processamento. Além disso, o emprego de um servidor HTTP/HTML não é tão mais complexo e não utiliza muito mais memória que um agente SNMP. Com isso, o fabricante de dispositivos pode vender um produto mais completo em termos de gerenciamento. Seu produto inclui suas próprias funções de gerenciamento e não depende de nada, exceto de um *browser* WWW para fazer o gerenciamento. E, no que diz respeito às funções de gerenciamento, o fabricante pode controlar tudo em relação ao dispositivo e seu gerenciamento, indo desde a operação até a sua GUI.

Capítulo 11 – Gerência Integrada de Redes e Serviços

As redes de telecomunicações podem ser vistas, independente do tipo e dos equipamentos utilizados, como dividida em três níveis principais: aplicação, serviço e arquitetura.

- **Camada de aplicação -** é aquela empregada diretamente pelo usuário final;
- **Camada de serviço** - deve ser projetada pelo provedor de rede para suportar todas as aplicações do usuário;
- **Camada de arquitetura -** provê as soluções de engenharia que devem prover o transporte de qualquer tipo de serviço vendido pela operadora ao usuário. O serviço é normalmente designado como a facilidade que o provedor vende a seus clientes e tipicamente suporta várias aplicações.

A necessidade de qualidade, a diversificação e a complexidade cada vez maior destes serviços implica em uma necessidade tão vital quanto o próprio serviço: a sua gerência.

Dentro deste conceito de gerenciamento de redes de telecomunicações, começaram a surgir alguns sistemas de supervisão específicos para cada situação (por exemplo, gerenciamento de falhas, de tráfego) e para cada fabricante, ou seja, os chamados sistemas de gerência proprietários. Podemos ter os equipamentos como sendo várias centrais telefônicas de fabricantes distintos, cada uma com seu próprio sistema de gerência. As centrais são interligadas entre si, mas os sistemas de gerência são isolados. Este tipo de sistema possui alguns problemas, como:

- A impossibilidade de interconexão entre sistemas de diferentes fabricantes devido ao uso de interfaces não padronizadas;
- Multiplicidade de sistemas: para cada novo tipo de equipamento/fabricante é necessário um novo sistema de supervisão específico;
- Multiplicidade de terminais e formas de operação: cada sistema tem seus próprios terminais e linguagem de comunicação homem-máquina;
- Multiplicidade de base de dados: cada sistema tem a sua própria base de dados local, sendo necessário atualizar cada sistema isoladamente, o que acaba resultando em duplicidades e inconsistências.

Estes fatores acarretam em uma falta de integração entre processos que impossibilita, por exemplo:

1. Obtenção de uma visão global do estado da rede e dos serviços;
2. Integração de forma automatizada das atividades operacionais;
3. Difusão de informações dos estados de circuitos e serviços de uma forma ampla;
4. Flexibilidade de roteamento na rede;
5. Operação e manutenção eficientes.

Como conseqüência disto, temos elevação do índice de falhas não detectadas, congestionamento na rede, falta de flexibilidade no roteamento, indicação múltipla da mesma falha, dados insuficientes para planejamento e deficiência de operação e manutenção, que acarretam em perda de ligações e de receitas, insatisfação do usuário e desperdício pelo aumento dos custos operacionais e investimentos extras.

Baseado nestes fatores tem-se procurado uma solução para o problema da falta de integração entre os sistemas, que possibilite a Gerência Integrada de Redes e Serviços (GIRS).

11.1 - Conceito de GIRS

Define-se GIRS como o conjunto de ações realizadas visando obter a máxima produtividade da planta e dos recursos disponíveis, integrando de forma organizada as funções de operação, manutenção, administração e aprovisionamento (OAM&P) para todos os elementos, rede e serviços de telecomunicações. A gerência deve ser integrada no sentido de:

- Ser única para equipamentos semelhantes de fabricantes distintos;
- Ser feita de maneira consistente pelos vários sistemas;
- Ser feita desde o nível de serviço até o nível dos equipamentos;
- Um operador ter acesso a todos os recursos pertinentes ao seu trabalho, independentemente do sistema de suporte à operação onde estes recursos estão disponíveis ou da sua localização geográfica;
- Os sistemas se "falarem" de modo que as informações fluam de maneira automática.

Para se atingir este objetivo, é necessário, então:

- Processos operacionais com fluxo contínuo;
- Facilidades de reconfiguração em tempo real;
- Dados em tempo real agilizando a manutenção;
- Detecção da causa raiz das falhas;
- Terminal de operação universal com apresentação padrão;
- Eliminação da multiplicidade de sistemas de supervisão;
- Dados de configuração confiáveis.

11.2 - Requisitos básicos de gerência

Para se chegar à integração das funções de gerência é necessário cumprir alguns itens básicos:

- Elaboração de um modelo conceitual de operação, administração, manutenção e aprovisionamento baseado nos objetivos e estratégias da empresa;
- Padronização dos modelos de informações de elementos de rede e serviços de telecomunicações;
- Padronização das interfaces homem-máquina;
- Automação de tarefas visando eficiência;
- Flexibilidade de arquitetura;
- Ambiente aberto, permitindo interconectividade e interoperabilidade;
- Alta confiabilidade e segurança.

11.3 - Objetivos Básicos

Integrando as funções de todas as camadas funcionais, podemos atingir alguns objetivos gerenciais, como:

- Minimizar o tempo de reação a eventos da rede;
- Minimizar a carga causada pelo tráfego de informações de gerenciamento;
- Permitir dispersão geográfica do controle sobre os aspectos de operação da rede;
- Prover mecanismos de isolação para minimizar riscos de segurança;
- Prover mecanismos de isolação para localizar e conter falhas na rede;
- Melhorar o serviço de assistência e interação com os usuários.

Referências Bibliográficas

[Bierman e Iddon 1996] Bierman, A., e Iddon, R., *Remote Network Monitoring MIB Protocol Identifiers, Internet Draft*, Janeiro de 1996.

[Bruins 1996] Bruins, B*. Some Experiences with Emerging Management Technologies*. The Simple Times, Volume 4, nº3, Julho de 1996.

[Burns e Quinn 1996] Burns, R. e Quinn M. *The Cyber Agent Framework*. The Simple Times, Volume 4, nº3, Julho de 1996.

[Case et al. 1990] Case, J. D., Fedor, M. S., Schoffstall, M. L., and Davin, C. *Simple Network Management (SNMP)*, RFC 1157, Maio 1990.

[Case et al. 1993] Case, J. D., McCloghrie, K., Rose, M. T., and Waldbusser, S. *An Introduction to Version 2 of the Internet-Standard Network Management Framework*, RFC 1441, Abril de 1993.

[Goldszmidt e Yemini 1993] Goldszmidt, G. e Yemini, Y*. Evaluating Management Decisions via Delegation*. Columbia University, Estados Unidos, Abril de 1993.

[Goldszmidt e Yemini 1995] Goldszmidt, G. e Yemini, Y*. Distributed Managemente by Delegation*. Ph.D Tese. Columbia University, Estados Unidos, Junho 1995.

[Goldszmidt 1996] Goldszmidt, G. *Distributed Managemente by Delegation*. Ph.D Tese. Columbia University, Estados Unidos, Abril 1996.

[Hunt 1992] Hunt, Craig. *TCP/IP Network Administration*. OÆReilly & Associates, Inc., 1992.

[ISO 1991] Information Technology Open Systems Interconection. *Common Management Information Protocol Specification*. Technical Report IS 9596, International Organization for Standardization, Maio 1991.

[McGloghie and Rose 1991] McCloghrie, K., Rose, M. T. *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II,* RFC 1213 Março 1991.

[Meira 1996] Meira, S. R. L. *Novos Paradigmas de Programação na Internet.* , 1996.

[Mullaney 1996] Mullaney, P*. Overview of a Web-based Agent*. The Simple Times, Volume 4, nº3, Julho de 1996.

[Rose and McGloghie 1990] Rose, M. T., McCloghrie, K. Structure and Identification of Management *Information for TCP/IP-based Internets*, RFC 1155, Maio de 1990.

[Stallings 1993] Stallings, William. *SNMP, SNMPv2, and CMIP - The Practical Guide to Network-Management Standards*. Addison Wesley, 1993

[Stallings 1996] Stallings, William. *RMON2 The Next Generation of Remote Netork Monitoring*. Connexions, vol 10, nº5, pág. 34-40, Maio de 1996.

[Stevens 1994]. Stevens, W. R. *TCP/IP Illustrated, Volume 1 - The Protocols*. Addison Wesley. 1994.

[Stevenson] Stevenson, D. W. *Network Management - What it is and what it isnÆt*.

[Tepedino 1996] Tepedino, J. F. *HTTP: Hypertext Transfer Protocol*. 1996.

[Uchôa 1995] Uchôa, R. C. *Suporte para Monitoramento e Controle de Carga em Ambientes Distribuídos.* Dissertação de Mestrado. Departamento de Informática PUC-RIO. Rio de Janeiro. 1995.

[Waldbusser 1991] Waldbusser, S., *Remote Network Monitoring Management Information Base*, RFC 1271, Novembro de 1991.

[Waldbusser 1993] Waldbusser, S., *Token Ring Extensions to the Remote Network Monitoring MIB*, RFC 1513, Setembro de 1993.
[Waldbusser 1995] Waldbusser, S., *Remote Network Monitoring Management Information Base*, RFC 1757, Fevereiro de 1995.
[Waldbusser 1996] Waldbusser, S., *Remote Network Monitoring MIB Version 2*, Internet Draft, Janeiro de 1996.
[Wellens e Auerbach 1996] Wellens, C. e Auerbach, K. *Towards Useful Management*. The Simple Times, Volume 4, nº3, Julho de 1996.
LAN - Uma introdução completa a Redes Locais - pelos redatores da Lan Magazine. Rio de Janeiro, RNP, 1994.
Neuman, J. Oliveira, A.; *Curso Avançado sobre Gerenciamento de Redes*. LAR - Laboratório Multiinstitucional de Redes e Sistemas Distribuídos - ETFCE - UFC - UECE. 1995.
Menezes, E.; *Gerenciamento de Redes: Estudos de Protocolos*. Workshop de Administração e Integração de Sistemas. Departamento de Informática. Universidade Federal de Pernambuco. Setembro de 1998.
Gerenciamento de Redes - Uma abordagem de Sistemas Abertos. Makron Books do Brasil, 1993
Sun Microsystems Business-Sun Connect, SunNet Manager 1.1 - Installation and User's Guide. 1991, p. 1-6.
AT&T Telecomunications Web Page. URL: http://www.att.nl/
*HP Openview Web Page.*URL: http://www.openview.hp.com/
STALLINGS, W.; *SNMP, SNMPv2 and CMIP The Practical Guide to Network-Management Standards*; Addison Wesley; 1993.
Tutorial sobre SNMP – UFRGS - URL:
http://penta.ufrgs.br/gr952/trab1/snmp_snmp.html
Gerenciamento de Redes: Conceitos Básicos sobre os Protocolos SNMP e CMIP -
URL: http://www.gta.ufrj.br/~alexszt/ger/snmpcmip.html
Intellinet technologies
URL: http://www.intellinet-tech.com/glossary/cmip.html
Definições de Gerência de Redes
URL: http://penta.ufrgs.br/~guga/gerencia/definicoes.html
Network Management
URL: http://netman.cit.buffalo.edu/Doc/DStevenson/
Network Management for the 90s
URL: http://www.sce.carleton.ca/netmanage/NMfor90s/SimpleNM.html
Yacc labs ltd - Network management
URL: http://www.yacc.co.uk/netman/netman.html
Simple Network management protocol - SNMP URL:
http://penta.ufrgs.br/gr952/trab1/snmp_snmp.html
Roxen Community: RFC 1098 A Simple Network Management Protocol SNMP - URL:
http://www.roxen.com/rfc/rfc1098.html
Remote Monitoring (RMON)
http://www.geocities.com/SiliconValley/Vista/5635/cap5.html
___, "TCP/IP Tutorial and Technical Overview", International Technical Support Center
___, NetView 6000 Programmers Guide, IBM
___, NetView 6000 Reference Guide, IBM

BRISA, “Gerenciamento de Redes - Uma abordagem de Sistemas Abertos”, Makron Books, 1992
Carrilho, J. A, Madeira, E. R. M., “Gerência por Domínios”, 12º Simpósio Brasileiro de Redes de Computadores, Anais vol. II, Curitiba, maio de 1994
Case, J., Fedor, M., Schoffstalll, M. e Davin, J., “A Simple Network Management Protocol (SNMP) (RFC 1157), ,aio de 1009
Commer D. C. , Stevens, D. L., “Internetworking with TCP/IP - Design Implementation and Internals”, Volume II, , Prentice Hall Segunda Edição, USA, 1992
Commer, D. C., “Internetworking with TCP/IP - Principles, Protocol and Architecture”, Volume I, Prentice Hall Segunda Edição, USA, 1991
Leuca, J. E, Estphall, C, B, Specialski, E. S., “Uma Arquitetura de Segurança para Gerência de Redes”, 12º Simpósio Brasileiro de Redes de Computadores, Anais vol II, Curitiba, maio de 1994
McCloghrie, K. e Rose, M. T., “Management Information Base for Networkk Management of TCP/IP based Internets (RFC 1156)”, maio de 1990.
Moutinho, C. M, Stanton. M. A, “Aplicações de Gerenciamento de Redes Inteligentes” 12º Simpósio Brasileiro de Redes de Computadores, Anais vol I, Curitiba, maio de 1994
Rocha, M. A, Westphall, C. B “Gerência de Redes de Computadores através de novos Agentes”, 12º Simpósio Brasileiro de Redes de Computadores, Anais vol II, Curitiba, maio de 1994
Stalllings, W., “Data and Computer Communications”, Macmillan Publishing Co., Segunda Edição, USA, 1998.
Tanembaum, A. S., “Modern Operationg Systems”, Prentice-Hall Inc., USA, 1992.
Weissheimer, C. G, Tarouco L. M. R, “Distribuição da Gerência na Rede”, 12º Simpósio Brasileiro de Redes de Computadores, Anais vol I, Curitiba, maio de 1994