UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

INTERFACE DE CONTROLE DE ACESSO PARA O MODELO DE GERENCIAMENTO OSI

por

Alexandre Moraes Ramos

Dissertação submetida como requisito parcial
para obtenção do grau de
Mestre em Ciência da Computação

Prof. Elizabeth S. Specialski
Orientadora

Florianópolis, Agosto de 1994

INTERFACE DE CONTROLE DE ACESSO
PARA O MODELO DE GERENCIAMENTO OSI

ALEXANDRE MORAES RAMOS

ESTA DISSERTAÇÃO FOI JULGADA PARA OBTENÇÃO DO TÍTULO DE

MESTRE EM CIÊNCIA DA COMPUTAÇÃO

ESPECIALIDADE SISTEMAS DE COMPUTAÇÃO E APROVADA EM SUA FORMA

FINAL PELO PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Profa. Elizabeth Sueli Specialski, M.Sc.
Orientadora

Prof. Hermann Adolf Harry Lücke, Dr.Ing.
Coordenador do Curso

BANCA EXAMINADORA

PRESIDENTE: Profa. Elizabeth Sueli Specialski, M.Sc.

Prof. Carlos Becker Westphall, Dr.

Prof. Rafael T. de Sousa Junior, Dr.

Aos meus pais Ary e Wanda
pelo amor, incentivo e carinho.

A minha ***Ana***
com muito amor...

AGRADECIMENTOS

Agradeço a todos que contribuiram de alguma forma para que eu pudesse realizar este projeto.

Meu agradecimento especial à professora e amiga Elizabeth Specialski por acreditar e apoiar este trabalho, pela paciência e notório saber.

Muito obrigado a toda minha família pelo amparo e força de sempre: Wania, André, Ângelo, Dulce, Tatiana, Ana Paula, Rafael, Mariana e Ana Cecília.

Agradeço a família Wisintainer pela especial acolhida em Florianópolis.

Ao meu amigo Ceará (Vicente Lima) pelas árduas horas de trabalho e companheirismo nesta jornada.

Aos meus amigos: Marisa Jordan, Hamilton Lourenço (Bsb), Simone Pereira Ilha (Bsb), Claudinha (moreníssima), Carla Merkle, Verinha (madalena) e Carlos Montez pelo grande incentivo.

A todo o Grupo de Redes de Computadores da Universidade Federal de Santa Catarina.

Aos amigos do Ministério da Educação, em especial: Clayton Geraldo (CRH), Vera Lúcia T. de Assis (CRH), André Nóia (CRH), Prof. Rúbia (Capes), Alba Peixoto (Demec/SC), Márcia (Demec/SC), a CRH e a todos os meus amigos.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ACD - Access Control Descriptor

ACI - Access Control Information

ACSE - Access Control Service Element

ADF - Access Control Decision Function

AEF - Access Control Enforcement Function

AOO - Abordagem Orientada a Objetos

AP - Application Process

ASEs - Application Service Elements

BDA - Base de Dados de Autorização

CMIP - Commom Management Information Protocol

CMIPM - Commom Management Information Protocol Machine

CMISE - Commom Management Information Service Element

DN - Distinguished Name

DOM - Identificador de Domínio

Grb - Group-based

IA - Identificador de Associação

IAG - Identificador de Processo Agente

IAT - Identificador de Atributo de Classe

IC - Informação de Contexto

ICA - Interface de Controle de Acesso

ICO - Identificador de Classe de Objeto Gerenciado

IdG - Identificador de Grupo de Iniciador

IdI - Identificador de Iniciador

ILCA - Identificador de Lista de Controle de Acesso

ILOG - Identificador de Lista de Instâncias de Objeto Gerenciado

Inb - Individual-based

IOG - Identificador de Objeto Gerenciado

IRO - Identificador de Rótulo

ISO - International Organization for Standardization

LCA - Lista de Controle de Acesso

LCO - Lista de Classes de Objeto Gerenciado

LME - Layer Management Entity

LOG - Lista de Instâncias de Objeto Gerenciado

LPA - Lista de Processo de Aplicação

MIB - Management Information Base

MIT - Management Information Tree

Mls - Multi-level Security

Mms - Modelo Militar de Segurança

NC - Identificador de Nível de Clearence

NS - Identificador de Nível de Sensibilidade

OG - Objeto Gerenciado

OP - Operação de Gerenciamento

OSI - Open Systems Interconnection

OSIMIS - Open Systems Interconnection Management Information Service

PA - Processo de Aplicação

PDUs - Protocol Data Units

RDN - Relative Distinguished Name

Rob - Role-based

ROSE - Remote Operation Service Element

SCA - Sistema de Controle de Autorização

SDA - Sistema de Definição de Autorização

SMAE - System Manegement Application Entity

SMASE - System Management Application Service Element

SMI - Structure Management Information

SMIB - Security Management Information Base

TAP - Tipo de Política de Acesso

TCP/IP - Transmission Control Protocol/ Internet Protocol

UFSC - Universidade Federal de Santa Catarina

RESUMO

As atividades de muitas organizações passaram a depender enormemente das redes de computadores, aumentando a importância do perfeito funcionamento destas. A necessidade de se manter uma rede sempre operando eficientemente tornou o gerenciamento dessas redes vital para as organizações.

Entretanto, o gerenciamento de redes, como qualquer aplicação, também, tem suas necessidades de segurança. A utilização de mecanismos de segurança para proteger as aplicações de gerência, decorre do fato de que estas aplicações manipulam informações extremamente sensíveis e valiosas para a manutenção da rede em perfeito funcionamento.

Um usuário, ao utilizar uma aplicação qualquer, normalmente, jamais teria acesso a informações tão importantes quanto as disponíveis através de um sistema de gerenciamento de redes. Portanto, deve-se controlar o acesso às informações de gerenciamento, não permitindo que pessoas não autorizadas possam manipulá-las, fazer uso ou mesmo divulgá-las incorretamente, pois, caso contrário, pode-se comprometer o desempenho da gerência e da própria rede.

Dentro desse contexto, este trabalho descreve uma Interface de Controle de Acesso, destinada às autoridades de segurança de sistemas de gerenciamento, que visa auxiliar a implementação de políticas de controle de acesso em sistemas com funcionalidade OSI.

ABSTRACT

The activities of many organizations became widely dependent of computer networks, increasing the importance of their perfect working. The necessity to mantain a network always operating efficiently turned the network management fundamental to the organizations.

However, just like any application, the network management also has security requeriments. The use of security mechanisms to protect the management applications arises because such applications deal with very sensible and valuable information to keep the network in perfect working.

Normally, a user dealing with any applications would never access very important information such as the available ones to the network management system. This way, the access to management information must be controled, preventing unauthorised people to manipulate them, make use or incorretly publish them, otherwise, can compromise the management and network performance.

In this context, this work describes an Access Control Interface dedicated to the security authority in management system, intends to help the implementation control access policies in systems with OSI funcionality.

1. INTRODUÇÃO

Uma rede de computadores pode ser definida como um conjunto de equipamentos autônomos e interligados com a finalidade de compartilhamento de recursos lógicos e físicos. Este compartilhamento é alcançado graças à facilidade para a troca de informações possibilitada pela interoperação dos sistemas residentes nos equipamentos interconectados.

O alcance da interoperabilidade só é possível se forem utilizadas interfaces comuns entre os sistemas comunicantes. Neste sentido, o Modelo de Referência para Interconexão de Sistemas Abertos (RM-OSI), da Organização Internacional para Padronização (ISO - *International Organization for Standardization*), oferece um conjunto de normas que oferecem soluções para os problemas de integração e limitação entre as diferentes interfaces de comunicação.

A manutenção do funcionamento de uma rede de computadores em níveis satisfatórios requer a utilização de aplicações qúe permitam o gerenciamento da rede. A ISO propôs a adição de um esquema básico de gerenciamento ao Modelo de Referência OSI, para possibilitar o desenvolvimento de sistemas em gerência de redes de computadores e sistemas de comunicação. Este esquema básico especifica um ambiente de gerenciamento no qual encontram-se funções de gerência, serviços e protocolos para troca de informações de gerência, necessárias para suportar o controle e a monitoração dos sistemas e recursos associados.

Dentro do esquema básico de Gerência de Redes, a ISO estabelece cinco áreas funcionais com objetivos bem definidos, que buscam resolver problemas relativos respectivamente a: falhas de componentes; níveis de desempenho alcançados; configuração da rede; contabilização; e segurança.

Cada área funcional contém funções de gerência que incluem requisitos, modelos e serviços. As funções são responsáveis por coletar informações junto aos componentes da rede e colocá-las à disposição da gerência. Estas informações são pré-processadas e comparadas com a política de gerência definida para rede. A análise desta comparação resulta em um processo de tomada de decisão que visa garantir a colocação em prática da política definida para a rede e, consequentemente, o perfeito funcionamento da rede.

A área de gerenciamento de Segurança é suportada pelas funções de Alarme de Segurança, de Auditoria e de Controle de Acesso que visam controlar, coordenar e monitorar os serviços e mecanismos de segurança definidos pela política de segurança adotada por uma rede. A função de Controle de Acesso tem como objetivo impedir que usuários não autorizados tenham acesso às informações manipuladas pelo sistema de gerenciamento.

Este trabalho tem como objetivo descrever uma Interface de Controle de Acesso, para dar suporte à implementação de políticas de controle de acesso em sistemas de gerenciamento com funcionalidade OSI.

O capítulo 2 apresenta o Modelo Básico de Referência OSI, os conceitos básicos e aspectos de gerência OSI, descrevendo o Modelo de Informação, o Modelo Funcional e o Modelo de Comunicação.

No capítulo 3, descreve-se modelos de política de acesso utilizados para proteção contra acessos não autorizados. Faz-se uma abordagem da Arquitetura de Segurança OSI, que contém os serviços e mecanismos que possibilitam a implementação das política de acesso. São descritas, também, as Funções de Gerência OSI, que visam garantir que as políticas sejam colocadas em prática conforme a sua definição.

No capítulo, 4 apresenta-se a Interface de Controle de Acesso, seus componentes e funcionalidades propostas, a interligação entre os diversos componentes da Interface, seu fluxo de comunicação interno e o seu relacionamento com os sistemas de gerenciamento.

O capítulo 5 contém a integração da Interface de Controle de Acesso à plataforma de suporte ao gerenciamento da Rede Local UFSC. Descreve-se o modelo da plataforma de suporte, enfatizando-se seus princípios básicos e componentes mais importantes. Em seguida, mostra-se a localização da Interface dentro da plataforma de suporte, suas implicações e justificativas para implementação. E, por último, aborda-se o relacionamento da Interface com os componentes da plataforma de suporte ao gerenciamento.

O capítulo 6 apresenta considerações sobre o desenvolvimento deste trabalho e sugestões para a continuidade do projeto de desenvolvimento e implementação da Interface de Controle de Acesso.

O apêndice A contém a especicação da Interface de Controle de Acesso em termos das classes de objeto criadas para dar suporte a implementação do protótipo da Interface que podem ser observadas através da hierarquia de herança. Apresenta, também, o relacionamento desta com a plataforma de suporte ao gerenciamento da Rede Local UFSC.

2. MODELO OSI

2.1 Modelo de Referência

O conceito de Gerência de Sistemas foi introduzido em [ISO 7498-1 - *Open Systems Interconnection: Basic Reference Model*], elaborado e aprofundado em [ISO 7498-4 - *OSI Management Framework*] [ISO 10040 - *Systems Management Overview*]. O Modelo de Referência OSI [ISO 7498-1] foi criado para permitir a interconexão de sistemas abertos que estejam de acordo com os padrões OSI.

Cada sistema aberto em uma rede de comunicação OSI é composto de um conjunto lógico de 7 níveis ou camadas sucessivas (Figura 2.1). Cada nível contém um conjunto bem definido de funções envolvidas na comunicação de dados. Os níveis são constituídos de uma ou várias entidades, as quais são objetos lógicos dentro de um nível e executam um conjunto bem definido de funções, em associação com outras entidades de mesmo nível de outros sistemas abertos.

A associação entre entidades de mesmo nível de sistemas abertos se dá através do protocolo do nível. Cada nível possui um protocolo que permite a suas entidades lógicas trocarem informações com entidades de mesmo nível de outros sistemas abertos, a fim de permitirem a interconexão dos sistemas em questão (Figura 2.1).

Cada nível, dentro de seu sistema aberto, fornece um conjunto definido de serviços para o nível superior e requer serviços do nível inferior. Os níveis são independentes e isolam os níveis superiores dos detalhes das implementações dos níveis inferiores.

As características de um nível podem ser trocadas sem afetar o resto do sistema aberto. Por exemplo, numa determinada camada, um protocolo orientado a caracter pode ser substituído por um protocolo orientado a *bit*. A maior vantagem desta independência dos níveis é a possibilidade do usuário alterar os produtos de comunicação OSI para satisfazer às necessidades particulares da rede [HEL92].

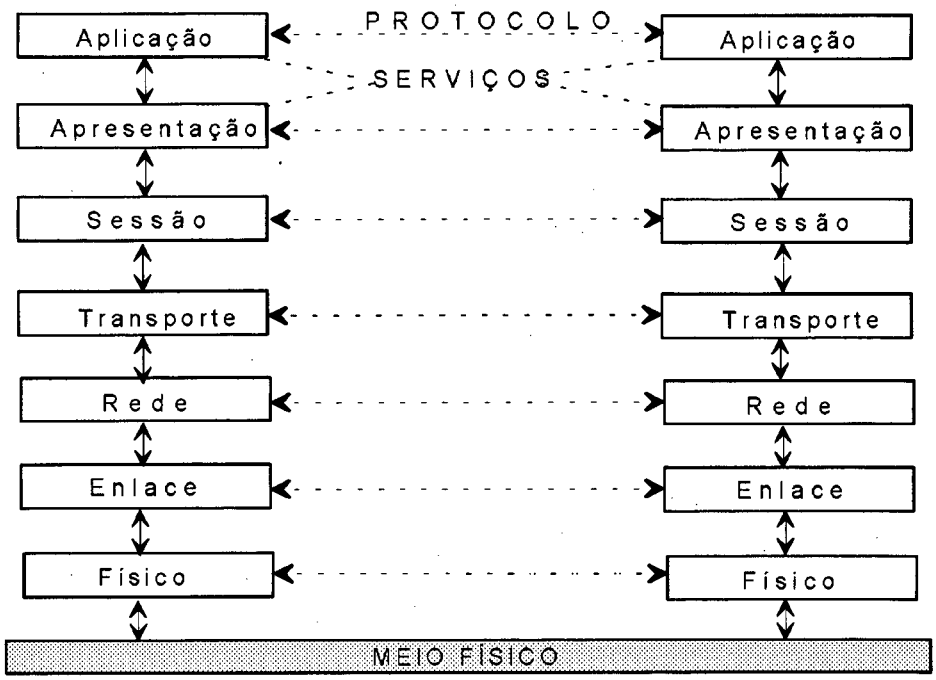


Figura 2.1 - Modelo de Referência OSI

2.1.1 Camadas do Modelo OSI

Nível Físico: é a camada mais baixa e o nível mais básico. Fornece as características mecânicas, elétricas e funcionais de uma conexão física para transmissão de dados entre dispositivos de comunicação (ex: regras de codificação, especificações de frequência, necessidades de cabo e níveis de voltagem). Sua função principal é permitir o envio de dados pela rede sem se preocupar com o significado ou como são agrupados. Como exemplos de interfaces padrão podemos citar: *CCITT V.24/RS-232; RS-422-A; OU RSA-423-A.*

Nível de Enlace: providencia os meios funcionais e os procedimentos para controlar as conexões de ligação de dados entre entidades de rede. Descreve como um dispositivo obtém acesso ao meio especificado na camada física. Detecta e opcionalmente corrige erros que por ventura ocorram no nível físico. Protocolos como *Binary Synchronous Communications* (BSC) e *High-Level Data Link Control* (HDLC) residem neste nível.

Nível de Rede: determina o caminho (rota) que as unidades de dados seguirão da origem até o destino e controla as sub-redes. É responsável pela segmentação, sequenciação e pelo controle do fluxo de dados.

Nível de Transporte: responsável por garantir que os dados recebidos pelo destinatário são corretos e íntegros. Isola os níveis superiores de problemas referentes a transmissão de dados, controla os erros e a sequenciação.

Nível de Sessão: fornece os meios necessários para organizar e sincronizar o diálogo entre duas entidades, chamado de sessão. Administra a troca de informações dentro de uma sessão.

Nível de Apresentação: resolve problemas de diferenças de sintaxe, formato ou código dos dados transmitidos entre o sistema fonte e o sistema destino (Criptografia/Decriptografia, Compressão/Descompressão de dados e ASCII/EBCDIC).

Nível de Aplicação: atua como uma interface, através da qual o usuário tem acesso aos serviços fornecidos pela aplicação do sistema aberto (transferência de arquivos, acesso a base de dados,...). Neste nível encontram-se, também, os serviços e protocolos de gerenciamento de sistemas OSI.

2.2 Modelo de Gerenciamento

O Gerenciamento de Sistemas OSI é realizado através de processos de aplicação que são capazes de monitorar, controlar e coordenar atividades de interconexão entre sistemas abertos. Estas atividades, funções de gerência, são realizadas através da manipulação de objetos gerenciados. Um Objeto Gerenciado pode representar qualquer recurso sujeito à gerência.

Os processos de gerência podem ser Gerentes e Agentes. Um Gerente administra objetos gerenciados, usando informações obtidas junto aos Agentes e através de operações de gerenciamento transmitidas aos Agentes. Um Agente executa operações de gerenciamento sobre os objetos gerenciados e transmite notificações, informações, dos objetos aos Gerentes.

As informações de gerência são armazenadas em uma Base de Informações de Gerenciamento (MIB - *Management Information Base*). A MIB é uma base conceitual de informações de gerenciamento, formada pelos objetos gerenciados. Estes são uma visão abstrata dos recursos da rede que podem ser gerenciados. As trocas de informações de gerência

são feitas através do protocolo de aplicação CMIP (*Commom Management Information Protocol*) [ISO 9596].

A Figura 2.2 apresenta um Sistema Aberto de Gerência que pode ser composto de um ou mais Gerentes trocando informações com um ou vários Agentes. Cada Agente manipula informações sobre os objetos que estão sob seu controle, armazenados na MIB.

A ISO não define como cada Agente deve trocar informações dentro de seu ambiente local, deixando isto a cargo de cada implementação. Ela padroniza as trocas de informações entre Sistemas de Gerência Abertos através do CMIP.

O modelo de gerenciamento OSI é definido através:

- da Estrutura de Gerenciamento;
- dos Modelos de Informação; Funcional; e de Comunicação.

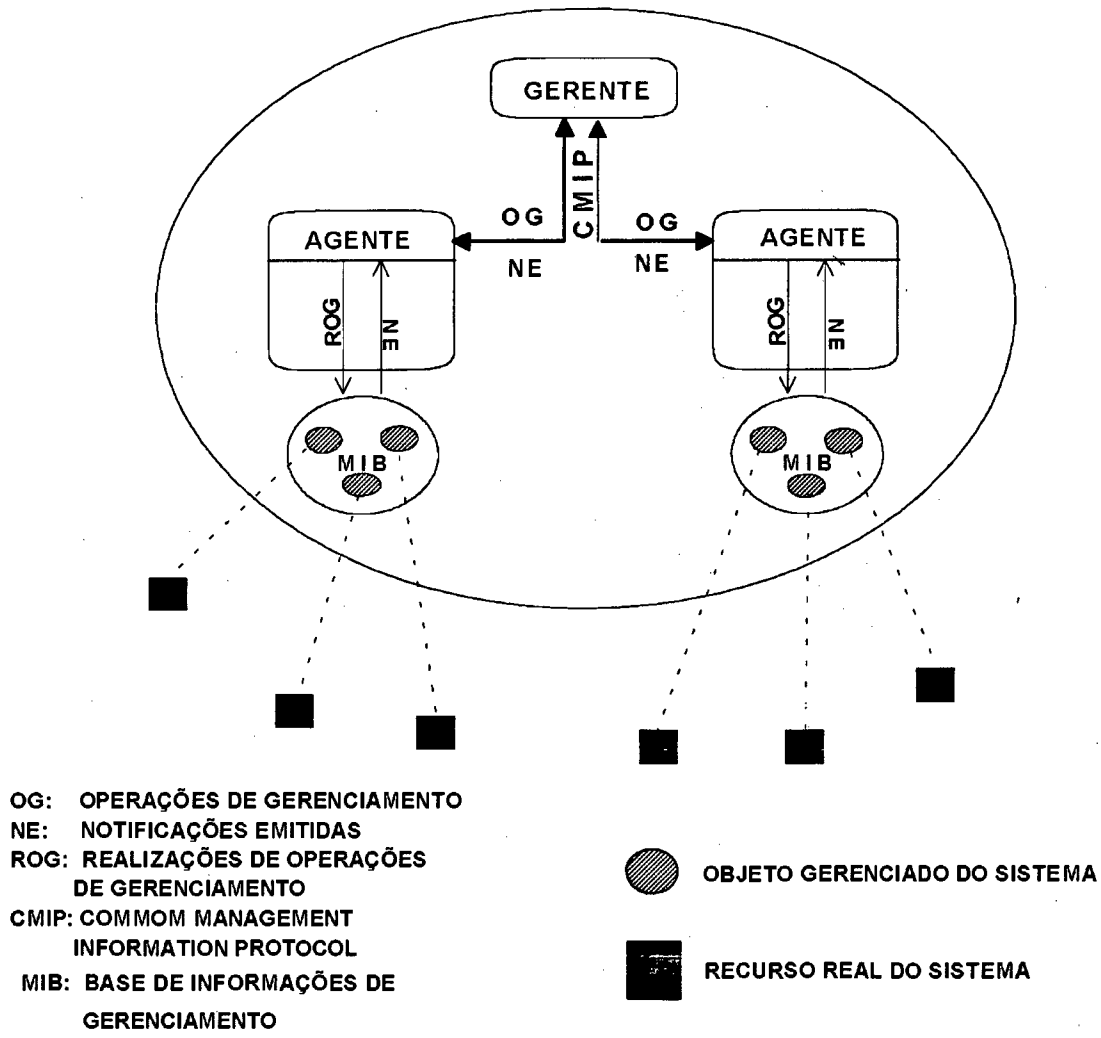


Figura 2.2 - Sistema Aberto de Gerência

2.3 Estrutura de Gerenciamento

A estrutura de gerenciamento OSI é dividida em três áreas de aplicação [ISO 7498-4] [ISO 10040]: gerência de sistemas; gerência de camada; e operação de camada.

Gerência de Sistemas: fornece mecanismos para manipular os recursos gerenciáveis associados a quaisquer ou a todas as camadas do Modelo de Referência. As informações de gerenciamento destes recursos são trocadas entre Entidades de Aplicação de Gerenciamento de Sistemas (SMAE - *System Management Application Entity*). As SMAE são entidades da camada de aplicação responsáveis pela comunicação entre entidades de gerenciamento de sistemas.

Gerência de Camada: fornece mecanismos para monitorar, controlar e coordenar os recursos relacionados com as atividades de comunicação dentro de uma determinada camada, através do uso de protocolos de gerência de sistemas e de protocolos da própria camada. Neste tipo de gerenciamento, cada camada possui uma Entidade de Gerenciamento de Camada (LME - *Layer Management Entity*) que oferece os serviços necessários para gerenciar a própria camada.

Operação de Camada: É a forma mais primitiva de gerenciamento. As atividades de monitoração, controle e coordenação são referentes a uma simples instância de comunicação, através do protocolo específico de cada camada, não necessitando dos protocolos de gerência.

As duas últimas áreas de aplicação do gerenciamento OSI (gerência de camada e operação de camada) são definidas pelas normas que padronizam as respectivas camadas. Já a gerência de sistemas é especificada dentro das normas de gerenciamento OSI.

As normas do Modelo de Referência OSI não permitem que a camada de aplicação acesse diretamente os serviços das outras camadas, exceto os da camada de apresentação. Entretanto, a Gerência de Sistemas consegue manipular recursos de todas as camadas. A SMAE tem acesso às LMEs através das operações sobre os objetos armazenados na MIB [THI93]. A Figura 2.3 apresenta o modelo de gerenciamento.

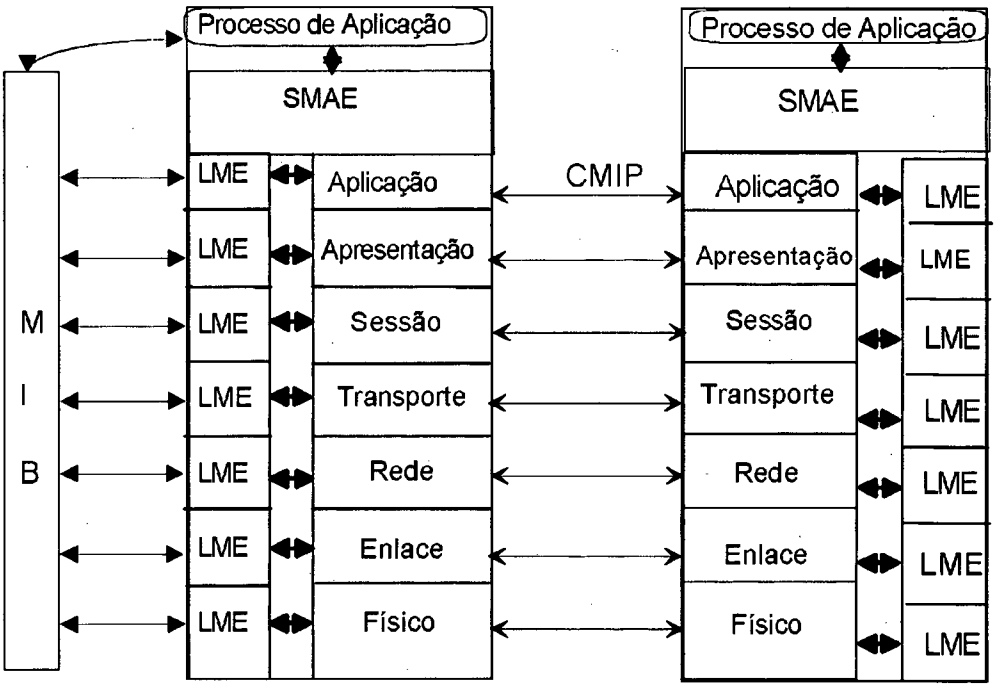


Figura 2.3 - Modelo de Gerenciamento

2.4 Modelo de Informação

O Modelo de Informação é baseado no paradigma da Orientação a Objetos, onde um objeto gerenciado (OG) é uma abstração de um recurso lógico ou físico. Para modelar os objetos, pode-se empregar os recursos do paradigma: classes, atributos, encapsulamento, herança, múltipla herança e alomorfismo, conforme definido pela SMI (*Structure Management Information*) [ISO 10165-1, 2, 3, 4].

Os OG são definidos em termos de seus atributos (propriedades dos recursos), operações (ações sobre os recursos), notificações (eventos relacionados com os recursos) e comportamento (alterações sofridas pelos recursos devido às ações). O conjunto destas informações formam a MIB.

Os OG que compartilham os mesmos atributos, operações, notificações e comportamento pertencem a uma mesma classe de objetos gerenciados. Dada a descrição de uma classe de objetos, pode-se moldar vários objetos dessa classe para uso no gerenciamento. Um objeto moldado, segundo a descrição de uma classe, é chamado de instância dessa classe.

Novas classes podem ser derivadas a partir de classes já existentes. A classe derivada é chamada de subclasse da classe que derivou, e esta, por sua vez, é chamada de superclasse.

As subclasses são derivadas através de uma especialização, ou seja, herdam as características de sua superclasse. Os OG devem obedecer regras de compatibilidade e herança definidas pelas normas da SMI.

O relacionamento entre subclasse e superclasse resulta em uma hierarquia, chamada hierarquia de herança ou árvore de herança (Figura 2.4).

A hierarquia de herança de classes de objetos gerenciados começa com a classe *TOP* que é uma superclasse de todos os objetos gerenciados. Esta classe não permite instanciação, porém contém características importantes do sistema de gerência. A Figura.2.5 mostra a hierarquia de herança do modelo de informação OSI com algumas classes já definidas na SMI, classes que podem ser utilizadas por qualquer sistema de gerência.

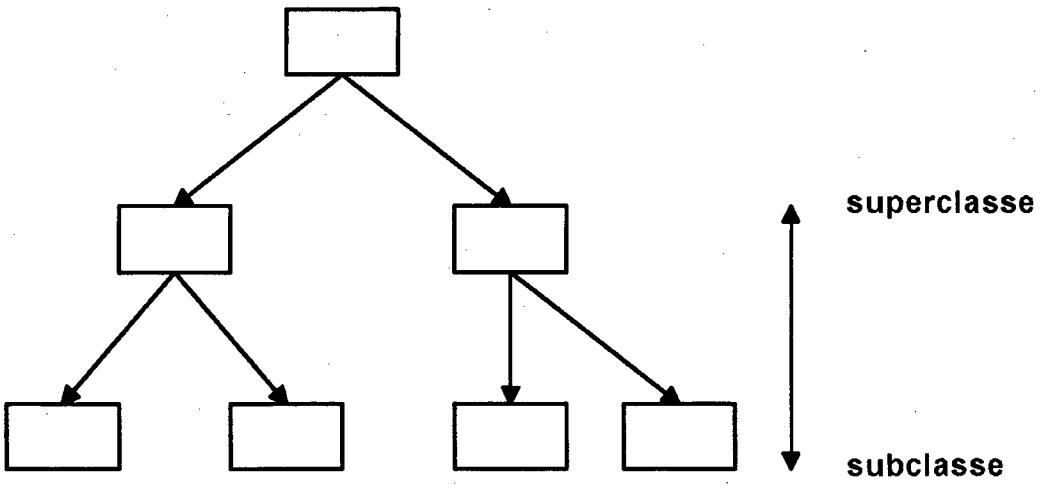


Figura 2.4 - Hierarquia de Herança

Adicionalmente à modelagem das classes de objetos gerenciados, em conformidade com o relacionamento de herança, a informação deve ser estruturada dentro de uma hierarquia de *containment*, chamada de hierarquia de nomeação, onde instâncias de objetos gerenciados podem estar fisicamente ou logicamente contidas dentro de instâncias de outros objetos [COS93].

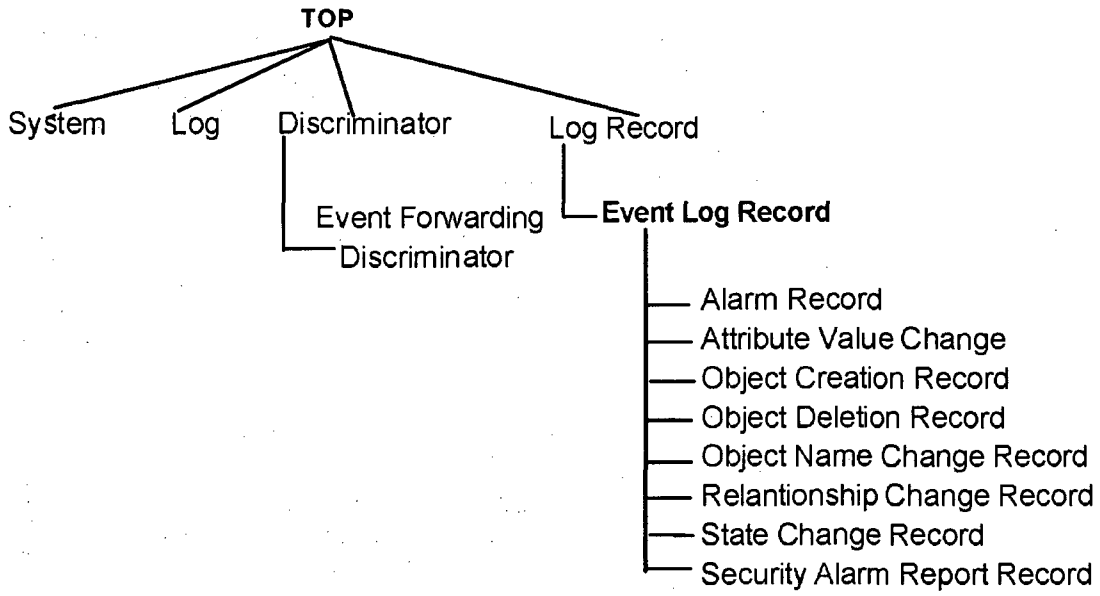


Figura 2.5 - Hierarquia de Herança OSI

A hierarquia de nomeação não implica em herança de características de uma classe superior, mas sim na definição dos relacionamentos entre objetos. Um OG pode conter outros objetos da mesma classe ou de classes diferentes. O OG que contém outros objetos é chamado de superior e os objetos contidos são chamados de subordinados. Por exemplo, uma instância de um objeto *equipamento* pode estar contida em uma instância de um objeto *nó*, isso modela o relacionamento e não implica que a classe do objeto *equipamento* herda atributos da classe do objeto *nó*. Para cada classe de objeto, uma ou mais regras devem ser definidas para identificar a classe superior. Estas regras são chamadas de *name-bindings*.

A hierarquia de nomeação estabelece os relacionamentos entre instâncias de objetos com seus respectivos nomes. Visto que podem existir muitas instâncias de uma classe de OG, cada instância deve ser acessada ou manipulada dentro do sistema de gerência por um único nome distinto, para evitar ambiguidades. Para permitir a construção de nomes únicos associados a cada instância de um OG, uma estrutura de hierarquia de nomeação foi adotada no gerenciamento OSI.

Os OGs são definidos em termos de seus atributos e estão organizados hierarquicamente na Árvore de Informação de Gerenciamento (MIT - *Management Information Tree*) constituindo a MIB (Figura 2.6).

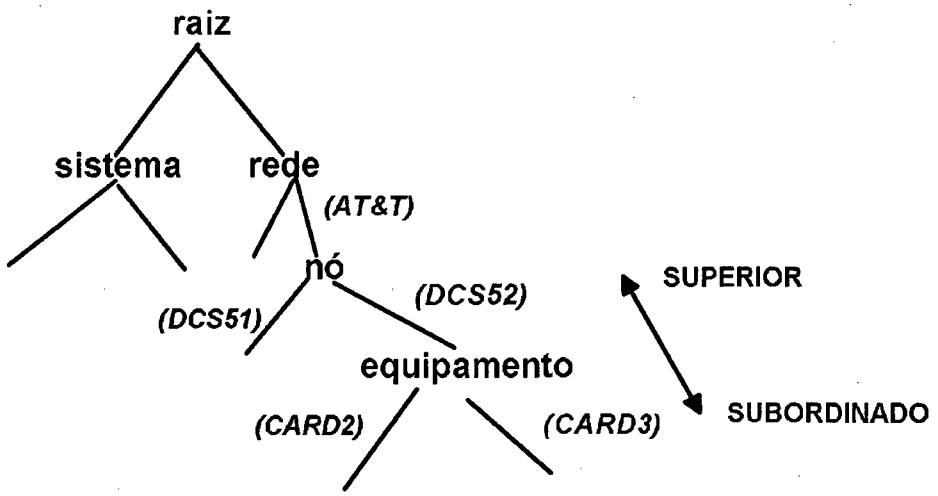


Figura 2.6 - Hierarquia de Nomeação

Cada OG possui um nome característico simples (RDN - *Relative Distinguished Name*), relacionado com o nome do recurso que ele representa de forma abstrata. Portanto, o nome do OG dentro da hierarquia (DN - *Distinguished Name*) é estabelecido através da concatenação do DN de seu superior com o seu próprio RDN (Figura 2.7).

CLASSE DO OG	RDN	DN
Raiz	( )	( )
Rede	(NetId=AT&T)	(NetId=AT&T)
Nó	(NodeId=DCS52)	(NetId=AT&T,NodeId=DCS52)
Equipamento	(UnitId=CARD3)	(NetId=AT&T,NodeId=DCS52,UnitId=CARD3)

Figura 2.7 - Nome de um Objeto Gerenciado dentro de uma Hierarquia de Nomeação

A hierarquia de herança caracteriza somente a estrutura estática. Não estabelece a situação atual do sistema. A real representação dinâmica do sistema é alcançada pela hierarquia de nomeação [THI93].

A MIB é uma visão abstrata de todos os objetos da rede que são importantes para o gerenciamento. A SMI fornece os meios para especificar os objetos contidos na MIB, mas não estabelece o dispositivo fisico de armazenamento (memória principal, arquivos, base de dados, ...). Além disso, define o conjunto de operações que pode ser realizado sobre os OG da MIB e o comportamento destes objetos mediante a execução dessas operações.

2.4.1 Alormorfismo

O alomorfismo é uma das propriedades da SMI que mais força e flexibilidade dá à modelagem dos objetos gerenciados no padrão de gerência de redes OSI [PAV93].

O alomorfismo refere-se a capacidade de uma instância de uma subclasse, dita alomórfica, parecer com sua superclasse. A subclasse é um tipo especial de especialização da sua superclasse, onde os dados e métodos encapsulados nas superclasses são redefinidos com restrições na subclasse alomórfica.

As restrições podem ser feitas sobre atributos (a faixa de valores de um atributo herdado deve ser a mesma ou um subconjunto da faixa de valores definida para o mesmo atributo de sua superclasse [BRI93]), ações e notificações [ISO 10165-1].

Segundo [KLE93], o alomorfismo permite a criação de visões (máscaras) de instâncias de objetos gerenciados. Se um fornecedor de serviços desejar esconder certos atributos e eventos de alguns usuários, uma subclasse deve ser definida a partir da classe do objeto gerenciado em questão, excluindo-se as características que devem ser escondidas (encapsuladas) dos usuários. O usuário terá acesso somente aos dados e métodos da superclasse se estes forem redefinidos para sua classe de acordo com seu perfil.

O alomorfismo é uma propriedade que permite ao implementador definir os relacionamentos das classes visíveis aos usuários de acordo com as necessidades do sistema de gerência [KLE93].

2.4.2 Operações de Gerenciamento de Sistemas

Em geral, os OG representam entidades ativas, manipuladas através das operações de gerência. Sendo os OG encapsulados, as operações de gerência são realizadas, sobre eles, através da passagem de parâmetros. As consequências da operação podem ser conhecidas através das notificações que os OG emitem com os resultados apropriados.

Uma operação, executada sobre um OG, pode ocorrer somente se o sistema gerente requisitor tiver o direito de acesso necessário para executar a operação, e se restrições de consistência não são violadas.

A decisão se uma operação é ou não executada sobre o OG está sujeita às restrições definidas na classe do OG, restrições estas que são verificadas pelo mecanismo de filtro. Exemplos de restrições são os relacionamentos que devem ser mantidos entre valores de atributos. Quando a realização de uma operação (substituição de um valor de atributo) causar a violação das restrições definidas, a operação não é executada e uma indicação de falha no processamento é retornada.

Um sistema gerenciado pode ser requisitado para executar uma operação sobre muitos OG com sincronismo atômico (todas as operações sobre os OG são executadas ou nenhuma). A definição da classe do objeto deve, portanto, especificar, para cada operação, todas as restrições dentro do OG e o critério para suportar pedidos de operação de gerenciamento para sincronismo atômico com outros OG.

As operações de gerência são divididas em operações orientadas a atributo e operações aplicadas sobre objetos. Vale ressaltar que as operações orientadas a atributo obedecem ao princípio do encapsulamento, ou seja não manipulam diretamente os atributos, mas só através da passagem de parâmetros e se os critérios definidos pela classe do OG forem respeitados.

Operações Orientadas a Atributo

As operações aplicadas sobre os atributos dos OG são:

- *Get attribute value*;
- *Set attribute value*.

Operações que são aplicadas aos atributos encapsulados no objeto sempre operam sobre uma lista de atributos. Toda operação orientada a atributo falhará se e somente se o comportamento do OG é tal que a operação não é executada sobre qualquer dos atributos no OG selecionado.

Quando o OG é requisitado para recuperar uma lista de valores de atributos ou modificar uma lista de valores de atributos por uma simples operação, a forma na qual a recuperação ou modificação é sincronizada através do atributo é determinada pelo comportamento definido na classe do OG e pelos atributos especificados na lista de atributos contidos na operação requisitada.

O OG, recebendo uma operação orientada a atributo, executa a operação na lista de atributos de acordo com as necessidades de sincronização especificadas na classe do OG. Se um atributo selecionado por uma operação não está encapsulado dentro do OG, ou se seu valor não pode ser alterado, o OG deverá indicar um erro.

O filtro determina como e se uma operação orientada a atributo deve ser executada.

Identificadores de atributos, seus valores associados para manipulação e indicações de erro para atributos que não podem ser manipulados estão disponíveis na fronteira do OG como resultado de uma operação orientada a atributo.

Indicadores de erro divididem-se em:

- indicadores de atributos desconhecidos;
- classe do objeto não é parte do conjunto alomórfico do OG;
- falha no processamento do pedido.

O efeito direto da execução da operação sobre um atributo de OG é definido pela operação de gerenciamento. A performance de uma operação de gerenciamento sobre um ou mais atributos no OG pode resultar em outras trocas observáveis, chamadas de efeitos indiretos.

Os seguintes efeitos indiretos podem ocorrer:

- a modificação de um atributo dentro do mesmo OG;
- a troca do comportamento do OG;
- a modificação de um atributo no OG relacionado;
- a troca do comportamento de um OG relacionado causado pela modificação de um ou mais atributos naquele OG.

Os três primeiros efeitos indiretos descritos acima são uma consequência do comportamento do OG que contém o atributo que estava sujeito a operação. O último efeito indireto é consequência do comportamento do OG relacionado ou da definição do relacionamento.

Get attribute value

Escopo: Esta operação aplica-se para todos os tipos de atributos, menos aqueles que não são definidos para leitura.

Semântica: Lê a lista de valores de atributos requisitados e retorna os valores dos atributos disponíveis para leitura. Se não há uma lista de atributos fornecidos para leitura, esta operação lê todos os valores de atributos e indica um erro para o valor de atributo que não pode ser lido.

Comportamento: Para que um sistema de gerenciamento possa determinar como e se a operação *get attribute value* pode ser executada, devem ser fornecidos os identificadores de atributo ou de grupo de atributo para valores de atributo que devem ser lidos.

Para aqueles atributos que não podem ser lidos através de um *get attribute value*, ocorrem indicações de erro: *atributos não disponíveis para leitura*.

Set attribute value

Escopo: esta operação não se aplica a atributos ou grupos de atributos que não estão disponíveis para escrita.

Semântica: Altera os valores dos atributos especificados pelos valores fornecidos.

Comportamento: Na determinação de como e se a operação *set attribute value* pode ser executada, estão disponíveis, como informação adicional, os identificadores de atributo ou de grupo de atributo e os novos valores associados àqueles que serão alterados.

Como resultado de um *set attribute value*, o OG pode apresentar indicações de erro, para aqueles atributos que não poderam ser alterados, com a seguinte informação adicional: *atributos não disponivies para leitura*.

Operações Aplicadas ao OG

As operações *Create*, *Delete* e *Action* são aplicadas sobre os OG como um todo e geralmente não estão restritas a modificações de valores de atributos.

Operações adicionais podem ser definidas através da operação *action*. A semântica destas operações faz parte da definição da classe do OG. Em particular, qualquer interação relacionada com outro OG deve ser especificada.

A operação de criação ou eliminação de um OG pode ser resultado de uma operação de um recurso normal (real) (isto é: o estabelecimento de uma conexão de rede ou de transporte, resulta na criação de um OG). Quando um OG é criado como resultado de uma operação de um recurso real, um identificador de instância é assinalado pelo sistema de gerenciamento através da execução de uma operação. Quando um OG é eliminado, o identificador da instância pode ser reutilizado.

Create

Escopo: Esta operação é aplicada para todo OG passível de criação como determinado pela definição da classe do OG.

Semântica: A operação requer a criação e inicialização de um OG. A operação de criação é única e aplica-se a OG que ainda não existe. A operação resulta na criação de um OG de uma classe específica ou em uma das suas subclasses alomórficas, dentro da hierarquia de nomeação. É uma operação de gerenciamento de sistemas e, além disso, tem efeitos sobre o recurso real que representa. A semântica precisa da instanciação do recurso deve ser descrita pelo definidor da classe do OG.

Comportamento: A operação cria um OG de uma específica classe ou subclasses alomórficas permitidas, dentro de um *containing* OG. O *containing* OG (o OG pai) já deverá existir antes do *contained* OG (filho) ser criado. Quando um OG é criado, são assinalados valores para os atributos encapsulados no objeto ou para qualquer dos seus pacotes de atributos especificados.

Os valores assinalados para os atributos ou para pacotes de atributos derivados da operação de *create* e da definição do objeto são os seguintes:

1) na operação de *create* é permitido especificar explicitamente valores de atributos individuais;

2) na operação de *create* é permitido especificar o objeto referente ao atributo na qual os valores poderão ser copiados;

3) na definição da classe do OG é permitido especificar como os valores iniciais nici
serão atribuídos para os atributos.

Para cada atributo individualmente, os valores são atribuídos de acordo com as especificações acima, sendo que o item 1 tem maior prioridade.

Objetos Gerenciados com ou sem pacotes condicionais são membros de uma mesma classe de OG. Para garantir que as capacidades mínimas requeridas para os recursos são selecionadas ou criadas, o gerente deve ser capaz de especificar as capacidades que o OG deve ter. Portanto, opções similares se aplicam para instanciação de pacotes condicionais quando um objeto é criado.

A instanciação de um pacote é requerida ou por um pedido explícito no pedido de criação, por sua inclusão na especificação do objeto referente, ou por *default*, como parte da especificação da classe do OG.

O pedido de criação irá falhar se:

- para qualquer atributo ou pacote nenhum dos 3 casos de valores assinalados para os atributos ou pacote de atributos, anteriormente descritos, se aplicam;
- se explicitas regras de criação incluem reservas sobre ou entre valores de atributos definidos pela classe do objeto tenham sido violadas;
- se o valor de atributo de um pacote condicional opcional tiver sido especificado e a instanciação do pacote não foi requisitada.

Uma definição de OG pode permitir um objeto ser criado sem especificação de seu nome de instância e sem especificação de seu *containing* OG. Uma definição de classe de OG pode também requerer que o nome da instância do objeto para ser criado ou seu *containing* OG ser explicitamente especificado na operação de criação. Vale observar que existe a possibilidade de que a classe do OG permita que o nome da instância seja especificado explicitamente ou atribuído na criação. A necessidade para esta possibilidade ainda não foi definida.

A operação de criação pode especificar a localização na hierarquia de nomeação, onde o novo objeto será colocado, ou pode permitir que o sistema de gerência escolha qualquer *containing* OG aceitável. Esta localização pode ser definida de duas formas:

- a operação pode explicitamente fornecer o nome do OG pai na qual a nova instância deve ser colocada;

- ou o nome do novo OG a ser criado pode ser especificado (o nome informa o local). O nome do OG filho contém o prefixo do OG pai.

Quando somente o nome do objeto pai é especificado, o RDN do filho é definido pelo sistema de gerência. Quando nem o nome do pai ou do filho é especificado, o sistema de gerência seleciona o objeto pai e atribui o nome do objeto filho.

Se a operação de criação não for executada ou se as informações associadas não estão corretas, o sistema de gerência deverá indicar erro.

Para determinar como e se a operação de criação pode ser executada, estão disponíveis para o sistema de gerência na execução de operações de criação:

- identificador da classe do objeto;

- atributos de pacotes, através da invocação de pacotes correspondentes;

- identificadores de atributo para aqueles atributos que tem valores assinados como parte da inicialização da instância do objeto explicitamente especificados;

- uma referência do identificador do OG, indicando de onde se pode obter informações de inicialização do OG, para aqueles atributos que não tem valores explícitos para serem atribuídos.

As seguintes informações podem estar disponíveis no limite do OG com o resultado da operação de criação:

- identificadores de atributos para aqueles atributos que tinham seus valores assinalados como parte da inicialização da instanciação do OG;

- indicações de erro no caso do OG não ser criado. Algumas das indicações de erro, em caso do OG não ser criado, são:

  - identificadores de atributo desconhecido;

  - identificador referente ao OG inválido;

  - especificação de *containment (name binding)* inválido;

  - falha geral no processamento do pedido de criação.

Delete

Escopo: Esta operação é aplicada para todos OG que podem ser eliminados remotamente.

Semântica: Esta operação requer que o OG elimine ele mesmo. A semântica desta operação deve ser definida pelo definidor da classe do OG.

Comportamento: Quando o OG recebe um pedido de eliminação, primeiro ele verifica se existem objetos contidos nele. Se existirem OG contidos no OG a ser eliminado, o comportamento do OG dependerá da forma escolhida para a especificação da classe do OG. O OG poderá eliminar todos os objetos contidos ou recusar a execução da operação até que todos os OG contidos sejam eliminados. O definidor de classes de OG deverá especificar as consequências precisas e a semântica da deleção de um OG que é instância daquela classe.

Action

Escopo: Esta operação pode ser usada por todas as classes de OG.

Semântica: Requer que o OG execute a ação especificada e indique o resultado da ação. A ação e a informação opcional associada fazem parte da definição da classe do OG.

Comportamento: Os efeitos precisos desta operação são especificados pela classe do OG. Ela deverá conter a identificação da ação especifica a ser executada. Caso a ação não possa ser executada, deverá ser indicado erro de operação:

- ação desconhecida;
- argumento desconhecido;
- valores de argumento inválidos;
- classe de objeto desconhecida;
- falha de processamento.

2.4.3 Escopo e Filtro

São mecanismos que permitem identificar e selecionar os OG e respectivos atributos dentro da hierarquia de nomeação. O escopo identifica sobre quais OG devem ser

executadas as operações de gerência. O filtro verifica se a operação requerida está de acordo com os critérios especificados para a classe do OG.

São usados pelos protocolos de gerenciamento e permitem verificar se a operação requerida está de acordo com os critérios da especificação da classe do OG.

2.4.4 Notificações

Os OG emitem notificações quando algum evento interno ou externo ocorre. As notificações são especificadas pela classe do OG. Muitos destes eventos são de interesse dos sistemas de gerenciamento e já encontram-se definidas na SMI.

2.5 Modelo Funcional

As atividades de gerenciamento de redes são realizadas pelas funções de gerência que permitem a monitoração, controle e coordenação das interconexões entre sistemas abertos. São processos de aplicação que manipulam os objetos gerenciados, através dos serviços oferecidos pela camada de aplicação OSI. A gerência de rede faz uso destas funções para monitorar (executar operações) e receber relatórios (notificações) sobre o estado da rede a fim de exercer um perfeito controle e coordenação dos sistemas de gerência.

Dentro deste contexto, as atividades de gerência do Modelo OSI são divididas em cinco áreas funcionais com objetivos bem definidos, que buscam resolver problemas relativos a falhas de componentes, níveis de desempenho alcançados, configuração da rede, contabilização e segurança (Figura 2.8). As áreas funcionais são:

- **Gerência de Falhas**: responsável pela detecção de falhas, isolamento e correção de operações anormais no ambiente OSI;

- **Gerência de Desempenho**: preocupa-se com o nível de performance da rede, faz levantamento estatístico para fins de avaliação e análise;

- **Gerência de Segurança**: garante a aplicação prática da política de segurança por meio de serviços e mecanismos que visam proteger o funcionamento da rede;

- **Gerência de Contabilização**: preocupa-se com a manutenção e monitoração de quais recursos e de quanto destes recursos estão sendo utilizados. É também responsável por determinar custos relativos ao uso destes recursos;

- **Gerência de Configuração**: responsável pela manutenção e monitoração da estrutura física e lógica da rede, incluindo a existência de componentes e sua interconectividade.

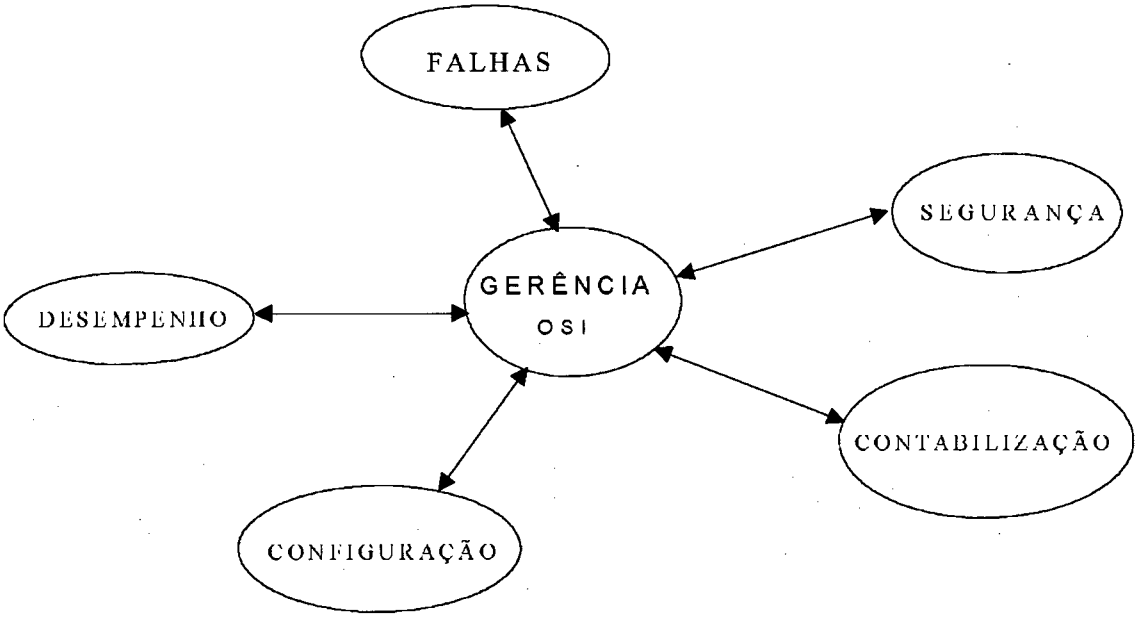


Figura 2.8 - Gerência OSI

Para dar suporte às áreas funcionais, foram definidas (mas não esgotadas) funções de gerência que incluem requisitos, modelos e serviços. Algumas destas funções são específicas a uma área funcional, mas a grande maioria serve de suporte a mais de uma área funcional. São elas:

1. Função de Gerenciamento de Objeto [ISO 10164-1];
2. Função de Gerenciamento de Estado [ISO 10164-2];
3. Atributos para Representação de Relacionamento [ISO 10164-3];
4. Função de Relatório de Alarme [ISO 10164-4];
5. Função de Gerenciamento de Relatório de Evento [ISO 10164-5];
6. Função de Controle de Log [ISO 10164-6];
7. Função de Relatório de Alarme de Segurança [ISO 10164-7];
8. Função de Registro para Auditoria de Segurança [ISO 10164-8];

9. Objetos e Atributos para Controle de Acesso [ISO 10164-9];

10. Função de Medida de Contabilização [ISO 10164-10];

11. Função de Monitoração da Carga de Trabalho [ISO 10164-11];

12. Função de Gerenciamento de Teste [ISO 10164-12];

13. Função de Sumarização [ISO 10164-13].

Uma descrição mais detalhada das áreas funcionais e funções de gerência pode ser encontrada em [BRI93].

As funções de gerência são responsáveis por coletar informações junto aos componentes da rede e colocá-las à disposição da gerência. Estas informações são pré-processadas e comparadas com as informações que refletem a política definida para a rede. A análise desta comparação envolve três tipos fundamentais de tomada de decisão:

- Operacional: decisões imediatas;
- Tática: decisões a curto e médio termo;
- Estratégica: decisões de longo alcance.

O processo de tomada de decisão visa garantir a colocação em prática da política estabelecida para a rede. Cada área funcional toma decisões operacionais, táticas e estratégicas, visando garantir a perfeita operação da rede.

2.6 Modelo de Comunicação

O modelo de comunicação requer o transporte orientado a conexão e conta com o ambiente da camada de aplicação. Mais detalhes da camada de aplicação podem ser encontrados na referência [ROSE90]. Em uma aplicação de gerência estão envolvidos os seguintes elementos de serviço de aplicação (ASEs - *Aplication Service Elements*):

- SMASE (*System Management Application Service Element*): Elemento de Serviço de Aplicação de Gerenciamento de Sistemas relacionado às áreas funcionais de gerência (falhas, contabilidade, configuração, desempenho e segurança).

- CMISE (*Commom Management Information Service Element*): Elemento de Serviço de Aplicação de Informação de Gerenciamento Comum que fornece serviços que permitem a troca de operações e notificações, através do protocolo de gerência CMIP

(*Commom Managemente Information Protocol*), entre duas entidades de gerenciamento que estão se comunicando.

- ROSE (*Remote Operation Service Element*): Elemento de Serviço de Operações Remotas usado para transportar as operações e notificações de gerência.

- ACSE (*Association Control Service Element*): Elemento de Serviço de Controle de Associação responsável pelo estabelecimento e liberação de associações entre aplicações.

Uma entidade SMAE é utilizada por um processo de aplicação (AP - *Application Process*) de gerenciamento de sistemas para comunicar-se com seus pares. Um processo AP pode usar diversas entidades SMAE, cada uma das quais provendo um conjunto específico de funções de comunicação para o processo AP. Uma entidade SMAE é composta pelos elementos de serviço de aplicação ASEs.

Dois processos de aplicação, através da entidade SMAE, estabelecem uma associação via serviço ACSE, onde negociam o contexto da associação, assumindo cada um o seu papel: gerente ou agente (Figura 2.9).

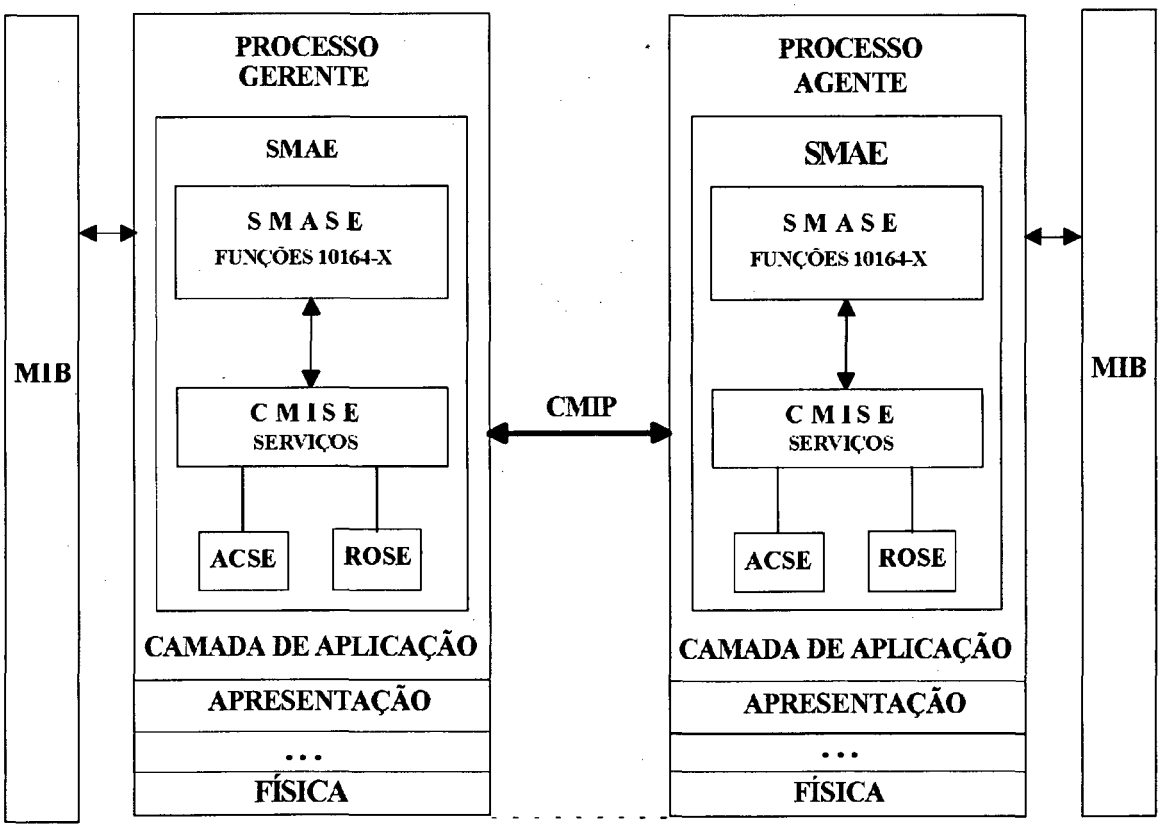


Figura 2.9 - Modelo de Comunicação

Uma entidade SMAE pode utilizar os serviços do CMISE, através do ROSE, para executar operações de gerência sobre os objetos gerenciados armazenados na MIB. Os serviços do CMISE são:

- M-Create : cria uma instância de um objeto gerenciado (OG);
- M-Delete: elimina uma instância de um objeto gerenciado;
- M-Get: lê valores de atributos;
- M-Set: atualiza valores de atributos;
- M-Action: executa ações sobre o objeto gerenciado;
- M-Event-Report: notifica a ocorrência de algum evento.

Os serviços CMISE são mapeados nas operações descritas na Figura 2.10.

SERVIÇOS CMISE	OPERAÇÕES NA MIB
M-Create	Create
M-Delete	Delete
M-Action	Action
M-Event-Report	Notificação
M-Get	Get
M-Set	(Replace, Set, Add e Remove)

Figura 2.10 - Mapeamento dos Serviços CMISE

3. SEGURANÇA EM REDES DE COMPUTADORES

3.1 Necessidades

A partir do momento em que as redes de computadores assumem um papel de importância estratégica dentro das empresas, garantir seu funcionamento de forma eficiente e seguro é vital para um bom desempenho empresarial.

As redes de computadores, como quaisquer sistemas de computação, estão sujeitas a problemas de quebra de segurança. Às vezes, até mais do que os sistemas de computação isolados, devido ao seu ambiente de operação ser mais complexo e vulnerável.

Os problemas surgem do fato das redes compartilharem vários recursos; operarem com sistemas complexos e diferentes; crescerem constantemente dificultando definir os limites da rede; terem muitos pontos passíveis de acesso; necessitarem de privacidade, integridade e autenticação; além de terem todos os problemas comuns aos sistemas de computação.

Os usuários de redes não possuem muito conhecimento destes problemas e das ameaças potenciais às suas informações transferidas através destes equipamentos interconectados, ou as ignoram. Sendo assim, agem com displicência. Pensam que nunca irão ocorrer incidentes de sabotagem ou destruição de informações em suas redes.

À medida que as empresas mais se comprometem com as redes de computadores, mais importância devem dar a sua segurança. Quanto mais importantes forem as informações transferidas através da rede, maior será o prejuízo em caso de ocorrência de algum incidente de perda ou destruição. Portanto, segurança está tornando-se um ponto crítico e essencial às redes de computadores.

A segurança de redes consiste em protegê-la contra penetração, escuta, destruição ou alteração de dados por pessoas não autorizadas [FOR94].

As redes de computadores devem garantir à informação que transferem:

- confidencialidade: garantir que a informação não é descoberta ou revelada por la p pessoas não autorizadas;

- integridade: garantir a consistência de dados (evitar a criação, alteração ou deleção de dados sem autorização);

- disponibilidade: garantir acesso à informação e aos recursos para usuários legítimos;

- uso legítimo: garantir que os recursos não são utilizados por pessoas e para fins não autorizados;

Para suprir estas necessidades, o administrador de rede deve definir uma política de segurança para a rede e colocá-la em prática através de medidas de segurança, considerando as seguintes categorias:

- Segurança de Comunicação: método de esconder informações sensíveis, importantes, e protegê-las contra falsificação enquanto transportadas;

- Segurança de Sistema: proteção da informação dentro de um sistema de computação (SO, MIB, ...);

- Segurança Física e Pessoal: proteção contra instalações e equipamentos, cuidados com os recursos humanos envolvidos.

3.2 Política de Segurança

Medidas de segurança, geralmente, aumentam o custo de um sistema e podem dificultar sua operação. Antes de projetar um sistema seguro, primeiramente, deve-se identificar reais ameaças (violação potencial de segurança [ISO 7498-2]) contra as quais é necessário adotar medidas de proteção.

Uma aplicação é vulnerável (qualquer fraqueza que pode ser explorada para violar uma aplicação ou a informação nela contida ISO [7498-2]) de diferentes modos, em especial as redes de computadores, mas somente alguns deles são importantes, ou porque os sabotadores necessitam de uma oportunidade, ou porque o resultado deste ataque não justifica o esforço e o risco de detecção.

A autoridade responsável por especificar uma política de segurança para um determinado domínio, ao defini-la deve:

- identificar as vulnerabilidades;

- analisar as probabilidades das ameaças a partir das vulnerabilidades identificadas;

- avaliar as consequências das ameaças potenciais;

- estimar os custos de cada ataque;

- estimar os custos das medidas de segurança;

- selecionar os serviços e mecanismos de segurança que sejam justificados possivelmente pela análise custo/benefício.

O objetivo, portanto, é reduzir os riscos de um ataque para níveis aceitáveis [ISO 7498-2].

Política de Segurança é um conjunto de regras, aplicadas sobre um domínio, que especifica o que é e o que não é permitido no campo da segurança.

Em [FOR94] são apresentados diferentes níveis de política de segurança:

- Objetivos da Política de Segurança: especificam as metas de uma organização em relação a proteção dos recursos;

- Política de Segurança Organizacional: conjunto de leis, regras ou práticas que regulamentam como uma organização protege e distribui recursos para alcançar as metas traçadas;

- Política de Segurança de Sistema: especifica como um sistema de informação pode suprir as necessidades da política organizacional. As especificações dos níveis de segurança englobam todas as categorias de segurança: pessoal; física; comunicação; e sistema. As categorias de comunicação e sistema são, principalmente, definidas através da política de segurança de sistemas.

3.2.1 Políticas de Segurança de Sistema

São também chamadas Políticas de Controle de Acesso e estabelecem as autorizações, concessões de direitos aos usuários (quem pode fazer o que e para que). A natureza da autorização é que distingue as várias políticas de segurança [ISO 7498-2] e podem ser divididas em: *Identity-based Policy*; *Role-based Policy*; *Multi-level Policy* ou algumas vezes, as políticas de segurança são categorizadas como *mandatory access control* ou *discretionary access control* [FOR94].

Políticas *mandatory* são impostas pela autoridade do domínio de segurança e não podem ser evitadas pelos usuários. Políticas *discretionary* fornecem a usuários particulares tipos de acesso aos recursos e deixam a cargo destes usuários o controle de novos acessos. Mais detalhes sobre estes modelos podem ser encontrados em [MCL90].

A Arquitetura de Segurança OSI [ISO 7498-2] não utiliza a terminologia *mandatory/discretionary*, mas sim *identity-based* e *rule-based*. Pode-se considerar *identity-based* e *discretionary* equivalentes, e também equivalentes *rule-based* e *mandatory* [FOR94].

Em geral, estas políticas podem ser combinadas e adotadas de acordo com as necessidades e benefícios identificados pela autoridade de segurança. Em seguida, serão apresentados alguns tipos específicos de política de segurança, que podem ser encontrados com mais detalhes em [FOR94] e [PFL89], tais como:

- *Identity-based* (*discretionary*) incluindo *individual-based* e *group-based*;
- *Rule-based* (*mandatory*) incluindo *multi-level e* modelo militar;
- *Role-based* que tem características tanto de *identity-based* como de *rule-based*.

Individual-based

É uma política do tipo *identity-based*, definida em termos dos objetos sujeitos ao controle de acesso, através de uma lista que contém uma entrada para cada usuário, identificando o que o usuário pode fazer sobre o objeto. Pode ser implementada através do mecanismo de matriz de acesso que é descrito em [PFL89]. Como exemplo, temos a Figura 3.1, onde para o objeto *x*, o usuário *a* tem direito de leitura e o usuário *b1* tem direito de leitura e gravação.

	objeto *x*	objeto *y*
usuário *a*	leitura	leitura
usuário *b1*	leitura gravação	leitura
usuário *b2*	leitura gravação	leitura gravação

Figura 3.1 - Matriz de Acesso

Group-based

É um outro caso de política *identity-based*, onde a vários usuários são garantidos algumas permissões para um determinado objeto. Múltiplos usuários são agrupados e referenciados por um identificador comum. Como exemplo, pode ser utilizado a matriz de controle de acesso (Figura 3.1), onde os usuários *b1* e *b2* formam um grupo do tipo *b*. A política de controle de acesso para o objeto *x* pode ser expressa como:

a) para o usuário do tipo *a* é permitido ler;

b) para o grupo *b* é permitido ler e gravar.

Uma vantagem é que a troca de membros entre grupos não afeta os direitos de acesso associados aos grupos. Estas características tendem a tornar esta política mais fácil e eficiente quanto a implementação de políticas do tipo *identity-based*.

Role-based

É um tipo de política que pode ser considerada como uma variação de *group-based*. Identifica os grupos com níveis de privilégios, onde um grupo tem maior significância que o outro (hierarquia de privilégios).

A diferença está na modelagem das regras de autorização, ou seja, cria grupos com níveis de operações distintas. As operações mais simples (ex: *get* e *set*) são associadas a grupos com menor prioridade e as operações mais importantes (ex: *create* e *delete*) são associadas a grupos com prioridade mais elevada:

Exemplo:

grupo: gerente de rede - autorização: *create, delete, action, set e get*;

grupo: técnico de rede - autorização: *action, set e get*;

grupo: operador de rede - autorização: *set e get*.

Segundo [FOR94], este tipo de política é muito poderosa. Primeiro, é definida de forma simples, onde é facilmente compreendida por pessoas com pouco conhecimento técnico. E segundo, porque é facilmente expressa através de uma matriz de controle de acesso, ou pela política *group-based*.

A política *Role-based* pode, também, ser considerada como uma política do tipo *rule-based* ou *mandatory*, porque se faz cumprir através de um domínio de segurança [FOR94].

O ponto crítico para utilização desta política é justamente na modelagem dos grupos associados às regras. A modelagem deve ser capaz de fornecer a granularidade de segurança requerida pelo sistema de gerência.

Multi-level

É um tipo de política *mandatory*, onde a autoridade classifica hierarquicamente as informações, sob seu domínio de segurança, com um nível de sensiblidade dentro de uma hierarquia de níveis como na Figura 3.2. Os usuários são, também, classificados com níveis da hierarquia adotada, chamados de *clearence*.

Entre a *clearence* do usuário e a sensibilidade da informação é estabelecida uma relação de autoridade. Específicas regras são definidas para garantir o direito de escrita e leitura da informação.

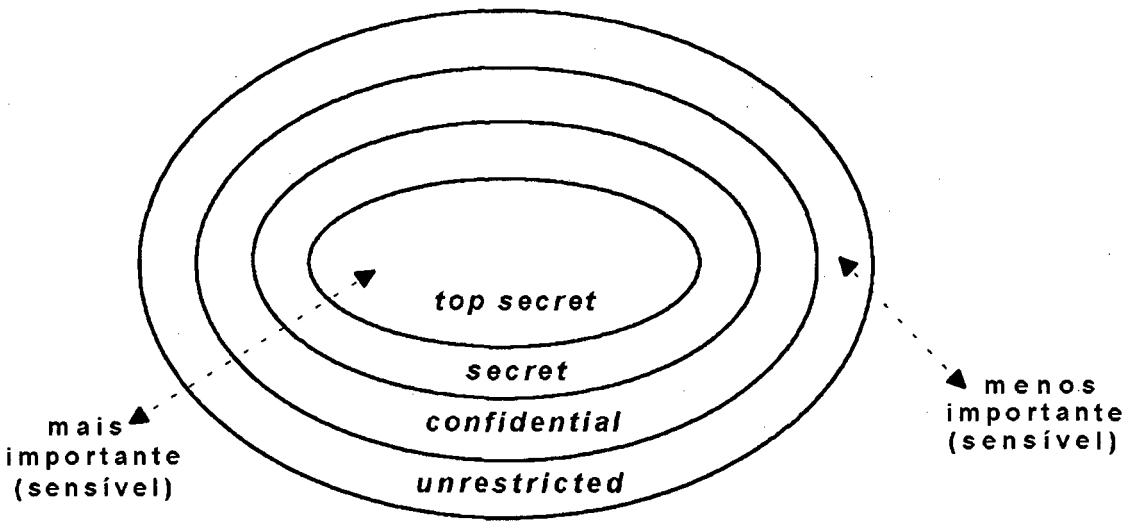


Figura 3.2 - Nívies de Sensibilidade

A regra para leitura, conhecida como *Simple Security Condition*, estipula que um usuário com um dado nível de *clearence* só pode ler informações com o mesmo ou menor nível de sensibilidade.

A regra para escrita, conhecida como **-property*, estipula que um usuário com um dado nível de *clearence* somente escreve para informações com o mesmo ou maior nível de sensibilidade. A razão para esta regra é prevenir um usuário de um nível superior transferir dados, através da escrita, para um objeto de nível inferior.

A política *Multi-level* também é utilizada pelas forças armadas, mas o modelo militar apresenta uma pequena variação. Além do nível de sensibilidade, a informação é classificada em áreas de utilização, chamadas de domínios. Domínios são usados para garantir a necessidade de conhecer a informação somente quem, realmente, precisa e deve utilizá-la (*need-to-know*).

A classificação da informação é dada pela combinação de {*nível, domínio*}. O usuário para ter acesso a informação tem que ter autorização (*clearence*). A autorização do usuário, também, é expressa pela combinação de {*nível, domínio*}.

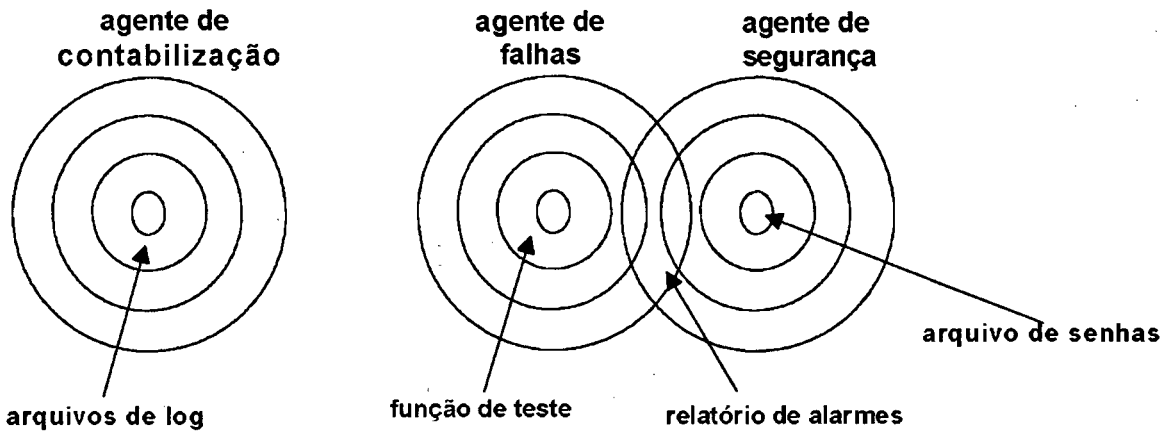


Figura 3.3 - Modelo Militar

O usuário só poderá acessar a informação, se o nível do objeto for menor ou igual ao do seu próprio nível e se seu domínio contiver o domínio do objeto.

Conforme a Figura 3.3, encontram-se como exemplos de domínio *agente de contabilização, agente de falhas e agente de segurança*. Uma informação é relacionada a um ou mais domínios de acordo com a área de utilização a que está associada:

- arquivo de log {*secret, agente de contabilização*};
- função de teste {*secret, agente de falhas*};
- relatório de alarmes {*unrestricted, agente de falhas, agente de segurança*};

- arquivo de senhas {*top-secret, agente de segurança*}.

Por exemplo, uma informação classificada como {*secret, segurança/falhas*} só pode ser acessada por usuários com nível de *clearence* {*top-secret, agente de segurança ou agente de falhas*} ou {*secret, agente de falhas ou agente de segurança*}, mas não é possível por alguém com uma *clearence* {*top-secret, agente contabilização*}.

Tendo a autoridade de segurança identificado e definido a política ou a combinação de políticas que irão suprir as necessidades de segurança do domínio sob sua responsabilidade, o próximo passo é definir os serviços e mecanismos que permitirão a colocação em prática das políticas estabelecidas.

A ISO definiu um Modelo de Segurança [ISO 7498-2] que é composto por serviços e mecanismos, além de funções de gerenciamento de segurança para ambientes heterogêneos.

3.3 Modelo de Segurança OSI

O Modelo de Segurança OSI define elementos que podem ser aplicados para proteger a comunicação entre sistemas heterogêneos conforme especificado pelo Modelo de Referência OSI. O modelo referente a segurança distingue dois conceitos:

- Arquitetura de Segurança [ISO 7498-2];
- Funções de Gerenciamento de Segurança [ISO 10164-7, 8, 9].

3.3.1 Arquitetura de Segurança

A Arquitetura de Segurança tem como objetivos definir:

- formalmente vários termos e conceitos utilizados por padrões de segurança de sistemas abertos;

- serviços de segurança para comunicação entre sistemas abertos e identificar os tipos de mecanismos que podem ser usados para fornecer estes serviços;

- a posição dos serviços e mecanismos de segurança dentro do Modelo de Referência.

Mais detalhes sobre a Arquitetura de Segurança (conceitos, serviços e mecanismos) podem ser encontrados em [ISO 7498-2] e [FOR94].

3.3.1.1 Serviços de Segurança

Os Serviços de Segurança são definidos pela Arquitetura de Segurança para garantir a comunicação segura e confiável entre sistemas remotos:

- controle de acesso (só pessoas autorizadas têm acesso aos recursos da rede);
- confidencialidade (os dados são privativos, não podem ser divulgados para usuários, entidades ou processos não autorizados);
- integridade (o conteúdo dos dados é real, não pode ser alterado ou destruído);
- não-rejeição (ninguém pode negar o envio e/ou a recepção de mensagens);
- autenticação (validação das entidades pares).

A política de segurança para um dado domínio irá determinar se algum serviço deve ser usado dentro do domínio ou na comunicação deste com outros domínios. Irá, também, definir sob quais circunstâncias o serviço será utilizado e quais níveis de serviços são necessários.

3.3.1.2. Mecanismos de Segurança

A Arquitetura Segurança não descreve como os serviços de segurança serão fornecidos. Identifica um conjunto de mecanismos de segurança que podem ser utilizados para implementar os serviços. Alguns exemplos de mecanismos adotados são:

- controle de chaves (chaves de criptografia, de roteamento e de assinatura numérica);
- criptografia (forma de proteger o conteúdo dos dados por embaralhamento. Só pessoas de posse da chave criptográfica podem decifrar o seu conteúdo. Mecanismo de base utilizado na maior parte dos serviços de segurança, em particular a autenticação, a integridade e a confidencialidade);
- controle de acesso (através de senhas);
- troca de autenticação (mecanismo pelo qual duas entidades trocam, com ajuda da criptografia, senhas de identificação. Serve para autenticação de entidades pares);

- controle de roteamento (permite que uma rota preferencial seja utilizada numa comunicação, de modo a evitar a circulação de informações em sub-redes inseguras ou desprotegidas e serve para garantir a confidencialidade);

- tráfego de desnorteamento (forma de despistar ou desnortear intrusos ou observadores indevidos);

- notarização (registro junto a terceiros do envio de uma mensagem. Serve para garantir a integridade e a não rejeição).

O uso dos serviços e mecanismos, ou de subgrupos destes em um determinado sistema aberto, é definido pela Política de Segurança adotada no sistema.

3.3.1.3 Localização dos Serviços e Mecanismos de Segurança

A Arquitetura de Segurança OSI define a localização dos serviços de segurança que devem ser oferecidos pelas camadas do Modelo de Referência OSI. A utilização destes serviços é opcional, depende das necessidades do sistema. Maiores esclarecimentos podem ser encontrados em [ISO 7498-2] e [FOR94]. Segue abaixo um pequeno resumo da localização dos serviços e mecanismos de segurança conforme descrito em [FOR94]:

- camada física: serviço de confidencialidade das instâncias de comunicação com conexão e/ou confidencialidade de tráfego;

- camada enlace: serviço de confidencialidade das instâncias de comunicação com conexão e sem conexão;

- camada de rede: serviços de autenticação, controle de acesso, confidencialidade e integridade;

- camada de transporte: autenticação, controle de acesso e integridade;

- camada de sessão: nenhum serviço de segurança é fornecido por esta camada;

- camada de apresentação: esta camada não fornece serviços de segurança, mas facilidades que permitem a implementação dos serviços na camada de aplicação. As facilidades fornecidas são necessárias aos mecanismos que manipulam transparência de dados com codificação (técnicas de criptografia);

- camada de aplicação: pode fornecer um ou mais serviços de segurança, combinados ou não, de acordo com as necessidades da aplicação. Portanto, nenhum serviço é pré-determinado.

A Arquitetura de Segurança, além da localização dos serviços dentro das camadas do Modelo de Referência OSI, ilustra o relacionamento entre os serviços e mecanismos de segurança, definindo quais mecanismos sozinhos ou combinados com outros são apropriados para fornecimento de cada serviço.

3.3.2 Funções de Gerência de Segurança OSI

As políticas de segurança são colocadas em prática através dos serviços e mecanismos de segurança. A gerência de segurança tem como objetivo garantir que a política de segurança seja colocada em prática conforme sua definição.

As atividades da gerência de segurança são divididas em três categorias descritas abaixo e podem ser encontradas com mais detalhes em [ISO 7498-2] e [BRI93]:

- Gerenciamento da Segurança do Sistema: abrange os aspectos de gerência de segurança do ambiente OSI:

a) gerenciamento da política de segurança, em especial a manutenção da coerência das bases de dados;

b) interação com outras funções de gerência OSI;

c) interação com o gerenciamento de serviços e mecanismos de segurança;

d) gerenciamento do tratamento de eventos.

- Gerenciamento dos Serviços de Segurança:

a) determinação das regras que servem para selecionar mecanismos específicos a serem empregados no fornecimento dos serviços de segurança;

b) invocação dos mecanismos de segurança específicos.

- Gerenciamento dos Mecanismos de Segurança: aborda o gerenciamento dos mecanismos que permitem o fornecimento dos serviços de segurança OSI:

a) gerenciamento de chaves;

b) gerenciamento de controle de acesso;

c) gerenciamento de trocas de autenticação;

d) gerenciamento de tráfego de desnorteamento;

e) gerenciamento do controle de roteamento;

g) gerenciamento de notarização.

As atividades de gerência de segurança, descritas anteriormente, são implementadas através das funções de gerenciamento de segurança.

As Funções de Gerência de Segurança dão suporte às atividades da Área Funcional da Gerência de Segurança. Elas são responsáveis por garantirem a execução da política de segurança adotada e também o aperfeiçoamento da proteção da rede. Periodicamente, necessita-se avaliar a eficácia das medidas de segurança e suas habilidades para proteger os equipamentos físicos, bem como manter a integridade e privacidade dos dados [TER87].

As principais atividades desta área funcional são:

- fornecer relatórios de eventos relativos à segurança e informações estatísticas;
- a manutenção e análise dos registros de histórico relativos à segurança;
- a seleção dos parâmetros dos serviços de segurança;
- a alteração, no que se refere à segurança, do modo de operação do sistema aberto, pela ativação e desativação dos serviços de segurança.

Do ponto de vista da área funcional relativa à segurança, existem três funções básicas que dão suporte às atividades de gerência de segurança do modelo OSI:

- Função de Relatório de Alarme de Segurança (*Security Alarm Reporting Function*) [ISO10164-7];
- Função de Registro para Auditoria de Segurança (*Security Audit Trail Function*) [ISO10164-8];
- Função de Controle de Acesso (*Objects and Attributes for Access Control*) [ISO10164-9].

3.3.2.1 Função de Relatório de Alarme de Segurança

A Função de Relatório de Alarme de Segurança [ISO 10164-7] tem o objetivo de veicular notificações de eventos, relativos à segurança, ao usuário do gerenciamento de segurança. Estes eventos podem ser operações errôneas nos serviços e mecanismos de segurança, atentados e violações contra a segurança.

Existe sempre o risco de ocorrer problemas quanto ao funcionamento dos serviços e mecanismos que garantem a proteção da rede. Portanto, a função de alarme de segurança

implementa facilidades que permitem detectar eventos suspeitos ou relacionados com segurança e notificá-los ao gerente, administrador ou operador humano.

A função de Alarme possui um Discriminador de Repasse de Alarmes de Segurança que determina, entre os eventos ocorridos na rede, quais são relativos à segurança. O discriminador contém uma estrutura de armazenamento que especifica as características que um evento deve ter para ser relacionado e remetido como alarme de segurança. Sendo um evento relativo à segurança, o discriminador define o tipo, a causa e a severidade do alarme de segurança a ser remetido através de relatórios para o gerente. A Figura 3.4 apresenta o modelo de operação da função de Alarme.

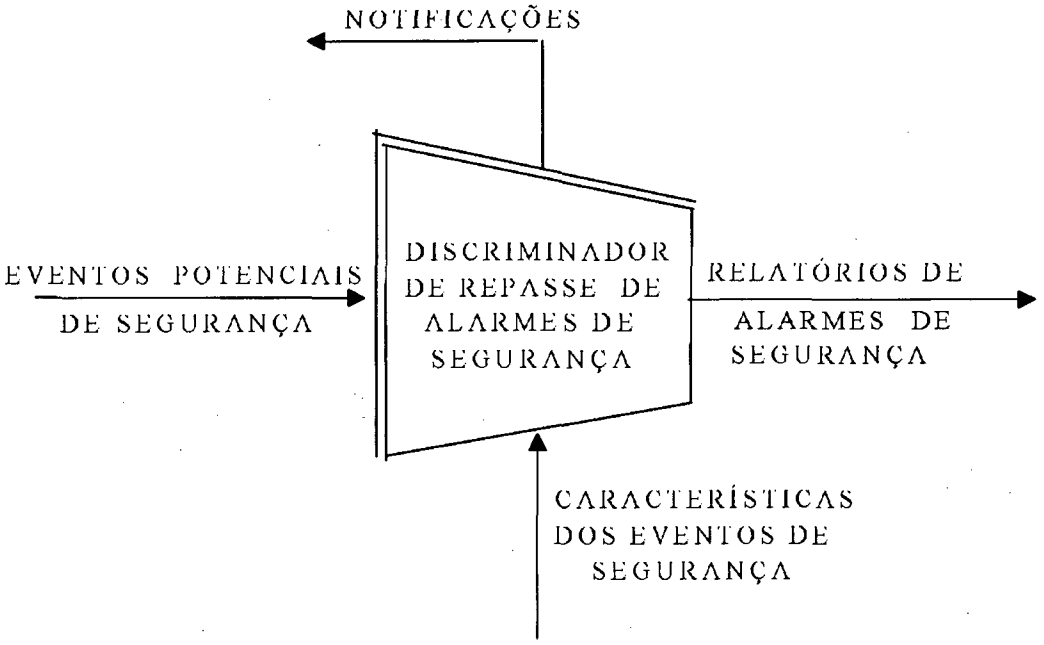


Figura 3.4 - Modelo da Função de Alarme de Segurança

3.3.2.2 Função de Registro para Auditoria de Segurança

A Função de Registro para Auditoria de Segurança [ISO 10164-8] tem o objetivo de gravar todos os eventos potenciais, relativos à segurança, que ocorrem no domínio de gerenciamento. O objeto, no qual são gravados tais eventos, é o *log* de auditoria de segurança. Comparando a utilização planejada para o sistema gerenciado com a utilização real gravada em

logs, o usuário da função pode avaliar como estão sendo atendidos os requisitos da política de segurança adotada.

A análise ou auditoria dos relatórios e alarmes de segurança permite, ao usuário, detectar desvios com relação às normas da política de segurança e descobrir pontos vulneráveis ou mau funcionamento relativo à segurança.

O modelo da Função de Registro para Auditoria de Segurança (Figura 3.5) é similar ao da Função de Relatório de Alarme de Segurança. Todos os eventos relativos à segurança são selecionados por um discriminador, mais as conexões, as desconexões, a utilização dos mecanismos de segurança, as próprias operações de gerenciamento de rede e a contabilização de utilização dos recursos gerenciados. O conjunto destas informações é gravado em *logs* de auditoria de segurança que possibilitam a realização de auditoria.

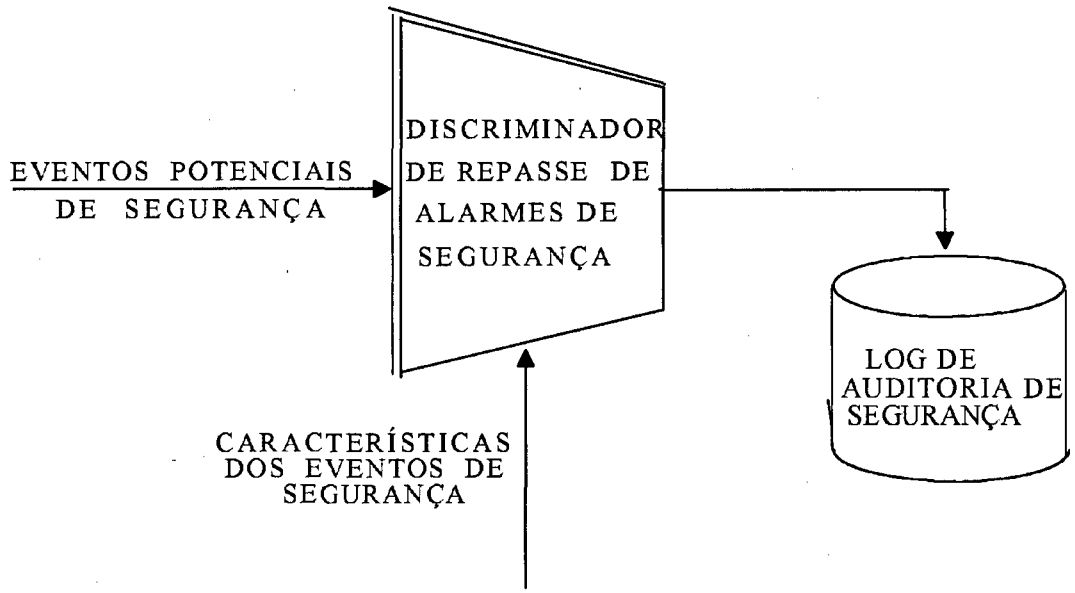


Figura 3.5 - Modelo da Função de Registro para Auditoria de Segurança

3.3.2.3 Função de Controle de Acesso

A Função de Controle de Acesso [ISO 10164-9] constitui uma forma específica de controle dentro dos sistemas de gerenciamento. Provê proteções aos recursos de gerenciamento que são os objetos gerenciados armazenados na MIB, aos gerentes e aos agentes do sistema de gerenciamento.

Um sistema de gerenciamento, devido a sua importância para uma rede de computadores, necessita prevenir-se contra acessos não autorizados aos recursos de gerenciamento. Para isto são providos de mecanismos de controle de acesso que visam assegurar que somente usuários autorizados possam ter acesso a um recurso de gerenciamento específico. Podem ser necessários também vários níveis de acesso:

- acesso para ler e escrever, apenas para ler ou nenhum acesso;
- acesso apenas para objetos específicos;
- proibição até do estabelecimento de comunicações para gerência de recursos do sistema aberto.

Faz-se também necessário que as notificações de gerência, inclusive os alarmes de segurança, não sejam enviados para usuários sem autorização. Entidades não autorizadas não devem ter acesso a operações de gerência e, de modo geral, estas informações devem ser protegidas contra divulgação indesejável.

A fim de suprir as necessidades descritas, a autoridade de segurança deve definir uma política de controle de acesso, que faz parte da política de segurança, para os recursos de gerenciamento.

Os recursos de gerenciamento são modelados através dos objetos gerenciados e seus atributos. Portanto, ao controlar o acesso aos objetos gerenciados e aos seus atributos, automaticamente controla-se o acesso aos recursos da rede.

A política de controle de acesso para recursos de gerenciamento deve identificar quais são as informações de gerenciamento que devem ter o acesso controlado, identificar quem pode manipulá-las e sob que condições, e identificar quais são as regras que controlam o acesso a estas informações de gerenciamento.

A informação de gerenciamento que necessita de controle de acesso é associada a um outro objeto de controle de acesso, chamado de *target*. Este contém atributos para representar as informações e regras de controle de acesso a serem aplicadas ao seu objeto associado, ou seja a informação que ele representa. Por exemplo, um *target* pode representar um objeto gerenciado, um atributo de objeto gerenciado, um valor de atributo ou, até mesmo, uma ação de gerenciamento.

Faz parte da definição de uma política de controle de acesso para recursos de gerenciamento a especificação dos objetos de controle de acesso, das informações e regras que eles representam.

Existem dois tipos de controle de acesso nos casos específicos de gerenciamento OSI:

- para associação de aplicações de gerência, que visa garantir que iniciadores não-autorizados não podem estabelecer associações de gerência;

- para operações de gerência, que visa garantir que essas operações sejam feitas pelas entidades autorizadas, mas sob restrições relativas a horário, tipo de operação, recurso e informações envolvidas.

A Função de Controle de Acesso, que tem seu modelo básico apresentado na Figura 3.6, é composta pelas funções:

- *Access Control Enforcement Function* (AEF);

- *Access Control Decision Function* (ADF).

A função AEF é responsável por receber os pedidos de acesso, feitos por um usuário, chamado de iniciador (*initiator*), selecionar os parâmetros de controle de acesso do pedido e repassá-los à função ADF.

O iniciador pode ser um sistema de gerenciamento ou um usuário deste sistema de gerenciamento. Entre os parâmetros de controle de acesso encontram-se as informações de controle de acesso do iniciador (*Initiator ACI - Access Control Information*), a operação de gerenciamento e a informação de gerenciamento a ser manipulada.

A função ADF é responsável por receber os parâmetros de controle de acesso da função AEF e decidir se o pedido de acesso é válido ou não.

Decisões de acesso são baseadas nas regras de acesso descritas pela política de controle de acesso. Existem três tipos de regras de acesso:

- *Global rules* que são usadas pela autoridade de segurança para proteger todos os *targets* de um domínio de particulares iniciadores ou de classes de iniciadores;

- *Item rules* que são regras específicas aplicadas a específicos *targets*;

- *Default rules* que são aplicadas quando não se aplicam *Global rules* e *Item rules*.

Para validar pedidos de acesso, a função ADF compara os parâmetros dos pedidos recebidos com as regras da política de controle de acesso definida para rede. Se um pedido está de acordo com as regras, a função valida o pedido. Caso contrário, o pedido é rejeitado. Uma vez tomada a decisão, a função ADF repassa-a para a função AEF. Se a decisão for negativa, a função ADF também entrega à função AEF as instruções de rejeição, que podem ser, por exemplo, só uma resposta negativa ou, até mesmo, uma instrução para abortar a conexão.

Na prática, é muito difícil distinguir o gerenciamento de segurança dos próprios mecanismos de segurança. Fica a cargo de cada implementação garantir a troca de informações de uma forma segura e confiável, e controlar o acesso aos objetos gerenciados armazenados na MIB.

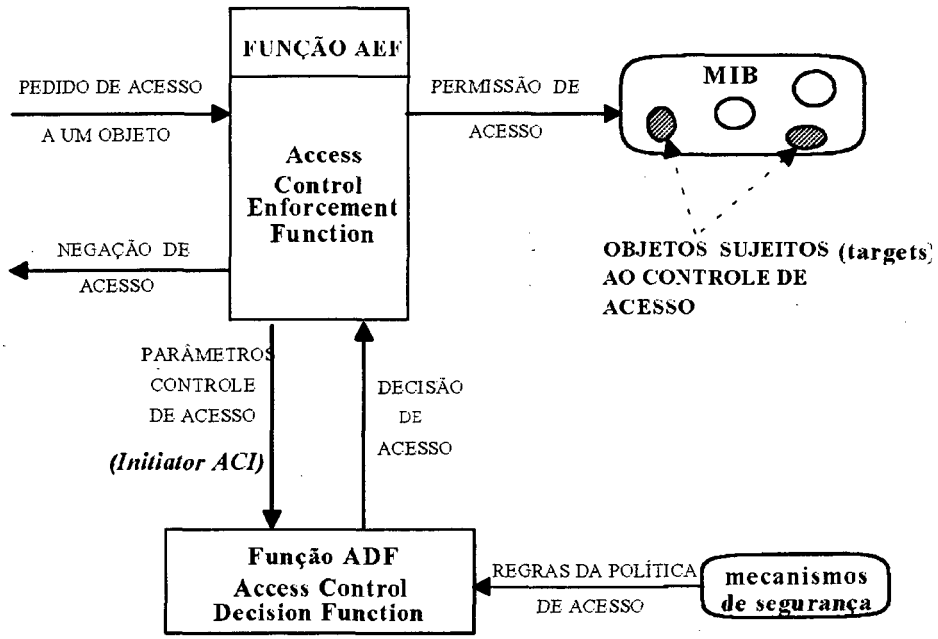


Figura 3.6 - Modelo Básico da Função de Controle de Acesso

3.4 Objetos de Controle de Acesso

A cada objeto gerenciado sujeito ao controle de acesso é associado um objeto de controle de acesso. A norma [ISO 1064-9] define as classes de objetos para controle de acesso e os atributos utilizados pelo serviço de controle de acesso. São três as classes definidas pela norma: *Access Control Descriptor (ACD); Target Acess Control Information (Target ACI); Authorised Initiators.*

A classe ***Access Control Descriptor*** é usada especificar as informações de gerência que são utilizadas pelo serviço de controle de acesso. Esta classe contém as informações que caracterizam a política de controle de acesso adotada. Esta classe inclui os seguintes atributos:

- *Access Control Descriptor Name*: nome do objeto descritor de controle de acesso;

- *Access Control Policy Name*: nome da política de controle de acesso que é representada pelo objeto descritor de controle de acesso;

- *Access Control Domain Names*: nomes dos domínios dos quais o descritor de controle de acesso é um membro;

- *Global Rules*: regras que são usadas para proteger qualquer objeto gerenciado dentro do domínio em que se aplica a política de acesso;

- *Default Rules*: as regras aplicadas quando não se aplicam *global rules* e *item rules*;

- *Access Control Descriptor Rule*s: são as regras *item rules* aplicadas às instâncias desta classe ACD;

- *Access Control Information Rules*: são as regras aplicadas as classes *Target ACI* e *Authorised Initiators* que estão contidas na classe ACD;

- *Access Control Informaiton Operations*: conjunto de operações de gerenciamento sujeitas às restrições de acesso definidas pela política de controle de acesso.

Já a classe ***Target Access Control Information*** é usada para especificar os elementos de informação de gerenciamento que devem ser protegidos e as regras de controle de acesso que se aplicam. É formada pelos seguintes parâmetros:

- *Target Access Control Information Name*: nome do objeto *Target ACI*;

- *Object List*: lista de objetos gerenciados sujeitos ao controle de acesso;

- *Management Information Rules*: são as regras *item rules* aplicadas para os objetos gerenciados identificados pelo atributo *Object List*;

- *Management Information Operations*: especifica o conjunto de operações de gerenciamento cujo as restrições de acesso estão associadas para qualquer objeto identificado pelo atributo *Object List.*

A classe ***Authorised Initiators*** é usada para identificar a lista de usuários autorizados a acessar a informação de gerenciamento. Esta classe é composta por apenas dois atriubutos:

- *Authorised Initiators Name*: nome do objeto da classe;

- *Initiator List*: define os usuários autorizados a acessar a informação de gerenciamento.

Do ponto de vista da hierarquia de herança, as classes de objetos de controle de acesso estão organizadas no Modelo OSI como ilustra a Figura 3.7.

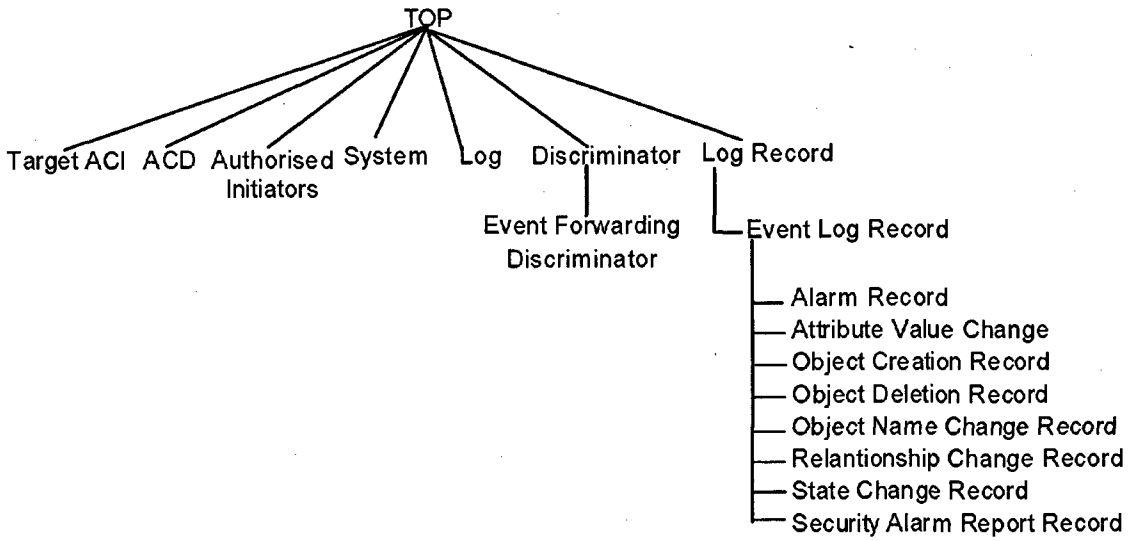


Figura 3.7 - Modelo da Hierarquia de Herança contendo as Classes de Controle de Acesso

Os relacionamentos entre os objetos de controle de acesso, especificados através do conjunto de *name-bindings*, são definidos pela norma [ISO 10164-9] e estão organizados na hierarquia de *containment* ou nomeação conforme a Figura 3.8.

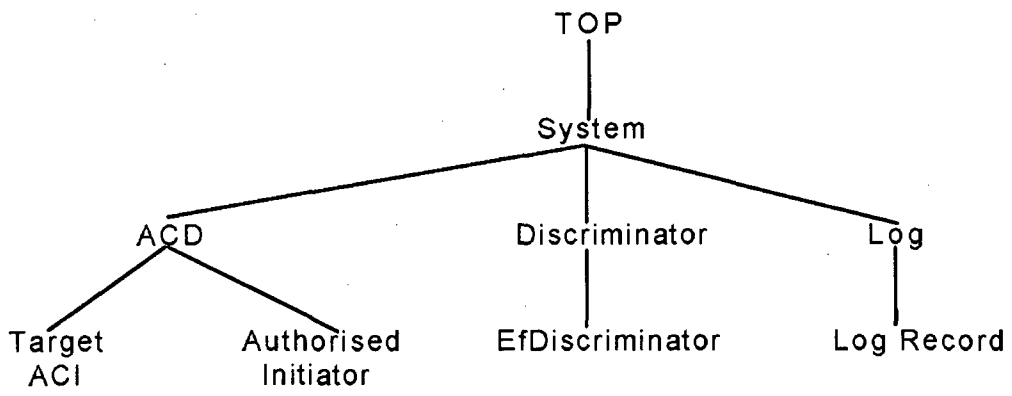


Figura 3.8 - Modelo da Hierarquia de Nomeação contendo as Classes de Controle de Acesso

A política de controle de acesso é representada pelos objetos gerenciados para controle de acesso. Estes objetos identificam os elementos de informação de gerenciamento que devem ser protegidos. A especificação dos objetos gerenciados para controle de acesso pode ser separada da especificação dos mecanismos que serão empregados para protegê-los [ISO 10164-9].

3.5 Segurança da Gerência

As funções de Alarme e Auditoria de segurança exercem controle sobre os serviços e mecanismos de segurança implementados nas camadas do Modelo de Referência OSI e, sendo assim, garantem a execução da política de segurança.

Entretanto, a gerência de redes OSI, como qualquer aplicação, também, tem suas necessidades de segurança. A implementação das medidas de segurança para a gerência decorre do fato de que a gerência manipula informações extremamente importantes para a manutenção da rede em perfeito funcionamento.

Um usuário, ao manipular um sistema qualquer, jamais teria acesso a informações tão sensíveis quanto as disponíveis em um sistema de gerenciamento de redes. Um sistema de gerência controla todos os objetos gerenciados, que nada mais são do que os recursos reais de um sistema, executa operações sobre estes, gera relatórios estatísticos, alarmes, auditoria e etc.

Além dos problemas abordados acima, um outro fator que compromete ainda mais a segurança de um sistema de gerência de redes é que seus processos de aplicação, ao trocarem informações para cooperarem entre si, utilizam protocolos de comunicação padronizados e amplamente difundidos.

Um ótimo estudo sobre as necessidades da segurança da gerência pode ser encontrado em [LUC93]. Segundo [LUC93], apesar da gerência de redes criar mecanismos de controle que são úteis na manutenção da segurança da rede, também, cria vulnerabilidades à rede, tornando-a mais insegura. Portanto, a gerência de redes é uma aplicação muito importante que requer a implementação de serviços e mecanismos de segurança para sua proteção.

Os serviços e mecanismos de segurança, implementados para a gerência de redes, localizam-se na camada de aplicação e, também, estão sob o controle das funções de Alarme e Auditoria.

Dentro deste contexto, uma informação de gerência OSI (ver Figura 3.9), ou está armazenada na MIB (categoria de segurança de sistema) ou está trafegando na rede (categoria de segurança de comunicação) e necessita diretamente dos seguintes serviços de segurança:

- confidencialidade: pode ser implementado através de mecanismos de criptografia;
- integridade: mecanismos de criptografia e *checksum*;
- autenticação: mecanismos de criptografia;
- controle de acesso: função de gerência de controle de acesso e mecanismos de segurança.

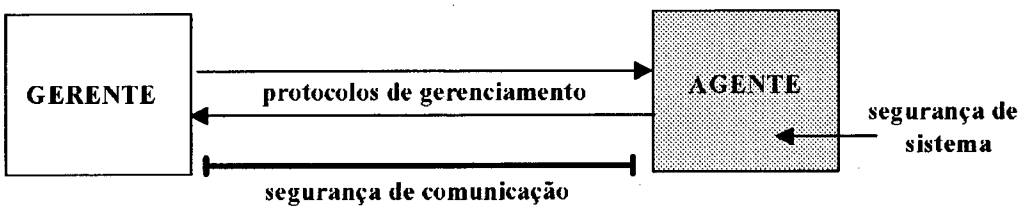


Figura 3.9 - Categorias de Segurança

A categoria de segurança de comunicação pode ser realizada através dos serviços de confidencialidade e integridade. Já a categoria de segurança de sistema pode ser implementada pelos serviços de autenticação e controle de acesso.

O serviço de autenticação pode ser fornecido por diversos mecanismos [FOR94]. Um deles seria por criptografia [LUC93]. Este serviço é importante porque garante que o gerente, que deseja manipular a MIB, é realmente quem ele diz ser, evitando assim ataques de mascaramento (entidade falsa apresentando-se como verdadeira).

Uma vez satisfeita a necessidade de autenticação, o sistema de gerenciamento ainda precisa verificar se a entidade gerente que deseja operar sobre a MIB pode, realmente, estabelecer a associação requerida e, posteriormente, controlar as atividades desta entidade.

Portanto, após o serviço de autenticação, o sistema de gerenciamento de redes necessita do serviço de controle de acesso.

O serviço de controle de acesso de um sistema de gerenciamento OSI, em especial, é implementado através da função de Controle de Acesso [ISO 10164-9]. Este serviço, apesar de ser implementado através de uma função de gerência, também é gerenciado pelas funções de Alarme e Auditoria.

A função de Controle de Acesso tem como objetivo avaliar e autorizar os pedidos de acesso aos objetos gerenciados armazenados na MIB, baseada em mecanismos de segurança, de acordo com a política de controle de acesso definida para a gerência da rede.

As informações necessárias ao gerenciamento de segurança e à segurança da gerência (chaves criptográficas, senhas, regras de autorização, alarmes, objetos de controle de acesso, etc) devem ser armazenadas e mantidas em uma base de informações de segurança distribuída, definida apenas em nível conceitual, denominada *Security Management Information Base* (SMIB). A base SMIB pode ou não ser integrada em parte ou no todo à MIB.

A OSI não define os métodos de manipulação da base SMIB. Podem ser através dos protocolos de gerência ou externamente. Também não indica qualquer dispositivo de armazenamento físico (memória, disco, fita, etc). Apenas, fornece alguns mecanismos de segurança que permitem modelar logicamente estas informações de acordo com as políticas de segurança. A manipulação da base SMIB requer medidas de segurança. Cabe à autoridade de segurança, responsável pela base SMIB, definir estas medidas de acordo com as necessidades de segurança requeridas.

4. INTERFACE DE CONTROLE DE ACESSO

A **Interface de Controle de Acesso** é destinada às autoridades de segurança. Visa auxiliar a implementação de políticas de controle de acesso em sistemas de gerenciamento OSI ou com funcionalidade OSI.

Para um melhor entendimento das funções de gerência de segurança OSI, nos capítulos anteriores destacou-se a importância da gerência de redes, ao manipular informações extremamente sensíveis, e as necessidades de proteção que o gerenciamento requer. Dentro deste contexto, conforme o item 3.5, a gerência de redes é uma aplicação importantíssima e necessita de medidas de segurança. As funções de gerência de segurança permitem avaliar e controlar os serviços e mecanismos de segurança que são empregados na proteção da rede e da gerência.

A função de Controle de Acesso é uma função especial de segurança que, em conjunto com as funções de Alarme e Auditoria, propicia o gerenciamento da segurança interna do sistema de gerência OSI (ver item 3.3.2.3 e 3.5).

A proteção interna recai sobre a MIB. Ela contém o conjunto dos objetos gerenciados, atributos e operações e é o núcleo principal de um sistema de gerenciamento. Garantir o acesso à MIB só para usuários autorizados é controlar o acesso, através do sistema de gerência, aos recursos reais da rede relacionados com o ambiente OSI.

O controle de acesso é o princípio de autorização. Define quais os objetos que os usuários podem manipular e com que finalidade. As políticas de controle de acesso expressam o conceito de autorização (ver item 3.2).

A Interface permite à autoridade de segurança estipular as regras de autorização de seu domínio de segurança, oferecendo-lhe mecanismos de segurança que possibilitam a implementação das políticas de acesso: *Individual-based, Group-based; Role-based; Multi-level;* e *Modelo Militar*.

A Interface tem como principais objetivos:

- controlar o acesso à MIB;

- controlar o estabelecimento de associações;

- fornecer uma ferramenta amigável que permita à autoridade de segurança definir e administrar as regras de autorização definidas por uma política de segurança;

- fornecer uma base de regras de autorização que permita armazenar as regras definidas.

O modelo proposto é composto por três elementos principais conforme ilustrado na Figura 4.1:

- um Sistema de Definição de Autorização (SDA);

- um Sistema de Controle de Autorização (SCA);

- uma Base de Dados de Autorização (BDA).

O sistema SDA é um sistema interno e independente do padrão OSI. É composto por métodos comuns que permitem a manipulação da base BDA (inclusão, alteração, exclusão e consulta).

O sistema SCA implementa a funcionalidade das funções de controle de acesso AEF e ADF do modelo de gerência OSI [ISO 10164-9].

A base BDA é formada pelos objetos de controle de acesso modelados através de mecanismos de segurança que permitem a implementação das políticas de acesso definidas no item 3.2.

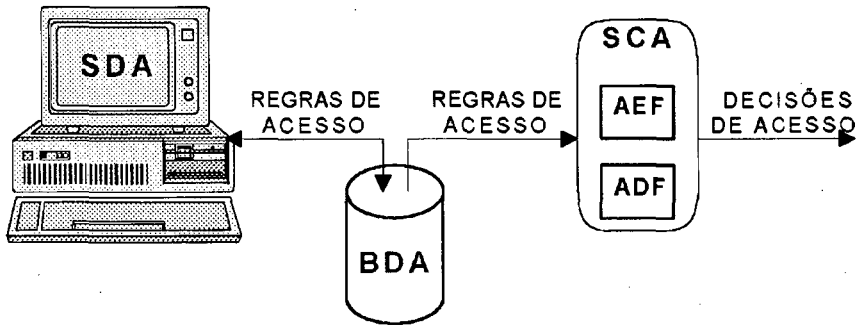


Figura 4.1 - Modelo Genérico da Interface de Controle de Acesso

A Interface de Controle de Acesso interage com um ambiente de gerenciamento através da troca de informações com a Entidade de Gerenciamento de Sistemas (SMAE) de um

processo de aplicação, a fim de validar os pedidos de associação e de operações de gerenciamento (ver Figura 4.2).

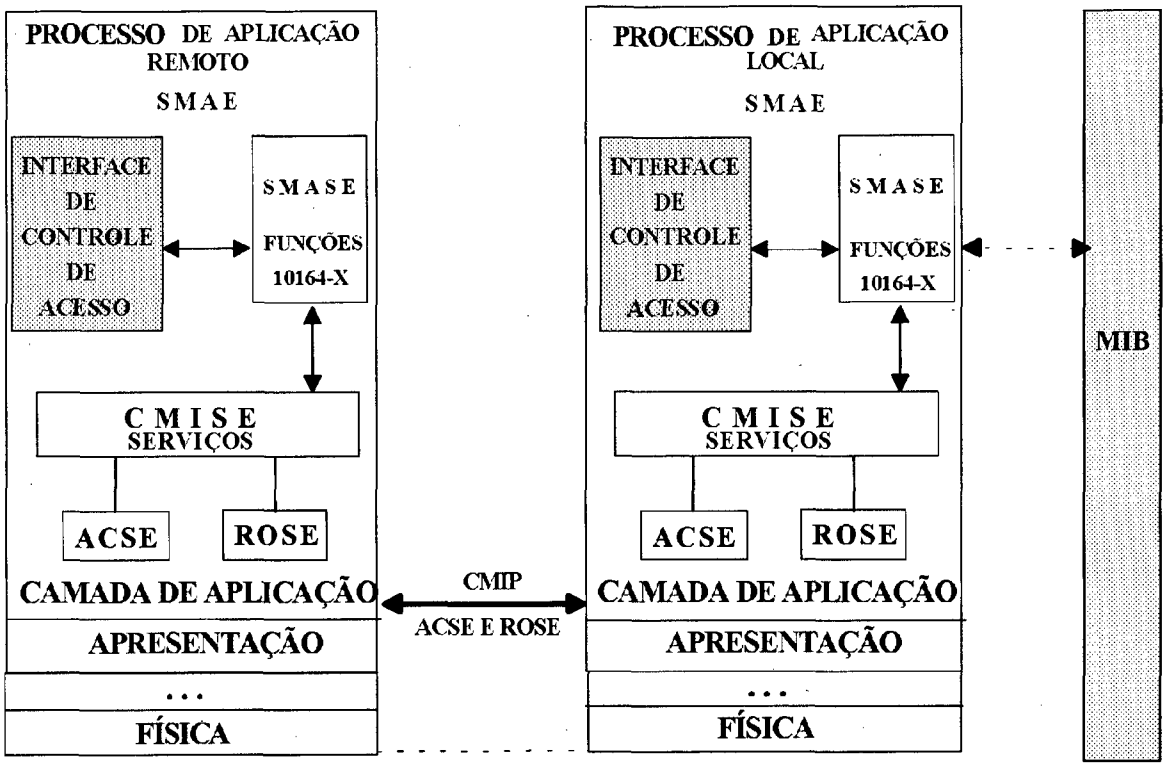


Figura 4.2 - Localização da Interface de Controle de Acesso

4.1 Base de Dados de Autorização (BDA)

A Base de Dados de Autorização (BDA) armazena as regras de autorização para os objetos gerenciados de um sistema de gerência. Estas regras são especificadas de acordo com o modelo de política de acesso adotado. As autoridades responsáveis por segurança em sistemas de gerência, ao definirem a política de segurança, especificam qual ou quais os modelos de políticas de acesso a serem adotados. A Figura 4.3 mostra um cenário hipotético de sistemas de gerenciamento e seus modelos de política de acesso.

Cada sistema de gerência pode ser composto por um ou mais agentes (ver item 2.2). A política de acesso, adotada para o sistema, pode ser a mesma para todos os agentes ou combinadas para garantir um melhor nível de granularidade (ver item 3.2.1) (Figura 4.4).

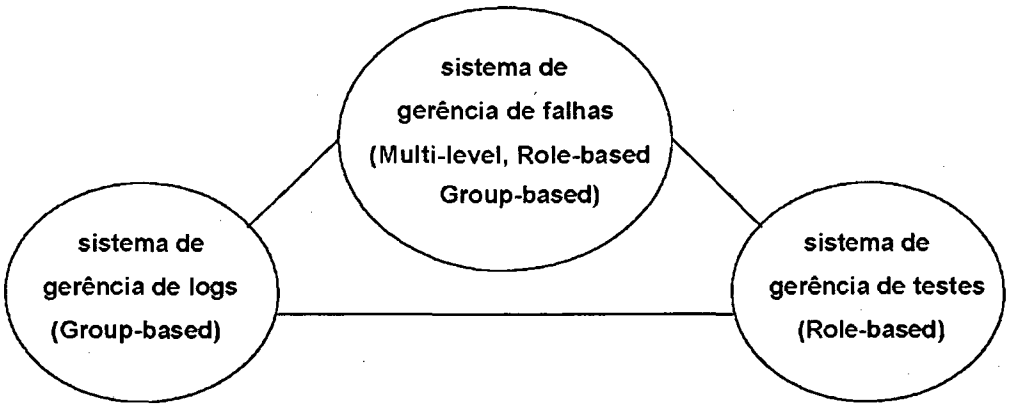


Figura 4.3 - Sistemas de Gerência e Políticas de Acesso

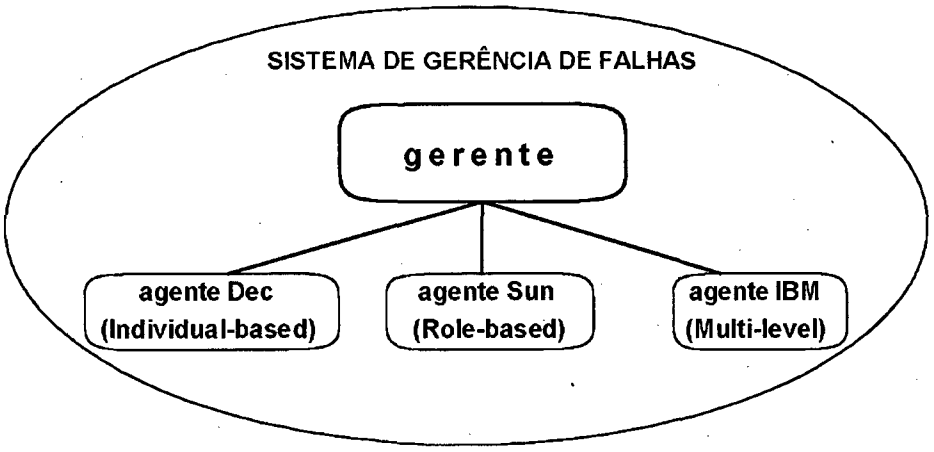


Figura 4.4 - Política de Segurança para um Domínio

A Interface de Controle de Acesso contém mecanismos de segurança que possibilitam a implementação das políticas de controle de acesso que a Interface oferece. Estes mecanismos expressam as regras de autorização para os elementos de gerência que necessitam de proteção de acesso, chamados de objetos *target*.

O serviço de controle de acesso é requerido em dois níveis: a nível de associação e a nível de operação. As associações de gerenciamento são estabelecidas com os processos de aplicação agente que são os responsáveis pela execução das operações sobre os objetos gerenciados. Já os objetos gerenciados são submetidos às operações de gerenciamento que representam ações sobre recursos reais de rede.

Dentro deste contexto, a Interface de Controle de Acesso fornece mecanismos de segurança para dois tipos de objetos *target*: processos de aplicação agente e de objetos

gerenciados juntamente com seus respectivos atributos. Dentro de cada política de acesso, a Interface possui uma lista para cada um destes dois tipos de *targets* que contém quais os objetos para controle de acesso de cada tipo. As listas são:

- Lista de Processo de Aplicação (LPA): é formada por todos os processos de aplicação agente que requerem controle de acesso a nível de associação. Cada entrada da lista LPA corresponde a um objeto da classe *Target ACI*;

- Lista de Classes de Objeto Gerenciado (LCO): é formada pelas classes de objetos gerenciados sujeitos ao controle de acesso (*Global Rules*). Cada entrada da lista LCO corresponde a um objeto da classe *Target ACI*.

Os objetos da classe *Target ACI* são formados pelos atributos *TargetACIName* e *ObjectList* (ver item 3.5). O primeiro atributo descreve o nome do objeto para controle de acesso. O segundo atributo é formado por dois itens. Um item, chamado de *managedObjectClass*, serve para indicar a classe do objeto gerenciado sujeito ao controle de acesso. O outro item, chamado de *managedObjectList*, é uma lista opcional de instâncias da classe indicada no primeiro item. A lista opcional informa quais as instâncias que possuem suas próprias regras de acesso (*Item rules*), independente das regras da classe *Global rules*. Se a lista opcional estiver vazia, indica que as regras gerais da classe (*Global rules*) valem para todas as suas instâncias.

Na Interface de Controle de Acesso, os objetos da classe *Target ACI* do tipo processo de aplicação agente não possuem lista opcional, enquanto que os objetos da classe *Target ACI* do tipo classe de objeto gerenciado possuem a lista opcional chamada de Lista de Instâncias de Objeto Gerenciado (LOG).

A lista LOG é formada por todas as instâncias da classe a que está associada que necessitam de regras de controle de acesso específicas *Item Rules*.

Às listas LPA, LCO e LOG, que contém os objetos para controle de acesso, estão associados os mecanismos particulares da política de acesso da qual fazem parte. Nos ítens seguintes, segue a descrição destes mecanismos de segurança e as suas relações com as listas de objetos para controle de acesso dentro de cada modelo oferecido pela Interface.

4.2 Individual-Based

A política *Individual-based* é expressa em termos de uma lista para cada objeto *target*, lista que apresenta quais usuários podem executar ações e quais ações podem ser executadas sobre os objetos *target*. Esta lista, chamada de Lista de Controle de Acesso (LCA), é um atributo do objeto *target* integrante da Lista de Processo de Aplicação (LPA) e da Lista de Classes de Objeto Gerenciado (LCO).

Uma lista LPA, na política *Individual-based*, é composta por um identificador de processo de aplicação agente e de um identificador para a lista LCA associada a este agente.

O identificador de processo de aplicação agente (IAG) é um descritor de identificação do agente dentro do sistema de gerenciamento.

O identificador de lista LCA (ILCA) é um apontador de localização de associação do processo de aplicação agente a sua respectiva lista de controle de acesso. A Figura 4.5 apresenta um modelo da lista LPA.

IAG	ILCA
Ag Falhas	LCA1
Ag Segurança	LCA2
Ag Testes	LCA3
Agente Log	LCA4

Figura 4.5 - Lista de Processo de Aplicação na Política Individual-based

A lista LCA, que é um atributo de um *target*, contém as regras de acesso para o objeto a que está associada. A lista LCA para objetos *target* do tipo processo de aplicação agente, na política *Individual-based*, é composta por um identificador de iniciador e das informações de contexto. A ação que o iniciador pode executar neste caso é *default*: estabelecimento de associação de gerenciamento.

O identificador de iniciador (IdI) é o registro de identificação do iniciador dentro do sistema de gerenciamento. Um iniciador (ver item 3.4) pode ser um usuário de sistema de gerenciamento, um processo de aplicação de gerenciamento ou até mesmo um sistema de gerenciamento. O iniciador deve ser cadastrado previamente entre os sistemas cooperantes de gerenciamento com um registro único para identificação. Este parâmetro identifica o iniciador autorizado a estabelecer associação de gerenciamento com o processo agente ao qual está vinculado.

As informações de contexto (IC) são condições que a associação deve cumprir para ser estabelecida, tais como: hora do dia, *host* de origem, canal de comunicação, etc. Este parâmetro é estabelecido de acordo com as necessidades de segurança particular de cada sistema de gerenciamento. A Figura 4.6 apresenta um modelo da lista LCA para esta política.

IdI	**IC**
User Paulo	< ..... >
User João	< ..... >
User IBM	< ..... >
User Sistema de Falhas Sun	< ..... >

Figura 4.6 - Lista LCA para Agentes na Política Individual-based

A Figura 4.7 apresenta um modelo hipotético de controle de acesso, na política *Individual-based*, para associação de processos de aplicação agente, onde relaciona a lista LPA com as listas LCA.

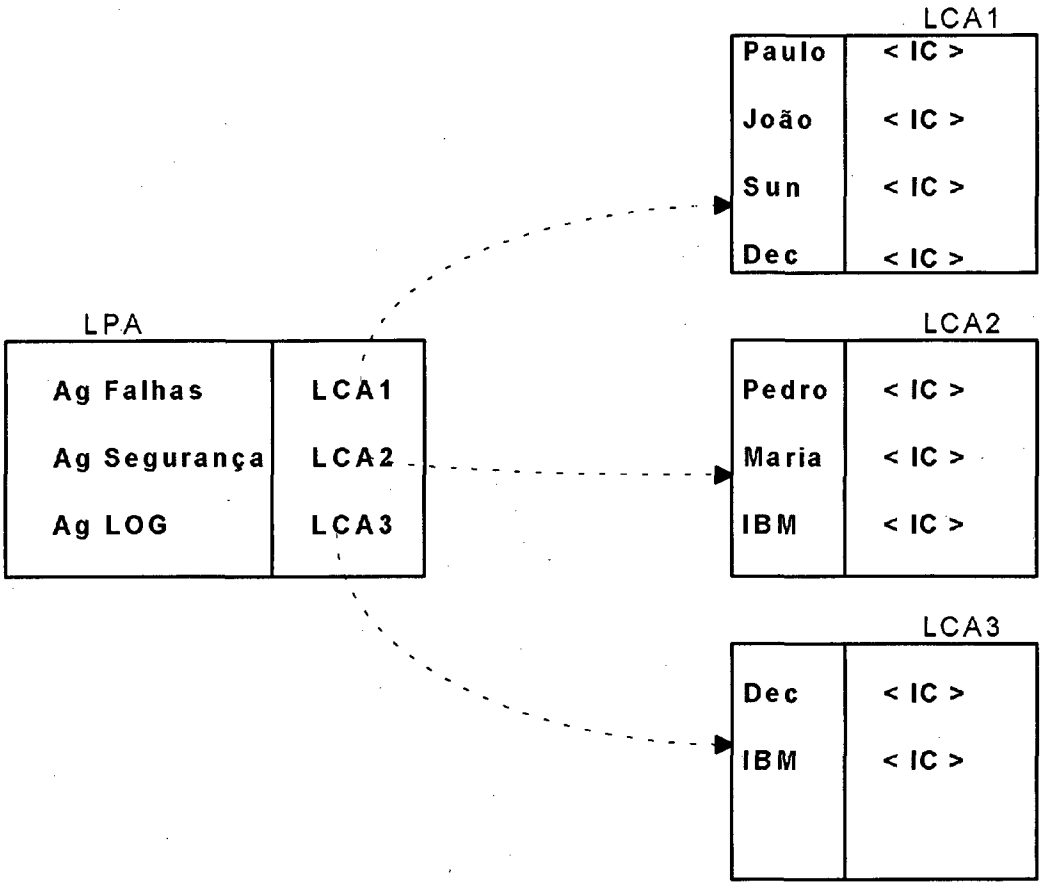


Figura 4.7 - Modelo de Controle de Acesso para Associação na Política Individual-based

A lista LCO (Figura 4.8), para objetos *target* do tipo objeto gerenciado, contém as classes (ICO) e os atributos (IAT) dos objetos gerenciados que necessitam de proteção. As operações de gerenciamento são orientadas a atributo ou sobre o objeto como um todo. Portanto, não só os objetos gerenciados necessitam de proteção como também seus atributos.

Cada entrada da lista LCO, também, tem associada uma lista LCA que apresenta as regras gerais (*Global Rules*) para todos os objetos gerenciados e atributos da classe.

ICO	IAT	ILCA	ILOG
Class Modem		LCA1	LOG1
Class Modem	Atr Velocidade	LCA1	LOG1
Class Servidor		LCA2	
Class Roteador		LCA2	

Figura 4.8 - Modelo da Lista LCO para a Política Individual-based

A lista LCA apontada na lista LCO, na política *Individual-based*, é composta por um identificador de iniciador, pelas operações de gerenciamento e pelas informações de contexto.

O identificador de iniciador (IdI) é o registro de identificação do iniciador dentro do sistema de gerenciamento. Um iniciador (ver item 3.4) deve ser cadastrado previamente entre os sistemas de cooperantes de gerenciamento com um registro único para identificação. Este parâmetro identifica o iniciador autorizado a pedir a execução de uma operação de gerenciamento para o objeto gerenciado ao qual o parâmetro está vinculado.

As operações de gerenciamento (OP) identificam quais as operações o iniciador está autorizado a executar sobre o objeto *target*. As operações podem ser: *create*, *delete*, *action*, *get* e *set* (ver item 2.4.2).

As informações de contexto (IC) são as condições que a operação de gerenciamento deve cumprir para ser realizada tais como: hora do dia, *host* de origem, canal de comunicação, etc. Este parâmetro é estabelecido de acordo com as necessidades de segurança particular de cada sistema de gerenciamento. A Figura 4.9 apresenta um modelo da lista LCA, associada a lista LCO, para esta política.

IdI	OP	IC
User Paulo	*Create, Delete, Action, Set, e Get*	< ..... >
User João	*Action, Set e Get*	< ..... >
User Sistema de Falhas	*Set e Get*	< ..... >
User Sistema de Log	*Get*	< ..... >

Figura 4.9 - Modelo da Lista LCA Associada à Lista LOC para a Política Individual-based

A lista de instâncias LOG, apontada pela lista LCO, é opcional e contém as instâncias da classe pela qual é apontada que necessitam de regras específicas de controle de acesso *Item Rules*. Estas regras específicas de controle de acesso são definidas através de uma lista de controle de acesso. A lista LOG é composta por um identificador de objeto gerenciado (IOG) e por um identificador de lista LCA (ILCA).

O identificador IOG é o registro único de identificação do objeto gerenciado dentro do sistema de gerenciamento. O identificador ILCA é um apontador de associação do objeto gerenciado com sua respectiva lista de controle de acesso.

IOG	ILCA
Modem 18	LCA5
Modem 19	LCA5
Modem 20	LCA6

Figura 4.10 - Modelo da Lista Opcional LOG na Política Individual-based

A lista LCA, associada aos de objeto gerenciados da lista LOG, tem a mesma formação das listas LCA associadas às classes da lista LCO. A única diferença é para as operações de gerenciamento, pois a operação do tipo *create* não pode ser realizada sobre objetos gerenciados, somente sobre as classes dos objetos gerenciados. Portanto, este parâmetro só pode assumir as seguintes operações de gerenciamento: *delete, action, get* e *set.*

A Figura 4.11 apresenta a estrutura das listas utilizadas pelo serviço de controle de acesso, que compõem o mecanismo de segurança, para objetos gerenciados e atributos na política *Individual-based.*

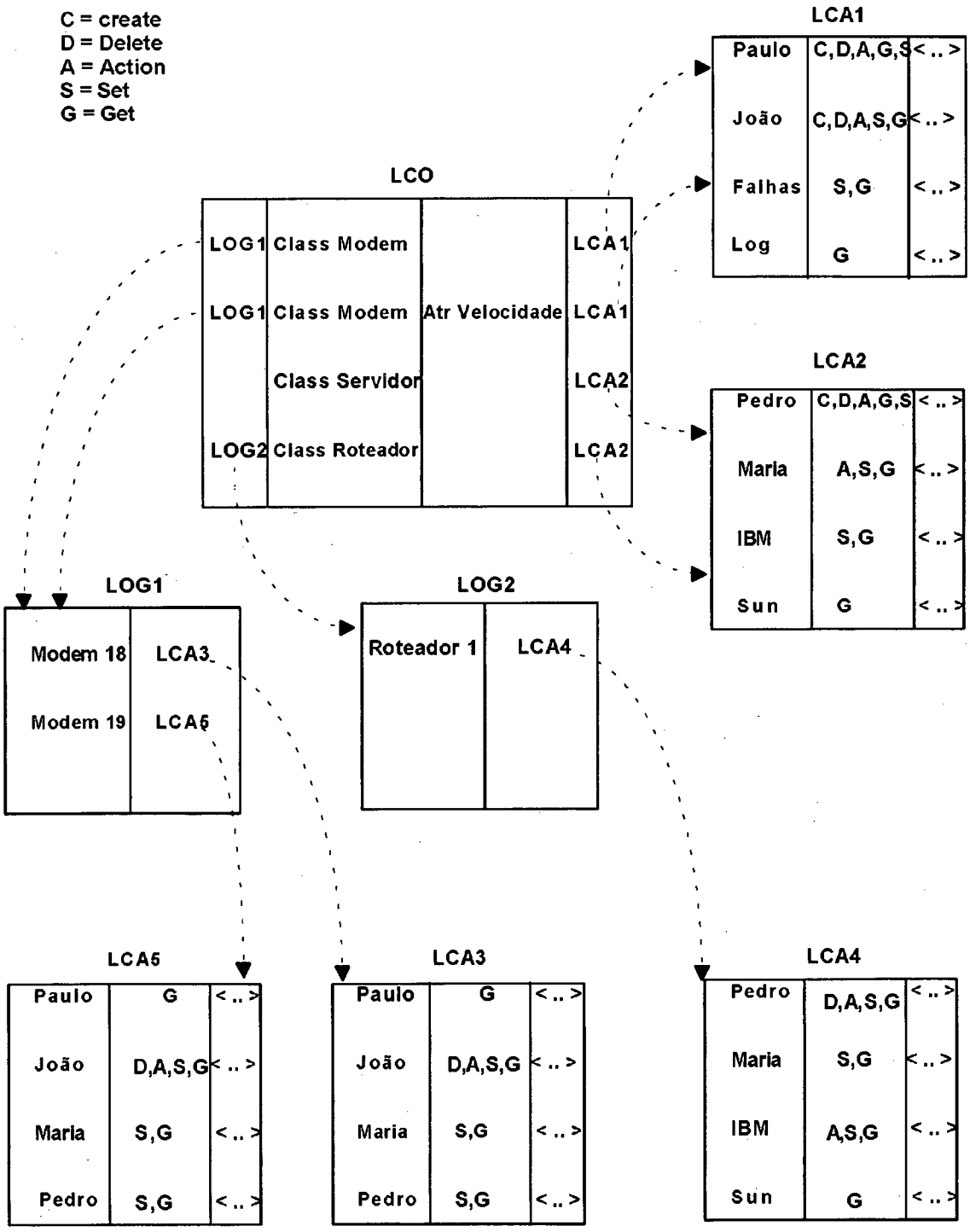


Figura 4.11 - Modelo de Controle de Acesso para Objetos Gerenciados na Política Individual-based

Quando um pedido de acesso é feito para um objeto *target* do domínio de segurança *Individual-based*, as regras aplicadas para a decisão de acesso seguem os seguintes critérios:

1) Se um pedido de acesso é feito para um objeto cuja a classe deste objeto não se encontra na lista LCO, o acesso a este objeto é permitido, pois este objeto não está sujeito ao controle de acesso;

2) Se um pedido de acesso é feito para um objeto cuja a classe se encontra na lista LCO, deve-se fazer as seguintes considerações para decidir se o acesso a este objeto *target* é válido ou não:

a) Se existir lista opcional LOG associada a classe deste objeto, e a instância requerida deste objeto fizer parte desta lista opcional LOG, aplicam-se as regras da lista LCA associada à instância deste objeto gerenciado da lista opcional LOG;

b) Se existir lista opcional LOG associada a classe deste objeto, e este objeto não fizer parte desta lista opcional LOG, então aplicam-se as regras da lista LCA associada a classe do objeto gerenciado que se encontra na lista LCO.

As regras contidas nas listas LCA garantem o acesso ao objeto a que estão associadas, somente para os iniciadores nelas contidos. Caso faça parte da lista LCA, o iniciador só terá direito de acesso se a operação que deseja executar estiver contida no conjunto de operações permitidas para ele, e se o pedido de acesso estiver de acordo com as informações contextuais. Se o iniciador não fizer parte desta lista, automaticamente o acesso, para este iniciador, é negado.

De acordo com o exemplo da Figura 4.11, os iniciadores *Paulo* e *João* podem executar todas as operações de gerenciamento para a classe *Modem*. Mas, para a instância *Modem 18* desta classe, *João* só pode executar operação *get*, enquanto *Paulo* pode executar as operações *delete*, *action*, *set* e *get*. Já para a instância *Modem 19*, ocorre o contrário: *João* pode executar as operações *delete*, *action*, *set* e *get*, enquanto *Paulo* só pode executar operação *get*.

No mesmo exemplo, *Pedro* e *Maria* não estão incluídos na lista LCA associada à classe *Modem*, porém nas listas LCA associadas às instâncias *Modem 18* e *Modem 19*, os iniciadores *Pedro* e *Maria* podem executar operações *get* e *set* somente para estas instâncias da classe, ao passo que para as outras instâncias da classe o acesso, para eles, é negado.

4.3 Group-Based

A política *Group-based* juntamente com a política *Individual-based* (ver item 3.2.1) formam as políticas do tipo *Identity-based*. Este tipo de política pode ser implementada através de listas de controle de acesso.

O modelo da política *Group-based* é similar ao modelo *Individual-based* descrito anteriormente. Contém uma lista LPA para processos de aplicação agente, e contém as listas LCO e LOG para classes e atributos de instâncias de objetos gerenciados que necessitam de controle de acesso. Associadas a estas listas encontram-se os mecanismos de listas de controle de acesso (LCA).

A diferença entre uma política e outra está na modelagem e definição dos iniciadores. Na política Individual-based, os iniciadores são identificados particularmente, enquanto que na política *Group-based*, vários iniciadores são agrupados e associados a um único identificador. Este identificador é usado para referenciar um grupo de iniciadores com interesses comuns dentro de um sistema de gerenciamento. Cabe à autoridade de segurança identificar estes grupos de interesses afins dentro de seu sistema.

Na Figura 4.11, as listas LCA2 e LCA4 que estão associadas à lista LPA, apresentam uma entrada para *User IBM*, que pode perfeitamente ser um identificador para os iniciadores pertencentes ao grupo *IBM* dentro do sistema de gerenciamento. Dentro deste contexto, a política *Group-based* segue o mesmo modelo de controle de acesso da política *Individual-based.*

4.4 Role-Based

A política *Role-based* é um outro modelo de política que pode, particularmente, ser implementada através de listas de controle de acesso. Conforme descrito anteriormente no item 3.2.1, esta política é uma variação da política *Group-based*, isto é, os iniciadores são agrupados não por áreas de interesses comum, mas por atividades de significância hierárquica, onde um gerente de rede tem mais direitos de acesso do que um técnico de rede, e este tem mais autorização que um operador de rede e assim por diante. As atividades mais importantes assumem níveis com maior autorização.

A política *Role-based* na Interface de Controle de Acesso, também, contém listas LPA, LCO e LOG iguais as da política *Group-based*. As diferenças entre uma política e outra refletem nas listas de controle de acesso (LCA) que expressam as atividades autorizadas a cada grupo particularmente.

A Figura 4.12 apresenta uma lista LPA, do domínio de segurança Role-based, contendo os processos de aplicação agente que necessitam de controle de associação através desta política. A estes processos estão associadas listas LCA. Estas listas LCA, associadas aos processos agentes, não sofrem alteração pois controlam um único tipo de atividade de gerenciamento: estabelecimento de associação.

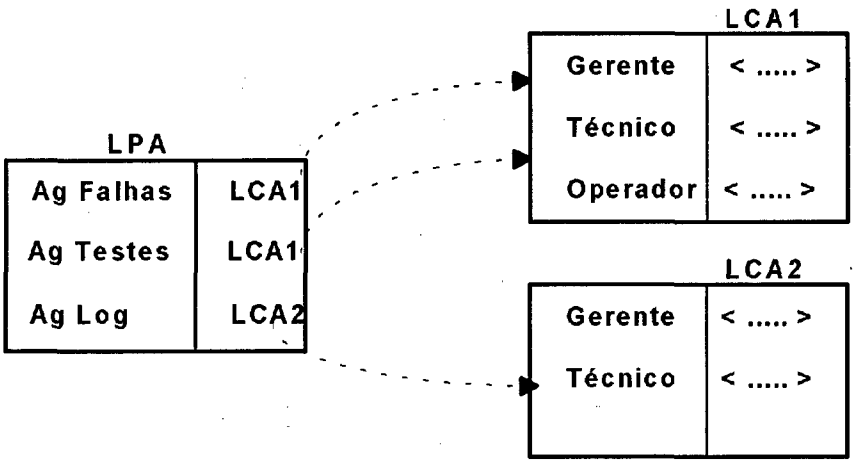


Figura 4.12 - Modelo de Lista LPA para a Política Role-based

As listas LCO e LOG, ilustradas na Figura 4.13, tem a mesma estrutura e filosofia do modelo *Group-based*. As listas LCA, apontadas por estas listas LCO e LOG, não apresentam diferenças quanto a estrutura. Possuem um identificador de iniciador (IdI), operações de gerenciamento e informações de contexto. Os mesmos critérios utilizados pela políticas *Individual-based* e *Group-based*, para decidir se um acesso é válido ou não, também são válidos para a política *Role-based*.

A diferança está na modelagem das regras de autorização contidas na lista LCA. Esta modelagem se encontra fora do escopo deste trabalho. Cabe a autoridade de segurança identificar, dentro de seu sistema de gerenciamento, e especificar as regras, expressas nas listas

LCA, correspondentes aos grupos com significância hierárquica na formulação da política de controle de acesso.

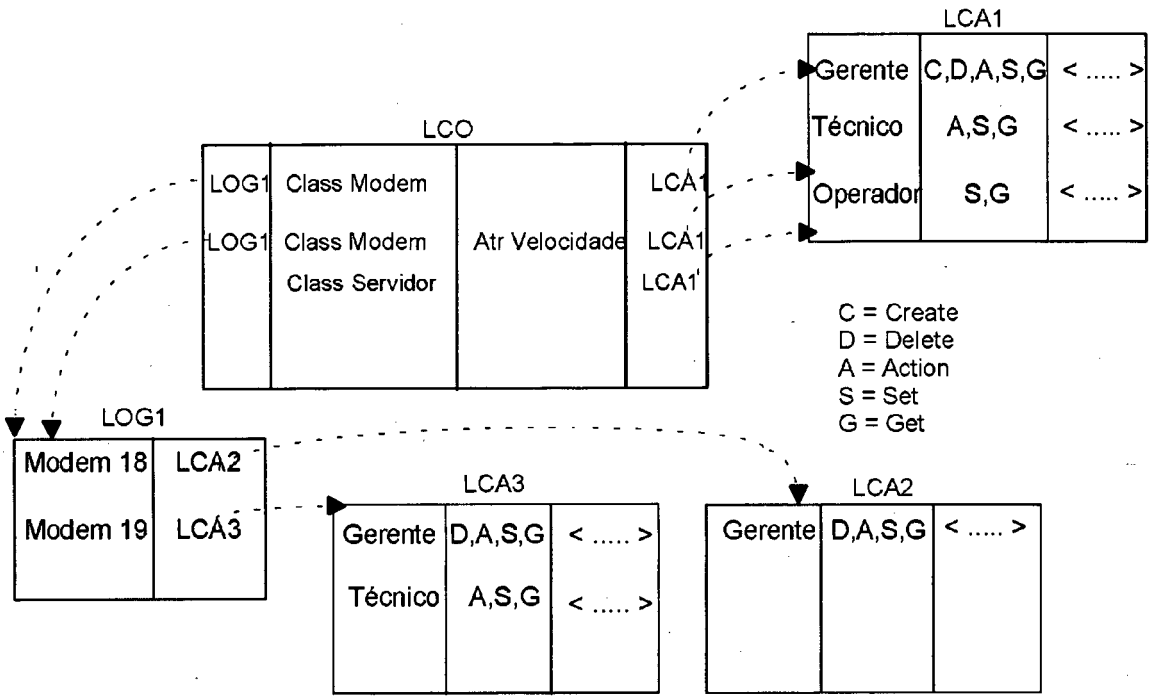


Figura 4.13 - Modelo de Controle de Acesso para Objetos Gerenciados na Política Role-based

4.5 Multi-Level

Seguindo as características desta política, abordadas no item 3.2.1, aos objetos *target* são associados nívies de sensibilidade e aos iniciadores níveis de *clearence*. Esta política, também, é implementada pelas listas LPA (Lista de Processo de Aplicação), LCO (Lista de Classes de Objeto Gerenciado), e LOG (Lista de Instâncias de Objeto Gerenciado).

Os processos de aplicação agente, que necessitam de controle de acesso, integrantes da lista LPA, deste domínio de segurança, são classificados com níveis hierárquicos de sensibilidade e associados a informações de contexto.

Os iniciadores, que desejam estabelecer associação de gerenciamento com um determinado processo de aplicação agente *target*, apresentam sua *clearence* que é comparada, pela função ADF do Sistema de Controle de Autorização (SCA), com o nível de sensibilidade do agente requerido. A associação só é aceita se o nível de *clearence* do iniciador é maior ou igual ao nível de sensibilidade do processo de aplicação agente e se estiver de acordo com as

informações de contexto. A Figura 4.14 apresenta um exemplo do modelo da lista LPA para a política *Multi-level*.

A lista LPA é composta por um identificador de processo de aplicação e por um identificador de rótulo. O identificador de processo de aplicação agente (IAG) é um descritor de identificação do agente dentro do sistema de gerenciamento. O identificador de rótulo (IOG) é um apontador para o nível de sensibilidade e para as informações de contexto associadas ao objeto *target:* processo de aplicação agente.

O identificador de nível de sensibilidade (NS) é um descritor de nível de sensibilidade dentro de uma hierarquia de níveis como: *top-secret, secret, confidential* e *unrestricted* para estabelecimento de associação.

As informações de contexto são as condições que a operação de gerenciamento deve cumprir para ser realizada, tais como: hora do dia, *host* de origem, canal de comunicação, etc. Este parâmetro é estabelecido de acordo com as necessidades de segurança particulares de cada sistema de gerenciamento.

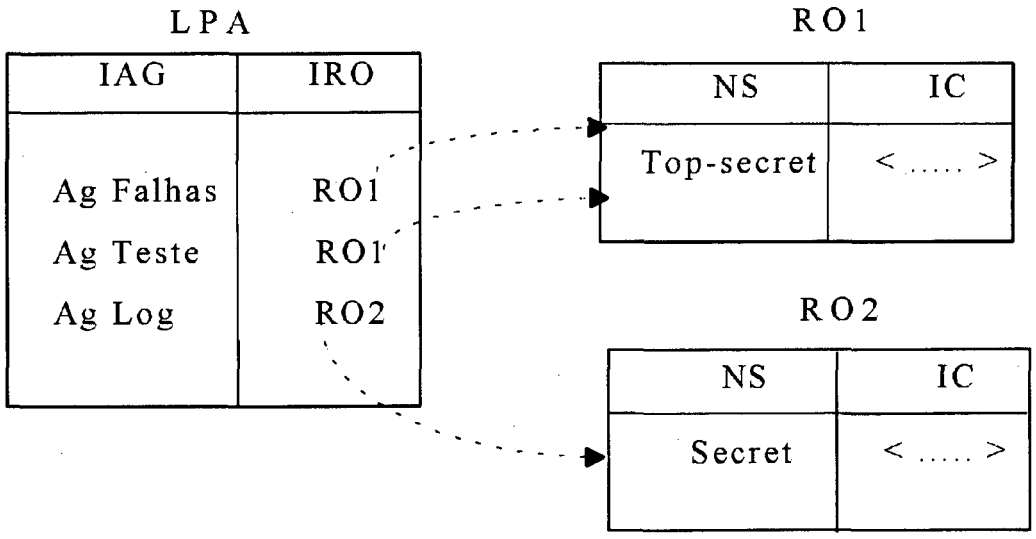


Figura 4.14 - LPA da Política Multi-level

Sobre as classes e atributos de classes de objetos gerenciados, integrantes da lista LCO, também, são associados níveis de sensibilidade que, por sua vez, são comparados com o nível de *clearence* dos iniciadores pela função ADF do sistema SCA para decidir se as operações de gerenciamento, sobre estes objetos *target*, são permitidas ou não.

A lista LCO da política *Multi-level* contém um identificador de classe de objeto gerenciado, um identificador de atributo de classe, um identificador de rótulo e um identificador para listas LOG.

O identificador de classe de objeto gerenciado (ICO) é o registro único de identificação da classe do objeto gerenciado dentro do sistema de gerenciamento.

O identificador de atributo de classe (IAT) é o registro único de identificação do tipo do atributo dentro do sistema de gerenciamento.

O identificador de rótulo (IRO) é um apontador para o identificador de nível de sensibilidade e para as informações de contexto.

O identificador da lista LOG (ILOG) é o apontador de associação do objeto *target* a sua respectiva lista opcional.

O identificador de nível de sensibilidade (NS) é um descritor de nível de sensibilidade dentro de uma hierarquia de níveis como: *top-secret, secret, confidential* e *unrestricted* para operações de gerenciamento.

As informações de contexto são as condições que a operação de gerenciamento deve cumprir para ser realizada, tais como: hora do dia, *host* de origem, canal de comunicação, etc. Este parâmetro é estabelecido de acordo com as necessidades de segurança particulares de cada sistema de gerenciamento.

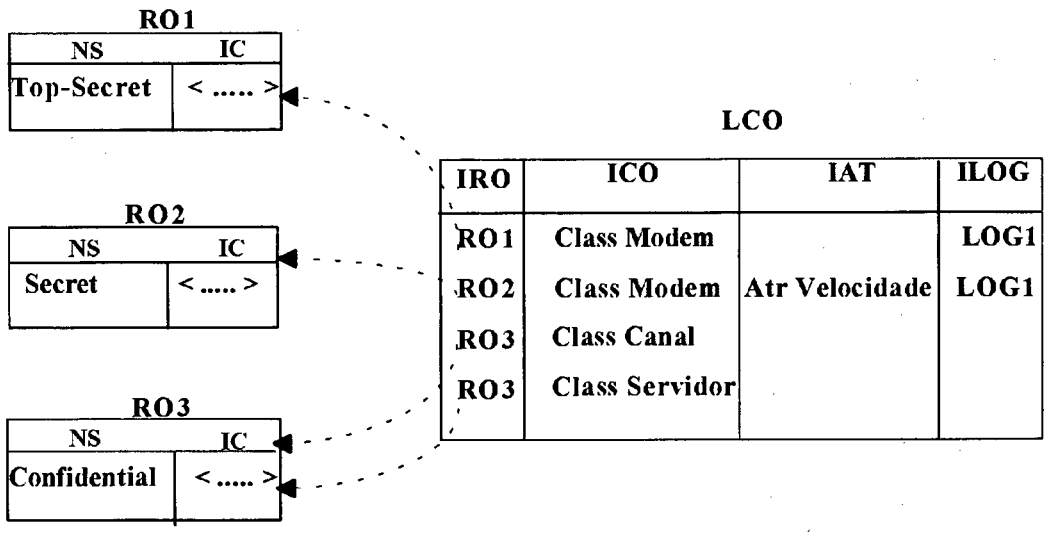


Figura 4.15 - Lista LOC da Política Multi-level

A função ADF, implementada através do sistema SCA, utiliza os seguintes critérios para permitir ou negar o pedido de operação de gerenciamento sobre um objeto *target* integrante da lista LCO:

- operação *create* só é permitida para iniciadores com *clearence* do mesmo nível ou menor que o nível de sensibilidade da classe do objeto gerenciado. Esta regra é empregada para não permitir que um iniciador de nível hierarquicamente superior crie objetos para usuários de nível inferior (regra **_property*);

- operação *set*: só é permitida para usuários com *clearence* do mesmo nível ou menor que o nível de sensibiliade do atributo que será manipulado. Baseia-se na mesma regra empregada para operações *create* (regra **_property*), para não permitir que iniciadores de nível superior passem, através da operação *set*, informações de nível superior para iniciadores com *clearence* inferior;

-operações *get*, *action* e *delete* só é garantida para iniciadores com *clearence* do mesmo nível ou maior que o nível de sensibilidade do OG que será manipulado. Esta regra é conhecida como *Simple Security Condition* (ver item 3.2.1).

A lista opcional LOG, com regras específicas para instâncias, é formada por um identificador de instância de objeto gerenciado (IOG) e por um identificador de rótulo (IRO).

O identificador IOG é o registro único de identificação do objeto gerenciado dentro do sistema de gerenciamento.

O identificador IRO é um apontador para o rótulo que é composto por um identificador de nível de sensibilidade e pelas informações de contexto.

O identificador de nível de sensibilidade (NS) é um descritor de nível de sensibilidade dentro de uma hierarquia de níveis como: *top-secret*, *secret*, *confidential* e *unrestricted* para operações de gerenciamento.

As informações de contexto são as condições que a operação de gerenciamento deve cumprir para ser realizada tais como: hora do dia, *host* de origem, canal de comunicação, etc. Este parâmetro é estabelecido de acordo com as necessidades de segurança particular de cada sistema de gerenciamento.

A Figura 4.16 ilustra um exemplo da lista LOG para o domínio de segurança *Multi-level.*

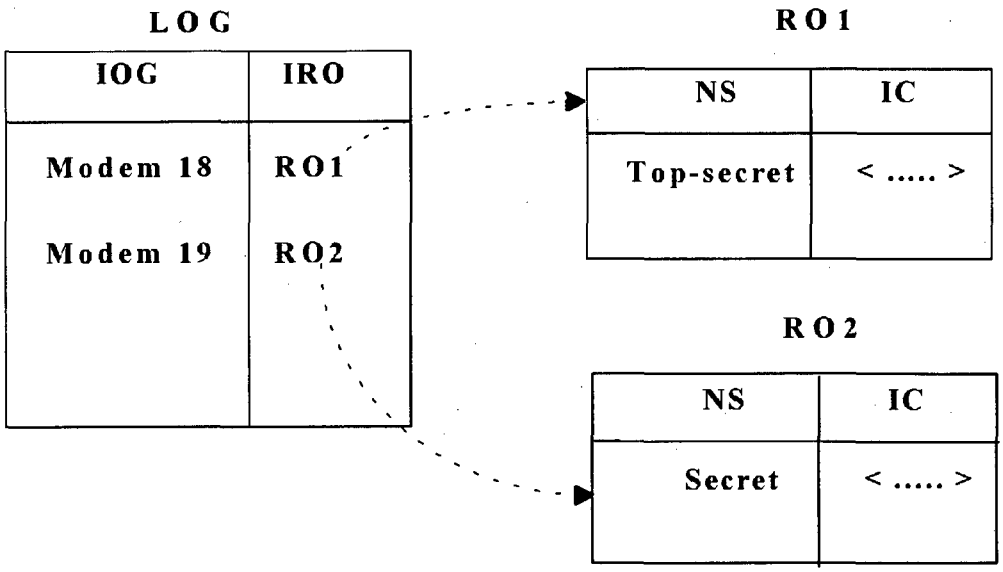


Figura 4.16 - LOG da Política Multi-level

Para as listas opcionais LOG, a função ADF do sistema SCA, ao decidir se uma operação de gerenciamento sobre uma instância ou um atributo de uma instância de objeto gerenciado é válida ou não, adota os mesmos critérios de precedência entre as listas LCO e LOG descritos na política *Individual-based* e, depois, aplica as regras **_property* e *Simple Security Condition* descritas anteriormente na lista LCO.

4.6 Modelo Militar

O Modelo Militar de Segurança é um tipo de política *Multi-level* mais rigorosa, conforme descrito no item 3.2.1. Além de classificar a informação com um nível de sensibilidade, este modelo emprega a regra conhecida como *need-to-kow*. As informações de gerenciamento que necessitam de proteção de acesso, *targets*, são associadas a domínios, ou seja áreas de utilização. As regras de autorização são associadas às listas LPA, LCO e LOG. Um pedido de acesso a um objeto *target*, integrante destas listas, neste modelo de política, deve satisfazer as regras **_property*, *Simple Security Condition* e *need-to-know* para ser autorizado pela função ADF do Sistema de Controle de Autorização (SCA) da Interface.

As listas para processos de aplicação LPA contém o identificador de agente (IAG) e o identificador de rótulo (IRO). O rótulo é composto pelo identificador de nível de sensibilibidade (NS), pelas informações de contexto (IC) e por um identificador de domínio DOM.

Os identificadores IAG, NS, e IC são os mesmos empregados para a política *Multi-level*. O identificador DOM indica a área ou as áreas de utilização (*need-to-know*) a que está vinculado o objeto *target* e, consequentemente, o iniciador deve pertencer para estabelecer aassociação de gerência. Na Figura 4.17, pode-se observar um exemplo da lista LPA para a política empregada pelo Modelo Militar.

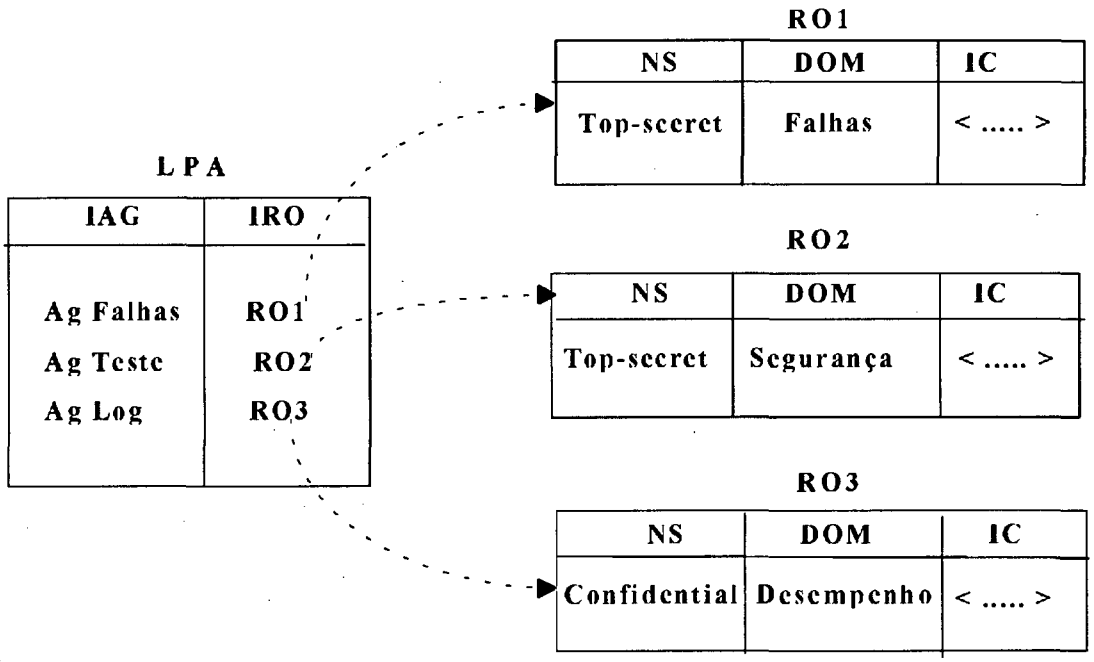


Figura 4.17 - LPA da Política do Modelo Militar

Às listas de classes e atributos de objetos gerenciados LCO, também, são associados níveis de sensibilidade, domínio e as informações de contexto, através de rótulos, aos seus objetos *target*. O conteúdo da lista LCO para esta política é formado por: um identificador ICO; um identificador IAT; um identificador de rótulo IRO; e um identificador de lista opcional ILOG.

O identificador IRO é um apontador para o nível de sensibilidade, para o identificador DOM e para as informações de contexto IC associadas ao objeto *target*. O

conteúdo dos outros identificadores é o mesmo utilizado pelas outras políticas. A Figura 4.18 ilustra o conteúdo desta lista para a política do Modelo Militar.

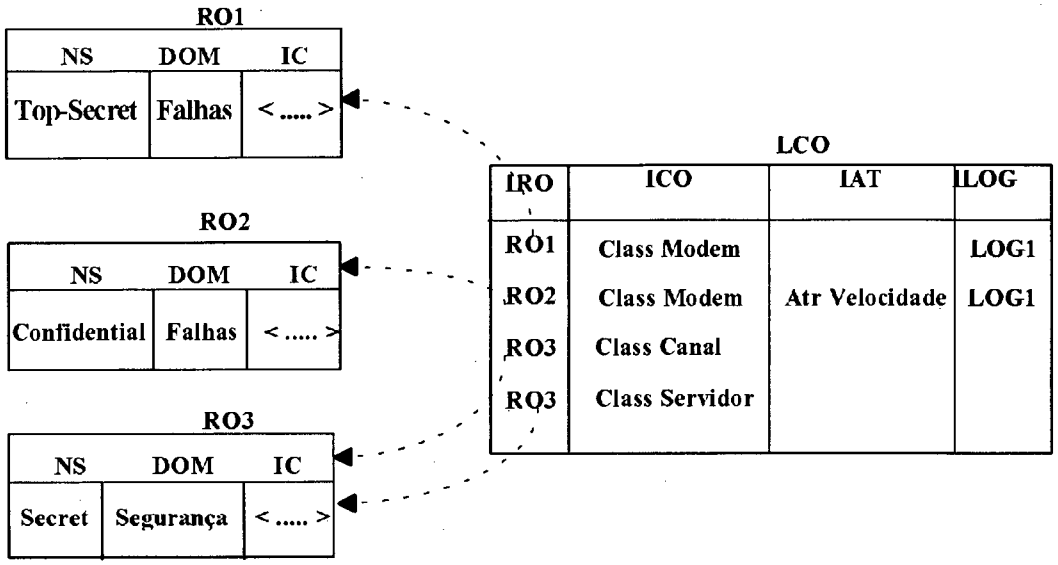


Figura 4.18 - LCO da Política Modelo Militar

A lista opcional para instâncias de objetos gerenciados LOG, apontada pela lista LCO, segue a mesma filosofia da lista para classes e atributos de objetos gerenciados LCO: aos objetos *target* da lista LOG, através de rótulos, associa-se um identificador NS, um identificador DOM e as informações de contexto IC. A Figura 4.19 apresenta um modelo da estrutura da lista LOG para esta política.

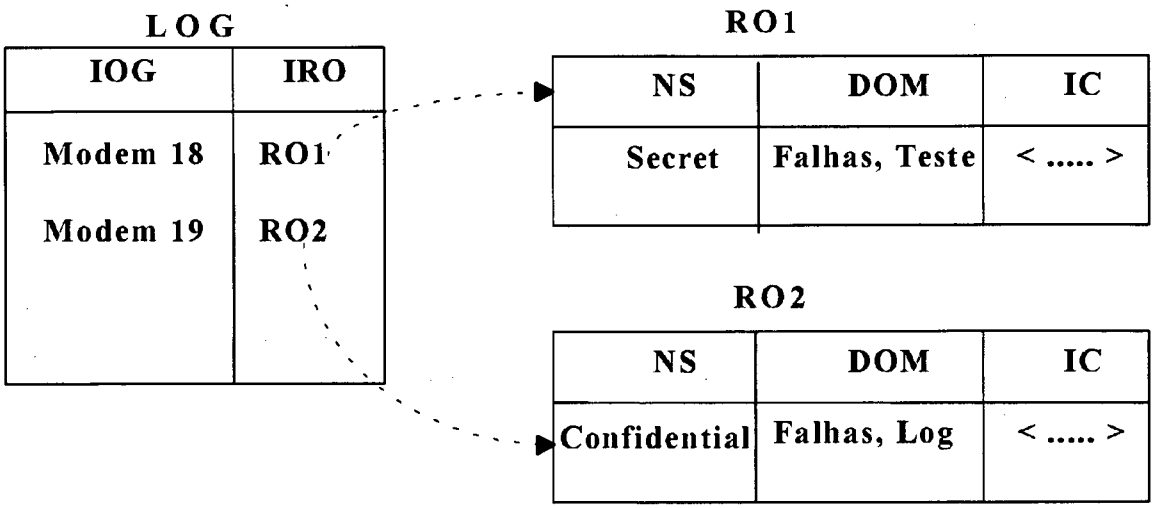


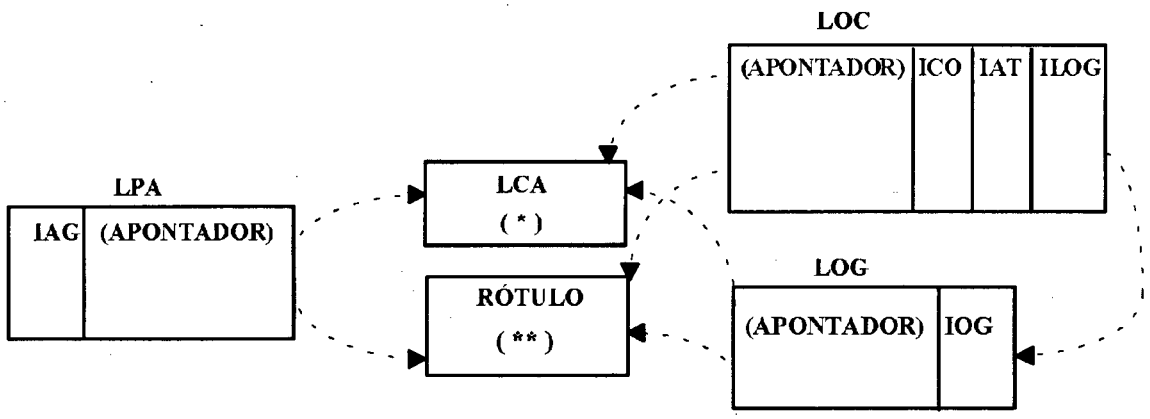
Figura 4.19 - LOG do Modelo Militar

4.7 Mecanismos de Proteção e a Base BDA

As listas LPA, LCO, LOG, LCA e o rótulo fazem parte dos mecanismos de segurança utilizados pela Interface de Controle de Acesso para implementar as políticas de controle de acesso. Estes mecanismos encontram-se armazenados na Base de Definição de Autorização (BDA) e contém as regras de autorização utilizadas pelo Sistema de Controle de Autorização (SCA) para decidir se um pedido de acesso é válido ou não.

As listas LPA, LCO e LOG contém os elementos de informação de um sistema de gerenciamento que necessitam de proteção contra o acesso de iniciadores não autorizados. Cada entrada destas listas corresponde a um objeto *target* que possui um atributo, do tipo apontador, para identificar as regras de autorização usadas na proteção deste objeto.

Independente do modelo de política de acesso utilizado, as listas LPA, LCO e LOG possuem a mesma estrutura, conforme a Figura 4.20.



(*) - implementa políticas Individual-based, Group-based e Role-based

(**)- implementa políticas Multi-level e Modelo Militar

Figura 4.20 - Modelo Genérico dos Relacionamentos entre as Listas LPA, LCO e LOG

Para distinguir o tipo de política de acesso empregada para proteger um objeto *target*, componente destas listas, um novo atributo, chamado *Tipo de Política de Acesso* (TAP) é usado. Este atributo é incluído para todos os objetos *target* contidos nas listas LPA, LCO e LOG, conforme apresentado na Figura 4.21, e permite ao administrador de segurança combinar diferentes políticas de acesso, conforme as necessidades de proteção de seu sistema de gerenciamento.

Dentro deste contexto, cada domínio de gerenciamento contém, armazenada em sua base BDA, uma única lista LPA, para os processos de aplicação, e uma única lista LCO, para classes e atributos de objetos gerenciados, que permitem a implementação de diferentes políticas de controle de acesso.

A base BDA é um componente da base de informações de segurança SMIB (*Security Management Information Base*) utilizada pela área funcional de segurança e, como a própria SMIB (ver item 3.5), é distribuída ao longo de cada domínio de sistema aberto que necessita de controle de acesso.

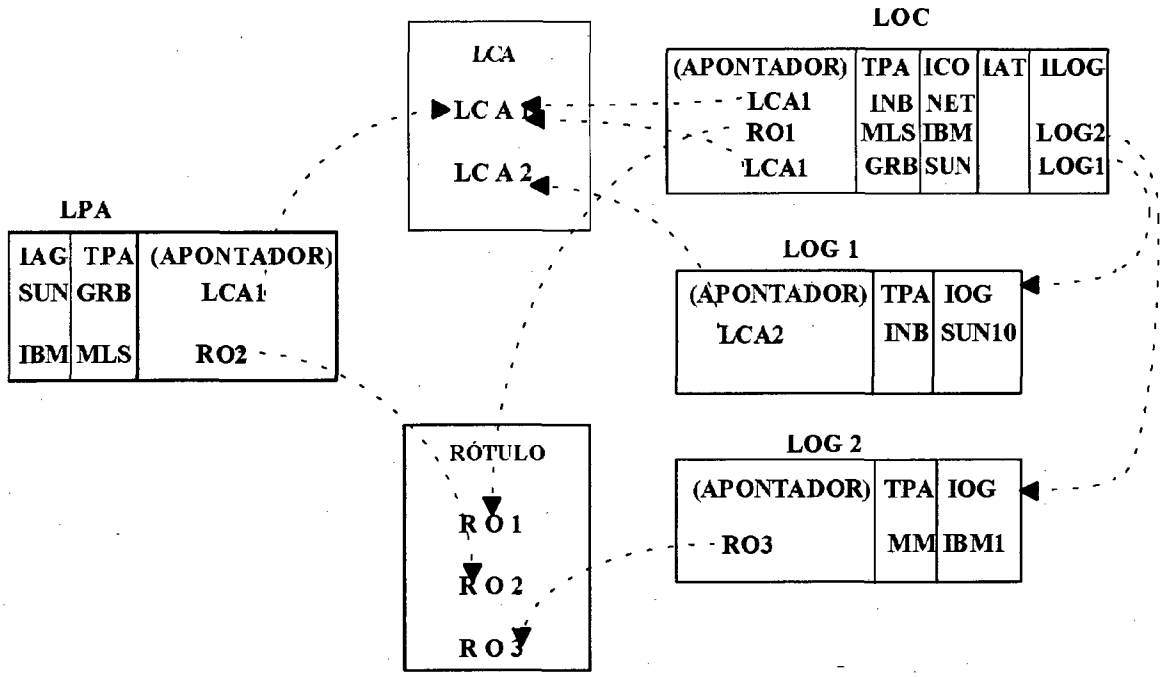


Figura 4.21 - Modelo de Armazenamento das Listas na Base BDA

4.8 Sistema de Controle de Autorização (SCA)

O Sistema de Controle de Autorização (SCA) tem a funcionalidade de controle de acesso baseada na Função de Controle de Acesso [ISO 10164-9] (ver item 3.3.2.3) e é composto pelas funções:

- *Access Control Enforcement Function* (AEF);
- *Access Control Decision Function* (ADF).

As funções AEF e ADF trabalham em conjunto com as listas LPA, LCO, LOG, LCA e o rótulo a fim de proteger os recursos de rede manipulados por um sistema de gerência. Não permitem que entidades não autorizadas estabeleçam associações e controlem as operações de gerenciamento sobre os objetos gerenciados, armazenados na MIB.

O sistema SCA, através da função ADF, trabalha como um motor de inferências que age sobre a base BDA, usando uma estratégia de encadeamento para frente, onde decide se o pedido de acesso é permitido ou não.

Estratégia de encadeamento para frente baseia-se em regras que codificam sobre como responder a certas configurações de entrada [RIC94].

A função AEF recebe os pedidos para estabelecimento de associação e para operações de gerenciamento. Seleciona os parâmentros importantes para o controle de acesso (identificador do iniciador; identificador da classe do objeto; identificador do objeto gerenciado; identificação do atributo da classe; operação de gerenciamento; hora; endereço; etc) e repassa-os para a função ADF. A função ADF é responsável por receber os parâmetros da função AEF e decidir se o pedido é valido ou não. Para isto, ela compara os parâmetros recebidos com as regras de autorização armazenadas na base BDA.

Em outras palavras, quando a função AEF fornece os parâmetros, a função ADF faz referência às informações na base BDA e aplica as técnicas de encadeamento para frente [LEV88]. A técnica de encadeamento para frente é descrita através de um conjunto de condições e consequências que nada mais são do que um sistema de regras do tipo *se / então*.

De acordo com o modelo da Função de Controle de Acesso [ISO 10164-9], a função ADF após negar um pedido de acesso, deve enviar, também, à função AEF, instruções de prosseguimento à negação, como por exemplo, enviar uma resposta negativa, ignorar o pedido de acesso ou simplesmente abortar a conexão.

Porém, as instruções de prosseguimento à negação estão diretamente ligadas a política particular adotada para cada sistema de gerência, e o modelo da Interface de Controle de Acesso proposto, objetiva atender às políticas de segurança de uma forma genérica. Portanto, ao negar um pedido de acesso, a função ADF não indica instruções especiais de negação, a não ser a própria resposta negativa de acesso.

Em seguida, descreve-se as inferências de encadeamento para frente do sistema SCA para as políticas modeladas na base BDA. Para cada política modelada na base BDA, existem dois tipos de sistemas de regras: um para descrever as condições e consequências a nível de estabelecimento de associação e outro para o nível de operações de gerenciamento.

4.8.1 Inferências Individual-Based

O Sistema de Controle de Acesso (SCA) através da função AEF filtra os seguintes parâmetros do pedido de estabelecimento de associação:

- identificador de agente (IAG): descritor do agente com o qual deseja-se o estabelecimento de associação;

- identificador de iniciador (IdI): descritor do usuário que requer o estabelecimento de associação;

- informações de contexto (IC): condições que o pedido deve satisfazer para que a associação seja estabelecida.

Após filtrar os parâmetros acima, a função AEF repassa-os para a função ADF do sistema SCA que faz referência à Lista de Processo de Aplicação LPA armazenada na base BDA e aplica as regras apresentadas na Figura 4.22.

SE $(IAG_{pedido} = IAG_{LPA})$
E $(IdI_{pedido} = IdI_{LPA})$ (*)
E $(IC_{pedido} \subseteq IC_{LPA})$ (*)
ENTÃO
associação permitida
retém informações do iniciador
SENÃO
associação negada

RETORNA DECISÃO DE ACESSO PARA FUNÇÃO AEF

(*) - parâmetros IdI_LPA e IC_LPA são da lista LCA apontada pela lista LPA

Figura 4.22 - Inferências para Associações de Gerenciamento na Política Individual-based

Para as operações de gerenciamento, a função AEF seleciona, do pedido de acesso, os parâmetros de controle de acesso e repassa-os à função ADF para ela inferir de acordo com

as regras de autorização que se encontram nas listas LCO e LOG, referentes ao domínio de segurança armazenadas na base BDA.

Os parâmetros de controle de acesso selecionados e enviados à função ADF são o identificador da classe do objeto ICO; identificador da instância do objeto, exceto para operações do tipo *create*; identificador de atributo de classe IAT para operações orientadas a atributo (quando a operação for para o objeto como um todo (*create*, *action* e *delete*) este parâmetro é nulo); a operação de gerenciamento (OP) e as informações de contexto IC.

A função ADF infere sobre as listas LCO e LOG de acordo com as regras da Figura 4.23.

SE $(ICO_{pedido} = ICO_{LCO})$
E $(IAT_{pedido} = IAT_{LCO})$
ENTÃO
  SE $(ILOG_{LCO} \neq NULO)$
  ENTÃO
    SE $(IOG_{pedido} = IOG_{LOG})$
    ENTÃO
      SE $(IdI_{retido} = IdI_{LOG})$ (*)
      E $(OP_{pedido} \subseteq OP_{LOG})$ (*)
      ENTÃO
        operação permitida
      SENÃO
        operação negada
    SENÃO
      // sem restrição para instância de classe
      // pesquisa na lista LCO
  SENÃO
    (Pesquisa na Lista LCO)
    SE $(IdI_{retido} = IDI_{LCO})$ (**)
    E $(OP_{pedido} = OP_{LCO})$ (**)
    ENTÃO
      operação permitida
    SENÃO
      operação negada
SENÃO
  operação permitida

RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF

(*) - parâmetros IdI_LOG e OP_LOG são da lista LCA apontada pela lista LOG
(**) - parâmetros IdI_LCO e OP_LCO são da lista LCA apontada pela lista LCO

Figura 4.23 - Inferências para Operações de Gerenciamento na Política Individual-based

4.8.2 Inferências Group-Based e Role-Based

As inferências feitas pela função ADF para a política *Individual-based*, da Figura 4.21, são as mesmas utilizadas para as políticas *Group-based* e *Role-based*.

A política *Group-based* difere da política *Individual-based* na modelagem dos iniciadores, mas a estrutura das listas LPA, LCO, LOG e LCA, utilizadas pela função ADF para decidir se um pedido de acesso é válido ou não, são idênticas. O mesmo acontece com a política *Role-based*. Esta política difere da política *Group-based* na modelagem das operações permitidas. Enquanto que no modelo *Group-based*, as atividades são identificadas particularmente em cada grupo (*política discretionary*), na política *Role-based* os grupos se adequam as atividades (*política mandatory*).

4.8.3 Inferências Multi-level

Nesta política, a função AEF do sistema SCA, ao receber um pedido de associação para um processo de aplicação, do domínio de segurança *Multi-level*, seleciona os seguintes parâmetros de controle de acesso do pedido para enviá-los a função ADF: identificador de agente IAG; identificador do nível de *clearence* NC do iniciador que requer a associação; e informações de contexto IC.

A função ADF, ao receber os parâmetros de controle de acesso, faz referência a lista LCA, armazenada na base BDA e aplica as regras para associação contidas na Figura 4.24.

SE $(IAG\_pedido = IAG\_LPA)$
E $(NC\_pedido \geq NC\_LPA)$
E $(IC\_pedido \subseteq IC\_LPA)$
ENTÃO
associação permitida
informações do iniciador retidas
SENÃO
associação negada
RETORNA DECISÃO DE ACESSO PARA FUNÇÃO AEF

(*) - parâmetros NC_LPA e IC_LPA são do rótulo apontado pelo identificador IRO da lista LPA

Figura 4.24 - Inferências para Associação na Política Multi-level

Uma vez estabelecida a associação de gerência, a função AEF passará a receber pedidos de operação de gerenciamento e a enviar os parâmetros de controle de acesso, para a função ADF, tais como: identificador da classe do objeto ICO; identificador de atributo da classe IAT; operação de gerenciamento (OP); informações de contexto IC. O identificador IAT para operações *create*, *delete* e *action* é nulo.

A função ADF, ao receber os parâmetros de controle de acesso, junta-os com as informações retidas do pedido de associação do iniciador (identificador NC) e infere sobre as listas LCO e LOG para garantir ou negar o pedido de autorização de acordo com as regras da Figura 4.25(a) e 4.25(b).

```
// inferências para operações de gerenciamento na política Multi-level

SE      (ICO_pedido = ICO_LCO)
        E       (IAT_pedido = IAT_LCO)
        ENTÃO
                testa apontador da lista LOG
        SENÃO
                operação permitida

RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF


// teste do apontador da lista LOG

SE      (ILOG_LCO ≠ NULO)
ENTÃO
        infere sobre a lista LOG
SENÃO
        infere sobre a lista LOC
```

Figura 4.25(a) - Inferências para Operações de Gerenciamento na Política Multi-level

// inferência sobre a lista LOG da política Multi-level

SE (IOG_pedido = IOG_LOG)
E (IC_pedido ⊆ IC_LOG) (*)
ENTÃO
SE (NC_retido ≤ NS_LOG) (*)
ENTÃO
SE (OP_pedido = set)
ENTÃO
operação permitida
SENÃO
operação negada
SENÃO
SE (OP_pedido = delete ou action ou get)
ENTÃO
operação permitida
SENÃO
operação negada
RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF

SENÃO
infere sobre a lista LCO

(*) - parâmetros IC_LOG e NS_LOG são do rótulo apontado pelo identificador IRO da lista LOG

// inferência sobre a lista LCO da política Multi-level

SE (NC_retido ≤ NS_LCO)
ENTÃO
SE (OP_pedido = set ou create)
ENTÃO
operação permitida
SENÃO
operação negada
SENÃO
SE (OP_pedido = delete ou action ou get)
ENTÃO
operação permitida
SENÃO
operação negada
RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF

(*) - parâmetro NS_LCO são do rótulo apontado pelo identificador IRO da lista LCO

Figura 4.25(b) - Inferências para Operações de Gerenciamento na Política Multi-level

4.8.4 Inferências Modelo Militar

As inferências desta política assemelham-se às inferências da política *Multi-level*. Além de todas as regras utilizadas para o modelo *Multi-level*, às inferências da política do Modelo Militar acrescenta-se mais uma restrição de acesso que é o identificador de domínio (DOM).

A função AEF filtra dos pedidos de estabelecimento de associação, além do parâmetro identificador de nível de clearence NS do iniciador, o parâmetro identificador de domínio (DOM). Estes parâmetros são comparados pela função ADF com as regras da lista LPA. Esta inferência é feita conforme apresentado na Figura 4.26.

SE $(IAG\_pedido = IAG\_LPA)$
E $(NC\_pedido \geq NC\_LPA)$ (*)
E $(IC\_pedido \subseteq IC\_LPA)$ (*)
E $(DOM\_pedido \subseteq DOM\_LPA)$ (*)
ENTÃO
associação permitida
informações do iniciador retidas
SENÃO
associação negada
RETORNA DECISÃO DE ACESSO PARA FUNÇÃO

(*) - parâmetros NC_LPA, IC_LPA e DOM_LPA são do rótulo apontado pelo identificador IRO da lista LPA

Figura 4.26 - Inferências para Associação no Modelo Militar

A Figura 4.27(a) e 4.27(b) apresenta as inferências feitas pela função ADF do sistema SCA sobre as listas LCO e LOG política do Modelo Militar.

```
// inferências para operações de gerenciamento no Modelo Militar

SE      (ICO_pedido = ICO_LCO)
        E       (IAT_pedido = IAT_LCO)
                ENTÃO
                        testa apontador da lista LOG
                SENÃO
                        operação permitida
RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF

// teste do apontador da lista LOG do Modelo Militar

SE      (ILOG_LCO ≠ NULO)
ENTÃO
        infere sobre a lista LOG
SENÃO
        infere sobre a lista LOC

// inferência sobre a lista LOG do Modelo Militar

SE      (IOG_pedido = IOG_LOG)
E       (IC_pedido ⊆ IC_LOG)                    (*)
E       (DOM_pedido ⊆ DOM_LOG)                  (*)
ENTÃO
        SE      (NC_retido ≤ NS_LOG)            (*)
                ENTÃO
                SE      (OP_pedido = set)
                ENTÃO
                        operação permitida
                SENÃO
                        operação negada
        SENÃO
                SE      (OP_pedido = delete ou action ou get)
                ENTÃO
                        operação permitida
                SENÃO
                        operação negada
        RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF

SENÃO
        infere sobre a lista LCO
```

(*) - parâmetros IC_LOG, DOM_LOG e NS_LOG são do rótulo apontado pelo identificador IRO da lista LOG

Figura 4.27(a) - Inferências para Operações de Gerenciamento no Modelo Militar

```
// inferência sobre a lista LCO do Modelo Militar
SE    (IC_pedido ⊆ IC_LCO)          (*)
E     (DOM_pedido ⊆ DOM_LCO)        (*)
ENTÃO
      SE    (NC_retido ⊆ NS_LCO)    (*)
      ENTÃO
            SE    (OP_pedido = set ou create)
            ENTÃO
                  operação permitida
            SENÃO
                  operação negada
      SENÃO
            SE    (OP_pedido = delete ou action ou get)
            ENTÃO
                  operação permitida
            SENÃO
                  operação negada
SENÃO
      operação negada

RETORNA DECISÃO DE ACESSO PARA A FUNÇÃO AEF
```

(*) - parâmetros IC_LCO, DOM_LCO e NS_LCO são do rótulo apontado pelo IRO da lista LOG

Figura 4.27(b)- Inferências para Operações de Gerenciamento no Modelo Militar

4.9 SISTEMA DE DEFINIÇÃO DE AUTORIZAÇÃO (SDA)

O Sistema de Definição de Autorização (SDA) é uma ferramenta de apoio às autoridades de segurança. Permite que as regras de autorização de um sistema de gerência sejam definidas de forma automática, dentro de um ambiente simples e amigável.

O sistema SDA implementa serviços específicos para a manipulação dos mecanismos de segurança da Base de Dados de Autorização (BDA). É através do sistema SCA que a autoridade consegue administrar as regras de autorização armazenadas em forma de listas na base BDA.

A modelagem da política de autorização, ou seja a definição de quem pode fazer o que, com quem, e quando, deve ser feita fora do escopo da Interface de Controle de Acesso, pois não é especificada pelo padrão OSI. Cabe à autoridade de segurança modelar suas

necessidades da melhor maneira possível, a fim de obter o nível de segurança requerido para o seu sistema de gerência.

A Arquitetura de Segurança OSI [ISO 7498-2] sugere que a autoridade, depois de definir os aspectos globais da política a serem adotados, utilize processos de refinamento sucessivo, adicionando mais detalhes em cada estágio do domínio que se deseja proteger, até que se tenha uma política mais precisa. A política aperfeiçoa-se à medida que é colocada em prática e que novos refinamentos são feitos com este objetivo. Dentro deste contexto, o sistema SDA necessita não só de serviços e funções para incluir definições na base BDA, mas também de funções que permitam alterações em busca de aperfeiçoamento.

A autoridade de segurança define qual ou quais são as políticas de segurança adotadas em seu domínio, ou seja define a política a ser empregada nos agentes e nos objetos gerenciados que formam o domínio, estipulando as regras de associação e de operação de gerenciamento. Estas regras são armazenadas na base BDA através do sistema SCA.

O ambiente do sistema SCA oferece ao administrador de segurança as políticas de acesso descritas no iterm 3.2.1: *Individual-based* (Inb); *Group-based* (Grb); *Role-based* (Rob); *Multi-level* (Mls); *e Modelo Militar* (Mms) (ver Figura 4.28, n.1). Após selecionar a política a ser empregada, a autoridade de segurança escolhe qual a função que se deseja executar sobre a base BDA (*incluir, excluir, alterar e consultar*) (ver Figura 4.28, n.2).

Uma vez escolhida a política a ser adotada e a função a ser executada, o próximo passo é definir o domínio a ser manipulado (ver Figura 4.28, n.3). Para isto, informa-se o domínio de gerenciamento ao qual as regras de autorização ficarão vinculadas. Para finalizar o processo de configuração do ambiente de definição de autorizações, a autoridade de segurança escolhe qual o tipo de acesso ele quer administrar: controle de acesso para associação (LPA) ou controle de acesso para oerações de gerenciamento (LCO e LOG) (ver Figura 4.28, n.4).

Depois da configuração do ambiente de autorização, a autoridade de segurança interage diretamente com o ambiente particular de cada política. Cada ambiente permite criar objetos para controle de acesso do domínio de gerenciamento ao qual estão vinculados. Para isto, deve-se informar os parâmetros básicos necessários para a definição de um objeto *target* nestas listas (ex: identificador de agente; identificador de nível de sensibilidade; informações de contexto para a lista LPA da política *Multi-level).*

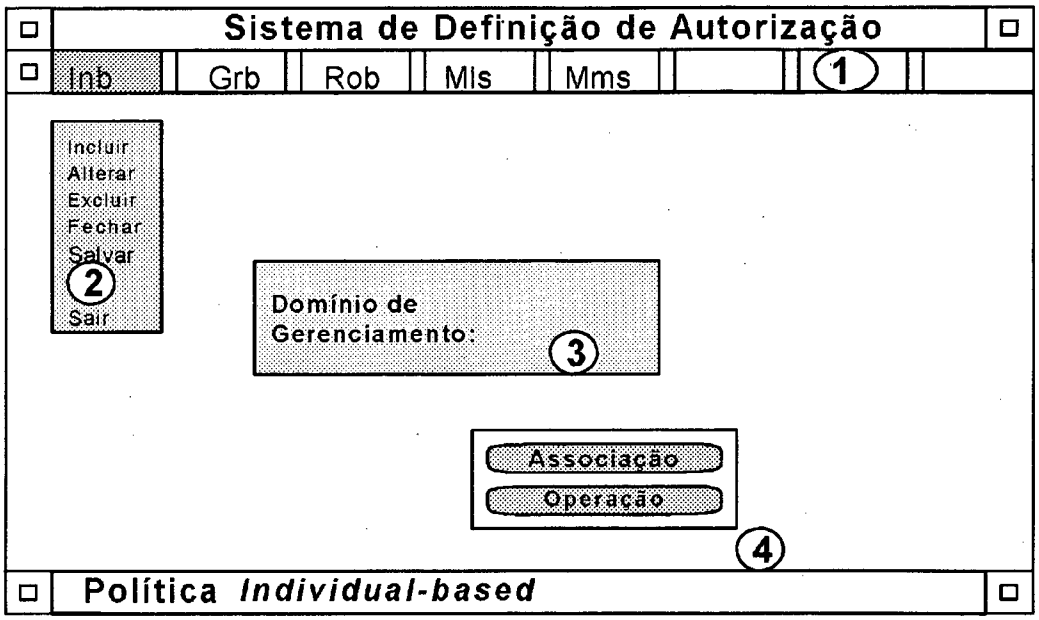


Figura 4.28 - Ambiente do Sistema SDA

Como exemplo de configuração de um ambiente no sistema SDA (Figura 4.29), supõe-se que a autoridade de segurança deseja usar o sistema SDA para definir uma política *Individual-based* (1); para executar a função de *incluir* (2) na lista *LPA* (4); para um suposto Agente de Falhas IAG = *Falhas_rede_ufsc* (3), pertencente ao domínio de gerenciamento *Falhas*. A Figura 4.29 ilustra este exemplo e a sequência de ações é identificada pelo números 1, 2, 3 e 4.

O ambiente do Sistema de Definição de Autorização da política *Individual-based* (Figura 4.30) para estabelecimento de associação requer a definição dos seguintes parâmetros básicos (ver Figura 4.5 e 4.6):

- identificador de agente (IAG): descritor de identificação de agente dentro de um domínio de gerenciamento;

- identificador de usuário (IdI): descritor de identificação de usuário que mantém atividades cooperantes de gerência com o domínio;

- informações de contexto (IC): condições que a associção deve cumprir para ser estabelecida, tais como: hora do dia, *host* de origem, canal de comunicação, etc.

Estes parâmetros permitem a autoridade incluir uma entrada na lista LPA da política Individual-based. Sendo assim, a Figura 4.30 ilustra a inclusão de uma associação nova

para o agente *Falhas_rede_ufsc* (1). O iniciador que está sendo autorizado a estabelecer associação com este agente é *User_paulo_ufsc* (2). O parâmetro informações de contexto (IC) é um parâmetro do tipo opcional e cabe à política de acesso definir quais as condições necessárias para estabelecimento da associação (3). A autoridade de segurança ao *confirmar* (4) os dados informados, cria uma entrada na lista LPA da política *Individual-based* (ver item 4.30), permitindo assim que o iniciador *User_paulo_ufsc* estabeleça associações com o agente *Falhas_rede_ufsc*.

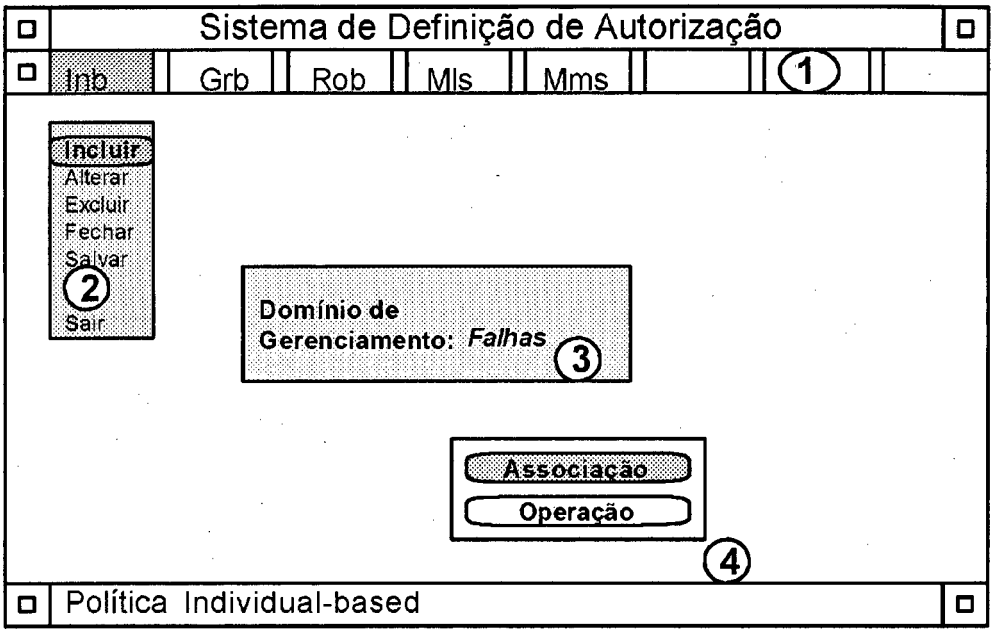


Figura 4.29 - Configuração de um Ambiente no Sistema SDA

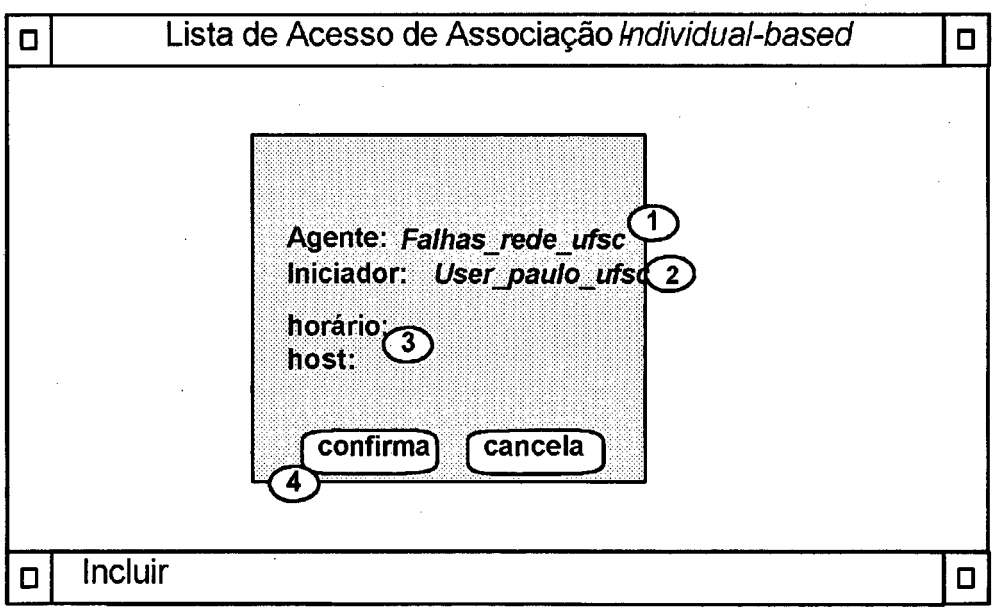


Figura 4.30 - Inclusão na Lista LPA para a Política Individual-based através do Sistema SDA

4.10 Fluxo de Comunicação

O fluxo de comunicação da Interface de Controle de Acesso ocorre em dois níveis:

- interno: interação dos componentes da Interface (Sistema de Definição de Autorização; Sistema de Controle de Acesso; e Base de Dados de Autorização);

- externo: interação do Sistema de Controle de Acesso com o sistema de gerenciamento.

A nível interno, a base BDA faz o elo de comunicação entre o sistema SDA e o sistema SCA.

O primeiro passo para funcionamento da Interface, ocorre a nível conceitual, onde a autoridade de segurança de um sistema de gerência define a política de segurança a ser adotada e, consequentemente, as regras de autorização do sistema.

A partir daí, a autoridade pode, através do sistema *on-line* SDA, alimentar e administrar a base BDA com as regras definidas. Estas regras são modeladas através das listas de regras que compõem a base BDA.

Uma vez que as regras estão modeladas e introduzidas na base BDA, o sistema SCA pode entrar em operação. Toda vez que um sistema de gerência for requisitado para estabelecer associação de gerência ou para realizar uma operação de gerenciamento, este invoca o sistema SCA para inferir sobre a base BDA e decidir se o pedido é valido ou não (Figura 4.31).

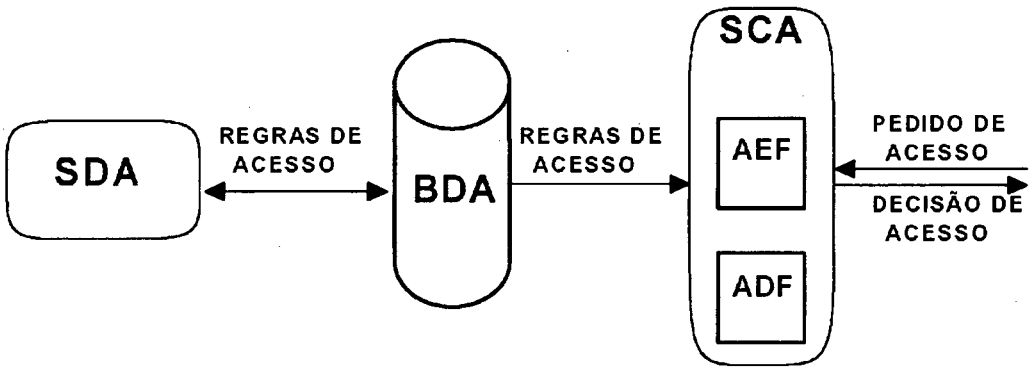


Figura 4.31 - Fluxo de Comunicação Interno da Interface de Controle de Acesso

A nível externo, a comunicação do sistema SCA interage com um processo de iniciação de associação e com o processo de aplicação agente de um sistema de gerência. Esta comunicação não é padronizada pela OSI.

Um iniciador de uma entidade de aplicação remota, através de um processo de aplicação remoto (PA remoto), ao tentar manter atividades cooperantes de gerência com um PA local, envia um pedido de estabelecimento de associação, através da primitiva *A-Associate-Request* do serviço ACSE (ver Figura 4.32).

O processo iniciador de associação local, ao receber um pedido, utiliza o serviço de autenticação para validar o iniciador da associação. Este serviço não faz parte do escopo deste trabalho. Se o serviço de autenticação validar a entidade par, o processo iniciador de associação local invoca o sistema SCA para verificar se o pedido oriundo do PA remoto está de acordo com as regras de autorização de associação, estabelecidas para o domínio de segurança deste processo de aplicação.

O sistema SCA é invocado por um pedido de acesso. Sua função AEF, ao receber este pedido, seleciona e repassa as informações necessárias à função ADF, para esta inferir sobre a base BDA. As informações necessárias são: informações de contexto; operação desejada (neste caso: associação); a identificação do processo de aplicação local requerido para associação de gerência; e os parâmetros de controle de acesso.

Os parâmetros de controle de acesso são definidos através do atributo *Initiator access control Information* (*Initiator ACI*) [ISO 10164-9]. Este atributo está contido entre os parâmetros de informação do iniciador (*CMIPUserInfo*) do serviço *A-Associate*.

Na Interface de Controle de Acesso, o atributo *Initiator ACI* é um conjunto formado pelos identificadores:

- identificador de iniciador (IdI);
- identificador de grupo do iniciador (IdG);
- identificador de nível de clearence (NC);
- identificador de domínio do iniciador (DOM).

O identificador IdI é requerido pela política *Identity-based.* As políticas *Group-based* e *Role-based* utilizam o identificador IdG como descritor de iniciador IdI. O

identificador NC é obrigatório para as políticas *Multi-level* e Modelo Militar que ainda requer o terceiro idenficador DOM.

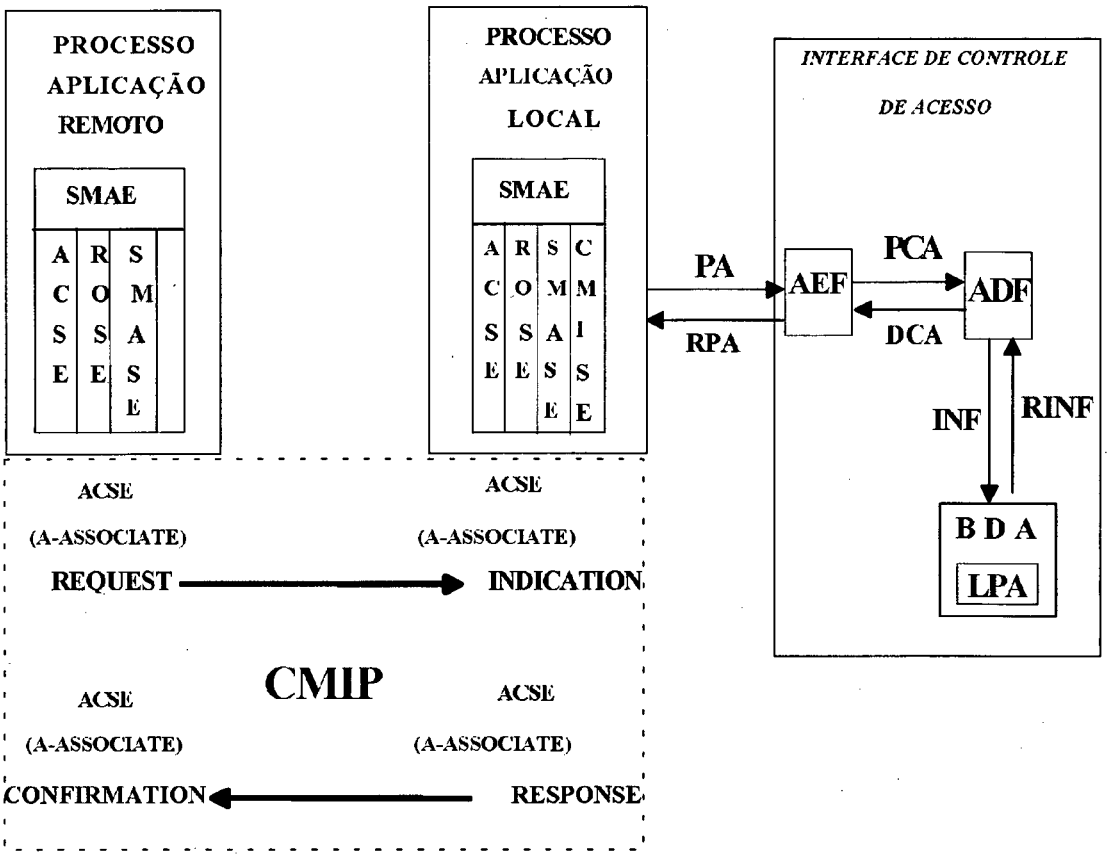
A autoridade de segurança, além de definir as regras para os objetos *target*, deve também especificar o atributo *Initiator ACI* e associá-lo a cada iniciador autorizado a estabelecer associação e a executar operações de gerenciamento em seu domínio.

Todos os identificadores que compõem o atributo *Initiator ACI* são necessários para a função ADF inferir sobre a base BDA, pois a Interface permite que a autoridade de segurança combine diferentes tipos de política para proteger seu domínio de gerenciamento. Caso nem todas as políticas sejam utilizadas, seus identificadores correspondentes assumem valor nulo.

A função ADF, ao ser solicitada, faz referência às informações na base BDA e compara os dados de controle de acesso recebidos da função AEF com as regras de autorização, definidas para o PA local, contidas na lista LPA do seu sistema de gerenciamento local.

Se o pedido de estabelecimento de associação for procedente, a função ADF envia um resposta positiva para a função AEF e retém os parâmetros de controle de acesso para uso futuro com as operações de gerenciamento. Caso a resposta seja negativa, a função ADF informa, também, os motivos da rejeição do pedido (ex: pedido fora do horário permitido; canal de comunicação inválido; dia da semana; etc).

O processo iniciador de associação, de posse da resposta do sistema SCA sobre o pedido de estabelecimento de associação, responde ao PA remoto através da primitiva *A-Associate-Response* do serviço ACSE, com o parâmetro *Result* informando se a associação foi aceita ou não.



AEF = Access Control Enforcement Function

ADF = Access Control Decision Function

BDA = Base de Dados de Autorização

SMAE = Entidade de Aplicação de Gerenciamento de Sistemas

ACSE = Elemento de Serviço de Controle de Associação

ROSE = Elemento de Serviço de Operação Remota

CMISE = Elemento de Serviço de Aplicação de Gerenciamento Comum

SMASE = Elemento de Serviço de Aplicação de Gerenciamento de Sistemas

PA = Pedido de Associação

RPA = Resposta do Pedido de Associação

PCA = Parâmetros de Controle de Acesso

DCA = Decisão de Controle de Acesso

INF = Inferências

RINF = Resultado das Inferências

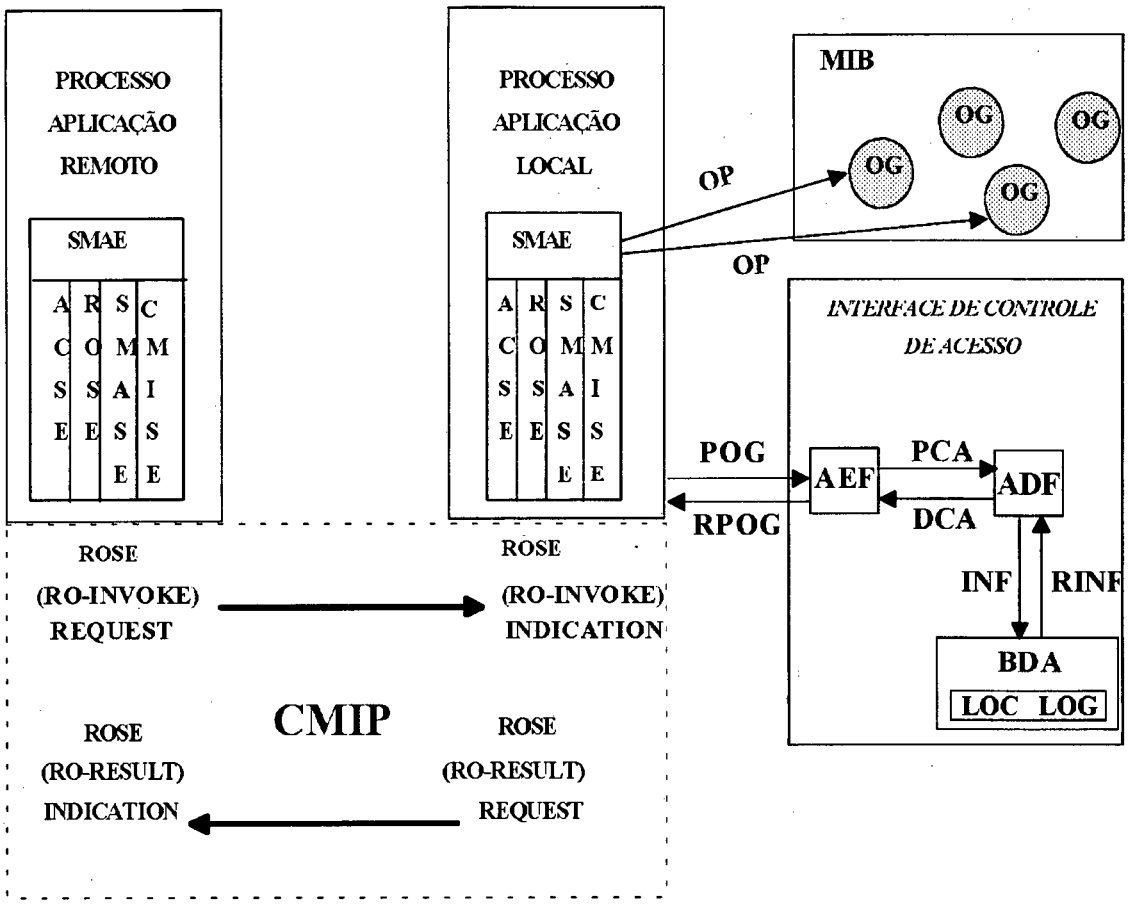
Figura 4.32 - Fluxo de Comunicação para Associação de Gerenciamento

Uma vez estabelecida a associação, o PA remoto pode começar a enviar as operações de gerenciamento para o PA local manipular os objetos gerenciados armazenados na MIB, através da primitiva *RO-Invoke-Request* do serviço ROSE (Figura 4.33).

O PA local, antes de executar qualquer operação de gerência, consulta o sistema SCA para verificar se a operação é válida ou não. A função AEF seleciona as informações de controle de acesso do pedido de operação de gerenciamento e repassa-os à função ADF.

A função ADF compara as novas informações e os parâmetros de controle de acesso, retidos anteriormente, com as regras contidas nas listas LCO do sistema de gerenciamento do qual os objetos *target*, requeridos para a operação de gerenciamento, fazem parte.

A função ADF repassa a resposta da inferência para a função AEF. Caso a resposta seja negativa, repassa também o motivo da recusa (ex: operação inválida; objeto gerenciado não disponível; fora do horário permitido; etc). Se a resposta do sistema SCA for positiva, o PA local executa a operação de gerenciamento. Caso contrário, o PA local retorna uma notificação ao PA remoto, através da primitiva *RO-Result-Request* do serviço ROSE, notificando que o acesso não foi permitido.



AEF = Access Control Enforcement Function

ADF= Access Control Decision Function

BDA = Base de Dados de Autorização

SMAE = Entidade de Aplicação de Gerenciamento de Sistemas

ACSE = Elemento de Serviço de Controle de Associação

ROSE = Elemento de Serviço de Operação Remota

CMISE = Elemento de Serviço de Aplicação de Gerenciamento Comum

SMASE = Elemento de Serviço de Aplicação de Gerenciamento de Sistemas

POG = Pedido de Operação de Gerência

RPA = Resposta do Ped. de Oper. de Gerência

PCA = Parâmetros de Controle de Acesso

DCA = Decisão de Controle de Acesso

INF = Inferências

RINF = Resultado das Inferências

OP = Operações de Gerência

OG = Objeto Gerênciado

MIB = Base de Informações de Gerência

Figura 4.33 - Fluxo de Comunicação de Operações de Gerenciamento

Em seguida, apresenta-se o comportamento de um processo de aplicação ao ser solicitado para estabelecer uma associação de gerência e, consequentemente, para executar operações de gerenciamento (Figura 4.34).

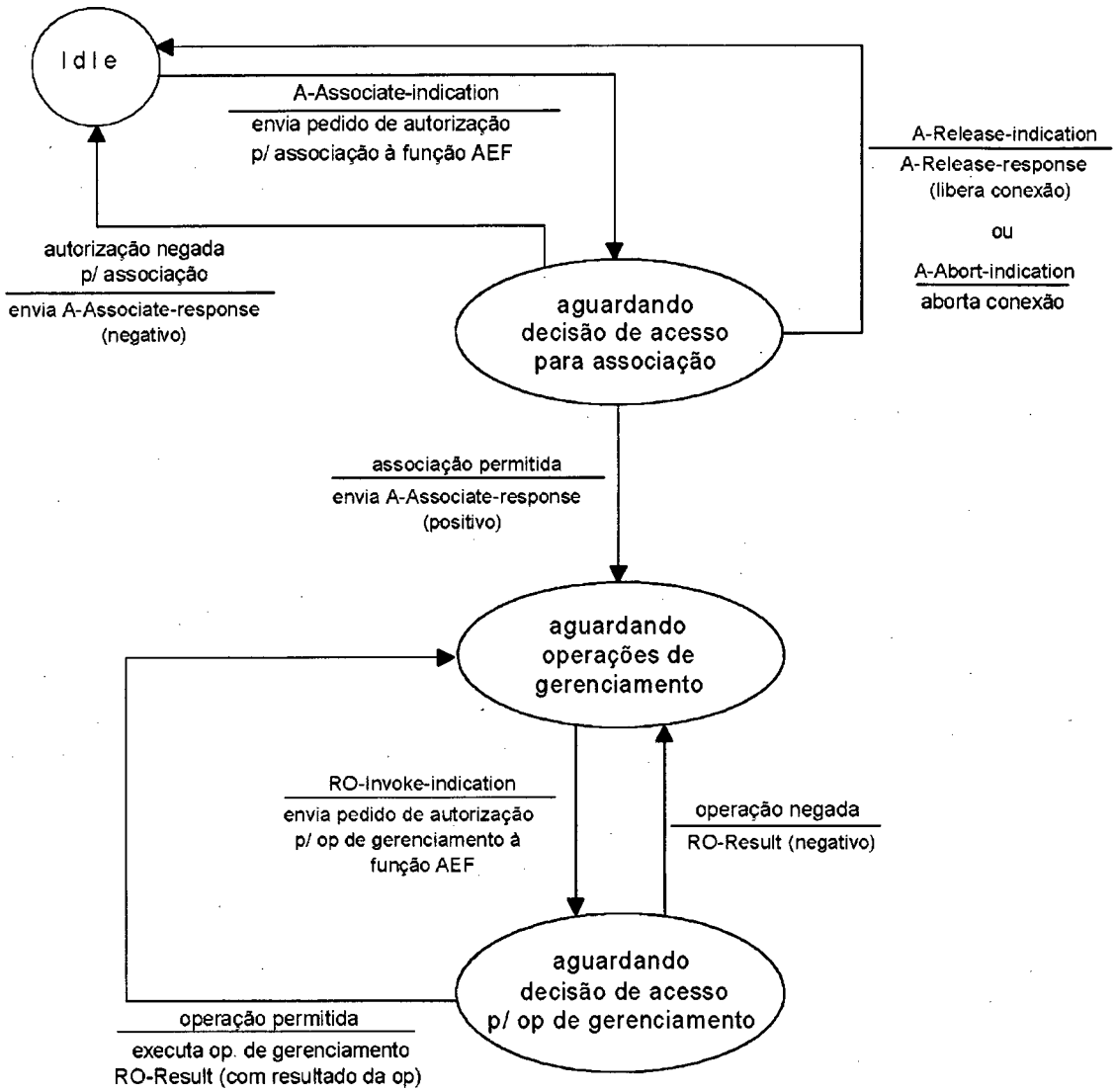


Figura 4.34 - Comportamento de um Processo de Aplicação ao Receber um Pedido de Acesso

Os diagramas das Figuras 4.35 e 4.36 ilustram o comportamento das funções AEF e ADF do sistema SCA ao ser invocado para validar um pedido de acesso.

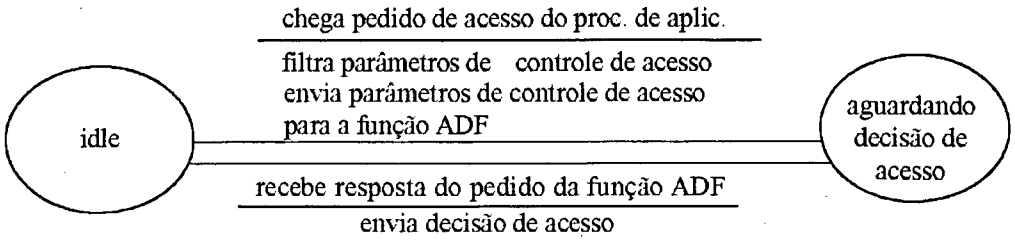


Figura 4.35 - Comportamento da Função AEF do Sistema SCA

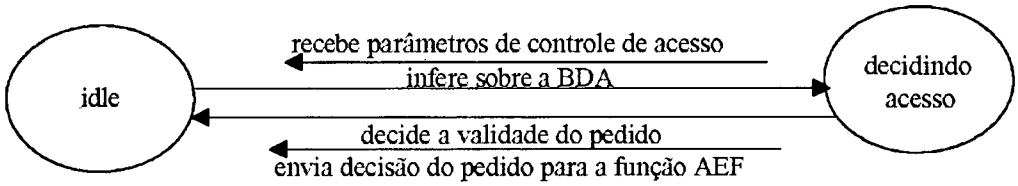


Figura 4.36 - Comportamento da Função ADF do Sistema SCA

A Interface de Controle de Acesso possui a funcionalidade do modelo da função de controle de acesso [ISO 10164-9] e pode ser implementada em platarformas de gerência de redes que possuam a funcionalidade OSI.

5. INTEGRAÇÃO DA INTERFACE À PLATAFORMA DE SUPORTE A GERÊNCIA DA REDE LOCAL UFSC

A Interface de Controle de Acesso faz parte do Projeto de Especificação e Implementação de uma plataforma de suporte ao gerenciamento com funcionalidade OSI [THI93] que está sendo desenvolvido pelo Grupo de Redes de Computadores da Universidade Federal de Santa Catarina (UFSC).

A plataforma de suporte ao gerenciamento é proposta para redes heterogêneas considerando, para tal, as normas da ISO através do Modelo de Referência OSI. Consiste de um suporte para o desenvolvimento de sistemas de gerência e não para implementação de um sistema de gerenciamento OSI especificamente.

A Interface de Controle de Acesso, por sua vez, consiste de ferramentas de suporte para implementação do serviço de controle de acesso para sistemas de gerência com funcionalidade OSI.

5.1 Plataforma de Suporte ao Gerenciamento

A implementação da plataforma de gerenciamento está, inicialmente, ocorrendo na Rede Local da Universidade Federal de Santa Catarina (UFSC) visando suprir as necessidades de gerenciamento da rede desta instituição conforme descrito em [THI93].

A Rede Local UFSC adota a arquitetura *Internet* com protocolos TCP/IP (*Transport Control Protocol/Internet Protocol*) sob um sistema operacional Unix. A plataforma de suporte ao gerenciamento utiliza mecanismos de *Sockets* para permitir a simulação dos serviços OSI: ACSE (*Association Control Service Element*) e ROSE (*Remote Operation Service Element*). A Figura 5.1 apresenta o modelo de gerenciamento adotado.

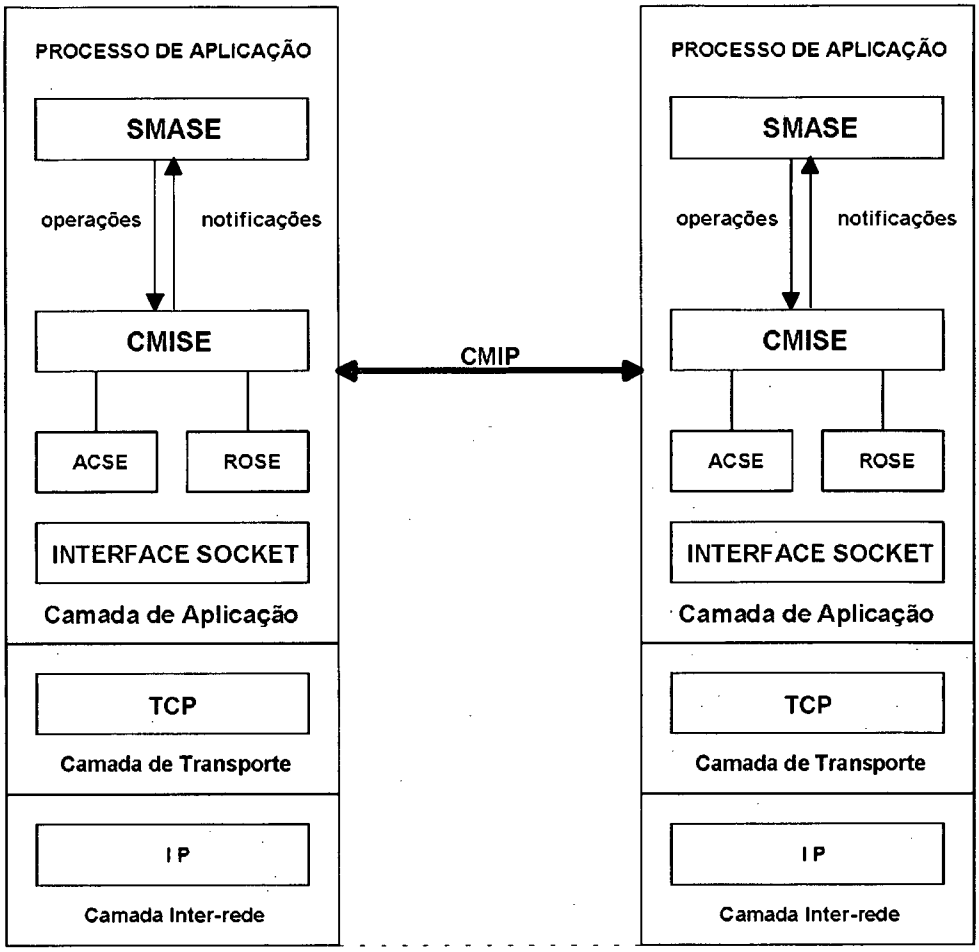


Figura 5.1 - Modelo da Plataforma de Gerenciamento

O CMISE (*Commom Management Information Service Element*) atua como intermediário entre o SMASE (*System Management Application Service Element*) (ver item 2.6) e o protocolo CMIP (*Commom Management Information Protocol*), através de serviços oferecidos para transporte das informações de gerência (operações e notificações) entre entidades de gerenciamento. Os usuários destes serviços CMISE são processos de aplicação de gerenciamento (Gerentes e Agentes).

Os serviços CMISE utilizam a Máquina de Protocolo de Informação de Gerenciamento Comum (CMIPM - *Commom Management Information Protocol Machine*) que é um mecanismo de suporte para troca de informações de gerenciamento. A máquina de protocolo tem como função aceitar primitivas do serviço CMISE e emitir PDU's (*Protocol Data Units*) no formato do protocolo de gerenciamento CMIP. A máquina de protocolo implementa os serviços definidos pelo CMISE (*get*, *set*, *action*, *delete*, *create*, *event*). Fisicamente, consiste em um processo continuamente em execução em cada *host* da rede.

Um processo de aplicação ao manter atividades cooperantes de gerência, executa funções de gerenciamento. O Modelo de Gerenciamento OSI refere-se ao conjunto destas funções como sendo o Elemento de Serviço de Aplicação de Gerenciamento de Sistemas (SMASE) (ver item 2.6).

Um processo de aplicação, ao executar funções de gerência, envia operações e notificações para um processo de aplicação destino. Estas operações e notificações são mapeadas através do serviço CMISE. O CMISE repassa a informação para o processo CMIPM que faz a verificação do destino e envia para o CMIPM remoto. Se o serviço for do tipo confirmado, o CMIPM remoto envia a confirmação ao CMIPM local (origem) que, por sua vez, retorna o resultado ao CMISE local, que se encarrega de encaminhar ao processo de aplicação que originou a comunicação.

O elemento de serviço SMASE é implementado em duas partes: "biblioteca SMASE" e "SMASE centralizador".

A biblioteca SMASE é vista pelo processo de aplicação de gerenciamento e contém apenas a definição dos serviços oferecidos pelas funções de gerenciamento.

O SMASE centralizador é um processo que atua como servidor de gerenciamento aos processos de aplicação, contém, além da biblioteca das funções de gerenciamento, a biblioteca CMISE. O SMASE centralizador é a interface entre os processos de aplicação de gerenciamento locais e remotos. A comunicação entre o SMASE centralizador e os processos de aplicação é feita através da interface *Socket*. A Figura 5.2 apresenta o relacionamento da biblioteca SMASE com o SMASE centralizador.

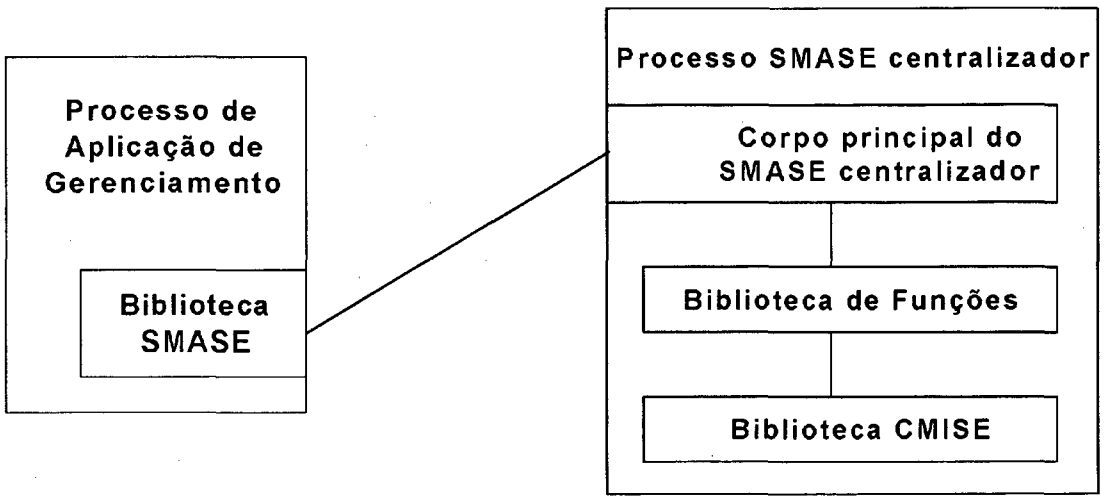


Figura 5.2 - Relacionamento da Biblioteca SMASE com o Processo SMASE Centralizador

Na plataforma de suporte ao gerenciamento, ver Figura 5.3, cada processo gerente ou agente possui uma biblioteca SMASE, enquanto que cada *host* possui apenas um único processo SMASE centralizador. O SMASE centralizador atua como um tratador de eventos que podem ser gerados pelos processos locais de aplicação ou pelo processo CMIPM. Quando o evento é gerado pelo CMIPM significa que o pedido foi feito por um processo de aplicação remoto. Após identificar o evento, o SMASE centralizador repassa-o ao processo de aplicação local destinatário (gerente ou agente). A biblioteca CMISE é utilizada somente pelo processo SMASE centralizador para acessar o protocolo de gerenciamento CMIP.

Algumas funções do processo SMASE centralizador são:

- manter tabela de correspondência entre agentes e classes de objetos gerenciados;
- atuar como discriminador de eventos;
- cadastrar endereços locais (internos ao *host*) para processos agentes;
- gerenciar comunicação entre processos de aplicação.

A Base de Informações de Gerenciamento (MIB) da plataforma de suporte inclui objetos gerenciados, atributos e as informações para configuração do sistema. As informações da MIB são armazenadas em dois tipos de processos:

- nos processos agentes que contém os objetos gerenciados, responsabilizando-se pela manipulação direta de seus atributos;
- nos processos SMASE centralizador que contém informações de gerenciamento para o controle dos processos de aplicação (agentes e gerentes) e para configuração da plataforma de suporte ao gerenciamento.

Entre as informações armazenadas no processo SMASE centralizador incluem-se:

- cadastro de agentes e gerentes;
- cadastro de agentes e classes de objetos;
- cadastro das classes de objetos;
- tabela de pendências;
- tabela de configuração.

A Figura 5.3 apresenta um visão geral da plataforma de gerenciamento empregada para a Rede Local UFSC.

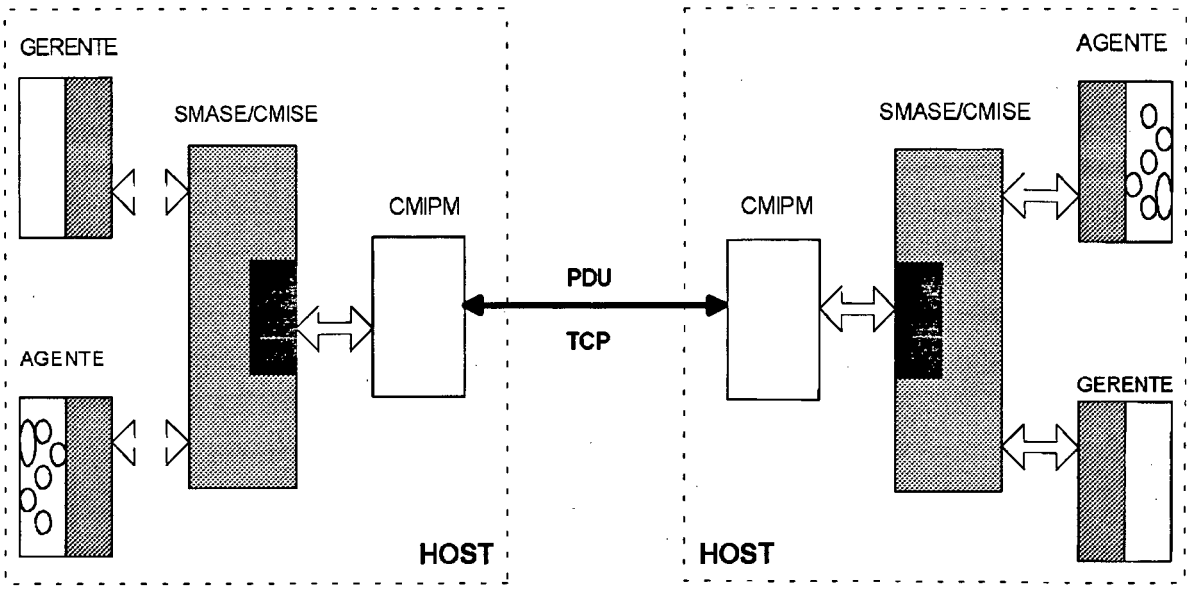


Figura 5.3 - Visão Geral da Plataforma de Gerenciamento

5.2 Localização da Interface na Plataforma

A integração da Interface de Controle de Acesso à plataforma de suporte ao gerenciamento visa garantir o controle de acesso à nivel de associação e a nível de operação de gerenciamento.

Na plataforma de suporte, o SMASE centralizador é um processo único em cada *host* da Rede Local UFSC e é a interface responsável por gerenciar a comunicação entre os processos de aplicação locais e remotos. Contém a tabela de correspondência entre agentes e gerentes, e a tabela de correspondência entre agentes e classes de objetos gerenciados.

A Interface de Controle de Acesso, também, é única por *host* e interage com o SMASE centralizador, através de seu Sistema de Controle de Autorização (SCA), para decidir se os pedidos de associação e de operação recebidos pelo *host* são válidos ou não. A Figura 5.4 apresenta a localização da Interface de Controle de Acesso dentro da plataforma.

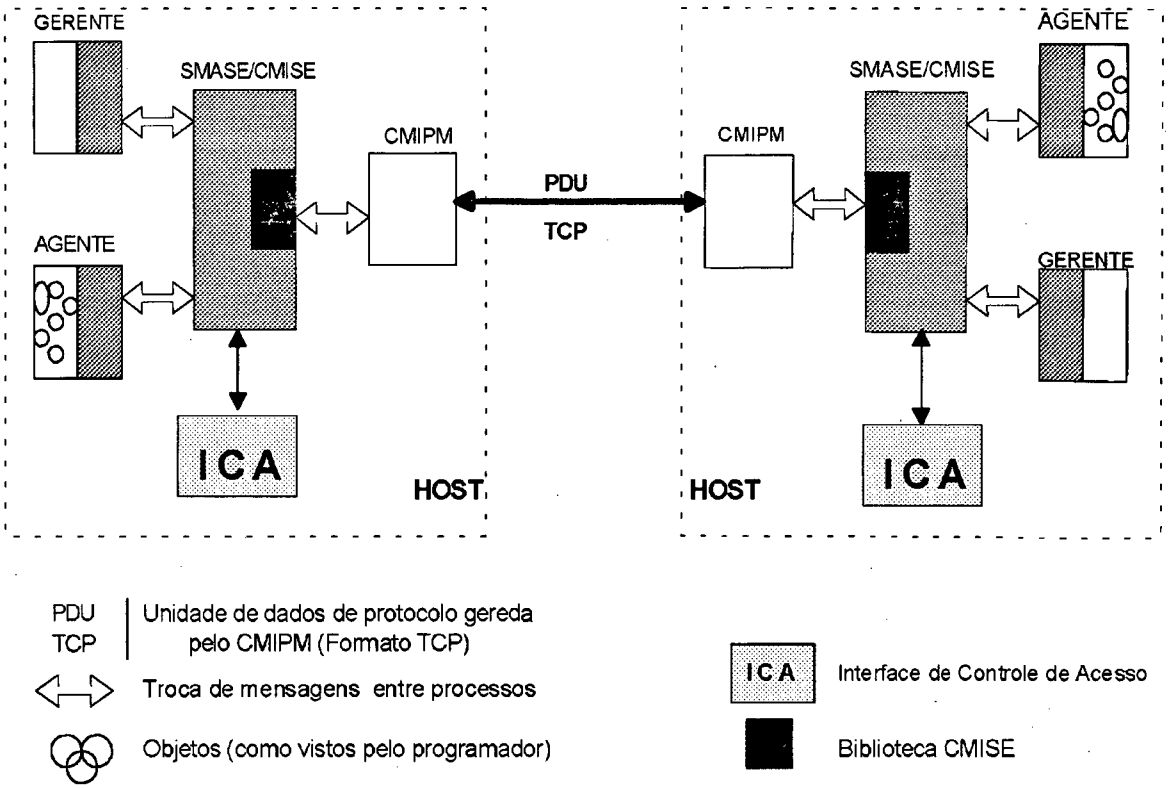


Figura 5.4 - Localização da Interface de Controle de Acesso na Plataforma de Gerenciamento

A interação da Interface de Controle de Acesso com o SMASE centralizador, e não com a biblioteca SMASE dos processo de aplicação que compõem um *host*, justifica-se pelo fato de que o SMASE centralizador é o responsável por gerenciar a comunicação entre os processos de aplicação e por conter as tabelas de correspondências, enquanto que a biblioteca SMASE funciona simplesmente como um conjunto de chamadas ao processo SMASE centralizador [THI93].

Além disso, a Interface de Controle de Acesso interagindo com o SMASE centralizador de cada *host* da rede local, evita que o SMASE centralizador tenha que estabelecer conexões desnecessárias com as bibliotecas SMASE dos processos de aplicação, caso o pedido não tenha autorização para ser efetuado, ou seja, não esteja de acordo com as regras autorização definidas na base BDA. A Figura 5.5 ilustra o *host* ***A*** que é a opção de integração adotada para a interface à plataforma. E apresenta o *host* ***B*** que é a opção descartada em virtude das justificativas apresentadas.

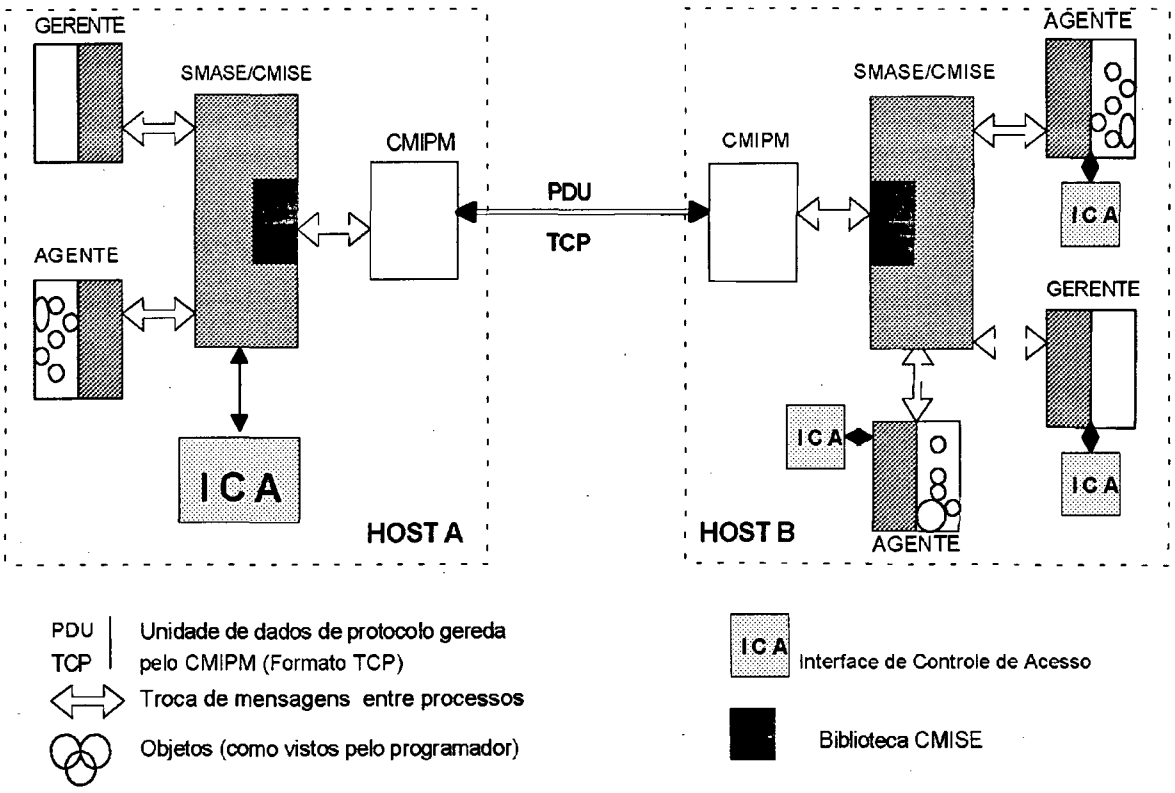


Figura 5.5 - Integração da Interface à Plataforma

Na plataforma de gerenciamento, um processo de aplicação ao tentar executar funções de gerenciamento, sobre um objeto gerenciado manipulado por um processo de aplicação de um *host* remoto, utiliza os elementos de serviço ACSE e ROSE simulados pela interface *Socket* [THI93].

Inicialmente, o processo de aplicação, gerente no caso, deve estabelecer associação com o processo de aplicação agente reponsável por executar o gerenciamento desejável. Esta etapa é requerida antes de usar os serviços de operação e notificação de gerenciamento. Para tanto, o serviço *A-Associate* do ACSE é invocado pelo usuário do serviço CMISE para estabelecimento de associação com seu par. A informação do usuário do CMISE torna-se disponível a CMIPM e inclui o atributo *Initiator access control Information* (*Initiator ACI*), codificado através do parâmetro *CMIPUserInfo* da primitiva *A-Associate* do serviço ACSE.

O processo SMASE centralizador, do *host* remoto, que é o processo responsável pela iniciação de associação, ao receber a primitiva *A-Associate-indication* repassa o pedido de

associação à função AEF do Sistema de Controle de Autorização (SCA) da Interface de Controle de Acesso. A função AEF filtra a operação do pedido de acesso, o identificador do processo de aplicação agente e o atributo *Initiator ACI* do iniciador da associação de gerenciamento e repassa-os à função ADF.

De posse das informações recebidas da função AEF, a função ADF infere sobre a lista LPA, armazenada na base BDA do SMASE centralizador remoto e decide se a associação é válida ou não de acordo com as inferências correspondentes à política implementada para proteger o processo de aplicação.

Quando a decisão tomada é uma permissão de acesso para a associação de gerenciamento, a função ADF prepara a informação de controle de acesso, chamada de *ACI retida*, que é conservada para uso com futuros pedidos de operação. A informação *ACI retida* é composta pelo identificador de associação IA e pelo *Initiator ACI* do iniciador.

Após decidir se o acesso é válido ou não, a função ADF envia a decisão à função AEF que se encarrega de devolver a resposta ao SMASE centralizador que originou a consulta de permissão de acesso.

Se o pedido de acesso for aceito pela Interface de Controle de Acesso, o parâmetro *CMIPUserInfo*, da primitiva *A-Associate* do serviço ACSE, torna-se disponível ao usuário do serviço CMISE do *host* remoto e a CMIPM remota fica aguardando pela resposta deste usuário.

Ao receber a primitiva *A-Associate-response*, indicando associação *aceita*, do usuário do serviço CMISE remoto, a CMIPM remota está pronta para aceitar as primitivas de serviço do CMISE remoto. Se a resposta for negativa, indicar associação *rejeitada*, a instância CMIPM deixa de existir. A associação *aceita* ou *rejeitada* é indicada através do parâmetro *Result* das primitivas *A-Associate-response* e *A-Associate-confirmation*.

A máquina de protocolo CMIPM do host iniciador, ao receber a primitiva *A-Associate-confirmation*, de acordo com o parâmetro *Result*, estabelece associação, se este indicar sucesso, ou, se indicar insucesso, não estabelece associação e a instância da CMIPM do SMASE centralizador iniciador deixa de existir.

Após o estabelecimento de associação, o SMASE centralizador remoto fica aguardando a chegada de operações de gerenciamento. Toda vez que o SMASE centralizador receber pedidos de operações de gerenciamento, invoca o Sistema de Controle de Acesso (SCA), repassando o pedido à função AEF.

A função AEF, ao receber os pedidos de operação de gerenciamento, filtra os dados de controle de acesso, envia-a à função ADF que compara-os com a *ACI retida* do iniciador e também com as regras da lista LCO armazenada na base BDA do *host* remoto.

Após inferir de acordo com as regras de inferência pertinentes a política de acesso do objeto, a função ADF envia a decisão de acesso para a função AEF que se encarrega de repassá-la ao SMASE centralizador.

6. CONSIDERAÇÕES FINAIS

Este trabalho concentra-se no estudo dos aspectos relacionados com a Gerência de Segurança OSI e, em especial, com a Função de Controle de Acesso [ISO 1064-9] que implementa o serviço de controle de acesso para as informações de gerência armazenadas na MIB. Para isto, a Interface de Controle de Acesso requer que uma política de acesso seja definida para os elementos de informação de gerenciamento que necessitam de proteção.

Dentro deste contexto, diferentes modelos de políticas de acesso foram estudadas e adaptadas considerando-se, particularmente, as características dos elementos de informação de gerenciamento, pois todas as bibliografias utilizadas descrevem modelos de políticas para elementos de informação genéricos.

Conforme o Modelo OSI, há necessidade de projetar-se mecanismos de controle de acesso que assegurem acesso aos recursos gerenciados somente para usuários autorizados. Mas cada sistema de gerenciamento é criado e definido de acordo com as necessidades básicas de gerenciamento da rede a que ele está associado. Portanto, definir uma ferramenta genérica para controle de acesso, que permita a combinação de diferentes políticas de acesso para suprir as necessidades específicas de cada sistema de gerenciamento, interferindo o mínimo possível na definição e no funcionamento do próprio sistema de gerenciamento, é algo extremamente complicado.

A Interface de Controle de Acesso apresentada pode ser integrada em sistemas de gerência com funcionalidade OSI, ou seja, que implementem os serviços ACSE e ROSE. Foi projetada para permitir que administradores de segurança possam, através dela, implementar políticas de acesso para os recursos de gerência de uma forma amigável e transparente. Porém sua utilização requer, primeiramente, que a autoridade de segurança identifique, em seu sistema de gerenciamento, quais são as reais ameaças e contra as quais é necessário e vantajoso adotar-se medidas de proteção.

Especificamente para sistemas de gerência, a autoridade deve identificar quem são os elementos de informação de gerenciamento que apresentam vulnerabilidades e quais destas vulnerabilidades são importantes em virtude das conseqüências de um possível ataque. A autoridade deve, também, estimar os custos de cada possível ataque, os custos das medidas de

segurança e selecionar o modelo de política de acesso, oferecido pela Interface, que sejam justificados por essa análise.

A estimativa do custo da utilização da Interface de Controle de Acesso, apesar de não ser o objetivo de estudo deste trabalho, está sendo considerada em um projeto complementar, desenvolvido como trabalho de conclusão de curso por alunos de graduação em Ciência da Computação da UFSC. Esse projeto consiste na construção de um protótipo da Interface que, inicialmente, será integrado à plataforma de gerenciamento da Rede Local UFSC. Deve-se ressaltar que as normas da ISO para gerenciamento não estabelecem qualquer característica de implementação, estando a responsabilidade dessa tarefa inteiramente a cargo dos projetistas de *software* e *hardware*.

A interpretação e tradução das especificações contidas nas normas da ISO constituem uma etapa difícil e complexa. A falta de estabilidade das normas (ainda em forma de *drafts*) é um outro fator que dificulta a sua utilização. Este trabalho não foi uma exceção, e sendo assim, procurou-se dar uma contribuição, através da solução das dificuldades encontradas, para pesquisas e trabalhos futuros dentro da área de Gerência de Segurança e em especial a Função de Controle de Acesso.

A Função de Controle de Acesso necessita, para ser implementada, que a autoridade de segurança especifique o parâmetro de controle de acesso que será transportado através dos protocolos de gerenciamento, que defina quem são os elementos de informação de gerenciamento que necessitam de proteção (objetos *target*) e quais as regras de proteção para estes elementos, e também defina os iniciadores autorizados a estabelecer associação e a executar operações de gerenciamento.

A Interface de Controle de Acesso já tem definido o parâmetro de controle de acesso para ser transportado através dos protocolos de gerência que, a saber, é o atributo *Initiator ACI*. Contém, também, o Sistema de Definição de Autorização (SDA) que permite definir os objetos *target* e suas regras de proteção. Falta especificar para a Interface um módulo para definição de iniciadores autorizados. Este módulo pode, perfeitamente, seguir a mesma filosofia da Interface, ou seja, utilizando-se o sistema SDA para a definição dos iniciadores autorizados e armazenando estas definições na Base de Definição de Autorização

(BDA). Os grupos de graduação que estão desenvolvendo estudos para viabilizar a construção do protótipo da Interface, também estão especificando este módulo.

Desta forma, a Interface de Controle de Acesso abre diversas possibilidades de continuação:

- a especificação do módulo para definição dos usuários autorizados;

- o desenvolvimento de um módulo para manutenção das listas armazenadas na base BDA. O sucesso dos mecanismos de controle de acesso dependem muito das listas estarem sempre organizadas;

- o desenvolvimento de um estudo de impacto da implementação da Interface em sistemas de gerência;

- a integração da Interface em outras plataformas de gerenciamento (OSIMIS);

- a especificação, implementação e integração das Funções de Alarme de Segurança e Auditoria de Segurança com a Interface de Controle de Acesso;

- a incorporação de um mecanismo de inferência para a função de decisão de acesso ADF indicar as ações a serem tomadas pelo sistema de gerência em função de uma rejeição de serviço.

O desenvolvimento deste trabalho mostrou, ainda, que o serviço de controle de acesso às informações de um sistema de gerenciamento pode ser realizado através da exploração do conceito de Alomorfismo, descrito no item 2.4.1. É recomendável o estudo da utilização deste recurso como alternativa de implementação do serviço de controle de acesso.

BIBLIOGRAFIA

[BRI93] BRISA, Gerenciamento de Redes: *Uma Abordagem de Sistemas Abertos*, Makron Books, São Paulo, 1993.

[COO89] COOPER, J. A., *Computer and Communications Security: Strategies for the 1990s*, McGraw-Hill, Singapore, 1989.

[COS93] COSTA, A., *Aspectos de uma Metodologia para Modelagem de uma Base de Informação de Gerenciamento para o Modelo OSI*, Dissertação de Mestrado - COPIN UFPB, Paraíba, Agosto, 1993.

[FOR94] FORD, W., *Computer Communications Security: Principles, Standards Protocols and Techniques*, Prentice-Hall, New Jersey, 1994.

[HAL90] HALSALL, F. e MODIRI, N., *An Implementation of an OSI Network Management System*, IEEE Network Magazine, Julho, 1990.

[HEL92] HELD, G., *Network Management: Techiniques, Tools and Systems*, John Wiley & Sons, England, 1992.

[IAB 1446] IAB - RFC 1446 - *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPV2)*, Abril, 1993.

[ISO 7498] ISO/IEC 7498 - Information Processing Systems - Open Systems Interconnection - *Basic Reference Model*, Outubro, 1984.

[ISO 7498-2] ISO 7498-2 - Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: *Security Architecture*, Fevereiro, 1989.

[ISO 7498-4] ISO/IEC 7498-4 - Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4: *Management Framework*, Novembro, 1989.

[ISO 9545] ISO/IEC DIS 9545 - Information Processing Systems - Open Systems Interconnection - *Aplication Layer Structure*, Setembro, 1988.

[ISO 9595] ISO/IEC 9595 - Information Technology - Open Systems Interconnection - *Commom Management Information Service Definition*, Abril, 1991.

[ISO 9596] ISO/IEC 9596 - Information Technology - Open Systems Interconnection - *Commom Management Information Protocol Specification*, Maio, 1990.

[ISO 10040] ISO/IEC DP 10040 - Information Processing Systems - Open Systems Interconnection - *System Management Information Overview*, Maio, 1989.

[ISO 10164-1] ISO/IEC DIS 10164-1 - Information Technology - Open Systems Interconnection - Systems Management - Part 1: *Object Management Function*, Março, 1991.

[ISO 10164-2] ISO/IEC DIS 10164-2 - Information Technology - Open Systems Interconnection - Systems Management - Part 2: *State Management Function*, Março, 1991.

[ISO 10164-3] ISO/IEC DIS 10164-3 - Information Technology - Open Systems Interconnection - Systems of Management - Part 3: *Attributes for Representing Relationships*, Março, 1991.

[ISO 10164-4] ISO/IEC DIS 10164-4 - Information Technology - Open Systems Interconnection - Systems of Management - Part 4: *Alarm Report Function*, Março, 1991.

[ISO 10164-5] ISO/IEC DIS 10164-5 - Information Technology - Open Systems Interconnection - Systems of Management - Part 5: *Event Report Management Function*, Março, 1991.

[ISO 10164-6] ISO/IEC DIS 10164-6 - Information Technology - Open Systems Interconnection - Systems of Management - Part 6: *Log Control Function*, Março, 1991.

[ISO 10164-7] ISO/IEC DIS 10164-7 - Information Technology - Open Systems Interconnection - Systems of Management - Part 7: *Security Alarm Reporting Function*, Março, 1991.

[ISO 10164-8] ISO/IEC CD 10164-8 - Information Technology - Open Systems Interconnection - Systems of Management - Part 8: *Security Audit Trail Function*, Novembro, 1990.

[ISO 10164-9] ISO/IEC CD 10164-9 - Information Technology - Open Systems Interconnection - Systems of Management - Part 9: *Objects and Attributes for Access Control*, Outubro, 1991.

[ISO 10164-10] ISO/IEC CD 10164-10 - Information Technology - Open Systems Interconnection - Systems Management - Part 10: *Accounting Meter Function*, Janeiro, 1991.

[ISO 10164-11] ISO/IEC DIS 10164-11 - Information Technology - Open Systems Interconnection - Systems Management - Part 11: *Workload Monitoring Function*, Outubro, 1990.

[ISO 10164-12] ISO/IEC DIS 10164-12 - Information Technology - Open Systems Interconnection - Systems Management - Part 12: *Test Management Function*, Julho, 1991.

[ISO 10164-13] ISO/IEC DIS 10164-13 - Information Technology - Open Systems Interconnection - Systems Management - Part 13: *Summarization Function*, Julho, 1991.

[ISO 10165-1] ISO/IEC DIS 10165-1 - Information Technology - Open Systems Interconnection - Structure of Management Information - Part 1: *Management Information Model*, Março, 1991.

[ISO 10165-2] ISO/IEC DIS 10165-2 - Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: *Definition of Management Information*, Março, 1991.

[ISO 10165-3] ISO/IEC DP 10165-3 - Information Technology - Open Systems Interconnection - Structure of Management Information - Part 3: *Definition of Management Attributes*, Março, 1989.

[ISO 10165-4] ISO/IEC DIS 10165-4 - Information Technology - Open Systems Interconnection - Structure of Management Information - Part 4: *Guidelines for the Definition of Managed Objects*, Março, 1991.

[KAR91] KARILLA, A. T., *Open Systems Security: An Architectural Framework*, Tese de Doutorado, Helsink, Finlândia, Junho, 1991.

[KLE88] KLERER, M., *The OSI Management Architecture an Overview*, IEEE Network, Vol.2, N.2, Março, 1988.

[KLE93] KLERER, M., *System Management Information Modeling*, IEEE Communications Magazine, Maio, 1988

[LEV88] LEVINE, R. I. et alli, *Inteligência Artificial e Sistemas Especialistas: Aplicações e Exemplos*, McGraw-Hill, São Paulo, 1988.

[LUC93] DE LUCCA, J. E., *Arquitetura para Segurança em Gerência de Redes*, Trabalho Individual - CPGCC UFSC, Santa Catarina, Dezembro, 1994.

[MCC88] MCCONNELL, J., *Internetworking Computer Systems: Interconnecting Networks and Systems*, Prentice-Hall, New Jersey, 1988.

[MCL90] MCLEAN, J., *The Specification and Modeling of Computer Security*, IEEE Computer, Vol.23, N.1, Janeiro, 1990.

[OSI93] OSIMIS, The OSI Management Information Service: User's Manual, Version 1.0 for system version 3.0, University College London, England, Janeiro, 1993.

[PAV93] PAVLOU, G. et alli, *The ISO Development Environment, A Generic Management Information Base Browser*, Versão 8.0, University College London, 1993.

[PFL89] PFLEEGER, C.P., *Security in Computing*, Prentice-Hall, New Jersey, 1989.

[RAM93] RAMAN. L., *CMISE Functions and Services*, IEEE Communications Magazine, Maio, 1993.

[RIC93] RICH, E. e KNIGHT, K., *Inteligência Artificial*, Makron Books, São Paulo, 1993.

[ROB91] ROBBINS, C. J. e KILLE, S. E., *ISODE - The ISO Development Environment: User's Manual: Quipu*, Vol.5, Versão 7.0, X-Tel Services Ltd e University College London, England, Julho, 1991.

[ROS90] ROSE, M. T., *The Open Book: A Pratical Perspective on OSI*, Prentice-Hall, New Jersey, 1990.

[ROS91] ROSE, M. T. et alli, *ISODE - The ISO Development Environment: User's Manual: Applications Services*, Vol.1, Versão 7.0, Performance Systems International, Inc.,England, Julho, 1991.

[SNM89] SUNNET MANAGER - *Tutorial: How to Write an Agent*, Versão 1.0, Sun Microsystems, Inc., USA, Outubro, 1989.

[SOU90] DE SOUSA, R. T. et alli, *Um projeto de Redes Auxiliado por Inteligência Articial - SGA*, Atas de Telemática, Porto Alegre, Setembro, 1990.

[SOU92] DE SOUSA, R. T., *Arquitetura de Segurança e Gerência de Segurança no Modelo OSI*, Anais do 2. Congresso 3. Demonstração de Interoperabilidade de Sistemas Abertos (OSI 92), São Paulo, 1992.

[TAN89] TANENBAUM, A. S., *Computer Networks*, Prentice-Hall, New Jersey, 1989.

[TAR86] TAROUCO, L. M . R., *Redes de Computadores: Locais e de Longa Distância*, McGraw-Hill, São Paulo, 1986.

[TER87] TERPLAN, K., *Communication Networks Management*, Prentice-Hall, New Jersey, 1987.

[THI93] THIRY, M., *Definição de uma Plataforma de Gerenciamento para a Rede Local UFSC*, Dissertação Mestrado - CPGCC UFSC, Santa Catarina, Dezembro, 1993.

[YEM93] YEMINI, Y., The OSI Network Management Model, IEEE Communications Magazine, Maio, 1993.

APÊNDICE A

A.1 Especificação da Interface

O protótipo de implementação da Interface de Controle de Acesso, inicialmente, está sendo integrado à plataforma de suporte ao gerenciamento da Rede Local UFSC. A metodologia utilizada para a especificação e implementação da Interface proposta está baseada em uma Abordagem Orientada a Objetos (AOO), a mesma empregada para a plataforma de suporte ao gerenciamento.

A plataforma de suporte possui uma hierarquia de herança (ver Figura A.1) que não é o mapeamento do Modelo de Informação OSI observado na Figura 2.5. Contém outras classes de objeto que foram criadas para dar suporte à plataforma, maiores detalhes podem ser encontrados em [THI93].

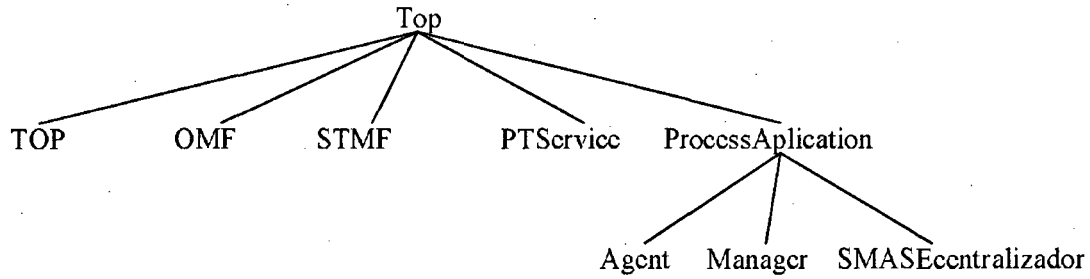


Figura A.1 - Hierarquia de Herança para a Plataforma de Gerenciamento

Dentro deste contexto, a Interface de Controle de Acesso foi modelada através da abordagem AOO e as classes ICA, BDA, SDA e SCA foram criadas para dar suporte à Interface. O relacionamento entre estas classes pode ser observado através da hierarquia de herança apresentada na Figura A.2.

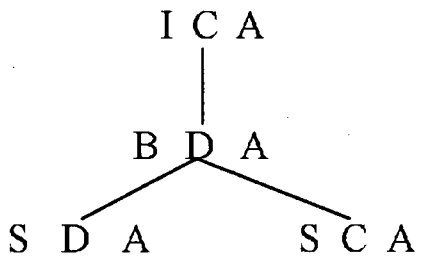


Figura A.2 - Hierarquia de Herança para a Interface de Controle de Acesso

A.2 Classe ICA

A classe ICA serve de base para a hierarquia de classes da Interface de Controle de Acesso, todas as demais classes são derivadas direta ou indiretamente da classe ICA. Ela possui um função especial *construtora*, chamada de *Ica* (funções *construtoras* possuem o mesmo nome da classe), reponsável pelo processo de inicialização requerida pela Interface. Toda vez que a Interface for ativada em um *host* da plataforma de gerenciamento, esta função será executada. Quando a Interface for desativada, sair de execução por algum motivo qualquer, uma função especial destrutora, chamada de *~Ica* será utilizada para finalizar o processo de operação da Interface.

Classe ICA	
Atributos	
Métodos	
Ica()	*{cria o objeto (instância)}*
~Ica()	*{elimina o objeto}*

A.3 Classe BDA

A classe BDA define as estruturas das listas organizadas na base BDA que formam os mecanismos de segurança: LPA; LCO; LOG; LCA; Rótulos. A estrutura das listas são definidas no arquivo *Listas.h* ilustrado na Figura A.3. A classe BDA possui métodos específicos para a manipulação e organização da base BDA. O sucesso de operação da Interface depende da periódica manutenção e organização da base BDA.

Classe BDA: derivada de ICA	
Atributos	
LPA LCO LOG LCA RotuloMls RotuloMms	*{definidos em Listas.h}*
Métodos	
Bda()	*{cria o objeto (instância)}*
~Bda()	*{elimina o objeto}*
Manutenção()	*{manutenção da listas}*

A.4 Classe SDA

A classe SDA herda os atributos da classe BDA e adiciona seus próprios métodos para manipulação das listas armazenadas na base BDA: Incluir(); Excluir(); Alterar(); e Consultar(); permitem o gerenciamento de objetos *target* na base BDA.

Classe SDA: derivada de BDA	
Atributos	
Métodos	
Sda()	*{cria um objeto (instância)}*
~Sda()	*{elimina um objeto}*
Incluir()	*{inclui um objeto target na base BDA}*
Excluir()	*{exclui um objeto target na base BDA}*
Alterar()	*{altera um objeto target na base BDA}*
Consultar()	*{consulta um objeto target na base BDA}*

```
// Listas.h

struct LPA {
        int Iag;
        void *p;  (apontador para o mecanismo de segurança: LCA ou rótulo)
};

struct LCO {
        int Ico;
        int Iat;
        void *p;  (apontador para o mecanismo de segurança: LCA ou rótulo)
        int *log; (apontador para a lista opcional LOG)
};

struct LOG {
        int Iog;
        void *p;  (apontador para o mecanismo de segurança: LCA ou rótulo)
};

struct LCA {
        int Idi;
        unsigned int op;
        struct Ic;
};

struct RotuloMls {        (rótulo para a política Multi-level)
       int Ns;
       struct Ic;
};

struct RotuloMms {        (rótulo para a política Modelo MIlitar)
        int Ns;
        int Dom;
        struct Ic;
};

struct Ic {
       (definida de acordo com as necessidades
       de cada sistema de gerenciamento)
};
```

Figura A.3 - Arquivo Listas.h

A.5 Classe SCA

A classe SCA contém os métodos que implementam as funções AEF e ADF da função de Controle de Acesso [ISO 10164-9] do Modelo de Gerenciamento OSI.

Classe SCA: derivada de BDA	
Atributos	
PedidodeAcesso	
ParâmentrosdeControledeAcesso	
DecisãodeAcesso	
Métodos	
Sca()	*{cria um objeto (instância)}*
~Sca()	*{elimina um objeto}*
Aef(PedidodeAcesso)	*{retorna os parâmetros de controle de acesso}*
Adf(ParâmetrosdeControledeAcesso	*{retorna a decisão do pedido de acesso}*

A.6 Hierarquia de Herança

A hierarquia de herança da Interface de Controle de Acesso, descrita nesta seção, corresponde à definição das classes de objetos requeridas para a construção do protótipo da Interface. A Figura A.4 apresenta a integração das hierarquias de herança da Interface (Figura A.2) e da plataforma de suporte ao gerenciamento (Figura A.1).

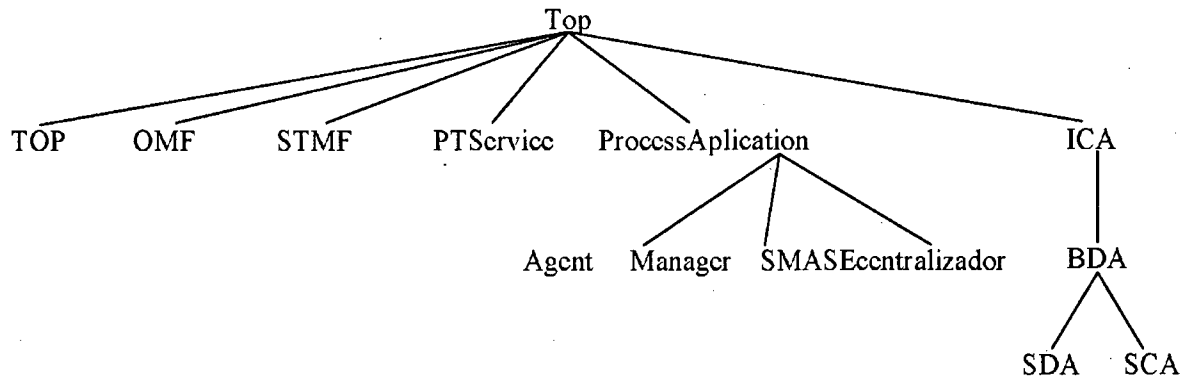


Figura A.4 - Integração das Hierarquias de Herança