Uma Proposta para Gerência de Correio Eletrônico

Ana Cristina Benso da Silva *
Liane M. Rockenbach Tarouco †

CPGCC, Instituto de Informática, UFRGS
Caixa Postal 15064
91501-970 Porto Alegre - RS

Sumário

Este artigo apresenta uma proposta para gerência de uma das aplicações mais difundidas no ambiente de redes de computadores, o correio eletrônico. Baseando-se nos modelos organizacional, funcional e informacional definidos pela ISO foi realizado um levantamento dos requisitos necessários à gerência do correio eletrônico, que resultou na definição de uma MIB (Management Information Base) específica para esta aplicação.

Abstract

This work propose a electronic mail management model. Based on organization, function and information models defined by ISO, the requirements needed to the electronic mail management were elicited. And based on this requirements a specific MIB Mail was defined.

*Bcs em Informática (PUCRS). Mestranda do Curso de Pós-Graduação em Ciência da Computação - UFRGS, e-mail: benso@inf.ufrgs.br

†Phd em Engenharia Elétrica (USP). Professora do CPGCC/UFRGS; e-mail: liane@penta.cesup.ufrgs.br

1 Introdução

Internet *mail* e MHS X.400 são sinônimos para uma das aplicações mais difundidas no mundo das redes de computadores, o correio eletrônico.

O MHS X.400 [CCITT 89] tenta satisfazer a maioria das exigências de um sistema de correio eletrônico completo: serviço de transporte confiável; mecanismos para armazenar as mensagens; segurança na transmissão das mensagens; interoperabilidade entre sistemas; utilização do serviço de diretórios; serviço de notificação de envio e recebimento de mensagens.

Em contraste o correio Internet, padrão de facto na comunidade das redes de computadores acadêmicas, possui uma arquitetura simples e antiga, tendo como principal objetivo estabelecer um meio de comunicação. O protocolo de transferência de mensagens do correio Internet não fornece aos usuários facilidades tais como a transmissão de mensagens multimídia, segurança e serviço de notificação de entrega de mensagens. Mas atualmente, já existem novos mecanismos que estão implementando a transferência de mensagens multimídia e requisitos de segurança sem que seja necessário alterar o protocolo de transferência, como exemplo o MIME [BOR 92]. O protocolo que implementa o correio eletrônico em redes TCP/IP [COM 91] é o SMTP [POS 82]. O padrão X.400 foi desenvolvido pelo CCITT e é o padrão internacional para correio eletrônico. Este padrão é baseado no modelo OSI da ISO, em particular no nível de aplicação (nível 7).

Independente de ser Internet ou X.400, o sistema de correio eletrônico é composto por uma série de mecanismos, mais complexos ou menos complexos, variando de padrão para padrão, transparentes ao usuário e dos quais dependem o bom desempenho e confiabilidade da aplicação.

Manter o bom desempenho e confiabilidade da aplicação é o objetivo deste trabalho que busca implementar tal tarefa através da gerência da aplicação.

A gerência de sistemas de correio eletrônico deve incluir a habilidade de controlar componentes do sistema, AU (Agente do Usuário), RM (Repositório de Mensagens), ATM (Agente de Transferência de Mensagens) e Gateways para outros sistemas de correio eletrônico, bem como os serviços por estes prestados. Os resultados da gerência devem auxiliar os usuários na avaliação do sistema e manutenção da qualidade do serviço através de resultados estatísticos, do reconhecimento de falhas de forma ágil, de histórico de eventos do sistema e de ferramentas inteligentes que baseadas nos históricos

são capazes de diagnosticar, analisar tendências e reagir a eventos do sistema.

Neste trabalho é apresentada uma proposta de um paradigma de gerência de um ATM (Agente de Transferência de Mensagens do Sistema de Mensagens X.400). A opção pelo X.400 deve-se ao fato deste ser o padrão internacional para correio eletrônico, e a tendência para os próximos anos em sistemas públicos é migrar do padrão TCP/IP para o padrão OSI.

As seções seguintes apresentam o contexto do MHS X.400, os requisitos para gerência do sistema de correio eletrônico, e a integração dos diversos elementos utilizados no desenvolvimento de um protótipo do paradigma elaborado.

2 MHS X.400 - Conceitos Básicos

A coleção de AUs (Agentes do Usuário), RMs (Repositório de Mensagens), UAs (Unidades de Acesso) e ATMs (Agentes de Transferência de Mensagens) é chamada MHS (Message Handling System). A figura 1 mostra simplificadamente o esquema funcional do modelo, tal como proposto em [CCITT 89].

Neste modelo um usuário é uma pessoa ou um processo. Usuários podem ser diretos (usam diretamente o MHS) ou indiretos (precisam de um sistema de comunicação intermediário para acessar o MHS). Um usuário é referido como sendo o originador ou receptor das mensagens. As recomendações da série X.400 definem um conjunto de tipos de mensagens e permissões que habilitam o originador a transferir mensagens para um ou mais receptores.

Um originador prepara uma mensagem com a ajuda de seu AU. O STM (Sistema de Transferência de Mensagens) transmite as mensagens submetidas a ele, para um ou mais AU receptores, UAs ou RMs e retorna a notificação de entrega aos originadores. O STM é formado por um conjunto de ATMs que operam juntos de maneira *store-and-forward* para transmitir as mensagens até seu destino.

2.1 Agente do Usuário - AU

O AU interage diretamente com o usuário, auxiliando a compor e submeter as mensagens para transmissão. O AU também assiste o usuário em

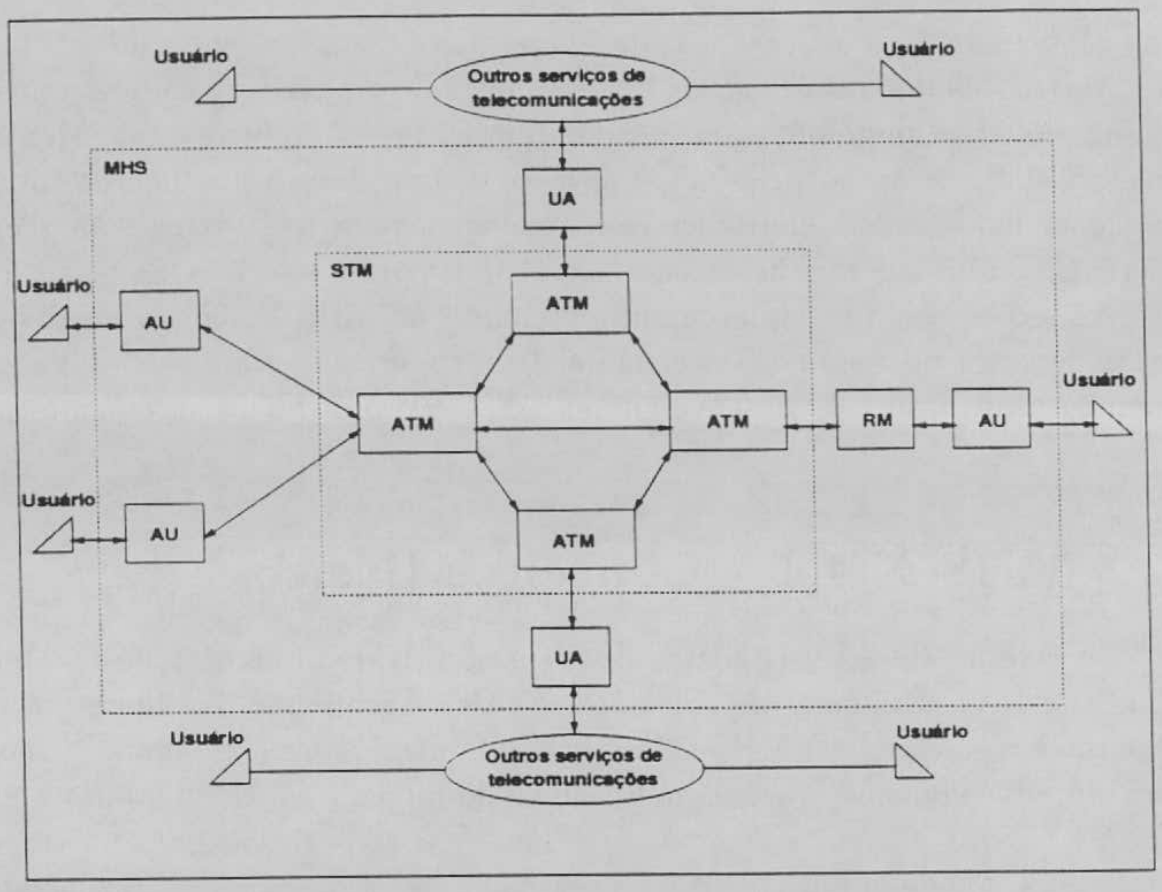

Figura 1: Modelo Funcional do MHS X.400

outras funções como armazenar, recuperar, responder e apagar mensagens. Este elemento submete mensagens ao ATM para transmissão através da rede, usando o protocolo de acesso ao STM (P3), que é usado entre um agente do usuário remoto e o STM para prover o acesso aos serviços do STM definidos na recomendação X.411 do CCITT [CCITT 89]. O AU também permite a recuperação de mensagens do RM usando o protocolo de acesso ao RM (P7), que é aplicado entre um agente do usuário remoto e um RM para prover o acesso aos serviços do RM especificados na recomendação X.413 do CCITT [CCITT 89].

2.2 Agente de Transferência de Mensagens - ATM

O ATM aceita as mensagens submetidas pelo AU ou RM e as entrega aos destinatários. Caso o destinatário seja conhecido pelo ATM a mensgen

é entregue. Caso contrário o ATM transfere a mensagens para outro ATM até que a mensagem chegue ao seu destino. As mensagens são transferidas usando o protocolo de transferência de mensagens do STM (P1), cujo propósito é prover as operações distribuídas do STM conforme especificado na recomendação X.411 do CCITT [CCITT 89].

2.3 Repositório de Mensagens - RM

Um RM é uma entidade funcional do MHS X.400 introduzida nas recomendações de 1988. Esta entidade tem como propósito primário armazenar e permitir a recuperação das mensagens do usuário. O RM também permite a submissão de mensagens diretamente ao STM.

2.4 Unidade de Acesso - UA

Uma UA usa os serviços de transferência de mensagens proporcionados pelo STM. Uma UA é uma entidade funcional associada com um ATM para prover intercomunicação entre o MHS e outros sistemas ou serviços, tais como fax ou correio tradicional.

3 Requisitos para Gerência do Correio Eletrônico

As tarefas básicas da gerência em redes, simplificadamente, são obter informações da rede, tratar estas informações, possibilitando um diagnóstico, e encaminhar as soluções dos problemas. Para cumprir estes objetivos, *funções de gerência* devem ser embutidas nos diversos componentes de uma rede, possibilitando descobrir, prever e reagir a problemas.

Para transferir as informações de gerência existem protocolos de gerência em redes de computadores. O modelo Internet utiliza o protocolo SNMP (Simple Network Management Protocol). O modelo OSI utiliza o protocolo CMIP (Common Management Information Protocol). Uma comparação entre as arquiteturas e seus protocolos é feita em [CAR 93]. Este trabalho adota o protocolo de gerência SNMP [ROS 91], porque, embora a aplicação gerenciada seja construída usando a arquitetura OSI, os sistemas de gerência,

bem como as aplicações de gerência atualmente usados nas redes acadêmicas são baseados neste protocolo, e assim o gerenciamento da aplicação de correio eletrônico ficará inserida no contexto geral. Todavia, a MIB projetada para permitir o gerenciamento da aplicação ATM poderá ser facilmente adaptada para permitir o gerenciamento num contexto OSI-CMIP, quando o mesmo se tornar um lugar comum.

Para resolver os problemas associados à gerência em redes, o OSI/NM propôs três modelos [WES 91];

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

Baseado nestes modelos pode-se definir os elementos necessários à gerência de um ATM X.400.

3.1 Modelo Organizacional

Os domínios de gerência para o correio eletrônico podem ser baseados na definição de domínio de autoridade e responsabilidade desta aplicação.

O padrão X.400 define domínios de gerência (DG - Domínio de Gerência) como uma coleção de uma ou mais ATMs, zero ou mais AUs e zero ou mais RMs operados por uma administração ou organização. Um DG gerenciado por uma administração é chamado um *Administration Management Domain (ADMD)*. Uma organização que não seja uma administração pode ter um ou mais ATMs, zero ou mais AUs e zero ou mais RMs formando um *Private Management Domain (PRMD)*, o qual pode interagir com um ADMD, como mostra a figura 2.

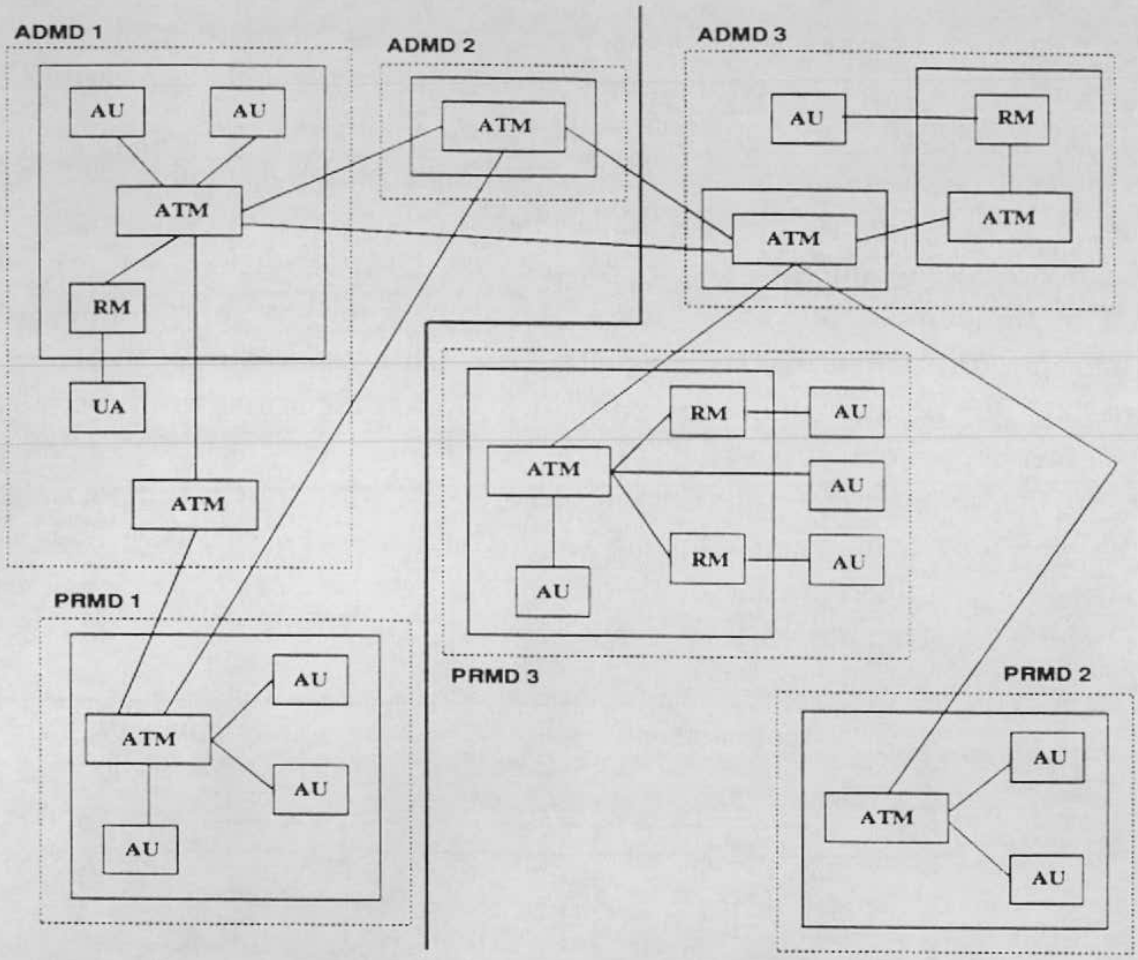

Figura 2: Domínios de Gerência

Como pode-se deprender na figura 2, a gerência do sistema de correio eletrônico, depende da interoperabilidade entre domínios de gerência e da habilidade de trocar informações entre elementos de um mesmo domínio e entre elementos de diferentes domínios. Essa troca de informações é fundamental quer pela necessidade de reunir dados recolhidos em diversas localidades para comparação e análise conjunta, quer pela inadequação para apresentação de dados dos equipamentos que os coletam. Conceitualmente no modelo OSI essas relações são: relações intradomínio e relação interdomínio [CAR 93]. A relação intradomínios neste caso é exemplificada pela comunicação entre entidades SNMP que pertencem ao mesmo domínio de gerência. A relação interdomínios seria a relação entre entidades SNMP que não pertencem ao mesmo domínio de gerência, e a comunicação seria estabelecida entre geren-

tes (comunicação *manager-to-manager*). Os gerentes envolvidos na comunicação atuam ora como gerentes, ora como agentes. O gerente que recebe a requisição passa agir como um agente em relação ao outro gerente, originador da requisição, e como gerente em realção aos agentes subordinados. Devido à complexidade inerente, neste trabalho, não é utilizada tal arquitetura.

Como o gerenciamento efetivo da rede da UFRGS utiliza o contexto SNMP e também o software SunNet Manager, a relação interdomínios é estabelecida diretamente entre o agente e o gerente de domínios diferentes, figura 3. Cabe observar que o gerente SunNet Manager utiliza um protocolo proprietário, transportado por RPC (Remote Procedure Call) [SUN 89a], e portanto não comunica-se com o protocolo SNMP diretamente, precisando de um *proxy* para interagir com o SNMP. Como mostra a figura 3 as requisições RPC do gerente são enviadas a um processo, local, *proxy* e este as envia como requisição SNMP ao agente local ou remoto.

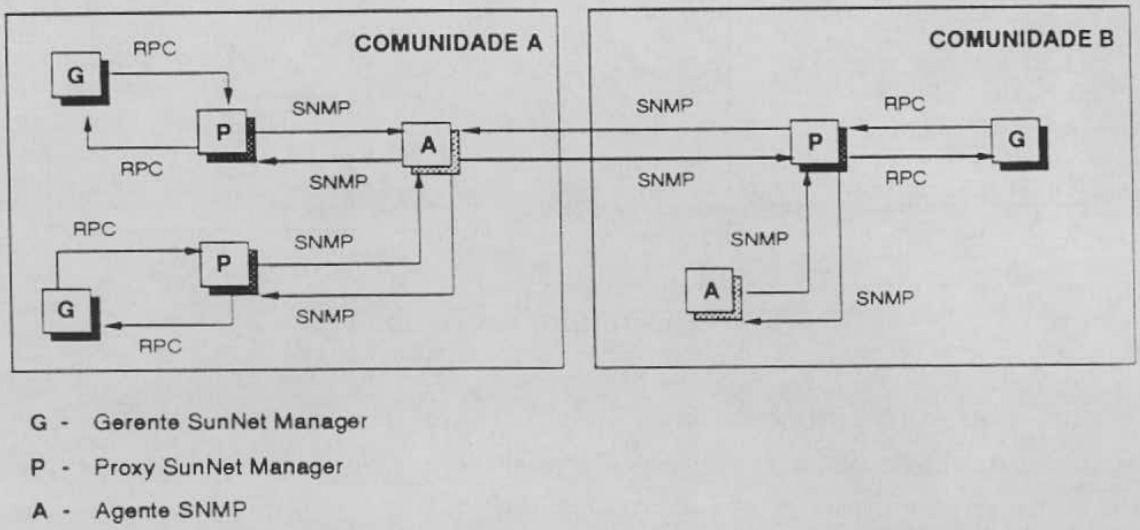

Figura 3: Comunicação entre entidades de gerência

Essas relações exigem segurança para os dados de gerência. Neste sentido o protocolo SNMP define dois mecanismos: comunidade e direitos de acesso [ROS 91]. Através do conceito de comunidade o SNMP v1 implementa uma forma trivial de autenticação, isto é, uma entidade SNMP para acessar informações de outra entidade deve identificar-se como membro da comunidade.

O segundo mecanismo, direitos de acesso, descreve as operações que po-

dem ser efetuadas nos objetos gerenciados. Os objetos da MIB tem o atributo "ACCESS:", que descreve os direitos de acesso ao objeto. Este atributo pode assumir os valores: *read-write*, *read-only*, *wirte-only* e *not_accessible*. Este conceito aplica-se também a entidades SNMP, como forma de proteger os dados da MIB. Uma entidade SNMP que deseja acessar dados de outra entidade SNMP, pertencente ou não a mesma comunidade, deve ser primeiro autenticada, e conforme a comunidade a que pertence são estabelecidos os direitos de acesso, desta entidade, aos objetos gerenciados e quais são os objetos acessíveis.

O SNMP v1 do ISODE [ROS 90], usado na implementação do protótipo em desenvolvimento na UFRGS, provê um arquivo de configuração, o *snmpd.rc*, onde são definidas diretivas que estabelecem as comunidades, os direitos de acesso e os objetos que são visíveis para determinada comunidade. O *snmp.rc* também permite configurar qual gerente deve receber os *traps* gerados pelo agente. As diretivas são:

- **community name address access view**
  Define uma comunidade SNMP chamada **name** com o nível de acesso indicado em **access**. O token **address** pode ser um *hostname*, um endereço IP, ou um endereço de rede. Se o valor deste token for diferente de 0.0.0.0, as requisições a esta comunidade devem ser oriundas do endereço especificado. O token **access** pode assumir os valores: *read-write* ou *read-only*. Caso este token não tenha um valor associado, o valor *default* é *read-only*. O token **view** é um identificador de objeto, que identifica a visão da MIB a qual esta comunidade tem acesso. Se este token não possui um valor associado, o *default* é a visão conter todos os objetos conhecidos pelo agente.

- **view name subtree**
  Define uma coleção de objetos gerenciados com um dado identificador de objeto como **nome**. O token **subtree** define as subárvores (grupos SNMP) que compõem a visão. Se nenhuma subárvore for especificada, a visão é composta por todas variáveis conhecidas pelo agente.

- **trap name address view**
  Define um **trap** para a comunidade SNMP chamada **name**, o qual é

enviado ao endereço especificado em **address**. Por *default* o parâmetro **view** não é utilizado.

3.2 Modelo Funcional

As classes funcionais definidas pelo modelo funcional são: gerência de falhas, gerência de configuração, gerência de contabilidade, gerência de desempenho e gerência de segurança.

Gerenciar um sistema de correio eletrônico é gerenciar os elementos que compõem este sistema, ou seja, gerenciar AUs, RMs, ATMs e UAs. Um ponto importante é a monitoração das mensagens fim-a-fim para verificar se as mensagens submetidas ao MHS estão sendo entregues aos destinatários corretos com alto grau de certeza, integridade e segurança.

A seguir estão especificados os requisitos para gerência de ATMs, segundo as áreas funcionais. Estes requisitos são baseados no estudo do padrão X.400 e nos levantamentos feitos em [McC 93].

3.2.1 Gerência de Falhas

Caracteriza-se por gerência de falhas o conjunto de funções que habilitam um gerente ou aplicação detectar, isolar e corrigir falhas de componentes e/ou serviços. Os requisitos identificados que dizem respeito à área gerência de falhas são:

- detectar, isolar e corrigir falhas em ATMs;
- emitir notificações sobre falhas aos responsáveis;
- interação entre entidades de gerência para detecção e correção de falhas, bem como para possíveis alterações de configuração decorrentes de falhas;
- manter *trace* das mensagens fim-a-fim;
- emitir notificações sobre congestionamento no sistema de correio eletrônico;

- criar arquivos de *log* de falhas para auxiliar em diagnósticos futuros, análises de comportamento e na correção automática e inteligente de falhas através da análise de soluções, anteriormente aplicadas. Um registro em um *log* deve conter os seguinte itens básicos:
  - data da ocorrência da falha;
  - identificação do ATM;
  - descrição do problema;
  - solução adotada;
  - *status* dos demais elementos do sistema;
  - responsável pela correção da falha.

3.2.2 Gerência de Configuração

Caracteriza-se por gerência de configuração o conjunto de atividades usadas para controlar a configuração do sistema. Gerência de configuração também inclui *engineering support*, que é o processo usado para determinar o sistema ótimo, baseado nos dados de desempenho, utilização dos recursos e requisitos do sistema. Os requisitos identificados que dizem respeito à área de gerência de configuração são:

- suportar serviço de diretórios;
- capacidade de alterar a configuração do sistema automaticamente;
- prover uma base de dados de configuração para suportar operações de administração, análise e planejamento;
- capacidade de localizar componentes e recursos de software;
- suportar informações de roteamento sobre ATMs e suas interfaces;
- capacidade de alterar a configuração de roteamento, conforme análise do tráfego e filas do ATM.

3.2.3 Gerência de Contabilidade

Caracteriza-se por gerência de contabilidade o conjunto de funções usadas para medir o uso do serviço e prover informações de cobrança sobre os serviços utilizados. Os requisitos identificados que dizem respeito à área de gerência de contabilidade são:

- medir o uso do correio eletrônico, pelo volume de mensagens transmitidas e recebidas;
- coletar dados de contabilidade;
- capacidade de analisar o custo operacional de componentes e sumarizar o custo de múltiplos recursos;
- capacidade de gerar informações de cobrança para agências de cobrança;
- registrar informações de contabilidade relacionado ao uso dos recursos em arquivos de *log*.

3.2.4 Gerência de Desempenho

Caracteriza-se por gerência de desempenho o conjunto de funções que avaliam, relatam e otimizam o comportamento operacional do sistema e serviços do usuário. Os requisitos identificados que dizem respeito à área de gerência de desempenho são:

- monitorar e diagnosticar condições de tráfego de correio eletrônico insatisfatórias;
- capacidade de coletar dados para análise de desempenho em ATMs. Em especial controlar as filas do ATM;
- capacidade de gerar análises estatítiscas de desempenho a curto, médio e longo prazo;
- capacidade de gerar notificações sobre problemas de desempenho aos responsáveis.

- histórico de problemas de desempenho, que contém no mínimo os seguintes dados:
  - data do problema;
  - causa suspeita;
  - ação corretiva;
  - *status* atual dos componentes do sistema;
  - responsável pela correção.

3.2.5 Gerência de Segurança

Caracteriza-se por gerência de segurança o conjunto de funções usadas para manter a autenticação dos componentes do sistema, contabilidade, confidencialidade, integridade e controle de acesso. Os requisitos identificados que dizem respeito à área de gerência de segurança são:

- autenticação e controle de acesso às informações de gerência;
- proteção das mensagens do usuário contra acessos não autorizados;
- manter a integrigadade das mensagens que transitam no STM.

3.3 Modelo Informacional

O Modelo Informacional define os objetos de gerência, as relações e as operações sobre estes objetos. Uma MIB (Management Base Information) é necessária para armazenar os objetos gerenciados.

Estes objetos são informações relevantes à gerência e que devem satisfazer os requisitos estabelecidos no Modelo Funcional. Há vários grupos trabalhando na intenção de elaborar uma MIB específica para correio eletrônico. Alguns documentos sobre MIB para X.400 já estão disponíveis, mas ainda em caráter informal. Recentemente foi publicada a RFC1566 [KIL 94] que define uma MIB para o correio eletrônico Internet.

Este trabalho não utiliza a RFC1566, pois propõe-se a definir objetos para a monitoração do ATM do MHS X.400. O IETF (*Internet Engenering Task Force*) e o ISO ITU *Study Group* 7 estão somando seus esforços para chegarem a uma definição conjunta da MIB para o MHS X.400.

Os objetos aqui apresentados formam um conjunto conciso de informações que permitem monitorar ATMs X.400, e foram identificados pelo estudo do padrão X.400. Os objetos são:

1. Informações referentes a configuração e identificação do ATM

   - ATMname - nome do ATM (nome da máquina);
   - ATMaddr - endereço do ATM (endereço IP da máquina);
   - ATMdomain - domínio do ATM;
   - Appname - nome da aplicação;
   - Protname - nome do protocolo;
   - Protversion - versão do protocolo;
   - ATMmode - modo de operação do ATM (1984, 1988);
   - ATMstatus - estado do ATM no momento.

2. Informações referentes a ATMs adjacentes que servem para agilizar a detecção de falhas e fornecer informações necessárias ao roteamento das mensagens. Estas informações compõe uma tabela, na qual cada entrada é composta pelo conjunto de objetos especificados no item 1

   - ATMadjTable - tabela de ATMs adjacentes;

3. Informações para o controle do fluxo de mensagens no ATM:

   - ATMqueueIn - tamanho da fila de mensagens submetidas;
   - ATMqueueOut - tamanho da fila de mensagens a serem transferidas;

4. Informações para controle de falhas ocorridas no ATM

   - ATMdateStart - data de inicialização do ATM;
   - ATMlastFault - data da última falha;
   - ATMfaultTotal - total de falhas do ATM.

5. Informações sobre o volume de mensagens que trafegam pelo ATM, possibilitando a avaliação e contabilização do uso dos recursos

   - SubmitedMsgTotal - total de mensagens submetidas ao ATM;
   - TransferedMsgTotal - total de mensagens transferidas a outros ATMs;
   - StoredMsgTotal - total de mensagens armazenadas pelo ATM;
   - RejectedMsgTotal - total de mensagens rejeitadas pelo ATM;
   - SubmitedMsgVolume - volume de mensagens submetidas ao ATM;
   - TransferedMsgVolume - volume de mensagens transferidas a outros ATMs;
   - StoredMsgVolume - volume de mensagens armazenadas pelo ATM.

6. Informações para avaliação de desempenho e monitoração das mensagens através do sistema de correio eletrônico

   - MsgId - identificação da mensagem;
   - ATMtimeIn - data da chegada no ATM;
   - ATMtimeOut - data em que foi transferida ou destinada ao usuário;
   - ElementFromType - tipo de elemento (UA, RM, ATM) que submeteu a mensagem;
   - ElementToType - tipo de elemento (UA, RM, ATM) que receberá a mensagem;
   - ATMFromAdd - endereço do ATM que submeteu a mensagem;
   - ATMToAdd - endereço do ATM que receberá a mensagem;
   - MsgSize - tamanho da mensagem;
   - UserFromAdd - endereço do usuário originador da mensagem;
   - UserToAdd - endereço do destinatário.

7. Informações sobre as funções de conversão de tipos de mensagens executadas pelo ATM

   - ATMconversionTable - tabela com tipos de conversão efetuadas (de: formato X para: formato Y);

8. Informações que permitem controlar as operações de associação entre entidades do sistema de correio eletrônico

   - InAssocTotal - total de associações requisitadas ao ATM:
   - OutAssoctotal - total de associações requisitadas pelo ATM:
   - LastInAssoctime - data da última associação requisitada ao ATM e estabelecida;
   - LastOutAssoctime - data da última associação requisitada pelo ATM e estabelecida;
   - RejectInAssoctotal - total de associações requisitadas ao ATM e rejeitadas;
   - RejectOutAssoctotal - total de associações requisitadas pelo ATM e rejeitadas;
   - AbortedAssoc - total de associações abortadas;

9. Informações individuais de cada asocciação estabelecida ou não

   - Associd - identificação da associação;
   - Initiatoradd - identificação da entidade requisitante da associação;
   - Acceptoraddr - identificação da entidade par que recebe a solicitação;
   - AssocTime - tempo de duração da associação.
   - TrasferedMsgVolume - volume de mensagens de correio eletrônico transferidas na associação;
   - Assocstatus - estado da associação;
   - AssocReason - razão da rejeição ou fim da associação;

Além dos objetos da MIB, são utilizados outros meios de manter informações para enriquecer o potencial da gerência. Um destes meios é a criação de arquivos de *log*. Estes arquivos mantém um histórico de eventos do sistema e possibilitam análises do comportamento do sistema, diagnósticos de possíveis falhas e análise de tendências de comportamento.

3.4 Descrição do Protótipo

Para validar o paradigma de gerência proposto, está sendo implementado um protótipo. O trabalho está sendo desenvolvido em ambiente TCP/IP, utilindo as implementações disponíveis para a área acadêmica: o ambiente ISODE versão 8.0, o agente SNMP v1 do ISODE e o PP versão 6.0, o qual implementa um ATM que suporta vários protocolos de transferência de mensagens, entre eles o X.400 P1. As informações de gerência estão sendo canalizadas para o ambiente SunNet Manager.

3.4.1 ISO Development Environment

O ISODE [ROS 90] é uma implementação não proprietária de alguns protocolos definidos pela ISO/IEC. O propósito de tornar este software *shareware* é acelerar o processo de desenvolvimento de aplicações no conjunto de protocolos OSI.

Este softaware pode suportar diferentes serviços de rede abaixo do *transport service access point* (TSAP). Um desses serviços de redes é o TCP. Isto permite o desenvolvimento de protocolos dos níveis superiores do modelo OSI em ambiente Internet.

O ISODE é composto basicamente pelos seguintes módulos:

- serviço de tranporte OSI classe 0 conforme rfc1006 [ROS 87];
- serviço de apresentação e sessão:
- compilador ASN.1;
- os elementos de serviço de aplicação ACSE, ROSE e RTSE;
- ftam e um gateway ftam-ftp;

- terminal virtual (vt);
- serviço de diretórios OSI, QUIPU;
- agente SNMP v1.

3.4.2 PP

O PP [KIL 91] é um ATM que suporta uma variedade de protocolos de transferência de mensagens, incluindo: X.400 (1984) P1, X.400 (1988) ISO(10021) P1; e outros protocolos baseados na rfc822 [CRO 82]

O PP é fruto do desenvolvimento conjunto de diversas instituições, em particular do UK Joint Network Team (JNT) [KIL 91]. É baseado na experiência prévias com ATMs, e tem as seguintes características:

- trabalha com grande volume de mensagens;
- características de gerência;
- facilidades para conversão de protocolos, particularmente para mapeamento entre protocolos baseados na rfc822 [CRO 82] e X.400 de acordo com rfc987 [KIL 86] e rfc1148 [KIL 90].
- conversão de formatos do corpo das mensagens;
- suporte para o desenvolvimento de agentes do usuário, particularmente para aqueles que desejam usar X.400 e/ou capacidades multimídia.

O PP é portável para sistemas Unix e sistemas compatíveis com Unix. Para comunicação interna o PP precisa do OSI/ROS, que é implementado pelo ISODE, bem como os níveis supeiores da pilha OSI. As ferramentas ASN.1 do ISODE também são necessárias para a instalação do PP.

A documentação do PP versão 6.0 especifica o uso do ISODE versão 7.0. Mas neste trabalho está em uso o ISODE versão 8.0, e nehum problema foi detectado até o presente momento.

3.4.3 SunNet Manager

O SunNet Manager [SUN 89] é uma coleção de ferramentas para gerenciar uma rede heterôgenea. O SunNet Manager provê uma plataforma comum baseada em todas as funções de rede e em uma interface com o usuário. Este ambiente possui um conjunto de agentes e gerentes os quais formam uma forte ferramenta para monitorar e controlar vários aspectos da rede.

A comunicação entre agentes e gerentes é realizada por RPC (Remote Procedure Call). O SunNet Manager oferece também agentes *proxy* SNMP.

Além de agentes e gerentes, o SunNet Manager, mantém uma base de dados que representa o modelo do ambiente gerenciado. Esta base de dados contém informações sobre os agentes que são suportados e os objetos que são gerenciados em cada componente da rede. As informações nesta base de dados determina como o SunNet Manager apresenta o *layout* da rede, das máquinas, características e menus associados.

Outra base de dados mantida pelo SunNet Manager são os arquivos *schema*. No arquivo *schema* são definidos os atributos, por nome e tipo, que o agente monitora.

Além dos agentes e gerentes oferecidos pelo SunNet Manager, está disponível uma API (Application Program Interface) para o desenvolvimento de novas funções de gerência.

3.4.4 Integração

A arquitetura do protótipo proposto é apresentada na figura 4. Os elementos utilizados no desenvolvimento do protótipo estão distribuídos na rede.

A figura mostra a interação entre cada módulo do sistema. O gerente comunica-se com o *proxy* através do protocolo RPC. O *proxy* traduz as requisições do gerente para o protocolo SNMP e as envia ao agente. No caminho inverso as resposta são traduzidas de SNMP para RPC.

O gerente executa em uma única máquina da rede, na configuração atual, e o *proxy* é executado na máquina onde é executada a console do SunNet Manager. O agente SNMP está instalado na máquina que tem funções de ATM, onde deve estar também o ISODE.

O SunNet Manager tem sua forma própria de representar os objetos que o agente monitora. Para que o gerente reconheça os objetos da MIB para

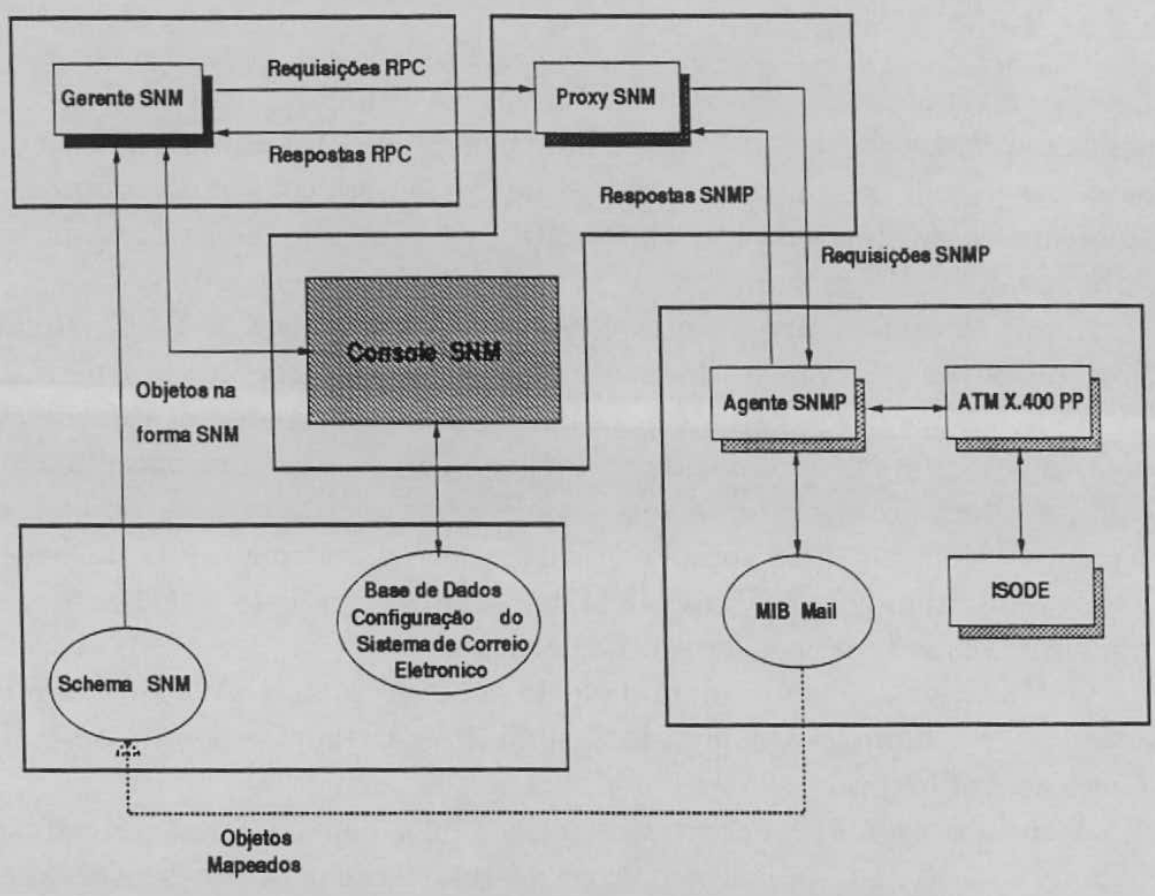

Figura 4: Integração dos diversos softwares

correio eletrônico é necessário mapear estes objetos para o formato SunNet Manager, criando o arquivo *agente.schema*. Esse mapeamento é realizado somente uma vez, a menos que ocorram alterações na MIB.

Os dados de configuração do sistema de correio eletrônico são armazenados na base de dados do SunNet Manager. Esta base de dados e o *agente.schema* estão armazenados no servidor de arquivos da rede, em diretórios conhecidos pelo SunNet Manager.

4 Conclusões

Gerenciar uma rede é uma tarefa interessante que torna-se mais atraente ao passo que descobre-se detalhadamente como encaixam-se as peças deste complicado "quebra-cabeça" e quais são os procedimentos, transparentes aos

usuários, que colocam a rede em funcionamento. Mais atraente é o fato de controlar a rede tornando-a confiável, integra e ágil.

Este trabalho cumpre seus objetivos, desvendando mecanismos do sistema de correio eletrônico, identificando quais são as informações necessárias para controlar este sistema e estabelecendo uma arquitetura para implementação do processo de gerência.

A MIB definida abstrai detalhes do funcionamento de um ATM e sua interface com outros elementos do sistema, mas é o começo para a exploração da gerência deste elemento e fornece informações suficientes para monitorar um ATM segundo os requisitos do Modelo Funcional.

Referências

[BOR 92] BORENSTEIN, N. and Freed, N. **MIME (Multipurpose Internet Mail Extensions)**. Reuqest For Comments 1341, June, 1992.

[CAR 93] CARVALHO, Tereza C. M. B. at all. **Gerenciamento de Redes de Computadores - Uma abordagem de Sistemas Abertos**. Makron Books do Brasil Ltdas, São Paulo 1993.

[CCITT 89] CCITT. **Data Communication Networks - Message Handling System**. Recommendations X.400-X.420, Blue Book, Geneva, 1989.

[COM 91] COMER, D. E. **Internetworking with TCP/IP: Principles, Protocols, and Architeture**. Volume 1. Seg. Edição. Prentice-Hall, Englewood Cliffs, NJ, 1991.

[CRO 82] CROCKER, David H. **Standard for the Format od ARPA Internet Text Messages**. Request for Comments 822, August 1982.

[KIL 86] KILLE, Steve. **Mapping between X.400 and RFC 822**. Requeste For Commmentes 987, June, 1986.

[KIL 90] KILLE, Steve. **Mapping between X.400(1988) / ISO 10021 and RFC 822**. Request For Comments 1148, March 1990.

[KIL 91] KILLE, Steve and Onion, Julian. **The PP Manual**. Volume 1, 2 e 3, 1991.

[KIL 94] KILLE, Steve and Freed, N. **Mail Monitoring MIB**. Request For Comments, January 1994.

[McC 93] McCOY, Emily and Freiwirth, Ray. **Email Management Requiremnets**. Working Draft, Joint IFIP WG6.5 and 6.6 Eletronic Mail Management Working Group, 1993.

[POS 82] POSTEL, Jonathan B. **Simple Mail Transfer Protocol**. Request For Comments 821, August 1982.

[ROS 87] ROSE, Marshall T. and Cass, D. **ISO Transport Service on top of the TCP**. Request for Comments 1006, 1987.

[ROS 90] ROSE, Marshall T. **The Open Book: A Practical Perspective on OSI**. Englewood Cliffs, Prentice-Hall, 1990.

[ROS 91] ROSE, Marshall T. **The Simple Book**. Prentice-Hall Inc., Englewood Cliffs, New Jersey 1991.

[SUN 89] SunMicrosystem. **SunNet Manager - Installation and User's Guide**. SunMicrosystem Inc., Mountain View 1988.

[SUN 89a] Sun Microsystem Inc. **Network Programming Guide**, 1989.

[WES 91] WESTPHALL, C. B. **Conception et développement de l'architecture d'administration d'un réseau métropolitain**. *Thèse de Doctorat nouveau régime*. Université Paul Sabatier. Toulouse, 16 Juillet 1991.