UM SISTEMA DE APOIO À GERÊNCIA DE REDES LOCAIS

Fernando Luís Dotti
Liane Margarida Rockenbach Tarouco

Curso de Pós-Graduação em Ciências da Computação
Instituto de Informática
Universidade Federal do Rio Grande do Sul

Resumo

Este artigo apresenta um estudo sobre a aplicação de recursos de inteligência artificial no apoio à tarefa de gerência de redes de computadores, mais especificamente redes locais do tipo CSMA/CD. São apresentadas as linhas gerais da arquitetura de um sistema para realizar tal função.

Abstract

This paper presents an investigation about the application of artificial intelligence technics aidding in the computer networks management task. A general architecture of a system to perform this task in a local area network is presented.

1 Introdução

O número e tamanho das redes de computadores instaladas estão crescendo continuamente e sua flexibilidade e versatilidade vem apoiando diversos tipos de áreas informatizadas. Com o uso crescente, os problemas das instalações começam a emergir e à tarefa de gerenciamento de redes é atribuida maior importância.

Este artigo aborda o complexo problema de gerência de redes locais, mais especificamente de redes locais do tipo CSMA/CD, cujo parque instalado é mais significativo.

Defende-se a idéia de que, a partir do tráfego gerado, pode-se inferir o perfil ou estado da rede, derivando ou antecipando os problemas da instalação que não poderiam ser

"sentidos" pelo administrador da rede de outra maneira [DOT90]. A partir desta idéia foi projetada a estrutura de uma ferramenta de apoio à gerencia de redes, que está em desenvolvimento na UFRGS como parte de uma dissertação de mestrado.

Este trabalho descreve em linhas gerais a arquitetura do sistema, e apresenta algumas conclusões a partir do trabalho até então realizado.

2 O Problema

O gerenciamento de uma rede local de porte considerável é uma tarefa complexa que não se esgota somente no trabalho de garantir a conectividade entre os componentes de hardware da rede. Deve-se realizar um trabalho mais extenso, envolvendo: detecção e isolamento de falhas, avaliação da performance, cuidados com a segurança dos recursos e contabilização de utilização.

Para que tais serviços possam ser supridos, o gerente da rede deve dispor de algumas ferramentas de apoio. Ferramentas para este fim tem surgido na comunidade pesquisadora e usuária, permitindo a monitoração do tráfego na rede [MOL87], [HAU87]. As informações assim obtidas permitem o acompanhamento periódico da rede, obtendo-se dados estatísticos sobre erros, *time-outs*, utilização de recursos, além de outras informações relevantes, podendo levar o gerente da rede ou construtor do software a diagnosticar possíveis problemas com mais exatidão e rapidez.

Contudo, o excesso de informações derivadas da monitoração e tabulação dos dados concernentes ao tráfego da rede pode inibir uma análise mais acurada , fenômeno conhecido como "indigestão de informações". Nota-se, ainda, a necessidade de uma ferramenta que efetue um tratamento preliminar dos dados "brutos", de forma a apresentá-los em volume e forma mais adequada.

3 Objetivos

Dentro do contexto acima descrito, verifica-se a utilidade de uma ferramenta para auxiliar o gerente de rede, dando apoio na tomada de decisões.

É neste sentido que estão sendo direcionados os esforços envolvidos no desenvolvimento de um Sistema de Apoio à Gerência

de Redes Locais. Este sistema tem como objetivo a captação, diagnose e auxilio à correção de problemas em redes locais, informando e justificando ao gerente da instalação os problemas detectados, os fatores causadores destes problemas e sugerindo procedimentos de correção adequados. Para realizar tal tarefa, são utilizados recursos de inteligência artificial, como veremos a seguir.

O sistema está sendo orientado ao gerenciamento de sistemas abertos (tal como definido no modelo OSI da ISO) o qual será descrito sucintamente na seção seguinte.

4 Arquitetura de Gerenciamento OSI

Para o desenvolvimento de padrões na área de gerenciamento de redes, a ISO estabeleceu o SC21/WG4 em Março de 1985. Segundo seu cronograma estes padrões não estarão completos até 1992. Apesar disso, vários conceitos já estão bem sedimentados e serão apresentados a seguir.

O Gerenciamento OSI é definido, em [ISO86], como: "as facilidades proporcionadas pela operação de gerenciamento de sistemas e gerenciamento de camadas para supervisionar e controlar os recursos OSI". Desta forma, o ambiente de Gerenciamento OSI consiste de dados e serviços necessários para controlar e supervisionar as atividades de interconexão e qualquer objeto gerenciado associado. A arquitetura de Gerenciamento OSI é assim distribuída pelas estações da rede, realizando tarefas que vão desde a captação de pequenas porções de informação sobre elementos remotos até a agregação destas informações em um nodo gerente, inferindo o estado da comunicação.

4.1 Domínio de Gerenciamento

Domínio de Gerenciamento está relacionado com a extensão gerenciada da rede. Um domínio de gerenciamento pode ser composto de uma coleção de Sistemas Gerentes e uma coleção de Sistemas Gerenciados.

4.2 Sistema Gerente

Um Sistema Gerente é responsável por uma fração do Domínio Gerenciado agregando as informações dos Sistemas Gerenciados de sua responsabilidade. Para obtenção destas informações, o Sistema Gerente, através de um Processo Gerente, invoca o Sistema Gerenciado, mais especificamente o Processo Agente no Sistema Gerenciado, que tem acesso aos Objetos Gerenciados naquele nodo.

4.3 Sistema Gerenciado

O Sistema Gerenciado abriga uma coleção de Objetos Gerenciados e responde, através do Processo Agente, aos pedidos de informação e comandos do Sistema Gerente sobre seus objetos. Ao Agente cabe, também, reportar ao Sistema Gerente os eventos ocorridos com os seus Objetos Gerenciados.

4.4 Objeto Gerenciado

Objetos Gerenciados (Managed Objects - MO) são o alvo de todas as operações de gerenciamento OSI. O local dos Objetos Gerenciados corresponde ao local dos recursos gerenciados relacionados. Um Objeto Gerenciado consiste de:

a. Atributos - representam valores do recurso relacionado (sendo gerenciado) que podem ser lidos e alterados pelo Sistema Gerente ao qual este objeto pertence;

b. Eventos - são mensagens pré-definidas que serão relatadas do Sistema Gerenciado para o Gerente no caso de uma transição de estado relevante.

c. Ações - podem ser iniciadas no Sistema Gerenciado, isto permite ao Sistema Gerente pedir a um sistema aberto que inicialize seus recursos, reinicialize-se, ou mesmo realize funções de teste, mantendo o nível de abstração;

d. outros Objetos Gerenciados contidos neste objeto - esta característica leva a uma estrutura hierárquica (em árvore) em que, por exemplo, o objeto de nível mais alto é da classe "Sistema" e representa toda estação através de uma composição de objetos.

Uma instância de Objeto Gerenciado é definida pelo seu nome (Identificador do Objeto) e seu tipo (Classe do Objeto), incluindo as operações possíveis sobre a instância e suas características (atributos, eventos, ações, objetos contidos).

4.5 Base de Informações Gerenciais

A Base de Informações Gerenciais (Management Information Base - MIB) é uma base de dados conceitual formada pela coleção de todos Objetos Gerenciados contidos no Domínio Gerenciado. A MIB é distribuída sobre todos os Sistemas Gerentes e Gerenciados da rede.

4.6 Entidade de Camada

Uma Entidade de Camada - *N* (Layer Entity - LE) é responsável pela monitoração e controle das comunicações relativas à camada *N*, utilizando-se para isso dos protocolos da camada *N*.

4.7 Entidade de Gerenciamento de Camada

Uma Entidade de Gerenciamento de Camada *N* (Layer Management Entity - LME) é responsável pelas operações de gerenciamento restritas à camada *N*, utilizando-se para isso dos protocolos de gerenciamento da camada *N*.

4.8 Entidade de Aplicação para Gerenciamento de Sistemas

Uma Entidade de Aplicação para Gerenciamento de Sistemas (Systems Management Application Entity - SMAE) utiliza-se de um protocolo para gerência de sistemas que possibilita o acesso aos dados de gerenciamento de todas camadas em um nodo. Com tal poder, a SMAE fornece um eficiente serviço de apoio aos Processos de Aplicação para Gerenciamento de Sistemas (SMAP - exposto no ítem seguinte). O interfaceamento entre o SMAE e o SMAP acontece através de um Elemento de Serviço de Aplicação para Gerenciamento de Sistemas (SMASE - Systems Management Application Service Element), que define um conjunto de primitivas para cada área funcional de gerenciamento (ver ítem 4.10).

4.9 Processo de Aplicação para Gerenciamento de Sistemas

O Processo de Aplicação para Gerenciamento de Sistemas (SMAP - Systems Management Application Process) tem acesso, através da MIB, aos dados de gerenciamento de todas camadas do nodo nela contidos. Um SMAP assume o papel de um Processo Gerente ou Processo Agente, ou ambos. Qualquer SMAP pode comunicar-se com um SMAP remoto para trocar informações de gerenciamento, utilizando-se para isso do SMAE.

A estrutura até então descrita pode ser visualizada da seguinte forma:

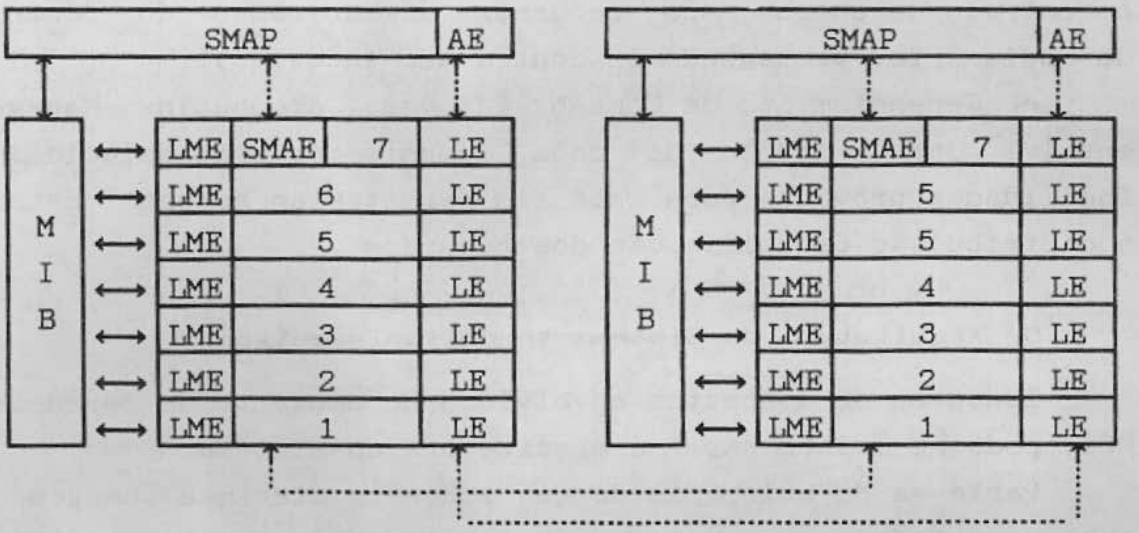


Figura 1: Ambiente de gerenciamento OSI.

4.10 Áreas funcionais de gerenciamento

Na padronização OSI, as diferentes tarefas de gerenciamento em uma rede são classificadas em cinco grupos denominados Áreas Funcionais Específicas de Gerenciamento (SMFAs - Specific Management Functional Areas), são elas:

a. Gerenciamento de Falhas ("Fault Management" envolve um conjunto de facilidades que permitem a detecção, isolamento e correção de uma operação anormal da rede).

b. Gerenciamento de Configuração ("Configuration Management" envolve tanto o gerenciamento lógico quanto o físico. A

configuração lógica inclui nomeação, parâmetros de interfaces, parâmetros de protocolos, etc. A configuração física trata da localização física dos nodos, configuração de hardware, etc).

c. Gerenciamento de Performance ("Performance Management" realiza a avaliação, controle e predição da performance da rede; esta avaliação envolve o acompanhamento das diversas camadas do Modelo OSI. Para isso, existem definidas no âmbito desta função de gerenciamento uma série de facilidades para obtenção de dados estatísticos dos Objetos Gerenciados de cada camada, possibilitando a derivação da performance da rede, pontos críticos, futuros gargalos, etc).

d. Gerenciamento de Segurança ("Security Management" envolve o controle de acesso aos recursos e sub-redes do Domínio de Gerenciamento, protegendo-os contra uso indevido).

e. Gerenciamento de Contabilizações ("Accounting Management" envolve dar o custo de cada comunicação estabelecida. As facilidades providas para este fim permitem ao gerente determinar a distribuição da utilização dos recursos).

5 Arquitetura do Sistema sendo implementado

Tendo-se os conceitos envolvidos no ambiente de gerenciamento OSI, pode-se melhor expor a arquitetura do sistema.

Parte-se do princípio de que todos os sistemas abertos estão interconectados a uma mesma rede local e que não têm condições de atuar como sistemas agentes. Esta foi a situação real encontrada na UFRGS onde juntamente com o software OSI desenvolvido localmente [TAR88] [WIL86] [WIL89], é preciso conviver com software recebido pronto.

O sistema está dividido em duas partes principais bem distintas: detecção de problemas e diagnóstico, que serão abordadas a seguir.

5.1 Detecção de Problemas

Para a construção do sistema em questão, optou-se por dedicar uma das máquinas à tarefa de monitoração da rede. Nesta máquina, os quadros que trafegam na rede Ethernet são capturados por um

driver que coloca a placa de rede em modo promíscuo ; este modo permite que quadros endereçados a quaisquer estações sejam captados pela estação em que o sistema esta instalado. Assim todo tráfego pode ser analisado.

Cada unidade de dado capturada passa por um processo de desencapsulamento, gerando uma estrutura interna que a representa. O desencapsulamento destas unidades de dados se dá conforme as camadas de protocolos de comunicação em uso, assim como na estrutura OSI da ISO [TAR90]. As informações de cada camada, para uma mesma unidade de dado, servem de entrada para processos de contabilização, modificando estruturas de contabilização (propostas abaixo). Estas contabilizações são disparadas exatamente nos pontos onde existem Objetos Gerenciados, alimentando a MIB (analogia com o sistema de gerenciamento OSI), e existem para agregar as informações conforme as necessidades de um especialista.

A contabilização de cada evento relativo a um objeto gerenciado se dá em uma estrutura individual suportando as informações necessárias para representar o comportamento da rede com relação àquele objeto. No momento da atualização da estrutura referente ao objeto gerenciado verificam-se limites de tolerância do objeto para ocorrência daquele evento e se estes limites forem ultrapassados isto é notificado em um "histórico" da instalação guardando os alarmes que aquela rede apresentou durante o tempo, na observação dos objetos - alimentando, novamente, a MIB.

Para cada alarme diferente existe uma estrutura diferente no histórico representando-o, informando sobre possíveis causas e efeitos colaterais - fazendo parte da MIB. Juntamente com a atualização dos históricos, também é atualizada uma lista de objetos e alarmes consequentes servindo de entrada para um processo de inferência. Esta lista é dividida em conjuntos de pares objeto/alarme detectados por nível, conforme as camadas de protocolos - ela é a interface entre a MIB e o processo de aplicação para gerência de sistemas (SMAP) que no caso é um sistema especialista.

O processo acima descrito está ilustrado na figura 2 abaixo.

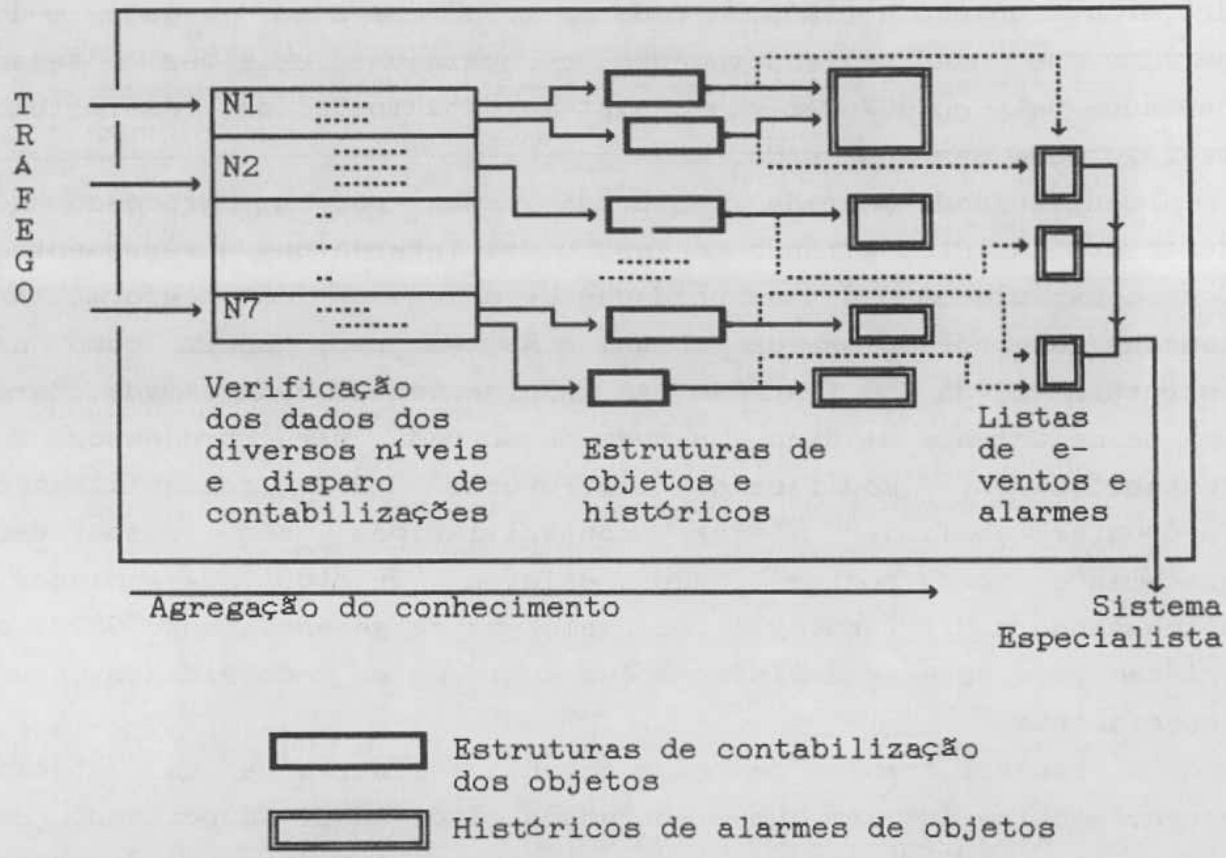


Figura 2: Detalhe da MIB.

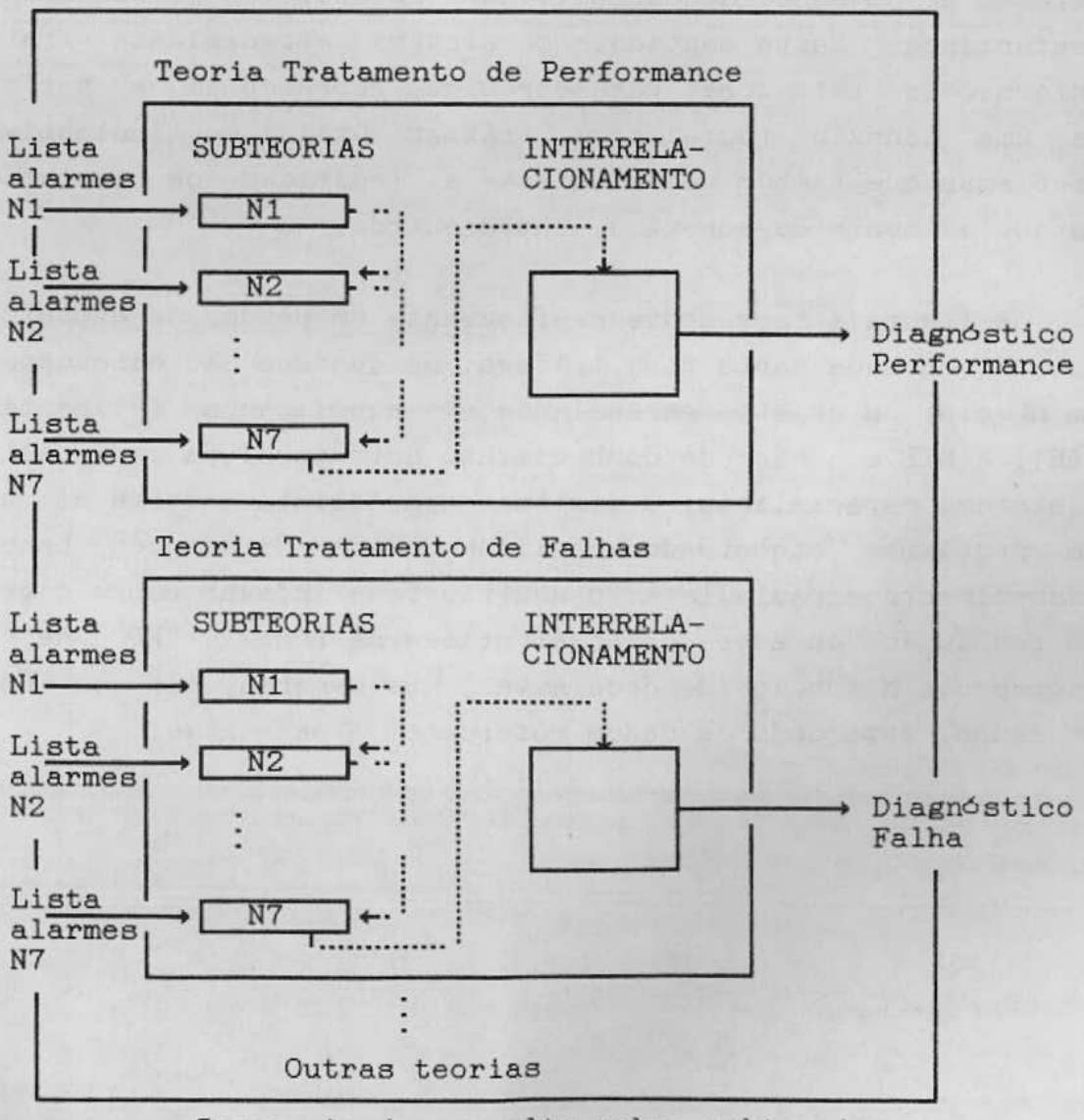
5.2 Processo de diagnóstico

Para alimentar o processo de diagnóstico, além das listas de objeto/alarme por nível e dos dados da MIB anteriormente descrita, também se faz necessária uma base de conhecimento estrutural da rede, informando sua estrutura, os diversos componentes, sua distribuição, os pontos servidores, e demais características relevantes.

O conhecimento do especialista é dividido em bancos específicos conforme as áreas funcionais descritas no ambiente de gerenciamento OSI, particularizando o conhecimento em teorias. Cada teoria para cada área funcional está dividida em "subteorias" que tratam os problemas de cada nível de protocolo, seguindo o MR-OSI. Assim, as listas de objeto/alarme por nível geradas na fase de detecção de problemas entram na teoria específica para o nível e área funcional em tratamento.

Uma "subteoria" agrega conhecimento de um nível específico e gera diagnósticos de uma área funcional para aquele nível, sem levar em consideração os demais níveis.

O trabalho de relacionamento de diagnósticos dos diversos níveis é feito através de um outro banco de conhecimento. Este, por sua vez, é alimentado pelas saídas das diversas subteorias, interrelacionando-as. Neste processo de interrelacionamento, os diagnósticos de níveis isolados podem ser validados, ou cancelados por serem resultado de um problema único que interfere em vários níveis, neste último caso o sistema especialista infere o problema "raiz".



..... Sequencia de consulta sobre subteorias, encadeamento para frente em amplitude.

Figura 3: Teorias e subteorias no processo de diagnose

Verificando-se o domínio do problema , foi constatado que o motor de inferência deve realizar encadeamento progressivo (pois os estados iniciais da inferência são em número menor que os estados finais possiveis) e em amplitude já que se colecionam os problemas dos diversos níveis de protocolo e depois são interrelacionados. O mesmo motor de inferência age sobre os diversos bancos de conhecimento.

A figura 3 ilustra como as várias teorias estão organizadas para o processo de diagnóstico.

Neste trabalho, esforços estão sendo direcionados para a criação de um banco de conhecimentos relativo a gerenciamento de performance. Neste sentido, o sistema especialista trata com informações tais como: parâmetros que representam a performance de uma conexão (duração X tráfego útil) ou indicativos de problemas que também podem afetá-la (rejeição de tentativa de estabelecimento de conexão), entre outros.

A figura 4 representa graficamente um resumo do exposto. Uma estação da rede capta todo tráfego; os quadros são desencapsulados em níveis; os objetos gerenciados são atualizados (alimentando a MIB); a MIB e a base de conhecimento estrutural da rede alimentam o sistema especialista; o sistema especialista informa ao usuário os problemas encontrados utilizando os diferentes bancos de conhecimento especialista; o usuário pode indagar sobre o processo de resolução, ou sobre características da rede. "FD" na figura representa a função (de cada nível) que desencapsula as unidades de dados, separando os dados referentes a cada nível.

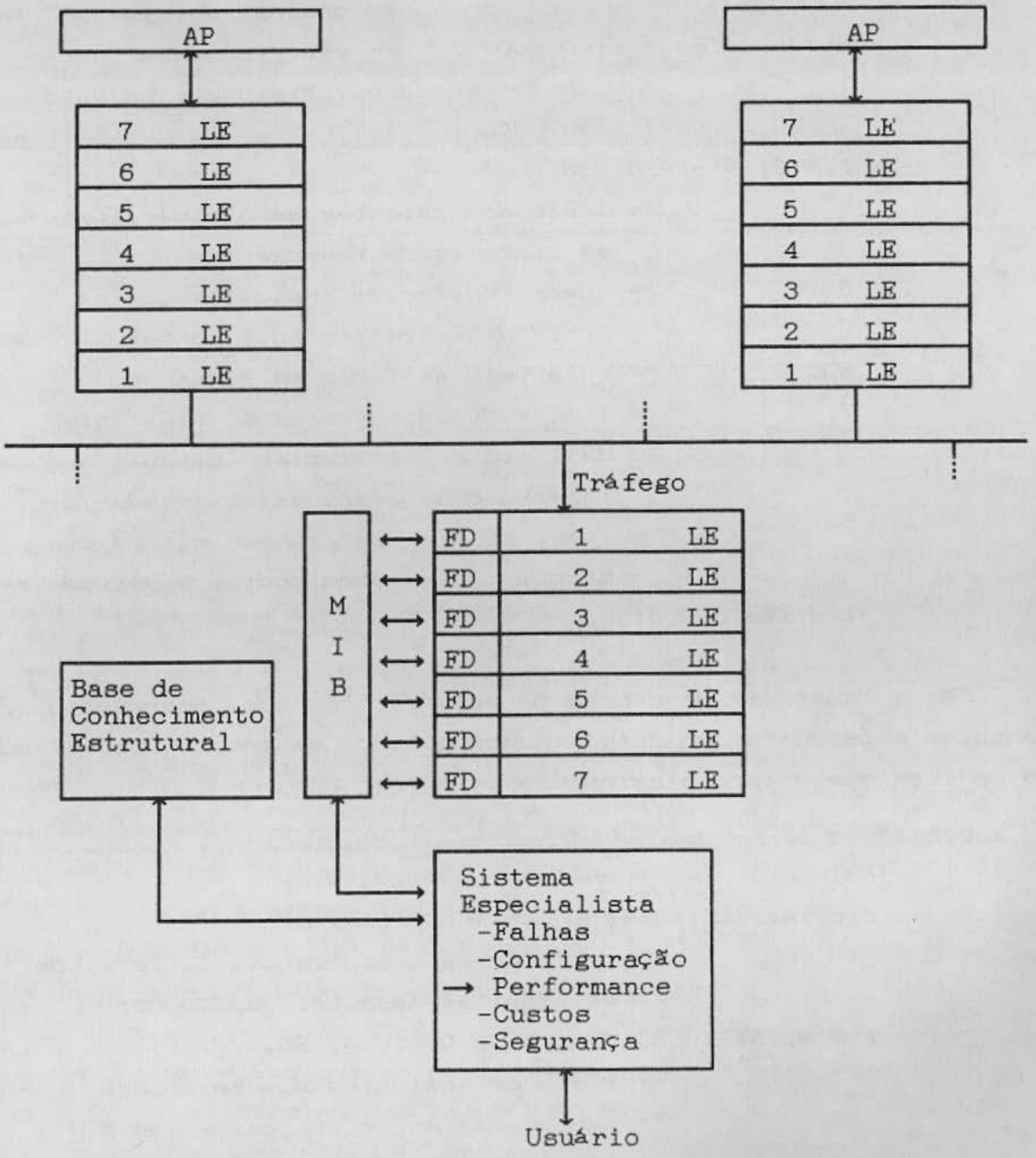


Figura 4: O sistema proposto.

A seguir está apresentado um pequeno exemplo para o processo de detecção de problemas (contabiliações na MIB) e diagnóstico (Sistema Especialista).

Como explanado anteriormente, o tráfego capturado é analizado e conforme os eventos ocorridos, são criadas e alteradas algumas estruturas de contabilização do tipo:

```
contab(
        N2,                              /* análise do nível 2  */
        ausência(msgs_de(000001)),  /* verifica-se a ausên-
                        cia de mensagens originadas na esta-
                        ção 000001                          */
        [15.01.91-10:01:30,...],
                        /* lista de instantes em que verificou-
                           se ausência de mensagens         */
        30              /* número máximo de instantes que a
                           lista de instantes pode conter   */
        500,            /* intervalo de tempo em segundos   */
        7,              /* limite de ocorrências de instantes
                           na lista de instantes durante o
                           intervalo de tempo especificado a-
                           cima, se for verificada ocorrência
                           maior, o sintoma abaixo é ativado */
        inativa(000001)
    )
```

Obs.: "ausência de mensagem" significa a não ocorrência da mensagem esperada em um determinado período de tempo (verificado na análise que altera a estrutura acima).

```
contab(
        N4,             /* análise do nível 4 */
        ocorrência(rejeição_conex(000001)),
                        /* verifica-se a ocorrência de rejeição
                           de conexões pela estação 000001  */
        [15.01.91-10:30:09, 15.01.91-10:31:35, ...],
                        /* lista de instantes das rejeições */
         25,            /* número máximo de instantes que a
                           lista de instantes pode conter   */
         800,           /* intervalo de tempo em segundos   */
         15,            /* limite de ocorrências de instantes
                           na lista de instantes dentro do
                           intervalo de tempo especificado a-
                           cima, se for verificada ocorrência
                           maior, o sintoma abaixo é ativado */
```

```
        não_conectável(000001)
    )
```

O alarme é ativado colocando-o em uma lista de entrada para o processo de diagnóstico e em um histórico do alarme. Suponha que a lista de alarmes do nível 4, em determinado momento, seja:

```
[não_conectável(000001)]
```

Também o conhecimento estrutural é necessário ao diagnóstico, por exemplo:

```
estrutura(000001, serv_arq, 500Mb).
estrutura(000002, serv_arq, 900Mb).
...
```

No processo de diagnóstico, na teoria de tratamento de performance, na "subteoria" de nível 4, aplica-se a regra:

```
...
SE não_conectável(X) E    /* o sintoma está ativo */
   not(inativa(X))   E    /* o sintoma está inativo */
   estrutura(X,serv_arq,_)   /* X é servidor */
ENTÃO (Estação saturada devido à demanda de serviços-
       Possíveis soluções:...)
...
```

este diagnóstico passa, ainda, pelo processo de interrelacionamento, onde é validado como diagnóstico final ou contribui para a formação do um diagnóstico que identifica o problema "raiz". O processo como um todo, fornece o problema e as soluções possíveis para o gerente em um arquivo de log. Além de consultar o log de problemas e possíveis soluções, o gerente pode consultar, alterar e criar contabilizações de eventos e históricos, bem como expandir a base de regras.

6 Conclusões

A utilização de recursos de inteligência artificial tem sido crescente na gerência de redes visando criar melhores condições para dominar a complexidade do problema. Isto se deve, principalmente, à habilidade com que se pode tratar as dificuldades enfrentadas pelas formas convencionais de

processamento da informação, permitindo chegar a soluções mais naturais, emulando um especialista humano na busca de respostas.

No presente caso, a utilização destas técnicas impõe um processamento pesado, penalizando em parte a performance do sistema gerenciador e dificultando sua utilização em modo real-time. Acredita-se que este problema poderá ser amenizado com a evolução constante do hardware (CPUs mais rápidas, *fuzzy logic*) e com pesquisas na área de inteligência artificial, buscando algorítmos mais eficientes.

A centralização e "passividade" (o sistema não gera mensagem na rede) são também características importantes que interferem na forma como o sistema atua apresentando vantagens e desvantagtens, algumas vantagens são:

- os demais sistemas permanecem inalterados, mas controlados;
- o sistema não depende da rede sendo controlada para exercer sua função (no que diz respeito a troca de mensagem de gerenciamento);
- o gerente da rede pode dispor de uma ferramenta de apoio a um custo relativamente baixo;

Algumas desvantagens desta característica são:

- o sistema não pode agir sobre a rede, sua função se restringe a detectar o problema, diagnosticá-lo, e alertar o gerente ou administrador;
- um subconjunto menor de objetos podem ser gerenciados, isto é, somente os objetos possíveis de serem acompanhados pelo tráfego da rede, não permitindo o acompanhamento de objetos exclusivos de estações remotas (visíveis apenas internamente);

Nota-se, apesar das desvantagens, que um bom trabalho pode ser desenvolvido com este tipo de sistema. No caso particular em desenvolvimento, o gerenciamento de performance pode acontecer através do acompanhamento das diversas conexões, mediante:

- determinação de recursos mais disputados pelas estações;
- determinação do perfil de tráfego da rede;
- derivação do comportamento futuro da rede com o crescimento de tráfego, tendo o perfil atual;
- detecção de tipos de transações mais comuns;
- determinação das características dos usuários (em termos de

tráfego gerado);

- localização de recursos disponíveis que podem ser melhor utilizados;
- localização de pontos onde expansões devem acontecer;
- etc.

Enfim, a utilização de recursos de inteligência artificial apoiando tarefas de gerência de redes mostra-se de relevante contribuição em ambas as áreas de interesse: em inteligência artificial aplicam-se novas formas de modelagem através do trato com novos problemas; em gerência de redes o domínio da complexidade dos problemas se torna mais factível. Pode-se afirmar que os sistemas futuros serão mais abrangentes, gerenciando um número maior de objetos e agindo sobre a rede, mas para chegar a este ponto o trabalho atual é necessário.

Referências Bibligráficas

[WIN84] WINSTON, P. *Artificial intelligence.* Addison-Wesley, E.U.A. , 1984, 2ª edição.

[WIL86] WILKENS, Maria J. e TAROUCO, Liane M. R. *Implantação de um sistema padrão de transferência de mensagens distribuído.* In: Congresso Nacional de Informática, 19. SUCESU, Rio de Janeiro, 18 a 24 de Agosto de 1986, pp. 387-392.

[ISO86] ISO DP 7498-4 : *Information Processing Systems - OSI Reference Model Part 4: Management Framework* - oct. 1986.

[MOL87] MOLVA, R. et al. *Observer: A Traffic Analysis Tool for Local Area Networks.* IFIP TC6 WG6.4 International In-Depth Symposium on Local Communication Systems: LAN and PBX. Tolouse, France, 26-28 November, 1986.

[HAU87] HAUGDAHL, J. S. *Analyzing Network Traffic.* PC Tech Journal, 10(5), 1987.

[LIE88] LIEBOWITZ, J. *Expert systems applications to telecommunications.* John Wiley & Sons, 1988.

[TAR88] TAROUCO, Liane et al. *Interconexão Micro-Mainframe para Processamento Cooperativo.* In: XXI Congresso

Nacional de Informática., Rio de Janeiro, 22 a 26 de Agosto de 1988.

[WIL89] WILKENS, Maria J. e TAROUCO, Liane M. R. *X400: O que, porque e quando.* In: CIL 89 - Convención Informática Latina, 13 a 17 de Março de 1989. Anais. pp. 296-307.

[MAN89] MANTELMAN, L. *How an exper system eases a variety of network management tasks.* Data Communications International, 18(13), 1989.

[HUN89] HUNTINGTON, J. *OSI-based net management: Is it too early, or too late?* Data Communications International, 18(3), 1989.

[TAR90] TAROUCO, L.M.R. & DOTTI, F.L. *MEFISTO- Mechanism Efficient to Foster the Implementation of Software Totally OSI.* IFIP TC6 WG6.4a International Symposium on Local Communications Systems Managemet. University of Kent at Canterbury, U.K. 18-19 Setembro, 1990.

[DOT90] DOTTI, Fernando L. *Um Sistema de Apoio à Análise de Tráfego": Trabalho Individual.* Porto Alegre. Curso de Pós-Graduação em Ciências da Computação - UFRGS.