Uma Ferramenta para Monitoração das Tabelas de Rotas e da Configuração de Roteadores em um Backbone

Mário L. Moura Júnior Antônio A. F. Loureiro Mário F. M. Campos
{mjunior, loureiro, mario}@dcc.ufmg.br

Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
Belo Horizonte, MG

Resumo

A correta configuração e operação de roteadores e equipamentos de conexão em um *backbone* é um fator primordial para o seu funcionamento. Este trabalho apresenta uma ferramenta baseada no protocolo SNMP capaz de identificar as redes adjacentes a um *backbone*, monitorar a configuração das portas dos roteadores e das suas respectivas tabelas de rotas corrigindo automaticamente as falhas detectadas. A ferramenta implementa gerência proativa utilizando o princípio da superimposição que é apresentado e discutido também neste trabalho. A ferramenta apresenta como contribuições a capacidade de detectar e corrigir automaticamente alterações indevidas na configuração e nas tabelas de rotas dos roteadores, a identificação de números IPs alocados porém não utilizados e a adoção do princípio da superimposição na sua implementação.

Abstract

The correct configuration and maintenance of routers and connection equipments in a backbone is a key issue for its proper operation. This paper presents a tool based on SNMP which given a backbone is able to identify its neighbor network and monitor the interfaces and routing tables of the routers present in the backbone. The tool also corrects automatically any error present in the routing tables. It implements proactive management using the principle of superimposition. The main contributions of this paper are the ability to detect automatically changes in both the interface configuration and routing tables, identify IP numbers not in use, and the adoption of superimposition as a principle to implement the proactive management.

Palavras chave: Gerência de Redes, Gerenciamento Proativo, SNMP, Internet

1 Introdução

A correta configuração e operação de roteadores e equipamentos de conexão em um *backbone* é um fator primordial para o seu funcionamento [Souza, 1997]. Para isto, aspectos relativos às cinco áreas de gerência devem ser constantemente analisados. Um roteador configurado incorretamente, seja por desconhecimento da sua operação ou por má fé, pode implicar em falhas no seu funcionamento e de toda a rede. Eventualmente, tais falhas podem ser propagadas para fora dos domínios da rede de origem ocasionando problemas em escala maior e nem sempre de fácil resolução e detecção.

Uma ferramenta capaz de monitorar alterações na configuração dos roteadores, verificar dinamicamente as suas tabelas de rotas e apresentar os resultados de forma simples e

direta constitui importante contribuição para o gerenciamento de um *backbone* Internet. Para isto, a ferramenta deve possuir as seguintes características:

- Monitoração da configuração dos roteadores: Alterações não autorizadas na configuração dos roteadores podem atrapalhar o roteamento interno e externo do *backbone*. Uma ferramenta para este fim deve ser capaz de detectá-las e, idealmente, corrigi-las automaticamente.
- Geração de histórico de alterações: O armazenamento das configurações anteriores, além de fornecer um histórico das diversas alterações, auxilia o administrador no retorno a uma configuração antiga caso alguma tomada de decisão tenha sido realizada indevidamente.

Monitoração das tabelas de rotas: Falhas no roteamento podem ser causadas, por exemplo, pela utilização de endereços IP não alocados, ligação de uma instituição a diversos *backbones* e conexões não autorizadas aos roteadores. Uma ferramenta para este fim deve ser capaz de detectar rotas indevidas, eliminando-as o mais rápido possível.

- Pesquisar as redes vizinhas aos roteadores: A determinação da topologia e da vizinhança do *backbone* possibilita um melhor entendimento de sua estrutura e funcionamento, auxiliando assim, o administrador na tomada de decisões.
- Interface simples: A interface da ferramenta deve ser simples, independente de plataforma de acesso e permitir a utilização remota.

Neste trabalho é apresentada uma ferramenta com as características descritas acima. Esta ferramenta, além de executar funções relacionadas com o gerenciamento de configuração, implementa funcionalidades relacionadas com a gerência proativa, sendo apresentada a adoção do princípio da superimposição como base para a implementação deste esquema de gerência. O objetivo final é identificar e solucionar problemas relacionados com o roteamento antes que estes afetem o funcionamento da rede e de suas vizinhanças.

O trabalho está organizado da seguinte forma. A seção 2 discute os trabalhos relacionados com monitoração de tabelas de rotas, configuração de roteadores e gerenciamento proativo. A seção 3 apresenta o modelo de gerência proativa adotado neste trabalho. A seção 4 descreve a implementação da ferramenta e as decisões de projeto. Na seção 5 são descritos os resultados obtidos. Finalmente, na seção 6 são apresentadas as conclusões e trabalhos futuros.

2 Trabalhos Relacionados

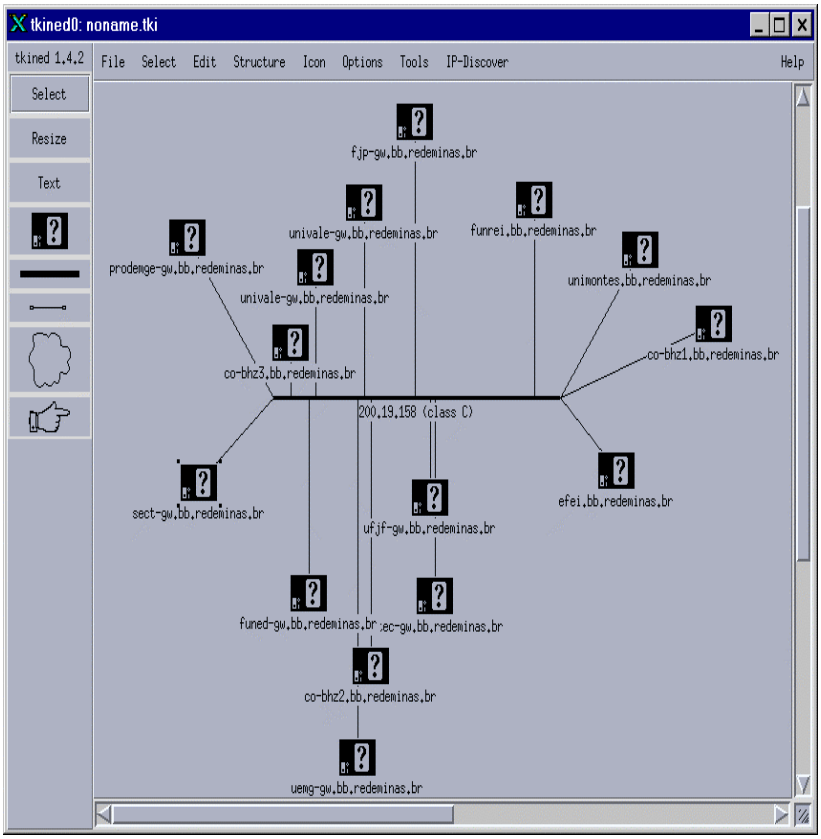
Esta seção descreve alguns trabalhos relacionados ao monitoramento das tabelas de rotas e da configuração de roteadores e ao gerenciamento proativo.

Segundo [Souza, 1997], a gerência de redes geograficamente dispersas deve estar centrada na monitoração constante dos canais de comunicação (modems e linhas de comunicação) e dos equipamentos de interconexão (roteadores). O autor apresenta uma discussão sobre o intervalo de tempo adequado para *polling* em elementos de rede com funcionalidades diferentes. Os dispositivos cujas características variem com maior intensidade ou cuja alteração possa trazer maiores conseqüências a rede devem apresentar menores tempos entre leituras.

O sistema desenvolvido apresenta como pontos principais a interface WWW, a facilidade de incorporação das informações geradas por outras ferramentas e a constante

avaliação do desempenho dos equipamentos da rede. Por outro lado, não é capaz de monitorar alterações na configuração dos equipamentos.

[Schonwalder, 1993] apresenta um software de gerência de redes (*Scotty*) que possui, entre outras características, a capacidade de determinar a topologia de uma rede e de suas vizinhanças. A determinação é feita através de consultas às tabelas de rotas dos roteadores envolvidos. Esta abordagem, apesar de simples, apresenta falhas pois roteadores com mais de um número IP têm cada um dos seus endereços identificados como roteadores independentes (Figura 1). Além disso, o *Scotty* apresenta restrições de uso devido a adoção da plataforma X11 que limita a sua utilização a máquinas que suportem o ambiente XWindows.



Roteadores reais
co-bhz1.bb.redeminas.br
co-bhz2.bb.redeminas.br
co-bhz3.bb.redeminas.br

Roteadores classificados incorretamente como mais de um roteador
co-bhz1.bb.redeminas.br
funrei-gw.bb.redeminas.br
unimontes-gw.bb.redeminas.br
efei.bb-gw.redeminas.br
co-bhz2.bb.redeminas.br
uemg-gw.bb.redeminas.br
ufjf-gw.bb.redeminas.br
funed-gw.bb.redeminas.br
cetec-gw.bb.redeminas.br
co-bhz3.bb.redeminas.br
univale-gw.bb.redeminas.br
sect-gw.bb.redeminas.br
prodemge-gw.bb.redeminas.br
fjp-gw.bb.redeminas.br

Figura 1 – *Backbone* simplificado da Rede Internet Minas gerado pelo *Scotty*

O *Sun Net Manager* (SNM) [Sun, 1995] consiste em um software comercial para gerenciamento de redes amplamente utilizado no mercado. O SNM possui um módulo capaz de realizar consultas às tabelas de rotas dos roteadores e de pesquisar as vizinhanças do *backbone*, embora com as mesmas restrições do *Scotty* para a identificação de roteadores. Algumas restrições ao uso do SNM são o custo do produto, a plataforma restrita de acesso (*SunOs / Solaris - X11*) e o grande consumo de recursos computacionais.

[Snell, 1996] afirma que a Web é o ambiente ideal para o desenvolvimento de aplicações para gerência de redes, pois a interface é padronizada entre os diversos sistemas operacionais, os custos de treinamento são reduzidos e as aplicações são independentes da plataforma de acesso.

A gerência proativa permite que problemas potenciais sejam detectados antes que eles se materializem. Deste modo, consegue-se rapidamente executar contramedidas, reduzindo-se as proporções do possível problema. Os diversos trabalhos acadêmicos consultados durante o

projeto mostraram uma tendência em concentr o foco de ação nos aspectos de gerência de falhas, tipicamente correlação de alarmes [Dilmar et al., 1997] [Grimes et al., 1997] [Hood et al., 1998] [Kätker et al., 1997] [Katzela et al., 1993], e de desempenho, tipicamente controle de tráfego [Cruz et al., 1997] [Rocha et al., 1997]. Por outro lado, as implementações comerciais pesquisadas tendem a abordar basicamente o gerenciamento proativo de configuração [3com, 1999] [Cisco a, 1999] [Cisco b, 1999] [HP a, 1999] [HP b, 1999]. O esquema de gerência adotado nestas aplicações, com exceção do *Netsys* [Cisco b, 1999], é uma variação da idéia original onde o agente é capaz de corrigir problemas automaticamente. Ao ser detectada uma falha na configuração, o sistema aciona o administrador para este atuar proativamente na rede.

O software *Netsys* é apresentado como uma ferramenta para gerenciamento de configuração, desempenho e falhas na rede. A ferramenta é capaz de armazenar configurações dos elementos de rede, verificando e corrigindo se necessário; distribuir relatórios sobre a "saúde" relativa dos recursos da rede; determinar e solucionar problemas de roteamento e indicar o *status* operacional dos roteadores. O maior problema associado ao *Netsys* é o seu custo de aquisição.

3 Modelo de Gerência Proativa

Existem vários algoritmos distribuídos que executam algum tipo de supervisão de um algoritmo de rede *A* durante sua execução. O algoritmo de *"consistent global snapshot"* proposto por Chandy e Lamport [Chandy et al., 1985] é um exemplo desta classe de algoritmos. Neste cenário é importante notar que existem duas computações distribuídas. A primeira está relacionada com algoritmo de rede *A* chamado também de substrato. Este é o algoritmo de interesse que deseja-se supervisionar. A segunda computação distribuída está relacionada com a execução do algoritmo de supervisão responsável por alguma tarefa específica como por exemplo depuração ou detecção de uma propriedade. Este algoritmo é chamado algoritmo de superimposição [Barbosa, 1996][Lynch, 1996].

Neste trabalho é proposto o uso do princípio de superimposição em gerência proativa. Neste caso, o substrato corresponde ao gerenciamento tradicional do elemento de rede e o algoritmo de superimposição ao algoritmo de gerência proativa, como mostrado na Figura 2. O algoritmo de superimposição pode ser usado para modificar o comportamento do algoritmo do substrato de acordo com as condições da rede em um determinado momento do tempo.

A adoção deste princípio apresenta duas vantagens principais. A primeira consiste na distinção clara entre as funções de gerenciamento de rede tradicional e de gerência proativa. A segunda é a possibilidade de utilizar algoritmos distribuídos de supervisão no suporte a gerência proativa [Barbosa, 1996] [Loureiro et al., 1996] [Lynch, 1996].

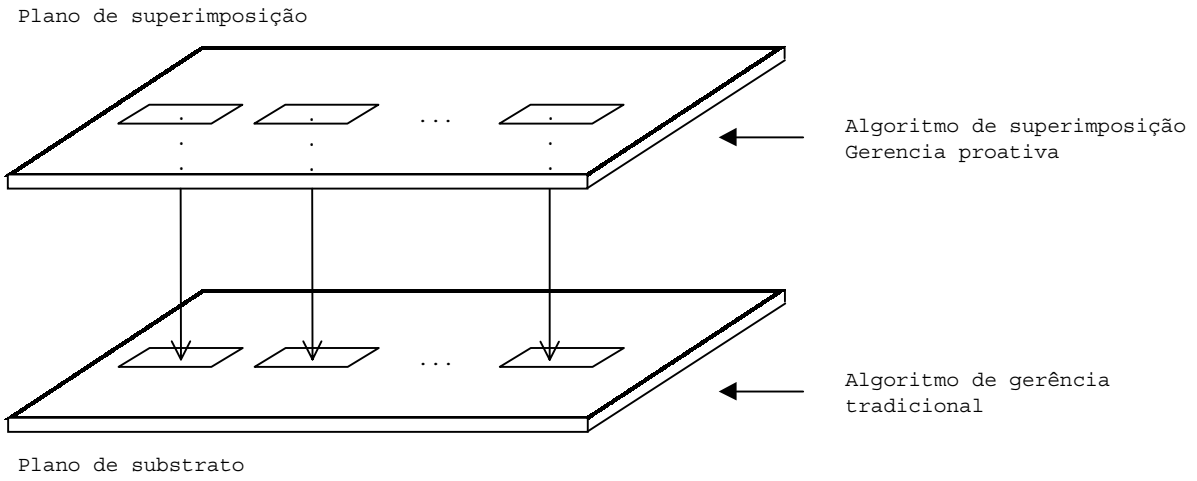


Figura 2 – Princípio da superimposição

4 Uma Ferramenta para Monitoramento de Roteadores

A ferramenta foi desenvolvida para o gerenciamento dos roteadores do *backbone* da Rede Internet Minas (RIM) embora possa ser facilmente adaptada para outros ambientes. A RIM é um convênio entre a Fundação de Amparo a Pesquisa de Minas Gerais (FAPEMIG), a Universidade Federal de Minas Gerais (UFMG) e a Secretaria de Estado de Ciência e Tecnologia de Minas Gerais (SECT-MG) para provimento de acesso a Internet às instituições federais de ensino superior (IFES) do estado de Minas Gerais. O seu *backbone* está organizado em estrela, sendo o nó central (Centro de Gerência e Operação - CGO) localizado no Departamento de Ciência da Computação da UFMG conforme mostrado na Figura 3. Os roteadores adotados na RIM são da marca Cisco e as linhas de comunicação são fornecidas pela operadora de telefonia local.

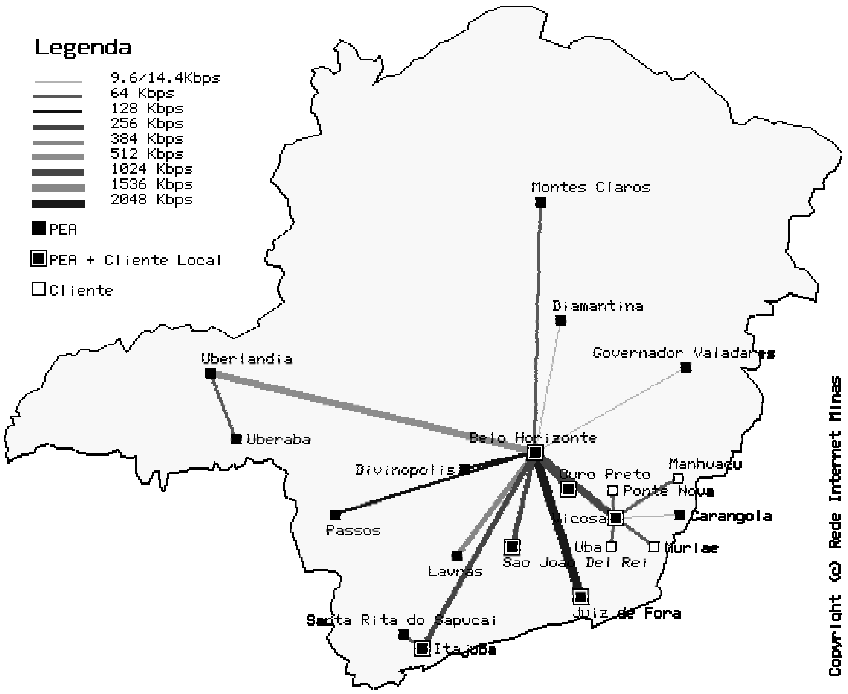


Figura 3 – *Backbone* da Rede Internet Minas

4.1 Descrição da solução adotada

O funcionamento da ferramenta pode ser melhor entendido a partir do diagrama da Figura 4:

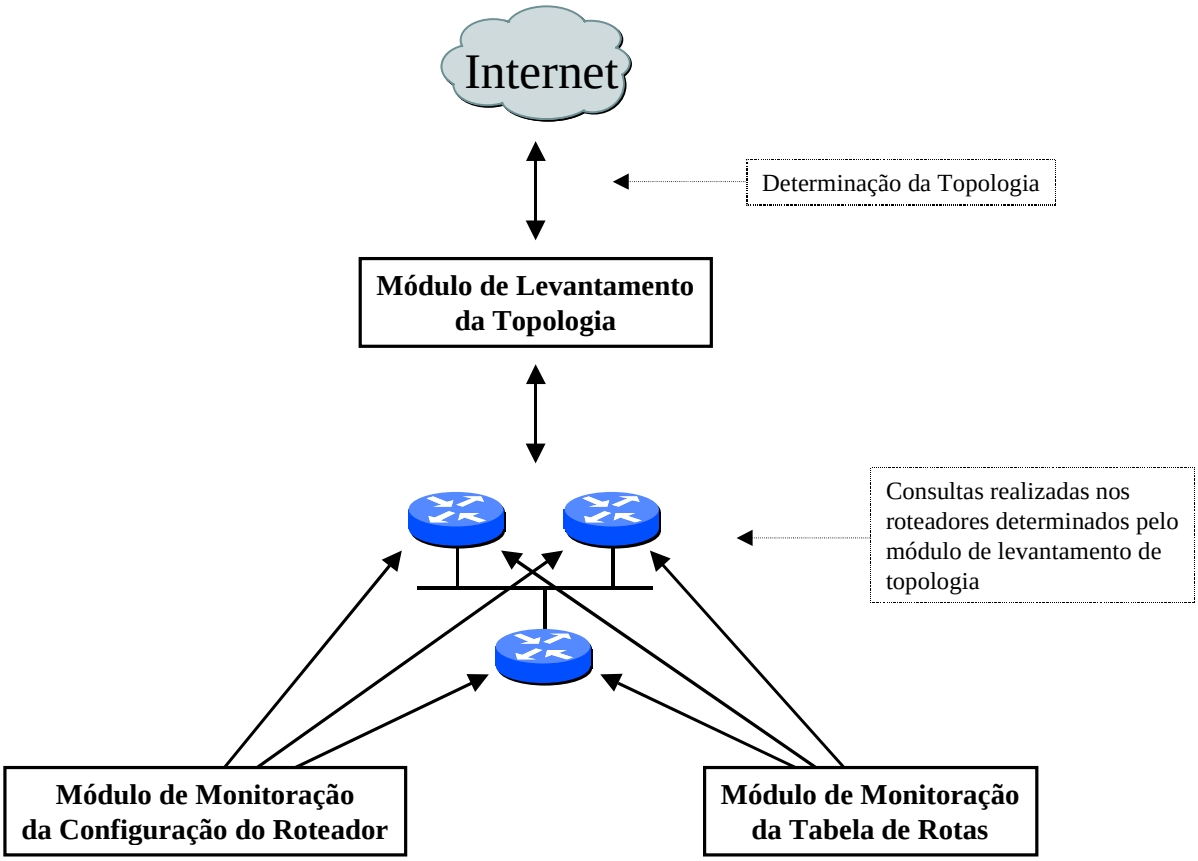


Figura 4 – Estrutura da Ferramenta

4.1.1 Módulo de levantamento da topologia

Este módulo é responsável por determinar a topologia da rede e fornecer os dados necessários para a execução dos demais módulos. Para isto define-se um roteador de origem para a pesquisa da topologia e a profundidade desejada, ou seja, a distância (em roteadores) de uma máquina ao roteador de origem. Determinados os parâmetros iniciais, executa-se o seguinte algoritmo:

Lê os parâmetros iniciais
Percorre as interfaces do roteador inicial determinando as redes ativas no nível 0
Nível = 1;
Enquanto Nível <= Profundidade
    Para cada uma das redes do Nível I – 1 determine os roteadores ativos do Nível I
    Para cada um dos roteadores do Nível I pesquise as interfaces determinando as redes do Nível I
    Nível = Nível + 1
Fim Enquanto

A determinação das redes ativas é feita a partir de consultas a MIB (Management Information Base) SNMP (Simple Network Management Protocol). Para isto, são acessados os endereços contidos na Tabela 1.

Posição	***Conteúdo***
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr	*Endereço IP da interface*
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex	*Interface associada ao IP*
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask	*Máscara de rede da interface*
Interfaces.iftable.ifEntry.ifAdminStatus	*Status administrativo da interface Up 1, Down 2, Test 3*

Tabela 1 – Campos da MIB utilizados para a identificação das redes ativas

A determinação dos roteadores é feita em duas etapas:

- Determinação das máquinas ativas
- Determinação dos roteadores

A determinação das máquinas ativas de uma rede é feita a partir do envio de um *ping* ICMP aos endereços válidos determinados pela máscara e número IP obtidos via SNMP. Para cada um dos endereços cuja resposta for positiva, realizam-se consultas às variáveis descritas na Tabela 2.

Posição	***Conteúdo***
System.sysName	*Nome do dispositivo*
System.sysServices	*Serviços providos pelo dispositivo*
ip.ipForwarding	*Função do equipamento: 1 gateway, 2 não gateway*
Interfaces.ifNumber.0	*Número de interfaces do dispositivo*

Tabela 2 – Campos da MIB utilizados para a identificação de roteadores

Considerou-se nesse trabalho um roteador como sendo um equipamento que responda as requisições SNMP com os seguintes valores:

- O valor contido em system.sysServices deve estar com o bit 2 ativado. Este campo possui um valor numérico cuja decomposição binária indica que o bit da i-ésima posição corresponde a (n+1)-ésima camada do modelo OSI [Stallings, 1993]
- O valor de ip.ipForwarding = 1
- Número de interfaces de rede (interfaces.ifNumber) ≥ 2

Foi definido o conceito de ID para evitar que um roteador com mais de um endereço IP seja classificado incorretamente como vários roteadores independentes ou que um mesmo roteador seja visitado várias vezes durante a determinação da topologia. O ID corresponde a junção entre o campo system.sysName e o endereço IP da sua primeira interface (ip.ipAddrTable.ipAddrEntry.ipAdEntAddr). Finalizado o processo de levantamento da topologia, os demais módulos são executados.

4.1.2 Módulo de monitoração da configuração do roteador

O módulo de monitoração da configuração do roteador tem por objetivos detectar possíveis alterações não autorizadas nas portas dos roteadores, corrigindo-as e reportando-as através de alarmes e relatórios aos administradores da rede. Este módulo é subdividido em duas camadas. A primeira camada ou substrato é responsável pela monitoração dos

roteadores. A segunda camada ou superimposição é responsável pela tomada de decisões caso uma alteração seja detectada na configuração do roteador.

O monitoramento das portas do roteador é feito a partir de leituras em intervalos regulares de tempo dos campos da MIB SNMP contidos na Tabela 3. O intervalo entre leituras para este módulo e para o módulo de controle da tabela de rotas foi parametrizado em 10 minutos. Este é um valor que permite controlar todos os aspectos da rede sem gerar um tráfego de gerência significativo.

Posição	***Conteúdo***
interfaces.ifNumber	*Numero de interfaces do dispositivo*
interfaces.ifTable.ifEntry.ifIndex	*Índice da interface*
Interfaces.ifTable.ifEntry.ifDescr	*Descrição da interface*
Interfaces.iftable.ifEntry.ifType	*Tipo da interface*
Interfaces.iftable.ifEntry.ifSpeed	*Velocidade da interface*
Interfaces.iftable.ifEntry.ifAdminStatus	*Status administrativo da interface Up 1, Down 2, Test 3*
ip.ipForwarding	*Função do equipamento: 1 gateway, 2 não gateway*
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr	*Endereço IP da interface*
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex	*Interface associada ao IP*
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask	*Máscara de rede da interface*

Tabela 3 – Campos da MIB utilizados para a monitoração da configuração de um roteador

Quando um dos campos sofre alteração, um alarme é enviado ao administrador reportando as modificações e um *script* de gerência é acionado para retornar a configuração ao valor original. Este processo é uma utilização típica dos conceitos envolvidos em gerência proativa.

O sistema também gera uma página WWW com as seguintes informações: a data e o horário da última verificação e da última alteração na configuração, a configuração atual e a última modificação. Um exemplo desta página pode ser encontrada na Figura 5.

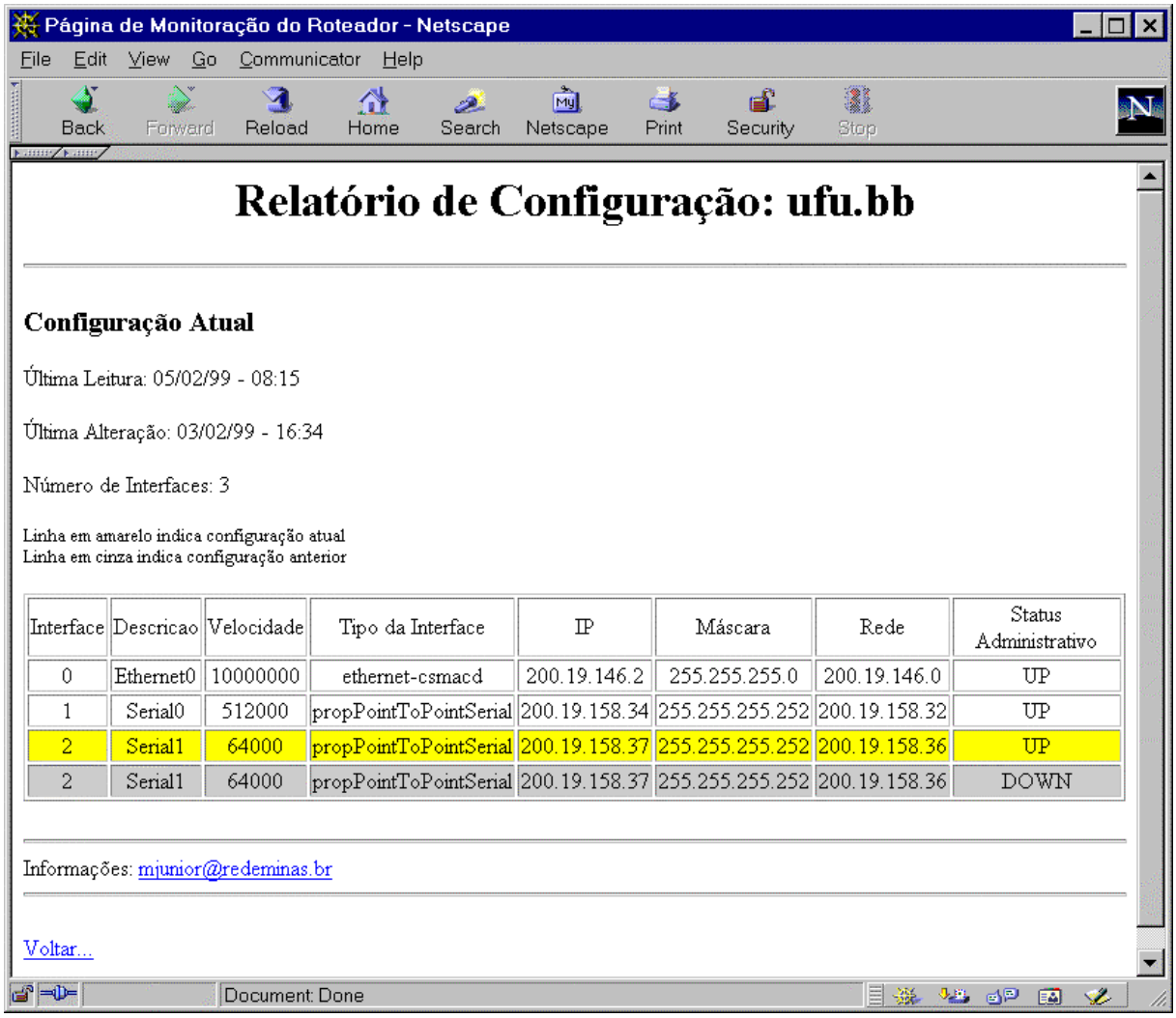


Figura 5 – Tela do módulo de monitoração da configuração dos roteadores

4.1.3 Módulo de monitoração da tabela de rotas

Este módulo tem por objetivo percorrer as tabelas de rotas dos diversos roteadores detectando e eliminando rotas indevidas cuja existência possa comprometer a eficiência e correção do roteamento interno e externo ao *backbone*. Para isto, este módulo também foi subdividido em duas camadas. O substrato executa a leitura da tabela de rotas de cada um dos roteadores comparando o seu conteúdo à base de dados com os endereços IP alocados para cada uma das instituições da RIM. As rotas para endereços não alocados são enviadas para a camada de superimposição que a partir de um sistema baseado em regras elimina da tabela de rotas as rotas indevidas e reporta ao administrador a sua ação. Feito isso, o administrador deve então tomar as providências necessárias para a completa resolução dos possíveis problemas de roteamento.

Para o monitoramento das rotas, os seguintes campos da MIB SNMP são consultados (Tabela 4):

Posição	***Conteúdo***
ip.ipRouteTable.ipRouteEntry.ipRouteDest	*Endereço IP para ser roteado (Rota)*
ip.ipRouteTable.ipRouteEntry.ipRouteNextHop	*Endereço para onde a rota é direcionada*

Tabela 4 – Campos da MIB utilizados para a monitoração da tabela de rotas de um roteador

A Figura 6 apresenta um exemplo de relatório de falhas gerado pelo sistema. Com o objetivo de preservar a segurança e o anonimato da instituição envolvida, o nome e os endereços foram intencionalmente trocados.

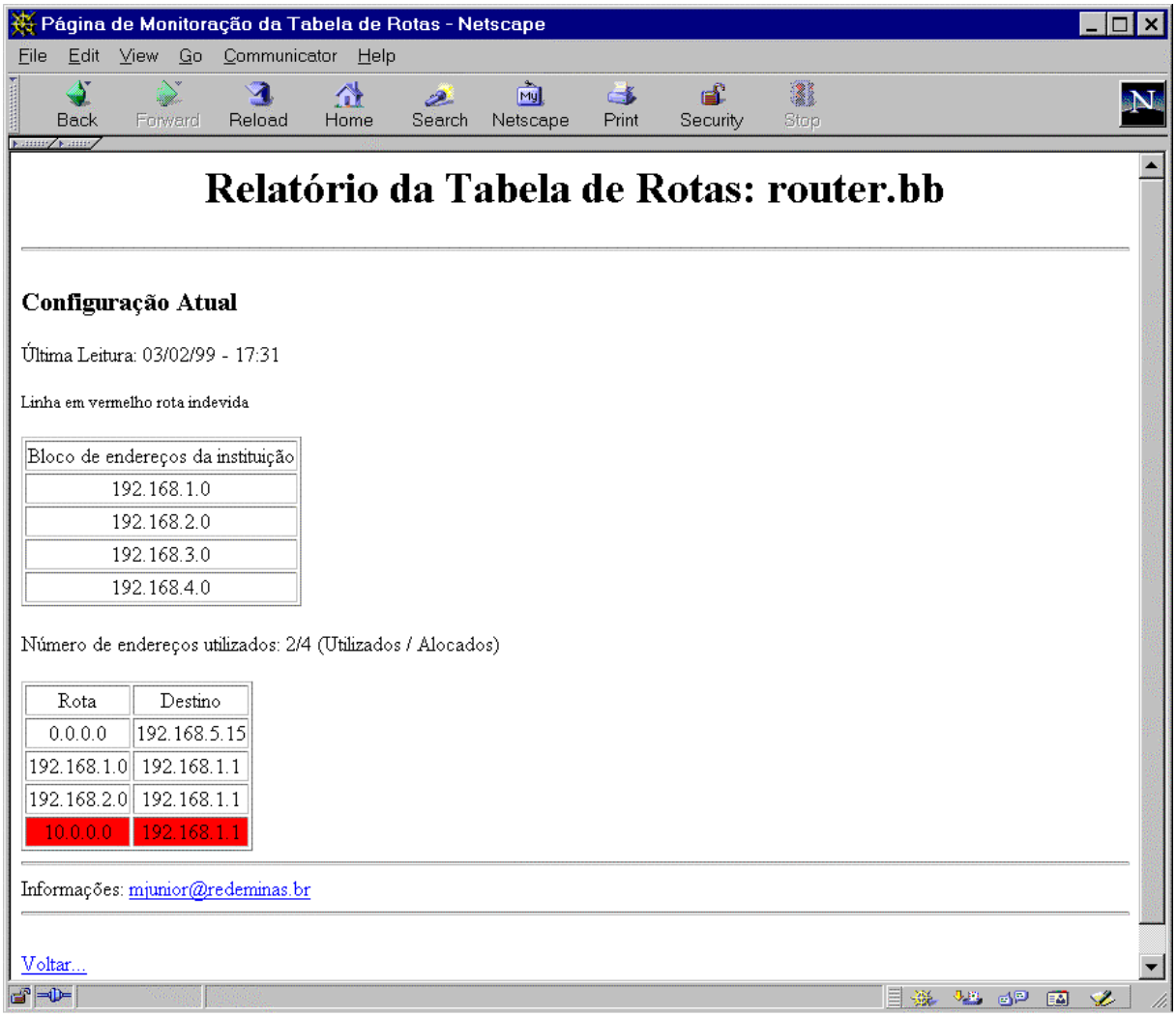


Figura 6 – Tela do módulo de controle da tabela de rotas

5 Resultados obtidos

Nesta seção são descritos os resultados obtidos para o *backbone* da Rede Internet Minas.

5.1 Módulo de levantamento da topologia

A imagem de topologia gerada por este módulo é de fácil interpretação e não apresenta os problemas de identificação presentes no SNM e no Scotty, onde um roteador com mais de um endereço IP aparece replicado para cada um dos endereços (Figura 7).

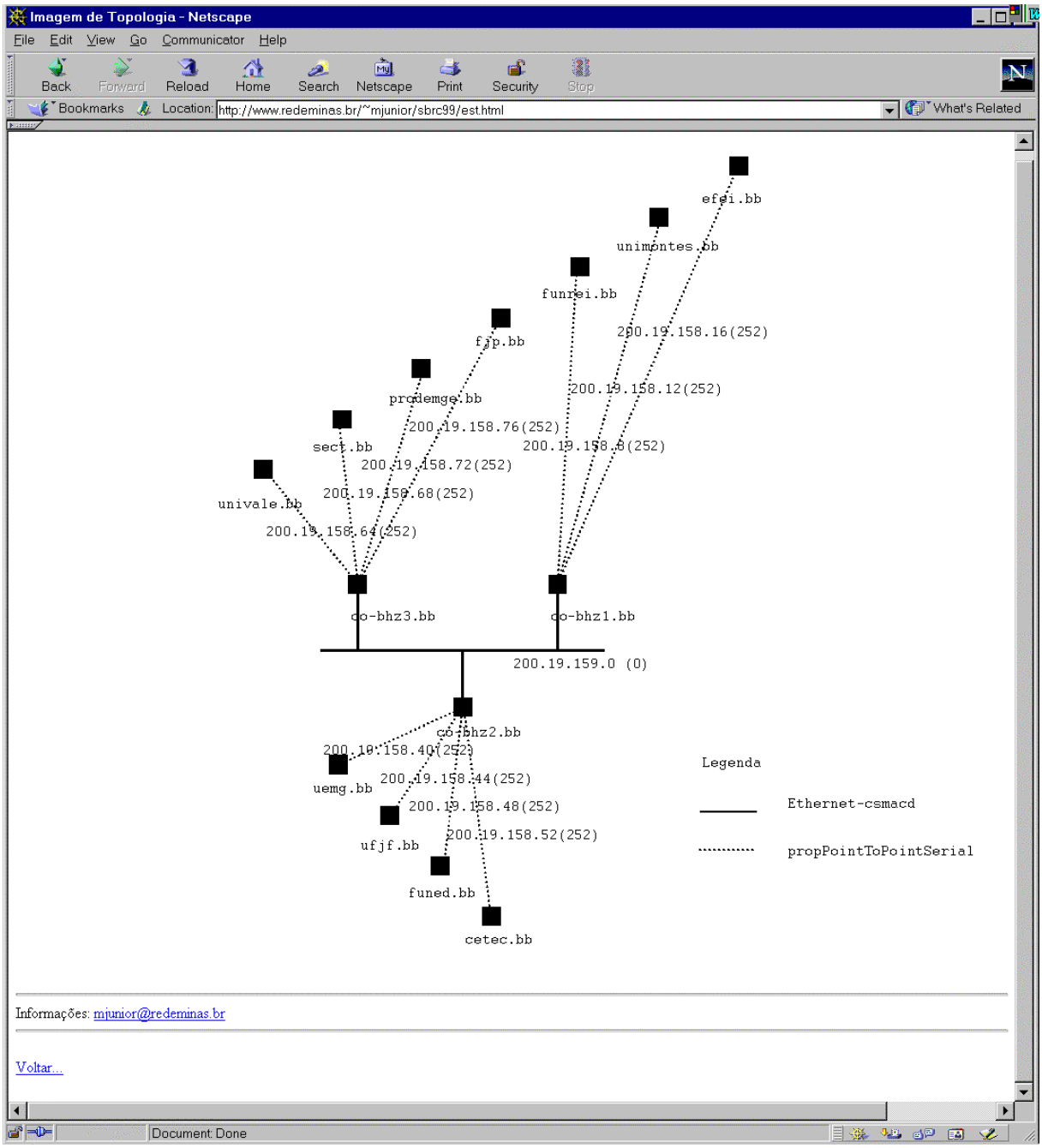


Figura 7 - Imagem de topologia obtida com profundidade 0 para os roteadores da rede ethernet

O processo de descoberta de topologia apresenta os seguintes tempos médios de execução (Tabela 5):

Profundidade	*Tempo de Execução (minutos)*
0	*00:08*
1	*04:10*
2	*35:04*

Tabela 5 – Tempo de processamento durante o levantamento da topologia

Os tempos foram medidos através do aplicativo *time* do sistema operacional. O processamento foi realizado em uma estação de trabalho Sun Sparc Ultra 10, HD IDE 4.3GB, 512MB RAM e sistema operacional Solaris 2.6. O aumento do tempo de execução com a mudança da profundidade é devido ao:

- Crescimento exponencial do número de máquinas ativas no momento em que se acrescenta um nível a estrutura, e
- O tempo necessário para a expiração das requisições SNMP.

O crescimento do número de máquinas está relacionado ao acréscimo das máquinas ligadas às redes em barramento e/ou anel dos diversos roteadores da RIM. Sendo assim, para cada roteador identificado pode-se adicionar até N * 255 máquinas, onde N é o número de interfaces *ethernet* ou *token ring* do equipamento.

Para cada nova máquina ativa executa-se um conjunto mínimo de requisições SNMP para determinação da sua função. Assim sendo, deve-se aguardar a devida resposta ou a expiração da requisição. Como o número de máquinas sem agente SNMP e/ou comunidade conhecida cresce também com o número de máquinas descobertas, deve-se esperar pelo menos M * S segundos, onde M é o número de máquinas sem resposta do agente SNMP e S é o tempo de expiração. No caso da biblioteca utilizada (CMU-SNMP), o tempo é de 20 segundos.

5.2 Módulo de monitoração da configuração do roteador

O curto intervalo de tempo entre leituras dos dados dos roteadores possibilita um controle eficiente da configuração e permite detectar rapidamente alterações não autorizadas. O formato de visualização das informações facilita a verificação das configurações dos equipamentos e auxilia na sua manutenção.

Durante os testes, em um primeiro momento sem o esquema de gerenciamento proativo, foram detectados erros na configuração de alguns roteadores, sendo a maioria relacionada a utilização indevida de máscaras de rede. Um exemplo foi a utilização de máscara de rede 255.255.255.0 em uma rede ponto a ponto. Neste caso, dos 254 números IP disponíveis apenas dois seriam utilizados, sendo desperdiçados os demais. Para este tipo de situação, o ideal é a adoção de uma máscara 255.255.255.252 que subdivide a rede em 62 sub-redes de duas máquinas. Deste modo consegue-se reduzir o desperdício de endereços.

No passo seguinte, com o gerenciamento proativo habilitado, foi possível detectar e corrigir automaticamente as alterações executadas durante a rotina de testes. A rotina de testes consistiu em fazer alterações na configuração das portas. Ao final do processo todas modificações foram devidamente detectadas e corrigidas.

O histórico de alterações possibilita o arquivamento das modificações das configurações e auxilia no retorno a uma configuração antiga caso alguma tomada de decisão tenha sido realizada incorretamente.

5.3 Módulo de monitoração da tabela de rotas

O módulo de monitoração da tabela de rotas possibilitou em um primeiro momento a descoberta de problemas de roteamento no *backbone* da RIM. Foram detectados basicamente dois tipos de falhas:

- Rotas de endereços públicos sendo exportadas internamente no *backbone*, sendo que a sua atuação deveria estar restrita aos domínios da instituição.
- Instituições ligadas a mais de um *backbone* exportando rotas indevidas na RIM. As rotas de outro *backbone* não podem ser exportadas indiscriminadamente sob o risco da instituição se transformar incorretamente em um PIR (Ponto de Interconexão de redes). Uma instituição só pode exportar essas rotas para a RIM se utilizar o protocolo de roteamento BGP4 (Border Gateway Protocol), devendo possuir um bloco CIDR (Classless InterDomain Routing) próprio.

Depois de detectados e corrigidos tais problemas, a ferramenta possibilitou a elaboração de estatísticas relacionadas ao número de endereços IP alocados por uma instituição. Deste modo, conseguiu-se determinar a utilização efetiva de endereços e indicar os locais onde ocorreram excessos na sua alocação.

6 Conclusões e Trabalhos Futuros

Considerando-se as características da ferramenta, os resultados obtidos e as suas inovações em relação aos trabalhos relacionados, pode-se afirmar que a ferramenta representa importante contribuição para o gerenciamento das tabelas de rotas e da configuração de roteadores de um *backbone*.

O controle da configuração dos equipamentos aumentou a segurança e a confiabilidade do *backbone*, já que em um intervalo de no máximo 10 minutos quaisquer alterações não autorizadas na configuração dos equipamentos serão canceladas. Um passo seguinte neste controle será a criação de uma ferramenta para analisar automaticamente a configuração de todo o roteador (filtros, terminais, etc.) a partir de um conjunto de premissas. Neste caso, será implementado um *parser* para executar este processo.

O controle da tabela de rotas possibilitou a eliminação de problemas de roteamento anteriormente não detectados e auxilia na prevenção e detecção de possíveis falhas no *backbone* da RIM. A estatística de utilização dos IPs alocados auxilia no processo de concessão de mais números IPs e na sua utilização racional.

A adoção da interface WWW permite que a ferramenta seja independente da plataforma de acesso e possibilita ainda a sua utilização remota. Esta é uma característica interessante pois a Web tende a se tornar o console típico de aplicações de gerência de redes.

O aumento do tempo necessário para descobrir a topologia dificulta pesquisas com profundidade maior ou igual a três. Pretende-se resolver esse problema com a adoção futura de *threads* para paralelizar a pesquisa.

A adoção do princípio de superimposição apresenta como principais vantagens a independência entre os módulos de gerência tradicional e proativa, a redução da complexidade de implementação, a possibilidade de executar algoritmos distribuídos de

gerenciamento permitindo assim o tratamento da rede como um todo, a facilidade para migrar o código entre diferentes plataformas e a possibilidade de adotar diferentes técnicas de gerência proativa sem profundas alterações no código e na estrutura da ferramenta. Estes aspectos são importantes e serão explorados em trabalhos futuros.

A ferramenta possibilitou solucionar uma série de pequenos problemas no *backbone* da RIM que antes eram atribuídos a problemas de linha, servidores temporariamente inoperantes e que na verdade eram reflexo de problemas de roteamento. Além disso, a ferramenta automatiza a resolução deste tipo de problema que tradicionalmente é feita manualmente e nem sempre com os resultados esperados.

Agradecimentos

Este trabalho foi apoiado em parte pelos convênios FAPEMIG SHA 250/94, TEC 609/96 e CNPq 522618/96-0

Bibliografia

[3Com, 1999] *SuperStack II Switch 1000.* http://www.3com.com/products/dsheets/400324.html. Acessado em janeiro de 1999

[Barbosa, 1996] Valmir C. Barbosa. *An Introduction to Distributed Algorithms*. The MIT Press, 1996.

[Cisco a, 1999] *TrafficDirector Version 4.1*. http://www.cisco.com/warp/public/734/traffdir/tdir_ds.htm. Acessado em janeiro de 1999

[Cisco b, 1999] *Proactive Network Management with Cisco Netsys Connectivity Service Manager*. http://www.cisco.com/warp/public/734/nslms/proac_wp.htm. Acessado em janeiro de 1999

[Chandy et al., 1985] K.M. Chandy and L. Lamport. *Distributed Snapshots: Determining Global States in DistributedSystems*. ACM Transactions on Computer Systems, Volume 3, Number 1, 1985.

[Cruz et al., 1997] Fernando A. S. Cruz, Mirela S. M. A. Notare, Fernando Gauthier, Bernardo G. Riso, Carlos B. Westphall. *Uso de Inteligência Artificial na Implementação de um Sistema de Gerência Pró-ativo para Redes ATM*. XXIII Conferência Latino-americana de informática, 1997.

[Meira et al., 1997] Dilmar M. Meira, José Marcos S. Nogueira. *Métodos e Algoritmos para Correlação de Alarmes em Redes de Telecomunicações.* Anais 15º Simpósio Brasileiro de Redes de Computadores, 1997.

[Grimes et al., 1997] Garry Grimes, Brian P Adley. *Intelligence Agents for Network Fault Diagnosis and Testing.* Integrated Network Management V, 1997.

[Hood et al., 1998] Cynthia S. Hood, Chuanyi Ji. *Intelligent Agents for Fault Detection.* IEEE Internet Computing, Volume 2, Number 2, March April, 1998.

[HP a, 1999] *HP Increases Network Manager Control with New Proactive Networking Solution.* http://www.hp.com. Acessado em janeiro de 1999

[HP b, 1999] *Moving from Reactive to Guaranteed Network Services.* http://www.hp.com. Acessado em janeiro de 1999

[Huitema, 1995] Christian Huitema. *Routing in the Internet*. Prentice Hall, 1995.

[Kätker et al., 1997] S. Kätker, M. Paterok. *Fault Isolation nad Event Correlation for Integrated Fault Management.* Integrated Network Management V, 1997.

[Katzela et al.,1993] I. Katzela, M. Shwartz. *Schemes for Fault Identification in Communication Networks.* IEEE International Conference on Communications, 1993.

[Leinwand, 1996] Allan Leinwand, Karen F. Conroy. *Network Management – A Practical Perspective.* Addison Wesley, 1996.

[Loureiro et al., 1996] Antônio A.F. Loureiro, Osvaldo S.F. de Carvalho. *Testing unstable properties in communication protocols*. Anais 14° Simpósio Brasileiro de Redes de Computadores, 1996.

[Lynch, 1996] Nancy A. Lynch. *Distributed Algorithms*. Morgan Kaufmann Publishers, 1996.

[Moura et al., 1997] Mário L. Moura Júnior, Márcio L. B. Carvalho, Mário F. M. Campos. *Topos – Uma Ferramenta para Levantamento Automático de Topologia*. Anais 15° Simpósio Brasileiro de Redes de Computadores, 1997.

[Rocha et al., 1997] Marco A. Rocha, Carlos B. Westphall. *Proactive Management od Computer Networks Using Artificial Intelligence Agents and Techniques.* Integrated Network Management V, 1997.

[Rose et al, 1995] Marshal T. Rose, Keith McCloghrie. *How To Manage Your Network Using SNMP.* Prentice Hall, 1995.

[Schonwalder, 1993] J. Schonwalder, H. Langendorfer. *How To Keep Track of Your Network Configuration.* Proc. 7th Conference on Large Installation System Administration, 1993.

[Soares et al., 1995] Luiz Fernando G. Soares, Guido Lemos, Sérgio Colcher. *Redes de Computadores: das LANs, MANs e WANs às redes ATM.* 2.ed. rev. e ampliada. Campus, 1995.

[Souza, 1997] João G. M. Souza. *Sistema para Gerenciamento de Redes de Longa Distância.* Dissertação de Mestrado. DCC/UFMG, 1997.

[Sun, 1995] *Sun Net Manager 2.2.3 - Reference Manual.* Sun Microsystems, 1995.

[Snell, 1996] Monica Snell. *Administração baseada na Web.* Lan Times, Volume 2, Número 7, Outubro 1996.

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

[Tanenbaum, 1996] Andrew S. Tanenbaum. *Computer Networks – Third Edition.* Prentice Hall, 1996.

[Waldbusser, 1992] Steven L. Waldbusser. *Exposing the Myths About Autotopology.* The Simple Times, Volume 1, Number 1, 1992.