

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

**UMA METODOLOGIA DE GERÊNCIA DE REDES NA INSTITUIÇÃO FARN
USANDO O PROTOCOLO SNMP**

Monografia apresentada ao curso de
Graduação em Sistemas de Informação da
Faculdade Natalense para o Desenvolvimento
do Rio Grande do Norte, para obtenção da grau
de Bacharelado em Sistemas de Informação.

Vanêssa de Araújo Lima

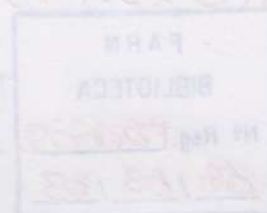
Orientador:

Altair Farias de Rocha Neto

**NATAL
2002**

LIGA DE FACULDADES DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

UMA METODOLOGIA DE GERÊNCIA DE REDES NA INSTITUIÇÃO FARN
USANDO O PROTOCOLO SNMP



Vanêssa de Araújo Lima

Monografia apresentada e aprovada em _____ de _____ de 2002 pela banca
examinadora composta pelos seguintes membros:

**UMA METODOLOGIA DE GERÊNCIA DE REDES NA INSTITUIÇÃO FARN
USANDO O PROTOCOLO SNMP**

Aluizio Ferreira da Rocha Neto

Prof. Aluizio Ferreira da Rocha Neto
Lima, Vanêssa de Araújo

Uma metodologia de Gerência de Redes na Instituição FARN usando o
protocolo SNMP

Prof. Aluizio Ferreira da Rocha Neto

1. Informática - monografia 2. Redes - monografia

Prof. Aluizio Ferreira da Rocha Neto

CDU 004.7

Monografia apresentada ao curso de
Graduação em Sistemas de Informação da
Faculdade Natalense para o Desenvolvimento
do Rio Grande do Norte para obtenção do grau
de Bacharelado em Sistemas de Informação.

Orientador:

Aluizio Ferreira da Rocha Neto

**NATAL
2002**

RB-13.745M



004.7

T 711m

2002

UMA METODOLOGIA DE GERÊNCIA DE REDES NA INSTITUIÇÃO FARN
USANDO O PROTOCOLO SNMP

Lima, Vanêssa de Araújo

Uma metodologia de Gerência de Redes na Instituição FARN usando o
Protocolo SNMP/Vanêssa de Araújo Lima. Natal: FARN, 2002

53 p

Monografia (Graduação em Sistemas de Informação) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

Orientador: Aluizio Ferreira da Rocha Neto

1. Informática – monografia. 2.- Sistemas de Informações –
monografia. 3. Redes – monografia.

RN/FARN/BC

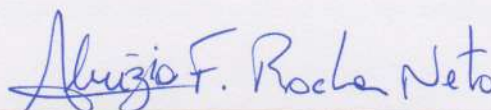
CDU 004.7

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

UMA METODOLOGIA DE GERÊNCIA DE REDES NA INSTITUIÇÃO FARN
USANDO O PROTOCOLO SNMP

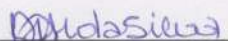
Vanêssa de Araújo Lima

Monografia apresentada e aprovada em ____ de ____ de 2002 pela banca
examinadora composta pelos seguintes membros:



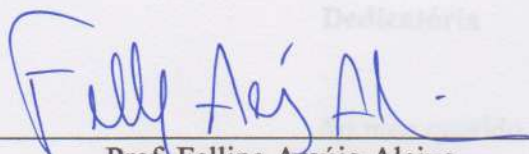
Prof. Aluizio Ferreira da Rocha Neto

Orientador



Prof. Livia Maria Martins da Silva

Examinador



Prof. Felipe Araújo Aleixo

Examinador

Natal, ____ de ____ de 2002.

AGRADECIMENTOS

Os meus sinceros agradecimentos

Primeiramente, a Deus por ter tido a oportunidade de aprofundar meus conhecimentos, e a coragem e força concedida, para o término deste curso.

Ao meu orientador, pelo incentivo, cooperação, disponibilidade e por acreditar que eu ultrapassaria os meus limites.

Aos meus amigos, Ana Angélica e Rodrigo pela força que me deram nos momentos delicados pelos quais passei, pelo companheirismo, amizade sincera e o carinho dedicado durante esta jornada.

Aos primos Eugênio e Christiana, pela contribuição e comprometimento no apoio na realização desta monografia.

A todos os Professores que contribuíram no meu crescimento e desenvolvimento na minha formação acadêmica.

Por fim, a todos aqueles que direta ou indiretamente contribuíram para a minha conclusão deste curso, deixo minha sincera gratidão.

Dedicatória

Ao meu querido pai (*in memoriam*).

AGRADECIMENTOS

Os meus sinceros agradecimentos

Primeiramente, a Deus por ter tido a oportunidade de aumentar meus conhecimentos, e a coragem e força concedida, para o término deste curso.

Ao meu orientador, pelo incentivo, cooperação, disponibilidade e por acreditar que eu transpor os meus limites.

Aos meus amigos, Ana Angélica e Rodrigo pela força que me deram nos momentos delicados pelos quais passei, pelo companheirismo, amizade sincera e o carinho dedicado durante esta jornada.

Aos primos Eugênio e Chistianne, pela contribuição e compreensão no apoio na realização desta monografia.

A todos os Professores que contribuíram no meu crescimento e desenvolvimento na minha formação acadêmica.

Enfim, a todos aqueles que direta ou indiretamente contribuíram para a minha conclusão deste curso, deixo minha sincera gratidão.

SUMÁRIO

CAPÍTULO 1	INTRODUÇÃO	10
1.1	Organização do Trabalho	12
CAPÍTULO 2	SISTEMA DE GERENCIAMENTO	14
2.1	OBJETIVOS DO GERENCIAMENTO	14
2.2	ARQUITETURA FUNCIONAL	15
2.3	POLÍTICA DE GERENCIAMENTO	16
2.4	ÁREAS FUNCIONAIS DE GERENCIAMENTO	17
2.4.1	Gerenciamento de Configuração	17
2.4.2	Gerenciamento de Falhas	18
2.4.3	Gerenciamento de Performance	19
2.4.4	Gerenciamento de Contabilização	20
2.4.5	Gerenciamento de Segurança	20
CAPÍTULO 3	O PROTOCOLO SNMP	21
3.1	SNMP – UM PARADIGMA AGENTE / GERENTE	21
3.2	MIB (<i>MANAGEMENT INFORMATION BASE</i>)	23
3.2.1	Critérios e Filosofia para o Padrão MIB	26
3.2.2	Identificadores de Objetos	27
3.3	OPERAÇÕES SUPORTADAS PELO SNMP - TIPOS DE MENSAGENS	27
3.4	FORMATO DAS MENSAGENS SNMP	28
3.4.1	Transmissão de uma Mensagem SNMP	29
3.4.2	Recebimento de uma Mensagem SNMP	30
3.5	SEGURANÇA NO PROTOCOLO SNMP	31
3.6	MECANISMO DE TRANSPORTE	32
3.7	RMON (<i>Remote Monitoring</i>)	33
3.7.1	Controle de Monitores Remotos	34
CAPÍTULO 4	FERRAMENTAS DE GERENCIAMENTO DE REDE	35
4.1	TIVOLI	35
4.2	MRTG	38
4.2.1	Como Funciona O MRTG	38

4.2.2	O MRTG, SNMP e outras Fontes de Informação	40
CAPÍTULO 5 A REDE FARN		41
5.1	INVENTÁRIO DE SISTEMAS	41
5.1.1	Sistemas Operacionais	41
	Servidor	41
	Sistema Operacional	41
5.2	INVENTÁRIO DE EQUIPAMENTOS	41
5.3	ASPECTOS LÓGICOS	42
5.4	ASPECTOS FÍSICOS	43
CAPÍTULO 6 PROPOSTA DE GERENCIAMENTO PARA A REDE FARN		44
6.1	AUDITORIA PRELIMINAR	44
6.1.1	Ações tomadas após auditoria preliminar	45
6.1.2	Ações tomadas imediatamente	45
6.2	ANÁLISE DE CAPACIDADE	45
6.3	PREDIÇÃO E DEMANDA FUTURA	46
6.4	MONITORAMENTO SISTEMÁTICO	46
6.5	FERRAMENTAS UTILIZADAS	46
CAPÍTULO 7 CONCLUSÃO		49
REFERÊNCIA BIBLIOGRÁFICA		50
BIBLIOGRAFIA CONSULTADA		51

ÍNDICE DE FIGURAS

Figura 1: Níveis de Funcionalidade	15
Figura 2: Gerenciamento de Falhas	19
Figura 3: Paradigma Gerente / Agente.....	23
Figura 4: Árvore de organização das informações de gerência.....	25
Figura 5: Composição da mensagem SNMP.....	29
Figura 6: Tivoli: Exemplos de utilização. (a) Análise de tráfego; (b) Pequena rede apresentada no NetView	38
Figura 7: Gráficos de monitoramento diário e semanal gerados pelo MRTG	39
Figura 8: Diagrama do núcleo da Rede FARN.....	Erro! Indicador não definido.
Figura 9: MRTG monitorando o acesso da FARN à Internet	47

RESUMO

Este trabalho apresenta um estudo abordando os paradigmas de gerenciamento de redes, sua importância, conceitos e formas de realizar este gerenciamento.

É feito também um estudo sobre o protocolo SNMP, mais importante protocolo utilizado nas atividades de gerenciamento. São apresentadas duas ferramentas largamente utilizadas para suportar esta monitoria, o Tivoli e o MRTG.

Finalmente, é apresentada uma proposta de utilização do protocolo SNMP, juntamente com uma ferramenta, para auxiliar no monitoramento e controle da rede da FARN a fim de maximizar a utilização dos recursos.

ABSTRACT

This work presents a survey of Network Management paradigms, concepts and its importance. It is studied in details the SNMP protocol, the main protocol for Network Management activity. Tools like Tivoli and MRTG are also presented.

Finally, it is presented a proposal of network management good practices using SNMP for the FARN's network.

CAPÍTULO 1 INTRODUÇÃO

O número e o tamanho das redes de computadores têm crescido a uma taxa exponencial. Elas deixaram de ser pequenas e separadas e passaram a ser grandes e interconectadas.

A rede de computadores da Faculdade Natalense para o desenvolvimento do Rio Grande do Norte (FARN) não foge deste contexto. Objetivo de análise desta monografia, é apresentar uma política de gerenciamento pró-ativa da rede FARN, incluindo análise de ferramentas, mecanismos de garantir conectividade 24x7 (24 horas por dia, 7 dias por semana), técnicas de detecção de falhas e administração remota de equipamentos, a fim de mantê-la com o menor nível de interrupção possível, é o principal objetivo deste trabalho.

Gerenciamento de rede está associado ao controle de atividades e ao monitoramento do uso e recursos de uma rede de dados, a fim de maximizar sua eficiência e produtividade (TANENBAUM, 1997). Para que isso aconteça é importante; monitorar e manter equipamentos de interconectividade de diferentes fabricantes, além de várias plataformas de computadores e programas utilizados. São definidas cinco áreas de gerenciamento de rede: gerenciamento de configuração, de falhas, de performance, de contabilização e de segurança.

A **gerência de configuração** é o processo de iniciação, fase de verificação, é a manutenção e monitoração da estrutura física e lógica de uma rede. O que permite a detectar erros, se não houver, a rede entra em fase operacional.

A **gerência de falhas** detecta as irregularidades. Os sistemas com problemas devem ser identificados, isolados e consertados ou substituídos.

A **gerência de performance** avalia o comportamento dos recursos gerenciados e dos novos sistemas que estão sendo adicionados para viabilizar o crescimento da rede quando se constata a necessidade de mais recursos para atender o tráfego.

A **gerência de contabilização** provê registro sistemático dos acessos aos recursos da rede permite efetuar a contabilização e análise de tendências.

A **gerência de segurança** é o aspecto essencial, que é o controle de acesso, deve ser constantemente efetuado para evitar que os recursos da rede sejam utilizados indevidamente.

A necessidade de um protocolo para o gerenciamento de uma rede é primordial.

Conforme COMER (2002), a primeira tecnologia em protocolo utilizado foi o *Simple Network Management Protocol*, que surgiu como resposta aos problemas de comunicação entre diferentes tipos de rede. Seu objetivo inicial era o de ser uma solução temporária até que uma melhor proposta se tornasse disponível, o que nunca aconteceu. O SNMP tornou-se, então, um padrão para redes TCP/IP. Seu funcionamento baseia-se na troca de mensagens (PDUs – *Protocol Data Unit*) entre a estação de gerenciamento (**gerentes**) e os equipamentos gerenciados (**agentes**).

Portanto, se um administrador de rede quer saber, por exemplo, se uma máquina conectada à rede está ativa, ele pode usar o SNMP para enviar uma mensagem de leitura àquele terminal. Se o terminal estiver ativo, o administrador recebe de volta uma mensagem com o seu valor significando “sim, o terminal está ativo”. Caso contrário, ele recebe uma mensagem de notificação que o avisa deste fato.

As mensagens podem ser de leitura, alteração, resposta ou notificação. Os dados de informação sobre todos os elementos gerenciáveis da rede são armazenados em um banco de dados chamado MIB (*Management Information Base*). É essa base de informação que é acessada pelas estações de gerenciamento através das mensagens.

Quando uma estação de gerenciamento monitora um dispositivo na rede, ela deve periodicamente pesquisá-lo para descobrir seu *status*. Para permitir que o SNMP monitore dispositivos remotos com mais eficiência, diminuindo a carga do tráfego gerado pelas pesquisas, os agentes nos dispositivos devem ser providos com MIB RMON. A MIB RMON é um conjunto de dados de estatísticas, análises e diagnósticos, coletados a partir do monitoramento de cada *interface* dos dispositivos configurados, ou seja, um dispositivo na rede pode ser configurado para monitorar outros dispositivos, entrando em contato com a estação de gerenciamento somente quando os dispositivos monitorados param de se comunicar ou reiniciam a sua comunicação.

Portanto, os agentes funcionam como uma espécie de monitores em cada subrede, que realizam detecção de problemas, relatórios, controle de tráfego, captura e análise de pacotes, etc. Através destes dados, alarmes podem ser configurados, isto é, se um dado limite definido pelo administrador é ultrapassado, a estação de gerenciamento deve ser notificada e uma ação apropriada pode ser disparada.

O RMON, enfim, é um eficiente meio de monitoração remota de equipamentos, com grande utilidade no gerenciamento de redes.

1.1 Organização do Trabalho

São apresentadas a seguir informações organizadas que levam a mostrar conceitos de gerenciamento, descrição dos recursos da rede da FARN, contextualização destes recursos no ambiente de gerenciamento e finalmente recomendações de como otimizar este gerenciamento.

No **Capítulo 2** serão apresentados os principais conceitos envolvidos na atividade de gerenciamento de redes. Definições, classificações, diferentes ambientes, principais desafios no gerenciamento, técnicas de abordagem de problemas.

No **Capítulo 3** é feita uma análise mais profunda do protocolo SNMP e sua importância para o contexto do gerenciamento de redes. São apresentados os conceitos, estrutura do protocolo e seu funcionamento. São apresentados também tópicos sobre segurança, performance e principais aplicações.

O **Capítulo 4** apresenta algumas ferramentas de monitoramento e gerenciamento de redes. São apresentadas as principais características, interfaces e aplicações.

A rede da FARN é apresentada no **Capítulo 5**. É apresentado o projeto da rede instalada e o inventário dos recursos.

No **Capítulo 6** são feitas uma análise e recomendações de procedimentos de gerenciamento na rede da FARN.

Finalmente, o **Capítulo 7** apresenta uma conclusão do referido trabalho onde são ressaltados os resultados obtidos, assim como sugestões para trabalhos futuros.

Sistema de gerenciamento é um conjunto de ferramentas que tem como objetivo prover formas de automatizar (executar em computadores) funções de gerenciamento.

Em outras palavras, um sistema de gerenciamento deve oferecer facilidades de atuação nas cinco áreas funcionais de gestão, através da aplicação de uma política de gerenciamento.

Este capítulo apresenta uma visão geral sobre a arquitetura funcional de um sistema de gerenciamento, além dos tipos de política de gestão e conceitos gerais sobre as cinco áreas de atuação de gerenciamento: configuração, falhas, performance, contabilidade e segurança.

2.1 OBJETIVOS DO GERENCIAMENTO

Por que é necessário o Gerenciamento de Redes? Por que não se pode apenas montar uma rede e colocá-la para funcionar? A medida que aumenta a necessidade de se organizar as informações em rede aumenta também o custo de sua manutenção. Por isso é necessário limitar o aumento do custo de operação quando há o aumento do uso das redes. Investimentos são feitos principalmente em:

- **Disponibilidade** - Poucos minutos de inatividade são suficientes para causar prejuízos milionários. É inevitável que uma rede para SNMP possa ser utilizada para detectar e prevenir situações de grande potencial de risco através do monitoramento sistemático.
- **Performance** - Apenas manter uma rede operando não é suficiente para atender às necessidades de um usuário. Toda rede precisa oferecer o máximo da Qualidade do Serviço (QoS) ou qualidade de transmissão. SNMP ajuda a prevenir situações gerando histórico de performance.
- **Redução do Custo de Propriedade** - O custo de manutenção de uma rede pode ser várias vezes superior ao custo de aquisição dos equipamentos se não forem adotadas

CAPÍTULO 2 SISTEMA DE GERENCIAMENTO

Sistema de gerenciamento é um conjunto de ferramentas que tem como objetivo prover formas de automatizar (executar em computador) funções de gerenciamento.

Em outras palavras, um sistema de gerenciamento deve oferecer facilidades de atuação nas cinco áreas funcionais de gerência, através da aplicação de uma política de gerenciamento.

Este capítulo apresenta uma visão geral sobre a arquitetura funcional de um sistema de gerenciamento, além dos tipos de política de gerência e conceitos gerais sobre as cinco áreas de atuação de gerenciamento: configuração, falhas, performance, contabilização e segurança.

2.1 OBJETIVOS DO GERENCIAMENTO

Por que é necessário o Gerenciamento de Redes? Por que não se pode apenas montar uma rede e colocá-la para funcionar? À medida que aumenta a necessidade de se organizar as informações em rede aumenta também o custo de sua manutenção. Por isso é necessário limitar o aumento do custo de operação quando há o aumento do uso das redes. Investimentos são feitos principalmente em:

- Disponibilidade – Poucos minutos ou até segundos de parada de certas redes podem gerar prejuízos milionários. É inevitável que uma rede pare. SNMP pode ser utilizado para detectar e prevenir situações de grande potencial de risco através de monitoramento sistemático
- Performance - Apenas manter uma rede operando não é suficiente para atender às necessidades de seu uso. Toda rede precisa oferecer o mínimo de Qualidade de Serviço (QoS) ou qualidade de transmissão. SNMP ajuda a prever futuros gargalos baseando-se em relatórios de performance.
- Redução do Custo de Propriedade – O custo de manutenção de uma rede pode ser várias vezes superior ao custo de aquisição dos equipamentos se não forem utilizadas

ferramentas e metodologias adequadas para sua operação. Profissionais de “Suporte de Redes” precisam ser extremamente especializados e, por isso, encarecem muito este custo. Ferramentas que viabilizem o gerenciamento Proativo e implementem as várias práticas de gerenciamento podem reduzir drasticamente este custo.

2.2 ARQUITETURA FUNCIONAL

Sistema de gerenciamento de rede tem três níveis básicos de funcionalidade, onde cada nível tem um conjunto de tarefas definidas para prover, formatar ou coletar dados necessários ao gerenciamento de objetos. A Figura 1 ilustra esses níveis de funcionalidade.

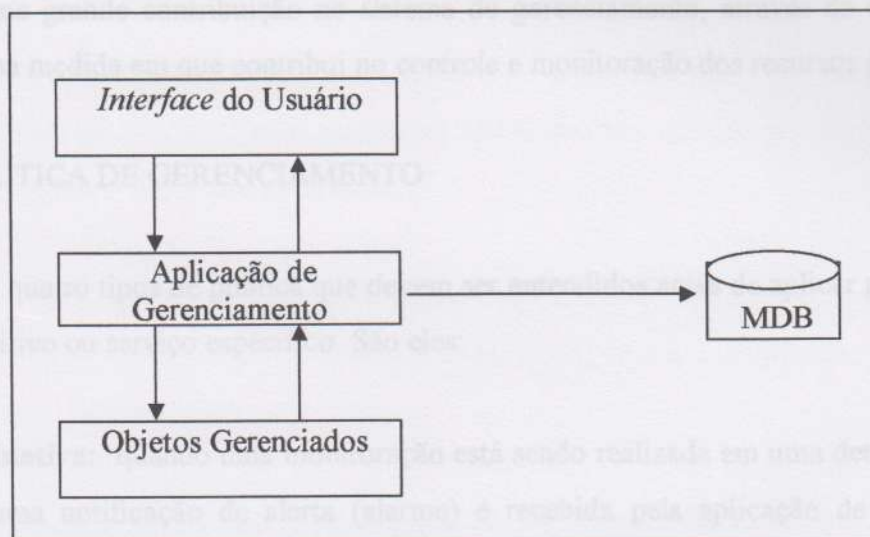


Figura 1: Níveis de Funcionalidade

Um objeto gerenciado representa um recurso que pode ser um servidor, estação de trabalho, modem, *gateway*, concentrador, etc. Cada objeto pode ser visto como uma coleção de variáveis que podem ser lidas ou alteradas.

A aplicação de gerenciamento deve tornar o trabalho de gerência mais fácil e mais rápido. A informação associada com o problema ou sintoma deve significar alguma coisa para o pessoal de suporte. Se um problema é detectado, eles devem saber a que área específica o problema pertence e o que fazer para começar o processo de isolamento. Outras pessoas da instituição devem saber que um técnico específico está verificando o problema e como ele pode estar afetando outras áreas.

Além disso, o pessoal de *HelpDesk*, se houver, deve saber o que está acontecendo e quem está trabalhando no sentido de contornar as falhas.

Um ponto importante nesta arquitetura é a *interface* do usuário, pois se a informação coletada dos objetos gerenciados através da aplicação de gerenciamento não puder ser distribuída, isto é, ser informada às pessoas responsáveis, o propósito geral de um sistema de gerenciamento de rede falhou na sua implementação. Os dados não significam nada se eles não são usados para tomadas de decisões que otimizem os sistemas e as funções.

Neste contexto, a padronização do gerenciamento, baseado no modelo gerente-agente, na interação usando um protocolo de gerenciamento e na noção de objetos gerenciados, fornece uma grande contribuição no sistema de gerenciamento, através de uma política de gerência, na medida em que contribui no controle e monitoração dos recursos gerenciados.

2.3 POLÍTICA DE GERENCIAMENTO

Há quatro tipos de política que devem ser entendidos antes de aplicar gerenciamento a um dispositivo ou serviço específico. São eles:

- **Inativa:** quando uma monitoração está sendo realizada em uma determinada área e uma notificação de alerta (alarme) é recebida pela aplicação de gerenciamento, devendo ser ignorada.

Ex.: uma pessoa é responsável pelo gerenciamento dos equipamentos da 3Com e outra, pelo gerenciamento de servidores. Se a primeira pessoa receber um alarme proveniente de um servidor, ela deve ignorá-lo, pois esta área não é de sua competência. Não esquecendo que o inativo para uma, pode não ser para a outra.

- **Reativa:** quando é detectado um problema em uma área que não está sendo monitorada e uma reação é realizada como consequência, para que o problema seja sanado.

Ex.: o que ocorre atualmente em redes sem Gerenciamento : nada é monitorado e quando se toma conhecimento de um problema, esforços são despendidos na tentativa de isolar e corrigir a falha para que a rede volte à operação normal.

- **Interativa:** quando uma monitoração está sendo realizada e interativamente se deve trabalhar no sentido de eliminar os motivos causadores da geração de um alarme, realizando o isolamento e encontrando a causa raiz.

Ex.: um alarme é recebido avisando que o percentual de utilização de uma determinada porta de um *switch* ultrapassou um limite preestabelecido. A partir daí, procurar-se-á a causa geradora do problema para que ele seja corrigido.

- **Pró-ativa:** quando uma monitoração está sendo realizada, um alarme é recebido e processos de restauração automática são realizados, quando possível, para minimizar o tempo de interrupção da rede.

Ex.: considere o mesmo problema do caso anterior, entretanto, quando o alarme é gerado, uma desativação automática da porta que causou a notificação é realizada.

Definir uma política interativa e, principalmente, pró-ativa de gerenciamento de rede é necessário na medida em que visa a controlar os recursos da instituição, acompanhar a evolução da rede, aprimorar o serviço, balancear as necessidades, reduzir o tempo de interrupção e controlar os custos, onde um dos principais problemas enfrentados é o número crescente de equipamentos, além da variedade de fornecedores.

2.4 ÁREAS FUNCIONAIS DE GERENCIAMENTO

As seções seguintes apresentam conceitos gerais sobre as cinco áreas funcionais de gerenciamento: configuração, falhas, performance, contabilização e segurança.

2.4.1 Gerenciamento de Configuração

Gerenciamento de configuração é, provavelmente, a parte mais importante do gerenciamento da rede, pois não se pode gerenciá-la apropriadamente sem que se possa gerenciar a sua configuração. Mudanças, adições e remoções na rede precisam ser

coordenadas com o pessoal do sistema de gerenciamento. Atualização dinâmica da configuração precisa ser acompanhada periodicamente para garantir que ela seja conhecida.

O gerenciamento de configuração consiste basicamente nos seguintes pontos:

- Permitir que os dispositivos possam ser configurados para atuar de modos diferentes;
- Iniciar parâmetros de configuração e eventualmente alterá-los;
- Permitir que novos componentes possam ser adicionados, mantendo o registro atualizado;
- Manter atualizadas as ligações (físicas e lógicas) entre os componentes;

2.4.2 Gerenciamento de Falhas

Gerenciamento de falhas é a detecção de um problema, o isolamento da falha e a sua correção, para que a rede possa voltar à operação normal. Trata-se de uma das áreas mais importantes na Rede FARN e consiste mais detalhadamente em:

- Determinar com exatidão a localização do problema;
- Isolar o resto da rede do segmento problemático a fim de que ela possa continuar funcionando;
- Reconfigurar ou modificar a rede de modo a minimizar o impacto operacional sem o componente com falhas;
- Consertar ou substituir o componente defeituoso para que a rede possa voltar a funcionar normalmente;
- Registrar, acompanhar e eliminar os fatores que impedem a efetiva comunicação;
- Acionar serviço de manutenção, monitorando prazos de atendimento e realizando testes de aceitação.

A Figura 2 ilustra esses passos:

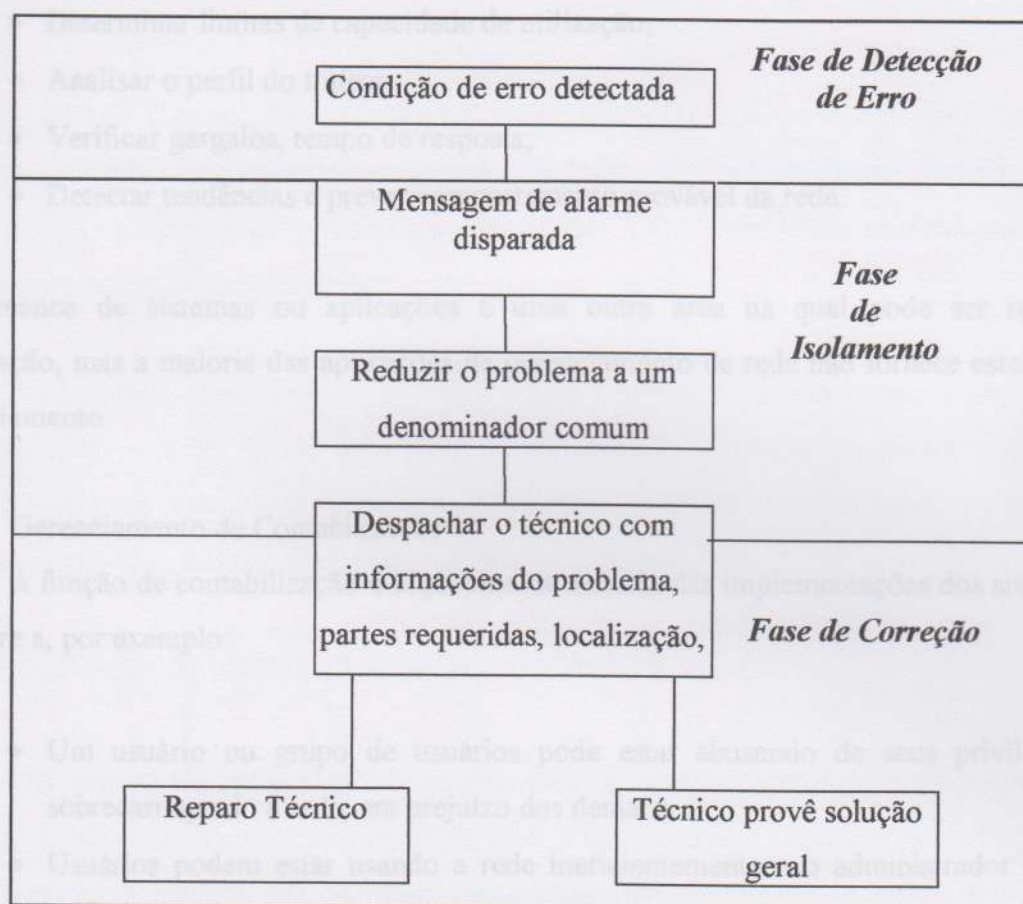


Figura 2: Gerenciamento de Falhas

A maioria dos sistemas pesquisa os objetos gerenciados em busca de condições de erro e ilustram o problema em um formato gráfico ou em uma mensagem textual. Muitas destas mensagens são definidas pelo gerente do sistema que configura a pesquisa na aplicação de gerenciamento de rede, além dos tipos de pesquisa pré-definidos, cujo intervalo pode ser configurado pelo gerente.

2.4.3 Gerenciamento de Performance

Gerenciamento de performance está mais relacionado com a monitoração de dados estatísticos que representam a eficiência com que a rede está operando. É através desta monitoração que se pode avaliar se a rede precisa ou não de mais recursos ou de uma reconfiguração para funcionar a contento.

O seu gerenciamento consiste em:

- Monitorar e controlar os recursos da rede;

- Estabelecer padrão de normalidade;
- Determinar limites de capacidade de utilização;
- Analisar o perfil do tráfego;
- Verificar gargalos, tempo de resposta;
- Detectar tendências e prever comportamento provável da rede.

Performance de sistemas ou aplicações é uma outra área na qual pode ser realizada otimização, mas a maioria das aplicações de gerenciamento de rede não fornece este tipo de gerenciamento.

2.4.4 Gerenciamento de Contabilização

A função de contabilização é esquecida na maioria das implementações dos sistemas e se refere a, por exemplo:

- Um usuário ou grupo de usuários pode estar abusando de seus privilégios e sobrecarregando a rede, em prejuízo dos demais;
- Usuários podem estar usando a rede ineficientemente e o administrador da rede pode auxiliar a alterar procedimentos que melhorem a performance;
- Conhecendo a atividade dos usuários com suficiente detalhamento, a gerência de rede tem mais condições de planejar o seu crescimento;
- Manter o controle sobre o acesso e o uso da rede;
- Quem acessa que recursos? Com que frequência?

2.4.5 Gerenciamento de Segurança

Gerenciamento de segurança consiste em procurar meios de evitar que usuários não autorizados tenham acesso às informações de gerenciamento e possam alterá-las, além de procurar evitar que dispositivos não autorizados se conectem à rede.

Gerenciamento de segurança deve prover:

- Monitoração e controle do acesso aos recursos da rede e às informações;
- Coleta, armazenamento e exame de registros de auditoria e *logs* de segurança.

CAPÍTULO 3 O PROTOCOLO SNMP

O SNMP (*Simple Network Management Protocol*) é o protocolo desenvolvido e recomendado para o gerenciamento de redes TCP/IP. Definido ao nível de aplicação, o SNMP utiliza os serviços do protocolo de transporte UDP (*User Datagram Protocol*) para a troca de mensagens através da rede.

Desde que foi desenvolvido em 1988, o SNMP tem se tornado o padrão de fato para o gerenciamento de rede. Ele é extensível, o que permite a adição de novas funções de gerenciamento aos produtos já existentes. Além disso, o SNMP também separa a arquitetura de gerenciamento da arquitetura de dispositivos de hardware.

3.1 SNMP – UM PARADIGMA AGENTE / GERENTE

Um sistema de gerenciamento de rede contém dois elementos primários: gerentes e agentes. O gerente é o *console* através do qual o administrador de rede realiza funções de gerenciamento, e agentes são entidades que acessam os dispositivos a serem gerenciados. *Bridges, hubs*, roteadores ou servidores de rede são exemplos de dispositivos gerenciados que contém **objetos gerenciáveis**. Estes podem ser informações sobre o hardware, parâmetros de configuração, estatísticas de performance, entre outros.

Os agentes coletam junto aos objetos gerenciados as informações relevantes para o gerenciamento. O gerente consulta os agentes e processa as informações recolhidas com o objetivo de detectar a presença de falhas no funcionamento da rede. Isto permite que sejam tomadas providências que contornem os problemas decorrentes destas falhas.

As informações sobre os objetos gerenciados são armazenadas em um banco de dados chamado MIB (*Management Information Base*). O funcionamento do SNMP baseia-se na troca de mensagens entre o gerente e o agente. É através desta troca que o gerente solicita ao agente a informações ou modificações de um objeto na MIB. Nessas trocas de informações são aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede.

O protocolo SNMP define o formato e a ordem que deve ser seguida no intercâmbio de informações de gerenciamento.

A Figura 3 apresenta os componentes básicos de uma arquitetura de gerência baseada no paradigma Gerente / Agente, que é estruturada nos seguintes elementos:

- Gerente Humano: operador do sistema de gerência.
- Gerente: responsável pela coleta das informações, oferecendo ao gerente humano ferramentas de monitoramento e controle dos dispositivos gerenciados.
- Agente: componente responsável pela interação direta com o dispositivo gerenciado, ou seja, a coleta de informações armazenadas na base de informações gerenciais e a execução das requisições enviadas pelo gerente.
- Protocolo de Gerenciamento: definição da sintaxe e semântica dos serviços e unidades de informação (*Protocol Data Units*), trocadas entre duas entidades, normalmente gerente e agente, caracterizando o protocolo da camada, cuja aplicação é responsável pela comunicação.
- Base de Informações Gerenciais: repositório das informações relevantes ao processo de gerência manipulado remotamente pelo gerente através do agente.

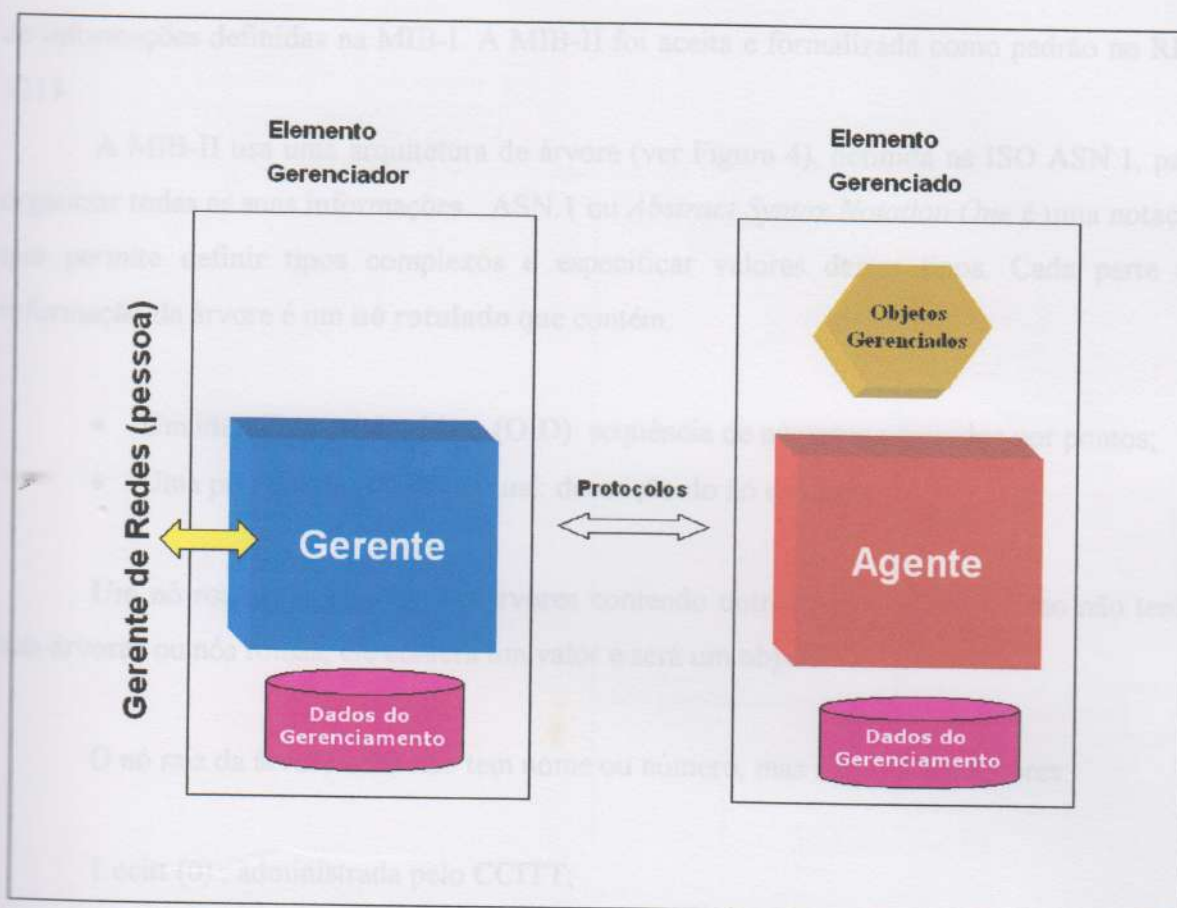


Figura 3: Paradigma Gerente / Agente

3.2 MIB (MANAGEMENT INFORMATION BASE)

MIB é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede. Neste contexto, objeto gerenciado é a visão abstrata de um recurso real do sistema. Todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas de dados resultantes são os objetos gerenciados. Estes podem ter permissões para serem lidos ou alterados, onde cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso.

O documento RFC 1066 (*Request for Comments*) apresentou a primeira versão da MIB para uso com o protocolo TCP/IP, a MIB-I. Conforme MAURO (2001), este documento explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas no protocolo TCP/IP. O RFC 1066 foi aceito pela IAB (*Internet Activities Board*) como padrão no RFC 1156. O RFC 1158 propôs uma segunda MIB, a MIB-II, que expandiu a base

de informações definidas na MIB-I. A MIB-II foi aceita e formalizada como padrão no RFC 1213.

A MIB-II usa uma arquitetura de árvore (ver Figura 4), definida na ISO ASN.1, para organizar todas as suas informações. ASN.1 ou *Abstract Syntax Notation One* é uma notação que permite definir tipos complexos e especificar valores destes tipos. Cada parte da informação da árvore é um **nó rotulado** que contém:

- Um identificador de objeto (OID): sequência de números separados por pontos;
- Uma pequena descrição textual: descrição do nó rotulado.

Um nó rotulado pode ter sub-árvores contendo outros nós rotulados. Caso não tenha sub-árvores ou nós folhas, ele conterá um valor e será um **objeto**.

O nó raiz da árvore MIB não tem nome ou número, mas tem três subárvores:

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

Sob o nó iso (1) estão outras sub-árvores, como é o caso da sub-árvore org (3), definida pela ISO para conter outras organizações. Uma das organizações que está sob a sub-árvore org (3) é o Departamento de Defesa dos EUA (DOD), no nó dod (6). A Internet (1) está sob o dod (6), e possui quatro sub-árvores:

- directory (1): contém informações sobre o serviço de diretórios OSI(X.500);
- mgmt (2): contém informações de gerenciamento. É sob esta sub-árvore que está o nó da mibII, com o identificador de objeto 1.3.6.1.2.1;
- experimental (3): contém os objetos que ainda estão sendo pesquisados pela IAB;
- private (4): contém objetos definidos por outras organizações.

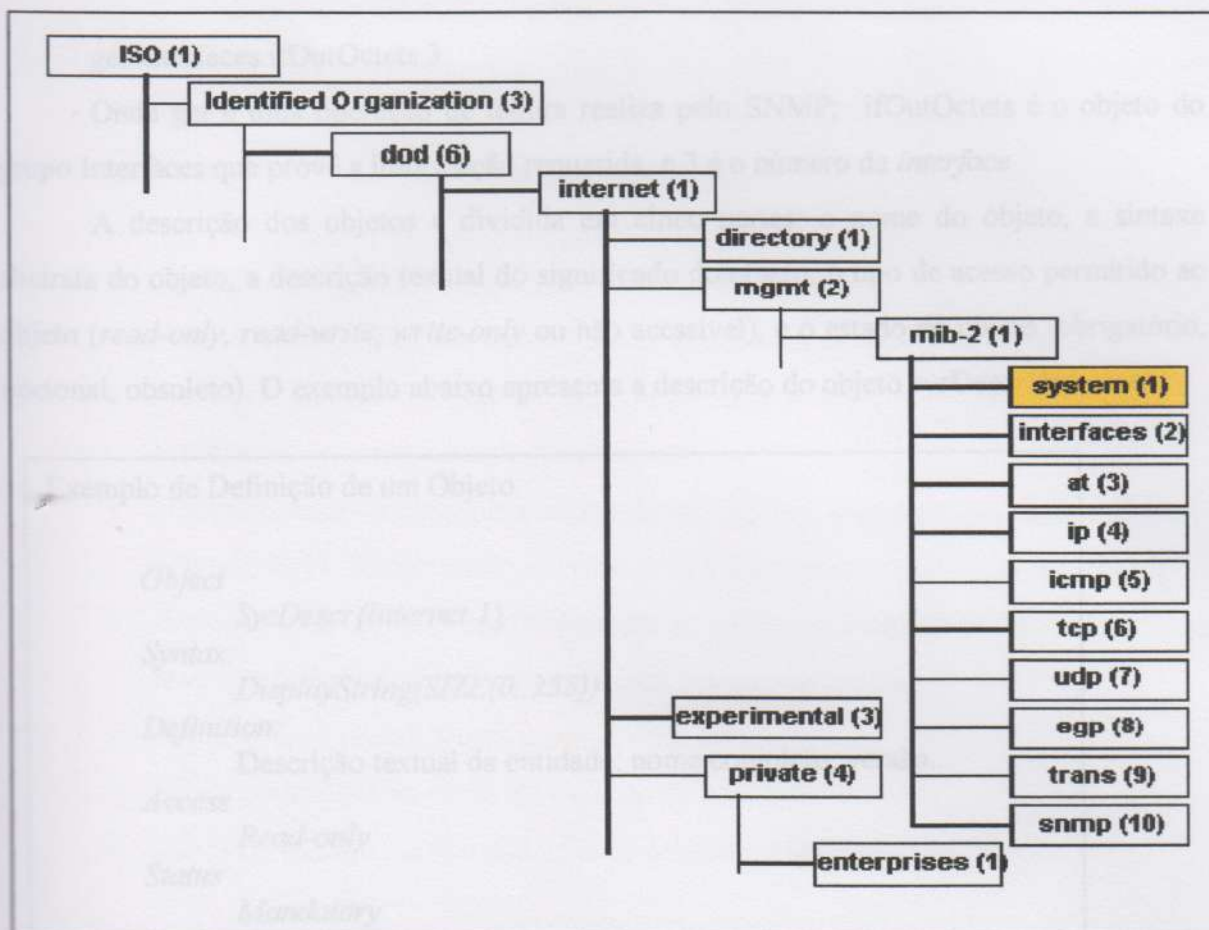


Figura 4: Árvore de organização das informações de gerência

Abaixo da árvore mibII estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos são divididos em dez grupos, abaixo especificados:

Grupos	Informações
<i>System</i> (1)	informações sobre o sistema no qual se encontra a entidade gerenciada
<i>Interfaces</i> (2)	oferece dados sobre cada <i>interface</i> de rede de um dispositivo gerenciável da rede
<i>Address translation</i> (3)	mapeamento de endereços IP em endereços físicos
<i>ip</i> (4)	informações sobre o protocolo IP na entidade em questão
<i>icmp</i> (5)	informações sobre o protocolo ICMP
<i>tcp</i> (6)	informações sobre o protocolo TCP
<i>udp</i> (7)	informações sobre o protocolo UDP
<i>egp</i> (8)	informações sobre o protocolo EGP
<i>Transmission</i> (9)	informações sobre o meio específico
<i>snmp</i> (10)	informações sobre o protocolo SNMP

Por exemplo, para ler o número de pacotes IP's que saíram da 3ª *interface* de um dispositivo, na notação apresentada, faria-se uma pesquisa do tipo:

get interfaces.ifOutOctets.3

Onde get é uma operação de leitura realiza pelo SNMP; ifOutOctets é o objeto do grupo Interfaces que provê a informação requerida, e 3 é o número da *interface*.

A descrição dos objetos é dividida em cinco partes: o nome do objeto, a sintaxe abstrata do objeto, a descrição textual do significado do objeto, o tipo de acesso permitido ao objeto (*read-only*, *read-write*, *write-only* ou não acessível), e o estado do objeto (obrigatório, opcional, obsoleto). O exemplo abaixo apresenta a descrição do objeto sysDescr{Internet1}

Exemplo de Definição de um Objeto

Object

SysDescr{Internet 1}

Syntax:

DisplayString(SIZE(0..255))

Definition:

Descrição textual da entidade: nome completo, versão...

Access

Read-only

Status

Mandatory

3.2.1 Critérios e Filosofia para o Padrão MIB

Novos objetos implementados na MIB não podem ser criados aleatoriamente. Existem critérios e regras universais a serem seguidas, que padronizam a árvore de gerenciamento. Logo abaixo são especificados os critérios estabelecidos.

- Os objetos devem ser unicamente identificados;
- Os objetos devem ser essenciais;
- A estrutura abstrata deve ser universal;
- A MIB deve manter apenas um pequeno número de objetos;
- Deve permitir extensões privadas;
- Os objetos devem ser gerais e não dependentes de dispositivo;
- Os objetos não devem ser facilmente derivados dos objetos já existentes;
- Se o agente deve ser gerenciável através do SNMP, então é obrigatório implementar a MIB Internet (MIB-II).

3.2.2 Identificadores de Objetos

Para que os objetos sejam acessados, eles precisam ser identificados unicamente. Essa padronização segue algumas regras abaixo relacionadas:

- O nome do objeto é dado pelo seu nome na árvore;
- A todos os nós filhos são dados valores inteiros únicos dentro da nova sub-árvore;
- Os filhos podem ser pais de uma futura sub-árvore filha, onde o esquema de numeração é recursivamente aplicado;
- O identificador de objeto (ou nome) de um objeto é a seqüência de valores inteiros não negativos, atravessando a árvore até o nó requerido;
- A alocação de um valor inteiro para um nó na árvore é um ato de registro por quem quer que tenha autoridade delegada para aquela sub-árvore;
- Este processo pode ir a uma profundidade arbitrária;
- Se um nó tem filhos, então ele é um nó agregado;
- Filhos do mesmo pai não podem ter o mesmo valor inteiro.

3.3 OPERAÇÕES SUPORTADAS PELO SNMP - TIPOS DE MENSAGENS

Os gerentes se comunicam com os agentes através de operações que possibilitam a leitura e modificação dos valores dos objetos na MIB.

O SNMP também provê meios de o agente se comunicar com o gerente sem que este último faça algum tipo de solicitação. Isto acontece, geralmente, quando alguma condição de erro se verifica.

Abaixo são especificados os tipos de operações existentes e como elas podem ser utilizados.

Get: o gerente solicita aos agentes uma leitura no valor das variáveis dos objetos gerenciados.

Ex. : O gerente solicita a um agente a informação sobre a porta 10 de um dado *switch*. Ele quer saber se ela está habilitada ou não.

Set: o gerente solicita aos agentes a modificação no valor de uma variável de um objeto gerenciado.

Ex. : O gerente determina que a porta 10 de um *switch* seja desabilitada.

Response: é a resposta dos agentes ao gerente sobre a solicitação de comando que foi dado por este último.

Trap: um agente informa ao gerente sobre a ocorrência de um evento específico.

Ex. : Um agente avisa ao gerente de que a porta 10 de um *switch* perdeu o *link* em um determinado instante (*link down*).

3.4 FORMATO DAS MENSAGENS SNMP

No SNMP, informações são trocadas entre uma estação de gerenciamento e um agente na forma de uma mensagem SNMP.

Cada mensagem SNMP tem o formato:

- *Version* – número da versão;
- *Community* – nome da comunidade – explicado em detalhes na seção 3.5;
- Uma ou mais PDUs (*Protocol Data Unit*) SNMP – assumindo autenticação trivial.

Cada PDU SNMP, exceto *trap* tem o seguinte formato:

- *Request-id* – identificador único de uma requisição;
- *Error-status* – usados para indicar que uma exceção ocorreu durante o processamento de uma requisição;
- *Error-index* – quando um *error-status* é não 0, *error-index* pode prover informações adicionais indicando qual variável na lista causou a exceção;
- *Variable-bindings* – uma lista de nomes de variáveis e valores correspondentes.

PDUs *traps* têm o seguinte formato:

- *Enterprise* – identifica o subsistema de gerenciamento de rede que causou o *trap*;
- *Agent address* – endereço IP do agente que enviou o *trap*;
- *Generic trap id* – tipo genérico de *trap* – *traps* comuns, isto é, pré-definidos;
- *Specific trap id* – código específico do *trap* – *traps* específicas de empresas ou fabricantes;

- *Time stamp* – tempo entre a última reinicialização da entidade da rede que emitiu o *trap* e a geração do *trap*;
- *Variable bindings* – lista de nomes de variáveis e valores correspondentes que podem ser importantes à NMS (*Network Management Station*).

i) Mensagem SNMP

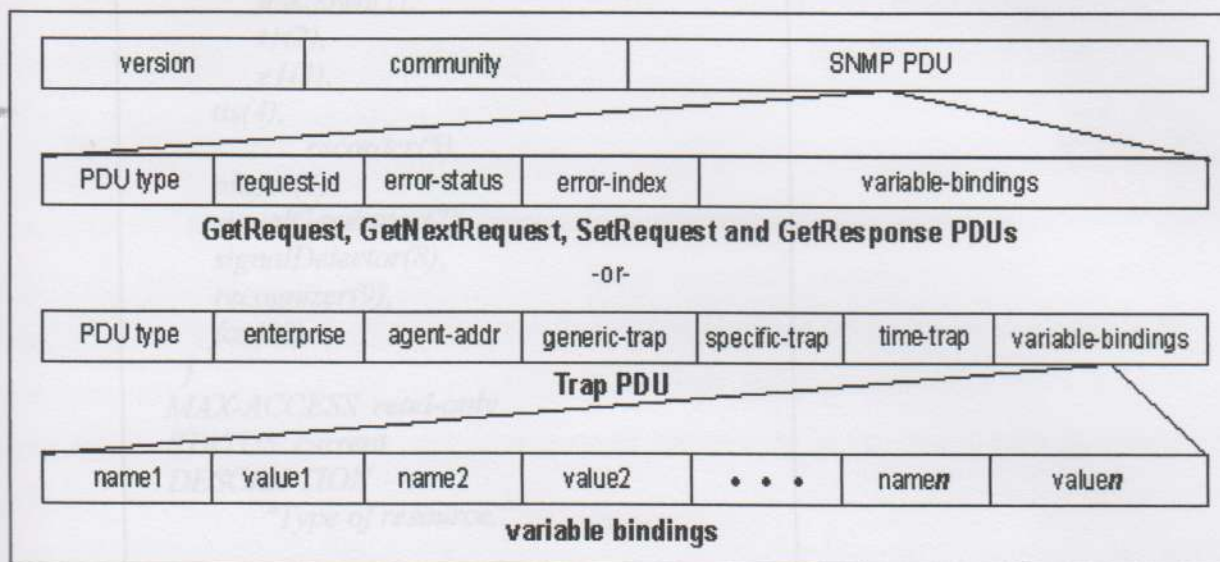


Figura 5: Composição da mensagem SNMP

3.4.1 Transmissão de uma Mensagem SNMP

Uma entidade SNMP realiza as seguintes ações para transmitir uma PDU para outra entidade SNMP.

a) O PDU é construído usando a estrutura ASN.1 (*Abstract Syntax Notation One*), definida na RFC 1157.

b) Este PDU é então passado para um serviço de autenticação, junto com o endereço de origem e destino e o nome da comunidade. O serviço de autenticação realiza qualquer transformação para esta troca, assim como criptografia ou a inclusão de um código de autenticação e retorna o resultado.

c) A entidade do protocolo então constrói a mensagem, consistindo de um campo versão, nome da comunidade e o resultado do passo b.

d) O novo objeto ASN.1 é representado usando as regras básicas de codificação, e passado ao serviço de transporte.

Abaixo encontra-se parte da codificação de uma MIB utilizando ASN.1

```
ectfContentsResourceType OBJECT-TYPE
SYNTAX INTEGER {
    unknown(1),
    t1(2),
    e1(3),
    tts(4),
    recorder(5),
    player(6),
    signalGenerator(7),
    signalDetector(8),
    recognizer(9),
    fax(10)
}
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Type of resource."

 ::= { ectfResourceEntry 4 }
```

3.4.2 Recebimento de uma Mensagem SNMP

Em princípio, uma entidade SNMP realiza as seguintes ações assim que recebe uma mensagem SNMP:

- Realiza uma supervisão na sintaxe básica da mensagem e descarta a mensagem se ela falhar na verificação;
- Verifica o número da versão e descarta a mensagem se ela for incompatível;
- A entidade do protocolo então passa, o nome do usuário, o campo PDU da mensagem e os endereços de origem e destino da mensagem para um serviço de autenticação; Se a verificação falha, o serviço de autenticação avisa à entidade do protocolo SNMP, que descarta a mensagem;

b) Caso contrário, o serviço de autenticação retorna na forma de um objeto ASN.1.

- A entidade do protocolo faz uma supervisão na sintaxe básica da PDU. Por outro lado, usando o nome da comunidade, o plano de acesso SNMP apropriado é selecionado, e o PDU é processado de acordo.

3.5 SEGURANÇA NO PROTOCOLO SNMP

O protocolo de gerência SNMP pode realizar operações de reconfiguração na rede alterando características de equipamentos ou até desligando máquinas, sendo não existe qualquer mecanismo de segurança aplicado ao conteúdo das mensagens. O controle é feito através da verificação do conteúdo de um campo especial no pacote do SNMP, denominado comunidade. A comunidade é definida como sendo o relacionamento entre duas entidades do SNMP. É definida como um conjunto de *bytes* formando caracteres *ASCII* que serão utilizados para efetuar este relacionamento. Dessa forma quando é realizada a comunicação entre duas entidades do SNMP a entidade destinatária da mensagem realiza a verificação do conteúdo da comunidade para averiguar se esta informação é proveniente do remetente indicado.

Através da comunidade é possível que o agente realize uma verificação da integridade do gerente realizando autenticação e políticas de acesso (agente controla que diferentes gerentes podem obter diferentes variáveis da MIB) através deste campo. O mais importante no entendimento de comunidade, é que sem o conhecimento prévio da comunidade de um determinado equipamento gerenciável, será impossível a qualquer aplicação de gerência acessar as informações da MIB. Outra consideração importante é que um equipamento pode ter mais de uma comunidade configurada, como uma com direitos somente de leitura, outra com direitos de leitura e escrita e finalmente outra com direitos de leitura, escrita e *trap*. Portanto, um mesmo equipamento poderá contar com três *strings* de comunidade diferentes. Isto tem o objetivo de se aumentar a segurança no acesso aos equipamentos.

Segue abaixo algumas características da MIB:

- identificação da origem: a comunidade é transmitida sem qualquer proteção sendo que a mensagem SNMP pode ser interceptada por algum intruso que poderá copiar o mesmo nome de comunidade e entrar na MIB
- integridade da mensagem: ao ser interceptada a mensagem não garante qualquer proteção referente ao conteúdo

- tempo-limite: período de tempo que a mensagem pode ficar presa por algum serviço
- privacidade: qualquer serviço pode monitorar uma comunicação entre entidades SNMP
- autorização: não há controle de autorização de acesso aos dados da MIB

3.6 MECANISMO DE TRANSPORTE

O SNMP assume que o caminho de comunicação é uma subrede de comunicação não orientado à conexão. Em outras palavras, nenhum caminho de comunicação é pré-estabelecido antes da transmissão dos dados. Como resultado deste fato, tem-se que o SNMP não dá garantia sobre a entrega destes dados, embora, na prática, a maioria das mensagens chegue aos seus destinos e as que não chegam podem ser retransmitidas. Os protocolos primários que o SNMP utiliza são *User Datagram Protocol* (UDP) e *Internet Protocol* (IP).

A simplicidade do SNMP e a comunicação não orientada à conexão também produzem um grau de robustez. Nem o gerente, nem o agente confiam um no outro para as suas operações. Desta forma, um gerente pode continuar a funcionar mesmo que um agente remoto falhe. Quando o agente reassume a sua função, ele pode enviar um *trap* ao gerente, notificando-o de sua mudança no estado operacional.

Apesar de utilizar UDP como transporte padrão, deve-se manter em mente que o SNMP é independente de transporte e pode ser implementado em outros transportes como: TCP, Mapeamento direto sobre *Ethernet*, X25 e ATM.

No transporte UDP:

- O agente escuta no UDP, porta 161;
- Respostas são enviadas de volta à porta da NMS original através de uma porta dinâmica, embora muitos agentes usem a porta 161 também para esse propósito;
- O tamanho máximo de uma mensagem SNMP é limitado pelo tamanho máximo da mensagem UDP (65507 octetos);
- Todas as implementações SNMP devem receber pacotes com, pelo menos, 484 octetos de comprimento;

- Alguma implementação SNMP pode tratar incorretamente ou não tratar pacotes que excedam 484 octetos;
- Traps assíncronos são recebidos pela porta 162 do NMS;
- UDP é mais adequado que o TCP, quando mudanças na rota dinâmica ocorrem com frequência (quando há problemas na rede);
- Pacotes UDP minimizam as demandas colocadas na rede;
- Agentes e NMS são responsáveis por determinar a recuperação dos erros.

3.7 RMON (*Remote Monitoring*)

A especificação RMON é uma definição de uma MIB. Seu objetivo é definir funções de monitoração e *interfaces* para a comunicação entre agentes/gerentes SNMP. Essa monitoração é realizada através de monitores, que são dispositivos providos de um agente de gerenciamento com MIB RMON, configurados para monitorar outros dispositivos. Normalmente, o monitor RMON e o agente SNMP estão no mesmo equipamento gerenciado. Essa configuração minimiza a carga do tráfego entre a estação de gerenciamento de rede e os dispositivos gerenciados, já que estes últimos só precisam se comunicar com a estação quando alguma condição de erro acontece nos dispositivos monitorados ou quando a estação gerente deseja coletar dados estatísticos, análises e diagnósticos destes dispositivos.

O RMON tem como metas:

- Operação *off-line*: em geral o monitor deve coletar falhas, performance e informações de configuração continuamente, mesmo não sendo alvo de pesquisa (*poll*) de um gerente, pois a rotina de pesquisa pode cessar se o gerente ou a comunicação falhar. O monitor continua a acumular estatísticas que podem ser recuperadas depois pela estação de gerenciamento ou pode também notificá-la se eventos excepcionais ocorrer.
- Monitoramento preemptivo: se o monitor tiver recursos suficientes, pode executar continuamente diagnósticos e registrar a performance da rede. Numa falha na rede, pode notificar a estação gerente da falha e prover informações proveitosas no seu diagnóstico.

- Detecção de problemas e relatório: o monitor pode passivamente reconhecer certas condições de erro e outros, como congestionamento no tráfego observado. Quando uma situação configurada ocorrer, ele pode tentar notificar a estação gerente.
- Análise de dados: o monitor pode realizar análises específicas após coletados os dados na subrede. Por exemplo, pode determinar que *host* gera a maior parte do tráfego ou erros na subrede.
- Múltiplos gerentes: uma configuração de rede pode ter mais que uma estação gerente para gerar confiança, executar funções diferentes e prover capacidades de gerência para unidades diferentes na organização.

3.7.1 Controle de Monitores Remotos

Um monitor remoto pode ser implementado como uma função disponível ou como um dispositivo dedicado. Com esses recursos dedicados, o monitor é capaz de efetuar funções complexas.

Tipicamente, um monitor remoto necessita ser configurado para coletar dados. A configuração dita o tipo e a forma dos dados a serem coletados. A MIB é organizada em grupos funcionais. Cada grupo tem uma ou mais tabelas de controle e uma ou mais tabelas de dados. Uma tabela de controle contém parâmetros que descrevem o dado na tabela de dados, que é somente para leitura. Assim, a estação gerente define os parâmetros apropriados à configuração do monitor remoto para coletar os dados desejados.

CAPÍTULO 4

FERRAMENTAS DE GERENCIAMENTO DE REDE

4.1 TIVOLI

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

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

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

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

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

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

Além desses módulos de gerenciamento o Tivoli utiliza-se do *Netview*, ferramenta também desenvolvida pela IBM, para o diagnóstico e controle de redes de comunicação.

Seu objetivo era substituir uma gama variada de produtos similares já existentes.

O mais conhecido desses produtos é o *Network Communication Control Facility* (NCCF) que funciona como uma aplicação *Virtual Telecommunication Access Method* (VTAM), fornecendo uma visão do estado da rede através de um monitor de controle e uma base de dados.

Outros produtos de controle são o *Network Problem Determination Application* (NPDA), que opera na detecção de problemas e o *Network Logical Data Manager* (NLDM), que gerencia dados lógicos.

O principal objetivo do *NetView* foi então reunir as funcionalidades destes produtos em um só, melhorando o desempenho e introduzindo novos conceitos no gerenciamento de redes.

Três componentes são definidos na arquitetura do *NetView*: Pontos Focais (*focal points*), gerentes que realizam as funções de controle integrado; Pontos de Entrada (*entry points*), agentes tratados como recursos gerenciados, que reportam seus dados de gerenciamento via SNA (*System Network Protocol*) aos pontos focais; e pontos de serviço (*services points*), destinados a prover *gateways* traduzindo protocolos não padrões SNA no protocolo (NMVT), o que permite a integração de dispositivos não-SNA ao esquema de gerenciamento *NetView*.

A Figura 6 mostra duas imagens capturadas do Tivoli em ação. Na imagem (a), o Tivoli, monitora o tráfego gerado por um computador, apresentando um gráfico estatístico em termos de número de pacotes que trafegam em determinados instantes. Na imagem (b), o *NetView* apresenta a situação da conectividade de uma rede em um determinado instante. Existe um padrão de cores para sinalizar o estado atual de cada ponto de interconexão. Por exemplo, o vermelho indica uma falha. Amarelo indica que está acontecendo algum problema naquele ponto que requer atenção do gerente. E verde indica que aquele ponto está funcionando normalmente.

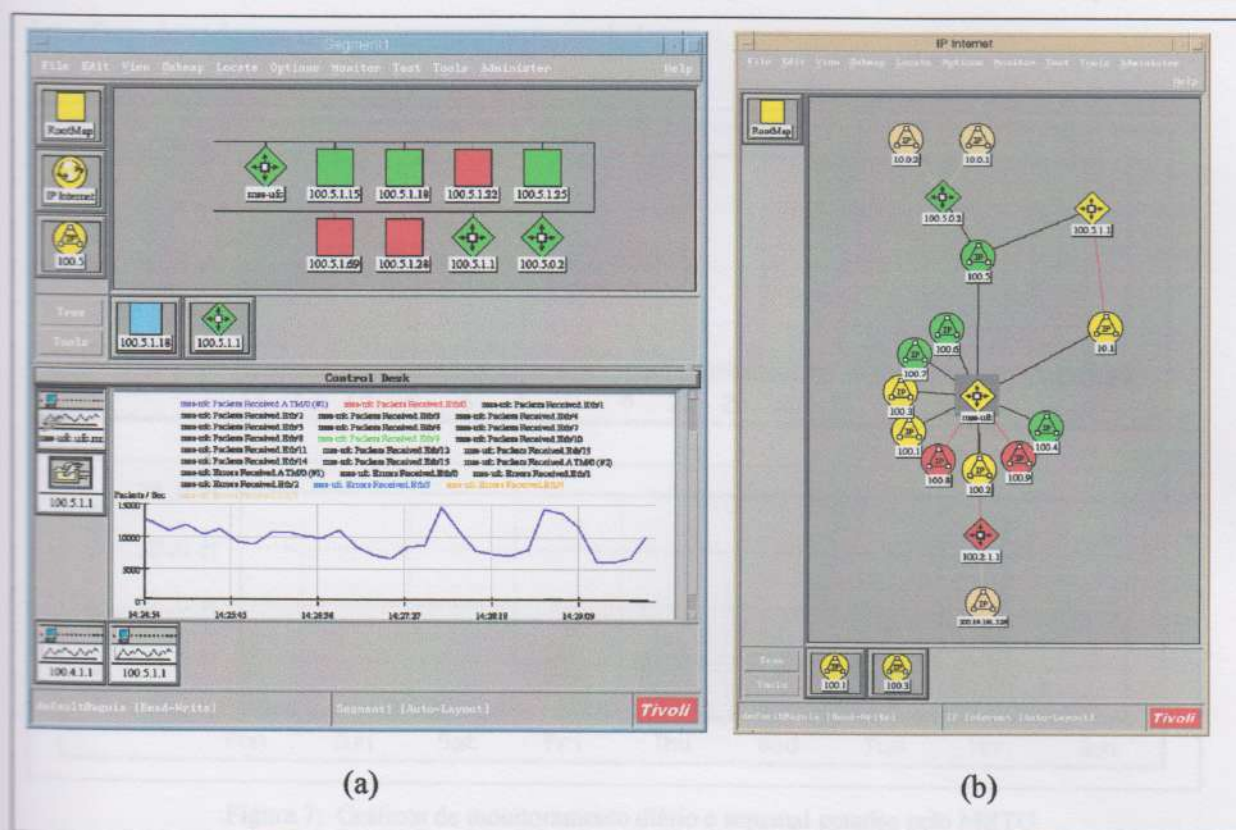


Figura 6: Tivoli: Exemplos de utilização. (a) Análise de tráfego; (b) Pequena rede apresentada no NetView

4.2 MRTG

O *Multi Router Traffic Grapher* (MRTG) é uma ferramenta de análise de tendências. Devido ao fato de ser distribuído gratuitamente e de sua facilidade de configuração este tem se tornado uma das ferramentas mais utilizadas para realizar monitoramento e predição de estados de recursos.

4.2.1 Como Funciona O MRTG

Esta ferramenta é composta de um pacote de pequenos agentes que geram diversos relatórios e estatísticas de utilização. Pode-se utilizar o MRTG para monitorar grau de utilização de discos rígidos, memória, processador, dispositivos de redes, etc.

O Usuário, na configuração do MRTG, deverá informar que objetos da árvore da MIB serão monitorados pelo software. O MRTG utiliza o protocolo SNMP nos agentes para pesquisar estes objetos, enviando mensagens do tipo *get* para colher as informações desejadas.

A Figura 7 mostra dois gráficos estatísticos, gerados pelo MRTG, sobre a utilização de uma interface de rede em um equipamento gerenciado.

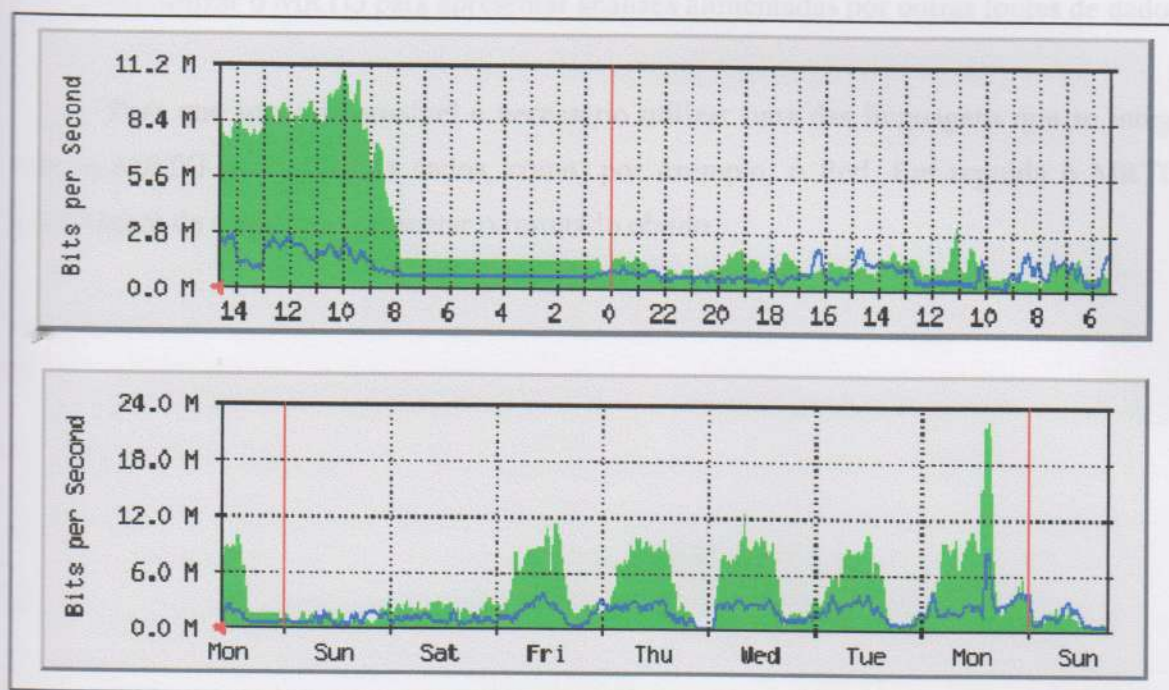


Figura 7: Gráficos de monitoramento diário e semanal gerados pelo MRTG

No primeiro gráfico, tem-se a média a cada 5 minutos de utilização do link em bits por segundo. No eixo das coordenadas temos o volume de tráfego utilizado em Mbps, e no eixo das abscissas tem-se o horário de utilização durante o dia. O gráfico em verde representa o tráfego de rede que chega na interface, e o azul o tráfego que sai da interface. O segundo gráfico mostra a mesma análise mudando a taxa de amostragem, passando de horas do dia (visto no primeiro gráfico) para os dias da semana.

O programa necessário para visualizar o gerente MRTG é um navegador de Internet. Isto porque o MRTG gera seus gráficos estatísticos em páginas HTML. Os relatórios são exibidos em forma de imagens GIF, o que deixa aplicação extremamente leve.

O MRTG pode ser adquirido no *site* (www.mrtg.org). Deve-se fazer o *download* do software para o Sistema Operacional adequado, assim como seus “pré-requisitos”, e em seguida integrá-lo a um *Web Server*.

4.2.2 O MRTG, SNMP e outras Fontes de Informação

O MRTG adquire dados nativamente apenas a partir do protocolo SNMP. No entanto, é possível utilizar o MRTG para apresentar análises alimentadas por outras fontes de dados.

Para que isto seja possível é necessário utilizar uma das linguagens que se integram com o MRTG para obter os dados, como, por exemplo, o Perl. Em seguida o MRTG se encarregará de analisar e apresentar o resultado obtido.

4.1 INVENTARIO DE SISTEMAS

Em termos de Sistemas de Informação, a FARN faz uso dos seguintes sistemas e a rede: Controle Acadêmico (em arquitetura Cliente-Servidor), Sistema de Vestibular (com a publicação dos resultados na Web) e Correio Eletrônico Corporativo (baseado em Internet).

4.1.1 Sistemas Operacionais

Servidor	Sistema Operacional
Controladores de Domínio	MS Windows 2000
Web Server/mail	Linux
Firewall	Linux
Estações	Windows 9x e 2000

4.2 INVENTARIO DE EQUIPAMENTOS

Item	Qtd	Configurações
Roteador	1	Cisco 1600
Switchs	15	Intel e 3Com, 12 e 24 portas de 10 e 10/100Mbps
Hubs	10	Variados de 10/100Mbps
Portas de Rede	170	Variados de 10 e 10/100Mbps
Estações de Trabalho	163	De Pentium II 200 a Pentium III 600
Controlador de Domínio AD&M	1	Pentium III 500, 128Mb de RAM e 20Gb de HD
Controlador de Domínio Labs	1	Pentium III 500, 128Mb de RAM e 20Gb de HD
Firewall	1	Pentium III 500, 128Mb de RAM e 20Gb de HD
Servidor Web	1	Pentium III 500, 128Mb de RAM e 20Gb de HD

CAPÍTULO 5 A REDE FARN

A FARN disponibiliza os principais serviços de rede: DNS, Servidor *Web*, Email, Controladores de Domínio, Proxy, *Firewall*, etc. Estes serviços são disponibilizados pelos seguintes recursos.

5.1 INVENTÁRIO DE SISTEMAS

Em termos de Sistemas de Informação, a FARN faz uso dos seguintes sistemas em rede: Controle Acadêmico (em arquitetura Cliente-Servidor), Sistema de Vestibular (com a publicação dos resultados na Web) e Correio Eletrônico Cooperativo (baseado em *Intranet*).

5.1.1 Sistemas Operacionais

Servidor	Sistema Operacional
Controladores de Domínio	MS <i>Windows</i> 2000
Web Server/Email	Linux
<i>Firewall</i>	Linux
Estações	<i>Windows</i> 9x e 2000

5.2 INVENTÁRIO DE EQUIPAMENTOS

Item	Qtd	Configurações
Roteador	1	Cisco 1600
<i>Switchs</i>	15	Intel e 3Com, 12 e 24 portas de 10 e 10/100Mbps
<i>Hubs</i>	10	Variados de 10/100Mbps
Pontos de Rede	170	Variados de 10 e 10/100Mbps
Estações de Trabalho	163	De Pentium II 200 a Pentium III 600
Controlador de Domínio ADM	1	Pentium III 500, 128Mb de RAM e 20Gb de HD
Controlador de Domínio Labs	1	Pentium III 500, 128Mb de RAM e 20Gb de HD
<i>Firewall</i>	1	Pentium III 500, 128Mb de RAM e 20Gb de HD
Servidor <i>Web</i>	1	Pentium III 500, 128Mb de RAM e 20Gb de HD

5.3 ASPECTOS LÓGICOS

A Figura 8, a seguir, apresenta um esquema simplificado de como é organizada a rede da FARN.

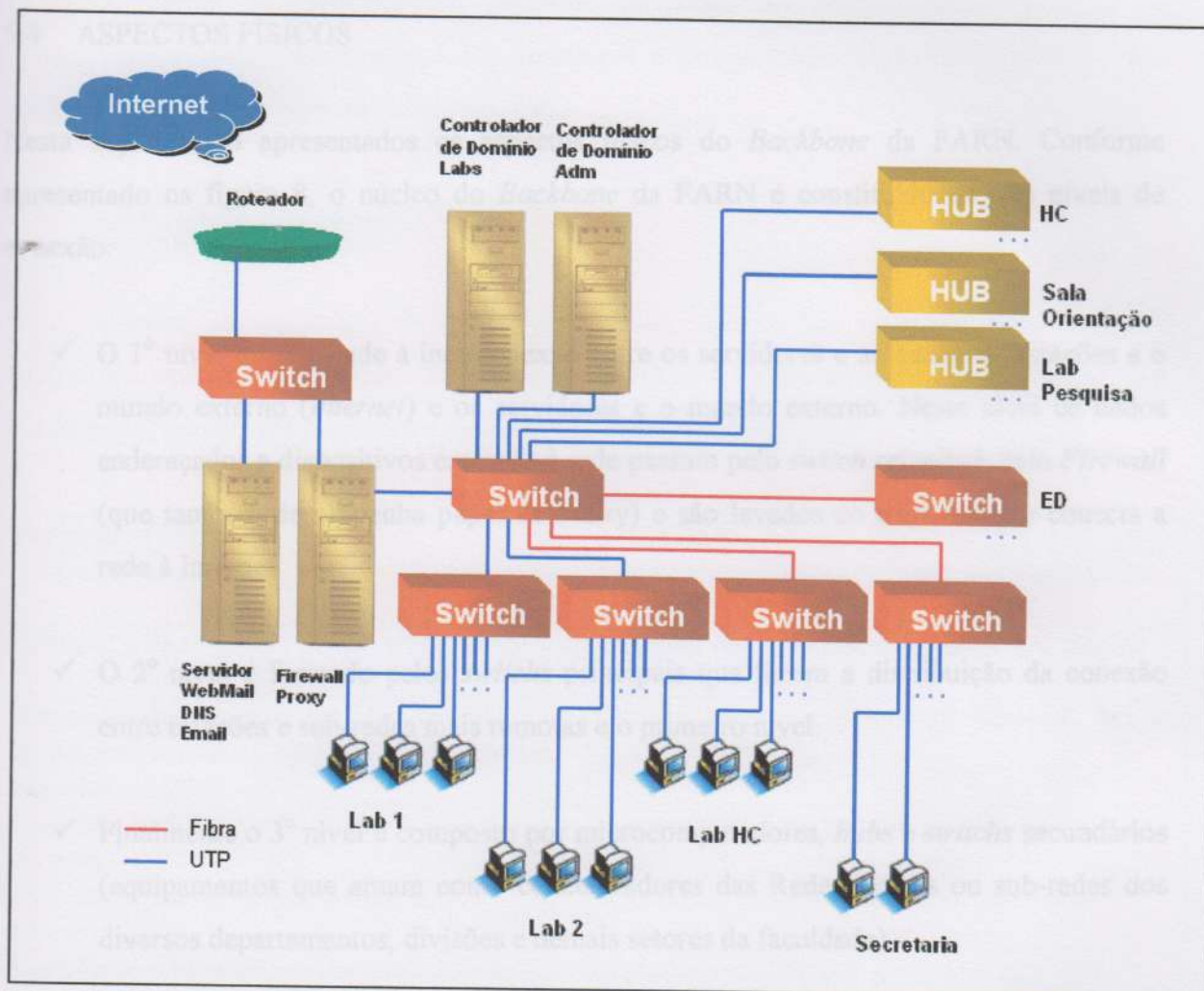


Figura 8: Diagrama do núcleo da Rede FARN

O Controlador de Domínio Adm controla a rede administrativa, servindo de Servidor de Arquivos, Servidor de Aplicações e de *Logon* para as estações dos setores administrativos. O Controlador de Domínio Labs controla as redes acadêmicas, como os laboratórios.

O *Firewall* realiza a tarefa de tradução de endereços (transformar endereços internos, que são inválidos, em um endereço válido antes de enviar um pacote para o mundo externo à rede), bloquear requisições de acesso externas (exceto para as permitidas nas regras de roteamento) e limitar as portas e protocolos de acesso.

O Linux que implementa o Servidor de Emails encontra-se na *Extranet* (parte visível por usuários da Internet) para permitir que os usuários de email consigam receber seus emails quando estiverem fora da rede e para disponibilizar acesso a *sites* (*Web Server*).

5.4 ASPECTOS FÍSICOS

Nesta seção serão apresentados os aspectos físicos do *Backbone* da FARN. Conforme apresentado na figura 8, o núcleo do *Backbone* da FARN é constituído de três níveis de conexão:

- ✓ O 1º nível corresponde à interconexão entre os servidores e as estações, estações e o mundo externo (*internet*) e os servidores e o mundo externo. Neste nível os dados endereçados a dispositivos externos à rede passam pelo *switch* principal, pelo *Firewall* (que também desempenha papel de Proxy) e são levados ao roteador que conecta a rede à Internet.
- ✓ O 2º nível é formado pelos *switchs* principais que fazem a distribuição da conexão entre estações e sub-redes mais remotas e o primeiro nível.
- ✓ Finalmente o 3º nível é composto por microcomputadores, *hubs* e *switchs* secundários (equipamentos que atuam como concentradores das Redes Locais ou sub-redes dos diversos departamentos, divisões e demais setores da faculdade).

Os quatros servidores suportam gerenciamento SNMP através dos seus Sistemas Operacionais. Os *Switches* Principais suportam gerenciamento SNMP, no entanto é necessário verificar se estes módulos, que em geral são opcionais, foram adquiridos pela faculdade.

A interconexão entre os *switchs* principais e os *switchs* secundários e servidores se dá em *Fast Ethernet*, 100Base TX e FX.

CAPÍTULO 6 PROPOSTA DE GERENCIAMENTO PARA A REDE FARN

A seguir são apresentadas algumas sugestões de como utilizar técnicas de gerenciamento, discutidas nos capítulos anteriores, a fim de melhorar o desempenho da rede da FARN e reduzir o custo de administração.

6.1 AUDITORIA PRELIMINAR

Através da aplicação *Inventory* do Tivoli, deverá ser realizada uma auditoria preliminar para obter o máximo de informações sobre o estado atual dos recursos em rede. Deverão ser levantados parâmetros tais como:

Parâmetro Medido	Finalidade
Utilização dos discos rígidos	Detectar gargalos decorrentes de alta taxa de utilização dos discos
Utilização da memória dos servidores	Detectar gargalos decorrentes de alta taxa de utilização dos discos
Utilização dos adaptadores de rede dos servidores, portas do <i>switch</i> e adaptadores de rede das estações.	Ordenar os ramos da rede por demanda de uso
Capacidade de transmissão dos adaptadores de rede	Agrupar recursos por capacidade máxima de uso
Utilização dos diferentes protocolos no <i>Firewal</i>	Identificar possíveis falhas na segurança
Identificar principais recursos utilizados pelas estações	Agrupar estações por grupos de recursos

Todos os servidores apresentam módulos de gerenciamento SNMP. Estes módulos devem ser utilizados para aquisição das informações acima.

Em geral os fabricantes dos equipamentos fornecem os módulos de gerência SNMP como um "opcional", vendido separadamente. Por este motivo é possível que não estejam disponíveis estes módulos para as ferramentas de monitoramento. Para contornar este problema devem ser levantadas as alternativas de softwares fornecidas pelos fornecedores, fabricantes do Sistema Operacional ou mesmo outras ferramentas disponíveis no mercado.

6.1.1 Ações tomadas após auditoria preliminar

- ✓ Redistribuição dos pontos: Deverão ser utilizadas as informações de que estações utilizam que recursos para estas estações estejam mais “próximas” dos recursos. Colocar, por exemplo, os funcionários que mais utilizam Internet no mesmo *switch* em que está o *proxy* reduzirá a taxa de erro de toda a rede e aumentará o desempenho no acesso dos usuários.
- ✓ Agrupar usuários por capacidade de acesso: Deverão ser identificados os usuários com capacidade de acesso de rede de 10 e 100Mbps. Colocar um usuário com adaptador de 10Mbps em um *hub* com outros de 100Mbps automaticamente restringirá a capacidade de acesso de todos para 10Mbps.
- ✓ Redistribuir aplicações: Em geral aplicações com grande taxa de acesso a disco demandam Servidores com discos SCSI, várias controladoras, etc. Por outro; Aplicações que realizam muitos cálculos demandam muita capacidade de Processamento; Aplicações com grande demanda de memória, como servidores *Proxy*, devem estar instaladas em equipamentos com configuração adequada de compartilhamento de memória, restrição de memória por processo, etc. De posse destes conceitos deve-se fazer uma análise nos recursos de software e hardware da FARN e verificar a possibilidade de redistribuir aplicações para aumentar a capacidade de utilização

Através desta auditoria serão criadas as interfaces de leitura de informações que posteriormente serão utilizadas na análise sistemática da rede.

6.1.2 Ações tomadas imediatamente

Recomenda-se que o Servidor de Emails/*Web* esteja “atrás” do *Firewall* para permitir assim que seja incrementada sua proteção. Sua localização física hoje deixa este servidor extremamente vulnerável a ataques externos.

6.2 ANÁLISE DE CAPACIDADE

Deverá ser analisada a utilização da rede em diversos horários e detectar se a capacidade instalada da Rede é suficiente para a demanda de uso. Para esta análise devem ser

monitoradas as utilizações dos diversos protocolos durante todo o dia, a utilização da memória e utilização dos processadores dos Servidores. Deve ser analisada também a utilização da conexão com a Internet.

6.3 PREDIÇÃO E DEMANDA FUTURA

Deve-se preparar um plano de expansão/crescimento da demanda da Rede. A partir das informações de capacidade e utilização deve-se identificar quais serão os gargalos que aparecerão na rede e quando ocorrerão. A partir desta informação será possível fazer planejamento de expansão e evitar quedas de qualidade do serviço (QoS).

Outra utilização deste plano é o remanejamento de tarefas que possam ser executadas em horários de menor demanda, como, por exemplo, o backup, rotinas administrativas, etc.

6.4 MONITORAMENTO SISTEMÁTICO

Deverá ser montado um procedimento de acompanhamento sistemático das informações da Rede. Este procedimento possibilita a previsão de gargalos, identificar invasões na rede, picos de utilização, falhas de recursos, dentre outros.

O monitoramento Sistemático deverá prever ações de contingência em casos críticos, pessoal responsável pela execução das tarefas, relatório de execução das tarefas, relatórios gerenciais periódicos descrevendo status e recomendações.

Somente através do monitoramento sistemático é possível ter uma gerência de redes eficaz.

6.5 FERRAMENTAS UTILIZADAS

Após o inventário feito pelo Tivoli, deverá ser utilizado o MRTG como principal ferramenta de análise de informações, através dos gráficos estatísticos gerados pelo mesmo. Devido ao pequeno grau de complexidade da rede da FARN, recomenda-se a utilização deste software, pois pequenas análises podem gerar grandes ganhos de desempenho e segurança da

Rede. Na Figura 9, podemos observar o monitoramento que já é feito atualmente pela FARN para o seu link com a Internet.

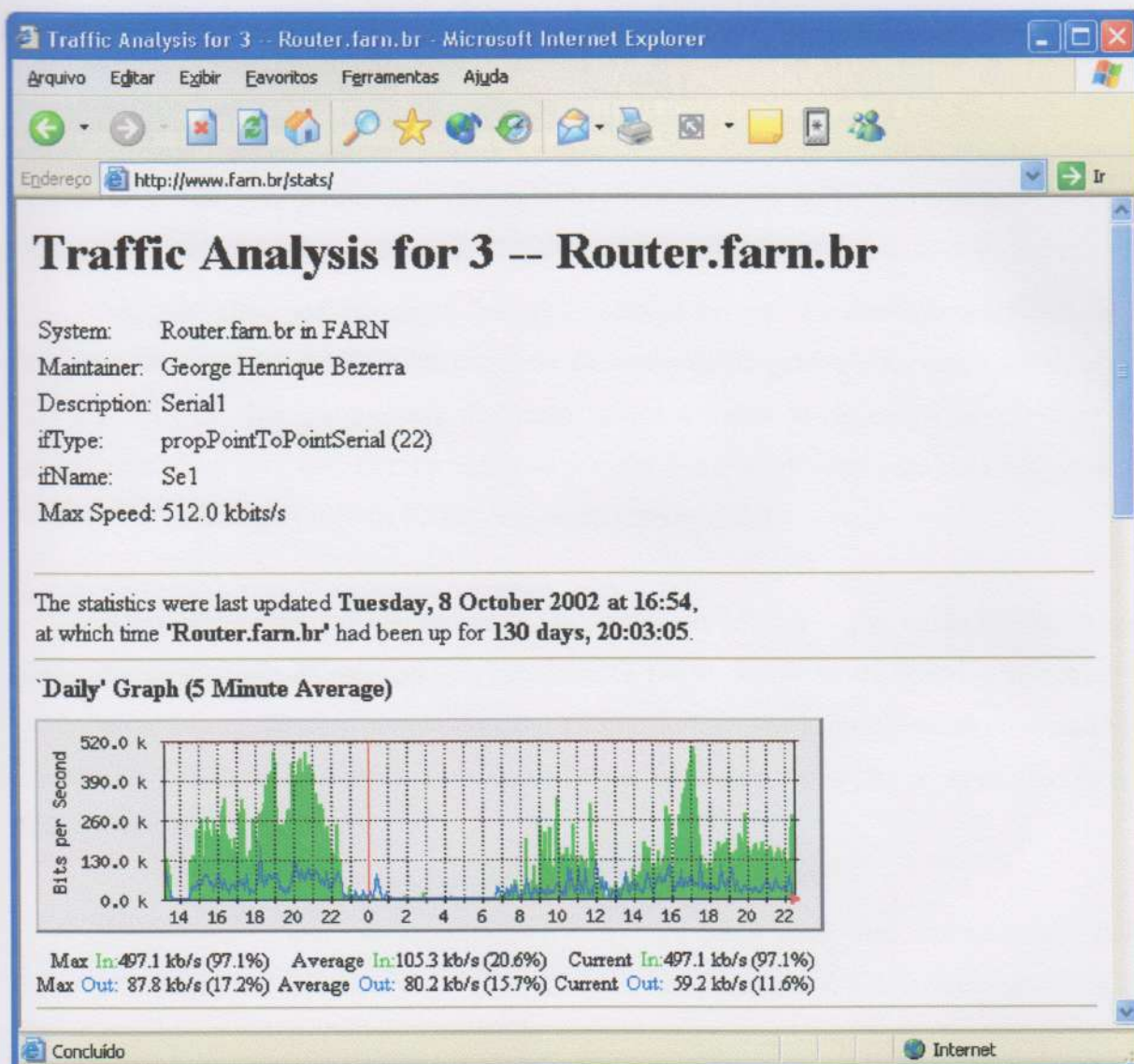


Figura 9: MRTG monitorando o acesso da FARN à Internet

Ferramentas complementares devem ser utilizadas quando não for possível, através do MRTG para adquirir informações, tais como a Performance Monitor do *Windows NT/2000* para monitorar acesso a disco, rede e memória.

Deve-se utilizar também os agentes SNMP dos Sistemas Operacionais e equipamentos, pois estes softwares utilizam pouquíssima banda para operar e têm grande grau de confiabilidade.

Uma vez que os agentes estejam funcionando adequadamente pode-se criar uma aplicação gerente SNMP que manipule as informações geradas pelos agentes. Pode-se construir esta aplicação utilizando o MRTG como fonte de informações de gerência, e o navegador da *Web* para visualizar estas informações.

Fazendo uma análise deste trabalho, verifica-se que foi extremamente válida a iniciativa de sugerir à FARN uma proposta de melhoria na gerência de redes utilizando o protocolo SNMP. Isto porque este protocolo atende a todos os requisitos na atividade de gerência de redes. Por este motivo optou-se por direcionar o trabalho para uma proposta de melhoria na gerência da rede da FARN utilizando este protocolo.

As duas ferramentas apresentadas - o Tivoli e o MRTG - são muito utilizadas em atividades de gerência de redes nas corporações. O Tivoli, apesar de ter recursos de análise e controle muito sofisticados, trata-se de uma ferramenta cara que exige treinamento específico para ser utilizada. Por isso só deverá ser utilizada se o custo de aquisição e operação for compensado pelos benefícios.

Já o MRTG, mostrou-se como sendo a ferramenta ideal para ser utilizada, pois apresenta interface compatível com todos os sistemas operacionais, é extremamente fácil de usar e configurar, além de ser distribuída gratuitamente. Por estes motivos recomenda-se a maior utilização nas atividades de gerência de redes.

Como sugestões para trabalhos futuros, podemos citar os seguintes tópicos:

- Verificar na prática o funcionamento do protocolo SNMP, como também a utilização das ferramentas Tivoli e MRTG;
- Desenvolvimento e implementação de uma ferramenta, pelos alunos da FARN, para a atividade de gerência de rede, onde poderiam ser aplicadas todas as conceitos técnicos relativos ao protocolo SNMP.

CAPÍTULO 7 CONCLUSÃO

Foram apresentados neste trabalho os principais conceitos de gerência de redes; conceitos envolvidos na utilização do protocolo SNMP, seus benefícios e aplicações; alguns procedimentos que podem melhorar, a curto prazo, o desempenho e a segurança da rede, sem necessariamente implicar em novos custos; assim como, observações que podem melhorar a utilização dos recursos disponíveis, aumentando a capacidade da rede instalada.

Fazendo uma análise deste trabalho, verifica-se que foi extremamente válida a iniciativa de sugerir à FARN uma proposta de melhoria na gerência de redes utilizando o protocolo SNMP. Isto porque este protocolo atende a todos os requisitos na atividade de gerência de redes. Por este motivo optou-se por direcionar o trabalho para uma proposta de melhoria na gerência da rede da FARN utilizando este protocolo.

As duas ferramentas apresentadas - o Tivoli e o MRTG - são muito utilizadas em atividades de gerência de redes nas corporações. O Tivoli, apesar de ter recursos de análise e predição muito sofisticados, trata-se de uma ferramenta cara que exige treinamento específico intenso. Por isso só deverá ser utilizada se o custo de aquisição e operação forem compensados pelos benefícios.

Já o MRTG, mostrou-se como sendo a ferramenta ideal para ser utilizada, pois apresenta interface compatível com todos os sistemas operacionais, é extremamente fácil de usar e configurar, além de ser distribuída gratuitamente. Por estes motivos recomenda-se difundir sua utilização nas atividades de gerência de redes.

Como sugestões para trabalhos futuros, podemos citar os seguintes tópicos:

- Verificar na prática o funcionamento do protocolo SNMP, como também a utilização das ferramentas Tivoli e MRTG;
- Desenvolvimento e implementação de uma ferramenta, pelos alunos da FARN, para a atividade de gerência de rede, onde poderiam ser aplicados todos os conceitos teóricos relativos ao protocolo SNMP.

REFERÊNCIA BIBLIOGRÁFICA

COMER, Douglas E., **Redes de Computadores e Internet**, Abrange Transmissão de Dados, Ligação Inter-redes e Web. 2ª ed., São Paulo: Bookman, 2001.

MAURO, Douglas R.; SCHMIDT, Kevin J., **SNMP essencial**. Trad. Tereza Cristina F. Souza, 1ª.ed., Rio de Janeiro. Campus, 2001.

RFC 1156, **Management Information Base for network management of TCP/IP – based internets**, maio 1990.

RFC 1213, **Management Information Base for network management of TCP/IP – based internets: MIB II**, março 1991.

RFC 1157, **Simple Network Management (SNMP)**, maio 1990.

SILVA, Lucena Jeane, **Relatório de Graduação**, Sistema de Gerencia da Rede UFRN, Natal. 1999.

TANENBAUM, Andrew. **Redes de Computadores**, 3ª ed., Rio de Janeiro: Campus 7ª Triagem, 1997.

BIBLIOGRAFIA CONSULTADA

BLACK Box Explica... SNMP. Disponível em:

<<http://www.blackbox.com.br/pages/explica/snmp.htm>> Acesso em 15 mar. 2002.

COMER, Douglas E.; STEVENS, David L. **Internetworking with TCP/IP**. Disponível em:

<<http://www.gta.ufrj.br/~alexszt/get/nv6000.html>> Acesso em 15 mar. 2002.

FREITAS, João Carlos da Silva. **Internetworking with TCP/IP2**. Disponível em:

<http://www.gta.ufrj.br/00_1/joao/snmp.htm> Acesso em 15 mar. 2002.

FREIRE, Raissa Dantas. **Um Survey Sobre Aplicações de Gerência de Redes**. Disponível em: <<http://dsc.ufpb.br>> Acesso em 23 mar.2002.

GERÊNCIA de Redes de Computadores. Disponível em:

<<http://www.rafiro.hpg.ig.com.br/mibs/HTML/gr1.htm>> Acesso em: 20 mar. 2002.

O SNMP (Simple NetworkManagement Protocol). Disponível em:

<http://penta.ufrgs.br/gr952/trab1/snmp_snmp.html> Acesso em 15/03/2002.

SNMP Research International, Inc. Disponível em:

<<http://www.snmp.com/>> Acesso em 15 mar. 2002 (a).

SNMP - Simple Network Managment Protocol. Disponível em:

<<http://rad.com/networks/1995/snmp>> Acesso em 23 mar. 2002 (b).

SNMP - Modelo de Gerenciamento ou Protocolo. Disponível em:

<<http://pucmgmt.metropoa.tcche.br/snmp/modeloprotocolo.htm>> Acesso em 23 mar.2002 (c).

SZTAJNBERG, Alexandre. **SNMP/CMIP**. Disponível em:

<<http://www.gta.ufrj.br/~lexszt/ger/gerencia.html>> Acesso em 15 mar. 2002.

TUTORIAL sobre Gerenciamento de Redes. Disponível em: <<http://www.ufc.br/rmav>> Acesso em 23 mar. 2002.