

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

**GERENCIAMENTO DE REDES DE COMPUTADORES:
Estudo de caso para a Rede FARN**

**GERENCIAMENTO DE REDES DE COMPUTADORES:
Estudo de caso para a Rede FARN**

Adriano Costa de Souza Roque

**NATAL/RN
2005**

ADRIANO COSTA DE SOUZA ROQUE

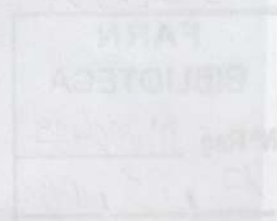
**GERENCIAMENTO DE REDES DE COMPUTADORES:
Estudo de caso para a Rede FARN**

Monografia apresentada ao Curso de Bacharelado em Sistema de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte para a obtenção do grau de Bacharelado em Sistema de Informação.

Orientador:

Aluizio Ferreira da Rocha Neto

**NATAL/RN
2005**



Roque, Adriano Costa de Souza

GERENCIAMENTO DE REDES DE COMPUTADORES: Estudo de caso para a Rede FARN /Adriano Costa de Souza Roque. Natal:FARN,2005

42 p

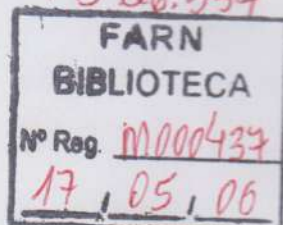
Monografia (Monografia em Sistema de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte./

Orientador: Aluizio Ferreira da Rocha Neto

1.Informática – monografia. 2. Sistema de Informações – monografia 3. Redes – monografia.

RN/FARN/BC

CDU 004.7



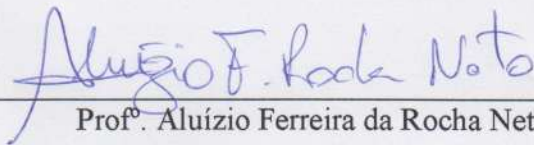
M
004.7
R69g
2005

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

**GERENCIAMENTO DE REDES DE COMPUTADORES:
Estudo de caso para a Rede FARN**

Adriano Costa de Souza Roque

Monografia apresentada em 17 de DEZEMBRO de 2005 pela banca examinadora composta pelos seguintes membros:



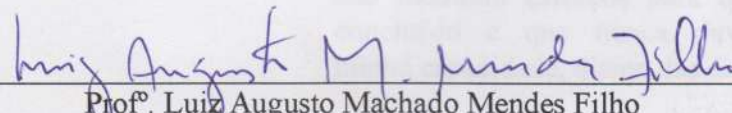
Prof.º Aluizio Ferreira da Rocha Neto

Orientador



Prof.º Ricardo Kleber Martins Galvão

Examinador



Prof.º Luiz Augusto Machado Mendes Filho

Examinador

Natal, 17 de DEZEMBRO de 2005

AGRADECIMENTOS

Os meus sinceros agradecimentos

Primeiramente, a Deus, por ter-me dado a oportunidade de alcançar os meus conhecimentos e a força concedida para o término deste curso.

Aos meus orientadores, pelo incentivo, compreensão, disponibilidade e por ampliar os horizontes dos meus limites.

A todos os Professores que contribuíram com meu crescimento e desenvolvimento na minha formação acadêmica.

Aos meus pais, que foram as principais incentivações e cooperadores para a conclusão deste curso.

Por fim, a todos aqueles que contribuíram de forma direta ou indireta para a conclusão deste curso, deixo minha eterna gratidão.

Dedico este trabalho aos meus Pais, que não mediram esforços para que pudesse concluí-lo e que nunca duvidaram da minha capacidade, diante das dificuldades.

AGRADECIMENTOS

Os meus sinceros agradecimentos:

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

Ao meu orientador, pelo incentivo, cooperação, disponibilidade e por acreditar na transposição dos meus limites.

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

Aos meus pais, que foram os principais incentivadores e cooperadores para a conclusão deste curso.

Enfim, a todos aqueles que contribuíram de forma direta ou indireta para a conclusão deste curso, deixo minha eterna gratidão.

Palavra-chave: Agradecimento; Redes; Protocolo SNMP.

ABSTRACT

RESUMO

Este trabalho apresenta um estudo sobre rede de computadores, sua importância e seus conceitos, além das formas de gerenciamento. Foi feito também, um estudo sobre o protocolo de gerenciamento SNMP, sendo detalhadas as formas de transmissão e recepção de uma mensagem, os tipos de mensagens, a segurança que o protocolo emprega e a flexibilidade de gerenciamento que o protocolo proporciona. São apresentadas três ferramentas para gerenciamento: NETWORK SUPERVISOR, MIBBROWSER e o MRTG. Por fim, são apresentados um estudo de caso de uso da utilização do protocolo SNMP e ferramentas de gerenciamento na rede da FARN, para efeito de entendimento da necessidade de um gerenciamento de rede que proporcione rapidez na solução de problemas de forma rápida e precisa.

Palavra-chave: Gerenciamento; Redes; Protocolo SNMP.

ABSTRACT

This work presents a research about network computers, its concepts and importance, and management kinds. It is studied in details the SNMP protocol, with your ways of transmitting and receipting a message, the types of messages, the protocol security, and the flexibility of management that the protocols provides. Tools like NETWORK SUPERVISOR, MIB BROWSER e MRTG are also presents. Finally, it is presented a case study of utilization SNMP protocol and tools previously reported, to support in management and control of FARN network, resolving the problems in quick and precise form.

Key-word: Management; Network; SNMP Protocol.

ÍNDICE DE FIGURAS

Figura 1: Esboço dos componentes básicos (Fonte: GERENCIAMENTO, 2005).....	14
Figura 2 : Posicionamento de agentes e gerentes (Fonte: GERENCIAMENTO, 2005)	23
Figura 3: Topologia da Rede FARN	28
Figura 4: Interface do Network Supervisor	30
Figura 5: Interface do monitoramento de um switch	31
Figura 6: Interface das formas de Alerta.....	32
Figura 7: Interface do monitoramento detalhado	32
Figura 8: Navegação pela árvore de uma MIB usando o MIB Browser.....	34
Figura 9: Versões de MIBs pré-instaladas com o MIB Browser.....	35
Figura 10: Testando a conectividade com o PING do MIB Browser	36
Figura 11: Configuração do MIB Browser	37
Figura 12: Gráficos de monitoramento diário, semanal, mensal e anual (Fonte: MRTG, 2005)....	39
2.3 O GERENTE DA REDE.....	17
2.4 HARDWARE DE REDES	16
2.4.1 Topologias das Redes de Computadores	16
2.4.2 Cabos.....	17
2.4.3 Equipamentos de Conectividade.....	19
2.5 PROTOCOLOS DE REDE.....	20
2.6 O PROTOCOLO SNMP	21
2.6.1 Agente / Gerente.....	22
2.6.2 Operações Suportadas pelo SNMP – Tipos de Mensagens	23
2.6.3 Transmissão e Recepção de uma Mensagem SNMP	24
2.6.4 Segurança no Protocolo SNMP	24
2.6.5 Mecanismo de Transporte	25
2.7 RMON (Remote Monitoring).....	26
2.7.1 RMONv2	26
3 UM ESTUDO DE CASO SOBRE O GERENCIAMENTO NA REDE FARN	27
3.1 A REDE FARN.....	27
3.2 MONITORAMENTO SISTEMÁTICO	27
3.3 SOFTWARES DE GERENCIAMENTO	28
3.3.1 3COM NETWORK SUPERVISOR	29
3.3.2 MIBBROWSER	33
3.3.3 MRTG	27
4 CONCLUSÕES.....	40
REFERENCIAL BIBLIOGRÁFICO.....	41

SUMÁRIO

1	INTRODUÇÃO.....	9
1.1	PROBLEMA DE PESQUISA	10
1.2	OBJETIVOS	10
1.2.1	Objetivo geral	10
1.2.2	Objetivos específicos.....	11
1.3	JUSTIFICATIVA	11
2	REFERENCIAL TEÓRICO.....	12
2.1	REDES DE COMPUTADORES.....	12
2.2	GERÊNCIA DE REDES.....	13
2.3	O GERENTE DA REDE.....	15
2.4	HARDWARE DE REDES.....	16
2.4.1	Topologias das Redes de Computadores	16
2.4.2	Cabos.....	17
2.4.3	Equipamentos de Conectividade	19
2.5	PROTOCOLOS DE REDE.....	20
2.6	O PROTOCOLO SNMP	21
2.6.1	Agente / Gerente.....	22
2.6.2	Operações Suportadas pelo SNMP – Tipos de Mensagens	22
2.6.3	Transmissão e Recepção de uma Mensagem SNMP	24
2.6.4	Segurança no Protocolo SNMP	24
2.6.5	Mecanismo de Transporte.....	25
2.7	RMON (<i>Remote Monitoring</i>).....	26
2.7.1	RMONv2.....	26
3	UM ESTUDO DE CASO SOBRE O GERENCIAMENTO NA REDE FARN.....	27
3.1	A REDE FARN.....	27
3.2	MONITORAMENTO SISTEMÁTICO	27
3.3	SOFTWARES DE GERENCIAMENTO	28
3.3.1	3COM NETWORK SUPERVISOR	29
3.3.2	MIBBROWSER	33
3.3.3	MRTG	37
4	CONCLUSÕES.....	40
	REFERENCIAL BIBLIOGRÁFICO.....	41

1 INTRODUÇÃO

A origem da idéia da rede de computadores, como a conhecemos hoje, remonta aos anos 60. Era a época da Guerra Fria entre as duas potências mundiais, os EUA e a União Soviética. As inovações na manipulação de dados eletrônicos provinham principalmente de iniciativas militares, nas quais tinham a intenção de proteger os importantes dados militares. A solução viável era uma rede eletrônica de dados. Os mesmos dados deveriam estar armazenados em diversos computadores, distantes uns dos outros (A HISTORIA, 2005).

A *Advanced Research Projects Agency* (ARPA), ou seja, agência de projetos e pesquisas avançadas, integrante do sistema militar americano, realizou o projeto idealizado. Foi por este motivo que, nos primeiros anos, a rede foi chamada de ARPA-Net. No final de 1969, foram conectados os primeiros quatro computadores ao ARPA-Net. Três anos mais tarde, já eram 40 (A HISTORIA, 2005).

A fusão dos computadores e das comunicações teve uma profunda influência na forma como os sistemas computacionais eram organizados. O conceito de "centro de computação" como uma sala com um grande computador ao qual os usuários levam seu trabalho para processamento, agora está completamente obsoleto. O velho modelo de um único computador atendendo a todas as necessidades computacionais da organização foi substituído pelas chamadas redes de computadores, nas quais os trabalhos são realizados por um grande número de computadores separados, mas interconectados (LOPES, 2003).

Atualmente as redes de computadores e os seus recursos associados, além das aplicações distribuídas, tem se tornado fundamental e de tal importância para uma organização, que elas basicamente "não podem falhar". Isto significa que o nível de falhas e de degradação de desempenho considerados aceitáveis está cada vez mais diminuindo, sendo este nível igual ate a zero, dependendo da importância da rede para uma instituição (GERENCIAMENTO, 2005).

De acordo com Lopes (2003):

Embora não se tenha conseguido estabelecer uma distinção entre as atividades de administração e de gerenciamento de redes, inicialmente, poderemos considerar que a administração de redes compreende o desempenho de processos destinados a projeção, implantação e manutenção do hardware e software básico utilizados no desenvolvimento de aplicações e serviços de rede - e que, gerenciamento de redes, compreende o monitoramento e o controle automatizado dos dispositivos (hardware e software) que

além de suas funções principais, foram instrumentalizados com funcionalidades de gerenciamento.

Gerenciar um ambiente, onde a inovação tecnológica ocorre em curtos períodos de tempo, torna-se cada vez mais uma tarefa de difícil execução. O aumento significativo no uso de recursos computacionais distribuídos e interligados, tem exigido a adoção do gerenciamento de redes como forma de aliviar e qualificar processos de monitoramento e controle de determinados recursos, aplicações e serviços de rede (LOPES, 2003).

Portanto essa pesquisa irá mostrar uma visão geral da tecnologia existente hoje para rede de computadores e demonstrar a necessidade de um gerenciamento de rede bem estruturada para deixá-la mais segura e confiável.

1.1 PROBLEMA DE PESQUISA

Um dos principais problemas que envolvem a gerência de redes hoje está relacionado ao tempo para a resolução e/ou detecção de um problema na rede. Quando uma rede é pequena por exemplo, rede de até 10 computadores, não se tem tanta dificuldade de resolver problemas, mas em uma grande empresa onde o número de máquinas e cabos é bastante considerável, faz-se necessário um gerenciamento de rede que dê a rapidez e a exatidão da solução dos problemas. Para isso existem hoje, softwares que dão quase que total controle ao gestor de redes, mostrando-lhe detalhes relacionados ao funcionamento, disposição, alarmes, de todos os hardwares ligados à rede (GERENCIAMENTO, 2005).

Diante destes fatos, o questionamento da pesquisa é saber quais os benefícios que se pode ter com a implantação de softwares de gerenciamento de rede.

1.2 OBJETIVOS

1.2.1 Objetivo geral

A monografia tem como objetivo principal demonstrar ferramentas (*softwares*) que produzam um gerenciamento mais consistente e seguro para uma rede de computadores.

1.2.2 Objetivos específicos

Os objetivos específicos são os de analisar os benefícios que os softwares de gerenciamento podem gerar para uma melhor gestão de uma rede de computadores e estudar o protocolo de gerenciamento de rede SNMP.

1.3 JUSTIFICATIVA

Essa monografia se justifica pela importância de se entender a necessidade de um gerenciamento de rede bem estruturado para obter a integridade dos dados, que nela transitam, através da utilização de ferramentas de gerenciamento.

Partindo do fato que problemas diversos podem surgir a qualquer momento, e estes podem gerar perdas irreparáveis, o gerente de rede deve estar preparado, através de softwares gerenciais que o auxiliam, para que no exato momento em que eles ocorram, sejam tomadas providências imediatas, inclusive a detecção rápida dos locais afetados.

2 REFERENCIAL TEÓRICO

2.1 REDES DE COMPUTADORES

A rede de computadores é um conjunto de computadores autônomos interconectados por diferentes tecnologias com o único objetivo de compartilhar todos os recursos disponíveis na rede ao alcance de todos os usuários (TANEMBAUM, 2003).

Segundo Lopes (2003):

Há modelos de redes de computadores, como por exemplo o modelo cliente/servidor, no qual os dados são armazenados em poderosos computadores chamados servidores. Em contraste, os funcionários têm em suas escrivaninhas máquinas mais simples, chamadas clientes, com as quais eles acessam dados remotos que encontram-se no servidor , pois estão ligados em rede. Outro modelo é o chamado ponto-a-ponto, com o objetivo de possibilitar a comunicação em um grupo livre, entre uma ou mais pessoas, não existindo assim, nenhuma divisão fixa entre cliente e servidores.

Computadores móveis, como *notebooks* e PDAs (*Personal Digital Assinants*), constituem um dos segmentos de mais rápido crescimento da indústria de informática – As redes sem fio. O objetivo é o de acessar arquivos remotos e se conectar a máquinas distantes, em qualquer parte do planeta. Devemos observar uma distinção entre redes sem fio fixas e sem fio móveis.

As redes também podem ser locais, conhecida também como LAN (*Local Área Network*), entre cidades conhecida como MAN (*Metropolitan Área Network*) e entre países ou continentes chamada de WAN (*Wide Área Network*).

As redes locais são privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais de empresas, permitindo o compartilhamento de recursos, com exemplo, impressoras e a troca de informações.

Uma rede metropolitana abrange uma grande área geográfica, com freqüência um país ou continente.

Existem muitas redes no mundo, com freqüência apresentando diferentes tipos de hardware e software. Normalmente, as pessoas conectadas a redes distintas precisam se comunicar entre si. Para que esse desejo se torne realidade, é preciso que se estabeleçam conexões entre redes quase sempre incompatíveis, às vezes por meio de máquinas chamadas *gateways*, que estabelecem a conexão e fazem a conversão necessária, tanto em termos de

hardware quanto de software. Para este conjunto de redes interconectadas é dado o nome de inter-rede ou bastante conhecido como Internet.

2.2 GERÊNCIA DE REDES

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 da rede já em uso.

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, permitindo efetuar a contabilização e análise de tendências.

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

Para Gerenciamento (2005), a área de gerência de redes foi inicialmente impulsionada pela necessidade de monitoração e controle do universo de dispositivos que compõem as redes de comunicação.

Para Lopes (2003, p. 08):

O objetivo de gerência de redes é monitorar e controlar os elementos da rede, assegurando um certo nível de qualidade de serviço. Para realizar esta tarefa, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Um sistema de gerência de redes pode ser definido como uma coleção de ferramentas integradas para a monitoração e o controle da rede.

A arquitetura geral dos sistemas de gerência de redes apresenta quatro componentes básicos mostrado na Figura 1: elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência.

Os elementos gerenciados possuem um software especial que permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência. A estação de gerência oferece uma interface através da quais usuários autorizados podem gerenciar a rede. Para que a troca de informações seja possível na rede, é necessário que se fale o mesmo idioma, ou seja,

tenham o mesmo protocolo de gerência, na qual permite operações de monitoramento (leitura) e controle (escrita).

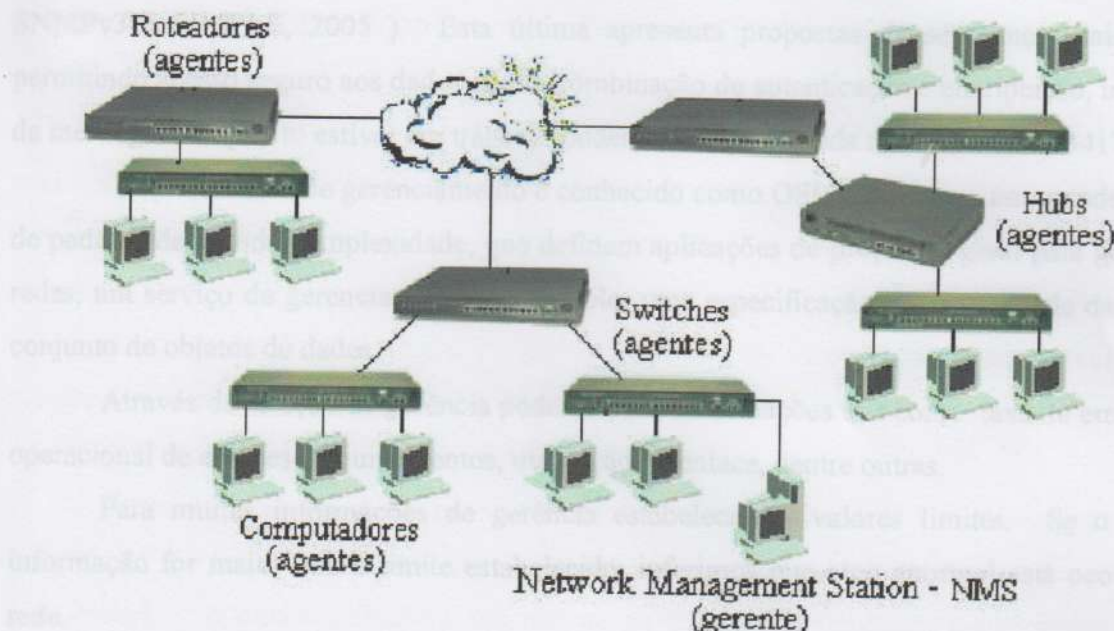


Figura 1: Esboço dos componentes básicos (Fonte: GERENCIAMENTO, 2005)

As informações de gerência definem os dados que podem ser referenciados em operações de controle de gerência, isto é, dados sobre os quais gerente e agente conversam. O gerente é o software de estação que conversa diretamente com os agentes e o agente é o software dos elementos gerenciados.

Roteadores, comutadores, repetidores, impressoras, servidores e estações clientes, todos estes equipamentos podem ter agentes instalados. A estação de gerência deve obter informações de gerência destes gerentes usando o protocolo SNMP. O protocolo SNMP (*Simple Network Management Protocol*) refere-se a um conjunto de padrões para gerenciamento que inclui um protocolo, uma especificação de estrutura de dados, e um conjunto de objetos de dados (GERENCIAMENTO, 2005). A versão SNMPv2 trouxe algumas mudanças não somente na segurança como também adicionou outras operações e tipos de dados. Esta versão chamada de SNMPv2 pode ser encontrada nas RFCs 1441, 1445, 1446, 1448, 1449. Porém as deficiências

das duas primeiras versões, como por exemplo, contadores grandes, segurança limitada, protocolo WAN pobre, acabaram por abrir espaço para o surgimento da terceira versão, o SNMPv3 (SIMPLE, 2005). Esta última apresenta propostas de segurança mais robusta, permitindo acesso seguro aos dados com a combinação de autenticação e encriptação, integridade da mensagem enquanto estiver em trânsito, podendo ser encontrada da RFC 3411 a 3417.

Outro sistema de gerenciamento é conhecido como OSI. Refere-se a um grande conjunto de padrões de grande complexidade, que definem aplicações de propósito geral para gerência de redes, um serviço de gerenciamento e protocolo, uma especificação de estrutura de dados, e um conjunto de objetos de dados.

Através da estação de gerência pode-se obter informações tais como: taxa de erros, estado operacional de enlaces e equipamentos, utilização de enlace, dentre outras.

Para muitas informações de gerência estabelecemos valores limites. Se o valor da informação for maior que o limite estabelecido, inferimos que algo anormal está ocorrendo na rede.

Não importante quanto obter estas informações é saber interpreta-las. Por exemplo, em determinado momento, a estação de gerência informa que a taxa de erros de um certo enlace é 1%.

Quando a estação de gerência percebe que uma interface parou de operar, por exemplo, um alarme pode ser gerado.

Além do sistema de gerência de redes, outras ferramentas nos auxiliam a gerenciar uma rede. Dentre elas encontram-se analisadores de protocolos e outras ferramentas mais simples, como os comandos *PING*, *TRACEROUTE* e *NETSTAT*, disponíveis sob vários sistemas operacionais.

Como os analisadores de protocolos, podemos ver quais dados estão trafegando na rede. Eles nos permitem tirar raios-x da rede, sendo, portanto, ferramentas importantes de gerência.

2.3 O GERENTE DA REDE

Um dos objetivos da gerência de redes é prevenir e solucionar problemas na rede. Geralmente esta tarefa é realizada por uma equipe. O gerente da equipe de gerência de rede não deve ser, necessariamente, um técnico em redes. O gerente tem um certo conhecimento em redes, mas não no nível do suporte técnico. Dentre as atividades deste gerente encontram-se:

avaliar o desempenho da sua equipe de suporte, solicitar compra de equipamentos, aplicações ou outros recursos necessários. Providenciar treinamento adequado para a equipe, re-escalonar a solução de problemas para outros membros da equipe quando a solução demora, dentre outras (LOPES, 2003).

É comum que na equipe comandada pelo gerente de redes, existirem profissionais que executem quatro tarefas distintas: O pessoal do *help desk* para lidar com alguns problemas que forem reportados. Com relação ao que os usuários usam como: Computadores nas suas mesas, aplicações, serviços, problemas na rede, etc.

A equipe do suporte técnico é quem pode solucionar os problemas mais abrangentes que surgirem ou que possam surgir e que não foram solucionados pela equipe de *help desk* ou pelo operador do sistema.

O operador da rede é o profissional encarregado de acompanhar os alarmes gerados pela estação de gerência. Quando, por exemplo, um equipamento passa para o estado não operacional, o operador perceberá um alarme na estação de gerência, e percebendo que um problema está ocorrendo ou pode ocorrer, ele tenta resolver o mesmo ou o encaminha à equipe de suporte técnico (LOPES, 2003).

2.4 HARDWARE DE REDES

2.4.1 Topologias das Redes de Computadores

Ao longo da historia das redes, varias topologias foram experimentadas, com maior ou menor sucesso. Os três tipos abaixo são esquemas básicos empregados na conexão dos computadores (REDES, 2005). Os outros são variantes deles:

- **Estrela** - Todas as conexões partem de um ponto central (concentrador), normalmente um *hub* ou *switch*. É o modelo mais utilizado atualmente.
- **Anel** - Todos os computadores são conectados em um anel. É a topologia das redes *Token Ring*, popularizadas pela IBM nos anos 80. Hoje, esse modelo é mais utilizado em sistemas de automação industrial.
- **Barramento** - Os computadores são conectados num sistema linear de cabeamento em sequência. Esse arranjo era usado nas primeiras gerações de redes *Ethernet*. Está sendo lentamente abandonado.

2.4.2 Cabos

O projeto de cabeamento de uma rede, que faz parte do meio físico usado para interligar computadores, é um fator de extrema importância para o bom desempenho de uma rede. Esse projeto envolve aspectos sobre a taxa de transmissão, largura de banda, facilidade de instalação, imunidade a ruídos, confiabilidade, custos de interface, exigências geográficas, conformidade com padrões internacionais e disponibilidades de componentes.

Em matéria de cabos, os mais utilizados são os cabos de par trançado, os cabos coaxiais e cabos de fibra óptica. Cada categoria tem suas próprias vantagens e limitações, sendo mais adequado para um tipo específico de rede.

2.4.2.1 Cabo de Par Trançado

É o mais usado, pois tem um melhor custo benefício, ele pode ser comprado pronto em lojas de informática, ou feito sob medida, ou ainda produzido pelo próprio usuário, e ainda são 10 vezes mais rápidos que os cabos coaxiais (REDES, 2005).

Vantagens

- **Preço.** Mesma com a obrigação da utilização de outros equipamentos na rede, a relação custo beneficia se torna positiva.
- **Flexibilidade.** Como ele é bastante flexível, ele pode ser facilmente passado por dentro de conduítes embutidos em paredes.
- **Facilidade.** A facilidade com que se pode adquirir os cabos, pois em qualquer loja de informática existe esse cabo para venda, ou até mesmo para o próprio usuário confeccionar os cabos.
- **Velocidade.** Atualmente esse cabo trabalha com uma taxa de transferência de 100 Mbps.

Desvantagens

- **Comprimento.** Sua principal desvantagem é o limite de comprimento do cabo que é de aproximadamente 100 por trecho.
- **Interferência.** A sua baixa imunidade à interferência eletromagnética, sendo fator preocupante em ambientes industriais.

2.4.2.2 Cabos Coaxiais

Permitem que os dados sejam transmitidos através de uma distância maior que a permitida pelos cabos de par trançado sem blindagem (UTP), mas por outro lado não são tão flexíveis e são mais caros que eles. Outra desvantagem é que a maioria delas requer o barramento ISA, não encontradas nas Placas mães novas (REDES, 2005).

Vantagens

- **Interferência.** Imunidade à interferência eletromagnética de baixa intensidade.

Desvantagens

- **Custo.** elevado, instalação mais difícil e mais fragilidade.
- **Instalação.** instalação mais difícil e mais fragilidade, se o terminador for retirado do cabo, toda a rede sai do ar.

2.4.2.3 Cabos de Fibra-ótica

Permitem transmissões de dados a velocidades muito maior, e são completamente imunes a qualquer tipo de interferência eletromagnética, porém, são muito mais caros e difíceis de instalar, demandando equipamentos mais caros e mão de obra mais especializada. Apesar da alta velocidade de transferência, as fibras ainda não são uma boa opção para pequenas redes devido ao custo (REDES, 2005).

Vantagens

- **Distância.** Maior alcance. 40 Km
- **Interferência.** Imunidade a interferências eletromagnéticas.
- **Velocidade.** Maior velocidade. De 10 a 15 GHz

Desvantagens

- **Custo.** Tecnologia caríssima.

2.4.2.4 Wireless

A palavra wireless provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios. Wireless então caracteriza qualquer tipo de conexão para transmissão de informação sem a

utilização de fios ou cabos. Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar. Pela extrema facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais. Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), bluetooth e Wi-Max (WIRELESS, 2005).

Vantagens

- **Mobilidade.** Acesso em tempo real em qualquer lugar.
- **Custo de manutenção.** Baixo
- **Interferência.** Alta imunidade a ruídos.

Desvantagens

- **Custo de aquisição.** Tecnologia caríssima.
- **Segurança.** É mais fácil de ser burlada.

2.4.3 Equipamentos de Conectividade

O primeiro componente de uma rede é justamente a **placa de rede**. Além de funcionar como um meio de comunicação, a placa de rede desempenha várias funções essenciais, como a verificação da integridade dos dados recebidos e a correção de erros.

De acordo com Redes (2005):

O **repetidor** é um dispositivo responsável por ampliar o tamanho máximo do cabeamento da rede. Ele funciona como um amplificador de sinais, regenerando os sinais recebidos e transmitindo esses sinais para outro segmento da rede.

Hubs são dispositivos concentradores, responsáveis por centralizar a distribuição dos quadros de dados em redes fisicamente ligadas em estrelas. Funcionando assim como uma peça central, que recebe os sinais transmitidos pelas estações e os retransmite para todas as demais (REDES, 2005).

Bridges são repetidores inteligentes. Ela tem a capacidade de ler e analisar os quadros de dados que estão circulando na rede. Com isso ela consegue ler os campos de endereçamentos MAC do quadro de dados. Fazendo com que a ponte não replique para outros segmentos de origem. Outro papel que a ponte, em principio poderia ter, é o de interligar redes que possuem arquiteturas diferentes (REDES, 2005).

Switches são hubs que, em vez de ser um repetidor, são pontes. Com isso, em vez dele replicar os dados recebidos para todas as suas portas, ele envia os dados somente para o micro que requisitou os dados através da análise da camada de link de dados onde possui o endereço MAC da placa de rede do micro, dando a idéia assim de que o switch é um hub inteligente (REDES, 2005).

Roteadores são pontes que operam na camada de Rede do modelo OSI (camada três), essa camada é produzida não pelos componentes físicos da rede (Endereço MAC das placas de rede, que são valores físicos e fixos), mais sim pelo protocolo mais usado hoje em dia, o TCP/IP, o protocolo IP é o responsável por criar o conteúdo dessa camada. Isso Significa que os roteadores não analisam os quadros físicos que estão sendo transmitidos, mas sim os datagramas produzidos pelo protocolo que no caso é o TCP/IP, os roteadores são capazes de ler e analisar os datagramas IP contidos nos quadros transmitidos pela rede. O papel fundamental do roteador é poder escolher um caminho para o datagrama chegar até seu destino (REDES, 2005).

2.5 PROTOCOLOS DE REDE

Toda a parte física de rede: cabos, placas, *hubs*, etc., serve para criar um meio de comunicação entre os micros da rede, mas para haver realmente a comunicação, é preciso que ambos utilizem o mesmo protocolo de rede.

Um protocolo é um conjunto de regras que definem como os dados serão transmitidos; como será feito o controle de erros e retransmissão de dados; como os computadores serão endereçados dentro da rede (MORIMOTO, 2005).

Um micro com o NetBEUI instalado, só será capaz de se comunicar através da rede com outros micros que também tenham o protocolo NetBEUI, por exemplo. Graças aos protocolos, é possível que computadores rodando diversos sistemas operacionais, ou mesmo computadores de arquiteturas diferentes se comuniquem, basta apenas que todos tenham um protocolo em comum (MORIMOTO, 2005).

O TCP/IP, por exemplo, é uma família de protocolos suportada por praticamente todos os sistemas operacionais. O uso do TCP/IP é que permite o milagre de computadores de arquiteturas totalmente diferentes, como PCs, Macs, *Mainframes* e até mesmo, telefones celulares e micros de bolso poderem se comunicar livremente através da Internet (MORIMOTO, 2005).

NetBEUI é uma espécie de “vovô protocolo”, pois foi lançado pela IBM no início da década de 80 para ser usado junto com o IBM PC *Network*. Ao contrário de outros protocolos, o NetBEUI foi concebido para ser usado apenas em pequenas redes.

O protocolo **IPX/SPX** foi desenvolvido pela *Novell*, para ser usado em seu *Novell Netware*. Como o *Netware* acabou tornando-se muito popular, outros sistemas operacionais de rede, incluindo o Windows, passaram a suportar esse protocolo.

O **IP** é um protocolo de identificação que cada micro ligado à rede recebe, sendo o mesmo único. O endereço IP é dividido em duas redes. A primeira identifica a rede ao qual o computador esta conectado e a segunda identifica o computador dentro da rede.

O protocolo **DHCP** serve para que os *hosts* da rede obtenham endereço ip automaticamente, para evitar erros na hora de configurar manualmente uma rede.

O **DNS** permite usar nomes amigáveis ao invés de endereços IPs para acessar servidores. Ao invés de você digitar os números do endereço IP, pode-se digitar um nome fantasia, e o protocolo se encarregará de converter esse nome para o endereço real e poder acessa-lo. Já o **WINS** tem a mesma função do DNS, só que é usado apenas pela família Windows, ao contrário do DNS que aceita qualquer sistema operacional (MORIMOTO, 2005).

O **HTTP** é o protocolo usado para a transmissão de dados no sistema *World-Wide Web*. Cada vez que você aciona um link, seu *browser* realiza uma comunicação com um servidor da Web através deste protocolo.

O **SNMP** é o protocolo de rede, desenvolvido na família de protocolos TCP/IP, encarregado de possibilitar uma troca de mensagens com informações de gerência entre dispositivos de uma rede.

2.6 O PROTOCOLO SNMP

O **SNMP** – *Simple Network Management Protocol* é o protocolo desenvolvido e recomendado para o gerenciamento de redes TCP/IP. Definido no nível de aplicação, o SNMP utiliza os serviços do protocolo UDP (*User Datagram Protocol*) para a troca de mensagens através da rede ajudando administradores a localizar e corrigir problemas da rede (LIMA, 2005).

2.6.1 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 podem conter objetos gerenciáveis. Estes podem ser informações sobre o hardware, parâmetros de configuração, estatísticas de performance, entre outros (LIMA, 2005).

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 agente, como mostra a Figura 2. Nessas trocas de informações, são aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede.

2.6.2 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.

A seguir, 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 (GERENCIAMENTO, 2005).

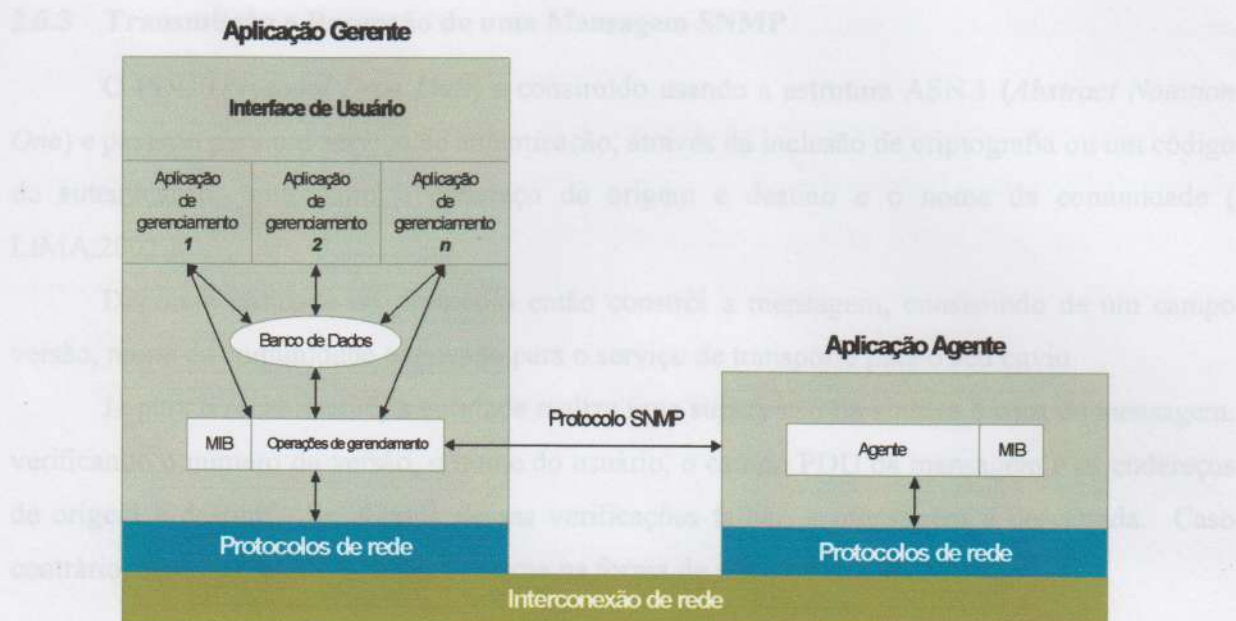


Figura 2 : Posicionamento de agentes e gerentes (Fonte: GERENCIAMENTO, 2005)

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.

GET-NEXT: Geralmente é usado para solicitar valores de uma tabela da MIB. Após a solicitação do primeiro valor usando o comando Get, os valores seguintes são solicitados usando este comando (GERENCIAMENTO, 2005).

SET: O gerente solicita aos agentes a modificação no valor de uma variável de um objeto gerenciado (GERENCIAMENTO, 2005).

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 (GERENCIAMENTO, 2005).

TRAP: um agente informa ao gerente sobre a ocorrência de um evento específico (GERENCIAMENTO, 2005).

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

2.6.3 Transmissão e Recepção de uma Mensagem SNMP

O PDU (*Protocol Data Unit*) é construído usando a estrutura ASN.1 (*Abstract Notation One*) e passado para um serviço de autenticação, através da inclusão de criptografia ou um código de autenticação, junto com o endereço de origem e destino e o nome da comunidade (LIMA,2002).

Depois a entidade do protocolo então constrói a mensagem, consistindo de um campo versão, nome da comunidade e passado para o serviço de transporte para o seu envio.

Já para o recebimento, a entidade realiza uma supervisão na sintaxe básica da mensagem, verificando o número da versão, o nome do usuário, o campo PDU da mensagem e os endereços de origem e destino. Se alguma dessas verificações falhar, a mensagem é descartada. Caso contrário, o serviço de autenticação retorna na forma de um objeto ASN.1.

2.6.4 Segurança no Protocolo SNMP

O protocolo SNMP pode realizar operações de reconfiguração na rede alterando características de equipamentos ou até desligando máquinas. O controle é feito através da verificação do conteúdo de um campo especial no pacote do SNMP, denominado comunidade (LIMA,2002). A comunidade é definida como sendo o relacionamento entre duas entidades do SNMP. É definida na MIB do agente 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 desta comunidade, é possível que o agente realize uma verificação da integridade do gerente realizando autenticação e políticas de acesso através deste campo. Sem o conhecimento prévio da comunidade de um determinado equipamento gerenciável, será impossível a qualquer aplicação de gerência, acessar as informações da MIB. A maioria dos fornecedores de hardware e software disponibilizam seus produtos com strings de comunidades padrão, "public" para comunidade read-only. Quando um equipamento destes for ativado em uma rede, principalmente se conectada na internet, sem que o agente altere a community padrão, possibilita que qualquer pessoa possa se apoderar do equipamento e com isso ter acesso tanto

para leitura como para escrita. Uma vez que alguém esteja de posse do equipamento, é possível alterar rotas e até mesmo indisponibilizar serviços.

O 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 aumentar a segurança no acesso aos equipamentos.

Segue abaixo algumas características da MIB segundo LIMA (2002):

- 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 nas duas primeiras versões do SNMP.

2.6.5 Mecanismo de Transporte

O SNMP assume que o caminho de comunicação é uma sub-rede 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). O primeiro tem como vantagem a velocidade.

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 saber que o SNMP é independente de transporte e pode ser implementado em outros transportes como: TCP, mapeamento direto sobre *Ethernet*, X25 e ATM.

2.7 RMON (*REMOTE MONITORING*)

A especificação RMON é uma definição de uma MIB. Seu objetivo é definir funções de monitoração e interface 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 esses 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 (LIMA, 2002).

De acordo com LIMA (2002), 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 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-los 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.
- **Deteção 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 sub-rede. Por exemplo, pode determinar que *host* gera a maior parte do tráfego ou erros na sub-rede.
- **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.

2.7.1 RMONv2

O RMON-II, sucessor natural do RMON, realiza um mapeamento de todos os grupos RMON nos mais populares protocolos de rede como IP, IPX, DECnet, AppleTalk, Vines e protocolos OSI em geral. Oferece, além disso, a capacidade de gerenciamento em qualquer um dos 7 níveis da camada OSI, além de permitir a administração de aplicativos distribuídos como Lotus Notes e Sybase SQL (PROTOCOLO, 2005).

3 UM ESTUDO DE CASO SOBRE O GERENCIAMENTO NA REDE FARN

3.1 A REDE FARN

A FARN disponibiliza os principais recursos de rede: DNS, Servidor *Web*, *E-mail*, controladores de domínio, *Proxy*, *Firewall*, dentre outros.

O controlador de domínios 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 domínios ACADEMICO controla as redes acadêmicas, como os laboratórios.

O *Firewall* realiza a tarefa de tradução de endereços (transformar endereços internos, que são privados à Intranet da FARN, em um endereço válido antes de enviar um pacote para o mundo externo à rede), bloquear requisições de acessos externos (exceto para as permitidas nas regras de roteamento) e limitar o uso de serviços de rede da Internet na Intranet.

O Linux que implementa o servidor de *e-mails* encontra-se na *Extranet* (parte visível pelos usuários da Internet), chamada de **DMZ** (Zona Desmilitarizada), para permitir que os *e-mails* provenientes da Internet consigam chegar neste servidor, além de permitir aos usuários da FARN acessarem suas mensagens quando estiverem fora da rede. A topologia geral da Rede FARN é mostrada na Figura 3.

Ligadas ao *Firewall* há 3 sub-redes, além da DMZ: a rede de laboratórios de alunos chamada de Acadêmica, a rede Administrativa e a rede dos colégios Henrique Castriciano e Escola Doméstica.

3.2 MONITORAMENTO SISTEMÁTICO

Através do uso das ferramentas de gerência abordadas neste trabalho, será possível a criação de um procedimento de acompanhamento sistemático das informações da Rede. Este procedimento possibilita a previsão de lentidão em um determinado ponto da rede, picos de utilização, falhas de recursos, dentre outros.

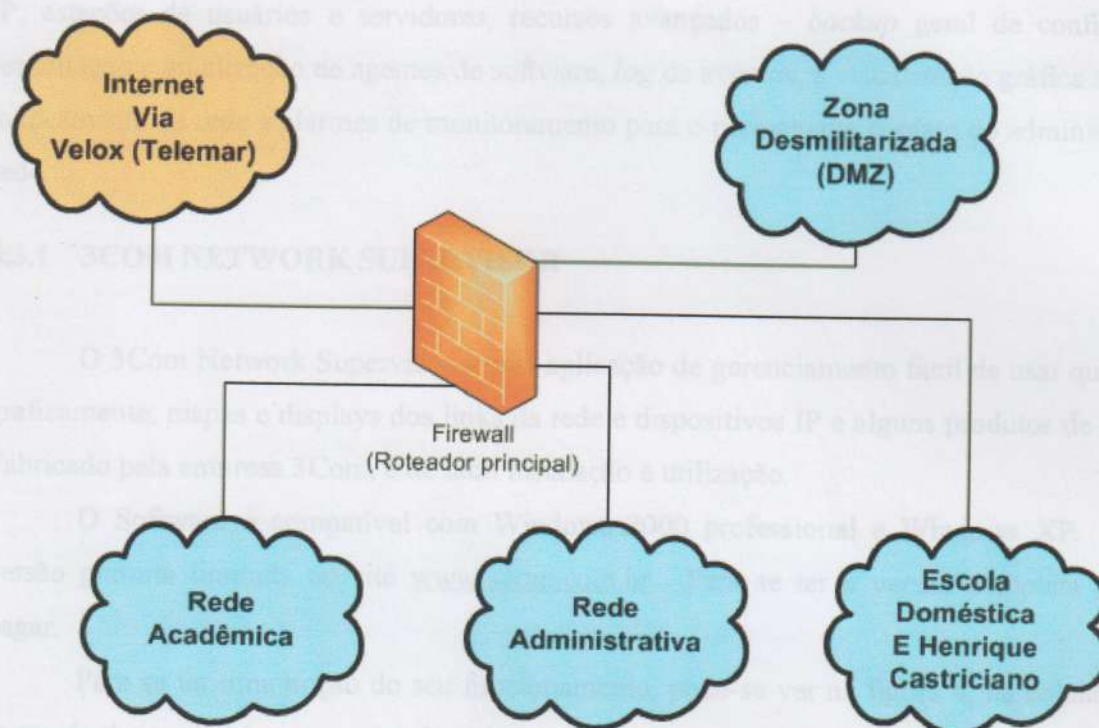


Figura 3: Topologia da Rede FARN

O monitoramento sistemático deverá prever ainda, ações de contingência em casos críticos, pessoal responsável pela execução das tarefas, relatório de execução das tarefas, relatórios gerenciais periódicos descrevendo status e recomendações, possibilitando o gerenciamento eficaz da rede.

3.3 SOFTWARES DE GERENCIAMENTO

Os softwares para gerenciamento de redes trabalham para simplificar o trabalho do pessoal de TI e melhorar a operação e a confiabilidade da rede. Existem avançados recursos como o reconhecimento e mapeamento de dispositivos de rede, ferramentas de configuração, programas de instalação de dispositivos e ferramentas de solução de problemas que podem localizar e reparar rapidamente os problemas da rede (SOFTWARE, 2005).

Pode ser feito o monitoramento e controle de sofisticadas redes de dados ou dados/telefonia, incluindo *switches*, roteadores, *access points wireless*, dispositivos de telefonia

IP, estações de usuários e servidores, recursos avançados – *backup* geral de configurações, restauração e atualização de agentes de software, *log* de eventos, a visualização gráfica através de mapeamento da rede e alarmes de monitoramento para o permanente contato do administrador da rede.

3.3.1 3COM NETWORK SUPERVISOR

O 3Com Network Supervisor é uma aplicação de gerenciamento fácil de usar que mostra, graficamente, mapas e displays dos links da rede e dispositivos IP e alguns produtos de terceiros. Fabricado pela empresa 3Com, é de fácil instalação e utilização.

O Software é compatível com Windows 2000 professional e Windows XP. Há uma versão gratuita limitada no site www.3com.com.br. Para se ter a versão completa é preciso pagar.

Para se ter uma noção do seu funcionamento, pode-se ver na figura 4, na coluna do lado esquerda da janela há uma árvore de todos os equipamentos existentes na rede mostrando através de cores o seu estado atual. Se for branco, o equipamento foi descoberto na rede, mas não está sendo gerenciado. Se for verde, significa equipamento gerenciado e sem problemas. Já se for vermelho, o equipamento gerenciado encontra-se com algum problema.

No gráfico mostrado na coluna do lado direito, vêem-se os equipamentos na forma como eles estão dispostos fisicamente na rede. Com este gráfico, o gerente pode visualizar prontamente quais os problemas existentes na rede e sua localização.

Com apenas um clique com o botão direito em cima da representação gráfica de qualquer computador conectado na rede, como mostra a Figura 4, tem-se acesso a diversas ferramentas que auxiliam o gerente, desde fazer testes em equipamentos de conectividade até gravar informações no mesmo.

Na barra de ferramentas do software, pode-se ver o que está de errado no equipamento. Se está tudo certo, o ícone "All OK" aparece. Se há algum problema, o ícone muda para "Alert". Vêem-se as formas de alerta que o programa pode dar ao gerente da rede, como mostra a Figura 5. Na opção "Alerts" é possível visualizar um relatório com todos os eventos acontecidos na rede, mostrando data, hora, equipamento, e local do acontecimento. Por último tem-se o "Show Monitoring" que mostra o monitoramento detalhado do equipamento mostrado na Figura 7.

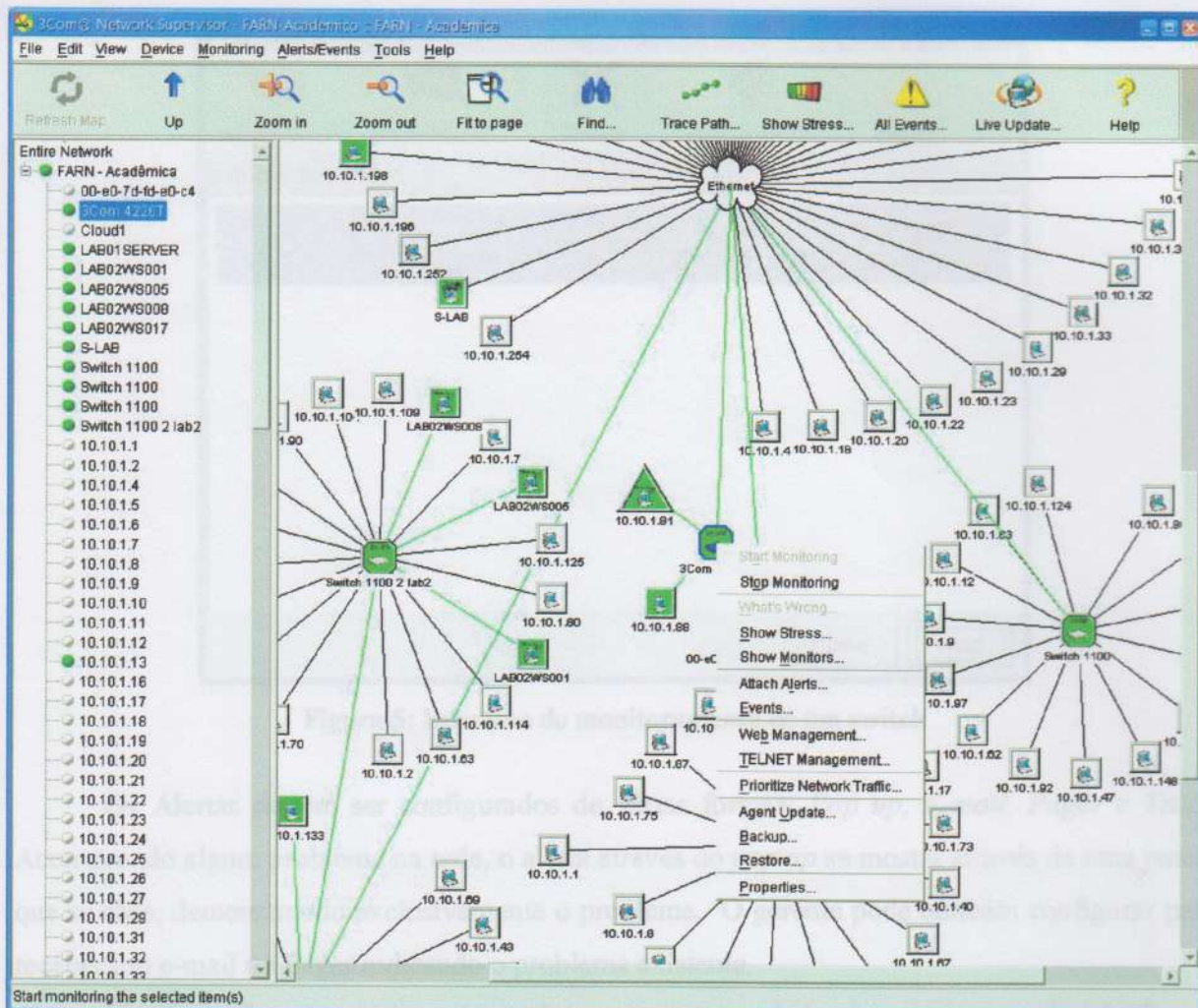


Figura 4: Interface do Network Supervisor

Na Figura 5 vê-se o monitoramento do nível de utilização do equipamento de conectividade através de um gráfico. Na barra de ferramentas do software onde está escrito *"What's Wrong"*, pode ser visto o que está de errado no equipamento. Já onde está escrito *"Attach Alerts"* vê-se as formas de alerta que o programa pode dar ao gerente da rede, como mostra a Figura 6. Na opção *"Events"* é possível visualizar um relatório com todos os eventos acontecidos na rede, mostrando data, hora, equipamento, e local do acontecimento. Por último tem-se o *"Show Monitoring"* que mostra a monitoração detalhada do equipamento mostrada na Figura 7.

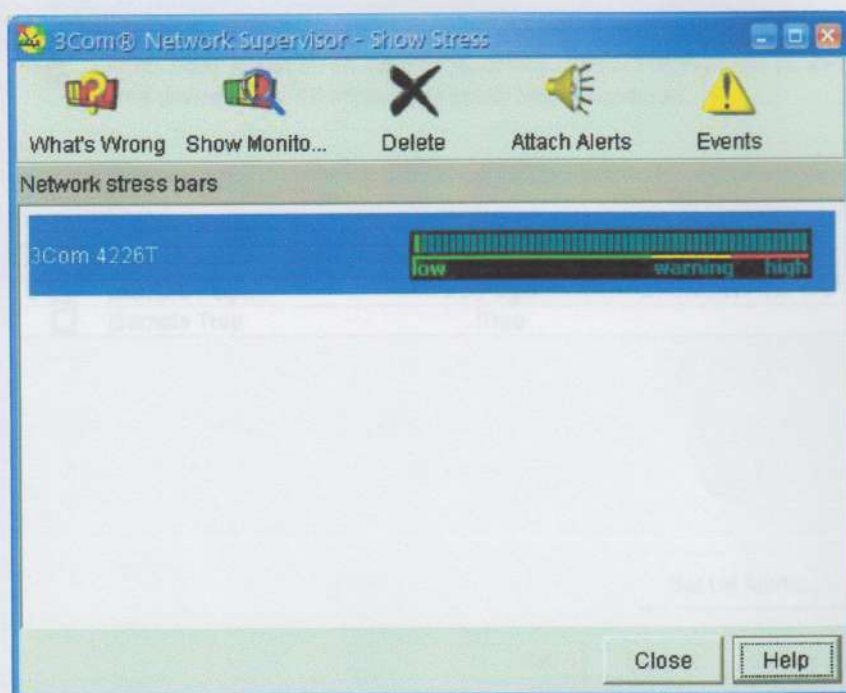


Figura 5: Interface do monitoramento de um switch

Os Alertas podem ser configurados de várias formas: *Pop up*, *E-mail*, *Pager* e *Trap*.. Acontecendo algum problema na rede, o alerta através do *pop up* se mostra através de uma janela que se abre, demonstrando exclusivamente o problema. O gerente pode também configurar para receber um e-mail ou Pager indicando o problema existente.

Na Figura 7, pode-se ver a página de monitoramento do hardware, serviço *ping* de IP, nós de ligação, estabilidade da rede e as portas do equipamento de conectividade.

Através desta ferramenta, pode-se visualizar o nível de utilização de cada um dos quesitos citados anteriormente, com a opção de selecionar qual se quer monitorar, podendo-se aplicar um estresse no equipamento através de um comando para avaliá-lo através de gráfico que mostra o seu nível do estresse. As portas do equipamento também podem ser avaliadas na forma de utilização através do gráfico, além de verificar quais portas estão sendo usadas, mostrando até a sua posição física no equipamento.

Figura 7: Interface do monitoramento de ligação

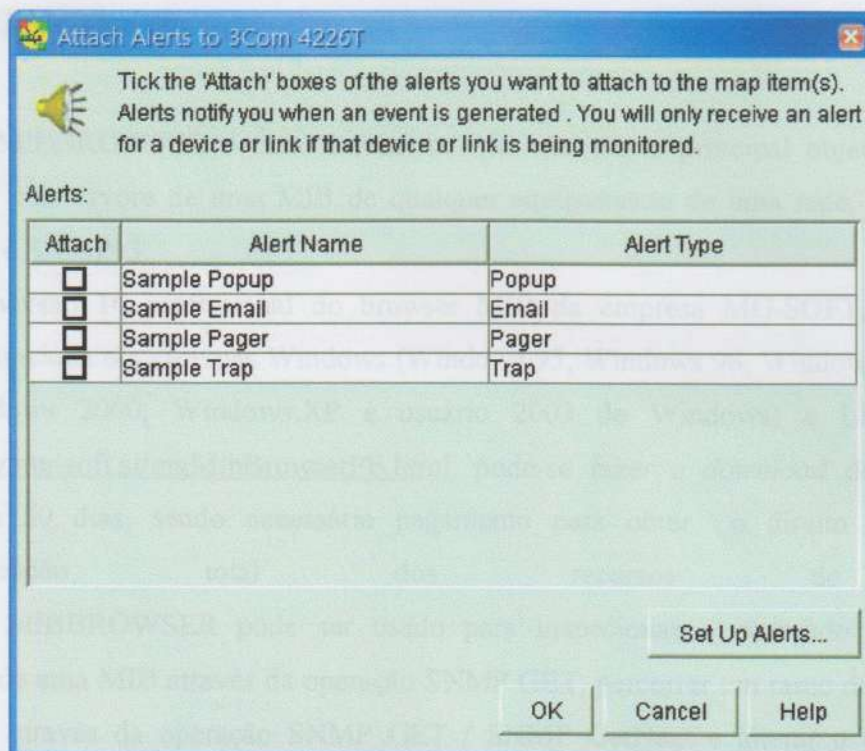


Figura 6: Interface das formas de Alerta

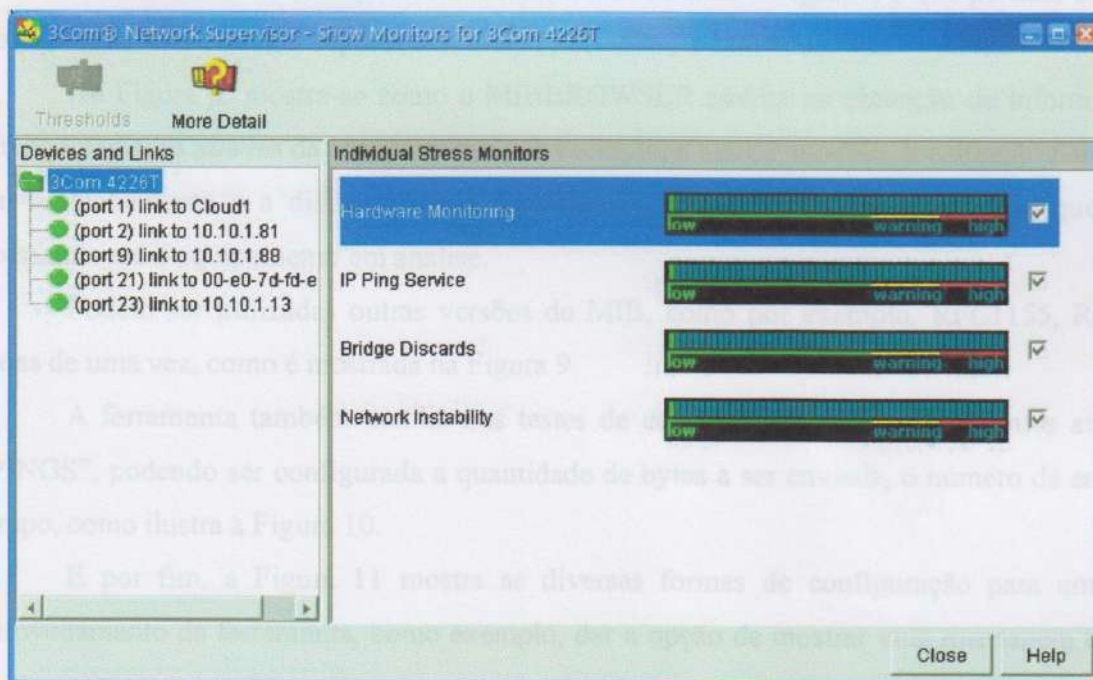


Figura 7: Interface do monitoramento detalhado

3.3.2 MIBBROWSER

O MIBBROWSER é uma ferramenta que tem como principal objetivo permitir uma navegação pela árvore de uma MIB de qualquer equipamento de uma rede, usando SNMPv1, SNMPv2c e SNMPv3.

A versão 10 profissional do browser MIB da empresa MG-SOFT, é extremamente flexível. Funciona em sistemas Windows (Windows 95, Windows 98, Windows MIM, Windows NT, Windows 2000, Windows.XP e usuário 2003 de Windows) e Linux. No site <http://www.mg-soft.si/mgMibBrowserPE.html>, pode-se fazer o *download* do programa, com licença de 30 dias, sendo necessário pagamento para obter o direito de atualização e disponibilização total dos recursos do software.

O MIBBROWSER pode ser usado para inspecionar o conteúdo de uma variável específica de uma MIB através da operação SNMP GET, percorrer um ramo de uma árvore MIB facilmente através da operação SNMP GET / SNMP GetNext e alterar o conteúdo de uma variável em uma MIB através da SNMP SET, além de permitir a captura de pacotes SNMP TRAPS.

A ferramenta também possui um compilador de MIB integrado, o que permite incorporar novas MIBs. Ela também suporta o SNMPv1, SNMPv2 e SNMPv3.

Na Figura 8, mostra-se como o MIBBROWSER auxilia na obtenção de informações de um equipamento através da árvore, como por exemplo, a marca, modelo, localização física, horas em funcionamento e a distância de pontos de conectividade do computador em que se está acessando até o equipamento em análise.

Podem ser utilizadas outras versões de MIB, como por exemplo, RFC1155, RFC1213, todas de uma vez, como é mostrada na Figura 9.

A ferramenta também auxilia nos testes de conectividade dos equipamentos através de "PINGS", podendo ser configurada a quantidade de bytes a ser enviada, o número de envios e o tempo, como ilustra a Figura 10.

E por fim, a Figura 11 mostra as diversas formas de configuração para um melhor aproveitamento da ferramenta, como exemplo, dar a opção de mostrar uma mensagem tipo *pop-*

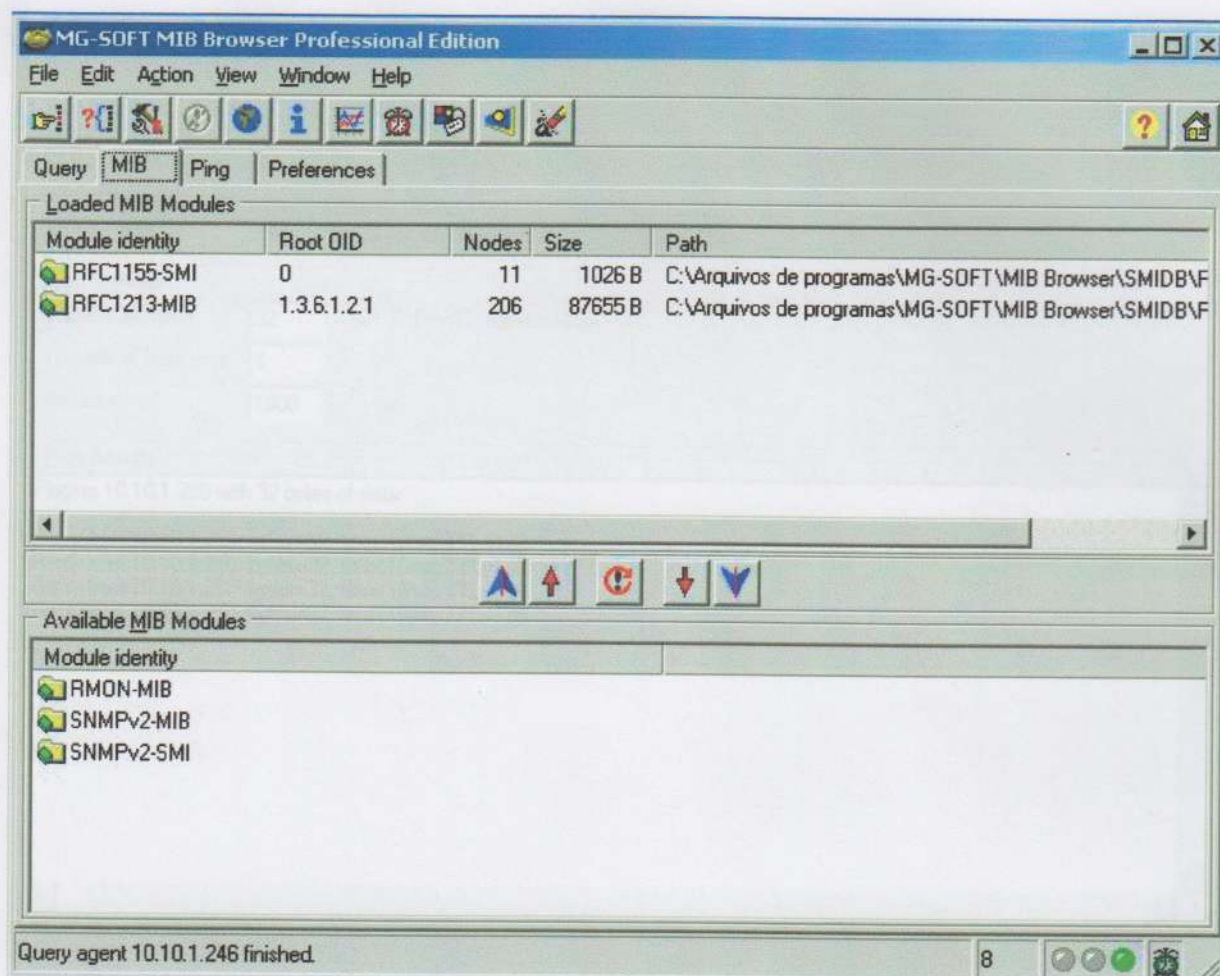


Figura 9: Versões de MIBs pré-instaladas com o MIB Browser

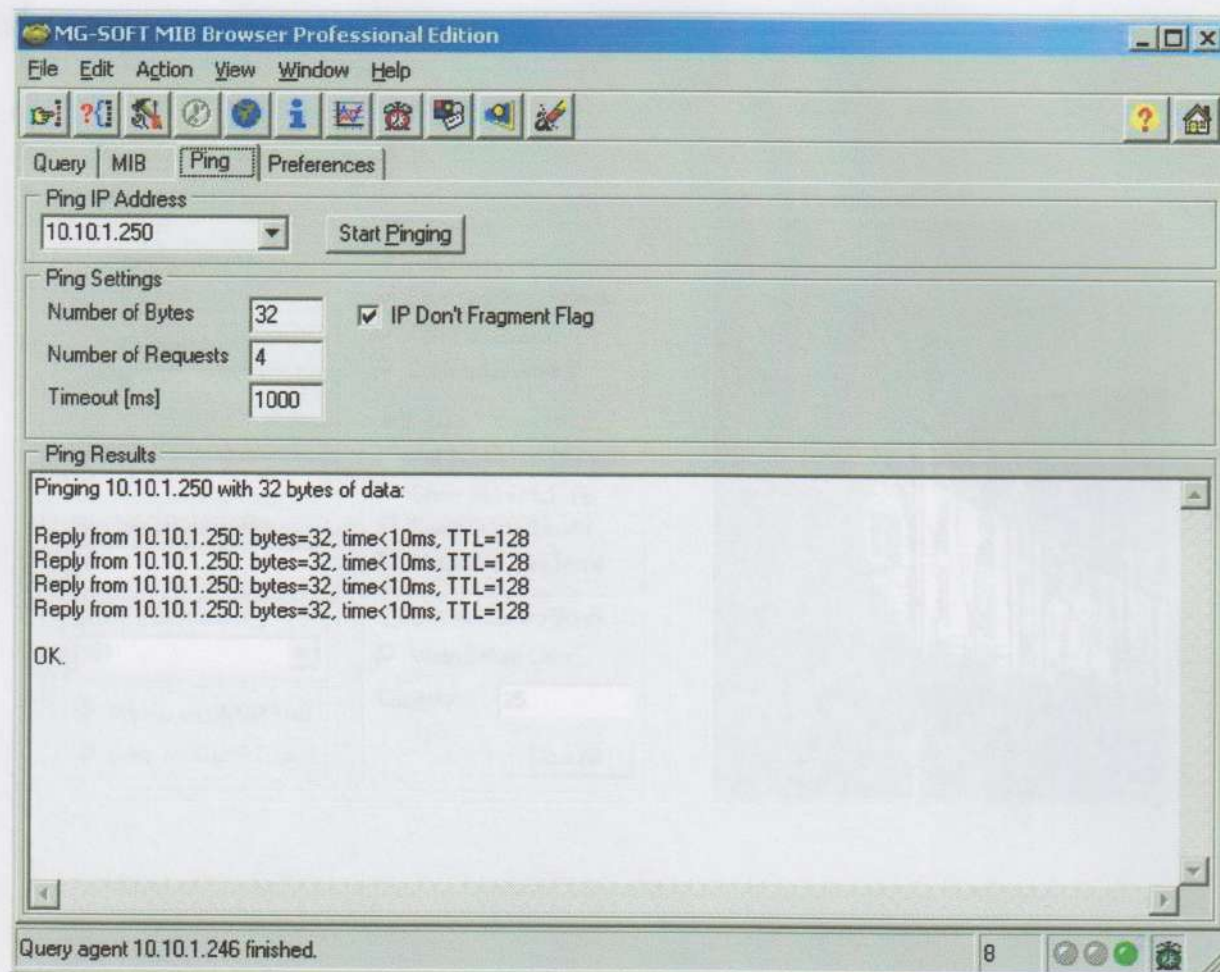


Figura 10: Testando a conectividade com o PING do MIB Browser

3.3.3 MRTG

O *Multi Router Traffic Grapher* (MRTG) é uma ferramenta para monitorar o estado da rede e a análise de tendências.

Esta ferramenta é composta de um pacote de pequenos agentes que geram gráficos relativos a estatísticas de utilização. Pode-se utilizar o MRTG para monitorar pontos de conexão de discos rígidos, memória, processador, dispositivos de rede, etc.

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

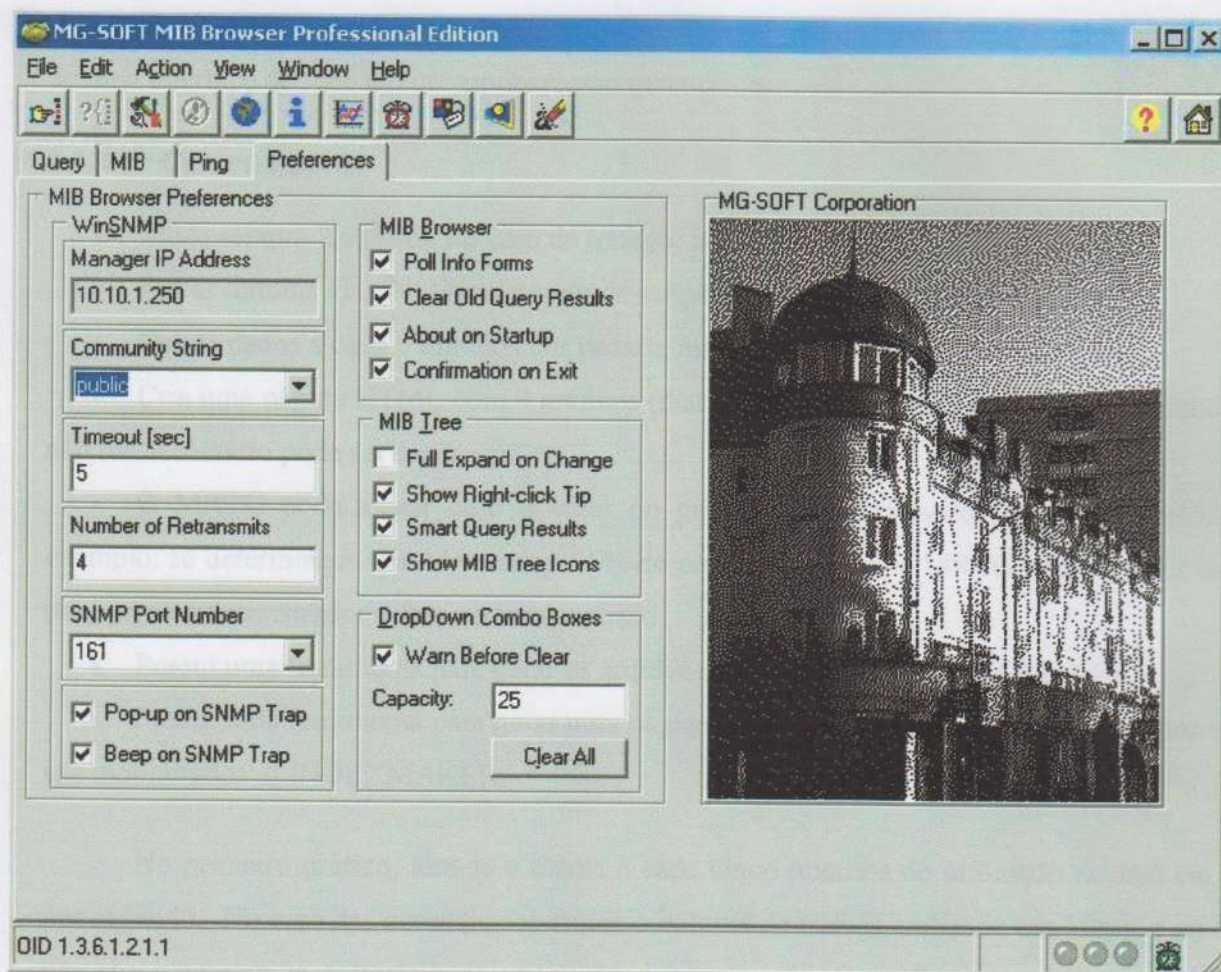


Figura 11: Configuração do MIB Browser

3.3.3 MRTG

O *Multi Router Traffic Grapher* (MRTG) é uma ferramenta para monitorar a carga de tráfego em *links* de rede e a análise de tendências.

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 monitores 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 12 mostra os quatro gráficos estatísticos, gerados pelo MRTG, sobre a utilização de uma interface de rede em um equipamento gerenciado.

3.3.3.1 Características

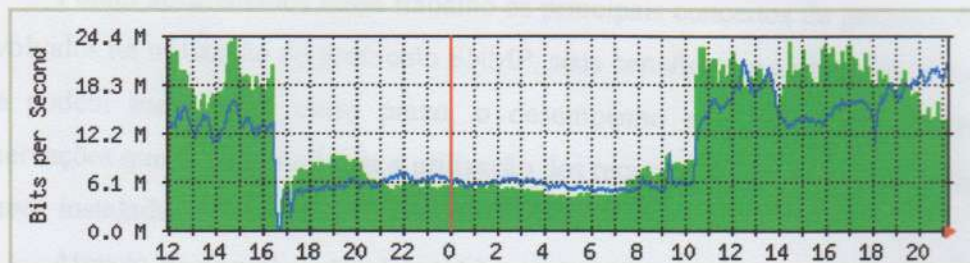
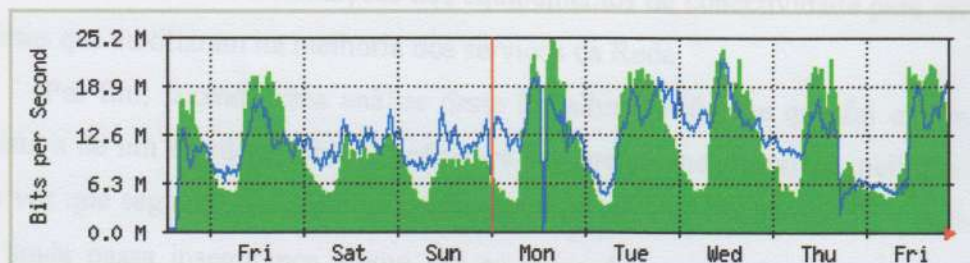
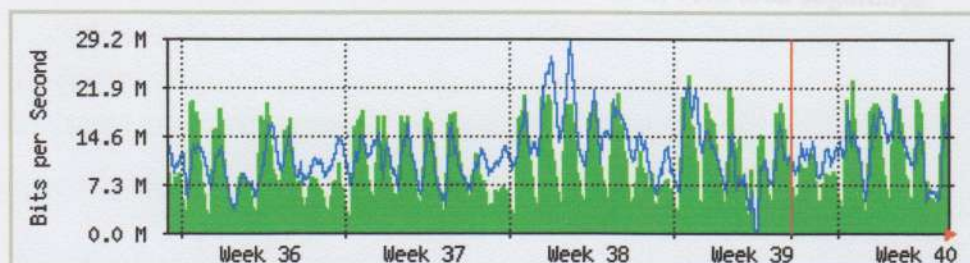
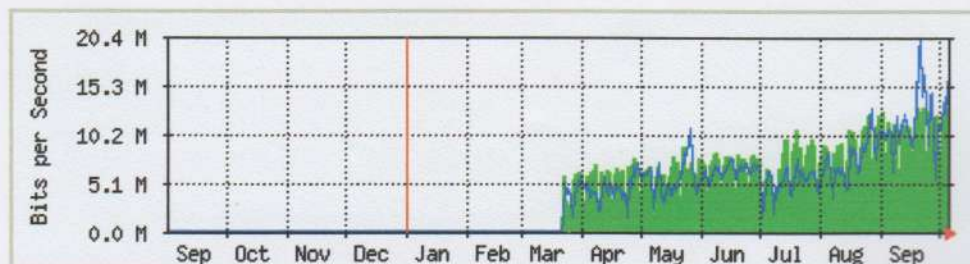
- Mede sempre 2 valores, no caso de tráfego, pode ser Entrada e Saída.
- Faz as leituras via SNMP ou através de script que retorne um formato padrão.
- Coleta dados a cada 5 minutos por padrão, mas este tempo pode ser aumentado.
- Cria uma página HTML com 4 gráficos (diário, semanal, mensal e anual). Se algum deles não for necessário pode ser suprimido.
- O MRTG pode avisar caso o valor do gráfico atinja um valor pré-estabelecido. Por exemplo: se determinado servidor atinge 95% do espaço do disco, o MRTG pode mandar um e-mail para o administrador informando o ocorrido.
- Possui uma ferramenta para gerar os arquivos de configuração: o CFGMAKER.
- Possui uma ferramenta para gerar uma página de índice para os casos em que muitos itens são monitorados: o INDEXMAKER.

No primeiro gráfico, têm-se a média a cada cinco 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, terceiro e quarto gráfico, mostram a mesma análise mudando a taxa de amostragem, passando de horas do dia (visto no primeiro gráfico) para os dias da semana, semanas do mês e meses do ano.

O programa necessário para visualizar o gerente MRTG é um navegador de Internet, por causa que o MRTG gera seus gráficos estatísticos em páginas HTML. Os relatórios são exibidos em formas de imagens PNG, o que deixa a aplicação mais 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 os seus pré-requisitos, e em seguida integrá-lo a um *Web Server*. Está disponível para os sistemas Windows e Linux.

Figura 12: Gráficos de monitoramento diário, semanal, mensal e anual (criados pelo MRTG)

'Daily' Graph (5 Minute Average)**'Weekly' Graph (30 Minute Average)****'Monthly' Graph (2 Hour Average)****'Yearly' Graph (1 Day Average)****Figura 12: Gráficos de monitoramento diário, semanal, mensal e anual (Fonte: MRTG, 2005)**

4 CONCLUSÕES

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 à curto prazo, o desempenho e a segurança da rede, assim como, observações que podem melhorar a utilização dos recursos disponíveis, aumentando a usabilidade da rede instalada.

Através da visualização dos gráficos vistos nos softwares NETWORK SUPERVISOR, MRTG e MIBBROWSER, pode-se traduzir o estado da Rede em tempo real, tornando o gerenciamento mais dinâmico, e através das informações obtidas através do MIBBROWSER, pode-se obter todas as informações dos equipamentos de conectividade para ser aproveitadas em análises que auxiliaram na melhoria dos serviços da Rede.

Por fim, fazendo uma análise deste trabalho, verifica-se que foi extremamente válida a iniciativa de um estudo acerca de softwares de gerenciamento para a melhoria da Rede FARN, uma vez que segurança e gerenciamento são hoje, assuntos de extrema importância num mundo que ainda passa insegurança, como são as redes de computadores, principalmente a Internet, fazendo com que surja um estímulo para que se possa descobrir ou desenvolver novas tecnologias com o intuito de fazer a Rede ser aproveitada ao máximo, com toda segurança.

REFERENCIAL BIBLIOGRÁFICO

A HISTÓRIA da internet. Disponível em:

<<http://www.numaboa.com.br/informatica/internet/web/index.php>>. Acesso em 04/06/2005.

LIMA, Vanessa de Araújo. **Uma metodotologia de gerência de redes na Instituição FARN usando o protocolo SNMP**. Natal: FARN, 2002. Monografia (Graduação em Bacharelado em Sistema de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, Natal, 2002.

LOPES, Raquel V. et al. **Melhores práticas para gerência de redes de computadores**. Rio de Janeiro: Campus, 2003.

MORIMOTO, Carlos E. Redes. Disponível em <<http://www.guiadohardware.net>>. Acesso em 04/06/2005

MRTG. Disponível em: <www.mrtg.org>. Acesso em: 12/11/2005.

GERENCIAMENTO de redes. Disponível em: <<http://www.rnp.br/newsgen/9708/n3-2.html#ng-introducao>>. Acesso em: 05/04/2005.

PROTOCOLO de gerenciamento rmon. Disponível em: <http://www.rnp.br/newsgen/9901/rmon.html>. Acesso em: 22/12/2005.

REDES de computadores. Disponível em:

<<http://www.babooforum.com.br/idealbb/view.asp?topicID=223648>>. Acesso em 04/06/2005.

SEGURANÇA e gerenciamento de redes. Disponível em:

<http://parks.ucpel.tche.br/docs/seguranca.pdf>. Acesso em: 21/12/2005.

SIMPLE network management protocol. Disponível em:

<file:///C:/Documents%20and%20Settings/lab1/Configura%E7%F5es%20locais/Temporary%20Internet%20Files/Content.IE5/MR27YTOT/276,11,SNMPv3> Acesso em: 21/12/2005.

SOFTWARE de gerenciamento de redes. Disponível em: <

http://www.3com.com/prod/pt_LA_AMER/prodlist.jsp?tab=cat&cat=65&subcat=267>. Acesso em: 14/06/2005.

TANEMBAUM, Andrews S. **Rede de Computadores**. Rio de Janeiro: Campus, 2003.

TECNOLOGIAS de redes wireless. Disponível em:

<http://www.rnp.br/newsgen/9805/wireless.html>. Acesso em: 21/12/2005.

WIRELESS. Disponível em: <http://www.babooforum.com.br/idealbb/view.asp?topicID=269602>.

Acesso em: 21/12/2005.