RODRIGO FELICIO DOS SANTOS

UMA PROPOSTA PARA A MELHORIA DA QUALIDADE DE ACESSO REMOTO À REDE UFLA

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da disciplina Projeto Orientado, para a obtenção do título de Bacharel em Ciência da Computação.

Orientador

Prof. Jones Oliveira de Albuquerque

LAVRAS
MINAS GERAIS - BRASIL
2002

RODRIGO FELICIO DOS SANTOS

UMA PROPOSTA PARA A MELHORIA DA QUALIDADE DO ACESSO REMOTO À REDE UFLA

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da disciplina Projeto Orientado, para a obtenção do título de Bacharel em Ciência da Computação.

APROVADA em

_____
Prof. Rêmulo Maia Alves

_____
Prof. Anderson Bernardo dos Santos

_____
Prof. Jones Oliveira de Albuquerque
UFLA
(Orientador)

LAVRAS
MINAS GERAIS – BRASIL

DEDICATÓRIA

Este trabalho é dedicado a meus amados pais, Ivan e Cláudia pelo empenho e dedicação durante toda a vida em dar-me condições para continuar meu caminho e por enxergarem o futuro. Ao meu querido irmão Rafael, pelo amor e amizade, a toda minha rica família pela atenção, à maravilhosa Ana Palmira, pelo carinho, valor e significado. A todos os amigos pelos momentos marcantes.

"*Embora o tesouro esteja enterrado em sua casa, você só irá descobri-lo quando se afastar*".
(Paulo Coelho)

AGRADECIMENTOS

Agradeço a Deus por abençoar-me com pais, irmão e uma família esplendida e feliz, a Ana Palmira por todo seu amor, dedicação e apoio nos momentos de tristeza e de alegria também, e a todos os seus familiares pelo carinho. Aos amigos da república pela família que são, aos amigos da sala, pelo prazer da companhia e pelos pagodes. Agradeço a todos por participarem da minha vida e por transformar-me em uma pessoa melhor. Amo todos vocês.

Agradeço sinceramente a todos os professores por tudo o que foi ensinado ao longo desses quatro anos, ao meu co-orientador Anderson por acreditar desde o princípio na minha capacidade, pela ajuda com este trabalho e por todos os ensinamentos na área de redes de computadores.

Ao professor Rêmulo por todo o apoio ao ingresso no mestrado e neste trabalho, e ao professor e orientador Jones por direcionar-me em toda a parte científica do presente trabalho.

RESUMO

Devido ao crescimento explosivo das redes de computadores, o gerenciamento torna-se justificável. Em redes de longa distância, a tarefa de gerenciamento é inerentemente mais complexa e indispensável. O presente trabalho propõe melhorias em gerenciamento e em qualidade de acesso remoto através de um RAS.

SUMÁRIO

Introdução 1
1.1 Por que gerenciar uma rede de computadores? 2
1.2 Descrição do Trabalho Proposto 3
Estado da Arte 5
2.1 Modelo de Gerenciamento de Redes OSI 5
2.1.1 Gerenciamento de Desempenho 6
2.1.2 Gerenciamento de Configuração 7
2.1.3 Gerenciamento de Contabilização 7
2.1.4 Gerenciamento de Falhas 8
2.1.5 Gerenciamento de Segurança 9
2.2 Acesso Remoto 9
2.2.1 RAS x VPN: opções diferentes para o alcance do mesmo objetivo 10
2.2.2 RAS: Conexão via ISDN ou via Modem? 15
2.2.3 RAS: Quantas Portas? 15
2.3 Heurística de Usabilidade 16
Modelagem 20
3.1 Apresentação do Equipamento Utilizado 20
3.1.1 O Protocolo RADIUS 23
3.1.2 O Servidor ChoiceNet 24
3.2 Adicionando o Servidor de Acesso Remoto ao Gerenciamento da Rede UFLA 26
3.2.1 SNMP – Simple Network Management Protocol 26
3.2.2 Configurando o Protocolo SNMP no RAS 29
3.3 Habilitando e Configurando a Tecnologia ISDN 34
3.3.1 ISDN - Integrated Services Digital Network 34
3.3.1.1 Arquitetura de Sistema ISDN 34
3.3.1.2 Interface ISDN 35
3.3.1.3 ISDN/BRI (Basic Rate Interface) 35
3.3.1.4 ISDN/PRI (Primary Rate Interface) 36
3.3.1.5 Benefícios 36
3.3.1.6 Perspectivas 36
3.3.2 Configurando a Tecnologia ISDN no RAS 37
3.4 Análise Heurística da Interface da Ferramenta PMVision 40
Conclusões 43
4.1 Trabalhos Futuros 44
Referências Bibliográficas 45

LISTA DE FIGURAS

Figura 1(a) - Servidor de Acesso Remoto.....14

Figura 1(b) - Virtual Private Network.....15

Figura 2 – PortMaster3.....21

Figura 3 (a) - Visão do Painel Traseiro do Servidor.....22

Figura 3 (b) - Visão do Painel Traseiro do Servidor através da Ferramenta Gráfica PMVision.....22

Figura 4 - A Ferramenta Gráfica PMVision.....23

Figura 5 - Tela para Habilitação do protocolo SNMP.....30

Figura 6 - Configuração SNMP.....31

Figura 7 (a) - Tela do software de gerenciamento MRTG.....32

Figura 7 (b) - Gráficos gerados pelo MRTG para o servidor PortMaster3.....33

Figura 8 (a) - As linhas ISDN a serem configuradas.....39

Figura 8 (b) - As linhas ISDN a serem configuradas.....39

Figura 9 - Tela inicial do PMVision.....40

Figura 10 – Tela de confirmação de auteração do protocolo SNMP no PMVision.....41

Capítulo 1

Introdução

A área de redes de computadores tem crescido explosivamente. Há duas décadas atrás, poucas pessoas tinham acesso a uma rede. Agora, a comunicação entre computadores tem se tornado uma parte essencial de nossa infra-estrutura. Redes são usadas em todo lugar onde haja a necessidade de comunicação. Conseqüentemente, empresas, entidades educacionais, estabelecimentos governamentais e organizações militares usam redes de computadores. Embora seja para diferentes finalidades, as redes de computadores estão em todo lugar [Com97].

Segundo [Tan97], existem dois tipos de redes: corporativas e para pessoas. Muitas empresas têm um número significativo de computadores em operação, freqüentemente instalados em locais distantes entre si. Mas, devido à necessidade de extrair e correlacionar informações, decidiu-se colocá-los em rede para que fosse possível o compartilhamento de recursos. A rede aumenta a confiabilidade do sistema, pois tem fontes alternativas de fornecimento. Outra vantagem oferecida é a escalabilidade, ou seja, a possibilidade de aumentar gradualmente o desempenho do sistema à medida que cresce o volume de carga.

Por outro lado, uma rede de computador pode oferecer um meio de comunicação altamente eficaz para funcionários que trabalham em locais muito distantes um do outro, além de aumentar a eficiência corporativa.

Com relação às redes para pessoas, a partir da década de 90, as redes de computadores começaram a oferecer serviços para pessoas físicas em suas respectivas casas, devido à grande vantagem de preço/desempenho das redes de

computadores pessoais em relação aos *mainframes*, o que acarretou um aumento na popularidade das mesmas. Dentre os serviços a serem oferecidos, podem ser citados o acesso a informações remotas, como por exemplo, jornais e bibliotecas *on-line*, comunicação pessoa a pessoa (e-mail) e diversão interativa (filmes e jogos *on-line*).

O rápido crescimento da Internet é um dos fatores determinantes do crescimento da área de redes, já que há uma década atrás, a Internet era um projeto de pesquisa que envolvia poucas dezenas de *sites*, e hoje alcança milhões de pessoas em 82 países em todos os continentes [Com97]. Além disso, o acesso remoto tem se tornado prioridade para muitas empresas. Isso ocorre pelo simples fato de que muitos empregados precisam de uma maneira segura e confiável de acessar *e-mail*, dados e aplicações remotamente enquanto estão trabalhando em casa ou em viagens de negócios [Pas99].

Para [Pet00], uma rede deve fornecer conectividade entre um conjunto de computadores, pois se trata de um sistema complexo, tanto em termos de números de nós envolvidos quanto em termos de conjunto de protocolos que podem ser rodados em qualquer nó.

1.1 Por que gerenciar uma rede de computadores?

Imaginemos uma rede com um número mínimo de máquinas conectadas. Logo, uma única pessoa é capaz de gerenciá-la. Porém, em redes de longa distância, a tarefa de gerenciamento é inerentemente mais complexa e indispensável, uma vez que cobre uma área geográfica extensa e envolve um grande número de equipamentos e usuários dependentes de seus serviços [Oda94b]. Ainda, de acordo com [Pet00], se nos preocuparmos apenas com os nós de um domínio administrativo, como um campus, por exemplo, podem ser notadas dúzias de roteadores e centenas ou até mesmo milhares de *hosts*

(máquinas cuja finalidade é executar os programas [Tan97]) a serem gerenciados. Se pensarmos em todo o estado que deve ser mantido e manipulado em todos os nós, como tabelas de tradução de endereço, tabelas de roteamento e estado de conexão *TCP* (*Transmission Control Protocol* – protocolo que atua na camada de transporte e permite a entrega sem erros de um fluxo de bytes originado de uma determinada máquina em qualquer computador da inter-rede [Tan97]), a justificativa ao gerenciamento de rede torna-se evidente.

Do ponto de vista de [Fre99], o gerenciamento consiste no monitoramento de uma rede de comunicações a fim de diagnosticar problemas e coletar dados estatísticos para administração e ajustes. Para [Oda94b], as atividades básicas do gerenciamento de redes consistem na detecção e correção de falhas, em um tempo mínimo, e em estabelecer procedimentos para a previsão de problemas futuros. A complexidade do gerenciamento de rede é diretamente proporcional ao tamanho da rede gerenciada.

Segundo [Sie02], a finalidade do gerenciamento de rede é garantir a operação regular de uma rede. Fatores determinantes de uma rede são a cooperação de diferentes funções dos componentes de rede e o modo de agir dos usuários.

Desde que existam nós a serem gerenciados, a única opção real é usar a rede para que a mesma seja gerenciada [Pet00].

1.2 Descrição do Trabalho Proposto

Considerando todos os problemas que podem ocorrer devido a proporções alcançadas por uma rede de computadores, o presente trabalho tem como objetivo, propor soluções para o problema da qualidade do acesso remoto à rede da Universidade Federal de Lavras – UFLA. Esta rede teve seu processo de expansão iniciado em 1996 com a compra de *switchs* (nó da rede que

transfere pacotes dos nós internos da rede para os externos baseado no cabeçalho de informação em cada pacote [Pet00]), *hubs* (repetidor multímodo[Pet00]) e servidores remotos [Ufl98]. Segundo [Ara01], a mesma abrange vários departamentos interligados por fibra ótica. Para isso, será usado um componente da rede, um servidor de acesso remoto cuja capacidade ainda não está totalmente adequada às necessidades da rede UFLA.

Os resultados obtidos através deste trabalho são relevantes no sentido de conseguir um melhor aproveitamento do servidor de acesso remoto. Desse modo, futuramente, ele poderá ser utilizado de maneira integral aumentando de maneira satisfatória o desempenho da rede UFLA bem como melhorar a qualidade do acesso remoto e a gerência da rede.

No Capítulo dois, o Estado da Arte, serão apresentados artigos sobre o modelo de gerenciamento de redes OSI, servidor de acesso remoto, sua utilidade e uma comparação entre esse tipo de equipamento e VPN (*Virtual Private Network* – Rede Privada Virtual), uma solução alternativa que pode ser adotada em determinados casos, além dos conhecimentos básicos para a avaliação de interfaces. No capítulo três encontra-se a modelagem do problema e, finalmente, no capítulo quatro, a conclusão deste.

Capítulo 2

Estado da Arte

2.1 Modelo de Gerenciamento de Redes OSI

De acordo com [Tan89], citado por [Oda94a], através dos benefícios oferecidos pelas redes e da diminuição do custo de hardware, o número de computadores interconectados começou a crescer dentro das organizações originando problemas administrativos. As tarefas de configuração, localização de falhas e gerenciamento de dispositivos e recursos da rede passaram a consumir tempo, elevando os gastos dentro das organizações. Paralelamente, as redes começaram a ser interconectadas rapidamente; redes locais conectavam-se a redes regionais, as quais por sua vez, conectavam-se a *backbones* nacionais. Já na metade da década de oitenta o número de redes conectadas a Internet chegou a quase dobrar de ano para ano, segundo [Ro91], citado por [Oda94a].

Cientes desses problemas, a ISO (*International Organization for Standardization*) e a IAB (*Internet Activity Board*), iniciaram pesquisas buscando soluções que permitissem aos gerentes de rede realizar tarefas tais como obter dados sobre desempenho e tráfego da rede em tempo real, diagnosticar problemas de comunicação e reconfigurar a rede atendendo às mudanças nas necessidades dos usuários e do ambiente. Porém, vários obstáculos teriam que ser superados, entre eles a heterogeneidade dos equipamentos de rede, dos protocolos de comunicação e das tecnologias de rede.

Desse modo, em 1989 [Oda94a], a ISO propôs uma arquitetura de gerenciamento capaz de viabilizar o controle e monitoração de redes que utilizam os protocolos OSI. Assim, o modelo de referência ISO/OSI foi estendido para acomodar a capacidade de gerenciamento, e foram especificados

protocolos para o transporte de informações de gerenciamento entre sistemas abertos.

Com relação à Estrutura de Gerenciamento ISO/OSI, são apresentados os conceitos de gerente, agente e objeto gerenciado. A interação entre os componentes ocorre da seguinte maneira: o gerente envia operações de gerenciamento aos agentes, a fim de obter informações sobre objetos gerenciados e controlá-los; o agente, por sua vez, recebe as operações e as executa sobre os objetos gerenciados. Além disso, o agente pode enviar ao gerente notificações geradas pelos objetos gerenciados ou sobre a ocorrência de eventos extraordinários.

[Cis99a] relata que a Organização Internacional de Padronização (ISO) tem contribuído muito para a definição dos padrões da área de redes de computadores. Tal modelo de gerenciamento de rede é indispensável para o entendimento de funções mais importantes de sistemas de gerenciamento de rede. Este modelo consiste de cinco áreas conceituais: gerenciamento de desempenho, de configuração, de contabilização, de falhas e de segurança, as quais estão descritas a seguir.

2.1.1 Gerenciamento de Desempenho

O objetivo do gerenciamento de desempenho é avaliar e tornar disponíveis vários aspectos de desempenho de rede para que o desempenho inter-redes possa manter-se em um nível aceitável. Como exemplos de variáveis de desempenho podem ser citadas a vazão da rede e a utilização da linha.

Este tipo de gerenciamento envolve três passos principais. Primeiro, dados de desempenho são armazenados em variáveis de interesse dos administradores de rede. Segundo, os dados são analisados para determinar níveis iniciais, ou de referência de desempenho. Finalmente, percentuais

mínimos de desempenho são determinados para cada variável importante que exceda estes percentuais indicando assim, um problema que mereça atenção.

Entidades de gerenciamento monitoram continuamente variáveis de desempenho. Quando um percentual mínimo é excedido, um alerta é gerado e enviado para o sistema de gerenciamento de rede.

Cada um destes passos descritos é parte do processo para configurar um sistema de reação. Quando o desempenho torna-se inaceitável devido a um percentual mínimo excedido, definido pelo usuário, o sistema reage enviando uma mensagem.

2.1.2 Gerenciamento de Configuração

Monitorar a rede e a informação de configuração do sistema é o objetivo deste tipo de gerenciamento para que os efeitos na operação de rede de várias versões de elementos de hardware e software possam ser encontrados e gerenciados. Cada dispositivo de rede tem sua variedade de versão. Subsistemas de gerenciamento de configuração armazenam este tipo de informação em um banco de dados. Quando um problema ocorre, este banco de dados pode ser procurado para que pistas sejam encontradas ajudando assim na resolução do problema. Como [Oda94a] relata, o gerenciamento de configuração permite que elementos de rede remotos sejam configurados, o que se torna necessário para acomodar mudanças nas necessidades do usuário, aliviar congestionamento na rede ou isolar falhas.

2.1.3 Gerenciamento de Contabilização

Segundo [Oda94a], esse tipo de gerenciamento oferece funções que permitem determinar os custos da utilização dos recursos da rede.

Para [Cis99a], o objetivo do gerenciamento de contabilização é determinar os parâmetros de utilização da rede para que usos da rede, tanto individuais quanto grupais, possam ser ajustados de maneira correta. Tal ajuste minimiza problemas de rede (porque os recursos podem ser distribuídos de acordo com suas capacidades) e maximiza o acesso à rede.

Assim como no gerenciamento de desempenho, o primeiro passo para um gerenciamento de contabilização apropriado é medir a utilização de todos os recursos mais importantes da rede. A análise dos resultados fornece a percepção dos padrões utilizados. Alguma correção será necessária para que seja alcançado um acesso ótimo. A partir deste ponto, uma medida avançada do uso de recursos pode produzir informação de faturamento, bem como informação usada para estimar uma utilização de recursos ótima.

2.1.4 Gerenciamento de Falhas

Como [Oda94a] e [Cis99a] relatam, o objetivo desse tipo de gerenciamento é detectar, documentar, notificar usuários sobre problemas, e automaticamente corrigí-los para manter a rede em atividade efetivamente. Devido às falhas causarem tempo ocioso ou degradação da rede, o gerenciamento de falhas é talvez o mais largamente implementado dos elementos de gerenciamento de rede ISO.

Assim como o gerenciamento de desempenho, o gerenciamento de falhas envolve três passos: primeiro, o gerenciamento de falhas determina sintomas e o isolamento do problema. Então, o problema é solucionado, e a solução é testada em todos os subsistemas importantes. Finalmente, a detecção e resolução do problema são gravadas.

2.1.5 Gerenciamento de Segurança

Segundo [Cis99a], o objetivo do gerenciamento de segurança é controlar o acesso aos recursos da rede de acordo com a política de rede para que a rede não seja sabotada (intencionalmente ou não) e informações restritas não sejam acessadas por aqueles que não tenham autorização devida. Um sistema de gerenciamento de segurança, por exemplo, pode monitorar usuários acessando um recurso de rede, negando acesso para aqueles que entrem com códigos de acesso inapropriados.

Subsistemas de gerenciamento de segurança trabalham particionando recursos de rede em áreas autorizadas e não autorizadas. Para alguns usuários, o acesso a qualquer recurso de rede não é autorizado, na maioria das vezes porque alguns usuários não pertencem aos usuários da rede. Para outros usuários, usuários internos, o acesso à informação originada de um determinado departamento é inapropriado.

Os subsistemas de gerenciamento de segurança executam várias funções. Eles identificam fontes de rede sensíveis (incluindo sistemas, arquivos, e outras entidades) e determinam mapeamentos entre recursos de sensíveis e configurações de usuários. Além disso, também monitoram pontos de acesso a recursos de rede sensíveis e gravam acesso inapropriado a esses recursos.

2.2 Acesso Remoto

Segundo [Kee98], o acesso remoto a redes locais e geográficas provavelmente obterá um desenvolvimento significante em muitas áreas. A Internet, que antes era apenas uma rede de cientistas, engenheiros e técnicos, e agora se tornou uma entidade comercial, servindo milhões de usuários remotos,

com seu incrível crescimento, será um dos mais importantes fatores no futuro do acesso remoto.

De acordo com [Kee98], a *Forrester Research* estimou que a partir de 1999 mais de 80% da força de trabalho empresarial teria pelo menos um dispositivo computacional móvel e que o acesso remoto via Internet cresceria exponencialmente a partir do ano 2000. Cerca de sessenta milhões de trabalhadores remotos estariam conectados pelo menos uma ou duas vezes por dia após a virada do milênio.

Como pode ser observado, o acesso remoto está se tornando indispensável em redes de computadores. As sub-seções abaixo apresentam dois tipos distintos de se obter acesso remoto: através de um RAS, ou através de VPN. Ambas são soluções viáveis para determinados casos.

2.2.1 RAS x VPN: opções diferentes para o alcance do mesmo objetivo

Se uma empresa possui uma considerável quantidade de empregados que viajam a negócios e necessitam de acesso à rede local, então uma possível solução seria um servidor de acesso remoto (*Remote Access Server – RAS*) [Fre99].

Um servidor de acesso à rede é o ponto de entrada inicial para a maioria dos usuários de serviços de rede. É o primeiro dispositivo da rede a fornecer serviços para um usuário final, e atua como um *gateway* (equipamento de rede que estabelece conexão e faz a conversão necessária entre duas redes incompatíveis [Tan97]) para alguns serviços como, por exemplo, autenticação e autorização. Como tal é de extrema importância para usuários e provedores de serviço [Mit00].

Segundo [Fre99], antes de escolher algum tipo de solução ao problema de acesso remoto para uma companhia, é necessário que sejam tomadas três importantes decisões: Primeiro é preciso escolher entre RAS e VPN (*Virtual Private Network – Rede Virtual Privada*), a qual tem a mesma função de um RAS, porém, conecta o usuário à rede local via conexão Internet. Segundo, se a escolha for um RAS, é necessário escolher entre ISDN (*Integrated Services Digital Network*), tecnologia discutida mais adiante, e linhas telefônicas tradicionais para a conexão ao RAS. Terceiro, é necessário escolher quantas linhas serão usadas para o acesso.

De acordo com [Gat00], o uso de servidores de acesso remoto é justificável devido ao número de pessoas que acessam a Internet ultrapassar a casa de 200 milhões e também à explosão global da mesma em muitas partes do mundo, ocasionando uma demanda muito forte para as plataformas RAS durante alguns anos.

[Fre99] relata que num RAS a conexão é feita diretamente através de discagem analógica ou linhas telefônicas ISDN. Usuários remotos conectam-se ao RAS utilizando-se modems e o mesmo software de discagem usado para acessar Internet. Os usuários que se encontram fora da área de acesso à rede local devem fazer chamadas de longa distância para estabelecer uma conexão com o RAS. O servidor de acesso remoto possui múltiplas portas, o que possibilita o acesso simultâneo.

Modernos sistemas RAS, os quais incluem gerenciamento e autotestes, exigem muita manutenção, já que são diferentes de muitos outros equipamentos de rede e requerem conhecimento de técnicas de comunicações através de discagem analógica. Além disso, muitas instalações tradicionais de servidores de acesso remoto não são ideais para acesso à Internet [Pas99].

Como aplicações típicas de RAS temos o uso na corporação para prover acesso remoto a clientes (*home banking*), por exemplo, a funcionários, e em

Provedores de Serviço Internet (*ISPs – Internet Service Providers*) para acesso discado à Internet [Cyc02].

Com relação ao fator custo, instalar e manter um grande sistema RAS pode ser caro devido ao número de linhas necessárias. Gastos periódicos com linhas tronco, por exemplo, aumentam rapidamente [Pas99].

Segundo [Fre99], uma grande vantagem de se usar uma VPN é que os usuários podem se conectar a rede local, não importa onde estejam, apenas executando uma chamada local para o número do ISP. Porém, VPNs requerem uma conexão Internet rápida e em tempo integral com a rede local.

Por fornecer um túnel autenticado e encriptado através da Internet ou intranets privadas, VPNs podem fornecer conexões entre localizações coorporativas e sócios, por exemplo. No entanto, o benefício imediato é a habilidade de simplificar e assegurar o acesso remoto à rede.

VPNs possuem algumas vantagens em relação ao RAS: qualquer ISP de qualquer localização pode ser usado para acesso à Internet já que de ambos os lados é criado um túnel através da rede; o software cliente é fácil de ser usado e estável em operação já que tolera latência de rede (tempo que uma mensagem leva para ir de um ponto da rede a outro, segundo [Pet00]) e automaticamente restabelece o sincronismo depois de interrupções; Alto nível de proteção de invasão devido ao túnel encriptado[Pas99].

Segundo [Kee98], a segurança é uma das grandes vantagens das VPNs já que os usuários precisam saber que informações privadas e confidenciais podem ser enviadas pela Internet sem serem vistas, alteradas, copiadas e ainda, intactas.

Por outro lado, o custo inicial de hardware para uma VPN equivale a um terço do custo de uma robusta instalação RAS. Com relação a suporte, o custo também é baixo, pois VPNs não envolvem muito gerenciamento administrativo e manutenção de equipamento [Pas99].

Como pode ser observado, VPNs possuem consideráveis vantagens em relação a servidores de acesso remoto, tanto em relação ao fator custo quanto ao fator tecnológico. No entanto, [Gat00] acredita que ISPs têm focalizado somente o acesso à internet via modem aos seus clientes. Porém, com a convergência de redes de voz e dados, há uma certa necessidade em fornecer serviços que utilizem tecnologias como voz sobre IP (*VoIP – Voice over IP*) por exemplo, como um modo de gerar novas fontes de rendimento. Sendo assim, as plataformas RAS terão que fornecer todos os serviços dessas tecnologias, o que representa uma grande expansão, no que diz respeito à função da plataforma RAS, impulsionando assim, o mercado da mesma.

Ainda com relação ao RAS, [Gat00] diz que com a onipresença da Internet e a crescente aceitação de programas de tunelamento, cada vez mais corporações estão direcionando o acesso remoto à sua rede local via Internet através de ISPs. Isto, combinado com a proliferação do acesso doméstico à Internet, tem criado uma crescente demanda por equipamentos RAS de alta densidade capaz de suportar milhares de conexões em um único servidor.

Contrariamente, [Pas99] relata que a necessidade de encriptação deve ser razão suficiente para usar VPN ao invés de RAS. [Pas99] ainda enfatiza que uma conexão discada tem um nível muito mais alto de segurança física do que uma conexão virtual através de uma rede de área geográfica pública, mas a interceptação de dados ainda é possível.

Definindo uma regra geral, [Fre99] conclui que RAS são mais baratos para se colocar em funcionamento se a maioria dos usuários estão na área local de chamadas, e VPNs são mais baratas se muitos dos usuários estão a longas distâncias.

Desse modo, como pode ser observado, justifica-se a utilização do RAS na Universidade Federal de Lavras – UFLA, já que se trata de um ISP. A instituição utiliza o servidor com o objetivo de prover acesso à Internet para usuários internos e remotos, os quais se localizam na área de chamadas local. A

seguir estão duas figuras ilustrativas sobre Servidor de Acesso Remoto e Redes Privadas Virtuais.

A Figura 1 (a), é uma representação de como é feito o acesso a um RAS: O cliente remoto conecta-se com o servidor de acesso remoto através de discagem. Em seguida, os respectivos dados do usuário são enviados ao servidor RADIUS (*Remote Authentication Dial-In User Service*), o qual será explicado na seção 3.1.1, efetua a autenticação do usuário transmitindo essa informação ao RAS, que por sua vez estabelece a conexão. Depois, o servidor ChoiceNet, de acordo com os dados do usuário, filtra os pacotes enviados e recebidos, de acordo com sua configuração, como será explicado na seção 3.1.2.

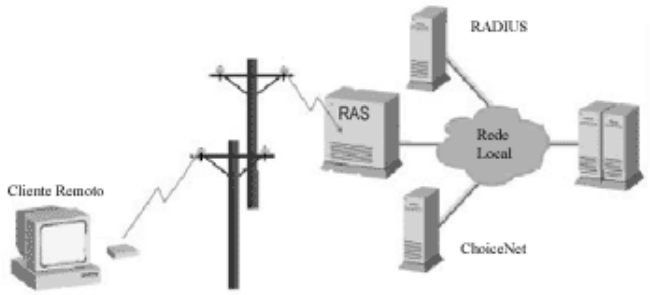

Figura 1 – (a) Servidor de Acesso Remoto

Na Figura 1 (b), é ilustrada uma conexão VPN. O usuário remoto disca para o provedor de Internet local e através de um software que efetua conexão VPN, conecta-se à rede corporativa.

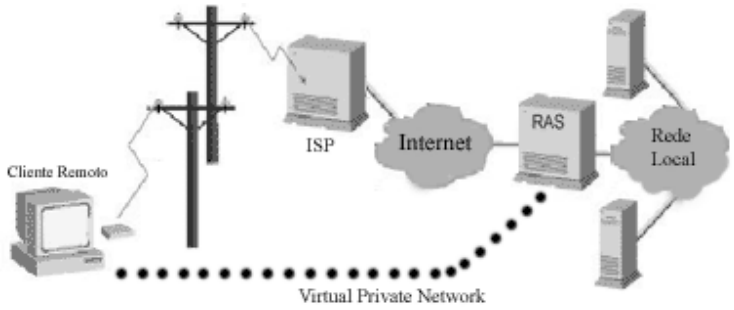

Figura 1 (b) – Virtual Private Network

2.2.2 RAS: Conexão via ISDN ou via Modem?

Se a primeira decisão a ser tomada for o RAS, então é necessário escolher entre ISDN ou serviços telefônicos analógicos para as conexões ao servidor. Linhas telefônicas possuem um preço acessível e são encontradas em qualquer lugar, mas também são lentas. Conexões analógicas são limitadas a 33,6 Kbps. Os novos modems V90 talvez sejam uma possível solução para o problema.

As linhas ISDN oferecem velocidades mais altas que modems, mas também são mais caras no que diz respeito à instalação e suporte. Por outro lado, uma única linha ISDN fornece duas conexões de 64Kbps independentes, portanto, cada linha ISDN pode lidar com duas chamadas ao mesmo tempo (detalhes técnicos sobre a tecnologia ISDN serão apresentados posteriormente).

Além de custo, é necessário analisar a finalidade da conexão. Para e-mail e transferências de arquivos, a linha analógica é aceitável; para um uso que exija um tráfego maior, ou para executar aplicações, é aconselhável ISDN. O uso de ISDN é justificável para usuários que necessitam de acesso em tempo integral para que possam atuar como se estivessem na rede local [Fre99].

2.2.3 RAS: Quantas Portas?

De acordo com [Fre99], se a empresa possui mais usuários em filiais do que usuários que viajam a negócios é recomendada uma relação de uma porta *dial-up* para cada dois usuários remotos.

Nesse trabalho, o número de portas a ser utilizado é importante, pois, objetivando uma melhoria da qualidade do acesso remoto, se um servidor de acesso remoto estiver funcionando com seu número máximo de portas, o número de acessos simultâneos também será máximo. Além disso, se um RAS possui uma quantidade de portas considerável, o acesso é feito mais rapidamente devido à ausência de congestionamento nas linhas telefônicas.

2.3 Heurística de Usabilidade

Os conceitos de usabilidade exibidos aqui serão utilizados para a análise da interface da ferramenta gráfica de gerenciamento do equipamento descrito neste trabalho.

A propriedade de uma interface com o usuário que permite classificá-la quanto à sua qualidade é conhecida na literatura como usabilidade, conceito definido tradicionalmente como a conjunção de cinco atributos:

1. Facilidade de aprendizado: o sistema deve permitir que o usuário aprenda a executar suas tarefas no prazo mais curto possível;
2. Eficiência de uso: o sistema, uma vez dominado pelo usuário, permite um alto grau de produtividade;
3. Retenção: o sistema deve ser relembrado facilmente mesmo pelo usuário, permite um alto grau de produtividade;
4. Minimização de erros; o sistema deve ter uma taxa baixa de erros de utilização. Além disso, os erro cometidos pelo usuário devem ser facilmente recuperáveis (por exemplo, volta a um estado seguro) e erros catastróficos não podem ocorrer;
5. Satisfação: o sistema deve ser agradável de usar, ou seja, seus usuários ficam subjetivamente satisfeitos com ele.

Segundo [Nie93], os seguintes princípios devem ser seguidos durante o projeto da interface com o usuário para se obter um produto final de qualidade:

Diálogo Simples e Natural: A interface com o usuário deve ser tão simples quanto possível. Cada elemento de diálogo ou item de informação extra colocado numa tela representa um item a mais para aprender, uma fonte a mais de possível confusão para o usuário e um obstáculo a mais quando se está procurando por outro item de informação desejada. A realização de tarefas com o sistema também deve minimizar a navegação do usuário pelo sistema.

O *design* gráfico da interface deve por si só mostrar as relações entre os elementos de diálogo. Regras básicas de percepção humana devem ser seguidas. Por exemplo, um conjunto de elementos é percebido como um grupo ou unidade se eles estão posicionados próximos um do outro.

Princípios de *design* gráfico também devem ser usados quando é necessário priorizar a atenção do usuário. Por exemplo, a informação é lida normalmente da esquerda para direita e de cima para baixo, o que quer dizer que os elementos de diálogo no topo da tela serão os que receberão mais atenção.

O uso da cor nos diálogos deve ser moderado. O uso de cinco a sete cores numa interface é suficiente para a maioria das aplicações.

Fale a Língua do Usuário: Os diálogos devem ser expressos claramente em palavras, expressões e conceitos familiares à comunidade de usuários, não em termos orientados ao sistema. As interações devem ser vistas da perspectiva do usuário. As metáforas usadas pela interface com o usuário devem respeitar o conceito que o usuário tem da metáfora.

Minimize a Carga de Memória do Usuário: O usuário não deve ser forçado a memorizar informações ao passar de uma parte do diálogo a outra. Em geral, as pessoas são muito melhores em reconhecer algo que lhes é mostrado do que em recuperar a mesma informação da memória sem nenhuma ajuda.

Para minimizar a carga de memória do usuário, o sistema deve se basear em um número reduzido de regras que se apliquem a várias situações dependendo do contexto.

Consistência: Se os usuários souberem que o mesmo comando ou a mesma ação terá sempre o mesmo efeito, eles se sentirão mais confiantes e o aprendizado do sistema ficará mais fácil porque a cada nova etapa uma parte do conhecimento necessário já estará disponível. A mesma informação deve ser apresentada no mesmo local em todas as telas e caixas de diálogo e deve ser formatada da mesma maneira para facilitar o seu reconhecimento.

Retorno: O sistema deve informar o usuário continuamente sobre o que está sendo feito e como a entrada do usuário está sendo interpretada. O retorno não deve esperar até que um erro ocorra, mas deve prosseguir paralelamente à entrada de informação. O retorno do sistema não deve ser expresso em termos gerais e abstratos mas deve reescrever a entrada do usuário. Outro ponto em que o retorno é essencial para evitar é na ocorrência de falhas do sistema. Deve ficar claro para o usuário que a falha foi do sistema e o que pode ser feito a respeito.

Saídas Claramente Marcadas: Nenhum usuário gosta de se sentir encurralado pelo computador. Para aumentar o sentimento de controle do usuário sobre o sistema, deve-se prover uma saída fácil e explícita de tantas situações quanto possível.

Atalhos: Conhecidos como aceleradores, incluem abreviações de comandos, combinações de teclas as quais são mapeadas em comandos do sistema, clique duplo do mouse sobre um elemento para realizar sua ação mais comum e menus de botões. O usuário deve reusar a sua história de interações.

Prevenção de Erros: Melhor do que apresentar uma boa mensagem de erro é evitar que o usuário experimente a situação que criou o erro. Geralmente é possível identificar os pontos em que os erros são mais prováveis e os sistemas podem ser adaptados de forma a contornar estas situações.

Boas Mensagens de Erro: Deve-se escrever mensagens de erro em linguagem clara e evitar o uso de códigos obscuros. Deve ser possível para o usuário entender a mensagem por si só sem ter que recorrer a manuais. As mensagens de erro devem ser precisas e não vagas ou genéricas, devem ser construtivas e ajudar o usuário a resolver o problema. As mensagens de erro devem ser educadas e nunca intimidar o usuário ou culpa-lo pelo erro. Termos fortes como *fatal, ilegal,* etc. devem ser evitados.

Ajuda e Documentação: A regra fundamental para a documentação é que a maioria dos usuários simplesmente não lê os manuais. O corolário desta regra é que quando os usuários recorrem aos manuais, eles estão provavelmente em algum tipo de situação de emergência e precisarão de ajuda imediata. Portanto, é essencial que o sistema de ajuda e o manual do usuário seja orientado por tarefas, liste passos concretos e use uma linguagem o mais clara e concisa possível.

Capítulo 3

Modelagem

3.1 Apresentação do Equipamento Utilizado

O equipamento utilizado nesse trabalho é um servidor de acesso remoto denominado *PortMaster3* da *Lucent Technologies* (Figura 2), o qual está localizado no Centro de Informática (CIN) da UFLA, aonde foi desenvolvido esse trabalho. O servidor é formado por um sistema de modems que contém seis *slots* para dez modems digitais cada, o que totaliza um número máximo de sessenta conexões simultâneas, além de dois feixes E1/T1 de trinta linhas telefônicas cada. A interface E1 é utilizada para a conexão via modem e a interface T1 é utilizada para conexão ISDN. Possui ainda uma porta *Ethernet* com conectores para cabo 10Base2, AUI, ou 10BaseT [Hpm02]. Todos esses componentes podem ser visualizados no painel traseiro do Portmaster3 Figura 3 (a).

Figura 2 – PortMaster3

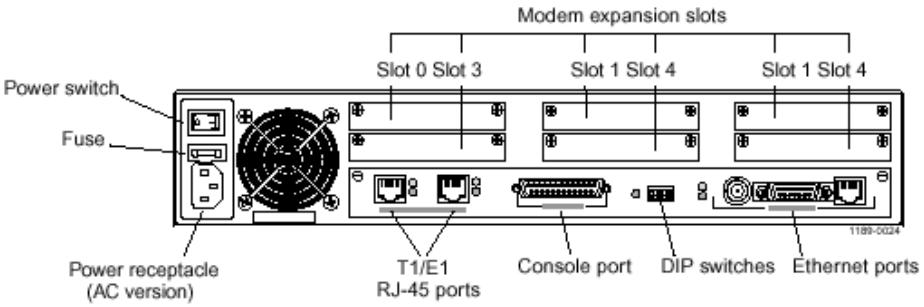

Figura 3 (a) – Visão do Painel Traseiro do Servidor [Pmv99].

Na Figura 3 (b), é mostrada uma visão do mesmo painel através da ferramenta gráfica de configuração PMVision. Nessa figura há uma legenda com relação ao estado atual de cada modem bem como as demais portas do equipamento (E1/T1, *Ethernet*).

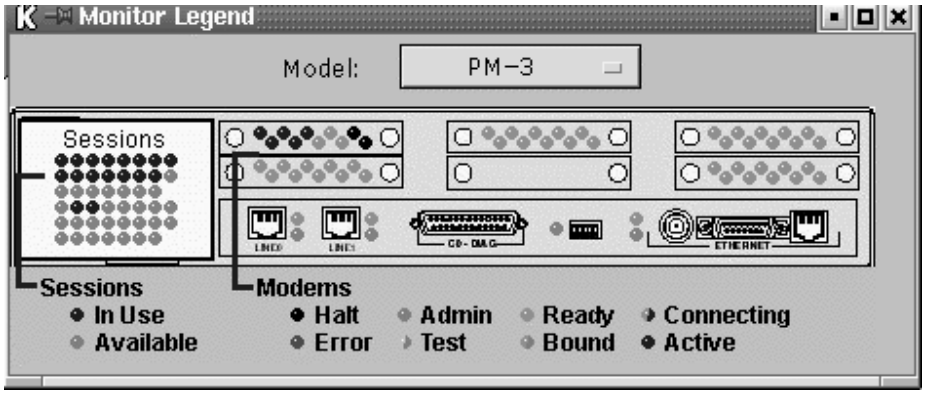

Figura 3 (b) – Visão do Painel Traseiro do Servidor através da Ferramenta Gráfica PMVision [Pmv99].

O PortMaster3 suporta diversos protocolos e serviços, como por exemplo, BGP (*Boder Gateway Protocol)*, ISDN (*Integrated Services Digital Network)*, NAT (*Network Address Translation)*, SNMP (*Simple Network Management Protoco)*, OSPF (*Open Shortest Path First)*, IPSec (*Internet Protocol Security)* [Pmc00]. Por outro lado, ainda possui um sistema operacional embutido, o ComOS, uma ferramenta com interface gráfica para configuração chamada *PMVision* (Figura 5), um protocolo de segurança cliente/servidor chamado *RADIUS* e um pacote de aplicação cliente/servidor chamado *ChoiceNet*.

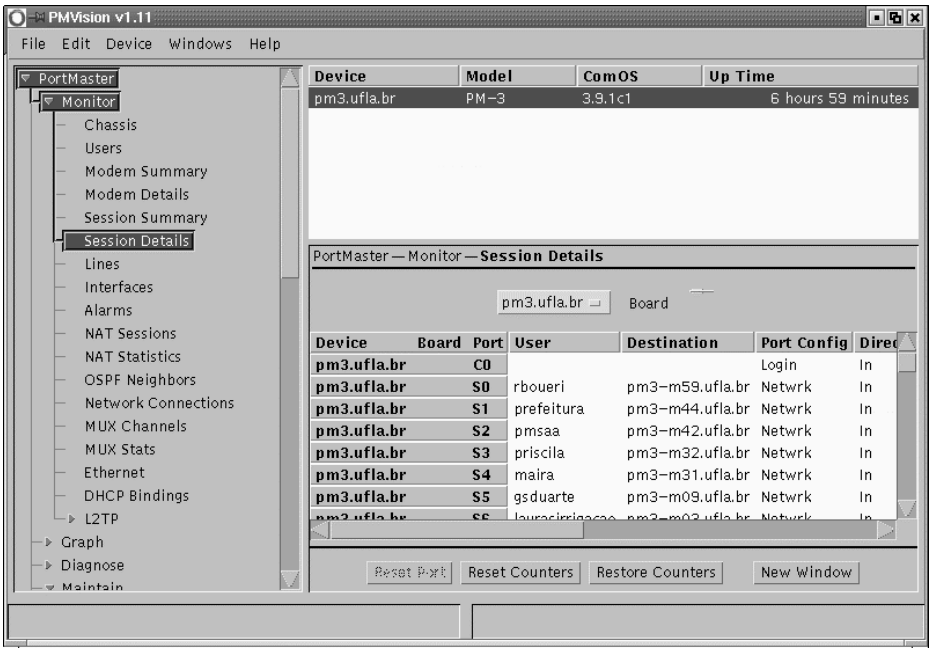

Figura 5 – A Ferramenta Gráfica *PMVision* [Pmv99].

3.1.1 O Protocolo RADIUS

O *Remote Authentication Dial-In User Service* (*RADIUS*) é um protocolo de segurança cliente/servidor criado pela *Livingston Enterprises*. Informação segura é armazenada no servidor RADIUS.

O cliente RADIUS (assim como o servidor de comunicações PortMaster) se comunica com o servidor RADIUS para autenticar usuários. Esse protocolo oferece as seguintes características:

- Alta Segurança: Em grandes redes, informações de segurança podem estar dispersas por toda a rede em diferentes dispositivos. RADIUS permite que informações de usuários sejam armazenadas em um host, minimizando o risco de falhas de segurança. Toda a autenticação e acesso aos serviços de rede são gerenciadas pelo servidor RADIUS.
- Flexibilidade: O software do servidor RADIUS é distribuído no formato código fonte. Desse modo, o protocolo RADIUS pode ser adaptado para trabalhar com sistemas de segurança e protocolos já existentes.
- Gerenciamento Simplificado: As informações de segurança são armazenadas em arquivos texto no servidor; novos usuários podem ser adicionados à base de dados ou informações existentes podem ser modificadas editando estes arquivos texto.
- Capacidade Abrangente de Documentação: As informações coletadas em um arquivo de log podem ser analizadas para propósitos de segurança, ou usadas para faturamento.

Suas funções primárias são autenticação, autorização e contabilização. Quanto à autenticação, a informação é armazenada em um arquivo de usuários local ou acessada de mecanismos externos de autenticação.A autorização controla o acesso a serviços específicos da rede. Uma vez que um usuário é

autenticado, o RADIUS informa ao PortMaster o que o usuário está autorizado a acessar. A contabilização RADIUS permite que administradores de sistemas tenham informações a respeito do histórico do usuário conectado. Esta informação é freqüentemente usada para propósitos de custo.

O servidor RADIUS está disponível para os sistemas operacionais AIX 4.1, Alpha Digital UNIX 3.0, BSD/OS 2.0, HP-UX 10.01, IRX 5.2, Linux 1.2.13 (ELF), Solaris 2.5.1, Solaris x86 2.5.1, SunOS 4.1.4, Windows NT 4.0 Workstation, Windows NT 4.0 Server [Rpm02].

3.1.2 O Servidor ChoiceNet

Consiste em um pacote de aplicação cliente/servidor que faz a filtragem de pacotes. Possui um mecanismo que filtra o tráfego de uma rede de acesso remoto discado. Estas informações são armazenadas no servidor ChoiceNet.

Os clientes ChoiceNet podem ser um ou mais Servidores PortMasters. A comunicação entre clientes e servidor ChoiceNet acontece com o objetivo de determinar o acesso de usuários. ChoiceNet possui as seguintes características:

- Acesso Personalizado: O servidor ChoiceNet usa listas de sites para controlar acessos a hosts específicos, Web sites, e endereços Internet. Com ChoiceNet, um único filtro pode especificar uma lista inteira de hosts ou endereços IP. Provedores de Serviço Internet podem direcionar o acesso para necessidades específicas de seus clientes. Por exemplo, um distrito escolar pode selecionar somente sites de orientação infantil para o acesso de estudantes.
- Gerenciamento Simplificado: Em grandes redes sem um servidor ChoiceNet, filtros devem estar dispersos por toda a rede em diferentes servidores de comunicação ou roteadores. O

servidor ChoiceNet permite que todos os filtros sejam armazenados em um único host. Dessa maneira, há uma liberação de memória no PortMaster para outras necessidades. O armazenamento central elimina a necessidade de atualização de tabelas de filtro em muitos dispositivos clientes.

- Alta Segurança: A filtragem feita pelo servidor ChoiceNet permite que administradores restrinjam acesso interno à rede.
- Flexibilidade: Permite a filtragem tanto de tráfego que chega à rede quanto ao tráfego que sai da rede.
- Capacidade de Documentação: Todas as atividades realizadas pelo servidor podem ser armazenadas em arquivo.

O servidor ChoiceNet está disponível para os sistemas operacionais AIX 4.1, Alpha Digital UNIX 3.0, BSD/OS 2.0, HP-UX 10.01, IRX 5.2, Linux 1.2.13 (ELF), Solaris 2.5.1, Solaris x86 2.5.1, SunOS 4.1.4. Suas duas principais funções são listas de sites centralizadas e gerenciamento centralizado de filtro.

Em relação às listas centralizadas de sites, é permitido escrever regras de filtros para especificar uma lista de sites no lugar de endereços IP. A regra pode permitir ou negar acesso a hosts pertencentes à lista ou para eles.

Quanto ao gerenciamento centralizado de filtro, é permitido, através do servidor, centralizar o armazenamento de um número infinito de filtros. Quando um usuário efetua uma conexão à rede, se um determinado filtro não está na máquina cliente, esta envia um pedido ao servidor ChoiceNet para obter o filtro. Esta é uma função importante porque quando filtros são armazenados localmente na memória não-volátil de cada roteador, ou servidor de comunicação, a quantidade de memória disponível nestes dispositivos limitam o número de regras em cada filtro e o número de filtros definidos.

Tanto o protocolo RADIUS quanto o servidor ChoiceNet já haviam sido configurados e funcionavam perfeitamente antes do início desse trabalho. Portanto, ambos foram estudados apenas com a finalidade de conhecimento já que fazem parte do servidor de acesso remoto [Cpm02].

3.2 Adicionando o Servidor de Acesso Remoto ao Gerenciamento da Rede UFLA

Após o estudo do servidor, seus serviços, protocolos e suas características, foi feita uma análise do mesmo em relação à Rede UFLA. Foi possível observar que apesar do equipamento em questão ser o único que provê acesso remoto à rede da Universidade, ele ainda não estava integrado ao sistema de gerenciamento da rede, ou seja, não era possível analisar os dados recebidos ou enviados à rede através do equipamento, nem fazer análises de tráfego, tampouco do dispositivo ou da rede. Sendo assim, foi habilitado e configurado o protocolo SNMP, o qual tem a função de gerenciamento de rede e é utilizado na Rede UFLA.

3.2.1 SNMP – Simple Network Management Protocol

O modelo SNMP de uma rede gerenciada consiste em quatro componentes:

1. Nós Gerenciados;
2. Estações de Gerenciamento;
3. Informações de Gerenciamento;
4. Um protocolo de Gerenciamento;

Os nós gerenciados podem ser *hosts*, roteadores, pontes, impressoras ou qualquer outro dispositivo capaz de comunicar informações de status para o mundo externo. Para ser diretamente gerenciado através do SNMP, um nó deve ser capaz de executar um processo de gerenciamento SNMP, denominado agente SNMP (*SNMP agent*). Cada agente mantém um banco de dados local contendo variáveis que não só descrevem seu estado e histórico como também afetam sua operação.

O gerenciamento de rede é feito a partir de estações de gerenciamento (management station), as quais são computadores genéricos que rodam um software especial. Na rede UFLA, o software utilizado é o *MRTG* (Multi Router Traffic Grapher). Consiste em um *script Perl* que usa o protocolo SNMP para ler as informações sobre tráfego e um programa em linguagem C que documenta os dados de tráfego. Além disso, o programa cria gráficos que representam o tráfego na conexão de rede monitorada. Esses gráficos são embutidos em páginas HTML. Além disso, o software cria representações visuais do tráfego durante os últimos sete dias ou das últimas quatro semanas ou dos últimos 12 meses, por exemplo. O usuário pode configurá-lo de acordo com os seus objetivos.

As estações de gerenciamento contêm um ou mais processos que se comunicam com os agentes espalhados pela rede emitindo comandos e obtendo respostas.

O SNMP descreve as informações exatas que cada tipo de agente deve manter e o formato a ser aplicado a essas informações. A maior parte do modelo SNMP se refere à definição de quem deverá acompanhar o que e ao modo como essa informação será comunicada.

Cada dispositivo de uma rede (*hosts*, pontes, roteadores, impressoras, etc), mantém uma ou mais variáveis que descrevem seu estado. Na literatura SNMP, essas variáveis são chamadas de objetos. O conjunto formado por todos

os objetos possíveis em uma rede é fornecido em uma estrutura de dados chamada de MIB (*Management Information Base*).

A estação de gerenciamento interage com os agentes utilizando o protocolo SNMP. Esse protocolo permite que a estação de gerenciamento consulte o estado dos objetos locais de um agente, e altere-os se necessário.

Às vezes, acontecem eventos que não estavam planejados, como por exemplo, congestionamentos e falhas. Cada evento significativo é definido em módulo da MIB. Quando um agente percebe que ocorreu um evento significativo, ele imediatamente informa sua ocorrência a todas as estações de gerenciamento de sua lista de configuração. Esse relatório é chamado de *trap* do SNMP.

Como a comunicação entre nós gerenciados e estação de gerenciamento não é confiável, é executado um *polling* (consulta seqüencial) para a confirmação do *trap*. Essa consulta ocorre em longos intervalos, havendo uma aceleração quando há o recebimento de um *trap*. Tal consulta seqüencial é chamada *trap directed polling*.

Segurança e autenticação têm um importante papel no SNMP. Uma estação de gerenciamento tem a capacidade de obter muitas informações sobre todos os nós que estão sob seu controle e também pode desativar todos eles. Portanto, é de grande importância que todos os agentes sejam convencidos de que as consultas que alegam estar vindo da estação de gerenciamento realmente estão vindo de lá.

O modo como o SNMP é normalmente usado é aquele em que a estação de gerenciamento envia uma solicitação a um agente solicitando informações a ele ou forçando-o a atualizar seu estado de alguma forma [Tan97].

3.2.2 Configurando o Protocolo SNMP no RAS

Para habilitar o protocolo SNMP no servidor de acesso remoto, é necessário marcar o item mostrado na Figura 6 e reiniciar o servidor.

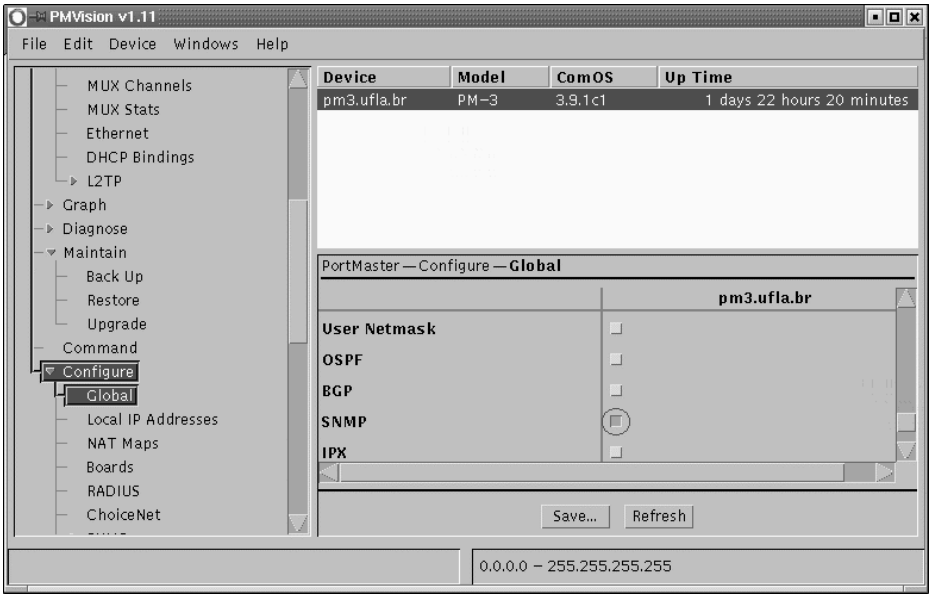

Figura 6 – Tela para habilitação do protocolo SNMP [Pmv99].

Após o reinício do RAS, o clique no item *Configure* e logo em seguida em *SNMP* no menu em forma de árvore, como é mostrado na Figura 7, é importante preencher os campos *Name System* (Nome do Sistema), *Read Community* (Comunidade de Leitura) e *Write Community* (Comunidade de Escrita). Por fim, é necessário clicar no botão *Save* para efetivar a configuração.

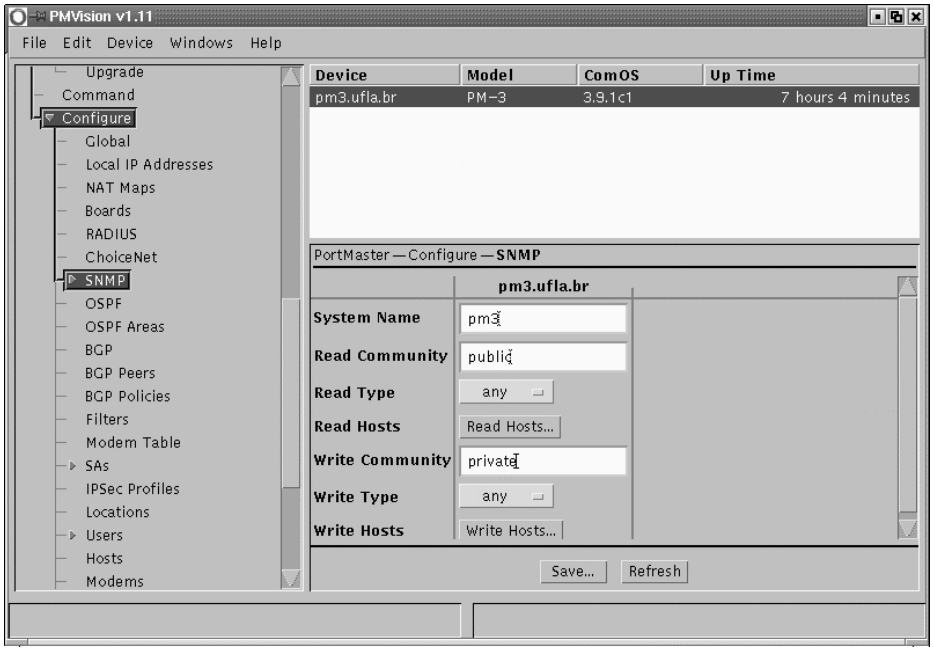

Figura 7 – Configuração SNMP [Pmv99].

As *strings community* permitem o acesso à base de dados MIB de dispositivos selecionados. As *strings community* de escrita e leitura atuam como senhas para permitir o acesso à informação do agente SNMP. A *string community* de leitura deve ser conhecida por qualquer dispositivo que tenha permissão de acesso ou leitura da informação MIB. A *string community* de leitura padrão é *public*. A *string community* de escrita deve ser conhecida por qualquer dispositivo antes que a informação possa ser utilizada pelo agente SNMP. A *string community* de escrita padrão é *private*.

Com a interface de linha de comando, os comandos de configuração são:

Command> **set snmp on|off** //habilita o protocolo

Command> **save all** //salva a configuração

Command> **reboot** //reinicia o servidor

Para configurar *strings community* de leitura e escrita:

Command> **set snmp readcommunity|writecommunity** *Strin*g //habilita as *strings community* de leitura e escrita.

Depois de instalado o protocolo SNMP, não foi observado nenhuma mudança no servidor. Não houve nenhuma mensagem de erro, e muito menos de uma confirmação de que a operação foi realizada corretamente. Para saber se obtivemos sucesso na instalação foi necessário confirmar no MRTG a presença do equipamento na rede gerenciada, como pode ser comprovado nas figuras abaixo:

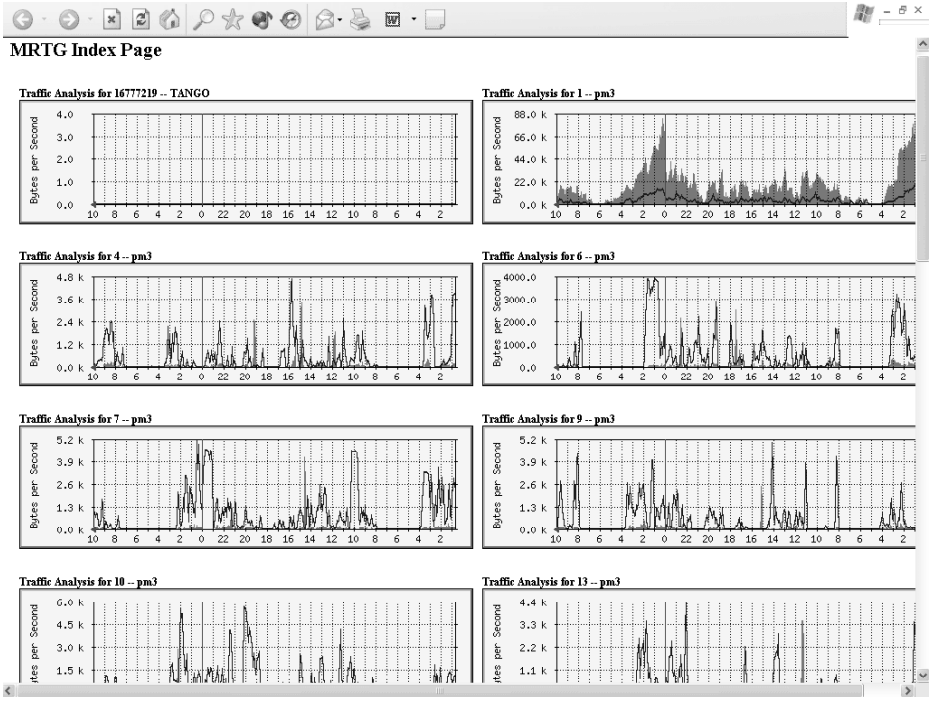

Figura 8 (a) – Tela do software de gerenciamento MRTG

Na Figura 8 (a) são mostrados gráficos dinâmicos do fluxo de dados de várias linhas telefônicas do PortMaster3. Cada gráfico é uma função do número

de bytes por segundo em função da hora. A função em verde representa o fluxo de dados recebidos e a função em azul, o fluxo de dados enviados. Se clicarmos em um desses gráficos de uma linha qualquer, imediatamente uma outra página HTML que ilustra a análise de tráfego da linha é aberta (Figura 8 (b)). Porém, são mostrados gráficos periódicos (gráfico diário, a cada cinco minutos, e semanal, a cada trinta minutos).

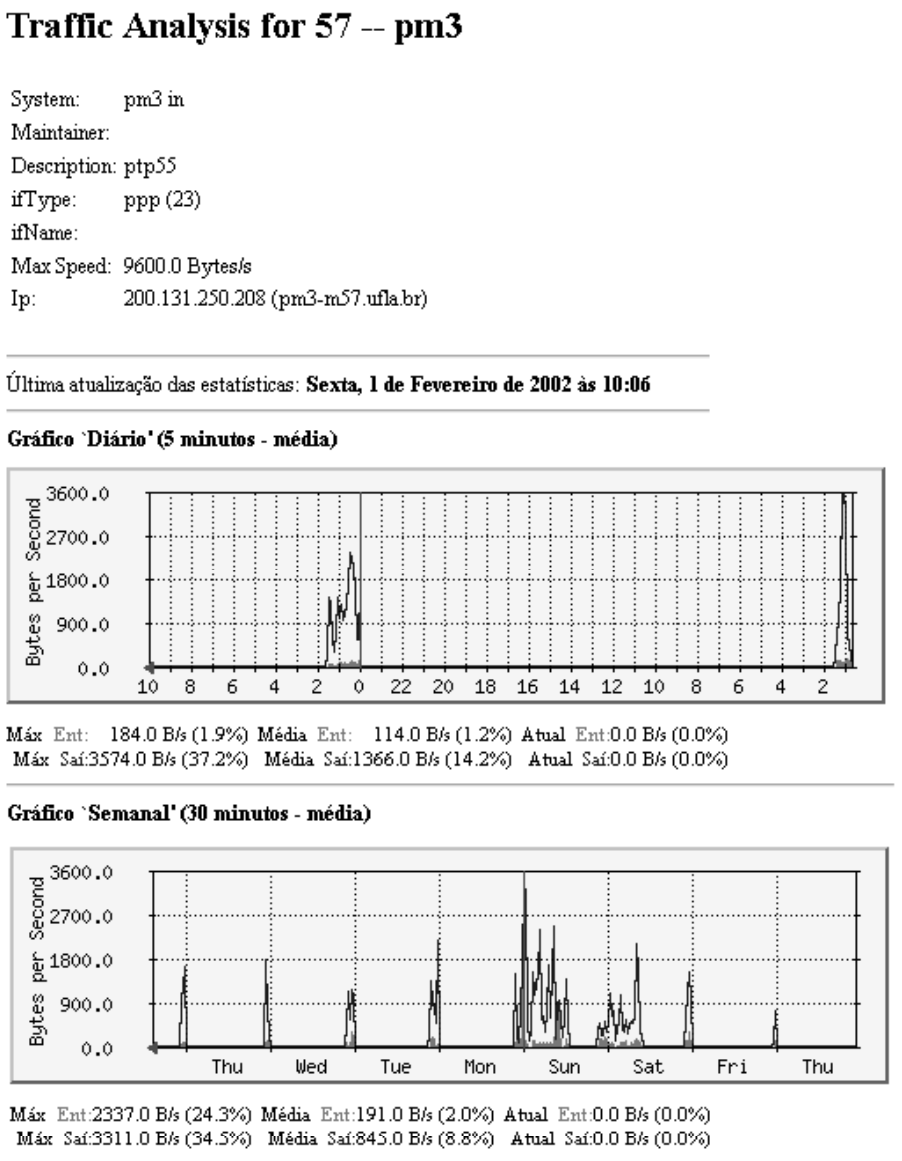

Figura 8 (b) – Gráficos gerados pelo MRTG para o servidor PortMaster3

3.3 Habilitando e Configurando a Tecnologia ISDN

Como foi dito na seção 3.1, o PortMaster3 possui dois feixes de linha E1/T1. No entanto, constatou-se que ambos os feixes estavam sendo usados apenas para conexões via modems, as quais são realizadas através de feixes E1, porém, poderiam estar sendo utilizados para ambas as interfaces.

Portanto, considerando que esta característica do servidor ainda não se encontrava em uso e objetivando uma melhor qualidade e velocidade do acesso remoto à Universidade, foi proposta a implantação do serviço ISDN.

3.3.1 ISDN - Integrated Services Digital Network

Tecnologia digital para telefonia que surgiu para substituir a tecnologia analógica de acesso telefônico existente. A nova tecnologia digital, além dos serviços de voz da telefonia convencional (analógica), torna disponíveis serviços de comunicação de dados, com velocidades superiores às de modems analógicos [Tan97].

3.3.1.1 Arquitetura de Sistema ISDN

A arquitetura utilizada é o túnel de bits digitais entre o cliente e a concessionária de comunicações, através da qual os bits fluem. O túnel de bits pode aceitar vários canais independentes através do uso da multiplexação por divisão do tempo no fluxo de dados.

3.3.1.2 Interface ISDN

O túnel de bits ISDN aceita vários canais interconectados pela multiplexação por divisão do tempo. Os seguintes tipos de canal podem ser padronizados:

A – Canal telefônico analógico de 4 Khz.

B – Canal PCM digital de 64 Kbps para voz ou dados.

C – Canal digital de 8 ou 16 Kbps.

D – Canal digital de 16 Kbps para sinalização fora da banda

E – Canal digital de 64 Kbps para sinalização ISDN interna.

H – Canal telefônico de 384, 1536 ou 1920 Kbps.

Existem dois tipos principais de interfaces ISDN: BRI (ou Básico), voltado ao assinante (residência/empresa) e o PRI (Primário), voltada aos provedores de acesso (ISP) e corporações [Tan97].

3.3.1.3 ISDN/BRI (Basic Rate Interface)

Utilizado em residências ou pequenas empresas, servindo como substituto para acessos telefônicos tradicionais. O ISDN/BRI é composto de dois canais de dados (canais B) de 64 Kbps, e um canal de sinalização (Canal D) de 16 Kbps. Cada canal B pode ser usado tanto para voz(ligação telefônica) quanto para dados (acesso à rede corporativa, a Internet, etc.) [Tea02].

Em uma única linha ISDN, é possível conectar vários dispositivos ISDN, sendo permitido, porém, a utilização simultânea de apenas dois deles. Os dois canais podem ser agrupados, resultando num único link de 128 Kbps para dados.

Na instalação do ISDN/BRI, a companhia telefônica fornece e instala um terminal de rede (NT – Network Terminator) na residência do usuário ou na

empresa. Os equipamentos ISDN (telefone, roteador, placa para PC, kit de vídeo conferência, etc.) são conectados diretamente a esse terminal de rede [Tea02].

3.3.1.4 ISDN/PRI (Primary Rate Interface)

É utilizado por empresas ou provedores de acesso à internet. Na versão européia, adotada pelas companhias telefônicas brasileiras, essa interface é composta por trinta canais de dados (B) e um canal de sinalização (D) de 64 Kbps, fornecidos através de um link interface E1. A versão americana por sua vez possui 23 canais B e um canal D, fornecidos através de um link interface T1.

Nessa interface os canais de dados também podem ser agrupados, além de possuir os serviços disponíveis para o ISDN/BRI. Na utilização em comunicação de dados, podem ser utilizados tanto para interligação de redes, quanto para acesso remoto.

Para instalação do ISDN/PRI, normalmente feita no provedor de acesso ou na empresa, a companhia telefônica fornece um tronco digital com interface ISDN/PRI (30 canais B e 1 canal D), que deve ser conectado diretamente a um equipamento do tipo RAS integrado que suporta esta interface[Tea02].

3.3.1.5 Benefícios

- Velocidade de transmissão de dados;
- Velocidade de estabelecimento de conexão;
- Disponibilidade da linha;

3.3.1.6 Perspectivas

Para uso doméstico, a maior demanda por novos serviços será, sem dúvida em relação aos serviços de vídeo sob demanda.

As LANs atualmente disponíveis oferecem pelo menos 10Mbps e estão sendo substituídas por LANs de 100 Mbps. Sendo assim, a tecnologia ISDN torna-se obsoleta para este fim.

Porém, essa tecnologia pode ser totalmente aplicada no acesso à Internet com um canal de até 128 Kbps [Tan97].

3.3.2 Configurando a Tecnologia ISDN no RAS

Antes de ser efetuada esta configuração, primeiramente foi atualizada a versão do sistema operacional do servidor, o ComOS. A versão foi atualizada da versão 3.8.2c4 para a 3.9.1c1. Para que o sistema operacional possa ser atualizado, é necessário que dois terminais sejam abertos por medida de segurança, já que o sistema operacional se encontra embutido no equipamento. Desse modo, se houver algum problema durante a atualização, haverá uma maneira de acessar o sistema através do outro terminal aberto anteriormente. A configuração da tecnologia ISDN no servidor de acesso remoto é feita através da interface de linha de comando:

```
//configuração da linha 0
Command> set line0 isdn
Command> set line0 signal r2generic
Command> set line0 framing crc4
Command> set line0 encode hdb3
Command> save all

//configuração da linha 1
```

Command> **set line1 isdn**

Command> **set line1 signal r2generic**

Command> **set line1 framing crc4**

Command> **set line1 encode hdb3**

Command> **set isdn euro**

Command> **save all**

Command> **reboot**

Semelhante à configuração do protocolo SNMP, depois de efetuados os procedimentos para a implantação da tecnologia ISDN não houve nenhuma mensagem de sucesso ou de erro. A confirmação de que a tecnologia foi habilitada só foi possível depois do acesso feito pelo primeiro usuário deste tipo de conexão. Além disso, a configuração também pode ser feita pelo modo gráfico.

Ao clicar no item *Configure* e em seguida em *Lines*, o administrador visualiza as linhas que podem ser configuradas graficamente (Figura 9(a)). Para configurar uma linha, é necessário selecioná-la e então clicar no botão *Edit* localizado na parte inferior central da tela.

Já na Figura 9 (b)A próxima tela está relacionada à linha escolhida. Nesse exemplo, a linha escolhida foi a linha 1 (Repare que o item *line 1* está marcado). Nessa tela, o administrador poderá configurá-la como foi efetuado no exemplo em linha de comando, já que os parâmetros são os mesmos.

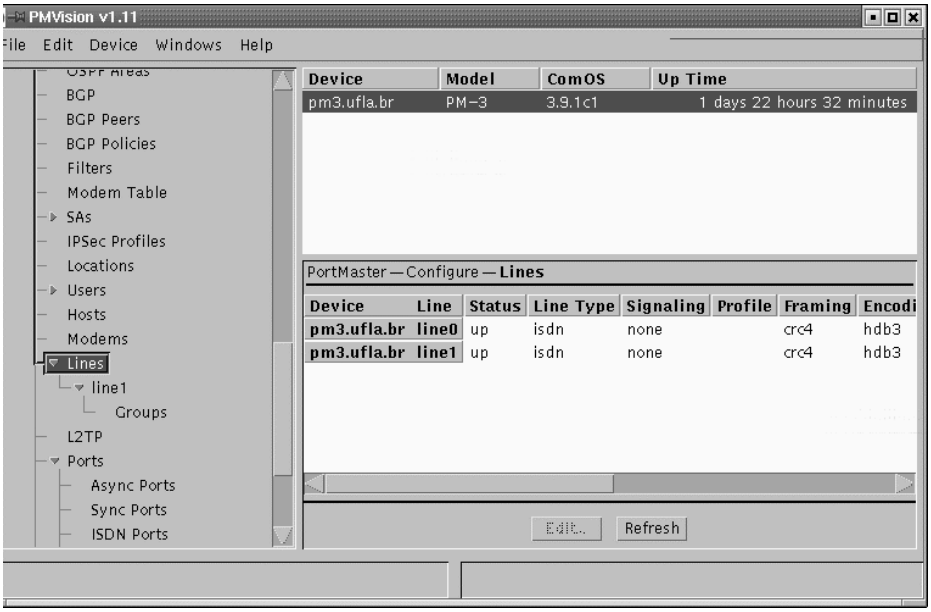

Figura 9 (a) – As linhas ISDN a serem configuradas.

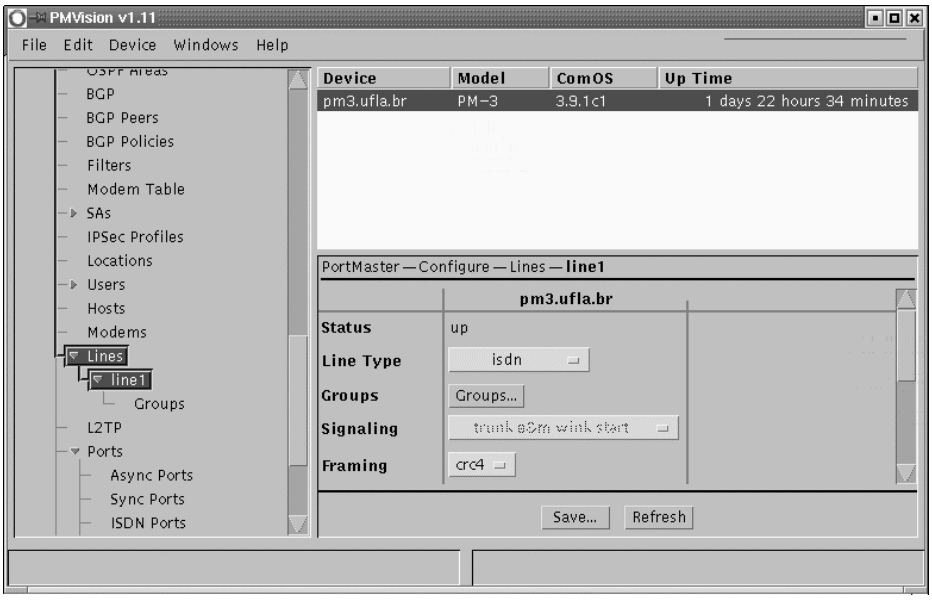

Figura 9 (b) – Linha ISDN a ser configurada [Pmv99].

3.4 Análise Heurística da Interface da Ferramenta PMVision

A ferramenta gráfica PMVision é parte integrante do servidor de acesso remoto, já que é utilizada para configuração e gerenciamento do RAS. Desse modo será feita uma Análise Heurística onde serão apresentados pontos favoráveis e desfavoráveis da ferramenta.

Em vista de a mesma idéia quanto à interface existir para as diversas possibilidades de serviços a serem configurados, e já que demonstrar aqui todas as telas existentes na ferramenta seria inviável para este trabalho, a configuração do protocolo SNMP foi escolhida para servir como exemplo (Figura 7) por fazer parte deste.

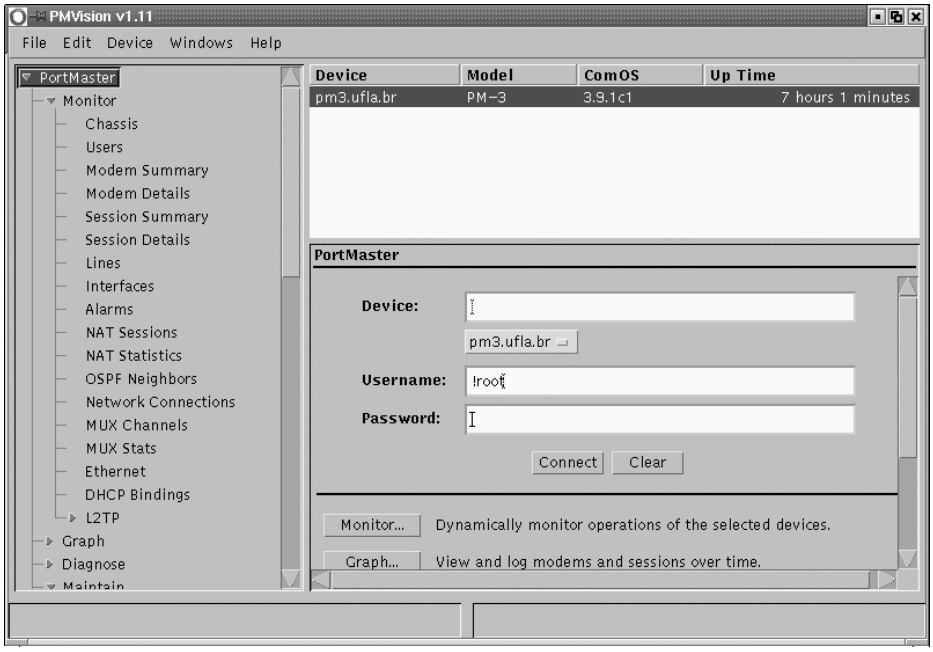

Figura 10 – Tela inicial do PMVision

A Figura 10 mostra a tela de entrada da ferramenta PMVision. O usuário, o qual é o administrador da rede, deve digitar o seu *username* e *password*, habilitando o trabalho com a ferramenta. É possível notar que há um *Diálogo simples e natural*, pois o administrador pode escolher um determinado tipo de serviço apenas selecionando-o no menu árvore no lado esquerdo da tela através do nome do serviço ou protocolo. Este tipo de interface aumenta a produtividade e torna a usabilidade do PMVision fácil se assumido que, por ser um administrador de rede, o usuário domina os serviços mostrados no menu. Dessa maneira, esta outra característica demonstra também que a interface da ferramenta *fala a língua do usuário*, apesar de não ocorrerem metáforas para facilitar minimizar o tempo ao acesso de alguma informação.

Ainda com relação às Figuras 7 e 10, pode-se notar que não há *saídas claramente marcadas*. A única saída existente é o ícone localizado no canto superior direito da tela. Ao clicar nesse ícone, a ferramenta é encerrada e a saída do usuário é feita automaticamente. Infelizmente esta informação não está explícita ao usuário. Além disso, não há opções de *retorno* devido à liberdade do usuário de navegar de modo fácil e intuitivo no menu árvore localizado à esquerda. Quanto à minimização de erros, o PMVision mostra uma tela com os parâmetros anteriores e com os futuros para a confirmação da mudança de configuração, como demonstra a Figura 10 com um exemplo de mudança de configuração SNMP.

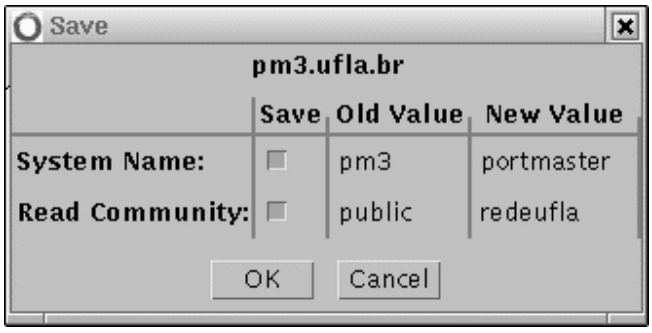

Figura 10 – Confirmação de mudança de configuração SNMP.

Ainda com relação à interface, a ajuda da ferramenta é bem completa e intuitiva. A documentação é rica, contendo manuais sobre configuração de hardware, do servidor ChoiceNet, RADIUS e sobre a ferramenta PMVision.

Capítulo 4

Conclusões

A Rede UFLA não estava sendo completamente gerenciada, pois um de seus principais componentes, o servidor de acesso remoto, não estava configurado para o gerenciamento.

Portanto, o presente trabalho, objetivando aumentar a qualidade do acesso remoto e considerando o Modelo de Gerenciamento OSI, contribuiu para um melhor gerenciamento da rede citada tratando exclusivamente desse componente da rede. Sendo assim, foram realizadas melhorias quanto ao gerenciamento de desempenho, configuração, contabilização e de falhas já que foi habilitada a tecnologia ISDN para o acesso mais veloz e eficiente (desempenho e configuração) foi configurado o protocolo SNMP para que o servidor pudesse integrar a rede gerenciada fornecendo informações sobre possíveis falhas, além de informações sobre tráfego e desempenho da rede (desempenho, falhas e contabilização).

A escolha de um RAS para prover acesso remoto à Rede UFLA é louvável já que servidores de acesso remoto são mais baratos para se colocar em funcionamento se a maioria dos usuários estão na área local de chamadas, e VPNs são mais baratas se muitos dos usuários estão a longas distâncias [Fre99].

Por ser um ISP, o servidor de acesso remoto deve prover o acesso tanto via modem quanto via tecnologia ISDN, pois o que está sendo priorizado é a qualidade do acesso.

Quanto ao número de portas a serem utilizadas, é necessário que seja utilizado o número máximo para a maioria dos usuários possam obter o acesso.

No entanto, por possuir sessenta modems, o que vem a ser uma quantidade insatisfatória devido ao número de usuários que necessitam do acesso, foi adquirido mais um RAS para suportar a demanda. Esse servidor é um MAX 6000 da Lucent Technologies, o qual possui 4 feixes E1/T1 com capacidade de trinta linhas cada feixe, possibilitando um total de 120 usuários acessando simultaneamente a rede. Desse modo, a Rede UFLA poderá suportar 180 usuários remotos simultâneos.

Portanto, após a conclusão deste, pode-se dizer que a qualidade do acesso remoto à Rede UFLA foi melhorada, pois uma nova forma de acesso foi configurada (ISDN), e o servidor de acesso remoto, o qual é um dos principais componentes da rede, está sendo gerenciado graças à execução deste trabalho, o que de certo modo justifica o investimento nesse equipamento tão poderoso.

É importante ressaltar também que, embora o trabalho tenha sido desenvolvido baseado nos problemas de gerenciamento de rede encontrados especificamente na Rede UFLA, ele pode ser aplicado a qualquer instituição ou organização onde o mesmo problema ou algo semelhante possa vir a ocorrer.

4.1 Trabalhos Futuros

Apesar desse trabalho cumprir o seu objetivo, pôde ser observado que o equipamento utilizado para o desenvolvimento deste possui muitos serviços a serem explorados em todos os tipos de gerenciamento de rede discutidos no modelo OSI.

Além disso, o RAS ainda não está sendo utilizado em toda sua capacidade, o que estimula ainda mais novos trabalhos para que futuramente, baseado nos problemas de gerenciamento encontrados na Rede UFLA, ele possa ser mais uma vez utilizado para minimizar tais problemas e maximizar a qualidade do acesso remoto.

Capítulo 5

Referências Bibliográficas

[Ara01] ARAGON B. C.; Artigo: Gerenciamento Remoto a Servidores de Redes Locais: Gerenciamento Via WEB x Gerenciamento Via Terminal, 2001.

[Cis99b] CISCO SYSTEMS INC; Integrated Services Digital Network, manuscrito1999. [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/isdn.htm].

[Cis99a] CISCO SYSTEMS INC.; Network Management Basic, manuscrito, 1999. [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics].

[Cyc02] CYCLADES; Servidores de Acesso Remoto, manuscrito 2002. [http://www.cyclades.com.br/doc_tecnicos/inf_wp_ce_04.php3].

[Com97] COMER, D.E; Computers networks and Internets, Prentice Hall, 1997.

[Fre99] FREED L; Being There: Remote Access Servers, 1999.

[Gat00] GATENS D; RAS plataforms transition, Communications News, 2000.

[Kee98] KEENAM, M; Remove Revs Up, Communication News, 1998.

[Mit00] MITTON D; BEADLES M; Network Access Server Requirements Next Generation (NASREQNG) NAS Model, 2000.

[Nie93] NIELSEN, J; Usability Engineering. Chestnut, MA : Academic Press, 1993.

[Oda94b] ODA, C.S; Artigo: Introdução à Gerência de Redes, 1994.

[Oda94a] ODA, C.S; Artigo: Gerenciamento de Redes de Computadores – Noções Básicas, 1994.

[Pas99] PASSMORE D; Will VPNs Replace RAS System? 1999.

[Pet00] PETERSON L. L., DAVIE B. S.; Computer Networks, 2 ed., Morgan Kauffman, 2000.

[Cpm02] PORTMASTER3; ChoiceNet Administrator's Guide, 2002.

[Pmc00] PORTMASTER3; PortMaster Configuration Guide, 2000.

[Hpm02] PORTMASTER3; Portmaster3 Hardware Installation Guide, 2002.

[Pmv99] PORTMASTER3; PMVision User's Guide, 1999.

[Rpm02] PORTMASTER3; RADIUS Administrator's Guide, 2002.

[Sie02] SIEGL M. R.; What is Network Management, manuscrito, 2002. [http://netman.cit.buffalo.edu/Doc/Papers/sie9412E.ps]

[Tan97] TANEMBAUM, A. S; Redes de Computadores, 4 ed., Campus, 1997.

[Tea02] TEAMNET, Tecnologia ISDN, manuscrito 2002. [http://www.teamnet.com.br/inf_wp_ce_11.html].

[Ufl98] UNIVERSIDADE FEDERAL DE LAVRAS. Relatório: Relatório de Atividades do Setor de Redes e Internet do CIN-UFLA de 1996 até o momento, 1998.