UNIVERSIDADE DE SÃO PAULO
INSTITUTO DE FÍSICA DE SÃO CARLOS
DEPARTAMENTO DE FÍSICA E INFORMÁTICA

**DESENVOLVIMENTO DE FERRAMENTAS PARA GERENCIAMENTO
REMOTO DE INTRANETS**

MARCELO QUINTINO DA SILVA

Dissertação apresentada ao Instituto de Física de São Carlos, Universidade de São Paulo, para
obtenção do título de Mestre em Ciências “Física Aplicada: Opção Física Computacional”

Orientador: Prof. Dr. Álvaro Garcia Neto

ou

USP/IFSC/SBI

8-2-001318

São Carlos – São Paulo
2000

IFSC-USP SERVIÇO DE BIBLIOTECA
INFORMAÇÃO

Silva, Marcelo Quintino da

"Desenvolvimento de ferramentas para gerenciamento remoto de intranets" / Marcelo Quintino da Silva – São Carlos, 2000

Dissertação (Mestrado) – Instituto de Física de São Carlos da Universidade de São Paulo, 2000
– páginas: 140

Área: Física Aplicada: Opção Física Computacional
Prof. Dr. Álvaro Garcia Neto

1. Redes de computadores, 2. HTML, 3. Gerenciamento

I. Título

**IFSC UNIVERSIDADE
DE SÃO PAULO**
Instituto de Física de São Carlos

Av. Dr. Carlos Botelho, 1465
CEP 13560-250 - São Carlos - SP
Brasil

Fone (016) 273-9333

Fax (016) 272-2218

**MEMBROS DA COMISSÃO JULGADORA DA DISSERTAÇÃO DE MESTRADO DE
MARCELO QUINTINO DA SILVA APRESENTADA AO INSTITUTO DE FÍSICA DE SÃO
CARLOS, DA UNIVERSIDADE DE SÃO PAULO, EM 09 DE MAIO DE 2000**

COMISSÃO JULGADORA:

Prof. Dr. Álvaro Garcia Neto/IFSC-USP

Prof. Dr. Jan Frans Willem Slaets/IFSC-USP

Prof. Dr. Eduardo Marques/ICMC-USP

E mail: wladerez@if.sc.usp.br

Apresentação

Esse trabalho visadesenvolver ferramentas para gerenciamento de uma rede IP de computadores. As ferramentas foram desenvolvidas para serem utilizadas por usuários com poucos conhecimento de redes de computadores e Unix. Para atingir essas metas o projeto selecionou os comandos do Unix necessários, mascarando-os através de ações específicas. Dessa forma foi disponibilizado os comandos mínimos necessários para um bom gerenciamento. O conjunto de ferramentas criado, denominado MSP, foi implantado em todas as Unimeds do estado de Santa Catarina para gerenciamento da UniRed. A UniRed é o nome da intranet das Unimeds de Santa Catarina.

Abstract

This work aims to develop tools to manage a IP network of computers. All tools were developed to be used by someone without extensive knowledge or background in computer networks or Unix. To achieve those goals, the project identified the required Unix commands and masked them behind especific procedures. This way, a set of tools become became available that enables good network management. The set of tools is named MSP and was used in all Unimeds in Santa Catarina/Brazil statesmanaging the UniRed. UniRed is the Santa Catarina intranet.

Ao Marcelo por
agüentar o Format.

Agradecimentos

Ao Professor Álvaro por acreditar em mim especialmente nas fases mais difíceis. Tenho um professor, um orientador e especialmente um amigo.

Valeu Professor Carlos Antonio *Totó* Rugiero por todas as respostas não dadas, com elas certamente eu teria aprendido menos.

A todos os amigos ao longo da graduação, onde esse trabalho teve início e me acompanharam até esse momento. Em especial ao Rodrigo *Belém* Tuma Rotta, Sérgio e ao Fernando *Doc* Delgado: regado a muitas pizzas e visitas a Guanabara, nós montamos um laboratório e uma família.

Aos demais amigos que foram chegando aos poucos: Andresal, Luiz Fernando *Sagui* Roldan, Philipe *Bino* Wegmüller e muitos outros. Tivemos o prazer de ensinar um pouco e aprender muito.

A duas pessoas especiais sem os quais eu não teria sequer saído de minha cidade: Seu Pedro e Dona Maria Hermínia, meus pais. Obrigado por sempre respeitarem minhas vontades e encorajar a continuar. Cada batalha vencida foi e sempre será compartilhada com vocês porque essas vitórias são nossas.

A minha esposa Elaine pela compreensão e suporte durante a finalização dessa tese.

Sumário

<u>1. PRINCÍPIOS DE GERENCIAMENTO REMOTO DE REDES</u>	<u>2</u>
1.1 CONTEXTO HISTÓRICO: UNIX E INTERNET	2
1.2 NECESSIDADES NO GERENCIAMENTO DE INTRANET À DISTÂNCIA	6
1.2.1 TIPOS DE PROBLEMAS	6
1.2.1.1 Pós evento	7
1.2.1.2 Durante o Evento	8
1.2.1.3 Detectando o Problema	9
1.2.1.4 Técnicas de Diagnóstico	10
1.2.1.5 Agilidade	10
1.2.2 GERÊNCIA	11
1.3 FERRAMENTAS ATUAIS DE GERENCIAMENTO DE INTRANET À DISTÂNCIA	12
1.3.1 SNMP	13
1.3.1.1 Vantagens e Desvantagens do SNMP	14
1.3.2 MIB E MIBII	15
1.3.3 RMON	16
1.3.3.1 Grupos do RMON	16
1.3.4 DESAFIOS	18
<u>2. SOFTWARES DE GERENCIAMENTO</u>	<u>20</u>
<u>3. DESCRIÇÃO DO SOFTWARE MSP</u>	<u>28</u>
3.1 EQUIPAMENTO UTILIZADO	28
3.2 CARACTERÍSTICAS DO SISTEMA	29

3.2.1	APACHE	29
3.2.2	NAVEGADORES	29
3.2.3	HTML	30
3.2.4	CGI	31
3.2.5	SSL – CRIPTOGRAFIA POR CHAVE PÚBLICA E CERTIFICADOS	31
3.3	GERENCIAMENTO NÍVEL 1: GERENCIANDO A MÁQUINA	32
3.3.1	SERVIDOR WWW	36
3.3.1.1	Configurar Servidor WWW	36
3.3.1.2	Ativar o Servidor WWW	39
3.3.1.3	Enviar Arquivo	40
3.3.1.4	Remover Arquivos ou Diretórios	42
3.3.2	SERVIDOR DE CORREIO ELETRÔNICO	44
3.3.2.1	Roteador de mensagens eletrônicas	45
3.3.2.2	Servidor de correio eletrônico	45
3.3.2.3	Grupos de usuários	47
3.3.3	SERVIDOR DE ARQUIVOS	55
3.3.3.1	Configuração do Servidor de Arquivos	56
3.3.3.2	Manutenção do Servidor de Arquivos	63
3.3.4	SERVIDOR DE NOMES	69
3.3.4.1	Criar o Servidor de Nomes	70
3.3.4.2	Ligar ou Desligar o Servidor de Nomes	71
3.3.4.3	Adicionar Nome	72
3.3.4.4	Listar Nomes	74
3.3.4.5	Remover Nomes	75
3.3.5	BANCO DE MODEMS	77
3.3.5.1	Configurando Modems	79

3.3.5.2	Especificar Servidor de Acesso	85
3.3.5.3	Obtendo Status Atual dos Modems	87
3.3.6	TABELA DE ROTEAMENTO	88
3.3.6.1	Listar Tabela de Roteamento	89
3.3.6.2	Adicionar Rota Estática na Tabela de Roteamento	90
3.3.6.3	Remover Rota Estática na Tabela de Roteamento	92
3.3.6.4	Remover Todas as Rotas	93
3.3.6.5	Testar Rota Específica	94
3.3.7	USUÁRIOS	95
3.3.7.1	Adicionar Usuário	98
3.3.7.2	Alterar Usuários.	101
3.3.7.3	Remover Usuário	103
3.3.8	SENHA	105
3.3.9	FUNCIONAMENTO	106
3.3.10	CONEXÃO REMOTA VIA MODEM	109
3.4	GERENCIAMENTO NÍVEL 2: GERENCIANDO OS RECURSOS	112
3.4.1	ALTERAR SENHA DE ACESSO DO GN2	113
3.4.2	ALTERAR SENHA DE ACESSO DO GN1	114
3.4.3	BACKUP COM ENVIO VIA FTP	115
3.4.4	BACKUP COM ARMAZENAGEM EM DISCO	118
3.4.5	RESTAURAR BACKUP	119
3.4.6	REDE - ALTERAR NOME, ENDEREÇO IP, ROTEADOR E MÁSCARA	120
3.4.7	PING	123
3.4.8	TRACEROUTE	126
4.	<u>ANÁLISE COMPARATIVA</u>	128

4.1	ESSE PACOTE TEM DUAS CARACTERÍSTICAS IMPORTANTES	128
4.2	QUALQUER PESSOA GERENCIA	129
4.3	GERENCIA IP	131
4.4	APLICAÇÃO – UNIRED SANTA CATARINA	132
5.	<u>TRABALHOS FUTUROS.</u>	<u>135</u>
6.	<u>BIBLIOGRAFIA</u>	<u>138</u>

Lista de Tabelas

TABELA 1 - CATEGORIAS DOS OBJETOS.

Lista de Códigos

CÓDIGO 1 - PORÇÃO DO WEBSERVER.PL QUE OBTÉM O NÚMERO IP E O NOME DA MÁQUINA.	37
CÓDIGO 2 - CÓDIGO DA PÁGINA DA FIGURA 7.	37
CÓDIGO 3- HABILITANDO O SERVIDOR DE MENSAGENS ELETRÔNICAS.	46
CÓDIGO 4 - DESABILITANDO O SERVIDOR DE MENSAGENS ELETRÔNICAS.	46
CÓDIGO 5 - ENVIANDO SINAL PARA REINICIALIZAR O PROCESSO INETD.	47
CÓDIGO 6 - SALVANDO ALTERAÇÕES E ATIVANDO ALIASES.	49
CÓDIGO 7 - ARQUIVO DE USUÁRIOS INSCRITOS.	49
CÓDIGO 8 – FORMATAÇÃO DA LISTA DE GRUPOS.	51
CÓDIGO 9 - FORMATAÇÃO DA LISTA DE USUÁRIOS.	51
CÓDIGO 10 - SALVANDO ALTERAÇÕES E ATIVANDO ALIASES.	53
CÓDIGO 11 - ATUALIZANDO ARQUIVO E SALVANDO ARQUIVOS ORIGINAIS.	54
CÓDIGO 12 – FORMATAÇÃO DA LISTA DE GRUPOS.	55
CÓDIGO 13 - CRIANDO MENSAGEM DE ENTRADA DO SERVIDOR DE ARQUIVOS.	59
CÓDIGO 14 - ALTERAÇÃO DO NÚMERO CLIENTES.	61
CÓDIGO 15 - ALTERANDO CONFIGURAÇÃO PARA ACESSO ANÔNIMO.	63
CÓDIGO 16 - VERIFICANDO A EXISTÊNCIA DO ARQUIVO /ETC/FTPSHUT.	64
CÓDIGO 17 – EXECUTANDO A AÇÃO DE LIGAR OU DESLIGAR O SERVIDOR DE ARQUIVOS.	64
CÓDIGO 18 - EXECUÇÃO DO COMANDO FTPWHO E FORMATAÇÃO DA SAÍDA.	66
CÓDIGO 19 - AÇÕES REGISTRADAS DO SERVIDOR DE NOMES NO ARQUIVO DE LOG.	70
CÓDIGO 20 - PASSANDO INFORMAÇÕES PARA CRIAR ARQUIVOS INICIAIS.	71
CÓDIGO 21 - INICIALIZANDO O SERVIDOR DE NOMES.	72
CÓDIGO 22 - TESTES DE VALIDAÇÃO DO NÚMERO IP.	74
CÓDIGO 23 - OBTENDO DADOS DO ARQUIVO DO SERVIDOR DE NOMES	75
CÓDIGO 24 - ATUALIZANDO ARQUIVO DE ESTADO DA LINHA SERIAL.	79

CÓDIGO 25 – <i>GETSTATUS</i> : DETECTANDO O ESTADO DA LINHA E EMITINDO SINAL SONORO.	79
CÓDIGO 26 - ARQUIVO <i>/TOTAL/MODEM/MODEM.STATUS</i> .	81
CÓDIGO 27 - ARQUIVO <i>/ETC/TTYS</i> .	83
CÓDIGO 28 - ARQUIVO <i>START_MULTSER.6</i> DE UMA LINHA DEDICADA COM PROTOCOLO <i>PPP</i> .	84
CÓDIGO 29 - ARQUIVO <i>START_MULTSER.7</i> DE UMA LINHA DEDICADA COM PROTOCOLO <i>SLIP</i> .	84
CÓDIGO 30 - ARQUIVO <i>START_MULTSER_7_CUAC6</i> PARA CONFIGURAÇÃO DA INTERFACE COM PROTOCOLO <i>SLIP</i> .	85
CÓDIGO 31 - FORMATANDO SAÍDA DA CONFIGURAÇÃO DA LINHA SERIAL.	88
CÓDIGO 32 - ARQUIVO <i>/TOTAL/ROUTE.TOTAL</i> .	88
CÓDIGO 33 - FORMATAÇÃO DA SAÍDA DO COMANDO <i>NETSTAT</i> .	90
CÓDIGO 34 - VALIDANDO OS VALORES PASSADOS.	91
CÓDIGO 35 - ADICIONANDO ROTA ESTÁTICA AO ARQUIVO <i>/TOTAL/ROUTE.TOTAL</i> .	92
CÓDIGO 36 - REMOVENDO ROTA DE <i>/TOTAL/ROUTE.TOTAL</i> E DA TABELA DE ROTEAMENTO ATIVA.	93
CÓDIGO 37 - REMOVENDO ROTAS ESTÁTICAS DO ARQUIVO <i>/TOTAL/ROUTE.TOTAL</i> E DA TABELA DE ROTEAMENTO.	93
CÓDIGO 38 - FORMATAÇÃO DE SAÍDA DO TESTE DE ROTA.	94
CÓDIGO 39 - GERANDO A PÁGINA DE MANUTENÇÃO DE USUÁRIOS (FIGURA 72)	97
CÓDIGO 40 - FORMATANDO A LISTAGEM DOS USUÁRIOS CADASTRADOS.	97
CÓDIGO 41 - ARQUIVO <i>/ETC/MASTER.PASSWD</i> .	97
CÓDIGO 42 - TESTANDO AS SENHAS PASSADAS; CHAMANDO A SUBROTINA PARA ADICIONAR USUÁRIO.	100
CÓDIGO 43 - CHAMADA DE SISTEMA PARA ADICIONAR USUÁRIO.	100
CÓDIGO 44 - VERIFICANDO ALTERAÇÃO DE INFORMAÇÕES.	103
CÓDIGO 45 - GERANDO O NOVO ARQUIVO DE SENHAS DO SISTEMAS.	103
CÓDIGO 46 - CHAMADA DE SISTEMA PARA REMOVER USUÁRIO.	104

CÓDIGO 47 - VALIDAÇÃO DAS SENHAS DIGITADAS.	105
CÓDIGO 48 - ARQUIVO DE SENHA PARA ACESSO AO GERENCIAMENTO NÍVEL 1.	106
CÓDIGO 49 - PORÇÃO DO CÓDIGO QUE CODIFICA SENHA.	106
CÓDIGO 50 - ARQUIVO <i>/ETC/CRONTAB</i> .	108
CÓDIGO 51 - CRIANDO ARQUIVO <i>/TOTAL/SISTEMAS/.REBOOT</i> .	108
CÓDIGO 52 - ARQUIVO <i>SUPPORT/PASSWORD.SISTEMAS</i> .	114
CÓDIGO 53 - ALTERAÇÃO DA SENHA DE ACESSO AO GERENCIAMENTO NÍVEL 1.	115
CÓDIGO 54 - TESTANDO PARÂMETROS DA MÁQUINA REMOTA.	116
CÓDIGO 55 - ENVIO VIA <i>FTP</i> DO <i>BACKUP</i> .	118
CÓDIGO 56 - CÓDIGO <i>JAVASCRIPT</i> QUE GERA O AVISO.	118
CÓDIGO 57 - CHAMADA DE SISTEMA PARA RESTAURAR <i>BACKUP</i> .	120
CÓDIGO 58 - ARQUIVO DE INICIALIZAÇÃO DA REDE.	122
CÓDIGO 59 - ARQUIVO DE CONFIGURAÇÃO DO SERVIDOR <i>HTTP</i> .	122
CÓDIGO 60 - REALIZANDO ALTERAÇÕES NOS ARQUIVOS DE CONFIGURAÇÃO DE REDE E DO SERVIDOR DE <i>HTTP</i> .	122
CÓDIGO 61 - CHAMADA DE SISTEMA DO COMANDO <i>PING</i> .	125
CÓDIGO 62 - CHAMADA DE SISTEMA DO COMANDO <i>TRACEROUTE</i> .	126

Lista de Figuras

FIGURA 1 - MENU DE CONFIGURAÇÃO DE REDE DA DIGITAL UNIX.	21
FIGURA 2 - INTERFACE DE CONFIGURAÇÃO NO OSF.	22
FIGURA 3 - DEFININDO PARTIÇÕES NO DIGITAL UNIX.	22
FIGURA 4 - INTERFACE DE ADMINISTRAÇÃO DO SOLARIS.	23
FIGURA 5 - ADICIONANDO USUÁRIO NO SOLARIS.	24
FIGURA 6 - GERENCIAMENTO DO SCO.	25
FIGURA 7 - CONFIGURANDO CORREIO ELETRÔNICO NO SCO.	25
FIGURA 8 - CRIANDO GUI PARA COMANDOS NO SOLARIS.	26
FIGURA 9 - MENSAGEM DE ERRO GERADA DA AÇÃO <i>BACKUP MANAGER</i> DO SCO.	27
FIGURA 10 - PROCESSO DE AUTENTICAÇÃO E CRIPTOGRAFIA	33
FIGURA 11 - SENHA DE ACESSO PARA O GERENCIAMENTO NÍVEL 1	34
FIGURA 12 - PÁGINA PRINCIPAL DO GERENCIAMENTO NÍVEL 1	34
FIGURA 13 - CONTROLE DO SERVIDOR WWW	37
FIGURA 14 - CONFIGURANDO O SERVIDOR WWW	38
FIGURA 15 - PÁGINA DE CONFIRMAÇÃO DE INSTALAÇÃO	39
FIGURA 16 - INICIALIZAR O SERVIDOR WWW	40
FIGURA 17 - TESTAR O SERVIDOR WWW	40
FIGURA 18 - ENVIAR ARQUIVO PARA O SERVIDOR WWW	41
FIGURA 19 - ENVIAR ARQUIVO VIA UNIDADE DE DISQUETE	42
FIGURA 20 - REMOVENDO ARQUIVOS OU DIRETÓRIOS DO SERVIDOR WWW.	43
FIGURA 21 - LISTA DE ARQUIVOS DO SERVIDOR WWW.	43
FIGURA 22 - LISTA DE DIRETÓRIOS DO SERVIDOR WWW.	44
FIGURA 23 - CONFIRMAÇÃO DA REMOÇÃO DE ARQUIVOS.	44
FIGURA 24 - ATIVIDADES DISPONÍVEIS PARA CORREIO ELETRÔNICO.	44
FIGURA 25 - ATIVAR OU DESATIVAR O ROTEADOR DE MENSAGENS ELETRÔNICAS.	45
FIGURA 26 - ATIVAR OU DESATIVAR SERVIDOR DE MENSAGENS ELETRÔNICAS.	46
FIGURA 27 - CONFIGURANDO GRUPOS E USUÁRIOS.	48

FIGURA 28 - ADICIONANDO USUÁRIO A GRUPOS.	48
FIGURA 29 - LISTA DE USUÁRIOS A SEREM REMOVIDOS DE LISTAS.	49
FIGURA 30 - CONFIRMAÇÃO DOS USUÁRIOS A SEREM REMOVIDOS DAS LISTAS.	50
FIGURA 31 - LISTAGEM DOS USUÁRIOS DE CADA LISTA.	51
FIGURA 32 - CRIANDO GRUPO DE USUÁRIOS.	52
FIGURA 33 - LISTAGEM DOS GRUPOS PARA SEREM REMOVIDOS.	53
FIGURA 34 - CONFIRMAÇÃO DOS GRUPOS A SEREM REMOVIDOS.	53
FIGURA 35 - LISTAGEM DOS GRUPOS EXISTENTES.	54
FIGURA 36 - GERENCIANDO O SERVIDOR DE ARQUIVOS.	56
FIGURA 37 - ALTERANDO MENSAGEM ATIVA DO SERVIDOR DE ARQUIVOS.	57
FIGURA 38 - MENSAGEM PADRÃO DO SERVIDOR DE ARQUIVOS.	59
FIGURA 39 - MENSAGEM DE ENTRADA OBTIDA PELO CLIENTE FTP.	60
FIGURA 40 - CONFIGURANDO NÚMERO DE CLIENTES DO SERVIDOR DE ARQUIVOS.	61
FIGURA 41 - CONFIGURANDO TIPO DE SENHA DE ACESSO AO SERVIDOR DE ARQUIVOS.	62
FIGURA 42 - DESLIGAR O SERVIDOR DE ARQUIVOS.	63
FIGURA 43 - LIGAR O SERVIDOR DE ARQUIVOS.	64
FIGURA 44 - CONEXÕES ESTABELECIDAS NO SERVIDOR DE ARQUIVOS.	66
FIGURA 45 - ENVIAR ARQUIVO PARA O SERVIDOR DE ARQUIVOS.	67
FIGURA 46 - SELECIONANDO TIPO DE REMOÇÃO DO SERVIDOR DE ARQUIVOS.	68
FIGURA 47 - REMOVENDO DIRETÓRIOS INTEIROS DO SERVIDOR DE ARQUIVOS.	68
FIGURA 48 - AÇÕES DO SERVIDOR DE NOMES.	69
FIGURA 49 - INFORMAÇÕES SOBRE O SERVIDOR DE NOMES PRIMÁRIO.	71
FIGURA 50 - LIGAR OU DESLIGAR O SERVIDOR DE NOMES.	72
FIGURA 51 - ADICIONANDO MÁQUINAS NO SERVIDOR DE NOMES.	73
FIGURA 52 - AVISO DE ERRO NO IP.	74
FIGURA 53 - LISTAGEM DOS DADOS DO SERVIDOR DE NOMES.	75
FIGURA 54 - LISTAGEM DOS NÚMEROS IPS A SEREM REMOVIDOS.	76
FIGURA 55 - CONFIRMAÇÃO DA REMOÇÃO NO SERVIDOR DE NOMES.	76

FIGURA 56 - STATUS DA REMOÇÃO NO SERVIDOR DE NOMES.	77
FIGURA 57 - CONFIGURAÇÃO DAS LINHAS SERIAIS.	78
FIGURA 58 - STATUS DA CONEXÃO DAS LINHAS SERIAIS.	79
FIGURA 59 - SELECIONANDO A LINHA SERIAL.	81
FIGURA 60 - ESPECIFICANDO TIPO DE LINHA TELEFÔNICA.	82
FIGURA 61 - CONFIGURANDO LINHA PARA TIPO DISCADA.	82
FIGURA 62 - CONFIGURANDO LINHA PARA TIPO DEDICADA.	84
FIGURA 63 - LINHA SERIAL CONFIGURADA COM SUCESSO.	85
FIGURA 64 - INFORMANDO O SERVIDOR DE AUTENTICAÇÃO.	86
FIGURA 65 - CONFIGURAÇÃO ATIVA DAS LINHAS SERIAIS.	87
FIGURA 66 - AÇÕES DISPONÍVEIS PARA GERENCIAMENTO DE ROTAS.	88
FIGURA 67 - LISTAGEM DA TABELA DE ROTEAMENTO.	89
FIGURA 68 - ADICIONANDO ROTA ESTÁTICA.	91
FIGURA 69 - LISTAGEM DAS ROTAS ATIVAS PARA REMOÇÃO.	92
FIGURA 70 - TESTAR ROTA.	94
FIGURA 71 - SAÍDA DE TESTE DE ROTA.	95
FIGURA 72 - MANUTENÇÃO DE CONTAS DE USUÁRIOS.	96
FIGURA 73 - CADASTRANDO NOVO USUÁRIO.	98
FIGURA 74 - ERROS NA SENHA DO USUÁRIO.	99
FIGURA 75 - USUÁRIO ADICIONADO COM SUCESSO.	101
FIGURA 76 - ALTERANDO INFORMAÇÕES E SENHA DE USUÁRIO.	102
FIGURA 77 - REMOVENDO USUÁRIO.	104
FIGURA 78 - ALTERAÇÃO DA SENHA DE ACESSO AO GERENCIAMENTO NÍVEL 1.	105
FIGURA 79 - MENU PARA DESLIGAR OU REINICIALIZAR A MÁQUINA.	107
FIGURA 80 - MENSAGEM DE AVISO SOBRE A REINICIALIZAÇÃO DA MÁQUINA.	108
FIGURA 81 - MENSAGEM DE AVISO SOBRE A DESLIGAMENTO DA MÁQUINA.	109
FIGURA 82 - SINGULARES DA UNIMED EM SANTA CATARINA.	110
FIGURA 83 - ESTABELECEENDO CONEXÃO REMOTA VIA MODEM.	111
FIGURA 84 - CONEXÃO REMOTA VIA MODEM ESTABELEECIDA.	112

FIGURA 85 – PÁGINA PRINCIPAL DO GERENCIAMENTO NÍVEL 2	113
FIGURA 86 - ALTERANDO SENHA DO GERENCIAMENTO NÍVEL 2	114
FIGURA 87 - PARÂMETROS DA MÁQUINA REMOTA PARA BACKUP.	115
FIGURA 88 - AVISO SOBRE TEMPO DE DURAÇÃO DO <i>BACKUP</i> .	116
FIGURA 89 - MÁQUINA REMOTA NÃO RESPONDE.	117
FIGURA 90 - NOME OU SENHA NA MÁQUINA REMOTA ESTÃO INCORRETOS.	117
FIGURA 91 - PROCESSO DE BACKUP TERMINADO COM SUCESSO.	117
FIGURA 92 - AVISO SOBRE A DURAÇÃO DO PROCESSO DE <i>BACKUP</i> .	118
FIGURA 93 - AVISO DE TÉRMINO DO PROCESSO DE <i>BACKUP</i> .	119
FIGURA 94 - PROCESSO DE RESTAURAÇÃO DO <i>BACKUP</i> FINALIZADO COM SUCESSO.	119
FIGURA 95 - CONFIGURAÇÃO ATIVA DA REDE.	120
FIGURA 96 - ALTERANDO CONFIGURAÇÃO DE REDE.	121
FIGURA 97 - NÚMERO IP DIGITADO INCORRETO.	122
FIGURA 98 - REDE CONFIGURADA COM SUCESSO.	123
FIGURA 99 - TESTANDO CONECTIVIDADE VIA <i>PING</i> .	124
FIGURA 100 - RESULTADO DO <i>PING</i> .	125
FIGURA 101 - NÃO FOI POSSÍVEL RESOLVER O NOME DA MÁQUINA.	125
FIGURA 102 - ESPECIFICANDO MÁQUINA PARA EXECUTAR <i>TRACEROUTE</i> .	126
FIGURA 103 - RESULTADO DO COMANDO <i>TRACEROUTE</i> .	127
FIGURA 104 - NOME DE MÁQUINA INVÁLIDO.	127
FIGURA 105 – INTERLIGAÇÃO DA SINGULARES À FEDERAÇÃO	133

1. Princípios de Gerenciamento Remoto de Redes

1.1 Contexto Histórico: Unix e Internet

Em 1956 o *Bell Labs*, a *General Electric Company* e o *Project MAC* do MIT agruparam esforços para criar um novo sistema operacional. Um dos alvos do sistema seria a capacidade de prover conexões simultâneas dos computadores de uma grande comunidade de usuários, gerenciar altas cargas computacionais e permitir o compartilhamento de recursos entre usuários. Esse sistema recebeu o nome de MULTICS. Entretanto os resultados obtidos não foram satisfatórios e o projeto foi cancelado. Para melhorar o ambiente de programação no *Computing Science Research Center* nos *Bell Laboratories*, *Ken Thomson*, *Dennis Ritchie* e outros definiram um novo sistema operacional. De suas idéias foi criado a primeira versão do UNIX, um trocadilho com o nome Multics. O novo sistema operacional foi primeiramente codificado para um computador GE645, passando para um PDP-7 e posteriormente para um PDP-11, em 1971. Em 1973 o sistema foi rescrito na linguagem C e em 1977, Thomson e Ritchie publicaram um artigo descrevendo o sistema UNIX. Isto levou a um crescimento do número de computadores com o novo sistema. Numerosas licenças foram fornecidas, tanto para fins comerciais como para universidades. O UNIX teve um grande impacto na comunidade de teleprocessamento, acabando por se tornar o sistema preferido das companhias telefônicas. Surgiu uma gama de sistemas operacionais UNIX, com pequenas diferenças entre si. Entre 1977 e 1983 surgem as mais fortes vertentes do UNIX, o System V da AT&T e o 4.3 BSD, da Universidade da Califórnia em Berkeley. Vários são os motivos que levaram à aceitação do UNIX na época:

o sistema é escrito em linguagem de alto nível o que facilita a manutenção do código bem como a codificação para outros computadores;

uma interface com o usuário simples e eficaz (lembremo-nos que a utilização de interfaces gráficas ainda estava em fase de desenvolvimento às escondidas nos laboratórios da Xerox em Palo Alto);

uma coleção de primitivas que permitem a criação de programas complexos à partir de outros mais simples;

o sistema é multiusuários e multiprogramado;

esconde do usuário a arquitetura da máquina;

provê uma interface simples e consistente para aparelhos periféricos.

Paralelamente ao desenvolvimento desse sistema, a ARPA (*Advanced Research Projects Agency*) encorajou pesquisadores universitários a utilizarem os novos protocolos TCP/IP. Financiou a integração dos protocolos ao UNIX na BBN (*Bolt Beranek e Newman, Inc.*) e na Universidade de Berkeley. Um segundo motivo é que novos computadores estavam sendo adquiridos pelas universidades surgindo a necessidade de conectá-los em rede. A distribuição de Berkeley passou a oferecer um conjunto de serviços de rede que se assemelhava com os serviços do UNIX. Essa similaridade como o UNIX foi fundamental para a disseminação do protocolo TCP/IP. A junção das qualidades do UNIX aliado às qualidades do TCP/IP transformaram o UNIX em sinônimo de sistema operacional para redes de computadores. Tanto a Internet quanto o UNIX foram desenvolvidas em grande parte dentro das universidades, criando uma cultura de rede. Nessa época, além das universidades, apenas grandes empresas eram capazes de manter os caros equipamentos necessários para se ter UNIX e uma rede de computadores. A

maturação do UNIX foi um passo importante para o desenvolvimento das redes. Outras tecnologias como meio de conexão e placas de rede precisaram ser desenvolvidas para uma popularização das redes de computadores.

Cada elemento de uma rede está conectado em rede através de algum meio físico. Até recentemente o protocolo Ethernet era a tecnologia mais empregada em todo mundo, embora atualmente existam outras opções como o SONET, ATM, *Fast Ethernet*, *Gigabit Ethernet* e o *Frame Relay*. A tecnologia Ethernet foi desenvolvida pela *Xerox PARC* na década de 70. A Xerox aliada à Intel Corporation e à Digital Equipment Corporation criaram o padrão em 1978, que sofreu algumas alterações por parte do IEEE, recebendo o número de 802.3. No início utilizou-se o cabo coaxial grosso. Atualmente há diversas formas para transmissão de dados sendo o par trançado (ou *Twisted Pair Ethernet*) o mais comum. Tecnologias como fibra ótica e *wireless* tem se popularizado devido a constante queda no preço. Para que cada elemento de uma rede troque informações entre si é necessário que haja uma interface de rede. Para cada tipo de protocolo há uma interface de rede diferente.

Interfaces de rede *Ethernet* com problemas geralmente criam um aumento do tráfego, porque utilizam o mecanismo de máximo esforço (*best-effort delivery*). Este mecanismo é utilizado porque o hardware não informa se a transferência foi ou não bem sucedida, ficando a cargo das camadas superiores do protocolo TCP/IP gerenciar o recebimento das informações. Se a placa não é capaz de capturar as informações destinadas a máquina, as camadas superiores continuarão a reenviar a informação. Para este exemplo deve-se considerar que uma falha no funcionamento do software também leva a um aumento no tráfego. Cada placa está continuamente testando o meio físico e só tenta transmitir quando nenhuma outra o está. Este modelo é

conhecido por *Carrier Sense Multiple Access/Collision Detect* (CSMA/CD). É uma estratégia de acesso múltiplo porque todas as máquinas tem acesso à rede simultaneamente e cada uma determina se pode ou não iniciar a transmissão quando o meio não conter uma onda portadora. Um tempo mínimo é esperado antes que a máquina comece a transmitir. Ao começar a transmitir, o sinal não atinge instantaneamente toda a extensão do cabo, podendo acontecer que duas máquinas iniciem a transmissão simultaneamente embaralhando os sinais. Esses incidentes são conhecidos por colisões. Durante a transmissão cada placa monitora o cabo para detectar interferência. Caso haja colisão, ambas as placas devem parar a transmissão e esperar um intervalo aleatório antes de reiniciarem. Caso uma segunda colisão seja detectada, espera-se o dobro; se uma nova colisão ocorre, espera-se quatro vezes mais e assim se vai dobrando sucessivamente à cada nova seguida colisão. Se a placa não é capaz de detectar se outra já está transmitindo, de detectar uma colisão ou de gerar tempos aleatórios corretamente, haverá um aumento no número de colisões e conseqüentemente degradação na qualidade das transmissões.

As redes de computadores podem cobrir pequenas ou grandes dimensões, variando de redes corporativas cobrindo todo um país até pequenas redes em uma sala (LAN, ou *Local Area Network*). As redes de grandes distâncias ficaram conhecidas por WAN (*Wide Area Network*). A tecnologia empregada em WAN não limita a distância, podendo conectar através do continente ou do oceano. Entretanto a velocidade de operação é muito menor que a das LANs e possuem um tempo de retardo grande. A tecnologia utilizada em LAN tem as mais altas velocidades. Como cobrem pequenas área, possui um baixo tempo de latência. Surgiu recentemente outro termo, MAN,

para designar uma rede que compreende uma cidade com as características de uma LAN.

Duas ou mais redes podem ser interligadas criando uma conexão inter redes. Um conceito básico para o funcionamento de uma inter rede é o de roteamento. O roteamento é o mecanismo responsável pela interconexão entre duas redes. Um roteador pode estar conectado à duas ou mais redes físicas sendo capaz de passar pacotes entre elas. Todo o tráfego da rede que não é destinado à alguma máquina à ela conectada é enviado ao roteador que por sua vez se encarrega de enviá-lo à outro roteador. O pacote é sucessivamente enviado para roteadores até atingir aquele cuja uma de suas interfaces esteja conectada à rede da máquina destino. O roteador provê a arquitetura básica da Internet e manipula todo o tráfego usando uma tabela de roteamento. A tabela de roteamento é composta por informações de endereços de rede e qual o endereço do próximo roteador.

A tabela deve ser de alguma forma inicializada, o que depende de cada sistema, e ser atualizada, manual ou automaticamente. Durante o processo de atualização automática pode ocorrer de rotas serem removidas, devido à uma falha na interface por exemplo. Os roteadores também são capazes de trocarem informações de rota entre si usando o *Exterior Gateway Protocol* (EGP).

1.2 Necessidades no Gerenciamento de Intranet à Distância

1.2.1 Tipos de Problemas

Diversos fatores levam uma rede de computadores a trabalhar de forma insatisfatória ou causado erros que degradam a qualidade da comunicação, indo desde o equipamento à configuração dos aplicativos.

Estando cada equipamento ligado corretamente à rede, o seu não funcionamento correto prejudica os demais, podendo propagar seus efeitos para outras redes. O roteador que tem cada uma de suas interfaces conectadas em uma rede física, pode começar a gerar tráfego desnecessário ou aumentar o número de colisões. O processo de atualização da tabela remove a rota para aquela rede e passa então a divulgar a nova informação para os demais roteadores. A perda de algumas rotas, por exemplo, num roteador que une quatro subredes, obriga o operador a adicioná-las novamente manualmente. Em cabeamentos com par trançado, um estiramento do cabo pode alterar o valor da resistência aumentando o nível de colisões

.Em uma rede que cresce continuamente, a configuração de novas máquinas requer a adição do nome no serviço de DNS. O serviço de DNS é responsável por prover a correta associação do nome ao número IP. Diversos serviços dependem da correta configuração do servidor de DNS para trabalharem corretamente. Uma falha na configuração pode comprometer o funcionamento de inúmeros serviços.

1.2.1.1 Pós evento

Um recurso útil de qualquer equipamento é a capacidade de armazenar um histórico de suas atividades conhecido como arquivo de log. Cada comando executado tem suas tarefas armazenadas até que seja finalizado. Por exemplo, um servidor DNS ao receber um pedido de resolução de nome executa diversos procedimentos:

- i. Determina se é autoridade sobre o nome.
- ii. Se for, executa uma busca em suas tabelas para encontrar o número IP associado.
- iii. Se não for e se recursividade estiver disponível, inicia uma busca a partir dos servidores raiz, até localizar o servidor de DNS responsável pelo domínio.

Cada uma destas etapas gera mensagens que podem ser armazenadas e a quantidade de informações sobre o processo pode ser controlada no início da execução do servidor de DNS.

Os aplicativos de controle de equipamento enviam cada comando para o arquivo de log ou para a aplicação do sistema responsável por armazenar os logs. Em alguns casos não é possível especificar uma granularidade maior no armazenamento dos logs. Informações maiores sobre o status do equipamento são obtidas com a execução de programas específicos, por exemplo, *swapinfo*, *w*, *uptime* ou *iostat* em máquinas com sistemas operacional UNIX.

Essa estratégia maximiza a possibilidade de resgate de ocorrência de erros uma vez que nem todos fazem com que a aplicação se encerre ou o equipamento pare de funcionar. Sendo a aplicação finalizada ou o equipamento parado, as últimas linhas do arquivo de monitoramento são fortes candidatas a indicar as causas da falha. Nesse caso o funcionamento continua, sendo possível o conhecimento do problema indiretamente. Política de rotinas de inspeção de log são adotadas em todos os sistemas UNIX e que podem ser reescaloadas ou refinadas. No sistema UNIX há um gerenciador geral de mensagens de log para aplicativos que por algum motivo não geram seus próprios arquivos. Este gerenciador geral é um típico programa que é executado durante a inicialização da máquina e permanece em execução indefinidamente. São conhecidos por daemons. O daemon de log é chamado de *syslogd*, uma abreviação de *system logger daemon*.

1.2.1.2 Durante o Evento

Uma rede de computadores é um sistema não homogêneo de equipamentos. O hub é um elemento na qual se liga as interfaces de redes através de cabos UTP. Repetidores

por sua vez são equipamentos que reforçam os sinais transmitidos pelos cabos UTP e geralmente servem para interligar hubs distantes. A distância máxima permitida pela categoria UTP é de cem metros. Em hubs e repetidores cada colisão ocorrida aciona um led no painel. Sucessivas colisões acabam por causar um acendimento contínuo. Os aplicativos do equipamento ao detectar sucessivas colisões passa a gerar mensagens de alerta que são enviadas para o console da máquina ou armazenadas nos arquivos de log. Estas mensagens podem ser interceptadas por uma aplicação que se encarrega de acionar os outros mecanismos de alerta secundários. Por exemplo, um sinal sonoro da máquina, o envio de uma mensagem eletrônica ou simplesmente uma mensagem de aviso em algum painel remoto.

1.2.1.3 Detectando o Problema

Para certos tipos de falha o equipamento ou aplicação não consegue identificar a causa. As mensagens obtidas nesses casos alertam apenas sobre as conseqüências e possíveis causas. É necessário um exame mais detalhado das mensagens reportadas que requerem a intervenção do gerente. Sistemas de Inteligência Artificial vêm, há anos, tentando desenvolver técnicas para detecção autônoma de erros, mas os resultados ainda são insatisfatórios para muitos casos.

Uma configuração incorreta das aplicações ou equipamento pode gerar falhas difíceis de identificar. Sintaxes complexas como do roteador de mensagens eletrônicas, *sendmail*, tornam comum o aparecimento de falhas. A vantagem é que uma vez corrigido o problema, somente uma alteração na rede, causará falhas. Salvo as danificações causadas por terceiros ou raros, mas não impossíveis, erros latentes que ocorrem somente sob certas circunstâncias. Este último é extremamente difícil de identificar exigindo conhecimento e experiência.

1.2.1.4 Técnicas de Diagnóstico

Durante o seu funcionamento, o equipamento fornece informações sobre suas atividades e estado. Estas informações são coletadas por aplicativos especializados próprios do equipamento e armazenados em arquivos. Toda ação ou somente as especificadas são armazenadas permitindo determinar as ações tomadas pelo equipamento e seu status em determinado tempo. Na maioria dos aplicativos é possível selecionar o nível da granularidade do relatório, induzir a ocorrência do erro e novamente analisar os arquivos de log. A possibilidade de erros decorrentes de uma incorreta configuração de aplicativos pode então ser detectada e corrigida se necessário.

Problemas decorrentes de mau funcionamento do equipamento exigem uma inspeção no equipamento e execução dos diagnósticos. Problemas com o cabo de alimentação respondem por muitas falhas. Testes de funções específicas do equipamento permitem a inspeção de possíveis falhas de funcionamento.

1.2.1.5 Agilidade

Sistemas resistentes à falhas são complexo e caros. As redes geralmente são projetos com baixa imunidade às falhas. Essas podem surgir de muitas formas. Uma rede de computadores atende a usuários com os variados níveis de conhecimento técnico. Inúmeros trabalhadores estão diretamente dependentes do correto funcionamento. Há servidores que armazenam aplicativos e gerenciam grandes bancos de dados. Impressoras podem ser compartilhadas. Existe uma gama muito grande de serviços disponíveis com a rede que são utilizados em operações rotineiras. Devido à esta alta dependência da rede, qualquer problema deve ser detectado de imediato. Inspeções rotineiras nas atividades da rede, em aplicativos e equipamento, devem ser realizadas

segundo uma política criteriosa que inclua manutenção preventiva. Dessa forma, tão logo uma falha ocorra, inicia-se os procedimentos para a correção.

1.2.2 Gerência

A responsabilidade pela manutenção da rede é do profissional denominado gerente ou analista de rede. O crescimento de uma rede local torna o seu monitoramento visual difícil. Diversos clientes de rede podem estar geograficamente espalhados. O correto funcionamento da rede depende de aplicativos e da conexão física dos elementos de rede. Para garantir o funcionamento ou averiguar os equipamentos pode ser necessário se deslocar até o equipamento. Esse tempo gasto para o deslocamento é um tempo perdido. É necessário manter uma completa e atualizada documentação sobre a localização física dos equipamentos o que pode ser difícil devido a dinâmica das atuais redes. A criação de mapas de rede pode ser feito com aplicativos específicos tipo CAD ou Visio. Esses aplicativos impõem que o gerente crie os mapas manualmente. Mas uma tecnologia que utiliza agentes circulantes pela rede, mapea cada equipamento encontrado. Ao final, o mapa dos elementos de rede encontrado que necessita de algumas poucas alterações. Ambos permitem fazer o desenho da topologia da rede, situar os diversos equipamentos contendo uma breve descrição.

Existe diversos tipos de equipamentos ligados à rede e que não estão diretamente relacionados com o funcionamento. São os hubs, switches, roteadores, bridges, etc. Cada um tem particularidades e características próprias. Por exemplo, entre dois hubs de marcas diferentes. A diferença está não apenas no projeto. Embora executem a mesma tarefa, suas características podem ser bastante distintas. As características de cada equipamento são descritas em seus respectivos manuais que devem permanecer

acessíveis. A criação de uma biblioteca com todos os manuais e documentações impressas agiliza a procura por informações.

Existe ainda o lado pessoal na gerência do sistema. Nem todos os usuários têm conhecimento sobre computação, mas conseguem influenciar na rede. Seja interrompendo um cabo coaxial de rede, configurando errado uma placa de rede ou até mesmo atribuindo um número IP errado à sua máquina. Ter uma boa interação com o usuário final no sentido de esclarecer e solucionar dúvidas, informar mudanças e alterações na rede é fundamental. Mais do que um bom relacionamento pessoal é necessário uma política de atuação e procedimentos.

1.3 Ferramentas Atuais de Gerenciamento de Intranet à Distância

As intraredes têm se tornado maiores e principalmente mais complexas. Com este aumento:

1. aumenta a dependência dos recursos oferecidos pela rede.
2. mais coisas podem dar errado, interrompendo o funcionamento parcial ou total da rede, ou degradando seu funcionamento.

Uma rede grande não pode ser deixada à cargo apenas da equipe de gerenciamento. São necessárias ferramentas-autômato para gerenciamento. Grandes redes tendem a possuir equipamentos de fabricantes diversos. Os softwares de gerenciamento dos equipamentos são específicos de cada fabricante. Cada pedaço da rede é gerenciado por uma ferramenta e não há troca de informações entre elas. Essa troca de informações é fundamental para a obtenção de um status uniforme do que está acontecendo com a rede. Em resposta à essa necessidade foi desenvolvido um padrão para gerenciamento de redes. Entre todos, o que se tornou mais comum foi o *Simple Network Management Protocol*, SNMP. O SNMP foi desenvolvido pelo IETF em

1987. Desde a sua criação tem aumentado o número de redes que usam SNMP bem como a sua complexidade.

1.3.1 SNMP

O SNMP foi desenvolvido para ser um protocolo de gerenciamento de rede de propósitos gerais. A arquitetura do SNMP identifica uma coleção de estações de gerenciamento de redes (*network management station*) e uma coleção de elementos de rede. As estações de gerenciamento são equipamentos onde as aplicações que monitoram e controlam os elementos de rede são continuamente executadas. As estações de gerenciamento são *stand-alone*, mas podem ser implementadas em um sistema multiprogramado. Os elementos de rede são equipamentos como computadores, gateways, switches, etc. que possuam agentes de gerenciamento responsáveis por atender aos pedidos de funções feitas pelas estações de gerenciamento. O SNMP é usado para trafegar as informações entre as estações de gerenciamento e os agentes nos elementos de rede.

Uma estação de gerenciamento deve ter no mínimo:

- um conjunto de ferramentas para análise de dados, recuperação de falhas, etc.

- uma interface através da qual o gerente de sistema monitora e controla a rede.

- a capacidade de atender as requisições do gerente de sistemas em funções de monitoração e controle à serem enviadas aos agentes.

- um banco de informações extraídas das MIBs de todas as entidades gerenciadas da rede.

Dentre as quatro, apenas as duas últimas fazem parte do padrão SNMP.

Outro elemento ativo do sistema de gerenciamento remoto é o agente de gerenciamento (*management agent*) que equipam os diversos elementos de rede. Os

agentes de gerenciamento respondem às requisições e comandos feitas pelas estações de gerenciamento. Também são capazes de assincronamente enviar às estações de gerenciamento informações importantes que não tenham sido solicitadas.

Os recursos da rede são manipulados como objetos que são essencialmente um valor atribuído a uma dada variável. A coleção de objetos é chamada de MIB, ou *management information base*. Esta coleção de objetos é padronizada entre os sistemas para cada classe particular, por exemplo, todos os switches suportam os mesmos objetos. O monitoramento é realizado requisitando o valor de determinado objeto, assim como a alteração do valor de um objeto pela estação de gerenciamento em um agente causa a execução de uma ação no elemento de rede. A alteração também pode causar uma reconfiguração no elemento de rede.

O protocolo SNMP possui as seguintes capacidades:

get: habilita a estação de gerenciamento à obter o valor de algum objeto do agente.

set: habilita a estação de gerenciamento à alterar o valor de algum objeto no agente.

trap: possibilita o agente à informar a estação de gerenciamento sobre algum evento importante.

1.3.1.1 Vantagens e Desvantagens do SNMP

A simplicidade do SNMP lhe confere as seguintes vantagens:

robustez frente à falha da rede;

baixo *overhead* nos equipamentos.

facilidade de depuração do próprio protocolo.

Desta forma o SNMP é limitado a usar o *User Datagram Protocol* (UDP) deixando à cargo do implementador a responsabilidade por gerenciar pacotes perdidos e a retransmissão quando necessário. Outro fato à ser considerado é que sendo executado continuamente é preciso que se consuma a menor largura de banda possível da rede. Diversas complexidades na implementação do SNMP utilizando UDP levaram a sua implementação sobre o TCP. Há vários benefícios de se usar SNMP sobre TCP os quais podemos citar as modernas implementações do TCP que podem maximizar os custos da largura de banda e já estão depurados o suficiente para fornecer uma conexão confiável.

1.3.2 MIB e MIBII

Os equipamentos de rede que suportam o protocolo SNMP mantém um conjunto de MIB de estatísticas da rede. As MIBs especificam quais objetos podem ser lidos e quais podem ter seus valores alterados pela estação de gerenciamento.

A MIB II é o padrão para o TCP/IP MIB e divide o gerenciamento de informações em oito categorias. Cada item é identificado usando o código da categoria (Tabela 1).

Categoria	Informações Sobre
System	sistema operacional do elemento de rede
Interfaces	interfaces individuais de rede
add.trans.	tradução de endereço (por exemplo, ARP)
Ip	aplicativo de Internet Protocol
Icmp	aplicativo de Internet Control Message Protocol
Tcp	aplicativo de Transmission Control Protocol
Udp	aplicativo de User Datagram Protocol
Egp	aplicativo de Exterior Gateway Protocol

Tabela 1 - Categorias dos objetos.

Os valores dos objetos são armazenados como variáveis inteiras, mas estruturas complexas podem ser definidas. Um exemplo são os valores para uma tabela de roteamento.

Um padrão separado define a criação dos objetos das MIB. As regras são conhecidas por *Structure of Management Information* (SMI). O SMI especifica que todos os objetos MIB devem ser definidos e referenciados usando a *Abstract Syntax Notation 1* (ASN.1) da ISO. A ASN.1 é uma linguagem formal que especifica como representar os valores e nomes dos objetos eliminando qualquer ambigüidade. É usado um espaço de nomes hierárquico para garantir que todos os objetos MIB sejam globalmente únicos, mas ainda permitindo que subgrupos criem nomes para partes do espaço de nomes. Esta hierarquia é similar ao serviço de DNS.

1.3.3 RMON

O *Remote Networking Monitoring Management Information Base* (RMON MIB), provê ao SNMP um padrão para o monitoramento do fluxo através da rede. O RMON especifica como a monitoração remota coleta e armazena dados relativos ao tráfego da rede. Estas informações são então enviadas para uma ou mais estação de gerenciamento centralizadora de SNMP para análise e conseqüente ação. A principal contribuição do RMON é que permitir monitores remotos de diferentes marcas trabalharem com as mesmas estações de gerenciamento. Esta habilidade para interoperabilidade é essencial para qualquer esforço despendido na criação de sistemas de gerenciamento distribuído para LANs e inter redes.

1.3.3.1 Grupos do RMON

As requisições aos objetos RMON MIB para obter as informações sobre a rede são divididas em nove grupos: estatística de tráfego, histórico, alarmes, estatísticas do equipamento, lista “*host top N*”, dados matriciais, filtros de pacotes, pacotes capturados, e eventos.

1. O grupo de estatística de tráfego abrange os dados medidos por agentes remotos no segmento de rede. Os agentes remotos somente são capazes de monitorar segmentos de rede ao qual estão diretamente conectados. É medida a qualidade da rede permitindo ao gerente do sistema detectar problemas assim que ocorram. Informações típicas fornecidas são CRCs e colisões.
2. O grupo de histórico mantém informações descritivas da rede num dado tempo. Estas informações são requisitadas pelo grupo de estatística de tráfego e armazenadas para futuras requisições e análises das estações de gerenciamento.
3. O grupo de alarme permite que seja configurado parâmetros mínimos para a qualidade da rede. Quando estes valores são ultrapassados é enviado uma informação de alerta.
4. O grupo de estatística do equipamento é responsável por detectar todas as interfaces da rede e manter uma lista dos endereços MAC. Os endereços MAC são obtidos a partir dos pacotes corretamente enviados ou recebidos.
5. O grupo “*host top N*” contém uma lista ordenada dos equipamentos segundo uma dada classificação. Por exemplo, a lista dos 12 equipamentos cuja interface gerou maior tráfego no segmento de rede. Os parâmetros e as tabelas “*host top N*” são controladas pelas estações de gerenciamento.
6. O grupo matricial contém informações sobre as comunicações no nível de MAC entre um conjunto de endereços. Isto permite ao gerente do sistema saber quais equipamentos estão comunicando com quais interfaces.
7. O grupo de filtros permite gerar informações sobre determinados pacotes. Por exemplo determinar qual o impacto que novos serviços de vídeo clips do servidor WWW está causando no tráfego da rede.

8. O grupo de captura prevê um buffer para capturar pacotes e um mecanismo de detecção que ativa automaticamente a detecção do caminho percorrido.
9. O grupo de eventos é uma tabela com dados gerados por todos os eventos dos agentes RMON. Controla a geração e notificação dos eventos da estação remota à estação de gerenciamento. Quando determinado evento ocorre é gerado uma notificação que é enviada à estação de gerenciamento.

1.3.4 Desafios

Para gerenciamento de redes há soluções novas à vista. Usuários de corporações estão adotando os padrões Web como navegadores e JAVA para gerenciar seus servidores e clientes de rede mais fácil e eficientemente. Diversas grandes corporações tem desenvolvido interfaces em navegadores para o gerenciamento de aplicações, dando ao gerenciamento de redes uma janela que possibilita visualizar a qualidade da rede. E mais, para qualquer cliente e em qualquer lugar, obviamente seguindo restrições impostas de acesso.

Os recursos atuais de Web permitem que as páginas sejam criadas no momento que são requisitadas as informações pertinentes sobre determinado contexto. Ou ainda que sejam mantidas no servidor enquanto suas informações são atuais e qualquer modificação causa a geração de uma nova página. Desta forma temos um panorama relativamente próximo do obtido quando utilizando uma estação de gerenciamento

Um consórcio de empresas propôs APIs, modelo de objetos e protocolos que prometem englobar todos os aspectos das aplicações e equipamentos das WANs, LANs, intra redes e servidores Internet. Diversos padrões para o gerenciamento estão sendo desenvolvidos. O JMAPS, ou *Java Management APIs* proposto pela *Sun Microsystems Inc.* foi adotado por vários fabricantes de equipamento. O modelo

JMAPI permite que aplicações baseadas em JAVA comuniquem as informações pela rede via método de requisição remota. Obviamente ambos os lados devem ter compatibilidade com JAVA. Um consórcio entre *BMC Software Inc.*, *Cisco Compaq Computer Corp*, *Intel Corp.* e *Microsoft Corp.* propôs um modelo de objeto e protocolo denominado WBEM, ou *Web-Based Enterprise Management*.

A *Cabletron System* foi uma das pioneiras nessa tecnologia desenvolvendo o *Cabletron's Spectrum*. *Cabletron's Spectrum* foi desenvolvido e primeiramente instalado em uma firma de corretagem com sede em St. Louis e em 3.400 filiais espalhadas pelo USA e Canadá.

As vantagens mais proeminentes são:

Os gerentes de rede não necessitam ter um terminal de X-Window ou estação de trabalho Unix para gerenciar a rede.

Um PC ou Macintosh equipado com navegador custa bem menos que uma estação de trabalho.

Uma interface gráfica familiar com o qual os gerenciadores estão acostumados a usar.

A interoperabilidade é melhorada pois a partir de um navegador o gerenciador consegue ter acesso a equipamentos de diferentes fabricantes.

Com o uso do navegador e de Java torna o trabalho do gerenciamento de redes e as aplicações muito mais fáceis de serem manuseadas e portanto mais eficientes.

2. Softwares de Gerenciamento

A versatilidade provida pela poderosa linha de comando do Unix é a grande aliada de administradores de sistemas experientes. Entretanto, essa versatilidade torna-se danosa para usuários pouco acostumados com o ambiente de gerenciamento de uma máquina com Unix. Há algumas formas para se contornar ou minimizar tais problemas:

- Diminuir as opções dos comandos.

- Criar novos comandos a partir de outros, por exemplo *reboot* é na verdade uma ligação simbólica para *shutdown -r now*.

- Criar uma GUI para a linha de comando.

Diminuir as opções dos comandos não é uma boa opção pois reduz a funcionalidade e versatilidade do próprio Unix. Funcionalidade e versatilidade essas adquiridas em anos de refinamentos do sistema. Criar novos comandos a partir de outros também não é uma boa solução pois implica em uma carga maior de aprendizado e memorização.

GUI para linha de comando por si só também não é uma boa opção pois:

- O usuário deixa de aprender os comandos realmente executados que são mascarados por menus, imagens ou botões.

- Aumenta a complexidade do comando se solicita ao usuário que faça uma escolha em todas as opções ou menus disponíveis.

- Reduz a versatilidade inerente do comando quando opções deixam de ser apresentadas. Essa solução pode induzir a erros pois o usuário passa a executar um mesmo comando para resolver problemas parecidos.

Aumenta o tempo de execução da tarefa quando se faz necessário passar por diversos menus até atingir a opção desejada que pode ser a última.

A Figura 1 mostra um exemplo de GUI do Unix da Digital. Para obter a configuração da placa de rede denominada *tu0* é necessário passar por 3 menus. Para um usuário experiente basta executar o comando *ifconfig tu0* para se obter as mesmas informações.

Figura 1 - Menu de configuração de rede da Digital Unix.

Outro exemplo de excesso de menus de uma interface de configuração um pouco mais antiga do OSF da Digital (Figura 2). Para se obter a mesma informação que a da Figura 1 deve-se passar diversos menus.

Figura 2 - Interface de configuração no OSF.

Uma das características intrínsecas do Unix é permitir ao super usuário **executar qualquer comando**. Inclusive comandos que por exemplo, removam arquivos necessários para o processo de *boot* ou até alterar a geometria do disco (Figura 3).

Figura 3 - Definindo partições no Digital Unix.

O Solaris, sistema operacional Unix da Sun, também agrupa as atividades rotineiras juntamente com complexas (Figura 4). Para adicionar usuário ao sistema, **feito** a partir da Figura 4, é apresentado um menu com várias opções a serem preenchidas e selecionadas (Figura 5). A maioria das opções são irrelevante. Também **não é informado** quais itens são mandatórios. Novamente, os mais experientes escolheriam uma linha de comando para executar a ação de adicionar usuário no sistema e, caso necessário, realizar alguma alteração posteriormente.

Figura 4 - Interface de administração do Solaris.

Admintool: Add User

USER IDENTITY

User Name:

User ID:

Primary Group:

Secondary Groups:

Comment:

Login Shell: /bin/sh

ACCOUNT SECURITY

Password:

Min Change: days

Max Change: days

Max Inactive: days

Expiration Date:

(dd/mm/yy)

Warning: days

HOME DIRECTORY

Create Home Dir: ☒

Path:

OK Apply Reset Cancel Help

Figura 5 - Adicionando usuário no Solaris.

O SCO, sistema operacional da empresa *The Santa Cruz Operation*, também agrupa comandos rotineiros com os mais complexos a partir de um menu (Figura 6). O SCO ainda utiliza menus de textos para a configuração de alguns recursos do sistema, como o servidor de correio eletrônico (Figura 7).

Figura 6 - Gerenciamento do SCO.

Figura 7 - Configurando correio eletrônico no SCO.

As GUIs empregadas pelos diversos sistemas normalmente são utilizadas para gerarem uma linha de comando. Os sistemas também permitem a criação de GUIs para comandos personalizados pelo usuário (Figura 8). O comando a ser executado é

especificado e atribuído a uma ação (*action name*). É também feita uma associação à um ícone. Portanto para a execução do comando basta selecionar o ícone.

Figura 8 - Criando GUI para comandos no Solaris.

Um inconveniente desse sistema é que a linha de comando gerada não é mostrada para o usuário. Assim, o usuário não fica sabendo qual comando foi executado e com quais opções. Se ocorrer um erro, a mensagem gerada não tem muita serventia. Veja o exemplo da Figura 9 onde tentou executar a ação *Backup Manager* sem sucesso. A mensagem de erro não ajuda, pois não foi possível saber qual comando foi executado ou com quais opções.

Figura 9 - Mensagem de erro gerada da ação *Backup Manager* do SCO.

A melhor forma de resolver esse problema é determinar qual o real uso para o sistema e disponibilizar os comandos mínimos necessários para um bom gerenciamento deste. As opções dos comandos devem ser reduzidas as necessárias, balanceando versatilidade com complexidade e serem mascaradas através de ações específicas.

3. Descrição do Software MSP

Durante essa seção iremos descrever o equipamento utilizado, sistema operacional, compiladores, linguagens de programação e a estrutura do projeto. Demos o nome de MSP ao conjunto de softwares e soluções.

3.1 Equipamento Utilizado

O MSP foi desenvolvido para cinco categorias de máquina. As máquinas são:

1. Portal B: composta dos servidores WWW, de arquivos e endereço eletrônico.
2. Portal A: contém o servidor de autenticação de acesso.
3. Portal R: contém o banco de modems.
4. Portal BAR: contém os servidores WWW, de arquivos, endereço eletrônico e autenticação de acesso e o banco de modems.
5. Portal BARF: contém os servidores WWW, de arquivos, endereço eletrônico e autenticação de acesso, banco de modems e um módulo que estabelece a conexão via linha discada com algum servidor de acesso. Essa máquina também contém um software de *firewall* proprietário da empresa Total Informática.

Cada máquina contém o sistema operacional FreeBSD rodando num Pentium 100MHz, 8 MB de memória RAM, placa de rede, unidade de disquete e disco de 2 GB. A empresa Total Informática desenvolveu uma versão do FreeBSD em português que foi utilizado em todas as máquinas comercializadas pela empresa. As alterações necessárias no MSP para se adequar ao sistema FreeBSD proprietário da empresa Total Informática são mínimas.

3.2 Características do Sistema

3.2.1 Apache

O servidor de HTTP Apache é originalmente baseado no código e idéias do servidor *httpd NCSA 1.3* de 1995. Tornou-se o mais popular dos servidores baseados em Unix devido a sua qualidade superior como funcionalidade, eficiência e velocidade. Atualmente, há versões para o sistema *Windows* da *Microsoft*. Os desenvolvedores do servidor Apache são voluntários e atualmente o desenvolvimento é coordenado pela *Apache HTTP Server Project*.

O servidor Apache utilizado é o Apache-SSL. O Apache-SSL é baseado no Apache e SSLeay que implementa as funcionalidades do *Secure Sockets Layer* (SSL - 3.2.5). O código fonte original do servidor Apache é alterado através de *patches* que adicionam as funcionalidades do SSL.

O servidor Apache pode ser tão seguro quanto se queira. Para tanto, deve-se seguir as instruções e sugestões sobre segurança fornecidas no *site* do projeto. Algumas vezes, entretanto, a segurança é restringida em favor da funcionalidade e comodidade de uso do desenvolvedor.

3.2.2 Navegadores

Navegador, ou *browser* é um programa cliente que se conecta a um servidor WWW utilizando o protocolo *HTTP* e é capaz de diagramar o conteúdo a partir do código *HTML* contido na página. Os navegadores mais comuns são Netscape Communicator e o Internet Explorer, da *Netscape Communications* e *Microsoft* respectivamente. O Netscape tem versões para os principais sistemas operacionais, enquanto o *Internet Explorer*, primeiramente apenas para o sistema operacional Windows. Recentemente

a *Microsoft* lançou o *Internet Explorer* para alguns sistemas operacionais UNIX. Outro navegador muito comum no início da WWW era o Mosaic, mas que aos poucos perdeu o espaço em popularidade para o Netscape. Existe muitos navegadores disponíveis, mas o que concentra o maior número de recursos é o Netscape. Há uma outra categoria de navegadores que apenas mostram o texto das páginas. Entre eles o mais conhecido é o *lynx*.

O software de gerenciamento foi desenvolvido utilizando como navegador o Netscape, entretanto evitou-se a utilização de recursos proprietário do Netscape. Um dos motivos para a escolha foi a capacidade de suportar conexões criptografadas utilizando o protocolo *HTTPS*.

3.2.3 HTML

HTML não é uma linguagem de programação, mas sim um sistema de formatação de documentos. A idéia é pegar um texto comum e ir adicionando etiquetas (*tags*) que são informações de como o navegador deve formatar o texto. A principal característica do HTML é a de ser hipertexto. Hipertexto significa adicionar no próprio texto formas diversas de navegação entre eles. Ou seja, cada texto possui caminhos para outros textos.

Novas funcionalidade, ou seja etiquetas, estão sendo continuamente adicionadas no padrão HTML. Navegadores como o Netscape e Internet Explorer tem etiquetas proprietárias. Essa é uma forma da indústria de software forçar a inclusão de novos padrões no HTML. Atualmente a padronização da linguagem de etiquetas HTML é definida pela RFC-2070. A RFC-2070 é adiciona basicamente a internacionalização ao HTML 2.0.

O software de gerenciamento utiliza o padrão HTML 2.0.CGI

CGI ou *Common Gateway Interface* define um método pelo qual o servidor WWW adiciona a si programas e serviços adicionais. A CGI permite ao servidor WWW aumentar a sua funcionalidade manipulando dados e processos externos através de uma ponte, daí o termo *gateway*, entre ambos. A CGI portanto tem um conjunto de especificações definidas pelos autores do HTTP. Uma característica da CGI é que os programas podem ser escritos em qualquer linguagem de programação como, por exemplo, C, C++, Perl, Java, Fortran, ou até mesmo *script* interpretado por algum *shell* disponível no sistema.

A linguagem empregada para desenvolver o software de gerenciamento foi inicialmente C/C++. Posteriormente, mudou-se para a linguagem Perl, mas diversas CGIs permaneceram em C/C++. Um estudo melhor da linguagem Perl forçou-nos mudar a linguagem. O tempo de aprendizado da linguagem Perl aliado com as funcionalidades inerentes a transformou na melhor escolha, mesmo em detrimento da segurança do código.

3.2.5 SSL – Criptografia por Chave Pública e Certificados

SSL (ou *Secure Socket Layer*) usa um algoritmo para criptografar chamado de criptografia por chave pública para autenticação. O algoritmo é baseado no conceito de chave pública e chave privada. O navegador e o servidor tem ambas as chaves. As chaves públicas e privadas tem uma relação funcional especial, mas há um postulado matemático garantindo que a partir de uma chave é difícil gerar por inspeção ou cálculo (força bruta computacional) o par correspondente.

A chave pública é divulgada para todos enquanto a chave privada é de conhecimento apenas do dono. Qualquer mensagem codificada com a chave pública de alguém

somente poderá ser decodificada com a chave privada correspondente. Estando essa em poder único e exclusivo do dono, apenas esse poderá decodificar a mensagem. O sistema é simétrico, portanto uma mensagem codificada com a chave privada somente será decodificada com a chave pública correspondente.

Para garantir a autenticidade da chave pública de alguém é utilizado algo conhecido por certificado. Esse certificado é uma forma de garantir que a chave pública passada por um indivíduo é legítima e de boa fé. O certificado contém a chave pública do servidor, por exemplo, e é assinado por uma terceira pessoa codificado com a sua chave privada. Dessa forma, qualquer um pode decodificar o certificado com a chave pública dessa terceira pessoa para a validação. Esse terceiro pode ser qualquer pessoa ou como é mais comum, uma empresa dedicada à tarefa de assinar certificados. A *Netscape Communications* usa a companhia *RSA Data Security* para assinar seus certificados.

3.3 Gerenciamento Nível 1: Gerenciando a Máquina

O Gerenciamento Nível 1 concentra as atividades rotineiras da máquina como manutenção nos servidores WWW, FTP e correio eletrônico, nas contas de usuários, nas conexões externas via modem e no funcionamento da máquina. As atividades de manutenção serão descritas em detalhes na próximas seções. O acesso é feito no endereço padrão para o servidor seguro:

<https://<nome da máquina ou número IP>/>

Ao fazer o acesso a URL o navegador checa a autenticidade do certificado apresentado pelo servidor. Entretanto o certificado não está assinado por nenhuma empresa conhecida pelo navegador, gerando uma série de avisos alertando para a confiabilidade do servidor. Note que as mensagens de aviso não indicam um

comprometimento da segurança da conexão, mas simplesmente emitem um juízo sobre a autenticidade do servidor.

Figura 10 - Processo de Autenticação e Criptografia

A Figura 10 - Processo de Autenticação e Criptografia mostra os vários passos da autenticação do site e criptografia. Após efetuada a troca de chaves permitindo um tráfego seguro de informações, o servidor solicita ao usuário que entre com o nome e senha (Figura 11 - Senha de Acesso para o Gerenciamento Nível 1)

Figura 11 - Senha de Acesso para o Gerenciamento Nível 1

Após o usuário *root* ser autenticado pelo servidor, o acesso ao Gerenciamento Nível 1 é realizado através das atividades apresentadas na página principal (Figura 12 - Página principal do Gerenciamento Nível 1).

Figura 12 - Página principal do Gerenciamento Nível 1

A Figura 12 é a página inicial para o Gerenciamento Nível 1. A partir desta tem-se o acesso a nove atividades de gerenciamento do MSP.

1. servidor WWW: gerencia o servidor WWW permitindo ativar ou desativar e remover ou adicionar arquivos ao servidor.

2. servidor de correio eletrônico: gerencia o roteador de mensagens eletrônicas (*sendmail*), o servidor de correio eletrônico (*popper*) e grupos de usuários (*aliases*).
3. servidor de arquivos: gerencia o servidor de arquivos (FTP) permitindo ativar ou desativar; remover ou adicionar arquivos e diretórios do servidor.
4. servidor de nomes: gerencia o servidor de nome (DNS) permitindo criar base de dados de servidor primário e secundário; listar, adicionar e remover nomes da base de dados do servidor DNS e do DNS reverso.
5. banco de modems: gerencia a configuração das conexões externas via modem; configura o autenticador de usuários.
6. tabela de roteamento: gerencia a tabela de roteamento estática da máquina permitindo listar, testar, adicionar ou remover rotas estáticas.
7. usuários: permite criar ou remover contas de usuários. Também permite alterar informações ou a senha de contas criadas.
8. senha: permite a alteração da senha de acesso ao Gerenciamento Nível 1.
9. Funcionamento: permite desligar ou reinicializar a máquina.

Cada módulo permite a configuração e manutenção de um serviço/recurso no sistema. Algumas configurações devem ser feitas apenas uma única vez, pois as manutenções subseqüentes geram informações/configurações baseadas na inicial. É o caso do DNS, por exemplo. Outras, entretanto podem ser alteradas sem que haja modificação nas informações adicionadas anteriormente.

As seções seguintes descrevem as diversas funções disponíveis para cada módulo. As linhas de código HTML ou das CGIs relacionadas serão expostas e comentadas

quando se fizer necessário. Porções de código de outros módulos que sejam análogas farão referência aos já descritos.

Para as máquinas Portal BARF com conexão via linha discada tem a opção de se conectarem à outras localidades através do modem. Essa funcionalidade somente está disponível nessa máquina. A seção 3.3.10 detalha o processo.

3.3.1 Servidor WWW

Este módulo gerencia o servidor de WWW da máquina. É preciso inicialmente configurar os arquivos de inicialização para que o servidor possa operar corretamente. Algumas informações para configurar os arquivos de inicialização são obtidos junto ao sistema enquanto outras são sugeridas com possibilidade de serem alteradas.

3.3.1.1 Configurar Servidor WWW

A Figura 13 contém a página inicial do módulo enquanto a Figura 14 contém a página gerada pela CGI *webserver.pl*. O nome e o número IP da máquina são configurados em outro módulo (seção 3.4.6) e foram obtidos diretamente do arquivo de inicialização do sistema. O Código 1 contém a porção da CGI *webserver.pl* que busca as informações nos arquivos de inicialização do sistema e que serão utilizados para a criação da página de instalação.

```
while ( $p = <ARQ> ) {
    chop $p;
    my @tmp = split(/\s+/, $p);
    #!/bin/sh
    #/sbin/ifconfig ed0 inet 200.231.229.2 netmask 255.255.255.240
    #/sbin/route add default 200.231.229.1
    #/bin/hostname diamante.fdsc.unimed.com.br

    $_ = $tmp[0];

    if (/ $command/) {
        if (/ $IFCONFIG/) { return $tmp[3]. " " . $tmp[5]; }
    }
```

```

        if (/ $ROUTE/)      { return $tmp[3]; }
        if (/ $HOSTNAME/)    { return $tmp[1]; }
    }
}

```

Código 1 - Porção do *webserver.pl* que obtém o número IP e o nome da máquina.

Figura 13 - Controle do Servidor WWW

As informações obtidas pela CGI *webserver.pl* são passadas para a CGI seguinte utilizando o modificador *hidden* do comando *input* da linguagem HTML. O Código 2 contém a porção do código da Figura 14 com os dados obtidos pela *webserver.pl*.

```

<form method="POST" action="/cgi-bin/server">
<input type="hidden" name="servname"
value="pepsi.ifqsc.sc.usp.br">
<input type="hidden" name="ipnumber" value="143.107.229.79">

```

Código 2 - Código da página da Figura 7.

Estes dados são obtidos junto ao sistema e não podem ser alterados.

Formulário de Configuração do Servidor WWW - Netscape

https://pepsi.ifqsc.sc.usp.br/cgi-bin/webserver.pl

Instalação do Servidor WWW

Configurando o Portal *pepsi.ifqsc.sc.usp.br* (143.107.229.79)

Na maioria das instalações de intranet não é necessário configurar esses parâmetros, pois os valores pré-configurados geralmente funcionam a contento. Estes dados são sugeridos, mas podem ser alterados caso se deseje.

Número da Porta do Servidor

Digite o número da porta associada ao protocolo HTTP. Os valores válidos são qualquer número entre 1.024 e 65.535 ou então 80, que é o endereço padrão.
Caso seja escolhida uma porta não-padrão (diferente de 80), o servidor somente responderá com declaração explícita da porta. Por exemplo, se o servidor for configurado para responder na porta 2300, a URL de <http://pepsi.ifqsc.sc.usp.br:2300/>.

Número da porta do Servidor WWW:

Número de Processos

O servidor WWW cria um número inicial de processos no **Portal-BA**, aguardando os pedidos de conexão. Um novo processo é criado automaticamente para cada conexão adicional até o número máximo de processos seja atingido, a partir do qual nenhuma nova conexão será aceita até que alguma das conexões ativas termine. Esse mecanismo impede que o **Portal-BA** fique sobrecarregado com uma quantidade excessiva de conexões.

Número inicial de processos:

Número máximo de processos:

Controle do Servidor

Continuar

Cancelar

Copyright (C) 1996 Total Informática Ltda. Todos os direitos reservados

Figura 14 - Configurando o Servidor WWW

Os arquivos de inicialização são copiados a partir de um diretório inicial, sofrem as alterações necessárias e finalmente são movidos para a árvore de diretórios definitivos.

Os dados enviados pela página da Figura 14 são tratados pela CGI *server* que gera uma página de confirmação (Figura 15).

Figura 15 - Página de Confirmação de Instalação

Caso a configuração não esteja correta pode-se cancelar a operação. Até este ponto houve apenas a coleta de informações necessárias para a configuração, portanto um cancelamento não altera a configuração ativa.

3.3.1.2 Ativar o Servidor WWW

Após configurado o servidor WWW, conforme descrito na seção 3.3.1.1, pode-se a partir dessa página iniciá-lo selecionando a opção continuar (Figura 16 - Inicializar o Servidor WWW). A Figura 10, confirma a inicialização do serviço e apresenta a opção para testar o funcionamento.

Figura 16 - Inicializar o Servidor WWW

Figura 17 - Testar o Servidor WWW

Podemos fazer o acesso ao servidor WWW selecionando o link *Testar o servidor WWW* na Figura 17 ou novamente retornar ao Controle do Servidor.

3.3.1.3 Enviar Arquivo

As opções “Transferir do micro”, “Transferir do disquete” e “Remover Arquivo” possibilitam o gerenciamento de arquivos e da árvore de diretórios do servidor WWW. É possível disponibilizar os 3 tipos básicos de arquivos no servidor:

HTML: arquivos no formato texto codificados em HTML.

Programa (ou CGI): programas compilados ou *scripts* em linguagem PERL ou *shell*.

Imagem: arquivos de imagem digitalizadas codificadas em algum formato padrão da linguagem HTML.

A Figura 18 apresenta a página para envio dos arquivos para o servidor WWW. O arquivo a ser enviado pode ser localizado através do *Browser*. No campo “Gravar como” é especificado o nome com que o arquivo deverá ser gravado no servidor. Esse campo não se limita aos 8 caracteres, característica dos DOS 6.x e inferiores. O nome pode conter o diretório que caso não exista será criado. Outro campo a ser

selecionado é o tipo de arquivo. Arquivos HTML tem o acesso feito através da URL <http://<nome da máquina ou IP>/>; imagens, através da URL <http://<nome da máquina ou IP>/icons/>; e CGI, <http://<nome da máquina ou IP>/cgi-bin/>.

Figura 18 - Enviar Arquivo para o Servidor WWW

Os arquivos do tipo HTML podem ser colocados em diretórios o que requer um tratamento especial na criação. Procura-se no nome do arquivo por caracteres especiais como |, ., @, etc. Duplo ponto (..) também é procurado.

Os arquivos do tipo CGI precisam ter os bits do modo de acesso de arquivo alterados para que o servidor possa executá-los.

Uma flexibilidade para envio de arquivos é a opção transferir os arquivos via unidade de disquete presente na máquina. Os arquivos devem estar gravados com no máximo oito caracteres para nome e três para extensão.

Figura 19 - Enviar Arquivo via Unidade de Disquete

Ao selecionar o botão continuar (Figura 19), o sistema listará todos os arquivos do disquete para que seja escolhido aquele a ser disponibilizado no servidor.

3.3.1.4 Remover Arquivos ou Diretórios

Através dessa opção pode-se remover qualquer arquivo (HTML, programas ou imagens) do servidor WWW ou diretórios. Os arquivos a serem removidos são listados em sua árvore de diretório dentro de uma das três categorias: HTML,

programas ou imagem (Figura 20). Dessa forma, toda a estrutura de arquivos pode ser visualizada permitindo uma rápida localização dos arquivos (Figura 21). A listagem para remoção de arquivos CGI e imagens é igual a dos arquivos HTML.

Figura 20 - Removendo arquivos ou diretórios do servidor WWW.

Figura 21 - Lista de arquivos do servidor WWW.

É possível também fazer a remoção de diretórios inteiros. Entretanto, na listagem para remoção de diretórios não é possível visualizar seu conteúdo (Figura 22). Antes que seja feita a remoção de qualquer arquivo ou diretório, todos os selecionados são listados. Pode-se então cancelar a remoção ou confirmá-la através dos botões apropriados.

Figura 22 - Lista de diretórios do servidor WWW.

Figura 23 - Confirmação da remoção de arquivos.

3.3.2 Servidor de Correio Eletrônico

As atividades executadas a partir dessa opção são de gerenciamento do serviço de correio eletrônico e do recurso de criação de grupos (*aliases*). A Figura 24 mostra as opções de atividades. Essas serão discutidas em detalhe nas seções seguintes.

Figura 24 - Atividades disponíveis para Correio Eletrônico.

3.3.2.1 Roteador de mensagens eletrônicas

Permite ativar ou desativar o programa responsável por enviar e receber mensagem eletrônica (Figura 25). Na maioria dos sistemas operacionais Unix é utilizado o programa *sendmail*.

Figura 25 - Ativar ou desativar o roteador de mensagens eletrônicas.

O roteador utilizado no FreeBSD, como na maioria dos sistemas é o *sendmail*. Para a opção de ativar, primeiramente o roteador *sendmail* é desligado sendo em seguida ativado com as opções padrões.

3.3.2.2 Servidor de correio eletrônico

Permite ativar ou desativar o servidor *popper*. *Popper* é uma implementação do servidor *Post Office Protocol* (Figura 26). Através desse servidor o usuário pode gerenciar suas mensagens eletrônicas no servidor.

Figura 26 - Ativar ou desativar servidor de mensagens eletrônicas.

A opção selecionada altera um dos arquivos de inicialização do sistema. Dessa forma, durante a próxima reinicialização o servidor de correio eletrônico somente será inicializado caso a opção escolhida tenha sido a de ativar. O arquivo do sistema alterado é o de configuração *inetd.conf*. O programa *inetd* espera conexões de soquetes da Internet. Quando uma conexão é requisitada ele decide para qual serviço corresponde o soquete e inicializa o programa para atender ao serviço requisitado. Dessa forma, o serviço somente é executado quando necessário economizando em processamento. O Código 4 mostra a parte do código responsável por alterar a linha do arquivo de configuração do programa *inetd* desativando o servidor de mensagens eletrônicas, enquanto o Código 3, ativa.

```
$line =~ s/^\#$POP3D/$POP3D/;  
@saida = (@saida, $line);
```

Código 3- Habilitando o servidor de mensagens eletrônicas.

```
$line =~ s/^\$POP3D/^\#$POP3D/;  
@saida = (@saida, $line);
```

Código 4 - Desabilitando o servidor de mensagens eletrônicas.

Após o arquivo de configuração ser alterado habilitando ou desabilitando o servidor de mensagens eletrônicas, o programa *inetd* recebe um sinal para reinicializar. O Código 5 mostra a porção responsável por obter o *PID* (número de identificação da

execução do processo) e enviar o sinal 1 (*HANGUP*) de reinicializar forçando o programa *inetd* a reler o seu arquivo de configuração.

```
if ($linha =~ /inetd/) {  
    @words = split(' ', $linha);  
    $pid = $words[0];  
    kill 1, $pid;  
}
```

Código 5 - Enviando sinal para reinicializar o processo inetd.

3.3.2.3 Grupos de usuários

Essa opção permite gerenciar o recurso de *aliases* do roteador de correio eletrônico *sendmail*. Esse recurso permite que ao enviarmos uma mensagem eletrônica para um endereço essa seja distribuída para uma lista (grupo) de usuários. As atividades relacionadas com esse serviço são adicionar, listar ou remover grupos e usuários (Figura 27). As seções seguintes discutem em detalhes as atividades realizadas em cada opção.

Figura 27 - Configurando grupos e usuários.

3.3.2.3.1 Adicionar Usuários

Permite adicionar o endereço eletrônico de usuário em qualquer lista já criada (Figura 28). É possível adicionar o mesmo endereço eletrônico em vários grupos já criados simultaneamente.

Figura 28 - Adicionando usuário a grupos.

Cada grupo existente tem o seu arquivo de usuários em */total/aliases/*. As alterações são feitas em uma cópia do arquivo do diretório */total/aliases/*. Após terminada as alterações o arquivo original é renomeado para */total/aliases/grupo.old* e o arquivo auxiliar para */total/aliases/grupo*. O mostra a porção do Código 6 que renomeia os arquivos e ativa as alterações no sendmail enviando o comando *newaliases*.

```
# Inicializando variaveis e paths
$NEWALIASES      = "/usr/bin/newaliases";
.....
#
# Atualizando e
```



```
# salvando /total/aliasas/file /total/aliasas/file.bak
#
#   system ( "/bin/cp -f $File $File.bak");
#   system ( "/bin/cp -f $TmpFile $File" );
#
# Atualizando sistema
#
$Output = '${NEWALIASES}';
return "Ok";
```

Código 6 - Salvando alterações e ativando aliasas.

Os usuários inscritos na lista estão um por linha no arquivo */total/aliasas/grupo*. O

Código 7 mostra um arquivo exemplo de uma lista.

```
andresal@ifq.sc.usp.br
elaine
marcelo
```

Código 7 - Arquivo de usuários inscritos.

3.3.2.3.2 Remover Usuários

Permite remover usuários em qualquer grupo criado. É fornecido uma lista de todos os grupos criados com os endereços eletrônicos dos usuários (Figura 29)

Figura 29 - Lista de usuários a serem removidos de listas.

Os grupos criados e presentes em */etc/aliases* têm seu conteúdo listado em forma de um formulário para seleção da remoção (Figura 29). A Figura 30 mostra o pedido para confirmação da remoção dos usuários nas listas. Até esse ponto nenhuma alteração nos arquivos das listas foi realizado. A confirmação para remover os usuários selecionados ativa a CGI *aliases_act.pl* responsável por remover usuários de listas. Para a remoção de usuários é feito uma cópia linha por linha, exceto aquelas que contém o endereço eletrônico a ser removido, do conteúdo de cada lista em um arquivo temporário. Finalizada a cópia, o arquivo original é renomeado recebendo uma extensão *old* e arquivo temporário recebe o nome do original.

Figura 30 - Confirmação dos usuários a serem removidos das listas.

3.3.2.3.3 Listar Usuários

Essa ação lista todos os grupos criados com os endereços eletrônicos dos usuários. A Figura 31 mostra uma listagem de todos os grupos criados presentes no arquivo */etc/aliases* com seus respectivos usuários cadastrados. Para cada grupo existente é feito uma varredura linha por linha de seu conteúdo formatando a saída em HTML.

Figura 31 - Listagem dos usuários de cada lista.

O Código 8 mostra a porção do código que lista o grupo enquanto o Código 9, a porção que lista cada usuário cadastrado.

```
my @arq = split (/:/, $word[1] );
$arq[2] =~ s/\\/ /g;
my $Group = basename($arq[2]);
print "<DD><LI>$Comment
<I>($Group\\@$Hostname)</I>: <I><font size=-1>";
```

Código 8 – Formatação da lista de grupos.

```
print "<OL>\n";
while ( $user = <ARQ2> ) {
    chop ($user);
    @tmp = split ( //, $user );
    if ( $tmp[0] ne "#" && $tmp[0]) { print
"<DD><LI>$user\n"; }
    }
print "</OL>\n";
```

Código 9 - Formatação da lista de usuários.

3.3.2.3.4 Adicionar Grupo

Essa ação cria um grupo aonde os usuários de uma mesma categoria tem adicionados seu endereço eletrônico. A criação de um grupo requer um nome e um comentário

sobre o grupo. A Figura 32 mostra as informações necessárias que devem ser entradas. As definições dos grupos são adicionadas no arquivo */etc/aliases*.

Figura 32 - Criando grupo de usuários.

As alterações são feitas em uma cópia do arquivo */etc/aliases* do sistema. Após terminada as alterações o arquivo original é renomeado para */total/aliases/aliases.bak* e o arquivo auxiliar para */etc/aliases*. O Código 10 mostra a porção do código que renomeia os arquivos e ativa as alterações no sendmail enviando o comando *newaliases* que reconstrói a base de dados do arquivo de *mail alias* do roteador de mensagens eletrônicas.

```
# Inicializando variaveis e paths
$NEWALIASES      = "/usr/bin/newaliases";
.....
#
# Atualizando e
# salvando /total/aliases/file /total/aliases/file.bak
#
    system ( "/bin/cp -f $File $File.bak");
    system ( "/bin/cp -f $TmpFile $File" );
#
# Atualizando sistema
#
    $Output = '${NEWALIASES}';
    return "Ok";
```

Código 10 - Salvando alterações e ativando aliases.

A tentativa de criação de um grupo que já exista não é permitida retornando uma mensagem de erro.

3.3.2.3.5 Remover Grupo

Essa ação permite a remoção de grupos de usuários existente. É feita uma listagem dos grupos existentes constantes do arquivo */etc/aliases* com suas descrições para que seja selecionado aqueles a serem removido(Figura 33). A Figura 34 mostra a listagem dos grupos que serão removidos solicitando a confirmação. A remoção dos grupos existentes é similar ao da remoção dos usuários de um grupo. É feito uma cópia linha por linha do arquivo */etc/aliases* para um arquivo temporário exceto pelas linhas correspondentes aos grupos sendo removidos. Após a cópia ser realizada os arquivos originais e temporários são renomeados respectivamente para */total/aliases/aliases.bak* e */etc/aliases*.

Figura 33 - Listagem dos grupos para serem removidos.

Figura 34 - Confirmação dos grupos a serem removidos.

```
while ( <AF2D> ){
    chop;
    if ( !/^$Group:/ && !/^\\#$Comment\\#/ ) {
        print TmpAF "$_\\n" ;
    }
}
```

```

close(TmpAF);
close(AF2D);
#
# Atualizando e salvando copia origina do /etc/aliases
# salvando /total/aliases/file /total/aliases/file.old
#
system ( "/bin/cp -f $ALIASES_FILE $ALIASES_FILE_BAK" );
system ( "/bin/cp -f /total/aliases/$Group
/total/aliases/$Group.old" );
system ( "/bin/cp -f $TmpFile $File" );
return "Ok";

```

Código 11 - Atualizando arquivo e salvando arquivos originais.

O Código 11 mostra a porção do código responsável por excluir as linhas correspondentes aos grupos sendo removidos, atualizar o arquivo */etc/aliases* e salvar uma cópia do arquivo acrescida da extensão *bak*.

3.3.2.3.6 Listar Grupo

Essa ação lista todos os grupos criados presentes no arquivo */etc/aliases*. Cada grupo é listado com seu nome e respectiva descrição (Figura 35).

Figura 35 - Listagem dos grupos existentes.

O Código 12 mostra a porção do código que executa a listagem dos grupos formatando a saída em HTML para uma lista não ordenada.

```

while (<ARQ>) {
    $Linha = $_;
    chop $Linha;

```

```

@word = split ( / /, $_ );
if ( $#word - $[ + 1 > 1 ) {
    @tmp = split ( //, $word[1] );
    @tmp1 = split ( //, $word[0] );
    if ( ($tmp1[0] ne "#") && ($tmp[0] eq "\"") ) {
        $word[0] =~ s/://g;
        print "<DD><LI>$Comment:
<I>$word[0]</I><p>\n";
    }
}
$Comment = $Linha;
$Comment =~ s/\#//g;
}

```

Código 12 – Formatação da lista de grupos.

3.3.3 Servidor de arquivos

As atividades executadas a partir desse módulo são de configuração , obtenção de status e gerenciamento do servidor de arquivos. O servidor de arquivos utilizado é o *wu-ftpd* da *Washington University*. Esse servidor tem recursos como:

Histórico dos arquivos transferidos: é arquivado uma listagem de todos os arquivos que foram copiados do servidor. Esse recurso está ativo.

Histórico dos comandos: é arquivado uma listagem de todos os comandos executados pelo usuário durante uma sessão. Esse recurso está ativo.

Classificação dos usuários por tipo e localização: é possível grupos de usuários por nome ou por nome de máquina.

Permissão de acesso ao sistema a nível de usuário: limita o usuário a ter acesso apenas a seu diretório raiz. Dessa forma não é do conhecimento do usuário o conteúdo dos arquivos do sistema ou do diretório de outros usuários. Esse recurso está ativo.

Restrição a conta anônima;

Mensagens de aviso geral e por diretórios;

Filtro de nome de arquivos.

As atividades desse módulo estão separados em configuração e manutenção e são descritas nas subseções seguintes. A Figura 36 mostra as ações disponíveis.

Figura 36 - Gerenciando o servidor de arquivos.

3.3.3.1 Configuração do Servidor de Arquivos

3.3.3.1.1 Configuração da Mensagem de Entrada

Essa opção permite alterar o conteúdo da mensagem de boas vindas do servidor de arquivos. Sempre que um usuário se conectar como anônimo (*anonymous* ou *ftp*) será mostrado essa mensagem.

Figura 37 - Alterando mensagem ativa do servidor de arquivos.

A Figura 37 mostra a mensagem ativa do sistema para que seja feita as alterações. O arquivo contendo a mensagem de entrada ativa é lido linha por linha e inserido no meio do código HTML para produzir a página como mostrada na Figura 37. O usuário deve fazer as alterações no quadro *Mensagem*. Para desfazer as alterações basta selecionar o botão “*Desfazer Modificações*”. Quando o usuário estiver satisfeito com as alterações é necessário selecionar o botão “*Usar Esta Mensagem*”

para tornar ativa a mensagem. O usuário tem a seu dispor um coleção de variáveis pré-definidas pelo servidor. São elas:

%T: horário local (da forma Thu Nov 15 17:12:42 1990).

%C: diretório corrente.

%E: endereço de e-mail do responsável.

%R: nome da máquina de quem está acessando.

%L: nome da máquina onde está o servidor de arquivos (Portal-BAR).

%U: username digitado.

%M: número máximo de usuários conectados simultaneamente.

%N: número de usuários conectados no momento.

Caso o usuário prefira, pode-se restaurar a mensagem ativa para uma mensagem padrão selecionando o botão “*Usar Mensagem Padrão*”. Será mostrado as opções com a mensagem padrão (Figura 38). Novamente o usuário tem a opção de fazer ajustes necessários na mensagem antes de torná-la ativa. Pode-se desfazer qualquer alteração ou retornar para alterações na mensagem ativa.

Figura 38 - Mensagem padrão do servidor de arquivos.

As alterações da mensagem são inseridas diretamente no arquivo `/home/ftp/welcome.msg`. O Código 13 mostra a porção do código que define o caminho do arquivo e a escrita do conteúdo.

```
# Definindo as variaveis.
$FtpDir    = "/usr/home/ftp";
.....
open ( ARQ, ">$FtpDir/welcome.msg" );
print ARQ $query->param('mensagem');
```

Código 13 - Criando mensagem de entrada do servidor de arquivos.

Ainda é possível, em ambos os casos, retornar ao menu principal de controle ou cancelar a operação voltando ao menu de controle do servidor de arquivos. A Figura

39 mostra a mensagem de entrada obtida no cliente de FTP para uma conexão ao servidor de arquivos.

Figura 39 - Mensagem de entrada obtida pelo cliente FTP.

3.3.3.1.2 Configurando Número Máximo de Clientes

Essa opção permite configurar o número máximo de acesso simultâneo ao servidor de arquivos. A Figura 40 mostra a configuração ativa do servidor de arquivos para o número máximo de conexões simultâneas. Qualquer alteração no número de clientes deve ser ativada através do botão “*Configurar Número Máximo de Clientes*”. Para obter o valor padrão do servidor basta selecionar “*Selecionar Número Padrão de Clientes*” e ativar através do botão “*Configurar Número Máximo de Clientes*”. Após selecionar o botão “*Configurar Número Máximo de Clientes*” o número selecionado é inserido no arquivo de configuração. O Código 14 mostra a porção do código que altera o arquivo de configuração do servidor de arquivos. Não é necessário reinicializar o servidor de arquivos pois ele é controlado pelo programa *inetd* (como mencionado anteriormente na seção 3.3.2.2).

Figura 40 - Configurando número de clientes do servidor de arquivos.

```
if ( $tmp[0] eq "limit" ) {  
    print TMP "limit    all    ".$maxclients."  
Any      /etc/mmsgs/msg.dead\n";  
} else { print TMP $_."\n"; }
```

Código 14 - Alteração do número clientes.

3.3.3.1.3 Configurando Tipo de Senha para Acesso Anônimo

Quando o usuário se conecta ao servidor de arquivos como anônimo utilizando o *username anonymous* ou *ftp*, uma senha é solicitada. Essa senha é arquivada nos logs do sistema apenas para efeito de estatística. A senha a ser digitada é sugerida como sendo o endereço eletrônico do usuário. Embora não seja possível validar o conteúdo digitado é possível forçar o usuário a usar:

1. Qualquer senha que contenha @: note que qualquer sequência de caracteres que contenha @ será aceito, como por exemplo, abcd@efgh.123.
2. Senha do tipo joao@usp.br: nesse caso apenas endereços eletrônicos corretos são válidos, embora não seja testado a existência.

3. Nenhuma senha é exigida.

Para um tipo de senha escolhida é possível configurar a ação tomada caso o valor digitado não se adequa ao exigido. São eles:

1. Avisa o usuário, mas permite o acesso: mesmo não tendo entrado uma senha adequada é permitido ao usuário acesso aos arquivos após mensagem de advertência.
2. Avisa o usuário, mas não permite o acesso: nesse caso é mostrado uma mensagem de acesso negado e sugerido nova tentativa com exemplo de senha a ser utilizada.

A configuração desses procedimentos é feita através da ação disponível na Figura 41.

Configuração do Servidor de FTP
Configurando Tipo de Senha

Tipo de Senha

Você deve especificar que senha um usuário que tentar o acesso ao servidor de arquivos com o *username anonymous* ou *ftp* deve digitar. É possível determinar também que ação tomar quando a senha digitada não for do tipo exigido.

Tipo de senha:

- ☐ Nenhuma senha é exigida.
- ☐ Qualquer senha desde que contenha o caracter '@'.
- ☒ A senha do tipo joao@unimed.com.br

Tipo de Ação:

- ☒ Avisa o usuário, mas permite o acesso.
- ☐ Avisa o usuário, mas não permite o acesso.

Configurar Apagar este Formulário

Controle do Servidor Continuar Cancelar

Copyright (C) 1996 Total Informática. Todos os direitos reservados.

Figura 41 - Configurando tipo de senha de acesso ao servidor de arquivos.

As opções selecionadas são enviadas para a CGI *passkind.pl* que as altera em uma cópia do arquivo de configuração. Finalizada as alterações na configuração, o arquivo temporário é copiado para */usr/local/etc/ftpaccess*. Os próximos acessos ao servidor de arquivos deverão seguir as normas estabelecidas na configuração. O Código 15 mostra a porção do código que altera as ações no arquivo de configuração.

```
while (<ARQ>) {
    chop;
    @tmp = split ( " ", $_ );
    if ( $tmp[0] eq "passwd-check" ) {
        print TMP "passwd-check" ".$password." ".$acao."\n";
        $Trocou = "yes";
    } else { print TMP $_."\n"; }
}
```

Código 15 - Alterando configuração para acesso anônimo.

3.3.3.2 Manutenção do Servidor de Arquivos

3.3.3.2.1 Ligar ou Desligar o Servidor

Ao selecionar a opção “*Ligar o Servidor*” ou “*Desligar o Servidor*” é feito uma checagem no sistema para o obter o status atual do servidor de arquivos. Caso esse já esteja ligado é fornecido a opção de desligá-lo conforme a Figura 42.

Figura 42 - Desligar o servidor de arquivos.

Se o servidor de arquivos estiver desligado é fornecido a opção para ligá-lo (Figura 43)

Figura 43 - Ligar o servidor de arquivos.

A ação de ligar ou desligar o servidor é controlada pela existência ou não do arquivo `/etc/ftpshut`. A CGI `ftpd.pl` verifica se o arquivo `/etc/ftpshut` existe, o que indica ao servidor de arquivos que qualquer conexão deve ser barrada, e mostra a mensagem para ligar o servidor (Figura 43). Caso o arquivo `/etc/ftpshut` não exista, indicando que o servidor está recebendo conexões, é mostrada a mensagem para desligar o servidor (Figura 42). O Código 16 verifica existência do arquivo `/etc/ftpshut`.

```
#Checando se existe /etc/shutftp
$FTPD = "on";
if ( -e $shutmsg ) { $FTPD = "off"; }
```

Código 16 - Verificando a existência do arquivo `/etc/ftpshut`.

Para que o servidor deixe de receber conexões é executado o comando `ftpshut` que força a interrupção das conexões estabelecidas e cria o arquivo `/etc/ftpshut`. O Código 17 mostra a porção do código que remove o arquivo `/etc/ftpshut` e interrompe as conexões, dependendo da ação escolhida pelo usuário.

```
$ftpshut = "/usr/local/bin/ftpshut now";
$shutmsg = "/etc/shutmsg";
....
```



```
if ( $query->param('start') eq "start" ) {  
    unlink ("$shutmsg" ) }  
else { system ($ftpshut); }
```

Código 17 – Executando a ação de ligar ou desligar o servidor de arquivos.

3.3.3.2.2 Listar Usuários

É possível obter o status do servidor de arquivos através da opção listar usuários. É listado todas as conexões ativas ao servidor com:

PID: número de identificação do processo.

Terminal de controle: para conexões remotas esse campo não pode ser identificado aparecendo apenas ??.

Status do processo: a primeira letra indica o estado de execução do processo como parado, sendo executado ou dormindo; enquanto a segunda letra traz informações extras como alteração na prioridade de execução da CPU, é um processo líder, suspenso durante a execução de chamada de sistema *vfork*, etc.. .

Tempo de conexão.

Nome da máquina do visitante.

Usuário e senha entrados

Número de usuários conectados de um total máximo permitido.

A Figura 44 mostra o servidor configurado para apenas 2 usuários com 1 conexão anônima e outra do usuário local.

Figura 44 - Conexões estabelecidas no servidor de arquivos.

As informações são obtidas utilizando um utilitário do servidor de arquivos chamado *ftpwho*. É feita uma chamada de sistema e a saída é agregada ao conteúdo da página para formatação correta. O Código 18 mostra a porção do código que executa a chamada de sistema e mais abaixo a inserção da saída na formatação da página.

```
$ftpwho = "/usr/local/bin/ftpwho";  
print "Content-type: text/html\n\n";  
.....  
<pre>  
__HEAD__  
    ;  
print ` $ftpwho `;  
print<<__FOOT__;  
</pre>
```

Código 18 - Execução do comando ftpwho e formatação da saída.

3.3.3.2.3 Inserir Arquivos

A partir dessa opção é possível estar enviando arquivos para que sejam disponibilizados via servidor de arquivos. Esse processo é análogo ao do servidor WWW (seção 3.3.1.3). A Figura 45 mostra a página de envio.

Figura 45 - Enviar arquivo para o servidor de arquivos.

Após selecionado o arquivo, deve-se escolher com que nome ele será disponibilizado. Todo arquivo a ser disponibilizado estará sob o diretório *pub*. Pode-se entrar com a árvore de diretório a ser criada. Por exemplo, um arquivo a ser gravado como */softwares/win95/winzip.exe* estará disponível no servidor de arquivos em */pub/softwares/win95/winzip.exe*. Caso o diretório */softwares/win95/* não exista ele será criado.

3.3.3.2.4 Remover Arquivos ou Diretórios

A partir dessa opção é possível estar removendo os arquivos ou diretórios do servidor de arquivos. É feita uma listagem dos arquivos ou diretórios para que seja escolhido aqueles a serem removidos. Ao selecionar um diretório, todo o seu conteúdo será removido inclusive subdiretórios que possam existir. Antes porém, de remover, é solicitado ao usuário que confirme a remoção dos itens selecionados. Essa ação é idêntica a executada na seção 3.3.1.4. A Figura 46 solicita que seja escolhido se deseja remover arquivos ou diretórios. A Figura 47 apresenta a listagem de todos os

diretórios do servidor de arquivos para que seja escolhido aqueles a serem removidos.

Figura 46 - Selecionando tipo de remoção do servidor de arquivos.

Figura 47 - Removendo diretórios inteiros do servidor de arquivos.

3.3.4 Servidor de nomes

As atividades executadas a partir dessa opção são de criação e manutenção do servidor de nomes (DNS). O servidor de nomes é responsável pela tradução do nome da máquina para o seu número IP. Diversos serviços podem ficar inaceitavelmente lentos caso não haja um servidor de nomes configurado corretamente na rede local. Alguns exemplos desses serviços são o telnet e o ftp.

As ações executadas são descritas em detalhes nas seções seguintes. A Figura 48 mostra as ações disponíveis para o servidor de nomes.

Figura 48 - Ações do servidor de nomes.

Para todas as ações executadas no servidor de nomes é gerado um log no arquivo `/var/log/rede.log`. O Código 19 mostra uma porção do arquivo com algumas ações registradas.

```
[Tue 13-Jul-1999 22:32:41] DNS Adicionando nome: kas,  
143.107.228.78
```

```
[Tue 13-Jul-1999 22:41:23] DNS Adicionando nome: coke,
143.107.228.79
[Tue 13-Jul-1999 22:47:37] DNS Removendo 143.107.228.78 de
/total/named/localdomain.rev.
[Tue 13-Jul-1999 22:47:37] DNS Removendo 143.107.228.79 de
/total/named/localdomain.rev.
[Tue 13-Jul-1999 22:47:37] DNS Removendo 143.107.228.78 (kas)
de /total/named/db.localdomain
[Tue 13-Jul-1999 22:47:37] DNS Removendo 143.107.228.79 (coke)
de /total/named/db.localdomain
[Tue 13-Jul-1999 22:53:45] DNS Error : tentando remover o IP
local (49) de /total/named/localdomain.rev.
[Tue 13-Jul-1999 22:53:45] DNS Error: tentando remover
hostname (rapper) de /total/named/db.localdomain
```

Código 19 - Ações registradas do servidor de nomes no arquivo de log.

3.3.4.1 Criar o Servidor de Nomes

A primeira ação a ser executada é a criação dos arquivos iniciais do servidor de nomes. Esse servidor de nomes será secundário do domínio hierarquicamente superior e primário do inferior. É solicitado que se ensira o número IP e o domínio do servidor de nomes primário. Essas informações são adicionadas a outras provenientes da CGI (Código 20) e através de uma chamada de sistema para um *shell script* que criará os arquivos.

Configuração do Servidor de Nomes
Criando Servidor de Nomes

A partir desta página você pode criar todo o seu Servidor de Nome. Cuidado! Toda e qualquer informação adicionada anteriormente será perdida!

Entre com o número IP e o domínio do Servidor de Nomes Primário do qual esse servidor será Servidor de Nomes Secundário:

Número IP: (Ex.: 192.0.2.3)

Domínio: (Ex.: univale.com.br)

Criar Servidor de Nomes

Copyright (C) 1996,1997 Total Informática. Todos os direitos reservados.

Figura 49 - Informações sobre o servidor de nomes primário.

```
&CreatDNSFiles($SecondDNS,$SecondDNSDomain);  
.....  
sub CreatDNSFiles{  
    local ($SECDNS, $SECDNSDOMAIN) = @_;  
    my $LocalDomain = &GetLocalDomain();  
    my $LocalIP = &GetLocalIP();  
    .....  
    return system "/usr/local/etc/httpd/admin/cgi-bin/named.sh  
$SECDNS $SECDNSDOMAIN $LocalIP $LocalDomain";  
}
```

Código 20 - Passando informações para criar arquivos iniciais.

Essa ação deverá ser executada somente uma vez pois caso já exista os arquivos, esses serão removidos e recriados.

O próximo passo é a inclusão de nomes e números IPs na base de dados do servidor de nomes.

3.3.4.2 Ligar ou Desligar o Servidor de Nomes

As ações disponíveis nessa página são de ligar ou desligar o servidor de nomes (Figura 50). A opção de desligar o servidor de nomes, inútil à primeira vista uma vez que diversos serviços não funcionarão corretamente, existe para efeito de depuração de erros e possíveis ataques maliciosos à rede. Por exemplo, se algum outro servidor de nomes está ativo e com informações erradas.

Figura 50 - Ligar ou desligar o servidor de nomes.

O Código 21 mostra a porção do código que inicializa o servidor de nomes. Antes de inicializar o servidor de nomes, é verificado se já está sendo executado . Caso esteja, o servidor é desligado e em seguida reinicializado.

```
# Path e Variaveis
$NAMED      = "/usr/sbin/named -b /total/named/named.boot";
$NAMED_PID  = "/var/run/named.pid";
{
# Imprimindo o Cabecalho
  print "Content-type: text/html\n\n";
# Desligando o Servidor de Nomes
  if ( -e $NAMED_PID) {
    kill -9, `cat /var/run/named.pid`;
  }
# Ligando o Servidor de Nomes
  $Output = system "$NAMED";
```

Código 21 - Inicializando o servidor de nomes.

Para a ação de desligar o servidor de nomes (Figura 50), é utilizado o mesmo processo que o apresentado no Código 21, exceto pela diretriz de inicialização.

3.3.4.3 Adicionar Nome

A ação executada a partir desse ponto é a inclusão de um nome e número IP correspondente no servidor de nomes. As informações são adicionadas nos arquivos cópias do DNS e do DNS reverso. Após as informações serem adicionadas nos arquivos correspondentes, os arquivos são atualizados e o servidor de nomes é reinicializado.

Configuração do Servidor de Nomes
Adicionar Nomes

A partir desta página você pode adicionar nomes. Abaixo há dois campos que devem obrigatoriamente ser preenchidos. Para cada número IP de sua rede pode-se associar um nome. Este nome deverá ser único em toda rede. O nome deve ser simples podendo ser composto por caracteres, além dos alfanuméricos, " " e "-". O nome deve iniciar obrigatoriamente com uma letra. Não coloque o domínio no nome!

Número IP: (Ex.: 192.0.2.3)

Nome: (Ex.: zigoto)

Copyright (C) 1996,1997 Total Informática. Todos os direitos reservados.

Figura 51 - Adicionando máquinas no servidor de nomes.

Os valores entrados são testados antes que qualquer alteração seja feita nos arquivos da base de dados do servidor de nomes. Valores inválidos para o IP geram uma mensagem resposta avisando do possível erro. O Código 22 mostra porções do código que testa o valor do número IP entrado. Durante a inserção do nome no arquivo de domínio reverso do servidor de nomes, é testado se o nome ou número IP já constam na base. Após inserir no arquivo de domínio reverso as informações são inseridas no arquivo de domínio e o servidor de nomes é reinicializado.

Figura 52 - Aviso de erro no IP.

```
if (($dig != 0) && (! $dig =~ /\d/) || ($dig =~ /\D/)) {
    return "<b>$dig</b> em <b><i>$IP</i></b>
n&atilde;o &eacute; n&uacute;mero"; }
.....
#
# Testando de entre 0 e 255
#
    if ( !$aux1[0] ) { return "Faltou digitar n&uacute;mero no
primeiro campo de <i>$IP</I>"; }
    elsif ( $aux1[0] > 255) { return
"<b>$aux1[0]</b>.$aux1[1].$aux1[2].$aux1[3] maior que 255"; }

    if ( $aux1[1] eq "" ){ return "Faltou digitar
n&uacute;mero no segundo campo de <i>$IP</I>"; }
```

Código 22 - Testes de validação do número IP.

3.3.4.4 Listar Nomes

Essa opção não requer a passagem de nenhum dado. O sistema retorna uma lista dos valores presentes no servidor de nomes com número IP e respectivo nome conforme mostrado na Figura 53.

Figura 53 - Listagem dos dados do servidor de nomes.

O Código 23 mostra a porção do código que obtém a partir da base de dados do servidor de nomes, o número IP e nome das máquinas cadastradas.

```
while ($Linha=<ARQF>){
    chop $Linha;
    $Linha =~ s/\s+/\#/g;
    my @campo=split(/\#/, $Linha);
    if ($campo[1] eq "IN" && $campo[2] eq "A" ) {
        $IPNumber = $campo[3];
        $Name = $campo[0];
        print "<DD><LI>$IPNumber: <I>$Name.$Domain</I>";
    }
}
```

Código 23 - Obtendo dados do arquivo do servidor de nomes

3.3.4.5 Remover Nomes

Essa ação permite a remoção de um ou mais nomes (e números IPs correspondentes) da base de dados do servidor de nomes. É apresentado uma lista (Figura 54) com todos os números IPs da base de dados do servidor de nomes para que seja selecionados aqueles a serem removidos.

Figura 54 - Listagem dos números IPs a serem removidos.

Os valores selecionados anteriormente (Figura 54) são agora listados novamente para que haja a confirmação da remoção (Figura 55). Até esse ponto não houve alteração alguma na base de dados do servidor de nomes.

Figura 55 - Confirmação da remoção no servidor de nomes.

Sendo confirmada a ação, as informações são removidas da base de dados do DNS e do DNS reverso. A Figura 56 retorna o status da remoção dos dados na base. Caso se tente remover o número IP do servidor local, uma mensagem de erro será retornada.

Figura 56 - Status da remoção no servidor de nomes.

3.3.5 Banco de Modems

Essa ação permite definir a configuração das linhas seriais da máquina. As linhas seriais são de uma placa multiserial modelo Cyclades-8Yo que permite a conexão de periféricos seriais como modems, terminais ou qualquer outro periférico que suporte interface RS-232. No nosso caso, apenas modems foram conectados nas portas seriais.

É possível configurar o tipo de linha telefônica (dedicada ou discada) e o tipo de protocolo (*slip* ou *ppp*). A Figura 57 mostra as ações disponíveis que serão discutidas em detalhe nas seções seguintes.

Figura 57 - Configuração das linhas seriais.

Há um processo chamado *slipd.pl* que roda continuamente monitorizando as conexões do protocolo *slip*. É feita uma verificação contínua no arquivo */var/log/messages* onde o sistema mantém um histórico das conexões seriais. O programa *slipd.pl* gera no diretório */var/log* um arquivo para cada linha serial com extensões *off*, *trying* ou *on*. Cada extensão está relacionada com o estado atual da conexão. Dentro do arquivo estão as informações obtidas no arquivo */var/log/messages* referente ao estado atual da conexão. Dessa forma torna-se mais fácil para a CGI *statusd.pl* gerar as informações sobre cada linha e montá-las na Figura 58. A Figura 58 é obtida sempre que entra na tela de Gerenciamento Nível 1 (Figura 12).

Figura 58 - Status da conexão das linhas seriais.

O programa *slipd.pl* roda continuamente sendo inicializado durante o processo de inicialização do sistema. O Código 24 está dentro de um laço infinito e a cada alteração do arquivo */var/log/messages* é feita uma chamada a subrotina *GetStatus* responsável por atualizar os arquivos de estado de cada linha serial. Em cada transição de estado da linha é emitido um sinal sonoro correspondente.

```
if ( $Old_ctime != $ctime ) {
    $Old_ctime=$ctime;
    $Pos = &GetStatus($arqname, $Pos);
}
```

Código 24 - Atualizando arquivo de estado da linha serial.

```
if (( $Linha =~ /(slattach[\d+])/ ) && ! ( $Linha =~ /(sl[\d+])/ ) ) {
    .....
    if (/SIGTERM/) { .....; &Beep(0); }
    elsif (/Configuring/) { .....; &Beep(1); }
    elsif (/SIGHUP/){ ..... ; &Beep(2); }
```

Código 25 – *GetStatus*: detectando o estado da linha e emitindo sinal sonoro.

O programa *statusd.pl* Figura 58 mostra as informações como início da conexão, tentativa de conexão ou desconexão e as atualiza a cada cinco segundos.

3.3.5.1 Configurando Modems

Essa ação permite configurar cada linha serial da placa multiseri al individualmente. Em cada linha há um modem externo compatível com os comandos Hayes. É possível definir:

Linha telefônica discada: deve ser definida para os modems que irão receber ligações via modem dos usuários. Essa conexão permitirá ao usuário ter acesso a rede de computadores. É o mesmo processo que os atuais provedores de Internet utilizam. Esse tipo de serviço também é conhecido por *Dial-in*.

Linha telefônica dedicada: deve ser definida para as conexões entre duas máquinas através de uma LP de dados ou voz da operadora de telefonia. Normalmente é utilizada para interligar duas redes usando o servidor de acesso como roteador.

Protocolo de comunicação: é o protocolo de comunicação utilizado para conectar os modems de linha dedicada. Pode ser *slip* ou *PPP*.

Número IP da interface: número IP da ponta do roteador para as conexões tipo dedicada; ou o número IP que a máquina do usuário irá receber no caso de conexão discada.

Velocidade da conexão: velocidade de conexão entre os modems. Normalmente deve-se utilizar a velocidade mais alta 115200Kbps, entretanto dependendo da qualidade da linha telefônica é necessário ajustar esse número para valores mais baixos. Problemas com qualidade da linha telefônica são menores quando se utiliza LP de dados.

Um resumo da configuração de cada linha é gerado no arquivo */total/modem/modem.status* (Código 26) que é alterado durante o processo de configuração da linha.

```
# Status do Banco de Modems
# modem <desativada/dedicada/discada> <ip> [ip_dest]
[velocidade]
1 dedicada 143.107.228.51 115200 slip
2 dedicada 143.107.228.48 115200 slip
3 dedicada 143.107.226.2 115200 slip
4 desativada
```


5 desativada
6 desativada
7 desativada
8 desativada

Código 26 - Arquivo */total/modem/modem.status*.

O primeiro passo para configuração da linha serial é selecionar uma dentre as oito disponíveis (Figura 59).

Figura 59 - Selecionando a linha serial.

Ao selecionar a linha serial a ser configurada, é mostrado o status atual da linha (Figura 60). O próximo passo é definir o tipo de linha telefônica de acordo com a utilização: interligar redes ou acesso *Dial-in*.

Figura 60 - Especificando tipo de linha telefônica.

Para as linhas discadas será mostrada a página da Figura 61 para que seja feito as configurações restantes. É necessário fornecer:

1. Número IP que o usuário receberá quando fizer o acesso.
2. Máscara de rede do número IP.
3. Velocidade da comunicação.

Figura 61 - Configurando linha para tipo discada.

As informações são passadas para o programa *modem_d.pl*. Os valores do número IP e máscara de rede são validados como citado anteriormente. É feito uma alteração no arquivo do sistema */etc/ttys* (Código 27) informando que a linha serial deverá receber um *shell* quando for estabelecida qualquer comunicação.

```
ttyc06  "/usr/libexec/getty std.115200"  unknown on secure
```

Código 27 - Arquivo */etc/ttys*.

O usuário que se conectar via modem nessa porta serial deverá informar o usuário e senha como sendo *unired*. O *shell* do usuário *unired* (*shell* proprietário da empresa Total Informática) solicita o nome e senha do usuário para autenticar no servidor *radius*. Sendo autenticado a dupla usuário e senha, fornece-se ao usuário a opção de escolher o tipo de protocolo a ser utilizado: *ppp* ou *slip*. Dessa forma estabelece uma conexão entre as duas máquinas utilizando o protocolo desejado. Atualmente o processo é um pouco diferente pois tem disponível um outro programa chamado *mgetty* responsável por fornecer o terminal na linha serial e configurá-la.

Note que se o usuário tiver uma *shell* é possível fazer a autenticação no sistema com a dupla usuário e senha. Dessa forma seria aberto um terminal remoto, ou *telnet*. Entretanto nenhum usuário, exceto os de manutenção, tem um *shell*. Outro detalhe, é que nos casos ideais, cada máquina seria responsável por uma atividade: banco de modems, autenticador *radius* e contas de endereço eletrônico. Novamente, por questões de custos uma única máquina passou a fazer vários papéis em detrimento da segurança.

Para a configuração de linha tipo dedicada, é necessário especificar o tipo de protocolo da comunicação: *slip* ou *ppp* (Figura 62). Os valores são passados para *modem_d.pl* que se encarrega de:

- Verificar o arquivo */etc/ttys*.

- Atualizar o arquivo `/total/modem.status`.
- Desligar processo de conexão ativa na linha.
- Criar arquivo de inicialização da linha `/total/modem/start_multiserial.<n>` (onde *n* é o número da porta serial (Código 28 e Código 29).
- Se o protocolo for do tipo *slip* criar o arquivo `/total/modem/start_multser_<linha>_<device>` (Código 30) responsável pela configuração da interface.
- Ativa o processo de conexão.

Figura 62 - Configurando linha para tipo dedicada.

```
#!/bin/sh
/usr/sbin/ppp crtscs 143.107.228.49:143.107.229.67 netmask
255.255.255.0 /dev/cuac5 115200
```

Código 28 - Arquivo `start_multser.6` de uma linha dedicada com protocolo *ppp*.

```
#!/bin/sh
/sbin/slattach -h -u /total/modem/start_multser_7_cuac6 -s
115200 /dev/cuac6
```

Código 29 - Arquivo `start_multser.7` de uma linha dedicada com protocolo *slip*.

```
#!/bin/sh
/sbin/ifconfig sl$2 143.107.228.49 143.107.229.65 netmask
255.255.255.240
```

Código 30 - Arquivo *start_multser_7_cuac6* para configuração da interface com protocolo *slip*.

Após configurar a linha e gerar os arquivos necessários é mostrado um aviso (Figura 63).

Figura 63 - Linha serial configurada com sucesso.

3.3.5.2 Especificar Servidor de Acesso

A autenticação do usuário para conexão ao modem da linha discada é deixada ao cargo de um servidor *radius*. O servidor *radius* é responsável por autenticar o usuário que está se conectando ao servidor via modem. Por questões de segurança, a máquina que roda o servidor *radius* deve ser uma outra. Entretanto devido a custos, a segurança foi diminuída definindo a máquina onde estão conectados os modems como servidora de autenticação.

Figura 64 - Informando o servidor de autenticação.

A Figura 64 mostra a configuração do número IP da máquina onde o servidor de autenticação (*radius*) está rodando. Quando o usuário estabelece a conexão com um dos modems, uma *shell* de propriedade da empresa Total Informática valida a dupla nome e senha do usuário na máquina aonde roda o *radius*. A informação do número IP da máquina com servidor de autenticação é obtida no arquivo */total/radius_server*. O arquivo */total/radius_server* contém uma única linha com o número IP da máquina servidora de autenticação que está rodando o *radius*. A CGI *radius.pl* valida o número IP entrado como descrito anteriormente e o escreve no arquivo */total/radius_server*.

3.3.5.3 Obtendo Status Atual dos Modems

Essa ação retorna a configuração dos modems. A Figura 65 mostra as informações sobre a configuração das linhas seriais. Para as linhas não desativadas, entre parênteses está o número IP da interface.

Figura 65 - Configuração ativa das linhas seriais.

O arquivo `/total/modem/modem.status` (Código 26) é lido para fornecer as informações da Figura 65. Código 31 (`modem_status.pl`) mostra a porção do código que formatada as informações de cada linha serial.

```
&GetModemStatus($STATUS_FILE);
.....
if (/desativada/){ print "<dd>Modem <b>$Modem</b>:
<i>Desativada</i><p>\n"; }
elsif (/dedicada/){ $IP = $aux[2];
                    print "<dd>Modem <b>$Modem</b>:
<i>Dedicada ($IP)</i><p>\n";}
elsif (/discada/){ $IP = $aux[2];
```

```
print "<dd>Modem <b>$Modem</b>: <i>Discada  
($IP)</i><p>\n";
```

Código 31 - Formatando saída da configuração da linha serial.

3.3.6 Tabela de Roteamento

As atividades executadas estão relacionadas com a tabela de roteamento da máquina. É possível estar inserindo, removendo, testando ou listando as rotas ativas. As rotas estáticas são carregadas sempre que a máquina for reinicializada. O arquivo */total/route.total* (Código 32) contém todas as rotas estáticas sendo executado durante o processo de inicialização do sistema. A Figura 66 mostra as ações disponíveis que serão discutidas em detalhe nas próximas seções.

Figura 66 - Ações disponíveis para gerenciamento de rotas.

```
#!/bin/sh  
/sbin/route add -net 200.144.101.0 -netmask 255.255.255.0  
200.144.101.10  
/sbin/route add -net 200.246.78.0 -netmask 255.255.255.0  
200.246.78.10
```

Código 32 - Arquivo */total/route.total*.

3.3.6.1 Listar Tabela de Roteamento

Essa opção lista a tabela de roteamento ativa da máquina. A Figura 67 traz as informações relativas as rotas ativas como:

- *Destination*: ou rede destino.
- *Gateway*: ou roteador para onde os pacotes devem ser enviados.
- *Flags*: características da rota.
- *Refs*: número de conexões que usaram a rota.
- *Use*: quantidade de pacotes trafegados.
- *Netif*: nome da interface de rede utilizada.
- *Expire*: informação proveniente do programa de roteamento dinâmico.

Figura 67 - Listagem da tabela de roteamento.

A listagem da tabela de roteamento ativa é feita executando uma chamada ao sistema do comando *netstat*. O Código 33 mostra a porção do código que executa a chamada ao sistema e insere a saída no meio do código formatado HTML.

```
<DD>Rotas ativas no momento:
<B>
<font size="-1">
<pre>
__HEAD_ROTAS__

    system "$NETSTAT -nr";

    print<<__FOOT_ROTAS__;
</pre>
</font></b>
```

Código 33 - Formatação da saída do comando *netstat*.

Essa ação não executa nenhuma alteração na tabela de roteamento ativa em qualquer arquivo de rotas estáticas.

3.3.6.2 Adicionar Rota Estática na Tabela de Roteamento

Essa ação adiciona uma rota estática a tabela de roteamento e insere no arquivo de inicialização de rotas estáticas (Código 32). É necessário a passagem do:

- IP da rede (ou endereço da máquina) para a qual se deseja rotear.
- Máscara da rede (ou da máquina).
- IP do roteador.

conforme a Figura 68.

Figura 68 - Adicionando rota estática.

A rota é adicionada e as informações são incluídas no arquivo `/total/route.total` (Código 32) sendo ativadas durante o processo de inicialização da máquina.

Os números IPs e máscara passados são validados como no Código 22 descrito na seção 3.3.4.3. O Código 34 mostra a porção código que testa os valores passados.

```
$Output = &ValidIP($Network);
if ( $Output ne "Ok" ){ &WrongAddress("rede"); exit; }
$Output = &ValidIP($Netmask);
if ( $Output ne "Ok" ){ &WrongAddress("máscara de rede"); exit; }
$Output = &ValidIP($Gateway);
if ( $Output ne "Ok" ){ &WrongAddress("roteador"); exit; }
}

$Output = &RouteAdd($Network,$Netmask,$Gateway);
```

Código 34 - Validando os valores passados.

Antes de inserir a rota no arquivo, é verificado se ela já está inclusa. O Código 35 mostra a porção do código que testa a existência da rota. Após as alterações no arquivo, a rota é ativada. Toda alteração é feita em um arquivo temporário e no final do processo salva-se uma cópia do original.

```
if ( $Net eq $NetIP ) { print ARQ_RT_TMP "/sbin/route add -net
$Net -netmask $Netmask $Gateway\n";
    $Achou = "Y";
}
else { print ARQ_RT_TMP "$Linha\n"; }
}
if ( $Achou eq "N" ) {
    print ARQ_RT_TMP "/sbin/route add -net $Net -netmask
$Netmask $Gateway\n";
```

Código 35 - Adicionando rota estática ao arquivo /total/route.total.

3.3.6.3 Remover Rota Estática na Tabela de Roteamento

Essa ação permite a remoção de uma rota da tabela de roteamento ativa. É listado todas as rotas ativas (Figura 69) para que seja selecionado aquelas que serão removidas.

Figura 69 - Listagem das rotas ativas para remoção.

As rotas *default* e de *loopback* (127.0.0.1) não podem ser removidas portanto não é possível de serem selecionadas. A alteração do roteamento *default* é realizado conforme instruções na seção 3.4.6 - Rede, do Gerenciamento Nível 2.

Caso a rota selecionada seja estática, as informações constantes no arquivo */total/route.total* (Código 32) serão removidas. O Código 36 mostra a porção do código que chama a subrotina para remoção da rota estática do arquivo */total/route.total* (Código 32) e remove da tabela de roteamento.

```
sub RouteDelete{
.....
        $Output = &RouteDel($IP);          # Removendo de
        /total/route.total
        $Output = ` $ROUTE delete $IP`; # Removendo da
        tabela de roteamento
```

Código 36 - Removendo rota de */total/route.total* e da tabela de roteamento ativa.

3.3.6.4 Remover Todas as Rotas

Essa ação remove todas rotas ativas inclusive a do roteamento *default*. As informações estáticas contidas no arquivo */total/route.total* são removidas. É executado através de uma chamada *system* o comando *route* com parâmetros para remoção de todas as rotas (Código 37). O roteamento *default* é restaurado e o arquivo de rotas estáticas é criado vazio.

```
# Definindo Path
$ROUTE_DEL_ALL = "/sbin/route -n flush";
$ROUTE_FILE     = "/total/route.total";
$SRC_CONF_TOTAL = "/total/rc.total_conf";
.....
# Removendo todas as rotas
    $Output = system "$ROUTE_DEL_ALL;";
# Restaurando roteamento default
    $Output = system "$SRC_TOTAL_CONF";
# Removendo arquivo de rotas estaticas
    unlink $ROUTE_FILE;
# Criando arquivo de rotas estaticas
    $Output = system "/usr/bin/touch $ROUTE_FILE";
    $Output = system "/bin/chmod a+x $ROUTE_FILE";
```

Código 37 - Removendo rotas estáticas do arquivo */total/route.total* e da tabela de roteamento.

3.3.6.5 Testar Rota Específica

Através dessa ação é possível determinar o caminho dos pacotes até determinada máquina. Deve-se entrar com o número IP ou nome da máquina destino conforme a Figura 70.

Figura 70 - Testar rota.

As informações obtidas são geradas a partir da chamada de sistema conforme Código 38.

```
<b><font size="-1">
<pre>
__HEAD_GET_ROTAS__
    system "$ROUTE -v get $IP 2>&1";
    print<<__FOOT_GET_ROTAS__;
</pre>
</font></b>
```

Código 38 - Formatação de saída do teste de rota.

São retornadas informações como interface, máscara de rede, próximo roteador e tempos de acesso (Figura 71).

Figura 71 - Saída de teste de rota.

3.3.7 Usuários

As atividades disponíveis são para criação, manutenção e remoção de contas de **usuários** no sistema. É necessário que todo usuário tenha sido cadastrado para ter acesso:

- remoto via modem.
- ao correio eletrônico.

A Figura 72 mostra os usuários já cadastrados com as opções para adicionar, alterar ou remover usuários. Essas opções serão discutidas em detalhes nas seções seguintes.

Figura 72 - Manutenção de contas de usuários.

O Código 39 mostra a porção do código escrito em linguagem C responsável por gerar a Figura 72. As partes inicial e final da página são fixas, portanto é simplesmente impresso o conteúdo do arquivo defino no cabeçalho do programa. Para apresentar as informações sobre os usuários, é feito uma chamada ao sistema do programa *getuserinfo.pl* (Código 40).

```
/* Configuracao Geral */
#define GETUSERINFO_PL "/usr/local/etc/httpd/admin/cgi-
aux/getuserinfo.pl\x0"
#define USERINFO_HEAD
"/usr/local/etc/httpd/admin/corpos/userinfo_head.html\x0"
#define USERINFO_FOOT
"/usr/local/etc/httpd/admin/corpos/userinfo_foot.html\x0"

int main() {
    PrintFile(USERINFO_HEAD);
    GetSystem(GETUSERINFO_PL);
}
```



```
PrintFile(USERINFO_FOOT);  
}
```

Código 39 - Gerando a página de manutenção de usuários (Figura 72)

```
while (<PASSWD_FILE>) {  
  
($user,$crypt_passwd,$uid,$gid,$cp1,$cp2,$cp3,$gcos,$home,$shell) = split(/:/);  
  
    if (($uid > 1001) && ($uid != 0) && ($crypt_passwd ne  
"*)) {  
        $user_count++;  
        print STDOUT "<TR><TD><INPUT TYPE=\"radio\"  
NAME=\"user_id\" VALUE=\"${uid}\"></TD>\n";  
        print STDOUT "<TD><font size=\"-  
2\">$user</font></TD>\n";  
        print STDOUT "<TD><font size=\"-  
2\">$crypt_passwd</font></TD>\n";  
        print STDOUT "<TD><font size=\"-  
2\">$uid</font></TD>\n";  
    }  
}
```

Código 40 - Formatando a listagem dos usuários cadastrados.

O programa *getuserinfo.pl* (Código 40) obtém as informações dos usuários cadastrados no sistema a partir do arquivo */etc/master.passwd* (Código 41). O arquivo */etc/master.passwd* contém as informações de um usuário por linha onde cada dado é separado pelo caracter “:”.

```
root:HderyIjKR7mk9:0:0::0:0:Ze Root:/root:/usr/local/bin/bash  
toor:*:0:0::0:0:Bourne-again Superuser:/root:  
daemon:*:1:1::0:0:Owner of many system  
processes:/root:/nonexistent  
operator:*:2:20::0:0:System &:/usr/guest/operator:/bin/csh  
bin:*:3:7::0:0:Binaries Commands and Source:/nonexistent  
ftp:*:14:0::0:0:FTP Anonimo:/home/ftp:/bin/date  
uucp:*:66:66::0:0:UUCP pseudo-  
user:/var/spool/uucppublic:/usr/libexec/uucp/uucico  
xten:*:67:67::0:0:X-10 daemon:/usr/local/xten:/nonexistent  
nobody:*:65534:65534::0:0:Unprivileged  
user:/nonexistent:/nonexistent  
netmaint:IkaKjretyikc3j2:1000:1000::0:0:Network  
maintenance:/home/netmaint:/usr/local/bin/bash  
joao:MAM$EzlsHsHmdf0:1003:1003::0:0:Joao Jose da  
Silva:/home/joao:/usr/local/bin/tcsh  
antonio:fSWqH/RZzqdHB1:1004:1004::0:0:Antonio de  
Jesus:/home/antonio:/usr/local/bin/tcsh  
marcelo:UkjadUk3k8kae4w1:1005:1005::0:0:Marcelo Quintino da  
Silva:/home/marcelo:/usr/local/bi  
n/bash
```

Código 41 - Arquivo */etc/master.passwd*.

Os usuários possuem ID (3º dado do usuário) sempre maior que 1000, portanto ID menores não devem ser mostrados na listagem.

3.3.7.1 Adicionar Usuário

Ao selecionar o botão adicionar podemos incluir um novo usuário no sistema. É solicitado (Figura 73) as seguintes informações:

- usuário: nome do usuário no sistema com tamanho máximo de oito caracteres.
- informações: nome completo do usuário, telefone, ramal, etc.
- senha: senha pessoal do usuário.
- verificação da senha.

The screenshot shows a Netscape browser window with the title 'Formulário de Conf...'. The address bar shows 'Location: sc.usp.br/cgi-bin/usrtl_conf'. The main content area has a heading 'Cadastrando Novo Usuário' followed by the instruction 'Digite abaixo os dados do novo usuário a ser cadastrado. Esse usuário passará a ter acesso à rede.' Below this are four input fields: 'Usuário', 'Informações', 'Senha', and 'Verificação'. The 'Senha' field has a note '(Max. de 8 caracteres)'. At the bottom of the form are three buttons: 'Controle do Servidor', 'Continuar', and 'Cancelar'. A copyright notice at the very bottom reads 'Copyright © 1996 Total Informática LTDA. Todos os direitos reservados.'

Figura 73 - Cadastrando novo usuário.

Caso as senhas estejam em branco ou não sejam iguais, é apresentado uma mensagem de erro e solicitado que sejam digitadas novamente. A Figura 74 mostra esses dois tipos de erros que são tratados pelo Código 42.

Figura 74 - Erros na senha do usuário.

```

/* Testando as senhas entradas */
/* Se nenhuma senha foi passada */
if (strlen(entries[3].val) == 0 ) {
    NoPassword(entries[1].val, entries[2].val);
}
/*Comparando as duas passwords*/
else if (strcmp(entries[3].val, entries[4].val) != 0) {
    PassMismatch(entries[1].val, entries[2].val);
}
/* Tudo Ok */
else {
    strcpy(aux, AddUser(entries[1].val, entries[2].val,
entries[3].val));
    if ( strcmp(aux, "Ok") == 0 ) { PrintFile(ADDUSER_OK); }
}

```

Código 42 - Testando as senhas passadas; chamando a subrotina para adicionar usuário.

A tentativa de adicionar um usuário já existente também é detectada gerando uma mensagem de erro similar (Código 43). O Código 43 mostra esses testes e executa uma chamada ao sistema para adicionar o usuário. Note que o ID do usuário é forçado a ser maior que 1002 através da opção *-uid 1002*, pois valores inferiores são para gerenciamento do sistema.

```

if ($new_user eq "root") { &Print_FAIL_ADD_ROOT(); }
else {
    if ( &does_entry_exist ($new_user) ||
&does_uid_entry_exist($new_uid)){&Print_FAIL_EXISTS_USER();}
    else {
        $command="$adduser -v -uid 1002 -message no -shell
no -group $new_gid -batch $new_user \"\" '$new_gcos' $password
";
        system "$command >/dev/null";
        &Print_USER_ADD_OK();
    }
}

```

Código 43 - Chamada de sistema para adicionar usuário.

Estando as informações corretas o usuário é adicionado. É dada a opção de adicionar novo usuário (Figura 75), retornar ao *Controle do Servidor* (Figura 13 - Controle do Servidor WWW) ou voltar a tela de manutenção de usuários (Figura 72).

Figura 75 - Usuário adicionado com sucesso.

3.3.7.2 Alterar Usuários.

Essa atividade permite alterar:

- as informações gerais como nome completo, telefone, ramal e escritório.

- senha pessoal de acesso do usuário.

Formulário de Configuração de Usuário - Netscape

File Edit View Go Communicator Help

Bookmarks Location: per.ifsc.sc.usp.br/cgi-bin/usrtl_conf What's Related

Altera Informação de Usuário

Digite os novos dados sobre esse usuário.

Usuário : marcelo

Informações :

Senha : (Max. de 8 caracteres)

Verificação :

Copyright © 1996 Total Informática LTDA. Todos os direitos reservados.

Document: Done

Figura 76 - Alterando informações e senha de usuário.

Note (Figura 76) que o campo usuário que o identifica unicamente no sistema não pode ser alterado. Para tal ação é necessário remover o usuário já existente (seção 3.3.7.3 - Remover Usuário) e adicionar outro (seção 3.3.7.1 - Adicionar Usuário).

Somente haverá modificação das informações cujo campo for alterado. Assim, se houver a necessidade de alterar apenas o nome completo do usuário, sua senha será preservada. O Código 44 mostra a porção do código que verifica qual campo sofreu alteração. Finalmente a nova linha do arquivo de senhas é gerado e escrito no arquivo temporário.

```

if ($new_user) { $user = $new_user; }
    if ($new_gcos) { $gcos = $new_gcos; }
    if ($password) {
        srand;
    }

```

```

rand(25)+97);
    $salt = sprintf("%c%c", rand(25)+65,
    $script_passwd = crypt($password, $salt); }
#
# Construindo a nova linha do arquivo de senhas
    $new_line =
$user." ".$script_passwd." ".$uid." ".$gid."::0:0: ".$gcos." ".$
home." ".$shell;

```

Código 44 - Verificando alteração de informações.

Após terminar as modificações, é executado uma chamado do sistema para gerar o novo arquivo de senhas a partir do temporário (Código 45).

```
$cmd = $pwd_mkdb." -p ".$NEW_PASSWD_FILE;
system "$cmd";
```

Código 45 - Gerando o novo arquivo de senhas do sistemas.

Qualquer tentativa de alterar dados de contas com privilégio do sistema é detectado e bloqueado.

3.3.7.3 Remover Usuário

Através dessa opção é possível remover o usuário do sistema. Sendo confirmada a operação (Figura 77) será removido:

diretório particular.

arquivo de mensagens eletrônicas.

informações referentes nos arquivos de senhas.

grupo particular.

Figura 77 - Removendo usuário.

Até esse ponto nenhuma ação foi executada podendo-se interrompê-la selecionando o botão de cancelar. A confirmação da ação ativa uma chamada ao sistema que remove o usuário (Código 46).

```
if ($Delete) {  
    &Print_USER_DELETE_OK();  
    system "$rmuser -y ${new_user} 2>/dev/null";  
}
```

Código 46 - Chamada de sistema para remover usuário.

Qualquer tentativa de remover contas com privilégio do sistema é detectado e bloqueado.

3.3.8 Senha

Essa ação altera a senha de acesso para o Gerenciamento Nível 1 do Portal (Figura 12). Para alterar a senha de acesso deve-se fornecer a senha atual e a senha nova (Figura 78). Por segurança, a senha nova deve ser digitada duas vezes.

Figura 78 - Alteração da senha de acesso ao Gerenciamento Nível 1.

Erros como senha antiga errada, senha nova em branco ou senha diferentes são detectadas e uma mensagem de erro é mostrada. O Código 47 mostra a porção do código que detecta esses erros.

```
if (!$Old_Passwd) { &Print_ERRO3; }
elseif (!$Passwd1) { &Print_ERRO2("1"); }
elseif (!$Passwd2) { &Print_ERRO2("2"); }
elseif ($Passwd1 ne $Passwd2) { &Print_ERRO4; }
....
$OldPasswd_f=&get_oldpasswd("root");
$OldPasswd_c=&encrypt($Old_Passwd);
if ($OldPasswd_f ne $OldPasswd_c) { &Print_ERRO5; }
```

Código 47 - Validação das senhas digitadas.

Note que essa senha não é a do usuário *root* (super usuário) do sistema, mas do usuário com acesso para manutenção da máquina. Caso a senha antiga tenha sido

esquecida, somente através do Gerenciamento Nível 2 (seção 3.4.1) poderá ser alterada.

As senhas são codificadas através do programa */usr/local/etc/apache/support/cripta* sendo alterado o par *root* e senha criptografada no arquivo */usr/local/etc/apache/support/passwd* (Código 48).

```
root:GGi29dlgekls
```

Código 48 - Arquivo de senha para acesso ao Gerenciamento Nível 1.

Uma porção do programa *cripta* responsável por codificar as senhas é apresentado no Código 49. É executado a função *crypt* de codificação DES do sistema passando como argumento a senha a ser criptografada e um modificador.

```
printf ("%s\n", (char*) crypt(argv[1],aux));
```

Código 49 - Porção do código que codifica senha.

3.3.9 Funcionamento

As ações executadas são:

- reinicializar o Portal: é dado um *reboot* na máquina através do comando *reboot*.
- desligar o Portal: o sistema é parado sendo todos os processos desligados através do comando *halt*. Após os processos serem desligados a máquina pode ter a energia elétrica desligada.

A Figura 79 mostra as 2 opções.

Figura 79 - Menu para desligar ou reinicializar a máquina.

A execução dos comandos *reboot* e *halt* são feitos indiretamente. Esses comandos não podem ser processos filhos do servidor *https*. Para que o sistema seja desligado corretamente todos os processos são desligados. Um processo é tido como finalizado quando seus processos filhos também são finalizados. Para que o servidor *https* seja desligado, todos os seus processos filhos, inclusive o *reboot* ou *halt*, devem ser desligados. Quando esses são desligados o processo de reinicialização ou parada do sistema é interrompido na metade deixando o sistema funcionando parcialmente.

Para evitar tal situação, o processo de reinicializar o sistema é executado pelo *crontab*. Ao selecionar a opção *Reinicializar* um arquivo chamado “*.reboot*” é criado no diretório */total/sistemas*, ou “*.halt*” no caso de *Desligar*. O serviço *crontab* executa a cada minuto um *shell script* que testa a existência desses arquivos. Se encontrado ele é removido e o processo de reboot (comando *reboot*) ou de parada do sistema (comando *halt*) é iniciado.

```
# Reboot ou Halt se necessario
*      *      *      *      *      root
/total/system/reboot.total
*      *      *      *      *      root
/total/system/halt.total
```

Código 50 - Arquivo */etc/crontab*.

A Figura 79 e Figura 81 são compostas por dois *frames*. O visível mostra a mensagem sobre o tempo de espera enquanto o outro executa a CGI (Código 51) que cria o arquivo *.reboot* ou *.halt* no diretório */total/sistemas*. A CGI que cria o arquivo *.halt* é similar ao Código 51.

```
REBOOT="/total/system/.reboot";
/usr/bin/printf "Content-type: text/html\n\n";
/usr/bin/printf "<html><head><title>Reinicializando o
sistema</title><head><body></body>";
touch $REBOOT;
```

Código 51 - Criando arquivo */total/sistemas/.reboot*.

Figura 80 - Mensagem de aviso sobre a reinicialização da máquina.

Figura 81 - Mensagem de aviso sobre a desligamento da máquina.

3.3.10 Conexão Remota via Modem

Essa ação permite à máquina se conectar remotamente via modem em um Portal R. No estado de Santa Catarina as diversas Unimed possuíam Portal R (ou Portal BAR ou BARF) permitindo que outras singulares (unidades da Unimed) estabelecessem conexão remota via modem. A Figura 82 mostra o mapa de Santa Catarina com todas as singulares.

Figura 82 - Singulares da Unimed em Santa Catarina.

Para iniciar o processo de conexão com alguma singular, basta posicionar o ponteiro do mouse sobre o nome e dar um clique com o botão esquerdo. Será iniciado um *script* do programa de comunicação com o modem chamado *kermit* cuja saída é atualizada por uma CGI na página resultante (Figura 83).

Figura 83 - Estabelecendo conexão remota via modem.

A Figura 83 mostra o processo de conexão em andamento. A Figura 84 mostra uma conexão remota via modem estabelecida com sucesso. A partir desse momento o usuário conectou via modem a sua rede com a rede da outra singular permitindo o tráfego IP. Selecionando o botão *Continuar* permite o administrador continuar executando qualquer atividade de gerenciamento da máquina.

Figura 84 - Conexão remota via modem estabelecida.

Para interromper a conexão, a página principal do Gerenciamento Nível 1 do Portal BARF contém uma ação apropriada. O processo para desconectar procura o PID do processo *slattach* referente a conexão e envia um sinal de parada.

3.4 Gerenciamento Nível 2: Gerenciando os Recursos

O Gerenciamento Nível 2 concentra as atividades que são realizadas com menor frequência como as de configuração de rede, cópias de segurança do sistema e testes de conectividade.

O acesso ao Gerenciamento Nível 2 é obtido através da URL:

http://<máquina>/sistemas/

como usuário *sistemas*. A janela para autenticação do usuário é igual ao Gerenciamento Nível 1 (Figura 11).

A Figura 85 mostra as ações que podem ser executadas. Elas serão discutidas em detalhe nas seções seguintes.

Figura 85 – Página principal do Gerenciamento Nível 2

As CGIs do Gerenciamento Nível 2 fica no diretório *sistemas/cgi-sistemas* com o controle de acesso igual aos da página do diretório *sistemas*.

3.4.1 Alterar Senha de Acesso do GN2

Essa ação permite a troca da senha de acesso ao Gerenciamento Nível 2 do usuário *sistemas* (Figura 86).

Figura 86 - Alterando senha do Gerenciamento Nível 2

O procedimento de troca de senha é análogo ao da seção 3.3.8. É utilizado o aplicativo `/usr/local/etc/apache/support/encrypta` para encriptar as senhas e uma vez validada a senha antiga, o par `sistemas` e senha nova encriptada é arquivado em `/usr/local/etc/apache/support/password.sistemas` (Código 52).

```
sistemas:GsETwa94kfa
```

Código 52 - Arquivo `support/password.sistemas`.

3.4.2 Alterar Senha de Acesso do GN1

A ação executada é a de alterar a senha de acesso ao Gerenciamento Nível 1 do usuário `root`. A rotina de alteração é idêntica a da seção 3.3.8 (Figura 78) exceto pelo fato de não ser solicitado a senha antiga (Código 53).

Código 53 - Alteração da senha de acesso ao Gerenciamento Nível 1.

O Gerenciamento Nível 2 é hierarquicamente superior ao Gerenciamento Nível 1, portanto não há a necessidade de autenticar a senha deste último.

3.4.3 Backup com envio via FTP

Essa atividade realiza uma cópia (*backup*) do sistema e a envia por FTP para a conta de um usuário em outra máquina. A Figura 87 mostra os dados necessários para que se dê início ao processo:

Figura 87 - Parâmetros da máquina remota para backup.

IP da máquina: deve-se entrar o número IP da máquina para onde será enviado o *backup*.

username: nome da conta do usuário onde o *backup* será armazenado.

senha: senha pessoal do usuário na máquina onde o *backup* será armazenado.

Uma mensagem de alerta sobre a demora do processo de compactação é gerado ao usuário (Figura 88). Ao confirmar, o processo tem início. Antes que o processo de compactação dos arquivos seja iniciado é feito três tentativas de conexão a máquina onde será armazenado com o nome do usuário e a senha. O Código 54 mostra a porção do código que testa a conexão e a conta.

Figura 88 - Aviso sobre tempo de duração do *backup*.

```
if (&ftp::open($IPNumber,"21","5","3") != 1) {  
    &Print_ERRO5($IPNumber,$Username);  
    &ftp::close;  
}  
if (&ftp::login($Username,$Password) != 1 ) {  
    &Print_ERRO6($IPNumber,$Username);  
    &ftp::close;  
};
```

Código 54 - Testando parâmetros da máquina remota.

Se a máquina não responder (Figura 89) ou a dupla usuário e senha não forem corretas (Figura 90), uma mensagem de aviso será mostrada.

Figura 89 - Máquina remota não responde.

Figura 90 - Nome ou senha na máquina remota estão incorretos.

Caso a conexão possa ser estabelecida e a dupla, conta e senha, sejam válidas, inicia-se o processo de *backup*. O arquivo de *backup* é gerado no diretório */Backup/backup/* Com o nome *backup-<IP máquina>-.tar.gz*

Finalizado a compactação dos arquivos é enviado para a máquina destino em 3 tentativas. A Figura 91 mostra um *backup* realizado com sucesso.

Figura 91 - Processo de backup terminado com sucesso.

Caso ocorra alguma falha durante o processo de compactação dos arquivos ou envio do arquivo até a máquina destino, será mostrado uma tela de aviso. O Código 55 transfere o arquivo para a máquina destino e testa se ocorreu erro.

```
if ( &ftp::put($BACKUP_TAR_GZ,$RBACKUP_TAR_GZ) == 1 ) {  
    $Status=$Status."\nEnvio: Ok";  
}  
else { $Status=$Status."\nEnvio: Erro"; }
```

Código 55 - Envio via *ftp* do *backup*.

3.4.4 Backup com armazenagem em disco

Essa atividade realiza a cópia dos arquivos do sistema (*backup*) e o armazena no diretório */Backup/*. A Figura 92 mostra o aviso de que a operação pode ser demorada e solicita confirmação para o início da execução. O processo de *backup* é similar ao da seção 3.4.3 exceto pelo fato de não haver o envio via *ftp* do arquivo gerado.

Figura 92 - Aviso sobre a duração do processo de *backup*.

O aviso é gerado através de um código escrito em JavaScript (Código 56) inserido no código HTML da página.

```
<LI><A HREF="/cgi-sistemas/backup.pl" onClick="alert('\n  
Aten&ccedil;&atilde;o!\n\nDentro de alguns minutos o backup  
estar&aacute; pronto e uma nova p&aacute;gina ser&aacute;  
mostrada.\n\n                    Enquanto isso apenas o  
&aacute;cone de espera estar&aacute; vis&aacute;vel.\n') ">Backup com armazenagem em disco</A></LI><p>
```

Código 56 - Código *JavaScript* que gera o aviso.

Sendo a operação confirmada e o *backup* terminado corretamente, o usuário é avisado através da Figura 93

Figura 93 - Aviso de término do processo de *backup*.

O arquivo é gerado no diretório */Backup/* com o nome ***Backup-<IP máquina>.tar.gz***

3.4.5 Restaurar Backup

Essa ação permite restaurar um arquivo de *backup* presente no diretório */Backup/* com o nome *backup.tar.gz*. Ao selecionar essa opção, uma mensagem de aviso sobre a duração do processo é emitida (Figura 92). Antes de executar a descompactação é realizado um teste de integridade do arquivo. Se não houver nenhum erro o arquivo é descompactado e um aviso é emitido (Figura 94).

Figura 94 - Processo de restauração do *backup* finalizado com sucesso.

```
` ${TAR} zxfC ${BACKUP_TAR_GZ} ${RESTORE_DIR} > ${BACKUP_LOG};
```

Código 57 - Chamada de sistema para restaurar *backup*.

O Código 57 mostra a porção do código que executa a chamada de sistema que executa a restauração do backup.

3.4.6 Rede - Alterar nome, endereço IP, roteador e máscara

Essa atividade é certamente a ação mais sensível a ser executada na máquina. Sendo todo o nosso sistema executado via navegador através da rede, uma configuração errada nesse ponto pode comprometer o acesso ao sistema.

É possível configurar:

- número IP e máscara de rede da placa conectada à rede pública.
- número IP e máscara de rede da placa conectada à rede privativa.
- nome da máquina.
- roteador de saída.

Na porção superior da página de configuração da rede (Figura 95) é apresentado a configuração atual (ativa) da máquina.

Figura 95 - Configuração ativa da rede.

[illegible]

Figura 96 - Alterando configuração de rede.

A parte inferior da página de configuração (Figura 96) permite a alteração da configuração da máquina. Todos os campos do formulário já estão preenchidos com as informações da configuração atual. Alterações realizadas na configuração deverão ser ativadas através do botão *Configurar* que executará um código responsável pela atualização das informações nos arquivos necessários. Os arquivos alterados são: */total/rc.conf_total* (Código 58) e o arquivo de configuração do servidor *HTTP*. O Código 60 mostra uma porção do código que realiza parte das alterações nos arquivos de configuração da rede e do servidor de *HTTP*. Detecções de erro de número IP e máscara de rede são realizadas, como nas seções anteriores, e uma mensagem de erro é mostrada (Figura 97).

```
#!/bin/sh
/sbin/ifconfig ed0 inet 143.107.228.49 netmask
255.255.255.192
```

```
/sbin/route add default 143.107.228.2  
/bin/hostname rapper.ifqsc.sc.usp.br
```

Código 58 - Arquivo de inicialização da rede.

```
ServerAdmin webmastr@rapper.ifqsc.sc.usp.br  
ServerName rapper.ifqsc.sc.usp.br
```

Código 59 - Arquivo de configuração do servidor *HTTP*.

```
print "<p><pre>Alterando o nome do <b>Portal</b>: ",  
&ChangeValue( $RC_TOTAL_CONF, "$HOSTNAME", $query->  
param('hostname')), "\n";  
  
# Placa 1  
if ( $query->param('ipnumber') eq "NO" || $query->  
>param('netmask') eq "NO") {  
    $NewIP = "\"\""; }  
else {  
    $NewIP= " ed0 inet ".$query->param('ipnumber')."  
netmask ".$query->param('netmask'); }  
print "Alterando número IP : ",  
&ChangeValue( $RC_TOTAL_CONF, "ed0", $NewIP), "\n";  
.....  
&ChangeConfCommand ( "ServerAdmin", $HTTPDCONF, $ServerAdmin  
);  
    &ChangeConfCommand ( "ServerName", $HTTPDCONF, $Hostname  
);
```

Código 60 - Realizando alterações nos arquivos de configuração de rede e do servidor de *HTTP*.

Figura 97 - Número IP digitado incorreto.

Entretanto, as alterações não são ativadas. Para que essas modificações tenham efeito é necessário que a máquina seja reiniciada. A Figura 98 mostra o status das alterações nos arquivos.

Figura 98 - Rede configurada com sucesso.

Para ativar as alterações é necessário reiniciar a máquina através do botão *Reinicializar*. Após aproximadamente um minuto a reinicialização é finalizada ativando as alterações com a máquina passando a responder com os novos valores.

3.4.7 Ping

Os comandos *ping* e *traceroute* (seção 3.4.8) compõem as duas ações para teste de conectividade da máquina com outras ligadas na rede. O comando *ping* envia uma mensagem *ICMP echo request* para a máquina destino que responde com uma mensagem *ICMP echo reply*. Ambas as mensagens trafegam em datagramas IP permitindo confirmar que:

- i) o software IP da máquina de origem consegue rotear o datagrama.
- ii) os roteadores, caso haja, entre a máquina de origem e a de destino estão funcionando e são capazes de rotear o datagrama.
- iii) a máquina destino está respondendo e os softwares de *ICMP* e IP estão funcionando.

A Figura 99 mostra as informações a serem fornecidas:

IP/Nome da máquina destino que se deseja testar a conectividade.

quantidade de pacotes contendo ICMP *echo request* a serem enviados.

tamanho da mensagem contida em cada pacote enviado.

Figura 99 - Testando conectividade via *ping*.

O resultado obtido é mostrado na Figura 100 com informações de:

tempo de resposta a cada porção da sequência.

quantidade de pacotes recebidos.

porcentagem de pacotes perdidos.

menor tempo de resposta

maior tempo de resposta.

tempo médio de resposta.
desvio padrão do tempo de resposta

Figura 100 - Resultado do ping.

Caso seja entrado o nome de uma máquina para testar e o servidor *DNS* não foi capaz de resolver, é mostrado uma mensagem de aviso (Figura 101). O Código 61 mostra a porção do código que executa a chamado de sistema para executar o comando *ping*. O resultado é enviado para a subrotina responsável pela formatação.

Figura 101 - Não foi possível resolver o nome da máquina.

```
$Output=`${PING} -c ${Count} -s ${Size} ${Host}`;  
$Output = "<dd>N&atilde;o foi poss&iacute;vel resolver o  
nome <i>${Host}</i>.<p>\n" if ! $Output;  
&Print_Resultado($Output);
```

Código 61 - Chamada de sistema do comando ping.

3.4.8 Traceroute

O comando *traceroute* é a segunda ação do teste de conectividade da máquina com as demais conectadas à rede. É possível traçar o caminho percorrido pelo pacote até a máquina destino através dos roteadores intermediários. A técnica empregada pelo comando *traceroute* é a de enviar uma sequência de pacotes contento *Time-To-Live* (*TTL*) crescente (1, 2, 3, ...) e usar as mensagens de *ICMP time exceeded* retornadas pelos roteadores.

A Figura 102 pede ao usuário para indicar o número IP ou nome da máquina destino.

Figura 102 - Especificando máquina para executar *traceroute*.

Selecionando o botão *Iniciar Traceroute* o comando é executado através de uma chamada *system* (Código 62).

```
$Output=`${TRACEROUTE} ${TRACEROUTE_ARGS} ${Host}`;  
if(!$Output) { $Output = "<dd>Erro. Use o endereço mero IP em  
vez do nome da máquina e tente novamente.<p>\n" }  
&Print_Resultado($Host,$Output);
```

Código 62 - Chamada de sistema do comando *traceroute*.

A resposta é apresentada contendo o trajeto dos pacotes até a máquina destino através dos roteadores intermediários (Figura 103)

Figura 103 - Resultado do comando *traceroute*.

Caso o usuário entre com o nome da máquina e o servidor de nomes não for capaz de resolvê-lo, uma mensagem de erro é devolvida (Figura 104).

Figura 104 - Nome de máquina inválido.

4. Análise Comparativa

Análise comparativa do MSP contra outros pacotes.

4.1 Esse pacote tem duas características importantes

O desenvolvimento do projeto teve como preocupação dois tópicos:

1. decisões de design.
2. segurança.

Para desenvolver o pacote levou-se em consideração quais tipos de serviços seriam disponibilizados e quais atividades seriam necessárias. Definido os serviços, as atividades relacionadas foram agrupadas de forma a prover uma coerente seqüência de gerenciamento. Os comandos necessários para executar as diversas atividades deveriam ser de fácil acesso. Para garantir o acesso rápido e fácil foi necessário cuidados especiais com a navegação. Durante a execução de qualquer atividade a navegação permitia retroceder ao início ou cancelar a atividade corrente. Dessa forma, toda atividade somente é concluída na última etapa da navegação quando todos os comandos são realmente executados no sistema. Assim, embora tenha-se navegado por toda as opções da atividade a execução pode ser cancelada sem que haja qualquer alteração no estado ativo do sistema. A alteração somente será executada com a confirmação na última etapa.

Outro detalhe de design considerado foi a escolha de quais serviços seriam disponibilizados em cada sistema. O Capítulo 3 descreve os vários tipos de sistemas e o conteúdo de cada um. A escolha de quais serviços seriam disponibilizados deveria se basear na menor quantidade de atividades possíveis, mas necessárias, sem

que houvesse comprometimento do gerenciamento. Essa preocupação foi a base para definir os tipos de sistemas.

A segurança foi outra preocupação para o desenvolvimento do projeto. O sistema deveria conter as atividades necessárias para um completo e correto gerenciamento de serviços. As atividades de gerenciamento de um sistema como o pretendido é de veras complexo e exige conhecimento. O projeto deveria então prover um meio de gerenciar o sistema sem a exigência previa de tal conhecimento. Para atingir essa meta, o sistema possui uma configuração prévia que deveria funcionar sempre. Essa configuração prévia deveria ser restaurada sempre que necessária, permitindo que durante o gerenciamento servisse de base para as alterações sendo executadas. Outro requisito é disponibilizar apenas as opções básicas para realizar as atividades. Uma característica intrínseca poderosa do Unix é a versatilidade na configuração que se torna altamente perigosa quando executada incorretamente. Para eliminar esse perigo, as opções completas para a execução da atividade são calculadas a partir dos dados entrado ou obtidas após uma pesquisa no sistema.

Esses dois fatores orientaram a filosofia do projeto que seria gerenciar uma rede IP com segurança por qualquer pessoa.

4.2 Qualquer pessoa gerencia

Implementar o projeto elaborado com base no gerenciamento do sistema por qualquer pessoa, requereu que uma série de recursos não ficassem disponíveis. Outros recursos por sua vez tiveram parte de suas funcionalidades não disponibilizadas.

Para a remoção das funcionalidades primeiramente selecionamos aquelas relacionadas com a instalação do sistemas operacional. Recursos para formatação de

discos e criação de *label* são utilizados apenas uma vez durante a instalação do sistema na máquina ou num posterior acréscimo de disco rígido. Na sequência vem a criação ou alteração de partições. Essas são atividades que exigem um alto grau de conhecimento de hardware, características e política de gerenciamento do sistema operacional e experiência para definição da árvore de diretórios.

Outro detalhe mascarado para o usuário é a estrutura de diretórios. Não é permitido ao usuário definir a localização dos diretórios de recursos como servidor de FTP ou WWW. O usuário durante a manutenção tem a impressão que está manuseando arquivos na raiz do sistema. Para garantir que não houvesse formas de fugir ou quebrar essa regra foi utilizado na programação um recurso do sistema chamado *chroot*.

Das várias atividades disponíveis todas tiveram suas funcionalidades alteradas ou diminuídas. Para a manutenção das contas de usuários não é necessário que haja a possibilidade de alteração do tipo de interpretador de comandos (*shell*), por exemplo.

O padrão para essas configurações foi definido durante o projeto devendo ser igual para todos os usuários. Um desses padrões, por exemplo, é a não disponibilização de um interpretador de comandos para o usuário. Dessa forma não é possível ao usuário estabelecer uma sessão remota (*telnet*) na máquina. Essa regra exigiu que o código do servidor de arquivos (*ftp*) fosse alterado e recompilado. O recurso de *chroot* também foi alterado no código do servidor de arquivos fazendo com que o usuário durante uma sessão de transferência de arquivos somente visualize sua árvore de diretórios. Esse recurso poderia originalmente ser alterado através de arquivos de configuração, entretanto devido a imaturidade do recurso na versão implantada preferiu-se que fosse feito diretamente no código.

O servidor de WWW também teve poucas opções de configuração disponíveis para alteração. A maioria das opções foram pré configuradas durante a instalação do sistema. O servidor DNS também teve a maioria das opções de configuração mascaradas. É permitido ao usuário apenas informar o nome e número IP das máquinas, mas em quais arquivos ou como ocorrerá a modificação desses arquivos, fica totalmente bloqueada.

Dessa forma impedimos que o usuário comprometa o funcionamento da máquina.

4.3 Gerencia IP

O projeto foi concebido para poder gerenciar uma rede IP com os recursos básicos necessários. Ele se assemelha aos recursos providos por um provedor de **acesso** a Internet. Para que seja possível, algumas características são essenciais. Essas características são encontradas no sistema operacional Unix desenvolvido pela Universidade de Berkeley, o FreeBSD. De todos os recursos disponíveis pelo FreeBSD, foi selecionado apenas o mínimo necessário seguindo as regras do projeto como discutido na seção 4.2.

A primeira característica é a possibilidade de configurar as placas de rede da máquina com números IP, nome, máscara de rede e roteamento padrão. Dessa forma, podemos colocar a máquina em qualquer rede IP de computadores.

Alguns serviços foram disponibilizados possibilitando que estações clientes, por exemplo computadores rodando o Windows 95, tenha acesso a recursos da Internet ou somente da Intranet. O serviço de roteamento está disponível permitindo a configuração da máquina como roteador de diversas redes. As redes podem estar conectadas a máquina através das placas de rede ou pelos modems conectados na

placa multiseriada. Em uma das interfaces podemos ter a conexão com a Internet e nas demais, conexão com outras redes privadas interligando-se a Intranet.

Para o funcionamento eficaz dos recursos Internet ou Intranet faz-se necessário a configuração do serviço de DNS. O servidor de DNS está disponível podendo ser configurado para prover resolução de nomes da classe pública de IP, permitindo o acesso aos recursos da Internet. Também é possível configurá-lo para que faça a resolução de nomes da classe privada de IP da Intranet. Nesse caso somente as máquinas clientes conectadas na classe privada tem acesso a esse serviço.

Por último, temos o recurso de acesso via modem. Esse acesso permite que o usuário de posse de um computador com modem se conecte via linha telefônica à rede de computadores. O projeto prevê que a autenticação da senha de acesso seja feita em uma máquina que possua o servidor de autenticação *radius*. Através dessa conexão via modem, a máquina cliente passa a fazer parte da rede privada com a possibilidade de usufruir de todos os recursos disponíveis.

Todos esses recursos estão disponíveis no FreeBSD.

4.4 Aplicação – UniRed Santa Catarina

Não é possível avaliar um sistema complexo como o do MSP apenas em laboratório. É necessário um teste mais amplo onde toda a sua capacidade pode ser realmente aproveitada e explorada. O teste de campo foi realizado com a implantação do projeto da UniRed. A UniRed é a intranet das Unimed de Santa Catarina. A Unimed de cada cidade é designada singular e responde para a Federação localizada em Joinville. A idéia da UniRed foi interligar as singulares de Santa Catarina à Federação em Joinville através de linhas telefônicas dedicadas e discadas. A Federação por sua vez possui uma linha dedicada com a Confederação na cidade de

São Paulo. Dessa forma criou-se uma rede de computadores distribuída por todo o estado de Santa Catarina interligada com São Paulo. Em São Paulo, a Confederação possuía ligações com outras singulares espalhadas pelo país. Em cada singular de Santa Catarina foi colocado uma (1) ou mais máquinas com o MSP e uma pessoa foi treinada na utilização das atividades. Como descrito na seção 3.1, dependendo das necessidades e custos, foram instaladas as máquinas. A Figura 105 mostra todas as singulares com o tipo de ligação telefônica à Federação.

Figura 105 – Interligação da singulares à Federação

As singulares de Florianópolis, Joinville e Blumenau se conectaram à Federação em Joinville através de linhas telefônicas dedicada. As demais singulares se conectaram utilizando linhas telefônicas discadas. As singulares com linha discada utilizavam-se da atividade descrita na seção 3.3.10 para se conectar à Federação. Cada singular possuía uma conta na Federação que era autenticada pelo Portal R. Autenticado o par nome e senha, a conexão era estabelecida e a singular recebia um número IP

passando a fazer parte da UniRed. Assim, era possível a qualquer máquina cliente da singular utilizar os recursos da UniRed e da Internet. Dentre os recursos disponíveis, os mais utilizados eram *ftp* para transferência de dados da cooperativa e correio eletrônico para comunicação entre os funcionários. Para que não houvesse uma demora muito grande na troca de mensagens eletrônicas, estabeleceu-se que cada singular com linha discada se conectaria à Federação no mínimo duas vezes ao dia, pela manhã e a tarde.

A UniRed de Santa Catarina funcionou utilizando computadores com o MSP, um *kernel* modificado do FreeBSD e alguns outros recursos desenvolvidos pela empresa Total Informática por aproximadamente dois anos. Nos meses seguintes, por motivos políticos internos à direção da Unimed, parte da UniRed foi desligada. Algumas singulares deixaram de utilizar os Portais. Entretanto, algumas singulares ainda utilizam o equipamento.

É importante notar que em nenhuma singular havia um técnico em informática com conhecimentos de Unix ou rede de computadores que utilizassem o protocolo TCP/IP.

5. Trabalhos futuros.

O MSP é um projeto que se mostrou ser robusto, de fácil manuseio e confiável para gerenciar um rede IP heterogênea como a UniRed das Unimeds de Santa Catarina. Entretanto, como todo software necessita de constantes aprimoramentos e acréscimos de funcionalidades. Dentro dessas necessidades três pontos são importantes de serem destacados: compilação, recodificação e acréscimo de funcionalidades.

O MSP utiliza-se em sua grande parte de programas codificados em linguagem Perl. O Perl, como descrito na seção 3.2.4 é uma linguagem interpretada. Atualmente há a possibilidade de se gerar código executável em Perl. A compilação possibilitaria um acréscimo de segurança dos programas. Por ser interpretado, é possível que o arquivo contendo o programa seja alterado facilmente também pode ser roubado para reutilização indevida. A compilação eliminaria esses problemas dificultando em muito a ação por parte de pessoas não autorizadas. Deve-se acrescentar que uma vez compilado, os programas ganham mais estabilidade. Entretanto, a compilação cria problemas de portabilidade pois o código gerado é específico para o sistema aonde foi compilado. Por vezes, específico para a arquitetura da máquina.

A portabilidade é algo que pode ser mantido com uma recodificação dos programas em Java, uma linguagem criada especialmente para atender essas necessidades. Durante a criação do MSP a linguagem Java ainda estava se iniciando portanto não foi considerada. Atualmente, há diversas vantagens em se usar essa linguagem. Outra opção para recodificação é a linguagem C ou C++. As vantagens de se gerar códigos a partir dessas linguagens são enormes, destacando-se a segurança, confiabilidade e rapidez. Novamente, cria-se o problema de portabilidade. O MSP deve ser compilado na plataforma a ser instalado.

O MSP atende as necessidades de gerenciamento de uma rede IP, entretanto algumas atividades podem ser melhoradas, acrescentadas ou atualizadas. Algumas atividades do MSP poderiam ter a sua interface modificada tornando mais fácil ou atualizada. Um exemplo é a atividade de manutenção dos arquivos do servidor WWW e FTP. A atividade de gerenciamento do banco de modems pode parecer um pouco confusa podendo ser melhorada. Relacionado com o banco de modems, o programa *ppp* contempla atualmente alguns recursos novos. Dentro desses novos recursos se destaca a operação *on demand* para conexões discadas. Esse recurso consiste em fazer o modem discar automaticamente sempre que houver a necessidade de algum pacote TCP/IP ser enviado pela saída serial. Dessa forma não haveria mais a necessidade da atividade descrita na seção 3.3.10. O programa *ppp* também acrescentou outros recursos quando utilizado como servidor de *dial-in* que poderiam estar disponíveis, como por exemplo configuração automática de servidor DNS. Esses são exemplos de novos recursos acrescentados em programas antigos que durante a criação do MSP não estavam disponíveis ou estáveis.

Outra sugestão para acrescentar no MSP são rotinas de teste para a configuração da rede utilizando a linguagem JavaScript. Atualmente o JavaScript permite que os valores digitados nos campos dos formulários sejam testados antes de serem enviados. Podemos então avisar o usuário, por exemplo, que o número IP digitado contém um caracter ilegal antes que seja apresentado a próxima página. Caso o usuário queira, uma nova janela com o navegador pode ser aberta contendo um ajuda para resolver dúvidas quanto ao problema.

Duas funcionalidades a serem acrescentadas no MSP são de monitorização da rede e agentes. A monitorização em tempo real é uma ferramenta necessária para o usuário:

- ter conhecimento do que está acontecendo com o tráfego da rede.
- do conteúdo que está trafegando na rede.
- controle do que está trafegando na rede.
- poder melhorar a qualidade do tráfego na rede.

Algumas ferramentas gratuitas estão disponíveis na Internet para utilização. O site CAIDA (<http://www.caida.org>) se especializou em prover informações sobre ferramentas de monitorização de rede. O MSP pode ser uma máscara para programas de análise do tráfego da rede em roteadores como o MRTG (<http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html>).

Como acontece com todo software, o MSP pode ter suas atividades melhoradas ou ampliadas. Mas cada nova funcionalidade a se acrescentada no MSP deve ser norteadada pelo objetivo descrito na seção 4.1.

6. Bibliografia

Bach, Maurice J. (1993). *The Design of the UNIX Operating System*.

Cheswich, W.; Bellovin, S. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, Reading, Massachusetts.

Comer, Douglas E. (1995). *Internetworking with TCP/IP*. Prentice Hall, Vol 1, 3 ed.

Comer, Douglas E. (1995). *Internetworking with TCP/IP*. Prentice Hall, Vol 2, 3 ed.

Comer, Douglas E. (1995). *Internetworking with TCP/IP*. Prentice Hall, Vol 3, 3 ed.

Corcoran, Cate T. (1996). *Managing Network ills*. INFO World, Volume 18, Issue 42, Outubro 1996.

Glover, Mike; Humphreys, Aidan; Weiss, Ed (1996). *Perl 5 How-To – The Definitve Perl Programming Problem-solver*. Waite Group Press.

GREG L. SATZ DE (1992). *A New View on Bulk Retrieval with SNMP*. Simple Times, Vol 1, Number 1, March/April 1992.

Lantronix Whitepaper (1996). *Using RMON to Manage Today's Switched Network Segments*.

Layland, Robin (1995). *Net Management Platforms: Time to Get Real*. Data Communications, Setembro 1995.

McCarthy, Vance (1997). *Use The Web To Manage Your Network*. Datamation, Janeiro 1997

Pappas, Chris H.; Murray, Willian H. (1994). *Borland C++ 4.0*. Makron, McGraw-Hill Books.

Perkins, David T. (1992). *Standards*. Simple Times, Vol 1, Number 1, March/April 1992.

Quillin, Robert (George Washington University) (1993). *The Integration of Network and System Management*. Telecommunications, Agosto 1993.

Schildt, H. (1990). *C Completo e Total*. Makron, McGraw-Hill Books.

Steven L. Waldbusser (1992). *Applications and Directions – Exposing the Myths about Autotopoly*. Simple Times, Vol 1, Number 1, March/April 1992.

Stewart, Robert L. (1992). *Working Group Synopses*. Simple Times, Vol 1, Number 1, March/April 1992.

Tittel, Ed; Gaither, Mark; Hassinger, Sebastian; Erwin, Mike (1996). *Web Programming Secrets with HTML, CGI and Perl*. IDG Books Worldwide, 1996.

Waldbusser, Steve (Carnegie-Mellon University); **Nair, Mohan** (Protocols Inc.); **Hoerth, Mark** (Hewlett-Packard Co) (1992). *SNMP Management Goes Down to the Wire*. Data Communications, Maio 1992.