



POP IN A BOX

Guia de Montagem de Pontos de Acesso à Internet
Versão preliminar

Sumário

| | |
|---|-----|
| Prefácio | 2 |
| O Projeto POP-IN-A-BOX | 3 |
| 1. Introdução à Internet | 5 |
| 2. Introdução às Redes | 7 |
| 3. O modelo OSI e o Protocolo TCP/IP | 10 |
| 4. Introdução às Redes Locais e de Longa Distância | 11 |
| 5. Roteamento | 15 |
| 6. Abrindo o POP-IN-A-BOX | 19 |
| 7. Conhecendo e Instalando o Sistema Operacional FreeBSD | 25 |
| 8. Montando o POP-IN-A-BOX | 32 |
| 9. Configurando o Serviço de Nomes (DNS) | 38 |
| 10. Serviços de Correio Eletrônico (SMTP e POP) | 45 |
| 11. Conhecendo e Instalando o Servidor WWW Apache | 48 |
| 12. Configurando o Serviço FTP | 50 |
| 13. Instalando o Servidor de Comunicações | 53 |
| 14. Considerações Finais | 65 |
| Anexo A: Obtendo os <i>Software</i> Utilizados | 66 |
| Anexo B: Comandos Básicos do FreeBSD | 67 |
| Anexo C: Configurações Suportadas pelo FreeBSD | 69 |
| Anexo D: Aspectos sobre Segurança | 71 |
| Anexo E: Configurando a Rede TCP/IP | 79 |
| Anexo F: Configurações Avançadas e Problemas mais Comuns | 83 |
| Anexo G: Glossário | 88 |
| Índice Remissivo | 99 |
| Anexo Avulso: Quanto Custa e Como Adquirir o POP-IN-A-BOX | 100 |

Prefácio

Caro leitor,

A Rede Nacional de Pesquisa – RNP – é um Programa Prioritário do Ministério da Ciência e Tecnologia – MCT, executado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, cuja missão básica é planejar e conduzir ações que assegurem a implantação e evolução de redes Internet no Brasil.

Em 1991, a RNP introduziu a tecnologia Internet no Brasil e vem desempenhando, desde então, um papel de destaque na implantação de um sólido backbone interligando todos os estados brasileiros, na disseminação de serviços e aplicações de rede em todo o país e na capacitação de recursos humanos na área de redes.

O POP-IN-A-BOX¹ é mais uma importante realização da RNP que tem por objetivo capacitar instituições a montar o seu próprio *ponto-de-acesso* à Internet. Buscamos reunir neste guia todas as informações necessárias para que empresas, escolas, bibliotecas, ou até mesmo profissionais autônomos, possam expandir sua presença na Internet, usufruindo da rede não só como usuários, mas também como provedores de serviços.

Assim, desejamos, com a elaboração e difusão deste material, popularizar e facilitar o provimento de serviços Internet no Brasil. Agindo desta forma, a RNP mantém sua função primordial de disseminação do uso de tecnologias de rede Internet no país.

José Luiz Ribeiro Filho
Coordenador RNP

¹ Na Internet, a expressão POP significa *ponto-de-presença*, ou seja um nó da rede onde estão disponíveis interconexão para comunicação global e vários outros serviços.

O Projeto POP-IN-A-BOX

O que é?

O projeto POP-IN-A-BOX, desenvolvido pela Rede Nacional de Pesquisa - RNP, tem por objetivo criar uma solução de software e hardware para a montagem de um servidor simplificado, onde os operadores possam estabelecer e manter serviços Internet, através de uma conexão permanente à rede.

Entre estes serviços, podemos destacar: acesso à Internet, servidor para abrigar páginas de homepage, arquivos, documentos, gerar listas de discussão, etc...

Procuramos viabilizar uma solução eficiente, e ao mesmo tempo com o menor custo possível, para que qualquer instituição (principalmente, pequenas e médias), tais como escolas, empresas, organizações governamentais e não-governamentais, possam montar seu próprio servidor.

A instituição terá que comprar um computador Pentium 100 (ver especificação abaixo) e utilizar o CD fornecido pela RNP.

Assim, seguindo passo-a-passo as informações do guia de instalação será possível montar o seu próprio ponto de acesso à Rede, ou POP-IN-A-BOX

Perfil do operador para montar o KIT

Recomendamos que os operadores que irão montar este KIT seja estudantes de últimos períodos de cursos de informática do terceiro grau e que tenham:

- a) experiência de montagem de microcomputadores;
- b) instalação de programas em computadores;
- c) uso avançado de Internet como usuário;
- d) noções de rede local e protocolos TCP/IP.

Componentes

O POP-IN-A-BOX é constituído pelo guia e um CD com todas as informações sobre *software*, *hardware*, procedimentos para instalação e configuração de serviços básicos da Internet, bem como formas de obtenção de equipamentos e custos envolvidos.

O guia aborda os vários serviços que você poderá utilizar, como o Web, correio eletrônico, listas de discussão, compartilhamento de arquivos, etc. Ele também fornece dicas importantes sobre várias outras facilidades e dispositivos, que apesar de não estarem presentes nesta versão, serão incorporados nas versões futuras.

Software

Através da utilização de *software* de domínio público, mas altamente consagrados e difundidos na Internet até mesmo em aplicações comerciais, este guia oferece uma solução de muito baixo custo para implementação de sua presença na rede. Por exemplo, utilizamos, como sistema operacional, o FreeBSD, que é uma versão gratuita do popular sistema Unix. Todos os software são fornecidos através de 01 CD-ROM POP-IN-A-BOX, da Rede Nacional de Pesquisa.

Hardware

Em relação ao *hardware*, já é suficiente que você disponha de um computador básico com processador Pentium 100 Mhz. A conexão física à Internet é realizada por uma placa adicional que você precisará adquirir para instalar no seu computador.

Em termos de *hardware* e *software*, o POP-IN-A-BOX constitui-se de um microcomputador com a seguinte configuração mínima:

- Pentium 100 MHz, 32 MB RAM, com:
 - 01 Placa SVGA 1MB;
 - 01 Disco Rígido de 2 GB;
 - 01 Unidade de CD-ROM;
 - 01 Unidade de Disco 1.44 MB;
 - 02 Portas Seriais e 01 Paralela;
 - 01 Placa Ethernet
 - 01 Bus Mouse
 - 01 Teclado;
 - 01 Placa Serial Síncrona ET-5025

Esperamos que este material atenda sua necessidade de estabelecer uma presença marcante na Internet e gostaríamos de ouvir suas sugestões e críticas através do endereço info@rnp.br. A RNP deseja ser a primeira a lhe dar boas-vindas à Internet!

As versão atualizada deste manual pode ser obtida em:

<http://www.rnp.br/produtos/popinabox.html>

Trabalharam neste projeto, em diferentes fases do seu desenvolvimento:

Adailton Silva
Alex Soares de Moura
Ana Carolina Murgel
André Valle e sua equipe da ACTECH
Antonio Forster
Claudine Bichara
Fábio Okamura
Gorgônio Araujo
Liliana V. Solha
Luciano Junqueira
Marcos de Castro Sylos
Mauro Pinheiro
Paloma de Almeida
Rodolfo Capeto

Capítulo 1

Introdução à Internet

Embora atualmente exista uma grande divulgação sobre assuntos e conceitos relacionados à Internet, provavelmente a maioria dos usuários ainda não entende exatamente o que é ou o que ela faz. Na verdade, a Internet revolucionou a utilização da Tecnologia da Informação e o mundo das comunicações através de sua incrível capacidade de integração de mídias.

O conceito inicial de Internet foi primeiro discutido por J. Licklider do MIT (*Massachusetts Institute of Technology* <<http://web.mit.edu>>), através de uma série de artigos, onde a idéia de uma Rede Galáctica era demonstrada. Foi vislumbrada uma rede global, onde todos poderiam rapidamente acessar dados e programas de qualquer computador. Também no MIT, Leonard Kleinrock publicou o primeiro artigo a respeito da teoria de comutação de pacotes em 1961, e um livro a respeito do assunto em 1965. Nesse mesmo ano, visando demonstrar a teoria de Kleinrock, Lawrence Roberts conseguiu interligar um computador TX-2 em Massachusetts a um Q-32 na Califórnia, utilizando uma linha discada de baixa velocidade.

Com o prosseguimento das pesquisas, em 1968 Roberts redefiniu o projeto da ARPANET², migrando a velocidade inicial do *backbone*³ de 2,4 a 50 kbps⁴. Em 1969, o laboratório de Kleinrock na UCLA (*University of California Los Angeles* <<http://www.ucla.edu>>) foi escolhido para funcionar como o primeiro nó⁵ da ARPANET, conectando-se em seguida a uma máquina na Universidade de Stanford. A partir desta interligação, foram mantidas as primeiras tabelas de nomes para endereçamento e enviadas as primeiras mensagens. Posteriormente, foram adicionados dois novos nós à rede, conectando as universidades de Santa Bárbara e Utah.

Nos anos seguintes, diversos novos computadores foram adicionados à ARPANET e vários *software* e protocolos de rede, como o NCP (*Network Control Protocol*), foram desenvolvidos. O ano de 1972 foi um marco no desenvolvimento da rede, com a primeira demonstração da ARPANET em uma conferência internacional de computação e com o desenvolvimento da primeira grande aplicação, o correio eletrônico.

As limitações do NCP levaram ao desenvolvimento de um novo protocolo de comunicações, o TCP/IP, adotado definitivamente em todas as máquinas da ARPANET em 1º de janeiro de 1983. Em 1985, o conceito de Internet como uma tecnologia de interconexão de diferentes sistemas já estava bem definido. Aplicações como o correio eletrônico já eram utilizadas diariamente por milhares de pessoas, tornando práticas as aplicações da rede.

Em 1985, foi iniciado o projeto NSFNET, da *National Science Foundation* (NSF), com o objetivo de interligar todas as universidades e centros de pesquisa americanos. A NSF passou, assim, a administrar a rede Internet existente. Foi estimulada a interligação de novas redes regionais e, posteriormente, a admissão de usuários não-acadêmicos. Proibindo o uso do seu *backbone* para fins comerciais, a NSF estimulou o aparecimento de *backbones* privados e, em 1995, teve o seu sistema totalmente desligado.

Atualmente (1998), a Internet é uma interligação de mais de 50.000 redes em todo o mundo, conectando mais de 50 milhões de usuários. A sua estrutura atual pode ser

² *Advanced Research Projects Agency Network*

³ Estrutura de nível mais alto em uma rede composta por várias sub-redes. Em português, espinha dorsal

⁴ KBites por segundo

⁵ Qualquer dispositivo, inclusive servidores e estações de trabalho, ligado a uma rede

considerada o protótipo da chamada Supervia da Informação, um projeto internacional de uma rede de alta capacidade que integrará praticamente todas as mídias existentes (Web⁶, TV, vídeo, fax, EDI⁷, etc).

Bibliografia

- Where Wizards Stay Up Late : The Origins of the Internet - Katie Hafnet, Matthew Lyon - Touchstone Books
- ISOC Internet History - <http://www.isoc.org/internet-history/>
- History of the Internet and WWW - <http://www.internetvalley.com/intval.html>

⁶ Sistema de localização e pesquisa de informações que permite o acesso, através de hiperlinks, a um número ilimitado de dados em escala mundial.

⁷ Electronic Data Interchange - Intercâmbio Eletrônico de Dados

Capítulo 2

Introdução às Redes

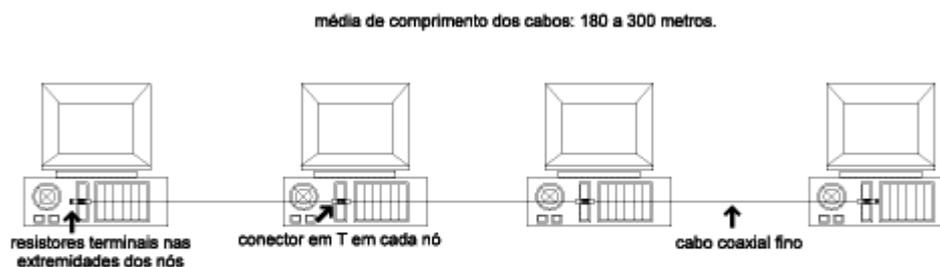
O objetivo deste capítulo é proporcionar noções básicas sobre redes de computadores. Conceitualmente, as redes são sistemas interativos para o transporte de informações, podendo cobrir áreas geográficas limitadas (redes locais) ou grandes extensões geográficas (redes de longa distância). As redes locais compreendem na maioria dos casos algumas dezenas de metros, enquanto que redes de longa distância, formadas por circuitos digitais de comunicação, podem cobrir distâncias até mesmo intercontinentais.

Independente de seu tamanho, uma rede de computadores segue uma determinada topologia, que caracteriza o seu lay-out físico e o meio de conexão dos seus dispositivos. Embora existam inúmeras topologias, as variações normalmente derivam de três tipos básicos mais freqüentemente empregados: as topologias em barramento, em anel e em estrela, que serão analisadas a seguir.

Nota: Os pontos no meio físico onde os dispositivos são conectados recebem a denominação de nós, e a estes estão associados endereços para que possam ser reconhecidos na rede.

Topologia em Barramento

Na Topologia em Barramento, todos os nós são conectados diretamente ao barramento de transporte, sendo que o sinal gerado por uma estação propaga-se em todas as direções ao longo do barramento, conforme a figura a seguir.

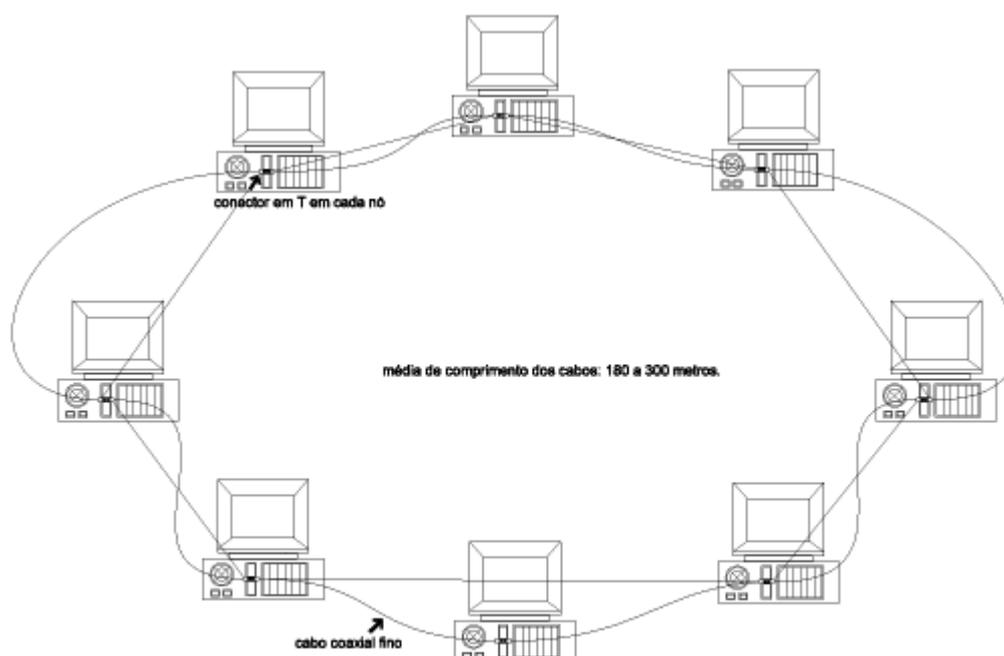


Topologia em Barramento

Topologia em Anel

Já a topologia em anel é caracterizada como um caminho unidirecional de transmissão, formando um círculo lógico sem um final definido. A estratégia de controle pode ser centralizada, através de uma controladora central, ou distribuída, controle em cada nó individual da rede.

O sinal originado por um nó passa por todo o anel, sendo que, em cada nó, é regenerado e retransmitido. Uma das vantagens desta topologia é a fácil detecção e isolamento de falhas ou interrupções no anel, já que o transmissor não recebe a confirmação da recepção da mensagem por ele enviada.

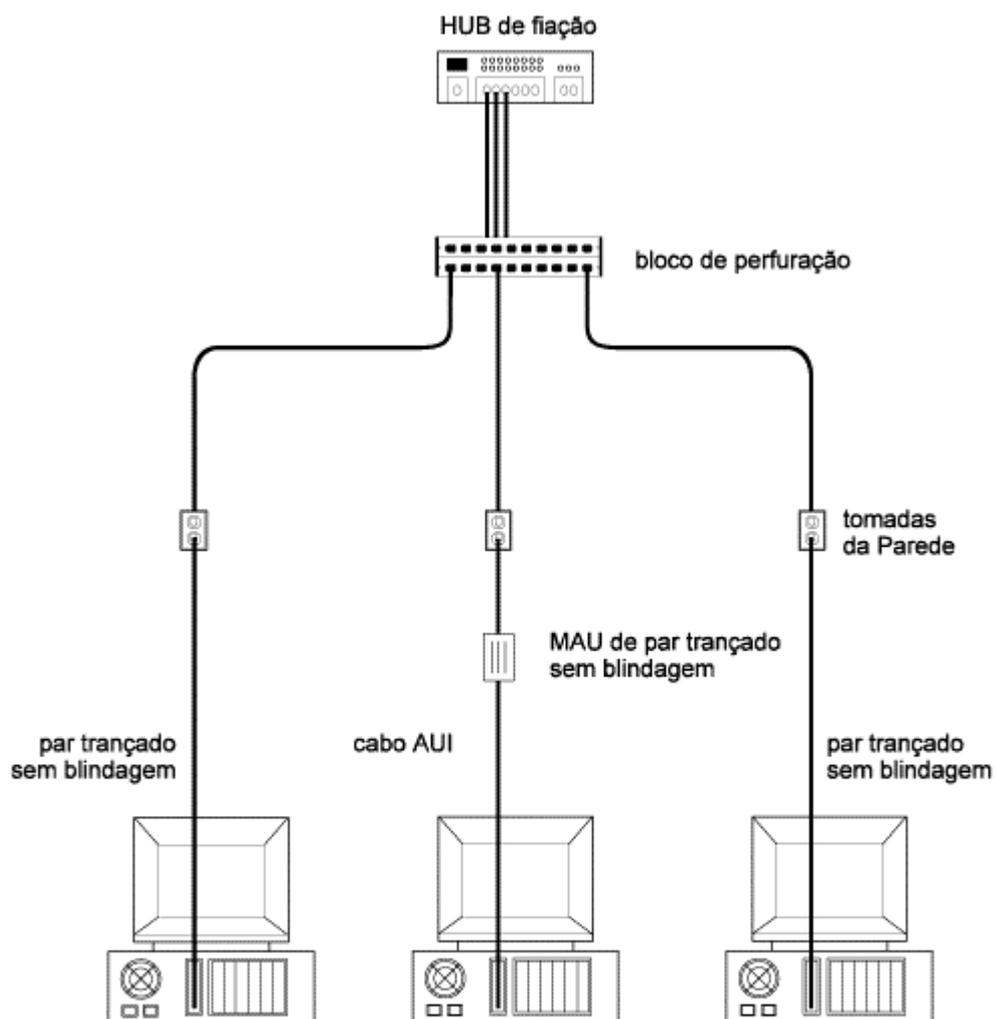


Topologia em Anel

Topologia em Estrela

A topologia em estrela é, sem dúvida, a mais utilizada atualmente. Sua principal característica é que todos os nós são conectados a um concentrador de comunicações, mais conhecido como *hub*.

O *hub*, que geralmente é microprocessado, controla todo o fluxo de informações da rede. Os modelos mais avançados possuem a capacidade de minimizar eventuais problemas da rede, através da duplicação de componentes críticos.



Topologia em Estrela

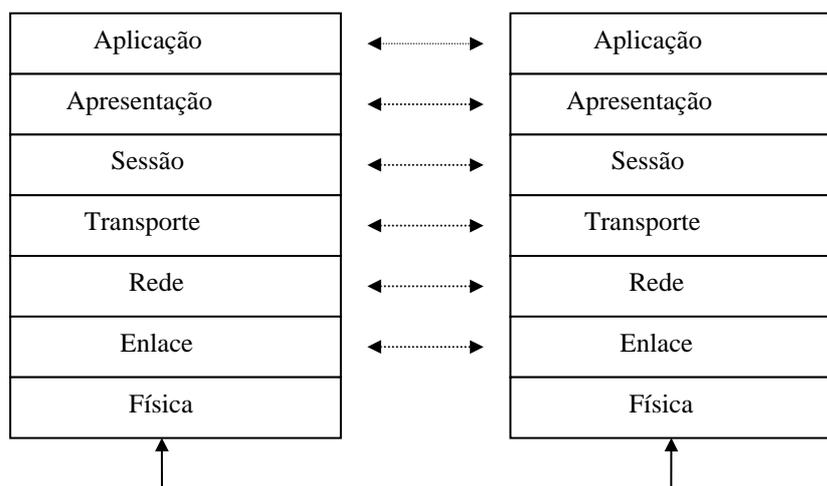
Bibliografia

- Guia de Conectividade - Frank J. Derfler, Jr. - Editora Campus, 1993

Capítulo 3

O modelo OSI e o Protocolo TCP/IP

O modelo de referência OSI (*Open Systems Interconnection*) é um método padronizado para o entendimento dos diversos níveis de comunicação em uma rede. Cada camada de rede recebe um nome que indica a sua funcionalidade no conceito geral.



O modelo OSI

Quando adotado na implementação de sistemas de comunicação, este modelo permite a interconexão de sistemas heterogêneos. Os sistemas, então, são ditos “abertos”⁸ e comunicam-se através de procedimentos normalizados ou padrões de protocolos de comunicação.

O modelo OSI é dividido em sete camadas, que normalmente são exibidas empilhadas verticalmente, de forma a representar a dependência da comunicação de uma camada com a outra.

Segundo Tanenbaum⁹, as camadas do modelo OSI foram definidas tendo em mente os seguintes ideais:

- Uma camada deve ser criada onde um nível diferente de abstração é necessário.
- Cada camada deve realizar uma função bem definida.

⁸ Atualmente, o modelo OSI é padronizado pelo Sub-comitê SC06, do comitê técnico conjunto ISO/IEC (*International Organization for Standardization* <<http://www.iso.ch>> e *International Electrotechnical Commission* <<http://www.iec.ch>>), e está representado pela família de normas 7498-X. No Brasil, a ABNT (Associação Brasileira de Normas Técnicas <<http://www.abnt.org.br>>) padronizou o modelo OSI na série NBR 1247X.

⁹ Andrew Tanenbaum, *Computer Networks*.

Os roteadores decidem ainda qual caminho deve ser usado para que os pacotes de dados alcancem o destino, utilizando regras de roteamento definidas por protocolos de alto nível (RIP, IGRP, BGP, OSPF, etc). Em relação ao modelo OSI, os roteadores atuam na camada de rede.

Outros dispositivos

Pontes: ou *Bridges*, são dispositivos que interligam segmentos de redes locais, não necessariamente iguais, mas similares (por exemplo, redes IEEE 802). No caso de segmentos de rede Ethernet, melhoram também as condições de acesso ao meio físico. As pontes atuam na camada de enlace e são muito utilizadas para isolar segmentos da rede utilizando endereços físicos (MAC address), impedindo o fluxo de dados desnecessários.

Nota: Roteadores de alguns fabricantes, tais como Cisco e 3Com, também realizam as funções de *Bridge* através de *software*. A estes equipamentos também dá-se o nome de *Brouters*.

Repetidores: também chamados *Repeaters*, são dispositivos simples que recebem, amplificam e transferem sinais elétricos entre segmentos de uma rede local, possibilitando a extensão dos segmentos de uma rede. Por exemplo, uma Ethernet 10base2 (coaxial fino) está limitada a 185 metros, mas com o uso de repetidores, a rede pode ser estendida até 925 metros (5 segmentos). Em relação ao modelo OSI, os repetidores atuam na camada física, interligando segmentos de rede iguais.

Comutadores: ou *Switches*, são equipamentos que interligam redes iguais (por exemplo, ATM¹⁰ e ATM) ou diferentes (Ethernet e ATM), podendo ser considerados como *Bridges* muito rápidas que disponibilizam alta velocidade em suas portas. Os *switches* atuam na camada de enlace com endereços MAC. Alguns *Switches* também realizam funções de roteamento, atuando nas camadas de enlace e de rede.

Gateways: são dispositivos que interligam sistemas diferentes, realizando a conversão de protocolos nas camadas mais altas (como por exemplo, entre aplicações X400 e SMTP). O termo *gateway*, principalmente na Internet, também é muito empregado para representar o roteador da rede.

Redes Ethernet

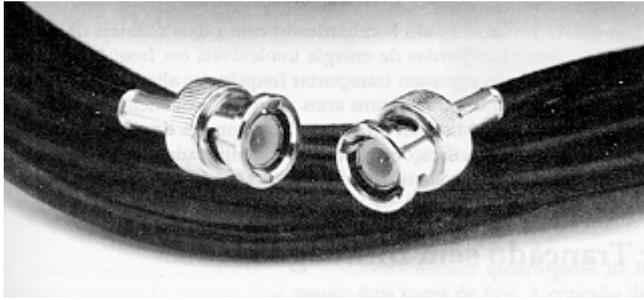
Conforme dito no capítulo 2, as redes locais são sistemas que cobrem áreas geográficas limitadas, na maior parte das vezes, algumas dezenas de metros. Algumas redes, no entanto, cobrem alguns quilômetros e ainda assim são qualificadas como redes locais.

Um dos padrões mais antigos, e de longe, o mais utilizado, de arquitetura de redes locais chama-se Ethernet¹¹.

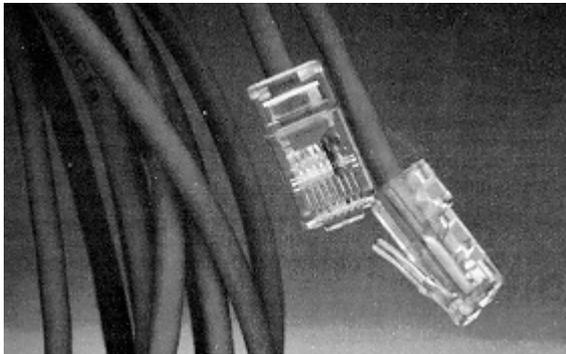
O Ethernet é uma especificação para vários tipos de meios físicos e velocidades de transmissão, sendo os mais comuns:

¹⁰ Asynchronous Transfer Mode

¹¹ O Ethernet foi inventado por Robert Metcalfe e David Boggs, no lendário laboratório PARC. A razão da escolha do nome Ethernet pelos seus inventores deve-se ao lendário poder de propagação de ondas eletromagnéticas pelo éter, como acreditava-se antigamente. O Ethernet foi posteriormente padronizado pelo IEEE (Institute of Electrical and Electronic Engineers) e pela ISO (International Standardisation Organization).



- 10Base2: utiliza cabo coaxial fino de 50 ohms e suporta até 30 estações, com espaços de no mínimo 0,5 metros entre si, num segmento de rede de até 185 metros. Com o uso de repetidores, a rede pode chegar até uma distância máxima de 925 metros (5 trechos). O seu uso deve ser evitado em distâncias maiores, pois devido à sua arquitetura em barramento, toda a rede pode ser interrompida quando há problemas ou manutenção.



- 10BaseT: utilizando cabos de par trançado de 4 pares de fios, pode suportar até 1024 estações com segmento de até 100 metros. O seu uso é recomendado devido à sua arquitetura em estrela, que facilita a manutenção e traz mais confiabilidade. O nome 10BaseT indica uma velocidade de 10 megabits por segundo, um esquema de sinalização de banda base e um cabeamento de par trançado utilizando uma topologia em estrela.

Dica: para a instalação de redes locais com o padrão 10baseT, recomenda-se a utilização de cabos de categoria 5 (CAT 5).

Nota: A evolução do padrão foi marcada pelo lançamento do FastEthernet, que permite velocidades de 100 Mbps. Para os meios físicos de comunicação, o FastEthernet possui as especificações 100BaseTX (até 100 m de cabo de pares trançados UTP - *Unshielded Twisted Pair*, categoria 5), 100BaseT4 (até de 100 m de cabo UTP categorias 3, 4 ou 5) e 100BaseFX (até 2 Km de fibra multimodo).

Redes de Longa Distância (WANs)

Redes Ponto-a-Ponto

Em geral, as redes de longa distância são formadas por circuitos digitais de comunicação de dados ponto-a-ponto. Os circuitos utilizados comercialmente no Brasil são denominados de E1 e E3. São circuitos ou linhas de comunicação digital dedicadas ou privativas, para transmissão de dados ou de canais de voz digital. Podem ser divididos em canais fracionais de menores velocidades (64 Kbps) e apresentam as seguintes velocidades:

- E1 - linha privativa a 2 Mbps;
- E3 - linha privativa a 34 Mbps;

Nota: o padrão americano, diferentemente do adotado no Brasil (padrão europeu), utiliza as designações T1 (linha privativa a 1.544 Mbps) e T3 (linha privativa a 45 Mbps).

Redes X.25 e *Frame Relay*

X.25: o X.25 é um protocolo padronizado para redes de comutação de pacotes a velocidades de até 2 Mbps, atuando nos três primeiros níveis OSI. Suporta múltiplas conexões através de circuitos SVC (*Switched Virtual Circuit*) ou PVC (*Permanent Virtual Circuit*).

Frame Relay: é um padrão ITU-T¹² que utiliza conceitos similares aos das redes de comutação de pacotes X.25, mas atua apenas nas duas primeiras camadas OSI, com quadros de tamanho variável. Como pressupõe que as linhas de comunicação sejam de alta qualidade, o *Frame Relay* maximiza a largura de banda através da redução de processamento do protocolo, deixando o controle de fluxo e a recuperação de erros a cargos dos dispositivos conectados nas pontas. Projetado especificamente para transmissão de dados, também tem se mostrado eficiente para transmissão de voz. A maioria dos equipamentos atualmente disponíveis suporta conexões de até 2 Mbps, mas permite velocidades de até 45 Mbps.

Bibliografia

- Guia de Conectividade - Frank J. Derfler, Jr. - Editora Campus, 1993

¹² International Telecommunications Union - Telecommunications Standards Section

Capítulo 5

Roteamento

Uma rota define um caminho pelo qual os pacotes de dados são transmitidos. A rota não define um caminho completo, e sim apenas um segmento do caminho, que pode ser de um *host* para um *gateway*, que retransmite pacotes para um destino, ou de um *gateway* para outro. As rotas podem ser definidas de acordo com os seguintes tipos:

Rota de Host: define um *gateway* que pode retransmitir pacotes para um *host* específico ou para um *gateway* em outra rede;

Rota de Rede: define um *gateway* que pode retransmitir pacotes para qualquer *host* numa rede;

Rota Default: Define um *gateway* que pode retransmitir todo pacote que não possui rota específica na tabela de roteamento.

Roteamento Estático

No roteamento estático, a tabela de roteamento não muda. É mais prático em redes pequenas e estáveis. Neste caso, a tabela de rotas é atualizada manualmente.

Roteamento Dinâmico

No roteamento dinâmico, os processos atualizam constantemente a tabela de rotas, trocando informações de roteamento com *gateways* e *hosts*. Essa troca de informações aumenta o tráfego na rede, mas o roteamento dinâmico se torna mais prático quando o número de *hosts* na rede é muito elevado.

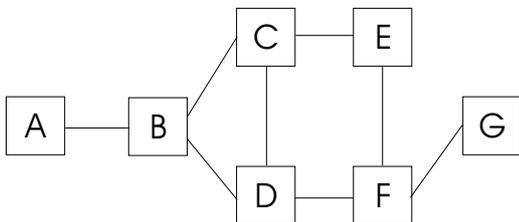
Até então, os protocolos de roteamento dinâmico mais comuns são o RIP (*Routing Information Protocol*), o IGRP (*Internal Gateway Routing Protocol* - da Cisco), o BGP (*Border Gateway Protocol*) e o OSPF (*Open-Short Path First*). No Unix, estes protocolos, exceto o IGRP, são implementados e inicializados por processos tais como **routed** e **gated**.

Métrica

Formada por um ou mais parâmetros, a métrica é a "medida de distância" utilizada pelos protocolos de roteamento durante o processo de decisão da melhor rota. No RIP, o único parâmetro da métrica é a quantidade de saltos (*hops*) na rota do pacote. Outros protocolos de roteamento definem a melhor rota compondo vários outros parâmetros como, por exemplo, velocidade, carga de utilização, estado e confiabilidade do *link*.

Implementação do Roteador

Considere o diagrama de blocos apresentado na figura a seguir, que representa a interligação de 7 computadores. A transmissão de dados entre os computadores A e B se faz através de uma única conexão existente entre eles.



Representação da Interligação de Computadores

No entanto, se A quisesse enviar dados para computador G, ele teria que dar passos intermediários até chegar ao destino. Um caminho viável poderia ser ABDFG. Outros caminhos que também poderiam existir são ABCEFG, ABCDFG e ABDCEFG. Surge então a dúvida: qual o melhor caminho?

A tarefa de escolha do melhor caminho é implementada calculando-se sempre qual o próximo ponto do caminho. O problema visto desta forma é mais simples, resumindo-se a achar qual o próximo computador a ser transmitida a mensagem. A cada passo, a tarefa de escolha do próximo computador é chamada de **roteamento**. Há vários algoritmos de roteamento que especificam a forma de calcular qual o próximo passo a ser seguido pelo pacote de dados, sempre visando encontrar a melhor rota.

O **roteador** é um computador projetado para implementar o roteamento de forma bastante rápida e eficiente, dedicado exclusivamente a esta tarefa.

Utilitários netstat, route, ping e traceroute

netstat - além de ter várias outras funcionalidades, este comando pode ser útil na verificação da tabela de rotas. O comando que mostra a tabela de rotas com os endereços na forma numérica é, por exemplo:

```
# netstat -rn
```

route - permite a inclusão ou a remoção de registros na tabela de rotas. O seguinte comando, por exemplo, cria uma rota *default* com métrica 1 através do *gateway* 192.168.1.2.

```
# route add 0 192.168.1.2 1
```

ping - utiliza o protocolo ICMP¹³ para enviar uma solicitação de ECHO (*Echo Request*) a uma máquina destino. Se esta responde (*Echo Reply*), então a conectividade está funcionando. O **ping** é muito útil para testar conexões e roteamento.

```
# ping 192.168.200.18
```

¹³ Internet Control Message Protocol

traceroute - é utilizado para traçar as rotas pelas quais o pacote trafega até atingir a máquina destino. É muito utilizado na detecção de problemas de roteamento, pois pode identificar claramente se há *loops* ou interrupção de rotas.

```
#traceroute 192.168.200.17
```

Exemplos

O diagrama da figura a seguir mostra o esquema de conexões físicas de uma rede local Ethernet, conectada a um PSI (Provedor de Serviços Internet) através de uma Linha Privativa de 64 Kbps. Apresenta, também, os endereços IP das interfaces de cada equipamento. A tabela de rotas necessárias em cada equipamento é mostrada a seguir.

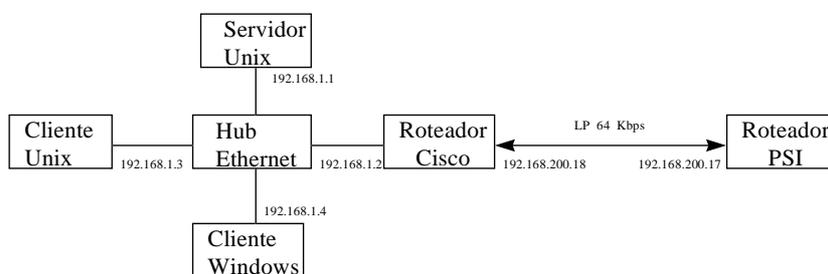


Figura 2.9.2 - Rede Local Ethernet

Roteador Cisco:

| destino | gateway | flags | métrica | máscara |
|-------------|-----------|-------|---------|---------------|
| 0.0.0.0 | Serial0 | UG | 1 | 0.0.0.0 |
| 192.168.1.0 | Ethernet0 | U | 0 | 255.255.255.0 |

Servidor Unix:

| destino | gateway | flags | métrica | máscara |
|-------------|-------------|-------|---------|---------------|
| 0.0.0.0 | 192.168.1.2 | UG | 1 | 0.0.0.0 |
| 192.168.1.0 | 192.168.1.1 | U | 0 | 255.255.255.0 |

Cliente Unix:

| destino | gateway | flags | métrica | máscara |
|-------------|-------------|-------|---------|---------------|
| 0.0.0.0 | 192.168.1.2 | UG | 1 | 0.0.0.0 |
| 192.168.1.0 | 192.168.1.3 | U | 0 | 255.255.255.0 |

Cliente Windows:

| destino | gateway | flags | métrica | máscara |
|----------------|----------------|--------------|----------------|----------------|
| 0.0.0.0 | 192.168.1.2 | UG | 1 | 0.0.0.0 |
| 192.168.1.0 | 192.168.1.4 | U | 0 | 255.255.255.0 |

Bibliografia

- Routing in the Internet - Christian Huitema - Prentice Hall, 1995.

Capítulo 6

POP-IN-A-BOX – o que é e diferentes opções

O POP-IN-A-BOX é um produto de fácil configuração e baixo custo, que reúne todos os informações necessárias à implementação da conexão da rede local de computadores de uma instituição à Internet. Veja todos os detalhes sobre a compra dos componentes no anexo **Quanto Custa e Como Adquirir o POP-IN-A-BOX**

Em termos de *hardware* e *software*, o POP-IN-A-BOX constitui-se de um microcomputador com a seguinte configuração mínima:

Hardware:

Em termos de *hardware*, o POP-IN-A-BOX constitui-se de um microcomputador com a seguinte configuração mínima:

- Pentium 100 MHz, 32 MB RAM (i), com:
 - 01 Placa SVGA 1MB;
 - 01 Disco Rígido de 2 GB;
 - 01 Unidade de CD-ROM;
 - 01 Unidade de Disco 1.44 MB;
 - 02 Portas Seriais e 01 Paralela;
 - 01 Placa Ethernet (ii)
 - 01 Bus Mouse
 - 01 Teclado;
 - 01 Placa Serial Síncrona ET-5025

Observação: O Módulo Roteador é implementado através da placa serial síncrona ET-5025. Neste caso, o sistema operacional FreeBSD implementa os protocolos de comunicação do roteador.

Nota: O POP-IN-A-BOX Avançado, ainda em desenvolvimento, incluirá também o módulo **Firewall** e outros serviços de redes mais sofisticados. Vale enfatizar que os aspectos de segurança de redes são bastantes importantes e devem ser cuidadosamente observados. Conseqüentemente, as instituições que adotarem o POP-IN-A-BOX devem estar atentas e tomar medidas preventivas referentes a possíveis problemas dessa natureza. Para isso, incluímos uma série de recomendações que podem aumentar a segurança do seu sistema no Anexo D.

Módulos Opcionais:

- i - Caso seja utilizado o Módulo *Firewall* ou se o POP-IN-A-BOX for suportar um número elevado de usuários, recomenda-se um valor mínimo de 64 MB de RAM;
- ii - Para a implementação e utilização do módulo *Firewall*, é necessário o emprego de uma **segunda placa Ethernet**;
- iii - O módulo Servidor de Comunicação requer uma **placa multiseri**al (de no mínimo 8 portas) e um número de modems externos equivalente à quantidade de portas que se deseja disponibilizar.
- iv - Para a instalação de algum dispositivo SCSI, como unidade de fita DAT ou disco rígido, é necessário utilizar uma placa SCSI.

Software

- 01 CD-ROM POP-IN-A-BOX, da Rede Nacional de Pesquisa.

O POP-IN-A-BOX prevê a utilização da versão 2.2.5 do sistema operacional Unix FreeBSD. Este sistema, bastante utilizado por provedores de serviço Internet, tem como vantagens a robustez e qualidade comprovadas e o fato de poder ser obtido gratuitamente, já que se enquadra na categoria de *software* de domínio público. Pode-se obter o FreeBSD através de distribuições de CD-ROM ou através da Internet, nos endereços <http://www.freebsd.org> e <http://www.cdrom.com>.

Nota: Os procedimentos descritos neste guia poderão ser utilizados, com pouquíssimas alterações, na instalação de versões posteriores à 2.2.5 do FreeBSD.

Comunicações:

Um fator básico para a ligação do POP-IN-A-BOX à Internet diz respeito ao backbone a ser utilizado para a sua interligação. No Brasil, existem diversos backbones de acesso, sendo que os três mais conhecidos são a a RNP, a Embratel, e a GlobalOne.

A RNP oferece acesso as redes acadêmicas regionais bem como diretamente as instituições de ensino e pesquisa nos estados que ainda não possuem tal infraestrutura, através de seus pontos de acesso regionais.

Contando com 90% do tráfego brasileiro, a Embratel é o maior backbone da América Latina, com mais de 100 MBps de capacidade de tráfego com a Internet mundial. Oferecendo o serviço IP DIRETO em quase todo o Brasil, a Embratel apresenta uma boa documentação no endereço http://www.embratel.net.br/internet/index_ipdir.html.

Finalizando, a Global One apresenta o GLOBAL IP BR, o braço brasileiro da sua rede IP mundial, conectada nos EUA ao SprintLink (serviço doméstico da Sprint).

Normalmente, a empresa que fornece os serviços de backbone se encarrega de providenciar o acesso físico junto da companhia telefônica local, no caso de ligação por cabos, ou por link de rádio. Este serviço não está incluído no custo do backbone, e deverá ser pago diretamente à concessionária.

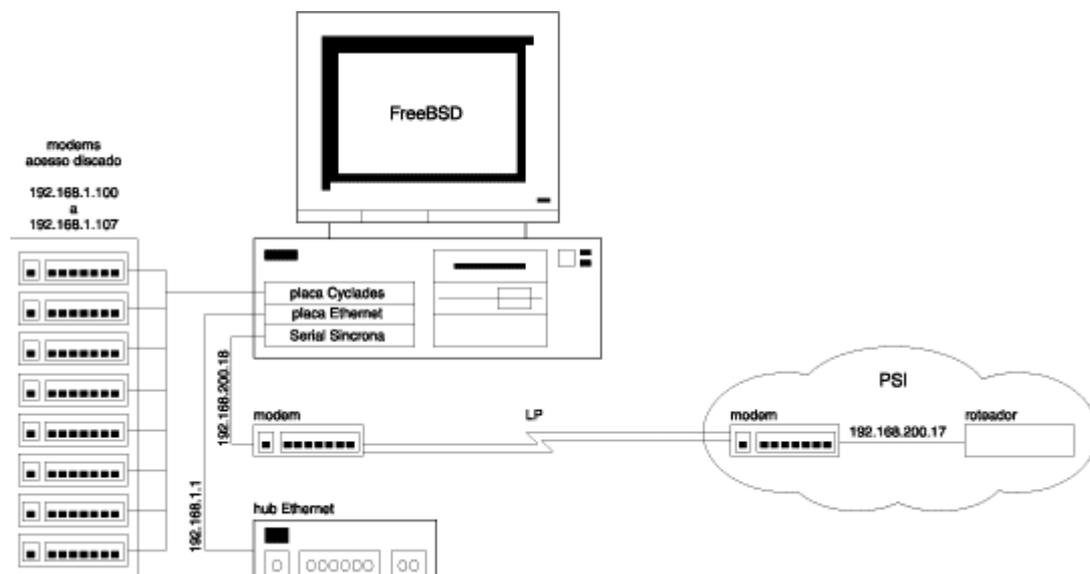
Outros serviços que normalmente são realizados pelas empresas de backbones são a distribuição de endereços IP e o registro de domínio principal junto à FAPESP. O anexo

Dica: Se você faz parte de uma instituição acadêmica, pode requerer um desconto de 50% nos preços dos serviços de interconexão à Internet. Consulte o documento <http://www.cg.org.br/docsoficiais/Tarifa.html> para maiores informações.

Esquema

O POP-IN-A-BOX, utilizando a placa *Emerging Technologies* ET-5025, é esquematizado a seguir:

POP-IN-A-BOX (utilizando a placa Emerging Technologies ET-5025)



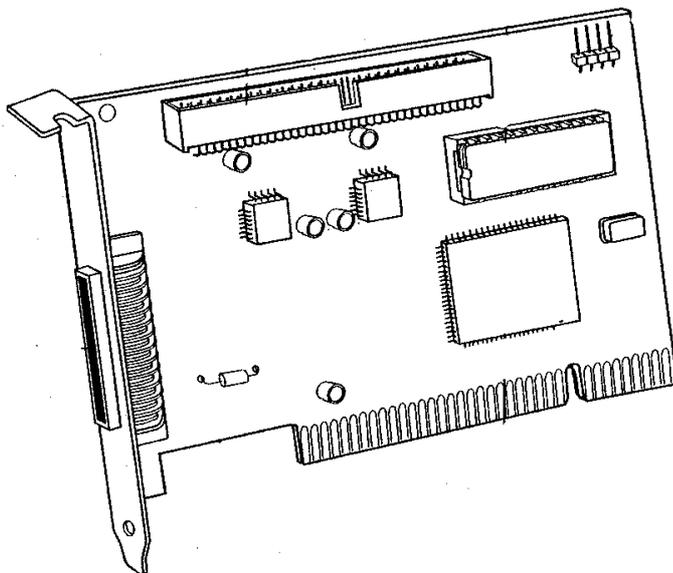
Instalando o POP-IN-A-BOX

O processo de montagem física do POP-IN-A-BOX inclui os seguintes passos, descritos em seguida:

- a) abrir o computador;
- b) conectar as placas necessárias para a correta utilização do sistema.
- c) fechar e conectar todos os cabos referentes a estas placas.

Antes de se proceder com a instalação do sistema operacional, é necessário montar fisicamente o POP-IN-A-BOX, ou seja, abrir o computador e conectar as placas necessárias para a correta utilização do sistema.

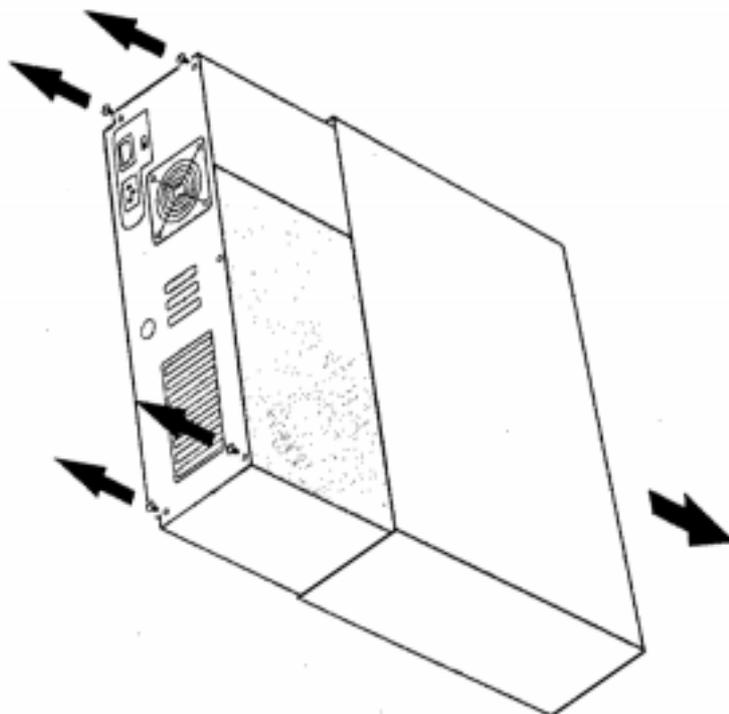
Basicamente, a única ferramenta necessária para esta tarefa é uma chave de fenda, mas diversas precauções devem ser tomadas contra a eletricidade estática, que pode inutilizar diversos componentes do sistema. Além disso, recomenda-se desconectar o computador da tomada de energia elétrica antes de abri-lo.



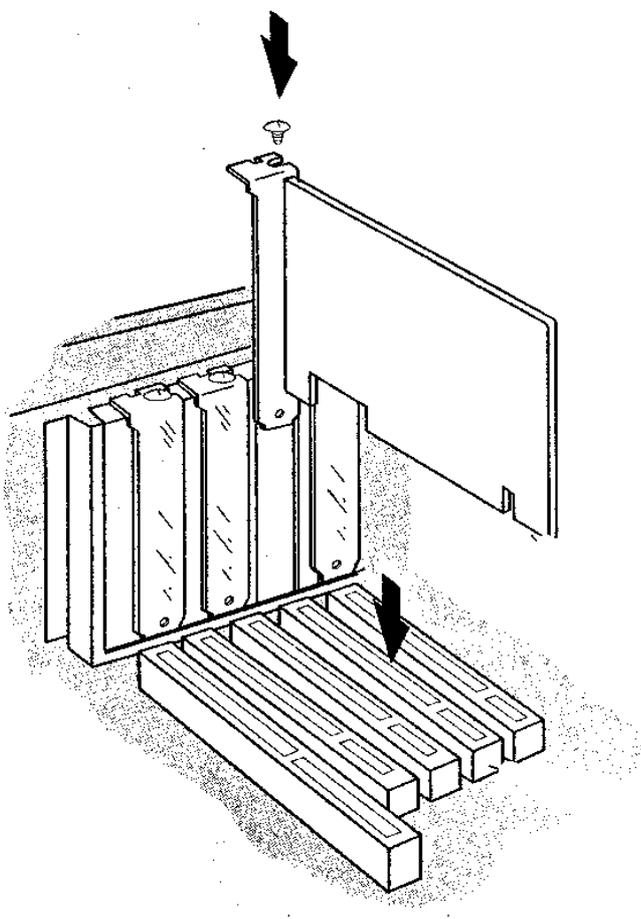
Uma placa adaptadora

Se você nunca montou e desmontou equipamentos, observe as seguintes precauções, que diminuem a possibilidade de danos nos componentes internos do computador:

- antes de manusear qualquer componente, descarregue a eletricidade estática do seu corpo tocando uma superfície aterrada.
- nunca utilize ferramentas imantadas.
- não remova as placas de suas embalagens originais até o instante de instalá-las.
- não toque nos componentes internos das placas. Manuseie-as pelas bordas.



O passo a seguir é desaparafusar o gabinete, e remover a sua tampa, deixando à mostra os componentes do computador.



Para instalar uma placa adaptadora, basta encaixá-la em um *slot* (conector da placa-mãe) vazio e em seguida aparafusá-la no gabinete. No entanto, existem pelo menos dois tipos de *slots*, ISA e PCI, incompatíveis entre si. Assim, uma placa adaptadora no formato ISA somente poderá ser colocada em um *slot* ISA (geralmente de cor preta), enquanto que uma placa formato PCI somente se encaixa em um *slot* de mesmo padrão (geralmente de cor branca ou bege).

Nota: embora dificilmente encontrados em novos computadores, outros tipos de *slots* podem existir em máquinas mais antigas. Entre estes *slots* podemos citar o VLB, o EISA e o MCA).

Uma boa prática é somente fechar o gabinete quando todo o sistema estiver funcionando.

Bibliografia

- Hardware Curso Completo - Gabriel Torres - Axcel Books do Brasil, 1998.
- Como montar e configurar o seu PC - Laércio Vasconcelos - LVC, 1998.

Capítulo 7

Instalando o Sistema Operacional FreeBSD

Mais detalhes sobre o FreeBSD. Ver no anexo 2

Instalando o FreeBSD

Etapas:

O processo de instalação consiste em:

- i Geração de um disquete de inicialização (*boot*);
- ii *Boot* pelo disquete;
- iii Criação do *slice* para o FreeBSD;
- iv Criação das partições do FreeBSD e seus sistemas de arquivos;
- v Instalação dos programas e arquivos do sistema;
- vi Configuração dos principais parâmetros do sistema, e;
- vii Instalação de algumas aplicações interessantes.

i — Geração de um Disquete de Inicialização (*Boot*) a partir de um sistema Windows ou DOS com uma unidade de CDROM:

- 1) Ligar o equipamento;
- 2) Entrar no DOS;

- Coloque o CD-ROM POP-IN-A-BOX na unidade X: (onde X é a sua unidade de CD-ROM);
- Coloque um disquete na unidade de leitura e gravação (drive); somente podem ser utilizados disquetes de 3.5", com a capacidade de 1.44MB.
- execute o *script* **makeflp.bat**, conforme as instruções a seguir;

```
d:\>makeflp <Enter>
```

```
Please insert a 1.44 MB Floppy and press return  
Press any key to continue... <Enter>
```

```
Now writing the boot.flp image onto the floppy  
Please wait  
Insert new diskette for drive A and press Enter when ready <Enter>
```

```
Done! When you are ready to install make sure that the boot floppy is in drive A and  
press the Reset button.
```

ii — *Boot* pelo disquete;

O passo seguinte é inserir o disquete de *boot* no drive, e reinicializar o seu computador. Durante o processo de *boot*, uma grande quantidade de informações será exibida na tela. Para verificá-las, com calma, pressione a tecla "**Scroll Lock**" e movimente o *scroll* para cima ou para baixo através das teclas "**Page Up**" e "**Page Down**". O sistema irá informar quais as controladoras foram detectadas e quais os seus parâmetros de comunicação com a CPU.

Perigo: Algumas BIOS permitem desabilitar o processo de *boot* através do disco A. Neste caso, a sequência a ser seguida deve ser A-C.

O processo de *boot* deve gerar uma mensagem semelhante à seguinte:

```
>> FreeBSD BOOT @ 0x10000: 640/31744 k of memory, internal console
Usage: bios_drive:interface(unit,partition)kernel_name options
  Bios_drive  0, 1, ...
  Interface   fd, wd or sd
  Unit        0, 1, ...
  Partition   a, c, ...
  Kernel_name name of kernel, or ? for list of files in root directory
  Options     -a (ask name) -C (cdrom) -c (userconfig) -D (dual consoles)
              -d (debug early) -g (gdb) -h (serial console) -P (probe kbd)
              -r (default root) -s (single user) -v (verbose)

Examples:
  1:sd(0,a)mykernel boot `mykernel' on the first SCSI drive when one IDE
              difve is present
  1:wd(2,a)          boot from the second (secondary master) IDE drive
  1:sd(0,a)?        list the files in the root directory on the specified
                    drive/unit/partition, and set the default bios_drive,
                    interface, unit and partition
  -cv              boot with the defaults, the run UserConfig to modify
                    hardware parameters (c), and present verbose messages (v)

boot:
```

Deve-se esperar um tempo aproximado de 5 segundos, findo os quais o processo de instalação carregará a configuração default e testará os requisitos de hardware do seu computador. Após este teste, a configuração encontrada será exibida na tela e o menu de configuração do kernel¹⁴ do FreeBSD será carregado.

Nota: devido às diferentes configurações possíveis na arquitetura Intel, existe a possibilidade do seu computador ter componentes não suportados pelo FreeBSD. O Anexo C lista os componentes que são suportados pelo sistema.

Selecione a seguir a opção **Skip kernel configuration and continue with the instalation.**

Será exibida uma série de mensagens informativas a respeito dos periféricos encontrados pelo kernel. Por exemplo, as mensagens abaixo indicam:

```
ahc0 <Adaptec 2940A Ultra SCSI host adapter> rev 1 int a irq 11 on pci0:20
ahc0: aic7860 Single Channel, SCSI Id=7, 3 SCBs
```

¹⁴ O kernel é a parte do sistema operacional que controla as funções primárias do computador.

- que foi detectada uma controladora Ultra SCSI Adaptec 2940A, que utiliza a IRQ 11 e está no barramento PCI;

```
ahc0 waiting for scsi devices to settle
(ahc0:4:0): "ARCHIVE Python 28454-XXX 4.44" type 1 removable SCSI 2
st0(ahc0:4:0): Sequential-Access density code 0x8c, 512-byte blocks, write-enabled
```

- a existência de uma unidade de fita (*tape drive*) nessa controladora;

```
Probing for devices on the ISA bus:
sc0 at 0x60-0x6f irq 1 on motherboard
sc0: VGA color <16 virtual consoles, flags=0x0>
ed0: disabled, not probed.
```

- que existe uma controladora VGA (ou SVGA) e um teclado utilizando a IRQ 1;

```
ed1 at 0x300-0x31f irq 9 on isa ed1: address 00:40:33:36:2d:be, type NE2000 (16 bit)
```

- a existência de uma placa de rede NE2000 utilizando os port addresses 0x300 até 0x31f, a IRQ 9 e cujo endereço Ethernet (MAC) é 00:40:33:36:2d:be;

```
sio0 at 0x3f8-0x3ff irq 4 on isa
sio0: type 16550A
sio1 at 0x2f8-0x2ff irq 3 on isa
sio1: type 16550A
```

- a existência de duas interfaces seriais, a sio0 (COM1) e a sio1 (COM2), os port addresses e IRQs utilizados

```
lpt0 at 0x378-0x37f irq 7 on isa
lpt0: Interrupt-driven port
```

- a existência de uma interface paralela;

```
lp0: TCP/IP capable interface
```

- que é possível utilizar a interface paralela como interface de rede;

```
lpt1 not found at 0xffffffff
```

- que não foi encontrada uma segunda interface paralela;

```
psm0: disabled, not probed.
```

- que o bus mouse do tipo PS2 está desabilitado;

```
fdc0 at 0x3f0-0x3f7 irq 6 drq 2 on isa
fdc0: NEC 72065B
fd0: 1.44MB 3.5in
```

- a existência de uma unidade de disquete de 1.44MB, utilizando os endereços 0x3f0 até 0x3f7, a IRQ 6 e a drq 2;

```
wdc0 at 0x1f0-0x1f7 irq 14 on isa
wdc0: unit 0 (wd0): <ST3660A D>
wd0: 520MB (1065456 sectors), 1057 cyls, 16 heads, 63 S/T, 512 B/S
wdc0: unit 1 (atapi): <MATSHITA CR-574/1.05>, removable, accel, iordis
wcd0: 689Kb/sec, 211Kb cache, audio play, 256 volume levels, ejectable tray
wcd0: medium type unknown, locked
```

- que há uma controladora IDE com um HD de 520 MB e uma unidade de CDROM MATSHITA;

```
npx0 on motherboard
npx0: INT 16 interface
```

- a existência de um co-processador.

Estas informações podem indicar que todo o equipamento está corretamente sendo utilizado pelo sistema operacional, ou que determinado dispositivo não está sendo corretamente detectado. Neste último caso, será necessário certificar-se ou modificar a configuração do periférico, ou certificar-se ou modificar a configuração do kernel do sistema operacional. Esta última possibilidade será considerada posteriormente.

Nota: Para modificar a configuração do periférico consulte a documentação do equipamento. Em geral, isso é feito via *jumps* ou *dip switches* da controladora, ou através da rotina de *setup* do computador, ou via *software*.

iii – Criação do *Slice* para o FreeBSD

Será, então, apresentado o menu principal do programa **sysinstall**. Selecione a opção **5 - Novice** e após teclar “**Enter**” na tela de mensagem, será acessado o menu do programa gerador do *slice*.

Nota: o conceito de *slice* e partição no FreeBSD é ligeiramente diferente do utilizado no MS-DOS/Windows 95. O que definimos como *slice* no FreeBSD é o equivalente a uma partição do MS-DOS. Além disso, um *slice* no FreeBSD pode ter até oito partições, que contém a estrutura básica do sistema de arquivos.

Se houver mais de um disco no equipamento, indique o disco onde será criado o *slice* desejada. Se houver algum *slice* anterior no disco, apague-o selecionando o *slice* através das teclas de setas e do comando **D**.

Repita a operação até remover todos os antigos *slices*. Feito isso, crie uma partição para todo o disco com o comando **A**, selecionando a opção “**yes**” da tela de confirmação. Selecione essa partição com as setas, indicando que blocos danificados sejam isolados (comando **B**) e que trata-se de uma partição *bootável* (comando **S**).

Ao sair desse menu (comando **Q**), utilizando as teclas de seta e a barra de espaço, selecione a opção **Standard** na tela de opções seguinte. Em seguida, teclre “**Enter**”.

iv – Criação das Partições do FreeBSD

Agora, devem ser criadas as partições do sistema. Após a tela de confirmação seguinte, o chamado Disklabel Editor, responsável pela criação das partições, será acessado. O comando **A** faz com que as partições sejam criadas automaticamente. Para finalizar, tecle **Q**.

Nota: pode-se instalar manualmente as diversas partições do sistema, como a partição “/” (**raiz**) e a de *swap*. Se o disco disponível for suficientemente grande, a alocação de 128 MB para o *swap* será uma garantia que o sistema conseguirá suportar um grande volume de processos. Se isso não for possível, uma boa opção é escolher um valor menor, porém, no mínimo, maior do que duas vezes a quantidade de memória RAM. Por exemplo, se o seu sistema tiver 32 MB de RAM, especifique no mínimo 64 MB de *swap*. Ao selecionar a opção **Label**, uma tela para criar as partições será mostrada. Selecionando o disco desejado, pressionando o **C**, o sistema perguntará qual o tamanho da partição desejada. A primeira partição será utilizada para instalar o diretório raiz. Se for alocado 128 MB para o *swap* e o resto para o diretório raiz, em um disco de 1600 MB, por exemplo, deve-se indicar que o tamanho da partição a ser criada será de 1472 MB. Em seguida, indica-se que a partição será de *file system* e que será montada no diretório raiz. Esta operação deverá ser repetida criando-se, neste exemplo, uma partição para *swap* de 128 MB. Outras partições igualmente necessárias são a */var*, que contém arquivos de registro e de mensagens recebidas pelo sistema, e a */usr*, que deverá conter os programas aplicativos.

v – Instalação dos Programas e Arquivos do Sistema

Indica-se, agora, o que do sistema será instalado, entrando-se na opção **Choose Distributions**. Para o POP-IN-A-BOX, a opção mais desejável é a **Developer**, que instala praticamente todas as opções necessárias para o FreeBSD.

Nota: para instalar a opção **Developer**, você precisará de 180 MB de espaço em disco.

A opção seguinte diz respeito à utilização da forma de criptografia utilizada pelo sistema. A opção “**yes**” instala o esquema DES, que é compatível com a maioria dos sistemas operacionais Unix. A opção **No** instala o esquema MD5, que apesar de ser mais seguro do que o DES, é incompatível com outros sistemas. De qualquer forma, a melhor opção para o POP-IN-A-BOX é a opção “**no**”. Selecione esta opção e tecle “**Enter**”.

A próxima opção diz respeito à instalação de programas adicionais. Selecione “**no**” e “**Enter**”.

Voltando ao menu de especificação de distribuições, tecle “**Enter**” para prosseguir.

Em seguida, especifica-se o tipo de mídia utilizado para instalar o FreeBSD. Em nosso caso, a opção 1, **CDROM**, deverá ser selecionada.

Após confirmar (selecione “**yes**” e tecle “**Enter**”), o processo de instalação é finalmente iniciado.

Perigo: Esta confirmação acarretará na perda de todas as informações eventualmente existentes no disco rígido.

O procedimento de instalação do sistema operacional se encerra em uma tela de congratulações. Tecele “**Enter**” para continuar.

vi – Configuração dos Principais Parâmetros do Sistema

Neste ponto, será perguntado qual a interface de rede a ser utilizada. Selecione a opção padrão Ethernet (opção **ed1**) e tecle “**Enter**” para continuar.

Para preencher os dados de configuração de rede, você deverá ter a mão os dados fornecidos pelo seu provedor de serviço básico de conectividade IP. A conectividade, ou seja, a interligação entre as diversas máquinas, é provida ao servidor do POP-IN-A-BOX através das interfaces Ethernet, para conexão à rede local, e Serial, para conexão à Internet.

A seguir, o sistema apresentará uma tela para a configuração da interface, com os seguintes campos:

host: aqui você vai entrar com o nome de sua máquina, ou seja, a identificação do computador que está sendo utilizado para o POP-IN-A-BOX. O nome da máquina é um parâmetro importante, mas pode ser escolhido de forma pessoal. Aconselha-se a utilização de no máximo 8 caracteres no nome da máquina.

domain: o domínio provisório da sua máquina. O domínio definitivo está sujeito a regras específicas.

gateway: o IP do roteador de saída, ou seja, IP do *gateway default*. No POP-IN-A-BOX (utilizando a placa *Emerging Technologies ET-5025*), como o próprio servidor FreeBSD realiza o roteamento, coloca-se o IP da interface Serial do roteador remoto, no caso 192.168.1.17.

Name server: o endereço IP do próprio servidor FreeBSD, que também atuará como servidor DNS.

Na seção **Configuration for Interface ...:**

IP address: o IP da sua máquina, de acordo com a faixa fornecida pelo provedor de serviço básico de conectividade IP.

Netmask: como em geral não se utiliza sub-redes, utilize o valor 255.255.255.0 para máscara de rede.

Opções extras de interface podem ser especificadas, caso necessário, no campo **Extra options to ifconfig**.

É aberta em seguida uma tela de confirmação a respeito da ativação da interface Ethernet. Selecione “**no**” e tecle “**Enter**”.

A tela seguinte especifica se a máquina será um *gateway* IP. Selecione “**yes**” e tecle “**Enter**”.

A seguir, escolha se a sua máquina permitirá ou não acesso FTP anônimo. Tecle “**Enter**” após escolher, e caso afirmativo, entre com as opções necessárias nos campos disponíveis. Após chegar à opção **OK**, tecle “**Enter**”, e indique se gostaria de editar uma mensagem de saudação para os usuários do seu FTP anônimo.

Na etapa seguinte, especifique se a sua máquina atuará como um servidor NFS, permitindo o compartilhamento remoto de arquivos. Selecione “**no**” e tecle “**Enter**”. Analogamente, especifique se a máquina atuará como cliente de um servidor NFS. Prossiga selecionando “**no**” e “**Enter**”.

Selecione novamente “**no**” e “**Enter**” para a possibilidade de customizar agora as configurações do terminal.

A configuração do fuso horário da máquina é o próximo passo da instalação. Selecione “**yes**” e tecle “**Enter**” para continuar. Prossiga selecionando “**no**” e “**Enter**” para informar a opção de hora local. Selecione as opções geográficas adequadas e prossiga da forma usual.

Informe a seguir se o sistema possui um mouse conectado.

vii – Instalação de Algumas Aplicações Interessantes

Ainda no menu **Configure**, pode-se instalar algumas aplicações interessantes: o editor de textos **emacs**, o interpretador **perl**, o leitor de e-mail **pine** e o shell **bash**. Todas essas aplicações e muitas outras podem ser encontradas dentro da opção **Packages**. Pode-se também optar por instalá-las no futuro. Após selecionar os pacotes desejados, retorne ao menu principal com o “**Esc**”.

Prossiga selecionando “**no**” e “**Enter**” para não adicionar novos usuários ao sistema neste momento, digitando “**Enter**” novamente para entrar com a senha do super-usuário (*root*).

Finalizando, selecione a seguir “**no**” e “**Enter**” para o registro do FreeBSD. Este registro pode ser feito posteriormente através do endereço <http://www.freebsd.org/register.html>.

Selecione a opção **Exit Install** do menu de configuração. E pronto, o sistema está instalado.

Dica: Um fórum de discussões sobre a utilização do FreeBSD pode ser atingido a partir do endereço <http://www.br.freebsd.org/freebsd-l/index.html>.

Bibliografia

- The Complete FreeBSD - Greg Lehey - Walnut Creek
- *site* do FreeBSD no Brasil - <http://www.br.freebsd.org/>

Capítulo 8

Montando o POP-IN-A-BOX

Para conectar o POP-IN-A-BOX à Internet, é necessário utilizar uma série de equipamentos e dispositivos, como placa serial síncrona, Linha Privativa de Comunicação de Dados (LPCD) e modem síncrono. A placa síncrona deve possuir as seguintes características:

- suportar velocidade mínima de 64 Kbps;
- suportar o protocolo PPP;
- utilizar padrões de conexão V.35, V.36 ou G.703.

Para o POP-IN-A-BOX, a placa escolhida foi a ET-5025, da empresa *Emerging Technologies*. As principais características desta placa são:

- utiliza barramento ISA
- requer 32 KB de memória RAM
- requer uma interrupção
- requer ainda 32 bytes de memória de entrada e saída
- não usa canais de DMA.

Como a versão 2.2.5 do FreeBSD não suporta na sua origem a ET-5025, torna-se necessário instalar manualmente o *driver* desta placa, disponível no CD-ROM do POP-IN-A-BOX. Isso pode ser feito seguindo os passos abaixo:

- 1) Dê *boot* no servidor
- 2) Entre na conta de super-usuário (*root*).
- 3) Para copiar os *drivers*, digite os comandos a seguir:

```
# mount /cdrom
# cd /cdrom/et5025
# cp freebsd25_2_27.tar /tmp; cd /
# tar -xvf /tmp/freebsd25_2_27.tar; rm /tmp/freebsd25_2_27.tar
```

Esta sequência de comandos irá copiar os *drivers* do CD-ROM, descompactá-los no diretório correto e limpar todos os arquivos intermediários criados.

```
# cd /usr/hdlc/dev; ./update
```

Nota: dependendo da versão do *driver* utilizada, será exibida uma mensagem parecida com a seguinte:

```
cp: v30/et5025v30.o: no such file or directory
Don't forget to delete et5025.o from your build directory!
```

Ignore-a!

Em seguida, conclua a instalação do *driver* com o seguinte comando:

```
# cat /usr/hdlc/dev/files.i386 >> /sys/i386/conf/files.i386
```

A seguir, modifique o arquivo de configuração do sistema, da seguinte maneira:

```
# cd /sys/i386/conf
# cp GENERIC ET5025
# ee ET5025
```

Adicione a linha a seguir no final do arquivo que está sendo editado:

```
device eth0 at isa? port 0x240 net irq 5 iomem 0xd0000 vector ethintr
```

Para gravar as alterações, tecle “**Esc**”, depois “**Enter**”, e finalizando, tecle “**a**”.

Para preparar o sistema, digite o seguinte comando:

```
# config ET5025
```

e em seguida

```
# cd ../../compile/ET5025  
# make
```

Não estranhe as inúmeras mensagens surgidas na tela. Neste momento, o kernel do sistema estará sendo compilado. Após o término da compilação, digite o seguinte comando:

```
# make install
```

Reinicialize o computador (através da combinação Ctrl+Alt+Del) para que o novo *kernel* seja lido. Verifique se a placa está corretamente instalada através do seguinte comando:

```
# dmesg | grep eth0
```

Uma mensagem semelhante a seguinte deverá ser exibida:

```
eth0 at 0x240-0x24f irq 5 maddr 0xd0000 on isa
```

Configuração do HDLC

HDLC é o protocolo de enlace necessário para o funcionamento de uma linha serial. O utilitário de configuração para este protocolo, o **hdlccfg**, requer que haja um arquivo de configuração para cada linha de dados ligada no sistema. Para configurar uma determinada linha, simplesmente execute o programa **hdlccfg**, utilizando como parâmetros o nome do arquivo de configuração e o número da linha (opcionalmente):

```
# /usr/hdlc/utl/hdlccfg fr0.cfg 1
```

O arquivo **fr0.cfg** contém importantes informações a respeito da linha de dados (no caso, frame relay) conectada ao sistema. O arquivo, que é parte integrante da distribuição da ET-5025, pode ser visualizado a seguir.

```
; level 2 configuration
```

```
ET5025      ;Board Definition  
0x14       ;Base Protocol (0x14=Frame Relay)
```

```
; Frame Relay Variables
```

```
10000      ;nT1 (User Mode) or nT2 (Network mode) in milliseconds  
1604       ;dN1 - maximum frame size  
5          ;nN1 - User mode Auto-LMI full status rate  
3          ;nN2 - LMI Error Threshold
```

```

5          ;nN3 - Measurement Interval for nN2

; Frame Relay Setup (ANSI ANNEX-D)

0          ;Management DLCI (0 for ANSI or 1023 for LMI)
0          ;Number of DLCIs (0=1024,1=8192)
0          ;Mode (0=User 1=Network, 2=LMI off)
0          ;Implementation (0=ANSI, 1=LMI (Cisco/Stratocom)
0          ;LMI Extensions
0          ;Not Used

; Board Configuration

0xd0000   ;memory base address
32        ;ram (32 or 64)
0         ;8-bit memory mode (1 = enable)
0         ;Wait State
0         ;memory sharing (1=enable)
0x240    ;io base address
5         ;irq interrupt
0         ;half duplex (0 = full duplex)
0         ;ignore modem control signals (1 = ignore CD and DSR)
20        ;clock oscillator rate (20 or 25)
0         ;cpu clock rate (0 = Normal, 1 = 20/25mhz)
0         ;baud rate (0 = External)

; HDLC controller setup

2         ; minimum flags between frames (1,2,4 or 6)
16        ; dma burst (2,16 or 64)
4         ; Hardware Tx buffers
8         ; Hardware Rx buffers
1         ; tx interrupt enable (0 = disabled)

```

Nota: Parâmetros adicionais podem ser especificados. Utilize, para isso, a documentação da ET-5025.

Configurando a Linha Serial para Rotear IP

Após a inicialização do protocolo de enlace, as linhas conectadas à placa estarão aptas a serem acessadas bem como qualquer interface de rede existente na sua máquina. Estas linhas serão acessadas pelos nomes **eth#**, onde **#** é o número da linha conectada.

Através do utilitário **ifconfig**, cada uma das linhas pode ser configurada individualmente dentro do sistema operacional. Veja um exemplo de uso do **ifconfig**:

```
# ifconfig eth0 192.168.200.18 192.168.200.17
```

Este comando irá configurar o endereço **IP 192.168.200.18** para a interface **eth0**, também especificando que o dispositivo do outro lado da linha possui o **IP 192.168.200.17**. Após a execução deste comando, a resposta do **ifconfig** deve ser algo como:

```
eth0: flags=51<UP, POINTOPOINT, RUNNING>
```

ou

```
eth0: flags=50<POINTOPOINT, RUNNING>
```

Do ponto de vista funcional, o endereço IP definido pelo **ifconfig** para a interface HDLC representa o endereço do roteador para o dispositivo remoto, endereço pelo qual o tráfego IP será enviado. Da mesma forma, o endereço local (192.168.200.18) é necessário para a entidade local de roteamento identificar a interface para onde enviar os pacotes via roteador 192.168.200.17.

Considerando o exemplo do POP-IN-A-BOX Modelo 1, os comandos abaixo especificam que a placa de rede Ethernet **ne0** está ligada na rede 192.168.1.0 e que a interface **eth0** possui endereço 192.168.200.18.

```
# ifconfig ne0 192.168.1.1  
# ifconfig eth0 192.168.200.18 192.168.200.17
```

Configurando a Rota *default*

Normalmente, o seu servidor estará conectado a uma máquina remota através de uma linha privativa. Desta forma, torna-se necessário estabelecer uma rota padrão, que será o caminho utilizado para interconectar as duas máquinas. Para estabelecer esta rota padrão devem ser obtidas algumas características da máquina remota, como o endereço IP do seu roteador. Supondo que o endereço IP do roteador é 192.168.200.17, deve-se executar o seguinte comando:

```
# route add default 192.168.200.17
```

Roteamento Dinâmico

Em geral, a rede de uma instituição possui apenas uma conexão à Internet. Neste caso, pode-se utilizar o roteamento estático, configurando-se as rotas manualmente através do comando **route**. Entretanto, se existir mais de uma conexão, a manutenção manual da tabela de rotas pode tornar-se dispendiosa frente às muitas possibilidades de alteração. Nesta situação, recomenda-se fortemente a utilização de um protocolo de roteamento dinâmico, como o RIP.

No FreeBSD, o RIP é implementado pelo programa **routed**, que gerencia todo o trabalho de roteamento dinâmico via RIP. Duas opções podem ser usadas:

- **routed -q**, que roda o **routed** em modo *quiet*, somente recebendo dados de roteamento dos outros roteadores;
- **routed -s**, onde o **routed** entra em modo *supplier*, enviando suas informações de roteamento para os outros roteadores conectados.

Configuração do PPP

PPP é um protocolo que pode ser usado como uma alternativa para o protocolo HDLC. A configuração do PPP também é feita mediante um arquivo de configuração, e, para isso, utilizaremos mais uma vez um arquivo de configuração já pronto. O protocolo PPP é recomendado para uso em quase todos os casos.

Outro Utilitário: ifhdlc

O disquete anexo à documentação da placa possui alguns utilitários que podem auxiliar no gerenciamento do roteamento na máquina.

Um destes utilitários é o **/usr/hdlc/utills/ifhdlc**, que recebe a interface a ser verificada como parâmetro opcional. Este utilitário fornece mais informações que o **ifconfig**.

Bibliografia

- Using ET/HDLC for BSD/OS and FreeBSD - <http://www.etinc.com/bsdman.htm>

Capítulo 9

Configurando o Serviço de Nomes (DNS)

Com o crescimento da Internet, a tarefa original de traduzir os nomes de domínio em endereços IP tornou-se uma tarefa complexa, e o sistema original centralizado pouco a pouco foi se tornando impraticável. Cada *host* continha a lista completa de todos os *hosts* e endereços em um arquivo local. Sempre que uma nova máquina era adicionada à rede, era necessário atualizar todos os arquivos de todos os computadores. Além disso, o tamanho do arquivo local começou a crescer

A saída encontrada foi a criação de um banco de dados distribuído, chamado de *DNS* (*Domain Name System*), que proporcionaria um mecanismo quase que transparente de mapeamento de nomes de domínio para endereços IP. O DNS possibilita, desta forma, a conversão destes endereços em nomes, que podem representar máquinas, redes ou mesmo aliases.

Esta tarefa é realizada através da divisão dos endereços Internet em grupos lógicos, que mantêm uma completa autoridade sobre as suas máquinas.

O DNS é um banco de dados distribuído com estrutura hierárquica semelhante a uma árvore, conforme esquematizado na figura a seguir. O serviço implementa a resolução de nomes em endereços numéricos e vice-versa, possibilitando a cada instituição, a administração independente do seu próprio segmento (domínio ou subdomínio).

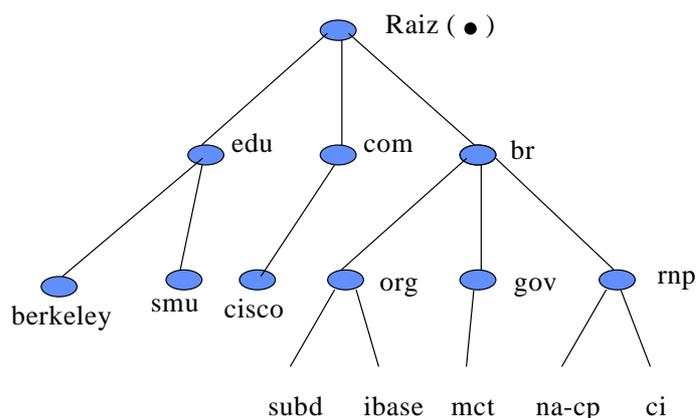


Figura 2.10.1 - Árvore de Domínios DNS

Cada nó (domínio ou subdomínio) da árvore representa uma parte do banco de dados do DNS. O domínio também tem um nome que identifica sua posição no sistema. Um nome de domínio completo é a seqüência de nomes separados por pontos, que vai do subdomínio até à raiz da árvore (exemplo: pop.org.br.).

Cada domínio pode ser administrado por organizações diferentes, e cada organização pode dividir o domínio em vários subdomínios e delegar responsabilidades sobre estes a outras instituições.

Servidores de Nomes

Servidores de nomes são programas (**named** ou **in.named**, em sistemas Unix) que armazenam informações sobre alguma parte do espaço de domínios, também chamada zona. Assim, o servidor de nomes é a autoridade responsável por sua zona e também pode ter responsabilidade por várias outras zonas.

Servidor Primário: Este servidor carrega, a partir de seus próprios arquivos, os dados da zona para a qual ele tem a responsabilidade, e pode delegar a outros servidores de nomes responsabilidades sobre seu domínio;

Servidor Secundário: Carrega seus dados a partir de um servidor de nomes primário. A cada inicialização e periodicamente, o servidor secundário atualiza seus dados;

Servidores Raiz: Também conhecidos como servidores cache, são responsáveis pelas informações dos domínios da raiz (com, edu, gov, br, etc). São tão importantes que, se todos caírem por um longo período, falharia qualquer resolução de nomes na Internet.

Registros e Arquivos DNS

Os dados associados a um domínio são contidos em registros de recursos (*Resources Records* ou RRs). Há vários RRs Internet e cada um possui uma sintaxe particular. Os mais comuns são:

A - Address: representa um endereço IP, para mapeamento de nome em endereço.

Exemplo: POP-IN-A-BOX1.pop.org.br. IN A 192.168.1.1

CNAME - Canonical NAME: especifica um *alias* para o nome canônico.

Exemplo: mailhost.pop.org.br. IN CNAME POP-IN-A-BOX1.pop.org.br.

MX - Mailer eXchange: especifica a preferência e a máquina que atua como servidora, realizando troca de mensagens.

Exemplos: pop.org.br. IN MX 0 POP-IN-A-BOX1.pop.org.br.
pop.org.br. IN MX 5 servunix2.pop.org.br.

NS - Name Server: especifica as máquinas que atuam como servidoras de nomes.

Exemplos: pop.org.br. IN NS POP-IN-A-BOX1.pop.org.br.
pop.org.br. IN NS servunix2.pop.org.br.

PTR - PoinTeR: representa o endereço reverso no qual in-addr.arpa é anexado, para mapeamento de endereços em nomes.

Exemplo: 1.1.168.192.in-addr.arpa. IN PTR POP-IN-A-BOX1.pop.org.br.

SOA - Start Of Authority: é o primeiro registro nos arquivos DNS. Indica que o servidor de nomes é a autoridade para o respectivo domínio.

Exemplo de configuração de DNS:

```
pop.org.br. IN SOA POP-IN-A-BOX1.pop.org.br. root.POP-IN-A-BOX1.pop.org.br. (  
    951017 ; serial  
    3600 ; refresh  
    1800 ; retry  
    3600000 ; expire  
    86400 ) ; minimum TTL
```

onde:

Serial – identifica a cópia original da zona. Transferências de zona preservam este valor. O servidor secundário compara este valor para iniciar uma nova transferência. Assim, sempre que houver modificações nos dados de algum arquivo DNS, o administrador deve incrementar o *serial number* para garantir a propagação para o demais servidores secundários;

Refresh – intervalo de tempo que indica a freqüência em que o servidor secundário verifica a precisão de seus dados;

Retry – intervalo de tempo entre as tentativas de transferência de zona pelo servidor secundário;

Expire – indica o intervalo de tempo durante o qual, se houver falha de contato entre os servidores primário de secundário, os dados são invalidados e o servidor secundário deixa de responder

Minimum TTL (Time to Live) – valor que se aplica a todos os RRs do arquivo. O servidor de nomes fornece o TTL nas respostas, permitindo que os outros servidores mantenham em *cache* os dados durante este intervalo.

O DNS é configurado basicamente através de cinco arquivos. Em geral, nomeia-se os arquivos de alguma forma associada ao domínio. Assim, considerando o domínio pop.org.br, tem-se:

named.boot - este é o arquivo de inicialização do programa servidor de nomes **named** (ou **in.named**) e possui as indicações dos arquivos de dados a serem lidos pelo DNS. Geralmente o **named** lê este arquivo a partir do diretório **/etc**, mas isto pode ser modificado através da linha de comando na execução do **named**.

pop.zone - este arquivo possui os dados, no formato DNS *Resource Records*, para mapeamento direto (nome/endereço) da zona sobre a qual o servidor de nomes é o responsável.

pop.rev - este arquivo possui os dados, também no formato DNS *Resource Records*, do domínio **in-addr.arpa** para mapeamento reverso (endereço/nome).

pop.local - este arquivo possui os dados, no formato DNS *Resource Records*, sobre a rede 127 (interface local *loopback*), cujo endereço reservado é 127.0.0.1.

named.root - ou **named.cache**, este arquivo possui informações sobre os servidores de nomes para o domínio raiz (o ponto da árvore). Este arquivo é único para todos os servidores de nomes de toda Internet, e deve ser atualizado regularmente. As informações podem ser buscadas via FTP anônimo na máquina **rs.internic.net** ou em **nic.ddn.mil**.

Utilitário nslookup

Após configurado e inicializado, o DNS deve ser testado através de aplicativos como o **nslookup**. O **nslookup** é um programa interativo para busca de informações sobre os domínios da Internet. É também um bom utilitário na detecção de problemas de configuração nos servidores de nomes. As informações sobre as opções do **nslookup** podem ser vistas digitando-se “?” no seu *prompt*.

O exemplo a seguir ilustra uma navegação pelo domínio pop.org.br, através do servidor de nomes POP-IN-A-BOX1.pop.org.br:

```
# nslookup
Default Server: POP-IN-A-BOX1.pop.org.br
Address: 192.168.1.1
> ls pop.org.br
```

Configuração do DNS

Certamente a máquina do POP-IN-A-BOX deverá também responder pelo serviço de nomes, ou seja, ser servidora DNS para o seu domínio. Com base nos exemplos a seguir, crie os respectivos arquivos de configuração do DNS.

O FreeBSD oferece uma opção de criação de um arquivo exemplo. Para isso, altere as permissões do arquivo **/etc/namedb/make-localhost** e execute este *script* da seguinte forma:

```
# chmod u+x /etc/namedb/make-localhost
# /etc/namedb/make-localhost
```

Este *script* deverá criar, no diretório **/etc/namedb/**, o arquivo **localhost.rev**, que poderá servir de modelo para a criação dos outros arquivos.

Após a criação dos arquivos, edite o arquivo **/etc/rc.local**, incluindo, no seu final, o comando **/usr/sbin/named**, para que o DNS seja inicializado quando a máquina for reiniciada.

Exemplos de Arquivos DNS

O DNS é configurado basicamente através de cinco tipos de arquivos. Para exemplificar, serão utilizados os arquivos de um servidor primário de nomes de uma rede com domínio pop.org.br e endereço 192.168.1.0, conforme apresentado nos dois modelos do POP-IN-A-BOX. Os exemplos abaixo assumem que o diretório de localização dos arquivos DNS é **/etc/namedb**.

Arquivo named.boot

```
; Inicio
directory                /etc/namedb
cache                    .          named.root
primary                  pop.org.br      pop.zone
primary                  1.168.192.in-addr.arpa pop.rev
primary                  0.0.127.in-addr.arpa      popr.local
; Fim
```

Arquivo pop.zone

```
; Arquivo pop.zone - definicao de hosts do dominio pop.org.br
; Serial : aammddl (aa=ano, mm=mes, dd=dia, l=versao)
@ IN SOAPOP-IN-A-BOX1.pop.org.br. root.POP-IN-A-BOX1.pop.org.br. (
    9509171 ; serial
    3600 ; refresh
    1800 ; retry
    3600000 ; expire
    86400 ) ; minimun TTL
    IN NSPOP-IN-A-BOX1.pop.org.br.
    IN MX 0POP-IN-A-BOX1.pop.org.br.
;
localhost. IN A 127.0.0.1
;
POP-IN-A-BOX1 IN A 192.168.1.1
mailhost IN CNAME POP-IN-A-BOX1
;
cisco-eth IN A 192.168.1.2
; Fim
```

Arquivo pop.rev

```
; Arquivo pop.rev - definicao de enderecos para o 1.168.192.in-addr.arpa
; Serial : aammddl (aa=ano, mm=mes, dd=dia, l=versao)
1.168.192.in-addr.arpa. IN SOA POP-IN-A-BOX1.pop.org.br. root.POP-IN-A-BOX1.pop.org.br.(
    9509171; serial
    3600 ; refresh
    1800 ; retry
    3600000 ; expire
    86400 ) ; minimun
    INNS POP-IN-A-BOX1.pop.org.br.
;
1 IN PTRPOP-IN-A-BOX1.pop.org.br.
2.1.168.192.in-addr.arpa. INPTR cisco-eth.pop.org.br.
; Fim
```

Arquivo pop.local

```
; Arquivo pop.local - definicao do localhost do domínio pop.org.br
; Serial : aammddl (aa=ano, mm=mes, dd=dia, l=versao)
@ IN SOAPOP-IN-A-BOX1.pop.org.br. root.POP-IN-A-BOX1.pop.org.br. (
    9509171; serial
    3600 ; refresh
    1800 ; retry
    3600000 ; expire
    86400 ) ; minimun TTL
    IN NS POP-IN-A-BOX1.pop.org.br.
1 IN PTR localhost.
; Fim
```

Arquivo named.root

```
; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC registration services
; under anonymous FTP as
; file /domain/named.root
; on server FTP.RS.INTERNIC.NET
; -OR- under Gopher at RS.INTERNIC.NET
; under menuInterNIC Registration Services (NSI)
; submenuInterNIC Registration Archives
; file named.root
;
; last update: May 19, 1997
; related version of root zone: 1997051700
;
; formerly NS.INTERNIC.NET
. 3600000 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A198.41.0.4
; formerly NS1.ISI.EDU
. 3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A128.9.0.107
; formerly C.PSI.NET
. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A192.33.4.12
; formerly TERP.UMD.EDU
. 3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A128.8.10.90
; formerly NS.NASA.GOV
. 3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A192.203.230.10
; formerly NS.ISC.ORG
. 3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000 A192.5.5.241
; formerly NS.NIC.DDN.MIL
. 3600000 NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET. 3600000 A192.112.36.4
; formerly AOS.ARL.ARMY.MIL
. 3600000 NS H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET. 3600000 A128.63.2.53
; formerly NIC.NORDU.NET
. 3600000 NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET. 3600000 A192.36.148.17
; temporarily housed at NSI (InterNIC)
. 3600000 NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET. 3600000 A198.41.0.10
; temporarily housed at NSI (InterNIC)
. 3600000 NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET. 3600000 A193.0.14.129
; temporarily housed at ISI (IANA)
. 3600000 NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET. 3600000 A198.32.64.12
```

```
; temporarily housed at ISI (IANA)
.           3600000 NS   M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET. 3600000 A198.32.65.12
; End of File
```

Bibliografia

- DNS and BIND - Paul Albitz & Cricket Liu, O'Reilly.

Capítulo 10

Serviços de Correio Eletrônico (SMTP e POP)

O correio eletrônico é um dos serviços básicos de rede que funciona através de mecanismos do tipo *store-and-forward*. Possui alguns elementos importantes para o seu funcionamento que são:

- Os MTAs (*Message Transfer Agents*), sendo exemplos o MHS (*Message Handling Service*) do Unixware e do Netware, e o **sendmail** do Unix, este o mais popular;
- Os programas de interface com o usuário, também conhecidos como UAs (*User Agents*), como o **elm**, o **pine**, o **eudora**, o **winmail/pmail** e o **mailtool** (do X-Windows da Sun);
- Os *Mailers*, agentes utilizados para efetuar a transferência de mensagens entre os vários sistemas de comunicação como UUCP, TCP/IP, BITNET, DECNET, etc.

Sendmail/SMTP

O **sendmail** é um MTA de uso geral que implementa o SMTP (*Simple Mail Transfer Protocol*), de acordo com as RFC 822 (*Internet Mail Format Protocol*), RFC 821 (SMTP), RFC 1123 (*Internet Host Requirements*) e RFC 1425 (*SMTP Service Extensions*) [RFC: *Request for Comments*, pode ser considerado como sendo um documento de normalização da Internet]. Devido à sua grande versatilidade, o **sendmail** torna-se bastante vulnerável com relação aos aspectos de segurança. São recomendáveis, portanto, a instalação de versões mais novas (maior número de bugs corrigidos) e a configuração correta do programa, para que seja garantido o bom funcionamento do correio eletrônico e sejam evitados possíveis problemas de segurança.

Nos sistemas Unix, em geral, o **sendmail** é configurado através do arquivo **sendmail.cf**, que possui parâmetros para especificar o nome da máquina (*hostname*), o domínio, o diretório de mensagens (*mailbox*), o arquivo de apelidos (*aliases*), etc.

Servidores POP

O POP (*Post Office Protocol*), cuja versão mais popular é o POP3 (RFC 1725), permite que o usuário carregue todas as mensagens de correio eletrônico do servidor para o seu microcomputador, via rede local ou via acesso discado. Para isso, basta a que o seu PC ou Macintosh tenha um UA compatível com POP, **eudora** ou **pegasus mail**, por exemplo.

Configurando o SMTP (Sendmail)

O **Sendmail** já é instalado automaticamente durante a instalação do FreeBSD. Entretanto, são aconselháveis algumas mudanças em sua configuração original.

Encontre as linhas correspondentes e faça as seguintes alterações no arquivo **/etc/sendmail.cf**:

- Coloque seu domínio após a cláusula **CW** (sem espaços), por exemplo: CWpop.org.br;
- A linha da cláusula **Fw** deve ser a seguinte: **Fw -o /etc/sendmail.cw**. Se não existir esta linha no arquivo, insira-a;
- Após a cláusula **DM**, coloque seu domínio, assim como na cláusula **CW**.

Crie o arquivo **/etc/sendmail.cw**, que deverá conter as seguintes informações, uma em cada linha: seu domínio, nome de todas as máquinas pelas quais seu servidor receberá mail, inclusive o seu próprio nome. Por exemplo:

```
pop.org.br
POP-IN-A-BOX1.pop.org.br
mailhost.pop.org.br
www.pop.org.br
```

Nota: Caso esta máquina não seja o servidor de mail de seu domínio, as únicas alterações nos procedimentos acima são: deixar a cláusula **CW** em branco, e, no arquivo **/etc/sendmail.cw**, só colocar os nomes das máquinas pelas quais este servidor receberá mail, sem, é claro, colocar seu domínio.

Nota: Informações mais detalhadas, novas versões e configurações mais complexas, como anto-spam e anti-relay, podem ser encontradas em <http://www.sendmail.org>.

Instalando e Configurando o POP

Com o CDROM do POP-IN-A-BOX devidamente montado no **/cdrom**, execute o programa de instalação **sysinstall**, conforme os comandos abaixo:

```
# /stand/sysinstall
```

Instalação

- Escolha a opção **Configure**;
- Pressione **“Enter”** sobre a opção **Packages**;
- Escolha a opção **CD-ROM**;
- Com a barra de espaço, marque a opção **Mail**;
- Confirme em **OK**;
- Selecione as opções **fetchmail-4.3.1**, **imap-uw-4.1b** e **procmail-3.11p7**;
- Termine a seleção de pacotes com **Cancel**;
- Confirme o pacote a ser instalado na tela **Target Package** em **OK**, e confirme a instalação com **“Enter”**.

Para a configuração do servidor POP, altere a linha abaixo correspondente ao serviço pop3 no arquivo **/etc/inetd.conf**:

```
#pop3 stream tcp nowait root /usr/local/libexec/popper popper
```

Retire o comentário (o caractere #), trocando a sequência **/usr/local/libexec/popper** por **/usr/local/libexec/1pop3d** e **popper** por **ipop3d**. A linha modificada deve ficar da seguinte forma:

```
pop3 stream tcp nowait root /usr/local/libexec/ipop3d ipop3d
```

Basta reinicializar o *daemon* inetd (`$ kill -1 número_do_processo`) para que o servidor POP3 entre em funcionamento.

Bibliografia

- Sendmail - Bryan Costalles, Eric Allman & Gigi Estabrook - O'Reilly.

Capítulo 11

Conhecendo e Instalando o Servidor WWW Apache

O Apache é um servidor WWW baseado no código do NCSA HTTPd 1.3. Em pouco tempo, desde o início do seu desenvolvimento (em 1995), ele se igualou à maioria dos servidores Web baseados em Unix, tornando-se tão bom ou melhor que seus concorrentes. Embora o Apache e o NCSA sejam ambos excelentes produtos, existem algumas diferenças fundamentais entre eles. Uma delas é com relação a licenciamento. O Apache é gratuito em qualquer situação, enquanto que o NCSA só fornece licença gratuita de uso para fins não lucrativos. Como o Apache é compatível com o NCSA, muitos dos arquivos de configuração são idênticos. O servidor oferece ainda a possibilidade de configuração da geração de arquivos de logs, além de módulos de expansão.

O esforço no desenvolvimento do servidor Apache foi e continua sendo realizado por um grupo de especialistas voluntários, sem nenhuma participação do setor comercial. O servidor foi criado porque seus membros temiam mudanças na política de licenciamento do servidor NCSA e queriam um produto superior que implementasse uma série de características não encontradas em outros servidores.

O nome Apache é originário de um jogo de palavras. Originalmente dizia-se que o projeto era "*A PATChy server*", ou seja, um servidor com arquivos patch. Arquivos patch são pequenas correções de bugs e características em software.

Entre os planos futuros para o Apache estão a sua continuação como um servidor HTTP de domínio público e a sua atualização em relação aos avanços do protocolo HTTP e de desenvolvimento do Web em geral. O desenvolvimento do Apache proporciona uma volta aos "bons tempos" do desenvolvimento de software, onde as limitações de hardware faziam da programação uma arte. O desenvolvimento do FreeBSD e do Linux perseguem objetivos parecidos.

Um fato interessante que dá mais credibilidade ainda ao trabalho dos voluntários do Apache é que as novas versões do servidor NCSA utilizam parte do código desenvolvido pelo Apache, melhorando assim a sua performance.

O servidor Apache tem o seu código fonte disponibilizado no endereço <<http://www.apache.org>>, além de diversos binários pré-compilados para várias plataformas Unix, entre elas Solaris 2.4 e 2.5, SunOS 4.1.3, BSDI 2.0, IRIX 5.3, HPUX 9.07, Linux ELF e A.OUT, freeBSD 2.1, UnixWare 1.1.2, AUX 3.1, Next, e outros. Recomenda-se o *download* do programa e de sua documentação, que pode ser obtida nos formatos PostScript, PDF (*Adobe Acrobat*) ou HTML. A documentação do Apache é bem feita, e possui diversos tópicos como FAQs, notas de instalação, etc.

Instalação e Configuração do Apache

Esta seção fornecerá os procedimentos de como instalar e configurar o servidor WWW, usando o Apache versão 1.2.4, que acompanha o FreeBSD.

Com o CDROM do FreeBSD devidamente montado no **/cdrom** execute o programa de instalação **sysinstall**, conforme os comandos abaixo.

```
# mount /cdrom
# /stand/sysinstall
```

Siga com os procedimentos de **instalação**

- Escolha a opção **Configure**;
- Pressione “**Enter**” sobre a opção **Packages**;
- Escolha a opção **CD-ROM**;
- Escolha a opção **WWW**;
- Com a barra de espaço, marque a opção **Apache-1.2.4**;
- Confirme em **OK**;
- Termine a seleção de pacotes com **Cancel**;
- Confirme o pacote a ser instalado na tela **Target Package** em **OK**, e confirme a instalação com “**Enter**”.

Configuração

- Entre na opção **Configure** do **sysinstall**;
- Escolha a opção **Networking**, teclando “**Espaço**” sobre **WEB Server**;
- Entre com os dados requeridos como *hostname*, endereço IP, *Default Document*, etc, tomando o cuidado de trocar tanto *Default User ID* e *Default Group ID* de **bin** para **nobody**;
- Confirme com **OK** e reinicialize a máquina.

Acesse o seguinte diretório:

```
# cd /usr/local/etc/apache
```

Crie os arquivos de configuração:

```
# cp access.conf-dist access.conf
# cp httpd.conf-dist httpd.conf
# cp mime.types-dist mime.types
# cp srm.conf-dist srm.conf
```

Edite, em seguida, o arquivo httpd.conf:

```
# ee httpd.conf
```

Retire o comentário (o caractere #) da linha *ServerName*, e insira o nome do servidor no lugar de *new.host.name*. A linha deverá ser parecida com a seguinte:

```
ServerName www.pop.org.br
```

Após a reinicialização do sistema, o *daemon httpd* deve estar “rodando” no sistema. Se for aceito o diretório *default* para a localização dos documentos Web (HTML), então esses documentos já poderão ser colocados em **/usr/local/www/data**.

Bibliografia

- Apache - The Definitive Guide - Ben Laurie & Peter Laurie - O'Reilly - 1997

Capítulo 12

Configurando o Serviço FTP

O FTP, uma das aplicações mais antigas da Internet, é um acrônimo para *File Transfer Protocol*, ou seja, protocolo de transferência de arquivos. Como o próprio nome diz, é utilizado para transferir arquivos entre diferentes máquinas conectadas, como servidores e máquinas desktop, etc.

O FTP começou a ser desenvolvido em 1971, através da criação de diversos mecanismos para transferência de arquivos de servidores no MIT (*Massachusetts Institute of Technology* <<http://web.mit.edu>>). Em 1973, foi editado o primeiro documento “oficial” sobre o FTP, o RFC 454 (*Request for Comments*, ou RFC, pode ser considerado como sendo um documento de normalização da Internet).

Segundo a RFC 959, que possui a sua especificação mais recente, os objetivos do FTP são:

- Proporcionar o intercâmbio de arquivos (programas de computadores ou dados);
- Estimular o uso indireto ou explícito de computadores remotos;
- Isolar o usuário de variações de sistemas de armazenamento de arquivos entre diversos servidores;
- transferir dados de forma confiável e eficiente.

De fato, embora o FTP possa ser utilizado diretamente por um usuário em um terminal, o seu desenvolvimento teve como objetivo principal a sua utilização por *software*.

Instalação e Configuração do WU-Ftp

É aconselhável trocar o servidor FTP pelo WU-Ftp, que é um servidor mais seguro e eficiente.

Se, durante a instalação do sistema, o WU-Ftp foi instalado, passe para o tópico "Configuração do WU-Ftp". Caso contrário, instale-o com o comando **/stand/sysinstall** ou proceda da seguinte forma:

Instalação

- Escolha a opção **Configure**;
- Pressione “**Enter**” sobre a opção **Packages**;
- Escolha a opção **CD-ROM**;
- Escolha a opção **Net**;
- Com a barra de espaço, marque a opção **wu-ftpd-2.4.2b15**;
- Confirme em **OK**;
- Termine a seleção de pacotes com **Cancel**;
- Confirme o pacote a ser instalado na tela **Target Package** em **OK**, e confirme a instalação com “**Enter**”.

Configuração do WU-Ftp

Configure o WU-Ftp, seguindo os procedimentos descritos abaixo:

Altere o nome do servidor de FTP localizado em **/usr/libexec/**, de **ftpd** para **ftpd.old**

```
# mv /usr/libexec/ftpd  
/usr/libexec/ftpd.old
```

Mova o **ftpd**, localizado em **/usr/local/libexec/** para **/usr/libexec/**

```
# mv /usr/local/libexec/ftpd /usr/libexec/ftpd
# cd /usr/local/etc
# cp ftpconversions.example ftpconversions
# cp ftpusers.example ftpusers
# cp ftpaccess.example ftpaccess
```

Finalmente, copie os arquivos exemplos de configuração do WU-Ftp (novo **ftpd**), localizados em **/usr/local/etc**, para arquivos de mesmo nome sem a extensão **.example**.

Utilizando o FTP

Os principais comandos do FTP são:

- **ascii** - estabelece o modo de transmissão para ASCII (texto puro).
- **binary** - estabelece o modo de transmissão para binário.
- **bye** - termina a sessão FTP e sai do programa
- **cd** - muda o diretório da máquina remota.
- **close** - finaliza uma sessão FTP.
- **get** - inicia o processo de *download* do arquivo remoto.
- **ls** - lista o conteúdo do diretório remoto
- **mdelete** - apaga múltiplos arquivos.
- **mget** - idêntico ao **get**, só que para múltiplos arquivos.
- **mkdir** - cria um diretório na máquina remota.
- **mput** - inicia o upload de múltiplos arquivos.
- **open** - inicia uma conexão FTP conectando-se a um servidor.
- **put** - inicia o processo de upload de um arquivo local para o servidor remoto.
- **pwd** - exibe o diretório corrente na máquina remota.
- **quit** - finaliza a sessão FTP.
- **rename** - renomeia um arquivo.
- **rmdir** - apaga um diretório na máquina remota.

Como exemplo, para efetuar a transferência do arquivo **top-3.4.tar.gz** do diretório **/pub/packages/top** do servidor FTP da RNP para a sua máquina local, deve-se proceder da seguinte forma:

```
$ ftp ftp.rnp.br
```

Após a conexão, o sistema solicita o seu username. A maioria dos sistemas públicos aceitam o username *anonymous*, e solicitam que você entre com o seu endereço de correio eletrônico como senha.

Em seguida, deve-se acessar o diretório especificado, o que pode ser feito pelo comando:

```
ftp> cd pub/packages/top
```

Como o arquivo a ser transferido é binário, deve-se especificar este modo de transferência

```
ftp> bin
```

E finalmente, solicitar a transferência do arquivo desejado

```
ftp> get top-3.4.tar.gz
```

Após alguns minutos (dependendo da velocidade da sua conexão à Internet), o arquivo deverá estar transferido para a sua máquina local.

Bibliografia

-
-

Capítulo 13

Instalando o Servidor de Comunicação

O servidor de comunicação é um equipamento dedicado que tem a função básica de prover conectividade IP para acesso discado, através de protocolos como PPP ou SLIP. Em geral, possui várias portas seriais assíncronas para conexão de modems e, em alguns casos, pode também ser utilizado como roteador, provendo conexões assíncronas dedicadas.

Para o POP-IN-A-BOX, o servidor de comunicação é implementado por uma placa multiseriada, com protocolo PPP assíncrono e sistema de autenticação PAP, ambos suportados pelo FreeBSD.

Requisitos de *Hardware*

Placa Multiseriada

No caso particular do POP-IN-A-BOX, foi utilizada a placa multiseriada Cyclom-8Yo da Cyclades, cujas principais características são as seguintes:

- Baseada em tecnologia RISC;
- 8 saídas seriais assíncronas (RS-232C);
- Barramento ISA;
- Desempenho de 115 Kbps em todos os canais;
- Compatível com vários sistemas operacionais, como: Windows NT, Unix, OS/2, etc;
- Suporte a TCP/IP;
- *Dial-in/Dial-out*.

Dentre as aplicações mais típicas que este produto oferece, podem-se citar:

- Acesso *dial-up* de clientes remotos;
- Aplicações SOHO (*Small Office Home Office*);
- De provedor de Serviços Internet;
- Conexão de terminais e impressoras num ambiente Unix.

Modems Externos

Para a implementação do servidor de comunicação e a plena disponibilidade dos serviços de acesso discado, será necessário um ou mais (no máximo 8) modems externos com as seguintes características:

- Suporte aos comandos *Hayes*;
- Suporte a compressão de dados e correção de erros;
- Compatibilidade com os protocolos V.34Plus e anteriores.

O modem deve ser configurado com os seguintes atributos:

- Resposta automática;
- Desconexão e auto-reinicialização quando ocorrer mudança de **ON** para **OFF** da linha DTR;
- Controle de fluxo RTS/CTS, mas aceitar conexões sem nenhum controle;
- Velocidade constante com o servidor de comunicação;
- Negociação da velocidade com o modem remoto.

Para modelos padrão *Hayes*, o seguinte comando deverá facilmente atribuir estas características e deixá-las na memória não volátil, isto é, as informações serão gravadas no próprio modem:

```
AT &C1 &D3 &K3 &Q6 S0=1 &W
```

Instalação e Configuração da Placa Multiserial

Instalação

- i. Selecione uma interrupção (IRQ) e endereço de memória RAM livres, de modo que não exista conflito de *hardware*;
- ii. Baseado na escolha feita no passo (i), configure os *dip-switches* da placa. No caso particular da placa Cyclom-8Yo, esta configuração deverá obedecer à Tabela do Capítulo 4 do Guia do Usuário que acompanha o produto. A configuração de fábrica desta placa é IRQ10, 0xD4000 e, na maioria dos casos, deverá funcionar;
- iii. Desligue o computador. Caso já tenha instalado o sistema operacional FreeBSD na sua máquina, não esqueça de utilizar o comando *shutdown* para desligá-la:

```
# shutdown -h now
```

Para maiores informações sobre este comando, digite:

```
# man shutdown
```

- iv. Encaixe a placa em algum *slot* ISA livre e ligue o computador;
- v. Se existir conflito de *hardware*, repita os passos (i) e (ii), até o conflito desaparecer;
- vi. Conecte firmemente o cabo Octopus (com as 8 saídas seriais) à placa;
- vii. Opcionalmente, use o **CYCTEST** (programa que acompanha o produto) para garantir a funcionalidade da sua placa Cyclom-8Yo.

Configuração

A seguir, modifique o arquivo de configuração do sistema, da seguinte maneira:

Se foi utilizado o POP-IN-A-BOX modelo 1 (que utiliza a placa *Emerging Technologies* ET-5025) use os seguintes comandos:

```
# cd /sys/i386/conf
# cp ET5025 CYCLON
# ee CYCLON
```

Adicione as linhas a seguir no final do arquivo que está sendo editado:

```
device cy0
device cy1 at isa? tty irq 9 iomem 0xd8000 iosiz 0x2000 vector cyintr
```

Para gravar as alterações, tecle “**Esc**”, depois “**Enter**”, e finalizando, a tecla “**a**”.

Para preparar o sistema, digite o seguinte comando:

```
# config CYCLON
```

e em seguida

```
# cd .././compile/CYCLON  
# make
```

Nota: no caso da utilização do POP-IN-A-BOX modelo 2, substitua a palavra **ET5025** por **GENERIC**.

Não estranhe as inúmeras mensagens surgidas na tela. Neste momento, o kernel do sistema estará sendo compilado. Após o término da compilação, digite o seguinte comando:

```
# make install
```

Reinicialize o computador (através da combinação Ctrl+Alt+Del) para que o novo kernel seja lido. Verifique se a placa está corretamente instalada através do seguinte comando:

```
# dmesg |grep cy
```

Uma mensagem semelhante a seguinte deverá ser exibida:

```
cy1 at irq 9 maddr 0xd8000 on isa
```

Perigo: alguns comandos, como **for**, só são implementados em shells como o **bash**; verifique se este foi instalado propriamente. O item **vii (Instalação de Algumas Aplicações Interessantes)** do capítulo 7 possui instruções para a instalação deste shell.

Em seguida, verifique se os *nós* correspondentes às saídas da sua placa multiseriada têm, respectivamente, uma entrada no diretório **/dev**. Caso contrário, crie-as da seguinte forma:

```
# cd /dev  
# for i in 0 1 2 3 4 5 6 7;do ./MAKEDEV cuac$i ttyc$i;done
```

No caso particular da Cyclom-8Yo, o acesso às portas seriais é feito através dos dispositivos: **/dev/ttycMN** (com **N** variando de 0 a 7 e **M** variando de 0 ao [número de controladoras Cyclades] - 1) para *dial-in* e **/dev/cuacMN** (com **N** variando de 0 a 7 e **M** variando de 0 ao [número de controladoras Cyclades] - 1) para *dial-out*. Estes nós precisam ser criados, pois eles não tem entrada no diretório **/dev**;

Configuração do Servidor PPP

- i. Verifique se o sistema tem suporte a PPP. Uma forma fácil de fazer isto é através do comando:

```
# netstat -i
```

Em algum lugar da saída, deverá aparecer uma ou mais linhas indicando, o suporte ao protocolo PPP. No exemplo abaixo, só existe um adaptador PPP configurado, o **ppp0**.

| Name | Mtu | Network | Address | Ipkts | Ierrs | Opkts | Oerrs | Coll |
|------|------|---------|---------|-------|-------|-------|-------|------|
| ppp0 | 1500 | 0 | 1 | 0 | 0 | 0 | 0 | |

- ii. Caso não apareça uma linha similar, será preciso configurar novamente o kernel, incluindo no arquivo de configuração do kernel, ou simplesmente retirando o caractere de comentário (#), caso ela já exista, a seguinte linha:

```
pseudo-device ppp X
```

onde **X** indica o número de adaptadores PPP que se deseja configurar. Será preciso um adaptador PPP para cada conexão simultânea a ser suportada pelo o sistema;

- iii. Verifique se o *daemon* PPP (**pppd**), programa que gerencia a implementação PPP a nível de kernel, se encontra no diretório **/usr/sbin**. Por *default*, ele é incluído no momento da instalação.

O *daemon* **pppd** pode trabalhar:

- como "cliente", no caso de conectar-se a algum sistema remoto via PPP;
 - como "servidor", no caso de estar conectado em rede e oferecer acesso remoto a usuários.
- iv. Constate a existência do diretório **/etc/ppp**. Caso ele não exista, deverá ser criado. Tanto o cliente quanto o servidor PPP, utilizam arquivos de configuração contidos neste diretório.
- v. As opções *default* do PPP são armazenadas no arquivo **/etc/ppp/options**. Nesse caso em particular, para configurar o sistema como servidor PPP, será preciso, no mínimo, as seguintes entradas:

```
crtstcts          # Controle de fluxo de hardware
domain pop.org.br # substituir pelo nome de seu domínio
passive           # espera por LCP
modem             # linha do modem
dns1 192.168.1.1  # substitua pelo IP do seu servidor DNS primário
dns2 192.168.1.5 #se existir, substitua pelo IP do seu servidor DNS
secundário
proxyarp         # usa roteamento ARP proxy
```

As opções *dns1* e *dns2* são utilizadas para resolver nomes de domínios.

A opção *proxyarp* cuida de todo o roteamento, de modo que tudo o que precisa ser feito para que sejam atribuídos endereços IP aos clientes remotos é colocar os clientes remotos na mesma sub-rede que o endereço IP do servidor PPP.

Nota: maiores informações sobre as opções do **pppd** poderão ser encontradas no manual *on-line*. Basta digitar:

```
# man pppd
```

- vi. Atribuir endereços IP a cada uma das saídas onde serão conectados os modems. No exemplo, foi seqüencialmente atribuído um endereço IP a cada porta (modem) e não ao usuário em si. A configuração utilizada foi:

```
IP do servidor PPP = 192.168.1.1
IP do modem-1 = 192.168.1.100 (Modem conectado à porta 1)
IP do modem-2 = 192.168.1.101 (Modem conectado à porta 2)
IP do modem-3 = 192.168.1.102 (Modem conectado à porta 3)
IP do modem-4 = 192.168.1.103 (Modem conectado à porta 4)
```

IP do modem-5 = 192.168.1.104 (Modem conectado à porta 5)
IP do modem-6 = 192.168.1.105 (Modem conectado à porta 6)
IP do modem-7 = 192.168.1.106 (Modem conectado à porta 7)
IP do modem-8 = 192.168.1.107 (Modem conectado à porta 8)

- vii. Para cada uma das saídas seriais, será necessário criar um arquivo **/etc/ppp/options.ttycMN** (com **N** variando de 0 a 7 e **M** variando de 0 ao [número de controladoras Cyclades] - 1), cujo único conteúdo será uma linha com o seguinte formato:

```
xxx.xxx.xxx.xxx:yyy.yyy.yyy.yyy      # IP's da máquina local (servidor PPP)  
                                       # e das máquinas remotas (clientes PPP)
```

Onde xxx.xxx.xxx.xxx, representa o IP do servidor PPP (ou seja, o servidor FreeBSD) e yyy.yyy.yyy.yyy representa o endereço IP de cada uma das saídas seriais onde conectam-se os clientes remotos.

No caso particular da multiseriada com 8 portas, os arquivos **options.MN** (com **N** variando de 0 a 7 e **M** variando de 0 ao [número de controladoras Cyclades] - 1), ficarão da seguinte maneira:

```
/etc/ppp/options.ttyc00:  
  
192.168.1.1:192.168.1.100  
  
/etc/ppp/options.ttyc01:  
  
192.168.1.1:192.168.1.101  
  
/etc/ppp/options.ttyc02:  
  
192.168.1.1:192.168.1.102  
:  
:
```

e assim por diante.

Configuração do Acesso *Dial-Up*

Habilitação do Usuário

- i. Siga o manual de instruções dos seus modems e conecte-os, em ordem indistinta, nas portas seriais da sua placa;
- ii. Crie, no arquivo **/etc/ttyd**, uma entrada para cada um dos modems. Este arquivo simplesmente lista todas as portas onde o sistema operacional espera *login*.

No caso da placa multiseriada Cyclom-8Yo, as linhas acrescentadas serão as seguintes:

```
ttyc00 "/usr/libexec/getty std.57600" dialup on insecure  
ttyc01 "/usr/libexec/getty std.57600" dialup on insecure  
ttyc02 "/usr/libexec/getty std.57600" dialup on insecure  
ttyc03 "/usr/libexec/getty std.57600" dialup on insecure  
:  
e assim por diante.
```

O primeiro campo **ttyc00** indica que a primeira porta serial da única Cyclom-8Yo (**/dev/ttyc00**) tem um modem conectado cuja velocidade de transmissão é de 57600 bps. O tipo de terminal para esta porta é "*dialup*", comumente utilizado para conexões *dial-up*. A porta foi habilitada (**on**) e caracterizada como insegura. Deste modo, não será possível fazer *login* como **root**, o que é, por questões de segurança, bastante recomendável.

As portas só poderão ser habilitadas (**on**), quando houver algum modem conectado a essa porta.

iii. Digite o seguinte comando:

```
# kill -HUP 1
```

Isto fará com que o processo **init**, processo que controla a inicialização do sistema, leia novamente o arquivo **/etc/ttys**. O processo **init** inicializará, então, os processos **getty** em todas as portas habilitadas (**on**).

iv. Verifique se os processos **login**, que acabaram de ser criados, se encontram realmente ativos. Isto é possível através do seguinte comando:

```
# ps -ax | grep  
ttyc
```

O sistema deverá exibir na tela, para cada uma das portas habilitadas, algo do tipo:

```
130 ?? | 0:00.02 /usr/libexec/getty std.57600 ttyc0
```

Criação do Usuário

Esta tarefa só poderá ser realizada pelo usuário *root*, caso contrário, surgirão mensagens de erro, indicando "*command not found*" ou "*permission denied*".

- i. Verifique se já existe o grupo no qual se deseja incluir o usuário *dial-up*. Para isto, procure o nome do grupo desejado no arquivo **/etc/group**.
 - Caso o grupo já tenha sido criado, o seu nome aparecerá no começo de uma das linhas do arquivo, no campo [nome_do_grupo]. Para maiores informações sobre este arquivo:

```
# man group
```

- Caso o grupo não tenha sido criado, faça-o antes de prosseguir com a inclusão de usuário, através do seguinte comando:

```
# groupadd dialuser
```

- ii. Digite, como super-usuário, o comando **adduser**. Surgirá uma mensagem similar à apresentada a seguir, com questões relacionadas ao usuário a ser criado. Responda conforme o exemplo:

```
(c) Copyright 1995 Wolfram Schneider
Use option ``-silent" if you don't want see all warnings & questions.
```

```
Check /etc/shells
Check /etc/master.passwd
User news: illegal shell: ``/nonexistent"
User xten: illegal shell: ``/nonexistent"
Check /etc/group
Enter your default shell: csh date no sh [sh]: <Enter>
Your default shell is: sh -> /bin/sh
Enter your default HOME partition: [/home]: <Enter>
Copy dotfiles from: /usr/share/skel no [/usr/share/skel]: no
Send message from file: /etc/adduser.message no
[/etc/adduser.message]: no
Do not send message
Use passwords (y/n) [y]: <Enter>
```

```
Write your changes to /etc/adduser.conf? (y/n) [n]: n
```

```
Ok, let's go.
Don't worry about mistakes. I will give you the chance later to correct any input.
Enter username [a-z0-9]: dial1
Enter full name []: Usuario DIAL-UP #1
Enter shell csh date no sh [sh]: Enter
Uid [1001]: 3001
Enter login class: default []: <ENTER>
Login group dial1 [dial1]: dialusers
Login group is "dialusers". Invite dial1 into other groups: guest no [no]: Enter
Enter password []: di@11
```

Repare que os campos em negrito e itálico, deverão adequar-se às suas necessidades.

- iii. Após ter criado o usuário **dial1**, no grupo **dialusers**, aparecerá a seguinte mensagem:

```
Name:dial1
Password: di@11
Fullname: Usuario DIAL-UP #1
Uid: 3001
Gid: 3000 (dialusers) *O GID é obtido do arquivo /etc/group
Groups: dialusers
HOME:/home/dial1
Shell: /bin/sh
OK? (y/n) [y]:
```

Confirme as informações apresentadas. A seguinte mensagem aparecerá na tela:
Added user "dial1".

iv. Diante da pergunta:

Add another user? (y/n) [y]: **Enter**

Digite "**Enter**" para aceitar a opção "**yes**", caso queira adicionar outro usuário.

Sugere-se que todos os usuários *dial-up* sejam colocados num único grupo.

v. Para cada usuário *dial-up* criado, será incluída automaticamente uma entrada nos arquivos **/etc/passwd** e **/etc/master.passwd**. Sendo que a única diferença entre esses arquivos é a exibição, ou não, da senha do usuário. A título de ilustração, é mostrada a seguir a entrada do usuário **dial1** no arquivo **/etc/passwd**:

```
dial1:*:3001:3000:Usuario DIAL_UP #1::/home/dial1
```

e no arquivo **/etc/master.passwd**:

```
dial1:$1$ptZpdRF9$YiAcBgFIdo58VhTOg.uAO1:3001:3000:UsuarioDIAL_UP
#1::/home/dial1
```

vi. Edite o arquivo de senhas utilizando o comando **vi** e, para cada um dos usuários *dial-up* criados, faça as seguintes mudanças:

- Esvazie o campo **home**, caso não queira que seus usuários tenham uma área de trabalho;
- Atribua **pppd** como *shell default*. Para tal, coloque **/usr/sbin/pppd** no lugar de **/bin/sh**. Deste modo, toda vez que o usuário executar *login* no seu servidor *Dial-Up*, a conexão PPP será automaticamente estabelecida.

Autenticação usando PAP

Caso a opção seja pela autenticação dos usuários via PAP (*Password Authentication Protocol*), deverá ser executado o seguinte procedimento:

i. Edite, como "root", o arquivo **/etc/ppp/options** e inclua a seguinte entrada:

```
+pap
```

Esta opção forçará a autenticação dos seus clientes via PAP.

ii. Crie o arquivo de autenticação **/etc/ppp/pap-secrets**

A autenticação através do PAP é baseada em senhas obtidas a partir deste arquivo. Cada linha no arquivo de autenticação contém, no mínimo, 3 campos, na seguinte ordem: cliente, nome_do_servidor e senha.

Para cada um dos seus usuários, crie uma entrada do tipo:

```
nome_do_usuario_1* senha_do_usuario_1
```

Portanto, considerando os usuários **dial1** e **dial2** com as respectivas senhas sendo **di@I1** e **di@I2**, as seguintes entradas deverão ser incluídas:

```
dial1 * di@I1
dial2 * di@I2
```

O caracter * no campo nome_do_servidor indica que pode ser aceito qualquer nome de servidor.

Se a senha provida pelo cliente não conferir com a senha constante no arquivo, a senha então é criptografada usando **crypt()** e comparada novamente com a senha do arquivo. Sendo assim, as senhas do arquivo de autenticação podem ser também armazenadas no formato criptografado.

Para maiores informações sobre este arquivo, veja a *manpage* do *pppd*, bastando digitar, na linha de comando:

```
# man pppd
```

- iii. Edite o arquivo **/etc/ttys** e, substitua cada uma das referências às saídas seriais da placa Cyclom-8Yo (**ttycMN**, com **N** variando de 0 a 7 e **M** variando de 0 ao [número de controladoras Cyclades] -1) por uma entrada similar a:

```
ttyc0 "/usr/sbin/pppd -detach 28800" dialup on insecure
```

No caso particular da placa multiseriada Cyclom-8Yo, as linhas:

```
ttyc00 "/usr/libexec/getty std.57600" dialup on insecure
ttyc01 "/usr/libexec/getty std.57600" dialup on insecure
ttyc02 "/usr/libexec/getty std.57600" dialup on insecure
ttyc03 "/usr/libexec/getty std.57600" dialup on insecure
:
:
```

e assim por diante, deverão ser substituídas por:

```
ttyc00 "/usr/sbin/pppd -detach 57600" dialup on insecure
ttyc01 "/usr/sbin/pppd -detach 57600" dialup on insecure
ttyc02 "/usr/sbin/pppd -detach 57600" dialup on insecure
ttyc03 "/usr/sbin/pppd -detach 57600" dialup on insecure
:
:
```

e assim por diante.

O primeiro campo **ttyc00** indica que a primeira porta serial da única Cyclom-8Yo (**/dev/ttyc00**) tem um modem conectado cuja velocidade de transmissão é de 57600 bps. O tipo de terminal para esta porta é *dialup*, comumente utilizado para conexões *dial-up*. A porta foi habilitada (**on**) e caracterizada como insegura, deste modo não será possível fazer *login* como *root*, o que é bastante recomendável por questões de segurança.

Não esqueça da opção **-detach**, caso contrário isto poderá gerar problemas quando o processo **init** for reinicializado.

- iv. Então reinicie o **init**, digitando o seguinte comando:

```
# kill -1
1
```

Isto forçará o processo **init** (processo que controla a inicialização do sistema) a ler novamente o arquivo **/etc/ttys**. O **init** inicializará, então, os processos **pppd** em todas as portas habilitadas (**on**).

- v. Verifique se os processos **pppd** que acabaram de ser criados se encontram realmente ativos. Isto poderá ser feito utilizando o seguinte comando:

```
# ps -ax | grep  
ttyp
```

O sistema deverá exibir na tela, para cada uma das portas habilitadas, algo do tipo:

```
130 c0 ls+0:00.02 /usr/sbin/pppd -detach ttyp00 57600
```

O resultado final é que não haverá uma sessão inicial à qual o usuário poderá acessar. Qualquer chamada recebida, inicializará imediatamente o servidor PPP, que por sua vez, usará PAP para autenticar o cliente.

Aspectos de Segurança

São evidentes as inúmeras vantagens que um servidor de comunicação oferece. No entanto, a implementação de um serviço deste tipo traz diversos riscos à sua rede local, tornando-a vulnerável a ataques. Com os sistemas de telefonia atuais, o simples fato de conectar seu modem na linha telefônica implica, em tese, que qualquer pessoa no mundo pode conectar-se a sua máquina.

É preciso, portanto, garantir que seus modems sejam instalados apropriadamente e, principalmente, garantir que eles façam exatamente o que se espera, nada além disso.

As seguintes recomendações pretendem tornar isso possível:

- i. Verifique as permissões dos arquivos de configuração (arquivos de comandos, valores de inicialização do PPP, etc.) dos *software* associados ao seu modem. Para tal, recomenda-se ler, cuidadosamente, a documentação de qualquer *manpage* associada ao *software*, pois normalmente é incluída uma seção chamada FILES na qual são listados os arquivos envolvidos.
- ii. As permissões dos dispositivos associados ao modem devem ser atribuídas de modo que os modems não possam ser acessados por usuários comuns. Normalmente, estas permissões devem obedecer o modo 600 (leitura e escrita somente para o dono), sendo que os donos poderão ser o usuário *root* ou *uucp*. É possível verificar os atributos e modos dos dispositivos utilizando o comando:

```
# ls -lg /dev/tty*
```

- iii. Certifique-se que, quando algo inesperado acontecer, o seu computador se comporte de uma forma "razoável". Por exemplo, se uma conexão telefônica for perdida, seu computador deverá "matar" os processos associados e desconectar o usuário, não permitindo ao próximo usuário que acessar remotamente, digitar comandos no *shell* do usuário anterior. Caso isto aconteça, seu modem pode estar configurado inapropriadamente.
- iv. Proteja fisicamente seus modems. Um intruso que ganhar acesso a sua linha telefônica, pode conectar o modem dele à linha e interceptar as suas ligações antes que elas atinjam o seu computador.

Problemas conhecidos

Ao longo dos vários procedimentos na configuração do servidor de comunicação, nos deparamos com algumas dificuldades. Em vista disso, foi elaborado um *troubleshooting*, cujo principal objetivo é auxiliar o usuário na solução de problemas:

- i. Caso o sistema não reconheça a sua placa Cyclom-8Yo, verifique se foi inserido, no arquivo de configuração do kernel, o seguinte comando:

```
device cy00 at isa? irq [IRQ_escolhido] iomem [endereço_escolhido]
iosiz 0x2000 vector cyintr
```

O IRQ e o endereço escolhidos não deverão estar em conflito com nenhum outro dispositivo já instalado. Caso esta entrada não tenha sido incluída, inclua-a e recompile o kernel.

- ii. Se após executar o comando:

```
# netstat -i
```

for verificado que o sistema não tem suporte a PPP, inclua a seguinte linha no arquivo de configuração do kernel [ou remova caractere de comentário (#)]:

```
pseudo-device ppp X
```

onde **X** indica o número de adaptadores PPP que se deseja configurar. Será preciso um adaptador PPP para cada conexão simultânea que o sistema suportará. Depois, recompila o kernel novamente.

- iii. Se o servidor de acesso não rotear os pacotes provenientes dos clientes PPP, verifique se a seguinte linha foi incluída no arquivo de configuração do sistema **/etc/rc.conf**. Caso não exista, esta linha deverá ser incluída.

```
gateway_enable = "YES"
```

- iv. Se os clientes PPP não conseguirem resolver os nomes de domínios, verifique se no arquivo de opções do servidor PPP **/etc/ppp/options** existe uma entrada indicando o servidor DNS primário (**dns1**) e, eventualmente, o servidor DNS secundário (**dns2**). Estas entradas propagam a informação para os clientes PPP. Caso o servidor primário (**dns1**) não tenha sido incluído, proceda com a sua inclusão.

Bibliografia

- Cyclom FAQ - <http://www.cyclades.com/techsup/faq000.html#y>

Capítulo 14

Considerações Finais

Esperamos que a leitura deste guia possa ter proporcionado uma forma eficaz de implementar o seu sistema Internet. No entanto, inúmeras outras aplicações podem ser implementadas para melhorar ou estender a funcionalidade do seu sistema. Entre elas podemos citar:

XWindows/XFree86

O XWindows é uma interface gráfica para os sistemas Unix, como o FreeBSD. Através desta interface, pode-se gerenciar de forma rápida e intuitiva todos os recursos do sistema.

Perigo: a configuração do XWindows requer certo cuidado, pois danos permanentes ao monitor de vídeo podem ocorrer caso uma configuração errônea seja feita.

O versão do XWindows para o FreeBSD se chama XFree86, e pode ser obtida no endereço <<http://www.xfree86.org/>>

SAMBA

O SAMBA é uma implementação do protocolo SMB (*Server Message Block*), e sua função básica é permitir o mapeamento dos recursos da rede do FreeBSD como se fossem nativos à rede Windows. Desta forma, pode-se copiar, mover, apagar ou gerenciar arquivos, ou utilizar impressoras do sistema FreeBSD como se fizessem parte da sua rede local.

Majordomo

O Majordomo é um gerenciador de listas de discussão, que são sistemas de distribuição de mensagens, via correio eletrônico, relacionadas com um determinado assunto.

Existem milhares de listas na Internet e cada uma tem um assunto. Ao assinar uma lista, o usuário passa a receber em sua caixa postal as mensagens enviadas pelos outros assinantes. Pode-se também enviar uma mensagem para a lista perguntando algo (dentro do assunto da lista, claro) ou respondendo a uma pergunta de outro assinante.

Instalando-se o Majordomo no seu sistema, você poderá criar suas próprias listas de discussão.

O Majordomo pode ser obtido através do seguinte endereço:
<<http://www.greatcircle.com/majordomo/>>

Bibliografia

- Managing Mailing Lists - Alan Schwartz - O'Reilly, 1998.
- XFree86 Available Documentation - <http://www.xfree86.org/3.3.2/index.html>
- SAMBA Web Pages - <http://samba.isca.uiowa.edu/samba/samba.html>

Anexo A

Obtendo os Software Utilizados

Os software utilizados neste guia, listados a seguir, podem ser obtidos no CD-ROM anexo.

- FreeBSD 2.2.5
- Apache 1.2.6
- Wu-FTP
- Sendmail 8.9.0
- *Driver* da placa ET-5025
- *Driver* da placa Cyclom-8Yo
- E outros...

Além disso, novas versões podem obtidas gratuitamente na Internet, nos endereços listados a seguir:

- FreeBSD: *<http://www.freebsd.org>*
- Centro de Informações da RNP: *<http://www.ci.rnp.br>*
- Free Software Foundation: *<http://www.gnu.org>*

Anexo B

Comandos Básicos do FreeBSD

Na lista abaixo, resumimos os comandos mais freqüentes utilizados em um sistema FreeBSD. Maiores informações podem ser obtidas através do manual on-line, acessado através da seguinte sintaxe:

man <comando>

| Sintaxe | Ação |
|---|---|
| awk/nawk [opção] <i>arquivo</i> | Procura por padrões em um arquivo e processa os resultados |
| cat [opção] <i>arquivo</i> | Concatena ou lista um arquivo |
| cd [diretório] | Muda o diretório corrente |
| chgrp [opção] <i>grupo arquivo</i> | Muda o grupo de um arquivo |
| chmod [opção] <i>arquivo</i> | Substitui as características de permissão de um arquivo ou diretório |
| chown [opção] <i>arquivo</i> | Substitui a característica de propriedade de um arquivo, somente podendo ser feito pelo administrador do sistema |
| cmp [opção] <i>arquivo1 arquivo2</i> | Compara dois arquivos e lista suas diferenças |
| compress [opção] <i>arquivo</i> | Comprime o arquivo e grava-o (##) como <i>arquivo.Z</i> |
| cp [opção] <i>arquivo1 arquivo2</i> | Copia <i>arquivo1</i> em <i>arquivo2</i> |
| date [opção] | Exibe a data e hora corrente |
| diff [opção] <i>arquivo1 arquivo2</i> | Compara dois arquivos texto e lista suas diferenças |
| du [opção] [<i>diretório or arquivo</i>] | Exibe o espaço em disco disponível |
| ed [opção] <i>arquivo</i> | Editor de linha de comando |
| emacs [opção] <i>arquivo</i> | Editor de tela inteira |
| file [opção] <i>arquivo</i> | Classifica o tipo de arquivo |
| find <i>diretório</i> [opção] [actions] | Procura arquivos por tipo ou padrão |
| finger [opção] | Exibe informações a respeito de usuários em máquinas locais ou remotas |
| ftp [opção] <i>host</i> | Transfere arquivos utilizando o FTP (Protocolo de Transferência de Arquivos) |
| grep [opção] 'string' <i>arquivo</i> | Procura pela ocorrência de uma string em um arquivo |
| gzip [opção] <i>arquivo</i> gunzip [opção] <i>arquivo</i> zcat [opção] <i>arquivo</i> | Comprime, descomprime ou lista arquivos. Os arquivos comprimidos são gravados com a terminação <i>.gz</i> |
| head [-n] <i>arquivo</i> | Exibe as (n) primeiras linhas de um arquivo |
| hostname | Exibe ou especifica (somente o administrador) o nome da máquina corrente |
| kill [opção] [-sinal] [pid#] [%job] | Envia um sinal ao processo (através do seu número de processo(pid#) ou número de controle de trabalhos (%n)), sendo que o padrão é a interrupção do processo. |
| ln [opção] <i>arquivo_fonte arquivo_alvo</i> | Estabelecer um link entre <i>arquivo_fonte</i> no <i>arquivo_alvo</i> |
| lpq [opção] lpstat [opção] | Exibe o status dos trabalhos de impressão |
| lpr [opção] <i>arquivo</i> | Imprime em uma impressora definida |

| | |
|---|--|
| lp [opção] <i>arquivo</i> | |
| lprm [opção] cancel [opção] | Remove um trabalho da lista de impressão |
| ls [opção] [<i>diretório</i> ou <i>arquivo</i>] | Lista o conteúdo de um diretório ou as características de permissão de arquivos |
| mail [opção] [usuário] mailx [opção] [usuário] Mail [opção] [usuário] | Utilitário simples para envio de mensagens de correio eletrônico |
| man [opção] <i>comando</i> | Exibe a sintaxe completa para um comando do FreeBSD |
| mkdir [opção] <i>diretório</i> | Cria um diretório |
| more [opção] <i>arquivo</i> less [opção] <i>arquivo</i> pg [opção] <i>arquivo</i> | Navega por um arquivo de texto |
| mv [opção] <i>arquivo1 arquivo2</i> | Move o <i>arquivo1</i> para <i>arquivo2</i> |
| passwd [opção] | Estabelece ou muda sua senha |
| ps [opção] | Exibe o status dos processos ativos |
| pwd | Exibe o diretório corrente |
| rcp [opção] <i>hostname</i> | Copia remotamente arquivos de uma máquina para outra |
| rlogin [opção] <i>hostname</i> | Estabelece uma conexão (login) em outra máquina |
| rm [opção] <i>arquivo</i> | Apaga um arquivo ou um diretório |
| rmdir [opção] <i>diretório</i> | Remove um diretório |
| script <i>arquivo</i> | Grava tudo o que aparece na tela em um arquivo de log até que o comando exit é executado |
| sort [opção] <i>arquivo</i> | Ordena as linhas de um arquivo |
| tail [opção] <i>arquivo</i> | Exibe as últimas linhas de um arquivo |
| telnet [host [port]] | Protocolo de comunicação para conexões remotas |
| uudecode [<i>arquivo</i>] | Decodifica um arquivo de formato uue |
| uencode [<i>arquivo</i>] <i>novo_nome</i> | Codifica um arquivo no formato uue (ASCII de 7 bits) |
| vi [opção] <i>arquivo</i> | Editor de tela inteira |
| who or w | Exibe a lista de usuários conectados e quais processos estão sendo executados |

Anexo C

Configurações suportadas pelo FreeBSD

O FreeBSD pode ser executado em sistemas que implementam os barramentos ISA, VLB, EISA e PCI, embora este último seja mais recomendado que os demais por razões de performance.

Perigo: máquinas baseadas no barramento MicroChannel não suportam o FreeBSD

Embora seja possível instalar o FreeBSD com um mínimo de 4MB de RAM, para os propósitos do projeto POP-IN-A-BOX, um mínimo de 32 MB é requerido.

São suportadas as seguintes controladoras de disco:

- WD1003 (any generic MFM/RLL)
- WD1007 (any generic IDE/ESDI)
- IDE
- ATA
- Adaptec 1505 ISA SCSI controller
- Adaptec 152x series ISA SCSI controllers
- Adaptec 1535 ISA SCSI controllers
- Adaptec 154x series ISA SCSI controllers
- Adaptec 174x series EISA SCSI controller in standard and enhanced mode.
- Adaptec 274x/284x/2940/2940U/3940 (Narrow/Wide/Twin) series EISA/VLB/PCI SCSI controllers
- Adaptec AIC7850 on-board SCSI controllers
- Adaptec AIC-6360 based boards, which includes the AHA-152x and SoundBlaster SCSI cards
- Buslogic 545S & 545c Note: that Buslogic was formerly known as "Bustek".
- Buslogic 445S/445c VLB SCSI controller
- Buslogic 742A/747S/747c EISA SCSI controller.
- Buslogic 946c PCI SCSI controller
- Buslogic 956c PCI SCSI controller
- NCR 53C810/53C815/53C825/53C860/53C875 PCI SCSI controller.
- NCR5380/NCR53400 ("ProAudio Spectrum") SCSI controller.
- DTC 3290 EISA SCSI controller in 1542 emulation mode.
- UltraStor 14F/24F/34F SCSI controllers.
- Seagate ST01/02 SCSI controllers.
- Future Domain 8xx/950 series SCSI controllers.
- WD7000 SCSI controllers.

Os seguintes drives de CD-ROM podem ser utilizados:

- SoundBlaster SCSI e ProAudio Spectrum SCSI (cd)
- Mitsumi (mcd)
- Matsushita/Panasonic (Creative) CR-562/CR-563 (matcd)
- Sony (scd)
- ATAPI IDE (wcd)

As seguintes placas de rede Ethernet são suportadas:

- Novell NE1000, NE2000 e NE2100

- Allied-Telesis AT1700 e RE2000 cards
- SMC Elite 16 WD8013, WD8003E, WD8003EBT, WD8003W, WD8013W, WD8003S, WD8003SBT, WD8013EBT e Elite Ultra
- DEC EtherWORKS III NICs (DE203, DE204 e DE205)
- DEC EtherWORKS II NICs (DE200, DE201, DE202 e DE422)
- DEC DC21040/DC21041/DC21140
- ASUS PCI-L101-TB
- Accton ENI1203
- Cogent EM960PCI
- Compex CPXPCI/32C
- D-Link DE-530
- DEC DE435
- Danpex EN-9400P3
- JCIS Condor JC1260
- Linksys EtherPCI
- Mylex LNP101
- SMC EtherPower 10/100 (Modelo 9332)
- SMC EtherPower (Modelo 8432)
- SMC EtherPower (2)
- Zynx ZX342
- DEC FDDI (DEFPA/DEFEA) NICs
- Fujitsu FMV-181 e FMV-182
- Fujitsu MB86960A/MB86965A
- Intel EtherExpress
- Intel EtherExpress Pro/100B 100Mbit.
- Isolan AT 4141-0 (16 bit)
- Isolink 4110 (8 bit)
- 3Com 3C501 cards
- 3Com 3C503 Etherlink II
- 3Com 3c505 Etherlink/+
- 3Com 3C507 Etherlink 16/TP
- 3Com 3C509, 3C579, 3C589 (PCMCIA) Etherlink III
- 3Com 3C590, 3C595 Etherlink III
- HP PC Lan Plus (27247B e 27252A)
- Toshiba
- Cartões PCMCIA da IBM e National Semiconductor.

Perigo: o FreeBSD ainda não suporta características plug-and-play de algumas placas citadas anteriormente, e desta forma, caso seja possível, esta característica deve ser desabilitada.

Anexo D

Aspectos sobre Segurança

O FreeBSD já é um sistema operacional com bom nível de segurança, mas alguns cuidados extras são bastante recomendáveis. A instalação de aplicativos de monitoramento, filtros, atualização de software e outros procedimentos são técnicas para manter a segurança de seu servidor, tentando impedir assim que ataques ao sistema tenham sucesso. Neste anexo, trataremos de alguns desses procedimentos básicos.

Recomendações Gerais

1) Como primeira recomendação geral, os seguintes serviços devem ser desabilitados no arquivo de configuração **/etc/inetd.conf** por serem serviços supérfluos e oferecerem risco a segurança do sistema.

- shell (rsh)
- login (rlogin)
- finger
- ntalk

2) É também recomendável que o administrador do sistema mantenha-se atualizado a respeito de problemas de segurança no FreeBSD. Duas boas fontes de informação são o próprio site do FreeBSD, onde são divulgados os "*FreeBSD Security Advisories*" (<<http://ftp.freebsd.org/pub/FreeBSD/CERT/index.html>>), e a lista de discussão brasileira sobre o FreeBSD (<<http://www.br.freebsd.org/lista.html>>).

3) Com relação a montagem de *filesystems* (sistemas de arquivos), é aconselhável que eles sejam sempre montados utilizando *flags* (marcadores) como nos exemplos abaixo:

```
/dev/sd0s1a on / (local)
/dev/sd0s1h on /home (local, nosuid)
/dev/sd0s1f on /tmp (local, nosuid)
/dev/sd0s1e on /usr (local)
/dev/sd0s1g on /var (local, nosuid)
procfs on /proc (local)
```

A *flag* **local** indica que o *filesystem* em questão só pode ser montado localmente, enquanto a *flag* **nosuid** indica que não podem ser executados comandos com SetUID.

No caso do XFree86, é recomendável que ele seja instalado somente em partições que sejam montadas com a opção **nosuid** explicada acima, e que ele seja chamado sempre utilizando-se o **/usr/X11R6/bin/xdm**.

4) O *Network Information System* (NIS) pode facilitar bastante a administração de uma rede com várias máquinas, mas também é muito prejudicial na questão de segurança. Evite utilizá-lo.

5) Para aumentar o nível de confiabilidade de seus *logs*, é interessante que o **syslogd** só registre mensagens locais (isto se sua máquina não for um *loghost*). Para tal, especifique a *flag* **-s** no arquivo **/etc/rc.conf** na linha **syslogd_flags**.

6) Deve-se tomar muito cuidado com a manipulação de senhas do sistema. Desde a escolha de senhas, armazenamento, até forma de passar essas senhas para outras pessoas. É comum a utilização de métodos de engenharia social (*CERT Advisory CA-91:04.social.engineering* - <ftp://ftp.cais.rnp.br/pub/info/cert_adv/CA-91:04.social.engineering>) por *hackers* para obtenção de senhas.

7) É de grande importância que se utilize conexões seguras na Internet. Hoje existem vários pacotes que proporcionam esse tipo de comunicação, sendo que o mais conhecido é o **ssh**. O **ssh** permite que se faça conexões tipo terminal (como **telnet** e **rlogin**, por exemplo) de forma segura, com um sistema de autenticação confiável e criptografia dos dados em trânsito. É uma ótima alternativa ao **telnet**. A versão mais atual do **ssh**, 1.2.25, pode ser encontrada em <ftp://ftp.unicamp.br/pub/security/tools/ssh>. Uma boa versão *shareware* do cliente **ssh** para *Windows* pode ser encontrada em <http://www.datafellows.com/>. O pacote compilado pode ser encontrado em <http://www.freebsd.org/ports>.

Devemos lembrar também que não existe sistema totalmente seguro. Um sistema é considerado seguro se for configurado corretamente, e principalmente, se houver atenção do administrador no que diz respeito a segurança e monitoramento do sistema.

Sistemas de segurança

Tcp wrappers

O **tcp wrappers**, ou **tcpd**, é um *software* que permite, além do monitoramento de serviços, implementar regras de acesso a esses serviços. Ele permite auditoria nos acessos através da geração de logs que indicam a origem do acesso, serviço acessado e se o acesso foi permitido ou negado.

O **tcpd** também pode bloquear conexões que tenham alguma característica estranha, como por exemplo, em casos onde o resultado de uma pesquisa de DNS direto e inverso não sejam consistentes.

Internamente, o **tcpd** atua entre o **inetd** e o **daemon** que responde pelo serviço, fazendo todas as checagens necessárias, gerando os *logs*, e depois repassando a conexão ao servidor, que responde normalmente como se tivesse sido chamado pelo **inetd**.

Instalação

A instalação do **tcp wrappers** é bastante simples. Basta instalar o pacote pré-compilado que pode ser encontrado no CD "*ports*" da distribuição do FreeBSD. Montando-se o *cdrom*, basta adicionar o pacote:

```
# mount /cdrom
# pkg_add /cdrom/packages/net/tcp_wrappers-*.tgz
```

Para que o **tcpd** funcione perfeitamente, deve-se alterar a configuração do *daemon inetd (/etc/inetd.conf)* para que o **tcpd** intercepte as conexões antes do *daemon* responsável pelo serviço.

O sexto campo das linhas do arquivo **/etc/inetd.conf** indica o **path** completo do servidor que responde pelo serviço. Para que o **tcpd** intercepte as conexões, ele é quem deve ser chamado, ao invés do servidor, e para isso as linhas referentes aos serviços que ele monitorará devem ser alteradas como no exemplo abaixo:

Linha original:

```
telnet stream tcp    nowait root    /usr/libexec/telnetd    telnetd
```

Linha após alteração:

```
telnet stream tcp nowait root /usr/local/libexec/tcpd /usr/libexec/telnetd
```

Utilizamos nesse exemplo o serviço de **telnet**, mas essa alteração pode ser feita para a maioria dos serviços controlados pelo **inetd**.

Após a alteração feita no **/etc/inetd.conf**, basta que o *daemon* **inetd** seja re-inicializado para que o **tcpd** entre em ação.

```
# kill -1 `cat /var/run/inetd.pid`
```

Os *logs* gerados pelo **inetd**, se utilizado o pacote pré-compilado que acompanha a distribuição do FreeBSD, serão gerados com prioridade **auth** e facilidade **info**, ou seja, o **syslogd** gravará os *traps* no arquivo que receba as mensagens do tipo **auth.info** (verifique no arquivo de configuração do **syslogd**, **/etc/syslog.conf**, onde essas mensagens estão sendo gravadas).

O controle de acesso implementado pelo **tcp wrappers** aos serviços é configurado através de dois arquivos colocados no diretório **/usr/local/etc**. No arquivo **hosts.allow**, são colocados os **hostnames**, redes, domínios ou IPs (entre outras opções) que podem acessar cada serviço, e no **hosts.deny**, as mesmas configurações referentes a quem não deve acessar cada serviço.

Segue abaixo um exemplo de cada um desses arquivos:

```
/etc/hosts.allow
```

```
/usr/libexec/ftpd: LOCAL,.rnp.br  
/usr/libexec/telnetd: LOCAL, .rnp.br, 172.18.10.  
/usr/libexec/fingerd: LOCAL  
/usr/local/libexec/popper: LOCAL
```

```
/etc/hosts.deny
```

```
ALL: ALL: spawn /usr/local/bin/alarm %d %h %u %a &
```

O exemplo do **hosts.deny** acima bloqueia tudo que não foi permitido explicitamente no **hosts.allow**, utilizando uma outra opção do **tcpd** que pode ser encontrada no manual que acompanha o pacote, executando um programa arbitrário utilizando argumentos fornecidos pelo **tcpd** (como *data*, *horário*, *username* e *serviço*) quando alguma conexão for recusada.

É aconselhável que o usuário leia atentamente a página **man** que acompanha o **tcpd** para que possa usufruir de todas as *features* desse *software*.

IP Firewall

O *firewall* nativo do FreeBSD é um filtro de pacotes que permite que o administrador do sistema controle e restrinja de forma eficaz o que vai acessar ou não a rede interna em questão, assim como o que vai ser acessado nesse sistema. Além de controle, o **ipfw** gera registros de forma a permitir que o administrador monitore o que tem sido acessado no servidor, através de *logs* bem completos.

Implementação

A implementação do **ipfw** é feita no kernel, e para isso, ele deve ser re-compilado. Já a configuração das listas de acesso (*access lists*) é feita através de comandos no *prompt*, ou, como normalmente é feita, através de um arquivo **batch** executado durante o *boot* da máquina.

Abaixo temos as instruções para geração do kernel com suporte ao **ipfw**:

- Para preparar a configuração para recompilação do kernel com suporte ao **ipfw**, é necessário que as três linhas abaixo sejam colocadas no arquivo de configuração.

```
options      IPFWALL           #habilita o firewall
options      IPFWALL_VERBOSE   #ativa sistema de logs para o firewall
options      "IPFWALL_VERBOSE_LIMIT=100" #limita a 100 o número máximo de
# logs de um mesmo tipo
```

Para fazer essas inclusões, no diretório **/usr/src/sys/i386/conf**, digite o seguinte comando:

```
# cp GENERIC IPFW; grep IPFWALL LINT >> IPFW;
```

- Configure e compile o novo kernel com os seguintes comandos:

```
# config IPFW
# cd ../../compile/IPFW
# make
# make install
```

Tendo então o novo kernel sido gerado e instalado, o administrador deverá configurar o **syslogd** para armazenar os *logs* gerados pelo **ipfw**. Para isso, bastará incluir a seguinte linha na configuração do **syslogd (/etc/syslog.conf)**, e a criação do arquivo que receberá os *logs*:

Inclusão no **syslog.conf**:

```
kern.crit                /var/log/ipfw.log
```

Criação do arquivo de *log*:

```
# touch /var/log/ipfw.log
```

Seria interessante que o administrador incluísse o arquivo de *log* do **ipfw** no sistema de rotação de *logs*, executado pelo **newsyslog**. Para isso, edite o arquivo **/etc/newsyslog.conf**, incluindo a seguinte linha ao final do mesmo:

```
/var/log/ipfw.log 644 7 * 168 Z
```

Essa linha fará com que o **newsyslog** faça rotação do arquivo de *log* do **ipfw** uma vez por semana, comprimindo o arquivo antigo. Serão mantidos os 7 últimos arquivos de *log* do **ipfw**, e estes serão mantidos com opção de leitura global. Para obter mais informações sobre o **newsyslog**, verifique sua página **man**.

O próximo passo é a inclusão das regras de acesso (ou listas de acesso) na configuração do *firewall*. Abaixo temos um exemplo de configuração completa. Nesse exemplo, cada linha foi comentada para que o usuário possa entender como são feitas as listas de acesso e possa customizá-la de maneira a melhor adaptá-la a realidade de seu site. Essas regras devem ser colocadas em um arquivo no diretório **/etc**.

Nesse exemplo, vamos supor que o endereço da rede do usuário seja 172.18.10.0/24, e que o endereço IP do servidor seja 172.18.10.3.

É aconselhável que o leitor tenha lido antes a página **man** do **/sbin/ipfw** para que possa entender a sintaxe das linhas abaixo.

```
# Permite a saída de qualquer pacote com origem no servidor;  
add 00001 allow ip from 172.18.10.3 to any
```

```
# Permite o tráfego de qualquer conexão que já tenha sido estabelecida;  
add 00002 allow tcp from any to any established
```

```
# Bloqueia qualquer pacote com origem na rede interna com endereço de origem  
# diferente de 172.18.10.x (bloqueio de IP spoofing), gerando logs das conexões;  
add 00003 deny log ip from not 172.18.10.0/24 to any out
```

```
# Bloqueio de qualquer pacote com origem na rede externa que tenha endereço de  
# origem igual a 172.18.10.x (também bloqueio de spoofing), gerando logs e estes  
# serão mantidos com opção de leitura global.  
# Para obter mais informações sobre o newsyslog, verifique sua página man das  
# conexões;  
add 00004 deny log ip from 172.18.10.0/24 to any in
```

```
# Bloqueio de pacotes ICMP (ping, por exemplo) com destino ao endereço de  
# broadcast da rede interna (bloqueio a smurf), gerando logs das conexões.  
# Cuidado: se seu netmask for diferente de 255.255.255.0, a configuração para  
# bloqueio desse tipo de ataque será diferente;  
add 00005 deny log icmp from any to 172.18.10.255
```

```
# Permite pacotes ICMP para a rede interna e externa;  
add 00006 allow icmp from any to any
```

```
# Permite conexões na porta 20/tcp (ftp-data);  
add 00007 allow tcp from any to 172.18.10.3 20
```

```
# Permite conexões na porta 21/tcp (ftp);  
add 00008 allow tcp from any to 172.18.10.3 21
```

```
# Permite conexões na porta 22/tcp (ssh);  
add 00009 allow tcp from any to 172.18.10.3 22
```

```
# Permite conexões na porta 23/tcp (telnet) desde que com origem na rede  
# interna;  
add 00010 allow tcp from 172.18.10.0/24 to 172.18.10.3 23
```

```
# Permite conexões na porta 25/tcp (SMTP - sendmail);  
add 00011 allow tcp from any to 172.18.10.3 25
```

```
# Permite pacotes direcionados a porta 53/udp (DNS);  
add 00012 allow udp from any to 172.18.10.3 53
```

```
# Permite conexões na porta 80/tcp (www);  
add 00013 allow tcp from any to 172.18.10.3 80
```

```
# Permite conexões na porta 110/tcp (pop3) desde que com origem na rede interna;  
add 00014 allow tcp from 172.18.10.0/24 to 172.18.10.3 110
```

```

# Permite conexões na porta 113/tcp (ident);
add 00015 allow tcp from any to 172.18.10.3 113

# Bloqueia pacotes direcionados a porta 2049/udp e tcp (NFS);
add 00016 deny ip from not 172.18.10.0/24 to 172.18.10.0/24 2049

# Bloqueia conexões nas portas de 6000 a 6010 (XWindows);
add 00017 deny tcp from any to 172.18.10.3 6000-6010

# Permite pacotes tcp e udp que sejam direcionados a portas não-privilegiadas;
add 00018 allow tcp from any to 172.18.10.0/24 1023-65535
add 00019 allow udp from any to 172.18.10.0/24 1023-65535

# Bloqueia o tráfego de netbios;
add 00020 deny tcp from any to any 137-139
add 00021 deny udp from any to any 137-139

# Faz accounting (contagem) de início de conexões tcp direcionadas a portas não-
# privilegiadas;
add 00022 count tcp from any to any 1024-65535 in setup

# Permite conexões ao endereço de localhost (127.0.0.1) que sejam através
# da interface de loopback;
add 00023 allow ip from any to 127.0.0.1 via lo0

# Bloqueia tudo que não foi explicitamente permitido nas regras acima, gerando
# logs do que for bloqueado;
add 20000 deny log ip from any to any

```

Apos a geração do arquivo de regras, o administrador (usuário) deverá alterar o arquivo **/etc/rc.conf** para que estas regras sejam carregadas no *boot* da máquina.

Para isso, o arquivo **/etc/rc.conf** deverá ser editado, e o nome do arquivo com as regras deverá ser apontado pela opção **firewall_type**, como no trecho de exemplo abaixo do arquivo **/etc/rc.conf** (supondo que o arquivo de regras tenha sido gravado como **/etc/ipfw.rules**):

```

[...]
#### Basic network options: ###
hostname="pob.lct.rnp.br"    # Set this!
nisdomainname="NO"          # Set to NIS domain if using NIS (or NO).
firewall_enable="YES"       # Set to YES to enable firewall functionality
firewall_type="/etc/ipfw.rules" # Firewall type (see /etc/rc.firewall)
firewall_quiet="NO"         # Set to YES to suppress rule display
tcp_extensions="YES"
[...]

```

Completados todos esses passos, a máquina deverá ser reinicializada para que o **ipfw** entre em funcionamento.

Nota: Não é aconselhável que a configuração do *firewall* seja feita em qualquer terminal que não seja o *console* da máquina.

Anexo E

Configurando a Rede TCP/IP

Protocolo IP - Endereçamento, ARP, RARP e ICMP

O TCP/IP possui um sistema de endereçamento único que permite aos usuários e às aplicações identificarem um *host* ou uma rede para se comunicarem. Ele fornece padrões para endereçamento de redes, sub-redes, *hosts*, e para uso de endereços especiais para *broadcast*, *multicast* e *loopback*.

O endereço IP atual (IP versão 4) é formado por um campo de 32 bits, dividido em 4 octetos (bytes) e representados por quatro números decimais separados por ponto, como mostrado no exemplo a seguir na forma binária e decimal:

11000000 10101000 00000001 00001010
192 168 1 10

Conceitualmente, o endereço é dividido em duas partes: o endereço de rede (**netid** - *network identifier*), à qual o *host* está conectado, e o endereço de *host* (**hostid** - *host identifier*). Por convenção, o endereço de *host* 0 (zero) é designado para representar a própria rede.

Classes de Endereços

Há cinco classes de endereços IP que são as classes A, B, C, D e E. A classe E está reservada para uso futuro. As diferentes classes de endereços são obtidas através da forma de alocação dos 32 bits. Na prática, cada endereço IP possui uma das formas apresentadas na figura a seguir.

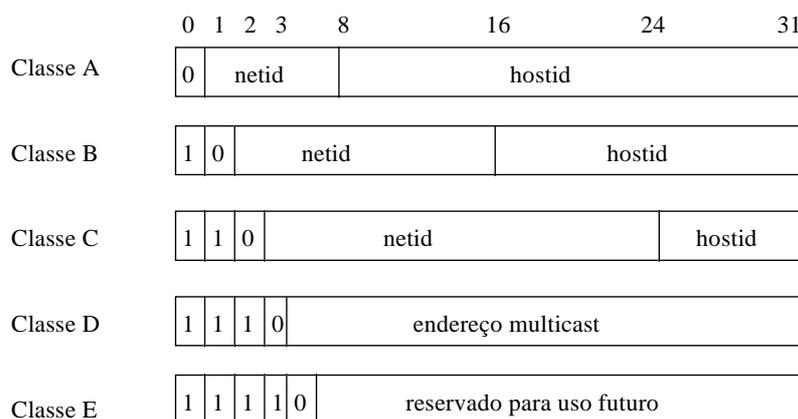


Figura 2.8.1 - Classes de Endereços IP

Assim, tem-se então a seguinte alocação de endereços:

- 0 - reservado;
- Classe A: de 1 a 126 - quantidade de redes 126, quantidade de *hosts*/rede 16.777.214;

- 127 - Reservado - interface *loopback*;
- Classe B: de 128 a 192 - quantidade de redes 16.384, quantidade de *hosts/rede* 65.534;
- Classe C: de 192 a 223 - quantidade de redes 2.097.152, quantidade de *hosts/rede* 254;
- Classe D: 224 - reservado (*Multicasting*);
- Classe E: de 225 a 255 - reservado.

ARP e RARP

O protocolo ARP (*Address Resolution Protocol*) mapeia endereços IP em endereços de *hardware* (MAC address), permitindo que, dado o endereço IP, uma máquina obtenha dinamicamente, através de *broadcast*, o endereço MAC de uma máquina remota.

O RARP (Reverse ARP) mapeia endereços de *hardware* (MAC address) em endereços IP. Permite que uma estação *diskless* ou uma máquina sem IP obtenha seu próprio endereço IP de um servidor.

ICMP

O ICMP (*Internet Control Message Protocol*) é um componente do protocolo IP, que fornece um mecanismo de controle, permitindo à máquina destino reportar mensagens de erros à máquina de origem. A exemplo do comando **ping**, as aplicações das camadas superiores usam essa informação para tomar medidas corretivas.

Interfaces de Redes

Cada dispositivo conectado à rede possui uma interface a qual estão associados um nome e um endereço IP. Por exemplo, interfaces Ethernet, ATM ou Serial (Frame Relay, HDLC, PPP ou SLIP).

Se um dispositivo possui mais de uma interface de rede, cada interface deve pertencer a redes ou sub-redes diferentes, ou seja, os endereços IP devem ser de redes ou sub-redes diferentes. Mas há exceções, por exemplo, alguns roteadores aceitam a configuração de um mesmo IP em duas interfaces diferentes (exemplo: Ethernet e Serial).

Comandos arp, ifconfig e netstat

arp - Em sistemas Unix, este comando mostra e modifica a tabela de conversão de endereços Internet (IP) para endereços MAC Ethernet, usada pelo protocolo de resolução. O comando a seguir mostra todos os registros da tabela ARP:

```
# arp -a,
```

ifconfig - este comando é usado para configurar uma interface de rede, associando um endereço e outros parâmetros à interface do Unix. Também pode ser utilizado para mostrar a configuração corrente da interface. Por exemplo:

```
# ifconfig ed1 "inet 192.168.1.1 netmask 255.255.255.0"
```

Este comando configura e ativa a interface com estes parâmetros. O **ifconfig** deve ser utilizado durante a inicialização do sistema para definir o endereço IP de cada interface e, posteriormente, pode também ser utilizado para redefinir ou mudar estes endereços.

netstat - mostra informações e estatísticas, em vários formatos, de diversas estruturas de dados relacionadas à rede. Dentre as várias opções do comando relacionadas às interfaces de rede, tem-se:

```
# netstat -l ed1
```

que mostra o estado da interface **ed1**, ou ainda

- -i , que mostra o estado das interfaces que são usadas para tráfego TCP/IP;
- -p, que mostra a tabela ARP.

Sub-redes

O endereçamento por sub-redes permite a divisão de uma única rede em várias sub-redes, compartilhando o mesmo endereço de rede (*netid*). Por exemplo, uma instituição pode ter apenas um endereço de rede, que é conhecido externamente, e internamente este endereço pode ser dividido em várias sub-redes departamentais.

Máscara de Rede - *Netmask*

Para a criação de sub-redes , a parte do endereço de *host* (*hostid*) é dividida em duas partes, uma que identifica a sub-rede e outra que identifica o *host*. Esta divisão é realizada através da máscara de rede. A seguir é apresentado um exemplo de como uma rede Classe C pode ser dividida em algumas sub-redes.

Exemplo: Suponha que uma instituição possui 5 departamentos e receba o endereço de rede Classe C 192.168.1.0. Esta instituição poderá dividir o endereço de rede e alocar uma sub-rede independente para cada departamento. Neste caso, o endereço de rede 192.168.1.0 pode ser dividido em 8 (2^3) sub-redes, utilizando os 3 bits mais significativos do último byte da máscara original, com cada sub-rede possuindo 32 (2^5) endereços de *hosts* (os 5 bits restantes). A máscara resultante passa a ser:

Último byte

11111111 11111111 11111111 ,111,00000, = 255.255.255.224.

sub-rede hosts

Tem-se, então, as seguintes sub-redes:

Sub-rede 0: Não deve ser utilizada.

Sub-rede 32

- 192.168.1.32 - identifica a sub-rede;
- 192.168.1.(de 33 a 62) - endereços IP para os *hosts* da sub-rede;
- 192.168.1.63 - utilizado como endereço de *broadcast* da sub-rede.

Sub-rede 64

- 192.168.1.64 - identifica a sub-rede;
- 192.168.1.(de 65 a 94) - endereços IP para os *hosts* da sub-rede;
- 192.168.1.95 - utilizado como endereço de *broadcast* da sub-rede.

Sub-rede 96

- 192.168.1.96 - identifica a sub-rede;
- 192.168.1.(de 97 a 126) - endereços IP para os *hosts* da sub-rede;
- 192.168.1.127 - utilizado como endereço de *broadcast* da sub-rede.

Sub-rede 128

- 192.168.1.128 - identifica a sub-rede;
- 192.168.1.(de 129 a 158) - endereços IP para os *hosts* da sub-rede;
- 192.168.1.159 - utilizado como endereço de *broadcast* da sub-rede.

Sub-rede 160

- 192.168.1.160 - identifica a sub-rede;
- 192.168.1.(de 161 a 190) - endereços IP para os *hosts* da sub-rede;
- 192.168.1.191 - utilizado como endereço de *broadcast* da sub-rede.

Sub-rede 192

- 192.168.1.192 - identifica a sub-rede;
- 192.168.1.(de 193 a 222) - endereços IP para os *hosts* da sub-rede;
- 192.168.1.223 - utilizado como endereço de *broadcast* da sub-rede.

Sub-rede 224 - Não deve ser utilizada.

Anexo F

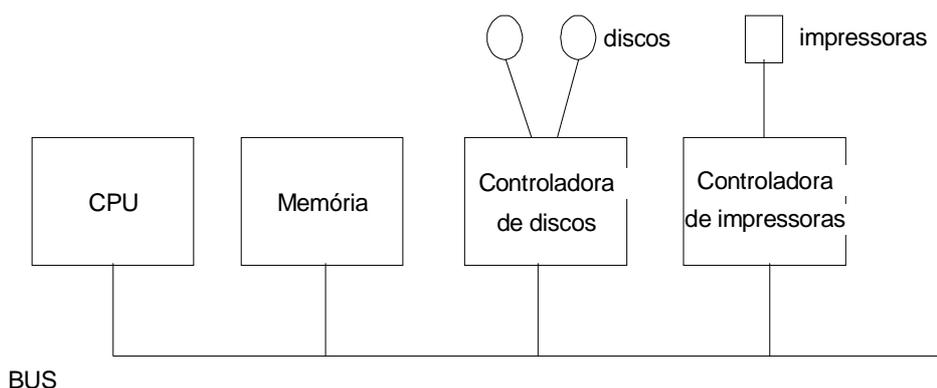
Configurações avançadas de dispositivos e problemas mais comuns

Para um perfeito funcionamento do POP-IN-A-BOX, são explicados os procedimentos sobre como as diversas controladoras de dispositivos e o sistema operacional devem ser configurados, e como um disco rígido é organizado para uso pelo sistema.

Configuração de *Hardware*: IRQs, DMA, I/O Addr e Ports

Um computador utiliza-se de diversos dispositivos que expandem a capacidade do equipamento possibilitando, além do processamento, a realização de outras tarefas como impressão, armazenamento de informações, comunicação com o ser humano e com outros computadores, etc. Estas tarefas são realizadas por dispositivos especializados para tal fim, como impressoras, discos, monitores de vídeo, teclados, mouses, e placas de rede. Estes dispositivos são ligados aos computadores via circuitos eletrônicos chamados controladoras.

Em geral, essas controladoras são placas de circuito impresso conectadas aos *slots* de barramento dos computadores, mas torna-se cada vez mais freqüente a produção de computadores com muitas controladoras incluídas na própria placa principal do equipamento. As controladoras "conversam" com a CPU via barramento do computador, como esquematizado na figura a seguir.



Esquema de Barramento do Microcomputador

A "conversa" entre a CPU e as controladoras, através do barramento, se dá utilizando quatro métodos não mutuamente exclusivos: via *ports*, interrupções, DMA e memória de E/S.

Ports - são registradores especiais de 1 byte utilizados por algumas controladoras. Seus identificadores, os *port addresses*, em geral são representados por dois bytes na forma hexadecimal. Por exemplo, 0x3f8-0x3ff indica que tal controladora está usando 8 *ports* da 0x3f8 até a 0x3ff. Este é um exemplo comumente utilizado pela UART (*Universal Asynchronous Receiver and Transmitter*), a controladora serial, para a *sio0* (COM1). Um *port* não pode ser compartilhado entre controladoras.

Interrupções - são utilizadas por algumas controladoras para indicar à CPU que algum evento ocorreu, como a chegada dos dados previamente solicitados, por exemplo. No total tem-se 15 interrupções, da *Interrupt Request* (IRQ) 1 até a 15, mas infelizmente algumas são reservadas. A Tabela a seguir indica as utilizações mais comuns das IRQs:

| IRQ | UTILIZAÇÃO |
|-----|--------------------------|
| 1 | Teclado |
| 2 | Mesma IRQ 9 |
| 3 | COM2 |
| 4 | COM1 |
| 5 | |
| 6 | Floppy |
| 7 | LPT1 |
| 8 | Timer |
| 9 | |
| 10 | |
| 11 | |
| 12 | PS/2 Mouse (se presente) |
| 13 | Float Point |
| 14 | 1ª. IDE |
| 15 | |

Tabela - Alocação Mais Comum para as IRQs

Embora algumas controladoras permitam o compartilhamento de uma IRQ, em geral, utiliza-se uma IRQ para cada controladora. Portanto, um PC genérico dispõe de 5 a 6 IRQs para alocar outras controladoras, nem sempre comuns, mas que poderão ser utilizadas no POP-IN-A-BOX, como placas Ethernet, SCSI, multiseriadas e placa serial síncrona. Um exemplo factível para alocação dessas interrupções restantes é:

IRQ 5 - Ethernet
 IRQ 9 - Serial Síncrona
 IRQ 10 - Multiserial
 IRQ 11 - SCSI

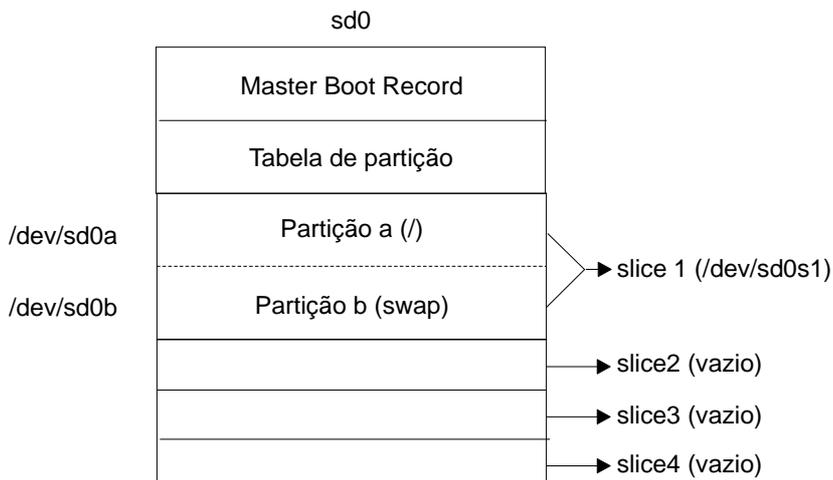
DMA - Algumas controladoras podem escrever e ler diretamente em qualquer lugar da memória RAM, conforme indicado pela CPU. Para que essa operação seja realizada sem a intervenção do processador, liberando-o para outras atividades mais nobres, essas controladoras fazem uso de um mecanismo chamado *Direct Memory Access* (DMA). O DMA, no barramento ISA, possui 7 canais para comunicação com a CPU, por onde são indicados os espaços de memória a serem utilizados. Não é possível o compartilhamento de canais de DMA entre duas controladoras. Nesse caso, felizmente, apenas a controladora de floppy utiliza um canal fixo, o *DMA Request* (DRQ) 2. Outras controladoras que costumam utilizar um DRQ são algumas SCSI e algumas placas de rede.

On Board Memory - Finalmente, a quarta forma de comunicação entre a CPU e as controladoras é através de *On-Board Memory*. Geralmente localizadas entre os endereços 0xa0000 e 0xefff, essas memórias, embora localizem-se nas placas controladoras, funcionam como se fizessem parte da memória RAM. Nesses casos, não apenas o endereço inicial da memória é especificado (maddr), mas também o tamanho dessa memória (msize). Evidentemente, também não pode haver compartilhamento de memória entre duas controladoras. As controladoras mais comuns dos PCs não utilizam este método. No caso do POP-IN-A-BOX, algumas controladoras multiseriadas e síncronas o utilizam.

É importante que, ao acrescentar novas placas ao seu micro, as suas configurações sejam de tal forma que não haja conflito com nenhum dos quatro parâmetros apresentados. Será visto na seção "Procedimentos para Instalação", a possibilidade de fazer eventuais reajustes nos parâmetros *default* de cada controladora no núcleo (kernel) do FreeBSD.

Configuração de Disco

Um disco físico no PC pode ser dividido em até quatro segmentos lógicos, chamados *slices* (no DOS chama-se partições). Cada *slice* no FreeBSD pode abrigar até 8 partições, que funcionarão como discos lógicos independentes. Cada *slice* pode conter um sistema operacional diferente, permitindo que um computador hora seja inicializado com um sistema, hora com outro. O POP-IN-A-BOX utiliza apenas um sistema operacional, assim utiliza-se apenas o *slice* 1. Esquemáticamente tem-se:



Divisão de um Disco no FreeBSD

Outras partições podem ser criadas, buscando dar maior organização ao sistema de arquivo e maior facilidade de *backup*. A configuração com apenas duas partições, uma para todo o sistema de arquivos (/) e outra para o *swap*, visa apenas facilitar a utilização do sistema de arquivos, poupando o leitor da responsabilidade de bem dimensionar as partições no instante da instalação do sistema operacional.

Problemas com a Placa de Rede

Se durante o *boot*, a inicialização da placa apresentar a mensagem *device timeout*, verifique se a placa está configurada para trabalhar com os mesmos parâmetros encontrados no config (IRQ, DMA e I/O Mem). Para alterar os valores da placa, altere os *jumpers* na mesma, e caso ela não os tenha, utilize o *software* de configuração que deve acompanhar a placa.

Para reconfigurar a placa de rede no FreeBSD, caso esta ainda continue apresentando este problema, faça o seguinte:

Reinicie seu computador. Quando aparecer "*Boot*:" entre com "-c" seguido de <Enter>: Com isto, o sistema entrará em modo de **config**.

```
config>port <ed0 ou ed1> <endereço>
config> irq <ed0 ou ed1> <número>
config> enable <ed0 ou ed1>
config> quit
```

Respectivamente, a sequência de comandos acima altera o endereço da interface, altera a IRQ, habilita a mesma e sai com **config**, continuando com a inicialização da máquina.

Instalação e Configuração do *Hardware*

Esta seção irá apresentar, em linhas gerais, os passos que devem ser seguidos para a correta configuração da ET-5025. Inicialmente, deve-se verificar alguns atributos de hardware, como a escolha correta das interrupções (IRQs) utilizadas pelo seu sistema. As interrupções possíveis de se configurar nesta placa são 2, 3, 4, 5, 7, 10, 11 e 15, sendo que a padrão é a 5. Após a escolha da IRQ, altere os *jumpers* próprios na placa. Use o manual para saber onde encontrar os *jumpers* e como posicioná-los. Lembre-se de anotar a IRQ escolhida, pois este dado será necessário para a configuração.

Escolha do Endereço da Memória Principal

A placa ET-5025 necessita de 32 Kb da memória principal para funcionar. Os endereços que podem ser usados como endereços base para esta memória são: 0xA0000, 0xA8000, 0xB0000, 0xB8000, 0xC0000, 0xC8000, 0xD0000, 0xD8000, 0xE0000, 0xE8000.

Encontre, dentre os endereços listados acima, algum que esteja livre e configure os *jumpers* para o endereço escolhido, mais uma vez orientando-se pelo manual. Anote o endereço escolhido.

Atenção: deve-se tomar bastante cuidado, pois o endereço que vem configurado de fábrica é conflitante com o endereço da placa Cyclades 8Yo, usada no módulo Servidor de Comunicação.

Escolha do Endereço da Memória de Entrada e Saída

A placa ET-5025 também necessita de 32 bytes da memória de entrada e saída para funcionar. Os endereços que podem ser usados como endereços base para esta memória são: 0x200, 0x220, 0x240, 0x260, 0x280, 0x2A0, 0x2C0, 0x2E0, 0x300, 0x320, 0x340, 0x360, 0x380, 0x3A0, 0x3C0, 0x3E0.

Agora, serão listadas as utilidades de cada uma destas faixas de endereços. Isso pode servir como uma pista para descobrir qual destas não está sendo usada:

- 200-21F geralmente é usada pela porta de jogos do PC;
- 220-23F muito usada por placas de som;
- 240-25F não é usada - é o endereço que vem configurado de fábrica;
- 260-27F não é usada;
- 280-29F não é usada;
- 2A0-2BF não é usada;
- 2C0-2DF não é usada;
- 2E0-2F0 usada pelas portas seriais do PC - COM2 e COM4;
- 300-31F em geral é usada pelas placas de rede;
- 320-33F muito usada por placas de som;
- 340-35F não é usada;
- 360-37F usada pela porta paralela do PC - LPT1;
- 380-39F muito usada por placas de som;
- 3A0-3BF usada pela placa de vídeo do PC;
- 3C0-3DF usada pela placa de vídeo do PC;
- 3E0-3F0 diversos usos no PC - não usar este endereço.

Uma vez escolhido o endereço de entrada e saída, configure os *jumpers* de acordo com o manual e anote o endereço escolhido.

Anexo G

Glossário

Acrônimo: termo formado pelas primeiras letras de uma das palavras de uma frase. Por exemplo, a ferramenta de busca em sites Gopher se chama VERONICA - *Very Easy Rodent-Oriented Net-wide Index to Computerized Archives*.

Agent: Um programa de computador ou processo que opera sobre uma aplicação cliente ou servidor e realiza uma função específica, como uma troca de informações.

Alias: Significa segundo nome, ou apelido. Pode referenciar um endereço eletrônico alternativo de uma pessoa ou grupo de pessoas, ou um segundo nome de uma máquina. É também um dos comandos básicos do UNIX.

Âncora: é um termo utilizado na especificação da linguagem HTML e significa o alvo de um link. Também é o nome de um novo ícone no menu do Netscape 3.0.

ANSI: *American National Standards Institute*. É o órgão nacional norte-americano de padronização de normas técnicas.

Aplicação: Programa que faz uso de serviços de rede tais como transferência de arquivos, *login* remoto e correio eletrônico.

Archie: ferramenta para procura de arquivos para transferência via FTP anônimo.

Archie: Um serviço de busca de arquivos armazenados em FTP anônimo. Pouco disseminado no Brasil.

ARPANET: *Advanced Research Projects Agency Network*. Rede de longa distância criada em 1969 pela *Advanced Research Projects Agency* (ARPA, atualmente *Defense Advanced Projects Research Agency*, ou DARPA) em consórcio com as principais universidades e centros de pesquisa dos EUA, com o objetivo específico de investigar a utilidade da comunicação de dados em alta velocidade para fins militares. É conhecida como a rede-mãe da Internet de hoje e foi colocada fora de operação em 1990, posto que estruturas alternativas de redes já cumpriam seu papel nos EUA.

Arquivo de assinatura: um arquivo texto contendo informações que são sempre anexadas ao final de mensagens de correio eletrônico, como se fosse uma assinatura. 2. Ato de subscrever uma lista de discussão ou *newsgroup*; 3. Informação que autentica uma mensagem.

ASCII: *American Standard Code for Information Interchange*. Código numérico usado para representar caracteres da língua inglesa em computadores e dispositivos de armazenamento eletrônico de dados.

Atributo: relativamente às linguagem HTML e Java, são parâmetros relativos aos rótulos e aos applets.

Autenticação: é o processo de identificação. Pode ocorrer, por exemplo, entre um usuário e uma máquina ou entre duas ou mais máquinas.

Backbone: Estrutura de nível mais alto em uma rede composta por várias sub-redes. Em português, espinha dorsal.

Baud rate: Medida de taxa de transmissão elétrica de dados em uma linha de comunicação. Mede o número de sinais elétricos transmitidos por unidade de tempo. Ver também: bps.

BBS: *Bulletin Board System* é um sistema que tipicamente oferece serviços de correio eletrônico, repositório de arquivos (de programas, dados ou imagens) e outros serviços tais como conversação *on-line*. Seus assinantes tipicamente tem acesso através de linhas telefônicas (isto é, de voz) utilizadas via computador pessoal e modem.

BITNET: *Because It's Time Network* é uma rede educacional internacional que liga computadores em aproximadamente 2500 universidades e institutos de pesquisa nos EUA, Europa e Japão. A BITNET não usa protocolo da família TCP/IP, mas pode trocar mensagens eletrônicas com a Internet. O protocolo empregado é o RSCS (*Remote Spooling Communication System*).

Bookmarks: endereços (URLs) considerados relevantes pelo usuário, que os adiciona a um banco de dados (lista de *bookmarks*), de forma a facilitar o acesso aos sites.

Bps: Bites por segundo. Uma medida da taxa de transferência real de dados de uma linha de comunicação. Variantes ou derivativos importantes incluem Kbps (= 1000 bps) e Mbps (= 1000 000 bps). Ver também: baud rate

bridge: Um dispositivo que conecta duas ou mais redes de computadores, transferindo, seletivamente, dados entre ambas. Ver também: repetidor

browser: software cliente que permite a navegação através dos servidores que formam o *World Wide Web*. Tipicamente, um *browser* será um programa em um computador pessoal que acessará, através de uma linha telefônica, um servidor (isto é, um programa que atende a demanda de clientes remotos) contendo informações de interesse amplo. Ver também: cliente, servidor, Gopher, Mosaic, *Web*

Cache: para o browser, são áreas de memória RAM ou de disco que são utilizadas para armazenar arquivos HTML, GIF e JPG das páginas mais recentemente acessadas pelo usuário, de forma que, caso não haja alterações nestes arquivos no servidor Web, estes sejam carregados localmente, acelerando a navegação.

CCITT: Acrônimo de *Comité Consultatif Internationale de Telegraphie et Telephonie*, um órgão da *International Telecommunications Union* (ITU) das Nações Unidas que define padrões de telecomunicações. (Em 1993, foi extinto e suas atribuições passaram para o ITU-TSS, *Telecommunications Standards Section* da ITU.)

CERN: Trata-se do *European Laboratory for Particle Physics*, possivelmente o mais importante centro para pesquisas avançadas em física nuclear e de partículas, localizado em Genebra, Suíça. O nome CERN relaciona-se ao seu nome anterior, *Conseil Europeen pour la Recherche Nucleaire*. Para os usuários Internet, o CERN é conhecido como o local onde foi desenvolvido a *Web*. Ver também: Web

CGI : *Common Gateway Interface*. Uma interface padronizada que permite o intercâmbio de informações entre o browser e o servidor Web.

Ciberespaço: Conjunto de computadores e serviços que constitui a rede Internet. Termo cunhado em analogia com o espaço sideral explorado pelos astronautas.

Cliente/Servidor: tecnologia que separa computadores em duas categorias: clientes e servidores. Quando você acessa um site na Internet, você é o cliente. O computador que disponibilizou as informações é o servidor.

Cliente: É um processo ou programa que requisita serviços a um servidor. Ver também: servidor

Container: na sintaxe HTML, significa um rótulo que possui terminador. Por exemplo, o rótulo <APPLET> é um container, já que necessariamente tem que ser encerrado com o terminador </APPLET>.

Correio Eletrônico: serviço de comunicação que consiste na troca de mensagens através de redes de computadores.

Criptografia: método de “esconder” dados, através de códigos, embaralhamento, ou outro, mas que permite recuperação da informação original através de uma chave ou código secreto.

Daemon: um termo herdado do Unix que significa um programa que roda permanentemente em um servidor, esperando por solicitações de um determinado serviço que ele proporciona. Por exemplo, os servidores Web são denominados *httpd* (*Hyper Text Transport Protocol Daemon*) porque são executados permanentemente e ficam esperando solicitações dos browsers, como o Netscape ou o Explorer.

Datagrama: Pacote de informação que permite a transferência de dados numa rede.

DDN: Acrônimo para *Defense Data Network*, uma porção da Internet que conecta bases militares norte-americanas e seus fornecedores, e é usada para comunicações não-confidenciais. MILNET é uma das redes DDN.

Default: normalmente, a configuração “de fábrica” ou padrão.

Dialer: software que conecta o seu computador, através do modem e da linha telefônica, a um provedor de acesso à Internet. O *Trumpet Winsock* é um dialer.

Dial-up networking: meio de acesso a redes remotas via linha telefônica, com o uso de modems, discando o número onde está a rede ou computador.

DNS: *Domain Name System* (DNS) é um serviço e protocolo da família TCP/IP para o armazenamento e consulta a informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes Internet em seus números correspondentes.

Domínio público (*software* de): Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso. Em geral, o *software* é utilizável sem custos para fins estritamente educacionais, e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inesgotável de *software* de domínio público, com excelente qualidade, que circula pela rede. Ver também: shareware

Domínio: É uma parte da hierarquia de nomes de grupos ou *hosts* da Internet, que permite identificar as instituições ou conjunto de instituições na rede. Sintaticamente, um nome de domínio da Internet consiste em uma seqüência de nomes separados por ponto, por exemplo, colibri.hq.rnp.br. Neste caso, dentro do domínio hq.rnp, o administrador do sistema pode criar diferentes grupos como info.hq.rnp ou staff.hq.rnp, conforme ele desejar.

Download: O processo de se transferir uma cópia de um arquivo em um computador remoto para outro computador através da rede; o arquivo recebido é gravado em disco no computador local. O computador de onde os dados são copiados é subentendido como “maior” ou “superior” segundo algum critério hierárquico, enquanto o computador

para o qual os dados são copiados é subentendido “menor” ou “inferior” na hierarquia. O sentido literal é, portanto “puxar para baixo”.

E-Mail: (*Electronic Mail*). Correio Eletrônico. Correspondência trocada entre computadores, enviada ou recebida eletronicamente.

Ethernet: Um padrão muito usado para a conexão física de redes locais, originalmente desenvolvido pelo *Palo Alto Research Center* (PARC) da Xerox nos EUA. Descreve protocolo, cabeamento, topologia e mecanismos de transmissão.

FAQ (*Frequently Asked Questions*): arquivos que contêm perguntas e respostas sobre o assunto em questão, em geral voltado para leigos ou neófitos. É uma boa prática ler os arquivos FAQ antes de fazer alguma pergunta.

FDDI: Acrônimo de *Fiber Distributed Data Interface*, um padrão para o uso de cabos de fibras óticas em redes locais (LANs) e metropolitanas (MANs). A FDDI fornece especificações para a velocidade de transmissão de dados (alta velocidade, 100 Mbps) em redes em anel, podendo, por exemplo, conectar 1000 estações de trabalho a distâncias de até 200 Km.

FidoNet: Rede mundial de BBS, baseada no uso do protocolo Fido, interligando computadores pessoais via linhas telefônicas.

Finger: Um serviço Internet que permite obter informações sobre usuários de uma máquina.

Firewalls: dispositivo de segurança que, uma vez instalado, controla e autoriza o tráfego de informações transferidas entre redes.

Folder: pasta ou diretório que armazena arquivos ou outros folders.

Freenet: Uma máquina na Internet que é dedicada a acesso pela comunidade sem cobrança de nenhuma taxa. O acesso é fornecido através de bibliotecas públicas ou acesso *dial-up*. Oferece serviços de BBSs, correio eletrônico e acesso (restrito, em geral) a Internet.

Freeware: Ver: Domínio público

FTP: Um protocolo padrão da Internet que é usado para transferência de arquivos entre computadores.

FTP anônimo: Serviço que possibilita o acesso a repositórios públicos de arquivos via FTP. Ver também: FTP

FYI: Acrônimo de *For Your Information* (FYI), um sub-conjunto das RFCs com conteúdo consideravelmente menos técnico.

Gateway: 1. Sistema que possibilita o intercâmbio de serviços entre redes com tecnologias completamente distintas, como BITNET e INTERNET; 2. Sistema e convenções de interconexão entre duas redes de mesmo nível e idêntica tecnologia, mas sob administrações distintas. 3 Roteador (terminologia TCP/IP).

GIF (*Graphics Interchange Format*): formato de arquivo gráfico muito utilizado para a exibição de imagens em páginas Web, cuja tecnologia foi desenvolvida pela Unisys e popularizado através da rede Compuserve.

Gopher: Um sistema distribuído para busca e recuperação de documentos que combina recursos de navegação, por meio de menus hierárquicos, através de coleções de documentos e bases de dados indexadas. O protocolo de comunicação e o *software* seguem o modelo cliente-servidor, permitindo que usuários em sistemas heterogêneos naveguem, pesquisem e recuperem documentos armazenados em diferentes sistemas, de maneira simples e intuitiva.

Hiperlink: palavras ou textos em destaque nos documentos HTML que, quando clicados, acessam outros dados, endereços ou servidores na Web.

Hipermídia: aplicações que utilizam as propriedades do hipertexto para interligar elementos multimídia, como texto, vídeos, sons e imagens gráficas.

Hipertexto: cadeia de informações que contém links (ligações) para acessar dados e informações na Web.

Home-page: página de apresentação de um endereço eletrônico capaz de acessar outros documentos e servidores através de hiperlinks.

Host: computador que “hospeda” usuários externos fornecendo arquivos, serviços ou compartilhando seus recursos. Pode ser sinônimo de nó da Internet.

HTML (*Hypertext Markup Language*): linguagem de programação utilizada na criação de documentos e páginas que serão acessados na Web. É uma variante da SGML (*Standard Generalized Markup Language*), bem mais fácil de aprender e usar, que possibilita preparar documentos com gráficos e *links* para outros documentos para visualização em sistemas que utilizam *Web*.

HTTP (*Hypertext Transfer Protocol*): protocolo de transferência de documentos e informações em hipertexto na rede. O HTTP permite que os autores de hipertextos incluam comandos que permitem saltos para recursos e outros documentos disponíveis em sistemas remotos, de forma transparente para o usuário.

HTTPS (*Secure Hypertext Transfer Protocol*): protocolo de transferência segura de documentos e informações em hipertexto.

Imagem Clicável: uma imagem inserida em uma página HTML que associa determinadas áreas a URLs. Também conhecido como *imagemap*.

Internet: 1. Com inicial maiúscula, significa a "rede das redes", originalmente criada nos EUA, que se tornou uma associação mundial de redes interligadas, que utilizam protocolos da família TCP/IP. A Internet provê transferência de arquivos, *login* remoto, correio eletrônico, *news* e outros serviços; **2.** Com inicial minúscula significa genericamente uma coleção de redes locais e/ou de longa distância, interligadas por pontes, roteadores e/ou *gateways*.

IP (*Internet Protocol*): protocolo de funções básicas da Internet, responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na Internet. É o mais importante dos protocolos em que a Internet é baseada.

IRC (*Internet Relay Chat*): uma ferramenta da Internet que permite aos usuários “conversar” através de mensagens digitadas “on-line”.

ISDN [RDSI]: Uma rede digital que integra serviços de diversas naturezas como voz, dados, imagens, etc. que deve substituir gradualmente a infra-estrutura física atual de

comunicações, em que cada serviço tende a trafegar por segmentos independentes. Não disponível em termos comerciais amplos no Brasil.

ISO: A *International Organization for Standardization* (ISO) , uma organização internacional formada por órgãos de diversos países, tais como a ANSI (americana), a BSI (inglês), a AFNOR (francês) e a ABNT (brasileira), e que estabelece padrões industriais de aceitação mundial.

ISOC (*Internet Society*): sociedade sem fins lucrativos que promove a Internet e seus padrões.

ITU: *International Telecommunications Union.* Órgão da ONU responsável pelo estabelecimento de normas e padrões em telecomunicações.

Java: uma linguagem de programação orientada a objeto e baseada no C++, desenvolvida pela *Sun Microsystems*. O Java permite a inserção do chamado “conteúdo interativo” às páginas HTML.

JPEG (*Joint Photographic Experts Group*): comitê que desenvolve padrões na área de compressão de imagens. Também é a extensão do arquivo gráfico que utiliza estes padrões. O formato JPEG é utilizado para exibição de imagens nas páginas Web.

Kermit: Um programa de transferência de arquivos e emulação de terminal.

LAN [Rede Local]: Acrônimo de *Local Area Network*, rede de computadores limitada a distâncias de até 10 km. Em geral, limitada a um prédio ou conjunto de prédios de uma instituição.

Listserv: aplicação da Internet que envia automaticamente coletâneas de mensagens, por meio de correio eletrônico, para um grupo de assinantes, sendo definido como um servidor de listas de discussões.

Login remoto: Acesso a um computador via rede para execução de comandos. Para todos os efeitos, o computador local que “loga” em um computador remoto, passa a operar como se fosse um terminal deste último.

MAN: Acrônimo de *Metropolitan Area Network*, uma rede de abrangência metropolitana.

MIME (*Multipurpose Internet Mail Extensions*): é um padrão Internet que permite especificar e manipular vários tipos distintos de mídia (áudio, vídeo, imagem, texto, aplicações, etc.). Através do MIME, as capacidades normais de correio eletrônico são estendidas, permitindo acentuação em diversos idiomas, anexação de arquivos, etc. Ver RFC 1522 ou 1523.

Mosaic: Um programa cliente de fácil utilização projetado para procura de informações disponíveis na *Web*. Distribuído como freeware, o Mosaic foi criado *pelo National Center for Supercomputing Applications* (NCSA) dos EUA e tem capacidade multimídia.

Multicast: Um endereço para uma coleção específica de nós numa rede, ou uma mensagem enviada a uma coleção específica de nós. É útil para aplicações como teleconferência.

Navegação: Ato de conectar-se a diferentes computadores da rede distribuídos pelo mundo, usando as facilidades providas por ferramentas como *browsers Web*. O navegador da rede realiza uma “viagem” virtual explorando o ciberespaço, da mesma forma que o astronauta explora o espaço sideral. Cunhado por analogia ao termo usado em astronáutica.

NCSA (National Center for Supercomputing Applications): um centro de pesquisas onde o browser Mosaic (o pai de todos os browsers) foi desenvolvido.

Net: 1) *The Net* ou Internet; 2) rede.

Netiquette: Um conjunto de regras de etiqueta para o uso socialmente responsável da Internet, ou seja, o modo como os usuários devem proceder na rede, especialmente na utilização de correio eletrônico.

Netnews: *Usenet News, Usenet ou News.* Serviço de discussão eletrônica sobre vasta gama de assuntos, cada qual ancorado por um grupo de discussão.

News: Ver: netnews

Newsgroup: Grupo temático de discussão do *netnews*, ou seja, um fórum para discussão de assuntos e troca pública de mensagens entre participantes da Internet, dividido em áreas de interesse específicas.

NFS: O *Network File System* é o protocolo de compartilhamento de arquivos remotos desenvolvido pela *Sun Microsystems*. Faz parte da família de protocolos TCP/IP.

NIC: *Network Information Center.* Um centro de informação e assistência ao usuário da Internet, que disponibiliza documentos como RFCs, FAQs e FYIs, realiza treinamentos, etc.

NIS: Acrônimo para *Network Information Service* (também conhecido como *yellow pages*). Desenvolvido pela *Sun Microsystems* e utilizado por vários outros *UNIX flavors*, é um sistema distribuído de bases de dados que permite gerência centralizada de recursos de várias máquinas da rede.

NIS+: Versão atualizada do NIS, cuja implementação é mantida em segredo pela Sun. É um sistema bem mais seguro que o NIS, pois trabalha com autenticação e criptografia na comunicação entre as máquinas. Sua única desvantagem é ser proprietário, o que impede que seja usado em uma rede heterogênea.

NNTP (Network News Transport Protocol): protocolo utilizado para enviar mensagens de newsgroups da Usenet de um computador para outro.

Nó: Qualquer dispositivo, inclusive servidores e estações de trabalho, ligado a uma rede.

NOC [CO] (Network Operations Center): Um centro administrativo e técnico que é responsável por gerenciar os aspectos operacionais da rede, como o controle de acesso a mesma, "roteamento" de comunicação, etc.

Nome de Domínio: A parte do nome de um *host* que representa o domínio que contém o *host*. Por exemplo, no endereço *ci.rnp.br*, o nome de domínio é *rnp.br*.

Número IP: endereço Internet formado por um número dividido em quatro partes, separadas por pontos. Cada computador na Internet possui um número IP.

OSI-~~Θ~~ (Open Systems Interconnection): é um modelo conceitual de protocolo com sete camadas definido pela ISO para a compreensão e o projeto de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores de diferentes fabricantes. Ver também: ISO

Pacote: Dado encapsulado para transmissão na rede. Um conjunto de *bits* compreendendo informação de controle, endereço fonte e destino dos nós envolvidos na transmissão.

Ping: O ping (*Packet Internet Group*) é um programa usado para testar a acessibilidade a um *host*, enviando a nós remotos uma requisição e esperando por uma resposta.

PIR (Ponto de Interconexão de Redes) : Locais previstos para a inter-conexão de redes de mesmo nível (*peer networks*), visando assegurar que o roteamento entre redes seja eficiente e organizado. No Brasil, os três principais PIR's estão previstos em Brasília, Rio de Janeiro e São Paulo.

POP: 1 *Point-of-Presence*, em português Ponto-de-Presença (PoP). Ver também: PP; 2. *Post Office Protocol*. Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

Porta: Uma abstração usada pela Internet para distinguir entre conexões simultâneas múltiplas para um único *host* destino. O termo também é usado para denominar um canal físico de entrada e saída de um dispositivo.

Postmaster: E-mail do responsável pelo correio eletrônico de uma máquina ou domínio.

PP (Ponto de Presença) : Ponto de Presença de uma espinha dorsal de rede. Local onde uma rede permite acesso a sub-redes e a provedores de serviços. Uma rede madura cobre sua região de atuação através de pontos-de-presença nas principais cidades/distritos dessa região: interligados por um conjunto de linhas dedicadas, compondo um *backbone*.

PPP (*Point to Point Protocol*): protocolo serial que permite a um computador estabelecer uma conexão TCP/IP à Internet, utilizando uma linha telefônica e um modem, e se tornando um ponto da rede. O *Point-to-Point Protocol* estabelece um método de acesso a Internet em que um computador, ligado a um *host* Internet via telefone e um modem de alta velocidade, aparece para o *host* como se fosse uma porta Ethernet no sistema de rede local do *host*. É considerado o sucessor do SLIP por ser confiável e mais eficiente.

Protocolo: Um conjunto de regras padronizado que especifica o formato, a sincronização, o seqüenciamento e a verificação de erros em comunicação de dados. Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. O protocolo básico utilizado na Internet é o TCP/IP.

Provedor de Acesso: Instituição que se liga à Internet, via um Ponto-de-Presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não, através de linhas discadas ou dedicadas.

Provedor de Informação: Instituição cuja finalidade principal é coletar, manter e/ou organizar informações *on-line* para acesso através da Internet por parte de assinantes da rede. Essas informações podem ser de acesso público incondicional, caracterizando assim um provedor não-comercial ou, no outro extremo, constituir um serviço comercial onde existem tarifas ou assinaturas cobradas pelo provedor.

Provedor de Serviço: Tanto o provedor de acesso quanto o de informação.

Proxy: Servidor que age como intermediário na comunicação entre máquinas da rede interna e da rede externa. Pode ser utilizado com várias funções, entre elas, de *cache*, ou então em sistemas de firewall, para retransmitir dados entre a rede interna e externa.

Repetidor: Um dispositivo que propaga (regenera e amplifica) sinais elétricos em uma conexão de dados, para estender o alcance da transmissão, sem fazer decisões de roteamento ou de seleção de pacotes. Ver também: bridge, roteador.

RFC ~~Acronimo para~~ (**Request For Comments**): RFCs constituem uma série de documentos editados desde 1969 e que descrevem aspectos relacionados a Internet, como padrões, protocolos, serviços, recomendações operacionais, etc. Uma RFC é em geral muito densa do ponto de vista técnico.

Roteador: Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Tipicamente, uma instituição, ao se conectar à Internet, deverá adquirir um roteador para conectar sua Rede Local (LAN) ao Ponto-de-Presença mais próximo. Roteadores vivem se falando aos pares, como modems.

Servidor: 1. No modelo cliente-servidor, é o programa responsável pelo atendimento a determinado serviço solicitado por um cliente. Serviços como *archie*, Gopher, WAIS e WWW são providos por servidores; 2. Referindo-se a equipamento, o servidor é um sistema que provê recursos tais como armazenamento de dados, impressão e acesso *dial-up* para usuários de uma rede de computadores.

Shareware: Programa disponível publicamente para avaliação e uso experimental, mas cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. Note-se que *shareware* é distinto de *freeware*, no sentido de que um *software* em *shareware* é comercial, embora em termos e preços diferenciados em relação a um produto comercial "ortodoxo". Ver também: freeware, domínio público.

Site [instalação]: 1. Uma instituição, onde computadores são instalados e operados; 2. Um nó Internet. 3. local virtual dos integrantes do ciberespaço (empresas, entidades, pessoas), cuja entrada dá acesso à sua home page.

SLIP (*Serial Line Internet Protocol*): protocolo que, analogamente ao PPP, permite uma conexão TCP/IP à Internet. Este padrão vem sendo substituído gradativamente pelo PPP.

Smiley: Uma "carinha" construída com caracteres ASCII para ajudar a contextualizar uma mensagem eletrônica. Por exemplo, a mais comum é :-), que significa humor e ironia. Você deve girar o *smiley* 90 graus para a direita para entendê-lo.

SMTP (*Simple Mail Transfer Protocol*): protocolo básico que implementa funções para o envio de mensagens de correio eletrônico pela Internet.

SNMP (*Simple Network Management Protocol*): ~~é um~~ protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP. É o padrão adotado pela RNP para a gerência de sua rede.

Socks: Software de firewall baseado em filtragem de pacotes.

SSL (*Secure Sockets Layer*): protocolo desenvolvido pela Netscape para o estabelecimento de conexões seguras na Internet.

Sysop: A pessoa que opera e mantém um BBS. Abreviatura de *system operator*.

Talk: Serviço que permite a comunicação escrita *on-line* entre dois usuários da Internet.

TCP/IP: ~~Acronimo de~~ (**Transmission Control Protocol/Internet Protocol**), ~~é a~~ família de protocolos para a comunicação de dados inter-redes, originalmente proposta para a

Advanced Research Products Agency (ARPA). Hoje é um padrão de fato para inter-redes abertas, e seu uso é amplamente difundido dentro e fora dos EUA.

Telnet: ferramenta que permite a um usuário acessar remotamente outras máquinas ligadas à Web. A conexão via Telnet funciona exatamente como se o usuário estivesse usando o computador remoto ou fosse um terminal dele.

Transceiver: Dispositivo para conexão física de um nó de uma rede local.

Transferência de arquivos: Cópia de arquivos entre duas máquinas via rede. Na Internet, implantada e conhecida por FTP.

UDP ~~Acrônimo para~~ (**User Datagram Protocol**), é protocolo de transporte sem conexão da família TCP/IP, usado com aplicações como o de gerenciamento de redes (SNMP) e de serviço de nomes (DNS).

Upload: ato de transferir um arquivo do seu computador para um servidor.

URL (Uniform Resource Locator). Endereço para localização de informações na WWW. É formado por 3 partes distintas : o protocolo, o nome principal e o diretório. Por exemplo, no URL <http://www.rnp.br/produtos/>, o protocolo é *HTTP*, o nome principal é *www.rnp.br* e o diretório é *produtos*.

Usenet News: Ver: Netnews.

Usenet: Ver: Netnews.

UUCP (Unix-to-Unix CoPy): é uma coleção de programas para intercomunicação de sistemas Unix. Possibilita transferência de arquivos, execução de comandos e correio eletrônico. Ver também: aplicação.

Veronica ~~Acrônimo para~~ (**Very Easy Rodent-Oriented Net-wide Index to Computerized Archives**) ; ferramenta para pesquisa no *GopherSpace*, o conjunto de servidores Gopher disponíveis na Internet.

Waffle: Um programa que possibilita a um BBS tornar-se um site *Usenet*.

WAIS ~~Acrônimo para~~ (**Wide Area Information Server**), é um serviço de bases de dados distribuídas acessíveis via Internet, cuja principal peculiaridade é a conversão automática de formatos para visualização remota de documentos e dados.

WAN (Rede de longa distância): Acrônimo de *Wide Area Network*, uma rede que interliga computadores distribuídos em áreas geograficamente distantes

Web: Ver: WWW.

Whois: WHOIS é um banco de dados de informações sobre domínios, redes, *hosts* e pessoas, fornecendo um serviço de diretório de usuários da Internet.

World Wide Web (Web ou WWW ou W3): traduzindo, significa teia de alcance mundial. Sistema de localização e pesquisa de informações que permite o acesso, através de hiperlinks, a um número ilimitado de dados em escala mundial. O acesso utiliza o conceito de hipermídia, conectando mídias do tipo texto, vídeos, sons e imagens.

WORM: ~~Acrônimo de~~ (**Write Once Read Many**): 1. Ferramenta de busca na rede *Web*; 2. Verme, programa que, explorando deficiências de segurança de *hosts*, logrou propagar-se de forma autônoma na Internet na década de 80.

X.25: Protocolo de roteamento muito utilizado em redes públicas de pacotes.

X.400: Um protocolo que especifica serviços do tipo *store-and-forward*, sendo o serviço de correio eletrônico *Message Handle System* (MHS) o mais conhecido deles, como parte das recomendações OSI/ISO.

X.500: É um padrão ITU-TSS/ISO para serviços de diretório eletrônico.

Yellow pages: Ver: NIS.

Índice Remissivo

.....

Anexo Avulso

Quanto Custa e Como Adquirir o POP-IN-A-BOX?

A instituição interessada em montar o POP-IN-A-BOX, terá que adquirir os itens especificados em sua composição, como apresentado a seguir. Assim, para uma configuração mínima e alguns itens opcionais, tem-se a seguinte estimativa de preços:

| | US\$ |
|--|-------------|
| Servidor Internet | 2650 |
| 01 Pentium 100 MHz, 32 MB RAM, 01 placa SVGA 1MB, 02 GB de disco rígido, 01 unidade de disco 1.44MB, 02 portas seriais, 01 porta paralela, 01 bus mouse, 01 teclado, 01 unidade de CDROM | 2500 |
| 01 FreeBSD 32bit O/S for the 386 com 01 The Complete FreeBSD Book | 70 |
| 01 Placa Ethernet | 100 |
| | |
| Dispositivos de Backup (opcional) | 1720 |
| 01 Controladora SCSI Adaptec 2940 | 380 |
| 01 Unidade de Fita DAT SCSI SUN | 2170 |
| | |
| Módulo Roteador | 595 |
| 01 Placa ET-5025 V.35 FreeBSD | 555 |
| 01 ETV35-3 Adapter Cables | 40 |
| | |
| Módulo Servidor de Comunicação | 920 |
| 01 Placa Multiserial Cyclades Cyclom-8Yo | 520 |
| 02 Modems Externos 28800 bps | 400 |
| | |
| TOTAL | 5885 |

Antes de iniciar o processo de aquisição destes equipamentos, deve-se, pesquisar os possíveis fornecedores e fazer uma tomada de preços, considerando também as condições de entrega e de pagamento.

O processo de aquisição, tanto nacional quanto internacional, pode ser firmado através de Fax, E-Mail, Web ou telefone, sendo que através deste último não se tem o registro das etapas realizadas.

Aquisições Internacionais

O veículo mais utilizado para as aquisições internacionais é a Web. O exemplo abaixo, mostra como itens, especificamente para o POP-IN-A-BOX, podem ser adquiridos via serviços Web. Em geral, ao acessar a URL do fornecedor, é apresentado um formulário de solicitação de aquisição, a ser preenchido com dados cadastrais, pedido propriamente dito, forma de pagamento e forma/prazo de entrega.

Para pagamento via cartão de crédito internacional, o processo será mais eficiente, porém deve-se dar preferência às URL's que oferecerem segurança na transação durante todo o processo. Após a confirmação dos dados e submissão do formulário, a autenticação do pedido será automaticamente enviada ao solicitante.

Sistema Operacional FreeBSD

URL: <http://www.cdrom.com/titles/os/freebsd.htm>

Placa Síncrona ET-5025 V.35 FreeBSD e ETV35-3 Adapter Cables

Emerging Technologies

URL = <http://www.etinc.com/>

Os processos de importação estão sujeitos à fiscalização alfandegária e às normas do SISCOMEX - Sistema Integrado de Comércio Exterior (<http://www.receita.fazenda.gov.br>). Se uma pessoa física ou jurídica adquirir apenas um item para uso próprio, num valor de até US\$500.00, a aquisição não é interpretada como aquisição para fins comerciais. Assim a mercadoria não estará sujeita a retenção na alfândega.

Em caso de retenção, o interessado será comunicado rapidamente sobre o fato, para as providências pertinentes ao desembaraço. Quando a empresa responsável pelo transporte da mercadoria não se responsabiliza por processos de desembaraço sem custo, será necessária a contratação de despachante aduaneiro. Os honorários dos serviços prestados pelo despachante, bem como as taxas e impostos da Receita Federal, estão diretamente relacionados ao valor da mercadoria.

Um exemplo de retenção de mercadoria aconteceu com o processo de aquisição das duas placas síncronas ET-5025. Para desembaraçá-las em Março/97, através de despachante aduaneiro, foi cobrada a quantia total de R\$1.423,65.

Outro exemplo ocorreu com a aquisição de quatro conjuntos do *software* FreeBSD, compostos por CD-ROMs e livros. O desembaraço desta remessa foi feito diretamente pela transportadora DHL, mas sem nenhum custo adicional.

Aquisições Nacionais

As aquisições nacionais, a exemplo dos itens abaixo, foram realizadas através de compra direta com os fornecedores.

Considerando que um microcomputador PC Pentium é facilmente adquirido junto a qualquer fornecedor especializado em informática, as informações sobre seu processo de aquisição foram propositalmente omitidas.

Comunicações

Compilamos a seguir, uma tabela comparativa com os preços dos principais serviços de conexão dedicada:

| | Velocidade (Kbps) | | | |
|-----------|-------------------|-----------|-----------|-----------|
| Backbone | 64 | 128 | 256 | 512 |
| Embratel* | R\$ 1.260 | R\$ 2.205 | R\$ 3.780 | R\$ 7.200 |
| RNP** | R\$ 1.200 | R\$ 2.175 | R\$ 3.680 | R\$ 7.030 |

* Preços sem impostos.

** Preços praticados pelo POP-RJ, sem impostos.

Endereços

Placa Mutiserial Cyclades Cyclom-8Yo

Pointer Informática - Tel: (011)3068-8780

Fabricante: <http://www.cyclades.com.br/>

Placa Controladora SCSI Adaptec 2940

MVM Comercio e Informática Ltda - Tel: (019)254-5852

Fabricante: <http://www.adaptec.com/>