Guia de operações Internet/Brasil

- versão 2.0 -

abril 1996

Documento N° RNP/RPU/0015F
Código CI-004

SOBRE ESTE GUIA

Este documento faz parte de um conjunto de quatro guias, a saber:

- Guia do Usuário Internet/Brasil
- Guia do Empreendedor Internet/Brasil
- Guia de Operações Internet/Brasil
- Guia de Montagem de Informações na Internet/Brasil

Como um todo, os quatro guias visam apoiar as atividades de **implantação de serviços Internet no Brasil**, condensando, organizando e apresentando em português informações originalmente dispersas em vários pontos na rede mundial.

. . .

Em consonância com esse objetivo, nenhum dos guias se destina ao usuário final ou ao interessado casual em redes. Todos eles pressupõem um conhecimento mínimo do leitor sobre aspectos técnicos de informática, telecomunicações e serviços de informações *on-line*. Por outro lado, tampouco se presume que um único leitor será capaz de entrar nos meandros de cada guia. A audiência ideal do conjunto de guias é uma equipe de quatro pessoas, a saber:

- O coordenador geral de um potencial empreendimento ou instalação Internet no Brasil *(Guia do Usuário* e *Guia do Empreendedor)*;
- O coordenador técnico de um time de implantação de uma instalação Internet comercial no Brasil *(Guia do Empreendedor)*;
- O responsável técnico por infra-estrutura e operações em um time de implantação de uma instalação Internet no Brasil *(Guia de Operações* e *Guia de Informações)*; e
- O responsável técnico pela implantação de serviços e aplicações em uma instalação Internet no Brasil *(Guia de Informações)*.

. . .

Comentários e sugestões sobre os Guias serão altamente apreciados e considerados para futuras versões dos documentos. Qualquer correspondência nesse sentido deve ser endereçada à:

Rede Nacional de Pesquisa
A/C Centro de Informações
R. Vicente de Souza, 34
Botafogo
Rio de Janeiro - RJ
CEP 22531-070
Fax: +21 246-5685
E-mail: **info@ci.rnp.br**

SUMÁRIO

ANEXO

1. O GUIA DE OPERAÇÕES INTERNET BRASIL

1.1. Introdução

O *Guia de Operações Internet Brasil* busca orientar os responsáveis técnicos pela infra-estrutura de operações de empreendimentos Internet no Brasil, indicando boas referências bibliográficas, *on-line* e *off-line*, e boas implementações de ferramentas e servidores, no meio ao vasto material disponível sobre o assunto, abordando aqui soluções amplamente testadas e utilizadas pela rede para os serviços básicos de uma rede TCP/IP.

Os *softwares* e referências bibliográficas aqui citados não implicam em nenhuma forma de responsabilidade pelo seu uso por parte da RNP, ou dos autores. As licenças que os acompanham devem ser lidas cuidadosamente assim como os termos de responsabilidade (ou de não responsabilidade), devendo o interessado decidir, por sua conta e risco, sobre a utilização ou não do material indicado.

O material (documentação e pacotes de *software*) descrito neste documento é de volume reduzido quando comparado com o disponível em geral na Internet. Porém, a disponibilidade local, via

ftp://ftp.ci.rnp.br

(aqui referênciado apenas como repositório, ou repositório local), agiliza o processo de distribuição de *software* e de documentação. Além disso, os itens constantes do repositório são bem selecionados e refletem a experiência da RNP na operação de redes acadêmicas ao longo de vários anos no pais.

Cabe ressaltar que a tecnologia envolvida na Internet, em particular os pacotes de *software*, estão em constante evolução sendo a própria rede o mecanismo de divulgação de novidades. Portanto, e importante observar a dinâmica de atualização das informações na rede, e consultar periodicamente outros repositórios e serviços de informação disponíveis.

Críticas e sugestões sobre este guia e sobre o repositório associado são muito bem-vindas e devem ser enviadas, através do correio eletrônico, para o endereço:

info@ci.rnp.br.

1.2. Audiência

O conteúdo do repositório de Operações do CI/RNP é essencialmente técnico e indicado para administradores de sistemas responsáveis pela conexão de equipamentos a uma rede Internet, em particular a INTERNET/BR.

O pleno aproveitamento das informações contidas neste documento requer que o leitor tenha acesso à Internet e familiaridade com seus recursos, podendo, através da rede, consultar algumas das referências indicadas.

1.3. Organização

O repositório é organizado em tópicos que correspondem às várias atividades relacionadas à operação de equipamentos conectados a redes TCP/IP e à manutenção de serviços de rede.

As técnicas, os pacotes de *software* e demais arquivos referenciados neste documento, incluídos no repositório, são acompanhados por um conjunto mínimo de informações, abrangendo:

- uma introdução e descrição do mecanismo, técnica ou produto em questão;
- referências a documentos e outras fontes de informação (tais como: referências bibliográficas, FAQs, newsgroups e listas de discussão); e
- referências a repositórios, no caso de pacotes de software.

2. MODELO CANÔNICO DE UM PROVEDOR DE SERVIÇOS

Principiamos com a apresentação de um modelo para um Provedor de Serviços na Internet (conforme Fig. 1), como forma de ambientar o leitor ao Guia de Operações. Maiores informações sobre a montagem de um Provedor podem ser encontradas no Guia do Empreendedor em:

http://www.ci.rnp.br/ci/ci.html

Em cada seção a seguir introduzimos um dos itens do modelo, dando opções de configuração, desde a mais barata até as mais sofisticadas, e citando outras referências, quando houver.

Figura 1 - Modelo Canônico de um Provedor de Serviços

2.1. LPCD

Uma ou mais Linhas Privadas de Comunicação de Pacotes (LPCDs) farão a ligação do Provedor com outro Provedor ou com um Ponto de Presença (POP) regional ou federal. Ao contratar uma LPCD de uma Concessionária de Telecomunicação é pago um valor fixo mensal, independentemente da utilização da linha, em função da taxa disponível.

A LPCD de menor capacidade recomendada para a ligação de um Provedor a Internet e de 64kbps. Consulte a Concessionária local acerca de disponibilidade, prazos e tarifas para as linhas desejadas.

Com velocidades iguais ou superiores a 64kbps utilizam-se Linhas Dedicadas Especializadas, onde os modems são fornecidos pela Concessionária de Telecomunicação. Os modems empregados nas Linhas Especializadas possuem, em geral, interfaces síncronas entre o modem e o roteador. No Brasil, dependendo da velocidade da linha e da Concessionária que a fornece, são utilizados seguintes padrões:

- ITU-T V.35; ou
- ITU-T V.11/V.36 (RS-449); ou ainda
- ITU-T G.703, não balanceada, com conectores BNC.

A V.36, padrão americano, tem uma relação Taxa x Distância melhor. A V.35, padrão europeu, emprega menos condutores. Em geral, as LPCDs nacionais utilizam interfaces V.35 para linhas de 64 kbps e G.703 para taxas de 2 Mbps, mas essa informação deve ser confirmada junto à concessionária local. Alguns fabricantes fornecem roteadores com interfaces V.35 e V.36, se assim solicitado; com a possibilidade de escolha de um ou outro padrão, em tempo de instalação do equipamento.

O importante aqui é, ao contratar a linha e o serviço Internet e ao adquirir os roteadores, garantir que as interfaces dos roteadores/modems sejam as mesmas.

2.2. Roteador

Este é o equipamento que fará o roteamento de pacotes da sua rede local para a Internet e vice-versa. A ele é atribuída a responsabilidade de manutenção e atualização das informações de roteamento (vide seção 4.1).

A melhor opção aqui, do ponto de vista técnico, é a utilização de equipamentos dedicados projetados especificamente para roteamento, que são conhecidos como roteadores dedicados. A utilização de um roteador dedicado dará maior confiabilidade e melhor desempenho a sua ligação com a rede, já que esses equipamentos são mais estáveis do que computadores para uso geral, configurados como roteadores. É importante que o roteador escolhido seja realmente compatível com o roteador do ponto ao qual o Provedor estará ligado. Para tanto, entre em contato com o responsável técnico da instituição que proverá acesso ao seu Provedor e com o seu fornecedor, garantindo assim esse item. A compatibilidade deverá ser não apenas no nível da ligação física com os modems da LPCD, como explicado na seção anterior, mas também no nível do protocolo de enlace, i.e., deve haver pelo menos um protocolo de enlace comum aos dois roteadores. Os protocolos de enlace mais utilizados são: PPP, HDLC, SDLC.

Uma opção aparentemente mais barata, embora menos eficiente e segura, é o emprego de servidores como roteadores (vide seção 2.7).

É importante especificar o roteador em função do tráfego previsto. O seu roteador deverá ter um desempenho suficiente para encaminhar o fluxo de pacotes de cada interface a ele ligada. É comum a especificação do desempenho de um roteador em pacotes por segundo (pps), sendo utilizados pacotes de 64 kbytes. Para o dimensionamento do roteador deveremos estimar com folga o fluxo gerado por cada interface.

Uma interface serial de 64 kbps gerará sempre um fluxo de no máximo 125 pps. Uma interface E1 gerará, no máximo, 32 vezes isso. E assim por diante. Para estimar o fluxo gerado por interfaces de redes locais, como *Ethernets* e FDDIs utilizamos os dados medidos em laboratório, encontrados em:

ftp://nsdndev.harvard.edu/pub/ndtl/

Assim temos a seguinte tabela de fluxo por tipo de interface:

Interface	Desempenho [pps]
64 Kbps	125
E1 (2 Mbps)	4000
Ethernet (10 Mbps)	3100
Ethernet (100 Mbps)	31000
FDDI (100 Mbps)	98000

Devemos considerar que um roteador conseguirá rotear de uma interface, no máximo, o fluxo correspondente a soma do fluxo das outras interfaces. Desta forma, se tivermos, por exemplo, um roteador com duas interfaces de 64 Kbps (2 x 125 pps) e uma Ethernet 10baseT (3100 pps), o fluxo máximo da Ethernet que poderá ser absorvido pelo roteador será o de 250 pps. Assim, um roteador com um Ehternet 10baseT e duas seriais de 64Kbps deverá ter um desempenho de pelo menos 500 pps.

Consulte sempre o seu fornecedor de roteadores para especificar o modelo que se adequa as suas necessidades atuais e futuras.

2.3. SCs

O Servidor de Comunicação (SC) cuida do acesso dos usuários via Linhas Discadas (LDs), i.e., via rede pública de telefonia. As diversas formas de conexão possíveis estão descritas na seção 3.1.

Por um lado, o SC terá uma interface com os modems, se servindo, em geral, de interfaces RS-232C. Há SCs que já possuem os modems internamente, em cujo caso a interface será diretamente a linha telefônica (RJ-45, RJ-11 ou tomada Telebrás). Por outro lado, o SC deverá ter uma interface para a rede local que você estiver utilizando.

A melhor opção, novamente do ponto de vista técnico, é a utilização de SCs especializados, que são equipamentos projetados apenas para essa função. Já encontramos no mercado roteadores e servidores de comunicação em um único produto, que pode ser uma opção para pequenos *sites*.

Uma opção mais barata, embora menos eficiente, pode ser a utilização de servidores Internet com uma ou mais placas multiseriais, como SC.

Caberá aos servidores de comunicação a questão da autenticação e, possivelmente, a bilhetação dos usuários. A bilhetagem pode ser feita tanto externamente ao provedor, por exemplo, utilizando-se do serviço 900 da concessionária local de telecomunicações, quanto internamente, em conjunto com a autenticação, pelo servidor de comunicações.

Para a autenticação (e bilhetagem), emprega-se um servidor de autenticação, que rode no servidor Internet, que deverá ser fornecido pelo fabricante do servidor de comunicação em conjunto com o equipamento ou via seu *site* Internet(1). Os servidores de autenticação mais utilizados são o *tacacs* e o *radius*. Além de fazer a autenticação e registro de entrada e saída dos usuários, um provedor de acesso necessita também de ferramentas para gerenciar esses registros, fazer totalização, fazer *backups* das bases de dados de registros, gerar faturas e finalmente fazer a cobrança. Há alguns pacotes no mercado que facilitam esse processo, na página *Scripts and Patches for ISP's* ,

(**http://www.westnet.com/providers/**)
os interessados podem encontrar algumas sugestões.

Nota: (1) É importante garantir que o servidor de autenticação a ser utilizado rode no seu servidor Internet.

2.4. *Gateway* X.25

Um *gateway* X.25 possibilita a ligação do Provedor com a Rede Nacional de Pacotes (RENPAC) ou outras redes X.25 públicas ou privadas. A ligação X.25 é útil para que usuários localizados em cidades distantes do seu Provedor tenham uma forma para conexão alternativa à utilização direta da rede pública de telefonia.

Pode-se usar a rede pública de pacotes também como forma alternativa. Em alguns é casos, mais barata, porém menos eficiente para interligação do Provedor com a Internet. Ao utilizar uma rede X.25 como meio de transporte para interligar duas redes IP, a técnica adotada é o chamado tunelamento, onde os pacotes IP são inseridos em pacotes X.25 pelo *Gateway* X.25, enviados ao seu destino pela rede de pacotes, quando são finalmente retirados do pacote X.25 no *Gateway* do destino. Esse processo acarreta em um *overhead* de cerca de 25%.

Como *gateway* X.25 existem três opções:

1) utilizar o seu roteador;
2) utilizar o SC; ou
3) utilizar o servidor Internet.

O uso de qualquer uma delas irá depender da capacidade do seu equipamento de trabalhar com X.25. No servidor Internet, em geral, vendem-se *drivers* separados para X.25. Porém, existem servidores como o *FreeBSD* e o *NetBSD* e o *Windows-NT* que já suportam o protocolo X.25 (vide seção 2.7). Aqui, pelas mesmas razões descritas no item anterior, a opção mais confiável é a utilização de equipamentos dedicados para a tarefa (opções (1) e (2)).

2.5. Linhas Discadas

As LDs são, em princípio, linhas telefônicas comuns que serão usadas para receber ligações de usuários feitas através dos seus computadores. Este tipo de acesso e conhecido como Acesso Discado (AD, vide seção 3.1.2.).

No AD é importante dimensionar o número de linhas em função da quantidade de usuários do Provedor. Considerando uma política de acesso onde o tempo é ilimitado, é recomendável que a relação número de usuários/linha não seja superior a 10. É claro que este valor deverá ser ajustado em função do perfil dos usuários e, para tanto, se faz necessário que o uso das linhas seja devidamente monitorado.

2.6. Modems

Modems para AD serão necessários quando o seu SC não possuir modems internamente. Em ambos os casos, devem-se utilizar modems que implementem os protocolos padrões V.34, V.42 e V.42bis.

O uso de modems que implementam os protocolos V.34 (28.800bps), V.42 (correção de erros) e V.42Bis (compressão) possibilitará o fornecimento de acesso da melhor forma possível, se o usuário dispuser também de modems com a mesma característica (o que é uma forte tendência, já que o custo de modems que trabalham a taxas maiores acaba sendo amortecido pela conta telefônica e pela conta no próprio provedor). Porém, é preciso garantir o acesso a aqueles usuários que ainda não dispõem de modems V.34/V.42/V.42bis, assegurando-se que os modems adquiridos sejam também capazes de trabalhar com taxas menores, i.e., que seja compatíveis com os protocolos V.32bis (14.400bps e 9.600bps), V.22bis (2400 e 1200 bps). É indispensável que estes modems tenham a facilidade de atender chamadas telefônicas e é desejável que eles utilizem os comandos do padrão Hayes, que são empregados pela maioria esmagadora dos servidores de comunicação para programação desses dispositivos.

A tabela a seguir resume a especificação mínima de um modem para o serviço:

Padrão	Característica
V.34	28.800 bps
V.32bis	14.400 bps
V.42	correção
V.42bis	compactação
V.22bis	2.400 bps e 1.200 bps

Acesso Discado próprio para acesso discado
Comandos Hayes aceita comandos hayes

2.7. Servidores

A Internet baseia-se no modelo cliente-servidor, no qual uma máquina, chamada "servidor", tem por função básica tornar um determinado serviço disponível para acesso por uma outra máquina, denominada "cliente".

Servidor, a rigor, é um processo que implementa um determinado serviço, como por exemplo: servidor de correio eletrônico (*sendmail*), servidor de listas (*listserv*/*marjordomo*), servidor Gopher (*gopherd*), servidor de *news* (nntpd), servidor *Web* (httpd), servidor de impressão (lpd), servidor de sistema de arquivos (nfsd), servidor de nomes ou DNS (*named*), dentre outros.

Uma prática comum, em redes locais ou em *sites* não muito grandes, é centralizar os vários serviços em uma única máquina, denominada servidora.

É possível ter diversas combinações de *hardware/software* para um servidor, desde um PC 486 com um sistema operacional como *FreeBSD*, *Linux*, *NetBSD*, *WindowsNT*, etc. até uma estação de trabalho incrementada executando *AIX*, *NetBSD*, *OSF/1*, *Solaris*, *WindowsNT*, etc. A escolha da plataforma adotada deverá levar em conta os serviços que pretendem ser providos, a quantidade de usuários total do sistema, o volume de disco previsto para utilização pelos serviços locais e pelos usuários, a quantidade de usuários para acesso simultâneo ao servidor e o tipo de acesso permitido. As plataformas com *Unix* são as mais utilizadas por provedores de serviços comerciais, por oferecer escalabilidade, e por tratar-se de um padrão de fato como sistema operacional de servidores Internet.

O indispensável é que a plataforma adotada suporte os serviços Internet desejados. Os serviços básicos para uma provedor Internet, são:

- DNS (vide seção 4.2)
- Correio Eletrônico -- SMTP (vide seção 4.3.1)
- Correio Eletrônico -- POP (vide seção 4.3.2)

São listados a seguir os sistemas operacionais frequentemente utilizados em servidores de rede, acompanhados pela respectiva lista de referências:

Referências:

AIX
http://www.ibm.com
comp.unix.aix

BSDI
http://www.bsdi.com
comp.unix.bsd

FreeBSD
http://www.freebsd.org
ftp://ftp.freebsd.org
comp.os.386bsd
comp.unix.bsd

FAQs
http://www.freebsd.org/How/faq

HP/UX
http://www.hp.com
comp.sys.hp.hpux

Irix
http://www.sgi.com
comp.sys.sgi =20

Linux
http://www.linux.org
comp.os.linux

NetBSD
http://www.netbsd.org
ftp://ftp.netbsd.org
comp.os.386bsd
comp.unix.bsd
Listas:
http://www.netbsd.org/MailingLists/index.html

Netware
http://www.novell.com
ftp://ftp.novell.com/pub/netware
gopher://gopher.novell.com
comp.os.netware

OS/2
http://www.ibm.com
comp.os.os2

OSF/1
http://www.digital.com
ftp://ftp.digital.com/pub/Digital/OSF1
comp.unix.osf.osf1

SCO UNIX
http://www.sco.com
ftp://ftp.sco.com/SCO
comp.unix.xenix.sco

Solaris/SunOS=20
http://www.sun.com
comp.sys.sun
lista
sun-managers@eecs.nwu.edu (subscrição:
sun-managers-request@eecs.nwu.edu)

UNIX
comp.unix.admin

*Unix*Ware
http://www.novell.com
ftp://ftp.novell.com/pub
comp.unix.unixware

WindowsNT
http://www.microsoft.com
gopher://gopher.microsoft.com
ftp://ftp.microsoft.com
comp.os.ms-windows.nt

2.8. Estações

Estações são os equipamentos de uso geral da operação de um Provedor. Elas podem ser desde estações de trabalho *Unix* até PCs com *Windows* ou *OS/2*. O leque de opções disponíveis no mercado brasileiro e o mais amplo possível. O importante, aqui, é que as estações tenham acesso à rede TCP/IP.

3. ACESSO A REDE

Em seguida, são descritos aspectos relacionados ao acesso à Internet, isto é, ao Provedor de Acesso (PA), pelo usuário. O acesso caracteriza-se pela forma (dedicado, discado e X.25) e pelo tipo de enlace adotado (PPP, SLIP ou terminal).

3.1. Quanto à conexão

A conexão física pode ser de dois tipos: dedicada ou discada, descritas a seguir.

3.1.1. Dedicada

Em geral, uma conexão dedicada e utilizada por usuários que possuem uma rede local e não apenas uma máquina ligada à linha telefônica. Nesses casos, justificam-se custos adicionais, associados à manutenção de uma conexão dedicada, pelo número de usuários beneficiados pelo serviço, pelos tipos de serviço de rede viabilizados ou por razões comerciais (veja o Guia do Empreendedor Internet/Brasil).

A escolha da LPCD vai depender da capacidade do PA, da necessidade do usuário e da disponibilidade da Concessionária Local de Telecomunicações. É inútil, para ter acesso a um PA, utilizar uma LPCD com maior capacidade do que a LPCD do próprio PA destinada ao resto da rede. A opção mais econômica e a utilização de uma LPCD não especializada, em que a Concessionária entrega apenas um par de fios, e cabe ao usuário e ao PA a responsabilidade pela compra e instalação dos modems. Nesse caso devem-se empregar modems V.34/V.42bis/V.42 próprios para LPCD.

Preferêncialmente, as LPCDs devem ser ligadas a roteadores dedicados, que garantem maior confiabilidade à ligação.

O protocolo de enlace utilizado deve ser comum aos dois extremos da conexão, tais como: PPP, HDLC, SDLC, (vide seção 3.2.1), ou, em última opção, SLIP (vide seção 3.2.2). Esta escolha dependerá da disponibilidade do serviço nas duas pontas.

3.1.2. Discada

O acesso discado, em geral, é utilizado por um **usuário individual**, através de um microcomputador com modem ligado a rede telefônica. No PA, o SC é configurado para que o acesso seja feito por meio de um ou mais dos seguintes serviços:

- PPP (vide seção 3.2.1)
- SLIP (vide seção 3.2.2)

ou *shell Unix*.

3.2. Quanto ao enlace

Após o estabelecimento da conexão física, é preciso um protocolo que controle o acesso a esta conexão, isto e, que controle o fluxo de pacotes IPs pela linha serial. Com esta função, destacam-se o PPP e o SLIP.

3.2.1. PPP

O *Point-to-Point Protocol* (PPP) provê um método de transmitir datagramas por uma linha serial de forma confiável, isto e, sem perdas nem embaralhamento da informação. O PPP encontra-se implementado numa vasta gama de arquiteturas: *Windows*, a maioria dos *Unix*, CSs e roteadores dedicados.

O procedimento de instalação e configuração do PPP depende da plataforma empregada. Roteadores e CSs geralmente suportam o PPP (verifique na própria documentação do produto a disponibilidade e como habilitá-lo). Nos sistemas operacionais BSDs que não têm o PPP embutido como o *SunOS*, por exemplo, pode-se instalar o pppd.

Referências:

- Jacobson, V. *Compressing TCP/IP Headers for Lowspeed Serial Links*. RFC 1144. Fevereiro de 1990.

- Lloyd, B.; Simpson, W.A. *PPP authentication protocols* RFC 1334. Outubro de 1992.

- McGregor, G. *PPP Internet Protocol Control Protocol (IPCP)* RFC 1332. Maio de 1992.

- Simpson, W.A. *The Point-to-Point Protocol (PPP)*' RFC 1548. Dezembro de 1993.

- Simpson, W.A. *PPP in HDLC Framing* RFC 1549. Dezembro de 1993

Repositórios:

ftp://ftp.ci.rnp.br/pub/packages/ppp
ftp://merit.edu/pub/ppp

3.2.2. SLIP

O SLIP (*Serial Line Internet Protocol*) permite a transmissão de pacotes TCP/IP através de uma linha serial.

Referências:

http://www.cis.ufl.edu/help-system/slip-stuff/
http://www.micro.umn.edu/products/slip/slip.html
http://reality.sgi.com/employees/scotth/dialup_support.html

3.2.3. X.25

Quando a rede pública de pacotes é utilizada para acesso de usuários remotos, o PPP ou SLIP sobre o X.25 podem ficar disponíveis. Aqui, novamente, teremos um *overhead* pela utilização do X.25 e do PPP ou SLIP. Uma opção para viabilizar esse tipo de acesso é prover um *shell* no seu servidor Internet.

4. SERVIÇOS BÁSICOS

Aqui introduzimos os serviços básicos de uma rede ligada a Internet. São eles: roteamento (seção 4.1), DNS (seção 4.2), correio eletrônico (seção 4.3) e gerência de redes (seção 4.4).

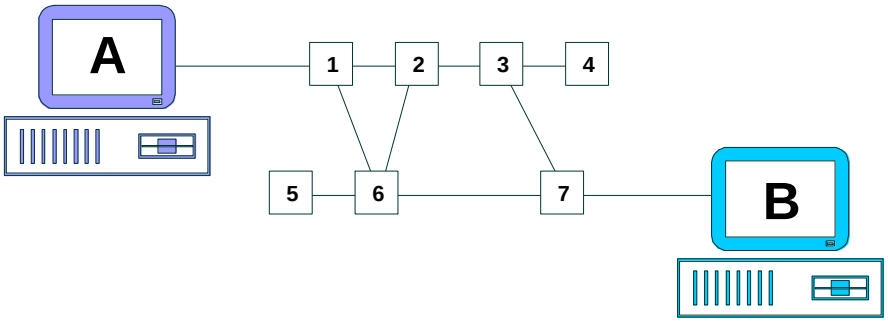
4.1. Roteamento

A infra-estrutura física de uma grande rede de computadores pode ser comparada a uma estrutura rodoviária. As cidades seriam as instituições, com seus diversos computadores e redes locais, e as rodovias os canais de comunicação, interligando essas instituições.

Quando consultamos um mapa rodoviário conhecemos os vários caminhos possíveis de ligação entre as cidades. Se a nossa intenção é fazer uma viagem, procuramos escolher o melhor caminho. No universo das redes a mesma coisa acontece, ou seja, dentre os diversos caminhos possíveis de comunicação entre computadores, tenta-se usar o melhor segundo um conjunto de critérios.

A atividade de encaminhamento de unidades de informação (pacotes) por essa estrutura de rede recebe o nome de roteamento. O caminho de comunicação é conhecido como rota.

Imagine que o computador A deseja estabelecer uma conexão com o computador B, e cada ponto indicado por um número seja um nó dessa rede de computadores (Fig. 2):



f11095pb.cdr

Figura 2 - Roteamento

Essa conexão pode ser estabelecida usando (1,2,3,4,7) ou (1,5,6,7) ou (1,2,3,6,7), etc..

Em algumas tecnologias de rede, o caminho inicial escolhido para a conexão pode ser alterado, durante a comunicação entre os sistemas. Isso evita que uma comunicação seja interrompida em virtude de uma falha em algum nó ou uma queda em algum dos canais de comunicação.

Na tecnologia TCP/IP, o roteamento é feito com base em números de rede IP e em tabelas de roteamento.

Por exemplo:

rede	destino
200.6.48.0	ethernet
192.153.200.0	serial2
200.19.20.0	200.6.48.6
default	serial5

Nessa pequena tabela, as seguintes informações são apresentadas: sistemas da rede 200.6.48 são conectados via ethernet (rede local); os sistemas 192.153.155.1, 192.153.155.2,..., são acessíveis via interface serial 2 (uma conexão PPP por exemplo); do host 200.6.48.6 (máquina que atua como gateway) se chega a rede 200.19.20; finalmente, para qualquer outro endereço de rede, o destino e a interface serial 5.

Formas de Roteamento

Basicamente existem duas formas de roteamento em uma rede de computadores: o roteamento estático e o roteamento dinâmico.

No primeiro, as rotas de comunicação são estabelecidas previamente e não são alteradas, a não ser por intervenção de um operador, durante a comunicação.

Esse tipo de roteamento só é viável em redes pequenas e estáveis do ponto de vista de crescimento e mudanças. A vantagem dessa forma é a simplicidade de implementação (desde que a rede seja pequena).

No roteamento dinâmico as rotas são determinadas e atualizadas continuamente, em pequenos intervalos de tempo (três minutos, por exemplo). A determinação do melhor caminho e feita por meio de um protocolo de troca de informações de roteamento entre os nos envolvidos no processo (os roteadores) e da aplicação de um algoritmo de escolha de rota.

A maior dificuldade nesse tipo de roteamento e a escolha correta das fontes de informação de roteamento. Se a definição não é bem feita, uma possível divulgação de rotas inconsistentes e erradas colocará em risco toda a rede.

A escolha de uma rota pode levar em conta a distância (em termos de número de nós percorridos), o tempo gasto na comunicação, a capacidade de transmissão do canal, a confiabilidade do meio de transmissão, etc.

Na tecnologia TCP/IP existem dois grandes grupos de protocolos de roteamento: os de roteamento interior e os de roteamento exterior. O conceito por trás destes dois tipos é o de sistema autônomo.

Um sistema autônomo consiste em múltiplas redes e roteadores subordinados a uma única autoridade administrativa. Dentro de um sistema autônomo define-se o tipo de roteamento e a forma como ele será implementado. Esse é o roteamento interior.

O roteamento exterior consiste na troca de informações de roteamento entre diferentes sistemas autônomos.

Representando o primeiro grupo temos os protocolos RIP, HELLO, OSPF e outros. No segundo grupo, o mais utilizado atualmente e o BGP4.

Referências:

- Commer, Douglas E. *Interneworking With TCP/IP - Vol. I: Principles, Protocols, and Architecture*. Prentice-Hall International, Inc. ISBN 0-13-474321-0.

  gated(8) - implementa os protocolos RIP1/2, HELLO, OSPF, EGP, BGP1/2/4, IS-IS e o DVMRP no *Unix*.

- Hedrick, C. *Routing Information Protocol* RFC1058. STD 34. Atualizado por [Mal94]. Junho de 1988.

- Malkin, G. *RIP Version 2 Carrying Additional Information* RFC1723. Novembro de 1994.

- Moy, J. *OSPF Version 2* RFC 1583. Março de 1994.

- Rekhter, Y.; Gross, P. *Application of the Border Gateway Protocol in the Internet*, RFC1772. Março de 1995. 19 p.

- Rekhter, Y.; Li, T. *Border Gateway Protocol 4 (BGP-4)* RFC1771. Julho de 1994. Março de 1995.

routed(8) - implementa o RIP no *Unix*.

- Socolofsky, T.; Kale, C. *TCP/IP Tutorial* RFC1180. Janeiro de 1990.

- Traina, P. *Experience with the BGP-4 protocol*, RFC1773. Março de 1995. 9 p.

- Willis, S.; Burruss, J.; Chu, J. *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*, RFC1657. Julho de 1994. 21p.

Repositório:
http://www.gated.org/ (Merit)

4.2. DNS

Nesta seção fazemos uma introdução ao serviço de nomes da Internet, o chamado *Domain Name System* (DNS), e ao procedimento de registro de redes e domínios da INTERNET/BR.

O DNS é o serviço Internet que tem como objetivo principal a conversão de nomes de maquinas em endereços IPs e vice-versa. As máquinas são agrupadas em domínios, que podem estar contidos em outros domínios, formando assim uma estrutura hierárquica, análoga a uma estrutura de diretórios usada em alguns sistemas operacionais. Nesta analogia, um domínio corresponde a um diretório, e um arquivo corresponde a uma máquina. Por exemplo, o nome www.ci.rnp.br denomina a maquina ``www'' do domínio ci.rnp.br, e o domínio ci.rnp pertence ao domínio br.

Este serviço possui uma base de dados distribuída, controlada por servidores de nomes (DNS *servers*), como o *named* (seção 4.2.2). Cada domínio deve ter um servidor primário e um ou mais servidores secundários. O servidor primário e o responsável pelas informações sobre o seu domínio. Os servidores secundários apenas mantêm as informações obtidas junto ao servidor primário de um domínio, cuidando de atualizar esta informação periodicamente, sempre que necessário.

A base de dados do DNS pode ser vista como um único domínio raiz ("."), equivalente ao "/" do *Unix*. Ligado diretamente ao "." temos um subdomínio para cada país. Assim "br", para Brasil, "ar", para Argentina, etc. Dentro do "br" ha subdomínios em função da natureza da atividade desenvolvida pela instituição. Assim, temos:

- **br.** - para instituições educacionais (como *default*)
- **com.br.** - para instituições comerciais
- **gov.br.** - para instituições governamentais
- **mil.br.** - para instituições militares
- **net.br.** - para instituições provedoras de *backbones*
- **org.br.** - para organizações não governamentais sem fins lucrativos

O domínio arpa.in-addr abriga os subdomínios de números IPs, também chamados de domínios reversos. Enquanto os domínios diretos são utilizados para localizar os números IPs de uma máquina, conhecendo-se um dos seus nomes, o domínio reverso é utilizado para localizar o nome de uma máquina conhecendo-se um dos seus números IPs.

Para que o DNS funcione, é preciso que o servidor de um determinado domínio conheça todos os seus subdomínios, bem como quais são seus servidores e quais os seus respectivos números IPs. O processo de criação de um novo domínio em um servidor é chamado de registro. Em seguida abordaremos os processos de aquisição de números IPs e registros no DNS.

4.2.1. Aquisição de Endereços IPs e Registro no DNS

A seguir, são indicados os procedimentos necessários para realizar a ligação de uma rede a INTERNET/BR. São eles:

- solicitação de números IPs
- registro no DNS do seu domínio
- registro no DNS do seu domínio reverso

Solicitação de Números IPs

O emprego de endereços oficiais é indispensável para realizar a ligação de máquinas à Internet. Posto que duas máquinas não podem ter o mesmo endereço e que todo o roteamento de pacotes, nos *backbones*, é feito por blocos de endereços, torna-se necessário que uma máquina, ligada a INTERNET/BR, utilize um endereço destinado a esta rede.

A obtenção de endereços oficiais é, portanto, requisito indispensável para ligação de uma rede à Internet.

Endereços IPs oficiais devem ser solicitados ao provedor de acesso ou de *backbone* ao qual sua rede está ou irá conectar-se.

Registro no DNS

De posse de endereços IPs oficiais, um servidor DNS deve ser configurado como servidor do seu domínio (seção 4.2.2), para posteriormente ser solicitado o respectivo registro.

A solicitação de registro do seu domínio no DNS deve ser feita à instituição responsável pelo domínio imediatamente superior. Assim, se seu domínio for meu-dep.empresa.com.br, você deve encaminhar a solicitação ao responsável pelo domínio empresa.com.br.

A solicitação de registro no DNS deve ser feita apenas após haver a disponibilidade de endereços IPs oficiais e após a correta configuração do seu servidor de nomes. Portanto, você deve aguardar o recebimento desses endereços antes de solicitar o registro no DNS.

O endereço do responsável por determinado domínio pode ser encontrado por meio do comando nslookup, do *Unix*, da seguinte forma:

```
nslookup
> server 143.108.1.17
Default Server: dixit.ansp.br
Address: 143.108.1.17

> set type=3Dsoa
> fapesp.br
Server: dixit.ansp.br
Address: 143.108.1.17

fapesp.br
origin =3D dixit.ansp.br
mail addr =3D root.dixit.ansp.br
serial =3D 95015500
refresh =3D 7200 (2 hours)
retry =3D 7200 (2 hours)
expire =3D 3600000 (41 days 16 hours)
minimum ttl =3D 86400 (1 day)
>
```

onde fapesp.br deve ser substituído pelo domínio desejado (exemplo, empresa.com.br) e root.dixit.ansp.br indica que o endereço eletrônico do responsável técnico do domínio em questão é root@dixit.ansp.br.

Registro no DNS do seu Domínio Reverso

O registro do domínio reverso permitirá que uma máquina, conhecendo um endereço IP, consiga saber qual o nome completo (nome.domínio) correspondente a este endereço.

A solicitação de registro no DNS do seu domínio reverso deve ser feita apenas após o registro no DNS do seu domínio direto (procedimento anterior) ter sido concretizado.

Formulários Internet/BR

O formulário de solicitação de números IPs para redes que serão ligadas diretamente ao *backbone* Internet Brasil, o formulário de solicitação de registro nos domínios br., com.br., gov.br, mil.br., org.br. e o formulário de requisição de registros do domínio reverso estão disponíveis em:

http://www.ci.rnp.br/doc/formularios/formularios.html

4.2.2. Servidor DNS

O *software* servidor de DNS mais popular é o *Berkeley Internet Name Domain* (BIND), de Kevin Dunlap, o *named*. Portado para a maioria dos *Unix*, ele é distribuído, em geral, como parte integrante desses sistemas.

Referências:

- Albitz, Paul; Liu, Cricket. *DNS and BIND*/ O'Reilly & Associates, Inc. 1992. ISBN 1-56592-010-4.

- Gerich, E. *Guidelines for Management of IP Address Space*, Ann Arbor, MI: Merit Network, Inc.; May 1993; RFC 1466. 10 p. (DS.INTERNIC.NET RFC1466.TXT).

- Harrenstien, K.; Stahl, M.K.; Feinler, E.J. *DoD Internet Host Table Specification*. Menlo Park, CA: SRI International, DDN Network Information Center; 1985 October; RFC 952. 6 p. (RS.INTERNIC.NET POLICY RFC952.TXT). Obsoletes: RFC 810

- Harrenstein, K.; Stahl, M.K.; Feinler, E.J. *Hostname Server*. Menlo Park, CA: SRI International, DDN Network Information Center; 1985 October; RFC 953. 5 p. (NIC.DDN.MIL RFC:RFC953.TXT). Obsoletes: RFC 811

- Mockapetris, P. *Domain Names - Concepts and Facilities*. Marina del Rey, CA: University of Southern California, Information Sciences Inst.; 1987 November; RFC 1034. 55 p. (RS.INTERNIC.NET POLICY RFC1034.TXT). Updated-by: RFC 1101 Obsoletes: RFC 973; RFC 882; RFC 883

- Mockapetris, P. *Domain names - Implementation and Specification*. Marina del Rey, CA: University of Southern California, Information Sciences Inst.; 1987 November; RFC 1035. 55 p. (RS.INTERNIC.NET POLICY RFC1035.TXT). Updated-by: RFC 1101 Obsoletes: RFC 973; RFC 882; RFC 883

- Mockapetris, P. DNS *Encoding of Network Names and Other Types*. Marina del Rey, CA: University of Southern California, Information Sciences Inst.; 1989 April; RFC 1101. 14 p. (RS.INTERNIC.NET POLICY RFC1101.TXT). Updates: RFC 1034; RFC 1035

- Mogul, J.; Postel, J.B. *Internet Standard Subnetting Procedure*. Stanford, CA: Stanford University; 1985 August; RFC 950. 18 p. (DS.INTERNIC.NET POLICY RFC950.TXT).

named(8) - o servidor DNS do *Unix*.

nslookup(8) - ferramenta para depuração do DNS, distribuída com o BIND e com a maioria dos *Unix*.

- Postel, J.B.; Reynolds, J.K. *Domain Requirements*. Marina del Rey, CA: University of Southern California, Information Sciences Inst.; 1984 October; RFC 920. 14 p. (RS.INTERNIC.NET POLICY RFC920.TXT).

resolv.conf(5) - o arquivo de configuração do resolver (cliente DNS) no *Unix*.

- Rekhter, Y., Moskowitz. B., Karrenberg, D., de Groot, G. *Address Allocation for Private Internets*, IBM Corp., Chrysler Corp., RIPE NCC; March 1994; RFC 1597. 8 p. (DS.INTERNIC.NET RFC1597.TXT).

- Reynolds, J.K.; Postel, J.B. *Assigned Numbers*. Marina del Rey, CA: University of Southern California, Information Sciences Inst.; 1992 July; RFC 1340. 139p. (DS.INTERNIC.NET POLICY RFC1340.TXT). Note: the current version is always available as "STD 2".]

- Stahl, M.K. *Domain Administrators Guide*. Menlo Park, CA: SRI International, DDN Network Information Center; 1987 November; RFC 1032. 14 p. (RS.INTERNIC.NET POLICY RFC1032.TXT).

Repositórios:

ftp://ftp.ci.rnp.br/pub/packages/dns/bind
ftp://ftp.vix.com/pub/bind

4.3. Correio Eletrônico

O correio eletrônico é um serviço clássico da rede e provavelmente o mais popular. Sendo um serviço do tipo *store-and-forward*, ele possui alguns elementos importantes para o seu funcionamento. São eles:

- os programas de interface com o usuário, conhecidos como UAs *(User Agents*), como o *mail* do *Unix*, o *elm*, o *pine*, o EUDORA ou o PMAIL;
- os MTAs (*Message Transfer Agents*), do correio eletrônico, sendo o *sendmail* do *Unix* o mais popular;
- os *mailers*, que são agentes usados para efetuar a transferência de mensagens entre diversos sistemas de comunicação como o TCP/IP, UUCP, DECNET, BITNET, etc.

4.3.1. *Sendmail*

O *sendmail* é um MTA de propósito geral que, quando utilizado sobre o TCP/IP, implementa o *Simple Mail Transfer Protocol* (SMTP). Entre suas capacidades destacamos também os mecanismos de *alias*, *forward*, inclusão e execução de processos remotos, além da capacidade de conversão de formatos de mensagens.

Foi desenvolvido por Eric Allman da Universidade da California - Berkeley, de acordo com as RFC 822 (*Internet Mail Format Protocol*), RFC 821 (SMTP), RFC 1123 (*Internet Host Requirements*) e RFC 1425 (SMTP *Service Extensions*). O sistema e tão flexível que pode ser configurado com requisitos adicionais que superam os padrões especificados nas RFCs.

O *sendmail* foi portado para diversas plataformas, dentre a quais citamos: *AIX, ConvexOS, FreeBSD, HP-UX, IRIX, Linux, NetBSD, OSF/1, SOLARIS, SunOS, ULTRIX*. A versão mais recente, onde foram corrigidos *bugs* clássicos, pode ser encontrada em:

ftp://ftp.ci.rnp.br/pub/packages/mail/sendmail
ftp://ftp.cs.berkeley.edu/pub/sendmail

A versatilidade do *sendmail* torna-o vulnerável com relação à segurança. Portanto, é importante e recomendável configurá-lo corretamente, não apenas para o perfeito funcionamento do serviço, mas também como forma de precaução quanto a possíveis problemas de segurança.

A configuração é bastante simples: o pacote contém vários arquivos *.mc que refletem as diversas características e opções do sistema. Com o m4 (macro processor), são gerados os arquivos de configuração *.cf.

Referências:

FAQs:
ftp://rtfm.mit.edu/pub/usenet/news.answers/mail/sendmail-faq
ou envie uma mensagem com conteúdo
send usenet/news.answers/mail/sendmail-faq para
mail-server@rtfm.mit.edu

Newsgroups:
comp.mail.sendmail

RFCs:
- RFC 821 - SMTP protocol
- RFC 822 - Mail header format
- RFC 974 - MX Routing
- RFC 976 - UUCP mail format
- RFC 1123 - Host requirements
- RFC 1413 - Identification server
- RFC 1341 - MIME: Multipurpose Internet Mail Extensions
- RFC 1344 - Implications of MIME for Internet Mail Gateways
- RFC 987 - Mapping between RFC 822 and X.400
- RFC 1049 - Content-Type header field (extensão para RFC 822)

- Costales, Bryan; Allman, Eric; Rickert, Neil.. *sendmail*. O'Reilly & Associates, Inc. ISBN 1-56591-056-2

4.3.2. POP

O servidor POP, *Post Office Protocol* server, é um gerenciador de *mailboxes* que pode ser executado em uma variedade de Sistemas *Unix*, e no *WindowsNT*.

Através do POP, o correio eletrônico pode ser utilizado diretamente em equipamentos como PCs e *Macintosh*, executando nesses equipamentos programas "*user agent*"s (UA) como PMAIL e Eudora.

Basicamente, a manutenção das *mailboxes* e feita por um servidor que implementa o sistema de correio eletrônico (MTA) e o serviço POP. Através do POP, portanto, a *mailbox* e transferida para o computador pessoal em questão, onde as mensagens, *folders*, etc., são manipulados localmente.

Foi desenvolvido pela Universidade de Berkeley na California atendendo as especificações contidas nos RFC1081 e RFC1082.

Repositórios:
ftp://ftp.ci.rnp.br/pub/packages/mail/POP/qpopper
ftp://ftp.qualcomm.com/quest/unix/servers/popper

4.4. Gerência de Redes

A administração técnica de uma rede envolve uma série de atividades que, conjuntamente, visam ao funcionamento adequado da mesma, e incluem:

- monitoração da performance da rede e de máquinas (utilização da banda, CPU, memória, etc.);
- detecção de falhas (queda de conexões, problemas no cabeamento da rede, queda de servidores, etc.);
- previsão de problemas futuros (equipamentos e linhas sobrecarregados).

Para auxiliar o administrador da rede a desempenhar estas tarefas, existem ferramentas comerciais e de domínio público, que podem ser divididas em quatro categorias:

- ferramentas de âmbito físico que detectam problemas em termos de cabos e conexões de hardware;
- monitores de rede, que se conectam às redes monitorando o tráfego;
- analisadores de rede, que auxiliam no rastreamento e correção de problemas encontrados nas redes; e
- sistemas de gerência de redes, os quais permitem a monitoração e controle de uma rede inteira a partir de um ponto central.

A escolha por um ou outro produto depende basicamente do grau de gerenciamento do tamanho da rede, das plataformas utilizadas e do capital disponível. Uma recomendação básica a ser feita na hora da escolha do produto de gerenciamento e dos equipamentos gerenciados (roteadores, servidores de comunicação, etc.) é a existência do protocolo de gerência SNMP (*Simple Network Management Protocol*). O SNMP e considerado protocolo padrão para gerência de redes TCP/IP.

Alguns dos produtos comerciais disponíveis no mercado para gerência de redes estão relacionados a seguir:

- CABLETRON
  http://www.ctron.com
  Spectrum 3.0
  Spectrum Portable Management Application (família de aplicações e módulos de gerência para dispositivos da Cabletron) Remote LANVIEW/Windows

- CISCO
  http://www.cisco.com
  CiscoWorks
  Workgroup Director
  NetScout
  Connectivity Baseliner

Connectivity Solver
Network Drawing Tool

- 3COM
  http://www.3com.com
  Transcend

- DIGITAL
  http://www.dec.com
  Polycenter

- HP
  http://www.hp.com
  HP-OpenView
  NetServer (gerenciador de servidores)
  HP Openview Operations Center

- IBM
  http://www.ibm.com
  Netview/6000
  TT/6000 (sistema de Trouble ticket)
  System Monitor

- NEWBRIDGE
  http://www.vivid.newbridge.com
  VIVID System Manager
  VIVID Router Server

- NOVELL
  http://www.novell.com
  Manage Wise
  NetWare Management System
  NetWare Management Agent
  NetWare Management Agent for Netview
  NetWare LANalyser Agent

LANanlyse for Windows
Netware Navigator
Netware HUP Services

- SUN
  http://www.sun.com
  Solstice
  SNM for Solstice
  Netra System Management Server

- SYNOPTICS (Bay Networks)
  http://www.synoptics.com
  Optivity 6.0

- TIVOLI
  http://www.tivoli.com
  TME

A seguir, são listados alguns *softwares* de domínio público, juntamente com os endereços dos repositórios onde podem ser encontrados. Na FAQ do SNMP é mantida, também, uma lista de pacotes para gerência distribuídos gratuitamente.

- BTNG (Beholder- The Next Generation)
  monitor de redes Ethernet
  ftp: dnpap.et.tudelft.nl:/pub/btng

- HNMS (NAS Hierarchical Network Management System)
  sistema de gerência de redes para monitorar o status e gerar estatísticas de trafego para uma rede IP
  ftp: ftp.netcom.com:/pub/heyjude

- Nocol (Network Operations Center OnLine)
  monitor de redes TCP/IP
  ftp.jvnc.net:pub/jvncnet-packages/nocol

Pacotes para desenvolvimento de ferramentas de gerência:

- CMU Package
  ftp: lancaster.andrew.cmu.edu

- MIT Package
  ftp: thyme.lcs.mit.edu:/pub/snmp

- OSIMIS
  http://www.cs.ucl.ac.uk/people/knight/osimis/osimis.htm

- ISODE
  ftp: gatekeeper.dec.com:/.3/net

Repositório de MIBs Internet:
ftp: venera.isi.edu:/mib

Referências:
http://www.slac.stanford.edu/netdoc/perf-rep.html
(Monitoração e Analise de redes da Universidade de Stanford)
http://smurfland.cit.buffalo.edu/NetMan/index.html
(Informações gerais sobre gerência de redes)
http://snmp.cs.utwente.nl
(Informações gerais sobre gerência de redes).

Apresentação de Padrões:

- BRISA. Gerenciamento de Redes, Uma Abordagem de Sistemas Abertos. São Paulo, Makron Books, 1993
- PERKINS, DAVID T. Understanding SNMP MIBS. Rev. 1.1.6, September, 1993
- RFC1157 - CASE, J. et. al. A Simple Network Management Protocol (SNMP), 1990
- RFC1156 - MCGLOGHRIE, K.; ROSE, M. Management Information Base for TCP/IP-based internets, 1990

- RFC1065 - ROSE, M; MCGLOGHRIE, K. Structure and Identification of Management Information for TCP/IP-based internets, 1990
- RFC1158 - ROSE, M. Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, 1990
- STALLINGS, WILLIAM. SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards. Addison-Wesley, 1993

Textos Introdutórios:

- FEIT, SIDNIE. SNMP: A Guide to Network Management. McGraw-Hill, 1994.
- FISHER, S. Dueling Protocols. BYTE, v.16, n.3, p.183-190, 1991.
- RNP/DOC/0037 - ODA, C. S. Introdução à Gerência de Redes, 1994
- RNP/DOC/0034 - ODA, C. S. Gerenciamento de Redes de Computadores - Noções Básicas
- ROSE, M. The Simple Book- An Introduction to Management of TCP/IP-based Internet. 2nd edition. Englewood Cliffs, Prentice-Hall, 1991.
- SCHNAIDT, P. Keep It Simple. Lan Magazine, p.82-92, julho 1990

Exemplos de Aplicação Prática:

- HARNEDY, SEAN J. Total SNMP: Exploring the Simple Network Management Protocol. CBM Books, 1994
- LEINWAND, ALLAN, AND FANG, KAREN. Network Management: A Practical Perspective. Addison-Wesley, 1993
- MILLER, MARK E., P.E., Managing Internetworks with SNMP: The Definitive Guide to the Simple Network Management Protocol (SNMP) and SNMP version2. M&T Books, 1993
- ROSE, MARSHALL T. AND MCCLOGHRIE, KEITH Z. How to Manage Your Network Using SNMP: The Network Management Practicum. Prentice-Hall, 1995 (published in 1994)

5. SEGURANÇA

O propósito desta seção é guiar o provedor de serviços Internet buscando instrumentá-lo para fornecer um serviço seguro aos seus clientes, operando o seu *site* com segurança. Indicamos aqui ferramentas de apoio a uma política de segurança, os principais fóruns sobre segurança e referências bibliográficas interessantes.

A segurança das máquinas e da rede de um provedor de serviços Internet, sob a responsabilidade do provedor, é apenas um dos aspectos de uma política de segurança acordada entre os responsáveis pela rede e os usuários. A concepção de uma política adequada de segurança deve sempre levar em conta os custos para implementação dessa política, os seus benefícios e valor do objeto segurado, i.e., das informações contidas na sua rede. A RFC 1244, *Site Security Handbook* ([HR91]), é um guia para a implantação de uma política e procedimentos de segurança em uma rede ligada à Internet.

A implantação dos procedimentos de segurança, decorrentes da política de segurança adotada, é de responsabilidade da operação da rede em questão. É fundamental o conhecimento dos recursos computacionais disponíveis, servidores (Internet e de comunicação) e roteadores assim como manter-se atualizado sobre os sistemas empregados. A documentação dos sistemas utilizados é uma leitura indispensável. Os fóruns disponíveis na própria rede sobre cada sistema e indicados na seção 2.7.2 devem ser lidos periodicamente. Esses o manterão atualizado sobre os problemas e soluções também no tocante à segurança do sistema operacional utilizado pelo seu servidor Internet. Outros fóruns e organismos importantes são:

cvv@dixit.ansp.br Para onde devem ser enviadas denúncias ou suspeitas de violações na Internet Brasil.

CERT - *Computer Emergency Response Team* - Criado em 88 pela Defense Advance Research Projects Agency (DARPA), funciona como ponto central de denúncias de violações.

O CERT publica recomendações sobre segurança da rede através do newsgroup:

comp.security.announce

ou da lista:

cert-advisory@cert.org (subscrições em
cert-advisory-request@cert.org)

As recomendações são arquivadas em

ftp://ftp.cert.org/pub/cert_advisories

e espelhadas em

ftp://ftp.ci.rnp.br/pub/net-info/cert_advisories

DDN - Defense Data Network - Security Bulletins - Similar aos boletins do CERT, voltado para a DDN.

Lista: subscrições para **nic@nic.ddn.mil**

Arquivo: **ftp://nic.ddn.mil/scc**

Improving the Security of Your UNIX System ([Cur90]), apesar debaseado no antigo *SunOS*, da *Sun*, possui uma boa *check list* para ser feita no seu sistema. *Computer Security Basics* ([RG91]) explica conceitos básicos de segurança em computadores. *Pratical UNIX Security* ([GS91]) é uma excelente leitura para quem utiliza o UNIX (BSD ou System V) e se preocupa com segurança.

Apresentaremos a seguir algumas das mais populares ferramentas de segurança disponíveis na Internet. Em geral, essas ferramentas são encontradas na forma de código fonte, escritas em C, para sistemas *Unix*. Dividimos em quatro tipos: para o controle de acesso ao servidor Internet (seção 5.1); para o monitoramento da rede (seção 5.2); para auditoria da rede (seção 5.3); e para o controle de acesso à rede (seção 5.4).

5.1. Auditoria do Servidor

Ferramentas de auditoria no servidor buscam encontrar furos ou potenciais furos de segurança. O COPS e o tiger são equivalentes quanto a seus objetivos, buscando auditorar todo o sistema. O *crack* busca descobrir, a partir de um conjunto de dicionários e de uma coleção de senhas cifradas pelo *crypt*(3) do *Unix* (mantidas, em geral, no /etc/passwd), quais são essas senhas. O uso do *crack* é aconselhado se o seu *Unix* não usa *shadow password* (senhas escondidas) ou se você utiliza o *Network Information Service* (NIS). O *tripewire* busca detectar, por meio da comparação de assinaturas, modificações em arquivos que, em princípio, não deveriam ser modificados, como os executáveis do sistema.

COPS (Computer Oracle and Password System)
ftp://ftp.ci.rnp.br/pub/packages/security/system_monitoring/cops
ftp://ftp.cert.org/pub/tools/cops

Crack
ftp://ftp.cert.org/pub/tools/crack

Tiger
ftp://ftp.ci.rnp.br/pub/packages/security/system_monitoring/tiger
ftp://net.tamu.edu/pub/security/TAMU

Tripewire
ftp://ftp.ci.rnp.br/pub/packages/security/system_monitoring/tripwire
ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire

5.2. Controle de Acesso ao Servidor

Ferramentas de controle de acesso a um servidor Internet buscam bloquear ou autorizar o acesso a determinados serviços (FTP, WWW, *telnet*, *rlogin*, *lpd*, etc.) por parte de um determinado conjunto de máquinas. É o caso aqui do *tcp wrappers*, que também possibilita o *log* do acesso a esses mesmos serviços. O *courtney* visa detectar o ataque do SATAN a determinado servidor. Foi colocado aqui também o *npasswd*, que busca instruir os usuários do *Unix* durante a troca de suas senhas, procurando inibir senhas que são facilmente descobertas por ferramentas como o *crack*. O *identd*, de fato, não controla o acesso ao servidor local, mas fornece o nome do usuário que está utilizando um servidor remoto a partir do servidor local. O *identd* implementa o protocolo descrito na RFC 1413 ([Joh93]).

courtney
ftp://ftp.ci.rnp.br/pub/packages/security/network_monitoring/courtney
ftp://ciac.llnl.gov/pub/ciac/sectools/unix

ident
ftp://ftp.ci.rnp.br/pub/packages/security/pidentd
ftp://ftp.lysator.liu.se/pub/ident/servers

npasswd
ftp://ftp.ci.rnp.br/pub/packages/security/authentication/npasswd
ftp://ftp.cc.utexas.edu/pub/npasswd

tcp wrappers
ftp://ftp.ci.rnp.br/pub/packages/security/network_monitoring/argus/tcp_wrappers
ftp://ftp.sei.cmu.edu/pub/argus-1.5

5.3. Monitoramento da Rede

As ferramentas para monitorar a rede possibilitam o *log* pacotes ou partes de pacotes de rede, podendo ser utilizado também para deburação de problemas com a rede ou como grampo, buscando identificar o que é mandado em determinados pacotes. Além do *sniffer* e do *tcpdump* verifique se o sistema adotado não possui já alguma ferramenta semelhante.

sniffer
tcpdump
ftp://ftp.ee.lbl.gov/tcpdump2.2.1.tar

5.4. Auditoria da Rede

As ferramentas de auditoria da rede buscam encontrar furos de segurança em serviços e servidores disponíveis. Elas devem ser rodadas apenas na sua rede local, buscando descobrir seus furos. O SATAN, em especial, aparece uma opção bastante interessante, pela farta documentação que o acompanha.

iss
ftp://ftp.ci.rnp.br/pub/packages/security/system_monitoring/iss
ftp://ftp.iss.net/pub/iss

SATAN (Security Administrator Tool for Analyzing Network)
ftp://ftp.ci.rnp.br/pub/packages/security/network_monitoring/courtney
ftp://ciac.llnl.gov/pub/ciac/sectools/unix

5.5. Controle de Acesso à Rede - *Firewalls*

O controle de acesso a toda uma rede é feito habilitando ou desabilitando a passagem de um conjunto predeterminado de pacotes por um determinado roteador ou conjunto de roteadores, chamados *firewalls*. Um *firewall* pode ser implementado utilizando-se equipamentos dedicados como *firewall*, ou aproveitando recursos disponíveis em roteadores dedicados, como indicado na *Internet Firewalls* FAQ

(**http://www.access.digex.net/~nuance/firewall.html**),

ou, ainda, configurando um servidor Internet como roteador e *firewall*, como é feito pelo screend. *Building Internet Firewall* ([CZ95]) aprofunda a técnica. Em

http://heimdal.sysadmin.com/security/firewalls.html

encontramos uma lista de firewalls comerciais.

screend
ftp://gatekeeper.dec.com/pub/DEC/screend/screend.tar.Z

5.6. Referências

- Cheswick, Bill; Bellovin, Steve. *Firewalls and Internet Security*. Reading, MA: Addison-Wesley, 1994. ISBN 0-201-63357-4.

- Curry, David A. *Improving the Security of Your UNIX System*. ITSTD-721-FR-90-21. SRI International. Information and Telecommunications Sciences and Technology Division. Abril de 1990. **ftp://ftp.cr-df.rnp.br/pub/netinfo/security/unix-security.ps**

- Chapman, D. Brent; Zwicky, Elizaabeth D. *Building Internet Firewall*. 350 p. ISBN 1-56592-124-0. O'Reilly & Associates, Inc.

- Garfinkel, Simson; Spafford, Gene. *Pratical UNIX Security*. 512 p. ISBN 0-937175-72-2. O'Reilly & Associates, Inc.

- Johns, M. St. *Identification Protocol*. RFC 1213. Fevereiro 1993. 8 p. **ftp://ftp.ci.rnp.br/pub/net-info/rfc/rfc1213.txt ou ftp://ftp.cis.ohio-state.edu/pub/internic/rfc/rfc1213.txt.**

- Holbrook, P; Reynolds, J. *Site Security Handbook*. RFC 1244. Julho 1991. 101 p. FYI 8. **ftp://ftp.ci.rnp.br/pub/net-info/rfc/rfc1244.txt ou ftp://ftp.cis.ohio-state.edu/pub/internic/rfc/rfc1244.txt.**

- Russell, Deborah; Gangemi Sr., G.T. *Computer Security Basics*. Julho de 1991. 464 p. ISBN 0-937175-71-4. O'Reilly & Associates, Inc.

ANEXO

A. REFERÊNCIAS DE OURO

Administração de sistemas *Unix*

- Nemeth, Evis; Snyder, Garth; Seebass, Scott; Hein, Trent R. *UNIX System Administration Handbook* Prentice Hall. ISBN 0-13-151051-7.

Pontos de intercâmbio entre provedores Internet

David's Amazing Internet Creations
http://www.amazing.com/

Scripts and Patches for ISP's
http://www.westnet.com/providers/

Protocolos TCP/IP

- Commer, Douglas E. *Interneworking With TCP/IP - Vol I: Principles, Protocols, and Architecture*. Prentice-Hall International, Inc. ISBN 0-13-474321-0.

Programação em rede c/ *Unix*

- Stevens, W. Richard. *UNIX Network Programming* Prentice Hall. ISBN 0-13-949876-1.

FYI 8.
ftp://ftp.ci.rnp.br/pub/net-info/rfc/rfc1244.txt ou
ftp://ftp.cis.ohio-state.edu/pub/internic/rfc/rfc1244.txt.

- Russell, Deborah; Gangemi Sr., G.T. *Computer Security Basics*. Julho de 1991. 464 p. ISBN 0-937175-71-4. O'Reilly & Associates, Inc.