Universidade de Lisboa
Faculdade de Ciências

Departamento de Informática

RELATÓRIO DE ESTÁGIO

sobre

Participação na montagem da infraestrutura necessária para disponibilizar acesso directo à Internet

realizado no

PUUG - Grupo Português de Utilizadores do Sistema Unix

por

Carlos José Martins Canau

Lisboa, Setembro de 1994
Universidade de Lisboa
Faculdade de Ciências

Departamento de Informática

RELATÓRIO DE ESTÁGIO

sobre

Participação na montagem da infraestrutura necessária para disponibilizar acesso directo à Internet

realizado no

PUUG - Grupo Português de Utilizadores do Sistema Unix

por

Carlos José Martins Canau

Responsável pela FCUL: Prof. Pedro Veiga
Responsável pelo PUUG: Prof. José Legatheaux Martins

Lisboa, Setembro de 1994

AVISO

Este relatório tem carácter confidencial e só deve ser acessível ao júri de avaliação do mesmo

Índice

Capítulo 1

Introdução

Este relatório destina-se a descrever o trabalho efectuado pelo autor durante o estágio que realizou no quinto ano da Licenciatura em Informática da Faculdade de Ciências da Universidade de Lisboa (FCUL). Este estágio foi proposto ao Departamento de Informática da FCUL pelo Grupo Português de Utilizadores do Sistema Unix (PUUG) e teve o seu início em Janeiro de 1994 e terminou em Agosto do mesmo ano.

Intitulado "*Participação na montagem da infraestrutura necessária para disponibilizar acesso directo à Internet*", tinha como objectivo primordial participar na transformação do PUUG num "service provider" dando acesso sem restrições à Internet em Portugal (até à altura o PUUG só dava acesso a E-mail e News).

Os orientadores do estágio foram o Prof. Doutor José Legatheaux Martins, por parte do PUUG e o Prof. Doutor Pedro Veiga, por parte do Departamento de Informática da FCUL.

O presente relatório foi organizado nos seguintes capítulos principais:

• *Estágio* - Em que é descrita a instituição de acolhimento, o PUUG, e a forma como o estagiário se integrou na equipa. De seguida descrevem-se os objectivos do estágio e o plano elaborado para o mesmo. É ainda descrita a colaboração do estagiário no projecto em que o estágio se inseriu.

• *Internet* - A necessidade para a inserção deste capítulo deve-se ao facto da Internet ser o produto em questão no projecto. Assim, descreve-se o nascimento, evolução e a situação actual da Internet. Faz-se referência às principais aplicações existentes na Internet.

• *Apresentação do trabalho desenvolvido* - O trabalho que o estagiário desenvolveu no PUUG descrito detalhadamente. Este capítulo foi dividido nos seguintes subcapítulos:

- *Internet para individuais*
  - *Login*
  - *IP por linha série*
  - *Apoio a utilizadores*
- *Conectividade Internet por dialup*
- *Accounting de recursos*

• *Conclusões* - Conclusões sobre o trabalho efectuado e continuação do trabalho já desenvolvido.

Capítulo 2

Estágio

2.1 PUUG

O PUUG é uma instituição sem fins lucrativos, filiada na EurOpen (European Forum for Open Systems) e representa em Portugal a EUnet, consórcio europeu de 28 redes nacionais que dão acesso ao Internet mundial. Correntemente tem as suas instalações situadas nos edifícios da Uninova no *campus* da Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa.

Esta instituição surgiu em 1989 através da associação de várias pessoas ligadas a empresas que comercializam o sistema operativo Unix e investigadores universitários interessados neste sistema, destacando-se entre elas os dois responsáveis por este estágio, os Profs. Legatheaux Martins e Pedro Veiga.

Tendo como objectivos promover os sistemas abertos em geral e o Unix em particular, o PUUG tem levado a efeito diversas iniciativas neste sentido, passando por cursos, debates e seminários. Destaca-se o último evento em que o PUUG participou como entidade organizadora que está directamente relacionado com este estágio, concretamente o seminário 'Portugal na Internet' que ocorreu no LNEC - Laboratório Nacional de Engenharia Civil (entidade colaboradora do PUUG), em Fevereiro de 1994.

A principal iniciativa do PUUG é a manutenção do ramo português da EUnet através da qual fornece aos seus aderentes ligação à Internet tendo o presente estágio sido inserido nesta actividade. Esta rede existe em Portugal desde 1987 sendo inicialmente gerida pelo INESC - Instituto de Engenharia de Sistemas e Computadores. A partir do segundo semestre de 1990 a sua gestão passou para a responsabilidade do PUUG, altura em que este a pôs à disposição dos seus associados. Neste momento, o PUUG já entrou numa fase que lhe permite levar a Internet ao cidadão comum.

Comecei a colaborar com o PUUG quando frequentava o quarto ano da licenciatura em Informática da FCUL. Esta colaboração começou pela manutenção de software e mais tarde passou para a administração de sistemas Unix. Uma vez que já colaborava com o PUUG há mais de um ano aquando do início do estágio, não tive dificuldade em me inserir na equipa de trabalho do PUUG ao passar a estar presente a tempo inteiro.

2.2 Objectivos e plano de trabalho

Este estágio destinava-se a colocar um estagiário no projecto que o PUUG estava a iniciar na altura: a disponibilização de acesso directo à Internet. Anteriormente o acesso fornecido aos aderentes apenas passava pelo correio electrónico e pelos foruns de discussão da Usenet. O acesso IP apenas era disponibilizado até ao equipamento do PUUG.

Assim o estagiário deveria participar na montagem duma infraestrutura destinada a

satisfazer os objectivos do projecto. Esta infraestrutura deveria também permitir o acesso de aderentes individuais à Internet. O período de duração previsto para o projecto estava calculado num intervalo de tempo entre os seis e os oito meses. Tinha como pontos principais os seguintes:

- Estudo dos mecanismos de routing a utilizar e definição da arquitectura global;
- Desenho e concepção de sistemas de controlo, de accounting e de assistência aos utilizadores;
- Montagem do equipamento e ensaios preliminares;
- Seguimento da entrada em produção.

O estagiário tinha como objectivos preparar e montar um sistema de acesso a aderentes individuais, preparar a disponibilização de acesso DIALUP, desenvolver programas de vigilância e de accounting dos diversos subsistemas e seguir a colocação do novos serviços na fase de produção.

2.3 Inserção no PUUG

De salientar que o estagiário já estava inserido na equipa de trabalho do PUUG aquando do início do estágio, tendo participado na preparação inicial do projecto de acesso à Internet. Esta participação passou pela instalação e montagem de um novo *backbone* central no PUUG. Esta nova máquina era necessária para suportar a carga prevista para fornecer os serviços de rede assim que se disponibilizasse o novo acesso. A instalação implicou a conversão de todo o sistema de gestão de rede e de utilizadores existente no anterior *backbone*.

Capítulo 3

Internet

3.1 O que é ?

A Internet é uma rede de interconexão de redes baseadas nos protocolos TCP/IP. Esta rede, que se estende pelos cinco continentes, engloba uma comunidade de pessoas que usa e desenvolve as redes que a constituem. A partir destas redes, os utilizadores têm ao seu dispôr o acesso a uma imensa colecção de recursos informativos disponibilizados pelas mais diversas entidades. Tal como o vice-presidente dos Estados Unidos, Al Gore, refere, a Internet constitui o embrião das futuras "auto-estradas electrónicas da informação".

A Internet engloba cerca de 2,5 milhões de computadores interligados entre si englobados em cerca de 60000 redes. É estimado que o número de utilizadores que acedem à Internet ronde os 25 milhões de pessoas. Com base nestes números e na imensidão de recursos que disponibiliza, a Internet constitui a maior colecção mundial de servidores de informação bem como a maior rede mundial de correio electrónico. Com base nas diversas entidades que a utilizam, universidades, institutos de investigação, etc., a Internet torna-se num laboratório avançado de novas tecnologias de comunicações em produção real.

3.2 Como surgiu ?

No princípio surgiu a ARPAnet, uma rede experimental de longa distância ligando computadores e *terminal servers* subsidiada pelo Departamento de Defesa dos Estados Unidos (DoD). Foram criados métodos para regular a atribuição de endereços de rede e para criar standards para gerir a rede. Ao longo do tempo mais e mais redes locais se foram ligando. Isto implicou que surgisse a necessidade de criar um protocolo de rede que permitisse a interoperação entre as diversas redes. Assim surgiu o Internet Protocol (IP).

A evolução da Internet ao longo dos anos 80 foi promovida, essencialmente, por universidades e organismos de investigação. A partir do final desta década, a Internet espalhou-se para todo o mundo e perdeu o carácter de rede de investigação. No momento actual, a Internet dobra a sua dimensão e número de utilizadores todos os anos e mais de 60% dos computadores a ela ligados pertencem a organizações privadas.

3.3 Quem a controla ?

Quando surgiu como projecto financiado pelo DoD, era governada por este organismo. Mais tarde, na altura em que existia uma rede a cobrir os Estados Unidos financiada pelo governo americano, esta função passou para as mãos da NSFnet. Hoje em dia quem dita as

regras é a Internet Society (IS). Este organismo está dividido em vários grupos cada um com a sua função específica. O Internet Advisory Board (IAB) é responsável pela aprovação das normas e das políticas gerais, em particular, cria os standards da Internet e publica os Request For Comments (RFC). O IAB possui duas importantes organizações, a Internet Engineering Task Force (IETF) e a Internet Research Task Force (IRTF). Estas organizações tratam de questões técnicas através de vários grupos de Investigação (Research Groups) ou de Trabalho (Working Groups). Entre várias outras funções, a Internet Assigned Numbers Autorithy (IANA) tem a função de coordenar a atribuição de valores aos parâmetros dos protocolos da Internet que lhe é delegada pelo IAB. Entre estes inclui-se a atribuição de número de RFC a um documento. Por último a Internet é controlada pelos "Internet Providers" ao nível regional.

3.4 Acesso à Internet

Uma empresa, instituição ou pessoa individual, para aceder à Internet necessita de o fazer através do estabelecimento de um contracto com um "provider". Estes dividem-se em dois tipos principais, os puramente comerciais que existem como fornecedores de serviços, e os subsidiados, isto é, que recebem fundos de uma instituição ou de um governo para fornecer acesso à Internet. Estes últimos têm a possibilidade de oferecer o acesso gratuito criando o que por vezes se chama "freenets".

De referir que por vezes também surgem associações a fornecer acesso aos seus associados. De referir também que nos Estados Unidos já não existem "providers" totalmente gratuitos para as Universidades.

Um "provider" fornece um ponto de interligação à Internet, isto é, uma porta de entrada na rede global. À parte dele, os individuais ou as instituições têm os seus computadores integrados na malha mundial que é a Internet.

3.5 Aplicações

O correio electrónico (e-mail) permite a troca de mensagens entre indivíduos ou entre grupos de indivíduos. Permite ainda a comunicação com servidores de informação de forma a obter uma variedade de serviços. O e-mail é implementado na Internet através do protocolo "Simple Mail Transfer Protocol" (SMTP).

O protocolo TELNET permite a emulação de um terminal num sistema remoto. Este protocolo suporta um vasto leque de tipos de terminal e permite, por exemplo, que um utilizador trabalhe num computador situado em qualquer ponto da rede Internet. Vários organismos colocam ao dispôr do utilizador, via este protocolo, bases de dados e serviços informativos.

O "File Transfer Protocol" (FTP) implementa um serviço de transferência de ficheiros entre computadores que estejam ligados entre si através do protocolo TCP/IP. Com este protocolo um utilizador tem a possibilidade de obter um ficheiro de qualquer computador ligado à Internet, desde que este último o permita.

As Usenet News constituem foruns de debate repartidos por alguns milhares de grupos de discussão. Estes grupos são constituidos por artigos que são enviados para todos os computadores da Internet que aceitem receber o grupo. O método de difusão destes artigos é por "flooding".

O "Archie" é constituido por diversas bases de dados que contêm informação sobre ficheiros existentes em arquivos electrónicos da Internet. A obtenção da informação é efectuada através da pesquisa em indíces e é orientada por palavras chave. Pode ser utilizado

para procurar um programa específico através do seu nome.

As aplicações mais recentes que têm surgido na Internet estão viradas para a disponibilização de informação. São constituidas por ferramentas de pesquisa e acesso a informação, serviços de informação distribuídos e integrados, e por ferramentas de acesso a documentos de hipertexto que possibilitam a existência de aplicações multimedia.

Os dois protocolos de distribuição de informação mais vulgares são o "gopher" e o "World Wide Web" (WWW ou W3). O gopher põe ao dispôr do utilizador um conjunto de documentos organizados segundo uma estrutura arborescente em que cada ramo pode apontar para outro servidor ou para um documento. O WWW é constituido por documentos de hipertexto que podem incluir texto, imagem, som ou som e imagem (filme). A navegação nestes documentos é feita através da selecção de "ponteiros" para outros documentos semelhantes ou para outros servidores de protocolos diferentes (por exemplo: gopher, telnet ou ftp).

3.6 O que é que se passou com a Europa ?

Até 1989 a evolução da Internet na Europa atravessou uma expansão tímida tendo-se tornado actualmente no segundo motor mundial da expansão da Internet contando com cerca de 25% do total dos computadores ligados. Desde 1991 que existe uma participação activa da comunidade de investigação europeia tendo-se formado organizações de gestão sólidas, o RIPE e o RARE.

A EUnet surgiu em 1982, fundada por especialistas de *networking* ligados ao European Unix Users Group (EUUG), que tinham como objectivo primordial ligar os vários sistemas de correio electrónico utilizados pelos vários institutos de investigação e universidades europeus. A partir de 1989 a EUnet colocou disponível ligações directas à Internet através do protocolo TCP/IP. Neste momento a EUnet representa a maior rede de dados europeia entre organizações disponibilizando vários serviços de rede a mais de dez mil organizações.

3.7 Situação em Portugal

Em Portugal a primeira ligação global foi estabelecida em 1991 através de um projecto piloto financiado pela FCCN. Actualmente a totalidade das Universidades públicas portuguesas estão ligadas à Internet através desta entidade.

Neste momento existem em Portugal dois "providers", a FCCN, que fornece o acesso apenas a universidades e a laboratórios de Investigação e Desenvolvimento, e o PUUG que não tem restrições quanto ao tipo dos seus membros. Existe um novo "provider" comercial em vias de aparecer, a Telepac, empresa pública de telecomunições. Várias entidades têm manifestado intenções de fornecer acesso em Portugal, mas até ao momento, apenas as duas citadas, FCCN e PUUG, demonstraram a capacidade para o fazerem. É de esperar que, agora que o PUUG ajudou a demonstrar que a Internet é de grande interesse, surja um mercado concorrencial de "providers" com todas as vantagens e desvantagens que tal facto possa ter para os potenciais utilizadores.

3.8 TCP/IP

As aplicações descritas atrás estão implementadas sobre o protocolo Transmission Control Protocol/Internet Protocol (TCP/IP). Este nome é utilizado para designar um conjunto de mais de 100 protocolos de comunicação de dados utilizados para organizar computadores e

equipamento de comunicações de dados em redes de computadores. Este protocolo foi desenvolvido para ligar computadores pertencentes a três redes, a ARPANET, a PRNET e a SATNET, entretanto desaparecidas. O TCP/IP é o protocolo utilizado para ligar os computadores e restante equipamento de comunicação de dados da Internet.

Neste ponto não se desenvolve mais porque existe uma extensa bibliografia sobre o assunto. Para obter informação em maior detalhe, ver [BLA92] e [COM91].

Capítulo 4

Apresentação do trabalho desenvolvido

4.1 Internet para individuais

4.1.1 Motivação e estudo

Pensado com o objectivo de levar a Internet a um utilizador individual da forma mais simples possível, este tipo de serviço foi colocado à disposição do público pelo PUUG em Fevereiro de 1994. Alguns factores levaram a que o PUUG tomasse a decisão de iniciar o fornecimento do acesso à Internet para pessoas individuais. Entre eles destacam-se os seguintes:

- Desde que o PUUG possui acesso à Internet que existiam pedidos para disponibilizar um serviço deste género;
- Como representante português da EUnet, o PUUG ainda não fornecia este tipo de serviço;
- Em Setembro de 1993 o backbone do PUUG foi instalado numa nova máquina. A antiga ficou disponível tornando-se possível ter uma máquina apenas dedicada ao serviço de individuais.

Após a decisão de estabelecer o serviço foi procurado mais equipamento destinado a servir de suporte ao serviço. Além de uma máquina a funcionar como servidor eram ainda necessários um novo terminal server e novos modems destinados a suportar as ligações por linha comutada. Foi escolhido um terminal server da Livingston, o Portmaster 2 com suporte para 10 linhas série, e modems ZyXEL U-1496plus. As opções foram tomadas tendo em função a qualidade demonstrada pelo equipamento tanto pelos vários representantes da EUnet de outros países como em testes feitos com variado equipamento no PUUG.

O equipamento indicado acima permite o suporte de dois tipos de acesso individual: login numa máquina Unix e acesso à Internet por SLIP/PPP. Restava instalar software de apoio na máquina Unix e estudar a configuração do hardware de apoio. Posteriormente a gestão de utilizadores seria automatizada de forma a simplificar a administração do serviço.

De seguida é descrito o estudo e implementação deste serviço, sendo apresentado dividido nos dois tipos de acesso que o PUUG disponibilizou.

4.1.2 Serviço individual Login

Objectivos

Assegurar um login no servidor Unix de modo a permitir o acesso aos vários programas clientes das aplicações Internet como telnet, ftp, news, gopher, www, etc. Garantir a segurança em todos os aspectos no acesso ao servidor. Implementar uma política de administração de utilizadores e de accounting de recursos utilizados.

Hardware

No momento em que foi iniciada a implementação do sistema de suporte ao serviço Login, o servidor destinado ao suporte do mesmo ainda estava em produção. Assim, foi necessário efectuar a implementação num servidor semelhante de modo a facilitar a transferência do código fonte para a sua localização final no servidor. O terminal server e os novos modems foram adicionados ao futuro servidor entrando de imediato em produção.

4.1.2.1 Software geral

Estudo da arquitectura base

Pretendia-se implementar o acesso à máquina de forma a proteger duas coisas, a informação a que o utilizador tem acesso e as acções que o mesmo pode executar. Partindo da estrutura base do sistema de ficheiros do sistema operativo Unix, surge a implementação de uma estrutura hierárquica de directorias de suporte ao sistema Login. Desta forma simula-se um 'pseudo-sistema' operativo paralelo dedicado ao serviço.

A raíz da hierarquia foi colocada numa partição exclusiva de modo a facilitar o gestão do sistema a nível de backups e de controle de quotas (gestão de espaço em disco ocupado). É a seguinte a estrutura implementada:

/public/individual/
- *bin/*
- *etc/*
- *home/*
- *lib/*
- *man/*
- *src/*
- *tmp/*

fig. 1

A descrição de cada directoria é idêntica à do Unix:

bin/ Programas a que utilizador pode executar;
etc/ Ficheiros de configuração do subsistema;
home/ Directoria pai das subdirectorias de cada utilizador;
lib/ Ficheiros de dados de vários programas;

man/ Directoria com informação sobre os programas utilizados;
src/ Código-fonte dos diversos programas disponíveis;
tmp/ Directoria temporária para os programas do utilizador.

Escolha do software de suporte

Um dos factores com maior peso na escolha dos programas a inserir no sistema foi o suporte ou não do modo de terminal 'vt100'. Este modo é o mais vulgar estando implementado na maioria do software de comunicações interactivo. Através da utilização de posicionamento de cursor e de caracteres de cor inversa, permite a construcção de interfaces bastante simples mas funcionais e fáceis de utilizar.

Foram analisados vários programas disponíveis na Internet em código-fonte de forma a seleccionar os mais indicados para suportar o acesso aos recursos da Internet pelo utilizador. De seguida descrevem-se os programas seleccionados, o recurso a que acedem, a razão porque foram escolhidos e as alterações que foi necessário efectuar de forma a que o sistema mantivesse o grau máximo de segurança. Foram seleccionados os seguintes programas:

- **telnet** - Permite o acesso ao protocolo TELNET, i.e., o utilizador pode abrir sessões remotas noutras máquinas ou pode aceder a servidores que estejam à escuta em portas pré-determinadas em máquinas remotas.
  O software utilizado para implementar este tipo de acesso foi o distribuido com o código fonte do Berkeley Software Distribution (BSD). Foi escolhido devido ao facto de estar compilado em muitos sistemas operativos e de ser considerado bastante estável. Apenas foi utilizada a parte cliente do protocolo.
  Foi eliminado o 'shell escape' - possibilidade de executar um interpretador de comandos a partir do programa; o comando que permite alterar o valor das variáveis de ambiente foi também, retirado; foi eliminada a possibilidade de suspender o programa e retornar ao programa-pai que executa o telnet. O objectivo principal com estas alterações era permitir que o programa apenas executasse o que o utilizador tem acesso através do protocolo TELNET. Exemplos: conta numa máquina remota, acesso a uma base de dados por telnet, acesso a um servidor através de uma porta específica, etc. Todas as possibilidades de acesso à máquina local foram retiradas.

- **ftp** - É um cliente para o File Transfer Protocol. Permite transferir ficheiros entre máquinas que utilizem o protocolo TCP/IP. Em especial permite o acesso aos vários arquivos de informação, de software public-domain e de shareware existentes na Internet.
  Tal como para o programa telnet, optou-se pelo código fonte do cliente que é distribuido com o BSD. As razões para esta escolha foram as mesmas.
  Foram eliminados os comandos que permitem a execução duma shell e a possibilidade de colocar o programa em debug. O FTP permite dois modos de transferência de ficheiros, binário e ASCII. Como os ficheiros binários transferidos em ASCII ficam corrompidos, o código foi alterado para iniciar em modo binário. Devido ao facto de os modems de acesso estarem parametrizados com um timeout de cinco minutos, i.e., ao fim de cinco minutos de inactividade a chamada é desligada, o código, por defeito, utiliza o caractér '#' (hash) para indicar o progresso da transferência dos ficheiros. Desta forma há actividade na ligação servidor-modem-utilizador. Caso contrário uma transferência que demorasse mais de cinco minutos provocaria a queda da chamada.
  Após a análise dos tipos de acessos ao sistema de ficheiros local permitidos pelo programa, chegou-se à conclusão de que seria ideial que o programa apenas permitisse o acesso a

uma pequena parcela do sistema local. A solução encontrada foi alterar o código de forma a este efectuar uma mudança de entrada no sistema de ficheiros (*chroot*(2)). Esta mudança permite resolver o problema do acesso local (por exemplo, evita situações no género do comando '`put /etc/passwd passwd`'), mas acarreta consigo novos problemas que é necessário resolver. Em primeiro lugar, para um programa ter permissão de efectuar a chamada ao sistema '*chroot*(2)' necessita de estar a correr em nome do utilizador privilegiado, root. Isto resolve-se se o programa for SUID e se pertencer ao utilizador root. O utilizador fica, assim com a possibilidade de executar o programa em nome de root podendo então efectuar o '*chroot*(2)'. Esta solução levanta outro problema bem mais grave: o utilizador está a utilizar um programa em modo privilegiado! Nova alteração no código e a seguir ao '*chroot*(2)' são efectuadas mais duas chamadas ao sistema: mudança de grupo, '*setgid*(3)', e mudança de identificação de utilizador, '*setuid*(3)', para os valores do utilizador. Desta forma o programa passa a correr em nome do utilizador. Se não for possível obter os valores do utilizador, ou se alguma chamada ao sistema falhar, o programa aborta com o aviso de que o utilizador deverá entrar em contacto com a administração do serviço.

- **archie** - Permite a pesquisa em bases de dados que contêm milhares de entradas para os ficheiros que estão disponíveis em arquivos de FTP anónimo em todo o mundo.
  O acesso a um servidor de archie pode ser feito através do protocolo TELNET efectuando uma sessão remota na máquina onde o servidor está a correr. Este tipo de acesso obriga a uma maior carga nos servidores e obriga o utilizador a utilizar uma linha de comando para interrogar o servidor. Este tipo de acesso tem vindo a ser retirado dos servidores mundiais de archie. Assim, optou-se por procurar um cliente de archie que permitisse pesquisas não interactivas, i.e., que não obrigassem a que o servidor mantivesse uma sessão para cada cliente. Foi escolhido o cliente de archie posto à disposição pública na Internet por Brendan Kehoe. Este programa foi contruido pelo mesmo a partir da interface para o protocolo Prospero implementada por George Ferguson e Clifford Neuman.
  As únicas alterações ao código distribuido limitaram-se à actualização da tabela de servidores de archie conhecidos pelo programa e à alteração do servidor inquirido por defeito. Foi seleccionado para esta última opção o servidor localizado o mais perto possível do serviço, o archie.inesc.pt.
  Uma vez que o programa está preparado para ser utilizado segundo uma sintaxe de linha de comando, foi necessário preparar o sistema de forma a possuir uma interface para este programa. Isto é descrito mais à frente no ponto referente ao programa fesh.

- **tin** - Este programa é um cliente que permite o acesso às Usenet News. Torna possível a leitura dos milhares de grupos que constituem o sistema Usenet. Com ele o utilizador pode compor um artigo a publicar num grupo ou grupos à sua escolha. O tin pode aceder a artigos colocados no sistema de ficheiros local ou através do protocolo NNTP a um servidor remoto.
  Este programa foi desenvolvido por Iain Lea e de entre os vários leitores de news existentes na Internet destaca-se por ser bastante *user-friendly* e permitir uma rápida adaptação do utilizador às News..
  Foi necessário efectuar várias pequenas alterações no programa. O tin permite um acesso muito aberto ao sistema de ficheiros e à execução de programas externos. Consultar o ponto sobre 'Técnicas gerais de protecção' onde são descritas as alterações efectuadas neste e noutros programas ao nível do acesso ao sistema de ficheiros e à execução de programas externos.
  Várias opções de configuração do programa foram alteradas dos valores por defeito. A

execução do interpretador de comandos e a possibilidade de enviar corpos de artigos para programas externos foram inibidos. Foram inseridas novas directivas de compilação de forma a eliminar as seguintes possibilidades: impressão, suspensão do programa, envio para programa externo e utilização de arquivos '*shar*' - ficheiros arquivados sobre a forma de código de interpretador de comandos.

- **pine** - Este programa é um User Agent de correio electrónico bastante complexo e ao mesmo tempo bastante simples de utilizar. Permite que o utilizador trabalhe com vários 'folders', tem um sistema de ajuda orientado por contexto e além disso fornece ao utilizador uma agenda de endereços. Este programa foi desenvolvido por Mike Seibel, Mark Crispin, Steve Hubert, Sheryl Erez, David Miller e Laurence Lundblade no University of Washington Office of Computing and Communications.
  Baseado originalmente no elm, um outro User Agent, suporta uma grande variedade de protocolos entre eles MIME, IMAP e NNTP. O protocolo IMAP (Interactive Mail Access Protocol é definido em [RFC1176]) foi desenvolvido pela mesma equipa que desenvolveu o pine, tem algumas semelhanças com o protocolo POP3 sendo muito mais avançado que este (consultar [GRA93]). Uma das suas principais funcionalidades é a possibilidade de aceder a múltiplas mailboxes remotas. A interface para o protocolo NNTP permite utilizar o programa como leitor de Usenet News.
  Junto com o pine vem incluido um editor de texto bastante fácil de utilizar, o pico - *pi*ne *co*mposer. Este editor é ligado ao comando executável do pine como biblioteca. Pode ser utilizado externamente como editor de texto ou simplesmente para visualizar ficheiros de texto (edição proibida).
  Foi necessário proteger o acesso sempre que são referidos nomes de ficheiros. Foram feitas alterações suficientes no código fonte de forma a o utilizador ficar limitado a apenas poder referir ficheiros abaixo da sua directoria pessoal. Consultar o ponto sobre 'Técnicas gerais de protecção'.

- **fman** - Permite fazer a gestão dos ficheiros do utilizador. É orientado por ficheiros e directorias permitindo ao utilizador viajar na sua estrutura de directorias seleccionando acções sobre ficheiros ou grupos de ficheiros. Inclui acções como remoção, edição, visualização, compressão, cópia e transferência nos dois sentidos para a máquina do utilizador.
  Após alguma procura por programas de gestão de ficheiros chegou-se à conclusão de que não existiam programas disponíveis de fácil utilização. Assim, aproveitando o facto de o pico possuir um modo de seleccionar ficheiros de uma forma bastante cómoda, foi decidido partir desta pequena secção do pico para um gestor de ficheiros. Retirou-se o visualizador de ficheiros e sobre ele acrescentaram-se os vários comandos necessários ao funcionamento do gestor. De notar que o visualizador já vem equipado com alguns comandos de gestão que foram aproveitados. Na documentação do pacote pine, a equipa de desenvolvimento indica que pretende avançar com o pico de forma a implementar, também um gestor de ficheiros a inserir no pacote.
  Alguns programas de suporte são acessíveis através de acções sobre ficheiros. Estes programas não estão ao inteiro dispôr do utilizador - são executados pelo fman. Entre estes conta-se o gzip, compressor da GNU para comprimir e descomprimir ficheiros segundo um formato próprio, o sz e o rz, destinados a implementar o protocolo ZMODEM para fazer o *upload* e *download* de ficheiros e o pico, utilizado para editar ou visualizar um ficheiro.
  Os problemas de acesso a ficheiros e a comandos foram tomados em consideração desde o início do desenvolvimento do fman.
  Este programa é também utilizado para acesso interactivo ao arquivo de software local na

máquina destinada ao serviço. Esta opção permite o *download* imediato do arquivo local para a máquina do utilizador.

- **gopher** - Através deste programa o utilizador tem acesso ao Internet Gopher. O Gopher é um serviço de entrega de documentos distribuido. Permite ao utilizador aceder a vários tipos de dados distribuidos por vários servidores na Internet de uma forma simples. O utilizador viaja por uma hierarquia de menus e submenus seleccionando opções. O cliente gopher faz um pedido ao servidor que lhe responde com um documento. Esse documento pode ser um ficheiro de texto, uma imagem, um outro menu de opções, etc. Cada documento tem várias características associadas sendo uma delas o servidor onde está disponível.
  A implementação de um cliente do protocolo Gopher utilizada foi a que a Universidade do Minnesota distribui mantida por Paul Lindner. Utiliza a biblioteca de programação *curses*(3x) permitindo deste modo uma fácil inserção do programa na filosofia seguida na implementação do sistema de acesso do PUUG.
  Como o software em questão já vem preparado para executar num modo se segurança, as alterações feitas no código fonte foram mínimas. Como para o restante software ao dispôr do utilizador, foi tomada especial atenção ao acesso a ficheiros e à execução de comandos externos.

- **lynx** - Cliente de sistemas de informação, permite o acesso a servidores de Gopher, HTTP, NNTP, WAIS e FTP. Funciona com uma interface orientada por caracteres em que o utilizador navega num documento de hipertexto seleccionando ponteiros para outros documentos. Tal como os restantes clientes de sistemas de informação existentes na Internet (por exemplo, o Mosaic), o lynx utiliza URL's (Uniform Resource Locator) para denominar documentos.
  O lynx é mantido por Lou Montulli da Universidade do Kansas e encontra-se disponível na Internet.
  Tal como para os restantes programas já descritos, a preocupação a nível de protecções foi dirigida para a execução de comandos e para o acesso a ficheiros.

- **talk** - Permite ao utilizador ligar-se a um outro utilizador num outro sistema ligado à Internet e "conversar" interactivamente através da divisão do ecrán em duas partes, uma para escrita e outra para leitura.
  Optou-se por utilizar o programa distribuido com o sistema operativo do servidor.

- **finger** - É utilizado para interrogar uma máquina acerca dos utilizadores que estão de momento em sessão.
  Tal como para o talk, utilizou-se o programa distribuido com o sistema operativo do servidor.

- **last/quota** - Estes dois programas permitem ao utilizador controlar o tempo de utilização do sistema e o espaço que ocupa no mesmo, respectivamente.
  O programa quota faz parte do sistema de quotas do servidor. O seu output é filtrado de forma a retirar apenas a informação referente à quantidade de espaço ocupado pelo utilizador. O programa last foi seleccionado no código fonte do sistema BSD. Devido ao facto de o comando last original do servidor possuir um output muito complexo e de não apresentar toda a informação desejada para este tipo de serviço, foram efectuadas ligeiras alterações no código. Devido ao facto do programa original apresentar muita informação, o código foi alterado de forma à informação apresentada ao utilizador ser mais atraente e

mais explícita com o objectivo que se pretende: dia, hora início, hora fim e tempo de ligação. No final é indicado o tempo total em que o utilizador esteve ligado ao sistema.

- **passwd -** Destinado a permitir ao utilizador a alteração da sua palavra chave de acesso ao sistema. O comando utilizado é o distribuido com o sistema do servidor. É utilizado de forma segura garantindo que a única acção que o utilizador pode tomar é alterar a sua palavra chave.

- **uqwk -** Empacotador de correio electrónico e de Usenet News. Permite que o utilizador faça o *download* do seu correio electrónico e dos artigos de news que ainda não leu. Desta forma o utilizador não necessita de estar ligado ao servidor enquanto lê o correio e os artigos, diminuindo os seus encargos. Este programa permite, também, que o utilizador envie correio e que faça 'posts' nas news.
  O QWK é o formato mais popular para pacotes de 'offline-reading' que existe no mundo das BBS's. São inúmeros os programas existentes para a leitura offline, tanto para a arquitectura MSDOS/MSWindows como para o Apple Macintosh. O uqwk é uma implementação deste formato de pacote para as plataformas Unix, sendo distribuido em código-fonte. A principal diferença para os empacotadores encontrados em BBS's, é o suporte de uma pequena linguagem de comandos que permite visualizar e editar offline o ficheiro *.newsrc* do utilizador - este ficheiro controla os grupos e artigos que se deseja subscrever/ler. Esta implementação foi desenvolvida por Steve Belczyk.
  O código foi alterado de forma a eliminar da linguagem de edição o comando 'SHELL' que permitiria a execução de um programa no servidor e enviar por correio electrónico o output do mesmo ao utilizador.

- **rz/sz -** Implementação do protocolo ZMODEM. Possibilitam a transferência de ficheiros entre o servidor e a máquina do utilizador. Estes dois programas são utilizados sempre que o utilizador pretende receber ficheiros do servidor ('download') ou pretenda enviar ficheiros para o servidor ('upload'). A transferência de pacotes QWK é feita através destes programas.
  O protocolo ZMODEM e esta implementação para o Unix foram desenvolvidos por Chuck Forsberg.
  O código foi alterado de forma a eliminar um comando definido no protocolo [FOR88]- a execução de um programa no servidor. Consultar 'Técnicas Gerais de Protecção'.

- **gzip/gunzip -** Utilitários que permitem comprimir e descomprimir ficheiros através do algoritmo LZ77. É o formato de compressão standard na distribuição GNU. Permite ao utilizador optimizar o tempo de *download* e de *upload* de ficheiros .
  Não foi necessário alterar o código fonte do programa.

- **zip/unzip -** Utilitário de compressão necessário ao processo de envio e recepção de pacotes QWK. Não foram efectuadas alterações no código fonte.

Técnicas gerais de protecção

Qualquer sistema que seja acessível por vários indivíduos deve estar protegido de forma a garantir a privacidade e a segurança de cada um. O acesso ao sistema por um número, à partida

indeterminado, de utilizadores obriga a uma certa rigidez nas funcionalidades do mesmo a nível de acesso.

Com base nas afirmações anteriores, especial cuidado foi tomado na instalação e configuração dos diversos programas seleccionados para suportar o acesso à Internet. O facto de o software existente na Internet ser distribuído em código-fonte (quase só em linguagem C), permite alterações de forma a possibilitar (ou a não possibilitar) uma acção específica. É possível separar em dois grupos os tipos de alterações efectuadas: acesso a informação (ficheiros) e execução de programas.

De notar que será necessário algo para "envolver" os programas colocados à disposição do utilizador de forma a que tudo o que aqui se discute acerca de alterações de código tenha sentido.

Acesso ao sistema de ficheiros

Voltando à hierarquia escolhida para implementar o sistema de acesso, faz-se a referência mais uma vez à seguinte sub-àrvore da hierarquia:

/public
/individual
/home

fig. 2

Esta subdirectoria foi destinada, à semelhança com certos sistemas Unix, a conter as subdirectorias "home" dos utilizadores do sistema. É numa destas subdirectorias que um utilizador particular tem os seus ficheiros e que pode utilizar da forma que bem entender.

Os diversos programas de acesso ao sistema de ficheiros foram alterados de modo a que o utilizador apenas possa ter conhecimento dos seus ficheiros, nomeadamente ao apenas permitir a escrita de novos ficheiros na sua directoria "home". Foi necessário procurar no código dos programas referências a acesso em escrita ao sistema de ficheiros. Este acesso foi condicionado através da escrita de um novo bloco de código ligado a cada programa particular que valida a localização do ficheiro. Toda e qualquer tentativa de escrita fora da directoria "home" por parte do utilizador devolve um erro de acesso negado.

O acesso em leitura foi condicionado de forma semelhante ao acesso em escrita. O utilizador apenas abre com sucesso um ficheiro para leitura se ele estiver localizado na sua directoria "home".

De referir que certos programas têm de aceder a ficheiros fora da directoria do utilizador. Esse acesso é transparente para o utilizador que não tem controle nenhum sobre o mesmo. Deste modo apenas foi necessário garantir que o acesso não prejudicava a segurança do sistema. Alguns exemplos: ficheiros temporários e acesso ao ficheiro das passwords para tirar informação sobre o utilizador.

Certos ficheiros especiais para o sistema Unix habitualmente existentes nas directorias "home" do utilizador foram protegidos de forma a que o utilizador não lhes possa aceder. Um deles é o ficheiro "*.forward*" (este ficheiro permite execução de programas externos). Outro é o "*.rhosts*" que permite o acesso à conta do utilizador sem necessidade de fornecer uma password ao sistema. A forma encontrada de proteger o seu acesso foi através da garantia de que o utilizador nunca poderá aceder as estes dois ficheiros nos diversos programas.

Execução de programas

Para além dos programas seleccionados para o utilizador aceder à Internet e para gerir a sua conta, garantiu-se que não fosse possível executar mais nenhum programa. O utilizador não pode indicar o nome de um ficheiro para executar, tendo sido efectuadas pequenas mudanças no código de forma a que esta hipótese nunca esteja disponível.

O código fonte de cada programa foi analisado de forma a procurar todas as chamadas ao sistema que permitem lançar programas externos. Destas destaca-se a possibilidade de execução de um interpretador de comandos. Vários programas permitem ao utilizador sair para uma "shell" onde pode executar diversos comandos. Esta opção foi removida sempre que o programa em questão o permitisse.

A chamada ao sistema "*system*(3)" permite a execução de um programa externo. Sempre que surge esta chamada no código, analisou-se o mesmo de forma a garantir que o programa executado é válido. Por vezes um programa necessita de invocar outro de forma a efectuar uma acção mais complexa não inserida no próprio programa. Por exemplo, o programa de leitura/composição de correio electrónico necessita de invocar o programa "*sendmail*(8)" para entregar uma mensagem composta pelo utilizador.

Tendo em vista a necessidade de proteger o sistema contra a execução de programas não desejados dedicou-se especial atenção às chamadas a "*system*(3)". Esta função executa o programa "*/bin/sh*" tendo como parâmetros os mesmos com que é chamada. Nesta situação é necessário tomar em atenção que todos os parâmetros enviados a "*system*(3)" serão processados pelo interpretador de comandos. Neste caso particular apresenta-se o exemplo que consiste em utilizar um parâmetro inserido entre pelicas ("`"). Ao encontrar esta situação, "*/bin/sh*" substitui o texto entre os caracteres indicados pelo resultado obtido através da execução do texto. Uma solução utilizada passa pela utilização das chamadas ao sistema "*fork*(2)" seguida de "*execl*(3)". Garante-se desta forma que os parâmetros não serão interpretados. Uma solução mais simples seria garantir que os parâmetros enviados ao sistema não comprometem a segurança dos sistema através da, por exemplo, escrita de código de pesquisa de parâmetros.

"*fork*(2)" gera um novo processo no sistema idêntico ao processo que a chama, permitindo que um processo lance outro paralelo a si. Habitualmente um programa executa esta chamada ao sistema e o segundo processo executa um novo programa. A chamada ao sistema que permite a um programa transformar-se num outro é a função "*execl*(3)". O código foi analisado e modificado com o objectivo de que esta função não lance programas inválidos.

4.1.2.2 fesh - Front End SHell

O fesh é um programa desenvolvido de raíz para assistir o utilizador no acesso ao sistema. Está para o utilizador tal qual "*/bin/sh*" (ou outra shell qualquer) está para o utilizador de um sistema Unix. Foi implementado de forma a proteger o sistema contra acessos indevidos e a possibilitar ao utilizador o acesso aos programas instalados através de uma interface simples e eficiente.

Shell

O fesh foi construido como sendo a shell do utilizador no sistema Unix. Desta forma torna-se o sistema mais seguro, evita a execução de "*/bin/sh*" e é mais eficiente uma vez que esta shell é mais simples e é dedicada apenas a uma função. Na base da construção deste programa

foi analisado o funcionamento da shell original. Certas funções de "*/bin/sh*" consideradas importantes foram mantidas e outras foram alteradas ou modificadas. Como exemplo, cita-se a utilização de um ficheiro MOTD (message of the day) dedicado apenas ao sistema e, como exemplo de acções eliminadas cita-se a remoção da inicialização de algumas variavéis de ambiente como PATH, SHELL e EDITOR.

Este programa foi desenvolvido utilizando a linguagem de programação C. Devido à complexidade que envolve um programa de tal envergadura, foi analisado o código fonte de várias shells existentes. O destaque vai para o código do programa bash - Bourne Again SHell da GNU. Os aspectos que mereceram mais atenção foram a inicialização do programa, o tratamento de sinais e a execução de programas externos.

Uma shell ao iniciar executa certas acções. Mostra ao utilizador o ficheiro */etc/motd*, inicializa variáveis de ambiente e faz o "*chdir*(2)" para a directoria home do utilizador, entre outras acções. Após a inicialização, a shell entra num ciclo em que aceita comandos do utilizador numa linha de comando. No fesh a inicialização é semelhante. O ficheiro mostrado ao utilizador é */public/individual/etc/motd*, onde é colocada informação que pode ser actualizada diariamente). Ao contrário duma shell normal, as variáveis de ambiente são destruidas de forma a evitar a possibilidade que alguns programas que alteram o seu comportamento dependendo deste valor, quebrem a segurança do sistema. Como exemplo cita-se as variáveis que podem referir um comando externo. No entanto as situações em que os programas instalados pesquisam os valores deste tipo de variáveis foi tratado de forma devida. O risco existe em programas em que foi instalado o binário distribuido com o sistema. O fesh também faz o "*chdir*(2)" para a directoria "home" do utilizador: */public/individual/home/*<username>. De seguida também entra em ciclo a processar os comandos do utilizador com a diferença que apresenta um menu de opções ao contrário de uma linha de comando (ver fig. 4).

Uma shell está preparada para tomar certas acções dependendo do tipo de sinal que recebe. Por exemplo, SIGINT nas shells tradicionais costuma estar associado com a limpeza da linha de comando introduzida. No fesh os sinais são processados de uma forma coerente.

- SIGINT (gerado quando o utilizador carrega em Ctrl+C) provoca que seja pedido ao utilizador que confirme que pretende abandonar o programa;

- SIGQUIT (pode ser gerado através de Ctrl+\) abandona automaticamente o sistema.

Outros sinais também tiveram tratamento especial:

- SIGHUP é gerado quando a linha "caí" e o modem corta a conexão - nesta situação o programa procura terminar de uma forma limpa libertando possíveis recursos que esteja a ocupar;

- SIGWNCH é gerado quando uma janela muda de tamanho, por exemplo num ambiente gráfico com a shell a correr num *xterm* - embora o programa esteja preparado para tratar este sinal ele não tem nenhum efeito. Em futuras versões provavelmente virá a ter uma acção importante caso a interface se torne mais complexa.

Os sinais devem ser convenientemente tratados quando o sistema lança um programa externo.

O fesh destina-se a lançar os programas preparados para o utilizador. Este lançamento é feito de modo a que quando o programa termine o fesh retome o controle da sessão. No início é feito um "*fork*(2)". O processo pai é o fesh original. Este processo passa a ignorar todos os sinais descritos atrás e espera que o processo obtido a partir do "*fork*(2)" termine. Esta espera é realizada através da chamada ao sistema "*wait*(2)".

O processo filho refere-se ao programa a executar. São preparados os parâmetros do programa que serão passados à chamada ao sistema "*execl*(3)". Após a execução desta chamada o processo é substituido pelo programa e fica com o controle da sessão uma vez que o processo pai está parado à espera que ele termine.

Interface

Este programa foi construído tendo como base uma árvore de submenus. Geralmente cada selecção do menu está associada à execução de um dos programas instalados para o sistema.

No desenho da interface procurou-se atingir dois objectivos:

- simplicidade. Torna o desenvolvimento e a manutenção do código mais rápida e fácil. O utilizador habitua-se rapidamente ao ambiente.

- eficiência. Uma selecção de um menu é atingida através de uma tecla.

As figuras 3 e 4 mostram o ecrân inicial que inclui o *motd* e o menu principal, respectivamente.

```
===     ____                                ===       EUnet Portugal
===    /      /    /    ___     ___   _/_ ===       PUUG - c/o UNINOVA
===   /----   /    /   /    /   /___/   /   ===       Quinta da Torre
=== /____   /___/   /    /   /___     /     ===       2825 Monte da Caparica
=====                                 =====       PORTUGAL
===== Connecting Europe since 1982 =====       Fax: + 351 (1) 295 77 86

EUnet connectivity is provided in Portugal by PUUG
fesh 1.1.7.94.08.18
Copyright 1994 PUUG - Portuguese Unix Users Group

Welcome to EUnet LOGIN

        Telefones de acesso ao servico:
                LISBOA: (01) 315 0985/6/7, (01) 521 305, (01) 316 0560/72
                PORTO:  (02) 600 2287 (3 linhas)

        NNA X.25: 0942104202

        Bugs e comentarios para: Carlos.Canau@puug.pt

Press a key...
```

fig. 3

```
EUnet LOGIN
                                                canau@individual.puug.pt

H - Online MANUAL               Big Dummy's Guide to the Internet
F - Remote FILE TRANSFER        Transfers files from remote sites
T - Remote LOGIN                Open a session in another site
S - ARCHIE Search               Ask Archie about whereabouts of information
N - Usenet NEWS                 Read news from Usenet Bulletin Board
M - MAIL                        Read/Send mail
Z - File MANAGER                Copy, Delete, Download, ...
A - Local File ARCHIVE          Copy files from local archive
G - GOPHER                      Gopher InfoService
W - WWW                         World Wide Web Entry Point
K - TALK                        Talk to someone
I - FINGER                      Finger someone or some machine
L - ACCOUNT                     Reports your logins and disk usage
O - OFFLINE                     Offline reading and writing
C - CONFIGURATION               Change password, signature, ...
Q - LOGOUT                      Exit EUnet Login system

Option ? >
```

fig. 4

Protecções

As técnicas descritas em 'Técnicas Gerais de Protecção' foram levadas em consideração durante a implementação do fesh. Uma vez que este programa foi construido de raiz, a sua protecção e desenho foram estudadas em detalhe ao longo do seu desenvolvimento.

Como foi referido em 'Shell', o programa está preparado para aguentar várias situações estranhas ao funcionamento normal que possam ocorrer, como por exemplo, queda da linha, interrupção pelo utilizador, etc.

4.1.2.3 **gopherd** - servidor de documentos para clientes gopher

Juntamente com a instalação de um cliente gopher, foi instalado um servidor local gopherd. Esta opção surgiu de forma a possibilitar que o utilizador possua um menu de arranque para outros servidores remotos.

O servidor foi configurado para apenas permitir o acesso a clientes locais. O menu inicial que oferece ao utilizador permite que este tenha um ponto de partida para vários outros gophers e ainda permite o acesso por FTP ao arquivo do PUUG. Como é habitual nos menus principais destes servidores, foi incluida uma página com informação sobre a instituição que gere o servidor.

```
                Internet Gopher Information Client 2.0 pl11

                   Root gopher server: individual.puug.pt

 -->  1.  About PUUG...
      2.  PUUG's FTP archive server/
      3.  FCT-UNL Gopher/
      4.  Mother of all gophers (University of Minnesota)/
      5.  European root gopher/
      6.  Wiretap (electronic books)/



Press ? for Help, q to Quit                                  Page: 1/1
```

fig. 5

4.1.2.4 **WWW** - Página de arranque.

O programa lynx permite o acesso a servidores httpd, que põem ao dispôr dos clientes documentos de hipertexto escritos na linguagem HTML (HyperText Markup Language). Quando o lynx é inicializado necessita que lhe seja fornecido um URL ao qual se possa ligar. Para o efeito foi escrito um documento em HTML de forma a fornecer ao utilizador uma página inicial com um certo número de 'links' para outros servidores remotos. Tal como para o servidor de gopher, inclui-se nesta página um ponteiro para informação sobre o PUUG.

```
                                                        World Wide Web

                              ORGANIZATION:
_____________________________________________________________________

                                 P.U.U.G.

                          PORTUGUESE UNIX USERS GROUP
_____________________________________________________________________

                              DOMAIN: PUUG.PT


                          WORLD WIDE WEB ENTRY POINT



-------------------------------------------------------
If you need help, mail to: admin@puug.pt
-------------------------------------------------------

Link to:

   * Portuguese National DNS Archive Service
   * Faculdade de Ciencias e Tecnologia da Univ. Nova de Lisboa
   * Faculdade de Ciencias da Univ. de Lisboa
   * Gateway X.500 no INESC
   * ARCHIE.INESC.PT File archive
   * EUnet Network Information Services
   * O'Reilley's Global Network Navigator _@_
   * CERN - Index of World Wide Web Servers
   * World Wide Web - World Home Page
```

fig. 6

4.1.3 Serviço individual IP

Acesso SLIP

O protocolo SLIP, Serial Line Internet Protocol, foi o primeiro protocolo a ser desenvolvido com o objectivo de implementar o protocolo IP sobre linhas série. Está definido em [RFC1055].

Este protocolo torna possível a comunicação através do protocolo TCP/IP sobre linhas comutadas. Devido ao facto de apenas necessitar de um modem ligado à rede telefónica, a utilização deste protocolo para fornecer conexão directa à Internet torna-se bastante barata.

Van-Jacobson ([RFC1144]) desenvolveu um método que permite eliminar alguma da informação constante no header de cada pacote TCP/IP encapsulado segundo o método SLIP. A variante do protocolo que utiliza este tipo de compressão chama-se CSLIP, isto é, "Compressed SLIP".

Acesso PPP

O PPP, Point-to-Point Protocol é um standard criado pela IETF, Internet Engineering Task Force, com o objectivo de possiblitar a implementação do nível *data link* sobre linhas série. A sua definição como standard pode ser obtida em [RFC1171], [RFC1172] e [RFC1331]. É muito mais complexo que o protocolo SLIP (este último não é um standard).

Após o estabelecimento de uma conexão PPP são negociados vários parâmetros. De destacar a negociação do endereço IP entre ambos os parceiros. Este pormenor é de particular importância para o serviço.

Portmaster e SLIP/PPP

O terminal server Portmaster da Livingston tem a possibilidade de comunicar em SLIP ou PPP nas portas série, por isso foi seleccionado para suportar as ligações por linha comutada dos aderentes a ambos os serviços.

Embora o terminal server possa fazer routing de pacotes IP através do protocolo RIP, tal não é necessário para este serviço. Os endereços IP atribuidos às portas série pertencem à mesma rede que o terminal server. O encaminhamento de pacotes para as portas série é feito através do protocolo ARP - o Portmaster responde a todos os pedidos ARP para os endereços que tem activos no momento.

A configuração por defeito do Portmaster foi feita de forma a que uma ligação seja tratada como uma sessão de login no servidor, i.e. por defeito o Portmaster actua como um terminal server vulgar. Para um utilizador ter a possibilidade de estabelecer uma ligação SLIP ou PPP com o Portmaster é necessário que o mesmo possua uma entrada na tabela de utilizadores do mesmo. Esta tabela define o perfil de cada utilizador reconhecido pelo terminal server, parâmetro em particular que permite defini-lo como utilizador de rede, i.e., possui uma conexão IP. Um outro parâmetro permite definir o protocolo utilizado pelo software do utilizador.

IP fixo vs. IP variável

A definição de um utilizador rede no Portmaster inclui, como seria de esperar, o endereço IP do mesmo. Tomando a opção de atribuir um endereço IP a cada aderente ao serviço surgiria um problema importante quando se atingisse um número de aderentes superior a 250 - uma rede classe C está limitada a 254 endereços. O Portmaster está numa destas redes que partilha com o servidor e mais algumas máquinas. A solução para o problema surge através de um valor especial que se pode atribuir ao campo que representa o endereço IP do utilizador. Este valor - "assigned", define um endereço IP de início que é atribuido à primeira ligação que um utilizador rede efectue. À próxima ligação rede será atribuido o valor imediatamente a seguir. Assim sucessivamente até se esgotar o número de portas definidas para suportar ligações rede. Nesta altura o valor volta ao início.

Seguindo o processo indicado acima, é definido um intervalo de endereços IP que são colocados no DNS do PUUG de forma a que as ligações rede dos aderentes possam ter *reverse-mapping*. Este factor é utilizado por vários tipos de servidores na Internet para aceitar conexões de um endereço específico, em particular a implementação mais vulgar do servidor de FTP anónimo, o *wu-ftpd*. A informação colocada no DNS em RR's A tem a seguinte forma:

```
dial205         IN      A       192.84.62.5
dial206         IN      A       192.84.62.6
dial207         IN      A       192.84.62.7
   .                                    .
   .                                    .
```

fig. 7

O nome escolhido é construido a partir do nome do terminal server, dial2. Permite a um potencial interessado deduzir facilmente que se trata de um host que tem uma ligação temporária.

Obtenção do endereço IP

Após estabelecer a ligação por linha comutada, o utilizador necessita de fornecer o seu nome de login e a sua password. Quando o Portmaster aceita um login de um utilizador rede, envia-lhe como resposta em ASCII o endereço que lhe está atribuido. O utilizador fica perante duas situações distintas. Se utiliza o protocolo PPP tem de configurar o seu software de forma a que o mesmo aceite o IP que o Portmaster lhe atribui. O protocolo PPP permite que o IP seja negociado. No caso em que o protocolo utilizado é o SLIP, a situação torna-se mais delicada, uma vez que este protocolo não permite negociações de parâmetros. Assim, o utilizador tem de obter a string com o endereço que o Portmaster lhe envia e configurar o seu software com este valor. Isto pode ser automatizado em algum software.

Software de apoio

Existe disponível na Internet uma grande variedade de software para computadores pessoais que permite estabelecer uma conexão IP por linha série.

A solução sugerida a utilizadores que adiram ao serviço pretendendo estabelecer a ligação utilizando um Apple Macintosh é que adquiram extensões TCP/IP para o sistema - MacTCP. O

MacPPP é uma aplicação que permite utilizar o protocolo PPP com o MacTCP. Esta aplicação está disponível na Internet. Também disponíveis estão clientes para vários protocolos: FTP, Telnet, Gopher, Archie e WWW entre outros.

Para a linha de computadores pessoais compatíveis IBM/PC, o software sugerido é o Trumpet Winsock. Esta aplicação shareware permite a utilização do protocolo SLIP. Como vantagens cita-se dois factores bastantes importantes. É uma aplicação para MS Windows, a interface gráfica mais vulgar neste tipo de hardware. A sua linguagem simples de estabelecimento de conexão, semelhante ao *chat script* do UUCP, permite o *parsing* do endereço IP enviado pelo Portmaster.

Por cima desta aplicação o utilizador tem a possibilidade de correr qualquer software compatível com a biblioteca WINSOCK.DLL. Na Internet existem clientes shareware ou public domain para os diversos protocolos de acesso.

Uma segunda opção é a utilização de um *packet driver* compatível com a norma criada pela FTP Inc. para tornar o software independente das diversas placas de rede. Existem várias versões de packet drivers que implementam SLIP ou PPP. Nesta opção é necessário que o software seja compatível com a norma citada (por exemplo, o NCSA Telnet utiliza esta norma). Com este método é possível colocar o Trumpet Winsock sobre PPP, uma vez que o mesmo também é compatível com a norma.

Sempre que o aderente não tem a possibilidade ou o conhecimento necessário para obter o software, o PUUG encarrega-se de lho fornecer. Este software é sempre seleccionado prioritariamente entre o software existente na Internet uma vez que o mesmo é public domain ou shareware. Este princípio destina-se a tornar os encargos do utilizador mais baixos. No entanto também é reconhecida a qualidade do mesmo freeware/shareware chegando certos programas a serem superiores a produtos comerciais semelhantes.

Servidor POP

A utilização das diferentes aplicações de acesso ao Internet não colocam problemas de maior ao utilizador. No entanto, existe uma que pelas suas características necessita de ser tratada de forma especial, o e-mail. Na Internet, em geral, sempre que se pretende entregar uma mensagem de correio electrónico contacta-se com um servidor que recebe a mensagem e a coloca na caixa de correio do receptor. Este tipo de acesso não permite que o utilizador possua uma caixa do correio no seu computador devido ao facto de efectuar ligações esporádicas. Logo é necessário que exista algo a receber o seu correio e a guardá-lo. Este tipo de problema foi resolvido através da utilização de um servidor de POPmail. Um servidor deste tipo destina-se a permitir que um utilizador remoto aceda a uma caixa de correio (*mailbox*) situada na máquina servidora de e-mail.

Paralelamente ao desenvolvimento do pine, a equipa responsável também desenvolve servidores dos protocolos POP (Post-Office Protocol) e IMAP, estando as sources disponíveis na Internet. O pacote em questão inclui três servidores, ipop2d, ipop3d e imapd para os protocolos POP2, POP3 e IMAP, respectivamente. O protocolo POP é descrito em detalhe em [RFC1460]. [GRA93] contém uma comparação das vantagens e das desvantagens dos dois protocolos.

Para permitir que os aderentes ao serviço SLIP/PPP possam receber correio electrónico, instalou-se na máquina de suporte ao serviço o servidor ipop3d.

Acesso à POP mailbox

A validação do acesso a uma mailbox por um POP server é feita do mesmo modo que o programa login. O utilizador tem de existir no sistema - tem de possuir uma entrada no ficheiro das passwords. Para ter a possibilidade de ler a sua mailbox necessita de fornecer a password da área em questão.

O acesso pode ser feito através de um qualquer cliente POP. Nesta situação particular o cliente escolhido foi o PCEudora, cliente de POPmail vulgar no Macintosh transposto para a plataforma IBM/PC.

O envio de mensagens pode ser feito por um cliente POP através de uma ligaçaão ao servidor POP ou através de um programa que implemente o envio de mensagens através do protocolo SMTP. Uma vez que o utilizador tem uma ligação IP ao servidor, pode utilizar qualquer um destes dois protocolos.

4.1.4 Gestão de utilizadores

A partir de um certo número de utilizadores, a gestão destes torna-se extremamente difícil. Devido a este facto assim que se iniciou a implementação do sistema foi decidido automatizar a gestão de utilizadores. Esta gestão deveria ser responsável pela manutenção de informação acerca do utilizador, criação e remoção de contas.

Tendo como inspiração o sistema de gestão da rede do PUUG desenvolvido por Jorge Frazão em 1992 [OLI92], foi construído um sistema com uma sintaxe semelhante. Visto que apenas é necessário garantir o acesso aos dados do utilizador e adicionar e remover utilizadores com base nessa informação, simplificou-se o sistema de forma a ser constituido por:

- ficheiro de texto simples, com uma sintaxe própria;
- comando de adição de utilizador, orientado segundo a informação do ficheiro acima - addindividual;
- comando de remoção do utilizador - removeindividual.

Ficheiro de dados

A semelhança da sintaxe introduzida por [OLI92], foi implementada a seguinte sintaxe para o ficheiro de dados sobre um utilizador:

```
# linhas iniciadas por # sao ignoradas
customer        individual
#       individual | slip | ppp
loginname       demo
#       username no sistema (/etc/passwd)
mailname        Demo
#       ficheiro generics
puug-hdl        1984
#       UID no /etc/passwd
country         pt
organization    PUUG
person          Demo Account
#       Nome completo no /etc/passwd (gecos)
email           demo@individual.puug.pt
telephone       +351 1 294 2844
fax             +351 1 295 7786
address         PUUG - Grupo Portugues de Utilizadores de Sistemas UNIX
address         c/o UNINOVA, Quinta da Torre
address         2825 MONTE DA CAPARICA
address         PORTUGAL
introduced      Carlos.Canau@puug.pt  940126
```

fig. 8

Comando addindividual

Este comando foi desenvolvido a partir do script adduser distribuido com o sistema operativo original. Apenas tem um parâmetro, o nome do utilizador no sistema.

Com base em vários campos no ficheiro de dados do utilizador é criada uma conta no servidor. São feitos vários testes de forma a evitar situações de erro, nomeadamente, falta de ficheiros, erros de sintaxe no ficheiro de dados, novo UID válido.

A conta é criada através da inserção de uma entrada para o utilizador no ficheiro de passwords do sistema. É criada uma directoria "home" para o utilizador, sendo nela instalados os ficheiros de configuração do utilizador. O comando permite que a password da nova conta seja inserida durante a sua criação.

É necessário configurar o sistema de correiro electrónico para contêr um "alias" para a mailbox do utilizador. Em geral, este alias, é construido com duas palavras separadas por um ponto que podem representar o primeiro e o último nome do utilizador, por exemplo: "Carlos.Canau". Isto é implementado através de um programa escrito para o efeito em Perl. Este programa verifica se o alias do utilizador já existe no ficheiro de aliases do sistema, inserindo-o em caso negativo.

O endereço de correio electrónico do utilizador deverá ser visto do exterior como sendo o alias. Ou seja, o campo que indica o remetente no envelope das mensagens enviadas pelo utilizador deverá identificar o utilizador pelo alias (consultar [RFC822] e [IDA]). O programa que actualiza os aliases é também responsável por mais esta configuração. Consulta o ficheiro de dados de forma a inserir a informação sobre o utilizador.

O sistema de correio electrónico é actualizado com base nos novos dados inseridos pelo programa.

Comando removeindividual

À semelhança do comando anterior, este comando apenas tem como parâmetro o nome do utilizador a remover. Também foi desenvolvido tendo como base um script do sistema operativo, o removeuser.

Efectua vários testes de validação antes de proceder à remoção do utilizador pedindo a confirmação das diversas acções que toma: a eliminação da entrada referente ao utilizador no ficheiro das passwords, a remoção da directoria home e da sua mailbox.

Foi escrito um script em Perl para remover a informação sobre o utilizador na configuração do sub-sistema de correio electrónico. Este script é semelhante ao escrito para o comando addindividual procedendo de forma inversa.

O comando não remove o ficheiro de dados sobre o utilizador. É deixado à consideração do administrador o que fazer com o mesmo (por exemplo, arquivá-lo).

Mailing-list individuals

Os dois comandos referidos gerem uma mailing-list que inclui o endereço de correio electrónico de cada utilizador. O comando addindividual acrescenta o endereço do utilizador e o comando removeindividual elimina-o.

Esta lista destina-se a que os administradores do sistema tenham a possibilidade de enviar uma mensagem a todos os utilizadores simultaneamente. Como exemplo cita-se as situações de problemas com o sistema em que é necessário avisar os utilizadores que o mesmo estará inacessível durante um período de tempo específico.

Nesta lista incluem-se também os utilizadores do serviço SLIP/PPP.

Gestão de utilizadores SLIP/PPP

Um utilizador SLIP/PPP não necessita de possuir espaço em disco numa máquina do PUUG uma vez que o seu computador fica ligado directamente à Internet, necessitando apenas que o terminal server a que se liga o reconheça. Ou seja, é necessário que o utilizador possua uma entrada na tabela de passwords do terminal server.

Uma ligação deste tipo necessita que o utilizador possua uma mailbox em algum local que não a sua máquina. O utilizador não possui endereço fixo na Internet e faz ligações esporádicas. De modo a resolver este problema, foi instalado um servidor POP na máquina destinada a suportar o serviço de individuais.

A gestão de contas deste serviço é feita de um modo semelhante às contas do serviço Login. Uma vez que foi instalado e preparado após a entrada em funcionamento do serviço Login, a gestão foi implementada através do upgrade da gestão já existente de forma a suportar os dois serviços.

Nova sintaxe do ficheiro de dados

O campo customer passa a aceitar dois novos valores além de individual. O valor 'slip' define um utilizador que acede ao serviço através do protocolo SLIP e o valor 'ppp' corresponde ao protocolo PPP.

Com base neste campo, os novos scripts addindividual e removeindividual decidem as acções a tomar.

Novo comando addindividual

Quando o tipo de utilizador é slip ou ppp, o comando altera o seu comportamento do seguinte modo. O utilizador slip/ppp necessita de possuir uma entrada no ficheiro das passwords de forma a ter a possibilidade de aceder à sua mailbox. No entanto não deve conseguir efectuar um login na máquina. Assim o valor que representa a sua shell no ficheiro de passwords fica com um valor inválido. Uma vez que o utilizador não faz login na máquina, não se cria uma directoria home para o mesmo.

A configuração do sistema de correio electrónico mantém-se idêntica, o utilizador tem um alias para sua mailbox e o correio electrónico enviado pelo utilizador tem o endereço alterado.

O comando passa a pedir duas passwords para a nova conta em vez de uma. A primeira password destina-se a validar o acesso ao terminal server. A segunda password destina-se ao ficheiro das passwords do servidor de suporte de modo a permitir que o utilizador tenha permissão de aceder à sua mailbox.

Uma entrada para o novo utilizador é criada no terminal server remotamente. O software distribuido com o Portmaster inclui um comando que permite a configuração remota do mesmo.

Novo comando removeindividual

Este comando foi estendido de modo a remover a entrada do utilizador no terminal server. Não há a necessidade de remover a directoria home uma vez que esta não existe, no entanto, é necessário remover o utilizador do ficheiro /etc/passwd e remover a sua mailbox.

4.1.5 Accounting

Uma vez que o acesso dos utilizadores é contabilizado, o sistema tem de estar preparado para registar a utilização dos seus recursos. O sistema de acesso à Internet para individuais é contabilizado pelo PUUG considerando o tempo que o utilizador esteve ligado durante o mês.

Serviço Login

Devido ao facto deste serviço estar implementado num sistema operativo Unix, o sistema de accounting é baseado na informação de acessos ao sistema fornecida pelo próprio sistema de registo de logins do Unix (programas login e last, ficheiro */etc/utmp*).

O ficheiro */etc/utmp* regista tempos. Sempre que um utilizador entra ou sai do sistema, é registado neste ficheiro a data e hora em que tal ocorre. Sendo esta informação utilizada pelo programa last, foi desenvolvido um programa na linguagem *awk*(1) de modo a processar o seu output. Este programa soma os logins e os tempos totais de cada utilizador.

A informação de accounting necessita de ser arquivada de forma a ser possível apresentar relatórios da utilização do sistema. Esta necessidade é reforçada pelo facto de ser com base nesta informação que se cobra o acesso ao serviço.

No último dia de cada mês o ficheiro */etc/utmp* é arquivado. De seguida é inicializado para o novo mês. O ficheiro arquivado é processado através do programa referido atrás e esta informação é enviada para contabilidade do serviço. O ficheiro é arquivado de forma a estar presente em caso de futura necessidade.

É de referir dois pormenores acerca deste accounting. O primeiro é que os ficheiros de registo de logins são de importância vital para o funcionamento do sistema. Assim, além de arquivados estão protegidos segundo um esquema de backup incremental implementado em todos os sistemas do PUUG. O segundo é que foi necessário instalar no sistema operativo um novo comando que permita a leitura de diferentes ficheiros de registo. O comando last distribuido com o sistema operativo apenas permite o processamento do ficheiro */etc/utmp*, i.e., não é possível indicar um ficheiro alternativo a processar. O comando instalado foi obtido na distribuição de software BSD. Este novo comando, instalado com o nome *bsdlast* com o objectivo de o distinguir do original, permite a passagem como parâmetro do nome do ficheiro a processar.

Serviço Individual IP

Uma vez que o login efectuado pelo utilizador se situa no Portmaster e não no sistema Unix, é necessário possuir um tipo diferente de accounting para este serviço. O sistema operativo do Portmaster está preparado para fazer registo de informação numa máquina remota. Esta informação é registada através da comunicação com o servidor syslogd na máquina remota.

O "*syslogd*(8)" é o servidor responsável por registar em ficheiro a actividade do sistema operativo. Entre a informação registada referem-se como exemplos problemas com o sistema operativo, informação acerca das mensagens enviadas ou recebidas pelo sistema de correio electrónico e registo de actividade do DNS.

Após estar definida uma máquina como sendo o host que aceita o registo de actividade, o Portmaster envia registos para o syslogd desta máquina. Este está configurado de forma a enviar toda a informação vinda do Portmaster para o ficheiro */var/log/Portmaster*.

O ficheiro de registo de actividade do Portmaster é tratado da mesma forma que o ficheiro

utmp para o serviço de Login, nomeadamente a nível de arquivo mensal e de protecção por backup.

O Portmaster regista vários tipos de informação. Para esta situação particular apenas interessa a informação registada pelos logins e pelos logouts dos utilizadores rede (SLIP ou PPP). Este tipo de registo tem uma sintaxe própria para cada tipo de ligação. De forma a facilitar o accounting de tempos de utilização, foi desenvolvida uma aplicação de accounting, descrita em detalhe em 'dial-account - contabilização do acesso DIALUP'. O seu resultado é uma lista que descreve para cada utilizador o número de ligações que efectuou no mês, bem como o tempo total de ligação.

4.1.6 Backup do sistema

Um sistema como este em que os utilizadores contam que esteja sempre à sua disposição, necessita de estar protegido de uma forma eficiente e segura. É necessário garantir que seja possível garantir a recuperação do sistema no menor período de tempo possível em caso de acidentes graves (como uma falha de disco, por exemplo).

O sistema está protegido contra perdas de dados motivadas por falhas de hardware ou de software através de uma política de backup. É garantida a existência de backups diários até dois dias. Ou seja existem sempre três versões do sistema, duas de segurança e a cópia actual. No fim de cada mês é feito um backup integral de todo o sistema operativo. São guardadas duas cópias deste backup integral. Uma para cada um dos dois meses anteriores.

O backup é guardado em hardware separado daquele onde o sistema reside.

4.1.7 Apoio aos utilizadores do serviço

Embora o serviço de individuais do PUUG tenha sido planeado de modo a tornar a sua utilização o mais cómoda e fácil possível, é sempre necessário apoiar os utilizadores nas mais diversas situações. Um bom serviço de apoio ajuda imenso a aumentar a qualidade do serviço. Uma vez que não foi feita publicidade ao serviço, investiu-se bastante neste aspecto.

São várias as situações em que o utilizador necessita de apoio. Falta de experiência com o computador e com o sistema operativo que está a utilizar, falta de informação acerca da Internet e como utilizar os programas de acesso, problemas técnicos na instalação e utilização de software, etc.

Para além do apoio técnico, é fornecido ao utilizador uma cópia do livro "Big Dummy's Guide to the Internet" e software para acesso ao serviço caso necessite.

Apoio técnico

O apoio técnico a este serviço é feito através de telefone. Os aderentes ao serviço têm a possibilidade de entrar em contacto com o PUUG de forma a resolver as diversas questões que tenham acerca do acesso ou utilização. Este serviço está à disposição dos aderentes durante as horas de expediente e não é cobrada a sua utilização.

Documentação

O livro referido está disponível na Internet e foi escrito por Adam Gaffin. É uma excelente introdução ao que é a Internet, como aceder e ensina como utilizar alguns dos programas que lhe permitem aceder como o telnet, o ftp, clientes de www, etc. No serviço Login este livro foi colocado à disposição do utilizador para consulta no formato HTML.

Um outro livro na mesma linha do 'Big Dummy's Guide to the Internet' é o 'Zen and the Art of the Internet' escrito por Brendan P. Kehoe também disponível na Internet.

Software

O software mínimo necessário para utilizar o serviço Login é um programa de comunicações para IBM/PC ou para Macintosh (ou para outra plataforma qualquer) que possua emulação de terminal vt100 e que permita o *upload* e *download* de ficheiros através do protocolo ZMODEM. Sempre que o utilizador não possua este tipo de software, é-lhe enviado um ou mais programas que lhe permitam aceder ao serviço. De referir que na Internet estão disponíveis inúmeros programas public domain ou shareware nas condições referidas.

Para aceder ao serviço SLIP/PPP existem várias soluções possíveis. Algumas delas são referidas em 'Serviço individual IP'. Foi preparada uma solução específica para a plataforma mais vulgar; MS Windows 3.1. Este ambiente gráfico possue uma interface de janelas, é '*user-friendly*' dentro do possível e permite a execução simultânea de várias aplicações.

Foi preparada uma diskette contendo o software referido atrás para acesso ao Internet através do MS Windows 3.1. Nesta diskette foi incluido um script de instalação. Este pequeno programa coloca o software na máquina do aderente e prepara todos os ficheiros de inicialização do mesmo duma forma automática. Esta automatização é obtida através da definição de certas variáveis específicas sobre o utilizador como o nome de login e o nome completo, num ficheiro de configuração personalizado.

Na diskette existe um ficheiro com instruções de instalação e com alguma informação sobre os programas incluidos. O software é constituido pelo Trumpet Winsock e vários programas que correm sobre a biblioteca Winsock: QVTNET (telnet, ftp, mail e news), WSARCHIE (cliente archie), MOSAIC (cliente www e gopher), PCEUDORA (cliente POPmail) e WINVN (cliente NNTP - leitor de news). Este software é public domain ou shareware. Na segunda hipótese é indicado, na documentação incluída, que o utilizador deverá registar este software.

Com este software o utilizador tem as portas abertas para a Internet. Na documentação são sugeridos locais (arquivos de ftp anónimo) onde é possível obter outros clientes para acesso que corram sobre Winsock (por exemplo, clientes de IRC, finger, talk, etc.).

4.2 Conectividade Internet por DIALUP

Com o surgimento de protocolos como o SLIP e o PPP que tornam possível a utilização do protocolo IP sobre linhas série, a ligação à Internet por DIALUP é uma opção de baixos custos. Aproveitando este facto, o PUUG decidiu passar a fornecer este novo tipo de ligação aos seus aderentes. Anteriormente apenas era possível que o aderente acedesse à Internet através de X.25. Embora mais potente a nível de protocolo e a nível de fiabilidade de conexão, este tipo de ligação é bastante cara quando comparada com uma ligação por linha comutada.

Tal como os serviços já fornecidos pelo PUUG, também este permite definir um domínio DNS abaixo de pt. para o aderente gerido pelo PUUG. Além deste serviço, o PUUG assegura as ligações de correio electrónico e das Usenet News para a instituição aderente.

Para estabelecer este serviço foi necessário seleccionar equipamento específico de suporte. O sistema de gestão da administração de ligações dos aderentes à rede do PUUG foi modificado de modo a suportar esta nova modalidade de acesso. De seguida descrevem-se estes procedimentos bem como diversos problemas que surgiram e as soluções adoptadas para os resolver.

4.2.1 Equipamento de suporte

O equipamento de suporte escolhido para este serviço é constituido por um conjunto de modems, um terminal server e um servidor de suporte aos diversos protocolos de ligação postos ao dispôr do aderente.

Tal como para o serviço de individuais procurou-se uma marca de modems que oferecesse garantias de excelente qualidade de serviço. Os modems escolhidos foram ZyXEL U-1496plus pelas mesmas razões apontadas atrás: testes no PUUG e relatórios bastante favoráveis das outras EUnets.

O terminal server escolhido para providenciar os protocolos SLIP e PPP através de linhas série foi o Portmaster 2e da Livingston. Esta máquina distingue-se da escolhida para o serviço de individuais no número máximo de portas série, trinta nesta contra dez na máquina anterior. A opção por esta marca de terminal server foi motivada por vários factores. O principal é a possibilidade de utilizar as portas série para efectuar todos os tipos de ligações: login, uucp e conexões IP sobre linha série.

O host de apoio ao serviço, relay.puug.pt, é o backbone do PUUG para ligação à Internet. Esta máquina, uma Sun SPARCClassic a correr o sistema operativo SunOS 4.1.3C, é usada como servidor dos protocolos DNS, SMTP e NNTP. Como servidor de DNS principal do PUUG, a relay responde a pedidos da parte dos aderentes aos serviços de rede de forma a permitir-lhes a obtenção da informação necessária para estabelecer conexões para hosts remotos. É também o mail relay do PUUG e como tal tem a seu cargo o encaminhamento das mensagens de correio electrónico para todos os aderentes aos serviços de rede do PUUG e deles para a Internet. Por último, faz a distribuição pelos aderentes dos artigos das Usenet News que recebe directamente da EUnet em Amsterdão.

4.2.2 Routing IP e o Portmaster

No momento da implementação deste serviço o PUUG ainda não tinha a possibilidade de fazer routing para a Internet de redes que não lhe pertencessem. Desta forma os aderentes a este serviço não podem ter a sua rede (ou conjunto de redes) por detrás desta ligação ao equipamento do PUUG. Devido a este facto bastante incómodo torna-se necessário que o aderente possua uma máquina com o endereço IP numa rede do PUUG ficando assim a instituição aderente limitada a uma máquina com conexão total para a Internet.

Em princípio o aderente deverá utilizar a máquina como gateway para os serviços da Internet que não necessitem de ligação interactiva como são o correio electrónico e as Usenet News. Os serviços interactivos como o telnet e o ftp terão de ser utilizados a partir desta

máquina pelos utilizadores da instituição. A utilização simultânea requer que o sistema operativo da máquina seja multitasking.

Um utilizador no Portmaster é definido através de uma entrada numa tabela constituida por vários campos. Esta tabela, chamada tabela de passwords, tem semelhanças com a tabela de passwords do sistema Unix, de modo que tem dois campos de acesso, o nome do utilizador e a respectiva password. O Unix define a directoria home e o programa de acesso ao sistema que o utilizador corre enquanto que o Portmaster define o tipo de ligação do utilizador.

Naturalmente os campos nome e password destinam-se a validar o utilizador durante o estabelecimento da ligação. Através do nome do utilizador é obtida a informação referente ao tipo de ligação que lhe está atribuida. Esta é constituida pelos campos:

address - endereço IP.
protocol - SLIP ou PPP.
netmask - máscara da rede.
várias opções booleanas definindo a entrada.

A cada novo aderente ao serviço é atribuido um endereço IP na mesma rede em que estão o terminal server e o servidor do PUUG, a relay. Assim, o parâmetro *netmask* será igual para todos, i.e., é o mesmo da rede do PUUG. Esta atribuição de endereços está limitada à partida pela quantidade de endereços disponíveis nesta rede.

O routing é configurado no lado do aderente de forma a utilizar o Portmaster como gateway, ou seja, é definida a route por defeito para o Portmaster que sabe como encaminhar os pacotes para a Internet. O encaminhamento de pacotes para a máquina do aderente torna-se possível devido ao facto de o Portmaster anunciar-se como destino, através do protocolo ARP, para os endereços IP das conexões activas em cada momento.

A partir do momento que seja possível ao PUUG fazer o routing das redes dos seus aderentes, as alterações a nível do Portmaster serão bastante simples. Este faz routing de redes ligadas às suas portas série através do protocolo RIP. Uma vez que o utilizador definido no Portmaster tem uma rede por detrás ele passará a anunciar esta rede para o exterior. Do lado do aderente mantém-se a definição da mesma rota por defeito.

4.2.3 Gestão do serviço

A gestão da configuração dos diversos sub-sistemas de acesso à rede do PUUG encontra-se automatizada através da utilização de uma base de dados com informação específica de cada aderente ([OLI92]).

De seguida descreve-se o sistema de gestão existente, bem como se define um aderente aos serviços de rede com conexão à Internet através de X.25. Na base deste tipo de acesso e da sua definição na base de dados, foi feito o upgrade do sistema de gestão de forma a este suportar o acesso à Internet por Dialup.

Sistema de gestão

O sistema de gestão é constituido por três componentes: um conjunto de ficheiros que descrevem cada aderente, várias tabelas em formato gdbm (GNU dbm) e um conjunto de

programas de manutenção e de configuração.

Cada aderente institucional, chamado "entidade" neste sistema de gestão, é descrito num ficheiro através de vários atributos. Certos atributos são meramente informativos e incluem dados como contactos com a instituição, morada e números de telefone. Os restantes campos destinam-se a providenciar a informação necessária sobre a ligação do aderente de modo a configurar os diversos sub-sistemas para o acesso do mesmo. Neste subsistemas incluem-se o correio electrónico, as news, o DNS, o UUCP e a configuração do router do PUUG.

Com base no conteúdo da informação sobre cada entidade, são mantidas várias tabelas gdbm de forma a optimizar a pesquisa da base de dados. Tal como se utiliza no desenvolvimento de projecto aplicacionais, as tabelas são mantidas actualizadas através da utilização do programa make. Os ficheiros de configuração dos subsistemas são verificadas contra o conteúdo das tabelas gdbm através de comandos próprios para o efeito. Caso não estejam actualizados, são reconstruídos de novo de modo a manterem-se coerentes com a informação corrente.

No geral o funcionamento do sistema de gestão baseia-se na alteração de um ficheiro de dados de um aderente seguido da execução do programa make para actualizar o sistema.

Entidade com acesso Internet por X.25

Apresenta-se o ficheiro de dados que descreve uma entidade com acesso à Internet através do PUUG e que acede ao router do PUUG através do protocolo X.25.

```
customer        mail
country         pt
machine         <hardware> ; <sistema operativo>
organization    <designacao do aderente>
person          <contacto na instituicao/empresa>
email           <email do contacto>
telephone       <numero de telefone>
fax             <numero de fax>
address         <morada>
address         <morada>
address         <morada>
# Routing
transport       TCP/IP-X25
x25-map         193.126.4.146 000000000 reverse
i-link          gt-aderente 4.146
primary         aderente.pt
host            <maquina> 193.126.4.146
bind-db         PTUNET-ONLY
introduced      canau@puug.pt 940704
remarks         passou a x25 internet 940704
```

Os atributos que tornam esta entidade como tendo acesso à Internet são:

```
# atributo      endereco IP NNA
x25-map         193.126.4.146     000000000 reverse
```

O atributo x25-map é inserido automaticamente na configuração do router do PUUG de modo a permitir o acesso, a partir do NNA indicado, ao mesmo. O endereço IP do indicado será atribuido ao outro lado da ligação e está numa rede do PUUG com acesso à Internet.

```
# atributo  informacao DNS
i-link            gt-aderente 4.146
```

Este atributo é utilizado para actualizar a zona DNS do PUUG através da sua inserção num conjunto de macros m4 que geram esta zona. Neste exemplo é inserido o A record gt-aderente.puug.pt 193.126.4.146.

```
# atributo  dominio
primary           aderente.pt
```

Um serviço adicional prestado pelo PUUG é a manutenção do primário do domínio DNS do aderente. Esta linha cria o SOA na configuração do servidor DNS do PUUG.

```
# atributo  maquina     endereco IP
host        <maquina>   193.126.4.146
```

Este atributo insere um A record no domínio DNS do aderente. Neste exemplo, <maquina>.aderente.pt 193.126.4.146. Este host é a máquina do aderente com acesso à Internet. A sintaxe da base de dados permite que existam várias linhas com o atributo host.

Alterações para o acesso DIALUP

Com base nos campos apresentados atrás para o acesso X.25, o sistema de gestão foi alterado de forma a configurar os sub-sistemas de rede para o acesso DIALUP. A sintaxe da base de dados foi aumentada e foram acrescentados novos comandos de forma a permitir que a mesma suporte o acesso DIALUP.

De seguida apresenta-se uma entidade DIALUP e indica-se a nova sintaxe da base de dados.

```
customer          mail
country           pt
machine           <hardware> ; <sistema operativo>
organization      <designacao do aderente>
person            <contacto na instituicao/empresa>
email             <email do contacto>
telephone         <numero de telefone>
fax               <numero de fax>
address           <morada>
address           <morada>
address           <morada>
# Routing
transport         CSLIP
s-link            gt-aderente 4.86
dialup            <maquina>.aderente.pt
host              <maquina> 193.126.4.86
primary           aderente.pt
bind-db           PTUNET-ONLY
introduced        canau@puug.pt 940601
```

Os novos atributos que surgem são s-link, que substitui i-link, e dialup. O primeiro mantêm os objectivos do i-link a nível de configuração da informação do DNS. Este novo atributo provoca a configuração automática de uma entrada para o aderente no terminal server. O atributo dialup é utilizado para configurar o sub-sistema de correio electrónico de forma a que exista uma nova queue para a entidade. O atributo x25-map deixa de ser necessário.

4.2.4 Sistema de correio electrónico

Análise

Uma ligação IP DIALUP funciona perfeitamente sempre que o aderente pretende uma conexão para o exterior, por exemplo, utilizando o protocolo TELNET ou o protocolo FTP. Em particular não tem problemas de maior quando pretende enviar correio electrónico. Basta que o sistema do aderente tenha a possibilidade de estabelecer a conexão automaticamente. No sentido inverso apenas se pode atingir o sistema do aderente quando este está ligado.

Pondo de parte os restantes tipos de conexões para o sistema do aderente, especial atenção tem de ser dada à entrega de correio electrónico para o domínio do aderente. O facto de apenas existir conexão para o aderente enquanto este mantém a ligação provoca que seja impossível enviar-lhe correio electrónico através do protocolo SMTP sem elaborar um esquema dedicado.

O backbone do PUUG tem por missão ser o mail relay de todos os aderentes aos serviços de rede. Neste sistema, relay.puug.pt, está instalada a versão *sendmail-5.67a+IDA-1.5* do sendmail IDA. Este programa é um mailer, i.e., é um programa cujo objectivo é fazer routing de correio electrónico. Ao utilizar o sendmail para entregar as mensagens aos aderentes DIALUP verificar-se-ia que as mensagens ficariam muito tempo na queue do programa e que apenas seriam entregues se o aderente efectuasse uma ligação no momento em que o sendmail processa a queue (geralmente de hora a hora). O facto de o sendmail ter de correr a queue todas as horas para estas mensagens traria uma carga insuportável para o sistema.

Uma solução para este problema passa pela utilização do protocolo UUCP para a entrega do correio electrónico. Uma vez que neste as mensagens apenas são entregues quando um dos lados estabelece uma ligação UUCP, o problema existente para o SMTP não se verifica. Esta solução acarreta consigo vários factores para ambos os lados - PUUG e aderente. Do lado do aderente, obriga-o a que instale e configure no seu sistema software de UUCP. No lado do PUUG obriga a que exista uma nova entidade no sistema de gestão, ficando assim o aderente representado por uma entidade DIALUP e uma UUCP. Embora esta solução tenha as suas vantagens e desvantagens, procurou-se uma outra solução que permitisse a utilização do protocolo SMTP para entregar o correio electrónico.

Solução implementada

A configuração dos MX RRs está feita de forma a que a mensagem seja entregue primeiro ao mail relay do aderente. Com a prioridade imediatamente a seguir vem o mail relay do PUUG. O que é que acontece quando existe uma mensagem em qualquer ponto da Internet para entregar a uma mailbox no domínio do aderente ? Primeiro o DNS é interrogado sobre a quem deve ser entregue a mensagem. O mailer emissor recebe como resposta os MX RRs definidos e como o mail relay do aderente tem precedência tenta abrir uma conexão SMTP para este. Se consegue obter a conexão entrega a mensagem, senão tenta o mail relay de precedência seguinte, o do PUUG. A relay.puug.pt após receber uma mensagem para um host DIALUP tenta novamente entregá-la ao mail relay do aderente e se falhar coloca-a em queue.

De hora a hora a queue é varrida apenas para os aderentes DIALUP e tenta-se entregar novamente as mensagens. Se a máquina do aderente não estiver acessível as suas mensagens são movidas para uma queue particular. De momento este passo é efectuado através de uma entrada no crontab da relay.puug.pt, sendo muito provável que venha a ser implementado através de um servidor dedicado.

Sempre que uma máquina estabelece a conexão no terminal server, este envia uma mensagem para o syslogd da relay.puug.pt. Esta tem um servidor especial a correr que detecta esta mensagem. Com base na informação escrita no syslog, o servidor invoca o sendmail com indicações para varrer a queue particular do aderente. Neste momento já existe conexão para o aderente e é possível entregar-lhe as mensagens a ele destinadas. É óbvio que o mail relay do aderente deve estar preparado para aceitar conexões SMTP.

Caso o aderente esteja sem ligar durante muito tempo pode ocorrer que a sua queue provoque a falta de espaço no sistema de ficheiros onde está instalada. Para resolver este problema cada queue deverá ser varrida periodicamente (por exemplo, uma vez por dia) para provocar o timeout das mensagens antigas e provocar a sua devolução ao emissor.

A máquina relay.puug.pt foi configurada com o sendmail IDA para entregar correio electrónico a sistemas com acesso por DIALUP segundo o processo descrito atrás. O sistema está implementado e está totalmente automatizado.

Análise da solução implementada

A solução implementada apresenta duas pequenas inconveniências. A primeira é o intervalo de tempo que pode ocorrer desde o momento que uma mensagem chega à relay.puug.pt e ao momento em que ela é entregue ao destinatário. De forma a tentar minimizar este intervalo, sempre que o sendmail processa uma mensagem, tenta-se que ela seja entregue imediatamente. Isto provoca a segunda inconveniência: se o mail relay do aderente não está acessível haverá uma sobrecarga desnecessária para a relay.puug.pt. Este pormenor ainda está em estudo. De salientar que o programa sendmail é juntamente com o sistema INN os responsáveis pelas ocorrências de maior carga na máquina.

A análise do intervalo de tempo indicado atrás é bastante complexa uma vez que estão em jogo vários factores sendo um deles bastante inconstante. Este factor principal é a própria ligação do aderente que levanta as questões: O aderente faz polling ? Com que frequência ? Qual o tempo de cada ligação ?

Não foi feita uma análise aprofundada desde intervalo de tempo. Partindo do princípio que a mensagem é entregue depois de ter sido movida para a queue particular é possível uma análise simples de tempos de espera:

- a mensagem chega à relay.puug.pt num tempo T;
- de hora a hora esta queue é varrida, por ex.: no minuto M;
- a mensagem é entregue assim que o aderente efectuar uma nova ligação após o minuto M.

É garantido que a diferença de tempos entre T e o próximo minuto M nunca excede uma hora. Se o aderente ligar no momento em que a mensagem estiver na queue principal, esta não é varrida para ele. A configuração normal do sendmail define um varrimento da queue principal de hora a hora o que provoca a entrega da mensagem ao aderente se o seu mail relay estiver acessível.

4.2.5 News

Análise

Para um acesso por linha comutada é possível assegurar um feed de Usenet News através de dois protocolos diferentes: UUCP e NNTP. Ambos têm as suas vantagens e desvantagens.

Tal como para o correio electrónico, um feed de news por UUCP obriga a que exista uma nova entidade a gerir na base de dados do backbone do PUUG. Uma segunda desvantagem é o batching de artigos que é feito para a spool do sistema UUCP. Este factor envolve a duplicação dos artigos para os vários sites que recebem news por UUCP. Esta é a situação corrente de vários aderentes do PUUG por UUCP. Este tipo de distribuição tem a vantagem de permitir que o aderente separe a ligação IP DIALUP da ligação para receber o feed de news.

O segundo protocolo indicado atrás, o NNTP, não implica o spooling de artigos uma vez que o software instalado para gerir o sistema Usenet News no PUUG, o INN tem um funcionamento diferente. Os artigos a enviar para o site do aderente são indicados num ficheiro dedicado ao feed do aderente. Aqui surge a mesma questão que surge para o correio electrónico: quando enviar os artigos para o aderente ? A solução passa por um processo semelhante ao desenvolvido para o correio electrónico, a ligação é detectada e imediatamente é executado o comando para o envio do feed. Problema: o aderente pode não desejar ter a linha saturada com a transferência de artigos sempre que liga... O que fazer ?

Soluções

Com base na análise indicada atrás indicam-se três formas de enviar um feed de news para o aderente. Embora se possa discutir com o aderente qual o tipo de transferência a utilizar, a mais indicada para este tipo de acesso é a terceira, NNTP passivo.

- UUCP
- NNTP activo - Estes dois tipos de ligação estão descritos acima.
- NNTP passivo - Com este tipo de ligação a gestão no lado do sistema de news do PUUG limita-se a permitir o acesso por NNTP à máquina do aderente. A configuração dos grupos a receber é da responsabilidade do mesmo. O funcionamento baseia-se em o aderente ligar quando desejar e fazer um pedido no género: "Quero receber todos os artigos dos seguintes grupos que aí chegaram depois de uma certa hora".

Utilizando o NNTP passivo resolve-se o problema do envio dos artigos para o aderente e tem a vantagem de simplificar imenso a gestão dos grupos que o aderente deseja receber. Sempre que o aderente deseja receber um novo grupo, ou deixar de receber um antigo, basta alterar a configuração do seu sistema de news.

4.2.6 Evolução do serviço

Tal como é descrito em 'Routing IP e o Portmaster' este serviço passará a permitir que um aderente aceda à Internet através da sua rede IP própria. A nível da gestão e automatização do sistema de manutenção deste serviço será necessário encontrar uma solução para incluir a configuração do routing de redes na base de dados. Este processo passará, muito provavelmente, pela inclusão de um ou mais atributos na definição da sintaxe dos campos da base de dados (por exemplo, o atributo "rede") e pela implementação de um ou mais scripts de manutenção e gestão.

Ao nível de equipamento, é de esperar que o número de modems aumente bem como os mesmos passem a suportar velocidades superiores.

4.3 Accounting de recursos

Os serviços do PUUG descritos nos capítulos anteriores requerem que cada componente gira relatórios precisos de actividade de forma a contabilizar os recursos utilizados pelos aderentes. Para cada serviço disponibilizado pelo PUUG foi necessário construir ferramentas de accounting específicos. Estas ferramentas, em geral, processam os ficheiros de registo de actividade de cada componente e enviam relatórios pormenorizados destinados à contabilização. De salientar que todos os ficheiros relacionados com accounting estão protegidos pelo esquema de backup automático que protege todos os sistemas do PUUG.

De seguida são descritos os vários programas utilizados na gestão dos serviços de rede do PUUG.

4.3.1 sendmail-account - contabilização de tráfego de correio electrónico

A necessidade para este programa surgiu assim que o PUUG começou a disponibilizar serviços de rede em que está incluida a contabilização do correio electrónico. Foi desenvolvido inicialmente por Salvador Pinto Abreu em 1991, e era composto por vários scripts escritos na linguagem awk interligados entre si por shell scripts. Esta primeira implementação servia perfeitamente para o accounting de um número reduzido de mensagens de correio electrónico. Com a expansão do número de aderentes ao serviço, o número de mensagens a contabilizar subiu exponencialmente sendo necessário optimizar o programa de accounting. A segunda versão do programa foi escrita pelo autor em 1992. Esta nova versão difere da primeira no facto do núcleo de decisão (quem paga) ser totalmente escrito em linguagem C. Os diversos componentes da ferramenta têm sofrido ligeiras correcções de erros e ligeiros aperfeiçoamentos ao longo do tempo.

O funcionamento deste programa baseia-se em processar os registos do programa sendmail com base no emissor e receptor da mensagem de modo a decidir duas coisas: qual dos dois paga a mensagem e qual a classe da mesma - nacional ou internacional.

São arquivados os registos do syslogd gerados pelo programa sendmail e ainda o output deste programa.

4.3.2 Login/last - contabilização de individuais

Tal como está descrito no capítulo sobre os serviços para individuais, o acesso à Internet é feito através do login numa máquina Unix e dum subsistema dedicado. O sistema Unix inclui um modelo de accounting de utilização baseado no registo dos tempos de entrada e de saída dos utilizadores. O accounting de acessos do serviço Login foi implementado tendo como base esta informação.

Para registar e pesquisar os acessos ao sistema, o Unix tem duas componentes dedicadas: um comando de pesquisa - comando last, e um ficheiro de registo - */var/adm/wtmp* (este ficheiro é dependente do tipo de sistema Unix, tendo por vezes um nome diferente ou em vez de um serem dois ficheiros). O registo é feito neste ficheiro através do programa que gere os acessos ao sistema - login. Este ficheiro é binário e tem um formato próprio reconhecido pelo comando last que o lê e coloca a informação num formato de texto de forma a possibilitar a sua leitura.

No entanto a informação dada pelo comando last não está na forma mais apropriada para fazer o accounting do serviço uma vez que mostra os vários logins de cada utilizador e o pretendido é a quantidade total de logins e o tempo total desses. Assim, foi escrito um programa em linguagem awk para processar o output do comando last de forma a somar o tempo total de ligação bem como o número total de logins. Este programa foi escrito por Jorge Frazão em 1992 enquadrado no estágio descrito em [OLI92].

O esquema de accounting descrito atrás não está preparado para guardar informação de accounting ao longo do tempo. No fim de cada intervalo de tempo de accounting, um mês, o ficheiro de registo era simplesmente truncado a zero. O esquema preparado para este accounting passou a enviar no final de cada mês o accounting mensal para os administradores, a guardar uma cópia do ficheiro de registo e a truncar o ficheiro.

O ficheiro arquivado referente a um dado mês está no formato específico que o comando last consegue ler. Como o last original do sistema não suporta a pesquisa de ficheiros que não sejam o ficheiro de registo foi necessário instalar no sistema um novo comando last que permitisse a utilização de um ficheiro de registo arbitrário. Desta forma é possível pedir ao sistema que faça o accounting de um dado mês já arquivado.

4.3.3 dial-account - contabilização de acesso DIALUP

Os acessos aos dois serviços de DIALUP disponibilizados pelo PUUG - DIALUP IP individual e DIALUP IP institucional, são suportados por um terminal server Portmaster. O registo de actividade desta máquina é feita através da utilização do envio de mensagens de registo de actividade para uma máquina onde esteja a correr o servidor syslogd. A informação enviada é variada sendo apenas importante para o accounting as mensagens referentes aos inícios e fins de sessão dos utilizadores.

Devido ao facto do accounting ser orientado para o nome de utilizador esta informação é utilizada para fazer o accounting dos dois tipos de utilizadores que acedem a estes serviços.

Os dados recebidos do Portmaster são guardados num ficheiro dedicado e processados de forma a obter o accounting. O ficheiro é constituido por linhas de texto com uma sintaxe própria que é necessário processar para fazer o matching entre a entrada e a saída do utilizador de modo a calcular o tempo da sessão.

De forma a contabilizar os tempos de sessão em relação aos utilizadores foi desenvolvido um programa em linguagem C para processar os registos. Este programa está codificado de forma a fazer o parsing dos diversos formatos gerados pelo Portmaster no syslogd. Com base nos vários campos das mensagens o programa associa-as duas a duas para gerar um registo de sessão em que é indicada a duração da mesma. O registo de todas as sessões é em seguida processado através de vários programas escritos em shell e em awk. O resultado pode ser genérico indicando a totalidade do accounting do Portmaster ou específico, por exemplo, apenas para um tipo de utilizadores ou apenas para um utilizador.

As mensagens geradas pelo Portmaster são guardadas no ficheiro */var/log/Portmaster* que no fim de cada período de tempo - um mês, é processado sendo o resultado enviado para os administradores. De seguida é arquivado e preparado para o novo mês. Os dados processados são também arquivados com a referência do mês de modo a evitar a necessidade de um novo processamento.

Os ficheiros envolvidos no accounting das ligações ao Portmaster estão protegidos pelo mesmo esquema de backups descrito atrás.

4.3.4 cisco-report - contabilização de tráfego IP

O acesso à Internet através de X.25 foi posto ao dispôr dos aderentes do PUUG no primeiro semestre de 1994. O acesso a este serviço é suportado por um router Cisco ligado à rede nacional de X.25 da Telepac. Pretende-se contabilizar o tráfego que passa pelo router vindo desta ligação e das ligações DIALUP institucionais.

O accounting deste acesso é efectuado através da contabilização da quantidade de informação que passa pelo router do PUUG com origem ou com destino no equipamento do aderente. O router regista em memória cada byte que transfere entre dois endereços.

Com base na informação registada é possível imaginar uma tabela de duas entradas, origem e destino, cujo valor é a quantidade de bytes passado. O sistema operativo do Cisco permite ligar e desligar o registo de accounting de IP e possui comandos para consultar a tabela corrente de accounting e para a apagar de forma a implementar um período de accounting. No caso do PUUG este período é de um dia devido à necessidade de manter uma vigilância apertada sobre o tráfego internacional. Como efeito secundário evita-se a sobrecarga da memória do router uma vez que se o período de limpeza da tabela fosse o mesmo do de accounting (um mês) surgiria o risco de perder a tabela por *crash* do router ou por falha eléctrica.

A tabela de accounting do cisco é arquivada todos os dias num ficheiro próprio para cada dia. No final do mês estes ficheiros são processados em conjunto de forma a construir a tabela de tráfegos com o objectivo de contabilizar cada aderente.

Em vez de começar por escrever uma aplicação própria destinada a fazer o accounting do tráfego IP foi decidido pesquisar na Internet por uma ferramenta que já implementasse esta função. No arquivo da Cisco, ftp.cisco.com, existem várias aplicações de accounting de IP escritas por utilizadores dos seus produtos e postos à disposição pública pelos mesmos. Após experimentar vários programas, foi escolhida a aplicação *getipacct* desenvolvida por Daniel Karrenberg em 1990.

A principal dificuldade a superar quando é pretendido obter informação de um router deve-se ao facto de não existir nenhum mecanismo para retirar informação do mesmo de uma forma simples. Assim, observando que é possível visualizar a tabela de accounting através de uma secção de telnet para o router, imediatamente surge a idéia de utilizar o programa expect para retirar a tabela do router. O que a aplicação *getipacct* faz é algo semelhante ao expect servindo-se para tal do protocolo telnet para ligar ao router e enviar-lhe comandos. O resultado destes comandos, login no server, leitura da tabela e limpeza da mesma permite guardar uma tabela com o accounting diário do router.

A aplicação é constituida por um programa em C destinado a obter a tabela de accounting, um programa em C para transformar endereços IP em nomes e por vários scripts em shell e awk que a processam. De forma a utilizar esta aplicação para fazer o accounting do tráfego IP do router do PUUG, foi necessário alterar os scripts e escrever novos scripts. O programa de ligação ao router e o programa de transformação de endereços não foram alterados. Os novos scripts destinam-se a apresentar o accounting orientado para dois tipos de tráfego, nacional e internacional e dividido por aderente.

O funcionamento geral deste sistema de accounting baseia-se num programa executado todos os dias a partir do cron que arquiva a tabela diária de accounting e envia o processamento da mesma para os administradores. No final do mês, os programas de accounting são corridos sobre todas as tabelas diárias de modo a criar uma tabela de tráfego IP mensal. Esta tabela é também arquivada.

Tanto as tabelas arquivadas como as tabelas diárias estão protegidas pelo sistema de backup de ficheiros do PUUG.

4.3.5 Fiabilidades/falhas

Um sistema de accounting que é utilizado para cobrar o serviço aos aderentes do PUUG tem de ser robusto o suficiente de modo a não permitir falhas e a produzir valores correctos. No desenho e implementação procurou-se minimizar a possibilidade de falha ao máximo, no entanto há situações em que é impossível ter a garantia de que o accounting está completo. Como exemplo citam-se duas situações em que é possível perder informação de accounting. O primeiro exemplo surge no router do PUUG. Se esta máquina tem um crash, perde-se toda a informação de accounting de tráfego IP até à última execução do accounting diário. A segunda surge com o Portmaster. Esta máquina envia a informação de registo de actividade para o syslogd através do protocolo UDP/IP. Por (raras) vezes surgem perdas de pacotes e perdas de conexão entre o Portmaster e o servidor. Nestas situações perdem-se mensagems, o que provoca que, se apenas existir o registo de começo ou o registo de fim de uma sessão, o programa de accounting perca o valor de uma sessão.

Estes problemas apenas trazem problemas para o accounting para o lado do PUUG uma vez que em caso de perda de informação o valor a cobrar ao aderente ao serviço é inferior ao valor real. No entanto procura-se previnir estas situações e resolvê-las imediatamente após a sua detecção.

Capítulo 5

Conclusões

Longe de estar terminado, o projecto do PUUG para o estabelecimento de um "service-provider" dando acesso sem restrições à Internet em Portugal ainda necessita de dar mais alguns passos importantes. O principal problema que até ao momento impede o PUUG de atingir este objectivo em pleno é a falta de uma linha directa para o estrangeiro. Este recurso de vital importância para o PUUG porque permitirá que este coloque na Internet os seus aderentes de um modo semelhante ao verificado para as instituições de ensino superior ligadas à Fundação para o Desenvolvimento dos Meios Nacionais de Cálculo Ciêntifico (FCCN). Este aspecto impediu em parte que um dos objectivos do estágio não tenha sido alcançado, o estudo dos mecanismos de routing a utilizar e os protocolos de routing exteriores (o outro pormenor foi o envolvimento necessário nos restantes serviços). Quando uma linha internacional estiver disponível, será necessário criar uma estrutura de gestão e de manutenção do equipamento do PUUG de uma forma semelhante à que já existe para os restantes serviços. Este método de gestão terá como objectivos uma manutenção facilitada dos recursos e dos aderentes, facilidade na obtenção de relatórios de utilização e controle de questões relacionadas com a segurança do equipamento.

É de esperar que os serviços de individuais venham a ser melhorados através da instalação de novas versões de software, correcção de problemas com o acesso, melhoria da interface, etc.

O trabalho no PUUG obriga a que se aceda remotamente a várias máquinas de modo a possibilitar a sua administração e vigilância. Deste modo, para suportar as minhas tarefas de administração e de trabalho de estágio, o PUUG adquiriu uma workstation NeXT. Este equipamento embora descontinuado a nível de hardware, oferece uma interface gráfica bastante avançada e agradável de utilizar tendo contribuido bastante para facilitar a execução do meu trabalho. Além deste equipamento tive à minha disposição computadores pessoais IBM-PC e Apple Macintosh de modo a efectuar diversos testes nos serviços de acesso que ajudei a implementar, a instalar e a administrar. As bases de testes com estes computadores apenas ficariam completas com vários tipos de modem destinados ao acesso à rede do PUUG através das linhas telefónicas. No equipamento de produção do PUUG trabalhei com dois computadores RISC, o anterior backbone do PUUG, um DecSystem 3100, antiga dec4pt.puug.pt, correntemente individual.puug.pt, e o novo backbone, uma Sun SPARCClassic, a relay.puug.pt. Além destes servidores trabalhei com routers Cisco e com terminal servers Portmaster da Livingston.

Um estágio com estas características permitiu-me adquirir elevados conhecimentos no campo da administração do sistema UNIX passando por variados aspectos, desde a conversão de software entre diversos "sabores" do sistema, BSD vs. SYSV, até experiência com questões de segurança. A concepção e instalação do acesso DIALUP ao PUUG permitiu-me adquirir experiência com variados sistemas e com variado equipamento. A participação nos diversos passos deste projecto permitiu-me ter a sensibilidade necessária para lidar com diversos tipos de situações e de problemas que um "service provider" tem de enfrentar na montagem e na

manutenção dos seus serviços.

Este tipo de experiência adquirida coloca o estagiário numa posição chave no mercado de trabalho ligado ao ramo dos serviços Internet e de informação em Portugal. Maior importância tem este pormenor devido ao facto de a Internet estar, lenta mas definitivamente, a implantar-se em Portugal e vir a surgir a necessidade de elementos experientes no ramo tanto nas empresas que se liguem a ela como junto de futuros "service providers".

Pode-se concluir que este estágio foi um sucesso tanto para o estagiário, a nível de experiência profissional, como para o PUUG, a nível da disponibilização de novos serviços.

Bibliografia

[BLA92] *Black, U.*, TCP/IP and Related Protocols, McGraw-Hill, 1992

[COM91] *Comer, D. E.*, Internetworking with TCP/IP, Vol. I: Principles, Protocols and Architecture, 2nd Edition, Prentice-Hall, 1991

[COS93] *Costales, B., E. Allman* e *N. Rickert*, sendmail, O'Reilly & Associates Inc., Nov. 1993

[FOR88] *Forsberg, C.*, The ZMODEM Inter Application File Transfer Protocol, Omen Technology Inc, Out. 1988

[GAR91] *Garfinkel, S.* e *G. Spafford*, Pratical Unix Security, O'Reilly & Associates Inc., Jun. 1991

[GRA93] *Gray, T.*, Comparing Two Approaches to Remote Mailbox Access: IMAP vs. POP, Documentação do pacote pine3.89, University of Washington, Mai. 1993

[HUN92] *Hunt, C.*,TCP/IP Network Administration, O'Reilly & Associates Inc., Ago. 1992

[IDA] Documentação do programa *sendmail-5.67a+IDA-1.5*

[OLI92] *Oliveira, J. F.*, Construção de Ferramentas de Monitoragem e Detecção de Anomalias na Rede PTEUnet, Relatório de estágio, Dept. Informática da FCUL, Jul. 1992

[QUA90] *Quarterman, J. S.*, The Matrix - Computer Networks and Conferencing Systems Worldwide, Digital Press, 1990

[RFC822] *Crocker, D.*, "Standard for the format of ARPA Internet text messages", 08/13/1982

[RFC1055] *Romkey, J.*, "Nonstandard for transmission of IP datagrams over serial lines: SLIP", 06/01/1988

[RFC1144] *Jacobson, V.*, "Compressing TCP/IP headers for low-speed serial link", 02/01/1990

[RFC1171] *Hobby, R.* e *Perkins, D.*, "The Point-to-Point Protocol (PPP) Initial Configuration Options", 07/24/1990

[RFC1172] *Hobby, R.* e *Perkins, D.*, "The Point-to-Point Protocol (PPP) Initial Configuration Options", 07/24/1990

[RFC1176] *Crispin, M.*, "Interactive Mail Access Protocol - Version 2", 08/20/1990

[RFC1332] *McGregor, G.*, "The PPP Internet Protocol Control Protocol (IPCP)", 05/26/1992

[RFC1331] *Simpson, W.*, "The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links". 05/26/1992

[RFC1460] *Rose, M.*, "Post Office Protocol - Version 3", 06/16/1993.

[WAL92] *Wall, L.* e *R. L. Schwartz*, Programming Perl, O'Reilly & Associates Inc., Mar. 1992