

RELATÓRIO - SERVIÇOS INTRANET



Universidade do Porto

FEUP Faculdade de
Engenharia

Manuel Maia (ei00128@fe.up.pt)
Ricardo Batista (ei00132@fe.up.pt)
Michel Diaz (ei04101@fe.up.pt)
Pedro Sampaio (ei00118@fe.up.pt)

Arquitectura de Redes e Serviços 2004/2005

23 de Julho de 2005

Conteúdo

1	Introdução	4
1.1	Objectivos	4
1.2	Estrutura do Relatório	4
2	Arquitectura da Rede	5
3	Serviços de Suporte	6
3.1	LDAP	6
3.1.1	Introdução	6
3.1.2	Configuração do Servidor	6
3.1.3	Configuração do Cliente	8
3.1.4	Servidor Cache de LDAP	9
3.1.5	LDAP via Web	9
3.2	DNS	10
3.2.1	Introdução	10
3.2.2	Instalação do servidor	10
3.2.3	Configuração do servidor	10
3.2.4	Configuração do cliente	14
3.3	DHCP	16
3.3.1	Introdução	16
3.3.2	Instalação do servidor	16
3.3.3	Configuração do servidor	16
3.3.4	Instalação do cliente	17
3.3.5	Configuração do cliente	18
4	Sistema de Ficheiros Distribuido	19
4.1	NFS	19
4.1.1	Configuração do Servidor de LDAP	19
4.1.2	Instalação do Servidor	19
4.1.3	Configuração do Servidor	19

4.1.4	Configuração dos clientes	20
4.2	Samba	21
4.2.1	Introdução	21
4.2.2	Instalação do Servidor	21
4.2.3	Configuração do servidor	21
4.2.4	Introduzir utilizadores	22
5	Serviço de E-Mail	23
5.1	Servidor de SMTP	23
5.2	IMAP	25
5.3	POP	26
5.4	SMTP no Relay	26
5.5	IMP	27
6	Serviços Web	29
6.1	HTTP	29
6.1.1	PHP e Base de dados	29
6.1.2	Acesso controlador por PAM	30
6.1.3	Domínios Virtuais	31
6.2	Proxy	32
6.3	Estatísticas	33
7	Criação de novas contas	34
8	Conclusão	37

Lista de Figuras

1	Arquitectura da rede	5
---	--------------------------------	---

1 Introdução

Este trabalho realiza-se no âmbito da disciplina de Arquitecturas de Redes e Serviços, do 4º ano da Licenciatura em Engenharia Informática e Computação.

1.1 Objectivos

O objectivo principal deste trabalho é o de construir uma Intranet com a maioria dos serviços necessários. Neste trabalho serão incluídos os serviços de suporte e os serviço de utilizador final. Como serviços de utilizador final temos:

- Correio electrónico
- Web
- Ficheiros Distribuídos (Network File System e Samba)

Como serviços de suporte temos:

- Serviço de directório - LDAP
- DNS
- DHCP

O enunciado detalhado do trabalho pode ser encontrado em:

http://netlab.fe.up.pt/~oliveira/sci/trabalho_intranet.pdf

1.2 Estrutura do Relatório

Para além desta Introdução e de uma Conclusão em que se explicam algumas das opções tomadas, este relatório contém um capítulo sobre a rede implementada e um capítulo por cada categoria de serviços instalada.

2 Arquitectura da Rede

Não foi feita nenhuma configuração no material activo que compõe a rede, nomeadamente *switches e routers*. O objectivo deste trabalho incidia na instalação e configuração dos serviços mais comuns numa Intranet. A arquitectura resume-se na separação das várias categorias de serviços pelas diferentes máquinas disponíveis:

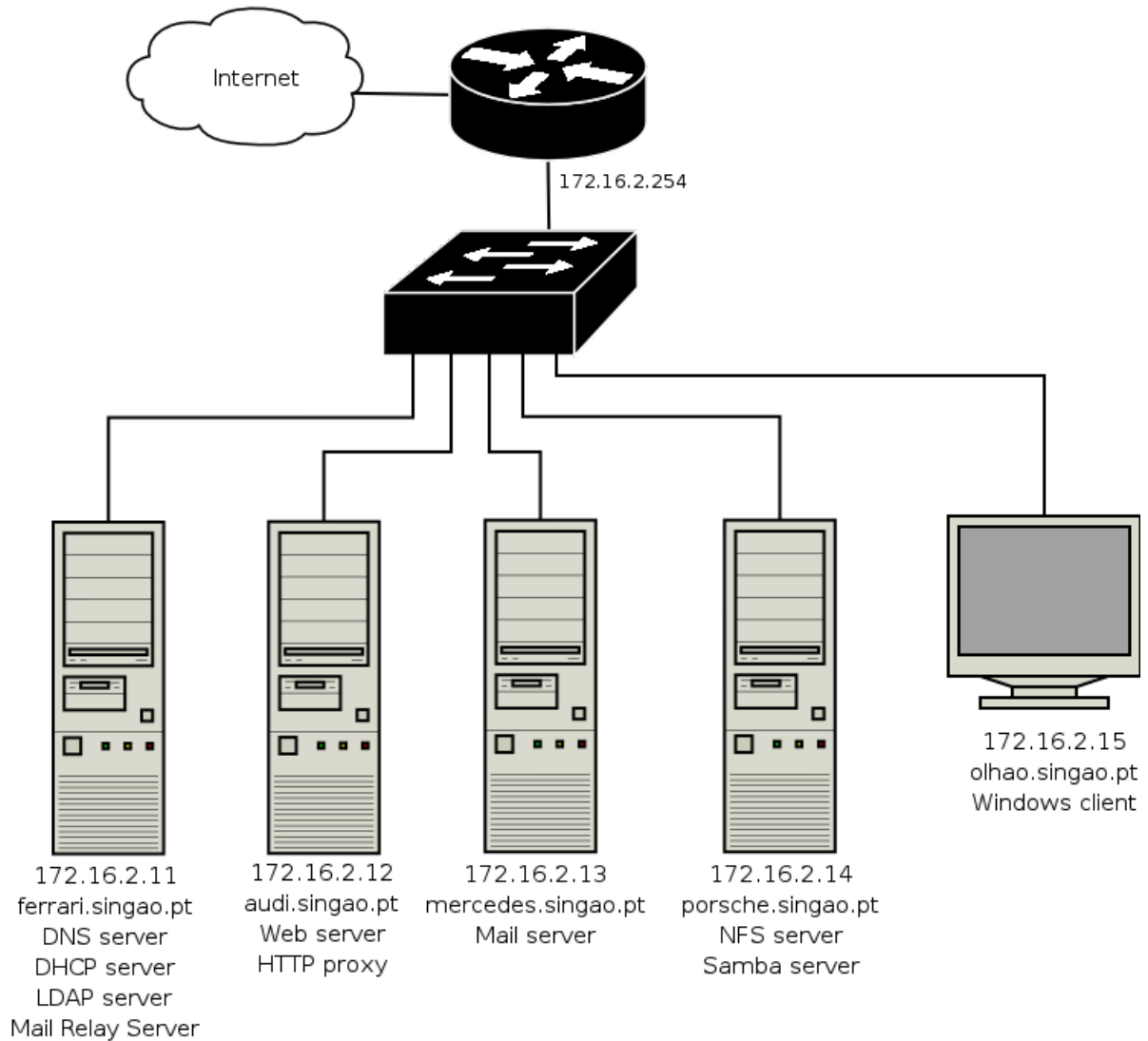


Figura 1: Arquitectura da rede singao.pt

3 Serviços de Suporte

3.1 LDAP

3.1.1 Introdução

O serviço de informação escolhido foi o LDAP (Lightweight Directory Access Protocol), que permite a autenticação dos utilizadores de estações Windows e Linux. Foi também instalada uma aplicação de gestão do LDAP via web.

3.1.2 Configuração do Servidor

Para instalar o servidor instala-se os seguintes pacotes:

```
apt-get install slapd ldap-utils migrationtools
```

Devem ser respondidas algumas perguntas durante a instalação, como por exemplo as entradas relativas ao domínio *singao.pt*. As configurações são guardadas no ficheiro */etc/ldap/slapd.conf* e devem ter o seguinte conteúdo:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/automount.schema
```

```
suffix "dc=singao,dc=pt"
rootdn "cn=admin,dc=singao,dc=pt"
rootpw pass
```

```
access to attribute=userPassword
by dn="cn=admin,dc=singao,dc=pt" write
by anonymous auth
by self write
by * none
access to *
by dn="cn=admin,dc=singao,dc=pt" write
by * read
access to dn=".*,ou=Roaming,o=morsnet"
by dn="cn=admin,dc=singao,dc=pt" write
by dnattr=owner write
```

Depois de efectuar alterações no ficheiro de configuração é sempre necessário reiniciar o servidor LDAP para que as alterações entrem em funcionamento:

```
/etc/init.d/slapd restart
```

Para inserir a informação sobre utilizadores e grupos no LDAP existem várias formas, como por exemplo utilizar as ferramentas do pacote migrationtools da PADL para gerar automaticamente os ficheiros LDIF, criar os ficheiros LDIF manualmente, utilizar o nosso script para adicionar utilizadores, ou via web com a ferramenta de gestão phpLDAPAdmin.

Se se optar por introduzir os utilizadores via web ou script, primeiro tem que se adicionar a base dos utilizadores e grupos ao directório LDAP.

Para isso cria-se um ficheiro base.ldif com o seguinte conteúdo:

```
dn: dc=singao,dc=pt
dc: singao
objectClass: top
objectClass: domain
dn: ou=People,dc=singao,dc=pt
ou: People
objectClass: top
objectClass: organizationalUnit
dn: ou=Groups,dc=singao,dc=pt
ou: Group
objectClass: top
objectClass: organizationalUnit
```

Para adicionar o ficheiro usa-se o comando:

```
ldapadd -c -x -D "cn=admin,dc=singao,dc=pt-W -f base.ldif
```

Em alternativa pode-se usar o método de migração das contas locais dos utilizadores (guardadas em /etc/passwd e /etc/group) . Para isso usa-se o seguinte procedimento.

Inicialmente é necessário configurar o ficheiro migrate_common.ph com os dados do domínio *singao.pt* :

```
vi /usr/share/migrationtools/migrate_common.ph
```

ou

```
vi /etc/migrationtools/migrate_common.ph
```

Em seguida, gera-se os ficheiros LDIF para inserir no directório de informação LDAP:

```
cd /usr/share/migrationtools/
./migrate_base.pl > /etc/ldap/base.ldif
./migrate_group.pl /etc/group /etc/ldap/group.ldif
./migrate_passwd.pl /etc/passwd /etc/ldap/user.ldif
```

Neste momento, em /etc/ldap temos os ficheiros LDIF com a informação a ser inserida no servidor de LDAP. O ficheiro base.ldif contém a estrutura base da árvore LDAP, ou seja, os registos dos objectos de classe top e organizationalUnit. O ficheiro group.ldif contém a informação sobre os grupos e o ficheiro user.ldif a informação sobre os utilizadores.

Para adicionar os ficheiros no directorio do LDAP é necessário executar os comandos para cada ficheiro:

```
ldapadd -c -x -D "cn=admin,dc=singao,dc=pt" -W -f base.ldif
ldapadd -c -x -D "cn=admin,dc=singao,dc=pt" -W -f users.ldif
ldapadd -c -x -D "cn=admin,dc=singao,dc=pt" -W -f groups.ldif
```

3.1.3 Configuração do Cliente

Para que uma máquina possa consultar o servidor de LDAP, e permitir a autenticação através deste serviço é necessário instalar os seguintes pacotes:

```
apt-get install libpam-ldap libpam-cracklib libpam-modules
apt-get install libnss-ldap libnet-ldap-perl
```

Durante a instalação terão que ser respondidas algumas perguntas sobre a configuração, que ficaram guardadas no ficheiro `/etc/ldap/ldap.conf` e deverão ter o seguinte conteúdo:

```
BASE      dc=singao, dc=pt
URI       ldap://ldap.singao.pt
```

Da mesma maneira o ficheiro `/etc/libnss-ldap.conf` e `/etc/pam.ldap.conf` deverá conter:

```
host 172.16.2.11
base dc=singao,dc=pt
ldap_version 3
binddn cn=admin,dc=singao,dc=pt
bindpw pass
```

No ficheiro `/etc/nsswitch.conf` é necessário alterar as seguintes linhas:

```
passwd: compat ldap
group:  compat ldap
shadow: compat ldap
```

Por fim, existe um directório `/etc/pam.d/` que contém um ficheiro referente a cada um dos serviços que irão utilizar autenticação via LDAP. Deverá existir um `/etc/pam.d/login` para permitir autenticação nas máquinas via LDAP, assim como um `ssh,ftp,passwd,wdm,etc.`

O conteúdo destes ficheiros é igual para todos e deverá ser o seguinte:

```
##PAM-1.0
auth required /lib/security/pam_nologin.so
auth sufficient /lib/security/pam_ldap.so
```

```
auth required /lib/security/pam_unix_auth.so try_first_pass
account sufficient /lib/security/pam_ldap.so
account required /lib/security/pam_unix_acct.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_ldap.so
password required /lib/security/pam_unix.so use_first_pass
session required /lib/security/pam_unix_session.so
```

3.1.4 Servidor Cache de LDAP

Para evitar estar sempre a consultar o servidor de LDAP sem necessidade, instalou-se um servidor de cache.

```
apt-get install nscd
```

Este servidor pode ser reiniciado com o seguinte comando:

```
/etc/init.d/nscd restart
```

3.1.5 LDAP via Web

O software escolhido para se poder utilizar o serviço de LDAP através de um browser é o phpLDAPAdmin
Para instalar:

```
wget http://unc.dl.sourceforge.net/sourceforge/phpldapadmin/phpldapadmin-0.9.6c.tar.gz
tar -zxvf phpldapadmin-0.9.6c.tar.gz -C /var/www/ldapadmin/
mv phpldapadmin-0.9.6c ldapadmin
```

Para configurar é apenas necessário editar o ficheiro *config.php.example* e gravá-lo como *config.php* e alterar os seguintes parâmetros:

```
$servers[$i]['host'] = '172.16.2.11';
$servers[$i]['base'] = 'dc=singao,dc=pt';
$servers[$i]['auth_type'] = 'session';
$servers[$i]['login_dn'] = '';
$servers[$i]['login_pass'] = '';
$servers[$i]['auto_uid_number_search_base'] = 'ou=People,dc=singao,dc=pt';
$servers[$i]['auto_uid_number_min'] = 5000;
```

Para que se possa aceder via *www.singao.pt/ldapadmin*, é necessário que o servidor web, com suporte PHP, esteja em funcionamento.

3.2 DNS

3.2.1 Introdução

O DNS (Domain Name Service) é uma base de dados distribuída que relaciona nomes de máquinas com os seus respectivos IPs. Isto significa que através de um nome é possível aceder ao IP correspondente e vice-versa. Ao introduzir uma nova máquina na rede bastará actualizar o servidor DNS para que a máquina seja encontrada pelo seu nome. No nosso trabalho usamos o servidor bind8 (Berkeley Internet Name Daemon).

3.2.2 Instalação do servidor

Para instalar o bind corremos o seguinte comando:

```
apt-get install bind
```

Para configurar o servidor de nomes é necessário modificar o ficheiro `/etc/bind/named.conf` e criar os ficheiros `/etc/bind/db.singao` e `db.singao.rev`.

Após a configuração do servidor é necessário reiniciar o bind com o seguinte comando:

```
/etc/init.d/bind restart
```

Para verificar se os ficheiros de configuração estão bem escritos pode usar, num novo terminal, o comando:

```
tail -f /var/log/syslog
```

3.2.3 Configuração do servidor

Ficheiro `/etc/named.conf`

Este é o ficheiro principal de configuração do nosso servidor de nomes, aqui criamos o nosso domínio, `singao.pt`. É necessário acrescentar as secções `singao.pt` e `2.16.172.in-addr.arpa`, para, respectivamente, resolver nomes e a partir de um IP e encontrar o nome correspondente para um determinado IP.

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you might need to uncomment the query-source
    // directive below. Previous versions of BIND always asked
```

```
// questions using port 53, but BIND 8.1 and later use an unprivileged
// port by default.

// query-source address * port 53;

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

forwarders {
192.168.109.2;
};

// reduce log verbosity on issues outside our control
logging {
category lame-servers { null; };
category cname { null; };
};

//prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
```

```

        type master;
        file "/etc/bind/db.255";
};

// add entries for other zones below here
zone "singao.pt" {
notify no;
type master;
file "/etc/bind/db.singao";
allow-update {
any;
};
};

zone "2.16.172.in-addr.arpa" {
notify no;
type master;
file "/etc/bind/db.singao.rev";
allow-update {
any;
};
};

```

Ficheiro /etc/bind/db.singao

Neste ficheiro mapeamos o nome e os "alias" da máquina ao IP correspondente. O servidor consulta estes dados para resolver um nome, isto é, descobrir para um determinado nome o seu IP correspondente.

```

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions 8.2.1
// and later, *BEFORE* you customize this configuration file.
//

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you might need to uncomment the query-source
    // directive below. Previous versions of BIND always asked
    // questions using port 53, but BIND 8.1 and later use an unprivileged
    // port by default.

```

```
// query-source address * port 53;

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

forwarders {
192.168.109.2;
};
};

// reduce log verbosity on issues outside our control
logging {
category lame-servers { null; };
category cname { null; };
};

//prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

```
// add entries for other zones below here
zone "singao.pt" {
notify no;
type master;
file "/etc/bind/db.singao";
allow-update {
any;
};
};

zone "2.16.172.in-addr.arpa" {
notify no;
type master;
file "/etc/bind/db.singao.rev";
allow-update {
any;
};
};
```

Ficheiro /etc/bind/db.singao.rev

Neste ficheiro mapeamos os IPs ao nome principal da máquina, faz o mapeamento reverso.

```
;BIND DUMP V8
$ORIGIN 16.172.in-addr.arpa.
2 604800 IN NS ns1.singao.pt. ;Cl=5
604800 IN SOA ns1.singao.pt. ferrari.singao.pt. (
200031702 604800 86400 2419200 604800 ) ;Cl=5
$ORIGIN 2.16.172.in-addr.arpa.
14 604800 IN PTR porsche.singao.pt. ;Cl=5
12 604800 IN PTR audi.singao.pt. ;Cl=5
13 604800 IN PTR mercedes.singao.pt. ;Cl=5
11 604800 IN PTR ferrari.singao.pt. ;Cl=5
```

3.2.4 Configuração do cliente

Para obrigar as máquinas clientes a resolver nomes para IP e vice-versa no nosso servidor de nomes é preciso modificar o ficheiro /etc/resolv.conf, esta configuração só é necessária para máquinas que não estejam configuradas para usar DHCP.

```
search singao.pt
nameserver 172.16.2.11
```

nameserver 172.16.2.12

3.3 DHCP

3.3.1 Introdução

O serviço DHCP (Dynamic Host Configuration Protocol) consiste num protocolo de configuração automática de estações IP. Neste trabalho optou-se pela atribuição manual de endereços de máquinas conhecidas, o que significa que atribui um IP fixo a uma máquina que apresente um endereço MAC conhecido. Para máquinas com endereços desconhecidos é usada alocação dinâmica, pois permite reutilizar IPs automaticamente.

3.3.2 Instalação do servidor

O servidor que usamos foi o DHCP2 e é instalado com o seguinte comando:

```
apt-get install dhcp
```

Para monitorar os pedidos e atribuições do servidor de DHCP pode monitorar o log de sistema:

```
tail -f /var/log/syslog
```

3.3.3 Configuração do servidor

Ficheiro /etc/dhcpd.conf

Neste ficheiro estão presentes as configurações para a nossa rede. Os IPs atribuídos de modo dinâmico ficam no intervalo 172.16.2.128 até 172.16.2.253. O endereço 172.16.2.254 já foi atribuído ao router.

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
#ddns-update-style none;

default-lease-time 36000;
max-lease-time 36000;

option subnet-mask 255.255.255.0;
option broadcast-address 172.16.2.255;
option routers 172.16.2.254;
option domain-name-servers 172.16.2.11, 172.16.2.12;
option domain-name "singao.pt";

subnet 172.16.2.0 netmask 255.255.255.0 {
range 172.16.2.128 172.16.2.253;
```

```
default-lease-time 1800;
}

# Fixed IP addresses can also be specified for hosts.  These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.  Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.

#o host ferrari é o servidor de dhcp
host audi {
    hardware ethernet 00:80:C8:E7:E6:46;
    fixed-address 172.16.2.12;
    option host-name "audi.singao.pt";
}

host mercedes {
    hardware ethernet 00:01:02:9F:80:7F;
    fixed-address 172.16.2.13;
    option host-name "mercedes.singao.pt";
}

host porsche {
    hardware ethernet 00:01:02:21:82:5F;
    fixed-address 172.16.2.14;
    option host-name "porsche.singao.pt";
}

host ferrari {
    hardware ethernet 00:C0:DF:05:3B:A9;
    fixed-address 172.16.2.11;
    option host-name "ferrari.singao.pt";
}
```

3.3.4 Instalação do cliente

Para instalar o cliente de DHCP usamos o seguinte comando, embora o cliente venha instalado por omissão:

```
apt-get install dhcp-client
```

Para re-iniciar a carta de rede após a configuração:

```
/etc/init.d/networking restart
```

3.3.5 Configuração do cliente

Ficheiro `/etc/network/interfaces`

Este ficheiro contém todos os dados para configurar o equipamento de rede, no maioria dos casos é so necessário alterar a opção `static` por `dhcp` e eliminar as restantes configurações que dizem respeito à placa de rede por defeito, a `eth0`.

```
#The loopback interface
# Interfaces that comes with Debian Potato does not like to see
# "auto" option before "iface" for the first device specified.
iface lo inet loopback
auto lo

# Device eth0 configured by System Configurator

auto eth0
iface eth0 inet dhcp
# address 172.16.2.12
# netmask 255.255.255.0
# broadcast 172.16.2.255
# network 172.16.2.0
# gateway 172.16.2.254
```

4 Sistema de Ficheiros Distribuido

4.1 NFS

4.1.1 Configuração do Servidor de LDAP

O primeiro passo é configurar correctamente o servidor de LDAP, de modo a permitir a montagem automática das contas. Para tal, é necessário adicionar alguma informação ao LDAP, nomeadamente a entrada do ficheiro `autofs.ldif`.

```
dn: ou=auto.home,dc=singao,dc=pt
ou: auto.home
objectClass: top
objectClass: organizationalUnit
```

Após a criação deste ficheiro, adicionamos esta informação ao servidor com o seguinte comando:

```
ldapadd -c -x -D ''cn=admin,dc=singao,dc=pt'' -W -f autofs.ldif
```

Neste momento, o servidor de LDAP tem uma entrada `auto.home` que irá ser consultada pelos clientes de NFS. Seguidamente, irá ser adicionada uma entrada `cn` por cada utilizador. Esta informação consta do script de criação de novas contas.

4.1.2 Instalação do Servidor

Para instalar o servidor basta correr o comando:

```
apt-get install nfs-kernel-server
```

4.1.3 Configuração do Servidor

De seguida, configura-se o ficheiro `/etc/exports` com a informação dos directórios a serem exportados, com a seguinte informação:

```
/home *.singao.pt(rw, sync)
```

Isto permite exportar o directório `/home` que contém as contas dos utilizadores, com permissões de leitura e de escrita para as máquinas do domínio `singao.pt`.

Após a configuração do servidor, temos de o reiniciar, com o comando:

```
/etc/init.d/nfs-kernel-server restart
```

Neste momento, o servidor de NFS fica correctamente configurado e pronto a funcionar.

4.1.4 Configuração dos clientes

Para configurar o cliente de NFS, é necessário instalar os pacotes do autofs e o respectivo suporte LDAP. Este serviço vai permitir fazer a automontagem das contas. É necessário também instalar o cliente de NFS. Para isto, usam-se os seguintes comandos:

```
apt-get install autofs autofs-ldap
```

```
apt-get install nfs-common
```

De seguida, é necessário comentar as linhas 138 e 139 do ficheiro `/etc/init.d/autofs`. Depois, configuramos o ficheiro `/etc/auto.master`, que vai conter a informação de automontagem. Para que esse ficheiro seja consultado, o ficheiro `/etc/nsswitch.conf` deverá conter a seguinte entrada:

```
automount: files
```

Ficheiro `/etc/auto.master`

```
/home ldap 172.16.1.11:ou=auto.home,dc=singao,dc=pt
```

Neste ficheiro, indicamos que deverá ser consultada a entrada `ou=auto.home` no servidor de LDAP indicado. De seguida, é necessário iniciar o serviço de automontagem através do seguinte comando:

```
/etc/init.d/autofs restart
```

Neste momento temos o cliente de NFS correctamente configurado e a correr.

4.2 Samba

4.2.1 Introdução

Grande parte das estações de trabalho utilizam o sistema operativo Windows, então os utilizadores Windows devem poder aceder aos seus ficheiros tanto em Linux como em Windows. Para este efeito instalou-se um servidor Samba.

4.2.2 Instalação do Servidor

Para instalar o servidor basta correr o comando:

```
apt-get install samba
```

4.2.3 Configuração do servidor

Para configurar o funcionamento do servidor de samba, basta editar o ficheiro `/etc/samba/smb.conf` e o ficheiro `/etc/samba/users.map`

Ficheiro `/etc/samba/smb.conf`

```
# SMB.CONF
# Samba 2.2.x configuration file
# thegoldenear.org

# NOTE: this config file demonstrates how easy Samba is to setup
# for basic file sharing BUT this config isn't optimised so may
# give you problems. It is only a demonstration of the basics of
# Samba file sharing

[global]
workgroup = singao

netbios name = smb.singao.pt

# required for Windows 2000
encrypt passwords = yes

security = share

# required to browse for the share
wins support = yes

# define user mappings between this system and Windows systems.
# without this you get asked for a password even if none is required
```

```
# (users.map would contain something like: root = admin administrator)
username map = /etc/samba/users.map

[homes]
writable = yes
browseable = yes

#[home]
#path = /home
#public = no
#browseable = yes
#writable = yes

# you'll have to do apply the same permissions as the following
# to the directory itself, with 'chmod 777 /shared'
force create mode = 0777
force directory mode = 0777
```

Ficheiro /etc/samba/users.map

```
manel
ricardo
michel
pedro
```

4.2.4 Introduzir utilizadores

Depois da configuração do servidor, é preciso reiniciar o servidor de samba:

```
/usr/sbin/smbd restart
/usr/sbin/nmbd restart
```

Depois de reiniciar o servidor é preciso dizer quais são os utilizadores windows:

```
smbpasswd -w admin
smbpasswd -a root

smbpasswd -a manel
smbpasswd -a rb
smbpasswd -a mdiaz
smbpasswd -a pedro
```

5 Serviço de E-Mail

Na nossa intranet o serviço de email está representado pelo conjunto de um servidor de email primário ("mail.singao.pt"), mais um relay ("ferrari.singao.pt"). As mensagens enviadas para o domínio singao.pt são recebidas em primeiro lugar pelo relay, sendo posteriormente reencaminhadas, para o servidor primário no caso de se verificar que o domínio do destinatário efectivamente pertence à lista de domínios a aceitar.

Em ambos os servidores, optou-se pela utilização do QMAIL, pela sua robustez e porque possui todas as funcionalidades e serviços necessários para os objectivos do nosso trabalho. Para os servidores de IMAP, optou-se pela instalação do courier-imap com suporte LDAP, tornando o processo de configuração dos mecanismos de autenticação quase transparente. Para o servidor POP, optou-se pelo courier-pop, pela sua facilidade de instalação.

Como informação adicional podemos referir que os maiores sítios de emails como, Yahoo, Hotmail e outros utilizam o QMAIL como servidor de correio.

5.1 Servidor de SMTP

Como primeiro passo, fazemos:

```
apt-get remove exim -purge
```

Para garantir que não ocorrem conflitos com outras instalações de serviços de email já existentes.

Garantida a inexistência de conflitos, passamos à compilação e instalação das sources necessárias.

```
apt-get install qmail-src ucspi-tcp-src daemontools-installer
```

A compilação das sources daemontools e ucspi-tcp realiza-se facilmente com:

```
build-daemontools build-ucspi-tcp
```

Agora para compilar o QMAIL, executamos:

```
build-qmail
```

A instalação deve ser suspensa aquando do início da compilação, acedendo-se de seguida ao directorio onde a source se encontra temporariamente, através de outra shell. É necessario editar o ficheiro extra.h modificando os valores das variáveis QUEUE_EXTRA para "Tlogs" e QUEUE_EXTRALEN para 6. Estas alterações devem garantir que o utilizador "logs" recebe uma cópia de todas as mensagens enviadas pelo servidor. Pode prosseguir normalmente o build-qmail.

O passo seguinte envolve indicar ao servidor quais os domínios com que deve lidar para isso fazemos.

```
echo singao.pt > /var/qmail/control/rcpthosts
echo singao.pt > /var/qmail/control/locals
echo singao.pt > /var/qmail/control/me
```

Verificar que /var/qmail/control/rcpthosts deve conter os domínios de que o servidor deve aceitar mensagens neste caso de singao.pt, muito embora essa filtragem já deva ter sido efectuada pelo RELAY. Por outro lado

`/var/qmail/control/me` deve conter o domínio do próprio servidor de email.

Para garantir que o servidor SMTP é inicializado no arranque no qmail, torna-se necessário alterar o ficheiro `qmail` em `/etc/init.d/` de modo a que inclua as seguintes entradas:

```
sh -c "start-stop-daemon -start -quiet -user root
-exec /usr/bin/tcpserver -
-x /etc/qmqp.cdb -u 'id -u qmaild' -g 'id -g nobody' 0 628
/usr/sbin/qmail-qmqpd &"
```

Caso a instalação tenha sido concluída com sucesso, basta ultimar os pormenores de monitorização do correio transferido. Para esse efeito, basta criar um filtro com o `procmail` e colocá-lo em `/home/logs/.procmailrc`. O filtro consiste nas seguintes linhas:

```
SHELL = /bin/sh
LINEBUF=4096
HOME=/home/logs
PATH=HOME/bin : /bin/ : usr/bin/ : /usr/local/bin : /sbin : /usr/sbin :

VERBOSE=off
MAILDIR=HOME/Maildir/
DEFAULT=MAILDIR
LOGFILE=HOME/logfile
FORMAIL=/usr/bin/formail
SENDMAIL=/usr/sbin/sendmail

:0
* ^TO_singao.pt
HOME/Maildir/.outbound/
```

As subdirectorias `.inbound` e `.outbound` devem ser criadas com o comando `maildirmake`.

O último passo a executar é adicionar os utilizadores, de modo a estarem ligados ao LDAP, os comandos a executar são:

```
vi /var/qmail/users/assign
```

Adicionar ao ficheiro `assign` os utilizadores da forma:

```
=address:user:uid:gid:directory:dash:extension:
```

Onde `address` é o endereço onde está a conta, `user` é o utilizador criado, `uid` é o user id atribuído no LDAP ao utilizador, `gid` é o id do grupo atribuído no LDAP ao utilizador, e `directory` o directorio onde seram entregues os emails. Desta forma adiciona-se todos os utilizadores incluindo o "logs". O conteúdo do ficheiro seria:

```
=rb:rb:5001:1002:/home/Maildir:::
=mdiaz:mdiaz:5002:1002:/home/Maildir:::
```

```
=manel:manel:5003:1002:/home/Maildir:::
=pedro:pedro:5004:1002:/home/Maildir:::
=logs:logs:5005:1002:/home/Maildir:::
.
```

E com estes procedimentos se conclui a instalação do servidor SMTP (qmail).

Para verificar se está correctamente instalado podemos fazer o teste de envio de um email com os seguintes comandos:

```
telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 singao.pt ESMTTP
mail from: rb@singao.pt
rcpthost to: mdiaz@singao.pt
data
Isto é um teste, só um teste singao!!!!!!
.
quit
```

Para ver se foi enviado correctamente, fazemos login numa das maquinas da nossa intranet com o utilizador mdiaz e na pasta /Maildir/new deve aparecer o email enviado, pode-se utilizar o vi para ver o email.

5.2 IMAP

A instalação do servidor imap é bastante fácil, consistindo apenas na instalação e compilação da source. A unica coisa que pode trazer dificuldade é a necessidade de efectuar algumas pequenas configurações de modo a garantir que a autenticação de utilizador se processe de acordo com a informação no servidor LDAP. Assim, executa-se um conjunto de comandos:

```
apt-get install courier-imap courier-ldap
```

Instalado o courier-imap com suporte LDAP, resta proceder à sua configuração. Esta implica modificar o conteúdo de vários ficheiros, sendo que o primeiro, /etc/courier/authdaemonrc, indica qual o tipo de autenticação que o daemon deve utilizar (LDAP). No caso particular, basta alterar a variável authmodulelist para authldap.

Por sua vez, /etc/courier/authldaprc contém informação acerca de como fazer as pesquisas para autenticação, bem como de onde localizar os directórios onde as mensagens devem ser armazenadas. É necessário alterar um conjunto de campos, cuja lista é apresentada de seguida:

```
LDAP_SERVER ldap
LDAP_PORT 389
LDAP_BASEDN dc=singao, dc=pt
```

```
LDAP_BINDPW admin
LDAP_MAIL mail
LDAP_DOMAIN singao.pt
LDAP_HOMEDIR homeDirectory
LDAP_MAILDIR mailDir
LDAP_FULLNAME cn
LDAP_CRYPTPW userPassword
LDAP_UID uidNumber
LDAP_GID gidNumber
```

O ficheiro `/etc/courier/imapd` contém as configurações do servidor IMAP, de entre as quais é necessário alterar a indicação do ip deste. Para esse efeito, torna-se necessário alterar a variável `ADDRESS` para o valor `172.16.2.13`

Também no ficheiro `/etc/pam.d/imap` contém informação acerca do modo de autenticação adoptado pelo IMAP, e deve ter o conteúdo explicado no capítulo de Configuração do Cliente LDAP.

Com isto a instalação do servidor IMAP fica concluída, só resta testar da seguinte maneira:

```
telnet localhost 143
Trying...
Connected to singao.pt
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE
      THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE
      ACL ACL2=UNION] Courier-IMAP ready.
AB login teu_login tua_password
AB OK LOGIN OK.
AB logout
```

5.3 POP

A instalação do servidor POP3 é ainda mais simples que o do IMAP, já que apenas requer uma pequena alteração no que toca ao modo de autenticação (mais uma vez, recorre-se ao servidor LDAP).

O primeiro comando a executar:

```
apt-get install courier-pop
```

À semelhança do que sucede no servidor IMAP, `/etc/pam.d/pop3` contém informação acerca do modo de autenticação adoptado pelo POP, e deve ter o conteúdo explicado no capítulo de Configuração do Cliente LDAP.

5.4 SMTP no Relay

Basta a instalação básica do QMAIL neste servidor conjuntamente com as configurações necessárias ao redireccionamento para o servidor primário.

Procede-se à remoção de outras instalações locais de serviços de SMTP

```
apt-get remove exim --purge
```

De seguida, realiza-se a instalação do qmail, seguindo os passos por defeito.

```
apt-get install qmail-src ucspi-tcp-src daemontools-installer
build-daemontools
build-ucspi-tcp
build-qmail
```

Para garantir o redireccionamento das mensagens, basta no ficheiro `/var/qmail/control/qmqpservers` colocar a localização (ip) do servidor primário, para onde os emails devem ser reenviados (por SMTP). Por seu turno, `/var/qmail/control/me` deverá dispor de uma referência à identidade da máquina de Relay. Finalmente, `/var/qmail/control/rcpthosts` deve armazenar informação acerca do conjunto de domínios aceites pelo servidor.

```
echo 172.16.2.11 >> /var/qmail/control/qmqpservers
echo ferrari >> /var/qmail/control/me
echo singao.pt >> /var/qmail/control/rcpthosts
```

Adicionalmente, à semelhança do que sucede com o servidor primário, o ficheiro `/etc/init.d/qmail` deve ser modificado por forma a garantir a inicialização do cliente qmqp quando o arranque do servidor QMAIL. Para esse efeito, é necessário incluir a seguinte linha de comandos nesse ficheiro:

```
sh -c "start-stop-daemon -start -quiet -user root
-exec /usr/bin/tcpserver -
-x /etc/qmqp.cdb -u 'id -u qmaild' -g 'id -g nobody' 0 628
/usr/sbin/qmail-qmqpd &"
```

Com isto fica concluída a instalação do servidor Relay para o email.

5.5 IMP

A aplicação de Webmail escolhida foi o IMP, que corre na *framework* Horde. Para tal, executamos o comando:

```
apt-get install imp4
```

Este comando procede à instalação dos pacotes necessários, nomeadamente os de PHP, PEAR, PHPLDAP, PHPIMAP e HORDE3. Deste modo, apenas foi preciso configurar os scripts quer do Horde quer do IMP. Devido à extensão dos scripts, iremos apenas salientar os pontos principais da configuração.

O primeiro passo foi a autenticação por LDAP. Para tal, escolhemos como autenticação LDAP, indicando o servidor e os dados de acesso. Após este passo, podemos indicar no IMP o servidor de IMAP ao qual queremos aceder. Esta informação encontra-se no ficheiro `servers.php`

Ficheiro `servers.php`

```
$servers['imap'] = array(
    'name' => 'IMAP Server',
    'server' => 'mail.singao.pt',
    'hordeauth' => true,
    'protocol' => 'imap',
    'port' => 143,
    'folders' => '',
    'namespace' => 'INBOX.',
    'maildomain' => 'singao.pt',
    'smtp host' => 'mail.singao.pt',
    'smtp port' => 25,
    'quota' => 'courier',
    'realm' => '',
    'preferred' => '',
    'dotfiles' => false,
    'hierarchies' => array()
);
```

É de realçar a linha `'hordeauth' => true`. Deste modo, o utilizador não precisa de se autenticar novamente para aceder ao seu e-mail.

As restantes configurações (e activação das várias aplicações instaladas sobre a plataforma Horde) podem ser feitas na interface online da aplicação, pelo que não terá interesse reproduzir aqui *screenshots* sucessivas de parâmetros de fácil compreensão.

Introduzimos os scripts fornecidos pelo Horde na base de dados com o comando:

```
mysql -u root -p scripts/sql/create_mysql.sql
```

Neste momento, a aplicação fica completamente configurada.

6 Serviços Web

6.1 HTTP

O servidor web usado foi o apache. Adicionalmente foi instalado o módulo de PHP bem como uma pequena base de dados MySQL. Para instalar o servidor executa-se o seguinte comando:

```
apt-get install apache
```

A configuração e personalização do servidor apache pode ser feita em */etc/apache/httpd.conf*. No fim das alterações e para que estas entrem em funcionamento é necessário reiniciar o servidor com o seguinte comando:

```
/etc/init.d/apache restart
```

6.1.1 PHP e Base de dados

Para exemplificar o uso de base de dados e o seu acesso a partir de páginas web dinamicas foram instalados os seguintes pacotes:

```
apt-get install php4 php4-ldap php4-imap php4-mysql
apt-get install mysql-server
```

Para o apache reconhecer o módulo de PHP é necessário adicionar em *httpd.conf* a seguinte linha:

```
LoadModule php4_module /usr/lib/apache/1.3/libphp4.so
```

Em seguida foi criado o ficheiro *bd.sql* com o seguinte conteúdo da base de dados :

```
CREATE DATABASE esumsingao;
USE esumsingao;
CREATE TABLE alunos (nome VARCHAR(50), email VARCHAR(50));
INSERT INTO alunos VALUES ("Ricardo Batista", "ei00132@fe.up.pt");
INSERT INTO alunos VALUES ("Manel Maia", "ei00128@fe.up.pt");
INSERT INTO alunos VALUES ("Michel Diaz", "ei04101@fe.up.pt");
INSERT INTO alunos VALUES ("Pedro Sampaio", "ei00118@fe.up.pt");
```

Para adicionar a base de dados executa-se os seguintes comandos:

```
/etc/init.d/mysql start
mysql -u root < bd.sql
```

O ficheiro PHP para acesso a base de dados tem o seguinte código:

```
<? $ligacao = mysql_connect("localhost", "root")
```

```

or die("Erro ao tentar ligar ao mysql: " . mysql_error());
echo "Efectuada ligacao ao mysql<br>";
mysql_select_db("esumsingao")
or die("Erro ao selecciona BD: " . mysql_error());
echo "Efectuada ligacao a BD<br>";
$string_sql = "SELECT * FROM alunos";
echo "<br>Grupo Singao.pt :<br>";
$resultado = mysql_query($string_sql)
or die ("Erro na query<br>");
$num_linhas = mysql_num_rows($resultado);
if ($num_linhas > 0)
{
    $i = 0;
    while ($linha[$i] = mysql_fetch_array($resultado))
    {
        echo "<br> - <br>Nome:" . $linha[$i] ['nome'] .
        "<br>Email:" . $linha[$i]['email'];
        $i++;
    }
}
mysql_close($ligacao);
?>

```

Este ficheiro é guardado em `/var/www/paginaph/index.php` e pode ser acedido directamente em `www.singao.pt/paginaph` ou através dum link colocado na página principal em `www.singao.pt`.

6.1.2 Acesso controlador por PAM

Para controlar páginas com acesso restrito foi utilizado o módulo de autenticação PAM.

```
apt-get install libapache-mod-auth-pam
```

Para activar este módulo é necessario inserir a seguinte linha no ficheiro de configuração "`httpd.conf`" do apache.

```
LoadModule pam_auth_module /usr/lib/apache/1.3/mod_auth.pam.so
```

Para usar autenticação num determinado directório, basta apenas criar um ficheiro `.htaccess` dentro do mesmo e adicionar o seguinte conteúdo:

```
AuthName " Area Reservada"
AuthType Basic
require valid-user
```

É ainda necessário configurar o apache para permitir o uso de regras de acesso locais. Para isso basta editar o ficheiro *httpd.conf* de forma a ficar com o seguinte conteúdo:

```
<Directory /home/*/public_html>
AllowOverride All
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
</Directory>
```

Após isto é necessário inserir no directório */etc/pam.d* um ficheiro *httpd*, cujo conteúdo é igual aos outros ficheiros de configuração PAM, e que se encontram explicados na secção do serviço LDAP.

6.1.3 Domínios Virtuais

Para configurar domínios virtuais basta editar o ficheiro *httpd.conf*. Foram criados como exemplo domínios virtuais para a página principal, webmail e página do *phpldapadmin*. Para que os domínios virtuais funcionem é necessário também serem acrescentados no servidor DNS com referência à máquina do servidor web. As alterações efectuadas foram as seguintes:

```
#Dominio virtual que representa o site base
<VirtualHost 172.16.2.12>
DocumentRoot /var/www
ServerName www.singao.pt
ServerAlias www
CustomLog /var/log/apache/www-access.log
</VirtualHost>

#Dominio virtual que representa o site do webmail
<VirtualHost 172.16.2.12>
DocumentRoot /var/www/horde/imp
ServerName webmail.singao.pt
ServerAlias webmail
CustomLog /var/log/apache/webmail-access.log
</VirtualHost>

#Dominio virtual que representa o site do ldapadmin
<VirtualHost 172.16.2.12>
DocumentRoot /var/www/ldapadmin
ServerName ldapadmin.singao.pt
ServerAlias ldapadmin
CustomLog /var/log/apache/ldapadmin-access.log
</VirtualHost>
```

Para que as alterações entrem em funcionamento é necessário fazer restart ao servidor apache. Pode ser feito com o seguinte comando: `/etc/init.d/apache restart`

6.2 Proxy

Para implementar o proxy para acesso ao exterior (Internet), que permita controlar os débitos dos utilizadores e o acesso restrito sujeito a autenticação por LDAP foi usada a aplicação Squid.

Para instalar basta executar o seguinte comando:

```
apt-get install squid
```

Para configurar o squid deverão ser realizadas no ficheiro */etc/squid.conf* as seguintes alterações:

```
http_port 3128
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
authenticate_program /usr/lib/squid/ldap_auth.sh

acl LDAP_AUTH proxy_auth REQUIRED

delay_pools 1
delay_class 1 2
delay_parameters 1 100000/200000 10000/
delay_access 1 allow LDAP_AUTH
delay_access 1 deny all

http_access allow LDAP_AUTH
```

É ainda necessário colocar na directoria */usr/lib/squid/* o script *ldap_auth.sh* com o seguinte conteúdo:

```
#!/bin/sh
exec /usr/lib/squid/ldap_auth -b "ou=People,dc=singao,dc=pt" 172.16.2.11
```

Devem ser dadas as permissões necessárias ao script.

```
chmod 755 /usr/lib/squid/ldap_auth.sh
```

No fim das configurações deve-se reiniciar o servidor para que as alterações entrem em funcionamento:

```
/etc/init.d/squid restart
```

Para se usar o proxy deve-se configurar os browsers com o seguinte endereço

```
"http://proxy.singao.pt:3128"
```

Na linha de comandos pode ser feito da seguinte maneira:

```
export http_proxy=http://proxy.singao.pt:3128
```

Para testar pode ser recorrer ao browser Lynx:

```
lynx www.singao.pt
```

6.3 Estatísticas

Para obter uma série de estatísticas de forma amigável, relativamente aos acessos aos serviços web foi instalado o webalizer.

```
apt-get install webalizer
```

Para que este analise o log gerado pelo Squid (/var/log/squid/access.log) deve-se configurar o webalizer alterando o ficheiro /etc/webalizer.conf e colocando-o no directório /var/www/stats/www/ onde irá ser colocado também a página html de estatística gerada pelo webalizer.

As alterações a fazer no ficheiro webalizer.conf são as seguintes:

```
LogFile /var/log/apache/access.log
OutputDir /var/www/stats/www
ReportTitle Estatísticas do servidor
HostName www.singao.pt
```

Para gerar as estatísticas do proxy deve se fazer uma cópia do ficheiro /var/www/stats/www/webalizer.conf para /var/www/stats/proxy e modificar para o seguinte:

```
LogFile /var/log/squid/access.log
OutputDir /var/www/stats/proxy
ReportTitle Estatísticas do servidor
HostName proxy.singao.pt
```

Para que as estatísticas sejam criadas e actualizadas automaticamente deve -se adicionar as seguintes linhas ao ficheiro /etc/crontab :

```
0-59/5 * * * * root webalizer -c /etc/squid.webalizer.conf
0-59/5 * * * * root webalizer -c /etc/webalizer.conf
```

Neste caso as estatísticas são actualizadas a cada 5 minutos, mas o tempo de intervalo pode ser modificado.

7 Criação de novas contas

Para adicionar um novo utilizador, criámos dois. O script `adduser` adiciona o utilizador ao LDAP e invoca um outro script `createdirs` no servidor de NFS.

Ficheiro `adduser.sh`

```
#!/bin/bash

if test $# -lt 3
then
    echo "Utilização:\n\t $0 username 'Nome do Utilizador' password"
    exit 1
fi

# VARS
contas="/home"
#profiles="/var/samba/profiles"

userid=$1
nome=$2
password=$3

home_dir=$contas/$userid
#profiles_dir=$profiles/$userid
templdif=`tempfile`

#procurar o prox UID livre, ignorar user nobody=>uidNumber=65534
let UID1=`ldapsearch -x '(& (objectClass=posixAccount) (! (uidNumber=65534)))'\
| grep uidNumber | cut -b 12- | sort -g | tail -n 1 `+1

GID1=1527
group="singao"

# LDAP
echo "dn: uid=$userid,ou=People,dc=singao,dc=pt" > $templdif
echo "cn: $nome" >> $templdif
echo "gidNumber: $GID1" >> $templdif
echo "homeDirectory: $home_dir" >> $templdif
echo "uid: $userid" >> $templdif
echo "uidNumber: $UID1" >> $templdif

echo "loginShell: /bin/bash" >> $templdif
echo "userPassword: $password" >> $templdif

#echo "mail: $userid@singao.pt" >> $templdif
```

```

#echo "sn: $userid" >> $templdif

echo "objectClass: account" >> $templdif
echo "objectClass: posixAccount" >> $templdif
echo "objectClass: top" >> $templdif
echo "objectClass: shadowAccount" >> $templdif

echo >> $templdif

echo "A inserir $userid na base de dados LDAP..."
ldapadd -c -x -D "cn=admin,dc=singao,dc=pt" -W -f $templdif || exit 1

echo "dn: cn=$userid,ou=auto.home,dc=singao,dc=pt" > $templdif
echo "objectClass: automount" >> $templdif
echo "automountInformation: -rw,hard,intr 172.16.2.14:$home_dir" >> $templdif
echo "cn: $userid" >> $templdif

echo >> $templdif

echo "A criar auto.home..."
ldapadd -c -x -D "cn=admin,dc=singao,dc=pt" -W -f $templdif || exit 1

echo "Adicionado ao LDAP..."

# SAMBA
/usr/local/samba3/bin/smbpasswd -a $userid $password

echo "A criar directoria no servidor NFS..."
rsh -l root porsche /root/adduser $userid $GID1

rm -f $templdif
echo "Pronto..."

```

Ficheiro createdirs.sh

```

username=$1
group=$2

home_dir=/home/$username

mkdir $home_dir
chmod 755 $home_dir
mkdir $home_dir/public_html
chmod 701 $home_dir/public_html

```

```
mkdir $home_dir/Maildir
mkdir $home_dir/Maildir/cur
mkdir $home_dir/Maildir/new
mkdir $home_dir/Maildir/tmp
echo "./Maildir/" > $home_dir/.qmail

chown -R $username:$group $home_dir
```

8 Conclusão

A elaboração deste trabalho foi uma experiência bastante interessante, evidenciamos as potencialidades do sistema operativo Linux para prestar serviços de rede numa intranet. Solidificamos conhecimentos de Linux e ficamos a conhecer o que está por detrás de uma Intranet e o seu funcionamento.

Para muitos de nós tratou-se de uma experiência completamente diferente daquelas por que já passamos, revelou-se um projecto complexo devido à integração de todos os serviços, é um trabalho que pelos seus requisitos poderá ser semelhante a um projecto real num futuro próximo.

Concluimos que é possível, de uma forma económica, fazer uma rede completa, profissional, estável e segura com um sistema operativo que é completamente livre, grátis e com enormes potencialidades.

Referências

- [1] Lamport, L., *LaTeX : A Documentation Preparation System User's Guide and Reference Manual*, Addison-Wesley Pub Co., 2nd edition, August 1994.
- [2] Vidal, R., *Acetatos das aulas teóricas*, 2004-2005.
- [3] Life With Qmail, <http://www.lifewithqmail.com/>
- [4] LDAP HowTo, <http://www.tldp.org/HOWTO/LDAP-HOWTO/>
- [5] Squid FAQ, <http://www.squid-cache.org/Doc/FAQ/FAQ.html>