Yararlı LINUX Sunucu ve Servis Yazılımları

13

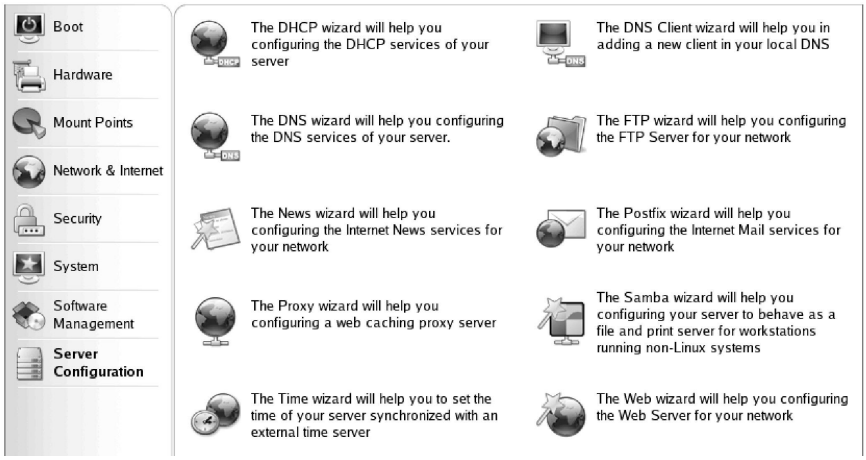
- **Yararlı LINUX Sunucu Yazılımları**
  - **`ftp` Sunucusu**
  - **`apache` Web Wunucusu**
  - **`postfix` e-Posta Sunucusu**
  - **`procmail`**
  - **`samba` Sunucusu**
  - **`named` (DNS) Sunucusu**
  - **`ssh` Sunucusu (Secure Shell)**
  - **NIS Sunucusu (Network Information Services)**
  - **`iptables` Ateş Duvarı**
  - **DHCP Sunucusu**
  - **MySQL ve PostgreSQL Veritabanı Sunucuları**
  - **`squid` Proxy Sunucusu**
  - **`ppp` Çevirmeli Ağ Sunucusu**

Mandrake LINUX'un, çeşitli sunucu yazılımlarını denetlemeyi kolaylaştıran "**Server Configuratio**n" isimli bir GUI (Graphical User Interface : Grafik Kullanıcı Arabirimi) aracı vardır; ancak bu araç siz özellikle kurmadıkça "Mandrake Control Center" menüsünde yer almaz. Her ne kadar bu bölümde "Server Configuration" yazılımının kullanımını anlatmayacaksak da, şimdi bu yazılımı yüklemenizde yarar var.

"**Server Configuration**", Mandrake dağıtım CD'lerinizin ilkinde yer almaktadır. Yazılımı yüklemek için birinci CD'yi takıp

```
rpm -ivh /mnt/cdrom/RPMS/drakwizard-1.8-1mdk.noarch.rpm
```

komutunu verin. "Server Configuration" yazılımı kurulacak ve bundan sonra Mandrake Control Center yazılımını çalıştırdığınızda seçenekler arasında görünecektir:



Artık bu yeni araçla oynayıp yeteneklerini keşfetmek size düşüyor. Biz, önemli sunucu yazılımlarına ve bunlarla neler yapabileceğinize dönelim.

Yararlı LINUX Sunucu Yazılımları

Mandrake ve diğer tüm LINUX dağıtımları içinde son derece güçlü, yetenekli bir çok sunucu yazılımı yer almaktadır. Bunların neredeyse herbiri birer kitap yazılmasını gerektirecek kadar kapsamlı yazılımlar olduğu için burada yalnızca işlevleri hakkında kaba bilgi vermekle yetineceğiz. LINUX'unuzla yapmak istediğiniz işler için yararlı olacak yazılımları ayrıca çalışmanız ve öğrenmeniz gerekecektir. Standart kurulumlarda, burada sözünü ettiğimiz sunucu yazılımların hepsi kurulmaz; bazılarını ayrıca özel olarak kurmanız gerekecektir. Bu sunucu yazılımların çoğunun ayarları **webmin** ile yapılabilmektedir.

ftp Sunucusu

"File Transfer Protocol", Internet protokolleri arasında en önemlilerinden; daha doğrusu en çok kullanılanlarından birisidir. TCP/IP ağlarda (bir başka deyişle: İnternet'te) bilgisayarlar arası dosya transferinde kullanılır. Uygun FTP istemci programlarıyla (**ncftp**, **gftp** gibi) bir FTP sunucusu ile yetkileriniz doğrultusunda iki yönlü dosya transferi yapabilirsiniz.

Bilgisayarınızda **proftpd** sunucu yazılımı çalışıyorsa FTP istemcileri size dosya gönderebilir, sizden dosya çekebilir. Sizin bilgisayarınızda hesabı olan

kullanıcılar bir FTP istemci yazılımıyla sisteminize bağlandıklarında, kendi kullanıcı yetkileri çerçevesinde dosya çekip gönderebilirler. Eğer bilgisayarınızda hesabı olmayan kullanıcıların da bilgisayarınızdan dosya çekip göndermelerine izin vermek istiyorsanız "**anonymous**" (kimliği belirsiz) kullanıcıların erişimine izin vermeniz gerekir.

FTP sunucunuzu bir "anon ftp sunucusu" olarak kurmak istiyorsanız **/etc/proftpd.conf** konfigürasyon dosyasını aşağıdaki gibi düzenleyip "**/etc/rc.d/init.d/proftpd restart**" komutuyla FTP sunucu yazılımını durdurup tekrar başlatmalısınız.

```
ServerName                  "Benim Sunucum"
ServerType                  standalone
DefaultServer               on
Port                        21
Umask                       022
MaxInstances                30
User                        nobody
Group                       nogroup
<Directory /*>
 AllowOverwrite             on
</Directory>
<Anonymous ~ftp>
 User                       ftp
 Group                      ftp
 UserAlias                  anonymous ftp
 MaxClients                 10
 DisplayLogin               welcome.msg
 DisplayFirstChdir      .message
 <Limit WRITE>
  DenyAll
 </Limit>
</Anonymous>
```

Bu arada bir hatırlatma yapmadan geçemeyeceğiz: Eğer FTP sunucu yazılımınız olan **proftpd** daemon'u sisteminiz açıldığında otomatik olarak çalıştırılmıyorsa

"**chkconfig proftpd on**" komutuyla bu sorunu halledebilirsiniz.

Bundan sonra yapmanız gereken küçük bir iş daha var: **/etc/passwd** dosyasına bakarsanız burada "**ftp**" diye bir kullanıcının tanımlı olduğunu fakat bu kullanıcının kabuk programının "**/bin/false**" olduğunu göreceksiniz. "**/bin/false**" aslında bir kabuk değildir; başlatıldığında hemen duran bir programdır. Genellikle kullanıcıların sisteme telnet ve ssh istemcileriyle bağlanmalarını önlemek için kullanılır.

"ftp" isimli kullanıcının sisteminize bağlanmasını istemeyeceğiniz; ama ftp ile dosya alıp vermesine izin vermek isteyeceğiniz için **/etc/passwd** dosyasındaki kabuk tanımını değiştirmeden **/etc/shells** dosyasında **/bin/false**'un kabul edilebilir bir kabuk olduğunu belirtmelisiniz. Bu işi vi ile **/etc/shells** dosyasına, içinde "**/bin/false**" olan bir satır ekleyerek yapabilirsiniz. (Bakın! Sonra uyarmadılar demeyin... vi öğrenmeden olmaz!)

apache Web Sunucusu

Dünyanın en iyi, en gelişmiş, en güvenli ve en yetenekli web sunucusu Apache'dir. Bu yalnızca bizim fikrimiz değil. *survey.netcraft.com* adresine bir göz atarsanız dünyadaki web sunucularının yüzde yetmişe yakın bir bölümünün Apache ile servis verdiğini göreceksiniz. MS-IIS'de fena değil aslında ama bir de güvenlik ve performans sorunları olmasa... IIS, yalnızca web uygulamalarını ASP ile yazmakta ısrar edenler için anlamlı. Ehh.. kendileri bilir. (Gene sataşmadan duramadık.)

Apache web sunucusu, kendinden önceki web sunucu yazılımlarına saygıdan olsa gerek "**httpd**" (hyper text transfer protocol daemon) adıyla kaydedilmiş bir program dosyasıyla çalışır. Bu nedenle sisteminizde çalışmakta olan süreçlerin listesini aldığınızda, içinde "**apache**" geçen bir süreç göremezsiniz. Apache sunucunuz çalışırken

```
ps ax | grep httpd
```

komutunu verirseniz birden fazla **httpd** süreci çalıştığını göreceksiniz. Bu normaldir. Apache sunucusu, başlatıldığında, gelebilecek web isteklerini ayrı ayrı süreçlerle karşılayabilmek için kendisinin bir kaç kopyasını birden başlatır. Web istekleri artarsa, gerektiği kadar kendi kopyasını başlatır (UNIX dünyasında bu kavrama "spawning" denir). Süreç numarası en küçük olan **httpd** sürecini öldürürseniz, tüm **httpd** süreçleri ölür ve bilgisayarınız artık web servisi vermez.

Bilgisayarınızdan web servisini başlatmak için sabırsızlanıyorsanız **/var/www/html** dizinine uygun bir **index.html** dosyası yerleştirerek hemen yayına başlayabilirsiniz. Web sitenizle ilgili tüm html dosyaları bu dizinde yer almalıdır. **CGI** (**C**ommon **G**ateway **I**nterface), yani web uygulama yazılımlarınız varsa onları da **/var/www/cgi-bin** dizinine yerleştirebilirsiniz.

Apache, hakkında bunun gibi bir kitap daha yazılması gereken bir yazılımdır. Ayarları oldukça karmaşık olabilmektedir. Ancak, basit bir web servisi için hiçbir ayar değiştirmenize gerek olmayacaktır. Merak ediyorsanız, Apache'nin ayar dosyalarını **/etc/httpd/conf** altında bulabilirsiniz.

Apache web sunucusunu durdurma, yeniden başlatma gibi işlemleri **/usr/sbin/apachectl** komutuyla yapmak daha doğrudur. Örneğin web sunucunuzun ayarlarında bir değişiklik yaptığınızda

```
/usr/sbin/apachectl restart
```

komutuyla programın yeni ayarlarla tekrar başlatılmasını sağlayabilirsiniz. Durdurmak için

```
/usr/sbin/apachectl stop
```

Güvenli iletişim yetenekleriyle (Secure Socket Layer) başlatmak istediğinizde ise

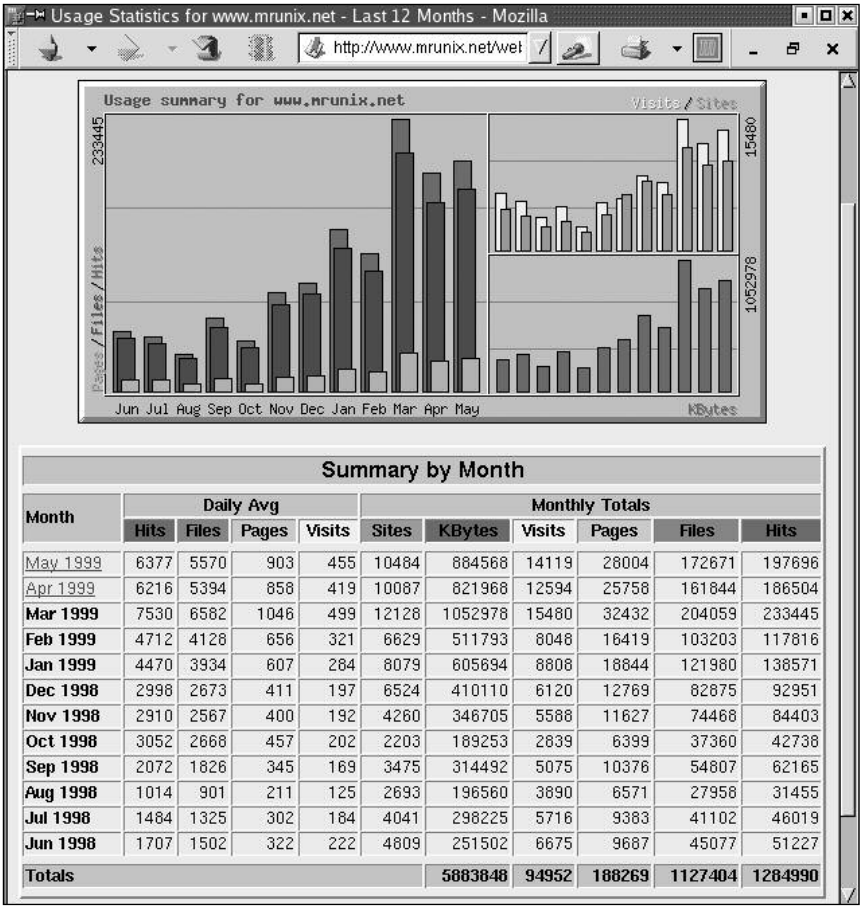
```
/usr/sbin/apachectl startssl
```

komutlarını kullanabilirsiniz.

Kullanıcılarınız, kendi kişisel web sitelerini yayınlamak isterlerse, kendi kişisel dizinlerinde "**public_html**" dizini yaratıp, altına kendi web sitelerine ilişkin dosyaları yerleştirirlerse, Apache sunucunuz bu sayfaları "**http://www.abc.com.tr/~kullanici**" adresinden yayınlayacaktır.

Apache'nin yetenekleri arasında "sanal web sunucusu" hizmeti de vardır. Bir bilgisayarla birçok web sitesinin yayınını yapabilirsiniz. **/etc/httpd/conf/vhosts/Vhosts.conf** ayar dosyasında yapacağınız değişikliklerle bilgisayarınıza **http://www.abc.com.tr** adresiyle ile gelen isteklere ayrı; **http://www.xyz.org.tr** adresiyle gelenlere ayrı web siteleri sunabilirsiniz.

Web sitelerinin başarısı ziyaretçi sayısıyla ölçülür. Apache web sunucusu, sunduğu sayfaları kime ve ne zaman sunduğunu kaydeder. Apache log dosyalarını **/var/log/httpd/access.log** isimli dosyada bulabilirsiniz. Gözle izlenmesi olanaksız olan bu log dosyasının analizi ve görsel raporlar elde etmek için **webalizer** yazılımını kullanmanızı öneririz.



Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
May 1999	6377	5570	903	455	10484	884568	14119	28004	172671	197696
Apr 1999	6216	5394	858	419	10087	821968	12594	25758	161844	186504
Mar 1999	7530	6582	1046	499	12128	1052978	15480	32432	204059	233445
Feb 1999	4712	4128	656	321	6629	511793	8048	16419	103203	117816
Jan 1999	4470	3934	607	284	8079	605694	8808	18844	121980	138571
Dec 1998	2998	2673	411	197	6524	410110	6120	12769	82875	92951
Nov 1998	2910	2567	400	192	4260	346705	5588	11627	74468	84403
Oct 1998	3052	2668	457	202	2203	189253	2839	6399	37360	42738
Sep 1998	2072	1826	345	169	3475	314492	5075	10376	54807	62165
Aug 1998	1014	901	211	125	2693	196560	3890	6571	27958	31455
Jul 1998	1484	1325	302	184	4041	298225	5716	9383	41102	46019
Jun 1998	1707	1502	322	222	4809	251502	6675	9687	45077	51227
Totals						**5883848**	**94952**	**188269**	**1127404**	**1284990**

Web tabanlı uygulama programlarında çok yaygın olarak kullanılan PHP programlama dili desteği Apache ile birlikte kurulmaktadır. Geliştireceğiniz web uygulamalarının her türlü bilgisayar donanım ve işletim sistemi platformunda çalışabilmesini istiyorsanız; hele yüksek performans istiyorsanız; hele hele web ziyaretçilerinizin her gelişlerinde sitenizden yararlanabilmelerini istiyorsanız PHP öğrenmenizi ve kullanmanızı öneririz. Tamam, tamam biliyoruz... Web uygulamaları ASP ile de geliştirilmekte, hem de çok yaygın

olarak; ama biz profesyonel iş yapacak olan yazılımcılara sesleniyoruz.
Bu arada web uygulamalarında tartışmasız üstünlüğü olan bir betik dili olan Perl programlama dilinin de LINUX dağıtımınızla birlikte standart olarak kuruluduğunu belirtmeliyiz. Uygulamalarınızda ister PHP, ister Perl, ister C, ister Python, ister bir başka dil/araç ya da karışımını kullanın; artık o sizin bileceğiniz iş.

`postfix` e-Posta Sunucusu

e-Posta servisi olmayan İnternet sunucusu olur mu? Olmaz tabii. Aslında olur! Windows tabanlı İnternet servislerinde genellikle web servisi için ayrı; e-posta sunum hizmetleri için ayrı bilgisayar kullanılmak zorunda kalındığı için e-posta servisi olmayan İnternet sunucusu olur diye kabul etmek zorundayız. LINUX dünyasındaysa, birkaç yüz Mega Hertz'lik alçakgönüllü bir bilgisayar hem web servisinizi, hem ftp servisinizi, hem de e-posta servisinizi verebilir.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) günümüz e-posta sunucuları arasında e-posta mesajı iletiminde kullanılan standart protokoldür. UNIX dünyasında SMTP servisi için yaygın olarak kullanılan üç yazılım bulunmaktadır: **`sendmail`**, **`postfix`** ve **`qmail`**. Bunlar arasında kurulması en kolay olanı; üstelik virüs ve spam kontrolunun en kolay yapılanı **`postfix`** yazılımıdır.

`postfix` sunucusunun temel ayarları **`/etc/postfix`** dizinindeki **`main.cf`** dosyasında yapılır. Bu ayar dosyası içindeki açıklayıcı notlar, ayarları kolayca yapmanızı sağlayacaktır. **`postfix`** ile virüs ve spam filtreleri kurulmasına ilişkin Türkçe "Nasıl" belgelerini **`www.belgeler.org`** adresinde bulabilirsiniz.

`postfix` ile e-posta alışverişi yanında yapılabilecek yararlı işlere birkaç örnek vermek gerekirse:

- Virüs ve spam filtreleme yapabilirsiniz (amavis, spamassassin gibi ek ve tabii ki özgür yazılımların desteği ile),
- e-posta dağıtım listeleri; yani jenerik e-posta adresleri yaratabilirsiniz. Örneğin web sayfanızda "**`bilgi@abc.com.tr`**" olarak ilan ettiğiniz bir e-posta adresine gelen mesajları 5 değişik gerçek e-posta adresine dağıtabilirsiniz (**`/etc/aliases`** dosyası),

- kullanıcılarınız kendilerine gelen tüm e-posta mesajlarını başka bir adrese yönlendirebilirler (**~/.forward** dosyaları).

e-Posta iletim mekanizmasını kısaca anlatmak için çok uygun bir noktaya geldik galiba:

İşyerinizin alan adının **abc.com.tr**; e-posta sunucusu olarak seçtiğiniz bilgisayarın adının da **sunucu.abc.com.tr** olduğunu varsayalım. Böylece kullanıcılarınızın e-posta adresleri **ali@abc.com.tr** veya **ali@sunucu.abc.com.tr** olacaktır. Dünyanın herhangi bir yerinden gönderilecek bir e-posta mesajının e-posta sunucunuzu bulabilmesi için **abc.com.tr** alanı için e-posta sunucusunu belirten bir "MX kaydının" dünyaya ilan edilmesi gerekir.

MX kayıtları (Mail Exchange), ait oldukları alanların DNS kayıtlarını tutan sunucular tarafından tutulur ve yayınlanır. Örneğin **abc.com.tr** şirketi DNS kayıtlarını kendisi tutuyorsa, şirketin DNS sunucusuna **sunucu.abc.com.tr** için bir MX kaydı girmelidir. Eğer şirket DNS kayıtlarını kendi tutmuyorsa büyük olasılıkla İnternet servis sağlayıcısı tutuyordur; bu durumda MX kaydı İSS'na yaptırılmalıdır.

Şimdi artık Patagonya'dan **ugur@abc.com.tr** adresine bir e-posta göndermek isteyen bir bilgisayar kendi DNS sunucusuna "*abc.com.tr'nin e-Posta sunucusu kim?*" diye sorduğunda yanıt olarak **sunucu.abc.com.tr** alacaktır. Ardından, "sunucu.abc.com.tr kim?" diye sorgulayıp IP adresini (örneğin 195.194.12.32) öğrenecektir. e-Posta sunucunuzun IP adresini öğrenen Patagonya'daki bilgisayar, 195.194.12.32 IP adresli bilgisayarınızla SMTP protokolünde bir görüşme başlatacaktır. Eğer 195.194.12.32, SMTP konuşabilen bir bilgisayar ise (örneğin **postfix**, **qmail** veya **sendmail** gibi bir e-posta sunum programı çalışıyorsa) aralarında aşağıdakine benzer bir iletişim gerçekleşecektir:

- ben Patagonya'dan falanca, sizin kullanıcılardan birine e-posta iletilmesini isteyecektim...

- Kullanıcının adı ne?

- cayfer

- İyi... Gönder...

- Mesajın ayrıntıları şöyle:

```
From: ...
To: ...
BCC: ...
Subject: ...
Body: ...
Ekleri: ...
bitti.
```

- Tamam.. Aldım.. Ben iletirim...

- Kapatıyorum... Görüşürüz...

Sizin sunucunuz mesajın tamamını aldıktan sonra, alıcının posta kutusuna yerleştirilmek üzere mesajı olduğu gibi **procmail** yazılımına iletecektir. **procmail** de varsa kullanıcının filtrelerini (spam filtresi, virus filtresi gibi) uygulayacak; eğer mesaj kabul edilecekse, **/var/spool/mail** dizininde kullanıcın adıyla anılan posta kutusu dosyasının sonuna ekleyecektir.

Kullanıcınız, posta kutusunda kendisini bekleyen e-postaları görmek istediğinde birkaç şey yapabilir:

1. LINUX sisteminize login olur, **pine** veya **mail** konsol komutuyla posta kutusunda kendisini bekleyen mesajları görebilir, yanıtlayabilir, silebilir;
2. Bir **POP3** (**P**ost **O**ffice **P**rotocol **3**) istemcisi kullanarak (KMail, Eudora, Mozilla Thunderbird, Evolution, hatta tehlikeyi seven birisi ise Outlook) mesajlarını görebilir, yanıtlayabilir, silebilir;
3. Bir **IMAP** (Internet **M**essage **A**ccess **P**rotocol) istemcisi kullanarak (KMail, Eudora, Mozilla Thunderbird, Evolution, hatta tehlikeyi seven birisi ise Outlook) mesajlarını görebilir, yanıtlayabilir, silebilir.

e-posta mesajının sizin bilgisayarınızdan gönderilmesi durumunda da aynı senaryo tekrarlanacaktır. Mesajınızı gönderen yazılım (örneğin KMail), siz gönder butonunu tıkladığınızda mesajı, kendi ayarlarında **SMTP** (**S**imple **M**ail **T**ransfer **P**rotocol) sunucusu olarak gösterilmiş olan bilgisayara iletir. O bilgisayardaki **postfix**, **sendmail** veya **qmail** gibi bir servis sizin mesajınızdaki alıcının adresinde görünen alanın (domain) MX kaydını DNS kana-

lıyla sorgular. MX kaydı bulunursa, kayıtta belirtilen sunucu ile bir SMTP görüşmesi açar ve mesajı gönderir. Mesajın alıcının posta kutusuna yerleştirilmesi artık karşıdaki e-posta sunucusunun görevidir.

procmail

procmail sunuculukla pek ilgisi olmayan bir yazılımdır. Tüm kullanıcılarınızın farkında olmadan çok sık kullanacakları; bu nedenle hem varlığından, hem de neler yaptığından haberiniz olması gereken bir program olduğu için söz etmeden geçemedik.

procmail, kullanıcılarınıza iletilmek üzere bilgisayarınıza ulaşan e-posta mesajlarını karşılayan ve kullanıcıların posta kutularına yerleştiren yazılımdır. Eğer kullanıcıların kişisel dizinlerinde kendileri için hazırladıkları **.procmailrc** diye bir dosya varsa, bu dosyada yer alan satırlar procmail'e komut (makrosu) olarak yorumlanıp gelen e-posta mesajı bu komutlar doğrultusunda değerlendirilir. Gelen mesaj bu kontrol sonunda özel bir posta kutusuna yerleştirilebilir, çöpe atılabilir, bir başkasına yönlendirilebilir ya da normal posta kutusuna yerleştirilebilir. Aşağıdaki örnek **.procmailrc** dosyası,

a. cyberspam.com adresinden gelen mesajların doğrudan çöpe atılmasını (**/dev/null** dipsiz kuyusuna yönlendirilmesini),

b. omer@ayfer.net'den gelen mesajların da "**omer**" isimli bir dosyaya aktarılmasını sağlamaktadır.

```
# Örnek .procmailrc dosyası
SHELL=/usr/bin/sh
MAILDIR=${HOME}/Mail
LOGFILE=${MAILDIR}/procmail.log

:0
* ^From: *@cyberspam\.com
/dev/null
# Omerden gelen mesajları ayrı posta kutusunda sakla
:0:
* $ ^From:.*omer@ayfer\.net
/home/cayfer/Mail/omer
# Diger mesajlari kabul et
:0:
```

${DEFAULT}

samba Sunucusu

samba, "Server Message Block (SMB)" adıyla anılan protokolun LINUX işletim sistemine bir uyarlamasıdır. "NETBIOS", "LanManager" ve "Common Internet File System (CIFS)" isimleriyle de anılan bu protokol, Windows tabanlı bilgisayarların dosya ve yazıcı kaynaklarının ağ üzerinden paylaşmasını sağlayan protokoldur.

Üzerinde **samba** sunucusu çalışan bir LINUX bilgisayar, buluduğu ağ üzerinde bir NT sunucusu gibi davranır. Gerek yazıcı ve dosya paylaşımı, gerekse "Domain Controller" işlevlerinde son derece başarılıdır. Samba ile LINUX bilgisayarınızı bir iş grubuna (Workgroup) yerleştirip seçeceğiniz dizin ve yazıcıları Windows tabanlı bilgisayarlar kullansın diye paylaşıma açabilirsiniz.

Samba sunucunun ayarları **/etc/samba/smb.conf** dosyasından yapılır. Oldukça uzun olan bu ayar dosyasının ayrıntılarını gerek dosyanın açıklama satırlarında, gerekse internette "Samba Nasıl" sözcükleriyle yapacağınız arama sonucunda karşınıza gelecek dokümanlarda bulabilirsiniz.

Bir Windows bilgisayarın paylaşıma açtığı kaynaklara LINUX bilgisayarınızdan erişmeniz gerektiğinde ise, samba paketinin **smbclient veya smbmount** isimli yazılımın yararlanabilirsiniz. LINUX/UNIX ve Windows tabanlı işletim sistemleriyle kullanılan bilgisayarların birlikte kullanıldığı ağlarda iki işletim sistemi arasındaki paylaşımları hep LINUX/UNIX işletim sistemi üzerinden yapmanızı öneririz.

named (DNS) Sunucusu

TCP/IP protokoluyla çalışan her bilgisayarın bir **DNS** (**D**omain **N**ame **S**ystem) sunucusuna gereksinimi vardır. DNS sunucuları, sembolik İnternet adreslerinin sayısal IP adreslerine çevrilmesini sağlayan; bir bakıma İnternet'in "bilinmeyen numaralar" servisleridir. Bu servisin yazılımı, ilk olarak Berkeley Üniversitesi'nde geliştirilmiş olan BIND (Berkeley Internet Name Domain) paketidir. Paketin adının BIND olmasına rağmen, çalışan programın adı "**named**"dir.

İnternet üzerinde bir bilgisayara erişebilmeniz için ağa basacağınız paketlerin alıcı adresi bölümünde karşıdaki bilgisayarın IP adresi bulunmalıdır. Sayısal IP adreslerini ezberlemek zor olduğu için İnternet bilgisayarlarına sistematik bir şekilde düzenlenmiş, alan adları içeren sembolik isimler verilir.

Örneğin

`www.bilkent.edu.tr`

sembolik adresi, "**`tr`**" alanının, "**`edu`**" alt alanında yer alan "**`bilkent`**" ağının "**`www`**" isimli bilgisayarı demektir. TCP/IP bir ağ üzerinde yer alan bu bilgisayarın bir de IP adresi olmalı ve birileri bu IP adresinin hangi sembolik isme karşılık geldiğini bilmeli ve soran olduğunda da bunu bildirmelidir.

DNS mekanizması ana hatlarıyla şöyle çalışır:

Patagonya'da web tarayıcısının başında oturan bir kullanıcı, URL olarak "**`http://www.bilkent.edu.tr`**" girdiğinde, o tarayıcı yazılımın, **`www.bilkent.edu.tr`** isimli bilgisayarın IP adresini öğrenmesi ve http protokulunun web sayfası isteme kurallarına uygun bir paket hazırlayıp, paketin alıcı adresi bölümüne bu IP adresini yerleştirmesi gerekir.

Bunun için, Patagonya'daki kullanıcının kullandığı işletim sistemi, kendi TCP/IP ayarlarında belirtilmiş olan DNS sunucusuna "*www.bilkent.edu.tr de kim ola ki?*" sorusunu; yani DNS sorgusunu gönderir.

Diyelim ki, Patagonya'daki bilgisayar ağından Bilkent'e yönelik daha önce hiç bir sorgu yapılmamış olsun... Bu durumda Patagonya'daki DNS sunucusu bu sorguya ne yanıt vereceğini bilemeyecektir. Bu kez, Patagonya'daki DNS sunucusu, sorguyu kendi TCP/IP ayarlarında belirtilmiş olan bir üst düzey DNS sunucusuna aktaracaktır.

Sorgu bu şekilde yukarı doğru çıkarken, yol üzerinde biryerlerde bir DNS sunucusu "*www.bilkent.edu.tr'yi bilemem ama 'edu.tr' adreslerini kimin bildiğini biliyorum!*" yanıtını verecektir. Bu örneğimiz için edu.tr adreslerini bilen DNS sunucusu, ODTÜ'deki bir DNS sunucusu olacaktır.

Bu yanıt, Patagonya'daki bilgisayara geri iletilince, bu bilgisayar sorgusunu biraz değiştirerek ODTÜ'deki sunucuya "*bilkent.edu.tr adreslerini kim bilir?*" olarak yöneltir. ODTÜ bu soruya "*139.179.10.13 IP adresli bilgisayara tüm bilkent.edu.tr adreslerini sorabilirsin!*" yanıtını verir.

Son adımda da Patagonya'daki bilgisayar Bilkent Üniversitesi'nin 139.179.10.13 IP adresli DNS sunucusuna "*www.bilkent.edu.tr'nin IP adresi nedir?*" diye sorar, yanıtını alır ve http istek paketini bu adrese gönderir. Adresi çözülen kayıtlar, DNS sunucuları tarafından "*belki birazdan birileri gene sorar*" mantığıyla "DNS kaşesi" adı verilen tampon bellekte bir süre saklanır.

Bu senaryo, sorguların aktarıldığı hiyerarşideki DNS sunucularının ayarlarına bağlı olarak değişebilirse de, ana hatlarıyla mekanizma bu şekilde işler. Eğer hiç kimsenin tanımadığı bir adres sorgulandıysa, sorgu internetin en üst düzey DNS sunucularına kadar çıkabilir. En üst düzeydeki bu DNS sunucular (*root level servers, top level servers*) fazla ayrıntıya girmeden "**.com**", "**.edu.tr**" gibi ağ alanlarına DNS servisi veren bilgisayarların listesini tutarlar. Yani, bu en üst düzey DNS sunucular, örneğin "**bilkent.edu.tr**" ağının kayıtlarını tutan bilgisayar ya da bilgisayarları bilmeyebilir, ama "**edu.tr**" alanının kayıtlarını tutan bilgisayar ya da bilgisayarları bilirler. "**edu.tr**" kayıtlarını tutan DNS sunucusu, "**bilkent.edu.tr**" için kayıtları kimin tuttuğunu bilir. Bilkent Üniversitesi'nin DNS sunucusu da üniversitedeki tüm kayıtlı bilgisayarları bilir.

Çok sık yanlış anlaşılan bir kavrama burada açıklık getirmek istiyoruz: bir bilgisayarın sembolik adresleri çözebilmesi için o bilgisayarda DNS sunucusu yazılımı çalışması gerekmez. Aslında tek gereksinim olan, söz konusu bilgisayara makul bir sürede yanıt verebilecek bir DNS sunucusunun yakınlarda biryerlerde bulunmasıdır. Küçük ağlarda (yaklaşık 250 bilgisayara kadar) ve daha önemlisi genellikle "sorgulayan" istemcilerden oluşan ağlarda, DNS hizmeti genellikle internet servisini sağlayan kuruluştan alınır. Eğer ağınızda çok bilgisayar varsa ve/veya ağınızdaki bilgisayarların IP adresleri çok sorgulanıyorsa kendi DNS sunucunuzu kurmanız genel ağ performansını arttıracaktır.

"*Kendi DNS sunucunuzu kurmanız yararlı olur*" dediğimize bakıp da bu iş için yeni bir bilgisayar satın almanız gerektiği sonucunu çıkarmayın sakın. Ağ üzerindeki herhangi bir LINUX bilgisayar bu işi rahat rahat yapacaktır. DNS sunucunuzu Windows tabanlı bir işletim sistemi üzerinde çalıştıracaksanız; yani bir WINS sunucu kuracaksanız o zaman başka... Salt DNS işleri için oldukça güçlü bir bilgisayar ve işletim sistemi lisansı satın almanız ve bu bilgisayarda başka iş çalıştırmamanız gerekecektir.

named ayarları **/etc/named.boot** dosyası ve **/var/named** dizini altındaki dosyalarda yapılır. DNS sunucu kurmak kolay değildir. DNS mantığını iyice öğrenmek ya da kurulmuş bir sistemi inceleyip, ona bakarak çalışmak gerekir.

ssh Sunucusu (Secure Shell)

Yerel ağ hatlarını dinlemek, gelip geçen tüm Ethernet paketlerini seyretmek hatta kaydetmek mümkündür. Bilişim terminolojisinde "Sniff etmek, yani koklamak" olarak anılan bu işi yapmak için pek çok yazılım bulmak olasıdır. Bu yazılımlar bilgi çalmanın yanısıra ağ yöneticileri tarafından ağ sorunlarını bulmak için de yoğun olarak kullanılmaktadır.

Ethernet ağlarda "Hub" yerine "Switch" kullanarak hattın dinlenmesini önleyebileceğinizi sanıyorsanız yanılıyorsunuz. Nasıl yapıldığını bu kitapta elbette anlatmayacağız ama bunun mümkün olduğunu bilmenizde yarar var.

Hattın dinlenmesini önleyemeyeciğinize göre bari dinleyenlerin neler olup bittiğini izleyemeyecekleri bir düzen kurmalısınız. Hırsıza kilit dayanmayacağı gibi çözülemeyecek bir şifre sistemi kurmak ta olası değil ama hiçbir şey yapmadan da olmaz. Secure Shell kavramı işte bu iş için geliştirilmiştir. İki bilgisayar haberleşmeye başlamadan önce karşılıklı bir şifre/parola sistemi üzerinde anlaşırlar ve haberleşme seansı boyunca bu sistemi kullanırlar. Yeni bir seans başladığında yepyeni bir şifre/parola sistemi kullanılır. Bu haberleşmeleri dinleyip de kırmak isteyenler epeyce uğraşacaktır.

ssh, bilgisayar bilimlerinde "Symmetric Key Encryption" olarak sınıflandırılan "RSA", "3DES" ve "Bluefish" sistemlerini kullanarak hat üzerinde gelip giden tüm paketleri kriptolar. LINUX bilgisayarınıza klasik "telnet" yerine "**ssh**" istemcisini kullanarak bağlanırsanız hatlarınızı dinleyenler neler olup bittiğini anlayamayacaktır. **ssh** ile terminal bağlantısı kurduğunuzda görsel olarak hiçbir şey değişmeyecek, size herşey telnet ekranı gibi bir ekranda görünecektir. Bilgisayarlar arası dosya kopyalarken "**rcp**" yerine "**scp**" kullanabilirsiniz. ssh kullanan ftp istemcileri de bulabilirsiniz (Mandrake LINUX dağıtımında **sftp** isimli bir güvenli ftp istemcisi, "secure ftp" yer almaktadır.)

ssh sunucunuzun ayarlarını **/etc/ssh/** dizinindeki dosyalarda yapabilirsiniz. Eğer paranoyak değilseniz, varsayılan ayarlar işinizi görecektir. Ancak; unutmayın; internete bağlı hiçbir bilgisayar yüzde yüz güvenli iletişim yapamaz!

NIS Sunucusu (Network Information Services)

NIS'in ne işe yarayacağını en kolay bir örnekle açıklayabiliriz. Diyelim ki, işyerinizde 10 tane UNIX/LINUX bilgisayar ve 30 da kullanıcınız var. Bu durumda bilgisayarlar paylaşılıyor demektir; yani, kimin ne zaman hangi bilgisayarın önüne oturacağı ya da uzaktan login edeceği belli olmayacaktır. Bir kullanıcının rastgele seçtiği bir bilgisayara login olabilmesi için, seçtiği bilgisayarda tanımlı bir kullanıcı hesabına sahip olması gerekir. Bir başka deyişle sistem yöneticisinin, örneğin, **cayfer** kullanıcısı için 10 bilgisayarda da birer hesap açması gerekecektir. Daha da kötüsü, bu kullanıcı şifresini değiştirmek istediğinde 10 bilgisayarda da bu değişikliği yapması gerekecektir. Olacak iş değil! İşte buna benzer durumlarda NIS kullanmanız gerekecektir. Bir ağda yer alan bilgisayarlar arasında paylaşılacak **/etc/passwd**, **/etc/shadow**, **/etc/hosts** gibi dosyaları NIS ile bilgisayarlar arasında paylaştırabilirsiniz. Makinelerinizden birini ya da bir kaçını NIS sunucu olarak belirleyip, örneğin **/etc/passwd** ve **/etc/shadow** dosyalarınızı bu bilgisayara yerleştirip, kullanıcı hesaplarını tek noktadan yönetebilirsiniz.

NIS servisinin adı eskiden "Yellow Pages" idi. Ancak, "Yellow Pages" sözcüklerinin isim hakkı AT&T telefon şirketine ait olduğu için bu isim terkedildi ve yerine NIS kullanılmaya başlandı. Daha önce de belirttiğimiz gibi, UNIX dünyası "tutucu" denebilecek kadar geleneklere bağlı olduğu için NIS ayar dosyaları ve ilgili süreç/program isimleri "**yp**" ile başlar şekilde kaldı. NIS ayarları da bu nedenle **/etc/ypserv.conf** isimli dosyadan yapılmaktadır.

iptables Ateş Duvarı

Bilgisayarınıza gelen ve bilgisayarınızdan çıkan TCP/IP paketleri üzerinde tam bir denetim kurmak istiyorsanız, bir "*firewall*" yazılımı, yani bir "ateş duvarı" yazılımı kullanmanız gerekir. Aslında **iptables**, sunucu kategorisine giren bir yazılım değildir. Sisteme, ağ ara birimleri üzerinden gelen ve giden paketleri filtrelemek, değiştirmek ve gerektiğinde yönlendirmek için kullanılır.

LINUX altında bu aracınız da hazır: son derece güçlü, yetenekli ve hızlı bir ateş duvarı yazılımı olan **iptables** ile **/etc/hosts.deny** ve **/etc/hosts.allow** dosyalarıyla denetleyemeyeceğiniz trafiği de kontrol altına alabilirsiniz. Örneğin, 140.1.13.23 adresinden ağınızdaki 134.43.23.1 adresli makineye gelen SMTP paketlerini kesebilirsiniz. Ağınızdaki 134.43.23.1 adresli bilgisayara gelen http paketlerini yük dağıtımı yapmak üzere 134.32.23.250 adresli bilgisayara yönlendirebilirsiniz.

iptables ile port düzeyinde filtreler kurabilirsiniz. Örneğin, günün birinde MS-SQL sunuculara musallat olan SQL Slammer gibi bir virüsün 1434 numaralı porttan saldırdığını öğrendiğinizde

```
/sbin/iptables -I FORWARD -p udp --dport 1434 -j DROP
```

komutunu vererek 1434 numaralı porttan gelen tüm UDP paketleri durdurabilirsiniz.

iptables ayarları yeni başlayanlara biraz karışık görünecektir; bu nedenle **shorewall** paketi, **iptables** ayarlarını yapmanızı kolaylaştıracak bir paket olarak geliştirilmiş ve tabii ki özgür bir yazılım olarak hizmetinize sunulmuştur.

DHCP Sunucusu

Bir TCP/IP ağda yer alacak her bilgisayar için, IP numarası, ağ maskesi (*netmask*), ağ geçidi (*gateway*), DNS sunucusu ya da sunucularının belirtildiği ayarların bir şekilde yapılması gerekir. Bu ayarlar, statik olarak elle yapılabileceği gibi, otomatik olarak da yapılabilir. TCP/IP ayarların otomatik yapılmasını sağlayan servis **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) servisidir. Bu servisi kullanan ağlarda, bilgisayarların TCP/IP modüllerine, ayarların DHCP ile yapılması gerektiği belirtilirse, TCP/IP modülleri yüklendiğinde ağ arabirimine

> "*MAC adresim 03:04:de:3a:29:1f; bana IP ayarlarımı verecek bir DHCP servisi var mı?*"

anlamına gelen bir paket gönderirler. Eğer ağda DHCP sunucusu varsa, bu sunucu yazılımı, gelen isteği, değişik politikalara göre değerlendirip istekte bulunan bilgisayara

"IP adresin 192.168.23.45,
ağ geçidin 192.168.2.1,
ağ masken 255.255.255.0,
DNS sunucun da 192.168.2.240"

gibi bir yanıt gönderir.

DHCP politikaları arasında, verilen bir IP adresinin ne kadar süreyle bir başkasına verilmeyeceği, belirli MAC adresine sahip istemcilere önceden kararlaştırılmış IP adreslerinin verilmesi gibi kavramlar kullanılabilir.

DHCP kullanıp kullanmamak bir ağ yönetim stratejisidir. Kimi ağ yöneticileri, kullanıcılarının trafiklerini izlemek ve denetlemek istedikleri için statik IP adresleri tahsis etmeyi tercih ederler. Örneğin, **iptables** veya benzeri bir ateş duvarı yazılımıyla ağınızdaki bilgisayarların üzerinden geçen trafik üzerinde sınırlamalarınız varsa, DHCP ayağınıza bağ olacaktır. Düşünsenize; siz 192.168.3.2 IP adresli bilgisayara ftp trafiği gelmesini istemediğiniz için iptables ayar dosyasına bir satır eklemişsiniz ama bir sonraki gün, söz konusu bilgisayar DHCP servisinden bir başka IP adresi alarak açılmış. Linux'ta çare tükenmez... Siz de uygun IP adresleriyle durduramıyorsanız, bir iptables filtresi kullanarak MAC adresiyle durdurursunuz.

Öte yandan, yeni yeni yaygınlaşan telsiz Ethernet teknolojisi (Wireless Ethernet, 802.11b, 802.11a, 802.11g standartları, Wi-Fi) sizi DHCP kullanmaya zorlayacaktır. Wi-Fi hizmeti verdiğiniz bir bölgeye kucağında bilgisayarıyla gelen bir kullanıcının önce ağ yöneticisini bulup, uygun bir IP numarası istemek zorunda olması hiç de mantıklı olmaz.

DHCP kulanıp kullanmamak sizin kararınıza kalmıştır. Bu kararı alırken, kullanıcılarınızı DHCP kullanmaya zorlayamayacağınızı bilmelisiniz. Siz DHCP servisi verseniz de vermeseniz de, ağınızdaki bir kullanıcı bilgisayarına istediği IP adresini girebilecektir. Tahmin edebileceğiniz gibi DHCP sunucu yazılımı **dhcpd**'nin ayarları **/etc/dhcpd.conf** dosyasından yapılabilir.

Dikkat ettiyseniz neredeyse tüm sunucu yazılımların ayar dosyaları **/etc** dizininin altında yer alıyor. Hatırlarsanız, daha önce yedeklemeden söz ederken **/etc** dizininin önemini vurgulamıştık. Haklıymışız; değil mi?

MySQL ve PostgreSQL Veritabanı Sunucuları

Her ikisi de özgür yazılım dünyasının çok beğenilen, güvenilen birer "ilişkisel veritabanı yönetim" (**RDBMS: R**elational **D**atabase **M**anagement **S**ystem) sistemleridir. İsimlerinden de anlaşılacağı üzere; her ikisi de SQL veritabanı sorgulama dilini desteklemektedir. Hangisinin daha iyi olduğu konusunda birşey söylemek oldukça güçtür.

PostgreSQL'in, işleyebildiği SQL komut sayısı ve komut varyasyonları daha zengindir. Eğer bir veritabanı uzmanıysanız, MySQL, PostgreSQL, Oracle, Sybase, MS-SQL, IBM DB2, Informix gibi veritabanı yönetim sistemlerinin çok ayrıntılı bir karşılaştırmasını

http://www.mysql.com/information/features.html

adresinde incelemeden hangi veritabanı sistemini kullanacağınıza karar vermeyin.

Sıradan bir veritabanı yönetim sistemine gereksinim duyuyorsanız, ya da bu işlere yeni başlayacaksanız, MySQL kullanmanızı öneririz. Aslında MySQL ya da PostgreSQL sunucularından birini seçmek zorunda değilsiniz; ikisini birden kurup çalıştırabilirsiniz. Unutmayın, LINUX dünyasındasınız; alışmanız belki biraz zaman alacak ama özgürsünüz.

Eğer MySQL seçerseniz, gerek veritabanı sunucusunu, gerekse veritabanlarınızı yönetmek için web tabanlı bir uygulama olan **phpMyAdmin** yazılımını kurmanızı öneririz (*www.phpmyadmin.net*).

İlişkisel veritabanlarını pek tanımayan okuyucularımız için kısaca özetlemek gerekirse; veritabanı sunucu yazılımları, desen olarak birbirine benzeyen ve çok sayıda veri kaydı arasından belirli bir koşulu sağlayan kayıtları çok hızlı bir şekilde bulup çıkarmak için geliştirilmiş yazılımlardır. Doğal olarak bu sunucu yazılımları, veritabanlarına kayıt ekleme, güncelleme, kayıt çıkarma işlevlerini; ve en önemlisi çok kullanıcılı ortamda erişimi de desteklemektedir. Uygulama programları, ilişkisel veritabanı yönetim sistemi denetimindeki dosyalara doğrudan erişemezler. Veritabanına bir kayıt eklemek gerektiğinde, uygulama programı veritabanı sunucusuna

```
INSERT musteriler values (“ABC Ltd”, “Falanca Mah”,
“602.Sokak”, “Bayi”);
```

benzeri SQL komutları gönderir ve komutun yerine getirilmesini bekler. Kayıtlı veriler arasından seçim yapmak içinse

```
SELECT firma_adi, adresi FROM musteriler
                              WHERE tip = “Bayi”;
```

benzeri bir SQL komutu gönderip, tipi “Bayi” olan müşterilerin kayıtları istenebilir. Verilen kriterleri sağlayan kayıtlar bir küme olarak uygulama programına geri gönderilir.

Perl dili ile MySQL kullanımı hakkında ayrıntılı bilgiye gereksinim duyarsanız, PUSULA Yayıncılık tarafından yayınlanmış olan *Perl ve MySQL ile CGI Programlama* (ISBN:975-7092-89-4) kitabını önerebiliriz.

`squid` Proxy Sunucusu

LINUX dünyasının en çok kullanılan “proxy” sunucusudur. “Proxy server” teriminin Türkçe karşılığı olarak “vekil sunucu” kullanılmaktaysa da “vekil” sözcüğü “proxy” sözcüğünün anlamını tam olarak vermediği için; biz “proxy” demeye devam edeceğiz.

Proxy sunucuları, bir bilgisayar ağının İnternet çıkışında devreye “seri” olarak girmiş ve proxy yazılımı çalışan bilgisayarlardır. Genellikle, proxy sunucudan yararlanmak isteyenler TCP/IP istemci yazılımlarının (örneğin web tarayıcılarının) ayarlarında bunu belirtirler. Böylece söz konusu uygulama TCP/IP paketlerini proxy sunucuya yönlendirirler. Örneğin, “http proxy” görevini yapan bir proxy sunucu, içerden kendisine gelen tüm http isteklerini yakalar; gerekiyorsa istemci olarak kendisini göstererek paketi yeniden düzenler ve alıcısına öyle gönderir. Gelen yanıtları da önce kendi diskine kaydeder, sonra da dosyayı istemiş olan, içerdeki bilgisayara iletir. Bir süre sonra ağın içinden birileri gene bu dosyayı İnternet'ten indirmek isterse, bu isteği İnternet hattına aktarmak yerine kendi disklerine kaydettiği dosyayı geri gönderir. Aslında mekanizma bu kadar basit değildir; örneğin, istenen bir dosyayı kendi disklerinden sunmadan önce dosyanın istendiği yerden o dosyanın en son değişikliğe uğradığı saat ve tarihi öğrenir; eğer kendi diskindeki kopya daha eski değilse, dosyayı İnternet'ten indirmek yerine kendi diskinden gönderir.

Proxy sunucuları internet hatlarından tasarruf sağlar; ayrıca sık sık ziyaret edilen web sitelerinin kullanıcılara çok daha hızlı sunulmasını sağlar.

Proxy sunucuları sadece web iletişiminde kullanılmaz, FTP proxy sunucuları da anlamlıdır.

Proxy sunucusu olarak kullanılacak bir bilgisayarın işe yarar bir disk kapasitesine sahip olması gerekir. Arkasındaki ağın büyüklüğüne; daha doğrusu arkadaki kullanıcı sayısına ve bunların web davranışlarının özelliklerine bağlı olarak birkaç Gigabyte'dan birkaç yüz GigaByte'a kadar disk gerekecektir. Bir üniversite için, 60 GByte civarında bir proxy sunucu disk kapasitesi iş görecektir; oysa bir servis sağlayıcı için daha fazlası gerekecektir.

Proxy sunucuları kullanıcı tarafında genellikle isteğe bağlı olarak kullanılır. Yani istemeyen kullanıcılar, web tarayıcılarının proxy ayarlarını yapmayarak proxy sunucunuzdan yararlanmamayı seçebilir. Servis verdiğiniz ağın özelliklerine bağlı olarak kullanıcılarınızı proxy sunucusunu kullanmaya zorlamak isteyebilirsiniz. Böyle bir durumda squid yazılımını "saydam proxy sunucusu" (transparent proxy server) olarak kurmalısınız.

Kurduğunuz bir proxy sunucusunun yararını ölçmek istediğinizde, sunucunun raporlarından ve log kayıtlarından yararlanmalısınız. "Kaşe isabet oranı" (*Cache hit ratio*), sunucunuzun başarı düzeyini en iyi gösterecek olan değerdir.

`squid`, sorumlu olduğu ağdaki trafiği çok sıkı denetlemek isteyen yöneticiler için önemli bir araçtır. Yerel ağda kopyası bulunan bir dosyayı almak için internet hattının boşuna işgal edilmesini engellediği gibi, ağ içinde kimin hangi adrese gittiğinin de ayrıntılı bir şekilde izlenmesine olanak sağlar. İşyerinizdeki kullanıcıların bütün gün chat yaptıklarından, fal ve oyun sayfalarında dolaştıklarından şüpheleniyorsanız, squid kurup istatistik raporlarını inceleyebilirsiniz. "tor" ve "privoxy" gibi yazılımlarla squid'in yetenekleri daha da genişletilebilir. Örneğin "privoxy" ile spam filtrelemeye benzer bir yöntemle web sitelerindeki reklamlar filtrenebilir.

ppp Çevirmeli Ağ Sunucusu

İşyerinizde kurduğunuz LINUX bilgisayara evden modemle bağlanmak istediğinizde iki seçeneğiniz vardır:

1. Basit telnet bağlantısı kurmak
2. ppp bağlantısı kurup, hem LINUX makinenize, hem de onun üzerinden internete de bağlanmak.

ppp (Point-to-Point protocol), seri arabirimler üzerinden TCP/IP bağlantısı kurmak için geliştirilmiş bir protokoldur. İki bilgisayar arasında ppp protokolu çalışmaya başladığında her iki tarafta da seri arabirimlere birer IP numarası verilir. Böylece aranan bilgisayarın iki ağ arabirimi olur: biri Ethernet arabirimi; diğeri de modemin bağlı olduğu seri arabirim.

"Aranan bilgisayar" artık iki bilgisayar ağı üzerinde aynı anda yer alan bir yönlendiricidir (router).

Aralarında ppp bağlantısı olan bilgisayarların arasında istemci-sunucu gibi bir ilişki yoktur; her ikisi de eşit düzeyde noktadan-noktaya bağlı bilgisayarlardır; bir başka deyişle "ppp sunucusu" aslında pek doğru bir deyim değildir.

Bir bilgisayarın, modem üzerinden gelen seri bağlantıları kabul edebilmesi için söz konusu seri arabirimin (**`/dev/ttySn`**) basit terminal bağlantısı yapabilir şekilde ayarlanmış olması gerekir. Bu ayarı yapabilmek için, örneğin ilk seri arabirim **`/dev/ttyS0`** için **`getty`** programı çalışabilir durumda olmalıdır.

`getty` servisiyle normal terminal bağlantısı yapabilen bir kullanıcı, kendi bağlantısı için bir pppd süreci başlatıp kendi bilgisayarıyla aradığı bilgisayar arasında bir ppp bağlantısı kurabilir.

Evet! Yukarıdaki satırlarda biraz garip laflar ettiğimizin farkındayız ama ne yapalım, bu işler böyle. Bu kitapta, bir bilgisayarın ppp servisini verecek şekilde kurulması için yapılması gereken herşeyi anlatmaya olanak yok; amacımız yol göstermek. Eğer bu konuda ayrıntılı bilgiye gereksinim duyuyorsanız, internette çok sayıda kopyasını kolayca bulabileceğiniz "Serial Howto" ve "ppp Howto" dokümanlarını okumalısınız.

LINUX işletim sistemi ile birlikte gelen veya sonradan yüklenebilen önemli ağ servisleriyle ilgili daha ayrıntılı bilgiye gereksinim duyduğunuzda PUSULA Yayıncılığın *LINUX Ağ Servisleri* isimli kitabından yararlanabilirsiniz (ISBN: 975-6477-13-x).

BUNLARI BİLİYOR MUYDUNUZ?

Linux Dağıtımları

Mayıs 2006 tarihinde, dağıtılan, satılan ve desteklenen 357 değişik LINUX dağıtımı olduğunu biliyor muydunuz?

Evet, tam 357 değişik LINUX dağıtımından'dan söz ediyoruz... Bu kitabın birinci baskısının yayınlandığı Temmuz 2003'de dağıtım sayısı 135 idi.

LINUX'un arkasında profesyonel destek olmadığını, sorunların çözülmesinde kullanıcıların yalnız olduğunu iddia edenlere ithaf olunur.

LINUX dağıtımlarını sürekli izleyen, inceleyen, irdeleyip eleştiren *www.distrowatch.com* sitesinde ayrıntılı bilgi bulabilirsiniz.