

- **Sistem Hakkında**
 - **Sistemin Açılması**
 - **Sistemin Kapatılması**
 - **Disklerin Yönetimi**
 - **Bellek Yönetimi**
- **Kullanıcı Yönetimi**
 - **Kullanıcı Hesapları**
 - **Kullanıcı Grupları**
- **Log Dosyalarının Yönetimi**
- **Ağ Yönetimi**
- **TCP/IP Ayarları**
- **Yazıcı Yönetimi**
- **Yedekleme**
- **Periyodik İşlerin Yönetimi**
- **LILO Yönetimi**
- **Webmin**
- **“root” Şifresini Unuttuğunuzda...**

Kim Korkar LINUX'tan?

UNIX sistem yöneticiliği bir meslektir, hem de önemli bir meslek! İnternet'in hızla yayılması nedeniyle de "Ağ Yönetimi" ve "Sistem Yönetimi" diye anılan iş kolları birbirlerine iyice yaklaşmış; hatta birleşmiştir.

Artık sistem yöneticileri ağ yönetiminden; ağ yöneticileri de sistem yönetiminden anlamak zorundadır.

Bir "Sistem Yöneticisi"nin öncelikli görevi sistemi ayakta tutmaktır. Bu sistem tek bir bilgisayardan oluşabileceği gibi dünyaya yayılmış birçok bilgisayardan da oluşabilir. LINUX işletim sisteminin çok güvenli olduğunu defalarca tekrarladık ama sonuçta insan yapısı bir bilgisayar üzerinde çalıştığını da unutmamak gerekir.

Bir bilgisayar sisteminin düzgün çalışmasında; iyi servis verilmesinde belki de en önemli etken sistem yöneticisidir. Yeterince iyi bir sistem yöneticisi, işletim sistemi ve donanım özellikleri ne olursa olsun (Linux veya Windows; IBM veya toplama bilgisayar) başarılı ağ hizmetleri sunmayı başarabilir.

Donanım arızaları, kullanıcı hataları, sistem yöneticisi hataları, saldırılara yenik düşme, iletişim hataları, sahtekarlık, sabotaj gibi bir sürü nedenle bir sistem çökebilir. İşte sistem yöneticileri bu çöküşlerde sistemi hızla yeniden çalışır duruma getirmek, çöküş olasılığını azaltmak, çöküş olduğunda da zararı olabildiğince küçültebilmek için çalışmak, hem de çok çalışmak zorundadır.

Bir sistem yöneticisinin ikinci öncelikli görevi ise sistemin kullanıcılara sürekli ve güvenilir hizmet vermesini sağlamaktır. Bu görevin gerektirdiği bir sürü alt görev olmakla beraber en genel ve önemli olanları şunlardır:

- Sistemin kaynaklarının verimli bir şekilde kullanılmasını sağlamaya yönelik önlemleri almak.
- İşletim sistemini ve uygulama programlarını güncellemek.
- Sistemde yüklü program ve verilerin yedeklenmesi işlerini düzenlemek.
- Sistemin güvenliğini sürekli olarak denetlemek ve yeni saldırı teknikleriyle yeni ortaya çıkan güvenlik açıklarına karşı önlem almak.

Sistem Hakkında

Sistemin Açılması

Sistem yöneticilerinin en iyi bilmeleri gereken süreçlerden biri sistemin açılış sürecidir.

“boot” adı verilen sistemin açılış sürecini LINUX işletim sisteminde denetleyen yazılım genellikle LILO’dur. “**LILO**”; Linux Loader sözcüklerinden elde edilmiş bir kısaltmadır. Diğer bir popüler açılış yönetici yazılımı ise GRUB’dur, ama bu kitapta yalnızca LILO’dan söz edeceğiz.

Bilgisayara elektrik verilmesi ve kullanıcının bir login ekranıyla karşılaşması arasında olup bitenleri, fazla ayrıntısına girmeden de olsa, olabildiğince iyi anlamanız birçok sistem yönetimi konusunu kavramanıza yardımcı olacaktır. Şimdi bu açılış sürecini adım adım gözden geçirelim:

1. Bilgisayarınıza elektrik enerjisi verince anakartın üstündeki BIOS çipinde kayıtlı bulunan küçük bir program çalışmaya başlar.
2. Bu program, BIOS ayarlarınıza bağlı olarak sırasıyla sisteme bağlı disket, CD, disk sürücülerinin birinde işletim sistemini yükleyebilecek bir program arar. Bu program, “**boot sektörü**” olarak bilinen alanda, kullanılmakta olan sürücüden işletim sistemini yükleyebilecek bir program olmalıdır.
3. Bilgisayarınıza LINUX kurduğunuzda ilk diskin “**boot**” sektörüne (**MBR: Master Boot Record** da denir) LILO yazılımı yerleştirilir. (Elbette, GRUB ya da bir başka boot yöneticisi seçtiyseniz, boot sektörüne seçtiğiniz program kaydedilmiş olacaktır.)
4. LILO yazılımı BIOS tarafından belleğe yüklenip çalışmaya başladığında kullanıcıya çeşitli açılış seçenekleri sunabilir. Örneğin, üzerinde hem Windows XP, hem LINUX yüklü bir bilgisayarda kullanıcıya, sistemi istediği işletim sistemiyle açabilmesi için bir seçenek listesi sunulur:



LILO için gerekli ayarlar **/etc/lilo.conf** dosyasında yapılır. Ancak, LILO programı çalıştığı sırada ortada sistemi denetleyen bir işletim sistemi olmadığı için LILO, **/etc/lilo.conf** dosyasına erişemez. **lilo.conf** dosyasında değişiklik yaparsanız, **/sbin/lilo** komutuyla LILO'nun yeni ayarlara göre çalışacak şekilde yeniden hazırlanıp diskin boot sektörüne yazılmasını sağlamalısınız.

5. LILO'nun sunacağı seçenekler arasında "LINUX" seçtiğinizi varsayarak açılış sürecini incelemeye devam edelim... LILO, **/boot** dizininde **vmlinuz** dosyasında bulunan LINUX çekirdiğini (kernel) belleğe yükler ve çalıştırır.
6. Çekirdek programı, konsolun ekran kartına uygun bir görüntü ayarına geçer ve sisteme bağlı olan donanım unsurlarını tarayarak (bellek, merkezi işlem birimi, görüntü kartı, disk arabirimleri, ses kartları, paralel ve seri arabirimler, ağ bağlantı arabirimleri gibi) bunları tanımaya ve ilgili sürücü yazılımlarını (*device driver*) yüklemeye başlar.
7. Çekirdek, daha sonra yine LILO ayarlarında belirtildiği şekilde root dosya sistemini (yani **/** dizininin olduğu fiziksel diski) ilişitir (mount eder). Bu dosya sistemi ilk aşamada sadece okuma için (*read-only*) ilişitirilir ve izin yapısı kontrol edildikten sonra, yani bu dosya sistemi için **fsck** yazılımı çalıştırıldıktan sonra **oku-yaz** (*read-write*) kullanımı için tekrar ilişitirilir.
8. Bir sonraki adımda, sisteminiz açık kaldığı süre boyunca, "1" süreç numarasıyla sürekli çalışacak olan **init** programı başlatılır. Bu süreç, sistemi kullanıma hazır hale getirmek için **/etc/inittab** dosyasında belirtilen ayarlara göre bir dizi kabuk programı çalıştırarak sistemin "çalışma düzeyini" (*run level*) aşama aşama artırır.

Çalışma düzeyleri, işletim sisteminin hangi yeteneklerinin çalışmaya başladığını belirler. Tipik bir LINUX sisteminde yedi çalışma düzeyi vardır:



- 0: Sistemin kapanma işlemlerinin başlatıldığı düzey. (*Halt Level*)
- 1: Tek kullanıcı çalıştırma düzeyi. (*Single-user*)
- 2: Ağ desteği olmadan çok kullanıcı çalıştırma düzeyi.
- 3: Çok kullanıcı çalıştırma düzeyi. (*Multi-user*)
- 4: Bu çalışma düzeyi nedense kullanılmaz.
- 5: X Window'un çalışmaya başladığı düzey. (Grafik kullanıcı arabirimi)
- 6: Yeniden başlatma işlemlerinin başlama düzeyi. (*Reboot*)

Normal koşullarda; yani başarıyla açılmayı tamamlamış bir LINUX bilgisayar üçüncü (X Window kullanılmıyorsa) veya beşinci düzeyde çalışmasını sürdürür.

Sistemi kapatmak istediğinizde

```
init 0          veya
init 6
```

komutlarından biriyle sisteminizi sıfıncı düzeye indirerek kapatabilir (*halt-shutdown*) veya altıncı düzeye geçirerek yeniden başlatabilirsiniz. (*reboot*)

Yapacağınız bir yazılım veya veri bakım çalışması nedeniyle bilgisayarın başka kullanıcılara hizmet vermeksizin sadece konsoldaki kullanıcıya hizmet verecek şekilde çalışmasını isterseniz

```
init 1
```

komutuyla tek kullanıcı düzeyine dönüp, işiniz bittiğinde

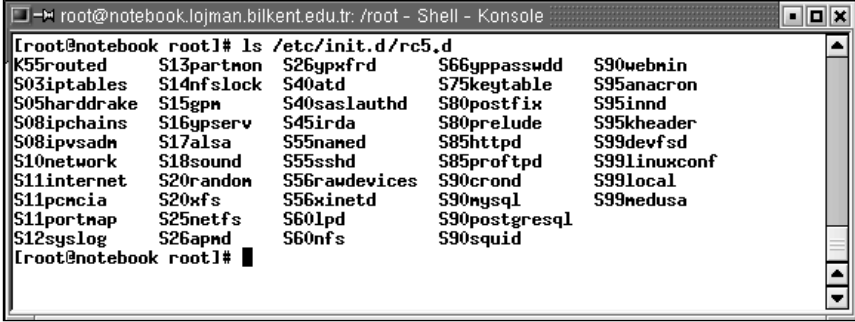
```
init 3
```

komutuyla tekrar çok kullanıcı düzeyine geçebilirsiniz. Tabi bu arada kullanıcılarınız sizi dövdüp sağlık düzeyinizi değiştirmiyse...

Sistemin açılışı sırasında her çalışma düzeyinde yapılacak işler **/etc/inittab** dosyasına tanımlanır. Bu dosyanın deseni ve içeriği konusunda daha fazla ayrıntıya girmek istemiyoruz. Meraklı okuyucular "man **inittab**" komutuyla oldukça ayrıntılı bilgi edinebilirler.

Kim Korkar LINUX'tan?

/etc/rc.d dizini altında değişik çalışma düzeylerine geçerken gerekli ve ilgili hizmetlerin başlatılıp durdurulması için kullanılan kabuk programları yer alır. Örneğin, **/etc/rc.d/rc5.d** dizinindeki dosyalar, sistemin beşinci çalışma düzeyine, yani X ortamına geçerken çalıştırılacak kabuk programlarıdır.



```
root@notebook.ijman.bilkent.edu.tr: /root - Shell - Konsole
[ root@notebook root ]# ls /etc/init.d/rc5.d
K55routed      S13partnon    S26ypxfrd     S66ypasswdd   S90webnbin
S03iptables   S14nfslock    S40atd        S75keytable    S95anacron
S05harddrake  S15gpm        S40sasauthd   S80postfix     S95innd
S08ipchains   S16ypserv     S45irda       S80prelude     S95kheader
S08ipvsadm    S17alsa       S55named      S85httpd       S99devfsd
S10network    S18sound      S55sshd       S85proftpd     S99linuxconf
S11internet   S20random     S56rawdevices S90cron        S99local
S11pcmcia     S20xfs        S56xinetd     S90mysql       S99medusa
S11portnap    S25netfs      S60lpd        S90postgresql
S12syslog     S26apnd       S60nfs        S90squid
[ root@notebook root ]#
```

Sistem, beşinci düzeye geçtiğinde, **/etc/rc.d/rc5.d** dizinindeki kabuk programlarını, isimlerinin alfabetik sırasına göre (**ls** komutuyla listelendikleri sırada) çalıştırmaya başlar.

Bunun gibi **/etc/rc.d/rc3.d** dizinindeki dosyalar sistemi üçüncü düzeye çıkarmak için başlatılacak işleri düzenleyen komut ve programları içerir.

/etc/rc.d/rc.local dosyası, sistemin açılışı tamamlandıktan sonra varsa, başlatılacak işlere ilişkin komutları içerir. Örneğin sistemin açılışı tamamlandığında birilerine bunun otomatik olarak haber verilmesini istiyorsanız **/etc/rc.d/rc.local** dosyasının içine (sonuna olabilir)

```
echo `date` Sistem acildi | mail admin@bilkent.edu.tr
```

gibi bir satır ekleyerek her açılıştan sonra **admin**'e açılış tarihini ve saatini bildiren bir e-posta gönderilmesini sağlayabilirsiniz.

Sistemdeki çeşitli servisleri başlatıp durdurmak için kullanılacak kodları içeren dosyalar **/etc/rc.d/init.d** dizininde de yer alır. Bu dizindeki dosyalar, çeşitli sunucu yazılımları başlatıp durduracak şekilde yazılmış kabuk programlarıdır. Bu dosyaları devreye almak ve devreden çıkarmak için

chkconfig

komutunu kullanmalısınız.

Örneğin, açılırken artık sisteminizde web sunucusu yazılımı olan `httpd`'nin başlatılmasını istemiyorsanız

```
chkconfig --del httpd veya chkconfig httpd off
```

komutunu verebilirsiniz. Apache web sunucusunun sisteminiz açılırken tekrar otomatik olarak çalıştırılmasını istediğinizde

```
chkconfig --add httpd veya chkconfig httpd on
```

komutu iş görecektir. Bu kitabın düzeyi açısından **chkconfig** yazılımının daha fazla ayrıntısına girmeyeceğiz, ama meraklı okuyucuların komutun man sayfalarına bir göz atmasını öneririz.

`/etc/rc.d/rcn.d` dizinlerindeki program dosyaları aslında birer dosya değil; `/etc/rc.d/init.d` dizinindeki program dosyalarına bağlantıdır; (link) `/etc/rc.d/init.d` dizinindeki dosyalar sistem yöneticilerinin oldukça sık olarak kullandıkları araçlardır. Örneğin, bir yazılım konfigürasyon değişikliği nedeniyle sisteminizin web sunucusu yazılımını durdurup yeniden başlatmanız gerekirse (sistemi kapatıp açmayı aklınıza dahi getirmeyin; o yöntem eski işletim sisteminizde kullandığınız bir yöntemdi) vermeniz gereken komut



```
/etc/rc.d/init.d/httpd restart
```

olacaktır. Bu linklerin isimlendirilme sistemi, çalışma düzeyi değişirken her bir kabuk programının nasıl bir parametreyle ve hangi sırada çalıştırılacağını gösterir. Adı "S" ile başlayanlar "start" parametresiyle; "K" ile başlayanlar "stop" parametresiyle (kill) çalıştırılır.

Aslında birçok yazılım, konfigürasyon değişikliklerinden sonra, durdurulup tekrar başlatılmak yerine bu değişikliğin kendilerine bildirilmesiyle yetinir. Örneğin, DNS sunucunuzda yeni bir sembolik isim tanıtımı yaptığınızda **named** isimli sunucu yazılımı durdurup başlatmak yerine, **ps** komutuyla **named** programının süreç numarasını öğrenip, bu sürece **HUP** (*hang-up*) mesajını gönderebilirsiniz. **named** yazılımı, **HUP** mesajı aldığı anda konfigürasyon dosyalarını yeniden okuyacak şekilde programlanmıştır.

```
ps ax | grep named  
kill -HUP 893
```

Konu dağıldı gene ya; neyse...

Sistemin Kapatılması

Tüm UNIX bilgisayarlarda olduğu gibi LINUX işletim sisteminin de adabına uygun bir şekilde kapatılması gerekir. Her ne kadar disklerinizi **ext3**, **reiserfs** gibi dosya sistemleriyle düzenleyerek enerji kesintilerine karşı önlem almış olsanız da, sistemleri düzgün kapatmak her zaman için iyi bir alışkanlıktır.

Bir LINUX bilgisayarı kapatmanın en kolay yolu, root kullanıcının herhangi bir terminalden

shutdown -h now

komutunu vermesidir.

init 0

komutu da sistemin çalışma düzeyini sıfır yapmak; yani kapatmak için kullanılabilir.

KDE'nin grafik ekranını kullanarak sistemi kapatmayı zaten şimdiye kadar çoktan keşfetmiş olmalısınız.

Acemilik dönemlerinizde bilgisayarı kapatıp açmaya (bir diğer deyişle "reboot etmeye") gereksinim duyabilirsiniz. Bu gibi durumlarda

reboot

komutunu da kullanabilirsiniz.



Deneyimli sistem yöneticileri sistemlerini reboot etmekten pek hoşlanmazlar. Bir şeyler aksamaya başladığı zaman bu aksaklığa hangi sürecin neden olduğunu bulup o süreci durdurmaya çalışırlar. Bu yöneticiler için sistemlerinin uzun süre kesintisiz çalışması (sistemin ne kadar zamandır "up" olduğu) bir övünç kaynağıdır. LINUX dünyasında "up" süreleri genellikle aylarla ölçülür. Windows sistem yöneticilerine biraz garip gelebilir ama işletim sistemi sürüm güncellemeleri ve donanıma müdahale dışında LINUX sistemlerini kapatmaya gerçekten pek fazla gerek olmaz.

Pek kolay kolay olmaz ama, sisteminize komut veremediğiniz bir duruma düşerseniz tek çözüm bilgisayarınızı anahtarından kapatıp açmak olacaktır elbette. “**x**” altında bir kilitlenme sorunu yaşarsanız Ctrl-Alt-F1 tuşlarıyla grafik olmayan bir konsola geçip sistemi toparlamanız genellikle mümkün olabilmektedir. Ctrl-Alt-F1 ile elde edeceğiniz konsolda root olarak sisteme girip adında X geçen tüm süreçleri öldürmek işe yarayabilir. Eğer bu da işe yaramazsa bu konsol ekranından “reboot” komutunu vererek sistemin düzgünce kapatılmasını sağlayabilirsiniz. Yeri gelmişken; LINUX işletim sistemi altında bu duruma genellikle donanım arızalarından dolayı düşersiniz. Eğer sık sık bilgisayarınızı kapatıp açmak zorunda kalıyorsanız bellek modüllerinizi, CPU soğutma fanını ve güç kaynağını gözden geçirmenizi öneririz.

Disklerin Yönetimi

Tüm bilgisayarların belki de en önemli kaynağı diskleridir. Daha doğrusu en kolay tükenen ve en kolay arızalanan; bu nedenle de en çok sorun çıkaran kaynak genellikle disklerdir.

Disklerinizi ve disk bölümlerinizi başarıyla yönetebilmeniz için kitabın önceki bölümlerinde anlatılmış olan “**disk bölümleme**” ve “**mount**” kavramlarını iyi anlamış olmanız gerekir.

İyi bir sistem yöneticisi her sabah disklerinin dolu/boş oranlarını şöyle bir gözden geçirip, gerekirse sabah temizliği yapmalıdır. Daha da iyi sistem yöneticileri bu işleri otomatik yapacak kabuk programları yazıp, **cron** ile her sabah çalışmasını sağlarlar.

Disklerin dolu-boş oranlarını ve durumlarını gözlemek için en uygun komut

```
df -h          veya
df -k
```

komutudur.

```
cayfer@cayfer.bilkent.edu.tr: /home/cayfer - Shell - Konsole
[cayfer@cayfer cayfer]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda1        4.0G  2.7G  1.1G   72% /
/dev/hdc2        19G   17G  1.2G   94% /depo
/dev/hda8        5.2G  4.1G  1.1G   80% /hone
/dev/hda5        6.5G  3.4G  2.8G   55% /var
/dev/hda7        2.1G   70M  1.9G    4% /var/spool/nail
[cayfer@cayfer cayfer]$

[cayfer@cayfer cayfer]$ df -k
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/hda1      4122352    2789184   1123760   72% /
/dev/hdc2      19370244   17186600  1199664   94% /depo
/dev/hda8      5350200    4265552   1084648   80% /hone
/dev/hda5      6734212    3506432   2885692   55% /var
/dev/hda7      2105808     70944    1927892    4% /var/spool/nail
[cayfer@cayfer cayfer]$
```

Göreceli olarak hızlı büyüyen sistem dosyaları genellikle **/var/log** altındaki log dosyalarıdır. **/tmp** dizini de, herkesin yazma hakkı olmasından dolayı disklerin kolayca dolmasına neden olan bir dizindir. Bu dizinleri zaman zaman kontrol edip, eski ve büyük dosyaları silmelisiniz.

/var/log dizinininde sistemde olup biten herşeyin kaydedildiği dosyalar yer alır; bu nedenle bu dizinin diskte kapladığı alan sürekli artar. Her ne kadar **logrotate** süreci bu dosyaları dönüşümlü olarak değiştirip, eskileri kaldırıp atsa da, bu dizin hiç değilse haftada bir gözden geçirilmelidir.

Bir dizinin diskte ne kadar yer harcadığını merak ettiğinizde

```
du -s /home/cayfer
```

gibi bir komutla yanıt alabilirsiniz.

```

cayfer@cayfer.bilkent.edu.tr: /home/cayfer - Shell - Konsol
[cayfer@cayfer cayfer]# du -s /home/cayfer
3751652 /home/cayfer
[cayfer@cayfer cayfer]# du /home/cayfer
4 /home/cayfer/tnp
16 /home/cayfer/bcc
7668 /home/cayfer/Desktop/Trash
16 /home/cayfer/Desktop/Renovable media
7764 /home/cayfer/Desktop
76 /home/cayfer/GNUstep/Library/AfterStep/non-configurable
88 /home/cayfer/GNUstep/Library/AfterStep/desktop/thenes
92 /home/cayfer/GNUstep/Library/AfterStep/desktop
184 /home/cayfer/GNUstep/Library/AfterStep
4 /home/cayfer/GNUstep/Library/Icons
4 /home/cayfer/GNUstep/Library/WindowMaker/Styles
4 /home/cayfer/GNUstep/Library/WindowMaker/Thenes
4 /home/cayfer/GNUstep/Library/WindowMaker/Backgrounds
4 /home/cayfer/GNUstep/Library/WindowMaker/IconSets
4 /home/cayfer/GNUstep/Library/WindowMaker/Pixmaps
4 /home/cayfer/GNUstep/Library/WindowMaker/Sounds
4 /home/cayfer/GNUstep/Library/WindowMaker/SoundSets
180 /home/cayfer/GNUstep/Library/WindowMaker

```

du komutu dizinde yer alan dosyaların toplam büyüklüğünü 1024 byte uzunluğunda “blok” cinsinden verir. Dikkat ederseniz **du** komutu, **-s** (summary) parametresiyle ilgilendiğiniz dizinin diskte işgal ettiği toplam kapasiteyi; **-s** parametresi olmadan kullanırsanız da alt dizinlerin toplam disk alanlarını rapor ediyor.

fdisk

Disklerin bölümlenme tablolarıyla ilgili işlemler için kullanılır.

fdisk /dev/hda

gibi bir komutla birinci IDE kanalındaki ilk diskin bölümlenme tablosu üzerinde çalışmaya başlayabilirsiniz. Bölümlenme tablolarıyla oynamak tehlikelidir. Ne yaptığınızı bilmeden dolu diskler üzerinde bu komutu denememenizi öneririz.

fdisk programına verilebilecek komutları görmek için programı başlattıktan sonra “**m**” seçimini kullanabilirsiniz.

```
root@notebook.igjman.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# fdisk /dev/hda

The number of cylinders for this disk is set to 2432.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
 1) software that runs at boot time (e.g., old versions of LILO)
 2) booting and partitioning software from other OSs
    (e.g., DOS FDISK, OS/2 FDISK)

Command (n for help): n
Command action
  a toggle a bootable flag
  b edit bsd disklabel
  c toggle the dos compatibility flag
  d delete a partition
  l list known partition types
  n print this menu
  n add a new partition
  o create a new empty DOS partition table
  p print the partition table
  q quit without saving changes
  s create a new empty Sun disklabel
  t change a partition's system id
  u change display/entry units
  v verify the partition table
  w write table to disk and exit
  x extra functionality (experts only)

Command (n for help): █
```

mkfs

fdisk ile bölümlenmesi yapılmış disklerde disk bölümleri üzerine dosya sistemi yaratmak için kullanılır. Örneğin:

```
mkfs -t reiserfs /dev/hda3
```

komutuyla ilk diskin üçüncü bölümü üzerine boş bir **reiserfs** dosya sistemi yaratılabilir.

Aynı iş:

```
mkfs.reiserfs /dev/hda3
```

komutuyla da yapılabilir. **mkfs** komutunun **-t** ile belirtilen parametreleri arasında **ext2**, **msdos** gibi seçenekler de bulunmaktadır. **-t** ile yaratılacak dosya sisteminin tipini belirtmezseniz **ext2** kabul edilir.

mount

mount komutuyla sisteminizde disk bölümlerindeki dosya sistemlerinin bağlanmış olduğu dizinleri görebilir; bunları çözebilir, bağlı olmayanları bağlayabilirsiniz. Daha önce ayrıntılı olarak açıkladığımız **mount** komutunu

burada yalnızca disk yönetimi ile yakından ilgili olması dolayısıyla tekrar an-
dık.

showmount -a

Bu komutla, bilgisayarınızda NFS üzerinden paylaşım açılmış disklerin kim-
ler tarafından kullanılmakta olduğunu görebilirsiniz.

```

root@notebook.lojman.bilkent.edu.tr: /root - Shell - Konsolle
[root@lists /root]# showmount -a
All mount points on lists:
cayfer:/bcc
cayfer:/home/cayfer
cayfer:/home/httpd
loj08031.lojman.bilkent.edu.tr:/disk2/mdk9.0
[root@lists /root]#

```

Yukardaki örnek listeye göre lists makinesi üzerinde paylaşım açılmış olan
“/bcc, /home/httpd, home/cayfer” dizinleri **cayfer** makinesi tarafından;
/disk2/mdk9.0 dizini de **loj08031** makinesi tarafından kullanılmaktadır.

NFS paylaşımı bir UNIX bilgisayar üzerindeki dizinlerin başka UNIX bilgi-
sayarlar tarafından “mount edilebilmesini” sağlayan servistir. Bu servisin de-
netimi, yani hangi dizinlerin hangi makineler için, bunlardaki hangi kullanıcı-
lar için paylaşım açılacağını denetimi **/etc/exports** dosyası ile yapılır.

```

root@notebook.lojman.bilkent.edu.tr: /root - Shell - Konsolle
[root@lists /root]# cat /etc/exports
/projeler      cayfer(rw) 192.168.0.3(rw,no_root_squash)
/bcc           *.bcc.bilkent.edu.tr(rw)
/usr          *.bilkent.edu.tr(ro)
/pub          (ro,all_squash)
/pub/ozel     (noaccess)

[root@lists /root]#

```

Yukardaki örnek **exports** dosyasında,

- **/projeler** dizinine **cayfer** isimli makineden gelen bağlantı isteklerine (mount isteklerine) okuma yazma ve tam yetkiyle erişim hakkı verilmiş. **cayfer** isimli makinenin IP adresi öncelikle **/etc/hosts** dosyasındaki listeden; orada yoksa DNS servisi üzerinden araştırılır.

/projeler dizinine, **cayfer** makinesinden başka bir de 192.168.0.3 IP adresli makineden oku-yaz olarak erişilmesine izin verilmiş ve bu erişimin root yetkisi ile yapabileceğini belirtilmiş. (**no_root_squash** parametresi.)

- **/bcc** dizinine **bcc.bilkent.edu.tr** ağındaki tüm makinelerden oku-yaz olarak erişilmesine izin verilmiş.
- **/usr** dizinine **bilkent.edu.tr** ağındaki tüm makinelerden yalnızca okumak için erişilmesine izin verilmiş. (*ro*)
- **/pub** dizinine heryerden yalnızca okumak için izin verilmiş, ancak erişen herkesin kullanıcı kodunun “**nobody**” kabul edilmesi ve paylaşılan **/pub** dizinindeki dosya erişim yetkilerinin bu kullanıcı koduna göre düzenlenmesi için gereken ayar yapılmış.
- **/pub** dizinine herkese erişim hakkı verilmiş olmasına rağmen bu dizinin altındaki **/pub/ozel** dizinine hiçbir şekilde dışardan erişilememesi sağlanmış.

/etc/exports dosyasında bir değişiklik yapıldığında; örneğin **/home/cayfer/public_html** gibi bir dizini paylaşım açmak için gereken satır eklendiğinde

```
exportfs /home/cayfer/public_html
```

komutuyla paylaşımı başlatabilirsiniz.

Paylaşılmakta olan bir dizini dışarıdan erişime kapatmak istediğinizde

```
exportfs -u /pub
```

gibi bir komut kullanabilirsiniz.

```
exportfs -ua
```

tüm paylaşımları kapatır.

```
exportfs -a
```

/etc/exports dosyasında adı geçen tüm paylaşımları açar.

/etc/rc.d/init.d/nfs kabuk programı NFS servislerini başlatıp durdurmak için kullanılabilir.

```
/etc/rc.d/init.d/nfs start
/etc/rc.d/init.d/nfs stop
```

gibi...

Eğer LINUX makinenizdeki bir dizini bir Windows makinenin erişimine açmak istiyorsanız NFS servisi işinizi göremeyeceği için; daha doğrusu Windows işletim sistemi NFS servislerinden nasıl yararlanılacağını bilmediği için; **samba** servisini kullanmalısınız. **samba** servisi bir LINUX bilgisayarın NT sınıfı bir sunucu gibi çalışmasını sağlar. Bir başka deyişle, Windows makineler yakınlarında gördükleri bir **samba** servisini NT sunucu zannederler. Çok ilginçtir ki, üzerinde **samba** çalışan bir LINUX makine, aynı donanım üzerinde çalışan bir NT sunucudan performans açısından daha başarılıdır. Gene politikaya girdik... Burada keselim, yoksa kalp kıracağız.



samba'nın kurulumu ve daha da önemlisi ayarlarının yapılması bu kitabın amaçları dışında kaldığı için ayrıntıya girmeyeceğiz. Aslında, Mandrake LINUX'unuzu kurarken siz aksini seçmediyseniz **samba** makinenizde kurulmuş ve çalışıyor olacaktır. **samba** kullanacaksanız, yapmanız gereken **/etc/samba/smb.conf** dosyasındaki parametreleri gereksinimlerinize göre değiştirip **samba**'yı



```
/etc/rc.d/init.d/smb restart
```

komutuyla yeni konfigürasyonla tekrar başlatmak olacaktır.

samba konfigürasyonu ile ilgili ayrıntıları

<http://www.belgeler.org>

adresindeki "Samba – Nasıl" dokümanında bulabilirsiniz.

ls of

Bilgisayarınızda bir şekilde kullanılmakta olan açık dosyaları ve soketleri listelemek için kullanılır. (Soket, TCP/IP programlamayla ilgili bir kavramdır. Ne anlama geldiğini bilmiyorsanız üzerinde durmayınız.) Çeşitli internet hizmetleri veren tipik bir LINUX bilgisayarında bu listede 10.000'den fazla dosya yer alabilir; dolayısıyla listeyi gözle taramak pek anlamlı değildir. **ls of** genellikle çıktısı **grep** ve **more** ile filtrelenerek kullanılarak belirli bir kulla-

nıcının açmış olduğu dosyaları ya da belirli bir programın kullandığı dosyaları gözlemek için kullanılır.

lsdf | grep cayfer | more

gibi.

```
root@notebook.lojman.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# lsdf | grep cayfer | more
bash      2112  cayfer  cwd    DIR      3,6    8192    309463 /home/cayfer
bash      2112  cayfer  rtd    DIR      3,6    4096    2 /
bash      2112  cayfer  txt    REG      3,6    675276 745307 /bin/bash
bash      2112  cayfer  nen    REG      3,6    539887 698241 /lib/ld-2.2.5
.so
bash      2112  cayfer  nen    REG      3,6    6876   923086 /usr/lib/gcon
v/IS08859-9.so
bash      2112  cayfer  nen    REG      3,6    22523  226702 /usr/share/lo
cale/tr/LC_COLLATE
bash      2112  cayfer  nen    REG      3,6    59     745233 /usr/share/lo
cale/tr_TR/LC_NUMERIC
bash      2112  cayfer  nen    REG      3,6    371    601093 /usr/share/lo
cale/en_US/LC_IDENTIFICATION
bash      2112  cayfer  nen    REG      3,6    29     601092 /usr/share/lo
cale/en_US/LC_MEASUREMENT
bash      2112  cayfer  nen    REG      3,6    65     601088 /usr/share/lo
cale/en_US/LC_TELEPHONE
bash      2112  cayfer  nen    REG      3,6    161    601094 /usr/share/lo
cale/en_US/LC_ADDRESS
bash      2112  cayfer  nen    REG      3,6    83     601090 /usr/share/lo
cale/en_US/LC_NAME
--More--
```

Bellek Yönetimi

LINUX işletim sisteminde bellek yönetimiyle ilgili pek fazla işiniz olmayacaktır. Eksik bellekle çalışıyorsanız, elbette ki performans sorunlarınız olacaktır. LINUX genellikle bellek eksikliği hakkında doğrudan şikayet etmez. Eğer **takas alanı** (*swap partition*) olarak ayırdığınız disk bölümü yetmiyorsa bellek yetersizliği ile ilgili mesaj alabilirsiniz. Takas alanı, gerçek belleğin yetmeme durumunda işletim sisteminin diskten yararlanması için kullanılır. Çalışan bir sürece bellek tahsis etmek gerektiğinde, ana bellekte yer kalmadıysa, beklemede olan süreçler kaldıkları yeri ve durumu işaretleyen bilgilerle birlikte diske atılır, böylece kazanılan bellek gereksinim duyan sürece tahsis edilebilir. Bu yöntem doğal olarak programların çalışmasını çok ciddi şekilde yavaşlatır. Takas alanı kullanmanın mantığı, bellek yetersizliği yüzünden programların kesilmesini önlemektir; yoksa kesin bir çözüm değildir. Takas alanınızın kullanımını sık sık gözleyip, aşırı kullanılmaya başlarsa sisteminizin belleğini arttırmalısınız. Takas alanı kullanımıyla ve süreçlerin bellek kullanımıyla ilgili bilgileri **top** komutuyla alabilirsiniz.


```

root@notebook.ijman.bilkent.edu.tr: /root - Shell - Konsol
2:04pm up 5:40, 3 users, load average: 0.00, 0.00, 0.00
113 processes: 112 sleeping, 1 running, 0 zombie, 0 stopped
CPU states: 0.0% user, 0.5% system, 0.0% nice, 99.4% idle
Mem: 255420K av, 239320K used, 15500K free, 0K shrd, 20976K buff
Swap: 248936K av, 0K used, 248936K free, 113280K cached

```

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	COMMAND
3328	root	18	0	1068	1068	816	R	0.5	0.4	0:00	top
1	root	6	0	484	484	420	S	0.0	0.1	0:04	init
2	root	9	0	0	0	0	SM	0.0	0.0	0:00	keventd
3	root	19	19	0	0	0	SMN	0.0	0.0	0:00	ksoftirqd_CPU0
4	root	9	0	0	0	0	SM	0.0	0.0	0:00	kswapd
5	root	9	0	0	0	0	SM	0.0	0.0	0:00	bdflush
6	root	9	0	0	0	0	SM	0.0	0.0	0:00	kupdated
7	root	-1	-20	0	0	0	SM<	0.0	0.0	0:00	ndrecoveryd
11	root	9	0	0	0	0	SM	0.0	0.0	0:00	kjournald
98	root	9	0	968	968	768	S	0.0	0.3	0:00	devfsd
184	root	9	0	0	0	0	SM	0.0	0.0	0:00	khud
857	root	9	0	652	652	488	S	0.0	0.2	0:00	cardmgr
872	rpc	9	0	532	532	448	S	0.0	0.2	0:00	portmap
886	root	9	0	588	588	476	S	0.0	0.2	0:00	syslogd
894	root	9	0	1144	1144	416	S	0.0	0.4	0:00	klogd
954	root	9	0	496	496	432	S	0.0	0.1	0:00	gpm

Eğer takas alanı hiç kullanılmıyorsa bilgisayarınızda gereksiniminizden daha fazla bellek var demektir. Ziyan etmemek için birazını o makineden söküp bir başkasına takabilirsiniz.

Takas alanı az geliyorsa ilk akla gelen diskin takas alanını büyütme ancak bu disk bölümlenmesinin değiştirilmesini gerektirir; bu da doğal olarak önce yedekleme, sonra diski yeniden düzenleyip (formatlayıp), dosya sistemlerini yeniden oluşturma ve yedekleri geri yükleme demektir ki, bu işlemler çalışan bir sistem için uzun süreli bir kesinti demektir.

Takas alanınız yetersiz kaldığında, takas alanı olarak ayrılan disk bölümünü yeniden oluşturmak yerine takas alanına ek yapmayı düşünmelisiniz. Bu yöntem, tek bir takas alanı kullanmak kadar yüksek performans sağlamasa da sisteminizi yeniden kurmayı göze alacağınız zamana kadar idare edecektir.

Bunun için önce disklerinizden birinde uygun boyda bir takas dosyası yaratın:

```
dd if=/dev/zero of=/tmp/ek_takas bs=1024 count=100000
```

komutu, **/tmp** altında yaklaşık 100 Mbyte uzunluğunda **ek_takas** isimli boş (daha doğrusu içi sıfırlarla dolu) bir dosya yaratacaktır. (Dosyanın blok uzunluğu 1024 byte olduğu için 100.000 blok aşağı yukarı 100 Mbyte eder.)



dd (device-to-device copy) komutu zaman zaman çok işe yarar. “**if=**” parametresi (input file) kopyalamanın nereden yapılacağını; “**of=**” parametresi de (*output file*) kopyalamanın nereye yapılacağını belirtir.

/dev/zero, aynı **/dev/null** gibi LINUX'un özel bir “çevre birimi” veya dosyasıdır. Yalnızca okunabilir. Boyu sonsuzdur; yani bu dosyadan sonsuza kadar veri okuyabilirsiniz. Ancak, okuduğunuz tüm veriler 0x00, yani ikil (*binary*) sıfırlardan oluşur.

Yukarıdaki takas dosyası yaratma komutu, **/dev/zero** dosyasından herbiri 1024 byte uzunluğunda 100000 blok okuyup bunları **/tmp/ek_takas** dosyasına kopyalıyor. Aslında, içi tamamen ikil sıfırlarla dolu 100 MByte'lık bir dosya yaratıyor.

Sonra bu dosyanın sahibini root kullanıcı yapın ve erişim yetkilerini, bu dosyaya root dışında kimsenin erişemeyeceği şekilde değiştirin:

```
chown root:root /tmp/ek_takas  
chmod 600 /tmp/ek_takas
```

Daha sonra **/etc/fstab** dosyası içine

```
/tmp/ek_takas swap swap defaults 0 0
```

satırını ekleyin.

Son olarak da yeni takas alanını devreye sokun:

```
swapon /tmp/ek_takas
```

Takas alanı değişikliklerinde bile sistemi “reboot” etmenize gerek olmadığı dikkatinizi çekti mi?

/etc/fstab'a eklediğiniz satır sayesinde sistemi her açışınızda bu takas alanı devreye girecektir.

Ek takas alanı olarak ayırdığınız disk alanına ihtiyacınız olursa

```
swapoff /tmp/ek_takas
```

gibi bir komutla, bu dosyanın takas olanı olarak kullanımına son verebilir ve dosyayı silip `/tmp` altında yer açabilirsiniz. `/etc/fstab` dosyasından ilgili satırı çıkarmayı da unutmayın ki bir dahaki sistem açılışında sorun çıkmasın.

Kullanıcı Yönetimi

Kullanıcı Hesapları

Kullanıcı hesaplarının açılıp kapatılmasının yanısıra, kullanıcıların kullanabilecekleri sistem kaynaklarını belirleme ve gerekirse sınırlama işleri de sistem yöneticisinin önemli görevlerindedir.

LINUX'ta kullanıcı hesabı açmanın pek çok yolu vardır; çünkü “hesap açma” temelde `/etc/passwd` ve `/etc/shadow` dosyalarına birer satır eklemekten oluşur.

```

root@cayfer etc]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:2:2:daemon:/sbin:/bin/sh
apache:x:72:72:system user for apache:/var/www:/bin/sh
mysql:x:78:78:MySQL server:/var/lib/mysql:/bin/bash
cayfer:x:501:501:Can Ugur Ayfer:/home/cayfer:/bin/bash
oner:x:502:502:Omer Ayfer:/home/oner:/bin/bash
sener:x:506:506:Metin Sener,php mysql:/home/sener:/bin/bash
paul:x:507:507:Paul Martin:/home/paul:/bin/bash
tulin:x:508:508:Tulin Tenizel:/home/tulin:/bin/bash
[root@cayfer etc]#

[root@cayfer etc]# cat /etc/shadow
root:$1$pXEMqqi6$3.z4q0.NjvDE.jk89A:12055:0:99999:7:::
daemon*:12055:0:99999:7:::
apache:!:12055:0:99999:7:::
mysql:!:12055:0:99999:7:::
cayfer:$1$9yQ9F/C.j$zpNbbB.JMCR1N1351:11875:0:99999:7:::1073862910
oner:$1$pk6yJ4UT$pS5CkuAbziF430/zT:11454:0:99999:7:::
sener:$1$r31z/vax$yYkkB.BTvgKtD.jn1hi:11972:0:99999:7:::1073862910
paul:$1$zMOugxSL$1B0uN439MeJOYD0.isQ:11505:0:99999:7:::-1073744384
tulin:$1$6XMeJtQ/$RnDot0/nb7juvXfS13tZHO:11519:0:99999:7:::-1073744432
[root@cayfer etc]#

```

`/etc/passwd` dosyası, adının aksine şifrelerle ilgili hiçbir bilgi içermez. Eskiden, tüm UNIX'lerde `/etc/passwd` dosyası kullanıcıların şifre dahil her türlü bilgisinin tutulduğu dosya idi. Ancak, internet yaygınlaştıkça güvenlik sorunları da artmaya başladı. Kullanım mantığı gereği `/etc/passwd` dosyasının herkesin okuyabileceği bir dosya olması, kötü niyetli kişilerin kriptolanmış da olsa kullanıcı şifrelerini alıp başka bilgisayarlarda deneme yanılma yoluyla kırma çabalarına yol açtı. Bunun üzerine `/etc/passwd` dosyasının şifre hariç tüm özellikleri aynen korunacak şekilde şifrelerin başka dosyaya, yani `/etc/shadow` isimli bir dosyaya taşınması kararlaştırıldı ve root kulla-

Kim Korkar LINUX'tan?

nıcı dışında herkesin bu dosya üzerindeki tüm yetkileri kaldırıldı. Artık modern UNIX uyarlamalarının hemen hemen hepsi kullanıcı şifrelerini **/etc/shadow** dosyasında saklamaktadır. Yeri gelmişken; UNIX dünyasında kullanıcı hesaplarını ve şifrelerini saklamanın tek yolu **/etc/passwd** ve **/etc/shadow** dosyaları değildir. Bu iki dosya, en yaygın olarak kullanılan yöntemlerdir.

Bir hesap açmak ya da kapatmak için bu dosyaları **vi** ile düzenleyebileceğiniz gibi bu işi sizin yerinize yapacak özel araçlar da kullanabilirsiniz. KDE ortamında kullanıcı hesaplarının yönetimi için **userdrake** kullanabilirsiniz. Yeni kullanıcı tanımlarken terminal penceresinden komut vermeyi yeğlerseniz

```
adduser -c "Can Ugur Ayfer" -d /home/cayfer cayfer
```

komutundan yararlanabilirsiniz. Bu komutun aslında daha birçok parametresi vardır; ancak günlük kullanımda daha fazlası pek gerekmiyor. Komutun ayrıntılarını öğrenmek isterseniz komutu parametresiz olarak verin. Kendi kullanım kılavuzunu kendisi görüntüleyecektir.

Hatırlarsanız kitabın başlarında UNIX'te kullanıcı kodlarının çok da anlamlı olmadığını, esas kimlik belirleyicisinin sayısal kullanıcı numarası olduğunu belirtmiştik. İşte bu konu şimdi gene gündeme geldi. **adduser** komutu, yeni tanıtılan kullanıcılara numara verme işini kendisi halleder; bunu yaparken de en son verilmiş numaranın bir fazlasını seçer. Bir nedenle kullanıcılarınıza kendiniz numara vererek hesap açmak isterseniz, **adduser** komutunun **-u** parametresinden yararlanabilirsiniz.

Bazen kodunu bildiğiniz ama açık adını hatırlayamadığınız; ya da tam tersine, açık adının bir kısmını da olsa bildiğiniz ama kodunu hatırlayamadığınız kullanıcılar olacaktır. Bu gibi durumlarda

finger

komutu çok işinize yarayacaktır.

Komutu "**finger ayfer**" şeklinde verirseniz, kullanıcı açık adında "**ayfer**" geçen kullanıcıların; "**finger -m ayfer**" şeklinde verirseniz de, kullanıcı kodu "**ayfer**" olan kullanıcının ayrıntılı bilgilerine erişirsiniz.

```

root@notebook.1ojman.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# finger Ugur Ayfer
Login: cayfer                               Name: Can Ugur Ayfer
Directory: /home/cayfer                     Shell: /bin/bash
On since Tue Feb 11 08:31 (EET) on vc/1     1 hour 37 minutes idle
(messages off)
On since Tue Feb 11 12:49 (EET) on pts/0    1 hour 37 minutes idle
(messages off)
On since Tue Feb 11 12:52 (EET) on pts/1    12 minutes 25 seconds idle
(messages off)
On since Tue Feb 11 14:19 (EET) on pts/2 (messages off)
No mail.
No Plan.
[root@notebook root]#

```

```

root@notebook.1ojman.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# finger -n cayfer
Login: cayfer                               Name: Can Ugur Ayfer
Directory: /home/cayfer                     Shell: /bin/bash
On since Tue Feb 11 08:31 (EET) on vc/1     1 hour 38 minutes idle
(messages off)
On since Tue Feb 11 12:49 (EET) on pts/0    1 hour 38 minutes idle
(messages off)
On since Tue Feb 11 12:52 (EET) on pts/1    12 minutes 47 seconds idle
(messages off)
On since Tue Feb 11 14:19 (EET) on pts/2 (messages off)
No mail.
No Plan.
[root@notebook root]#

```

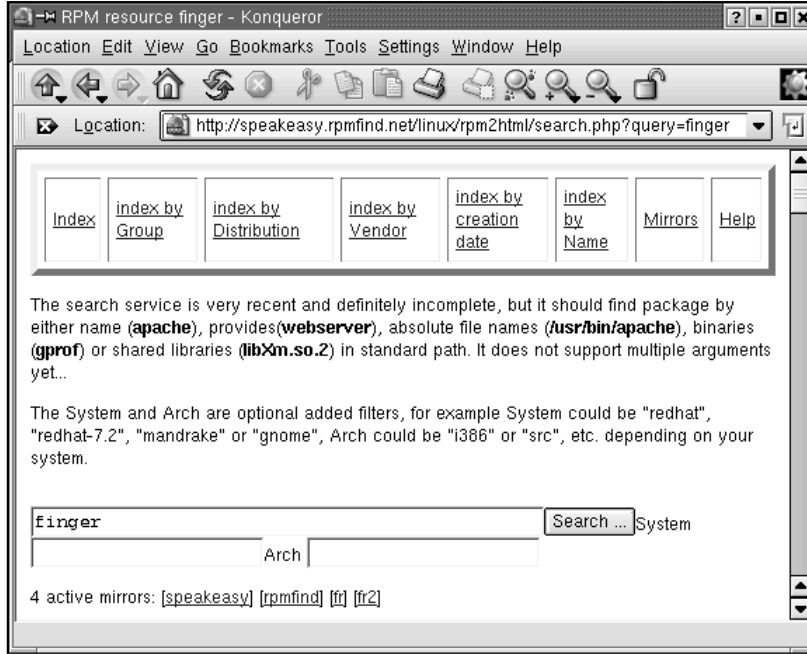
Kurulum sırasında **finger** programının kurulmasını özellikle istemediyse-
niz yukarıdaki **finger** komutu örneklerini denemek istediğinizde “**fin-
ger: command not found**” mesajını alacaksınız.

İsterseniz, yeri gelmişken **finger** programını sisteminize birlikte kuralım:

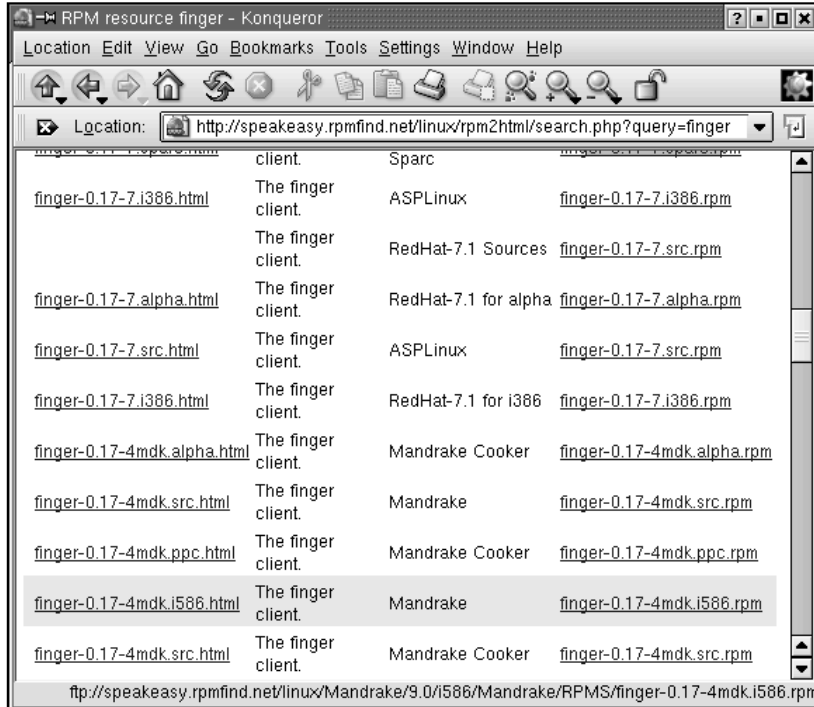
Bir LINUX programını kurmanın en kolay yolu o programın rpm paketini
(RedHat Packet Manager sözcüklerinin baş harfleri) bulup, paketi **rpm** ko-
mutuyla kurmaktır. Kurulum sırasında kurulmamış rpm paketlerini Mand-
rake dağıtım CD’lerinden birinde bulabilirsiniz; ama üç tane CD olduğunu
düşünürseniz bunlar arasında aramaktansa İnternet’te aramak daha kolay
olacaktır.

LINUX paketlerinin güncel sürümlerini indirmek için en uygun servisler-
den biri www.rpmfind.net sitesidir.

Kim Korkar LINUX'tan?



Anahtar sözcük kutusuna “**finger**” sözcüğünü yazıp aramayı başlatın.



Bulunan **rpm** paketleri arasında Mandrake dağıtımı için hazırlanmış olanlardan güncel bir sürüme ilişkin paketi seçin. Eğer varsa, adında i586, i686 geçen paketlerden birini seçin.

Adında “**src**” geçen paketler, programların kaynak kodlarını içeren paketlerdir. Kurulum için bu paketi kurduktan sonra modülleri derlemek gerekecektir. Boşyere derlemekle uğraşmamak için adında “**noarch**” (mimariden bağımsız) geçen hazır derlenmiş paketleri kurmak çok daha kolay olabilir.

Öte yandan, kendi sisteminize uyarlanması yerinde olan programlar (örneğin ekran kartınıza ve cpu cinsine göre daha iyi çalışacak şekilde derlenebilecek mplayer video oynatıcısı) kaynak kodlarından derlendiğinde daha başarılı olabilir.

finger komutunun **rpm** paketini, örneğin **/tmp** dizinine, indirdikten sonra

```
rpm -i /tmp/finger-0.17-4mdk.i586.rpm
```

komutuyla kurabilirsiniz.



Neyse, konumuza dönelim...

Bir kullanıcının hesabını kapatmak istediğinizde

```
userdel [-r] kullanıcı
```

komutunu kullanabilirsiniz. “**userdel kullanıcı**” komutu **/etc/passwd** ve **/etc/shadow** dosyalarından kullanıcı ile ilgili satırları siler. Kullanıcının (varsa) kişisel dizinini de silmek isterseniz **-r** parametresini kullanmalısınız.

Açılmış bir kullanıcı hesabıyla ilgili bilgileri değiştirmek istediğinizde

```
usermod parametre[ler] kullanıcı_adi
```

komutunu

Kim Korkar LINUX'tan?

```
[-c açık_adı]  
[-d kişisel_dizin]  
[-s kabuk]  
[-p şifre]  
[-u kullanıcı_sayısal_kodu]  
[-G grup1[,grup2[, ...]]]
```

gibi parametrelerle kullanabilirsiniz. Örneğin açık adı yanlışlıkla “Can Ugur Ayfer” olarak girilmiş olan **cayfer** kullanıcısının açık adını düzeltmek için

```
usermod -c "Can Ugur Ayfer" cayfer
```

komutunu verebilirsiniz. Bu arada tekrar hatırlatmadan geçemeyeceğiz: Aynı işi **/etc/passwd** dosyasını **vi** ya da bir başka editör ile düzenleyerek de yapabildiniz.

usermod komutunun oldukça kullanışlı üç parametresi daha vardır. Örneğin,

```
usermod -e 2002-12-31 cayfer
```

komutu, **cayfer** isimli kullanıcının şifresini 31 Aralık 2002 tarihinde geçersiz kılarak bu kullanıcının sisteme erişim hakkına son verecektir. Hesap kapanmayacak; ancak şifre bilinmeyen bir değere değiştirildiği için sistem yöneticisi yeni bir şifre verene kadar bu kullanıcı sisteme bağlanamayacaktır. Kullanıcılar şifrelerinin geçersiz kılınacağı tarih yaklaşınca sistem bu kullanıcıları uyarmaya başlar; ancak kullanıcıların bu uyarıyı görebilmeleri için sisteme “**login**” olmaları gerekir. Kabuk kullanmayan kullanıcılar (e-postalarını POP servisiyle uzaktan okuyanlar, yani sistemi doğrudan kullanmayanlar) doğal olarak bu uyarı mesajını göremeyecektir.

Bazen sistem yöneticileri bir kullanıcının hesabını geçici olarak erişilmez hale getirmek isterler. Örneğin bir hesabın bir başkası tarafından kullanıldığından şüphelendiğinizde ya da sisteminizin kullanım kurallarına uymayan kullanıcıların sisteme erişim yetkilerini geçici olarak kaldırmak istediğinizde

```
usermod -L cayfer
```

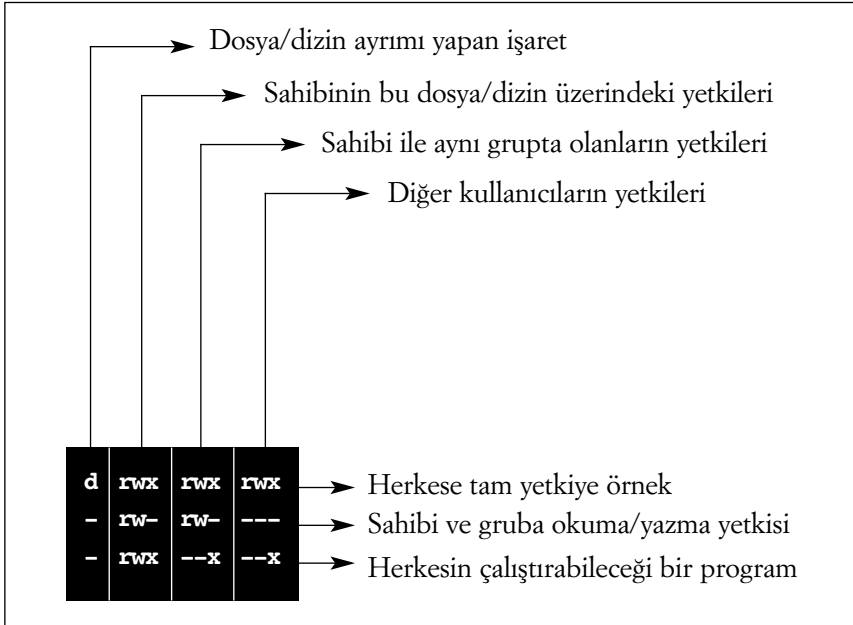
gibi bir komutla, **cayfer** isimli kullanıcının hesabını kilitleyebilirsiniz. Hesabı kilitlenmiş bir kullanıcının hesabını geri açmak için

usermod -U cayfer

komutu kullanılabilir.

Kullanıcı Grupları

Dosya erişim yetkilerini şöyle bir gözünüzün önüne getirirseniz ortadaki üçlünün “dosyanın sahibiyle aynı gruptaki kullanıcıların” yetkileri olduğunu hatırlayacaksınız.

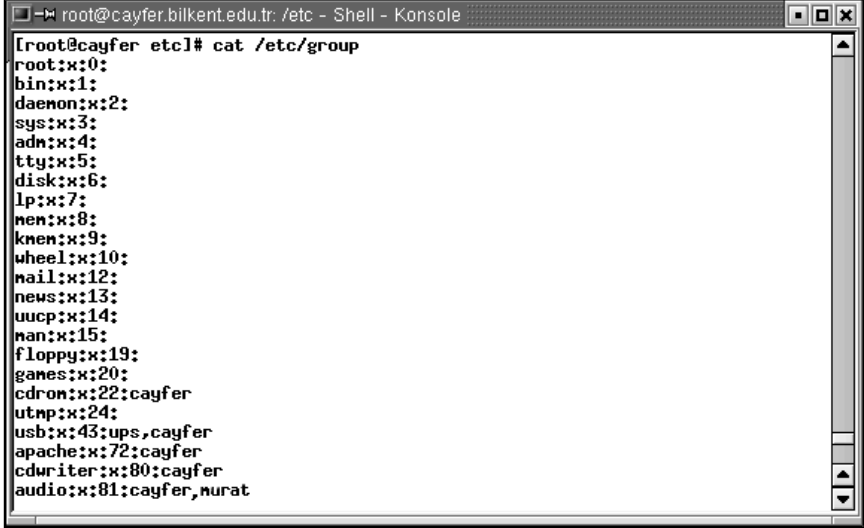


Kullanıcıları gruplayarak dosya ve dizinlere erişim yetkilerini düzenlemek oldukça kullanışlı bir yöntemdir. Örneğin, aynı yazılım projesi üzerinde çalışan tüm programcıları aynı gruba yerleştirip, bu projeye ilgili dizin ve dosyaların grup erişim haklarını istediğiniz gibi verebilirsiniz.

Bu arada herhangi bir kullanıcının birden fazla grupta yer alabileceğini de belirtmekte yarar var.

Kim Korkar LINUX'tan?

Sistemde tanımlı kullanıcı gruplarına ilişkin kayıtlar **/etc/group** dosyasında saklanır.



```
root@cayfer.bilkent.edu.tr: /etc - Shell - Konsol
[ root@cayfer etc ]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:
news:x:13:
uucp:x:14:
nan:x:15:
floppy:x:19:
games:x:20:
cdrom:x:22:cayfer
utmp:x:24:
usb:x:43:ups,cayfer
apache:x:72:cayfer
cdwriter:x:80:cayfer
audio:x:81:cayfer,murat
```

Bu dosyadaki grup tanım kayıtlarının genel formunda önce grubun adı, sonra varsa grubun şifresi, sonra grubun sayısal numarası (kullanıcı hesaplarında olduğu gibi aslında önemli olan grupların isimleri değil, sayısal kodlarıdır), sonra gereği kadar virgülle ayrılmış olarak bu grubun üyelerinin isimleri yer alır.

Sisteminize yeni bir grup eklemeniz gerektiğinde, uygun bir grup tanım kaydını **/etc/group** dosyasına herhangi bir editörle ekleyebileceğiniz gibi

groupadd [-g grup_no] yeni_grup

komutunu da kullanabilirsiniz.

Benzeri şekilde grup iptal etmek istediğinizde

groupdel grup_adi

komutunu kullanabilir veya **/etc/group** dosyasını edit edebilirsiniz.

Bir kullanıcının hangi gruplara dahil olduğunu görmek isterseniz

groups kullanıcı

komutunu kullanabilirsiniz.

Gruplarınızdan birine yeni bir kullanıcı eklemek istediğinizde en kolayı **/etc/group** dosyasını düzenleyerek ilgili grubun tanıtım kaydının sonuna bu kullanıcının adını eklemektir.

Örneğin **cayfer** isimli kullanıcıyı **apache** grubuna eklemek için **/etc/group** dosyasındaki **apache** grubuna ilişkin satırı

```
apache:x:48:webmaster,cayfer
```

olacak şekilde değiştirmeniz yeterlidir.

Kullanıcı gruplarıyla ilgili olarak sözünü etmek istediğimiz önemli bir komut daha var:

```
chgrp grup dosya
```

```
chgrp grup dizin
```

```
chgrp -R grup dizin
```

chgrp komutu bir dosyanın, bir dizinin veya altındaki herşeyle birlikte bir dizinin ait olduğu grubu değiştirmek için kullanılır. Çok büyük ölçüde **chown** komutuna benzer.

Bir kullanıcı sisteme bağlandığında kendisi için **/etc/passwd** dosyasında belirtilmiş olan grup kimliğine sahip olur. Oysa bir kullanıcının birden fazla grubun üyesi olabileceğini söylemiştik. Bir nedenle (ki bu genellikle erişim yetkileriyle ilgili bir neden olur) kullanıcı kimliğinizi değiştirmeden grup kimliğinizi değiştirmek isteyebilirsiniz. O zaman

```
newgrp grup_adi
```

komutunu kullanmalısınız. Eğer bu yeni grup şifre gerektiren bir grupsa, sizden grup şifresini girmeniz istenecektir.

Kullanıcıların bir grup kimliğine bürünmek için **newgrp** komutu kullandıklarında şifre sorulmasını istediğinizde

```
gpasswd grup
```

komutuyla o gruba bir şifre vermeniz gerekir.

Kullanıcı Disk Kotaları

Ne kadar hızlı ucuzlasa da bilgisayar sisteminizin en değerli kaynağı disk kapasitesidir. Disk kapasiteleri 5 MegaByte iken de böyleydi, 100 TeraByte olduğunda da böyle olacak. Tipik kullanıcı davranışlarından birisi de hiçbir dosyayı silmemektir. Sahipleri “*Sakla samanı gelir zamanı*” diye düşünüyor olsalar gerek, MP3 ve DIVX dosyalar kişisel dizinlerinde döner dururlar.

Bu gibi durumlarda sistem yöneticilerinin en önemli silahlarından biri **disk kota** sistemidir.

Kullanıcıların kullanabilecekleri disk alanlarını kısıtlama işlemi her dosya sistemi için ayrı ayrı yapılır, ancak pratikte kullanıcı kişisel dizinlerinin yer aldığı **/home** dizininin yer aldığı dosya sisteminde kota uygulaması yapmak yeterlidir.

Kota uygulamaya başlamadan önce sisteminizin çekirdeğinde (*kernel*) “**kota desteği**” olduğuna emin olmalısınız. Bunun için

```
grep -i quota /var/log/dmesg
```

komutunu verdiğinizde

```
VFS: Diskquotas version dquot_6.5.0 initialized
```

gibi bir yanıt alırsanız, sisteminizin çekirdeğinde kota desteği var demektir. Eğer kota desteği olmayan bir LINUX çekirdeği kullanıyorsanız, kendinize disk kotası desteği olan bir çekirdek hazırlayıp, bu çekirdeği derleyip sistemin bu çekirdekle açılmasını sağlamalısınız. Çekirdek seçeneklerinde değişiklik yapıp yeniden derleme, bu kitabın kapsamı dışında kalan ileri düzey bir iştir. Çekirdek derlemeniz gerekirse başka kaynaklara başvurmanız gerekecektir.

Kota uygulamaya başlamak için **/etc/fstab** dosyasında, kota uygulanacak dosya sistemlerine ilişkin

```
/dev/hda3 /home ext2 defaults,usrquota 1 1
```

benzeri satırlar olacak şekilde bir düzenleme yapmalısınız. (**usrquota** parametresini eklemelisiniz.)

Bu değişikliğin ardından ilgili dosya sistemini yeniden mount etmeniz gerekir. Bunun en kolay yolu

mount -a

komutunu kullanmaktır. (Sisteme bağlı kullanıcılarınız varsa, büyük olasılıkla **/home** dizini altındaki kişisel dizinlerini kullanıyor olacaklarından bu komut **/home** dosya sistemini çözüp tekrar bağlamayacaktır. Bu nedenle **mount -a** komutundan önce sistemde sizden başka çalışan kimse olmamasına dikkat etmelisiniz.)

Daha sonra bu dosya sistemi için kota sistemini çalışır duruma getirmelisiniz:

quotaon /dev/hda3

Kota sistemini ilk kez çalışır duruma getirdiğinizde

quotacheck /dev/hda3

gibi bir komutla diskte kimin ne kadar yer harcadığının ve harcama hakkı olduğunun hesabının tutulduğu **aquota.user** dosyasının yaratılmasını sağlamalısınız. Eğer birden fazla disk bölümünde kota uygulayacaksanız, **quotacheck** komutunu her bir bölüm için ayrı ayrı vermelisiniz.

Şimdi sıra kotasını sınırlamak istediğiniz kullanıcılar için **/home** dizininde oluşturabilecekleri dosyaların toplam büyüklüğünü belirtmeye geldi. Bunun için **edquota** komutunu kullanmak gerekiyor:

edquota cayfer

İşte **vi** kullanmanızı gerektiren bir noktaya geldiniz. Zamanında uyardığımız! **vi** bilmeden olmaz diye...

/dev/hda6 diskinde o kullanıcıya ait dosyalarının kotası 200 MB olur; ancak geçici bir süre için (7 gün) toplamın 220 Mbyte'a kadar çıkmasına izin verilir. Bu sürenin dolmasından sonra, kullanıcının yeni dosya kaydetmesine izin verilmez.

Sistemde disk kotası verilmiş olan tüm kullanıcıları, kotalarını ve bu kotalarının ne kadarının kullanılmış olduğunu görmek için **repquota** komutunu kullanabilirsiniz.

repquota -a

```

root@notebook.ijman.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# repquota -a
      Block limits
User  used  soft  hard  grace  File limits
      used  soft  hard  grace
root  -- 175419  0      0      0      14679  0      0
bin   -- 18000   0      0      0       735   0      0
uucp  --  729    0      0      0       23    0      0
man   --  57     0      0      0       10    0      0
cayfer -- 13046 19200 15360 806    2250 1500
oner  -- 2838   5120  6400  377   1500 1000
[root@notebook root]#

```

Log Dosyalarının Yönetimi

Log dosyalarının bir sistem yöneticisinin en önemli araçlarından olduğunu daha önce de belirtmiştik. Sisteme ne zaman kimin telnet ile bağlandığını, kimin FTP ile dosya çektiğini, kime kimden e-posta gittiğini, belirli bir saatte başlamak üzere programlanan işlerin başına neler geldiğini, sistemin açılması sırasında olup bitenleri, disk arızalarını, kimin hangi web sayfanıza baktığını ve bunun gibi birçok kayda değer olayı **/var/log** altındaki çeşitli dosyaları inceleyerek görebilirsiniz.

Log dosyaları genellikle ilgili oldukları işin adını içeren ya da anımsatan dosyalardır. Örneğin **/var/log/httpd/access.log** dosyası, web sitenizi ziyaret edenlerle ilgili bilgileri; **/var/log/messages**, sisteminizde oluşabilecek sorunlara; daha doğrusu çeşitli sistem yazılımlarının kayda değer bulduğu olaylara ilişkin kayıtları içerir.

Bazı log dosyalarını okuyabilmek için özel komutlar kullanmanız gerekebilir; örneğin sisteme telnet ile ya da konsoldan bağlanan (login eden) kullanıcıları görmek için **last** komutunu kullanmalısınız. Bu kayıtların tutulduğu

Kim Korkar LINUX'tan?

`/var/log/lastlog` dosyası basit bir metin dosyası olmadığı için **more** ya da **less** komutuyla bu log dosyasına göz atamazsınız.

```
cayfer@notebook.lojman.bilkent.edu.tr: /home/cayfer - Shell - Konsole
lcayfer@notebook cayfer]# last | more
odavid      ftp      ppp109.bcc.bilke Sun Feb  9 12:16 - 12:21 (00:05)
murat      pts/5    oper1.bcc.bilken Sun Feb  9 12:07 - 12:08 (00:01)
alkin      pts/5    labb30706.bcc.bi Sun Feb  9 11:54 - 11:54 (00:00)
robin      ftp      ppp106.bcc.bilke Sun Feb  9 11:51 - 12:07 (00:15)
odavid      ftp      ppp109.bcc.bilke Sun Feb  9 11:37 - 11:51 (00:14)
karin      pts/4    dalyan.ee.bilken Sun Feb  9 11:10 - 12:20 (01:09)
akgul      pts/2    loj04051.lojman. Sun Feb  9 10:54 - 12:28 (01:34)
rabian     ftp      pc530b.cs.bilken Sun Feb  9 10:32 - 10:32 (00:00)
rabian     pts/2    pc530b.cs.bilken Sun Feb  9 10:30 - 10:32 (00:01)
alkin      pts/2    oper1.bcc.bilken Sun Feb  9 10:21 - 10:25 (00:03)
oner       pts/2    139.179.12.190   Sun Feb  9 09:57 - 09:57 (00:00)
stephen    ftp      sbz17-a.fen.bilk Sun Feb  9 09:52 - 09:53 (00:00)
ozdemir    pts/4    pclib31.lib.bilk Sun Feb  9 09:14 - 09:24 (00:09)
ozdemir    pts/2    pclib31.lib.bilk Sun Feb  9 09:11 - 09:21 (00:10)
menderes   pts/2    firat            Sun Feb  9 07:06 - 08:32 (01:25)
cahitakn   ftp      loj15601.lojman. Sun Feb  9 05:50 - 05:51 (00:00)
murata     ftp      d79011c.dorn.bil Sun Feb  9 00:14 - 00:14 (00:00)
menderes   pts/4    oper1.bcc.bilken Sat Feb  8 23:58 - 08:32 (08:33)
fast       ftp      ppp116.bcc.bilke Sat Feb  8 23:56 - 00:12 (00:15)
fae        ftp      ppp116.bcc.bilke Sat Feb  8 23:49 - 23:56 (00:07)
nur        pts/2    slip4.bcc.bilken Sat Feb  8 23:32 - 00:02 (00:29)
arslann    ftp      charon.bcc.bilke Sat Feb  8 23:25 - 23:25 (00:00)
kaliber    ftp      loj34131.lojman. Sat Feb  8 22:59 - 23:00 (00:00)
arslann    ftp      piranha.bcc.bilk Sat Feb  8 22:39 - 22:40 (00:00)
urucbey    pts/4    139.179.89.229   Sat Feb  8 22:26 - 22:26 (00:00)
kursadd    ftp      loj15671.lojman. Sat Feb  8 20:34 - 20:38 (00:03)
--More--
```

Bir sorunun kaynağını bulmak için hangi log dosyasına bakmanız gerektiğine karar vermek ve bu dosyaların içindeki kayıtları yorumlamak biraz deneyim gerektirmektedir. Merak etmeyin, kısa zamanda bu dosyaları yorumlamayı öğreneceksiniz.



`/var/log` dizinindeki dosyalar bir UNIX sistem yöneticisinin en önemli araçlarından biridir. Neredeyse sistemde olup biten herşeyin bu dosyalarda bir kaydını bulabilirsiniz. `/var/log/dmesg` dosyasında da sisteminizin en son açılışı sırasında olup bitenlerin kaydı tutulur. Her açılıшта bu dosya yeniden oluşturulur.

Açılış sırasında, modüller ve donanım sürücülerini yükledikçe bu dosyaya kayıt düşülmür. Bu log dosyalarında hep olumsuz mesajlar yer almaz; başarıyla tamamlanan işler de buraya kaydedilir.

`/var/log/dmesg` dosyasının içeriğini görmek için

```
dmesg | less
```

komutunu kullanabileceğiniz gibi

```
less /var/log/dmesg
```

komutundan da yararlanabilirsiniz.

Log dosyalarının esas sorunu içeriklerinin yorumlanmasından çok devamlı büyüyen dosyalar olmalarıdır. Diskiniz ne kadar büyük olursa olsun, log dosyaları günün birinde bu diski de dolduracaktır. Log dosyalarının aşırı büyümesini önlemek için LINUX sistemlerde **logrotate** isimli bir program çalışır.

logrotate programının görevi arada sırada log dosyalarını arşivlemek, eskiyen arşivleri de silip atarak **/var/log** dizininin aşırı büyüüp diski doldurmasını önlemektir. Örneğin, **logrotate** programı **messages** isimli log dosyasını haftada bir kez **messages.1.gz** isimli bir dosyaya dönüştürür ve yeni log kayıtlarını yeni bir **messages** dosyasında biriktirmeye başlar. Bu arada varsa eski **messages.1.gz** dosyası **messages.2.gz**'ye, varsa eski **messages.2.gz** **messages.3.gz**'ye dönüştürülür. Tipik olarak **messages.4.gz**, **messages.5.gz**'ye dönüştürülmeden önce, varsa **messages.5.gz** silinir. Böylece log dosyaları her hafta “döndürülmüş” olur. Log dosyaların döndürülmesinde kullanılacak mantık **/etc/logrotate.conf** dosyasında belirtilir. **logrotate.conf** dosyasına kurulum sırasında yerleştirilen değerler tipik bir LINUX sunucu için son derece uygun değerler olduğu için bunları değiştirmeye gerek duymayacağınızı varsayarak bu konuda daha fazla ayrıntıya girmek istemiyoruz.

```

root@notebook.loyman.bilkent.edu.tr /root - Shell - Konsol
[root@notebook root]# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or utmp -- we'll rotate them here
/var/log/utmp {
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/lastlog {
    monthly
    rotate 1
}

# system-specific logs may be configured here
[root@notebook root]#

```

Ağ Yönetimi

Tüm UNIX sistemlerde olduğu gibi LINUX için de doğal ağ yazılımı TCP/IP üzerine kurulmuştur. Bu nedenle LINUX ağ yönetimi aslında TCP/IP ağ yönetimidir. TCP/IP ağ yönetimi başlıbaşına bir kitap konusu olduğu için bu kitapta tüm ayrıntılara girmemize olanak yok. Bir LINUX makinenin bir TCP/IP ağa nasıl bağlanacağını ve bu bağlantının nasıl denetleneceğini kısaca anlatmakla yetineceğiz.

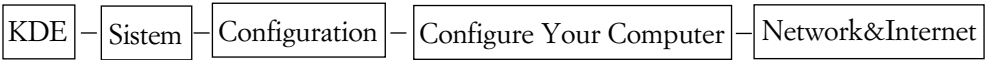
TCP/IP Ayarları

Bir bilgisayarın TCP/IP ağa bağlanabilmesi için o ağa bağlı en az bir ağ arabirimi olmalı ve bu arabirim için bir IP adresi, bir ağ geçidi (*gateway*), bir DNS sunucusu ve ağ maskesi (*netmask*) tanımlanmış olmalıdır.

Eğer bilgisayarınızı ağa Ethernet arabirimi kullanarak bağlayacaksanız bu ayarlar **/dev/eth0** adıyla erişilen ağ arabirimi için yapılmalıdır. Yok bağlantınızı bir modem aracılığıyla yapacaksanız bu ayarları **/dev/ttyS0** gibi bir isimle anılan seri arabirim veya **/dev/modem** adıyla anılan modem arabirimi için yapmalısınız. Kablo-Net veya DSL servisi üzerinden yapacağınız ağ bağlantıları için servis sağlayıcınıza danışmanızı öneririz.

Özellikle DSL bağlantılar için özel **PPPoE** (*Point to Point Protocol over Ethernet*) yazılımını kurmanız gerekebilir.

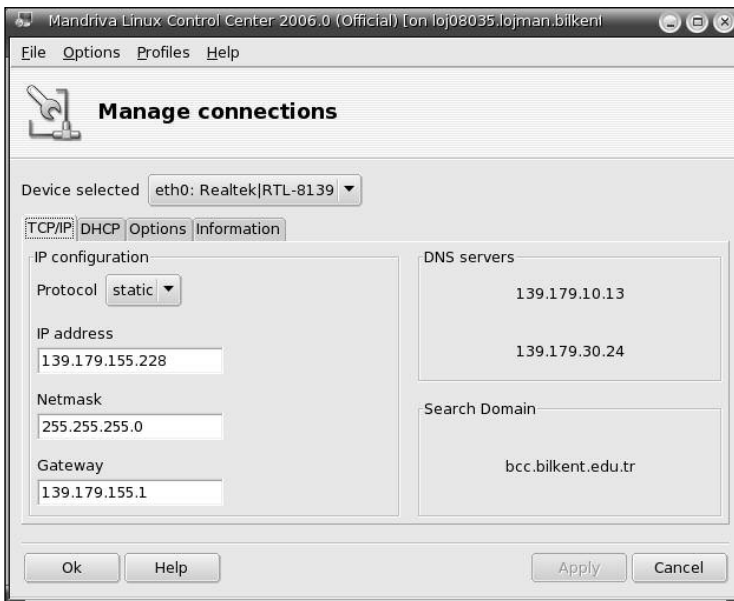
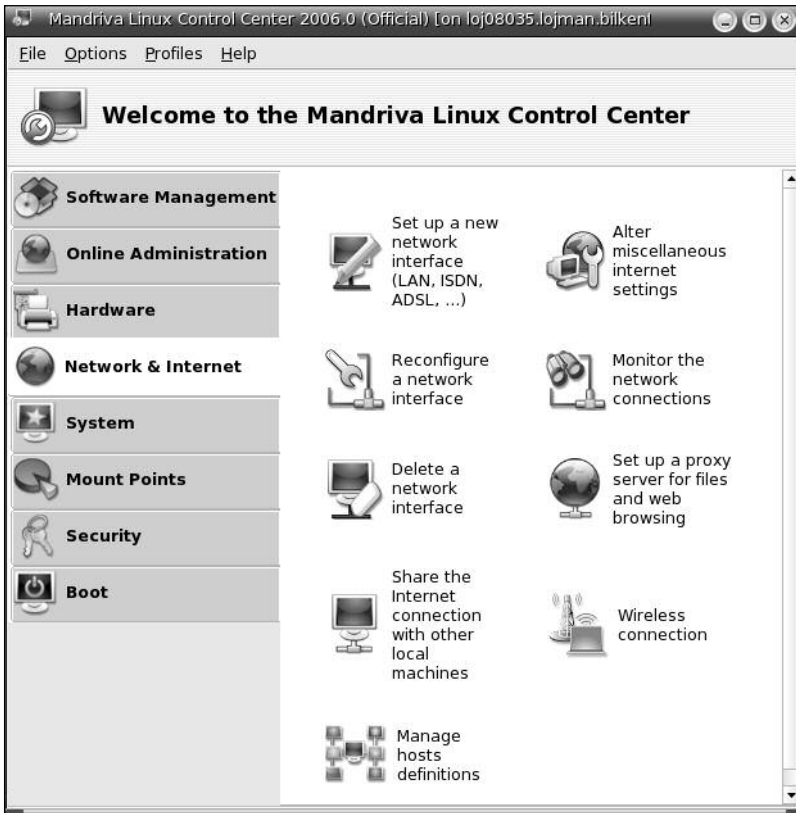
LINUX'ta TCP/IP ayarları için en kolay kullanılan araçlardan biri "**drakconf**" komutuyla da başlatılabilen "mandriva Control Venter" yazılımıdır. Bunun için:



seçimlerini yapabileceğiniz gibi root kullanıcı yetkisiyle çalışmakta olduğunuz bir terminal penceresinden

/usr/sbin/drakconf

komutunu verebilirsiniz. Her iki yöntem de bilgisayarınızın TCP/IP ayarlarını yapmak için kullanışlıdır.

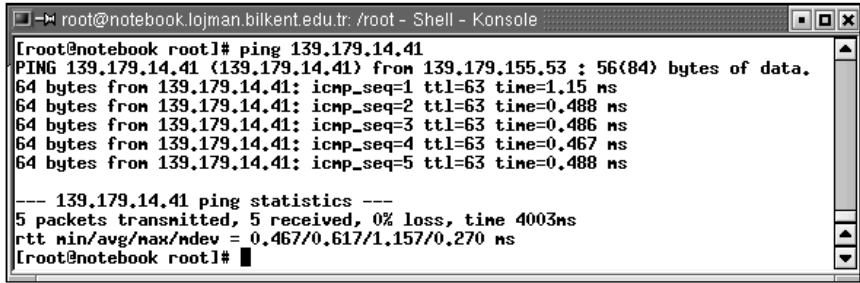


Kim Korkar LINUX'tan?

Ağ arabiriminiz ne olursa olsun, TCP/IP ayarlarınızı kontrol etmek için en kullanışlı komut **ping** komutudur:

ping 192.168.12.1

gibi bir komutla sizinle aynı ağda yer alan bir başka bilgisayara erişip erişemediğinizi kontrol edebilirsiniz. **ping** komutunun adı, masa tenisinden esinlenilmiştir. Temel olarak “*orda mısın?*” sorusu gönderip “*evet*” yanıtını bekleyen bir programdır. “*Orda mısın?*” sorusuna hiçbir zaman “*Hayır*” yanıtı gelmez.



```
root@notebook.lojman.bilkent.edu.tr: /root - Shell - Konsole
[root@notebook root]# ping 139.179.14.41
PING 139.179.14.41 (139.179.14.41) from 139.179.155.53 : 56(84) bytes of data.
64 bytes from 139.179.14.41: icmp_seq=1 ttl=63 time=1.15 ms
64 bytes from 139.179.14.41: icmp_seq=2 ttl=63 time=0.488 ms
64 bytes from 139.179.14.41: icmp_seq=3 ttl=63 time=0.486 ms
64 bytes from 139.179.14.41: icmp_seq=4 ttl=63 time=0.467 ms
64 bytes from 139.179.14.41: icmp_seq=5 ttl=63 time=0.488 ms

--- 139.179.14.41 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4003ms
rtt min/avg/max/ndev = 0.467/0.617/1.157/0.270 ms
[root@notebook root]#
```

Hattınızın kalitesini; yani paket kaybı olup olmadığını kontrol etmek için 1500 byte uzunluğunda paketleri sürekli gönderebilirsiniz:

ping -s 15000 -c 200 192.168.12.1

Yerel ağda bir bilgisayara sorunsuz ulaştığınıza emin olduktan sonra

ping 128.12.3.66

gibi bir komutla sizin ağın dışında yer alan ve çalışır durumda olduğuna emin olduğunuz bir bilgisayarı ping'lemeyi deneyin. Başarısız olursanız kontrol edilmesi gereken ilk ayar ağ geçidi ayarınızdır.

Bir sonraki aşama DNS sunucu ayarlarınızı kontrol etmek amacıyla ping'lenecek bilgisayarın IP adresi yerine adını kullanmak olacaktır:

/bin/ping www.sunucu.com.tr

gibi bir komutla **www.sunucu.com.tr** makinesini de ping'leyebiliyorsanız bilgisayarınız sembolik internet adreslerinden sayısal IP adreslerini çözümlenebiliyor demektir. Üstelik ağ geçidiniz olan yönlendiricinin ayarlarını da doğrulamış olursunuz.

drakconf için “TCP/IP ayarlarını yapmak için kullanılan en kolay araçlardan biri” demiştik. TCP/IP ayarlarıyla ustaların yaptığı gibi konsoldan oynamak istediğinizde kullanmanız gereken komutlardan biri **ifconfig** komutudur.

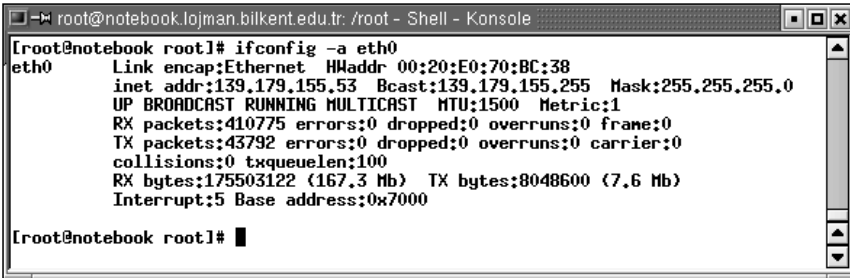
```
/sbin/ifconfig eth0 192.168.10.3 netmask 255.255.255.0  
broadcast 192.168.10.255
```

(Aslında bu komut tek satır olmalı ama sayfaya sığmadı, ne yapalım.)

/dev/eth0 ağ arabiriminizin ne durumda olduğunu, hangi IP adresine ayarlı olduğunu, çalışmaya başladığından bu yana kaç paket gönderdiğini ve aldığı, bu transferler sırasında ne kadar iletişim hatası olduğunu

```
/sbin/ifconfig -a eth0
```

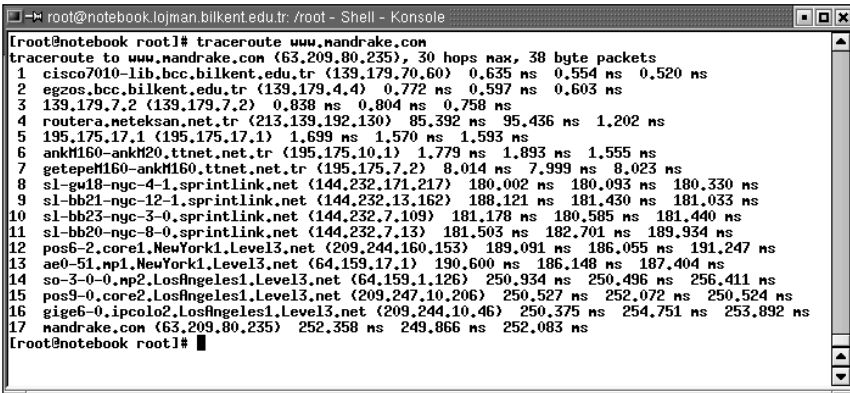
komutuyla görebilirsiniz.



```
[root@notebook root]# ifconfig -a eth0
eth0      Link encap:Ethernet  HWaddr 00:20:E0:70:BC:38
          inet addr:139.179.155.53  Bcast:139.179.155.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:410775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43792 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:175503122 (167,3 Mb)  TX bytes:8048600 (7,6 Mb)
          Interrupt:5 Base address:0x7000

[root@notebook root]#
```

traceroute komutuyla bir başka ağdaki bilgisayara gönderdiğiniz paketlerin izlediği yolu gözleyebilirsiniz. Bu komut, yerel ağınızın internet’e birden fazla çıkışı olduğu durumlarda çok işe yarayacaktır.



```
[root@notebook root]# traceroute www.mandrake.com
traceroute to www.mandrake.com (63.209.80.235), 30 hops max, 38 byte packets
 1  cisco7010-lib.bcc.bilkent.edu.tr (139.179.70.60)  0,635 ns  0,554 ns  0,520 ns
 2  egzos.bcc.bilkent.edu.tr (139.179.4.4)  0,772 ns  0,597 ns  0,603 ns
 3  139.179.7.2 (139.179.7.2)  0,838 ns  0,804 ns  0,758 ns
 4  routera.neteksan.net.tr (213.139.192.130)  85,392 ns  95,436 ns  1,202 ns
 5  195.175.17.1 (195.175.17.1)  1,699 ns  1,570 ns  1,593 ns
 6  ankM160-ankM20.ttnet.net.tr (195.175.10.1)  1,779 ns  1,893 ns  1,555 ns
 7  getepeM160-ankM160.ttnet.net.tr (195.175.7.2)  8,014 ns  7,999 ns  8,023 ns
 8  s1-gw18-nyc-4-1.sprintlink.net (144.232.171.217)  180,002 ns  180,093 ns  180,330 ns
 9  s1-bb21-nyc-12-1.sprintlink.net (144.232.13.162)  188,121 ns  181,430 ns  181,033 ns
10  s1-bb23-nyc-3-0.sprintlink.net (144.232.7.109)  181,178 ns  180,585 ns  181,440 ns
11  s1-bb20-nyc-8-0.sprintlink.net (144.232.7.13)  181,503 ns  182,701 ns  189,934 ns
12  pos6-2.core1.NeuYork1.Level3.net (209.244.160.153)  189,091 ns  186,055 ns  191,247 ns
13  ae0-51.np1.NeuYork1.Level3.net (64.159.17.1)  190,600 ns  186,148 ns  187,404 ns
14  so-3-0-0.np2.LosAngeles1.Level3.net (64.159.1.126)  250,934 ns  250,496 ns  256,411 ns
15  pos9-0.core2.LosAngeles1.Level3.net (209.247.10.206)  250,527 ns  252,072 ns  250,524 ns
16  gige6-0.ipcolo2.LosAngeles1.Level3.net (209.244.10.46)  250,375 ns  254,751 ns  253,892 ns
17  mandrake.com (63.209.80.235)  252,358 ns  249,866 ns  252,083 ns

[root@notebook root]#
```

Kim Korkar LINUX'tan?

Ağ bağlantınızın genel durumu ile ilgili ayrıntılı bilgi almak istediğinizde **netstat** komutu çok işinize yarayacaktır. Özellikle sizin bilgisayarınızla herhangi bir TCP/IP bağlantısı olan bilgisayarları görmek için çok kullanışlı bir komuttur.

“/bin/netstat -s” bilgisayarınızın TCP, UDP, ICMP trafik istatistiklerini listeler. Bunların ne anlama geldiğini bilmiyorsanız hiç dert etmeyin. O kadar da önemli değil.

“/bin/netstat -r” bilgisayarınız tarafından kullanılmakta olan yönlendirme tablosunu gösterir. Bilgisayarınızı bir yönlendirici (*router*) olarak kullanıyorsanız çok işinize yarayacaktır.



Yönlendiriciler, TCP/IP ağların belkemiğini oluşturur. Yönlendiriciler birden fazla bilgisayar ağını birbirine bağlamak için kullanılır. Örneğin, işyerinizdeki 50 bilgisayarı internet'e bağlamak istediğinizde şirketinizin ağını internet servis sağlayıcı kuruluşun bilgisayar ağına bağlayabilmek için bir yönlendirici kullanmanız gerekir. Bir modemle basit bir PPP bağlantısı bile kursanız aslında bu PPP bağlantıyı sağlayan bilgisayar bir yönlendirici olarak görev yapacaktır. Kullanılacak yönlendiricinin ağ arabirim sayısı ve çeşitleri bağlantı ortamına ve ağ gereksinimlerine göre büyük çeşitlilik gösterse de ilke olarak hepsi aynıdır: Birden fazla ağ üzerinde oturan ve gelip giden paketleri varış adreslerine göre uygun arabirime yönelten bilgisayarları “yönlendirici” (*router*) denir.

Piyasada satılmakta olan yönlendiricilerin neredeyse tamamının salt yönlendirme işi yapacak şekilde, disksiz olarak UNIX işletim sistemiyle çalışabilen birer bilgisayar olduğunu düşünürseniz LINUX işletim sistemi ile kursuz bir yönlendiriciyi çok ucuza kurabilirsiniz.

Çok sayıda meslektaşımız bu uygulamaya “arkasında ciddi bir firma olmadığı” gerekçesiyle karşı çıksa da, deneyimlerimiz 30.000 ABD doları tutarında yüksek performanslı bir yönlendirici yerine 2.000 ABD Doları karşılığında iki adet PC (bir tanesi yedek olarak hazır tutulmak üzere) ve LINUX işletim sistemiyle 3 internet bağlantısı olan, yaklaşık 5.000 bilgisayardan oluşan bir ağa mükemmel yönlendirme ve ateş duvarı (*firewall*) koruması sağlanabileceğini göstermiştir.

“/bin/netstat -a” bilgisayarınız üzerinde kurulu bulunan TCP/IP bağlantılarını, bu bağlantıların kullandığı port numaralarını ve bağlı bilgisayarın IP adreslerini veya açık adlarını listeler.

```

cayfer@notebook.lojman.bilkent.edu.tr: /home/cayfer - Shell - Konsolle
[root@charon /root]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 charon.bcc.bilkent.:www 195.87.142.4:1039      ESTABLISHED
tcp      0      0 charon.bcc.bilkent.:www 195.112.138.253:3280  ESTABLISHED
tcp      0 256 charon.bcc.bilkent.:ssh  firat.bcc.bilkent:48218 ESTABLISHED
tcp      0      0 charon.bcc.bilkent.:3552 139.179.11.24:inap2   TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:www 195.112.138.253:3279  TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:3551 139.179.11.24:sntp    TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:www  vp180129.reshsg.uc:1679 ESTABLISHED
tcp      0      0 charon.bcc.bilkent.:www  vp180129.reshsg.uc:1679 FIN_WAIT2
tcp      0      0 charon.bcc.bilkent.:3550  firat.bcc.bilkent:inap2 TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:www 195.112.138.253:3277  TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:www 195.112.138.253:3276  TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:www 195.112.138.253:3275  TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:3549  firat.bcc.bilkent:inap2 TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:3548  firat.bcc.bilkent:inap2 TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:3547 139.179.11.24:inap2   TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:www 217.131.5.151:36741   TIME_WAIT
tcp      0      0 charon.bcc.bilkent.:2721  firat.bcc.bilkent:inap2 ESTABLISHED
tcp      0      0 charon.bcc.bilkent.:www  ads1-64-171-7-189.:3287 CLOSE
tcp      0      0 charon.bcc.bilkent.:ssh  firat.bcc.bilkent:39285 ESTABLISHED

```

DNS çözümlemesi yapmak için kullanılan **host** komutunu

```
host www.mandriva.com
```

şeklinde kullanırsanız, bilgisayarınızın TCP/IP ayarları arasında belirtilmiş olan DNS sunucusundan **www.mandriva.com** bilgisayarının IP adresi sorulacaktır. Eğer birden fazla DNS sunucusu tanıtılmışsa ve birinciden yanıt gelmezse sorgu ikinci DNS sunucusuna yönlendirilecektir.

```

root@notebook.lojman.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# host cayfer.bilkent.edu.tr
cayfer.bilkent.edu.tr has address 139.179.14.40
[root@notebook root]#

[root@notebook root]# host 139.179.14.40
40.14.179.139.in-addr.arpa domain name pointer cayfer.bilkent.edu.tr.
[root@notebook root]#

```

Komutu

```
host www.cnn.com 128.12.34.1
```

şeklinde verirseniz **www.cnn.com** sembolik adresinin sayısal IP adresine iliş-

Kim Korkar LINUX'tan?

kin sorgu TCP/IP ayarlarındaki DNS sunucusuna değil, 128.12.34.1 IP adresli bilgisayara yönlendirilir.

Komutu

host 64.236.16.52

şeklinde bir IP adresiyle verirseniz, verdiğiniz IP adresinin hangi sembolik adrese karşılık geldiği sorgulanır.

Ağ yöneticileri zaman zaman *“falanca ağ / makine kime ait acaba?”* sorusuyla karşılaşır. Örneğin **abc.com** diye bir ağdan bilgisayarınıza yönelik bir saldırı olduğunda bu ağın hangi kişi ya da kuruluşa kayıtlı olduğunu bulma gereğini hissedersiniz. Eğer ağın bir web sunucusu var ve burada da iletişim için e-posta adresi, telefon numarası varsa sorun olmaz. Ancak her zaman bu bilgileri bulamayabilirsiniz. Tüm internet “domain” isimlerinin kaydedilmesi gereğinden yola çıkarak sözkonusu ağın adının kimin üzerine kayıtlı olduğunu bulabilirsiniz. (Kötü niyetli kişiler gerçek isim ve telefonlarını vermezler ama olsun, bir ipucudur genede...)

Bu iş için **whois** programından yararlanabilirsiniz. (Eğer yazılım yönetimi bölümünde verdiğimiz örneği uygulamadıysanız **whois** programı bilgisayarınızda yüklü olmayacaktır.)

```
root@cayfer.bilkent.edu.tr: /root - Shell - Konsolle
[root@notebook root]# whois google.com
Registrant:
  Google Inc.
  (DOM-258879)
  2400 E. Bayshore Pkwy Mountain View
  CA
  94043 US

Domain Name: google.com

Registrar Name: Alldomains.com
Registrar Whois: whois.alldomains.com
Registrar Homepage: http://www.alldomains.com

Administrative Contact:
  DNS Admin
  (NIC-1340142)
  Google Inc.
  2400 E. Bayshore Pkwy Mountain View
  CA
  94043 US
  dns-admin@google.com +1.6503300100 Fax- +1.6506181499
Technical Contact, Zone Contact:
  DNS Admin
  (NIC-1340144)
  Google Inc.
  2400 E. Bayshore Pkwy Mountain View
  CA
  94043 US
  dns-admin@google.com +1.6503300100 Fax- +1.6506181499
```


Yazıcı Yönetimi

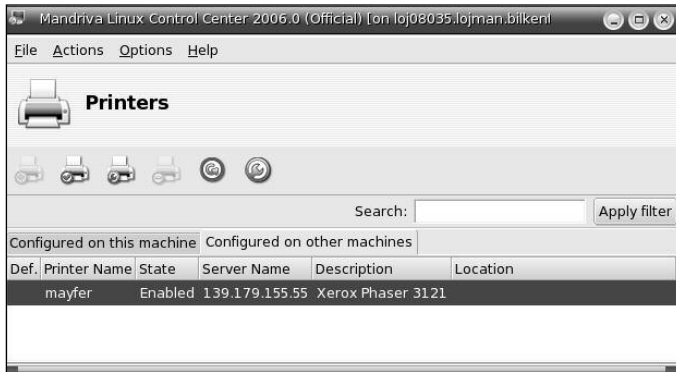
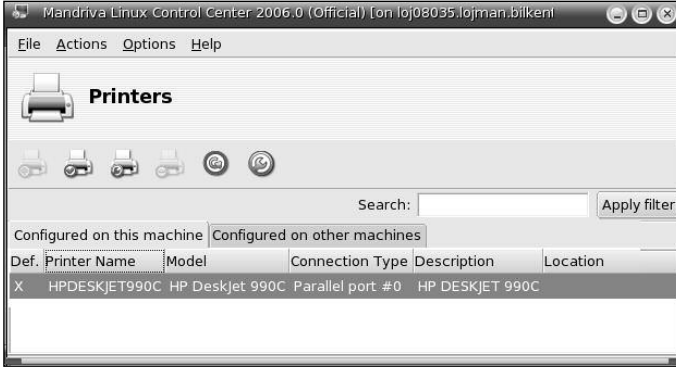
Genel olarak UNIX sisteminde yazıcı yönetimi sistem yöneticilerinin pek sevmediği bir konu olagelmıştır. Ancak, LINUX'un yaygınlaşmasıyla birlikte son derece başarılı ve kolay kullanılan yazıcı denetim sistemleri geliştirilmiştir. Bunların günümüzde en yaygın olarak kullanılanı **CUPS**'dir. (*Common UNIX Printing System*)

Doğrudan bilgisayarınıza da bağlı olsa, bir ağ yazıcısı da olsa, yazıcınızı CUPS ile yönetmenizi öneririz.

Doğal olarak ilk iş yazıcınızın sisteme tanıtılmasıdır. Bunun için Mandriva Control Center içinde **“Hardware”** ve **“Printers”** seçimlerini yaparak işe başlayabilirsiniz.



CUPS ile hem doğrudan bilgisayarınıza bağlı (local) yazıcıları; hem de ağ üzerinden erişilebilen yazıcıları (network printer) kullanabilirsiniz.



Kim Korkar LINUX'tan?

CUPS sunucunuzu bir web tarayıcısıyla yönetebilirsiniz. Bunun için **cupsd** isimli daemon yazılımının arka planda çalışıyor olması gerekir. Bu son cümleyi eski konuları gözden geçirmek için bir fırsat olarak değerlendirmek istiyoruz



- **cupsd** yazılımının arka planda çalışıp çalışmadığı nasıl kontrol edilir?

"**ps -ax | grep cupsd**" komutuyla sisteminizde çalışmakta olan tüm süreçlerin listesinden, içinde "**cups**" sözcüğü geçen satırları listeleyebilirsiniz.

- **cupsd** yazılımını arka planda çalışmıyorsa nasıl çalıştırılır?

"**/usr/sbin/cupsd &**" komutuyla **cupsd** programını arka planda çalıştırabilirsiniz. ("**&**" karakterinin işlevini hatırladınız, değil mi?)

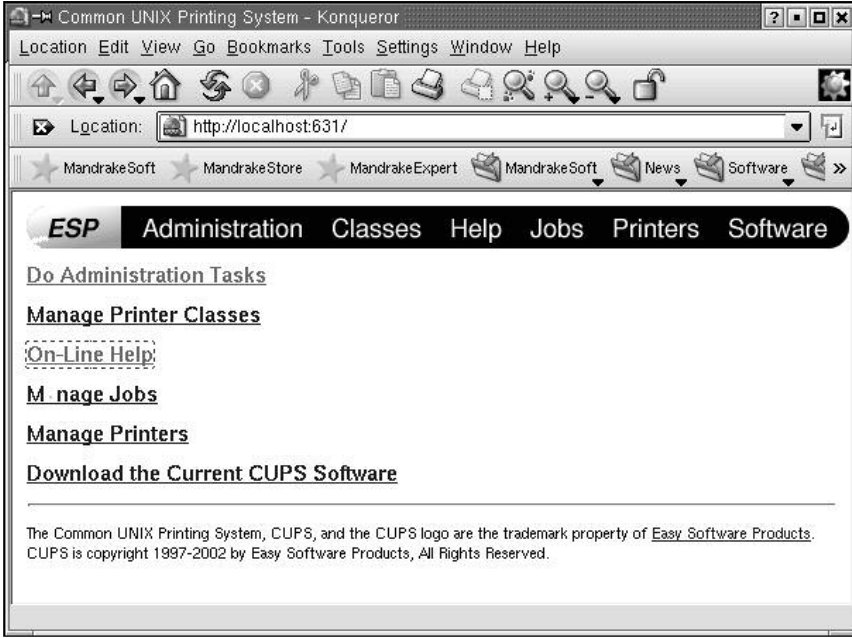
- **cupsd** yazılımını yüklü değilse ne yapmalı?

Yüklemeli... "Mandriva Control Center" sonra "Install Software"...

- **cupsd** yazılımının sistemin her açılışında otomatik olarak başlaması için ne yapmalı? (Her açılıştan sonra konsoldan root olarak "**/usr/sbin/cupsd &**" komutunu vermek zorunda kalmak hiç de hoş değildir doğrusu.)

"**chkconfig --add cups**" komutuyla **/etc/rc.d** dizinindeki düzenleme yapıldığını sağlayabilirsiniz.

Evet, artık **cupsd** servisi çalıştığına göre CUPS denetimini web tarayıcıyla yapmak üzere beğendiğiniz web tarayıcısını çalıştırıp URL olarak **http://localhost:631** girebilirsiniz. Web tabanlı CUPS yöneticisi, standard http portu olan 80 numaralı port üzerinden değil, kendisine özel 631 numaralı port üzerinden servis verir.



Yedekleme

Sistem yöneticisinin en önemli görevi ya da önemli iki-üç görevinden biri “**yedekleme**”dir. Bilgisayarınızı hiç bozulmayacakmış gibi kullanmalı ama her dakika çökecekmiş gibi yedeklemelisiniz. Arızalanan bir diski değiştirmek kolay ve ucuzdur; ancak uygulama yazılımlarını tekrar baştan kurmak, sistem ayarlarını yeniden yapmak, özellikle de kayıtlı verileri yerine koymak çok zordur. Hatta bazen olanaksız olabilmektedir.

Sisteminizde yapılan işlerin önemine ve erişebildiğiniz donanım kaynaklarının özelliklerine göre kendinize özgü bir yedekleme stratejisi geliştirmeli ve bu stratejiye harfi harfine uymalısınız. Örneğin değerli dosyalarınızı ve dizinlerinizi periyodik olarak bir ikinci disk üzerine ya da daha iyisi, bir başka bilgisayara kopyalamalısınız.

Tipik bir LINUX sisteminde en değerli sistem dosyaları **/etc**, **/var** ve **/usr/local** dizinlerinde yer alır. **/home** da özenle yedeklenmesi gereken bir dizindir.

Kim Korkar LINUX'tan?

Daha önceki bölümlerde yedekleme için **tar** komutunu önermiştik. Aslında iki önemli yedekleme aracı daha vardır:

- **dump**
- **rsync**

dump büyük sistemlerde özellikle teyp kasetlerine yedekleme için kullanılır. Kullanması biraz deneyim gerektirir. Bu yüzden bu kitapta **dump** komutunun ayrıntılarına girmeyeceğiz. **dump** ile yedek alırken ayda bir “**tam yedek**” alıp, sonra da her gün “**artımlı yedekleme**” yapabildiğinizi belirtmek isteriz. (*incremental backup*, Türkiye Bilişim Derneği, Bilişim Terimleri Sözlüğü, <http://www.tbd.org.tr/sozluk.html>) “**Artımlı yedekleme**” de, en son tam yedeklemeden bu yana değişen dosyalar yedeklenir. Böylece yedekleme çabuk biter. Günümüzün tipik sunucu disk kapasitelerinin yüzlerce gigabyte olduğunu ve bu kapasiteleri yedeklemenin teyp veri transfer hızlarıyla saatlerce süreceğini düşünürseniz artımlı yedeklemenin ne denli önemli olduğunu kabul edersiniz herhalde.

rsync diskten diske ya da yerel bir ağ üzerinde makineden makineye yedekleme için kullanılabilen çok kullanışlı bir araçtır. Temel mantığı iki dizini senkronize etmektir.

Diyelim ki alçakgönüllü bir ağın yönetiminden sorumlusunuz ve ortalıkta bazı önemli dizinlerini yedeklemek istediğiniz on tane makine var. Her gece yarısı bu makinelerden **rncp** komutuyla yedeklemek istediğiniz dizin ve dosyaları yedekleme makinesine kopyalayabilirsiniz.

web sunucusunda

```
rncp -r /home depo:/web
```

```
rncp -r /etc depo:/web
```

e-posta sunucusunda

```
rncp -r /var/spool/mail depo:/mail
```

ya da

depo makinesinde

```
rncp -r web:/home /web
```

```

rcp -r web:/etc /web
rcp -r mail:/var/spool/mail /mail
rcp -r muhasebe:/var/data /mhsb

```

gibi komutlar vererek bu şekilde bir yedekleme yapılabilir.

Ancak on makine için bu işler oldukça uzun sürecektir. Onun için **r**cp ile kopyalamak yerine **r**sync ile yalnızca değişen dosyaları kopyalamayı düşünebilirsiniz.

depo makinesinde vereceğiniz

```

/usr/bin/rsync -az muhasebe:/var/data/ /mhsb/var/data

```

komutuyla muhasebe makinesindeki **/var/data** dizinindeki dosya ve alt dizinlerle komutun verildiği makinedeki **/mhsb/var/data** dizinindeki dosyalar ve alt dizinlerin son değişiklik tarihleri karşılaştırılır. Eğer **muhasebe** makinesindeki dosya ve dizinlerin tarihi daha yeniyse, o dosyalar komutun verildiği makineye (**d**epo makinesine) kopyalanır.

Önemli bir nokta da şu: Daha önce yedeklenmiş olan **mhsb:/var/data** dizinindeki **2002_bilancio** isimli bir dosya **muhasebe** makinesinden silinirse, **d**epo'daki kopyası kalacaktır, çünkü son değişiklik tarih-saat karşılaştırması yalnızca gönderen makinedeki dosya ve dizinler için yapılır. Aslında bu özellik arada sırada işe de yarar. Yanlışlıkla silinmiş birçok dosyayı bu özellik sayesinde kurtarmak mümkün olabiliyor. Ancak bu “kalıntı” dosyalar büyük dosyalarsa, o zaman da disk kapasitesi sorununa yol açabiliyor. Eğer bu gibi durumlarda gönderici makinede yok olmuş dosyaların altı makineden de silinmesini isterseniz **r**sync komutunu **--delete** parametresiyle kullanabilirsiniz.

```

/usr/bin/rsync -az --delete muhasebe:/var/data/ /mhsb/var/data

```

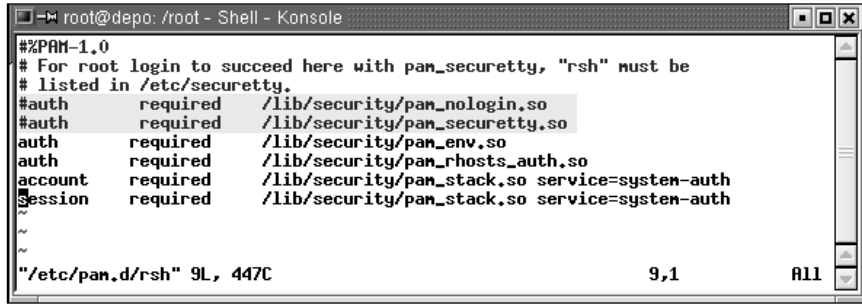
rsync programını kullanarak makineler arası yedekleme yapabilmemiz için hem gönderen hem alan makinelerde **r**sync ve **r**sh modülleri kurulu olmalıdır. Yedekleme işini genellikle root yetkisiyle yapmak isteyeceğiniz için güvenlik duvarlarını aşmak için yapmanız gereken iki iş daha olacaktır:

1. Gönderici makine üzerinde **/root** dizininde yani root kullanıcının kişisel dizininde adı **.rhosts** olan bir dosya yaratmalı ve bu dosyanın içine

192.168.0.12 root cayfer

gibi bir satır eklemelisiniz. Burada 192.168.0.12 yalnızca bir örnek olup, “diğer makine”nin IP numarası olarak değerlendirilmelidir. Bu satır, 192.168.0.12 IP adresli bilgisayardan gelen “root” ve “cayfer” kimlikli kullanıcıların her iki makinede de tanımlı olmak kaydıyla aynı kimliklerle kabul edilmelerini sağlamak içindir. **.rhosts** dosyasını düzenlerken liberal olmamanızı öneririz; önemli bir güvenlik geđiğ açabilirsiniz.

2. İkinci olarak da **/etc/pam.d/rsh** dosyasında **pam_nologin.so** ve **pam_securetty.so** satırlarının başına birer “#” yerleştirerek bu seçimleri geçersiz kılmalısınız. (Bunun neden yapıldığını ve pam’ın ne olduğunu açıklamak biraz zor. Yeni başlayanlar için “pam” sözcüğünün “Password Authentication Module” isminin kısaltması olduğunu ve kullanıcıların özellikle ağ üzerinden yapabilecekleri işlerde yetki ve şifre değerlendirmelerinin nasıl yapılacağını belirleyen bir servis olduğunu açıklamak yeterli olacaktır. Güvenlik konusunda deneyim kazandıkça pam konusunda da bilginiz ve hakimiyetiniz artacaktır.)



```
root@depo: /root - Shell - Konsolle
#%PAM-1.0
# For root login to succeed here with pam_securetty, "rsh" must be
# listed in /etc/securetty.
#auth required /lib/security/pam_nologin.so
#auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_env.so
auth required /lib/security/pam_rhosts_auth.so
account required /lib/security/pam_stack.so service=system-auth
Session required /lib/security/pam_stack.so service=system-auth
" /etc/pam.d/rsh" 9L, 447C 9,1 ALL
```

Periyodik İşlerin Yönetimi

Sisteminiz geliştikçe, daha doğrusu sisteminize bağımlılığınız arttıkça sistem yöneticisi olarak üstlendiğiniz sorumluluklar da artacaktır. Kullanıcılarınıza “*disk dolmuş da ondan falanca servis çalışmıyormuş*” dememelisiniz.

Bu sorumluluğun gereği olarak bazı işlerin periyodik olarak yapılması gerekecektir. Örneğin belirli dizinlerin her akşam yedeğinin alınması, her Pazartesi belirli geçici dizinlerin temizlenmesi, her gün 6 saate bir bazı raporların hazırlanıp müşteriye ya da patrona e-posta ile gönderilmesi gibi...

Bu şekilde belirli bir plana-programa bağlanmış işler LINUX altında **cron** servisinin desteğiyle yapılır.

cron servisi aslında üç unsurdan oluşur:

1. **crond**: cron daemon, geri planda pusuda yatan, yapılacak işlerin zamanının gelmesini bekleyen yazılım.
2. **cron dosyaları**: Her kullanıcı için hangi saatlerde, günlerde hangi işlerin yapılacağını saklandığı dosyalar. (**/var/spool/cron** altında, her kullanıcı için, kullanıcının adıyla anılan bir dosya yer alır.)
3. **crontab komutu**: Kullanıcının cron dosyalarını düzenlemek için kullanacağı komut.

/var/spool/cron altındaki dosyaları elle düzenlememelisiniz. Bu dosyalarda bir değişiklik yapmanız gerektiğinde

crontab -e

komutunu kullanmalısınız. **-e** parametresi dosyayı düzenlemek istediğinizi (*edit*) belirtmektedir.

crontab komutu, komutu veren kullanıcıya ait **cron** dosyasını **vi** editörüyle açar ve gerekli değişikliklerin yapılmasını bekler. **vi** editöründen çıktığında yeni **cron** dosyası devreye girmiş olur.

```

root@cayfer.bilkent.edu.tr: /etc - Shell - Konsole
0 4 * * * /usr/local/bin/yedekle
0,15,30,45 * * * * /hone/cayfer/ping.pl
30 0 * * * (cd /var/www/html/traffic/; perl gen_log.pl)
~
~
~
~
~
~
4,0-1 All

```

Yan sayfadaki örnekte **/usr/local/bin/yedekle** programı –ki aslında bir bash kabuğu için bir betik programıdır– (betik: script; Türkiye Bilişim Derneği, Bilişim Terimleri Sözlüğü – www.tbd.org.tr) hergün sabaha karşı saat

Kim Korkar LINUX'tan?

dörtte çalıştırılmaktadır. Bu cron dosyası “root” kullanıcıasına ait olduğu için de bu yedekle betiği root yetkileriyle çalışacaktır.

Gene aynı örneğe göre **/home/cayfer/ping.pl** betiği 15 dakikada bir çalıştırılan bir Perl programdır. Görevi bazı önemli bilgisayarlara erişilebildiğini kontrol etmektedir. Söz konusu Perl programı ping'lenemeyen bilgisayarları bir e-postayla sistem yöneticisine bildirmektedir. (Bu arada Perl dilini öğrenmeyi düşünürseniz Pusula Yayıncılığın “Perl ve MySQL ile CGI Programlama” kitabını önerebiliriz.)

Son **crontab** satırı ise her geceyarısı 00:30'da **/var/www/html/traffic** dizinine geçilmesini ve ardından “**perl gen_log.pl**” komutunun çalıştırılmasını sağlar.

Şimdi gelelim **cron** dosyasının ayrıntılarına:

cron dosyalarında 6 bilgi alanı vardır. Bunlardan ilk beş tanesi işlerin başlatılacağı gün, saat ve dakikaları belirtmek için kullanılır, altıncısı da işleri başlatmak için kullanılacak komutları belirler.

Alan	Anlamı	Değer Aralığı	Açıklama
1	İşin seçilen saat başından kaç dakika sonra başlatılacağını belirler.	0 - 59	“30”, “saat başını otuz dakika geçe” demektir.
2	İşin hangi saatte başlatılacağını belirler.	0 - 23	Sayı yerine “*” girilirse “ her saat ” anlamına gelir.
3	İşin hangi günler başlatılacağını belirler.	1 – 31	Sayı yerine “*” girilirse “ hergün ” anlamına gelir. 7, 14, 21, 28 yazılırsa “her ayın 7’si, 14’ü, 21’i ve 28’i” anlamına gelir.
4	İşin hangi aylarda yapılacağını belirler.	1 – 12	Sayı yerine “*” girilirse “ her ay ” anlamına gelir. “1, 6” yazılırsa iş sadece Ocak ve Haziran aylarında çalıştırılır. “1-3” yazılırsa iş yalnızca Ocak, Şubat ve Mart aylarında çalıştırılır.
5	İşin haftanın hangi günlerinde çalıştırılacağını belirler.	0 - 7	Sayı yerine “*” girilirse “ ne gün olursa olsun ” anlamına gelir. 0. ve 7. günler Pazar kabul edilir. “1, 2” yazılırsa “Pazartesi ve Salı” anlamına gelir. “1-3” yazılırsa Pazartesi, Salı ve Çarşamba günleri anlamına gelir.



Sisteminizde **crond** çalışmıyorsa, **cron** dosyalarını düzenlemeniz bir işe yaramayacaktır. Sisteminizin her açılışında **crond**'nin de başlatılması için

```
chkconfig --add crond
chkconfig crond on
```

komutlarını vererek **/etc/rc.d** dosyalarında gerekli düzenlemelerin yapılmasını sağlayabilirsiniz.

İşte birkaç örnek:

15 * * * * prog1	prog1 15 dakikada bir çalışır.
0 17 * * * prog1	prog1 hergün saat 17'de çalışır.
0 10,12,14,16,18 * * * prog1	prog1 hergün saat 10 ile 18 arasında iki saatte bir çalışır.
59 23 * * 1-5 prog1	prog1 her iş günü geceyarısına bir kala çalışır.
* * * * * prog1	Sistemi mahvedebilecek bir cron satırı. Hergün, her saat ve her dakika yeni bir prog1 başlatılacak demektir. Artık neler olacağı prog1 programına bağlıdır.

LILO Yönetimi

LILo, yani **LI**nux **LO**ader sisteminizin önemli bir yazılımıdır. Görevi, sistemin açılış sırasında hangi disk bölümünden (*partition*) hangi işletim sisteminin hangi parametrelerle belleğe yükleneceğini belirlemek ve yönetmektir. Aynı amaca yönelik **GRUB** isimli bir yazılım da LINUX dünyasında oldukça yaygın olarak kullanılmaktadır, ama bu kitapta biz yalnızca **LILo**'dan söz edeceğiz.

LILO sayesinde istediğiniz işletim sistemini istediğiniz diskin istediğiniz bölümünden yükleyebilirsiniz; üstelik bu yüklenen işletim sistemi LINUX olmak zorunda da değildir.

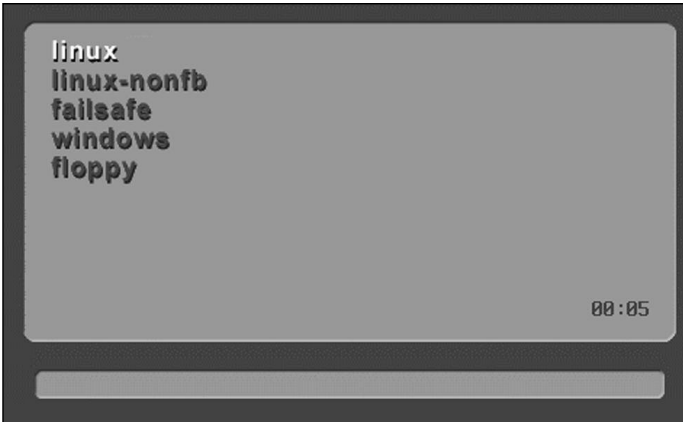
LILO'yu bilmek ve yönetebilmek, özellikle sistemini bazen Windows bazen de LINUX işletim sistemiyle açmak isteyen kullanıcılar için önemlidir. LINUX dünyasına yeni girenlerde gözlediğimiz ortak yaklaşım genellikle eski işletim sisteminin elinin altında olmasını istemeleridir. LINUX'u beğenip, işlerini bu platforma taşıyanlar bir süre sonra eski işletim sistemini içeren disk bölümüne bir “**mkfs atıp**”, o bölümü de LINUX disk alanı olarak kullanmaya başlıyorlar. Neyse...

Tekrarlama olacağını bile bile, burada PC türü bilgisayarların “**boot**” sürecini hatırlatmak istiyoruz.

Bilgisayarın BIOS yazılımı bellek, görüntü kartı gibi önemli bazı donanım unsurlarını kontrol ettikten sonra BIOS ayarları çerçevesinde disket sürücü, CD gibi birimleri kontrol eder ve genellikle bu sürücülerde bir ortam takılı olmadığı için diskten “boot etmeye” karar verir.

BIOS, diskten “boot etmeye” karar verirse birinci diskin “boot sektörü” diye adlandırılan bölgesinden bilgisayarın işletim sistemini yükleyecek yazılımı belleğe alır.

LILO işte bu boot sektöründen yüklenen yazılımdır. Sistem ilk açıldığında BIOS, boot sektöründen LILO'yu belleğe yükler. LILO da kendi ayarları doğrultusunda kullanıcıya işletim sistemi yüklemeye ilgili seçenekleri sunar.



Kim Korkar LINUX'tan?

LILO yazılımı **/etc/lilo.conf** dosyasından yönetilir. Bu dosyada gereksinimleriniz doğrultusunda değişiklik yaptıktan sonra **/sbin/lilo** komutuyla yeni düzenlenen LILO konfigürasyonuna göre birinci diskin boot sektörlerine gerekli kayıtlar yerleştirilir.

Her ne kadar Mandriva Linux Control Center menüsündeki LinuxConf aracıyla LILO konfigürasyon dosyalarını düzenlemek mümkünse de bu işin temelini öğrenmenizde yarar vardır. Bu nedenle örneklerimizi **/etc/lilo.conf** üzerinde editörle değişiklik yapıp **/sbin/lilo** programını çalıştırma üzerine kuracağız.

Öncelikle tipik bir **lilo.conf** dosyasına göz atalım:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
vga=normal
default="linux"
keytable=/boot/tr_q-latin5.klt
prompt
nowarn
timeout=100
message=/boot/message
menu-scheme=wb:bw:wb:bw
#
image=/boot/vmlinuz
    label="linux"
    root=/dev/hda6
    initrd=/boot/initrd.img
    append="devfs=mount acpi=off"
    read-only
other=/dev/hdd1
    label="windows98"
    table=/dev/hdd
other=/dev/fd0
    label="floppy"
unsafe
```

Dikkat ederseniz bu konfigürasyon dosyasının başında “**boot=**” diye başlayıp “**menu-scheme=**” diye biten global değişkenler ve ardından “**image**” ve “**other**” parametreleriyle bloklanmış gruplar yer alıyor.

Global parametreler arasında önemli olanlar:

boot=/dev/hda	LILO'nun ilk diskin boot sektörüne yerleştirileceğini belirtiyor.
timeout=100	Sistem açıldığında kullanıcı LILO menüsünden timeout/10 saniye içinde bir seçim yapmadığı takdirde varsayılan boot konfigürasyonunun kullanılacağını belirtiyor. Dikkat edin! timeout parametresi saniye cinsinden değil, saniyenin onda biri cinsinden belirtilir.
default="linux"	timeout/10 saniye sonunda hâlâ bir seçim yapılmadıysa etiketi “ linux ” olan konfigürasyonun kullanılacağını belirtiyor.

“**image=**” diye başlayan bloklar LINUX işletim sistemine ait tanımları içerir.

Örneğin,

```
image=/boot/vmlinuz
  label="linux"
  root=/dev/hda6
  initrd=/boot/initrd.img
  append="devfs=mount acpi=off"
  read-only
```

satırları “**linux**” isimli tanım için:

- Bu grubun “**linux**” ismiyle anılacağını,
- Bu grubun seçilmesi durumunda işletim sisteminin çekirdeğinin **/boot/vmlinuz** isimli dosyadan yükleneceğini,
- **root** dizin olarak ilk diskin altıncı bölümünün kullanılacağını (hda6),
- Yükleme sürecinde kullanılacak sanal disk görüntüsünün (*image*) **/boot/initrd.img** dosyasında yer aldığını (bunun ne demek olduğu, yalnızca çekirdek kodu geliştirenleri ilgilendirir),

Kim Korkar LINUX'tan?

- İşletim sisteminin çekirdeğine “**devfs=mount acpi=off**” parametrelerinin geçirileceğini,
- Dizinlerin salt oku mount edileceğini (LINUX gerekli kontrolleri yaptıktan sonra herşey yolundaysa, gereken tüm dizinler oku-yaz olarak yeniden mount edilir) belirtiyor.

“**other=**” diye başlayan bloklar LINUX olmayan işletim sistemine ait tanımları içerir.

Örneğin,

```
other=/dev/hdd1  
    label="windows98"  
    table=/dev/hdd
```

satırları:

- Bu grubun “windows98” ismiyle anılacağını,
- Bu grubun seçilmesi durumunda yüklenen işletim sisteminin kullanacağı bölümlene tablosunun (*partition table*) ikinci IDE kanalındaki ikinci diskten (hdd) okunacağını belirtiyor.

Şimdi diyelim ki sisteminize üzerinde Windows-XP yüklenmiş yeni bir diski birinci IDE kanalının ikinci diski (*hdb, slave*) olarak taktınız ve sisteminizi bu diskten de açabilmek istiyorsunuz. Yapmanız gereken **/etc/lilo.conf** dosyasına

```
other=/dev/hdb1  
    label="windows-XP"  
    table=/dev/hdb
```

satırlarını ekleyip

```
/sbin/lilo
```

komutunu çalıştırmak olacaktır. Bir daha reboot ettiğinizde **LILO** size Windows-XP yüklemeyi de bir seçim olarak sunacaktır. Bu işleri yapabilmemiz için sisteminizi önce LINUX ile açmanız gerektiğini belirtmeye gerek yok herhalde. Aslında sisteminizi neden XP ile açma gereksinimi duyduğunuzu da anlamadık ya, neyse...

Webmin

Bu bölümü okuyunca bize kızacaksınız... “Madem webmin vardı, ne diye bir sürü komut ve ayar dosyası anlattınız?” diyeceksiniz.

Gerçekten de “webmin”, LINUX işletim sistemini tek yazılımla yönetmek için geliştirilmiş web tabanlı bir uygulamadır.

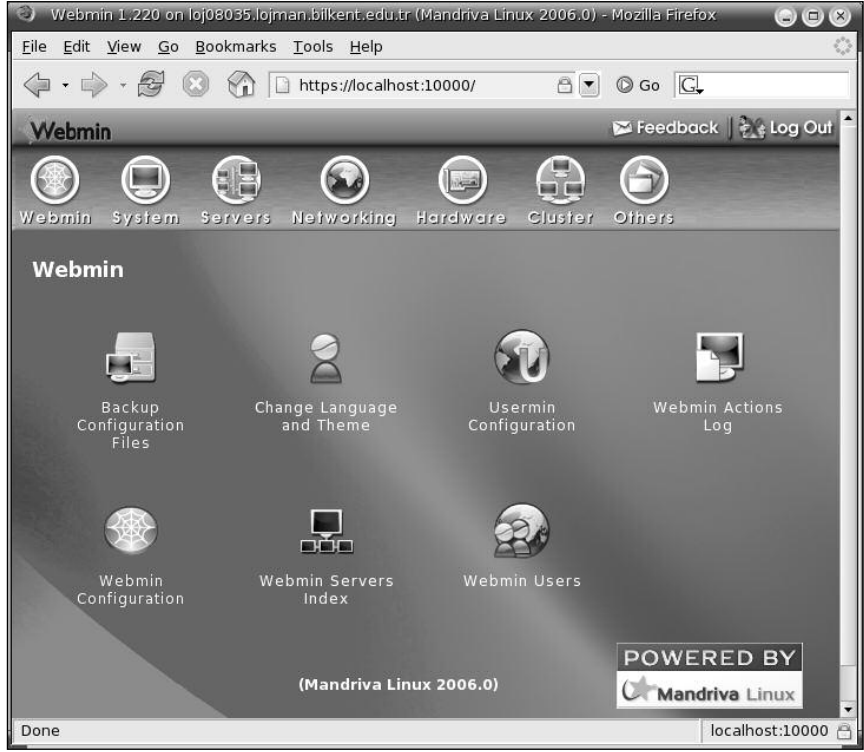
Webmin’i kullanmak için bilgisayarınızda herhangi bir web tarayıcı; örneğin Konqueror başlatıp URL olarak

https://localhost:10000

yazınız. Yani, 10000 numaralı porttan web servisi isteyiniz.



Kim Korkar LINUX'tan?



Doğal olarak root kullanıcı kimliğiyle servise bağlanmanız gerekecektir.

Artık webmin menüsünden yararlanarak, sisteminizin neredeyse tüm yönetim işlerini bu arabirim ile yapabilirsiniz.

Webmin'in işlevlerini bu kitapta anlatmayacağız. LINUX işletim sisteminin yönetim kavramlarının temellerini öğrenmiş olduğunuza göre gerisini siz kendiniz araştırabilir ve keşfedebilirsiniz.



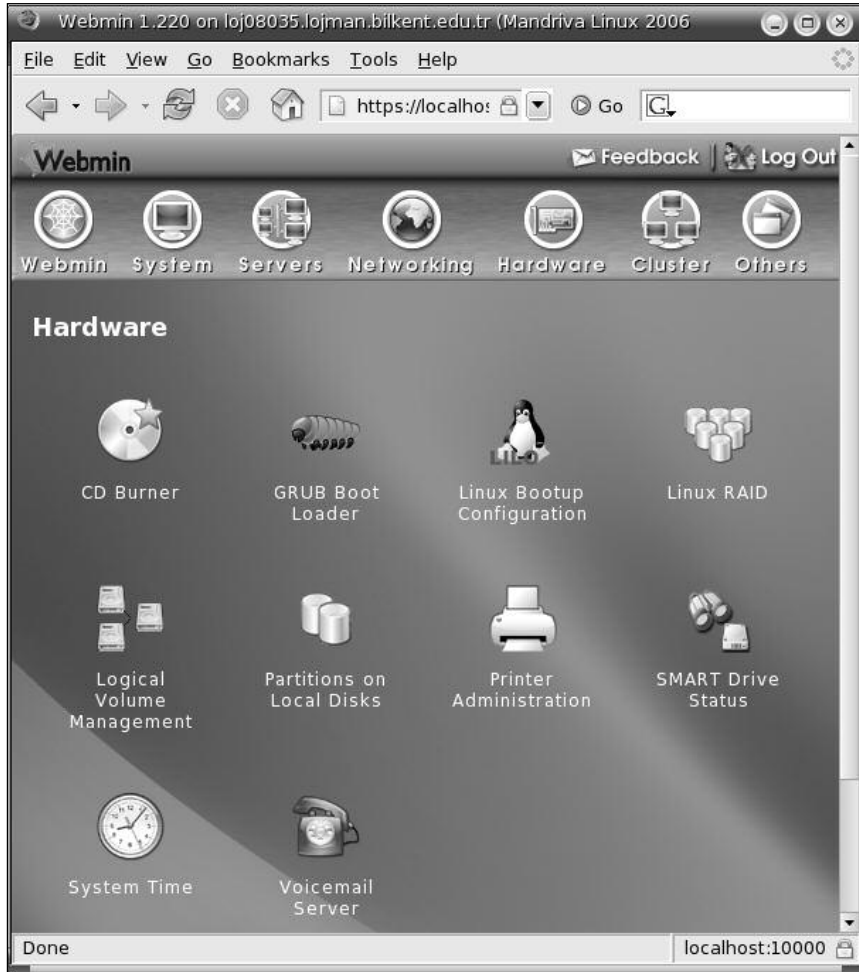
Kim Korkar LINUX'tan?



Apache web sunucusu, MySQL veritabanı yönetim sistemi, Postfix e-posta sunucusu, FTP sunucusu gibi LINUX'u LINUX yapan birçok sunucu servisinin ayarlarını bu menüden yapabilirsiniz.



Kim Korkar LINUX'tan?





“root” Şifresini Unuttuğunuzda...

Bir LINUX sistemin “root” şifresinin bilinmemesi, sanıldığı kadar az karşılaşılan bir durum değildir. Sistem yöneticisi şifreyi unutabilir; tatildeyken ya da işten ayrıldıktan sonra sisteme başkalarının “root” olarak bağlanması gerekebilir, ya da en kötüsü sisteminizi kıran birisi “root” şifresini değiştirebilir.

“root” şifresi bilinmeyen bir sistem üzerinde denetimi ele tekrar almanın tek yolu, “root” şifresini bilinen bir şifreyle değiştirmektir. Hatırlarsanız, daha önce kullanıcı şifrelerinden bahsederken, UNIX ve LINUX işletim sistemlerinde şifrelemenin tek yönlü olduğunu, şifrelenmiş hali bilinen bir şifrenin açık halinin ne olduğunun bulunmasının olanaksız olduğunu belirtmiştik. “root” şifresini değiştirmek için sisteminizi kapatın. Yeniden açılış sırasında LILO size yüklenebilecek işletim sistemlerini gösterdiği sırada bir kez Esc tuşuna basın.

Kim Korkar LINUX'tan?

Karşınıza

boot:

hazır işareti çıkacaktır. Bunun karşısına “**linux single**” yazıp Enter tuşuna basınız.

boot: linux single

LINUX çekirdeği belleğe yüklendiğinde “**single**” sözcüğü çekirdeğe parametre olarak geçirilecektir. LINUX çekirdeği de bu parametreyi görünce açılışı birinci çalışma düzeyi (run level 1) tamamlandığında kesecektir.

LINUX çalışır durumda olacak ancak yalnızca konsoldaki kullanıcıya hizmet edecektir. Yani, varsa web servisi, ftp servisi, e-posta servisi gibi hizmetleri yürüten yazılımlar başlatılmayacaktır.

Ayrıca, konsoldaki kullanıcının kendisini sisteme tanıtmayı da istenmeyecektir. “root” yetkileriyle bir **bash** kabuğu başlatılıp kullanıcıdan komut girilmesi beklenenecektir.

Bu konumda

passwd

komutunu vererek o anda geçerli olan kullanıcının; yani “root”un şifresini değiştirebilirsiniz. **passwd** komutunu veren kullanıcı “root” olduğu için de eski şifre sorulmayacaktır.

Şifreyi değiştirdiğinizde

exit

komutunu vererek çekirdeğin açılışa devam etmesini sağlayabilirsiniz.

Meraklısına...

Bir LINUX bilgisayarın açılışı sırasında LILO'ya "**linux single**" yazarak sistemin tek kullanıcı ve şifre sormadan "**root**" kullanıcı olarak açılmasını önleyebilirsiniz.



/etc/lilo.conf dosyasında ilgili ayar satırları arasına

```
password=eb!TKY-2  
restricted
```

gibi satırlar ekleyip

lilo

komutunu vererseniz, artık sistem tek kullanıcı düzeyde açılırken bile "**eb!TKY-2**" şifresinin girilmesini isteyecektir. Dikkatinizi çekeriz... Bu şifre sistemin "**root**" şifresi değildir; tek kullanıcı düzeyde açma şifresidir.

Bu şifreyi pek fazla kullanmayacağınız için unutmaya olasımanız çok daha yüksektir. Günün birinde, "**root**" şifresini unuttuğunuz için sisteminizi tek kullanıcı düzeyde açmanız gerekirse bu şifreyi hatırlamayacağınıza bahse gireriz. Bu nedenle, tek kullanıcı çalışma düzeyi koruması için **lilo.conf** dosyasına bu satırları koymanızı hiç önermiyoruz.

Eğer bir sistemin tek kullanıcı düzey şifresi ve root şifresi unutulursa yapılacak iş, diski sökmek ve bu diski şifreleri bilinen bir başka LINUX bilgisayara ikinci disk olarak takmak ve diskin üzerindeki **etc/shadow** dosyasında root kullanıcıya ait satırdaki kriptolanmış şifreyi bir editörle silmektir.

Kim Korkar LINUX'tan?