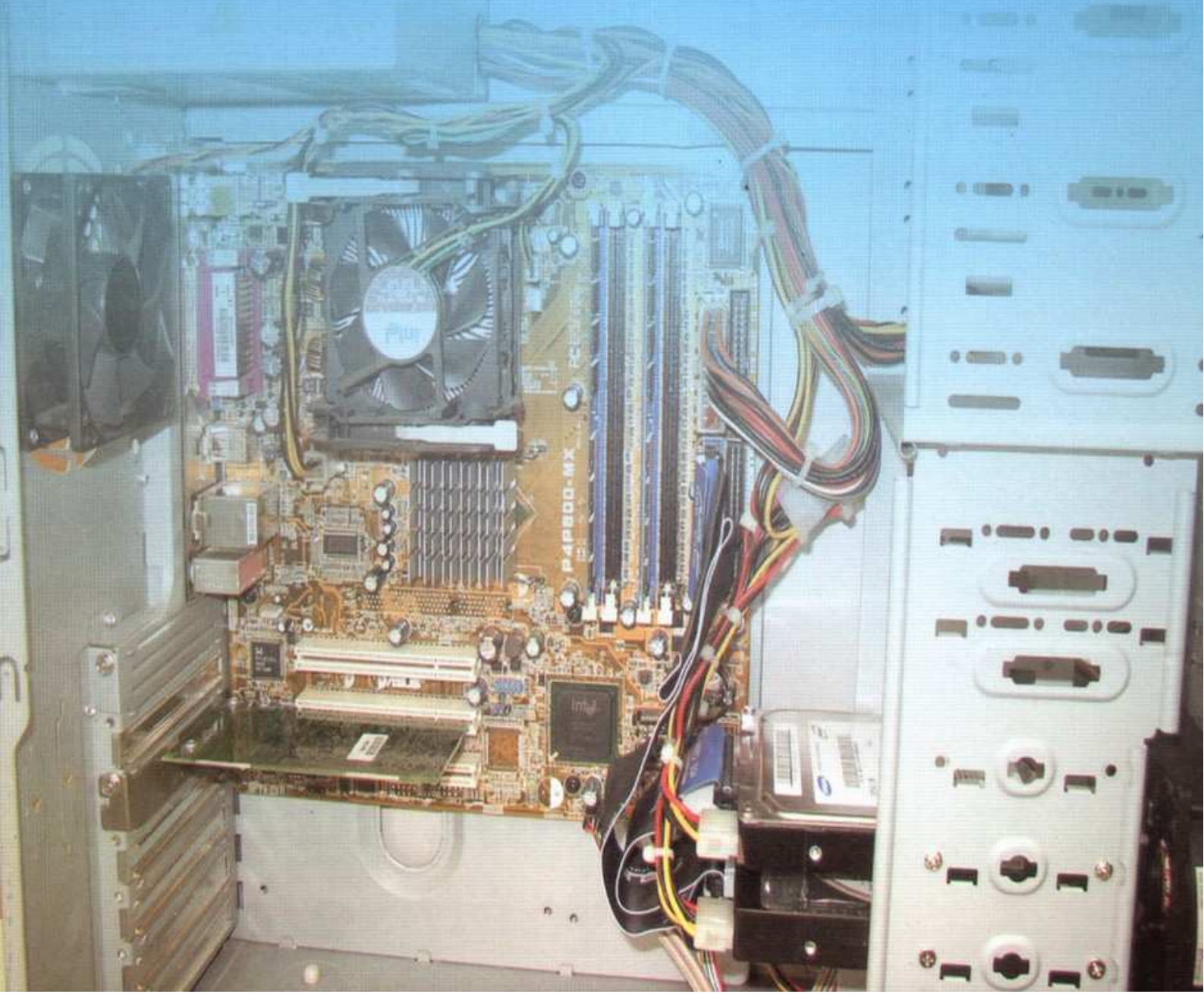


Pallay Ferenc

Hálózati kiszolgáló kialakítása oktatási intézményben GNU/Linux operációs rendszeren



ЗАКАРПАТСЬКИЙ УГОРСЬКИЙ ІНСТИТУТ ІМ. ФЕРЕНЦА РАКОЦІ ІІ



II. RÁKÓCZI FERENC KÁRPÁTALJAI MAGYAR FŐISKOLA

Pallay Ferenc

**Hálózati kiszolgáló kialakítása
oktatási intézményben
GNU/Linux operációs rendszeren**

Beregszász - 2008

A könyv sok képpel illusztrálva bemutatja egy hálózati kiszolgáló telepítését és alapvető beállításait. Gyakorlati szempontból útmutatást ad, hogy szerény anyagi és technikai feltételek mellett hogyan lehet felépíteni egy számítógépes kiszolgálót Linux operációs rendszeren. Részletesen kitér a leggyakrabban használt szerver funkciókra, és a munkaállomások beállítására is.

Elsősorban oktatási intézményekben dolgozó rendszergazdáknak és informatika tanároknak ajánlott, akik szeretnének megismerkedni a Linux operációs rendszer alapjaival

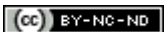
Lektorálták: *az FSF.hu Alapítvány aktivistái*

A kiadásért felel: *Orosz Ildikó, Soós Kálmán*

Korrektúra: *a szerző*

Tördelés: *Fábián Zoltán*

Borítóterv: *Beregszászi István*



Hálózati kiszolgáló kialakítása oktatási intézményben GNU/Linux operációs rendszeren
by Pally Ferenc is licensed under a [Creative Commons Nevezd meg!-Ne add el!-Ne változtasd! 2.5
Magyarország License](https://creativecommons.org/licenses/by-nc-nd/2.5/hu/)

Nyomtatásban megjelent:

PoliPrint Kft.
Ungvár, Turgenyev u. 2.
Felelős vezető: Kovács Dezső

ISBN 978-966-7966-66-9

TARTALOMJEGYZÉK

BEVEZETŐ	6
I. A HARDVER KIVÁLASZTÁSA	7
II. A TELEPÍTÉS	8
ELŐKÉSZÜLETEK	8
A TELEPÍTÉS MENETE	9
III. ISMERKEDÉS AZ OPERÁCIÓS RENDSZERREL	19
NÉHÁNY ALAPVETŐ PARANCS	19
HÁLÓZATI KAPCSOLATOK ELLENŐRZÉSE	23
ADSL KAPCSOLAT BEÁLLÍTÁSA	25
A MIDNIGHT COMMANDER TELEPÍTÉSE	26
NÉHÁNY KONFIGURÁCIÓS ÁLLOMÁNY MÓDOSÍTÁSA	27
AZ OPERÁCIÓS RENDSZER FRISSÍTÉSE	28
IV. KAPCSOLAT RENDSZEREK KÖZÖTT. ADMINISZTRÁCIÓ	30
A PUTTY	30
A WINSCP	33
V. A RENDSZER FELHASZNÁLÓI	35
FELHASZNÁLÓK LÉTREHOZÁSA	35
TÁRKORLÁTOK BEÁLLÍTÁSA: A QUOTA	37
FELHASZNÁLÓK TÖRLÉSE	42
VI. AZ INTERNET MEGOSZTÁSA	44
LEHETŐSÉGEK	44
NÉHÁNY PORT MEGNYITÁSA A BELSŐ HÁLÓZAT FELÉ	44
A SQUID	45
A KLIENSEK BEÁLLÍTÁSA	47
A SQUIDGUARD	50
AZONOSÍTÁS NÉLKÜLI INTERNET-HASZNÁLAT	56
SÁVSZÉLESSÉG-KORLÁTOZÁS	57
VII. A HÁLÓZATI FORGALOM ELLENŐRZÉSE	59
SARG - SQUID ANALYSIS REPORT GENERATOR	59
MRTG - MULTI ROUTER TRAFFIC GRAPHER	61
VIII. BIZTONSÁGI BEÁLLÍTÁSOK	63
FELOLDÓ GYORSÍTÓTÁRAS NÉVKISZOLGÁLÓ	63
NEM HASZNÁLT SZOLGÁLTATÁSOK KIKAPCSOLÁSA	64
AZ SSH BELÉPÉS KORLÁTOZÁSA	66
CSOMAGSZŰRÉS	66
IDŐSZINKRONIZÁLÁS	75
IX. KAPCSOLAT RENDSZEREK KÖZÖTT. A SAMBA	76
A SAMBA BEÁLLÍTÁSA	76
A MUNKAÁLLOMÁS BEÁLLÍTÁSA. WINDOWS 98	79
A MUNKAÁLLOMÁS BEÁLLÍTÁSA. WINDOWS XP	84
OKTATÁSI ANYAGOK HASZNÁLATA A KISZOLGÁLÓN	92
ZÁRTHELYI DOLGOZATOK BEGYŰJTÉSE PROGRAM SEGÍTSÉGÉVEL	94
X. A LINUX MINT MUNKAÁLLOMÁS	96
TELEPÍTÉS	96
NÉHÁNY BEÁLLÍTÁS A MUNKAÁLLOMÁSON	105
KAPCSOLÓDÁS A FÁJLSZERVERHEZ	107
ÁLLANDÓ FELHASZNÁLÓI KÖRNYEZET BIZTOSÍTÁSA	109
XI. WEBSZERVER	112
XII. A WEBMIN	116
JELSZÓMÓDOSÍTÁS BÖNGÉSZŐBŐL	119

XIII. BIZTONSÁGI MENTÉSEK.....	121
USB ADATTÁROLÓ ESZKÖZÖK HASZNÁLATA	121
FELHASZNÁLÓI AZONOSÍTÓK MENTÉSE	121
A MÁSODIK MEREVLEMEZ BEÁLLÍTÁSA.....	123
KÖNYVTÁRAK TÜKRÖZÉSE.....	127
A RENDSZER VISSZAÁLLÍTÁSA.....	129
XIV. A RENDSZER FELÜGYELETE	132
SMART – MEREVLEMEZEK ÁLLAPOTA	132
LOGWATCH – RENDSZERNAPLÓ ELEMZÉS	133
MUNIN – TELJESÍTMÉNYADATOK WEBES FELÜLETEN	135
XV. VÉGSZÓ.....	138
XVI. A FELHASZNÁLT ÉS AJÁNLOTT IRODALOM ÖSSZEVONT JEGYZÉKE	139

Bevezető

A legtöbb iskolában ma már van számítógépekkel felszerelt szaktanterem. Gyakran ezek a számítógépek lokális hálózatba vannak kapcsolva, és egyre több intézmény rendelkezik valamilyen Internet kapcsolattal is. Előbb-utóbb felmerül az igény egy kiszolgáló számítógépre, amelyiken oktatási anyagokat lehet elérhetővé tenni a belső hálózaton, felügyelni és szabályozni lehet az Internet hozzáférést, és központi tárhelyet is biztosít a felhasználóknak.

Ez a könyv megpróbál segítséget nyújtani azoknak az iskolai rendszergazdáknak, informatika-tanároknak, akik szeretnék a meglévő, gyakran minimális, eszközök felhasználásával hálózati kiszolgálót telepíteni és olyan hálózati szolgáltatásokat nyújtani a felhasználóknak, amik színesebbé és eredményesebbé tehetik az oktatást.

Sok képpel illusztrálva, lépésről lépésre szeretném bemutatni egy Linux kiszolgáló telepítését, megismertetni az olvasóval néhány alapvető szolgáltatás működését és beállítását a kiszolgálón. A munkaállomások operációs rendszereként a Microsoft Windows 98, a Windows XP és a Mandriva Linux van tárgyalva.

A Windows 2000 és a Windows Vista operációs rendszereknél a kapcsolat beállítása nem tér el alapvetően a Windows XP-től, ezeket részletesen nem mutatom be.

A Linux munkaállomás telepítésének lépéseit is részletesen tárgyalja a könyv. Nagyon kevés helyen használnak ma még Linuxot munkaállomásokon, holott napjaink Linux disztribúciói modern számítógépeken, jól használható és ingyenes alternatívát jelentenek. A gyakorlat azt mutatja, hogy ha egy felhasználó elsajátítja az alapvető irodai és felhasználói programok használatát Linux operációs rendszeren, más rendszer sem fog számára problémát jelenteni. A Mandriva Linux helyett használhatunk más disztribúciót is. Mindenképp meg kell említeni az utóbbi időben igen népszerű Ubuntu Linux-ot, de a magyar fejlesztésű UHU Linux is alternatíva lehet. A grafikus felület KDE vagy GNOME legyen, vegyes környezetben a KDE talán előnyösebb.

A kiszolgálón a Linux disztribúció kiválasztásánál az volt a legfontosabb szempont, hogy a telepítése felhasználóbarát legyen, és olyan kezdő, vagy eddig csak a Windows-t használó, rendszergazdának se okozzon problémát, akinek ez az első linuxos próbálkozása. A másik nagyon fontos szempont a rendszer fejleszthetősége volt. Ha a rendszergazda a későbbiekben újabb szolgáltatásokat akar indítani a kiszolgálón, ehhez megfelelő leírásokat és programokat találjon az Interneten. Így esett a választás a CentOS (*Community ENTERprise Operating System*) 4.4-re, ami az egyik legnagyobb disztribúció, a Red Hat Enterprise Linux nyílt forrású, szabadon hozzáférhető csomagjaiból épül fel. Ez az operációs rendszer letölthető az Internetről és nagyon sok Red Hat Linux dokumentációt, könyvet találhatunk, amelyek minden szempontból használhatóak a CentOS-hoz is.

Természetesen ez a könyv nem helyettesíthet egy részletes Linux monográfiát. Bemutatja a rendszer kiépítésének a lépéseit, de az üzemeltetéséhez alapvető Linux/Unix ismeretekre lesz szükség. A felmerülő kérdésekre választ kaphatunk valamelyik, az irodalomjegyzékben felsorolt könyvből, és az Interneten is egyre több magyar nyelvű szakirodalmat, leírást, fórumot találunk.

Pallay Ferenc
palferi@kmf.uz.ua

I. A hardver kiválasztása

Egy valódi, folyamatos üzemre tervezett kiszolgáló számítógép (szerver) beszerzésére a legtöbb iskolában nincs lehetőség. Egy ilyen szerver ára több 10 000 hriveny. Viszont egy stabilan működő, megfelelő szellőzésű személyi számítógép is megfelelhet első szerverünknek. Mindenképpen jó minőségű tápegység legyen benne, és fontos, hogy a merevlemez légáramba kerüljön. Ha ez nincs így, építsünk be pótlólagos ventilátorokat a számítógépházba.

A merevlemez minimális kapacitása attól függ, hogy milyen szolgáltatásokat fogunk nyújtani a kiszolgálón. Internetes átjárónak néhány GB-os is megfelel, ha a kiszolgáló fájlserver is lesz, lehetőleg két 40 (vagy több) GB-os merevlemez szerezzünk be.

Ha van lehetőség, szünetmentes tápegységet is vásároljunk. Ezek közül azok a típusok a legjobbak, amelyek kommunikálni tudnak a számítógéppel és hosszabb áramszünet esetén leállítják az operációs rendszert.

Szerencsés, ha az alaplap BIOS-ában be lehet állítani, hogy áramkimaradás után induljon a számítógép. Így egy több órás áramkimaradás után nem kell kézzel bekapcsolni a szervert, hanem automatikusan elindul.

Floppy meghajtóra nem lesz szükség, CD-olvasóra is csak a telepítéshez, utána kisserelhetjük a kiszolgálóból. A processzor Pentium II vagy modernebb legyen és 128 vagy több megabájt RAM legyen a gépben.

Két hálózati kártyára lesz szükség, lehetőség márkás, kiszolgálókhoz ajánlott típusok közül válasszunk. Alaplaphoz integrált hálózati eszköz esetén, használhatjuk azt is, ekkor csak egyet szereljük a PCI foglalatok egyikébe.

Az alaplapi hangkártyát, ha van az alaplapunkon ilyen, az alaplap leírása alapján kapcsoljuk ki, arra biztosan nem lesz szükség a kiszolgálón.

Szerverünkbe bármilyen videokártya megfelel, de lehetőleg kerüljük a ventilátorral szereltek.

A kiszolgáló működését két konfiguráción is ellenőriztem. Az első akár kéttucat kliens gép, és felhasználó kiszolgálására is megfelel: 1200 MHz Intel Celeron Tualatin processzor, Asus TUSL2-M alaplap, 320Mb RAM, Seagate Barracuda 7200.7 40 GB merevlemez, Chieftec ATX-310 táp, 2 db Intel 82558 hálókártya. A második egy minimális konfiguráció: Pentium II 350 processzor, 128 Mb RAM, 4,3 GB merevlemez, 2 db Realtek 8139 hálókártya. Internet megosztásra ez is megfelel, ha nincs modernebb gépünk erre a célra. Fájlservernek viszont csak korlátozottan.

Telepítés előtt a Memtest programmal ellenőrizzük a RAM-ot. Az ellenőrzés több órát tartson (modern, több gigabájt-os rendszereknél akár egy napig is), ha ez alatt az idő alatt nem ír ki hibás memóriarészt a program, hozzákezdhetünk a telepítéshez.

Tartsunk be minden tűz- és érintésvédelmi előírást. Felügyelet nélkül ne üzemeljen a kiszolgáló hosszú ideig. Hétvégére és a szünidők ideje alatt kapcsoljuk ki és áramtalanítsuk.

II. A telepítés

Előkészületek

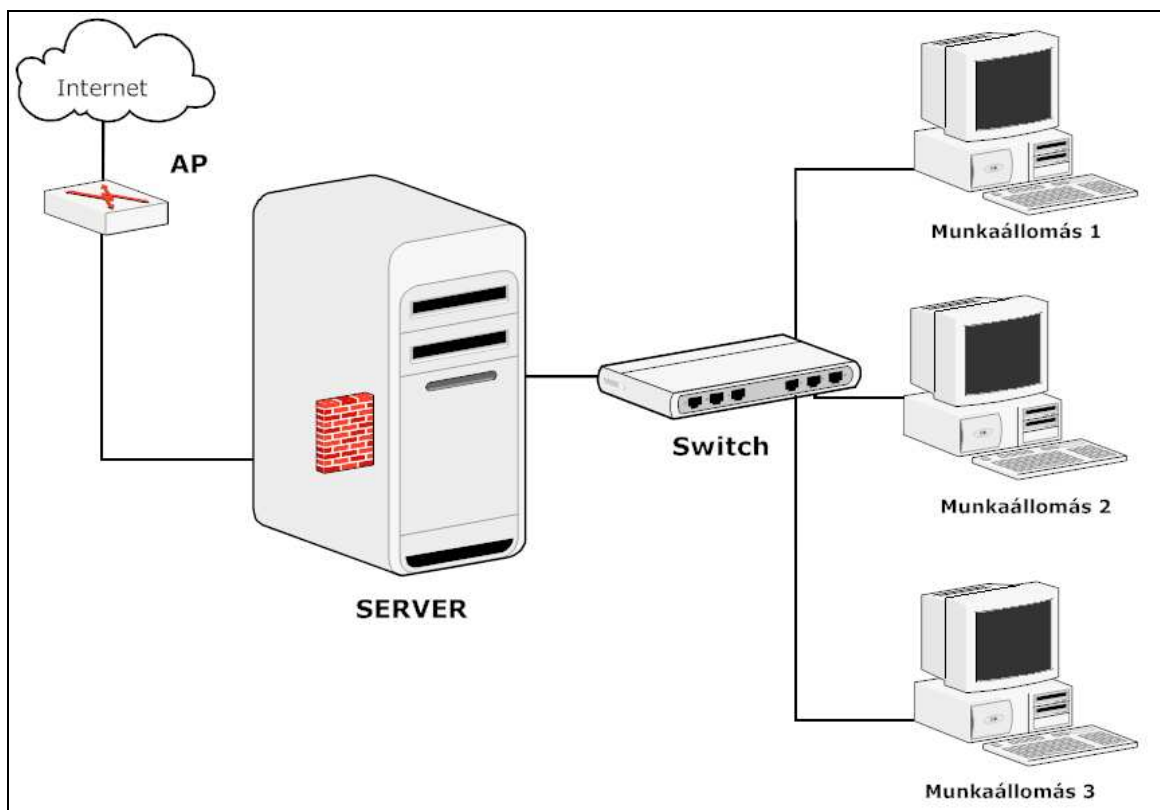
Telepítés megkezdése előtt készítsük elő a hardvert és pontosítsuk az Internet szolgáltatónk által biztosított adatokat. Ezek minimum a következők:

1. IP cím.
2. Alhálózati maszk.
3. Alapértelmezett átjáró.
4. DNS kiszolgáló vagy kiszolgálók

Tisztázzuk, hogy milyen eszközöket telepített a szolgáltató az Internet kapcsolatot kialakításához. Az utóbbi években a legelterjedtebbek a vezeték nélküli hozzáférési pont (AP), vezeték nélküli hálózati interfészkártyával kiegészített számítógép vagy valamilyen DSL modem. Ennek az eszköznek az Ethernet portját fogjuk a szerverünk egyik hálózati kártyájához csatlakoztatni. A másik hálózati kártya csatlakozik majd a switch-hez, ahová a munkaállomásokat is csatlakoztatjuk. Az 1. ábra a hálózat vázlatos képét mutatja. Az ábrán három munkaállomás van feltüntetve, de természetesen, a switch portszámától függően többet is beköthetünk. A switch-hez is kapcsolhatunk további hub-ot vagy switch-et.

Működő rendszer esetén járjunk el körültekintően: ne a meglévő hálózat-megosztást megvalósító gépre (pl. Windows XP) telepítsük fel a szervert, hanem egy újra. Megoldás lehet a merevlemez ideiglenes cseréje is. Ha elsőre nem sikerül a kiszolgálót úgy beállítani, ahogyan szeretnénk, visszatérhetünk az előző, működő megoldáshoz.

Amennyiben a szolgáltatónk privát IP tartományból oszt ki számunkra IP címet, (nem szerencsés megoldás, de előfordul) a saját hálózatunk gépeinek más alhálózatot válasszunk. Például, ha a szolgáltató által megadott cím 192.168.0.89 akkor a kiszolgáló második hálózati kártyája kapja pl. a 192.168.25.1 IP címet 255.255.255.0 alhálózati maszkkal. Ebben az esetben a munkaállomásoknak bármilyen IP címet adhatunk a 192.168.25.2-192.168.25.254 tartományból.

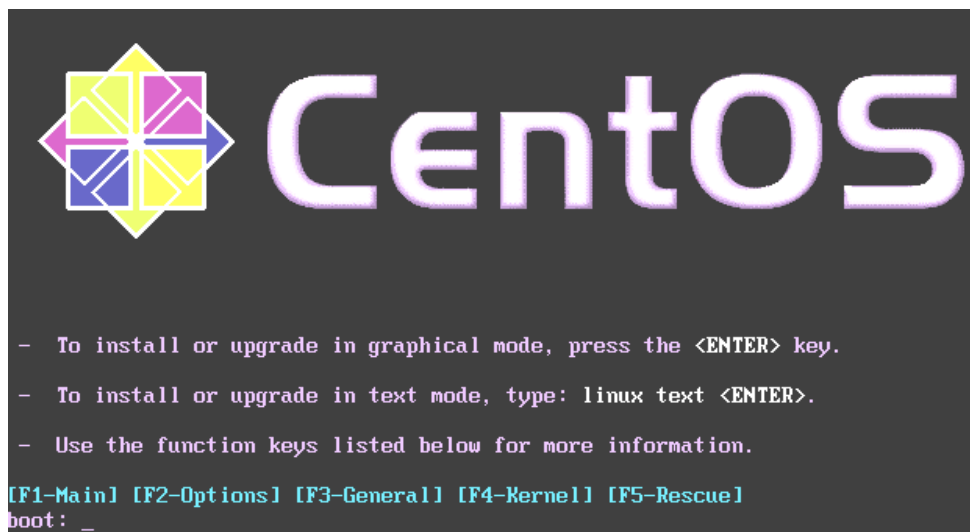


1. ábra

A telepítés menete

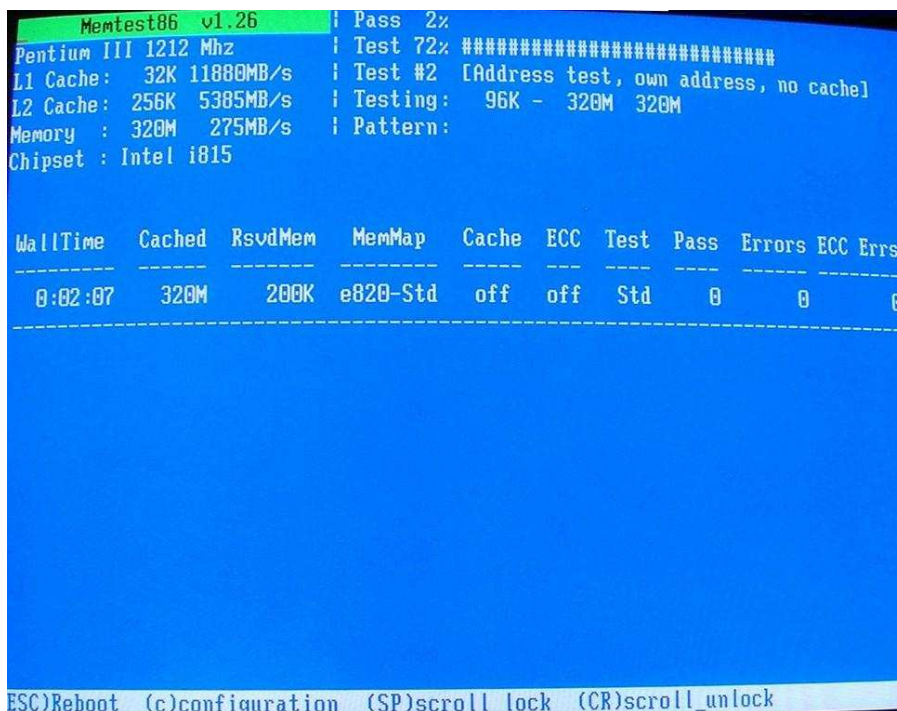
A telepítés legegyszerűbben CD-ről történhet. Az Interneten elérhető a www.centos.org címen, a telepítő CD iso formátumban. A <http://isoredirect.centos.org/centos/4/isos/i386/> címen válasszuk ki a hozzánk legközelebbi tükör-szervert és töltsük le a **CentOS-4.4.ServerCD-i386.iso**¹ állományt (580 Mb). A cd-képet írjuk ki valamilyen programmal (pl. NERO) egy CD-R lemezre.

A számítógép BIOS-ában állítsuk be, hogy a gépünk CD-ről induljon. Helyezzük be lemezt a meghajtóba és indítsuk újra a gépet. (2. ábra)



2. ábra

Telepítés előtt ellenőrizzük le a RAM memóriát a gépben. Ezzel sok kellemetlen és megmagyarázhatatlan problémát kerülhetünk el. Írjuk be a **memtest** szöveget és üssük le az Enter-t (3. ábra). Ha órák múlva is az Errors oszlopban 0-t látunk, akkor bátran hozzákezdhetünk a telepítéshez.

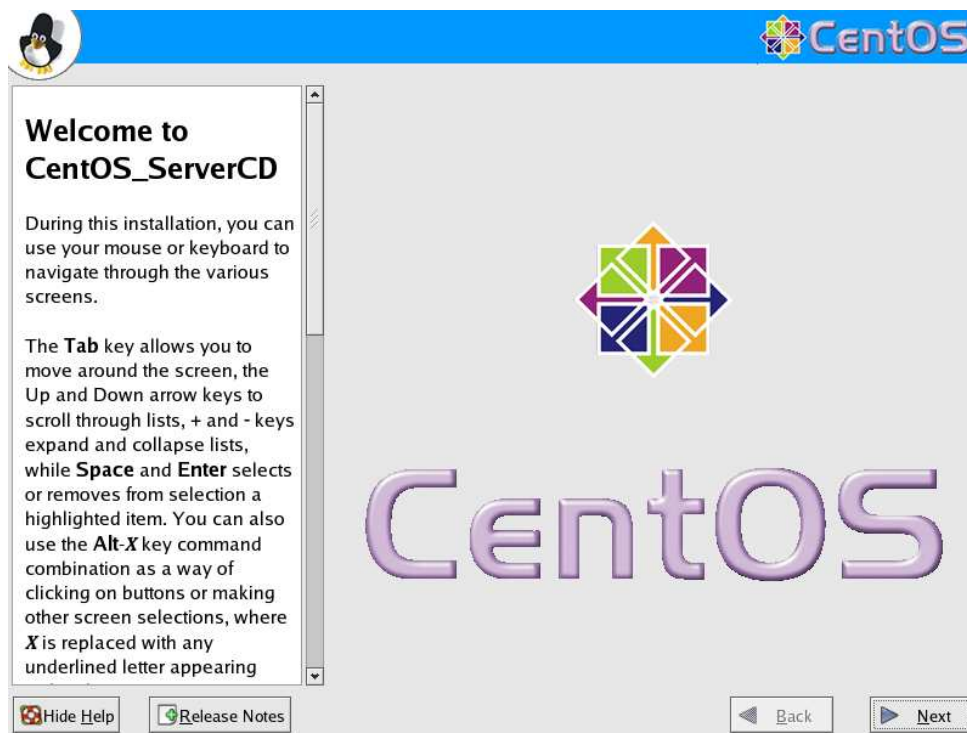


3. ábra

¹ 2008. október 17. megjelent a 4.7-es változat. A telepítés menete nem különbözik. A feltelepített 4.4-es változat az első frissítéskor automatikusan 4.7-ra vált.

Az Esc billentyű lenyomásával újraindul a rendszer, és most már válasszuk a grafikus telepítést, vagyis, ha megjelenik a képernyőn a 2. ábrán látható kép, üssük le az Enter-t.

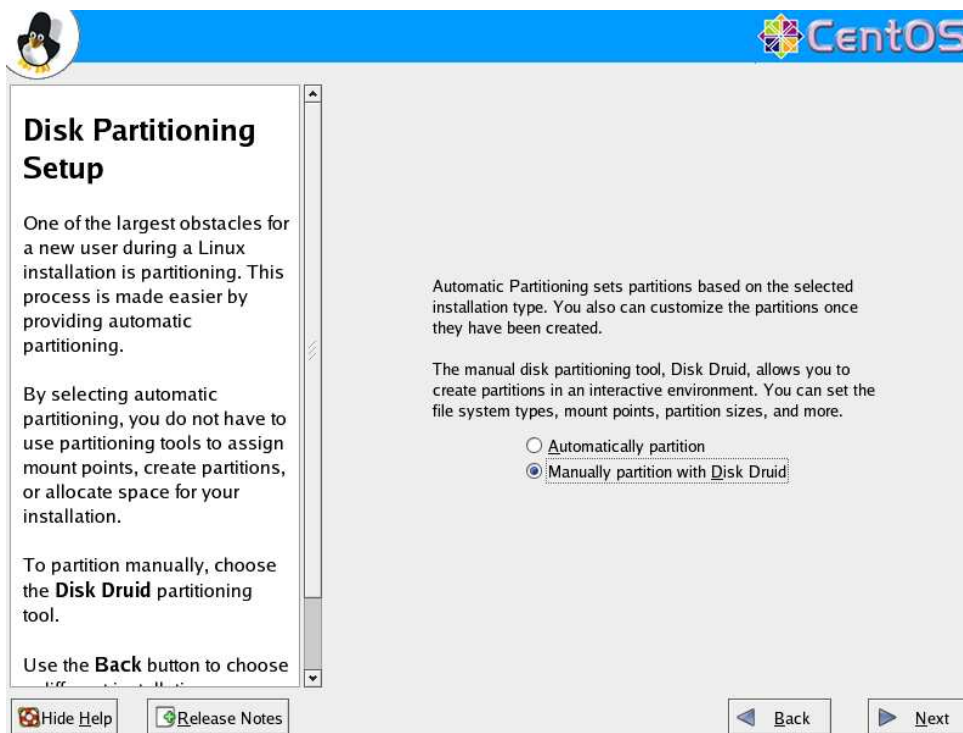
A képernyőn egy angol nyelvű felirat jelenik meg, amiben a telepítő felajánlja, hogy leellenőrizi a CD lemezt. Nem ellenőrzünk, TAB-billentyűvel válasszuk a skip-et, majd Enter. A telepítés grafikus felületen folytatódik. (4. ábra.) A telepítés során használhatjuk az egeret is. Amennyiben nem jelenne meg a grafikus felület, indítsuk újra a gépet és írjuk be a **linux text** szöveget a karakteres telepítéshez. De ez csak nagyon régi vagy különleges alaplappal, illetve videokártyával fordulhat elő.



4. ábra

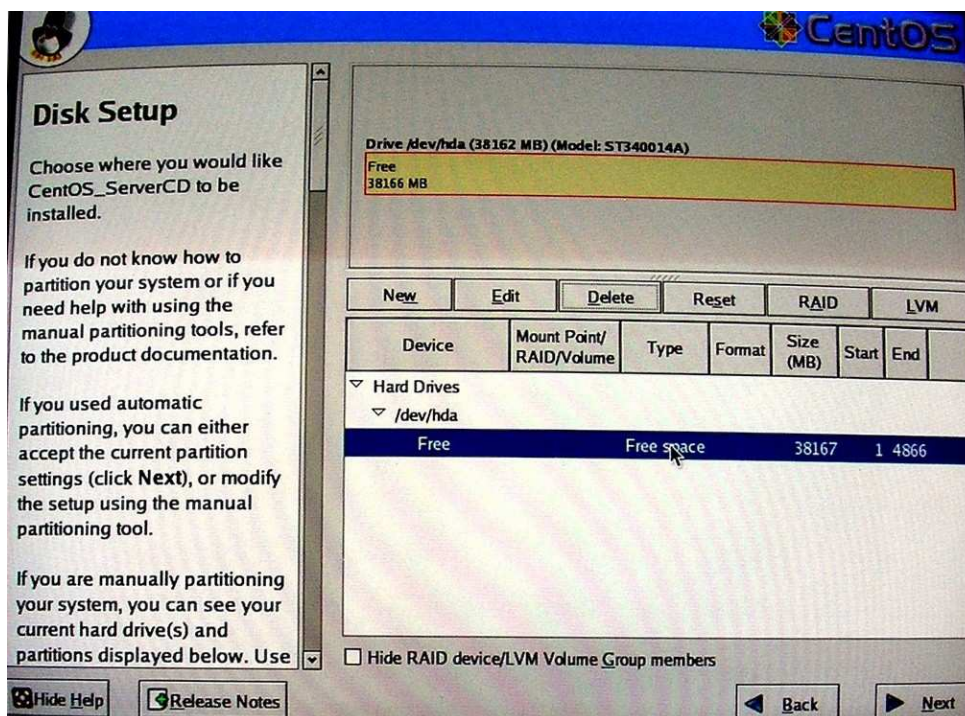
A NEXT gombra kattintva a következő képen kiválasztjuk az operációs rendszer nyelvét. Választhatunk magyar nyelvet is, de én mégis az angolt javaslom. A gyakorlat azt mutatja, hogy az angol nyelvű rendszeren bizonyos feladatok egyszerűbben megoldhatók, és a parancsok magyarázatai úgy is angolok maradnak. Ha nincs magyar billentyűzetünk mindenképp szerencsésebb az angol nyelv választása. Persze választhatunk németet vagy ukránt is, de általában a kiszolgáló gépekre angol nyelvű operációs rendszert telepítenek.

A következő ablakban billentyűzet kiválasztása történik, ha angol/ukrán billentyűzetünk van, válasszuk az U.S. English-t. Az ezt követő lépések nagyon fontosak és meghatározzák a kiszolgálónk egyik alapvető tulajdonságát: részekre, partíciókra fogjuk osztani a merevlemez. Automatikus felosztást is választhatunk, de jobb, ha mi magunk határozzuk meg az arányokat (5. ábra)



5. ábra

A Linux operációs rendszerben az elsődleges IDE csatolóra kapcsolt master eszköz jele **hda**. Az elsődleges slave egység jele **hdb**, és a másodlagos IDE vonalra kapcsolt eszközök jelei **hdc** és **hdd**. Tehát ha az elsődleges IDE csatolóra csatlakoztattuk a merevlemezt és az master eszköz, akkor 6. ábrához hasonló képet kell hogy lássunk.

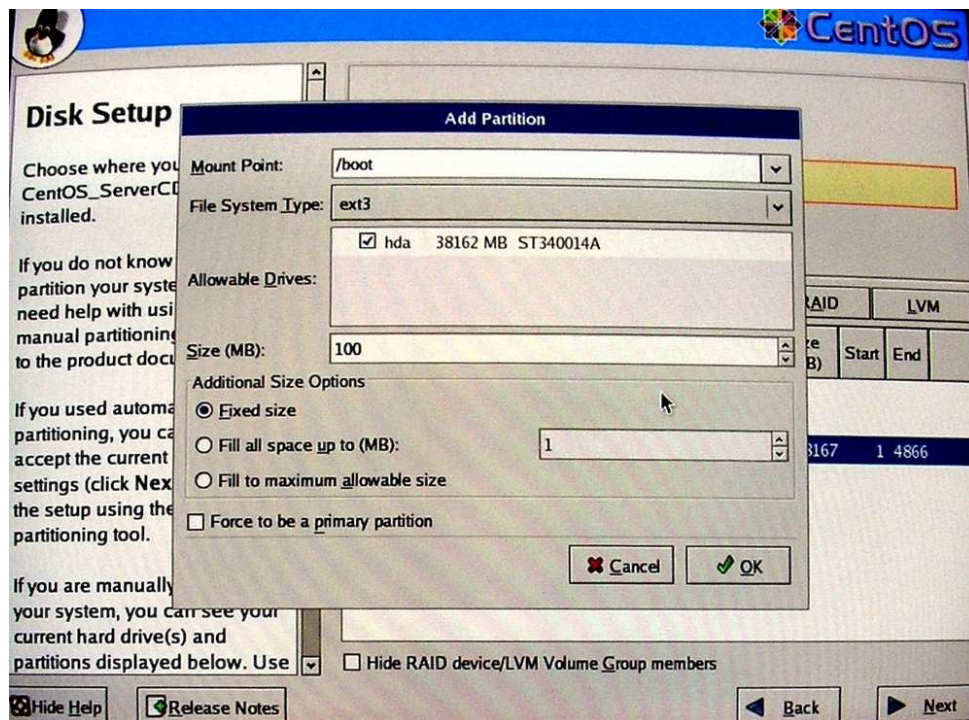


6. ábra

Partíciókat tartalmazó merevlemez esetén töröljük minden lemezrész, kiválasztva azt az egérrel és Delete kapcsolóra kattintva. Természetesen minden adat visszavonhatatlanul elvész az eszközről! A 6. ábrán azt látjuk, hogy egy 40 Gb-os, üres merevlemez van a gépünkben.

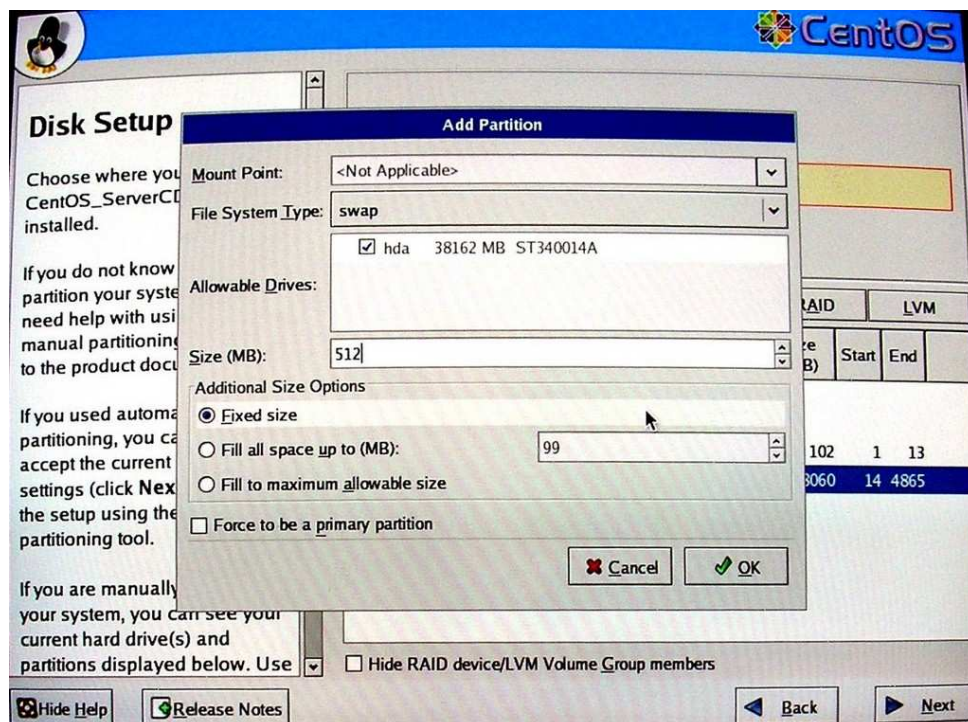
Hozzuk létre az első lemezrész. Ehhez kattintsunk a New (Új) gombra. A megjelenő ablakban a Mount Point (csatolási pont) sorban válasszuk a **/boot** -ot, a Size (Mb): (méret, megabájtban) sorba

írjunk 100-at. (7. ábra) Ezzel azt értük el, hogy a /boot könyvtár a rendszerünkön külön lemezrészre kerül.



7. ábra

A második lemezrész a swap lesz. Ez valójában a fizikai memória (RAM) kiterjesztése. Általában elegendő ha a mérete a RAM kétszerese, de 512 Mb-nál nagyobb nem szükséges. Ismét a new gombra kattintva File System Type (fájlrendszer típus) sorban válasszuk a **swap** -ot, a Size sorba pedig írjunk 512-t. (8. ábra)



8. ábra

A boot lemezrészhez hasonlóan hozzuk létre a következő lemeztérképet:

Csatolási pont	Méret (Mb)
/	3000
/var	4000
/var/spool/squid	2000
/home	28000

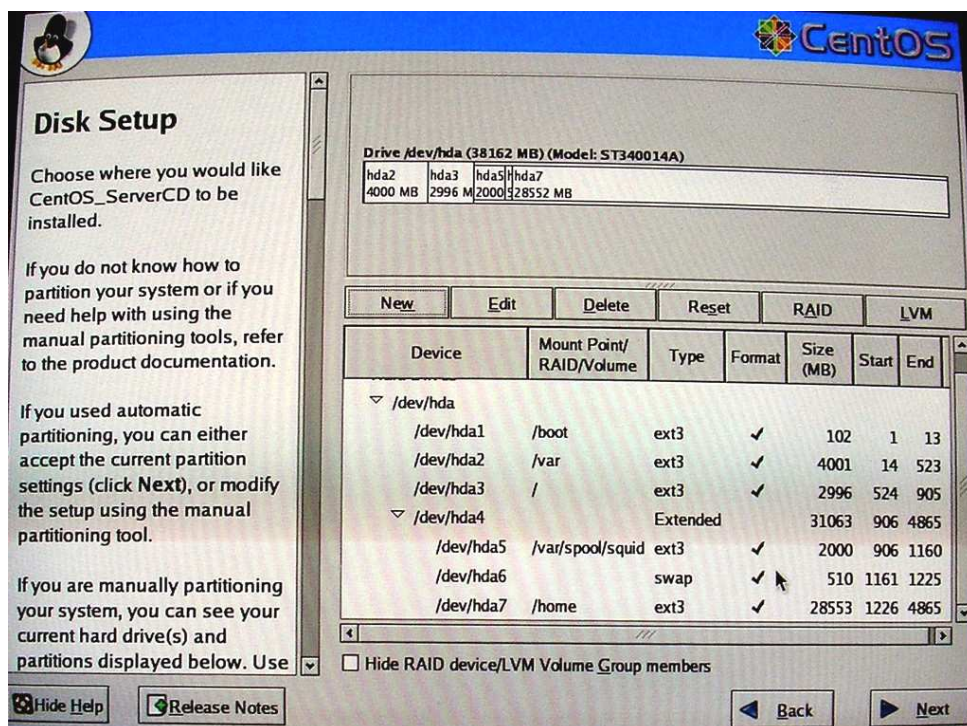
Nagyon fontos a /, vagy ahogyan általában nevezik, a fő- vagy gyökérkönyvtár létrehozása. Az általam kiválasztott arányok természetesen módosíthatóak, különösen, ha nem 40 Gb-os, hanem annál nagyobb merevlemez áll rendelkezésünkre.

A rendszer működése során a **/var** könyvtárba kerülnek a naplóbejegyzések, az Internet-használat statisztikai adatai és webkiszolgáló adatai is. Ha sok oktatási anyagot szeretnénk közzétenni a belső hálózaton, különálló, több GB-os partícióra tegyük a **/var/html** könyvtárat.

A **/var/spool/squid** csatolási pontot nem választhatjuk ki, ezért írjuk be a Mount Point sorba. Ide a proxy kiszolgáló adatai kerülnek majd.

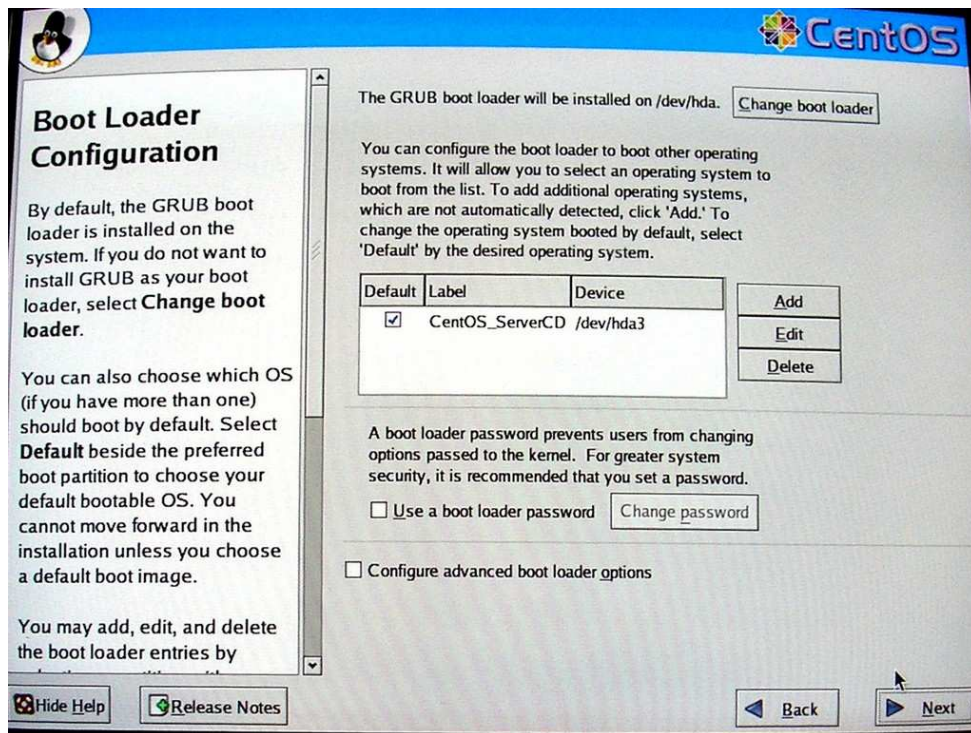
Az utolsó **/home** lemeztérkép létrehozásánál válasszuk a „Fill to maximum allowable size” kapcsolót, ezzel a teljes szabad tárterületet lefoglaljuk számára. A **/home** könyvtárban a felhasználóink saját könyvtárai jönnek majd létre, amit a munkaállomásokról, Windows operációs rendszer alatt is elérhetnek, saját felhasználói név és jelszó megadásával. Erre a részre tárhely korlátozást, *quota-t* is alkalmazunk majd. Általában egy felhasználónak 100 Mb tárterület elegendő, vagyis 28 Gb akár 280 felhasználónak is elegendő tárhelyet biztosít.

A fenti táblázatban megadott értékekkel létrehozott lemeztérképet a 9. ábra mutatja.



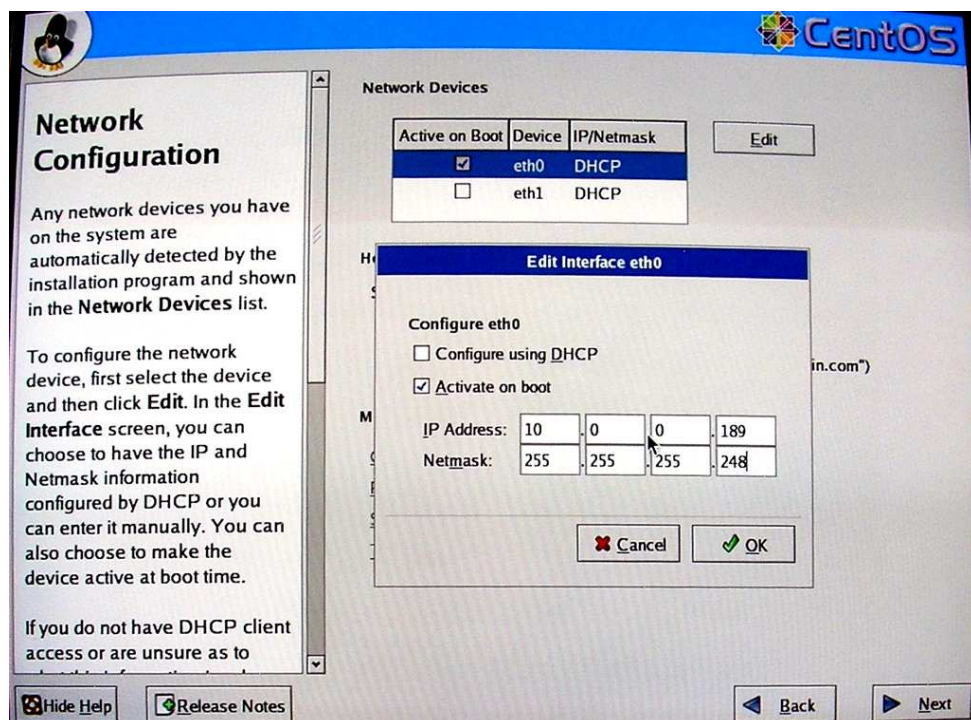
9. ábra

A következő ablakban a rendszerbetöltő program helyét és tulajdonságait módosíthatjuk. (10. ábra) Itt semmit sem kell módosítani, kattintsunk a Next -re.



10. ábra

Itt a hálózati csatolók tulajdonságait kell megadnunk. (11. ábra) A Linux operációs rendszerben az első hálózati csatolónak **eth0**, a másodiknak **eth1** a neve. Az ábrán látjuk, hogy mindkét eszközt felismerte a rendszer. Ki kell választani és az Edit (szerkesztés) kapcsolóval beállítani az eszközt. A DHCP kapcsolót kapcsoljuk ki.

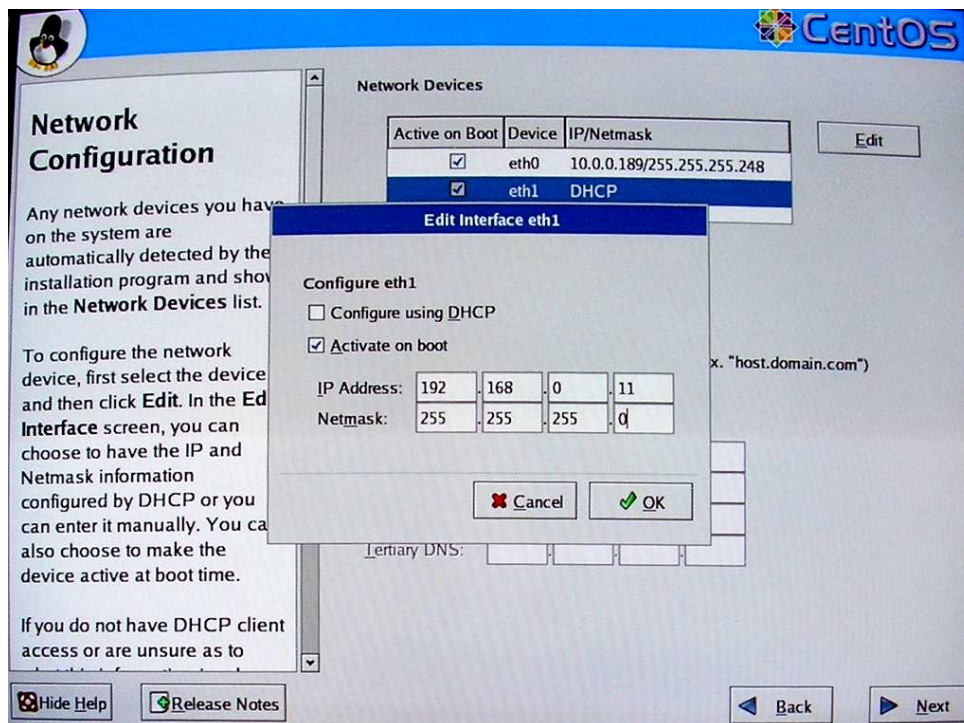


11. ábra

Az eth0 hálózati kártya az Internet szolgáltató által telepített eszközhöz csatlakozik¹, a megjelenő ablakba beírjuk a szolgáltatótól kapott adatokat: IP cím és Hálózati maszk. A második

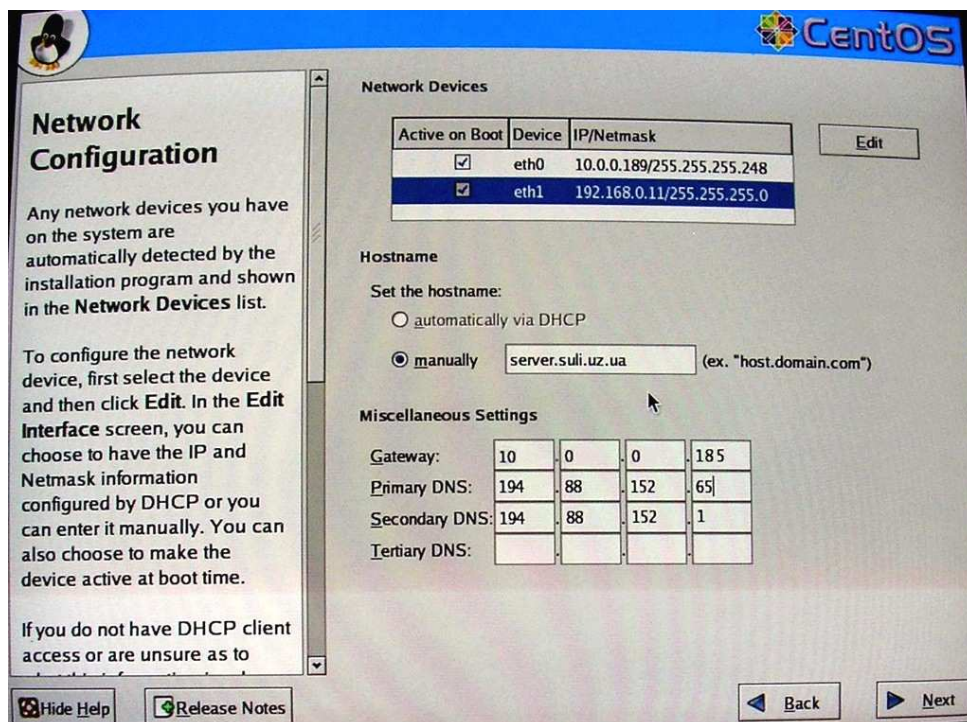
¹ PPPoE protokollt használó ADSL kapcsolat esetén nem kell módosítani az eth0 eszköz beállításait. Telepítés után az adsl-setup paranccsal állíthatjuk majd be a kapcsolatot.

eszközt kiválasztva beírjuk az általunk választott privát IP tartományból egy IP címet. Tulajdonképpen bármit választhatunk a 192.168.X.Y tartományból, ahol $X = 0 - 254$, $Y = 1 - 254$. Arra viszont ügyeljünk, hogy ha az első két szám egyezik a két IP címbe (vagyis a szolgáltató is belsőhálózati címet adott), a harmadiknak már különbözni kell. Ebben a hálózatban, ahol kipróbáltam a rendszert a 192.168.0.1 már foglalt volt, ezért a 192.168.0.11-et választottam. (12. ábra) A hálózati maszk 255.255.255.0 legyen.



12. ábra

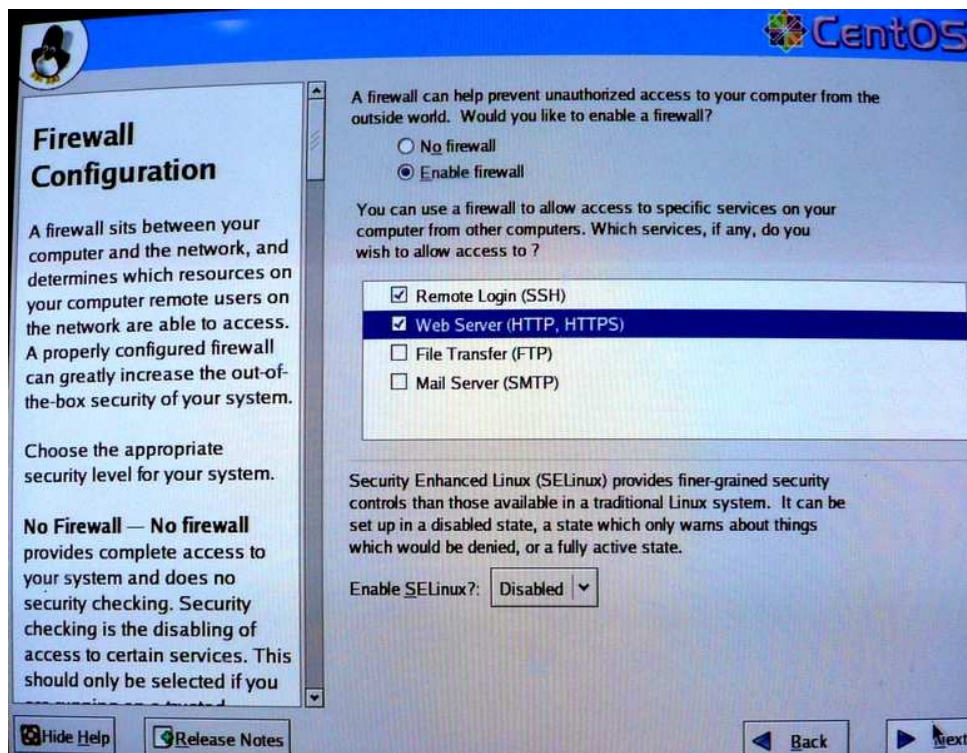
A hostname (gépnév) beállítása előtt egyeztessünk a szolgáltatóval, amennyiben az nem határozott meg nevet, választhatunk bármit. Nagyon fontos a Gateway (átjáró), és a Primary DNS (elsődleges névkiszolgáló, vagy DNS) pontos megadása. Ezeket az IP címeket a szolgáltató közli. Ha van másodlagos DNS adatunk, azt is írjuk be. (13. ábra)



13. ábra

A képen látható eth0 IP cím, átjáró és DNS adatok minden szolgáltatónál és minden ügyfélnél mások. A rendszer csak akkor fog működni, ha a saját szolgáltatónk által közölt, általa számunkra meghatározott paramétereket adjuk meg.

A következő lépésben a tűzfal programot kapcsolhatjuk be és módosíthatjuk a beállítást. Állítsuk be, hogy a tűzfal legyen bekapcsolva (Enable firewall) és a szolgáltatások közül válasszuk ki az első kettőt: Távoli belépés (Remote Login (SSH)) és Webszerver (Web Server (http, HTTPS)). Az Enable SELinux?-nál is válasszuk a Disabled (kikapcsolva) lehetőséget. (14. ábra) A megjelenő ablakban a Proceed (tovább) –ot.

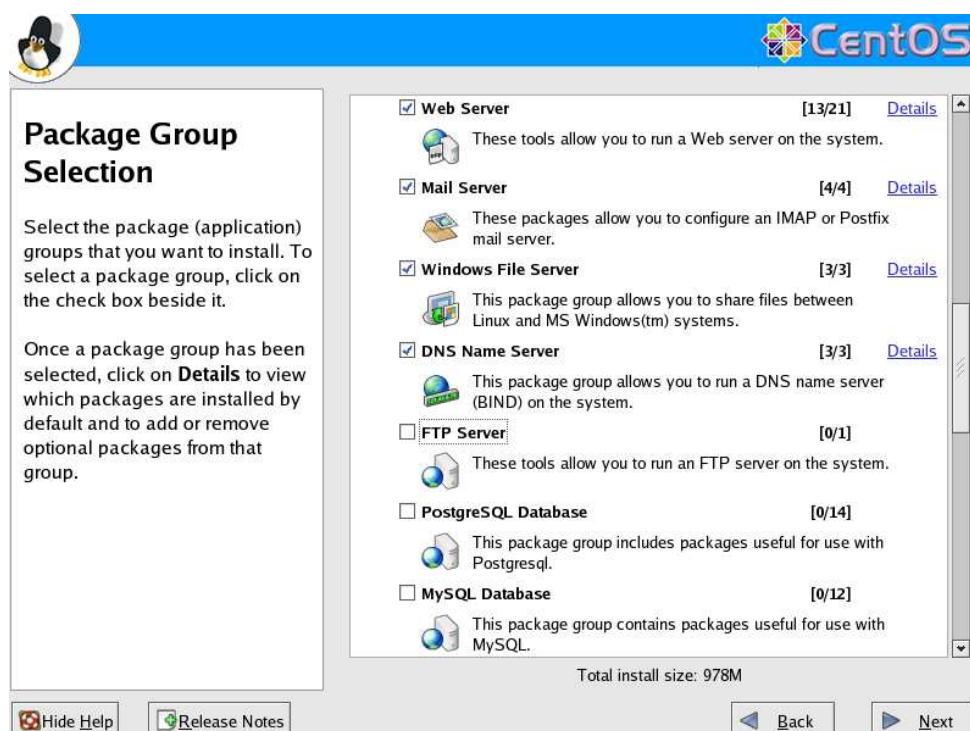


14. ábra

A következő ablakban másodlagos nyelvet választhatnánk, de mint említettem, kiszolgálón nincs ilyenre szükség, kattintsunk a Next kapcsolóra.

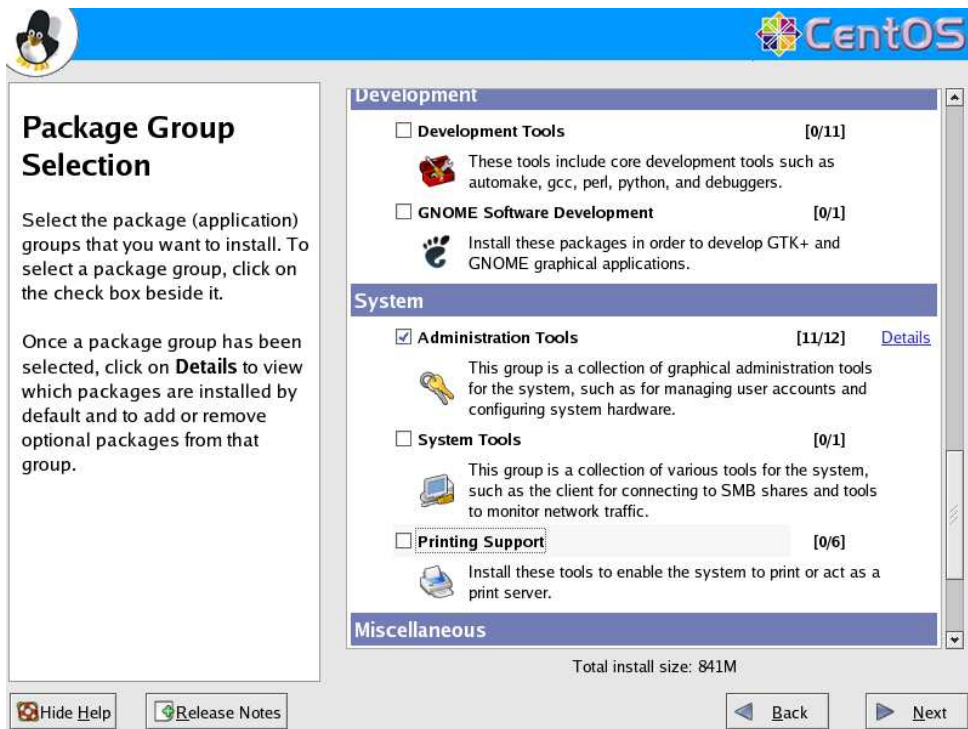
Az időzóna kiválasztásánál keressük ki az Europe / Budapest sort, és a következő ablakban elérkeztünk a root jelszó megadásához. A root nevű felhasználó a Linux rendszerünk elsődleges felhasználója. A root bármilyen állomány módosíthat és letörölhet, gyakorlatilag bármit megtehet a rendszeren. Az alapvető szabályokat betartva kell a jelszavát kiválasztani: legalább 8 karakterből álljon, kis- és nagybetűt, számokat és speciális karaktereket (? , . - _ @ \ stb.) is tartalmazzon. **A root jelszót ne írjuk fel sehová, ne felejtsük el, és ne áruljuk el senkinek!** Ezt a jelszót kétszer begépelve és a Next gombra kattintva a telepítendő csomagok kiválasztásához jutunk. Itt válasszuk a „Customize software packages to be installed” (egyesedi csomagválasztás) kapcsolót.

A következő ablak a csomagcsoportokat és azok tartalmát mutatja. Kapcsoljuk ki az Ftp Server telepítését, (15. ábra) s ha nem szeretnénk nyomtató-kiszolgálóként is használni szervertünket (ez a leírás nem tárgyalja) a Printing Support –ot (nyomtatók támogatása) is kapcsoljuk ki. (16. ábra)

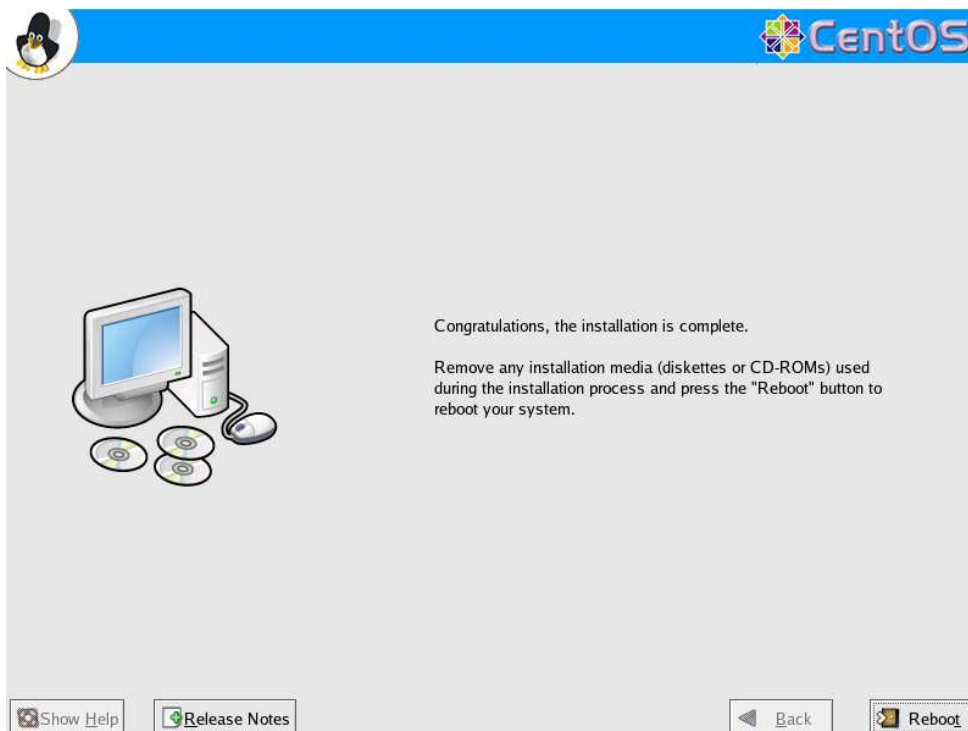


15. ábra

Ezután indulhat a telepítés, ami a gépünk sebességétől függően 5 – 10 percre tarthat. A folyamat végeztével a rendszer figyelmeztet, hogy távolítsuk el a CD-ROM-ot a meghajtóból és Reboot kapcsolóval a gép újraindul. (17. ábra)



16. ábra



17. ábra

III. Ismerkedés az operációs rendszerrel

Néhány alapvető parancs

Jelentkezzünk be a rendszerre root-ként: a „login:” után írjuk be hogy root, és üssük le az Enter-t. A megjelenő „Password:” után a telepítéskor megadott jelszót írjuk.

Az alapértelmezett prompt után villog a kurzor, a rendszer várja a parancsainkat:

```
[root@server ~]#
```

A prompt-ból látjuk, hogy root-ként, a server nevű gépen vagyunk bejelentkezve, a ~ jel arra utal, hogy a jelenlegi aktuális könyvtár a saját home könyvtárunk. Ezt ellenőrizzük is le a **pwd** parancssal:

```
[root@server ~]# pwd
/root
```

A root felhasználónak a /root könyvtár a home könyvtára, minden további felhasználó home könyvtára a /home könyvtárba kerül.

Lépünk a gyökérkönyvtárba a **cd /** parancssal:

```
[root@server ~]# cd /
[root@server /]#
```

A prompt megváltozott, a ~ helyett a gyökérkönyvtár jele, a / szerepel benne

Az **ls** parancssal kilistázhathatjuk egy könyvtár tartalmát. -l paraméterrel kiadva¹ a fájlokról minden információt megjelenít:

```
[root@server /]# ls -l
total 158
drwxr-xr-x  2 root root 4096 Dec 14 02:30 bin
drwxr-xr-x  4 root root 1024 Dec 13 23:46 boot
drwxr-xr-x 10 root root 4820 Dec 18 19:15 dev
drwxr-xr-x 71 root root 4096 Dec 18 19:15 etc
drwxr-xr-x  4 root root 4096 Dec 15 23:36 home
drwxr-xr-x  2 root root 4096 Feb 22  2005 initrd
drwxr-xr-x 11 root root 4096 Dec 16 18:38 lib
drwx----- 2 root root 16384 Dec 14 00:43 lost+found
drwxr-xr-x  3 root root 4096 Dec 18 19:15 media
drwxr-xr-x  3 root root 4096 Dec 16 01:23 mir
drwxr-xr-x  2 root root 4096 Aug 13 12:46 misc
drwxr-xr-x  2 root root 4096 Feb 22  2005 mnt
drwxr-xr-x  2 root root 4096 Feb 22  2005 opt
dr-xr-xr-x 59 root root    0 Dec 18 20:14 proc
drwxr-xr-x  3 root root 4096 Dec 16 01:19 root
drwxr-xr-x  2 root root 12288 Dec 14 02:30 sbin
drwxr-xr-x  2 root root 4096 Dec 13 23:44 selinux
drwxr-xr-x  2 root root 4096 Feb 22  2005 srv
drwxr-xr-x  9 root root    0 Dec 18 20:14 sys
drwxrwxrwt  3 root root 4096 Dec 18 20:20 tmp
drwxr-xr-x 14 root root 4096 Dec 13 23:45 usr
drwxr-xr-x 22 root root 4096 Dec 13 23:49 var
```

A gyökérkönyvtárban könyvtárakat látunk, erre utal a jogosultság mező első karaktere a „d”. A mezők jelentését a /bin könyvtár példáján a következő táblázat mutatja

Jogosultság	Linkszám	Csoport	Felhasználó	Fájl méret	Idő	Fájl név
drwxr-xr-x	2	root	root	4096	Dec 14 02:30	bin

¹ Egy parancs használható paramétereit lekérdezhetjük a --**help** paraméterrel. Részletes lírását a parancsról a **man parancsnév** segítségével jeleníthetünk meg a képernyőn. Kilépés a man-ból: **q** billentyű.

A jogosultság mező 2.-9. karaktere hármas csoportokra bontva a következő jogosultságokat mutatja:

rwX	r-X	r-X
Saját jog u: user	Csoport joga g: group	Többiek joga o: others

ahol r: read - olvasási jog, w: write - írási jog, x: execution - végrehajtási jog. Az olvasási jog a fájl vagy könyvtár tartalmának a megtekintését teszi lehetővé. Az írási jog a fájl illetve könyvtár írására és törlésére ad lehetőséget. A végrehajtási jog pedig fájlok esetén azt jelenti, hogy futtathatjuk a fájlt, könyvtárak esetén pedig beléphetünk a könyvtárba.

Lépünk be a home könyvtárunkba:

```
[root@server ~]# cd ~
```

Hozzunk létre egy proba.txt állományt a **touch** paranccsal:

```
[root@server ~]# touch proba.txt
```

Az **ls -l** paranccsal kilistázzuk az állomány tulajdonságait:

```
[root@server ~]# ls -l proba.txt
-rw-r--r-- 1 root root 0 Dec 18 21:55 proba.txt
```

Bontsuk fel a jogosultság mezőt 1+3+3+3 karaktercsoportokra:

-	Egyszerű fájl
rw-	Az állományt tulajdonosa (root) olvashatja és írhatja. Nem futtathatja
r--	A csoporttulajdonos olvashatja, nem írhatja és nem futtathatja
r--	A többiek olvashatják, nem írhatják és nem futtathatják

A **chmod** parancs a jogosultságok módosítására szolgál. A következő parancs megvonja az olvasási jogot a többiektől:

```
[root@server ~]# chmod o-r proba.txt
[root@server ~]# ls -l proba.txt
-rw-r----- 1 root root 0 Dec 18 22:12 proba.txt
```

Látjuk hogy a parancs sikeresen végrehajtott, a 8. helyen szereplő „r” karakter „-” re változott. Tehát az állományt csak a root felhasználó és a root csoportba tartozó felhasználók olvashatják, mások nem.

A következő táblázat a **chmod** parancs használatát magyarázza:

Kinek / kitől		Mit
u (user) - saját magunk	+ adunk - elveszünk	r (read) olvasási jogot
g (group) - a csoport		w (write) írási jog
o (other) - a többiek		x (execution) végrehajtási jog
a (all) - mindenki		

Jogosultságot egy háromjegyű számmal is meghatározhatunk, aminek az első számjegye a saját, a második csoport, a harmadik pedig mindenki más jogosultságát mutatja. Az olvasási jog (r) négyet, az írási jog (w) kettőt a futtatási jog (x) egyet ér. Ezeket kell összeadni, hogy megkapjuk a jogosultságot beállító számot. Például:

```
[root@server ~]# chmod 710 proba.txt
[root@server ~]# ls -l proba.txt
-rwx--x--- 1 root root 0 Dec 18 22:12 proba.txt
```

Magyarázat: 7 (saját jog) 4+2+1= rwx
1 (csoport jog) 1= --x
0 (mindenki más) 0= ---

Egyetlen parancs kiadásával beállítottuk, hogy mi olvashatjuk, írhatjuk és futtathatjuk az állományt. Csoportunk futtathatja és másoknak nincs semmilyen jogosultságuk

A **du** paranccsal könyvtárak méretét kérdezhetjük le. Az **/sbin** könyvtár mérete:

```
[root@server ~]# du -h /sbin
16M    /sbin
```

A **--max-depth=n** paraméterrel meghatározhatjuk a lekérdezendő alkönyvtárak szintjeinek számát. Az **/usr** könyvtár alkönyvtárainak mérete:

```
[root@server /]# du -h --max-depth=1 /usr
359M    /usr/share
176K    /usr/local
8.0K    /usr/etc
8.0K    /usr/src
888K    /usr/include
358M    /usr/lib
8.0K    /usr/games
1.6M    /usr/kerberos
46M     /usr/bin
9.2M    /usr/X11R6
1.9M    /usr/libexec
20M     /usr/sbin
795M    /usr
```

A **df** parancs összegzi a szabad területet a merevlemezen és kiírja, hogy az adott könyvtár a fájlrendszer melyik pontjához csatlakozik

```
[root@server /]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/hda3        2.9G  776M  2.0G  28% /
/dev/hda1         99M   8.4M   86M   9% /boot
none            157M    0  157M   0% /dev/shm
/dev/hda7        28G   77M   26G   1% /home
/dev/hda2        3.9G   73M   3.6G   2% /var
/dev/hda5        2.0G   53M   1.8G   3% /var/spool/squid
```

Látjuk a telepítésnél létrehozott lemezrészek méreteit, a foglalt és a szabad tárterületét méretét és a foglalt terület százalékarányát.

Linux rendszereken az **/etc** könyvtárban találjuk magának az operációs rendszernek és különböző programoknak konfigurációs állományait. Ahhoz, hogy valamilyen program működését megváltoztassuk, általában egy szöveges állományt kell szerkesztenünk és az adott programot újraindítani.

A **cat** paranccsal megjeleníthetjük szöveges állományok tartalmát képernyőn. A **resolv.conf** állomány a telepítésnél megadott DNS kiszolgálók IP címeit tartalmazza.

```
[root@server ~]# cat /etc/resolv.conf
search sul.uz.ua
nameserver 194.88.152.1
nameserver 194.88.152.65
```

Hosszabb szöveges állományok megjelenítésére használhatjuk a **more** parancsot, ilyenkor szóközzel lapozhatunk a szövegben:

```
[root@server ~]# cat /etc/inittab | more
#
# inittab          This file describes how the INIT process should set up
#                  the system in a certain run-level.
#
# Author:          Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#                  Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
```

```
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have
networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
```

A képernyőrészlet az `/etc/inittab` szöveges állomány első néhány sorát mutatja. Ez az állomány mutatja, hogy operációs rendszerünkön milyen futási szintek léteznek és ezek közül melyik az alapértelmezett. Különböző futási szinteken különböző szolgáltatások indulnak el automatikusan, és vannak speciális szintek, amelyek a rendszer kikapcsolását (0 – halt) és újraindítását (6 – reboot) okozzák. Az **id:3:initdefault:** sor mutatja, hogy a 3. szint az alapértelmezett, vagyis ha egy szolgáltatást ki akarunk kapcsolni, akkor be kell állítani, hogy ezen a szinten ne induljon el.

A következő parancs:

```
[root@server ~]# clear;cat /etc/inittab | tail -23
```

letörli a képernyő tartalmát, megjeleníti az előbbi szöveges állomány utolsó 23 sorát. Figyeljük meg, hogy `;`-vel elválasztva több parancsot is írhatunk egy sorba, valamint a `|` jel az egyik parancs kimenetét átirányítja a másik parancs bemenetére. A képernyőn megjelenő szöveg első két sora a következő:

```
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Az első sor, mivel `#` jellel kezdődik, konfigurációs állományban nincs más szerepe csak a következő sor vagy sorok szerepét magyarázza. A második sor azt mutatja, hogy mi történik a `Ctrl+Alt+Del` billentyűk lenyomásakor. Alapértelmezés szerint rendszer újraindul (`shutdown -r:` kikapcsol és újraindul). Ezt a későbbiekben módosítani fogjuk. Nem szerencsés ha a kiszolgálót ilyen könnyen újra lehet indítani.

A rendszert leállítani a **halt -p** paranccsal tudjuk.

Szöveges állományok szerkesztéséhez az `mcedit` programot fogjuk használni, ami az **mc** (Midnight Commander) programcsomag része. Telepítése előtt ellenőrizzük le a hálózat működését.

Hálózati kapcsolatok ellenőrzése

Telepítésnél már beállítottuk a két hálózati kártyát, az egyik az Internet kapcsolatot biztosító eszközhöz, a másik a munkaállomásokkal együtt a switch-hez csatlakozik. Hogy a két eszköz közül melyik a belsőhálózati, legegyszerűbben úgy ellenőrizhetjük, hogy az egyik eszközt a switch-hez csatlakoztatjuk és szintén a switch-hez kapcsolt és megfelelően beállított munkaállomáson elindítjuk a Windows Parancssort. Először az ipconfig paranccsal leellenőrizzük a munkaállomás hálózati beállításait:

```
C:\Documents and Settings\pferi>ipconfig

Windows IP konfiguráció

Ethernet-adapter Helyi kapcsolat:

    Kapcsolatspecifikus DNS-utótag. . . . . :
    IP-cím. . . . . : 192.168.0.31
    Alhálózati maszk. . . . . : 255.255.255.0
    Alapértelmezett átjáró. . . . . : 192.168.0.11
```

Majd a **ping** paranccsal a kapcsolat meglétét a munkaállomás és a szerver között:

```
C:\Documents and Settings\pferi>ping 192.168.0.11

192.168.0.11 pingelése 32 bájt méretű adatokkal:

Válasz 192.168.0.11: bájt=32 idő=1 ms TTL=64
Válasz 192.168.0.11: bájt=32 idő=1 ms TTL=64
Válasz 192.168.0.11: bájt=32 idő<10 ezredmp. TTL=64
Válasz 192.168.0.11: bájt=32 idő=1 ms TTL=64

192.168.0.11 ping-statisztikája:
    Csomagok: küldött = 4, fogadott = 4, elveszett = 0 (0% veszteség),
    Oda-vissza út ideje közelítőlegesen, milliszekundumban:
        minimum = 0ms, maximum = 1ms, átlag = 0ms
```

Természetesen a ping parancs után a telepítéskor megadott IP címet írjuk. Ha a fentihez hasonlóan kapunk válaszokat a szervertől, akkor eltaláltuk a csatolót, ha nem, akkor az UTP vezeték csatlakoztassuk a másik hálókártyához.

Csatlakoztassuk az 1. ábrának megfelelően a másik hálókártyát az AP eszközhöz. Ajánlatos un. UTP Patch Cord kábelt alkalmazni.

A Linux-on az **ifconfig** paranccsal megjeleníthetjük a hálózati eszközök tulajdonságait:

```
[root@server /]# ifconfig

eth0      Link encap:Ethernet  HWaddr 00:08:C7:69:A7:8C
          inet addr:10.0.0.189  Bcast:10.0.0.191  Mask:255.255.255.248
          inet6 addr: fe80::208:c7ff:fe69:a78c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6896 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7044 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8401527 (8.0 MiB)  TX bytes:649325 (634.1 KiB)

eth1      Link encap:Ethernet  HWaddr 00:02:B3:1E:F1:1A
          inet addr:192.168.0.11  Bcast:192.168.0.255
          Mask:255.255.255.0
          inet6 addr: fe80::202:b3ff:fe1e:f11a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7629 errors:0 dropped:0 overruns:0 carrier:0
```

```

collisions:0 txqueuelen:1000
RX bytes:619451 (604.9 KiB) TX bytes:8237526 (7.8 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2612 (2.5 KiB) TX bytes:2612 (2.5 KiB)

[root@server /]#

```

A **mii-tool** paranccsal leellenőrizhetjük, hogy mindkét hálózati csatoló kapcsolata rendben van-e és milyen a kapcsolat sebessége. Ugyanez a parancs **-v** paraméterrel részletes információt szolgáltat a hálózati eszközökről:

```

[root@server /]# mii-tool
eth0: negotiated 100baseTx-FD flow-control, link ok
eth1: negotiated 100baseTx-FD flow-control, link ok

[root@server etc]# mii-tool -v
eth0: negotiated 100baseTx-FD flow-control, link ok
      product info: Intel 82555 rev 0
      basic mode:   autonegotiation enabled
      basic status: autonegotiation complete, link ok
      capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
      advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-
control
      link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-
control
eth1: negotiated 100baseTx-FD flow-control, link ok
      product info: Intel 82555 rev 4
      basic mode:   autonegotiation enabled
      basic status: autonegotiation complete, link ok
      capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
      advertising:  100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-
control
      link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-
control

```

A félkövér formázással kiemelt szövegrész az eszköz típusát mutatja, ha különbözőket alkalmaztunk, megkönnyíti az eth0 és eth1 eszközök megkülönböztetését.

Ellenőrizzük a ping paranccsal, hogy van-e kapcsolat az átjáróval. Természetesen a 10.0.0.185 helyett a szolgáltató által megadott IP címet írjuk. Ha megjelent a képernyőn néhány sor a Ctrl+C billentyűkombinációval állítsuk le a parancs végrehajtását.

```

[root@server ~]# ping 10.0.0.185
PING 10.0.0.185 (10.0.0.185) 56(84) bytes of data.
64 bytes from 10.0.0.185: icmp_seq=0 ttl=64 time=0.880 ms
64 bytes from 10.0.0.185: icmp_seq=1 ttl=64 time=0.235 ms
64 bytes from 10.0.0.185: icmp_seq=2 ttl=64 time=0.257 ms

--- 10.0.0.185 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.235/0.457/0.880/0.299 ms, pipe 2
[root@server ~]#

```

A kapcsolat rendben van, a „0% packet loss” azt jelenti, hogy nem volt elveszett csomag. A következő ping paranccsal leellenőrizhetjük a DNS kiszolgálóval a kapcsolatot. Ha a domain névhez meghatároz a rendszer IP címet, akkor a névkiszolgáló beállításai is megfelelőek:

```
[root@server ~]# ping www.centos.org
PING www.centos.org (204.10.37.194) 56(84) bytes of data.
64 bytes from CentOS.org (204.10.37.194): icmp_seq=0 ttl=29 time=369 ms
64 bytes from CentOS.org (204.10.37.194): icmp_seq=1 ttl=29 time=319 ms
64 bytes from CentOS.org (204.10.37.194): icmp_seq=2 ttl=29 time=319 ms
64 bytes from CentOS.org (204.10.37.194): icmp_seq=3 ttl=29 time=319 ms

--- www.centos.org ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 319.419/332.134/369.612/21.649 ms, pipe 2
```

ADSL kapcsolat beállítása

Amennyiben az Internet szolgáltatóval a kapcsolatot ADSL modem biztosítja (18. ábra), csatlakoztassuk a modemet a telefonvonalhoz és UTP Patch Cord kábelrel az eth0 hálózati interfészhez. Kapcsoljuk be a modemet a dokumentációjában leírtak szerint.



18. ábra

Adjuk ki a következő két parancsot:

```
[root@server ~]# ifconfig eth0 0.0.0.0 up
[root@server ~]# adsl-setup
```

A második parancs elindít egy programot, ami segít beállítani a kapcsolatot. A megjelenő kérdések közül az első a szolgáltatótól kapott felhasználó névre vonatkozik (LOGIN NAME), a második a hálózati eszközre (INTERFACE). Ez esetünkben eth0. A harmadik kérdés arról szól, hogy megszakítsa-e a kiszolgáló kapcsolatot, ha nincs adatforgalom. Itt nem kell semmit beírni, csak üssük le az Enter-t (alapérték – nem). A következőkben a szolgáltató által megadott DNS kiszolgáló IP címét, vagy ha nem adott meg ilyet a szolgáltató a **server** szót. Ezután írjuk be a jelszót kétszer (PASSWORD). A következő kérdésre a válasz legyen nem (no), így a rendszerünk felhasználói nem bonthatják a kapcsolatot. A tűzfal (FIREWALLING) kiválasztásánál válasszunk a 0-t, hiszen a későbbiekben mi magunk fogjuk meghatározni a tűzfalszabályokat. A következő kérdésre

válaszoljunk yes-t, hogy a kapcsolat felépüljön a gép indulásakor. Ezután a program megjeleníti az általunk beírt adatokat. Elfogadva ezeket a kapcsolat beállítása befejeződik.

A következő parancs felépíti a kapcsolatot:

```
[root@server ~]# adsl-start
```

Ellenőrizzük a kapcsolat működését a ping paranccsal.

Amennyiben nem épül fel a kapcsolat, ellenőrizzük a modem állapotát (megfelelően csatlakoztatott kábelek, világító LED-ek) a dokumentációban leírtak szerint. Ellenőrizzük, hogy az általunk megadott adatok megfelelnek a szolgáltatóval kötött szerződésben foglaltakkal.

A Midnight Commander telepítése

A fájlkezelési műveleteket és a szöveges állományok szerkesztését nagyon megkönnyíti a Midnight Commander program. Tulajdonképpen ez egy Norton Commander szerű, kétpaneles fájlkezelő program, a legtöbb funkcióbillentyű rendeltetése is ugyanaz. (F3 - nézőke, F4 – szerkeszt, F5 - másol, F6 - áthelyez, F8 - töröl, F10 - kilép, Tab billentyű - váltás panelek között)

Az Internetről letöltött programcsomagok épségét ellenőrzi a rendszer. Adjuk meg az ellenőrzéshez szükséges kulcsot:

```
[root@server ~]# rpm --import /usr/share/rhn/RPM-GPG-KEY*
```

Az mc telepítéshez adjuk ki a következő parancsot:

```
[root@server ~]# yum install mc
```

A rendszer figyelmeztet, hogy 1,7 Mb-ot fog letölteni az Internetről, ami a hálózat sebességétől függően néhány perc alatt lezajlik. (19. ábra) A telepítés végeztével adjuk ki az mc parancsot (20. ábra)

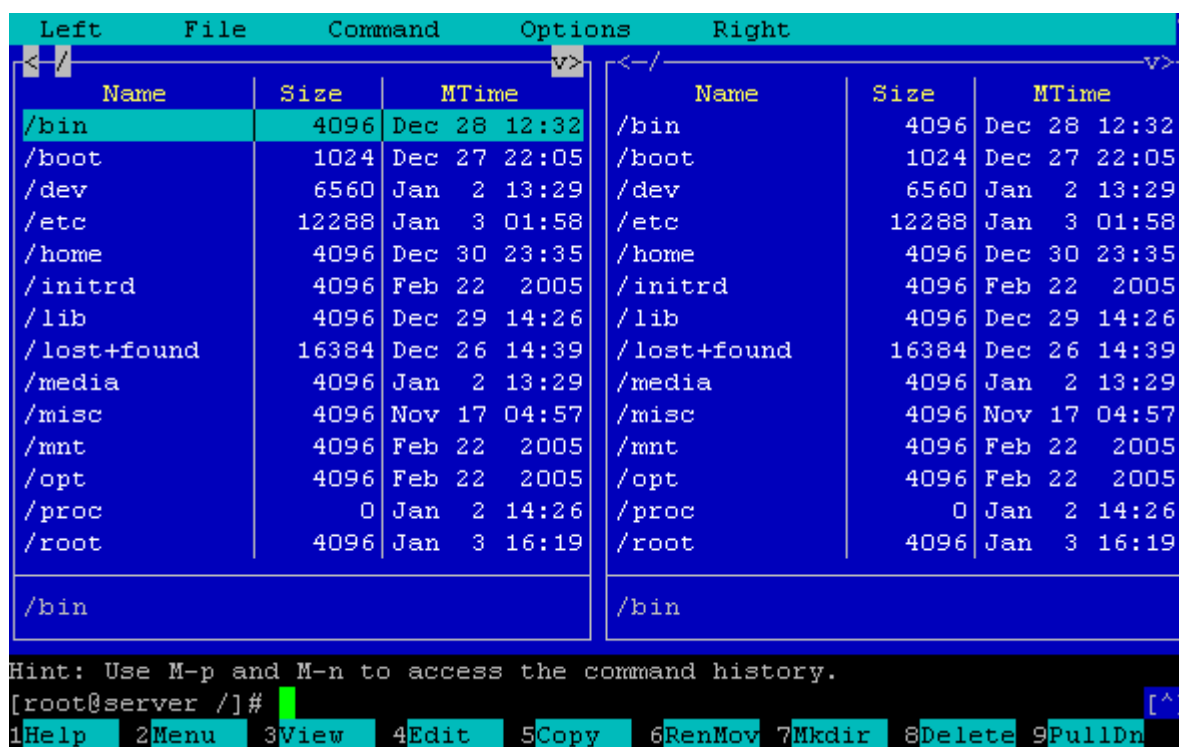
```
Dependencies Resolved

=====
Package                Arch      Version      Repository    Size
=====
Installing:
mc                     i386      1:4.6.1-0.8.1  base          1.7 M

Transaction Summary
=====
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)
Total download size: 1.7 M
Is this ok [y/N]: y
Downloading Packages:
(1/1): mc-4.6.1-0.8.1.i386 100% |=====| 1.7 MB    07:36
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: mc                                     ##### [1/1]

Installed: mc.i386 1:4.6.1-0.8.1
Complete!
[root@server ~]#
```

19. ábra



20. ábra

Néhány konfigurációs állomány módosítása

A Midnight Commander segítségével könnyen szerkeszthetünk szöveges állományokat. Lépünk be az /etc könyvtárba és keressük meg az **inittab** állományt. Az F4 billentyűvel nyissuk meg szerkesztésre. A 17. sort módosítjuk a következőre:

```
ca::ctrlaltdel:/bin/echo "Nem indul újra. Használja a reboot parancsot!"
```

Az F2 billentyű lenyomásával mentjük a módosított állományt, az mc megerősítést kér, üssük le az Enter-t. A Ctrl+O billentyűparanccsal a Midnight Commander ablakát elrejtethetjük, majd ugyanúgy vissza is állíthatjuk. Adjuk ki az **init q** parancsot:

```
[root@server etc]# init q
```

Ezután a Ctrl+Alt+Del billentyűk lenyomásakor már nem indul újra a kiszolgáló, hanem a beírt szöveg jelenik meg a képernyőn. Ha a szerver minden munkanap végén leállítjuk megfontolandó, hogy az inittab állományt a következőképp módosítsuk:

```
ca::ctrlaltdel:/sbin/halt -p
```

Az **init q** parancs kiadása után akár bejelentkezés nélkül is leállíthatjuk a rendszert a Ctrl+Alt+Del billentyűk lenyomásával.

Módosítsuk az **/etc/sysconfig/i18n** állomány első sorát a következőre:

```
LANG="en_US"
```

Mentsük a módosított állományt és az F10 funkcióbillentyűvel lépünk ki az mc-ből.

Operációs rendszerünk a hálózati eszközök beállításait szöveges állományokban tárolja. Az eth0 hálózati eszköz paramétereit az **/etc/sysconfig/network-scripts/ifcfg-eth0** az ez eth1 eszközt pedig értelemszerűen a **/etc/sysconfig/network-scripts/ifcfg-eth1** állományban. Jelenítsük meg a képernyőn ennek a két állománynak a tartalmát:

```
[root@server ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.0.0.191
HWADDR=00:08:C7:85:12:F5
IPADDR=10.0.0.189
NETMASK=255.255.255.248
NETWORK=10.0.0.184
ONBOOT=yes
TYPE=Ethernet

[root@server ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=static
BROADCAST=192.168.0.255
HWADDR=00:50:DA:38:36:CC
IPADDR=192.168.0.11
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
TYPE=Ethernet
```

A HWADDR sor a hálózati eszköz fizikai címét mutatja, amit MAC (Media Access Controll) címnek is neveznek. Ez egy 6 bájttal hosszúságú szám, amit tizenhatos számrendszerben, kettőspontokkal elválasztva ábrázolnak. Minden eszköz a gyártó által meghatározott és egyedi MAC címmel rendelkezik.

A Midnight Commander szerkesztőjének segítségével, ha szükséges, módosíthatjuk az IP címet, hálózati maszkot és az átjáró beállításait. Ahhoz, hogy az új beállítások érvényre jussanak, indítsuk újra a hálózatot:

```
[root@centos44 ~]# service network restart
```

Az operációs rendszer újraindításával is érvényesíthetjük a beállításokat. Ezt a **reboot** paranccsal tehetjük meg.

Az operációs rendszer frissítése

Nagyon fontos, hogy időközönként frissítsük a rendszerünket. Frissítéskor a rendszer leellenőrzi, hogy milyen csomagokat kell frissíteni, letölti őket és telepíti. Az első frissítéskor több 10 MB-ot tölt le, így ez a kapcsolat sebességétől függően akár órákig is tarthat.

```
[root@server ~]# yum update
```

A rendszerünk megjeleníti a frissítendő csomagokat és megerősítést kér a csomagok letöltéséhez. (21. ábra)

```

openssh-clients      i386      3.9p1-8.RHEL4.17.1  update      341 k
openssh-server       i386      3.9p1-8.RHEL4.17.1  update      208 k
openssl             i686      0.9.7a-43.14        update      1.1 M
php                  i386      4.3.9-3.22          update      1.3 M
php-ldap             i386      4.3.9-3.22          update       34 k
php-pear             i386      4.3.9-3.22          update      267 k
python               i386      2.3.4-14.3          update      4.8 M
rpmdb-CentOS         i386      2:4.4-0.20060823     base        28 M
sysreport            noarch    1.3.15-8            update       18 k
tzdata               noarch    2006m-3.el4         update      444 k
up2date              i386      4.4.69-25.centos4.7  update      1.8 M
xorg-x11-Mesa-libGL   i386      6.8.2-1.EL.13.37.2  update      378 k
xorg-x11-font-utils   i386      6.8.2-1.EL.13.37.2  update      302 k
xorg-x11-libs         i386      6.8.2-1.EL.13.37.2  update      2.7 M
xorg-x11-xauth        i386      6.8.2-1.EL.13.37.2  update      280 k
xorg-x11-xf86         i386      6.8.2-1.EL.13.37.2  update      315 k

Transaction Summary
=====
Install      1 Package(s)
Update      25 Package(s)
Remove       0 Package(s)
Total download size: 67 M
Is this ok [y/N]: y

```

21. ábra

A frissítés sikeres, ha a következő sorokhoz hasonlóak jelennek meg a képernyőn. A próbarendszeren öt és fél óráig tartott a csomagok letöltése. Igaz, 32 kilobit/sec sávszélességen. A következő frissítésnél már lényegesen kevesebb adatot fog letölteni.

```

Cleanup : openssh-server      ##### [40/49]
Cleanup : php-ldap            ##### [41/49]
Cleanup : info                 ##### [42/49]
Cleanup : up2date              ##### [43/49]
Cleanup : comps                ##### [44/49]
Cleanup : php-pear             ##### [45/49]
Cleanup : gzip                 ##### [46/49]
Cleanup : elinks               ##### [47/49]
Cleanup : gnupg                ##### [48/49]
Cleanup : sysreport            ##### [49/49]

Installed: kernel.i686 0:2.6.9-42.0.3.EL
Updated: comps.i386 2:4.4CENTOS-0.20060823 elinks.i386 0:0.9.2-3.3
gnupg.i386 0:1.2.6-8 gzip.i386 0:1.3.3-16.rhel4 hwdatas.noarch
0:0.146.23.EL-1 info.i386 0:4.7-5.el4.2 iproute.i386 0:2.6.9-
3.EL4.3.centos4 nss_ldap.i386 0:226-17 openssh.i386 0:3.9p1-8.RHEL4.17.1
openssh-clients.i386 0:3.9p1-8.RHEL4.17.1 openssh-server.i386 0:3.9p1-
8.RHEL4.17.1 openssl.i686 0:0.9.7a-43.14 php.i386 0:4.3.9-3.22 php-
ldap.i386 0:4.3.9-3.22 php-pear.i386 0:4.3.9-3.22 python.i386 0:2.3.4-
14.3 rpmdb-CentOS.i386 2:4.4-0.20060823 sysreport.noarch 0:1.3.15-8
tar.i386 0:1.14-12.RHEL4 tzdata.noarch 0:2006m-3.el4 up2date.i386
0:4.4.69-25.centos4.7 xorg-x11-Mesa-libGL.i386 0:6.8.2-1.EL.13.37.2
xorg-x11-libs.i386 0:6.8.2-1.EL.13.37.2 xorg-x11-xauth.i386 0:6.8.2-
1.EL.13.37.2
Complete!

```

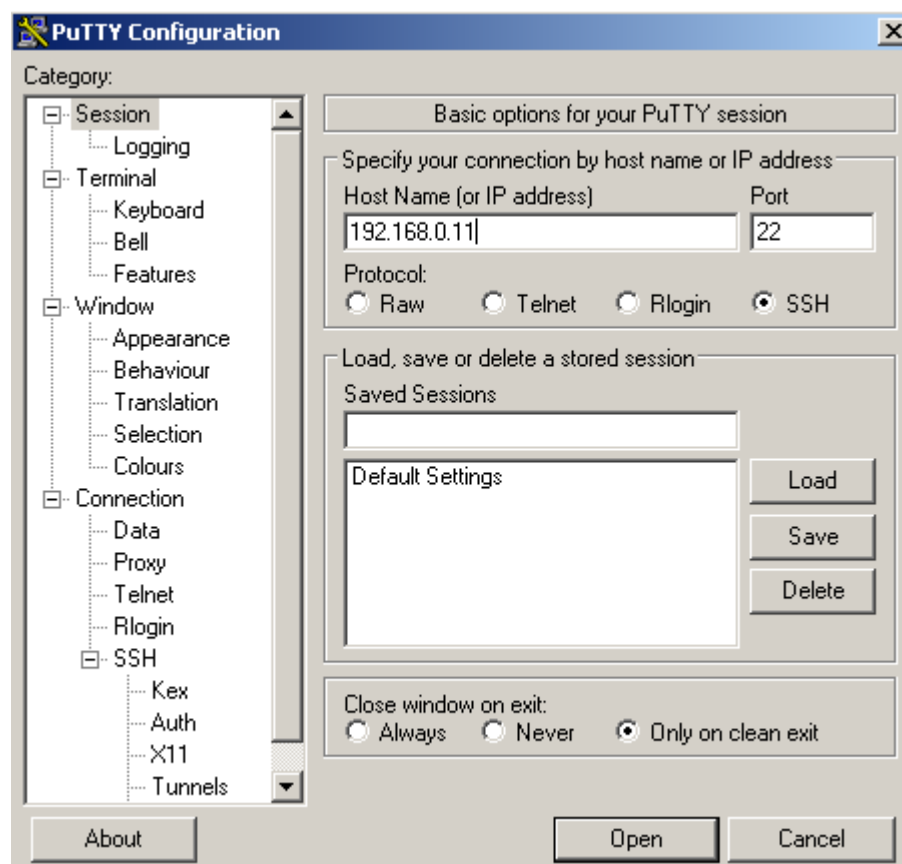
IV. Kapcsolat rendszerek között. Adminisztráció

A PuTTY

Serverünk adminisztrálását egy Windows munkállomásról is megoldhatjuk, speciális segédprogramok felhasználásával. Az egyik ilyen programot a PuTTY-t, a <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> oldalról letölthetjük, illetve a <http://kmf.uz.ua/centos/serverhez1.zip> csomagban is megtaláljuk.

Letöltve a putty.exe állományt bemásoljuk valamelyik mappába, pl. a Program Files –be és készítünk róla egy parancsikont az asztalra.

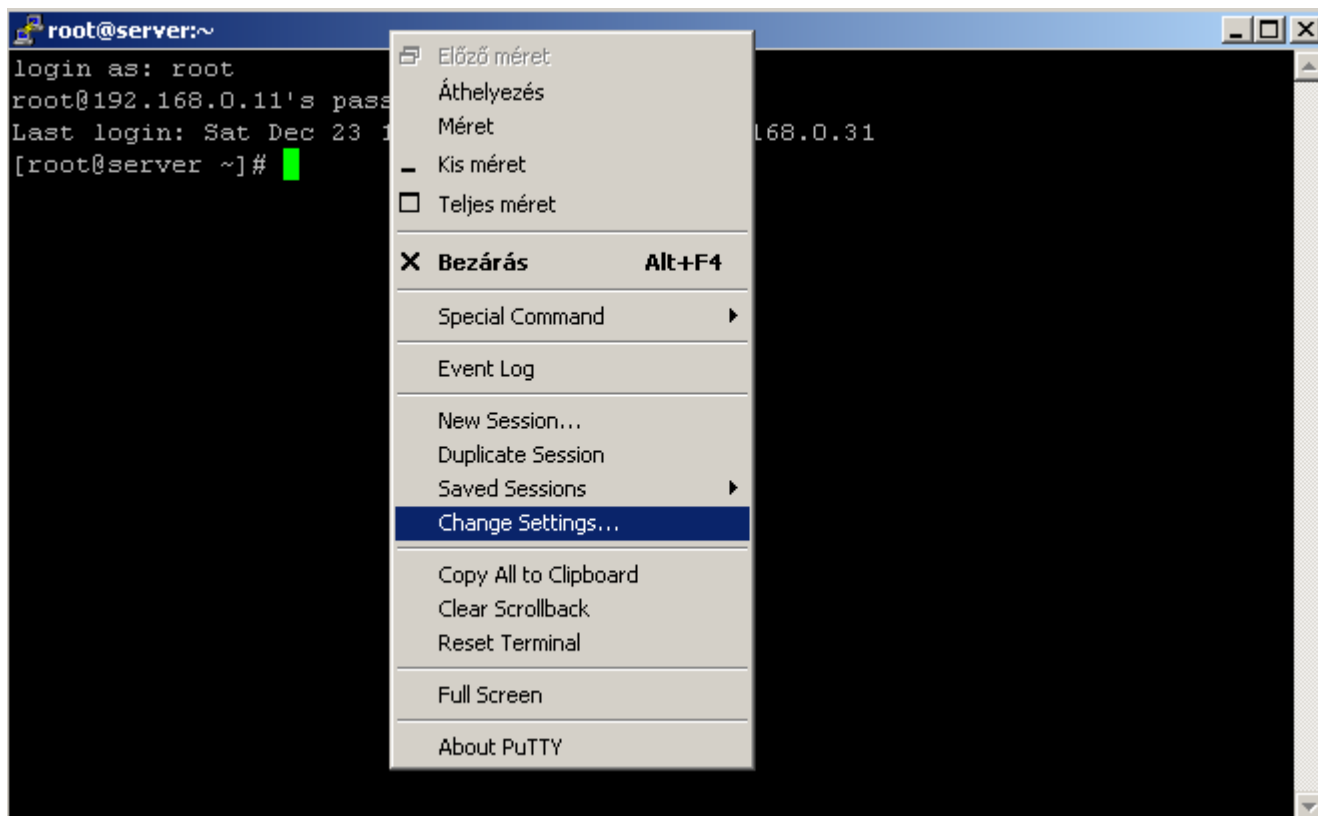
Elindítva írjuk be szerverünk belsőhálózati IP címét a „Host Name (or IP address)” mezőbe és kattintsunk az Open kapcsolóra. (22. ábra. Természetesen, ha más IP címet adtunk meg telepítéskor, akkor azt)



22. ábra

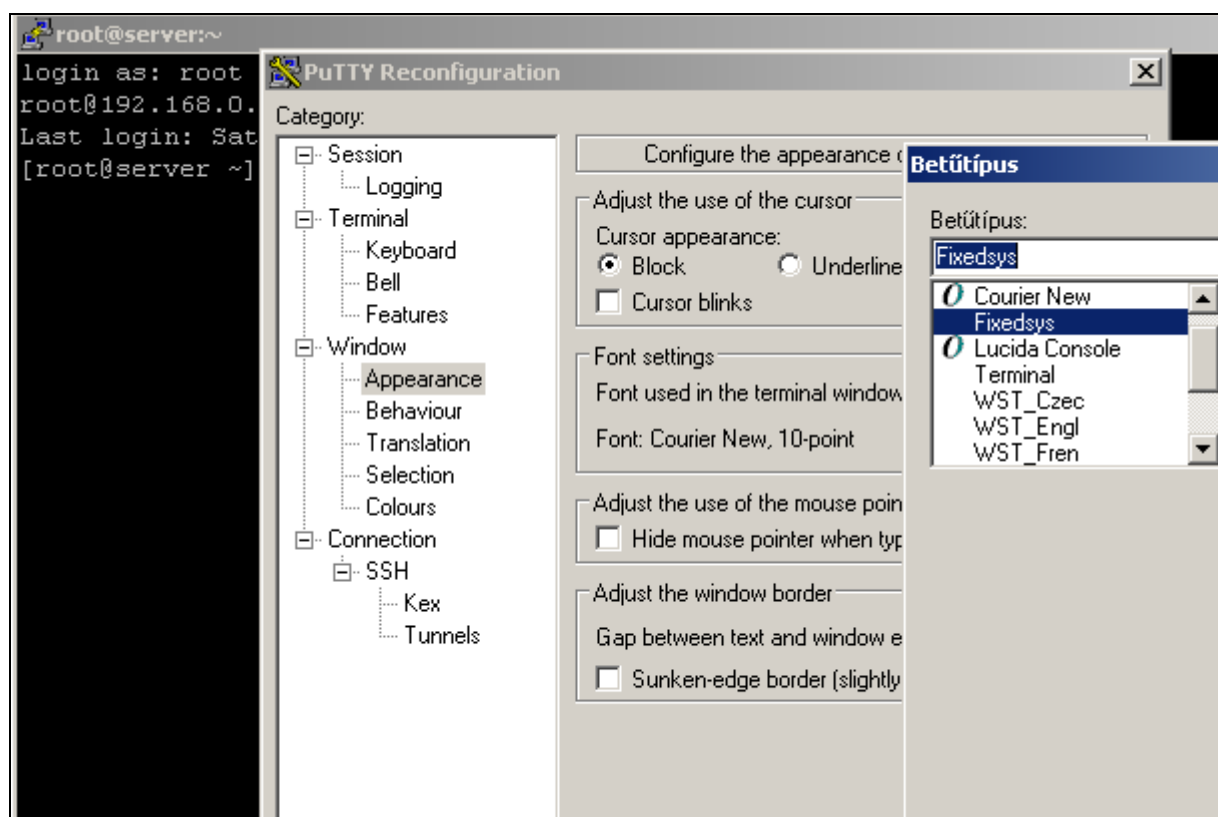
A megjelenő ablak figyelmeztet, hogy ez az első kapcsolat a kiszolgálóhoz, kattintsunk az Igen gombra és jelentkezünk be root-ként. A PuTTY program egy ssh kliens, (a kiszolgálón fut az ssh szerver) segítségével ugyanúgy dolgozhatunk a kiszolgálón, mintha előtte ülnénk. A kiszolgálóhoz sem monitort, sem billentyűzetet nem kell csatlakoztatnunk. A kommunikáció kódoltan zajlik a kliens és szerver között.

Módosítsunk néhány beállítást a programban. Kattintsunk jobb egérgombbal a címsávra és válasszuk a „Change Settings...”-et. (23. ábra)

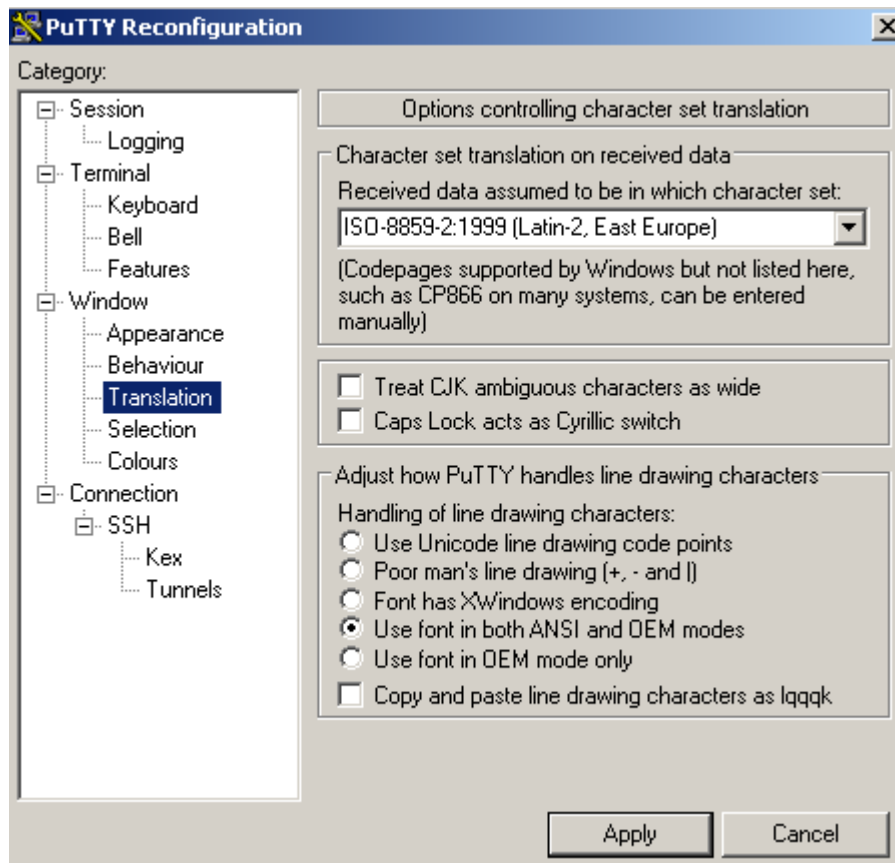


23. ábra

A megjelenő ablakban az „Appearance”-ra kattintva módosíthatjuk a PuTTY által használt betűtípust. A „Change...” kapcsolóval megjelenik a Betűtípus ablak, itt válasszuk a Fixedsys-t. (24. ábra) A „Translation”-t választva kapcsoljuk be az „Use font in both ANSI and OEM modes”-t. (25. ábra)

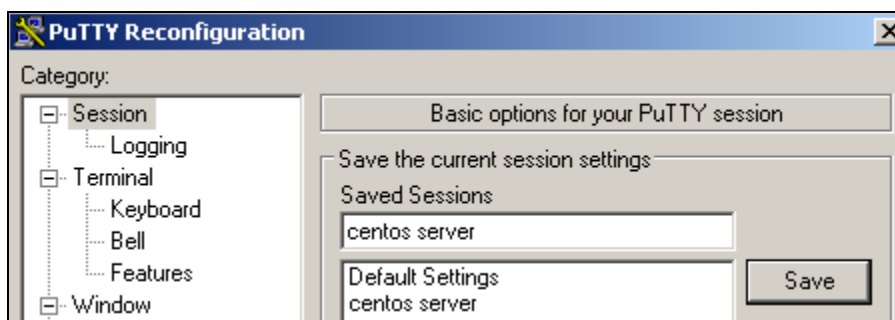


24. ábra



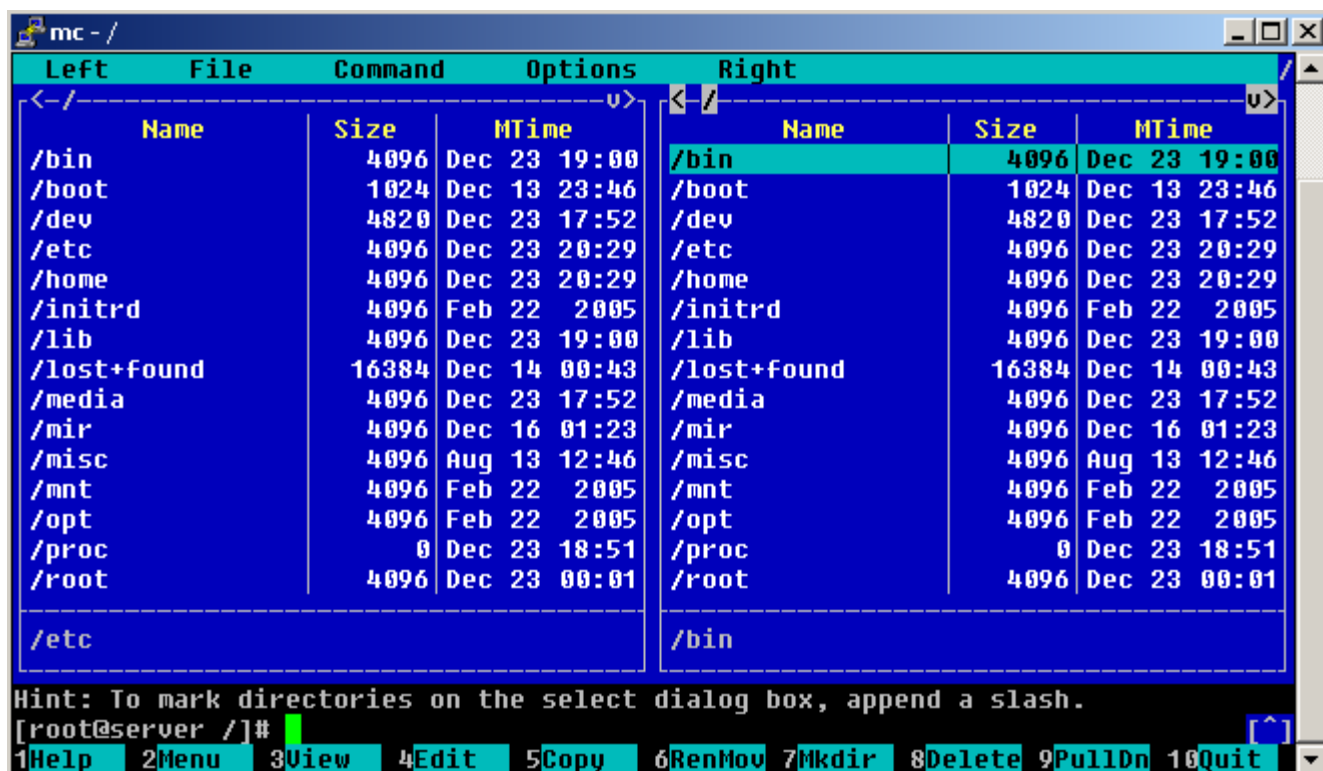
25. ábra

A „Session”-t választva elmenthetjük a kapcsolatot, így a következő kapcsolódáskor csak ki kell választani a kapcsolat nevét. Ehhez írunk be egy nevet a Saved Sessions mezőbe és kattintsunk a „Save” kapcsolóra (26. ábra). Az Apply kapcsolóval elmentjük a beállításokat. A PuTTY következő indításakor válasszuk a „centos server”-t.



26. ábra

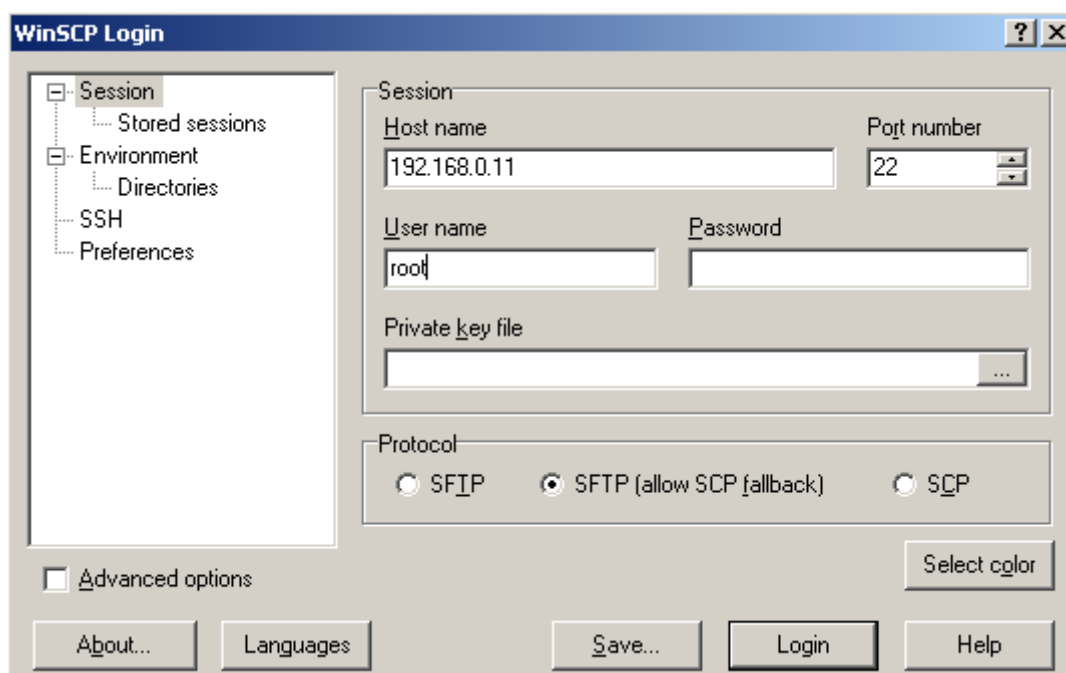
A Midnight Commander programot is használhatjuk a PUTTY ablakában (27. ábra), sőt a funkcióbillentyűk is működnek. Sajnos állományok szerkesztésénél a numerikus billentyűzeten a számok nem működnek, használjuk az alfanumerikus részt. A program használatához válasszuk angol billentyűzetkiosztást. Akár egérrel is használhatjuk, de én semmiképp sem javaslom. Ne feledjük, hogy rendszergazdaként vagyunk bejelentkezve, bármit megtehetünk. Egy hibás kattintás és tönkretelhetjük a működő szervert, vagy akár a felhasználók fontos adatait is letörölhetjük. Minden Enter leütése előtt gondoljunk erre is, és ha nem értjük a megjelenő üzenetet, üssünk inkább Esc-t.



27. ábra

A WinSCP

E program segítségével állományokat és könyvtárakat másolhatunk a Windows-os munkaállomás és Linux szerver között. Ez a program is titkosított protokollt használ, a neve WinSCP. A <http://winscp.net/eng/download.php> oldalról letölthető, a mérete kb. 1,7 Mb. A PuTTY-hoz hasonlóan szabad szoftver és igen népszerű, ami az oldalon olvasható 12 millió feletti letöltésszám is igazol. A 3.8.2 verzió megtalálható a <http://kmf.uz.ua/centos/serverhez1.zip> csomagban is.

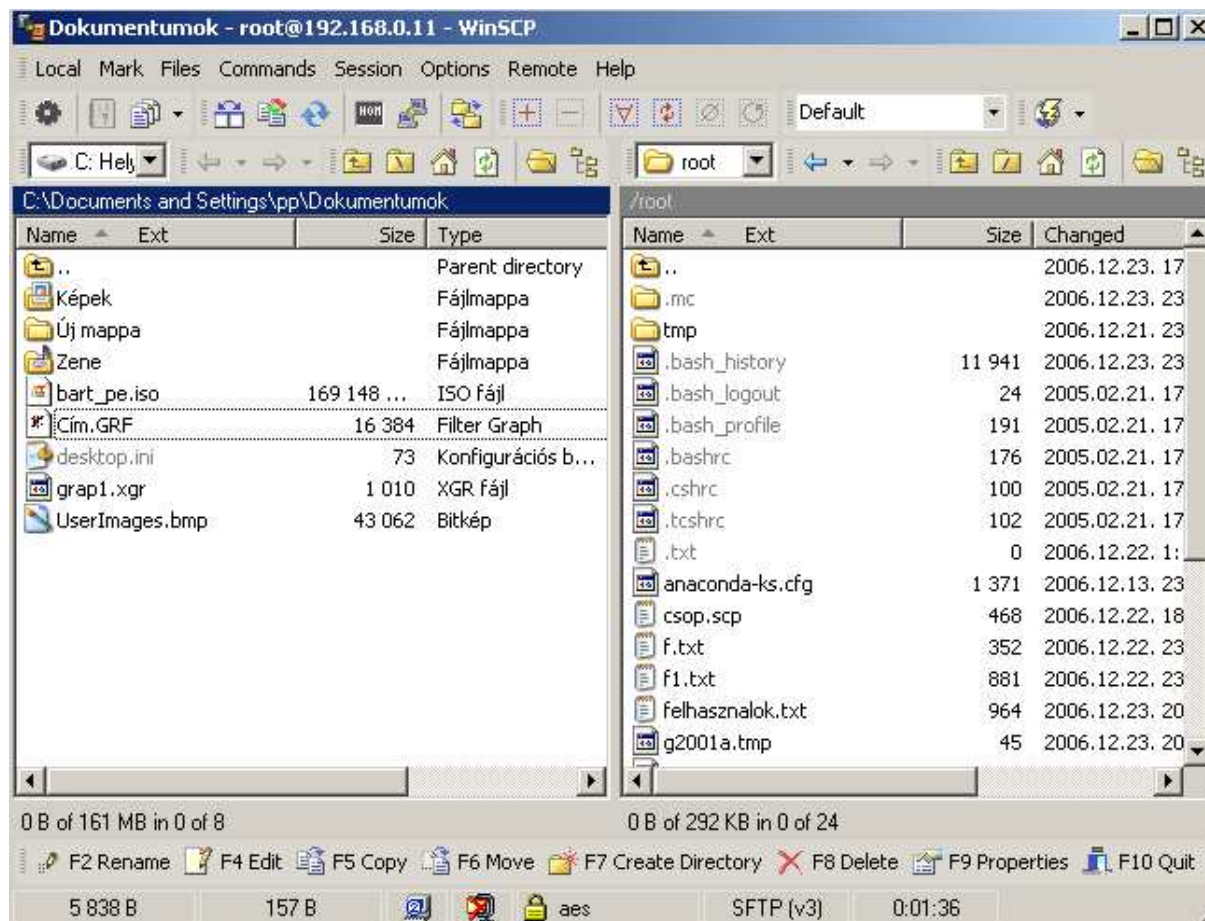


28. ábra

A telepítéshez a Windowson, rendszergazdaként el kell indítani a winscp382setup.exe állományt és a Next-re kattintani néhányszor. A program kétpaneles (Norton Commander-szerű), vagy Intéző-szerű felülettel is működhet, én az elsőt javaslom.

Elindítva a WinSCP-t írjuk be az IP címet és felhasználónak a root-ot. (28. ábra).

A Login kapcsolóra kattintva írjuk be a jelszót, és megjelenik a WinSCP ablaka. Valóban hasonlít egy kétpaneles fájlkezelő programra, csak itt a bal panelben választható a Windows XP bármelyik meghajtója és mappája, a jobban pedig a Linux szerver bármelyik könyvtára. Mivel root-ként csatlakoztunk itt a /root könyvtárat látjuk (29. ábra)



29. ábra

A kapcsolat beállításait itt is elmenthetjük,¹ de mivel a mindennapi rendszergazdai teendőkhöz ritkán van szükség a használatára, nem szükséges. A telepítendő programokat és konfigurációs beállításokat viszont ezzel könnyen átmásolhatjuk a kiszolgálóra.

Használjuk igen körültekintően, hiszen egy F8 vagy Delete billentyű leütése (+ Enter) végzetes lehet bármelyik operációs rendszerre nézve.

¹ Biztonsági szempontból nem ajánlott elmenteni. A szerver éles használata előtt olvassuk el a „Biztonsági beállítások” című fejezetet

V. A rendszer felhasználói

Felhasználók létrehozása előtt ejtsünk néhány szót a Linux operációs rendszer felhasználókezeléséről. A Linux a felhasználói azonosítókat az `/etc/passwd` állományban tárolja. Ez egy szöveges állomány, minden sora egy felhasználó adatait tartalmazza. A következő bekezdés a `passwd` állomány egy lehetséges sorát mutatja.

```
atti44:x:509:510:Kovacs Attila:/home/atti44:/bin/bash
```

A kettősponttal elválasztott mezők jelentése a következő:

1. Felhasználói név
2. Régebben a kódolt jelszót tárolta a rendszer ebben a mezőben. Shadow password használata esetén (napjainkban szinte minden Linux használja) itt egy `x` karaktert látunk.
3. Felhasználói azonosító (UID)
4. A felhasználó elsődleges csoportazonosítója (GID)
5. A felhasználó neve
6. A felhasználó saját könyvtára
7. A felhasználó által használt héjprogram

A **passwd** állomány első sorában a root felhasználó adatait tartalmazó sort találjuk, az 500-nál alacsonyabb felhasználói azonosítóval a rendszerfelhasználók rendelkeznek. Az első felhasználó, aki azonosítót kap a rendszerhez 500-as UID-et kapja, a második 501-et és így tovább.

A felhasználói csoportok nyilvántartására szolgáló **/etc/group** állomány is hasonló felépítésű: az első mezőben a csoport nevét látjuk, a negyedikben csoporthoz tartozó összes felhasználói nevet, vesszővel elválasztva. Mindkét állomány minden felhasználó számára olvasható, de módosítani csak a root tudja őket.

A jelszavakat a rendszer titkosítva tárolja az **/etc/shadow** állományban. Ez csak a root számára olvasható. A következő három parancs a három állomány tulajdonságait mutatja.

```
[root@server etc]# ls -l /etc/passwd
-rw-r--r-- 1 root root 1851 Dec  2 18:04 /etc/passwd

[root@server etc]# ls -l /etc/group
-rw-r--r-- 1 root root 706 Dec  2 18:04 /etc/group

[root@server etc]# ls -l /etc/shadow
-r----- 1 root root 1261 Dec  2 18:04 /etc/shadow
```

Felhasználók létrehozása

A felhasználók létrehozása előtt tervezzük meg, hogy milyen csoportokba rendezzük felhasználóinkat. A tanulókat érdemes osztályonként csoportokba foglalni. Csoportneveknek ne használjuk az osztályazonosítókat, hiszen akkor a 8b csoportot jövőre át kellene nevezni 9b-re. Szerencsésebb, ha olyan csoportazonosítókat használunk, ami egyértelműen azonosítja az osztályt tanulmányaik éve alatt. Például a **g1998b** csoport jelentheti azt az osztályt, amelyik 1998-ban kezdte meg tanulmányait. Hozzuk létre a tanár csoportot és az osztályok csoportjait a `groupadd` paranccsal.

```
[root@server etc]# groupadd tanar
[root@server etc]# groupadd g2002a
[root@server etc]# groupadd g2001b
...
```

Minden osztály és a tanárok csoportját létrehozva, hozzákezdhetünk a felhasználói azonosítók létrehozásához. Szerencsés, ha felhasználók egyedül választhatnak azonosítót, és nem mi határozzuk meg önkényesen mindenkinek. Az alapvető szabályokat elmagyarázva a felhasználóknak (max. 12 karakter, az angol ábécé kisbetűi és számok) kitöltik a jelentkezési ívet, beírva nevüket és az igényelt felhasználói nevet. Gyakran hasznos, ha tanárok és a tanulók azonosítói formailag is különböznek, például a tanulói azonosító utolsó karaktere lehet szám.

A szerver üzembe helyezésekor a csoportok és a felhasználók létrehozása nagy odafigyelést és sok munkát igényel a rendszergazdától, de a következő évben már csak az új csoportokat kell felvenni.

A jelentkezési ívek alapján létrehozuk a felhasználókat. A következő program segít létrehozni a felhasználókat a szerverünkön és a **samba**¹ jelszót is létrehozza, hogy a felhasználók a munkaállomásokról hozzáférjenek a **home** könyvtárukhoz. A program bekéri a felhasználó csoportját majd a teljes nevét és a felhasználói nevet. Létrehoz egy véletlen jelszót 6 karakterből, ami angol ábécé kis- és nagybetűiből, valamint néhány speciális karakterből állhat. A karakterek az **array1** tömbből választódnak. A tömbben nem szerepelnek a z és az y, valamint az O és a 0 karakterek, mert ezeket a felhasználók gyakran felcserélik a jelszó begépelésénél. A program megjeleníti a jelszót a képernyőn, ezt kikapcsolhatjuk, kitörölve az **echo \$PASS** sort. Természetesen a felhasználói névnek egyedinek kell lennie, ha már létezik a rendszeren a beírt felhasználó, figyelmeztet erre és kilép. A belépési jogot a szerverre csak az informatika tanároknak adjunk, egyszerű felhasználóknak nem!

A felhasználói adatokat a program beírja a `/root/felhasznalok.txt` állományba, minden felhasználót egy új sorba, a mezőket egymástól | jellel elválasztva. A következő bekezdés erre mutat egy példát:

```
[root@server ~]# cat felhasznalok.txt
tanar | Nagy Peter | nagypeti | 06 Dec 21 | /bin/false | xLDFgc | 503 |
503 | xLDFgBc
```

A mezők jelentése sorrendben a következő: csoport, név, felhasználói név, létrehozás dátuma, héjprogram, jelszó, azonosító, azonosító, jelszó. Ez a fájl megkönnyíti a jelszavak kiosztását, ezt a saját home könyvtárba, vagy SCP-vel a munkaállomásunkra másolva, formázhatjuk és kinyomtathatjuk a felhasználói jelszavak kiosztásához. Az azonosító és a jelszó azért van ismételt az utolsó két oszlopban, mert a felhasználók csak azt kapják meg. Természetesen minden felhasználó csak a sajátját. A jelszavak átadásánál hívjuk fel a felhasználók figyelmét arra, hogy azt tartsák titokban, soha senkinek ne mondják meg. A rendszergazda bárki jelszavát megváltoztathatja a **passwd** paranccsal, de ne feledjük, hogy ilyenkor a samba jelszót is módosítani kell. Pl.:

```
[root@centos ~]# passwd peti
Changing password for user peti.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

A **passwd** paranccsal megváltoztattuk peti felhasználó jelszavát. Az új jelszót kétszer be kell írni.

```
[root@centos ~]# smbpasswd -a peti
New SMB password:
Retype new SMB password:
[root@centos ~]#
```

Az **smbpasswd** paranccsal a samba jelszót is módosítottuk.

A program (valójában egy egyszerű bash script) könnyen megérthető és igény szerint módosítható. Letölthetjük a <http://kmf.uz.ua/centos/serverhez1.zip> címről. A kiszolgálón is letölthetjük az állományt a következő paranccsal:

¹ A SAMBA fájl- és nyomtató erőforrásokat tesz elérhetővé Windows operációs rendszert használó számítógépeknek. Később tárgyaljuk a beállítását.

```
[root@centos ~]# wget http://kmf.uz.ua/centos/serverhez1.zip
```

A Midnight Commander segítségével másoljuk a serverhez1.zip csomagból az uj_felhasznalo.scp állományt a /root könyvtárba (Enter-el beléphetünk a zip állományba, mint könyvtárba) majd adjuk ki a következő parancsokat:

```
[root@server ~]# mkdir /etc/skel/Dokumentumok
[root@server ~]# mkdir /etc/squid/csoportok
[root@server ~]# chmod u+x uj_felhasznalo.scp
```

Az első kettővel könyvtárakat hozunk létre, a harmadikkal futási jogot biztosítottunk magunknak, vagyis a program futtatható. Indítsuk el:¹

```
[root@server ~]# ./uj_felhasznalo.scp
Milyen csoportba fog tartozni a felhasználó?
(tanulo eseten: g2004a, pl.)
(tanaroknak: tanar)
tanar
A felhasználó teljes neve:
Pallay Feri
Felhasználó user neve:
pferi
Vs7wBk
Kap belepesi jogot Pallay Feri a serverre? (y/n)
y
Changing password for user pferi.
passwd: all authentication tokens updated successfully.
startsmfilepwent_internal: file /etc/samba/smbpasswd did not exist.
File successfully created.
Added user pferi.
```

A félkövérrel kiemelt sorokat be kell írni, értelemszerűen a saját nevünket és felhasználói nevünket írjuk. Ellenőrizzük a /root/felhasznlok.txt állomány tartalmát:

```
[root@server ~]# cat felhasznlok.txt
tanar | Pallay Feri | pferi | 06 Dec 21 | /bin/bash | Vs7wBk | 500 | 500
| Vs7wBk
```

Hozzuk létre a következő két felhasználót az **uj_felhasznalo.scp** program segítségével:

Csoport	Név	Felhasználói név	Belépési jog
tanar	Quota User1	proba90	N
tanar	Quota User2	proba300	N

Létrehoztuk az első felhasználókat a rendszeren. A további felhasználók létrehozása előtt állítsuk be tárkorlátot a /home könyvtárat tartalmazó lemezrészén.

Tárkorlátok beállítása: a quota

A felhasználók által felhasznált lemezterület célszerű korlátozni. Ha nem korlátoznánk a lemezterületet, egyes felhasználók elfoglalnák az egész lemezrészét, lehetetlenné téve a többi felhasználó munkáját. Mivel a felhasználók csak a saját könyvtárukba írhatnak adatokat, a /home könyvtárra fogunk tárkorlátot, kvótát (angolul quota) alkalmazni.

Indítsuk el a Midnight Commander-t és nyissuk meg szerkesztésre az /etc/fstab állományt. Keressük meg a /home lemezrészét meghatározó sort:

¹ A TAB billentyűvel kiegészíthetjük a fájlneveket és a parancsokat. Pl. ha a **./u** begépelése után leütjük a TAB billentyűt, akkor megjelenik teljes fájlnev, amennyiben nincs más u betűvel kezdődő állomány az aktuális könyvtárban.

LABEL=/home	/home	ext3	defaults	1	2
-------------	-------	------	----------	---	---

A defaults szó után írjuk a userquota,grpquota szavakat vesszővel elválasztva:

LABEL=/home	/home	ext3	defaults,usrquota,grpquota	1	2
-------------	-------	------	----------------------------	---	---

Mentsük az állományt, aztán adjuk ki a következő parancsokat:

```
[root@server etc]# touch /home/aquota.user /home/aquota.group
[root@server etc]# chmod 600 /home/aquota.*
[root@server etc]# mount -o remount /home
[root@server etc]# quotacheck -avugm
```

Az elsővel létrehozuk a quota adatokat tároló állományokat. A jogosultságok beállítása után újracsatoljuk a lemezrész. A negyedik parancs lemezkorlát-nyilvántartás ellenőrzését végzi. Ilyenkor a rendszer kigyűjti a felhasználók által használt területek nagyságát. A parancs kiadása után különböző figyelmeztetések jelennek meg a képernyőn, majd a következő szöveg:

```
quotacheck: Scanning /dev/hda7 [/home] done
quotacheck: Checked 10 directories and 31 files
```

(természetesen a számok különbözhetnek)

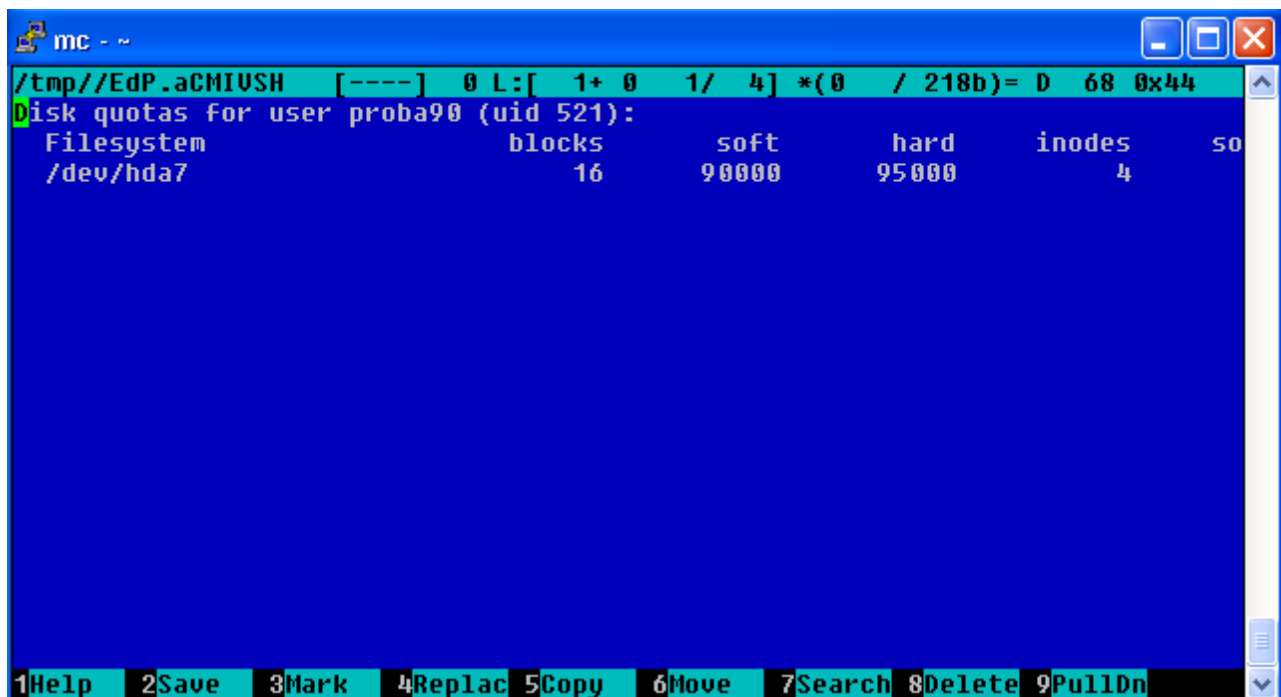
Kapcsoljuk be a kvótát:

```
[root@server etc]# quotaon -avug
/dev/hda7 [/home]: group quotas turned on
/dev/hda7 [/home]: user quotas turned on
```

A rendszer kész tárkorlátok kezelésére, minden felhasználóhoz lemezkorlátot rendelhetünk. A kiszolgálónkon tanároknak 300 Mb-ot, tanulóknak 90 Mb-ot fogunk biztosítani. Ezeket az értékeket is az **uj_felhasznalo.scp** program fogja beállítani, de ehhez először a proba90 és a proba300 felhasználóknhoz kell tárkorlátot rendelni. Adjuk ki a következő két parancsot:

```
[root@server ~]# export EDITOR=mcedit
[root@server ~]# edquota proba90
```

Az mc szerkesztőprogramjában megjelenő szöveges állományt módosítsuk: „soft” alatti 0-t módosítsuk 90000-re, a „hard” alattit pedig 95000-re. (30. ábra)



30. ábra

Mentsük az állományt és lépünk ki a szerkesztőprogramból. Ezzel beállítottuk proba90 nevű felhasználónak 90 Mb-os kvótát amit egy bizonyos ideig átléphet 95 Mb-ig. Ezt az időt türelmi vagy méltányossági időnek nevezhetjük (grace period), az alapértéke hét nap.

Állítsuk be proba300 felhasználó tárkorlátait hasonlóképpen a soft és a hard oszlopokba 300000-et és 330000-et írva. A repquota -a paranccsal lekérdezzük a beállított értékeket:

```
[root@server ~]# repquota -a
*** Report for user quotas on device /dev/hda7
Block grace time: 7days; Inode grace time: 7days
Block limits
User          used      soft    hard   grace
-----
root          --    77900         0         0
pferi         --    3928         0         0
proba90       --     16    90000    95000
proba300      --     16   300000   330000
File limits
User          used      soft    hard   grace
-----
root          --     6         0         0
pferi         --     8         0         0
proba90       --     4         0         0
proba300      --     4         0         0

[root@server ~]#
```

Látjuk, hogy a proba userek megkapták a korlátozott értékeket. A root és pferi sorokban a 0 azt jelenti, hogy rájuk semmilyen tárkorlátozás nem vonatkozik, ők a lemezterület tetszőleges részét elfoglalhatják. Természetesen a /home lemezrész méretétől és a felhasználók számától függően más kvótaértékeket is meghatározhatunk.

Az **uj_felhasznalo.scp** program utolsó néhány sora megállapítja, hogy a felhasznalok.txt állomány hány soros, és ha ez az érték több mint három, akkor a tanároknak olyan kvótát állít be, mint proba300 felhasználónak van. Mindenki másnak (tehát a tanulóknak), pedig olyat, mint proba90-nek. Ha valamelyik felhasználó nagyobb tárhelyet szeretne, akkor azt a proba90 felhasználóhoz hasonlóan módosíthatjuk, de általában a program által beállított lemezterületek elegendőek.

Az **uj_felhasznalo.scp** program:

```
#!/bin/bash
# Felhasznalo letrehozasa
clear;echo
echo "    Milyen csoportba fog tartozni a felhasznalo?"
echo "    (tanulo eseten: g2004a, pl.)"
echo "    (tanaroknak: tanar)"
read GP
# Ellenorzi, hogy a csoport letezik-e
GFOG=`grep -w $GP /etc/group | cut -d":" -f1 | wc -c`
if test $GFOG -le 1
then
    echo "A $GP csoport nem letezik !!!"
    exit 0
fi
#
echo "A felhasznalo teljes neve:"
read NEV
echo "Felhasznalo user neve:"
read UNEV
# Leellenorzi, hogy a felhasznaloi nev foglalt-e
FOG1=`grep -w $UNEV /etc/passwd | wc -c`
FOG2=`grep -w $UNEV /etc/group | wc -c`
FOG=`expr $FOG1 '+' $FOG2`
if test $FOG -ge 1
then
    echo "A $UNEV felhasznaloi nev mar foglalt!!!"
    exit 0
fi
```

```

PASS=""
PASSLEN=6
array1=( q w e r t u i o p a s d f g h j k l x c v b \
n m Q W E R T U I P A S D F G H J K L X C V B N M \
1 2 3 4 5 6 7 8 9 \, \. \? \! )
MODNUM=${#array1[*]}
count=0
while [ ${count:=0} -lt $PASSLEN ]
do
    number=$(( $RANDOM%$MODNUM ))
    PASS="$PASS"${array1[$number]}
    ((count++))
done
echo $PASS
#
echo "Kap belepesi jogot $NEV a serverre? (y/n)"
read SH1
    if test $SH1 = y
    then
        SH1=/bin/bash
    else
        SH1=/bin/false
    fi
# létrehozzuk a felhasználót
useradd -G $GP -c "$NEV" -s $SH1 $UNEV
# Letrehozzuk a /root/tmp könyvtarat ha nincs
if test ! -d /root/tmp
then
mkdir /root/tmp
fi
# A felhasználó azonosítószáma
IDS=`cat /etc/passwd | grep -w $UNEV | cut -d":" -f3`
# a felhasználói adatait beírjuk egy szöveges állományba:
DM=`date '+%y %b %d'`
echo "$GP | $NEV | $UNEV | $DM | $SH1 | $PASS | $IDS | $IDS | $PASS " >>
/root/felhasznalok.txt
#
# létrehozzuk a jelszót:
echo $PASS | passwd $UNEV --stdin
#
# SAMBA jelszo létrehozasa
(echo $PASS; echo $PASS) | smbpasswd -s -a $UNEV
#
# Tanároknak 700, mindenki masnak 755
if test $GP = "tanar"
then
chmod -R 700 /home/$UNEV
else
chmod -R 755 /home/$UNEV
fi
#
# Letrehozzuk a csoportlistákat
cat /etc/group | grep -w 'g[1-2][0-9][0-9][0-9][a-d]' >
/etc/squid/csoportok/csoportok.txt
cat /etc/group | grep -w 'tanar' >> /etc/squid/csoportok/csoportok.txt
CR='\012'
for i in `cat /etc/squid/csoportok/csoportok.txt`
do
f=`echo $i | cut -d":" -f1`;touch /etc/squid/csoportok/$f.txt
echo $i | tr [=,: ] $CR > /root/tmp/$f.tmp
cat /root/tmp/$f.tmp | sed '1,3 d' > /etc/squid/csoportok/$f.txt
done
#
# a tanulao.txt állományba minden tanulót

```

```

if test -f /etc/squid/csoportok/tanulok.txt
then
rm /etc/squid/csoportok/tanulok.txt
fi
for j in `ls /etc/squid/csoportok/g[1-2][0-9][0-9][0-9][a-d].txt`
do
cat $j >> /etc/squid/csoportok/tanulok.txt
done
# Ha több mint 3 sor van a felhasználok.txt állományban
# beállítja a quota-t
# a tanároknak 300 Mb, tanulókank 90 Mb
SOR=`wc -l /root/felhasznalok.txt | cut -d" " -f1`
if test $SOR -gt 3
then
if test $GP = "tanar"
then
edquota -p proba300 $UNEV
echo "quota 300 Mb"
else
edquota -p proba90 $UNEV
echo "quota 90 Mb"
fi
fi
# a proxy server újrakonfigurálása ha fut...
SR=`/sbin/service squid status | grep running | wc -c`
if test $SR -gt 0
then
/usr/sbin/squid -k reconfigure
fi

```

A figyelmes olvasó észrevehette, hogy a tárgyalatokon kívül a program létrehoz még szöveges állományokat az /etc/squid/csoportok könyvtárban. Ezeknek a később tárgyalat szolgáltatásoknál lesz szerepük. Ezen kívül a program utolsó sorai egy szolgáltatás működését vizsgálja és újrakonfigurálja azt.

Ha nem szeretnénk, hogy a beépített jelszógenerátor hozza létre a felhasználók jelszavát, töröljük ki a **PASS=""** és az **echo \$PASS** sorokat és a közöttük lévőket. Helyettük a következő néhány sort írjuk:

```

echo "Írja be $NEV jelszavát:"
echo
read PASS

```

A rendszer működésének ellenőrzéséhez a próbaszerveren létrehoztam három csoportot: tanar, g2002a, g2001a. Értelmszerűen a tanar csoportban tanárok vannak, a két g-vel kezdődő csoport két osztály tanulóit tartalmazza. A minden csoportba 4-4 felhasználót vettem fel. A szerver beállításakor, természetesen, nem szükséges ezt a mintát pontosan követni, létrehozhatunk valódi csoportokat és felhasználókat, de az éles üzemmód előtt mindenképp javaslok egy próbát.¹

tanar	
Kovacs Aladar	kali
Nagy Peter	nagypeti
Hideg Robert	hrobi
Birs Peter	birspeti

g2002a	
Szabo Hajnalka	hajni04
Szegedi Pál	szepi3
Ligeti Lajos	lajcsi5
Nagy Piroska	piri14

g2001b	
Sinko Lajos	sini55
Solymos Kata	lala4
Nagy Aladar	ala15
Molnar Istvan	isti8

A csoportokat létrehoztam a groupadd paranccsal. Az **uj_felhasznalo.scp** programmal felvettem a fenti 12 felhasználót. Nézzük meg hogy a quotabeállítások megfelelőek-e:

```

[root@server /]# repquota -a
*** Report for user quotas on device /dev/hda7

```

¹ A kiszolgáló üzembe helyezése előtt mindenképp olvassuk el a „Biztonsági beállítások” című fejezetet!

Block grace time: 7days; Inode grace time: 7days								
		Block limits			File limits			
User		used	soft	hard	grace	used	soft	hard

root	--	77904	0	0		7	0	0
pferi	--	3928	0	0		8	0	0
proba90	--	16	90000	95000		4	0	0
proba300	--	16	300000	330000		4	0	0
kali	--	16	300000	330000		4	0	0
nagypeti	--	16	300000	330000		4	0	0
hrobi	--	16	300000	330000		4	0	0
birspeti	--	16	300000	330000		4	0	0
hajni04	--	16	90000	95000		4	0	0
sini55	--	16	90000	95000		4	0	0
lala4	--	16	90000	95000		4	0	0
ala15	--	16	90000	95000		4	0	0
isti8	--	16	90000	95000		4	0	0
szepi3	--	16	90000	95000		4	0	0
lajcsi5	--	20	90000	95000		5	0	0
piri14	--	20	90000	95000		5	0	0

Látjuk, hogy a tanárok 300, a diákok 90 Mb-os tárkorlátot kaptak. A program elkészített néhány szöveges állományt az /etc/squid/csoportok könyvtárba:

```
[root@server /]# ls -l /etc/squid/csoportok/
total 20
-rw-r--r-- 1 root root 145 Dec 26 18:50 csoportok.txt
-rw-r--r-- 1 root root 25 Dec 26 18:50 g2001b.txt
-rw-r--r-- 1 root root 30 Dec 26 18:50 g2002a.txt
-rw-r--r-- 1 root root 52 Dec 26 18:50 tanar.txt
-rw-r--r-- 1 root root 55 Dec 26 18:50 tanulok.txt
```

Minden létrehozott csoport nevével létrejött egy txt állomány, amelyek a felhasználói neveket tartalmazzák. A tanulok.txt minden tanuló felhasználói nevét tartalmazza. Az mc nézőkéjével (F3), vagy belépve a csoportok könyvtárba a **cat** paranccsal ellenőrizzük ezt:

# cat g2001b.txt	# cat g2002a.txt	# cat tanulok.txt	# cat tanar.txt
sini55	hajni04	sini55	pferi
lala4	szepi3	lala4	proba90
ala15	lajcsi5	ala15	proba300
isti8	piri14	isti8	kali
		hajni04	nagypeti
		szepi3	hrobi
		lajcsi5	birspeti
		piri14	

Ezek a fájlok megkönnyítik a későbbi munkánkat a csoportokkal.

Felhasználók törlése

A felhasználók törlésére a **torol_felhasznalo.scp** programot használhatjuk.

FIGYELEM! A program nem csak az azonosítót, hanem a felhasználó home könyvtárát is törli! Csak akkor használjuk, ha a felhasználó már mentette adatait. Törli a felhasználó sorát a felhasználok.txt állományból és frissíti a fenti állományokat is. Tehát, ha ezt a két programot használjuk felhasználók létrehozására és törlésére, akkor az /etc/squid/csoportok könyvtár szöveges állományai és a felhasználok.txt mindig az aktuális állapotot fogják mutatni. A programot tartalmazza a <http://kmf.uz.ua/centos/serverhez1.zip> címről letölthető állomány.

A `torol_felhasznalo.scp` program :

```
#!/bin/bash
clear;echo
echo " F e l h a s z n a l o   t o r l e s e !"
echo
echo " Irja be a felhasznaloi nevet:"
read UNEV
# Leellenorzi, hogy a felhasznaloi letezik-e
FOG=`grep -w $UNEV /etc/passwd | cut -d":" -f1 | wc -c`
if test $FOG -lt 1
then
    echo "   Nincs ilyen felhasznalo: $UNEV   !!!"
    exit 0
fi
echo "Biztosan letorli a kovetkezo felhasznalot? (y/n)"
echo "A felhasznalo HOME könyvtara is torlodik"
echo
echo $UNEV ---- `grep -w $UNEV /etc/passwd | cut -d":" -f5`
echo
read Y1
if test $Y1 = y
then
    smbpasswd -x $UNEV
    userdel -r $UNEV
    sed -i '/' '$UNEV' /d' /root/felhasznalok.txt
fi
# Frissitjuk a csoportlistákat
cat /etc/group | grep -w 'g[1-2][0-9][0-9][0-9][a-d]' >
/etc/squid/csoportok/csoportok.txt
cat /etc/group | grep -w 'tanar' >> /etc/squid/csoportok/csoportok.txt
CR='\012'
for i in `cat /etc/squid/csoportok/csoportok.txt`
do
    f=`echo $i | cut -d":" -f1`;touch /etc/squid/csoportok/$f.txt
    echo $i | tr [=,: ] $CR > /root/tmp/$f.tmp
    cat /root/tmp/$f.tmp | sed '1,3 d' > /etc/squid/csoportok/$f.txt
done
# a tanulo.txt allomanyba minden tanulot
rm /etc/squid/csoportok/tanulok.txt
for j in `ls /etc/squid/csoportok/g[1-2][0-9][0-9][0-9][a-d].txt`
do
    cat $j >> /etc/squid/csoportok/tanulok.txt
done
# a proxy server ujrakonfiguralasa ha fut...
SR=`/sbin/service squid status | grep running | wc -c`
if test $SR -gt 0
then
    /usr/sbin/squid -k reconfigure
fi
```

Egy felhasználó hozzáférését a rendszerhez ideiglenesen kikapcsolhatjuk, ha megváltoztatjuk a jelszavát. A későbbiekben látni fogjuk, hogy a **passwd** paranccsal meghatározott jelszó az Internet hozzáférést biztosítja a felhasználóknak. Az **smbpasswd -a** paranccsal pedig azt a jelszót határozzuk meg, amivel a saját HOME könyvtárukhoz férhetnek hozzá. Alapértelmezés szerint ez a két jelszó megegyezik.

VI. Az Internet megosztása

Lehetőségek

Kiszolgálónk egyik legfontosabb feladata az Internet kapcsolat biztosítása a kliens számítógépeknek. Alapvetően két megoldás létezik erre a feladatra: hálózati címfordítás és proxy szerver alkalmazása.

Az első megoldásban a kliens számítógép adatcsomagjait fogadja a szerver és a kliens IP címét megváltoztatja a sajátjára és úgy továbbítja az Internet felé. Automatikusan oda-vissza fordítja a csomagokat, lehetővé téve, hogy kapcsolatot nyissunk a helyi hálózathoz a világhálóra. Ez a NAT (network address translation), hálózati címfordítás. A Linux kernel (rendszermag) valósítja meg a NAT-ot. Beállítani egyszerű, ezt alkalmazva a kliensek minden korlátozástól mentes Internetet kapnak.

A másik módszernél a proxy szerver (gyorsítótár, webcache) kliensek által lekért tartalmat (weblapot) letölti az Internetről, tárolja és a kliensnek átadja. Ha a felhasználóink, ugyanazt az oldalakat böngézik, a proxy szerver a második felhasználónak a tartalmat nem az Internetről, hanem a saját tárolójából adja vissza. Ezzel akár 20% is gyorsabbnak tűnhet a kapcsolat. Oktatási intézményben különösen fontos lehet a proxy-val megvalósítható funkciók:

- korlátozhatjuk vele a nem kívánt internetes címek látogatását
- korlátozhatjuk az Internet-hozzáférést felhasználói azonosítás vagy IP cím alapján
- szűrhetünk vele internetes tartalmat (speciális szűrők közbeiktatásával)
- felhasználhatjuk statisztika készítésre
- reklám-jellegű tartalmak kikapcsolásával sávszélességet takaríthatunk meg
- korlátozhatjuk a kliensek felé nyújtott sávszélességet

Sajnos a web proxy viszont csak http, https és ftp protokollokat támogat, például egy külső mail szerverhez a klienseknek nem biztosít hozzáférést.

Szerverünkön a Squid proxy szervert fogjuk beüzemelni, a tanterem minden gépének ez a szolgáltatás fogja biztosítani az Internetet. Ahol feltétlen szükséges, ott majd NAT-ot alkalmazunk.

Néhány port megnyitása a belső hálózat felé

A Squid beüzemelése előtt módosítsuk a telepítésnél beállított tűzfalszabályokat. Adjuk ki root-ként a következő parancsot:

```
[root@ server ~]# system-config-securitylevel
```

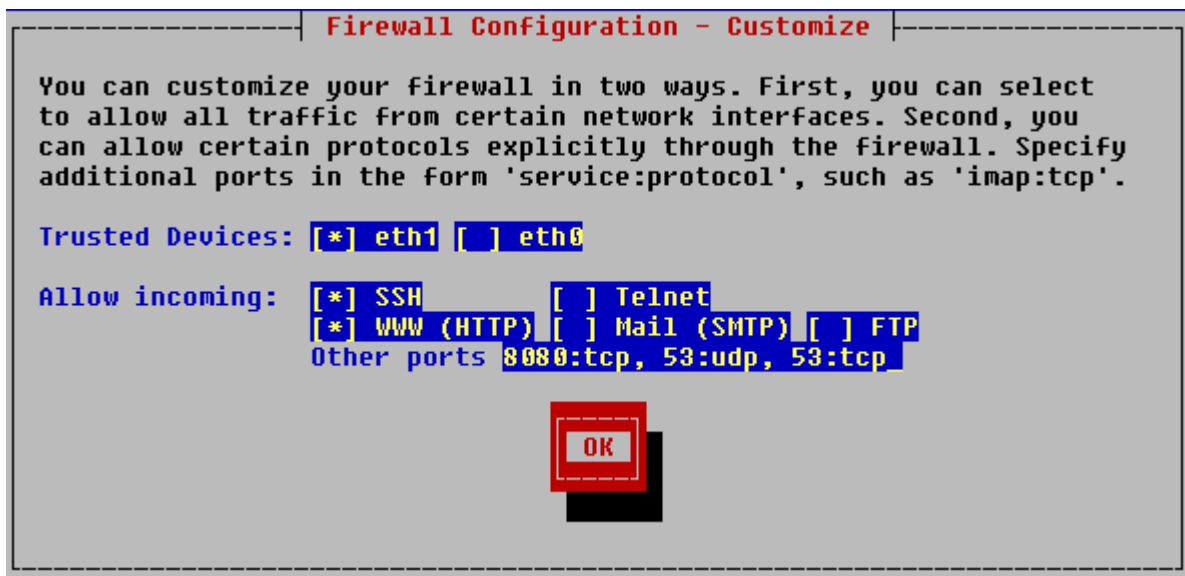
A programban a Tab billentyűvel válasszuk a Customize (Testreszabás) feliratot (31. ábra) és üssük le az Enter-t vagy a Szóközt.



31. ábra

A megjelenő ablakban a Tab és a Szóköz billentyűkkel válasszuk az **eth1** hálózati eszközt, az SSH és a WWW (http) szolgáltatást, valamint az Other ports (Egyéb portok) sorba írjuk be a következő szöveget:

8080:tcp, 53:udp, 53:tcp



32. ábra

Válasszuk a OK-t és üssük le az Enter-t. Ezzel engedélyeztük, hogy a belső hálózatunk gépei ezeken a portokon hozzáférjenek a kiszolgálóhoz.

A Squid

A Squid angol szó jelentése: tintahal. A világon a legnépszerűbb web-proxy program. A Squid szolgáltatás felkerült a kiszolgálónkra telepítéskor, de alapértelmezés szerint ki van kapcsolva. A program konfigurációs állománya az /etc/squid/squid.conf. Ez egy szöveges állomány, rengeteg angol nyelvű magyarázattal, több mint 3000 sor a terjedelme. Az /etc/squid könyvtárban a másolatát is megtaláljuk ez a squid.conf.default néven. Másoljuk a serverhez1.zip csomagban található squid.conf állományt az /etc/squid könyvtárba. Ezzel felülírjuk az ott lévő, de mivel van róla másolat, szükség esetén visszaállíthatjuk az eredetit.

Ez a konfigurációs állomány feltételezi, hogy belső hálózatunk címe 192.168.0.0/255.255.255.0
Más IP beállítás esetén módosítsuk a következő sort:

```
acl mynetwork src 192.168.0.0/255.255.255.0
```

Olyan beállításokat tartalmaz, hogy az Internet csak felhasználói név és jelszó megadásával fog működni.

A **squid.conf** állomány:

```
error_directory /etc/squid/errors
http_port 8080
icp_port 3130
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 8 MB
cache_dir diskd /var/spool/squid 1700 16 256
cache_store_log none
debug_options ALL,1
# redirect_program /usr/bin/squidguard -c /etc/squid/squidguard.conf

auth_param basic program /usr/lib/squid/pam_auth
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

authenticate_ip_ttl 60 seconds
half_closed_clients off
acl password proxy_auth REQUIRED
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl mynetwork src 192.168.0.0/255.255.255.0
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
#
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
### http_access allow mynetwork
http_access allow password
http_access deny all
#
icp_access allow all
miss_access allow all
visible_hostname server.suli.uz.ua
memory_pools off
```

A következő paranccsal indítsuk el a squid-et:

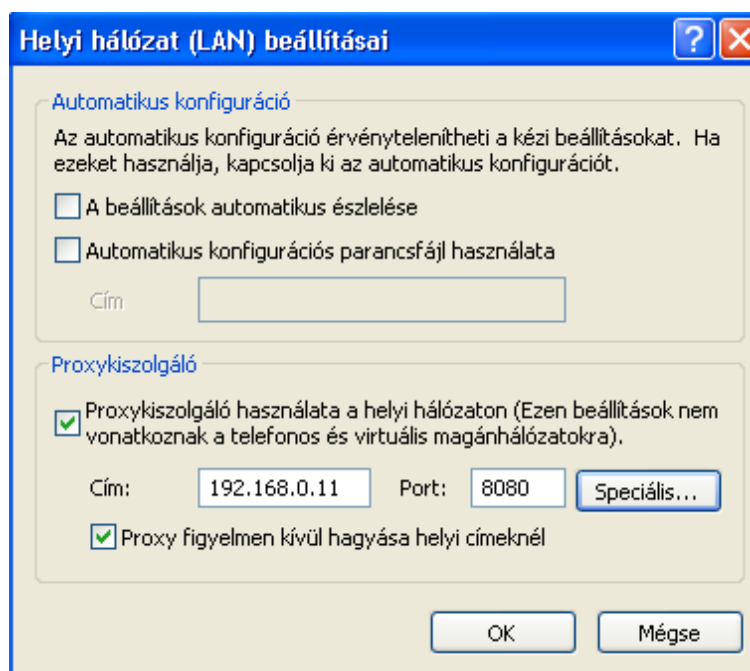
```
[root@server squid]# service squid start
```

Állítsuk be, hogy a squid automatikusan induljon.

```
[root@server squid]# chkconfig --levels 235 squid on
```

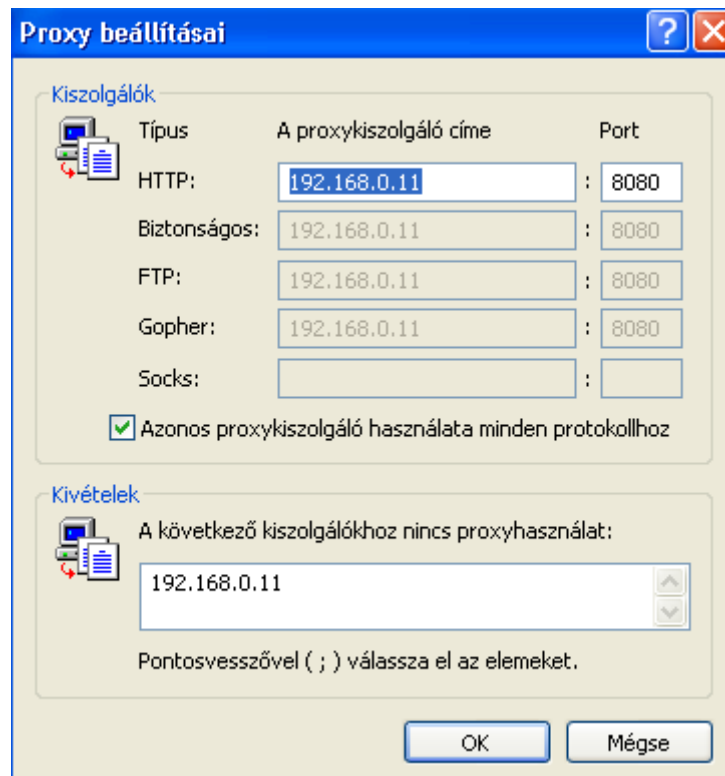
A kliensek beállítása

Az Internet Explorer használata esetén válasszuk az Eszközök / Internetbeállítások... / Kapcsolatok / LAN-beállítások ablakot. Itt állítsuk be azt az IP címet, amit a szervernek adtunk (pl.: 192.168.0.11) és a port mezőbe írjunk 8080-at. (33. ábra)



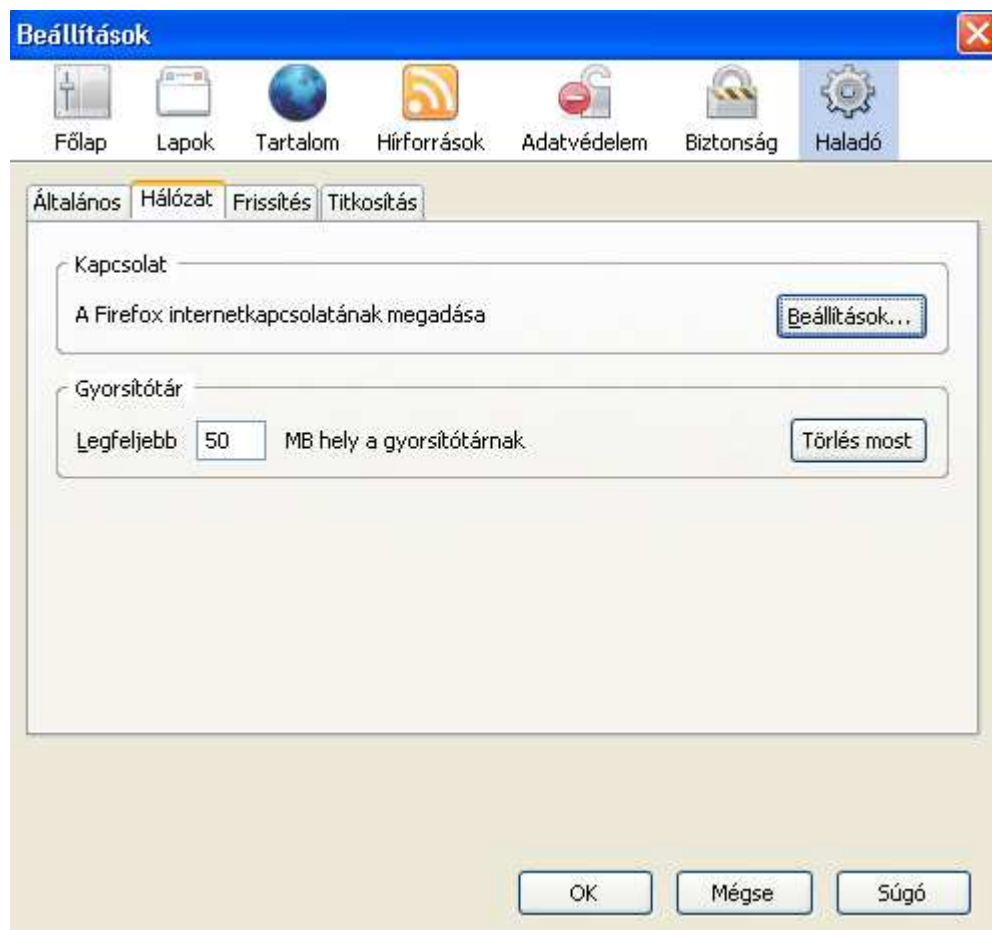
33. ábra

A Speciális... kapcsolóra kattintva állítsuk be, hogy minden protokollhoz ezt a kiszolgálót használja és magához a kiszolgálóhoz ne legyen proxyhasználat. (34. ábra)

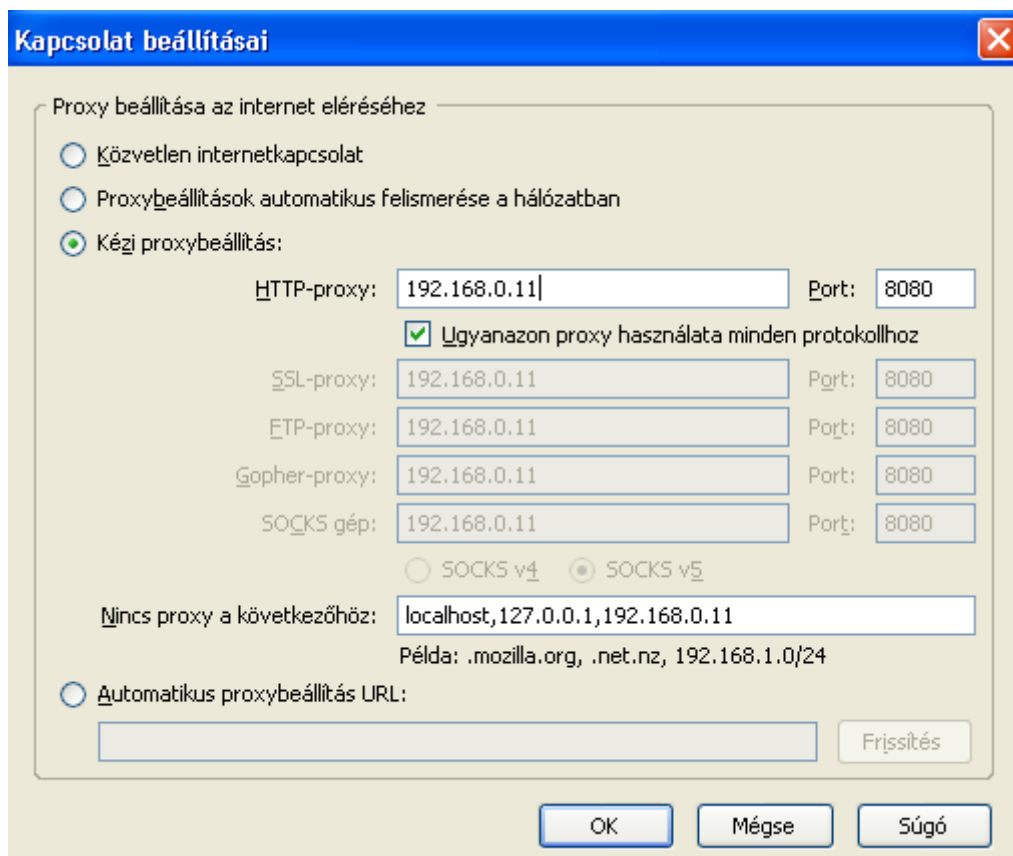


34. ábra

Mozilla Firefox böngésző használata esetén 35. és a 36. ábra mutatja a proxy server beállítását.

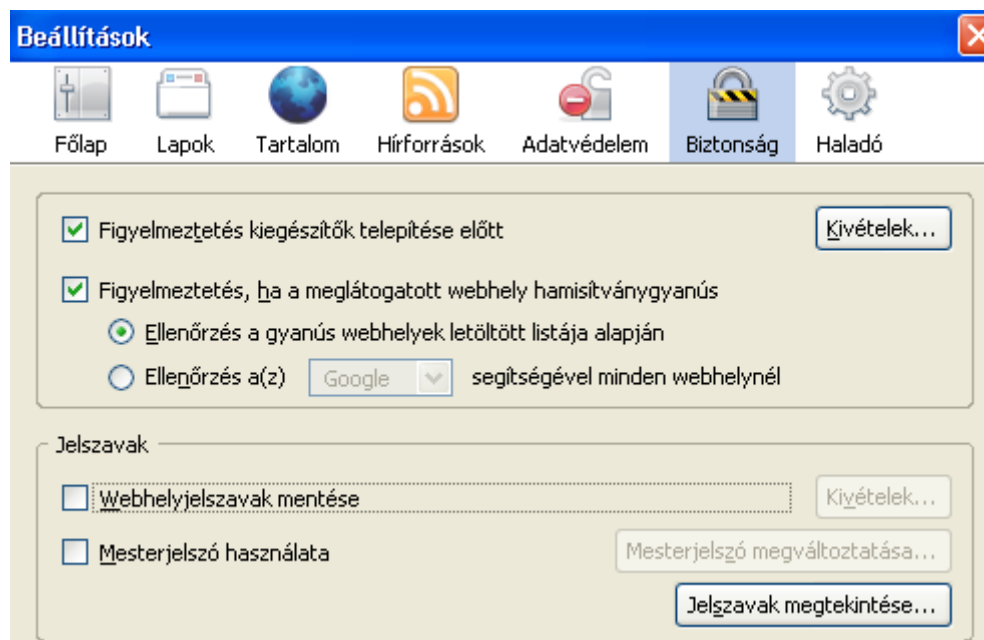


35. ábra



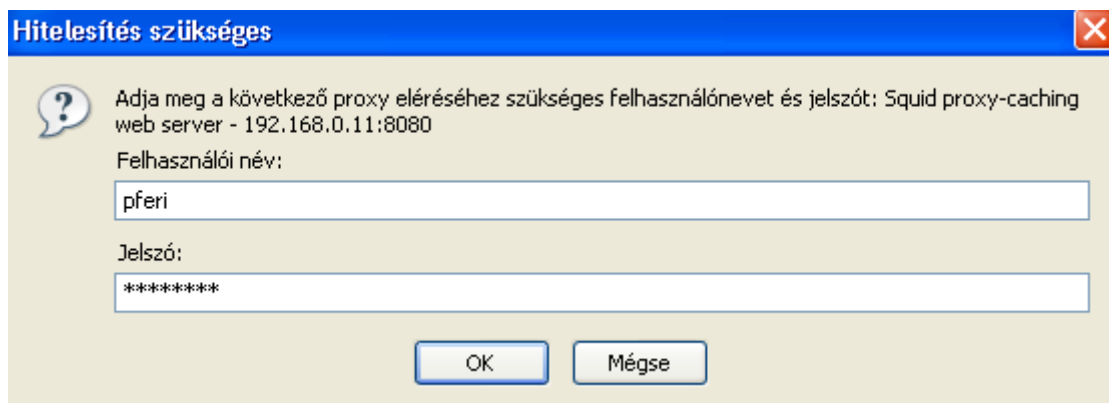
36. ábra

Sokak szerint a Firefox biztonságosabb mint az Internet Explorer, az viszont biztos, hogy a webhely jelszavak mentését egyszerűbben ki tudjuk kapcsolni. Tegyük is meg. (37. ábra)



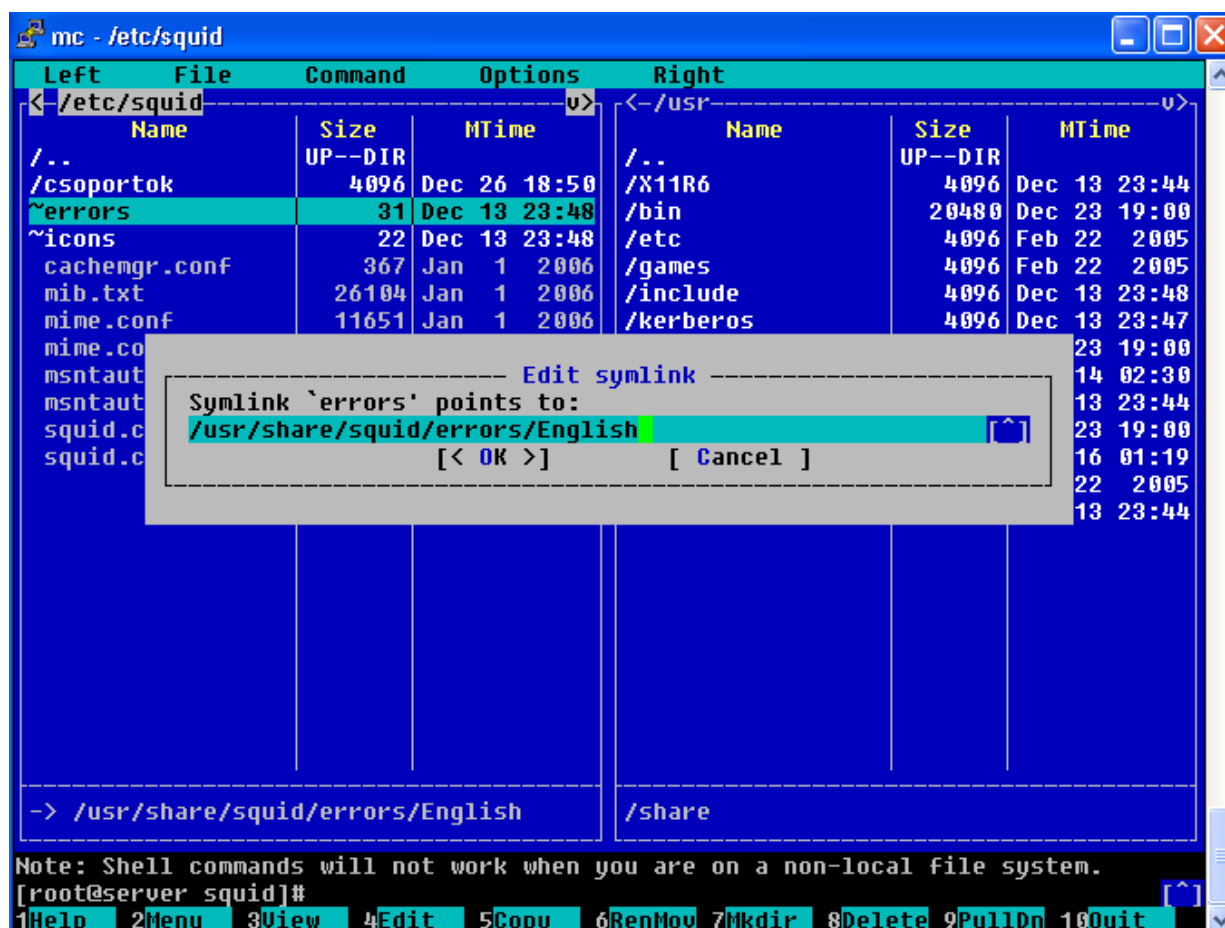
37. ábra

Ellenőrizzük az Internet hozzáférést a munkaállomáson. Azonosítás után (38. ábra) megjelenik a kért weboldal. A létrehozott felhasználók bármelyikével kell, hogy működjön az Internet.



38. ábra

Hibás bejelentkezés esetén a squid hibaüzenetei angol nyelven jelennek meg a képernyőn. Hogy magyarra váltsunk, az mc-ben válasszuk az /etc/squid könyvtárat és vezessük a kurzort **~errors** sorra. Válasszuk az F9 / File / edit symlink parancsot (39. ábra) és az English szót javítsuk ki Hungarian-ra.



39. ábra

A SquidGuard

A SquidGuard egy átirányító és elérést szabályozó kiegészítés a Squid számára. Szabad szoftver, rugalmas és gyors szűrést tesz lehetővé a Squid gyorsítáron. A Squid szabványos átirányítási felületét használja.

A SquidGuard program telepítéséhez hozzá kell adni az RPMforge tárolót (repository-t) az alapértelmezettekhez. Ehhez adjuk ki a következő parancsokat:

```
[root@server ~]# yum update
[root@server ~]# rpm -Uvh http://apt.sw.be/packages/rpmforge-release/rpmforge-release-0.3.6-1.el4.rf.i386.rpm
```

A rendszer frissítése és a tároló hozzáadása után már telepíthetjük a programot:

```
[root@server ~]# yum install squidguard*
```

A parancs két csomagot tölt le és telepít. Magát a squidguard-ot és egy adatbázist, ami kategóriákba rendezve több tízezer Internetes címet tartalmaz. E kategóriák felhasználásával szabályozhatjuk hozzáférést az Internethez felhasználók, felhasználói csoportok, IP címek és időintervallumok alapján. Azt viszont ne gondoljuk, hogy ezzel megoldottuk a tanulók számára nem ajánlott oldalak tiltását. Az Internet naponta változó világában ez nem lehetséges, és nem is lehet cél. Az iskola vezetésével egyeztetve ki kell dolgozni egy szabályzatot erre vonatkozólag, és azt ismertetni a felhasználókkal.

A telepítés után az /etc/squid könyvtárban találjuk a squidguard.conf állományt, ami egy minta a program beállításához. Készítsünk róla másolatot a /root/eredeti könyvtárba:

```
[root@server ~]# mkdir /root/eredeti
[root@server ~]# cp /etc/squid/squidguard.conf /root/eredeti
```

A következő parancsokkal hozzunk létre az **advertising** nevű könyvtárat, benne két állományt és ezeket adjuk a squid felhasználó tulajdonába.

```
[root@server ~]# mkdir /var/lib/squidguard/advertising
[root@server ~]# touch /var/lib/squidguard/advertising/domains
[root@server ~]# touch /var/lib/squidguard/advertising/urls
[root@server ~]# chown -R squid /var/lib/squidguard/advertising
[root@server ~]# chgrp -R squid /var/lib/squidguard/advertising
```

Másoljuk a serverhez1.zip csomagban található **squidguard.conf** állományt az /etc/squid, a **nulbanner.png** állományt a /var/www/html a **squidGuard.cgi** állományt pedig a /var/www/cgi-bin könyvtárba.

A squidGuard.cgi tulajdonságait módosítsuk:

```
[root@server ~]# chmod 755 /var/www/cgi-bin/squidGuard.cgi
```

A **squidGuard.conf** állomány:

```
#-----
#   SquidGuard CONFIGURATION FILE
#-----
# CONFIGURATION DIRECTORIES
dbhome /var/lib/squidguard
logdir /var/log/squidguard
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t = tue, w = wed, h = thu, f = fri, a = sat
# s = vasarnap, m = hetfo, t = kedd, w = szerda, h = csutortok, f =
pentek, a = szombat

time tanulo-k-time {
    weekly m 11:15-11:35 12:15-16:59
    weekly t 11:15-11:35 12:15-16:59
    weekly w 11:15-11:35 11:46-16:59
    weekly h 11:15-11:35 11:46-16:59
    weekly f 11:15-11:35 11:46-16:59
    weekly a 11:15-11:35 11:46-16:59
    weekly s 09:01-12:00
}
time tanar-time {
    weekly * 00:00-24:00    # tanaroknak mindig
```

```

}
#
# SOURCE ADDRESSES:
# Csoportokat hozunk létre felhasználói nevük szerint
#
src tanulok {
    userlist /etc/squid/csoportok/tanulok.txt    # a tanulok csoport
}
src tanar {
    userlist /etc/squid/csoportok/tanar.txt      # tanar csoport
}
# DESTINATION CLASSES:
dest adult {
    domainlist adult/domains
    urllist adult/urls
    expressionlist adult/expressions
}
dest aggressive {
    domainlist aggressive/domains
    urllist aggressive/urls
}
dest ads {
    domainlist ads/domains
    urllist ads/urls
}
dest gambling {
    domainlist gambling/domains
    urllist gambling/urls
}
dest violence {
    domainlist violence/domains
    urllist violence/urls
    expressionlist violence/expressions
}
dest advertising {
    domainlist      advertising/domains
    urllist         advertising/urls
    redirect http://192.168.0.11/nulbanner.png
    log             /var/log/squidguard/advertising.log
}
# ACLs
acl {
# A TANULOK szabályai
tanulok within tanulok-time {
    pass !adult !aggressive !ads !gambling !violence !advertising all
        redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&srcclass=%s&targetclass=%t&url=%u
    } else {
        pass none
        redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&srcclass=%s&targetclass=%t&url=%u
    }
}
#
# TANAROK szabályai
tanar within tanar-time {
    pass !adult !ads !advertising all
        redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&srcclass=%s&targetclass=%t&url=%u
    } else {
        pass none
        redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&srcclass=%s&targetclass=%t&url=%u
    }
}
default {

```

```
pass none
redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&srcclass=%s&targetclass=%t&url=%u
}
}
```

A „TIME RULES” részben meghatározunk időszakokat, amikor a tanulók használhatják az Internetet. Természetesen módosíthatjuk az intervallumokat, vagy újakat adhatunk hozzá. A tanároknak is beállíthatunk időkorlátot, de a fenti állomány korlátlan hozzáférést biztosít (* 00:00-24:00)

A „SOURCE ADDRESSES” részben a tanulók és a tanárok csoportját határozzuk meg a fentebb tárgyalt, az /etc/squid/csoportok könyvtárban lévő állományokkal.

A „DESTINATION CLASSES” részben meghatározzuk azokat az Internet-cím osztályokat, amelyek alapján a szűrést majd végezzük.

Az „ACLs” (*Access Control List*) részben maguk a korlátozó szabályok vannak. Vizsgáljuk meg a tanulók szabályait részletesebben:

1. # A TANULOK szabalyai
2. tanulok within tanulok-time {
3. pass !adult !aggressive !ads !gambling !violence !advertising all
4. redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&srcclass=%s&targetclass=%t&url=%u

Az első sor csak megjegyzés. A második sor meghatározza, hogy a **tanulok** csoportra a **tanulok-time** időszakokban a 3. sorban meghatározott szabály érvényes: engedélyez mindent kivéve adult, aggressive, stb. Tiltott oldal estén átirányít a squidGuard.cgi állományra (4. sor), olyan paraméterekkel, ami megjeleníti a kliens számítógép IP címét, csoportot, a tiltott oldal címét, a tiltás okát és a kiszolgáló lokális idejét. A **tanulok-time** időszakon kívül szintén átirányít a squidGuard.cgi állományra, de a tiltás osztálya sorba (Target class:) **none** jelenik meg.

Az advertising (hirdetés, reklám) nevű osztályt mi hoztuk létre, az állományok üresek. Ha a /var/lib/squidguard/advertising/domain állományba beírunk domain címeket, akkor az azokról érkező tartalmakat a böngészőprogram nem jeleníti meg, hanem a Squid az előbb felmásolt nulbanner.png képpel helyettesíti. Sok reklámképet és reklám-animációt tartalmazó portálok esetén, érdemes megvizsgálni, hogy ezeket a számunkra fölösleges tartalmakat melyik domain-ről, vagy url-ről szolgáltatják. Azt beírva az **advertising** könyvtár megfelelő állományba, ezek a fölösleges tartalmak nem töltődnek le, helyettük az előbb említett képet látjuk. Ezzel a módszerrel sokkal gyorsabban jelennek meg az ilyen portálok, hiszen előfordul, hogy a reklám tartalmak kilobájtban kifejezve nagyobbak mint a hasznos tartalom. A portál üzemeltető szemszögéből nézve ez aggályos megoldás, de kis sávszélesség esetén számunkra mindenképp hasznos.

Keressük meg az /etc/squid.conf állományban a következő sort és töröljük a sor eleji # karaktert:

```
redirect_program /usr/bin/squidguard -c /etc/squid/squidguard.conf
```

Módosítsuk az /etc/httpd/conf/httpd.conf állományt. Az "AddDefaultCharset UTF-8" sort módosítsuk a következőre:

```
AddDefaultCharset Off
```

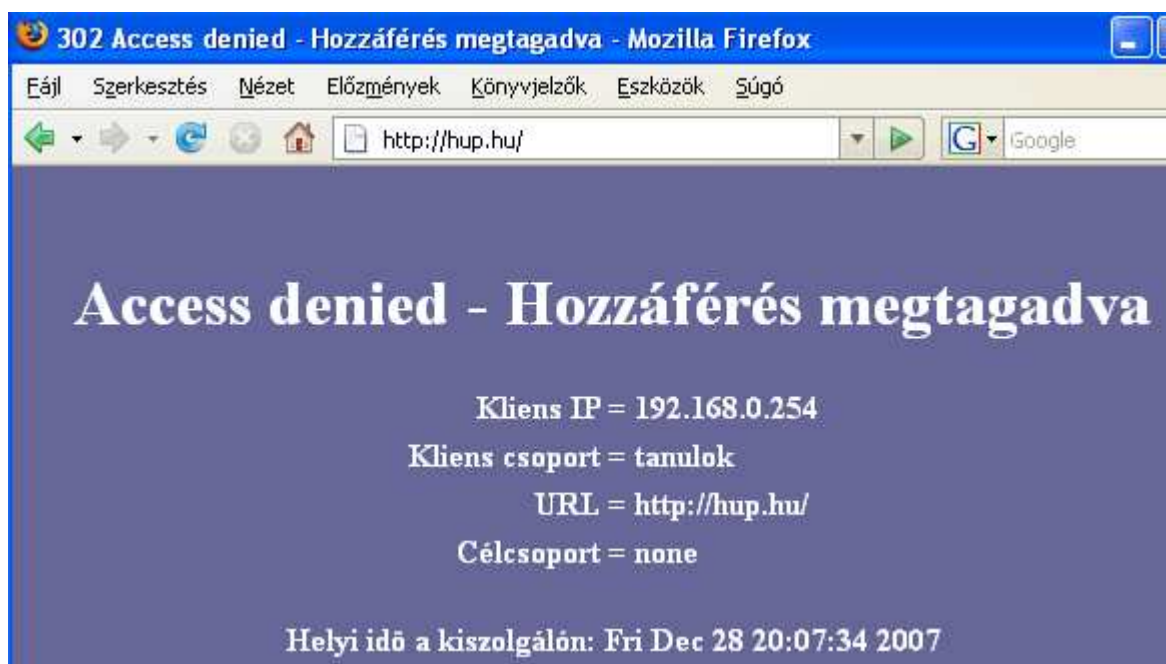
A squidGuard működésének ellenőrzéséhez indítsuk el a webszervert és állítsuk be, hogy automatikusan induljon:

```
[root@server /]# service httpd start
[root@server /]# chkconfig --levels 235 httpd on
```

Indítsuk újra a Squid-et:

```
[root@server /]# service squid restart
```

Ellenőrizzük le az Internet működését saját felhasználói nevünkkel. Mivel a tanár csoportnak vagyunk a tagja, a squidGuard engedélyezi a hozzáférést. Tanulói azonosítóval viszont a 40. ábrán látható oldal jelenik meg, amennyiben nem a tanulók számára meghatározott időben vagyunk.

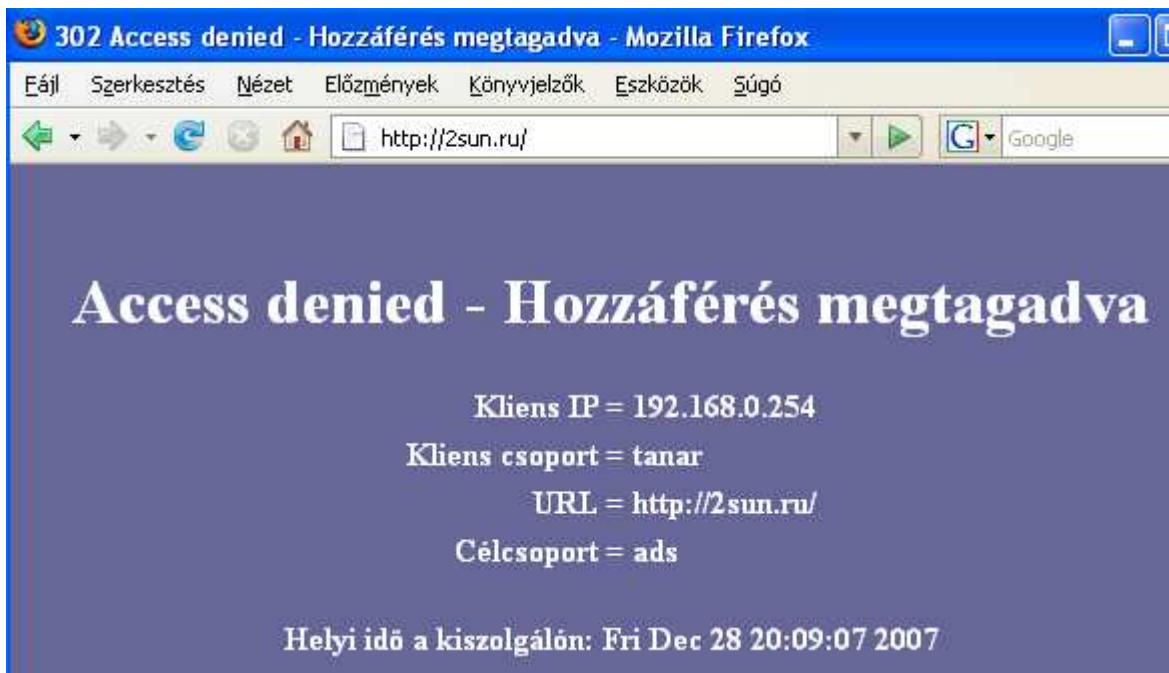


40. ábra

A tanár csoportnak tiltva vannak az ads (hirdetés) osztály címei, ellenőrizzük ezt begépelve a 2sun.ru címet. (Előzőleg megnéztem, hogy a `/var/lib/squidguard/ads/domains` állomány tartalmazza.) Látjuk, hogy a tiltás és az átirányítás működik. (41. ábra)

Az osztályok domain és urls állományai egyszerű szöveges állományok, tartalmukat mi magunk is módosíthatjuk. Módosításukkor viszont két dolgot is figyelembe kell venni. A SquidGuard a gyorsabb működés érdekében átalakítja Berkeley DB formátumba (erre szükség is van, az adult/domains állomány több mint 500 000 sort tartalmaz). Alapértelmezés szerint ha létezik domains.db akkor azt használja, ha nem akkor a domains szöveges állományt. Másod sorban a Squid indításakor olvassa be ezeket az állományokat, ahhoz, hogy a módosítást is figyelembe vegye, újra kell indítani.

Itt jegyzem meg, hogy a tanárok és tanulók listáját az `/etc/squid/csoportok` könyvtárból is induláskor olvassa. Ezért a felhasználók létrehozására és törlésére használt két szkript utolsó sorai megvizsgálják, hogy fut-e Squid, és működő szolgáltatás esetén újrakonfigurálják azt. Így a létrehozott felhasználói névvel és jelszóval azonnal működik az Internet.

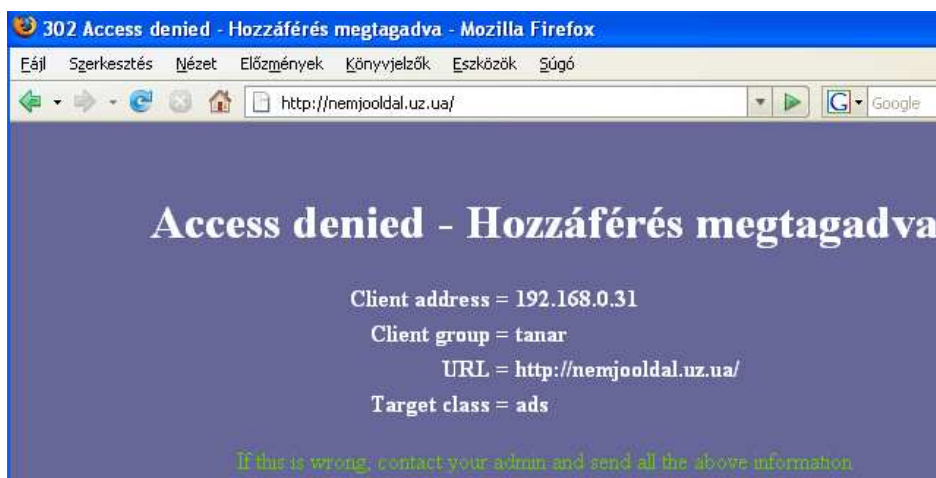


41. ábra

A serverhez1.zip csomagban találjuk a rebuild.scp állományt. Másoljuk a /root könyvtárba. Adjunk futási jogot neki és nézzük meg a tartalmát:

```
[root@server ~]# chmod u+x /root/rebuild.scp
[root@server ~]# cat /root/rebuild.scp
#!/bin/bash
/usr/bin/squidGuard -C all
chown -R squid /var/lib/squidguard
chgrp -R squid /var/lib/squidguard
squid -k reconfigure
```

A program újraépíti a db adatbázisokat a szöveges állományok alapján, azokat a squid felhasználó tulajdonába adja és újraindítja a Squid-et. Próbáljuk ki a gyakorlatban. Írjuk az /var/lib/squidguard/aggressive/domains állomány végére a nemjooldal.uz.ua címet. Mentsük az állományt és futtassuk a /root/rebuild.scp szkriptet. A 42. ábrán látjuk az eredményt: a SquidGuard megtagadta a hozzáférést az oldalhoz.



42. ábra

Azonosítás nélküli Internet-használat

A squid.conf, és a squidGuard.conf állományok módosításával megoldható, hogy bizonyos IP címmel rendelkező munkaállomásról felhasználói név és jelszó megadása nélkül is működjön az Internet.

Oldjuk meg, hogy a 192.168.0.31, 192.168.0.72 és a 192.168.0.82 IP címekről ne kérjen jelszót a proxy. A squid.conf állományba írjuk be a következő három sort a meglévő acl sorok elé:

```
# 31, 72 es 82 IP rol nem ker jelszot
acl nopass src 192.168.0.31 192.168.0.72 192.168.0.82
http_access allow nopass
```

A squidGuard.conf állományt két helyen is módosítani kell. Az src sorok elé írjuk a következő három sort, meghatározva ezzel a nojelszo forrást IP cím alapján:

```
src nojelszo {
    ip 192.168.0.31 192.168.0.72 192.168.0.82
}
```

A következő sorok pedig kerüljenek az acl sorok elé, amelyekkel engedélyezzük a hozzáférést:

```
acl {
# A nojelszo src-nek:
nojelszo {
pass !adult !aggressive !ads !gambling !violence !advertising all
    }
}
```

Utasítsuk a squid-et, hogy olvassa újra a konfigurációs állományokat:

```
[root@server ~]# squid -k reconfigure
```

Ezután a fenti IP címekről az Internet bármikor, felhasználói név és jelszó megadása nélkül is használható. A Squid nem ellenőrzi sem az időt, sem a felhasználói nevet ezekről az IP-kről érkező kérdéseknél. Az ads, adult, stb. osztályok szerinti tiltás viszont továbbra is fennáll. (43. ábra)



43. ábra

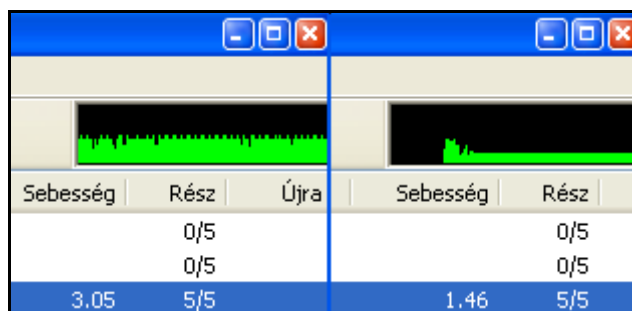
Sávszélesség-korlátozás

Gyakran felvetődik a kérdés, hogy hogyan lehetne leginkább igazságosan elosztani a meglévő sávszélességet. Különösen letöltésvezérlő programok használatakor egy munkaállomás elfoglalhatja szinte az egész sávot, a többi gépen pedig a böngészés is majd használhatatlanná lassul. Erre jelenthet megoldást, ha a Squid segítségével korlátozzuk az egy gépre jutó maximális sávszélességet. A következő néhány sort írjuk be a squid.conf állományba a http_access sorok után.

```
#
delay_pools 1
delay_class 1 2
delay_parameters 1 -1/-1 1500/25000
delay_access 1 allow mynetwork
delay_access 1 deny all
#
```

A konfigurációs állomány első részében meghatároztuk a mynetwork forráscímet, ami belső hálózatunk összes gépét jelenti: 192.168.0.0/255.255.255.0 Az egész hálózat megkapja a teljes sávszélességet (-1/-1 nincs korlát). Az 1500/25000 meghatározza, hogy egy gép 25 kilobájtól nagyobb állomány letöltésekor, az ezt meghaladó részt már csak 1500 bájt/másodperc sebességen kapja.

A szolgáltató által biztosított sávszélesség függvényében módosítsuk az értékeket. 128 kbit/sec (körülbelül 16 kilobájt/másodperc) sebességű kapcsolat esetén beállíthatunk kb. 5500/40000 értéket. Ez a böngészés sebességét nem csökkenti jelentősen, de a nagyobb állományok letöltésénél csak a sáv harmadát engedélyezi egy munkaállomásnak.



44. ábra

A 44. ábrán egy letöltésvezérlő program ablakának részleteit látjuk, ami a letöltési sebességeket mutatja. Az ábra bal oldala a squid.conf módosítás előtti állapotát tükrözi: a teljes 32 kilobit/sec „sebességet” használja a program. Az ábra jobb oldalán már a fenti sorokat is tartalmazza a squid.conf állomány, és a Squid is újraolvasta azt (**squid -k reconfigure**). Jól látszik, hogy a letöltés indításakor a teljes sávszélesség rendelkezésre áll, de egy idő után a 1500 bájt/másodpercre korlátozódik.

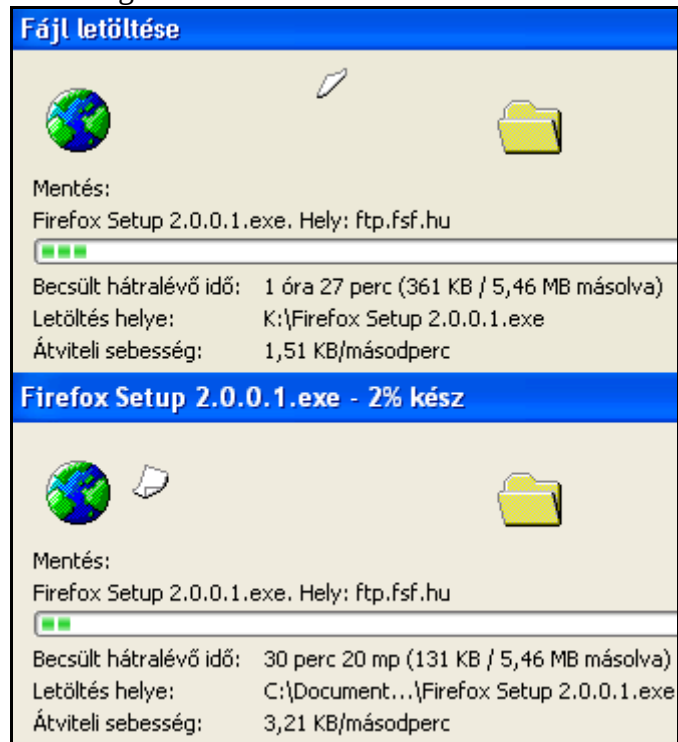
A következő példában két korlátozást használunk. Az első a nopass src-ben meghatározott IP címeknek nagyobb sávszélességet biztosít. A második pedig az előző példához hasonló korlátot állít be mindenki másnak.

```
#
# ----- A nopass IP-knek nagyobb sav
delay_pools 2
delay_class 1 2
delay_parameters 1 -1/-1 3500/25000
delay_access 1 allow nopass
delay_access 1 deny all
# ----- Mindenki masnak
delay_class 2 2
delay_parameters 2 -1/-1 1500/25000
delay_access 2 deny nopass
```

```
delay_access 2 allow mynetwork
delay_access 2 deny all
#
```

Ennek a beállításnak az eredményét látjuk a 45. ábrán. A kép alsó részén a 192.168.0.37 IP című, tehát a nopass src-hez tartozó gép, fölötte pedig egy másik munkaállomás letöltési folyamata látható. A két letöltés különböző időben történt. Az átviteli sebesség értékeiből jól látható, hogy a két korlátozás megfelelően működik.

Meg kell említeni, hogy ha a korlátozás érvénybe lép, akkor az nem csak az adott folyamatot, hanem a gép teljes forgalmát érinti. Tehát ha a felhasználó elindít még egy leöltést, a két folyamat osztozik a korlátozott sávszélességen.



45. ábra

VII. A hálózati forgalom ellenőrzése

A kiszolgáló `/var/log` könyvtárban találjuk a naplóállományokat. A legnagyobb forgalmú naplóállomány a `/var/log/messages`. Ebben látjuk a rendszer üzeneteit démonok indításáról, leállításáról, rendszermag-szintű hibákról és még sok egyéb üzenet. Az Internet használat naplóállománya a `/var/log/squid/access.log`.

A használatot ellenőrizhetjük a `tail -f` paranccsal:

```
[root@server ~]# tail -f /var/log/squid/access.log
1167583811.023 6800 192.168.0.31 TCP_MISS/200 3527 GET
http://www.google.hu/ pferi DIRECT/209.85.129.99 text/html
```

A fenti sorban láthatjuk hogy a 192.168.0.31 IP címről pferi felhasználó a `www.google.hu` oldalt látogatja. A mezők szóközzel vannak elválasztva, az első oszlop dátum és idő, csak szabvány UNIX formátumban, vagyis az 1970 óta eltelt másodpercek számát mutatja.

A `squidlog.scp` állományt a `serverhez1.zip` csomagban megtaláljuk. Másoljuk a `/root` könyvtárba és módosítsuk tulajdonságait és nézzük meg a tartalmát. Látjuk, hogy egy egyszerű perl szkript:

```
[root@server ~]# chmod 755 squidlog.scp
[root@server ~]# cat ./squidlog.scp
#!/usr/bin/perl -p
s/^\\d+\\.\\d+\\/localtime $&/e;
```

Figyeljük meg a működését:

```
[root@server ~]# tail -f /var/log/squid/access.log | /root/squidlog.scp
Sun Dec 31 19:28:59 2006 4803 192.168.0.31 TCP_MISS/200 3527 GET
http://www.google.hu/ pferi DIRECT/209.85.129.104 text/html
```

Sarg - Squid Analysis Report Generator

A Sarg nagy teljesítményű jelentéskészítő eszköz. A program a Squid log állományaiából naponta jelentést készít a webservert könyvtárába. A jelentések megjelenítéséhez webservert kell futtatni a kiszolgálón. Telepítéséhez adjuk ki a következő parancsot:

```
[root@server ~]# yum install sarg
```

Módosítsuk az `/etc/httpd/conf.d/sarg.conf` állományt. A 192.168.0.31 helyett a saját munkaállomásunk IP címét írjuk:

```
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
    DirectoryIndex index.html
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
    Allow from 192.168.0.31
    # Allow from ::1
    # Allow from your-workstation.com
</Directory>
```

Mivel a SARG által összeállított jelentés bizalmas információkat tartalmaz, semmiképp se engedélyezzük hozzáférést bármilyen IP-ről. Az oldal tartalmát mi magunk is kezeljük ennek megfelelően. A felhasználói jelszók kiosztásakor figyelmeztessük a felhasználókat, hogy az Internet használatát a rendszer naplózza.

Ahhoz, hogy a jelentés magyar nyelven készüljön, az `/etc/sarg/sarg.conf` állományban a

```
# language English
```

sort módosítsuk a következőre:

language Hungarian

A SARG minden éjjel 04:02 kor készíti el az előző napi jelentéseket. Mivel csak a 192.168.0.31 IP-című munkaállomásról engedélyeztük a hozzáférést, erről a gépről a <http://192.168.0.11/sarg/> címen tekinthetjük meg az Internet-használati statisztikákat. A napi statisztikákat a „daily” felírra kattintva tekinthetjük meg. A kiszolgálón a **sarg** parancsot kiadva a program elkészíti az aktuális statisztikát, ezt a „ONE-SHOT” link alatt láthatjuk. A program által készített sokféle statisztika közül a 46. ábrán pferi felhasználó december 31.-i Internet-használatát láthatjuk.



Squid Analysis Report Generator

Squid User Access Report

Periódus: 2006Dec31-2006Dec31

Felhasználó: pferi

Sorrend: BYTES, reverse

Felhasználó Kimutatás

	MEGLÁTOGATOTT HELY	KAPCSOLAT	BYTE-ok	%BYTE-ok	IN-CACHE-OUT		ELTÖLTÖTT IDŐ	MILISEC	%IDŐ
	inetobsd.wsak.hu	16	1.23M	31.81%	0.00%	100.00%	00:21:58	1.31M	24.59%
	hvg.hu	60	435.41K	11.19%	0.00%	100.00%	00:13:05	785.43K	14.65%
	www.google.hu	46	400.97K	10.30%	0.00%	100.00%	00:05:58	358.47K	6.68%
	forum.hwsz.hu	50	262.07K	6.73%	0.00%	100.00%	00:03:55	235.30K	4.39%
	vei.obuda.kando.hu	5	150.75K	3.87%	0.47%	99.53%	00:01:12	72.55K	1.35%
	hu.opensuse.org	19	148.72K	3.82%	0.00%	100.00%	00:03:36	216.56K	4.04%
	www.jaky.hu	16	143.36K	3.68%	0.00%	100.00%	00:03:26	206.39K	3.85%
	index.hu	29	142.96K	3.67%	11.26%	88.74%	00:02:57	177.19K	3.30%
	webisztan.blog.hu	24	136.68K	3.51%	10.04%	89.96%	00:00:58	58.66K	1.09%
	www.index.hu	12	113.63K	2.92%	5.82%	94.18%	00:03:21	201.36K	3.76%
	img.index.hu	11	69.99K	1.80%	0.59%	99.41%	00:01:52	112.10K	2.09%
	sial.org	6	67.73K	1.74%	0.00%	100.00%	00:00:56	56.34K	1.05%
	pcforum.hu	15	61.44K	1.58%	0.00%	100.00%	00:00:48	48.29K	0.90%
	www.prog.hu	15	58.61K	1.51%	2.31%	97.69%	00:01:01	61.47K	1.15%
	www.karpatinfo.net	10	52.40K	1.35%	1.18%	98.82%	00:00:37	37.00K	0.69%

46. ábra

MRTG - Multi Router Traffic Grapher

A Multi Router Traffic Grapher (MRTG) egy olyan program, amellyel ellenőrizni tudjuk a két hálózati eszközön átmenő forgalmat. Az MRTG a hálózati forgalomból különböző szempontok alapján HTML oldalakat készít, amelyekben png kiterjesztésű képekként láthatjuk a grafikonokat.

Az MRTG telepítéshez adjuk aki a következő két parancsot.

```
[root@cent44 snmp]# yum install mrtg
[root@cent44 snmp]# yum install net-snmp
```

Az első az **mrtg-2.10.15-2a.i386.rpm** csomagot telepíti, a csomag mérete kb. 900 kilobájt. A második a **net-snmp** csomagokat telepíti, a csomagok mérete 2,6 Mb.

Készítsünk másolatot az **/etc/snmp/snmpd.conf** állományról **snmpd.conf.ei** néven:

```
[root@server ~]# cp /etc/snmp/snmpd.conf /root/eredeti/snmpd.conf.ei
```

Másoljuk a **serverhez1.zip** csomagban lévő **snmpd.conf** állományt az **/etc/snmp** könyvtárba. A **syslocation** és a **syscontact** értékeket természetesen megváltoztathatjuk.

```
[root@server ~]# cat /etc/snmp/snmpd.conf
com2sec user1 default user1
group user1 v1 user1
group user1 v2c user1
group user1 usm user1
view all included .1 80
access user1 "" any noauth exact all none none
syslocation Valahol
syscontact admin@valami.hu
```

Indítsuk el az **snmpd** szolgáltatást és állítsuk be, hogy automatikusan induljon:

```
[root@server /]# service snmpd start
Starting snmpd: [ OK ]
[root@server /]# chkconfig --levels 235 snmpd on
```

Adjuk ki a következő parancsot:

```
[root@server /]# cfmaker user1@192.168.0.11 >> /etc/mrtg/mrtg.cfg
```

A kiszolgáló belsőhálózati IP címét írjuk a **192.168.0.11** helyett.

Az **/etc/mrtg/mrtg.cfg** fájlba írjuk be a következő sort: (amennyiben tartalmazza, töröljük a sor eleji **# -et**)

```
Options[_]: growright, bits
```

Mentsük az állományt és adjuk ki a következő parancsot (egy sor):

```
[root@server /]# indexmaker /etc/mrtg/mrtg.cfg >
/var/www/mrtg/index.html
```

Módosítsuk a **/etc/httpd/conf.d/mrtg.conf** állományt a következőre:

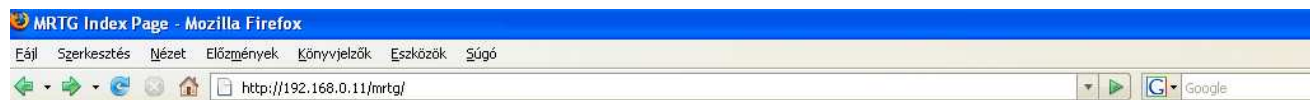
```
Alias /mrtg /var/www/mrtg
<Location /mrtg>
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
    Allow from ::1
    Allow from 192.168.0.0/24
</Location>
```

Indítsuk újra a webszerveret:

```
[root@server /]# service httpd restart
```

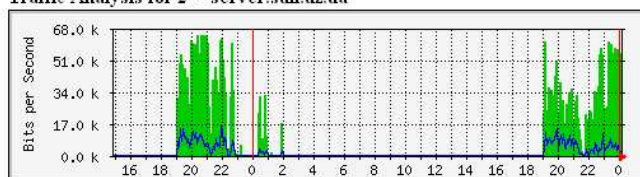
Az MRTG ötpercenként, a hálózati forgalom átlagából készít statisztikát. A <http://192.168.0.11/mrtg/> címen a 47. ábrához hasonló grafikonokat láthatunk. Kettőt, mivel két interfész van a kiszolgálóban.

A grafikonokra kattintva az elmúlt 30 perc átlagáról (heti nézet - weekly view), az elmúlt 2 óra átlagáról (havi nézet - monthly view), és az elmúlt 1 nap átlagáról (éves nézet - yearly view) látunk statisztikákat. A grafikonokon a zöld színnel a bejövő, kézzel a kimenő forgalmat látjuk.

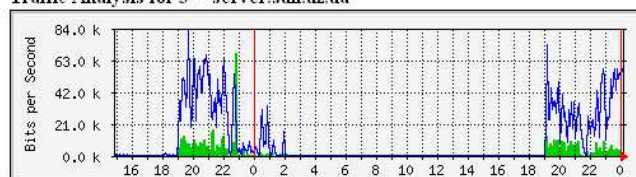


MRTG Index Page

Traffic Analysis for 2 -- server.suli.uz.ua



Traffic Analysis for 3 -- server.suli.uz.ua



MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.10.15
Tobias Oetiker <oetiker@ee.ethz.ch>
and Dave Rand <dln@bunqi.com>

47. ábra

VIII. Biztonsági beállítások

Az Internetre kapcsolt számítógépet a lehető legbiztonságosabbra kell beállítani. Alapvetően hibás az az elgondolás, hogy semmilyen titkos dolog nincs a kiszolgálón, ugyan ki akarná feltörni? A betörők igyekeznek védelem nélküli számítógépeket hídfőállásnak használni, és róluk indítani más gépek elleni támadásokat. Ha a betörő a naplóállományokat eltávolítja, lehet, hogy nekünk kell majd magyarázkodni a hatóságoknak...

Minden kiszolgálón a hálózati biztonság kiemelt fontosságú. Linux rendszereken a netfilter szolgáltatással a hálózati csomagok szűrését és átalakítását valósíthatjuk meg. Az ilyen csomagszűrésen alapuló védelmet tűzfalnak vagy angol szóval *firewall*-nak nevezzük.

A csomagszűrő beállítása előtt módosítsunk néhány hálózati beállítást a rendszeren.

Feloldó gyorsítótáras névkiszolgáló

Telepítésekor felkerült kiszolgálókra a BIND (*Berkeley Internet name daemon*, Berkeley internetes név-démon) programcsomag, ami DNS kiszolgálót valósít meg. Ezt a programot mint feloldó gyorsítótáras névkiszolgálót (*caching name server*) fogjuk használni. Minden kliens számítógépünknek a kiszolgálónk fog névszolgáltatást nyújtani, úgy, hogy ő lekéri a szolgáltatónk DNS szerveréről a kért információt. A lekért DNS információkat tárolja is, tehát a következő kérést ki tudja szolgálni a szolgáltató gépének felkeresése nélkül is. Ezzel a DNS kérések kiszolgálása gyorsabb lehet, és sávszélességet is megtakaríthatunk használatával.

Az `/etc/resolv.conf` állományt módosítsuk, második sornak írjuk be a következőt:

```
nameserver 127.0.0.1
```

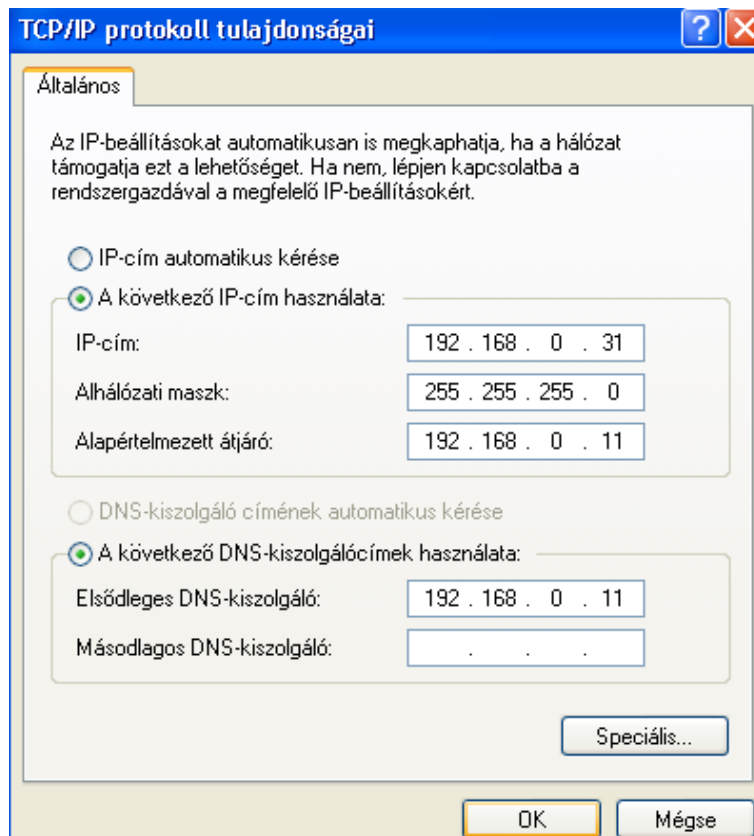
Tehát tartalma a következő lesz, természetesen a szolgáltatónk által megadott DNS kiszolgálók IP címei legyenek a harmadik és a negyedik (ha van másodlagos DNS) sorokban

```
search sul.uz.ua
nameserver 127.0.0.1
nameserver 194.88.152.1
nameserver 194.88.152.65
```

Indítsuk el a névkiszolgálót és állítsuk be, hogy automatikusan elinduljon a szerver indításakor:

```
[root@server /]# service named start
[root@server /]# chkconfig --levels 235 named on
```

A kliens számítógépeken állítsuk be alapértelmezett átjárónak és elsődleges DNS-kiszolgálónak a szerver belsőhálózati IP címét. (48. ábra)



48. ábra

A Windows XP vagy Windows 2000 esetén az nslookup paranccsal ellenőrizhetjük a beállított szolgáltatás működését. Pl.:

```
C:\> nslookup index.hu
Address:  192.168.0.11

Nem mérvadó válasz:
Név:      index.hu
Address:  217.20.131.2
```

Kiszolgálónk az index.hu domain címhez tartozó IP címmel válaszolt, a szolgáltatás működik.

Nem használt szolgáltatások kikapcsolása

A CentOS operációs rendszer több olyan szolgáltatást is tartalmaz és alapértelmezés szerint futtat, amelyek nem szükségesek egyszerű kiszolgálónkon. Főlegesen foglalják rendszerünk erőforrásait és biztonsági kockázatot is jelentenek. Az induló szolgáltatásokat a következő paranccsal kilistázzhatjuk nevük szerint rendezve, sorszámozva:

```
[root@server ~]# chkconfig --list | grep 3:on | sort | cat -n
```

A képernyőn olvasható, több mint harminc induló szolgáltatás közül kapcsoljuk ki a következőket:

```
[root@server ~]# chkconfig apmd off
[root@server ~]# chkconfig autofs off
[root@server ~]# chkconfig cpuspeed off
[root@server ~]# chkconfig cups off
[root@server ~]# chkconfig kudzu off
[root@server ~]# chkconfig mdmonitor off
[root@server ~]# chkconfig netfs off
[root@server ~]# chkconfig nfslock off
[root@server ~]# chkconfig portmap off
```

```
[root@server ~]# chkconfig rpcgssd off
[root@server ~]# chkconfig rpcidmapd off
[root@server ~]# chkconfig sendmail off
[root@server ~]# chkconfig xinetd off
```

A szolgáltatások a rendszer következő indításakor már nem fognak elindulni. A reboot paranccsal indítsuk újra a kiszolgálót.

A kikapcsolt szolgáltatások közül érdemes megemlíteni néhányat. A **kudzu** nevűre szükség lehet, ha valamit cserélünk vagy bővítünk a kiszolgálóban, hiszen feladata az új hardver detektálása és beállítása. Ilyen esetben kapcsoljuk újra be. A **sendmail** program továbbítja a leveleket, de kiszolgálónk nem fog mail szolgáltatást nyújtani a felhasználóknak. Szükség lehet viszont magáról a kiszolgálóról leveleket továbbítani szolgáltatónk valamelyik postafiókjába, például adminisztrációs célokból. Ebben az esetben inkább a postfix programot használjuk. A következő parancsokkal telepíthetjük a postfix-et, eltávolítjuk a sendmail-t és beállítjuk postfix automatikus indítását.

```
[root@server ~]# yum install postfix
[root@server ~]# yum remove sendmail*
[root@server ~]# chkconfig --levels 235 postfix on
```

A postfix működéséhez az /etc/postfix/main.cf állományba, az INTERNET HOST AND DOMAIN NAMES részbe írjuk be kiszolgálónk nevét (egyedi nevet írjunk!):

```
myhostname = server.suli.uz.ua
```

Elindítjuk a postfix-et:

```
[root@server ~]# service postfix start
```

A postfix segítségével leveleket küldhetünk azoknak a felhasználóknak, akik kaptak bejelentkezési jogot a kiszolgálóra. Példaként a rendszerbe bejelentkezettek listáját elmentjük a /root/bejelentkeztek.txt szöveges állományba:

```
[root@server mail]# last > /root/bejelentkeztek.txt
```

és tartalmát elküldjük e-mailben pferi felhasználónak:

```
[root@server mail]# mail -s Fontos pferi < /root/bejelentkeztek.txt
```

A levél tárgya a „Fontos” szó lesz. pferi-ként bejelentkezve a mail paranccsal elolvashatjuk a levelet. A félkövérral szedett részek a begépelte parancsokat mutatják:

```
[pferi@server ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/pferi": 1 message 1 new
>N  1 root@suli.uz.ua      Tue Jan  2 14:55  23/1050  "Fontos"
& 1
Message 1:
From root@suli.uz.ua  Tue Jan  2 14:55:07 2007
X-Original-To: pferi
Delivered-To: pferi@suli.uz.ua
To: pferi@suli.uz.ua
Subject: Fontos
Date: Tue,  2 Jan 2007 14:55:07 +0100 (CET)
From: root@suli.uz.ua (root)

root      pts/0          192.168.0.31    Tue Jan  2 12:51    still logged in
root      pts/0          192.168.0.31    Tue Jan  2 02:30 - 03:14  (00:44)
reboot    system boot    2.6.9-42.EL     Tue Jan  2 02:28             (12:09)
root      pts/0          192.168.0.31    Mon Jan  1 16:43 - down    (09:43)
reboot    system boot    2.6.9-42.EL     Mon Jan  1 16:39             (09:48)
root      tty1           192.168.0.31    Mon Jan  1 11:00 - down    (00:10)
reboot    system boot    2.6.9-42.EL     Mon Jan  1 10:55             (00:15)
root      tty1           192.168.0.31    Mon Jan  1 04:10 - down    (00:01)
```

```
wtmp begins Mon Jan  1 04:06:51 2007

& q
Saved 1 message in mbox
[pferi@server ~]$
```

Távolítsunk el néhány csomagot a rendszerből:

```
[root@server ~]# yum remove telnet
[root@server ~]# yum remove finger
[root@server ~]# yum remove ypbind
[root@server ~]# yum remove nfs-utils
[root@server ~]# yum remove unix2dos
[root@server ~]# yum remove pcmcia-cs
[root@server ~]# yum remove wireless-tools
[root@server ~]# yum remove webalizer
```

Ha a későbbiekben mégis szükség lesz valamelyikre a **yum install csomagnév** paranccsal feltelepíthetjük.

Az SSH belépés korlátozása

A fokozottabb biztonság érdekében a root felhasználónak általában megtiltják a közvetlen ssh kapcsolat kiépítését. Ebben az esetben felhasználói nevünkkel kell kiépíteni az ssh kapcsolatot, és root jogosultságot a **su** - paranccsal kérhetünk. Természetesen a root jelszó megadásával.

Nyissuk meg szerkesztésre az **/etc/ssh/sshd_config** állományt és keressük meg benne a következő sort:

```
#PermitRootLogin yes
```

Azt módosítsuk a következőre:

```
PermitRootLogin no
```

Indítsuk újra az ssh szerveret:

```
[root@centos44 ssh]# service sshd restart
```

Csatlakozzunk saját felhasználói nevünkkel a kiszolgálóhoz és kérjünk root jogosultságot:

```
[pferi@centos44 ~]$ su -
Password:
[root@centos44 ~]#
```

Ezután a WinSCP-vel is csak felhasználóként csatlakozhatunk, és csak saját HOME könyvtárunkba másolhatunk vele állományokat, könyvtárakat. Ezeket root-ként bejelentkezve áthelyezhetjük és módosíthatjuk a jogosultságait. Ennyi pluszmunkát érdemes elvégeznünk a kiszolgáló biztonsága érdekében.

Csomagszűrés

A Linux csomagszűrő szolgáltatása két feladatot is ellát majd a kiszolgálónkon: megvédi az Internet felőli támadásoktól, és a Squid által nem támogatott szolgáltatások használatát is lehetővé teszi a kliens gépeknek.

A csomagszűrő beállítása előtt módosítsuk az **/etc/sysconfig/syslog** állományt, hogy a rendszerüzenetek ne jelenjenek meg a kiszolgálónk képernyőjén. A **KLOGD_OPTIONS** sort írjuk át a következőképpen:

```
KLOGD_OPTIONS="-2 -c 1"
```

Indítsuk újra a rendszernaplózó szolgáltatást:

```
[root@server ~]# service syslog restart
```

A következő parancs az /etc/sysctl.conf állomány első hét sorát mutatja:

```
[root@server ~]# head -7 /etc/sysctl.conf
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled. See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 0
```

Módosítsuk a net.ipv4.ip_forward értékét **0**-ról **1**-re és mentjük az állományt.

Indítsuk újra a hálózatot:

```
[root@server ~]# service network restart
```

Magát a csomagszűrést a Linux kernelében egy programrész végzi, és a rendszergazda az **iptables** programmal konfigurálhatja működését. A programrész képes a beérkező (INPUT), a kimenő (OUTPUT) és az áthaladó (FORWARD) csomagok vizsgálatára és szűrésére. Ezzel a három szabálylistával indul rendszer, amiket láncoknak nevezünk. Egy bejövő csomag, ha célja maga szerver az INPUT láncba kerül, ha nem, akkor a FORWARD láncba. Ha a kiszolgáló maga akar csomagokat küldeni, azok az OUTPUT láncba kerülnek.

A csomagokon többféle műveletet tudunk végezni: elfogadjuk (ACCEPT), eldobjuk (DROP), visszautasítjuk (REJECT), naplózzuk (LOG). Ezeknek a műveleteknek a végrehajtását különböző szempontok szerint szabályozhatjuk: célcím, forráscím, protokoll, portszám stb.

A csomagszűrő szabályok meghatározásánál érdemes Rusty Russell útmutatásait figyelembe venni:

„Általános bölcsesség a számítógépes biztonságban, hogy mindent le kell zárni, és ezután egyesével megnyitni azokat a lyukakat, melyeket szükségesnek tartunk. Ezt általában úgy jellemzik, hogy "minden, amit nem engedek meg kifejezetten, az tiltva van". Ajánlom ezt a megközelítést, ha a biztonság az alapvető célod. Ne futtass olyan szolgáltatást, amit nem szükséges futtatnod, vagy ha úgy gondolsz, akadályozd meg hogy hozzáférjenek.

Ha tűzfalat építesz, úgy kezd, hogy ne fusson rajta semmi, és minden forgalmat tiltson ki. Ezután egyesével add hozzá a szolgáltatásokat és engedélyezd azokat a csomagokat, amelyek ezt igénybe veszik. ”

Itt terjedelmi okok miatt nincs lehetőség részletesen bemutatni az iptables használatát. Mindenképp olvassunk el az Interneten az iptables-t részletesen tárgyaló cikket, mielőtt módosítanánk az általam javasolt szabályrendszert. Nyomtatásban kiváló leírást olvashatunk Pere László: „GNU/Linux rendszerek üzemeltetése II. Hálózatok” című könyvében.

Másoljuk át a serverhez1.zip csomagban lévő tuzfal.scp állományt a /root könyvtárba. Állítsuk be a jogosultságokat:

```
[root@server ~]# chown root /root/tuzfal.scp
[root@server ~]# chgrp root /root/tuzfal.scp
[root@server ~]# chmod 755 /root/tuzfal.scp
```

Vizsgáljuk meg vázlatosan a script működését. Az első sorokban változóknak adunk értékeket. A többségük már ismerős. Módosítsuk a beírt IP címeken, az IP_EXT értékét biztosan módosítani kell, szerverünk külső hálózati kártyájának IP címét írva oda. A 192.168.0.0/24 belső hálózatunk címe és az alhálózati maszk rövidített beírása (24 = 255.255.255.0, tehát a 32 bites számban az 1-ek száma). Az SMTPIP és a POP3IP a szolgáltatónk által megadott SMTP és POP3 szerverek IP címei. A szolgáltatótól biztosan kaptunk e-mail címeket és ezekhez tartozó SMTP és POP3 kiszolgálói adatokat. Határozzuk meg a host paranccsal ezekhez tartozó IP címeket:

```
[root@server ~]# host smtp.bereg.net.ua
smtp.bereg.net.ua has address 194.88.152.1
```

```
[root@server ~]# host pop3.bereg.net.ua
pop3.bereg.net.ua has address 194.88.152.2
```

Természetesen a saját szolgáltatónk által megadott kiszolgálóneveket írjuk be. Az IP címeket írjuk be a szkript megfelelő soraiba. Ez sajnos azt is jelenti, hogy ha a szolgáltatónk megváltoztatja mail szervereinek IP címait, akkor itt ismét módosítani kell, és addig nem fog működni a levelezés a kliensgépe(ke)n.

A „start” és a „;;” sorok közötti rész tartalmazza azokat a szabályokat és parancsokat, melyek a **/root/tuzfal.scp start** parancs kiadásakor végrehajtódnak. (Ezt a parancsot először lehetőleg magán a szerveren adjuk és ne a PuTTY ablakában. Az ssh kapcsolat megszakadhat a kliens és szerver közt, és újra be kell jelentkeznünk) A script kiírja a hálózat alapbeállításait is:

```
[root@server ~]# /root/tuzfal.scp start
indul....
-----
A belso halo: 192.168.0.0/24
-----
      A tuzfal BELSO halokartyaja: eth1
      inet addr:192.168.0.11 Bcast:192.168.0.255 Mask:255.255.255.0
-----
      A tuzfal KULSO halokartyaja: eth0
      inet addr:10.0.0.189 Bcast:10.0.0.191 Mask:255.255.255.248
-----
A tuzfal csomagszuroinek betoltese
```

Ebben a részben néhány kernel paraméter beállítása után az alapértelmezett tiltás beállítása következik, aztán a beérkező szabályok sorai következnek.¹ A szabályok előtt magyarázatokat olvashatunk. Így egyszerűen módosíthatóak. A beérkező (INPUT) szabályokat nem feltételen kell módosítani: engedélyezett **csak** a belső hálóról a http (webszerver), SSH (PuTTY-val, WinSCP-vel csatlakozhatunk bármelyik belső IP-ről), DNS kérés, SAMBA (fájlszerver), proxy-szerver és az icmp protokoll (ping parancs). Az INTERNET felől csak az icmp engedélyezett. A szolgáltató tehát a ping parancssal le tudja ellenőrizni a kapcsolatot a kiszolgálónkkal, de semmilyen szolgáltatását nem tud igénybe venni.

A kimenő szabályok (OUTPUT) engedélyezik, hogy a kiszolgáló DNS szerverekhez csatlakozzon, http, https és ftp protokollon csatlakozzon külső kiszolgálókhoz (a Squid-nek kell és a rendszer frissítéséhez is), leveleket küldjön (ezt a sort akár ki is kapcsolhatjuk a sor elején # jellel) és engedélyezve van a belső háló felé a SAMBA által használt portok.

A továbbítási (FORWARD) szabályok rész különösen fontos, hiszen azt a részt biztosan módosítani kell². Tulajdonképpen a belső gépeink e nélkül is tudják használni az Internetet a Squid-en keresztül: a kiszolgálónknak engedélyeztük, hogy csatlakozzon webszerverekhez, a klienseknek pedig azt, hogy használják a 8080-as portot és ott a proxy szerver figyel.

Ez a rész valójában csak egy privilegizált gép (pl. a saját gépünk: 192.168.0.31) szabályait tartalmazza. Mint már említettem, vannak az Interneten olyan szolgáltatások, amelyek nem használhatóak proxy kiszolgálóval. Ezek közül először a mail szerverhez történő csatlakozást nézzük át.

A következő három sor engedélyezi 192.168.0.31-es gép által küldött tcp, udp és icmp csomagok továbbítását:

```
$IPTABLES -A FORWARD -p tcp -s 192.168.0.31 -j ACCEPT
$IPTABLES -A FORWARD -p icmp -s 192.168.0.31 -j ACCEPT
```

¹ Vegyük figyelembe, hogy több „\$IPTABLES”-el kezdődő sor nem fér el egy sorban, és nyomtatásban két sornak tűnik.

² PPPoE protokollt használó ADSL kapcsolat esetén általában dinamikusan változó IP címet kapunk a szolgáltatótól. Ilyenkor a címfordítás részben a „-j SNAT --to-source \$IP_EXT” helyett a „-j MASQUERADE”-et kell használni. Módosítani kell az állomány harmadik sorát is: **IFACE_EXT=ppp0**

```
$IPTABLES -A FORWARD -p udp -s 192.168.0.31 -j ACCEPT
```

Ezt a részt követő négy \$IPTABLES kezdetű sor azokra a csomagokra vonatkozik, amelyeket a kliens gép a szolgáltatónk SMTP és POP3 kiszolgálójához küld. Ezeket a Linux kernel az iptables NAT táblájának segítségével naplózza és átalakítja, majd úgy küldi tovább, mint a sajátjait. Az ezekre érkező válaszokat a kernel szintén átalakítja és 192.168.0.31-es gépnek küldi. Tehát az adott szolgáltatást úgy használja a gépünk, mintha közvetlen Internet-kapcsolata lenne. Figyeljük meg, hogy ebben az esetben a célport (--dport 25) és a cél IP (-d \$SMTPIP) is meghatározott. A többi szabályt nem fogjuk ennyire szigorúan meghatározni, de ezt a protokollt előszeretettel használják vírusok is levéltovábbításra. Lehetőleg csak olyan kliens gépekre alkalmazzuk, amelyeken megfelelően beállított vírusellenőrző program, valamint spyware (kémprogram) és adware (reklámokkal zavaró beépülő program) eltávolító programok is telepítve vannak.

Az ezt követő sorok a NEPTUN rendszerhez biztosítanak hozzáférést a kliens gépnek. A NEPTUN a magyarországi felsőoktatási Egységes Tanulmányi és Felvételi Rendszer, működéséhez a 3389 portot kell engedélyezni. Ha nem használja senki intézményünkben, ki is kapcsolhatjuk.

Ezután néhány biztonsági beállítás következik, majd az open sor után az a rész, ami a tűzfalat kikapcsolja. Ehhez a **/root/tuzfal.scp open** parancsot kell kiadni, de éles rendszeren ez nem ajánlott. A stop paraméterrel indítva minden szabályt kikapcsol és csak az alapértelmezett elutasítás marad. Restart vagy reload paraméterrel történő indítás egyenértékű a stop és a start egymás utáni használatával.

A **tuzfal.scp** program **start** paraméterrel futtatva beállítja a megfelelő szabályokat, viszont a számítógép újraindításakor ezek elvesznek. Ahhoz, hogy elmentsük a beállításokat, ki kell adni a **service iptables save** parancsot is

```
[root@server ~]# /root/tuzfal.scp start  
[root@server ~]# service iptables save
```

A tűzfalbeállításokat a rendszer az /etc/sysconfig/iptables szöveges állományba menti, ahonnan induláskor visszatölti. Az aktuális szabályokat ellenőrizhetjük a következő paranccsal:

```
[root@server ~]# service iptables status
```

A tuzfal.scp nem csak az iptables szabályokat állítja be, hanem kernel modulokat is betölt és biztonsági beállításokat módosít. Kiszolgálónk indulásakor ezeket újra be kell állítani. A szerverhez1.zip csomagban megtaláljuk a kernp.scp szkriptet. Másoljuk a /root könyvtárba, módosítsuk a tulajdonságait és oldjuk meg, hogy az operációs rendszer indulásakor lefusson. A következő parancs ezt valósítja meg:

```
[root@server ~]# chmod 755 /root/kernp.scp  
[root@server ~]# echo "/root/kernp.scp" >> /etc/rc.d/rc.local
```

Az rc.local állomány a rendszer indulásakor, a szolgáltatások elinulása után lefut, hasonlóképpen az MS-DOS autoexec.bat állományához.

A **tuzfal.scp** állomány:

```
#!/bin/bash  
# Vezessünk be néhány változót:  
IFACE_EXT=eth0  
IFACE_INT=eth1  
NET_INT=192.168.0.0/24  
#  
IP_EXT=10.0.0.189  
IP_INT=192.168.0.11  
SMTPIP=194.88.152.1  
POP3IP=194.88.152.2  
#  
IPTABLES=/sbin/iptables  
case "$1" in
```

```

start)
echo "indul...."
# Nehany biztonsagi beallitas:
# Enable broadcast echo protection
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
# Disable source routed packets
for f in /proc/sys/net/ipv4/conf/*/accept_source_route; do
echo 0 > $f
done
# Enable TCP SYN cookie protection
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
# Disable ICMP Redirect acceptance
for f in /proc/sys/net/ipv4/conf/*/accept_redirects; do
echo 0 > $f
done
# Don't send Redirect messages
for f in /proc/sys/net/ipv4/conf/*/send_redirects; do
echo 0 > $f
done
# Drop spoofed packets coming in on an interface, which if replied to,
# would result in the reply going out a different interface
for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
echo 1 > $f
done
# Log packets with impossible addresses
for f in /proc/sys/net/ipv4/conf/*/log_martians; do
echo 1 > $f
done
# IP-tovabbitas a kernelben
echo 1 > /proc/sys/net/ipv4/ip_forward
echo "-----"
echo "A belso halo:"      $NET_INT
echo "-----"
echo "          A tuzfal BELSO halokartyaja: " $IFACE_INT
ifconfig $IFACE_INT | grep "inet addr"
echo "-----"
echo "          A tuzfal KULSO halokartyaja: " $IFACE_EXT
ifconfig $IFACE_EXT | grep "inet addr"
echo "-----"
echo "A tuzfal csomagszuroinek betoltese"
# Eloszor a kernel modulokat toltasuk be
modprobe ip_tables
modprobe ip_conntrack_ftp
modprobe iptable_nat
modprobe ip_nat_ftp
# A regi szabalyokat es a regi egyeni tablakat toroljuk
$IPTABLES --flush
$IPTABLES --delete-chain
$IPTABLES --flush -t nat
$IPTABLES --delete-chain -t nat
#
# Alapertelmezett visszautasitasi szabalyok
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD DROP
$IPTABLES -P OUTPUT DROP
#
# A loopback interface-nek szabad kezert
$IPTABLES -I INPUT -i lo -j ACCEPT
$IPTABLES -I OUTPUT -o lo -j ACCEPT
#
#-----
# Beerkezo szabalyok
#-----

```

```

# A korábban már jóváhagyott kapcsolatok részeként beerkezo csomagok
elfogadása
$IPTABLES -A INPUT -j ACCEPT -m state --state ESTABLISHED,RELATED
#
# Minden TCP kapcsolatnak a SYN kifejezéssel kell kezdodnie:
$IPTABLES -A INPUT -p tcp ! --syn -m state --state NEW -j LOG --log-
prefix "Rejt. letepogatasi kiserlet?"
$IPTABLES -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
# Webservert a belso halora
$IPTABLES -A INPUT -p tcp -i $IFACE_INT -s $NET_INT --dport 80 -m state
--state NEW -j ACCEPT
# SSH a belso halorol. Ezt lehetne korlatozni IP(k)-re...
$IPTABLES -A INPUT -p tcp -i $IFACE_INT -s $NET_INT --dport 22 -m state
--state NEW -j ACCEPT
# A DNS-t a belso gepeknek
$IPTABLES -A INPUT -p udp -s $NET_INT --dport 53 -m state --state NEW -j
ACCEPT
$IPTABLES -A INPUT -p tcp -s $NET_INT --dport 53 -m state --state NEW -j
ACCEPT
# SAMBA a belso gepeknek
$IPTABLES -A INPUT -p udp -s $NET_INT --dport 137 -m state --state NEW -
j ACCEPT
$IPTABLES -A INPUT -p udp -s $NET_INT --dport 138 -m state --state NEW -
j ACCEPT
$IPTABLES -A INPUT -p tcp -s $NET_INT --dport 139 -m state --state NEW -
j ACCEPT
$IPTABLES -A INPUT -p tcp -s $NET_INT --destination-port 445 -m state --
state NEW -j ACCEPT
# Pingek a belso halozatnak
$IPTABLES -A INPUT -s $NET_INT -p icmp -j ACCEPT
# Pingek kivulrol
$IPTABLES -A INPUT -i $IFACE_EXT -p icmp -j ACCEPT
# Proxy hozzaferes a belso halonak:
$IPTABLES -A INPUT -p tcp -i $IFACE_INT -s $NET_INT --dport 8080 -m
state --state NEW -j ACCEPT
# Naplozz mindent, amit fent elutasitottal:
$IPTABLES -A INPUT -j LOG --log-prefix "Visszautasitva (INPUT):"
$IPTABLES -A INPUT -j DROP
#
#-----
# Kimeno szabalyok
#-----
# Amennyiben jóváhagyott kapcsolatok reszet kepezik, engedd ki
$IPTABLES -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
# A kimeno pingek engedelyezese
$IPTABLES -A OUTPUT -p icmp -j ACCEPT
# A kimeno DNS lekerdezesek engedelyezese:
$IPTABLES -A OUTPUT -p udp --dport 53 -j ACCEPT
# A kimeno http engedelyezese:
$IPTABLES -A OUTPUT -p tcp --dport 80 -j ACCEPT
# A kimeno https engedelyezese
$IPTABLES -A OUTPUT -p tcp --dport 443 -j ACCEPT
# A kimeno ssh engedelyezese
# $IPTABLES -A OUTPUT -p tcp --destination-port 22 -j ACCEPT
# A kimeno ftp engedelyezese
$IPTABLES -A OUTPUT -p tcp --dport 21 -j ACCEPT
# A kimeno mail engedelyezese + log
$IPTABLES -A OUTPUT -p tcp --dport 25 -j LOG --log-prefix "mail-ki "
$IPTABLES -A OUTPUT -p tcp --dport 25 -j ACCEPT
#
# SAMBA
$IPTABLES -A OUTPUT -p udp -d $NET_INT --dport 137 -j ACCEPT
$IPTABLES -A OUTPUT -p udp -d $NET_INT --dport 138 -j ACCEPT

```

```

$IPTABLES -A OUTPUT -p tcp -d $NET_INT --dport 139 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $NET_INT --dport 445 -j ACCEPT

$IPTABLES -A OUTPUT -p udp -d $NET_INT --sport 137 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $NET_INT --sport 139 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -d $NET_INT --sport 445 -j ACCEPT
#
# NTP (pontos ido keres + log)
$IPTABLES -A OUTPUT -p udp --dport 123 -j LOG --log-prefix "ntp-
kiszolgalohoz "
$IPTABLES -A OUTPUT -p udp --dport 123 -j ACCEPT
#
# Naplozz mindent, amit fent elutasitottal:
$IPTABLES -A OUTPUT -j LOG --log-prefix "Visszautasitva (OUTPUT):"
$IPTABLES -A OUTPUT -j DROP
#
#-----
# Tovabbitasi szabalyok
#-----
# A korabban mar jovahagyott kapcsolatok reszekent tovabbitando csomagok
$IPTABLES -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
#
# Minden TCP kapcsolatnak a SYN kifejezessel kell kezdodnie:
$IPTABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j LOG --log-
prefix "Letepogatasi kiserlet?"
$IPTABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j DROP
#
# A 192.168.0.31 gep beallitasai:
#$IPTABLES -t nat -A PREROUTING -s 192.168.0.31 -p tcp --dport 80 -j
REDIRECT --to-port 8080
$IPTABLES -A FORWARD -s 192.168.0.31 -j ACCEPT
# CIMFORDITAS Levelek ki + log
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -d $SMTPIP -p tcp --
dport 25 -o $IFACE_EXT -j LOG --log-prefix "mail ki-31 "
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -d $SMTPIP -p tcp --
dport 25 -o $IFACE_EXT -j SNAT --to-source $IP_EXT
# CIMFORDITAS Levelek be + log
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -d $POP3IP -p tcp --
dport 110 -o $IFACE_EXT -j LOG --log-prefix "mail be-31 "
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -d $POP3IP -p tcp --
dport 110 -o $IFACE_EXT -j SNAT --to-source $IP_EXT
# NEPTUN-hoz kell:
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p tcp --dport 3389 -o
$IFACE_EXT -j LOG --log-prefix "NAT 3389 "
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p tcp --dport 3389 -o
$IFACE_EXT -j SNAT --to-source $IP_EXT
# Ping, tracert (csak ha kell)
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p icmp -o $IFACE_EXT -j
LOG --log-prefix "NAT icmp "
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p icmp -o $IFACE_EXT -j
SNAT --to-source $IP_EXT
#
# Syn-flood elleni vedelem:
$IPTABLES -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
# Portscan elleni vedelem:
$IPTABLES -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --
limit 1/s -j ACCEPT
# Ping-flood elleni vedelem:
$IPTABLES -A FORWARD -p icmp --icmp-type echo-request -m limit --limit
1/s -j ACCEPT
# Logoljuk az atiranyitast
$IPTABLES -A FORWARD -j LOG --log-prefix "Visszautasit(FWD)! "
$IPTABLES -A FORWARD -j DROP
#

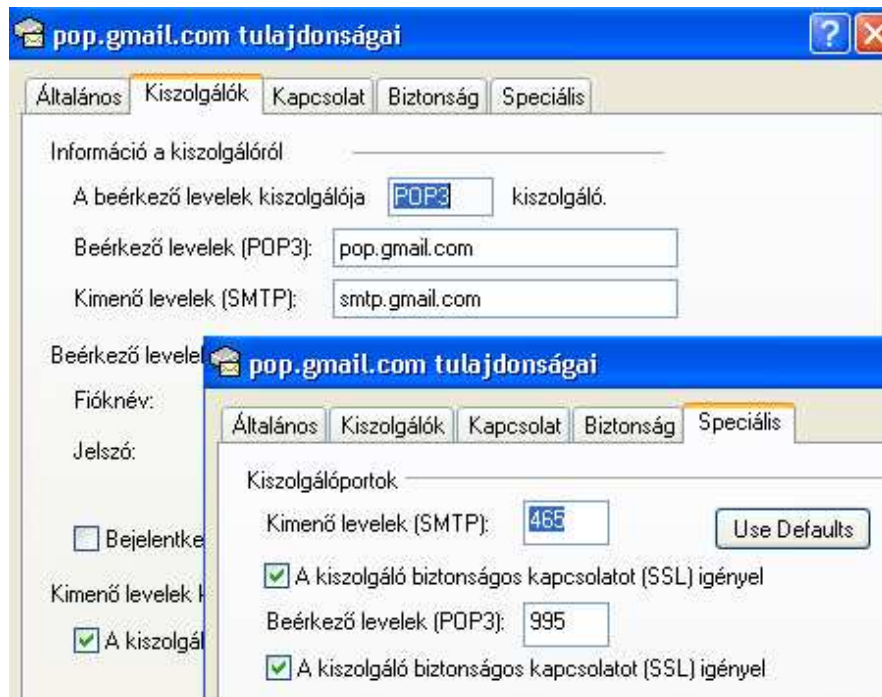
```

```
;;
# Ez az amit nem szabad:
open)
echo "VIGYAZAT! A tuzfal kikapcsolasa! MEGORULTEL??!!"
#
$IPTABLES --flush
$IPTABLES --delete-chain
$IPTABLES --flush -t nat
$IPTABLES --delete-chain -t nat
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT
;;
# Kikapcsol minden tuzfalszabalyt, csak az alapertelmezett elutasitas
marad
# Kenelben IP-tovabbitas ki
stop)
echo "A tuzfal leallitasa zart allapotban!"
echo 0 > /proc/sys/net/ipv4/ip_forward
$IPTABLES --flush
;;
status)
echo "A iptables allapotanak lekerdezese..."
echo " (valojaban az iptables-save parancs vegrehajtasa)..."
$IPTABLES-save
;;
restart|reload)
$0 stop
$0 start
;;
*)
echo "Statusz: $0 {start|open|stop|status|restart|reload}"
exit 1
;;
esac
exit 0
```

Ha a szolgáltató által biztosított e-mail cím kevés, vagy egyáltalán nem biztosít, az Interneten sok ingyenes webmail szolgáltatást nyújtó céget is találunk. Használatához regisztrálni kell az adott portálon, és a fogadható levelek összmérete is korlátozott. Némelyik POP3 és SMTP szolgáltatást is nyújt. Az alábbi sorok lehetővé teszik, hogy az igen népszerű **gmail.com** rendszert használjuk Outlook Express vagy más hasonló programmal. Ezeket a sorokat nem tartalmazza az átmásolt tuzfal.scp állomány, nekünk kell őket beírni. Mivel mindkét szolgáltatás azonosítással és titkosítással működik, itt nem ellenőrizzük a célcímet csak a célportot. Valójában ezeken a portokon nyújtott szolgáltatások bármilyen kiszolgálóról működni fognak.

```
# CIMFORDITAS  GMAIL  Levelek be + log
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p tcp --dport 995 -o
$IFACE_EXT -j LOG --log-prefix "gmail be-31 "
#
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p tcp --dport 995 -o
$IFACE_EXT -j SNAT --to-source $IP_EXT
#
# CIMFORDITAS  GMAIL  Levelek ki + log
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p tcp --dport 465 -o
$IFACE_EXT -j LOG --log-prefix "gmail ki-31 "
#
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.31 -p tcp --dport 465 -o
$IFACE_EXT -j SNAT --to-source $IP_EXT
```

Amennyiben van gmail.com postafiókunk¹ és megfelelően beállítottuk a kliensprogramot akkor a 192.168.0.31 gépen küldhetünk és fogadhatunk leveleket. A kliens program beállításának két részletét a 49. ábra mutatja.



49. ábra

A log állományban a következő sorok jelennek meg levelek küldésénél és fogadásánál. Természetesen ehhez a fenti sorokat be kell írni az iptables állományba és újraindítani a szolgáltatást.

```
[root@server ~]# tail -f /var/log/messages
Jan  4 22:44:21 server kernel: gmail ki-31 IN= OUT=eth0 SRC=192.168.0.31
DST=66.249.93.109 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13545 DF
PROTO=TCP SPT=1802 DPT=465 WINDOW=65535 RES=0x00 SYN URGP=0

Jan  4 22:44:35 server kernel: gmail be-31 IN= OUT=eth0 SRC=192.168.0.31
DST=66.249.93.111 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13562 DF
PROTO=TCP SPT=1803 DPT=995 WINDOW=65535 RES=0x00 SYN URGP=0

Jan  4 22:45:52 server kernel: gmail be-31 IN= OUT=eth0 SRC=192.168.0.31
DST=66.249.93.111 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13749 DF
PROTO=TCP SPT=1819 DPT=995 WINDOW=65535 RES=0x00 SYN URGP=0
```

Amennyiben más kliensgépeknek is akarunk a fenti szolgáltatások valamelyikét nyújtani, akkor az adott szövegrészt a Midnight Commander editorával kijelölhetjük és másolhatjuk. (F3-kijelölés kezdete, iránybillentyűkkel kijelölés, ismét F3 kijelölés vége és az F5 a kurzor pozíciójába beilleszt.) Az átmásolt sorokban kijavítjuk az IP címet és a --log-prefix utáni részt és újraindítjuk az iptables-t. Így minden gép forgalmát be tudjuk azonosítani a /var/log/messages állományban.

Természetesen arra is van mód, hogy egy gépnek minden szolgáltatást biztosítsunk a kiszolgálón keresztül az Internet felé. A következő néhány sorban arra látunk példát, hogy a 192.168.0.32 IP címmel rendelkező gép minden csomagját NAT-olja a kiszolgáló, függetlenül portszámtól, a protokolltól vagy célcímtől. Ezt a módszert a gyakorlatban nem javaslom. Az adott gép bármelyik programja küldhet adatokat az Internet felé, egy vírusfertőzés esetén ennek kellemetlen következményei lehetnek. Több program a háttérben kéretlenül is forgalmat bonyolít, főlegesen

¹ Természetesen más cég is nyújt hasonló szolgáltatást. Ha van valamilyen webmail postafiókunk, a honlapján tájékozódjunk, hogy van-e ilyen szolgáltatásuk. Olvassuk el a kliens beállításának leírását, abból kiderül, hogy mely portokon működik.

terhelve ezzel a hálózatot. Az alábbi sorok naplózást is beállítanak ezekre a csomagokra, és ez rövid idő alatt igen nagyméretű messages állományt eredményez. Ha viszont kikapcsoljuk a naplózást, akkor csak az MRTG grafikonjából következtethetünk az adott kliens gép hálózati forgalmára.

```
$IPTABLES -A FORWARD -s 192.168.0.32 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.32 -o $IFACE_EXT -j LOG --
log-prefix "NAT-32 "
$IPTABLES -t nat -A POSTROUTING -s 192.168.0.32 -o $IFACE_EXT -j SNAT --
to-source $IP_EXT
```

Ahhoz, hogy a módosított tűzfalszabályok érvényre jussanak le kell futtatni a skriptet ismételten start paraméterrel:

```
[root@server ~]# /root/tuzfal.scp start
```

A szabály mentéséhez, pedig a következő parancsot is ki kell adni:

```
[root@server ~]# service iptables save
```

Időszinkronizálás

Szerverünk óráját szinkronizáljuk az ntpd szolgáltatás segítségével külső kiszolgálóhoz. Mivel a munkaállomások a szerverhez fogják igazítani saját óráikat, ezért fontos, hogy a kiszolgálónk órája pontos legyen. Az első szinkronizáció előtt állítsuk le a Squid proxy servert, mivel nagyobb időeltolódás esetén gond lehet vele:

```
[root@server ~]# service squid stop
```

Szinkronizáljuk gépünk óráját a **hu.pool.ntp.org** szerverhez:

```
[root@server ~]# ntpdate hu.pool.ntp.org
2 Jan 20:24:11 ntpdate[9891]: step time server 62.112.213.213 offset
-84.623566 sec
[root@server ~]# ntpdate hu.pool.ntp.org
2 Jan 20:24:15 ntpdate[9892]: adjust time server 62.112.213.213 offset
-0.007776 sec
```

A parancs első kiadásakor 84 másodpercet sietett a gépünk, második szinkronizáláskor az eltérés gyakorlatilag nulla.

Indítsuk el az ntpd szolgáltatást és állítsuk be, hogy automatikusan induljon:

```
[root@server ~]# service ntpd start
[root@server ~]# chkconfig --level 235 ntpd on
```

Ezzel be is állítottuk a szinkronizálást. A squid-et indítsuk el újra:

```
[root@server ~]# service squid start
```

IX. Kapcsolat rendszerek között. A Samba

Kiszolgálónk másik nagyon fontos szolgáltatása az Internet-megosztás mellett a fájlserver működtetése. Linux operációs rendszeren ezt a Samba nevű programcsomaggal valósítjuk meg. A Samba szabad szoftver, és használatával egy kis vagy közepes intézmény számára állomány- és nyomtatószervert alakíthatunk ki.

Ebben a fejezetben beállítjuk a kiszolgálót, hogy a felhasználóknak bármelyik kliensről hozzáférhető tárhelyet biztosítson adatai számára. Az adatokat a /home könyvtárban tárolja a kiszolgáló, és a munkaállomásokról felhasználói név és jelszó beírásával elérhető. Ebben a fejezetben a munkaállomások operációs rendszereként Windows 98-at, Windows 2000-et, Windows XP-t és a Windows Vista-t tárgyaljuk.

A Samba beállítása

A Samba programcsomag felkerült a rendszerre telepítéskor, viszont az alapbeállítás szerint nem indul rendszerindításkor. A következő paranccsal ellenőrizhetjük, hogy a program melyik változata van feltelepítve:

```
[root@server ~]# rpm -qa | grep samba
system-config-samba-1.2.21-1
samba-common-3.0.10-1.4E.9
samba-client-3.0.10-1.4E.9
samba-3.0.10-1.4E.9
```

A service smb status parancs pedig a szolgáltatás állapotát árulja el:

```
[root@server ~]# service smb status
smbd is stopped
nmbd is stopped
```

A Samba két démonja, az smb és a nmb segítségével működik. Az smb hitelesíti a felhasználókat és az adatok átvitelét végzi, az nmb pedig a névszolgáltatás.

A Samba konfigurációs állománya az /etc/samba/smb.conf. Ebben az állományban nem csak a # karakterrel, hanem a pontosvesszővel kezdődő sorok megjegyzéseknek minősülnek. Az mc editorával megváltoztathatjuk az állományt, de még mielőtt módosítanánk, készítsünk másolatot a /root/eredeti könyvtárba:

```
[root@server ~]# cp /etc/samba/smb.conf /root/eredeti/
```

A konfigurációs állomány több egységre tagolható. A **global** részben a szolgáltatás egészére vonatkozó beállításokat találjuk. A **homes** részben a /home könyvtárra, vagyis a felhasználók adataira vonatkozó bejegyzések vannak. A homes részhez hasonlóan létrehozhatunk bejegyzéseket, amelyek megosztásként jelennek meg majd a hálózaton.

A serverhez1.zip csomagban megtaláljuk az általam javasolt konfigurációs állományt. Mielőtt átmásolnánk ezt az /etc/samba könyvtárba, hozzunk létre néhány könyvtárat:

```
[root@server /]# mkdir /inst
[root@server /]# mkdir /inst/client
[root@server /]# mkdir /oktat
[root@server /]# mkdir /home/tanar
[root@server /]# mkdir /oktat/oktatasi_anyagok
[root@server /]# mkdir -p /usr/local/samba/lib/netlogon
```

Módosítsuk a /home/tanar könyvtár tulajdonságait:

```
[root@server ~]# chown pferi /home/tanar
[root@server ~]# chgrp tanar /home/tanar
[root@server ~]# chmod 770 /home/tanar
```

A következő smb.conf segítségével beállított Samba működését vizsgáljuk meg a gyakorlatban. Az eredeti állományból nem töröltem ki a megjegyzéseket és a mintabeállításokat tartalmazó sorokat, későbbi módosításoknál még szükség lehet rájuk. A következő paranccsal kilistázzhatjuk az állományt üres sorok, valamint # és ; vel kezdődő sorok nélkül:

```
[root@server ~]# cat /etc/samba/smb.conf | sed '/^#/d; /^;/d; /^ *$/d'
```

tehát csak azok a sorok jelennek meg a képernyőn, amelyek ténylegesen befolyásolják a Samba működését.

Az **smb.conf** állomány:

```
[global]
  workgroup = HOME
  netbios name = server44
  server string = Samba Server
  interfaces = eth1 lo
  bind interfaces only = yes
  hosts allow = 192.168.0. 127.
  hosts deny = 0.0.0.0/0
  log file = /var/log/samba/%m.log
  max log size = 50
  security = user
  encrypt passwords = yes
  smb passwd file = /etc/samba/smbpasswd
  socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
  local master = yes
  os level = 88
  domain master = yes
  preferred master = yes
  domain logons = yes
  logon script = login.bat
  name resolve order = wins lmhosts bcast
  wins support = yes
  dns proxy = no
  dos charset = 852
  unix charset = ISO8859-2
  display charset = ISO8859-2
  idmap uid = 16777216-33554431
  idmap gid = 16777216-33554431
  template shell = /bin/false
  winbind use default domain = no
[homes]
  comment = Home Directories
  path = %H/Dokumentumok
  browseable = no
  writable = yes
  create mask = 0644
  directory mask = 0755
[netlogon]
  comment = Network Logon Service
  path = /usr/local/samba/lib/netlogon
  guest ok = yes
  browsable = no
  writable = no
  share modes = no
[adminhome]
  comment = csak adminisztracios celokra!
  path = /home
  valid users = pferi hrobi
  public = no
  writable = no
```

```

    printable = no
    browseable = no
[inst]
    comment = install programok
    path = /inst
    public = yes
    writable = no
    printable = no
    browseable = yes
[oktat]
    comment = oktatasi anyagok inditofajljai
    path = /oktat/oktatasi_anyagok
    public = yes
    writable = no
    printable = no
    browseable = yes
[tanaroknak]
    comment = tanaroknak irhato
    path = /home/tanar
    public = no
    writable = yes
    printable = no
    browseable = no
    valid users = @tanar

```

A **[global]** részben beállítjuk a munkacsoport nevét: **workgroup = HOME**, ezt módosítsuk. Ez a név nem tartalmazhat szóközt és speciális karaktereket. Lehetőleg az intézményre utaló szó legyen, pl. SULI. Ezt majd minden Windows munkaállomáson be kell állítani.

A **netbios name = server44**, a kiszolgáló nevét adja meg. Módosíthatjuk, vagy maradhat a server44 is. A következő sor azt a hálózati interfészt határozza meg, melyiken működik a Samba, esetünkben ez az eth1. A következő sor feltételezi, hogy belső hálózatunkon 192.168.0.1 - 192.168.0.254 IP címmel rendelkező gépek vannak. Ha szükséges, módosítsuk.

A **dos charset = 852**, és az utána következő két sor segítségével beállítottuk, hogy a kiszolgálóra mentett fájlok nevében előforduló ékezetes karakterek megfelelően jeljenek meg mind a Linux-on, mind a Windows-on. Szerencsés, ha a felhasználók nem írnak ő vagy ű betűket mappa- vagy fájlnevbe, de a kiszolgálón ezzel nem lesz gond. Probléma lehet viszont a cirill betűs nevekkal, a felhasználókat figyelmeztessük erre. Amennyiben a kliens operációs rendszerek nyelve orosz vagy ukrán, módosítsuk a fenti sorokat.

A **[home]** részben meghatároztuk, hogy minden felhasználó könyvtárában lévő Dokumentumok könyvtárat kapják meg a felhasználók saját megosztásként. Ez a könyvtár minden felhasználó könyvtárában ott van, mivel az /etc/skel könyvtárban létrehoztuk. Erre első sorban azért van szükség, hogy a felhasználó könyvtárában lévő ponttal kezdődő állományok ne legyenek elérhetőek. Ezekre a azoknak a felhasználóknak van szüksége, akik bejelentkeznek a kiszolgálóra.

A **create mask = 0644** sor beállítja, hogy milyen jogosultságokkal jöjjön létre állomány a kiszolgálón, ha munkaállomásról a HOME könyvtárunkba mentünk. A következő sor ugyanezt állítja be könyvtárra.

A **[netlogon]** részben beállítunk egy speciális megosztást, amelyikben a login.bat állomány végrehajtódik a kliens számítógépen, ha Windows 98 operációs rendszerről kapcsolódunk a kiszolgálóhoz. Másoljuk át a login.bat állományt az **/usr/local/samba/lib/netlogon** könyvtárba.

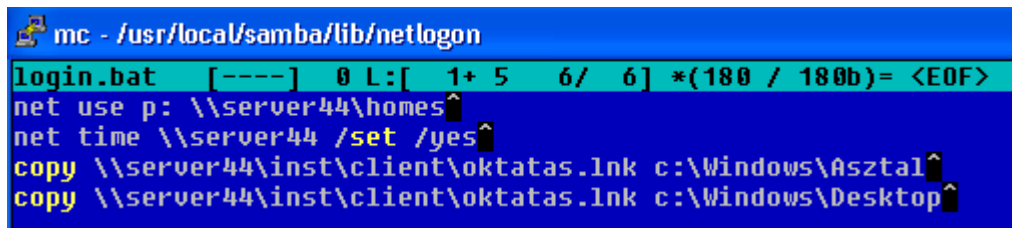
A **login.bat** állomány:

```

net use p: \\server44\homes
net time \\server44 /set /yes
copy \\server44\inst\client\oktatasi.lnk c:\Windows\Asztal
copy \\server44\inst\client\oktatasi.lnk c:\Windows\Desktop

```

Mivel a Windows és a Linux sorvég formátuma különbözik, a kiszolgálón módosított login.bat nem biztos hogy megfelelően fog működni a munkaállomáson. A legegyszerűbben ezt úgy kerülhetjük el, ha Windows-os gépen módosítjuk a login.bat-ot. Ott kipróbáljuk, és ha megfelelően működik átmásoljuk a kiszolgálóra. Amennyiben a kiszolgálónak más nevet adtunk, módosítsuk a sorokat. A windowsos sorvég karaktereket láthatjuk, ha megnyitjuk szerkesztésre az állományt. (50. ábra)



```
mc - /usr/local/samba/lib/netlogin
login.bat [----] 0 L:[ 1+ 5 6/ 6] *(180 / 180b)= <EOF>
net use p: \\server44\homes
net time \\server44 /set /yes
copy \\server44\inst\client\oktatas.lnk c:\Windows\Asztal
copy \\server44\inst\client\oktatas.lnk c:\Windows\Desktop
```

50. ábra

A login.bat első a homes részben meghatározott megosztást létrehozza a Windows-on mint **P:** meghajtó. Ez a meghajtó a quota-ban meghatározott méretű lesz, tehát tanulóként csatlakozva 90 Mb, tanárként 300 Mb.

A következő sor a Windows óráját a kiszolgálóéhoz igazítja. Tehát, ha bejelentkeznek a felhasználók, minden számítógép órája pontos lesz.

A harmadik sor átmásol egy lnk kiterjesztésű állományt a Windows Asztalára. Az utolsó sor ugyanezt teszi csak angol nyelvű Windows 98 esetén. Ezt az állományt a kliensen hozzuk létre.

A következő **[adminhome]** részben beállíthatjuk, hogy bizonyos felhasználók (pl. az informatika-tanárok) olvasási joggal hozzáférhessenek a diákok home könyvtárához is. Ehhez a `valid users = pferi hrobi` sort módosítsuk. Azoknak a tanároknak a felhasználói nevét írjuk ide, akiknek ezt a lehetőséget biztosítani akarjuk. A tájékoztatón a tanulók figyelmét hívjuk fel erre. Ha nem akarjuk használni ezt a megosztást, töröljük a sorokat vagy a sorok elé írunk `#` karaktert.

Az **[inst]** részben létrejön egy megosztás, ami mindenki számára olvasható lesz. Az `/inst` könyvtárba olyan programokat másolhatunk, amelyek a munkaállomások beállításához szükségesek. A `browseable = yes` sor tállózzhatóvá teszi ezt a megosztást. A fenti adminhome megosztásra ez nem igaz, azt csak úgy érhetjük el, ha pontosan hivatkozunk rá: `\\SERVER44\adminhome`.

Az **[oktat]** részben meghatározott megosztásból, oktatási anyagokat fogunk majd indítani a munkaállomásokon. Tulajdonságai megegyeznek az inst megosztásáéval.

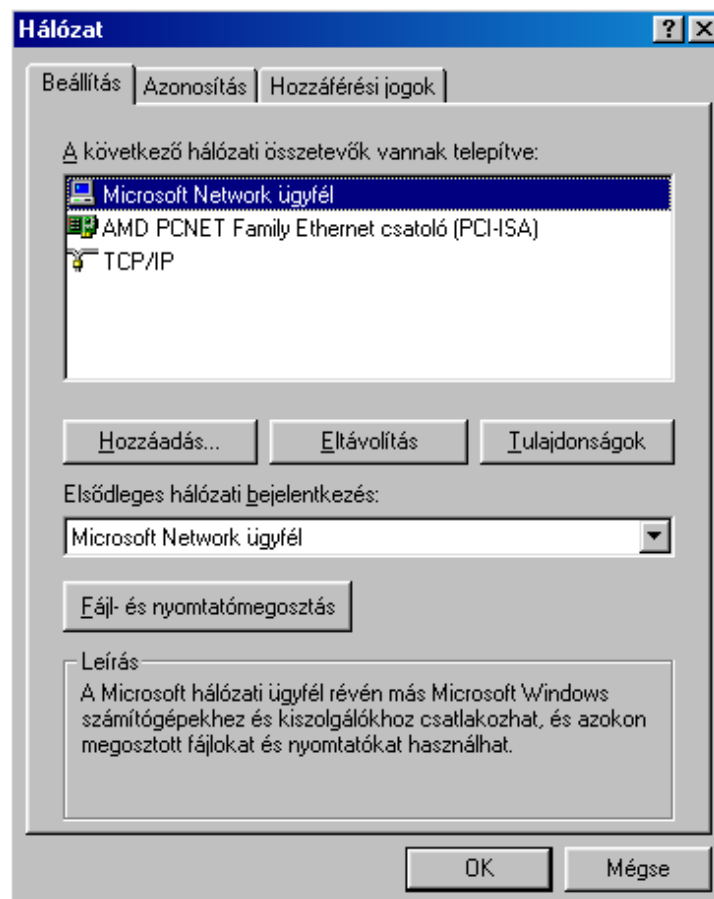
Az utolsó **[tanaroknak]** részben egy speciális megosztást hozunk létre. Lehetőséget teremtünk vele, hogy a tanárok állományokat oszthassanak meg egymással. Ez is csak pontos hivatkozással érhető el, és csak a tanar csoportba tartozó felhasználók férhetnek hozzá. Mivel ez a megosztás is a /home könyvtárban jön létre, a tanárok által ide másolt állományaira is érvényes lesz a tárkorlátozás.

Indítsuk el a Samba-t és állítsuk be, hogy automatikusan induljon:

```
[root@server ~]# service smb start
[root@server ~]# chkconfig --levels 235 smb on
```

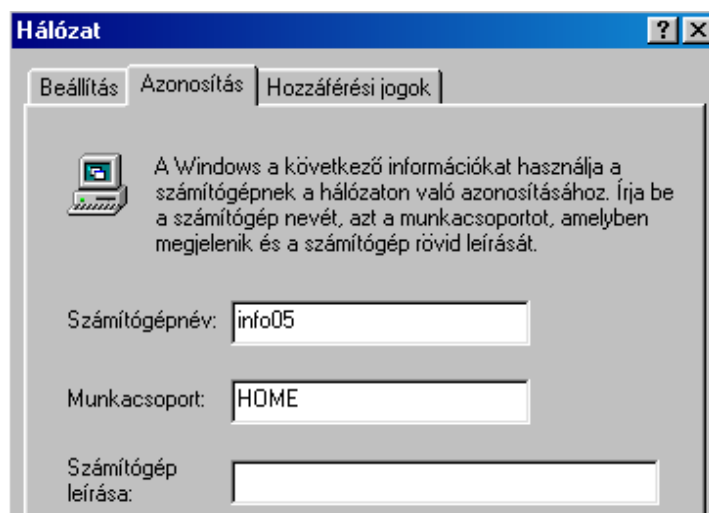
A munkaállomás beállítása. Windows 98

Windows 98 esetén először ellenőrizzük a hálózat beállítását. Szerencsés, ha a fájl és nyomtatómegosztás nincs bekapcsolva. Ha a kliensek egymás közt állományokat másolhatnak, az biztonsági kockázatot jelent. (már ha 98 alatt beszélhetünk egyáltalán biztonságról...) Csak a következő hálózati összetevők legyenek telepítve: Microsoft Network ügyfél, TCP/IP protokoll és a hálózati csatoló. (51. ábra) Ha más hálózati szolgáltatás is telepítve van, távolítsuk el őket.



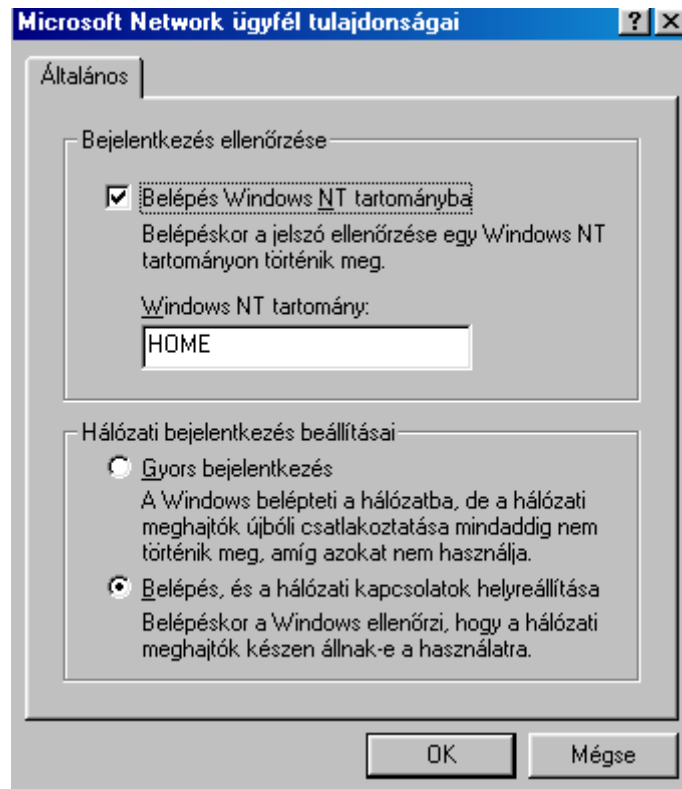
51. ábra

Az azonosítás ablakba írjuk be a munkacsoport nevét. Ez minden kliens gépnél ugyanaz legyen: amit beirtunk az smb.conf állományba a „**workgroup**” sorba. A Számítógépnév viszont legyen egyedi. Szerencsés, ha a névből következtetni lehet a számítógép sorszáma vagy teremben elfoglalt helyére. (52. ábra)



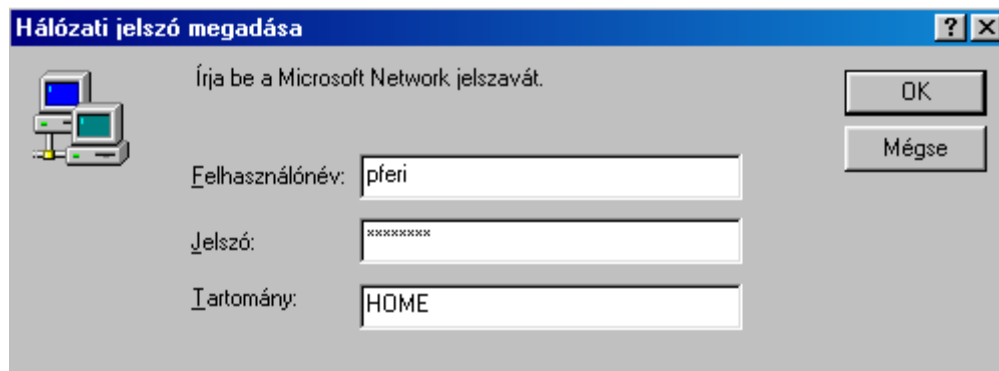
52. ábra

Ezután válasszuk ki 51. ábrán látható „Microsoft Network ügyfél” sort és kattintsunk a tulajdonságokra. Kapcsoljuk be az 53. ábrán látható kapcsolókat és írjuk be a Windows NT tartomány sorba is a munkacsoport nevét.



53. ábra

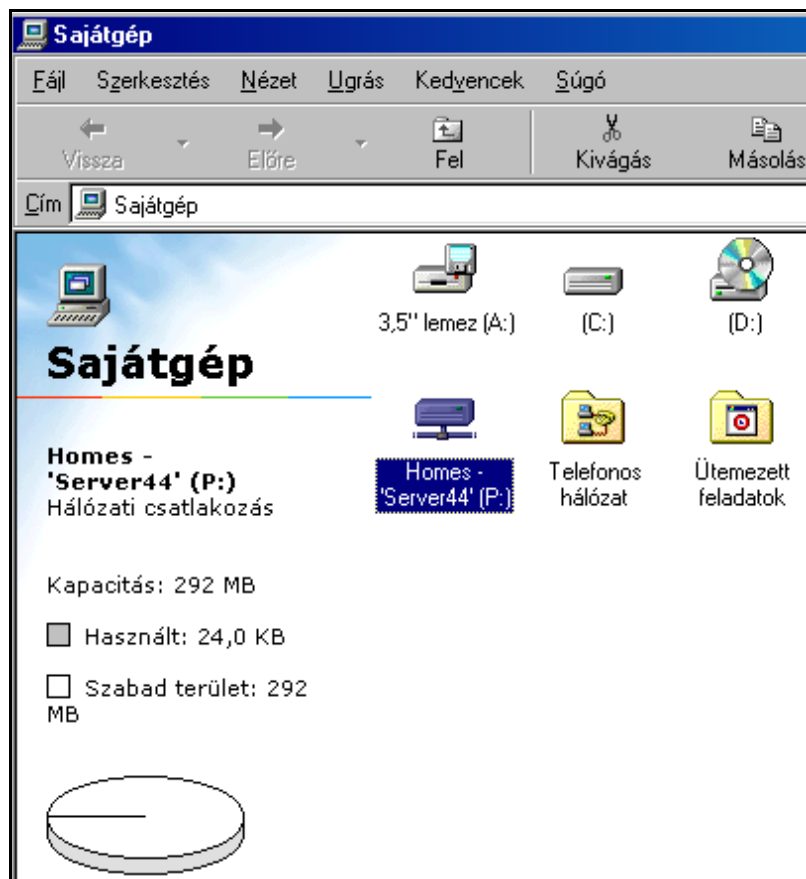
A Windows 98 újraindul, a megjelenő ablakba írjuk be a felhasználói nevünket és a jelszót. (54. ábra) Ha a bejelentkezés sikeres, a bal felső sarokban ablakok tűnnek fel: a kliens lefuttatja a bejelentkezési parancsfájlokat, esetünkben a login.bat-ot. A következő „Windows jelszó megadása” ablakba nem kell a jelszót ismét beírni, kattintsunk a Mégse gombra.



54. ábra

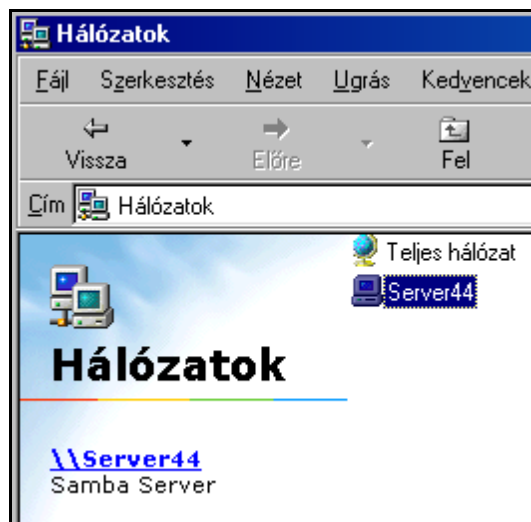
Nyissuk meg a Sajátgépet. Látunk egy **P:** meghajtót, ami 300 Megabájt kapacitású, (55. ábra) a kiszolgálón helyezkedik el, esetünkben a /home/pferi/Dokumentumok könyvtárban. Számunkra írható-olvasható, más a jelszavunk ismerete nélkül nem férhet hozzá. Bármelyik számítógépről is jelentkezőnk be, mindig a saját HOME könyvtárunkat kapjuk **P:** meghajtóként. Munkánkat befejezve mindig jelentkezünk ki a munkaállomáson! Erre hívjuk fel a kollégák és a tanulók figyelmét is.

A **P:** meghajtóról letörölt fájlokat nem lehet visszaállítani, használjuk igen körültekintően!



55. ábra

Nyissuk meg a Hálózatok rendszermappát az asztalon. Kiszolgálónk megjelenik az ablakban (56. ábra) azt megnyitva látjuk azt a három megosztást, amelyeken engedélyeztük a browseable, tallózás opciót. Ezek az inst, oktat és látjuk a felhasználói nevünket is megosztásként, ami valójában megegyezik a **P:** meghajtóval.



56. ábra

Készítsünk parancsikont a Windows asztalra az **oktat** megosztásról. Egyszerűen próbáljuk egérrel az asztalra húzni, és a Windows felajánlja, hogy készít egy parancsikont. Nevezzük át a parancsikont oktat-as-ra, ékezet nélkül. Másoljuk a P: meghajtóra. Ezután a kiszolgálón (vagy a PuTTY ablakában) helyezzük át a **/inst/client** könyvtárba. Ezzel megoldottuk, hogy ez a parancsikon minden bejelentkezéskor ott lesz a kliensek asztalán, akkor is ha a tanulók előzőleg letörölték.

Ellenőrizzük, a többi megosztás működését is. Hozzunk létre valamelyik mappában egy Tanar.bat nevű állományt. Nyissuk meg szerkesztésre és írjuk be a következő parancsot:

```
net use n: \\server44\tanaroknak
```

Készítsünk egy parancsikont az asztalra a fájlról, nevezzük át pl. „Közös tanároknak”-ra és választhatunk egy másik ikont is hozzá. (57. ábra)



57. ábra

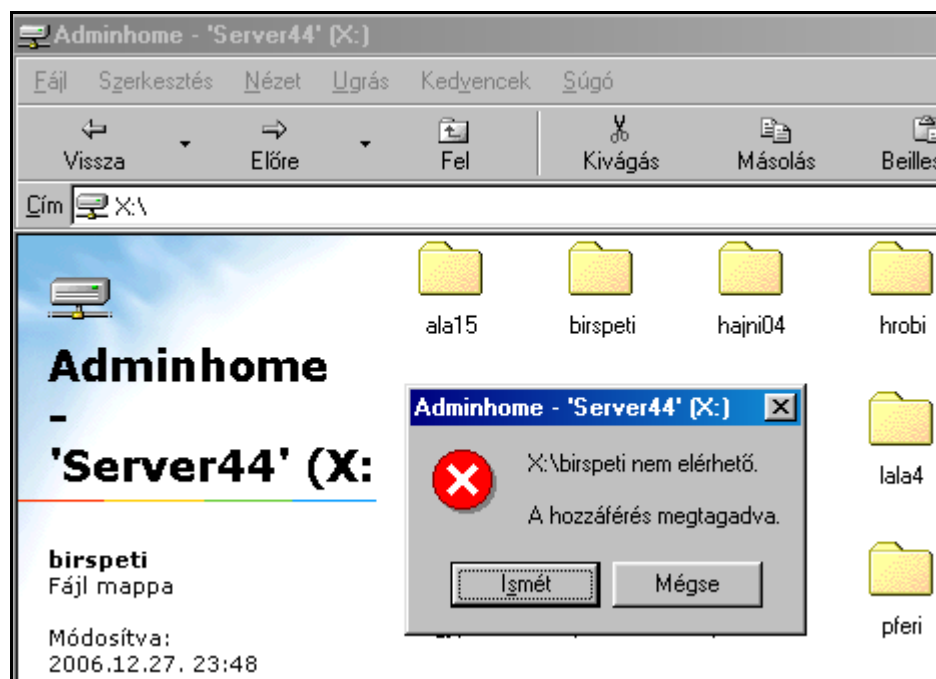
Kettőt kattintva a parancsikontra végrehajtódik a net use parancs és kapunk egy **N:** meghajtót is, ahová szintén menthetünk fájlokat létrehozhatunk mappákat. Ezt minden kolléga láthatja és mi is olvashatjuk mások által ide elmentett állományokat. Törölni viszont mindenki csak a saját dokumentumát, mappáját tudja. Ezzel a tanárok dokumentumokat tudnak egymással megosztani, ami megkönnyíti, hogy közös projekteken dolgozzanak.

Tanulóként bejelentkezve a gépre a **P:** meghajtó létrejön, de a mérete csak 90 Megabyte lesz. A fenti, csak tanároknak létrehozott megosztás nem érhető el. A tanulók hibaüzenetet kapnak a parancsikontra kattintva.

Ha létrehoztuk az adminhome megosztást is, az előzőhöz hasonlóan hozzunk létre admin néven bat állományt és arról asztalra parancsikont. Csak azoknak a tanároknak a gépén hozzuk létre ezeket az állományokat, akiknek a felhasználói nevét beírtuk a valid users sorba. Tartalma a következő lehet:

```
net use x: \\server44\adminhome
```

Lefuttatva az admin.bat állományt, kapunk egy **X:** meghajtót is. Megnyitva látjuk mindenkinek a Home könyvtárát. A tanulókét meg tudjuk nyitni, de csak olvasásra. A tanárok nevére kattintva, hibaüzenetet kapunk, a kiszolgáló megtagadja a hozzáférést. (58. ábra). Ezzel a módszerrel tanárok ellenőrizhetik a tanulók munkáit, kigyűjthetik a beadandó dolgozatokat.



58. ábra

A munkaállomás beállítása. Windows XP

Amennyiben a munkaállomások operációs rendszere Windows XP Professional vagy Windows 2000, Windows tartományt is használhatunk. Vagyis a Samba felhasználók képesek bejelentkezni a munkaállomásokra saját felhasználói nevükkel és jelszavukkal, és akár mozgó profilt (*roaming profile*) is kialakíthatunk. Ha az összes munkaállomás operációs rendszere ilyen, és a kiszolgálót is nagy teljesítményű és megbízhatóan működő számítógépre telepítettük, megfontolandó a tartomány kialakítása.

Én mégsem ezt a módszer fogom bemutatni. Ennek több oka is van. Először is a legtöbb iskolában igen vegyes Windows változatok vannak, és az XP Home Edition változata sem képes tartományban működni. Másod sorban, ha egy gépet több tucat felhasználó is használ, és általában ez a helyzet iskolákban, a munkaállomásokon igen nagy káosz keletkezhet. A tartományba lépéskor ugyanis a munkaállomáson létrejön a felhasználó könyvtárba, amit a kiszolgálóra másol kijelentkezéskor. Másik gépre bejelentkezve, ezt ott is létrehozza, a szerverről letöltve az adatokat. Tehát előbb-utóbb minden gépen lesz minden tanulónak könyvtára a Documents and Settings könyvtárban. Nem beszélve a hálózati forgalomról, amit pl. 20 tanuló bejelentkezése generál több 10 megabájtos profilokkal.

A *roaming profile*-t ki is kapcsolhatjuk, akkor viszont a felhasználók fogják nehezen megtalálni a dokumentumaikat, hiszen amikor a gépen dolgoznak, valóban van egy „saját” könyvtáruk. Azt tudom javasolni, hogy olvassunk szakirodalmat a tartományvezérlőként való használatról, és csak akkor alkalmazzuk, ha megvannak hozzá a feltételek. Én azt tapasztaltam, hogy oktatási intézményben, ha valóban saját felhasználói azonosítókat biztosítunk a tanulóknak, több problémát vet fel a használata, mint amennyit megold.

Az általam javasolt módszer a következő: minden kliens számítógépen létrehozunk egy korlátozott jogosultságú felhasználót, és ennek a felhasználónak a jelszava is mindenki számára publikus. Vagyis bárki használhatja az operációs rendszert, bárki beléphet, viszont ez a felhasználó nem módosíthatja az alapvető rendszerbeállításokat, nem telepíthet programokat, nem módosíthatja a jelszavát. Az NTFS jogosultságok beállításával egyszerűen megoldható, hogy az Asztal és a Start menü tartalmát sem módosíthatja ez a felhasználó. A gpedit.msc programmal (Start / Futtatás / gpedit.msc) beállítható a helyi biztonsági házirend. Ennek a felhasználónak a jogosultságával a

tanulók hozzáférnek a hálózat mindenki számára elérhető megosztásaihoz. A személyes HOME könyvtáruk pedig, egy kis program segítségével, saját felhasználói nevük és jelszavuk beírásával érhető el. A tanulók tudnak ideiglenes állományokat a munkaállomásra is menteni, de hamar megtanulják, hogy csak amit a **P:** meghajtóra mentenek el, azt érhetik el bármelyik gépről. Kijelentkezve a munkaállomásról a HOME könyvtárukhoz más nem férhet hozzá.

Az is e megoldás mellett szól, hogy a hálózat vagy a kiszolgáló meghibásodása esetén a munkaállomások ugyanúgy használhatóak, csak a hálózat nem érhető el. Valamint a tanulók úgy is használhatnak bizonyos szolgáltatásokat, például multimédiás oktatóanyagot, hogy nincs felhasználói azonosítójuk a kiszolgálón.

Mielőtt létrehoznánk a tanuló felhasználót a munkaállomásokon, a következő rövid programmal hozzuk létre a kiszolgálón:

Az **xp_prof_user.scp** program:

```
#!/bin/bash
# Felhasználó létrehozása
#
# A felhasználói név
UNEV=tanulo
# Jelszo
PASS=tanulo543
#
useradd -M -c "Tanulo Felhasználó" -s /bin/false $UNEV
# létrehozzuk a jelszót:
echo $PASS | passwd $UNEV --stdin
# SAMBA jelszo létrehozása
(echo $PASS; echo $PASS) | smbpasswd -s -a $UNEV
```

A felhasználói neve **tanulo**, a jelszava **tanulo543** lesz, de a megfelelő sorokat átírva ezeket módosíthatjuk. Természetesen a felhasználói névnek egyedinek kell lenni, és később már körülményes megváltoztatni, mert minden kliens gépen lokálisan is létrehozzuk. Ennek a felhasználónak nem lesz HOME könyvtára, és nem tagja az eddig létrehozott csoportok egyikének sem.

Hozzuk létre a munkaállomásokon új felhasználói fiókot. A fióknév a fenti felhasználói név legyen, a fióktípus korlátozott. A gyors felhasználóváltást és az üdvözlőképernyő használatát kapcsoljuk ki. A Felügyeleti eszközök / Számítógép-kezelés / Helyi felhasználók és csoportok / Felhasználók ablakban, a **tanulo** felhasználó tulajdonságainál állítsuk be, hogy a jelszavát ne változtathassa meg. (59. ábra)

Az XP Professional operációs rendszerben Vezérlőpult / Mappa beállításai / Nézet ablakban kapcsoljuk ki az „Egyszerű fájlmegosztás használata” utáni négyzet jelölését. Ezután már mappákra és állományokra is módosíthatjuk az engedélyeket. Ajánlatos beállítani, hogy a rendszerpartíció gyökérkönyvtárban ne hozhasson létre **tanulo** felhasználó mappákat és állományokat. Legjobb, ha csak a C:\Dokuments and Settings\tanulo\Dokumentumok könyvtárba hozhatnak létre állományokat és mappákat.

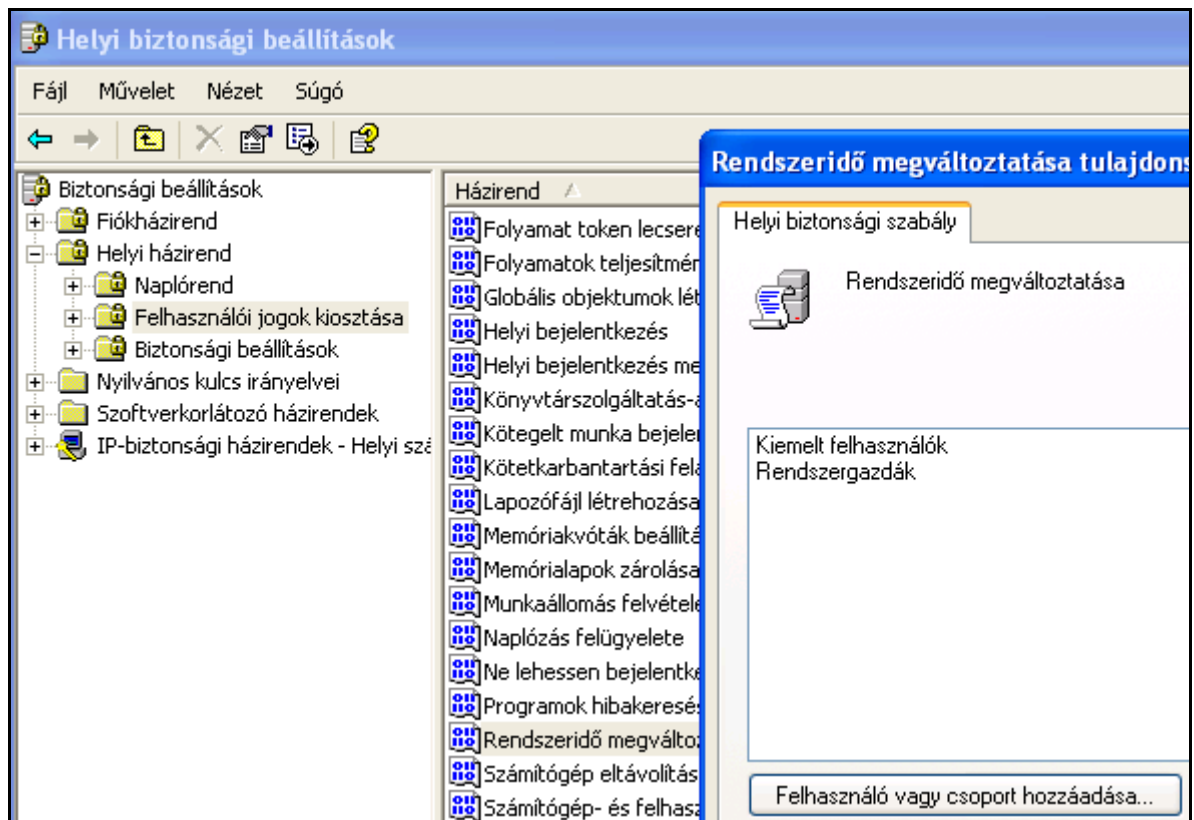
XP Home Edition esetén már nem ilyen egyszerű helyzet, itt az egyszerű fájlmegosztás mindig be van kapcsolva. Megtalálhatjuk a megoldást, ha rákeresünk az Interneten a következő kifejezésre: „Windows XP Home NTFS Security Shell Extension”. A néhány kilobájtos kiegészítés telepítése után a Professional-hoz hasonlóan beállítható.

Vezérlőpult / Mappa beállításai / Nézet ablakban kapcsoljuk ki az „Hálózati mappák és nyomtatók automatikus keresése” utáni négyzet jelölését is.



59. ábra

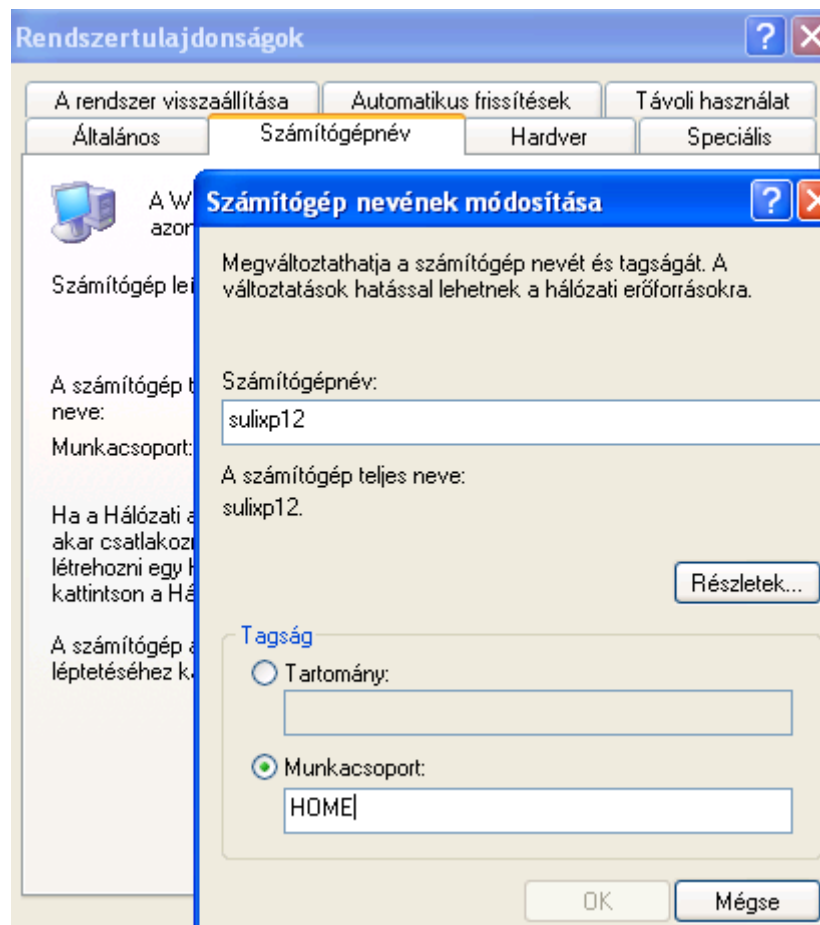
Mivel a tanulo felhasználó bejelentkezésekor a munkaállomás a kiszolgáló órájához próbálja igazítani a saját óráját, a helyi biztonsági házirendben engedélyezzük a rendszeridő megváltoztatását **tanulo** felhasználónak. Ehhez válasszuk a Felhasználó vagy csoport hozzáadását (60. ábra) és írjuk be a felhasználó nevet.



60. ábra

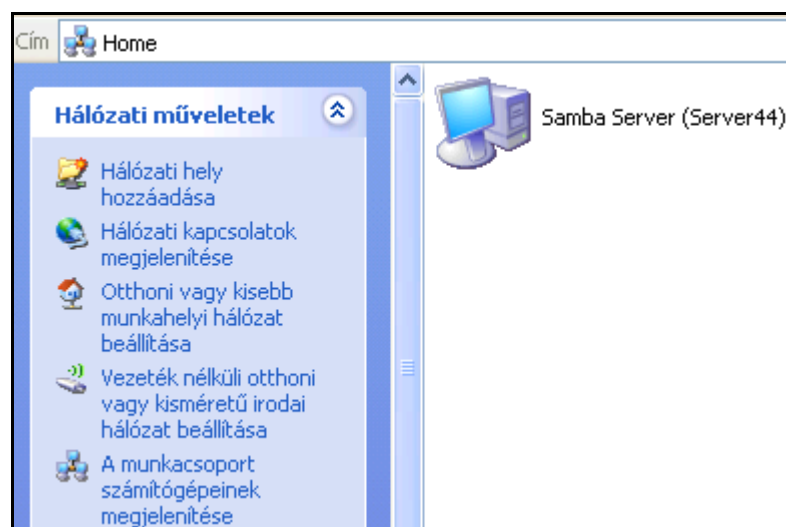
Azt, hogy az Internet Explorer ne ajánlja fel a jelszó mentését az serverhez1.zip csomagban található DisablePasswordCaching.vbs szkript lefuttatásával érhetjük el. A Windows registry több bejegyzését módosítja a szkript, **tanulo** felhasználóként bejelentkezve futtassuk le. Másoljuk ezt az állományt a kiszolgáló /inst/client könyvtárba, az inst megosztás segítségével könnyen hozzáférünk bármelyik gépről.

Állítsuk be a Windows XP a munkacsoportunk tagja legyen. A Vezérlőpult / Rendszer / Számítógépnév ablakba írjuk be a munkacsoport nevét és az egyedi számítógépnévét (61. ábra)



61. ábra

Jelentkezzünk be **tanulo** felhasználóként és ellenőrizzük, a megosztásokat. Nyissuk meg a „Hálózati helyek” rendszermappát és kattintsunk „A munkacsoport számítógépeinek megjelenítése” feliratra. A kiszolgálónak meg kell jelenni az ablakban (62.ábra) Azt megnyitva látjuk a három megosztást: inst, oktat, tanulo.



62. ábra

A tanulo megosztás valójában nem létezik, mivel a kiszolgálón a nincs /home/tanulo könyvtár. A felhasználó létrehozásánál a useradd parancsot -M paraméterrel futtattuk, ami megakadályozza a felhasználói home könyvtár létrejöttét. Ha létrehoztuk volna, a tanulók nagyon egyszerűen cserélhetnének állományokat egymás közt, ami például egy zárthelyi dolgozat eredményének objektivitását megkérdőjelezné.

A tanulo megosztás megnyitásakor hibaüzenetet kapunk és a Samba is bejegyzést készít a /var/log/messages állományba:

```
Jan 11 01:38:16 server smbd[3905]: '/home/tanulo/Dokumentumok' does not exist or is not a directory, when connecting to [tanulo]
```

Hogy ezt elkerüljük, létrehozhatjuk a könyvtárat, és olyan jogosultságot állítunk be rajta, hogy a tanulók ne tudják megnyitni. A másik megoldás, hogy szerkesszük az /etc/passwd állományt, ugyanis a Samba ebből következtet a könyvtárra. A következő sort:

```
tanulo:x:540:540:Tanulo Felhasznalo:/home/tanulo:/bin/false
```

módosítsuk az alábbira:

```
tanulo:x:540:540:Tanulo Felhasznalo::/bin/false
```

Legyünk igen körültekintőek! A Linux felhasználói adatbázisát módosítjuk! A Samba újraindítása után nem látunk tanulo nevű megosztást.

Visszatérve a Windows 98-ra, a tanulo felhasználó ott is hasznos lehet, amikor olyan csoportnak kell a hálózat szolgáltatásait bemutatni, akiknek nincs felhasználói nevük. Az oktat és az inst megosztást használhatják, de home könyvtárt nem kapnak.

Ahhoz, hogy Windows XP-n (vagy 2000-n) bejelentkezett felhasználó hozzáférjen a saját HOME könyvtárához, és az megjelenjen mint **P:** meghajtó, két módszert is javasolok.

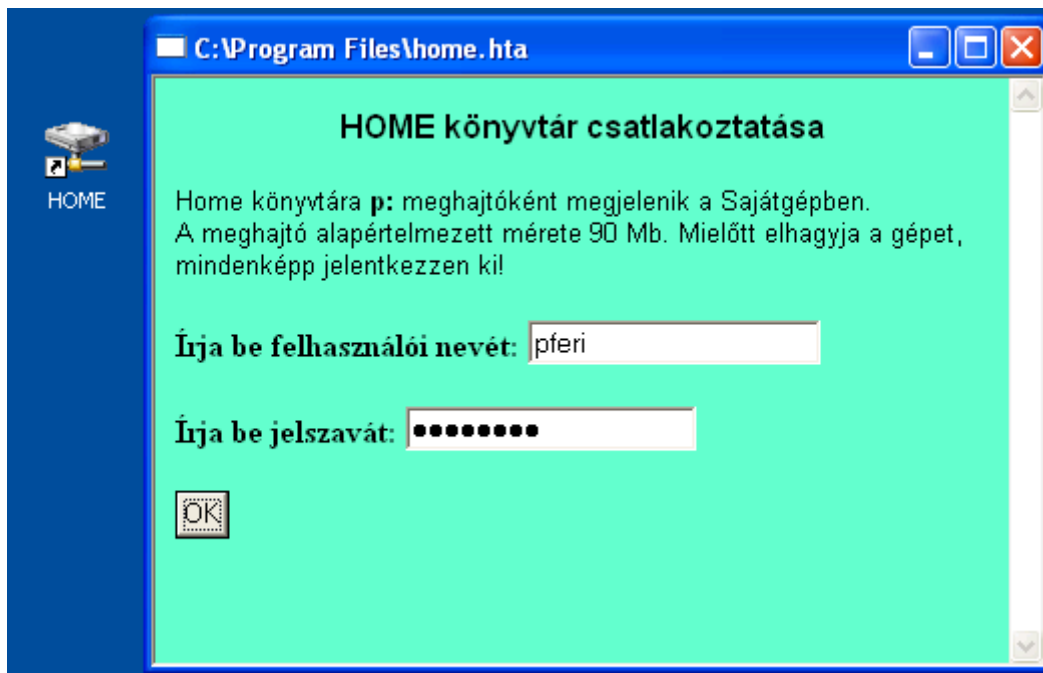
Az első a **home.hta** nevű program, ami megtalálható a serverhez1.zip csomagban.

A programban szerepel a kiszolgáló neve, ha másik nevet adtunk, akkor keressük meg a **server44** kifejezést a programban, és írjuk át az általunk választott névre.

Rendszergazdaként másoljuk a munkaállomásra, például a Program Files könyvtárba. Készítsünk róla parancsikont az asztalra, majd azt helyezzük át a C:\Documents and Settings\All Users\Asztal könyvtárba. Így minden felhasználó asztalán meg fog jelenni. Válasszunk olyan ikont a parancsikonnak, amiből következtetni lehet a jellegére. Állítsuk be a jogosultságokat, hogy tanulo felhasználó ne törölhesse. Nevezzük át HOME-ra.

Elindítva a parancsikont a megjelenő ablakba beírhatjuk felhasználói nevünket és jelszavunkat. (63. ábra) A jelszó beírásakor a karakterek szimbólummal helyettesítődnek. A mezők között egérrel vagy a TAB billentyűvel válthatunk. Az OK gombra kattintva, vagy a TAB-al kiválasztva és az Enter billentyűt leütve létrejön a **P:** meghajtó és a Windows intéző ablaka is megnyílik a **P:** meghajtó tartalmával.

A módszer hibájaként meg kell említeni, hogy ha huzamosabb ideig dolgozunk tanulo felhasználóként a gépen, és ezután próbáljuk a **P:** meghajtót csatlakoztatni, a kapcsolat nem épül fel, hibaüzenetet kapunk. Kijelentkezve és ismét bejelentkezve már használhatjuk a HOME könyvtárat. Ez a kellemetlenség elkerülhető, ha létrehozunk egy parancsikont a home.hta-ról az indítópultban, ami automatikusan elindítja a programot bejelentkezéskor, figyelmeztetve a felhasználót, hogy a HOME könyvtár használatához be kell jelentkeznie.



63. ábra

A **home.hta** nevű program (a net use parancsot tartalmazó sor egysoros)

```
<html>

<head>
<body onload="window.resizeTo(455,330)">
<meta http-equiv="Content-Language"
content="hu">
<meta name="ProgId"
content="FrontPage.Editor.Document">
<title></title>
</head>

<script language="VBScript">
    <!--
        Sub OKButton_OnClick
            driveletter = "Z:"
            name = UserNameBox.value
            name = Trim(name)
            pswd = PasswordBox.value
            pswd = Trim(pswd)
            UserNameBox.value = ""
            PasswordBox.value = ""
            Set WshShell = CreateObject("Wscript.Shell")
            WshShell.Run "net use p: \\server44\homes /PERSISTENT:NO
" & pswd & " /user:" & name,,True
            WshShell.Run "explorer p:"
        End Sub

    '--->
</script>
<body bgcolor="#66FFCC">

<p></p>
<p align="center"> <font face="Arial">
<b>HOME könyvtár csatlakoztatása</b></font></p>
<p align="left" style="margin-top: 0; margin-bottom: 0">
```

```

<font face="Arial" size="2">Home könyvtára <b>p:</b> meghajtóként
megjelenik a Sajátgépben. </font>
</p> <p align="left" style="margin-top: 0; margin-bottom: 0"> <font
face="Arial"
size="2"> A meghajtó alapértelmezett mérete 90 Mb. Mielőtt elhagyja a
gépet, mindenképp jelentkezzen ki!</font></p>
<p><b>Írja be felhasználói nevét: </b>
<input TYPE="text" Name="UserNameBox" size="20"> </p>
<p><b>Írja be jelszavát: </b>
<input TYPE="password" Name="PasswordBox" size="20"> </p><p>
<input NAME="OKButton" TYPE="BUTTON" VALUE="OK"> </p><p></p>
</body>
</body>
</html>

```

Ismételten elindítva programot hiába írunk másik felhasználói nevet és jelszót, a **P:** meghajtó az első bejelentkezett felhasználó home könyvtárát mutatja. Kijelentkezéskor a kapcsolat megszakad, tanuló-ként újra bejelentkezve, nincs hálózati meghajtó csatlakoztatva. A felhasználókat figyelmeztessük, hogy munkájuk végeztével jelentkezzenek ki, vagy kapcsolják ki gépet, hogy a személyes adataikhoz más ne férhessen hozzá.

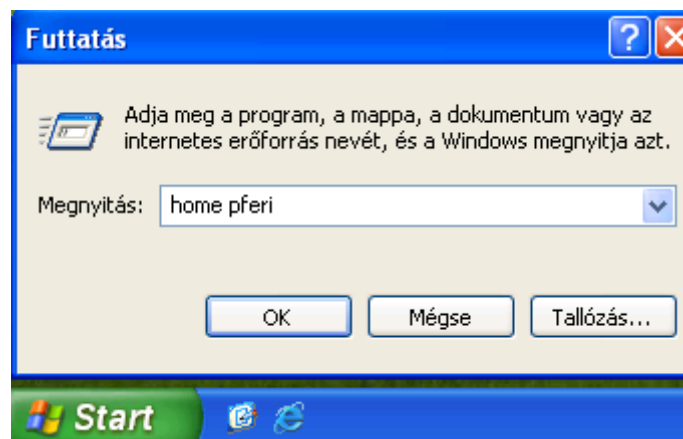
A második módszer az elsőnél egyszerűbb. Rendszergazdaként bejelentkezve a Windows könyvtárban hozzunk létre egy **home.cmd** állományt a következő tartalommal:

```

net use p: /user:%1 \\server44\homes /PERSISTENT:NO
explorer p:

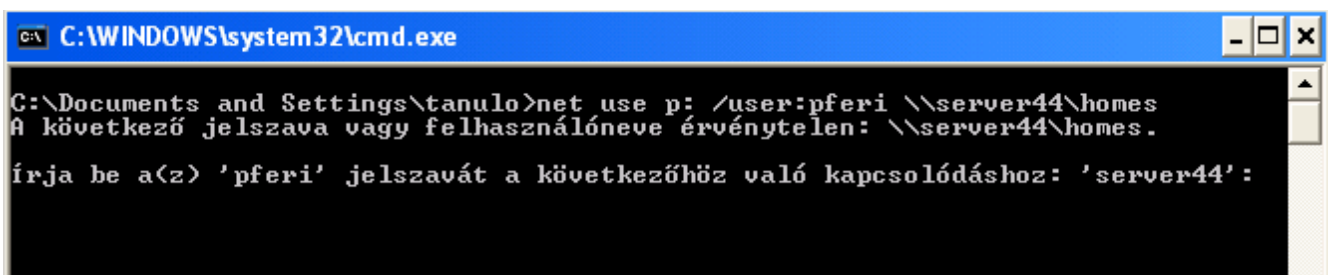
```

A HOME könyvtár csatlakoztatásához a Start / Futtatás ablakba írjuk be a home parancsot és a saját felhasználói nevünket szóközzel elválasztva. (64. ábra)



64. ábra

Megnyílik a Parancssor ablak, ahová a saját jelszavunkat kell beírni. (65. ábra) A jelszó nem jelenik meg az ablakban.



65. ábra

A **tanaroknak** és az **adminhome** megosztást ugyanúgy csatlakoztathatjuk, mint Windows 98 esetén. Az első esetben hozzuk létre **Tanar.bat** állományt ugyanazzal a tartalommal:

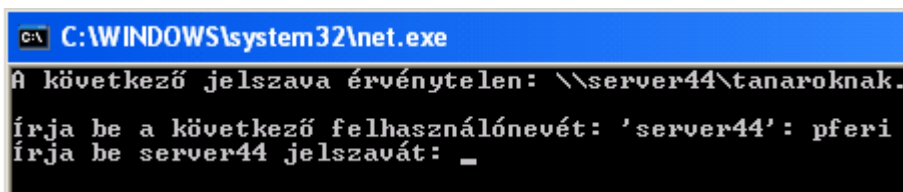
```
net use n: \\server44\tanaroknak
```

Készítsünk egy parancsikont az asztalra a fájlról, nevezzük át pl. „Közös tanároknak”-ra.

Az **adminhome** megosztás eléréséhez az admin.bat állomány tartalma:

```
net use x: \\server44\adminhome
```

Mindkét megosztás felhasználói név és jelszó beírása nélkül használható, ha előzőleg valamelyik módszerrel bejelentkeztünk a HOME könyvtárunkba. Ha nem jelentkeztünk be, és úgy indítjuk el a Tanar.bat állományt, a megjelenő ablakba kell beírni felhasználói nevünket és jelszavunkat. (66. ábra)



66. ábra

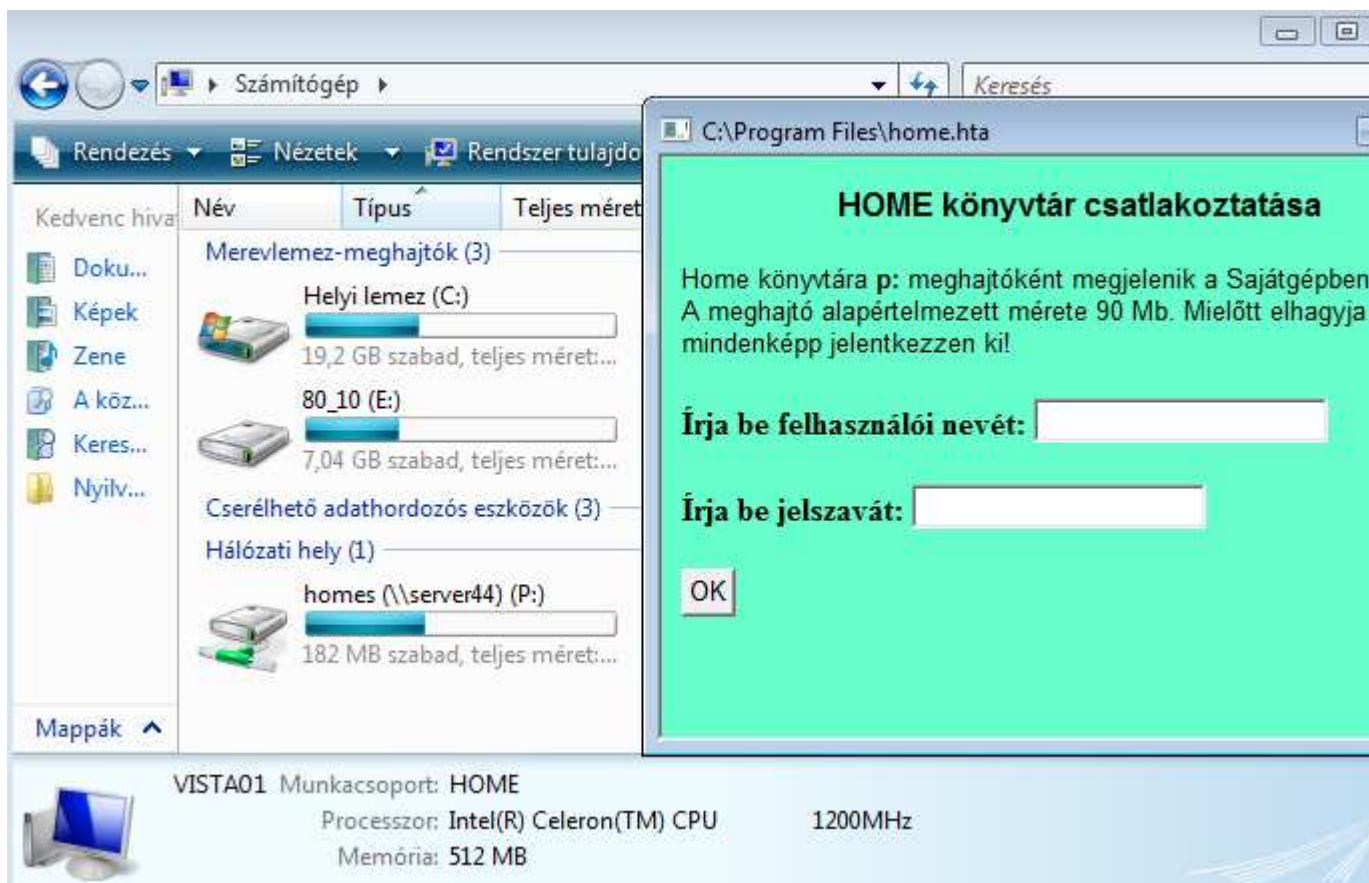
Készítsünk parancsikont az asztalra az **oktat** megosztásról. Nevezzük át a parancsikont oktatásra, ékezet nélkül. Helyezzük át a C:\Documents and Settings\All Users\Asztal könyvtárba. Állítsuk be a jogosultságokat, hogy tanuló felhasználó ne törölhesse.

Hozzuk létre a C:\Documents and Settings\All Users\Start Menu\Programs\Indítópult könyvtárban a boot.bat állományt a következő tartalommal:

```
net time \\server44 /set /yes  
NET USE P: /delete /yes  
NET USE N: /delete /yes  
NET USE X: /delete /yes  
NET USE M: /delete /yes
```

A kötegfájl minden bejelentkezésnél lefut és szinkronizálja a munkaállomás óráját a kiszolgálóéhoz. Ezen kívül bontja az esetleg fennálló kapcsolatokat a kiszolgálóval.

A Microsoft Vista operációs rendszert az XP-hez hasonlóan állíthatjuk be. A HOME könyvtár felcsatolására a home.hta programot a Vista-n is használhatjuk. Viszont ennél az operációs rendszernél az All Users mappa listázása alapértelmezés szerint a rendszergazdának sem engedélyezett. Módosítsuk az engedélyeket, majd a fent tárgyalt állományok, parancsikonok másolása és létrehozása után állítsuk vissza. Amennyiben olyan Vista verziónk van, amelyik támogatja a kapcsolat nélküli fájlok használatát, akkor a Vezérlőpultban ezt a szolgáltatást tiltsuk le. A 67. ábrán a **P:** meghajtóként felcsatolt HOME könyvtárat látjuk.



67. ábra

Oktatási anyagok használata a kiszolgálón

A kiszolgálón elhelyezhetünk oktatási és ismeretterjesztő anyagokat, ami minden munkaállomásról elérhető lesz. Az Interneten sok szabadon használható oktatási anyagot találhatunk különböző témakörökben.

A <http://www.szoftverbazis.hu/szoftver/manomatek-4-magyar--ZC7.html> oldalról letölthető „Manómatek 4” program példáján mutatom be a rendszer működését.

Vázlatosan a rendszer a következőképpen működik:

1. Létrehozunk egy alkönyvtárat a kiszolgáló /**oktat** könyvtárában
2. Ebbe a könyvtárba másoljuk a programot
3. Az **smb.conf** állományban egy megosztást hozunk létre erre a könyvtárra
4. Készítünk egy kötegfájlt, amit elhelyezünk a már megosztott és minden munkaállomás asztaláról elérhető /**oktat/oktatási_anyagok** könyvtárban
5. A kötegfájl leválasztja az esetleg létező **M:** meghajtót, (ha előtte egy másik oktatóanyagot használtunk) **M:** meghajtóként csatlakoztatja az új megosztást a munkaállomáshoz és elindítja az oktatási anyagot.

Ennek a módszernek az az előnye, hogy az oktatási anyag közzétételéhez nem kell semmit sem módosítani a munkaállomásokon.

Letöltjük a zip állományt, kitömörítjük és felmásoljuk a kiszolgálóra (68. ábra)

< /oktat/manomatek4_demo >		
Name	Size	MTime
/..	UP--DIR	
/Xtras	4096	Jan 10 18:52
/manomatek4_demo	4096	Jan 10 18:52
Olvasz.el	1357	Sep 18 2002
id.txt	32	Jun 25 2003
lingo.ini	83	Jun 25 2003
programkalauz.bmp	1440054	May 9 2003
programkalauz.rtf	9462	May 30 2003
start.bmp	1440054	May 30 2003
start.exe	71579	Apr 24 2003
start.ini	70	May 22 2003

68. ábra

Az smb.conf állományt bővítjük a következő sorokkal:

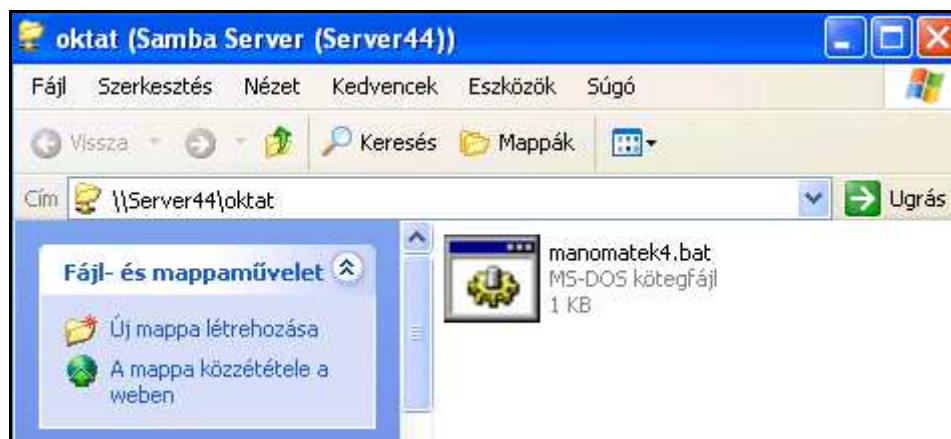
```
[manomatek4]
comment = Manomatek 4
path = /oktat/manomatek4_demo
public = yes
writable = no
printable = no
browseable = no
```

Az /oktat/oktatási_anyagok könyvtárba létrehozuk a **manomatek4.bat** állományt:

```
net use m: /delete /yes
net use m: \\server44\manomatek4
m:
start.exe
```

Az állományt a Windows-on hozzuk létre, és WinSCP-vel, vagy a P: meghajtó segítségével másoljuk a szerverre, hogy sorvégi karakterek megfelelőek legyenek.

Megnyitva az **oktat** parancsikont az asztalon, látjuk a kötegfájlt (69. ábra). Elindítva létrejön az M: meghajtó, és elindul a program.



69. ábra

Nemcsak programokhoz használhatjuk, hanem minden esetben, amikor könnyen elérhetővé kell tenni dokumentumokat, képeket, prezentációkat vagy akár oktatófilmeket. Ebben az esetben a bat állomány csak két soros: leválasztja az esetleg létező **M:** meghajtót és a megfelelő megosztást felcsatolja **M:** meghajtóként. A felhasználók a meghajtó tartalmát a munkaállomásokról nem módosíthatják.

Zárthelyi dolgozatok begyűjtése program segítségével

Informatika órákon gyakran problémát okoz, hogy a tanulók által készített munkákat nem egyszerű összegyűjteni a tanároknak. A HOME könyvtár segítségével az megoldott, hogy a tanulók nem cserélhetnek állományokat egymással. A következő rövid program segítségével a tanár másolatot készíthet az adott osztály tanulóinak munkáiról. A program lefuttatása után a tanulók már hiába módosítják munkáikat, a javítandó másolatok már a tanár könyvtárában vannak.

A program működéséhez nincs szükség root jogosultságra. A tanárok közül bárki használhatja, akinek belépési jogot biztosítottunk a kiszolgálóra.

A **dolgozat.scip** program:

```
#!/bin/bash
clear
TANAR=pferi
DATE=`date +%Y_%b_%d`
echo "A tanulok onallo munkainak masolasa"
echo "Irja be az osztaly csoportazonositojat"
echo
read CSOPORT
if test -s /etc/squid/csoportok/"$CSOPORT".txt
then
echo "Ennek az osztalynak tanuloi"
for i in `cat /etc/squid/csoportok/"$CSOPORT".txt`
do
cat /etc/passwd | echo -n " " `grep -w $i | cut -d":" -f5 `
done
echo
echo ?
read B
if test $B = "y"
then
mkdir /home/$TANAR/Dokumentumok/dolgozat_"$DATE_"_"$CSOPORT"
echo "Ird be a könyvtár nevét amit a tanulók létrehoztak:"
read DIR
for j in `cat /etc/squid/csoportok/"$CSOPORT".txt`
do
NEV=`cat /etc/passwd | grep -w $j | cut -d":" -f5 `
mkdir /home/$TANAR/Dokumentumok/dolgozat_"$DATE_"_"$CSOPORT"/"$NEV"
cp -R /home/"$j"/Dokumentumok/"$DIR"/*
/home/$TANAR/Dokumentumok/dolgozat_"$DATE_"_"$CSOPORT"/"$NEV"
done
fi
exit 0
else
echo "nincs ilyen csoport!"
fi
```

A programot másoljuk a home könyvtárunkba, és azoknak a tanároknak a home könyvtárába, akiknek adtunk belépési jogot a kiszolgálóra. A harmadik sorban változtassuk meg a felhasználói nevet. A program futtatásához a **./dolgozat.scip** parancsot kell kiadni, és beírni az osztály csoportazonosítóját. A képernyőn megjelenő osztálynévsor alapján leellenőrizhetjük, hogy megfelelő osztályt választottunk. Ezután be kell írni annak a könyvtárnak a nevét, amit a tanulók létrehoztak a **P:** meghajtón a dolgozat megírásához, és amelyikbe mentették dokumentumaikat. A dolgozat megírása előtt a tanulóknak létre kell hozni ezt a könyvtárat. Fontos, hogy e könyvtár neve pontosan megegyezzen az általunk megadottal (kis- és nagybetű és egy szóköz is számít).

A program ellenőrzéséhez a g2002a csoport felhasználói neveivel bejelentkeztem különböző munkaállomásokra és a **P:** meghajtón létrehoztam a 070115 könyvtárat. Ebbe a könyvtárba

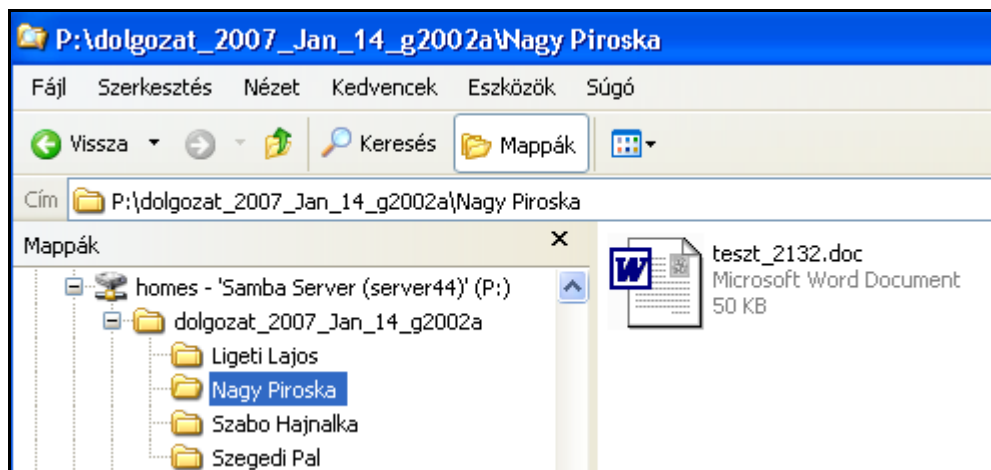
elmentettem egy vagy több dokumentumot minden munkaállomáson. Felhasználói azonosítóval bejelentkezve a kiszolgálóra (a PuTTY segítségével) lefuttattam a programot. A következő néhány sorban látjuk a program működését. A félkövérrel kiemelt sorokat be kell írni.

```
[pferi@server ~]$ ./dolgozat.scp

A tanulok onallo munkainak masolasa
Irja be az osztaly csoportazonositojat

g2002a
Ennek az osztalynak tanuloi
  Szabo Hajnalka  Szegedi Pal  Ligeti Lajos  Nagy Piroska
?
y
Irja be a könyvtár nevét, amit a tanulók létrehoztak:
070115
[pferi@server ~]$
```

A 70. ábrán látjuk, hogy a **P:** meghajtón létrejött egy mappa, amelynek nevében szerepel az aktuális dátum és a csoportazonosító. Ebben minden tanulónak van könyvtára, benne az átmásolt dokumentumokkal.



70. ábra

X. A Linux mint munkaállomás

Telepítés

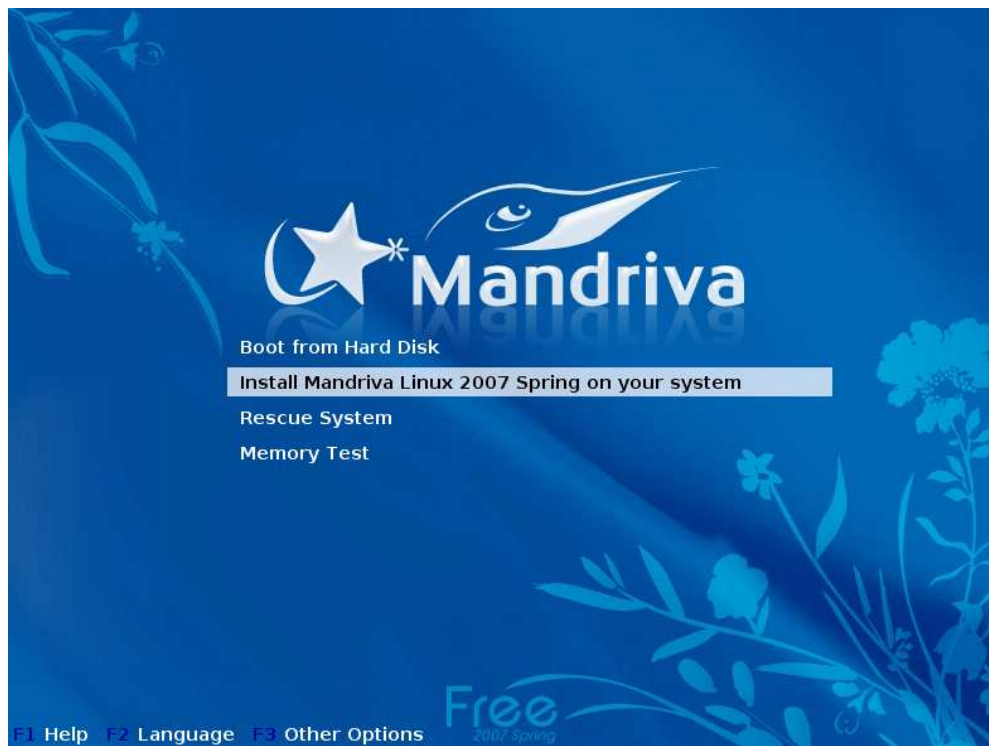
A bevezetőben már említettem, hogy Linux operációs rendszeren munkaállomást is kialakíthatunk. Ebben a fejezetben a Mandriva Linux 2007 Spring operációs rendszer telepítését és néhány beállítását tekintjük át.

A Linux operációs rendszert a Windows mellé is telepíthetjük, ilyenkor a számítógép bekapcsolásakor választhatunk, hogy melyik rendszer induljon el.

A Mandriva Linux weboldalán (www.mandriva.com) nézzük meg az operációs rendszer hardverigényét (<http://www.mandriva.com/en/linux/>). Láthatjuk, hogy a legújabb változat telepítéséhez legalább 512Mb RAM szükséges. Ha nem rendelkezünk ilyen számítógéppel, használhatjuk a Mandriva Linux 2007 Spring-et, ami 256 Mb-al is használható. Ezt az ISO állományt letölthetjük a Mandriva tükrök valamelyikéről, például a következő:

<http://mandriva.mirror.dkm.cz/pub/mandriva/official/iso/2007.1/mandriva-linux-2007-spring-free-dvd-i586.iso>. Mivel DVD-méretű képfájlról van szó, lassú Internet kapcsolaton a letöltés több napig is tarthat.¹

A telepítéshez szükség lesz egy DVD olvasóra is, de azt, természetesen telepítés után kisserelhetjük a munkaállomásból. A boot-olás után a következő kép fogad minket: (71. ábra)



71. ábra

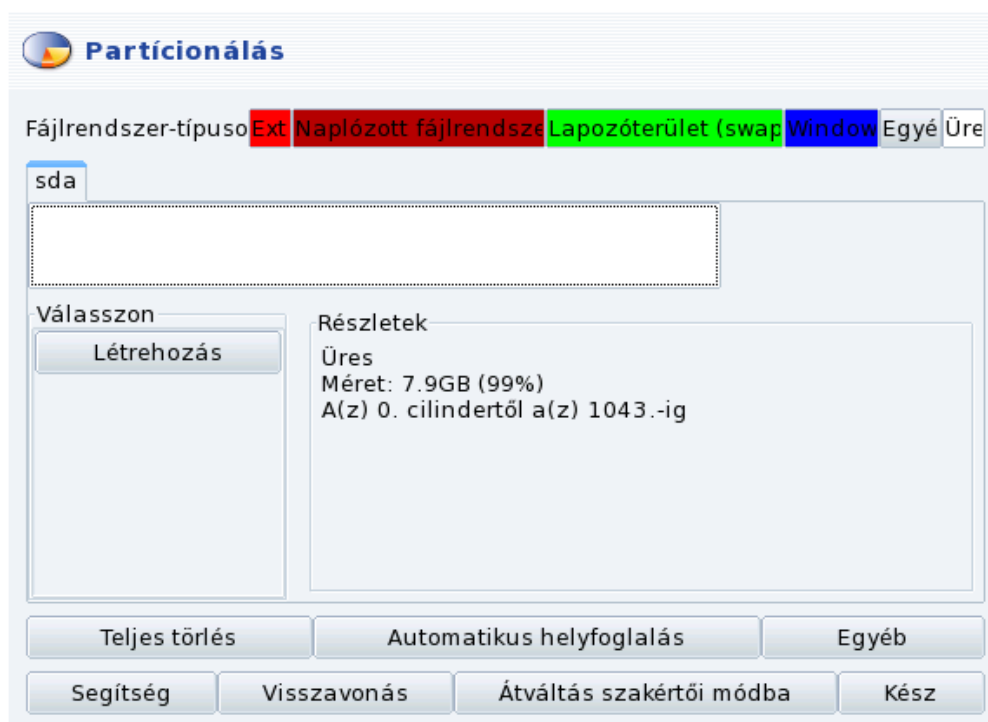
Itt válasszuk a képen látható második sort és üssük le az Enter-t. A következő ablakban az operációs rendszer nyelvét adhatjuk meg, magyart válasszunk. A licencegyezmény elfogadás után a Biztonság ablak fogad minket (72. ábra), válasszuk a Szabványos szintet.

¹ E-mail-en történő egyeztetés után nagyon szívesen felírom bárkinek a DVD-t.



72. ábra

A partícionálás ablakban válasszunk az egyéni lemezpartícionálást. A 73. ábrán egy 8 Gb-os üres SATA merevlemez látunk. Párhuzamos ATA csatolású merevlemez esetén az eszköz neve hda lenne. A kényelmes használathoz körülbelül ekkora helyre van szükség, hiszen a telepítő lemez több 100 különböző alkalmazást is tartalmaz.



73. ábra

Kattintsunk egérrel a Létrehozás gombra és hozzunk létre 5,7 Gb-os, ext3 típusú fájlrendszert. Csatolási pont a / legyen (74. ábra).



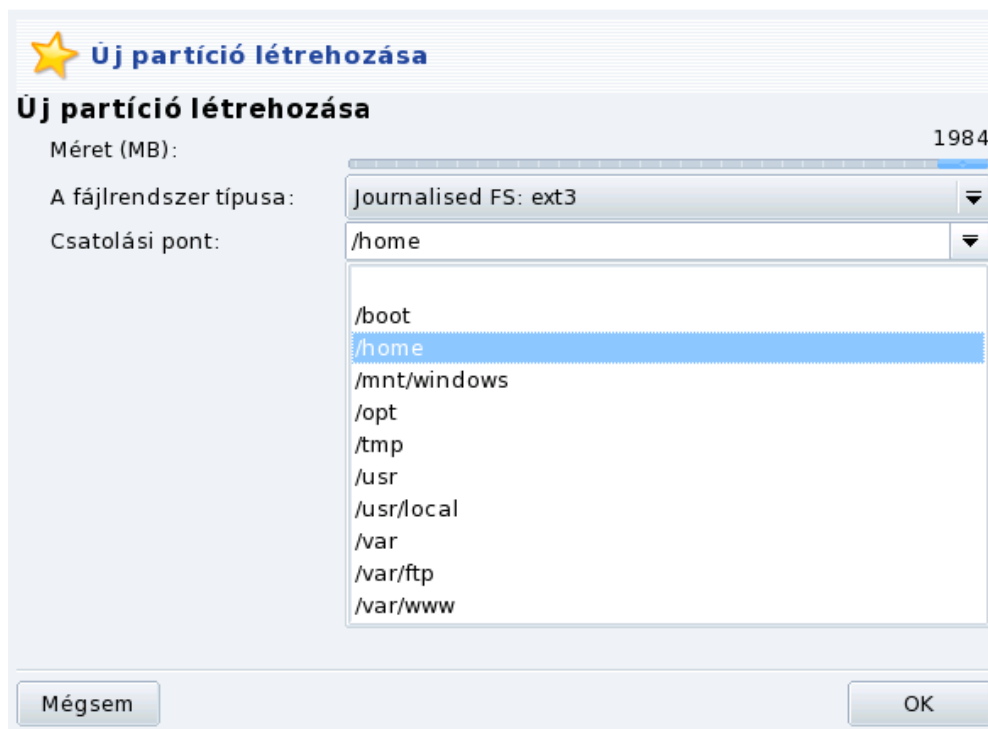
74. ábra

Ezután ismételten a szabad helyre kattintva hozzunk létre egy 512 Mb-os lemezrész. Ennek típusa Linux swap legyen.



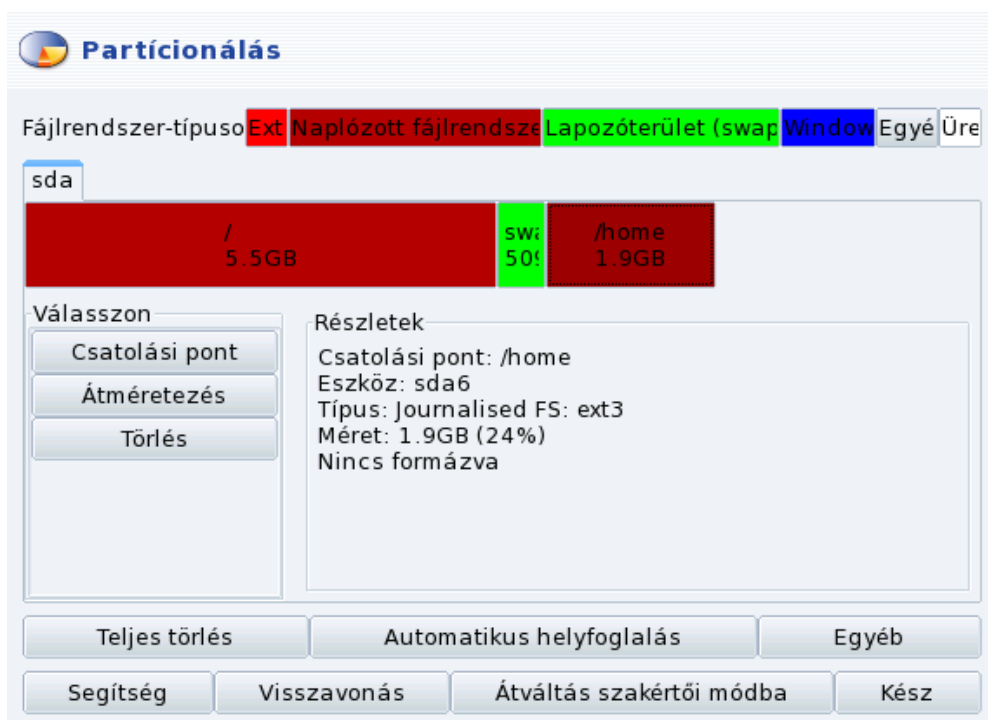
75. ábra

A fennmaradó teljes szabad helyen /home csatolási ponttal, ext3 típusú fájlrendszer legyen (76. ábra). Nagyobb merevlemez, vagy üres lemezrész esetén a fentieknél nagyobb lemezrészeket is létrehozhatunk.



76. ábra

Figyeljük meg a létrehozott lemezrészeket (77. ábra) és kattintsunk a Kész feliratú gombra.



77. ábra

A csomag-csoportok kiválasztása következik (78. ábra). Itt kapcsoljuk be a csomagok egyedi kiválasztását.



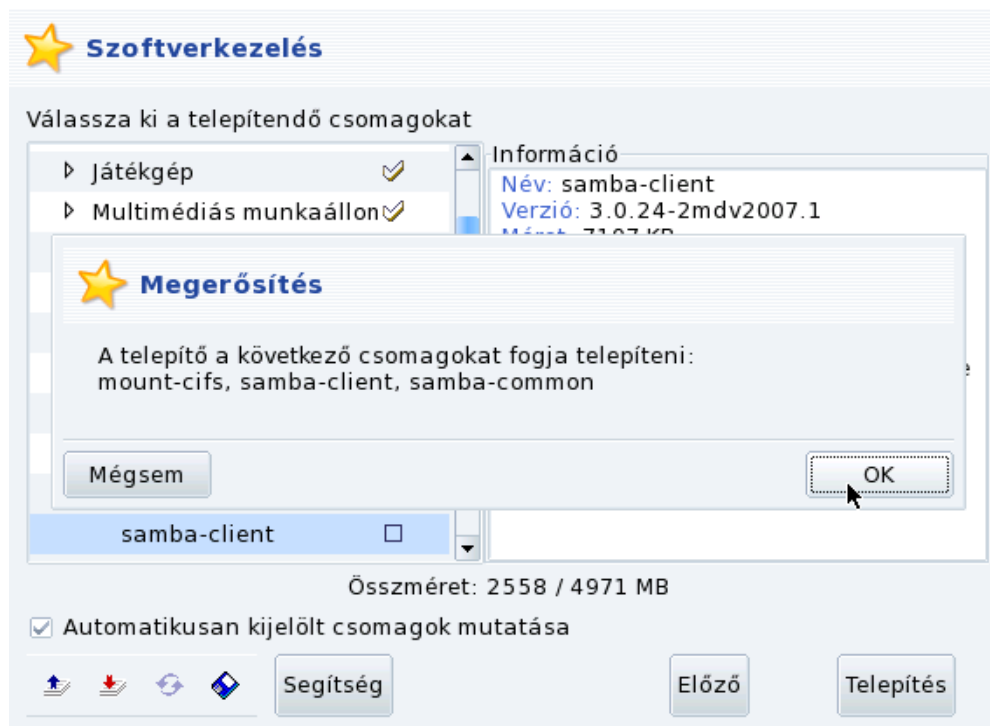
78. ábra

A Szoftverkezelés ablakban jelöljük be az openssh-server nevű csomagot (79. ábra), aminek a segítségével távolról is adminisztrálhatjuk a munkaállomást.



79. ábra

A Munkaállomás / Hálózati számítógép (kliens) kategóriában jelöljük be a samba-client csomagot is, ami lehetővé teszi hogy a Samba kiszolgálóhoz csatlakozzunk. A csomaghoz a samba-common és a mount-cifs csomagokat is telepíteni kell, a megerősítés ablakban kattintsunk az OK gombra.



80. ábra

A következő ablak figyelmeztet minket, hogy két kiszolgáló szolgáltatást választottunk: az előbb kiválasztott openssh-server-t és cups-ot, ami a nyomtatást teszi lehetővé a munkaállomáson. Olvassuk el az ablak szövegét és indulhat a telepítés. Ez a számítógép teljesítményétől függően kb. 20 perc alatt lezajlik.

Ezután a root jelszó megadása következik. A kiszolgálónál említett szabályok szerint válasszuk ki a jelszót, de semmiképp se legyen azonos a szerverünk root jelszavával! A következő ablakban hozzuk létre a saját azonosítónkat (81. ábra) és a tanuló felhasználót (82. ábra). A tanuló felhasználó jelszava egyezzen meg a kiszolgálón és a Windows XP-n létrehozottal. Ez nem titkos, minden tanuló ezzel a felhasználói névvel lép majd be a munkaállomásra. Tehát a Linux-ra ugyanúgy kell bejelentkezni a felhasználóknak, mint a Windows XP-re. Ez vegyes környezetben mindenképp szerencsés, és ezzel a módszerrel a munkaállomásokat akkor is használhatjuk, ha kiszolgáló vagy a hálózat nem működőképes.

Felhasználó felvétele

Adjon meg egy felhasználónevet

Valódi név: Pallay Ferenc

Bejelentkezési név: pferi

Jelszó: *****

Jelszó (még egyszer): *****

▸ Speciális

Segítség Név elfogadása Következő

81. ábra

Felhasználó felvétele

Adjon meg egy felhasználónevet
(már fel van véve: Pallay Ferenc)

Valódi név: tanulo

Bejelentkezési név: tanulo

Jelszó: *****

Jelszó (még egyszer): *****

▸ Speciális

Segítség Név elfogadása Következő

82. ábra

A következő ablakban beállíthatjuk, hogy rendszerindításkor egy felhasználó automatikusan bejelentkezzen. Esetünkben nincs szükség erre a lehetőségre. Ezután a rendszerindító program helyét adhatjuk meg. Ez legyen a lemezmeghajtó legelső sektora (MRB).

Válasszuk ki a monitorunk típusát és elérkeztünk az összefoglalás ablakhoz (83. ábra), ahol egy néhány beállítást el kell végezni.



83. ábra

Állítsuk be a hálózati eszközt (84. ábra). Az IP cím és a gépnév minden munkaállomáson különböző legyen.



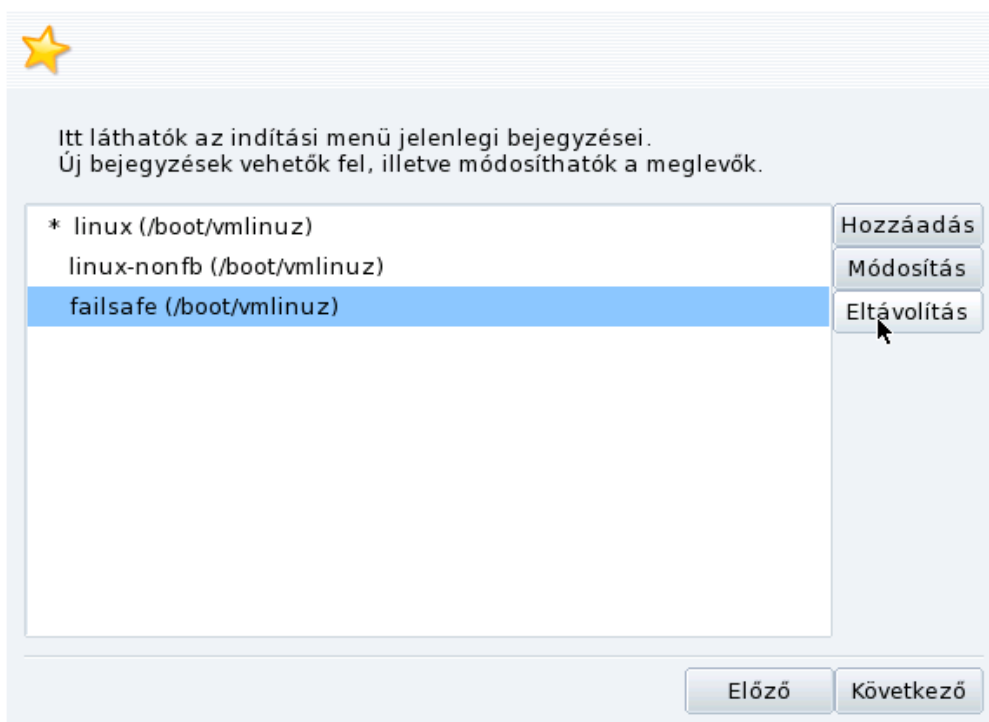
84. ábra

A tűzfal beállításait a 85. ábra mutatja. A képen látható beállításokkal bejelentkezhethünk a munkaállomásra az SSH-kiszolgáló segítségével és a ping-re is válaszolni fog.



85. ábra

A Rendszerindítási beállítások második ablakában az indítási menüből töröljük a *failsafe* sort, mivel ezzel jelszó beírása nélkül is rendszergazdai jogokhoz jutna a felhasználó. Kattintsunk a *failsafe* szót tartalmazó sorra és az eltávolítás gombra (86. ábra).

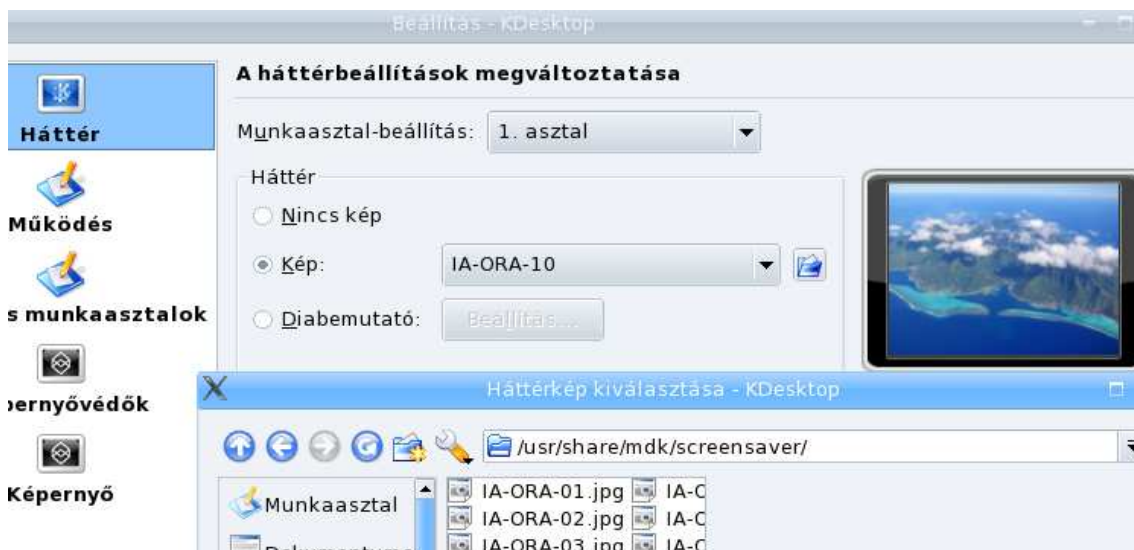


86. ábra

Ezzel a beállításokat befejeztük. A következő Frissítések c. ablakban az alapértelmezett beállítást nem módosítjuk, a rendszer frissítéseit később töltjük le. Ezzel a telepítés véget ért, vegyük ki a DVD-t a meghajtóból, olvassuk el az utolsó ablak szövegét és válasszuk az Újraindítás-t.

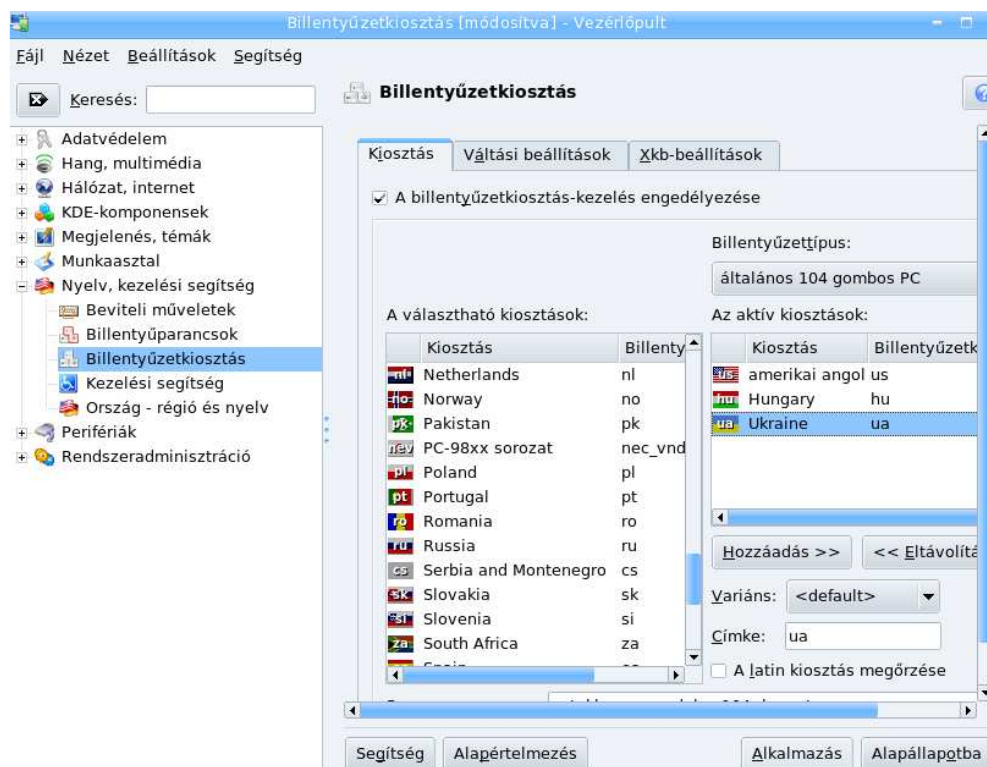
Néhány beállítás a munkaállomáson

Az első indításnál felbukkanó varázslót hagyjuk ki. Jelentkezzünk be a munkaállomásra tanuló felhasználói névvel. A KDE asztalon kattintsunk jobb egérgombbal és válasszuk a Munkaasztal beállítását. Itt a munkaasztalok számát csökkentjük 2-re. A munkaasztalokra válasszunk különböző háttérképeket. (87. ábra, az /usr/share/mdk/screensaver könyvtárban is találunk képeket) Az asztali ikonok elrendezése legyen rácsponthoz igazítva.



87. ábra

Indítsuk el a Vezérlőpult programot (Rendszer / Beállítás / Vezérlőpult). Itt engedélyezzük a billentyűzetkiosztás-kezelést és adjuk hozzá az aktív kiosztásokhoz a magyart és az ukránt. (88. ábra)



88. ábra

Csökkentsük az ikonok méretét 48 pontról 32-re (Megjelenés, témák / Ikonok / Speciális). A panelek méretét állítsuk kicsire (Munkaasztal / Panelek / Elrendezés). Az asztalról töröljük le a Subscribe, Buy it és az Üdvözljük linkeket.

Indítsuk el a Számítógép beállítása programot: Rendszer / Beállítás / A számítógép beállítása. A megjelenő ablakban meg kell adnunk a root jelszót. A Hálózat és Internet csoportban a Proxykiszolgáló beállításainál adjuk meg a kiszolgálónk adatait. (89. ábra)



89. ábra

Indítsuk el a Mozilla Firefox böngészőprogramot és ellenőrizzük a kapcsolat beállításainál a proxy-ra vonatkozó sorokat és az Internet működését. A webhelyjelszavak mentését kapcsoljuk ki és módosítsuk a kezdőlapot.

A Konsole programban (Rendszer / Terminálok / Konsole) kérjünk root jogosultságot, és indítsuk el az mc programot:

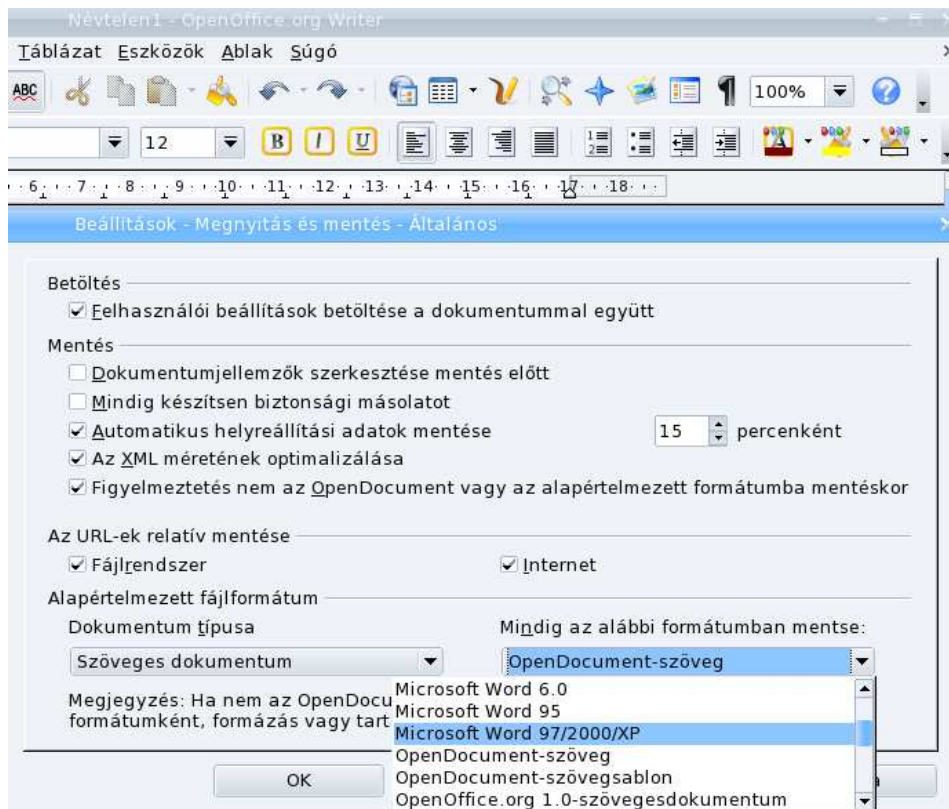
```
[tanulo@localhost ~]$ su -
Jelszó:
[tanulo@localhost ~]# mc
```

Az /etc/hosts állományt módosítsuk a következőre:

```
127.0.0.1      localhost
192.168.0.11  suliserver
```

A munkaállomáson az alapértelmezett telepítéssel is nagyon sok programot találunk. Az OpenOffice.org programcsomagban megtaláljuk a szövegszerkesztőt, táblázatkezelőt, prezentációkészítőt, adatbázis-kezelőt, mint a Microsoft Office-ban. Az OpenOffice-ben állítsuk be, hogy alapértelmezett formátum Microsoft Office formátuma legyen, így a mentésnél a legelterjedtebb fájlformátum lesz az alapértelmezett (90. ábra).

Terjedelmi okok miatt különböző programok telepítését nem mutatom be, a howtoforge.com portálon részletes leírást olvashatunk erről angol nyelven. A cikk címe:
http://www.howtoforge.com/the_perfect_desktop_mandriva_2007_spring_free



90. ábra

Kapcsolódás a fájlserverhez

Telepítésnél feltelepítettük a samba-client csomagot is, ezzel kapcsolódhatnak a felhasználóink a kiszolgálón található HOME könyvtárukhoz. A home.scp nevű rövid scriptet másoljuk a tanulo /home/tanulo könyvtárba. A scriptet megtaláljuk a serverhez1.zip állományban.

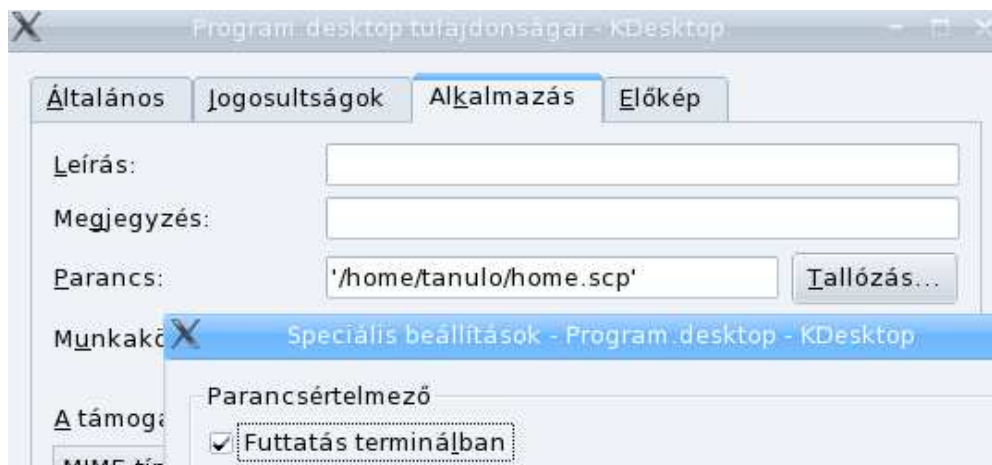
A home.scp script:

```
#!/bin/bash
echo "Home könyvtár csatlakoztatása"
echo "A fileszerveren található HOME könyvtára"
echo "elérhető lesz a Saját Könyvtár /home alkönyvtárában"
echo "a teljes elérési út: /home/tanulo/home"
echo "a számítógép elhagyása előtt mindenképp jelentkezzen ki!"
sleep 2
echo "Írja be felhasználói nevét:"
read UNEV
smbmount //server44/homes /home/tanulo/home -o username=$UNEV,ip=192.168.0.11
konqueror /home/tanulo/home
```

Hozzuk létre a /home/tanulo/home könyvtárat és a home.scp jogosultságait állítsuk be úgy, hogy a tanulo felhasználó ne törölhesse, de futtatni tudja:

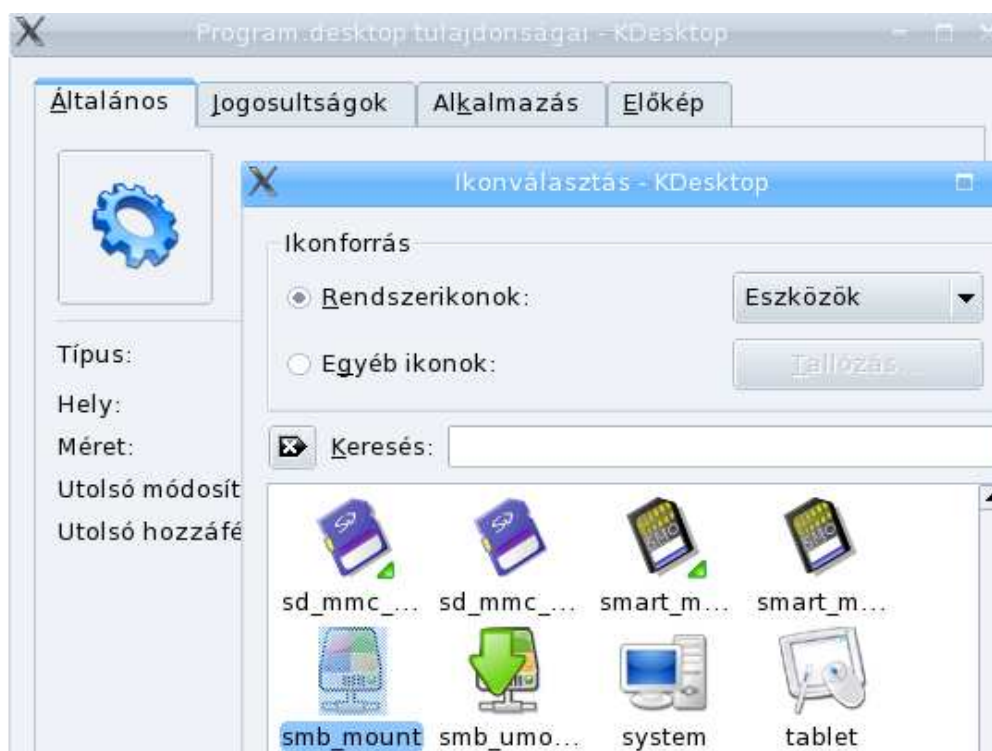
```
[root@m07 tanulo]# mkdir /home/tanulo/home
[root@m07 tanulo]# chown root:root ./home.scp
[root@m07 tanulo]# chmod 755 ./home.scp
[root@m07 tanulo]# ls -l ./home.scp
-rwxr-xr-x 1 root root 466 szept 23 00:23 ./home.scp*
```

Az asztalon hozzunk létre egy új asztalelemet: jobb egérgomb / Új elem létrehozása / Alkalmazásra mutató link... A neve legyen „HOME könyvtár”, a tallózás gombbal keressük ki a home.scp fájlt és a Speciális beállításoknál kapcsoljuk be a Futtatás terminálban ablakot.



91. ábra

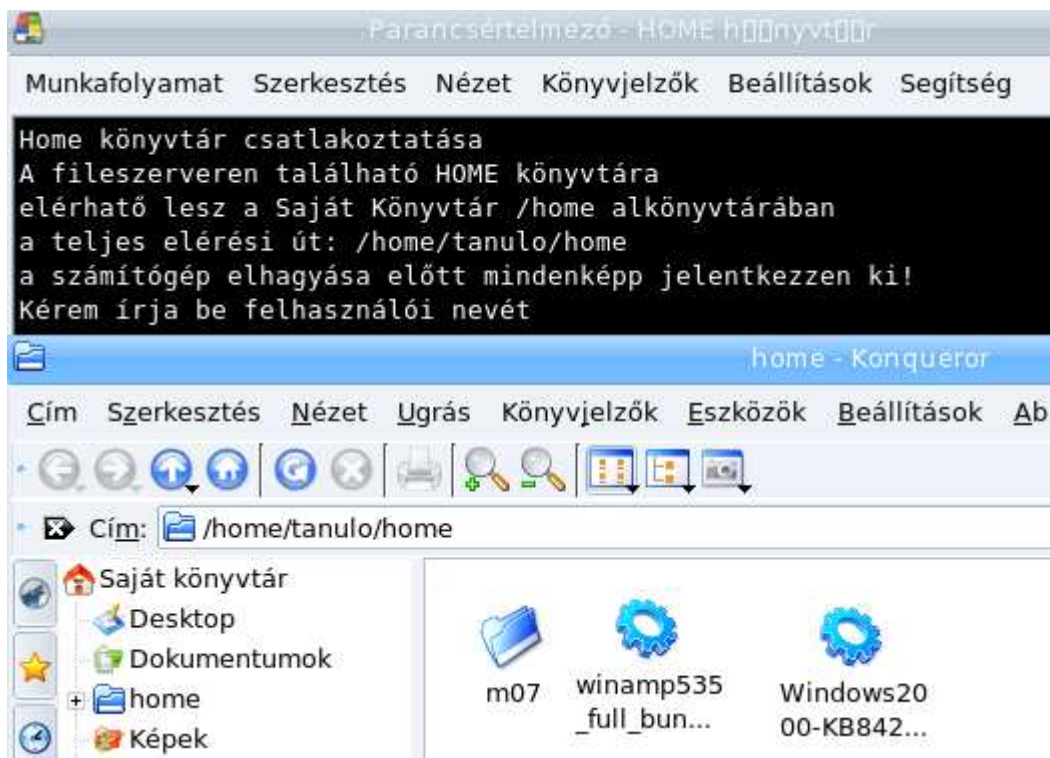
Az alapértelmezett ikonra kattintva az eszközök rendszerikon-csoportból válasszuk az smb_mount nevűt (92. ábra).



92. ábra

Elindítva megjelenik egy terminálablak, felhasználói nevünket és jelszavunkat megadva megnyílik a KDE fájlkezelője a Konqueror és benne a HOME könyvtárunk a kiszolgálóról (93. ábra). Kijelentkezéskor a kapcsolat megszakad a kiszolgálóval, de készíthetünk hasonlóképpen egy másik alkalmazásra mutató linket is, pl. „HOME-bont” néven, ami a következő kétsoros szkriptre mutat:

```
#!/bin/bash  
smbumount /home/tanulo/home
```



93. ábra

Állandó felhasználói környezet biztosítása

A tanuló felhasználó alapértelmezés szerint módosíthatja a saját felhasználói felületének beállításait. Ezt különböző jogosultságok módosításával korlátozhatjuk, de én egy ennél egyszerűbb módszert javaslok: készítsünk másolatot a beállított felhasználói fiókról (a /home/tanulo könyvtárról) a /root könyvtárba és azt a rendszer minden bekapcsolásakor másolja vissza a /home-ba. Kicsit drasztikus megoldásnak tűnik, de így a tanulók is szabadon módosíthatnak sok beállítást a Linux munkaállomáson, jobban megismerkedhetnek az operációs rendszerrel és a változatlan felhasználói környezet is biztosított. Rendszergazdaként egyszerűen módosíthatjuk az esetleges változásokat: csak felül kell írni a /root könyvtárban lévő tanulo könyvtárat a módosítottal.¹

A /tanulo könyvtárban lévő Dokumentumok, Képek, Letöltés és Videó könyvtárakat nem írjuk felül, ide menthetik el a tanulók az ideiglenes állományaikat. Ezeket újraindítás után is megtalálják a felhasználók. Tárhely korlátot, quota-t is lehetne alkalmazni, de mivel a /home könyvtár külön lemezzsre került nem feltétlenül szükséges beállítani.

Az mc programmal másoljuk a /tanulo könyvtárat és az /etc/shadow állományt a /root könyvtárba. A következő tanmasol.scp nevű szkriptet szintén a /root könyvtárba másoljuk és állítsunk be az x jogosultságot. A szkriptel megtaláljuk a serverhez1.zip állományban is.

A tanmasol.scp szkript:

```
#!/bin/bash
/usr/bin/mirrordir -i -F /root/nemmasol.txt /root/tanulo /home/tanulo
cp /root/shadow /etc
```

A szkript a lementett shadow állományt is az /etc könyvtárba másolja, visszaállítva ez által az esetlegesen módosított tanulo jelszót². A tanmasol.scp szkript a /root/nemmasol.txt állományra

¹ A speciális állományok miatt egyszerűbb letörölni és újramásolni

² Megoldhatjuk úgy is, hogy az /etc/init.d/rc.local fájlhoz hozzáírjuk a következő sort:
echo tanulo543 | /usr/bin/passwd tanulo --stdin

hivatkozik: ebben vannak felsorolva azok a könyvtárak, amelyeket nem ír felül a program. Az állomány tartalma:

```
/root/tanulo/Dokumentumok/  
/root/tanulo/Képek/  
/root/tanulo/Letöltés/  
/root/tanulo/Videó/  
/root/tanulo/Zene/
```

Az /etc/rc.d/rc.local állományhoz írjuk hozzá a következő sort:

```
/root/tanmasol.scp
```

Ezzel beállítottuk, hogy az operációs rendszer indulásakor visszaállítódik a tanulo felhasználó általunk lementett összes beállítása.

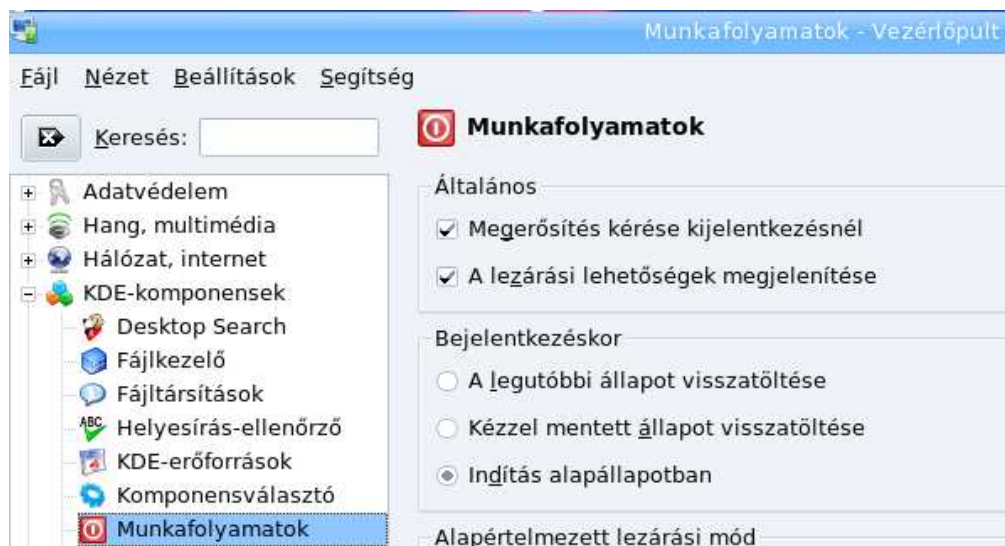
Próbáljuk ki a rendszer működését. Hozzunk létre az asztalon tetszőleges állományokat és könyvtárakat, állítsunk be más háttérképet és a Letöltés könyvtárba is mentsünk egy állományt. Újraindítva a Mandriva Linuxot azt tapasztaljuk, hogy az asztalon létrehozott állományoknak, könyvtárak eltűntek, a háttérkép az eredetileg beállított lett ismét, viszont a Letöltés könyvtárba mentett állományunk megvan.

A felhasználókat figyelmeztessük, hogy az Asztalra ne mentsenek dokumentumokat, és a Firefox programot is állítsuk be, hogy az alapértelmezett mentési hely a Letöltés könyvtár legyen és ne az Asztal (94. ábra).



94. ábra

A KDE vezérlőpultban válasszuk az Indítás alapállapotban kapcsolót. (95 ábra)



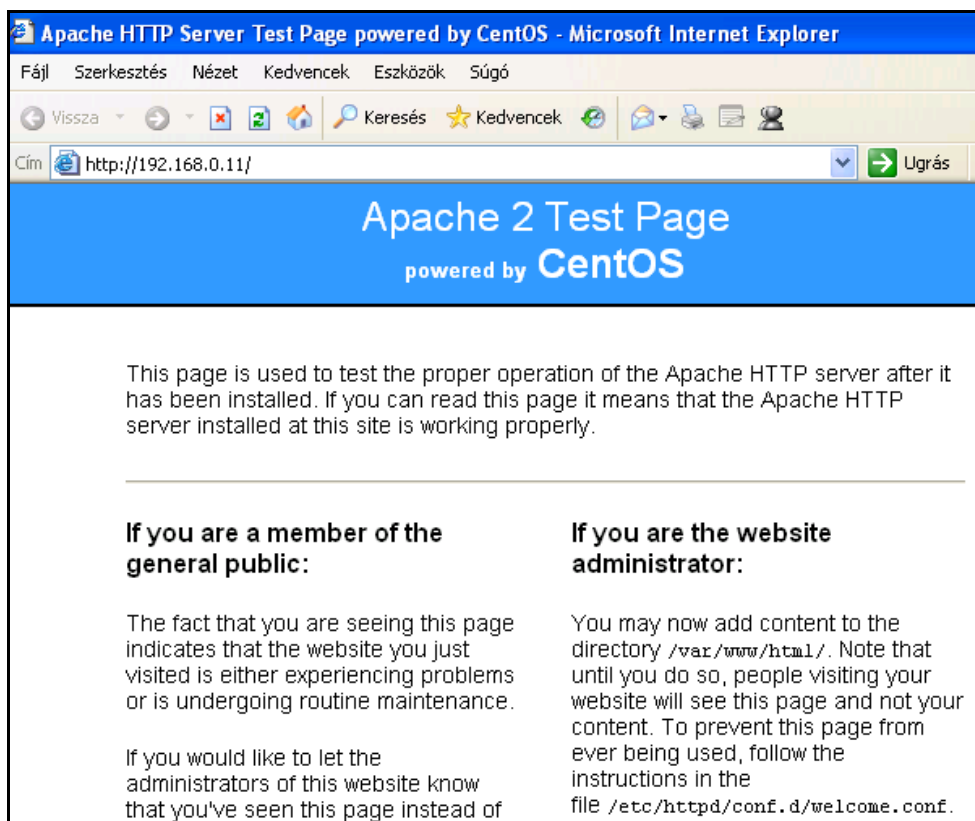
95. ábra

XI. Webszerver

A hálózati forgalom ellenőrzése c. fejezetben már volt szó a web szerverről, az MRTG és SARG statisztikákat és grafikonokat az jeleníti meg. Ellenőrizzük a szolgáltatás állapotát:

```
[root@server ~]# service httpd status
httpd (pid 3031 3030 3028 3027 3026 3025 3024 3023 2985) is running...
```

A kiszolgálón futó webszervert használhatjuk html anyagok közzétételére a belső hálózaton. A tűzfal beállításának köszönhetően csak a belső hálózatról érhető el. A webszerver gyökérkönyvtára a `/var/www/html`. Ha ide másolunk egy html dokumentumot `index.html` néven, akkor azt a webszerver megjeleníti. Amíg nincs ilyen nevű dokumentum az említett könyvtárban, a CentOS alapbeállításai szerint a következőt mutatja:



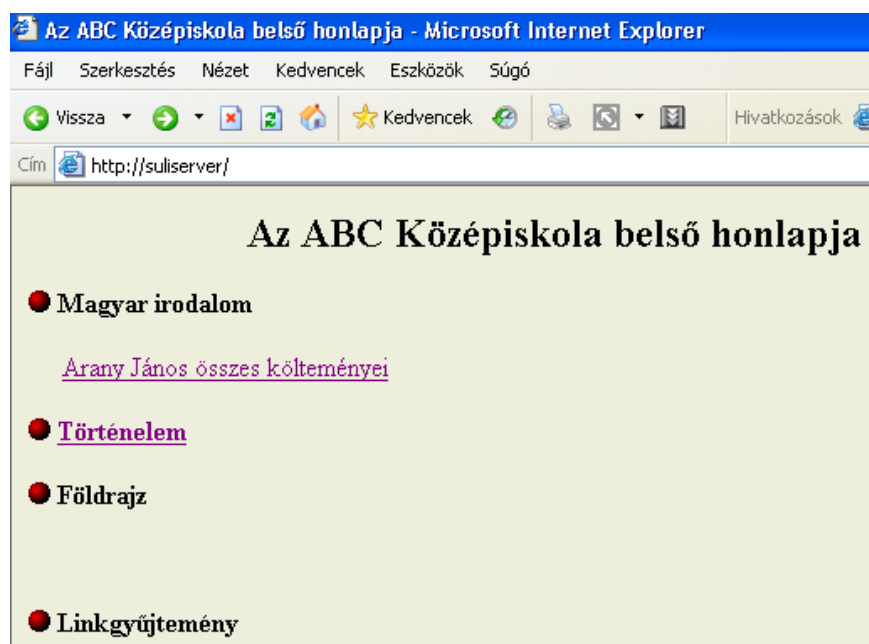
96. ábra

Egyszerűen megoldhatjuk, hogy ne IP címmel érjük el a kiszolgálónkat. A Windows hosts állományába írjuk be a következő sort:

```
192.168.0.11      suliserver
```

Windows 98 esetén a C:\Windows könyvtárban lévő hosts.sam állományt nevezzük át hosts – ra, és írjuk hozzá a fenti sort. Windows 2000 és XP esetén a fájl a C:\WINDOWS\system32\drivers\etc könyvtárban található és csak rendszergazdai jogosultságokkal módosíthatjuk. Természetesen a suliserver helyett más nevet is adhatunk a kiszolgálónknak.

A módosítás után nem csak a szerver IP címével, hanem a <http://suliserver/> gépnévvel is elérhető a kiszolgáló nyitóoldala. (97. ábra) Állítsuk be hogy ez legyen a böngészőprogramunk kezdőlapja. Mozilla Firefox böngésző használata esetén módosítsuk a kapcsolat beállításait. A suliserver szót írjuk hozzá a „Nincs proxy a következőkhöz:” listához.

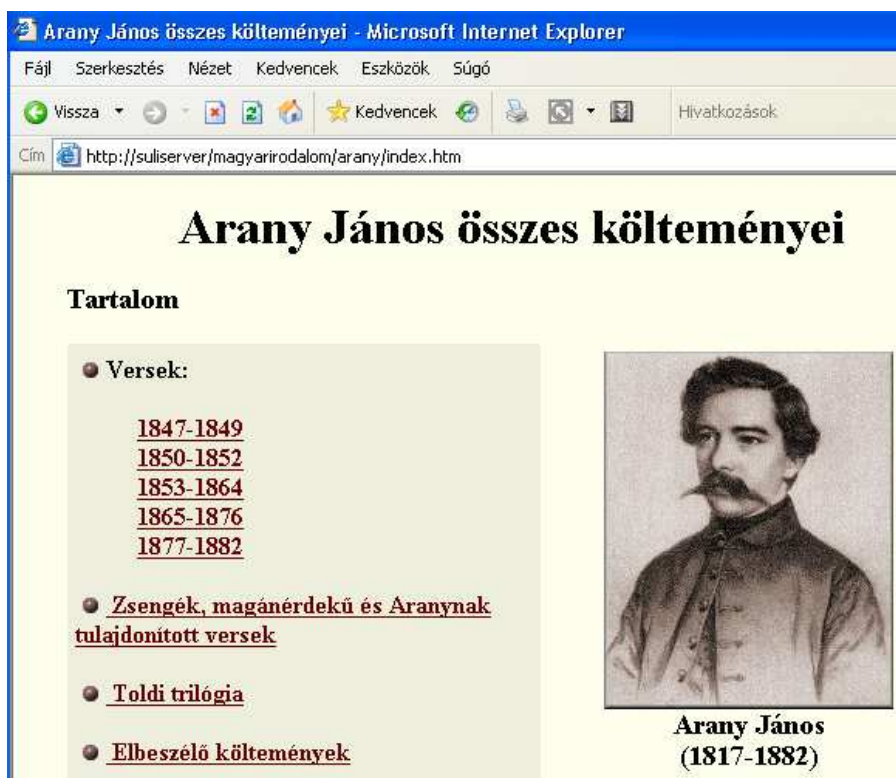


98. ábra

A kiszolgáló működését a Magyar Elektronikus Könyvtár (<http://mek.oszk.hu/>) honlapjáról letöltött Arany János összes költeményeinek példáján nézzük meg. Hozzuk létre a következő könyvtárakat az mkdir parancs vagy az mc segítségével:

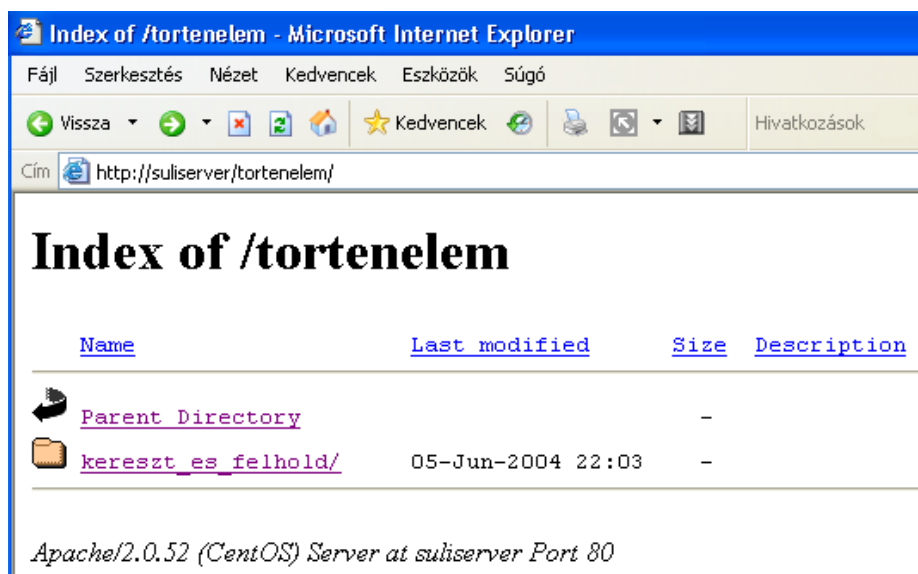
```
/var/www/html/magyarirodalom
/var/www/html/magyarirodalom/arany
/var/www/html/tortenelem
```

A /var/www/html/magyarirodalom/arany könyvtárba másoljuk a MEK-ről letöltött 00597html.zip állomány tartalmát. Az Arany János költeményei linkre kattintva megjelenik a letöltött weblap (99. ábra)



99. ábra

A Történelem link a /var/www/html/tortenelem könyvtárra mutat. Alapbeállítás szerint a webszerver megjeleníti a könyvtár tartalmát. (100. ábra) Ha valamelyik könyvtár tartalmaz index.html állományt, akkor az jelenik meg. Ez nem a legjobb módja weboldalak közzétételének, de nagyon gyors és egyszerű megoldás: létrehozunk egy könyvtárat és belemásoljuk a dokumentumokat. (101. ábra).



100. ábra



101. ábra

(A Kereszt és félhold: A török kor Magyarországon (1526-1699) c. mű is a Magyar Elektronikus könyvtárban található.)

XII. A Webmin

A webmin egy olyan segédeszköz, aminek segítségével rendszeradminisztrációs feladatokat végezhetünk el böngésző segítségével. Szinte az összes eddig tárgyalt szolgáltatás beállításait módosíthatjuk: felhasználókat hozhatunk létre és törölhetünk, konfigurálhatjuk a hálózati eszközöket, szolgáltatásokat menedzselhetünk, a Samba, a Squid működését is módosíthatjuk grafikus felületen. Aki nagyon idegenkedik a karakteres felülettől, szöveges állományok szerkesztésétől, annak elnyeri tetszését a webmin egyszerű kezelhetősége. De ne feledjük, hogy ugyanilyen könnyen el is ronthatjuk a kiszolgáló beállításait.

Nem javaslom, hogy a felhasználók létrehozását, törlését a webmin-el végezzük, mert így nem módosulnak azok a szöveges állományok, amelyek az Internet hozzáférést biztosítják.

A usermin program a webminhez hasonló, csak segítségével a felhasználók módosíthatják saját beállításait. Ezzel a két programmal oldjuk meg, hogy felhasználóink önállóan is jelszót módosíthassanak bármelyik munkaállomásról böngésző segítségével. Nagyszámú felhasználó esetén előbb-utóbb felmerül az igény a jelszómódosításra. Csak akkor követelhetjük meg a felhasználóktól, hogy tartsák titokban saját jelszavukat, ha megteremtjük a lehetőségét a jelszómódosításnak.

Töltsük le a <http://www.webmin.com/download.html> oldalról az aktuális legfrissebb verzióit a **webmin** és az **usermin** programoknak. A könyv írásakor ezek a következők voltak: **webmin-1.380-1.noarch.rpm** és a **usermin-1.320-1.noarch.rpm**. Mindkettő elérhető a következő címen is:

<http://www.kmf.uz.ua/centos/webmin-1.380-1.noarch.rpm>

<http://www.kmf.uz.ua/centos/usermin-1.320-1.noarch.rpm>

A két fájlt másoljuk a /root/inst könyvtárba és telepítsük őket:

```
[root@server inst]# rpm -ivh webmin-1.380-1.noarch.rpm
[root@server inst]# rpm -ivh usermin-1.320-1.noarch.rpm
```

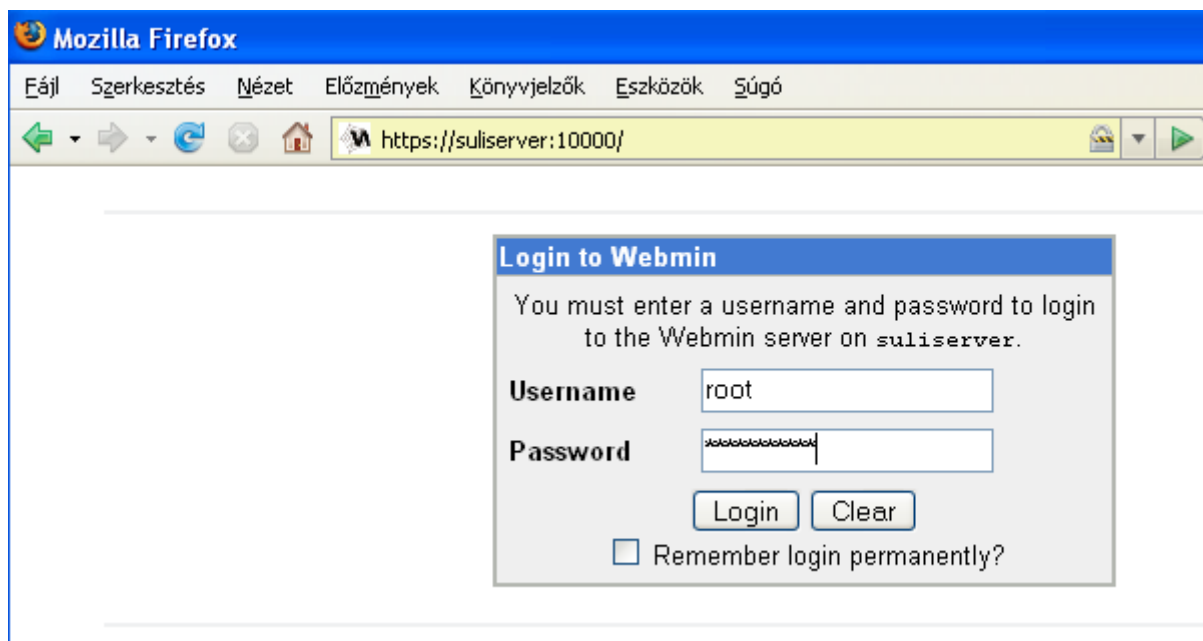
A /root/tuzfal.scp állományba az INPUT rész Samba portjait engedélyező sorai után írjuk a következő sorokat (az \$IPTABLES kezdetű sorok egysorosak):

```
# Webmin usermin
$IPTABLES -A INPUT -p tcp -s $NET_INT --destination-port 10000 -m state
--state NEW -j ACCEPT
$IPTABLES -A INPUT -p tcp -s $NET_INT --destination-port 20000 -m state
--state NEW -j ACCEPT
```

Indítsuk el a szkriptet start paraméterrel és mentjük a beállításokat:

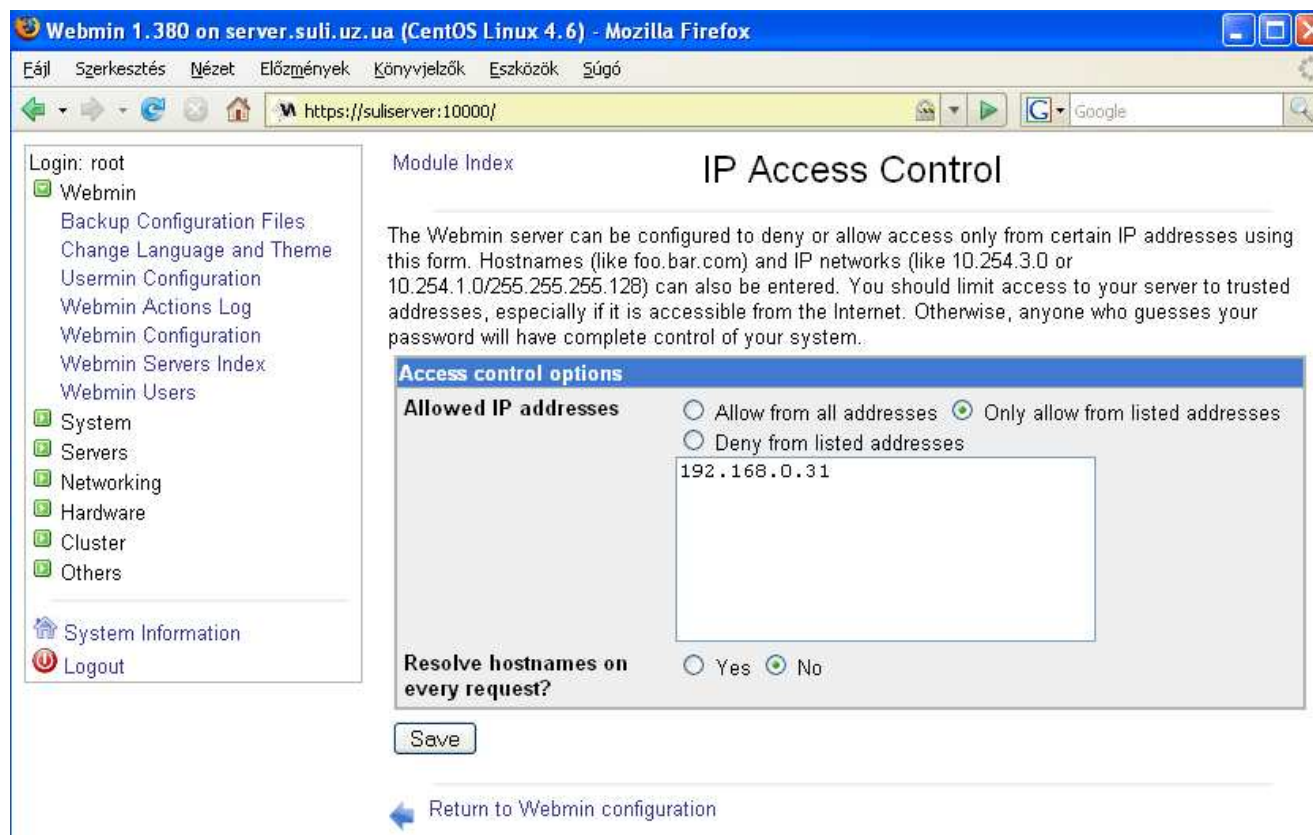
```
[root@server ~]# /root/tuzfal.scp restart
[root@server ~]# service iptables save
```

A munkaállomásunk böngészőprogramjába írjuk a következő címet: <https://suliserver:10000> (102. ábra)



102. ábra

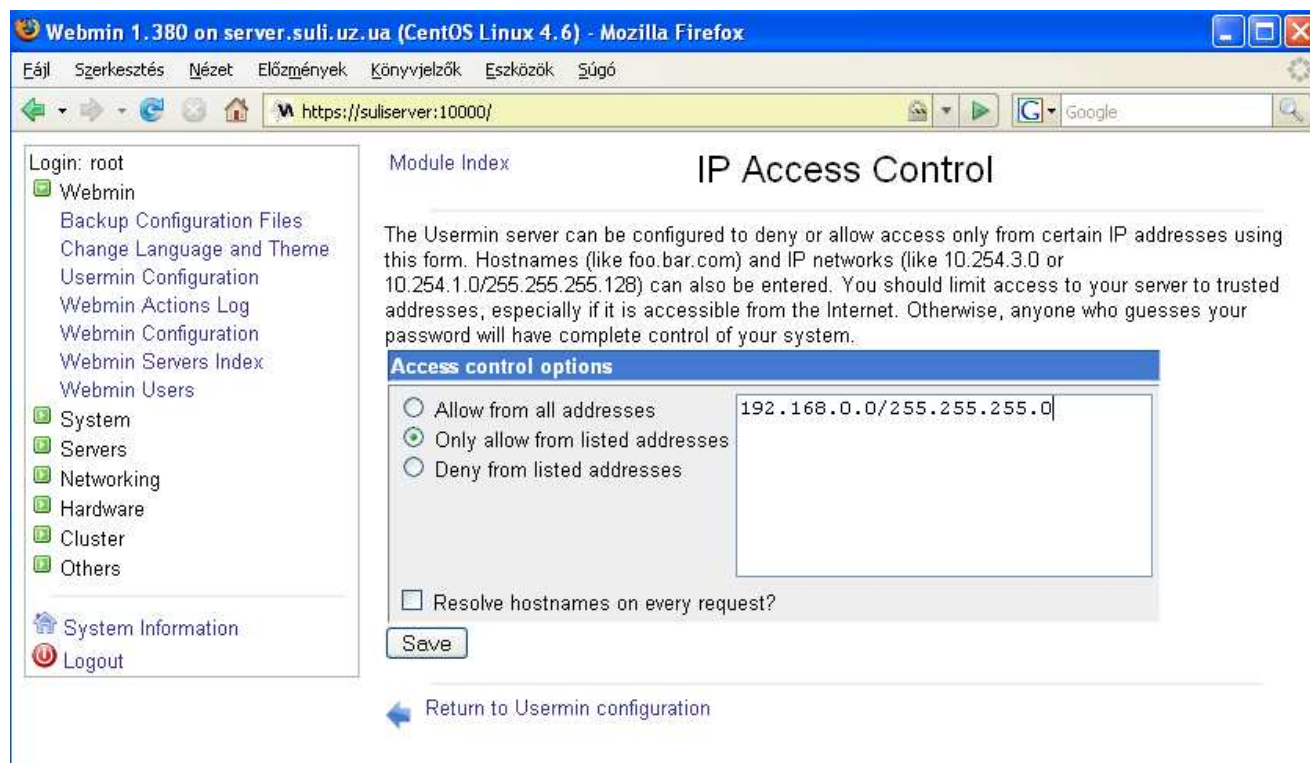
root-ként bejelentkezve egy információs oldalt látunk, azon a kiszolgáló nevét, lemez- és memóriahasználatát. Először állítsuk be, hogy csak saját munkaállomásunk IP címéről lehessen hozzáférni a webminhez. A baloldalon válasszuk a Webmin, majd a Webmin Configuration parancsot. Az "IP Access Control" ablakba írjuk be a munkaállomásunk IP címét és válasszuk az "Only allow from listed addresses" kapcsolót. (103. ábra)



103. ábra

Mentsük a beállítást a Save kapcsolóval.

A Usermin Configuration / IP Access Control ablakban állítsuk be, hogy a usermin szolgáltatás belső hálózatunk bármelyik gépéről elérhető legyen: 192.168.0.0/255.255.255.0 (104. ábra) Mentsük a beállítást.



104. ábra

A Usermin Configuration / Available Modules-nél a csak 105. ábrán látható modulok legyenek engedélyezve:

Module Index

Available Modules

Use this page to select which installed Usermin modules are visible to users.

☐ Apache Options Files	☒ Change Language	☒ Change Password
☒ Change Theme	☐ Change User Details	☐ Command Shell
☐ Custom Commands	☒ Disk Quotas	☐ Fetchmail Mail Retrieval
☐ File Manager	☐ Filter and Forward Mail	☐ GnuPG Encryption
☐ HTTP Tunnel	☐ Login Scripts	☐ MIME Type Programs
☐ Mail Forwarding and Replies	☐ Mount Filesystems	☐ MySQL Database
☐ Plan File	☐ PostgreSQL Database	☐ Procmail Mail Filter
☐ Protected Web Directories	☐ Read Mail	☐ Running Processes
☐ SSH Configuration	☐ SSH/Telnet Login	☐ Scheduled Commands
☐ Scheduled Cron Jobs	☐ Scheduled Emails	☐ SpamAssassin Mail Filter
☐ System Documentation	☐ Upload and Download	

105. ábra

Mentsük a beállítást. A felhasználóknak ezzel csak a jelszómódosítást engedélyezzük.

A 106. ábrán látjuk azt a beállítást a Usermin Configuration / User Interface ablakban, amivel bejelentkezés után a jelszómódosítás lesz az alapértelmezett.

After login, always go to module	Change Password
----------------------------------	-----------------

106. ábra

Fontos még, hogy a jelszómódosítás ablaka ne ajánlja fel a bejelentkezési jelszó mentését. A Webmin / Usermin Configuration / Authentication ablakban kapcsoljuk ki az „Offer to remember login permanently?” kapcsolót. (107. ábra)

Authentication and session options	
☐	Disable password timeouts
☒	Enable password timeouts
☒	Block hosts with more than 5 failed logins for 60 seconds.
☐	Block users with more than failed logins for seconds.
☐	Log blocked hosts, logins and authentication failures to <code>syslog</code>
☐	Disable session authentication
☒	Enable session authentication
☐	Auto-logout after minutes of inactivity
☐	Offer to remember login permanently?
☒	Show hostname on login screen?

107. ábra

Jelszómódosítás böngészőből

Ellenőrizzük, hogy működik-e a jelszómódosítás. Jelentkezzünk ki a webmin-ből a Logout gombbal és írjuk a böngészőbe a <https://suliserver:20000> címet. A megjelenő ablakba írjuk saját felhasználói nevünket és jelszavunkat. A Jelszómódosítás ablak fogad, ahol megváltoztathatjuk a jelszavunkat a jelenlegi, az új, és az új jelszó ismételt beírásával. (108. ábra) Mind a Linux (bejelentkezés, Internet-hozzáférés), mind a Samba (HOME könyvtár) jelszavunk megváltozik.

108. ábra

Hozzunk létre egy új sort a `/var/www/html/index.html` állományban a „Linkgyűjtemény” sor után. Ez létrehozza a „Jelszómódosítás” sort a weboldalunkon:

```
<p><b> <a href="https://suliserver:20000/">  
Jelszómódosítás</a></b></p>
```

Erre kattintva megjelenik a usermin bejelentkezőablaka, ahol a felhasználók megváltoztathatják jelszavaikat.

A webmin és a usermin szolgáltatásként fut. Ha csak a jelszómódosítást szeretnénk használni, leállíthatjuk a webmin-t és kikapcsolhatjuk automatikus indítását:

```
[root@server ~]# service webmin stop  
Stopping Webmin server in /usr/libexec/webmin  
[root@server ~]# chkconfig webmin off
```

XIII. Biztonsági mentések

Minden számítógépen nagyon fontos az adatok biztonsági mentésének megoldása. Különösen igaz ez kiszolgáló esetén. Többféle módon készíthetünk biztonsági mentéseket. Időközönként CD-re, vagy DVD-re írhatjuk ki a fontos adatainkat, a belső hálózat egy másik gépére hálózati mentést készíthetünk, vagy használhatunk szalagos egységeket is. RAID megoldásoknál adatainkat az operációs rendszer több merevlemezen tárolja. Sajnos egy ilyen rendszer kiépítése meglehetősen költséges. A Linux támogatja szoftveres RAID-et is, ami hagyományos merevlemezre történő párhuzamos írást jelent. Telepítésnél választhatjuk ezt a megoldást is.

USB adattároló eszközök használata

USB flash drive-ot is csatlakoztathatunk a kiszolgálóhoz. Leginkább akkor hasznos, ha a hálózat valamilyen okból nem érhető el. Adjuk ki a következő parancsot, hogy a képernyőn megjelenjenek a messages állomány azon sorai, melyek tartalmazzák az „sd” szöveget. Csatlakoztassuk a kiszolgálóhoz az eszközt:

```
[root@server /]# tail -f /var/log/messages | grep sd
Jan 18 23:50:15 server kernel: SCSI device sda: 1001472 512-byte hdwr
sectors (513 MB)
Jan 18 23:50:15 server kernel: sda: Write Protect is off
Jan 18 23:50:15 server kernel: sda: assuming drive cache: write through
Jan 18 23:50:15 server kernel: SCSI device sda: 1001472 512-byte hdwr
sectors (513 MB)
Jan 18 23:50:15 server kernel: sda: Write Protect is off
Jan 18 23:50:15 server kernel: sda: assuming drive cache: write through
Jan 18 23:50:15 server kernel: sda: sda1
Jan 18 23:50:15 server kernel: Attached scsi removable disk sda at
scsi4, channel 0, id 0, lun 0
Jan 18 23:50:16 server fstab-sync[27841]: added mount point
/media/KINGSTON for /dev/sda1
```

Az eszköz típusától függő, de a fentihez hasonló sorok jelennek meg a képernyőn. Az utolsó sor mutatja, hogy a rendszer létrehozott egy könyvtárat a /media –ban, és az eszközön található lemezrész /dev/sda1 néven érhető el. Adjuk ki a következő parancsot:

```
[root@server /]# mount -t vfat /dev/sda1 /media/KINGSTON
```

Ezzel mount-oltuk az eszközt, vagyis elérhető a /media/KINGSTON/ könyvtárban. A Midnight Commander-el másolhatunk az eszközre adatokat, vagy róla a kiszolgálóra. Mielőtt lecsatlakoztatjuk, adjuk ki az **umount /media/KINGSTON** parancsot.

Felhasználói azonosítók mentése

Oldjuk meg, hogy bizonyos időközönként a szerver mentést készítsen a felhasználói azonosítókról, jelszavakról és az általunk módosított konfigurációs állományokról.

A következő script létrehoz a /root/backup könyvtárban egy alkönyvtárt, aminek a neve az aktuális dátum. Első indításkor létrehozza a /root/backup könyvtárat is. A könyvtár nevét a következő parancs kimenete határozza meg:

```
[root@server ~]# date +%Y_%b_%d'
2007_Jan_06
```

Ebbe a könyvtárba másolatot készít a /root/felhasznalok.txt állományról. Átnevezi, hogy a fájlnevében a mentés dátuma is szerepeljen. Létrehoz állományokat a felhasználói és csoportazonosítókat tartalmazó rendszerfájlok azon soraival, melyek az általunk létrehozott

felhasználókat azonosítják a szerveren. A következő táblázat a rendszerfájlok, és a belőlük létrehozott biztonsági másolatok neveit mutatja:

/etc/passwd	1pass.txt
/etc/shadow	1shad.txt
/etc/group	1group.txt
/etc/gshadow	1gshad.txt

Az 1shad.txt állomány felhasználóink jelszavait is tartalmazza kódolt formában. A script a /root/felhasznalok.txt állományhoz hasonlóan másolatot készít a következő fájlokról is:

```
/etc/squid/squidGuard.conf  
/etc/squid/squid.conf  
/etc/samba/smb.conf  
/etc/samba/smbpasswd  
/root/tuzfal.scp
```

A könyvtár a következő állományokat tartalmazza:

```
[root@server 2007_Jan_06]# ls -l  
total 48  
-rw-r--r--  1 root root   380 Jan  6 19:35 1group.txt  
-rw-r--r--  1 root root   323 Jan  6 19:35 1gshad.txt  
-rw-r--r--  1 root root   859 Jan  6 19:35 1pass.txt  
-rw-r--r--  1 root root   979 Jan  6 19:35 1shad.txt  
-rw-r--r--  1 root root  1394 Jan  6 19:35 2007_Jan_06_fk.txt  
-rw-r--r--  1 root root 11024 Jan  6 19:35 2007_Jan_06_smb.conf  
-rw-----  1 root root  1683 Jan  6 19:35 2007_Jan_06_smbpasswd.conf  
-rwxr--r--  1 root root  2580 Jan  6 19:35 2007_Jan_06_squid.conf  
-rwxr--r--  1 root root  2580 Jan  6 19:35 2007_Jan_06_squidGuard.conf  
-rw-r--r--  1 root root    23 Jan  6 19:35 gmind.txt  
-rw-r--r--  1 root root   131 Jan  6 19:35 umind.txt
```

Az umind.txt szöveges állomány a felhasználók, a gmind.txt pedig a csoportok neveit tartalmazza.

FONTOS! A program csak akkor működik helyesen, ha minden csoport kettő, vagy több felhasználót tartalmaz. Mivel ez a gyakorlatban szinte mindig így van, csak arra kell ügyelnünk, hogy a program indításakor ne legyen olyan csoport, amelyiknek csak egy tagja van.

Az **userment.scp** program :

```
#!/bin/bash  
DATE=`date +%Y_%b_%d`  
if test -d /root/backup/$DATE  
then  
echo "Mar van ilyen konyvtar"  
exit 0  
fi  
mkdir -p /root/backup/$DATE  
cp /root/felhasznalok.txt /root/backup/$DATE/"$DATE"_fk.txt  
#  
cat -A /root/backup/$DATE/"$DATE"_fk.txt | cut -d"|" -f3 | sed 's/ //' >  
/root/backup/$DATE/umind.txt  
cat -A /root/backup/$DATE/"$DATE"_fk.txt | cut -d"|" -f1 | sort | uniq -  
d > /root/backup/$DATE/gmind.txt  
#  
# Csoportok  
for j in `cat /root/backup/$DATE/gmind.txt`  
do  
cat /etc/group | grep -w $j >> /root/backup/$DATE/1group.txt  
cat /etc/gshadow | grep -w $j >> /root/backup/$DATE/1gshad.txt  
done  
#
```

```
# Felhasználók
for i in `cat /root/backup/$DATE/umind.txt`
do
cat /etc/passwd | grep -w $i >> /root/backup/$DATE/1pass.txt
cat /etc/shadow | grep -w $i >> /root/backup/$DATE/1shad.txt
cat /etc/group | grep "^$i:" >> /root/backup/$DATE/1group.txt
cat /etc/gshadow | grep "^$i:" >> /root/backup/$DATE/1gshad.txt
done
cp /etc/squid/squidguard.conf /root/backup/$DATE/"$DATE"_squidguard.conf
cp /etc/squid/squid.conf /root/backup/$DATE/"$DATE"_squid.conf
cp /etc/samba/smb.conf /root/backup/$DATE/"$DATE"_smb.conf
cp /etc/samba/smbpasswd /root/backup/$DATE/"$DATE"_smbpasswd.conf
cp /root/tuzfal.scp /root/backup/$DATE/"$DATE"_tuzfal.scp
cp /root/kernp.scp /root/backup/$DATE/"$DATE"_kernp.scp
/usr/sbin/repquota -a > /root/backup/$DATE/"$DATE"_quota.txt
```

Ahhoz hogy az **userment.scp** program automatikusan minden nap elinduljon és elkészítse a mentéseket a **/etc/cron.d** könyvtárban létrehozunk egy **mentes** nevű állományt a következő tartalommal:

```
40 15 * * * root /root/userment.scp
```

Ebben az esetben minden nap 15:40-kor lefut az **userment.scp** nevű program. Az időzítést megváltoztathatjuk az első öt szóközzel elválasztott mező módosításával. Jelentésük sorrendben a következő:

- perc, 0 - 59
- óra, 0 - 23
- hónap napja
- hónap, 1 -12
- a hét napja, 0 - 6, 0 a vasárnapot jelenti

Ha csak hetente szeretnénk mentést készíteni, akkor módosítsuk a **mentes** állományt a következőre:

```
40 15 * * 3 root /root/userment.scp
```

Ebben az esetben minden héten, szerdán 15:40-kor készül el a biztonsági mentés.

A második merevlemez beállítása

Felhasználóink HOME könyvtárainak biztonsági másolatát valamilyen módon meg kell oldani. Különösen, hogy az általunk kiszolgálóként használt számítógép valójában egy hagyományos PC. Legalább a legsérülékenyebb alkatrész, a merevlemez, meghibásodására fel kell készülnünk. Építsünk be egy az elsővel megegyező kapacitású, vagy nagyobb merevlemezt a kiszolgálóba és arra készítsünk biztonsági másolatot a /home könyvtárról naponta.

Hasznos lenne, ha az oktatási anyagok és a webkiszolgáló könyvtára is egy-egy különálló, néhány gigabyte-os partícióra kerülne, hiszen az előző fejezetben bemutatott a multimédiás anyagok is több tíz megabyte-ot foglalnak el. A SARG napi statisztikái is több száz megabyte-ot jelentenek a /var/www/sarg könyvtárban.

Ellenőrizzük az elsődleges IDE csatlakozó master eszköz lemezrészeinek méreteit és foglaltságát:

```
[root@server etc]# df -h | grep hda | sort
/dev/hda1      99M    11M    83M    12% /boot
/dev/hda2     3.9G   280M    3.4G     8% /var
/dev/hda3     2.9G   1.1G    1.8G    37% /
/dev/hda5     2.0G   333M    1.5G    18% /var/spool/squid
/dev/hda7     28G    107M    26G     1% /home
```

Kapcsoljuk ki a számítógépet és csatlakoztassuk a második merevlemezt a másodlagos IDE csatlóóra. Kapcsoljuk be a számítógépet és figyeljük meg azokat a sorokat a `/var/log/dmesg` állományban, melyekben benne van a `hd`, de nincs benne a `hda` kifejezés. Tehát nem az első merevlemez tulajdonságait mutatják. Látjuk, hogy az új merevlemez a **hdc**:

```
[root@server log]# cat /var/log/dmesg | grep hd | grep -v hda
    ide1: BM-DMA at 0xa808-0xa80f, BIOS settings: hdc:DMA, hdd:pio
hdb: ASUS CRW-5232AS, ATAPI CD/DVD-ROM drive
hdc: ST340014A, ATA DISK drive
hdc: max request size: 1024KiB
hdc: 78165360 sectors (40020 MB) w/2048KiB Cache, CHS=16383/255/63,
UDMA(100)
hdc: cache flushes supported
    hdc: hdc1 hdc2
hdb: ATAPI 52X CD-ROM CD-R/RW drive, 2048kB Cache, UDMA(33)
[root@server log]#
```

A `fdisk -l` paranccsal jelenítsük meg a merevlemezen meglévő lemezz részeket:

```
[root@server log]# fdisk -l /dev/hdc

Disk /dev/hdc: 40.0 GB, 40020664320 bytes
255 heads, 63 sectors/track, 4865 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hdc1    *           1         1530     12289693+    7  HPFS/NTFS
/dev/hdc2           1531         4865     26788387+    c  W95 FAT32 (LBA)
```

A merevlemezen egy 12 Gb-os NTFS, és egy 26 Gb-os FAT partíció található. Az ezután következő parancsokat csak akkor adjuk ki, ha biztosak vagyunk benne, hogy minden fontos adatot mentettünk előzőleg róluk.

Az új merevlemezről eltávolítjuk meglévő a partíciókat, és három részre osztjuk. Az első legyen 30 Gb-os, ide kerül majd a `/home` könyvtár másolata. A második és a harmadik 5 Gb-os lesz, ide helyezzük át az `/oktat` és a `/var/www/html` könyvtárak tartalmát. Nevezzük át ezt a két könyvtárat:

```
[root@server /]# mv /oktat/ /oktatold/
[root@server /]# mv /var/www/html/ /var/www/htmlold/
```

Indítsuk el az `fdisk` programot `/dev/hdc` paraméterrel és a **p** paranccsal írassuk ki a lemezz részeket:

```
[root@server /]# fdisk /dev/hdc
Command (m for help): p

Disk /dev/hdc: 40.0 GB, 40020664320 bytes
255 heads, 63 sectors/track, 4865 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hdc1    *           1         1530     12289693+    7  HPFS/NTFS
/dev/hdc2           1531         4865     26788387+    c  W95 FAT32 (LBA)
```

A **d** parancs a lemezz részek törlésére szolgál. Első esetben meg kell adni, hogy melyiket töröljük (1), a második esetben már nem kell, mivel csak egyetlen partíció van. A **p** paranccsal látjuk, hogy a merevlemez nem tartalmaz partíciókat.

```
Command (m for help): d
Partition number (1-4): 1

Command (m for help): d
Selected partition 2
```

```

Command (m for help): p

Disk /dev/hdc: 40.0 GB, 40020664320 bytes
255 heads, 63 sectors/track, 4865 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot           Start          End      Blocks   Id  System

```

Command (m for help):

Az **n** paranccsal létrehozunk egy elsődleges (primary) partíciót a merevlemez kezdetén. Ahhoz, hogy 30Gb-os legyen a mérete a „+30G” – t kell beírni:

```

Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-4865, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-4865, default 4865): +30G

```

A következő lemezrész is elsődleges legyen, létrehozásánál meg kell adni, hogy a második számút hozzuk létre. Kapacitása 5 Gb:

```

Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (3649-4865, default 3649):
Using default value 3649
Last cylinder or +size or +sizeM or +sizeK (3649-4865, default 4865):
+5G

```

Mivel csak három részre osztjuk fel a merevlemezt, a harmadik is lehet elsődleges. Ezután már csak az Entert kell leütöni, hiszen alapértelmezés szerint a partíció az előző után kezdődik és a teljes szabad területet elfoglalja:

```

Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (4258-4865, default 4258):
Using default value 4258
Last cylinder or +size or +sizeM or +sizeK (4258-4865, default 4865):
Using default value 4865

```

A **p** paranccsal ellenőrizzük, hogy a partíciók megfelelőek:

```

Command (m for help): p

Disk /dev/hdc: 40.0 GB, 40020664320 bytes
255 heads, 63 sectors/track, 4865 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot           Start          End      Blocks   Id  System
/dev/hdc1             1           3648    29302528+   83  Linux
/dev/hdc2            3649           4257    4891792+    83  Linux
/dev/hdc3            4258           4865    4883760     83  Linux

```

Valójában az fdisk nem ír semmit a lemezre, amíg a **w** parancsot ki nem adjuk. Tehát a lemezzrészek megfelelőek lépünk ki az fdisk-ből a **w** paranccsal:

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@server /]#
```

Formázzuk meg mindhárom lemezzrészt ext3 naplózott fájlrendszerre a következő három parancs kiadásával. Minden esetben megjelennek különböző információk a formázás menetéről.

```
[root@server /]# /sbin/mke2fs -j /dev/hdc1
[root@server /]# /sbin/mke2fs -j /dev/hdc2
[root@server /]# /sbin/mke2fs -j /dev/hdc3
```

Hozzuk létre a következő három címkét, és aztán a könyvtárakat:

```
[root@server /]# e2label /dev/hdc1 /mentesek
[root@server /]# e2label /dev/hdc2 /oktat
[root@server /]# e2label /dev/hdc3 /var/www/html
[root@server /]# mkdir /mentesek
[root@server /]# mkdir /oktat
[root@server /]# mkdir /var/www/html
```

A Midnight Commander editorával módosítsuk az /etc/fstab állományt. A három félkövér formázással kiemelt sort hozzuk létre:

```
[root@server /]# cat /etc/fstab
# This file is edited by fstab-sync - see 'man fstab-sync' for details
LABEL=/1 / ext3 defaults 1 1
LABEL=/boot /boot ext3 defaults 1 2
none /dev/pts devpts gid=5,mode=620 0 0
none /dev/shm tmpfs defaults 0 0
LABEL=/home /home ext3
defaults,usrquota,grpquota 1 2
none /proc proc defaults 0 0
none /sys sysfs defaults 0 0
LABEL=/var /var ext3 defaults 1 2
LABEL=/var/spool/squid /var/spool/squid ext3 defaults 1 2
LABEL=/mentesek /mentesek ext3 defaults 1 2
LABEL=/oktat /oktat ext3 defaults 1 2
LABEL=/var/www/html /var/www/html ext3 defaults 1 2
LABEL=SWAP-hda6 swap defaults 0 0
/dev/hdb /media/cdrecorder auto
pamconsole,exec,noauto,managed 0 0
```

Ügyeljünk, hogy a címkék egyezzenek meg az e2label paranccsal létrehozottakkal. Legyünk igen körültekintőek az fstab állomány szerkesztésénél, hibás beírás esetén előfordulhat, hogy az operációs rendszer nem indul el! Ha leellenőriztük és elmentettük az állományt, indítsuk újra a számítógépet a reboot paranccsal.

Az mc segítségével az **/oktatold** könyvtár tartalmát helyezzük át az **/oktat** könyvtárba, és töröljük az **/oktatold**-ot. A **/var/www/htmlold** és a **/var/www/html** könyvtárakkal járunk el hasonlóképpen. Eztán ellenőrizzük a lemezzrészeket:

```
[root@server /]# df -Th | grep hd | sort
/dev/hda1 ext3 99M 11M 83M 12% /boot
/dev/hda2 ext3 3.9G 261M 3.4G 7% /var
/dev/hda3 ext3 2.9G 905M 1.9G 33% /
/dev/hda5 ext3 2.0G 333M 1.5G 18% /var/spool/squid
/dev/hda7 ext3 28G 107M 26G 1% /home
/dev/hdc1 ext3 28G 77M 27G 1% /mentesek
```

/dev/hdc2	ext3	4.6G	161M	4.3G	4%	/oktat
/dev/hdc3	ext3	4.6G	61M	4.3G	2%	/var/www/html

Látjuk, hogy mind az **/oktat**, mind a **/var/www/html** könyvtár külön partícióra került és közel 5 Gb adatot másolhatunk mindkettőre.

Az újraindítás után ellenőrizzük a megosztások és webszerver működését.

A **hdparm** nevű programmal részletes információk jeleníthetők meg a merevlemezről, és megváltoztathatunk vele különböző I/O-val kapcsolatos beállításokat. Az alapbeállításokat módosítva növelhetjük a merevlemez elérési sebességét. Mielőtt bármit is megváltoztatnánk, olvassuk el a gyártó honlapján az eszköz jellemzőit és tanulmányozzuk a parancs leírását (**hdparm --help** és **man hdparm**). Csak olyan rendszeren kísérletezzünk, amelyikről van biztonsági mentésünk. A következő parancs részletes információkat jelenít meg az új merevlemezről:

```
[root@server etc]# hdparm -i /dev/hdc

/dev/hdc:

Model=ST340014A, FwRev=3.04, SerialNo=3JX0ESAS
Config={ HardSect NotMFM HdSw>15uSec Fixed DTR>10Mbps RotSpdTol>.5% }
RawCHS=16383/16/63, TrkSize=0, SectSize=0, ECCbytes=4
BuffType=unknown, BuffSize=2048kB, MaxMultSect=16, MultSect=16
CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=78165360
IORDY=on/off, tPIO={min:240,w/IORDY:120}, tDMA={min:120,rec:120}
PIO modes: pio0 pio1 pio2 pio3 pio4
DMA modes: mdma0 mdma1 mdma2
UDMA modes: udma0 udma1 udma2 udma3 udma4 *udma5
AdvancedPM=no WriteCache=enabled
Drive conforms to: ATA/ATAPI-6 T13 1410D revision 2:

* signifies the current active mode
```

Az eszköz olvasási sebességét megállapíthatjuk a **-Tt** paraméterek segítségével. A gyorstárról, és a fizikai felületről történő olvasási sebességeket is méri a **hdparm** program:

```
[root@server etc]# hdparm -Tt /dev/hdc

/dev/hdc:
Timing cached reads:   504 MB in  2.01 seconds = 250.66 MB/sec
Timing buffered disk reads: 112 MB in  3.01 seconds = 37.20 MB/sec
```

Könyvtárak tükrözése

Biztonsági másolatot a **/home** könyvtárról egyszerűen készíthetünk a **mirrordir** program segítségével. Első indításkor a program teljes másolatot készít az első paraméterként megadott könyvtárról a másodikba. Ha ugyanezekkel a paraméterekkel ismét elindítjuk, már csak az új fájlokat és másolja és azokat írja felül a második könyvtárban, amelyek az elsőben módosultak. Az első könyvtárból eltávolított állományokat a másodikból is törli. Tehát a program gyorsan kialakítja az első könyvtár pontos tükröképét. Ezért nem is tekinthető valódi biztonsági mentésnek, de a legtöbb iskola lehetőségeit és eszközparkját figyelembe véve ez az a megoldás, ami még megvalósítható.

Telepítsük a **mirrordir** programot:

```
[root@server ~]# yum install mirrordir
```

Hozzuk létre a következő könyvtárakat:

```
[root@server ~]# mkdir /mentesek/home
[root@server ~]# mkdir /mentesek/root
```

A mirrordir programmal készítsünk másolatot a /home és a /root könyvtárakról a /mentesek könyvtárba:

```
[root@server ~]# /usr/bin/mirrordir -G aquota.* -X /home/lost+found/  
/home /mentesek/home  
[root@server ~]# /usr/bin/mirrordir /root /mentesek/root
```

Az első parancs paraméterei miatt nem készül másolat a az „aquota” kezdetű állományokról és a „lost+found” könyvtárról.

A mirrordir parancs használata közben legyünk igen körültekintőek! Ha felcseréljük a két paramétert, az üres könyvtárat fogja tükrözni a /home könyvtárra, visszavonhatatlanul törölve minden felhasználó könyvtárát!

A következő néhány soros szkript segítségével automatikussá tehetjük a mentéseket. A program leellenőrzi, hogy a /var/log/messages állomány utolsó 1000 sora közt van-e olyan, ami a hda meghajtó meghibásodására utal. Ha nincs, akkor elkészíti a biztonsági másolatot. Ha van, e-mail-ben elküldi a sorokat a root-nak.

A **mirror.scp** program:

```
#!/bin/bash  
DATE=`date +%Y_%b_%d`  
tail -1000 /var/log/messages | grep hda | grep rror >  
/root/tmp/"$DATE"_hiba.hda  
SOR=`wc -l /root/tmp/"$DATE"_hiba.hda | cut -d" " -f1`  
# echo $SOR  
if test $SOR -gt 0  
then  
mail -s HIBA_a_hda_merevlemezen! root < /root/tmp/"$DATE"_hiba.hda  
else  
rm /root/tmp/"$DATE"_hiba.hda  
/usr/bin/mirrordir -G aquota.* -X /home/lost+found/ /home /mentesek/home  
/usr/bin/mirrordir /root /mentesek/root  
fi
```

A mirror.scp állomány megtalálható a serverhez1.zip csomagban. Másoljuk a /root könyvtárba, és ha szükséges állítsuk be a futtatási jogosultságot. A következő paranccsal (egy sor!) hozzuk létre a mirror nevű állományt az /etc/cron. könyvtárban, amivel megoldjuk, hogy minden éjjel készüljön biztonsági másolat:

```
[root@server ~]# echo "16 2 * * * root /root/mirror.scp" >  
/etc/cron.d/mirror
```

Ennek eredményeként minden éjjel 2 óra 16 perckor lefut a mirror.scp program, elkészítve a biztonsági másolatokat. Ha a kiszolgálót a munkanap végén általában leállítjuk, módosítsuk az /etc/cron.d/mirror állományt, hogy a mentés a délutáni órákban történjen.

Ezzel a módszerrel lehetőség nyílik arra is, hogy a felhasználók által a nap folyamán véletlenül letörölt állományokat visszaállítsuk. Hívjuk fel a felhasználók figyelmét, hogy minden éjjel készül biztonsági másolat a HOME könyvtárukról, és a rendszergazda vissza tudja másolni az adott napon törölt állományokat. Az előző nap törölt állományokat már nem, azok végérvényesen elvesznek.

A mirrordir programmal megoldottuk, hogy a legfontosabb adatok két merevlemezen is tárolódnak. Ezzel bármelyik merevlemez meghibásodása esetén néhány óra alatt újra üzembe tudjuk állítani a kiszolgálót. Ha második merevlemez megy tönkre, akkor az előző fejezetben leírtaknak megfelelően. Az első merevlemez meghibásodása utáni teendőket a következő fejezet tárgyalja. Az /oktat és a /var/www/html könyvtárakba másolt oktatási anyagokról legyen biztonsági másolat CD-n, DVD-n, vagy valamelyik munkaállomás merevlemezén.

Ne gondoljuk azonban, hogy adataink 100%-ban biztonságban vannak. Például a tápegység bizonyos hibája, szerencsétlen esetben, tönkretelheti mindkét merevlemez. Ezért is elsődleges

fontosságú egy jó minőségű, lehetőleg márkás tápegység használata a kiszolgálóban. Ügyelni kell a szerver fizikai biztonságára is. Lopás vagy rongálás esetén minden adatunk elveszhet!

A rendszer visszaállítása

A merevlemez vagy a teljes szerver cseréje esetén a létrehozott biztonsági mentés segítségével megoldható, hogy ne kelljen ismét fáradságos munkával létrehozni a felhasználókat, és konfigurációs állományokat. Ehhez persze rendelkezniünk kell a /root/backup könyvtár tartalmával¹. A merevlemez meghibásodása esetén ez is elveszhet, fontos, hogy időközönként mentjük el a könyvtárat valamilyen más hordozóra (pl. CD) is. Tároljuk biztonságos helyen, hiszen személyes adatokat tartalmaz.

Az új szerveren végezzük el a telepítést és a beállításokat az I-IV fejezetekben leírtaknak megfelelően. A VII. fejezetben leírtak alapján telepítsük a Sarg és az MRTG programokat. Ezután másoljuk át a /root könyvtárba a backup könyvtárat. Ellenőrizzük, hogy tartalmazza azt a könyvtárat (pl. 2007_Jan_12), amelyikben a mentett adataink vannak. Másoljuk ebbe a könyvtárba a **visszaallit.scp** programot és belépve a könyvtárba indítsuk el. A program megjelenít néhány figyelmeztető sort és két másodperc várakozás után megjeleníti a könyvtár állományait:

```
Felhasznalok létrehozasa backup allomany alapjan
csak ujonnan feltelptitett rendszeren es csak egyszer alkalmazzuk!!!

---- KILEPES: Ctrl+C ----

1group.txt 1pass.txt 2007_Jan_06_fk.txt      2007_Jan_06_smbpasswd.conf
ch.scp      umind.txt
1gshad.txt  1shad.txt  2007_Jan_06_smb.conf  2007_Jan_06_squidGuard.conf
gmind.txt   visszalit.scp

Irjuk be a backup fajl datumat
2007_Jan_06 formatumban:
2007_Jan_06
```

Ismét 2 másodperc után bekéri a mentett állományok nevében található dátumot. A program leellenőrzi, hogy létezik-e a beírt dátummal mentett állomány, majd azt is, hogy a mentésben megtalálható első felhasználó valóban nincs létrehozva ezen a rendszeren. Ezután visszaállítja a csoportokat és azonosítókat, jelszavakat és az elmentett konfigurációs állományokat. Beállítja a tűzfalszabályokat és a kenelmodulok betöltését. Létrehozza a felhasználók könyvtárait, azokat a felhasználó tulajdonába adja és beállítja a jogosultságokat.

Az **visszaallit.scp** program:

```
#!/bin/bash
clear
echo "Felhasznalok létrehozasa backup allomany alapjan"
echo "csak ujonnan feltelptitett rendszeren alaklmazzuk!!!"
echo;echo "---- KIKLEPES: Ctrl+C ----"
echo;sleep 2
ls;sleep 2;echo;D=`date +%Y_%b_%d`
echo "Irjuk be a backup fajl datumat"
echo " $D formatumban:"
read DATE
if test -s ./"$DATE"_fk.txt
then
# csoportok, felhasznalok
U1=`head -1 ./1pass.txt | cut -d":" -f1`
FU=`grep -w $U1 /etc/passwd | wc -c`
if test $FU -ge 1
```

¹ Amennyiben az előző fejezetekben tárgyaltak alapján beépítettünk második merevlemezt, és beállítottuk a biztonsági mentést, a /mentesek/root/backup könyvtárban megtaláljuk az állományokat.

```

then
echo "MAR VANNAK FELHASZNALOK!"
exit 0
fi
cat ./1group.txt >> /etc/group
cat ./1gshad.txt >> /etc/gshadow
cat ./1pass.txt >> /etc/passwd
cat ./1shad.txt >> /etc/shadow
# Konfiguracios allomanyok
cp ./"$DATE"_fk.txt /root/felhasznalok.txt
cp ./"$DATE"_squid.conf /etc/squid/squid.conf
cp ./"$DATE"_squidguard.conf /etc/squid/squidguard.conf
cp ./"$DATE"_smb.conf /etc/samba/smb.conf
cp ./"$DATE"_smbpasswd.conf /etc/samba/smbpasswd
cp ./"$DATE"_tuzfal.scp /root/tuzfal.scp
chmod 700 /root/tuzfal.scp
cp ./"$DATE"_kernp.scp /root/kernp.scp
chmod 700 /root/kernp.scp
echo "/root/kernp.scp" >> /etc/rc.d/rc.local
# Tuzfal:
/root/tuzfal.scp start
/sbin/service iptables save
# Felhasznaloi konyvtarak létrehozasa
mkdir /etc/skel/Dokumentumok
mkdir /etc/squid/csoportok
for i in `cat ./umind.txt`
do
if test -d /home/$i
then
echo "a /home/$i konyvtar mar letezik"
else
cp -R /etc/skel /home/$i
fi
chown -R $i /home/$i
chgrp -R $i /home/$i
chmod -R 744 /home/$i
done
else
echo "Nincsenek ilyen fajlok!!"
fi

```

Ezután hozzunk létre egy felhasználót az **uj_felhasznalo.scp** programot elindítva. Erre a lépésre mindenképp szükség van, hiszen ez a program készíti el a /squid/csoportok könyvtár állományait. Hozzuk létre egy fiktív felhasználót, akit akár azonnal törölhetünk is, a **torol_felhasznalo.scp** programmal. Ellenőrizzük, hogy a /squid/csoportok könyvtár valóban tartalmazza az állományokat.

A második merevlemezt, rajta a biztonsági mentésekkel, már telepítésnél is beállíthatjuk. Ügyeljünk arra, hogy a telepítő ne formázza a rajta lévő partíciókat, és megfelelő könyvtárakként csatolja a rendszerhez. Amennyiben a telepítés után szereljük a gépbe, ebben a fejezetben leírtak szerint járunk el, természetesen az **fdisk** és a **mke2fs** parancsokat kihagyva! Az **e2label** paranccsal létrehozzuk a címkéket és módosítjuk az fstab állományt.

A Midnight Commander segítségével a /mentesek/home könyvtár tartalmát átmásoljuk a /home könyvtárba. A mirror.scp programot addig **ne** használjuk, míg meg nem bizonyosodunk, hogy a /home könyvtár minden felhasználó adatát tartalmazza.

Állítsuk be a tárkorlátokat az V. fejezetben leírtak szerint. A proba90 és proba300 felhasználókat a **visszallit.scp** program létrehozta, állítsuk be számukra quota-t. Ezután már lefuttathatjuk az **alapquota.scp** programot. Ez minden tanulónak 90 és minden tanárnak 300 megabyte tárkorlátot állít be és a jogosultságokat is beállítja.

Az `alapquota.scp` program:

```
#!/bin/bash
# Tanulok alapquotaja
for i in `cat /etc/squid/csoportok/tanulok.txt`
do
chown -R $i /home/$i
chgrp -R $i /home/$i
chmod -R 755 /home/$i
edquota -p proba90 $i
done
# Tanarok alapquotaja
for j in `cat /etc/squid/csoportok/tanar.txt`
do
chown -R $j /home/$j
chgrp -R $j /home/$j
chmod -R 700 /home/$j
if test $j = "proba90"
then
echo "proba90 - 90M"
else
edquota -p proba300 $j
fi
done
```

A tárkorlát szempontjából az eredeti rendszerhez képest a különbség az, hogy ott az első felhasználó (vagyis mi magunk) nem kapott semmilyen korlátozást. Módosítsuk ezt, ha szükséges az V. fejezetben leírtak szerint. Az egyedi, a felhasználó kérésére módosított quota beállításokat is ismét létre kell hozni. Ezt könnyíti meg a `<dátum>_quota.txt` állomány, amit a backup könyvtárban találunk és a quota értékeket tartalmazza.

XIV. A rendszer felügyelete

A Linux operációs rendszeren több program is rendelkezésünkre áll kiszolgálónk teljesítményének megfigyelésére és elemzésére. A **top** programmal megfigyelhetjük a processzorterhelés átlagát, üzemidőt, a gépen futó folyamatok számát és még sok egyéb információt. A top 3 másodpercenként automatikusan, a szóköz leütésére azonnal frissíti az adatokat a képernyőn. Megfigyelhetjük vele melyik folyamat milyen mértékben használja az erőforrásokat. A k billentyű leütésével és a folyamat pid-jének megadásával az adott folyamatot megszakíthatjuk. Kilépni a programból a q billentyű leütésével tudunk.

```
[root@server ~]# top
top - 22:29:11 up 3:34, 2 users, load average: 0.15, 0.11, 0.06
Tasks: 90 total, 1 running, 89 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.7% us, 0.7% sy, 0.0% ni, 97.7% id, 1.0% wa, 0.0% hi, 0.0% si
Mem: 255852k total, 249864k used, 5988k free, 10080k buffers
Swap: 522104k total, 192k used, 521912k free, 143504k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     TIME+  COMMAND
 24759 root        17   0   3660   952   764  R   0.7   0.4    0:00.05 top
   3006 squid      15   0 22580  16m 1876  S   0.3   6.7    0:27.40 squid
     1 root        16   0   3148   548   468  S   0.0   0.2    0:00.84 init
     2 root        34  19     0     0     0  S   0.0   0.0    0:00.00 ksoftirqd/0
     3 root         5 -10     0     0     0  S   0.0   0.0    0:00.06 events/0
     4 root         5 -10     0     0     0  S   0.0   0.0    0:00.02 khelper
     5 root         5 -10     0     0     0  S   0.0   0.0    0:00.00 kblockd/0
     6 root        15   0     0     0     0  S   0.0   0.0    0:00.00 khubd
    34 root        15   0     0     0     0  S   0.0   0.0    0:00.01 kapmd
    37 root        20   0     0     0     0  S   0.0   0.0    0:00.00 pdflush
    38 root        15   0     0     0     0  S   0.0   0.0    0:00.65 pdflush
    39 root        15   0     0     0     0  S   0.0   0.0    0:00.32 kswapd0
    40 root         7 -10     0     0     0  S   0.0   0.0    0:00.00 aio/0
   186 root        25   0     0     0     0  S   0.0   0.0    0:00.00 kseriod
   430 root         6 -10     0     0     0  S   0.0   0.0    0:00.00 ata/0
   431 root         7 -10     0     0     0  S   0.0   0.0    0:00.00 ata_aux
   436 root        15   0     0     0     0  S   0.0   0.0    0:00.11 kjournald
```

SMART – merevlemezek állapota

A rendszeren ellenőrizhetjük a merevlemezek állapotát a SMART (Self-Monitoring, Analysis and Reporting Technology) értékek lekérdezésével. Szinte minden merevlemez támogatja. A telepítés után beállított hdc eszközön a következő paranccsal kapcsolhatjuk be a SMART értékek figyelését:

```
[root@server /]# smartctl -s on /dev/hdc
smartctl version 5.33 [i686-redhat-linux-gnu] Copyright (C) 2002-4 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF ENABLE/DISABLE COMMANDS SECTION ===
SMART Enabled.
```

A parancsot --help paraméterrel kiadva olvassuk el a paraméterek magyarázatát. A -H paraméterrel lekérdezhetjük az eszköz általános állapotát:

```
[root@server /]# smartctl -H /dev/hdc
smartctl version 5.33 [i686-redhat-linux-gnu] Copyright (C) 2002-4 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF READ SMART DATA SECTION ===
```

```
SMART overall-health self-assessment test result: PASSED
```

Minden SMART értéket megjelenít a parancs -a paraméterrel futtatva. A merevlemez hőmérsékletét a 194-el kezdődő sor mutatja:

```
[root@server /]# smartctl -a /dev/hdc | grep ^194
194 Temperature_Celsius      0x0022    034    051    000    Old_age    Always
-          34
[root@server /]# smartctl -a /dev/hda | grep ^194
194 Temperature_Celsius      0x0022    031    048    000    Old_age    Always
-          31
```

Mindkét merevlemez hőmérsékletét lekérdeztük. A primary master 31 °C, a secondary master 34 °C. Ha 40 °C feletti értékeket mérünk, építsünk be pótlólagos ventilátorokat az eszközök hűtése érdekében.

A kiszolgálón rendszeresen ellenőrizzük a partíciók foglaltságát. A /var könyvtár mérete néhány hét alatt akár több Gigabájtosra is nőhet, különösen, ha a munkaállomások valamelyikén letöltésvezérlő programot használnak. Leginkább a /var/www/sarg könyvtár méretét kell figyelniük, és a régi, már nem szükséges statisztikákat törölni belőle.

LogWatch – rendszernapló elemzés

Az CentOS operációs rendszer a LogWatch nevű program által minden nap üzenetet küld a root-nak, amiben az előző nap szinte minden fontosabb rendszerüzenetét megtaláljuk: kernel üzenetek (iptables-log), új felhasználók, csoportok, ssh-val bejelentkezettek listája, root-jogosultságot kérő felhasználók (su), hibás bejelentkezések stb. Minden levél végén a merevlemez partícióinak foglaltságát is látjuk:

```
##### LogWatch 5.2.2 (06/23/04) #####
Processing Initiated: Mon Dec 31 13:06:22 2007
Date Range Processed: yesterday
Detail Level of Output: 0
Logfiles for Host: server.suli.uz.ua
#####

-----

----- Disk Space -----
/dev/hda3      2.9G  1.1G  1.7G  40% /
/dev/hda1      99M   12M   83M  12% /boot
/dev/hda7      28G   77M   26G   1% /home
/dev/hda2      3.9G  442M  3.3G  12% /var
/dev/hda5      2.0G  134M  1.7G   8% /var/spool/squid
##### LogWatch End #####
```

A root leveleit átirányíthatjuk a saját felhasználói nevünkre, hozzáírva az /etc/aliases állományhoz a következő sort:

```
root: pferi
```

Természetesen pferi helyett a saját felhasználói nevünket írjuk. A postfix szolgáltatást újra kell indítani a beállítás érvényre jutásához:

```
[root@server /]# service postfix restart
```

Az is könnyen megoldható, hogy saját munkaállomásunk levelezőkliense letöltse ezeket a leveleket. Ehhez telepíteni kell a dovecot nevű programot a kiszolgálón, (előtte ellenőrizzük, hogy jelenleg nincs-e telepítve: **rpm -qa | grep dovecot**)

```
[root@server /]# yum install dovecot
```

módosítani az /etc/dovecot.conf állomány „protocols” értékét, hogy a pop3 protokollt is támogassa,

```
protocols = imap imaps pop3 pop3s
```

valamint a tuzfal.scp szkriptet az INPUT részen, hogy a munkaállomásunk hozzáférhessen a 110-es TCP porthoz:

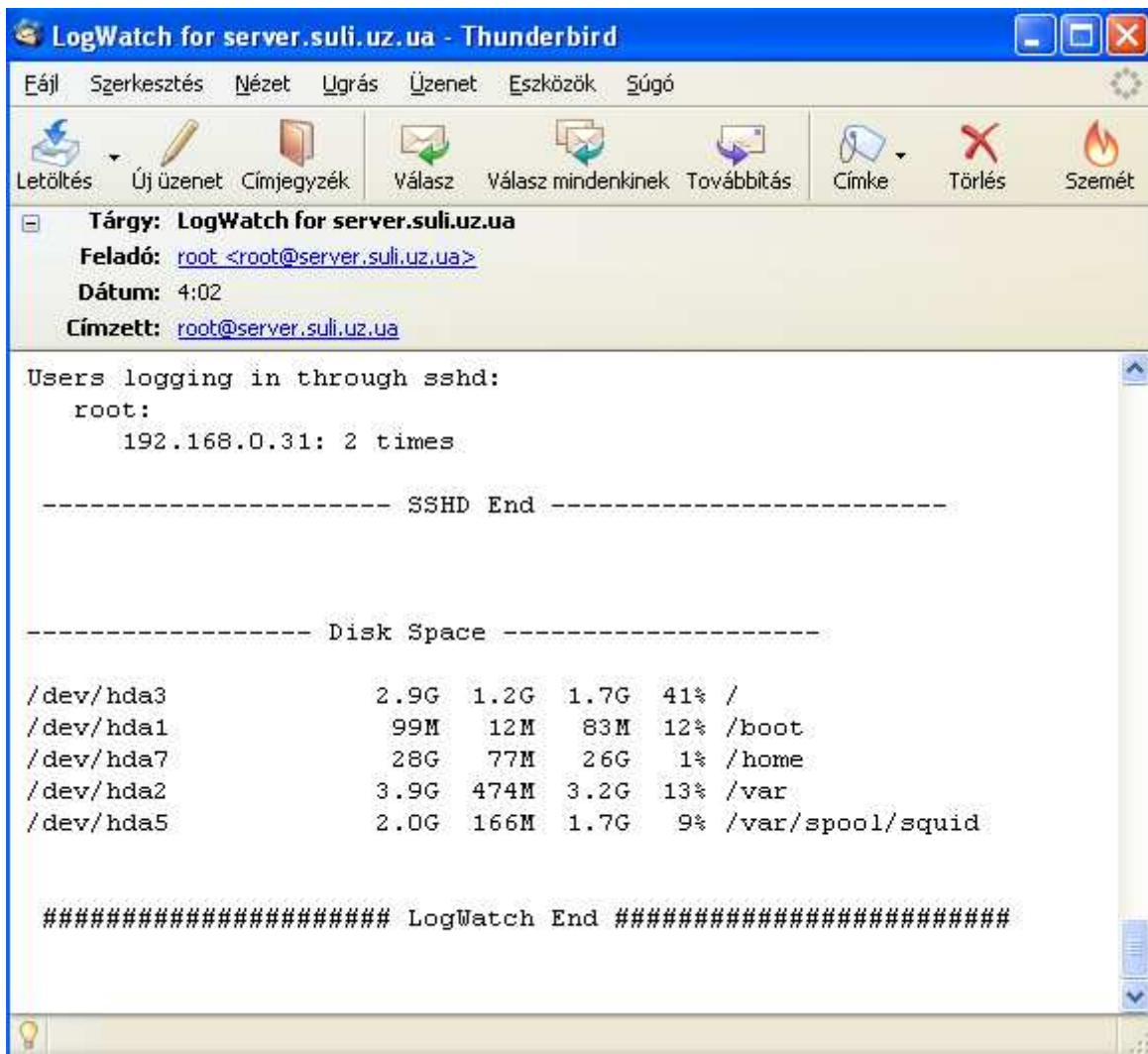
```
$IPTABLES -A INPUT -p tcp -i $IFACE_INT -s 192.168.0.31 --destination-port 110 -m state --state NEW -j ACCEPT
```

Indítsuk újra a tűzfalat és indítsuk el a dovecot szolgáltatást:

```
[root@server /]# /root/tuzfal.scp restart
[root@server /]# service iptables save
[root@server /]# service dovecot start
[root@server /]# chkconfig --levels 235 dovecot on
```

Most már létrehozhatjuk munkaállomásunk levelezőkliensében a postafiókot (109. ábra), és a CentOS minden nap levelet küld erre a postafiókra a rendszerünk állapotáról (110. ábra).

109. ábra



110. ábra

MUNIN – teljesítményadatok webes felületen

A MUNIN egy olyan program, ami az MRTG-hez hasonlóan, webes felületen mutatja a kiszolgáló működésének különböző paramétereit. Működése kliens-szerver alapú, ezért akár több gép monitorozását is megvalósíthatjuk vele. Telepíteni és beállítani egyszerű, és kiválóan alkalmas szerverünk különböző paramétereinek megjelenítésére: a CPU-kihasználástól kezdve a merevlemezek hőmérsékleteinek változásáig.

A telepítéshez adjuk ki a következő parancsokat:

```
[root@server /]# yum install munin
[root@server /]# yum install munin-node
```

Az első program gyűjti a teljesítményadatokat és rajzol belőlük grafikont, a második küldi az adatokat. Több kiszolgáló monitorozása esetén azokra csak a másodikat kell telepíteni.

Módosítsuk a munin könyvtár tulajdonosát:

```
[root@server /]# chown -R munin:munin /var/www/munin
```

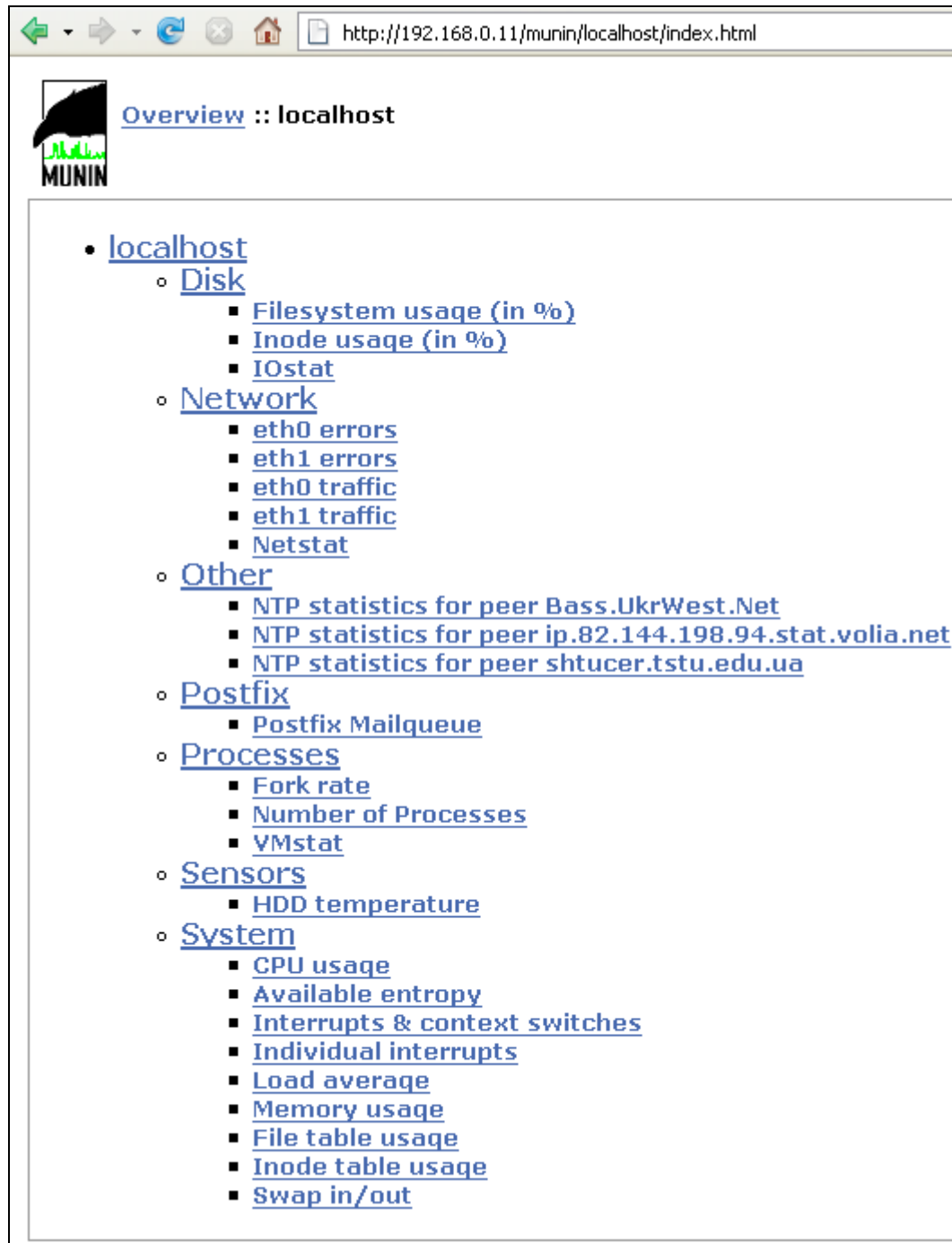
Az /etc/munin/munin.conf állományban a htmldir kezdetű sort módosítsuk a következőre:

```
htmldir /var/www/munin
```

A következő két parancs a munin-node szolgáltatást indítja el és beállítja az automatikus indítását:

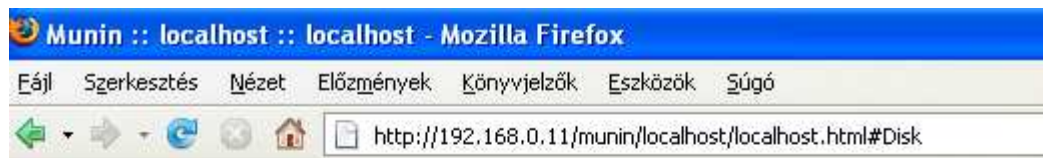
```
[root@server /]# /etc/init.d/munin-node start
[root@server /]# chkconfig --levels 235 munin-node on
```

Ötpercenként készíti a statisztikákat és a <http://192.168.0.11/munin/> címen érhető el. A 111. ábra a kiszolgálón monitorozható szolgáltatások közül mutat néhányat.



111. ábra

A [Filesystem usage \(in %\)](#) sorra kattintva a következő képet látjuk néhány óra elteltével:

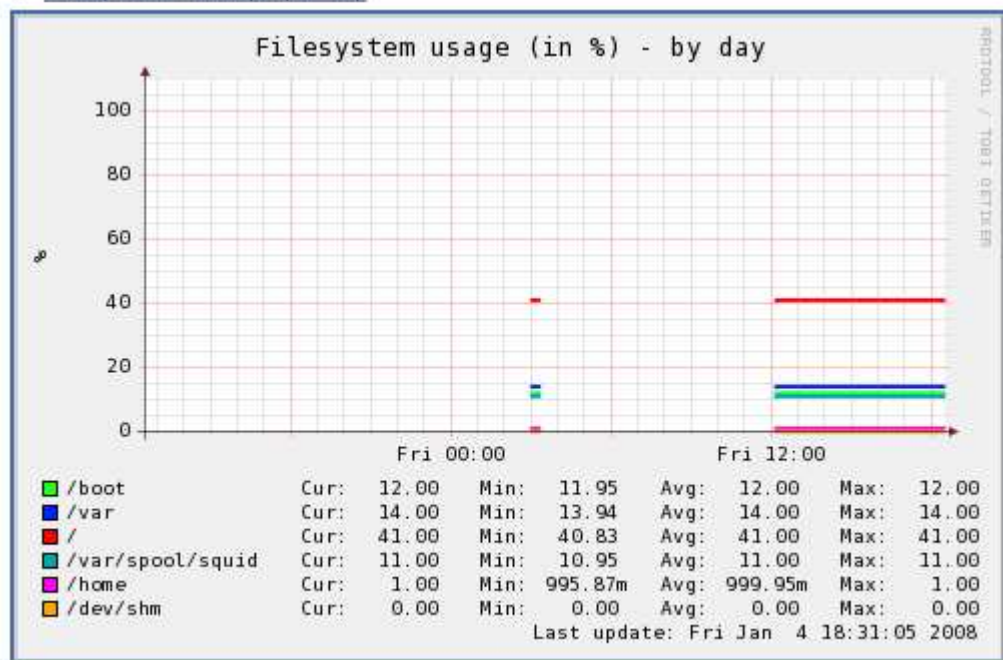


[Overview](#) :: [localhost](#) :: [localhost](#)

[localhost](#) :: [[Disk](#) [Network](#) [Other](#) [Postfix](#) [Processes](#) [Sensors](#) [Sys](#)

Disk

:: [Filesystem usage \(in %\)](#)



112. ábra

XV. Végző

E könyvben megpróbáltam bemutatni, hogy szerény anyagi és technikai feltételekkel hogyan lehet felépíteni egy működő rendszert. Ne gondoljuk azonban, hogy az általam bemutatott megoldások az egyedül célravezetők. A Linux és a szabad szoftverek rugalmassága lehetővé teszi, hogy a feladatokat többféle módon oldjuk meg.

A CentOS vagy más Linux disztribúció segítségével a bemutatottaknál összetettebb szolgáltatásokat is megvalósíthatunk. Hasznos lehet egy saját mail-webmail szerver beüzemelése, amit csak az Internet szolgáltatóval egyeztetve tudunk megvalósítani. Vegyük figyelembe viszont, hogy az utóbbi időben egyre több spam és vírus miatt ez a szolgáltatás az eddig tárgyaltaknál több adminisztrációt igényel a rendszergazdától.

Végezetül elmondható, hogy próbáljuk megismerni minél alaposabban a Linux operációs rendszert és törekedjünk a legegyszerűbb, a legkönnyebben kezelhető és automatizálható megoldásokra.

XVI. A felhasznált és ajánlott irodalom összevont jegyzéke

1. Ács Zsolt (2004): Linux operációs rendszer(váltás), ComputerBooks Kft.
2. Büki András (2002): UNIX / Linux héjprogramozás, Kiskapu Kft.
3. Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes (2004): Linux biztonsági eljárások, Kossuth kiadó
4. Michael D. Bauer (2003): Szerverek védelme Linuxal, Kossuth kiadó
5. Molnár Hajnalka (2004): A Linux alapjai, Kossuth kiadó
6. Pere László (2001): Linux felhasználói ismeretek I., Pere László
7. Pere László (2002): Linux felhasználói ismeretek II., Kiskapu Kft.
8. Pere László (2005): GNU/Linux rendszerek üzemeltetése I -II, Kiskapu Kft.
9. Наба Бакарати (2004): Red Hat Linux. Секреты профессионала, Диалектика
10. Эви Немет, Гарт Снайдер, Трент Р. Хейн (2003): Руководство администратора Linux, Вильямс
11. Пол Хадсон, Эндрю Хадсон, Билл Болл, Хойт Дафф (2006): Red Hat Fedora 4 полное руководство, Вильямс
12. <http://www.centos.org/docs/4/html/yum>
13. http://www.howtoforge.com/perfect_setup_centos_4.4
14. http://www.brandanhutchinson.com/installing_squid.html
15. http://www.opennet.ru/base/net/squid_inst.txt.html
16. <http://dag.wieers.com/home-made/squidguard/>
17. http://www.opennet.ru/docs/RUS/squid_filter/squidguard.html
18. <http://hu.opensuse.org/>
19. <http://wiki.hup.hu>
20. <http://www.maxsworld.org/index.php/how-tos/mrtg/>
21. <http://www.mjmwired.net/resources/mjm-services-fc6.html>
22. <http://tldp.fsf.hu/HOWTO/TimePrecision-HOWTO-hu/ntp.html>
23. <http://www.szabilinux.hu/iptables/>
24. <http://www.iopus.com/guides/bestpopsmtmp.htm>
25. <http://mail.google.com/support/bin/topic.py?topic=1555>
26. <http://www.vcsk.hu/~szistvan/linux/samba/szakdolgozat/>
27. <http://support.microsoft.com/kb/229940>
28. http://kbase.redhat.com/faq/FAQ_80_4166.shtm
29. http://kbase.redhat.com/faq/FAQ_79_3648.shtm
30. http://www.linuxvilag.hu/content/files/cikk/64/cikk_64_58_60.pdf