

# Sulinet Expressz informatikai és informatika alapú továbbképzések

## Rendszergazda Linux haladó

Pallagi László

Lektorálta:  
Sándor Antal

Sulinet Expressz, 2003.11.01.

# Tartalomjegyzék

Tartalomjegyzék .....	2
Bevezetés.....	5
1. Alapismeretek.....	6
1.1 Linux, mint operációs rendszer.....	6
1.2 Internet.....	9
1. ARPA verem rétegei.....	10
2. IP címek .....	12
3. IP hálózatok .....	14
4. Routerek.....	15
5. Névfeloldás az Interneten.....	16
1.3 Védelem .....	19
6. Tűzfalak.....	19
7. Tűzfalak típusai .....	19
8. Tűzfal helye a hálózatban, a hálózat felépítése .....	20
1.4 Telepítéshez szükséges alapismeretek.....	23
9. Partíciók .....	24
10. Programok .....	25
1.5 Gyakorlat.....	29
1.6 Ellenőrző kérdések.....	29
1.7 Felhasznált, ajánlott irodalom.....	30
2. Telepítés.....	31
2.1 RedHat Linux 9.0.....	31
11. Telepítés megkezdése.....	31
12. Rendszerindító képernyő.....	31
13. Telepítés nyelvének kiválasztása (Language Selection) .....	33
14. Billentyűzet nyelvének kiválasztása (Keyboard) .....	34
15. Egér beállítása (Mouse Configuration) .....	35
16. Telepítés típusa (Installation Type).....	36
17. Lemez partícionálása.....	37
18. Boot Loader beállítása.....	38
19. Hálózati kártyák beállítása (Network Devices).....	39
20. Tűzfal beállítása.....	41
21. Nyelvek kiválasztása .....	42
22. Időzóna beállítások.....	43
23. ROOT jelszó beállítása .....	44
24. Felhasználók azonosításának beállításai .....	44
25. Program csomagok csoportjainak kiválasztása .....	45
26. Csomagok kiválasztása .....	46
27. Függőségek kezelése .....	48
28. Csomagok felmásolása .....	48
29. Indítólemez készítése .....	49
30. Webmin telepítése .....	49
2.2 Debian GNU/Linux 3.0 R1 .....	50
31. Telepítés megkezdése.....	50
32. Telepítés nyelvének kiválasztása (Choose The Language).....	51
33. Telepítőrendszer főmenü.....	51

34.	Újraindítás után.....	55
35.	DSELECT .....	58
36.	Szükséges csomagok telepítése .....	59
2.3	SUSE LINUX 8.2 Professional .....	62
37.	Telepítés megkezdése.....	62
38.	Rendszerindító képernyő.....	62
39.	Telepítés nyelvének kiválasztása (Language Selection) .....	63
40.	Telepítési beállítások .....	64
41.	Első indítás .....	69
2.4	Gyakorlat.....	70
2.5	Felhasznált, ajánlott irodalom.....	70
3.	Finomhangolás, ismerkedés a rendszerrel.....	70
3.1	Első belépés.....	70
3.2	Hasznos parancsok.....	75
3.3	Webmin beállítása.....	77
3.4	Gyakorlat.....	79
3.5	Ellenőrző kérdések.....	80
3.6	Felhasznált, ajánlott irodalom.....	80
4.	SSH (Secure shell).....	80
4.1	Alapismertek.....	80
4.2	SSH szerver beállítása konzolról.....	81
4.3	SSH kulcsok generálása .....	81
4.4	Programok használata .....	82
4.5	Gyakorlat.....	82
4.6	Ellenőrző kérdések.....	83
4.7	Felhasznált, ajánlott irodalom.....	83
5.	Felhasználók, jogosultságok kezelése .....	83
5.1	Alapismertek.....	83
5.2	Felhasználó kezelése konzolról.....	86
5.3	Jogosultságok beállítása konzolról.....	87
5.4	Felhasználói quota .....	88
5.5	Gyakorlat.....	90
	Vegyük fel a következő felhasználókat:.....	90
5.6	Ellenőrző kérdések.....	91
5.7	Felhasznált, ajánlott irodalom.....	92
6.	Samba fájl- és nyomtatószerver .....	92
6.1	Alapismertek.....	92
6.2	Samba beállítása kézzel .....	93
43.	Globális beállítások.....	94
44.	Megosztások.....	97
6.3	SWAT .....	98
6.4	Egyéb kézi adminisztrációk .....	100
6.5	Gyakorlat.....	101
6.6	Ellenőrző kérdések.....	102
6.7	Felhasznált, ajánlott irodalom.....	103
7.	Apache .....	103
7.1	Alapismertek.....	103
7.2	Apache beállítása kézzel.....	104
	Általános beállítások:.....	104
	Modulok betöltése .....	105

Könyvtár és fájl beállítások.....	106
Log állományok kezelése .....	107
Virtuális hostok beállítása.....	107
7.3 Jelszókezelések .....	108
7.4 Gyakorlat.....	108
7.5 Ellenőrző kérdések.....	108
7.6 Felhasznált, ajánlott irodalom.....	109
8. Sendmail .....	109
8.1 Alapismertek.....	109
8.2 Sendmail kézi beállítása.....	112
8.3 Gyakorlat.....	113
8.4 Ellenőrző kérdések.....	113
8.5 Felhasznált, ajánlott irodalom.....	113
9. Squid proxy .....	114
9.1 Alapismertek.....	114
9.2 Squid beállítása.....	115
9.3 Szűrés .....	116
9.4 Transzparens üzemmód.....	117
9.5 Gyakorlat.....	118
9.6 Ellenőrzőkérdések a kilencedik fejezethez.....	118
9.7 Felhasznált, ajánlott irodalom.....	118
10. Egyéb szerverek .....	118
10.1 Xinetd csúciszerver .....	118
10.2 Proftpd szerver .....	119
10.3 DHCP szerver .....	121
10.4 DNS szerver.....	122
10.5 Ellenőrző kérdések.....	125
10.6 Felhasznált, ajánlott irodalom.....	125
11. Csomagszűrés.....	125
11.1 Alapismertek.....	125
11.2 NAT .....	131
11.3 Példák .....	131
11.4 Ellenőrző kérdések.....	132
11.5 Felhasznált, ajánlott irodalom.....	132

## Bevezetés

Ez a könyv azoknak szól, akik a Linux rendszert szeretnék megismerni rendszergazda szemmel.

A könyv szerkesztésénél megpróbáltunk elméleti és gyakorlati tudást egyaránt nyújtani. Természetesen az anyag terjedelme nem engedte meg, hogy minden részletet és a Linux rendszerek teljes tudását bemutassuk, ezért elsősorban egy kiindulási alapot tartalmaz.

Törekedtünk arra, hogy a leírtak segítségével működő megoldáshoz jussanak a hallgatók. Emellett egy-két tippet is elhelyeztünk az anyagban, amely gyakorlati tapasztalatokon alapszik.

A tananyag és a könyv szerkezete RedHat Linux disztribúcióra íródott. A telepítésnél vázoljuk a SUSE LINUX és a DEBIAN GNU/LINUX első lépéseit is. A további fejezetekben viszont már előfordulhatnak disztribúciós eltérések.

A beállításoknál elsősorban kézi megoldásokat vesszük végig. A telepítésnél viszont a WEBMIN nevezetű webes felületű beállító rendszert is felrakjuk. Ez rendszer a legtöbb disztribúció alá elérhető, tehát általánosnak mondható. Kézenfekvő lehetőség a beállítások ismerkedéséhez, hiszen jól tagoltan tartalmazza a lehetőségeket. Érdekes egy ismeretlen rendszer esetében a lehetőségek átnézésére.

Jó szárnyalást kívánunk a pingvin varázslatos világában!



# 1. Alapismeretek

## 1.1 Linux, mint operációs rendszer

A Linux rendszer fejlesztése a 90-es évek elején kezdődött el Linus Torvalds munkájával, amelyet teljes egészében publikált az Interneten. Torvalds a 0.02-es változatnál az Interneten feladott hirdetésében szabad kapacitással rendelkező fejlesztőket keresett. A fejlesztés gőzerővel haladt tovább és 1994-ben megjelent az 1.0.0 Linux. Ekkora már rengetegen fejlesztettek Linux alá alkalmazásokat is. Ebben lényeges szerepet játszott, hogy az egyetemeken UNIX rendszereken futó programokat könnyen be lehetett fordítani Linux alá. Ekkor jelentek meg az alkalmazásokat összefoglaló disztribúciók (terjesztések) is.

Az így kialakult Linux operációs rendszer sok szempontból alkalmas Internetes szerverek telepítésére. Előnyei közé tartozik, hogy jó rendszergazdai tevékenység mellett, nagyon biztonságossá tehető. Ezt elősegíti a nyitottsága és jól dokumentáltsága. Ha valaki hajlandó elmélyülni a részletekben, az olyan szervereket alkothat, melyeket nyugodt szível, stabilan üzemeltethet.

Amikor Linux rendszerekről beszélünk, egy több részből összeállított programcsomagot tartunk szem előtt. Minden Linux rendszer magja a kernel, amelyet egy központi fejlesztőcsapat alkot. A kernelek kisebb módosításokkal minden Linux disztribúciónál ugyanazok. Jelenleg túl vagyunk a 2.2-es és a 2.4-es sorozaton, hiszen már a 2.6-es kernelből is megjelentek az első verziók.

Itt érdemes megjegyezni, hogy a 'Linux' Linus Torvalds bejegyzett védjegye. A Linux, mint fogalom elsősorban a kernel és ennek kiegészítéseit jelenti. Azaz az operációs rendszert. Ez egyik disztribúciónak sem tulajdona. A disztribúciók erre a magra építik fel, saját elképzeléseik szerint, a csomaggyűjteményüket. Ezek rengeteg alkalmazást, programot tartalmaznak, amelyet külön-külön cégek, csoportok fejlesztenek. Természetesen a disztribúciókat semmi sem kötelezi arra, hogy az így kialakult gyűjteményt (amelyek saját fejlesztéseiket is tartalmazzák) ingyen adják.

A Linux rendszerek és szoftverek egy kialakult licence rendszerrel vannak ellátva. Ennek az egyik fajtája a GPL (érdeemes utána nézni). Ezeknek a licencek a nagy előnyük, hogy kötelezővé teszik a forráskóddal együtt való terjesztést. Ezért mondjuk ezekről a rendszerekről, hogy nyílt forráskódúak. Ez viszont nem jelenti azt, hogy minden esetben ingyenesek.

A Linux rendszereket telepítő csomagokban adják ki, az erre specializálódott cégek, szervezetek. Talán a legismertebb disztribúció a Debian GNU/Linux. De még nagyon sok elterjedt kiadás létezik:

- **Debian GNU/Linux.** Egyike a legrégebbi és legnagyobb támogatást élvező disztribúcióknak. Jelenleg a 3.0-s (R1) woody névre keresztelt verziónál tartunk. Telepítése és beállítása nehézkes, viszont a csomagok frissítése a legegyszerűbb. Elsősorban fejlesztőknek, rendszergazdáknak készült. Szemlélete is ezt tükrözi. Csak stabil, tesztelt megoldásokat használ és kerüli a

kényelmi szempontokból történő egyszerűsítéseket. Információi elérhetőek (részben magyarul is) a <http://www.debian.org> oldalon.

- **Slackware Linux.** Az első Linux disztribúciók egyike (lehet, hogy a legelső?). Jelenleg a 9.1-es verziónál tart. (<http://www.slackware.com>)
- **RedHat Linux.** Szintén régi disztribúciónak számít. Könnyen telepíthető, egyszerű megoldásokat tartalmaz. Jellemző rá, hogy a telepített programok alapbeállításai biztonságosnak mondhatóak. Nagyon jó lehetőséget ad kezdőknek is használható rendszer telepítésére. Jelenleg a 9.0-as verziónál tart. Ennek a sorozatnak a támogatását a RedHat nemsokára megszünteti. A továbbra is ingyenes, támogatott verzió a RedHat Fedora Core 1. Mivel az üzleti Linux piacon a legnagyobb forgalommal rendelkezik, elsősorban a pénzes megoldásokat tette előtérbe. (<http://www.redhat.com>)
- **SUSE LINUX.** A SUSE LINUX Európa legelterjedtebb Linux disztribúciója. Az első kiadása 1992-ben jelent meg, most éppen a 9.0-ás verziónál tart. A SUSE LINUX könnyen telepíthető és beállítható, a megfelelő tudással szerverfunkciókhoz is használható a disztribúció. A SUSE LINUX-ot ISO formában ugyan nem lehet letölteni, de az Internetről telepíthető vagy frissíthető, és ugyanúgy másolható, mint a legtöbb disztribúció. A 7.1-es verzió óta a SUSE LINUX magyar nyelven és magyar dokumentációval is elérhető. A SUSE LINUX Professional disztribúció mellett üzleti termékekkel is rendelkezik a SUSE, elsősorban vállalatok és iskolák számára. Az üzleti termékek alapja a SUSE LINUX Enterprise Server. A SUSE LINUX Openexchange Server például egy levelezőszerver és csoportmunka megoldás közepes és nagy cégek számára. A SUSE LINUX Standard Server egy minden-egyben megoldás kis és közepes vállalatoknak, a SuSE Linux School Server iskoláknak nyújt teljes körű megoldást, a SUSE LINUX Firewall On CD, pedig egy CD-ről futó tűzfal-rendszer. A SUSE LINUX üzleti termékei mind nyílt forráskódúan, azonban nem szabadon hozzáférhetőek, és nem szabadon másolhatók. (<http://www.suselinux.hu>)
- **UHU Linux.** MAGYAR Linux disztribúció. Három vonalon külön-külön kiadással vannak jelen. Az UHU-Linux Office jelenleg az 1.0 (és az 1.1 Beta 4) verziónál tart. Kifejezetten kliensek telepítésére alkalmas, rengeteg magyar és magyarított alkalmazással. Az UHU-Linux Firewall tűzfalak telepítésére alkalmas, speciálisan optimalizált elemekkel. Nagy előnye, hogy tartalmazza a Zorp GPL 2.0 tűzfal-rendszert (<http://www.balabit.hu>), ami szintén magyar fejlesztés. Ez a párosítás igen figyelemreméltó GPL tűzfal megoldás. Létezik továbbá egy UHU-Linux Server kiadás is, ezzel teljessé téve a palettát. <http://www.uhulinux.hu>

Természetesen ez a felsorolás nem teljes. Ha minden Linux disztribúciót fel szeretnék sorolni, a lista teljesen elfoglalná eme jegyzet erőforrásait. Azért még szeretnék megemlíteni egy-két érdekességet:

- **Astaro Linux.** Kifejezetten tűzfal szervernek kialakított Linux disztribúció. Ugyan fizetős, de oktatási intézményeknek ingyenes. Web-es beállító felülete egyszerű és jól használható. (<http://www.astaro.com>)
- **IPCOP.** Szintén speciálisan tűzfal szerepeket betöltő disztribúció. Ingyenes. A Shoothwall egyik fejlesztője vitte tovább az elgondolásait. Könnyen telepíthető és Web-es felületen állítható be. Egyszerűsége és ingyenessége végett megtalálható a Sulinet egy-két iskolájában is. (<http://www.ipcop.org>).

- **Freesco Linux.** Az egyik kedvencem. A projekt alkotói megpróbálták egy router funkciókat kiszolgáló, egyszerűen beállítható 1 lemezes (1,44 MB) megoldást alkotni. Azt hiszem sikerült nekik. A teljes lemezt elfoglaló rendszerbe be van építve DNS, DHCP, Printer, HTTP, Remote Access szerver is. (<http://www.freesco.org>)
- **Devil-Linux.** Egyszerűen beállítható tűzfal disztribúció. CD-ről boot-olható és nincs szükség merevlemezre sem. Már 486-os processzortól használható (<http://www.devil-linux.org>)
- **KRUD.** RedHat Linux-on alapuló disztribúció. Biztonsági szempontokat figyelembe véve Kevin Fenzi (Linux Security HOW-TO alkotója) optimalizálta. (<http://www.tummy.com/krud>)
- **Lindows.** Windows programok futtatására készített disztribúció. Már a kiadása idejében nagy port vert fel, a Microsoft részéről ért támadások miatt. (<http://www.lindows.com>)
- **MkLinux.** Az Apple Computer támogatásával írt disztribúció. Futtatható PowerPC architektúrán. (<http://www.mklinux.org>)
- **SULIX!!!!!!!** Knoppix alapokra helyezett csomagválogatás. CD-ről fut, telepíteni nem szükséges. Fontos, hogy csak szabadon terjeszthető elemeket tartalmaz, így legálisan másolható a diákoknak is. Magyar összeállítás, kifejezetten a magyar oktatás igényei alapján. Minden szükséges alkalmazás megtalálható rajta. Jelenleg az 1.1-es verziónál tart. Nagyon jól használható tesztelésre is, hiszen minden hálózati alkalmazást, klienst tartalmaz és pillanatokon belül rendelkezésre áll. (<http://www.sulix.hu>)

Ha valaki részletesen szeretne elmélyedni a Linux világába, annak ajánlom a <http://www.linux.org/dist/list.html> címen található disztribúciós listát.

A disztribúciókban szereplő programok nagy részét elérhetjük a program készítőinek oldalain is. Itt mindig gyorsabban jelennek meg a frissítések, új verziók. Egy szerver elkészítése után a legfontosabb dolgunk a hibajavítások követése.

A linux rendszerek egyik legnagyobb előnye, hogy az előforduló, detektált biztonsági hibákat nagyon gyorsan javítják. Gyakran jellemző, hogy a hiba publikálása és a javítás megjelenítése ugyanarra a napra tehető. Érdeemes figyelni azokat a fórumokat, melyek ezekről tájékoztatást adnak.

A legtöbb disztribúciónál lehetőség van a frissítések automatikus letöltésére, telepítésére. A rendszerünk kiválasztásánál érdemes utánanézni, mennyire gyorsan jönnek ki rá a javítások.

Talán itt érdemes beszélni a Linux támogatottságáról. Más rendszerekkel ellentétben a Linux-nak az elsődleges support-ját szervezetek adják. Szinte minden problémára létezik már dokumentált megoldás valahol, csak meg kell találnunk. Kiemelt szerepet kapnak a levelező listák és ezek archívumai. Szintén nagyon jól használhatóak, az un. Howto-k (hogyanok), melyeket nagy mennyiségben lehet elérni az Interneten. Nézzünk meg egy pár lényeges Internet címet.

Magyar Linux Felhasználók (<http://mlf.linux.rulez.org/mlf/>) levelező listái:



- **Linux-kezdő lista.** Ez egy kezdőknek szóló levelezőlista, egyszerű kérdésekkel, sok segítőkész emberrel. Ideális nem csak a kezdőknek, hanem azoknak is akik szívesen segítenek másoknak átküzdeni magukat az első bakikon. Az RTFM e listán nem megengedett kifejezés.
- **Linux lista.** Az első magyar nyelvű Linuxos lista volt, mára a már nem kezdő Linux felhasználók számára kíván segítséget nyújtani. Ha elakad pl. a Linux beállításával, érdemes körülnézni az archívumban. Ezen a listán már nem meglepő, ha valaki válaszként csak ennyit kap: RTFM.
- **Linux++.** A haladó Linuxosoknak szánt fórum. Levél küldése előtt kérjük, olvassa el a lista célkitűzéseit.
- **Linux-flame.** A Linuxosoktól a szórakozás sem idegen... csak erős idegzetűeknek ajánlott.

A fenti listák ismertetését (szó szerint) a Linux-felhasználók Magyarországi Egyesülete oldaláról (<http://lme.linux.hu/levlista.html>) származik. Az egyesület tevékenysége meghatározó a linux Magyarországi terjedésében:

Az egyesület oldala: <http://www.lme.hu>

Pingvin füzetek: <http://www.lme.hu/meh/pingvinfuzetek.html>

Linux.hu: <http://www.linux.hu>

Sok információt tartalmazó, lényeges oldalak lehetnek még:

Magyar nyelvű anyagok, hogyanok gyűjteménye: <http://linux.vv.hu>

Hasonló oldal az előzőhöz: <http://www.szabilinux.hu>

Szintén: <http://tldp.fsf.hu/HOWTO/HOWTO-INDEX/>

FSF.hu Alapítvány: <http://www.fsf.hu>

Linuxos linkek: <http://www.linuxbazis.hu>

Hírek, információk: <http://www.hup.hu>

SuLinux levelező lista: <http://sulinux.wmszki.hu>

Linuxvilág magazin: <http://www.linuxvilag.hu>

## 1.2 Internet

Az Internet működésének alapja a közös szabványokon alapuló kommunikáció. Ezeket a szabványokat nagyrészt a protokollok leírásai alkotják. Ha valaki el szeretne mélyedni a témában, nézzen utána az IETF (Internet Engineering Task Force) által kiadott RFC dokumentumokban (<http://www.ietf.org>). Például az Internet Protokoll (IP) leírása a rfc760, amely 1980-ban látta meg a napvilágot.

A 60-as, 70-es években a Pentagon megbízásából elindult az ARPANET fejlesztése. Alapkritériumok a következők voltak:

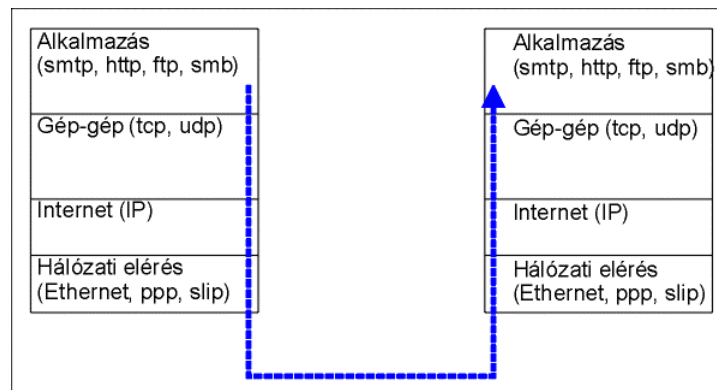
- Nem lehet centralizált, azaz nem rendelkezhet semmilyen központtal a rendszer.
- Hibatűrőnek, redundánsak kell lennie, azaz egy-egy hálózati eszköz leállása esetén alkalmas legyen alternatív útvonalak használatára.
- Többfeladatosnak kell lennie, azaz egy gépnek több géppel is kommunikálnia kell egyidejűleg.

- Aszinkron módban kell működnie, azaz az adatok küldése és fogadása egymástól független legyen.

1980-ban már a TCP/IP szabvány létezett, ez alapján megindult a Berkley egyetemen UNIX alá történő beillesztése. Mivel az amerikai törvények szerint az államilag fejlesztett megoldások az amerikai állampolgárok tulajdona, a TCP/IP szabvány szabadon használható lett. Szintén szabadon használható volt a Berkley egyetem által kifejlesztett UNIX-os megvalósítása. Ez nagyban elősegítette az elterjedését. Az egyetemeken elindult a hálózatok kialakítása, majd ezen hálózatok egyetemek közötti összekapcsolása. CSNET néven jött létre az amerikai egyetemeket összekapcsoló hálózat (később NSFNET). Majd a TCP/IP elterjedése következtében létrejött az a hálózat, melyet Internet néven ismerünk.

## 1. ARPA verem rétegei

A TCP/IP kliens-szerver alapú kommunikációját az ARPA verem modellezi. Amíg a szabvány OSI modell 7 rétegből áll, addig az Interneten használt ARPA verem



modellje csak 4 réteget jegyez:

- **Alkalmazás réteg.**  
Az alkalmazások a saját protokolljaik szerint összeállítják a küldendő adatot. Ezen a szinten beszélhetünk olyan protokollokról, mint az **SMTP**, a **HTTP**, a **POP3**, stb.
- **Gép-gép réteg.**  
Ez a réteg szabályozza a hálózati átvitelt. Ezen a szinten három protokollról beszélhetünk:
  - **TCP** (Transmission Control Protocol)  
Az adatokat, a küldő gépen kisebb csomagokra (datagram) bontja, az adatátvitel megkönnyítésére. A fogadó gépnél ez a szint gondoskodik a csomagok összeillesztéséről. Az alkalmazások jellemzően ezt a protokollt használják.
  - **UDP** (User Datagram Protocol)  
A gépek közötti egyszerű üzenetcsereét valósít meg, egyetlen csomag (datagram) segítségével. Hálózati üzemeltetési feladatok ellátására alkalmazzák.
  - **ICMP** (Internet Control Message Protocol)

Vezérlő üzenetek küldésére alkalmas protokoll. Hálózat működésének vizsgálatára alkalmazzák, mint például a ping üzenetek (ICMP\_ECHO\_REQUEST, ICMP\_ECHO\_REPLY).

- **Internet**

Itt csak egyféle protokoll az **IP** (Internet Protocol) dolgozik. Ez a réteg határozza meg, hogy a csomagnak merre kell mennie. Azaz itt kapja meg a csomag a célgép IP címét (erről még lesz szó), illetve azt, hogy melyik interfészen (hálózati eszköz) távozzon.

- **Hálózati elérés**

Ez a réteg gondoskodik a csomagok, az interfész részére ismert protokollra (**Ethernet, PPP, SLIP**) való átalakításáról. Megkeresi a cím IP-vel rendelkező gépet a hálózaton és továbbítja a csomagot a fizikai közegegen keresztül.

Az alkalmazási réteg elkészíti az üzenetet, amelyet egy másik gépnek szeretne elküldeni. A gép-gép réteg kisebb darabokra vágja (TCP-esetén) és datagram-ot (csomagot) készít belőle, azaz ellátja az üzeneteket egy fejléccel. A fejléc tartalmazza többek között:

- Azt az értéket, amely alapján a gép-gép réteg a küldő alkalmazást azonosítja, ez a kiindulási port.
- Azt az értéket, amellyel a címzett alkalmazást lehet azonosítani, ez a célport.
- Egy sorszámot, amely mutatja, hogy a csomag a teljes adathalmazban hol foglal helyet. Ez a sorszám alapján lesznek összerakva a csomagok a célgépen.
- Ellenőrző összeget, amely alapján következtetni lehet az adatok sérülésére.

UDP esetén is hasonló információkat tartalmaz az UDP fejléc, viszont az alkalmazás adatai nem lesznek eldarabolva.

Az így létrehozott csomagok átkerülnek az Internet réteghez. Itt szintén egy fejléccet kapnak, így kialakítva IP csomagokat. Az IP fejléc érdekesebb adatai:

- IP protokoll verziója.
- Csomag hossza.
- Tovább lépési idő (TTL).
- Gép-gép réteg protokolljának a kódja. (6-TCP, 17-UDP)
- Ellenőrző összeg.
- Forrás IP címe.
- Cél IP címe.

A hálózati réteg az így megalkotott IP csomagot eljuttatja a megadott célgéphez.

Amikor a címzett fogad egy csomagot, a hálózati réteg átadja az Internet rétegnek. Itt lefejtődik róla az IP fejléc, és továbbkerül (mint TCP, UDP, vagy ICMP csomag) a gép-gép réteghez. Ez a réteg a célport alapján a megfelelő alkalmazásnak átadja a csomagokból összeállított üzenetet.

Az alkalmazási rétegen több protokoll is beszélhetünk. A gép-gép réteg, a csomag fejlécében rögzített célportra juttatja el a csomagot, ahol egy alkalmazás (szolgáltatást kiszolgáló szerver) figyel. A kapott csomagot az alkalmazás megpróbálja feldolgozni. Természetesen csak akkor sikerülhet, ha általa ismert szabvány (protokoll) alapján készült.

Ugyan állítható, melyik portot figyelje az adott alkalmazás, de mindegyiknek megvan a jellemző (alapértelmezett) portja. Ezek alapján párosítható az alkalmazás típusa, a fogadóport és a protokoll. Nézzünk ezek közül néhány ismertebbet:

<b>Port:</b>	<b>Protokoll:</b>	<b>Alkalmazás:</b>
21	ftp	Fájlletöltő szerver, pl.: proftpd
22	ssh	Security Shell szerver, pl.: sshd
23	telnet	Telnet szerver
25	smtp	Mail szerver, pl.: sendmail
53	dns	Name szerver, pl.: bind 9
80	http	Web-szerver, pl.: apache
110	pop3	Levelek letöltése, pl.: popper, ipop3d
113	ident	Ident szerver
143	imap	Levelek kezelése. Imap szerver
443	https (ssl+http)	Web-szerver, pl.: apache (titkosított)
993	ssl+imap, tsl+imap	Levelek kezelése (titkosított)
995	ssl+pop3, tsl+pop3	Levelek letöltése (titkosított)

A fenti listában láthatunk, olyan protokollokat is amelyet beágyaztak egy ssl titkosítási protokollba. Ebben az esetben, a fogadó szerver alkalmazás, először az ssl csomagot bontja, majd értelmezi a bele ágyazott saját protokollt.

## 2. IP címek

A későbbiek megértéséhez nézzük meg, mi az IP cím. Az Internetre kötött gépeknek, hogy a részükre küldött csomag meg is érkezzon, egyedi azonosítóval kell rendelkezniük. Ezeket az egyedi azonosítókat nevezzük a gép IP címének.

Az IP cím 32 bit hosszú számsor, melyet jellemzően byte-onként ponttal elválasztott formában írunk. Például: 195.199.67.88. Ezek alapján minden (ponttal elválasztott) szám nullától 255-ig terjedő értéket vehet fel.

Az IP címek kiosztása a Network Information Center (NIC) feladata. Persze ez a nemzetközi szervezet nem ad IP címet minden egyes felhasználó részére. Jellemzően egy-egy címcsoporthoz ad ki szolgáltatóknak, melyet később a szolgáltató oszt tovább. ([http://www.nic.com/nic\\_info/whois.htm](http://www.nic.com/nic_info/whois.htm))

A rohamosan növekvő igény az Internetre és ezzel az IP címekre, már a 90-es évek elején megmutatta a jelenleg használt IP szabvány nagy hiányosságát. Ugyanis napjainkban már kezd elfogyni a rendelkezésre álló IP cím. Ezért 1992-ben megkezdtek egy új szabvány, az IPV6 (más néven IPnG) kidolgozását. A korábbi 32 bites helyett már 128 bites címet használ. A fejlécformátum egyszerűsödik. Azonosítást és kódolást használhat. Multimédia átvitelére alkalmas képességekkel rendelkezik. Ugyan nagy munkálatok folynak ebben a témában, még nem állt össze a kép teljesen. Jelenleg az átállással kapcsolatos problémákon dolgoznak.

Természetesen az IP címek nem önálló számok, hanem pontosan meghatározott halmazokra vannak bontva. Ezek egy része speciális célra van lefoglalva, a többit pedig hálózati osztályokba rendezik.

Az osztályokra bontásnál a szempont, hogy a 32 bitből mennyi vonatkozik az adott hálózatra és mennyi az adott hálózaton elhelyezkedő gépekre.

- 'A' osztályú hálózat: Az IP címből 7 bit határozza meg a hálózatot és 24 bit a hálózaton található gépeket. 125 ilyen hálózat létezik és egy-egy hálózaton 16 777 216 gép létezhet. Ilyen címtartományt a NIC csak olyan nagy hálózatoknak oszt ki, mint például az IBM. Ezen hálózatok IP címeinek első számjegye 1 és 127 közé esik.
- 'B' osztályú hálózat: Az IP címből 16 bit határozza meg a hálózatot és 16 bit a hálózaton található gépeket. 16 382 ilyen hálózat létezik és egy-egy hálózaton 65 536 gép létezhet. Ezen hálózatok IP címeinek első számjegye 128 és 191 közé esik.
- 'C' osztályú hálózat: Az IP címből 24 bit határozza meg a hálózatot és 8 bit a hálózaton található gépeket. 2 097 150 ilyen hálózat létezik és egy-egy hálózaton 256 gép létezhet. Ezen hálózatok IP címeinek első számjegye 192 és 223 közé esik.

Az IP címkészletben vannak fenntartott címek is, ilyenek :

- 224.0.0.0 - 239.255.255.255 : Multicasting eljárás számára fenntartva.
- 240.0.0.0 - 255.255.255.254 : Internet saját céljára fenntartva.
- 0.0.0.0 és a 255.255.255.255 : Sajátos feladattal rendelkező címek.
- 10.0.0.0 - 10.255.255.255 : Privát A osztályú tartománynak fenntartva.
- 172.16.0.0 - 172.31.255.255 : Privát B osztályú tartománynak fenntartva.
- 192.168.0.0 - 192.168.255.255 : Privát C osztályú tartománynak fenntartva.

Itt jegyzem meg, hogy az osztályba sorolás elmélete már nem teljesen állja meg a helyét. Ez legfőképpen az Internet szabad szerkezetének és a fogyóban lévő IP címnek köszönhető. Az RFC1918-as szabvány a következő privát címtartományokat említi meg: 10/18, 172.16/12, 192.168/16.

A privát címeket, olyan hálózatok számára tartják fent, amely nincs közvetlen kapcsolatban az Internettel, de IP protokollt használ. Ilyenek lehetnek a lokális hálózatok. Privát IP címmel rendelkező gépet tehát nem lehet Interneten keresztül elérni.



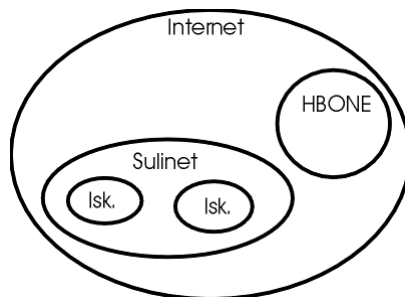
A fentiek alapján kiosztott IP cím tartományok természetesen további alhálózatokra oszthatóak. A Sulinet esetében is így történt. A Sulinetes IP címek első számjegyéből megállapítható, hogy C osztályú címről van szó (melyből a Sulinet többel is rendelkezik.). Ezek tovább lettek bontva, így egy-egy iskola 16 IP címet használhat. Tehát a 32 bitből 28 bitet a hálózat meghatározására használnak, 4 bitet pedig az egyes gépek címzésére.

A hálózatok meghatározásánál szükségünk van a hálózat IP címére és a hálózati maszkra. A hálózat IP címe mindig a hálózatban használható legelső IP. A hálózati maszk pedig olyan IP cím formátumban leírt 32 bites szám, melynél a hálózat meghatározására használt bitek 1-el, míg a gépek meghatározására szolgáló bitek 0-val vannak feltöltve. Amennyiben hálózatra hivatkozunk, az Hálózat Címét a hálózati maszktól / jellel elválasztva tesszük. Nézzünk néhány példát:

- 'A' osztályú hálózat: 116.0.0.0/255.0.0.0
- 'A' osztályú privát hálózat: 10.0.0.0/255.0.0.0
- 'B' osztályú hálózat: 184.17.0.0/255.255.0.0
- 'B' osztályú privát hálózat: 172.17.0.0/255.255.0.0
- 'C' osztályú hálózat: 195.199.56.0/255.255.255.0
- 'C' osztályú privát hálózat: 192.168.8.0/255.255.255.0
- Bontott hálózat: 195.199.57.128/255.255.255.240 (16 IP)

### 3. IP hálózatok

Már a fentiekből is feltételezhető, hogy az Internetre kötött számítógépeket hálózatokba csoportosítjuk. A hálózatok kialakítását meghatározhatja a szolgáltatóunktól (vagy a NIC-től) kapott címtartomány. Természetesen a rendelkezésre álló címtartományt saját hálózatunkon belül tovább bonthatjuk.

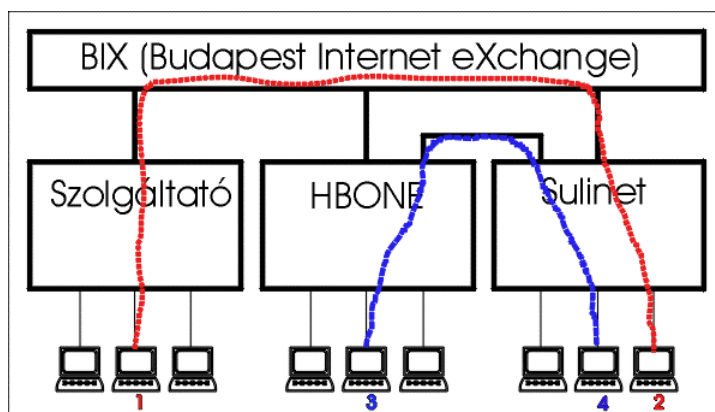


Az Internet gyakorlatilag a fenti elvekkel kialakított hálózatok halmaza. Ezen hálózatok összeköttetésben lehetnek egymással. Két jellemző hálózat létezik. Az egyik a nemzetközi gerinchálózat, a másik az országokon belül kialakított gerinchálózat. Magyarország gerinchálózat, ismertebb nevén BIX (Budapest Internet eXchange), egy gyors átvitelre rendelkező központ, kapcsolatot biztosít a szolgáltatók

között.

A szolgáltatók, egyrészt a BIX-re kapcsolódva biztosítják más magyar szolgáltatók elérhetőségét, másrészt nemzetközi kapcsolatokkal is rendelkeznek. A BIX-re kapcsolódó tagok listáját elérhetjük a <http://www.bix.hu/index.php3?lang=hu&page=members> címen. Nem ritka, hogy a szolgáltatók egymás között is kialakítanak átkötést, ezzel is tehermentesítik a BIX felé menő vonalukat.

A mi szempontunkból két érdekes hálózatot (szolgáltatót) szükséges kiemelni. Az egyik a Sulinet, amely a hazai általános és középiskolák számára nyújtja az Internet kapcsolatot. A Sulinet hálózat felépítését a <http://www.sulinet.hu/info/uzemeltetes/terkep.html> címen találhatjuk meg. A másik a HBONE, amely a felsőoktatási intézmények kapcsolatát biztosítja. (<http://www.hungarnet.hu/index.php?headline=infra&menu=menu-kapcs.html&text=infra1.html>)



A fenti ábra mutatja két Internetre kapcsolt gép közötti kapcsolatot. Láthatjuk, hogy a 1-es és a 2-es gép közötti kommunikáció a BIX-en megy át, míg a 3-as és 4-es gép a két szolgáltató között kialakított vonalon lép egymással kapcsolatba.

#### 4. Routerek

A különböző hálózatok közötti kapcsolatot, úgynevezett útvonalválasztók (router-ek) biztosítják. Ha egy csomag címzettje nem található meg a hálózaton, akkor a hálózaton lévő router kapja meg a csomagot továbbküldés céljából. A hálózaton elhelyezett gépek szempontjából ezt a router nevezzük alapértelmezett átjárónak (default gateway).

A router a megkapott csomagokat továbbküldi. Azt, hogy mégis merre küldje ezeket, egy táblázat alapján határozza meg, melyet routing táblának nevezünk.

Routing tábla:

Célhálózat	Hálózati maszk	Átjáró	Interfész
196.12.80.0	255.255.255.0	-	eth0
210.85.60.0	255.255.255.0	-	eth1
198.166.40.0	255.255.255.0	196.12.80.10	eth0
0.0.0.0	0.0.0.0	196.12.80.20	eth0

A fenti táblázatban található egy router 'routing táblája'. Látható, hogy a routernek két kapcsolata van, ezek az eth0 és eth1 hálózati interfészek. A 196.12.80.0/255.255.255.0 hálózatra címzett csomagokat egyszerűen kiadja a eth0 interfészre kapcsolt hálózatra, hiszen a címzett ott található. Szintén így tesz a 210.85.60.0/255.255.255.0 hálózatra címzett csomagokkal, csak az eth1-es interfészen keresztül. A 198.166.40.0/255.255.255.0 hálózatra címzett csomagokat továbbadja egy másik routernek, konkrétan a 196.12.80.10-es címre hallgatónak, további feldolgozásra. Amennyiben a címzett a fent említett hálózatoknak nem tagja, úgy a csomag a 196.12.80.20-as címen lévő routerre kerül, ami elvégzi a továbbküldését.

A routing táblát négyféle információ alapján készíti a router:

- Közvetlen az interfészeire kapcsolt hálózatok adataiból,
- Kézzel beállított adatokból (statikus route),
- A környezetében lévő routerektől kapott adatokból (dinamikus route)
- Alapértelmezett átjáró adataiból.

A statikus route-ot kézzel tudjuk beállítani, míg a dinamikus route-ot erre a célra készített router protokollokon keresztül építi fel és folyamatosan frissíti a routerünk.

Az Interneten a feladó és a címzett között akár több útvonalválasztó is elhelyezkedhet. Nézzük meg, hogy egy veszprémi középiskolából a Veszprémi Egyetem webszerveréig hány routeren megy keresztül a csomag (traceroute [www.vein.hu](http://www.vein.hu)):

- router.iskola.sulinet.hu (Iskola saját routere, cisco)
- 195.199.0.137 (Itt már a Székesfehérvári sulinet központban vagyunk.)
- 195.199.2.1
- 195.199.0.57 (Ez már biztosan a Budapesti sulinet központ)
- gsr16-sulinet.vh.hbone.hu (Átkerültünk az egyetemi hálózatra)
- c6k-c72.veszprem.hbone.hu
- c72-c6k.veszprem.hbone.hu (Megtaláltuk a Veszprém felé vezető utat)
- proxy2.vein.hu (Ez már az egyetem bejárata)
- almos.vein.hu (Megvan a webszerver)

Térjünk egy gondolatra vissza az IP fejlécben tárolt adatokra. Minden IP csomag kap egy TTL-t (Továbblépési idő kódot). Ez egy 0 és 255 közé eső szám. Amennyiben a csomag áthalad egy routeren a TTL értéke egyel csökkenni fog, ha eléri a nulla értéket, akkor a csomag megsemmisül. Erre azért van szükség, mert a Internet szerkezetéből adódhat, hogy egy csomag nem érkezik meg a címzethez, hanem a routerek között kering egy zárt hurokban kísértetként. A TTL alkalmazása nem ad erre lehetőséget.

## 5. Névfeloldás az Interneten

Mint, már említettük, az Internetre kötött összes gép rendelkezik egyedi azonosítóval. Ez alapján címezzük a csomagot a gép részére. Mivel ezek megjegyzése nehézkes, a kliens programoknál neveket használunk az egyes gépek azonosítására, melyeket domain neveknek nevezünk. A domain név alapján mindig meghatározható a célszámítógép IP címe. A domain név használatának több előnye is lehet:

- Könnyen megjegyezhető, informatív.
- Amennyiben egy gépet áthelyezünk egy másik hálózatra, az IP címét meg kell változtatnunk, viszont a neve állandó maradhat.
- Több domain nevet rendelhetünk hozzá egy IP címhez, ezért, például, egy szerver több cég, szervezet weboldalait kiszolgálhatja.



A domain neveknek ponttal elválasztott szövegrészekből állnak össze. Értelmezésük jobbról balra történik. Jobb felől az első szintű domainnal kezdődik és baloldalon a konkrét gép nevével zárjuk. Kitüntetett elemei a következők:

- top-level (első szintű, TLD) domain. A domain típusát, vagy a országot határozza meg.
- Second-level (másodsztintű, SLD) domain. A hálózat nevét adja meg. Általában a cég nevére, vagy a szolgáltatás témájára utal.
- host name (gép neve). Az egyedi gép neve az adott hálózatban.

Nézzünk példákat az egyszerű domain névre:

- www.sulinet.hu
- www - host name
- sulinet - second-level domain
- hu - top-level domain
  
- mail.ibm.net
- mail - host name
- ibm - second-level domain
- net - top-level domain

Aldomain-t használó példa:

- pc12.iskola-varos.sulinet.hu
- pc12 - host name
- iskola-varos – aldomain
- sulinet - second-level domain
- hu - top-level domain

Tehát a domain név a gép nevével kezdődik, majd az aldomain lista következik (nincs megkötve hány elemből áll), végül a másodsztintű és első szintű domain.

A top-level domainokat a ICANN hozza létre és adja ki a kezelését szervezeteknek. Ilyen első szintű domaineik lehetnek:

- .com - Üzleti domaineik
- .edu - Oktatási intézmények
- .gov - Állami intézmények
- .int - Nemzetközi szervezetek
- .net - Nem NIC által kezelt domaineik
- .museum - Múzeumok

Szintén első szintű domainnal rendelkezik minden ország. Pl.:

- .hu – Magyarország
- .pl – Lengyelország
- .it – Olaszország
- .de - Németország

Az első szintű domainekről bővebb információt találhat a <http://www.icann.org> oldalon.

Tehát minden első szintű domaint valamilyen szervezet kezel. A .hu domaint az Internet Szolgáltatók Tanácsa (ISZT Kht.) kezeli. Minden .hu alatt lévő másodszintű domain bejegyzését náluk kell kezdeményezni. A másodszintű domain részére két egymástól független hálózaton található name szerveren kell nyilvántartani (elsődleges és másodlagos DNS). Amennyiben a bejegyzésnek nincs akadálya, úgy a .hu domain name szerverébe rögzítésre kerül a másodszintű domain neve és az azt nyilvántartó két DNS IP címe. A .hu alá bejegyzett domaineik, és a bejegyzés szabályai a <http://www.nic.hu/> oldalon olvashatóak.

A másodszintű domainok alatt lévő host-okat, vagy további aldomainokat a másodszintű domaint igénylők saját name szerverekkel oldják meg.

A fentiekből is már sejteni lehet, hogy a domain információkat domain name szerverek (DNS) tárolják. Ezek a szerverek felelősek a domainnevek IP címmé történő átalakításáról, illetve az IP címekre bejegyzett domain nevek meghatározásáról (rev DNS). Ezt a folyamatot nevezzük névfeloldásnak.

A névfeloldásnál a kliens először az INTERNIC által üzemeltetett központi DNS-ekhez fordul, melyek tájékoztatják, hogy a top-level domain nyilvántartása melyik DNS-en történik. A kliens, a már ismert, top-level nyilvántartó szerveréhez fordul, amely megadja, hogy mi a domain (second-level) name szervere. Végül ettől a szervertől megkapja a kért IP címet.

Ez a folyamat igen időigényes és nagyon gyakori. Ezért a hálózatokon létre szoktak hozni caching DNS szervereket, amelyek közel vannak a kliensekhez, így az elérésük gyorsabb. A kliensek ezektől kérik a névfeloldást, és ezek hajtják végre a fenti folyamatot. Közben az adatokat eltárolják. Ha ismert domainnak kérik a kliensek az IP címét, akkor az már a saját adataikból szolgálják ki. Természetesen ezen adatok érvényességük idejűk lejáráskor frissülniük kell.

Napjainkban egyre több program védekezik a DNS információk hamisítása ellen. Ennek a legjobb megoldása, hogy az IP címhez tartozó domain nevet lekéri, majd lekéri a kapott domain név IP címét. A kiinduló és az eredmény IP címnek azonosnak kell lennie. Ez az eljárás a mi szempontunkból azért jelentős, mert a lokális hálózaton nem gyakori a saját DNS szerver, amelyben nyilván tartjuk a privát IP címekhez rendelt hoszt nevét. Ebben az esetben viszont ezen a hálózaton működő szervernek az ellenőrzése hibás lesz. Ilyent tapasztalhatunk például mysql szerver kívülről történő elérésénél. A hibát ki lehet küszöbölni a kérdéses gépek felvételével a hosts fájlba.

## 1.3 Védelem

Amikor egy Internetre közvetlenül csatlakoztatott gépet (szervert) telepítünk, lényeges szempont, hogy miképpen óvjuk meg az identitását. Minden alkalmazás, szolgáltatás kiválasztásánál, a beállítások tervezésénél ez az elsődleges szempont. A védelem és a biztonság a leglényegesebb kérdés, amely átítatja teljes munkánkat.

Az Internettel kapcsolatban lévő gépeknél minden esetben érdemes feltenni a következő kérdéseket:

- Mennyire védett a külső behatolások ellen?
- Mennyire védett a vírusok, férgek, trójai programok ellen?
- Hogyan vesszük észre, ha a rendszerfájlok megváltoznak, módosítják őket?
- Hogyan vesszük észre, ha betörési kísérlet, vagy valós betörés történt?

Természetesen ezekre a kérdésekre a válasz az alkalmazott technológia, programok és a tervezés részleteiben található.

Fontos továbbá, hogy a rendszerben és adatainkban kárt okozó esemény nem csak az Internet felől érkezik. Védekeznünk kell a belülről (intézmény területéről) érkező tudatos és nem tudatos támadások ellen is. Azaz a rendszerünket (gépünket) a saját felhasználóinktól és saját magunktól is védeni kell.

## 6. Tűzfalak

A tűzfalakkal a védendő gép, rendszer biztonságát növeljük a hálózati kommunikáció szintjén. Természetesen egy-egy gépre is elhelyezhetünk tűzfalat, de a központi adminisztráció miatt elsősorban a hálózati csomópontokon szokás védeni egy rendszert.

Amennyiben egy intézményi hálózatot kívánunk védeni, fontos az előtervezés. A rendszer felépítésének és az engedélyezett szolgáltatások tervezése mindig az adott intézmény informatikai stratégiájából indul ki, arra alapul.

A következőkben átnézzük a tűzfal rendszereknek a felépítését lépésről-lépésre. Itt kell megjegyeznem, hogy a védelmi rendszerek tervezéséről komoly szakirodalom létezik. Az itt leírtak nem terjednek ki mindenre, erre nem is lenne lehetőség. Ezért az itt leírtakon túl érdemes még utána nézni a konkrét megvalósításnak.

## 7. Tűzfalak típusai

A tűzfalakkal különböző típusokról beszélhetünk. Lényeges, hogy a rendelkezésre álló lehetőségekből a lehető leghatékonyabbat használjuk.

**Bastion host:** Egy megfelelően védett szerver. Egyaránt kapcsolódik a lokális hálózatunkra és az Internetre is. Viszont nem végez csomagtovábbítást. Amennyiben belső hálózatunkról használni szeretnénk az Internetet, úgy be kell jelentkeznünk a

Bastion Host-ra és ezen futtatni a kliens programot. Tehát ez egy olyan kliens gép, amelyről használhatjuk az Internetet és lehetőséget biztosít arra hogy terminálról rájelenkezünk.

**Csomagszűrés (Packet filtering):** A bejövő, kimenő és áthaladó (router esetén) csomagokat szűri a Internet és gép-gép rétegen (ARPA verem) rétegen. Azaz megnézi az IP és a TCP, ICMP, UDP csomagok fejlécét és a feltételek alapján meghatározott minták szerint szűr.

**Továbbfejlesztett csomagszűrés (Stateful Packet filtering):** A hagyományos csomagszűrés hiányosságait javították benne. Például követik a töredécsomagokat. Tiltják a kapcsolathoz nem rendelhető csomagokat. Kis mértékben az adatmező tartalmát is ellenőrzik.

**Alkalmazás szintű átjáró (proxy) tűzfal:** Proxy-k összessége. A proxy-k olyan speciális programok, amelyek adott alkalmazás szintű protokollon közvetítenek a kliens és a szerver között. Nem továbbítanak csomagot, tehát nem képeznek közvetlen kapcsolatot a két kommunikáló fél között. Ennek a felépítésnek köszönhetően aktívan képesek szűrni és ellenőrizni az alkalmazási réteg szintjén, hiszen a datagramokat összeillesztve egybe vizsgálják az adatokat.

**Moduláris alkalmazás szintű tűzfal:** Napjainkban egyre elterjedtebb, hogy az alkalmazási rétegen több egymásba ágyazott protokollt használunk. Ilyen lehet az SSL-be ágyazott HTTP is, azaz a HTTPS. Ebben az esetben az SSL kapcsolatot vizsgáló proxy az alprotokollra is meghív egy másik proxy-t. Tehát a modulárisan felépített proxy-k egymásba ágyazásával a szállított adatok legmélyebb szintjét is képesek vizsgálni.

## 8. Tűzfal helye a hálózatban, a hálózat felépítése

A hálózat megtervezésénél sajnos a költségtényezők is szerepet játszanak. Viszont egy rosszul felépített védelem következtében, a károk értéke és a hibajavítás költsége, a többszöröse lehetnek a kiépítés költségének. Ezért fontos, hogy a tervezésnél a legnagyobb körültekintéssel, lehetőleg kompromisszumok nélkül járjunk el.

Sokszor tapasztalom, hogy egy rendszer tervezésénél az elsődleges cél az Internet elérés megléte. A biztonság csak ez után következik. Pedig egy biztonsági hibával rendelkező rendszer üzemeltetésével nem csak magunknak, de MÁSOKNAK IS KÁRT OKOZHATUNK. Ilyen eset lehet, amikor vírusfertőzést kapunk és az észrevétlenül továbbterjesztjük, vagy a feltört szerverünk segítségével (és az mögé elbújva) törnek fel más szervereket.

Amennyiben biztonságilag nem megfelelő rendszert tudatosan üzemeltetünk, az kimerítheti a szándékos károkozás fogalmát is. Ezért, ha felmerül a rendszerünk sérthetősége, haladéktalanul szüntessük meg a kapcsolatot a hibás rész és az Internet között a probléma elhárításáig.

Mivel nincs lehetőség több variáció megjelenítésére, ezért a továbbiakban egy iskola szintű szervezet igényeit kiszolgáló optimális rendszer felépítését tárgyaljuk. Természetesen ezt egyszerűsíteni és bonyolítani is lehet.

A iskola szempontjából a következő szolgáltatásokat kell biztosítanunk.

- Internet elérése az iskola belső hálózatáról (tűzfal, router)
- HTTP, HTTPS elérése, azaz Interneten található honlapok látogatása.
- FTP elérése, azaz fájlok letöltése.
- IRC, ICQ elérése, azaz chat.
- Egyéb meghatározott protokollok.
- Levelek (POP3) letöltése az iskola e-mail szerveréről.
- Levelek küldése az iskola e-mail szerverén keresztül.
- Iskola címére érkező levelek fogadása az Internet felől.
- Iskola honlap szolgáltatása az Internet felé.
- Fájlszerver az iskolai belső hálózatának.

Természetesen ezeket a feladatokat technikailag meg lehet oldani 1 kiszolgálóval is (1997-es Sulinet modell), viszont ez biztonságtechnikailag nem jó megoldás. Ráadásul az 1 szerveres megoldás üzemeltetés szempontjából sem kívánatos.

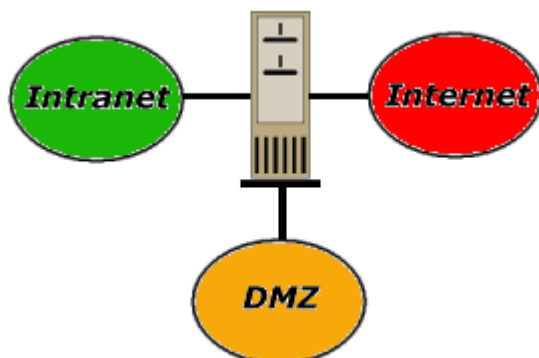
Mindenképpen külön szerverre érdemes tenni a következő szolgáltatás csoportokat:

- **Tűzfal.** Minden rá telepített szolgáltatás további lehetőséget biztosít a betörésre. Ezért a tűzfalak csak a legszükségesebb csomagokat tartalmazzák. Például a tűzfalra telepített web-szerver esetén a web-szerver minden biztonsági hibája növeli a tűzfal sérthetőségét. A másik indok, hogy a tűzfalak telepítésére külön Linux disztribúciók, biztonságosabb egyedi megoldások is léteznek. (pl. UHU FIREWALL, ASTARO, IPCOP) Ezeket a disztribúciókat könnyebb telepíteni és beállítani.
- **Fájlszerver.** A tárolt adatok fokozott védeltséget kívánnak. A fájlszerver szolgáltatás csak a belső hálózat felé kell eszközölni (külső elérés esetén VNP használatánál is ez a helyzet). Még lényeges indok lehet, hogy a fájlszerver és csoport munka szolgáltatás jellemzően a leginkább hardver igényes és operációs rendszer választásának szempontjából eltérhet az Internet kiszolgálóktól, tűzfalaktól.
- **Internet kiszolgálás.** Ebbe a csoportba az iskola e-mail és webszervere tartozik. Ezeket a szolgáltatásokat szintén külön gépre szokás tenni. Biztonsági szempontból célszerű lehet tovább bontani és az e-mail szervert leválasztani minden más Internet felé irányuló szolgáltatásról, hiszen az felhasználók levelei szintén fokozottan védett adatnak számítanak.

Ez tehát minimum 3 különböző szervert (gépet) igényel. Ez azért is lényeges mert a gépek helye is máshol található a rendszeren. Tehát nézzük az így kialakult rendszert:

A Tűzfal három hálózati kártyával rendelkezik, így három hálózatra kapcsolódik. Ezek a hálózatok a következők:

**Internet.** Minden ami a védett hálózaton kívül helyezkedik el. Kezdvé a Sulinet által biztosított, publikus IP címekkel rendelkező iskolai szegmenstől a router-en keresztül az Internetig.



**Intranet.** Az iskola belső hálózata. Az iskola összes kliensét tartalmazza. Itt található a fájlserver is.

**DMZ.** Mindkét hálózattól védett zóna. Ide kerülnek a védendő szerverek, például a web-szerver és az e-mail szerver, esetleg FTP szerver. A védetség szempontjából itt is lehetne a fájlserver, de ezt nem célszerű amennyiben

csoportmunka kiszolgálóról van szó, vagy VPN-t használunk.

A tűzfal tehát védi az Intranet hálózatunkat az Internet felől érkező támadások ellen és a DMZ hálózatot mindkét helyről. Az Intranet hálózaton elhelyezett fájlservert érdemes ellátni a fájlserveren futó tűzfal védelemmel, hiszen a belső hálózatról is érheti támadás. A DMZ hálózaton nincsenek kliensek, ennek ellenére az Internet felé szolgáltató (itt elhelyezkedő) szervereket is el szoktuk látni csomagszűrő védelemmel.

Az így kialakított 3 zóna esetében már meghatározható a tűzfal működése, azaz felvázolható, hogy a zónák között milyen alkalmazás szintű forgalmat engedjen.

TO FROM	Intranet	Internet	DMZ	Tűzfal
Intranet		HTTP, HTTPS, FTP, IRC, SSH	HTTP, HTTPS, POP3, POP3S, SSH	DNS, SMTP, NTP, SSH
Internet			HTTP, HTTPS, POP3S	SMTP, DNS
DMZ				SMTP, SYSLOG
Tűzfal	SYSLOG	SMTP, DNS		

Ezt egy szolgáltatási mátrix táblázatba vázoljuk. A fenti szolgáltatási mátrixból kiolvashatóak, hogy:

- Az Intranet (belső) hálózatról az Internet felé kell http, https, ftp, irc, ssh elérés. Tehát a belső hálózaton lévő felhasználók szeretnének weboldalakat nézni (http, https), fájlokat letölteni (ftp), chetelni (irc), és bejelentkezni más szerverekre (ssh).

- Az Intranet (belső) hálózatról a DMZ zóna felé kell http, https, pop3, pop3s, ssh. Tehát a belső hálózaton lévő felhasználók szeretnék letölteni a leveleiket az intézmény mail szerveréről (pop3, pop3s), szeretnék látni az intézmény weboldalát (http, https), szeretnék adminisztrálni az dmz szervereket (ssh).
- A tűzfal az Intranet (belső) hálózat felé szolgáltat dns-t és ntp-t, lehetőség van az elérésére adminisztráció végett (ssh). Továbbá fogadja a belső hálózatról küldött leveleket, amelyeket ellenőrzés után célba juttat (smtp). Ezek alapján a tűzfal dns és ntp cache-ként és smtp proxy-ként működik.
- Az Internetről Az Intranet felé NEM ENGEDÉLYEZÜNK FORGALMAT. Csak a válasz csomagokat továbbítjuk DNAT alapján.
- Az Internetről a DMZ zóna felé engedélyezzük a http, https csomagokat, hogy az intézmény weboldalát elérjék kívülről, és engedélyezzük a mail szerverről a levelek letöltését, de csak titkosított pop3 kapcsolattal.
- Az Internetről a tűzfalra érkehetnek levelek, amelyeket továbbít a DMZ zónában lévő mail szervernek (smtp), illetve engedélyezzük DNS információk lekérését (csak akkor lényeges, ha publikus DNS szerverünk üzemel).
- A DMZ zónában lévő szerverekről kifelé történő e-mail küldést a tűzfal fogadja és küldi tovább. Továbbá a log állományokat is fogadja.
- A tűzfal az Intranet felé továbbítja a DMZ zónában keletkezett log állományokat.
- A tűzfal az Internet felé továbbíthat leveleket (smtp) és kérhet DNS információkat.

Nagyjából erről szól a szolgáltatás mátrix. Ez alapján a védelem megtervezése könnyebbé válik.

Az Intranet (belső) hálózatot is lehet további zónákra bontani. Ennek jelentősége abban rejlik, hogy az intézmény, olyan csoportokra bomlik, amelyek más-más szolgáltatásokra van igénye (engedélye). Ilyen zónák lehetnek:

- Hálózat-, szerveradminisztrátorok gépei
- Tanári, gazdasági gépek
- Tanulói gépek

Az így kialakult zónákat érdemes külön alhálózatokkal jelezni.

## **1.4 Telepítéshez szükséges alapismeretek**

A továbbiakban elsősorban a DMZ zónában lévő szolgáltató szerverekkel foglalkozunk. Pontosabban egy szerverrel, amely nyújtja a szükséges szolgáltatásokat. Telepítés előtt érdemes átgondolni, milyen programok kerüljenek rá, milyen legyen a partíció kiosztása, mik a szükséges adatok a telepítéshez.

A telepítés tervezésénél, illetve a további fejezetekben a Sulinet (1997) egy szerveres modelljét vesszük alapul. Azaz minden szolgáltatást egy kiszolgáló végez. Ez a megoldás az előzőekben leírtak miatt nem megfelelő, sőt, elkerülendő, de a tanfolyam lehetőségei és a gyakorlás végett célszerű.

## 9. Partíciók

A partíciók meghatározása az egyik leglényegesebb eleme a szerver kialakításának. Két szempontból érdemes partíciókra bontani a rendszerünket:

- Vannak olyan területek, melyeken tőlünk független, változó méretű adatokat tárolunk. Ilyenek lehetnek a log-állományok (/var/log), a felhasználó könyvtárak (/home), az ideiglenes állományok (/tmp, /var/tmp). Ezek esetlegesen megtelhetnek, de ha külön partíción vannak, akkor nem befolyásolják kritikusan a rendszer működését.
- Különböző könyvtárakban más-más stílusú adatokat tárolunk. A partíciókat ennek megfelelő jogosultságokkal kezelhetjük. Például megtilthatjuk róla a program futtatást (noexec), vagy írásvédetté tehetjük (ro). Ezen beállításokkal tovább fokozhatjuk rendszerünk biztonságát

Nézzük meg, egy Linux rendszer könyvtárszerkezete, milyen lényeges részekből áll.

- /boot könyvtár. Ebben tároljuk a kernelt. A későbbiekben tárgyalt boot loader innen indítja a rendszerünket. Mindenképpen elsődleges partícióként vegyük fel, lehetőleg a meghajtónk elejére. Nem tartalmaz változó adatokat, ezért írásvédetté tehető (ro). Nem fogunk róla programokat sem futtatni (noexec).
- / könyvtár, azaz a gyökérkönyvtár. A külön nem tett könyvtárakat fogjuk itt tárolni, ebbe a könyvtárszerkezetbe fogjuk felfűzni a többi partíciót.
- /usr könyvtár. Szerverünkön ez lesz a legnagyobb helyet igénylő könyvtár a telepítés után. Itt tároljuk a futtatható állományokat és azok kiegészítéseit, azaz a programokat. Telepítés befejezése után írásvédetté tehetjük.
- /var könyvtár. Változó adatokat tároló könyvtár. Jellemzően olyan adatokat tárolunk benne, melyeket a szerveren futó programok használnak. Ide történik a naplózás, itt találhatóak a level Inbox-ok. Ezeket a könyvtárakat a terheltségük és a fontosságuk függvényében szintén érdemes külön tenni. Például a proxy szerver cache könyvtára, ezt folyamatosan használja a squid, ezért nagy terhelésnek lehet kitéve. Érdemes akár külön meghajtóra is elhelyezni.
  - /var/log napló állományok helye
  - /var/www web-oldalak helye
  - /var/spool/squid Squid proxy cache könyvtára
  - /var/lib/mysql mysql adatbázisok könyvtára
  - /var/tmp temporary könyvtár
  - /var/named DNS szerver adatai.
  - /var/spool/mail mail inbox-ok
  - /var/spool/mqueue postázásra váró levelek
- /etc könyvtár. A Linux rendszer és a programok összes beállítása.
- /tmp könyvtár. Ideiglenes fájlok tárolója. (temporary). Lényeges lehet, hogy tiltsunk minden féle futtatást rajta.
- /home könyvtár. Felhasználók könyvtárai. Itt szóba jöhet a bővítés is. Amennyiben a telepítésnél kialakított hely elfogyott, egy másik meghajtó behelyezésével, csak ezt a könyvtárat helyezzük át. Továbbá meg lehet oldani, hogy a /home könyvtárról ne lehessen futtatni állományokat.



Linux rendszereken többféle partíció típust tudunk használni. A legelterjedtebb talán az ext2 típusú normál fájlrendszer. Van lehetőségünk ezenkívül naplózó (ext3) fájlrendszer használatára is. Ez ugyan kicsit lassabb, mint az ext2, de jobban viseli az áramszüneteket és megbízhatóbb. A virtuális memória részére is külön partíciót kell létrehozunk. Ezt célszerű a merevlemez elejére elhelyezni. Méretét a memória méretének kétszeresére (csak a memória háromszorosaig, maximum 2 GB) érdemes felvenni. A virtuális partíció típusa swap legyen.

Ez természetesen nem azt jelenti, hogy csak a fent említett fájlrendszer típusok léteznek. A linux rengeteg egyedileg fejlesztett típussal dolgozik. Érdemes utánanézni, melyek lehetnek számunkra a megfelelőek.

A következő táblázatban egy lehetséges megoldás található:

Csatolási pont	Méret	Típus	Opciók
/	200 MB	Ext3	Default, (ro)
/boot	20 MB	Ext3	Default, ro, nosuid, noexec, nodev
/usr	500 MB	Ext3	Default, ro, nodev
/tmp	100 MB	Ext3	Default, nosuid, noexec, nodev
/var	200 MB - 1 GB	Ext3	Default, nosuid, noexec, nodev
/var/spool/squid	500 MB - 2 GB	Ext3	Default, nosuid, noexec, nodev
/home	500 MB - 2 GB	Ext3	default, nosuid, noexec, nodev, usquota
-	256 MB	swap	-

Opciók:

- noauto. Csak kifejezett parancs hatására csatolódik.
- nodev. Karakteres, vagy blokkos eszközfájlokat nem tartalmazhat.
- noexec. A rajta lévő futtatható bináris fájlok futtatását nem engedi.
- nosuid. Tiltja a suid és a sgid bitek használatát.
- ro. Csak olvasható a fájlrendszer.

A partíciók csatolási beállításainál talán az írásvédettséget kell a legkörültekintőbben kezelni. Ha a /usr könyvtárat írásvédetté tesszük, akkor rosszakaróink nem tudnak trójait becsempészni, de mi sem tudunk csomagokat frissíteni. Ezért ezt az opciót csak tapasztaltabbaknak ajánlom.

## 10. Programok

A programok kiválasztásánál két elsődleges szempont van. Minek nem szabad egy szerveren rajta lenni és milyen programok kellenek a kívánt feladat megoldásához. A tiltott programokat biztonságtechnikai szabályok befolyásolhatják, de jelentős a 'nem használom, ne is legyen fent' elv is.

Sokan kedvelik a kernel és a programok egyedi fordítását. Ehhez C fordító szükséges. Egy C fordítónak viszont semmi keresni valója sincs egy szerveren. A fordítást ezért mindig egy másik gépen végezzük.

2002 augusztusában hódított egy féreg (slapper, cinik, unlock), amely egy OpenSSL hibát használt ki Apache-on keresztül. A forráskódját a /tmp könyvtárba juttatta, lefordította és futtatta. Amennyiben a /tmp könyvtár noexec csatolási opcióval rendelkezik, vagy nincs GCC fordító a szerveren, a férgek nem tud aktivizálódni.

A felhelyezett csomagoknál általában az igényelt szolgáltatást végző programokat szoktuk jegyezni. Természetesen ezeknek a programoknak más csomagokra is szükségük lehet (pl.: A Web-szerver működéséhez szükségesek a hálózat kezelő csomagok). Ezt a kapcsolatot függőségnek nevezzük. A telepítők nagy része a függőségeket kulturáltan kezeli, ezért nekünk elég megadni a feladatainkhoz szükséges ismertebb csomagokat. Természetesen, egy szervernél, a teljes felkerült csomaglistával érdemes valamilyen szinten tisztában lenni, de ezt a tapasztalat hozza magával.

Mi az, ami ne legyen a szerveren:

- GCC, CPP azaz semmi féle C fordító.
- FTP, Telnet, Finger, Talk kliensek és szerverek, azaz régebbi, nem biztonságos szabványok megvalósulásai.
- Rsh, rsync, vagy bármilyen távoli eljárás hívás.
- Semmilyen grafikai, média program, beleértve az X-et is.
- NFS rendszert csak különleges esetekben telepítsünk.
- És általában semmi, ami a telepítést követő 1 héten belül nincs elindítva. ☺

Mi az, ami legyen egy szerveren? Természetesen ezt csak a feladatok tükrében lehet meghatározni. Egyes területeken belül elképzelhető, hogy más-más megoldást, programot használunk. A következő lista csak példa értékű.

Mindenképpen célszerű felrakni:

- **sudo**  
Root jogokat kezelő program. Segítségével meghatározhatjuk, hogy egy-egy felhasználó milyen programokat, parancsokat futtathat root jogon. Ezzel minimalizálható a root felhasználóval való munka, amely a biztonságot növeli.
- **xinetd**  
Kapcsolatkezelő szerver. A szolgáltatásokat kezelő programokat kétféleképpen indíthatjuk. Lehetőségünk van rá, hogy folyamatosan fusson (a memóriában legyen), vagy csak az igénybevétele pillanatában legyen elindítva. Az xinetd figyel a portokat. Ha nála regisztrált portra érkezik kérés, akkor meghívja a megfelelő kezelőprogramot.
- **mc**  
Fájlmenedzser. Hasonló a DOS-on futó NC, vagy VC programokhoz.

Biztonsági elemző programok

- **mrtg**  
SNMP kimenetből webstatisztikát készít
- **webalizer**  
Web-szerver logból webstatisztikát készít
- **iptraf**  
Hálózati forgalom figyelő
- **logWatch**

- Lefutásakor átnézi a log állományokat, az érdekesebb dolgokról e-mail-ben tájékoztat.
- **sysstat**  
Rendszermonitor. Statisztikákat készít (iostat, mpstat, sar). Ezeket rögzíteni is tudja.
  - **tripwire**  
Fájlintegritás ellenőrző. Amikor kész vagyunk a rendszerrel, készítünk egy adatbázist a nem változó tartalmú könyvtárakról. Amennyiben az ellenőrzésekor hibát érzékel a program, akkor riaszt.
  - **Snort**  
Sok disztribúció tartalmazza. Ez egy IDS, azaz betörés detektáló program.

Segéd programok:

- **traceroute**  
Megvizsgálhatjuk vele, hogy a célgépig haladó csomag, milyen router-eken megy keresztül. Jól használható hálózati hibák azonosítására.
- **mtr**  
Mint előző, azzal a kiegészítéssel, hogy ez a router-ekkel osztott hálózatokon külön-külön sebességet mér.
- **lynx**  
Karakteres böngésző program. Nagyon jól jön, ha hirtelen szeretnénk információhoz jutni.
- **wget**  
Segítségével http oldalakról, oldalakat tudunk letölteni a gépünkre.
- **bind-utils**  
Name szerver tesztelésére szolgáló programok (pl: nslookup)

SSL security kezelő csomagok:

- **openssh**  
SSL kulcsgeneráló, kulcsolvasó programok és lib-ek.
- **openssh-clients**  
Titkosított terminál és fájl másoló kliensek (ssh, scp, sftp).
- **openssh-server**  
SSH szerver.

Eddig olyan csomagokat néztünk, amelyeket minden szerverre érdemes felrakni. Most nézzük meg, milyen csomagokat rakunk fel a szerverek szolgáltatása szerint:

Webszerver esetén rakjuk fel:

- **php**  
PHP script nyelv értelmezője.
- **php-imap**  
PHP kiegészítése imap levelezés kezelésére.
- **php-mysql**  
PHP kiegészítése mysql adatbázis kezelésére.
- **mysql-server**  
Mysql adatbázis kezelő szerver. Gyors és egyszerű. PHP-vel jól használható web-lapok elkészítésére.
- **mysql**

Parancssoros mysql kliens. Adatok, adatbázisok kezelésére alkalmas.

- **mysqlclient9**

Mysql szervert kezelő lib-ek.

- **apache**

Modulos szerkezetű web-szerver. Moduljai:

- mod-auth-any
- mod-auth-mysql
- mod-bandwidth
- mod-dav
- mod-perl
- mod-ssl
- mod-throttle

Samba (SMB) szerver esetén:

- **samba**

SMB protokollal működő fájl és nyomtató szerver. Kompatibilis Windows hálózatokkal.

- **samba-client**

Kliens program Samba szerverhez és Windows hálózatokhoz.

- **swap**

A Samba egyszerűen kezelhető webes beállító felülete.

Nameszerver, DNS cache esetén:

- **bind**

Szabvány DNS szerver.

- **caching-nameserver**

DNS cache kiegészítés

Nyomtató szerver esetén:

- **LPRng**

Nyomtatási sorok kezelésére alkalmas.

Egyéb szerver programok:

- **NUT**

Szünetmentes táp kezelésére, menedzselésére alkalmas program.

- **dhcp**

DHCP Szerver

- **imap**

Alternatív levélkezelő szerver – IMAP

- **squid**

Http, ftp proxy szerver

## 1.5 Gyakorlat

1. Tervezd meg a következőkben telepítésre kerülő szervered. A tervezésnél 1 db szerver áll rendelkezésedre. Mindenképpen legyenek telepítve a következő szolgáltatások:

- Apache szerver
- Sendmail szerver
- Samba szerver
- DHCP szerver
- DNS szerver
- Squid proxy
- SSH szerver
- Webmin

A tervezésnél határozd meg a partíció kiosztást és a telepítendő programokat. Határozd meg milyen portok engedélyezése szükséges a szolgáltatások működéséhez. Írd össze a hálózat beállításához szükséges adatokat szükséges, melyben mindenképpen térj ki a következőkre:

- Szerver IP címe
- Hálózat címe
- Hálózati maszk
- Átjáró IP címe
- DNS szerverek IP címei
- Szerver neve
- Domain név

Amennyiben több hálózati kártyával rendelkezik a gép, úgy minden kártyára külön-külön. Rajzzal illusztráld a számítógép helyét a hálózatban. A vázlaton megtalálható legyen az alapértelmezett átjáró és az intézmény hálózata (esetleg zónákra bontva).

2. Az előző feladathoz hasonlóan, tervezd meg egy több gépes (szerveres) kiszolgáló parkot. Legyen vázrolva a tűzfal helye a hálózatban, létezzen DMZ-ben elhelyezett web és e-mail szerver. A fájlserver a belső hálózaton kapjon helyet.

## 1.6 Ellenőrző kérdések

1. Mit hívunk Linux-nak?
2. Mik a disztribúciók?
3. Sorolj fel három disztribúciót és jellemezd őket!
4. Sorold el a gép-gép réteg protokolljait!
5. Mit nevezünk port-nak?
6. Írj le három portot és a hozzá kapcsolódó protokollt!
7. Mivel azonosítjuk (egyedi azonosító) a gépeket az Interneten?
8. Írj fel egy belsőhálózaton használható privát IP cím tartományt!
9. Mit jelent a hálózati maszk fogalom?

10. Mi a hálózati cím?
11. A 192.168.1.15 IP című gép egy olyan hálózaton van, ahol 254 gép van. Mi a hálózati címe és a hálózati maszkja?
12. Mi a BIX?
13. Milyen feladata van egy router-nek?
14. Mi a domain név?
15. Mi a host név?
16. Milyen feladatai vannak a DNS szervernek?
17. Jellemezd a csomagszűrő típusú tűzfalat!
18. Hol helyezkedik el a tűzfal a hálózatban?
19. Mi a DMZ?
20. Mi a partíciókra bontás indoka a szervernél?
21. Milyen fájlrendszereket használ a linux általában?
22. Mennyi partícióra bontanál egy meghajtót, linux szerver esetén?
23. Milyen csomagokat (programokat) telepítenél feltétlenül egy web-szerverhez?
24. Mi az a függőség?

## **1.7 Felhasznált, ajánlott irodalom**

Stefan Strobel - Thomas Uhl : Linux (Kossuth)

Richard Petersen : Linux Teljes referencia (Panem)

Kirch, Olaf : A Linux hálózati adminisztrátor kézikönyve (Kossuth)

Fred Butzen, Christopher Hilton : Linux hálózatok (Kiskapu)

Othmar Kyas : Számítástechnikai hálózatok biztonságtechnikája (Kossuth)

Linux támogatás-Mini HOGYAN

<http://linux.vv.hu/hogyanok/mini/Linux-tamogatas-Mini-HOGYAN/index.html>

A Linux (eddig) története

<http://linux.vv.hu/konyv/linux-tortenet/index.html>

Bevezetés az Internet Protokollba

<http://linux.vv.hu/egyebek/halozat/tcpip/tcpip.html>

Az Internet alapjai

<http://linux.vv.hu/egyebek/halozat/internet-alap/alap.html>

ZorpGPL-UHU felhasználói dokumentáció

UHU-Firewall Linux telepítő CD, /doc könyvtár

## 2. Telepítés

### 2.1 RedHat Linux 9.0

#### 11. Telepítés megkezdése

A RedHat linux telepítéséhez szükséges (3db) CD-ket letölthetjük az <ftp://ftp.redhat.com/pub/redhat/linux> oldalról iso típusú állományokban. (a jelenlegi 9.0 verzió ISO fájljai: <ftp://ftp.redhat.com/pub/redhat/linux/9/en/iso/i386> ) Ezekből, cd író program segítségével, készíthetjük el a telepítő CD-ket.

A hivatalos oldalon kívül, úgynevezett, tükör kiszolgálókról is letölthetjük a rendszert. Ilyenek például:

```
ftp://ftp.fsn.hu/pub/CDROM-Images/redhat/linux/9/en/iso/i386/  
ftp://ftp.mirror.ac.uk/sites/ftp.redhat.com/pub/redhat/linux/9/en/iso/i386/
```

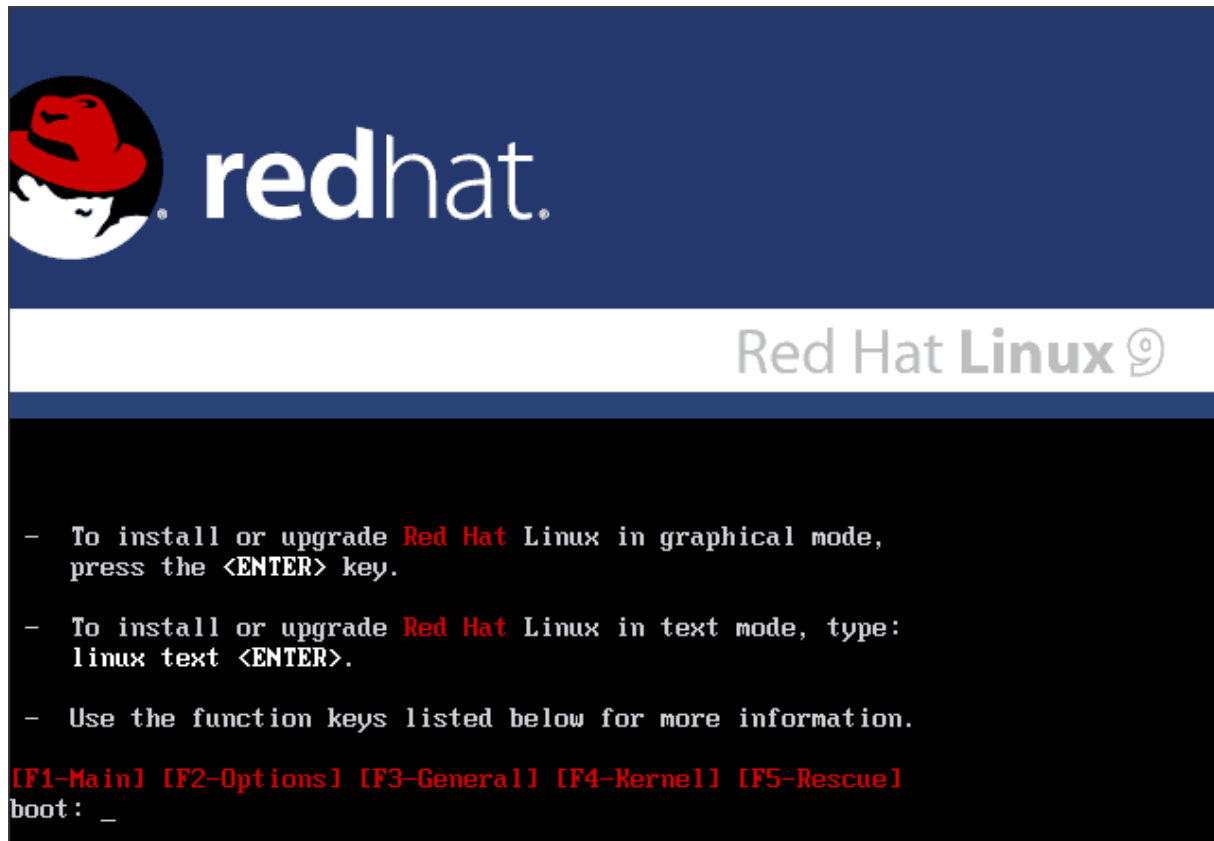
A cd-k boot-olhatóak. Ha erre nem alkalmas a gépünk, akkor készíthetünk indítólemezt. Az első cd /image könyvtárban megtalálhatjuk a különböző körülményekhez elkészített indítólemez fájlokat. Ezeket lemezre írhatjuk a /dosutils könyvtárban található rawrite.exe programmal, vagy meglévő linux rendszeren a dd paranccsal:

```
> rawrite -f \images\boot.img -d a:  
$ dd if=/mnt/cdrom/images/boot.img of=/dev/fd0
```

Indítsuk el a számítógépet a telepítő cd, vagy az elkészített telepítő lemez segítségével.

#### 12. Rendszerindító képernyő

A telepítő elindítása után a kezdőképernyő fogad minket. Itt beállíthatunk extrákat a telepítő programnak és kernelnek.



Van lehetőségünk kernel paramétert és telepítési opciókat megadni a 'boot:' sorba:

- **linux noprobe.** A hardver teszteket kihagyja.
- **linux mediacheck.** Ellenőrzi és telepíti a média drivereket.
- **linux rescue.** Karakteres javító rendszer indítása.
- **linux dd.** Amennyiben hajlékony lemezen van driverünk.
- **linux updates.** Automata update.
- **linux lowers.** 640\*480-as grafika.
- **linux text.** Karakteres telepítés.

A funkcióbillentyűk segítségével információkat kaphatunk a különböző beállítási lehetőségekről. Enter megnyomásával továbbléphetünk.

#### Telepítési média ellenőrzése

Miután beindul a telepítőrendszer, a megjelenő ablak megkérdez, szeretnénk-e ellenőrizni a telepítőlemezeket. Amennyiben először használjuk a CD-inket ezt érdemes megtenni, egyenként betenni őket, majd OK. Most viszont nem ellenőrzünk, tehát a SKIP-et válasszuk.

Ekkor elindul az 'Anaconda' névre keresztelt rendszer telepítő program. (Ez külön csomagban is megtalálható.) Elindulás után láthatjuk az üdvözlő képernyőt. Innen NEXT gombbal megyünk tovább.

Ha a telepítés közben információkra van szükségünk, akkor használhatjuk a virtuális terminálokat. A jelenleg látható grafikus telepítő az CTRL+ALT+F7 gombbal érhető



el. A további terminálok elérhetőek, amelyekről lényeges információkat meríthetünk hiba esetén:

- **CTRL+ALT+F1** Anaconda indítása.
- **CTRL+ALT+F2** Telepítés közben shell elérése.
- **CTRL+ALT+F3** Modulok betöltődése.
- **CTRL+ALT+F4** Futó események üzenetei.
- **CTRL+ALT+F7** Grafikus telepítő rendszer.

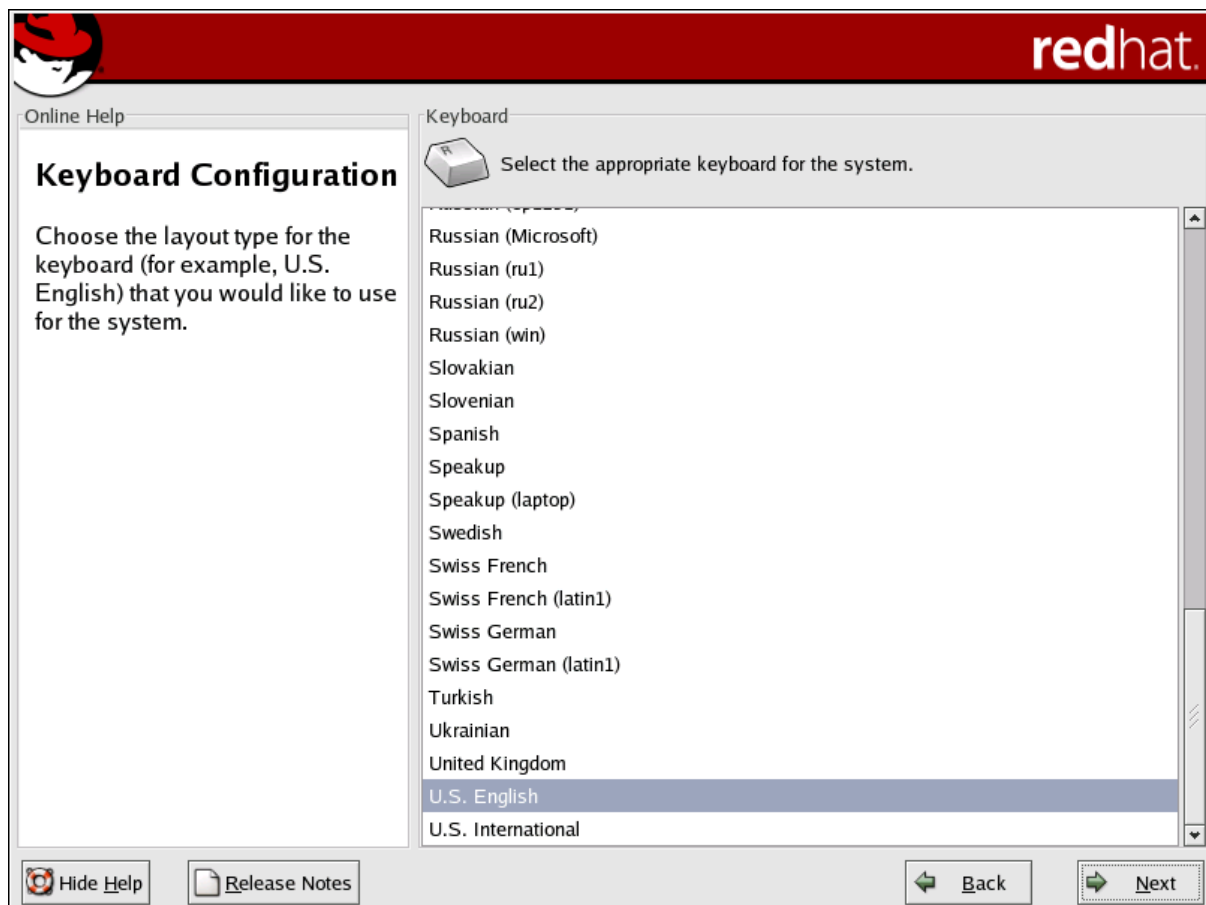
### 13. Telepítés nyelvének kiválasztása (Language Selection)

A RedHat jelenlegi verziójában nincs lehetőségünk magyar nyelvű telepítésre, ezért az angol (English) nyelvet választva haladunk tovább. Itt kizárólag a telepítőprogram nyelvét állítjuk, nem lesz összefüggésben a telepített rendszerünkkel.



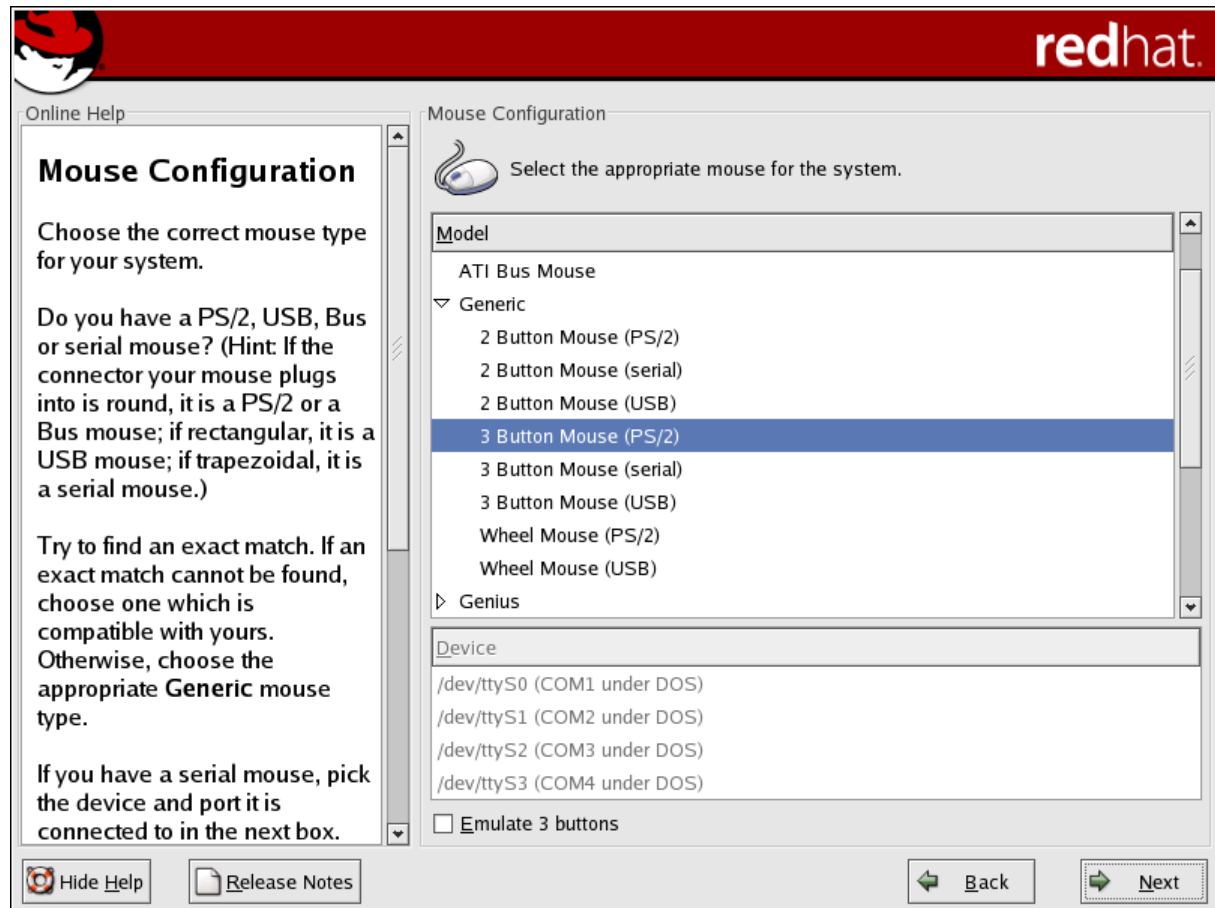
## 14. Billentyűzet nyelvének kiválasztása (Keyboard)

A listából kiválaszthatjuk a billentyűzet nyelvét. Magyar billentyűzet esetén a Hungarian-t, míg angolnál az U.S.English-t válasszuk.



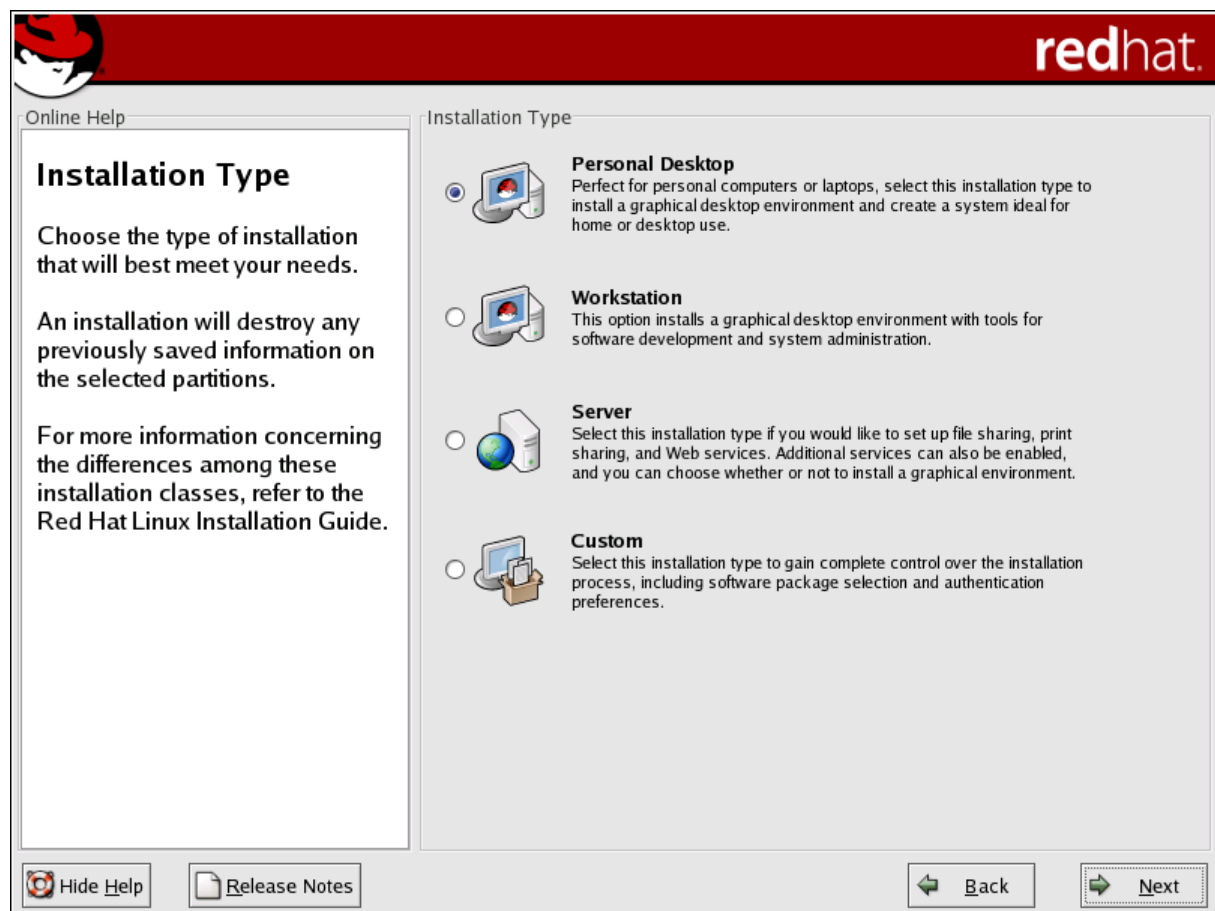
## 15. Egér beállítása (Mouse Configuration)

Kiválaszthatjuk egerünk típusát. Soros egér esetén még azt kell megadni, hogy melyik soros porton található. A telepítő rendszer, jellemzően eltalálja, melyik típusal működik jól az egerünk. Amennyiben egerünk 3 gombos, úgy mindenképpen ennek megfelelően válasszunk típust, vagy 2 gombos egér esetén jelöljük be a 3 gombos emulációt (Emulate 3 Buttons), ugyanis ezzel karakteres képernyőn is lesz lehetőségünk a szövegmásolás, behelyezés funkciót kihasználni.



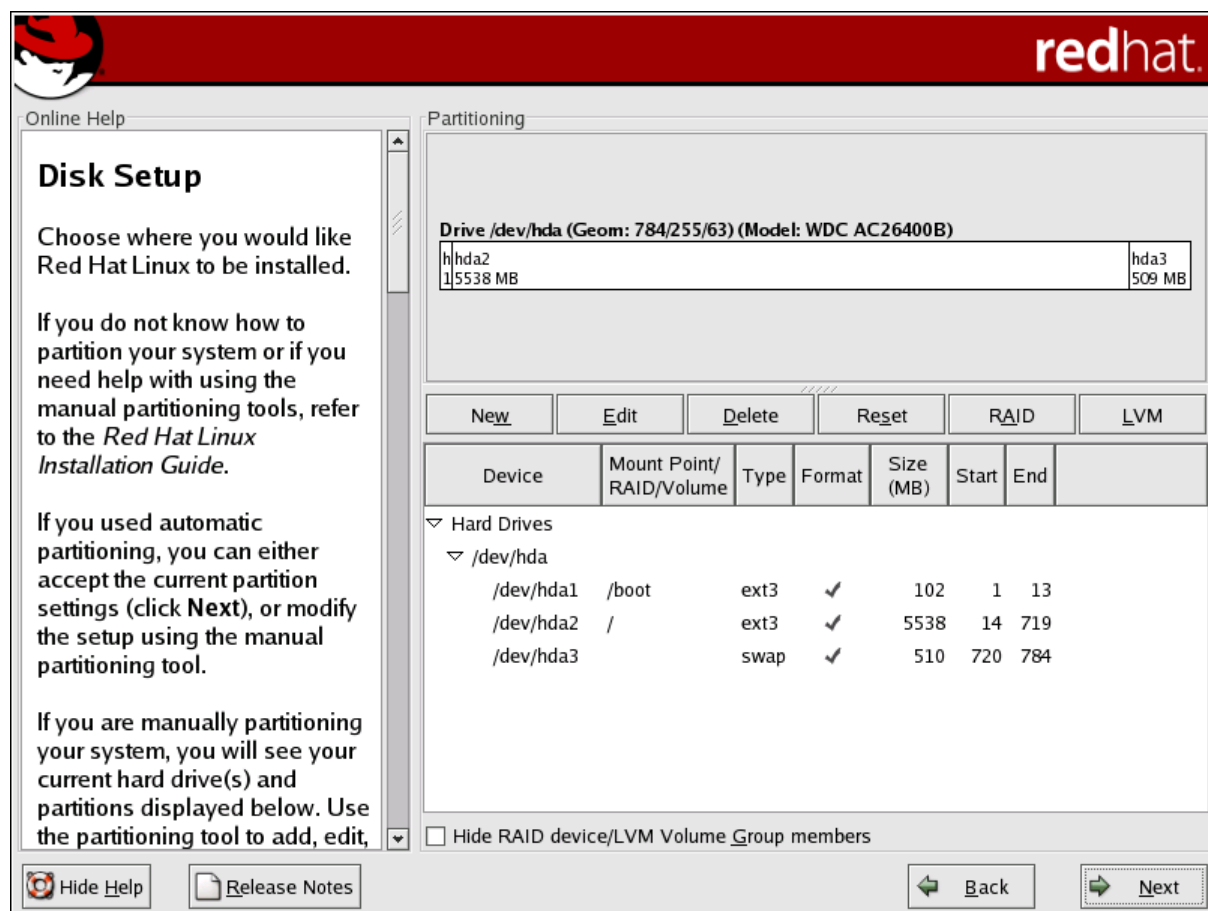
## 16. Telepítés típusa (Installation Type)

Itt választhatunk az önálló számítógép (Personal Desktop), a munkaállomás (Workstation) és a szerver (Server) telepítése között. Ezekben az esetekben, a választottnak megfelelően segítséget nyújt a telepítendő csomagok, programok kiválasztásában. Kipróbálhatjuk bármelyik lehetőséget, de szerver telepítése esetén célszerű az egyedi kialakítást (Custom) választani.

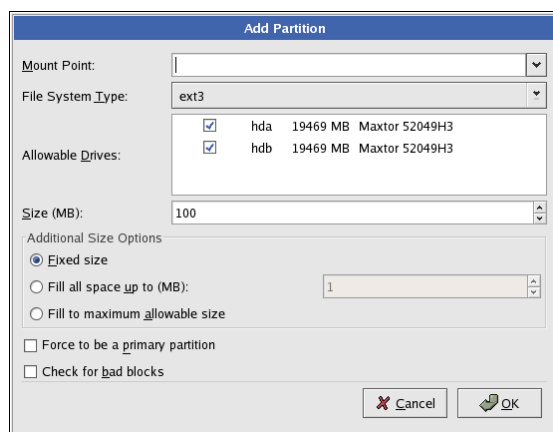


## 17. Lemez partícionálása

Két lehetőségünk van a lemez partícionálására. Első lehetőségünk az automatikus partícionálás (Automatically partition), amelyet lehetőleg kerüljünk el szerverek telepítésénél. Ugyanis a telepítő rendszer egy általános séma alapján bontja szét a meghajtónkat és nincs lehetőségünk ennek igényeinknek megfelelő módosítására. Beállíthatjuk még a partíciókat Disk Druid programmal, amely a telepítő része (ezt fogjuk választani most).



A Disk Druid kiválasztása (Manually Partition with Disk Druid) után, a következő képernyőn felvehetjük a partícióinkat. Amennyiben lemezünkön volt már partíció, azt a Delete gombbal törölhetjük. A New gombbal vehetünk fel újakat.



A New gombot használva feljön az új partíció adatait kérő ablak. Mount Point-nál meg tudjuk adni, hogy a könyvtárszerkezetben hol foglaljon helyet a létrehozott partíció, azaz hova illesszük be. Itt beírhatjuk, vagy kiválaszthatjuk azon könyvtárat, amelyet külön partícióra kívánunk elhelyezni. Swap típusú partíció esetén nincs csatolási pont.

A Filesystem Type-nál tudjuk megadni a partíció típusát. Itt ext2-es és ext3-as könyvtárszerkezetet választhatunk, illetve swap partíció típust is. Allowable Drivers-nel kiválaszthatjuk, mely meghajtókra kívánjuk a partíciót létrehozni. Size-nel adjuk meg a partíció méretét MegaByte-ban. Továbbá megadhatjuk a partíció létrehozásakor lezajló méret meghatározás kritériumait. A Disk Druid ugyanis némileg felülbírálja az általunk megadott beállításokat. Jellemzően a fix méret (Fixed size) beállítást használjuk, míg az utolsó partíciónál használhatjuk a maradék hely kitöltését (Fill to maximum allowable size).

Lentebb kiválaszthatjuk, hogy a most felvett partíció mindenképpen elsődleges legyen (Force to be a primary partition). Az elsődleges partíció erőltetésére a /boot-nál lehet szükségünk. Megjelölhetjük a hibás szektorok ellenőrzését (Check for bad blocks) is, ami fontos lehet egy szerver telepítésénél.

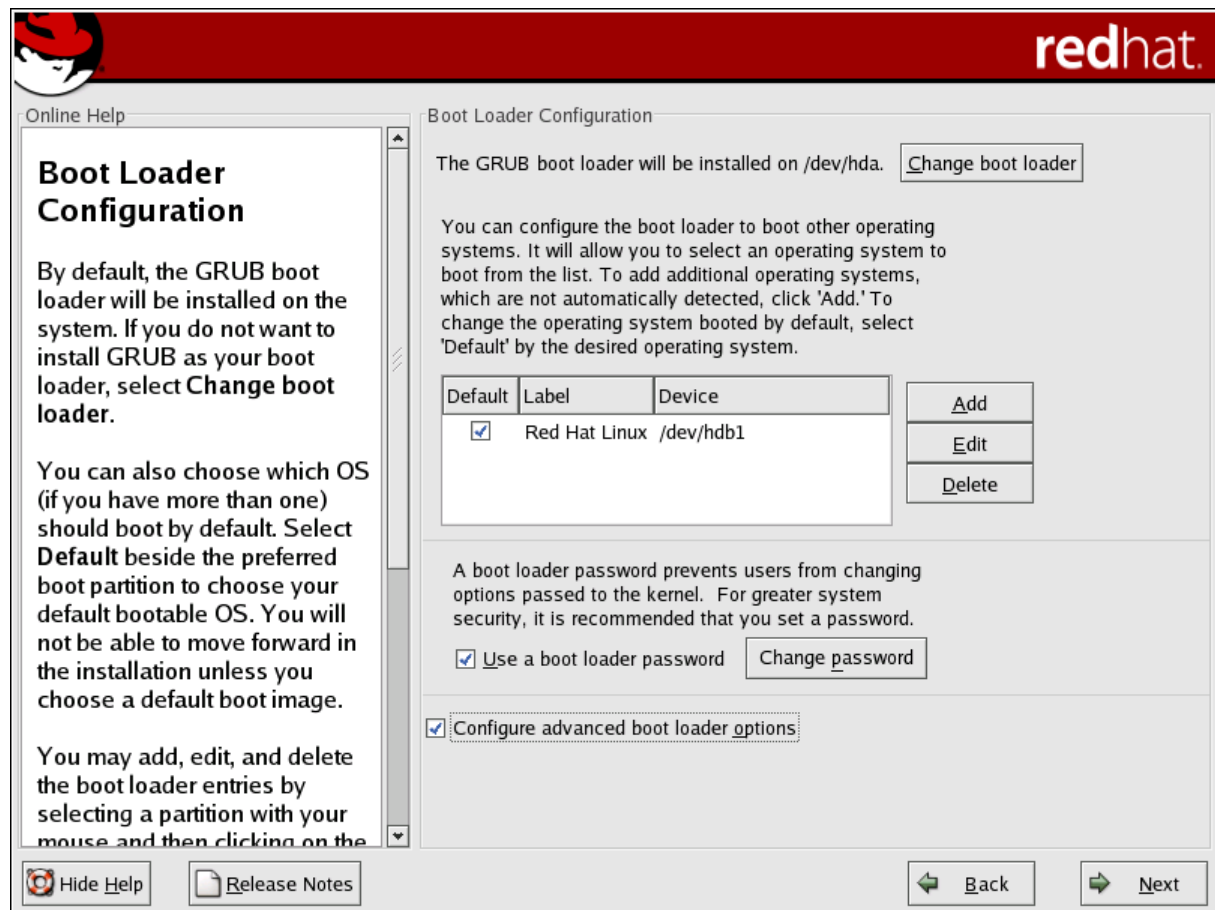
Most vegyük fel a következő partíciókat:

Csatolási pont	Típus	Méret		
/boot	Ext3	100	Fixed size	Primary
/	Ext3	500	Fixed size	Primary
-	Swap	256	Fixed size	Primary
/usr	Ext3	1000	Fixed size	
/tmp	Ext3	200	Fixed size	
/var	Ext3	1000	Fixed size	
/var/spool/squid	Ext3	2000	Fixed size	
/home	Ext3	-	Allowable	

## 18. Boot Loader beállítása

A linux rendszerek úgynevezett boot loadert használnak. Ez a program nem csak azt határozza meg, hogy melyik partícióról induljon a rendszer, hanem azt is, hogy melyik kernel induljon el. A boot loader mindenképpen szükséges az indításhoz.

Válaszuk ki, melyik boot loadert szeretnénk használni. Két lehetőségünk van: a Grub és a Lilo. A Lilo hagyományosabb, régóta létező megoldás. A Grub újabb, több kiegészítő tulajdonsága van, amelyet jól használhatunk hibajavításnál.



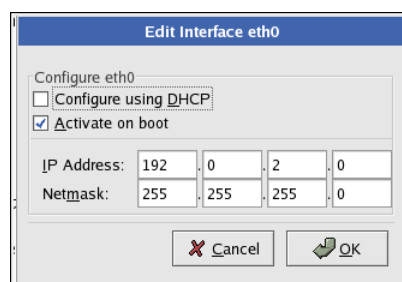
Elhelyezés szempontjából tehetjük a master boot record-ra (MBR), és a /boot partíció első szektorára. Jelenleg az MBR lehetőségét (/dev/hda) van beállítva. A másik lehetőség akkor jöhet számításba, ha több operációs rendszer is van a számítógépen és saját boot menedzsert használunk.

Lejebb vehetünk fel új sort (új operációs rendszert) az indítandók közé. Erre egy szervernél ritkán van szükség. Lehetőség van a boot loader jelszóval való ellátására is.

Jellemzően ezen az oldalon nem kell állítani. Mehetünk is tovább.

## 19. Hálózati kártyák beállítása (Network Devices)

A képernyő felső részében, a táblázatban láthatjuk a megtalált hálózati kártyákat. Alapban DHCP kezelés van megadva. Ez egy szervernél nem célszerű, ezért válasszuk ki a kártyát és kattintsunk az EDIT gombra.

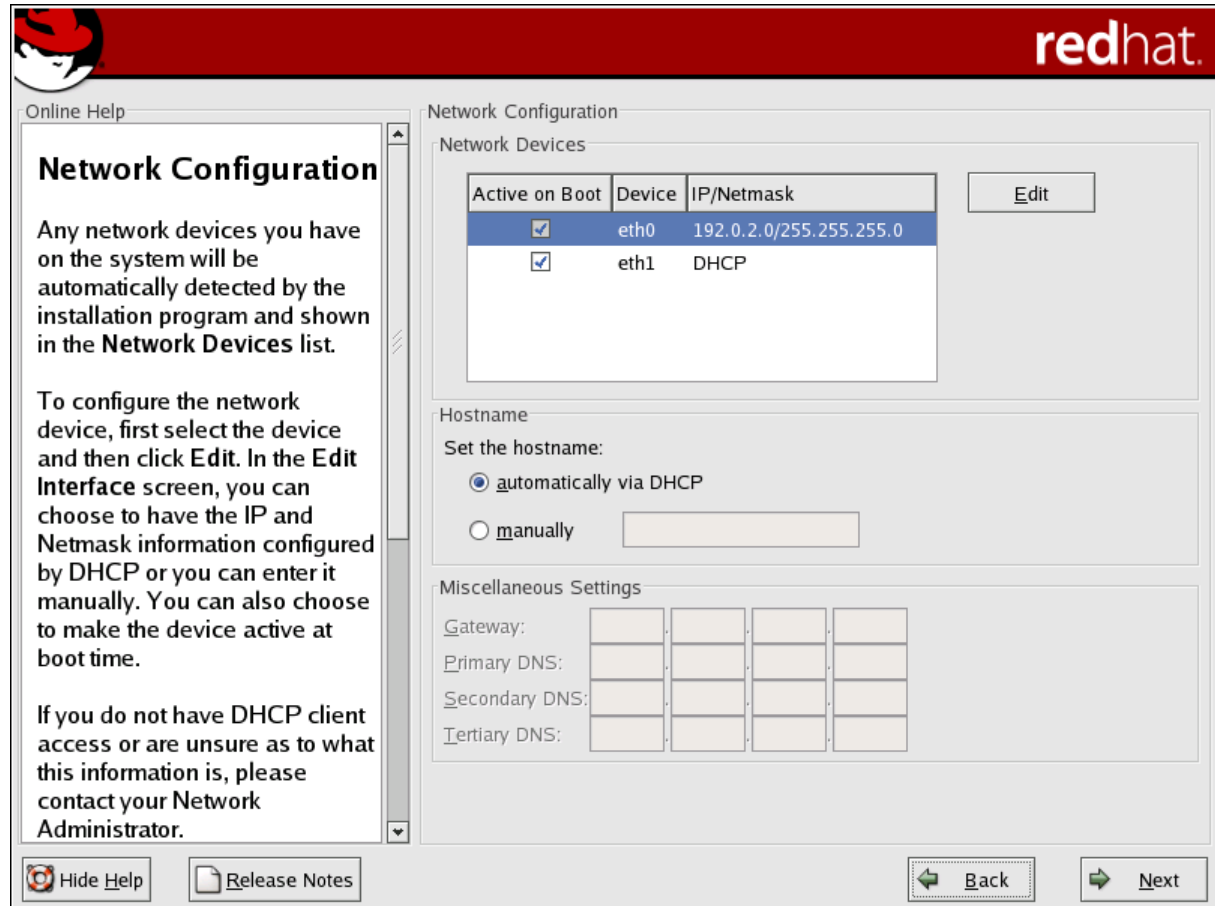


A feljövő ablakban állíthatjuk a kártya paramétereit. Szedjük le a pipát a 'Configure using DHCP' sor mellől, hogy fix IP-t állíthassunk. Az 'Activate on Boot' mellett maradjon pipa, hogy induláskor működjön az eszköz. Az 'IP Address' sorban adjuk meg az IP címet (pl. 10.0.1.13), majd alatta a 'Netmask'-ot

(255.255.255.240). Ugyan így adjuk meg a többi eszköz adatait is.

Alatta a 'Hostname' beállításnál a 'manually' sorba írjuk be a gép nevét (server).

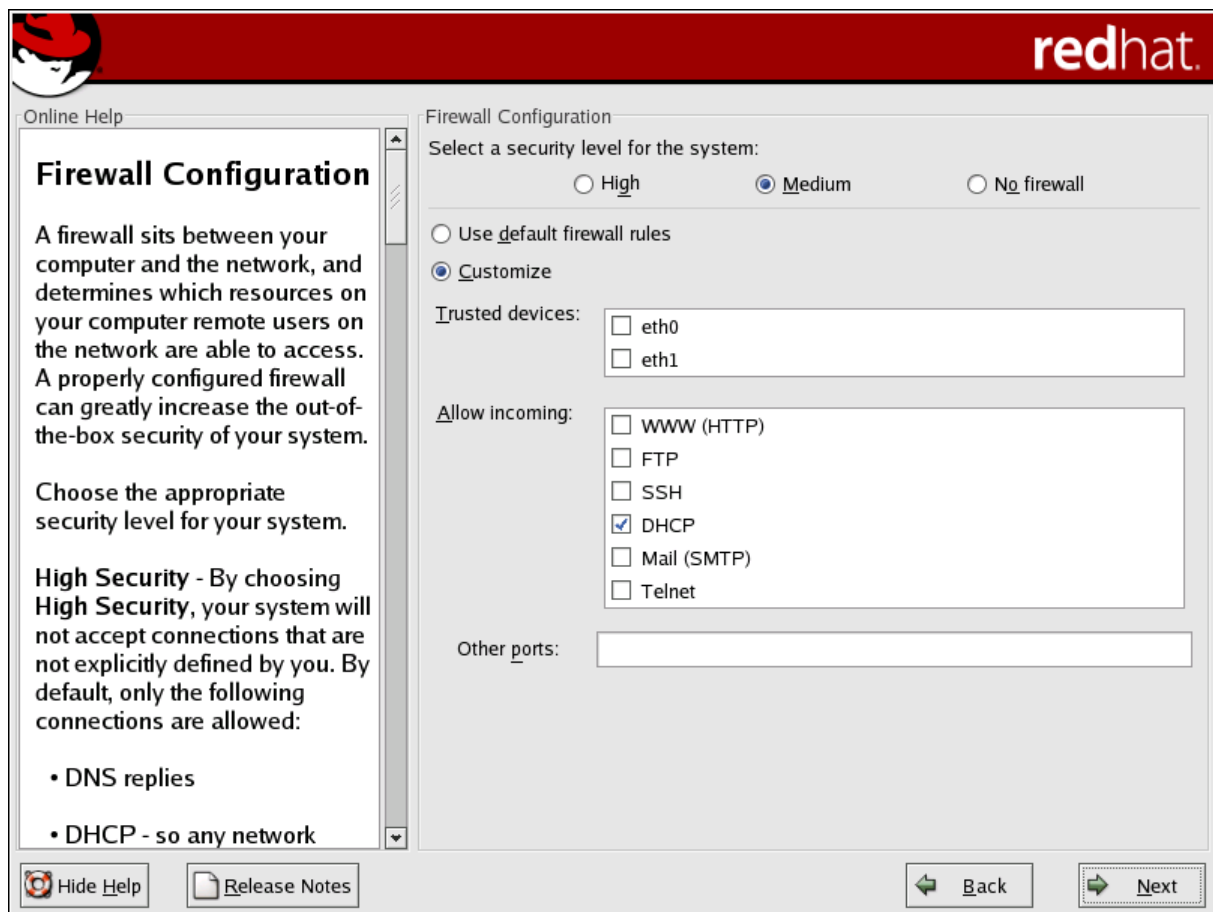
Az átjárót (Gateway) és a DNS-eket szintén adjuk meg.





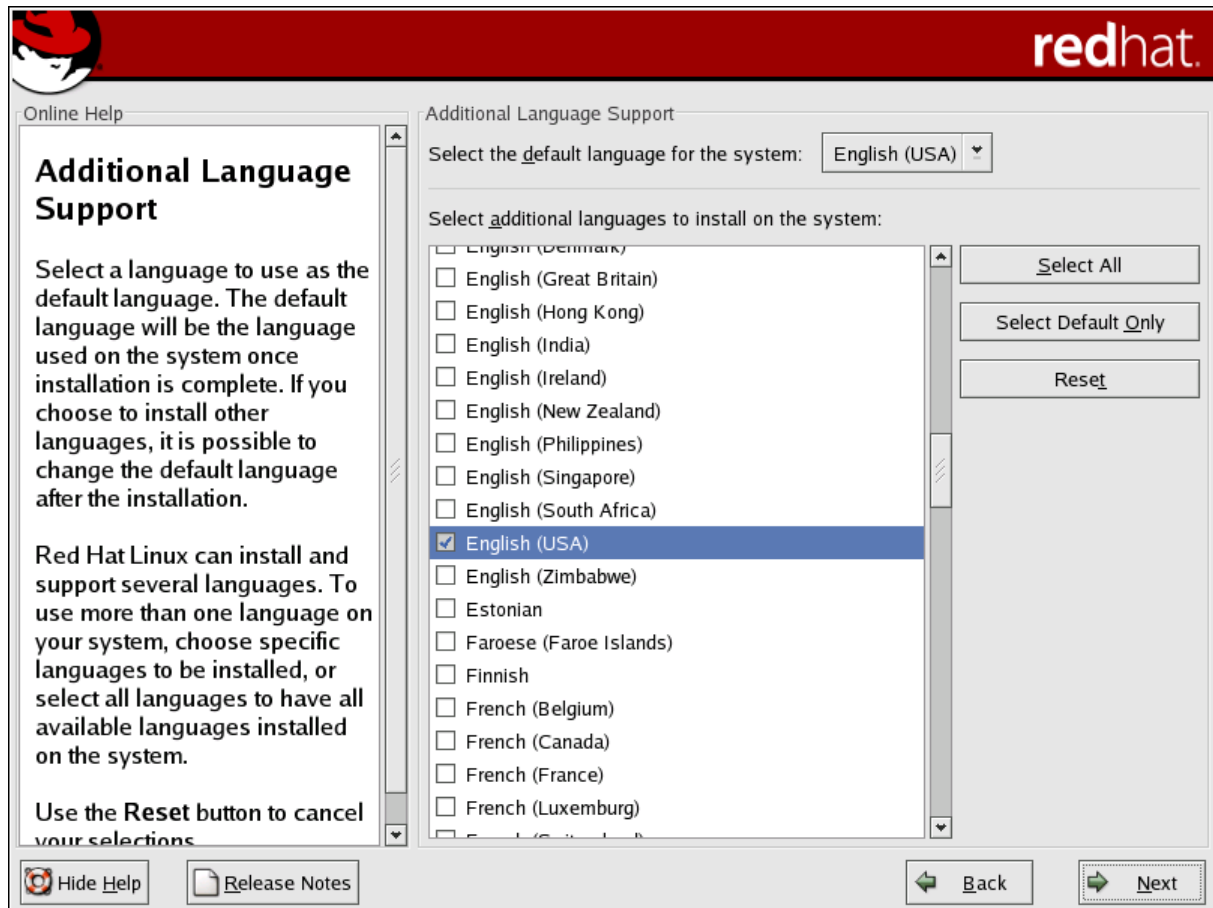
## 20. Tűzfal beállítása

Lehetőségünk van csomagszűrés beállítására is. Ez minden szervernél kötelező. A csomagszűrés beállítását már a telepítésnél megkezdhetjük, de mindenképpen szükségünk lesz későbbi finomításokra. Javasolt egyéni beállítás alkalmazása. Biztonsági szintnek (Select a security level for the system) medium-ot választunk. Beállításra használjunk egyéni (Customize) és pipáljuk be az allow incoming felsorolásnál, hogy milyen szolgáltatásokat engedünk be a szerverünkre. Különösebb indok nélkül a telnet és az ftp szolgáltatást ne jelöljük be. Alatta (other ports) megadhatjuk a felsorolásban nem található, de szükséges portok listáját. (pl.: '110:tcp, 10000:tcp)



## 21. Nyelvek kiválasztása

Itt választhatjuk ki, hogy mi legyen a programok alapértelmezett nyelve (Select the default language for this system) és, hogy a programok még milyen nyelvet telepítsenek (Select additional languages to install on the system). Itt az angolt (English USA) és a magyart (Hungarian) mindenképpen válasszuk ki.



## 22. Időzóna beállítások

A térkép, vagy a lista segítségével választjuk ki Budapestet. Ha szeretnénk UTC megoldást használni, akkor jelöljük meg és az UTC Offset fülecskénél állítsuk be az időcsúszást (+1).

**Time Zone Selection**

You can set your time zone either by selecting your computer's physical location, or by your time zone's offset from Universal Time, Coordinated. (also known as UTC).

Notice the two tabs at the top of the screen. The first tab offers you the ability to configure by location. With this option, you can choose your view. In choosing View, your options are: World, North America, South America, Pacific Rim, Europe, Africa, and Asia.

From the interactive map, you can click on a specific city, as indicated by the yellow dots, and a red X will appear at your selection.

Location UTC Offset

Location	Description
America/Montserrat	
America/Nassau	
America/New_York	Eastern Time
America/Nipigon	Eastern Time - Ontario & Quebec - places that did
America/Nome	Alaska Time - west Alaska

System clock uses UTC

Hide Help Release Notes Back Next

## 23. ROOT jelszó beállítása

Írjuk be a root (teljes jogú) felhasználó jelszavát. Ezt lehetőleg ne felejtsük el, mert nagy szükségünk lesz rá.

## 24. Felhasználók azonosításának beállításai

Itt állíthatjuk be, hogyan történjen a felhasználók azonosítása. Van lehetőség másik gépen tárolt felhasználók átvételére is. Ennek kihasználásával csak egy gépen kell a felhasználókat nyilvántartani. Beállíthatunk kapcsolatot NIS, LDAP, Kerberos szerverekkel, vagy használhatjuk a SMB protokollon keresztüli azonosítást, akár Windows kiszolgálóról is. Ezen lehetőségeket akkor engedélyezzük, ha tudjuk, hogy ilyen szerver működik, egyébként ne.

Mindenképpen válasszuk ki viszont a jelszavak titkosított tárolását (Enable MD5 passwords) és a jelszavak különválasztását a felhasználó azonosító fájljától (Enable shadow passwords). Ez nem csak a biztonság miatt fontos, hanem a programok helyes működése végett is.

Online Help

### Authentication Configuration

You can skip this section if you will not be setting up network passwords. If you are unsure, ask your system administrator for assistance.

Unless you are setting up an NIS password, you will notice that both MD5 and shadow are selected. Using both will make your system as secure as possible.

- **Enable MD5 Passwords** - allows a long password to be used (up to 256 characters).
- **Use Shadow Passwords** - provides a very secure method of retaining passwords for you.

Authentication Configuration

Enable MD5 passwords

Enable shadow passwords

NIS | LDAP | Kerberos 5 | SMB

Enable NIS

NIS Domain:

Use broadcast to find NIS server

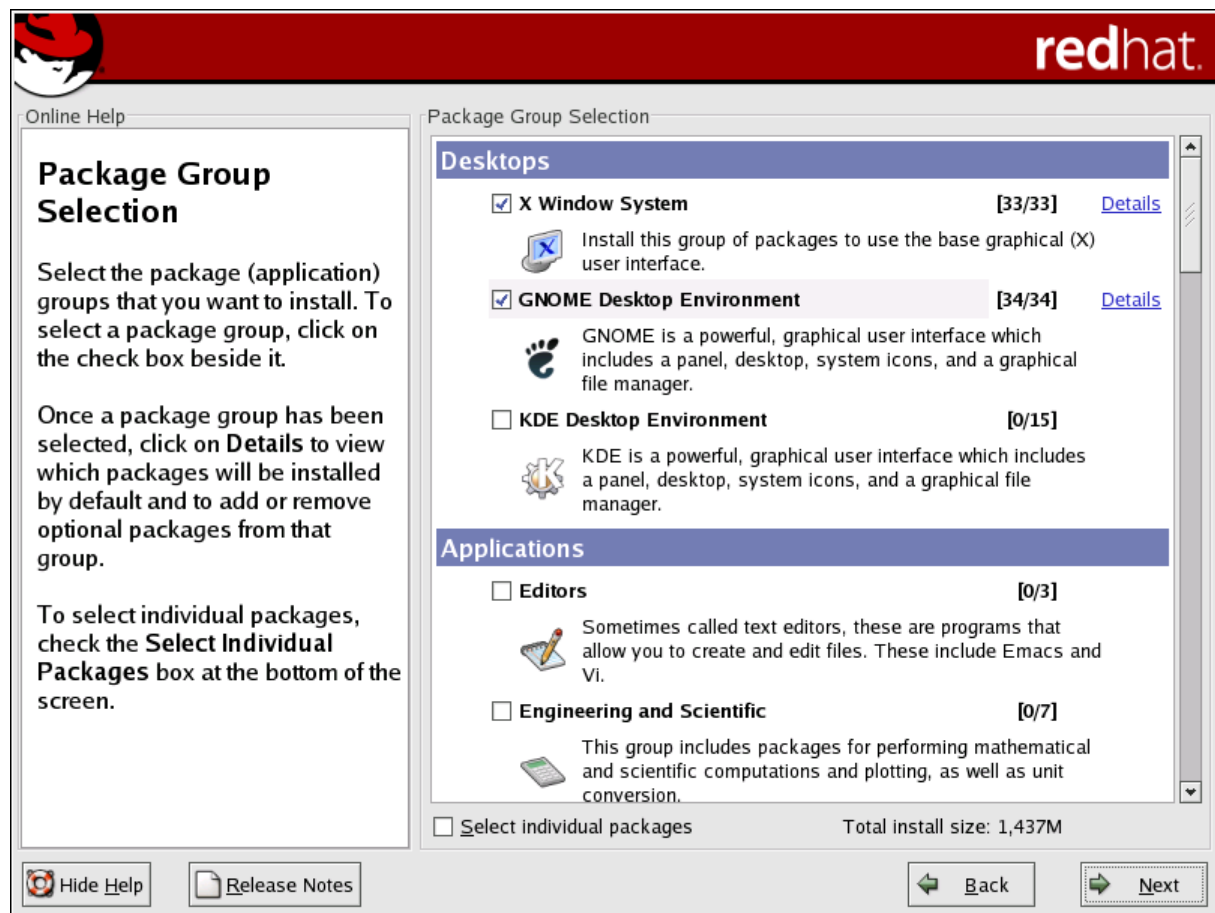
NIS Server:

Hide Help | Release Notes | Back | Next

## 25. Program csomagok csoportjainak kiválasztása

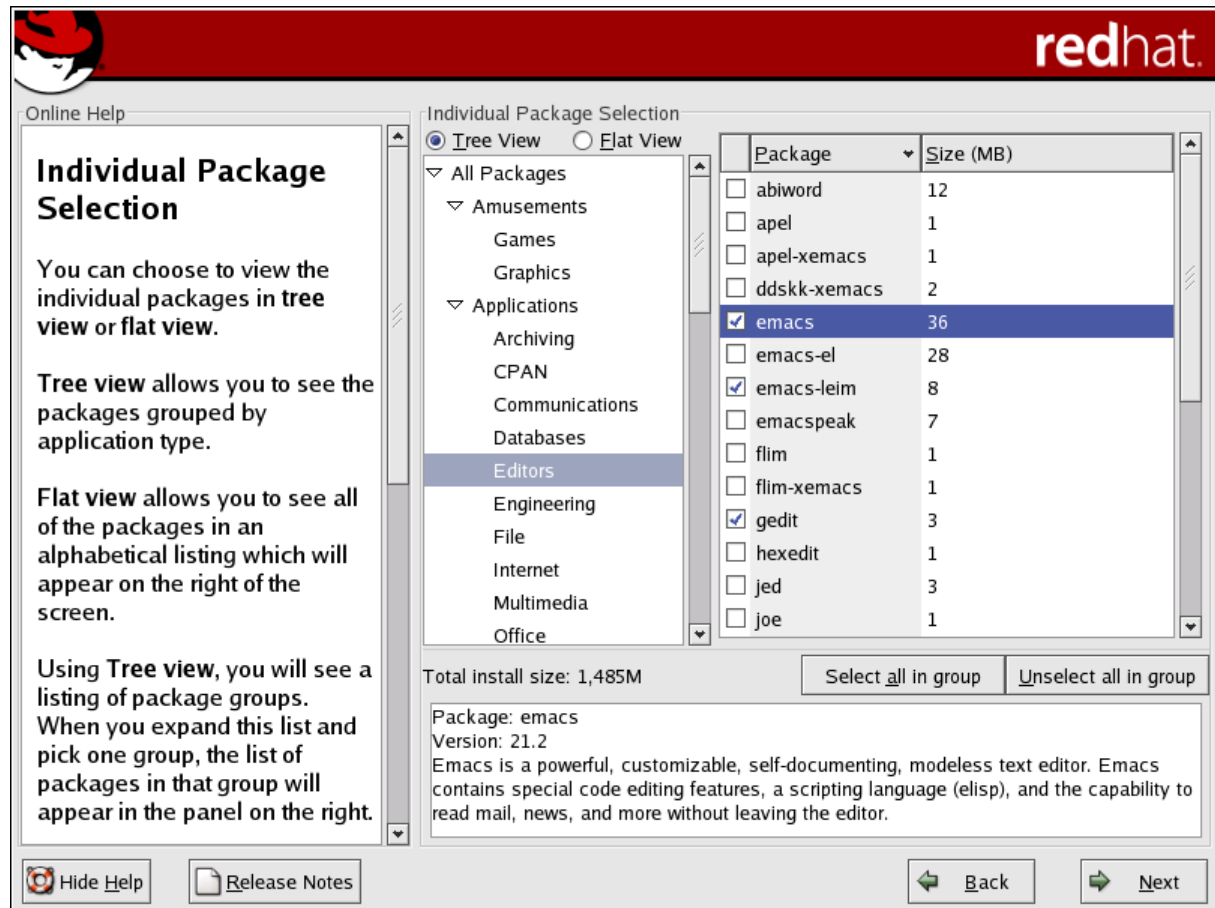
A telepítő rendszer számtalan csoportot ajánl fel választási lehetőségként. Ez gyakorlatilag egy elméleti összeállítás. A szerzők megpróbálták bizonyos körökbe összeválogatni a csomagokat, hogy ezzel is egyszerűsíthessék a telepítést. Szerver telepítésénél nem javaslom a csoportok használatát. Mindenképpen legyünk tisztában vele, milyen csomagokat telepítünk a szerverünkre, ezért az egyéni válogatást válasszuk. Továbbá a csoportok használatával elképzelhető, hogy valami kimarad a telepítésből. (ilyen például a Midnight Commander, amely egyik csoportban sincs benne).

Vegyük le a csoportokról a kiválasztást. A csoportok alatt válaszuk ki a csomagok egyéni kiválasztását (select individual packages), más ne is legyen kijelölve. Ez 479 MegaByte-os alaprendszer telepítését jelenti.



## 26. Csomagok kiválasztása

Amennyiben a 'select individual packages' be volt jelölve, akkor kapunk egy részletes csomagkiválasztó képernyőt. Itt több száz csomag (program) van felsorolva kategóriákba szedve.



Amennyiben szervert telepítünk, a következő csomagokra NEM lesz szükségünk, ezek mellől vegyük le a pipát:

- Applications/Internet
  - finger
  - jwhois
  - rsh
  - rsync
  - talk
  - telnet
- Applications/System
  - Irda-utils
  - Isdn4k-utils
- System Environment/daemons
  - nfs-utils
  - ORBIT

Amennyiben szervert telepítünk, a következő csomagokra lesz még szükségünk, ezek mellé tegyük pipát:

- Applications/Database
  - mysql
  - mysql-server
- Applications/Internet
  - fetchmail
  - lynx
  - mrtg
  - spamassassin
  - squirrelmail
  - webalizer
- Applications/System
  - iptraf
  - samba-client
  - samba-common
  - samba-swat
  - tripwire
- Development/Language
  - php
  - php-imap
  - php-mysql
- System Environment/daemons
  - bind
  - caching-nameserver
  - cups
  - dhcp
  - httpd
  - imap
  - LPRng
  - mod\_auth\_mysql
  - mod\_perl
  - mod\_ssl
  - samba
  - sendmail-cf
  - squid
  - xinetd

Amennyiben kiválasztottuk a számunkra szükséges csomagokat, továbbléphetünk a telepítési folyamatban.

## 27. Függőségek kezelése

Minden csomagnál, programnál konkrétan meghatározott milyen más csomagokra van szükségük a működéshez, ezt hívjuk függőségeknek.

A telepítő rendszerünk megvizsgálja, hogy az általunk feltenni kívánt csomagoknak még mire van szükségük a tökéletes működéshez. A következő képernyőn (Unresolved Dependencies) fel is hívja a figyelmünket a számára szükséges, de általunk nem kijelölt csomagokra.

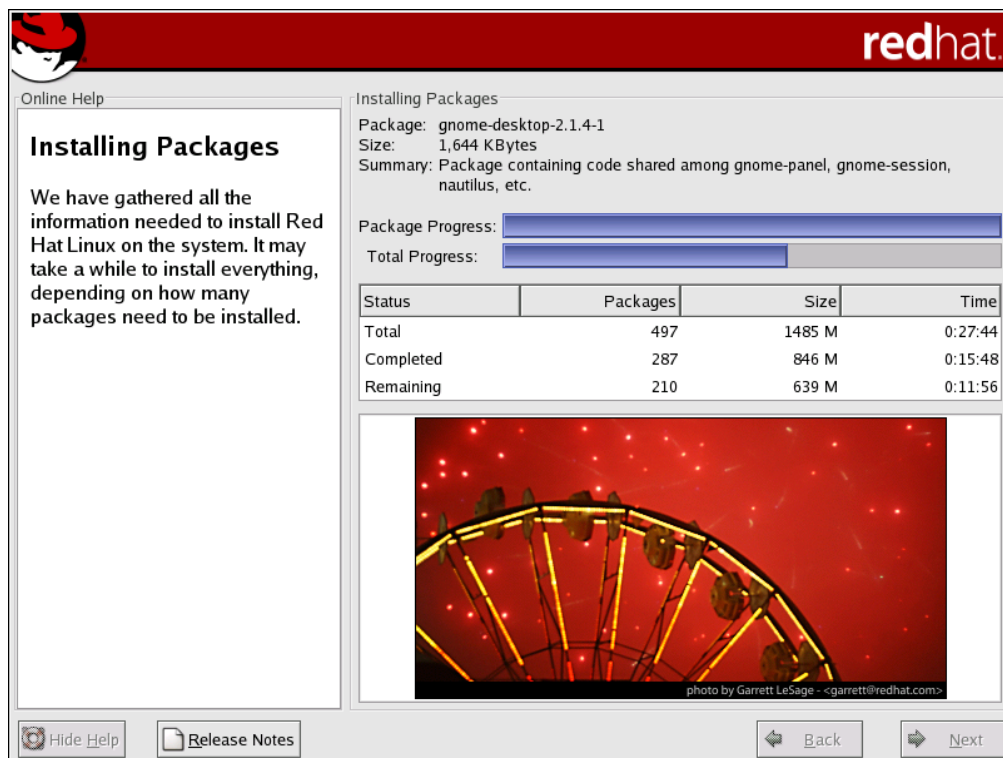
Három lehetőségünk van ezek kezelésére:

- Feltelepítjük a szükséges csomagokat (Install packages to satisfy dependencies)
- Kihagyjuk azokat az általunk kijelölt csomagokat, aminek gondja van (Do not Install packages that have dependencies)
- Feltesszük az általunk kiválasztott csomagokat, de a függőségek miatt felsoroltakat nem. (Ignore packages dependencies)

Amennyiben az utolsó lehetőséget válasszuk (Ignore packages dependencies), akkor komoly gondjaink lesznek szerverünk működésével. A legcélszerűbb választás a függőségek miatt kilistázott csomagok telepítése. Tehát válasszuk az első lehetőséget (Install packages to satisfy dependencies) és folytassuk a telepítés folyamatát.

## 28. Csomagok felmásolása

Most jön az a rész, amikor a telepítőnk egy kicsit önállóan dolgozik. A beállított partíciókra elkészíti a fájlrendszert, majd felmásolja és beállítja a kiválasztott csomagokat. Itt lesz majd szüksége a többi telepítő CD-re is.





## 29. Indítólemez készítése

Miután a csomagok másolása megtörtént, a telepítő szeretne indítólemezt készíteni. Tegyük be egy lemezt a floppy meghajtóba és engedjük meg neki, hogy indítólemezt készítsen. A későbbiekben rengeteg probléma megoldásában segíthet nekünk a lemez.

Ezzel a telepítési folyamat a végére ért. Amennyiben grafikát igénylő csomagot választottunk ki, úgy még a monitor típus és az X beállítása hátra van. Majd a számítógép újraindulása után a szerverünk telepítésével végeztünk.

Nagyon fontos, hogy addig még ne hagyjuk a gépünket a hálózaton, amíg a finomhangolását nem végeztük el. A teljes biztonsági szintet csak utána fogja elérni és nem lenne célszerű, hogy pont ebben a rövid időben törjék fel.

## 30. Webmin telepítése

A Webmin rendszer, egy saját web-kiszolgálón futó, perl alapokat használó beállító rendszer. Szinte mindent be tudunk állítani vele, amely szoba jöhet egy linux szervernél. Modulós szerkezetű, akár bővíthető is. A Webmin-ben van lehetőségünk magyar nyelv kiválasztására, sajnos a fordítás nem teljes.

A webmin csomaghoz hozzájuthatunk a program hivatalos oldaláról. Letölthetjük másik gép segítségével is, de szerverünkről is megoldható a lynx nevű böngészővel. A következő lépéseket tegyük meg.

1. Írjuk be a parancssorba, hogy: `$ lynx www.webmin.com`
2. Keressük meg az oldalon (legalul) a 'Download' sor és mellette az RPM linkre nyomjunk ENTER-t.
3. Keressük meg az oldalon az 'aleron logo...' sort és a download linkre nyomjunk ENTER-t.
4. Az oldal tetején lévő : <http://aleron.dl.sourceforge.net/sourceforge/webadmin/webmin-1.121-1.noarch.rpm> linkre nyomjunk ENTER-t.
5. A megjelenő kérdésre d gombbal válaszoljunk.
6. A letöltés után a 'Save to Disk'-et válasszuk. Majd a fájlnevnél ENTER.
7. Q-val lépünk ki a lynx-ből.

Amennyiben a letöltés sikerült a csomag a rendelkezésünkre áll. Telepíthetjük az rpm program segítségével.

```
[root@server root]# rpm -i webmin-1.121-1.noarch.rpm
Operating system is Redhat Linux 9.0
Webmin install complete. You can now login to http://192.168.1.1:10000/
as root with your root password.
```

A webmin rögtön ellenőrzi a gépen lévő linux verziót, és azt beállítja magának. Kíírja, hogy milyen címen érjük el, és szól, hogy a linux root usert, jelszóval áttette a saját felhasználói közé.

## 2.2 Debian GNU/Linux 3.0 R1

### 31. Telepítés megkezdése

A Debian GNU/Linux telepítéséhez szükséges (7db) CD-ket letölthetjük, például, az [ftp://ftp.fsn.hu/pub/CDROM-Images/debian/3.0\\_r1/images/i386/](ftp://ftp.fsn.hu/pub/CDROM-Images/debian/3.0_r1/images/i386/) oldalról ISO típusú állományokban. Ezekből, CD író program segítségével, készíthetjük el a telepítő CD-ket. A letöltéshez információkat találunk a <http://www.debian.org/distrib/ftplist> oldalon.

A CD-k boot-olhatóak. Ha erre nem alkalmas a gépünk, akkor készíthetünk indítólemezt. Az első CD /install könyvtárában megtalálhatjuk a különböző körülményekhez elkészített indítólemez fájlokat (\*.bin). Ezeket lemezre írhatjuk a /install könyvtárban található rawrite2.exe programmal:

```
rawrite2 -f root.bin -d a:  
rawrite2 -f rescue.bin -d a:
```

A két lemez közül a rescue lemezről kell boot-olni. A root lemezt később fogja kérni.

Indítsuk el a számítógépet a telepítő CD, vagy az elkészített telepítő lemez segítségével.

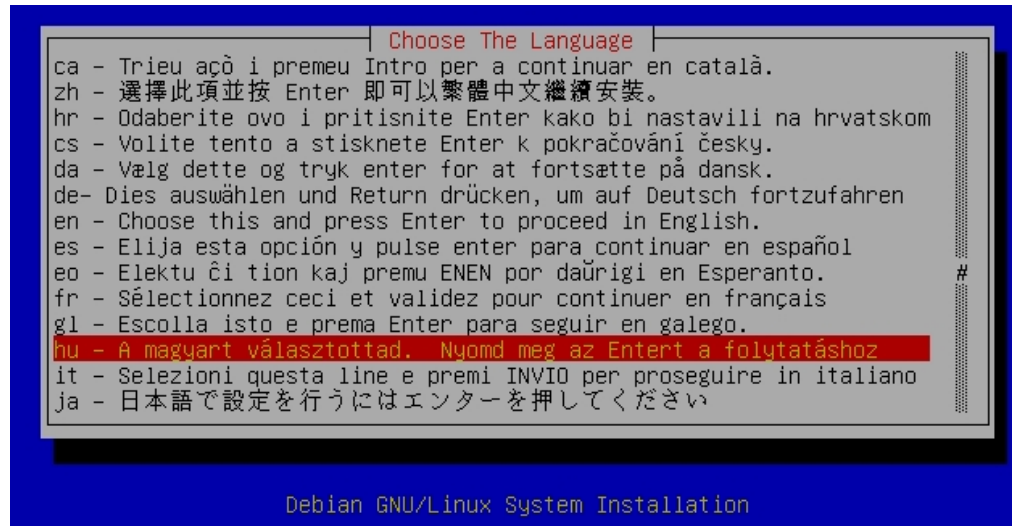
### Rendszerindító képernyő

A telepítő elindítása után a kezdőképernyő fogad minket. Itt beállíthatunk extrákat a telepítő programnak és kernelnek. Az F1 billentyű hatására erről kapunk tájékoztatást. ENTER hatására indíthatjuk a telepítést.

```
Welcome to Debian GNU/Linux 3.0!  
  
This is a Debian CD-ROM. Keep it available once you have installed  
your system, as you can boot from it to repair the system on your hard  
disk if that ever becomes necessary (press <F3> for details).  
  
For a "safe" installation with kernel 2.2.20, you can press <ENTER> to begin.  
If you want additional features like modern hardware support, specify a  
different boot flavor at the boot prompt (press <F3> to get an overview).  
If you run into trouble or if you already have questions, press <F1>  
for quick installation help.  
  
WARNING: You should completely back up all of your hard disks before  
proceeding. The installation procedure can completely and irreversibly  
erase them! If you haven't made backups yet, remove the CD-ROM  
from the drive and press <RESET> or <Control-Alt-Del> to get back to  
your old system.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law. For copyright information, press <F10>.  
  
Press <F1> for help, or <ENTER> to boot.  
  
boot: _
```

### 32. Telepítés nyelvének kiválasztása (Choose The Language)

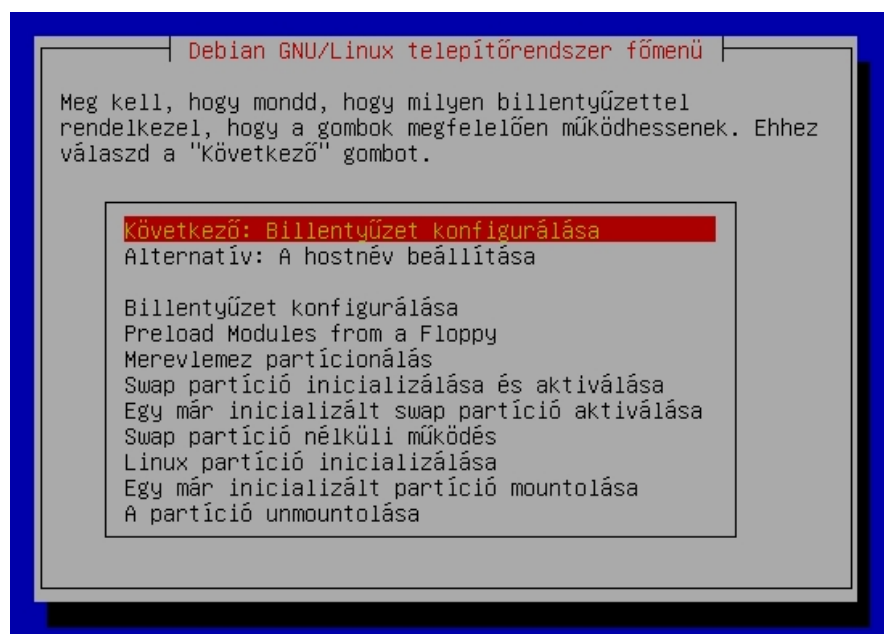
Miután betöltődött a kernel, elindul a telepítő program. Az első képernyőn kiválaszthatjuk a program nyelvét. Ez csak a telepítésre vonatkozik. Természetesen a magyart (hu – A magyart választottad) válasszuk.



A következő képernyőn egy egyszerű 'Válassz variánst!' felszólításnál tovább részletezhetjük a kívánságainkat. Itt az első sorban lévő 'Magyar' kiválasztásával haladunk tovább.

### 33. Telepítőrendszer főmenü

Most már célnál vagyunk. Ebben a telepítőrendszerben fogunk tovább kalandozni. A rendszer mindig felajánlja a következő lépést, illetve két alternatívát. Alatta, felsorolás szerűen, további lehetőségek. A lépéseket érdemes a felajánlott sorrendben végigcsinálni, de lesz olyan rész ahol a sorrendet megbolygatjuk.



### 2.2.1.1 Billentyűzet választása

A rengeteg billentyűzet kiosztás közül mi most a 'qwertz/hu : Hungarian' –t választjuk. Ez a telepített rendszerben lesz majd érvényes.

Amennyiben a winchesteren már létezett Linux rendszer és swap partíció, úgy a következő lépés ennek inicializálása lenne. Nekünk viszont még partícionálnunk is kellene. Ezért keressük meg a 'Merevlemez Partícionálása' sort és azt válasszuk.

### 2.2.1.2 Merevlemez partícionálása

A megjelenő ablakban felszólítást kapunk a merevlemez kiválasztására. Válasszuk is ki melyiket szeretnénk módosítani. Ez egy darab meghajtó esetén nem lehet gond.

A kiválasztás után kapunk egy szép hosszú 'A LILO hibái' szöveget. Ezt érdemes végig olvasni. Számunkra az a leglényegesebb üzenete, hogy a /boot partíció mindenképpen a lemez elejére kerüljön.

Folytatva a cfdisk partícionáló programba kerülünk. A felső részen láthatjuk felsorolva a partíciókat, ezek között a le-fel gombbal válogathatunk. Alatta a parancsok láthatóak, itt a jobbra-balra nyíllal navigálhatunk. Válasszuk ki a

```

cfdisk 2.11n

                Disk Drive: /dev/hda
                Size: 1082460160 bytes
    Heads: 64   Sectors per Track: 63   Cylinders: 524

-----
Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
hda1     Boot       Primary   Linux ext2   850.53
hda2                          Primary   Linux ext2   80.52
hda3                          Primary   Linux swap   150.71

```

```

[Bootable] [ Delete ] [ Help ] [Maximize] [ Print ]
[ Quit ] [ Type ] [ Units ] [ Write ]

```

Write partition table to disk (this might destroy data) **|**  
meglévő partíciókat és egyesével töröljük (Delete) őket.

A New paranccsal új partíciót vehetünk fel. Ilyenkor megkérdezi, elsődleges (Primary) , vagy logikai (Logigal) partícióról van szó. A /boot a / és a swap esetében az elsődlegest válasszuk. Mindjárt a méretnél tartunk (Size (in MB) :

.....). Írjuk be a kívánt méretet, majd ENTER. Kiválaszthatjuk, hogy előre (Beginning), vagy hátra (End) kerüljön. És már készen is vagyunk.

Egy lefele nyíllal menjünk az üres helyre (Free Space) és már vehetjük is fel a következő partíciót. Arra figyeljünk, hogy 3 elsődleges partíció után már csak logikai partíciókra van lehetőség.

Ha szemünk előtt vannak az összes felvett partíció, válasszuk ki melyik lesz a /boot könyvtárat tartalmazó és tegyük boot-olhatóvá a Bootable paranccsal.

Még hátra van a partíciók típusának megadása is. Ezt a Type paranccsal tehetjük meg. A Linux ext2 a 85, a Linux swap a 82 sorszámú.

A következő partíciókat kell felvennünk:

Csatolási pont	Típus	Méret		
/boot	Ext3	100	Fixed size	Primary
/	Ext3	500	Fixed size	Primary
-	Swap	256	Fixed size	Primary
/usr	Ext3	1000	Fixed size	
/tmp	Ext3	200	Fixed size	
/var	Ext3	1000	Fixed size	
/var/spool/squid	Ext3	2000	Fixed size	
/home	Ext3	-	Allowable	

Mindenképpen érdemes megjegyezni, hányas számú partíciót hova szeretnénk mount-olni, ugyanis a telepítő a csatolásnál már nem mutat méretet. Ha készen vagyunk ezzel is akkor a Write paranccsal kiírhatjuk a beállítást és a Quit paranccsal kiléphetünk.

Visszalépve a főmenübe, most már jöhet a Swap partíció inicializálása.

### 2.2.1.3 Swap partíció inicializálása és aktiválása

Az első ablakban egy kérdés, szeretnénk-e a hibás blokkokat keresni. Most mi nem szeretnénk, de új merevlemezen mindenképpen érdemes.

A telepítő megkeresi azt a partíciót, melynek a típusát 82-re állítottuk, majd megkérdezi, hogy ezt szeretnénk-e swap partíciónak inicializálni. Igen a válasz.

Következnek a Linux partíciók. Ezeket inicializálni kell. Ezt a lépést minden partíció esetén el kell végeznünk. Tehát erre a menüre többször kell rámenünk, amíg el nem fogynak a partíciók.

### 2.2.1.4 Linux partíció inicializálása

Több partíció esetén választanunk kell, melyiket inicializáljuk. Mindig azzal a partícióval kezdjük, amely a gyökér lesz (/). És jön is a szokásos kérdés, szeretnénk-e a hibás blokkokat keresni. Most mi nem szeretnénk, de új merevlemezen mindenképpen érdemes. A következő ablakban megerősítést kér. Igen-t válaszolva el is kezdi a munkát.

Amennyiben ez az első inicializált partíciónk, rákérdez, hogy szeretnénk-e a / (gyökérbe) mount-olni. Ha nem az első, akkor felajánl pár lehetőséget, illetve kézzel is megadhatjuk a csatolási pontot.

Amennyiben olyan partíciónk van a meghajtón, amelyet nem változtattunk és már találhatóak rajta adatok, akkor azt nem kell inicializálni csak csatolni az 'Egy már inicializált partíció csatolása' menüvel.

A következő feladat a rendszer kernel és modulok másolása. Felszólít, hogy helyezd be a telepítő CD-t. Igen válaszra már dolgozik is.

### 2.2.1.5 Elérkeztünk a kezelőprogramok beállításához.

#### Kezelőprogramok (modulok) konfigurálása

Itt a legfontosabb dolgunk a hálózati kártya beállítása lesz. Válaszuk a net sort. Ilyenkor próbálja megkeresni, detektálni a kártyát. Ha nem találja, akkor egy lista jelenik meg, ebből választhatjuk ki.

Kiválasztva a megfelelő modult, rákérdez, hogy telepítse-e a kernelbe. Természetesen Igen. A következő képernyőn a modulnak adhatunk paramétereket. A pci-os hálózati kártyáknak ez ritkán kell.

A következő képernyőn a próbálkozás után jelzi hogy sikerült-e (Installation succeeded) vagy nem (Installation failed) a modul betöltése. Vigyázat, többszöri sikeres próbálkozás több hálózati kártyát eredményez, még akkor is, ha csak egy van.

Ha megvagyunk a hálókártya beállításával akkor Exit-el kiléphetünk a modulok beállításából.

### 2.2.1.6 Hálózat konfigurálása

Az első lapon kéri a számítógép hoszt nevét. Ez nálunk 'server' lesz. Több hálókártya esetén kiválaszthatjuk, melyiket szeretnénk beállítani. Rákérdez a DHCP beállítására, de ezt ne erőltessük. És jönnek is kérdések:

IP cím: 10.0.1.13

Netmaszk: 255.255.255.240

Átjáró: 10.0.1.14  
Domain név: isk1-proba.sulinet.hu  
DNS kiszolgáló: ...

### 2.2.1.7 Az alaprendszer telepítése

Semmi mást nem kell tenni, mint várni.

### 2.2.1.8 A rendszer bootolhatóvá tétele

A megjelenő ablakban kiválaszthatjuk, hogy hova szeretnénk tenni a lilo-t. Partícióra tenni csak akkor kell, ha más operációs rendszer is van a gépünkön és az rendelkezik saját boot loaderrel. Mi most, általában a szerverek esetében, az MBR-be telepítjük. Tehát válasszuk a /dev/hda sort.

A következő a bootfloppy készítése. Ez a lemez használható fel, ha a lilo-val valami baj történik. Érdeemes készíteni, de ki is hagyható.

Légvégül válasszuk a rendszer újraindítását. A telepítő CD-t vegyük ki, hogy a merevlemezről indulhasson a feltelepített alaprendszer.

## 34. Újraindítás után

Az első indításnál automatikusan elindul a Debian System Configuration (/usr/sbin/base-config), amely ellát bennünket eldöntendő kérdésekkel.

### 2.2.1.9 Time Zone Configuration

Az első kérdés, hogy szeretnénk GMT-et használni. Itt érdemes igennel válaszolni. A következő ablakban válasszuk ki Európát, majd keressük meg Budapestet.

### 2.2.1.10 Password setup

A 'Shall I enable md5 passwords?' kérdésre mindenképpen yes-t válaszoljunk. Az MD5 jelszókódolással elérhetjük, hogy 8 karakternél hosszabb jelszavakat használhassunk, egy biztonságosabb kódolásban.

A 'Shall I enable shadow passwords?' kérdésre mindenképpen yes-t válaszoljunk. A shadow password kezeléssel elérhetjük, hogy a jelszavak nem a /etc/passwd állományban, hanem egy védettebb árnyékfájlban találhatóak.

Írjuk be a root felhasználó jelszavát, majd a következő képernyőn ismételjük meg.

Szeretnénk felvenni hagyományos felhasználót? Saját magunkat mindenképpen vegyük fel. Ha igenel válaszolunk, akkor egymás után megkérdezi a beállítóprogram az adatokat:

- Felhasználói név
- Teljes név
- Jelszó
- Jelszó ismétlése

### 2.2.1.11 Még két kérdés

A következő kérdés arra vonatkozik, hogy a telepített PCMCIA eszközmeghajtókat eltávolítsa-e. Ez általában PCMCIA eszközök hiányában tökéletes megoldás. Tehát válaszolhatunk rá igent.

Szeretnénk-e ppp kapcsolatot beállítani. Mivel nekünk csak hálózati kártya kapcsolatunk van, ezért a válasz nem.

### 2.2.1.12 APT Configuration

Itt állíthatjuk be, hogy a csomagokat milyen forrásról vegye a rendszer. Választhatunk cdrom, http, ftp, könyvtár között. Amennyiben a hálózat még nem rendelkezik Internet eléréssel, akkor a cdrom-ot válasszuk. Olyan Internet elérés esetén, amely megfelelő sebességű, választhatjuk az ftp, http lehetőséget. Ennek előnye, hogy Internetes forrásról a legújabb csomagokat kapjuk.

**FTP** beállítása esetén az első kérdés, hogy non-US csomagokat telepítsen-e a rendszer. Ezeket a csomagokat az Amerikai Egyesült Államok területén kívül lehet használni. Igennel kell válaszolnunk. Majd nem-el válaszoljunk a 'Használni szeretnél nem szabad programokat is?' kérdésre. Válasszuk ki az országot, ugye ez most Hungary lesz? A következő oldalon fel lesznek sorolva a kiválasztott országban lévő tükörszerverek. Válaszunk egyet. A választás után a szerverről letölti a csomaginformációkat.

**CDROM** választása esetén először a meghajtó forrását kell megadni, ez általában /dev/cdrom. Természetesen közben tegyük be az első lemezt. Ilyenkor a lemez tartalmát átnézve letárolja a rajta lévő csomaginformációkat. Később az így elkészült adatbázis alapján válogathatunk. Az első CD végeztével megkérdezi, hogy van-e másik CD. Tegyük be a következő lemezt és válaszoljunk igennel. Ezt egész addig végezzük, amíg el nem fogynak a CD-k.

És végül szeretnénk-e másik forrást is megadni. Lehetőség van több forrás használatára is.

A következő kérdés arra vonatkozik, hogy a frissítések letöltésére szeretnénk-e a security.debian.org hosztot használni. Ha igennel válaszolunk, akkor megpróbál csatlakozni a szerverhez és letölteni az ott található csomaginformációkat.



### 2.2.1.13 Csomag csoportok

Megint egy lépéssel előrébb vagyunk. Most a beállító program tájékoztat mindet, hogy igen kevés dolgot telepített fel a gépre és érdeklődik, hogy indítsa-e el a 'tasksel'-t. Ez egy csomagcsoport telepítő rendszer. Kipipálgathatunk számunkra érdekes telepítési témákat. Nekünk most nincs rá szükségünk, egyesével bajlódnánk a csomagokkal. Tehát a válasz nem.

### 2.2.1.14 DSelect

A Debian rendszerben már elhíresedett dselect program a csomagok telepítésére alkalmas. A beállító rendszerünk most érdeklődik, hogy elindítsa-e. Válaszoljunk nemmel, hogy később magunk indíthassuk.

### 2.2.1.15 Végjáték

Még csak az alapsomagok vannak fent, de aki Internet forrást adott meg, annak máris van frissítésre szoruló csomagja, ezen felül a pcmcia-cs csomagot is el kellene tüntetni. Tehát válaszoljunk Y-el.

A Debian-ra jellemzően a feltelepített csomagok egy részénél rögtön megkezdhetjük a beállításokat. Azaz a csomag telepítése után kérdéseket tesz fel nekünk. Ezért nem érdemes egyszerre nagy mennyiségű csomagot telepíteni, mert sokáig tartanak a kérdések.

Az eddig feltelepített csomagok közül az Exim is felteszi a kérdéseit. Ez egy mail szerver, pontosabban MTA. Mivel a könyvben majd a Sendmail-t fogjuk tárgyalni, az Exim csomag úgymint lekerül. A kérdésre válasszuk az 5-öst, azaz nem konfiguráljuk.

Ha minden jól megy ezzel vége is az előtelepítésnek.

## 35. DSELECT

Indítsuk el a dselect programot. Ez a program felelős a csomagok telepítéséért, frissítéséért és törléséért. Az alábbi menük között választhatunk:

Debian `dselect' package handling frontend.

```
* 0. [A]ccess      Choose the access method to use.
  1. [U]pdate     Update list of available packages, if possible.
  2. [S]elect     Request which packages you want on your system.
  3. [I]ninstall  Install and upgrade wanted packages.
  4. [C]onfig     Configure any packages that are unconfigured.
  5. [R]emove     Remove unwanted software.
  6. [Q]uit       Quit dselect.
```

Move around with ^P and ^N, cursor keys, initial letters, or digits;  
Press <enter> to confirm selection. ^L redraws screen.

Version 1.9.21 (i386).

Copyright (C) 1994-1996 Ian Jackson.

Copyright (C) 2000 Wichert Akkerman.

This is free software; see the GNU General Public Licence version 2  
or later for copying conditions. There is NO warranty. See  
dselect--licence for details.

- **Access.** A csomagok elérésének forrását lehet állítani.
- **Update.** A már telepített csomagok tekintetében ellenőrzi a beállított forráson lévő új verziókat és telepíti azokat (update).
- **Select.** Itt választhatjuk ki a telepítendő, illetve törlendő csomagokat.
- **Install.** A telepítésre kijelölt csomagok telepítése.
- **Config.** Az újonnan telepített csomagok beállítását végzi. A csomagok egy részének beállítása már az Install menünél megtörténik.
- **Remove.** A törlésre kijelölt csomagok törlése.
- **Quit.** Kilépés a dselectből.

A Select menüpontot válasszuk. A bejelentkező képernyő szököz billentyű leütésére továbblép. Most nézzük, hogy navigálhatunk:

```
dselect - main package listing (avail., priority) mark:+/=- verbose:v help:?
EIOM Pri Section Package Inst.ver Avail.ver Description
- All packages -
--- Up to date installed packages ---
----- Up-to-date Required packages -----
----- Up-to-date Required packages in section base -----
*** Req base base-files 3.0.2 3.0.2 Debian base system miscel
*** Req base base-passwd 3.4.1 3.4.1 Debian Base System Passwo
*** Req base bash 2.05a-11 2.05a-11 The GNU Bourne Again SHel
*** Req base bsduutils 2.11n-7 2.11n-7 Basic utilities from 4.4B
*** Req base debianutils 1.16.2woody 1.16.2woody Miscellaneous utilities s
*** Req base diff 2.7-29 2.7-29 File comparison utilities
All packages
The line you have highlighted represents many packages; if you ask to
install, remove, hold, &c it you will affect all the packages which match
the criterion shown.

If you move the highlight to a line for a particular package you will see
information about that package displayed here. You can use 'o' and 'O' to
change the sort order and give yourself the opportunity to mark packages in
different kinds of groups.
```

```
description
```

Nyilak (le, fel) és a Page-Up, Page-Down gombokkal tudjuk a csomaglista gördíteni. A '/' gomb után szöveget beírva kereshetünk a listában.

A '+' gombbal tudunk telepítésre kijelölni.

A '-' gombbal tudunk törlésre kijelölni.

A '\_' (aláhúzás) gombbal tudunk törlésre kijelölni ez a konfigurációs fájlokat is törli.

A Shift+Q-val tudunk visszatérni a dselect főmenübe.

Az F1 billentyűre további funkciókról láthatunk segítséget.

A lista elején láthatjuk a már telepített csomagokat. Már vannak kijelölve alapcsomagok, amelyek még nem lettek telepítve. Most ne jelöljünk ki semmit, viszont pár csomagot levehetünk (aláhúzás billentyűvel):

- g++
- gcc
- gcc-3.0
- gcc-3.0-base
- gdb
- cpp
- finger
- nfs-commen

Ha ezeket a csomagokat kijelöltük törlésre, akkor a SHIFT+Q-val térjünk vissza a főmenübe. Itt egymás után menjük végig a következő menüpontokon:

- Install (lehet hogy egy-két csomag alapvető beállításokra kérdez rá)
- Configure
- Remove

Ezzel valóban befejeztük az alaptelepítést, viszont a szerver-szolgáltatások még nincsenek fent. Az utóbeállítások miatt ne telepítsünk egyszerre túl sok csomagot. Érdeemes csoportokra bontani. A megoldás mindig azonos. A Select menüpontban kiválasztjuk a csomagokat, majd Install és Configure menü.

## 36. Szükséges csomagok telepítése

### Midnight Commander

Az első esetben nézzük meg részletesen, milyen lépéseken kell végigmennünk:

- Keressük meg az mc csomagot (opt/utils).
- '+'-al jelöljük ki telepítésre.
- Függségek vannak, erről tájékoztatást kapunk.
- Szóközzel tovább léphetünk a üzenet képernyőről.
- Látjuk a függőségeket.
  - A mc-common, libglib1.2, libgpmg1 csomagok mindenképpen kellene, ezek már be is vannak jelölve.
  - A gpm, rpm csomagok javasoltak, de ezeket nekünk kell bejelölni, most nem tesszük.

- ENTER-el visszamehetünk a csomaglistára, ezzel elfogadjuk a javasoltakat.
- SHIFT+q-val a csomagkiválasztást nyugtázzuk és megyünk a főmenübe.
- Install menüpontot válasszuk, itt láthatjuk, hogy 4 csomagot kell felhelyezni.
- ENTER-el vagy Y ENTER-el elfogadjuk, hogy telepítsen.
- A csomagok letöltése (CD esetén másolása) és a telepítés folyamatban van.
- Telepítés után kérdés, törölje-e a csomagot, válaszoljunk igent.
- Visszatérünk a főmenübe, itt a Config menüpontot választjuk.
- Ez pillanatok alatt megvan.
- Vége, a Midnight Commander telepítve lett.

### **Alap csomagok:**

- Opt/admin/quota
- Opt/admin/sudo
- Opt/admin/sysstat
- Opt/misc/gpm
- Opt/net/iptraf
- Opt/net/traceroute
- Opt/utils/openssl
- Xtr/net/xinetd

### **E-mail és E-mail szerver:**

- Opt/mail/fetchmail
- Opt/mail/fetchmailconf
- Opt/mail/fetchmail-common
- Opt/mail/ipopd-ssl
- Xtr/mail/sendmail

### **Samba fájlserver**

- Opt/net/samba
- Opt/net/samba-common
- Opt/net/swat

### **DNS szerver, DHCP szerver, SQUID, MYSQL:**

- Opt/net/bind9
- Opt/net/dhcp3
- Opt/net/dhcp3-client
- Opt/net/dhcp3-common
- Opt/net/dhcp3-server
- Opt/net/dhcp3-relay
- Opt/web/squid
- Opt/misc/mysql-client
- Opt/misc/mysql-common
- Opt/misc/mysql-server

### **APACHE web szerver:**

- Opt/web/apache
- Opt/web/apache-common
- Opt/web/apache-ssl
- Opt/web/php4
- Opt/web/php4-gd
- Opt/web/php4-imap
- Opt/web/php4-mysql

**Web-alapú programok:**

- Opt/web/squirrelmail
- Opt/web/wealizer
- Xtr/net/mrtg
- Xtr/web/phpmyadmin

**WEBMIN:**

- Opt/admin/webmin
- Opt/admin/webmin-burner
- Opt/admin/webmin-quota
- Opt/admin/webmin-samba
- Opt/admin/webmin-software
- Opt/admin/webmin-squid
- Opt/admin/webmin-status
- Opt/admin/webmin-apache
- Opt/admin/webmin-core
- Opt/admin/webmin-dhcpd
- Opt/admin/webmin-ipadmin
- Opt/admin/webmin-mysql
- Opt/admin/webmin-ppp
- Xtr/admin/webmin-fetchmail
- Xtr/admin/webmin-grub
- Xtr/admin/webmin-sendmail
- Xtr/admin/webmin-sshd
- Xtr/admin/webmin-xinetd

A csomagok telepítése közben, néhánynál beállításokra vonatkozó kérdéseket is kapunk. Ezekre értelemszerűen lehet válaszolni. A lényegi beállítások úgyis ezután fognak következni.

Amennyiben ezzel készen vagyunk, már majdnem készen van a szerver a beállításokhoz. A sendmail telepítése után érdemes elindítani a sendmailconfig programot. Ez készíti el az alapbeállítás fájljait.

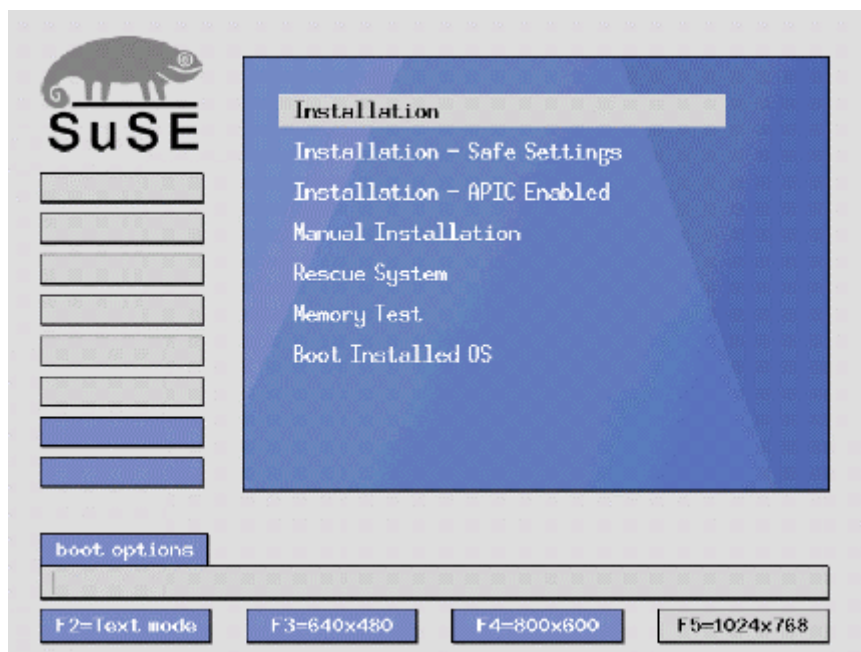
## 2.3 SUSE LINUX 8.2 Professional

### 37. Telepítés megkezdése

A SUSE LINUX 8.2 telepítéséhez szükséges (5 db) CD-ket nem lehet ISO állományban letölteni, viszont a másolása és a felhasználása nem korlátozott. Hozzájuthatunk kereskedelemben a telepítő csomaghoz (5 CD, 2 DVD, magyar nyelvű könyv), vagy elkérheti ismerősétől és másolhatja (ez is legális). A CD-k bootolhatóak. Indítsuk el a számítógépet a telepítő CD segítségével.

### 38. Rendszerindító képernyő

A telepítő elindítása után a kezdőképernyő fogad minket. A menük közül (10 másodpercen belül) válasszuk ki a nekünk megfelelőt.



- **Boot from Harddisk**  
A már telepített rendszer indítása.
- **Installation**  
Normál telepítés.
- **Installation – ACPI Disabled**  
Régebbi gépeknél még támogatott fejlett programozható megszakításvezérlő (ACPI) tiltása.
- **Installation – Safe Settings**  
A rendszermag betöltésénél (telepítés közben) kikapcsolódnak a nem szükséges funkciók. (pl.: DMA, Energiagazdálkodás). Normál telepítés fagyásánál érdemes használni.
- **Manual Installation**

A driver-eket nem felismerés útján határozza meg a telepítő, hanem egyenként kézzel kell beállítani őket. Akkor érdemes használni, ha a telepítő egy eszközt nem ismer fel (pl.: régi ethernet kártya).

- **Rescue System.**

A CD-ről egy karakteres rendszer indul el. Kiválóan alkalmas a telepített rendszer hibáinak javítására, ha nem képes elindulni.

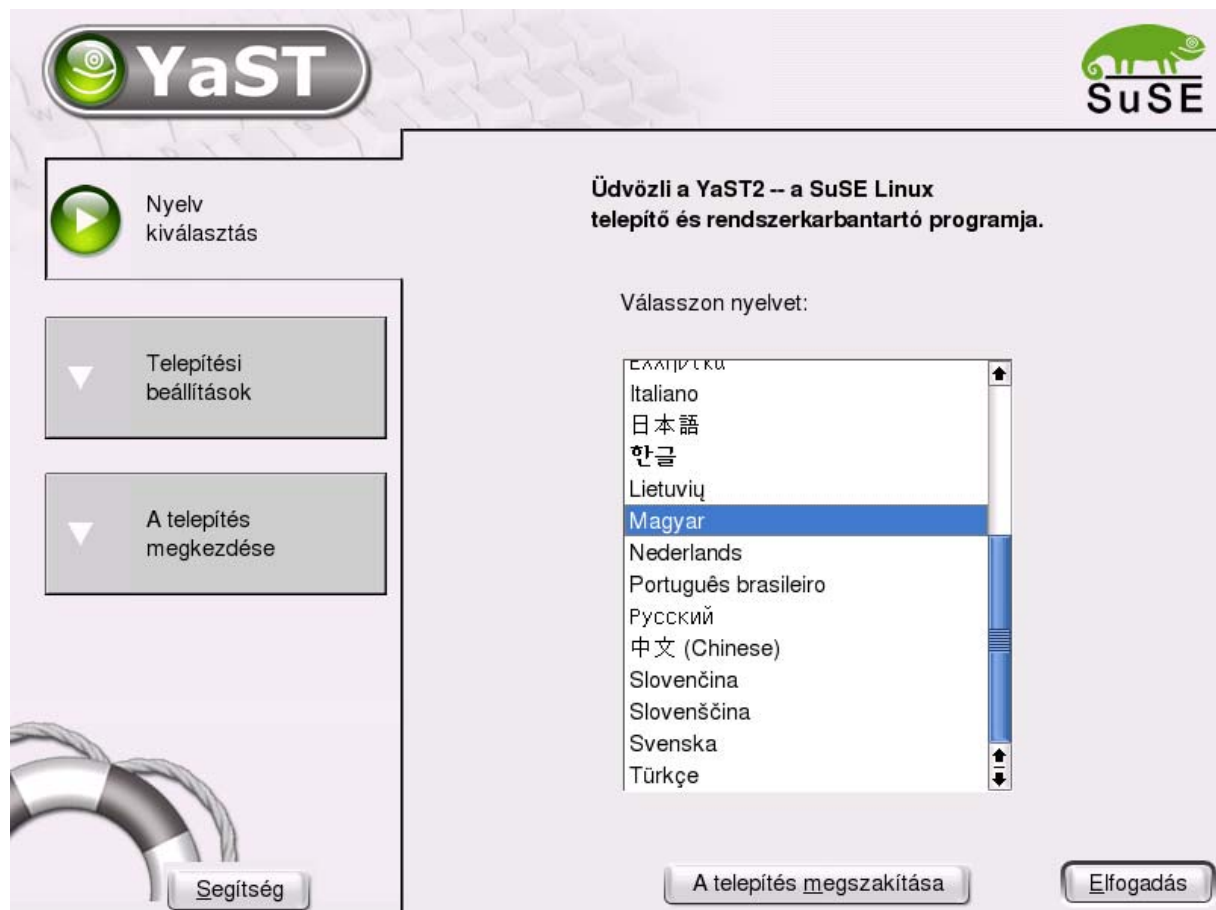
- **Memory Test.**

Elindítja a Memtest-86 v3.0 programot, amely a memória ellenőrzésére szolgál.

A kernelnek indulási opciókat is megadhatunk a boot options sornak. Itt adhatjuk meg a teljes képernyős szöveges mód használatát is. Paraméterként írjuk be 'textmode=1'.

Válasszuk a normál telepítési módot 'Installation'. A továbbiakban, a kernel betöltődése után, a YaST telepítőprogram fog elindulni.

### 39. Telepítés nyelvének kiválasztása (Language Selection)



Válasszuk ki a Magyar nyelvet majd kattintsunk az elfogad gombra. Ilyenkor a telepítő feltérképezi a gépet, majd megjelenő ablakban válasszuk az 'Új telepítés'-t.

## 40. Telepítési beállítások

A telepítési beállításokat átnézzük, illetve módosítjuk. Amennyiben az elfogadás gombra kattintunk, a telepítés megkezdődik. Ilyenkor már nem módosíthatjuk a beállításokat.

A beállításokat átnézve az elején a telepítési mód, billentyűzet, egér paramétereit látjuk. Ezt már nem feltétlenül kell módosítanunk.

### 2.3.1.1 Partícionálás

Az első módosítandó rész a 'Partícionálás' lesz. Kattintsunk is rá a címsorra. A következő képernyőn a javasolt partícionálás jelenik meg. Alul kérdéssor:

- Javaslat elfogadása. Ez természetesen nem felel meg nekünk, ugyanis a saját meghatározott bontásunkkal szeretnénk dolgozni.
- Kézi partícionálás a Yast2 javaslata alapján.
- Szakértői kézi partícionálás

Miután a kézi partícionálást választottuk, megjelennek a meghajtók és a jelenlegi partíciók. Álljunk rá a megfelelő partícióra és töröljük a 'TÖRLÉS' gombbal.

A merevlemez partícionálása...

Csak **szakértőknek** ajánljuk. Ha nincs tisztában azzal, hogy mi a **partíció** és hogy hogyan kell azt használni, javasoljuk, hogy térjen vissza az **automatikus** partícionáláshoz.

Jó ha tudja, hogy **semmi nem változik a merevlemezén**, amíg meg nem erősíti a telepítést az utolsó telepítési párbeszédablakban. Egészen addig, bármikor biztonságosan kiléphet a telepítéből.

Az LVM beállításához azt javasoljuk, hogy hozzon létre nem-LVM alapú root partíciót és cserepartíciót. E két partíción kívül létre kell hoznia azokat a partíciókat is (legalább egyet), melyekre az LVM épül majd.

A jobb oldali táblázatban láthatja merevlemezei jelenlegi

**Szakértői partícionálás**

Eszköz	Méret	F	Típus	Csatolás	Kezdet	V
/dev/hdc	3.0 GB		QUANTUM FIREBALL SE3.2A		0	
/dev/hdc1	82.7 MB	F	Linux native (Ext3)	/boot	0	
/dev/hdc2	500.0 MB	F	Linux native (Ext3)	/	21	
/dev/hdc3	259.8 MB	F	Linux swap	swap	148	
/dev/hdc4	2.1 GB		Extended		214	
/dev/hdc5	1000.1 MB	F	Linux native (Ext3)	/usr	214	
/dev/hdc6	82.7 MB	F	Linux native (Ext3)	/tmp	468	
/dev/hdc7	1000.1 MB	F	Linux native (Ext3)	/var	489	
/dev/hdc8	153.5 MB	CF	Linux native (Reiser)	/home	743	

Létrehozás Szerkesztés Törlés Átméretezés

LVM... RAID... Titkosított Fájl... Szakértő...

Vissza Következő



Miután minden felesleges partíciót eltüntettünk, megkezdhetjük felvenni a sajátjainkat. Először mindenképpen a /boot partícióval kezdjük.

A létrehozás gombbal tudjuk elkezdeni a munkát. A megjelenő ablakban válasszuk ki, hogy elsődleges, vagy kiterjesztett partíciót szeretnénk felvenni. Elsődleges partícióból 4 db lehet, amelyből egyet levesz a kiterjesztett partíció lehetősége.

A megjelenő ablakban tudjuk beállítani a partíció tulajdonságait. A formázás nélkül lehetőséget akkor használjuk, ha egy meglévő, tartalommal rendelkező partíció csatolási pontját szeretnénk beállítani. Itt ki kell választani a partíció meglévő fájlrendszerét. A SUSE LINUX alapértelmezett esetben a ReiserFS fájlrendszert használja. Amennyiben a linuxos hagyományos felhasználókezelést (tulajdonos, csoport, a többiek) ki szeretnénk egészíteni az ún. hozzáférési listákkal (Access Control Lists, ACL), ahol minden egyes felhasználó számára külön-külön be lehet állítani a hozzáférési jogosultságokat, akkor mindenképpen a ReiserFS fájlrendszert használjuk. Ebben a tananyagban az egyszerűség kedvéért SUSE LINUX alatt is az ext3-at használjuk.

Egy létező partíció esetén csak két beállítási lehetősége van: Megadhatja a csatolási pontot és dönthet a formázásról.

**Partíció szerkesztése/dev/hdc1**

Formázás

Formázás nélkül

Fájlrendszer azonosító (ID):

0x83 Linux

Formázás

Fájlrendszer

Ext3

Opciók

Fájlrendszer titkosítása

Méret

Cilinder méret: 3.93 M

Kezdő cilinder:

0

Vége: (9 vagy +9M vagy +3.2GB)

+80M

Fstab opciók

Csatolási pont

/boot

OK Mégsem

A formázás lehetőséget használjuk új telepítésnél. Itt lehetőségünk van kiválasztani, milyen típusúra legyen formázva a partíciónk. Normál partíció esetén válasszuk az ext3-at, swap partíció esetén a SWAP-et. Beállíthatjuk a fájlrendszer paramétereit is, erre általában nincs szükség, illetve titkosíthatjuk is.

A jobb oldalon adhatjuk meg a kezdő cilinder és az utolsó cilinder számát, azaz mettől meddig tartson a partíció. Alapban ez mindig a rendelkezésre álló hely eleje és vége. A vége részhez írhatjuk be a partíció méretét is +100M formában, ekkor a kezdő cilindert ne módosítsuk.

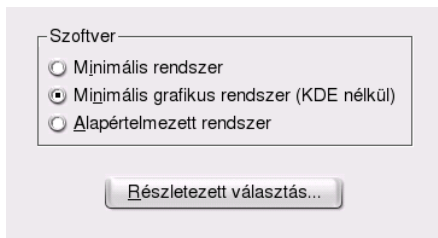
A csatolási pont beállítása jobb alul lehetséges. Felette a csatolási paramétereket lehet állítani (fstab opciók) ezt még szintén nem érdemes bántani.

Most vegyük fel a következő partíciókat:

Csatolási pont	Típus	Méret		
/boot	Ext3	100	Fixed size	Primary
/	Ext3	500	Fixed size	Primary
-	Swap	256	Fixed size	Primary
/usr	Ext3	1000	Fixed size	
/tmp	Ext3	200	Fixed size	
/var	Ext3	1000	Fixed size	
/var/spool/squid	Ext3	2000	Fixed size	
/home	Ext3	-	Allowable	

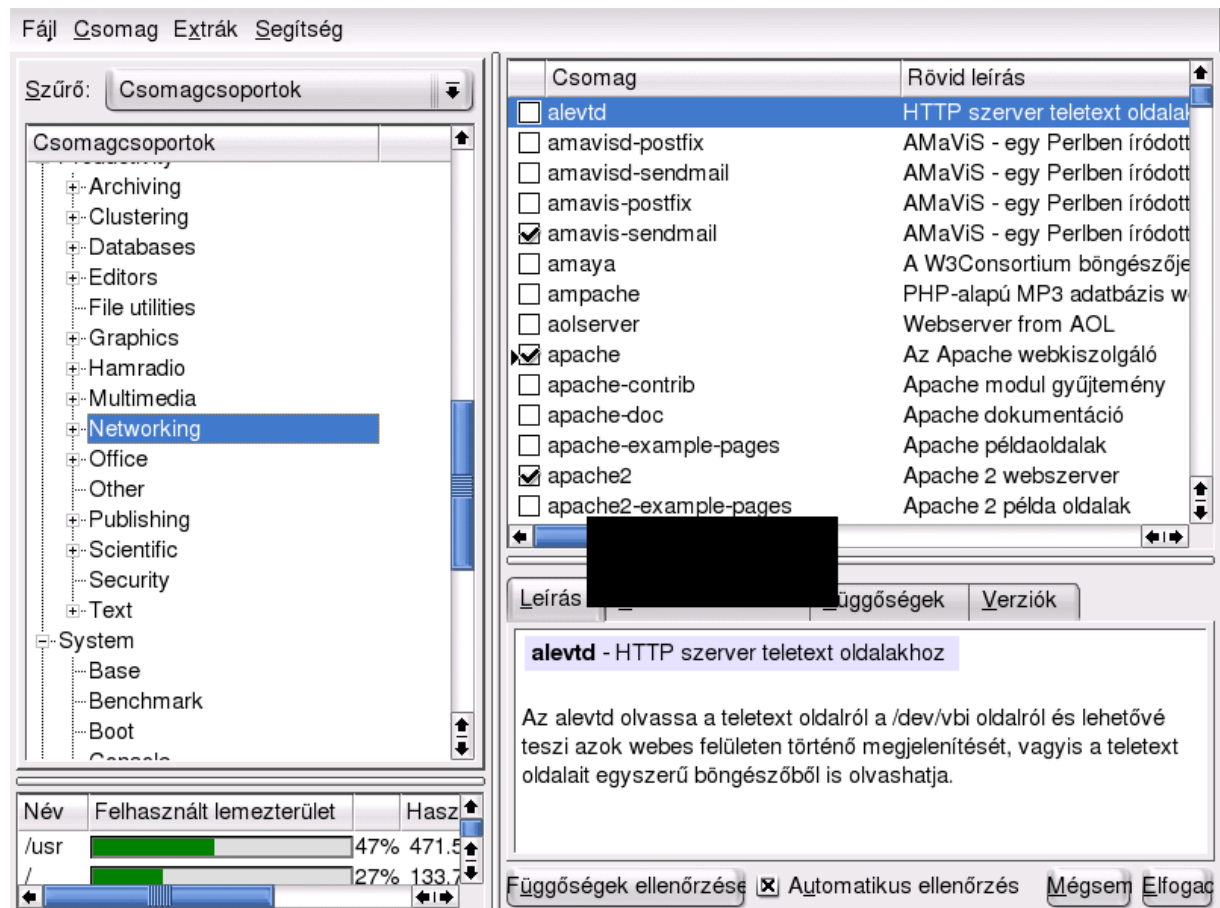
Ha készen vagyunk az elfogadásával visszatérünk a Telepítési Beállítások képernyőre.

### 2.3.1.2 Szoftver



Elérkeztünk a telepítendő programok meghatározásához. A Szoftver címsorra kattintva máris választhatunk három lehetőség közül. Nekünk a minimális rendszer a megfelelő. Rákattintva a részletek változtatására, a csomagokat egyenként tudjuk kijelölni. Nekünk pont ez kell.

A csomagok listázását bal felül váltsuk át csomagcsoportok szűrő módba. Ezzel könnyebb dolgunk lesz a kategóriáknál. Jobb alul pipáljuk ki a függőségek automatikus ellenőrzését.



Amennyiben szervert telepítünk, a következő csomagokra NEM lesz szükségünk, ezek mellől vegyük le a pipát:

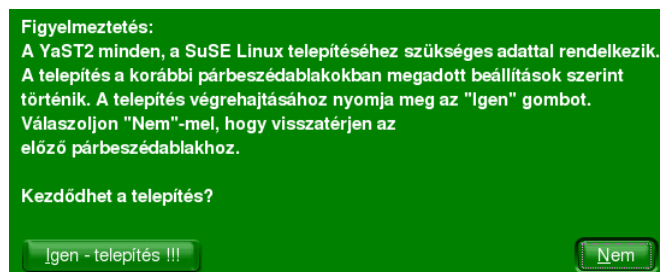
- Development/Languages
  - cpp
- Productivity/Networking
  - finger
  - rsh
  - telnet
  - w3m

Amennyiben szervert telepítünk, a következő csomagokra lesz még szükségünk, ezek mellé tegyük pipát:

- Productivity/Database
  - mysql
  - mysql-bench
  - mysql-client
  - mysql-Max
- Productivity/File utilities
  - mc
- Productivity/Networking
  - apache2
  - apache2-mod\_php4 (itt függőség problémánk lesz, válasszuk a messasoft telepítését)

- apache2-prefork
- apache2-worker
- bind9 (bind9-utils)
- dhcp-server (dhcp-base, dhcpd)
- fetchmail
- fetchmailconf
- iptraf
- lynx
- mod\_frontpage
- mod\_php
- mod\_php-core
- mod\_ssl
- mrtg
- mtr
- phpmyadmin
- samba
- samba-client
- samba-vscan
- sendmail (itt függőség problémánk lesz, válasszuk a postfix eltávolítását)
- squid
- webalizer
- wget
- xinetd
- popper
- spamassassin
- squirrelmail
- amavis-sendmail
- Security
  - tmpwatch
  - tripwire
- System/Base
  - sudo
- System/Management
  - webmin

A csomagok kiválasztása után menjünk tovább az elfogad gombbal. A telepítő tájékoztat minket a további függőségekről, ezt is fogadjuk el.



Ekkor visszatérünk ismét a telepítési beállításokhoz. Mást már itt nem kell módosítanunk, lépünk tovább. Ekkor a telepítő felmásolja az első cd-t, végez egy kis beállítást és újraindítja a rendszert. Az újraindulást már a merevlemezről végezni, ha bennt maradt a telepítő cd, akkor ne bántsuk, az első menüpont alapján dolgozzon.

## 41. Első indítás

Még hátra van a többi cd felmásolása. Rögtön itt is folytatjuk, szépen adagoljuk a CD-eket.

### 2.3.1.3 Root jelszó megadása

Adjuk meg a root felhasználó jelszavát, majd ismételjük meg. A Szakértői beállítások (Expert options) alatt állítsuk át a jelszavak kódolását MD5-re. Ha kész vagyunk, kattintsunk Következő (NEXT) gombra.

### 2.3.1.4 Hálózat beállítása

A telepítő detektálja a hálózati eszközöket, majd az eredményt megjeleníti. Nekünk csak a Hálózati eszköz (Network interfaces) érdekes, lépünk is bele. A felső részen új hálózati kártyát adhatunk kézzel hozzá, alul a már meglévő (betöltött) kártyák látszanak. Lépünk rá a jobb alul lévő Szerkesztésre (change), majd az eth0-s kártyára.

A DHCP lekérést állítsuk át Statikus címre és adjuk meg az IP-címet, hálózati maszkot. Állítsuk be a gép nevet és a DNS-eket. Majd a útválasztásnál (routing) az alapértelmezett átjárót. Ezzel a hálózati kártyánkat beállítottuk, léphetünk tovább. A hálózati beállítás mentésre kerül.

### 2.3.1.5 Internet kapcsolat ellenőrzése

Megjelenik egy kérdés, hogy ellenőrizze-e az Internet kapcsolatot, ezt elfogadhatjuk (ha már van kapcsolat).

### 2.3.1.6 Online Updates

Amennyiben az Internet kapcsolat ellenőrzése nem mutatott hibát, lehetőségünk van a feltelepített csomagok frissítésére. Érdeemes kihasználni ezt a lehetőséget, de később is megoldható a YaST-al.

### 2.3.1.7 Felhasználó azonosításának helye

Itt állíthatjuk be, hogyan történjen a felhasználók azonosítása. Van lehetőség másik gépen tárolt felhasználók átvételére is. Ennek kihasználásával csak egy gépen kell a felhasználókat nyilvántartani. Beállíthatunk kapcsolatot NIS, LDAP szerverekkel, ezen lehetőségeket akkor engedélyezzük, ha tudjuk, hogy ilyen szerver működik, egyébként ne. Ne módosítsunk a beállításokon, menjünk tovább.

### 2.3.1.8 Felhasználók felvétele

Van lehetőségünk megkezdeni a felhasználók felvételét. Egy adminisztratív felhasználót vegyünk fel, a többit hagyjuk későbbre. Érdemes kijelölni, hogy ez a felhasználó kapja a rendszerüzeneteket.

Ezzel végeztünk is a telepítéssel.

## 2.4 Gyakorlat

Telepíts fel a leírás alapján egy szerveret az általad kiválasztott Linux disztribúcióval. A telepítésnél figyelj a csomagok kiválasztására, ugyanis ezen a szerveren fogunk dolgozni a következő fejezetekben. A folyamat az előző fejezetben kialakított terv alapján történjen.

## 2.5 Felhasznált, ajánlott irodalom

SUSE LINUX Rendszerkézikönyv  
`suselinux-adminguide_hu-8.2.0.1-0.i586.rpm`

SUSE LINUX Felhasználói kézikönyv  
`suselinux-userguide_hu-8.2.0.1-0.i586.rpm`

A Redhat Package Manager használata  
[http://www.szabilinux.hu/rpm/rpm\\_hasznalata.html](http://www.szabilinux.hu/rpm/rpm_hasznalata.html)

apt - a dpkg egyik frontendje.  
<http://www.szabilinux.hu/apt/index.html>

dselect - a dpkg "másik" frontendje  
<http://www.szabilinux.hu/dselect/index.html>

## 3. Finomhangolás, ismerkedés a rendszerrel

### 3.1 Első belépés

Indulás után először a boot loader-el találkozunk. Ha nem nyulunk hozzá, akkor pár másodperc után elindítja az alapértelmezett kernel-t. Két ismertebb boot loaderrel találkozhatunk, a lilo és a grub. A grub boot loader fejlettebb, ezért manapság ezt használják.

A kernel beindulásának folyamatát követhetjük végig a képernyőn. A kernel és a kernel modulok betöltődése után elindul az alapértelmezett (init3) inicializáló. Ez a folyamat gondoskodik a rendszer működéséhez szükséges programok elindulásáról. Minden program jelezni fogja, hogy indulása sikeres, vagy sikertelen. Erre érdemes figyelni.

Ha egy-egy program indulására szokatlanul sokat kell várni, akkor valami hálózati beállítási hibáról lehet szó. Ilyen lehet, ha a hálózati kártya nem tudja DHCP-n keresztül letölteni a címeket, vagy rossz beállítás esetén a sendmail várakozhat.

A folyamat végén megjelenik a bejelentkező képernyőnk (virtuális konzol). Alapértelmezésben 6 karakteres konzolunk van. Az ALT gomb mellett az első 6 funkcióbillentyűvel (ALT+F1, ALT+F2 ... ALT+F6) tudunk kapcsolgatni közöttük. Grafikus konzolok az utolsó karakteres konzol után találhatóak (CTRL+ALT+F7). Akár több konzolon is dolgozhatunk egyszerre, ez néha megkönnyíti a munkánkat.

A bejelentkező képernyő némi bemutatkozás után kéri a felhasználó nevét, majd ENTER után a felhasználó jelszavát. Lépjünk be a root felhasználóval és azzal a jelszóval, melyet telepítéskor megadtunk. Amennyiben a felhasználónév és a jelszó megfelelő volt, a rendszer kiírja az utolsó belépésünk idejét és tájékoztat a leveleinkről, majd megkapjuk a shell-t, azaz a parancssort. A virtuális konzolról az exit, vagy a logout paranccsal jelentkezhethetünk ki.

A shell prompt-jának a vége root felhasználó esetén #, míg normál felhasználónál \$ jel. Lehetőleg még saját szerverünkre se lépjünk be root-ként, hacsak nem olyasmit szeretnénk tenni, ami mással nem megy. Némi beállítással (sudo) megoldható, hogy a rendszergazda műveletek egy részét engedélyezzük normál felhasználónak. Ezzel a biztonságot növeljük és teljesen elkerülhetjük a root felhasználó alkalmazását.

Tájékozódjunk egy kicsit a rendszerünkön. Ehhez nagy segítséget tud nyújtani a Midnight Commander. Indítsuk el az mc paranccsal.

```

Left      File      Command  Options  Right
< /etc/httpd/conf v>
  Name    Size    MTime
  /..     4096   ul 25 2001
  /ssl.crl 4096   pr 30 14:11
  /ssl.crt 4096   pr 30 14:11
  /ssl.csr 4096   ul 25 2001
  /ssl.key 4096   pr 30 14:11
  /ssl.prm 4096   pr 30 14:11
  acces~conf 285    ep 6 2001
  httpd.conf 50861  ug 18 20:05
  magic   12441  ep 6 2001
  @Makefile 37     ug 18 18:42
  roami~conf 198    un 25 2001
  srm.conf 297    ep 6 2001

  Name    Size    MTime
  /..     4096   ug 19 13:54
  /bin    4096   pr 30 14:06
  /boot   4096   pr 30 14:16
  /dev    77824  ug 19 13:54
  /etc    4096   ug 19 13:54
  /home   4096   ug 18 16:09
  /initrd 4096   un 21 2001
  /lib    4096   pr 30 14:06
  /lost+found 16384  pr 30 13:56
  /mnt    4096   pr 30 18:06
  /opt    4096   ug 23 1999
  /proc   0       ug 19 13:53
  /root   4096   ug 19 10:14
  /sbin   4096   pr 30 14:13
  /tmp    4096   ug 19 10:12

/..
Hint: The file listing format can be customized; do "man mc" for
[root@192 conf]#
1Help 2Menu 3View 4Edit 5Copy 6RenMov 7Mkdir 8Delete

```

A gyökérben a következő könyvtárakat találjuk:

/bin	Linux szabvány parancsait és a shell-eket tárolja.
/boot	Linux kernel (kernelek) találhatóak benne. Innen indul el a rendszer
/dev	Eszközkönyvtár. Tartalmát a kernel induláskor állítja össze. Minden eszköz ebben a könyvtárban található meg eszközfájl formájában. Ezért például a lemezes meghajtóra /dev/fd0, a merevlemezre /dev/hda, a nyomtatóra /dev/lp0 néven hivatkozhatunk.
/etc	Ebben a könyvtárban találhatóak a rendszer és a programok beállításai. Jellemző, hogy text fájlokban állítjuk be a paramétereket. Ennek előnye, hogy a mindehhez elég egy egyszerű editor és másolhatóak egyik gépről a másikra.
/home	Itt találhatóak a felhasználók könyvtárai.
/lib	Osztott rutinkönyvtárak találhatóak benne.
/mnt	Ez a könyvtár alá fűzhetjük be a nem állandó meghajtókat. Pl: /mnt/floppy, /mnt/cdrom
/proc	Tartalmát a futó programok (processzek) információi töltik ki.
/root	Root felhasználó könyvtára
/sbin	Parancskönyvtár, jellemzően rendszer közeli parancsok fájljait tartalmazza.
/tmp	Átmeneti fájlok helye
/usr	A rendszer indításához és alapvető működéséhez nem szükséges programok helye.
/var	Változó adatok könyvtára

A fenti listából, a mi szempontunkból leglényegesebb könyvtár a /etc. Itt találhatóak a beállítások text fájlban. A fájlokat Midnight Commander F4 gombjával, vagy editáló programmal (vi, vim, joe) tudjuk szerkeszteni. Mielőtt elkezdünk ismerkedni vele, mentsük le a tartalmát. Lényegesegek lehetnek a Linux által használt jogosultsági attribútumok, hiszen olyan mentési megoldást kell találnunk, amely ezeket megőrzi. Ismerkedjünk meg a tar csomagoló programmal. Ez egy parancssoros csomagoló és a jogosultságokat megőrzi.

Aktuális könyvtár becsomagolása: `tar -cf /root/mentes.tar ./*`

Kicsomagolás az aktuális könyvtárba: `tar -xf /root/mentes.tar`

Akkor csomagoljuk össze a /etc könyvtárat, hogy ha valami galibát csinálunk, akkor legyen egy kiindulási pontunk.

```
# cd /etc
# tar -cf /root/etc.tar ./*
```

Telepítés után, a telepítő rendszer hagy maga után a telepítés folyamatát mutató log állományokat a /root könyvtárban. Érdekes ezt is elmentenünk.

Ha már a mentetetésnél tartunk, akkor ne felejtsük el a partíciós táblát elmenteni egy lemezre, később még jól jöhet.

Partíciós tábla mentése:

```
# mount /mnt/floppy
```



```
# dd if=/dev/hda of=/mnt/floppy/server.part bs=512 count=1
```

Partíciós tábla visszatöltése: (ezt majd később használjuk ☺ )

```
# mount /mnt/floppy
```

```
# dd if=/mnt/floppy/server.part of=/dev/hda bs=1 count=64 skip=446 seek=446
```

## **/etc könyvtár ismertebb fájlljai**

Nézzünk meg néhány jellemző beállítási fájlt.

### - **/etc/fstab**

Ebben a fájlban találjuk meg a partíciók csatolási adatait.

### - **/etc/host.conf**

Itt állítjuk, hogy a névfeloldás hogyan történjen. Mindjárt állítsunk is egy kicsit rajta. Jelenleg 1 sort tartalmaz:

**order hosts, bin**

ez azt jelenti, hogy először a /etc/hosts fájlban próbálkozik, utána a DNS szerverrel. Írjunk hozzá még két sort:

**multi on**

A névhez tartozó összes IP-t kérje le.

**nospoof on**

Kiküszöböli a DNS átejtést.

### - **/etc/host**

Ebbe a fájlba vehetünk fel IP, hostnév párosítást. A névfeloldásnál ezt a fájlt (mint az /etc/host.conf-ban láttuk) előbb hajtja végre, mint a DNS kérést, ezért érdemes felvenni a saját gépünk adatait. Tehát adjunk hozzá egy sort (ipcím <tab> hostnév).

**196.110.12.1 server.iskola-varos.sulinet.hu**

### - **/etc/resolv.conf**

Ez az állomány tartalmazza, hogy a névfeloldáshoz melyik name szervereket használja a rendszer:

nameserver 195.199.0.133

nameserver 195.199.0.121

### - **Csoportokat és felhasználókat kezelő fájlok.**

A felhasználók adatait a /etc/passwd tartalmazza. A felhasználónevek kezelése miatt mindenki számára olvashatóvá kell tenni, ezért a jelszavakat nem itt, hanem a /etc/shadow állományban tároljuk. A csoportok adatai a /etc/group állományban találhatóak, melynek szintén létezik árnyékfájlja, ez a /etc/gshadow.

/etc/passwd felhasználók

Felépítés (kettősponttal elválasztva):

felhasználónév:x:userID:csoportID:teljes név:home könyvtár:shell

Példa:

kati:x:501:500:Katalin:/home/kati:/bin/false

```
/etc/shadow jelszavakat tartalmazó fájl
/etc/group csoportok
Felépítés (kettősponttal elválasztva):
csoportnév:x:csoportID:csoport tagjai vesszővel elválasztva
Példa:
Users:x:500:kati,evi,laci
/etc/gshadow
```

#### - Felhasználók felvételét szabályozó beállítások

Felhasználókat adduser paranccsal tudunk felvenni (törlés: userdel, jelszó: passwd). A felhasználók adatai a /etc/adduser.conf, vagy a /etc/default/useradd alapján állítódnak be. A home könyvtárunkba bemásolódik a /etc/skel könyvtár tartalma.

A USERS\_GID-nél (vagy a GROUP-nál) állíthatjuk be az alapértelmezett csoportot. A DHOME (HOME) beállítás tartalmazza a felhasználó könyvtárának helyét. A DSHELL-nél (SHELL-nél) a felhasználó belépésekor elinduló shell alapértelmezését tudjuk megadni. Amennyiben /bin/false-t (esetleg /bin/nologin) adunk meg, úgy a belépés tiltva van.

#### - init beállítások.

/etc/inid.d könyvtár tartalmazza a futó démonok indító állományait. Az állományokat start, stop, restart, status paraméterekkel lehet meghívni. Nézzünk meg hogy történik ez a web-szerver esetében.

```
Indítás: /etc/init.d/httpd start
Leállítás: /etc/init.d/httpd stop
Újraindítás: /etc/init.d/httpd restart
Állapot lekérdezése: /etc/init.d/httpd status
```

A rendszer indításakor is ezekkel a fájlokkal indulnak a szükséges démonok. Alapértelmezett indulási folyamat az init3. A /etc/rc3.d könyvtárban található meg azon scriptek linkjeit, melyek elindulnak bekapcsoláskor.

#### - /etc/sysconfig könyvtár (REDHAT)

Itt találhatóak a rendszer indulásához szükséges paraméterek, környezeti változók beállításai. Kevés kivétel híján, ritkán van szükség az itt található állományok szerkesztésére. Telepítés közben megadott adatokból nagyon sokat megtalálunk itt. Nézzünk egy-két példát:

```
keyboard. Megadja a billentyűzet típusát és nyelvét.
network. A számítógép host-nevét található meg benne.
ipchains. 2.2-es sorozatú kernel csomagszűrőjének beállítása.
iptables. 2.4-es sorozatú kernel csomagszűrőjének beállítása.
network-scripts/ifcfg-eth0. Első hálózati kártya adatai.
```

#### - szerver kiszolgálók beállító fájljainak helye:

```
Sendmail : /etc/mail/*, /etc/sendmail.cf, (/etc/sendmail.cw)
Apache : /etc/httpd/conf/*
```

```
SNMP : /etc/snmp/snmpd.conf
Squid : /etc/squid/*
Ssh : /etc/ssh/*
Xinetd : /etc/xinetd/*
Samba : /etc/samba/*
```

## 3.2 Hasznos parancsok

Rögtön indulásnál érdemes megismerni néhány jól használható parancsot. Az első feladatunk, feltérképezni a számítógépünk hálózatát.

### - ping

A ping parancs egy 'echo' ICMP üzenetet küld a célszámítógépnek, amelyre az válaszol. A válasz visszaérkezéséből kiderül, hogy a kapcsolat életben van-e. További információk lehetnek a csomagvesztés, amelyből a kapcsolat minősége és terheltsége és a válaszidő, amelyből a vonal sávszélessége és terheltsége következik. Adjuk ki a ping parancsot, melynek a paramétere a legközelebb lévő átjáró IP címe legyen:

```
server:~# ping 192.168.1.1

PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=1.4 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.1 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.1 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.1 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.1 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.1/1.4 ms
```

A parancs működését leállítani a CTRL-C-vel lehet. Az eredményből láthatjuk, hogy az elküldött csomagok sorban érkeztek vissza (icmp\_seq=1..). Az alsó összesítésből megállapíthatjuk, hogy 5 kiküldött csomagból 5 visszaérkezett, csomagvesztés nem volt (0% packet loss). A válaszidő pedig 1,1 ms és 1,4 ms között volt, a válaszidő átlaga 1,1 ms (alsó sor).

A parancs paramétereinek adhatjuk a saját IP-címünket is. Ha nem érkezik válasz, akkor nálunk van beállítási gond. Amennyiben paraméternek a legközelebb lévő gép IP címét adjuk és nem válaszol, továbbá a saját IP címünkre válaszolt, akkor kábelszakadás (esetleg a hálózati kártya csatlakozója) lehet. Ilyenkor a hálózat fizikai közegét érdemes ellenőrizni.

Érdemes kipróbálni a `-f` opciót (árasztás) helyi hálózaton, miközben a célgépen figyeljük a csomagmozgást.

### - traceroute

Ezzel a paranccsal azt tudjuk megnézni, hogy egy tőlünk távolabb lévő gép és mi közöttünk hány routeren keresztül megy a csomag. Paraméterként adjuk meg a célgép IP címét.

```
server:~# traceroute 195.199.0.133

traceroute to 195.199.0.133 (195.199.0.133), 30 hops max, 38 byte packets
 1 192.168.1.1 (192.168.1.1)  1.360 ms  1.033 ms  0.976 ms
 2 lol.uac0-gyor-nrp3.matav.net (145.236.238.123)  20.560 ms  22.243 ms  25.219 ms
 3 pcl-82.core0-ip4.matav.net (145.236.245.130)  26.285 ms  25.728 ms  25.115 ms
 4 bix.elender.hu (193.188.137.51)  29.884 ms  41.867 ms  46.293 ms
 5 core2.sulinet.hu (212.108.254.10)  44.963 ms  41.887 ms  45.419 ms
 6 195.199.0.58 (195.199.0.58)  33.492 ms  28.910 ms  31.977 ms
 7 szfv.sulinet.hu (195.199.0.133)  31.620 ms  33.124 ms  32.549 ms
```

Szépen sorban láthatjuk a routerek felénk eső oldalának nevét, IP címét, illetve a csomag mozgásának idejét. Amennyiben egy ponton a program csillagozni kezd és egy idő után megáll, láthatjuk, hogy ott szakadt meg a kapcsolat. Amennyiben az Internet kapcsolatunkkal baj van, érdemes megnézni ezt a parancsot, kiderülhet, hogy nálunk van a baj, vagy máshol.

## - ifconfig

Ezzel a paranccsal tudjuk beállítani a hálózati kártyánk IP adatait, illetve lekérdezni azokat. Nézzünk meg egy lekérdezést, paraméternek írjuk be a hálózati interfész nevét:

```
server:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:40:F6:CC:D8:C8
          inet addr:192.168.1.115  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:62084 errors:0 dropped:0 overruns:0 frame:7
          TX packets:57723 errors:0 dropped:0 overruns:0 carrier:0
          collisions:14 txqueuelen:100
          RX bytes:42010449 (40.0 MiB)  TX bytes:21782338 (20.7 MiB)
          Interrupt:12 Base address:0xe800
```

Máris egy halom információval okosabbak lettünk. Látjuk, hogy az eth0-s interfészünk 192.168.1.115 IP címmel rendelkezik, leolvashatjuk a broadcast címet és a hálózati maszkot. Érdekes információ még a kimenő és bejövő csomagok (RX, TX packets) száma és a hibák értéke.

Ezzel a paranccsal tudunk a hálózati kártyánknak IP adatokat adni, ennek a formátuma a következő képen néz ki:

```
ifconfig eth0 192.168.1.115 network 255.255.255.0 broadcast 192.168.1.255
```

## - route

Az rouet tábla lekérdezésére és beállítására szolgál. Érdekes `-n` paraméterrel meghívni, ugyanis ebben az esetben nem ellenőrzi a következő roter-el a kapcsolatot.

```
server:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
192.168.1.0      0.0.0.0         255.255.255.0  U        0      0      0 eth0
0.0.0.0          192.168.1.1    0.0.0.0        UG       0      0      0 eth0
```

Az adatokból megállapítható, hogy az eth0 kártya felé a 192.168.1.0/24 hálózat található. Nem erre a hálózatra címzett csomagokat a (0.0.0.0) az alapértelmezett átjárónak (Gateway: 192.168.1.1) adja tovább.

#### - arp

Azonos fizikai hálózaton lévő gépekkel a hálózati réteg (ARPA rétegek) az ethernet kártya fizikai címe (MAC Address) alapján tartja a kapcsolatot. A MAC address és a IP cím kapcsolatát egy táblázatban tárolja a rendszer, ezt hívjuk arp táblának. Kártya vagy IP cseré esetén adódhatnak problémák. Az arp paranccsal tudjuk listázni és állítani az arp táblát.

```
server:~# arp
Address                HWtype  HWaddress          Flags Mask          Iface
192.168.1.1            ether   00:40:95:A1:0C:8C  C                   eth0
192.168.1.88          ether   00:60:97:95:19:E6  C                   eth0
192.168.1.112         ether   00:E0:29:46:2B:68  C                   eth0
```

#### - iptraf

Hálózati csomagfigyelő program. Több szempontból lehet figyelni a hálózat forgalmát. Menüszerkezetes, kezelése egyszerű.

#### - ps

Futó programok listája. Az `-ax` paramétert használva az összes futó processzról tájékoztatást kapunk. A listában az első oszlopban van a processz sorszáma (PID).

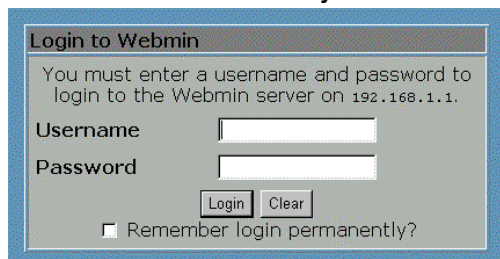
### 3.3 Webmin beállítása

A SUSE LINUX 8.2 Professional-ban a webmin csomag gyári hibás. A javított csomag elérhető az update-k között. Tehát ha a teljes csomagfrissítést választjuk, akkor a hiba megoldódik.

A javított csomag ftp-n is elérhető. Címe:

`ftp://ftp.suselinux.hu/update-8.2/rpm/noarch/webmin-1.070-44.noarch.rpm`

Nyissunk egy másik gépen egy böngészőprogramot és hívjuk meg a webadmin felületet a telepítésnél kiírt címmel. (`http://192.168.1.1:10000/`) A belépési képernyőn azonosítsuk magunkat a root felhasználóval és jelszóval.



Login to Webmin

You must enter a username and password to login to the Webmin server on 192.168.1.1.

Username

Password

Remember login permanently?

A felső részen találhatóak a beállítási csoportok. Választhatunk belőle, milyen jellegű beállításokat szeretnénk eszközölni.

- Webmin. Webmin rendszerrel kapcsolatos beállítások
- System. Rendszerrel kapcsolatos beállítások. Mint például az indulási és leállási folyamatok, meghajtók beállítása, felhasználók és csoportok kezelése.
- Server. Szerver szolgáltatások beállítása. Web, DHCP, DNS, stb.
- Hardware. A gép hardver elemeivel kapcsolatos beállítások. RAID, cd-író, nyomtató, hálózat. Itt kaptak helyet a boot loader-ek is.
- Cluster. Több gép összekapcsolása cluster-ben.
- Other. Egyéb, munkánkat segítő lehetőségek.

Mielőtt a munkánkat elkezdjük, be kell állítanunk a webminünket, hogy némileg fokozzuk a biztonságát. Ezt a webmin részben tehetjük meg.

Lépjünk be a webmin users oldalra és vegyünk fel egy új felhasználót (Create a new Webmin user). Írjuk be a felhasználó nevét (Username) és a jelszavát (Password). A felhasználó ne szerepeljen a normál linux felhasználók között. A jelszó beállításánál a 'set to' opciót használjuk. SSL kulcsot egyelőre ne állítsunk be. Nyelvhez (Language) beállíthatjuk a Magyarat.



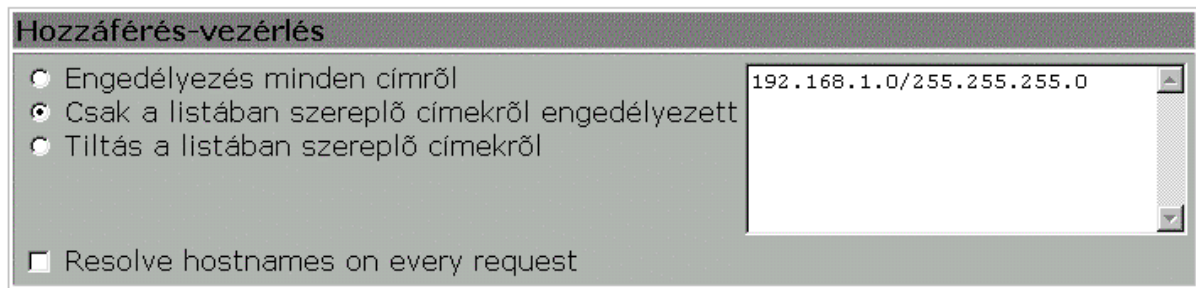
Még lényeges beállítás, az IP cím elérés, ezzel határozzuk meg, hogy a felhasználó honnan tud majd belépni. Az 'IP access control'-t állítsuk be úgy, hogy csak a felsorolt IP címekről engedélyezzük a belépést (Only allow from listed addresses). És soroljuk fel az adminisztrátori gépek címait.

A modules résznél jelöljük be azokat a feladatokat, melyeket adminisztrálni szeretnénk ezzel a felhasználóval. Most akár mindet bejelölhetjük, bár érdemes kiválasztani, azon dolgokat, melyeket ténylegesen állítani fogunk.

Lényeges, hogy ennél a felhasználónál a Webmin beállításai ki legyenek választva. A legfontosabb, hogy a Webmin Users be legyen jelölve. Amikor készen vagyunk, az alsó save gombbal mentjük el a felhasználót.

A jobb felső sarokban lévő Log Out gombbal lépünk ki és jelentkezzünk be az új felhasználónkkal. Láthatjuk, hogy a felület átállított magyarré. Így talán könnyebben tudunk dolgozni.

Még néhány dolgot át kellene állítanunk. Lépünk be a 'Webmin beállítások'-ba. Itt módosíthatjuk a program általános beállításait.



- IP hozzáférés-vezérlés :  
Állítsuk át a 'Csak a listában szereplő címekről engedélyezett' üzemmódra és írjuk be azon IP címeket (192.168.1.0/255.255.255.0), melyekről a felületet el szeretnénk érni. Ezzel is kizárva az illetéktelenek hozzáférését.



- Port és Cím:  
Állítsuk át a webmin elérési portját (mondjuk 13550-ra). Ez azért lehet lényeges, mert ha valaki megvizsgálja a szervert és látja, hogy a 10000-es port nyitva áll, akkor következtethet a webmin jelenlétére.  
Amennyiben több hálózati kártyánk is van a gépben, úgy beállíthatjuk, hogy csak a belső kártya felé szolgáltsa a webmin, így külső hálózatról, Internetről nem lehet majd elérni.  
Ha ezt a beállítást elmentjük, akkor a kapcsolat megszakad. Újra be kell lépünk, de immár a módosított port-al jelentkezünk be: <http://192.168.1.1:13550/>.

Még egy lényeges feladatunk van. Lépünk be ismét a Webmin felhasználók pontba és keressük meg a root felhasználót. A root névre kattintva belépünk a root felhasználó beállításainak módosításába. Az IP cím hozzáférési listánál engedélyezzük a 'Csak a megadott címekről'-t és a felsoroláshoz írjuk be, a 192.168.1.1 (azaz a szervertől). Majd mentés.

A beállítás következtében a root felhasználó csak a szerverről tudja elérni a Webmint. Innentől kezdve az adminisztrátor felhasználóval (melyet nemrég vettünk fel) tudunk csak kívülről belépni.

### 3.4 Gyakorlat

Nézzük át a telepített rendszerünkön, az /etc könyvtárban található fájlok tartalmát! Próbáljuk meg feltérképezni, melyik fájl milyen program, szolgáltatás beállításait tartalmazza! Jegyezzük le, a rendszerünk és a könyvben leírt helyek, fájlnevek eltéréseit! Böngésszük a könyvtárszerkezetet (elsősorban a /var), hogy melyik könyvtár milyen programhoz, szolgáltatáshoz kapcsolódhat!

## 3.5 Ellenőrző kérdések

1. Mi a shell?
2. Mire használhatjuk a Midnight Commandert?
3. Linux-nál melyik könyvtárban találod a beállító fájlokat?
4. Hol vannak a felhasználók könyvtárai?
5. Mi a jellegzetessége a /var könyvtárnak?
6. Mit lehet a /etc/resolv.conf fájlban állítani?
7. Melyik fájlban tároljuk a felhasználók adatait?
8. Melyik fájlban tároljuk a jelszavakat?
9. Melyik fájlban tároljuk a csoportok adatait?
10. Mire és hol használjuk a csomagszűrőt?
11. Mire való a Webmin?
12. Mit kell indulásnál beállítani a Webmin-ben?
13. Mi a virtuális konzol?
14. Mi a tar csomagoló szerepe a mentésnél a jogosultságok függvényében?
15. Mit jelent az inicializáló folyamat (Init3)?
16. Hogyan indítunk egy szerver szolgáltatást (pl.: webszerver)?
17. Mire jó a ping parancs?
18. Mit tudunk beállítani az ifconfig segítségével?
19. Milyen információkat szerezhetünk a paranccsal?

## 3.6 Felhasznált, ajánlott irodalom

Dos-ról, Windows-ról, Linuxra-HOGYAN

[http://linux.vv.hu/hogyanok/hogyan/Dos\\_Win-rol-Linuxra-HOGYAN/DOSWin-rol-Linuxra-HOGYAN.html](http://linux.vv.hu/hogyanok/hogyan/Dos_Win-rol-Linuxra-HOGYAN/DOSWin-rol-Linuxra-HOGYAN.html)

Linux abszolút kezdő-HOGYAN

<http://linux.vv.hu/hogyanok/hogyan/Linux-abszolot-kezdo-HOGYAN/lak.html>

Linux rendszeradminisztrátorok kézikönyve

<http://linux.vv.hu/konyv/adminisztratorok-kezikonyve/sag-hu.html>

Konfiguráció-HOGYAN

<http://linux.vv.hu/hogyanok/hogyan/Konfiguracio-HOGYAN/Config.html>

RPM-HOGYAN

<http://linux.vv.hu/hogyanok/hogyan/RPM-HOGYAN/RPM-hogyan.html>

## 4. SSH (Secure shell)

### 4.1 Alapismertek

Internetre kötött szerverünkön semmiképpen se telepítsünk telnet és ftp szervert. Mivel ezek kódolatlanul küldik adataikat a jelszavaink is így vándorolnak a hálózaton.



A fenti alkalmazások helyett használjunk openssh szervert, amely titkosított kommunikációt biztosít.

A titkosítás lényege, hogy a hálózaton az adatok kódoltan áramoljanak, azaz ne lehessen visszafejteni és ne lehessen hamisítani a kommunikációt. Ehhez az információt a feladó egy kulccsal kódolja és a címzett ennek a kulcsnak a párjával visszakódolja azt.

A kódolásnál kulcs párokat használunk, ezért a fogadó fél a titkos kulcsának a párját (nyilvános kulcs) átküldi a küldő félnek, hogy azt használja kódolásakor. Ennek segítségével szimmetrikus kulcsot cserélnek. A továbbiakban a szimmetrikus kulcsot használják a folyamatos kódoláshoz.

## 4.2 SSH szerver beállítása konzolról

Az SSH szerver beállításait a `/etc/ssh/sshd_config` állományban találjuk. Az alapbeállítások jellemzően jók szoktak lenni, nézzünk ezek közül néhányat:

- Port 22  
Milyen porton figyeljen az SSH szerver. Amennyiben csak mi szoktunk SSH-val belépni adminisztráció végett, érdemes megváltoztatni valami egyénire.
- Protocol 2  
Az SSH v1 és SSH v2 két külön protokoll. Itt azt adjuk meg, hogy melyikkel dolgozzon a szerver. Van lehetőség mindkettőre, akkor protocol 1,2 kerül ebbe a sorba.
- PermitRootLogin yes  
Yes-re állítva tiltja a root felhasználó belépését.
- PasswordAuthentication yes  
Yes-re állítva engedélyezi a jelszavas autentikációt.
- PermitEmptyPasswords no  
No-ra állítva tiltja az üres jelszóval való belépést.

És amit még érdemes lehet mellé írni:

- ListenAddress 192.168.1.115  
Megadjuk melyik hálózati címet (kártyát) figyelje a szerver. Akkor is érdemes beállítani, ha csak 1 hálózati csatlakozásunk van.
- AllowUsers adminuser  
Csak a feltüntetett felhasználóknak (adminuser) engedélyezi a belépést. Ezt akkor érdemes megadni, ha csak adminisztrációs célból használjuk az ssh-t.

## 4.3 SSH kulcsok generálása

A kulcsok generálása az `ssh-keygen` paranccsal történik. Minden felhasználó létrehozhatja a kulcsát. A program elindítása után várni kell egy kicsit a véletlen szám generálására. Megkérdezi tőlünk, hogy hova mentse le a kulcsot. Választhatjuk az alapértelmezettet, ekkor a felhasználó home könyvtárában lesz a kulcs a `.ssh`

alkönyvtár alatt. A generáló kér egy jelszót, amivel megvédhetjük a kulcsunkat. Nem kötelező kitölteni.

```
# ssh-keygen
```

```
Generating public/private rsa1 key pair.
```

```
Enter file in which to save the key (/home/user/.ssh/identity):
```

```
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
```

```
Your identification has been saved in /home/polip/.ssh/identity.
```

```
Your public key has been saved in /home/polip/.ssh/identity.pub.
```

```
The key fingerprint is:
```

```
.....
```

A program létrehozza a titkos kulcsunkat (identity) és a publikus kulcsot (identity.pub). Ha kulccsal szeretnénk azonosítani magunkat egy szerveren, akkor az identity.pub állomány tartalmát hozzá kell fűzni a szerveren lévő (home könyvtárunk .ssh alkönyvtárába) authorized\_keys állományhoz.

## 4.4 Programok használata

Az SSH szerver egyik elérési módja a terminál üzemmód. Ez a régi telnet parancs mai megfelelője. Egy szerverre történő belépés a következőképpen történik:

```
# ssh server.iskola.hu
```

Ha nem azzal a felhasználóval szeretnénk belépni, amelyikkel a kiinduló rendszeren bent vagyunk, akkor használjuk a -l opciót.

```
# ssh -l felhasználonev server.iskola.hu
```

A másolás az scp paranccsal történik. Nézzünk meg egy-két lehetőséget:

```
# scp felhasználó@server.iskola.hu:/home/felh/letoltom.zip  
/home/felh/ebbeakonyvtarba
```

```
# scp /home/felh/feltoltom.zip server.iskola.hu:/home/felh
```

SSH szervert Windows rendszerről kényelmesen a putty és a winscp2 programokkal érhetünk el, melyeket az Internetről ingyenesen letölthetünk.

## 4.5 Gyakorlat

Állítsuk be az SSH szervert, hogy csak egy felhasználó (lehetőleg mi magunk) tudjon bejelentkezni. Próbáljuk ki az ssh és az scp használatát.

## 4.6 Ellenőrző kérdések

1. Mi az ssh?
2. Írd le a kulcspáros kódolás folyamatát!
3. Melyik programmal generálhatunk kulcsot?
4. ssh-val szeretnél a www.iskola.hu gépre jelentkezni admin felhasználóként, írd le a pontos parancsot!
5. Milyen parancsot használhatunk ssh szervernél kódolt fájlmozgatásra?

## 4.7 Felhasznált, ajánlott irodalom

SSH és SSH port forwarding használata  
<http://www.szabilinux.hu/security/ssh/ssh.html>

SSH villam HOGYAN  
<http://linux.vv.hu/hogyanok/villam/SSH-villam-HOGYAN/sshlightning.html>

SSH - a biztonságos alternatíva az RSH helyett  
<http://linux.vv.hu/egyebek/halozat/biztonsag/ssh/ssh.html>

## 5. Felhasználók, jogosultságok kezelése

### 5.1 Alapismertek

A többfelhasználós (multiuser) rendszerekre jellemzően, a Linux, tökéletesen alkalmas a felhasználók kezelésére. A felhasználók a meglévő, beállított jogosultságokkal futtathatják programjaikat és használhatják a szolgáltatásokat.

A mi szempontunkból viszont érdemes a felhasználók kezelését máshogy is megközelíteni. Egy szerver használatánál, manapság már, nem jellemző, hogy az átlag felhasználó terminálszerver üzemmódban dolgozik a gépen, vagy parancssorból programokat futtat. Sokkal inkább egyéb szolgáltatásokat használ kliens-szerver üzemmódban, meghatározott alkalmazás szintű protokollokkal (pop3, smtp, http).

Ezért a gépen lévő felhasználókat az alábbi csoportokra oszthatjuk:

- **Rendszerfelhasználók.** Nem személyhez kötött felhasználók. Egy-egy programhoz, szolgáltatáshoz kapcsolhatók. Azért fontosak, hogy a folyamatosan futó programoknál meg tudjuk határozni a jogosultságait. Például az apache szerver (web) általában apache felhasználó jogosultságaival éri el a fájlrendszert.
- **Adminisztrátori felhasználók.** Ez gyakorlatilag a root és bizonyos jogosultságokkal felruházott (sudo) adminisztrátori felhasználók. A karbantartásért és az üzemeltetésért felelős személyek használják.
- **Normál felhasználók.** Ezek azok a személyek, akik a szerver szolgáltatásait használják. Mivel manapság ritka, hogy terminál üzemmódban belépnek a

szerverre és ott futtatják kliensprogramjaikat, ezért van amikor az ilyen felhasználókat leválasztják a rendszerről és külön tárolják egy-egy szolgáltató program részére. Például a levelező szerver (exim) felhasználóit adatbázisban tároljuk, így a Linux részére nem léteznek, csak az MTA látja őket.

A felhasználók és az adataik a `/etc/passwd` fájlban találhatóak. Ezek a következők lehetnek:

Felhasználó sorszáma (user id)  
Felhasználó belépési neve (user name)  
Felhasználó teljes neve (real name)  
Felhasználó egyéb adatai  
Felhasználó SHELL-je  
Felhasználó HOME könyvtára  
Felhasználó elsődleges csoportja

Minden felhasználó rendelkezik egy elsődleges csoporttal, sok rendszeren ez a felhasználó felvételekor automatikusan keletkező, felhasználó nevével megegyező csoport. Ez alapján minden felhasználónak saját elsődleges csoportja van és ebbe a csoportba csak ő tartozik. Ennek a jogosultságok kiadásánál lehet jelentősége.

Más csoportokhoz is hozzá lehet rendelni a felhasználót. A hozzárendeléssel keletkezett csoporttagságot másodlagos csoportnak nevezzük. A csoportok adatait és a másodlagos csoport hozzárendeléseket a `/etc/group` fájlban tároljuk. A tárolt adatok a következők:

Csoport Sorszáma (group id), csoport neve, hozzárendelt felhasználók (user name) felsorolva

A fentiek alapján kialakul egy csoport-felhasználó szerkezet. Régebben a jelszó a `/etc/passwd` állományban tárolódott, de ehhez minden olyan programnak hozzá kell férnie, amely felhasználókkal működik (pl. MTA programok). Ez sérülékenységet okozott a rendszerben ezért a jelszavakat védettebb árnyék fájlba helyezték el. Ez a fájl a `/etc/shadow`. Természetesen itt is kódolva találhatóak a jelszavak.

A felhasználók és a csoportok kezelésére szolgáló parancsok:

- `useradd` Felhasználó létrehozása.
- `usermod` Felhasználó módosítása.
- `userdel` Felhasználó törlése.
- `users` Bejelentkezett felhasználók listája.
- `who` Bejelentkezett felhasználók listája.
- `whoami` Milyen felhasználó névvel vagyok bent.
- `groupadd` Csoport létrehozása.
- `groupmod` Csoport törlése.
- `groupdel` Csoport törlése.
- `passwd` Jelszó változtatása.

A jogosultságok kezelése a fájlrendszerben van meghatározva. Azt adjuk meg, hogy egy könyvtárhoz, fájlhoz kinek van joga. Minden bejegyzésnek (könyvtár, fájl, egyéb)

van egy tulajdonosa és egy csoportja. Ez alapján annak eldöntésére, hogy a felhasználó mit tehet a bejegyzéssel, először el kell dönteni, hogy milyen státusza van. Amennyiben az adott felhasználó a bejegyzés tulajdonosa (owner), úgy a tulajdonosnak beállított jogait veszi át. Amennyiben a tulajdonos csoportnak (group) a tagja, úgy a csoportjogokat. Ha nem a tulajdonosa és nem tagja a tulajdonos csoportnak, akkor az egyéb felhasználó (others) jogosultságaival kezelheti a bejegyzést.

Mindhárom státuszhoz (owner, group, other) három féle jogosultság kapcsolható. Ezek az írási (write), az olvasási (read) és a futtatási (execute) jog. A futtatási jog a könyvtárak esetén a megnyitási, tartalomlistázási jognak felel meg.

set user ID	on	4000	tulajdonos jogaival futtatható
set group ID	on	2000	csoport jogaival futtatható
Sticky bit		1000	'ragadós' bit, tulajdonos öröklődése
read by owner		0400	tulajdonos olvashatja
write by owner		0200	tulajdonos írhatja
Execute/search	by	0100	tulajdonos futtathatja
read by group		0040	csoport olvashatja
write by group		0020	csoport írhatja
Execute/search	by	0010	csoport futtathatja
read by others		0004	bárki olvashatja
write by others		0002	bárki írhatja
Execute/search	by	0001	bárki futtathatja

A fenti táblázatban látható egy fájlrendszer bejegyzés attribútum listája. Az előzőekben említett jogosultságokon kívül még három érdekes attribútumot találhatunk. Ezek tárgyalásához tudnunk kell, hogy alapesetben egy program mindig annak a felhasználónak a jogosultságaival fut, aki azt elindította. Természetesen vannak olyan programok, ahol ez nem vezetne eredményre. Például a passwd (jelszóváltoztatás), hiszen a felhasználónak, aki elindítja, nem lehet joga a jelszavakat tároló fájlhoz, de ezt a programnak módosítani kell.

- **set user ID on execution (SUID)**. Amennyiben ez a bit aktív, beállított, úgy a program futása közben nem az őt indító felhasználó, hanem a tulajdonos (owner) jogait öröklí.
- **set group ID on execution (SGID)**. Amennyiben ez a bit aktív, beállított, úgy a program futása közben nem az őt indító felhasználó, hanem a tulajdonos csoport (group) jogait öröklí. Amennyiben könyvtárra helyezük, úgy a könyvtárba helyezett fájlok nem a létrehozó felhasználó elsődleges csoportjával, hanem a könyvtár csoportjával jön létre.
- **sticky bit**. (Ragadós bit) Fájlknál azt jelenti, hogy az elindított program memóriában marad, ezzel gyorsabbá téve a következő használatát, hiszen nem kell újratölteni. A könyvtáraknál mindenki számára írható/olvasható (számítanak az alapjogosultságok), de mindenkinek csak a saját tulajdonú fájlhoz vannak jogai.

A tulajdonos és a jogosultságok kezelésére használhatjuk a következő parancsokat:

- `chown` Bejegyzés tulajdonosának megváltoztatása

- chgrp Bejegyzés csoportjának megváltoztatása
- chmod Bejegyzés jogosultságainak megváltoztatása

## 5.2 Felhasználó kezelése konzolról

Felhasználók felvételét az useradd paranccsal végezzük. A 'useradd smoky' parancs hatására a következők történnek:

- /etc/passwd és a /etc/shadow fájlba felveszi a smoky nevű felhasználót a /etc/default/useradd fájlban leírt alaptulajdonságokkal.
- Létrehozza a felhasználó home könyvtárát.
- A home könyvtárba belehelyezi a /etc/skel könyvtárban található fájlkat.
- A home könyvtár és a benne található fájlok tulajdonosának a smoky felhasználót állítja be.
- /etc/group és a /etc/gshadow fájlban létrehoz egy új csoportot smoky néven, amely az új felhasználónk elsődleges csoportja lesz.

Természetesen a useradd parancs tökéletesen paraméterezhető. A fenti folyamat minden elemét megadhatjuk számára. A

```
useradd -d /home/users/valaki -s /bin/bash -u 1000 -e 2002-12-30 -g felh -G tanar valaki
```

parancs a felveszi a 'valaki' nevű felhasználót. A felhasználó home könyvtára (-d) /home/users/valaki, a shell-je (-s) /bin/bash, a user id-je (-u) 1000 lesz. Ez az account 2002 december 30-án lejár. Alapértelmezett csoportja a 'felh' lesz, de tagja lesz a 'tanar' csoportnak is.

A felhasználó adatainak módosítására a 'usermod' paranccsal van lehetőségünk. Paraméterezése megegyezik a 'useradd' parancsával.

```
usermod -c 'Nagy Felhasznalo' valaki
```

A fenti paranccsal a felhasználó teljes nevét (comment mezőjét) változtatjuk meg.

A felhasználót a 'userdel' paranccsal törölhetjük. Csak egy paramétere van, a -r, ha ez szerepel benne, akkor a felhasználó home könyvtárát is törli, egyébként nem.

```
userdel -r valaki
```

Egyéb felhasználói adatokat megváltoztató parancsok:

```
'passwd valaki' valaki felhasználó jelszavának megváltoztatása.
```

```
chfn -f 'Teljes Nev' valaki valaki felhasználó teljes nevének megváltoztatása.
```

```
chsh -s /bin/bash valaki valaki felhasználó shell-jének beállítása.
```

A csoportokat a következő parancsokkal kezeljük:

```
groupadd [-g groupid] group  
groupdel group
```

A fentiek alapján hozzunk létre egy új csoportot és helyezük bele a 'valaki' felhasználót:

```
groupadd gazdasagi
usermod -G gazdasagi valaki
```

### 5.3 Jogosultságok beállítása konzolról

Mint már említettük, a jogosultságokat a fájlrendszer bejegyzéseihez adjuk meg. Amennyiben szeretnénk megtekinteni egy bejegyzés jogosultságait, ezt megtehetjük így:

```
ls -axl
```

Ez a parancs az aktuális könyvtár bejegyzéseit listázza ki a jogosultságokkal együtt. A jogosultságokat (azaz a bejegyzés attribútumait) 10 karakterrel a sor elején jelzi. Az első karakter a bejegyzés típusát mutatja meg, ezek lehetnek:

'-'	normál fájl
'b'	blokkos eszköz
'c'	karakteres eszköz
'd'	könyvtár
'l'	szimbolikus link
'p'	pipe
's'	socket

Utána három karakterben a tulajdonos jogait, majd szintén három karakterben a csoport jogait láthatjuk. Az utolsó három karakter a minden más felhasználó jogait mutatja. Ezek lehetnek:

'r'	olvasási engedély
'w'	írási engedély
'x'	futtatási engedély
's'	SUID, vagy SGID engedély
't'	Sticky bit

A jogosultságok megváltoztatását a `chmod` paranccsal végezhetjük. A paraméterekben először meg kell határozni, hogy kinek a jogosultságait módosítjuk. Ha a tulajdonosét, akkor 'u'-t használunk. Ha a csoportét, akkor 'g'-t használunk. Ha mindenki másét, akkor 'o'-t használunk. Van lehetőség mindhárom jogviszony egyszerre történő módosítására is az 'a' használatával. Utána meg kell adnunk, hogy levesszük '-' vagy felrakjuk '+' a jogosultságot, majd a jogosultság következik (r, w, x).

Példák a beállításokra:

- chmod u+x filename	A tulajdonosnak futtatási jogot ad.
- chmod g-w filename	A csoport írási jogát elveszi.

- `chmod a+r filename` Mindhárom jogviszony (tulajdonos, csoport, mindenki más) olvasási jogot kap.

Van lehetőség, hogy pontosan meghatározzuk egy jogviszony jogosultságait:

- `chmod o=rx filename` A minden más felhasználónak olvasási és futtatási joga lesz, írási nem.

A jogosultságokat számértékként is meg lehet adni, illetve értelmezni. Ehhez egy 3 karakteres numerikus értéket használunk. Az első karakter a tulajdonos, a második a csoport, a harmadik a mindenki más jogosultságait tartalmazza. A karakterpozíciókban lévő számértékek a következők lehetnek:

- 0 nincs jogosultság
- 1 futtatási jog
- 2 írási jog
- 4 olvasási jog

Ezek összegzéséből kialakuló értékek:

- 3 futtatási és írási jog
- 5 futtatási és olvasási jog
- 6 írási és olvasási jog
- 7 futtatási, írási és olvasási jog

Ezek alapján ha egy bejegyzésnél az mondjuk, hogy 640 akkor a tulajdonosnak (6) írási és olvasási joga van, a csoportnak (4) olvasási joga van, a többi felhasználónak (0) nincs joga. Ezt az értéket a `chmod` parancsban is használhatjuk:

- `chmod 740 filename`

Az `'ls -axl'` listában láthatjuk a tulajdonos és a csoport felhasználó nevét is a bejegyzések mellett. Természetesen ezeket is megváltoztathatjuk. A bejegyzés tulajdonosát a `chown` paranccsal, a csoportját pedig a `chgrp` paranccsal módosíthatjuk:

- `chown <felhasznalo> <bejegyzés>`
- `chown root filename`
- `chown kispista /home/kispista`
- `chgrp <csoport> <bejegyzés>`
- `chgrp users /home/kozos`
- `chgrp tanarok /home/kozos/readme`

## 5.4 Felhasználói quota

A quota-val meghatározhatjuk, hogy egy felhasználó, vagy egy csoport az egyes partíciókon mekkora lemezterületet használhat. A `/etc/fstab` állományban meg kell adnunk, mely partíciókon szeretnénk a korlátozást használni. A partíciók csatolási



paramétereikhez kell beírni a `usrquota` (csoport korlátozás esetén: `grpquota`) paramétert. Ez a `/home` partíció esetén a következőképpen néz ki:

```
/dev/hda5 /home ext3 defaults, nosuid, noexec, nodev, usrquota, grpquota
1 2
```

Ha készen vagyunk a `/etc/fstab` átírásával, akkor `mount`-oljuk újra fel a partíciót, vagy egyszerűen indítsuk újra a gépet, hogy aktivizáljuk a beállítást.

Most indítsuk el a `quotacheck` programot. Ez leellenőrzi a partíciót, amelyre a quotát tettük és létrehozza a `quota.user`, `qouta.group` állományokat:

```
quotacheck -a -vug
```

Az előbeállításokkal már készen is vagyunk. Most jönnek a felhasználók és a csoportok korlátozásainak megadása. Mielőtt belekezdünk keresünk egy 'vi' doksit, ugyanis ezzel a szövegszerkesztővel kell a beállításokat módosítani. Addig is egy-két szükséges parancs:

A `vi` indulásnál nincs szerkesztési üzemmódban. Az 'a' billentyűvel lehet rábírni, hogy átírassuk a sort.

Nyomjuk meg az 'esc' billentyűt, majd ':q'. Ha az alsó sorba kiírja a `:q-t`, akkor jók vagyunk. Ez a kilépés parancs, ha módosítottunk, akkor nem működik.

Esc :q! Kilépés mentés nélkül.

Esc :wMentés

Felhasználók beállítása:

```
edquota <felhasználónév>
```

```
edquota kriszti
```

Erre valami ilyesmi fog bejönni:

Disk quotas for user kriszti (uid 501):

Filesystem	Blocks	soft	hard	inodes	soft	Hard
/dev/hda3	20	0	0	5	0	0

~

A filesystem a partíciót mutatja. Két értéket lehet korlátozni. A felhasználó állományainak partíción elfoglalt helyét block-okban (1 block=1024 Byte) és az inodok korlátozását. Két féle korlátot állíthatunk be. A hard korlát a maximálisan elfoglalt területet jelenti, ha ezt túllépi a felhasználó, akkor egy 'partíció megtelt' üzenetet kap. A soft korlát ideiglenesen meghaladható, de bizonyos időn belül (grace) törlődik a felette lévő rész. A nulla (0) érték beállítása esetén a korlátozás kikapcsolódik.

Most állítsunk be a felhasználónak 1200 Kbyte hard korlátot és 1000 Kbyte soft korlátot. A inodes korlátozás legyen hard:120, soft:100.

Disk quotas for user kriszti (uid 501):

Filesystem	blocks	soft	Hard	inodes	soft	Hard
/dev/hda3	20	1000	1200	5	100	120

~

Mentsük el a beállítást. Hasonlóan működik a csoportok esetén is a beállítás. Az `edquota -g <csoporthív>` paranccsal tudjuk állítani. A csoportkorlát esetén a csoport tagjai együttesen nem léphetik túl a megadott értéket. Például:

```
edquota -g tanar
```

Lehetőségünk van a beállítások másolására két felhasználó között. Így beállítunk egy felhasználót és gyorsabban tudjuk ezt klónozni a többire.

```
edquota -p user1 user2
```

A fenti példában a `user1` felhasználó beállításait kapja a `user2` felhasználó.

A `grace` beállítása határozza meg, hogy a `soft` korlát feletti rész mennyi idő múlva legyen törölve. Ez alapban 7 nap. Átállítása szintén az `edquota` paranccsal történik:

```
edquota -t
```

Grace period before enforcing soft limits for users:

Time units may be: days, hours, minutes, or seconds

Filesystem	Block grace period	Inode grace period
/dev/hda3	7days	7days

~

Amennyiben a beállításokkal készen vagyunk már csak el kell indítanunk a `quota-t`.

```
quotaon -a -vug
```

A felhasználó is lekérdezheti beállításait a `'quota'` paranccsal.

## 5.5 Gyakorlat

Vegyük fel a következő felhasználókat:

Kisse Kiss Elemér  
Nagyj Nagy János  
Balan Balla Nárcisz

Vegyük fel a következő csoportokat:

tanar  
iskola

Másodlagos csoport hozzárendeléssel alakítsuk ki a következő szerkezetet:

Tanar csoport: kisse, nagyj  
Iskola csoport: kisse, nagyj, balan

Hozzunk létre egy közös könyvtárat a tanar és egyet az iskola csoport részére a /home könyvtárban és állítsuk be a következő jogosultságokat:

/home/tanar  
tulajdonos: kisse (rwx)  
csoport: tanar (rwx)  
egyéb felhasználó: nincs jogosultság

/home/iskola  
tulajdonos: kisse (rwx)  
csoport: iskola (rwx)  
egyéb felhasználó: nincs jogosultság  
sticky bit beállítva.

42. A /home könyvtárra (partícióra) helyezzünk fel felhasználói kvótát a következő értékekkel minden felhasználónál:

Soft quota: 30 Mbyte (inodes: 800)  
Hard quota: 40 Mbyte (inodes: 1000)

## 5.6 Ellenőrző kérdések

1. Milyen adatokat kell megadni egy felhasználó felvételénél?
2. Mit jelent a Secondary Groups (másodlagos csoportok)?
3. Hol használhatjuk a /bin/false-t?
4. Melyik paranccsal tudunk felhasználót felvenni?
5. Mire szolgál az /etc/skel könyvtár tartalma?
6. Mit csinál a 'usermod -c 'Nagy Felhasznalo' valaki' parancs?
7. Hogyan törölünk felhasználót?
8. Mit csinál a 'groupadd tanulo' parancs?
9. Milyen jogosultságokat ismersz fájlok esetén?
10. Írd le a SUID bit lényegét és veszélyeit!
11. Mire való a sticky bit a könyvtáraknál?
12. Milyen paranccsal állítjuk egy fájl tulajdonosát?
13. Írd le számmal (pl: 664) a következő jogosultságokat:
  - a. Tulajdonos – írás, olvasás, futtatás
  - b. Csoport – olvasás, futtatás
  - c. Más felhasználó nem rendelkezik jogokkal
14. Mi a felhasználói quota?
15. Milyen előbeállításokra van szükség a quota beüzemeléséhez?
16. Mire jó az edquota parancs?
17. Mi a soft és hard quota közötti különbség?

## 5.7 Felhasznált, ajánlott irodalom

Process Accounting-Mini HOGYAN

<http://linux.vv.hu/hogyanok/mini/Process-Accounting-Mini-HOGYAN/processz-account.html>

Quota-Mini HOGYAN

<http://linux.vv.hu/hogyanok/mini/Quota-Mini-HOGYAN/quota-hu.html>

Vi-villám HOGYAN

<http://linux.vv.hu/hogyanok/villam/Vi-villam-HOGYAN/vi-villam.html>

## 6. Samba fájl- és nyomtatószerver

### 6.1 Alapismeretek

Andrew Tridgell 1991-ben kezdte meg egy fájlkiszolgáló program fejlesztését. Ebből a programból alakult ki a SAMBA, amely az SMB protokoll segítségével nyomtató és fájlmegosztásokat végez. Ezt a protokollt használják a Windows rendszerek is. A SAMBA tökéletesen alkalmas a Windows hálózatokkal való együttműködésre, tartomány kezelésére.

Az IBM által kifejlesztett NETBIOS egy hálózati funkciók kezelésére alkalmas BIOS kiterjesztésnek indult a '80-as évek elején. Később a licenz a Microsofthoz került, aki felhasználta Windows sorozatának hálózatkezeléséhez. A Linux esetében a NETBIOS és a TCP/IP összekapcsolásáról van szó.

A NETBIOS a gépek azonosítására neveket használ. A nevek feloldása kétféleképpen történhet. Az egyik megoldás szerint a hálózaton, broadcast (speciális üzenet, melyet a hálózaton lévő összes gép feldolgoz) üzenettel megkérdezzük, ki használja ezt és ezt a nevet. A nevet használó számítógép válaszol erre a kérdésre és megkapjuk tőle a IP címét. A másik lehetőség, hogy egy névszervernél (NBNS) kell regisztrálni a névigénylést és a nevek feloldását is tőle kell kérni.

A számítógépek csoportokba vannak rendezve. Ezeket hívjuk munkacsoportoknak, vagy tartománynak. A tartomány annyiban jelent többet, hogy rendelkezik egy tartományvezérlő szerverrel (logon kiszolgáló). A tartományvezérlő kétféle protokollt használ a kliensekkel való kommunikációhoz, mást a Win95-98, és mást az NT felé. Windows NT gépekkel történő kommunikáció a 2.2.4-es Samba-tól felfelé használható. A tartományvezérlőkből létezik elsődleges (PDC), amelyik éppen aktív és másodlagosak (BDC), amelyek átvehetik az elsődleges szerepét, amennyiben megszakad vele a kapcsolat.

A tartományban (munkacsoportban) található gépek a társaik részére fájl és nyomtató erőforrásait kiajánlhatják, ezeket megosztásoknak (shared) mondjuk. A saját megosztását mindenki broadcast üzenetekkel hirdetik. Amennyiben a hálózatunkon található helyi főállító, az átveszi ezt a szerepet és jelentősen

csökkenti a hálózat foglaltságát. Viszont ennek hiányában a hálózaton lévő gépek és a megosztások megjelenítése gondot okozhat.

A Microsoft továbbfejlesztette a névkiszolgáló szerveret, melyet WINS szervernek hív. Ebből is létezik tartalék. A Samba képes elsődleges WINS kiszolgálóként működni, viszont tartalékként nem. Szintén nem képes tartalék tartományvezérlőként és tartalék tallózóként működni.

Egy samba szerver beállítása három lépésre tagolható. Először beállítjuk az általános beállításait (Global), majd a megosztásokat, végül pedig a felhasználók kezeléséről beszélünk.

A globál beállításainál használhatunk megosztott erőforrásokra vonatkozó paramétereket is. Ezek öröklődni fognak a megosztásokra, ahol felülbíráhatjuk őket.

## 6.2 Samba beállítása kézzel

A Samba beállításait tartalmazó smb.conf állomány tartalmazza. Ezt a /etc/samba könyvtárban található. A tartalmát tekintve szakaszokra bontható. Egy-egy különálló szakaszt szögletes zárójelbe írt kifejezés nyit meg. A globális beállításokat a [global] kifejezés nyitja és addig tart, amíg egy új szakasznyitó kifejezéshez, vagy a fájl végéhez nem érünk. Ezután jönnek a megosztás leíró szakaszok. Itt a szögletes zárójelben a megosztás neve található. Speciális ezek közül a [homes] - felhasználók home könyvtárak a felhasználó belépési nevével megosztva és a [printers] - nyomtató megosztások. A beállításoknál használhatunk változókat is. Ezek, a teljesség igénye nélkül, a következők lehetnek:

%h	Samba szerver DNS neve
%L	Samba szerver NetBios neve
%v	Samba verziója
%T	Aktuális dátum és idő
%u	Aktuális felhasználó unix felhasználója
%g	Aktuális felhasználó unix felhasználójának csoportja
%U	Aktuális felhasználó neve
%G	Aktuális felhasználó csoportja
%H	Felhasználó home könyvtára
%a	Kliens oprendszere (Samba, WfWg, WinNT, Win95)
%l	Kliens IP címe
%m	Kliens NetBIOS neve
%M	Kliens DNS neve

Lehetőség van rá, hogy az smb.conf állomány beállításait másik fájlba helyezzük el. Ebben az esetben az smb.conf-ba be kell szúrunk a fájlt a következő sorral:

```
include = /etc/samba/kozosshare.conf
```

Alkalmazhatunk változókat is. A lenti példában a kliens gép nevének megfelelő beállításokat tölthetünk be. Ha a TANARI nevű gépről jelentkeznek be, akkor a kozosshare\_TANARI.conf állomány illesztődik be.

```
include = /etc/samba/kozosshare_%m.conf
```

A Samba szerver, működés közben is, meghatározott időközönként újraolvassa az smb.conf állományt és érvényesíti a változásokat.

### 43. Globális beállítások

Nézzük át a globális beállítások leglényegesebb részeit. A Samba szerverünket nagyon kevés beállítással életre lehet kelteni. A következőket mindenképpen érdemes megadni:

- Munkacsoport neve (workgroup). Ide írjuk be a hálózat munkacsoportjának a nevet. Tartomány esetén még lényegesebb ez a beállítás, ekkor a tartomány nevét jelzi.  
Például: workgroup = ISKOLA
- A szerver neve a hálózatban, azaz a netbios név (netbios name).  
Például: netbios name = SERVER
- Van lehetőség leíró szöveget is hozzárendelni. Ez a windows keresőben zárójelben jelenik meg, csak információ értékű.  
Például: server string = %h server (Samba %v)
- Elérkeztünk a Samba leglényegesebb beállításához (security). Négy beállítási lehetőségünk van, amely meghatározza a szerver alapvető működését. Gyakorlatilag az autentikáció beállításáról van szó.
  - SHARE. A régi WfW megoldásra jellemző autentikáció. Felhasználó ellenőrzés nincs. A megosztásra tehetünk jelszó ellenőrzést. Tehát a jelszó nem a felhasználóhoz, hanem a megosztáshoz kapcsolódik. A valid user opció (később szó lesz róla) itt is érvényesül, viszont a felhasználót nem veszi figyelembe. Elég ha a jelszó egyezik bármelyik engedélyezett felhasználó jelszavával.
  - USER. A kliens a csatlakozásnál elküld egy felhasználónevet és egy jelszót. Amennyiben ezek megfelelnek, a kapcsolat létrejött. A kliens kap egy azonosítót, amellyel később igénybe veheti a megosztásokat. Egy kliens többszöri azonosítást is végezhet (más más felhasználói adatokkal).
  - SERVER. Ennél a lehetőségnél a 'password server' paraméternél meg kell adni a PDC nevét. Amennyiben azonosítási kapcsolat érkezik a Samba szerverhez, akkor ezt elküldi a Password szervernek. Ha elfogadja, akkor a Samba is engedélyezi a kapcsolatot.
  - DOMAIN. Szintén meg kell adni a 'password server'-t. Hasonlóan eredménye van, mint a SERVER beállításnak. Viszont rengeteg előnnyel jár. Ebben az esetben a Samba lényegesen jobban integrálódik a tartományba. A tartományvezérlő nem csak a felhasználó érvényességét adja vissza, hanem az adatait is. Ezen kívül ki tudjuk használni a Microsoft tartományvezérlő lényeges szolgáltatásait.

Önálló Samba szerver esetében a USER beállítása az általános.

Például: security = user

- Az Samba képes WINS szerverként is működni. Ez a NBNS továbbfejlesztett változata, jó ha ezt a szerepet egy állandóan bekapcsolat szerver veszi át. Tehát lehetőleg kapcsoljuk be a 'wins support = true' bejegyzéssel. Amennyiben már van WINS szerver a hálózaton, úgy adjuk meg azt a ' wins server = winsservername' bejegyzéssel.
- Van rá lehetőség, hogy a Samba főtallózóként működjön, ehhez adjuk meg az 'os level' szintet. Ez még nem jelenti azt, hogy a Samba lesz a főtallózó, ugyanis ez a Windows hálózatonál szavazással dől el. A szavazásnál az nyer, akinek a prioritási értéke (protokoll verziójából, op.rendszer verziójából, bekapcsolási időből és a gazdanévből számított) magasabb. A Samba erre egy kitűnő megoldást használ, megadjuk kézzel, a számításból az operációs rendszer értéke lesz a 'os level' értéke. A 70-es érték már elég esélyes ☺. 90-nél nagyobbat viszont ne adjunk meg.  
Például: os level = 80
- Ha NT, vagy 2000-es klienseket használunk, akkor be kell kapcsolnunk a jelszó kódolását (encrypt passwords = yes). Ha egyszer yes-re állítjuk, akkor már ne nagyon módosítsuk, mert problémák lehetnek a jelszavakat tároló állomány értelmezésével, ugyanis ott kódolva lesznek a jelszavak.
- Amennyiben egynél több hálózati kártya van a számítógépben, a Samba az első hálózati kártyára engedélyezi csak a szolgáltatását. Ha nem szeretnénk, hogy sajátos érvei alapján döntse el, melyikre, akkor adjuk meg az értékeket az 'interfaces' beállításnál.  
Például: interfaces = 192.168.1.115/255.255.255.0
- Szükség lehet rá, hogy a windows hálózaton módosított jelszót a rendszer módosítsa unix szintes is, ehhez meg kell adni a passwd parancs elérését és a párbeszéd formáját. Például:  
update encrypted = Yes  
unix password sync = Yes  
pam password change = Yes  
passwd program = /usr/bin/passwd %u  
passwd chat = \*Enter\snew\sUNIX\spassword:\* %n\n  
\*Retype\snew\sUNIX\spassword:\* %n\n
- Esetleg szeretnénk letiltani felhasználókat, főleg a root felhasználót, ezt a következő sorral tudjuk megtenni:  
invalid users = root
- A windows rendszerek és a Linux rendszerek között erős kódolási és szabványi különbség lehet a fájlnevekben. Ha szeretnénk, hogy ez ne okozzon problémát, akkor kellenek a következő beállítások is:  
client code page = 852  
character set = ISO8859-2

A fentiek talán a leglényegesebb beállítások, de nézzünk még lehetőségeket példán keresztül:

[global]

# A fájlnevekben található ékezetes betűk kezelésére a kódlapot be kell állítanunk:

client code page = 852

character set = ISO8859-2

# Munkacsoport neve:

workgroup = ISKOLA

```
# Szerver információs szöveg:
server string = Iskolai Szerver
# Kapcsolatok kezdeményezését a következő hálózatokra engedélyezzük:
interfaces = 192.168.1.1/255.255.255.0 192.168.2.1/255.255.255.0
# Kódolt jelszó használata:
encrypt passwords = Yes
# Engedélyezzük a Microsoft formátumú jelszófájl frissítését:
update encrypted = Yes
# Amennyiben a felhasználó változtatja a Windows jelszavát, akkor ez frissíti
# A unix jelszót is: (a jelszómódosítás egyéb beállításával).
pam password change = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password*
%n\n
*passwd:*all*authentication*tokens*updated*successfully*
unix password sync = Yes
# Log állomány helyének és méretének beállítása:
log file = /var/log/samba/log.%m%U
max log size = 50
# A névfeloldás sorrendjét állítjuk be:
name resolve order = wins lmhosts bcast
# Belépési profájlok helye és neve:
logon script = %U.bat
logon path = \\%L\Profiles\%U
# Windows hálózaton betöltött feladatok (logon szerver, tartományvezérlő, WINS
szerver,
# főtallózó):
domain logons = Yes
preferred master = True
domain master = True
os level = 88
wins proxy = Yes
wins support = Yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
# Megosztások alapbeállításai (engedélyezett hostok, vendégfelhasználó unix neve,
# DOS flagek mentése
hosts allow = 192.168. 127.
guest account = guest
map system = Yes
map hidden = Yes
```

A fenti egy hosszabb beállítás, ahol a Samba szerverünk egyedül dolgozik a hálózaton. Azért nézzünk meg, még mi az, amivel bővíthetjük:

```
# Authentikáció kezelés (ezt azért hagytuk ki, mert a user alapértelmezett beállítás)
security = user
# Felhasználó térkép:
username map = /var/spool/samba/user.map
# Nyomtató alapértelmezés:
printing = LPRNG
```



```
load printers = yes
printcap name = /etc/printcap
```

```
# Fájlnév kezelési opciók:
preserve case = yes
short preserve case = yes
case sensitive = no
```

#### 44. Megosztások

A különböző típusú megosztásokra nézzünk egy-egy példát:

```
# Hagyományos home könyvtár megosztás:
# Tiltjuk a ponttal kezdődő állományok megjelenítését. Nem írásvédett és nem kereshető.
```

```
# Az új fájlokhoz csak a tulajdonosnak lesznek jogai.
```

```
[homes]
comment = Home Directories
read only = No
browseable = No
hide dot files = yes
create mode = 0700
```

```
# Belépéskezeléshez szükséges netlogon könyvtár:
```

```
[netlogon]
comment = Network Logon Service
path = /home/netlogon
guest ok = Yes
browseable = No
writable = no
share modes = No
```

```
# Proffájlokat tartalmazó könyvtár:
```

```
[Profiles]
path = /home/profiles
guest ok = Yes
browseable = No
create mode = 744
directory mode = 755
```

```
# Nyomtatóink megosztása:
```

```
# Csak a tanár és a nyomtat csoportba tartozóknak van joga használni.
```

```
[printers]
comment = All Printers
path = /var/spool/samba
read only = No
guest ok = Yes
printable = Yes
browseable = No
```

```
public = no
writable = no
create mode = 0700
valid users = @tanar, @nyomtat
```

# Egy alap könyvtármegosztás mindenki számára, de csak a tanárok írhatják:

```
[kozos]
comment = Közös Könyvtár
path = /home/public
write list = @tanar
guest ok = Yes
```

# Egy csoport számára megosztott könyvtár

```
[10c]
comment = 10C könyvtára
path = /home/10c
valid users = @10c
public = no
writable = yes
printable = no
force user = 10cof
force group = 10c
create mode = 770
```

# CD-megosztás:

```
[CD_ROM]
path = /mnt/cdrom/
read only = yes
available = yes
share modes = no
locking = no
browseable = yes
public = yes
```

## 6.3 SWAT

A Samba beállítására létezik egy kifejezetten ezt a célt szolgáló felület is a SWAT. Előnye, hogy gyorsabban követi a verzióváltozásokat. Szintén külön kiszolgálóval megoldott http protokollon keresztül elérhető webes felületről van szó. Viszont nem állandóan futó démon, hanem az xinetd csúcsdémon hívja meg.

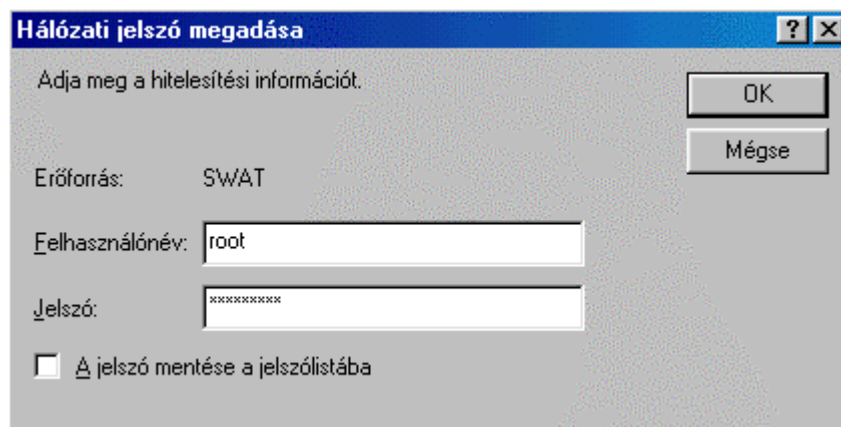
A SWAT működéséhez a `/etc/service` fájlban jelen kell lennie a `'swat 901/tcp'` sornak. Ellenőrizzük, ha nincs benne, akkor vegyük fel. A másik beállítás, az xinetd figyelésének megadása a 901-es portra. Keressük meg a `/etc/xinetd/swat` fájlt és a tartalmát állítsuk át a következőre:

```
service swat
{
    port          = 901
    socket_type   = stream
    wait          = no
    only_from     = 192.168.1.0# A hálózat címe, amelyről használni szeretnénk.
    user          = root
    server        = /usr/sbin/swat
    log_on_failure += USERID
    disable       = no
}
```

Ha a fájl nem létezik, akkor hozzuk létre a fenti tartalommal. A művelet elvégzése után indítsuk újra az xinetd-t.

`/etc/init.d/xinetd restart`

A böngészőbe a `http://szerverip:901` (pl: `http://192.168.1.1:901`) ULR-t használva léphetünk be a SWAT-ba, amely rögtön kéri az azonosítónkat. Mivel rendszerszintű beállításról van szó, root felhasználóval azonosíthatjuk magunkat.



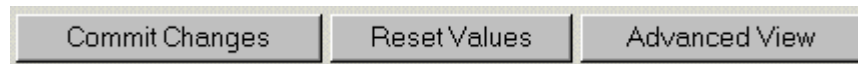
Itt jegyezném meg, hogy minden ehhez hasonló program sok segítséget nyújthat, de csak addig, amíg a beállításokat végezzük. Viszont a működésük biztonsági lyukat is jelenthet. Ezért csak akkor indítsuk el, ha szükségünk van rá és használat után állítsuk le. A SWAT esetében a megoldás az `/etc/xinetd/swat` fájlban a `disable=yes` beállítása.

Visszatérve az eredeti témánkhoz, a sikeres autentikáció után a SWAT kezdőoldala (HOME) vár bennünket némi angol nyelvű dokumentációval.



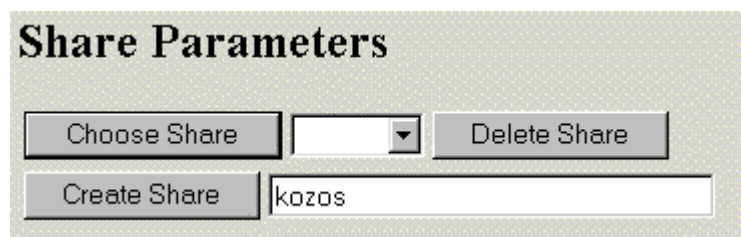
A globals ikonra kattintva állíthatjuk be a globális változókat. Mivel itt is a már említett paramétereket találjuk, a beállításokat nem elemezzük újból. A kezelést nézzük inkább meg. A beállított értékek a Commit Changes gomb hatására kiíródnak a

konfigurációs fájlba. A Reset Values gombbal visszaállítjuk az utolsó mentett állapotot.



A képernyőn először csak az alapvető beállítások és az általunk módosítottak találhatóak. Az Advanced View gomb hatására az összes beállítás megjelenik. A Basic View gombbal pedig visszaállhatunk az egyszerűbb verzióra. A beállítások csoportokra bontva találhatóak. Mindegyik mellett található Help link, amely angol nyelvű segítséget hív meg.

Shares oldalon a fájlmegosztásokat tudjuk állítani. A legördülő menüvel és a Choose Share gombbal kiválaszthatjuk a módosítani kívánt megosztást, vagy a beíró mezővel és a Create Share gombbal újat vehetünk fel. A már kiválasztott megosztást a Delete Share gombbal törölhetjük.



A megosztások kiválasztása után a beállítás hasonló a Global-nál tapasztaltakhoz. Szintén hasonló kezelőfelülettel rendelkezik a Printers oldal is. Itt állíthatjuk a nyomtatómegosztásainkat.

A Status oldalon a Samba működésével kapcsolatos információkat, míg a View oldalon a kész smb.conf állományt láthatjuk.

## 6.4 Egyéb kézi adminisztrációk

A /etc/samba könyvtárban találjuk az lmhosts állományt. Ebbe kézzel is írhatunk IP-NetBIOS név párosokat a könnyebb névfeloldás kedvéért.

PI:

192.168.1.10admin

192.168.2.20igazgato

Szintén itt található az smbusers állomány, amely a unix felhasználó-Samba felhasználó kapcsolásokat tartalmazza, azaz hogy a Samba felhasználó mely Unix felhasználó jogosultságait örökölje.

PI:

unix = samba1 samba2

tanulo = 10c 11c

Az smbpasswd fájl tartalmazza a kódolt Samba jelszavakat. Új felhasználót jelszóval felvehetünk a következő paranccsal:

```
smbpasswd -a ujuser
```

Meglévő felhasználó jelszavának módosítása:

```
smbpasswd ujuser
```

Amennyiben XP, 2000, NT klienseink vannak a hálózaton, akkor szükséges lehet a gépek felvétele, unix felhasználónak és samba felhasználónak. Ezt sajnos igénylik ezek a kliensek.

Gép felvétele unix felhasználóként:

```
adduser -s /bin/false -M gepnev$
```

Gép felvétele samba felhasználóként:

```
smbpasswd -a -m gepnev
```

A másik lehetőség, hogyha a Samba kiszolgálónkhoz ami PDC-ként működik, felvesszünk egy root felhasználót is. Természetesen jelszava ne egyezzen meg a Unix oldali jelszóval! Amikor egy új géppel lépünk be a tartományba, a root felhasználót adjuk meg, ekkor automatikusan felveszi a Samba a gépet.

Az XP gépek egy újfajta jelszótitkosítást használnak. Ezt a 2-es sorozatú Samba nem tudja kezelni, ezért XP-ről nem lehet felcsatlakozni. A regisztriben meg lehet változtatni a jelszó kódolását. Egy regisztri kulcsot kell 1-ről 0-ra állítani. Hogy melyiket, ezt az első belépési hiba után az event log-ban megtaláljuk.

## 6.5 Gyakorlat

Vegyük fel Samba felhasználóként a következő (már létező) Linux felhasználókat:

Kiss Elemér  
Nagy János  
Balla Nárcisz

Állítsuk be a szamba szerverünk általános beállításait (Global) és hozzuk létre a következő megosztásokat:

- Minden felhasználó látja és írhatja a saját home könyvtárát.
- Minden felhasználó használhatja a szerver nyomtatóját.
- Az iskola csoportba tartozó felhasználók látják és írhatják a /home/iskola könyvtárát.
- Az tanar csoportba tartozó felhasználók látják és írhatják a /home/tanar könyvtárát.

Hozzuk létre egy olyan megosztást, amely külön konfigurációs állományban van és csak a tanar csoport esetében érvényesül. A megosztás a szerverben található CD-ROM-ot osztja meg.

## 6.6 Ellenőrző kérdések

1. Mi a Samba?
2. Mi a tartomány?
3. Mi a megosztás?
4. Írd le az SMB protokoll lényegét?
5. Mire használhatunk egy Wins szerveret?
6. Mi az a Master Browser (főtallózó)?
7. Milyen autentikációs lehetőségeket ismersz a Samba-nál (security), magyarázd is meg őket.
8. Mikor kell feltétlenül kódolt jelszavakat használni a Samba-nál?
9. Milyen buktatói vannak a Samba felhasználó kezelésének?
10. Milyen jellegzetesebb megosztás típusokat ismersz?
11. Milyen problémák adódhatnak a fájlnevek kezelésével a megosztásoknál?
12. Mi az a SWAT?
13. Hol található a Samba beállítását tartalmazó fájl?
14. Milyen a beállító fájl felépítése?
15. Mit jelent a 'workgroup = ISKOLA' global beállítás?
16. Mit jelent a 'security = user' global beállítás?
17. Elemezd ki az alábbi megosztást:  
[homes]  
comment = Home Directories  
read only = No  
browseable = No  
hide dot files = yes  
create mode = 0700
18. Elemezd ki az alábbi megosztást:  
[printers]  
comment = All Printers  
path = /var/spool/samba  
read only = No  
guest ok = Yes  
printable = Yes  
browseable = No  
public = no  
writable = no  
create mode = 0700  
valid users = @tanar, @nyomtat
1. Elemezd ki az alábbi megosztást:  
[kozos]  
comment = Közös Könyvtár  
path = /home/public  
write list = @tanar  
guest ok = Yes
2. Mire használjuk a smbusers állományt?
3. Hogyan adjuk meg a Samba jelszavát egy új felhasználónak?

## 6.7 Felhasznált, ajánlott irodalom

Samba-villám HOGYAN

<http://linux.vv.hu/hogyanok/villam/Samba-villam-HOGYAN/sambalightning.html>

Samba (Kossuth kiadó könyve, letölthető)

<http://linux.vv.hu/konyv/samba/index.html>

SMB protokollt használó munkaállomások kiszolgálása Linux szerverrel

<http://linux.vv.hu/konyv/smb-protokoll/index.html>

## 7. Apache

### 7.1 Alapismeretek

Az Apache szerver egy igen dinamikusan fejlődő http kiszolgáló. Fejlesztése az Illionis-i egyetemen található NCSA-ban kezdődött. Az NCSA Web szerver foltozgatásából keletkezett. Manapság az Internetre kötött Web kiszolgálók 60%-a ezt használja. Dinamikus fejlődésének példája, hogy nemrégiben megállapodás született a Microsoft és a Covalent között az ASP.NET Apache-on történő implementálására.

Az Apache modulus szerkezetű. Ennek rengeteg előnye van. Mivel szabvány API-val rendelkezik, ezért más cégek, társaságok is fejlesztenek alá modulokat. Másrészt erőforrást takarítunk meg azzal, hogy a nem használt modulok nem töltődnek be a memóriába.

Egy Web szerver beállításánál talán a leglényegesebb feladat, eldönteni mely modulokat használjuk. Természetesen minden modulnak vannak önálló beállítási paraméterei. Ezekkel és a funkcióikkal kapcsolatban lényeges segítséget kapunk a <http://modules.apache.org> oldalon. Nézzünk egy-két lényegesebb modult:

mod_access	Szabályozza, az oldalhoz milyen hostok férjenek hozzá
mod_actions	Script futtatása (CGI)
mod_alias	Álnevek és átirányítások
mod_asis	Az .asis fájl header
mod_auth	Felhasználó azonosítás szöveges fájlokból
mod_auth_anon	Névtelen felhasználó azonosítás
mod_auth_db	Felhasználó azonosítás a Berkeley-féle DB adatbázisból
mod_auth_dbm	Felhasználó azonosítás DBM adatbázisból
mod_auth_digest	Felhasználó azonosítás MD5 jelszókódolással
mod_autoindex	Automatikus könyvtártartalom listázása
mod_cern_meta	HTTP fejléc meta elemeinek támogatása
mod_cgi	CGI script-ek futtatása
mod_digest	MD5 kódolású jelszó kezelése
mod_dir	Alapszintű könyvtárkezelés
mod_env	Környezeti változók átadása CGI script-eknek

mod_example	API minták
mod_expires	Oldalak érvényességi ideje
mod_headers	HTTP fejlécek
mod_imap	Images fájlterkép
mod_include	Szerveroldali objektumok (SSI)
mod_info	Szerver információk
mod_log_agent	Felhasználói, böngésző adatok tárolása a naplóban
mod_log_config	Naplózás beállítása
mod_log_referer	Honnan jött a kliens információk rögzítése a naplóban
mod_mime	Objektumtípus megállapítása fájlkiterjesztésből
mod_mime_magic	Objektumtípus megállapítása tartalomból
mod_mmap_static	Fájlok térképének bevitele a memóriába
mod_proxy	HTTP gyorsítótár
mod_rewrite	Reguláris kifejezések használata
mod_setenvif	Környezeti változók beállítása kliens információk alapján
mod_so	Futás közbeni modul-betöltés támogatása
mod_speling	Automatikus hibajavítás az URL-ekben
mod_status	Szerver állapot megjelenítése Web-lapként
mod_userdir	A felhasználók könyvtárait kezeli (public_html)
mod_unique_id	Kérés azonosító generálása minden lekéréshez
mod_usertrack	Felhasználó-követés sütik (cookies) segítségével
mod_vhost_alias	Virtuális szerver-támogatás

## 7.2 Apache beállítása kézzel

Az Apache a beállításait a /etc/httpd/conf könyvtárban tárolja. A legnagyobb és gyakran egyetlen beállító fájl a httpd.conf. Ezt fogjuk átnézni a következőkben. Az beállítások sorrendje néha lényeges lehet. Használunk olyan opciókat, amelyek modulokhoz tartoznak, ezeknek a szóban forgó modul betöltődése után kell lenniük.

Általános beállítások:

```

ServerType standalone          # A szerver külön démonként üzemel, nem
                               az inetd indítja.
ServerRoot "/etc/httpd"       # Adatkönyvtár helye. Konfig állományok,
                               modulok, logok.
User apache                   # Milyen felhasználó jogosultságon fusson.
Group apache                  # Milyen csoport jogosultságon fusson.
ServerAdmin admin@iskola.hu   # Hiba esetén ezt a címed adja kontaktnak.
UseCanonicalName On          # A linkeket kiegészíti a gépnévvel.
HostnameLookups Off          # IP cím feloldása. Nagyon lassítaná, ha nincs
                               közelbe DNS cache.
LockFile /var/lock/httpd.lock # Indítási tiltás fájl.
PidFile /var/run/httpd.pid    # Indulási folyamat azonosító száma.
ScoreBoardFile /var/run/httpd.scoreboard # Futási információk.
Timeout 300                   # Időtűllépés
KeepAlive On                  # Tartós kapcsolatok a klienssel.
MaxKeepAliveRequests 100     # Mennyi kérést tartson fenn.
KeepAliveTimeout 15          # Időtűllépés kapcsolat esetén
MinSpareServers 5            # Minimum mennyi felesleges szerver működjön.

```



```
MaxSpareServers 20      # Maximum mennyi felesleges szerver működjön.
StartServers 8         # Indulásnál mennyi felesleges szerver
működjön.
MaxClients 150        # Maximum hány kapcsolat élhet.
MaxRequestsPerChild 100 # Hány kérés után öljön meg egy alszervet.
Port 80               # Ezeket a portokat figyeli.
Listen 80
Listen 443
```

#### Modulok betöltése

Az alapbeállítások után a modulok betöltése és elindítása következik. Döntsük el mely modulokat szeretnénk használni és a felesleget kommentezzük ki.

```
LoadModule env_module modules/mod_env.so
....
ClearModuleList
AddModule mod_env.c
....
```

#### A **php** modulok betöltése és beállítás:

```
LoadModule php4_module modules/libphp4.so
AddModule mod_php4.c
AddType application/x-httpd-php .php4 .php3 .phtml .php
AddType application/x-httpd-php-source .phps
```

#### A **perl és cgi** modul betöltése és beállítása:

```
LoadModule perl_module modules/libperl.so
AddModule mod_perl.c
Alias /perl/ /var/www/perl/
<Location /perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
</Location>
ScriptAlias /cgi-bin/ "/home/httpd/cgi-bin/"
<Directory "/home/httpd/cgi-bin">
    SetHandler perl-script
    PerlHandler Apache::Registry
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>
```

Még érdemes beállítanunk a következő értékeket:

```
TypesConfig /etc/mime.types # mime típusokat tároló fájl helye
```

```
DefaultType text/plain          # Alapértelmezett típus ismeretlen esetén.
AddType text/html .shtml        # Server oldali inside
AddHandler server-parsed .shtml
AddHandler imap-file map        # imap fájl kezelése
```

### Könyvtár és fájl beállítások

```
DocumentRoot "/var/www"        # A dokumentumok gyökérkönyvtára
# Minden könyvtárra külön szabályokat állíthatunk be. Ezt a <Directory ..>
# meghatározással tehetjük
# A következő beállítás az összes könyvtárra él.
<Directory />
  Options FollowSymLinks
  AllowOverride None
</Directory>
# Szerver gyökérkönyvtára:
<Directory "/var/www">
  Options Indexes Includes FollowSymLinks
  AllowOverride None
  Order deny, allow
  Allow from all
</Directory>
# A könyvtárak az options-al adjuk meg és a következők lehetnek:
# none - semmi
# all - összes
# Indexes - a meghatározott index állomány behívása könyvtárhivatkozás esetén.
# Includes - Futtathat szerver oldali scriptet
# FollowSymlinks - Követi a szimbolikus linkeket.
# ExecCgi: CGI scriptek futatását engedi.
# Az order beállítással tudjuk megadni, hogy tiltást vagy az engedélyezést
ellenőrizze először.
# Allow - engedélyezés pl: Allow from 192.168.0.0/255.255.0.0
# Deny - tiltás pl: Deny from rosszdomain.hu

# Meghatározzuk, hogy könyvtárhivatkozás esetén milyen sorrendben mely
állományokat indítson.
DirectoryIndex index.html index.htm index.php index.php4
# Megadjuk a könyvtárban lévő egyedi beállításokat tartalmazó fájl nevét, majd
letiltjuk a közvetlen olvasását.
AccessFileName .htaccess
<Files ~ "\.ht">
  Order allow,deny
  Deny from all
</Files>

# Autentikált könyvtárak esetén a következő beállítás kell:
<Directory /var/www/html/admin>
  AuthName "Ezt a szöveget írja ki"
  AuthType Basic                # autentikáció típusa
  AuthUserFile /etc/httpd/conf/jelszo.conf # honnan vegye a felhasználókat
```

```

AuthAuthoritative on
Require valid-user          # minden ismert felhasználónak engedje
# Require igazgato          # csak az igazgato felhasználónak engedi
</Directory>

```

### Log állományok kezelése

```

ErrorLog /var/log/httpd/error_log # hibák kiírása
LogLevel warn                    # Alap logolási szint
# Egyedi beállítások különböző lehetőségei:
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
# A log állományunknál a common nevű egyénileg definiált stílust használjuk:
CustomLog /var/log/httpd/access_log common

```

### Virtuális hostok beállítása

```

# virtual host modul betöltése:
LoadModule vhost_alias_module  modules/mod_vhost_alias.so
AddModule mod_vhost_alias.c
# virtual host neve:
NameVirtualHost 192.168.1.1

<VirtualHost 192.168.1.1:80>    # 80-as porton érkező kéréseket figyel
    ServerAdmin admin@iskola.hu
    DocumentRoot /var/www/html # az oldal helye
    ServerName 192.168.1.1     # erre a névre hivatkozott oldalakat nézi
    CustomLog logs/html_access.log combined
</VirtualHost>

```

### Virtual host **ssl** beállítással:

```

# SSL modul betöltése és alapbeállítása
LoadModule ssl_module          modules/libssl.so
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
SSLPassPhraseDialog builtin
SSLSessionCache dbm:/var/run/ssl_scache
SSLSessionCacheTimeout 300
SSLMutex file:/var/run/ssl_mutex
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
SSLLog /var/log/httpd/ssl_engine_log
SSLLogLevel warn

<VirtualHost 192.168.1.1:443>
    DocumentRoot "/var/www/htmls"

```

```
ServerName 192.168.1.1
SSLEngine on
SSLCipherSuite
ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile /etc/httpd/conf/ssl/server/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl/server/server.key
SSLCACertificatePath /etc/httpd/conf/ssl/cac
SSLCARevocationPath /etc/httpd/conf/ssl/car
SSLVerifyClient none
SSLVerifyDepth 10
SSLOptions +ExportCertData +StrictRequire
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
SetEnvIf Request_URI \.gif$ gif-image
</VirtualHost>
```

### 7.3 Jelszókezelések

Mint már láthattuk, hogy van lehetőségünk egyes könyvtárak elérését felhasználó azonosításhoz kötni. A felhasználókat és a jelszavakat célszerű külön fájlban tárolni. Új felhasználó felvétele a következőképpen történik:

```
# htpasswd jelszo.conf felhasználonev
New password:
Re-type new password:
Adding password for user felhasználonev
```

Amennyiben még nincs létező jelszófájl, úgy használjuk a -c paramétert:  
# htpasswd -c jelszo.conf felhasználonev

### 7.4 Gyakorlat

A telepített szerverünkön állítsuk be az apache Web-szervert. Működését ellenőrizzük is le egy kliens segítségével.

### 7.5 Ellenőrző kérdések

1. Mire használnál egy apache szervert?
2. Határozd meg mik a modulok!
3. Magyarázd az ssl fogalmát!
4. Milyen portot használ egy webszerver alapértelmezésben?
5. Mi a virtuális hoszt?
6. Hol találjuk az apache beállításait?
7. Mit jelent a 'ServerType standalone' beállítás?
8. Magarázd az alábbi beállításokat:
  - MinSpareServers 5
  - MaxSpareServers 20
  - StartServers 8
9. Elemezd az alábbi beállításokat:
  - <Directory /var/www/html/admin>

```
AuthName "Admin oldal"  
AuthType Basic  
AuthUserFile /etc/httpd/conf/jelszo.conf  
AuthAuthoritative on  
Require valid-user  
</Directory>
```

10. Mire használható a htpasswd program?

## 7.6 Felhasznált, ajánlott irodalom

Ben Laurie : Apache (Kossuth)

Az Apache

<http://linux.vv.hu/egyebek/halozat/apache2/hozzavalo.html>

Authentikált oldalak Apache web szerver alatt

<http://linux.vv.hu/egyebek/halozat/apache/authent.html>

Biztonságos Web-szerver kialakítása Debian GNU/Linux 2.2 rendszeren

<http://linux.vv.hu/konyv/biztonsagos-web-szerver/bw00.html>

Web-szerver kialakítása Red Hat Linux 6.2 alatt

<http://linux.vv.hu/common/konyv.shtml>

## 8. Sendmail

### 8.1 Alapismeretek

A Sendmail általános levelezést valósít meg SMTP protokollon keresztül. Hogy megértsük az Internetes levelezés lényegét, nézzük meg, mit csinál a Sendmail valójában.

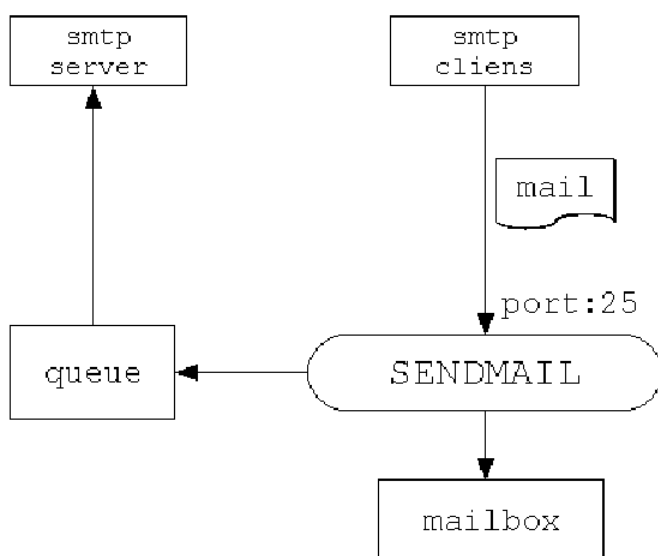
Az Levelek a 25-ös porton keresztül érkeznek meg a levelezőszerverre. Két esetben érkezik ez szabályosan meg:

- Ha a levelező szervert kimenő SMTP szerverként használja egy kliens. Ebben az esetben a levelező program juttatja oda a levelet, továbbküldés céljából. A hagyományos SMTP protokollban nincs autentikációs lehetőség. Ezért nem tudjuk ellenőrizni az esemény jogosultságát. Ennek kompenzálásra megadjuk azokat a hálózatokat, melyekről engedélyezzük a szolgáltatás elérését. Ezeket a hálózatokat mondjuk Relay Domain-oknak. Az RFC 2554 (SMTP kiegészítő) szabvány alapján van lehetőségünk az autentikált SMTP szolgáltatásra.
- Továbbá, ha a levél a mi számítógépünkre van címezve. Ebben az esetben is egy ellenőrzésen esik át a levél. A levelező szerver megnézi, hogy a levél által megcímezett domain szerepel-e a Local Domain listában. Ha szerepel, akkor ellenőrzi, hogy létezik-e a felhasználó. A felhasználó azonosításánál figyelembe veszi az alias neveket is.

Ezek alapján meg kell adnunk azon domain-ek listáját, amelyekre az érkező leveleket elfogadja a szerverünk. Ezen kívül be kell állítanunk, hogy honnan fogadjuk el kimenő levelet.

A beérkező levelek érkehetnek többféle domainra is. A levelet az a felhasználó fogja megkapni, akinek a felhasználó neve azonos a címzettjével. Olyan szervereken, amelyek több domaint látnak el, problémát okozhat a más domainon, de ugyanazon a néven szereplő felhasználók. Ezért lehetőségünk van rá, hogy megadjuk az e-mail-hoz tartozó felhasználót. Ezt nevezzük virtualuser beállításnak.

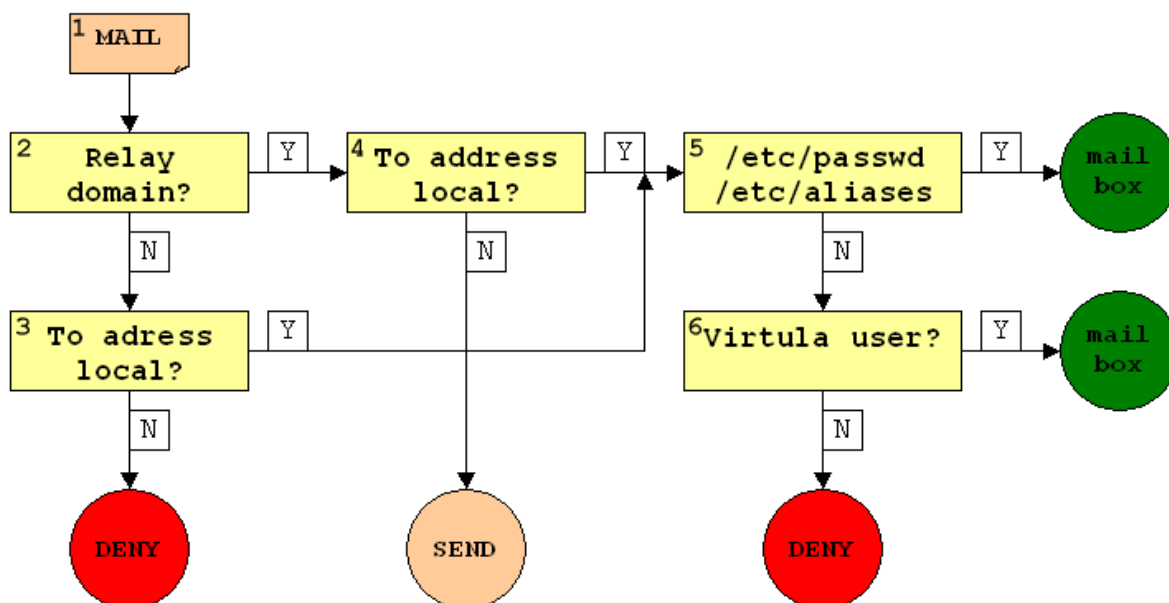
Nézzük meg egy levél útját a klientsztől a címzett szerverig:



- A levelező kliens a beállításai alapján az SMTP szerveréhez küldi a levelet.
- A szerver megvizsgálja, hogy a levél címzettjét ő kezeli-e, ha igen akkor az adott szerveren található címzett mailbox fájljához hozzáfűzi.
- Ha a címzett egy másik szerveren található, akkor a queue sorba rakja be. Ez egy könyvtár, jellemzően a /var/spool/mqueue.
- Néha lefuttat a sendmail

egy rutint, ami a queue-ben található leveleket megpróbálja elküldeni a címzett szervernek. Ha ez nem sikerül (például abban a pillanatban nem üzemel a szerver), akkor bent hagyja a queue-ben és a következő alkalommal újra megpróbálja elküldeni.

Vázlatosan leírva ez egy levél sorsa, de mi van akkor, ha nem csak a kliensek fordulnak a szerverhez levélküldés céljából, hanem más szerverek is az itt kezelt postafiókok miatt. A beérkező levél jogosultságának ellenőrzése már egy bonyolultabb folyamat. Nézzük ezt is egy vázlat alapján:



- 1. MAIL - Beérkezik egy levél
- 2. Relay Domain? - A szerver megvizsgálja, hogy a levelet olyan helyről küldték-e, ahol legális kliensek vannak?
  - Ha IGEN, akkor mindenképpen el kell fogadnia a levelet > 4.
  - Ha NEM, akkor csak abban az esetben ha helyi felhasználónak címzett. >3
- 3. Ha nem kliens küldte a levelet, akkor megnézi, hogy helyi felhasználónak van-e címezve?
  - Ha IGEN, akkor bejöhét a levél > 5.
  - Ha NEM helyi felhasználónak szól, akkor a levél tiltva lesz. > DENY(vissza megy a feladónak hibás domainnel)
- 4. Ha legális kliens küldte a levelet, akkor megnézi, hogy helyi felhasználónak van-e címezve?
  - Ha IGEN, akkor bejöhét a levél >5.
  - Ha NEM, akkor a levél továbbítódik a címzett felé, azaz queue sorba kerül. SEND
- 5. Ide, azok a levelek érkeznek el, amik helyi felhasználónak szólnak a domain alapján. Most megnézi a szerver, hogy létezik-e ez a felhasználó?
  - Ha IGEN, akkor a felhasználó mail boksza-ába kerül a levél.
  - Ha NEM, akkor a virtualuser ellenőrzésre > 6.
- 6. Ellenőrzi, hogy a címzett szerepel-e a virtual user táblában.
  - Ha IGEN, akkor megállapítja a helyi felhasználót (ezt is ellenőrzi, mint 5. pont) és a levél a felhasználó mail boksza-ába kerül.
  - Ha NEM, akkor a levél tiltva lesz. > DENY (vissza megy a feladónak hibás felhasználóval)

Igen nagyotlan ezeken a fő vizsgálatokon kell átesnie egy levélnek. Persze még lehetne finomítani, bontani az eseménysorozatot, de a további munkánkhoz elég lesz ezeket az eseményeket érteni.

## 8.2 Sendmail kézi beállítása

A Sendmail config állomány a `/etc/sendmail.cf` állomány tartalmazza. Megtervezésénél az alkotók, azt tartották a fontosnak, hogy a Sendmail könnyen és gyorsan tudjon működni. Emiatt a `sendmail.cf` enyhén szólva nem emberbaráti. A beállítás könnyítésére ugyan van egy fordítási lehetőségünk, de az is elég nehézkesre sikerült. Ebből az okból azokat a beállításokat, amelyek általánosak, kihozták fájlalba. Ezeket a fájlokat a `/etc/mail` könyvtárban találhatjuk. Nézzük meg ezeket az állományokat:

- `access`

A levelek elfogadását szabályozó feltételeket állíthatjuk be. Itt kell beállítani a Relay domainokat is:

```
192.168 RELAY
```

Ezzel azt engedjük meg, hogy a `192.168.0.0/255.255.0.0` hálózat gépei használhassák sendmailunkat SMTP szervernek.

```
spam.hu REJECT
```

Itt nem fogadjuk el a `spam.hu` domainról érkező leveleket.

- `local-host-names`

Ide soroljuk fel azokat a domainokat, amelyeket a sajátjaként kezel a mail szerverünk, azaz elfogadjuk az ezekre érkező leveleket. Minden domaint új sorba írunk.

- `mailertable`

Itt tudjuk beállítani a domainok átirányítást másik szerverre. Például:

```
.iskola.hu smtp:192.168.1.20
```

Itt az `iskola.hu` címre érkező leveleket (a címzett megváltoztatása nélkül) tovább küldünk a `192.168.1.20` IP című, belső hálózaton lévő szerverre.

- `virtusertable`

Itt a beérkező leveleket tudjuk átirányítani.

```
kis.janos@iskola.hu janika
```

# Itt a `kis.janos@iskola.hu` címre érkező leveleket a `janika` nevű felhasználónak adjuk.

```
@regiiskola.hu %1@iskola.hu
```

# Itt a `regiiskola.hu` domainra érkező leveleket továbbítjuk az `iskola.hu` domainre

# a címzett megváltoztatása nélkül.

A fenti fájlok a lényegesebb beállításokat tartalmazzák. Van egy-két beállítás melyet a `sendmail.cf`-ben érdemes megváltoztatnunk. A legegyszerűbb megoldás, hogy rákeresünk a beállításra és módosítjuk. Vigyázzunk a szintaktika megmaradására.

- A levelek maximális mérete: (alapbeállítás nincs, byte-ban megadva)

```
O MaxMessageSize=1000000
```

- Amennyiben a levelet nem lehet továbbítani, akkor ennyi idő múlva küld figyelmeztetést a feladónak:

```
O Timeout.queuewarn=4h
```



- Ha nem tudja a megadott időn belül postázni a levelet, akkor visszaküldi a feladónak.  
O Timeout.queueereturn=5d
- O DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA  
Töröljük, vagy kommentezzük ki a fenti sort, mert különben csak a lokális gépről tudunk kifelé levelet küldeni.

A felhasználók elhelyezhetnek a home könyvtárban .forward állományt. Ezzel megadhatják, hogy leveleiket hova irányítsa tovább a rendszer. A fájlban több sorban (soronként egyet) több címet is megadhatunk. Ha azt szeretnénk, hogy az eredeti címen is jelentkezzen a levél, akkor azt is fel kell venni a listába.

A postázásra váró levelek a /var/spool/mqueue könyvtárban találhatóak. A várakozó levelek listáját a mailq paranccsal listázhatjuk ki és a 'sendmail-q' paranccsal tudjuk erőltetni a kiküldésüket.

### **8.3 Gyakorlat**

Állítsunk be egy Sendmail szerveret a megfelelő domainre. Egy meghatározott hálózatról lehessen SMTP szervernek használni. A felhasználóknak ne csak a felhasználó nevükre lehessen e-mailt küldeni, hanem a teljes nevükre is ponttal elválasztva (kisse@domain.hu és kiss.elemer@domain.hu)

### **8.4 Ellenőrző kérdések**

1. Mire használjuk a Sendmail programot?
2. Mi az smtp?
3. Mi a pop3?
4. Milyen ellenőrzéseken kell átesni egy levélnek, amikor a levelezőszerverhez érkezik?
5. Magyarázd a relay domain fogalmat!
6. Mit nevezünk local domain-nak?
7. Mi a virtual user?
8. Mi a queue egy levelezőszerver esetén?
9. Hol találjuk a sendmail beállításait?
10. Mit állítunk a /etc/mail/access fájlban?
11. Mit állítunk a /etc/mail/local-host-names fájlban?
12. Mit állítunk a /etc/mail/virtusertable fájlban?

### **8.5 Felhasznált, ajánlott irodalom**

RICHARD BLUM: Sendmail Linuxra (Kossuth)

Sendmail telepítése és beállítása  
<http://linux.vv.hu/konyv/sendmaildoc/index.html>

GPG-Mini HOGYAN

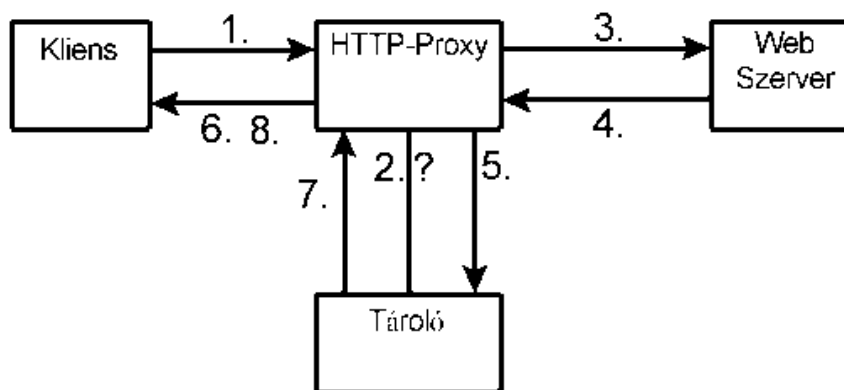
<http://linux.vv.hu/hogyanok/mini/GPG-Mini-HOGYAN/GPGMiniHowto.html>

## 9. Squid proxy

### 9.1 Alapismeretek

Napjainkban a hálózat forgalmának nagy része a Web-oldalak eléréséből adódik. Egy lokális hálózatnak az Internet kapcsolata mindig szűkös szokott lenni. Az intézményben jellemzően többen is nézik ugyanazon oldalakat, melyeknek minden eleme többször is átmegy a szűk szegmenset képző bekötésen. Ezen ismétlődések megszüntetésével, akár 30% forgalomcsökkenést is elérhetünk.

A http proxy-eknek éppen ez az egyik feladata. Betelepszik a kliens és az Internet közé. Ha a böngésző le akar tölteni egy oldalt, akkor az nem az oldalt tároló szerverrel, hanem a lokális hálózaton elhelyezett proxy szerverrel közli. A proxy megnézi, hogy a tárolójában (cache) megtalálható-e az oldal. Ha nem található meg, akkor azt letölti a Web-szerverről a tárolójába, majd az oldalt átküldi a kliensnek.



Nézzük meg a folyamatot konkrétan:

1. A kliens elküldi a proxy-nak, hogy szüksége van a [www.linux.hu](http://www.linux.hu) oldalra.
2. A proxy megnézi, megtalálható-e ez az oldal a tárolóban.

Ha nincs tárolva az oldal:

3. A web-szervernek jelzi az igényét.
4. Letölti az oldalt a web-szerverről.
5. Elrakja az oldalt a tárolóba.
6. Elküldi az oldalt a kliensnek.

Ha tárolva van már az oldal:

7. Betölti a tárolóból az oldalt.
8. Elküldi a kliensnek az oldalt.

Általában a dolog nem ilyen egyszerű, de a folyamatot meg lehet érteni belőle. Például a dinamikus oldalakat nincs értelme tárolni, ugyanis azok esetenként is változhatnak. Ami viszont lényeges, hogy egy átlagos web-oldal teljes méretének (Byte-ban) a 60-80%-a a képekből áll, ami ritkán szokott változni.

A squid proxy működése közben érdemes lesz figyelni két értéket, a találati arányt dokumentumokban, amely azt határozza meg, hogy az összes kliens lekérdezésből hány objektumot (html fájlt, kép fájlt, stb.) tudott a tárolóból kiszolgálni és a byte találati arányt, amely az Interneten keresztül letöltött és a tárolóból kiszolgált adatok mennyiségét határozza meg.

Ha proxy szervert üzemeltetünk, akkor a kliensnek meg kell adni, a szerver elérési paramétereit, azaz az IP címét és a portszámát. Van lehetőségünk ennek elkerülésére, ha transzparens proxy-t állítunk be. Ebben az esetben a kimenő forgalmat kezelő tűzfalon el kell csípnünk a kifelé irányuló web-oldal lekéréseket (80-as port) és át kell irányítanunk a proxy címére. Így elkerülhetjük a kliensek böngészőinek állítását. Erről a kézi beállításoknál még lesz szó.

## 9.2 Squid beállítása

A Squid beállításait a `/etc/squid/squid.conf` állományban találhatjuk. A beállító fájl tökéletesen kommentezett. Nem sokat kell rajta állítanunk. Nézzük tehát az érdekesebb beállításokat:

```
http_port 3128
http_port 192.168.1.1:3128
```

Itt tudjuk beállítani, hogy a proxy melyik portot figyelje a munkája során. A Sulinetre jellemző a 8080-as port használata, viszont a Squid alapértelmezett portja a 3128-as. Bármelyiket használhatjuk kedvünkre. Amennyiben több hálózati kártyánk van a gépen, akkor be kell állítanunk, melyiken keresztül lehessen csatlakozni a proxy-nkra. Soha se nyissuk meg az Internet felé, tehát az jó beállítjuk a kártya IP címét is beállítás. Írjuk be a belső hálózati kártya címét.

```
cache_peer proxy.szfv.sulinet.hu parent 8080 8080 default
```

A felsőbb proxy-t határozza meg. Ez nálunk lényeges lehet, hiszen nagy kapacitású proxy szerverek dolgoznak a Sulineten belül, jó lenne kihasználni. Állítsuk be területi Sulinet proxy szervert, méghozzá parent módba. Ez azt jelenti, hogy a mi proxynk ezt fogja használni kimenő proxy-ként. Sorban a következő adatok találhatóak:

- A proxy neve, vagy IP címe.
- A másik proxy típusa, illetve a kapcsolatunk típusa.
- Parent. Olyan proxy-nal használjuk, ahonnan mi kérünk le adatokat.
- Sibling. Olyan proxy-nál használjuk, amelyek tőlünk kérnek adatokat.
- Multicast. Egyenlő oda-vissza kapcsolat.
- A másik szerver proxy portja.
- A másik szerver proxy ICP portja.
- Default. Beállíthatjuk alapértelmezettnek, ez azt jelenti hogy a proxy-nk alapesetben ezt a kapcsolatot használja.

```
cache_mem 16 MB
```

Ez a paraméter azt a memóriaterületet határozza meg, amelybe a proxy a cached könyvtár tartalmának jegyzékét teszi el. Tehát ez függ a cached könyvtár méretétől. Viszont ha túl nagy értéket határozunk meg, akkor a Squid más igényeinek nem jut

elég hely, így gyakran nyúl a virtuális memóriához, ami lassítja a működését. Jellemző érték a Squid-nak szánt memória harmada.

```
Cache_dir ufs /var/spool/squid 1000 256 256
```

A 'Cache\_dir' beállításnál adjuk meg a cache könyvtár adatait. A beállításnál adjuk meg a kezelés típusa általában ufs szokott lenni, az elérési útját és a cache könyvtár méretét (Mbyte-ban). A cache könyvtárat érdemes külön partícióra tenni, erre nagyon érzékeny a Squid. A méretnél vegyük figyelembe a partíción lévő szabad helyet, ennek a 80-90%-ra érdemes beállítani. Tehát még külön partíció esetén se foglaljuk le a teljes rendelkezésre álló szabad helyet. A Squid egy könyvtárszerkezetet fog létrehozni önmaga számára, amelybe később az objektumokat elhelyezi. Ennek két szintje lesz. Az utolsó két paraméterrel megadhatjuk, hogy hány alkönyvtárat hozzon létre a két szinten.

```
cache_access_log /log/squid/access.log
cache_log /log/squid/cache.log
cache_store_log /log/squid/store.log
```

Itt adjuk meg a log állományok helyét. Soha ne logoljunk arra a partícióra, ahol a cache könyvtár van. A log fájl növekedésére is oda kell figyelni. Ha be van kapcsolva az acces és a store log akkor minden oldalváltás egy teljes sorban tárolódik. Az idén terjedőben lévő Opasoft worm (klienseket fertőző) olyan forgalmat volt képes produkálni, hogy 1 fertőzött kliensnél is percenként 10 Mbyte-al nőhet a log állományok mérete. Ha nem szeretnénk a log állományokat tárolni, akkor adjuk meg paraméterben a /dev/null-t.

```
ftp_user squid@iskola.sulinet.hu
```

Az ftp szerverek vendég bejelentkezéskor jelszó helyett egy e-mail címet kérnek. Itt ezt adjuk meg, hogy a Squid ftp letöltés esetén mit használjon.

## 9.3 Szűrés

A átmenő forgalom és a proxy elérésének szűrését két lépcsőben lehet megadni. Az első lépés, hogy generálunk egy ACL-t. Az ACL-ek, gyakorlatilag, logikai igaz-hamis kimenettel rendelkező feltételek és a következőképpen néznek ki:

```
acl feltétel_neve típus érték
```

A típus sokféle lehet. Igazából az esemény tulajdonságaiból egy paraméter. Paraméterként meg lehet adni stringet és aposztrófban fájlnevet. Például a proxy-t használó számítógépek IP címét szeretnénk meghatározni. Ez a src típus. Az érték ebben az esetben egy IP cím, vagy hálózati cím lehet.

```
acl adminisztratori_gep src 192.168.1.143
```

A fenti meghatározásban, az esemény függvényében, akkor lesz igaz az 'adminisztratori\_gep' acl, ha a kérés a 192.168.1.143 IP című gépről érkezik.

Érdekesebb típusok:

- src. Az oldalt kérő kliens IP címe, vagy hálózatának címe.
- dst. A oldalt tároló szerver IP címe, vagy hálózatának címe.
- dstdom\_regex. Regexp kifejezés keresése az oldalt tároló szerver nevében.
- url\_regex. Regexp kifejezés keresése a kért URL-ben.
- time. A kérés ideje napokban [M|T|W|H|F|A|S] , vagy óra percben [h1:m1-h2:m2].
- port. A lekérés célportja.

A feltételek meghatározása után tudjuk megadni mit is csinálunk vele, illetve mit ne. Tudjuk például szabályozni az elérést (http\_access)

Nézzünk meg egyfajta alapértelmezett beállítást:

```
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl belsohalo src 192.168.0.0/255.255.0.0
acl Safe_ports port 80          # http
acl Safe_ports port 443        # https
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 901        # SWAT
```

```
http_access deny !Safe_ports
http_access allow localhost
http_access allow belsohalo
http_access deny all
```

A fentiek azt írják le, hogy a proxy kiszolgálás szempontjából csak a Safe\_port-ban felsorolt célportokat engedélyezi, valamint csak a belsohalo-ról és a localhost-ról érkező kérést teljesíti, minden mást tilt.

## 9.4 Transzparens üzemmód.

Mint már említettük a transzparens üzemmód esetében a tűzfalat is be kell állítani. Amennyiben Ipchains csomagszűrőt használunk, akkor a következő sort kell elhelyeznünk benne:

```
ipchains -A input -p tcp -s 192.168.0.0/255.255.0.0 -d 0/0 80 -j REDIRECT 3128
```

Ezzel a 192.168.0.0/255.255.0.0 hálózatról érkező, bármilyen cím 80-as portjára irányuló csomagot átküldjük a Squid portjára (3128).

Ugyanez a Iptables esetén :

```
iptables -t nat -A PREROUTING -s 192.168.0.0/255.255.0.0 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

A squid.conf-ba a következő értékeket kell beállítani:

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

## 9.5 Gyakorlat

Állítsuk be a Squid-ot az alábbi adatok szerint és generáljuk le a cache könyvtárat.

- Cache könyvtár helye a telepítésnél erre a célra különválasztott partíció csatolási pontja legyen és a mérete a partíció méretének 90%-a.
- Csak az iskola belső hálózata felé néző hálózati kártyát figyelje a 3129-es porton.
- A memória foglalása (cache jegyzék) a gépben lévő memória nyolcada legyen.
- Engedélyezzük, hogy az iskola belő hálózata használja a proxyt, kivéve egy számítógép IP címét.

## 9.6 Ellenőrzőkérdések a kilencedik fejezethez

1. Milyen célt szolgál a Squid proxy egy hálózaton?
2. Mit jelent a transparens proxy?
3. Milyen előnyei vannak egy proxy lánc üzemelésének?
4. Mi az ICP?
5. Milyen objektumokat nem érdemes proxy-ban tárolni?
6. Mik azok az ACL-ek?
7. Az ACL beállításánál milyen típusokról beszélhetünk?
8. Mit jelent a Cache inicializálás?
9. Milyen előnyei vannak, ha a cache könyvtár külön partíción van?
10. Hol találhatjuk a squid beállításait?
11. Mit jelent a 'http\_port 192.168.1.1:3128' beállítás?
12. Mit jelent a 'Cache\_dir ufs /var/spool/squid 1000 256 256' beállítás?

## 9.7 Felhasznált, ajánlott irodalom

SQUID web cache server, ipchains csomagszűrővel telepítés  
<http://linux.vv.hu/egyebek/halozat/squidip/squidip.htm>

SQUID - egy erőteljes http/ftp proxy program  
<http://linux.vv.hu/egyebek/halozat/squid2/index.html>

# 10. Egyéb szerverek

## 10.1 Xinetd csúcserver

Vannak olyan szolgáltatások, amelyek nem igényelnek folyamatosan futó szerverprogramot. Elég ha a igény esetén elindulnak és csak addig vannak a memóriában, amíg kiszolgálják az adott kérést. Természetesen a kérés érkezését

figyelni kell. Az Xinetd (vagy az inetd) olyan program, ami a számára beállított portokat figyeli, ha kapcsolatkérés érkezik rá, akkor elindítja a porthoz rendelt programot. Manapság azt leginkább a pop3 (levelek letöltése) szolgáltatásnál használják.

Az Xinetd beállító fájlja az /etc/xinetd.conf. Ebben találhatóak a működésével kapcsolatos sorok. Jellemzően a szolgáltatások beállítását külön fájllokba helyezik a /etc/xinet.d könyvtárba (includedir /etc/xinetd.d).

Nézzük meg a pop3 beállításait:

```
service pop3
{
    socket_type = stream
    wait        = no
    user        = root
    server      = /usr/sbin/ipop3d
    log_on_success += USERID
    log_on_failure += USERID
    only_from   = 128.138.193.0 128.138.204.0
    redirect    = 192.168.1.1 23
    bind        = 192.168.1.11
    port        = 901
    protocol    = tcp
    disable     = no
}
```

Ami ebből nekünk lényeges lehet:

- Service (fejlécben): azon szerviz neve, amelyet definiálunk. A portot és a protokollt, ez alapján, a /etc/services állományból állapíthatjuk meg.
- Server: a program neve és elérési útja, amelyet elindít kérés érkezésekor.
- User: a meghívott program milyen felhasználó jogaival fusson.
- Disabled: (yes, no): amennyiben yes van megadva az xinetd nem definiálja a portot, azaz figyelmen kívül hagyja. Ezért a könyvtárban olyan szolgáltatások beállítása is megtalálható, amelyet nem alkalmazunk. A használt szolgáltatásoknál no-t kell az értéknél adni.
- Port: az a port amelyre elfogadjon kérést.
- Protocol: az a protokoll amiben elfogadjon kérést (tcp, udp).
- Bind: az a IP cím amire elfogadja a kérést.
- Redirect: az érkezett kérés továbbdobása a beállított IP-re és portra.
- Only\_from: milyen IP-ről, vagy tartományból fogadjon el kéréseket.

## 10.2 Proftp szerver

Az FTP szerverek biztonságánál nem csak az a probléma, hogy kódolatlanul száguldanak a jelszavak az Interneten. További gondot okoz a régi és bonyolult alapszabvány, amelyet nehéz hibamentesen alkalmazni. Az átlag FTP szerver programokban rengeteg biztonsági hiba található, ezért kerülendő a használatuk.

Ha már feltétlenül FTP szervert kell beüzemelnünk, legalább jól beállítható és viszonylag biztonságos megoldást válasszunk. Ilyennek mondható a Proftpd szerver.

A <http://www.proftpd.org/> címen érhetjük el a program oldalát. Letölteni pedig a következő címről lehet Redhat Linux alá csomagban: <ftp://ftp.proftpd.org/distrib/packages/RPMS/proftpd-1.2.9-1.9.i386.rpm>

A proftpd szerver-nek nagyon jó és könnyen érthető dokumentációja van. Ezen kívül az alap konfigurációs állomány is megfelelő, amely a `/etc/proftpd.conf` néven található. Nézzünk meg egy olyan konfigurációs fájlt, amely speciálisan weboldal ftp feltöltésére készült:

```
ServerName "Szerver neve"           # Szerver neve
ServerType standalone               # külön szerverként fut, nem az inetd hívja meg
Port 21                             # 21-es portot figyeli
Umask 022                           # A fájlok jogosultsági maszkja írásnál.
User nobody                          # Felhasználó jogosultsággal fut
Group nobody                          # Csoport jogosultsággal fut
MaxInstances 30                      # Egyszerre max 30 alprocessz
TimeoutStalled 300                   # Időtűllépés
AllowOverwrite on                    # Felülírást enged
MaxLoginAttempts 2                   # Egy felhasználó egyidőben
MaxClients 50                        # Max engedélyezett kapcsolat
DefaultRoot /var/www                 # Gyökérfájl
# Információs fájl és naplózás beállítása
ScoreboardPath /var/run/proftpd
TransferLog /var/log/ftp/xferlog.legacy
LogFormat default "%h %l %u %t \"%r\" %s %b"
LogFormat auth "%v [%P] %h %t \"%r\" %s"
LogFormat write "%h %l %u %t \"%r\" %s %b"
TransferLog /var/log/ftp/ns2-transfer.log
# A következő felhasználókat engedélyezzük belépésre:
<Limit LOGIN>
    Allowuser admin
    Allowuser webmester
    DenyAll
</Limit>
# Minden /var/www alkönyvtár jogosultságát megadjuk.
<Directory /var/www/html>
    <Limit ALL>
        AllowUser webmester
        AllowUser admin
        DenyAll
    </Limit>
</Directory>
<Directory /var/www/cgi-bin>
    <Limit ALL>
        AllowUser admin
```



```
DenyAll
</Limit>
</Directory>
```

## 10.3 DHCP szerver

A DHCP szerver dinamikus IP cím kiszolgáló, de ennél egy kicsit még több. Ha a klienseinknek nem szeretnénk megadni hálózati adatokat, akkor elég egy DHCP szerver elérést beállítani, onnan az összes hálózati információt képes lesz letölteni. Ennek köszönhetően olyan kliensekkel tudunk dolgozni, amelyek nem rendelkeznek egyedi beállításokkal és egy központi helyről menedzselhető a hálózati beállításuk.

Találkozni fogunk még a BOOTP fogalmával. A BOOTP szerver volt a DHCP elődje. Olyan kliensekhez fejlesztették ki, amelyekben csupán egy hálózati kártya volt (boot eprommal) és nem rendelkezett háttértárral. A BOOTP szerverről töltötték le a hálózati adataikat. Szintén így kaptak információt a szerverről, amelyet háttértárként használnak és az indító fájl helyéről. Ezeket a feladatokat a DHCP szerver is képes elvégezni.

### Beállítás

A beállító állománya a /etc/dhcpd.conf. Nézzük meg a tartalmát:

```
# Ez a beállítás vonatkozik azokra a gépekre, amelyek a 192.168.10.0/255.255.255.0
hálózatra
# kötött kártya felől jelentkeznek.
subnet 192.168.10.0 netmask 255.255.255.0 {
    # A kliensnek kiküldött információk:
    # Alapértelmezett átjáró:
    option routers 192.168.10.1;
    # Hálózati maszk:
    option subnet-mask 255.255.255.0;
    # Domain név:
    option domain-name "iskola.hu";
    # DNS Szerver név:
    option domain-name-servers 192.168.10.1;

    # A kisztható IP címek tartománya
    range dynamic-bootp 192.168.10.100 192.168.10.254;
    # Alapértelmezett lejáratási idő
    default-lease-time 21600;
    # Maximális lejáratási idő
    max-lease-time 43200;
    # Lehetőségünk van rá, hogy bizonyos gépeknek mindig ugyanazt a címet
adjuk.
    # Ebben az esetben a gép hálózati kártyájának fizikai címe alapján történik az
azonosítás. PI:
    host tanar {
        hardware ethernet 00:00:1C:BE:08:42;
```

```
        fixed-address 192.168.10.2;
    }
    host nemtanar {
        hardware ethernet 00:40:95:1c:64:36;
        fixed-address 192.168.10.3;
    }
}
```

Természetesen egy ilyen szervernek több tartományt is meg lehet adni.

## 10.4 DNS szerver

A DNS szerver feladata a domain nevek és az IP címek közötti váltás. Amennyiben Domain név alapján ad vissza IP címet, akkor normál módban dolgozik. Az IP címből domain név megadása a reverse DNS. Ezen kívül még DNS cache üzemmódban szoktak működni.

Zónának nevezzük egy meghatározott hálózat, vagy egy domain adatainak összességét. Kétféle zónát tudunk kezelni. A master-t, a zónában beállított domain szempontjából elsődleges névszerverén. A slave-et pedig a másodlagos névszerveren. Próbálkozzunk meg egy elsődleges zóna beállításával.

A zónákról a következő adatokat állíthatjuk be:

- A kezelni kívánt domain név, vagy IP tartomány (zone).
- Zóna típusa (type). Azt határozza meg, hogy a zóna elsődleges (master) name szerveren található, vagy másodlagoson (slave). A másodlagos zóna tartalmát nem kell kitölteni, azt a DNS az elsődleges szervertől kérdezi le.
- Az adatokat táró fájl neve (file).
- Elsődleges DNS szerver neve vagy címe (master). Ezt csak másodlagos DNS-ként működő zónának lehet megadni.

Egy zónafájlban a bejegyzések többek közt lehetnek:

**"NS" Névszerverek:** A domain elsődleges és másodlagos névszerverét. Az zónában tehát meg kell adni a névszerver hosztnevét .

**"MX" Domain mail szervere:** Az MX rekord szabályozza, hogy a domain névre (valaki@iskola.hu) érkező levelet melyik szerver kapja meg. Többet is felvehetünk belőlük. Ebben az esetben a prioritási érték dönti el hányadik a sorban. A küldő mail szerver először a legkisebb prioritású MX rekordot dolgozza fel, ha arra a szerverre nem tudja valami miatt továbbítani a levelet, akkor továbblép.

**"A" Normál hoszt:** Ezek a normál gépek névfeloldási bejegyzései. A hoszt nevéhez rendeljük az IP címet, amelyet a DNS szerverünknek vissza kell adnia. Természetesen az összes gépet fel kell vennünk, de mindenképpen érdemes a www, mail, ftp bejegyzést beállítani.

**"CN" Álnév:** Amennyiben több bejegyzés mutat ugyanarra a címre, akkor használhatunk aliasokat is. Például a www címre már be lett állítva erre csinálunk egy ftp álnevet.

## Beállítás

A DNS szerver (elterjedtebb nevén, Bind) beállításait a /etc/named.conf fájlban találhatjuk. Az alapbeállítások a options blokkban találhatóak, majd a zónák definiálása következik. Zónának hívunk egy fődomainhoz tartozó adatokat. Nagyon fontos tudnunk, hogy a bind beállító állományában nem lehet # jelet használnia a megjegyzéshez.

```
/* beállítjuk a bind adatkönyvtárának helyét: */
options {
    directory "/var/named";
};
/* Gyökérzóna megadása, ebben az állományban találhatóak a fő nameszerverek: */
zone "." in {
    type hint;
    file "named.root";
};
/* Belső hálózat zónája: */
zone "localhost" in {
    type master;
    file "local/named.local";
};
/* Belső hálózat reverse zónája: */
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "local/db.127.0.0";
};

/* Egy normál zóna definíciója: */
zone "iskola.hu" in {
    type master;
    file "db.iskola.hu";
};

/* Másodlagos nameszerver esetén egy zóna: */
zone "suli.hu" in {
    type slave;
    file "db.suli.hu";
    masters {
        195.199.30.22;
    };
};
```

Nézzünk meg egy zóna fájlt elsődleges name szerveren. (db.iskola.hu)

```
@    IN    SOA    ns1.mienk.hu. admin.mienk.hu. (
```

```
                2002090122      ; Serial
                10800           ; Refresh
                3600            ; Retry
                604800          ; Expire
                86400 )         ; Default TTL

    IN  NS    ns1.mienk.hu.
    IN  NS    ns2.mienk.hu.

iskola.hu.  IN  MX    10 mail.iskola.hu.
www         IN  A     195.36.70.22
mail        IN  A     195.36.70.23
ftp         IN  CNAME www
```

A először megadott SOA rekord a nameszerver nevével kezdődik (ns1.mienk.hu.), majd az adminisztrátori e-mail cím következik (admin.mienk.hu.). A serial kódot minden változtatással módosítanunk kell. Ebből tudja a többi szerver, hogy az adatok módosultak. Az ezt követő számok a frissítési időket jelentik.

Meg kell adnunk a domain két name szerverének nevét (IN NS ns1.mienk.hu.). Mint máshol is az állományban, itt is . zárja le a domain név végét.

Az iskola.hu. domainra érkező leveleket a mail.iskola.hu gépre küldje. Ezt adja meg az MX rekord.

Megadjuk a www.iskola.hu és a mail.iskola.hu gépek IP címét, aztán teszünk egy alias a www.iskola.hu bejegyzésre ftp néven.

A másodlagos name szerveren a zónafájl nem kell létrehozni, mert a named -q paranccsal letölti az elsődleges name szerverről.

A zóna beállításait leellenőrizhetjük a <http://www.nic.hu/regcheck.cgi> oldal segítségével.

Végül két trükkös beállítás.

Bizonyára sokszor lehet követelmény, hogy egy weboldal ne csak a www.valami.hu címre jöjjön be, hanem a valami.hu címre is. Azaz a www-t elhagyva is működjön. Ezt egy sor beiktatásával lehet megoldani:

```
@ IN A 195.36.70.22
```

A @ (kukac) a sor elején mindig a domainra vonatkozó információt határozza meg. Amennyiben ezt a sort beékeljük, a domainnak magának is lesz lekérhető IP címe.

Szintén nem túl gyakran fordul elő, hogy nem szeretnénk DNS szerver szinten bíbelődni, a domain alá tartozó hosztok IP címeinek megadásával, hiszen egy Web szerver kezeli őket. Például a weboldalunk meg van bontva tanar.iskola.hu és diak.iskola.hu oldalakra. Vagy szeretnénk a felhasználóinknak vezeteknev.iskola.hu oldalt biztosítani.

Ebben az esetben is van megoldás. Minden ismert hosztnevet bejegyzünk a zónába. És arra készülve, hogy az összes többi hosztnév ugyanarra az IP címre fog mutatni, kiegészítjük egy sorral:

```
* IN A 195.36.70.22
```

A sor elejére tehát \* (csillag) kerül. Ebben az esetben minden olyan kérésre, aminél a hosztnevet az iskola.hu előtt nem tudja a DNS szerver azonosítani, a csillag sorral jelölt IP címet adja.

## 10.5 Ellenőrző kérdések

1. Mire használjuk elsősorban az Xinetd szerveret?
2. Mit jelent a disable=yes beállítás az Xinetd-nél?
3. Milyen szolgáltatást végez a proftpd szerver?
4. Magyarázd az alábbi proftpd szerver beállítást:

```
<Directory /var/www/cgi-bin>
  <Limit ALL>
    AllowUser admin
    DenyAll
  </Limit>
</Directory>
```
5. Miért lényeges egy belső hálózaton a DHCP szerver?
6. Milyen adatok kaphat a kliens a DHCP szervertől?
7. Mire használjuk a DNS szerveret?
8. Mit hívunk zónának a DNS szerver esetében?
9. Magyarázd az alábbi beállítást dns szerver esetén: `www IN A 195.36.70.22`

## 10.6 Felhasznált, ajánlott irodalom

Bind

<http://linux.vv.hu/egyebek/halozat/bind/bind.html>

DNS - elv és konfiguráció

<http://linux.vv.hu/egyebek/halozat/dns/dns.html>

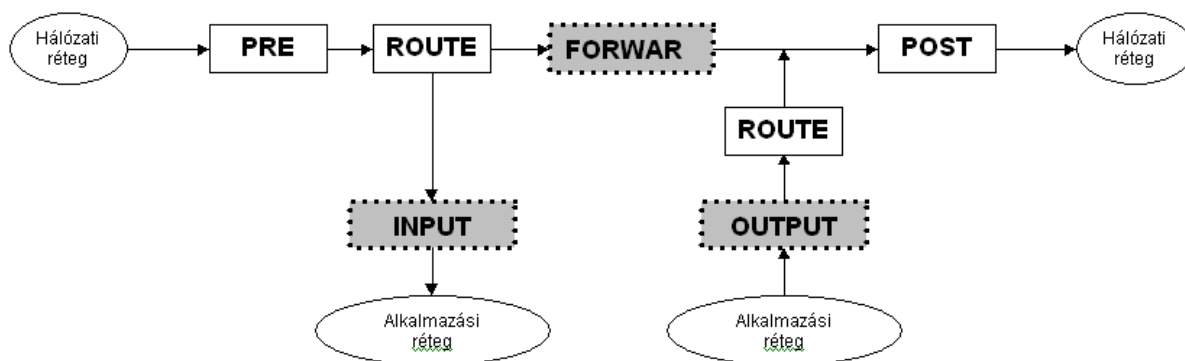
## 11. Csomagszűrés

### 11.1 Alapismertek

A Linux kernelbe beleágyazott csomagszűrő kapott helyet. Ez a csomagokat megvizsgálja a csomagfejléc adatai alapján és egy szűrőfeltétel lista alapján eldönti a sorsát. A csomagszűrő feltételrendszerét egy paranccsal tudjuk kezelni. Az 2.0 kernelnél ez a parancs még a ipfwadm volt, a 2.2 kernelnél az ipchains, manapság a 2.4 kernelnek világában ez a iptables.

Az iptables paranccsal beszúrhatunk és törölhetünk szabályokat a csomagszűrő táblájába. A táblában tárolt adatok viszont újraindításnál elvesznek. Van lehetőség szabályok automatikus felvitelére a gép indulásánál, viszont ez disztribúciónként más és más. Erről később még lesz szó.

Nézzük meg, hogy milyen utakon haladhat egy csomag és milyen csomópontjai lehetnek a csomagszűrésnek. Az itt látható rajz egy vázlatos útvonalat tartalmaz a könnyebb megértés végett.



A vizsgált számítógépre címzett csomagok útja:

1. A csomag beérkezik, átesik egy alapvető ellenőrzésen. Hibás, csonkolt csomagok már itt eldobásra kerülnek. A PRE ponton, ahol az ide vonatkozó bejegyzések alapján módosításra kerülhet (pl.: DNAT ).
2. A ROUTE eldönti, hogy egy csomag a gépnek szól, vagy tovább kell küldeni a hálózat felé. Ha a gépnek szól, akkor az INPUT láncba kerül. Ha nem a gépnek szól és a routing tábla szerint tovább kell küldeni, akkor a FORWARD láncban köt ki.
3. Az INPUT láncra kerülő csomagok egy szűrőlistán haladnak végig, ha elfogadható a csomag, akkor a megfelelő alkalmazáshoz kerül.

A vizsgált számítógépen áthaladó csomagok (routing):

1. A csomag beérkezik, átesik egy alapvető ellenőrzésen. Hibás, csonkolt csomagok már itt eldobásra kerülnek. A PRE ponton, ahol az ide vonatkozó bejegyzések alapján módosításra kerülhet (pl.: DNAT ).
2. A ROUTE eldönti, hogy egy csomag a gépnek szól, vagy tovább kell küldeni a hálózat felé. Ha a gépnek szól, akkor az INPUT láncba kerül. Ha nem a gépnek szól és a routing tábla szerint tovább kell küldeni, akkor a FORWARD láncban köt ki. A továbbküldendő csomagok eldobásra kerülnek, ha a packet forward (gyakorlatilag a routolás) nincs bekapcsolva, engedélyezve.
3. Az FORWARD láncra kerülő csomagok egy szűrőlistán haladnak végig, ha elfogadható a csomag, akkor a továbbhalad a POST felé, ahol az ide vonatkozó bejegyzések alapján módosításra kerülhet (pl.: SNAT ).
4. A csomag kilép a számítógépből.

A vizsgált számítógépből kifelé haladó csomagok:

1. Az alkalmazás elkészíti a csomagot, ami az OUTPUT láncra kerül.

2. Az OUTPUT láncra kerülő csomagok egy szűrőlistán haladnak végig (itt lehetőség van DNAT-ra), ha elfogadható a csomag, akkor a továbbhalad a POST felé, ahol az ide vonatkozó bejegyzések alapján módosításra kerülhet (pl.: SNAT).
3. A csomag kilép a számítógépből.

A fentiek alapján látható, hogy a csomag, az újtától függően, három helyen kerülhet szűrésre. Ezeket a helyeket láncoknak hívjuk, mert egymás után lévő szabályok döntenek el a csomag útját.

Három alapértelmezett lánc létezik:

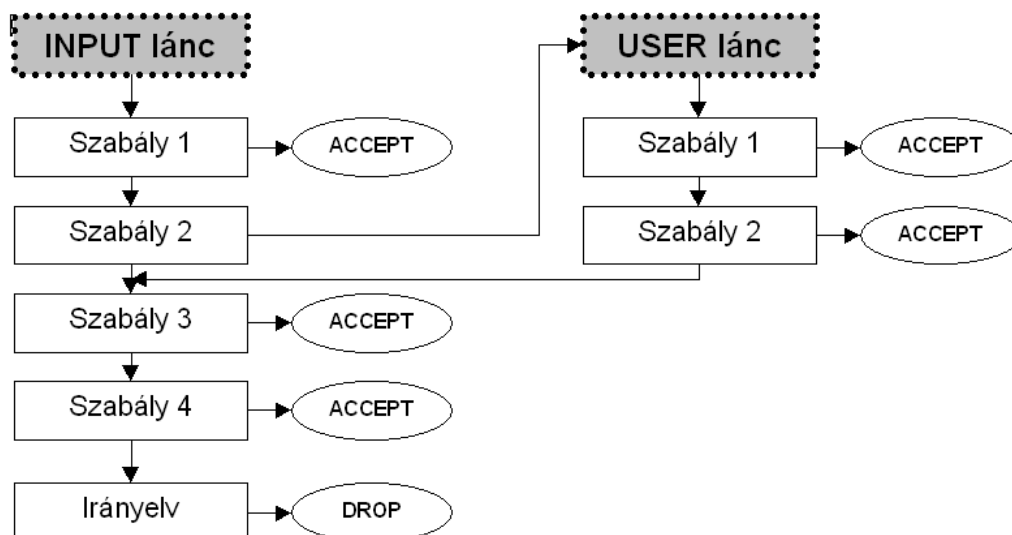
- INPUT lánc, a bejövő csomagok részére.
- OUTPUT lánc, a kimenő csomagok részére.
- FORWARD lánc, az átmenő csomagok részére.

Minden láncnak van egy alapértelmezett szabálya (irányelv), amely akkor érvényesül, ha a lánc szabályai közül egyiknek sem felel meg a csomag. Van rá lehetőség, hogy új láncot hozzunk létre és ezt becsatoljuk valamely alapértelmezett láncba. Ennek akkor lehet értelme, ha a szabályokat a mennyiség miatt, átláthatóbban csoportosítjuk.

A lenti ábrán végighaladva, nézzük meg, hogyan történik ez. Ebben az esetben a vizsgált számítógépre címzett csomagról van szó, tehát az INPUT láncnál kerül vizsgálatra.

- Amennyiben a csomag adatai megegyeznek a szabály 1 feltételeivel, a csomag elfogadásra kerül, tehát bejut az alkalmazás szintre.
- Ha a csomag adatai megfelelnek a szabály 2-ben leírtaknak, akkor a vizsgálat a 'USER lánc' definiált listán halad tovább. A 'USER lánc'-on két szabály van, bármelyikkel egyezést mutat a csomag fejléce, akkor elfogadjuk a csomagot. Egyébként az ellenőrzés az INPUT lánc 3. Szabályánál folytatódik.
- A szabály 3 és a szabály 4 megfelelése esetén a csomag szintén elfogadásra kerül.
- Ha a csomag egyik fentebb vizsgált szabálynak sem felel meg, akkor az INPUT lánc irányelve érvényesül, azaz elutasításra kerül a csomag.

Ha egy csomag valamely szabálynak megfelel, akkor a szabályban meghatározott esemény történik vele és az ellenőrzés nem folytatódik tovább.



A szabályban meghatározott események (célpontok) lehetnek:

- ACCEPT: elfogadjuk a csomagot.
- DROP: eldobjuk a csomagot.
- STOLEN: kiveszi a csomagot a szűrőből.
- QUEUE: sorba állítja a csomagot a felhasználói terület számára.
- REPEAT: megismétli a csomag ellenőrzését az elejétől.
- REDIRECT: Továbbítja a csomagot egy másik portra, esetleg IP-re.
- LOG: naplózza a csomagot.
- REJECT: csomag elutasítása, visszajelzéssel (port unreachable).
- RETURN: A csomag egyből a lánc irányelvéhez kerül további ellenőrzések nélkül.

Most már tudjuk, hogy hol és hogyan történik az ellenőrzés és hogy milyen célpontok lehetnek a feltételek egyezése esetén. Nézzük meg, milyen szűrési feltételeket adhatunk meg:

- **Forráscím meghatározása (-s, --source, --src)**  
A forráscím a csomagot küldő számítógép IP címe. Erre tudunk megfeleltetést írni. Használhatunk konkrét IP címet, de akár hálózati definíciót is. Például:
  - -s 0/0
  - -s 192.168.10.33
  - -s 192.168.1.0/24
  - -s 192.168.0.0/255.255.255.0
- **Célcím meghatározása (-d, --destination, --dst)**  
A célcím a csomag címzettjének IP címe. Erre tudunk megfeleltetést írni. Használhatunk konkrét IP címet, de akár hálózati definíciót is. Például:
  - -d 0/0
  - --dst 192.168.10.33
  - --destination 192.168.1.0/24
- **protokoll meghatározása (-p, --protocol)**  
A csomag gép-gép szintű protokollja. A megfeleltetésnél használhatjuk a protokoll nevét és a kódját is. Például:
  - -p tcp
  - -p 17



- --protocol ICMP
- --protocol UDP
- **Interfész meghatározása**

Két féle meghatározás lehet, az az interfész, melyen a csomag bejön (**-i, --in-interface**), illetve amin kimegy (**-o, --out-interface**). Ebből adódik hogy az INPUT láncon csak bejövő interfész létezhet (-i), az OUTPUT láncon pedig csak kimenő interfész (-o). A FORWARD láncon mindkét tulajdonságot lehet vizsgálni. A szabály nem jelez hibát, ha a szabályban megjelölt interfész nem létezik, de az eredmény nem egyezés. Példák:

  - -i eth0
  - -i ppp0
  - -o eth+
  - -o ppp+

Az interfész sorszámának helyén a '+' jel hatására a feltétel az összes eszköznek, melynek neve a jel előtt álló karaktorsorozattal kezdődik. Azaz a eth+ az összes ethernet hálózati kártyát jelzi.
- **Töredék csomagok meghatározása (-f, --fragment)**

Amikor egy csomag túl nagy ahhoz, hogy egyben elküldésre kerüljön, a csomag töredékekre bontódik és a célba éréskor újra összeillesztődik. Ezzel a gond csak annyi, hogy az első csomagon kívül egyik sem tartalmazza a teljes IP fejléctet. Nem tudjuk megállapítani, hogy milyen gép-gép szintű protokollról van szó. Azaz a töredék csomagok, az első töredéken kívül, nem tudnak illeszkedni a szabályokra. A -f opció alkalmas a töredék csomagok jelzésére. Azaz ha egy szabályban -f van, akkor az csak a fent említett csonkított fejléccel rendelkező (nem első töredék) töredékekre felel meg. A töredék csomagokkal egy szabályban csak az IP címeket vizsgálhatjuk. Például:

  - -f
  - --fragment
  - -f -d 192.168.1.1

A fent említett meghatározások az IP fejlécben található adatokat vizsgálják. A csomagszűrő bővítményeivel azonban a TCP csomagokat fejlécét is vizsgálhatjuk:

- **Forrás port meghatározása (--sport, --source-port)**

A csomag forrásportja. Megfeleléshez használhatjuk a konkrét port számot, vagy a porthoz rendelt szolgáltatás nevét (/etc/services). Például:

  - --sport www
  - --sport 1134
- **Célport meghatározása (--dport, --destination-port)**

A csomag célportja. Megfeleléshez használhatjuk a konkrét port számot, vagy a porthoz rendelt szolgáltatás nevét (/etc/services). Például:

  - --dport www
  - --dport 25
  - --dport 80
  - --dport 110
- **TCP flag-ek meghatározása (--tcp-flags)**

A TCP fejlécben a csomag tulajdonságait meghatározó flag-ek találhatóak, erre tudunk megfeleltetést írni. Először meg kell adni, mely flag-eket szeretnénk vizsgálni (SYN, ACK, FIN, RST, URG, PSH), itt használhatjuk az 'ALL' kifejezést is, ami minden flag-et jelent. Majd meg kell adni, hogy mely

flagek legyen csak bekapcsolva a vizsgáltak közül, itt a 'NONE' kifejezést, amely jól jöhet. Például:

- --tcp-flags SYN,ACT SYN
- --tcp-flags ALL SYN
- --tcp-flags SYN NONE
- --tcp-flags SYN,RST,ACT SYN

- **SYN flag meghatározás (--syn)**

Gyakorlatilag a kapcsolódni vágyó csomagokat tudjuk meghatározni, azaz azokat a csomagokat, melyeknél a SYN flag be van kapcsolva, viszont az ACT és a RST nem.

UDP protokoll esetén is használhatjuk a forrás (--sport) és a célport (--dport) meghatározást, mint a TCP-nél. Az ICMP csomagoknál pedig az ICMP típusát határozhatjuk meg:

- ICMP típusának meghatározása (--icmp-type)  
A meghatározás vizsgálja az ICMP típusát, amelyet a kódjával és a nevével is megadhatunk. Például:
  - --icmp-type host-unreachable

A fent említett megfeleltetéseknel alkalmazhatjuk a negálást is. Ezt egy '!' jel beillesztésével tehetjük meg. Például:

- -i ! eth0
- -p ! UDP
- --sport ! 80

Persze még léteznek meghatározások ezeken kívül is, erről a csomagszűrő HOWTO-ban olvashatunk.

Lassan kezd összeállni a kép. Most tanuljuk meg az iptables parancs használatát. Egy parancs felépítése a következő:

```
iptables <művelet megadása> <lánc neve> <feltételek> <célpont>
```

Műveletek lehetnek a következők:

- Új lánc létrehozása (-N)
- Üres lánc törlése (-X) //alapértelmezett láncokon nem használható
- Irányelv meghatározása (-P) //csak alapértelmezett láncon használható
- Szabályok listázása (-L)
- Szabályok törlése (-F)
- Új szabály hozzáfűzése egy lánchoz (-A)
- Új szabály beszúrása egy láncba, adott helyre (-I)
- Az adott helyen lévő szabály cseréje újra (-R)
- Szabály törlése a láncból (-D)

A parancs használatát a későbbi példákból láthatjuk.

## 11.2 NAT

A NAT a kernel címfordító részéhez tartozó tábla. Fel van bontva további részekre, amelyek különböző helyeken hívódnak meg.

- Connection Tracking (kapcsolat-követés)  
Meghívódik az OUTPUT és a PRE résznél, azaz a csomag rendszerbe kerülésekor. Nem módosítja a csomagokat.
- SNAT (forrás változtatás)  
A csomag forrását változtatja meg. A POST részen hívódik meg.
- DNAT (cél változtatása)  
A csomag célját változtatja meg. A PRE és az OUTPOT részen hívódik meg.

A NAT-nak megvannak a saját célpontjai, minket kifejezetten a privát hálózat IP címeinek módosítása érdekel, hogy a belső hálózatról az Internetre kijussunk. Ez a MASQUERADE célpont. Ahhoz, hogy egy routeren az IP cím fordítás működjön, a packet forward-ot engedélyezni kell és a következő parancsot kell kiadni:

```
iptables -t NAT -A POSTROUTING -j MASQUERADE
```

A zavartalan működéshez még érdemes betölteni a kapcsolódó kernel modulokat.

## 11.3 Példák

### Masquerading

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -j MASQUERADE
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp
```

### Egyszerű tűzfal egykártyás szerverre:

```
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
iptables -A INPUT -i eth1 -d 195.199.1.112 -p tcp --destination-port 22 -j ACCEPT
iptables -A INPUT -i eth1 -d 195.199.1.112 -p tcp --destination-port 25 -j ACCEPT
iptables -A INPUT -i eth1 -d 195.199.1.112 -p tcp --destination-port 110 -j ACCEPT
iptables -A INPUT -i eth1 -d 195.199.1.112 -p tcp --destination-port 80 -j ACCEPT
iptables -A INPUT -i eth1 -d 195.199.1.112 -p tcp --destination-port 443 -j ACCEPT
```

**Syn-flood védelem:**

```
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

**Alattomos portscan elleni védelem:**

```
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
```

**A halál pingje elleni védelem:**

```
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

## 11.4 Ellenőrző kérdések

1. Milyen alapértelmezett láncokat ismersz?
2. Mikor halad végig az INPUT láncon a csomag?
3. Sorold el (címszavakban) milyen feltételeket vizsgálhatunk TCP és IP csomagnál!
4. Mi az a SNAT?
5. Mikor hajtódik végre egy definiált lánc?

## 11.5 Felhasznált, ajánlott irodalom

Linux 2.4 csomagszűrő-HOGYAN (IPtables)

<http://linux.vv.hu/hogyanok/hogyan/IP-tables-HOGYAN/index.html>

Linux IPchains-HOGYAN

<http://linux.vv.hu/hogyanok/hogyan/IPchains-HOGYAN/index.html>

Linux netfilter hacking-HOGYAN

<http://linux.vv.hu/hogyanok/hogyan/Netfilter-hacking-HOGYAN/netfilter-hacking-HOWTO.html>

IP-Masquerade-villám HOGYAN

<http://linux.vv.hu/hogyanok/villam/IP-Masquerade-villam-HOGYAN/IP-masq-lightning.html>

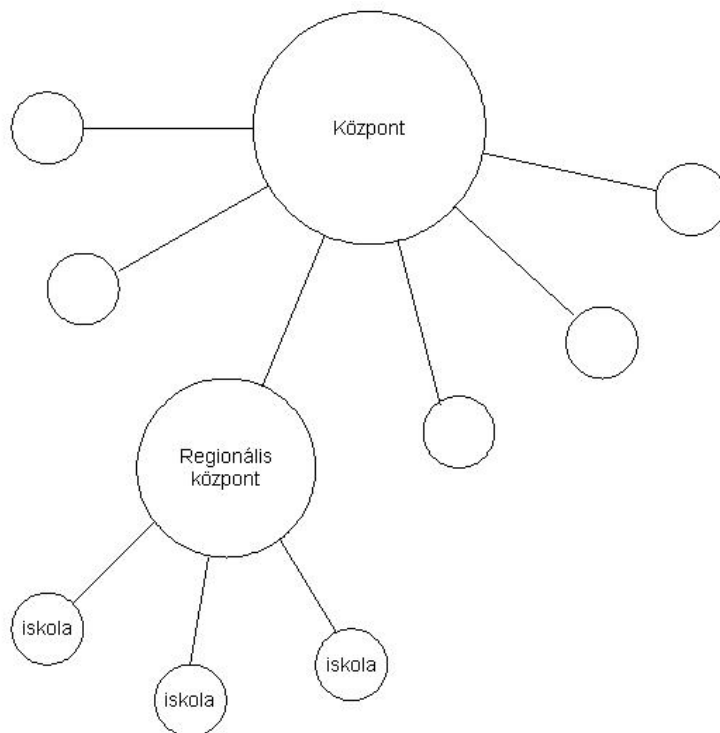
Packet filter firewall megoldások Linuxra

<http://linux.vv.hu/egyebek/halozat/biztonsag/packet-filter-firewall/packet-filter.htm>

### 1. függelék: SuliNet hálózat

A SuliNet hálózati szolgáltatást a PSINet Magyarország Kft. által vezetett konzorcium végzi. A szolgáltatás folyamatos, azaz napi 24 órában működni kell. Amennyiben hibát tapasztal a szolgáltatásban, úgy hívja a HELP-DESK telefonszámát.

Felépítését tekintve a SuliNet hálózat hierarchikus. A Budapesti központ kapcsolódik az Internetre, mind nemzetközi vonallal, mind pedig BIX csatlakozással rendelkezik. Erre csatlakoznak a regionális központok, amelyek az ország különböző területeit szolgálják ki (pl.: Győr, Székesfehérvár, Szeged). A regionális központokra kapcsolódnak az iskolák.

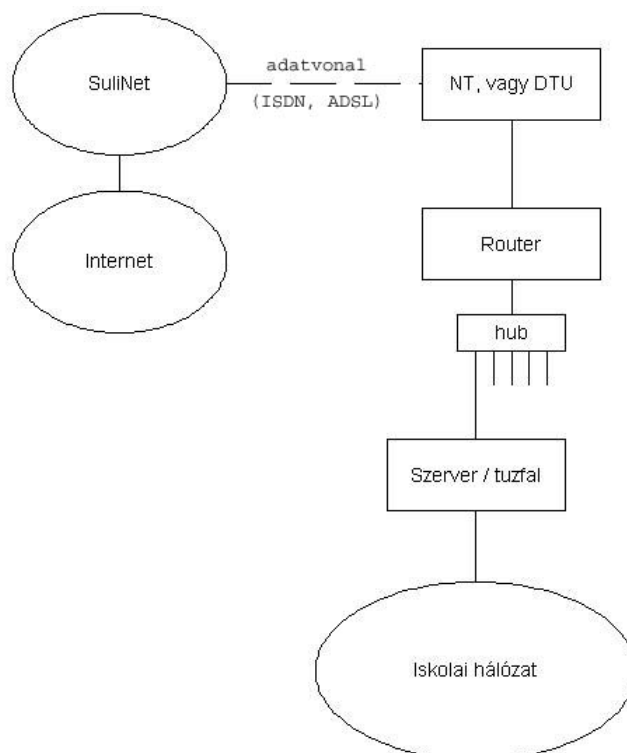


Az iskolák, a regionális központokkal vannak összeköttetésben a helyi lehetőségeknek megfelelő adatvonalon. Ezek lehetnek ISDN, ADSL, bérelt vonal (ritka esetben hagyományos telefonvonal). Erre a vonalra kerül (a SuliNet szekrényben elhelyezett) vonali végberendezés, amely kapcsolódik a SuliNet routerre.

A SuliNet router hálózati (Ethernet) portjára kell csatlakoztatni az iskola publikus IP címekkel rendelkező hálózatát. Ezt a szekrényben elhelyezett HUB segíti elő. Tehát minden olyan gépet, szervert, amely közvetlenül, publikus IP címmel éri el az Internet hálózatot, erre a HUB-ra kell kapcsolnunk.

Mivel 13 db (12+1 szerver) publikus IP, és korlátozott mennyiségű HUB port áll rendelkezésünkre, ezért ide csak a szervereket (esetleg 1 adminisztrációs kliens gépet hiba esetére) szoktuk kapcsolni.

A szerverhez kapott programok segítségével (nem kötelező a szerveren a SuliNet által biztosított program használata) megoldható, hogy a szerver egyik hálózati kártyája az Internet felé néz, míg a másik az iskolában kialakított belső hálózat felé. A belső hálózaton privát IP címeket használhatunk (pl.: 10.0.0.1, 192.168.0.1), de ez nem alkalmas közvetlen az Interneten való kommunikációra. A szerverre hárul a feladat az iskola belső hálózata és az Internet közötti kapcsolat megteremtésére, a címek fordítására. Ezt NAT-nak, vagy masquerading-nak nevezzük.



Ebben az esetben az iskola belső hálózata egy privát IP címekkel rendelkező önállóan működőképes hálózat lehet, amelyre az intézmény összes gépét lehet csatlakoztatni. Internet használat esetén, a szerveren keresztül kommunikálnak, a szerver külső IP címét felhasználva.

Ebben az esetben az iskolai hálózat egy alapvédeltséget élvez az Internet felől, amelyet a szerveren elhelyezett tűzfal segítségével növelhetünk.

A hálózat kialakításához az iskola egy domain nevet és 16 címet tartalmazó IP tartományt kapott használatra.

### IP tartomány

Az iskola által használható IP címekről a Sulinet adatlapból (Üzemeltetési paraméterek táblázata) kaphatunk némi információt (1,2,3,9 sorok). Sajnos az adatlap nem tartalmazza konkrétan a szükséges adatokat. Nézzünk egy példát:

1.	Munkaállomások számára allokalált címtartomány:	195.199.16.145- 195.199.16.157
2.	A hozzá tartozó netmaszk:	255.255.255.240
3.	A tartományból a router számára már felhasznált IP cím:	195.199.16.158
9.	Az intézményi szerver javasolt címe és kezdetben megadott domain neve:	195.199.16.157 server.isk-varos.sulinet.hu

Ezeknél az adatoknál nekünk azért többre lenne szükségünk. Meg kell határoznunk a hálózati címet és a broadcast címet is. Mivel a router a legutolsó használható IP címet szokta kapni ezért induljunk ki ebből az adatból.

- 255.255.255.240-es hálózati maszk annyit tesz, hogy a hálózatban 16 IP cím szerepel (256-240).
- A router címe a legutolsó alkalmazható IP cím. Utána következik a broadcast cím. Tehát:  
Broadcast = Router cím+1 = 195.199.16.158 + 1 = 195.199.16.159
- A hálózati cím mindig a tartomány legelső címe. Tehát:  
Hálózati cím = broadcast – 16 + 1 = 195.199.16.159 – 16 + 1 = 195.199.16.144

Tehát a hálózatot a következőképpen tudjuk meghatározni:

- Hálózati cím: 195.199.16.144
- Hálózati maszk: 255.255.255.240
- Broadcast cím: 195.199.16.159
- Átjáró: 195.199.16.158

## Domain

Minden iskolának bejegyeznek egy SuliNet-es aldomaint. Alapértelmezésben ez iskola-varos.sulinet.hu formátumú. Az aldomain alá, a hosztokat is regisztrálják. A fenti IP példa alapján ez a következő lehet:

pc1.iskola-varos.sulinet.hu	195.199.16.145
pc2.iskola-varos.sulinet.hu	195.199.16.146
pc3.iskola-varos.sulinet.hu	195.199.16.147
pc4.iskola-varos.sulinet.hu	195.199.16.148
pc5.iskola-varos.sulinet.hu	195.199.16.149
pc6.iskola-varos.sulinet.hu	195.199.16.150
pc7.iskola-varos.sulinet.hu	195.199.16.151
pc8.iskola-varos.sulinet.hu	195.199.16.152
pc9.iskola-varos.sulinet.hu	195.199.16.153
pc10.iskola-varos.sulinet.hu	195.199.16.154
pc11.iskola-varos.sulinet.hu	195.199.16.155
pc12.iskola-varos.sulinet.hu	195.199.16.156
server.iskola-varos.sulinet.hu	195.199.16.157
router.iskola-varos.sulinet.hu	195.199.16.158

A szerver gép ezek szerint a server.iskola-varos.sulinet.hu címmel rendelkezik. Mivel a szerveren különböző szolgáltatások futnak, ezért alisaok (álnevek) vannak bejegyezve rá:

mail.iskola-varos.sulinet.hu	server.iskola-varos.sulinet.hu
www.iskola-varos.sulinet.hu	server.iskola-varos.sulinet.hu
ftp.iskola-varos.sulinet.hu	server.iskola-varos.sulinet.hu

Ezek alapján a szerver mind a négy névre hallgatni fog. Van lehetőség az iskolában e-mail szerver kialakítására. A iskola címei 'munkatars@iskola-varos.sulinet.hu' formátumúak lehetnek. Ahogy látszik az e-mail nem konkrét gép, hanem az iskola domainjára van címezve. Hogy a leveleket mégis a megfelelő gép kapja meg, a DNS szerverben, úgynevezett, MX rekordot kell beállítani:

iskola-varos.sulinet.hu preference = 60, mail exchanger = mail.core.sulinet.hu  
iskola-varos.sulinet.hu preference = 50, mail exchanger = mail.szfv.sulinet.hu  
iskola-varos.sulinet.hu preference = 10, mail exchanger = server.iskola-  
varos.sulinet.hu

Az MX rekordnál több gép is meg van adva. Ezeket egy 'preference' sorszámmal látják el. Amikor a levél kézbesítésre kerül, akkor a küldő gép először a legkisebb sorszámmal rendelkező szerverre próbálja meg eljuttatni. Amennyiben ez nem elérhető, úgy a következővel próbálkozik. A magasabb sorszámú szerverek úgy vannak beállítva, hogy fogadják a leveleket és folyamatosan próbálkozzanak a legkisebb sorszámú szerverre való juttatásával.

### **SuliNet által biztosított szolgáltató szerverek**

Minden regionális központban található regionális szerver. Ez a következő szolgáltatásokat biztosítja:

- Domain Name Server  
Az iskolához legközelebb lévő DNS szerver. Ha az iskolának nincs saját DNS cache szervere, akkor ezt a szervert érdemes beállítani a klienseken, mint névfeloldó szerver.
- Proxy szerver  
Az iskolához legközelebb lévő proxy (FTP, Gopher, HTTP). Nem kötelező használni, de jelentős sebességnövekedést is elérhetünk.
- News szerver
- POP3 és SMTP szerver  
Minden iskolának létrehoznak egy adminisztrációs postafiókot a regionális szerveren. Ez elsősorban a SuliNet üzemeltetés és az iskola közötti kommunikációt szolgálja, de más célokra is használható. A levelek letöltéséhez szükséges POP3 és levelek küldéséhez szükséges SMTP szolgáltatást is a regionális szerver végzi.

A SuliNet központ is szolgáltat DNS és proxy elérést a core.sulinet.hu szerveren.

### **Segítség a munkához**

Ezen dokumentum megírása a <http://support.sulinet.hu> oldal anyagai és az üzemeltetési útmutató (<http://www.sulinet.hu/info/uzemeltetes/>) felhasználásával készült.

Ajánlott levelezési listák:

- TechInfo (<http://lista.sulinet.hu>)  
SuliNettel kapcsolatos kérdések, problémák, észrevételek.
- 1let (<https://www.1let.hu/mailman/listinfo/forum>)  
Közoktatási Rendszergazda Egylet ([www.1let.hu](http://www.1let.hu)) levelezési listája.
- SuliNetware (<http://www.snw.info.hu/INTRANWL/index.htm>)  
IntranetWare iskolai telepítési és működtetési tapasztalataival kapcsolatos levelezés.



- Sulinux (<http://server.wesselenyi-bp.sulinet.hu/mailman/listinfo/sulinux/>)  
Iskolák linuxos listája.
- TechNetKlub (<https://www.technetklub.hu/Technetklubportal/faq.htm>)

#### Ajánlott weboldalak:

- root.hu számítástechnikai magazin  
<http://www.root.hu>
- Linux-felhasználók Magyarországi Egyesülete által üzemeltetett Linuxos híroldal.  
<http://www.linux.hu>
- Hungarian Unix Portal  
<http://portal.fsn.hu/>
- Magyar BSD egyesület oldala  
<http://www.bsd.hu>
- Tech.Net magazin MSHU oldalai  
[http://www.microsoft.com/hun/technet/default.asp?MSCOMTB=ICP\\_MSHUN|%20Tech.Net%20magazin](http://www.microsoft.com/hun/technet/default.asp?MSCOMTB=ICP_MSHUN|%20Tech.Net%20magazin)
- SuliNetWare oldala  
<http://www.snw.info.hu/>
- Sulinet support oldal  
<http://support.sulinet.hu>
- Közoktatási Rendszergazda Egylet oldala  
<http://www.1let.hu>