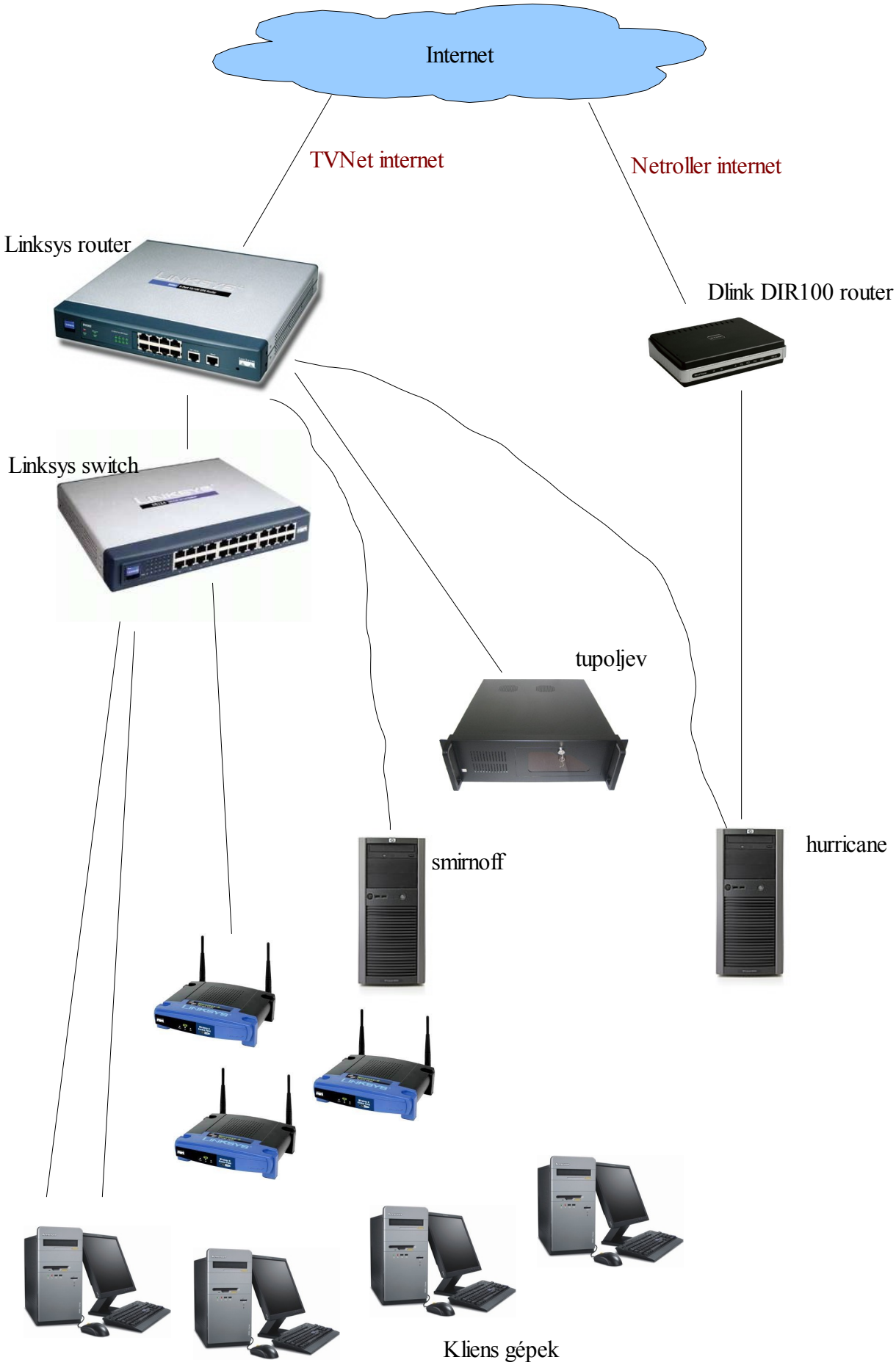
# IT Rendszer dokumentáció
# (nem teljes)

# A hálózat


Internet
TVNet internet
Netroller internet
Linksys router
Dlink DIR100 router
Linksys switch
tupoljev
smirnoff
hurricane
Kliens gépek

| | | |
|---|---|---|
| **TVNet**: | 85.238.91.201 (website.dyndns.org) | |
| **Netroller**: | 195.70.46.13 (**sirus.infomap.ws**, website2.dyndns.org) | |
| **Dlink DIR-100**: | 10.1.10.1 | |
| **Hurricane**: | 10.1.10.100 | |
| | 192.168.1.125 | |
| **Linksys router**: | 192.168.1.1 | |
| **Linksys switch**: | 192.168.1.50 | |
| **Linksys Wireless Access Point-ok**: | | 192.168.1.220 |
| | | 192.168.1.230 (elsődleges AP) |
| | | 192.168.1.240 |
| **Smirnoff**: | 192.168.1.100 | |
| **Tupoljev**: | 192.168.1.150 | |

**A kliens gépek** nevei a jövőben *machine01...12* illetve továbbiakra lett tervezve, az esetleges gépcserék és avval járó „névváltoztatás-kavarodás" kivédése képpen. Jelenleg a felhasználó neve a gépneve is, illetve valamilyen módosulata. Jelenleg a DHCP szerver is a felhasználó nevében osztja ki a hostnevet, amit ugyebár a Windows nem vesz figyelembe.. De a DHCP „névkiosztásának" átállítása is természetesen folyamatosan kell történjen.

*A képen nem látszó, további fontosabb hálózati eszközök:*
**Konica Minolta C250**: 192.168.1.200 (website)
**Konica Minolta C205**: 192.168.1.190 (contactual)
**HP 3015**-ös nyomtató/fax-ot kiszolgáló printerszerver: 192.168.1.203
**Berija (riasztó admin gép)**: 192.168.1.120
A többi fontos IP cím és név a hurricane szerver dhcpd.conf fájljából kideríthető.

*A szerverek távoli (internet felőli) elérései* is lehetségesek, a
Hurricane: 3126
Tupoljev: 3124
Smirnoff: 3122
portok segítségével.
Természetesen a **direkt root login tiltva** van, így csak az engedélyezett felhasználók léphetnek be, majd a root jelszó ismeretében egy su-val rendszergazdai módba válthatnak.

*A hurricane-on „futó" levelezés is elérhető az internet felől*. Egyelőre titkosítás nélkül, az 5143-as IMAP porton keresztül. (Budawest levelezéshez volt rá szükség)

*A biztonsági kamerá*k képe IE alól szintén ellenőrizhetők. Ehhez a 7000-es portot kell használni.

## Internet:

Két internet előfizetés aktív jelenleg. Az egyik a TVNet-é, a másik a Netroller-é. Mindkét internet előfizetés statikus IP-vel rendelkezik.
TVNet: 85.238.91.201 (website.dyndns.org)
Netroller: 195.70.46.13 (**sirus.infomap.ws**, website2.dyndns.org)
A TVNet elméletileg 16M/512k.
A Netroller sebessége 4/4Mbit.
A számítógépek alapértelmezetten a Tvnet-es kapcsolaton kommunikálnak, de a \\tupoljev\system alatt található 2 windows-os scriptel átállíthatók, hogy egy-egy nagyobb feltöltés alkalmával a Netroller-es internetet használják.
A „set_fastupload_routing.bat" beállítja a netroller-es kapcsolatot, a „set_normal_routing.bat" pedig visszaállítja a tvnet-es kapcsolatot.
(A netroller-es kapcsolat esetén az átjáró a hurricane szerver)

## Dlink DIR100:

A netroller által adott egyszerű router, ami kompatibilis a pppoe protokoljukkal. (Se a linksys, sem a linux nem tudott kapcsolódni a szolgáltatóhoz egyébként).
A router IP címe: 10.1.10.1
A routeren jó néhány port forward is be van állítva, hogy bármelyik szolgáltatás, bármelyik internetkapcsolat segítségével elérhető legyen.
A router beállító felülete elérhető, ha a hurricane-t választjuk átjárónak és a böngészőbe beírjuk a DLink router IP címét.

## Hurricane:

A hálózat
Net-megosztó (netroller)
Tűzfal (Port forwardolások)
DHCP
DNS (named)
Levelező (Postfix, dovecot /IMAP,Pop3/ )
szervere.
A „külső" hálózati kártyája a Dlink routerel kommunikál (10.1.10.100), míg a belső (192.168.1.125) értelemszerűen a linksys router illetve switch segítségével a lokális hálózattal.
A gép Slackware 11.0 rendszerrel fut.

## Tupoljev:

A hálózat Samba szervere (PDC = elsődleges domain kontrollere). Ezen a gépen tárolódnak a felhasználók samba jelszavai, elsődleges home könyvtárai, illetve a megosztások.
A gép egy 64bit-es Debian Ethc-el fut.

## Smirnoff:

A website fejlesztői szervere. Ez a szerver a hálózat
Web (apache+php)
Adatbázis (MySQL, másodsorban postgres)
Samba (fejlesztői megosztások)
szervere.
Ez a szerver úgy lett kialakítva, hogy az interneten futó website-os éles szerverekhez minél jobban hasonlítson. Apache, PHP, mysql verziók követése, stb, hogy az oldal feltöltése és „élesbe állítása" minél kevésbé legyen körülményes.
A telepített rendszere egy Debian Etch.

## Linksys Router:

A TVNet internet-et megosztó router.
IP címe: 192.168.1.1
Elméletileg 2 internet kapcsolatot is képes kezelni, de a sorozatos problémái miatt, a fentebb látható hálózati topológia hatékonyabbnak bizonyult.
Ezen a routeren is szintén jó pár port forward szabály van beállítva, hogy a belső szolgáltatások ezen a routeren keresztül is elérhetők legyenek.

## Linksys switch:

Csak működik (szerencsére) :)

## Linksys Access Point-ok:

Az iroda Wireless hálózattal való teljes lefedettségért felelősek.
IP címeik: 192.168.1.220
192.168.1.230 (elsődleges AP)
192.168.1.240
Nincs különösebb korlátozás (pl: MAC cím tiltás) beállítva rajtuk. Egyszerűen csak a wireless hozzáféréshez szükséges jelszót ismerőnek „osztják” az internet-et.
Az SSID-t (hálózat neve) szórását több kompatibilitási probléma miatt, egyszerűbbnek találtuk bekapcsolni, illetve az eredeti jelszavukat módosítani.
**SSID: hawkeye**

# A szerverek

# **Hurricane**:

Részemről az egyik legmegbízhatóbbnak tartott és legkönyebben konfigurálható operációs rendszerrel, a Slackware linux 11.0-s verziójával lett telepítve a gép.
A gép Intel Celeron 1.7Ghz-es CPU-val, ~788Mb RAM-al, egy 80Gb-os rendszer, és 2x110Gb-os HDD-vel (RAID tömbben) rendszelkezik.

A root felhasználó könyvtárában, a scripts alkönyvtárában található néhány a gép feladatához szükséges script.

Az **internet meosztás**ához is az egyik ilyen scriptet használja. Pontosabban a */root/scripts/firewall_rules* fájlt. Ebben a fájlban szimplán csak be vannak írva azok a parancsok, amikkel a netosztást, tűzfal beállítása történik. Ez a fájlt bootoláskor a /etc/rc.d/rc.local fájl segítségével fut le.
Ha valami probléma lenne a tűzfallal, vagy véletlen elállítottuk akkor két lehetőségünk van:

1. újraindítjuk a gépet
2. kiadjuk az *iptables -F; iptables -F -t nat; bash /root/scripts/firewall_rules* parancsot, amivel a tűzfalszabályok újra beállítódnak.

A **DHCP szolgáltatás**t a /etc/dhcpd.conf fájlal alatt tudjuk rajta beállítani. Beállítás vagy módosítás után az új beállításokat a folyamat kilövésével (pl: ps ax | grep -i dhcpd | kill -9 `awk '{print $1}'` ) tudjuk érvényesíteni.
Bootoláskor a szolgáltatás szintén a /etc/rc.d/rc.local fájl segítségével indul el.

A **DNS szolgáltatás**t a /etc/named.conf, illetve a fel/vissza-oldandó neveket a /var/named/website könyvtáron belül található fájlok segítségével állíthatjuk.
A szolgáltatás elindulásáért szintén a /etc/rc.d/rc.local fájl felelős.

A DHCP és (belső) DNS szolgáltatás erősen összefügg, ezért az egyikben történt változások befolyásolják a másik müködését is. Gondolva itt a számítógépek neveire. (Értelemszerűen)
Pl: ha a DHCP-ben megváltozik egy gép neve, akkor annak a nevét a DNS szerver configjában is át kell írni, különben nem lesz helyes a visszafejtés, elérés.

A **levelezés** (levelek továbbítása) az egyszerűen hangolható ***postfix*** programmal történik. A beállítását a /etc/postfix könyvtáron belül található fájlokkal végezhetjük. A fő beállításokért értelemszerűen a main.cf fájl a felelős.
A levelezés kiszolgálása, amelyik kliens esetén az szükséges, ***dovecot*** programmal történik. Beállítását a /etc/dovecot.conf fájl segítségével végezhetjük. Pop3 és IMAP szolgáltatásokra van beállítva jelenleg. Mivel a tűzfalakona pop3 nincs engedélyezve, ezért természetesen a pop3 csak a hálózaton belül használható. A külső IMAP elérés engedélyezve van az otthoni levelezés miatt az 5143-as porton.

A hurricane-ra beállított felhasználók levelezése a saját home könyvtárukba, egy kis trükk segítségével pedig a RAID tömbre (/dev/md0) mentődik, hogy biztonsági másolat is legyen belőlle. A könnyebb átláthatóság kevéért a /home könyvtár egy-egy alkönyvtára linkel át a /dev/md0/mail könyvtár megfelelő bejegyzésére.

**Például:**
Egy info usernevű felhasználó szeretne Maildir segítségével levelezni.
*user*: info
*alapértelmezett home könyvtár*: /home/info
a user account elkészítése:
*useradd -g users -d /home/info -s /bin/false -m info*
# -g users = csoport neve
# -s az alapértelmezett parancsvégrehajtója, ami biztonsági okoból a /bin/false,

# hogy ne lehessen a user nevében belépni a gépre
# természetesen aki távolról is el akarja érni a gépet (ssh login), annak ez /bin/bash
*mailto info*
# küldeni kell egy levelet az info usernek, hogy a postfix elkészítse a Maildir könyvtárat
# a teszt levelet a ctrl-d-vel küldhetjük el
*mv /home/info /mnt/md0/mail/info; ln -s /mnt/md0/mail/info /home/info*
# a home könyvtár áthelyezése, így talán áttekinthetöbb hosszú távon

Ezután következhet a levelzésének beállítása. A skel segítségével az alap levél letöltő script már a helyén van. Így csak az alábbiakat kell végrehajtani, hogy az „új felhasználó" levelezését a hurricane szerver tárolja.
Mivel a user felvételekor a shell-t /bin/false-ra lett állítva, ezért a su felhasználónév nem müködik.
Tehát root jogokkal:
cd /home/info
cd .getmail
cp -f getmailrc_orig getmailrc-info_levelezese
# itt a getmailrc- névkezdet fontos, mert a getmail_script ezt keresi!
# utána viszont bármi állhat
mcedit getmailrc-info_levelezese
# és be kell állítani a megfelelő usernevet és jelszót
# pl: username = infouser
chown info.users *
# állítsuk be a jogosultságot a fájlokhoz
crontab -e -u info
# szerkesszük a user crontabját, hogy töltögesse a leveleket bizonyos időközönként
# és egy insert megnyomása után (nagy valószínűséggel egy vi editort kapunk) írjuk be az alábbit
*/5 * * * * ~/.getmail/getmail_script
# az 5-ös jelenti a 5 percenként való leszedést. Túl kevésre nem érdemes állítani, mert ha
# nagyméretű a levél...
# egy ESC :wq beütése után mentsük a módosítást és kész is vagyunk.

Ezután beállíthatjuk az új felhasználónak a levelezését a kliens gépen, ahol a hurricane-on lévő felhasználó nevét és jelszavát kell használni!

Egy másik script (/root/scripts/home_backup) segítségével ezek a levelek nemcsak a tükrözött RAID tömbön tárolódnak, hanem pár napra visszamenőleg (scriptben állítható) egy megadott könyvtárba is készül róluk biztonsági másolat.

# Tupoljev:

A hálózat opensource domain controllere. A fő samba kiszolgáló. Mint már említett, ezen a gépen tárolódnak a felhasználók adatai, jelszavai, és ehhez a szerverhez fordul a smirnoff gép is az authentikáció hitelesítéséért.

A gép egy AMD 64bit 3200+ (2,2Ghz) processzorral, 2Gb RAM-al, 80Gb-os és 2x300Gb többfelé particinált RAID0-s és 2db 300Gb-os, szintén több particióra osztott, különböző megosztásokhoz használt HDD-kel rendelkezik. (Érdemes majd újra felosztani a vinyókat, mert nagy a katyvasz..)

Mivel a gépen egy 64bit-es debian rendszer fut, ezért előfordul, hogy bizonyos programok, csomagok hibásak. Emiatt például a metamail-el sem tudtam rendesen levelet küldeni a szerver illetve backup állapotáról.A jövőben ezért érdemes lenne a gép leváltásáról vagy a linux disztribúció lecserélésén elgondolkodni.

A Samba megosztásokat, mint ismeretes a /etc/samba/smb.conf fájlban lehet managelni. Módosítások után viszont a /etc/init.d/samba restart paranccsal érdemes a szolgáltatást újraindítani.

Az azonosításhoz szükség van a számítógépnév felvételére is, mint egy linux, illetve samba user a gépre. Ennek megkönnyítése érdekében a /root/scripts könyvtár alatt található egy *add_machine_to_samba* és egy *add_user_to_samba* script, ami ezen felviteleket könnyíti meg. Mivel a hálózatban sajnos mindenki rendszergazdai jogosultsággal dolgozik a gépén, ezért egy csavart is be kell iktatni a felhasználó fevételébe. Pontosabban, hogy először a szerveren rendszergazdai (smbadmins) csoport tagjaiként kell felvenni a linuxba, majd közvetlen ezután felvenni a samba-ba, majd a végén a megfelelő csoport tagsággal érdemes, biztonsági szempontok miatt is visszaminősíteni.
(A scriptekből kivehetőek a megfelelő parancsok.)

**Példa:**
*tesztgep nevű számítógép felvétele:*
useradd -g users -G smbmachine -s /bin/false tesztgep$
smbpasswd -a -n -m tesztgep$
*script segítségével (ha jól müködik):*
/root/add_machine_to_samba tesztgep

*tesztuser nevű felhasználó felvétele:*
useradd -d /home/tesztuser -g smbadmins -m -s /bin/false tesztuser
smbpasswd -a tesztuser
usermod -g users -G contactual,website tesztuser

Az olyan megosztásokat, amikhez mindenkinek mindig hozzá kell férnie (pl: telepítő programok) érdemes nobody.nogroup jogosultsággal felvenni. (és esetleg 666-os fájl írási jogosultságot illetve 777-es könyvtár létrehozási jogosultságot „kierőszakolni”) Illetve az egész jogosultságrendszert jól átgondolni, hogy a közös dokumentumokkal kapcsolatban ne legyen jogosultsági probléma. Olyasmi problémák elkerülése végett, mikor az egyik felhasználó feltölti a dokumentumot, de a másik beleolvasni se tud, vagy esetleg módosítani se tudja.
Ilyen megosztásokon érdemes kikényszeríteni egy olyan user/csoport jogot, aminek mindenki a tagja.

A KonicaMinolta scannerek megosztásai is hasonló módon működnek, rá van „erőszakolva” a nobody.nogroup felhasználó jogosultsága.
Mindegyikhez van egy-egy megosztás rendelve (contactualscanner, websitescanner, budawestscanner), amit a felhasználó viszont nem lát, mert helyette a saját mappájában találja a scanner mappákat. Ezek a mappák a linux fájlrendszerén linkelve vannak.
Sajnos ez a Konica-k működési „zavara” miatt szükséges, mert nem mindig tudnak menteni jelszóval rendelkező megosztásba.

# Smirnoff:

A gép egy 2Ghz-es Celeron CPU-val, kb 766MB RAM-al, 1db 80Gb-os rendszer, 1db 120Gb-os és 2x300Gb-os HDD-vel rendelkezik. Ez utóbbi(ak) 3 felé vannak particionálva, 3 különböző RAID tömbbe fűzve. Ebből az egyik tömb a /home könyvtáré, a többi klönböző megosztásoké.

A gép php fejlesztői szerver, néhány megosztással, amik a munkákhoz szükségesek. Egy www megosztás, amibe a webfejlesztők dolgoznak, illetve mindenkinek a home megosztása, amibe szintén pár fontos dokumentumot, illetve fejlesztés alatt lévő oldalakat lehet tárolni. Ez utóbbiakat szintén el lehet érni apache alias-ok segítségével a böngészőből.
A megosztásaihoz való felhasználói authentikációt a tupoljev nevű szerver végzi, azaz tőle kérdezi le a user nevet és jelszó párost.

A samba www megosztása szintén „kierőszakolás" -al működik. Az apache által használt www-data felhasználó és csoport jogosultságot húzza rá egy-egy fájlra illetve könyvtárra a felmásolás során. Illetve a 660 jogosultságot új fájlnál, és 770-t új könyvtár esetén.
Ez a belső hálózat esetén jól működik. Az internet felől való eléréskor (pl: winscp-vel) azonban van egy kényelmetlensége. Az, hogy fájlt nem lehet módosítani, csak ha elötte letöröljük és utána felmásoljuk a módosítottat.
Természetesen ezt csak az a személy teheti meg, akinek a linuxos felhasználója tagja a www-data csoportnak.
Mivel azonban nem az elsődleges csoportja a felhasználónak a www-data, ezért a fájl felmásolása után a felhasznalonev.users lesz a fájl tulajdonosa. Ezt orvoslandó óránként lefut egy script, ami a /var/www könyvtár teljes tartalmára beállítja a www-data tulajdonost.
Ez a script a szokásos /root/scripts könyvtár alatt található www_chown néven.

A gépen az apache már megszokott debian-os módosulata található. A beállítása az interneten viszonylag jól van dokumentálva, ezért nem is tárgyalom tovább.
A php.ini a /etc/php5/apache2/php.ini alatt található, illetve a php4-es ini szintén hasonló útvonalon.

A mysql adatbázisok helye szerencsére a szokásos útvonalon, azaz a /var/lib/mysql alatt található.

*tesztuser nevű felhasználó felvétele:*
*useradd tesztuser*
utána egyértelmű paraméterek megadásával létre lehet hozni a felhasználót.

# Fontosabb nyomtatók telepítése

# HP 3015 (Edimax printer szerveres) nyomtató:

Sajnos az Edimax nyomtatószerverre kötött nyomatók csak speciális Edimax-os driverrel válnak rendesen elérhetővé és használhatóvá. (legalábbis ennél a típusnál).

Ez a driver a \\tupoljev\system\drivers\Edimax_printerserver alatt található.
Az autorun.exe-vel indítható, a felbukkanó ablakban pedig a Client Utility-t kell választani. Majd rá kell kattintani az „English version” szövegre és máris mehet a next-next-next-es telepítés, aminek a végén a hálózatban autmatikusan fel is térképezi az elérhető nyomtató-szervereket.
A következő lépés a printerserverre csatlakoztatott nyomtató feltelepítése.
A Vezérlőpult -> nyomtatók és faxok pontja alatt a nyomtató hozzáadás-ával ezt meg is tehetjük.
Válasszuk a Számítógéphez csatlakoztatott helyi nyomtatót, és a Plug and Play.... elől vegyük ki a pipát!
A „következő port használata”-nál válasszuk ki a megfelelő port-ot, amire a nyomtató van bedugva. (Pscb6c80-P2; P1 - LPT, P2 - USB, P3 – USB)
Ha van saját lemezünk (jobb ha van) tallózzuk be, majd folytassuk értelemszerűen a telepítést.

Pillanatnyilag a nyomtató a P2-es USB-s portba van dugva. Ide is érdemes csatlakoztatni, hisz a gépekre már ez a port van beállítva, ergó ha másikba csatlakoztatjuk nem fog tudni a gép nyomtatni.

Ha bármilyen gond lenne, vagy a nyomtató megosztásának módosítása szükséges, akkor az Edimax printerserver-t a 192.168.1.203-as IP címen érhetjük el.
Értelemszerűen a Printer Status pont alatt tudjuk ellenőrizni, a nyomtató helyes csatlakozását.
A beállításokat érdekesen a Setup Wizard alatt lehet módosítani.

# HP 2550 nyomtató:

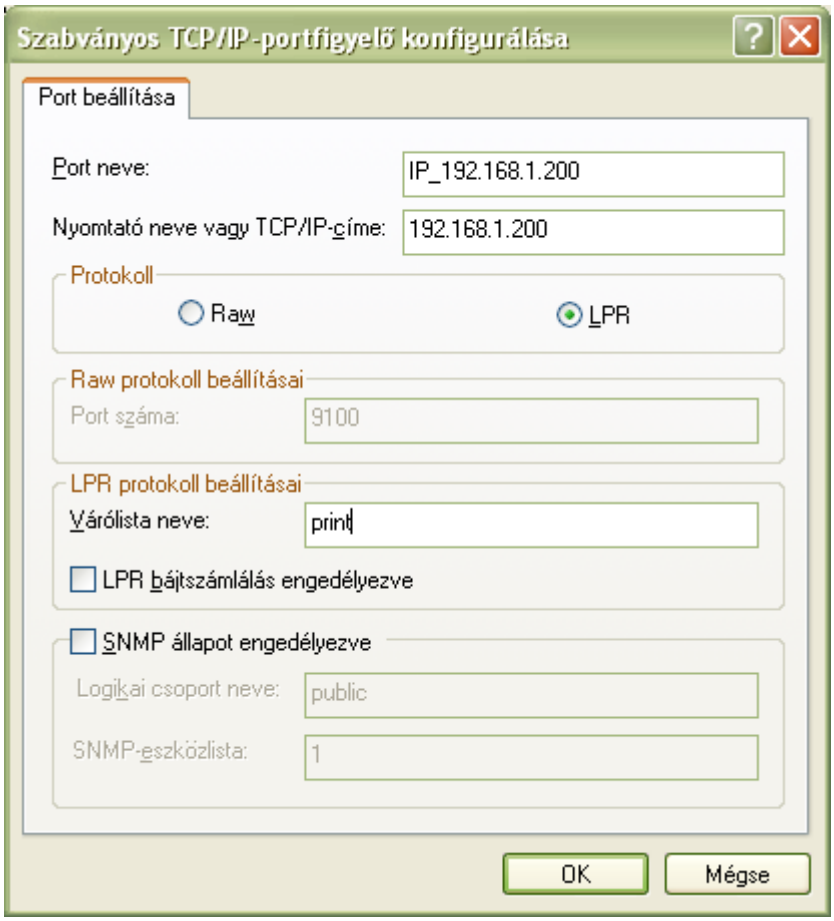
Ezt a nyomtatót elsősorban Erika használja, de mivel a hálózatra van csatlakoztatva, ezért bárki nyomtathat rá, akinek szüksége van. Természetesen csak ha fel van telepítve.

A nyomtatót a 192.168.1.201-es IP címmel lehet elérni, vagy a hp2550n néven, de sokkal stabilabb, ha az IP címmel éri el a gép a nyomtatót.

*Telepítése* hasonló az előbb már említett nyomtatóhoz.
Egyszerűen csak a nyomtató hozzáadása-val egy számítógéphez helyi nyomtatót kell telepíteni, a Plug and Play rész előtti pipa kiszedésével! (Megelőzve a felesleges hálózati nyomtatók felkerülését.)
A következő ablakon Új port létrehozásánál egy Standard TCP/IP portot kell létrehozni és a megfelelő helyre beírni az IP címet.
A telepítés során betallózni egy „saját lemez”-ként nevezett drivert és értelemszerűen folytatni a telepítést.

# KonicaMinolta-k:

A Konica Minolta-k elég érdekes telepítési procedúrát igényelnek, bár sok pontban azért megegyeznek egy átlagos hálózati nyomtató telepítésével.
A nyomtató hozzáadás-ával szintén a számítógéphez csatlakoztatott helyi nyomtatót kell kiválasztani. A következő lépésnél új port létrehozásánál a Standard TCP/IP portot kell kiválasztani. A megfelelő mezőbe be kell írni a megfelelő IP címet (192.168.1.190 vagy 192.168.1.200), majd a további információkat kérő ablakban az Egyéni lehetőséget választva, Beállítások gombra kattintva beállítani a nyomtatót a képen  látható módon.
Ha kész, akkor az OK-val majd a tovább-al haladhatunk tovább a telepítési lépéseken.




A saját lemeznél beadható driver a \\tupoljev\system\drivers megosztás alatt található. A driver betallózása után értelemszerűen folytassuk a telepítést, és az esetleges Microsoft aláírás hiányára figyelmeztető ablaknál pedig engedélyezzük a driver telepítését.

## **KonicaMinolta scannelési beállítása**:

A KonicaMinolta-k rendelkeznek egy nagyon kényelmes szolgáltatással. A pdf-be scannelés lehetőségével, ráadásul a cél akár egy hálózati megosztás is lehet. Sajnos viszont, ha ez a hálózati megosztás authentikációt igényel, akkor nem minden esetben sikerül a scannel-t fájl felmásolása a megosztásra. (kb 10-böl csak 4szer)

A cél beállítása, vagy a cél lista beállítása a Konica-k webes adminisztrációs felületén tehető meg. Ezt a webes felületet a nyomtató IP címének (vagy hálózati nevének) a böngészőbe beírásával tehetjük meg. Ehhez általában nem kell administrator-i jog a nyomtatón. (Ha valamihez szükséges, akkor először Logout-olni kell, majd administrator-i jogosultsággal belépni)
A cél lista a C250-esen a Scan, a C205-ön pedig a Store Address menüpont alatt bővíthető.
New Registration gombbal vehető fel új célkönyvtár illetve megosztás, a protokoll kiválasztásával.

A cél listákat sajnos a gép nem rendezi automatikusan ABC sorrendben, ezt minden új cél felvételekor kézzel kell megadni. Illetve azt is, hogy a cél főképernyőjén (Main) megjelenjen-e vagy csak tallózás, a megfelelő betű lenyomása után.