

TARTALOMJEGYZÉK

1. Bevezetés:.....	3
2. Fizikai megvalósítás.....	4
3. Hardware és software követelmények	10
3.1. Debian Linux 3.0 stable.....	10
3.1.1. Hardware követelmény:.....	10
3.1.2. Software díjak:	10
3.1.3. Szakember költsége:	10
3.1.4. Biztonság:.....	10
3.2. Windows 2000 Advanced Server.....	11
3.2.1. Hardware követelmény:.....	11
3.2.2. Software díjak:	11
3.1.3. Szakember költsége:	11
3.2.4. Biztonság:.....	11
3.3. Tesztgépek konfigurációja.....	12
3.3.1. Kiszolgáló gép konfigurációja:	12
3.3.2. Kliens gép konfigurációja:	12
4. Software beállítások.....	13
4.1. Windows 2000 Advanced Server, DHCP szerver:	15
4.1.1. A bejegyzés neve és megjegyzés.....	15
4.1.2. Az IP intervallum megadása:	15
4.1.3. Kizárt címtartomány megadása	16
4.1.4. Az IP cím érvényességi ideje	17
4.1.5. DHCP által kiosztott adatok beállítása	17
4.1.6. Router (alapértelmezett átjáró).....	18
4.1.7. Domain név és DNS szerver megadása	18
4.1.8. WINS szerver megadása	19
4.1.9. Beállítások aktiválása	19
4.1.10, MAC címhez állandó IP cím.....	19
4.1.11, A kiosztott címek állapota.....	20
4.2. Debian Linux 3.0 stable, DHCP szerver:	21
Az utasítások jelentése:	22
4.3. Windows 2000 Advanced Server, DNS server:.....	23

DNS forward-ok és reverse-ek hozzáadása	23
4.3.1. DNS forward hozzáadása.....	23
4.3.2. DNS reverse hozzáadása.....	24
4.4. Debian Linux 3.0 stable, DNS szerver:	28
4.4.1. DNS zónák hozzáadása.....	28
4.4.2. DNS forward hozzáadása.....	29
4.4.3. DNS reverse hozzáadása.....	29
4.5. Windows 2000 Advanced Server, FTP szerver	30
4.5.2. „Security Accounts” beállítófüls.....	32
4.5.5. „Directory Security” beállítófüls	35
4.6. Debian Linux 3.0 stable, FTP szerver (ProFTPd).....	37
A konfigurációs file tartalma	37
Az utasítások jelentése:	39
4.7. Windows 2000 Advanced Server, útválasztás és internetmegosztás	39
4.7.1. Az útválasztás engedélyezése.....	39
4.7.2. Az útválasztó kiszolgáló típusa:	40
4.7.3. Az útválasztó által használt protokoll beállítása	40
4.7.4. Modemes kapcsolat engedélyezése és tiltása	41
4.7.5. A beállítások befejezése.....	41
4.7.6. Alapértelmezett beállítások.....	42
4.7.7. Az útválasztó táblázat megtekintése.....	42
4.7.8. Hálózati címfordítás (NAT) hozzáadása.....	43
4.7.9. A NAT konfigurálása	43
4.8. Debian Linux 3.0 stable, útválasztás és Internet megosztás	45
4.8.1. Az útválasztó táblázat elemei.....	45
4.8.2. Az útválasztó táblázat módosítása.....	46
4.8.3. Az Internet elérés beállítása	46
5. Befejezés.....	48

1. Bevezetés:

A dolgozat célja, hogy szembe állítsa napjaink két legnagyobb szerverre szánt operációs rendszerét a Windows NT-t és a Linux-ot. A dolgozat megírásakor a legelterjedtebb Windows NT verzió a Windows 2000 Advanced Server, valamint a legelterjedtebb Linux, pedig a Debian Linux 3.0 stable. A Windows és a Linux felhasználók között örökös a harc, egyértelműen egyik sem jobb a másiknál. Viszont vannak szempontok, amik alapján az egyik kiemelkedően jobb lehet a másiknál, ezek alapján kell megválasztanunk az operációs rendszert.

Az összehasonlítás kiterjed a gazdaságossági szempontokra, a fizikai és szellemi erőforrás igényekre. A kis hálózatokban nagyon fontos lehet a kiszolgáló számítógép hardware és software költsége, ugyanis az anyagiakat a humán erőforrásokra áldozzák. De üzembe helyezés után a kiszolgáló karbantartás, a szakember költségei is meghatározóak lehetnek.

Software összehasonlítás:

- DHCP kiszolgáló az egyszerű TCP/IP kapcsolathoz
- Domain név szerver az IP címekhez való névrendeléshez
- FTP server a központi file elérhetőséghez
- Hálózatok összekapcsolása (útválasztás)
- Internet megosztás a teljes hálózat Internet eléréséhez

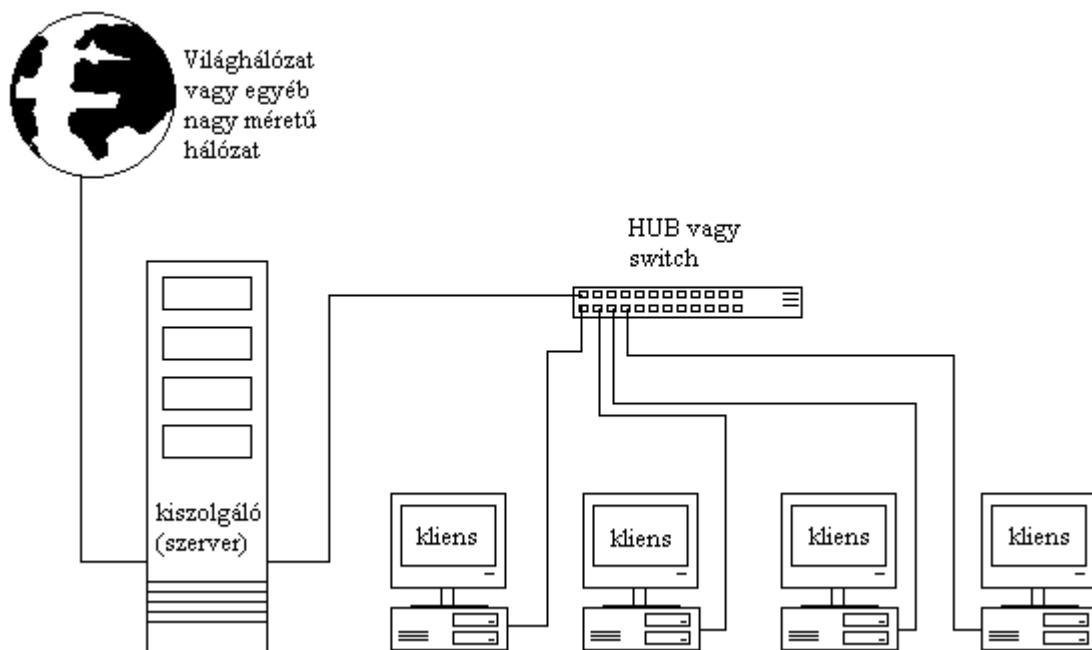
Hardware összehasonlítás:

- minimális hardware követelmény
- ajánlott hardware követelmény

Gazdaságossági összehasonlítás:

- hardware költségek minimális konfiguráció esetén
- software jogdíjak költségei
- üzemeltető szakember költségei

2. Fizikai megvalósítás



2-2. ábra.

A fizikai felépítés a napjainkban leggyakrabban használt csillag topológiájú, **100Mbit/másodperc** maximális adatátviteli sebességű **UTP** (árnyékolatlan csavart érpár) csatlakozású **Ethernet** (IEEE 802.3) hálózat. Ennek alapja az ütközésfigyeléses módszer, a CSMA/CD. A kapcsolat kiépítéséhez szükség van minden számítógépben Ethernet csatlóóra.

Az ethernet protokoll tulajdonságai:

- minden ethernet csatló egyedi címmel rendelkezik (6 Byte hosszúságú MAC address), amit a gyártó éget be a csatló ROM memóriájába. Ezeknek a kiosztásáról az IEEE rendelkezik.
- minden hálózatba kötött csatló egyszerre figyel a hálózat forgalmát, és képes bármikor üzenetet küldeni
- egyszerre csak egyetlen frame azaz adatcsomag élhet, viszont ha két csatló egyszerre szeretne adni, akkor véletlen hosszúságú várakozás után ismét megpróbálják elküldeni a csomagot
- az adó interfész mindig beírja az adatcsomagba a vevő csatló címét

- az adatcsomag minden csatolóhoz eljut, de csupán az dolgozza fel, amely számára címezve van, a többi figyelmen kívül hagyja

Az egyedi azonosító és az IP cím között összefüggés van. Az azonosítás kétféle lehet, ARP (Address Resolution Protocol) és RARP (Reverse Address Resolution Protocol).

- Az ARP az adott IP címhez társított MAC címet adja vissza. Ha egy gép egy másik gép MAC címét szeretné megtudni, akkor adatcsomagot küld a hálózatra, amit minden gép megkap. Ez az adatcsomag tartalmazza a küldő IP és MAC címét, és a fogadó gép IP címét. Ha létezik a keresett IP, akkor visszaküldi az adatcsomagot a saját MAC címével.

- A RARP-ot olyan eszközök használják, amik nem ismerik saját IP címüket. Ilyenek lehetnek például nyomtatók. Ebben az esetben az eszköz RARP adatcsomagot küld a hálózatra, ami csak a MAC címet tartalmazza. A kiszolgáló ezt megkapva kikeresi a MAC címhez tartozó IP címet, és az adatcsomagba beírva azt visszaküldi.

A csatolók összeköttetését biztosító kábel 4 érpárt tartalmaz, és RJ-45 típusú csatlakozóban végződik. Előnyei a koax típusú kábelezéssel szemben, hogy:

- a koaxnál nagyobb sebességre képes
- a hálózat kábelezési rendszere könnyen áttekinthető, központosított kábelezés
- a változtatások könnyebben kivitelezhetőek
- a fizikai kapcsolat szakadása csak az adott kábelre kötött interfészre lesz hatással

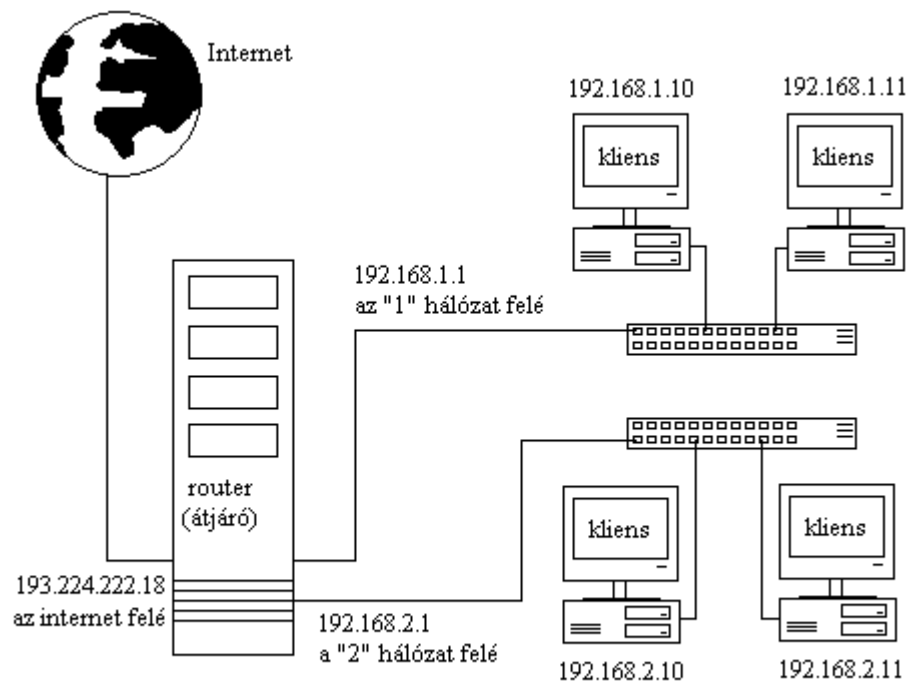
Viszont hátrányai, hogy:

- nem rendelkezik árnyékolással, zajos környezetben nem üzembiztos
- a speciális eszközök miatt drágább
- a központosított megvalósítás miatt több kábelre van szükség

A csatolók kapcsolatát **HUB**-al vagy **switch**-el oldhatjuk meg. A HUB egyszerűbb és olcsóbb eszköz, de csupán jelismétlőként működik, az egyik portján kapott csomagokat az összes többi portjára továbbítja. Ezzel szemben a switch intelligensebb megoldás, ugyanis csak a szükséges portra továbbítja a jelet. Ezekkel az eszközökkel csak annyi csatoló köthető össze, ahány csatlakozóhellyel rendelkeznek, de ezek a hálózati eszközök összekapcsolhatóak. Célszerű switch-et alkalmazni a stabilabb és gyorsabb hálózati működés eléréséhez. Szükség lehet **router** (útválasztó) berendezésre is, amely routolható hálózatokat kapcsol össze. Az útválasztás történhet megadott táblázat alapján, de programok által automatikusan konfiguráltan is. A hálózat címét használja a csomagok

irányítására, ezért csak olyan csomagokat tud feldolgozni ami tartalmazza a hálózat és azon belül a számítógép címét is. A routolás megoldható szoftveres úton és céleszköz alkalmazásával is.

Az átjárók képesek különböző protollokat összekapcsolni, viszont az útválasztók nem. Az átjáró egy olyan gazdagép, amely egyidejűleg két vagy több fizikai hálózathoz kapcsolódik és csomagoknak a köztük való továbbítására van konfigurálva. Ahhoz, hogy az IP felismerje, hogy az interfész rajta van-e a fizikai hálózaton, különböző fizikai hálózatoknak különböző IP hálózatokhoz kell tartozniuk. Az átjárónak minden hálózaton egyedi IP azonosítóval kell rendelkeznie. Az egyszerre két alhálózaton szereplő gazdagépek mindkét címükkel szerepelnek.



2-2. ábra.

A legelterjedtebb protokoll a **TCP/IP** (Transmission Control Protocol/ Internet Protokoll). Ugyanis az Internet és a Windows 2000 active directory is erre épül. Az IP cím egyértelmű azonosítást tesz lehetővé a hálózaton. Az IP címhez tartozik MAC azonosító és portszám. A MAC azonosító teljesen egyedi a hálózati csatolóra nézve, a gyártók állítják be. A portszám megadja, hogy az érkező csomagot melyik programnak kell megkapnia. Az IP protokollnak ma már 2 elterjedt típusa van, de a Windows 2000 miatt csak **IPv4** használható. Itt a cím hossza 4 Byte, ezzel szemben az IPv6 esetében 16 Byte. Helyi hálózat esetén tetszőlegesen megadhatjuk az IP címet, de ügyelnünk kell arra, hogy ne

alakuljon ki ütközés két azonos cím miatt. Ezért célszerű a DHCP szerver alkalmazása, melynek segítségével az IP címek automatizált úton kerülhetnek kiosztásra.

A TCP (Transmission Control Protokoll) feladata a nagy adatsomagok kisebb részekre bontása, továbbítása, majd újra egyesítése. Azért alkalmazzuk a TCP alapú kapcsolatot, mert így bizonyosságok szerezhethetünk arról, hogy a célállomás megkapta a kért adatmennyiséget. A **TCP kapcsolat felépülése:**

- 1, Ellenőrzi, hogy a vevő készen áll-e az adatok fogadására.
- 2, Ha a vevő készen áll, válaszol az adónak, és felkészül az adatok fogadására.
- 3, Amikor az adó megkapja a vevő nyugtázását, megkezdí az adattovábbítást.
- 4, Minden kis csomag esetében a vevő jelzi az adó számára, hogy a csomagot hibátlanul megkapta.
- 5, Ha elküldés után nem érkezik jelzés a vevőtől, akkor az adó megismétli a csomag továbbítását.
- 6, Az adatátvitel befejeztével bontják a kapcsolatot.

Az Internet Protokoll azonosítói az IP címek, amik interfészekhez vannak rendelve. Egy interfésznek több IP címe is lehet. Viszont egy IP címhez a pontos azonosítás miatt csak egy interfész tartozhat. Ezek az IP címek meghatározott módon vannak csoportosítva. Három osztályt különböztetünk meg:

„A osztály”: 8 bitet használ a hálózat, 24 bitet az interfész azonosítására. Így 16777216 interfész címezhető meg. Első számjegye 1 és 127 közé kell esen, így összesen 125 db ilyen hálózat lehetséges.

„B osztály”: 16 bitet használ a hálózat, 16 bitet az interfészek azonosítására. Így 65536 interfész címezhető meg. Első számjegyet figyelve a 121 és 191 közé eső címek, „B” osztályúak. Az Interneten 16382 db ilyen hálózat létezik.

„C osztály”: 24 bitet használ a hálózat, 8 bitet az interfészek azonosítására. Így 256 interfész címezhető meg. Első számjegyük 193 és 224 közé eshet, ezért 2097150 ilyen hálózat lehetséges.

„D osztály”: Speciálisan fenntartott címek, 224 és 239 közé eső címek, speciális eljárások számára fenntartott címek.

„E osztály”: Speciálisan fenntartott címek, 240 és 255 közé esnek, az Internet saját céljaira fenntartott címek.

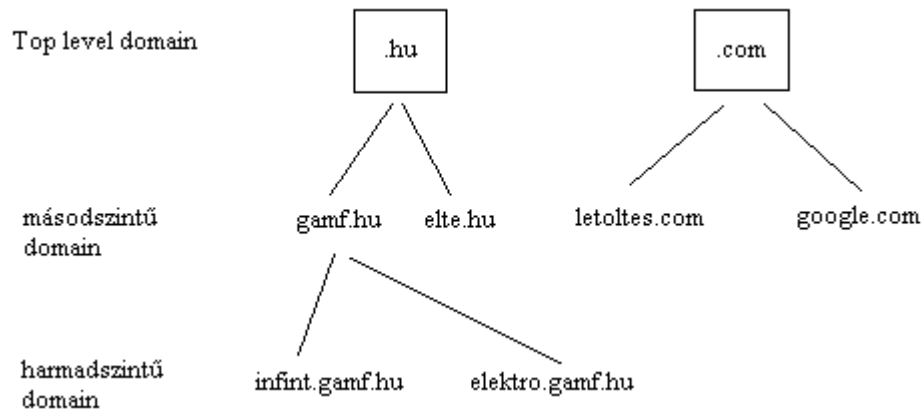
Privát címeket foglaltak le a hálózatok számára, ezeket lokális hálózatokon használhatjuk. „A osztály” esetében a 10.0.0.0 , „B osztály” esetében a 172.16.0.0 - 172.31.0.0 , „C osztály” esetében a 192.168.1.0 - 192.168.255.0 használhatunk címeket.

A domain nevek felépítése:

Windows 2000 esetében az Active Directory miatt szükséges DNS szerver használata, melynek segítségével az IP címeket könnyen azonosítható domain nevekkel rendelhetjük össze, ahogyan az Interneten is. Ez a domain név nem más, mint az IP cím szinonimája, a kapcsolat felépítését továbbra is az IP cím végzi. A DNS a gazdagép-neveket domain hierarchiába rendezi. Ebben a rendszerben elfoglalt hely szerint lehet egy domain felső (top level)-, másod-, vagy harmadrendű. Az Internet esetében a top level domain a hálózat általános típusát adja meg. Ami lehet ország-azonosító, vagy szervezeti egységeket azonosító, mint pl.: .mil az USA katonai domain nevei. A másodszintű domaint regisztrálni kell a megfelelő szervezetnél. Magyarországon a "www.nic.hu"-nál (Network Information Center) tehető ez meg. Harmad és további szintű domain-ek esetében a másodszintű domain üzemeltetője rendelkezik. A host név már számítógépet azonosít. Az adminisztrátoroknak minden géphez egyedi nevet kell rendelniük, amelyeknek az alábbi követelményeknek meg kell felelniük:

- egyedinek kell lennie az adott domain-en belül
- maximum 24 karakter hosszúság
- csak betűket, számokat, és „-”, „.” karaktert tartalmazhat

A domain neveket az IP címektől eltérően jobbról balra kell olvasni. A különböző szinteket „.” karakter választja el egymástól. A kis- és nagybetű között a domain név szerverek nem tesznek különbséget.



2-3. ábra.

A DNS (Domain Name Service - Domain Név Szolgáltatás):

A DNS valójában egy programot takar, amelynek segítségével azonosíthatók bejegyzések. Ez a program a „névfeloldó”. Domain név azonosítása során az operációs rendszerek először a saját bejegyzéseik között keresik a domain névhez tartozó IP címet (Linux esetében a keresési sorrend megváltoztatható), majd külső domain szerverhez fordulnak. Fordított keresés esetében (reverse) az IP címhez tartozó domain névre vagyunk kíváncsiak.

3. Hardware és software követelmények

3.1. Debian Linux 3.0 stable

3.1.1. Hardware követelmény:

CPU: minimális:	386 SX (2.0.x kernel), 486 SX (2.2.x kernel)
ajánlott:	Pentium 166 MHz
RAM: minimális:	12 MByte (2.2.x kernel) ; 16MByte (2.4.x kernel)
ajánlott:	64 Mbyte vagy több
HDD: minimális:	200 MByte + 64 MByte swap
ajánlott:	200 MByte vagy több + 128 MByte swap
VGA: minimális:	Hercules
ajánlott:	VGA kompatibilis
Grafikus felület:	nem szükséges

3.1.2. Software díjak:

operációs rendszer: ingyenes

(CD melléklet: szakirodalom\GNU tanusítvány magyar.doc)

3.1.3. Szakember költsége:

Az operációs rendszer, és programjainak részletes ismerete, nagy teljesítményű sok szolgáltatást nyújtó kiszolgáló üzemeltetése magas szintű ismereteket igényel, emiatt a megfelelő szakember költsége rendkívül magas lehet.

3.1.4. Biztonság:

Felépítéséből adódóan biztonságosabb. Hibák nyilvánosságra kerülésétől számítva órákon, esetleg napokon belül várható a javítás. A tűzfal kernel szintű, nagyon nagy pontossággal konfigurálható. Elenyészően kevés vírus létezik Linux-ra, és azok is csak a rendszergazdai figyelmetlenségével okozhatnak kárt a rendszeren. A Debian fejlesztői garantálják az esetleges biztonsági hibák 48 órán belüli javítását STABLE disztribúció esetén.

3.2. Windows 2000 Advanced Server

3.2.1. Hardware követelmény:

CPU: minimális:	Pentium I 133MHz
ajánlott:	Pentium III 1133MHz (maximum 8 darab)
RAM: minimális:	128 MByte
ajánlott:	256 (512) MByte vagy több
HDD: minimális:	2 GByte + swap
ajánlott:	3 GByte vagy több + swap
VGA: minimális:	VGA kompatibilis (min. 640x480)
ajánlott:	VGA kompatibilis 800x600 vagy nagyobb
Grafikus felület:	szükséges

3.2.2. Software díjak:

operációs rendszer 1 szerver 5 klienssel:	450 000 Ft + ÁFA
operációs rendszer 1 szerver 5 klienssel OEM:	250 000 Ft + ÁFA
kliensbővítés:	45 000 Ft / 5 kliens

3.1.3. Szakember költsége:

Az operációs rendszer működésének elsajátítása könnyen megtanulható, a rendszer könnyen konfigurálható a grafikus segédprogramok és a varázslók segítségével. A szakember képzése és alkalmazása így olcsóbb, mint a Linux esetében.

3.2.4. Biztonság:

Az Explorer alap gyengén védetté teszi a kiszolgáló gépet állandó internetes kapcsolat esetén. Rendkívül sok vírus található az összes Windows operációs rendszerre. A biztonsági frissítések jóval lassabban reagálnak a nyilvánosságra került hibákra, nem kritikus hibák esetén gyakran több hónap múlva jelenhet meg javítás, de még a kritikus hibák javítása is lassabb. Tűzfala kezdetleges, kiegészítő tűzfal software használata ajánlott.

3.3. Tesztgépek konfigurációja

3.3.1. Kiszolgáló gép konfigurációja:

(Kis teljesítményű kiszolgáló)

Processzor: Intel Pentium Celeron Tualatin 1100 MHz
Memória: 256 MByte SD-RAM
Háttértár: Seagate Barracuda 7200RPM 80GB
Videó: Ati Radeon 9000 128MB DDR-RAM
Hálózat: Realtek 8139 Fast Ethernet (100 MBit/sec)
Op. rendszer: Windows 2000 Advanced Server SP3 EN
Debian Linux 3.0 stable

3.3.2. Kliens gép konfigurációja:

(Kis teljesítményű munkaállomás)

Processzor: IBM Cyrix MII-300 (233MHz Pentium 1 osztály)
Memória: 80 MByte SD-RAM
Háttértár: Seagate Medalist 1.7GB
Videó: Ati Rage II 2MB
Hálózat: Realtek 8029 Ethernet (10MBit/sec)
Op. rendszer: Windows 98 HU

4. Software beállítások

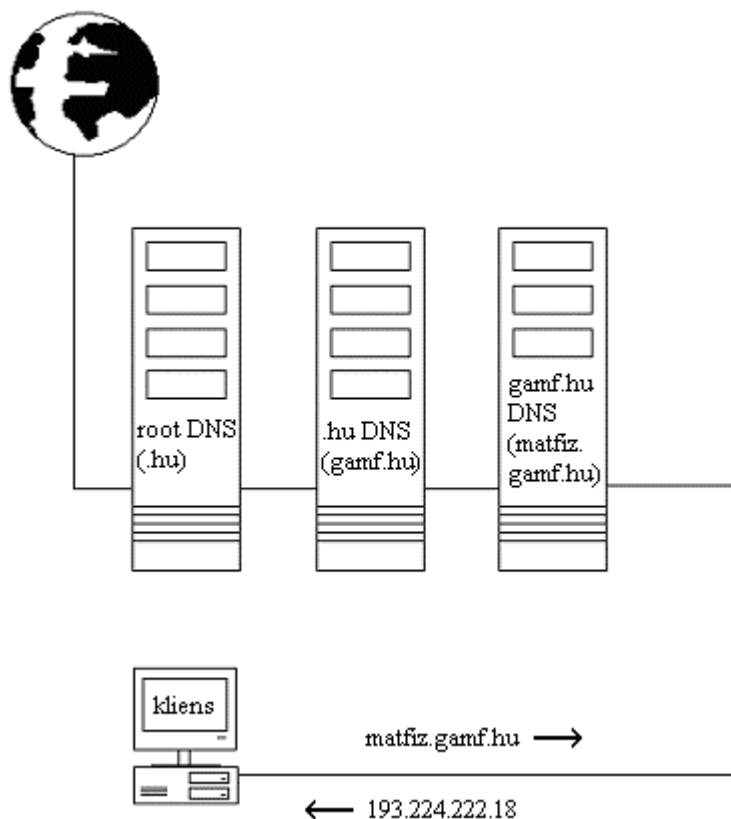
DHCP – Dynamic Host Configuration Protocol

A DHCP szerver feladata, hogy a hálózatba belépőknek automatikusan IP címet osszon, de egyéb hasznos információkat is továbbíthat (átjáró, DNS szerver, stb. IP címe). Ezáltal elkerülhető, hogy egy IP címet több csatoló kaphasson meg. Minél nagyobb egy hálózat annál célszerűbb alkalmazni. Megadható az egyedi azonosítóhoz (MAC cím) tartozó állandó IP cím, így minden hálózatba lépéskor az adott MAC címhez az adott IP fog tartozni. De lehetőség van az IP címeket dinamikusan kezelni, azaz a DHCP szolgáltatás automatikusan ad IP címet a hálózatba lépő csatolónak egy megadott intervallumban. Általában a DHCP szerverek automatikusan próbálkoznak egy adott MAC címhez az előzőleg kiosztott IP címet rendelni.

DNS – Domain Name Server

A DNS feladata, hogy megkönnyítse a számítógépek azonosítását könnyebben megjegyezhető nevekkkel, és a tartományhierarchia egyértelmű áttekinthetősége.

A DNS működésének legjobb példája az Internet, ahol az elsődleges (legfelső szintű) domain neveket root domain szerverek tárolják.



4-1. ábra.

A 4-1. ábrán látható módon az Internet böngészésekor a domain nevek feloldása jobbról balra történik. A példa szerint először a „.hu” feloldása történik a root DNS szerver által. A „gamf.hu” név feloldását már a .hu -hoz tartozó DNS szerver végzi. A „matfiz.gamf.hu” név feloldását már a „gamf.hu” DNS szervere végzi el.

FTP – File Transfer Protokoll

Az FTP feladata, hogy távoli file rendszereket érhessünk el, helyihez hasonlóan.

NETBIOS – régebbi protokoll, egyszerűsége miatt könnyen használható, de csak kis hálózatok esetében. Nagy hálózatok esetében nem célszerű használni, mert lassúvá teszi a hálózati kommunikációt. WINS szerver alkalmazásával növelhető működésének sebessége, mert így a hálózaton levő gépek azonosítása nem szórt üzenetekben történik, hanem a kliensek a WINS szervertől kérik a keresett csatoló adatait. A NETBIOS protokollt, ma már csak egyszerű file- és nyomtatómegosztásoknál használhatjuk.

A példa hálózati beállításai a /etc/network/interfaces alapján

Az interfész azonosítója Linux alatt:

```
iface eth0 inet static
```

A kiszolgáló IP címe. Célszerű állandó (nem DHCP által kiosztott) IP címet megadni a kiszolgálónak, mert a DHCP meghibásodása a kiszolgáló működését is lehetetlenné teszi:

```
address 192.168.1.1
```

Ez az alhálózati maszk 253 IP kiosztását teszi lehetővé a kiszolgáló címén kívül.

```
netmask 255.255.255.0
```

A hálózat azonosítója:

```
network 192.168.1.0
```

```
broadcast 192.168.1.255
```

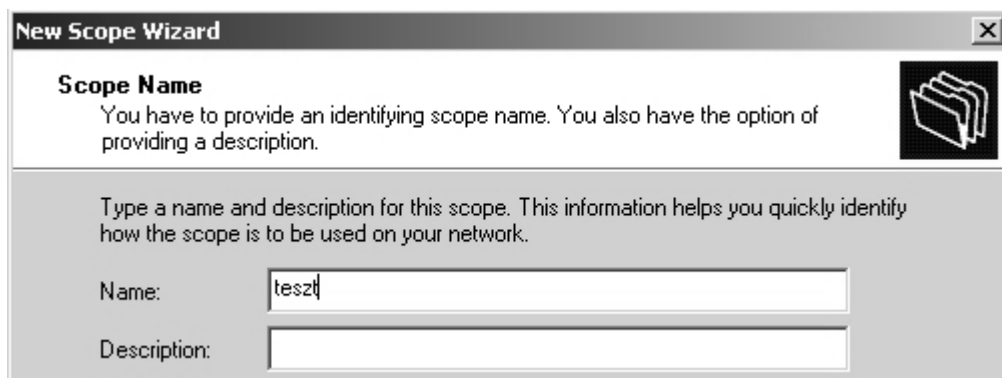
4.1. Windows 2000 Advanced Server, DHCP szerver:

A beállító program elérhető a START menü Programs / Administrative Tools / DHCP helyen.

Új bejegyzés hozzáadása:

Új bejegyzést a szerverrel jobb klikkelve, az New Scope menüponntal hozhatunk létre, ekkor felbukkan egy varázsló, amely a következő beállításokat segít elvégezni:

4.1.1. A bejegyzés neve és megjegyzés (4.1.1-1. ábra)



4.1.1-1. ábra.

„Name” - a DHCP bejegyzés neve

„Description” - megjegyzés a kiszolgáló nevéhez

4.1.2. Az IP intervallum megadása: kiinduló IP cím, és utolsó IP cím, hálózat azonosító hossza, alhálózati maszk (subnet mask) (4.1.2-1. ábra)

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 10

End IP address: 192 . 168 . 1 . 80

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

4.1.2-1. ábra.

- „Start IP address:” - első IP cím
- „End IP address:” - utolsó IP cím
- „Length” - hálózat azonosítójának hossza
- „Subnet mask” - alhálózati maszk

4.1.3. Kizárt címtartomány megadása (4.1.3-1. ábra)

New Scope Wizard

Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.

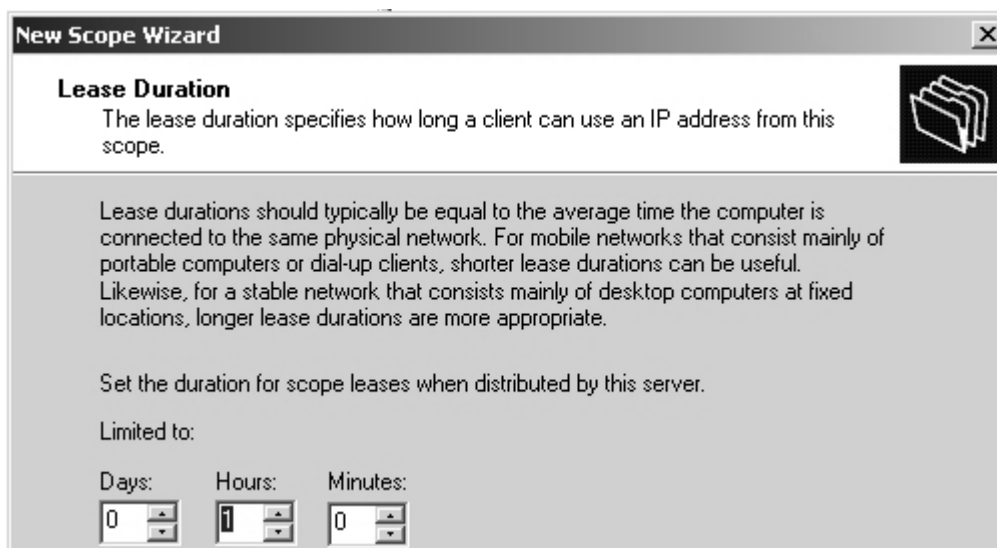
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: 192 . 168 . 1 . 21 End IP address: . . . Add

Excluded address range: Remove

4.1.3-1. ábra.

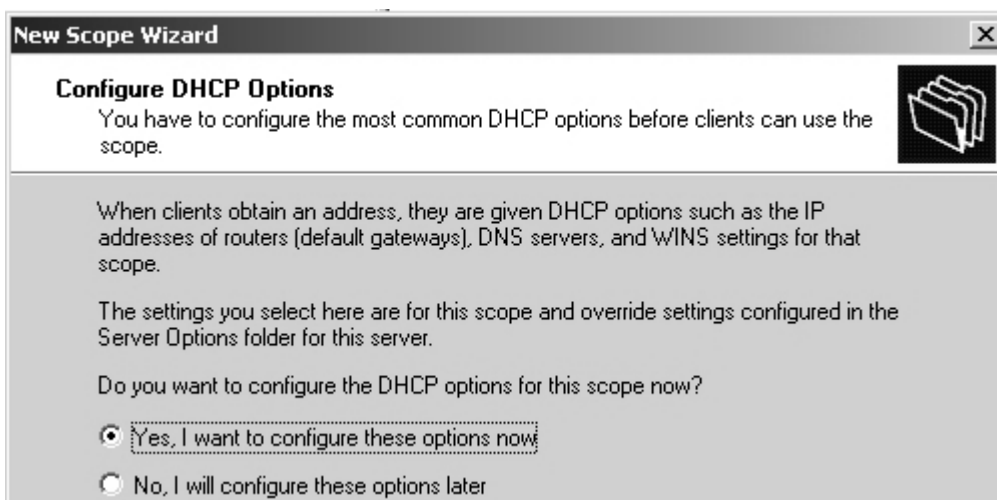
4.1.4. Az IP cím érvényességi ideje (4.1.4-1. ábra)



4.1.4-1. ábra.

Ez az érvényességi idő megadja, hogy a kiosztott IP cím, meddig érvényes a hálózaton. Lejárta után a kliens újra a DHCP kiszolgálóhoz fordul.

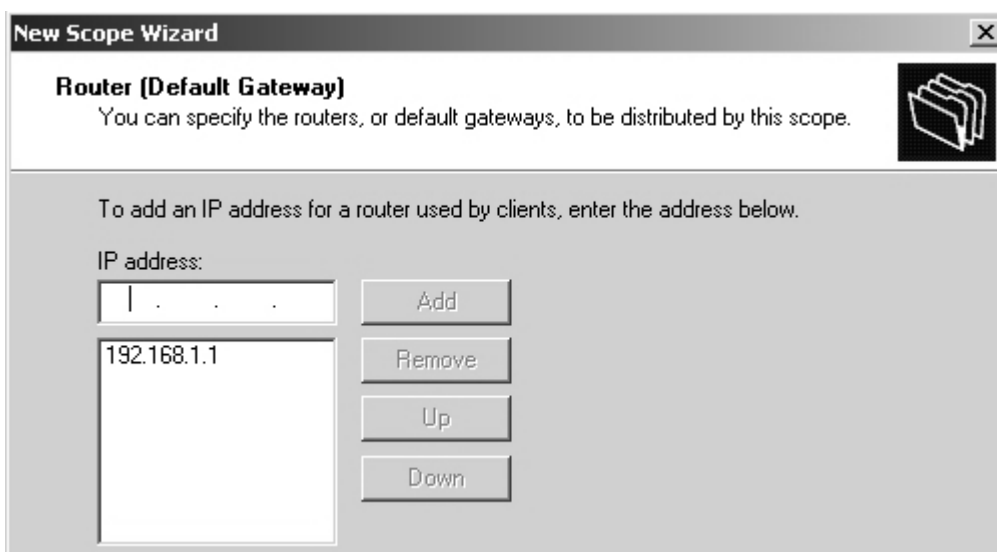
4.1.5. DHCP által kiosztott adatok beállítása (4.1.5-1. ábra)



4.1.5-1. ábra.

Megadhatjuk, hogy a DHCP kiszolgáló által kiosztott információkat kívánjuk-e beállítani. Ugyanis nem csak IP cím kiosztására alkalmas, de közölhetünk egyéb hasznos információkat, például: DNS szerver IP címe, átjáró IP címe, WINS szerver IP címe...

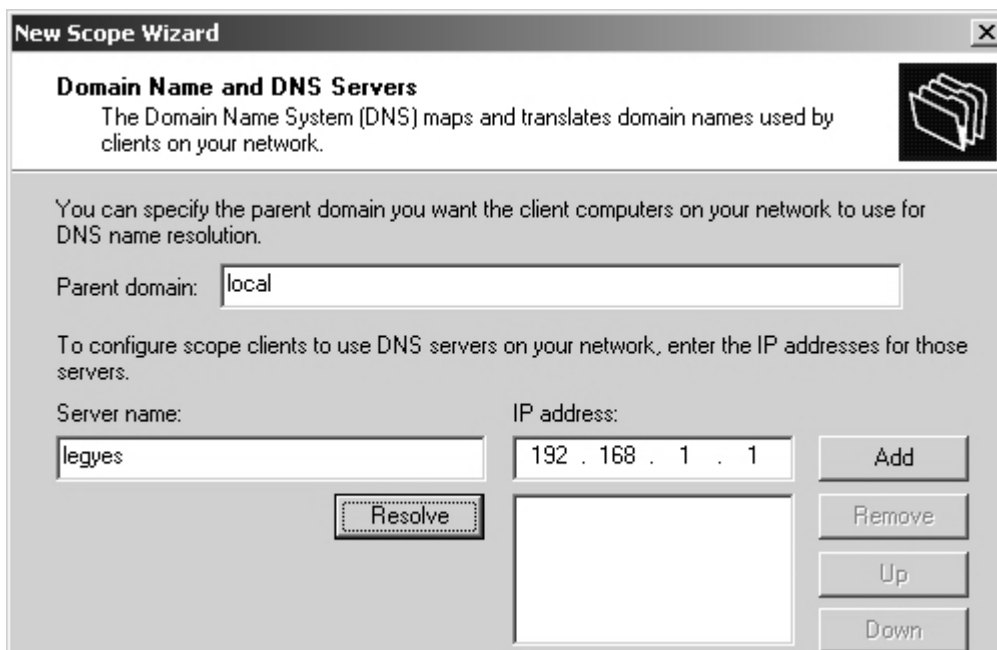
4.1.6. Router (alapértelmezett átjáró) (4.1.6-1. ábra)



4.1.6-1. ábra.

Routerek (átjárók) IP címét közölhetjük ennek segítségével a DHCP kliensekkel.

4.1.7. Domain név és DNS szerver megadása (4.1.7-1. ábra)

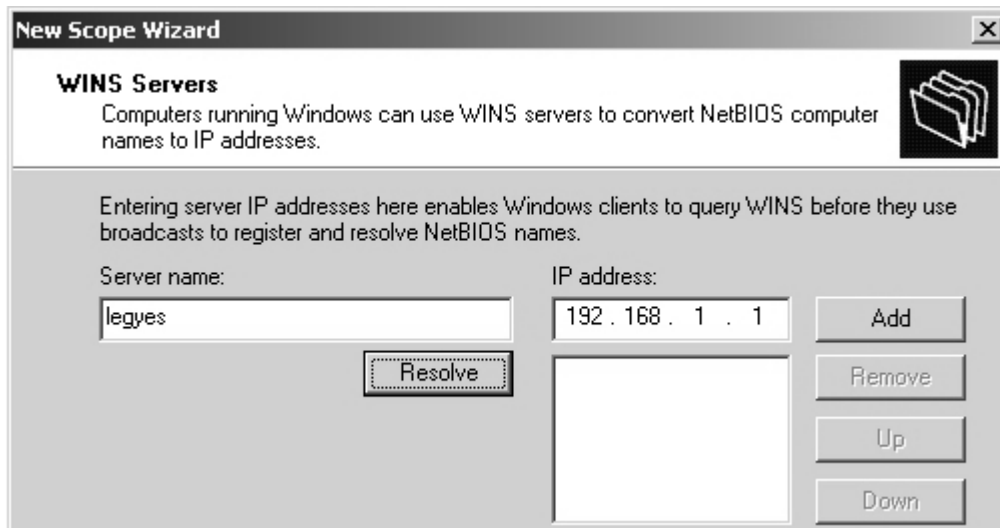


4.1.7-1. ábra.

Közölhetjük a domain nevet, és a DNS szerver IP címét.

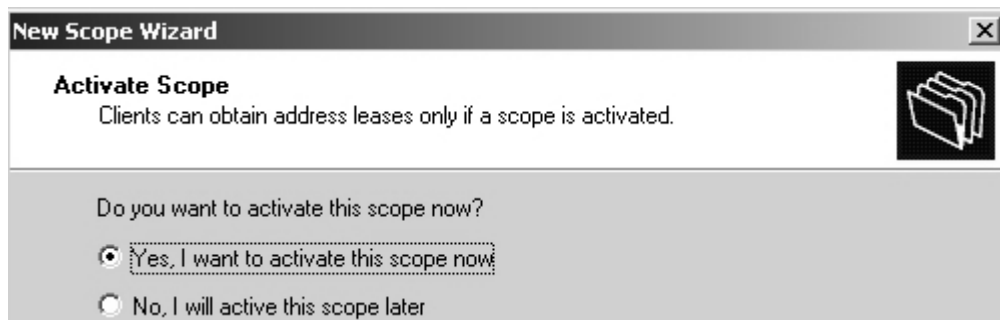
- „Parent Domain” - a szülő domain neve
- „Server name” - a DNS szerver neve
- „IP address” - a DNS szerver IP címe

4.1.8. WINS szerver megadása (4.1.8-1. ábra)



4.1.8-1. ábra.

4.1.9. Beállítások aktiválása (4.1.9-1. ábra)



4.1.9-1. ábra.

4.1.10, MAC címhez állandó IP cím rendelést a Reservations menüpontban tehetjük meg (4.1.10-1. ábra).

4.1.10-1. ábra.

„Reservation name:” - a foglalás neve

„IP address” - a lefoglalt IP cím

„MAC address” - a lefoglalt IP címhez tartozó egyedi Ethernet csatoló azonosító

4.1.11, A kiosztott címek állapota, statisztikája az ADDRESS LEASES menüpontban található meg (4.1.11-1. ábra).

Client IP Address	Name	Lease Expiration
192.168.1.15	cyrix.local	2003. 04. 14. 20:14:41

4.1.11-1. ábra.

4.2. Debian Linux 3.0 stable, DHCP szerver:

A szerver beállításai: /etc/network/interfaces

```
iface eth0 inet static
    address 192.168.1.1
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
```

Azaz a szerver IP címe 192.168.1.1, alhálózati maszkja 255.255.255.0, a hálózat azonosítója 192.168.1.0, broadcast címe 192.168.1.255

A DHCP szerver beállításai, egyszerű formában: /etc/dhcpd.conf

```
subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.50 192.168.1.120;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    option netbios-node-type 8;
    option netbios-name-servers 192.168.1.1;
}
```

Ez a konfigurációs file ezt teszi lehetővé, hogy a 255.255.255.0 alhálózaton, 192.168.1.50 és 192.168.1.120 intervallumban IP címet oszthassunk ki automatikusan. Továbbítja a router IP címét és a WINS szerver címét.

A kiosztott címek állapota: /var/lib/dhcp/dhcpd.leases~

```
lease 192.168.1.50 {
    starts 6 2003/05/03 23:10:29;
    ends 6 2003/05/03 23:20:29;
    hardware ethernet 00:c0:df:e0:62:a3;
    uid 01:00:c0:df:e0:62:a3;
    client-hostname "cyrix";
}
```

Ennek segítségével láthatjuk az aktuálisan kiosztott IP címeket. A „lease” mutatja a kiosztott IP címet, a „starts” a kiosztás idejét, az ends a végét. A „hardware ethernet” a hálózati csatoló MAC címét mutatja. A „client hostname” pedig a kliens állomás nevét.

Az utasítások jelentése:

option domain-name „név”	- domain név
option domain-name-servers „IPcím”	- DNS szerver(ek)
subnet „IPcím”	- alhálózat
netmask „IPcím”	- hálózati maszk
range „IPcím” „IPcím”	- IP intervallum
option netbios-node-type 8;	
option netbios-name-servers „IPcím”	- WINS szerver IP címe
option routers „IPcím”	- router IP címe
option broadcast-address „IPcím”	- broadcast cím
default-lease-time „érték”	- bérleti jog időtartama másodpercben
max-lease-time „érték”	- bérleti jog maximum időtartama (s)
host „név”	- számítógép azonosító neve
hardware ethernet „00:a0:24:65:4f:c5”	- hálózati csatoló MAC címe
fixed-address „IPcím”	- MAC címhez rendelt állandó IP cím

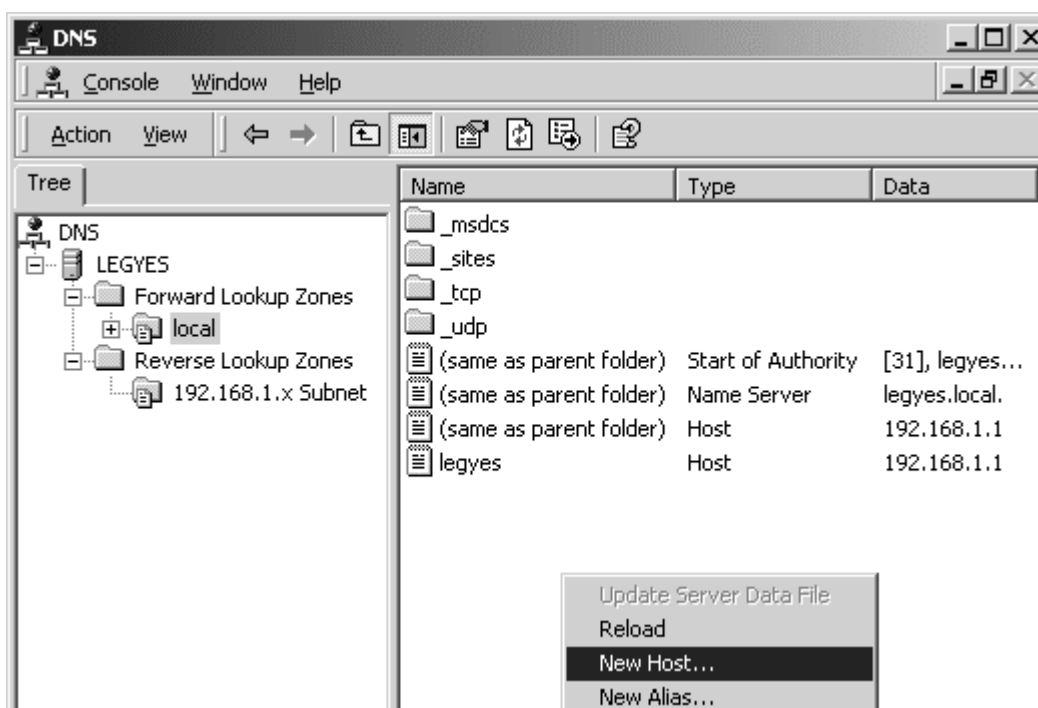
4.3. Windows 2000 Advanced Server, DNS server:

DNS forward-ok és reverse-ek hozzáadása.

Forward esetében a DNS névhez rendelünk hozzá IP címet, reverse esetében viszont az IP címhez rendelünk DNS-t.

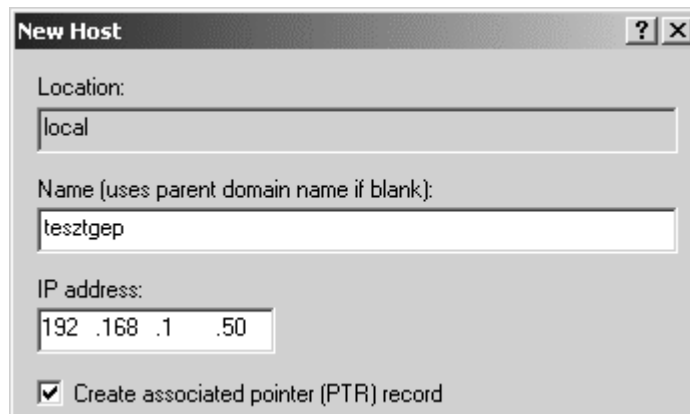
4.3.1. DNS forward hozzáadása

A domain-re jobb klikkelve a „New Host” menüponttal hozhatunk létre **új bejegyzést a domain alá.** (4.3-1. ábra)



4.3.1-1. ábra.

A „Location:” mezőben az **elsődleges domain** látható, ehhez tartozó aldomain lesz az általunk megadott (4.3-2. ábra). A „Name:” mezőbe a létrehozandó aldomain kerül, amennyiben ez a mező üres, úgy a szülő domain lesz érvényes. Az „IP address” mezőbe az aldomain IP címe kerül. Az „Add Host” gombra kattintva létrejön a bejegyzés. A példában a testtgep.local bejegyzés IP címe 192.168.1.50



4.3.1-2. ábra.

Az „**nslookup**” parancssori program alkalmazásával ellenőrizhetők a beállítások:

```
D:\>nslookup
```

```
Default Server: localhost
```

```
Address: 127.0.0.1
```

```
> tesztgep.local
```

```
Server: localhost
```

```
Address: 127.0.0.1
```

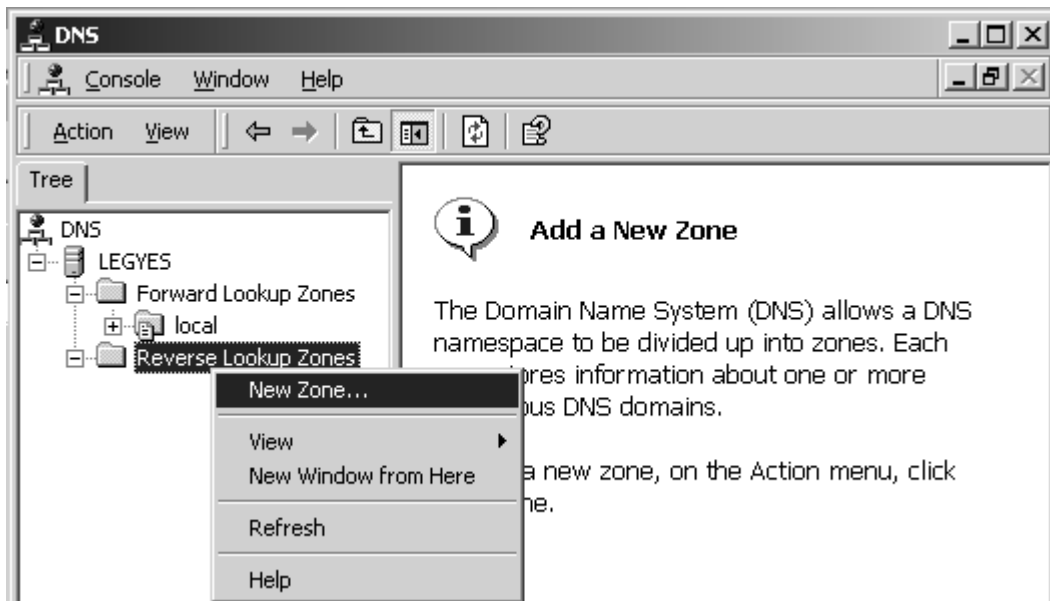
```
Name: tesztgep.local
```

```
Address: 192.168.1.50
```

```
>exit
```

4.3.2. DNS reverse hozzáadása

Új reverse bejegyzés létrehozása a „Reverse Lookup Zones” menüpontra jobb klikkelve a „New Zone” menüponttal lehetséges (4.3.2-1. ábra).

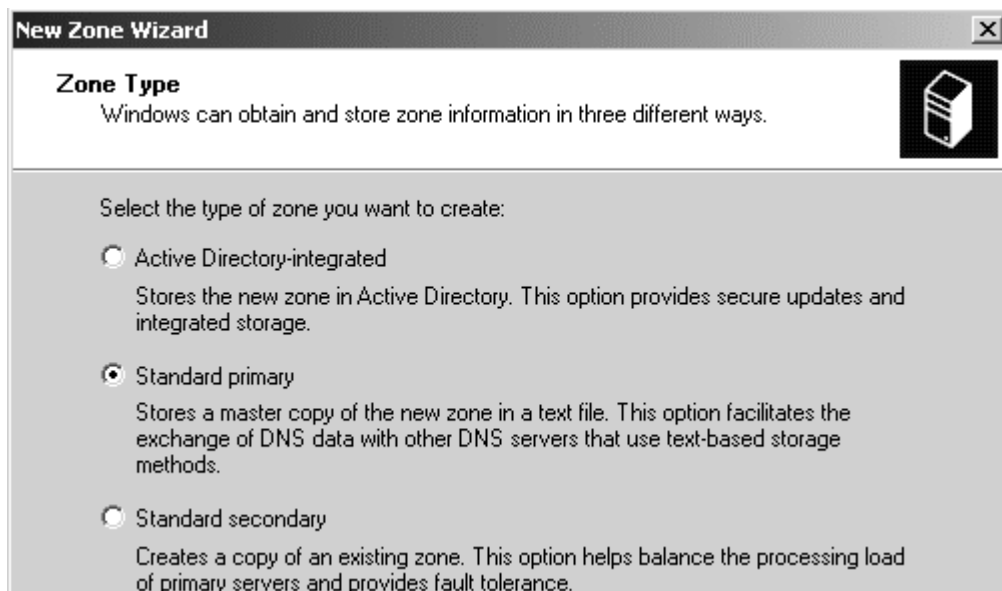


4.3.2-1. ábra.

Új zóna esetében meg kell adni a zóna típusát (4.3.2-2. ábra):

- active directory-ba integrált
- általános elsődleges
- általános másodlagos

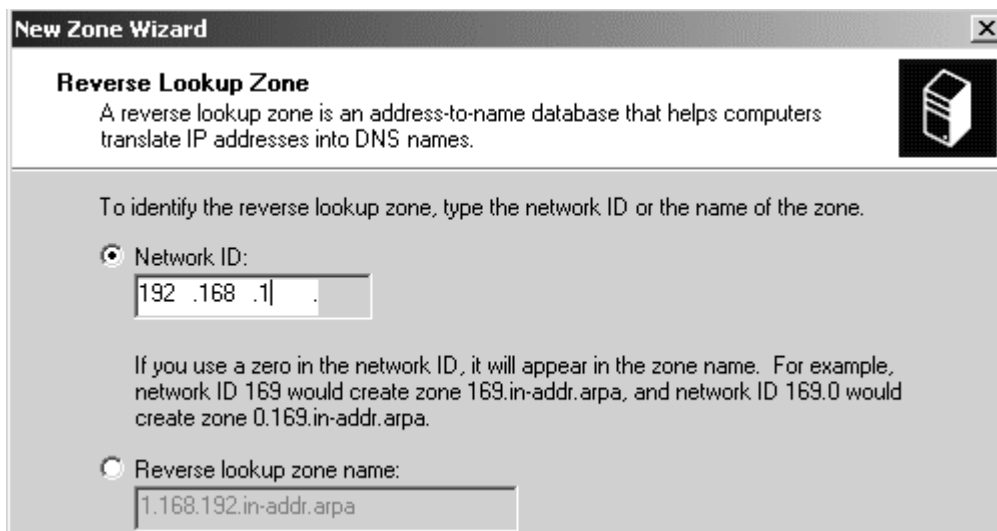
Az általános elsődleges zóna esetén egy szöveges file-ban tárolja el a beállításokat, amely file formátuma azonos a Linux DNS szerverének, a BIND-nek a file formátumával.



4.3.2-2. ábra.

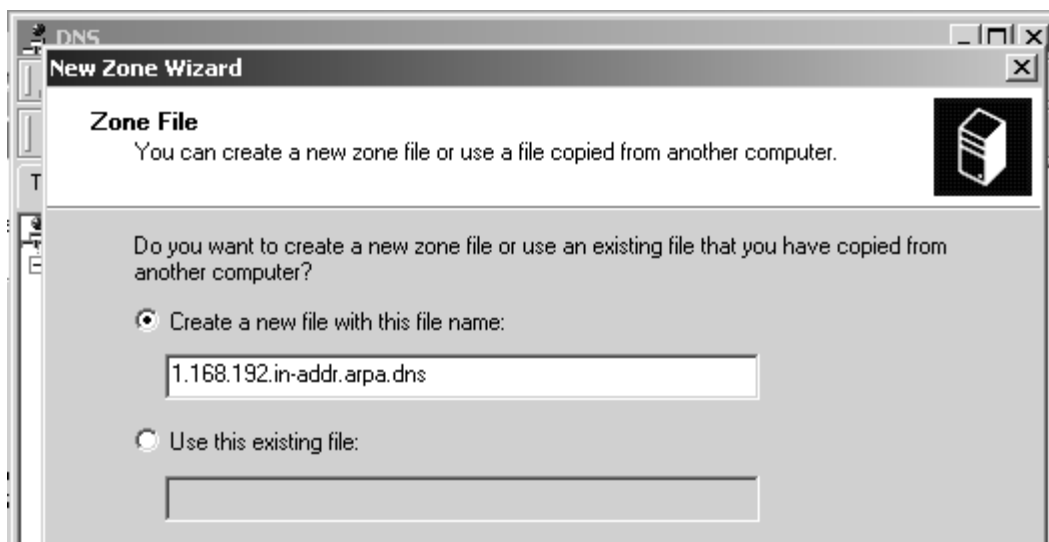
Reverse zóna azonosítása:

A hálózati azonosításhoz meg kell adni a hálózatot. A „Network ID” esetében egyszerűbben, még a „Reverse lookup zone name:” esetében a szabványos formában – ahogy a Linux is használja – adhatjuk meg a hálózatot (4.3.2-3. ábra).



4.3.2-3. ábra.

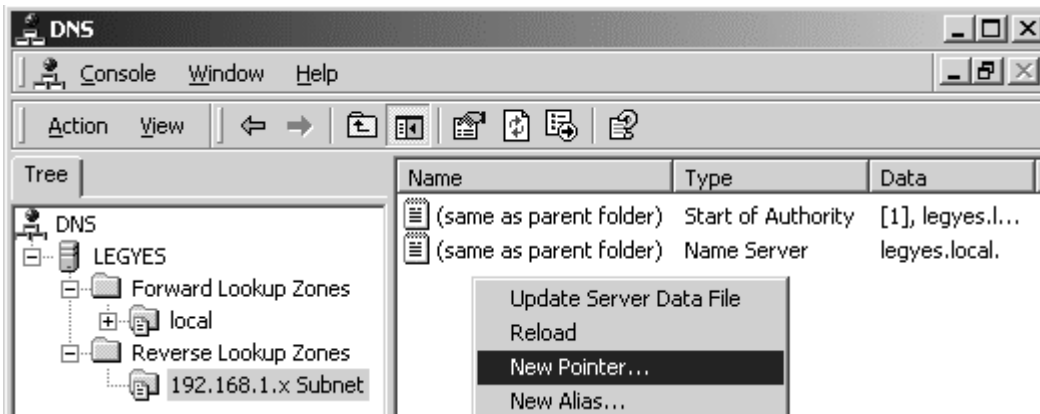
Ha **általános elsődleges típust** használunk, meg kell adni a file nevét, amiben a beállításokat tárolni fogjuk (4.3.2-4. ábra).



4.3.2-4. ábra.

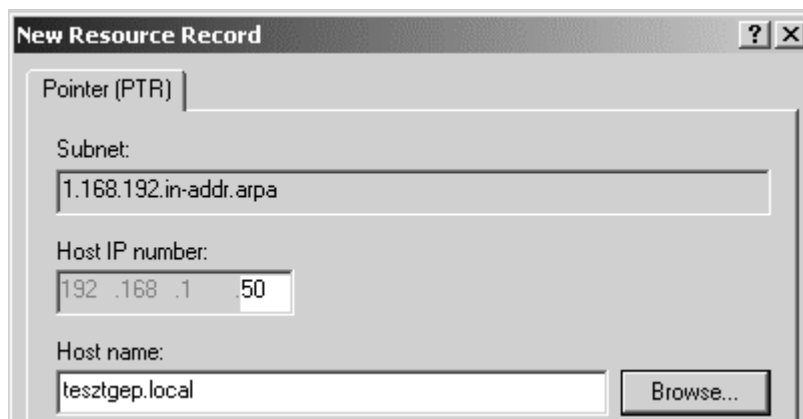
- „Create a new file with this file name” - új file létrehozása a következő névvel
- „Use this existing file” - meglevő file alkalmazása

Az **új reverse** zónában létrehozhatjuk a pointereket. A zónára jobb klikkelve a „New Pointer...” menüponttal tehetjük ezt meg (4.3.2-5. ábra).



4.3.2-5. ábra.

Új pointer hozzáadásakor a „Subnet:” mezőben a hálózat látható, a „Host IP number:” mezőbe pedig az IP címet kell megadnunk, amihez a reverse címet rendeljük. A „Host name:” mezőben megadjuk az IP címhez tartozó nevet. A „Browse” gomb segítségével kiválaszthatjuk a nevet a forward zónában megadottak közül (4.3.2-6. ábra).



4.3.2-6. ábra.

A reverse file tartalma:

```
; Database file 1.168.192.in-addr.arpa.dns for 1.168.192.in-addr.arpa zone.
; Zone version: 2
@           IN SOA legyes.local. admin.local. (
2           ; serial number
900        ; refresh
600        ; retry
```

```
86400 ; expire
3600 ) ; minimum TTL
@ NS legyes.local.
50 PTR tesztgep.local.
```

A beállítások ellenőrzése az „nslookup” parancssori programmal:

```
D:\>nslookup
Default Server: localhost
Address: 127.0.0.1
```

```
> 192.168.1.50
Server: localhost
Address: 127.0.0.1
```

```
Name: tesztgep.local
Address: 192.168.1.50
```

```
>exit
```

4.4. Debian Linux 3.0 stable, DNS szerver:

DNS kiszolgálónak a BIND9 programot alkalmazzuk. Ehhez szükség lehet a dnsutils és a bind9 nevű csomagokra, amit az apt-get install bind9 dnsutils paranccsal tehetünk meg.

4.4.1. DNS zónák hozzáadása

1, Zónák hozzáadása a /etc/bind/named.conf file-hoz:

Ezt a file-t csak a megadott rész után módosíthatjuk. A file végéhez a következő bejegyzést kell hozzáadni:

```
zone "szerver" {
    type master;
    file "/etc/bind/db.szerver";
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.1.168.192";
};
```

A „zone” bejegyzés a zóna azonosítóját tartalmazza, a „file” bejegyzés az adott zónához tartozó beállításokat tartalmazó file helyét adja meg.

4.4.2. DNS forward hozzáadása

2, A névkiszolgáló forward zónájának beállításai a /etc/bind/db.szerver file-ban találhatóak, ennek tartalma a következő:

```
@      IN      SOA    ns.szerver. root.szerver. (
                1          ; Serial
                604800       ; Refresh
                86400        ; Retry
                2419200      ; Expire
                604800 )    ; Negative Cache TTL
;
@      IN      NS     ns.szerver.
@      IN      A      192.168.1.1

cyrix  IN      A      192.168.1.50
```

A hostnevek megadásakor ügyelni kell arra, hogy a host végére pontot tegyünk, ellenkező esetben a szerver kiegészíti a bejegyzést az /etc/hostname file tartalmával.

Az „IN SOA ns.szerver” bejegyzés a domaint adja meg, a „root.szerver” azonos a „root@szerver” –el, ami a rendszergazda email címét tartalmazza, de a DNS szerverekben e-mail cím megadására a „@” karakter nem használható, helyette a „.” karaktert alkalmazzuk. Az „IN NS ns.szerver.” a névkiszolgálót azonosítja, az „IN A 192.168.1.1” pedig a kiszolgáló IP címét adja meg. További bejegyzéseket ezek után tehetünk. A példában a „cyrix.szerver” névhez rendeljük a 192.168.1.50-es IP címet. Ehhez hasonlóan adható hozzá a többi bejegyzés. Működését az „nslookup” és a „dig -x” konzolos parancsokkal ellenőrizhetjük a Windows 2000 Advanced Server -hez hasonlóan.

4.4.3. DNS reverse hozzáadása

3, A reverse zóna beállítása a /etc/bind/db.1.168.192 file-ban található, tartalma:

```
;
$TTL 604800
```

```

@      IN      SOA    ns.szerver. root.szerver. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200     ; Expire
                        604800 )   ; Negative Cache TTL

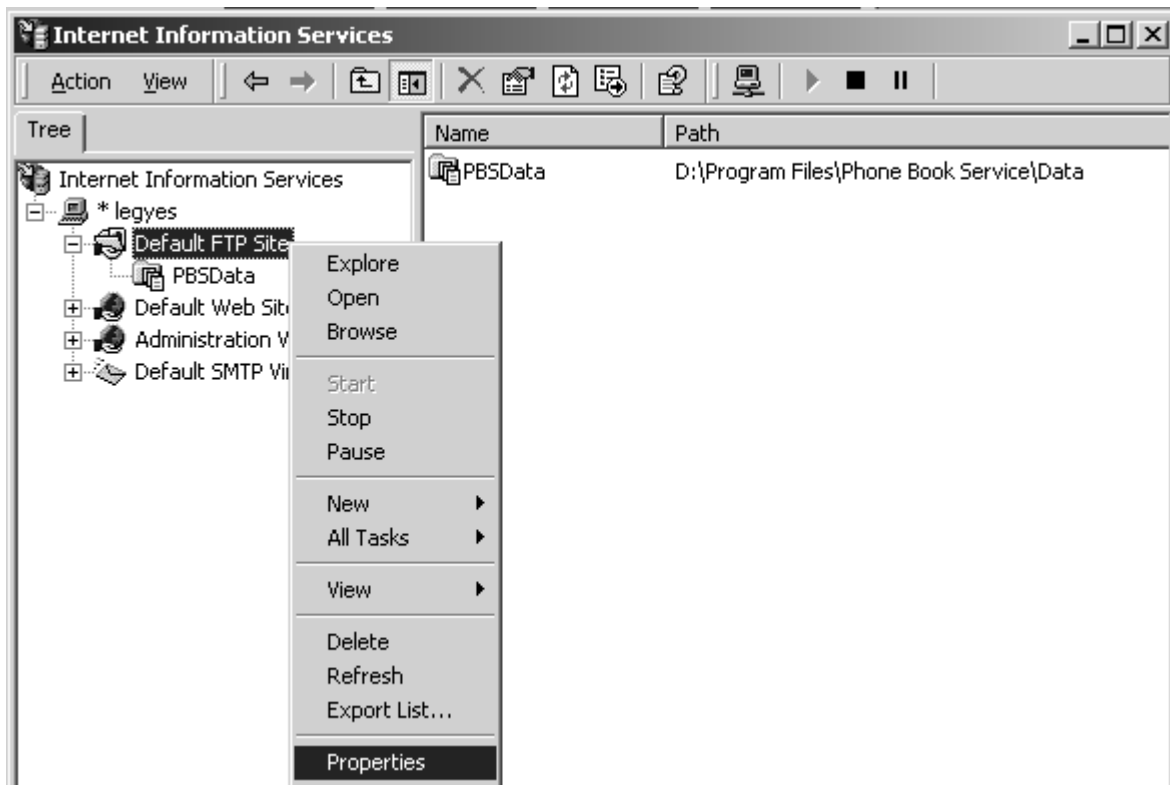
@      IN      NS     ns.szerver.
50     IN      PTR    cyrix.szerver

```

A bejegyzéseket az „IN NS ns.szerver.” sor után adhatjuk hozzá, a példának megfelelően, ahol az „50” az IP címet (192.168.1.50), a „PTR” mutatót, a „cyrix.szerver” pedig az IP címhez tartozó nevet jelenti. További bejegyzéseket a példának megfelelően adhatunk hozzá.

4.5. Windows 2000 Advanced Server, FTP szerver

Az FTP szerver az Internet Information Services (IIS) része, az inetmgr konzol módú paranccsal, vagy a START menü Control Panel / Administrative Tools / Internet Services Manager-el indítható el a beállító-panel. A beépített FTP kiszolgáló nagyon egyszerű program, ajánlott más szoftvercégtől származó, nagyobb tudású FTP program alkalmazása. Az IIS beállító-panelen az FTP szerver tulajdonságait, a „Default FTP Site” menüpontra jobb klikkelve, a „Properties” segítségével konfigurálhatjuk (4.5-1. ábra).

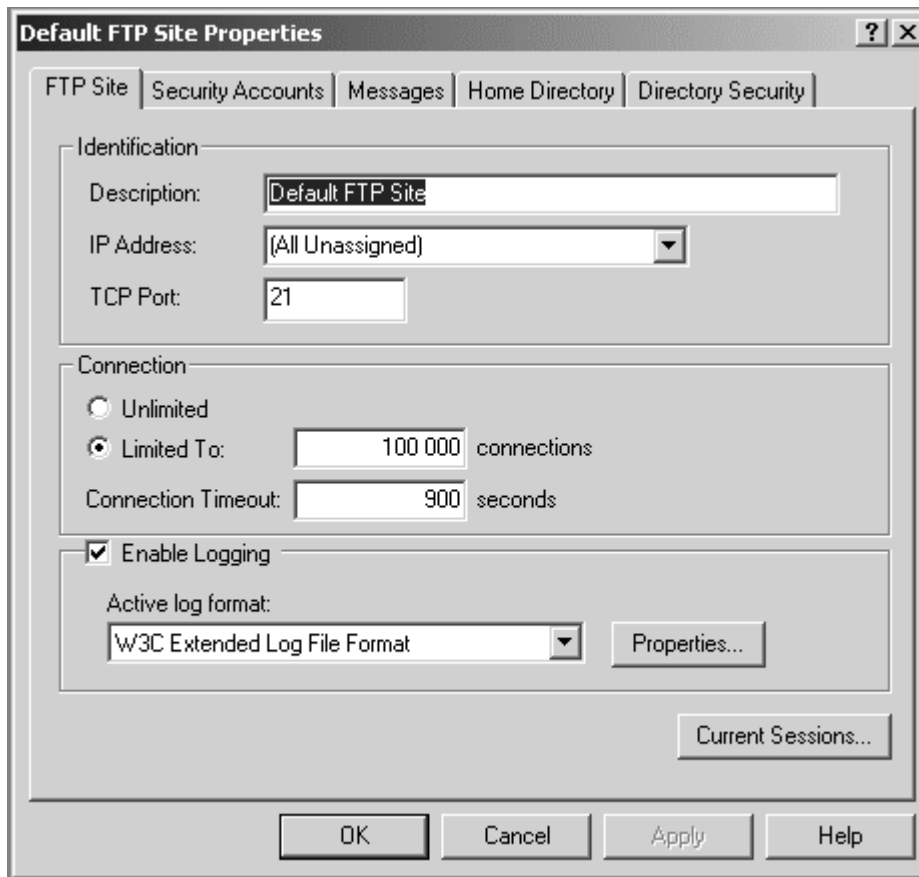


4.5-1. ábra.

4.5.1. „FTP Site” beállítófü

Segítségével megadhatjuk az FTP szerver főbb beállításait (4.5.1-1. ábra).

„Description”	- a szerver megjegyzése
„IP address”	- a szerver IP címe
„TCP port”	- a szerver portja (a szabványos FTP port a 21-es)
„Limited To”	- maximális csatlakozások száma („Unlimited” ha korlátlan)
„Connection Timeout”	- a kapcsolat időtúllépése (ha nincs aktív folyamat)
„Enable Logging”	- naplózás engedélyezése
„Current Sessions”	- kapcsolódások megtekintése, megszüntetése

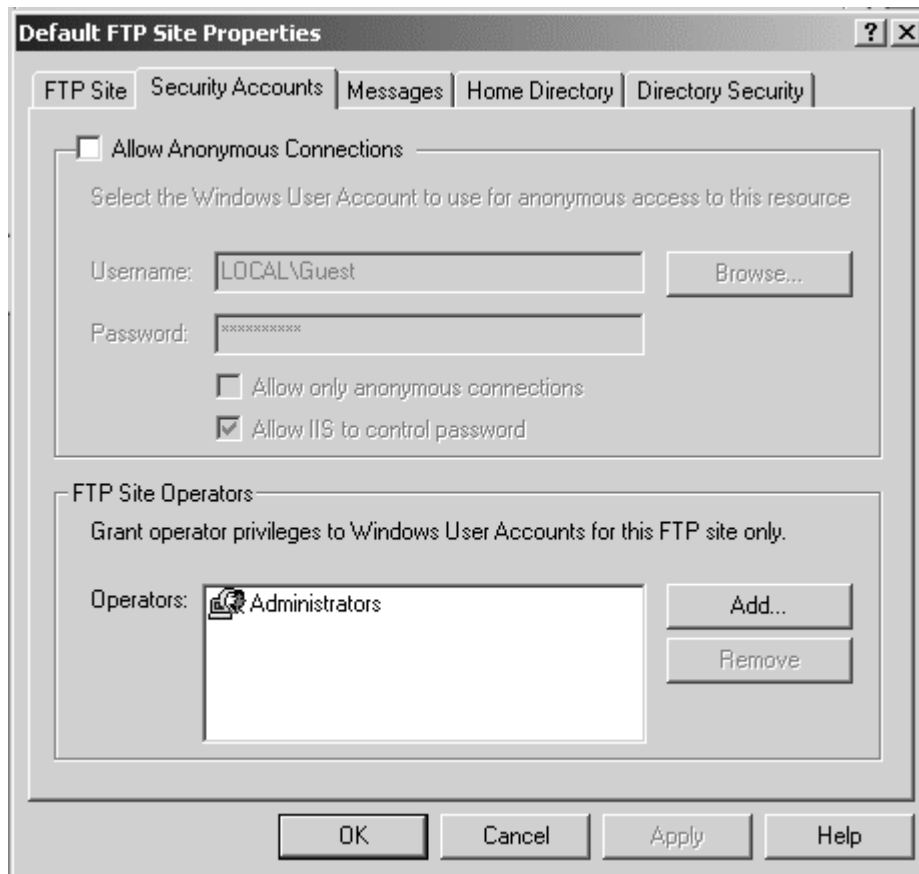


4.5.1-1. ábra.

4.5.2. „Security Accounts” beállítófü

Segítségével engedélyezhetjük névtelenül bejelentkező ügyfelek számára hozzáférést, megadhatjuk milyen felhasználó azonosítójával kezelje az operációs rendszer az ilyen felhasználókat. Amennyiben az „Allow Anonymous Connections” boxot nem jelöljük ki, úgy az operációs rendszeren érvényes felhasználónevek és jelszavak érvényesek a belépéshez.

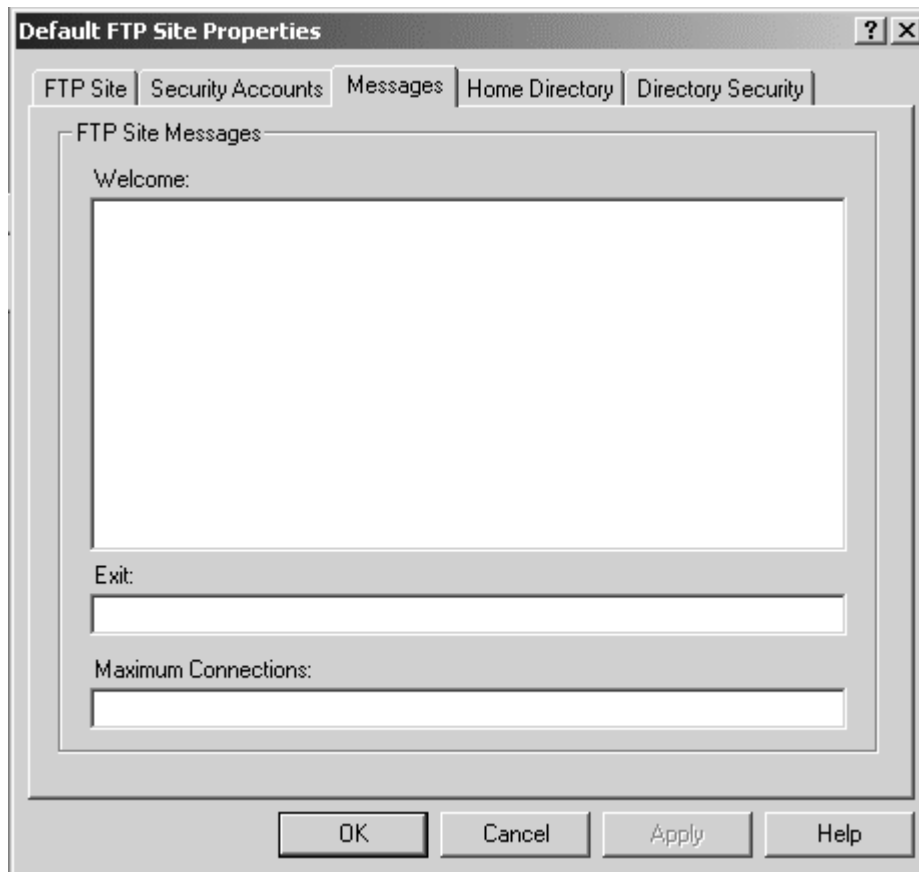
Az „FTP Site Operators” menüpontban megadhatjuk azokat a felhasználókat, akiknek teljes jogú hozzáférése van a szolgáltatáshoz (4.5.2-1. ábra).



4.5.2-1. ábra.

4.5.3. „Messages” beállítófül

A belépéskor megjelenő üdvözlőüzenet (Welcome), kilépéskor megjelenő elköszönés (Exit) és a maximális csatlakozások közlése (Maximum Connections) állítható be (4.5.3-1. ábra).



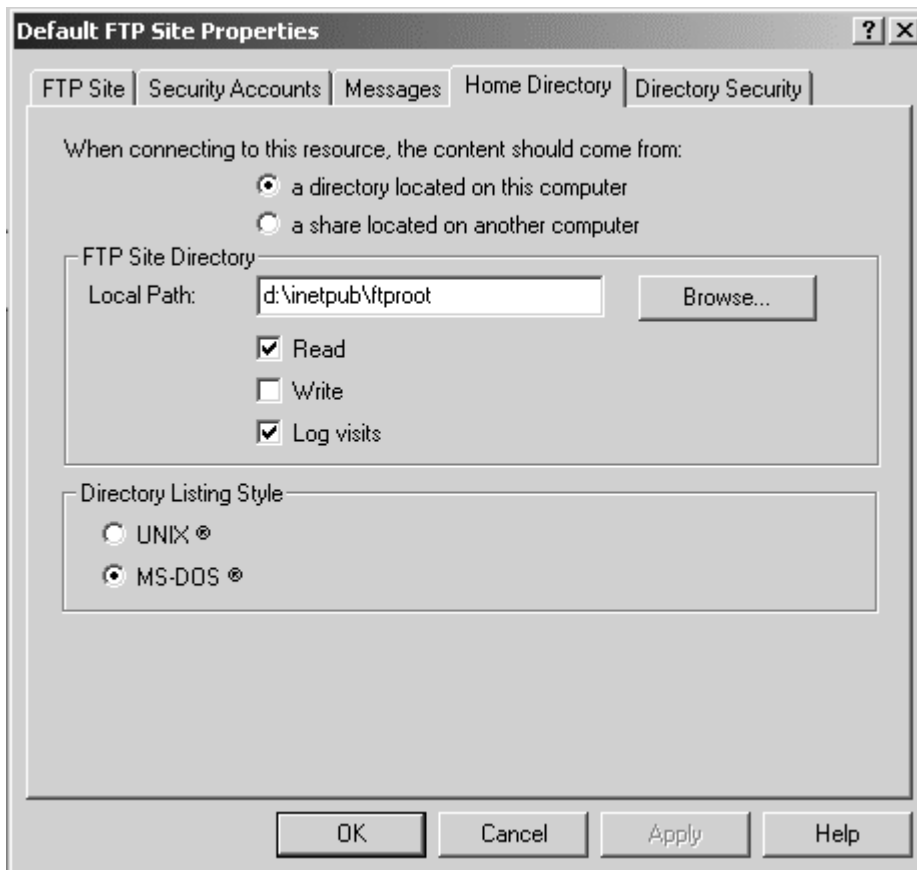
4.5.3-1. ábra.

4.5.4. „Home Directory” beállítófü

Rádiógommbal kiválasztható, hogy a home könyvtár az aktuális kiszolgálón található (a directory located on this computer) vagy egy másik kiszolgálón (a share located on another computer).

Az „FTP Site Directory” menüpontban adhatjuk meg a home könyvtár elérési útját és elérési jogait. Két jog közül választhatunk: olvasás (Read) és írás (Write). A látogatásokat lehetőség van naplózni, ezt teszi lehetővé a „Log visits” box megjelölése.

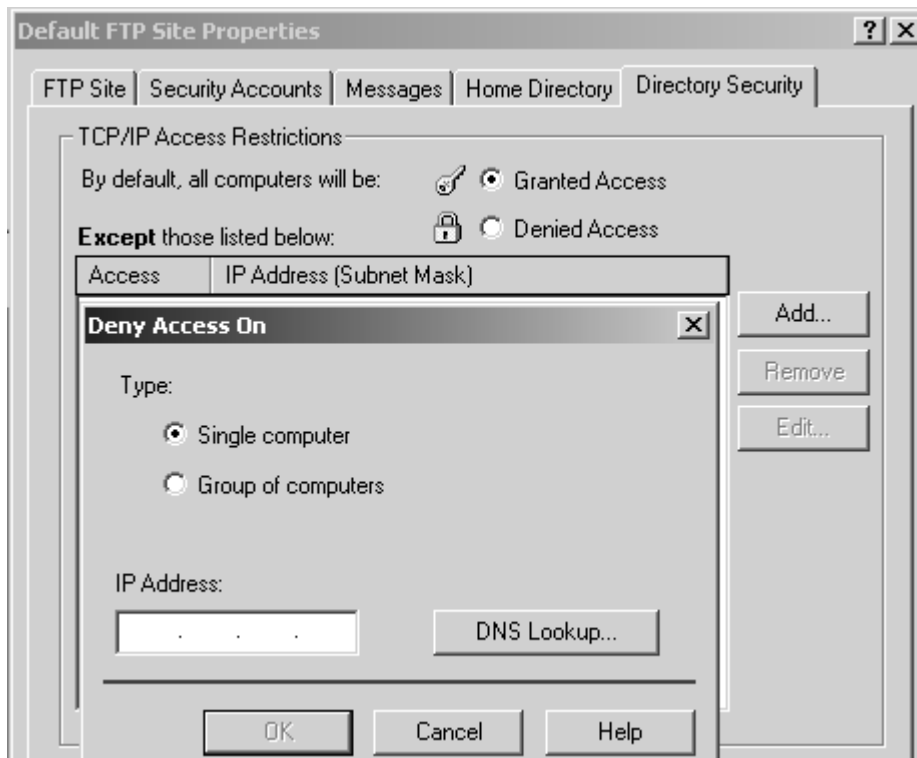
A könyvtárlistázás típusa (Directory Listing Style) lehet MS-DOS vagy UNIX kompatibilis (4.5.4-1. ábra).



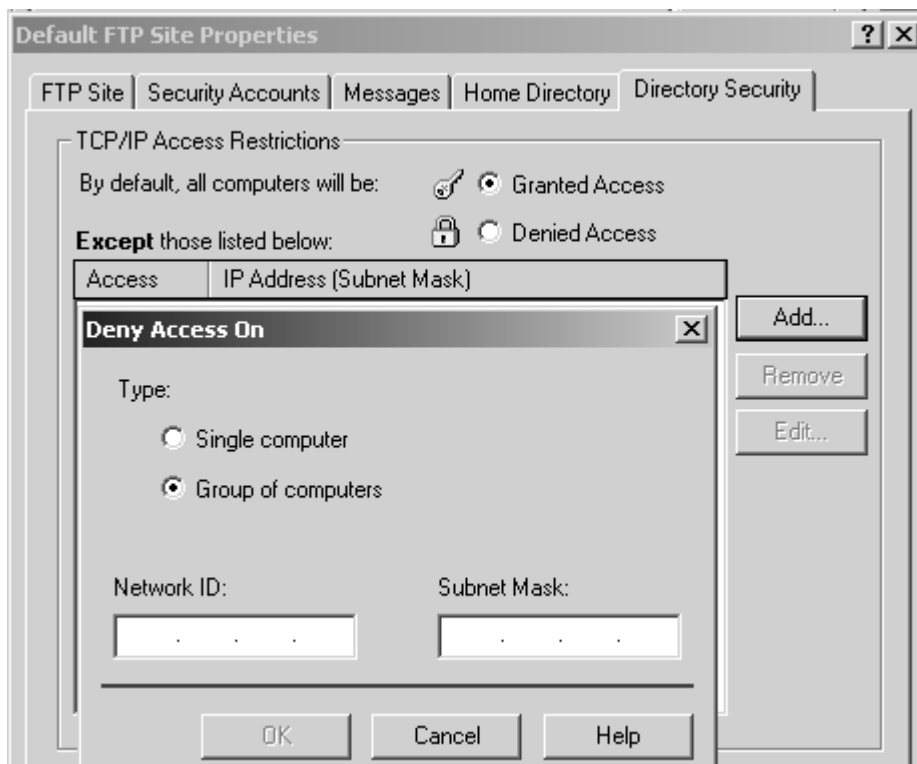
4.5.4-1. ábra.

4.5.5. „Directory Security” beállítófü

Engedélyezhetünk (Granted Access) vagy megtilthatunk (Denied Access) hozzáférést egy számítógép (4.5.5-1. ábra), vagy számítógép csoportok számára (4.5.5-2. ábra), az IP címük alapján.



4.5.5-1. ábra.



4.5.5-2. ábra.

4.6. Debian Linux 3.0 stable, FTP szerver (ProFTPD)

Linux operációs rendszeren a leggyakrabban elfogadott FTP kiszolgáló program a ProFTPD. Nagy tudású FTP szerver, SQL táblából is képes kezelni a konfigurációs beállításokat. A példában egy egyszerű konfiguráció szerepel. A beállításokat tartalmazó file a /etc/proftpd.conf .

A konfigurációs file tartalma

(egyszerű beállítás esetén):

```
ServerName                "ProFTPD Default Installation"
ServerType                standalone
DefaultServer            on
Port                      21
Umask                     022
# maximum number of child processes
MaxInstances              30
# Set the user and group that the server normally runs at.
User                      nobody
Group                     nogroup
# Normally, we want files to be overwriteable.
<Directory /*>
  AllowOverwrite          on
</Directory>
<Anonymous ~ftp>
  User                    ftp
  Group                   ftp
  MaxClients              10
  DisplayLogin            welcome.msg
  DisplayFirstChdir       .message
  UserAlias                anonymous ftp
# Limit WRITE everywhere in the anonymous chroot
<Limit WRITE>
  DenyAll
</Limit>
<Directory uploads/*>
  <Limit READ>
  DenyAll
</Limit>
```

```

    <Limit STOR MKD RMD>
        AllowAll
    </Limit>
</Directory>

</Anonymous>

<Anonymous ~legyes>
User                legyes
Group               legyes
MaxClients          10
# Limit WRITE everywhere in the anonymous chroot
<Limit WRITE>
    AllowAll
</Limit>

<Directory /home/ftp/*>
    <Limit READ>
        DenyAll
    </Limit>
    <Limit STOR>
        AllowAll
    </Limit>
</Directory>

</Anonymous>

```

Ez a konfigurációs file a névtelen bejelentkezők jogait, és a „legyes” nevű felhasználó jogait szabályozza. Névtelen bejelentkezés esetén csak az FTP gyökerében levő uploads könyvtárra van csupán írás, könyvtár létrehozás és törlés joga a kliensnek. De olvasási (letöltési) joga ebben a könyvtárban meg van tiltva. Így elkerülhető, hogy ideiglenes tárhelyként használják az FTP kiszolgálót. A home könyvtárban joga van az olvasáshoz (letöltés) is a kliensnek. Maximálisan 10 kliens csatlakozhat egy időben névtelenül. Bejelentkezett felhasználó esetén a felhasználóneveket, csoportokat, és az ezekhez tartozó jelszavakat (esetleg jogokat) az operációs rendszer kezeli. A példában a felhasználó azonosítója „legyes”, csoportja az operációs rendszerben ugyancsak „legyes”. Ennek a felhasználónak a saját home könyvtárán belül bárhol van írás joga.

Az utasítások jelentése:

„Umask”	- a jogokat meghatározó maszk
„MaxInstances”	- maximális folyamatok száma
„user”	- felhasználónév (PAM)
„group”	- csoport (PAM)
„AllowOverwrite”	- írásjog esetén a felülírás engedélyezése
„<Anonymous /home/ftp>	- a felhasználó home könyvtára
„MaxClients”	- maximum bejelentkezések száma
„<Limit WRITE> DenyAll </Limit>”	- a home könyvtár írásjogának tiltása/engedélyezése
„<Directory uploads/*> <Limit READ> DenyAll </Limit> <Limit STOR MKD RMD> AllowAll </Limit> </Directory>”	- az uploads-on belüli jogok szabályozása READ (olvasás), STOR (írás), MKD (könyvtár létrehozás), RMD (könyvtár törlés), LIST (listázás)

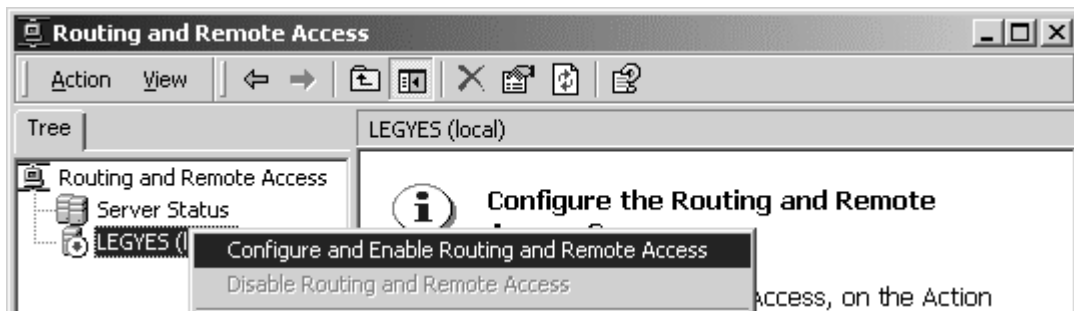
4.7. Windows 2000 Advanced Server, útválasztás és internetmegosztás

A route táblát a parancssori „cmd” parancs futtatásával tekinthetjük meg a legtöbb operációs rendszeren.

A beállítópanelt a „START” menü „Programs /Administrative Tools / Routing and Remote Access” érhetjük el.

4.7.1. Az útválasztás engedélyezése

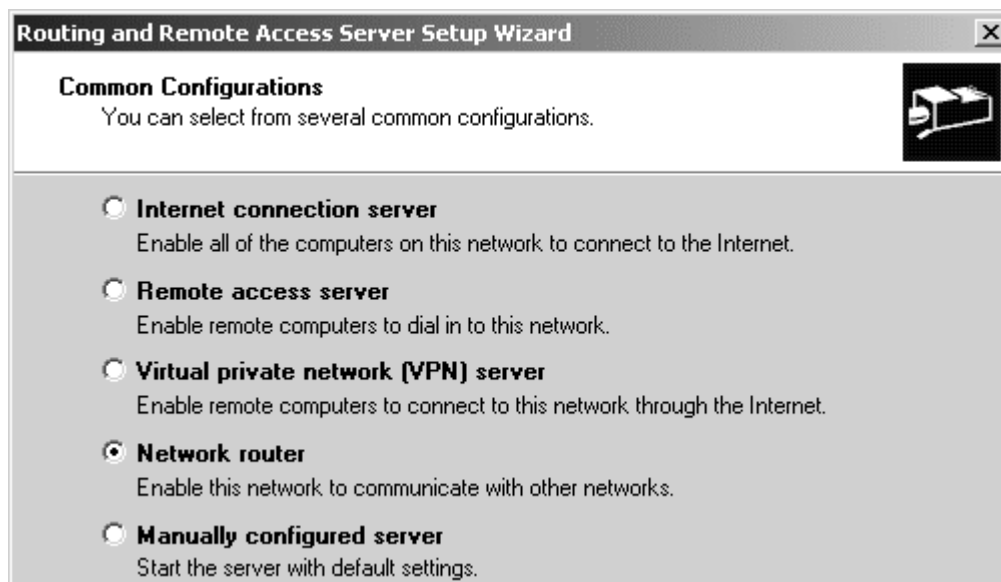
Az útválasztó kiszolgálót úgy engedélyezhetjük, hogy a nevére jobb klikkelve kiválasztjuk a „Configure and Enable Routing and Remote Access” menüpontot. Ekkor egy varázsló ablak ugrik elő, amelyen tovább lépve kiválaszthatjuk az útválasztó kiszolgáló típusát (4.7.1-1. ábra).



4.7.1-1. ábra.

4.7.2. Az útválasztó kiszolgáló típusa:

Példánkban a „Network router” opciót választjuk (4.7.2-1. ábra), majd a hálózati címfordítást manuálisan adjuk hozzá, amennyiben később az Internetet is elérhetővé szeretnénk tenni a kliens gépekről.



4.7.2-1. ábra.

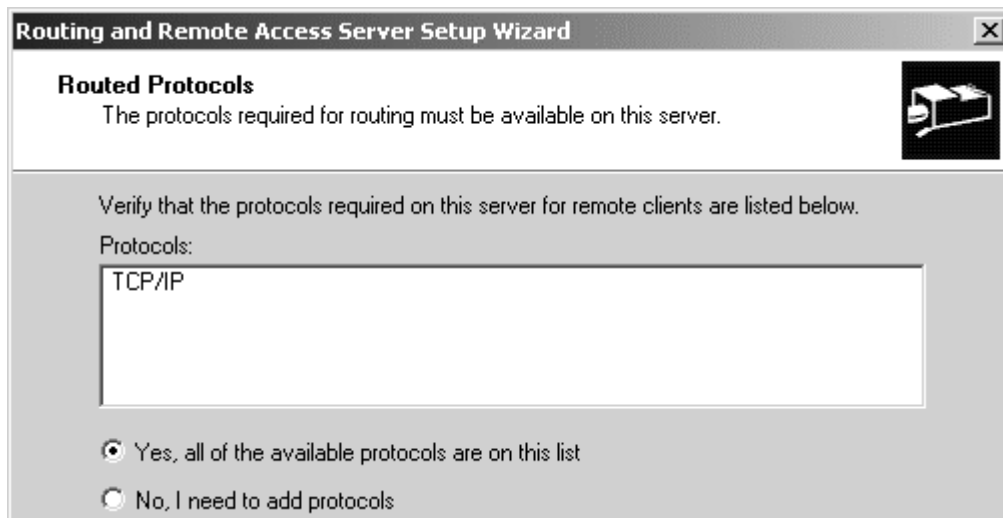
4.7.3. Az útválasztó által használt protokoll beállítása

Mivel a hálózat csak TCP/IP protokollt használ, ezért nem kell megváltoztatni a beállításokat.

„Yes, all of the available protocols are on this list” - minden protokoll szerepel a listán

„No, I need to add protocols” - nem, hozzá szeretnék adni

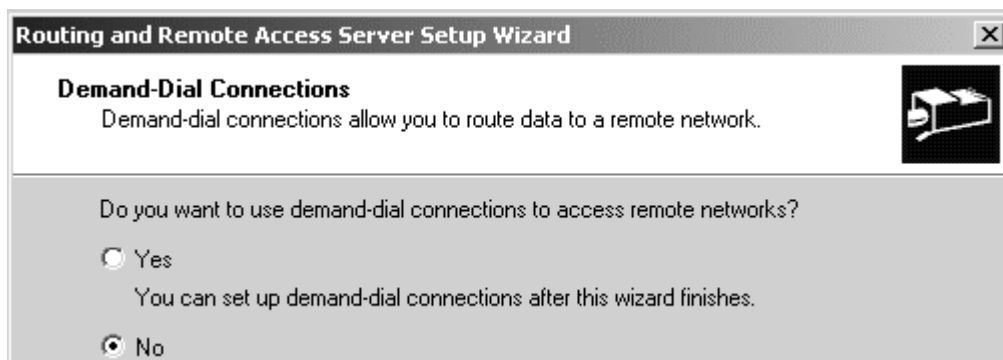
Itt az előbbit kell választanunk, ami az alapértelmezett beállítás (4.7.3-1. ábra).



4.7.3-1. ábra.

4.7.4. Modemes kapcsolat engedélyezése és tiltása

Itt megadhatjuk, ha egy másik hálózat eléréséhez telefonos kapcsolatra van szükség. Mivel nincs ilyen jellegű igény, nem engedélyezzük (4.7.4-1. ábra).



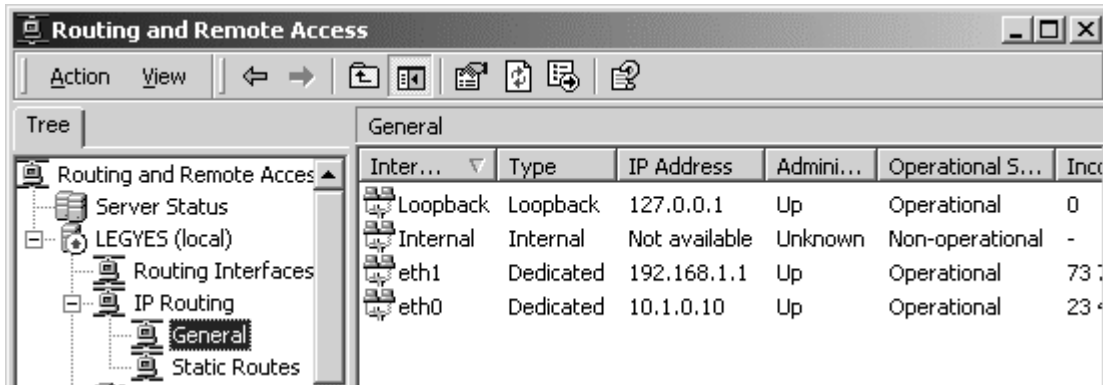
4.7.4-1. ábra.

4.7.5. A beállítások befejezése

A felsorolt beállítások elvégzése után, kis idő elteltével elindul az útválasztó szolgáltatás.

4.7.6. Alapértelmezett beállítások

Az operációs rendszer az interfész IP címe segítségével automatikusan meghatároz egy útválasztó táblázatot. Az interfészek állapota megtekinthető a szervertől belül, az „IP Routing / General” menüpontban (4.7.6-1. ábra).

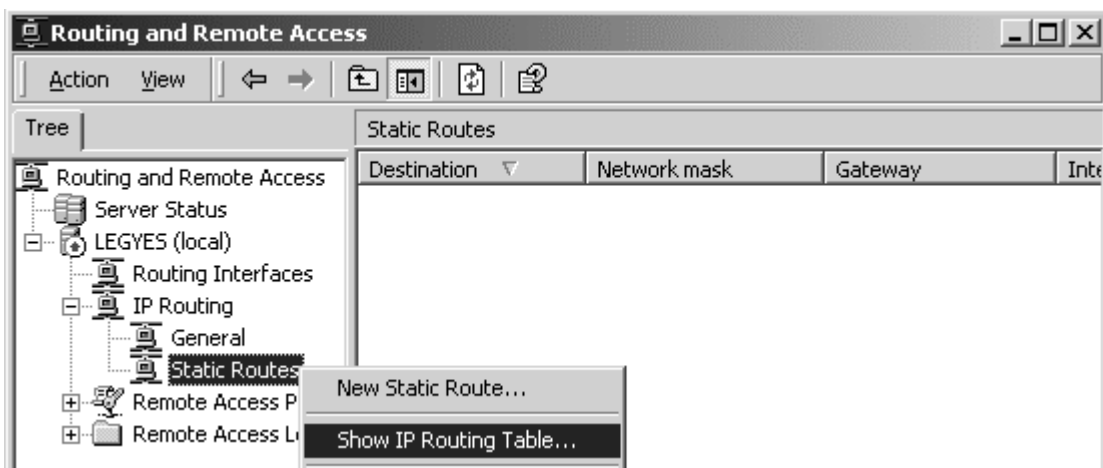


4.7.6-1. ábra.

A példában az eth0 azonosítóval rendelkező interfész egy helyi hálózathoz és az Internethez, az eth1 pedig másik helyi hálózathoz csatlakozik, amely nem rendelkezik Internet hozzáféréssel.

4.7.7. Az útválasztó táblázat megtekintése

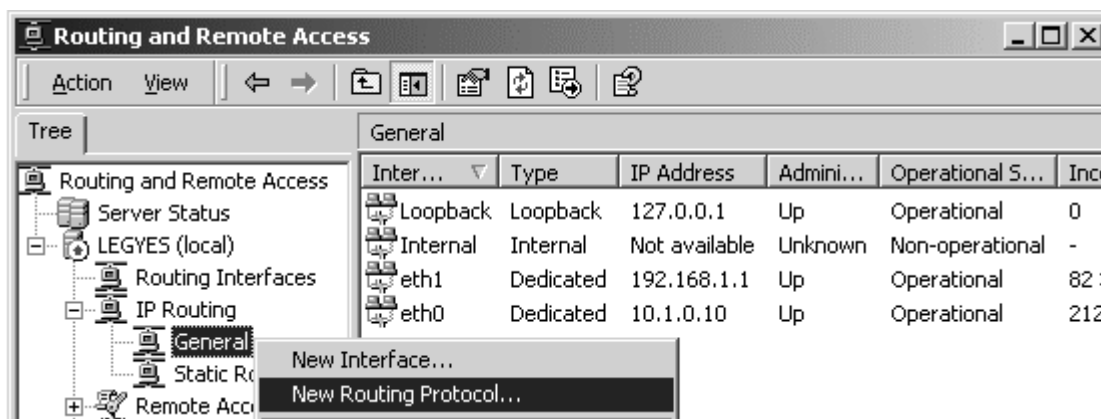
A táblázat megtekinthető a szervertől belül az „IP Routing / Static Routes”-re jobb klikkelve, és ott a „Show IP Routing Table”-t választva (4.7.7-1. ábra).



4.7.7-1. ábra.

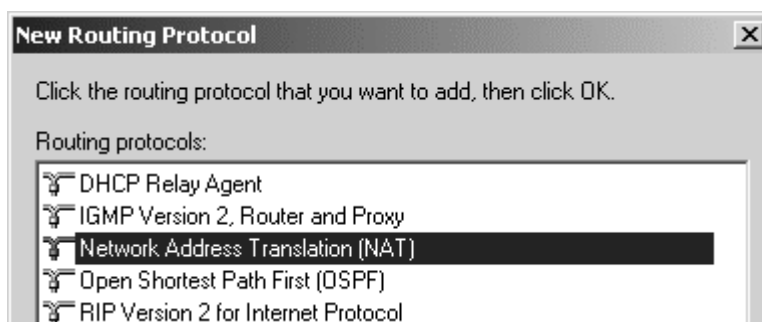
4.7.8. Hálózati címfordítás (NAT) hozzáadása

A hálózati címfordításra szükség van ahhoz, hogy helyi hálózatokról elérhessük az Internetet az útválasztó kiszolgálón keresztül. A címfordítási protokollt a szervertől a „IP Routing / General” menüpontra jobb klikkelve, a „New Routing Protocol” menüpontban tehetjük meg (4.7.8-1. ábra).



4.7.8-1. ábra.

Itt válasszuk a „Network Address Translation”-t (4.7.8-2. ábra).

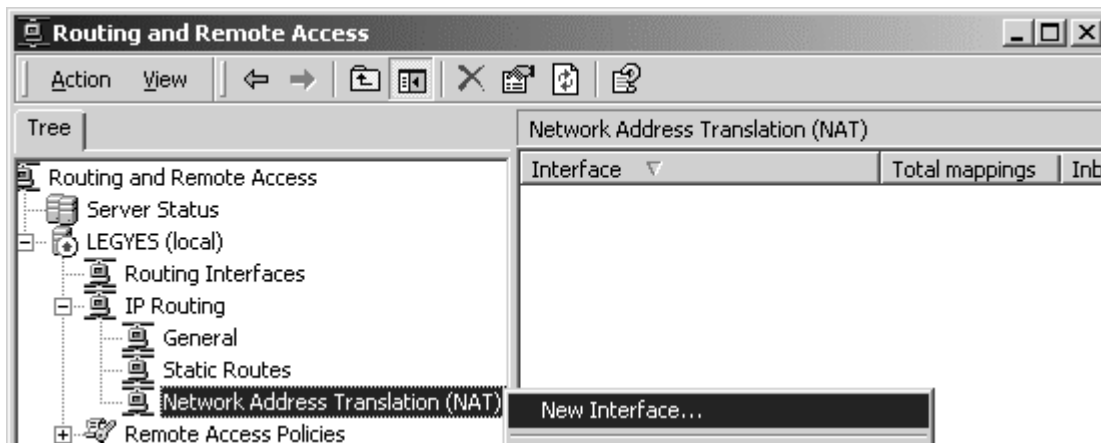


4.7.8-2. ábra.

Ekkor az „IP Routing”-on belül egy új menüpont jelenik meg „Network Address Translation (NAT)” néven.

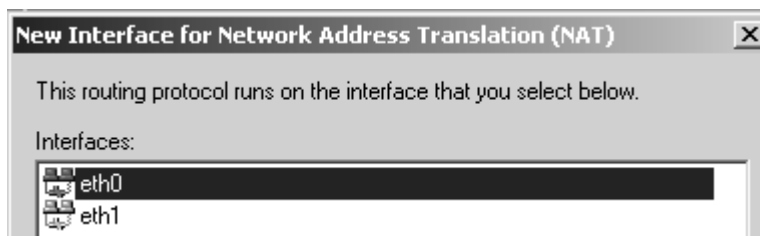
4.7.9. A NAT konfigurálása

A példában az „eth1” csatlóhoz tartozó helyi hálózat Internet elérését szeretnénk biztosítani a „eth0” segítségével, amin keresztül elérhető az Internet szolgáltatás. Ezért a NAT-hoz mindkét interfészt hozzá kell adnunk. Ezt a „Network Address Translation (NAT)” menüpontra jobb klikkelve, a „New Interface” menüponttal tehetjük meg (4.7.9-1. ábra).

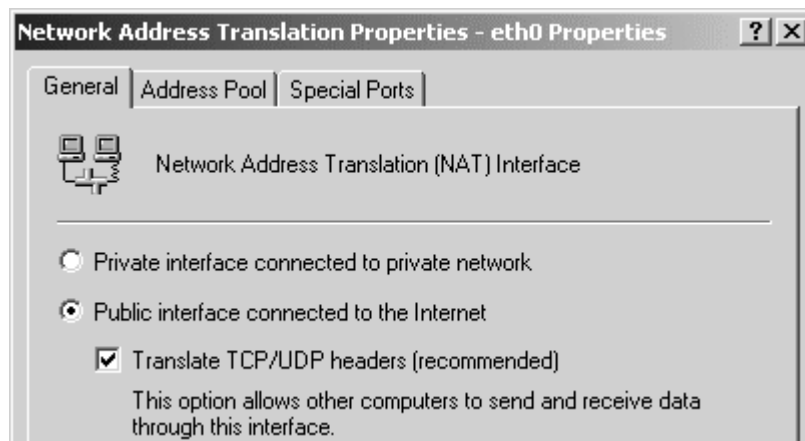


4.7.9-1. ábra.

Az első interfész hozzáadásakor – ami jelent esetben az „eth0” (4.7.9-2. ábra) – meg kell adnunk, hogy ez az interfész az Internethez kapcsolódik (4.7.9-3. ábra).

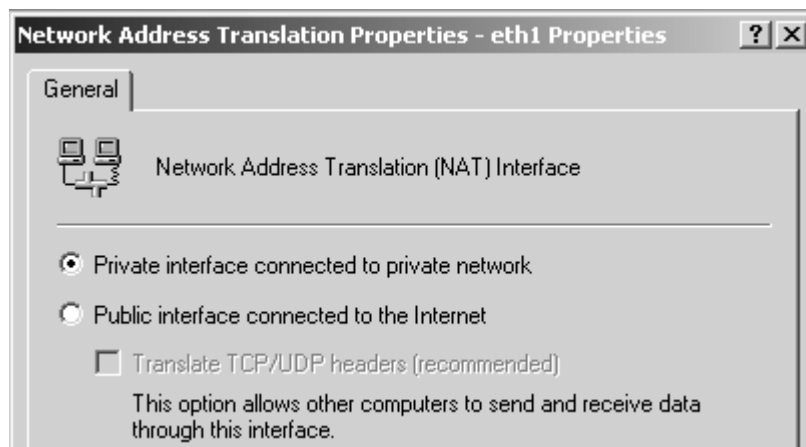


4.7.9-2. ábra.



4.7.9-3. ábra.

A helyi hálózat felé kapcsolódó további interfészeknél – ami jelen esetben az „eth1” – meg kell adnunk, hogy az interfész(ek) a helyi hálózathoz csatlakoznak (4.7.9-4. ábra).



4.7.9-4. ábra.

Végso beállításként gondoskodnunk kell arról, hogy a kliens gépek számára a DHCP kiszolgáló elküldje az útválasztó/átjáró IP címét, valamint célszerű a DNS keresési sorrendben megadni egy internetes DNS kiszolgálót, vagy a DNS kiszolgálóban megadni a további DNS kiszolgálókhöz való csatlakozást.

4.8. Debian Linux 3.0 stable, útválasztás és Internet megosztás

A Linux is törekszik egy automatikus útválasztó táblázat felállításához az interfészek alapján. Ezt a táblázatot a „route” parancs paraméterek nélküli beírásával tekinthetjük meg. A táblázat egyértelműen áttekinthető. A „default” beállítás jelzi azon csomagok útját, amelyre nem létezik továbbítási szabály. Alapértelmezésben példánk útválasztó táblázata a következő:

4.8.1. Az útválasztó táblázat elemei

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	*	255.255.255.0	U	0	0	0	eth1
10.1.0.0	*	255.255.255.0	U	0	0	0	eth0
default	10.1.0.1	0.0.0.0	UG	0	0	0	eth0

- „Destination” - a célhálózat
- „Gateway” - átjáró IP címe, ha nincs megadva, „*” karakter jelöli
- „Genmask” - alhálózati maszk
- „Flags” - beállításokat jelző flag-ek

„lface”

- interfész azonosítója

Az interfészek IP címei a következők:

eth0: 10.1.0.10 (internet kapcsolattal rendelkező helyi hálózat felé)

eth1: 192.168.1.1 (internet kapcsolat nélküli helyi hálózat felé)

4.8.2. Az útválasztó táblázat módosítása

A megfelelő működés érdekében meg kell változtatnunk az útválasztó táblázatot. Bejegyzést eltávolítani, illetve hozzáadni a következő módon lehet:

```
route del -net 192.168.1.0 netmask 255.255.255.0 eth1
route del -net 10.1.0.0 netmask 255.255.255.0 eth0
```

Ahol a „del” a bejegyzés törlését, „-net” hálózat azonosítót, „netmask” alhálózati maszkot, „eth1” pedig interfészt jelent. Ezzel kitöröltük az útválasztó táblázat megadott elemeit. Ezek után hozzáadjuk az új bejegyzéseket úgy, hogy megadjuk a hálózat saját átjáróját is.

```
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1 eth1
route add -net 10.1.0.0 netmask 255.255.255.0 gw 10.1.0.10 eth0
```

Az „add” paraméter jelenti a bejegyzés hozzáadását. Így az útválasztó táblázat a következő lesz:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	lface
192.168.1.0	192.168.1.1	255.255.255.0	UG	0	0	0	eth1
10.1.0.0	10.1.0.10	255.255.255.0	UG	0	0	0	eth0
default	10.1.0.1	0.0.0.0	UG	0	0	0	eth0

4.8.3. Az Internet elérés beállítása

Az iternet elérés megosztásához a Linux egy speciális címtovábbítási módját, a masquerade-t fogjuk használni. Ezt az ipchains vagy iptables segítségével tehetjük meg. Mindkét parancshoz kernel szintű támogatás kell. Az iptables használata bonyolultabb, de hatalmas tudású. Természetesen itt is szükség van a DNS szerverek megfelelő beállítására. A DNS kiszolgáló /etc/bind/named.conf nevű konfigurációs állományában a forwarders részénél meg kell adnunk internetes DNS kiszolgálókat. Valamint engedélyeznünk kell az

IP cím továbbítást a `/proc/sys/net/ipv4/ip_forward` file-ba „1”-et írva. (`echo 1 > /proc/sys/net/ipv4/ip_forward`) Az egyszerűség végett az `ipchains` segítségével állítjuk be az internet megosztást:

```
ipchains -A forward -j MASQ -s 192.168.1.0/24
```

A parancs egyszerű jelentése az, hogy a továbbítást maszkolja a 192.168.1.0 hálózatról érkező csomagok esetében. Itt az alhálózat megadása bitszámmal történik, azaz a 24 bit tulajdonképpen a 255.255.255.0 címet jelenti. Az `ipchains` segítségével szabályokat adhatunk meg a hálózati forgalom beállításaihoz. Ezért tűzfalként is használható. A kernel szintű tűzfal nagy fokú biztonságot garantál megfelelő beállítások esetén.

5. Befejezés

A **hardware igényekből** látható, hogy a Linux sokkal jobb választás a Windows-nál, ez utóbbi rendkívül nagy erőforrás igényvel rendelkezik. Az esetleges új típusú Windows NT szerverre való frissítés további nagy mértékű erőforrás igénynövekedést jelent.

Gazdaságossági szempontból nem lehet egyértelmű sorrendet felállítani, ugyanis a megfelelő Linux szakemberek költsége igen magas a Windows szakemberekéhez képest; viszont több szerver, vagy sok kliens esetében a Windows szoftver licenc költségei hatalmasak. További programok telepítése esetén Linux operációs rendszeren nagyon valószínű, hogy találunk az igényeinknek megfelelő ingyenes programot, ezzel szemben Windows-t használva erre kicsiny az esély.

A beállítások szempontjából a Linux sokkal finomabb beállításokat tesz lehetővé, ezáltal pontosabban beállítható, viszont a kiszolgáló programok magasabb szintű ismeretét teheti szükségessé. Windows-t használva szükség lehet más gyártótól származó – ugyancsak költséges – kiszolgáló programot alkalmazni, ha a szervert jobban ki akarjuk használni. Kezelése a Linux nagy bonyolultságát tekintve jóval egyszerűbb, a konfigurációs állományok tartalmát legtöbbször csak grafikus formában, felhasználóbarát módon láthatjuk.

Biztonsági szempontot tekintve a Linux egyértelmű fölényt élvez a Windows-zal szemben. Kernel szintű tűzfala jóval nagyobb mértékű szűréseket tesz lehetővé, a kernel részeként sokkal nagyobb biztonságot garantál. Távoli bejelentkezést használva igénybe vehetünk titkosított SSH protokollt, aminek sávszélesség igénye elhanyagolható a Windows távoli adminisztrációs programjaihoz képest. Windows esetében konzolos (kis sávszélesség igényű) beállítást, csak telnet segítségével végezhetünk, ami könnyű hozzáférést jelent a rendszergazda jelszávához. A Windows egyértelmű biztonsági hátrányát a vírusok, trójai programok, férgek és hasonló kártékony programok nagy száma okozza erre az operációs rendszerre. Sőt, mivel az egész operációs rendszer alapja egy webböngésző, ez további nagy mértékű sebezhetőséget tesz lehetővé. A biztonsági hibák javítása Linux esetén 48 órán belül garantált, még Windows esetében határozatlan idejű.

Felhasznált irodalmak

Rendszerkövetelmények:

[1] Internet – Windows 2000 Advanced Server és Debian Linux 3.0 stable rendszerigénye a CD mellékleten:

szakirodalom\A Windows 2000 Server család rendszerfeltételei.htm

szakirodalom\install_en.pdf

Fizikai megvalósítás:

[2] Holczer József - Benkovics Viktor – A Windows 2000 Server, Internet és Intranet (ISBN 963009338-3), Jedlik Oktatási Stúdió 2002

[3] Internet – TCP/IP alapok a CD mellékleten:

szakirodalom\tcpip_alapok.doc

szakirodalom\linux_halozat.pdf

Szoftveres megvalósítás:

[4] Holczer József - Benkovics Viktor – A Windows 2000 Server, Internet és Intranet (ISBN 963009338-3), Jedlik Oktatási Stúdió 2002

[5] Kis Balázs – Windows 2000 Server rendszergazdáknak (ISBN 9639131318), Szak kiadó 2001

[6] Internet – DNS, DHCP, FTP, ROUTING, NAT, MASQ a CD mellékleten:

szakirodalom\DHCP Server Setup for Linux.htm

szakirodalom\DNS - elv és konfiguráció.htm

szakirodalom\IP Masquerade.htm

szakirodalom\man dhcpd_conf.htm

szakirodalom\Proftpd full manual.htm

szakirodalom\Routing.htm