

**Internetes szolgáltatások**

**TÁMOP 2.2.3-09/1-2009-0010**



**SZÉCHENYI ISTVÁN**  
Térségi Integrált Szakképző Központ



**Szerkesztette: Vinnai Zoltán**

**Lektorálta: Domonkos Sándor**

A kiadvány a Széchenyi István Térségi Integrált Szakképző Központ fejlesztése TÁMOP 2.2.3-09/1-2009-0010 projekt keretén belül készült.



A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg

## TARTALOMJEGYZÉK

1.	A modul célja .....	4
2.	Előzetes feltételek.....	4
3.	Előzetes tudás elismerésének és beszámításának módja.....	4
4.	1. lecke: A szolgáltatások áttekintése 1.....	4
5.	2-3. lecke: A szolgáltatások áttekintése 2.....	8
6.	4. lecke: Windows Web szolgáltatás .....	12
7.	5-6. lecke: Windows Web szerver beállítás .....	14
8.	7-8. lecke: Windows FTP.....	16
9.	9. lecke: I. témazáró feladatsor .....	19
10.	10. lecke: Windows DHCP .....	21
11.	11. lecke: Windows WINS .....	25
12.	12-13. lecke: Windows DNS .....	28
13.	14-15. lecke: Windows DNS saját zóna beállítása, kezelése .....	31
14.	16. lecke: II. témazáró feladatsor .....	37
15.	17-18. lecke: Egy gép, két hálózat .....	39
16.	19-20. lecke: Windows NAT.....	43
17.	21-22. lecke: Windows Proxy .....	45
18.	23. lecke: Windows e-mail .....	52
19.	24-25. lecke: Windows e-mail 2.....	56
20.	26. lecke: III. témazáró feladatsor .....	59
21.	27. lecke: Összegző felmérés .....	61
22.	Értékelés, feladatmegoldások .....	63
23.	Irodalomjegyzék.....	64

## **1. A modul célja**

A modul célja, hogy a tanuló ismereteket szerezzen a számítógép-hálózatok legfontosabb hálózati szolgáltatásainak (web, FTP, DNS, DHCP stb.) szerepével, jellemzőivel, alkalmazási területükkel kapcsolatban. A tanuló a modul elsajátítása után képes lesz a web, FTP, DHCP, WINS, NAT, Proxy és e-mail szolgáltatások telepítésére, beállítására és használatára.

## **2. Előzetes feltételek**

A modul elsajátításához szükség van a Hálózati alapismeretek és a Hálózati operációs rendszerek modul sikeres teljesítésére.

## **3. Előzetes tudás elismerésének és beszámításának módja**

A tanuló előzetes tudását a tananyagban található témazáró feladatsorok és a tananyag végén található Összegző felmérés segítségével mérjük. Amennyiben az Összegző felmérést első próbálkozásra legalább 80%-os eredménnyel végzi el, a tanuló számára a modul elvégzése alól felmentés adható. Amennyiben nem éri el a 80%-os eredményt, akkor a sikeres közbelső témazáró feladatsorok alapján az órák meghatározott részeinek látogatása alól adható felmentés. Ebben az esetben a tanuló számára az Összegző felmérés ismételt kitöltése kötelező.

## **4. 1. lecke: A szolgáltatások áttekintése 1**

### **4.1 Részcélkitűzések**

A tanuló ismerje meg az internetes szolgáltatásokkal kapcsolatos alapfogalmakat. Legyen tisztában a webszerver szolgáltatások legfontosabb alapelveivel, működési módjaival. Értse a statikus és dinamikus oldalak közötti különbséget. Ismerje a webszerver szolgáltatás által használt portokat, protokollokat. Legyen tisztában az FTP szolgáltatás szerepével, működésével, az anonymous FTP fogalmával és a használt portszámokkal.

Értse a DHCP szerver szerepét, működését, illetve ismerje a DHCP protokollok által használt portokat.

## **4.2 Bevezetés**

Az internetes szolgáltatások elnevezés olyan szolgáltatásokat takar, amelyeket az interneten keresztül is el lehet érni. Ez azonban nem jelenti azt, hogy a használatukhoz minden esetben szükség van az internetelésre. Mindegyik szolgáltatás megvalósítható internetelés nélküli helyi hálózaton is.

A szolgáltatásokat nyújtó számítógépeket szervereknek, kiszolgálóknak nevezik, míg a szolgáltatásokat igénybe vevő számítógépeket klienseknek vagy munkaállomásoknak nevezik.

## **4.3 Webszerver szolgáltatások**

Ma már ez az egyik legáltalánosabb szolgáltatás. Lényege, hogy sajátos protokollon (HTTP – HiperText Transfer Protocol) keresztül biztosít hozzáférést különböző állományokhoz a felhasználók számára. Ebben az esetben a felhasználók gépein csak egy teljesen szabványos böngészőprogramra van szükség. A webszerver az internet elterjedésével kapott egyre nagyobb létjogosultságot, de alkalmazásához nincs szükség magára az internet elérésére. A webszerver szolgáltatás helyi hálózaton is alkalmazható, hiszen egyre több szolgáltatás (program) érhető el webes felületen keresztül is.

Az egyszerű statikus HTML oldalakból egyre kevesebb van, ma már inkább a dinamikusan előállított oldalak kerültek előtérbe. Ez azt jelenti, hogy a kliens számítógép által kért oldal tartalma a kérés beérkezésekor kerül előállításra magán a szerveren, és a kliens csak ezután kapja meg. Az oldal tartalma tehát minden lekérdezéskor dinamikusan változhat, aktuális információkat tartalmazva minden időpillanatban.

A szerveroldali feldolgozásra több lehetőség is van. Például:

- CGI,
- ASP,
- ASP.NET,
- PHP.

Manapság ezek közül a legelterjedtebb a PHP. A PHP egy C nyelvhez nagyon hasonló szintaktikájú, elsősorban weboldalak dinamikus előállítására szolgáló programozási nyelv. A PHP egy nyílt forráskódú, szabadon használható nyelv, ami ráadásul platformfüggetlen, gyakorlatilag minden rendszerben rendelkezésre áll.

A dinamikus oldalak legtöbbször valamilyen adatbázishátteret is használ az adatok tárolására. A legáltalánosabb adatbázis erre a célra a MySQL. Ez is nyílt forráskódú, így bárki szabadon használhatja, és elérhető minden rendszerre.

Windowsos környezetben az MSSQL adatbázis-környezet is rendelkezésre áll.

Elmondható, hogy a weboldalak tárolására szolgáló rendszereknél ma már legalább három összetevőre van szükség:

- magára a web szerverre,
- egy dinamikus oldalak előállítására szolgáló kiegészítőre,
- és egy adatbázisra.

Általános esetben az ingyenes webszerver az Apache, az adatbázis MySQL és a kiegészítő PHP. A három elem kezdőbetűit összeolvasva kapjuk az AMP-t. Több szabadon elérhető AMP rendszert találhatunk, akár Windows alá is, például:

- WAMP,
- XAMMP.

A web szolgáltatás a 80-as tcp portot használja alapértelmezésben, de a szerveren bármilyen portot hozzá lehet rendelni. Ha más portszámon mű-

ködik a webszerver, akkor a böngészőben is meg kell határozni azt úgy, hogy a szerver címe után „:portszám”-ot írunk.

Lehetőség van titkosított kapcsolat létesítésére is a webszerver és a kliens között. Ilyenkor harmadik fél nem tudja értelmezni az adatokat, mert az adatok titkosítva haladnak a kliens és a szerver között. Ezt a szolgáltatást nevezik HTTPS szolgáltatásnak, ahol az „S” a „Secure” (titkosított) átvitelre utal. Akkor használják, ha az átvinni kívánt adatok érzékenyek, mint például a jelszavak. Ezt a szolgáltatást alapesetben a 443-as tcp porton lehet elérni.

#### **4.4 FTP (File Transfer Protocol – fájl átviteli protokoll) szerver szolgáltatás**

Ez is egy általánosan használt internetes szolgáltatás, amely szintén állományok elérését biztosítja FTP protokollon keresztül, azonban további fájlkezeléssel kapcsolatos műveleteket is megenged, mint a törlés, az átnevezés vagy a könyvtárkezelés (létrehozás, átnevezés, törlés), jogosultságok beállítása stb. A web szolgáltatáshoz képest az FTP nemcsak letöltést enged, hanem lehetővé teszi a feltöltést is. Az FTP szolgáltatás használatára bármilyen szabványos FTP program alkalmas.

Az FTP hozzáférésnél a felhasználónak minden esetben azonosítania kell magát, vagyis meg kell adnia egy felhasználónevet és egy jelszót.

Speciális FTP szolgáltatásnak tekinthető az „Anonymous FTP”, ahol a felhasználói név minden esetben az „anonymous”, míg a jelszó tetszőleges lehet. Jellemző módon e-mail címet várnak el, azonban ez sem kötelező, sok helyen jelszó nélkül is csatlakozni lehet. Amikor böngészővel csatlakozunk egy FTP kiszolgálóhoz, az többnyire anonymusként azonosítja magát.

Az FTP szolgáltatás alapértelmezésben a 21-es tcp portot használja. Persze ezt is be lehet állítani más, magasabb portszámra.

## **4.5 DHCP (Dynamic Host Configuration Protocol – dinamikus átlomáskonfiguráló protokoll) szolgáltatás**

IP-alapú hálózatokban dinamikus IP-cím kiosztást megvalósító szolgáltatás.

A szerverek rendelkeznek egy IP-cím tartomány felett, és a saját nyilvántartásuk alapján kioszthatják ezeket a címeket a munkaállomások részére. A kiosztott IP-címek azonban csak bérbeadásra kerülnek, vagyis csak egy adott ideig használhatók a munkaállomások által. Ez az idő a bérleti idő (lease time), aminek lejártá előtt a munkaállomás hosszabbítást kérhet.

Egy DHCP szerverrel az is megoldható, hogy egy adott számítógép mindig ugyanazt az IP-címet kapja a DHCP szervertől. Ilyenkor a kliens gép MAC címe alapján tudja kiosztani az IP-címet. Ezt nevezik statikus kiosztásnak.

A kliens számítógépek indulásnál nem rendelkeznek semmilyen hálózati beállítással, azonban a DHCP kiszolgálóktól kérhetnek IP-címet. A kiszolgálók pedig felajánlhatnak a saját – még szabad – készletükből egyet, amelyet a kliens elfogadhat.

Az IP-cím mellett a munkaállomások rendszerint a következő hálózati beállításokat is megkapják:

- netmaszk,
- alapátjáró címe,
- DNS kiszolgálók címei.

A DHCP protokoll a 67-es udp porton kommunikál.

## **5. 2-3. lecke: A szolgáltatások áttekintése 2**

### **5.1 Részcélkitűzések**

A tanuló legyen tisztában a Windows környezetben használatos névfeloldás elméletével. Értse a WINS szolgáltatás előnyeit, alkalmazási korlátait. Ismerje a DNS szolgáltatás jelentőségét, a domainnevek szerepét, felépítését, a zóna fogalmát, a használt portcímeket. Ismerje a NAT szolgáltatás szükségességét, működését. Ismerje a tűzfal fogalmát, szerepét. Ismerje az elektronikus levelezéssel kapcsolatos legfontosabb fogalmakat, vala-



mint a szolgáltatások által használt alapértelmezett protokollokat és portcímeket.

## **5.2 WINS szolgáltatás**

A WINS szolgáltatáshoz tisztában kell lenni azzal, hogy minden windowsos gépnek van egy rövid neve, az úgynevezett NetBIOS név. Windowsos környezetben a számítógépek ezen név alapján azonosítják a gépeket. A hálózati kommunikáció azonban IP-cím alapján történik, így szükség van egy olyan szolgáltatásra is, ami névből IP-címet tud előállítani.

A WINS (Windows Internet Name Services – Windows Internetes Névservicek) a Windows operációs rendszerek beépített szolgáltatása, ami a helyi hálózaton gondoskodik a gépek neveinek IP-címekké történő átfordításáról, azaz a névfeloldásról.

WINS szolgáltatás nélkül a gépek ilyen esetben szórású üzenetekkel bombázzák a hálózatot, ha keresnek egy névhez tartozó IP-címet.

Ha a hálózati beállításoknál WINS szerver van megadva, akkor közvetlenül a szerverhez fordulnak a kérésekkel, csökkentve a hálózati forgalmat. A Windows rendszerek ilyen esetekben elindulásuk után elküldik a WINS kiszolgálónak a saját nevüket és IP-címüket, a WINS szerver pedig tárolja azokat.

Fontos azt is megjegyezni, hogy tartományi környezetben a WINS felesleges, mivel a Active Directory DNS szervere végzi el a névfeloldást.

## **5.3 DNS (Domain Name Service – domain név szolgáltatás) szolgáltatás**

Az alapvető internetes szolgáltatás az IP-címek és domainnevek összerendelését biztosítja. Ma már nélkülözhetetlen ez a szolgáltatás az interneten, mivel minden weboldalt név (pl. [www.index.hu](http://www.index.hu)) szerint érünk el.

A DNS kiszolgálók saját adatbázist tartanak fent az általuk delegált IP-címek és domainnevek kapcsolatainak nyilvántartásához. Ha egy kliens egy domainnévhez tartozó IP-címet keres, akkor a hálózati beállításaiban

szereplő DNS kiszolgálóhoz fordul a kéréssel, aki vagy azonnal tudja a választ a saját adatbázisa alapján, vagy másik DNS kiszolgálóhoz fordul a kéréssel.

A DNS szervernek lehet saját zónája, ami azt jelenti, hogy definiálhatunk egy egyedi tartománynevet, amelyben felsorolhatjuk a tartományba tartozó gépek neveit a hozzá tartozó IP-címekkel együtt. Ha a DNS szerver nyilvános, vagyis az interneten keresztül bárki elérheti, akkor a tartományt be kell jegyeztetni valamely arra jogosított szolgáltatónál.

A csak helyi hálózaton elérhető DNS kiszolgálók esetén bármilyen tartománynevet használhatunk, de megegyezés szerint ilyenkor a TLD mindig „local”, például „szemere.local”, megkülönböztetve az internetes TLD-ktől.

A DNS szolgáltatás az 53-as tcp és udp portokat használja.

#### **5.4 NAT (Network Address Translation – hálózati címfordítás) szolgáltatás**

A NAT szolgáltatás segítségével egy helyi hálózat (LAN) számítógépei is képesek használni az internet szolgáltatásait úgy, hogy a gépeknek lokális (10.0.0.0/8, 192.168.0.0/16, stb) IP-címei vannak. Alapesetben ugyanis ezek az IP-címek elérhetetlenek az internet felől.

A NAT tipikusan az alapátjárón beállított szolgáltatás, ami a kifelé menő csomagokban lecseréli a feladó belső hálózati IP-címét az átjáró publikus címére, és továbbküldi a csomagot. A visszaérkező válaszban szintén elvégzi az IP-cím módosítását, majd továbbítja.

#### **5.5 Tűzfal és proxy szerver**

Az internet terjedésével komoly problémává vált a biztonság, hogy a belső adatokhoz illetéktelenül ne férhessen hozzá senki. A tűzfal és a proxy szolgáltatás is a védelem megvalósításában segíthet.

A tűzfal szerepe az, hogy csak engedélyezett forgalom történjen a hálózat és az adott számítógép között. Tűzfal tehát minden számítógépen lehet, és többnyire szükség is van rá. Tipikusan a belső hálózat és az internet

között is lehet tűzfal, ami a belső hálózatot védi a külső hálózat (internet) felől érkező illetéktelen hozzáférések ellen.

Többféle tűzfaltípusról beszélhetünk:

- csomagszűrő,
- állapottartó csomagszűrő,
- alkalmazásszintű tűzfal,
- proxy.

A proxy egyben alkalmazásszintű tűzfal is, mivel teljesen szétválasztja a belső hálózat és a külső hálózat kommunikációját. A belső hálózaton lévő gép a kérését a proxynak küldi, aki értelmezi azt, majd külön végre is hajtja, és csak a választ küldi a kliensnek.

## **5.6 Mail szerver**

Elektronikus levelek kezelésére használt szolgáltatás. A szerverek az SMTP (Simple Mail Transfer Protocol – egyszerű levél továbbító protokoll) protokoll segítségével kommunikálnak. A kliensek a szervereken lévő postafiók-jukhoz többféleképpen is hozzáférhetnek:

- egyedi levelező programmal (outlook, thunderbird stb.),
- böngészőn keresztül tipikusan a szerverhez kapcsolódva.

A postafiók lekérdezéséhez azonban már más protokollt használnak. A két, jelenleg is használt protokoll:

- POP3 (Post Office Protocol version 3),
- IMAP (Internet Message Access Protocol).

A levelező programokban be kell tudni állítani a szerver eléréséhez szükséges adatokat: IP-cím, protokoll, felhasználói adatok. Webes felületen azonban egyszerű a helyzet, ott csak be kell jelentkezni. Ilyen esetekben jellemzően IMAP protokollt használnak a levelek eléréséhez.

Lehetőség van titkosított csatornán történő hozzáférésre is POP3 és IMAP esetén is.

Az SMTP protokoll a 25-ös tcp portot használja, a POP3 a 110/tcp-t, az IMAP pedig a 143/tcp portot.

## **6. 4. lecke: Windows Web szolgáltatás**

### **6.1 Részcélkitűzések**

A tanuló legyen tisztában, hogy Windows szerverre milyen webszerver szolgáltatásokat lehet telepíteni. Legyen képes telepíteni a beépített webszerver (IIS) szolgáltatást. Egy másik gépről a telepített webszerver szolgáltatás működését képes legyen ellenőrizni.

### **6.2 Lehetőségek**

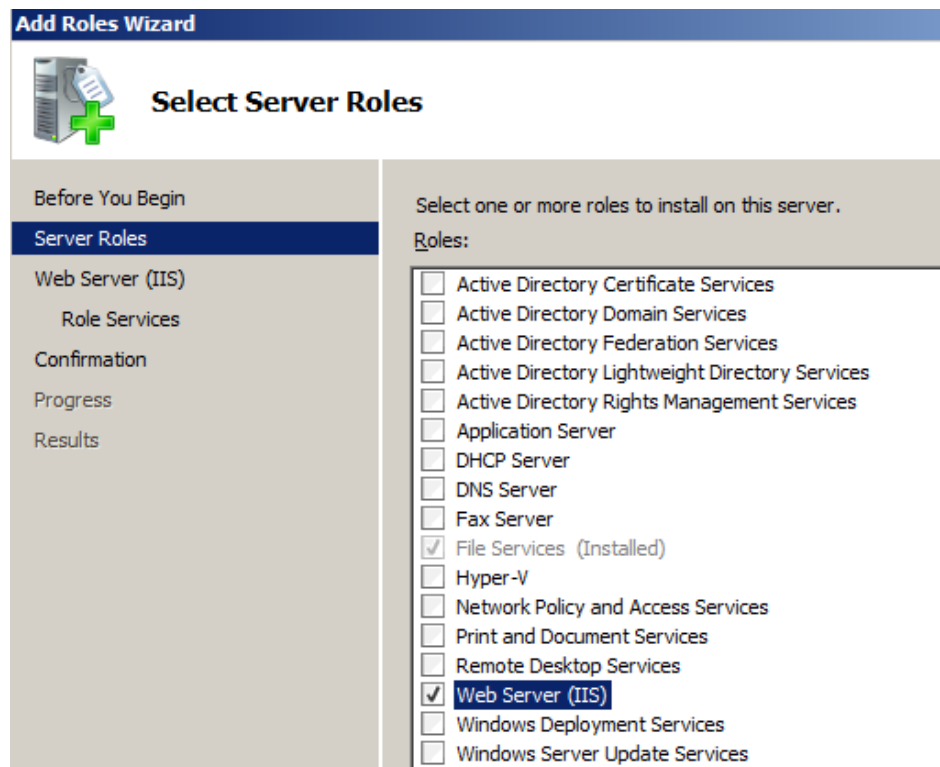
Windowsos gépek esetén a web és FTP szolgáltatást az IIS (Internet Information Services) szolgáltatás fogja össze. Ezt a szolgáltatást már a legtöbb – nem szerver – operációs rendszer esetén is fel lehet telepíteni.

Az IIS-en kívül azonban rendelkezésre állnak a különböző ingyenes AMP (Apache, MySQL, PHP) kiszolgáló csomagok, amelyeket egyszerűen le lehet tölteni, és fel lehet telepíteni bármilyen windowsos gépre.

A továbbiakban csak az IIS lehetőségeivel ismerkedünk meg a Windows Server 2008 R2 Eval változatán.

### **6.3 Telepítés**

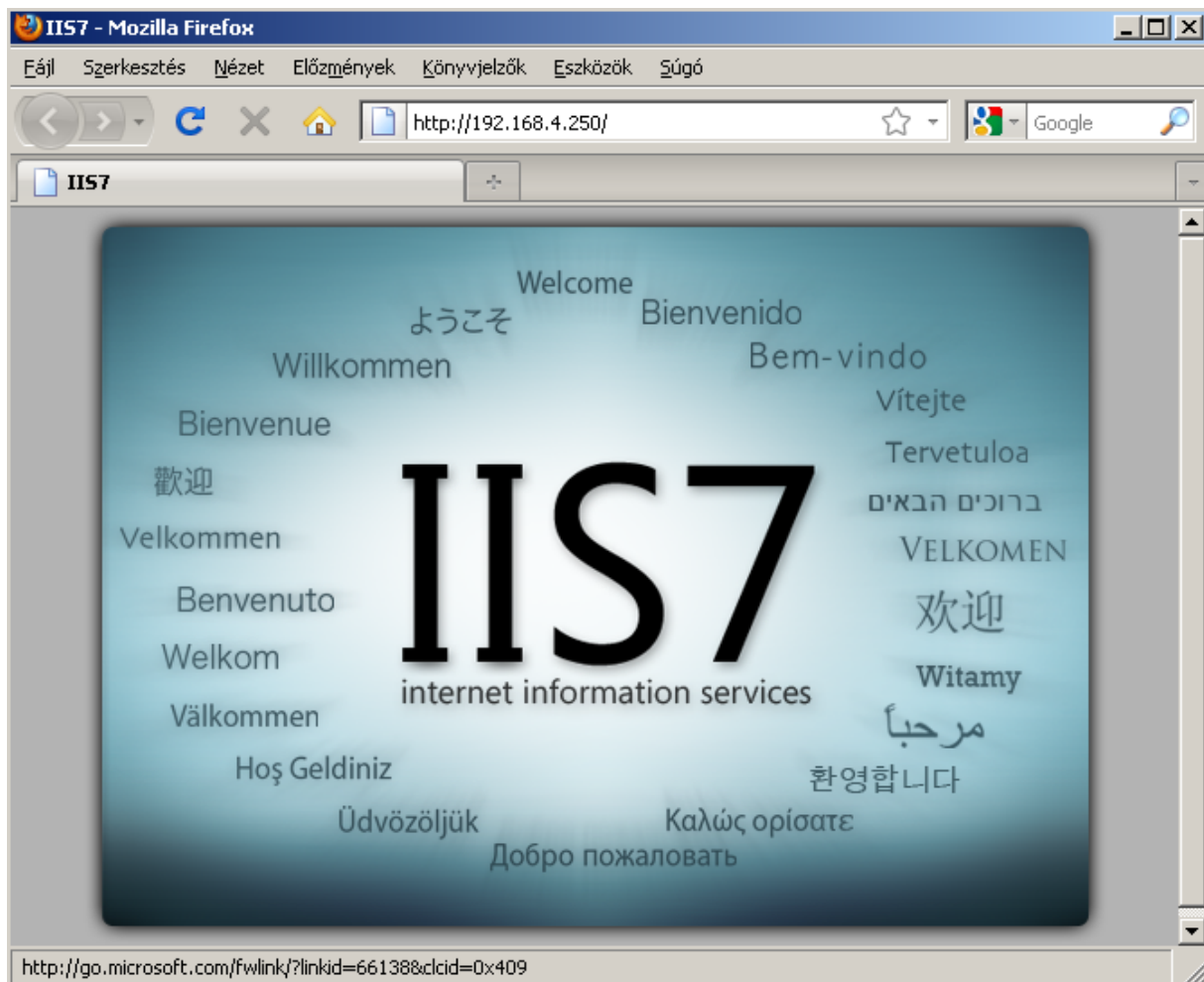
1. A „Server Manager” programban a „Roles” elem gyorsmenüjében ki kell választani az „Add Roles” menüpontot.
2. A következő lépésben a megjelenő ablakban „Next”, majd ki kell jelezni a „Web Server (IIS)” elemet, és „Next”, és „Next”.



**1. ábra. A Web Server (IIS) telepítése**

3. A „Role Services”-nél ki lehet választani, hogy milyen kiegészítő szolgáltatásokkal települjön az IIS. Alapesetben is elég sok szolgáltatás van kijelölve, de van néhány olyan elem, amit még ajánlott kiválasztani:
- „HTTP Redirection” – oldalátirányítás lehetősége,
  - „ASP.NET” – dinamikus oldalakhoz (más elemeket is bejelöl, ami szükséges a működéséhez),
  - „Basic Authentication”,
  - „Windows Authentication”,
  - „IP and Domain Restrictions”.
4. Az egyes beállítások később is módosíthatók a gyorsmenü „Role Services” menüpontjával.
5. Majd a következő lépésben egy összefoglaló képernyőn ellenőrizhető, hogy mit is szeretnénk, utána „Install”.

6. A telepítés befejezése után a „Server Manager” programban meg kell jelennie a „Web Server (IIS)” elemnek is.
7. A működés ellenőrzése. A távoli gépen elég beírni a böngészőbe a szerver IP-címét, és máris megjelenik az IIS nyitóoldala.



2. ábra. Az IIS nyitóoldala

## 7. 5-6. lecke: Windows Web szerver beállítás

### 7.1 Részcélkitűzések

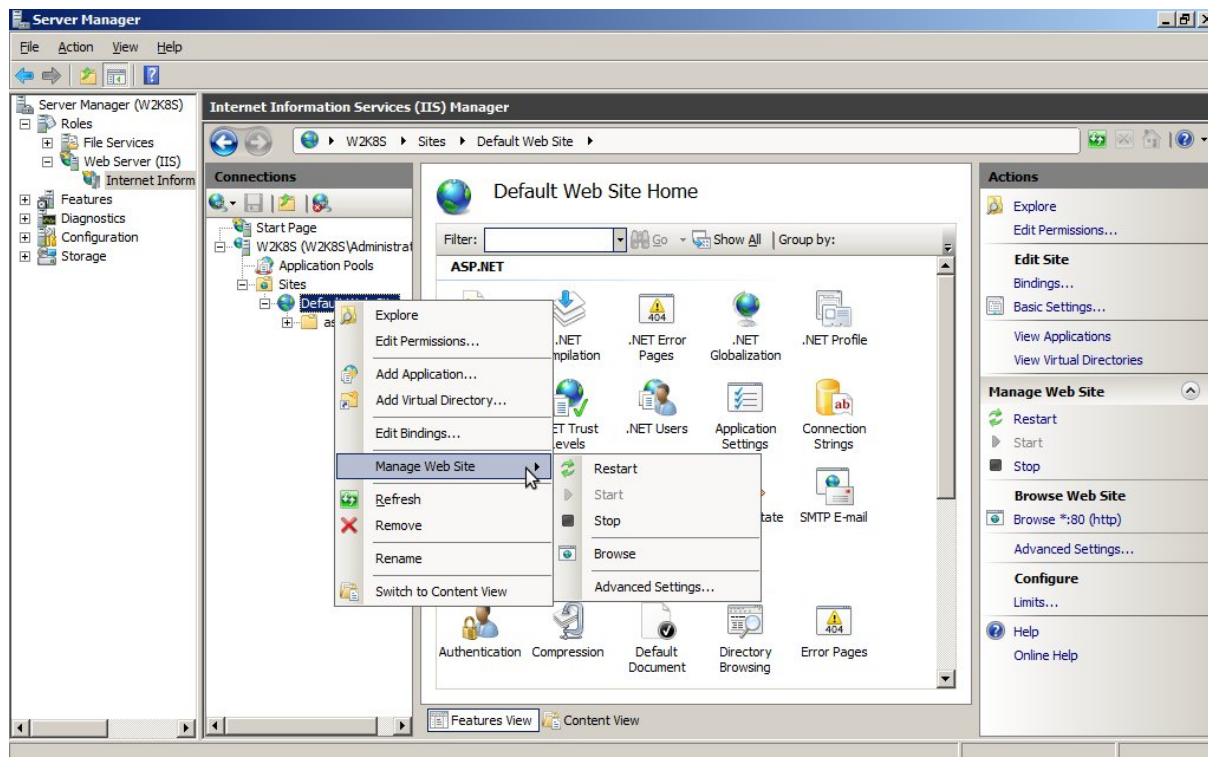
A tanuló legyen képes kezelni az IIS Web Servert. Tudja kezelni a webszerverrel kapcsolatos szolgáltatásokat. Legyen képes új web site-okat létrehozni, módosítani. Legyen képes a weboldalak állományainak szerkesztésére.

## 7.2 Beállítás, konfigurálás

Az IIS-sel kapcsolatos szolgáltatásokat a „Roles” elem „Web Server (IIS)” elemét kiválasztva lehet elérni. Ekkor jobboldalt megjelenik egy több részből álló ablak. Itt rögtön sok információhoz hozzá lehet jutni a szolgáltatással kapcsolatban, hiszen az első részben („Events”) a webszerverrel kapcsolatos utolsó események jelennek meg.

Kicsit lejjebb görgetve a webszerverrel kapcsolatos szolgáltatásokat („System Services”) lehet kezelni (leállítani, elindítani stb.), illetve még lejjebb a „Roles Services” részben az installált szolgáltatások listája látható.

Az IIS által kezelt oldalak (site) az „Internet Information Services (IIS) Manager” felületen érhetők el, illetve állíthatók be. Az alapértelmezett oldal a „Default Web Site”. Ha szükséges, módosítható (jobbaldalt „Advanced Settings”), de le is állítható (jobbaldalt „Stop”), valamint a fájlok is megjeleníthetők (középen alul, „Content View”).



3. ábra. Weboldalak (site) kezelése

Az alapértelmezett útvonal a C:\InetPub\wwwroot. A default site fájljai itt helyezkednek el.

Létrehozhatók új oldalak is, a „Sites” elem gyorsmenüjének „Add Web Site...” menüpontjával. Meg kell adni az oldal nevét, az oldal fájljainak helyét, az elérési protokollt, több szerver IP-cím esetén azt, hogy melyiken legyen aktív, illetve a portot.

Amennyiben olyan portot adunk meg, amelyik már használatban van, akkor figyelmeztetést kapunk, hogy az nem lesz addig elérhető, amíg nem orvosoljuk a problémát. Vagy valamelyik site-ot más portra aktiváljuk, vagy leállítjuk az egyiket.

Az új weboldalhoz tartozó fájlokat megnézhetjük a „Content View”-val középen, illetve jobboldalt az „Explore”-ral fájlkezelőben kezelhetjük az oldalhoz tartozó fájlokat.

## **8. 7-8. lecke: Windows FTP**

### **8.1 Részcélkitűzések**

A tanuló ismerje a Windows alatt elérhető FTP szolgáltatások lehetőségeit. Legyen képes FTP szolgáltatást telepíteni, konfigurálni a szerveren, a beépített FTP szerver segítségével. Tudja egy kliens számítógépről használni a telepített FTP szolgáltatást.

### **8.2 Lehetőségek**

Az IIS kezeli az FTP szolgáltatást is. Azonban FTP szervert is lehet Windows alá külön letölteni és telepíteni is. Ezek között van fizetős program, és van ingyenes, nyílt forráskódú is. Itt is csak az IIS lehetőségeivel foglalkozunk.

### **8.3 Telepítés**

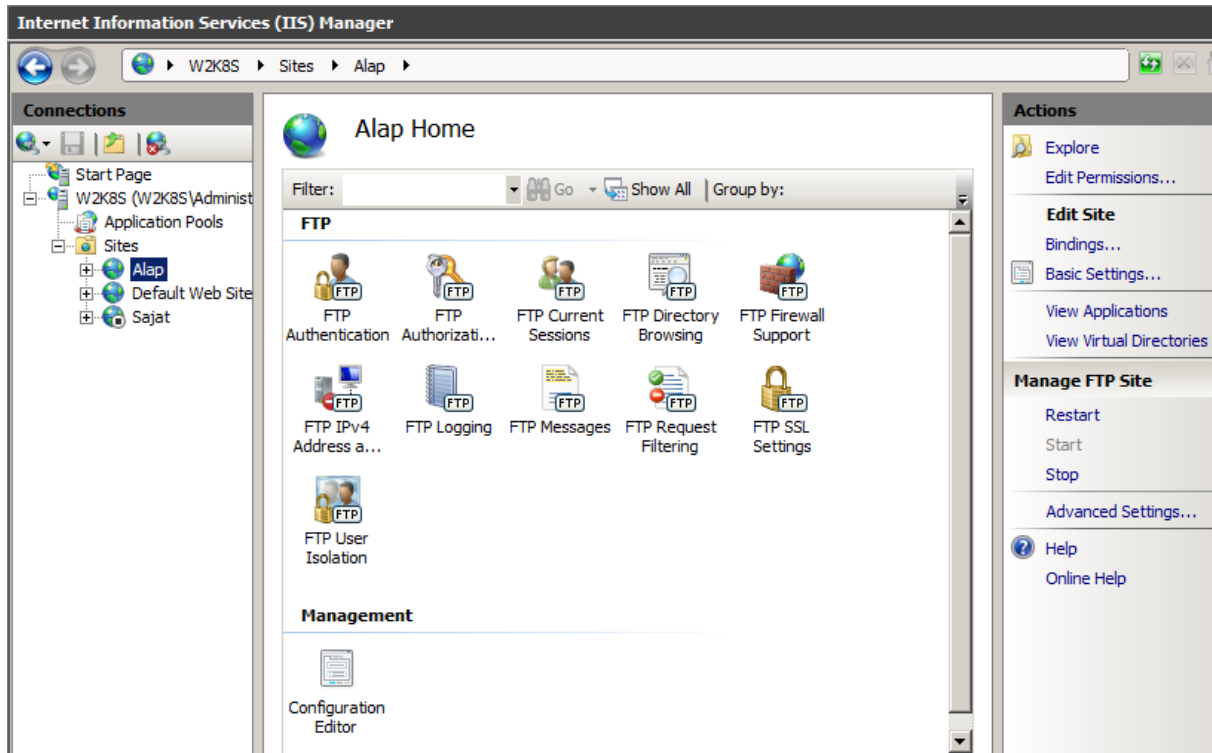
1. Ha még nem telepítettük az IIS-t, akkor először azt kell telepíteni a „Server Manager” „Roles” elemén, az „Add Roles”-t kiválasztva. A szolgáltatásoknál pedig alul ki kell választani az FTP-t.



2. Ha már fent van az IIS, akkor a „Web Server (IIS)” elemet kiválasztva, az „Add Role Services” menüponttal lehet hozzáadni az FTP szolgáltatást.
  3. A telepítés után még nem használható az FTP. Ehhez hozzá kell adni egy FTP site-ot az „Add FTP Site” gyorsmenüponttal. Első lépésben egy nevet adhatunk, illetve meghatározhatjuk az FTP kiinduló könyvtárát, ami lehet a létrehozott c:\inetpub\ftproot is.
  4. A következő lépésben itt is meg lehet határozni, hogy a szerver melyik IP-címén figyeljen és milyen porton. Itt lehet azt is meghatározni, hogy kérünk-e titkosítást az FTP-hez vagy sem. Három lehetőség közül választhatunk:
    - „No SSL” – nincs titkosítás,
    - „Allow SSL” – lehet titkosított kapcsolaton keresztül is használni,
    - „Required SSL” – kötelezően, csak titkosított kapcsolaton lehet elérni.
  5. Ezután még meg lehet határozni, hogy milyen módon azonosítsák magukat („Anonymous”, „Basic”), és kik férhetnek hozzá, illetve milyen módon („Read”, „Write”). A hozzáférési lehetőségek:
    - „All users” – minden felhasználó,
    - „Anonymous users” – csak anonymousként,
    - „Specified roles or users group” – adott szervezet vagy csoport, amit meg is kell adni,
    - „Specified users” – csak a megadott felhasználók.
- Most válasszuk az Anonymous lehetőségeket.
6. Ezek után már elérhető böngészővel is az FTP szolgáltatás úgy, hogy a címsorba az ftp://ip cím kerül.

## 8.4 Beállítás, konfigurálás

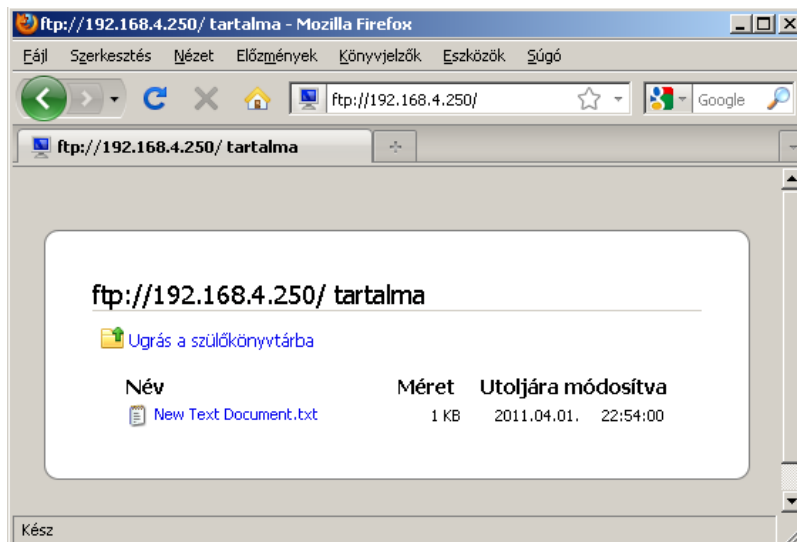
Az FTP szolgáltatást is a „Server Manager” programmal kell kezelni. Ha létrehoztunk egy FTP site-ot, akkor kiválasztva, középen megjelennek a beállítási lehetőségei. Itt mindent be lehet állítani.



4. ábra. FTP site beállítási lehetőségei

## 8.5 Használat

Ha anonymous FTP-t állítottunk, akkor böngészővel is használható. Más esetekben már szükség van valamilyen FTP programra.



**5. ábra. FTP kapcsolat böngészővel**

A fájlkezelők (pl. Total Commander vagy Unreal Commander) egy része is képes FTP kapcsolatokra, de léteznek kifejezetten FTP programok, pl. az ingyenes FileZilla. A csatlakozáshoz meg kell adni a szerver IP-címét, portját, valamint a felhasználó nevét és jelszavát.

## **9. 9. lecke: I. témazáró feladatsor**

### **1. Minek a rövidítése az AMP? Válassza ki a helyes megoldást! (1 pont)**

- a) Advanced Micro Processors
- b) Access Macro Process
- c) Apache MySQL PHP hármass elnevezése
- d) Apache Multiple Process rövidítése

### **2. Milyen porton szolgáltat a DHCP szerver? Válassza ki a helyes megoldást! (1 pont)**

- a) 80
- b) 443/tcp
- c) 67/udp
- d) 80/udp
- e) 53/tcp és 53/udp

**3. Egészítse ki a következő mondatot! (1 pont)**

A \_\_\_\_\_ a Windows operációs rendszerek beépített szolgáltatása, ami a helyi hálózaton gondoskodik a gépek neveinek IP-címekké történő átfordításáról, azaz a névfeloldásról.

**4. Válassza ki az elektronikus levelezés által használt protokollokat! Több jó válasz is lehetséges! (2 pont)**

- a) FTP
- b) SMTP
- c) Web
- d) IMAP
- e) POP3

**5. Hogyan lehet telepíteni egy Windows 2008 szerverre web szolgáltatást? Válassza ki a helyes megoldást! (1 pont)**

- a) Berakjuk a telepítő lemezt a CD-meghajtóba, majd az induló programban beállítjuk, amit szükséges.
- b) A „Control Panel”, „Add Programs”, „Windows Items” részben kiválasztani a listából a „Web Services”-t, és „Install”.
- c) A „Server Manager” program „Add Futures” elemével indítható programban kiválasztom a „Web Services” szolgáltatást, majd „Install”.
- d) A „Server Manager” program „Add Roles” elemét kiválasztva, és a „Server Roles” fülön bepipálni a „Web Server (IIS)” elemet, majd folytatni a telepítést.

**6. A „Default” website fájljai melyik könyvtárban találhatók alapértelmezésben? Írja le a teljes útvonalát! (1 pont)**

**7. Mit kell beírni egy böngészőbe, hogy csatlakozzon a 192.168.0.250-es IP című FTP serverhez „anonymous”-ként? Válassza ki a helyes megoldást! (1 pont)**

e) http://192.168.0.250:21

f) ftp://21/192.168.0.250

g) 192.168.0.250

h) ftp://192.168.0.250

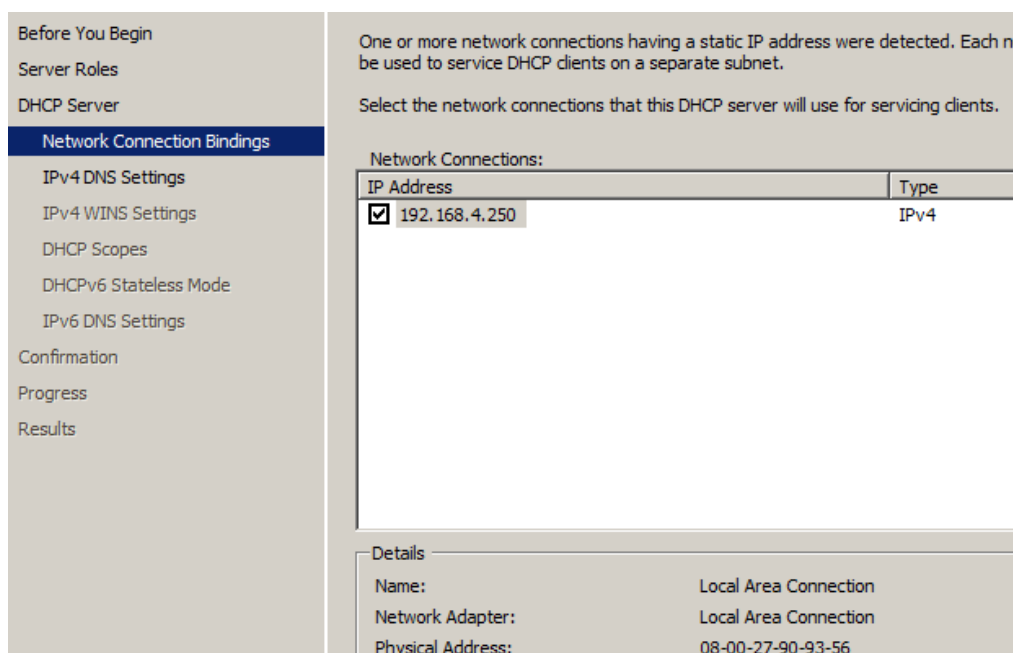
## **10. 10. lecke: Windows DHCP**

### **10.1 Részcélkitűzések**

A tanuló ismerje a DHCP server követelményeit. Legyen képes DHCP szolgáltatást telepíteni egy Windows serverre. Ismerje a DHCP server legfontosabb beállítási lehetőségeit, be is tudja azokat állítani az igényeknek megfelelően. Legyen képes új scope létrehozására, opcióinak megfelelő beállítására. Legyen képes fix IP-cím hozzárendelésére egy adott számítógéphez. Tudja ellenőrizni a DHCP server működését. Képes legyen egy kliens számítógép segítségével bemutatni a server használatát.

### **10.2 Telepítés**

1. Mielőtt DHCP servert telepítünk, ellenőrizzük, hogy a servernek fix IP-címe van-e! Ha nincs, akkor állítsunk be fix IP-t!
2. A „Server Manager” program „Roles” elemének „Add Roles” gyorsmenü pontjával lehet hozzáadni a DHCP szolgáltatást a rendszerhez.
3. Ha a serveren több IP-cím van, akkor ki lehet választani, hogy melyikhez kapcsolódjon DHCP szolgáltatás.

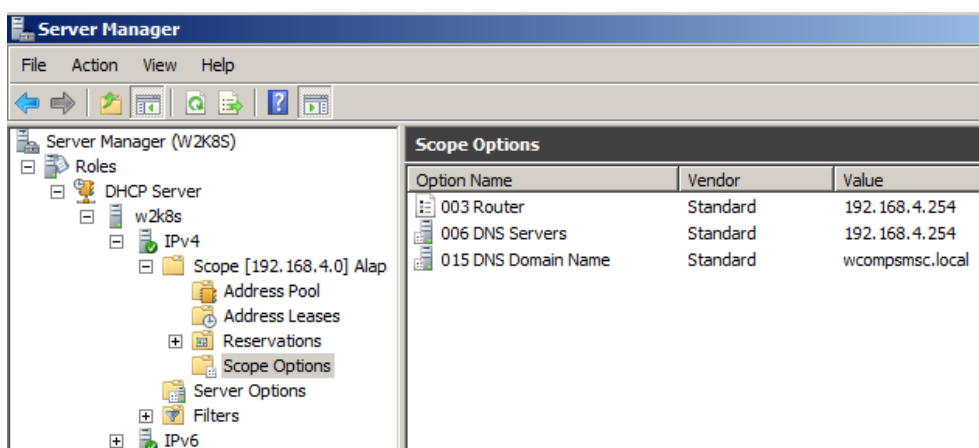


**6. ábra. DHCP telepítése**

4. DNS beállítás következik. Itt azt kell beállítani, hogy a DHCP milyen DNS információkat (domain, DNS szerver címe) adjon a klienseknek.
5. Ha van WINS szolgáltatás a hálózaton, akkor itt megadhatom a WINS kiszolgáló címét, a DHCP ezt is kiosztja a klienseknek.
6. A következő lépésben meg kell határozni azt az IP-tartományt (scope), ahonnan majd IP-címeket fog kiosztani. Itt lehet meghatározni az alapátjáró címét is.
7. A következő két lépésben az IPv6 beállításai jönnek. A domaint itt is meg kell adni.
8. A sikeres telepítés után azonnal el is indul a DHCP szerver szolgáltatás.

### **10.3 Beállítás**

A telepítésnél már beállításra kerültek a legfontosabb adatok, de ezeket bármikor lehet módosítani a „Server Manager” „Roles” szekció „DHCP Server”-en keresztül. Külön állítható az IPv4 és az IPv6.



**7. ábra. DHCP konfigurálása**

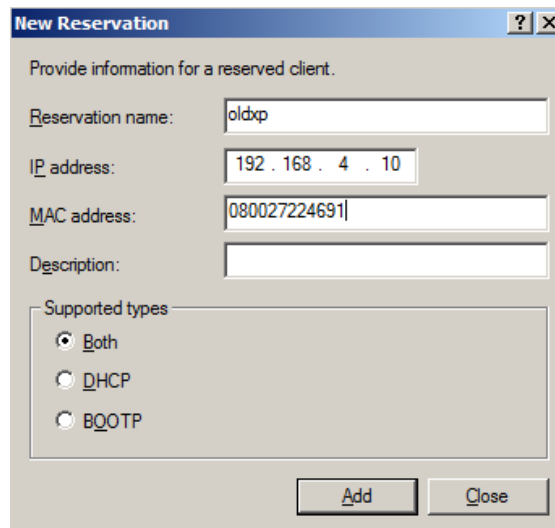
Több scope is lehet, mindegyiknek egyedi jellemzőkkel. Azonban figyelni kell arra, hogy csak olyan scope fog működni, amelyik hálózatához a szervert is tartozik IP-cím.

A scope-on belül állítható a kiosztható IP-cím tartomány („Address Pool”). Módosításához a scope-on kell jobb egérgombbal kattintani, majd a gyorsmenüből a „Properties”-t kiválasztani. Itt állítható be a „Lease Time”, vagyis a bérleti idő értéke is.

Az „Address Pool” gyorsmenüből elérhető a „New Exclusion Range”, amelynek segítségével ki lehet zárni a scope IP-címtartományából tetszőleges IP tartományt is. A kizárt IP-eket a szerver nem fogja kiosztani.

Az „Address Lease” elemet frissítve („Refresh”) megjelennek középen a kiosztott IP-címek és gépnevek, valamint a lejáratási idő.

A „Reservation” segítségével lehet egy adott gép számára mindig ugyanazt az IP-címet kiosztani. A gyorsmenü „New Reservation...” pontot kiválasztva a megnyíló ablakban adnunk kell egy nevet (jellemzően a gép nevét célszerű), az IP-címet, amit kapni fog, és meg kell adni még a gép MAC címét is, hiszen ehhez kerül hozzárendelésre az IP-cím.



**New Reservation** [?] [X]

Provide information for a reserved client.

Reservation name: oldxp

IP address: 192 . 168 . 4 . 10

MAC address: 080027224691

Description:

Supported types

☒ Both

☐ DHCP

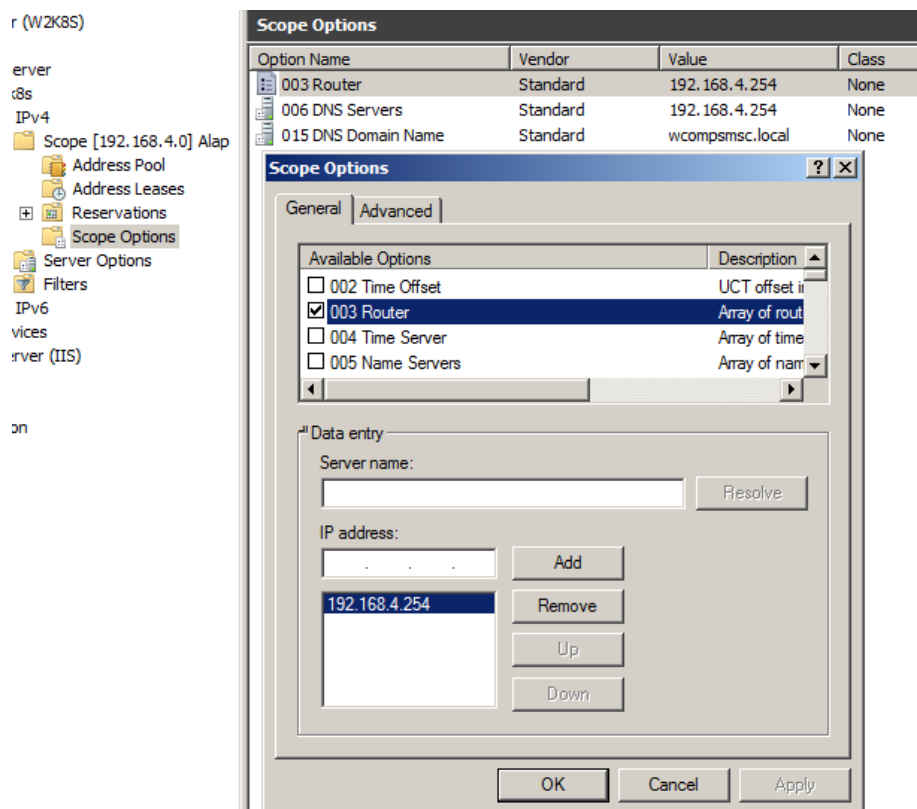
☐ BOOTP

[Add] [Close]

**8. ábra. DHCP statikus IP-cím meghatározása**

A beállítás után külön sorban jelennek meg a statikus IP-címek.

A „Scope Options” részben jelennek meg az IP-cím mellett kiosztott hálózati jellemzők. A jellemzők módosítása a gyorsmenü „Configure Options” elemével lehetséges.



Scope [192.168.4.0] Alap

Address Pool

Address Leases

Reservations

Scope Options

Server Options

Filters

IPv6

vices

erver (IIS)

on

**Scope Options**

Option Name	Vendor	Value	Class
003 Router	Standard	192.168.4.254	None
006 DNS Servers	Standard	192.168.4.254	None
015 DNS Domain Name	Standard	wcompsmsc.local	None

**Scope Options** [?] [X]

General | Advanced

Available Options

☐ 002 Time Offset UCT offset is

☒ 003 Router Array of rout

☐ 004 Time Server Array of time

☐ 005 Name Servers Array of nam

Data entry

Server name: [ ] [Resolve]

IP address: [ ] [Add]

[192.168.4.254] [Remove]

[Up]

[Down]

[OK] [Cancel] [Apply]

**9. ábra. DHCP scope opciók**



A scope-on kívül található a „Server Options” elem, ahol a DHCP szerver beállításait lehet megjeleníteni, illetve módosítani.

## 10.4 Használat

A kliens gépeken az IP-beállításoknál automatikus kérésre kell állítani az IP-t és a DNS-t is. A módosítás után parancssorban az „ipconfig /all” paranccsal lehet ellenőrizni, hogy tényleg működik-e a DHCP szerverünk.

```
Ethernet-adapter Helyi kapcsolat:
    Kapcsolatspecifikus DNS-utótag. . . . : wcompsmsc.local
    Leírás. . . . . : AMD PCNET Family PCI Ethernet ad
apter
    Fizikai cím . . . . . : 08-00-27-22-46-91
    DHCP engedélyezve . . . . . : Igen
    Automatikus konfiguráció engedélyezve : Igen
    IP-cím. . . . . : 192.168.4.20
    Alhálózati maszk. . . . . : 255.255.255.0
    Alapértelmezett átjáró. . . . . : 192.168.4.254
    DHCP kiszolgáló . . . . . : 192.168.4.250
    DNS-kiszolgálók . . . . . : 192.168.4.254
    Bérleti jog kezdete . . . . . : 2011. április 2. 11:15:27
    Bérleti jog vége. . . . . : 2011. április 10. 11:15:27
```

10. ábra. DHCP-vel kiosztott hálózati beállítások

Ha a listában van „DHCP kiszolgáló” sor, akkor biztosak lehetünk benne, hogy a gépünk DHCP szervertől kapott IP-címet, ráadásul a sorból azt is megtudhatjuk, hogy mi a DHCP szerver IP-címe. A fenti példában ez 192.168.4.250, vagyis a saját 2008-as szervertől kapott IP-címet a gép.

## 11. 11. lecke: Windows WINS

### 11.1 Részcélkitűzések

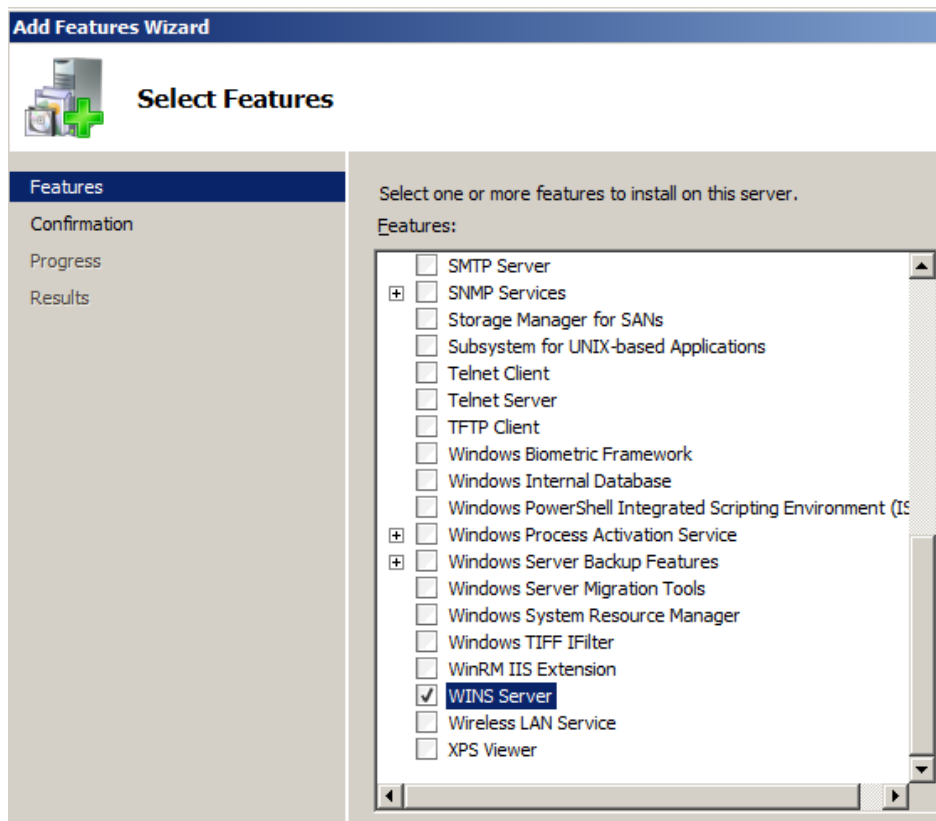
A tanuló legyen tisztában a WINS szolgáltatás céljával, működésével. Tudjon WINS szolgáltatást telepíteni Windows szerverre. Legyen képes beállítani, hogy a hálózat számítógépei használják is a WINS szolgáltatást.

### 11.2 Előzetes megfontolások

A WINS működésének és használatának legfontosabb alapelveit már az 5.2 fejezet tárgyalta, itt csak emlékeztetünk rá, hogy az ott leírtakat szem előtt tartva kell a WINS szolgáltatással kapcsolatban dönteni.

### 11.3 Telepítés

A „Server Manager” program „Features” elemének „Add Features” gyorsmenü pontjával lehet hozzáadni a WINS szolgáltatást a rendszerhez.

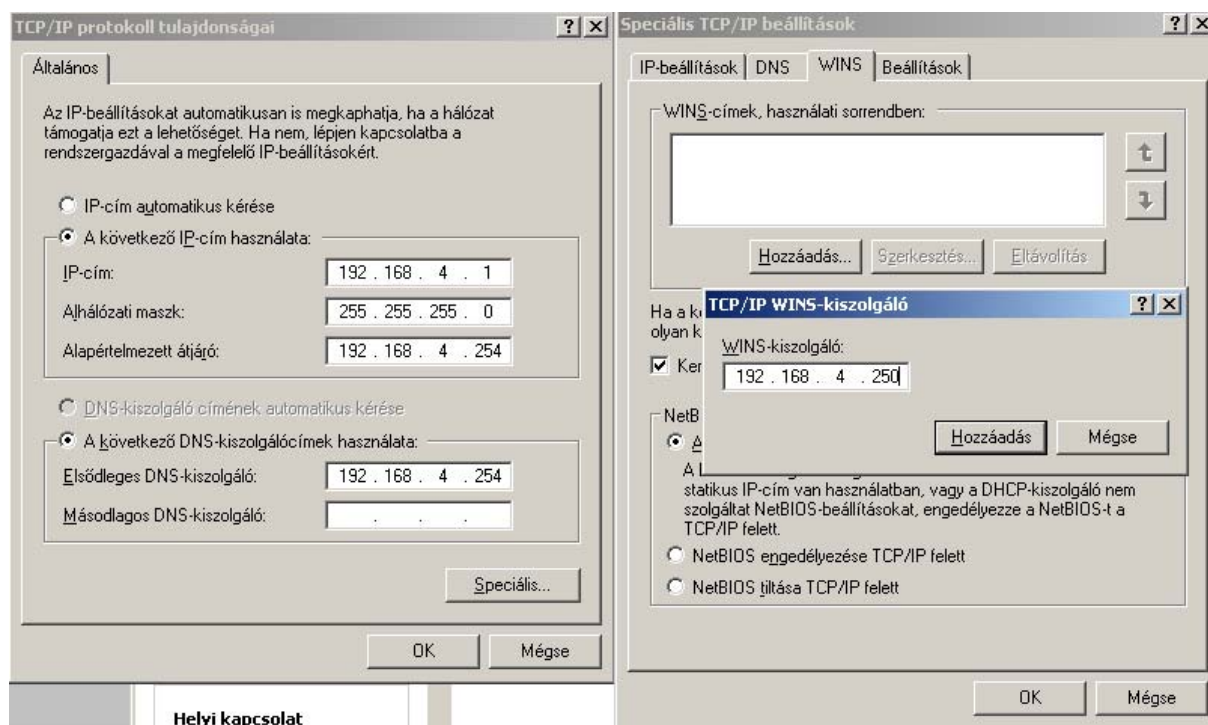


**11. ábra. WINS telepítés**

A telepítés után a WINS szolgáltatás automatikusan elindul. További beállításokra nincs szükség.

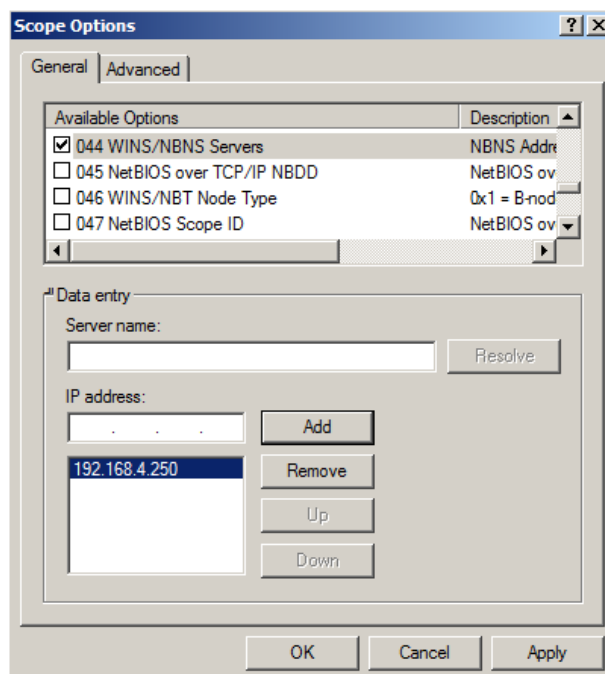
#### **11.4 Használat**

Ahhoz, hogy egy számítógép használja is a WINS szolgáltatást, be kell azt neki állítani a hálózati beállításoknál. Fix IP-cím használatakor az IP-beállításoknál a „Speciális...” gombra kell kattintani, majd a megnyíló ablakban a „WINS” fület kiválasztani. Itt a hozzáadás gombbal lehet a listába felvenni WINS kiszolgáló címet.



**12. ábra. WINS szerver megadása a kliens gépen**

Ha a kliensen automatikus IP-cím kérés van beállítva, akkor a szerveren kell módosítani a DHCP beállításokat a scope „Scope Options” eleménél.



**13. ábra. WINS megadás DHCP-vel**

A következő kiosztásnál már a WINS címet is megkapják a munkaállomások.

## **12. 12-13. lecke: Windows DNS**

### **12.1 Részcélkitűzések**

A tanuló ismerje a különböző DNS szerver működési módokat, alkalmazási területüket. Tudjon Windows szerverre DNS szolgáltatást AD nélkül is telepíteni. Tudjon beállítani resolver szervert. Legyen képes beállítani a szerveren és a hálózat számítógépein is, hogy a frissen telepített DNS szervert használják a névfeloldáshoz. Tudja tesztelni a DNS szerver működését a szerveren és a klienseken is. Legyen képes beállítani, hogy több IP esetén csak egyik IP-címen legyen elérhető. Tudja beállítani a forwarder szerverek IP-címeit, vagyis legyen képes forwarder szervert beállítani.

### **12.2 Előzetes megfontolások**

Ha a rendszeren van Active Directory, akkor ott már lennie kell DNS szolgáltatásnak is, anélkül ugyanis nem működik az AD. Ebben az esetben nem kell telepíteni.

A telepítés előtt célszerű átgondolni, hogy milyen célra is kell nekünk egy DNS kiszolgáló. Ha interneten elérhető szolgáltatást szeretnénk, akkor erősen megkérdőjelezhető a Windows szerver alkalmazása, ugyanis nem a legbiztonságosabb megoldás egy Windows szervert direkt módon elérhetővé tenni bárki számára is, nem beszélve arról, hogy felesleges erőforrás-pocsékolás is egyben, hiszen ugyanezt más operációs rendszer alatt, jóval kisebb teljesítményű számítógépek segítségével is meg lehet oldani.

Helyi hálózaton többféle céllal szoktak DNS kiszolgálót telepíteni. Az egyik esetben csak továbbítóként (forwarder) használják, ami cache-elni (átmenetileg tárolni) is képes a kéréseket. Ez annyiban segít, hogy ha ugyanazt a címet többen is használják, csak az első esetben terhelődik le a külső hálózati kapcsolat. Ezek a szerverek a hozzájuk érkezett kéréseket rendszerint az internet-hozzáférés szolgáltatója által üzemeltetett DNS szerverek felé továbbítják.

A másik esetben teljes értékű resolver (feloldó) szervert készítenek, amely a szolgáltatótól függetlenül képes elvégezni a névfeloldást úgy, hogy közvetlenül a gyökérszerverekhez fordulva elindítja a teljes névfeloldási folyamatot.

A harmadik esetben saját zónát (tartomány, domain) hoznak létre, amelyben akár minden gépnek lehet egyedi domainneve is, az internetes címekhez hasonlóan. A két működési mód nem zárja ki egymást, hiszen akár saját zóna üzemeltetése mellett is cache-elheti a külső oldalak címeit.

A továbbiakban mindegyik lehetőséget megvizsgáljuk.

### **12.3 Telepítés**

1. Mielőtt DNS szervert telepítünk, ellenőrizzük, hogy a szervernek fix IP-címe van-e! Ha nincs, akkor állítsunk be fix IP-t!
2. A „Server Manager” program „Roles” elemének „Add Roles” gyorsmenü pontjával lehet hozzáadni a DNS szolgáltatást a rendszerhez.
3. Utána összefoglaló képernyő, majd „Install”.

### **12.4 Beállítás, ellenőrzés**

A telepítés után még további feladatok is vannak, mielőtt használatba vehetnénk a DNS szerverünket.

Először is be kell állítani a hálózati kapcsolatoknál, hogy használják is a számítógépek a DNS szerveret. Magán a szerveren is be kell állítani, ott viszont a DNS szerver címéhez a 127.0.0.1-et kell írni.

Ellenőrizzük is le, hogy működik-e a névfeloldás a szerveren, például az „nslookup index.hu” paranccsal. Ha működik, akkor az eredményben azt kell látnunk, hogy a feloldó szerver a 127.0.0.1, és meg kell jelennie az index.hu domainhez tartozó IP-címnek is.

```
C:\Users\Administrator>nslookup index.hu
Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
Name: index.hu
Address: 217.20.130.97
```

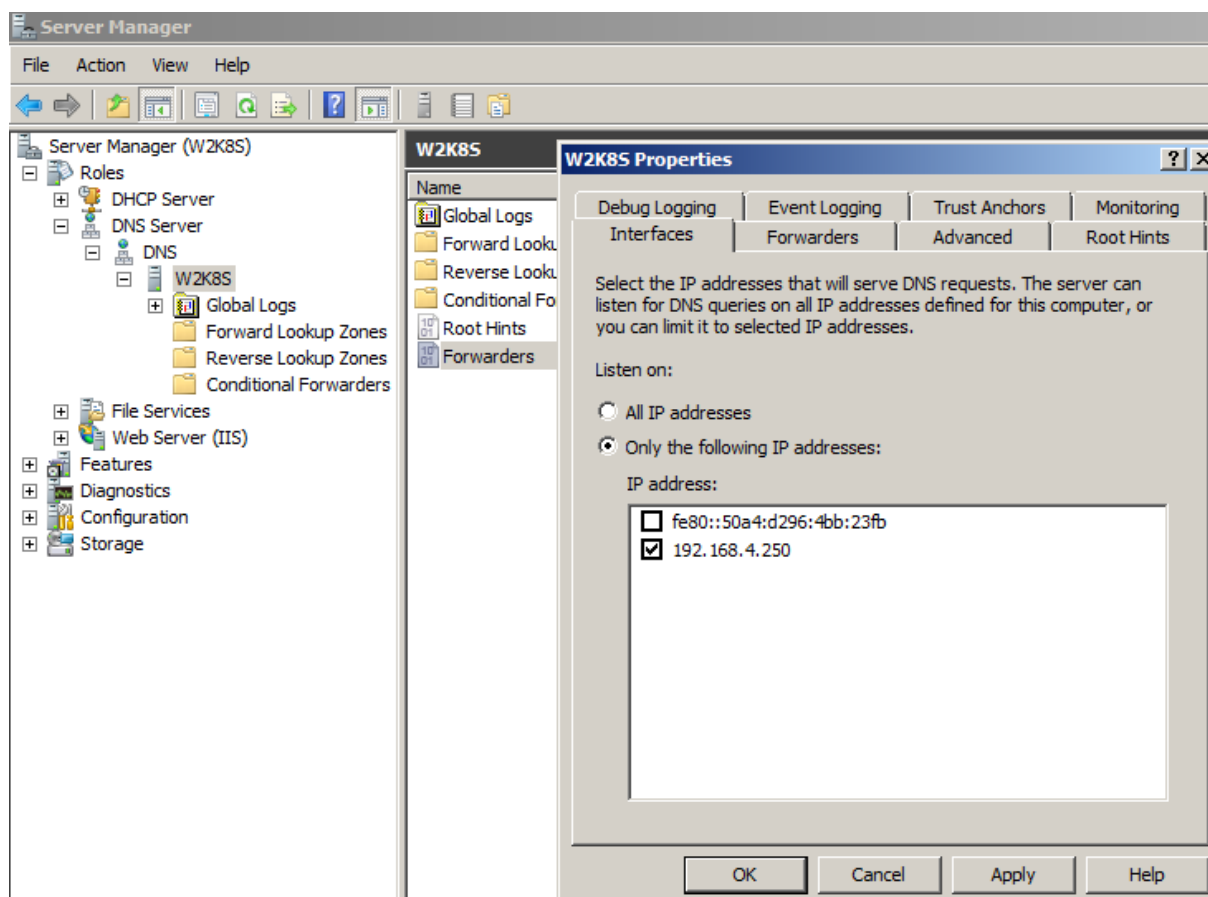
#### 14. ábra. Működő DNS szolgáltatás

Be kell még állítani, hogy minden más számítógép is ezt a DNS szerveret használja a névfeloldáshoz. Ezt vagy kézzel kell beállítani az adott gép hálózati kapcsolatainál, vagy a DHCP szerveren kell módosítani a „Server Options”-nál.

A DHCP beállításainak módosítása után a már üzemben lévő számítógépeken még nem fog változni a beállítás, csak akkor, ha újraindítják őket, vagy parancssorban kiadják az „ipconfig /release” és „ipconfig /renew” parancsokat. Ezzel újrakéri a címet. A munkaállomáson is ellenőrizzük le a névfeloldás működését!

Alapesetben a DNS szerver resolver (teljes értékű feloldó) módban működik, mivel nem adtunk meg semmilyen forwarder szerver opciót.

A további beállításokat a „Server Manager” DNS szekciójában, a szerver nevén keresztül elérhető gyorsmenü „Properties” menüpontjával lehet elérni.



**15. ábra. DNS szerver általános konfigurálása**

Itt beállítható többek között, hogy ha a szerver több IP-címmel rendelkezik, akkor melyik IP-en fogadjon DNS kéréseket („Interfaces” fül). Illetve, hogy ha szükséges, beállíthatóak a forwarder szerverek címei is („Forwarder” fül).

## **13. 14-15. lecke: Windows DNS saját zóna beállítása, kezelése**

### **13.1 Részcélkitűzések**

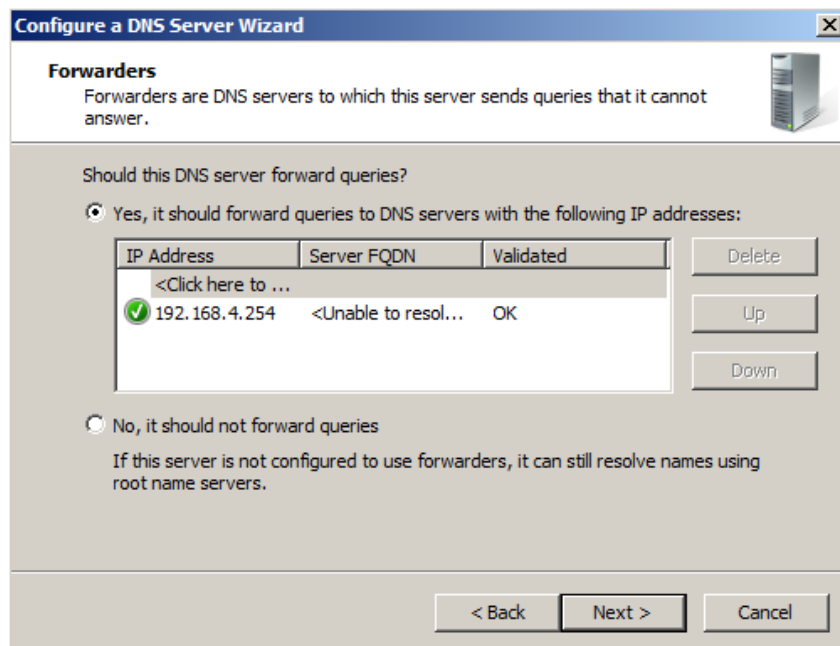
A tanuló legyen képes új zónát létrehozni, beállítani. Tudjon felvenni a zónába új hostot, és álnevet is a hosthoz. Tudja megfelelően kezelni a reverse zónát is. Ismerje a legfontosabb DNS rekordok típusait, jelentésüket, szintaktikájukat, paramétereik jelentését. Legyen képes a hálózat számítógépeiről használni az új zónát, teljesen meghatározott (FQDN) és rövid nevekkel is.

## 13.2 Új zóna létrehozása

A zóna beállítását elkészíthetjük varázslóval is, a szerver nevén elérhető gyorsmenü „Configure a DNS Server...” menüponttal, vagy külön a „Forward Lookup Zones”, illetve a „Reverse Lookup Zones” elemeknél.

1. A varázslót indítva először ki kell választani, hogy milyen típusú DNS szolgáltatást akarunk. Úgy illik, hogy a forward és a reverse zónát is beállítsuk, így a középső elemet („Create Forward and Reverse Lookup Zone...”) válasszuk.
2. Most hozzuk létre a forward zónát, vagyis „Yes”.
3. Elsődleges zónát akarunk, vagyis „Primary zone”.
4. Meg kell adni a zóna nevét, most jellemzően „pelda.local”.
5. Meghatározható a fájl neve, ahol a DNS beállítások tárolódnak. Maradhat az alapértelmezés.
6. Eldönthetjük, hogy engedélyezzük-e a dinamikus frissítést más számítógépektől. Az alapértelmezés, hogy nem, most is ez marad.
7. Akarunk reverse zónát, vagyis „Yes”.
8. A reverse is „Primary zone”.
9. Jelenleg IPv4-et használunk.
10. Meg kell adni a hálózat címét pontozott decimális alakban, most ez „192.168.4”. Nem kell a végére a 0!
11. A reverse adatok tárolására szolgáló fájlnevet is meghatározhatjuk, de jó az alapértelmezés.
12. Itt is dönthetünk a dinamikus frissítésről. Most se engedjük.
13. Megadhatjuk a forwarder szerver címét, most itt a „192.168.4.254” címet határozzuk meg.





**16. ábra. Új zóna forwarder beállítás**

14. Az összefoglaló képernyőn „Finish”, és indul a beállítás.

### 13.3 Új gép felvétele a zónába

Ki kell választani a zónát („pelda.local”), majd a gyorsmenüből „New Host (A or AAAA)...”. Ezután meg kell adni a gép nevét és IP-címét. Ne felejtsük el bepipálni a „Create Associated Pointer (PTR) Record”-ot! Ezzel kerül be a reverse listába is.

Most vegyük fel magát a szervert „server” névvel 192.168.4.250-es IP-vel, majd a kliensünket „xp” névvel, és a megadott IP-vel, ami most „192.168.4.10”, valamint vegyük fel az átjárót is „gw” névvel, „192.168.4.254” címmel. Valami ilyesmit kell kapnunk:

(same as parent folder)	Start of Authority (SOA)	[1], w2k8s., hostmaster.
(same as parent folder)	Name Server (NS)	w2k8s.
server	Host (A)	192.168.4.250
xp	Host (A)	192.168.4.10
gw	Host (A)	192.168.4.254

**17. ábra. Beállított forward zóna**

Ezek után tetszőleges álnevet (alias) is hozzárendelhetünk bármelyik, már felvett hosthoz. Ehhez a „New Alias (CNAME)” elemet kell választani a gyorsmenüből. Például a „server”-hez hozzárendelhetjük a „www”, „ftp”

vagy a „w2k8s” álnevet is. Figyeljünk arra, hogy a „server” megadásánál FQDN nevet adjunk meg, vagyis „server.pelda.local”-t kell írni.

A reverse zónában csak frissítés („Refresh”) után lesznek láthatóak a bejegyzések.

A módosítások érvényre juttatásához újra kell indítani a DNS szerveret, a szerver nevén (most „w2k8s”) elérhető gyorsmenü, „All Tasks” menü, „Restart” menüpontjával.

### 13.4 DNS rekordok típusai

A DNS szerverek bejegyzéseit rekordoknak nevezik. Többféle bejegyzés lehetséges. Az előzőekben már kétféle típust használtunk, az egyik a host, vagyis az „A” rekord, a másik az alias, vagyis a „CNAME” rekord. A teljesség kedvéért összefoglaljuk a lehetséges bejegyzéseket.

#### SOA – „Start of Authority” rekord, zóna kezdő rekord

A SOA rekord definiálja a zónára vonatkozó közös beállításokat. Szerkezete kötött, a következőben egy mintát láthatunk:

```
belso.local.    SOA                w2k8s.belso.local.    info.belso.local. (
                2011031201          ;Serial nr.
                86400                ;Refresh
                1800                  ;Retry
                604800               ;Expire
                43200)               ;TTL
```

Figyeljünk a záró pontokra és a sima zárójelekre. A „belso.local.” a domaint határozza meg, a „w2k8s.belso.local.” magát a szervert azonosítja, míg az „info.belso.local.” egy e-mail címet határoz meg (az első pont helyett egy „@” karaktert behelyettesítve).

A „;” utáni szövegrészek megjegyzések, vagyis a szerver nem veszi figyelembe.

A „Serial nr” sorban lévő szám a sorozatszám. Minden változtatás után ezt a számot is növelni kell. A szerepe abban nyilvánul meg, hogy a másodlagos szerverek ez alapján ellenőrzik, hogy az általuk nyilvántartott adatok frissültek-e vagy sem. A formája bármilyen lehet, de szokás szerint

ÉÉÉÉHHNNSS formát használják, ahol az „É” az évszámot jelenti, a „H” a hónapot, az „N” a napot, míg az „S” a sorszámot. Vagyis egy dátum, ami rendszerint a DNS szerver telepítésének dátuma szokott lenni, és csak az utolsó két számjegy az, ami a sorozatszámot határozza meg.

A további paraméterek másodpercben meghatározott értékek. A „Refresh” a frissítési időt határozza meg, ami a másodlagos szerverek részére írja elő, hogy mennyi időnként kell frissíteniük a saját adataikat.

A „Retry” szintén a másodlagos szervereknek szól, hogy mennyi idő múlva próbálkozzanak ismét a frissítéssel, ha az előzőleg nem sikerült.

Az „Expire” szintén a másodlagos szerverek számára határozza meg azt az időt, ameddig az elsődleges szerver nélkül is szolgáltatják a zóna adatait a külvilág számára.

### **NS – „Name Server” rekord, névszerver rekord**

Segítségével határozhatjuk meg az adott domain névszervereit. Például:

```
w2k8s      NS      belso.local.
```

Ajánlatos két szervert megadni, és egyben üzemeltetni is, hogy ha az egyik leáll, a másik még szolgáltatson. Fontos, hogy az így meghatározott névhez mindenképpen tartozzon egy „A” rekord is!

### **A – „Address” rekord, hoszt rekord**

Ezzel lehet egy névhez egy IP-címet hozzárendelni. Formája:

```
w2k8s      A       10.10.10.254
```

### **CNAME – „Canonical Name” rekord, alias vagy álnév rekord**

Egy adott hosthoz lehet másik nevet is hozzárendelni. Formája:

```
www        CNAME   w2k8s.belso.local.
```

Itt a „www” az álnév, jobboldalt pedig a teljesen meghatározott „A” rekorddal is rendelkező gépnévnek kell szerepelnie.

## **MX - Mail eXchanger, levelezőszerver rekord**

Segítségével határozható meg, hogy az adott domainre érkező leveleket hol is dolgozzák fel, vagyis mi az IP-címe a levelezőszervereknek. Több MX rekord is lehet, akik között prioritási sorrendet is fel lehet állítani. A prioritást egy szám határozza meg, minél kisebb ez szám, annál nagyobb a prioritás. A kisebb prioritású szerverek csak akkor dolgozzák fel a leveleket, ha magasabb prioritású szerver nem elérhető. A bejegyzés formája:

```
belso.local. 10 MX w2k8s.belso.local.  
belso.local. 20 MX barmi.belso.local.
```

Ebben a példában az alapértelmezett levelezőszerver a „w2k8s” nevű gép lesz, hiszen neki kisebb a száma, vagyis ő a magasabb prioritású. Arra azért figyelni kell, hogy az így meghatározott gépekhez lennie kell „A” rekordnak is bejegyezve.

## **SRV – „Service” rekord, szolgáltatásrekord**

A tartomány részére nyújtott szolgáltatást határoz meg. Gyakorlatilag az MX rekord kibővítése, hogy más szolgáltatásokat is be lehessen jegyezni a DNS-be. Általános alakja:

```
_service._proto.name TTL class SRV priority weight port target
```

Ahol a „\_service” a szolgáltatásnak adott név, a „\_proto” a szolgáltatást szállító protokoll (pl.: \_tcp), a „name” a tartomány neve, a TTL a „Time To Live” érték, a „class” mindig „IN”, a „priority” az MX rekordnál megismert prioritás, a prioritáson belüli súlyozás, a „port” a portcímet határozza meg, míg a „target” a célállomást határozza meg domain alakban, például:

```
_cs._udp.belso.local 86400 IN SRV 10 20 27015 cs.belso.local.
```

## **PTR – „Pointer” rekord, a reverse zóna bejegyzése**

Ez az „A” rekord fordítottja, ami az IP-címhez írja le a gép nevét. Ezt jellemzően szerverek használják, hogy kiderítsék, hogy egy hozzájuk érkezett IP-csomag milyen domainhez is tartozik. Formája:

```
254 PTR w2k8s.belso.local.
```

### 13.5 Használat

Minden olyan gépen, ahol ezt a DNS szerveret használják névfeloldásnak, a gépek meghatározásánál használhatók a domainnevek is. Például a szerver elérhető „server.pelda.local” vagy [www.pelda.local](http://www.pelda.local) névvel is.

A böngészőben megadva az előbbi nevet, bejön az IIS kezdőoldala. Vagy FTP esetén, a kiszolgáló címénél használhatjuk az [ftp.pelda.local](ftp://pelda.local) nevet.

A „ping” parancs paraméterének is megadhatjuk bármelyik általunk definiált domainnevet, pl. „ping xp.pelda.local”.

Ha nem szeretnénk mindig kiírni a domain nevét is, akkor minden gépen be kell állítani ezt. DHCP esetén azonban csak egy helyen kell állítani, a „Server Options” „DNS Domain Name” mezőt kell módosítani. Jelen példában a domainnév a „pelda.local”, tehát ezt kell ebbe a mezőbe is írni.

A munkaállomások frissítése után már használhatók lesznek a rövid nevek is egy gép eléréséhez. Például a „ping server” is működik.

## 14. 16. lecke: II. témazáró feladatsor

**1. Válassza ki azokat a hálózati jellemzőket, amiket egy DHCP szerverrel ki lehet osztani egy munkaállomásnak! Több jó válasz is lehetséges! (2 pont)**

- a) MAC cím
- b) DNS szerver címe
- c) Az alapátjáró címe
- d) Mail szerver címe
- e) WINS szerver címe

**2. A DHCP szerver beállításainál melyik elemnél kell felvenni fix IP-címet? Írja le, hogy mi az elnevezése ennek az elemnek! (1 pont)**

**3. Írja le, mire szolgál az „Exclusion Range” DHCP szerver „Address Pool” beállításánál! (2 pont)**

**4. Mit jelent magyarul a DHCP beállításoknál a „Lease Time”? Válassza ki a helyes megoldást! (1 pont)**

- a) Elengedési idő
- b) Bérleti idő
- c) Frissítési idő
- d) Dinamikus kiosztás ideje

**5. Milyen szolgáltatás mellett felesleges a WINS? Válassza ki a helyes megoldást! (1 pont)**

- a) DHCP
- b) FTP
- c) AD
- d) DNS

**6. Melyik az a parancs, amivel a DNS szerverek működését lehet ellenőrizni? (1 pont)**

**7. Válassza ki azokat a DNS rekordokat, amelyek hostokhoz kapcsolódnak! Több jó válasz is lehetséges! (2 pont)**

- a) A
- b) SOA
- c) SRV
- d) MX
- e) CNAME

## **15. 17-18. lecke: Egy gép, két hálózat**

### **15.1 Részcélkitűzések**

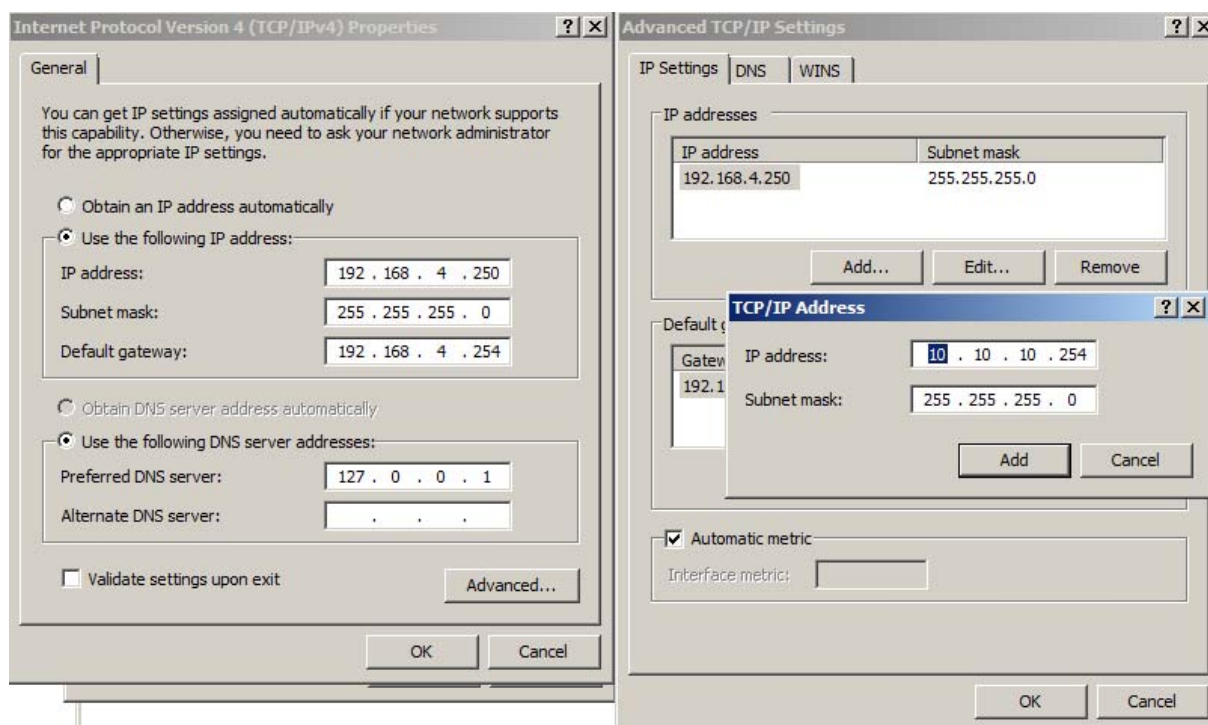
A tanuló ismerje a különböző címzési rendszereket, különbségeiket. Tudjon egy interfészhez több IP-címet is beállítani. Legyen képes két hálózati interfész esetén is beállítani a TCP/IP protokoll jellemzőit. Két interfész esetén is legyen képes a DNS szolgáltatást megfelelően konfigurálni. Legyen képes úgy beállítani a DHCP szolgáltatást, hogy csak az egyik interfészen szolgáltasson. Tudja ellenőrizni egy munkaállomásról is a hálózatok és beállított szolgáltatások (DNS, DHCP) elérhetőségét, működését.

### **15.2 Két IP egy gépen**

Minden hálózati interfésznek kell hogy legyen egy fizikai címe. Elvileg ezt a gyártó határozza meg, ami nem változik, amíg a kártya működőképes. Ennek a címnek egyedinek kell lennie, legalábbis azon a hálózati szegmensen, ahol a kártya kommunikál.

Az IP-címeket tekintve már rugalmasabb a rendszer. Bármilyen operációs rendszerről is van szó, egy interfészhez több IP-címet is hozzá lehet rendelni. Itt most csak a teljesség kedvéért van bemutatva, hogy hogyan kell ezt beállítani, a NAT szolgáltatáshoz ez nem szükséges!

A TCP/IP beállításoknál, ahol az IP-címet meg lehet adni, lennie kell egy speciális beállításnak is, a Windows Server 2008-nál ez az „Advanced...” gombbal érhető el.



**18. ábra. Második IP-cím beállítása**

### 15.3 Két interfész egy gépben

Az első hálózati kártya beállításai rendben vannak. A szerver ezzel kapcsolódik a 192.168.4.0/24-es hálózatra.

A második interfésznél be kell állítani, hogy az IP-cím 10.10.10.254 legyen, a maszk 255.255.255.0, átjárót nem kell megadni, DNS-nek pedig a 127.0.0.1 kell.

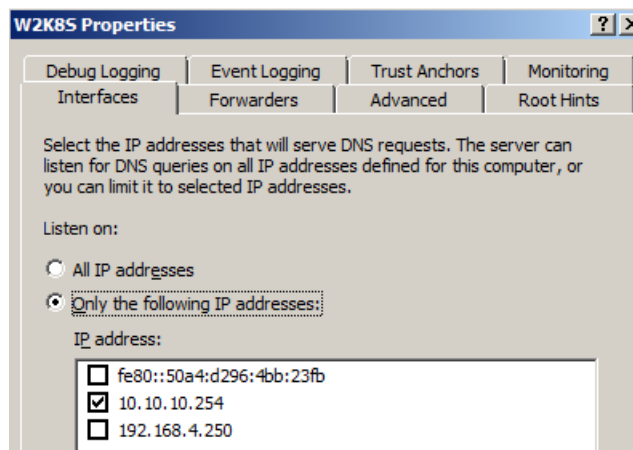
### 15.4 Egy szerver, két hálózat

A második IP-cím megadásával a szerver mindkét hálózatnak tagja lett. A 192-es hálózaton keresztül éri el az internetet, a 10-esen keresztül pedig majd a munkahelyeket. A helyes működéshez módosítani kell a DNS és DHCP szolgáltatásokat, mivel a munkahelyek innentől kezdve már csak a szerveren keresztül tudnak majd kommunikálni.

### 15.5 A DNS szolgáltatás beállítása

A DNS szerver beállításainál (gyorsmenü „Properties” menüpont) kiválasztva az „Interface” fülön állítsuk be, hogy csak a 10-es hálózaton szolgáltasson.



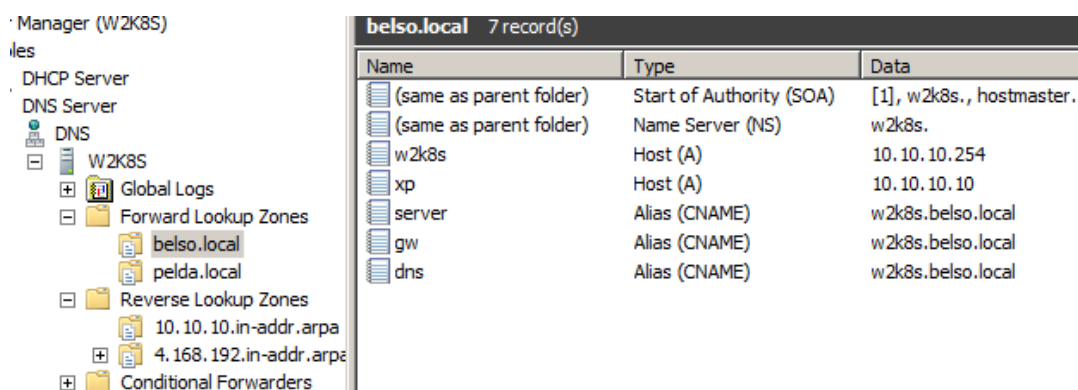


**19. ábra. DNS beállítás módosítása**

Módosítani kell továbbá a zóna bejegyzéseit is. Mivel a 192-es hálózat felől nem fogadunk el kéréseket, minden 192-es bejegyzés feleslegessé vált. A saját zónánk ugyanis csak a 10-es hálózatra korlátozódik. Ennek megfelelően módosítsuk a bejegyzéseket.

Ezt legegyszerűbben úgy tehetjük meg, hogy létrehozunk egy új zónát, mondjuk „belso.local” névvel, a DNS telepítésénél leírtaknak megfelelően, akár a varázslóval is, vagy a szerver („W2k8S”) gyorsmenüjéből „New Zone...” menüponttal. Az utóbbi esetén most is elsődleges („Primary zone”) zónát akarunk, először „Forward lookup zone”, a zóna neve „belso.local”, a fájlnev marad, és nem engedélyezzük a dinamikus frissítést. Megint új zóna, megint elsődleges, most a „Reverse lookup zone”-t választjuk, IPv4, majd a hálózathoz („Netword ID”) „10.10.10”-et írunk, a fájlnev marad, és most sincs frissítés.

Válasszuk ki a „belso.local” zónát a forward zónák közül. Majd vegyük fel a szerverhez „w2k8s” névvel és 10.10.10.250-es IP egy „A” rekordot. Vegyük fel a munkaállomást is „xp” és 10.10.10.10 adatokkal. Vegyünk fel alias neveket („CNAME” rekord) a szerverhez: „server”, „gw” és „dns”. Ne felejtsük el mindig bepipálni a „Create associated pointer (PTR) record”-ot, hogy a reverse zónába is bekerüljenek az adatok!



**20. ábra. DNS új zóna beállítása**

## 15.6 A DHCP szolgáltatás beállítása

A célunk az, hogy a munkaállomásunk 10.10.10.0/24-es hálózathoz kapjon IP-címet, és az átjáró és a DNS is a 10.10.10.254, vagyis a szerver legyen, és a domainnév már a „belso.local”.

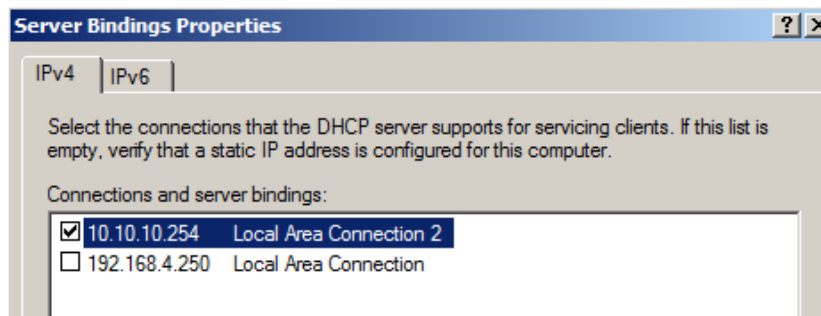
Első lépésben tiltsuk le az előzőleg létrehozott scope-ot. Ehhez a scope gyorsmenüjében válasszuk ki a „Deactivate” elemet.

Hozzunk létre egy új scope-ot az „IPv4” gyorsmenü „New Scope...” menüpontjával. A név legyen „Belso”, a „Start IP Address” és az „End IP Address” legyen egyaránt „10.10.10.100”, a maszk pedig legyen „255.255.255.0”. Az „Add Exclusions and Delay” oldalon pedig zárjuk is ki rögtön a fenti IP-t, vagyis a „10.10.10.100”-at. A „Lease Duration” maradhat az alapértelmezés. Az opciókat beállíthatjuk most vagy később is. Most egyszerűbb. A „Router (Default Gateway)”-nél a „10.10.10.254”-et adjuk meg. A „Domain Name and DNS Servers”-nél a „Parent Domain” legyen a „belso.local”, az IP-címet pedig írjuk át 10.10.10.254-re, mivel a belső hálózathoz ezen a címen lehet elérni a DNS szerveret. Megadhatjuk a WINS szerver címét, ami most szintén a szerver belső hálózatos címe. És végül azonnal aktiválhatjuk is a scope-ot.

Végül vegyük fel a munkaállomást a „Reservations” részben, 10.10.10.10-es IP-címmel.

A DHCP szervernél is be kell állítani, hogy melyik interfészen keresztül szolgáltatson. Itt is az a cél, hogy csak a belső hálózat felé szolgáltatson.

Ehhez a szerver gyorsmenüjében válasszuk ki az „Add/Remove Bindings...” menüpontot, majd csak a 10-es IP előtt hagyjuk meg a pipát.



**21. ábra. DHCP csak egy IP-n**

## **15.7 Ellenőrzés**

A munkaállomáson frissítsük a hálózati beállításokat („ipconfig /release” és „ipconfig /renew” parancsokkal, vagy újraindítással). Ellenőrizzük, hogy a saját szerverünktől kaptunk-e IP-címet („ipconfig /all”).

A ping és nslookup parancsok segítségével ellenőrizzük a számítógépek (szerver és munkaállomás) elérhetőségét, valamint a DNS szolgáltatás működését. Külső cím nem lesz elérhető a belső hálózathoz, hiába van jól beállítva a szerver. Ami hiányzik, az a NAT. Mindaddig, amíg nincs beállítva, külső kapcsolatot nem lehet felépíteni, például az index.hu sem elérhető el, sem pinggel, sem böngészőből.

## **16. 19-20. lecke: Windows NAT**

### **16.1 Részcélkitűzések**

A tanuló ismerje a NAT szolgáltatás feltételeit, a lehetőségek korlátait. Legyen képes megfelelően előkészíteni a hálózati beállításokat és szolgáltatásokat a NAT megvalósításához. Tudjon NAT szolgáltatást telepíteni a szerverre. Legyen képes beállítani az igényeknek megfelelően a NAT szolgáltatást, illetve legyen képes ellenőrizni a NAT szolgáltatás működését.

### **16.2 Előfeltételek**

NAT-olni csak két hálózat között lehet, ezért a használatához két különböző hálózatra van szükség. Az eddigi példákban a 192.168.4.0/24-es hálózat szerepelt. Most kiegészítésre kerül egy 10.10.10.0/24-es hálózattal.

A 192-es lesz a külső hálózati kapcsolat, míg a 10-es a belső. A munkaálomás a belső hálózat tagja lesz. A szerveren meg kell oldani, hogy mindkét hálózat tagja legyen. Ez megoldható úgy is, hogy még egy hálózati kártya kerül a gépbe, de úgy is, hogy még egy IP-címet kap a jelenlegi interfész. Ez utóbbi megoldás egyszerűbb ugyan, de a NAT beállításához nem jelent megoldást. Mindenképpen két hálózati kártyára van szükség. Ha virtuális gépen dolgozunk, akkor ez könnyedén megoldható, aktiválunk egy második hálózati interfészt.

A továbbiakban a szerveren módosítani kell a hálózati beállításokat, a második hálózati kártyához is be kell állítani a hálózatot. Majd módosításra szorulnak a DHCP és DNS beállítások is. Mindkét esetben be kellene állítani, hogy csak a belső hálózat (10.10.10.0/24) felé szolgáltatassanak. A DHCP szerveren új scope-ot érdemes felvenni, amelyben már a 10-es hálózat szerepel, az előzőt pedig érdemes letiltani („Deactivate”).

Miután ezek a módosítások megtörténtek, és a hálózati kapcsolatok ellenőrzése is rendben, csak utána érdemes telepíteni a NAT szolgáltatást a szerverre.

### **16.3 NAT telepítése**

1. A NAT telepítése is a „Server Manager” „Add Roles” gyosmenüpontjával történik.
2. A „Server Roles”-nál válasszuk ki a „Network Policy and Access Services”-t.
3. Majd a „Role Services”-nél a „Routing and Remote Access Services”-t.
4. Az összefoglaló képernyő után „Install”.

### **16.4 NAT beállítása**

1. Amíg nincs bekonfigurálva, nem is indul el a szolgáltatás. Beállítani a „Roles” listában a „Network Policy Access Services”-nél lehet, a „Routing and Remote Access”-t kiválasztva.

2. A gyorsmenüből válasszuk ki a „Configure ...” kezdetű elemet. Majd a felsorolásból válasszuk a NAT-ot („Network address translation (NAT)”).
3. Ki kell választani a publikus kapcsolatot, ami jelen pillanatban a 192.168.4.250-es IP-jű kapcsolat.
4. Majd „Finish”.
5. Innentől kezdve működik is.

## **16.5 Használat**

A kliens gépen most már működik a „ping index.hu”, de a böngészőben is elérhető minden külső internetes cím is.

## **17. 21-22. lecke: Windows Proxy**

### **17.1 Részcélkitűzések**

A tanuló ismerje a NAT és proxy szolgáltatás közötti különbségeket. Legyen tisztában a proxy Windows alatti megvalósítási lehetőségeivel. Legyen képes telepíteni a Microsoft Forefront TMG proxyt. Ismerje a TMG legfontosabb lehetőségeit, beállításait. Legyen képes az igényeknek megfelelően beállítani a TMG-t. Legyen képes a klienseken beállítani és használni a proxy szolgáltatást.

### **17.2 Előzetes megfontolások**

Egy proxy szerver hasonló funkciót lát el, mint a NAT, csak célzottan egy adott alkalmazási protokollra, jellemző módon a HTTP, vagyis a weboldalak elérésére használt protokollra.

A proxy előnyei a NAT-hoz képest, hogy cache-csel, vagyis átmenetileg tárolja a rajta átmenő oldalakat, valamint képes rengetegféleképpen szűrni az átmenő forgalmat.

A proxy nem része a rendszernek. Az SBS változatokon kívül egyetlen Windows szerverváltozat sem tartalmazza. Az előző hivatalos proxykat ISA (Internet Security and Acceleration Server) szervernek nevezik. Az

ISA változatokból egyáltalán nincs 64 bites, és nem lehet telepíteni egyiket sem 64 bitre.

Elkészült az új változat, aminek a neve megváltozott, most már „Forefont Threat Management gateway”. A korlátozott (120 napig használható) változata – regisztrálás után – letölthető a következő oldalról:

<http://www.microsoft.com/Forefront/en/us/trial-software.aspx>

Lehetőség van arra is, hogy nem Microsoft terméket használunk proxy szerverként. Elérhető például a WinGate nevű termék is, amiből van 64 bites változat is, persze ezért is fizetni kell. Több olyan fizetős termék is van, ami jó alternatívája lehet a windowsos proxy szervernek.

Létezik azonban ingyenes megoldás is erre a feladatra. Az alapvetően Linux rendszerekhez fejlesztett „Squid” proxy szervernek van Windows alatt futtatható változata is, ami teljesen ingyen, szabadon felhasználható, és futtatható 64 bites rendszeren is.

Itt most csak a Forefont TMG-vel foglalkozunk.

### **17.3 TMG Telepítés**

1. A letöltött TMG\_ENU\_EE\_EVAL\_AMD64.exe fájlt el kell indítani a szerveren.
2. Ki kell választani a célkönyvtárat, maradhat az alapértelmezés is.
3. Az install előtt frissíteni kell a rendszert a legutolsó „service pack”-re.
4. Telepíteni kell a szükséges szolgáltatásokat („Run Preparation Tool”). Itt az első kérdésnél a legfelső elemet kell választani, a „Forefont TMG Services and Management” elemet, majd a végén „Finish”, minek hatására automatikusan elindul a TMG telepítése.
5. El kell fogadni a licence-et („I accept ...”).
6. Megadható a felhasználói név és a szervezet.
7. Kiválasztható az a könyvtár, ahova telepítésre kerül a TMG.

8. Meg kell határozni a belső hálózatot. Ehhez először az „Add...”, majd a megnyíló ablakban az „Add Adapter”-t kell kiválasztani. Végül ki kell pipálni azt a hálózati interfészt, ami a belső hálózathoz kapcsolódik.

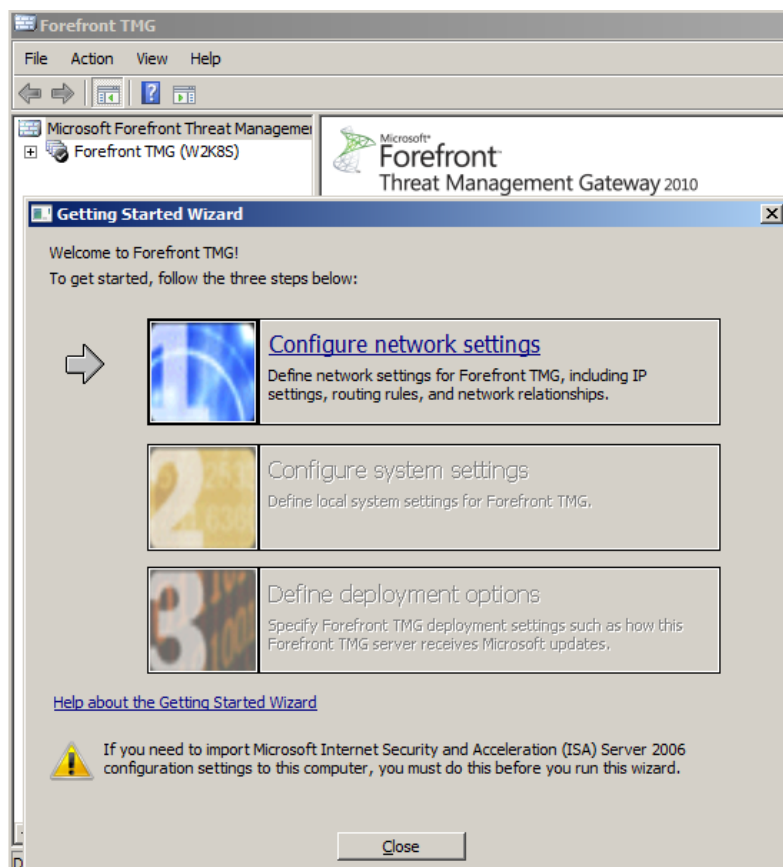
9. Majd „Install”.

## 17.4 TMG Beállítások

A TMG-nek külön kezelőprogramja van, nem épül be a „Server Manager” felületbe. A kezelőprogramot a „Start menü”, „All Programs”, „Microsoft Forefront TMG” menü „Forefront TMG Management” menüpontjával lehet indítani.

### 17.4.1 Hálózati beállítások

Az első indításnál megjelenik a beállító varázsló („Getting Started Wizard”), ahol első lépésként a hálózati beállításokat („Configure Network Settings”) kell elvégezni.



22. ábra. TMG konfigurálás

Ki kell választani a hálózat felépítését, pontosabban a proxy helyét a hálózatban. Jelenleg az „Edge Firewall” beállítás jó.

Ezután ki kell választani a LAN adaptert, ami a 10-es hálózat elérésére szolgáló kártyát jelenti.

A következő lépésben az internetbeállítások, vagyis a külső kapcsolat kiválasztása történik. Itt a 192-es hálózat kártyáját kell választani.

Majd a „Finish”-re befejeződik a hálózat beállítása.

#### **17.4.2 Rendszerbeállítások**

Következik a rendszer beállítása („System Configuration”). Első lépésben a gép azonosítóit kell meghatározni, illetve a DNS utótagot lehet beállítani. Ide érdemes megadni a belső hálózat domainnevét („belso.local”). Ha változtattunk valamelyik beállításon, azonnal újraindítja a szerveret.

Folytathatjuk a beállítást, majd következik a harmadik opció, a „Define Deployment Options”.

#### **17.4.3 Véglegesítési beállítások**

Bekapcsolhatjuk a „Microsoft Update” szolgáltatást a TMG részére.

A TMG használatához mindenképpen szükség van megfelelő licence-ekre. A frissítés csak így működik, frissítés nélkül pedig nem tekinthető megbízhatónak.

A következő lépésben visszajelzést lehet adni a termékkel kapcsolatban, most nem tesszük („No, ...”).

Az információküldés részletességét lehet állítani, most is azt választjuk, hogy nem adunk információt („None, no ...”).

Majd jöhet a „Finish” és utána a „Close”.

#### **17.4.4 Hozzáférési beállítások**

Automatikusa indul a „Web Access Policy Rules” varázsló, ami első lépésben felajánlja a minimálisan szükséges beállítások automatikus elvégzését. Hagyjuk neki, vagyis marad a „Yes ...” kezdetű beállítás.



Következő lépésben megjeleníti az általa veszélyesnek ítélt oldalak listáját, amit itt lehet még bővíteni az „Add...” gombbal. Most nem kell, tehát „Next”.

Bekapcsolva hagyhatjuk a tartalomfigyelést, ami nem fogja engedni a zip fájlokat sem.

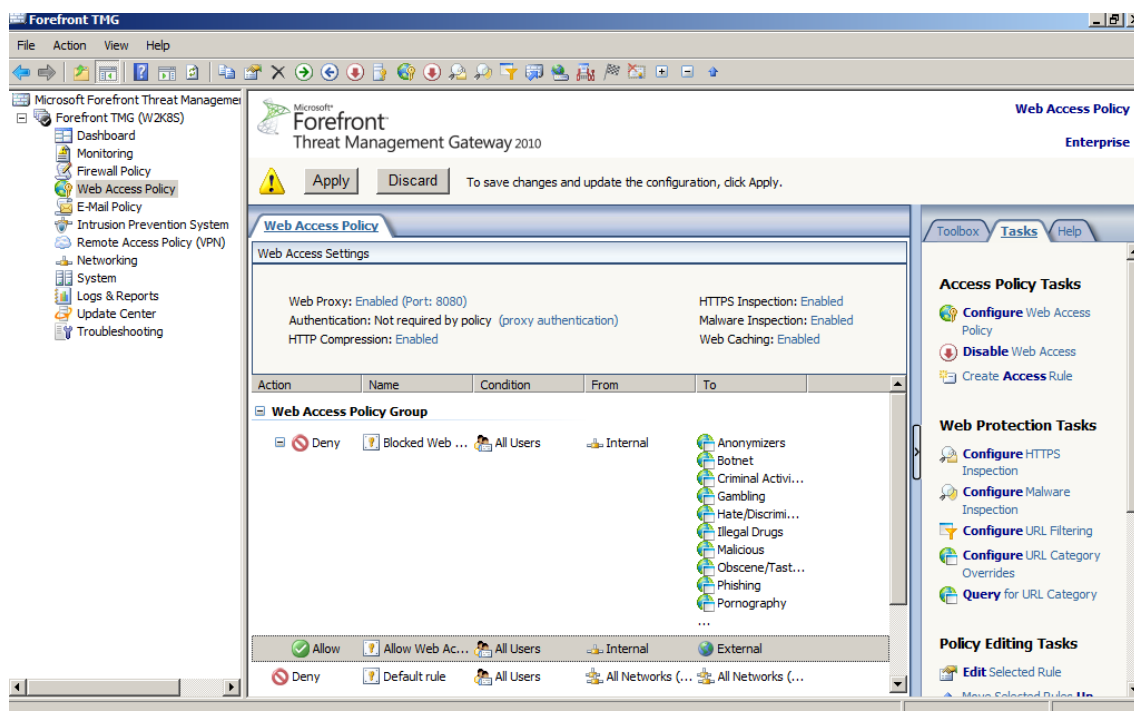
HTTPS azonosítási beállítás következik. Maradhat az alapértelmezés („Allow users ...”). A következő lépésben is marad az alapértelmezés.

Meg kell határozni egy útvonalat és egy fájlnévet, amiben a generált aláírás lesz tárolva. Most egyszerűen „w2k8s” lett megadva.

Meghatározhatjuk a cache helyét és méretét. A méretet mindenképpen be kell állítani, mert alapban 0. Döntsük el, mennyi helyet szánunk rá. Most legyen 200MB. Egyébként erre a célra mindenképpen célszerű külön partíciót kialakítani.

Majd az összefoglaló képernyőn „Finish”, és használatra kész a proxy.

A „Forefont Manager”-ben minden eddigi beállítás is módosítható, sőt több más is. Például módosítani lehet az alapértelmezésben 8080-as portot is.



**23. ábra. Forefont TMG konfigurálás**

Figyeljünk oda, hogy a Forefront TMG gyakorlatilag egy tűzfal, ami alpból blokkol mindent, amit nem engedünk. Első komoly meglepetés az lehet például, hogy a TMG után nem megy a DHCP szerver, mivel a 67-es portra irányuló kommunikációt is blokkolja. A szép az, hogy legalább logolja, így kiderül, hogy mi az, amit nem enged.

The screenshot shows the Microsoft Forefront Threat Management Gateway (TMG) 2010 interface. On the left is a navigation pane with options like Dashboard, Monitoring, Firewall Policy, Web Access Policy, E-Mail Policy, Intrusion Prevention System, Remote Access Policy (VPN), Networking, System, Logs & Reports, Update Center, and Troubleshooting. The main window is titled 'Forefront Threat Management Gateway 2010' and has tabs for 'Logging' and 'Reporting'. The 'Logging' tab is active, showing a table of log entries. The table has columns: Log Time, Client IP, Destination IP, Destination Port, Protocol, Action, and NIS. One entry is highlighted in blue, showing a denied DHCP request from 0.0.0.0 to 255.255.255.255 on port 67. Below the table, there is a detailed view of the selected log entry, titled 'Denied Connection' with the timestamp 'W2K85 2011.04.05. 17:59:37'. It shows the log type as 'Firewall service', status as 'The policy rules do not allow the user request.', rule as 'Default rule', source as 'External (0.0.0.0:68)', destination as 'Local Host (255.255.255.255:67)', and protocol as 'DHCP (request)'. Additional information includes 'Number of bytes sent: 0', 'Number of bytes received: 0', 'Processing time: 0ms', and 'Original Client IP: 0.0.0.0'.

Log Time	Client IP	Destination IP	Destination Port	Protocol	Action	NIS
2011.04.05. 17:59:37	10.10.10.254	10.10.10.255	137	NetBios Name Ser...	Denied...	
2011.04.05. 17:59:37	0.0.0.0	255.255.255.255	67	DHCP (request)	Denied...	
2011.04.05. 17:59:37	0.0.0.0	255.255.255.255	67	DHCP (request)	Denied...	
2011.04.05. 17:59:37	10.10.10.254	10.10.10.255	137	NetBios Name Ser...	Denied...	
2011.04.05. 17:59:37	192.168.4.250	192.168.4.255	137	NetBios Name Ser...	Denied...	

**Denied Connection** W2K85 2011.04.05. 17:59:37

**Log type:** Firewall service  
**Status:** The policy rules do not allow the user request.  
**Rule:** Default rule  
**Source:** External (0.0.0.0:68)  
**Destination:** Local Host (255.255.255.255:67)  
**Protocol:** DHCP (request)

**Additional information**

- Number of bytes sent: 0 Number of bytes received: 0
- Processing time: 0ms Original Client IP: 0.0.0.0

#### 24. ábra. A Forefront TMG blokkolja a DHCP kommunikációt is

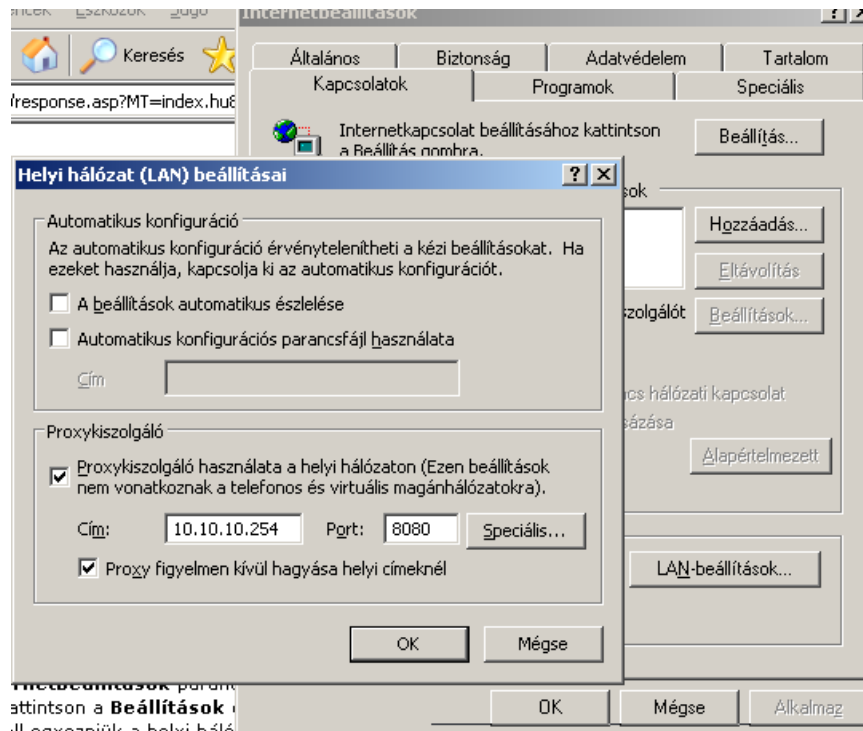
Ez ugyanígy volt az ISA szerverek esetén is. Mindent külön be kell neki állítani. A beállítások után ne felejtsünk el az oldal tetején középen az „Apply” gombra kattintani, különben nem jut érvényre a módosítás!

Külön szabályt kell felvenni a „Firewall Policy” részben, ahol engedni kell a „DHCP (request)” és a „DHCP (reply)” protokollt is. A forrás- és a célhálózathoz nem kell adni semmit, ha nem akarunk, ilyenkor ugyanis mindenki-re vonatkozik.

## 17.5 Használat

Azoknál a számítógépeknél, ahol szeretnénk használatba venni a proxyt, külön be kell állítani az internetkapcsolatnál. Ezt Internet Explorer esetén

az „Eszközök” menü „Internet beállítások menüpont kiválasztásával”, majd a „Kapcsolatok” fül, „LAN beállítások” gombot kiválasztva lehet beállítani. A megnyíló ablakban a „Proxy kiszolgáló” részbe tegyünk pipát, majd a „Cím”-hez írjuk be a proxy szerver IP-címét (Jelenleg ez 10.10.10.254), a „Port”-hoz pedig a beállított portot (alapesetben 8080).



**25. ábra. Proxy beállítás a kliensen**

A beállítás után újra kell indítani a böngészőt, és már működik is. Azonban, ha bármilyen oldalt beírunk, mindig ugyanazt az üzenetet kapjuk, de már a proxytól. Gyakorlatilag semmilyen kapcsolatot nem enged. Valamiért a beállított belső hálózatból kifelé menő engedélyezett forgalom nem megy. Újra kell engedélyezni a „Forefont TMG” „Web Access Policy”-ban. Itt a középső részben van egy „Allow” sor, amire duplán kattintva előjön a beállító ablak. Nem kell módosítani semmit, csak el kell fogadni, majd „Apply”.

## 18. 23. lecke: Windows e-mail

### 18.1 Részcélkitűzések

A tanuló ismerje és értse az elektronikus levelezéssel kapcsolatos legfontosabb alapfogalmakat. Ismerje a levelezésben használt protokollokat, használatukat. Legyen tisztában a levelező szolgáltatás Windows szerveren történő megvalósítás lehetőségeivel. Tudjon SMTP szolgáltatást telepíteni a szerverre, és legyen képes beállítani az SMTP szolgáltatást. Tudjon levelet küldeni egy kliens számítógépről a beállított SMTP szolgáltatáson keresztül.

### 18.2 Alapfogalmak

Az e-mail a weboldalak böngészése mellett a másik legelterjedtebb szolgáltatás. Mindenkinek lehet akár több ingyenes e-mail postafiókja.

A **postafiók** gyakorlatilag egy tároló hely, ahol a felhasználónak címzett levelek érkeznek és tárolódnak, valamint a küldött levelek is itt kerülnek elhelyezésre. A postafiókot egy felhasználói név és magának a szervernek a domainneve azonosítja. Például a [valaki@gmail.com](mailto:valaki@gmail.com) egy e-mail cím, ahol a „valaki” a felhasználó neve, míg a gmail.com a szerver domainneve, ahol a postafiók adatai tárolásra kerülnek.

A **levelezőszerver** feladata a levelek továbbítása a címzettek részére, valamint fogadni az érkezett leveleket, és elhelyezni azokat a megfelelő postafiókokban. A szerver a levelek küldésére és fogadására az SMTP protokollt használja, ezért **SMTP szervereknek** is nevezik őket.

A **levelező programok** olyan alkalmazások, amelyekkel a felhasználók férhetnek hozzá a postafiókjuk leveleihez. A leveleket letölteni a postafiókból vagy **POP3** vagy **IMAP** protokollon keresztül lehet. Ugyancsak a levelező programok azok, amelyek a beállított levelezőszerver felé küldik el azokat a leveleket, amiket a felhasználó ír. A küldéshez azonban már az **SMTP** protokollt használják a levelező programok is.

Ma már rendszerint **böngészővel** férünk hozzá a leveleinkhez. Ez a webes felület általában magán a postafiókokat tároló szerveren van. A felhasználó

lónak nem is kell tudnia arról, hogy a levelekhez IMAP protokollon fér hozzá, mivel ez a háttérben automatikusan megtörténik.

A **levelezés működése** során, amikor a felhasználó levelet küld, azt a saját SMTP szerverének küldi. A szerver megnézi, hogy a címzett saját postafiók-e, vagyis a célcím domainneve megegyezik-e a saját domainnével. Ha azonos, akkor közvetlenül elhelyezi a megfelelő postafiókban. Ha nem azonos, akkor DNS lekérdezésekkel megkeresi, hogy az adott céldomainhez milyen IP-címen érhető el az SMTP szerver, vagyis **MX rekord** bejegyzést keres. Ha megvan a szerver címe, akkor az SMTP protokollal továbbítja neki a levelet.

Fontos megjegyezni, hogy egy SMTP szerver nem fogad akárhonnan továbbításra (**relay**) leveleket. Jellemzően csak a saját hálózatát tekinti megbízhatónak, és mástól nem fogad el semmit. Az internetszolgáltatónk rendszerint üzemeltet saját levelezőszervert, és még postafiókot is biztosít rajta. Általában a kimenő SMTP forgalmat csak és kizárólag a saját szerverre felé engedélyezi. Vagyis ha ilyenkor normál levelező programmal akarunk levelet küldeni, akkor a kimenő szervernek a szolgáltató szerverét kell megadni.

### **18.3 Lehetőségek**

#### **Beépített SMTP szerver**

Az alap Windows Server 2008 R2 változatban csak SMTP szervert lehet telepíteni, POP3 és IMAP nélkül, ami azt jelenti, hogy postafiókok tárolására nem alkalmas. A felhasználók felől nézve azonban egy ilyen szerver elegendő arra, hogy a felhasználók levelet tudjanak küldeni a szerveren keresztül bárhova.

#### **MS Exchange szerver**

Több változata létezik, azonban a 2008 szerver alá már csak az Exchange 2007 és az Exchange 2010 telepíthető. A 2010-es változat már csak 64 bites rendszerre hajlandó települni. Használatához erősen ajánlott az Active Directory. A teljes változatért külön kell fizetni, nem része a Win-

dows Server 2008 változatoknak. Az MS Exchange 2010 120 napos próbaváltozata letölthető a következő címről:

<http://www.microsoft.com/exchange/en-us/try-it.aspx>

### **Fizetős e-mail szerverek**

Ha nem tetszik az alaprendszer, vagy nem akarunk exchange-et, akkor választhatunk más terméket is, hiszen több olyan rendszer is kapható, amelyik tudása megfelelő lehet. Néhány példa:

- Kerio MailServer – <http://www.kerio.com/mailserver>
- MailEnable Professional or above – <http://www.mailenable.com/>
- Softtalk Mail Server (Workgroup Mail Server) – <http://www.softtalkltd.com/products/workgroupmail/>

### **Ingyenes e-mail szerverek**

Több ingyenes e-mail szerver is elérhető Windows alá is, de a többség sajnos csak 32 bites, így 64 bites rendszeren nem használhatók. Az egyetlen kivétel a hMailServer, ami GPL alapú, és Windows 2008 64 bit alatt is fut.

## **18.4 SMTP szerver telepítés**

1. A „Server Manager” program „Futures” gyorsmenüjének „Add Futures” menüpontjával indítható a telepítés.
2. Ki kell választani a „Futures” listában az „SMTP”-t. Rögtön megjelenik egy ablak, megmutatva, hogy az SMTP szolgáltatáshoz milyen egyéb szolgáltatásokra van szükség. Adjuk is hozzá ezeket.
3. Az IIS-re is szükség van az SMTP-hez, így a következő lépésben ezt állíthatjuk, de már minden ki van jelölve, amire szükség van, így csak simán „Next”.
4. Az összefoglaló képernyőn pedig az „Install” hatására elindul a telepítés.

## 18.5 SMTP beállítás

Az SMTP szerver beállítása az IIS 6.0 Manager segítségével lehetséges. Ez a „Start menü”, „Administrative Tools”, „Internet Information Server (IIS) 6.0 Manager” menüponttal indítható el.

Az „SMTP Virtual Server #1” elem gyorsmenüjének „Properties” menüpontjával lehet elérni a beállításokat.

Amit mindenképpen célszerű beállítani, az az, hogy honnan fogadjon levelet, vagyis kiknek legyen átjáró (Relay). Ezt a felületet az „Access” fül „Relay” nyomógombjával lehet elérni. Célszerű felvenni itt a belső hálózatkat (10.10.10.0/24), valamint a localhostot (127.0.0.1) is.

## 18.6 Használat

Mivel az SMTP protokoll egy egyszerű szöveges, titkosítatlan protokoll, ezért egyszerűen a **telnet** parancs segítségével is lehet küldeni levelet az SMTP szolgáltatáson keresztül. A telnet segítségével csatlakozunk a levelezőszerver 25-ös portjára („telnet mail.belso.local 25”), majd a következő minta alapján pontosan – kis- és nagybetű is számít – soronként beírjuk a fejléc és a levél adatait. Bizonyos sorok után a szerver válaszát is meg kell várni. Akkor érdemes folytatni, ha a válasz „250”, mert ez jelenti azt, hogy „OK”.

```
HELO honnan.kuldom.hu
MAIL FROM: <en@honnan.kuldom.hu>
RCPT TO: <kinek@hova.kuldom.hu>
DATA
From: Tolem <en@honnan.kuldom.hu>
To: Neked <kinek@hoba.kuldom.h>
Subject: Barmi
Reply To: barhova@kuldheted.hu
Itt jöhet maga az üzenet szövege!
Akár több sorban.
A szöveg végét egy üres sorban beírt „.” jelzi.
.
QUIT
```

Az első három nagybetűvel kezdődő sor a fejléc. A „DATA” után elvileg bármi lehet.

## **19. 24-25. lecke: Windows e-mail 2**

### **19.1 Részcélkitűzések**

A tanuló legyen képes egy ingyenes levelezőszervert telepíteni és konfigurálni a szerveren. Legyen képes egy kliens gépen beállítani egy levelező programot a levelezőszerver használatához, és tudjon levelet küldeni és fogadni is.

### **19.2 hMailServer telepítése**

Indítsuk el a letöltött .exe fájlt, ami jelenleg a **hMailServer-5.3.3-B1879.exe**.

Adjuk meg a célkönyvtárat, például **c:\Mail\hMailserver**.

Kiválaszthatjuk a telepítendő összetevőket. Teljes telepítést („Full...”) akarunk.

Választhatunk, hogy a beépített vagy külső adatbázisrendszert kívánunk használni. Most a beépítettet használjuk.

Meghatározhatjuk a „Start menü”-ben megjelenő nevet. Alapban „hMailServer”, most jó ez.

Az összefoglaló képernyőn az „Install” hatására elindul a telepítés.

A telepítés végén meg kell adni az adminisztrátori jelszót.

Majd a „Finish” hatására el is indul az admin felület, ami indulásnál rákérdez, hogy kivel és hova akarok csatlakozni, majd a Connect hatására bekéri a jelszót is.

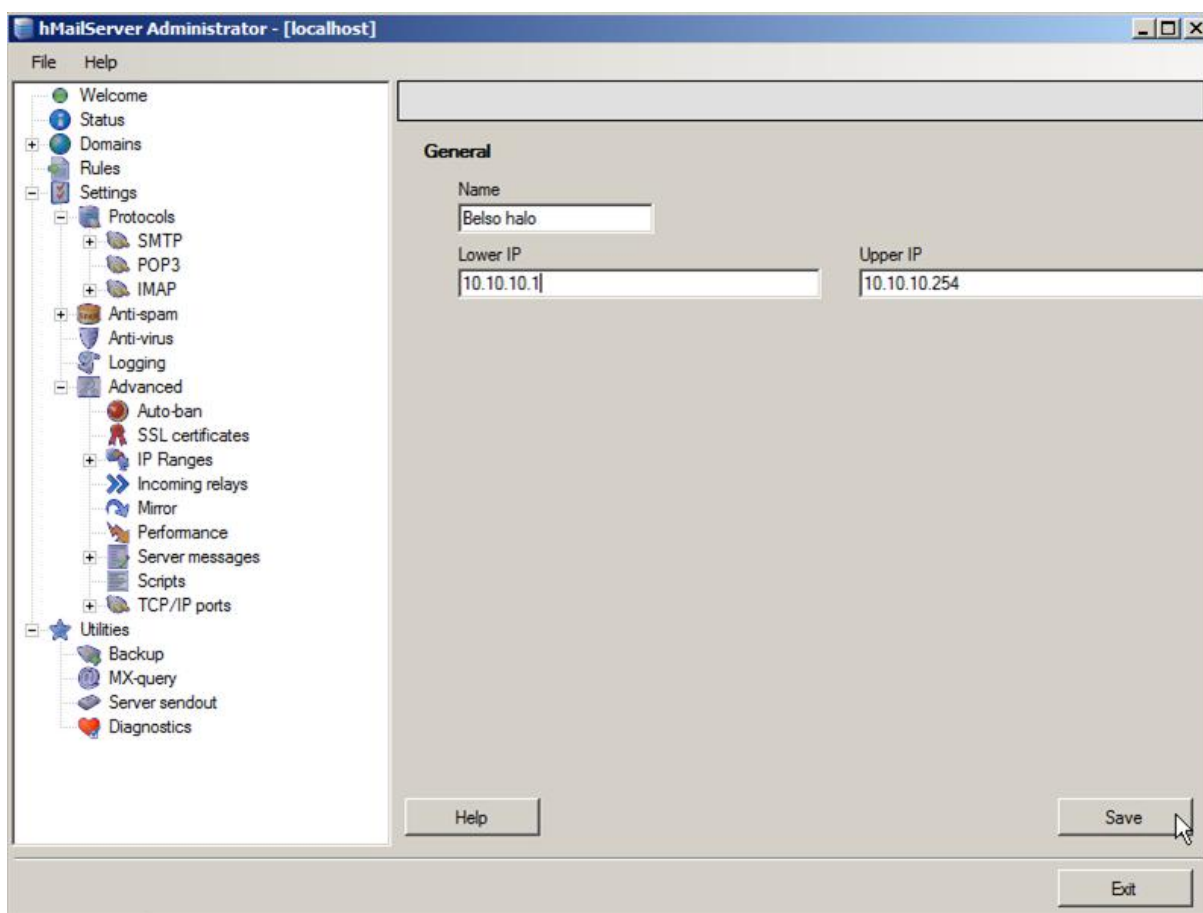
### **19.3 hMailServer beállítás**

Mielőtt használatba vennénk a szerverünket, módosítani kell a DNS beállításokat. Be kell állítani ugyanis egy MX rekordot, ami a szerver IP-címére mutat.



A hMailServer admin felületén pedig az első lépés a domainnév megadása, ami most a példában „belso.local”.

Célszerű rögtön az elején beállítani, hogy honnan is fogad el leveleket, amit továbbítani is fog. Most a példában csak a belső hálózat felől szeretnénk fogadni továbbításra leveleket, ezért a „Settings”, „Advanced”, „Incoming Relays” elemnél vegyünk fel („Add”) egy IP-tartományt, ami most célszerűen a 10.10.10.1 – 10.10.10.254.



## 26. ábra. hMailServer Relay tartomány beállítása

Ezek után következhet a felhasználók („Accounts”) felvétele. Ez gyakorlatilag a postafiókok létrehozását jelenti. Ami igazán probléma, hogy ezt egyenként kell megtenni. A felvétel a „Domains”, „belso.local”, „Accounts” részben lehetséges. A példa kedvéért vegyünk fel egy „info” és egy „teszt” fiókot.

Az AD-t tudja ugyan használni, de csak jelszó ellenőrzésére, a felhasználókat előtte fel kell venni, és be kell állítani, hogy tartományi felhasználó,

és meg kell adni a tartomány és a tartományi felhasználó nevet. Ezt a beállítást a fiókra kattintva, és jobboldalt az „Active Directory” fülön lehet elérni.

Érdemes bekapcsolni a logolást. Ezt a „Settings” „Login” szekciójában lehet megtenni, külön protokollokra bontva. Ugyanott a „Show Logs” gombra kattintva megnyílik a fájlkezelő, és megjeleníti a log fájlok könyvtárát. A logok egyszerű .txt fájlban kerülnek tárolásra, így a Notepaddel is megjeleníthető a tartalmuk.

Megfontolandó az „Auto-ban” szolgáltatás kikapcsolása vagy állítása. Alapban ugyanis, ha a felhasználó háromszor hibásan azonosítja magát, letiltja a felhasználót. Ezt a „Settings”, „Advanced”, „Auto.ban” részben lehet állítani.

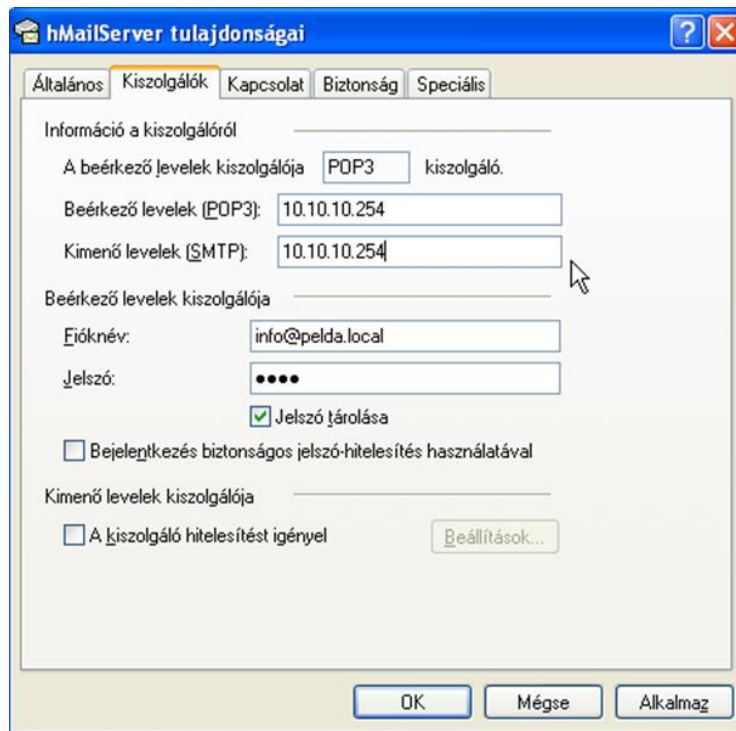
Szükségünk lehet arra is, hogy megadjuk, kin keresztül (relay szerver) továbbíthatunk leveleket. Ezt a „Settings”, „Protocols”, „SMTP” elem „Delivery of email” fülön, a „Remote Host Name” mezőben lehet megadni.

Engedélyezni kell még a Windows tűzfalán is az SMTP, POP3 és IMAP portokat. Ehhez fel kell venni egy új szabályt az „Inbound” részben, ahol egyszerre lehet engedni a 25, 110 és 143-as TCP portokat. Ha küldeni is akarunk, akkor külön szabály kell az „Outbound” részben, ahol elég csak a 25-ös portot engedni.

#### **19.4 hMailServer használat**

Kellemes lehetőség a hMailServer admin felületén, hogy egyszerre több felhasználónak (akár mindenkinek) is küldhetünk azonos tartalmú levelet. Ezt az „Utilities”, „Server sendout” eleménél érhetjük el.

A klienseken a levelező program beállításainál a szerver címe 10.10.10.254, a beérkező és a kimenő leveleknél is. Amire figyelni kell, hogy a felhasználó neve a teljes e-mail cím.



**27. ábra. Outlook Express beállítása**

## **20. 26. lecke: III. témazáró feladatsor**

### **1. Válaszoljon igennel vagy nemmel a következő kérdésre! (1 pont)**

Lehet-e egy hálózati interfésznek 3 IP-címe?

### **2. A „Server Roles”-nál melyik elemet kell kiválasztani, ha a NAT-ot szeretnénk telepíteni? Válassza ki a helyes megoldást! (1 pont)**

- a) Routing
- b) NAT
- c) Network Policy and Access Services
- d) AD
- e) IIS

### **3. Hogyan nevezik a Microsoft új proxy szerverét? (1 pont)**

**4. Melyik a Microsoft proxy alapértelmezett portja? Válassza ki a helyes megoldást! (1 pont)**

- a) 80/udp
- b) 80/tcp
- c) 3129/tcp
- d) 8080/tcp
- e) 443/tcp

**5. A kliens gépeken mit és hol kell állítani, ha használni szeretnénk a proxyt? (2 pont)**

**6. Melyik DNS rekord beállítására van szükség a levelezés helyes működéséhez? Válassza ki a helyes megoldást! (1 pont)**

- a) NS
- b) SOA
- c) A
- d) MX
- e) CNAME

**7. Mit nem tud a beépített SMTP szerver? Több jó válasz is lehetséges! (2 pont)**

- a) Levelet küldeni.
- b) POP3 protokollt kezelni.
- c) Postafiókokba elhelyezni a leveleket.
- d) Relay szerverként működni.
- e) Felhasználókat kezelni.

**8. Írja le azt a parancsot, amellyel a mail.teszt.hu gépen keresztül levelet lehet küldeni! (1 pont)**

## 21. 27. lecke: Összegző felmérés

A feladatok végrehajtásához szükség van egy frissen telepített Windows 2008 Serverre és egy Windows XP-s számítógépre (a gépek lehetnek virtuálisak is!). Mindkettőn telepítve kell lennie a legutolsó Service Pack-eknek, valamint a szükséges drivereknek!

A megoldás során az ellenőrzéseknél és a teszteléseknél készítsen képernyőmentéseket, amelyeket **felx\_y** névvel bmp vagy jpg kiterjesztésű fájlokban tároljon, ahol az „X” a feladat sorszáma, az „y” pedig a feladaton belüli mentés sorszáma, ha több képet is készít!

1. Állítsa be a szerver és kliens gépet úgy, hogy mindkettő a 10.3.xx.00/24 hálózat tagja legyen, a szerver 254-es IP-t kapjon, az XP pedig 15-öst! Az „xx” a munkahelyet azonosító szám! A kliensen az alapátjáró és a DNS címe is legyen 254, míg a szerveren ne állítsunk be átjárót, és DNS-t se! Ellenőrizze is a hálózati kapcsolatot a két gép között! (5 pont)
2. Nevezze át a szervert „Server”-re, az XP-s gépet pedig „Kliens”-re! (2 pont)
3. Telepítsen WINS szolgáltatást a szerverre, és állítsa a be a Kliens gépen azt, hogy használja is! (2 pont)
4. Telepítsen webszerver szolgáltatást a szerverre! Készítsen egyedi site-ot, „Sajat” névvel, ami a 8000-es porton lesz elérhető. Készítsen egy **index.html** fájlt a saját oldalhoz, amiben megjeleníti a nevét, osztályát és a dátumot, majd tesztelje is az oldal elérhetőségét a kliens gépről. (6 pont)
5. Helyezzen be egy második hálózati kártyát a szervergépbe! A hálózati beállításoknál adja meg a 192.168.xx.250/24 IP-t és maszkot, az átjáró és a DNS beállításoknál pedig a 192.168.xx.254-et. Az „xx” itt is a munkahelyet azonosító szám. A továbbiakban ez az interfész lesz a külső hálózati kapcsolat elérését biztosító interfész,

míg az alaplárcya a belső hálózathoz kapcsolódik. Ellenőrizze az átjáró és az internet elérhetőségét! (5 pont)

6. Telepítsen DNS szolgáltatást a szerverre! Állítsa be, hogy csak a belső hálózat interfészén (10.3.xx.254) legyen elérhető! Állítsa be a DNS szerveren, hogy a kéréseket a 192.168.0.254 (forwarder) felé továbbítsa! Állítsa be a hálózati beállításoknál, hogy a szerver mindkét interfészén és a kliensen is a most létrehozott DNS szerver címe legyen a DNS! Tesztelje a szerveren és a munkaállomáson is DNS szervere működését! (7 pont)
7. Készítsen a DNS szerveren egy új forward zónát, aminél a „vizsgaxx.local” zóna nevet állítsa be! Ne engedélyezzük a dinamikus frissítést! Készítsünk a belső hálózatunk részére egy reverse zónát is! Vegyük fel a zónákba a szervert „server” névvel, a kliens pedig „kliens” névvel. Készítsünk a szerverhez alias neveket, vegyük fel a „gw”, „dns”, „www” és „mail” alias neveket mindkét zónába! Készítsünk „NS” és „MX” rekordot a szerverhez! Tesztelje a szerver és a kliens alól is a névfeloldás működését! (10 pont)
8. Telepítse a DHCP szolgáltatást a szerverre! Állítsa be, hogy csak a belső hálózat (10.3.xx.0/24) felé szolgáltatson! A telepítésnél a scope neve legyen „Vizsgaxx”, a kiosztott tartomány pedig legyen 10.3.xx.50 – 10.3.xx.50! Állítsa be, hogy a kiosztott tartomány ki is legyen zárva! Vegye fel az XP gépet statikus, 10.3.xx.21 IP-címmel a DHCP megfelelő beállításánál, hogy mindig ezt a címet kapja! Állítsa be, hogy a kiosztott IP-cím mellett a következő adatokat is továbbítsa a szerver a klienseknek:
  - Maszk: 255.255.255.0
  - Átjáró: 10.3.xx.254
  - DNS: 10.3.xx.254
  - DNS: Domain Name: vizsgaxx.local
  - WINS: 10.3.xx.254

Ellenőrizze a kliens gép alól a DHCP szerver működését! (10 pont)

9. Telepítsen NAT szolgáltatást a szerverre! A külső kapcsolat a 192.168.xx.250-es! Ellenőrizze is a kliens gépről a NAT-olás működését! (3 pont)

10. Telepítsen a szerverre egy ingyenes e-mail szolgáltatást! Állítsa be, hogy a belső hálózathoz fogadjon el leveleket! Vegyen fel két felhasználót „proba1” és „proba2” névvel, és „pwd1” és „pwd2” jelszavakkal! Küldjön az admin felületről mindkét felhasználónak üdvözlő üzenetet! Állítsa be a Windows tűzfalat, hogy működjön is a levelezés! A kliens gépről az Outlook Express programmal töltse le a „proba1” felhasználó leveleit a szerverről, majd küldjön egy üzenetet a „proba2” felhasználónak! Vegyen fel az Outlook Expressben egy második fiókot, és ellenőrizze a „proba2” felhasználóval is, hogy megérkeztek-e a levelek! (10 pont)

## 22. Értékelés, feladatmegoldások

### I. témazáró feladatsor

1. c)
2. c)
3. WINS
4. b), d), e)
5. d)
6. C:\InetPub\wwwroot
7. h)

Összesen 8 pontot lehet szerezni. A pontozásnál a 2 pontos feladatoknál a részmegoldásért 1 pont jár. A témazáró akkor tekinthető eredményesnek, ha 80%-ot (6 pontot) sikerül elérni.

### II. témazáró feladatsor

1. b), d), e)
2. reservations
3. Segítségével ki lehet zárni a scope IP-címtartományából tetszőleges IP-tartományt. A kizárt IP-ket nem fogja kiosztani a szerver.
4. b)
5. c)
6. nslookup vagy ping
7. a), d), e)

Összesen 10 pontot lehet szerezni. A pontozásnál a 2 pontos feladatoknál a részmegoldásért 1 pont jár. A témazáró akkor tekinthető eredményesnek, ha 80%-ot (8 pontot) sikerül elérni.

### III. témazáró feladatsor

1. Igen
2. c)

3. Microsoft Forefont TMG
4. d)
5. Internet Explorer esetén az „Eszközök” menü „Internet beállítások” menüpont kiválasztásával, majd a „Kapcsolatok” fül, „LAN beállítások” gombot kiválasztva lehet beállítani. A megnyíló ablakban a „Proxy kiszolgáló” részbe tegyünk pipát, majd a „Cím”-hez írjuk be a proxy szerver IP-címét (Jelenleg ez 10.10.10.254), a „Port”-hoz pedig a beállított portot (alapesetben 8080).
6. d)
7. b), c), e)
8. telnnet mail.teszt.hu 25

Összesen 10 pontot lehet szerezni. A pontozásnál a 2 pontos feladatoknál a részmegoldásért 1 pont jár. A témazáró akkor tekinthető eredményesnek, ha 80%-ot (8 pontot) sikerül elérni.

### **Összegző felmérés**

Összesen 60 pontot lehet szerezni. A pontozásnál a részmegoldásokért is jár pont. A modulzáró akkor tekinthető eredményesnek, ha 60%-ot (36 pontot) sikerül elérni.

## **23. Irodalomjegyzék**

Kis Balázs, Szalay Márton: *Windows Server 2008 rendszergazdáknak*. 2008, Szak Kiadó Kft., 544 o.