DEBRECENI EGYETEM
INFORMATIKAI KAR

WINDOWS SERVER 2003 HÁLÓZATI MEGOLDÁSAI

Diplomamunka

Konzulens: Dr. Krausz Tamás
Egyetemi adjunktus

Készítette: Pistár Zoltán
Programtervező matematikus hallgató

Debrecen, 2008

Tartalomjegyzék

I. Bevezető

A Microsoft cég operációs rendszerei a világ számos pontján, az ipar számos területén képviseltetik magukat, az átlag felhasználóktól egészen a világ piacvezető, multinacionális cégeiig. Nap, mint nap hallunk a cég által bevezetett újdonságokról, forradalmian új technikákról, technológiákról. Dolgozatom témájának kiválasztásakor így arra törekedtem, hogy a Windows operációs rendszerek rejtelmeibe alaposabb belátást nyerjek, mivel én is ezen operációs rendszer család mellett teszem le a voksom. Diplomaszerzés után –akárcsak az egyetemi éveim alatt- Windows környezetben szeretnék fejleszteni, ezért a Windows Server 2003 hálózati megoldási című téma ideális választásnak tűnt számomra. Ezen dolgozattal egyúttal azt is szeretném bemutatni, hogy egy szerver üzemeltetése, egy hálózat karbantartása nem olyan ördögi faladat, mint azt az ember először gondolná, valamilyen konkurens operációs rendszer családról szerzett tapasztalatokból kiindulva.

Másik nem titkolt célom az egyetem során megszerzett hálózatkezelési ismereteim összegzése, megerősítése egy konkrét, elsősorban hálózati operációs rendszeren keresztül. (Pl: Windows Server 2003 DNS, DHCP, WINS szerverként való konfigurálása stb.)

A Windows Server 2003 több szempontból is mérföldkőnek számít a Microsoft életében. A korábban „Whistler Server” fedőnevű Windows Server 2003 termékcsalád a Windows Server operációsrendszer-sorozat következő generációja.

A „Whistler Server” Béta 1 és „Whistler Server” Béta 2 próbaverziókban alapozódtak meg az operációs rendszer kezelésének, megbízhatóságának, teljesítményének és biztonságának, illetve az XML alapú webes szolgáltatásoknak az újításai. A Windows Server 2003 3-as bétaverziója erre az alapra épít, és továbbfejlesztett együttműködési szolgáltatásokkal, illetve a Microsoft. NET keretrendszerrel bővíti a Windows Server 2003 szolgáltatásainak tárházát. A Windows Server 2003 termékcsalád hat alapvető tagja, melyek különböző célcsoportokat igyekszenek megnyerni:

1) Windows Server 2003 Web Edition
2) Windows Server 2003 Standard Edition
3) Windows Server 2003 Enterprise Edition
4) Windows Server 2003 Datacenter Edition
5) Windows Small Business Server 2003, Standard Edition

6) Windows Small Business Server 2003, Premium Edition

A fenti termékek szolgáltatásai és funkciói testre szabhatóak a megrendelő egyéni üzleti és informatikai igényei szerint. Ezen verziók a közös architektúrára támaszkodnak, de eltérőek a hardver igények, a skálázhatóság illetve a szolgáltatások terén. Az egyes változatokról a későbbiekben részletesebben is szólok.

A Windows Server 2003 egy többcélú operációs rendszer, ugyanis az igényekhez igazodva különböző kiszolgálói szerepköröket tölthet be centralizált vagy elosztott rendszerben. Néhány ilyen kiszolgálói szerepkör:

- Fájl- és nyomtató-kiszolgáló
- Webkiszolgáló és webalkalmazás-kiszolgáló
- Levelezési kiszolgáló
- Terminálkiszolgáló
- Távelérési/virtuális magánhálózati (VPN) kiszolgáló
- Címtárszolgáltatások, DNS-, DHCP-kiszolgáló, és WINS (Windows Internet Naming Service)
- Adatfolyam-kiszolgáló

I.1. A rendszer főbb jellemzői, a felvonultatott technológiák rövid áttekintése

*Megbízhatóság*át az üzleti információk védelmére tökéletesített nyilvános kulcsú infrastruktúra (PKI) biztosítja. A biztonságot szolgálja a biometrikus hitelesítés (pl.: újlenyomat, retina vizsgálat), illetve a Kerberos illetékesség- vizsgáló protokoll (a kliensek ne tagadhassák le a kilétüket a szerverek előtt).

Továbbfejlesztett fürttámogatása fokozott rendelkezésre állást eredményez, illetve ezen fürtszolgáltatások telepítése jóval egyszerűbb lett. A Windows Server termékcsalád maximum 8 csomópontos kiszolgálófürtöket támogat. Alkalmazza az úgynevezett *feladatátvétel*t, ez akkor lép életbe, amikor a fürt egyik csomópontja valami hiba folytán nem érhető el, ekkor egy másik csomópont azonnal megkezdi a szolgáltatást. Támogatja a hálózati terheléselosztást, amely a fürt csomópontjai között kiegyensúlyozza a beérkező IP forgalmat.

*Méretezhető*sége horizontális illetve vertikális irányba is megoldott, az előbbi a fürtszolgáltatásnak, az utóbbi a többprocesszoros feldolgozásnak (SMP) köszönhetően.
A vállalkozások hálózata jelentős mértékben kibővült, ezért a biztonság minden eddiginél fontosabb tényezővé lépett elő. Az egyik legfontosabb biztonságtechnikai alapprogramja a *Common Language Runtime* (közös nyelvű futási idő), amely fokozza a rendszer megbízhatóságát, illetve csökkenti a különféle programozói hibákból adódó szoftverhibákat és biztonsági rések számát. Ebből kifolyólag a rendszernek kevesebb sebezhető pontja van. A közös nyelvű futási időnek köszönhetően az alkalmazások hiba nélkül futhatnak.

A hálózati infrastruktúra maximális *hatékonyság*gal telepíthető, felügyelhető. Továbbfejlesztették a tárkezelési szolgáltatásokat. A Windows Server 2003 terminálszolgáltatása a Windows 2000 alkalmazás kiszolgálójára épül, segítségével a Windows alapú szolgáltatásokat, illetve a Windows asztalt olyan gépeken is el lehet érni, amelyek nem képesek a Windows futtatására.
Az alkalmazottak, partnerek illetve a rendszer közötti hatékonyabb kommunikációt az integrált webkiszolgáló és az adatfolyam kiszolgáló igyekszik elősegíteni. Az integrált alkalmazás kiszolgáló segítségével az XML alapú webes szolgáltatások fejlesztése jóval könnyebb.

A Windows Server 2003 a Microsoft Windows NT erősségeire épít, és teljes mértékben együttműködik a Windows 2000 alapú kiszolgálókkal. A jelenleg a Windows 2000 Server termékcsalád tagjait használó vállalkozások egyszerűen frissíthetnek Windows Server 2003 operációs rendszerre, és azonnal kihasználhatják annak jobb kezelhetőségéből, megbízhatóságából, biztonságából, teljesítményéből és az integrált XML alapú webes szolgáltatásokból fakadó előnyöket. A terméket beépített biztonsági központtal ruházták fel ahonnan a rendszeradminisztrátor egy lépésben át tudja látni a különféle biztonsági eszközök állapotát. Beépített tűzfal kapott benne helyet (Windows Firewall). Nagy átalakításon esett át a hálózatkezelésért felelős úgynevezett Active Directory.
A dolgozatban ezen témakör részletes tárgyalás alá kerül majd.

A nagyfokú megbízhatóság, rendelkezésre állási képesség, méretezhetőség, biztonságosság jellemzőinek birtokában a Windows Server 2003 az egyik legbiztonságosabb hálózati operációs rendszer.

II. A Windows Server 2003 termékcsalád bemutatása

A Windows Server 2003 termékcsalád különféle megoldásokat kínál az ügyfelek különféle igényeihez. Minden tagjában teljes mértékben támogatja az Active Directory-t, amelynek fontos tagja a Domain Controller. (Ez utóbbi alól csak a Web Edition képez kivételt.)

II.1. Windows Server 2003, Web Edition

A Windows Server 2003 WE a Windows Server 2000 család új tagjaként kelt életre, egy új vonalat hivatott képviselni, egy teljesítményorientált webkiszolgáló. Ezt a verziót szánták általános alkalmazás-kiszolgálónak. Erőssége, hogy könnyen üzembe helyezhető és kezelhető, átfogó és robusztus platformot kínál a webkiszolgáláshoz és tartalomszolgáltatáshoz. A .NET keretrendszer tagjaként forradalmi újításokat nyújtó Microsoft ASP.NET technológia használatával a Windows Server 2003 WE stabil platformot nyújt az XML alapú webes szolgáltatások és alkalmazások gyors fejlesztéséhez és üzembe helyezéséhez. A Windows Server 2003 WE támogatja a kétutas, szimmetrikus többprocesszoros feldolgozást (SMP max. 2 processzorral) és akár 2 GB memória kezelését. Nem támogatja a Domain Controllert, illetve nincs 64-bites verziója.

II.2. Windows Server 2003, Standard Edition

A Windows .NET Standard Server megbízható hálózati operációs rendszer, mellyel egyszerűen és gyorsan biztosíthatók az üzleti megoldások. Ez a rugalmas kiszolgálórendszer ideális választás bármely vállalkozás mindennapi igényeihez. A Windows Server 2003 SE fájl- és nyomtatómegosztást, biztonságos internet kapcsolatot, központi alkalmazástelepítést és együttműködést biztosít a dolgozók, üzleti partnerek és ügyfelek között. A Windows Server 2003 SE támogatja a kétutas szimmetrikus többprocesszoros feldolgozást (SMP max 4 processzorral) és akár 4 GB memória kezelését. Nem támogatja viszont a fürtszolgáltatást, és nincs 64-bites verziója.

II.3. Windows Server 2003, Enterprise Edition

A Windows Server 2003 EE a Windows 2000 Advanced Server továbbfejlesztése. A Windows Server 2003 EE a közép- és nagyvállalkozások számára készült. Ez a rendszer biztosítja a vállalati infrastruktúra, az üzletági alkalmazások és e-kereskedelmi tranzakciók használatához szükséges szolgáltatásokat. A Windows Server 2003 EE 8 processzort is támogatni képes operációs rendszer (SMP), amely nagyvállalati szintű funkciókat nyújt (például nyolc csomópontos fürtkezelés és 32 vagy akár 512 GB memória támogatása). 64 bites platformokra is elérhető.

II.4. Windows Server 2003, Datacenter Edition

A Windows Server 2003 DE a Windows 2000 Datacenter Server továbbfejlesztése. A legnagyobb teljesítményt és skálázhatóságot igénylő vállalkozások számára készült Windows Server 2003 DE, stabil alapot kínál a kritikus fontosságú adatbázisok létrehozásához, vállalati erőforrás-tervező (ERP) szoftverekhez, a nagy sebességű, valós idejű tranzakció-kezeléshez és a vállalati kiszolgálók felújításához. A Microsoft eddigi legnagyobb teljesítményű operációs rendszere támogatja az akár 32 utas szimmetrikus többprocesszoros feldolgozást (SMP), és szériatartozékként kínál nyolc csomópontos fürtkezelést és terheléselosztási szolgáltatást. A Windows Server 2003 DE szintén elérhető 64 bites platformokra is.

III. A Windows Server 2003 termékcsalád rendszerkövetelményei, telepítése

III.1. Windows Server 2003 rendszerkövetelményei

Termék	Windows Server 2003 WE	Windows Server 2003 SE	Windows Server 2003 EE	Windows Server 2003 DE
Minimum processzor sebesség	133 MHz	133 MHz	133 MHz (x86) 733 MHz (Itanium)	400 MHz (x86) 733 MHz (Itanium)
Ajánlott processzor sebesség	550 Mhz	550 MHz	733 MHz	733 MHz
Minimum memória	128 MB	128 MB	128 MB	512 MB
Ajánlott memória	256 MB	256 MB	256 MB	1 GB
Maximum memória	2 GB	4 GB	32 GB (x86) 64 GB (Itanium)	64 GB (x86) 512 GB (Itanium)
SMP támogatása	2 processzor támogatása	4 processzor támogatása	8 processzor támogatása	8, max 64 processzor támogatása
Telepítéshez szükséges lemezterület	1.5 GB	1.5 GB	1.5 GB (x86) 2.0 GB (Itanium)	1.5 GB (x86) 2.0 GB (Itanium)
Fürtözés	Nincs	Nincs	Van 8 kiszolgálófürt	Van 8 kiszolgálófürt
64 bites verzió	Nincs	Nincs	Van	Van

III.2. Windows Server 2003 telepítése

A telepítés főbb lépései a korábbi Windows verzióknál megszokott módon történnek, itt csak néhány főbb, fontosnak vélt dolgot igyekszem kiemelni.

A felhasználók a telepítést egyfajta frissítéssel, illetve teljesen új telepítéssel (clean install) végezhetik, ez utóbbi esetben a telepítést megelőzi az adatok, beállítások, alkalmazások kimenekítése, migrálása (ha korábban is szerverként használtuk gépünket). Néhány érv szól a frissítés mellett, mint például a gyorsaság, nem kell az alkalmazásokat újratelepíteni (néhány esteleges kivételével), megmaradnak a felhasználói azonosítók, beállítások, jogok. Újratelepítés mellett szóló érvek például a lemezhatékonyság növelése egy esetleges lemezformázás, majd particionálás során, illetve ilyenkor már tanulva korábbi hibáinkból pontosabban állítjuk be a rendszert.

A telepítés előtt mindig meg kell győződnünk arról, hogy a rendszerkövetelményekben leírt minimumnak megfelelő erőforrású géppel rendelkezünk-e! Célszerű még megnézni a Microsoft Hardver Kompatibilitási Listáját (HCL) is a telepítés előtt, a későbbi nehézségek elkerülése végett. Az operációs rendszer frissítése/újratelepítése eseten célszerű előbb a Microsoft Windows Upgrade Advisor-t futtatni a telepítő lemezről. Ez megvizsgálja a rendszer hardver, illetve szoftver kompatibilitását. Emellett arról is meg kell győződnünk, hogy bizonyos általunk használni kívánt programok futtathatóak-e a Windows ezen verziója alatt. E célt szolgálja Program Kompatibilitás Vizsgálat Varázsló.

Frissítés esetén nem kell külön gondot fordítanunk a beállításokra (pl.: TCP/IP), sőt a meglevő felhasználók, csoportok, jogok és jogosultságok, megosztások is megmaradnak. Emellett az alkalmazásaink, állományaink és mappáink szerkezete is változatlan marad és tartományvezérlő esetén a címtár frissítése is lezajlik a telepítés közben. Frissítés esetén a telepítési előkészületek többnyire csak az előző rendszer mentésére illetve többszerveres környezet esetén a szerver frissítések sorrendjének megtervezésére vonatkoznak.

Windows Server Web Edition kivételével (mivel ez új technológia) valamennyi Server 2003 verzió telepíthető a Server 2000-es verziók nekik megfelelő frissítéseként. Az alábbi táblázat ezt foglalja össze.

Termék	Windows Server 2003 SE	Windows Server 2003 EE	Windows Server 2003 DE
Windows NT Server 4.0	Frissíthető	Frissíthető	
Windows NT 4.0, Terminal SE	Frissíthető	Frissíthető	
Windows NT Server 4.0, Enterprise Edition		Frissíthető	
Windows 2000 Server	Frissíthető	Frissíthető	
Windows 2000 Advanced Server		Frissíthető	
Windows 2000 Datacenter Server			Frissíthető

Az úgynevezett tiszta telepítés már a Windows 2000 Servernél is két lépésből állt: az operációs rendszer és a címtár telepítéséből. Ez a Windows Server 2003-ban sem változott, ez tehát egyszerűsíti a dolgunkat. Ráadásul egy új telepítésnél általában nem merülnek fel sorrend vagy szerepköri kritériumok, hiszen ez a szerver lesz a tartomány első - és lehet, hogy egyetlen tartományvezérlője a jövőben is - így az összes úgynevezett FSMO (Flexibile Single Master Operations = egyedi főkiszolgáló-műveletek) szerepkör hordozója az alapértelmezés szerint.

Más a helyzet, ha egy aktív Windows 2000 tartományba szeretnénk behelyezni egy már tiszta telepítéssel felvértezett Windows Server 2003-at, mert ebben az esetben csak maximum a tagkiszolgálói szerepig folytathatjuk a telepítést. Ahhoz, hogy a szerver teljes jogú tartományvezérlő legyen, frissítenünk kell a Windows 2000 tartományt (pontosabban a sémát).

Tiszta telepítés migrálással: amikor ezt a telepítési módot választjuk, akkor részben le kell mondanunk az eddigi rendszer építőkockáiról és elemeiről. De csak részben, hiszen a régi, Windows NT4 vagy Windows 2000-es tartományunkból címtár objektumokat importálni (migrálni) nem túl nehéz. Nyilván ez a folyamat soha nem lehet olyan szintű beállítás- és jogosultság öröklés mint egy frissítés, de az erre a célra biztosított Microsoft célszoftverrel az Active Directory Migration Tools (ADMT) segítségével viszonylag biztonságosan végezhetjük. Az ADMT 3-as változatával felhasználók, számítógépek, szolgáltatások fiókjai, csoportok, jelszavak és más objektumok mozgatását is megoldhatjuk tetszőleges két

(Windows NT4, 2000 vagy 2003) tartomány között, persze mindezt csak az után, hogy megbízotti kapcsolatot (trust) létesítettünk közöttük. A felhasználói beállítások átörökítésére használhatjuk a User State Migration Tool (USMT) nevű eszközt a telepítő lemezről. Telepíthető a Windows Server 2003 SP2, amely az alap 2003-as verzióhoz kapcsolódó frissítések, javítások, bővítmények gyűjteményét tartalmazza.

IV. Hálózati diagnosztika eszközei, szolgáltatásai

A Windows Server 2003 termékcsalád a hálózati problémák felderítésére használható hálózati diagnosztikai szolgáltatásokkal egészült ki.

1) **Hálózati diagnosztika weblapja**

   Ez a weblap a súgó Eszközök (*Tools*) részéből tekinthető meg, illetve a súgó problémamegoldással vagy hálózatkezeléssel foglalkozó részéből. Ezen a weblapon egyszerűen lekérhetők a helyi számítógéppel és a hálózattal kapcsolatos fontos adatok. Ezen kívül különböző diagnosztikai tesztek is igénybe vehetők itt, amelyek hasznos segítséget nyújthatnak a hálózati problémák megoldásához.

2) **Netsh diagnosztikai parancsok**

   Új Netsh segítő DLL parancsai használhatók a netsh diag környezetben. Ezekkel, a parancsokkal részletes hálózati diagnosztikai információk jeleníthetők meg és diagnosztikai műveletek hajthatók végre parancssorból. A Netsh diagnosztikai parancsok futtatása a parancssorban kiadott netsh -c diag parancs segítségével lehetséges.

3) **A hálózati kapcsolatok javítása menüparancs**

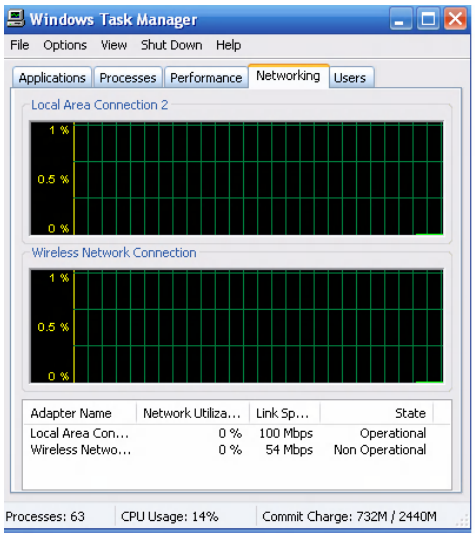
   Egyes esetekben a számítógép hálózati konfigurációja olyan állapotba kerül, amely nem teszi lehetővé a hálózati kommunikációt, azonban ez néhány gyakori eljárás, például az IP-cím konfigurációjának és a DNS-nevek regisztrációjának megújításával helyreállítható. A hálózati kapcsolatok helyi menüjében található Javítás parancs szükségtelenné teszi a műveletek kézi végrehajtását. A parancs választásakor a rendszer egy sor olyan műveletet hajt végre, amelyek nagy valószínűséggel megoldják a kommunikációs problémákat, mindenesetre nem idéznek elő súlyosabb hibákat.

4) A hálózati kapcsolatok Támogatás (*Support*) füle

A Hálózati kapcsolatok mappában található hálózati kapcsolatokhoz tartozó Állapot (*Status*) párbeszédablak kiegészült a Támogatás füllel. Ezen a fülön jeleníthetők meg a TCP/IP-konfiguráció adatai. A Támogatás lapon található Javítás (*Repair*) gomb egyenértékű a hálózati kapcsolathoz tartozó helyi menün található Javítás paranccsal.

5) A Feladatkezelő párbeszédablakának Hálózat (*Networking*) füle

A Feladatkezelő új Hálózat füle valós idejű adatokat jelenít meg a rendszerben található hálózati kártyákról. Ezek az adatok áttekintő képet adnak a hálózat működéséről. Ezt mutatja az alábbi ábra.



6) Frissített Netdiag.exe parancssori hálózati diagnosztikai eszköz

A Windows Server 2003 termékcsalád CD-lemezén található támogatási eszközök (*Support Tools*) között szerepel a Netdiag.exe is, amely a Windows 2000 Resource Kit által tartalmazott diagnosztikai eszköz továbbfejlesztett verziója. A támogatási eszközök telepítéséhez a Windows Server 2003 termékcsalád CD-lemezének Support\Tools mappájában található Support.msi fájlt kell indítani.

7) Menüparancs a távelérés naplózásához

A Hálózati kapcsolatok mappa Távelérés beállításai (*Remote Access Preferences*) párbeszédablaka az új Diagnosztika (*Diagnostics*) füllel egészült ki, amelynek

segítségével globálisan engedélyezhető a távelérésű kapcsolatok naplózása, illetve megtekinthetők és törölhetők a naplózott adatok. A Távelérés beállításai párbeszédpanel megjelenítéséhez a Hálózati kapcsolatok mappában válasszuk ki a Speciális opciót, majd a Távelérés beállításai elemet.

8) Hálózati telephely felismerése

Az úgynevezett hálózati telephely felismerő szolgáltatás segítségével a Windows Server 2003 felismeri, észleli azon hálózat beállításait, amelybe a számítógépet csatlakozattuk. A hálózat adatai a Windows Sockets alkalmazásprogramozási felületen keresztül is elérhetők, lekérhetőek.

9) Vezeték nélküli hálózatok kezelésének továbbfejlesztése

A vezeték nélküli (wireless) hálózatok területén is hozott néhány újdonságot elődjéhez képest. (pl.: automatikus kulcskezelés és a felhasználók hitelesítése, engedélyezése a hálózat elérését megelőzően.) Helyet kapott benne egy úgynevezett Vezeték nélküli hálózatfigyelő modul (Wireless Monitor Snap), amely segítségével megtekinthetők a vezeték nélküli elérései pontok (Access Point). A vezeték nélküli kapcsolatok jelszó alapú hitelesítése a PEAP (Protected Extensible Authentication Protocoll) segítéségével történik. Ez a protokoll az ügyfelet a hálózat felé jelszóval, a kiszolgálót valamint az elérési pontokat (AP) a kliens gép felé tanúsítvánnyal azonosítja.

Hitelesítés nélküli hálózati elérés támogatása segítségével a vezeték nélküli ügyfélnek nem kell semmiféle hitelesítő adatot - így pl. felhasználó nevet sem-küldenie a kapcsolat kiépítéséhez. Ezt a funkciót a Hálózati kapcsolatok mappában a vezeték nélküli kapcsolatok hitelesítésének beállításainál adhatjuk meg (Hitelesítés vendégként való engedélyezése). A használt protokoll az EAP-TLS (Extensible Authentication Protocol – Transport Level Security) A hitelesítés nélküli eléréshez a rendszer automatikusan bekapcsolja a vendég fiókot, és olyan távelérési házirendet állít be, amely engedélyezi a hitelesítés nélküli elérést a vendég fiókot tartalmazó csoportot használó EAP-TLS kapcsolatok számára.

10) Hálózatok távoli elérésének karantén alapú korlátozása (NAQC)

Network Address Quarantine Controll. Az RRAS és IAS közös szolgáltatása. Segítségével egy gépet csak akkor engedhetünk fel a hálózatra, ha azt leellenőriztük.

A karanténben lévő gépeknek egy adott időintervallum áll rendelkezésükre (ez alapértelmezés szerint 5 perc), hogy lefuttassanak néhány, a rendszergazda által meghatározott diagnosztikai parancsot. Az RRAS kiszolgáló ezen idő leteltével automatikusan bontja a kapcsolatot, amennyiben a diagnosztika eredménye szerint a kapcsolódó gép nem teljesíti a céges előírásokat.

11) A hálózati címfordítás és a tűzfal együttműködése

Az útválasztás és távelérés szolgáltatás továbbfejlesztett. A hálózati címfordítás egyszerű tűzfal összetevője tűzfalat is kezel, amely a Windows XP-ben meglévő tűzfal elve szerint működik. Ez a szolgáltatás lehetővé teszi a Windows Server 2003 rendszerrel működő és az Internet eléréséhez NAT-ot használó számítógép nyilvános hálózati kapcsolatának védelmét. A NAT védelmet nyújt a magánhálózatban található számítógépeknek, mert a címfordítást végző számítógép csak akkor továbbítja az Internetről érkező adatokat, ha a magánhálózat valamelyik ügyfele kéri ezt. A címfordítást végző számítógépet azonban érhetik támadások. A címfordítást végző számítógép nyilvános kapcsolatán engedélyezett egyszerű tűzfal kiszűri az összes olyan csomagot, amely az internetes felületen érkezett és nem felel meg a címfordítást végző számítógép által kért adatoknak (amelyeket saját maga vagy a magánhálózat ügyfelei számára kért).

12) Hálózati híd (network brigde)

Amikor otthon vagy az irodában építünk kisebb hálózatot, előfordulhat, hogy egyes hálózati adathordozók megfelelően működnek a hálózat adott részén, máshol azonban nem. Tegyük fel például, hogy egyes számítógépek telefoncsatlakozók közelében helyezkednek el, így azok a telefonvonalat használó hálózati eszközökkel csatlakoztathatók. Más számítógépek közelében azonban nincs telefoncsatlakozó, így azokhoz más hálózati adathordozót, például vezeték nélküli eszközöket kell használni. A Windows Server 2003 termékcsalád számos adathordozó-típust támogat, ezek közé tartozik például az Ethernet, a telefonvonal, az IEEE 802.11 vezeték nélküli eszközök és az IEEE 1394. Egy adott hálózati technológiával kommunikáló számítógépcsoport hálózati szegmenst alkot.

A különálló hálózati szegmensek TCP/IP alapú összekapcsolása hagyományosan több alhálózati cím beállítását és útválasztókat igényel, amelyek összekötik a

különböző adathordozókat. A Hálózati híd szolgáltatás lehetővé teszi a Windows Server 2003 rendszerrel működő számítógép számára egyetlen alhálózat kialakítását több hálózati szegmens áthidalásával. A hídként működő számítógépen egyszerűen összekapcsolhatók a hálózati szegmensek: a Hálózati kapcsolatok mappában az egér jobb gombjával kattintsunk az egyik kapcsolatra, és válasszuk a Hídkapcsolatok parancsot. Hálózati hidat csak olyan kapcsolatok között hozhatunk létre, amelyek nem használják az Internetkapcsolat megosztása szolgáltatást!

A Hálózati híd szolgáltatás használatának eredményeképpen az összes hálózati adathordozót összekapcsoló, egyszerűen beállítható alhálózatból álló hálózati konfiguráció áll elő. A hídként működő számítógép észleli, hogy melyik számítógép melyik hálózati szegmenshez tartozik, és továbbítja az adatcsomagokat a megfelelő szegmensek között.

13) A Hitelesítő adatok kezelőjének „kulcstartó” („key-ring”) szolgáltatása a távelérésben

A Windows Server 2003 termékcsaládban a Hitelesítő adatok kezelőjének kulcstartó szolgáltatása a rendszerben használatos különböző hitelesítő adatok csoportjaiból álló kulcstartót tárol. Ez lehetővé teszi több hálózat elérését (különböző felhasználónévből és jelszóból álló hitelesítő adatokkal) egy időben úgy, hogy közben nem kell újra és újra megadni a hitelesítő adatokat. A rendszer az elérni kívánt hálózati erőforrás adatai alapján (például a kiszolgáló és a tartomány neve) választja ki a megfelelő hitelesítő adatokat a kulcstartóról. A távelérés egy ideiglenes, alapértelmezés szerinti hitelesítő adatot (kulcsot) ad hozzá a kulcstartóhoz, amikor sikeresen létrejön egy-egy modemes vagy VPN-kapcsolat. Ezek a hitelesítő adatok a kapcsolat létrehozásához használt felhasználónevet és jelszót tartalmazzák, mivel gyakran ugyanezek az adatok szükségesek az adott hálózat erőforrásainak eléréséhez. Ez leegyszerűsíti a távoli hálózathoz való csatlakozást és a távoli, illetve a helyi hálózat erőforrásainak használatát.

14) Minden felhasználó számára elérhető távkapcsolat hitelesítő adatok

A minden felhasználó számára elérhető távkapcsolati hitelesítő adatok segítségével az adott számítógép összes felhasználójának hitelesítő adataiból álló (felhasználónév és jelszó) hitelesítő adat-csoporttal hozható létre kapcsolat.

Tegyük fel például, hogy egy felhasználó hálózati kapcsolattal csatlakozik otthoni számítógépéről a helyi internetszolgáltatóhoz. A felhasználó az Új kapcsolatvarázslóban megadhatja, hogy az adott kapcsolatot minden felhasználó igénybe veheti, és mentheti az összes felhasználóra vonatkozó hitelesítő adatokat. A családtagok ezt a kapcsolatot használhatják, és nem kell megjegyezniük az internetszolgáltatóhoz való csatlakozáshoz szükséges felhasználónevet és jelszót.

15) Az IEEE 1394 (IP/1394) alapú internet-protokoll támogatása

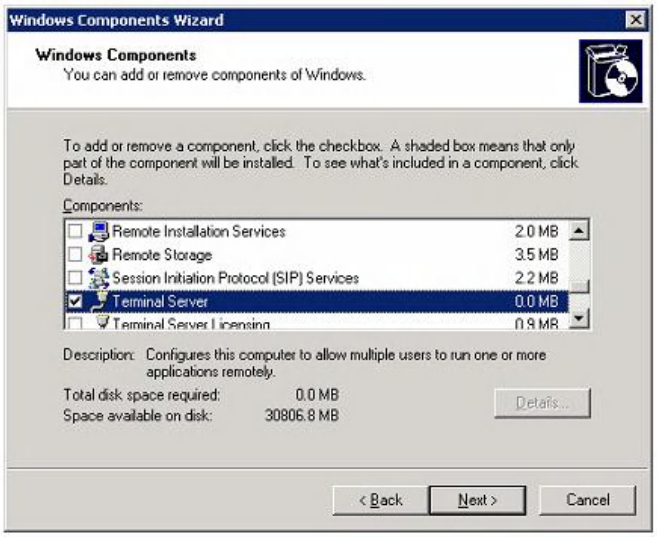
A Windows Server 2003 termékcsalád támogatja a TCP/IP-csomagok küldését és fogadását az IEEE 1394-es (más néven „Firewire") felületen keresztül. Ez olyan soros kommunikációs busz, amely 100 és 400 Mbit/s közötti sebességgel működik. Az IEEE 1394 leggyakrabban az audio- és videoberendezések csatlakoztatásához használatos, de kapható már ilyen lapolvasó vagy merevlemez is. Az IEEE 1394 támogatása kiterjed az IEEE 1394-keretek speciális kezelésére is, amely a Hálózati híd szolgáltatás számára szükséges. Az IEEE 1394-kapcsolatokat nem kell konfigurálni. A rendszer automatikusan észleli ezeket, és elvégzi a szükséges beállításokat.

16) Terminálszolgáltatás

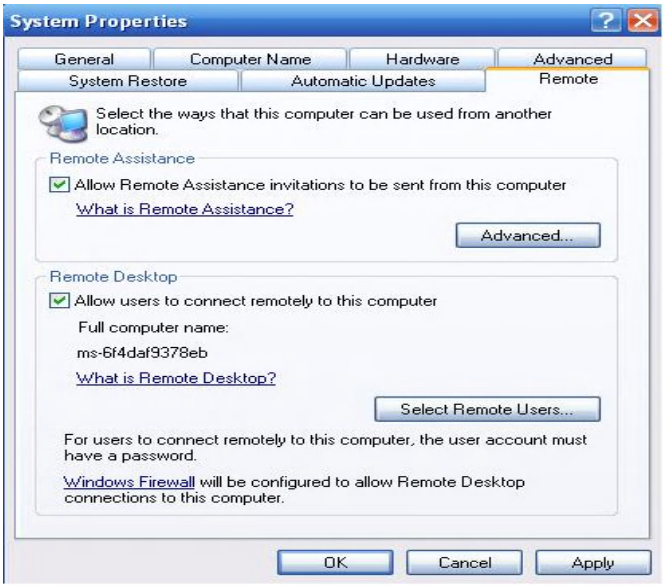
A Windows Server 2003 terminálszolgáltatása a Windows Server 2000 terminálszolgáltatására alapoz, tartalmazva a Windows Xp-ben megjelenő új ügyfélprogramot és protokollszolgáltatásokat. A Terminálszolgáltatások segítségével szinte bármely számítástechnikai eszközre (azokra is, amelyek képtelenek a Windows futtatására) eljuttathatók a Windows alapú alkalmazások vagy maga a Windows asztal.

Terminálszolgáltatás, a kiszolgáló engedélyezése

A terminálszolgáltatást a Vezérlőpultban a Programok telepítése/törlése (Windows komponensek hozzáadása, eltávolítása) varázsló segítségével végezhetjük. Ezt szemlélteti az alábbi ábra.



Ezután már csak engedélyeznünk kell gépünk távoli elérhetőségét. Ezt a Rendszertulajdonságok ablak segítségével végezhetjük az alábbiak szerint. (Engedélyezzük a felhasználóknak ezen számítógép távoli elérésének lehetőségét opció bekapcsolásával.)



A terminál szolgáltatás használatának előnyei, a kapcsolódás módja

A Terminál kiszolgáló nagyszerű lehetőséget teremt arra, hogy a Windows alapú alkalmazásokat az egész vállalat minden számítástechnikai eszközén alkalmazhatóvá tegyék. Különösen igaz ez a gyakran frissített, a ritkán használt, illetve a nehezen felügyelhető programokra. Ha egy alkalmazást nem az egyes eszközökön, hanem a

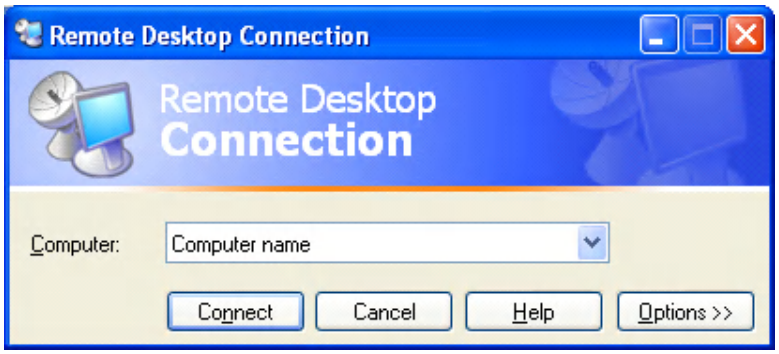
terminál kiszolgálón kezelnek, akkor a rendszergazdák mindig biztosak lehetnek benne, hogy a felhasználók az alkalmazás legújabb verzióját futtatják.
A Terminál kiszolgáló számottevő mértékben csökkenti az adatok távolról való eléréséhez szükséges hálózati sávszélességet.

Ha korlátozott sávszélességű (például telefonos vagy megosztott WAN) kapcsolaton Terminál kiszolgáló segítségével futtatják az alkalmazásokat, akkor az kivételes hatékonysággal alkalmazható nagy mennyiségű adat távoli elérésére és kezelésére, mivel a hálózaton csak az adatokat megjelenítő képernyő halad át, maguk az adatok nem.

A Terminál kiszolgáló elősegíti, hogy a felhasználók termelékenyebben végezhessék munkájukat: lehetővé teszi számukra, hogy bármilyen eszközön futtathassák a korszerű alkalmazásokat, beleértve a gyenge teljesítményű hardvereket és a nem Windows rendszerű asztali gépeket is. A Terminál kiszolgáló révén mindenhol használható a Windows, ezért kiaknázhatók az újabb és kisebb súlyú eszközök (például a Pocket PC) nagyobb feldolgozási lehetőségei.

A csatlakozás

A terminálszolgáltatások ügyfélprogramja (Távoli asztali kapcsolat) a korábbi verziókhoz képest jelentős mértékben továbbfejlődött. Csatlakozáshoz csak be kell írni az elérendő számítógép nevét. Ezt mutatja az ábra.



A csatlakozásnál speciális (pl.: sávszélesség) információk is beállíthatók az opciók fülre kattintva.

A Távoli asztali kapcsolat telepíthető olyan operációs rendszerekre, amelyek ezt nem tartalmazzák.

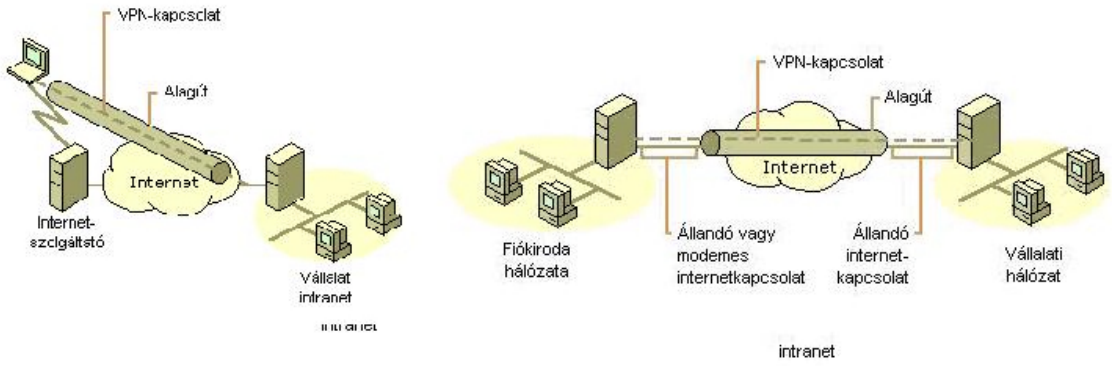
17) Távoli hozzáférés a virtuális magánhálózati (VPN) szerverhez

A Virtual Private Network (VPN) hálózatok használata előnyt jelent a vállalatok telephelyeinek, irodáinak kommunikációja során. Virtuális magánhálózat segítségével úgy küldhetünk adatokat két gép között, mintha a két gép közvetlen összeköttetésben lenne. Ezen magánhálózatok nemcsak az adatok vállalaton belüli biztonságos továbbítását szolgálják, hanem tökéletesen használhatók videókonferenciák, konferenciabeszélgetések lebonyolítására. A VPN technológiát egyre több vállalat arra használja, hogy segítségével az alkalmazottak otthonról is elérhetik a céges hálózatot.

A VPN összeköttetés két legismertebb megvalósítása:

1) Bérelt vonalak: a hálózatot különböző szolgáltatók által megvalósított bérelt vonalak alkotják

2) Internet feletti titkosított csatornák (IPSec): akkor bizonyulhat jó megoldásnak, ha a vállalat különböző telephelyein már rendelkezésre áll az internet szolgáltatás. Ilyenkor a vállalat az internet hozzáférést nemcsak magánhálózat kiépítésére kívánja használni, hanem internet hozzáférésre is. Ez erősen megköveteli tűzfal alkalmazások használatát, azon helyeken, ahol átjárás van a magánhálózatból az internet felé.



Ügyfél- kiszolgáló, Kiszolgáló- kiszolgáló modell

Windows Server 2003 a VPN kapcsolatok 2 fajtáját támogatja:

1) Point – to – Point Tunelling Protocoll (PPTP)
2) Layer Two Tunelling Protocoll (L2TP)

Virtuális magánhálózati (VPN) kapcsolat létrehozása

1) Nyissuk meg a Hálózati kapcsolatok segédprogramot.
2) Kattintsunk duplán az Új kapcsolatvarázsló ikonra, majd a tovább gombra.
3) Jelöljük be a Kapcsolódás a munkahelyem hálózatához választógombot, majd kattintsunk a tovább gombra.
4) Kattintsunk a Virtuális magánhálózat beállításra, majd a tovább gombra.
5) A Cégnév mezőbe írjuk be a kapcsolat nevét, majd kattintsunk a tovább gombra.
6) Ha már létesítettünk korábban telefonos kapcsolatot, hajtsuk végre a következő műveletek egyikét:
    - Ha a célhálózathoz történő bejutás előtt előbb létre kell hozni a kapcsolatot az Internet-szolgáltatóval vagy más hálózattal a célszámítógéphez, akkor kattintsunk A kezdeti kapcsolat automatikus tárcsázása választógombra, kattintsunk a listában a kívánt kapcsolatra, majd a tovább gombra.
    - Ha nem akarjuk automatikusan tárcsázni a kezdeti kapcsolatot, kattintsunk a Ne tárcsázza a kezdeti kapcsolatot választógombra, majd a tovább gombra.
7) Írjuk be annak a VPN-kiszolgálónak az állomásnevét vagy IP-címét, amelyhez csatlakozni kívánunk, majd kattintsunk a tovább gombra.
8) Végezzük el az alábbi műveletek valamelyikét:
    - Ha a kapcsolatot a számítógép minden felhasználója számára elérhetővé kívánjuk tenni, kattintsunk a bárki által használható választógombra, majd a tovább gombra.

- Ha saját használatra kívánjuk fenntartani a kapcsolatot, kattintsunk a Csak általam használható választógombra, majd a tovább gombra.

9) Ha szeretnénk létrehozni a kapcsolathoz egy ikont az asztalon, jelölje be a Parancsikon elhelyezése az Asztalon ehhez a kapcsolathoz jelölőnégyzetet.

10) Kattintsunk a befejezés gombra.

V. Hálózati infrastruktúra megtervezése, Windows Server 2003 hálózati protokolljainak ismertetése

V.I. A hálózat fizikai és logikai topológiája

Hálózat kialakítása során elsődleges szempont közé tartozik a vállalat igényeihez való igazodás, minden vállalatnak más-más elvárásai vannak. A kialakítás során a tervezőnek figyelembe kell venni a megrendelő, a felhasználók igényeit, hardver illetve szoftver komponenseket és ezeknek megfelelően kell kialakítani a hálózat fizikai és logikai struktúráját. A hálózati infrastruktúra felépítését tekintve két részre bomlik egy fizikai és egy logikai részre.

A fizikai felépítés alatt a hálózat hardver komponenseinek összességét értjük, mint például kábelek, jelismétlők, forgalomirányítók stb. A fizikai felépítés teljes mértékben a hálózat logikai felépítésétől függ, például, ha Ethernet adatkapcsolati protokoll kerül kialakításra ez magával vonzza az alkalmazandó kábel típusát.

A logikai felépítés a hálózat szoftver komponenseinek összessége, amelyek a fizikai kapcsolaton túli kapcsolat kialakításáért felelősek. Ezek egy részét szokás nevezni absztrakt szoftver elemeknek is (hálózati protokollok), illetve konkrét szoftver elemeknek (pl.: ftp szerver).

Egy összetett hálózat kivitelezését a következő paraméterek szabják meg:

- a hálózat fizikai topológiája
- a hálózaton végzett feladatok típusa
- a hálózaton végzett feladatok mennyisége
- az aktív felhasználók száma
- minőség/ár faktor
- hosszú távú fejlesztési tervek

Minél szegmentáltabb egy hálózat, annál optimálisabb a kihasználtsága, könnyebb a karbantartása/üzemeltetése, ugyanakkor összetettebb a felügyelete és költségesebb a kivitelezése.

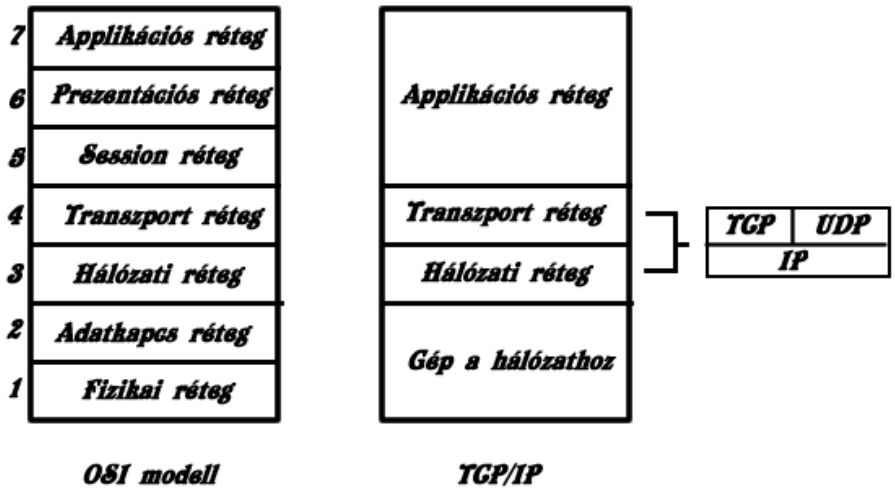
V.2. Windows Server 2003 ismertebb hálózati protokolljai

A Windows Server 2003, mint elődei is a rétegzett hálózati architektúrát használja. A rétegzett struktúrának is köszönhetően képes a különböző protokollokat valló munkaállomások közötti kommunikáció megvalósítására (multiprotokollos operációs rendszer). A Windows Server 2003 széles körű hálózati protokoll támogatással bíró hálózati operációs rendszer. Támogatja több hálózati adapter használatát.

Ismertebb hálózati protokolljai:

- TCP/IP (alapértelmezett)
- IPX/SPX
- NetBEUI
- AppleTalk

V.2.1. TCP/IP (Ipv4, Ipv6 támogatással):



Az 1970-es években sok különböző számítógép konfiguráció létezett, ezért szükség lett egy egységes, hardver független protokoll kialakítására. Ezt oldotta meg egyedi címzési rendszerrel felvértezett TCP/IP protokoll.

Két protokollon alapul, a szállítási rétegen operáló TCP protokollon, illetve a hálózati rétegen operáló IP protokollon. A TCP adattovábbítási egységeit *datagramm*oknak (adatcsomag) nevezzük. Ezek a csomagok a tényleges adat mellett tartalmazzák a feladó illetve a cél címét.

Ezek a címek az IP protokoll 32 bites úgynevezett IP címei (4 oktett) illetve Ipv6 esetében ezek a címek 128 bitesek. Azt hogy az IP protokollt –mint, ahogy a fenti ábra is mutatja- a TCP vagy az UDP protokollal kapcsoljuk össze, teljesen alkalmazásfüggő. A TCP-t kapcsolatorientált (összeköttetés alapú) protokollnak is szokták nevezni, ami annyit tesz, hogy mielőtt a kommunikáció végbemegy a kommunikálni kívánó pontok között megtörténik a kapcsolat kiépítése. A kapcsolat kialakítására a *3 utas kézfogást* használják. A kiépült kommunikációs vonal a kapcsolat végéig fennáll. Megbízható adattovábbítás jellemzi, minden egyes adatcsomag *nyugtázás*ra kerül a fogadó által, ha ez nem történik meg a küldő ezt a csomagot újraküldi. Miután minden egyes adatcsomag átment (nem kell feltétlenül sorrendhelyesen), megtörténhet az adatcsomagok összeillesztése a fogadó oldalán. A TCP/IP az egyik legelterjedtebb, legszélesebb körben alkalmazott kommunikációs protokoll.

UDP protokoll egy úgynevezett kapcsolatnélküli protokoll, ami annyit tesz, hogy a kommunikálni kívánó csomópontok a kapcsolat kiépítése, fenntartása nélkül végzik az adattovábbítást. Nem jelenik meg a TCP-nél ismertettet nyugtázási mechanizmus, ebből kifolyólag az adatátvitel gyorsabb, viszont kevésbé megbízható. Audio, video streamek átvitelére jól lehet használni.

V.2.2. IPX/SPX:

Az 1980-as években a Novell emberei a XNS illetve a TCP/IP protokollra alapozva hozták létre az IPX protokollt saját fejlesztésű NetWare operációs rendszerük számára. A Novell IPX protokollja a TCP/IP-vel ellentétben nem volt nyilvános, ezért a Microsoft létrehozta saját IPX protokollját NWLink néven, amelynek már a neve is a Novell szerverekhez való csatlakozást sugallta. Ezt a Windows 2003 Server is tartalmazza NWLink IPX/SPX/NetBIOS kompatibilis átviteli protokoll néven. A TCP/IP-hez hasonlóan az IPX is egyfajta protokoll gyűjtemény. Az IPX maga a hálózati réteg protokoll, az SPX pedig a TCP/IP TCP-jének megfelelő transzport réteg protokoll. Az UDP megfelelője a NetWare Core Protocoll (NCP). Az IPX is datagram, azaz csomag-alapú hálózati kommunikációs protokoll. A protokoll a csomagok céljának illetve forrásának azonosítására egy 12-bájtos címzési sémát alkalmaz. Ez a 12 bájt három részre bontható: a 4-bájtos hálózati címre (amely a hálózati szegmenst azonosítja), a 6-bájtos node-címre (ami a hálózaton belül a csomópontot azonosítja) valamint a 2-bájtos socket-címre. Ez utóbbi funkciója annak meghatározása, hogy a célállomáson futó folyamatok közül melyik kapta, illetve küldte a csomagot. Alapvető

különbség a TCP/IP és az IPX/SPX között, hogy míg az előbbi különböző méretű, típusú hálózatokat támogat, addig az utóbbi elsősorban a helyi hálózatokra (LAN) lett tervezve.

V.2.3. NetBEUI:

A Windows 3.1 alapértelmezett útválasztás nélküli hálózat- és szállítási rétegbeli protokollja volt a 90-es évek elején. A hálózatok ekkor még igen csak gyerekcipőben jártak, mind méretüket tekintve kicsit voltak és inkább egy helyre összpontosultak. A NetBEUI a Network Basic Input/Output System (NetBIOS) névtereket használja a számítógépek hálózaton történő azonosítására, amit később a DNS névterek váltanak le. A NetBIOS-név egy 16 bájtos cím, amely egy NetBIOS-erőforrást azonosít a hálózaton. A NetBIOS-név lehet egyedi (kizárólagos) vagy csoportnév (nem kizárólagos). Ha egy NetBIOS-folyamat egy számítógép adott folyamatával kommunikál, egyedi nevet használ. Ha egy NetBIOS-folyamat több számítógép több folyamatával kommunikál, akkor csoportnevet használ. Elsősorban a kisméretű Windows-os hálózatokban fájlmegosztás céljából létrejövő protokoll.

V.2.4. Apple Talk:

A protokollt az Apple Computer kezdte fejleszteni a 80-as években. Windows Server 2003-ban az Ethernet hálózati topológia az alapértelmezett, de támogatja a TokenRinget, FDDI-t, LocalTalk-ot és az ATM-et is. A Macintosh is fel van ruházva Ethernettel, de a LocalTalk az alapértelmezett a Machintosh hálózatokban. Apple Talk protokoll Windows Server 2003 alatt is elérhető, segítségével könnyen megvalósítható a Windows Server 2003-at futtató gép Macintosh hálózatba történő kapcsolása.

Két Apple Talk protokoll létezik: Appel Talk Phase 1, Apple Talk Phase 2

Az első verzió még csak 135 klienst illetve szervert volt képes kezelni egy hálózaton belül, a másodikban ez a szám 235-re növekedett, ráadásul a szegmentálódás miatt ez a korlátozás csak egy szegmensre vonatkozik. Több szegmens összekapcsolásával lényegesen nagyobb mértek érhetőek el. Adatcsomag alapú protokoll, a csomagok küldése, fogadása socketeken keresztül megy végbe.

V.3. Hálózati cím kiosztás

A címkiosztás megtörténhet:

- Statikus IP címkiosztás

  A mai hálózatok méreteit tekintve már nem igazán használatos, olyan problémák léphetnek fel, mint címütközés, nem megfelelő hálózati maszk használata. Nem igazán karbantarthatók.

- Dynamic Host Configuration Protokoll (DHCP) segítségével

  Mai hálózatok méretüket tekintve igen hatalmasak, sok munkaállomást tartalmaznak. Ha a rendszergazdáknak egyesével kellene leülni minden egyes géphez beállítani a megfelelő hálózati paramétereket (IP cím, DNS név, átjáró, hálózati maszk) igen csak nehezen lenne karbantartható egy nagy hálózat. Ezt könnyíti meg a DHCP címkiosztás, melynek a hasonló elven működő BOOTP volt az elődje. A BOOTP az IP cím osztás mellett olyan indítófájlokat is küldött, amelynek segítségével a bootolás hálózaton keresztül is megtörténhetett. A BOOTP-nek azonban voltak gyenge pontjai. Például nem volt dinamikus (a munkaállomás fizikai adapterének címe alapján kaphatott csak IP címet, amelyet a rendszergazda előzőleg beállított a kiszolgálón. Új gép esetén tehát kiszolgálón konfigurálni kellett.), nincs ideiglenes címek kezelésének lehetősége, minden egyes munkaállomás fizikai címére szükség volt. A BOOTP hátrányait kiküszöbölve jön létre a DHCP.

  A hálózatra kapcsolódó gépnek, egy vagy több DHCP kiszolgáló konfigurálásával biztosítunk IP címet. A konfigurálás során a DHCP kiszolgálót magát statikus IP címmel kell konfigurálni. Egy kiszolgáló egyszerre nyújthat DHCP illetve névfeloldási (DNS) szolgáltatást is. A DNS szolgáltatásról a következő témakörben írok. A DHCP meglehetősen leegyszerűsíti az IP címek kezelését nagyméretű hálózatok esetén. Előnyei elsősorban a központosított IP illetve host konfigurálás, skálázhatóság, rugalmasság. Lehetővé teszi, hogy egy számítógép hozzáférjen a hálózathoz bármilyen előzetes konfigurálás nélkül. DHCP használatával kiküszöbölhetők a statikus IP konfiguráció hátrányai, mint például a nem megfelelő hálózati maszk használata, IP cím ütközést (ugyanaz a cím több hálózati adapternek kerül kiosztásra).

Bootolás után a számítógép egy DHCPREQUEST nevű üzenet (ez egy broadcast üzenet) keretében igényel magának IP címet a DHCP szerverektől. A DHCP szerverek feldolgozzák a kérést, és ha a címtartományukban van még szabad IP akkor azzal megválaszolják (DHCPOFFER) a kérést. (címtartományok kiosztásáról beszélhetünk) A kliens ezek közül választ egyet és elküldi a választását az érintett DHCP szervernek, aki innentől kezdve ezt a címet a foglalt minősítéssel látja el. DHCPACK üzenetben jelzi a kliens felé, hogy bejegyezte ezt a címet hozzá. Ha nincs DHCPACK akkor a kliens egy bizonyos idő elteltével újra megpróbál címet szerezni magának. DHCPDECLINE segítségével a kliens is leellenőrizheti, hogy tényleg szabad-e a kapott IP cím. Ez egy Address Resolution Protokoll (ARP) kérdés, ami az esetben volt eredményes, ha nem érkezik rá válasz, mivel ez azt jelenti, hogy a cím tényleg nincs használatban jelenleg. A DHCPRELEASE segítségével a kliens a IP-t „visszaadja", újra kioszthatóvá válik. Ha a kliens egy új IP-t szeretne igényelni egyszerűen megteheti az *ipconfig /release* majd az *ipconfig /renew* parancsok parancssorból történő futtatásával. Újbóli DHCPREQUEST segítségével pedig az IP érvényességi intervallum (session time) hosszabbítható meg.

Az érvényességi intervallumot meghatározó tényezők:

- Kliensek száma

  Ha a kliensek száma megközelítőleg azonos a DHCP szerver címtartományában kioszthatói IP címek számával, akkor rövidebb érvényességi intervallum javasolt.

- Mobil felhasználók száma

  Ha az úgynevezett „mobil" felhasználók száma nem túl nagy, illetve a kliensek gépei nem vándorolnak gyakran a hálózatok között akkor hosszabb érvényességi intervallum javallott, ellenkező esetben rövidebb.

A DHCP egyik hátránya lehet, hogy nem ellenőrzött kliensek is kapcsolódhatnak a hálózatra, bár ez ellen fizikai cím (MAC) szűréssel lehet védekezni, de mivel a gépek fizikai címe Windows alatt átírható, így már ez sem jelent tökéletes biztonságot az illetéktelenek ellen.

Ha a telepítés során a Hálózati Beállítások panelen a Tipikus beállítást választjuk, akkor ezzel jelezhetjük, hogy a DHCP kiszolgálót a telepítés végeztével, később kívánjuk konfigurálni. Ha nincs a hálózatban DHCP kiszolgáló, akkor az Automatic Private Addressing (APIPA) nevű IP címzési protokoll kerül használatra. Ez esetben az APIPA által kiosztásra kerülő címtartomány a 169.254.0.1-169.254.255.254/16. Ezen címtartományba eső címeket az internet nem használja. Az APIPA szolgáltatást használó kiszolgáló nem tud az internetre kapcsolódni, mivel az APIPA szolgáltatást különálló hálózati szegmensekből felépülő hálózatokhoz tervezték. Ha telepítés közben már tudjuk, hogy melyik kiszolgáló(k) fogja(k) a DHCP szerver szerepkört ellátni akkor az Egyéni beállításokat kell választani.

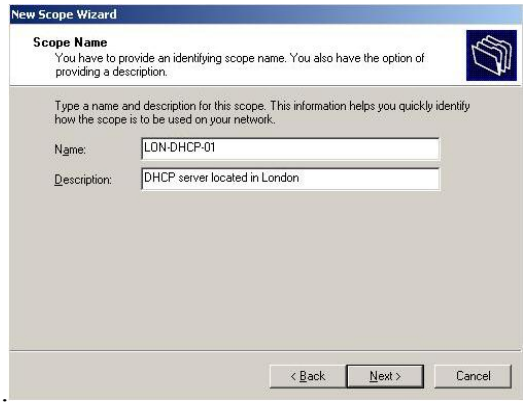
V.4. A DHCP szerver üzembe helyezése Windows telepítés után

A DHCP szerver segítségével a rendszergazdáknak nem kell minden egyes hálózatra csatlakozó gépet egyesével konfigurálni (nem kell egyesével beállítani az átjárót, DNS-t, hálózati maszkot, stb.). Segítségével központosított hálózatkezelés valósítható meg, a hálózati forgalom minimális növekedése mellett. Ha egyszer jól beállítjuk, akkor jó ideig nincs vele probléma.

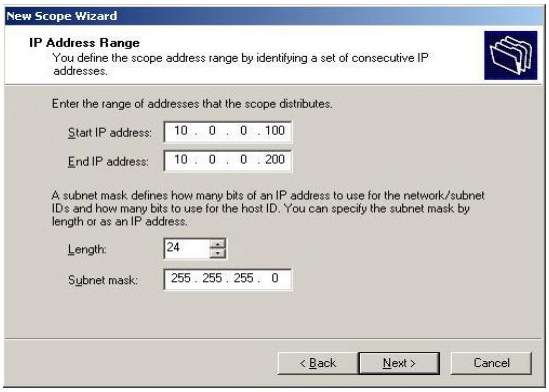
DHCP szerver telepítése Windows Server 2003 alatt meglehetősen egyszerű, csak a DHCP Server szerepkör installálása szükséges. Ezt a szerepkört vagy a Vezérlőpultból Windows összetevőként, vagy a Kiszolgáló kezelése ablakon keresztül telepíthetjük. A DHCP szervernek statikus IP címet kell megadni.

Ebben a pontban a Kiszolgáló kezelése ablakon keresztül történő telepítést ismertetem részletesebben.

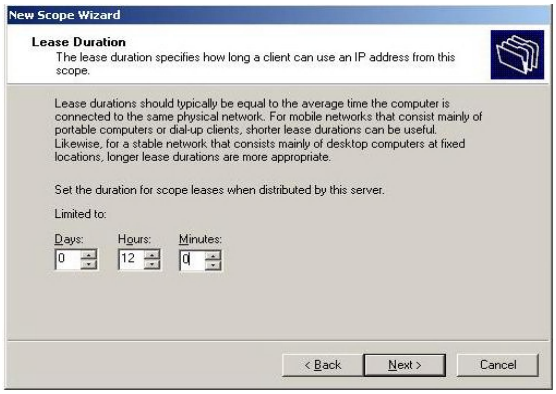
1) A Kiszolgáló kezelése ablakon válasszuk a szerepkör hozzáadása pontot, azon belül pedig a DHCP szerepkört. Itt meg kell adni a kiszolgáló nevét, illetve egy rövid leírását.



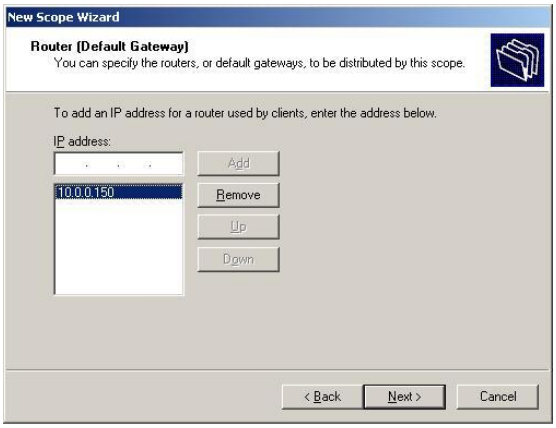
2) Ezután meg kell adni a kiosztásra kerülő IP címtartományt (hatókört), amelyből a munkaállomások az IP címeket kapják. Lehetőséget kapunk, hogy az előbb megadott tartományból ne osszon ki bizonyos címeket. Ez akkor szükséges, ha statikus címmel rendelkező gép van már abban a tartományban. Majd megadjuk hálózati maszk hosszát (length), illetve magát a maszkot.



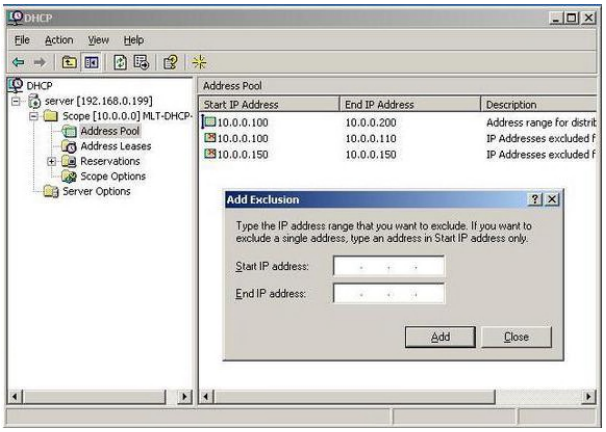
3) Ezután lehetőség nyílik az érvényességi intervallum (Lease duration) beállítására, hogy egy kliens milyen hosszan birtokolhat egy IP-t.



4) Ezután következik a forgalomirányító (router) megadása illetve a DNS és a tartománynév beállítása.



V.5. DHCP szerver konfigurálása



DHCP poolban új címtartományt lehet definiálni, amennyiben csak a kezdő IP címet adjuk meg akkor csak egyetlen IP-t definiáltunk. Itt nyílik majd lehetőségünk a fizikai cím szűrés beállítására, illetve a gépek neveinek IP címekhez való rendelésére is.

VI. AWindows Server 2003 különböző szerepkörökben

A Windows Server 2003-at futtató számítógépek a következő szerepkörök betöltésére képesek mind osztott, mind centralizált módon:

- **Fájl- és nyomtatószerver**

  A hálózat két alapvető funkcionalitását a fájloknak egy központosított helyre történő mentése illetve ezen fájloknak innen történő elérése, nyomtatása adja. A nyomtató szerverek biztosítják a hálózaton keresztül történő nyomtatást. A Windows Server 2003-at nyomtatószerverként konfigurálva lehetővé válik a nyomtatók távoli elérése a Windows Managment Instruments (WMI) használata segítségével. A WMI lehetővé teszi a nyomtatók megfigyelését, illetve távoli vezérlését.

  A Fájl szerverek a szerver merevlemezein tárolt fájlok osztott elérését szolgálják. Segítségükkel az alkalmazottak az adataikat a szerver merevlemezein tárolhatják saját PC-jük helyett, ezáltal lehetőség van az információk kollégákkal történő minél hatékonyabb megosztására, illetve az alkalmazottak a munkájukhoz szükséges adataikat tetszőleges gépről elérhetik a munka során. Ez különösen hasznos lehet a nagyvállalatok életében. A rendszergazdák feladata többek között az egyes felhasználók által a központi fájlszerveren birtokolt lemezterület méretének, illetve az ezekhez való hozzáférésnek a szabályozása.

- **Webszerver és webes alkalmazások szolgáltatása**

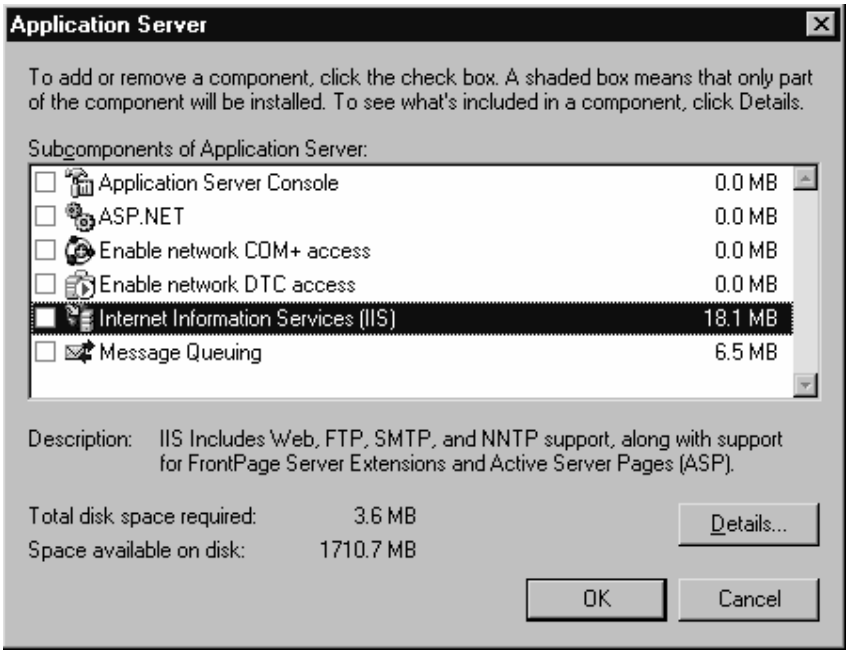
  Webszerver segítségével a vállalatok publikálhatják a saját webes oldalaikat az interneten illetve a helyi intraneten (LAN) belül. A Windows Server 2003 webszerver szolgáltatása az Internet Information Services 6.0 (IIS 6.0), amely több TCP/IP-re épülő protokollt is támogat:

  - Hypertext Transfer Protocoll (HTTP)
  - File Transfer Protocoll (FTP)
  - Network News Transfer Protocoll (NNTP)
  - Simple Mail Transfer Protocoll (SMTP)

Windows Server 2003 konfigurálása webszerverként:

Kétféle telepítési mód közül választhatunk. Használhatjuk a Szerver konfigurálása varázslót, illetve a vezérlőpultban a Windows összetevők hozzáadása/eltávolítása ablakot is. Az utóbbit mutatnám be az alábbi néhány sorban.

1) A Windows összetevők hozzáadása/eltávolítása ablakban válasszuk a Windows komponensek hozzáadása ikont, majd válasszuk az Alkalmazás szerver opciót, ahol a részletekre kattintva a következő ablakot kapjuk.



Itt több komponens közül választhatunk, válasszuk az IIS opciót. Ezután a telepítő elvégzi a komponens telepítését, és készen is vagyunk.

- **DNS, WINS szerverek**

DNS illetve WINS szerverek ugyanazt a szerepkört szolgálják, a számítógépek azonosítását illetve visszakeresését a hálózaton. A DHCP szerverek 32 bitse (IPv6 esetében 128 bit) IP címekkel azonosítják a számítógépeket. A DNS és a WINS szerverek ezen ember által nehezen megjegyezhető címeket oldják fel felhasználóbarát beszélő nevek segítségével.

A korábban ismertetett DHCP tehát a DNS illetve a WINS szerverekkel a Windows Server 2003 hálózati infrastruktúrájának alapkövét alkotja. Bekonfigurált DHCP szerver segítségével a kliensek előre meghatározott címtartományból kapják az IP címeiket egy előre rögzített időintervallumra. Ezeknek a hálózaton létező IP címeknek a megjegyzése igen nehézkes lenne, erre kínál megoldást a DHCP-vel összefonódó DNS szerver, ami nem mást szolgál, mint IP címeknek felhasználóbarát névre történő leképzését (illetve neveknek IP címre történő leképzését). A DNS a legelterjedtebb módja ezen úgynevezett névfeloldási (resolving) folyamatnak, ezt használja az internet is. A Windows Server 2003-ban a dolgozat későbbi részében bemutatásra kerülő Active Directory rendszer is ezt a névfeloldási módszert használja a hálózat erőforrásainak, felhasználóinak, hosztoknak, tartományvezérlőknek az elérésére. A DNS szerverek hierarchikusan kialakított adatbázisok, amelyek felhasználó barát név – IP összerendeléseket tartalmaznak.

A DNS névfeloldás a következőképpen mehet végbe:

- Egy alkalmazás kéri a névfeloldást saját DNS névszerverétől
- A névszerver megnézi hogy megtalálható-e a saját gyorsítótárában a kért információ.
    - ha igen megválaszolja
    - ha nem akkor megnézi, hogy a kérdés a saját zónájára vonatkozik-e?
        - ha az általa adminisztrált zónára vonatkozik akkor megválaszolja és a gyorsítótárat frissíti
        - ha nem akkor
            - vagy ismer olyan névszervereket, amelyek tudják a kért információt.
            - egyéb root domain-hoz tartozó névszerverek címével válaszol

A kérdést megválaszolása alapján iteratívnak (a névszerver mindig annak a névszervernek az IP címét adja vissza ahol a kérdést feltevőnek keresgélni kell) vagy rekurzívnak (a megszólított névszerverek maguk teszik fel a kérdést egy másik a kért információt esetleg tartalmazó névszervernek) nevezzük.

Ebben a példában az ügyfélszámítógép lekérdezi a DNS-kiszolgálót, hogy megkapja az a-allomas.pelda.microsoft.com DNS-tartománynév használatára beállított számítógép IP-címét. Mivel a kiszolgáló a saját helyi adatbázisában tárolt adatok alapján válaszolni tud a lekérdezésre, elküldi a kért információt tartalmazó választ, amely nem más, mint egy, az a-allomas.pelda.microsoft.com IP-címét tartalmazó A (állomás) erőforrásrekord.

A Windows Internet Name Service (WINS) egy másik ismert névfeloldási mód, amely IP címek NetBIOS nevekre történő leképzését végzi, illetve ennek a fordítottját. A NetBIOS-t a Windows 2000 használta, a visszafele kompatibilitás miatt a Windows Server 2003-ban is megtalálható. A WINS szerver segítségével lehetőség nyílik a kliensek számára, hogy nevük alapján érjék el a gépeket és egyéb hálózati erőforrásokat, az IP címek helyett. Egy kliensnek maximum két kiszolgáló adható meg. Ezek címét két módon tudhatja meg:

1) Beállítjuk magunk a gép konfigurálásánál
2) DHCP kiszolgálótól kapja meg

Replikált adatbázis szolgáltatást nyújt, amely segítségével lehetőség van NetNIOS nevek regisztrálására. Szerverünk tehát a WINS segítségével NetBIOS névkiszolgálóként is működhet. A WINS tehát IP címekhez rendeli a NetBIOS neveket és arra szolgál, hogy kiküszöbölje az útválasztásos környezetek NetBIOS névhozzárendeléséből eredő problémákat. Egyszerűbbé teszi a NetBIOS névtér kezelését TCP/IP hálózatban.

WINS használatakor a gépek bekapcsolás után bejelentkeznek a WINS kiszolgálóra, automatikusan regisztrálják a nevüket és az IP címüket. Innen kapják meg az elérhető számítógépek listáját. A WINS segítségével a felhasználók könnyen megtalálják a távoli hálózatokat. A WINS beállítása a Vezérlőpult Hálózatok ikonja

alatt a TCP/IP protokoll tulajdonságain belül a WINS fülön lehetséges, ahol a WINS címnek a szerverünk IP címét kell megadni.

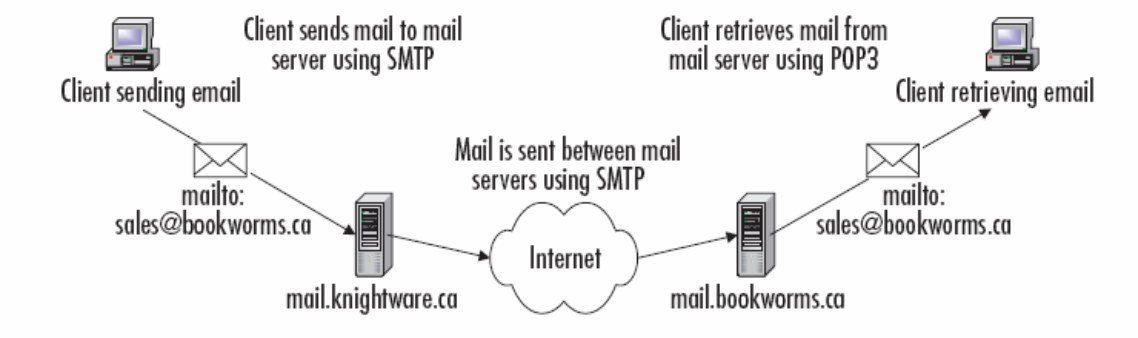
- **Adatbázis szerverek**

  Azon vállalatok számára előnyös a használata, ahol nagy adatbázisokra van szükség, az ügyfeleknek a megfelelő jogok birtokában különböző adatokhoz kell hozzáférni. Az adatbázis szerver egy olyan szerver, amely egy hálózati adatbázis alkalmazást futtat, mint például egy Microsoft SQL Server vagy Oracle Application Server.

- **Mail szerverek**

  Lehetővé teszik, hogy Windows Serverünket mail szerverként üzemeltessük, azaz képes legyen elektronikus üzenetek küldésére, fogadására. Amikor egy üzenet megérkezik a címzett mailserver tárolja, egészen addig, amíg a postafiókkal rendelkező felhasználó el nem olvassa, miután átkerül a saját postafiókjába. Ha a megszólított mailserver nem találja a címzettet, erről a feladót tájékoztatni fogja, úgynevezett Mailer Damon üzenet formájában.

  Két támogatott protokoll a Simple Mail Transfer Protocoll (SMTP) a levelek küldésére illetve a Post Office Post 3 (POP3) kizárólag a levelek szerverről való letöltésére. Ezt szemlélteti az alábbi ábra:



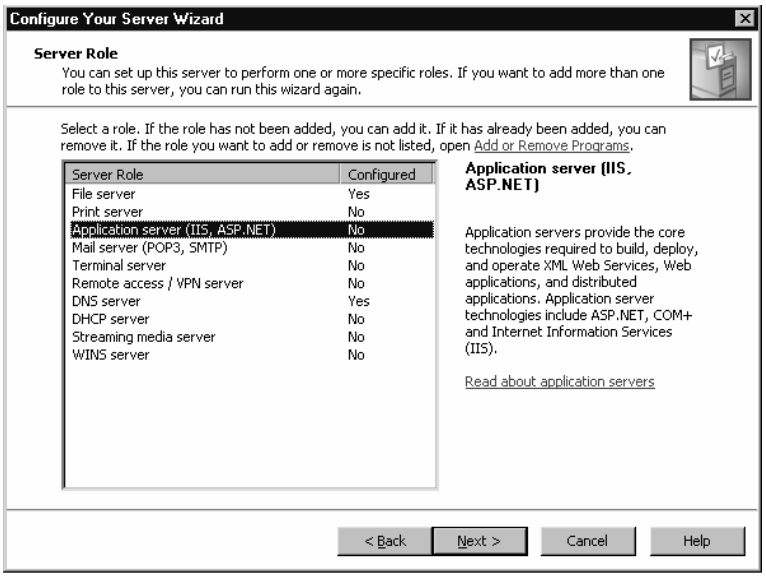
- **Alkalmazás szerverek**

  Az alkalmazásszerverek lehetővé teszik a felhasználóknak az alkalmazások hálózaton keresztül történő elérését, futtatását. Az alkalmazások ilyenkor részben vagy teljesen a szerveren futnak. Ezen alkalmazások különböző programnyelveken íródhattak (Perl,

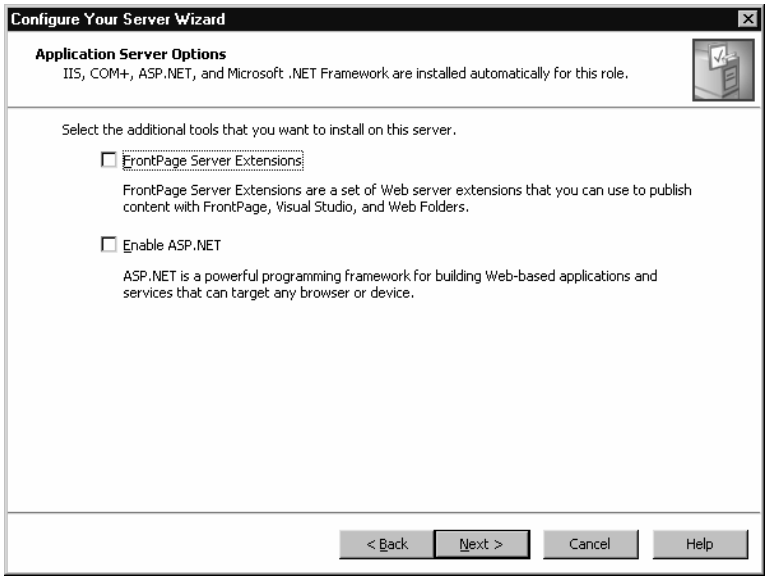
Visual Basic, Visual C++) kommunikációra pedig többnyire az Extensible Markup Languages (XML) technológia használatos. Ilyen például egy kliens gépen telepített adatbázis kezelő interfész, amely lehetővé teszi a felhasználók számára a szerveren található SQL adatbázishoz való hozzáférést.

Windows Server 2003 konfigurálása alkalmazásszerverként:

1) Start menü → Adminisztrációs eszközök → Szerver
2) Ezután válasszuk a *Szerepkör hozzáadása/eltávolítása* opciót.
3) A szerver konfigurálása ablakban feltételek elfogadása után kattintsunk a tovább gombra.
4) Ezután a telepítő ellenőrzi az OS verzióját, illetve a hálózati beállításokat, ezután megjelenik a *Szerver szerepkör* (Server Role) ablak. Itt válasszuk az Alkalmazás szerver (IIS, ASP.NET) opciót. Ezt mutatja a következő ábra:



5) Ezután az Alkalmazás szerver ablak jelenik meg, ahol a program komponensek hozzáadása történhet. Az IIS attól függetlenül kerül telepítésre, hogy melyik opciót választjuk a következők közül:
    - Front Page Server Extension
    - ASP.NET technológia alkalmazása



Ezt követően a telepítésre kerülő program komponensekről kapunk egy összesítést, majd a következő gombra kattintva végbemegy a telepítés.

VII. Az Active Directory bevezetése, a címtár filozófia

VII.1. Áttekintés

Az LDAP (Lightweight Directory Access Protocol) protokollon alapuló megoldásoknak az 1990-es évek közepén bekövetkező terjedése arra inspirálta a vállalatokat, hogy címtárakkal (a címtár: a hálózat minden erőforrását azonosítja, és hierarchikus rendszerben tárolja. Az azonosítás és tárolás mellett a hálózat fizikai felépítését és protokolljait átláthatóvá teszi, így a hálózat bármely erre feljogosított felhasználója elérheti a hálózat bármely erőforrását anélkül, hogy tudná hol találhatóak azok valójában, vagy hogyan is kapcsolódnak egymáshoz fizikailag.) integrált üzleti megoldásokat vezessenek be, amelyek olyan fontos problémákra nyújtanak megoldást, mint például a vállalati telefonkönyvek, több rendszerbe történő egyszeri bejelentkezés, nyilvánoskulcs-infrastruktúra vagy az üzleti alkalmazások és a hálózat felhasználóinak kezelése.

LDAP: az LDAP protokoll a TCP/IP-hálózatokhoz kifejlesztett kommunikációs protokoll. Az LDAP meghatározza, hogy egy adott címtárügyfél hogyan férhet hozzá a címtárkiszolgálóhoz, hogyan végezhet címtárműveleteket, illetve hogyan oszthatja meg a címtáradatokat. Az LDAP-szabványokat az Engineering Task Force (IETF) munkacsoportjai fektetik le. Az Active Directory az LDAP 2-es és 3-as verzióihoz kidolgozott, LDAP-attribútumokra vonatkozó előírásokat és IETF-szabványokat valósítja meg.

Mint ahogy a neve is jelzi, az LDAP a címtárszolgáltatásokhoz való hozzáférést segítő, hatékony, más címtárszolgáltatási protokollok bonyolultságát nélkülöző módszer. Az LDAP meghatározza, hogy melyik műveletek hajthatók végre az adatok lekérdezésekor és módosításakor, illetve, hogy miként lehet biztonságosan hozzáférni a címtáradatokhoz. Az LDAP így a címtárobjektumok keresésére és felsorolására, valamint az Active Directory lekérdezésére és felügyeletére használható.

E sikernek eredményeképpen napjainkban a legtöbb vállalatnál már létezik olyan címtárszolgáltatás, amely kezeli a hálózati operációs rendszerben a hitelesítést és az engedélyezést, azután egy olyan, amelyet a virtuális magánhálózat (VPN) nyilvánoskulcs-infrastruktúrája (PKI) használ, egy másik a céges telefonkönyv számára, és nagy valószínűséggel van egy olyan címtárszolgáltatás is, amely egyszeri bejelentkezést tesz lehetővé az extranetre vagy a webre. Nem ritkák az olyan vállalatok sem, ahol nemcsak több

címtárszolgáltatás üzemel, de ráadásul ezek a címtárszolgáltatások különböző technológiákon is alapulnak. Megtörténhet például, hogy a hálózati operációs rendszer címtára a Microsoft Active Directory szolgáltatáson alapul, a PKI címtára egy X.500 címtáron, a céges telefonkönyv és az üzleti alkalmazások címjegyzéke pedig megint egy másik címtár-technológián.

Ha ezek a címtárak mind az LDAP technológián alapulnak, nem kerülhető meg a nyilvánvaló kérdés, hogy miért nem sikerült a vállalatoknak egyetlen egységes címtár-technológiát bevezetniük. A kérdésre a fenti jelenség kialakulásában szerepet játszó tényezőkben rejlik a válasz.

- **A címtárak közötti átjárhatóság hiánya**

  Sok címtár van, amelyek egyszerűen nem képesek együttműködni egymással. Jó példa erre a múltból az eredeti X.500 címtár esete, amely nem támogatta az LDAP protokollt. Ma is vannak olyan termékek, amelyek az egész megoldás részeként címtárat is kialakítanak, ám mégsem támogatják az LDAP-ot, sem más széles körben használt protokollt.

- **A választási lehetőség hiánya**

  Egyes szoftvergyártók olyan megoldásokat szállítanak, amelyek a napjainkban használt címtárszolgáltatásoknak csak egy szűk körével tesztelték. Akik ilyet vásárolnak, azok a működési feltételek biztosítása miatt rákényszerülnek egy olyan címtárszolgáltatás bevezetésére, amelyet addig nem használtak a vállalatnál.

- **A koordináció hiánya**

  Bizonyos esetekben előfordult, hogy egymástól elszigetelten működő csoportok különböző üzleti megoldásokat vezettek be. Ennek következtében többféle címtár-technológia alkalmazására került sor.

- **A biztonsági átjárhatóság hiánya**

  Az üzleti megoldásokra nem jellemző, hogy lehetővé tennék a tőlük különböző címtárszolgáltatásban tárolt hitelesítési adatok használatát. Ez megint csak azt jelenti, hogy még több címtárszolgáltatást kell bevezetni azért, hogy mindegyik üzleti megoldásnak meglegyen a hitelesítő adatok biztonságos tárolására szolgáló összetevője.

Mára sok vállalat próbál megszabadulni a különféle címtárszolgáltatásokból származó rejtett költségektől:

- **Nagyobb biztonsági kockázat**

  A címtárszolgáltatáson alapuló üzleti megoldások terjedésével párhuzamosan egyre nehezebb biztosítani, hogy ezek a megoldások jól beépíthetők legyenek az üzleti folyamatokba. Létfontosságú, hogy amikor a dolgozók, partnerek, alvállalkozók és ügyfelek kapcsolatba lépnek a vállalattal, vagy éppen megszakítják azt, azonnali hatállyal létrejöjjön, illetve megszűnjön a VPN-hez, a PKI-hoz, a hálózati operációs rendszerhez és az egyéb üzleti megoldásokhoz való hozzáférési jogosultságuk. Ha a felügyeleti munka nehézkes, lassan jönnek létre ezek a feltételek, ami árt a termelékenységnek. Ha viszont a kapcsolat megszakadása nem tükröződik elég gyorsan a különféle címtárakban, biztonsági kockázat alakulhat ki abból fakadóan, hogy egy illetéktelen személy továbbra is hozzá tud férni valamelyik üzleti megoldáshoz.

- **Magas birtoklási költség**

  Minden, különböző címtár-technológián alapuló üzleti megoldáshoz szükség van:

  - az adott technológiára kiképzett dolgozókra
  - eltérő üzemeltetési és felügyeleti eljárásokra
  - további szoftverlicencek és külön támogatási szerződések kezelésére

- **A „sikeresség" költségeket von maga után**

  Vannak címtár-technológiák, amelyek licence a címtárban létrehozott objektumok számán alapul. Ez azt jelenti, hogy minél sikeresebb egy üzleti megoldás, annál gyorsabb ütemben ívelnek felfelé a költségek. Ez a szerencsétlen helyzet sok vállalatot érint napjainkban azok közül, amelyek több millió ügyfelet kiszolgáló extranetes hozzáférés-kezelési megoldások bevezetésére készülnek.

- **Az üzleti folyamatok integrációjának hiánya**

  A címtárakban szereplő adatok múlékony természetűek. A felhasználók más csoportba kerülnek, másik irodába költöznek, új telefonszámot kapnak, változik a nevük és a beosztásuk: mindennek a címtárban is tükröződnie kell. Ha más címtárat használó más

üzleti megoldásoknak is szüksége van ezekre az adatokra, akkor abban a másik címtárban is módosítani kell azokat. Ha ezek a módosítások nem foganatosíthatók automatikusan, a különböző identitástárak elavult, ellentmondó adatokat tartalmazhatnak.

A vállalatoknak valójában olyan címtárra van szükségük, amely alkalmazhatók a hálózati operációs rendszer infrastruktúrájaként (mint amilyen az Active Directory), és az alkalmazások is használhatják, hogy amikor az szükséges, kihasználhassák a hálózati operációs rendszer infrastruktúrájába épített biztonsági funkciókat. Az Active Directory alkalmazás módja megfelel erre a célra, ráadásul anélkül, hogy szükség lenne további oktatásra, újabb licencekre, illetve a címtárat használó alkalmazást kiszolgáló további címtárszolgáltatás telepítésével és üzemeltetésével járó költségekre.

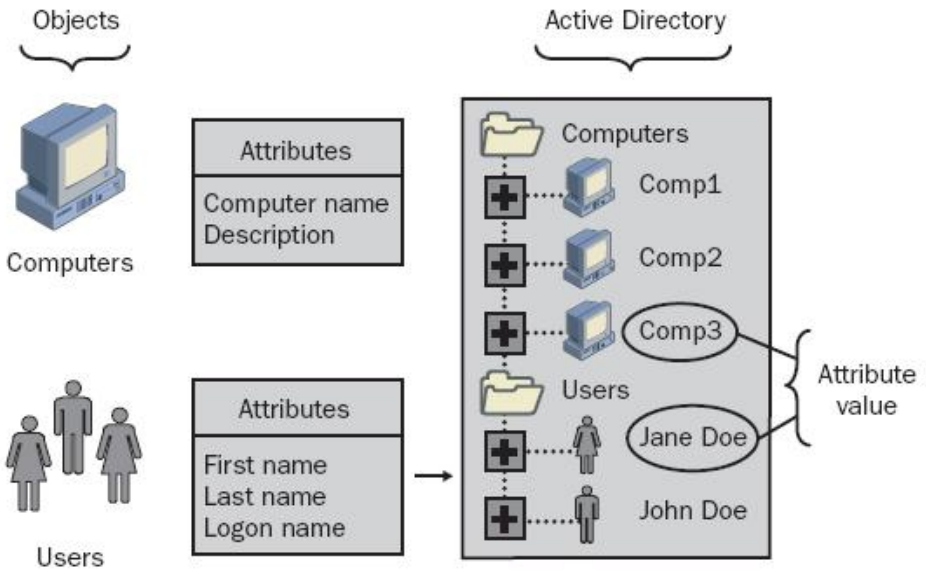
VIII. Windows Server 2003 Active Directory rendszerének bemutatása

Az Active Directory még a kevésbé megbízható távoli kapcsolatok esetén is nagyobb és egyenletesebb teljesítményt nyújt: ez a hatékonyabb replikációnak, illetve annak köszönhető, hogy a rendszer a hitelesítési adatokat a fiókirodák tartományvezérlőin, gyorsítótárban is elhelyezi.

A Windows Server 2003-ban a címtárszolgáltatást az Active Directory valósítja meg.

Az Active Directory olyasfajta könyvtárstruktúra kialakítást támogat, amely egyénileg testre szabható az adott vállalat (szervezet) elvárásainak, céljainak megfelelően. Az Active Directory könyvtárai a hálózat erőforrásairól tartalmaznak információt a felhasználók, rendszergazdák számára. Az alapja az objektumok tárolása, illetve ezek attribútumai. Kiterjedt számítógépes hálózatokban –mint például az internet is- nagyon sok objektum egy könyvtárstruktúrában való tárolására kell felkészülni. (fájl szerverek, alkalmazások, felhasználói profilok, felhasználói csoportok, nyomtatók, faxok, számítógépek).

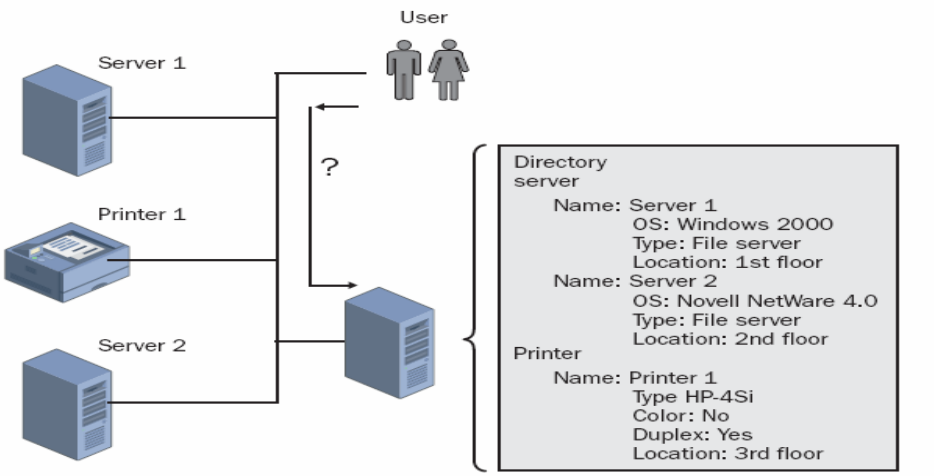
Ezt szemlélteti az alábbi ábra ahol a címtárunkban számítógép és felhasználó objektumok lesznek.



A felhasználók mind ezeket az „objektumokat” szeretnék elérni és használni. A rendszergazdák dolga lesz annak szabályozása, hogy ki, hogyan, honnan férhet hozzá ezekhez az objektumokhoz. A könyvtár szolgáltatás minden ilyen hozzáférésre, felhasználásra vonatkozó információt egy központosított helyen tárol ezzel is leegyszerűsítve ezen folyamatot.

A felhasználók legtöbbször nem fogják tudni a használni kívánt erőforrások pontos nevét, ők csak a jellemző vonásaikat ismerik. Például, tegyük fel, hogy egyik felhasználónknak egy színes nyomtatóra van szükség a cég harmadik emeletén. Az AD szolgáltatással ez igen egyszerű.

Ezt szemlélteti az alábbi ábra.



Ez különösen hasznos dolog lehet a hálózat növekedésének függvényében.

VIII.1. Az Active Directory tulajdonságai:

- Központosított adattárolás
- Központi adminisztrálhatóság
- Skálázhatóság
- Kiterjeszthetőség
- Kezelhetőség
- DNS szolgáltatással való összefonódás
- Rugalmasság
- Fokozott biztonság
- Csoportházirendek

VIII.2. Az Active Directory felépítése

VIII.2.1. Fizikia felépítés

A séma (Schema)

Az AD-ben tárolható objektumok szerkezetének leírást definiálja/tartalmazza.
Olyan objektum tulajdonságokat leíró gyűjtemény, amely meghatározza a címtárban lévő összes objektum (pl. felhasználói fiókok, szervezeti egységek, nyomtatók stb.) és attribútumok osztályát, az ezekre vonatkozó szabályokat és korlátokat, valamint az elnevezés formátumát. Minden olyan esetben, amikor új objektumtípusok kerülnek a címtárba, a sémát bővítenünk kell a rájuk vonatkozó leírással és szabályokkal (pl. Exchange Server telepítése, Windows 2000 Server frissítése Windows Server 2003-ra, stb.). A sémabővítés lehetősége minden alkalmazás számára nyitott (természetesen megfelelő jogosultságok birtokában).

A replikációs szolgáltatás (multimaster replication)

Az objektumok az AD-ben object class-ok halmazaként tekinthetők, ezen object class-ok írják le a sémában azt, hogy az adott objektum milyen attribútumokkal rendelkezik.

Nagyon fontos összetevő a replikációs szolgáltatás, amely a címtár adatait terjeszti a hálózaton. Mivel a tartomány összes tartományvezérlőjén módosíthatóak a címtár adatai, ezért az összes tartományvezérlő automatikusan részt is vesz a replikációban, tehát a címtáradatok bármilyen módosítását (pl.: megváltozik valamelyik objektum valamelyik attribútuma) a rendszer a tartomány összes tartományvezérlőjére replikálja. Magának a megváltozott érték eljuttatásának folyamatát nevezzük replikációs folymatnak. A tulajdonság megváltoztatása mindig egy tartományvezérlőn történik és a replikáció segítségével jut el a többi tartományvezérlőhöz. Ennek megfelelően az összes tartományvezérlő tartalmazza a tartományra vonatkozó összes aktuális címtáradatot.

Replikáció tulajdonságai:

- Csomag segítségével átvihető értékek száma: kb. 100.
- Egyetlen adatbázis művelettel írható értékek száma: 5000.
- Párhuzamosan több directory partíciót nem replikálnak a tartományvezérlők.
- Egy tulajdonság replikációra kész állapotba közvetlenül a címtárba írás után kerül (nincs késleltetés).
- A címtár replikáció store-and-forward típusú.
- Nagyszámú linked multivalue érték megváltozása esetén nem garantált, hogy az összes változtatás egyetlen tranzakcióban történik meg. Azonban az garantált, hogy azonos replikációs ciklusban megtörténik a változtatás végrehajtása.
- A multimaster a replikáció tulajdonság szinten történik
- Ha megváltozik egy tulajdonság, akkor nem a teljes objektum, hanem a megváltozott tulajdonság értékét replikáljuk.
- Egy replikációs ciklus ideje alatt átvihető értékek száma, korlátlan.
- Egy replikációs ütközéskezelés feloldása hatékony az órák szinkronizációja nélkül is.

Multimaster replikáció: minden tartományvezérlő elfogad módosítási kérelmet olyan objektumokhoz tartozóan, amiért authorative.

Tartományvezérlő (Domain Controller)

A tartományvezérlő a funkcionalitás csúcsa, egy tartomány fő (Primary Domain Contreller) avagy tartalék (Backup Domain Controller) vezérlője, a címtár esetleges létrehozója (az első tartományvezérlő) és tárolója (az összes tartományvezérlő), más kiszolgáló szoftverek háttérkörnyezete. Néhány esetben célszerű a tartományvezérlőre

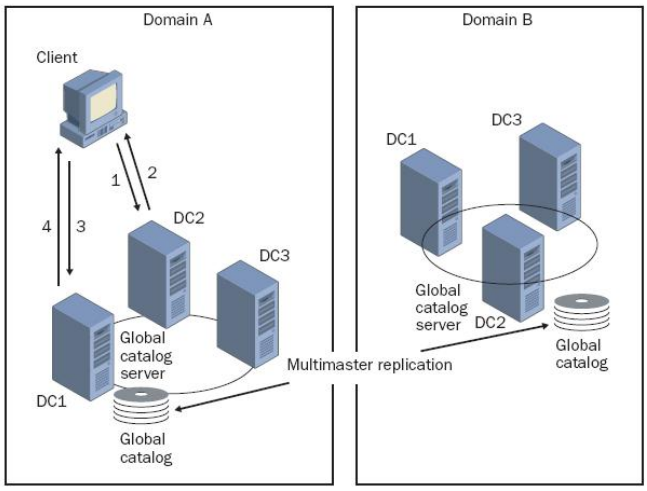
telepíteni a szerverszolgáltatást, pl. a belső tartományt kiszolgáló DNS szerver. Windows tartományon belüli autorizációs és autentikációs szolgáltatásokat nyújt. Tartalék tartományvezérlő a felhasználók autentikálására képes, de új kliensek, felhasználók felvétele csak az elsődleges tartományvezérlőben lehetséges.

A globális katalógus (Global Catalog)

Az AD lehetővé teszi a felhasználók illetve a rendszergazdák számára, hogy könnyen megtalálják az objektumokat, úgy mint nyomtatókat, faxokat, fájlokat, felhasználókat, csoportokat a saját tartományukon belül. A globális katalógus az AD által támogatott katalógusszolgáltatás. Lényegében egy központosított információ leíró adatbázis, a fákban illetve erdőben található objektumokról. A globális katalógust tartalmazó tartomány vezérlőt szokták *globális katalógus szervernek* is nevezni. Olyan tartományvezérlői szerep, amely hordozója a címtár összes objektumának alapadataival, elérhetőségeiknek információjával rendelkezik. A saját tartományából teljes, a további szorosan kapcsolódó tartományokból részleges méretű objektummásolatokat tartalmaz, így a globális katalógus segítségével kereshetőek a címtáradatok függetlenül attól, hogy valójában a címtár melyik tartománya tartalmazza azokat. Alapértelmezés szerint a frissítés előtti PDC, illetve az elsőnek telepített tartományvezérlő hordozza ezt a szerepet. Telephelyek esetén kötelező, de egyébként sem árthat, ha több globális katalógus kiszolgálónk van. Ezt az Active Directory Helyek és Szolgáltatások (Active Directory Sites and Services) MMC-ben, Helyek (Sites) faszerkezetet kibontva, az NTDS Settings tulajdonságait kibontva pipálhatjuk be. Kérdés feldolgozás (*Query Process*) a GC segítségével:

1) A kliens lekéri a DNS szervertől a globális katalógus szerver helyét (IP cím).
2) A DNS szerver azon domain controller IP címével tér vissza amely ezen globális katalógus szervernek van értelmezve.
3) A globális katalógus szerver elvégzi a lekérdezés feldolgozását.

Ezt a folyamatot szemlélteti az alábbi ábra:



Lekérdezési és indexelési rendszer

Ennek segítségével a felhasználók és alkalmazások objektumokat és azok tulajdonságait publikálhatják, illetve kereshetik meg.

Tagkiszolgáló (Member Server): a tartomány tagja, de nem tárolója a címtárnak, nem dolgoz fel a fiókbejelentkezéseket, nem vesz részt az Active Directory replikációjában. A tagkiszolgálók lehetnek fájlkiszolgálók, alkalmazás-kiszolgálók, adatbázis-kiszolgálók, webkiszolgálók, tanúsítvány-kiszolgálók (csak a stand-alone típus), tűzfal vagy távelérés-kiszolgálók. Néhány esetben kifejezetten célszerű a tagkiszolgálóra telepíteni a szerver szolgáltatást (pl. ISA Server Standard).

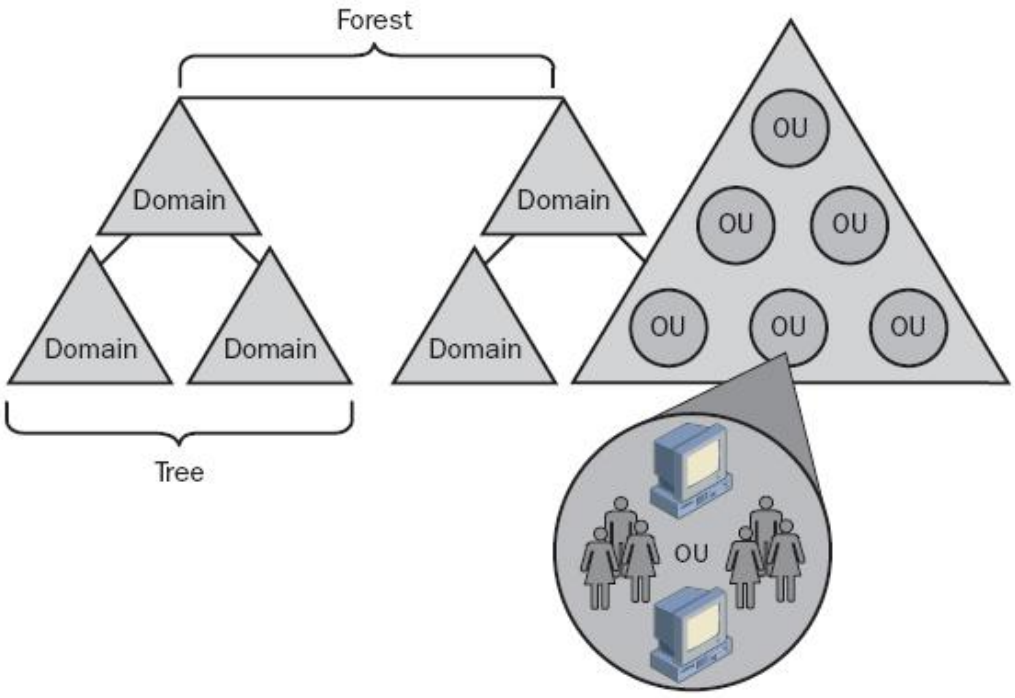
Különálló (Stand-alone Server): nem tagja a tartománynak, csak munkacsoportba beléptetett kiszolgáló, néhány speciális feladatra kihegyezve. Az ilyen típusú kiszolgáló csak a saját felhasználói adatbázisát tudja használni, ennek megfelelően saját maga is dolgozza fel a bejelentkezési kérelmeket. A fiókok adatait nem képes megosztani más gépekkel és nincs hozzáférése a tartományi fiókokhoz.

VIII.2.2. Logikai felépítés

- Tartományok (Domains)
- Szervezeti egységek (OUs)
- Fa (Tree)
- Erdő (Forest)

Az AD teljesen elkülöníti a logikai felépítést a fizikaitól.

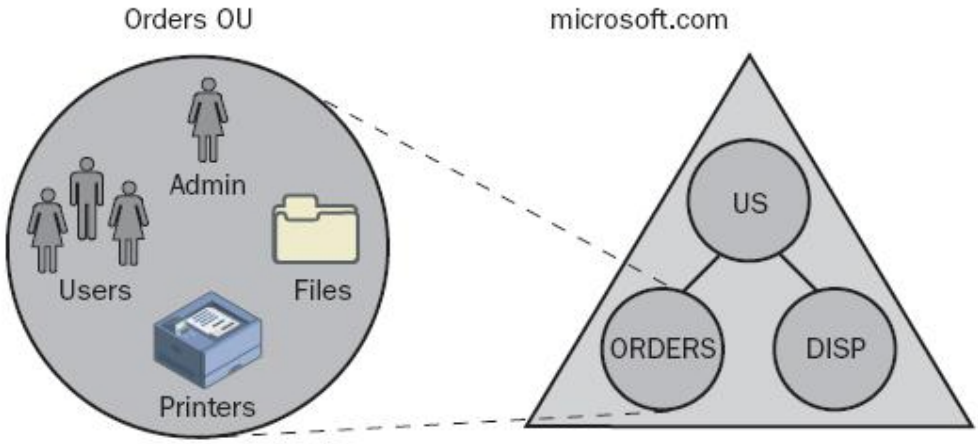
Az erőforrások logikai egységekbe sorolása lehetővé teszi, hogy egyszerűbb megtalálni őket a nevük alapján, mintsem emlékezni a tényleges elhelyezkedésükre. Az AD a hálózat logikai felépítését teszi láthatóvá a felhasználó számára. Az alábbi ábra az AD komponensei közötti kapcsolatot szemlélteti.



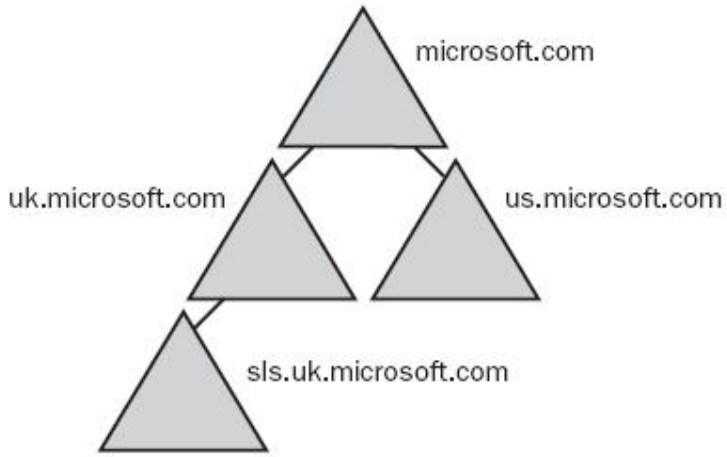
Tartomány (Domain): az AD logikai felépítésének magját képezi, több millió objektum tárolására képes. Minden egyes – a hálózatba kapcsolt- erőforrás egy tartományhoz tartozik és minden tartomány csakis az általa tárolt erőforrásokról (objektumokról) tartalmaz információt. A tartományok másik közös jellemzője, hogy egyfajta elszeparálódást,

biztonsági határvonalat is képeznek. A tartományon belüli objektumokhoz való hozzáférést a tartomány hozzáférési listája (Access Controll List) szabályozza.

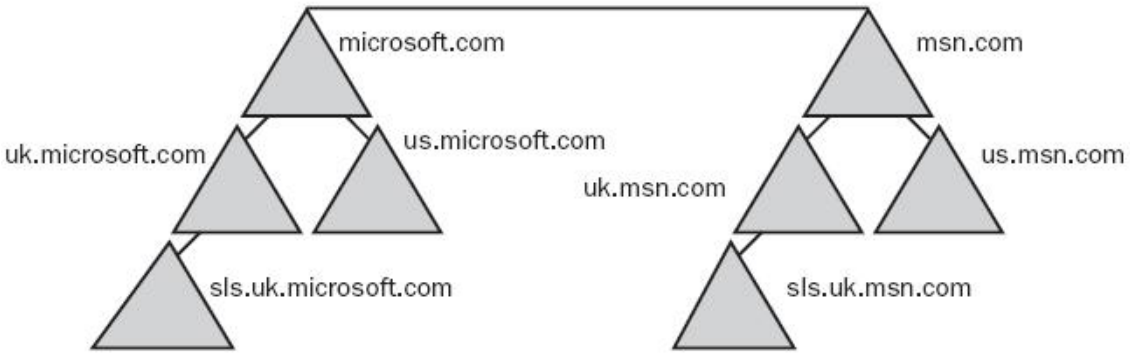
Szervezeti egység (OU): egy tartományon belüli kisebb részegységek, amelyek hierarchiákba is szervezhetőek. Ez úgy képzelhető el, mint egy nagyvállalaton belül a kisebb részlegek.



Fa (Tree): tartományok hierarchiája. Van egy szülő (gyökér), alá szerveződnek a gyermek domainek, akiknek további leszármazottaik lehetnek. Egy gyermek tartomány neve a szülőhöz képest relatív név.

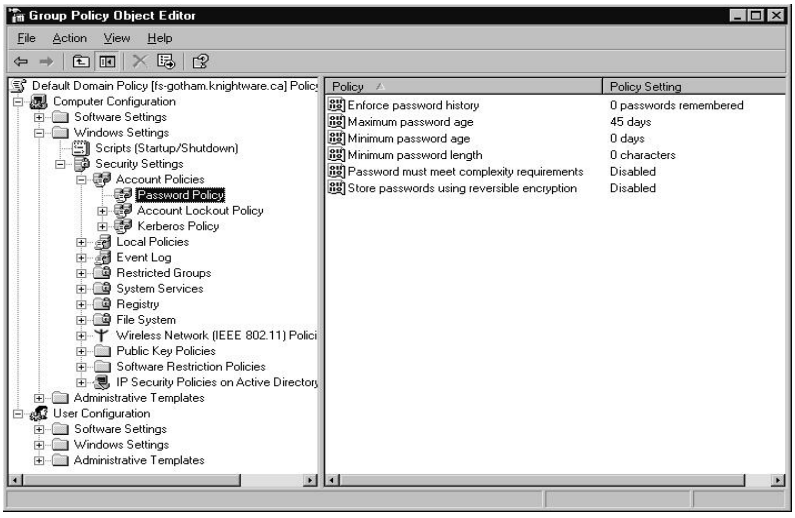


Erdő (Forest): az erdő egyfajta csoportosítása, hierarchikus elrendezése egy vagy több egymástól elkülönülő, tartományokból felépülő fának.



VIII.3. Active Directory csoport politikák (Group policies):

A csoport politikák felhasználók csoportjaihoz, számítógépek csoportjaihoz köthetők, a viselkedésmódot hivatottak befolyásolni, pl.: hogy milyen programok jelenjenek meg az egyes csoportok felhasználóinak asztalán, az egyes felhasználók milyen programokhoz férhetnek hozzá stb. Hogy felhasználók egy csoportjához egy specifikus asztali felületet adhassunk létre kell hozni úgynevezett Group Policy Objektumokat (GPOs). Ezek foglalják össze az egyes csoport politikákat. Alapértelmezésként létezik egy helyi (lokális) GPO, ezt lehet felülbírálni egy AD-alapú, úgynevezett nem lokális GPO segítségével. Ezen GPO-k tartományokhoz, szervezeti egységekhez, Site-okhoz kapcsolódva hozhatók éltre, hierarchikus kialakításban. A Group Policy Object Editor segítségével könnyen alakíthatjuk a különböző, biztonságot szolgáló beállításokat. Segítségével lehetséges a megszorításoknak sablonok formájába történő mentése (későbbi betöltés céljából), illetve már meglévő sablonok betöltése.



VIII.4. Az Active Directory címtár megtervezése

- Erdő megtervezése: törekedni kell arra, hogy egyetlen erdő jöjjön létre, ezzel elkerülvén a többszörösen kezelendő sémákat, konfigurációs gyűjteményeket, globális katalógusokat
- Tartomány megtervezése
- Szervezeti egység tervezése
- Site topológia kialakítása

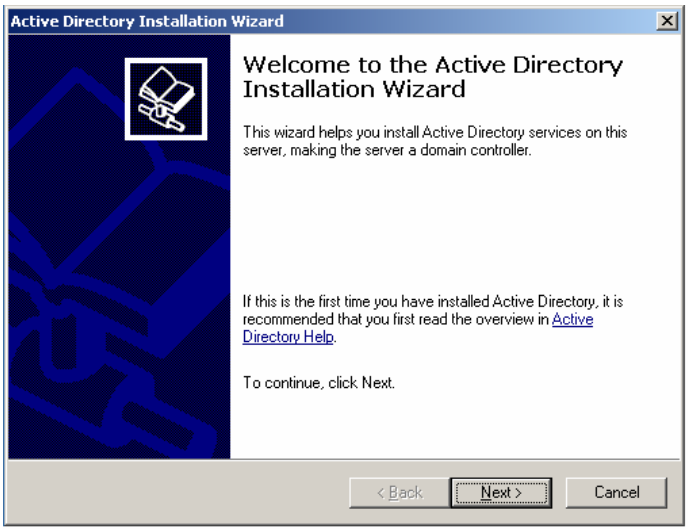
VIII.5. Az Active Directory telepítése.

Jónehány előfeltételt figyelembe kell venni az AD telepítése előtt, ezek többnyire a szervezet tartomány (domain) struktúrájára, az adatbázis tároló egységére, a rendszer kötet fájlaira, DNS konfigurálásra vonatkozó előfeltételek.

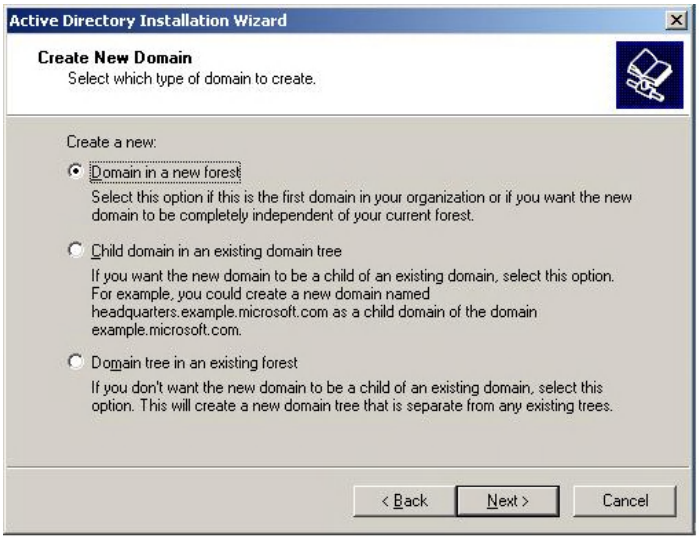
Mielőtt hozzálátnánk az AD telepítéséhez a következő dolgokat kell elvégezni:

- Domain struktúra (hierarchia) kialakítása, domain nevek meghatározása, DNS konfiguráció
- Adatbázis tároló egység illetve Naplófájlok elhelyezkedése

Az AD telepítését a DCPROMO.EXE parancs kiadásával (Start->Futtatás) kezdhetjük. A varázsló segítségével elvégezhetjük a szüksége beállításokat. Ezt szemléltetik az alábbi ábrák.


Active Directory Installation Wizard
Welcome to the Active Directory Installation Wizard
This wizard helps you install Active Directory services on this server, making the server a domain controller.
If this is the first time you have installed Active Directory, it is recommended that you first read the overview in Active Directory Help.
To continue, click Next.
< Back
Next >
Cancel


Active Directory Installation Wizard
Domain Controller Type
Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< Back
Next >
Cancel


Active Directory Installation Wizard
Create New Domain
Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< Back
Next >
Cancel

Készíthetünk egy úgynevezett “answer” fájlt is ekkor a */answer* kapcsolót kell alkalmazni (dcpromo /answer:eleresiut\config.txt)

A config.txt tartalmának a következőnek kell lennie:

- [DCINSTALL]-a Windows INI fájlokhoz hasonlóan egy fejléc szekcióval kezdődik. Ezt követik a különböző telepítési paraméterek (nem szükséges mindegyiket használni, de ha az adott körülmények között szükségeset kihagyjuk a rendszer megszakítja az automatikus telepítést és bekéri tőlünk):
- AdministratorPassword=*****
- AutoConfigDNS=Yes s

  Automatikus DNS névfeloldó konfigurás
- DomainNetBiosName="proba"

  A NetBios(Network Basic Inpu/Output System) szolgáltatás nevét adhatjuk meg.
- DNSOnNetwork=No|Yes

  Ha a tartomány első tartományvezérlőjének telepítését végezzük, akkor adjunk Yes értéket és a telepítő felrakja és bekonfigurálja a DNS-t.
- NewDomainDNSName="test.hu"

  A létrehozandó tartomány teljes specifikációnak megfelelő nevét adhatjuk meg.
- ParentDomainDNSName

  Egy létező tartomány új tartományvezérlőjének telepítésekor használatos.
- ChildName="egyetem"

  A már meglévő tartománynévhez fűz egy előtagot. Pl. itt a meglevő test.hu tartománynévhez viszonyítva az egyetem.test.hu tartomány jön létre.
- RebootOnSuccess=Yes

  Telepítés végén autómatikus újraindításról gondoskodik
- ReplicaOrNewDomain=Domain
- TreeOrChild=Tree

  Azt mondja meg, hogy az új tartomány gyökere egy új fának vagy pedig egy meglevő fához kapcsolódik
- CreateOrJoin=Create|Join

  A Create és a Join opciók közül választhatunk. Create-tel a tartomány első tartományvezérlőjének telepítésekor létrehoz egy új erdőt és egy fát. A Joinnal egy új tartományt hoz létre a létező erdőben.

- UserName=Administrator

  Annak a felhasználói fióknak a neve amely a megfelelő jogosultságokkal rendelkezik az AD telepítéséhez.
- Password=****

  A felhasználói fiókhoz tartozó jelszó.
- UserDomain=test

  A fenti felhasználói fiókot tartalmazó tartomány neve.
- DatabasePath

  Az AD adatbázisának tároló mappáját adhatjuk meg, ha nincs ilyen opció akkor a telepítő automatikusan létrehozza.
- LogPath

  A naplófájlok tárolási mappáját adjuk meg a segítségével.

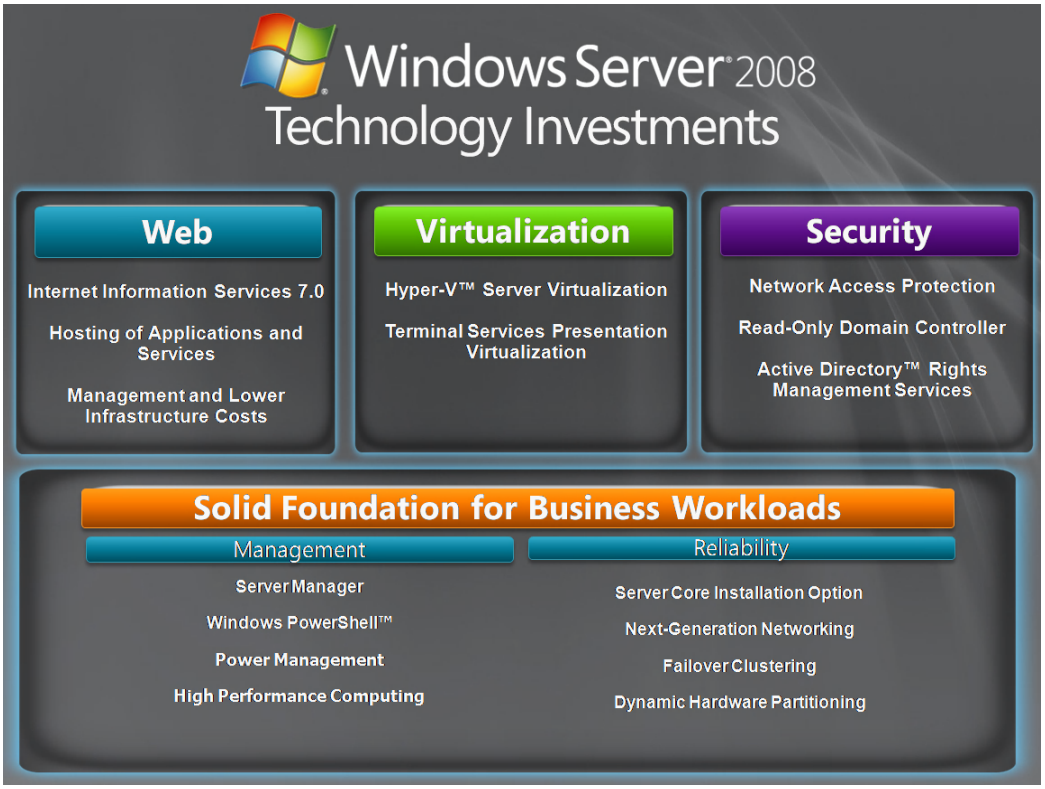
IX. A Windows Server 2008 rövid áttekintése

A Windows Server 2008 a Windows Server operációs rendszerek következő generációja, a Windows Server 2003 R2-es javítócsomagjának alapjaira építkezik. Fejlesztése során igen sokáig a Windows Longhorn nevet viselte, csakúgy mit a Windows Vista, hivatalos nevét (Windows Server 2008) Bill Gates jelentette be 2007 elején. A Microsoft a Longhorn fedőnévvel el szerette volna kerülni az Xp illetve a Windows Server 2003 eltolódott bevezetése után következő javítócsomag hercehurcát. A piac azonban megint közbeszólt és a Microsoft a Vista megjelenését előre hozat, az Xp-hez hasonlóan a Server 2003-al szemben. Kódbázisa a Windows Vista operációs rendszerével egyezik meg. Magyarországi bemutatására 2008. március 5-én került sor a Lurdy házban. Az elkövetkező évek a váltás jegyében fognak telni, a cégek mind inkább áttérnek a rengeteg technikai, technológiai újdonsággal felvértezett Windows Server 2008-ra.

Minden eddiginél magasabb hibatűrés, rendelkezésre állás jellemzi ezt a robosztus Microsoft terméket. A fejlesztések zöme a teljesítmény fokozására, megbízhatóságra, biztonságosabb hálózatkezelésre, kiszolgálói szerepkörök központi kezelésére, feladatátvételi fürtökre, központi telepítésre vonatkozik. Sok új diagnosztikai eszközt kínál. A továbbfejlesztések mellett jó néhány újdonságot is kínál (NAP, IIS 7.0, RDOC).
Termékpalettája némileg kibővült. A Server 2008 legtöbb kiadása elérhető 64 (x86-64) és 32 (x86-32) bites változatokban is.
Termékcsalád tagjai:

- Windows Server 2008, Standard Edition
- Windows Server 2008, Enterprise Edition
- Windows Server 2008, Datacenter Edition
- Windows Storage Server 2008
- Windows Web Server 2008
- Windows HCP Server 2008
- Windows Server 2008, Itanium alapú rendszerekre
- Windows Small Business Server 2008
- Windows Essential Business Server 2008

A következő ábra a Windows Server 2008 rövid technológiai áttekintését mutatja. A következőkben, ezen technológiák közül az érdekesebbek, fontosabbak kerülnek ismertetésre.



Windows Server 2008 fejlesztéseiről, újdonságairól dióhéjban:

- **Server Core telepítési opció**

  Server Core telepítést alkalmazva a grafikus komponensek nem telepítődnek, nincs Windows Explorer Shell, .Net Framework, MMC, Vezérlőpult, még IE sem. Parancssoros üzemeltetést tesz lehetővé, a kiszolgáló konfigurálása, karbantartása mind parancssorból történik. A grafikus felületből néhány alapeszköz érhető el csak, mint például a Területi és Nyelvi beállítások.

  Server Core telepítést alkalmazva lényegesen kevesebb lemezterületre van szükségünk, kb. 1,3 GB, ellenben egy teljes telepítéssel, amely kb. 6-7 GB lemezterületet igényel.

  Server Core telepítés szintén támogatja a szerver szerepkörök széles palettáját.

  Szerepkörök:

  - DHCP szerver
  - DNS szerver

- Fájl szerver
- Nyomtató szerver
- Hyper V virtuális szerver
- Active Directory tartományvezérlő
- Web szerver

Telepítés után egy konzolablakkal találkozunk, melyen keresztül végezhetjük szerverünk karbantartását.

Néhány opció:

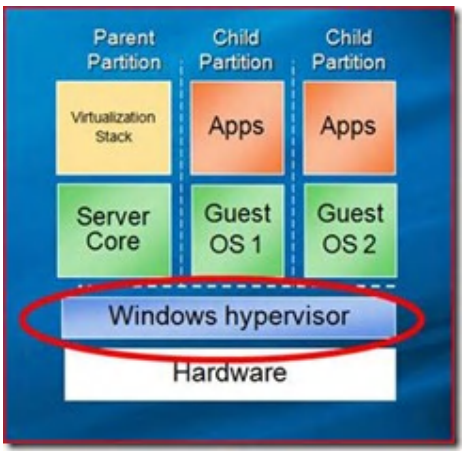
- Gép nevének beállítása:
  netdom renamecomputer %computername% /newname:<nev>
- IP cím beállítása:
  netsh interface ipv4 set address name="*nev*" source=static address=172.17.53.41 mask=255.255.0.0 gateway=172.17.53.1
- Szolgáltatás telepítése:
  ocsetup <szolgáltatás neve>
- Szolgáltatás eltávolítása:
  ocsetup <szolgáltatás neve> /uninstall

Ezt a telepítési opciót választva egy kezelhetőbb, kisebb erőforrás és lemezkapacitás igényű, megbízhatóbb szervert kapunk.

- **Hyper V technológia**

  A Hyper V egy hypervisor alapú hardver virtualizációs technológia. A Windows Server 2008 4 verziójában érhető el. A Hyper V egy szerepkörnek minősül.

  Egyfajta vékony szoftverréteg, amely a hardver és a gépen futó operációs rendszer között húzódik, lehetővé téve különböző operációs rendszerek fizikálisan ugyanazon szerveren történő szimultán futtatását. Így egyfajta partícionálódásról beszélhetünk. Minden partíció csak a saját hardver erőforrásaival gazdálkodik.



A Hyper V technológia segítségével a cégek tetszőleges operációs rendszert vásárolhatnak ezen szerepkör felé. Ezzel jelentős költségcsökkenés érhető el.

A virtualizációs technológia előnyös lehet például szoftver fejlesztéssel foglakozó cégek számára, a különböző platformokon való gyors, hatékony tesztelés segítéséhez.

A Hyper V technológia hatékony eszközöket tartalmaz a folyamatos üzemben tartás segítése végett, mint például az „élő” biztonsági mentés és a gyors áttelepítés.

- **Öngyógyító NTFS szolgáltatás**

  A korábbi Windows verziókban, ha a tároló lemezen hiba keletkezett azt a rendszer megbélyegezte, majd a következő indításkor *chkdsk* folyamattal állította helyre.

  A Windows Server 2008 ezt egy úgynevezett *NTFS worker* háttérfolyamattal oldja meg. Ez a folyamat az éppen sérült kötetek javítását azonnal, lecsatolás nélkül végzi a háttérben, ezzel is növelve a rendszer hatékonyságát. A javítás ideje alatt csak a sérült fájlok kerülnek zárolásra.

- **Windows Powershell**

  Kiterjesztett parancssori értelmező, amely objektumorientált programozási és vezérlési felület is egyben, .Net alapokon. Hozzáférést biztosít a fájlrendszerhez, mint a legtöbb parancssori ablak, illetve egyéb adatstruktúrákhoz is hozzá lehet férni, mint például a registry.

  A legtöbb parancssortól eltérően (szöveges parancsok) a Windows powershell .Net objektumokat vár és szolgáltat vissza. Ez minden eddiginél nagyobb szabadságot, rugalmasságot ad a rendszergazdák és a programozók kezébe, akik hasznos automatizálást segítő scripteket írhatnak segítségével. Ezek a scriptek parancsokból, -amit a Poweshell cmdletnek nevez- épülnek fel. A scriptek *.ps1 kiterjesztésűek.

129 db beépített parancsot tartalmaz, ezek többnyire a registry, a fájlrendszer és az események kezelésére vonatkoznak. Ezek a parancsok a nevük alapján könnyen felismerhetők, ige-főnév alakúak, pl. get-help.

A kellemetlenségek elkerülése végett a Powershell csak adminisztrátori jogosultsággal futtatható.

- **Network Address Protection (NAP)**

  Mint ahogy azt a neve is sugallja a hálózat, a hálózatba kapcsolt gépek biztonságáért felelős, a kilens gépek hálózati hozzáférését szabályozó technológia.

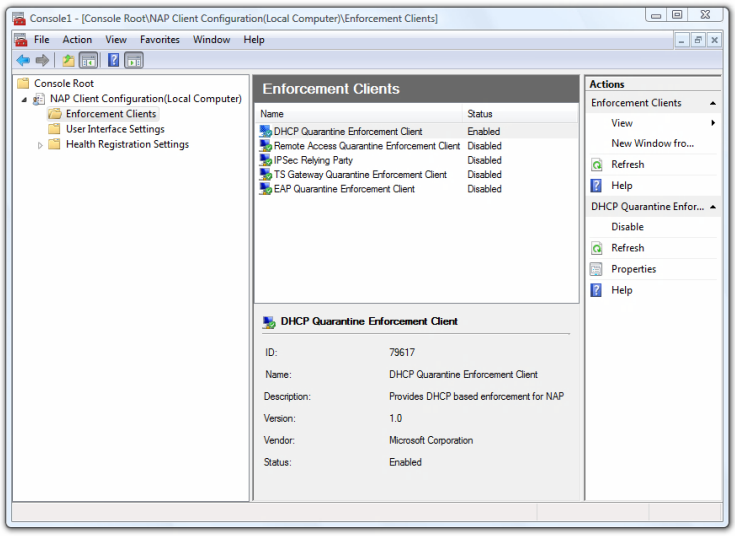
  A NAP biztosítja, hogy csak „egészséges” kliens férhessen hozzá a hálózati erőforrásokhoz, de nem csak ennek megállapítását teszi lehetővé, hanem segít ezen „egészséges” állapot elérésében is. Egy állapot akkor „egészséges”, ha megfelel a szerver NAP házirendjében (megfelelő vírusirtó, megfelelő tűzfal beállítások stb.) meghatározottaknak, ebből is látszik, hogy egy gép, amely egészséges az egyik hálózatban, nem feltétlenül egészséges a másikban.

  Ha gépünk nem felel meg ezen „egészséges” minősítésnek azt egy ilyen ablakkal jelzi felénk:

  NAP üzembe helyezése:

  A NAP szolgáltatást csak a lenti NAP klienst futtatni képes számítógépek vehetik igénybe. Ez Windows Vistában már megtalálható, a Windows XP illetve a Windows

Server 2003 SP2-esei is tartalmazzák. A kliens oldalon a konfigurációt a *napclcfg.msc* paranccsal végezhetjük.



A NAP technológiára való átváltást folyamatosan, alapos hálózati vizsgálatot követően végezzük, mert ellenkező esetben előfordulhat, hogy 100-200 gépet csatolunk le a hálózatról.

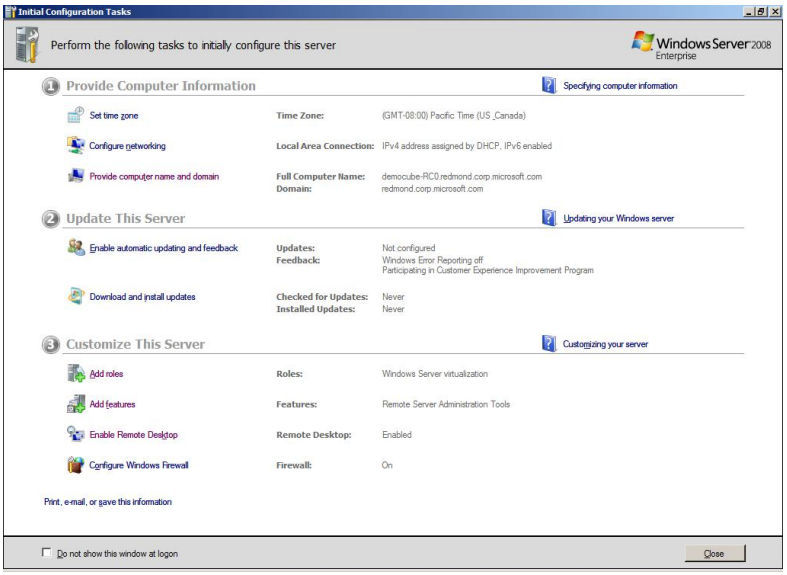
- **Csak olvasható tartományvezérlő (Read Only Domain Controller (RODC))**

  A Windows Server 2008 új, csak olvasható tartományvezérlő szerepkört is bevezet. A tartományvezérlőként funkcionáló számítógépek a címtár adatait adminisztrálják, egymással átfedésben vannak. Korábban a tartományvezérlők képesek voltak módosítani az adatokat. Server 2008-ban az adat replikáció a központ tartományvezérlők (DC) felől fog történni a telephelyeken elhelyezkedő RODC-k felé. Ezen technológiának köszönhetően a cégek a *read only* (RO) tartományvezérlőket közvetlenül a telephelyeken helyezhetik el, és nem kell félni attól, hogy hozzá nem értő személy módosít bele. Ezzel a módszerrel megoldódik a telephely céges gyökérhálózatba kapcsolódásakor tapasztalható sávszélesség felemésztési probléma, csökken a kapcsolódási idő, fokozva a biztonságot.

- **Initial Configuration Task**

  Lehetővé teszi a rendszergazdák számára, hogy a szerver egy meglevő tartományba kapcsolás a telepítés elvégzése után is megtörténhessen, nem kell feltétlenül telepítési időben megadni. Egyéb funkciói közé tartozik a szerepkörök létrehozása,

rendszergazda fiók módosítása, hálózat konfigurálása, Windows frissítések, illetve a tűzfal beállításainak karbantartása.



Összefoglalás

A hálózat biztonsága a számítógépes társadalom alapvető kérdése, problémája. Nap, mint nap hallunk az emberiséget károsító, a hálózatba való behatolásra irányuló támadásokról, elektronikus bűncselekményekről. Ezt szem előtt tartva a Microsoft igyekezett megfelelni ezen biztonságot előtérbe helyező kérdésnek Windows Server 2003 illetve 2008 operációs rendszerinek fejlesztése során.

A Windows Server 2003 a hálózat biztonságos üzemeltetésére, karbantartására eszközök széles skáláját kínálja, ezért ezek apró részletességig történő bemutatása nem tartozott, tartozhatott céljaim közé a dolgozat terjedelmi megkötöttsége miatt.

A dolgozatban ismertetésre került eljárások szinte minden modern hálózatban jelen vannak, illetve annak alapjait képezik. Célom, ezen hálózatos alapok olvasóval való megismertetése, megérttetése volt, a Windows Server 2003 nyújtotta lehetőségeket kihasználva. Remélem az olvasó hasznát veszi ezen információknak, és érdekesnek találtatnak számára az egyes témakörökben közölt információk.

Irodalomjegyzék, források

Craig Zacker:

Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Training Kit), Microsoft Press 2004

J.C. Mackin and Ian McLean:

Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Training Kit), Microsoft Press 2004

MCSE-Windows.Server.2003.Network.Security.Administrations

William Boswell:

Inside Windows Server 2003, Addison Wesley 2003

Martin Grasdal, Laura E. Hunter, Michael Cross:

Exam 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Study Guide), Syngress Publishing Inc. 2003

Windows_Server_2008_Reviewers_Guide

http://www.microsoft.com/

http://www.netacademia.net

http://technet.microsoft.com/en-us/windowsserver/default.aspx?wt.svl=leftnav

Köszönetnyilvánítás

Köszönettel tartozom dr. Krausz Tamásnak, a dolgozathoz rendelkezésemre bocsátott dokumentumokért illetve az elkészítéshez nyújtott segítségért.