DEBRECENI EGYETEM
INFORMATIKAI KAR

WINDOWS SZERVER 2003 HÁLÓZATI MEGOLDÁSAI

Diplomamunka

Konzulens: Dr. Krausz Tamás

Egyetemi adjunktus

Készítette: Serestyén Sándor

Programtervező matematikus hallgató

Debrecen, 2008

Tartalomjegyzék

I. Bevezetés 6

II. A Windows Server 2003 termékcsalád 7

II.1. Windows Server 2003, Standard Edition 7

II.2. Windows Server 2003, Enterprise Edition 7

II.3. Windows Server 2003, Datacenter Edition 8

II.4. Windows Server 2003, Web Edition 8

III. Kiszolgálói szerepkörök 8

IV. Alapvető technológiák 9

IV.1. Megbízhatóság 9

IV.2. Hatékonyság 10

V. A Windows Server 2003 termékcsalád hardverkonfigurációja 11

VI. A Windows Server 2003 telepítése 12

VI.1. Tiszta telepítés (clean install) 12

VI.2. Meglévő rendszer átalakítása frissítéssel (upgrade) 13

VI.3. Áttérés Windows NT Server platformról 15

VII. A .NET és a Windows Server 2003 16

VIII. Hálózati diagnosztikai szolgáltatások, eszközök 17

VIII.1. Hálózati diagnosztika weblapja 17

VIII.2. Netsh diagnosztikai parancsok 17

VIII.3. A hálózati kapcsolatok Javítás (Repair) menüparancsa 17

VIII.4. A hálózati kapcsolatok Támogatás (Support) füle 18

VIII.5. A Feladatkezelő párbeszédablakának Hálózat (Networking) füle 18

VIII.6. Menüparancs a távelérés naplózásához 18

VIII.7. Hálózati telephely felismerése 19

VIII.8. Vezetéknélküli helyi hálózatok kezelése 19

VIII.9. Az útválasztás és távelérés szolgáltatás (RRAS) újdonságai 20
VIII.10. TCP/IP feletti NetBIOS névfeloldási proxy 21
VIII.11. Hálózatok távoli elérésének karantén alapú korlátozása 21
VIII.12. A hálózati címfordítás és a tűzfal együttműködése 22
VIII.13. A terminálszolgáltatás ismertetése 22
IX. A hálózati kapcsolatok újdonságai 23
IX.1. Frissített csoportházirend a hálózati és a telefonos kapcsolatokhoz 23
IX.2. PPPoE a szélessávú internetkapcsolatokhoz 24
X. Hálózati topológia tervezése 25
X.1. A Windows Server 2003 és a hálózati infrastruktúra 25
X.1.1. Fizikai infrastruktúra 25
X.1.2. Logikai infrastruktúra 25
X.1.3. Hálózati infrastruktúra tervezése 25
X.1.4. Hálózati infrastruktúra megvalósítása 25
X.1.5. Hálózati infrastruktúra karbantartása 26
X.2. Az OSI referencia modell 26
X.3. A hálózati/szállítási réteg protokollok kiválasztása 27
X.3.1. TCP/IP használata 27
X.3.2. Az IPX használata 28
X.3.3. A NetBEUI használata 29
X.4. TCP/IP hálózati infrastruktúra tervezése 29
X.4.1. IP címek hozzárendelése 29
X.4.2. TCP/IP kliensek kézi konfigurálása 30
X.4.3. A DHCP használata 30
X.4.4. DHCP szerver beállítása a Kiszolgáló konfigurálása varázslóval 31
XI. Kiszolgálói szerepkörök 36

XI.1. Fájlkiszolgálói szerepkör ... 36
XI.2. Nyomtatókiszolgálói szerepkör ... 36
XI.3. Alkalmazáskiszolgálói szerepkör (IIS, ASP.NET) ... 36
XI.4. Levelezőkiszolgálói szerepkör (POP3, SMTP) ... 37
XI.5. Terminálkiszolgálói szerepkör ... 37
XI.6. Távelérési/virtuális magánhálózati (VPN) kiszolgálói szerepkör ... 37
XI.7. Tartományvezérlői szerepkör (Active Directory) ... 38
XI.8. DNS-kiszolgálói szerepkör ... 38
XI.9. DHCP-kiszolgálói szerepkör ... 38
XI.10. Adatfolyam-kiszolgálói szerepkör ... 38
XI.11. WINS-kiszolgálói szerepkör ... 39
XI.12. Kiszolgálói szerepkörök az Active Directory-ban ... 39
XI.12.1. Tartományvezérlők ... 39
XI.12.2. Tagkiszolgálók ... 39
XII. Active Directory ... 40
XII.1. Az Active Directory szolgáltatás jellemzői ... 40
XII.2. Active Directory objektumai ... 40
XII.3. Az Active Directory sémája ... 41
XII.4. Active Directory komponensei ... 42
XII.4.1. Logikai struktúra ... 42
XII.4.2. Fizikai struktúra ... 44
XII.5. Az Active Directory telepítése ... 47
XII.5.1. Az Active Directory telepítése varázsló segítségével ... 47
XII.5.2. Active Directory telepítése Answer fájl segítségével ... 49
XII.5.3. Active Directory telepítése a Kiszolgáló konfigurálása varázslóval ... 49
XIII. A DNS ... 50

XIII.1. A DNS komponensei 50
XIII.1.1. DNS kiszolgálók 50
XIII.1.2. DNS zónák 50
XIII.1.3. Erőforrásrekordok 51
XIII.2. DNS kiszolgáló telepítése 51
Összefoglalás 53
Irodalomjegyzék 54
Köszönetnyilvánítás 55

I. Bevezetés

A Windows Server 2003 a Microsoft piacvezető cég terméke, mely nagy teljesítményű infrastruktúrát biztosít a hálózatok, webszolgáltatások, és az összekapcsolt alkalmazások kiszolgálására. Dolgozatom célja, hogy az olvasóval megismertessem a rendszer legfontosabb hálózati alkalmazásait és funkcióit. Egyetemi tanulmányaim során Windows környezetben dolgoztam, és maximálisan elégedett vagyok a Microsoft termékeivel. E pozitív élmények után döntöttem el, hogy ezzel a témával kapcsolatban szeretném írni diplomamunkámat, melynek során jobban elmélyülhetek a hálózatok világában és a Windows Server 2003 által nyújtott hálózatkezelési szolgáltatásokban.

A Windows Server 2003 termékcsalád a Windows 2000 Server-en leginkább bevált technológián alapul, üzembe helyezése, felügyelete és mindennapi használata pedig könnyebbé vált. A Microsoft a Windows Server 2003 rendszerekben lényeges hálózatkezelési fejlesztéseket épített be, például az Ethernet-en keresztüli PPP (PPPoE).

A Windows Server 2003 növeli a fejlesztők hatékonyságát is, mert olyan eszközöket biztosít, amelyek segítségével tetszőleges programnyelven lehet elosztott szolgáltatásokat létrehozni. A Windows Server 2003 több újrafelhasználható objektumot, beépített szolgáltatást adott a fejlesztőknek, és tartalmazza a .NET-keretrendszert.

A hálózatkezelés és a kommunikáció minden eddiginél fontosabb szerepet tölt be a piaci versenyben résztvevő szervezetek működésében. Az alkalmazottaknak hálózati csatlakozásra van szükségük, függetlenül a helyszíntől, tetszőleges eszközről.

A hálózati infrastruktúrát kezelő rendszergazdák az új szolgáltatásoknak köszönhetően több, rugalmasabb megoldás közül választhatnak. Például biztonságos elérést állíthatnak be a vezeték nélküli helyi hálózatokhoz, csoportházirendek megadásával szabályozhatják a különböző felhasználói csoportok hálózatkezelési lehetőségeit vagy csatlakozáskezelő-profilt hozhatnak létre, amellyel az utazó felhasználók tartózkodási helyüknek megfelelően választhatják ki az optimális VPN-kiszolgálót (Virtual Private Network – Virtuális magánhálózat).

II. A Windows Server 2003 termékcsalád

A Windows Server 2003 termékcsaládnak 4 tagja van, melyeket a következő pontokban ismertetek.

II.1. Windows Server 2003, Standard Edition

Ez a megbízható kiszolgáló operációs rendszer képes kielégíteni bármilyen méretű vállalat mindennapi igényeit. Optimális megoldást jelent a fájl- és a nyomtatómegosztáshoz, biztonságos internetkapcsolatok kialakításához, központosított irodai alkalmazások telepítéséhez, valamint az alkalmazottak, partnerek és ügyfelek hálózati környezetének kialakításához. A Windows Server 2003 Standard Edition támogatja a *szimmetrikus multiprocesszálás* (SMP) szabványnak megfelelő processzor, illetve processzorok használatát. A szimmetrikus multiprocesszálás segítségével az operációs rendszer bármely elérhető processzoron tud végrehajtási szálakat futtatni, így az alkalmazások több processzort is használhatnak, ha további processzorteljesítményre van szükség a rendszer képességeinek növeléséhez. Az új szolgáltatások közé tartozik a szimmetrikus multiprocesszálás zárolási teljesítménye, a rendszerleíró adatbázis nagyobb teljesítménye, valamint a megnövelt terminál-kiszolgálói munkamenetek. Rendkívül hatékony operációs rendszer, amely biztonságos, megbízható és azonnal használható. Kiváló rendelkezésre állási és méretezhetőségi szolgáltatásokkal rendelkezik. Támogatja a speciális hálózati szolgáltatásokat, mint az Internetes hitelesítési szolgáltatás (IAS), hálózati híd, és az internetkapcsolat megosztása. 4 GB memória kezelését is támogatja.

II.2. Windows Server 2003, Enterprise Edition

A nagyvállalatok, valamint a kis- és közepes vállalkozások számára nyújt keretet biztonságos alkalmazások, webszolgáltatások, valamint infrastruktúra fejlesztésére és bevezetésére. Magas szintű megbízhatóság, teljesítmény és kiemelkedő üzleti érték jellemzi. Az Enterprise Edition 32-bites és 64-bites változatban is kapható. A Windows Server 2003 EE 8 processzort is támogatni képes kiszolgálói operációs rendszer. Nagyvállalati szintű funkciók ellátására is képes, ilyen például a nyolccsomópontos fürtkezelés és a 32 GB memória támogatása.

Elérhető Intel Itanium alapú számítógépekhez is. 64 bites platformokon is elérhető lesz (8 processzort és 64 GB memóriát támogat)

II.3. Windows Server 2003, Datacenter Edition

Ez a Microsoft legnagyobb teljesítményű operációs rendszere. 32 utas szimmetrikus többprocesszoros feldolgozást (SMP) és 64 GB memóriát is képes támogatni. Ez a változat olyan kritikus alkalmazások kiszolgálására alkalmas, amelyek a méretezhetőség és a rendelkezésre állás legmagasabb fokát követelik meg. A Datacenter Edition 32-bites és 64-bites változatban is hozzáférhető. A legmagasabb szintű méretezhetőséget és rendelkezésre állást igénylő alkalmazásokhoz készült. Alapszolgáltatásként biztosítja a nyolccsomópontos fürtkezelést és a terheléselosztási szolgáltatásokat. 64 bites platformokon is elérhető lesz (32 processzort és 128 GB memóriát támogat)

II.4. Windows Server 2003, Web Edition

A Web Edition a Windows operációsrendszer család új tagja, amely webkiszolgálásra és tárhelyszolgáltatásra lett optimalizálva. Ez a változat weboldalak kiszolgálására a legalkalmasabb, de megőrzi mindazokat az alapfunkciókat, amelyek a fokozott megbízhatóságot, felügyeletet és biztonságot nyújtják. 1 vagy 2 processzor használatát támogatja és 2 GB a használható RAM felső határa. Webalkalmazások, weblapok és XML alapú webszolgáltatások létrehozására és kiszolgálására készült. Elsősorban IIS 6.0 webkiszolgálóként futtatható. Az XML alapú webszolgáltatások és az ASP.NET technológiát használó alkalmazások gyors fejlesztéséhez és üzembe helyezéséhez biztosít platformot. Telepítés és kezelése egyszerű.

III. Kiszolgálói szerepkörök

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

- Fájl- és nyomtatókiszolgáló
- Webkiszolgáló és webalkalmazás-kiszolgáló

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

IV. Alapvető technológiák

IV.1. Megbízhatóság

A Windows Server 2003 termékcsaládot megbízhatósága, rendelkezésre állási képességei, méretezhetősége és biztonsága nagy megbízhatóságú platformmá teszi. A továbbfejlesztett fürttámogatás segítségével a Windows Server 2003 termékcsalád fokozott rendelkezésre állást (availability) biztosít. A termékcsalád maximum nyolc csomópontos kiszolgálófürtöket támogat. Biztosítja a *feladatátvételt*, amely azt jelenti, hogy ha egy fürt egyik csomópontja karbantartás vagy hiba miatt nem érhető el, akkor egy másik csomópont azonnal megkezdi a szolgáltatást az adott csomópont helyett. Támogatja a hálózati terheléselosztást is, amely a fürt csomópontjai között kiegyensúlyozza a beérkező IP-forgalmat.

Horizontálisan és vertikálisan is méretezhető a termékcsalád. Horizontálisan a fürtszolgáltatás által, vertikálisan pedig a szimmetrikus többprocesszoros feldolgozás (SMP) segítségével van megoldva a méretezhetősége.

A Windows Server 2003 több biztonsági újítást és fejlesztést is tartalmaz. Ilyenek például a következők:

- **The common language runtime (Közös nyelvű futásidő):**

  Ez az alapprogram fokozza a rendszer megbízhatóságát, lecsökkenti a szokásos programozói hibákból adódó szoftverhibák és biztonsági rések számát. Ezáltal a rendszernek kevesebb sebezhető pontja van. A közös nyelvű futásidő azt is garantálja, hogy az alkalmazások hiba nélkül futhatnak, és ellenőrzi a szükséges engedélyeket, hogy a kódok csak a szükséges műveleteket hajtsák végre.

- **Internet Information Services 6.0. (IIS)**

  Az IIS 6.0 és a Windows Server 2003 hibatűrési, kérelem-várólistázási, az alkalmazások működőképességét figyelő, automatikus alkalmazás-újrahasznosítási, gyorsítótárazási és egyéb szolgáltatásai révén a legmegbízhatóbb, leghatékonyabb, legintegráltabb webkiszolgáló megoldást kínálja.

IV.2. Hatékonyság

A Windows Server 2003 több olyan szolgáltatással is rendelkezik, melyek segítségével nő a hatékonyság a vállalaton belül. Ilyenek például a következők:

- **File and print services (Fájl és nyomtató szolgáltatás)**

  A rendszer megnövelt teljesítményű és funkcionalitású fájl- és nyomtató-megosztási szolgáltatásokkal rendelkezik.

- **Active Directory (Címtárszolgáltatás)**

  A hálózatban lévő objektumok címtár-információit logikus, hierarchikus rendben tárolja. Az új fejlesztések eredményeképpen gazdaságosabbá és megbízhatóbbá vált ez a szolgáltatás. A címtár tervezésében, üzembe helyezésében és kezelésében nagyobb rugalmasságot tesz lehetővé az előző verzióhoz képest.

- **Management services**

- **Storage management (Tárkezelési szolgáltatás)**

- **Terminal services (Terminálszolgáltatások)**

  A Terminálszolgáltatások segítségével Windows alapú alkalmazásokat, vagy magát a Windows asztalt elméletileg bármilyen eszközre eljuttathatja, olyanokra is, amelyek nem tudnak Windows operációs rendszert futtatni.

V. A Windows Server 2003 termékcsalád hardverkonfigurációja

A Windows Server 2003 termékcsalád által kihasználható legnagyobb hardver konfigurációját foglalja össze a következő táblázat.

Paraméter	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Maximális RAM	2 GB	4 GB	• 32 GB az x86-alapú számítógépekben • 64 GB az Itanium-alapú számítógépekben	• 64 GB az x86-alapú számítógépekben • 512 GB az Itanium-alapú számítógépekben
A kihasználható processzorok száma	maximum 2	maximum 4	Maximum 8	• minimum 8 (előírt) • maximum 32 az x86-alapú számítógépekben • maximum 64 az Itanium-alapú számítógépekben
Fürtözés	Nincs	nincs	maximum 8 csomópont	maximum 8 csomópont

VI. A Windows Server 2003 telepítése

Kétféle telepítés közül választhatunk:

- Tiszta telepítés
- Frissítéses telepítés (upgrade)

VI.1. Tiszta telepítés (clean install)

Ez a telepítéstípus már a Windows 2000 Servernél is két lépésből állt:

1. az operációs rendszer, és
2. a címtár telepítéséből.

Ez a Windows Server 2003-ban is így történik. Ráadásul egy új telepítésnél általában nem merülnek fel sorrend vagy szerepköri kritériumok, hiszen ez a szerver lesz a tartomány első - és lehet, hogy az egyetlen tartományvezérlője a jövőben is - így az összes ún. 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), különben a következő hibaüzenetet kapjuk az előléptetési kísérlet során:

Bizonyos esetekben, akkor is a tiszta telepítést kell választanunk, hogyha már van működő tartományunk, mert pl.:

- Eltérő nyelvi változatot szeretnénk
- Windows NT4 előtti tartományunk van (NT 3.51, 3.5)

Tiszta telepítés migrálással

Ennél a telepítési formánál részben le kell mondanunk az előző rendszer elemeiről. A Windows NT4 vagy Windows 2000-es tartományunkból címtár objektumokat migrálni (importálni) egyszerű feladat. Ez a folyamat soha nem lehet olyan szintű beállítás- és jogosultság öröklés, mint egy frissítés, de az Active Directory Migration Tool (ADMT) segítségével 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.

További hasznos eszközök:

- User State Migration Tool : felhasználói beállítások átörökítése
- IIS Migration Wizard: az Internet Information Server komponenseinek átörökítése

VI.2. Meglévő rendszer átalakítása frissítéssel (upgrade)

Ennek hátránya, hogy az előző (esetleg rosszul megtervezett) rendszer hátrányait, hiányosságait valószínűleg nem tudjuk kijavítani.

Előnye, hogy nem kell a különböző beállítások (partíciók, TCP/IP) tervezésére akkora gondot fordítani. A meglevő felhasználók, csoportok, jogok és jogosultságok, megosztások megmaradnak változatlan formában. Emellett az alkalmazásaink, állományaink és mappáink szerkezete is változatlan marad, és tartományvezérlő esetén a címtár frissítése is lezajlik a telepítés közben. A telepítési előkészületek többnyire csak az előző rendszer mentésére illetve többszerveres környezet esetén a szerver frissítések sorrendjének megtervezésére vonatkoznak.

A telepítés megkezdése előtt mindig ellenőrizni kell a minimális rendszerkövetelményeket. A Windows Server 2003 minimális és ajánlott rendszerkövetelményeit a következő táblázat tartalmazza:

Követelmény	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Minimális processzor-sebesség	133 MHz	133 MHz	• 133 MHz az x86-alapú számítógépekben • 733 MHz az Itanium-alapú számítógépekben	• 400 MHz az x86-alapú számítógépekben • 733 MHz az Itanium-alapú számítógépekben
Ajánlott processzor-sebesség	550 MHz	550 MHz	733 MHz	733 MHz
Minimális RAM	128 MB	128 MB	128 MB	512 MB
Ajánlott minimális RAM	256 MB	256 MB	256 MB	1 GB
A telepítéshez szükséges lemezterület	1.5 GB	1.5 GB	• 1.5 GB az x86-alapú számítógépekben • 2.0 GB az Itanium-alapú számítógépekben	• 1.5 GB az x86-alapú számítógépekben • 2.0 GB az Itanium-alapú számítógépekben

VI.3. Áttérés Windows NT Server platformról

A következő táblázat összefoglalja a támogatott frissítési módokat a Windows NT Server és a Windows Server 2003 között:

	Frissítés Windows Server 2003 Standard verzióra	Frissítés Windows Server 2003 Enterprise verzióra	Frissítés Windows Server 2003 Datacenter verzióra	Frissítés Windows Server 2003 Web verzióra
Windows NT 3.51 vagy korábbi	Nem lehetséges	Nem lehetséges	Nem lehetséges	Nem lehetséges
Windows NT4 Server	Lehetséges	Lehetséges	Nem lehetséges	Nem lehetséges
Windows NT4 Server Enterprise Edition	Nem lehetséges	Lehetséges	Nem lehetséges	Nem lehetséges
Windows NT4 Server Terminal Edition	Lehetséges	Lehetséges	Nem lehetséges	Nem lehetséges

A hardver és szoftver kompatibilitásra lényegesen jobban oda kell figyelnünk, mint a Windows 2000 esetén (gondoljunk csak az NT4-ben még nem létező Plug and Play-re vagy az USB-re), ezért kiemelendően fontos az előzetes kompatibilitás vizsgálat, a korábban már ismertetett módon. Ezeken kívül a (minimum) Service Pack 5 csomag jelenléte is alapkövetelmény. Több szerver esetén a frissítést kötelezően a PDC-vel (elsődleges tartományvezérlő) kell kezdenünk, és mielőtt ezt megtesszük (a Windows 2000 Server telepítési körülményeihez hasonlóan) érdemes egy BDC-t (egy másodlagos tartományvezérlőt) készíteni a hálózatról, azért, hogy erről egy esetlegesen sikertelen tartomány frissítés után az NT tartomány adatait vissza tudjuk állítani.

VII. A .NET és a Windows Server 2003

A Microsoft .NET olyan technológiák együttese, amelyek segítségével információt, embereket, rendszereket, és eszközöket összekapcsoló alkalmazásokat lehet készíteni.

A Windows Server 2003 megbízható, méretezhető, nagy teljesítményű operációs rendszer, alkalmas az XML-alapú webszolgáltatások készítésére, terjesztésére és kiszolgálására. A .NET-keretrendszer a Windows Server 2003 szerves része, így beépített eszközökkel támogatja az olyan webszolgáltatás-szabványokat, mint az XML (*eXtensible Markup Language*), a SOAP (*Simple Object Access Protocol*), a UDDI (*Universal Description, Discovery and Integration*) vagy a WSDL (*Web Service Description Language*). A Microsoft Passport pedig szervesen beépül a Windows Server 2003 hitelesítési rendszerébe, így biztonságos módszert nyújt az Internetről érkező felhasználók kezelésére.

Az UDDI-szolgáltatások megkönnyítik a webszolgáltatások és más programozható erőforrások megkeresését, megosztását és újrafelhasználását. Javítják a fejlesztés és az üzemeltetés hatékonyságát

A Windows Server 2003 mindemellett az IIS legújabb változatát is tartalmazza. Az IIS 6.0 funkciói nagymértékben javítják a rendszerek teljesítményét és a megbízhatóságát. Az IIS-en futó webes alkalmazások hatékonyabban használhatják ki a többprocesszoros számítógépek teljesítményét.

A Windows Server 2003 rendszerrel a Microsoft bevezette a nyelvfüggetlen futtatórendszert (*Common Language Runtime*, CLR). A CLR biztonságos futási környezetet nyújt, ezzel csökkenti a gyakori alkalmazásprogramozási hibákból eredő üzemzavarok és biztonsági rések számát. Amikor egy kódrész futtatható formában elkészül, a CLR ellenőrzi, hogy tud-e hiba nélkül futni, érvényesek-e a hozzáférési engedélyei, és nem hajt-e végre helytelen műveleteket. A CLR nyomon követi, hogy a kódot honnan töltötték le, vagyis ellenőrzi, hogy rendelkezik-e valamely megbízható fejlesztő aláírásával, illetve változott-e az aláírás óta.

A Windows Server 2003 a Microsoft Windows NT 4.0 és Windows 2000 operációs rendszerekben bevezetett szabványos adatvédelmi technológiák továbbfejlesztéseit is magában foglalja. A Windows Server 2003 olyan technológiákat tartalmaz, mint a Kerberos, a PKI (Public Key Infrastructure – nyilvános kulcsok infrastruktúrája) és az intelligens kártyával működő bejelentkezés.

VIII. Hálózati diagnosztikai szolgáltatások, eszközök

VIII.1. Hálózati diagnosztika weblapja

A Hálózati diagnosztika eszközzel gyorsan és könnyen jeleníthet meg információt a hálózati környezetről. Az eszköz a számítógépről, az operációs rendszerről, a hálózatról és a hálózati adapterekről nyújt információt. A Hálózati diagnosztika eszközzel, szabványos módszerekkel lehet ellenőrizni a hálózati kapcsolatokat, például a ping paranccsal egy kiszolgáló hálózati elérési útjának az ellenőrzésére van lehetőség, vagy kapcsolódni lehet egy kiszolgálóhoz. A Hálózati diagnosztika eszköz a hálózati erőforrásokhoz való sikeres és sikertelen hozzáférési kísérletekről is tájékoztat.

***Ping parancs*:** Internet Control Message Protocol (ICMP) visszhangkérő üzeneteket küldve ellenőrzi az IP-szintű kapcsolatot egy másik TCP/IP protokollos számítógéppel. A megfelelő visszhangválasz-üzenetek fogadását megjeleníti az oda-vissza út idejével együtt. A ping a kapcsolat, az elérhetőség, és a névhozzárendelés hibaelhárításához használható elsődleges TCP/IP parancs.

VIII.2. Netsh diagnosztikai parancsok

A Netsh parancssori parancsfájlkezelő segédprogram, amely lehetővé teszi egy futó helyi vagy hálózati számítógép hálózati beállításainak megjelenítését vagy módosítását. A Netsh parancsfájlkezelési szolgáltatást is nyújt, amely lehetővé teszi parancssorozatok futtatását kötegelt módban egy számítógépen. A Netsh segédprogram képes szövegfájlba menteni a konfigurációs parancsfájlt archiválás, vagy más kiszolgálók konfigurálásának elősegítése céljából. A Netsh dinamikus csatolású függvénytár (Dinamic Link Library - DLL) fájlokon keresztül működik együtt az operációs rendszer összetevőivel.

VIII.3. A hálózati kapcsolatok Javítás (Repair) menüparancsa

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

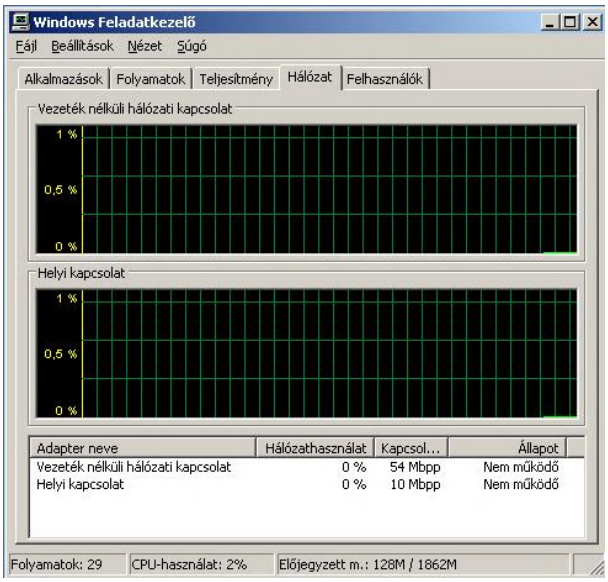
műveletek kézi végrehajtását. A parancs választásakor a rendszer egy sor olyan műveletet hajt végre, amelyek nagy valószínűséggel megoldják a kommunikációs problémákat.

VIII.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 menüben található Javítás paranccsal.

VIII.5. A Feladatkezelő párbeszédablakának Hálózat (Networking) füle

A Feladatkezelő új Hálózat füle valós idejű adatokat jelenít meg a rendszerben található hálózati kártyákról. A program könnyen átlátható módon jeleníti meg a számítógépen működő hálózat(ok) állapotát. A Feladatkezelőben csak akkor jelenik meg a Hálózatok fül, ha a számítógében van hálózati kártya. Itt megtekinthető a hálózati kapcsolat(ok) neve, a hálózat használata %-os arányban, a kapcsolat maximális sebessége, és a kapcsolat állapota.



VIII.6. 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 távelérési kapcsolatok konfigurációjával és használatával kapcsolatos adatokat lehet automatikusan rögzíteni a naplózás engedélyezésével. A naplófájl segítségével, a kapcsolatokkal összefüggő hibákat lehet megtekinteni. Ha a naplózás nem volt engedélyezve, és egy kapcsolat sikertelen volt, akkor a rendszer felkínálja a naplózás engedélyezésének lehetőségét. Majd ezután, a távelérési kapcsolat újratárcsázásával, tudjuk naplózni a sikertelen kapcsolattal összefüggő hibákat.

Távelérés: a távol vagy nem állandó munkahelyen dolgozó munkatársak a vállalati hálózatokhoz csatlakoztathatók. A távoli felhasználók úgy dolgozhatnak, mintha számítógépük fizikailag csatlakozna a hálózatra. A távelérésű kapcsolat engedélyez minden olyan szolgáltatást, amely a LAN-kapcsolattal rendelkező felhasználók számára általában elérhetők (például üzenetküldés, fájl- és nyomtatómegosztás).

VIII.7. Hálózati telephely felismerése

A hálózati telephelyet felismerő szolgáltatás lehetővé teszi a Windows Server 2003 rendszer számára, hogy észlelje annak a hálózatnak az adatait, amelyhez a számítógép csatlakozik. Ez lehetővé teszi az adott hely hálózati protokolljának helyes beállítását. Az új csoportházirend-beállítások a hálózati telephely észlelésén alapulnak. Ennek segítségével engedélyezhető, illetve tiltható le az internetkapcsolat megosztása (ICS), az internetkapcsolat tűzfala (ICF) és a hálózati híd. Ezek a szolgáltatások csak akkor lépnek érvénybe a számítógépen, amikor az csatlakozik ahhoz a hálózathoz, amelyre a lekért adatok vonatkoznak.

VIII.8. Vezetéknélküli helyi hálózatok kezelése

Ezen a területen is történtek fejlesztések. Újdonságnak számít az automatikus kulcskezelés és a felhasználók hitelesítése és engedélyezése a hálózat elérését megelőzően. A Windows Server 2003-ban megnövelték a biztonságot az Ethernet- és a vezetéknélküli-hálózatoknál. Konfigurációmentes vezetéknélküli kapcsolatot fejlesztettek ki, ami azt jelenti, hogy a rendszer felhasználói beavatkozás nélkül képesek választani az elérhető vezetéknélküli hálózatok közül a kívánt hálózatra irányuló kapcsolatok beállításához. Az egyes hálózatok beállításai elmenthetők, és automatikusan újból felhasználhatók, amikor az adott vezeték nélküli hálózat hozzárendelése megtörténik. A bevezetett szolgáltatások közé tartozik a DHCP-konfiguráció megújítása az újbóli társítás alkalmával, a szükség szerinti újbóli hitelesítés, valamint a konfigurációs beállítások kiválasztása attól a hálózattól függően,

amelyhez a számítógép csatlakozik. Az egyik új beépülő modul a vezeték nélküli hálózatok figyelésére alkalmas, amellyel megtekinthetők a vezeték nélküli elérési pontok (AP – Access Point), továbbá a vezeték nélküli ügyfelek beállításai és a statisztikai adatok. A Windows Server 2003 rendszer támogatja a vezeték nélküli hálózati kapcsolatokra vonatkozó PEAP (Protected Extensible Authentication Protocol) protokollt. Ez a protokoll a drótnélküli hálózati ügyfelet a hálózat felé jelszóval, az azonosítást és az autorizációt végző kiszolgálót, valamint a vezeték nélküli elérési pontokat (AP) az ügyfélgép felé tanúsítvánnyal azonosítja, így ezzel a jelenleg ismert legbiztonságosabb drótnélküli kapcsolatot biztosítja. A PEAP protokoll az AP tanúsítványának leellenőrzése után, annak nyilvános kulcsa segítségével titkosított csatornát hoz létre a hitelesítési folyamat elkezdése előtt.

VIII.9. Az útválasztás és távelérés szolgáltatás (RRAS) újdonságai

Az Extensible Authentication protokollt (EAP) használva tetszőleges hitelesítő mechanizmus érvényesíti a távkapcsolatot. A használandó pontos hitelesítési sémát a távelérésű ügyfél és a hitelesítő egyezteti. Az Útválasztás és távelérés szolgáltatás (RRAS – Routing and Remote Access) alapértelmezés szerint támogatja az EAP-TLS és az MD5-Challenge sémát.

EAP (Extensible Authentication Protocol): Az EAP a PPP (Point-to-Point Protocol) protokoll kiterjesztése, amely tetszőleges hitelesítési módszer alkalmazását teszi lehetővé, tetszőleges hosszúságú hitelesítő adatok és információcserék használatával.

Az EAP nyitott végű párbeszédet tesz lehetővé a távelérésű ügyfél és a hitelesítő között. A párbeszéd tartalma: a hitelesítő igazoló adatokat kér, a távelérésű ügyfél pedig válaszol. Ha például biztonsági token-kártyákkal használják az EAP protokollt, a hitelesítő külön-külön le tudja kérdezni a távelérésű ügyféltől a nevet, a PIN-kódot és a kártya token-értékét. Az egyes kérdések és az azokra adott válaszok után a távelérésű ügyfél újabb és újabb hitelesítési szintre kerül. Ha az ügyfél minden kérdésre kielégítő választ adott, a hitelesítése sikeresnek tekinthető.

A Windows Server 2003 termékcsalád tartalmazza az EAP-infrastruktúrát.

EAP-infrastruktúra: Az EAP olyan belső komponensekből áll, amelyek felépítésbeni támogatást biztosítanak minden beépülő modul formátumú EAP-típusnak. A sikeres hitelesítéshez, a távelérésű ügyfélre és a hitelesítőre, ugyanazt az EAP hitelesítő modult kell telepíteni.

A Windows Server 2003 termékcsalád a következő két EAP-típust biztosítja:

- MD5-Challenge
- EAP-TLS

MD5-Challenge (Message Digest 5 Challenge): olyan nélkülözhetetlen EAP-típus, amely ugyanazt a kihívás-kézfogás (challenge handshake) típusú protokollt használja, mint a PPP alapú CHAP (Challenge Handshake Authentication Protocol), de a kihívások és a válaszok EAP-üzenet formátumúak.

EAP-TLS (EAP-Transport Level Security): egy olyan EAP-típus, amelyet tanúsítványon alapuló biztonsági környezetben használnak. Az EAP-TLS a legerősebb hitelesítési és kulcs-meghatározási módszer. Egy *kölcsönös hitelesítési módszer*, ami azt jelenti, hogy mind az ügyfél, mind a kiszolgáló azonosítja magát. A hitelesítési folyamat során a távelérési ügyfél elküldi felhasználói tanúsítványát, a távelérési kiszolgáló pedig számítógép-tanúsítványát. Ha valamelyik tanúsítvány nem érkezik meg vagy érvénytelen, az összeköttetés megszakad.

VIII.10. TCP/IP feletti NetBIOS névfeloldási proxy

A TCP/IP feletti új NetBIOS (NetBT) proxy az Útválasztás és távelérés szolgáltatás beépített funkciója, amely lehetővé teszi az egy vagy több alhálózatból és egyetlen útválasztóból (amely Windows Server 2003 rendszerrel működő távoli elérésű kiszolgáló) álló hálózatokhoz csatlakozó távelérési ügyfelek számára a DNS-kiszolgáló vagy WINS-kiszolgáló nélküli névfeloldást.

VIII.11. Hálózatok távoli elérésének karantén alapú korlátozása

A karantén szolgáltatás az RRAS és az IAS (Internet Authentication Service) közös szolgáltatása. Célja, hogy a távolról a céges hálózatra kapcsolódó számítógépeket csak akkor engedjük be a hálózatra, ha azokat leellenőriztük. A hagyományos távoli kapcsolat létrejöttét követően a még ellenőrizetlen ügyfélgép egy úgynevezett karantén hálózatba kerül. Az ügyfél a hálózat erőforrásait – természetesen saját jogaival - már ekkor is elérheti. A karanténban lévő gépeknek egy adott időintervallum áll rendelkezésükre (ez alapértelmezés szerint 5 perc), hogy lefuttassanak néhány, a rendszergazda által meghatározott diagnosztikai parancsot. Az

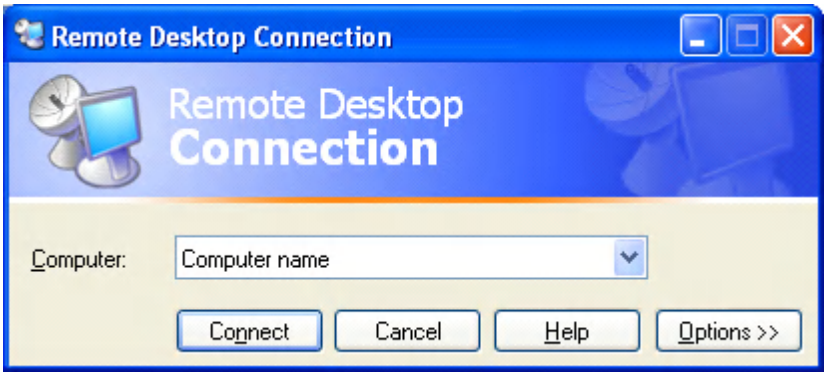
RRAS kiszolgáló ezen idő leteltével automatikusan bontja a kapcsolatot, amennyiben a diagnosztika eredménye szerint a kapcsolódó gép nem teljesíti a céges előírásokat (például: nem futtatja egy adott vírusirtó legfrissebb változatát, vagy nincs feltelepítve a legfrissebb szervizcsomag stb.).

VIII.12. A hálózati címfordítás és a tűzfal együttműködése

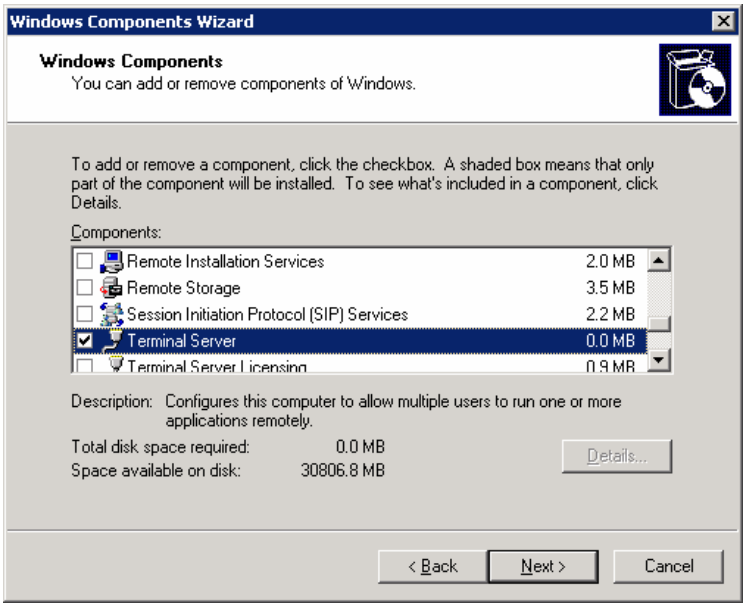
Az Útválasztás és távelérés szolgáltatás továbbfejlesztett Hálózati címfordítás/egyszerű tűzfal összetevője egyszerű tűzfalat is kezel, amely a Windows XP-ben meglévő tűzfal elve szerint működik. Ez a szolgáltatás lehetővé teszi a Windows Server 2003 rendszerrel működő és az Internet eléréséhez NAT-ot használó számítógép nyilvános hálózati kapcsolatának védelmét. A NAT (Network Address Translation) 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).

VIII.13. A terminálszolgáltatás ismertetése

A terminálszolgáltatások segítségével a Windows alapú alkalmazások bármely számítástechnikai eszközre eljuttathatók. Ha a felhasználók a Terminálkiszolgálón futtatnak egy alkalmazást, a program végrehajtása kizárólag a kiszolgálón történik, és a hálózaton csak a billentyűzet, az egér és a kijelző adatai haladnak át. Ha egy alkalmazást a terminálkiszolgálón kezelnek, akkor a felhasználók biztos, hogy az adott alkalmazás legújabb verzióját futtatják. A terminálszolgáltatások ügyfele az RDC (Remote Desktop Connection – Távol asztali kapcsolat). Az RDC használatához csak a távoli számítógép nevét kell megadni és a Csatlakozás gombra kattintani. Az alábbi ábra egy távoli számítógéphez történő kapcsolódást szemléltet az RDC használatával:



A beállításokon belül, a Minőség fülnél van lehetőség arra, hogy megadjuk a kapcsolat sebességét, és a távoli munkamenethez nem szükséges összetevőket kiiktathatjuk. Amikor egy intelligens kártya vagy egy port átirányítására kérés érkezik, akkor a rendszer egy biztonsági figyelmeztetést jelenít meg. Ilyenkor a felhasználó letilthatja az adott átirányítást, vagy pedig a kapcsolatot megszakíthatja. A Terminálszolgáltatások engedélyezése a Programok telepítése és törlése varázsló segítségével történik. Itt a Terminálkiszolgáló komponenst kell hozzáadni, ahogy a következő ábra is mutatja:



IX. A hálózati kapcsolatok újdonságai

IX.1. Frissített csoportházirend a hálózati és a telefonos kapcsolatokhoz

A Windows XP Professional vagy a Windows Server 2003 rendszerrel ellátott számítógéppel dolgozó felhasználók számára a hálózati összetevőket meghatározó csoportházirend adható meg. A rendszergazdák felvehetik a felhasználókat a Hálózatbeállítási felelősök csoportba,

amelynek tagjai hozzáférhetnek a hálózati kapcsolatok TCP/IP-beállításaihoz, és saját IP-címeket állíthatnak be. Ha egy felhasználói fiók a helyi Rendszergazdák csoportjának a tagja, akkor az adott felhasználó engedélyezheti az internetkapcsolat tűzfalát, az internetkapcsolat megosztása szolgáltatást, és a hálózati kapcsolatok beállításait.

IX.2. PPPoE a szélessávú internetkapcsolatokhoz

A PPPoE protokoll és egy szélessávú internetkapcsolat segítségével, a helyi hálózatot használók, egyedi hitelesített hozzáférést kaphatnak a nagysebességű adathálózatokhoz. Korábban egy külön szoftvert kellett ehhez telepíteniük a felhasználóknak. A Windows Server 2003 rendszernek ez a szolgáltatás már beépített összetevője.

X. Hálózati topológia tervezése

X.1. A Windows Server 2003 és a hálózati infrastruktúra

Egy hálózati infrastruktúra fizikai és logikai összetevőknek egy halmaza, amelyek biztosítják az összekapcsolhatóságot, a biztonságot, a forgalomirányítást (routing), az irányítást, a hozzáférést, és más beépített jellegzetességeket egy hálózaton.

X.1.1. Fizikai infrastruktúra

Egy hálózat fizikai infrastruktúrája a hálózat felépítése (topológiája), a hardver-komponensekkel együtt, mint például vezetékelés, routerek, switch-ek, hub-ok, szerverek és munkaállomások. A hálózat fizikai infrastruktúrájának tervezésekor kiválasztott hardvert gyakran a logikai infrastruktúra határozza meg.

X.1.2. Logikai infrastruktúra

Egy hálózat logikai infrastruktúrája sok szoftver összetevőből áll, amelyek a hálózaton a hosztokat összekapcsolják, kezelik és védelmezik. A logikai infrastruktúra a számítógépek közötti kommunikációt biztosítja, a fizikai topológián keresztül.

X.1.3. Hálózati infrastruktúra tervezése

Egy hálózat infrastruktúrájának megtervezésekor, a hálózat tervezőjének figyelembe kell vennie a hálózat felhasználóinak, a tulajdonosoknak és a hardver és szoftver összetevőknek a követelményeit. A tervezőnek minden veszélyt fel kell ismernie, amelyek a hálózatot fenyegethetik, és egy alkalmas biztonságos infrastruktúrát kell terveznie.

X.1.4. Hálózati infrastruktúra megvalósítása

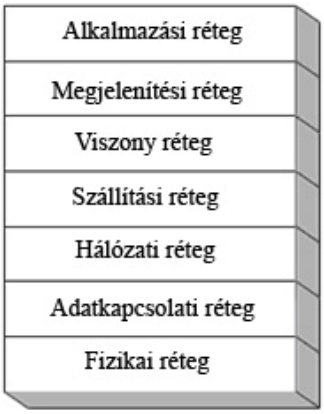
A hálózati kábelek beállítása mellett, az operációs rendszer és más szoftverösszetevők telepítése is a hálózati infrastruktúra implementálásának a része.

X.1.5. Hálózati infrastruktúra karbantartása

A hálózati infrastruktúra karbantartása magába foglalja az operációs rendszerek és alkalmazások frissítését, folyamatok felügyeletét, és a hibakeresési problémákat.

X.2. Az OSI referencia modell

1984-ben a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization – ISO) közzétett egy dokumentumot, amely az adathálózat funkcióit hét rétegbe osztotta föl. A következő ábra ezt a hét réteget szemlélteti:



Fizikai réteg: A fizikai réteg definiálja a hálózati közeg, és a továbbított jelek tulajdonságait.

Adatkapcsolati réteg: Az adatkapcsolati réteg definiálja a hálózati közeg és a számítógépen futó szoftver közötti interfészt. Ehhez a réteghez tartozik a fizikai címzés, hálózati topológia, közeghozzáférés, fizikai átvitel hibajelzése és a keretek sorrendhelyes kézbesítése. Az adatkapcsolati réteg két alrétegre osztható:

- *Logikai kapcsolatvezérlő (LLC)*: melynek feladata a hibaellenőrzés, keretszinkronizáció, és a folyamatvezérlés.
- *Közeghozzáférési vezérlés (MAC)*: a hálózati illesztőkártyák (NIC) közötti adatcsomagok mozgását vezérli.

Hálózati réteg: A hálózati réteg összeköttetést biztosít két hálózati csomópont között. Ehhez a réteghez tartozik a hálózati címzés és az útvonalválasztás (routing).

Szállítási réteg: A szállítási réteg megbízható hálózati összeköttetést létesít két csomópont között. Ez a réteg felelős a virtuális áramkörök kezeléséért, az átviteli hibák felismeréséért és javításáért, valamint az áramlásszabályozásért.

Viszonyréteg (Session): A viszonyréteg építi ki, kezeli és fejezi be az alkalmazások közötti párbeszédeket.

Megjelenítési réteg: A megjelenítési réteg felel a különböző csomópontokon használt különböző adatstruktúrákból származó információ-értelmezési problémák megoldásáért.

Alkalmazási réteg: Az alkalmazási réteg az alkalmazások működéséhez nélkülözhetetlen szolgáltatásokat biztosítja. Ilyen alkalmazás lehet például az állománytovábbítás, elektronikus levelezés. Ez a réteg széles körben igényelt protokollokat tartalmaz.

Egy hálózat fizikai interfészének tervezésekor a legfontosabb döntés a megfelelő adatkapcsolati réteg protokoll kiválasztása. Ez nemcsak az adatkapcsolati réteg feladataiért felelős, hanem meghatározza a hálózat fizikai rétegének megvalósítását is.

X.3. A hálózati/szállítási réteg protokollok kiválasztása

A Windows Server 2003 a következő három hálózati/szállítási réteg protokoll kombinációt támogat:

- TCP/IP
- IPX (Internetwork Packet Exchange)
- NetBIOS

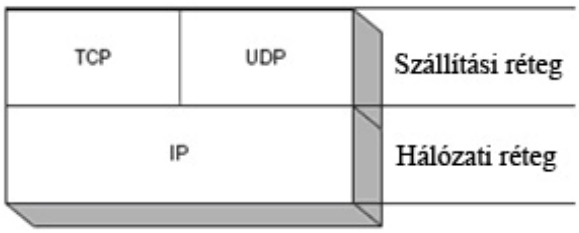
A TCP/IP és az IPX, protokollok gyűjteménye.

X.3.1. TCP/IP használata

A TCP/IP protokollok egy kollekciója, mely gondoskodik a hálózatkezelési szolgáltatásokról. Egyedül a TCP/IP biztosítja azt, amit a legtöbb hálózat megkövetel: a rugalmasságot, a kiterjeszthetőséget, és az internet kompatibilitást. A TCP/IP az 1970-es években fejlesztették ki a csomagkapcsoló hálózatok támogatására. A protokollokat hardverfüggetlen módon tervezték meg, mert nagyon sokféle típusú számítógépből állt ez a hálózat. A TCP/IP két elsődleges protokollja az Internet Protokoll (IP), és az átvitelvezérlő protokoll (TCP – Transmission Control Protocol). Van még egy másik szállítási réteg protokoll, ez pedig a

felhasználói adatcsomag protokoll (UDP – User Datagram Protocol). A TCP/IP a hálózati rétegben az IP protokollt használja, a szállítási rétegben pedig vagy a TCP-t vagy pedig az UDP-t.

A következő ábra a TCP/IP hálózati és szállítási réteg protokollokat szemlélteti:



Az adott alkalmazás követelményeitől függően használja a hálózati kommunikációs folyamat az IP-t TCP-vel vagy UDP-vel.

A TCP egy kapcsolatorientált protokoll, tehát mielőtt két számítógép kommunikálna egymással, azelőtt üzeneteket váltanak a kapcsolat stabilizálása érdekében a két gép között.

A TCP a következő funkciókat látja el:

- Garantálja az IP-datagramok kézbesítését
- Elvégzi a programok által küldött nagy adatblokkok szegmentálását és újraegyesítését
- Biztosítja a szegmentált adatok megfelelő rendezését és rendezett kézbesítését
- Ellenőrzőösszeg-számításokkal vizsgálja az átvitt adatok sértetlenségét
- Pozitív visszajelző üzeneteket küld, ha sikerült az adatok kézbesítése. A szelektív visszaigazolás használatával az adatátvitel sikertelensége esetén negatív visszaigazoló üzenetet küld.

Az UDP pedig egy kapcsolat nélküli protokoll, tehát itt nincs szükség a kapcsolat stabilizálására. Az UDP nem garantálja a datagramok kézbesítését és a végrehajtási sorrend ellenőrzését.

X.3.2. Az IPX használata

Az IPX protokollt a Novell fejlesztette ki saját NetWare operációs rendszerükhöz. 1998-ig - a NetWare 5-ös verziójának megjelnéséig - a számítógépek az IPX protokollt használták a NetWare szerverekkel való kommunikáció során. Az IPX szabványokat a Novell nem tette elérhetővé a szoftverfejlesztők számára. Ennek eredményeképpen a Microsoft kifejlesztette a saját IPX protokollját, amit NWlink-nek neveztek el. Ez tette lehetővé, hogy a Windows

operációs rendszereket összekapcsolassák a NetWare operációs rendszerrel. A Windows Server 2003 is támogatja az NWLink protokoll használatát, melynek neve NWLink IPX/SPX/NetBIOS kompatibilis átviteli protokoll.

Az IPX számos különböző protokollból áll. Az IPX maga a hálózati réteg protokoll, az SPX pedig a TCP/IP TCP-jének megfelelő szállítási réteg protokoll. Az UDP megfelelője a NetWare Core Protocol (NCP). Az IPX 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 kapja, illetve küldte a csomagot. Az IPX és a TCP/IP protokollok közötti alapvető különbség az, hogy az IPX protokoll csak helyi hálózatokra (LAN) lett tervezve, míg a TCP/IP protokoll bármilyen méretű és bármilyen típusú hálózatokat képes támogatni.

X.3.3. A NetBEUI használata

A NetBEUI volt az alapértelmezett hálózati protokollja a Windows NT 3.1 operációs rendszernek. Kezdetben a hálózatok viszonylag kicsik voltak és egy helyre összpontosultak. A NetBEUI a NetBIOS névteret használja a hálózaton lévő számítógépek azonosítására, amelyet később a DNS névterek váltanak fel. A NetBEUI nem egy programcsomag, hanem egy nagyon egyszerű hálózati protokoll, amely az alapvető fájlmegosztást biztosítja a Windows operációs rendszerrel ellátott számítógépek számára. A NetBEUI nem igényel semmilyen beállítást. Nem biztosítja az internet kapcsolódást. A NetBEUI kis helyi hálózatokra lett tervezve, és nem alkalmas nagy vállalati hálózatok kezelésére.

X.4. TCP/IP hálózati infrastruktúra tervezése

X.4.1. IP címek hozzárendelése

Két lehetőség közül lehet választani. Vagy minden számítógépet manuálisan kell beállítani, vagy pedig DHCP segítségével. A DHCP (Dynamic Host Configuration Protocol) egy automatizált konfigurációs szolgáltatás, amellyel a Windows Server 2003 és sok más operációs rendszer is rendelkezik.

X.4.2. TCP/IP kliensek kézi konfigurálása

Egy Windows operációs rendszerrel ellátott számítógépet nem nehéz kézzel beállítani, de amikor már több száz, vagy ezer számítógépről van szó, akkor már nagyon nehéz megfelelően konfigurálni a rendszert. Nem csak az a probléma, hogy minden egyes számítógéphez oda kell külön-külön menni és beállítani, hanem minden egyes számítógéphez egy olyan IP-címet kell rendelni, ami alkalmas az adott alhálózathoz, amelyben a számítógép található, és egyik IP-címet sem lehet többször felhasználni a rendszerben.

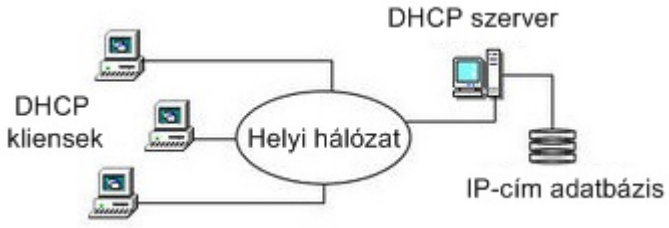
X.4.3. A DHCP használata

A DHCP szerver egy klienshez hozzárendel egy IP-címet, amelyet egy előzetesen meghatározott érvényességi tartományból vesz, egy bizonyos időre. Ha egy IP-címet hosszabb időre kérnek, mint az előre beállított idő, akkor a kliensnek egy kiterjesztést kell kérnie, mielőtt lejár a címbérlet időtartama. Ha a kliens nem kéri a címbérleti idő alatt a bérleti idő meghosszabbítását, akkor az adott IP-cím szabadon felhasználható egy másik kliens azonosítására. Ha a felhasználó meg szeretné változtatni az IP-címét, akkor a következő két parancsot kell begépelnie a parancssorba:

1) ipconfig /release (ezzel eltávolítja az aktuális IP-címet)
2) ipconfig /renew (ezzel pedig egy új IP-címet igényel)

A lefoglalások a DHCP szerveren vannak meghatározva. Az IP-címeket hozzá lehet rendelni vagy egy fizikai címhez, vagy pedig egy hoszt nevéhez. Ebben az esetben ezek a kliensek fix IP-címmel rendelkeznek.

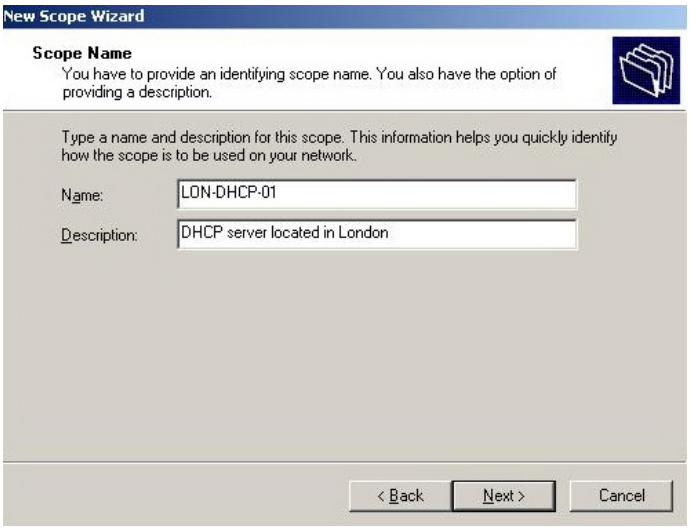
A következő ábra a DHCP szerver elhelyezkedését mutatja egy hálózatban:



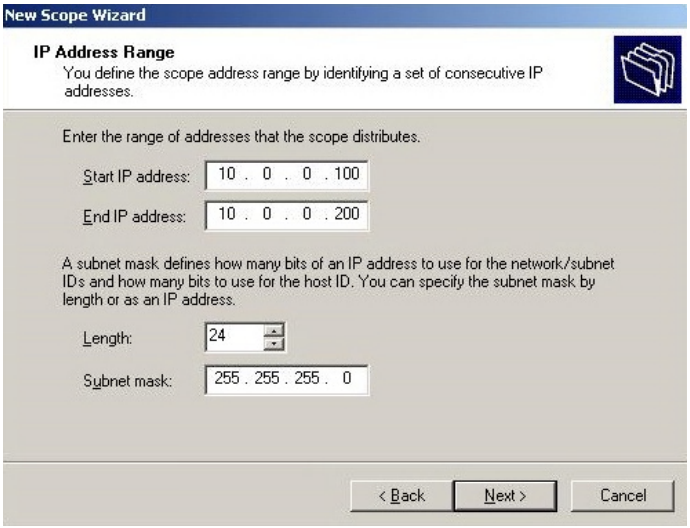
A DHCP szerver tartalmazza az IP-címadatbázist, amely nyilvántartja az összes használatban lévő IP-címet. Ha egy felhasználónak a TCP/IP protokoll tulajdonságainál, engedélyezve van az IP-cím automatikus kérése, akkor a DHCP szervertől elfogadja az IP-címet.

X.4.4. DHCP szerver beállítása a Kiszolgáló konfigurálása varázslóval

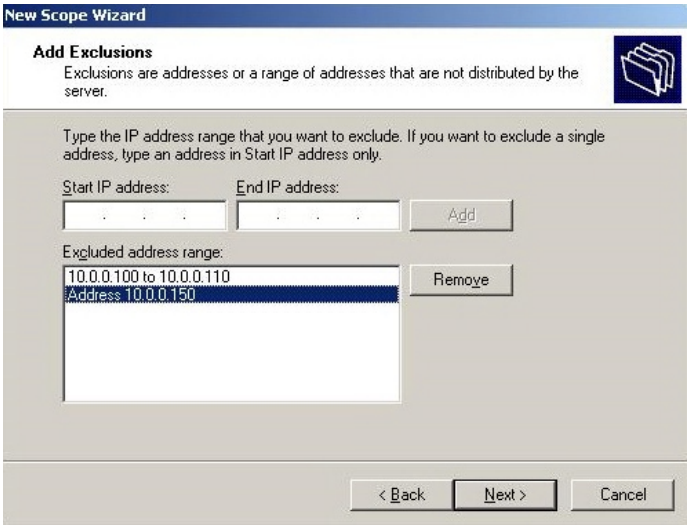
1) A varázsló elindítása után, a Kiszolgálói szerepkör lapon, válasszuk ki a DHCP-kiszolgáló elemet, majd kattintsunk a Tovább gombra. Ezután elindul az Új hatókör varázsló. Itt kell megadni a létrehozandó hatókör nevét és leírását.



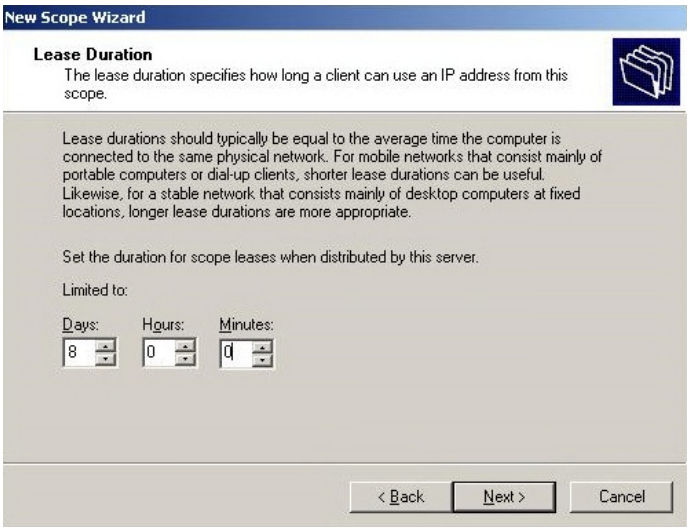
2) Az IP-címtartomány lapon meg kell adni a hatókör IP-címtartományát, azaz a tartomány kezdő és záró IP-címét. A varázsló automatikusan megállapítja a megadott cím alapján a helyes alhálózati maszkot. Ha ettől az alhálózati maszktól eltérőre van szükségünk, akkor azt be kell írni az Alhálózati maszk mezőbe, vagy pedig a Hossz mezőben állítsuk be az alhálózati maszk bitjeinek a számát.



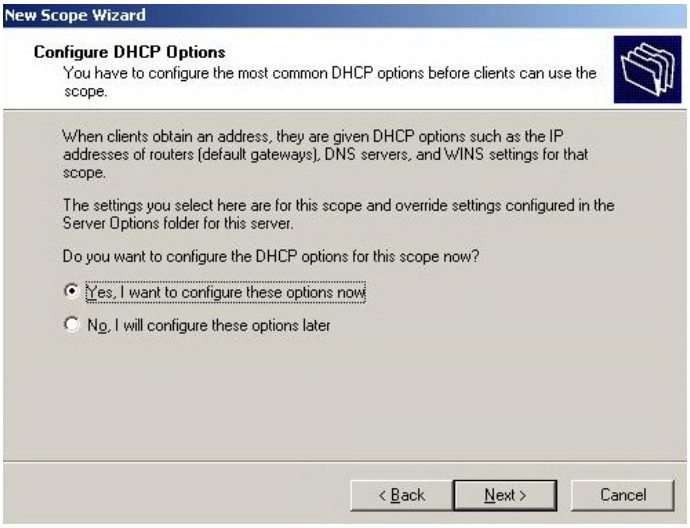
3) A Kizárások hozzáadása lapon lehet azokat az IP-címeket megadni, amelyeket a DHCP-kiszolgáló nem oszthat ki a kliensek számára. A DHCP-kiszolgálónak statikus IP-címmel kell rendelkeznie, amelyet nem szabad kiosztania más klienseknek. Lehetnek más eszközök is a hálózatban, amelyeknek szintén statikus az IP-címük, például hálózati nyomtatók. Ezeket az IP-címeket ki kell zárni, hogy a DHCP-kiszolgáló ne oszthassa ki őket. A kizárást a tartomány elejéről vagy végéről érdemes megtenni.



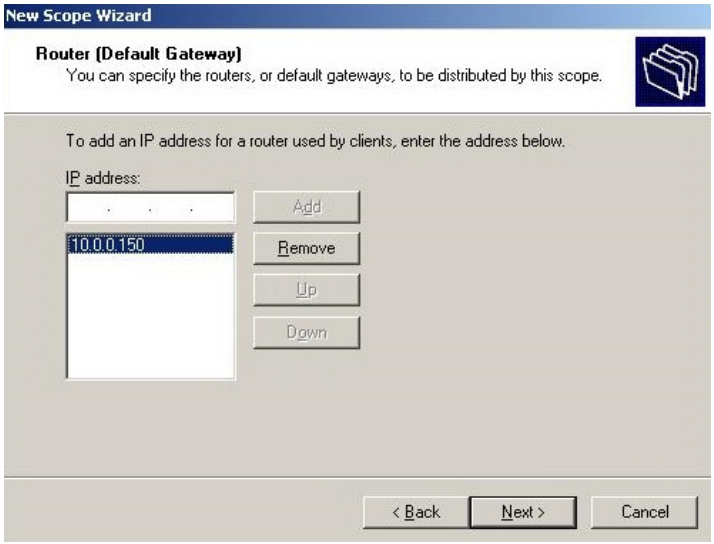
4) A Címbérlet élettartama lapon lehet megadni, hogy a kliensek milyen hosszú ideig használhatják a hatókör IP-címeit. A címbérlet meghatározott idő múlva lejár. Ahhoz, hogy a kliens tovább tudja használni az adott IP-címet, meg kell újítani a címbérletet. A címbérlet alapértelmezett élettartama nyolc nap.



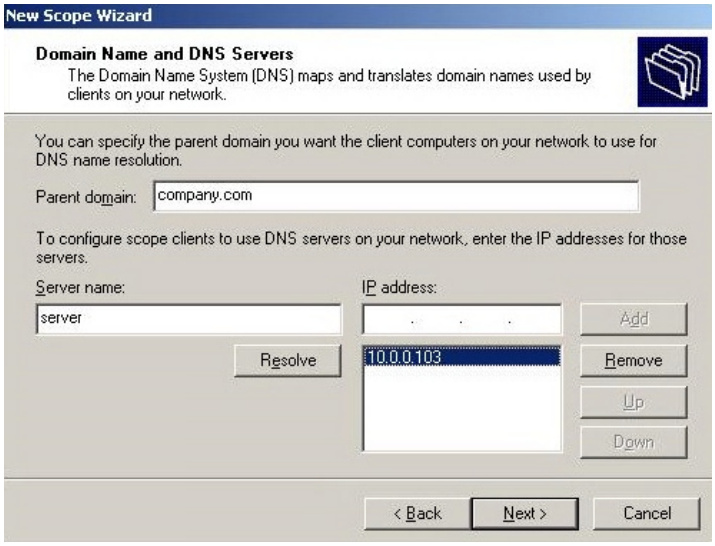
5) Ezután a DHCP-beállítások konfigurálása lapon kiválaszthatjuk, hogy akarjuk-e konfigurálni a DHCP-beállításokat. A javaslat az, hogy konfiguráljuk a DHCP-t, mert ha nem konfiguráljuk, akkor ugyan a varázsló létrehozza a hatókört, de nem aktiválja azt, ezért a DHCP-konzol segítségével kell aktiválni a hatókört ahhoz, hogy a kliensek a hatókörbe tartozó IP-címekből kaphassanak.



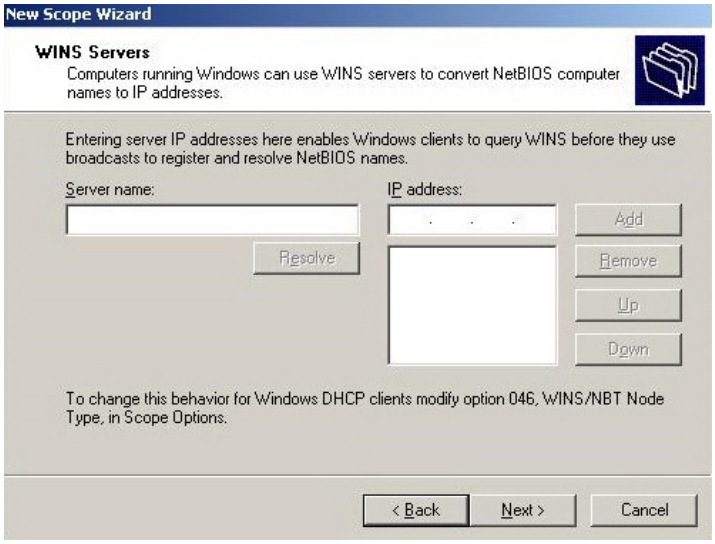
6) Az Útválasztó (Alapértelmezett átjáró) lapon lehet megadni azokat az útválasztókat, amelyeket a klienseknek kell használniuk. Itt az alhálózat összes útválasztójának IP-címét meg lehet adni.



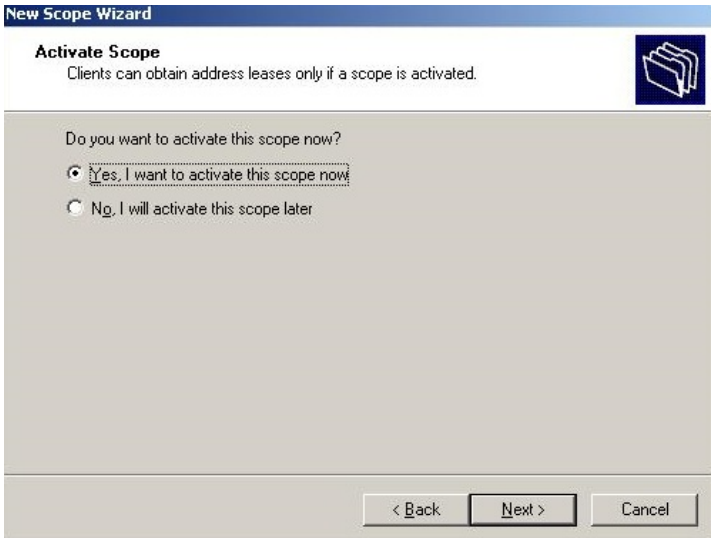
7) A Tartománynév- és DNS-kiszolgálók lapon lehet megadni annak a tartománynak a nevét, amelyet az alhálózatban lévő klienseknek kell használniuk a DNS-nevek feloldásakor.



8) A WINS-kiszolgálók lapon lehet megadni azt a WINS-kiszolgálót, amellyel a klienseknek a NetBIOS-nevek regisztrálása és feloldása során kommunikálniuk kell. Meg lehet adni a WINS-kiszolgáló IP-címét, vagy a nevét. Ha a nevét adjuk meg, akkor a Feloldás gombra kattintva, a varázsló meghatározza a kiszolgáló IP-címét. Egyszerre több WINS-kiszolgálót is meg lehet adni.



9) A Hatókör aktiválása lapon lehet a hatókört aktiválni. Ha itt nem aktiváljuk, akkor később a DHCP-konzolon lehet ezt megtenni. Ahhoz, hogy a hatókör alhálózatában található kliensek megkapják az IP-címeket a DHCP-kiszolgálóktól, aktiválni kell a hatókört.



XI. Kiszolgálói szerepkörök

A Windows Server 2003 termékcsalád számos kiszolgálói szerepkört tartalmaz. A kiszolgálói szerepkörök a Kiszolgáló konfigurálása varázslóval telepíthetők, és a Kiszolgáló kezelése eszközzel kezelhetők.

XI.1. Fájlkiszolgálói szerepkör

Kényelmes és központi hozzáférést biztosít a fájlok és könyvtárak eléréséhez az egyéni felhasználók, osztályok, és a teljes szervezet számára. Ezzel a szolgáltatással lehetőség nyílik a felhasználó lemezterületének kezelésére, a lemezkvóta engedélyezésével és konfigurálásával. Az indexelő szolgáltatás engedélyezésével pedig hatékonyabbá lehet tenni a fájlrendszerben történő keresést.

XI.2. Nyomtatókiszolgálói szerepkör

A kliens számítógépek számára a megosztott nyomtatók és a nyomtatókhoz szükséges meghajtóprogramok biztosításával, központosított és irányított hozzáférést biztosít a nyomtatókhoz. Ezt a szerepkört a Nyomtató hozzáadása varázslóval lehet beállítani. A varázsló segítségével fel lehet telepíteni a nyomtatókat, az Internet Information Services-t (IIS 6.0), beállítja az Internet Printing Protocol-t (IPP), és telepíti a web-alapú nyomtató adminisztrátori eszközöket.

XI.3. Alkalmazáskiszolgálói szerepkör (IIS, ASP.NET)

Nélkülözhetetlen infrastruktúrát és szolgálatokat biztosít a rendszeren lévő alkalmazásoknak. Egy tipikus alkalmazás-kiszolgáló néhány szolgáltatása lehet például:

- Erőforrás-készletezés
- Programok közötti aszinkron kommunikáció biztosítása (üzenetsor-kezelés)
- Feladatátvételi és az alkalmazások állapotát észlelő szolgáltatások

A Windows Server 2003 termékcsalád alkalmazás-kiszolgálója biztosítja az XML-webszolgáltatások, webalkalmazások és elosztott alkalmazások fejlesztését, bevezetését és

futás közbeni felügyeletét segítő funkciókat is. A kiszolgáló alkalmazás-kiszolgálóként történő beállítása során a rendszer telepíti az Internet Information Services (IIS) szolgáltatást. Az IIS a dinamikus hálózati eszközök közötti erős kommunikációs platform megteremtésére szolgáló eszköz. Ezen kívül más technológiák és szolgáltatások is telepíthetők (COM+, ASP.NET). A COM+ a COM (Component Object Model) kiterjesztése. Könnyebbé teszi a fejlesztők számára a szoftverkomponensek tetszőleges nyelven történő létrehozását és használatát, tetszőleges fejlesztői eszköz használatával.

Az ASP.NET egy egységes webfejlesztői platform, amely biztosítja a fejlesztőknek a vállalati szintű webalkalmazások létrehozásához szükséges szolgáltatásokat. Az ASP.NET új programozási modellje és infrastruktúrája nagyobb biztonságot és méretezhetőséget kínál, valamint olyan stabil alkalmazásokat, amelyek tetszőleges böngészőből, illetve eszközből elérhetők.

XI.4. Levelezőkiszolgálói szerepkör (POP3, SMTP)

Segítségével e-mail-szolgáltatás biztosítható a felhasználók számára. A POP3-szolgáltatás segítségével tárolni és kezelni lehet a levelező-kiszolgálón található e-mail fiókokat. Engedélyezni lehet, hogy a felhasználók POP3 protokollt támogató e-mail ügyfélprogrammal (például a Microsoft Outlook) kapcsolódjanak a levelező-kiszolgálóhoz, és letöltsék róla a leveleiket.

XI.5. Terminálkiszolgálói szerepkör

Egy Windows Server 2003 operációs rendszerrel ellátott számítógépen a terminálkiszolgálói szerepkörrel biztosítható, hogy az egy helyre telepített alkalmazáshoz több felhasználó is hozzáférjen. A felhasználók ugyanúgy használhatják a hálózati erőforrásokat, futtathatják a programokat és menthetik a fájlokat, mintha azok a saját számítógépükre lennének telepítve. Ezzel a szerepkörrel lehet biztosítani, hogy minden felhasználó ugyanazt a programverziót használhassa.

XI.6. Távelérési/virtuális magánhálózati (VPN) kiszolgálói szerepkör

Útválasztási szolgáltatást nyújt helyi hálózati (LAN) és nagy kiterjedésű hálózati (WAN) környezetek számára. Lehetővé teszi a távoli és utazó alkalmazottak számára a vállalati

hálózatnak a közvetlen kapcsolattal egyenértékű elérését, telefonos hálózati szolgáltatáson vagy a VPN-kapcsolattal az interneten keresztül. A távkapcsolatok segítségével minden olyan szolgáltatás használható, amely általában a LAN-hoz kapcsolódó felhasználók számára elérhető (például a fájl- és nyomtatómegosztás, a webkiszolgáló elérése). Meg lehet határozni, hogy a távoli felhasználók mikor és hogyan érhetik el a hálózatot. Ezzel a szerepkörrel hálózati címfordítási (NAT) szolgáltatások is biztosíthatók a hálózat számítógépei részére.

XI.7. Tartományvezérlői szerepkör (Active Directory)

A tartományvezérlők címtáradatokat tárolnak, kezelik a felhasználók és tartományok közötti kommunikációt. Az Active Directory tárolja a felhasználói fiókok adatait (nevek, jelszavak, telefonszámok, stb.), és biztosítja ugyanazon hálózat hitelesített felhasználói számára, hogy hozzáférjenek a tárolt információkhoz.

XI.8. DNS-kiszolgálói szerepkör

A DNS-szolgáltatás lehetővé teszi, hogy a hálózat ügyfélszámítógépei felhasználóbarát DNS-neveket regisztráljanak, és azokat feloldják.

XI.9. DHCP-kiszolgálói szerepkör

A DHCP (Dynamic Host Configuration Protocol) egy olyan TCP/IP-szabvány, amely csökkenti a címkonfigurációk felügyeleti feladatainak összetettségét. A DHCP-kiszolgálói szerepkör segítségével az IP-címeket és az azokhoz tartozó információkat központilag lehet kezelni. A DHCP segítségével kiküszöbölhető a címütközés.

XI.10. Adatfolyam-kiszolgálói szerepkör

Ez a szerepkör biztosítja a Windows Media Services (WMS) szolgáltatást, amely Windows Media-formátumú tartalom kezelését, továbbítását és archiválását végzi, intraneten és interneten egyaránt. Valósidejű adatszolgáltatást tesz lehetővé.

XI.11. WINS-kiszolgálói szerepkör

A Windows Internet Name Service (WINS) kiszolgálók az IP-címek és a NetBIOS-számítógépnevek, illetve a NetBIOS-számítógépnevek és az IP-címek közötti megfeleltetést végzik. A WINS-kiszolgálói szerepkör beállításával az IP-cím helyett a számítógépnév alapján is felkutathatók az erőforrások.

XI.12. Kiszolgálói szerepkörök az Active Directory-ban

A tartományon belül kiszolgálóként működő számítógépek tartományvezérlők vagy tagkiszolgálók lehetnek. A tartományon kívüli kiszolgáló önálló-kiszolgálók.

XI.12.1. Tartományvezérlők

A tartományvezérlők vagy a Windows 2000 Server, vagy a Windows Server 2003 termékcsalád valamelyik rendszerét futtatják. Az Active Directory-t használják a tartományi adatbázis írható-olvasható másolatának tárolására, részt vesznek a több főkiszolgálós replikációban, és hitelesítik a felhasználókat. A tartományvezérlők címtáradatokat tárolnak, valamint felhasználók és tartományok közötti kapcsolatokat kezelnek, többek között bejelentkezési eljárásokat, hitelesítéseket és címtárakban történő kereséseket. A tartományvezérlők több főkiszolgálós replikációval szinkronizálják a címtáradatokat, folyamatosan biztosítva ezzel az adatok konzisztenciáját.

XI.12.2. Tagkiszolgálók

A tagkiszolgálók is vagy a Windows 2000 Server, vagy a Windows Server 2003 termékcsalád valamelyik rendszerét futtatják. A tagkiszolgálók nem tartományvezérlők, és tartományhoz tartoznak. A tagkiszolgálók nem dolgozzák fel a fiókbejelentkezéseket. A tagkiszolgálók általában az alábbi típusú kiszolgálókként működnek: fájlkiszolgálók, alkalmazás-kiszolgálók, adatbázis-kiszolgálók, webkiszolgálók, tanúsítvány-kiszolgáló, tűzfal vagy távelérés-kiszolgáló.

XII. Active Directory

A Windows Server 2003 termékcsalád tartalmazza az Active Directory szolgáltatást. Az Active Directory tartalmazza a könyvtárat, amely információkat tárol a hálózati erőforrásokról, valamint az összes szolgáltatást, amely elérhetővé és használhatóvá teszi az információkat.

Az Active Directory címtárszolgáltatás a következő rendszereket futtató kiszolgálókra telepíthetők: Windows Server 2003 Standard Edition, Enterprise Edition és Datacenter Edition. Az Active Directory a hálózati objektumokra vonatkozó adatokat tárol, és egyszerűen hozzáférhetővé és felhasználhatóvá teszi azokat a rendszergazdák, valamint a felhasználók számára. A címtáradatokat logikusan, hierarchikusan lehet rendszerezni, az Active Directory strukturált adattárolása segítségével. A rendszergazdák egyetlen bejelentkezéssel kezelhetik a címtáradatokat a teljes hálózaton, a hitelesített hálózati felhasználók pedig a hálózaton bárhol hozzáférhetnek az erőforrásokhoz.

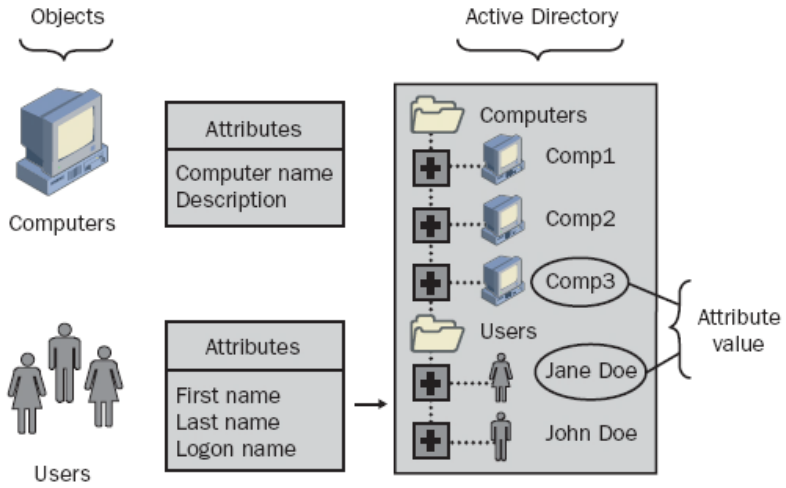
XII.1.Az Active Directory szolgáltatás jellemzői

- Központosított adattárolás
- Skálázhatóság
- Bővíthetőség
- Kezelhetőség
- DNS-integráció
- Kliens konfiguráció kezelése
- Információ replikációja
- Rugalmas, biztonsági hitelesítés és azonosítás
- Biztonság integrálása
- Együttműködés más könyvtár-szolgáltatással
- Titkosított LDAP forgalom

XII.2.Active Directory objektumai

Az adatok, mint például információk a felhasználókról, nyomtatókról, szerverekről, adatbázisokról, csoportokról, számítógépekről, és biztonsági elvekről, az Active Directory-ban vannak tárolva, objektumok formájában. Egy *objektum* egy egyedi névvel ellátott

attribútum halmaz, amely egy hálózati erőforrást reprezentál. Az *objektumtulajdonságok* az objektumok jellegzetességei a könyvtárban. Vannak olyan objektumok, amelyek más objektumokat tartalmaznak, ezeket *konténerek*nek nevezzük. A következő ábra egy példát mutat be, amelyben a két konténer objektum a Computers és a Users



XII.3.Az Active Directory sémája

A séma határozza meg az Active Directory-ban tárolható objektumokat. A séma, definíciók egy listája, amely meghatározza az Active Directory-ban tárolható objektumok fajtáját és az objektumokról tárolható információk típusát. A sémák is objektumok, ezért ugyanolyan módon lehet tárolni őket az Active Directory-ban, mint a többi objektumot. A következő két objektumtípussal van definiálva a séma:

- sémaosztály
- séma-attribútum

A ***sémaosztály*** a lehetséges Active Directory objektumokat írja le. Egy sémaosztály mintaként szolgál az új Active Directory objektumok létrehozásához. Minden sémaosztály, séma-attribútumoknak egy gyűjteménye. Egy sémaosztály létrehozásakor, a séma-attribútumok tárolják azt az információt, ami meghatározza az objektumot. Az Active Directory minden objektuma, egy sémaosztálynak a példánya.

A ***séma-attribútum*** meghatározza a sémaosztályt, amivel azokra lehet következtetni. Minden séma-attribútumot csak egyszer kell definiálni, és több sémaosztályban lehet felhasználni őket.

A tapasztalt fejlesztők és hálózati adminisztrátorok dinamikusan kiterjeszthetik a sémát úgy, hogy új osztályokat és attribútumokat definiálnak, a már meglévő sémához. A séma bővítésére lehetőség van grafikus felhasználói felületen (GUI) keresztül, parancssori eszközökkel, és parancsfájlokkal. Legkönnyebben az Active Directory-séma beépülő modul segítségével módosítható a séma, amely a Microsoft Management Console (MMC) segédprogramban található grafikus sémakezelési eszköz. A parancsfájllal történő módosításhoz az Active Directory Service Interfaces (ADSI) szolgáltatás ismerete, valamint programozási ismeretek szükségesek.

XII.4.Active Directory komponensei

Egy szervezetet az Active Directory komponensek két részre osztanak:

- logikai struktúra
- fizikai struktúra

Az Active Directory teljesen elkülöníti a logikai struktúrát a fizikai struktúrától.

A ***logikai struktúrát*** a következő Active Directory komponensek reprezentálják:

- tartományok
- szervezeti egységek (OUs)
- fák
- erdők.

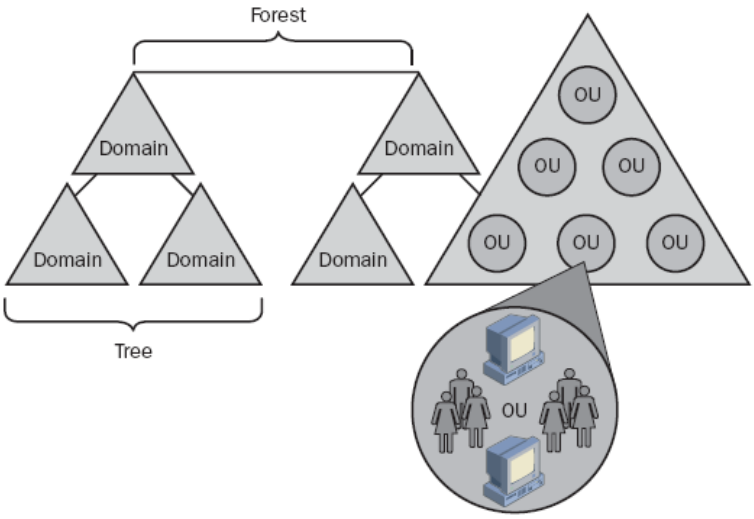
A ***fizikai struktúrát*** pedig a következő komponensek reprezentálják:

- helyek (fizikai alhálózatok)
- tartomány-vezérlők.

XII.4.1. Logikai struktúra

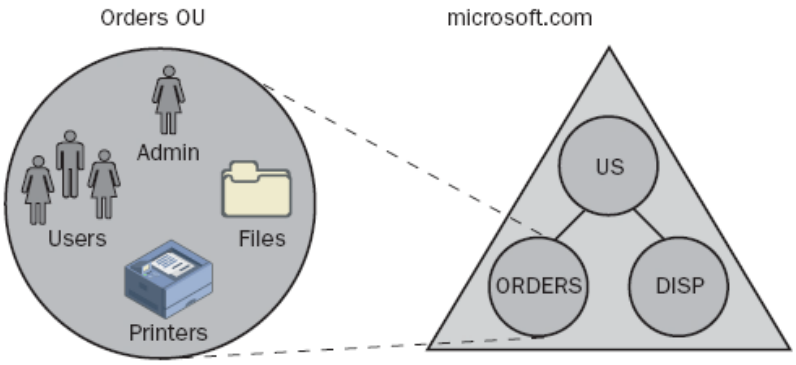
Az Active Directory-ban az erőforrásokat egy logikai struktúrába lehet szervezni, a domain-ek, a szervezeti egységek, a fák, és az erdők felhasználásával. Ez lehetővé teszi, hogy könnyen megtaláljunk egy erőforrást a neve alapján anélkül, hogy emlékezni kellene a fizikai elhelyezkedésére. A logikai struktúrának köszönhetően az Active Directory átláthatóvá teszi a hálózat fizikai struktúráját a felhasználók számára.

A következő ábra az Active Directory komponensei közötti kapcsolatot mutatja be.

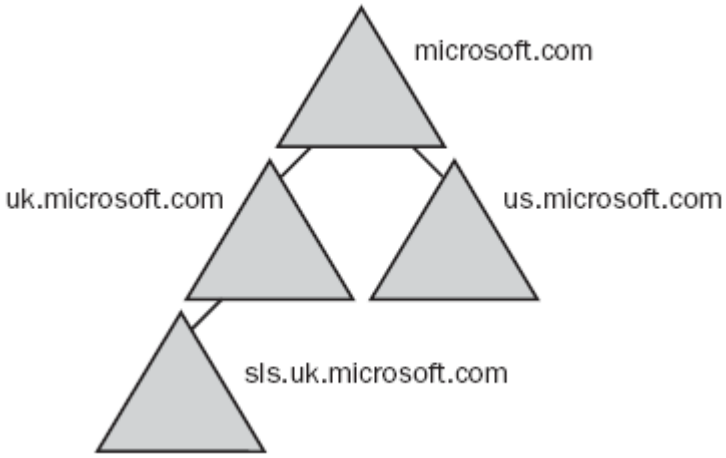


Tartományok (Domains): A logikai struktúra magját az Active Directory-ban a tartományok alkotják, amelyek több millió objektum tárolására képesek. Az egy tartományban tárolt objektumok létfontosságúak a hálózat számára. Minden hálózati objektum egy tartományban van, és minden egyes tartomány csak az általa tartalmazott objektumokról tárol információt. A tartomány objektumaihoz való hozzáférést, a hozzáférési lista (Access Control List – ACL) szabályozza.

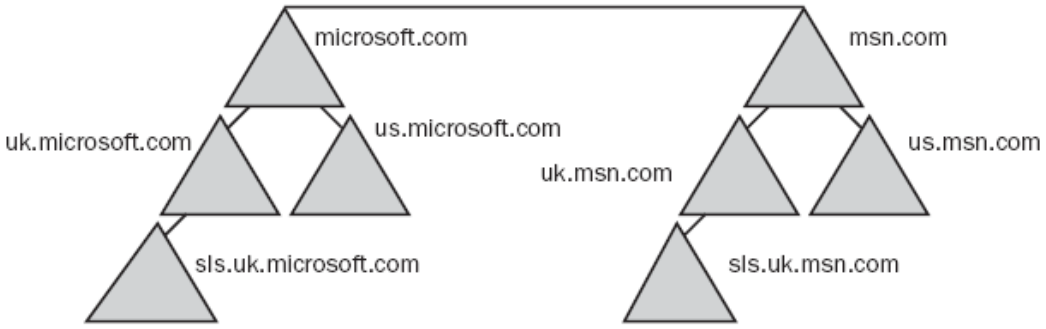
Szervezeti egységek (OUs): A szervezeti egységek az Active Directory szolgáltatás tárolói, amelyekbe felhasználókat, csoportokat, számítógépeket, illetve más szervezeti egységeket lehet elhelyezni. A szervezeti egységek más szervezeti egységeket is tartalmazhatnak.



Fa (Tree): Egy fa, egy vagy több Windows Server 2003 tartomány csoportosítása vagy hierarchikus elrendezése, amelyet úgy hozunk létre, hogy egy vagy több gyerek tartományt adunk egy szülő tartományhoz. Tehát a fa, tartományoknak egy hierarchiája. Egy gyermek tartomány neve a szülőhöz képest relatív név.



Erdő (Forest): Egy erdő, egy vagy több elkülönített, teljesen független fáknak egy csoportosítása, vagy hierarchikus elrendezése. Az erdő egy vagy több olyan tartomány, amely közös sémával és globális katalógussal rendelkezik. Az erdő biztonsági és felügyeleti határt jelent az erdőn belül elhelyezkedő objektumok számára. Az azonos erdőhöz tartozó fák nem alkotnak összefüggő névteret, tehát a DNS-neveik nem alkotnak folytonos sorozatot.



XII.4.2. Fizikai struktúra

Az Active Directory fizikai komponensei a helyek és a tartományvezérlők. Ezekkel egy könyvtár struktúrát lehet létrehozni, amely a szervezet fizikai struktúráját fejezi ki. A helyek és a tartományok abban különböznek egymástól, hogy a helyek a hálózat fizikai felépítését, míg a tartományok a szervezet logikai szerkezetét követik.

Helyek (Sites): Az Active Directory-ban a *hely* nagy sebességű hálózat, például helyi hálózat (LAN) által jó összeköttetéssel rendelkező számítógépek csoportja. Egy hely egy vagy több IP-alhálózatból áll. Az alhálózatok az IP-hálózat részegységei, ahol minden egyes alhálózat

saját egyedi hálózati címmel rendelkezik. A helyek és alhálózatok az Active Directory-ban hely- és alhálózati objektumként jelennek meg.

Tartományvezérlők (Domain Controllers): Egy tartományvezérlő, olyan Windows Server 2003 operációs rendszert futtató számítógép, amely tárolja az Active Directory adatbázisának egy másolatát. Minden egyes tartományvezérlő, az adott tartománynak, egy teljes másolatát tárolja az Active Directory összes információjáról, és kezeli az információknak a változását.

Globális katalógus: Egy katalógus-szolgáltatás a kiválasztott információkat tartalmazza az Active Directory összes tartományának minden objektumáról. Ez nagyon hasznos a keresések végrehajtásakor. A *globális katalógus* az Active Directory által támogatott katalógus-szolgáltatás.

A globális katalógus egy fa vagy erdő objektumaira vonatkozó információk központi gyűjteménye. A globális katalógus automatikusan jön létre a kezdeti tartományvezérlőn, az első tartományban. Azt a tartományvezérlőt, amely a globális katalógus egy másolatát tartalmazza, globális katalógus kiszolgálónak nevezzük. Bármelyik tartományvezérlő kijelölhető globális katalógus kiszolgálónak. A globális katalógus címtárszerepkörei a következők:

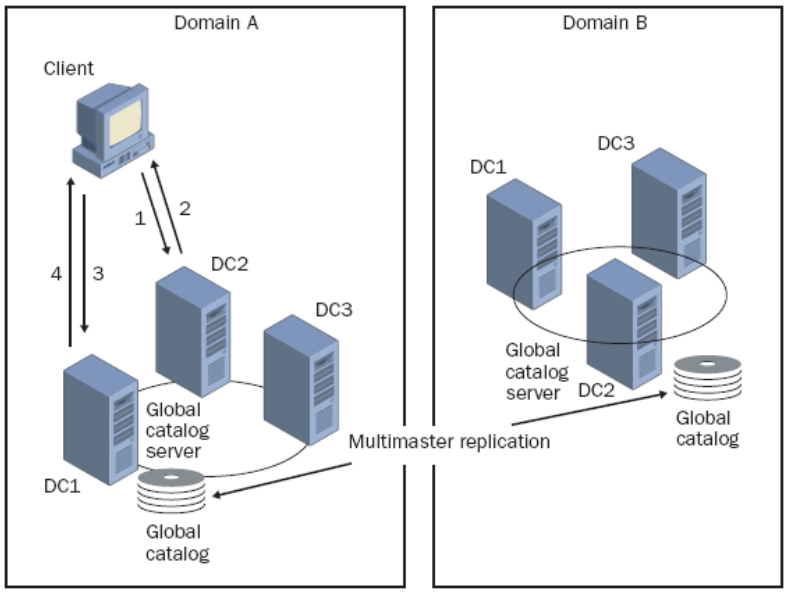
- Egyszerű felhasználónév hitelesítése
- Erdőn belüli objektumhivatkozások érvényesítése
- Univerzális csoporttagság-adatok szolgáltatása több tartományból álló környezetben
- Objektumok keresése

Amikor egy felhasználó bejelentkezik a hálózatba, a globális katalógus általános csoporttagság információt szolgáltat a felhasználói fióknak. Ha a hálózatban több tartományvezérlő található, akkor az egyik tartományvezérlő tartalmazza a globális katalógust. Ha egy felhasználó bejelentkezési folyamatának megkezdésekor egyik globális katalógus sem érhető el, akkor a felhasználó csak a helyi számítógépre tud bejelentkezni kivéve, ha a hely (site) speciálisan lett beállítva.

A globális katalógust arra tervezték, hogy objektumokra vonatkozó felhasználói és programozási lekérdezésekre reagáljon bárhol a fában vagy erdőben, maximális sebességgel és minimális hálózati forgalommal. Mivel egy egyedüli globális katalógus az erdő összes tartományában lévő összes objektumáról tartalmaz információkat, egy olyan objektumra vonatkozó lekérdezés, amelyet nem tartalmaz a helyi tartomány, feloldható egy globális katalógus szerver által.

A lekérdező folyamat: Egy lekérdezés egy speciális felhasználói kérés a globális katalógusra, abból a célból, hogy a felhasználó az Active Directory-ból adatot keressen vissza, módosítson, vagy töröljön.

A következő ábra szemlélteti a lekérdezési folyamatot:



A folyamat lépései:

1) A felhasználó DNS szerver segítségével meghatározza a globális katalógus szerver helyét.
2) A DNS szerver keresi a globális katalógus szerver helyét, és visszaadja annak a tartományvezérlőnek az IP-címét, amelyiket a globális katalógus szervernek jelölt ki.
3) A felhasználó lekérdezi a globális szervernek kijelölt tartományvezérlő IP-címét. A lekérdezés a tartományvezérlő 3286-as portjára lett elküldve. (a normál Active Directory kérések a 389-es portra érkeznek).
4) A globális katalógus szerver feldolgozza a kérést. Ha a globális katalógus tartalmazza a keresett objektumot, akkor válaszol a felhasználónak. Ha a globális katalógus nem tartalmazza a keresett objektumot, akkor a kérés az Active Directory-ra hivatkozik.

Replikáció: Az Active Directory a címtáradatok replikáit több tartományvezérlőn tárolja, ezáltal minden felhasználónak biztosítja a címtár elérhetőségét. Az Active Directory több főkiszolgálós replikációs modellt használ, azaz bármely tartományvezérlő fogadja és

replikálja a címtárváltozásokat. A replikáció a globális katalógus elérését is biztosítja a teljes erdőben.

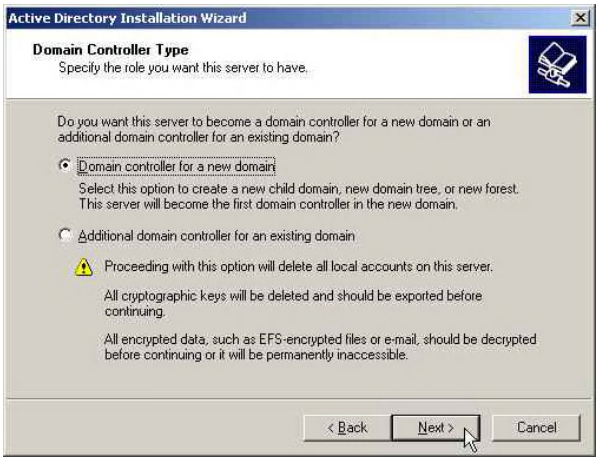
XII.5. Az Active Directory telepítése

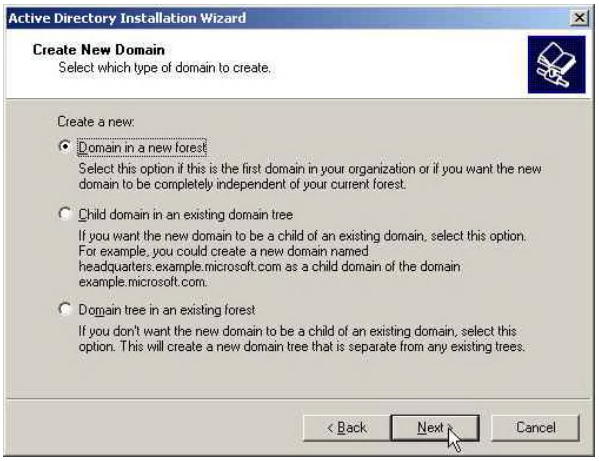
Az Active Directory telepítésének megkezdése előtt a következőket kell előkészíteni:

- A tartomány struktúrájának kialakítása
  - A fizikai környezet meghatározása
  - Az erdő gyökérkönyvtárának meghatározása
  - A tartományok számának meghatározása
  - Tartomány hierarchia definiálása
- Tartománynév meghatározása
- Az adatbázis és a log fájlok helyének meghatározása
- A DNS beállításának meghatározása
- Statikus IP-cím meghatározása a szervernek és egy DNS szerver kijelölése.

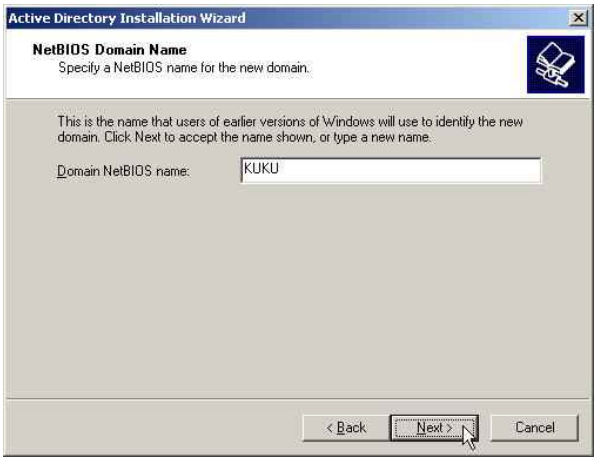
XII.5.1. Az Active Directory telepítése varázsló segítségével

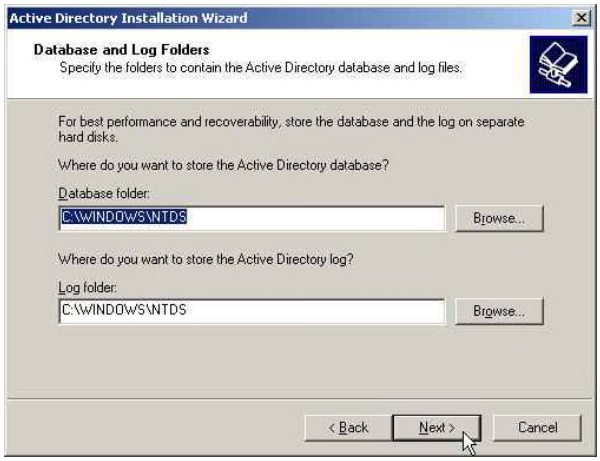
A varázsló elindítása a DCPROMO.EXE parancs begépelésével (Start menü → Futtatás) lehetséges. A varázsló segítségével telepíthetjük az Active Directory szolgáltatást. A varázsló lépéseit a következő ábrák szemléltetik:

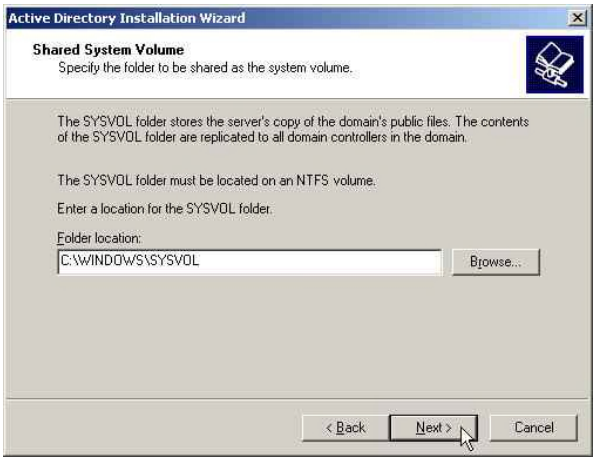


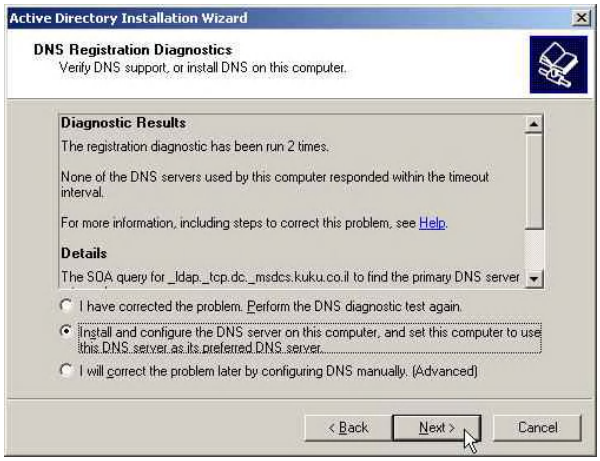



Active Directory Installation Wizard
New Domain Name
Specify a name for the new domain.
Type the full DNS name for the new domain.
(for example: headquarters.example.microsoft.com).
Full DNS name for new domain:
kuku.co.il
< Back
Next >
Cancel

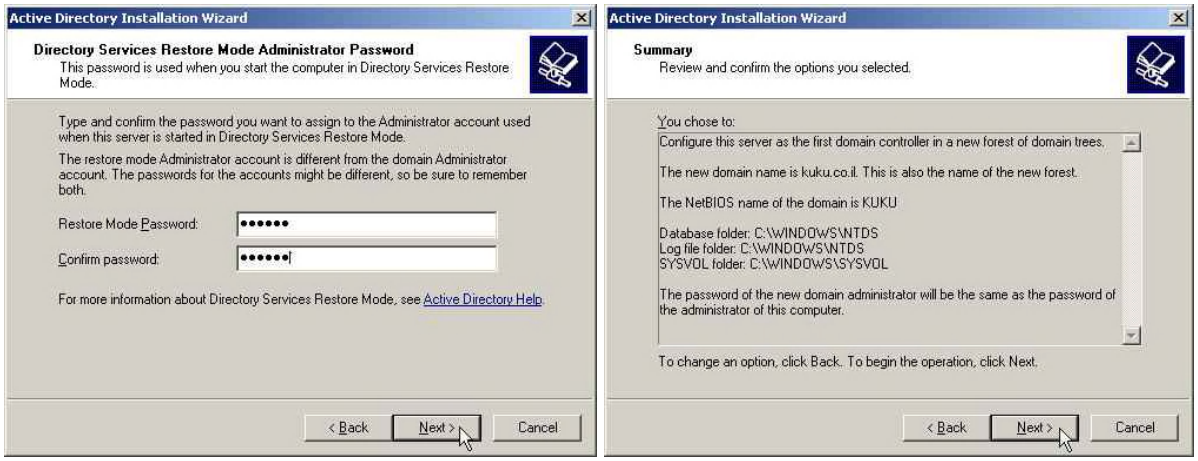

Active Directory Installation Wizard
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.
Domain NetBIOS name:
KUKU
< Back
Next >
Cancel


Active Directory Installation Wizard
Database and Log Folders
Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:\WINDOWS\NTDS
Browse...
Where do you want to store the Active Directory log?
Log folder:
C:\WINDOWS\NTDS
Browse...
< Back
Next >
Cancel


Active Directory Installation Wizard
Shared System Volume
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Folder location:
C:\WINDOWS\SYSVOL
Browse...
< Back
Next >
Cancel


Active Directory Installation Wizard
DNS Registration Diagnostics
Verify DNS support, or install DNS on this computer.
Diagnostic Results
The registration diagnostic has been run 2 times.
None of the DNS servers used by this computer responded within the timeout interval.
For more information, including steps to correct this problem, see Help.
Details
The SOA query for _ldap._tcp.dc._msdcs.kuku.co.il to find the primary DNS server
I have corrected the problem. Perform the DNS diagnostic test again.
Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.
I will correct the problem later by configuring DNS manually. (Advanced)
< Back
Next >
Cancel


Active Directory Installation Wizard
Permissions
Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain.
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< Back
Next >
Cancel



XII.5.2. Active Directory telepítése Answer fájl segítségével

Lehetőségünk van erre a telepítési módra is. Létrehozhatunk egy ún. answer fájlt. A telepítés során feltett kérdésekre tartalmazza a válaszokat. Minden olyan paramétert tartalmaznia kell, amely fontos az Active Directory varázsló számára ahhoz, hogy a szolgáltatást telepíteni tudja. Answer fájl segítségével történő telepítéshez a következő parancsot kell beírni a parancssorba:

DCPROMO /ANSWER:*answer_fájl_neve*

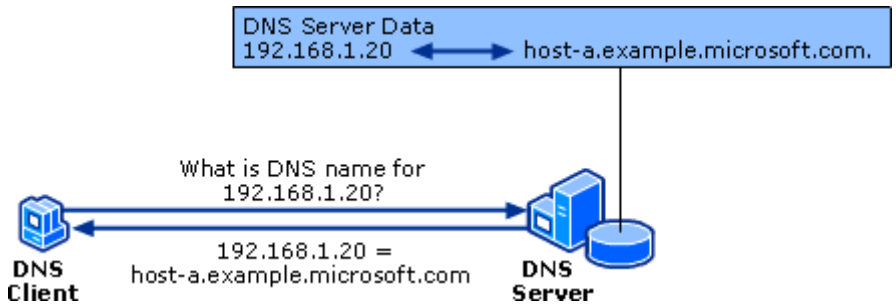
XII.5.3. Active Directory telepítése a Kiszolgáló konfigurálása varázslóval

Ez a varázsló a Kiszolgáló kezelése képernyőről érhető el. A Kiszolgáló konfigurálása varázslóval csak akkor lehet az Active Directory-t telepíteni, ha az adott számítógép az első kiszolgáló a hálózaton, és még nem volt konfigurálva. A szokásos telepítés és beállítás folyamata az alábbi lépésekből áll:

- Az Active Directory telepítése és a számítógép előléptetése tartományvezérlővé
- A DNS telepítése és a hálózat teljes tartománynevének létrehozása
- A DHCP-kiszolgáló szolgáltatás telepítése
- Statikus IP-cím hozzárendelése
- Alhálózati maszk hozzárendelése (a varázsló alapértelmezés szerint a 255.255.255.0 alhálózati maszkot rendeli a számítógéphez)
- Az Útválasztás és távelérés szolgáltatás telepítése
- Elsődleges DNS-kiszolgáló kijelölése

XIII. A DNS

A DNS (Domain Name System), olyan rendszer, amely számítógépek és hálózati szolgáltatások elnevezésére szolgál, és tartományok hierarchikus struktúrájából áll. A DNS-t TCP/IP-hálózatokon alkalmazzák (pl.: internet). A DNS működését a következő ábra szemlélteti:



XIII.1. A DNS komponensei

XIII.1.1. DNS kiszolgálók

Egy DNS kiszolgáló egy olyan számítógép, amely egy DNS kiszolgáló programot futtat. A DNS kiszolgálók egy DNS adatbázist tartalmaznak, amely információval szolgál a DNS tartomány struktúrájáról, és névfeloldást végez a DNS-ügyfél által küldött lekérdezésre. Egy ilyen lekérdezésre a DNS kiszolgáló vagy tud válaszolni, vagy egy olyan másik szolgáltatót javasol, amelyik tud válaszolni a lekérdezésre, vagy pedig azt mondja, hogy az információ nem elérhető vagy nem létezik.

XIII.1.2. DNS zónák

A DNS lehetővé teszi a DNS-névtér felosztását zónákra. A zónák egy vagy több DNS-tartományról tárolnak névinformációkat. A jobb elérhetőség érdekében egynél több DNS-kiszolgálóról is elérhetők a zónák a hálózaton. Egyetlen kiszolgáló használata esetén sikertelen lehet a névlekérdezés, ha a kiszolgáló nem válaszképes. A Windows Server 2003 rendszerrel működő DNS-kiszolgálók esetében a DNS-szolgáltatás támogatja a növekményes zónaletöltést. A *növekményes zónaletöltésnél* csak a módosított erőforrásrekordok letöltése történik meg. Ezáltal kisebb hálózati forgalom generálható, és a zónaletöltések is gyorsabban hajtódnak végre.

XIII.1.3. Erőforrásrekordok

Az erőforrásrekordok a DNS adatbázis bejegyzései, amelyek segítségével lehet megválaszolni a DNS-ügyfelek lekérdezéseit. Minden egyes erőforrásrekordnak egy jól meghatározott formátuma van. A formátumok a következő mezőkből állnak: tulajdonos, élettartam (TTL), osztály, típus és rekordfüggő adatok.

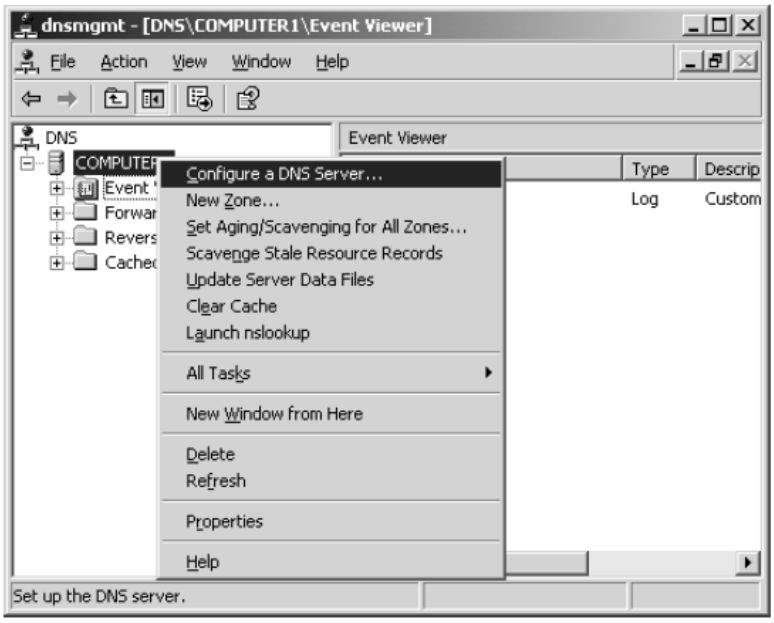
XIII.2. DNS kiszolgáló telepítése

Egy Windows Server 2003 operációsrendszerrel ellátott számítógépre csak úgy lehet feltelepíteni a DNS kiszolgáló szolgáltatást, hogy a kiszolgáló szerepkörei közé felvesszük a DNS kiszolgálói szerepkört. A szerepkör hozzáadása után a Felügyeleti eszközök programcsoportban megjelenik a DNS konzol. A DNS konzol segítségével lehet konfigurálni és felügyelni a DNS kiszolgálókat, zónákat, tartományokat és az erőforrásrekordokat.

DNS kiszolgáló telepítésének lépései:

1. A Windows Server 2003 telepítő CD-t a meghajtóba kell tenni
2. Ellenőrizni kell, hogy statikus IP-cím van–e a számítógéphez rendelve
3. Start menü → Kiszolgáló kezelése
4. Szerepkör hozzáadás és eltávolítása
5. A megjelenő lépések végrehajtása, majd Következő
6. A megfelelő kiszolgálói szerepkör kiválasztása, majd Következő
7. A Kijelölések összegzése oldalon erősíthetjük meg a kiválasztott beállításokat, majd Következő
8. A DNS kiszolgáló konfigurálásához el kell fogadni az alapértelmezett beállításokat, és ezután befejeződik a DNS kiszolgáló konfigurálása varázsló.

A következő ábra a DNS konzol elindítása után jelenik meg. Itt lehetőség van az adott DNS kiszolgáló konfigurálására, új zóna létrehozására, és egyéb műveletek elvégzésére.



Összefoglalás

Azokat a szolgáltatásokat, amelyeket egyszerre több munkaállomás is használ hálózati környezetben, célszerű különálló kiszolgáló számítógépekre bízni. A szerverek használatának előnyei között szerepel, a központosított konfiguráció és adatkezelés, hatékony felhasználó és jogosultságkezelés. Lehetőség van távoli felügyeleti eszközök alkalmazására, amennyiben a szerver internetes hozzáférése biztosított. Ezenkívül a szolgáltatásokhoz való távoli hozzáférés is biztosítható VPN segítségével, így biztonságos kapcsolaton keresztül távolról elérhetőek a céges dokumentumok, alkalmazások, és egyéb megosztott erőforrások.

Dolgozatomban ismertettem a Windows Server 2003 számtalan fontos szolgáltatásai közül azokat, amelyek a legtöbb hálózatban megjelennek. Dolgozatom célja a hálózatüzemeltetés főbb momentumainak, a Windows Server 2003 által támasztott lehetőségek által történő bemutatása volt. Remélem, hogy a felvonultatott szolgáltatások és technikák hasznosak voltak az olvasó számára.

Irodalomjegyzék

Jill Spealman, Kurt Hudson:

Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory 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

Dan Holme and Orin Thomas:

Managing and Maintaining a Microsoft Windows Server 2003 Environment (Training Kit) , Microsoft Press 2004

Kathy Ivens:

The Complete Reference Windows Server 2003, The McGraw-Hill Companies 2003

http://www.microsoft.com/en/us/default.aspx

http://technet.microsoft.com/hu-hu/windowsserver/2003/default(en-us).aspx

http://www.windowsnetworking.com/

Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Dr. Krausz Tamásnak a szakmai irányításért és a dolgozatom megírásához szükséges források biztosításáért, továbbá a felmerülő szakmai kérdésekre adott válaszaiért.