Debreceni Egyetem
Informatikai Kar

A WINDOWS SERVER 2003 HÁLÓZATI MEGOLDÁSAI

Témavezető:
Dr. Krausz Tamás
Számítástechnikai munkatárs

Készítette:
Lakatos Csaba
Programozó matematikus

Debrecen
2006

Tartalomjegyzék

Bevezetés

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 hálózatokra kívülről csatlakozó partnerek, szállítók, és más üzletfelek számára biztosítani kell az alapvető erőforrások megfelelően hatékony elérését, kulcsfontosságú kérdésként kezelve a biztonságot.

A Microsoft Windows Server 2003 a Windows operációs rendszer fejlődésének következő lépcsőfoka. A Windows Server 2003 a Windows 2000 Server technológiáira épül, azokat tökéletesíti és korszerűsíti.
A Microsoft tökéletesítette a Windows 2000 Server során bevezetett technológiákat, például az Active Directory-címtárszolgáltatást, a kiszolgálófürtöket és a hálózati terheléselosztást. Új technológiákat is bevezetett, például a nyelvfüggetlen futtatórendszer, amely megvédi a hálózatokat a rosszindulatú vagy rosszul megtervezett programkódoktól. A Microsoft emellett az IIS 6.0 új és tökéletesített adatvédelmi szolgáltatásai, a nyilvános kulcsú titkosítási infrastruktúra (*Public Key Infrastructure*, PKI), a Kerberos hitelesítési protokoll, valamint az intelligens kártyák és a biometriai hitelesítés támogatásával nagy lépéseket tett a biztonság területén is.
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 továbbfejlesztett rendszerfelügyeleti- és tároló funkciói mind a rendszergazdák, mind a végfelhasználók számára nagyobb hatékonyságot biztosítanak. A Windows Server 2003 termékcsaládban a Microsoft jelentősen előrelépett a rendszerfelügyelet terén. Az új, feladatorientált működés megkönnyíti a mindennapi teendők elvégzését. A felügyeleti konzol (Microsoft Management Console, MMC) és az Active Directory fejlesztései növelik a hatékonyságot és megkönnyítik a rendszer felügyeletét. A Windows Server 2003 új felügyeleti lehetőségeket is bevezet: a tartományok átnevezését, az erdők közötti bizalmi kapcsolatot, a metacímtár-szolgáltatást (*Microsoft Metadirectory Services*, MMS) és az eredő házirend (*Resultant Set of Policy*, RSOP) kezelését. A

továbbfejlesztett WMI-szolgáltatók és parancssori eszközök az eddiginél részletesebb felügyeleti lehetőségeket biztosítanak a kiszolgálóoldali feladatok végrehajtása során.
A Windows Server 2003 új fájlkiszolgálói funkciói között találjuk a kötet-árnyékmásolat szolgáltatást (*Volume Shadow Copy Services*, VSS). Az árnyékmásolatok online biztonsági mentéseket tesznek lehetővé és segítségükkel a mentésekből a felhasználók saját maguk végezhetnek adat visszaállítást. Ezáltal nagymértékben csökken a rendszergazdák által elvégzendő munka. A WebDAV-alapú dokumentummegosztás segítségével a fájl- és nyomtatószolgáltatások is tovább fejlődtek. Az elosztott fájlrendszer és a titkosító fájlrendszer (*Encrypting File System*, EFS) továbbfejlesztései hatékony és rugalmas fájlmegosztást és tárolást tesznek lehetővé.
Az Enterprise Edition és a Datacenter Edition támogatja a nyomtatófürtöket is.

A Windows Server 2003 termékcsalád hálózati fejlesztései és új funkciói megnövelik a hálózati infrastruktúra sokoldalúságát, kezelhetőségét és megbízhatóságát. Lehetővé teszi, hogy a felhasználók tetszőleges helyről tetszőleges eszköz segítségével kapcsolódjanak a hálózati infrastruktúrához. A Microsoft fontos hálózati fejlesztéseket épített a Windows Server 2003-ba: például az IPv6-ot (*Internet Protocol version 6*), az Ethernet feletti pont-pont protokollt (*Point-to-Point Protocol over Ethernet*, PPPOE), az IPSec-et címfordításos hálózatok között (*NAT-Traverse*, NAT-T).

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.

A Microsoft a Windows Server 2003 rendszerben új adatvédelmi funkciókat vezet be, például az internetes tűzfalat (*Internet Connection Firewall*, ICF) és a szoftverkorlátozási házirendet. Az ICF szoftveres tűzfal védi és figyeli a hálózat, illetve az Internet határán keresztül bonyolított forgalmat. A szoftverkorlátozási házirend olyan mechanizmust biztosít, amellyel a rendszergazdák azonosíthatják a tartományhoz tartozó számítógépeken futó programokat, és szabályozhatják végrehajtásukat.

A Microsoft Windows Server 2003 termékcsalád bemutatása

A Microsoft Windows Server 2003 termékcsalád, a korábbi termékek nyomdokain haladva, elődeinél is megbízhatóbb, nagyobb teljesítőképességet és magasabb szintű összekapcsolhatóságot mutat. A Windows Server 2003 termékcsaládnak 4 tagja van.

A Windows Server 2003 termékcsalád tagjai:

- **Windows Server 2003, Standard Edition**: megbízható kiszolgáló operációs rendszer tetszőleges méretű vállalat mindennapi szükségleteinek kielégítésére. Optimális megoldást jelent a fájl- és a nyomtatómegosztáshoz, biztonságos internetkapcsolatok kialakításához, központosított irodai alkalmazások telepítéséhez, valamint az alkalmazottak, partnerek és ügyfelek hálózati környezetének kialakításához.
- **Windows Server 2003, Enterprise Edition**: A nagyvállalatok, valamint a kis- és közepes vállalkozások számára nyújt keretet biztonságos alkalmazások, webszolgáltatások, valamint infrastruktúra fejlesztésére és bevezetésére. Magasabb szintű megbízhatóságot, teljesítményt és kiváló üzleti értéket nyújtó operációs rendszer; 32- és 64-bites kiadásban is. A Windows 2000 Advanced Sercer utódja. Nagyobb a processzor és megmóriatámogatása, támogatja a fürtözést, és továbbfejlesztett tanúsítványkezeléssel rendelkezik.
- **Windows Server 2003, Datacenter Edition**: 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 elérhető. Ez a verzió csak egy meghatalmazott viszonteladó által szállított hardver/szoftver csomag részeként vásárolható.
- **Windows Server 2003, Web Edition**: Ez a változat weboldalak kiszolgálására a legalkalmasabb, de megőrzi mindazokat az alapfunkciókat, amelyek a fokozott megbízhatóságot, felügyeletet és biztonságot nyújtják.

A Windows Server 2003 termékcsalád rendszerkövetelményei				
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

A Windows Server 2003 termékcsalád által kihasználható legnagyobb hardver konfigurációja

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

A Windows Server 2003 R2 újdonságai

A Windows Server 2003 R2 továbbfejleszti a Windows Server 2003 operációs rendszert, hatékonyabb módszereket nyújt a helyi és a távoli erőforrások felügyeletére és elérésének szabályozására, ugyanakkor problémamentesen beépül a meglévő Windows Server 2003 környezetbe. A Windows Server 2003 R2 skálázható, fokozott biztonságú webplatformot biztosít, és újszerű alkalmazási módokra ad lehetőséget, például a távoli irodákban működő kiszolgálók felügyeletére, az identitás- és a hozzáférés-kezelés tökéletesítésére, valamint hatékonyabb tárolás-felügyeletre.

Windows Server 2003 R2 a Windows Server 2003 Service Pack 1 (SP1) fokozott biztonságosságának, megbízhatóságának és teljesítményének alapjaira építkezve a helyi és a távoli erőforrásokon is kibővíti a kapcsolódási és a szabályozási lehetőségeket. Előnyei közé tartozik a költségek csökkenése és a hatékonyság növekedése, ami abból ered, hogy a vállalat egészén belül javul az erőforrások felügyelete és szabályozása. Egyszerűbben felügyelhetők a más telephelyen működő kiszolgálók. A Windows Server 2003 R2 kiadással megőrizhető a más telephelyen működő kiszolgálók teljesítménye, rendelkezésre állása és termelékenységi előnye, ugyanakkor elkerülhetők az ilyen kiszolgálómegoldásokkal általában felmerülő problémák, például a korlátozott kapcsolódási lehetőségek és a felügyelettel járó többletterhelés.

A távoli irodákra is kiterjeszthető a kapcsolat és a megbízhatóság, és javulnak az ott működi infrastruktúra birtoklási összköltségének szabályozási lehetősége.

- Centralizáltabb felügyelet. Központilag használható felügyeleti eszközöket biztosít a fájl- és a nyomtatási funkciók kezelésére.
- Kevesebb helyi felügyelet. Minimalizálható a helyben szükséges felügyeleti és biztonsági mentési tevékenység.
- A WAN jobb kihasználása. Gyorsabban replikálhatók az adatok a nagykiterjedésű hálózatokon.

Az identitás- és hozzáférés-kezelés továbbfejlesztése

A Windows Server 2003 R2 tartalmazza az Active Directory Federation Services (ADFS) nevű szolgáltatást, amelynek az a rendeltetése, hogy segítséget nyújtson a rendszergazdáknak

az identitáskezelési problémák megoldásában azzal, hogy biztonságosabbá teszi a felhasználók identitásadatainak a biztonsági határokat átívelő megosztását. A Windows Server 2003 R2 lehetőséget nyújt a UNIX jelszavak szinkronizálására is, ezáltal könnyebben integrálhatók egymással a Windows és UNIX rendszerű kiszolgálók, mivel egyszerűbben lehet megteremteni a biztonságos jelszóhasználat feltételeit.

Sokoldalú webes platform. A Windows Server 2003 R2 révén a vállalkozások a webre is kiterjeszthetik infrastruktúrájukat, ugyanakkor csökkenthetik a fejlesztési és a felügyeleti költségeket azoknak az előrelépéseknek köszönhetően, amelyekhez a Windows Server 2003 SP1, az x64 kiadások, a Windows SharePoint Services, a .NET-keretrendszer 2.0-s és az Internet Information Services 6.0-s változata segíti hozzá őket.

- A Windows SharePoint Services költséghatékony csoportmunka-megoldást nyújt, amely gyorsan telepíthető és konfigurálható, könnyen felügyelhető.
- Az ASP.NET és a .NET-keretrendszer segítségével rövid idő alatt készíthetők sokoldalú, a Dinamikus Rendszer Kezdeményezés (Dynamic System Initiative - DSI) elveinek megfelelő webszolgáltatások és alkalmazások.
- Az IIS 6.0 biztonságosabb nagyteljesítményű webkiszolgáló.
- Az x64-támogatással olcsóbban érhető el jobb teljesítmény.

Megnöveli az Active Directory címtár nyújtotta értéket azzal, hogy a következő módszerekkel a szervezetek és a platformok határain átnyúló biztonságos hozzáférésre ad módot:

- **A felhasználók hatékonyságának növelése.** Az extraneten is használható webes egyszeri bejelentkezési funkció és az identitások összefogása révén a felhasználóknak kevesebb jelszót kell használniuk mind a belső, mind a partnerek által működtetett webalkalmazások eléréséhez.
- **Az informatikusok hatékonyságának növelése.** Az extranetes alkalmazásokhoz való hozzáférés központilag felügyelhető, kevesebbszer kell új jelszót megadni, a felhasználókezelési jogok átruházhatók a megbízható partnerekre.
- **Magától értetődő, igényen alapuló webhozzáférés-kezelés.** Az extranetes alkalmazások elérésének központi felügyelete.

- **Fokozott biztonság.** A felhasználók Active Directory-fiókjának letiltásával automatikusan „zárolható” az extranet elérése.
- **A jogszabályok pontosabb betartása.** Naplózható az, amikor a felhasználók külső biztonsági tartományban, partnerek által működtetett alkalmazásokat érnek el.

Jobb együttműködő-képesség a heterogén rendszerekkel. A webszolgáltatások átjárhatósági specifikációin alapuló, több platformot átfogó webes egyszeri bejelentkezés és az identitások összefogása, a Windows és a Network Information Service (NIS) szolgáltatást használó UNIX rendszerek felhasználói fiókjainak kezelésére és dinamikus frissítésére szolgáló eszközök, beleértve az automatikus jelszó-szinkronizálást a Windows és a UNIX operációs rendszer között

Extranetes alkalmazásszolgáltatások A Windows Server identitásszolgáltatásának értékét kiterjeszti az internettel kapcsolatban álló webes környezetekre is:

- Az Active Directory Federation Services segítségével erősebb védelmet nyújtó hitelesítési és egyszeri bejelentkezési szolgáltatást vehetnek igénye az extranetes alkalmazások.
- Decentralizált alkalmazási címtárszolgáltatások az Active Directory alkalmazási módjával
- Az extranetes alkalmazások elérhetőségének szerepkörön alapuló szabályozása a Hitelesítéskezelő segítségével

- A heterogén felhasználókezelési környezetek átjárhatóságának megteremtése az identitások összefogása révén, amely a webszolgáltatások (WS-Federation) támogatásának köszönhető.

TCP/IP

A TCP/IP nem más, mint egy protokollkészlet, amelyet arra dolgoztak ki, hogy hálózatba kapcsolt számítógépek megoszthassák egymás között az erőforrásaikat. Eredetileg az amerikai Védelmi Minisztérium részére készült. A fejlesztés őse az NCP (Network Control Protocol), ami az ARPANET-hez készült az USA-ban.

A TCP/IP protokollkészlet egymásra épülő rétegekből áll. Ennek szemléltetésére nézzünk egy példát. Tipikus hálózati feladat a levelezés megoldása, amit protokoll szabályoz. A protokoll az egyik gép által a másiknak küldendő parancsokat definiálja, például annak meghatározására, hogy ki a levél küldője, ki a címzett, majd ezután következik a levél szövege. A protokoll feltételezi továbbá, hogy a kérdéses két számítógép között megbízható kommunikációs csatorna létezik. A levelezés, mint bármely más alkalmazási rétegbeli protokoll, a küldendő parancsokat és üzeneteket definiálja. A tervezéskor a TCP/IP-t vették alapul, tehát azzal együtt használható. A TCP a felelős azért, hogy a parancsok biztosan eljussanak a címzetthez. Figyel arra, hogy mi került át, és ami nem jutott el a címzetthez, azt újraküldi. Amennyiben a küldendő adat túl nagynak bizonyul (meghaladja egy datagramm méretét), akkor azt a TCP széttördeli több datagrammra és biztosítja, hogy azok helyes sorrendben érkezzenek célba. Mivel a fenti szolgáltatást sok alkalmazás igényli, ezért ezeket nem a levelezés, hanem egy külön protokoll tartalmazza. Az egész TCP tulajdonképpen nem más, mint rutinok olyan gyűjteménye, amelyet a különböző alkalmazások vesznek igénybe, hogy megbízható hálózati kapcsolatot építsenek ki más számítógépekkel. A TCP hasonlóképpen alapul az IP szolgáltatásokon. Habár a TCP szolgáltatásait sok alkalmazás igényli, vannak olyanok, amelyeknek nincs rájuk szükségük. Persze léteznek olyan szolgáltatások, amelyeket minden alkalmazás megkíván. Ezeket szedték egybe az IP-be. Ugyanúgy, ahogy a TCP, az IP is egy rutingyűjtemény, de ezt a TCP-t nem használó alkalmazások is elérhetik. A különböző protokolloknak ezt a szintekbe rendezését rétegezésnek nevezik. Ennek megfelelően az alkalmazási programok (mint például a levelezés), a TCP, illetve az IP külön réteget alkotnak, amelyek mindegyike az alatta lévő réteg szolgáltatásait használja. A TCP/IP alkalmazások általában a következő négy réteget veszik igénybe:

- alkalmazási protokollok (pl. levelezés, DNS, FTP, HTTP, RIP);
- a TCP-hez hasonló protokollok, amelyek rengeteg alkalmazás számára biztosítanak szolgáltatásokat;

- IP, amely a datagrammok célba juttatását biztosítja;
- a felhasznált fizikai eszközök kezeléséhez szükséges protokollok (pl. Ethernet, Token Ring)

A TCP/IP alapjául az ún. "catenet" modell szolgált. Az alapfeltevés az, hogy nagyszámú különböző hálózat áll egymással összeköttetésben átjárók (gateway) segítségével. Ezeken a hálózatokon lévő bármely számítógépet vagy erőforrást a felhasználónak el kell tudnia érni. Az adatcsomagok esetleg több tucat hálózaton is keresztülmehetnek mielőtt a célállomásra érkeznének. Az ezt megvalósító útvonal-választásnak természetesen láthatatlannak kell maradnia a felhasználó számára, abból mindössze egy Internet címet kell, hogy ismerjen. Ez egy olyan számnégyes, mint például a 193.6.135.88, ami tulajdonképpen egy 32 bites számot reprezentál. A felírás 4 darab 8 bites decimális szám formájában történik. (Az Internet dokumentációkban a byte helyett az oktet kifejezést használják a 8 bites számokra. Ez azért van így, mert a TCP/IP-t olyan számítógépek is használják, amelyek architektúrájában a byte nem 8 bites számot jelöl.) A cím alapján kideríthető, hogy hogyan lehet a rendszerhez eljutni. A fenti példában a 193.6 egy olyan hálózati szám, amelyet egy központi felügyeleti szerv adott ki a Debreceni Egyetem számára. Az egyetem a következő oktetet a karok azonosítására használja. A 193.6.135 az egyetem Informatikai Karát jelöli. A negyedik, egyben az utolsó oktet maximum 254 rendszert azonosíthat minden esetben (azért 254, mert a 0 és a 255 nem megengedett értékek). Jelen esetben a infotech.inf.unideb.hu nevű szervergépet azonosítja. Az Internet cím szerkezetéről bővebben a névfeloldásnál ejtek szót.

A TCP/IP összeköttetés-mentes hálózati protokollokat tartalmaz, ami azt jelenti, hogy az információ a datagrammok sorozataként terjed tovább. A datagramm adatok együttese, amely egy egyszerű üzenetként kerül továbbításra. A datagrammok egymástól függetlenül, egyesével indulnak útjukra. A küldendő információt egy meghatározott szinten a protokollok a fenti adatokra tördelik, amelyeket aztán a hálózat egymástól teljesen különállóként kezel. Tegyük fel például, hogy egy 15000 oktet méretű állomány továbbításáról van szó. Mivel a legtöbb hálózat nem tud ekkora datagrammal mit kezdeni, ezért azt a protokollok mondjuk 30 darab 500 oktetes darabra szedik szét, amelyek mindegyikét elküldik a célállomásra. Ott aztán belőlük összerakják az eredeti 15000 oktetes állományt. A datagrammok adása közben a hálózaton semmi nem utal arra, hogy közöttük bármiféle kapcsolat is létezne; előfordulhat, hogy egy a sorrendben eredetileg hátrább álló megelőz egy előtte állót. Az is lehetséges, hogy

a hálózaton valahol hiba keletkezik, és néhányuk nem érkezik meg a rendeltetési helyére. Ilyenkor újra kell adni a hiányzó datagrammot.

A Windows Server 2003 termékcsaládban használatos TCP/IP protokoll a rendszer alapértelmezés szerint telepített összetevője, amely nem távolítható el (a protokoll a Hálózati kapcsolatok mappában található kapcsolatok tulajdonságai között szerepel, neve **TCP/IP protokoll**). A korábbiakban a TCP/IP-konfigurációval kapcsolatos hibák egyik megoldási módja a TCP/IP protokoll eltávolítása és újratelepítése volt. A Windows Server 2003 termékcsaládban ez már nem lehetséges. A TCP/IP-konfiguráció az új **netsh** paranccsal állítható vissza a rendszer telepítésekor érvényben lévő alapértékekre. A parancssorban használandó új netsh parancs a következő: **netsh interface ip reset**.

A TCP szint

A TCP/IP datagrammok kezelésében két különböző protokoll játszik szerepet. Az üzenetek széttördelését, összeállítását, az elveszett részek újraadását, a datagrammok helyes sorrendjének visszaállítását mind a TCP (transmission control protocol -- átvitelvezérlési protokoll) végzi. Az egyes datagrammok útvonalának a meghatározását (routing) az IP (internet protocol) hajtja végre. Mindez azt a látszatot kelti, hogy a munka tetemes része a TCP-re hárul. Kis kiterjedésű hálózatokban ez így is van, azonban az Interneten egy datagrammnak a rendeltetési helyre való juttatása igen összetett feladatot jelenthet. Egy datagramm több hálózaton mehet keresztül, míg végül eljut a célállomásra. A különböző átviteli közegekből adódó inkompatibilitások kezelése és a célállomásokhoz vezető útvonalak végigkövetése komplex feladat. Meg kell jegyezni azonban, hogy a TCP és az IP közti interfész rendkívül egyszerű: a TCP egy datagrammot ad át az IP-nek egy rendeltetési címmel együtt. Az IP semmit sem tud arról, hogy ez az információ hogyan viszonyul más datagrammokhoz. A TCP-nek még azt is tudnia kell, hogy az adott datagramm melyik kapcsolathoz tartozik. A probléma megoldását a demultiplexálás v. nyalábbontás néven ismert eljárás adja, amely a TCP/IP-ben valójában több különböző szinten folyik. A demultiplexáláshoz szükséges információt az úgynevezett fejlécek hordozzák. A fejléc azokat az extra okteteket jelenti, amelyeket a különböző protokollok ragasztanak a datagrammok elejére, hogy azokat nyomon tudják követni. A dolog hasonlít ahhoz, amikor a levelet a borítékba tesszük, majd azt megcímezzük. A különbség annyi, hogy a modern hálózatokban ez jóval többször történik: olyan mintha a levelet egy kis borítékba tennénk, majd azt a

titkárnőnk egy nagyobb borítékba helyezné, amit a központ egy még nagyobb borítékban továbbítana stb...

Az IP szint

A TCP az általa feldolgozott datagrammokat átadja az IP-nek. Persze ezzel együtt közölnie kell a rendeltetési hely Internet címét is. Az IP-t ezeken kívül nem érdekli más: nem számít, hogy mi található a datagrammban vagy, hogy hogyan néz ki a TCP fejléc. Az IP feladata abban áll, hogy a datagramm számára megkeresse a megfelelő útvonalat és azt a másik oldalhoz eljuttassa. Az útközben fellelhető átjárók és egyéb közbülső rendszereken való átjutás megkönnyítésére az IP a datagrammhoz hozzáteszi a saját fejlécét. A fejléc fő részei a forrás, és a rendeltetési hely Internet címe (32 bites címek, pl. 128.6.4.94), a protokollszám és egy ellenőrző összeg. A forrás címe a küldő gép címét tartalmazza. (Ez azért szükséges, hogy a vevő oldal tudja honnan érkezett az adat.) A rendeltetési hely címe a vevő oldali gép címét jelenti. (Ez pedig azért szükséges, hogy a közbenső átjárók továbbítani tudják az adatot.) A protokollszám kijelöli, hogy a datagramm a különböző szállítási folyamatok közül melyikhez tartozik. A TCP egy biztos választási lehetőség, de léteznek egyebek is (pl. UDP). Végül az ellenőrzőösszeg segítségével bizonyosodik meg a vevő oldali IP arról, hogy a fejléc az átvitel során nem sérült-e meg. A TCP és az IP különböző ellenőrzőösszegeket használ. Az IP-nek meg kell tudnia győződni a fejléc sértetlenségéről, különben rossz helyre küldhet el adatot. A TCP és az IP a biztonság és a hatékonyság növelése miatt tehát külön ellenőrző összegeket használ.

Az Ethernet szint

Manapság a legtöbb hálózat Ethernetet használ. A következőkben az Ethernet fejléccel foglalkozunk. Sajnos az Ethernetnek megvan a saját címzési módszere, mivel a létrehozók biztosítani akarták, hogy semelyik két gépnek se legyen ugyanaz az Ethernet címe. Azt is el akarták érni, hogy a felhasználónak ne kelljen a címek hozzárendelésével foglalkozni, ezért minden Ethernet vezérlő gyárilag beégetett címmel rendelkezik. Hogy ne kelljen egyetlen címet se újra kiosztani, a fejlesztők az Ethernet cím hosszát 48 bitben határozták meg. Az Ethernet vezérlőket gyártó cégeknek regisztráltatniuk kell magukat egy központnál, hogy biztosak legyenek abban: az általuk kiadott címek még nem léteznek. Az Ethernet ún. üzenetszórásos közeg, azaz olyan, mint egy „partivonal”. Az Ethernetre ültetett csomagot a

hálózaton lévő összes gép látja, ezért valami még hiányzik, hogy azt biztosan a megfelelő gép kapja meg. Nem nehéz kitalálni, hogy itt jelenik meg az Ethernet fejléc. Minden Ethernet csomagnak egy 14 oktetes fejléce van, amely a forrás- és a célgép címét, valamint egy típuskódot tartalmaz. A hálózaton lévő gépek csak az olyan csomagokat figyelik, amelyek célmezőjében a saját Ethernet címüket találjak. Vegyük észre, hogy az Ethernet címek és az Internet címek között nincs semmiféle kapcsolat. Minden számítógépnek van egy táblázata, amelyben felsorolja, hogy milyen Ethernet cím milyen Internet címnek felel meg. A címek mellett a fejlécben szerepel még egy típuskód is. Ennek segítségével ugyanazon a hálózaton többfajta protokollkészlet használata is lehetséges: TCP/IP, DECnet, Xerox, NS stb... Ezen protokollok mindegyike különböző értéket helyez a típus mezőbe. Végül ott az ellenőrzőösszeg, amelyet az Ethernet vezérlő az egész csomagra vonatkozóan számít ki. A vételkor a célgép Ethernet vezérlője is kiszámítja ezt az ellenőrzőösszeget, és ha a kettő nem egyezik, akkor eldobja a csomagot. Az ellenőrzőösszeg nem a fejlécbe, hanem a csomag végére kerül. A csomagok megérkezésekor persze a fejlécek mindegyikét leszedi a megfelelő protokoll. Az Ethernet interfész az Ethernet fejlécet és az Ethernet ellenőrzőösszeget szedi le. Ezekután ellenőrzi a típuskódot. Mivel az az IP-re mutat, ezért a datagrammot átadja az IP-nek, amely a Protokoll mező tartalmát ellenőrzi. Itt azt találja, hogy TCP, ezért a datagrammot a TCP-nek adja át. A TCP a Sorszám mező tartalma és egyéb információk alapján állítja össze az eredeti állományt.

Ismertebb socketek és portok

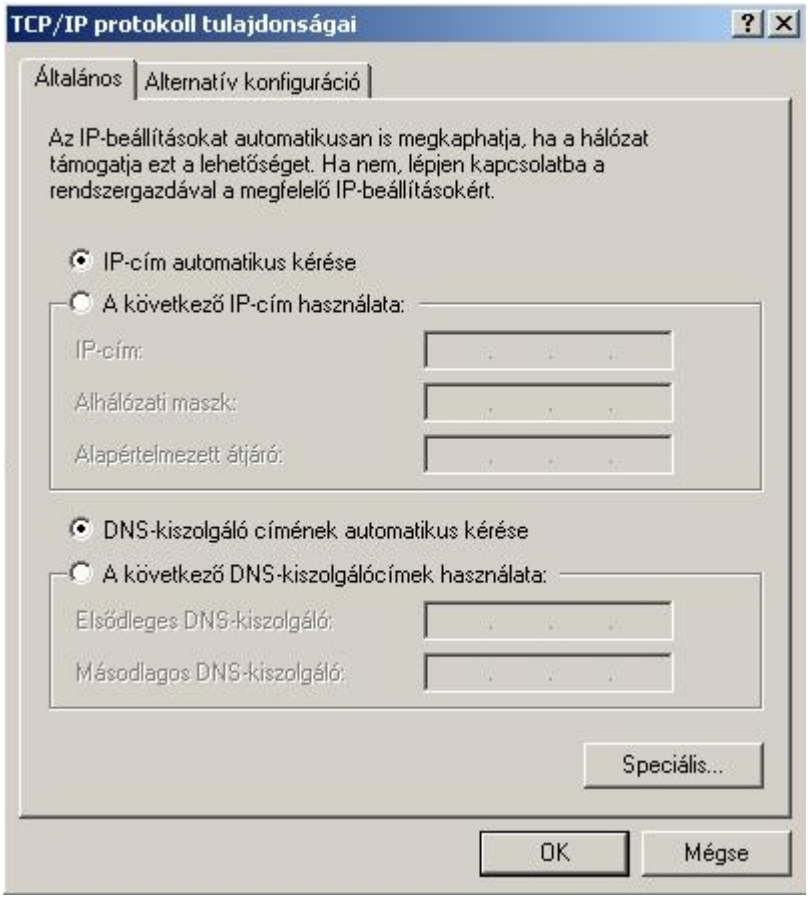
Az eddigiekben azt vettük sorra, hogy egy üzenet hogyan darabolódik szét, hogyan jut el egy géptől egy másikig, majd ott hogyan áll ismét össze. Mindez még kevés ahhoz, hogy hasznos dolgot lehessen végezni. Alapvetően minden visszavezethető arra, hogy két alkalmazás kommunikál egymással. Ez hasonló a telefonáláshoz. A hívónak tudnia kell a hívott telefonszámát, a hívottnak meg a telefon közelében kell lennie, hogy fogadni tudj a hívást. A TCP világban a telefonszám megfelelője a *socket*. Egy socket egy IP címből, egy port számból és egy olyan információból áll, amely megmondja, hogy TCP vagy UDP portról van-e szó, mert mindkettőnek meg van a maga portrendszere.

Egyszerre több hálózati program is futhat egy gépen, ezért, ha egy távoli gép kommunikálni akar egy éppen futó hálózati alkalmazással, akkor nem elég az IP címet tudnia, hanem magát a megszólítani kívánt alkalmazást is be kell azonosítania. Ezért minden TCP kommunikációt

folytató alkalmazás rendelkezik egy 16 bites értékkel, amely segítségével egyértelműen beazonosítható. Ez az érték az alkalmazás portja, amelyen az alkalmazás elérhető. A legtöbbet használt internetes alkalmazásokhoz (ftp, mail, stb.) rendelt portokat jól ismert (well-known) portoknak nevezik.

Alapértelmezett TCP/IP beállítások

Bármelyik kapcsolat TCP/IP beállításait meg lehet tekinteni a *Vezérlőpult/Hálózati kapcsolatok* alatt a kapcsolatra jobb egérgombbal kattintva a Tulajdonságok menüponton belül a TCP/IP Tulajdonságok menüjét kiválasztva.



Alapértelmezett TCP/IP beállítások

Mint az ábrából is látszik az IP cím egy alapértelmezett Windows telepítés után automatikusan kerül kiosztásra. Ha egy új gép kapcsolódik egy olyan hálózathoz, ahol nincs felkonfigurált DHCP szerver, akkor a számítógép kijelöl egy IP címet magának a 169.254.0.1-169.254..255.254 címtartományból. Ez a címtartomány az Automatic Private IP

Addressing (APIPA) nevű összetevőn keresztül érhető el. A DHCP-ről és az APIPA-ról a következő fejezetben részletesen beszélek.

Automatikus TCP/IP konfiguráció

DHCP

A DHCP (Dynamic Host Configuration Protocol) a DNS-sel (Domain Name System) együtt a Microsoft Windows Server 2003 hálózati infrastruktúrájának alapkövét adja. Még a legkisebb hálózatokban is a DHCP látja el a hosztokat egy IP konfigurációval. Ez a konfiguráció tartalmaz legalább egy IP címet és egy alhálózati maszkot, valamint általában magában foglalja az elsődleges tartomány utótagot, az alapértelmezett árjárót, az elsődleges és másodlagos DNS szervert, WINS szervereket és még néhány beállítást. Egyetlen hoszt bekapcsolása a hálózatba nem nagy kihívás a rendszergazda számára, de ha több ezer munkaállomást kellene kézzel beállítani, akkor igen hamar túlterhelődne az adminisztrátor egy ilyen konfigurációt megvalósító megbízható és automatikus erőforrás segítsége nélkül.

A DHCP egy IP standard, amit arra fejlesztettek ki, hogy megkönnyítse a címkiosztást a hálózati rendszerekben. A DHCP automatikusan szabályozza a címkiosztást és egyéb alapvető beállításokat is elvégez a hálózati kliensek számára.

A DHCP elődje a BOOTP (BOOTstrap Protocol) volt, amely hasonló elven működött. A BOOTP alapú boot folyamatnak két fázisa van: IP cím meghatározás majd a boot állomány letöltése. Legfőbb előnye a központi címkiosztás, de hátránya sokkal több volt:

- Statikus: a hálózati csatoló fizikai címe alapján került kiosztásra az IP cím, amelyet a rendszergazdának kellett beállítania a BOOTP szerveren. Tehát minden egyes új gép esetén újabb adminisztrációs munka merült fel.

- Az ideiglenes IP címeket nem kezelte.

- A BOOTP használatához ismernünk kell a hálózaton lévő összes gép fizikai címét, ami nem túl hatékony megoldás, mert minden egyes gépen ki kell adni az *ipconfig /all* parancsot.

Ezen problémák kiküszöbölésére alkották meg a DHCP-t. A DHCP-vel egy IP címtartomány dinamikus kiosztása válik lehetővé. Több DHCP szerver működése esetén a szerverek által kezelt címtartományok (alaphelyzetben) nem fedhetik át egymást. Ha egy csomópont kér egy címet, akkor üzenetszórásos küldéssel felteszi a kérdést, amelyet az alhálózat minden csomópontja megkap. A DHCP szerverek feldolgozzák a kérdést, és ha a kezelt címtartományukban még van szabad IP cím, akkor azzal megválaszolják a DHCP kérdést. A kliens a hozzá érkező DHCP válaszokból választ egyet, s visszajelzi a választását a megfelelő DHCP szervernek. A DHCP szerver „könyveli" a címválasztást (foglalt lett a cím), s a könyvelésről megerősítést küld a kliensnek.

Lehetőség van statikus IP címek megadására is. Ez tipikusan a DHCP szerver és az alapértelmezett átjáró címének kézi beállítását jelenti. Ezt a lehetőséget DHCP fenntartásnak nevezzük. Az általános javaslat az, hogy ahol lehet használjunk dinamikus címeket.

A kliensek a dinamikus címeket egy megújítható időtartamra kapják. Ezt az időtartamot a kiszolgálón kell beállítani. Az időtartam meghosszabbításával először a kapott időtartam felénél próbálkozik a kliens. Erre azért van szükség, hogy ne kelljen minden kommunikációt beszüntetni, amikor lejár a bérleti idő. Ha elérte a bérleti időtartam 87,5%-át és még mindig nem sikerült meghosszabbítani, akkor megpróbál új címet kérni, ha kell akár más DHCP kiszolgálótól.

A DHCP előnyei

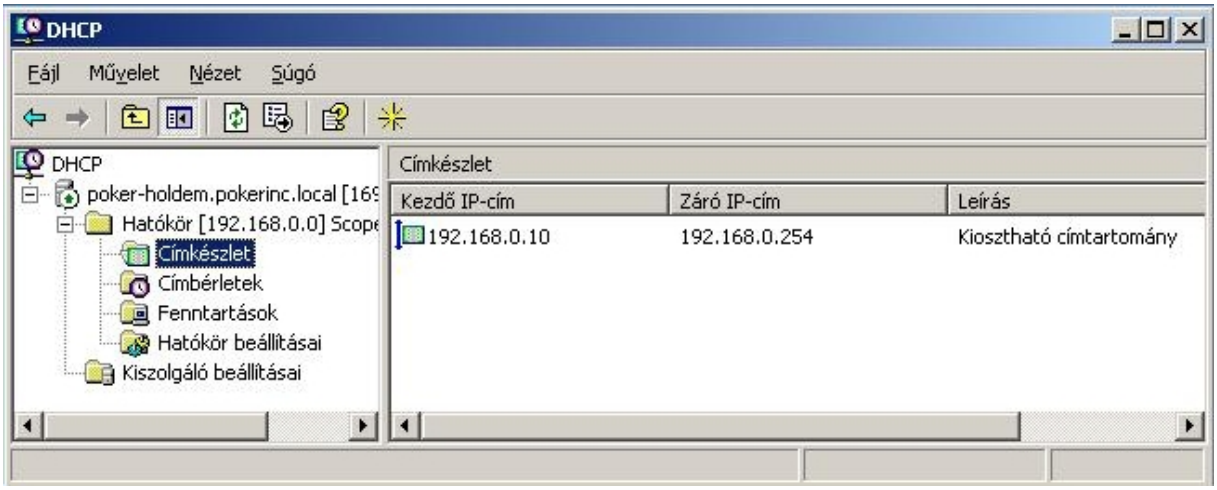
Az egyik legnagyobb előnye a DHCP használatának, hogy nagymértékben csökkenti a hálózati munkaállomások konfigurálásával és újrakonfigurálásával töltött időt. A DHCP nem csak az IP cím kiosztásával egyszerűsíti az adminisztrációs munkát, hanem opcionálisan megadhatja az alapértelmezett átjárók, DNS szerverek, WINS szerverek és egyéb a kliens számára hasznos szerverek címét. Egy másik előnye az automatikus címkiosztásnak, hogy segít elkerülni a manuális konfigurálásból származó hibákat (több száz hoszt esetén ez nem elképzelhetetlen). Például a DHCP segít megelőzni a címütközést, ha két gépnek véletlenül ugyanaz az IP cím lett kiosztva.

A DHCP szolgáltatás telepítése

A DHCP beállításához először a DHCP Server szerepkört kell installálni. Ez a szerepkör nem telepítődik automatikusan, de telepíthető Windows Összetevőként vagy a **Kiszolgáló kezelése** ablakon keresztül. Továbbá ki kell osztani egy statikus IP címet a DHCP kiszolgáló számára és meg kell állapítanunk a címtartományt, amelyből a DHCP szerver a címeket kioszthatja.

A Kiszolgáló kezelése ablakon keresztüli installáláshoz a Start menüből indítsuk el a Kiszolgáló kezelése ablakot, klikkeljünk a Szerepkör hozzáadása/törlése gombra és válasszuk ki a DHCP szerepkört. Kattintsunk a Tovább gombra a telepítés elkezdéséhez.
A telepítés más Windows összetevőkhöz hasonlóan nagyon egyszerűen elvégezhető a Vezérlőpult/Programok hozzáadása és eltávolítása menüponton keresztül is. Telepítés után a DHCP azonnal használható, nincs szükség újraindításra.

A DHCP beállításaihoz kattintsuk a Kiszolgáló kezelése ablakon belül az Aktuális DHCP kiszolgáló kezelése gombra-



DHCP konzol

A megjelenő DHCP konzolon beállíthatjuk a Kioszthatő címtartományt, a Hatókört, a Fenntartásokat és egyéb opciókat. Természetesen az összes fent említett művelet végrehajtásához adminisztrátori jogokkal kell rendelkeznünk.

DHCP szerver engedélyezése

Tartománykezelőt (Active Directory) használó hálózatba integrált DHCP szerver esetén szükség van a szerver engedélyezésére. Csak tartományvezérlőként és tagkiszolgálóként működő számítógépek vesznek részt az Active Directory-ban és csak ezeket a szerver típusokat lehet engedélyezni. Ha a hálózatban van Active Directory tartományvezérlő, akkor a legelső feltelepített DHCP szervernek engedélyezettnek kell lennie. A Microsoft Windows 2000 Server vagy Microsoft Windows 2003 Server alatt futó egyéni vagy munkacsoport DHCP szerverek nem lehetnek engedélyezettek az Active Directory hálózatokban, de párhuzamosan létezhetnek ezekkel a szerverekkel, amíg nem olyan alhálózatra vannak telepítve, amelyiknek van engedélyezett DHCP szervere. Az engedélyezett DHCP szerver mellett létező egyéni szervert nevezik csavargó DHCP szervernek. Ha egy csavargó DHCP szerver egy engedélyezett DHCP szervert észlel ugyanazon az alhálózaton belül, akkor automatikusan beszünteti a DHCP kiszolgáló működést és nem ad bérbe több IP címet.

DHCP kiszolgáló engedélyezése az Active Directoryban

1. Nyissuk meg a **DHCP** szolgáltatást.
2. Kattintsunk a konzolfa **DHCP** elemére.
3. Kattintsunk a **Művelet** menü **Engedélyezett kiszolgálók kezelése** parancsra.
4. Kattintsunk az **Engedélyezés** gombra.
5. Adjuk meg az engedélyezni kívánt DHCP kiszolgáló nevét vagy IP címét, majd kattintsunk az **OK** gombra.

A DHCP kiszolgáló teljesen minősített tartományneve (FQDN) nem lehet több 64 karakternél. Ha e név meghaladja a határértéket, akkor a kiszolgáló engedélyezési kísérlete nem sikerül, és a következő hibaüzenet jelenik meg: „Megszorításmegsértés történt.” Ebben az esetben a kiszolgálót IP címével, és ne teljesen minősített tartománynevével kell engedélyeznünk.

Hatókörök konfigurálása

A hatókör a DHCP szolgáltatást használó alhálózat számítógépeihez tartozó IP címek felügyeleti csoportja. A rendszergazda először minden egyes fizikai alhálózat számára létrehoz egy hatókört, majd a hatókört használja az ügyfelek által használt paraméterek megadásához. A hatókörök a következő tulajdonságokkal rendelkeznek:

- A DHCP szolgáltatás címbérleti szolgáltatásához használható vagy abból kizárt IP címek tartománya.
- Alhálózati maszk, amely egy adott IP cím alhálózatát határozza meg.
- A hatókör létrehozásakor a hatókörhöz rendelt hatókörnév.
- A dinamikusan lefoglalt IP címeket fogadó DHCP ügyfelekhez tartozó címbérlet-élettartam értékek.
- A DHCP ügyfelekhez való hozzárendelésre konfigurált valamennyi DHCP hatókörbeállítás, például a DNS kiszolgáló, az útválasztó IP címe és a WINS kiszolgáló címe.
- Az esetleg létrehozott fenntartások, melyek biztosítják, hogy egy-egy adott DHCP ügyfél mindig ugyanazt az IP címet kapja meg.

Hatókörök hozzáadása előtti teendők

A DHCP hatókör egy adott alhálózaton levő IP címek készletéből áll (például 192.168.0.1 – 192.168.0.254), amelyet a DHCP kiszolgáló az ügyfeleknek bérbe adhat. Mindegyik alhálózat csak egyetlen, összefüggő IP címtartománnyal rendelkező DHCP hatókört tartalmazhat. Ha a DHCP szolgáltatás egyetlen hatókörén vagy alhálózatán belül több címtartományt szeretne használni, először meg kell határoznia a hatókört, majd beállítani a szükséges kizárási tartományokat.

- **A hatókör meghatározása**

  Használhatjuk a helyi IP hálózatot alkotó egymást követő IP címek azon teljes tartományát, amelyhez a DHCP szolgáltatást engedélyezzük.
- **Kizárási tartományok beállítása**

  A hatókörön belül célszerű kizárási tartományokat létrehozni olyan IP címekből, amelyeket a DHCP kiszolgálónak nem szabad felajánlania vagy használnia a DHCP hozzárendeléshez. Kizárhatjuk például az előző példában említett hatókörben az első 10 címet a 192.168.0.1 – 192.168.0.10 címtartomány kizárásával.

  Ezzel a beállítással biztosíthatjuk, hogy a rendszer ezeket a címeket soha nem ajánlja fel azoknak a DHCP ügyfeleknek, melyek címbérlet-konfigurációt kérnek a kiszolgálótól. A kizárt IP címek aktívak lehetnek a hálózaton, de csak úgy, ha kézzel

konfiguráljuk őket azokon az állomásokon, amelyek a cím megszerzéséhez nem használják a DHCP szolgáltatást.

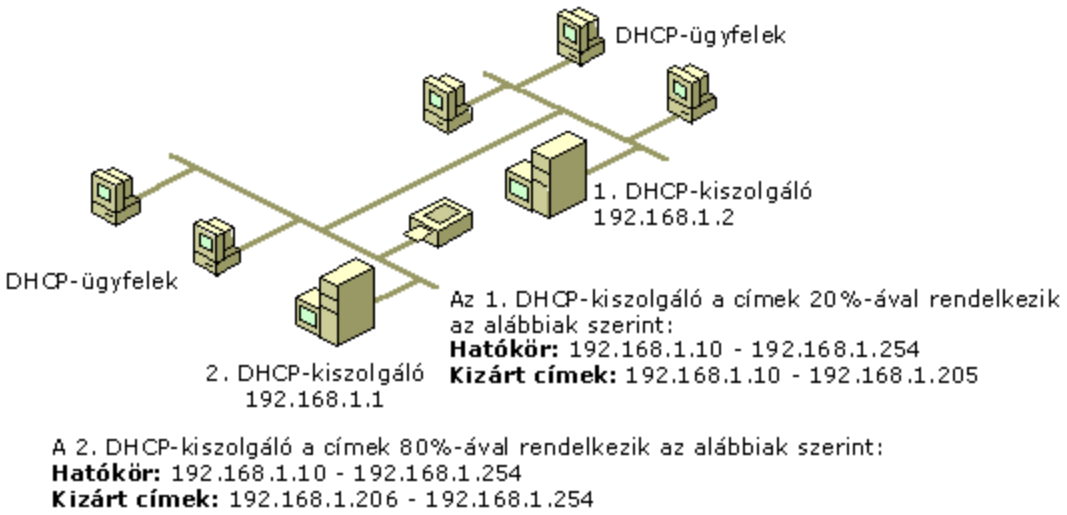
Hatókörök létrehozása

DHCP-hatókör létrehozásakor a DHCP konzolban adhatjuk meg a következő szükséges adatokat:

- Hatókörnév, amelyet a hatókört létrehozó rendszergazda határoz meg;
- Azon alhálózatot azonosító alhálózati maszk, amelybe az adott IP cím tartozik;
- A hatókörön belüli IP címtartomány;
- A *címbérlet élettartama* néven ismert időtartam, amely megadja, hogy a DHCP ügyfél mennyi ideig használhat egy hozzárendelt IP címet, mielőtt a DHCP kiszolgálón meg kellene újítania a címkonfigurációt.

A 80/20 szabály alkalmazása hatókörök esetén

A DHCP kiszolgálók kihasználtságának kiegyensúlyozásához érdemes követni az úgynevezett „80/20” szabályt, amellyel két DHCP kiszolgáló között meg lehet osztani a hatóköri címeket. Ha az 1. számú kiszolgáló úgy van konfigurálva, hogy a címek többségét (körülbelül 80 százalékát) tegye elérhetővé az ügyfeleknek, akkor a 2. számú kiszolgálót úgy konfigurálhatjuk, hogy az a többi címet (körülbelül 20 százalékot) szolgáltassa. A következő példa a 80/20 szabályt illusztrálja:



A 80/20 szabály alkalmazása két DHCP kiszolgáló esetén

Új hatókör létrehozásakor az ehhez használt IP címeknek nem szabad tartalmaznia a létező, statikusan konfigurált számítógépek címeit, például a DHCP kiszolgáló címét. Ezeknek a statikus címeknek vagy kívül kell esniük a hatókör tartományán, vagy ki kell zárni ezeket a hatókör címtartományából.

Hatókörök hozzáadása utáni teendők

A hatókör meghatározása után a következő feladatok végrehajtásával részletesebben konfigurálhatjuk a hatókört:

- **További kizárási tartományok beállítása**

  Bármely más olyan IP címet is kizárhatunk, amelyet nem szabad DHCP ügyfeleknek bérletbe adni. Minden statikusan konfigurálandó eszközhöz kizárásokat kell használni. A kizárt tartományoknak tartalmazniuk kell az összes olyan IP címet, amelyet kézzel rendeltünk hozzá más DHCP kiszolgálókhoz, nem DHCP ügyfelekhez, lemez nélküli munkaállomásokhoz, Útválasztás és távelérés szolgáltatást alkalmazó, illetve PPP-ügyfelekhez.
- **Fenntartások létrehozása**

  Dönthetünk úgy is, hogy bizonyos IP címeket a hálózaton lévő egyes számítógépek vagy eszközök állandó bérleti hozzárendeléséhez tartunk fenn. Csak olyan eszközökhöz célszerű fenntartásokat létrehozni, amelyek DHCP kompatibilisek, és amelyeket a hálózaton meghatározott célokra kell fenntartanunk (például a nyomtatókiszolgálók).
- **A címbérletek élettartamának beállítása**

  Módosíthatjuk az IP címbérlet hozzárendeléséhez használandó címbérleti élettartamot. Az alapértelmezett címbérleti élettartam nyolc nap.

  A legtöbb helyi hálózat esetében az alapértelmezett érték elfogadható, de tovább növelhető, ha a számítógépek helye ritkán változik. Ezenkívül beállíthatunk végtelen címbérleti élettartamokat is, de ezeket körültekintően kell használnunk.
- **A hatókörrel használandó beállítások és osztályok konfigurálása**

  Az ügyfelek teljes konfigurációjához konfigurálni és engedélyezni kell egyes DHCP-beállításokat a hatókör számára. A hatókörügyfelek speciális (és egyedi) kezeléséhez felhasználó vagy forgalmazó által megadott beállításosztályok is hozzáadhatók és engedélyezhetők.

A hatókör aktiválása

A hatókör meghatározása és konfigurálása után *aktiválni* kell a hatókört ahhoz, hogy a DHCP-kiszolgáló megkezdhesse az ügyfelek kiszolgálását. Új hatókört azonban mindaddig nem szabad aktiválni, amíg meg nem adjuk annak DHCP beállításait.

1. Nyissuk meg a DHCP szolgáltatást.
2. A konzolfán kattintsunk a megfelelő hatókörre.
    - DHCP
        - *A megfelelő DHCP-kiszolgáló*
            - *A megfelelő gyűjtőhatókör* (ha van)
                - *A megfelelő hatókör*
3. Kattintsunk a **Művelet** menü **Aktiválás** parancsára.

Hatókör aktiválására csak új hatókörök esetében, a címbérletkiosztás indításához van szükség. A hatóköröket aktiválni kell ahhoz, hogy a DHCP ügyfelek elérhessék azokat. Amikor a kijelölt hatókör aktív, a **Művelet** menüben lévő parancs az **Inaktiválás** parancsra változik. Általános elvárás, hogy csak akkor tegyünk inaktívvá hatókört, ha véglegesen ki szeretnénk azt vonni a hálózati használatból.

A DHCP újdonságai a Windows Server 2003 termékcsaládban

Osztály nélküli statikus útvonal

A DHCP ügyfelek ezzel a beállítással vehetik fel az útvonalak listáját az útválasztó táblába. A rendszergazdák például ezzel a szolgáltatással engedélyezhetik az ügyfeleknek az osztott bújtatást (*split tunneling*) a virtuális magánhálózati (VPN) és az internetes kapcsolatokban. Így az Internetre irányuló adatforgalomnak nem kell áthaladnia a VPN-kapcsolaton, de a felhasználó elérheti a szervezet magánhálózatában lévő erőforrásokat is.

DHCP-adatbázisok áttelepítése a netsh paranccsal

A DHCP adatbázisok egyik kiszolgálóról a másikra egyszerűbben telepíthetők át a **netsh** parancs használatával. Ezzel elkerülhető a kézi beállítások többsége, például a rendszerleíró adatbázis kézi szerkesztése vagy a hatókörök újbóli létrehozása. A netsh parancs lehetővé

teszi a kiszolgálók és az útválasztók helyi konfigurálását, és parancsfájlokat is felhasználhat a konfigurálási feladatok automatizálásához. Ez a következő esetekben lehet hasznos:

A rendszergazda lemezhibákra figyelmeztető üzeneteket kap a DHCP kiszolgálón, ezért a DHCP szolgáltatás áthelyezése mellett dönt, mielőtt még a lemez helyreállíthatatlanul meghibásodna.

A DHCP kiszolgálót tartalmazó hálózati szegmens teljesítményével kapcsolatos okokból a rendszergazdának fel kell osztania a DHCP kiszolgálót. A rendszergazda ezzel a szolgáltatással helyezheti át a DHCP adatbázis részeit más számítógépekre.

DHCP bérlet (lease) törlése a netsh paranccsal

Az új **netsh dhcp server scope** *hatókörnév* **delete lease** parancs használatával a parancssorból törölhetők a DHCP bérletek. Ez a szolgáltatás egyszerűbbé teszi a DHCP kiszolgálókkal kapcsolatos műveleteket, amelyek így a parancssorból és parancsfájlokkal hajthatók végre. Ez szükségtelenné teszi a DHCP beépülő modul használatát a bérletek törléséhez.

APIPA

A TCP/IP alapértelmezés szerint - ahol nincs elérhető DHCP szerver - az APIPA (Automatic Private IP Addressing) protokollt használja az automatikus konfigurációhoz, a 169.254.0.1-től 169.254.255.254-ig terjedő IP címtartománnyal és a 255.255.0.0 alhálózati maszkkal. Az alapértelmezett átjárón, DNS kiszolgálón és WINS kiszolgálón nincs automatikus beállítás, mivel az APIPA szolgáltatást különálló hálózati szegmensből álló hálózatokhoz tervezték, amelyeknek nincs internetkapcsolatuk sem. Az APIPA-címtartomány az IANA (Internet Assigned Numbers Authority) nevű szervezet tulajdona. Az ebbe a tartományba eső címeket az interneten nem használják. Az APIPA révén szükségtelenné válik az IP cím beállítása az internethez nem kapcsolódó, önálló, hivatali vagy otthoni hálózatok esetében.

APIPA tiltása

1. Indítsuk el a Rendszerleíróadatbázis-szerkesztőt (Start menü/Futtatás **regedit**).

2. A Rendszerleíróadatbázis-szerkesztőben keressük meg a következő rendszerleíró kulcsot:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

3. Kattintsunk a Parameters kulcsra, majd a **Szerkesztés** menüre.

4. Kattintsunk az **Új** menüpont **Duplaszó** parancsára.

5. Az új bejegyzés létrehozásához gépeljük be a következőt:

IPAutoconfigurationEnabled

6. Kattintsunk jobb gombbal az új bejegyzésre, és kattintsunk a **Módosítás** parancsra.

7. A **Duplaszó szerkesztése** párbeszédpanelen az **Érték** mező értékét állítsuk a **O** értékre.

8. Lépjünk ki a Rendszerleíróadatbázis-szerkesztőből, és indítsuk újra a számítógépet.

A művelet végrehajtásához a helyi számítógépen a Rendszergazdák vagy a Hálózatbeállítási felelősök csoportba kell tartoznunk. Ha az **IPAutoconfigurationEnabled** bejegyzés hiányzik, **1** az alapértelmezett érték, ami azt jelenti, hogy az APIPA protokoll használható.

Név- és információszervezés: a tartomány (domain) rendszer

A hálózati szoftvernek egy 32 bites Internet címre van szüksége ahhoz, hogy egy kapcsolatot felépíthessen, vagy hogy datagrammokat küldhessen. A felhasználók viszont inkább a számítógépek neveivel mintsem számokkal szeretnének hivatkozni rájuk, mivel a neveket könnyebben meg lehet jegyezni. Ezért létezik egy adatbázis, amelyből a hálózati alkalmazás kikeresheti a névnek megfelelő címet, és fordítva. Amikor az Internet még nem volt ilyen kiterjedt, akkor ez viszonylag könnyen megoldódott: minden gépnek volt egy adatállománya, amelyben az összes többi rendszer nevét és címét felsorolták. Ma már túl sok rendszer létezik ahhoz, hogy ez a megoldás kivitelezhető legyen. Emiatt ezeket az állományokat olyan névkiszolgálók váltották fel, amelyek a gépek neveit és a megfelelő címeket tartják nyilván. A sokfajta információ közül ez csak egy. Valójában ezek a kiszolgálók sokkal általánosabb feladatot látnak el. A valóságban egyetlen központi gép helyett az ilyen kiszolgálók egymással összekapcsolt halmaza használatos. Manapság már olyan sok különböző intézmény kapcsolódik az Internethez, hogy nem lenne praktikus, ha egy központi hatóságot kellene értesíteniük minden olyan esetben, amikor egy gépet a hálózatba be- vagy abból kikapcsolnak. Éppen ezért a névadásra az egyes intézmények a rendszerükön belül saját maguk jogosultak. Az így kialakított névkiszolgálók közösen egy fa struktúrát alkotnak, amely az intézmények hálózati szerkezetének felel meg. Ezt a szerkezetet a nevek is tükrözik. Tipikus példa erre a BORAX.LCS.MIT.EDU név, amely a MIT számítástechnikai laboratóriumának (LCS) egy számítógépét jelöli (ilyen példa lehetne még: infotech.inf.unideb.hu, ami az DE-IK Információ Technológia tanszékének infotech nevű gépét adja). A gép Internet címének meghatározásához 4 potenciális kiszolgálót kellene megkérdezni. Először egy központi kiszolgálótól (root - gyökér, ld. a fa struktúrát) kellene megtudakolni, hogy hol található az EDU kiszolgáló, amely nem más, mint a hálózatba kapcsolt oktatási intézmények nyilvántartása. A gyökérként szereplő kiszolgáló több EDU kiszolgáló nevét és Internet címét adná meg. Minden szinten több ilyen névkiszolgáló van, hogy az esetleges meghibásodások ne okozzanak fennakadást. A következő feladat lenne az EDU kiszolgáló lekérdezése a MIT névkiszolgálójáról. Itt is több kiszolgáló nevét és Internet címét kapnánk meg. Ezek közül általában nem mindegyik található az intézmény területén (egy esetleges áramszünet fellépte miatt). Ez után a MIT-től kérdeznénk le a

számítástechnikai laboratórium (LCS) névkiszolgálójának adatait, majd végül a laboratóriumi névkiszolgálók egyike adná a BORAX adatait.

A végső eredmény a BORAX.LCS.MIT.EDU gép Internet címe lenne. A fenti szintek mindegyike egy tartományt (domain) jelöl. A teljes BORAX.LCS.MIT.EDU név pedig egy tartománynév (domain name). Ugyanígy a felsőbb tartományok nevei is tartománynevek: LCS.MIT.EDU, MIT.EDU és EDU.

Az esetek nagy többségében szerencsére nem kell a fenti lépések mindegyikét végrehajtani. A legfelső kiszolgáló (gyökér) ugyanis egyben a legfelső szinten lévő tartományok (pl. EDU) névkiszolgálójaként is szerepel. Tehát a gyökér kiszolgáló felé irányuló egyetlen kérdéssel a MIT névkiszolgálójához lehet eljutni. Az alkalmazott szoftverek pedig a már feltett kérdésekre kapott válaszokra emlékeznek. Ez azt jelenti, hogy a LCS.MIT.EDU kiszolgáló lekérdezése után tudja, hogy hol keresse a LCS.MIT.EDU, a MIT.EDU és az EDU tartománybeli kiszolgálókat. A BORAX.LCS.MIT.EDU fordítására szintén emlékszik. Persze minden ilyen információnak van egy megfelelő élettartama, ami tipikusan pár napnak felel meg. Az élettartam lejárta után az információkat fel kell frissíteni. Az intézmények ilyen módon változtathatnak, ha akarnak.

A tartományrendszer feladata nem merül ki az Internet címek megtalálásában. Minden egyes tartománynév csomópontként szerepel egy adatbázisban. A csomópontnak különböző tulajdonságokat jellemző rekordjai lehetnek. Ilyen az Internet cím, a számítógép típusa, és a számítógép által biztosított szolgáltatások felsorolása. Egy program egy adott névvel kapcsolatban kérheti ezen információk valamelyikét, vagy az összest. Megoldható az is, hogy egy adatbázisbeli csomópont egy másik csomópont álneveként (alias) szerepeljen. Az is lehetséges, hogy a tartományrendszerben felhasználókról, levelezési listákról, vagy más objektumokról tároljunk adatokat.

A fenti adatbázisok működését, illetve az azok lekérdezését megvalósító protokollokat is Internet szabvány írja le. Minden hálózati alkalmazásnak meg kell tudnia valósítani ezeket a lekérdezéseket, mivel hivatalosan így történik a hosztnevek kiértékelése. Az alkalmazások általában saját rendszerükön (tartományukon) belül keresnek egy névkiszolgálót. Ez a kiszolgáló aztán a felsőbb szinten (az ő tartományán) lévő kiszolgálókkal veszi fel a kapcsolatot. Ezzel a módszerrel az alkalmazásokban lévő kód mennyiségét lehet lecsökkenteni.

A tartományrendszer fontos szerepet tölt be az elektronikus levelezésben. Az adatbázisokban szerepelhetnek olyan bejegyzések, amelyek megmondják, hogy melyik gép kezeli egy adott név leveleit, egy felhasználó levelei hová érkezzenek, illetve levelezési listákat is definiálhatnak.

Névfeloldás

A TCP/IP kommunikáció az IP címeken alapul. Minden IP adatcsomag, amelyet egy TCP/IP alapú számítógép közvetít, tartalmaz egy forrás IP címet, ami beazonosítja a küldő gépet, és egy cél IP címet, ami beazonosítja a célgépet, amelyik megkapja a csomagot. A routerek az IP címben található hálózati azonosítókat használják az adatcsomagok megfelelő helyre küldéséhez, tehát a végső célba való eljuttatásukhoz. Az embereknek a beszédes nevek használata a kényelmes, de a számítógépek a 32 bites (IPv6 esetén 128 bites) IP címekkel kommunikálnak egymással. A névfeloldás lehetővé teszi, hogy az IP címekhez alfanumerikus neveket feleltessünk meg, így téve felhasználóbaráttá a számítógépek és szolgáltatások elérését. Sokkal könnyebb megjegyezni, hogy a valaki@freemail.hu-ra küldök egy emailt vagy pedig a valaki@195.228.245.1 címre. A felhasználóbarát neveket csak az emberek által használatosak; nem változtatják meg a TCP/IP rendszerű gépek között a kömmunikációt. Bármikor, ha egy nevet használunk a cím helyett egy alkalmazásban, a számítógépnek át kell alakítania ezt a nevet egy IP címmé mielőtt elkezdené a kommunikációt a célgéppel. Ezt a név konverziót nevezzük névfeloldásnak.

Ahhoz, hogy tudjuk milyen névfeloldási stratégiát kell alkalmaznunk, ismernünk kell a feloldandó nevek fajtáit. A Microsoft Windows operációs rendszereket használó hálózatokban alapvetően kétféle nevet használnak a számítógépek és egyéb erőforrások megnevezésére: a Domain Name System (DNS) és a Network Basic Inpu/Output System (NetBIOS).
Az 1970-es években, amikor az Internet még csak egy kísérleti hálózat volt, amit ARPANET-nek neveztek, a rendszer adminisztrátorok rendelték hozzá a barátságos nevet a számítógépeikhez. Ezeket hívták hoszt neveknek. Minden egyes gépnek volt egy hoszt táblája, ami egy egyszerű szöveges állomány volt, amely tartalmazta a hoszt neveket és a velük ekvivalens IP címet, valahogy így:

```
102.54.94.97     rhino.acme.com          # forráskiszolgáló
38.25.63.10      x.acme.com              # x ügyfélállomás
127.0.0.1……      localhost
```

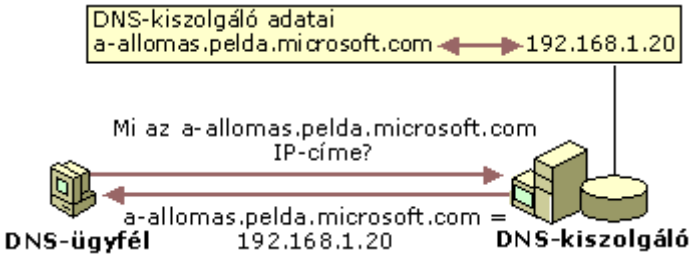
Az első oszlopban találhatók az IP címek, a másodikban a hoszt nevek, míg a harmadikban a #-jel után az adminisztrátorok megjegyzései, amelyekkel a gép nem foglalkozott. Ha egy alkalmazás szembetalálkozott egy hosztnévvel, akkor rögtön a hoszt fájlban kerete a névhez tartozó IP címet. A mai napig minden egyes TCP/IP alapú gép rendelkezik ezzel a hoszt

fájllal, bár igen kevés azoknak a hosztoknak a száma, amelyek használják is. A Windows Server 2003-at futtató számítógépen ennek a fájlnak a neve Hosts és a %Rendszer-könyvtár%\System32\drivers\etc könyvtárban található.

Mivel az ARPANET viszonylag kicsi volt, a hoszt állományok sem voltak nagyok és az adminisztrátoroknak nem is kellett gyakran módosítaniuk. Ahogy az ARPANET elkezdett növekedni, úgy nőttek ezek a fájlok is, aminek egy idő után az lett az eredménye, hogy kezelhetetlenül naggyá váltak. Ennek a problémának a megoldására kezdődött egy új fejlesztés, melynek eredménye lett a DNS.

DNS

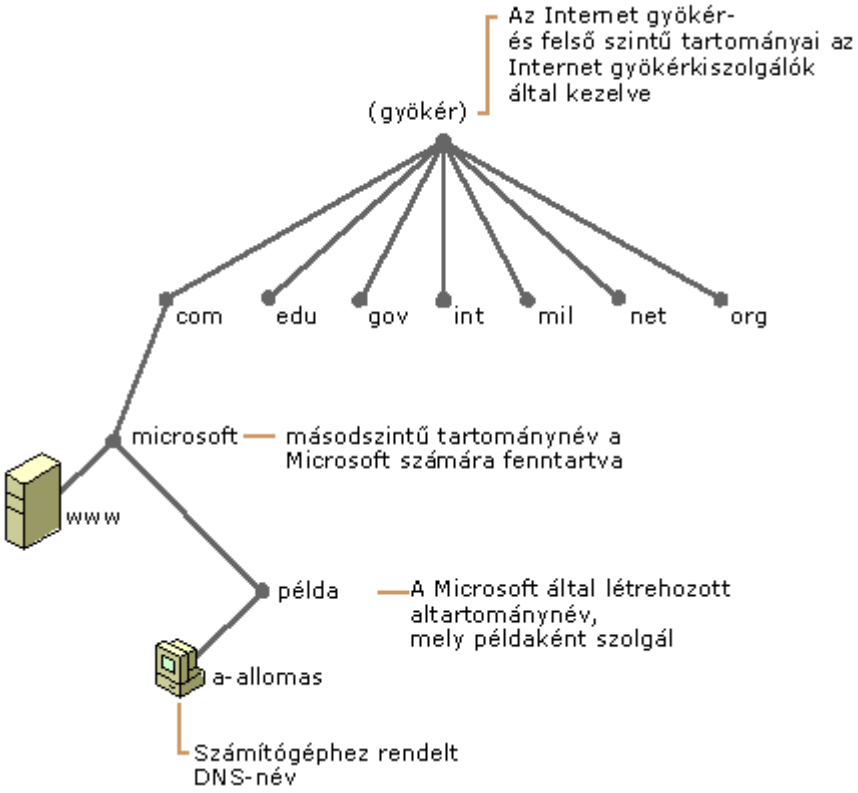
A DNS (Domain Name System) egy hierarchikus, elosztott adatbázis, amelyben DNS tartománynevek különböző adattípusokhoz (például IP címekhez) vannak hozzárendelve. A DNS-t TCP/IP hálózatokon, például az interneten alkalmazzák. Amikor a felhasználó egy alkalmazásban megad egy DNS-nevet, a DNS azt a nevet meg tudja feleltetni a névhez rendelt másik adatnak, például egy IP címnek (vagyis feloldja a nevet). Ha a hálózat homogén (minden állomáson ugyanaz az operációs rendszer fut), és nem a DNS névfeloldási módszert használja, továbbra is használhatja azt a módszert, nincs szükség a DNS szolgáltatásra. Ha a hálózat heterogén (az állomásokon különböző operációs rendszer fut), vagy az internetre csatlakozik, szükség lesz a DNS telepítésére, mivel az internet olyan protokollokból áll, amelyeken kötelező a DNS. A legtöbb felhasználó szívesen használ rövid nevet (ilyen a *pelda.microsoft.com* is) egy számítógép, például levelezőkiszolgáló vagy webkiszolgáló, hálózaton való megkeresésére. A rövid név könnyen megtanulható és felidézése nem okoz gondot. A számítógépek azonban a hálózaton numerikus címek alapján kommunikálnak egymással. A hálózati erőforrások használatának megkönnyítése érdekében a névszolgáltatások, például a DNS, a rövid számítógép- vagy szolgáltatásneveket hozzárendelik azok numerikus címeihez. Az alábbi ábrán a DNS fő felhasználási módja látható, a számítógép neve alapján a hozzá tartozó IP cím megkeresése.



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 példa egy egyszerű DNS lekérdezést mutat egyetlen ügyfél és DNS kiszolgáló részvételével. A gyakorlatban a DNS lekérdezések ennél bonyolultabbak és más lépéseket is tartalmazhatnak.

A DNS névtér

Az alábbi ábrán látható DNS névtér azon az elven alapszik, hogy a nevekkel rendelkező tartományok egy fastruktúra szerint helyezkednek el. A fában az egyes szintek a fa egy ágát vagy levelét jelképezik. Az ág egy olyan szint, ahol az elnevezett erőforrások egy csoportját egynél több név azonosítja. A levél egy nevet jelent, amely az adott szinten egyszer használt, és meghatározott erőforrást azonosít.



Az fenti ábrán látható, hogy az internetes gyökérkiszolgálók hogyan hitelesítik a Microsoftot a DNS tartományi névtér saját tulajdonát képező részében. A DNS kiszolgálók és ügyfelek a lekérdezések használatával rendelnek a fában található nevekhez meghatározott típusú erőforrás-információkat. Az információt a DNS kiszolgálók küldik el az ügyfeleknek a lekérdezésekre adott válaszokban. Az ügyfelek feldolgozzák az információt és továbbítják az alkalmazás felé, amely a név feloldását kérte. A névfeloldás folyamán szem előtt kell tartani, hogy a DNS kiszolgálók gyakran DNS ügyfélként működnek, amikor a lekérdezett név feloldása érdekében lekérdezéseket küldenek más kiszolgálóknak. A fában előforduló tartománynevek technikai szempontból egy tartományt jelentenek. A DNS-sel foglalkozó anyagok többségében azonban a neveket ötféleképpen különböztetik meg, a név szintjétől és használatának módjától függően. A Microsoft számára regisztrált DNS tartománynév (microsoft.com) például egy második szintű tartomány. Ennek oka az, hogy a név két részből áll (ezeket címkéknek nevezik), azaz a gyökér vagy a fa csúcsa alatt két szinttel helyezkedik el. A legtöbb DNS név két vagy több címkéből áll, és minden címke a fa egy szintjének felel meg. A nevekben a címkéket pontok választják el.

A tartomány gyökere a fa csúcsa, egy meg nem nevezett szint, melyet néha a nulla értéket képviselő két egymás melletti idézőjel ("") ábrázol. A DNS névben a gyökeret egy záró pont mutatja (.), ami azt jelzi, hogy a név a gyökér szintjén, a tartományi hierarchiában legfelül található (root). A példában a DNS tartománynév megadása teljesnek tekinthető, és az a névtérfa pontosan meghatározott helyére mutat. Az így megadott neveket teljesen minősített tartományneveknek nevezik (FQDN). A nevet egy pont (.) zárja le, például a „pelda.microsoft.com." névben látható módon. A legfelső szintű tartományban egy két vagy három betűből álló név azonosítja az országot vagy körzetet, illetve a nevet használó szervezetet típusát. Például a ".com" azt jelzi, hogy a név az Interneten üzleti célú felhasználásra van regisztrálva. A második szintű tartományban az Interneten egy magánszemélyt vagy szervezetet egy változó hosszúságú név azonosít. Ezek a nevek mindig egy legfelső szintű tartományhoz tartoznak, attól függően, hogy a nevet milyen szervezetben vagy földrajzi helyen használják. A második szintű „microsoft.com." nevet a Microsoft számára regisztrálta az internetes tartományneveket bejegyző szolgáltató. A következő szint az altartomány: Egy szervezet további neveket képezhet, amelyek a regisztrált második szintű tartománynévből származnak. Ezek a nevek egy szervezeten belül egy DNS-fát képeznek a szervezeti egységek vagy földrajzi helyek alapján. A „pelda.microsoft.com." név a Microsoft által kijelölt fiktív altartománynév. Az utolsó szint neve az állomás vagy erőforrás neve: Ezek a nevek a DNS fában egy levelet jelképeznek és egy adott erőforrást azonosítanak. A DNS tartománynév bal szélső címkéje általában egy adott számítógépet azonosít a hálózaton. Ha például a név egy A típusú erőforrásrekordban található, akkor az az IP cím hozzárendelésére szolgál. Az „a-allomas.pelda.microsoft.com." név első címkéje („a-allomas") a hálózaton található adott számítógép DNS-neve.

A DNS lekérdezés működése

Ha egy DNS ügyfélnek meg kell keresnie egy program által használt nevet, lekérdezést küld a DNS kiszolgálóknak a név feloldására. Az ügyfél által küldött lekérdezések három információt tartalmaznak, amelyek a kiszolgáló által megválaszolandó kérdést képezik:

- Egy meghatározott DNS tartománynév teljesen minősített tartománynévként megadva
- Egy meghatározott lekérdezéstípus, amely egy lekérési művelet speciális típusát, vagy egy erőforrásrekordot határozhat meg típus szerint
- A DNS tartománynév egy adott osztálya.

Windows DNS kiszolgálók esetén ezt mindig Internet (IN) osztályként kell meghatározni.

A megadott név lehet például egy számítógép teljesen minősített tartományneve (például „a-allomas.pelda.microsoft.com”), és az A rekord kereséséhez megadott lekérdezéstípus. A DNS lekérdezést egy olyan kérdésként lehet elképzelni, melyet az ügyfél tesz fel a kiszolgálónak, például: „Van A rekordja az 'allomasnev.pelda.microsoft.com.' nevű számítógéphez?” A kiszolgáló válaszának beérkezésekor az ügyfél elolvassa és értelmezi a válaszban szereplő A rekordot, és ezzel meghatározza a név szerint lekért számítógép IP címét.

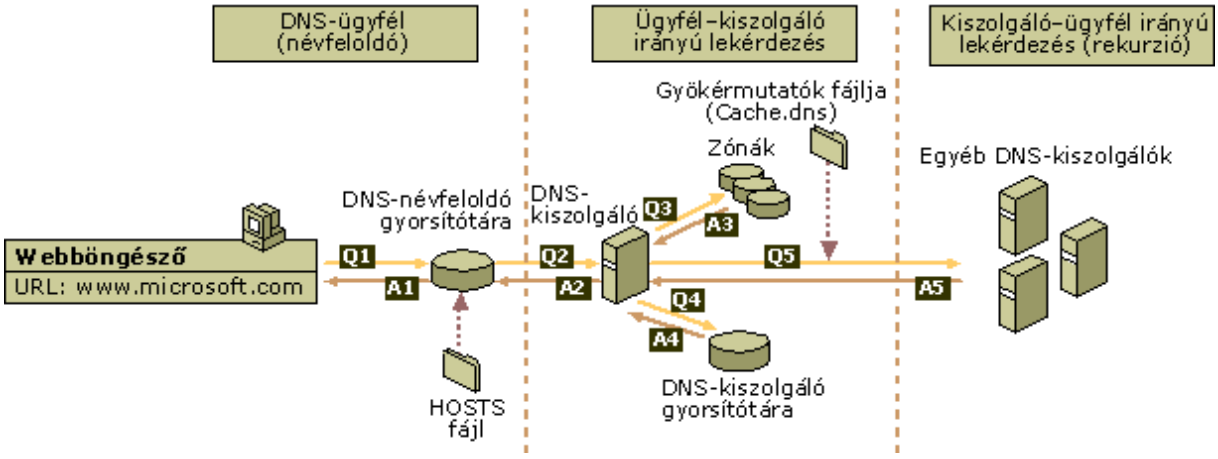
A DNS lekérdezések megválaszolása számos módon történhet. Az ügyfelek néha helyileg is válaszolhatnak a lekérdezésekre a korábbi lekérdezések alapján létrehozott gyorsítótár használatával. A lekérdezések megválaszolására a DNS kiszolgálók felhasználhatják saját gyorsítótárukat, melyben az erőforrásrekordokra vonatkozó információk szerepelnek. A DNS kiszolgáló lekérdezhet más DNS kiszolgálókat és kapcsolatba léphet azokkal az ügyfél nevében, majd visszaküldi a választ az ügyfélnek. Ez a művelet rekurzió néven ismert.

Ezenkívül az ügyfél is megpróbálhat kapcsolatba lépni más DNS kiszolgálókkal egy név feloldása érdekében. Ehhez a kiszolgálóktól kapott válaszok alapján további lekérdezéseket küld. Ez a művelet iteráció néven ismert.

A DNS lekérdezési művelet általában két részből áll:

- A névlekérdezés az ügyfélszámítógépnél indul, mely a DNS ügyfél szolgáltatásnak adja át a lekérdezést feloldás céljából.
- Ha a lekérdezés helyileg nem oldható fel, DNS kiszolgálók vehetők igénybe a névfeloldáshoz.

1. Helyi névfeloldó lekérdezése



A lekérdezési folyamat azzal kezdődik, hogy egy, a helyi számítógépen futtatott program DNS tartománynevet használ. A lekérést a DNS ügyfél szolgáltatás fogadja, mely a helyi gyorsítótárban tárolt információk alapján próbálja feloldani a nevet. Ha a lekérdezett név megtalálható a gyorsítótárban, akkor a szolgáltatás megválaszolja a lekérdezést, és a folyamat véget ér.

A helyi gyorsítótárban lévő információk két forrásból származhatnak:

•Ha van konfigurált helyi Hosts fájl, akkor a DNS ügyfél szolgáltatás indításakor a rendszer betölti a fájlban lévő hozzárendelési információkat a gyorsítótárba.

•A korábbi DNS lekérdezésekre küldött válaszból származó erőforrásrekordok a gyorsítótárba kerülnek és az ott beállított TTL (élettartam) érték idejéig ott maradnak.

Ha a helyi gyorsítótár alapján nem lehet megválaszolni a lekérdezést, akkor az ügyfél lekérdezést küld egy DNS kiszolgálónak a név feloldása érdekében.

2. DNS kiszolgáló lekérdezése

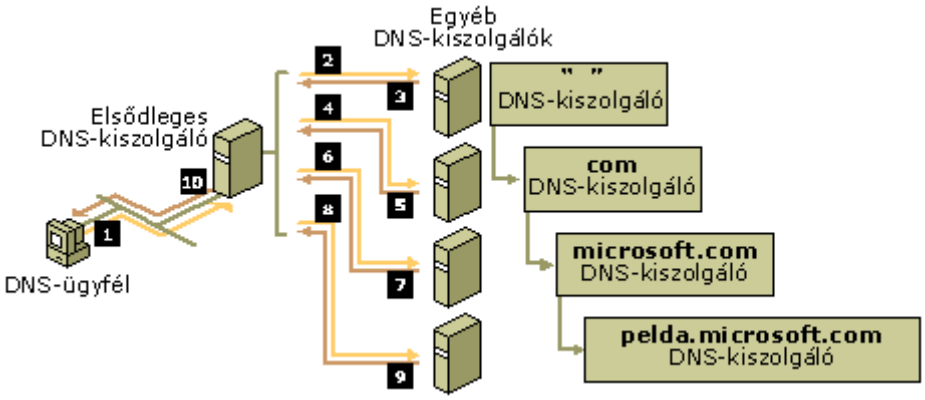
Amint azt az előző ábra mutatja, az ügyfél lekérdez egy elsődleges DNS kiszolgálót. A rendszer kiválasztja a folyamat első részében használt aktuális kiszolgálót egy globális listából. Ebben a keresési listában a kiszolgálók prioritási sorrendben szerepelnek. A lista minden olyan elsődleges és másodlagos DNS kiszolgálót tartalmaz, amely a rendszer aktív hálózati kapcsolataihoz be van állítva. Az elsődleges DNS kiszolgálók kapják a legnagyobb prioritást. Ha nincs elérhető elsődleges DNS kiszolgáló, a rendszer a másodlagos

kiszolgálókat használja. Ha pedig egy kiszolgáló nem válaszol, akkor átmenetileg lekerül a listáról.

A DNS kiszolgáló a lekérdezés beérkezésekor ellenőrzi, hogy a helyileg beállított zónájában lévő erőforrásrekord-információk alapján képes-e mérvadóan megválaszolni a lekérdezést. Ha a lekérdezett név megegyezik a helyi zónainformációk egyik erőforrásrekordjával, a kiszolgáló mérvadóan válaszol, és feloldja a lekérdezett nevet.

Ha a lekérdezett névhez nem található zónainformáció, a kiszolgáló ellenőrzi, hogy képes-e feloldani a nevet a korábbi lekérdezések gyorsítótárazott információi alapján. Ha van egyezés, a kiszolgáló megválaszolja a lekérdezést. Ha az elsődleges kiszolgáló képes a lekérdezés megválaszolására a gyorsítótár alapján, a lekérdezés befejeződik.

Ha a kiszolgáló gyorsítótára vagy zónainformációi alapján a lekérdezést nem lehet megválaszolni, a lekérdezés rekurzió használatával folytatódik. Ennek során a lekérdezés megválaszolásához más DNS kiszolgálók is lekérdezhetők. Alapértelmezés szerint a DNS ügyfél szolgáltatás azt kéri, hogy a kiszolgáló rekurziót használjon az ügyfél nevében a válasz visszaküldése előtt. A legtöbb esetben a DNS kiszolgáló alapértelmezés szerint úgy van beállítva, hogy támogassa a rekurziót. Lásd az alábbi ábrát:



Ahhoz, hogy a DNS kiszolgáló megfelelően végezze a rekurziót, információkra van szüksége a DNS tartományi névtérben található más DNS kiszolgálókról. Ezek az információk a *gyökérútmutató* formájában érhetők el. A gyökérútmutató olyan erőforrásrekordok listája, melyeket a DNS-szolgáltatás használ olyan más DNS kiszolgálók megkeresésére, melyek

mérvadók a DNS tartományi névtérfa gyökere számára. A gyökérkiszolgálók a tartomány gyökeréhez és a DNS tartományi névtérfa legfelső szintjéhez mérvadók. A DNS kiszolgálók gyökérútmutatók használatával keresik meg a gyökérkiszolgálókat, ezzel képesek a rekurzió megvalósítására. Elméletileg ez a művelet bármely DNS kiszolgáló számára lehetővé teszi azoknak a kiszolgálóknak a megtalálását, amelyek a névtérfa valamelyik szintjén használt más DNS tartománynevekre mérvadók.

A „b-allomas.pelda.microsoft.com” név keresésekor például vegye számításba a rekurzió használatát, ha az ügyfél egyetlen DNS kiszolgálót kérdez le. A rekurzió akkor következik be, amikor egy DNS kiszolgáló és egy ügyfél először indul el, ezért helyi gyorsítótáruk még nem tartalmaz információkat a névfeloldások elvégzésére. Ez feltételezi, hogy az ügyfél által lekérdezett név egy olyan tartománynévre vonatkozik, amelyről a kiszolgáló nem rendelkezik adatokkal a konfigurált zónái alapján.

Az elsődleges kiszolgáló elsőként elemzi a teljes nevet és megállapítja, hogy szüksége van a legfelső szintű tartományhoz („com.”) mérvadó kiszolgáló helyére. Ezután iteratív lekérdezést küld a „com” DNS kiszolgálónak, és megszerzi a „microsoft.com” kiszolgáló hivatkozását. A „microsoft.com” kiszolgáló ezután választ küld, mely hivatkozást tartalmaz a „pelda.microsoft.com” DNS kiszolgálóra. Végül a rendszer kapcsolatba lép a „pelda.microsoft.com” kiszolgálóval. Mivel ez a kiszolgáló konfigurált zónáinak részeként tartalmazza a lekérdezett nevet, mérvadó választ küld a rekurziót kezdeményező kiszolgálónak. Amikor az eredeti kiszolgáló fogadja a mérvadó válasz szerzéséről értesítő választ, továbbítja azt a lekérdezést küldő ügyfélnek, és ezzel a rekurzív lekérdezés befejeződik.

A rekurzív lekérdezések a fentiek szerint végrehajtva nagy erőforrásigényűek lehetnek, azonban biztosítanak bizonyos előnyöket a DNS kiszolgáló számára a teljesítménnyel kapcsolatban. A rekurzió végrehajtása során például a rekurzív keresést végző DNS kiszolgáló információkhoz jut a DNS tartományi névtérről. Az információkat a kiszolgáló tárolja a gyorsítótárában, és felhasználhatja a jövőbeli lekérdezések megválaszolása során. Az információ mennyiségének növekedésével a gyorsítótár jelentős területet foglalhat a kiszolgáló memóriájából annak ellenére, hogy a DNS szolgáltatás minden egyes be- és kikapcsolásakor törlődik.

A névlekérdezés

A DNS keresések során az ügyfelek általában címkeresést hajtanak végre, ami egy másik számítógép A rekordjában tárolt DNS-neve alapján végrehajtott keresés. Ez a lekérdezés egy IP címet tartalmazó rekordot vár a válaszban.

A DNS a névkeresést is lehetővé teszi, így az ügyfelek akár egy meglévő IP cím alapján is megkereshetik egy számítógép nevét. A névkeresés egy kérdés formájában valósul meg, például: „Meg tudja mondani annak a számítógépnek a DNS nevét, amelynek IP címe 192.168.1.20?”.

A DNS-t eredetileg nem tervezték az ilyen lekérdezések támogatására. A névlekérdezés támogatásának egyik problémája abból a különbségből adódik, ahogy a DNS névtér a neveket szervezi és indexeli, és ahogy az IP címek kiadása történik. Ha az előző kérdés megválaszolásának egyetlen módja a DNS névtérben lévő összes tartomány keresése lenne, a névlekérdezés túl hosszú ideig tartana és túl sok műveletet igényelne.

A probléma megoldására a DNS szabványokban egy speciális tartományt határoztak meg (az in-addr.arpa tartományt), melynek segítségével megbízhatóan és egyszerűen elvégezhetők a névlekérdezések. A fordított névterek létrehozásához az in-addr.arpa tartományon belüli altartományokat az IP címekben lévő számok fordított sorrendjével alakították ki.

A tartományokat azért kell fordított sorrendben szerepeltetni minden oktett érték esetén, mert a DNS nevekkel ellentétben az IP címek olvasása balról jobbra, értelmezése viszont fordított értelemben történik. Az IP címek balról jobbra olvasva a legáltalánosabb információktól (IP hálózati címtől) haladnak az egyre pontosabb információk felé (IP állomás címe).

Az IP címekben lévő oktettek sorrendjét ezért meg kell fordítani az in-addr.arpa tartományfa felépítésekor. Az in-addr.arpa DNS fa IP címeit cégeknek lehet delegálni, amikor azok egy megadott IP címet vagy címtartományt kapnak az Internet által meghatározott címosztályokon belül.

A DNS-be épített in-addr.arpa tartományfa egy további rekordtípus (a PTR rekord) meghatározását is igényli. Ezt az erőforrásrekordot a rendszer egy olyan hozzárendelés

létrehozására használja, mely általában egy állomás DNS számítógépnevéhez tartozó A rekordnak felel meg annak címkeresési zónájában.

Az in-addr.arpa tartomány használata az összes olyan TCP/IP hálózaton érvényes, amely az Internet Protokoll 4-es verziójú (IPv4) címzésen alapul. Az Új zóna varázsló automatikusan feltételezi ennek a tartománynak a használatát, amikor egy új névkeresési zónát hozunk létre.

Ha egy 6-os verziójú IP hálózatra (IPv6) telepíti a DNS-t és állítjuk be a névkeresési zónákat, az Új zóna varázslóban megadhatunk egy konkrét nevet. Ez lehetővé teszi olyan névkeresési zónák létrehozását a DNS-konzolban, amelyek felhasználhatók az eltérő tartománynevet (ip6.int tartományt) használó IPv6-hálózatok támogatására.

Nézzünk egy példát a névlekérdezésre egy szabványos IPv4 alapú hálózaton. A következő ábra olyan névlekérdezést mutat be, amelyet egy DNS-ügyfél (b-allomas) kezdeményezett egy másik állomás (a-allomas) nevének megszerzése érdekében annak IP címe alapján (192.168.1.20).

Példa névlekérdezésre

Az ábrán látható módon a névlekérdezés a következő lépések végrehajtásával történik:

1. Az ügyfél („b-allomas”) lekérdezi a DNS kiszolgálótól azt a PTR rekordot, mely az „a-allomas” IP címéhez (192.168.1.20) van rendelve.

   Mivel a lekérdezés a PTR rekordra vonatkozik, a feloldó megfordítja a címet és az in-addr.arpa tartományt hozzáfűzi a fordított cím végéhez. Ez alkotja a névkeresési zónában keresendő teljesen minősített tartománynevet („20.1.168.192.in-addr.arpa.”).

2. Ha a keresett információkat a rendszer megtalálja, a „20.1.168.192.in-addr.arpa” tartomány mérvadó DNS-kiszolgálója elküldi a PTR rekordot. Ez tartalmazza az „a-allomas” DNS-tartománynevét, így a névkeresési művelet befejeződik.

DNS kiszolgáló telepítése

Telepítéshez ajánlott a számítógépet úgy beállítani, hogy statikus IP címet használjon. Ha a DNS-kiszolgáló úgy van beállítva, hogy a DHCP szolgáltatással kiosztott dinamikus címeket használjon, amikor a DHCP kiszolgáló új címet ad ki a DNS kiszolgáló számára, a DNS kiszolgáló korábbi IP címének használatára beállított DNS ügyfelek nem tudják feloldani a korábbi IP címet, és nem fogják tudni megtalálni a DNS kiszolgálót. Ha Internetről érkező névfeloldási kérelmeket is teljesíteni akarunk, akkor olyan címet kell választanunk, amely az Interneten látható.

A telepítés az alábbi egyszerű lépésekből áll:

1. Nyissuk meg a Windows-összetevők varázslót (Start menü/Vezérlőpult/Programok telepítése és törlése).

2. Az **Összetevők** listában jelöljük be a **Hálózati szolgáltatások** jelölőnégyzetet, majd kattintsunk a **Részletek** gombra.

3. A **Hálózati szolgáltatások alösszetevői** listában jelöljük be a **Tartománynévrendszer (DNS)** jelölőnégyzetet, kattintsunk az **OK**, majd a **Tovább** gombra.

4. Amikor a program kéri, a **Fájlok másolása a következő helyről** mezőbe írjuk be a terjesztési fájlok teljes elérési útját, majd kattintsunk az **OK** gombra. A szükséges fájlokat a telepítőprogram a merevlemezre másolja.

Zónák ismertetése

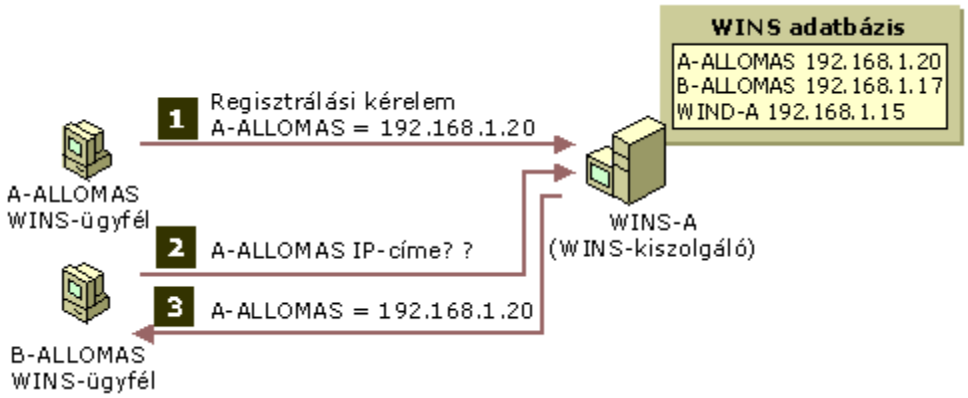
A tartománynévrendszer (DNS) lehetővé teszi a DNS-névtér felosztását zónákra, amelyek egy vagy több DNS tartományról tárolnak névinfomrációkat.

Fontosnak érzem, hogy kihangsúlyozzam a zónák és a tartományok közötti különbséget. A zóna először egy DNS tartománynév adatbázisának szerepét tölti be. A zóna létrehozásához használt tartomány alá hozzáadott tartományok lehetnek ugyanannak a zónának a részei, vagy tartozhatnak más zónához. A hozzáadott altartomány a következők valamelyike lehet: -Az eredeti zónarekordok részeként kezelt vagy belefoglalt; -Az altartomány támogatására létrehozott más zónához delegált.

A DNS-kiszolgáló telepítése után eldönthetjük, hogyan felügyeljük azt és annak zónáit. Bár lehetőség van a kiszolgáló rendszerindítási és zónafájljainak módosítására szövegszerkesztővel, ez a módszer nem ajánlott. A DNS-konzol és a DNS parancssori eszköze, a **dnscmd** program egyszerűvé teszik ezeknek a fájloknak a karbantartását, és mindig ezeket kell használni, amikor csak lehetséges. Ha megkezdjük a fájlok kezelését a konzol vagy a parancssori eszköz használatával, a fájlok közvetlen szerkesztése már nem ajánlott.

WINS

A Windows Internet Name Service (WINS) szolgáltatás olyan dinamikus, replikált adatbázis-szolgáltatást nyújt, amely segítségével lehetőségünk van NetBIOS nevek regisztrálására, illetve hálózaton használt IP címek hozzárendelésére. A WINS segítségével a Microsoft Windows Server 2003 alapú szerverünk NetBIOS névkiszolgálóként is működhet, a TCP/IP feletti NetBIOS (NetBT) szabványainak megfelelően regisztrálhatja és rendelheti hozzá a hálózaton található azon ügyfélszámítógépek nevét, amelyek számára a WINS engedélyezett. Tehát a WINS IP címekhez rendeli a NetBIOS neveket, és arra szolgál, hogy kiküszöbölje az útválasztásos környezetek NetBIOS névhozzárendeléséből eredő problémákat. A NetBIOS neveket a régebbi rendszerek használják, kifutóban vannak, de a régebbi Microsoft rendszerekkel történő kommunikációhoz elengedhetetlenek. A WINS egyszerűbbé teszi a NetBIOS névtér kezelését a TCP/IP alapú hálózatokban. A következő ábrán egy példa látható a WINS működésére.



Példa a WINS működésére

Ebben a példában a következő eseményeket figyelhetjük meg:

1. Az egyik WINS ügyfél (A állomás) beállított WINS kiszolgálójával (WINS-A) valamelyik helyi NetBIOS nevét regisztrálja.
2. Egy másik WINS ügyfél (B állomás) lekérdezi a WINS-A kiszolgálót, hogy megkeresse az A állomás IP címét a hálózaton.
3. A WINS-A megadja az A állomás IP címét (192.168.1.20).

A WINS lehetővé teszi, hogy a felhasználók könnyen megtalálják a távoli hálózatokat. Egy ügyfél gép hálózatra csatlakozásakor automatikusan sor kerül WINS regisztrációkra, ezért a dinamikus címek konfigurációjának módosításakor automatikusan frissül a WINS adatbázis. Ha például egy DHCP kiszolgáló új vagy módosított IP címet ad ki a WINS szolgáltatást használó ügyfélszámítógépnek, akkor frissülnek az ügyfél WINS adatai. Mindehhez nincs szükség a felhasználók vagy a hálózati rendszergazda beavatkozására.
A WINS egyik legnagyobb előnye az, hogy támogatja a hálózat korábbi NetBIOS alapú ügyfeleit, engedélyezi, hogy ezek az ügyféltípusok távoli Windows tartományok listáit böngésszék anélkül, hogy minden alhálózaton szükség lenne helyi tartományvezérlő jelenlétére. Másik előnye, hogy támogatja a DNS alapú ügyfeleket az úgynevezett WINS keresés integrálásával, így a DNS ügyfelek is megtalálhatják a NetBIOS erőforrásokat.

DNS újdonságok a Windows Server 2003-ban

A DNS a következő újdonságokkal bővült a Windows Server 2003 termékcsaládban.

Az Active Directory beépített DNS-zónáinak tárolása alkalmazás partíciókban

Ez a szolgáltatás lehetővé teszi, hogy a DNS-zónákat az Active Directory egy alkalmazás partíciójában tároljuk. A DNS-adatok alkalmazás partícióban történő tárolásával csökkenthető a globális katalógusban tárolt objektumok mennyisége. Ha alkalmazás partíció tárolja a DNS-zónaadatokat, a rendszer csak az alkalmazás partícióban megadott tartományvezérlőkre replikálja az adatokat. Alapértelmezés szerint a DNS-specifikus alkalmazás partíciók csak a DNS kiszolgálót futtató tartományvezérlőket tartalmazzák. Emellett a DNS-zónaadatok alkalmazás partícióban történő tárolása lehetővé teszi, hogy a DNS-zónát az Active Directory-erdő más tartományaiban futó DNS kiszolgálókra replikálhassuk. Ez az ajánlott megoldás abban az esetben, ha az Active Directoryval integrált DNS-zónák Windows Server 2003 alapú DNS kiszolgálón helyezkednek el.

Alapszintű kompatibilitás a DNS biztonsági bővítményeivel

A Windows Server 2003 DNS kiszolgálója az IETF (*Internet Engineering Task Force*) RFC 2535-ös szabványában leírt DNS biztonsági protokollal alapszintű kompatibilitást nyújt. A Windows Server 2003 a szabványban leírt rekordtípusok (KEY, SIG és NXT) tárolására alkalmas, és az RFC 2535 szabvány szerint ezeket a rekordokat alkalmazza a lekérdezésekre adott válaszokban. A kiszolgáló nem biztosít teljes kompatibilitást, és nem hajtja végre az RFC 2535 szabványban előírt titkosítási műveleteket (KEY/SIG rekordok létrehozása, üzenetek aláírása és az aláírások ellenőrzése). A kiszolgáló azonban tárolhatja és használhatja a más gyártót által készített szoftverrel létrehozott szabványos KEY és SIG rekordokat.

A Windows Server 2003 DNS kiszolgálókat másodlagos kiszolgálóként használható egy az RFC 2535-öt teljes mértékben támogató DNS kiszolgáló által aláírt zóna esetében.

Helytelenül konfigurált DNS észlelése a módosított tartománycsatlakoztatási eljárással

Ez a szolgáltatás egyszerűbbé teszi a helytelen DNS-konfiguráció felderítését és jelentését, valamint segít a DNS-infrastruktúra megfelelő beállításaiban a számítógépek tartományhoz való csatlakoztatása során. Ha az Active Directory tartományhoz csatlakozni próbáló számítógép nem talál tartományvezérlőt, mert például helytelen a DNS konfigurációja vagy a tartományvezérlők nem érhetők el, a szolgáltatás hibakeresést hajt végre a DNS-infrastruktúrában. A művelet végén elkészülő jelentés tartalmazza a hiba okát és a megoldási javaslatot.
Ha a DNS-infrastruktúra konfigurációja megfelelő, a számítógép csatlakozik a tartományhoz, és a szolgáltatás láthatatlan marad a rendszergazda számára. Ha azonban a DNS-konfiguráció helytelen, és a számítógép emiatt nem talál tartományvezérlőt, azaz nem tud tartományhoz csatlakozni, a szolgáltatás értesíti erről a rendszergazdát.

DNS ügyfelek kezelése csoportházirenddel

Ezzel a szolgáltatással a rendszergazdák csoportházirend használatával adhatják meg a Windows Server 2003-as DNS ügyfelek beállításait. Ez egyszerűbbé teszi a tartomány tagjain a DNS konfigurációt (például a DNS-rekordok ügyfél általi dinamikus regisztrációjának engedélyezése és letiltása, az elsődleges DNS-előtag visszafejtésének használata a névhozzárendelés során és a DNS-utótagok keresési listáinak feltöltése). Az egyszerűsített

felügyelet mellett fontos szerepet játszik a DNS-előtagok kezelése a csoportházirenddel. Erre a szolgáltatásra a NetBIOS nélküli környezetekre való áttérésnél van szükség.

A rendszergazdák a DNS ügyfelek konfigurálására használhatják ezt a csoportházirend-szolgáltatást.

Helyettes (stub) zónák és feltételes továbbítás

A helyettes zónák és a feltételes továbbítás a DNS kiszolgálók két olyan szolgáltatása, amellyel a DNS-adatforgalom útválasztása felügyelhető a hálózatokban. A helyettes zónák lehetővé teszik, hogy a DNS kiszolgálók a zóna teljes másolatának tárolása vagy a DNS-gyökérkiszolgálóknak küldött lekérdezések nélkül tudomást szerezzenek a zónák teljes másolataira jogosult kiszolgálók nevéről és címéről. A Windows 2000 rendszerű DNS kiszolgálók csak úgy állíthatók be, hogy a DNS kiszolgálók egy csoportjának továbbítsák a DNS lekérdezéseket. A Windows Server 2003 feltételes továbbítási szolgáltatása névtől függő továbbítást is támogat. A DNS kiszolgálók például a következő műveletek egyidejű végrehajtására is beállíthatók:

A usa.microsoft.com végződésű nevekre irányuló lekérdezések továbbítása a DNS kiszolgálók első csoportjának.
A europe.microsoft.com végződésű nevekre irányuló lekérdezések továbbítása a DNS kiszolgálók második csoportjának.
Az összes többi lekérdezés továbbítása a DNS kiszolgálók harmadik csoportjának.
A rendszergazdák a hálózat DNS-adatforgalmának útválasztását felügyelhetik ezzel a szolgáltatással.

Az EDNS0 protokoll támogatása

Az RFC 2671 szabványban definiált EDNS0 protokoll segítségével a DNS kiszolgálók 512 oktettnél nagyobb méretű UDP DNS üzeneteket fogadhatnak és továbbíthatnak. Ez a szolgáltatás akkor lehet hasznos a rendszergazdák számára, amikor a DNS-válaszok, például a helyi Active Directory tartományvezérlőkre vonatkozó SRV-lekérdezések mérete meghaladja az 512 oktettet. A Windows Server 2003 termékcsalád előtti verziókban a válaszoknak több körbejárásra volt szükségük a TCP-munkamenetek létrehozásához és megszakításához. A Windows Server 2003 termékcsaládban az EDNS0 protokoll használatával a válaszok

többsége egyetlen UDP-körbejárással visszaadható TCP-munkamenet létrehozása és megszakítása nélkül.

További fejlesztések

A Windows Server 2003 DNS kiszolgáló szolgáltatása a következő kiegészítő fejlesztéseket tartalmazza:
Round Robin statikus terhelés elosztási támogatás az RR (*Resource Rekord*) rekord-típushoz
A DNS kiszolgáló alapértelmezés szerint minden RR rekordnál végrehajtja Round Robin műveletet.
Továbbfejlesztett hibakeresési naplózás
A DNS kiszolgáló továbbfejlesztett hibakeresési naplója a DNS problémáinak megoldásához nyújt segítséget.

A Névkiszolgáló (NS) erőforrásrekord regisztrálásának kiszolgáló és zóna alapú automatikus vezérlése.

WINS újítások a Windows Server 2003-ban

A Windows Server 2003 WINS (*Windows Internet Name Service*) szolgáltatása a következő fejlesztésekkel egészült ki.

Rekordok szűrése

A továbbfejlesztett szűrési és az új keresési függvények segítségével kereshetők meg a megadott feltételeknek megfelelő rekordok. Ezek a függvények különösen hasznosak lehetnek az igen nagyméretű WINS-adatbázisok elemzésekor. A WINS-adatbázisokban több feltételen alapuló összetett keresések is végrehajthatók. A továbbfejlesztett szűrési szolgáltatással egyéni és pontos eredményeket adó lekérdezések állíthatók össze. A választható szűrők a következők: a rekord tulajdonosa, a rekord típusa, a NetBIOS-név, valamint az IP cím alhálózati maszkkal vagy anélkül.

A lekérdezések eredményei a helyi számítógép memóriájának gyorsítótárában tárolhatók, ami növeli a soron következő lekérdezések teljesítményét, egyúttal csökkenti a hálózat forgalmát.

Replikációs partnerek elfogadása

A szervezet replikációs stratégiájának meghatározásakor egy olyan lista állítható össze, amely a bejövő névrekordok forrását vezérli a WINS-kiszolgálók közötti lekéréses (*pull*) replikáció során. A meghatározott replikációs partnerektől származó névrekordok blokkolása mellett lehetőség van arra is, hogy csak azokat a névrekordokat fogadjuk el, amelyek megadott WINS-kiszolgálók tulajdonában vannak. A listában nem szereplő WINS kiszolgálók névrekordjait a replikáció során elutasítják.

Active Directory

Az LDAP protokollon alapuló megoldásoknak az 1990-es évek közepén bekövetkező terjedése arra inspirálta a vállalatokat, hogy címtárakkal 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. 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.

Az Active Directory a Windows Server 2003 Standard Edition, Enterprise Edition és Datacenter Edition címtárszolgáltatása. A címtárszolgáltatás nem más, mint a címtáradatok forrása, illetve az adatok elérését és használatát biztosító szolgáltatás együtt. A címtárszolgáltatás segítségével a felhasználók bármelyik objektumot megtalálhatják a címtárban az objektum valamelyik attribútuma alapján. Az Active Directory a hálózati objektumokra vonatkozó adatokat tárol, és egyszerűen hozzáférhetővé és felhasználhatóvá teszi azokat a rendszergazdák, valamint a felhasználók számára. Az Active Directory strukturált adattárolása révén lehetőség van a címtáradatok logikus, hierarchikus rendszerezésére. Ez az adattároló vagy más néven címtár egy olyan információforrás, amely személyekről, fájlokról és más Active Drirectory objektumukról tartalmaz adatokat. A fájlrendszerekben a címtár a fájlok információit tartalmazza. Ugyanez egy megosztott számítógépes környezetben, például egy Windows tartományban, a különböző objektumokról tartalmaz információkat (ilyen objektumok lehetnek a nyomtatók, a faxkiszolgálók, az alkalmazások, az adatbázisok és más felhasználók). Az Active Directory integrált rendszerbiztonsági szolgáltatása tartalmazza a bejelentkezési azonosítást, illetve az

objektumokhoz való hozzáférés szabályozását. A rendszergazdák egyetlen bejelentkezéssel kezelhetik a címtáradatokat a teljes hálózaton, a hitelesített hálózati felhasználók pedig a hálózaton bárhol hozzáférhetnek az erőforrásokhoz. A felügyeleti rendszer alapját képező házirend megkönnyíti a legbonyolultabb hálózat felügyeletét is.

Az Active Directory ugyan nem telepíthető Windows Server 2003, Web Edition rendszert futtató kiszolgálóra, de a kiszolgáló tagkiszolgálóként csatlakozhat egy Active Directory tartományhoz.

Az Active Directory részegységei

Séma: szabályok készlete, amely meghatározza a címtárban lévő objektumok és attribútumok osztályait, az objektumokra vonatkozó megkötéseket és korlátokat, valamint nevük formátumát. A séma objektumosztályokból és attribútumokból áll. Az alapséma (vagy alapértelmezett séma) sokféle objektumosztályt és attribútumot tartalmaz, így a legtöbb szervezet igényeit kielégíti. Az alapséma modellezése a Nemzetközi Szabványügyi Szervezet (ISO) – címtárszolgáltatásokra vonatkozó –X.500 szabványát követi. Az alapséma bővíthető, ezért osztály és attribútumai módosíthatók, illetve új osztályok és attribútumok adhatók hozzá. Hozzá kell tennem, hogy nagyon körültekintően kell eljárni bármilyen módosításnál, mert a séma bővítése a teljes hálózatot érinti.

Globális katalógus: tartalmazza a címtár összes objektumának adatait. Segítségével a felhasználók és rendszergazdák megkereshetik a címtáradatokat függetlenül attól, hogy ténylegesen a címtár melyik tartománya tartalmazza azokat. A globális katalógusban lévő tartományi objektumok részleges másolatai a felhasználói keresésekkor leggyakrabban használt attribútumokat tartalmazzák. Ezek az attribútumok sémadefiníciójukban meg vannak jelölve a globális katalógusba való felvételre. A tartományi objektumok leggyakrabban keresett attribútumainak a globális katalógusban való tárolása révén a felhasználók hatékonyan tudnak keresni anélkül, hogy a hálózat teljesítményét a tartományvezérlőkhöz történő szükségtelen átirányításokkal terhelnék.

Lekérdezési és indexelési rendszer, amellyel a hálózati felhasználók és alkalmazások objektumokat és azok tulajdonságait tehetik közzé, illetve kereshetik meg.

Replikációs szolgáltatás: a címtáradatokat terjeszti a hálózaton. A tartomány összes tartományvezérlője részt vesz a replikációban, és tartalmazza a tartományára vonatkozó

címtáradatok összességét. A címtáradatok bármilyen módosítását a rendszer a tartomány összes tartományvezérlőjére replikálja.

Ügyfélszoftverek: Az Active Directory ügyfélszoftvereinek támogatása, melynek köszönhetően a Microsoft Windows 2000 Professional vagy Windows XP Professional rendszerek számos szolgáltatása a Windows 95, Windows 98 és Windows NT Server 4.0 rendszert futtató számítógépeken is elérhetővé válik. Ha a számítógépen nem fut Active Directory ügyfélszoftver, a címtár Windows NT címtárként jelenik meg.

Végszó

A Windows Server 2003 nagy mérföldkőnek számít a Microsoft történetében. Ez az első olyan operációs rendszer, ahol külön kódbázisra épült az asztali és a kiszolgálókba szánt verzió. Továbbá minden eddiginél nagyobb figyelmet fordítottak az oly sokat kritizált biztonsági problémákra. A Windows Server 2003 hálózati megoldásai nagyon sokrétűek, teljes összefoglalásukra egy több száz oldalas dokumentáció is kevés lenne. Dolgozatomban igyekeztem a vállalatok által legtöbbet használt technológiákat bemutatni. Ezek azok a technológiák, amelyek segítségével könnyebbé válik a rendszeradminisztrátorok munkája, és átláthatóbbá válik az egész rendszer. Igaz, hogy csak alapszinten mutattam be az egyes eszközöket, de véleményem szerint ez az alapszintű tudás elengedhetetlen egy jó szakember számára, mert egy vállalat informatikai struktúrájának működése létkérdés a mai világban és ezen alapismeretek birtokában sokkal körültekintőbben lehet megtervezni egy adott hálózati infrastruktúrát. Remélem, hogy az Olvasó hasznos újdonságokat fedezett fel a dolgozatban és legalább olyan érdekesnek találta a hálózatkezelés témakörét, mint én.

Irodalomjegyzék és hivatkozások

J.C. Mackin and Ian McLean:

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

MD Deborah Littlejohn Shinder, Dr. Thomas W. Shinder:

Exam 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Study Guide), Syngress Publishing Inc. 2003

Craig Zacker:

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

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

Mark Minashi, Christa Anderson, Michele Beveridge, C.A. Callahan, Lisa Justice:

Mastering Windows Server 2003, Sybex 2003

William Boswell:

Inside Windows Server 2003, Addison Wesley 2003

A Microsoft Windows Server 2003 hivatalos honlapja:

http://www.microsoft.com/windowsserver2003/default.mspx

Egyéb hivatkozások:

http://www.sulinet.hu/tart/fkat/Kaac