PEARSON Education

ADDISON-WESLEY

Eric Tierling

Windows Server 2003

Einrichtung, Verwaltung, Referenz

2., aktualisierte Auflage

ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City • Madrid • Amsterdam

3 Windows Server 2003 im Netzwerkeinsatz

Windows Server 2003 steht für Networking. Wie sich ein Netzwerk logisch organisieren lässt, welche Protokolle zur Kommunikation miteinander zum Einsatz kommen und was es mit der Namensauflösung auf sich hat, erfahren Sie auf den nachfolgenden Seiten.

3.1 Organisationsformen für die Ressourcen des Netzwerks

Damit Zugriffe auf die im Netzwerk vorhandenen Ressourcen möglich sind, muss eine Organisationsform existieren. Windows Server 2003 unterstützt sowohl die Peer-to-Peer- als auch die Client/Server-Organisationsform.

3.1.1 Peer-to-Peer und Arbeitsgruppen

In den Anfängen der Vernetzung kam es vor allem darauf an, auf die Ressourcen anderer Rechner zuzugreifen. Ein – beliebiger, in das Netzwerk eingebundener – PC gibt dabei beispielsweise einen Ordner oder einen an ihn angeschlossenen Drucker im Netzwerk frei und agiert damit als *Server* (da er Ressourcen zur Nutzung durch die an anderen PCs sitzenden Benutzern freigegeben hat). Die anderen Rechner im Netzwerk sind nun in ihrer Funktion als *Clients* dazu in der Lage, auf die so freigegebenen Ressourcen anderer (Server-) Rechner im Netzwerk zuzugreifen. Dieses Verfahren ist als *Peer-to-Peer* bekannt:

Peer bedeutet so viel wie »gleichgestellt« oder »ebenbürtig« und deutet an, dass alle Peer-to-Peer-Teilnehmer gleichberechtigt miteinander kommunizieren.

Jeder Teilnehmer kann sowohl als Server als auch als Client agieren.

Gemeinsam nutzbare Ressourcen (beispielsweise freigegebene Dateien) befinden sich dezentral auf den einzelnen Computern. Eine Speicherung auf zentralen Servern findet nicht statt.

Einen zentralen Server gibt es bei der Peer-to-Peer-Technik nicht. Tritt beim Peer-to-Peer-Networking ein Computer als Server auf, so bedeutet das lediglich, dass er seine Ressourcen freigegeben hat und andere Teilnehmer darauf zugreifen können.

Peer-to-Peer ist auch unter der Abkürzung *P2P* bekannt.

Durch das Freigeben einer Ressource zur gemeinsamen Nutzung kommt eine *Freigabe* zustande, die einen eindeutigen Namen aufweist. Andere Benutzer können von ihren PCs aus alle freigegebenen Ressourcen sehen (falls diese nicht versteckt freigegeben sind) und auf diese Freigaben zugreifen. Voraussetzung dazu ist, dass die betreffenden Benutzer für die jeweilige Freigabe über entsprechende Berechtigungen verfügen, diese auch tatsächlich zu nutzen.

Beim Peer-to-Peer-Networking besitzt jede im Netzwerk zur Verfügung stehende Ressource einen Freigabenamen. Zudem gibt es ein schützendes Kennwort, um ungewollte Zugriffe zu verhindern.

Grundsätzlich unterscheidet man beim Peer-to-Peer-Networking in einem Microsoft-Netzwerk folgende Arten, was die Erteilung von Berechtigungen für den Zugriff auf Freigaben und somit ihre Zugriffssteuerung betrifft:

Kennwort für jede Freigabe erforderlich (*Zugriffssteuerung auf Freigabeebene*)
Um ungewollte Zugriffe zu verhindern, wird einer Freigabe bei ihrer Erstellung ein schützendes Kennwort zugeteilt. Jeder Benutzer im Netzwerk, der Kenntnis von diesem Kennwort besitzt, kann diese Ressource nutzen. Nach diesem Prinzip arbeiten standardmäßig zum Beispiel Windows für Workgroups und Windows 95/98/ME. Bei dieser Art der Zugriffssteuerung ist es nicht möglich, den Zugriff auf eine Ressource abhängig von dem Benutzer zu blocken – kennt er das Kennwort der Ressource, kann er diese auch nutzen. Jeder als Server agierende Rechner muss sich selbst in einer nur für ihn gültigen Datenbank merken, welche Ressourcen mit welchem Kennwort freigegeben sind.

Name und Kennwort eines Benutzers (*Zugriffssteuerung auf Benutzerebene*)
Hierbei führt jeder PC selber eine eigene Datenbank aller lokalen Benutzer (die *lokale Benutzerkonten-Datenbank*), wobei aus Sicherheitsgründen jeder Benutzer über ein persönliches Kennwort verfügt. Bei der Erstellung einer Freigabe ist nun festzulegen, welcher dieser lokal definierten Benutzer auf die Ressource in welchem Umfang zugreifen darf. Möchte nun ein an einem anderen Computer sitzender Anwender über das Netzwerk auf diese Freigabe zugreifen, muss er sich zunächst mit Benutzernamen und zugehörigem Kennwort bei diesem Rechner identifizieren. Hierbei handelt es sich um den Namen und das Kennwort eines Benutzers, der auf dem PC definiert sein muss, der auch die Freigabe bereitstellt. Nach diesem Prinzip arbeiten standardmäßig unter anderem Windows NT Workstation 4.0, Windows 2000 Professional und Windows XP Professional (sofern dort die Gast-Authentifizierung, die auch als einfache Dateifreigabe bekannt ist, deaktiviert und stattdessen klassische Authentifizierung und damit auch das klassische Freigabemodell, wie es von Windows 2000 Professional her bekannt ist, verwendet wird). Von da an lassen sich alle Freigaben nutzen, die auf diesem PC vorhanden sind und für die der betreffende Benutzer Berechtigungen besitzt. Die Angabe von Kennwörtern für jede Freigabe entfällt.

Windows 95/98/ME kann in Verbindung beispielsweise mit Windows XP Professional (sofern dort das klassische Freigabemodell verwendet wird), Windows 2000 Professional oder Windows NT Workstation 4.0 ebenfalls dafür konfiguriert werden, mit einer Zugriffssteuerung auf Benutzerebene zu arbeiten und so bei Freigaben exakt angeben zu können, welche Benutzer in welchem Umfang diese nutzen dürfen. Hierzu ist in den Netzwerk-Eigenschaften auf der Registerkarte ZUGRIFFSSTEUERUNG die Option ZUGRIFFSSTEUERUNG AUF BENUTZEREBENE zu aktivieren. Im sodann zugänglichen Eingabefeld BENUTZER- UND GRUPPENLISTE BEZIEHEN ist nun der Name eines Windows XP Professional-, Windows 2000- oder Windows NT 4.0-PCs einzugeben, auf dessen Benutzerkonten-Datenbank der Windows 95/98/ME-Rechner für die Zugriffssteuerung seiner Freigaben zurückgreifen soll.

Um eine möglichst große Flexibilität zu gewährleisten (das ist letztlich die Idee, die hinter dem Peer-to-Peer-Networking steckt), gibt es kaum Einschränkungen, welcher Benutzer in welchem Umfang auf welche Ressource zugreifen darf oder ob die Freigabe einer Ressource überhaupt erwünscht ist. Die Zugriffssteuerung auf Freigabeebene ist nur beim Einsatz in sehr kleinem Rahmen probat und für ernsthaftere Ansprüche kaum mehr geeignet, denn: Jeder, der das Kennwort weiß (oder »zufällig« davon erfahren hat), kann Zugriff auf die freigegebene Ressource erlangen und diese nutzen. Eine Unterscheidung zwischen verschiedenen Benutzern ist nicht möglich – was beispielsweise zur Folge hat, dass sich Anwender, deren »Spieltrieb« bekannt ist, nicht blocken und außen vor halten lassen, sobald diese um das Kennwort einer Freigabe wissen. Zudem ist es sehr mühselig, sich die Kennwörter der einzelnen Freigaben zu merken, die (allein aus Sicherheitsgründen) meist von Freigabe zu Freigabe verschieden sind. Benutzer müssen somit regelrechte Listen von Freigaben und ihren Kennwörtern führen. Ausgedruckt und an den Bildschirm des Arbeits-

platz-PCs geklebt, wie es in der Praxis durchaus zu beobachten ist, wird dann jeder Versuch sinnlos, Sicherheit ins Netz zu bringen und nicht allen Anwendern alles zu gestatten.

Besser hingegen verhält es sich mit der Zugriffssteuerung auf Benutzerebene: Hier sind alle Benutzer, die auf Freigaben zugreifen sollen, sauber mit Namen und Kennwort in der lokalen *Benutzerkonten-Datenbank* genau des PCs verzeichnet, der seine Ressourcen freigegeben hat.

Die lokale Benutzerkonten-Datenbank eines mit Windows NT 4.0 arbeitenden Rechners wird auch als *SAM-Datenbank* bezeichnet (SAM steht dabei für »Security Account Manager«). In einer Windows Server 2003- oder Windows 2000-Domäne werden Informationen über die im Netzwerk existierenden Benutzer stattdessen zentral im Active Directory hinterlegt.

Bei der Erstellung einer Freigabe wird nun exakt festgelegt, welcher dieser – lokal in der Benutzerkonten-Datenbank definierte – Benutzer die Freigabe nutzen darf. Zudem lässt sich angeben, in welchem Umfang eine Nutzung dieser freigegebenen Ressource erfolgen darf – einige Benutzer sollen möglicherweise nur lesenden Zugriff erhalten, während andere auch Änderungen durchführen können (also abhängig vom jeweiligen Benutzer und nicht von irgendeinem Kennwort). Der für die Anwender wahrscheinlich größte Vorteil der Zugriffssteuerung auf Benutzerebene liegt darin, sich zum Zugriff auf alle freigegebenen Ressourcen eines PCs nur noch ein einziges Kennwort merken zu müssen.

Windows XP Professional weist in dieser Hinsicht eine Besonderheit auf: Ist bei einem in das Netzwerk eingebundenen Windows XP Professional-PC die so genannte »einfache Dateifreigabe« aktiviert (was nach Ausführung des Netzwerkinstallations-Assistenten standardmäßig der Fall ist), finden alle über das Netzwerk getätigten Zugriffe auf den Windows XP Professional-PC als Gast-Benutzer statt – der nur eingeschränkte Berechtigungen aufweist. Während sich Windows XP Professional bei Bedarf auf das klassische Freigabemodell, wie es auch bei Windows 2000 Professional Verwendung findet, umstellen lässt, arbeitet Windows XP Home Edition zwingend mit dieser einfachen Dateifreigabe. Bei Windows Server 2003 dagegen existiert das Modell der einfachen Dateifreigabe nicht.

Freigaben werden beispielsweise in der Netzwerkumgebung aufgelistet. Je mehr Ressourcen freigegeben sind, desto größer und unüberschaubarer wird die Vielfalt der freigegebenen Ressourcen. Aus diesem Grund eignet sich das Peer-to-Peer-Networking vor allem für ein kleineres Netzwerk: Denn um auch bei einer Vielzahl freigegebener Ressourcen noch den Durchblick zu behalten, wurde das Verfahren der *Arbeitsgruppe* (englisch *Workgroup*) eingeführt. Hierbei handelt es sich um einen simplen Mechanismus, die in ein Netzwerk eingebundenen PCs sozusagen in einer Gruppe zusammenzufassen. Dieses Vorgehen soll es Anwendern erleichtern, Freigaben zu finden – indem sie sich an den Netzwerk-PCs orientieren, die Freigaben bereitstellen. Die im Netzwerk vorhandenen PCs werden sodann (etwa in der Netzwerkumgebung) in ihre jeweilige Arbeitsgruppe einsortiert dargestellt. Arbeitsgruppen dienen also dazu, die beim Peer-to-Peer-Networking freigegebenen Ressourcen logisch zu gruppieren.

Alle Betriebssysteme von Microsoft unterstützen die Teilnahme an einer Arbeitsgruppe zum Peer-to-Peer-Networking. Windows für Workgroups, Windows 95/98/ME, Windows NT, Windows 2000, Windows XP Professional und Windows Server 2003 verfügen bereits von Haus aus über die entsprechende Funktionalität und können ihre lokalen Ressourcen in einer Arbeitsgruppe freigeben (für DOS und das darauf aufsetzende Windows 3.1x ist ein entsprechendes Add-On erhältlich, um am Peer-to-Peer-Networking innerhalb einer Arbeitsgruppe teilzunehmen).

Welcher Arbeitsgruppe ein PC zugerechnet wird, ist bei der Installation seines Betriebssystems festzulegen (diese Einstellung lässt sich bei Bedarf auch im Nachhinein ändern). Wird dabei eine Arbeitsgruppe angegeben, die noch nicht existiert, kommt diese Arbeitsgruppe automatisch zustande. Eine zentrale Kontroll-Instanz gibt es dabei nicht.

Gleich, welches Verfahren – Zugriffssteuerung auf Freigabe- oder Benutzerebene – zum Einsatz gelangt: Beim Peer-to-Peer-Networking respektive in einer Arbeitsgruppe gibt es keine zentralen, klaren Verwaltungs- und Kontrollfunktionen. Was das bedeutet, lässt sich gut an einem kleinen Beispiel verdeutlichen: Stellen Sie sich vor, im Netzwerk befinden sich sechs PCs, die sich in einer gemeinsamen Arbeitsgruppe befinden. Alle Rechner sollen einige ihrer Ressourcen – Ordner auf ihrer lokalen Festplatte, CD/DVD-ROM-Laufwerke, Drucker etc. – im Netzwerk freigeben. Insgesamt kommen dafür jedoch neun Anwender in Betracht, die abwechselnd an den einzelnen Computern arbeiten. Das bedeutet: Es müssen alle neun Anwender in der lokalen Benutzerkonten-Datenbank eines jeden PCs eingerichtet werden.

Eine Möglichkeit, die lokalen Benutzerkonten-Datenbanken der einzelnen PCs in einem Peer-to-Peer-Netzwerk miteinander abzugleichen und zu synchronisieren, gibt es nicht (weder automatisch noch manuell). Es ist daher mehr als logisch, dass selbst in diesem Umfang der Verwaltungsaufwand schon relativ schnell Überhand nimmt und sich schnell Unlust und Fehler einstellen. Hier stößt das Peer-to-Peer-Networking schlichtweg an seine Grenzen und eine leistungsfähigere Organisationsform ist gefragt: Die Domäne.

Client/Server und Domänen

Im Gegensatz dazu stellt eine *Domäne* (englisch *Domain*) einen logischen Verbund von Computern dar, die eine zentrale, gemeinsame Benutzerkonten-Datenbank und damit verbunden auch gemeinsame Sicherheitsrichtlinien verwenden. Daraus ergeben sich zahlreiche Vorteile:

- Ein Benutzer braucht sich nur noch ein einziges Mal (und zwar an der Domäne) anzumelden, um Zugang zu den dazu gehörenden Ressourcen – freigegebene Ordner und Drucker, spezielle Dienste etc. – zu erhalten. Die mehrfache Anmeldung an jedem einzelnen Server, die Verwendung womöglich unterschiedlicher Benutzernamen und Kennwörter und dergleichen mehr gehören somit der Vergangenheit an.

- Die Anmeldung eines Benutzers an einer Domäne eröffnet ihm den Zugriff auf alle Ressourcen, die von einem Administrator für ihn freigegeben worden sind – unabhängig davon, auf welchem Server sich diese befinden. Die freigegebenen Ressourcen besitzen dabei keine Kennwörter.

Aufgrund der zentralen Architektur einer Domäne erfolgt die Freigabe von Ressourcen bedeutend strukturierter, als dies in einer Arbeitsgruppe der Fall sein kann. In einem Netzwerk können zudem mehrere Domänen vorhanden sein, was besonders bei verzweigten Netzwerken oder größeren Umgebungen sinnvoll ist.

Zum Aufbau einer Domäne ist mindestens ein Rechner erforderlich, der mit Windows Server 2003, Standard Edition oder höher (Windows Server 2003, Web Edition ist dazu nicht geeignet), einer der Server-Ausführungen von Windows 2000 oder einer der Server-Ausführungen von Windows NT 4.0 arbeitet und als *Domänencontroller* agiert. Während Domänen bereits seit Windows NT 3.1 (und sogar noch bei dessen »Vorgänger«, dem »LAN Manager«) existieren, hat Microsoft das Domänen-Konzept mit der Einführung von Windows 2000 und dem Active Directory wesentlich erweitert. War eine Domäne bis einschließlich Windows NT 4.0 lediglich als flache Liste realisiert und nur schwer erweiterbar, erlaubt das mit Windows 2000 eingeführte und in Windows Server 2003 ebenfalls enthaltene, dort in vielen Bereichen erweiterte *Active Directory*, eine hierarchische Strukturierung innerhalb einer Domäne vorzunehmen. Zudem kann ein einziges Active Directory mehrere Domänen umfassen, was die Verwaltung nicht nur in großen, sondern auch in verzweigten Strukturen wesentlich einfacher gestaltet.

Bei der logischen Domänen-Organisationsform für die Ressourcen des Netzwerks wird der Arbeitsplatz-PC eines Benutzers als *Client* einer Domäne bezeichnet. Clients können auf die freigegebenen Ressourcen von *Servern* zugreifen und die Dienste benutzen, die Server zentral bereitstellen. Ein solches Verfahren, das mit zentralen Servern arbeitet, deren Dienste und Ressourcen sich Clients bedienen können, ist als *Client/Server* bekannt. Generell wird ein Computer, der sich eines

Server-Dienstes bedient, als Client bezeichnet – auch dann, wenn es sich beim Client lediglich um eine kleine Software handelt, die wahlweise auf einem entfernten Computer oder demselben Computer wie der Server-Dienst läuft.

Server gibt es auch bei der dezentralen Peer-to-Peer-Technik. Ein Server in einer Client/Server-Netzwerkumgebung zeichnet sich dagegen durch andere Merkmale aus:

Zentral stellen Server dabei Dienste bereit, die für den Betrieb des Netzwerks unverzichtbar sind. Dabei kann es sich zum Beispiel um die zentrale Verwaltung der Ressourcen des Netzwerks wie etwa von Benutzern und Computern (der Server agiert dann als Domänencontroller) oder Server-Applikationen wie zum Beispiel einen E-Mail- oder Datenbank-Server (der Server agiert dann als Applikationsserver) handeln.

Server in einer Client/Server-Umgebung sind in der Regel darauf vorbereitet, eine zentrale Datenhaltung zu ermöglichen. Demzufolge warten sie mit entsprechend großen und schnellen Festplatten auf. Ein auf dem Server laufendes Backup-Programm sichert die Daten der Server regelmäßig.

Grundsätzlich zeichnet ein Server in einer Client/Server-Umgebung für die Verarbeitung von Anfragen verantwortlich, die Clients an ihn stellen. Dabei kann es sich zum Beispiel um die Verifizierung von Sicherheitsinformationen, die Bereitstellung einer zentral gespeicherten Datei oder aber die Suche in einer Datenbank handeln. Der Server liefert daraufhin das Ergebnis zum Client zurück, der dieses seinerseits lediglich darstellt. Das ermöglicht eine überaus leistungsfähige Form der Durchführung von Aufgaben (und bildet beispielsweise auch das Grundmodell für den Abruf von Webseiten mit einem Webbrowser für Inhalte, die häufig dynamisch zusammengestellt und von einem Webserver geliefert werden.

Server in einer Domäne sind zudem Rechner, die sowohl von ihrer Hardware als auch dem Betriebssystem her besonders auf ihre Aufgaben im Netzwerk ausgelegt sind: Server führen Netzwerkfunktionen und für den Betrieb des Netzwerks wichtige Dienste nicht nur nebenbei, sondern hauptsächlich aus – denn dies stellt schließlich die eigentliche Aufgabe von Servern dar.

Während Domänen bereits seit Windows NT 3.1 (und sogar noch bei dessen Vorgänger, dem »LAN Manager«) existieren, hat Microsoft das Domänen-Konzept mit der Einführung von Windows 2000 Server um eine richtungsweisende Funktion erweitert:

Bis einschließlich Windows NT 4.0 Server sind Domänen lediglich als flache Liste realisiert und nur schwer erweiterbar. Eine Unterteilung innerhalb einer Windows NT 4.0-Domäne ist dabei ebenso wenig möglich wie eine hierarchische Verbindung mehrerer Windows NT-Domänen.

Bei Windows 2000 Server und Windows Server 2003 hingegen ermöglicht es das *Active Directory*, eine hierarchische Strukturierung innerhalb einer Domäne vorzunehmen.

Zudem kann ein Active Directory mehrere, hierarchisch miteinander verbundene Domänen umfassen. Dies erlaubt nicht nur die einfache Verwaltung auch bei großen Netzwerken, sondern gestaltet auch den Umgang mit verzweigten Strukturen wesentlich einfacher, als es mit den flachen Windows NT-Domänen der Fall ist.

In Verbindung mit einem Active Directory ergeben sich zudem weitere Vorteile. Dazu zählt unter anderem die Möglichkeit, dass Administratoren eine zentrale Desktop-Verwaltung von Windows XP Professional (sowie darauf aufbauenden Ausführungen wie Windows XP Tablet PC Edition) und Windows 2000 Professional-PCs über das Netzwerk unter Verwendung von *Gruppenrichtlinien* vornehmen – was allein mit Windows XP Professional respektive einem Netzwerk ohne Active Directory so nicht machbar ist.

Ein mit Windows XP Home Edition ausgestatteter Computer lässt sich nicht in eine Domäne einbinden und gestattet keine zentrale Konfiguration über Gruppenrichtlinien.

3.1.3 Rollen eines Windows Server 2003-basierten Servers

Ein Windows Server 2003-basierter Server kann verschiedene Rollen ein- und somit unterschiedliche Aufgaben wahrnehmen.

Domänencontroller

Agiert ein Windows Server 2003 als *Domänencontroller* (englisch *Domain Controller*), zeichnet er für die Unterhaltung einer Domäne und des dortigen Verzeichnisses verantwortlich. Im Falle einer unter der Obhut von Windows Server 2003 (oder Windows 2000 Server) geführten Domäne ist diese in das *Active Directory* eingebunden. Der als Domänencontroller agierende Windows Server 2003 stellt dabei allen Diensten, die entsprechenden Zugriff wünschen (und über entsprechende Berechtigungen verfügen), Informationen aus diesem zentralen Verzeichnis bereit. Da eine Domäne eine gemeinsame Benutzerkonten-Datenbank verwendet, wickelt ein Domänencontroller die Anmeldung von Benutzern an der entsprechenden Domäne ab. Jede Domäne im Active Directory muss dabei mindestens einen Domänencontroller aufweisen, kann aber auch mehrere Domänencontroller enthalten.

Eine Unterscheidung zwischen verschiedenen Domänencontroller-Arten, wie es bei Windows NT 4.0-Domänen (ein primärer Domänencontroller »PDC« und mehrere Backup-Domänencontroller »BDCs«) der Fall ist, findet bei einer Windows Server 2003-Domäne respektive beim Active Directory nicht mehr statt. Hier ist jeder Domänencontroller vielmehr als gleichrangig zu betrachten und dazu in der Lage, auf die Verzeichnisdatenbank sowohl lesend als auch schreibend zuzugreifen.

Mitgliedsserver

Ein in eine Windows Server 2003- oder Windows 2000-Domäne eingebundener Windows Server 2003 kann aber nicht nur als Domänencontroller für das Active Directory operieren. Ist ein Windows Server 2003-basierter Server zwar in die entsprechende Domäne des Active Directory eingebunden, fungiert aber bei dieser nicht als Domänencontroller, handelt es sich um einen *Mitgliedsserver* (englisch *Member Server*).

Ein Mitgliedsserver ist nicht mit dem Overhead belastet, den die Arbeit als Domänencontroller zur Unterhaltung des Active Directory erfordert. Somit lassen sich die Leistungspotenziale des Windows Server 2003 anderweitig nutzen: Ein als Mitgliedsserver agierender Windows Server 2003 kann zum Beispiel als *Applikationsserver* – etwa als E-Mail-Server oder als Terminal-Server (falls auf ihm die Terminaldienste aktiviert sind) – zu Werke gehen.

Obgleich in die Domäne eingebunden, führt ein jeder Mitgliedsserver zudem seine lokale Benutzerkonten-Datenbank. Da ein Mitgliedsserver also an der gemeinsamen Verwaltung der Ressourcen des Netzwerks nicht teilnimmt (dafür zeichnen ja Domänencontroller verantwortlich), sondern diese lediglich nutzt, ist es einem Mitgliedsserver aber nicht möglich, beispielsweise Anmeldungen von Benutzern an der Domäne abzuwickeln. Diese Aufgabe ist vielmehr Domänencontrollern vorbehalten.

Ein als Mitgliedsserver operierender Windows Server 2003 kann mit dem Programm *DCPROMO* – dem *Assistenten zum Installieren von Active Directory* – zu einem Domänencontroller heraufgestuft werden, ohne das Betriebssystem auf dem betreffenden Windows Server 2003-Server neu installieren zu müssen. Umgekehrt ist es mit DCPROMO auch möglich, einen Domänencontroller zu einem Mitgliedsserver herabzustufen.

Eigenständiger Server

Es ist keineswegs zwingend erforderlich, einen Windows Server 2003-basierten Server als Domänencontroller oder Mitgliedsserver in eine Domäne einzubinden. Genauso kann ein Windows Server 2003-basierter Server auch als so genannter *eigenständiger Server* (englisch *Stand-alone Server*) betrieben werden. Hierbei gehört der Windows Server 2003 dann lediglich einer *Arbeitsgruppe* an – so, als gäbe es keine Domäne. Die Freigabe eigener Ressourcen sowie der Zugriff auf die Ressourcen anderer

Rechner erfolgt in diesem Fall wie beim Peer-to-Peer-Networking (siehe Abschnitt *Peer-to-Peer und Arbeitsgruppen*).

Da nicht in eine Domäne eingebunden, kann ein eigenständiger Server die Vorteile des Active Directory auch nicht nutzen – und somit nicht über das Active Directory zentral verwaltet werden. Daraus ergibt sich, dass ein eigenständiger Server seine vollkommen eigene, lokale Benutzerkonten-Datenbank unterhält, die demzufolge von einem Administrator auch separat zu pflegen ist.

3.2 Protokolle

Damit sich verschiedene Geräte über ein Netzwerk überhaupt miteinander verständigen können, müssen diese eine gemeinsame »Sprache« sprechen. In Bezug auf Netzwerke handelt es sich dabei um *Protokolle*. Vereinfacht ausgedrückt, legt dabei ein Protokoll exakte Regeln fest, wie die Kommunikation zwischen mehreren Beteiligten stattzufinden hat. Denn: Nur wenn zwei Geräte dieselben Regeln kennen und diese auch verwenden, können sie sich einwandfrei miteinander unterhalten.

3.2.1 TCP/IP

Das am meisten genutzte Protokoll stellt *TCP/IP* (die Abkürzung für *Transmission Control Protocol/Internet Protocol*) dar. Dieses verdankt seine Popularität nicht nur dem Internet, sondern auch der Tatsache, dass zahlreiche Hersteller der Informationstechnologie-Branche dieses Protokoll zum leichten Informationsaustausch mit anderen Umgebungen implementiert haben. Verbunden mit dem Siegeszug des Internet und seines im LAN genutzten Ablegers – dem »Intranet« – hat das zunächst nur bei Großrechnern oder im WAN genutzte TCP/IP-Protokoll schon vor vielen Jahren auch in lokalen Netzwerken seinen festen Platz erobert. Nicht zuletzt deshalb entspricht TCP/IP dem von Windows Server 2003 bevorzugten Protokoll.

Der Begriff »TCP/IP« bezieht sich auf den gesamten Protokoll-Stapel, der zur Einbindung eines Computers in das Internet oder ein Intranet dient. Der Begriff »IP« dagegen bezieht sich direkt auf das »Internet Protocol«, das innerhalb von TCP/IP das Netzwerkprotokoll darstellt.

TCP/IP eignet sich hervorragend zur Verbindung unterschiedlicher Rechnerwelten: So stellt es kein Problem dar, mit Windows Server 2003 auf einen Web-Server zuzugreifen, der auf Unix-Basis auf einem anderen Computer läuft. Ob dieser im unternehmenseigenen Intranet oder dem öffentlichen Internet hängt, spielt keine Rolle – solange Windows Server 2003 Verbindung mit dem Internet aufnehmen kann. Alle von Microsoft stammenden Betriebssysteme – angefangen bei Windows für Workgroups über Windows 95/98/ME bis hin zu Windows NT 4.0, Windows 2000, Windows XP und Windows Server 2003 (mit Zusätzen sogar MS-DOS sowie Windows 3.1) – verstehen den Umgang mit TCP/IP, sodass sich dieses Protokoll problemlos auch zur übergreifenden Kommunikation verwenden lässt.

TCP/IP besitzt ein paar charakteristische Eigenschaften: Jedes Gerät verfügt über (mindestens) eine IP-Adresse, die dieses eindeutig identifiziert und den Aufbau *n1.n2.n3.n4* besitzt (*n1*, *n2*, *n3* und *n4* können dabei Werte zwischen 0 und 255 annehmen). Zudem ist die so genannte *Subnetzmaske* (mit derselben Notation wie eine IP-Adresse) erforderlich, um das Subnetz, in dem sich das Gerät befindet, genau zu bestimmen.

Des Weiteren benötigt jedes mit TCP/IP arbeitende Gerät noch ein *Standard-Gateway*, um zu wissen, welcher *IP-Router* sich der Weiterleitung von Paketen an solche Geräte annimmt, die sich außerhalb des eigenen und somit in einem anderen Netzwerk befinden.

Der alleinige Umgang mit IP-Adressen – etwa, wenn es um das Besuchen eines Web-Servers geht – würde die Verwendung von TCP/IP jedoch sehr schwer und zudem anfällig für Eingabefehler machen. Aus diesem Grund wurde das *Domain Name System* (kurz *DNS*) ins Leben gerufen und in

TCP/IP integriert. Mit seiner Hilfe ist es möglich, aussagekräftige Namen – wie zum Beispiel *www.microsoft.com* zum Besuch von Microsofts Web-Server – zu verwenden. DNS ermittelt für solche DNS-Namen dann die für den Betrieb von TCP/IP zwingend erforderlichen IP-Adressen und führt somit eine Namensauflösung durch.

Verwechseln Sie eine Domäne des Active Directory nicht mit einer Domäne von DNS.

3.2.2 IPX/SPX

Einhergehend mit dem großen Erfolg des Netzwerkbetriebssystems *NetWare* von Novell hat das von diesem Hersteller entwickelte Protokoll *IPX/SPX* (Internetwork Packet Exchange/Sequenced Packet Exchange) Einzug in etliche lokale Netzwerke gehalten. IPX/SPX stellt neben TCP/IP das in lokalen Netzwerken am meisten verbreitete Protokoll dar und zeichnet sich durch seine gute Performance aus.

Obwohl IPX das Netzwerkprotokoll innerhalb von IPX/SPX bildet, wird IPX häufig auch als Abkürzung für den gesamten Protokoll-Stack verwendet.

Mit der hohen Verbreitung von NetWare in seinen zahlreichen Versionen ist auch das von diesen Netzwerkbetriebssystemen bevorzugte Protokoll IPX (sowie das darauf aufbauende SPX) in vielen Umgebungen anzutreffen. IPX/SPX gelangt vor allem in Netzwerken zur Anwendung, die mit NetWare 2.x, 3.x oder 4.x arbeiten. IPX-Netzwerke können durchaus weiter verzweigt sein, beispielsweise durch Nutzung von IPX-Routern.

Die zu Windows Server 2003 gehörende Ausführung von Routing und RAS (RRAS) gestattet es nicht, einen Windows Server 2003-basierten Server als IPX-Router einzusetzen.

Mit Einführung von NetWare 5.0 muss IPX/SPX nicht mehr das primäre Protokoll sein, vielmehr lässt sich statt dessen Intranet- und Internet-konform auch TCP/IP als primäres und alleiniges Protokoll heranziehen. Aufgrund dessen geht die Bedeutung von IPX/SPX zunehmend zurück.

Alle netzwerkfähigen Microsoft-Betriebssysteme, angefangen bei Windows für Workgroups über Windows 95/98/ME bis hin zu Windows NT 4.0, Windows 2000, Windows XP und Windows Server 2003 unterstützen IPX/SPX, um eine leichte Integration in NetWare-Umgebungen zu ermöglichen, die mit diesem Protokoll arbeiten. Neben der von Microsoft offerierten Client-Software für NetWare bietet Novell eine eigene, mit erweiterten Funktionen aufwartende Client-Software für NetWare an. Die Microsoft-eigene Client-Software für NetWare setzt dabei zwingend die Verwendung von IPX/SPX als primärem Protokoll voraus – lässt sich also beispielsweise in NetWare 6.x-Umgebungen, die für den alleinigen Einsatz von TCP/IP konfiguriert sind, nicht respektive nur mit Umwegen (beispielsweise über die IPX-Emulation von NetWare 6.x) verwenden.

Der zu Windows 2000 Server gehörende *Gateway Service für NetWare*, der für nur mit der Microsoft-Client-Software ausgestattete Computer eine Brücke zu mit IPX/SPX kommunizierenden NetWare-Servern schlägt, ist im Lieferumfang von Windows Server 2003 nicht mehr enthalten.

3.2.3 NetBEUI

1983 entwickelte die Firma Sytek für IBM das »Network Basic Input/Output System«, kurz *NetBIOS*. Dieses umfasste relativ simple Befehle, um den Auf- und Abbau von Verbindungen zu anderen PCs durchzuführen sowie diese zu unterhalten. 1985 stellten IBM und Microsoft mit dem »NetBIOS Extended User Interface« – kurz *NetBEUI* – eine erweiterte Fassung vor, die als Protokoll noch immer in vielen, vor allem kleinen, LANs zum Einsatz gelangt.

NetBEUI ist nicht mit »NetBIOS« zu verwechseln. NetBIOS stellt eine Anwendungsprogrammierschnittstelle (API) für Dienste und Applikationen dar, NetBEUI hingegen ein Transportprotokoll für den Austausch von Informationen zwischen Netzwerkadaptern. Während frühe, DOS-basierte NetBIOS-Implementationen mit dem Transportprotokoll sozusagen zusammengefasst waren, wird seit Einführung von Windows NT und somit auch bei Windows Server 2003 die NetBIOS-API sauber vom NetBEUI-Transportprotokoll getrennt behandelt. Auf diese Weise ist es möglich, NetBIOS unter Windows Server 2003 wahlweise in Verbindung mit den Transportprotokollen TCP/IP, NetBEUI oder IPX/SPX zu verwenden.

Das Protokoll NetBEUI wird dabei insbesondere in Umgebungen genutzt, in denen Microsoft-basierte Netzwerklösungen zum Einsatz kommen. Historisch bedingt stellte NetBEUI lange Zeit das von Microsoft bevorzugte Protokoll dar, während die Vorliebe für andere Protokolle wie zunächst IPX/SPX und dann TCP/IP bei Microsoft erst später erwachte. So verstehen beispielsweise Windows für Workgroups, Windows 95/98/ME, Windows NT 4.0, Windows 2000 und Windows XP den Umgang mit NetBEUI. Aufgrund der fehlenden Routing-Fähigkeit (dazu gleich mehr) sowie des Siegeszuges von Intranet/Internet geht die Bedeutung von NetBEUI allerdings stark zurück.

Die Unterstützung für NetBEUI ist im Lieferumfang von Windows Server 2003 nicht mehr enthalten. Es ist allerdings möglich, die betreffenden Protokoll-Komponenten beispielsweise von einer Windows XP Professional-CD-ROM einzuspielen und so Windows Server 2003 NetBEUI »beizubringen«. Dies gilt jedoch nur für die 32-Bit-Version von Windows Server 2003: Die 64-Bit-Version von Windows Server 2003 und Windows XP Professional unterstützen NetBEUI nicht.

Charakteristisch für das NetBEUI-Protokoll ist seine Einfachheit: Es ist keine weitere Konfiguration erforderlich. Um sich selbst im Netzwerk eindeutig für andere Geräte zu identifizieren, bedient sich NetBEUI nämlich keiner kryptischen numerischen Adresse wie TCP/IP oder IPX/SPX, sondern einfach des NetBIOS-Namens, den alle Geräte in einem Microsoft-Netzwerk tragen. Nach der Installation von NetBEUI ist dieses Protokoll also sofort einsatzbereit, eine weiter gehende Konfiguration ist nicht vorzunehmen. Computer, die mit NetBEUI arbeiten, können sich gegenseitig also sofort »sehen« (wenn sie sich im selben Netzwerksegment befinden).

Jedem PC, der mit Windows für Workgroups, Windows 95/98/ME, Windows NT 4.0, Windows 2000, Windows XP oder Windows Server 2003 arbeitet, muss bei der Installation ein Name erteilt werden. Diesen zieht das Betriebssystem automatisch als *NetBIOS-Namen* (mitunter ist auch vom *Computernamen* oder von *Prä-Windows 2000* die Rede) heran. Allerdings verwendet Windows Server 2003 – wie auch bereits Windows 2000 – den NetBIOS-Namen in erster Linie nur noch im Rahmen der Kompatibilität zu früheren Microsoft-Betriebssystemen. Denn im Zusammenspiel mit dem Active Directory braucht Windows Server 2003 keinen solchen NetBIOS-Namen mehr, sondern wickelt alle Identifikationsvorgänge rein über TCP/IP ab. Um jedoch ohne die Existenz vom Active Directory mit anderen (etwa Windows XP-) PCs, auf denen beispielsweise Windows 95/98/ME läuft, oder aber mit bestimmten Netzwerkgeräten (Hardware-basierte, externe Print-Server, CD-ROM-Server etc.) zu kommunizieren, ist NetBIOS aber auch bei Windows Server 2003 aus Kompatibilitätsgründen noch existent. Die Abschaltung von NetBIOS sollte somit erst dann erfolgen, wenn zuvor sichergestellt worden ist, dass kein Gerät mehr NetBIOS benötigt.

NetBEUI weist jedoch auch einen – aus heutiger Sicht vielfach gravierenden und dieses Protokoll häufig disqualifizierenden – Nachteil auf: NetBEUI ist (im Gegensatz etwa zu TCP/IP) nicht routingfähig: NetBEUI-Knoten können andere NetBEUI-Knoten, die sich in einem über einen Router angebundenen Segment befinden, somit nicht sehen. Es lässt sich also ausschließlich das Gerät identifizieren, nicht aber, in welches Netzwerksegment dieses eingebunden ist.

Der Grund dafür liegt in der Einfachheit der Netzwerkadressen von NetBEUI begründet, für die ausschließlich der NetBIOS-Name des jeweiligen Geräts herangezogen wird. Unter NetBEUI gibt es somit zwar eine Knotenadresse (nämlich den NetBIOS-Namen), aber keine Netzwerknummer, wie dies sowohl bei IPX als auch IP der Fall ist (IPX und IP sind daher routingfähig – im Gegensatz zu NetBEUI).

Für mit NetBEUI arbeitende Geräte sind daher NetBEUI-Geräte, die sich in einem anderen Netzwerksegment befinden, nicht sichtbar – und können somit auch nicht angesprochen werden. Im Gegensatz dazu arbeiten IPX/SPX und TCP/IP für jedes Gerät mit Netzwerkadressen, die nicht nur das jeweilige Gerät selbst identifizieren, sondern eindeutig auch das Netzwerksegment festlegen, in dem sich dieses befindet.

3.3 Namensauflösung

Windows Server 2003 benutzt das aus dem Internet bekannte Domain Name System »DNS«, um Domänen und Objekte innerhalb des Active Directory zu identifizieren. Auf diese Weise ist es letztlich auch möglich, eine Hierarchie im Active Directory zu realisieren, da DNS-Namen von sich aus bereits mit einer »eingebauten« Hierarchie versehen sind. DNS benutzt das im Internet sowie in Intranets zum Einsatz gelangende TCP/IP und lässt sich nicht mit anderen Protokollen (etwa IPX) verwenden.

Im Gegensatz dazu verwenden frühere Versionen wie zum Beispiel Windows NT 4.0 oder Windows 95/98/ME NetBIOS-Namen zur Identifizierung von Domänen, Diensten und weiteren Ressourcen. Diese Namen sind per se flach gehalten, eine Hierarchie ist nicht möglich. Bei NetBIOS handelt es sich um eine API, deren Verwendung immer ein Protokoll wie zum Beispiel TCP/IP, IPX oder NetBEUI erfordert. Aus Kompatibilitätsgründen unterstützt Windows Server 2003 auch IPX, doch spielt bei Windows Server 2003 allen voran TCP/IP die Hauptrolle, denn dieses Protokoll ist zum Betrieb des Active Directory unverzichtbar.

Bei TCP/IP aber bedarf es immer einer IP-Adresse, die einen für Benutzer aussagekräftigen Namen beispielsweise von Diensten – sei es ein DNS-Name oder ein NetBIOS-Name – in eine für Computer verwendbare IP-Adresse umwandelt. Genau dies ist die Aufgabe, die dem Aspekt der *Namensauflösung* zufällt. Aus diesem Grund ist es wichtig zu verstehen, welche Möglichkeiten der Namensauflösung von DNS- und NetBIOS-Namen in IP-Adressen Windows Server 2003 unterstützt.

3.3.1 Verfahren zur Namensauflösung in Verbindung mit TCP/IP

Ist ein PC in ein Netzwerk eingebunden, in dem TCP/IP zum Einsatz gelangt, stellt sich die Frage der Namensauflösung. Die Gründe hierfür sind denkbar einfach:

Niemand möchte beispielsweise in der Netzwerkumgebung von Windows Server 2003 die wenig aussagekräftigen IP-Adressen anderer Computer im Intranet angezeigt bekommen, sondern hier verständliche Namen sehen, mit denen sich auch eine Bedeutung verbinden lässt.

Genauso ist es in Intranet und Internet: Der Besuch von Webservern wird unpraktikabel, wenn man ausschließlich mit IP-Adressen arbeiten müsste, die sich in größerer Anzahl kaum jemand merken kann. Auch hierbei sind Namen gefragt, denn erst diese erlauben eine einfache Nutzung von Intranet und Internet.

Für genau diese beiden Bereiche beherrscht Windows Server 2003 Verfahren, die eine entsprechende Umsetzung von für den Anwender aussagekräftigen Namen in die für Computer erforderlichen IP-

Adressen erlauben. Anders ausgedrückt, sind in Windows Server 2003 Verfahren implementiert, mit solchen Namen zu arbeiten, während sich entsprechende Mechanismen darum kümmern, dass diese Namen automatisch in die entsprechenden IP-Adressen aufgelöst werden – denn erst mit diesen IP-Adressen kann der Computer (und TCP/IP) etwas anfangen. Diese Namensauflösung kann sowohl für auf NetBIOS basierende Computernamen – etwa *webserv* – in lokalen Netzwerken mit Microsoft-Betriebssystemen als auch für DNS-Namen – wie *www.company.com* – im Intranet und Internet stattfinden (siehe Abbildung 3.1).

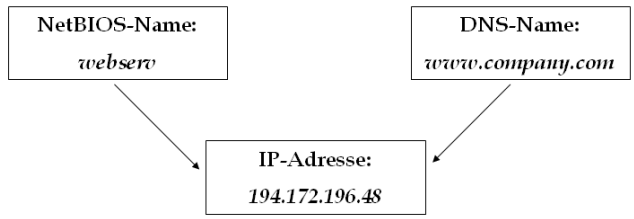

Abbildung 3.1: Dank der Namensauflösung lassen sich leicht zu verwendende NetBIOS- oder DNS-Namen automatisch in IP-Adressen auflösen

Damit die Namensauflösung funktionieren kann, muss an einer bestimmten Stelle verzeichnet sein, welcher Name welcher IP-Adresse zugeordnet ist. Konkret bestehen zwei unterschiedliche Möglichkeiten, Namen in IP-Adressen aufzulösen (siehe Abbildung 3.2):

Alle Zuordnungen werden in einer Datei festgehalten, die lokal auf der Festplatte eines jeden PCs abgelegt sein muss, der in das Netzwerk eingebunden ist und eine Namensauflösung durchführen soll. Für NetBIOS-Namen handelt es sich hierbei um die Datei *LMHOSTS*, während für DNS-Namen die Datei *HOSTS* zum Tragen kommt. Will ein Computer eine Namensauflösung vornehmen, kann er einen Blick in die betreffende Datei werfen und feststellen, ob dort ein entsprechender Eintrag existiert.

Es gibt einen entsprechenden Dienst, der auf einem oder mehreren Servern läuft und eine zentrale Datenbank mit allen relevanten Einträgen führt. Für NetBIOS-Namen ist dies *WINS*, für DNS-Namen entsprechend *DNS*. In dieser Datenbank werden nun die Namen und IP-Adressen aller in das Netzwerk eingebundenen Computer verzeichnet (entweder automatisch oder manuell). Möchte ein Computer die IP-Adresse zu einem bestimmten Namen erhalten, agiert er als Client für WINS oder DNS und fragt beim jeweiligen WINS- oder DNS-Server nach, ob dieser einen entsprechenden Eintrag besitzt.

Ist die IP-Adresse des Ziels ermittelt, führt *ARP* (Address Resolution Protocol) als integraler Bestandteil des TCP/IP-Protokolls eine Auflösung dieser IP-Adresse in die zugehörige physikalische MAC-Adresse des betreffenden Netzwerkadapters durch. Somit kann dann die Kommunikation unter Verwendung von TCP/IP einwandfrei stattfinden.

	NetBIOS-Name in IP-Adresse	DNS-Name in IP-Adresse
Lokale Datei	LMHOSTS	HOSTS
Server-Dienst	WINS	DNS

Abbildung 3.2: Zur Namensauflösung in IP-Adressen stehen für DNS- und NetBIOS-Namen unterschiedliche Verfahren zur Verfügung

3.3.2 NetBIOS-Namen: LMHOSTS und WINS

Frühere Betriebssystem von Microsoft – beispielsweise Windows für Workgroups, Windows 95/98/ME und Windows NT 4.0 – verwenden zur gegenseitigen Identifikation den *NetBIOS-Namen* des Computers (daher spricht man auch vom *Computernamen*). Diese NetBIOS-Namen erscheinen dann zum Beispiel in der Netzwerkumgebung, sodass man sich auf einfache Art und Weise mit den Freigaben anderer Computer verbinden und diese gemeinsam nutzen kann.

NetBIOS over TCP/IP (zum Transport von NetBIOS-Informationen via TCP/IP) wird auch als *NetBT* oder *NBT* bezeichnet.

Aus Gründen der Kompatibilität zu früheren Betriebssystemen – sowie älteren Geräten (etwa CD-ROM- oder Print-Server) – kann auch Windows Server 2003 noch auf diesen Mechanismus zurückgreifen. Der NetBIOS-Name wird dabei aus dem Namen des betreffenden Computers gebildet, den dieser bei der Installation des Betriebssystems erhält.

In einer Umgebung, in der ausschließlich Windows Server 2003, Windows 2000 Server, Windows XP Professional und Windows 2000 Professional zum Einsatz kommen, ist NetBIOS nicht mehr erforderlich. Sobald jedoch noch Computer mit früheren Betriebssystemen oder andere Geräte, die NetBIOS benötigen, im Netzwerk existieren, sollte NetBIOS auch weiterhin verwendet werden.

Wenn ausschließlich TCP/IP als Protokoll im Netzwerk zum Einsatz gelangen soll, sieht man sich mit einem Problem konfrontiert: TCP/IP arbeitet mit IP-Adressen (im Gegensatz zu NetBEUI) und nicht mit NetBIOS-Namen (wie es bei NetBEUI der Fall ist). Aus diesem Grund wurden Mechanismen entwickelt, die es ermöglichen, eine IP-Adresse einem NetBIOS-Namen zuzuordnen.

Eine Möglichkeit besteht in der Verwendung der Datei *LMHOSTS*, die jeder mit einem Microsoft-Betriebssystem arbeitende Computer besitzen kann. In dieser Textdatei sind einfach die IP-Adressen sowie die NetBIOS-Namen der im Netzwerk vorhandenen Computer aufgelistet. Will ein PC nun auf einen anderen Rechner zugreifen, prüft TCP/IP, ob in der Datei LMHOSTS (sofern diese verwendet wird, was nicht zwingend sein muss) für den angegebenen Namen eine IP-Adresse vorliegt. Ist dies der Fall, kann TCP/IP die betreffende IP-Adresse heranziehen und den gewünschten Zugriff dann ausführen. Der Nachteil von LMHOSTS liegt allerdings in der manuellen Konfiguration, die diese Datei erfordert: Jeder PC im Netzwerk muss hier mit seinem NetBIOS-Namen und seiner (festen!) IP-Adresse eingetragen werden.

Die Datei LMHOSTS befindet sich bei Windows Server 2003 im Ordner %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC. Standardmäßig gibt es die Beispieldatei LMHOSTS.SAM, in der die Syntax und eine kurze Beschreibung des inhaltlichen Aufbaus dieser Datei zu finden sind.

Um die aufwändige, zudem fehlerträchtige – und beispielsweise in Verbindung mit der dynamischen Zuweisung der TCP/IP-Konfiguration über DHCP gar nicht mehr nötige – manuelle Pflege von LMHOSTS auf jedem Computer nicht mehr durchführen zu müssen, hat Microsoft den *Windows Internet Name Service* (kurz *WINS*) entwickelt, der mitunter auch als »NetBIOS Name Service« bezeichnet wird.

Das im Client/Server-Verfahren realisierte WINS funktioniert prinzipiell wie folgt:

Ein *WINS-Server*, der beispielsweise auf Windows Server 2003 abläuft, registriert in seiner Datenbank automatisch alle Computernamen (die NetBIOS-Namen) der im Netzwerk vorhandenen Rechner sowie deren IP-Adressen.

Ein an einem *WINS-Client* arbeitender Benutzer kann nun auf einen bestimmten Computer über TCP/IP zugreifen, ohne dessen IP-Adresse kennen zu müssen, indem er einfach den NetBIOS-Namen des betreffenden Computers eingibt. Der WINS-Server ermittelt daraufhin die IP-Adresse des gewünschten Computers und gibt diese an den WINS-Client zurück, der dann seinerseits im Hintergrund über die IP-Adresse den Zugriff auf den gewünschten Computer abwickelt. WINS führt also eine Namensauflösung von NetBIOS-Namen in IP-Adressen durch.

Um sich der Dienste von WINS zu bedienen und als WINS-Client aufzutreten, muss auf einem Computer im Rahmen seiner TCP/IP-Konfiguration die IP-Adresse mindestens eines WINS-Servers spezifiziert werden.

Falls auf einem Windows Server 2003 unter Verwendung des Protokolls TCP/IP Probleme auftreten, die sich darin äußern, dass in der Netzwerkumgebung nur der eigene, nicht aber die anderen in das Netzwerk eingebundenen Rechner (insbesondere, wenn diese mit Windows 95/98/ME arbeiten) aufgeführt werden, handelt es sich mit hoher Wahrscheinlichkeit um ein Problem mit der Namensauflösung für NetBIOS. Gegebenfalls sollten Sie die betreffenden PCs dann für die Verwendung entweder der Datei LMHOSTS oder aber von WINS konfigurieren, um eine korrekte Namensauflösung von NetBIOS-Namen in IP-Adressen zu ermöglichen.

NetBIOS-Namen besitzen dabei lediglich einen flachen Namensraum, der keine Hierarchie zulässt (wie es bei DNS ja problemlos möglich ist). Das rührt nicht zuletzt daher, dass NetBIOS-Namen für Benutzer, Computer und Domänen maximal 16 Byte lang sein dürfen. Dabei ist das letzte Byte reserviert, denn es kennzeichnet den Ressourcen-Typ des jeweiligen NetBIOS-Namens, der entweder eindeutig – »U« für »unique« – ist oder eine Gruppe charakterisiert (siehe Tabelle 3.1).

Zur Diagnose der Namensauflösung von NetBIOS-Namen in IP-Adressen steht der Befehl *NBTSTAT* zur Verfügung.

NetBIOS-Name mit Ressourcen-Typ	Bedeutung
Computer[00]	Workstation-Dienst (U)
Domäne[00]	Domänen-Name (G)
Domäne[00]	Domänencontroller (G)
Computer[03]	Nachrichten-Dienst (U)
Benutzer[03]	Nachrichten-Dienst (U)
Computer[06]	RAS-Server-Dienst (U)
Computer[20]	Server-Dienst (U)
Computer[21]	RAS-Client-Dienst (U)

Tabelle 3.1: Aufbau und Bedeutung typischer NetBIOS-Namen

Darüber hinaus arbeitet NetBIOS mit einem *Knotentyp*. Dieser gibt an, auf welche Art und Weise die Namensauflösung stattfindet. Folgende NetBIOS-Knotentypen existieren:

Broadcast (»b-node«)
Falls sich ein Name nicht bereits im lokalen NetBIOS-Namenscache befindet, wird ein Broadcast im lokalen Subnetz ausgesandt, um eine Namensauflösung durchzuführen. Hierbei handelt es sich um das standardmäßige Vorgehen, falls der PC nicht als WINS-Client konfiguriert ist (also seine TCP/IP-Konfiguration nicht die IP-Adresse mindestens eines WINS-Servers umfasst).

Point-to-Point (»p-node«)
Bei diesem Knotentyp wird zunächst im lokalen NetBIOS-Namenscache nachgesehen, andernfalls ein WINS-Server kontaktiert.

Mixed Mode (»m-node«)
Als Erstes findet hierbei ein Blick in den lokalen NetBIOS-Namenscache statt. Schlägt dies fehl, wird ein Broadcast im lokalen Subnetz verschickt. Konnte auch dann keine Namensauflösung erfolgen, wird beim WINS-Server nachgefragt.

Hybrid (»h-node«)
Ist ein PC für diesen Knotentyp konfiguriert, versucht der PC eine Namensauflösung in der Reihenfolge lokaler NetBIOS-Namenscache, WINS-Server und Broadcast. Dieses ist das standardmäßige Vorgehen für einen als WINS-Client konfigurierten PC.

Mit welchem NetBIOS-Knotentyp ein PC tatsächlich arbeitet, lässt sich über den Befehl *IPCONFIG* (etwa unter Windows Server 2003, Windows XP, Windows 2000 oder Windows NT 4.0) respektive mit dem Windows-Utility *WINIPCFG* (bei Windows 95/98/ME) in Erfahrung bringen.

Im Intranet sowie im Internet übernimmt das *Domain Name System* (kurz *DNS*) die Aufgabe, Hostnamen von Geräten wie zum Beispiel Computern in IP-Adressen aufzulösen. Im Gegensatz zum flachen Namensraum bei NetBIOS arbeitet DNS dabei mit hierarchischen Namen, die den Aufbau *Host.Domäne* besitzen und so eine bessere, da strukturierte Zuordnung erlauben. Der als Web-Server agierende Host mit dem Host-Namen *web* in der Domäne *ticg.de* zum Beispiel würde daher über den Webbrowser mit *web.ticg.de* angesprochen. Diese Bezeichnung entspricht zudem dem DNS-Namen des betreffenden Hosts.

Um auf die nützlichen Dienste von DNS zurückgreifen zu können, gibt es *DNS-Server* – entweder im eigenen Netzwerk oder aber im Internet (jeder Internet-Service-Provider betreibt in der Regel einen primären und einen sekundären DNS-Server). Ein DNS-Server unterhält eine umfangreiche Datenbank, in der verzeichnet ist, welche Hosts in einer DNS-Domäne welche IP-Adresse tragen. Ein regelmäßiger Austausch entsprechender Informationen zwischen den einzelnen DNS-Servern stellt dabei sicher, dass diese »über ihren eigenen Horizont hinaus« auch Informationen darüber besitzen, welcher andere DNS-Server um die Namen und IP-Adressen einer bestimmten Domäne weiß. Letztlich wird darüber das Domain Name System des gesamten Internet weltweit abgewickelt. Grundlegend funktioniert DNS dabei folgendermaßen:

Ein als DNS-Server agierender Rechner kennt die Namen, die einzelne Geräte tragen, sowie ihre zugehörige Domäne. Auf Anfrage kann er sodann die einem bestimmten Host in einer bestimmten Domäne zugewiesene IP-Adresse zurückliefern (vorausgesetzt, es existiert ein entsprechender Eintrag). Ist der DNS-Server nicht selbst dazu in der Lage, diese Namensauflösung eines DNS-Namens in eine IP-Adresse zu beantworten, kontaktiert er einen anderen, übergeordneten oder vorgeschalteten DNS-Server, um diesen sozusagen um Mithilfe zu bitten (dieser kann wiederum weitere DNS-Server kontaktieren).

Jeder Computer, der über DNS eine Namensauflösung von DNS-Namen in IP-Adressen benötigt, agiert als *DNS-Client* (respektive *Resolver*). Im Rahmen dessen kontaktiert er einen oder mehrere DNS-Server, um von diesen die IP-Adresse für einen DNS-Namen zu erfragen. Dieser Prozess geschieht sozusagen im Hintergrund: Ein Benutzer beispielsweise gibt lediglich den DNS-Namen an. TCP/IP versucht sodann, diesen (unter Mithilfe eines DNS-Servers) in eine IP-Adresse aufzulösen, um den Vorgang sodann mit der IP-Adresse vorzunehmen. Schließlich arbeitet TCP/IP nun mal mit IP-Adressen und nicht mit DNS-Namen, die vielmehr für Menschen geschaffen wurden.

Um auf DNS zurückzugreifen und somit als DNS-Client zu agieren, muss für den Computer im Rahmen seiner TCP/IP-Konfiguration die IP-Adresse mindestens eines DNS-Servers angegeben werden.

Eine zu DNS alternative Form zur Namensauflösung von DNS-Namen in IP-Adressen besteht in der Verwendung der Datei HOSTS, die jeder Computer besitzen kann (bei Windows Server 2003 befindet sich die Datei HOSTS im Ordner %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC): In dieser Textdatei sind einfach die IP-Adressen sowie die DNS-Namen der betreffenden Geräte aufgelistet. Will ein PC nun auf einen anderen Rechner zugreifen, prüft TCP/IP, ob in der Datei HOSTS (sofern diese vom Client verwendet wird) für den angegebenen DNS-Namen eine IP-Adresse vorliegt. Trifft dies zu, kann TCP/IP die betreffende IP-Adresse heranziehen und den Zugriff auf den betreffenden Rechner sodann ausführen. Der Nachteil von HOSTS liegt allerdings in der manuellen Pflege dieser Datei. Jeder Rechner ist in dieser Datei manuell mit Namen und IP-Adresse zu verzeichnen, einen Automatismus gibt es nicht.

In der Regel verfügt jeder mit TCP/IP arbeitende Computer über die Datei HOSTS, denn in dieser ist ein wichtiger Eintrag festgehalten: Der Name *localhost* wird hierüber der reservierten IP-Adresse *127.0.0.1* zugeordnet, die den Rechner bezeichnet. Auf diese Weise ist es etwa möglich, durch Eingabe von ping localhost (Enter) den eigenen Rechner von TCP/IP kontaktieren zu lassen – um zu diagnostizieren, ob dieser überhaupt für TCP/IP konfiguriert ist.

Das Kapitel 16.11 gibt Auskunft über die Integration des Active Directory in DNS sowie die speziellen Techniken, mit denen dies realisiert wird.