- Zwischen der IP-Adresse und dem Host-Namen muss mindestens ein Leerzeichen stehen.
- Ein Host-Name darf maximal 255 Zeichen lang sein, wobei alphanumerische Zeichen und einige Sonderzeichen eingesetzt werden dürfen. Ein Host-Name, der nur aus Ziffern besteht, ist nicht zulässig.

HINWEIS

Der Unterstrich ist zwar als gültiges Zeichen eines Host-Namens zulässig, sollte aber vermieden werden, da dies unter Umständen zu Problemen führen kann.

- Die Groß-/Kleinschreibung bei Host-Namen wird auf UNIX-Systemen beachtet.
- Häufig benutzte Hosts sollten oben in der Datei stehen, da diese von oben nach unten gelesen wird.
- Pro IP-Adresse können mehrere Host-Namen zugeordnet werden, wobei mehrere Namenseinträge mindestens durch ein Leerzeichen getrennt sein müssen.
- Kommentarzeilen werden in einer Hosts-Datei immer mit dem Zeichen »#« eingeleitet.
- Die Hosts-Datei wird unter UNIX im Verzeichnis */etc* und auf einem Windows-System im Verzeichnis *\%systemroot\system32\drivers\etc* abgelegt.

HINWEIS

Neben der Hosts-Datei wird in der Literatur hin und wieder auch die Datei *lmhosts* erwähnt. Dies ist eine Datei, in der eine Zuordnung von NetBIOS-Namen zu IP-Adressen abgelegt werden kann.

Da selbst Microsoft auf seiner Homepage den Einsatz seines proprietären Dienstes zur Namensauflösung WINS nicht mehr empfiehlt und stattdessen auf die Einrichtung von DNS verweist, geht dieses Buch nicht weiter auf WINS ein.

5.3 Dynamische Namensauflösung

Die Probleme, die sich durch die Verwaltung von Internet-Hosts mittels einer Hosts-Datei ergaben, wurden bereits an anderer Stelle beschrieben. Als Folge dessen wurde das *DNS* (*Domain Name System* oder auch oft *Domain Name Service*) entwickelt, dessen wesentliche Aufgaben und Funktionen im nachfolgenden Abschnitt erläutert werden.

Das *Domain Name System* (DNS) stellt heutzutage das wichtigste System zur Verwaltung und Zuweisung von IP-Adressen zu Namen dar (Namensauflösung). Dies sicherlich nicht zuletzt aus der Tatsache heraus, dass es sich um ein standardisiertes Verfahren handelt, das in diversen RFCs immer wieder verfeinert und optimiert worden ist. So ist das DNS einer der wichtigsten Internetdienste, der in dem nahezu undurchdringlichen »Internetdschungel« von IP-Adressen die einzige Orientierungshilfe darstellt.

HINWEIS

Das DNS hat nichts mit Routing zu tun, denn es ist daraus grundsätzlich nicht abzuleiten, wo die einzelnen Endgeräte platziert sind. Es geht beim DNS ausschließlich um die Verwaltung von Namen und den zugehörigen IP-Adressen.

5.3.1 Aufgaben und Funktionen

Das DNS ist nicht nur für die Rechneradressierung über »sprechende« Namen zuständig, sondern erfüllt insgesamt einige wesentliche Aufgaben:

- Umwandlung »sprechender« Namen in IP-Adressen
- Umwandlung von IP-Adressen in »sprechende« Namen (Reverse Translation)
- Verwaltung einer oder mehrerer Domänen und ihrer Namensdatenbasis
- Verwaltung von MX-Records – Bereitstellung der Adressinformationen zuständiger Mail-Server für die jeweiligen Zieldomänen

Die Einrichtung von DNS-Servern ist nicht nur für die externe Kommunikation im Internet geboten, sondern sie stellt auch die Grundlage der Adressierung in einem Intranet dar. Jeder Anwender, der auf Informationen eines Intranetservers (unternehmensinterner Webserver) zugreifen will, benötigt den »Kontakt« zu einem internen DNS-Server. Kein Systemverwalter wird ernsthaft auf die Idee kommen, die interne Adressierung eines TCP/IP-Netzwerks auf die Verwendung von IP-Adressen zu beschränken. Die Vielzahl unterschiedlicher Serversysteme in einem Unternehmen würde zu einer »Orientierungslosigkeit« führen, da die verwendeten IP-Adressen keinerlei Rückschlüsse auf den Server zulassen. Die Adressierung eines Servers mit Namen »SAP-FINANZ« ist sicher besser nachzuvollziehen als die Angabe von »192.168.22.1«. Die Verwendung einer Hosts-Datei ist keine vernünftige Alternative, da diese Dateien auf jedem Client-System manuell gepflegt werden müssten.

5.3.2 Auflösung von Namen

Die Idee, die dem DNS zugrunde liegt, ist zunächst einmal sehr einfach. Da das Internet zu groß ist, um seine Namen und IP-Adressen zentral zu verwalten, muss eine Aufteilung in dezentrale Teilbereiche vorgenommen werden. Diese Teilbereiche werden dabei als *Domain* (Domäne) bezeichnet. Das DNS basiert auf der Idee von Domains, also unterteilten Bereichen, die organisatorisch für die Verwaltung der Host-Namen zuständig sind.

HINWEIS

DNS-Domänen besitzen keine inhaltliche Gemeinsamkeit mit Domänen, die beispielsweise in einem Windows-System zum Einsatz kommen.

Allgemein ausgedrückt handelt es sich bei dem Domain Name System (DNS) um eine verteilte hierarchische Datenbank, in der verschiedenste Informationen über die Endgeräte eines IP-Netzwerks gespeichert werden. So erfolgt per DNS beispielsweise die Auflösung von Rechnernamen, die besser zu merken sind als Zahlen, in die zugehörigen IP-Adressen, die wiederum für die weitere Verarbeitung benötigt werden. So ist es beispielsweise viel einfacher, statt einer entsprechenden IP-Adresse Folgendes als Webadresse (ULR) einzugeben:

```
http://www.dilaro.de
```

Internetadressen in der dargestellten Form kennen sicherlich die meisten, obwohl es sich streng genommen überhaupt nicht um Adressen handelt. Denn wie an anderer Stelle dieses Buches erläutert, stellen sich »echte« Internetadressen in folgender Form dar:

```
212.227.109.208
```

Da es naturgemäß schwieriger ist, sich Zahlenfolgen zu merken, wurde eine Systematik entwickelt, die es ermöglicht, einer Internetadresse einen Namen zuzuweisen. So verbirgt sich in dem obigen Beispiel hinter *www.dilaro.de* nichts anderes als die IP-Adresse 212.227.109.208. Die entsprechende Eingabe in der Adresszeile eines Webbrowsers könnte sich demnach auch wie folgt darstellen:

```
http://212.227.109.208
```

Bei der Frage nach der Verwaltung entsprechender Internetadressen und der zugeordneten Namen, wie beispielsweise *www.dilaro.de*, ergibt sich automatisch die Verbindung zum DNS. Das DNS ermöglicht, dass für die einzelnen Endgeräte eines IP-Netzwerks symbolische Namen (Host-Namen) vergeben werden. Auf diese Art und Weise ergibt sich der Zugriff auf ein Gerät nicht über die IP-Adresse, sondern über den zugewiesenen Namen.

Damit das DNS eine Namensauflösung (so wird die Konvertierung symbolischer Namen in IP-Adressen bezeichnet) durchführen kann, werden sogenannte *Nameserver* benötigt, wobei alle Adressen in einer großen hierarchischen, weltweit verteilten Datenbank abgelegt sind. Wenn ein Nameserver eine Adresse nicht umsetzen kann, gibt er die Anfrage an einen ihm übergeordneten Nameserver weiter. Durch dieses Verfahren sind die Adressen leichter zu merken (aussagekräftige Namen statt Zahlenkolonnen) und einfacher zu verwalten. Sobald ein Rechner eine andere IP-Adresse bekommt, muss nur der Eintrag auf dem Nameserver geändert werden. Der Name, unter dem er zu erreichen ist, bleibt gleich.

Organisationen mit eigenen Domains müssen einen Nameserver unterhalten, der die Namen in Internetadressen umsetzt. Dies ist notwendig, damit alle Rechner des Internets die symbolischen Rechnernamen einer Organisation in Internetadressen umsetzen lassen können, ohne die eine Kommunikation nicht möglich ist. Dabei sind Nameserver zunächst einmal nichts anderes als Rechner, die Datenbanken über Namen und die dazugehörigen IP-Adressen der betreffenden Domain verwalten. Ist ein Nameserver ein TLD-Server, so verfügt er über sämtliche Adressen aller anderen Top-Level-Nameserver.

Im Gegensatz zu den Nameservern werden die Programme, die die Informationen eines Nameservers nutzen, mit dem Begriff *Resolver* (Auflöser) umschrieben. Es handelt sich dabei in der Regel um Programme, die in die Anwendungen eingebunden werden und so die Funktionen nutzen (z.B. TELNET). Die Resolver-Software stellt Anfragen an den lokalen Nameserver, um Namen in IP-Adressen zu übersetzen. Entweder sind die dazu benötigten Informationen im lokalen Nameserver vorhanden oder dieser muss seinerseits andere Nameserver konsultieren, um die gewünschte Umsetzung zu leisten.

5.3.3 DNS-Struktur

Bis zum Jahr 1984 wurde die Zuordnung von Namen zu IP-Adressen von einer zentralen Stelle gepflegt, und zwar für alle weltweit vergebenen (offiziellen) IP-Adressen. Zuständig war das *Network Information Center* (NIC) in den USA. Da dieses Verfahren mit dem Anwachsen des Internets zu unübersichtlich wurde, wurde das DNS-Verfahren eingeführt. In Zeiten täglich zunehmender Internetnutzung spielt der Einsatz eines Namensdienstes wie DNS eine immer wichtigere Rolle. Jedoch auch im lokalen Netzwerk eines Unternehmens (LAN, WAN) ist das DNS ein unverzichtbarer Dienst. So werden beim DNS alle Namen (und deren IP-Adressen) in einer Domäne verwaltet, wobei die hierarchische Organisation einer DNS-Datenbank mit der Verzeichnisstruktur eines Dateisystems vergleichbar ist: Beide haben eine umgekehrte baumartige Struktur, bei der die Wurzel oben und die Zweige unten stehen. Namen, die alle Knoten zwischen dem Wurzel- und dem Endknoten enthalten, werden als *vollqualifizierte Domänennamen* (FQDN, *Fully Qualified Domain Name*) bezeichnet.

HINWEIS

Die gesamte Struktur einer hierarchisch organisierten DNS-Datenbank wird auch als *Domain Name Space* (Domänen-Namensraum) bezeichnet. Der Wurzelknoten (Ursprung des Baums) im Domain Name Space wird als *Root Domain* (Wurzel) oder Hauptdomäne bezeichnet. Domänen (Knoten), die direkt dem Wurzelverzeichnis untergeordnet sind, werden als *Top Level Domains* (Top-Level-Domänen) bezeichnet. Jeder Top Level Domain (TLD) können wiederum weitere Domänen (Subdomains) untergeordnet sein.

Die TLD bildet stets die oberste Ebene einer Domäne und wird auch als Wurzelverzeichnis (Root) bezeichnet.

Der gesamte Domänen-Namensraum wird in Zonen unterteilt; diese Zonen (*Subdomains*) wiederum sind Untermengen des DNS-Baums. Die Forderung nach Eindeutigkeit wird bei DNS auf den Bereich einer *Subdomain* beschränkt. So können in unterschiedlichen Subdomains durchaus gleiche Bezeichnungen (Namen) vergeben werden. Um eine große Anzahl von Namen zu verwalten und gleichzeitig den Organisationen Freiheit in der Namenswahl zu ermöglichen, wurde eine hierarchische Struktur entworfen.

Jeder Knoten im DNS-Baum trägt einen Namen, der bis zu 63 Zeichen lang sein kann. Die vollqualifizierten Domänennamen (*Fully Qualified Domain Name* = FQDN) beginnen immer mit dem Zielnamen und gehen zurück zur Root, wobei die einzelnen Knoten jeweils durch Punkte getrennt werden. Das Wurzelverzeichnis wird (laut Standard) durch einen nachgestellten Punkt gekennzeichnet, der jedoch in der Regel nicht mit angegeben wird. Ein vollständiger FQDN könnte somit beispielsweise wie folgt aussehen: *www.dilaro.doc.de*, dabei wäre die Schreibweise *www.dilaro.doc.de.* jedoch die richtige Schreibweise (mit Punkt am Ende). In diesem Beispiel ist *de* die Top Level Domain und jedes weitere Level definiert eine Subdomain (z.B. *doc*) bzw. einen Netzknoten (z.B. *dilaro*).

Jede Zone eines DNS-Baums muss mindestens über einen primären Nameserver verfügen. Ein zweiter (sekundärer) Nameserver sollte aus Gründen des Ausfallschutzes eingerichtet werden. Auf einem primären Nameserver werden in einem solchen Fall dann sekundäre Zonen eingerichtet, die als primäre Zonen auf dem sekundären Nameserver existieren. Umgekehrt werden die primären Zonen des sekundären Nameservers als sekundäre Zonen auf dem primären Nameserver eingerichtet. Die einzelnen Nameserver müssen die jeweiligen Zonendaten untereinander austauschen.

Den größten Domain Name Space stellt das Internet dar. Dort ist eine Reihe sogenannter Root-Nameserver in Betrieb (z.B. im NFSnet, MILNET, SPAN), die für die Top Level Domains verantwortlich sind. Die weitere Verwaltung der Nameserver in den unteren Zonen wird delegiert. In der zweiten und dritten Ebene sind hier juristische Personen wie Behörden und Universitäten mit dem Betrieb der Nameserver betraut. Diese sind jeweils für die Verwaltung ihrer Zweige im DNS-Baum verantwortlich.

5.3.4 DNS-Anfragen

Nach der Erläuterung des Grundprinzips stellt sich die Frage, wie eine entsprechende DNS-Namensauflösung in der Praxis abläuft. Wenn beispielsweise ein Endgerät ein Datenpaket an ein anderes Endgerät versendet, muss es zuerst herausfinden (lassen), welche IP-Adresse das andere Endgerät hat. Erst dann kann die eigentliche Wegewahl (Routing) beginnen, denn die Tabellen zur Wegewahl basieren allesamt auf IP-Adressen.

Um die Auflösung eines Host-Namens zu bewerkstelligen, wird ein entsprechender Nameserver (DNS-Server) eingesetzt. Es wurde bereits erwähnt, dass ein Anwendungsprogramm, das auf die Daten eines DNS-Systems zugreift, sich dabei den Einsatz des sogenannten *Resolver* zunutze macht.

HINWEIS

Der Vorgang, einen Nameserver abzufragen, wird als *Nameserver-Lookup*, als *DNS-Lookup* oder auch als *Forward DNS-Lookup* bezeichnet.

Der *Resolver* ist die Software, die auf einem DNS-Client für den Zugriff auf einen Nameserver sorgt. So erzeugt er auf einem DNS-Client (Host) eine DNS-Anfrage und sendet diese an den Nameserver. Der Nameserver sendet die Antwort (Auflösung des Namens) zurück an den Resolver, der die Daten verarbeitet und an die Anwendung liefert. Der Nameserver liefert die IP-Adresse zu einem vom Resolver übermittelten Namen, sofern sie ihm bekannt ist. Kennt er die IP-Adresse nicht bzw. kann er den Namen nicht auflösen, wird die Anfrage zum übergeordneten Nameserver weitergeleitet. Wenn nötig, wird die Anfrage zur obersten Ebene von Nameservern weitergeleitet, bis die Anfrage aufgelöst werden kann. Die Ergebnisse der letzten Namensauflösung speichert der Nameserver in einem lokalen Zwischenspeicher. Dies verkürzt die Anfrage, falls die IP-Adresse zur Namensauflösung sonst mehrere Nameserver durchlaufen müsste. Auch sind dem Nameserver hierdurch Adressen anderer Nameserver in anderen Zonen des DNS-Baums bekannt. Dadurch kann die Anfrage direkt an einen Nameserver in einer anderen Zone geleitet werden, ohne den Umweg über die oberste Ebene von Nameservern zu gehen.

Der Ablauf einer Namensauflösung ist grundsätzlich ein sehr aufwendiges Verfahren, das hier jedoch in vereinfachter Form dargestellt werden soll, um den generellen Ablauf zu verdeutlichen:

- Sobald eine Namensanfrage erfolgt (z.B. durch eine Anweisung der Form *telnet server01*), wird als Erstes überprüft, ob der lokale Name des betreffenden Endgeräts mit dem Host-Namen (hier: *SERVER01*) identisch ist.
- Ist dies nicht der Fall, wird in der lokalen Hosts-Datei ein Eintrag für den Host (SERVER01) gesucht. Ist ein entsprechender Eintrag vorhanden, wird die zugehörige IP-Adresse an die Anwendung (hier: TELNET) zurückübermittelt.

- Kann der Host-Name in der lokalen Hosts-Datei nicht aufgelöst werden, wird als Nächstes ein DNS-Server (Nameserver) angesprochen. Dies setzt natürlich voraus, dass das anfragende Endgerät auch als DNS-Client konfiguriert worden ist.
- Der DNS-Server (primärer DNS-Server) sucht den übermittelten Host-Namen in seiner Datenbank.
- Findet er den Namen in seiner Datenbank, sucht er die dazugehörige IP-Adresse heraus und übermittelt diese an den anfragenden Host.
- Kann der (primäre) DNS-Server den Host-Namen nicht auflösen, gibt er die Anfrage an einen übergeordneten DNS-Server weiter. Dies kann bis zu einem DNS-Server auf oberster Ebene führen.
- Besteht keine Möglichkeit, den angeforderten Namen aufzulösen, erscheint eine entsprechende Fehlermeldung (unbekannter Host, Zeitüberschreitung o.Ä.).

5.3.5 Umgekehrte Auflösung

Nameserver werden eingesetzt, um vorgegebene Namen in IP-Adressen umzuwandeln bzw. diesen Namen die entsprechenden IP-Adressen zuzuordnen. In der Praxis wird aber auch hin und wieder der umgekehrte Fall, also die Zuordnung eines Host-Namens zu einer vorgegebenen IP-Adresse, vorkommen. Für diesen speziellen Anwendungsfall der umgekehrten Auflösung steht im Internet die Domäne mit dem Namen ARPA zur Verfügung, die als in-addr.arpa. konfiguriert wird. Das Wesentliche bei der umgekehrten Zuordnung von IP-Adressen zu Namen ist, dass den einzelnen Knoten jeweils die IP-Adresse zugewiesen wird.

Die Domäne *in-addr.arpa.* kann insgesamt bis zu 256 Subdomains verwalten. Diese entsprechen dem ersten Oktett der IP-Adresse. Diese Subdomains (des ersten Oktetts) können jeweils 256 Subdomains haben, die dem zweiten Oktett der IP-Adresse entsprechen. Diese wiederum können 256 Subdomains entsprechend dem dritten Oktett der IP-Adresse besitzen. Die letzte Subdomain kann 256 Datensätze entsprechend dem letzten Oktett der IP-Adresse besitzen. Somit entspricht der Wert eines Datensatzes aus dem vierten Oktett der IP-Adresse dem FQDN der IP-Adresse.

HINWEIS

Der umgekehrte Vorgang der Auflösung einer IP-Adresse in einen Host-Namen wird auch als *Reverse DNS-Lookup* bezeichnet. Zum Einsatz kommt dabei eine spezielle Anweisung mit dem Namen NSLOOKUP.

5.3.6 Standard Resource Records

Die Basisdatei eines Nameservers, die auf UNIX-Systemen mit *named.boot* bezeichnet wird und zumeist im Verzeichnis */etc* zu finden ist, zeichnet für die Steuerung der DNS-Ressourcendateien verantwortlich. Windows-Systeme beziehen ihre Konfiguration in der Regel aus der Registry-Datenbank.

Das Satzformat der DNS-Ressourcendateien, die den relevanten Datenbestand aufnehmen sollen, ist festgelegt und besitzt einen besonderen Aufbau. Sie sind dem RFC 1035 entnommen:

- *NAME*
  Name des Eigners dieses Resource Record (Host-Name)
- *TYPE*
  Ein zwei Bytes umfassendes Feld mit folgendem Inhalt:
  - A: IP-Adresse
  - NS: autorisierter Nameserver
  - MD: alte Angabe; neu MX
  - MF: alte Angabe; neu MX
- *CNAME*
  Angabe eines Alias-Namens
- *SOA*
  Gibt den Beginn einer Zone an (Start Of Authority)
- *MB, MG, MR, NULL*
  Experimentell
- *WKS*
  Angabe von Diensten (*well known services*)
- *PTR*
  Angabe eines Zeigers auf eine Domäne
- *HINFO*
  Textinformation zur Beschreibung eines Hosts
- *MINFO*
  Mailbox- oder Mailing-List-Informationen
- *MX*
  Verteiler für Mail-Dienste
- *TXT*
  Zeichenketten

- *CLASS*
  Ein zwei Bytes umfassendes Feld mit folgendem Inhalt:
  - IN: Internet-Protokollfamilie TCP/IP
  - CS: alte Angabe; wird nicht mehr verwendet
  - CH: die CHAOS-Klasse; wird nicht verwendet
  - HS: Hesiod; wird nicht verwendet
- *TTL*
  Ein vier Bytes umfassendes Integer-Feld. Es gibt den Zeitraum (in Sekunden) für beim Nameserver erneut angeforderte DNS-Daten an. Wird hier kein Wert angegeben, so wird der entsprechende Eintrag im SOA-RR verwendet. Bei der Wahl dieses Wertes sollte man sorgfältig vorgehen. Bei einem zu niedrigen Wert wird nämlich die Leistungsfähigkeit des Servers durch häufiges Anfordern reduziert; hingegen wird die Reaktionszeit des Servers negativ beeinflusst, wenn der TTL-Wert (*Time to Live*) zu hoch angesetzt ist.
- *RDLENGTH*
  Ein zwei Bytes umfassendes Feld, das die Länge des folgenden RDATA-Felds angibt
- *RDATA*
  In Abhängigkeit des TYPE- und CLASS-Formats werden hier Daten mit variabler Länge zur Beschreibung der Ressource angegeben.

5.3.7 DNS-Message

Die DNS-Kommunikation wird durch das Wechselspiel zwischen *DNS-Request* (*Resolver*) und *DNS-Response* (*Server*) charakterisiert. Die Datenpakete sind im *DNS Message Format* beschrieben und umfassen die Abschnitte *Header*, *Question*, *Answer*, *Authority* und *Additional Information Sections*.

Wie bereits bei zahlreichen höheren Protokollen bilden auch hier ein *MAC-Header*, ein *IP-Header* und schließlich der *DNS-Header* die Grundlage für die eigentliche DNS-Message. Der *DNS-Header* umfasst die folgenden Felder:

- *Identifikation* (16)
  Erforderlich zur Antwort-Frage-Zuordnung.
- *Parameter* (16)
  Verschiedene Teilparameter werden hinterlegt:
  - operation type: query/response
  - query type: standard/inverse/obsolete
  - answer authorative
  - message is truncated
  - recursion is desired

- recursion is available
- number of questions

- *Anzahl Antworten* (16)
- *Anzahl Quellen* (16)
- *Anzahl Zusätze* (16)

Die Felder der DNS-Message sind hauptsächlich für die Formulierung der *questions* und den Empfang der *answers* zuständig:

- *Anfragen-Information (v)*:
  - Domain-Name der Anfrage
  - Art der Anfrage
  - Klasse der Anfrage (Protokollgruppe)
- *Antwort-Information (v)*:
  - resource domain name
  - type
  - class
  - time to live
  - resource data length
  - resource data
- *Quellen-Information (v)*:
  Enthält den Namen des Servers, der letztlich die Auflösungsinformationen geliefert hat (möglicherweise über die Kontaktaufnahme mehrerer vorgelagerter Server).
- *Zusatz-Information (v)*

5.3.8 Dynamic DNS (DDNS)

Unter *Dynamic DNS* versteht man die automatische Anpassung der Namensauflösung bei Änderung der IP-Adresse eines Endgeräts (z. B. Rechner). So stellt DDNS die automatische Anpassung der Namensauflösung bei der Änderung der IP-Adresse eines IP-Knotens sicher. Davon sind sowohl der *Forward-* (Auflösung vom Namen zur IP-Adresse) als auch der *Reverse*-Prozess (Auflösung von IP-Adresse zum Namen) betroffen. Der wesentliche Unterschied zum »klassischen DNS« besteht darin, dass die DNS-Registrierung der IP-Adresse eines Clients automatisch erfolgt und somit eine explizite Pflege einer statischen DNS-Datenbasis nicht mehr erforderlich ist. Die Registrierung wird von einem DHCP-Server nach folgendem Verfahren vorgenommen:

- Der Client sendet eine IP-Adressanforderung an den DHCP-Server.
- Der DHCP-Server empfängt die Anforderung, teilt eine IP-Adresse zu und legt die Gültigkeitsdauer fest (*Lease*).
- Die IP-Adresse des Clients wird vom DHCP-Server als A-Adresse beim DNS-Server registriert.
- Der DHCP-Server registriert beim DNS-Server den PTR-Eintrag zur Reverse-Zone der Domäne.

HINWEIS

Windows-Systeme können ihre IP-Adresse auch direkt beim DNS-Server registrieren; andere Clients werden über DHCP-Server registriert. Außerhalb der Windows-Betriebssysteme wird DDNS in der UNIX-Welt auch von BIND ab Version 8.1.2 unterstützt. Die RFCs 2136 und 2137 beschreiben die als DDNS definierten dynamischen DNS-Aktualisierungen.

5.3.9 Zusammenspiel von DNS und Active Directory

Verzeichnisdienste repräsentieren umfangreiche Datensammlungen, die möglichst viele und unterschiedliche Unternehmensressourcen in einer einzigen Datenbank zusammenführen. Eine solche Verzeichnisdatenbank wird zur Adressierung, Dokumentation und Inventarisierung eingesetzt und liefert dem Unternehmen eine solide Planungs- und Administrationsgrundlage.

Active Directory ist ein solcher Verzeichnisdienst und stellt eher eine organisatorische Kommunikationsstruktur dar als ein Kommunikationsprotokoll. Auch wenn es unterschiedliche Verzeichnisdienste gibt, haben sich die *Active Directory Services* (ADS) aus dem Hause Microsoft zumindest auf allen Windows-Plattformen durchgesetzt; aus diesem Grund stehen diese Dienste im Mittelpunkt der nachfolgenden Betrachtung. Dabei ist von entscheidender Bedeutung, dass bei einer Planung und Einführung der DNS-Integration in *Active Directory Services* (ADS) besondere Aufmerksamkeit gewidmet wird.

Mit *Active Directory Services* wird eine äußerst komplexe und vor allem global gültige Unternehmensdatenbank betrieben, die Informationen zu Benutzern und Ressourcen enthält sowie ihre Verknüpfungen und Freigaben. Mit ihr soll

- eine einheitliche Anmeldung ermöglicht,
- die Benutzer- und Ressourcenadministration vereinheitlicht und
- das Unternehmen hinsichtlich Netzwerken, Benutzern und sonstigen Ressourcen abgebildet werden.

Um diese Ziele zu erreichen, ist eine sehr gründliche und zeitlich aufwendige Projektphase erforderlich, denn die unterschiedlichen Implikationen und Abhängig-

keiten existierender Strukturen müssen konsequent ausnahmslos in die neue Active-Directory-Struktur überführt werden.

Active Directory Service (ADS)

Innerhalb einer ADS-Struktur werden Objekte und ihre Eigenschaften in sogenannte »Schemata« gespeichert. Dem Objekt »Benutzer« ist beispielsweise die Eigenschaft »Vorname« oder »Beschreibung« zugeordnet, wobei diese Eigenschaften natürlich mehrfach in unterschiedlichen Objekten auftreten können. Objekt-Container werden als Organisationseinheit bezeichnet und stellen den geografischen Bezug zur jeweiligen Domäne her.

Die ADS-Domänenstruktur baut auf einem streng hierarchischen Konzept auf, in dem Domänen und untergeordnete Subdomänen einem umfassenden *Namespace* zugewiesen werden. Dieser repräsentiert eine DNS-Namensstruktur, bestehend aus einem oder mehreren Namespace(s), in dem/denen die verschiedenen Domänen zusammengefasst sind.

Die *Active Directory Services* lassen sich in ihren Strukturen auf einer Vier-Komponenten-Architektur abbilden:

- *Datenmodell*
  Als Grundlage dient der X.500-Verzeichnisdienst sowie das *Lightweight Directory Access Protocol* (LDAP). Active Directory bedient sich einer streng hierarchischen Struktur von Ressourcen, Diensten und anderer Objekte.
- *Schema*
  In einem Schema wird beschrieben, welche Objekttypen im Directory gespeichert werden. Beispiel: Es werden drei Objektklassen definiert: Server, Organisationseinheiten (OU) und Benutzer. Diesen Klassen werden dann Objekte mit bestimmten Attributen einzelner Werte zugeordnet, wie beispielsweise der Wert 10.1.1.1 für das Attribut *IP-Adresse* und das Objekt *Printserver*. Schemata lassen sich natürlich jederzeit an neue Gegebenheiten anpassen, unterliegen dabei allerdings restriktiven Sicherheitsvorkehrungen hinsichtlich ihrer Administrationsrechte.
- *Sicherheit*
  ADS verwendet Kerberos zur Implementierung von Sicherheitsmechanismen. Dies ist insbesondere für die Authentifizierung beliebiger Ressourcen, Benutzer und Dienste relevant.
- *Administration*
  Die Active Directory Services ermöglichen eine bedarfsgerechte Möglichkeit zur Verwaltung mittels einer angepassten Rechtevergabe durch den Systemverwalter. Die Vergabe globaler Administrationsrechte für eine ganze Domäne, wie es beim herkömmlichen Windows-Domänenmodell üblich war, gehört der Vergangenheit an.

Die wichtigsten Komponenten eines *Active Directory Service* sind:

- *Namespace*
  DNS-Namensstruktur; sie umfasst die Root-DNS-Domäne samt ihren delegierten Sub-Domänen
- *Domäne*
  Ansammlung von Ressourcen, die einen gemeinsamen Namespace, ein gemeinsames Schema, eine gemeinsame Konfiguration und einen globalen Katalog (GC) besitzen
- *Domänenstruktur*
  Ansammlung von Domänen mit unterschiedlicher Verwendung der Sub-Domänen
- *Gesamtstruktur*
  Mehrere Domänen verfügen über verschiedene Namespaces, teilen sich aber dasselbe Schema, dieselbe Konfiguration und denselben GC.
- *Organisationseinheiten*
  Ein Container für Objekte innerhalb einer Domäne
- *Objekte*
  Ressource, Dienst oder Benutzerkonto innerhalb der ADS. Sie besitzen Attribute und werden mit Werten versehen, um eine eindeutige Identifizierung zu ermöglichen.
- *Schemata*
  Beschreibung der Objekte und deren Eigenschaften innerhalb der ADS
- *Standorte*
  Gruppe von IP-Subnetzen

DNS-Integration

Mit der Einführung der *Active Directory Services* (ab Windows 2000 Server) erhält DNS nun auch für Windows-Plattformen eine besonders wichtige Bedeutung. Während die Namensauflösung im Windows-Netzwerk früher durch den WINS-Dienst und entsprechende WINS-Server übernommen wurde, erfolgt dies nunmehr über DNS. Um sich beispielsweise an einem Windows-Domaincontroller anzumelden, erfolgt die Suche und Identifikation über DNS; insbesondere erfolgt die Kontaktaufnahme mit einem für die Domäne zuständigen DNS-Server, sofern auf einem Domaincontroller ADS installiert wird. Bleibt die Kontaktaufnahme erfolglos, so initiiert die Installationsroutine für ADS die Einrichtung eines DNS-Servers.

Voraussetzung für einen reibungslosen Einsatz von ADS ist allerdings die Verwendung der Serviceeinträge (*SRV-Records*), mit denen eine direkte Verbin-

dung zu wichtigen Diensten innerhalb der ADS hergestellt wird. So werden über die SRV-Records beispielsweise Domaincontroller oder andere Diensteserver ermittelt (bei UNIX-Systemen funktioniert dies allerdings erst ab BIND-Version 8.1.2). Entsprechende RFCs (2136 und 2137) beschreiben die als DDNS (*Dynamic DNS*) definierten dynamischen DNS-Aktualisierungen. Sowohl der Windows-Client als auch ein Windows-Server können beim DNS-Server die erforderlichen Registrierungen vornehmen. Eine enge Verzahnung mit dem DHCP-Server ist daher auch Bestandteil einer ADS- und DDNS-Implementierung.

Vorteile und Nachteile

In einer kurzen Übersicht sollen Vorteile und Nachteile des *Active Directory Service* einander gegenübergestellt werden:

- Vorteile
  - zentrale Verwaltungskonsole des gesamten Unternehmensnetzwerks (Einsatz von Gruppenrichtlinien)
  - einheitliche Anmeldung für alle Benutzer
  - einfache Integrierbarkeit bestehender Windows-Server mit älteren Betriebssystemen
  - Einsatz von Kerberos zur Absicherung notwendiger Vertrauensstellungen innerhalb der *Active Directory Services*
  - rasche Anpassungen an organisatorische Veränderungen innerhalb des Unternehmens durch flexible Strukturen
- Nachteile
  - *Active Directory Services* ist in Unternehmen mit Microsoft-unabhängigen Plattformen nicht einsetzbar – eine Umstellung von UNIX-basierten Systemen ist ohne Windows-Server nicht möglich.
  - Active Directory erfordert den Einsatz bestimmter DNS-Implementierungen (DDNS ist nicht unbedingt erforderlich, wird allerdings empfohlen), die zumindest Service-Ressourceneinträge (*SRV Records*) unterstützen müssen.
  - Active Directory erfordert eine globale Anpassung sämtlicher Administrationsaktivitäten und damit eine unter Umständen geänderte Vorgehensweise bei der Wahrnehmung bisheriger Serviceleistungen gegenüber den Benutzern.
  - Die Zusammenführung »alter« Windows-Domänen erfordert ein Höchstmaß an Sorgfalt und ausreichend geplante Mechanismen zur Realisierung eines möglichst störungsfreien Übergangs.

5.3.10 Auswahl der Betriebssystemplattform

In der Praxis wird heute in allen wichtigen Betriebssystemen das DNS als Dienst zur Namensauflösung verwendet. Selbst Microsoft empfiehlt bei Neu-Installationen den Einsatz von DNS und nicht mehr WINS, der viele Jahre den von Microsoft bevorzugten eigenen Dienst repräsentierte.

Mittlerweile erfolgt die Konfiguration von DNS auch über komfortable grafische Benutzeroberflächen, sodass einer raschen Einrichtung von DNS auf verschiedenen Betriebssystemplattformen nichts mehr im Wege steht.

5.4 Namensauflösung in der Praxis

Der Einsatz eines DNS-Systems bedingt das Einrichten bzw. die Verfügbarkeit eines Servers (DNS-Server) und die entsprechende Konfiguration der einzelnen Clients (DNS-Clients).

5.4.1 Vorgaben und Funktionsweise

Auf eine Detailbetrachtung der verschiedenen DNS-Servertypen (*primary*, *secondary*, *slave*, *forwarder*, *cache*) soll an dieser Stelle verzichtet werden; hier gilt der Hinweis auf weiterführende Literatur. Nachfolgend soll der Schwerpunkt auf der Einrichtung eines *Primary Name Server* (PNS) und eines *Secondary Name Server* (SNS), dem für einen Ausfall des PNS erforderlichen Backup-Systems, liegen.

Grundsätzlich erfolgt die Kommunikation innerhalb des DNS zwischen dem DNS-Server und dem DNS-Client (*Resolver*) in Form eines »Frage-und-Antwort-Spiels«. Kennt der lokale DNS-Server die IP-Adresse des angefragten Namens nicht, so muss er sich bei anderen, ihm bekannten Nameservern danach »erkundigen«.

Der grundsätzliche Ablauf einer DNS-Anfrage ist Abbildung 5–1 zu entnehmen. Wenn die *Root-Server* die Anfrage des lokalen DNS-Servers nicht beantworten können, so teilen sie dem lokalen DNS-Server die Zuständigkeiten (*Referrals*) für die angefragte Domain der ersten Hierarchiestufe mit (so z.B. den Nameserver des *Deutschen Network Information Centers*, wenn es sich um die Top Level Domain »de« handelt). Wenn auch dieser Nameserver den angefragten Namen nicht in eine ihm bekannte IP-Adresse umsetzen kann, so kennt er doch zumindest den Nameserver, der für die Second Level Domain zuständig ist. (Wenn beispielsweise der Host-Name *www.meier.de* angefragt wurde, so ermittelt dieser Top-Level-Nameserver nunmehr den zuständigen Second-Level-Nameserver für die Domain *meier.de*.) Wird dieser Server im nächsten Schritt kontaktiert, so liefert er dem ursprünglich angefragten lokalen DNS-Server die gewünschte IP-Adresse, da diese ja in seiner lokalen DNS-Datenbasis geführt wird. Nun kann der lokale DNS-Server die Anfrage seines Clients beantworten.