DNS

Christian Zahler

11 Domain Name System (DNS)

11.1 Allgemeines

DNS ist ein Protokoll der Anwendungsschicht (OSI-Schicht 7), das für die Verwendung mit der TCP/IP-Protokollsuite entwickelt wurde. Hauptaufgabe ist die Zuordnung von Computernamen zu IP-Adressen.

(a) **über einen DNS-Server**

(b) **statisch**:

Datei `HOSTS` im Verzeichnis

`\WINNT\SYSTEM32\DRIVERS\ETC`

bearbeiten mit Editor.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for
# Windows NT. # This file contains the mappings of IP addresses
# to host names. Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by
# the corresponding host name. The IP address and the host name
# should be separated by at least one space.
#
# Additionally, comments (such as these) may be inserted on
# individual lines or following the machine name denoted by a '#'
# symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
192.168.0.1     ilg.at
```

Diese Datei ordnet jeder IP-Adresse einen DNS-Namen *("friendly name")* zu.

Im selben Verzeichnis befindet sich auch die `LMHOSTS`-Datei, die die Zuordnung von IP-Adressen zu NetBIOS-Namen regelt (NetBIOS-Namen werden als "PC-ID" von Win NT standardmäßig verwendet).

Wichtig: Jeder PC im Intranet muss dieselbe HOSTS-Datei bekommen, da sonst der Server nicht mit dem *friendly name* angesprochen werden kann. (Also: Datei auf jeden PC im Netz kopieren!!!)

Für einen Anwender sind IP-Zahlenkombinationen schwer zu merken. Es werden daher statt dieser Zahlendarstellung symbolische Namen verwendet.

So gibt es etwa einen Server mit dem Namen

`noe.wifi.at`

Diesem Servernamen entspricht eine eindeutige IP-Adresse. Dabei setzt sich der Name aus Teilen zusammen, die eine Hierarchie angeben: Das Teilnetzwerk `noe` (fachchinesisch bezeichnet man ein solches Teilnetz als Domäne, englisch *domain*) ist ein Teil des Netzwerks `wifi`, dieses wiederum ein Teil des Netzwerks `at` (für Österreich). Das `at`-Netzwerk ist ein Teil der Domäne `the world` (die aber nie angegeben zu werden braucht).

Die Länderkennung ist ein Beispiel für eine *Top Level Domain* (TLD); so werden die „Haupt-Domänen" bezeichnet, die entweder einem Land oder einer „Kategorie" entsprechen.

Die Zuordnung IP-Adressen zu logischen Namen muss von einem eigenen Rechner durchgeführt werden, dem Domain Name System-Server (DNS-Server). Wenn nun ein Anwender einen Server `noe.wifi.at` anwählt, so "fragt" die Station zunächst beim DNS-Server des Anwenders (der meist beim Provider steht), ob er die IP-Adresse von `noe.wifi.at` kennt. Das wird nicht der Fall sein. In diesem Fall hat der DNS-Server die IP-Adresse des nächstliegenden DNS-Servers gespeichert und fragt bei diesem an, ob er die IP-Adresse kennt. Das geht so lang, bis ein DNS-Server erfolgreich ist, die IP-Adresse wird übermittelt, die Datenübertragung kann beginnen.

Das Internet ist also ein so genanntes **Teilstrecken-Netzwerk**; es genügt, wenn jeder Internet-Knotenrechner mit einem weiteren Knoten verbunden ist. Die physikalische Datenübertragung wird über äußerst leistungsfähige Kabel, so genannte „Backbones" realisiert.

Die zentrale Verwaltung der Domain-Namen mit den Top-Level-Domains `.com`, `.net`, `.org` und `.int` obliegt der **InterNIC**, einer Kooperation aus dem kommerziellen Unternehmen NSI *(Network Solutions Inc.)*, der Telefongesellschaft *AT&T* sowie der *US National Science Foundation*. Bisher wurden die angegebenen Domains ausschließlich von der NSI im Auftrag der InterNIC verwaltet. Die jährliche „Miete" eines Domännamens kostet ca. 50 US-$. Die Domain-Verwaltung soll jedoch bis 2001 von der NSI an die nichtkommerzielle Organisation ICANN *(International Corporation for Assigned Names and Numbers)* übergeben werden. Die Datenbank der NSI ist unter `www.networksolutions.com/cgi-bin/whois/whois` zu finden.

Die IANA *(Internet Assigned Numbers Authority, www.iana.org)* verwaltet die IP-Adressen.

Einen IP-Adressen-Index findet man unter `ipindex.dragonstar.net`.

Die ISPA *(Internet Service Provider Association Austria – www.ispa.at)* ist die Vereinigung der österreichischen Internet Service Provider, quasi eine „Dachorganisation". Die NIC.AT GmbH, ein Unternehmen der ISPA, ist mit der Verwaltung und Vergabe der Domänennamen mit dem Top Level Domain `.at` beauftragt (`www.nic.at`). Registrierungen und Online-Abfragen von at-Domainen sind unter `www.namen.at` möglich.

Dabei gibt es zum Beispiel als Länder-Top Level Domain (ISO-Norm 3166):

`at`	Austria (Österreich)
`de`	Deutschland
`jp`	Japan
`us`	USA (fehlt meist)

Zusätzlich zu den landesspezifischen Erweiterungen gab es folgende Kennzeichnungen, die ursprünglich nur US-amerikanischen Einrichtungen vorbehalten waren:

`com`	company (Firma)
`gov`	government (Regierung) – US
`edu`	education (Universitäten) – US
`mil`	military (Militär) – US
`int`	internationale Organisation
`org`	organization (gemeinnützige Organisation)
`net`	Provider

Nun werden die Adressen von 28 lizenzierten Firmen vergeben. Diese Firmen werden im CORE *(Council of Registrars)* zusammengefasst. Die neuen TLDs lauten:

`firm`	Firmen und Unternehmen
`arts`	Kunst und Kultur
`info`	Informationsservices
`rec`	Unterhaltung und Freizeit
`web`	WWW-Aktivitäten
`store`	Warenangebote
`nom`	Restkategorie

11.2 Ablauf einer DNS-Abfrage:

Quelle: Hilfe zu Microsoft Windows 2000 Server, alle Abb. © Microsoft Corp.

Wenn ein DNS-Cient nach einem Namen sucht, der in einem Programm verwendet wird, führt er zum Auflösen des Namens eine Abfrage der DNS-Server durch. Jede vom Client gesendete Abfragemeldung enthält drei Informationen, mit denen eine Frage an den Server festgelegt wird:

- Einen festgelegten **DNS-Domänennamen**, der als voll qualifizierter Domänenname *(FQDN = Fully Qualified Domain Name)* angegeben ist.
- Einen festgelegten **Abfragetyp**, über den entweder ein Ressourceneintrag nach Typ oder eine festgelegte Art von Abfragevorgang angegeben wird.
- Eine festgelegte **Klasse** für den DNS-Domänennamen. Für DNS-Server unter Windows sollte diese Klasse immer als Internetklasse (IN-Klasse) angegeben werden.

Bei dem angegebenen Namen kann es sich zum Beispiel um den FQDN für einen Computer handeln, etwa `host-a.beispiel.microsoft.com`, und der Abfragetyp wird so festgelegt, dass über diesen Namen nach einem A-Ressourceneintrag (Adresse) gesucht wird. Eine DNS-Abfrage ist im Grunde eine zweiteilige Frage des Clients an den Server, z. B. "Bestehen A-Ressourceneinträge für einen Computer namens `hostname.beispiel.microsoft.com`?" Wenn der Client eine Antwort vom Server empfängt, liest er den zurückgegebenen A-Ressourceneintrag, wertet ihn aus und erhält auf diese Weise die IP-Adresse des Computers, den er per Namen abgefragt hatte.

Auflösungen werden mit DNS-Abfragen auf unterschiedliche Arten durchgeführt. Ein Client kann eine Abfrage ggf. lokal beantworten, indem er zwischengespeicherte Daten aus einer vorherigen Abfrage verwendet. Der DNS-Server kann zum Beantworten einer Abfrage eigene zwischengespeicherte Ressourceneintragsdaten verwenden. Um dem anfragenden Client eine vollständige Namensauflösung zu ermöglichen, kann ein DNS-Server auch andere DNS-Server kontaktieren oder abfragen und dann eine Antwort zurück an den Client senden. Dieser Vorgang wird als Rekursion bezeichnet.

Darüber hinaus kann auch der Client selbst versuchen, eine Verbindung zu weiteren DNS-Servern herzustellen, um einen Namen aufzulösen. In einem solchen Fall verwendet der Client zusätzliche eigene Abfragen, die auf den Referenzantworten von Servern basieren. Dieser Vorgang wird als Iteration bezeichnet.

Im Allgemeinen wird ein DNS-Abfragevorgang in zwei Schritten durchgeführt:

- Auf einem Clientcomputer wird eine Namensabfrage gestartet und zum Auflösen an

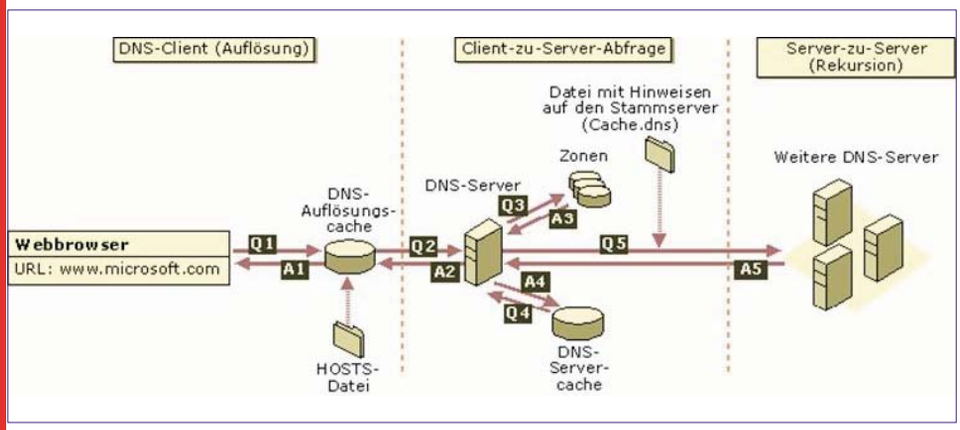
einen Auflösungsdienst, den DNS-Clientdienst, weitergeleitet.

- Wenn die Abfrage nicht lokal aufgelöst werden kann, können nach Bedarf DNS-Server zum Auflösen des Namens abgefragt werden.

Diese beiden Vorgänge werden in den folgenden Abschnitten näher erläutert.

11.2.1 Teil 1: Der lokale Auflösungsdienst

Die folgende Grafik zeigt eine Übersicht über den gesamten DNS-Abfrageprozess.



Wie aus den ersten Schritten des Abfrageprozesses zu ersehen ist, wird in einem Programm auf dem lokalen Computer ein DNS-Domänenname verwendet. Die Abfrage wird dann an den DNS-Clientdienst weitergeleitet, um eine Auflösung mit Hilfe lokal zwischengespeicherter Daten durchzuführen. Wenn der abgefragte Name aufgelöst werden kann, wird die Abfrage beantwortet, und der Prozess ist abgeschlossen.

Der Zwischenspeicher des lokalen Auflösungsdienstes kann Namensdaten enthalten, die aus zwei möglichen Quellen stammen:

- Wenn eine Hosts-Datei lokal konfiguriert wurde, werden beim Starten des DNS-Clientdienstes alle Zuordnungen von Namen zu Adressen aus dieser Datei in den Zwischenspeicher geladen.
- Ressourceneinträge, die in Antworten aus vorherigen DNS-Abfragen enthalten sind, werden dem Zwischenspeicher hinzugefügt und für eine bestimmte Zeit gespeichert.

Wenn für die Abfrage kein passender Eintrag im Zwischenspeicher vorhanden ist, wird der Auflösungsprozess fortgesetzt, indem der Client zum Auflösen des Namens einen DNS-Server abfragt.

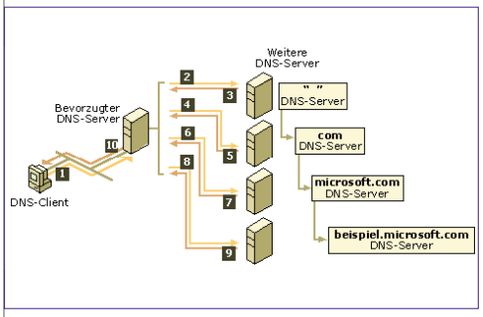
11.2.2 Teil 2: Abfragen eines DNS-Servers

Wie in der oben stehenden Grafik dargestellt, fragt der Client zunächst einen bevorzugten DNS-Server ab. Der zu Anfang des Client/Server-Abfrageprozesses verwendete Server wird aus einer globalen Liste ausgewählt.

Wenn ein DNS-Server eine Abfrage empfängt, überprüft er zunächst, ob er die Abfrage auf der Grundlage von Ressourceneintragsdaten, die in einer lokal konfigurierten Zone auf dem Server enthalten sind, autorisierend beantworten kann. Entspricht der abgefragte Name einem entsprechenden Ressourceneintrag in den lokalen Zonendaten, antwortet der Server autorisierend, indem er diese Daten zum Auflösen des abgefragten Namens verwendet.

Stehen für den abgefragten Namen keine Zonendaten zur Verfügung, überprüft der Server als Nächstes, ob er den Namen mit Hilfe lokal zwischengespeicherter Daten aus vorherigen Abfragen auflösen kann. Wird hier eine Entsprechung gefunden, antwortet der Server mit diesen Daten. Auch in diesem Fall ist die Abfrage abgeschlossen, wenn der bevorzugte Server mit einer entsprechenden Antwort aus dem Zwischenspeicher auf den anfragenden Client reagieren kann.

Wird auf dem bevorzugten Server weder in den Daten des Zwischenspeichers noch in den Zonendaten eine entsprechende Antwort für den abgefragten Namen gefunden, kann der Abfragevorgang fortgesetzt werden, indem der Name mit einem Rekursionsprozess vollständig aufgelöst wird. Für diese Art der Namensauflösung werden weitere DNS-Server zur Unterstützung herangezogen. In der Standardeinstellung wird der Server vom DNS-Clientdienst aufgefordert, einen Rekursionsprozess zu verwenden, um vor dem Antworten die Namen für den Client vollständig aufzulösen. Die in den meisten Fällen verwendete Standardkonfiguration des DNS-Servers für die Unterstützung des Rekursionsprozesses ist in der folgenden Grafik dargestellt.



Damit der DNS-Server die Rekursion ordnungsgemäß ausführen kann, benötigt er zunächst unterstützende Kontaktinformationen über andere DNS-Server im DNS-Domänennamespace. Diese Daten stehen in Form von Hinweisen auf den Stammserver zur Verfügung. Dies ist eine Liste vorläufiger Ressourceneinträge, die vom DNS-Dienst für die Suche nach anderen DNS-Servern verwendet werden kann, die für den Stamm der DNS-Domänennamespacestruktur autorisierend sind. Stammserver sind autorisierend für den Domänenstamm und die Domänen der obersten Ebene in der Namespacestruktur der DNS-Domäne.

Mit Hilfe der Hinweise auf den Stammserver für die Suche nach Stammservern kann ein DNS-Server den Rekursionsvorgang abschließen. Theoretisch ermöglicht dieser Prozess jedem DNS-Server die Suche nach autorisierenden Servern für alle anderen DNS-Domänennamen, die auf einer beliebigen Ebene der Namespacestruktur verwendet werden.

Angenommen, ein Client fragt einen einzelnen DNS-Server nach dem Namen `host-b.beispiel.microsoft.com` ab, und für die Suche wird der Rekursionsprozess verwendet. Dieser Prozess wird dann aktiviert, wenn ein DNS-Server und ein Client gestartet werden und keine lokal zwischengespeicherten Daten zum Auflösen der Namensabfrage zur Verfügung stehen. Es wird davon ausgegangen, dass sich der über den Client abgefragte Name auf einen Domänennamen bezieht, für den auf dem Server in den konfigurierten Zonen keine Daten zur Verfügung stehen.

Zunächst analysiert der bevorzugte Server den vollständigen Namen und stellt dann fest, dass für die Domäne der obersten Ebene, "com", der Standort des autorisierenden Servers benötigt wird. Dann wird eine iterative Abfrage an den DNS-Server für "com" gesendet, um eine Referenz zu dem Server für "microsoft.com" anzufordern. Als Nächstes erhält der DNS-Server für "beispiel.microsoft.com" eine Referenzantwort vom Server für `microsoft.com`.

Schließlich wird eine Verbindung zu dem Server für `beispiel.microsoft.com`. hergestellt. Da dieser Server den abgefragten Namen als Teil der konfigurierten Zonen enthält, sendet er eine autorisierte Antwort an den ursprünglichen Server, von dem aus die Rekursion gestartet wurde. Wenn der ursprüngliche Server die Mitteilung empfängt, dass auf die angeforderte Abfrage eine autorisierte Antwort vorliegt, sendet er sie an den anfordernden Client weiter, und der rekursive Abfrageprozess ist abgeschlossen.

Obwohl der rekursive Abfrageprozess ressourcenintensiv sein kann, wenn er wie oben beschrieben durchgeführt wird, bietet er für den DNS-Server einige Leistungsvorteile. Während des Rekursionsprozesses erhält der DNS-Server, über den das rekursive Lookup durchgeführt wird, z. B. Informationen über den DNS-Domänennamespace. Diese Informationen werden vom Server zwischengespeichert und können erneut verwendet werden, um die Beantwortung entsprechender nachfolgender Abfragen zu beschleunigen. Im Laufe der Zeit kann die Zahl der zwischengespeicherten Daten so anwachsen, dass ein beträchtlicher Teil der Serverspeicherressourcen verwendet wird, obwohl sie gelöscht werden, wenn der Abfragezyklus des DNS-Dienstes gestartet oder beendet wird.

11.3 Andere Abfrageantworten

Bei den vorangegangenen Erläuterungen von DNS-Abfragen wurde davon ausgegangen, dass der Prozess mit einer positiven Antwort an den Client abgeschlossen wird. Bei Abfragen können jedoch auch andere Antworten zurückgegeben werden. Es folgt eine Liste der häufigsten Antworten:

- Autorisierende Antwort
- Positive Antwort
- Referenzantwort
- Negative Antwort

Bei einer autorisierenden Antwort handelt es sich um eine positive Antwort an den Client, bei der das Autoritätsbit in der DNS-Meldung gesetzt ist. Auf diese Weise wird gekennzeichnet, dass die Antwort von einem Server emp-

fangen wurde, der für den abgefragten Namen über direkte Autorität verfügt.

Eine positive Antwort kann aus dem abgefragten Ressourceneintrag oder einer Liste von Ressourceneinträgen (auch Ressourceneintragssatz genannt) bestehen, die dem abgefragten DNS-Domänennamen und dem in der Abfragemeldung angegebenen Eintragstyp entspricht.

Eine Referenzantwort enthält zusätzliche Ressourceneinträge, deren Namen oder Typen in der Abfrage nicht angegeben sind. Dieser Antworttyp wird an den Client zurückgegeben, wenn der Rekursionsprozess nicht unterstützt wird. Die Einträge stellen hilfreiche Referenzantworten dar, die der Client verwenden kann, um die Abfrage mit Hilfe eines Iterationsprozesses fortzusetzen.

Eine Referenzantwort umfasst weitere Daten, z. B. Ressourceneinträge, die von dem abgefragten Typ abweichen. Wenn der abgefragte Hostname z. B. `www` ist und für diesen Namen in dieser Zone keine A-Ressourceneinträge, aber ein CNAME-Ressourceneintrag für `www` gefunden wird, kann der DNS-Server diese Information in die Antwort an den Client einschließen.

Kann der Client die Iteration verwenden, so vermag er mit Hilfe der in der Referenzantwort enthaltenen Informationen selbst zusätzliche Abfragen durchführen, um den Namen vollständig aufzulösen.

Eine negative Antwort vom Server kann darauf hinweisen, dass eines von zwei möglichen Ergebnissen gefunden wurde, während der Server versuchte, die Abfrage vollständig und autorisierend zu verarbeiten und rekursiv aufzulösen:

Ein autorisierender Server meldet, dass der abgefragte Name im DNS-Namespace nicht vorhanden ist.

Ein autorisierender Server meldet, dass der abgefragte Name zwar existiert, für diesen Namen jedoch keine Einträge des angegebenen Typs vorhanden sind.

Vom Auflösungsdienst werden die Abfrageergebnisse in Form einer positiven oder negativen Antwort an das anfordernde Programm weitergeleitet und zwischengespeichert.

11.3.1 Funktionsweise der Iteration

Bei einer Iteration handelt es sich um eine Art der Namensauflösung, die zwischen DNS-Clients und -Servern unter folgenden Bedingungen ausgeführt wird:

- Der Client fordert das Verwenden der Rekursion an, aber die Rekursion ist auf dem DNS-Server deaktiviert.
- Der Client fordert beim Abfragen des DNS-Servers das Verwenden der Rekursion nicht an.

Über eine iterative Abfrage informiert der Client den DNS-Server darüber, dass er von ihm die bestmögliche sofort verfügbare Antwort erwartet und keine Verbindung zu anderen DNS-Servern hergestellt werden soll.

Beim Verwenden der Iteration beantwortet ein DNS-Server eine Clientabfrage unter Berücksichtigung der abgefragten Namensdaten mit den eigenen Namespaceinformationen. Wenn ein DNS-Server im Intranet von einem lokalen Client z. B. die Abfrage nach `www.microsoft.com` empfängt, kann er die Antwort möglicherweise aus dem Namenszwischenspeicher zurückgeben. Ist der abgefragte Name im Namenszwischenspeicher des Servers aktuell nicht vorhanden, kann der Server mit einer Referenz antworten, d. h. einer Liste der NS- und A-Ressourceneinträge anderer DNS-Server, die dem abgefragten Namen am ehesten entsprechen.

Bei einer Referenzantwort übernimmt der DNS-Client die Verantwortung dafür, zur Namensauflösung iterative Abfragen an andere konfigurierte DNS-Server zu senden. Zum Auffinden der DNS-Server, die für die Domäne `com` autorisierend sind, kann der DNS-Client die Suche z. B. bis zu den Stammdomänenservern im Internet ausweiten. Nachdem ein Kontakt zu den Internetstammservern hergestellt ist, kann der Client weitere iterative Antworten von den DNS-Servern empfangen, die auf die Internet-DNS-Server für die Domäne `microsoft.com` zeigen. Wenn dem Client Einträge für diese DNS-Server zur Verfügung stehen, kann er eine weitere iterative Abfrage an die externen Microsoft DNS-Server im Internet senden, die mit einer endgültigen und autorisierenden Antwort reagieren können.

Beim Verwenden der Iteration kann ein DNS-Server bei der Auflösung einer Namensabfrage Unterstützung bieten, die über das Senden der für ihn bestmöglichen Antwort an den Client hinausgeht. Bei den meisten iterativen Abfragen verwendet ein Client eine lokal konfigurierte Liste von DNS-Servern, um einen Kontakt zu anderen Namensservern im DNS-Namespace herzustellen, wenn die Abfrage vom primären DNS-Server nicht aufgelöst werden kann.

11.3.2 Funktionsweise des Zwischenspeicherns

Beim Verarbeiten von Clientabfragen mit Hilfe von Rekursion oder Iteration ermitteln DNS-Server umfangreiche Informationen zum DNS-Namespace. Diese Informationen werden dann vom Server zwischengespeichert.

Das Zwischenspeichern bietet eine Möglichkeit, die Leistung für DNS-Auflösungen bei nachfolgenden Abfragen bekannter Namen zu beschleunigen, wodurch der DNS-bezogene Netzwerkverkehr deutlich reduziert wird.

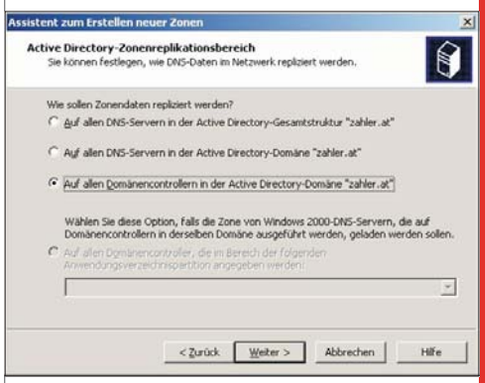
Beim Durchführen rekursiver Abfragen für Clients werden Ressourceneinträge von DNS-Servern vorübergehend zwischengespeichert. Zwischengespeicherte Ressourceneinträge enthalten empfangene Informationen von DNS-Servern, die für die DNS-Domänennamen autorisierend sind. Die Informationen stammen aus iterativen Abfragen und werden zum Suchen und vollständigen Beantworten rekursiver Abfragen für einen Client verwendet. Wenn andere Clients zu einem späteren Zeitpunkt in neuen Abfragen Ressourceneintragsinformationen anfordern, die den zwischengespeicherten Ressourceneinträgen entsprechen, können diese vom DNS-Server für eine Antwort verwendet werden.

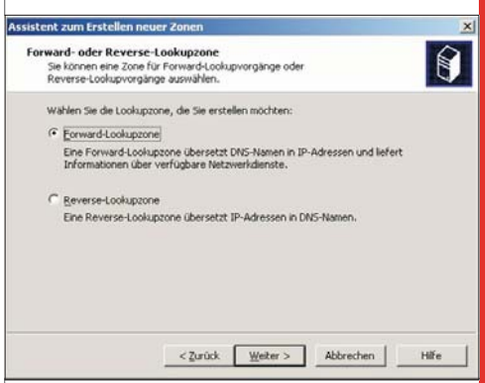
Beim Zwischenspeichern von Informationen wird allen zwischengespeicherten Ressourceneinträgen ein Wert für die Gültigkeitsdauer *(TTL = Time-To-Live)* zugeordnet. Während des Gültigkeitszeitraumes eines zwischengespeicherten Ressourceneintrags bleibt dieser im Zwischenspeicher des DNS-Servers enthalten und kann weiterhin zum Beantworten von Clientabfragen verwendet werden, für die dieser Ressourceneintrag zutreffend ist. In den meisten Zonenkonfigurationen ist den von den Ressourceneinträgen verwendeten TTL-Werten der Wert **Minimum TTL (Standard)** zugewiesen, der im Ressourceneintrag für den Autoritätsursprung *(SOA = Start Of Authority)* der Zone eingestellt ist. In der Standardeinstellung beträgt der Wert für **Minimum TTL (Standard)** 3.600 Sekunden (1 Stunde). Sie können diesen Wert jedoch ändern oder bei Bedarf für jeden Ressourceneintrag einen individuellen TTL-Wert für das Zwischenspeichern einstellen.

11.4 Konfiguration eines DNS-Servers in Windows 2000/2003

MMC-Snap-In "DNS"

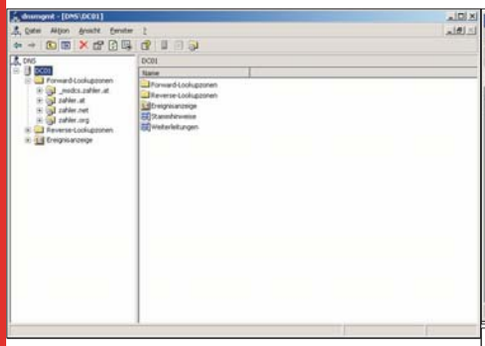
- neue Forward-Lookup-Zone



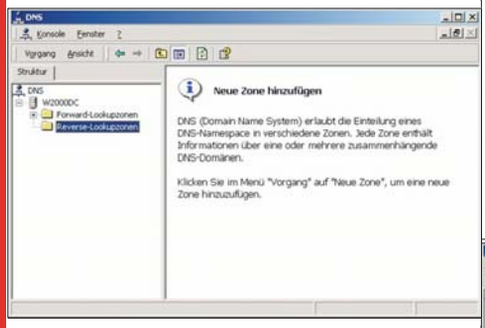


- neue Reverse-Lookup-Zone

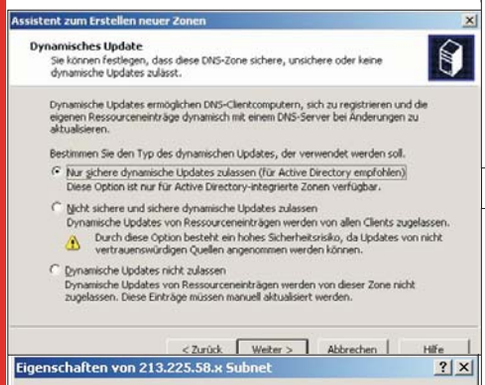
Standardmäßig ist keine Reverse-Loo-

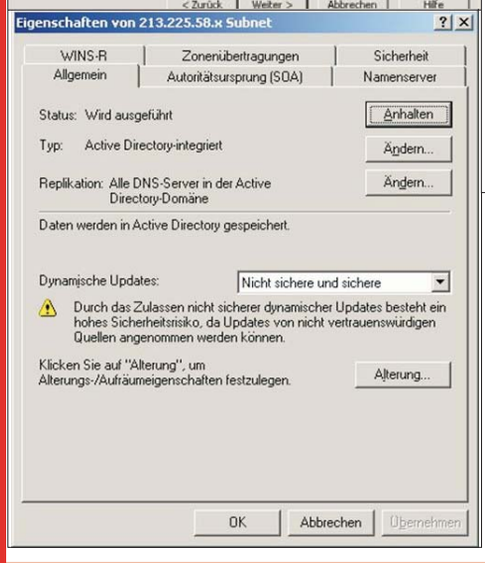


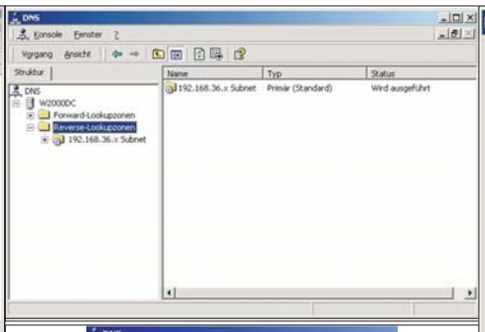
kup-Zone eingerichtet. Es wird dringend empfohlen, diese Zone manuell einzurichten!

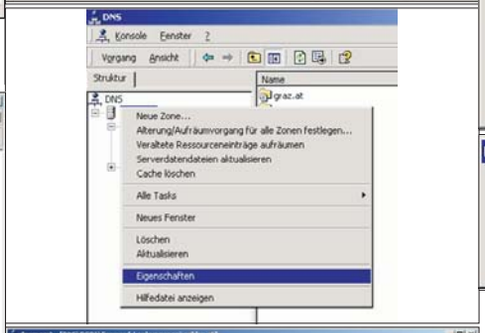


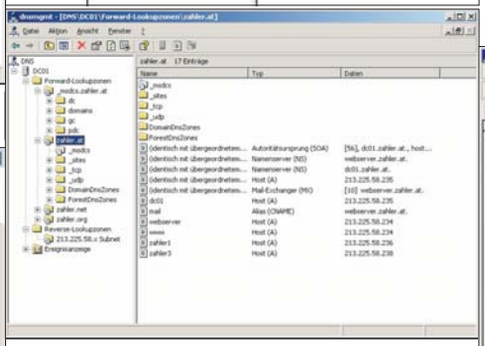
Alles auf "dynamisch" umstellen!



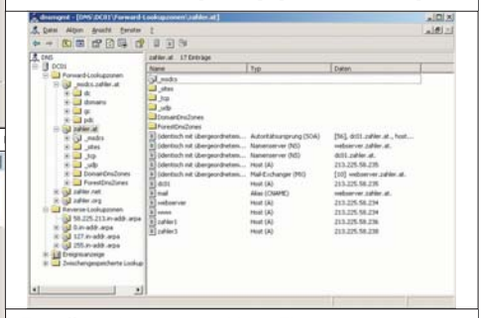




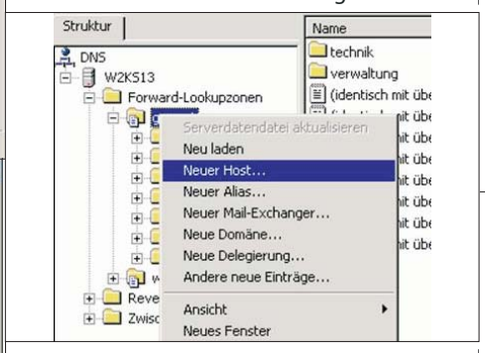




Erweiterte Ansicht *[Ansicht] - [Erweiterte Ansicht]*:



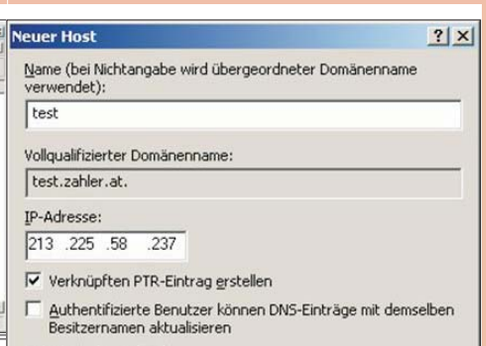
Erstellen eines neuen Host-Eintrags:



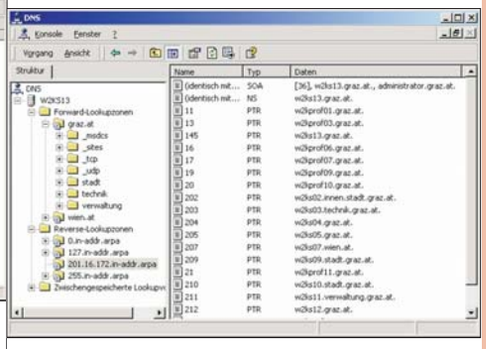
Gibt man ein, dass automatisch ein verknüpfter PTR-Eintrag erstellt werden soll, so wird ein solcher Eintrag bei der Reverse-Lookup-Zone erstellt:

Nach dem Erstellen einer Zone müssen weitere **Ressourceneinträge** hinzugefügt werden. Die folgenden Ressourceneinträge (RRs = Resource Records) werden am häufigsten eingefügt:

- **Host (A)** Zum Zuordnen eines DNS-Domänennamens zu einer von einem Computer verwendeten IP-Adresse.



- **Alias (CNAME)** Zum Zuordnen eines Alias-Domänennamens zu einem anderen prim**ären oder kanonischen Namen.**



- **Mail Exchanger (MX)** Zum Zuordnen eines DNS-Domänennamens zum Namen eines Computers, über den Mail ausgetauscht oder weitergeleitet werden.
- **Pointer (PTR)** Zum Zuordnen eines umgekehrten DNS-Domänennamens auf der Grundlage der IP-Adresse eines Computers, die auf den weitergeleiteten DNS-Domänennamen dieses Computers verweist.
- **Service location (SRV)** Zum Zuordnen eines DNS-Domänennamens zu einer angegebenen Liste mit DNS-Hostcomputern, die eine bestimmte Dienstart (z. B. Active Directory-Domänencontroller) anbieten.
- Weitere Ressourceneinträge entsprechend den aktuellen Anforderungen.

Ressourceneinträge für Host (A)

Ressourceneinträge für Host (A) werden in einer Zone verwendet, um DNS-Domänennamen von Computern (oder Hosts) ihren IP-Adressen zuzuordnen. Sie können einer Zone auf unterschiedliche Weise hinzugefügt werden:

- Sie können mit Hilfe der DNS-Konsole manuell einen A-Ressourceneintrag für einen TCP/IP-Clientcomputer erstellen.
- Windows 2000-Computer verwenden den DHCP-Clientdienst, um bei einer Änderung der IP-Konfiguration die eigenen A-Ressourceneinträge in DNS dynamisch zu registrieren und zu aktualisieren.
- Bei DHCP-Clientcomputern mit früheren Versionen von Microsoft-Betriebssystemen können die A-Ressourceneinträge nach Proxy

registriert und aktualisiert werden, wenn die IP-Lease von einem qualifizierten DHCP-Server stammt (dieses Feature wird gegenwärtig nur durch den im Lieferumfang von Windows 2000 Server enthaltenen DHCP-Dienst unterstützt).

Der Ressourceneintrag für Host (A) ist zwar nicht für alle Computer erforderlich, wird jedoch von Computern benötigt, die gemeinsam auf Ressourcen in einem Netzwerk zugreifen. Alle Computer, die Ressourcen gemeinsam nutzen und über ihre DNS-Domänennamen erkannt werden, müssen A-Ressourceneinträge verwenden, um der IP-Adresse des Computers die DNS-Namensauflösung zu ermöglichen.

Die meisten in einer Zone erforderlichen A-Ressourceneinträge können andere Arbeitsstationen oder Server, die gemeinsam auf Ressourcen zugreifen, andere DNS-Server, Mailserver sowie Webserver umfassen. Diese Ressourceneinträge stellen die Mehrheit der Ressourceneinträge in der Datenbank einer Zone dar.

Alias-Ressourceneinträge (CNAME)

Alias-Ressourceneinträge (CNAME) werden auch als so genannte kanonische Namen bezeichnet. Mit Hilfe dieser Einträge können Sie mit mehreren Namen auf einen einzigen Host verweisen, wodurch es leichter wird, auf einem Computer einen FTP-Server und einen Webserver zu verwenden. Allgemein bekannte Servernamen (ftp, www) werden z. B. mit Hilfe von CNAME-Ressourceneinträgen registriert, die dem DNS-Hostnamen, z. B. "server-1", für den Servercomputer zugeordnet sind, auf dem diese Dienste zur Verfügung stehen.

Es wird empfohlen, CNAME-Ressourceneinträge in folgenden Szenarios zu verwenden:

- Wenn ein in einem A-Ressourceneintrag angegebener Host in derselben Zone umbenannt werden muss.
- Wenn über einen generischen Namen für einen bekannten Server, z. B. www, eine Auflösung für eine Gruppe von Computern (jeder mit eigenen A-Ressourceneinträgen) stattfinden soll, die denselben Dienst bieten (dabei kann es sich um eine Gruppe redundanter Webserver handeln).

Beim Umbenennen eines Computers mit einem bestehenden A-Ressourceneintrag in der Zone können Sie vorübergehend einen CNAME-Ressourceneintrag verwenden, um Benutzern und Programmen eine Umstellungsfrist für die Verwendung des neuen Namens zu gewähren. Hierzu müssen folgende Aufgaben ausgeführt werden:

- Für den neuen DNS-Domänennamen des Computers wird der Zone ein neuer A-Ressourceneintrag hinzugefügt.
- Für den alten DNS-Domänennamen wird ein CNAME-Ressourceneintrag hinzugefügt, der auf den neuen A-Ressourceneintrag zeigt.
- Der ursprüngliche A-Ressourceneintrag für den alten DNS-Domänennamen (und ggf. der zugeordnete PTR-Ressourceneintrag) wird aus der Zone entfernt.

Geben Sie beim Verwenden eines CNAME-Ressourceneintrags zum Vergeben eines Alias oder eines neuen Namens für einen Computer eine Frist für die Verwendung des Eintrags in der Zone bis zu seiner Entfernung aus dem DNS an. Wurde der CNAME-Ressourceneintrag versehentlich nicht gelöscht und wird zu einem späteren Zeitpunkt der damit verbundene A-Ressourceneintrag gelöscht, belegt der CNAME-Ressourceneintrag ggf. unnötig Serverressourcen, wenn er versucht, Abfragen nach nicht mehr im Netzwerk verwendeten Namen aufzulösen.

Die häufigste und bevorzugte Verwendung eines CNAME-Eintrags besteht darin, mehreren Computern oder einer IP-Adresse, die auf einem Webserver verwendet werden, einen ständigen, über DNS vergebenen Alias für den Domänennamen zur Verfügung zu stellen, um die generische Namensauflösung eines Dienstnamens, z. B. www.example.microsoft.com zu ermöglichen. Im Folgenden wird die grundlegende Syntax für die Verwendung eines CNAME-Ressourceneintrags erläutert.

Aliasname IN CNAME primärer_kanonischer_Name

In diesem Beispiel soll ein Computer mit dem Namen host-a.example.microsoft.com als Webserver mit dem Namen `www.example.microsoft.com`. und gleichzeitig als FTP-Server mit dem Namen `ftp.example.microsoft.com` fungieren. Um den Computer für diesen Zweck zu benennen, können Sie folgende CNAME-Einträge in der Zone `example.microsoft.com` hinzufügen und verwenden:

```
host-a    IN  A      10.0.0.20
ftp       IN  CNAME  host-a
www       IN  CNAME  host-a
```

Wenn Sie später den FTP-Server auf einen anderen Computer verschieben möchten, der unabhängig vom Webserver auf "host-a" zur Verfügung steht, ändern Sie den CNAME-Ressourceneintrag in der Zone für `ftp.example.microsoft.com`, und fügen Sie der Zone für den neuen Hostcomputer mit dem FTP-Server einen zusätzlichen A-Ressourceneintrag hinzu.

Entsprechend dem vorhergehenden Beispiel lauten die neuen und überarbeiteten A- und CNAME-Ressourceneinträge folgendermaßen, wenn der neue Computer mit `host-b.example.microsoft.com` benannt wird:

```
host-a    IN  A      10.0.0.20
host-b    IN  A      10.0.0.21
ftp       IN  CNAME  host-b
www       IN  CNAME  host-a
```

Ressourceneinträge für Mail Exchanger (MX)

Ein MX-Ressourceneintrag wird von E-Mail-Anwendungen verwendet, um einen Mailserver auf der Grundlage eines DNS-Domänennamens zu suchen, der in der Zieladresse für den Empfänger einer E-Mail-Nachricht verwendet wird. Mit einer DNS-Abfrage nach dem Namen `example.microsoft.com` können Sie z. B. einen MX-Ressourceneintrag suchen, so dass über eine E-Mail-Anwendung für einen Benutzer mit der E-Mail-Adresse `user@example.microsoft.com` eine Mail weitergeleitet oder ausgetauscht werden kann.

Über den MX-Ressourceneintrag wird der DNS-Domänenname für den bzw. die Computer angezeigt, auf dem bzw. auf denen Mail-Nachrichten für eine Domäne verarbeitet werden. Wenn mehrere MX-Ressourceneinträge vorhanden sind, wird über den DNS-Clientdienst entsprechend der Priorität eine Verbindung zu den Mailservern hergestellt, vom niedrigsten Wert (höchste Priorität) zum höchsten Wert (niedrigste Priorität). Im Folgenden wird die grundlegende Syntax für die Verwendung eines MX-Ressourceneintrags aufgezeigt.

Mail_Domänenname IN MX Priorität Mailserver_Host

Mit Hilfe der unten aufgeführten MX-Ressourceneinträge in der Zone example.microsoft.com werden an user@example.microsoft.com adressierte Mails zunächst an user@mailserver0.example.microsoft.com gesendet (wenn möglich). Wenn dieser Server nicht zur Verfügung steht, kann der Client für Auflösungsdienste stattdessen den Eintrag user@mailserver1.example.microsoft.com verwenden.

```
@         IN  MX   1    mailserver0
@         IN  MX   2    mailserver1
```

Beachten Sie, dass mit dem Zeichen (@) in den Einträgen darauf hingewiesen wird, dass es sich beim DNS-Domänennamen um denselben Namen (`example.microsoft.com`) handelt, wie bei dem ursprünglichen Namen für die Zone.

PTR-Ressourceneinträge (Zeiger)

PTR-Ressourceneinträge unterstützen auf der Grundlage von in der in-addr.arpa-Domäne erstellten und residierenden Zonen den Reverse-Lookup-Prozess. Diese Einträge werden verwendet, um über die IP-Adresse nach einem Computer zu suchen und diese Daten in den DNS-Domänennamen für diesen Computer aufzulösen.

PTR-Ressourceneinträge können einer Zone auf verschiedene Weise hinzugefügt werden:

- Sie können mit Hilfe des DNS-Snap-In manuell einen PTR-Ressourceneintrag für einen TCP/IP-Clientcomputer erstellen, entweder als eigenständige Prozedur oder als Teil der Prozedur zum Erstellen eines A-Ressourceneintrags.
- Windows 2000-Computer können mit dem DHCP-Clientdienst bei Änderungen der IP-Konfiguration die PTR-Ressourceneinträge dynamisch registrieren und aktualisieren.
- Bei allen anderen DHCP-Clientcomputern können die PTR-Ressourceneinträge durch den DHCP-Server registriert und aktualisiert werden, wenn die IP-Lease über einen qualifizierten Server vergeben wurde. Der im Lieferumfang von Windows 2000 Server enthaltene DHCP-Dienst bietet diese Möglichkeit.

Der PTR-Ressourceneintrag wird nur in Reverse Lookup-Zonen verwendet, um Reverse Lookup-Vorgänge zu unterstützen.

SRV-Ressourceneinträge (Dienstidentifizierung)

Zum Suchen von Active Directory-Domänencontrollern in Windows 2000 sind SRV-Ressourceneinträge erforderlich. Die manuelle Verwaltung von SRV-Ressourceneinträgen ist in der Regel nicht mehr erforderlich, wenn Sie Active Directory installieren.

In der Standardeinstellung wird über den Assistenten zum Installieren von Active Directory die Liste der bevorzugten oder alternativen DNS-Server nach einem DNS-Server durchsucht, der in den TCP/IP-Clienteigenschaften für eine der aktiven Netzwerkverbindungen konfiguriert wurde. Wenn eine Verbindung mit einem DNS-Server hergestellt wird, der die dynamische Aktualisierung des SRV-Ressourceneintrags (und anderer Ressourceneinträge, die mit dem Registrieren von Active Directory als Dienst in DNS zusammenhängen) akzeptiert, ist der Konfigurationsprozess abgeschlossen.

Wenn während der Installation kein DNS-Server gefunden wird, der Aktualisierungen des zum Benennen des Active Directory erforderlichen DNS-Domänennamen akzeptiert, kann lokal ein Windows 2000-DNS-Server installiert und automatisch mit einer Zone auf der Grundlage der Active Directory-Domäne konfiguriert werden.

Handelt es sich bei der als erste in der Gesamtstruktur ausgewählten Active Directory-Domäne um example.microsoft.com, wird eine Zone im DNS-Domänennamen namens `example.microsoft.com` hinzugefügt und so konfiguriert, dass sie mit dem DNS-Server auf dem neuen Domänencontroller ausgeführt werden kann.

Wenn der im Lieferumfang von Windows 2000 enthaltene DNS-Server nicht installiert wird, wird während des Installationsprozesses von Active Directory eine Datei (Netlogon.dns) geschrieben und erstellt, in der die SRV-Ressourceneinträge sowie weitere für die Unterstützung von Active Directory notwendigen Ressourceneinträge enthalten sind. Diese Datei wird im Ordner `%SystemRoot%\System32\Config` erstellt.

Wenn Sie mit einem DNS-Server arbeiten, auf den eine der folgenden Beschreibungen zutrifft, verwenden Sie die Einträge in `Netlogon.dns`, um die primäre Zone auf diesem Server manuell für die Unterstützung von Active Directory zu konfigurieren.

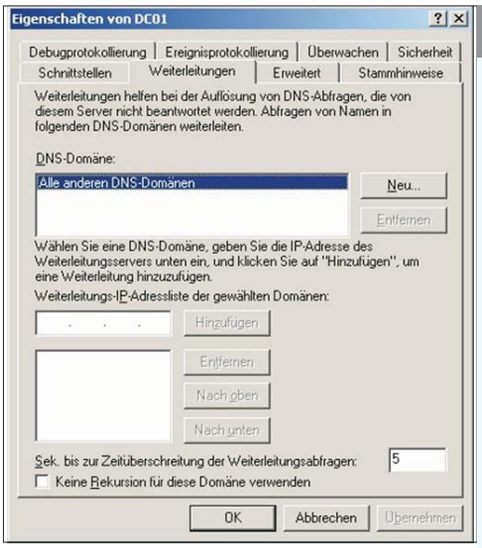
- Der Computer, auf dem der DNS-Server zur Verfügung steht, wird auf einer anderen Plattform ausgeführt, z. B. UNIX, und kann dynamische Aktualisierungen nicht akzeptieren oder erkennen.
- Der DNS-Server auf diesem Computer ist autorisierend für die primäre Zone, die dem DNS-Domänennamen für die Active Directory-Domäne entspricht.
- Wie im Internetentwurf "A DNS RR specifying the location# of services (DNS SRV)" definiert, wird der SRV-Ressourceneintrag zwar über den DNS-Server unterstützt, aber es werden keine dynamischen Aktualisierungen unterstützt.
- Der im Lieferumfang von Windows NT Server 4.0 enthaltene DNS-Dienst entspricht dieser Beschreibung, wenn eine Aktualisierung auf Service Pack 4 oder höher stattfindet.

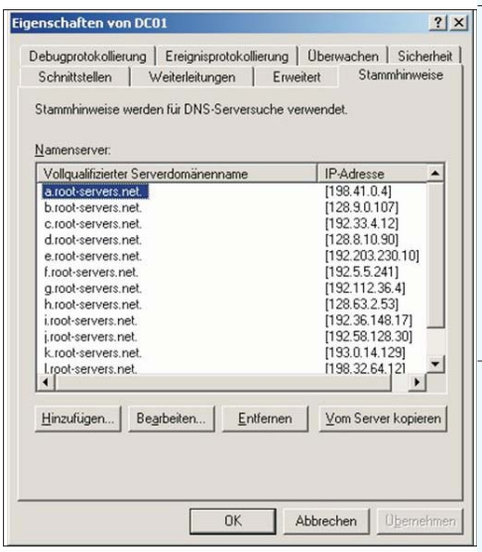
In zukünftigen Versionen kann der SRV-Eintrag auch verwendet werden, um andere bekannte TCP/IP-Dienste im Netzwerk zu registrieren und zu suchen, wenn mit den entsprechenden Anwendungen DNS-Namensabfragen implementiert und unterstützt werden, die diesen Eintragstyp angeben.

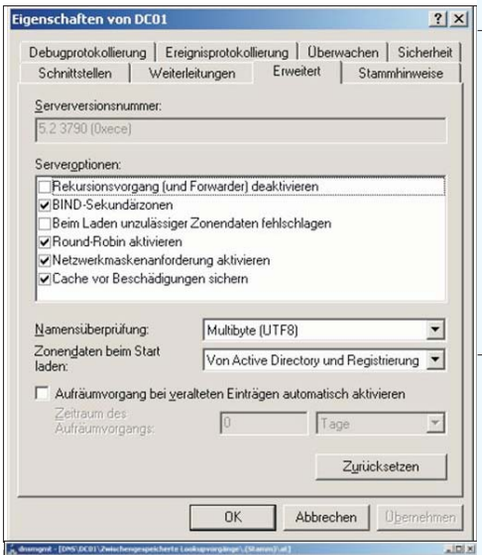
Um auch DNS-Einträge auflösen zu können, die außerhalb des privaten Netzwerks liegen, muss die Weiterleitung aktiviert werden (hier ist die IP-Adresse eines externen DNS-Servers angegeben):

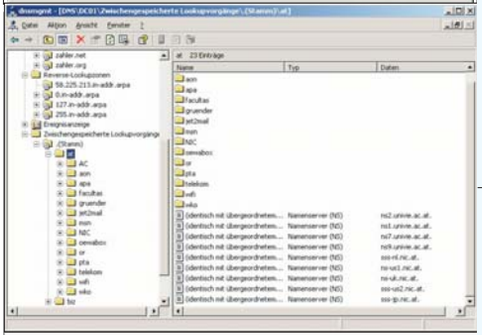
Die Hinweise auf das Stammverzeichnis sind nur dann sichtbar, wenn der DNS-Server keine Zone mit dem Namen "." (Punkt) aufweist. Diese Hinweise sind auch in der Datei CACHE.DNS ("Hints") enthalten, die im Verzeichnis `c:\winnt\system32\dns` enthalten ist.

Wichtig: Ein DNS-Server mit der "."-Zone ist selbst Root-Server; Internet-Namensauflösungen sind daher über einen solchen DNS-Server nicht möglich!









In der erweiterten Ansicht sind die bereits durchgeführten Lookup-Vorgänge im Internet sichtbar:

11.5 Abfragen eines DNS-Servers mit dem Kommandozeilenprog kup

```
Befehle:  (Kennungen werden in Großbuchstaben angezeigt, [] steht für optional)
NAME                - Info über Host/Domäne NAME (verwendet Standardserver)
NAME1 NAME2         - Wie oben; verwendet NAME2 als Server
help oder ?         - Info über allgemeine Befehle; siehe auch  nslookup(1)
set OPTION          - Legt eine Option fest
all                 - Zeigt alle Optionen, aktuelle Server und Hosts an
[no]debug           - Zeigt Debuginformationen an
[no]d2              - Zeigt ausführliche Debuginformationen an
[no]defname         - Fügt jeder Abfrage den Domänenname an
[no]recurse         - Rekursive Antwort auf Anfrage
[no]search          - Verwendet die Domänensuchliste
[no]vc              - Verwendet immer einen "virtual circuit"
domain=NAME         - Legt den Standarddomänennamen mit NAME fest
srchlist=N1[/N2/./N6] - Legt Domäne mit N1 und Suchliste mit N1,N2.. fest
root=NAME           - Legt den Stammserver mit NAME fest
retry=X             - Legt die Anzahl der  Neuversuche mit X fest
timeout=X           - Zeitüberschreitungsintervall mit X Sekunden
querytype=X         - Abfragetyp, z.B. A,ANY,CNAME,HINFO,NS,SOA,WKS
type=X              - Synonym mit "querytype"
class=X             - Abfrageklasse mit IN, CHAOS,  HESIOD oder ANY
server NAME         - Standardserver NAME
lserver NAME        - Standardserver NAME
finger [USER]       - Führt den Befehl "finger" für NAME aus
root                - Legt den aktuellen Standardserver mit "root" fest
ls [opt]DOMÄNE[>DATEI]- Zeigt Adressen in DOMÄNE an (Ausgabe in DATEI)
-a                  - Führt kanonische Namen und  Aliase auf
-d                  - Führt alle Einträge auf
-t TYP              - Zeigt Einträge des Typs (z.B. A,  CNAME, MX, usw.)
view DATEI          - Sortiert eine "ls"-Outputdatei und zeigt
sie mit "pg" an
exit                - Beendet das Programm, auch  EOF (z.B. ^D) möglich
```

Beispiel 1:

```
C:\>nslookup
*** Der Servername für die Adresse 194.96.13.3 konnte nicht gefunden werden:
Server failed
*** Die Standardserver sind nicht verfügbar.
Standardserver:  UnKnown
Address:  194.96.13.3
> www.noe.wifi.at.
Server:  UnKnown
Address:  194.96.13.3
Name:    www.noe.wifi.at
Address:  194.96.13.5
> set type=any       Damit können erweiterte Informationen abgerufen werden!
> www.noe.wifi.at
Server:  UnKnown
Address:  194.96.13.3
www.noe.wifi.at internet address = 194.96.13.5
noe.wifi.at     nameserver = ns.noe.wifi.at
noe.wifi.at     nameserver = ns1.via.at
ns.noe.wifi.at  internet address = 194.96.13.3
ns1.via.at      internet address = 194.
```

Beispiel 2: Beachten Sie den Punkt am Ende der Adresse (Root Domain!)

```
C:\>nslookup www.microsoft.com.
*** Der Servername für die Adresse 194.96.13.3 konnte nicht gefunden werden:
Server failed
*** Die Standardserver sind nicht verfügbar.
Server:  UnKnown
Address:  194.96.13.3
Nicht autorisierte Antwort:
Name:    microsoft.com
Addresses:  207.46.130.149, 207.46.130.45, 207.46.131.137, 207.46.131.30
207.46.130.14
Aliases:  www.microsoft.com
```

Beispiel 3:

```
> www.sbg.wifi.at
Server:  UnKnown
Address:  194.96.13.3
Nicht autorisierte Antwort:
www.sbg.wifi.at canonical name = WEBWIFI.sbg.wifi.at
sbg.wifi.at     nameserver = ns2.sbg.wifi.at
sbg.wifi.at     nameserver = ns.sbg.wifi.at
ns2.sbg.wifi.at internet address = 193.83.60.252
ns.sbg.wifi.at  internet address = 193.83.60.251
> WEBWIFI.sbg.wifi.at
Server:  UnKnown
Address:  194.96.13.3
Nicht autorisierte Antwort:
WEBWIFI.sbg.wifi.at     internet address = 193.83.60.233
sbg.wifi.at     nameserver = ns2.sbg.wifi.at
sbg.wifi.at     nameserver = ns.sbg.wifi.at
ns2.sbg.wifi.at internet address = 193.83.60.252
ns.sbg.wifi.at  internet address = 193.83.60.251
```

Beispiel 4: www.via.at

```
C:\>nslookup
> set type=any
> www.via.at
Server:  UnKnown
Address:  194.96.13.3
Nicht autorisierte Antwort:
www.via.at      internet address = 194.96.203.221
via.at  nameserver = ns1.via.at
via.at  nameserver = ns2.via.at
ns1.via.at      internet address = 194.41.60.10
ns2.via.at      internet address = 194.41.60.16
> 221.203.96.194.in-addr.arpa.
   ;Achtung: Man muss die gefundene Adresse von hinten eingeben!
Server:  UnKnown
Address:  194.96.13.3
Nicht autorisierte Antwort:
221.203.96.194.in-addr.arpa     name = www.via.at
203.96.194.in-addr.arpa nameserver = ns1.via.at
203.96.194.in-addr.arpa nameserver = ns2.via.at
ns1.via.at      internet address = 194.41.60.10
ns2.via.at      internet address = 194.41.60.16
```

Beispiel 5: Auflistung aller Rechner in einer Zone

```
C:\>nslookup
> ls noe.wifi.at
noe.wifi.at.                    NS      server = ns.noe.wifi.at
noe.wifi.at.                    NS      server = ns1.via.at
www                             A       194.96.13.5
www2                            A       194.96.13.3
ns                              A       194.96.13.3
kurs                            A       194.96.13.8
ns2                             A       194.96.13.5
```