16 Domain Name System (DNS)

Christian Zahler

16.1 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 leicht merkbaren DNS-Namen zu IP-Adressen. Alle modernen DNS-Implementierungen unterstützen sowohl IPv4 als auch IPv6.

Das DNS wurde 1983 von Jon Postel (1943 – 1998) und **Paul Mockapetris** für das Internet entworfen und in RFC 882 und 883 beschrieben. Beide wurden inzwischen von RFC 1034 und RFC 1035 abgelöst und durch zahlreiche weitere Standards ergänzt. Ursprüngliche Aufgabe war es, die lokalen hosts-Dateien abzulösen, die bis dahin für die Namensauflösung zuständig waren und die der enorm zunehmenden Zahl von Neueinträgen nicht mehr gewachsen waren. Aufgrund der erwiesenermaßen hohen Zuverlässigkeit und Flexibilität wurden nach und nach weitere Datenbestände in das DNS integriert und so den Internetnutzern zur Verfügung gestellt.

Die Auflösung von DNS-Namen in IP-Adressen wird als Forward Lookup bezeichnet, die Auflösung von IP-Adressen in FQDNs nennt man Reverse Lookup.

DNS-Namensauflösung wird heute nicht nur im Internet, sondern auch in Firmennetzwerken verwendet.

DNS-Namen können verwendet werden für:

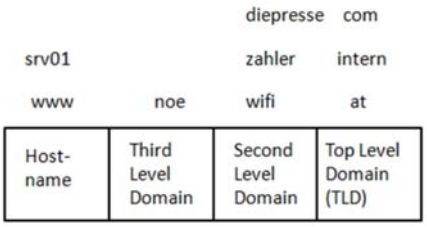
- Geräte in einem Netzwerk, etwa PCs, Router oder Drucker
- Ressourcen in einem Netzwerk, etwa Websites

Der Domain-Namensraum hat eine baumförmige Struktur. Die Blätter und Knoten des Baumes werden als Labels bezeichnet. Ein kompletter Domainname eines Objektes besteht aus der Verkettung aller Labels. Label sind Zeichenketten (alphanumerisch, als einziges Sonderzeichen ist der Bindestrich '-' erlaubt), die mindestens ein Zeichen und maximal 63 Zeichen lang sind, mit einem Buchstaben beginnen müssen und nicht mit '-' enden dürfen (RFC 1035, Abschnitt *„2.3.1. Preferred name syntax“*). Die einzelnen Labels werden durch Punkte (engl. *dots*) voneinander getrennt. Ein Domainname darf inklusive aller Punkte maximal 255 Zeichen lang sein.

Beispiele für DNS-Namen:

```
www.bmf.gv.at
srv01.zahler.intern
```

Ein vollständig angeführter DNS-Name wird auch als FQDN *(Fully Qualified Domain Name)* bezeichnet. Wie in der Grafik ersichtlich, besteht ein FQDN aus einem Hostnamen und einem mehrteiligen Domänennamen.



Das DNS-System ist hierarchisch aufgebaut. Die oberste Ebene *(Root-Domain)* wird durch einen Punkt repräsentiert, der in der praktischen Anwendung immer weggelassen wird.

Genau genommen, würden DNS-Namen also folgendermaßen aussehen:

```
www.bmf.gv.at.
srv01.zahler.intern.
```

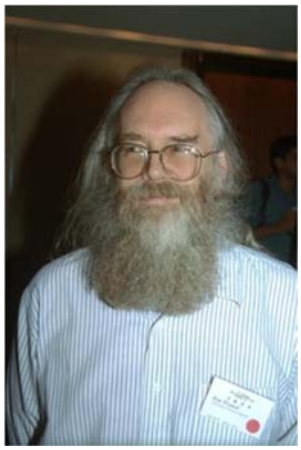
Die oberste Ebene von Bedeutung ist die Top Level Domain. Man unterscheidet TLDs, die für Internet-Ressourcen verwendet werden, und private TLDs.

16.2 DNS-Domain-Namen im Internet

Neue Top Level Domains werden von der ICANN (www.icann.org) festgelegt. Die ICANN *(Internet Corporation for Assigned Names and Numbers)* ist eine private Internet-Organisation mit Sitz in Marina del Rey, Kalifornien, die bestimmte zentrale Koordinierungsaufgaben im Internet übernimmt:

- **IP-Adressen**: ICANN koordiniert das IP-Adressensystem, und ist die oberste Instanz, die IP-Adressenblöcke vergibt. Die Blöcke werden an die regionalen IP-Registries vergeben, die sie dann weiter verteilen.
- **Domainnamen-System**: ICANN koordiniert das Domainnamen-System (DNS) und ist insbesondere die Instanz, die über die Einrichtung von Top-Level-Domains entscheidet.
- **Internet-Protokolle**: ICANN koordiniert die Zuweisung von Parametern mit Internet-Bezug und ist z.B. für die Vergabe von TCP/UDP-Port-Nummern zuständig.
- **DNS Root Server-System**: In diesem Punkt hat ICANN eine deutlich geringere Rolle als in den anderen Bereichen. ICANN überwacht zwar den Betrieb des Rootserver-Systems, bislang scheint die US-Regierung jedoch nicht bereit zu sein, die letzte Aufsicht darüber völlig abzugeben.

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



Dr. Jonathan „Jon“ Postel, Internet-Pionier, Gründer und erster Direktor der IANA

Länder-Domains (ccTLD, Country Code-Top Level Domains)

Derzeit sind mehr als 200 Länder-Top Level Domains (ISO-Norm 3166) zugelassen, zum Beispiel:

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

Derzeit (Stand: Juli 2008) sind mehr als 760.000 at-Domänen registriert.

Die Europäische Kommission strebt im Rahmen der eEurope-Initiative die Einrichtung einer .eu-Top-Level-Domain für die Länder der Europäischen Union an: Im Februar 2000 hat sie in einem Arbeitspapier dargelegt, dass sie .eu als Alternative zu .com für europäische Unternehmen ansieht.

Die .eu-Domain wurde als Ländercode-Domain eingerichtet, obgleich es sich bei der EU strenggenommen nicht um ein Land handelt. Die Registrierung von .eu-Domänen ist seit 2006 möglich.

Generische Top Level Domains der 1. Generation

Zusätzlich zu den landesspezifischen Erweiterungen gab es folgende generische Top Level Domains, 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 (gemeinnützig)
net      Provider
```

Generische Top Level Domains der 2. Generation

Ende des Jahres 2000 hat ICANN die Einrichtung neuer generischer Top-Level-

Domains beschlossen. Ausgewählt wurden sieben Domains:

biz	Firmen und Unternehmen
museum	Museen
info	Informationsservices
pro	Berufstätige, Freiberufler und Geschäftsleute
coop	Genossenschaften
aero	Luftfahrtindustrie
name	Privatpersonen

.aero

Domain nur für Unternehmen, die mit Flugverkehr zu tun haben, etwa Fluggesellschaften, Flughäfen und Reiseveranstalter.

.biz (für "business")

Nicht zugangsbeschränkte Top-Level-Domain zur geschäftlichen Nutzung, die in direkter Konkurrenz zu .com stehen soll.

.coop

Domain nur für Verbände, Vereinigungen und Genossenschaften, wobei der Schwerpunkt auf nichtkommerzieller Nutzung liegt.

.info

Nicht zugangsbeschränkte Top-Level-Domain für Informationsdienste, die mit .com konkurrieren soll.

.museum

Wie der Name bereits andeutet, ist .museum eine Domain ausschließlich für Museen und Ausstellungen.

.name

Top-Level-Domain für individuelle Nutzer, keine kommer¬zielle Nutzung erlaubt. Die Domains werden grund-sätzlich zweistufig angelegt (etwa vorname.nachname.name).

.pro

Zugangsbeschränkte Domain, die sich an Freiberufler („professionals“) wendet. Es gibt keine direkte Vergabe, sondern eine Rubrizierung verwenden. Derzeit gibt es folgende Rubriken:

law.pro	Rechtsanwälte
med.pro	Ärzte und medizinische Berufe
cpa.pro	Unternehmens- und Steuerberater (CPA = Certified Public Accountant)

Generische Top Level Domains der 3. Generation

2005 – 2008 wurden folgende Top Level Domains genehmigt:

asia	Asiatische Seiten
cat	catalan (katalanische Sprache und Kultur)
jobs	Plattformen für Arbeitsvermittlung
travel	Reiseveranstalter
post	ehemalige Post-Monopolisten
mobi	Mobilkommunikation
tel	Telekomunternehmen

Komplette Freigabe für Top Level Domains ab 2009

Nicht unerwartet hat ICANN angekündigt, dass ab 2009 praktisch jedes Wort in jeder Weltsprache als Top Level Domain verwendet werden kann.

Interessenten können einen entsprechenden Antrag stellen, der von der ICANN geprüft wird; für jede TLD ist ein Kostenbeitrag von bis zu € 100.000 vorgesehen. So hat die Stadt Paris bereits angekündigt, sich um die TLD .paris zu bewerben.

Wie bekommt man einen Internet-Domain-Namen?

Generell können Domainnamen bei verschiedenen Institutionen erworben werden; es gibt eine Liste registrierter Unternehmen, die Registrierungen durchführen dürfen. So findet man etwa eine Liste der für .com, .net und .org-Domänenregistrierungen zugelassenen „Registrare“ unter

www.internic.net

Für einen gültigen Antrag muss die IP-Adresse eines DNS-Servers angegeben werden. Üblicherweise ist dies der DNS-Server des Providers. Anmerkung: Natürlich muss der Provider erst um Erlaubnis gefragt werden, bevor die IP-Adresse an das Registrierunternehmen gemeldet wird. Unterlässt man dies, so führt das möglicherweise zu einer unerreichbaren Domain im Internet (und zu rechtlichen Schwierigkeiten!).

Hier kann man nachsehen, welche com, net, org und edu-Domains schon vergeben sind:

www.internic.net/cgi-bin/whois

Ripe (Réseaux IP Européens) verwaltet europäische Länder-Domains, unter anderem auch die für Österreich gültigen at-Domais.

www.ripe.net/db/whois.html

Weitere Registrare:

.at www.nic.at

.cc www.nic.cc

.de www.denic.de

.tv www.networksolutions.com

.nu www.activeisp.de

.to www.nic.to

.ac www.nic.ac

www.domaininfo.com

.com

.net

.org www.netsol.com

Für die Zuerkennung von Domänennamen bestehen verschiedene Voraussetzungen. Länderdomänen können beispielsweise einen Hauptwohnsitz im betreffenden Land voraussetzen. Interessant sind die genannten Domänen .cc, .to, .ac – diese Domänen waren ursprünglich für Kleinstaaten vorgesehen, werden aber nun (ähnlich wie .com-Domänennamen) international vergeben.

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-Domänen sind unter www.namen.at möglich.

Seit 2004 ist es nun auch möglich, Domänennamen zu registrieren, die länderspezifische Sonderzeichen (in Österreich sind dies zum Beispiel die Umlaute ä, ö und ü) enthalten, sogenannte IDNs (*International Domain Names*). Problematisch ist dabei, dass diese speziellen Zeichen auf nicht deutschsprachigen Tastaturen nicht auf einfachem Weg erreicht werden können – damit ist die internationale Erreichbarkeit solcher Web-Ressourcen nicht mehr gegeben. Die erste in Österreich vergebene „Umlaut-Domain“ war „börse.at“.

16.3 DNS-Dienste

DNS beruht auf einem Client-Server-Konzept.

In Microsoft-Betriebssystemen heißt der DNS-Clientdienst dnscache, der DNS-Serverdienst schlicht dns.

DNS-Serverdienste verwenden die Ports UDP 53 und TCP 53 auf der Transportschicht.

Mit allen Windows Server-Betriebssystemen werden DNS-Server-Komponenten mitgeliefert; als Open Source-Alternative steht BIND (Berkeley Internet Name Domain) zur Verfügung, eine Software, die in erster Linie auf UNIX- und Linux-Plattformen betrieben wird.

Alle Informationen, die zur Auflösung von Namen bzw. IP-Adressen notwendig sind, werden in sogenannten Zonen-Datenbanken auf verschiedenen DNS-Servern gespeichert.

Zonen können nach verschiedenen Gesichtspunkten untergliedert werden:

Nach der Art der Namensauflösung

- *Forward Lookup-Zone*: Diese Zonen enthalten Informationen zu Hostnamen und deren zugeordnete IP-Adresse. Typische Ressourceneinträge sind vom Typ A, AAAA und CNAME. Forward Lookup-Zonen heißen immer so wie der Namespace, für den sie autorisierend sind.
- *Reverse Lookup-Zone*: Solche Zonen enthalten Informationen zu IP-Adressen und deren zugeordneten Hostnamen. Typische Ressourceneinträge sind vom Typ PTR.

Nach der Beschreibbarkeit

- Primäre Zone: Primäre Zonen sind grundsätzlich editierbar. Seit Windows Server 2008 gibt es eine einzige Ausnahme: primäre DNS-Zonen auf RODCs sind schreibgeschützt.
- Sekundäre Zone: Sekundäre Zonen sind

schreibgeschützte Kopien primärer Zonen. Die Änderungen der Primärzonen werden durch den Mechanismus der Zonenübertragung zu den sekundären Zonen kopiert.

Nach der Art der Speicherung

- Standardzone: Standardzonen sind in Textdateien gespeichert. Sie sind betriebssystemunabhängig und entsprechen von der Struktur her den RFC-Vorgaben.
- Active Directory-integrierte Zone: AD-integrierte Zonen sind in einer AD-Partition gespeichert. AD-integrierte Zonen werden auf bestimmte Domänencontroller repliziert und sind grundsätzlich immer primäre Zonen.

16.4 HOSTS-Datei

Vor Einführung des DNS-Server-Systems waren mehrteilige Hostnamen bereits im Einsatz. Die Auflösung dieser Namen erfolgte allerdings statisch über eine lokal gespeicherte HOSTS-Datei.

Aus Kompatibilitätsgründen wird eine derartige Datei in jedem modernen TCP/IP-fähigen Betriebssystem mitgeliefert.

In Windows-Systemen befindet sich die Hosts-Datei im Verzeichnis

```
\%systemroot%\SYSTEM32\DRIVERS\ETC
```

Sie kann mit jedem Texteditor bearbeitet werden.

Beispiel für die mit Windows Server 2008 mitgelieferte Hosts-Datei:

```
# Copyright (c) 1993-2006 Microsoft Corp.

#

# This is a sample HOSTS file used by
Microsoft TCP/IP for Windows.

#

# 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 de-
noted 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

::1             localhost
```

Der Inhalt der lokalen Hosts-Datei wird beim Starten des DNS-Client-Dienstes in den lokalen DNS-Cache geladen und steht damit vor Beginn der ersten Namensauflösungsabfrage bereits zur Verfügung.

Hinweis: Sollten Sie noch mit HOSTS-Dateien arbeiten, dann beachten Sie bitte, dass diese Datei auf jeden PC kopiert werden muss, der die Informationen benötigt!

16.5 Ablauf einer DNS-Abfrage

Wenn ein DNS-Client 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 z. B. um den FQDN für einen Computer handeln, etwa "srv01.zahler.intern.", 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 'srv01.zahler.intern.'?" 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:

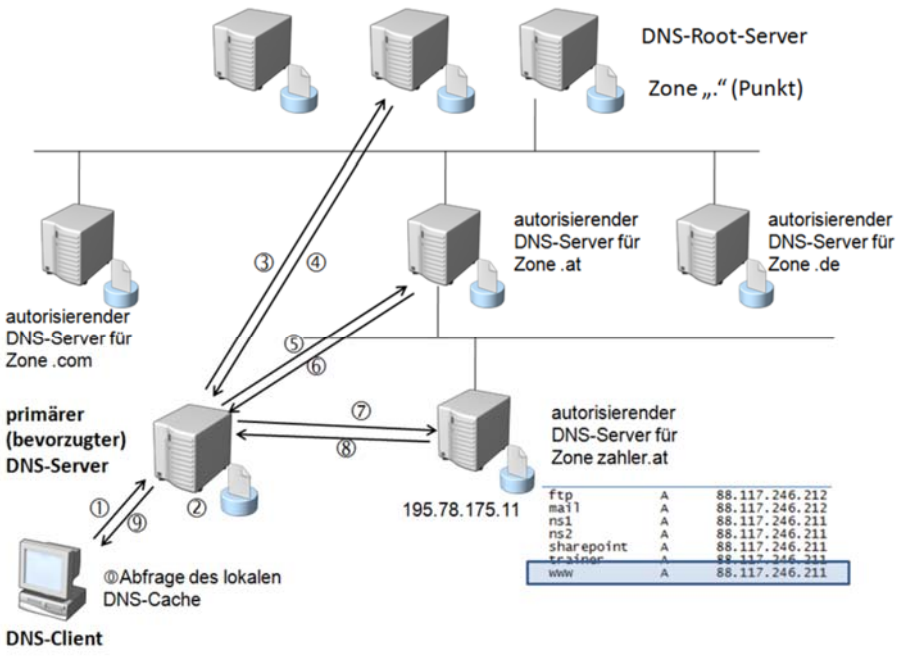
- Auf einem Clientcomputer wird eine Namensabfrage gestartet und zum Auflösen an einen Auflösungsdienst, den DNS-Clientdienst, weitergeleitet.
- Wenn die Abfrage nicht lokal aufgelöst werden kann, können nach Bedarf DNS-Server zum Auflösen des Namens abgefragt werden.

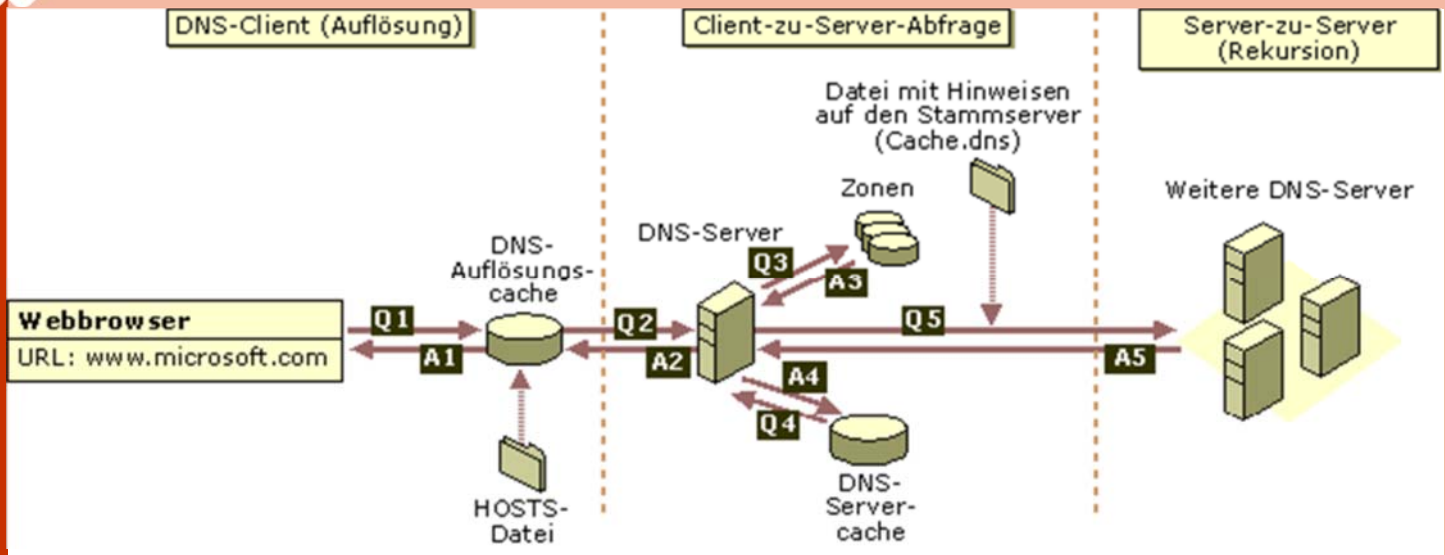
Diese beiden Vorgänge werden in den folgenden Abschnitten näher erläutert.

16.5.1 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.

16.5.2 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.

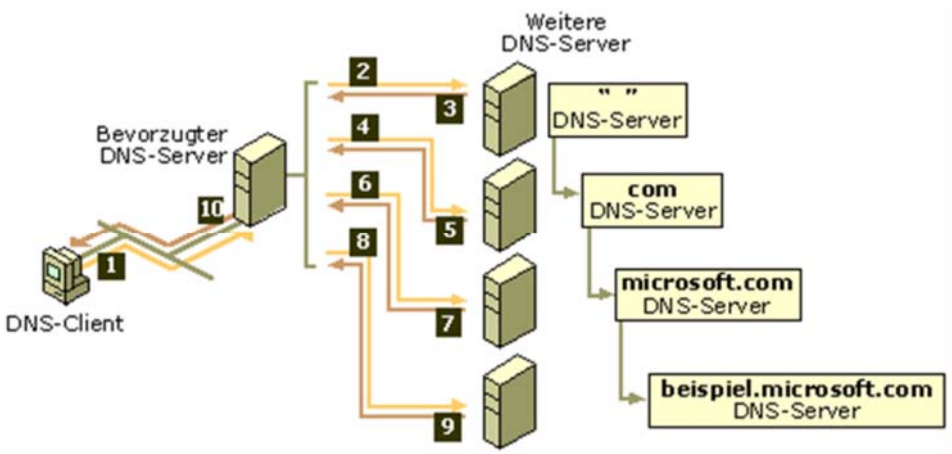
Wird auf dem bevorzugten Server weder in den Daten des Zwischenspeichers noch in den Zonendaten eine entsprechende Antwort für den abgefragten Namen gefunden, kann der Abfragevorgang fortgesetzt werden, indem der Name mit einem Rekursionsprozess vollständig aufgelöst wird. Für diese Art der Namensauflösung 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.

16.5.3 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 empfangen 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.

16.5.4 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.

16.5.5 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.

16.6 Konfiguration des DNS-Client-Dienstes

Eine Hauptaufgabe des DNS-Clientdienstes ist die Verwaltung des lokalen DNS-Caches. Dieser kann durch drei Schalter des Kommandozeilentools `ipconfig` beeinflusst werden:

```
ipconfig /displaydns
```

zeigt Einträge im DNS-Cache an

```
ipconfig /flushdns
```

löscht den lokalen DNS-Cache

```
ipconfig /registerdns
```

erneuert die Registrierung der eigenen IP-Adresse im lokalen DNS-Cache

Die Konfiguration des DNS-Clientdienstes selbst wird in erster Linie in den TCP/IP-Eigenschaften der Netzwerkschnittstelle durchgeführt.

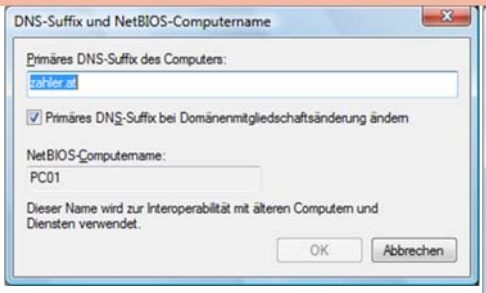
Hier sind folgende Einstellungen möglich:

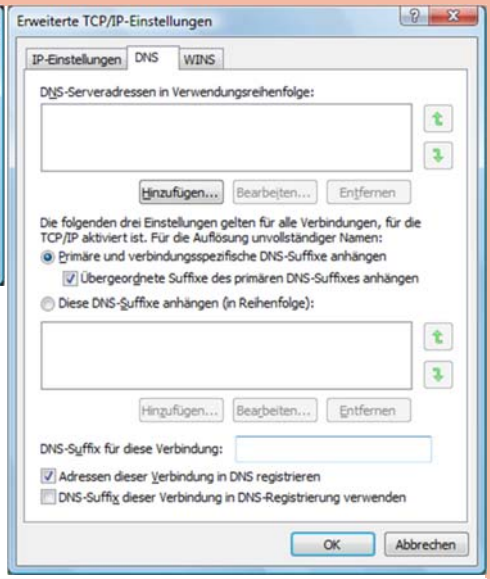
Bevorzugte DNS-Server

Es können beliebig viele IP-Adressen von DNS-Servern eingetragen werden; es wird aber nur dann ein weiterer DNS-Server gefragt, wenn der vorhergehende nicht antwortet.

DNS-Suffixe

Für Arbeitsgruppencomputer können verbindungsspezifische DNS-Suffixe definiert werden, die bei Verwendung unvollständiger DNS-Namen angehängt werden.



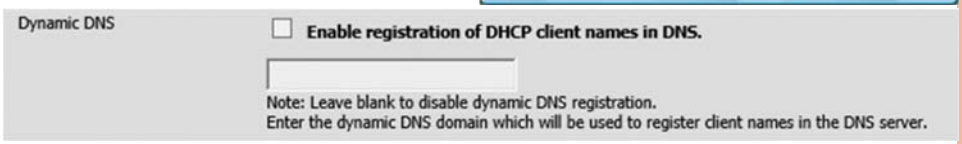


Dynamische DNS-Registrierung

Muss aktiviert sein, damit bei Änderung der IP-Adresse eine automatische Aktualisierung am DNS-Server erfolgt.

Konfiguration des primären DNS-Suffixes

Diese Einstellung kann nur in den Systemeigenschaften geändert werden. Üblicherweise ist der Beitritt zu einer AD-Domäne mit dem Setzen eines primären DNS-Suffixes verbunden.



Beachten Sie: Nur mit einem primären DNS-Suffix ist die dynamische DNS-Registrierung einer Netzwerkschnittstelle problemlos möglich!

16.7 Dynamic DNS (DDNS)

Wenn Sie keinen gerouteten Internetzugang haben, so müssen Sie DynDNS verwenden, wenn Sie von außen auf Ihr Heimnetzwerk zugreifen möchten.

Eine dauerhafte DNS-Namensauflösung ist nicht möglich, da das DSL-Modem/Router-Kombigerät auf der öffentlichen Netzwerkschnittstelle vom Internetanbieter ständig neue public IPs zugewiesen bekommt.

Es gibt mehrere DDNS-Anbieter, die derartige Namensauflösungsdienste anbieten. In Österreich bekannt sind

https://dyndns.org (40 USD/Jahr): wird von allen DSL-Modems unterstützt

https://my.noip.com/ (25 USD/Jahr oder kostenlos bei monatlicher Bestätigung per E-Mail)

Vorgangsweise

- Registrierung beim DDNS-Anbieter, Eintragen einer gewünschten DNS-Domäne (etwa `xy.dyndns.org` oder `xy.ddns.net`)
- Aktivieren von DDNS auf dem DSL-Modem
- Die Authentifizierung erfolgt über Benutzername und Kennwort

16.8 Abfragen von DNS-Informationen

Zum Abfragen von Zonendaten, die auf DNS-Servern gespeichert sind, verwendet man am besten das Kommandozeilentool `nslookup`.

Diese Informationen werden auch als „Ressourcen" bezeichnet. Folgende Informationen können in einer DNS-Zone enthalten sein:

- *IPv4-Host* (A) Zum Zuordnen eines DNS-Domänennamens zu einer von einem Computer verwendeten IPv4-Adresse.
- *IPv6-Host* (AAAA) Zum Zuordnen eines DNS-Domänennamens zu einer von einem Computer verwendeten IPv6-Adresse.
- *Alias* (CNAME) Zum Zuordnen eines Alias-Domänennamens zu einem anderen primären 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.

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:

```
C:\>nslookup
> 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
```