Domain Name System (DNS)

Autor: Moser Tobias

Datum: 25.03.2015

Typ: Information

Version: 1.0

Inhaltsverzeichnis

INHALT

1 Domain Name System

Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.

Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (den für Menschen merkbaren Namen eines Rechners im Internet) – zum Beispiel example.org. Diese sendet er als Anfrage in das Internet. Die URL wird dann dort vom DNS in die zugehörige IP-Adresse (die „Anschlussnummer“ im Internet) umgewandelt – zum Beispiel eine IPv4-Adresse der Form 192.0.2.42 oder eine IPv6-Adresse wie 2001:db8:85a3:8d3:1319:8a2e:370:7347, und führt so zum richtigen Rechner.

Domain Name System (DNS)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Namensauflösung
Ports:	53/UDP, 53/TCP

DNS im TCP/IP-Protokollstapel:

Anwendung	**DNS**				
Transport	UDP	TCP			
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	…

Standards:	RFC 1034 (1987)
	RFC 1035 (1987)

2 Überblick

Das DNS ist ein weltweit auf tausenden von Servern verteilter hierarchischer Verzeichnisdienst, der den Namensraum des Internets verwaltet. Dieser Namensraum ist in so genannte Zonen unterteilt, für die jeweils unabhängige Administratoren zuständig sind. Für lokale Anforderungen – etwa innerhalb eines Firmennetzes – ist es auch möglich, ein vom Internet unabhängiges DNS zu betreiben.

Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen („forward lookup“) benutzt. Dies ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst. Das DNS bietet somit eine Vereinfachung, weil Menschen sich Namen weitaus besser merken können als Zahlenkolonnen. So kann man sich einen Domainnamen wie example.org in der Regel leichter merken als die dazugehörende IP-Adresse 192.0.32.10. Dieser Punkt gewinnt im Zuge der Einführung von IPv6 noch an Bedeutung, denn dann werden einem Namen jeweils IPv4- und IPv6-Adressen zugeordnet. So löst sich beispielsweise der Name www.kame.net in die IPv4-Adresse 203.178.141.194 und die IPv6-Adresse 2001:200:0:8002:203:47ff:fea5:3085 auf.

Ein weiterer Vorteil ist, dass IP-Adressen – etwa von Web-Servern – relativ risikolos geändert werden können. Da Internetteilnehmer nur den (unveränderten) DNS-Namen ansprechen, bleiben ihnen Änderungen der untergeordneten IP-Ebene weitestgehend verborgen. Da einem Namen auch mehrere IP-Adressen zugeordnet werden können, kann sogar eine einfache Lastverteilung per DNS (Load Balancing) realisiert werden.

Mit dem DNS ist auch eine umgekehrte Auflösung von IP-Adressen in Namen (reverse lookup) möglich. In Analogie zum Telefonbuch entspricht dies einer Suche nach dem Namen eines Teilnehmers zu einer bekannten Rufnummer, was innerhalb der Telekommunikationsbranche unter dem Namen Inverssuche bekannt ist.

Das DNS wurde 1983 von Paul Mockapetris entworfen und in RFC 882 und RFC 883 (RFC = Request for Comments) 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 (siehe unten: Erweiterung des DNS).

DNS zeichnet sich aus durch:

dezentrale Verwaltung,
hierarchische Strukturierung des Namensraums in Baumform,
Eindeutigkeit der Namen,
Erweiterbarkeit.

3 Komponenten

3.1 Domain-Namensraum

Schematische Darstellung der DNS-Hierarchie
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 eines Pfades.

Labels sind Zeichenketten, die jeweils mindestens ein Oktett und maximal 63 Oktetts lang sind (RFC 2181) Einzelne Labels werden durch Punkte voneinander getrennt. Ein Domainname wird mit einem Punkt abgeschlossen (der letzte Punkt wird normalerweise weggelassen, gehört rein formal aber zu einem vollständigen Domainnamen dazu). Somit lautet ein korrekter, vollständiger Domainname (auch Fully Qualified Domain-Name (FQDN) genannt) zum Beispiel www.example.com. und darf inklusive aller Punkte maximal 255 Oktetts lang sein.

Ein Domainname wird immer von rechts nach links delegiert und aufgelöst, das heißt je weiter rechts ein Label steht, umso höher steht es im Baum. Der Punkt am rechten Ende eines Domainnamens trennt das Label für die erste Hierarchieebene von der Wurzel (engl. root). Diese erste Ebene wird auch als Top-Level-Domain (TLD) bezeichnet. Die DNS-Objekte einer Domäne (zum Beispiel die Rechnernamen) werden als Satz von Resource Records meist in einer Zonendatei gehalten, die auf einem oder mehreren autoritativen Nameservern vorhanden ist. Anstelle von Zonendatei wird meist der etwas allgemeinere Ausdruck Zone verwendet.

3.2 Nameserver

Ein Nameserver ist ein Server, der Namensauflösung anbietet. Namensauflösung ist das Verfahren, das es ermöglicht, Namen von Rechnern bzw. Diensten in eine vom Computer bearbeitbare Adresse aufzulösen (z. B. www.wikipedia.org in 91.198.174.192).

Die meisten Nameserver sind Teil des Domain Systems, das auch im Internet benutzt wird.

Nameserver sind zum einen Programme, die auf Basis einer DNS-Datenbank Anfragen zum Domain-Namensraum beantworten, im Sprachgebrauch werden allerdings auch die Rechner, auf denen diese Programme zum Einsatz kommen, als Nameserver bezeichnet. Man unterscheidet zwischen autoritativen und nicht-autoritativen Nameservern.

Ein autoritativer Nameserver ist verantwortlich für eine Zone. Seine Informationen über diese Zone werden deshalb als gesichert angesehen. Für jede Zone existiert mindestens ein autoritativer Server, der Primary Nameserver. Dieser wird im SOA Resource Record einer Zonendatei aufgeführt. Aus Redundanz- und Lastverteilungsgründen werden autoritative Nameserver fast immer als Server-Cluster realisiert, wobei die Zonendaten identisch auf einem oder mehreren Secondary Nameservern liegen. Die Synchronisation zwischen Primary und Secondary Nameservern erfolgt per Zonentransfer.

Ein nicht-autoritativer Nameserver bezieht seine Informationen über eine Zone von anderen Nameservern sozusagen aus zweiter oder dritter Hand. Seine Informationen werden als nicht gesichert angesehen. Da sich DNS-Daten normalerweise nur sehr selten ändern, speichern nicht-autoritative Nameserver die einmal von einem Resolver angefragten Informationen im lokalen RAM ab, damit diese bei einer erneuten Anfrage schneller vorliegen. Diese

Technik wird als Caching bezeichnet. Jeder dieser Einträge besitzt ein eigenes Verfallsdatum (TTL time to live), nach dessen Ablauf der Eintrag aus dem Cache gelöscht wird. Die TTL wird dabei durch einen autoritativen Nameserver für diesen Eintrag festgelegt und wird nach der Änderungswahrscheinlichkeit des Eintrages bestimmt (sich häufig ändernde DNS-Daten erhalten eine niedrige TTL). Das kann unter Umständen aber auch bedeuten, dass der Nameserver in dieser Zeit falsche Informationen liefern kann, wenn sich die Daten zwischenzeitlich geändert haben.

Ein Spezialfall ist der Caching Only Nameserver. In diesem Fall ist der Nameserver für keine Zone verantwortlich und muss alle eintreffenden Anfragen über weitere Nameserver (Forwarder) auflösen. Dafür stehen verschiedene Strategien zur Verfügung:

3.3 Zusammenarbeit der einzelnen Nameserver

Damit ein nicht-autoritativer Nameserver Informationen über andere Teile des Namensraumes finden kann, bedient er sich folgender Strategien:

Delegierung

Teile des Namensraumes einer Domain werden oft an Subdomains mit dann eigens zuständigen Nameservern ausgelagert. Ein Nameserver einer Domäne kennt die zuständigen Nameserver für diese Subdomains aus seiner Zonendatei und delegiert Anfragen zu diesem untergeordneten Namensraum an einen dieser Nameserver.

Weiterleitung (forwarding)

Falls der angefragte Namensraum außerhalb der eigenen Domäne liegt, wird die Anfrage an einen fest konfigurierten Nameserver weitergeleitet.

Auflösung über die Root-Server

Falls kein Weiterleitungsserver konfiguriert wurde oder dieser nicht antwortet, werden die Root-Server befragt. Dazu werden in Form einer statischen Datei die Namen und IP-Adressen der Root-Server hinterlegt. Es gibt 13 Root-Server (Server A bis M). Die Root-Server beantworten ausschließlich iterative Anfragen. Sie wären sonst mit der Anzahl der Anfragen schlicht überlastet.
Anders konzipierte Namensauflösungen durch Server, wie der NetWare Name Service oder der Windows Internet Naming Service, sind meistens auf Local Area Networks beschränkt und werden zunehmend von der Internetprotokollfamilie verdrängt.

3.4 Resolver

Schematische Darstellung der rekursiven und iterativen DNS-Abfrage
Resolver sind einfach aufgebaute Software-Module, die auf dem Rechner eines DNS-Teilnehmers installiert sind und die Informationen von Nameservern abrufen können. Sie bilden die Schnittstelle zwischen Anwendung und Nameserver. Der Resolver übernimmt die Anfrage einer Anwendung, ergänzt sie, falls notwendig, zu einem FQDN und übermittelt sie an einen normalerweise fest zugeordneten Nameserver. Ein Resolver arbeitet entweder rekursiv oder iterativ.

Im rekursiven Modus schickt der Resolver eine rekursive Anfrage an den ihm zugeordneten Nameserver. Hat dieser die gewünschte Information nicht im eigenen Datenbestand, so kontaktiert der Nameserver weitere Server, und zwar solange bis er entweder eine positive Antwort oder bis er von einem autoritativen Server eine negative Antwort erhält. Rekursiv arbeitende Resolver überlassen also die Arbeit zur vollständigen Auflösung ihrem Nameserver.

Bei einer iterativen Anfrage bekommt der Resolver entweder den gewünschten Resource Record oder einen Verweis auf weitere Nameserver, die er als Nächstes fragt. Der Resolver hangelt sich so von Nameserver zu Nameserver, bis er von einem eine verbindliche Antwort erhält.

Die so gewonnene Antwort übergibt der Resolver an das Programm, das die Daten angefordert hat, beispielsweise an den Webbrowser. Übliche Resolver von Clients arbeiten ausschließlich rekursiv, sie werden dann auch als Stub-Resolver bezeichnet. Nameserver besitzen in der Regel eigene Resolver. Diese arbeiten gewöhnlich iterativ.

Bekannte Programme zur Überprüfung der Namensauflösung sind nslookup, host und dig.

Siehe auch: Rekursive und iterative Namensauflösung

3.5 Protokoll

DNS-Anfragen werden normalerweise per UDP Port 53 zum Namensserver gesendet. Der DNS-Standard fordert aber auch die Unterstützung von TCP für Fragen, deren Antworten zu groß für UDP-Übertragungen sind.[1] Falls kein Extended DNS verwendet wird (EDNS), beträgt die maximal zulässige Länge des DNS-UDP-Pakets 512 Bytes. Überlange Antworten werden daher abgeschnitten übertragen. Durch Setzen des Truncated-Flags wird der anfragende Client über diesen Sachverhalt informiert. Er muss dann entscheiden, ob ihm die Antwort reicht oder nicht. Gegebenenfalls wird er die Anfrage per TCP Port 53 wiederholen.

Zonentransfers werden stets über Port 53 TCP durchgeführt. Die Auslösung von Zonentransfers erfolgt aber gewöhnlich per UDP.

4 Aufbau der DNS-Datenbank

Das Domain Name System kann als verteilte Datenbank mit baumförmiger Struktur aufgefasst werden. Beim Internet-DNS liegen die Daten auf einer Vielzahl von weltweit verstreuten Servern, die untereinander über Verweise – in der DNS-Terminologie Delegierungen genannt – verknüpft sind.

In jedem beteiligten Nameserver existieren eine oder mehrere Dateien – die so genannten Zonendateien – die alle relevanten Daten enthalten. Bei diesen Dateien handelt es sich um Listen von Resource Records. Von großer Bedeutung sind sieben Record-Typen:

Mit dem **SOA Resource Record** werden Parameter der Zone, wie z. B. Gültigkeitsdauer oder Seriennummer, festgelegt.
Mit dem **NS Resource Record** werden die Verknüpfungen (Delegierungen) der Server untereinander realisiert.
Mit folgenden Record-Typen werden die eigentlichen Daten definiert:
Ein **A Resource Record** weist einem Namen eine IPv4-Adresse zu.
Ein **AAAA Resource Record** weist einem Namen eine IPv6-Adresse zu.
Ein **CNAME Resource Record** verweist von einem Namen auf einen anderen Namen.
Ein **MX Resource Record** weist einem Namen einen Mailserver zu. Er stellt eine Besonderheit dar, da er sich auf einen speziellen Dienst im Internet, nämlich die E-Mailzustellung mittels SMTP, bezieht. Alle anderen Dienste nutzen CNAME, A und AAAA Resource Records für die Namensauflösung.
Ein **PTR Resource Record** weist einer IP-Adresse einen Namen zu (Reverse Lookup) und wird für IPv4 und IPv6 gleichermaßen benutzt, nur für IPv4 unterhalb der Domain „IN-ADDR.ARPA.“ und für IPv6 unterhalb von „IP6.ARPA.“.
Im Laufe der Zeit wurden neue Typen definiert, mit denen Erweiterungen des DNS realisiert wurden. Dieser Prozess ist noch nicht abgeschlossen. Eine umfassende Liste findet sich unter Resource Record.

Beispiele:

Folgender NS Resource Record ist in der Zonendatei der Domain „org.“ definiert: Die Zonendatei für die Domain „wikipedia.org.“ befindet sich auf dem Server „ns0.wikimedia.org.“. Der Punkt am Ende ist wichtig, da dieser klarstellt, dass kein relativer Name gemeint ist, also hinter „org“ nichts mehr zu ergänzen ist. „IN“ meint, dass der Eintrag die Klasse „Internet“ besitzt und die Zahl davor bedeutet die Time To Live (TTL) in Sekunden, sie besagt, wie lange diese Information in einem Cache zwischengespeichert werden könnte, bevor sie neu erfragt werden sollte. Bei dynamischen IP-Adressen liegt diese Zahl meistens zwischen 20 und 300 Sekunden.

```
wikipedia   86400  IN  NS   ns0.wikimedia.org.
```

Folgender CNAME Resource Record in der Zonendatei der Domain „wikipedia.org.“ definiert: Der Name „de.wikipedia.org.“ verweist auf den Namen „rr.wikimedia.org.“.

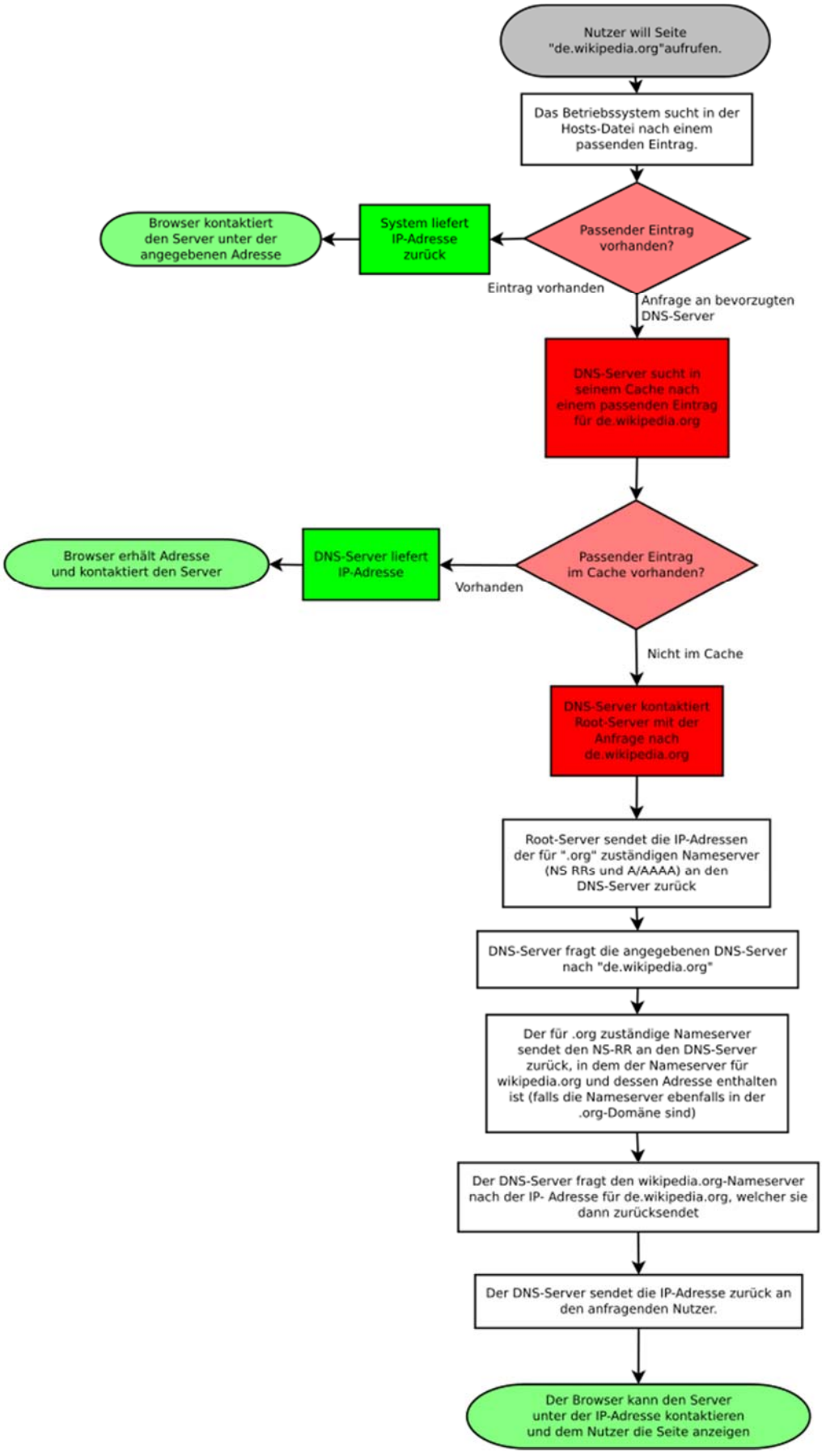
```
de          3600   IN  CNAME   rr.wikimedia.org.
```

Folgende Resource Records in der Zonendatei der Domain „wikimedia.org.“ definieren: Der Name „rr.wikimedia.org.“ verweist auf den Namen „rr.esams.wikimedia.org.“ und diesem wiederum ist die IPv4-Adresse 91.198.174.232 zugewiesen.

```
rr          600    IN  CNAME   rr.esams
rr.esams    3600   IN  A       91.198.174.232
```

Letztlich müssen also alle Rechner, die sich mit „de.wikipedia.org.“ verbinden möchten, IPv4-Pakete an die IP-Adresse 91.198.174.232 senden.

5 Auflösung eines DNS-Requests



Angenommen, ein Rechner X will eine Verbindung zu „de.wikipedia.org.“ (Rechner Y) aufbauen. Dazu braucht er dessen IP-Adresse. In den folgenden Schritten wird beschrieben, wie dies ablaufen könnte. Falls der Rechner X IPv6-fähig ist, läuft der Vorgang zunächst für IPv6 (Abfrage von AAAA Resource Record) und sofort danach für IPv4 (Abfrage von A Resource Record) ab. Dabei kann eine Anfrage nach einer IPv6-Adresse mittels IPv4-Übertragung an einen IPv4-DNS-Server gerichtet werden. Falls am Ende eine IPv6- und eine IPv4-Adresse für Rechner Y ermittelt werden, wird in der Regel laut der Default Policy Table in RFC 3484 die Kommunikation zwischen X und Y über IPv6 bevorzugt,[2] es sei denn im Betriebssystem oder in den benutzten Anwendungen, wie zum Beispiel dem Webbrowser, wurde dieses Verhalten anders eingestellt.

Der Rechner X sucht in seiner Hosts-Datei, ob die IP-Adresse für „de.wikipedia.org“ dort hinterlegt ist. Falls dem nicht so ist, fragt er beim DNS-Server nach. Dieser ist entweder fest eingetragen oder wurde per DHCP bzw. DHCPv6 automatisch zugewiesen und hat die Form nameserver 192.0.2.23 oder nameserver 2001:db8::23:cafe:affe:42.
Hat der DNS-Server von Rechner X eine IP-Adresse für den angefragten Namen zwischengespeichert, antwortet er damit und die Anfrage kommt zum Ende (siehe letzter Punkt). Andernfalls fragt er einen der 13 Root-Nameserver nach „de.wikipedia.org.“.
Der Root-Nameserver findet heraus, dass die Auflösung dieses Namens in der „org.“-Zone weitergeht und sendet die Namen und die IP-Adressen der „org.“-Nameserver (NS Resource Records und deren AAAA bzw. A Resource Records) zum DNS-Server von Rechner X.
Nun fragt der DNS-Server von Rechner X einen der Nameserver für „org.“-Domains nach „de.wikipedia.org.“.
Der „org.“-Nameserver sendet ihm die Namen der Nameserver (und deren IP-Adressen, sofern sie zur selben Top-Level-Domain gehören) für die Zone „wikipedia.org.“.
Anschließend fragt der DNS-Server von Rechner X einen „wikipedia.org.“-Nameserver wie die IP-Adresse des Namens "de.wikipedia.org." ist.
Mit dieser Adresse wird an den DNS-Server von Rechner X geantwortet und der ...
... sendet sie an den Rechner X, welcher nun zum Beispiel seine HTTP-Anfragen an die IP-Adresse von „de.wikipedia.org.“ senden kann.

6 Erweiterungen

Da sich das DNS als zuverlässig und flexibel erwiesen hat, wurden im Laufe der Jahre mehrere größere Erweiterungen eingeführt. Ein Ende dieses Trends ist nicht absehbar.

Dynamisches DNS
Im klassischen DNS ist es aufwendig, einem Namen eine neue IP-Adresse zuzuordnen. Das zugehörige Zonenfile muss (meist manuell) geändert und der Nameserver neu geladen werden. Zeitliche Verzögerungen bis hin zu mehreren Tagen sind üblich. Mit dynamischem DNS sind Änderungen durch Senden einer Aktualisierungsanfrage mit geringer Zeitverzögerung möglich.

Das Dynamische DNS gilt als Sicherheitsrisiko, da ohne spezielle Vorkehrungen jedermann DNS-Einträge löschen oder verändern kann. In Zusammenhang mit DHCP ist Dynamisches DNS nahezu zwingend erforderlich, da einem User häufig neue IP-Adressen zugewiesen werden. Der DHCP-Server sendet dazu bei jeder Adressänderung eine entsprechende Mitteilung an den Nameserver.

Internationalisierung
→ Hauptartikel: Internationalisierter Domainname
Bisher waren die Labels auf alphanumerische Zeichen und das Zeichen ‚-‘ eingeschränkt. Möglich, aber nicht standardkonform, ist bei Subdomains zudem ‚_‘. Dieser begrenzte Zeichenvorrat hängt vor allem damit zusammen, dass das DNS (wie auch das Internet ursprünglich) in den USA entwickelt wurde. Damit waren in vielen Ländern gebräuchliche Schriftzeichen (im deutschen Sprachraum zum Beispiel die Umlaute ä, ö und ü sowie ß) oder Zeichen aus komplett anderen Schriftsystemen (zum Beispiel Chinesisch) ursprünglich nicht in Domainnamen möglich.

Ein mittlerweile etablierter Ansatz zur Vergrößerung des Zeichenvorrats ist die 2003 in RFC 3490 eingeführte und 2010 mit RFC 5890 aktualisierte Internationalisierung von Domainnamen (IDNA). Um das neue System mit dem bisherigen kompatibel zu halten, werden die erweiterten Zeichensätze mit den bislang zulässigen Zeichen kodiert. Die erweiterten Zeichensätze werden dabei zunächst normalisiert, um unter anderem Großbuchstaben auf Kleinbuchstaben abzubilden, und anschließend per Punycode auf einen ASCII-kompatiblen String abgebildet. IDNA erfordert eine Anpassung der Netzwerkanwendungen (zum Beispiel Webbrowser), die Nameserver-Infrastruktur (Server, Resolver) braucht jedoch nicht verändert zu werden. Im deutschsprachigen Raum können seit März 2004 deutsche, liechtensteinische, österreichische und schweizerische Domains (.de, .li, .at und .ch) mit Umlauten registriert und verwendet werden. Auch bei anderen Top-Level-Domains, insbesondere im asiatischen Raum, ist die Verwendung von internationalisierten Domainnamen möglich.

Extended DNS
1999 beschrieb Paul Vixie im RFC 2671 einige kleinere, abwärtskompatible Erweiterungen am Domain Name System, die als EDNS Version 0 bezeichnet werden. Durch Einsatz eines Pseudo-Records als Header-Erweiterung kann der Anfragende zusätzliche Optionen setzen. Insbesondere kann er übermitteln, dass er UDP-Antworten größer als 512 Bytes entgegennehmen kann. DNSSEC-fähige Server und Resolver müssen EDNS beherrschen.

Verwaltung von Telefonnummern
Eine weitere aktuelle Erweiterung des DNS stellt ENUM (RFC 2916) dar. Diese Anwendung ermöglicht die Adressierung von Internet-Diensten über Telefonnummern, also das „Anwählen“ von per Internet erreichbaren Geräten mit dem aus dem Telefonnetz bekannten Nummerierungsschema. Aus dem breiten Spektrum der Einsatzmöglichkeiten bietet sich insbesondere die Verwendung für Voice over IP Services an.

RFID-Unterstützung
Mit der Radio Frequency Identification können auf speziellen RFID-Etiketten abgelegte IDs – so genannte elektronische Produktcodes oder EPCs – berührungslos gelesen werden. Das DNS kann dazu verwendet werden, zu einer ID den Server zu ermitteln, der Daten über das zugehörige Objekt enthält. Der Object Naming Service ONS wandelt dazu den EPC in einen DNS-Namen um und erfragt per Standard-DNS einen oder mehrere Naming Authority Pointer NAPTR.

Spam-Abwehr
Zur Filterung von Spam-Mails überprüfen viele Mailserver den DNS-Eintrag des sendenden Mailservers routinemäßig mit Hilfe des Reverse DNS Lookup. Dieser muss nicht nur auch vorwärts wieder korrekt auflösen und auf die IP-Adresse des sendenden Systems zeigen (Forward-confirmed reverse DNS), sondern muss auch dem im SMTP-Protokoll genannten HELO-Hostnamen des sendenden Systems entsprechen.

Mittels Sender Policy Framework wird versucht, den Versand von gefälschten Absendern durch Dritte möglichst zu unterbinden. Zu jeder Mail-Domain wird dabei über einen speziellen SPF Resource Record explizit aufgelistet, von welchen Servern und IP-Netzen mit E-Mails dieser Domain zu rechnen ist. SPF steht jedoch wegen zahlreicher technischer Schwierigkeiten, beispielsweise bei Weiterleitungen, in der Kritik.

Auch der Anti-Spam-Mechanismus DomainKeys (DKIM) greift auf Einträge im DNS zurück, indem sendende Mailserver in DNS-TXT-Records ihren Public-Key veröffentlichen, mit dem die Signatur ihrer ausgehenden E-Mails verifiziert werden kann.

Sonstiges
Neben den IP-Adressen können DNS-Namen auch ISDN-Nummern, X.25-Adressen, ATM-Adressen, öffentliche Schlüssel, Text-Zeilen usw. zugeordnet werden. In der Praxis sind derartige Anwendungsfälle aber die Ausnahme.

DNS im lokalen Netz
DNS ist nicht auf das Internet beschränkt. Es ist ohne weiteres möglich und mit der Definition verträglich, für die Auflösung lokaler Namen eigene Zonen im Nameserver einzurichten und dort die entsprechenden Adressen einzutragen. Der einmalige Aufwand zur Installation lohnt sich auch bei relativ kleinen Netzen, da dann alle Adressen im Netz zentral verwaltet werden können.

Bei größeren Firmen oder Organisationen ist häufig ein aus lokalem und Internet-DNS bestehendes Mischsystem (Split-DNS) anzutreffen. Die internen Nutzer greifen auf das lokale und die externen auf das Internet-DNS zu. In der Praxis können dadurch sehr komplizierte Konstellationen entstehen.

Der DNS-Server BIND kann auch mit DHCP zusammenarbeiten und damit für jeden Client im Netz eine Namensauflösung ermöglichen.

Unter Windows gibt es noch einen anderen Dienst zur Namensauflösung – WINS, der eine ähnliche Funktion zur Verfügung stellt, allerdings ein anderes Protokoll verwendet.

DNS-Serververbund
Es ist möglich, mehrere DNS-Server zu verbinden. Die als Master bezeichneten Server sind für eine oder mehrere Domains verantwortlich. Die Slaves aktualisieren nach einer Änderung selbst die Daten, der Master verteilt diese Daten nicht automatisiert. Die Abholung der Daten wird über einen Zonentransfer realisiert.

Beispielsweise kann eine Firma mit mehreren Standorten an einem Platz einen Master für ihr internes DNS betreiben, der die Server in den Außenstellen versorgt. Der Zonentransfer geht bei BIND über TCP (per Default Port 53) und erfordert empfohlenerweise Authentifizierung. Die Slaves aktualisieren sich, wenn sich die Seriennummer

für eine Zonendatei ändert oder sie eine entsprechende Nachricht vom Master erhalten. Die Freigabe für den Transferport sollte man per Firewall an die IP-Adresse des Masters binden. Bei anderen Softwarepaketen werden die Daten unter Umständen auf anderen Wegen abgeglichen, beispielsweise durch LDAP-Replikation, rsync, oder noch andere Mechanismen.

Sicherheit
Das DNS ist ein zentraler Bestandteil einer vernetzten IT-Infrastruktur. Eine Störung kann erhebliche Kosten nach sich ziehen und eine Verfälschung von DNS-Daten Ausgangspunkt von Angriffen sein. Mehr als zehn Jahre nach der ursprünglichen Spezifikation wurde DNS um Security-Funktionen ergänzt. Folgende Verfahren sind verfügbar:

Bei TSIG (Transaction Signatures) handelt es sich um ein einfaches, auf symmetrischen Schlüsseln beruhendes Verfahren, mit dem der Datenverkehr zwischen DNS-Servern und Updates von Clients gesichert werden kann.
Bei DNSSEC (DNS Security) wird von einem asymmetrischen Kryptosystem Gebrauch gemacht. Neben der Server-Server-Kommunikation kann auch die Client-Server-Kommunikation gesichert werden.

Angriffsformen
Hauptziel von DNS-Angriffen ist es, durch Manipulation DNS-Teilnehmer auf falsche Webseiten zu lenken, um anschließend Passwörter, PINs, Kreditkartennummern usw. zu erhalten. In seltenen Fällen wird versucht, den Internet-DNS durch Denial-of-Service-Attacken komplett auszuschalten und so das Internet lahmzulegen. Außerdem kann das DNS dazu verwendet werden, gezielte Angriffe auf Einzelpersonen oder Unternehmen zu intensivieren.

DDoS-Angriff auf Nameserver
Bei einer Distributed-Denial-of-Service-Attacke werden Nameserver durch einen hohen Datenstrom von DNS-Anfragen überlastet, so dass legitime Anfragen nicht mehr beantwortet werden können. Gegen DDoS-Angriffe auf Nameserver gibt es zurzeit keine Abwehrmöglichkeit. Als vorbeugende Maßnahme kann lediglich versucht werden, die Nameserver entsprechend zu dimensionieren bzw. ein verteiltes Netz mit möglichst vielen Servern zu installieren. Bei solchen Attacken werden häufig Botnetze und dergleichen eingesetzt.

DNS-Amplification-Angriff
Die DNS Amplification Attack ist ein Denial-of-Service-Angriff, bei der nicht der DNS-Server selbst das eigentliche Angriffsziel ist, sondern ein unbeteiligter Dritter. Ausgenutzt wird, dass DNS-Server in manchen Fällen auf kurze Anfragen sehr lange Antworten zurücksenden. Durch eine gefälschte Absenderadresse werden diese an die IP-Adresse des Opfers gesendet. Ein Angreifer kann damit den von ihm ausgehenden Datenstrom substanziell verstärken und so den Internet-Zugang seines Angriffziels stören.

DNS-Spoofing
Beim DNS-Spoofing bekommt ein anfragender Client eine falsche IP-Adresse als Antwort, um ihn (z.B. zwecks Internet-Zensur oder Phishing) auf eine falsche bzw. gefälschte Website zu führen.

Cache Poisoning
Beim Cache Poisoning werden einem anfragenden Client zusätzlich zur korrekten Antwort manipulierte Daten übermittelt, die dieser in seinen Cache übernimmt und später, möglicherweise ungeprüft, verwendet.

Offener DNS-Server
Wer einen autoritativen DNS-Server für seine eigenen Domains betreibt, muss natürlich für Anfragen von beliebigen IP-Adressen offen sein. Um zu verhindern, dass Internetteilnehmer diesen Server als allgemeinen Nameserver verwenden (z. B. für Angriffe auf Root-Server), erlaubt BIND es, die Antworten auf die eigenen Domains einzuschränken. Z. B. bewirkt die Option allow-recursion {127.0.0.1; 172.16.1.4;}; , dass rekursive Anfragen, d. h. Anfragen auf andere Domains, ausschließlich für den lokalen Host (localhost) sowie 172.16.1.4 beantwortet werden. Alle anderen IP-Adressen bekommen nur auf Anfragen auf eigene Domains eine Antwort.

Ein offener DNS-Server kann auch eine Falle sein, wenn er gefälschte IP-Adressen zurückgibt, siehe Pharming.

Spamabwehr
Bei schwarzen Listen (auch 'RBL'; Abkürzung für engl. Realtime Blackhole Lists) z. B. gegen Spammer, wird DNS angewendet, um abzufragen, ob ein Domainname oder eine IP-Adresse gelistet ist: Der Client schickt eine DNS-Anfrage an den Rbl-Server. Dieser antwortet mit '127.0.0.1', wenn die Adresse nicht gelistet ist, sonst mit '127.0.0.x', x>1. Der Wert von 'x' kann noch zusätzliche Informationen über die gelistete Adresse enthalten. Da der Bereich 127.0.0.0/8 für Localhost reserviert ist, sind Missdeutungen nicht möglich.

Domain-Registrierung
Um DNS-Namen im Internet bekannt machen zu können, muss der Besitzer die Domain, die diesen Namen enthält, registrieren. Durch eine Registrierung wird sichergestellt, dass bestimmte formale Regeln eingehalten werden und dass Domain-Namen weltweit eindeutig sind. Domain-Registrierungen werden von Organisationen (Registrars)

vorgenommen, die dazu von der IANA bzw. ICANN autorisiert wurden. Registrierungen sind (von wenigen Ausnahmen abgesehen) gebührenpflichtig. Für Domains unter .de ist die DENIC zuständig.

Detaillierte Informationen finden sich unter Domain-Registrierung.

Bonjour bzw. Zeroconf
Apple hat bei der Entwicklung von OS X mehrere Erweiterungen am DNS vorgenommen, welche die umfassende Selbstkonfiguration von Diensten in LANs ermöglichen soll. Zum einen wurde Multicast DNS („mDNS“) eingeführt, das die Namensauflösungen in einem LAN ohne einen dedizierten Namensserver erlaubt. Zusätzlich wurde noch DNS-SD (für „DNS Service Discovery“) eingeführt, die die Suche („Browsing“) nach Netzwerkdiensten in das DNS beziehungsweise mDNS ermöglicht. mDNS und DNS-SD sind bisher keine offiziellen RFCs des IETF, sind aber trotzdem bereits in verschiedenen (auch freien) Implementationen verfügbar. Zusammen mit einer Reihe von anderen Techniken fasst Apple DNS-SD und mDNS unter dem Namen „Zeroconf“ zusammen, als Bestandteil von OS X auch als „Rendezvous“ bzw. „Bonjour“. Die meisten Linux Distributionen unterstützen diese Erweiterung z.B. mit der avahi-Implementierung von Zeroconf.

Zensur und alternative DNS
Seit den Debatten um Sperrungen von Internetinhalten in Deutschland und Zensur im Internet allgemein, gibt es eine Reihe von alternativen DNS-Anbietern, die Domains nach eigener Aussage nicht zensieren. Beispiele sind Open Root Server Network, Cesidian ROOT, OpenNIC, Projekte von deutschen Vereinen wie dem Chaos Computer Club, digitalcourage und der German Privacy Foundation, sowie kommerzielle Anbieter wie OpenDNS.[3]

Namecoin
Namecoin ist ein alternatives verteiltes Domain-Name-System (DNS) auf der Basis der Bitcoin-Software. Es erweitert die Software derart, dass Transaktionen zum Registrieren, Aktualisieren und Übertragen von Domains dienen. Ebenso wie Bitcoin ist Namecoin ein Peer-to-Peer-System, das unter der Annahme einer ehrlichen Teilnehmermehrheit nicht durch einen einzelnen Staat oder eine Firma kontrolliert werden kann. Die Software ist Open Source und wird auf GitHub gehostet.

Nameserversoftware
Auswahl bekannter Software für Namensauflösung.

BIND (Berkeley Internet Name Domain) ist die meistgebrauchte Nameserversoftware und gilt als Referenzimplementierung der meisten RFCs zu DNS. Die erste Version von BIND war die erste öffentlich verfügbare Nameserver-Implementierung.
Bei djbdns hat der Autor Daniel J. Bernstein eine Prämie für das Finden von Sicherheitsproblemen ausgeschrieben. Djbdns wird von Bernstein nicht mehr weiterentwickelt, weil er es als fertig ansieht.
Dnsmasq ist ein Nameserver und DHCP-Server mit eingeschränkter Funktionalität. Es werden die Namen aus dem lokalen Netz entsprechend /etc/hosts aufgelöst. Dnsmasq verfügt über keinen vollständigen Resolver: unbekannte Namensanfragen werden weitergeleitet und im Cache gespeichert.
Knot DNS ist ein autoritativer Nameserver, der von CZ.NIC entwickelt wird, dem Betreiber von .cz.
Microsoft Windows DNS ist eine der wenigen kommerziellen Nameserver-Implementierung und in der Produktreihe Microsoft Windows Server enthalten. Der Nameserver unterstützt dynamische Updates, Zonentransfers und Notification. Zonendaten können in den aktuellen Versionen im Active Directory oder in Zonendateien gespeichert und repliziert werden.
NSD (Name Server Daemon) ist ein autoritativer Nameserver, der zum Einsatz als Top-Level-Domain- und Root-Nameserver entwickelt wurde. NSD kompiliert Antworten statisch vor, um die Server-Performance zu optimieren. Dynamische Zoneninhalte oder Round Robin werden nicht unterstützt.
PowerDNS ist ein Nameserver, der Zonen aus SQL-Datenbanken, LDAP-Verzeichnissen und anderen Backends lesen kann. PowerDNS begann als kommerzielle Implementierung und ist seit 2002 unter der GPL lizenziert.
Unbound ist ein DNS-Resolver, der DNSSEC-Validierung und Caching unterstützt. Unbound kann als Softwarebibliothek in Anwendungen eingebunden werden.