8. Verzeichnisdienste: Der Domain Name Service

8.1 Der Namensraum des Domain Name Service (DNS)

8.2 Die Protokolle des DNS

8.1 Der Namensraum des Domain Name Service (DNS) im Internet

Aufgabe des DNS

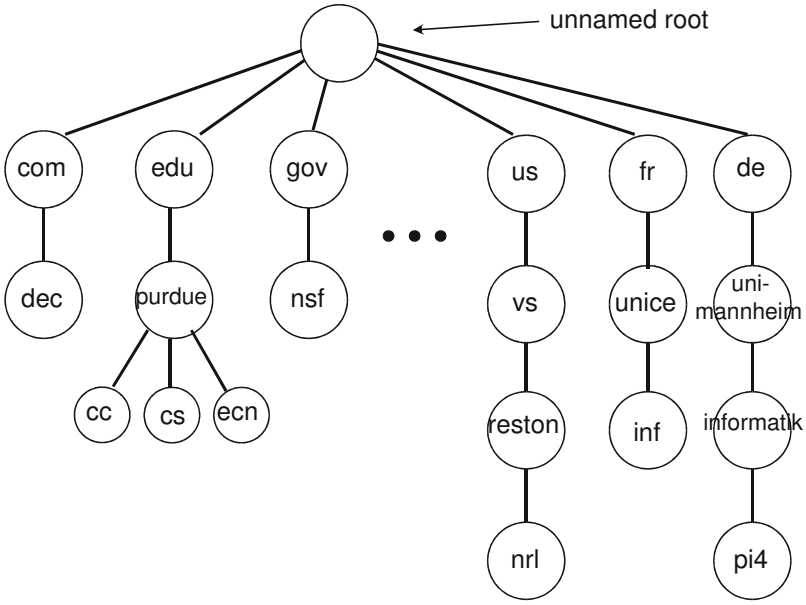
Abbildung von logischen Namen auf Internet-Adressen (IP-Adressen).

Die Namen im Internet sind hierarchisch strukturiert, z. B.:

- de
- uni-mannheim.de
- informatik.uni-mannheim.de
- pi4.informatik.uni-mannheim.de

Jede Hierarchiestufe entspricht einer **Domäne** von Adressen. Für jede Domäne existiert ein Name-Server, der die Hosts seiner Domäne kennt.

Struktur der Domänennamen



Für jede Domäne gibt es eine administrative Stelle für die Namensvergabe.

Bildung von zulässigen Namen

- Jeder Knoten hat einen Bezeichner (“label“), der höchstens 63 Buchstaben lang ist.
- Die Wurzel des DNS-Namensraumes hat einen leeren Bezeichner.
- Groß-/Kleinschreibung wird nicht unterschieden.
- Einen “absolute domain name / fully qualified domain name“ (FQDN) erhält man, wenn man von einem Blatt des DNS-Namensraumes zur Wurzel geht und dabei alle Bezeichner notiert; die Bezeichner werden mit einem Punkt voneinander getrennt.

8.2 Die Protokolle des DNS

Die wesentlichen Komponenten des DNS sind:

- ein verteiltes System zur Erbringung eines Verzeichnis-Dienstes, das aus einer Hierarchie von Name-Servern besteht,
- ein Protokoll der Anwendungsschicht, das es Hosts und Name-Servern ermöglicht, Host-Namen in IP-Adressen aufzulösen.

Das DNS-Protokoll setzt (in der Regel) auf UDP auf und benutzt Port 53.

Das DNS wird häufig von anderen Protokollen der Anwendungsschicht benutzt, um die vom Benutzer eingegebenen Hostnamen in IP-Adressen umwandeln zu lassen (z. B. von SMTP und HTTP).

Die wichtigsten Standards zum DNS sind RFC 1034 und RFC 1035.

Nebenfunktionen des DNS (1)

- **Host-Aliasing:** Ein Host mit einem komplizierten Hostnamen kann einen oder mehrere Aliasnamen haben. Beispielsweise könnte der Hostname relay1.westcoast.enterprise.com zwei Aliasnamen haben: enterprise.com und www.enterprise.com. In diesem Fall ist der Hostname relay1.west-coast.enterprise.com ein so genannter **kanonischer** Hostname.

  Sofern vorhanden, sind Alias-Hostnamen in der Regel leichter merkbar (“mnemonischer“) als kanonische Hostnamen.

Nebenfunktionen des DNS (2)

- **Lastverteilung:** Vermehrt wird DNS auch für die Durchführung einer Lastverteilung zwischen replizierten Servern, zum Beispiel replizierten Web-Servern, verwendet. Sehr stark frequentierte Websites, wie zum Beispiel cnn.com, werden auf mehreren Servern repliziert, wobei jeder Server auf einem anderen Host läuft und eine andere IP-Adresse hat. Mit einem replizierten Web-Server wird dann ein Gruppe von IP-Adressen mit einem kanonischen Hostnamen assoziiert. Die DNS-Datenbank enthält diese Gruppe von IP-Adressen.

  Wenn nun Clients eine DNS-Anfrage für einen Namen stellen, der auf eine Gruppe von Adressen abgebildet ist, antwortet der Server mit der gesamten Gruppe der IP-Adressen, stellt aber die Reihenfolge der Adressen in jeder Antwort um. Da ein Client normalerweise seine HTTP-Anfragenachricht an die IP-Adresse sendet, die an erster Stelle in der Gruppe steht, wird der Verkehr durch die DNS-Rotation auf alle replizierten Server gleichmäßig verteilt.

Lokale Name-Server

Lokale Name-Server: Jeder ISP (z. B. eine Universität, eine Fakultät, eine Firma oder ein kommerzieller ISP) verfügt über einen lokalen Name-Server (den man auch als “Default-Name-Server“ bezeichnet). Wenn ein Host eine DNS-Anfragenachricht ausgibt, wird die Nachricht zuerst an den lokalen Name-Server gesandt. Die IP-Adresse des lokalen Name-Servers wird in der Regel manuell in jedem Host konfiguriert (bei IP Version 4).

Der lokale Name-Server befindet sich normalerweise in der Nähe des Clients. Wenn ein Host die Übersetzung einer Adresse eines anderen Hosts anfordert, der zum gleichen lokalen ISP gehört, kann der lokale Name-Server die angeforderte IP-Adresse sofort bereit stellen.

Root-Name-Server

Root-Name-Server: Im Internet gibt es etwa ein Dutzend Root-Name-Server, die größtenteils in Nordamerika stehen. Wenn ein lokaler Name-Server eine Anfrage von einem Host nicht direkt beantworten kann, weil er keinen Eintrag für den angeforderten Hostnamen hat, verhält sich der lokale Name-Server seinerseits wie ein DNS-Client und fragt bei einem der Root-Name-Server an. Ist der betreffende Hostname bei dem Root-Name-Server verzeichnet, sendet dieser eine DNS-Antwortnachricht an den lokalen Name-Server, und der lokale Name-Server sendet dann eine DNS-Antwort an den anfragenden Host.

Autoritative Name-Server

Autoritative Name-Server: Jeder Host ist bei einem **autoritativen** Name-Server registriert. Normalerweise ist der autoritative Name-Server für einen Host ein Name-Server beim lokalen ISP. Ein Name-Server ist der autoritative Name-Server für einen Host, wenn er **ständig** über einen DNS-Eintrag verfügt, der den Hostnamen dieses Hosts in seine IP-Adresse übersetzt. Erhält ein autoritativer Name-Server eine Anfrage von einem Root-Name-Server, reagiert der autoritative Name-Server mit einer DNS-Antwort, in der sich die angeforderte Übersetzung befindet.

Viele Name-Server fungieren zugleich als lokale und als autoritative Name-Server.

Häufig ordnet man autoritative Name-Server 1:1 einer Domäne zu, das muss aber nicht so sein; die Topologie der Name-Server muss nicht mit der hierarchischen Struktur des Namensraumes übereinstimmen.

Funktionsweise der Namensauflösung

Zweistufiger Auflösungsmechanismus

- Der Client kontaktiert seinen lokalen Name-Server.
- Wenn keine lokale Namensauflösung möglich ist, wird die Hierarchie durchlaufen.

In der Praxis werden in vielen Fällen immer dieselben Namen benötigt. Deshalb ist eine signifikante Effizienzsteigerung durch Caching im lokalen Name-Server möglich.

Algorithmus zur Namensauflösung (1)

- Die DNS-Client-Software heißt "*name resolver*".
- Der *name resolver* kennt die Adresse von mindestens einem Name-Server. Dies ist der lokale Name-Server, meist ein Blatt-Knoten in der Baumstruktur des verteilten DNS-Systems.
- Der *name resolver* baut eine Anfrage-PDU auf ("domain name query") und sendet sie an den Name-Server. Dabei verlangt er entweder "recursive resolution" oder "non-recursive resolution".
- Der Name-Server prüft, ob er die Anfrage lokal beantworten kann.
  - Falls ja, sendet er die Antwort an den Client.
  - Falls nein und "**recursive resolution**" verlangt ist, kontaktiert er einen oder mehrere weitere Name-Server im Baum, bis er die Antwort hat. Jeder Name-Server muss mindestens einen Root-Server kennen (mit IP-Adresse und DNS-Port). Der zuerst kontaktierte Name-Server leitet dann die Antwort an den Client weiter.

Algorithmus zur Namensauflösung (2)

  - Falls nein und "**iterative resolution**" verlangt ist, meldet er dem Client den Namen eines anderen Name-Servers, den er versuchen könnte.
- Jeder Name-Server hat einen Cache für Einträge, die von einem anderen Name-Server geholt wurden. Die Cache-Einträge werden mit einem Timeout versehen („time-to-live"). Der Timeout dient zum Löschen von selten verwendeten Einträgen (typischer Timer-Wert: 2 Tage). Wird ein gesuchter Eintrag im Cache gefunden, so erhält der Client diese Information zusammen mit der Adresse des für den Eintrag zuständigen Name-Servers im Baum.
- Manche *name resolver* haben eigene Caches.

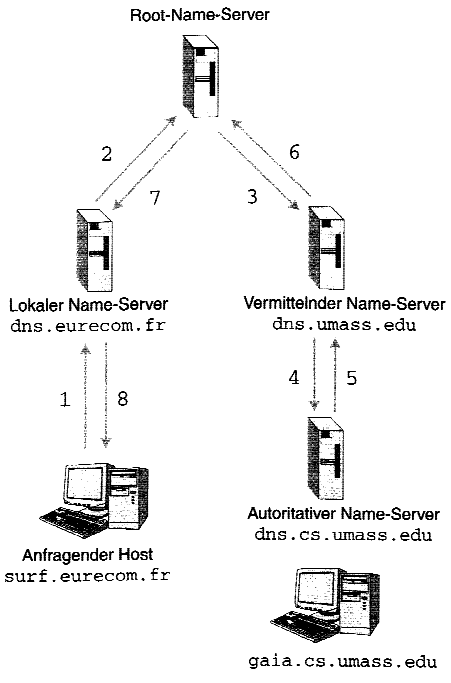
Root-Server erhalten in der Regel iterative Anfragen, alle anderen Name-Server rekursive Anfragen.

Beispiel für eine rekursive DNS-Anfrage

`surf.eurecom.fr`
fragt nach der IP-Adresse von
`gaia.cs.umass.edu`

Merke:

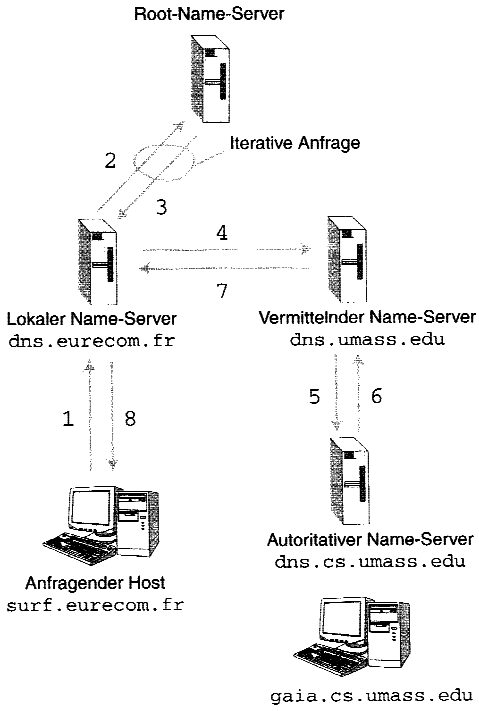
Eine **rekursive** Anfrage entspricht einem rekursiven Prozeduraufruf. Auf dem Rückweg folgen die Antworten dem Pfad der Anfrage.



Beispiel für eine iterative DNS-Anfrage

Eine **iterative** Anfrage wird für den Fall, dass der Server sich nicht auflösen kann, nicht mit der gesuchten IP-Adresse (nach entsprechenden Rückfragen) beantwortet, sondern mit der IP-Adresse des nächsten DNS-Servers in der Kette. Der anfragende Client muss dann selbst seine Anfrage dorthin senden.

Es kann auch entlang einer Kette eine Kombination aus rekursiven und iterativen Anfragen verwendet werden.



Format der DNS-Einträge (resource records) (1)

Die Name-Server, die zusammen die verteilte DNS-Datenbank implementieren, speichern so genannte **Resource-Records (RR)** für die Übersetzung von Hostnamen in IP-Adressen. Jede DNS-Antwortnachricht enthält einen oder mehrere Resource-Records.

Ein Resource-Record ist ein 5-Tupel, das folgende Felder enthält:

(*Name, Wert, Typ, Class, TTL*)

Die Bedeutung von *Name* und *Wert* hängen wie folgt von *Typ* ab:

- Wenn *Typ*=A, dann ist *Name* ein Hostname und *Wert* die IP-Adresse des Hosts. Folglich ermöglicht ein RR vom Typ A die Übersetzung eines Standard-Hostnamens in die IP-Adresse.
- Wenn *Typ*=NS (name server), dann ist *Name* eine Domäne (z. B. cnn.com) und *Wert* der Hostname eines autoritativen Name-Servers, der weiß, wie er die IP-Adressen für Hosts in dieser Domäne finden kann. Dieser RR wird benutzt, um DNS-Anfragen entlang der Abfragekette weiter zu leiten.

Format der DNS-Einträge (resource records) (2)

- Wenn *Typ*=CNAME (canonical name), dann ist *Wert* ein kanonischer Hostname für den Alias-Hostnamen *Name*. Dieser RR kann anfragenden Hosts den kanonischen Namen zu einem gegebenen Hostnamen liefern.
- Wenn *Typ*=MX (mail exchange), dann ist *Wert* der Hostname eines Mail-Servers, der einen Alias-Hostnamen *Name* hat. Beispielsweise ist (cnn.com, mail.bar.cnn.com, MX) ein MX-Record. MX-Records ermöglichen es, Hostnamen von Mail-Servern einfache Aliasnamen zu geben.

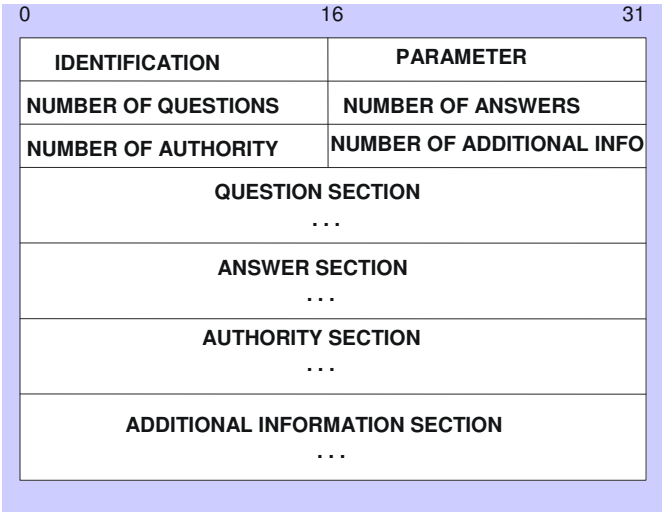
Wenn ein Name-Server für einen bestimmten Hostnamen autoritativ ist, dann enthält der Name-Server einen A-Record für diesen Hostnamen.

Format der DNS-Einträge (resource records) (3)

Das Feld ***Class*** wurde eingeführt, um auch anderen Netzen als dem Internet die Möglichkeit zur Nutzung des DNS zu geben. Für das Internet ist class=IN.

TTL (Time To Live) ist die Lebenszeit eines Eintrags; sie bestimmt die Zeit, nach deren Ablauf der Eintrag aus einem Cache eines anderen Rechners entfernt werden soll.

Die Protokolldateneinheit des DNS



Format von DNS-Nachrichten (1)

- Die ersten 12 Bytes bilden den **Header**. Das erste Feld ist eine 16-Bit-Nummer, die die Anfrage identifiziert. Dieser **Identifizierer** wird in die Antwortnachricht auf eine Anfrage kopiert, so dass der Client ankommende Antworten mit gesendeten Anfragen abstimmen kann. Im **Parameter**-Feld stehen mehrere Flags. Das 1-Bit-Flag *Query/Reply* informiert darüber, ob es sich bei der Nachricht um eine Anfrage (0) oder eine Antwort (1) handelt. Das 1-Bit-Flag *autoritativ* wird in einer Antwortnachricht gesetzt, wenn ein Name-Server der autoritative Server für einen angefragten Namen ist. Das 1-Bit-Flag *Recursion Desired* wird gesetzt, wenn ein Client (Host oder Name-Server) wünscht, dass der Name-Server einer Rekursion ausführt, falls er den gesuchten Eintrag nicht hat. Das 1-Bit-Flag *Recursion Available* wird in einer Antwort gesetzt, wenn der Name-Server Rekursion unterstützt. Ferner enthält der Header vier Felder *Number of* .... Diese Felder bezeichnen die Anzahlen, mit denen die vier Arten von „Daten“-Feldern vorkommen, die dem Header folgen.

Format von DNS-Nachrichten (2)

- Die **Question Section** enthält Informationen über die gestellte Anfrage. Dieser Abschnitt beinhaltet ein Namensfeld, in dem der angefragte Name steht, und ein Typfeld, in dem der Typ des gesuchten Namens angegeben wird (z. B. Typ A für eine Hostadresse).
- In einer Antwort von einem Name-Server enthält die **Answer Section** die Resource-Records des Namens, der ursprünglich angefragt wurde. Eine Antwort kann mehrere RRs umfassen, weil ein Hostname auf mehrere IP-Adressen abgebildet werden kann (z. B. bei replizierten Web-Servern).
- Die **Authority Section** enthält Records anderer autoritativer Server.
- Die **Additional Information Section** enthält weitere „nützliche“ Records. Das Antwort-Feld in einer Antwort auf eine MX-Anfrage enthält z. B. den Hostnamen eines Mail-Servers in Bezug zum Aliasnamen. In diesem Fall steht im Additional-Abschnitt ein A-Record, der die IP-Adresse für den kanonischen Hostnamen des Mail-Servers liefert.

Transportprotokolle im DNS

DNS funktioniert grundsätzlich über TCP oder UDP.

In der Regel wird UDP verwendet, bei Paketverlust erfolgt eine Übertragungswiederholung nach einem Timeout.

TCP wird nur verwendet:

- wenn DNS-Pakete größer als 512 Bytes sind
- beim Initialisieren von “secondary name servers“ durch die Übertragung aller Daten vom “primary name server“.