DNS

TSBE Bern
Höhere Fachschule

Kurzer Rückblick .....

Was versteht man unter DNS

Einsatz

Aufbau

Weiterleitung

Rekursiv / Iterativ

Resolver

Weiterleitung

Da das DNS hierarchisch aufgebaut ist, muss es einen Weg geben, die Verantwortung für weiter unten im Baum befindliche Teile an andere Nameserver weiterzuleiten.

Dies geschieht mittels *Nameserver Records,* die nicht für die ganze Domain, sondern für eine Subdomain gelten.

Ein Nameserver der auch rekursive Fragen anbietet, verwendet die Hintzone, um sich zu den Rootservern durchzufragen.

Hat ein Nameserver nicht die Möglichkeit, direkt mit den Rootservern zu kommunizieren, kann man ihm einen Nameserver vorgeben, mit dem er eine Verbindung eingehen kann und der die Auflösung vornehmen kann.

Weiterleitung

Dieses Verhalten wird durch die Anweisung „forwarders“ gesteuert. Sie enthält eine Liste von IP-Adressen, an welche die Anfragen gestellt werden können. Beispiel:

```
forwarders {
    174.186.1.24;
    174.186.1.25;
};
```

Falls keine Antwort zu erhalten ist, wird doch noch über die Rootserver direkt gefragt.

Ist dies aus irgend welchen Gründen nicht möglich, muss die Abfrage mit „*forwarders only;*“ unterbunden werden.

Die Suche

Bei der Frage an einen Nameserver gibt es ein Bit, das angibt, ob die Suche rekursiv sein soll.

Ist dieses Bit gesetzt und der Nameserver unterstützt dies, kümmert sich der befragte Server darum, eine Antwort von den Nameservern weiter oben im Baum zu erhalten.

Aus Sicht des Fragenden ist dies die einfachere Variante, da er sich nicht um die Auswahl des zuständigen Nameservers kümmern muss, sondern diese Aufgabe weiterdelegiert.

Schliesslich wird es einen Nameserver geben, der die Anfrage mit der nicht-rekursiven Methode abarbeitet.

Bei iterativen Anfragen gestaltet sich das Ganze komplizierter. Der Client fragt zunächst den ihm vorgelagerten Nameserver.

Dieser liefert aber nicht selbst die Antwort, sondern liefert lediglich einen Verweis auf einen Nameserver, der weiterhelfen kann.

Redundanz und Zonentransfers

Damit die Secondaries erkennen, ob sich etwas geändert hat, gibt es im SOA-Record der Domain ein Feld mit der *Serial Number.*
Diese soll jedesmal nach oben gezählt werden, wenn sich in der Zone etwas ändert.

Die Secondaries fragen in regelmässigen Abständen diesen Record vom Master ab.

Wenn sich die Serial Number erhöht hat, wird die Zone kopiert.

Andernfalls betrachtet der Secondary die Zone weiterhin als gültig.

Wie häufig die Secondaries den Primary befragen und wie lange sie die Daten für gültig halten, wird über weitere Parameter im SOA-Record der Zone gesteuert.

DNS

Ein NS-RR (**Name Server Resource Record**) ist ein Datensatz eines DNS Servers und kann zwei unterschiedliche Funktionen erfüllen:

- Er definiert, welche Nameserver für diese Zone offiziell zuständig sind, oder
- er verkettet Zonen zu einem Zonen-Baum (Delegation).

Ein NS-RR hat folgende Elemente:

Domäne → *für welche der Eintrag ist*
TTL → *gibt in Sekunden an, wie lange dieser RR in einem Cache gültig sein darf*
Protokoll → *IN*
Dienst → *NS (Name Service)*
Server → *Name des für diese Domäne autoritativen Nameservers*

Beispiel:

```
@     1800   IN   NS   names1.tsbe.ch.
@     1800   IN   NS   names2.tsbe.ch.
```

TSBE Bern
Höhere Fachschule

A-Record

Name → *veröffentlichter Name*

IN → ***class**: Internet*

A → *Record Type*

Adresse → *die IP-Adresse, unter der der gesuchte Server erreichbar ist*

Beispel:

```
hosta   3600  IN  A  172.27.171.106
```

TSBE Bern
Höhere Fachschule

E-Mail

Um einen zuständigen Mailserver zu finden, prüft der Sender zunächst, ob für die Zieldomain MX-Records existieren.

Ist dies der Fall, so sortiert er die Liste der MX-Records nach den Präferenzwerten (der kleinste zuerst) und probiert die gefundenen Server der Reihe nach durch.

Findet der Sender keine MX-RRs, sucht er nach A-Records, und wenn wenn er dabei erfolgreich war, versucht er, die E-Mail direkt an diese Adresse zuzustellen.

MX-RRs befinden sich üblicherweise am Anfang der Domain.

MX-Record

IN → ***class**: Internet*

Prio → *Priorität, kleine Zahl, hohe Priorität*

MX → *Record Type*

Adresse → *die Mail-Adresse*

Beispiel:

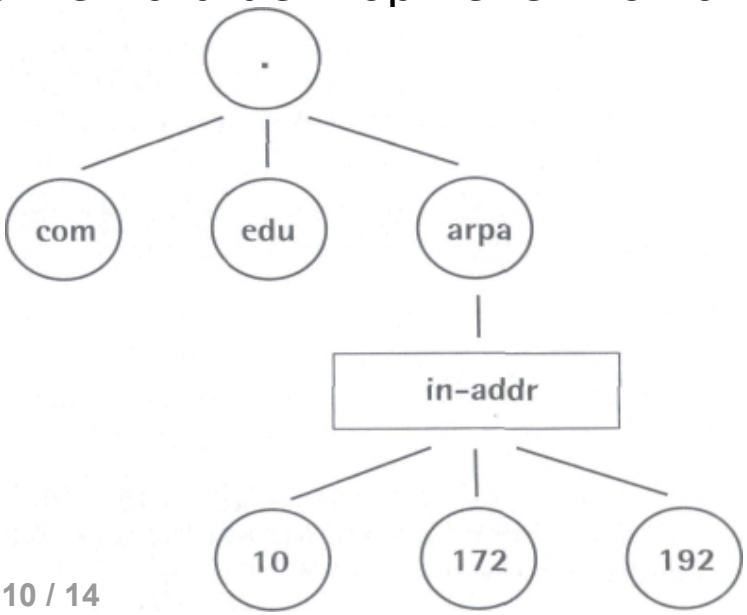
```
@       IN MX 10 mailhostl.example.com
@       IN MX 25 mailhost2.example.com
```

Reverse Auflösung

Bei einer DNS Anfrage wird normalerweise einem Namen „tsbe.ch“ eine IP-Adresse zugeordnet.
Ist ausnahmsweise aber nur die IP-Adresse bekannt und wird der Name gesucht, muss einer IP-Adresse ein Name zugeordnet werden. Diese Auflösung wird als Reverse DNS lookup bezeichnet.
Dazu wird eine eigenständige Domäne gebildet, die

in-addr.arpa

Domäne. Dazu wurde unterhalb der Top-Level Domain eine Domain .arpa eingeführt.



Reverse Auflösung

Aus zeitlichen Gründen, da es unmöglich ist bei einer inversen Anfrage den gesamten Baum zu durchsuchen, ist der PTR-Record eingeführt worden.

Dabei ist zu beachten, dass solche IP-Adressen in umgekehrter Reihenfolge geschrieben werden. Eine Adresse von 192.168.10.5 würde somit im PTR Record zu 5.10.168.192.in-addr.arpa

PTR Record

5.10.168.192.in-addr.arpa. 1800 IN PTR tsbe1.beispiel.ch

Dieser Eintrag entspricht dem A-Record

tsbe1.beispiel.ch. 1800 IN A 192.168.10.5

Host-Informationen

In den Anfangszeiten des Internet war das Netz eine „freundliche" Zone. Es ging darum, die damals teuren Grossrechner-Ressourcen gemeinsam zu nutzen.

Um kenntlich zu machen, welche Sorte von Rechner sich hinter einem Hostnamen verbirg und welche Dienste man auf diesem nutzen kann, wurden zwei RRs eingeführt, die diese Daten ebenfalls über das DNS bereitstellten.

In der heutigen Zeit sprechen Sicherheitsbedenken dagegen, diese Informationen öffentlich bereitszustellen, da sie es Angreifern leichter gezielte Angriffe gegen bestimmte Betriebssysteme oder Dienste zu starten.

In einem LAN kann es aber sinnvoll sein (etwa zur internen Verwaltung), die Informationen bereitzustellen.

Host-Informationen

Die zwei hierfür definierten RRs sind der Hostinfo-Record (HINFD) und der „Well known Services" (WKS).

Ein HINFD-RR enthält laut RFC Prozessortyp und Betriebssystem als zwei Strings.

Beispiel:

```
linserver    IN      A       192.168.1.6
              IN     HINFO   "PC-Pentium4-2GB" "Gentoo-Linux-2-6-17-r7"

winserver    IN      A       192.168.1.5
             IN      HINFO    "PC-Pentium4-lGB" "Windows2000-Buildl234"

Mac          IN      A       192.168.1.7
             IN      HINFO    "MAC-PPC5-2GB" "MACOSX-10-4-8" .
```

Spam und DNS

Ein Grossteil des Spams wird aus sogenannten Botnetzen versendet. Dabei handelt es sich um durch Viren gekaperte PCs, deren private Internetverbindungen missbraucht werden, um Spam (oder Viren) zu versenden.
Diese PCs haben häufig eine fehlende Reverse- oder Vorwärtsauflösung oder Vorwärts- und Reverseauflösung passen nicht zueinander.

Ein Mailserver, der eine eingehende Verbindung verarbeitet, kann also prüfen, ob es zur eingehenden IP-Adresse einen Hostnamen im DNS gibt und ob dieser Hostname sich auch wieder zur eingehenden IP-Adresse auflösen lässt. Passen die beiden nicht zueinander oder fehlt eine der Angaben, dann kann man den Mailserver so konfigurieren, dass er die SMTP-Verbindung ablehnt.

Werden gültige Mailserver verwendet, so kann man diese sperren, bis die Administratoren das Spam-Problem auf dem eigenen Server bereinigt haben.