LANDESBERUFSSCHULE 4 SALZBURG

Informatik

DNS

Domain Name Server

LBS 4

Dieses Skript dient als zusätzliche Lernunterlage für Informatik

Inhalt

Einleitung

Normalerweise wird ein Zielrechner mittels seines Hostnamens angesprochen. Die Zuordnung von IP-Adressen und Hostnamen – was man auch als Namensauflösung bezeichnet – kann lokal über die Konfigurationsdatei hosts erfolgen. Für Netze mit nur wenigen Rechnern mag dies ausreichend sein. Für größere Netze und im Internet ist aber ein Domain Name System (DNS) nötig. DNS ist ein offenes, sowie ein verteiltes Informationssystem. Maßgebliche Ergänzungen erhielt DNS für die Sicherheitserhöhung (DNSSEC), die Möglichkeit dynamischer Updates (DYNDNS) und die Unterstützung von IPv6.

Aus der Sicht eines Anwenders (Resolvers) geht es in der Regel darum, die IP-Adresse eines Rechners aufgrund seines Hostnamen zu ermitteln. Innerhalb des DNS-Systems findet dieser Hostname seine Entsprechung im „Full Qualified Domain Name“ (FQDN), und beim DNS-Server wird dieser Name als zonenspezifischer CName hinterlegt.

Eigenschaften

- löst Domain-Namen in IP-Adressen auf
- hierarchischer Verzeichnisdienst
- ist auf vielen Servern verteilt
- dezentrale Verwaltung, Aufteilung in Zonen
- hierarchische Strukturierung des Namenraums
- Eindeutigkeit der Namen
- typischerweise UDP und Port 53
- in 13 Zonen aufgebaut
    - eine in Europa

IPv4-Adressen 123.12.34.56 sind noch relativ einfach zu merken. Bei IPv6 2001:200:1:8ac2:203:47ff:fea2:123 ist das schon sehr schwierig.

Namensraum

Die DNS-Namen werden von rechts nach links gelesen und ist in mehrere Teile unterteilt.

Top-Level-Domain (TLD):

steht an erster Stelle und war ursprünglich geografisch (at, de, ch,…) und organisatorisch (com, org, net, ..) eingeteilt. Jetzt gibt es zwei Gruppen, allgemeine TLD‘s und länderspezifische TLD’s. Mittlerweile gibt es über 1500 verschiedene TLD-Namen. Verwaltet werden die TLD‘s von der Internet Assigned Numbers Authority (IANA). Jedes Land hat das Recht seine eigene TLD zu verwalten.

Second-Level-Domain (SLD):

Diese kann beliebig, aber eindeutig unter jeder TLD vergeben werden. In Österreich ist dafür die NIC.at (Network Information Center) zuständig.

Sub-Level-Domain:

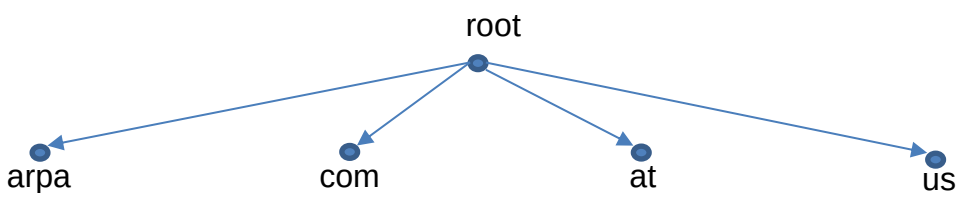
Diese kann vom Verwalter der SLD vergeben werden und muss in Bezug auf die SLD eindeutig sein.

Der Aufbau eines Domainnamens kann so wie nachstehend angeführt ist interpretiert werden.

http://www.lbs4.salzburg.at/hauptmenue/schule.html

http://	→ Protokoll
www	→ Serverbezeichnung gehört zum Server
lbs4	→ Subdomain
salzburg	→ Second-Level-Domain
at	→ Top-Level-Domain
/hauptmenue	→ Verzeichnispfad
/schule.html	→ Datei

Der Namensraum ist Baumförmig aufgeteilt. Root liegt an oberster Stelle.



Namensauflösung

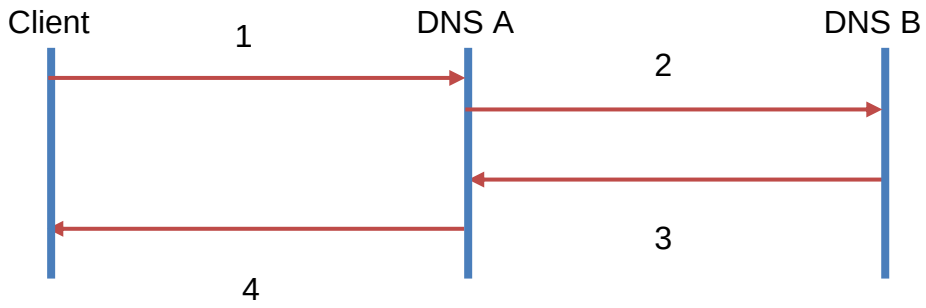
Die Root-Nameserver haben eine zentrale Rolle in der Namensauflösung. Sie besitzen eine gemeinsame, konsistente Datenbank über Informationen der einzelnen TLD-Nameserver. Für jeden beliebigen Domain-Namen kann der Rootserver zumindest auf den TLD-Server verweisen. Diese verfügen über eine Datenbank von SLD-Nameservern.

Resolver

Ist die Schnittstelle zwischen Anwendung und Namensserver. Der Resolver übermittelt die Anfrage an den zugeordneten DNS-Server. Dieser kann rekursiv (Client) oder iterativ (Nameserver) sein.

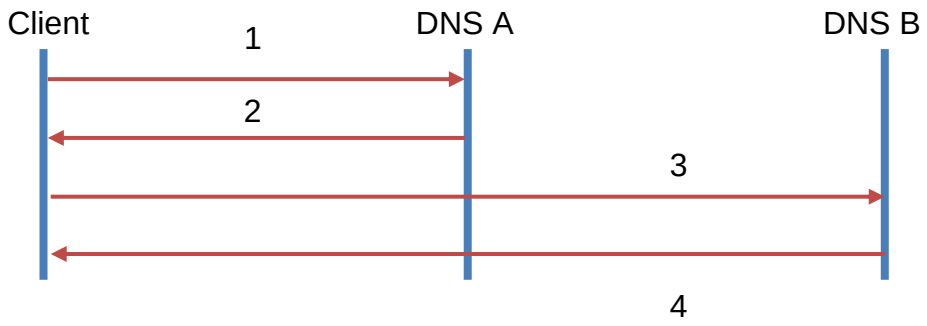
Rekursiv:

Client sendet deinen REQUEST an den DNS-A (1), wenn dieser den Eintrag nicht findet wird ein übergeordneter DNS-B (2) kontaktiert. Der übergeordnete Server sendet das Ergebnis an den DNS-A (3) und dieser liefert das Ergebnis an den Client aus (4).



Iterativ:

Der Client sendet einen REQUEST an den DNS-A (1), wenn dieser den Eintrag nicht auflösen kann, sendet DNS-A die Serveradresse für DNS_B an den Client. Der Client kontaktiert den DNS-B und dieser übermittelt die Antwort an den Client.



Aufbau DNS-Server

DNS-Server sind Rechner die auf Basis einer sehr großen, verteilten Datenbank arbeiten. Es gibt autorative- und nicht autorative Nameserver. Ein autorativer Server gibt Antworten aus seiner verwalteten Zone. Für jede Zone gibt es mind. einen autorativen DNS auf dem die Informationen gesichert liegen. Zonendateien sind sehr oft zusätzlich auf den Sekundär Servern abgelegt (Lastverteilung -> anycast).

DYN-DNS

Wenn keine eigene statische öffentliche IP-Adresse zur Verfügung steht kann ein dynamischer DNS verwendet werden. Dieser synchronisiert die eigene IP-Adresse mit einer statischen öffentlichen IP-Adresse. Für die Synchronisation wird ein Client verwendet, welcher die IP-Adresse übermittelt.

Domain Name System Security Extensions DNSSEC

DNSSEC sieht eine Reihe von Sicherheitsmechanismen zur Gewährleistung der Authentizität (Echtheit, Zuverlässigkeit) zur Erweiterung vor. DNSSEC verwendet ein asymmetrisches Verschlüsselungssytem. Das sieht einen privaten- und einen öffentlichen Schlüssel vor.

DNS kommuniziert noch immer unverschlüsselt über UDP. Somit besteht die Möglichkeit der Manipulation der Anfrage (spoofing, cache-poisoning). Die Extensions sichern die Übertragung der Ressource-Records, Authentifizierung von Servern oder Clients wird nicht unterstützt.

https://www.heise.de/security/meldung/Kommentar-zu-DNS-over-HTTPS-Die-Gruft-DNS-gehoert-ausgelueftet-4203225.html