Domain Name System

Uit Wikipedia, de vrije encyclopedie

Het **Domain Name System (DNS)** is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. Hoewel dit "vertalen" genoemd wordt gaat het gewoon om opzoeken in tabellen, waarin namen aan nummers gekoppeld zijn.

DNS is een client-serversysteem: een opvrager (*client*) gebruikt het DNS-protocol om aan een aanbieder (DNS-*server*) een naam of adres op te vragen, waarop de server een antwoord terugstuurt. Het opzoeken van een nummer bij een naam wordt *lookup* genoemd; het opzoeken van een naam bij een nummer *reverse lookup*.

De naamgeving is hiërarchisch opgezet: namen bevatten punten, en organisatorische eenheden corresponderen met onderdelen van de naam. Zo'n eenheid wordt een *domein* genoemd, en een naam een *domeinnaam'*. Zo is bijvoorbeeld de Nederlandstalige Wikipedia te vinden op de domeinnaam `nl.wikipedia.org`, die (op het moment van schrijven) correspondeert met het IP-adres `91.198.174.232`. Deze naam is onderdeel van het domein `wikipedia.org`, waarvan de domeinnamen door de organisatie van Wikipedia worden beheerd.

DNS wordt ook gebruikt in het SMTP-protocol om de mailservers voor een domein op te zoeken, de computers die de e-mail ontvangen die aan de desbetreffende organisatie geadresseerd is. Daarnaast is er een protocol, het Sender Policy Framework (SPF), waarmee van een e-mail versturende computer via DNS kan worden opgezocht of die daartoe volgens zijn organisatie het recht heeft. Dit is één van de instrumenten die zijn ingezet ter bestrijding van wereldwijde spam.

Inhoud

Geschiedenis

Elke computer die met het internet verbonden is moet een IP-adres hebben om van op afstand bereikbaar te zijn; zo'n computer wordt een *host* genoemd omdat hij fungeert als gastheer voor de gebruiker die er op afstand gebruik van maakt. Omdat zulke nummers voor mensen moeilijk te onthouden zijn, kreeg daarnaast elke computer een naam toegekend, en werd in de software die internetverbindingen maakt ingebouwd dat zulke namen gebruikt konden worden door hun nummer op te zoeken in een tabel.

Deze tabel was aanvankelijk een bestand, `/etc/hosts` (soms `hosts.txt` genoemd), dat op elke aan Internetverkeer deelnemende computer aanwezig moest zijn.

Naarmate het aantal en de omvang van de deelnemende netwerken groeide werd het actueel houden van dat bestand op elke deelnemende computer ondoenlijk. Daarom werd het DNS-protocol ontworpen, zodat deze informatie zelf over het Internet kon worden opgevraagd. Daardoor kan een organisatie de toewijzing van nummers aan namen altijd aanpassen zonder dat voor het doorvoeren van die wijziging bij anderen expliciete acties nodig zijn.

Alle software die Internetverbindingen gebruikt ondersteunt DNS, maar ook nog steeds het `hosts`-bestand. Soms wordt dit laatste bestand nog gebruikt om -bijvoorbeeld- lokale computers een makkelijke naam te geven of om tijdelijk voor een specifieke host het DNS systeem te negeren - soms handig bij het testen van een nieuwe website die nu nog een andere URL heeft of lokaal draait. Een 2e toepassing is het opnemen van een lijst van domeinnamen die als ongewenst zijn geklasseerd en in het hosts bestand een verwijzing naar een ander adres (dan een DNS-server) heeft, zoals naar 127.0.0.1. Anti-misbruikproducten zoals Spybot Search & Destroy maken hier ook gebruik van.

Basistechniek

DNS in praktische implementaties bestaat uit drie onderdelen:

- De *stub resolver*
- De *caching/recursing resolver* (ook wel *recursor* genoemd)
- De *authoritative nameserver*

Het opzoeken van data met behulp van DNS wordt in de regel een *lookup* genoemd. Software, zoals een webbrowser, die een lookup wil doen vraagt dit aan de *stub resolver*. Dit is relatief simpele software die, afhankelijk van de configuratie, de vraag kan stellen aan een *recursor* of eerst kan kijken in een bestand (zoals het onder o.a. Unix-afgeleiden bekende `/etc/hosts`).

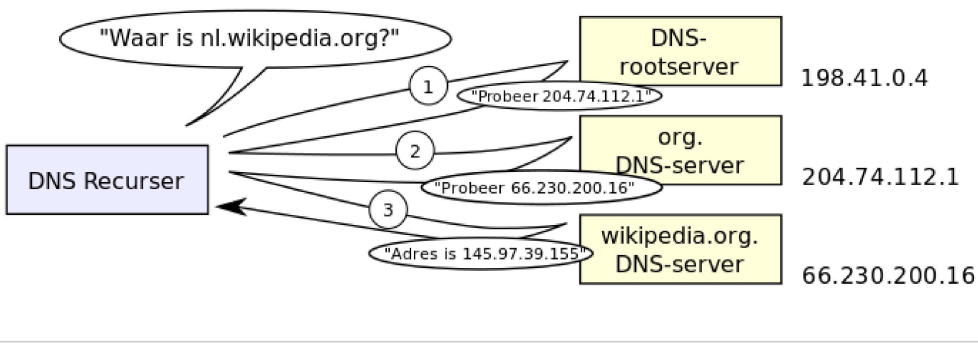
De *stub resolver* stelt een DNS-pakket samen en stuurt dit naar de *recursor*. Vaak levert de internetprovider een recursor en wordt deze gebruikt, alhoewel bij netwerken ook regelmatig een interne recursor wordt opgezet. De recursor is geavanceerder dan de stub resolver en zal in eerste instantie beginnen met het stellen van de vraag aan een DNS-rootserver. Deze kan dan doorverwijzen naar andere servers, vanaf waar weer doorverwezen kan worden naar andere servers, etc., totdat uiteindelijk een server bereikt is die het antwoord weet of weet dat de lookup niet mogelijk is. Van dit laatste kan sprake zijn indien de naam niet bestaat of de servers niet reageren. Het proces van het langslopen van verschillende authoritative servers heet recursie.

Bij het opzoeken van een domein wordt begonnen op het hoogste niveau (*root* genaamd) en daarna wordt steeds specifieker gezocht. Bij het zoeken naar een domein wordt meteen aan de DNS-rootserver gevraagd voor bijvoorbeeld `nl.wikipedia.org`. Er is geen tussenstap waarbij alleen om `org` gevraagd wordt. Het is immers theoretisch mogelijk dat de rootserver zelf al het antwoord voor `nl.wikipedia.org` weet. Zo weten rootservers bijvoorbeeld wel het antwoord voor `a.root-servers.net`. In de regel zal door de DNS-rootserver echter wel verwezen worden naar de nameservers voor `org`. Deze zou in het geval van `nl.wikipedia.org` dan verwijzen naar de nameservers voor `wikipedia.org` die vervolgens het antwoord weten.

Deze servers waar de recursor vragen aan kan stellen zijn de *authoritative nameservers*. Deze zijn ook relatief dom en geven simpele antwoorden. Deze antwoorden zijn vaak in bestanden of in een database opgeslagen. Een authoritative nameserver kan een antwoord geven, wat zowel een verwijzing naar een

andere server of een direct antwoord op de vraag kan zijn.

Zowel de recursor als de authoritative nameserver worden vaak DNS-server genoemd. Het is mogelijk om deze beide functies te combineren in één programma. Dit wordt bijvoorbeeld gedaan in BIND, een van de bekendste en meest gebruikte DNS-servers. Er bestaan ook programma's die slechts een van beide functies vervullen.



Vereenvoudigde weergave van recursie bij het resolven van `nl.wikipedia.org`

NSD is een voorbeeld van een puur authoritative nameserver. Bij programma's die beide functies combineren, is het vaak mogelijk om een van beide uit te schakelen of alleen open te stellen voor het interne netwerk.

Caching

Om te voorkomen dat recursors zeer regelmatig overbodige query's doen (DNS-data verandert relatief weinig) hoort een recursor *caching* te implementeren. Dit wil zeggen dat een eenmaal ontvangen antwoord enige tijd bewaard wordt. Deze tijd kan de beheerder per record aanpassen en wordt Time to live (TTL) genoemd. In de regel ligt deze tussen enkele minuten en enkele dagen.

Redundantie

In de regel zijn er meerdere authoritative servers voor dezelfde data. Dit om de mogelijke gevolgen van het uitvallen van een server te beperken.

In principe moet een recursor, als geconstateerd wordt dat een bepaalde authoritative server niet werkt, alle andere proberen. Uiteindelijk zal er een gevonden worden die wel werkt, of kan de recursor concluderen dat het niet mogelijk is om de naam te vertalen.

DNSSEC

Het DNS-protocol is kwetsbaar voor misbruik. Onder meer door middel van zogenaamde 'DNS cache pollution'-aanvallen (zoals de 'Kaminsky Aanval'), is het DNS om de tuin te leiden. Als gevolg hiervan kunnen argeloze gebruikers bijvoorbeeld naar een valse, malafide website worden gestuurd. In antwoord op deze bedreiging is een uitbreiding op het DNS protocol ontwikkeld: de 'Domain Name System Security Extensions', kortweg DNSSEC. Met behulp van deze internet-standaard zijn DNS-antwoorden cryptografisch te beveiligen, zodat ze niet meer kunnen worden vervalst. Dit gebeurt op basis van zogenaamde digitale handtekeningen, die met een private sleutel worden gegenereerd en met behulp van een publieke sleutel kunnen worden gevalideerd. Van DNS-antwoorden is zodoende de integriteit en authenticiteit gegarandeerd (ook als dit een ontkennend, of leeg antwoord is). Het is echter een misverstand om te veronderstellen dat DNSSEC het DNS-verkeer ook beschermt tegen afluisteren.

Resource records

Data in DNS wordt opgeslagen in een *Resource Record*. Een resource record bevat een type, een TTL, een naam en data. De data kan bijvoorbeeld een IP-adres zijn of een andere naam. Dit is afhankelijk van het type van het resource record.

Veel voorkomende types zijn:

- `SOA` Start-Of-Authority, met instellingen voor het (sub)domein, zoals TTL (Time-To-Live), serienummer, primaire server, responsible person
- `A` voor het bepalen van het IPv4-adres bij een naam
- `AAAA` voor het bepalen van het IPv6-adres bij een naam
- `CNAME` Canonical name voor het configureren van alias van een A of AAAA record
- `PTR` voor het bepalen van een naam bij een IPv4- of IPv6-adres (zie verder bij *Omgekeerde lookups*)
- `MX` voor het bepalen van de mailservers voor een domein, waarbij elke mailserver een eigen prioriteit toegewezen krijgt
- `NS` voor het aangeven welke nameservers de authoritative nameservers zijn (ook gebruikt voor het verwijzen naar andere nameservers)
- `TXT` aanvankelijk gebruikt voor ieder door de gebruiker gewenst commentaar. Nu mede in gebruik door het SPF anti-spam initiatief.
- `SRV` een relatief nieuw record dat gebruikt wordt om services aan te duiden.
- `DKIM` een relatief nieuw record dat word gebruikt om de authenticiteit van e-mail te kunnen valideren. Grote partijen zoals Gmail maken inmiddels van deze 'DomainKeys Identified Mail (DKIM)' gebruik.

Omgekeerde lookups

Omgekeerde of "reverse" lookups kunnen dienen om te weten te komen welke naam bij een IP-adres hoort. Voor het bepalen van de naam bij een IPv4- of IPv6-adres heeft DNS een op het eerste gezicht ingewikkelde constructie. Voor het bepalen van een naam bij een IPv4-adres, moet men de juiste naam opvragen die zich bevindt onder `in-addr.arpa`.

Voorbeeld: `1.2.3.4` wordt vertaald naar `4.3.2.1.in-addr.arpa`. En `52.61.63.53` wordt vertaald naar `53.63.61.52.in-addr.arpa`. Voor deze naam (deze naam is vanuit DNS-perspectief niet veel anders dan een naam als `wikipedia.org`) wordt het PTR-record opgevraagd. Hieruit komt vervolgens de naam behorend bij het IP-adres.

Voor IPv6 is dit vergelijkbaar, maar veel langer en de records bevinden zich in `ip6.arpa`. De reverse van bijvoorbeeld `2001:200:0:8000::42` kan worden verkregen door het opvragen van het PTR-record voor `2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.0.0.0.0.0.2.0.1.0.0.2.ip6.arpa`.

Nameserver tools

Voor het effectief beheer van een nameserver zijn verschillende diagnostische *tools* beschikbaar. De zogeheten BIND-tools zijn de bekendste. Hieronder vallen bijvoorbeeld *nslookup*, *host* en *dig*.

Zie ook

- Second-level-domein en subdomein

Externe links

Enkele DNS-RFC's (er zijn er nog vele andere met aanpassingen en toevoegingen)

- RFC1034 (http://www.ietf.org/rfc/rfc1034.txt): Domain names - concepts and facilities
- RFC1035 (http://www.ietf.org/rfc/rfc1035.txt): Domain names - implementation and specification
- RFC1912 (http://www.ietf.org/rfc/rfc1912.txt): Common DNS Operational and Configuration Errors
- RFC2182 (http://www.ietf.org/rfc/rfc2182.txt): Selection and Operation of Secondary DNS Servers
- RFC4033 (http://www.ietf.org/rfc/rfc4033.txt): DNS Security Introduction and Requirements
- RFC4044 (http://www.ietf.org/rfc/rfc4034.txt): Resource Records for the DNS Security Extensions

Overige links

- Sender Policy Framework (http://www.openspf.org/)

Internetprotocollen volgens het TCP/IP-model	
Toepassingslaag:	**DNS** · FTP · Gopher · HTTP · HTTPS · IMAP · IRC · NNTP · POP3 · RTP · SIP · SMTP · SNMP · SSH · TLS/SSL · Telnet · UUCP · XMPP
Transportlaag:	DCCP · SCTP · TCP · UDP
Netwerklaag:	ARP · ICMP · IGMP · IPv4 · IPv6 · RARP
Datalinklaag:	ATM · Ethernet · FDDI · PPP · Token ring · Wifi

Categorie: Domain Name System
