Domain Name Basics
DNS, DNSSEC, and DANE

Tobias Sattler
tobiassattler.com

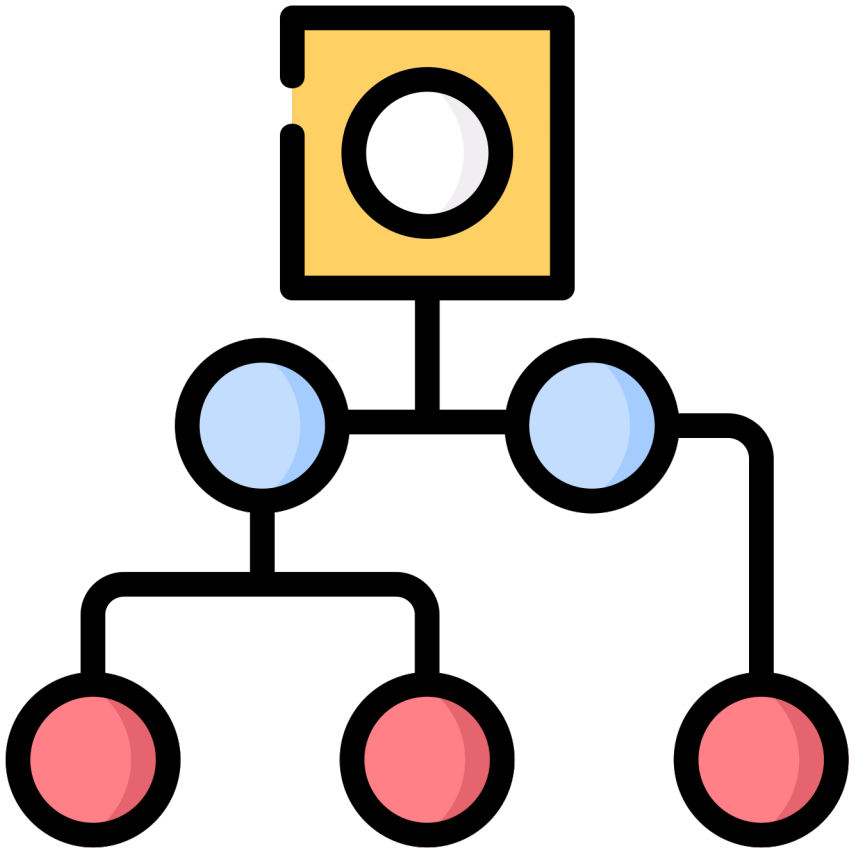
Domain Name System (DNS)

DNS is a hierarchical distributed naming system to **translate domain names** into **IP addresses**, which makes websites easier to remember, such as

- tobiassattler.com instead of 78.46.19.133

The domain namespace is a tree, and its root is a dot.

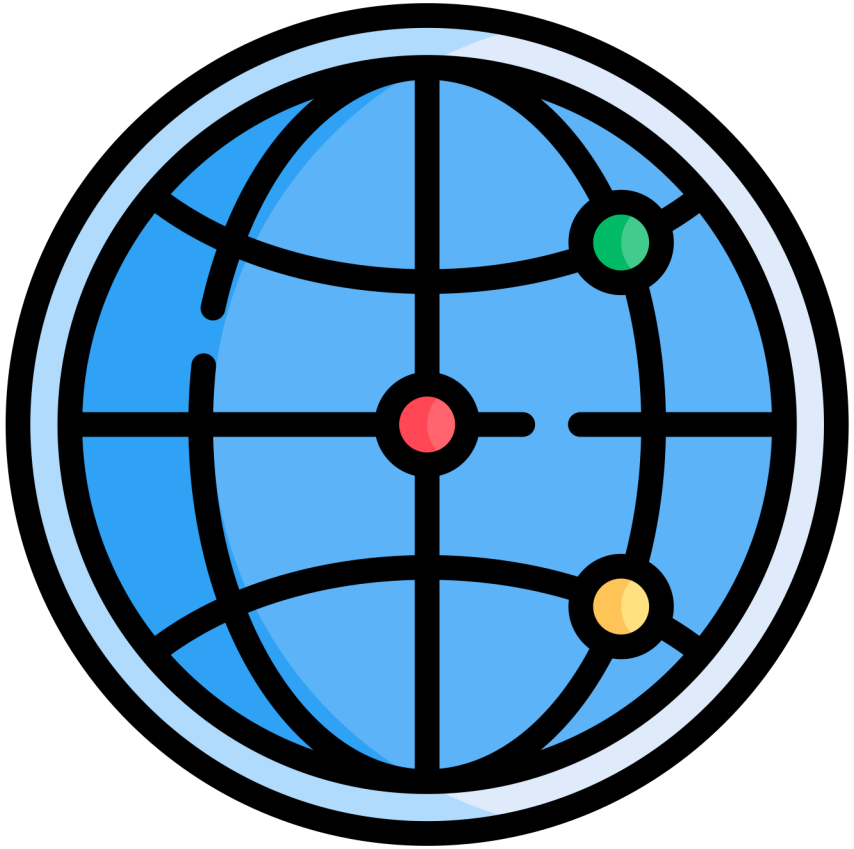
- www.tobiassattler.com.



Root Name Server

For **resolving domain names,** root name servers are needed. There are **13 root name servers**, which are **load-balanced**; therefore, there are more than hundreds of servers **worldwide**.

The root server zone file **contains** all **top-level domains** (.de, .com, .club) and the respectively **IP addresses** of their authoritative name server.



Who is maintaining the DNS?

The Internet Assigned Numbers Authority (**IANA**) and the Internet Corporation for Assigned Names and Numbers (**ICANN**) maintain the root DNS.

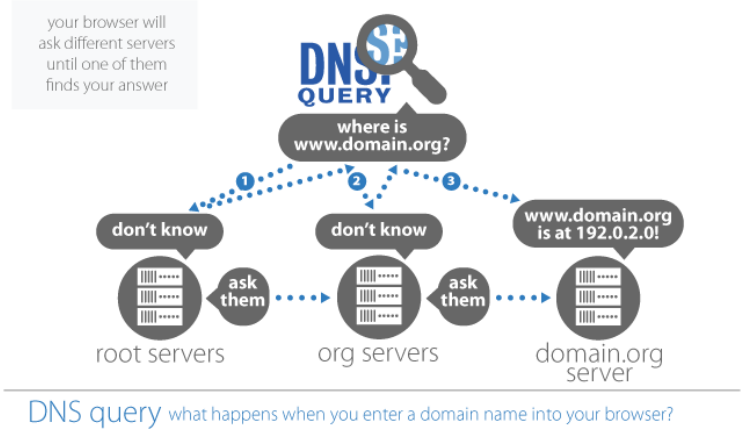
Registries, such as Verisign, donuts, Afilias, etc., maintain the Top-Level domains (TLDs) DNS.

Registrars like GoDaddy, IONOS, united-domains, etc., usually maintain the authoritative domain name servers.

What is a DNS query?

A **DNS query** is the **process** to inquire about the **IP address** for a **name**, such as tobiassattler.com into 78.46.19.133.

Domain name resolvers determine the domain name server responsible for the domain name in question by a sequence of queries starting with the right-most (top-level) domain label.



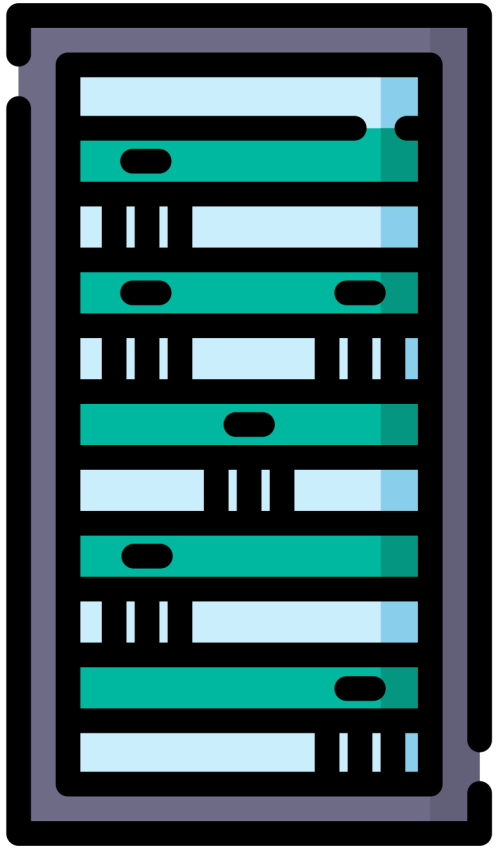
Source: https://whois.icann.org/en/dns-and-whois-how-it-works - Effective 03/2016

Name Servers

A **name server** is a server with **DNS server software** installed on it and **responds** to **queries** to locate the IP address of a web or email server.

Depending on the top-level domain (TLD), a domain name may have zero or more name servers assigned with it.

Usually, a domain name has at least two name servers.

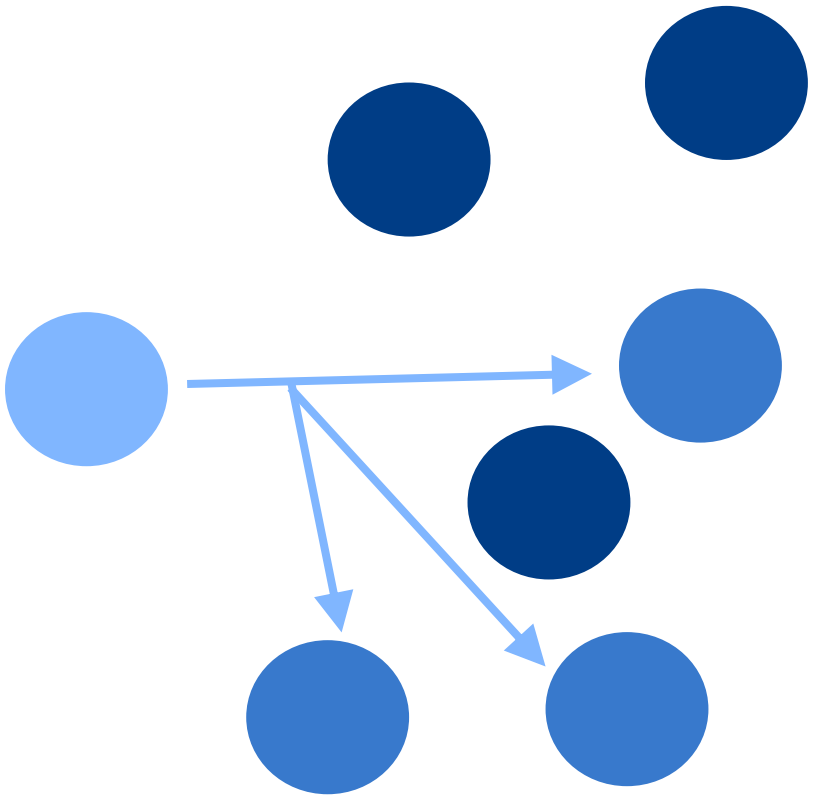


Anycast Name Servers

Anycast is a **network addressing** and **routing** methodology in which one source can ‘talk’ to a service that is advertised or hosted on multiple nodes configured with the same IP address.

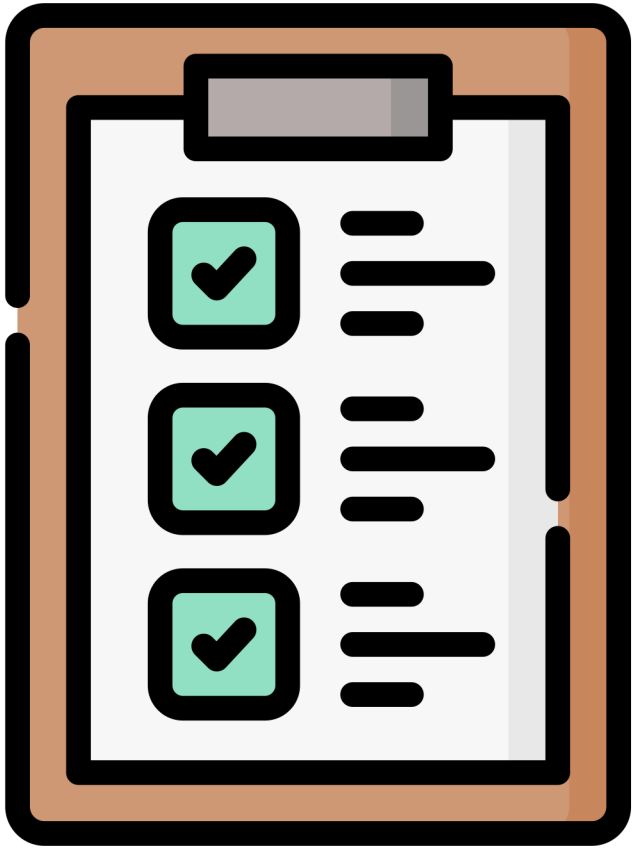
It announces the same IP address **simultaneously** from different servers on the web.

Network routing will route the packets to the ‘**nearest**’ **target** based upon topology.



What are the benefits of Anycast?

- Increased Reliability
- Load Balancing
- Improved Performance
- Enhanced Security
- Localized Impact of DoS Attacks
- Simplified Client Configuration



DNSSEC #1

The original design of the Domain Name System (DNS) did not include security and allowed false DNS data to be returned.

Domain Name System Security Extensions (**DNSSEC**) is a set of **extensions** to **DNS** which provide to DNS clients via a **digital signature** (resolvers) **origin authentication** of DNS **data**.

DNSSEC #2

DNSSEC **doesn't provide confidentiality** of data, and the responses are **authenticated** but not **encrypted**.

By checking the digital signature, a DNS resolver can check if the information is identical to the data published by the zone owner and served on an authoritative DNS server and thereby mitigate, such as 'man-in-the-middle attacks' (see also https://en.wikipedia.org/wiki/Man-in-the-middle_attack).

DANE

DNS-based Authentication of Named Entities (**DANE**) is a protocol to allow certificates (SSL) to be bound to DNS names using DNSSEC to limit security breaches from falsely issued certificates further.

DANE enables the administrator of a domain to **certify** the **keys** used in that domain's TLS clients or servers by storing them in the DNS.

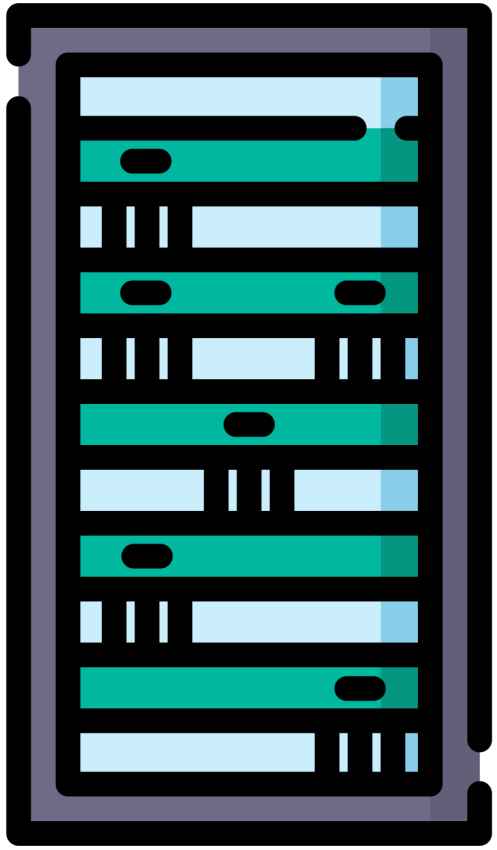
Resource Records #1

There are many DNS Resource Records. This list is an overview of the most commonly used records:

A – Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

AAAA – Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.

CNAME – Redirect to another name: the DNS lookup will continue by retrying the lookup with the new name.



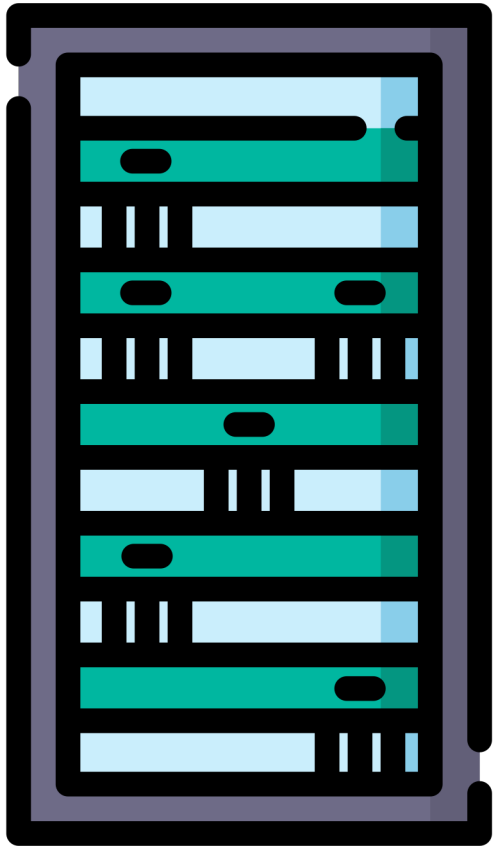
Resource Records #2

DNSKEY – The key record used in DNSSEC.

DS – The record used to identify the DNSSEC signing key of a delegated zone.

MX – Maps a domain name to a list of message transfer agents for that domain. Used for email.

NS – Delegates a DNS zone to use the given authoritative name servers.

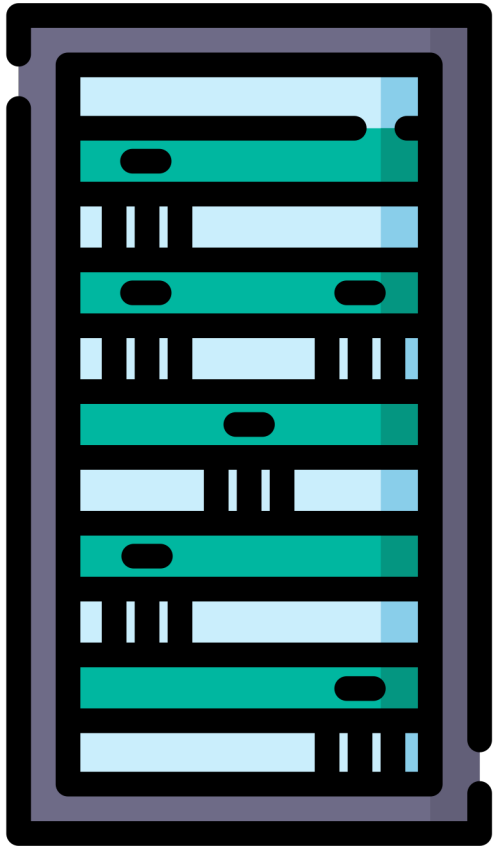


Resource Records #3

PTR – Pointer to a canonical name. Unlike a CNAME, DNS processing stops, and just the name is returned and used for reverse DNS lookups.

RRSIG – Signature for a DNSSEC-secured record set.

SOA – Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the zone serial number, and several timers relating to refreshing the zone.

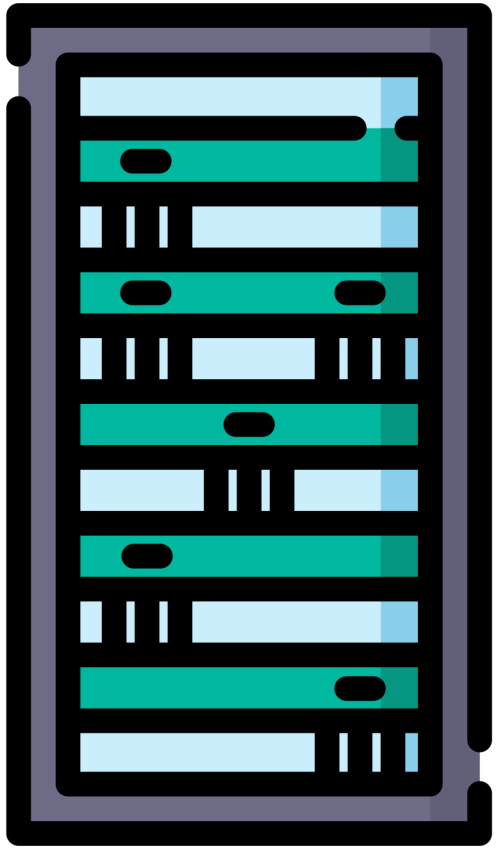


Resource Records #3

SRV – Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX. Commonly used for SIP (VoIP) and XMPP (Jabber / Instant Messenger).

TLSA – A record for DANE. This resource record is used to associate a TLS server certificate or public key with the domain name where the record is found.

TXT – Originally for arbitrary human-readable text in a DNS record. By now, they are usually used for DKIM, DMARC, SPF, etc.



DNS Zone File Example

```
;; QUESTION SECTION:
;tobiassattler.com.             IN      ANY

;; ANSWER SECTION:
tobiassattler.com.      3600    IN      RRSIG   HINFO 13 2 3789 20160823084652 20160821064652 35273 tobiassattler.com. IQqodcX0A5COKaK1tPYytcN+WNqVWGLal6P6ih6YF
egR9M3qmkb/Y9S+ Wq3Ty1bMoUiM+A0V4+j7ZHQW012Llw==
tobiassattler.com.      3600    IN      HINFO   "Please stop asking for ANY" "See draft-ietf-dnsop-refuse-any"
tobiassattler.com.      3600    IN      RRSIG   DNSKEY 13 2 3600 20160910150750 20160712150750 2371 tobiassattler.com. nF88qNPyn7MEmS5F6GjslMbDj17Wn5Km/ANAva+uN
BUXXul5KAnLs290 qXZaVgcLvECeRxslgJ39E83xDf7OBQ==
tobiassattler.com.      3600    IN      DNSKEY  257 3 13 mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+ KkxLbxILfDLUT0rAK9iUzy1L53eKGQ==
tobiassattler.com.      3600    IN      DNSKEY  256 3 13 koPbw9wmYZ7ggcjnQ6ayHyhHaDNMYELKTqT+qRGrZpWSccr/lBcrm10Z 1PuQHB3Azhii+sb0PYFkH1ruxLhe5g==
tobiassattler.com.      3600    IN      RRSIG   DS 8 2 86400 20160829043125 20160822032125 27452 com. eYrDZtZKYM4catcGZkwY78/0OJLmAZCr5+U7ywFSZpCUQsQahhFNHfm/ N
9lbL3OhK8ASk8U2jIxsHpqr2N7o7lBfquhetWsIre6J5G8mL6yyWWcj gLbbYDUelRhprf4vhBZ6PTqXlHNhdoiUdz4qtKRkFhBu3pApYBhx7dR4 mgc=
tobiassattler.com.      3600    IN      DS      2371 13 2 AEC28A9CE09F9D5EA2244D5D4ED4B732F79D0D6E2F2C0048E1C428A1 844A62CB
tobiassattler.com.      3600    IN      NS      kip.ns.cloudflare.com.
tobiassattler.com.      3600    IN      NS      ruth.ns.cloudflare.com.

;; AUTHORITY SECTION:
tobiassattler.com.      3600    IN      NS      ruth.ns.cloudflare.com.
tobiassattler.com.      3600    IN      NS      kip.ns.cloudflare.com.

;; ADDITIONAL SECTION:
kip.ns.cloudflare.com.  3600    IN      A       173.245.59.128
kip.ns.cloudflare.com.  3600    IN      AAAA    2400:cb00:2049:1::adf5:3b80
ruth.ns.cloudflare.com. 1361    IN      A       173.245.58.143
ruth.ns.cloudflare.com. 1361    IN      AAAA    2400:cb00:2049:1::adf5:3a8f
```

Thank you!

Icon made by Freepik from www.flaticon.com