DNS records for webservers

Benedikt Trefzer
benedikt.trefzer@cirrax.com

June 29, 2024

Cirrax GmbH

Table of contents

What is DNS

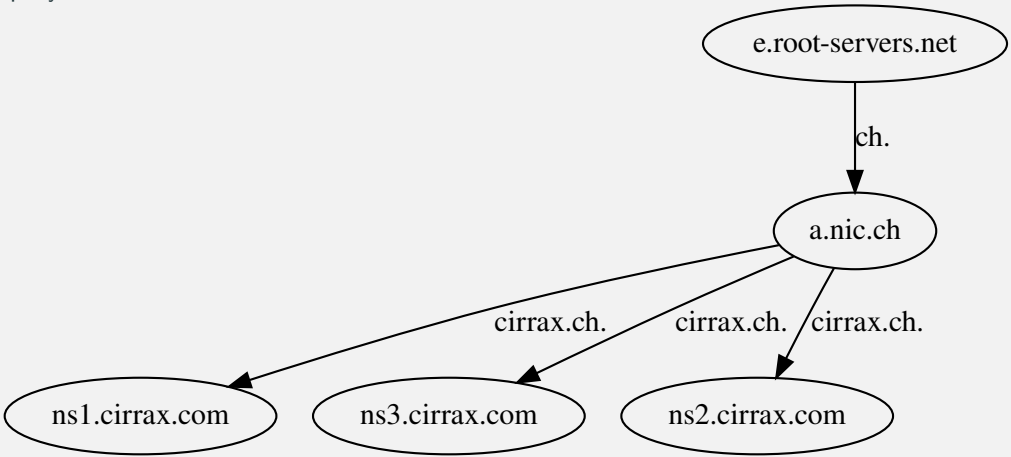
DNS (Domain Name System)

- User view: 'phonebook of the internet'
- Query a name, receive a address
- invented 1983 as a replacement of hosts.txt file maintained by NIC via phone[1]
- RFC1034[2], RFC1035[3] and updates
- DNS is characterized by:
  - decentralized administration
  - hierarchical structure (tree)
  - uniqueness of names
  - extensibility

[1] https://en.wikipedia.org/wiki/Domain_Name_System#History
[2] https://datatracker.ietf.org/doc/html/rfc1034
[3] https://datatracker.ietf.org/doc/html/rfc1035

DNS hierarchy[4]

query: www.cirrax.ch



[4] picture generated by https://www.zonecut.net/dns/, adapted

DNS hierarchy

```
$ dig +trace +nodnssec +nottlid www.cirrax.ch

; <<>> DiG 9.18.24-1-Debian <<>> +trace +nodnssec +nottlid www.cirrax.ch
;; global options: +cmd
.                   IN      NS      a.root-servers.net.
                   .............
.                   IN      NS      m.root-servers.net.
;; Received 239 bytes from 127.0.0.53#53(127.0.0.53) in 0 ms

ch.                 IN      NS      a.nic.ch.
                   .............
ch.                 IN      NS      f.nic.ch.
;; Received 346 bytes from 2001:500:1::53#53(h.root-servers.net) in 24 ms

cirrax.ch.          IN      NS      ns1.cirrax.com.
cirrax.ch.          IN      NS      ns2.cirrax.com.
cirrax.ch.          IN      NS      ns3.cirrax.com.
;; Received 106 bytes from 2001:678:20::39#53(d.nic.ch) in 24 ms

www.cirrax.ch.      IN      A       217.197.128.7
;; Received 58 bytes from 2a03:580:f000::a202:1#53(ns2.cirrax.com) in 20 ms
```

DNS resolver, how we use DNS

DNS: resolver

- do dns queries on behalf of user, use cache
- IP for resolver is usually provided by dhcp in local lan
- on linux `/etc/resolv.conf` configures resolver used[5]
- examples for public resolvers[6]:
  - 8.8.8.8 by Google[7]
  - 9.9.9.9 by Quad9[8]
  - Control D[9]
  - Digitale Gesellschaft[10]
- criteria for your selection:
  - privacy, trust in provider
  - filters used[11]

[5] if systemd-resolv is running, use resolvectl; some programms (eg. firefox) can set resolver independent of system settings

[6] https://en.wikipedia.org/wiki/Public_recursive_name_server

[7] https://developers.google.com/speed/public-dns/

[8] https://www.quad9.net/

[9] https://controld.com/free-dns

[10] https://www.digitale-gesellschaft.ch/dns/

[11] eg. CH Internet providers https://www.esbk.admin.ch/dam/esbk/de/data/illegalesspiel/zugangssperren/sperrliste-dfi.pdf.download.pdf/sperrliste-dfi.pdf

Query dns

- use dig[12]

```
dig www.cirrax.com A @ns1.cirrax.com
```

- use nslookup[13]

```
nslookup -type=A www.cirrax.com ns1.cirrax.com
```

- use a online webpage (not all query types are supported):
  - `https://dnslookup.online`
  - `https://www.nslookup.io`
  - `https://www.zonecut.net/dns` (check nameserver delegations)
  - `https://dnsviz.net` (check dnssec delegations)

[12] https://man.page/dig
[13] https://man.page/nslookup

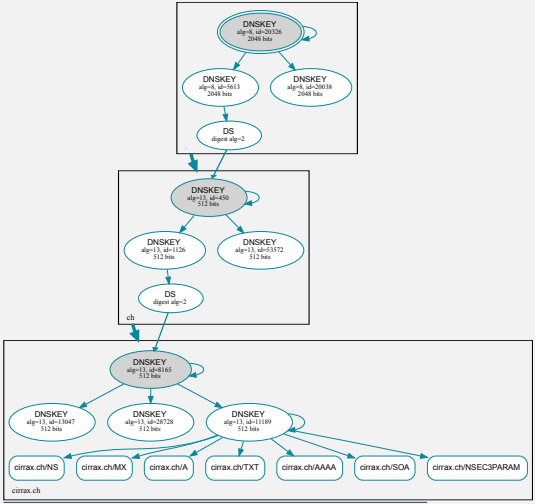
DNSSEC: Domain Name System Security Extension

DNSSEC: Domain Name System Security Extension

- original DNS design without any security features
- DNSSEC attempt to add security (RFC3833[14])
- public key and pre-generated signatures as DNS records, private key for (offline) creation
- ensure answer is identical by checking signature
- authentication chain from root to authoritative nameserver
- NSEC/NSEC3[15] for authentication of absence
- DNSSEC does not provide confidentiality of data (no encryption)[16]
- dnssec prove is the duty of the resolver

[14] https://datatracker.ietf.org/doc/html/rfc3833
[15] https://datatracker.ietf.org/doc/html/rfc5155
[16] use DNS over TLS or DNS over HTTPS

DNSSEC: Chain of trust[17]



[17] picture generated by `https://dnsviz.net`, adopted

DSSEC: Chain of trust

```
$dig +trace +nocrypto www.cirrax.ch
                    .............
ch.                 IN      NS      a.nic.ch.
                    .............
ch.                 IN      NS      f.nic.ch.
ch.                 IN      DS      450 13 2 [omitted]
ch.                 IN      RRSIG   DS 8 1 86400 20240711170000 20240628160000 5613 . [omitted]
;; Received 346 bytes from 2001:500:1::53#53(h.root-servers.net) in 24 ms

cirrax.ch.          IN      NS      ns1.cirrax.com.
cirrax.ch.          IN      NS      ns2.cirrax.com.
cirrax.ch.          IN      NS      ns3.cirrax.com.
cirrax.ch.          IN      DS      8165 13 2 [omitted]
cirrax.ch.          IN      RRSIG   DS 13 2 3600 20240715190652 20240617033002 1126 ch. [omitted]
;; Received 106 bytes from 2001:678:20::39#53(d.nic.ch) in 24 ms

www.cirrax.ch.      IN      RRSIG   A 13 3 86400 20240727213845 20240627213845 11189 cirrax.ch. [omitted]
www.cirrax.ch.      IN      A       217.197.128.7
;; Received 58 bytes from 2a03:580:f000::a202:1#53(ns2.cirrax.com) in 20 ms
```

DNS record types

SOA record

- 'SOA' stands for 'Start Of Authority'
- contains administrative information about zone
- mandatory for each zone

Example:

```
# Format: primary_master  admin_email serial refresh retry expire minimum
cirrax.com.  IN SOA ns1.cirrax.com. admin.cirrax.com. 1719612991 28800 7200 864000 300
```

A records

- 'A' stands for 'address'
- most fundamental type of DNS record
- maps a hostname to an IPv4 address
- defined in RFC 1035[18]

Example:

```
1 www.cirrax.com.          IN A 217.197.128.7
```

[18] https://datatracker.ietf.org/doc/html/rfc1035#page-12

AAAA records

- the 'new' IPv6 fundamental record
- 'AAAA' records also known as 'quad-A' record
- maps a hostname to an IPv6 address
- defined in RFC 3596[19]

Example:

```
1 www.cirrax.com.      IN AAAA 2a03:580:1:1000::7:1
```

[19] https://datatracker.ietf.org/doc/html/rfc3596

PTR records

- Pointer to a canonical (host) name
- used for reverse lookup to find the hostname of an IP address
- defined in RFC 1035[20]
- hint: use `dig -x $IP`

Example:

```
# ipv4
7.128.197.217.in-addr.arpa.                                              IN PTR pweb20.cirrax.com.

# ipv6
1.0.0.0.7.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.0.0.8.5.0.3.0.a.2.ip6.arpa.   IN PTR pweb20.cirrax.com.
```

[20] https://datatracker.ietf.org/doc/html/rfc1035#page-12

CNAME record

- maps a name (record) to another (alias)
- a lookup will continue by retrying the lookup with the new name
- if a CNAME is present for a name no other entry should be present[21],[22]
- a CNAME can point to another CNAME (inefficient but possible)
- a CNAME record cannot be present at the zone apex since a SOA record is needed in that case[23]

Example:

```
1 www.cirrax.net. IN CNAME www.cirrax.com.
```

[21] exception: DNSSEC related records such as RRSIG,NSEC etc. (RFC 1034 section 3.6.2

[22] RFC 1912 section-2.4: https://www.rfc-editor.org/rfc/rfc1912#section-2.4

[23] RFC 1034 section 4.2.1[4] demands a SOA record, section 3.6.2 declares no other records if SOA

DNAME record

- DNAME stands for "Delegation Name"
- provides redirection (alias) for a subtree of the domain
- all queries are redirected to the resulting domain
- defined in RFC 6672[24]

Example:

```
cirrax.ch.      IN DNAME cirrax.com.
```

[24] https://datatracker.ietf.org/doc/html/rfc6672

more DNS record types

TLSA records

- TLSA record with checksum of certificate (RFC 6698[25])
- adds an additional trust path for certificate
- to ensure trust path DNSSEC should be used
- need to trust DNSSEC root certificate
- no known browser support (plugin dnssec-validator.cz EOL 2018)[26]
- record checker for webserver `https://check.sidnlabs.nl/dane/`
- today mostly used for SMTP and XMPP servers

Example:

```
# _port._transport.domain. IN TLSA  usage selector match hash
#    usage:    which certificate in the chain to take
#    selector: which part of the certificate to take
#     match:    hash algorithm

_443._tcp.cirrax.com. IN TLSA  2 0 1 591E9CE6C863D3A079E9FABE1478C7339A26B21269DDE795211361024AE31A44
```

[25] https://datatracker.ietf.org/doc/html/rfc6698

[26] https://www.dnssec-validator.cz/2018-10-16-end-of-support.html

CAA records

- CAA stands for Certification Authority Authorization
- authorized a certificate authority to issue a certificate
- defined in RFC 8659[27] and RFC 8657[28]
- generator for CAA records: `https://sslmate.com/caa/`
- Problem: no guarantee that a CA respects CAA records

Example:

```
1 cirrax.com.     IN CAA 0 issue "letsencrypt.org"           # allow letsencrypt
2 cirrax.com.     IN CAA 0 issuewild ";"                     # no wildcard certs
3 cirrax.com      IN CAA 0 iodef "mailto:support@cirrax.com" # report violation
```

[27] https://datatracker.ietf.org/doc/html/rfc8659
[28] https://datatracker.ietf.org/doc/html/rfc8657

SRV records

- Service record specify a server and port for a service
- defined in RFC 2782[29]
- used for CalDAV, CardDAV, Ceph, Matrix, puppet, STUN, XMPP etc.
- but no support for http/https ;(

Example:

```
# _service._proto.name. IN SRV priority weight port target.

_https._tcp.cirrax.com. IN SRV 0 0 443 www.cirrax.com     # non working example
```

[29] https://datatracker.ietf.org/doc/html/rfc2782

new DNS record types

HTTPS record

- A SRV record for https !
- RFC 9460[30] November 2023: proposed Standard
- Similar to an SRV record but more powerfull
- goal performance: only one dns request for all information
- goal privacy: all information to establish secure connection[31]
- a generic record (SVCB) is specified for other services[32]
- two modes for HTTPS records: AliasMode and ServiceMode

[30] https://datatracker.ietf.org/doc/html/rfc9460/

[31] Encrypted ClientHello (ECH) https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-18

[32] HTTPS record is a subset of SVCB

HTTPS record: AliasMode

- delegates operational control for a resource
- similar to a CNAME alias
- allows aliasing at zone apex (where no CNAME is allowed)
- a HTTPS record directs the client to communicate over secure transport only (similar to HSTS[33])

Example:

```
# set priority to 0 for AliasMode

example.com. IN HTTPS 0 svc.example.net.
```

[33] https://datatracker.ietf.org/doc/html/rfc6797

HTTPS record: ServiceMode

- delegates operational control for a resource
- alpn and no-default-alpn: indicate the Application-Layer Protocol Negotiation (ALPN)[34]
- port: defines the tcp/udp port that should be used[35]
- ipv4hint/ipv6hint: IP addresses that clients may use to reach the service[36]
- ech: Encrypted Client Hello (in specification !)

Example:

```
# set priority to not 0 for ServiceMode

example.com. IN HTTPS 1  . alpn="h3,h2" ipv4hint="192.168.0.1" # main server can h3 and h2 and is on IP 192.168.0.1
example.com. IN HTTPS 10 svc10.example.net. alpn="h2"          # backup server h2 only
```

[34] https://datatracker.ietf.org/doc/html/rfc9460#section-7.1
[35] https://datatracker.ietf.org/doc/html/rfc9460#section-7.2
[36] https://datatracker.ietf.org/doc/html/rfc9460#section-7.3

Conclusion and questions

SVCB Service Binding

- SVCB stands for Service Binding
- defined in RFC9460[37]
- this is the generic HTTPS record
- Similar to an SRV record but more powerfull
- priority 0 sets AliasMode similar to CNAME (but also for zone apex)
- other priorities are ServiceMode, which defines a service to use
- do not know any working use case yet !

[37] https://datatracker.ietf.org/doc/rfc9460