Alex Shah

EN.695.741.81.SP25 Information Assurance Analysis

Mod 9 Assignment

March 30, 2025

Note: I wrote up A, AAAA, CNAME, MX, TXT, and PTR and then realized they were not all “other” DNS record types, so I have also included CAA, DNAME, DNSKEY, and LOC, making the assignment quite long, but I didn’t want to get rid of my existing work.

DNS Resource Records

Each DNS Resource Record type follows a format which typically includes the fields NAME, TYPE, CLASS, time to live (TTL), RDLENGTH, and RDATA.

The NAME field is either the domain, subdomain, or alias domain associated with the record and can be a variable length. The NAME is represented as a sequence of values prefixed by the length of each sequence and terminated by zero as a label sequence format. For example “www.google.com” would be represented as “3www6google3com0”.

The TYPE field defines which resource record type the record is defining and is a 16 bit value which translates into the record type (e.g. A=1, AAAA=28).

The CLASS field is a 16 bit value that usually is “1” for “IN” or Internet. Classes can be used to describe the same NAME for different classes, but mostly are unused. Other values have been used such as 3 and 4 used by MIT in the 80s. And values 254 and 255 for None and All, respectively are used as query classes and a description of the purpose and uses for CLASS can be found in RFC 2929.

TTL are 32 bit values in seconds used for telling a resolver how long to cache a record before querying again. Depending on the record type, the values might be short lived or long lived. For example in A/AAAA records translating domain names to IP addresses, the domain might be short lived for load balancing, or long lived if they are unlikely to change like a static IP.

The RDLENGTH field is a 16 bit value defining the number of bytes long the RDATA is. The RDATA field is a variable length field where the length is defined in the RDLENGTH field, where RDATA holds the data specific to the record type. For example, an A record might have an RDLENGTH of 4 to describe the 4 byte (32 bit) IPv4 address held in RDATA. An AAAA record would have an RDLENGTH of 16 bytes for the 128 bit IPV6 value held in RDATA for that record.

A Record

A records are defined in RFC 1035 to translate a domain name to a 32 bit IPv4 address to connect to, such as google.com to 142.250.65.174. Since people can't memorize the IP addresses of servers they want to connect to, A records help translate human readable domains to server IP addresses. This also enables multiple IP addresses to respond to the same domain name by having multiple A records, which is useful for load balancing and preventing DDoS. An A record also contains a time to live (TTL) in seconds, where the value can be short or long lived. For example, a static IP address would not change so the TTL could be long, but when using load balancing or cloud scaling, a short lived TTL would be better so the cached value doesn't live too long and refer clients to an old record address.

NAME – Domain Name

TYPE – A (1)

CLASS – Usually IN (1)

TTL – Can be short to long lived

RDLENGTH – 4 bytes

RDATA – 32 bit IPv4 address

AAAA Record

Similar to A records, AAAA records translate domain names into IPv6 addresses as defined in RFC 3596. The RDLENGTH for AAAA records is longer, 16 bytes, to hold the 128 bit IPv6 address in the RDATA field. The TTL can also be short or long lived depending on the use case.

NAME – Domain name

TYPE – AAAA (28)

CLASS – IN (1)

TTL – Can be short to long lived, same as A records

RDLENGTH – 16 bytes

RDATA – 128 bit IPv6 address

CNAME

CNAME records describe the canonical name which aliases one domain to another as defined in RFC 1035. For example, a CNAME record would point the alias domain “www.google.com” to the canonical domain name “google.com”. The CNAME record points one domain to another, until an A or

AAAA record can be found which provides an IP address to resolve to. This is used to point one or more subdomains to the same destination without needing multiple A/AAAA records, to point to a CDN, or for routing traffic and balancing load. CNAME records can also point a subdomain to other domains, for example owning the domain “xyz.com” can point a subdomain “media.xyz.com” to different domain “abc.com” by using a CNAME record to avoid using a changing IP address or a messy URL. It can point to an external domain from the one the subdomain is on. The alias and canonical domain names are represented in a prefix labeled sequence terminated by zero like “3www6google3com0”.

NAME – Alias domain name

TYPE – CNAME (5)

CLASS – IN (1)

TTL – Can be longer lived if the domain association is not likely to change

RDLENGTH – The length in bytes of the canonical name in RDATA to follow

RDATA – canonical domain name

MX

MX records are used for mail server applications on a domain, mapping a chosen domain name to the hostname of the mail server on the domain as defined in RFC 1035, and a special case for null MX records defined in RFX 7505 when the domain does not accept mail. The RDATA section of an MX record also includes a preference value, where lower numbers are preferential to accept mail. Multiple hostnames can be provided to accept mail, so the preference value indicates which server to

try first, or the preferences can all be the same which would load balance mail traffic in a round robin fashion.

NAME – Domain name for mail traffic

TYPE – MX (15)

CLASS – IN (1)

TTL – Can be longer lived

RDLENGTH – Length in bytes of RDATA to follow

RDATA – A 16 bit preference value, and a variable length label sequence of the mail server location as a FQDN

PTR

PTR records defined in RFC 1035 are used for reverse DNS lookup as a “pointer” from IP address to a domain/hostname. For example a reverse lookup on “150.0.0.1” would be represented as “1.0.0.150.in-addr.arpa”. The format for the NAME field is a reversed IP address as a FQDN ending in “.arpa” and is represented as a labeled sequence like usual. PTR records are not required and running reverse DNS lookups often don’t lead to a real domain.

NAME – Reversed IP sequence ending in .arpa

TYPE – PTR (12)

CLASS – IN (1)

TTL – Usually long, reverse DNS lookup is not time sensitive and not expected to change if set

RDLENGTH – Length in bytes of RDATA to follow

RDATA – A variable length domain name sequence of the domain pointed to

TXT

TXT is an optional DNS record defined in RFC 1035 for storing strings or notes that are commonly used for verification or authentication, or human readable information. For example, a TXT record can be used to prevent spoofing in some email authentication methods, authorize certificates for a domain, prove you own a domain by having some identifier, provide contact details for a website, and in general provides a blank space for strings and variables in a record associated with a domain.

NAME – Domain name

TYPE – TXT (16)

CLASS – IN (1)

TTL – Usually long lived if the authorizations or information is ongoing, or short lived if its part of some verification process that can be done once

RDLENGTH – Length in bytes of RDATA to follow

RDATA – An arbitrary length field for strings in prefixed by their length up to 255 characters, where multiple strings can be concatenated together

CAA

Certificate Authority Authorization records (CAA) are defined in RFC 8659 which allows a domain holder to specify the Certificate Authorities (CA) authorized to issue certificates to the domain. The RDATA contains a critical flag in the first byte to indicate when a certificate issuer must check if the property tags are correct before issuing. Next is the tag for what to issue, such as “issue” and “issuewild” to issue a certificate for the domain or a wildcard for that domain, or “iodef” to report invalid certificates in Incident Object Description Exchange Format, or “contactemail” and “contactphone” to publish contact information in places with GDPR restrictions on WHOIS. A blank issue tag record can be used to prevent any issuing of certificates for the domain.

NAME – Domain name

TYPE – CAA (257)

CLASS – IN (1)

TTL – Usually long lived since certificate authorization doesn’t usually change

RDLENGTH – Length in bytes of RDATA to follow

RDATA – A critical flag byte, followed by a tag prefixed by a length byte, then value string with the certificate authority or URL prefixed by a length byte

DNAME

Like CNAME, DNAME described in RFC 6672 redirects a given domain to a target domain, except DNAME allows for subdomains within the given domain to be redirected as well, compared to CNAME which requires new records for each subdomain to be redirected.

NAME – Domain name to redirect

TYPE – DNAME (39)

CLASS – IN (1)

TTL – Can be long lived for permanent redirects

RDLENGTH – Length in bytes of RDATA

RDATA – A target domain in label sequence format that will be followed for subdomains in the redirected domain

DNSKEY

DNSKEY defined in RFC 3757 is part of DNSSEC containing records for public keys used to verify signed DNS data. These keys and DNSSEC in general help prevent cache poisoning other DNS attacks. Zone Signing Keys (ZSK) are used to sign records within a managed DNS zone such as a domain and its subdomains, and Key Signing Keys (KSK) are used to sign the DNSKEY record. KSKs are longer and more secure keys used as “more important” keys to sign other keys that might be smaller or rotated more frequently. Using this key scheme helps create a trust chain and isolate risks when zone keys which only apply to a smaller subset of resources in a zone are compromised and need to be changed.

NAME – Domain name (containing zones)

TYPE – DNSKEY (48)

CLASS – IN (1)

TTL – Usually matches a zone's SOA (Start of Authority) record TTL length so keys and zone records are cached for the same amount of time to prevent issues with DNSSEC validation and key rotation. Usually hours to days long

RDLENGTH – Length in bytes for RDATA

RDATA – Contains flags, Secure Entry Point (SEP) flag at bit 15, protocol field, algorithm field, and public key in base64

LOC

LOC records for location information are described in RFC 1876 as an experimental protocol to hold geographic information about hosts, networks, and subnets without needing to provide separate records for multiple hosts nearby. It essentially provides a mechanism to describe a sphere around a center point used to position a server on Earth. This was probably the most interesting RFC to read, and the potential use cases describing visual traceroute and flow maps in 1996 evoke 90s hacker movie imagery. The security considerations section also points out that high precision location information could be used by attackers to plan a physical attack.

NAME – Domain name

TYPE – LOC (29)

CLASS – IN (1)

TTL – Long lived as geo coordinates are unlikely to change

RDLENGTH – Length in bytes for RDATA

RDATA – Contains fields and prefixes to describe the location. First is the version number (0 only currently). Next is the size of the sphere enclosing the point described in centimeters as a pair of 4 bit integers as base and power, for example 0e0 is 1cm, and 9e9 is 90,000 km, and 0e29 is used to express “worldwide”. Next are two fields using the same representation method to describe the total horizontal then vertical precision of the measurements, for example 1000m total precision would mean +/- 500m. Next are two 32 bit integers for the latitude then longitude of the center of the sphere in thousandths of a second arc. Lastly is the altitude as a 32 bit integer in centimeters using a reference spheroid (WGS 84) and caveats about the imperfectness of the earth and sea level values can lead to altitude and vertical precision value differences.

Sources

A – RFC 1035

AAAA – RFC 3596

CNAME – RFC 1035

PTR – RFC 1035

MX – RFC 1035, 7505

TXT – RFC 1035

CAA – RFC 8659

DNAME – RFC 6672

DNSKEY – RFC 3757

LOC – RFC 1876

Davis, C., Vixie, P., Goodwin, T., & Dickinson, I. (1996). A Means for Expressing Location Information in the Domain Name System (RFC 1876). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc1876

Eastlake 3rd, D., & Panitz, A. (2000). Reserved top level DNS names (RFC 2929). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc2929#section-3.2

Hallam-Baker, P., Stradling, R., & Hoffman-Andrews, J. (2019). DNS Certification Authority Authorization (CAA) Resource Record (RFC 8659). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc8659.html

Kolkman, O., Schlyter, J., & Lewis, E. (2004). Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag (RFC 3757). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc3757

Levine, J., & Gellens, R. (2015). A "null MX" no service resource record for domains that accept no mail (RFC 7505). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc7505.html

Mockapetris, P. (1987). Domain names - implementation and specification (RFC 1035). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc1035#page-12

Rose, S., & Wijngaards, W. (2012). DNAME Redirection in the DNS (RFC 6672). Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc6672

Thomson, S., Huitema, C., Ksinant, V., & Souissi, M. (2003). DNS extensions to support IP version 6 (RFC 3596). Internet Engineering Task Force. https://web.archive.org/web/20210414192537/https://tools.ietf.org/html/rfc3596