

# DNS Record

- DNS (Domain Name System) provides a simple way for us to communicate with devices on the internet without remembering complex numbers.
- A DNS record is a database record used to map a URL to an IP address.
- DNS records are stored in DNS servers and work to help users connect their websites to the outside world.
- When the URL is entered and searched in the browser, that URL is forwarded to the DNS servers and then directed to the specific Web server.
- This Web server then serves the queried website outlined in the URL or directs the user to an email server that manages the incoming mail.
- The most common record types are:
  - A record
  - AAAA record
  - CNAME record
  - MX record
  - TXT record
  - TTL record
  - SOA record
  - PTR record
- **A record** -
  - A stand for Address (IPv4 Address).
  - The record that holds the IP address of a domain.
  - Used to map a host name to an IP address. Generally, A records are IP addresses. If a computer consists of multiple IP addresses, adapter cards, or both, it must possess multiple address records.

```
user@thm:~$ nslookup --type=A website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: website.thm
Address: 10.10.10.10
```

- **AAAA record** -
  - AAAA stands for Address (IPv6 Address).
  - The record that contains the IPv6 address for a domain.

- **CNAME record** -

- CNAME stands for Canonical Name.
- Forwards one domain or subdomain to another domain, does NOT provide an IP address.
- Can be used to set an alias for the host name.

```
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com
```

- **MX record** -

- MX stands for Mail Exchange.
- Permits mail to be sent to the right mail servers located in the domain. Other than IP addresses, MX records include fully-qualified domain names.

```
user@thm:~$ nslookup --type=MX website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm mail exchanger = 30 alt4.aspmx.l.google.com
```

- **TXT record** -

- TXT stands for Text.
- Let's an admin store text notes in the record. These records are often used for email security.

```
user@thm:~$ nslookup --type=TXT website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"
```

- **TTL record** -

- TTL stands for Time-to-Live.
- Sets the period of data, which is ideal when a recursive DNS server queries the domain name information

- **SOA record** -

- SOA stands for Start of Authority.
- Stores admin information about a domain.
- Declares the most authoritative host for the zone. Every zone file should include an SOA record, which is generated automatically when the user adds a zone.

- **PTR record** -

- PTR stands for Pointer.
- Provides a domain name in reverse-lookups.
- Creates a pointer, which maps an IP address to the host name in order to do reverse lookups.

**Refernces:**

[DNS Records Explained - Types of DNS Records \(namecheap.com\)](#)

[DNS Records Explained \(ns1.com\)](#)

[DNS records | Cloudflare](#)