NS1.

What is a DNS Zone? DNS Zones Explained

What is a DNS Zone?

A DNS zone is a distinct part of the domain namespace which is delegated to a legal entity—a person, organization or company, who are responsible for maintaining the DNS zone. A DNS zone is also an administrative function, allowing for granular control of DNS components, such as authoritative name servers.

When a web browser or other network device needs to find the IP address for a hostname such as "example.com", it performs a DNS lookup - essentially a DNS zone check - and is taken to the DNS server that manages the DNS zone for that hostname. This server is called the authoritative name server for the domain. The authoritative name server then resolves the DNS lookup by providing the IP address, or other data, for the requested hostname.

DNS Zone Levels

The Domain Name System (DNS) defines a domain namespace, which specifies Top Level Domains (such as ".com"), second-level domains, (such as "acme.com") and lower-level domains, also called subdomains (such as "support.acme.com"). Each of these levels can be a DNS zone.

For example, the root domain "acme.com" may be delegated to a Acme Corporation. Acme assumes responsibility for setting up an authoritative DNS server that holds the correct DNS records for the domain.

At each hierarchical level of the DNS system, there is a Name Server containing a zone file, which holds the trusted, correct DNS records for that zone.

DNS Root Zone

The root of the DNS system, represented by a dot at the end of the domain name—for example, **www.example.com.**—is the primary DNS zone. Since 2016, the root zone is overseen by the Internet Corporation for Assigned Names and Numbers (ICANN), which delegates management to a subsidiary acting as the Internet Assigned Numbers Authority (IANA).

The DNS root zone is operated by 13 logical servers, run by organizations like Verisign, the U.S. Army Research Labs and NASA. Any recursive DNS query (learn more about **DNS query types**) starts by contacting one of these root servers, and requesting details for the next level down the tree—the Top Level Domain (TLD) server.

TLD Zones

There is a DNS zone for each Top Level Domain, such as ".com", ".org" or country codes like ".co.uk". there are currently over 1500 top level domains. Most top level domains are managed by ICANN/IANA.

Domain Zones

Second-level domains like the domain you are viewing now, "ns1.com", are defined as separate DNS zones, operated by individuals or organizations. Organizations can run their own DNS name servers, or delegate management to an external provider.
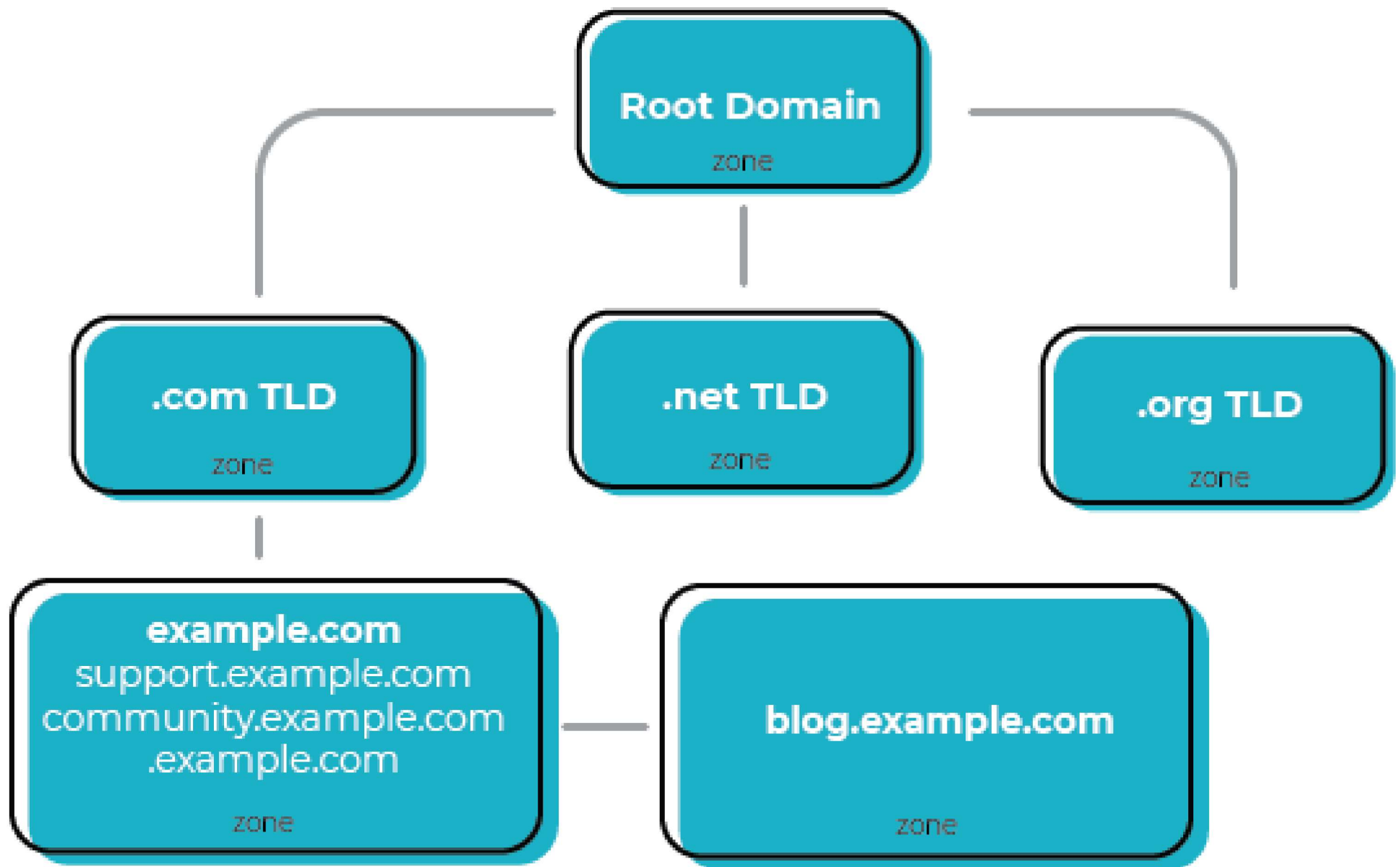
If a domain has subdomains, they can be part of the same zone. Alternatively, if a subdomain is an independent website, and requires separate DNS management, it can be defined as its own DNS zone. In the diagram above, "blog.example.com" was setup as a DNS zone, whereas "support.example.com" is part of the "example.com" DNS zone.

Secondary DNS Zones

DNS servers can be deployed in a primary/secondary topology, where a secondary DNS server holds a read-only copy of the primary DNS server's DNS records. The primary server holds the primary zone file, and the secondary server constitutes an identical **secondary zone**; DNS requests are distributed between primary and secondary servers. A DNS zone transfer occurs when the primary server zone file is copied, in whole or in part, to the secondary DNS server.

All About the DNS Zone File

DNS zone files are defined in <u>RFC 1035</u> and <u>RFC 1034</u>. A zone file contains mappings between domain names, IP addresses and other resources, organized in the form of resource records (RR).

To see the actual zone file for a domain, and test DNS zone transfers, you can perform a zone file lookup using one of many DNS tools.

DNS Zone Types

There are two types of zone files:

- A DNS Primary File which authoritatively describes a zone
- A DNS Cache File which lists the contents of a DNS cache—this is only a copy of the authoritative DNS zone

DNS Zone Records

In a zone file, each line represents a DNS resource record (RR). A record is made up of the following fields:

name	ttl	record class	record type	record data

- **Name** is an alphanumeric identifier of the DNS record. It can be left blank, and inherits its value from the previous record.

- **TTL (time to live)** specifies how long the record should be kept in the local cache of a DNS client. If not specified, the global TTL value at the top of the zone file is used.

- **Record class** indicates the namespace—typically IN, which is the Internet namespace.

- **Record type** is the DNS record type—for example an A record maps a hostname to an IPv4 address, and a CNAME is an alias which points a hostname to another hostname.

- **Record data** has one or more information elements, depending on the record type, separated by a white space. For example an MX record has two elements—a priority and a domain name for an email server.

Zone File Structure

DNS Zone files start with two mandatory records:

- **Global Time to Live (TTL)**, which specifies for how records should be kept in local DNS cache.

- **Start of Authority (SOA) record**—specifies the primary authoritative name server for the DNS Zone.

After these two records, the zone file can contain any number of resource records, which can include:

- **Name Server records (NS)**—specifies that a specific DNS Zone, such as "example.com" is delegated to a specific authoritative name server

- **IPv4 Address Mapping records (A)**—a hostname and its IPv4 address.

- **IPv6 Address records (AAAA)**—a hostname and its IPv6 address.

- **Canonical Name records (CNAME)**—points a hostname to an alias. This is another hostname, which the DNS client is redirected to

- **Mail exchanger record (MX)**—specifies an SMTP email server for the domain.

Zone File Tips

- When adding a record for a hostname, the hostname must end with a period (.)

- Hostnames which do not end with a period are considered relative to the main domain name—for example, when specifying a "www" or "ftp" record, there is no need for a period.

- You can add comments in a zone file by adding a semicolon (;) after a resource record.

DNS Zone File Example

```
$ORIGIN example.com. ; start of the zone file$TTL 30m ; default cache expiration time for resource recordsexample.co
m. IN SOA ns.example.com. root.example.com. ( 1999120701 ; serial number of this zone file1d ; frequency to refresh sec
ondary DNS (d=day)1d ; frequency to refresh secondary DNS in case of problem4w ; secondary DNS expiration time (
w=week)1h ; minimum caching time if resolution failedexample.com. NS dns1.dnsprovider.com. ; there are two name s
erver that can provide DNS services for example.comexample.com. NS dns2.dnsprovider.com.example.com. MX 10 mx
1.dnsprovider.com ; mail serverexample.com. MX 10 mx2.dnsprovider.comexample.com. A 192.168.100.1 ; IP address for r
oot domain www A 192.168.100.1 ; IP address for www subdomain
```

DNS Zones and Next-Generation DNS Services

Traditional DNS infrastructure has its limitations. Once upon a time, an IP address pointed to a single server. Now, one IP address can hide a pool of load balanced network resources, deployed on different data centers across the globe. To serve these resources efficiently to users, ensure high performance and allow quick propagation of changes, you should consider a next generation DNS provide like NS1.
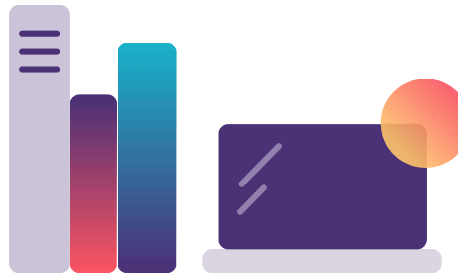
NS1 provides:

- <u>Managed DNS</u> - a DNS service powered by a high performance, anycast global DNS network, with advanced traffic management features.

- <u>Dedicated DNS</u> - fully managed DNS deployment, on premise or in the cloud, with advanced point-and-click traffic management
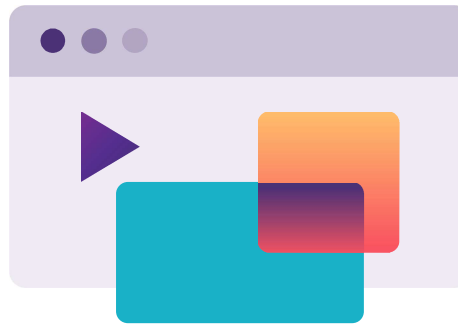
Gain Insight from Our Latest Resources

Learn How it Works with a Demo

Sign Up for Our Newsletter

Email Address

Subscribe

Contact Us

Company

Careers

Support

Help Center

News

Events

[Blog](.)

[Terms of Service](.)

[Privacy Policy](.)

[Responsible Disclosure](.)