DNS can be hard to understand and if you’re unfamiliar with the terminology, learning more about DNS can seem as daunting as learning a new language.

To help people who are new to the world of DNS, those looking to learn more, or even seasoned veterans who want a refresher, we’ve compiled a list of the need-to-know DNS terms along with their definitions.

Who We Are

Dyn is the worldwide Internet Infrastructure as a Service (IaaS) leader, powering Managed DNS, Traffic Management, Email Delivery & Email Reporting for more than four million enterprise, small business and personal users. With nearly 20 data centers around the world and industry-leading uptime for over 10 years, Dyn’s commitment to customer relationships and engineering excellence shines every day.

At Dyn, we do not discriminate between the hobbyist, the Fortune 500 company, or top sites on Alexa. We believe our users deserve premier performance, reliability, support and security – no matter what stage of the game they are at. We hold ourselves to the highest standards and have put a focus on engineering excellence and world-class customer support since day one.

We are passionate about what we do and we love our customers. We specialize in DNS and Email Delivery so they are free to specialize in their own areas of expertise to keep the Internet awesome.
The Master List of DNS Terminology

Table of Contents

/3 A Record THROUGH Cache
/4 CDN THROUGH DNS
/5 DNS Client THROUGH GSLB
/6 gTLD THROUGH Nameserver
/7 Node THROUGH Round Robin
/8 RTTM THROUGH Uptime/Downtime

Who Should Read This?

Novice
Beginner content is for readers who are new to email delivery. This content will typically walk you through the basics and give generalized overviews of various subjects.

Intermediate
Intermediate content is for readers with some experience in email delivery. This content will focus on techniques and strategies to take your delivery to the next level.

Expert
Expert content is for readers who are seasoned in email delivery. This content will focus on advanced techniques with a heavier tech focus.
A Record
Points a hostname to an IPv4 address.

AAAA Records
Points a hostname to an IPv6 address.

Active Failover
Active Failover enables your website to stay up and running – all while making the experience a seamless one for your visitors. When an outage is detected, your traffic is automatically re-routed to an alternate endpoint that you have pre-configured.

Anycast
DNS network topology that uses BGP to route DNS queries to the fastest nameserver on the network.

Auth Code
The “auth code” (sometimes called an “EPP code” or a “transfer code”) is a string, usually between 8 and 16 characters long and randomly created at the time of a domain’s registration, used to authorize transfers in certain Top Level Domains. The auth code provides an extra layer of security over the normal transfer request procedures.

Authoritative Nameserver
A nameserver which has been configured to provide answers for a specific domain, rather than simply getting and caching data about domains from other nameservers.

Cache
Caching refers to a process where Recursive DNS servers remember the results of a DNS Query for the time specified in the TTL (Time to Live). This reduces DNS query traffic as the Recursive DNS server already knows the answer. Once the TTL expires, the answer is removed from the cache.
CDN
A Content Delivery Network is a network of servers that serves content to end users from the closest node for the fastest load time.

CNAME
A CNAME is a special type of DNS record used to create an alias from one hostname to another. For example:
www.dyn.com is a CNAME to dyn.com
This means that someone accessing www.dyn.com will be pointed to the same IP address that dyn.com points to.
This is useful so that when your IP address changes, you only have to update dyn.com’s entry and then www.dyn.com will automatically point to the right place.

Cut Node
Cut nodes allow you to keep the DNS for your zone with your current DNS provider, but point or cut a specific node over to Dyn’s nameservers, allowing you to use one of our advanced features.

Data Center
Data centers house servers, computer systems, and other telecom- munication components, usually with redundant power and special security measures. They are designed to withstand major natural and man-made disasters.

DDoS
Distributed Denial of Service is an attack when multiple systems are used to flood servers with traffic in an attempt to overwhelm its available resources (bandwidth, memory, processing power, etc), making it unavailable to respond to legitimate users.

We have two whitepapers on DDoS:
Everything You Need To Know About A DDoS Attack
Defending Against DDoS Attacks To Managed DNS Systems

Delegate
To specify in DNS which nameservers handle a specific domain or sub- domain. See delegation.

Delegation
Delegation, as a verb (see delegate), is the process of designating the nameservers for a domain. As a noun, it is used to refer to the current set of nameservers to which a domain has been delegated.

DNS
DNS (the Domain Name System) provides mapping of hostnames to IP addresses and back again.
DNS Client
Also known as a DNS resolver, a DNS client is the system that makes a DNS request (e.g. your computer, smart phone, an ATM).

DNS Query
A request a client sends to a DNS server to resolve the IP address for a domain name or hostname.

DNS Zone
A portion of the DNS namespace that has been divided up for more granular administration of DNS. Zones hold DNS records that contain mapping information.

DNSSEC
DNSSEC is the act of adding special signatures to the root, TLD, and authoritative nameservers for your zone to establish a chain of trust. DNSSEC enabled zones ensure that the answer to a DNS query has not been tampered with.

DoS
A Denial of Service is an attack on a URL that is coming from one source.

Endpoint
End location that a client is getting to - IP address or CNAME.

Failover
When your primary server goes down, failover is the act of rerouting traffic to a redundant server. (Also see Active Failover.)

Forward Lookup
A forward lookup is when you use a host name (domain name) to find an IP address. Find out your IP address: [http://checkip.dyn.com/](http://checkip.dyn.com/)

Fully Qualified Domain Name
A fully qualified domain name is a complete hostname, like that which you would use when connecting to a server on the Internet. Fully qualified hostnames must be used when updating with a client, e.g., if your hostname is “myhost.dnsalias.net”, you must provide that entire hostname to the client, not simply “myhost”.

GSLB
Global Server Load Balancing responds to DNS requests by directing traffic with the best performing server in a geographic region.
**gTLD**
Global TLDs are TLDs that are not country specific and can be used by the entire Internet community. Examples of gTLDs are .com, .net, and .org.

**IP Address**
An IP address is how computers all over the Internet find each other. It is similar to your street address, except it is for computers. IPv4 addresses look like 207.127.235.88. IPv6 addresses look something like fe80::216:3eff:fe1e:c440. They are often hard to remember numbers, and they certainly don’t tell you very much about a computer. That is why we provide aliasing services. IP addresses can be static or dynamic.

Internet Protocol Version 4 (IPv4) was the first publicly used version of the Internet Protocol in 1981. Due to IPv4 address exhaustion, the IPv6 system was created & is slowly being integrated.

**ISP**
Internet Service Providers are those providing their customers access to the Internet. They are also commonly mailbox providers (e.g. AOL).

**Iterative Query**
An iterative query commonly takes place when a name server gives another name server the best answer it has for an IP query. An example of which is when a server asks root the location of example.com, the root responds with the best answer it can to the .com name server.

**Latency**
Latency is the length of a delay that end users experience when trying to access content.

**Load Balancing**
Load Balancing is used to distribute your traffic over several servers, resulting in increased reliability and efficiency.

**MX Record**
A Mail Exchanger record tells what mail server is responsible for accepting mail for a given domain. Sometimes, there can be more than one mail server so the server with the lowest priority (that is available) will receive the mail.

**Nameserver**
A nameserver is a server which has been set up to answer DNS queries, and provide information about a certain set of domains.
**Node**
A Node in our context is a DNS label. The parts of a domain between the dots. A Node can also refer to a Subdomain.

**PoP**
A Point of Presence is the physical location of a server, data center, etc.

**Primary DNS**
The DNS provider with control of zone file modification.

**PTR Records**
PTR records are a reverse lookup for an A record. Due to the nature of DNS and the way reverse lookups work, **PTR records can only be controlled by your ISP**.

**QPS**
Queries per Second is the measurement used in DNS to record how many queries a DNS server is receiving.

**Recursive Query**
A recursive query takes place when a DNS client makes a request to the recursive server for the IP address of a host name. The recursive server will either return the answer or an error message that the domain does not exist.

**Recursive Resolver**
The recursive server is typically supplied by your ISP and is the server that a DNS client makes its initial query to. Once the recursive server receives the correct information about an IP address from other name servers, the recursive server will cache the information.

**Redundancy**
Redundancy is having more than one server available. In the situation of a failure, a redundant server can be used as a backup.

**Reverse lookup**
Looking up an IP address to retrieve a host name.

**Root**
The root servers are nameservers that all other nameservers on the Internet know about, and contain very basic information about the DNS system, which will lead other servers along the path to finding out specific information about a host.

---

**Global Root Server Locations**
**Round Robin**
Distribute server load evenly across multiple servers.

**RTTM**
Real Time Traffic Management monitors all of your endpoints to detect the best-performing one and provides you with the lowest latency possible. RTTM collects real-time data to track the load time of each of your endpoints, rather than just routing your traffic to the closest geographical data center.

**Secondary DNS**
Secondary DNS provides backup DNS servers that download information from your primary DNS server and share its load. Secondary DNS servers essentially have a read-only copy of the zone that stays in sync with the master or primary DNS server.

**SoA Record**
Start of Authority record indicates the DNS server with the best source of information in a zone along with some basic zone configuration settings. It has the most authority to make changes in the domain or answer questions.

**Traffic Management**
Traffic Management is an advanced feature that allows for the weighted distribution of application load between global data centers, cloud providers, or your existing CDNs based on seven geographic regions. This gives customers the flexibility to route traffic in each region to the optimal endpoints in their infrastructure.

**TLD**
Top Level Domain - .com, .net, .org, etc.

**TTL**
TTL is the amount of time in seconds that a DNS record will be cached by an outside DNS server.

**TXT Records**
TXT records are used to store information. Common uses include SPF, DKIM, etc.

**Unicast**
In a Unicast network, there is only one responding server.

**Uptime/Downtime**
Uptime and Downtime refer to if a server is currently active or is unavailable, respectively.

Questions in regards to your Managed DNS infrastructure?

☎ +1 888 840 3258
✉ sales@dyn.com
🌐 http://dyn.com