

EBOOK:

The Authoritative Guide to DNS Terminology

From **A Record & DNS** to **Zones**

for which
to be best in any
point of view.
Performance
execution
or accomplish
doing so



Internet Performance Management (IPM): Building on the foundation of managed DNS

As more users and more online services (sites, microservices, connected “things,” etc.) join the global internet, the scale, complexity and volatility of that internet are also on the rise. Modern DNS is reemerging as a powerful tool for commercial internet infrastructure that puts control back in the hands of IT leaders.

The foundation of the Domain Name System or DNS, a distributed internet database that maps human-readable names to IP addresses, allows people to reach the correct online service (website, application, etc.) when entering a URL. For example, the domain name dyn.com translates to the IP address of 199.180.184.220.

Because DNS is the first step in the process of reaching online assets, it also provides an ideal “location” in the network to make decisions about where to send certain traffic. This is particularly useful as more organizations adopt cloud or use CDNs to optimize content delivery, spawning hybrid environments. DNS, particularly when coupled with intelligence about those destination endpoints and the network path between them, can help get the right user to the right asset, improving performance, reachability of those assets, and security posture.

Dyn has been in the managed DNS business for over 10 years (and pioneered Dynamic DNS before that), so the DNS terms in this guide are commonly heard around the proverbial water coolers at Dyn, but we realize they can be a bit arcane despite the importance of DNS.

That’s why we’ve assembled this *DNS Terminology Guide* as your reference. We hope you’ll find it helpful.

Table of Contents

A Record – Auth code	3
Authoritative Nameserver – DDoS	4
DDNS – Endpoint	5
GSLB – Primary DNS	6
PTR Records – Tracerout	7
Traffic Director – Zone	8

A Record

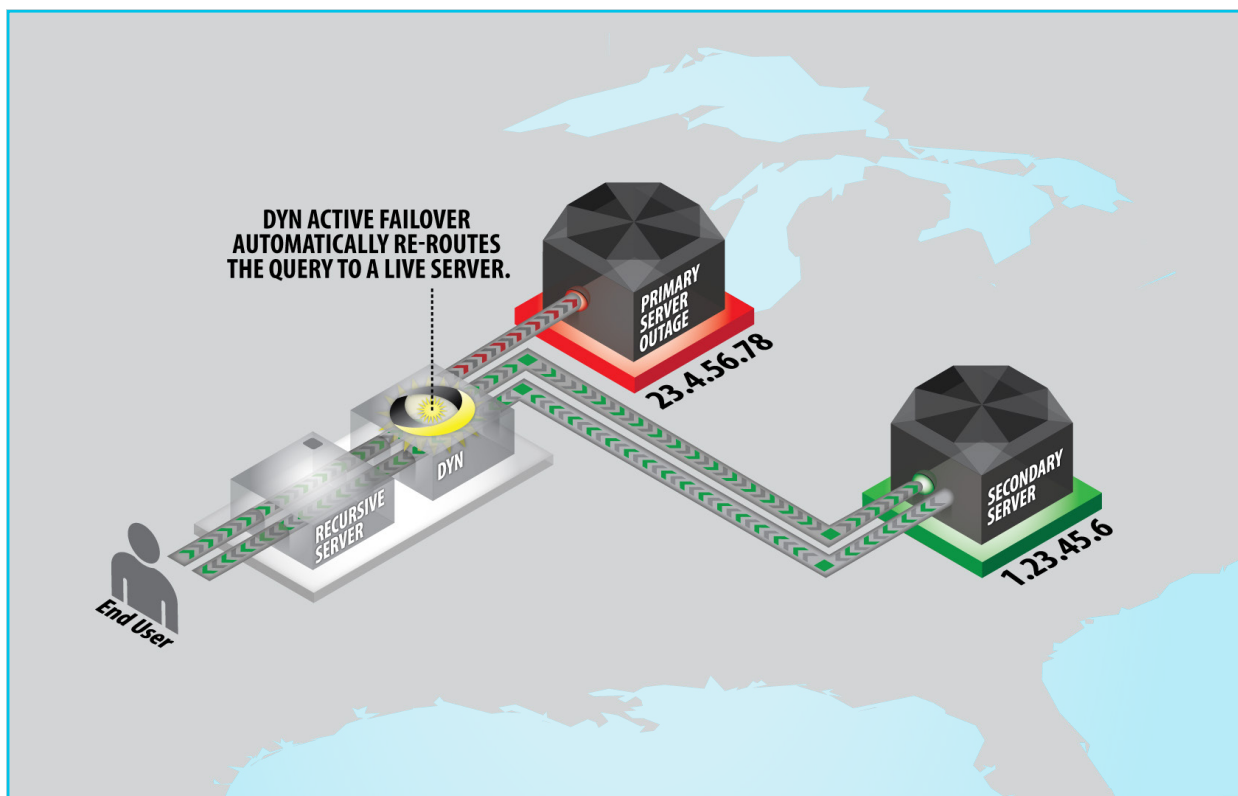
Points a hostname to an IPv4 address.

AAAA Records

Points a hostname to an IPv6 address.

Active Failover

Active Failover enables your online services 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

Anycast networks provide a one-to-many relationship between IP addresses and their associated nameservers. Anycast networks protect availability, achieving high redundancy and reducing risk of service interruption by distributing DNS service for each IP address across multiple nameservers strategically placed throughout the world. Anycast provides redundancy while reducing DNS query latency.

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.

Autonomous System (AS)

A collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet.

Border Gateway Protocol

BGP performs routing between multiple autonomous systems (domains) by finding the best path.

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. Companies are increasingly using CDNs to push rich content like streaming video and games closer to the user. Recently, the use of a multi-CDN strategy has emerged to improve performance to specific markets and ensure the best price-to-performance ratio.

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 telecommunication components, usually with redundant power and special security measures. They are designed to withstand major natural and man-made disasters. Data centers are generally managed by a company's IT department to support "on-premises" deployment of applications using their own infrastructure (vs. cloud deployment).

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.

DDoS Attacks are on the rise.

Research shows that DDoS attacks increased 125% year over year. DNS was the single most common attack vector. Furthermore, a single successful attack caused average site/service downtime of 17 minutes. These trends show why organizations are turning to managed DNS and Secondary DNS to replace or complement home-grown DNS infrastructure as part of a comprehensive DDoS mitigation strategy.

DDNS (Dynamic DNS)

DDNS is used mainly by home users to send dynamic IP address updates to a static hostname.

Delegate

To specify in DNS which nameservers handle a specific domain or subdomain. *See delegation.*

Delegation

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

DNS

DNS (the Domain Name System) provides mapping of hostnames to IP addresses and back again. It's akin to translating latitude and longitude into a postal address. DNS is a foundational component of IPM, increasing in strategic importance as the scale, complexity and volatility of the internet increase.

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.

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.

Dynamic Steering

Internet routing that utilizes DNS to make route changes autonomous of operator control based on real-time internet performance or other, pre-determined policies.

Endpoint

The target location for the client - IP address or CNAME.

Forward Lookup

A forward lookup is when you use a hostname (domain name) to find an IP address. Find out your IP address: <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".)

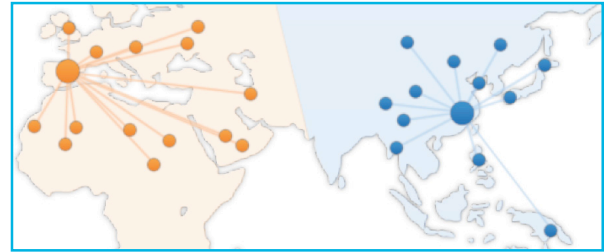
Hijacking

IP hijacking (sometimes referred to as BGP hijacking, prefix hijacking or route hijacking) is the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables.

GSLB

Global Server Load Balancing responds to DNS requests by directing traffic using the best performing server in a geographic region.

The value of GSLB has increased with the rise in distributed online applications and services. It has also evolved to embrace predictive, intelligent routing based on real-time internet conditions.



Hostname

See Node

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. It is 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.

ISP

Internet Service Providers are those providing their customers access to the Internet. ISPs provide the onramp to the internet for both users and service providers.

Iterative Query

An iterative query commonly takes place when a name server gives another nameserver 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 nameserver.

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

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. Primary DNS is generally the first responder to DNS queries and is often complemented by Secondary DNS for redundancy and performance considerations.

IPv6 has arrived.

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 being integrated.

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 DNS

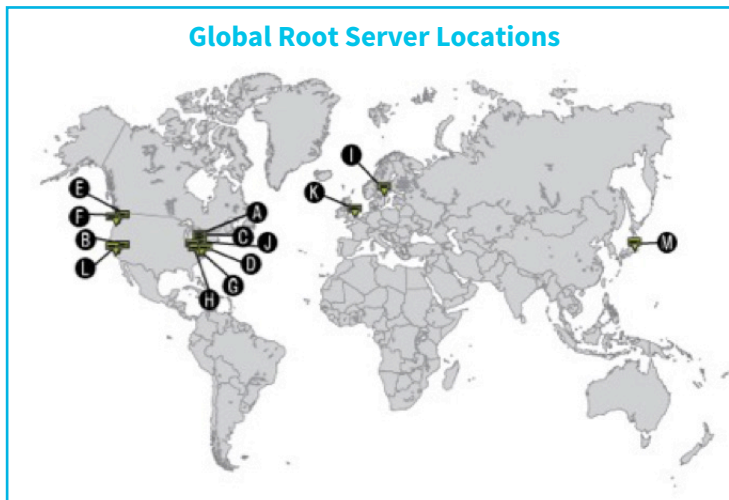
Recursive DNS is typically supplied by an ISP and is the server to which a DNS client makes its initial query. Once the recursive server receives the correct information about an IP address from other nameservers, the recursive server will cache the information.

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 hostname.



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 specific information about a host.

Round Robin

A method used to distribute server load evenly across multiple servers.

Secondary DNS

Secondary DNS provides parallel DNS server functions for the primary DNS Server and shares its workload. A read-only copy of the zone stays in sync with the master or primary DNS server and works in an “active-active” mode whereby the first and fastest DNS “wins” the query. Employing multiple DNS networks increases the resiliency of this critical service.

SoA Record

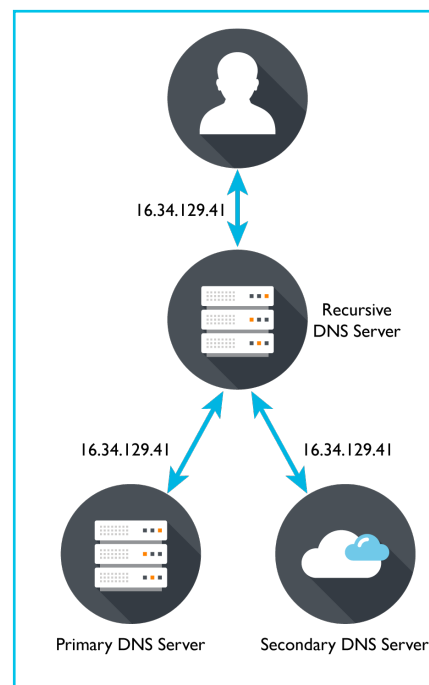
Start of Authority record indicates the DNS server with the best source of information in a zone along with some basic zone configuration settings. It has the most authority to make changes in the domain or answer questions.

TLD

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

Traceroute

A diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.



[High Availability DNS Paper available here.](#)

Traffic Director

An advanced service that integrates geographic load balancing with monitoring and failover features.

Transit

The service of allowing network traffic to cross or "transit" a computer network, usually used to connect a smaller ISP to the larger internet.

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

A DNS network topology in which there is only one responding server. Unicast is more susceptible to downtime/outage and generally performs DNS resolution with more latency vs. anycast DNS networks.

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.

About Dyn

Dyn is an Oracle Infrastructure-as-a-Service (IaaS) global business unit (GBU). Oracle's Dyn is a pioneer in DNS and a leader in cloud-based infrastructure to connect users with digital content and experiences across a global internet. Dyn's solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC. Adding Dyn's best-in-class DNS and email services extend the Oracle cloud computing platform and provides enterprise customers with a one-stop shop for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

[learn more](#)

For additional information about DNS visit: dyn.com