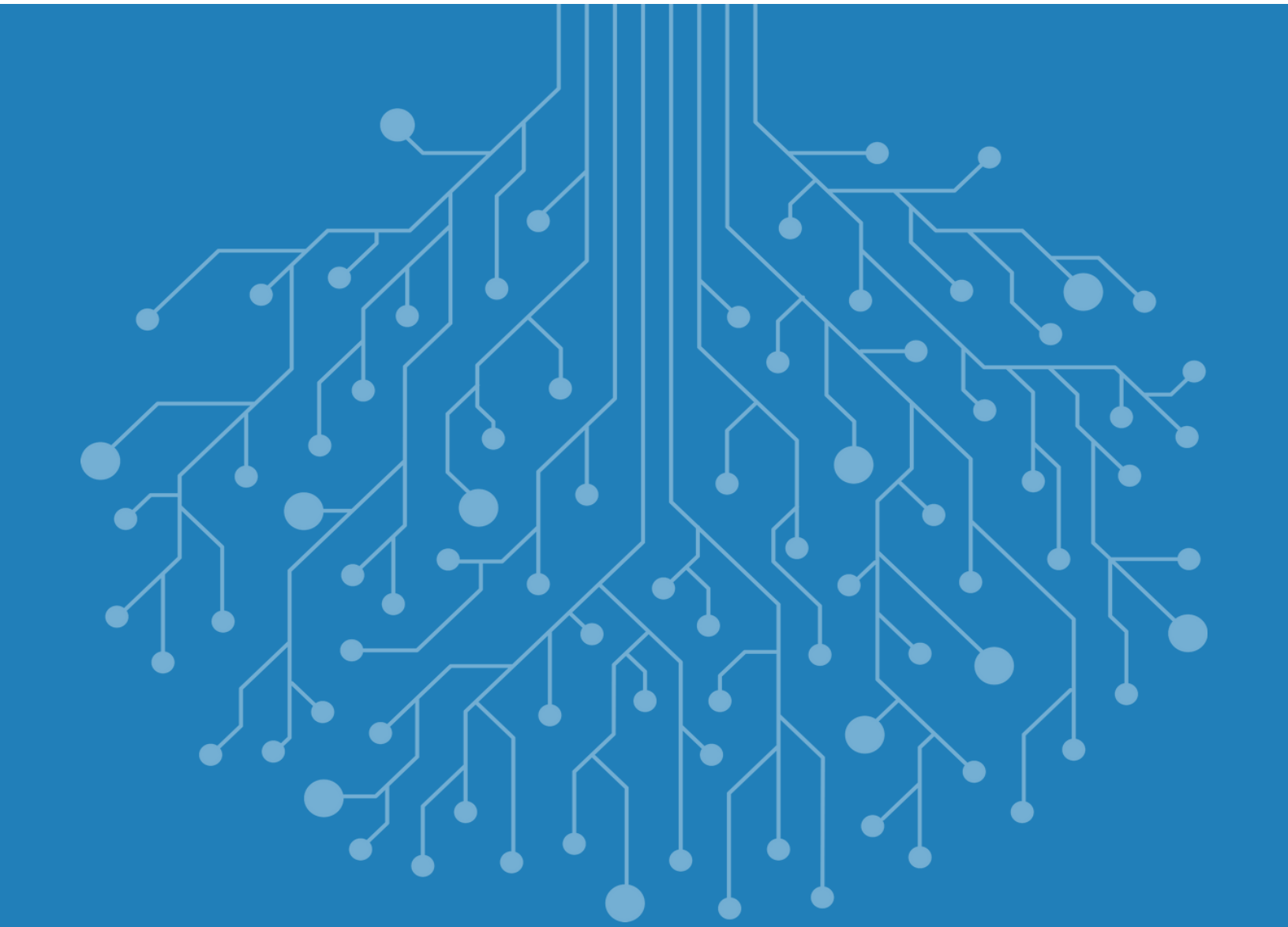
DNS

FOR NEWBIES, EXPERTS

& everyone in between



DNS MADE EASY

Table of Contents

CHAPTER 1

What is DNS?

8 in 10 Americans use the Internet. While that might sound pretty average, let's compare that to the whole planet where only 4 in 10 people use the Internet. With all this in mind, you'd think that Americans should be pretty tech savvy, right? And yet, only **0.003 % of Americans *** know that DNS is the reason the Internet continues to exist over 30 years later.

Pretty heavy stuff, so why don't the other 997 out of 1000 people know what this amazing system is? DNS gets taken for granted, because it's not something most people see when they use the Internet.

So what is this proverbial glue that holds the Internet together? First we need to understand that the Internet is essentially a network of computers that connect to each other. In order for computers to find each other, they need a common language.

In the beginning, web surfers connected to other computers (or websites) using long series of numbers (**IP addresses**) to describe themselves. This became troublesome very quickly because no one could remember all those long numbers, so the early "fathers and mothers" of the Internet developed a system to attribute a domain name to each of these IP addresses, enter the **Domain Name System**, or DNS for short.

* based on a poll

CHAPTER 2

What is a DNS query?

But what does this have to do with you wanting to check the latest cat video your friend tagged you in on Facebook? When you type facebook.com into your browser, you're actually sending out a query. Your computer doesn't know where facebook.com is, so it has to ask other computers, to learn where facebook.com is.

Think back to the days where we didn't have cell phones and had to use phone books to call people. DNS is basically the phone book of the Internet! It stores all the **IP addresses** (phone numbers) and **domain names** (people, places, and businesses).

Say you need a DNS provider, you'd ask yourself "what's the phone number for DNS Made Easy?" in a nutshell that's your query. In terms of DNS, your query is asking "what's the IP address for dnsmadeeasy.com?" Simple right?

Now this is where it gets a little more complicated. The domain in question has to be a **Fully Qualified Domain Name** (FQDN), which is the properly formatted name for a domain. That means that the domain has both a **hostname** and a **domain name**. Let's say we're trying to reach DNS Made Easy mail servers, which are hypothetically located at **mail.dnsmadeeasy.com**

- The **hostname** would be: **mail.**
- The **domain name**: **dnsmadeeasy.com**
- The query would be: **mail.dnsmadeeasy.com**
- The response would be: **10.200.300.201**

CHAPTER 3

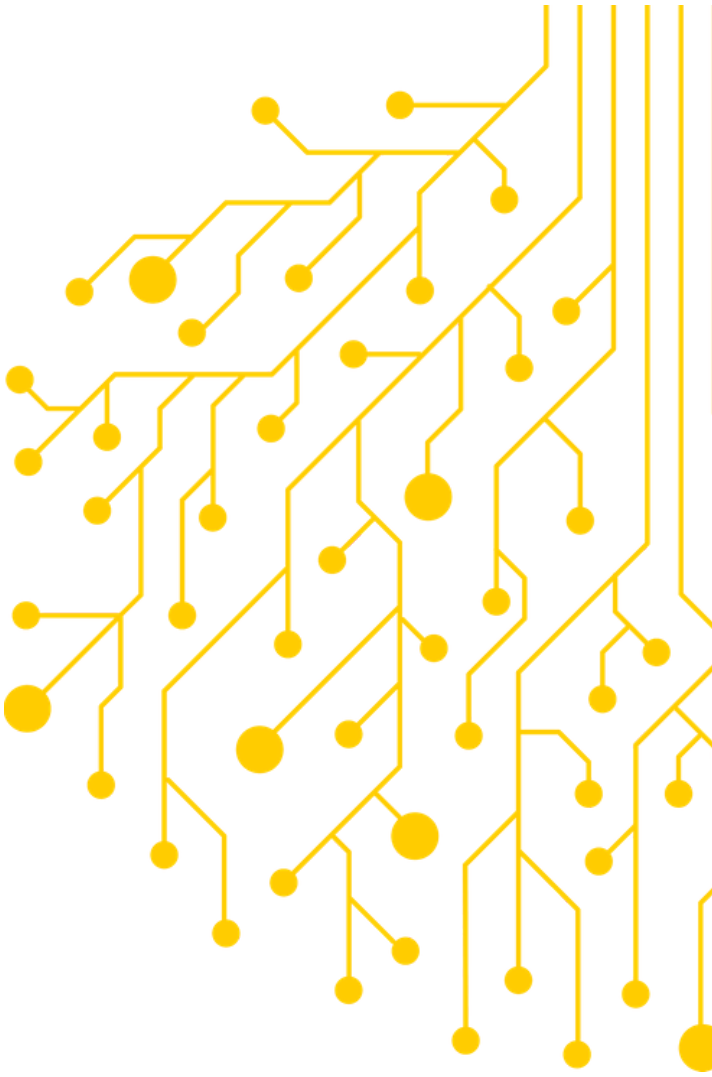
What is a DNS server?

Wait!

Before we get into how these queries travel the globe trying to find that pesky IP address, we first need to understand what a DNS server is.

Remember those **IP addresses** and **domain names** we were talking about a minute ago? These numbers and names had to be stored somewhere that was accessible to the entire Internet, so that's when the first DNS server was built.

Simply put, a **DNS server** is a computer (actually there are a bunch of these but we can get to that later) that holds parts of the database that contains all the IP addresses and their corresponding domain names for parts of the Internet.



When you type a website into your browser, normally you'll be connected to your desired page within a few milliseconds. This makes a lot of people think that there aren't that many steps or jumps between your computer and the server that hosts your desired website.

Wrong! Your query will end up taking hundreds of different jumps in between, and then is has to come all the way back to your computer. So let's break it down...

Say we want to visit the DNS Made Easy blog, which is found at:
social.dnsmadeeasy.com

Using the Domain Name system, we'd lookup the record by breaking down the address piece by piece.

Once you've found the IP address for your domain, this little piece of information has to come back to your browser before you're finally connected.

That's a lot of stuff going on in just a couple milliseconds.

To put this in perspective, DNS Made Easy provides their clients with sub 30ms resolution times in all major markets.

That's less than half the time it takes to blink your eye.

First, we have to go all the way back to the **root name servers**. These servers are really special, because they hold all of the domain names and their corresponding IP addresses

Then we ask the COM top level domain (TLD) name servers that handle all the traffic for sites ending in .com

From here, the .com name servers identify what name servers dnsmadeeasy.com is a responsible for

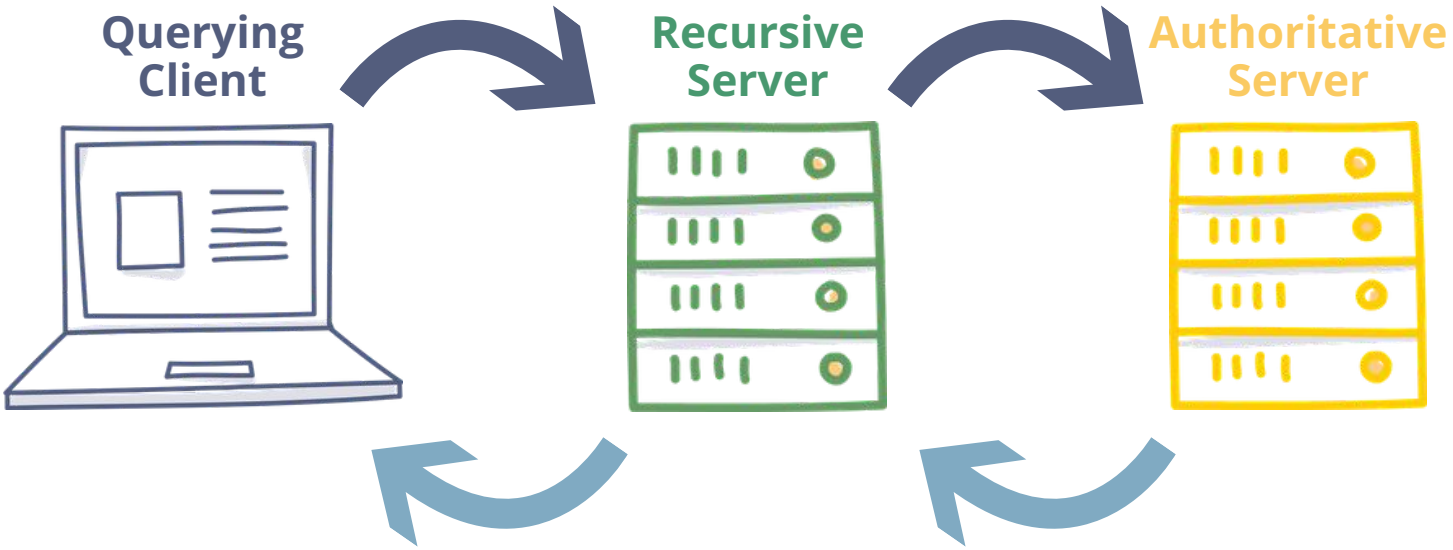
Finally, the authoritative servers for dnsmadeeasy.com respond with the appropriate IP address for social.dnsmadeeasy.com

CHAPTER 4

Misconceptions

There are two different kinds of DNS servers that you'll run your queries through: **Recursive DNS Servers** (or Caching Servers, sounds like "cashing") and **Authoritative Servers** (what DNS Made Easy provides).

In a nutshell, Authoritative DNS servers store the “maps” of your domain names to IP addresses. This domain name to IP mapping is usually configured by system administrators. A person that is visiting web sites asks Recursive DNS servers for the lookups. Recursive DNS servers than ask the necessary Authoritative Name Server for the answer. Then the Recursive name server will give this answer to the person needing the information.



Recursive servers are the work horses in the DNS lookup process. They often have to make numerous DNS lookups in order to respond with the proper IP for the querying client. These kinds of servers are typically managed by an **ISP** (Internet Service Provider) or specialty resolving DNS providers.

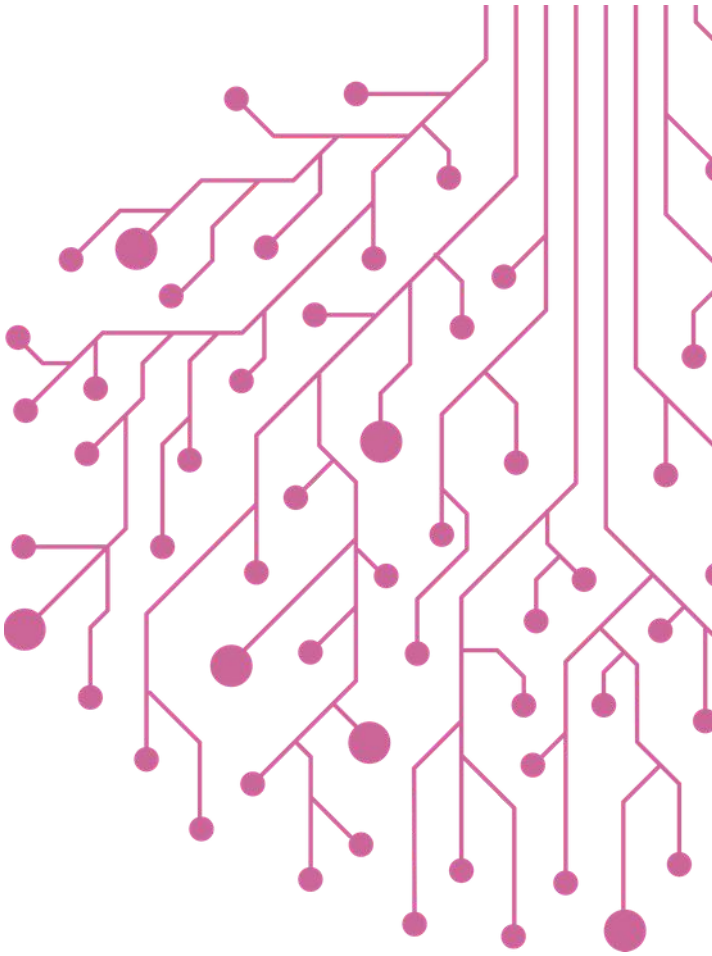
For example: Google runs their own public recursive DNS servers.

We actually have a great video that breaks all this down at **learndns.com**

If you own a domain name, at some point you will need to use an authoritative DNS server to map your domain names to an IP address. This is only done on an Authoritative DNS server.

Authoritative DNS servers are configured in a hierarchical structure. Everything starts with the dot root name servers (like we discussed earlier). These authoritative name servers know where to find the next level set in the hierarchy such as Top Level Domains.

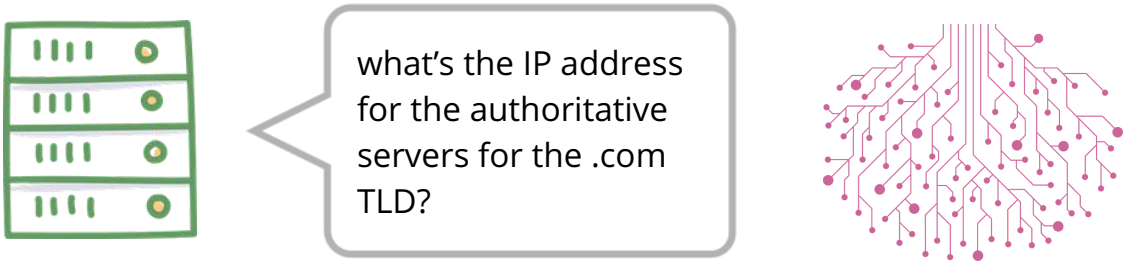
We briefly talked about the root name servers earlier, which are the original servers that hold all of the domain names and their corresponding IP addresses. The root servers are at the top of the proverbial DNS tree. They know exactly which IP addresses of the authoritative servers are the ones that handle DNS queries for **Top Level Domains** (TLD) like .com.



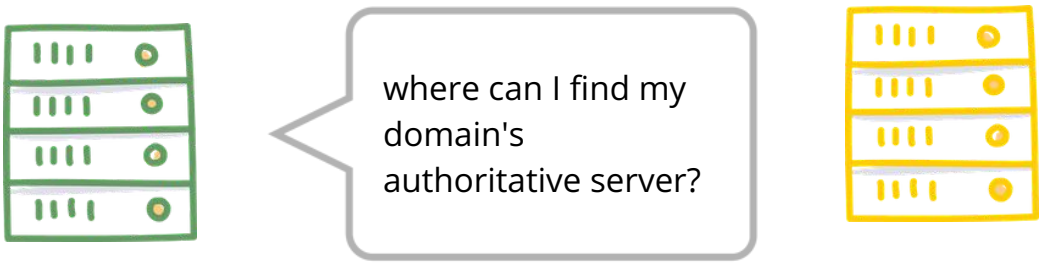
Back to

what we were talking about earlier, let's say that your recursive DNS server doesn't have any information cached. What steps would the recursive server take to find the IP address for said domain?

First the **recursive server** has to ask the **root domain servers**



Then it goes to the **authoritative server** designated as .com



These are called **recursive servers** because they recurse through the hierarchical DNS tree from top to bottom until they hit the **authoritative server** for the domain in question. Most of the time, recursive DNS servers are actually caching recursive DNS servers. This means they store the maps of URLs to IPs for a specified amount of time (known as the **TTL** or **time to live**). This means they don't have to repeatedly send the same queries to those same authoritative servers, saving the user a lot of time.

Recursive name server only knows where to find the root name servers (dot). Based up each level of name servers knowing where the next level is in the hierarchy, the answer is eventually found.

CHAPTER 5

DNS Register vs. Host

One of the biggest misconceptions our users face is struggling to understand the difference between a **domain registrar** and a **DNS host**. Understanding the difference is crucial to maintaining a reliable and fast website that's available to all of your users.

Let's start with the bare bones: a domain registrar offers services that allow you to pick a domain name and register it to an IP address. This is the first step you take when you want to build a website. You'll remember from earlier, your domain name, like **www.dnsmadeeasy.com**, is essentially the face of your IP address, **123.45.678.90**.

Did you know?

Whenever you run a "**whois**" command, or an online interface to the whois data, you're actually querying the domain name registry.

When you register a domain name, you have to go through a **DNS registrar**. These companies often deal directly with the registry operators who control the master list of all domain names. These registries are managed by **IANA** (International Assigned Numbers Authority), which is a department of **ICANN**, a nonprofit organizations that runs the root zone management in the Domain Name System.

Most times, you won't actually deal with a domain registrar directly; rather you end up purchasing a domain name through a Web Hosting Provider. These companies do all the work for you and register your domain through the registries all on your behalf... but we'll get more into this in a minute.

So then what's a DNS host? Once you've purchased your domain name, you have to tell it which domain name servers will be authoritative for that domain. A **DNS hosting provider** hosts these servers, which authoritatively respond for your domain.

Sometimes domain registries also offer DNS hosting, however the two services should never be confused. Before we go deeper into what a DNS host does, we need to clear up the different kinds of companies that offer DNS hosting.

- **Domain registrars** that offer DNS hosting as an additional service
- **Web hosting providers** that offer DNS hosting as an additional service
- **Dedicated DNS hosting companies** (that's all they do)
- **In-house DNS hosting** which is basically like having your own private DNS host

Too often people resort to using their web host's DNS services because they're offered as an add-on or included with the web hosting services. This tends to confuse most people; because they end up thinking the two are one in the same.

In a nutshell, web hosting is essentially the space where your website files are stored. While DNS hosting is what connects users to the site and keeps the domain online.

Why does all this matter? When you're deciding how you want to host your DNS, you need to be sure you understand the differences between the different kinds of hosts. Your decision could either keep your site online 100% of the time at a low cost, or knock you offline and cost you thousands in maintenance and cleanup. DNS is the end-all-be-all of your site's web presence. Without it, no one would be able to access your content. Dedicated DNS hosting providers tend to have faster and more reliable infrastructure, designed from the ground-up for hosting DNS query traffic and nothing else.

CHAPTER 6

How do Outages Happen?

Ever gone to a website and gotten an error message that said, “DNS host not resolved” or "host not resolvable"? This is because your DNS host is not reachable. It could be they're suffering an outage, or network error, not reliable, a network admin accidently deleted a record... or a DDoS attack.

Pretty much what's happening is the incoming traffic is so congested, it slows to a crawl. Or in some cases, the site will be knocked completely offline.

Often times it's the result of a **DDoS attack** (distributed-denial-of-service attack), which is the disruption or abolition of services of a host connected to the Internet. It’s a mouthful, but let’s break it down a little more with a relatable example. Think of these connections between the internet and your site like highways.

Say your site is connected to the World Wide Web via a two-lane highway. Now what if your site goes viral and you get millions of people speeding towards your website? The more popular you get, the more eyeballs you have on your site. This can attract both potential customers and attackers. The most cunning attacks use DDoS attacks which basically send floods of traffic at your site, but makes it appear as if many different computers are sending the traffic. This makes identifying an attack even harder, because it can appear to be normal visitors.

If we think of it like a highway, basically a DDoS attack mimics what rush hour would look like, inevitably bringing your site to a gridlock.

These kinds of attacks are orchestrated floods of **packets** (which you'll remember from earlier are like the queries you send to a DNS server to access a website's IP address).

Your site's name servers can only handle a finite amount of DNS requests or **PPS** (packets per second) before they fail. A DNS hosting provider, like DNS Made Easy, solves this problem by setting up hundreds of name servers worldwide on an **Anycast network.** It's pretty much like having a major interstate highway system that consists of many different highway networks spread across a large area.

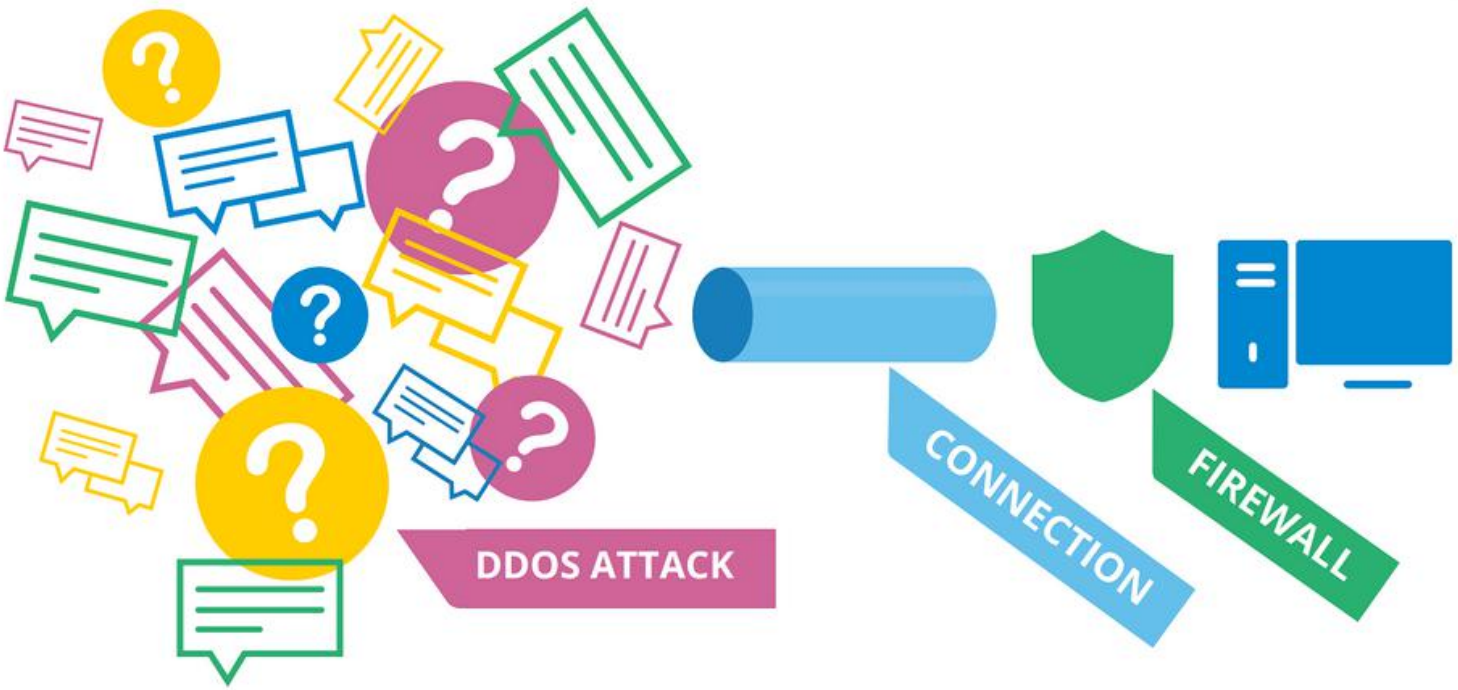
DNS Made Easy's Anycast + network serves DNS traffic across hundreds of name servers, allowing the network to manage exponentially more requests than an in-house network (also known as a **Unicast network**, because it only hosts DNS from one location).

There are many different ways to prevent DDoS attacks, but some of these methods can be very costly and not practical for small businesses. Some enterprise organizations use **in-house DNS infrastructures** (unicast networks), however these can cost thousands to set up, and even more to maintain. Not to mention, expensive firewalls to protect these servers.

Want to learn more about the benefits of using an IP Anycast + network? Our experts wrote a whole white paper on it! **Read it here for free.**

What most of these in-house DNS users don't realize is no matter how large the **firewall** is, if their incoming connections into their network aren't large enough, then it's game over.

Back to our highway analogy, if they don't increase the number of lanes in their highway, it doesn't matter how many shields they have up to fend off attackers. The attack will actually break the system before the packets even reach the firewalls. Even if the attack does reach the firewalls, DDoS attackers are notorious for bypassing them, because they are sending tiny packets that don't normally raise red flags for most security systems.



Our experts have actually developed a much larger list of ways to prepare, based off of years of fighting DDoS attacks that we've mitigated on a weekly (sometimes daily) basis. See what our engineers have to say about protecting your domains from in-house implementations to even outsourcing all of your networking needs to a cloud-friendly DNS provider. You can **read more here.**

CHAPTER 7

Why Outsource?

Now that we have covered all the basics, how can you start to take control of your own DNS? There a many different methods out there that have helped people from home users to large enterprises. We've already discussed a few ways such as bundling your DNS hosting with your web host, or implementing an in-house DNS infrastructure.

While these options may promise fast speeds or a hands-off approach (preconfigured services and minimal customizability) to DNS services, you're lacking some pretty basic features such as **Failover** and **Global Traffic Director**. These services come standard with outsourced DNS providers and allow you set up fail safes in the event that your site goes down.

So then what's a **DNS provider**? It's really simple actually, DNS providers only offer DNS hosting and management services. Their infrastructures are designed by industry experts, built for the cloud, and engineered for the lowest resolution times and 100% reliability.

The best part? You can take advantage of a DNS provider's global network without having to pay for all the infrastructure and maintenance costs of having dozens of worldwide facilities.

CHAPTER 8

What is Failover?

Where do you start then? If you've made the decision to let a managed DNS provider handle your query traffic... then you still need to make a few more decisions. Providers offer a lot of different features and services that can help with everything from setting up your cloud-based DNS infrastructure, to backup plans in case something goes wrong.

Many providers will try to bundle or oversell you with products you don't need. That's why you need to learn what each of these features do, so that you can make decisions personalized for you, based on your needs.

When you start out managing your own DNS, the first thing you'll probably set up is DNS Failover. It's simple to set up and you can keep your site online even if the worst happens.

Remember those DDoS attacks we were talking about earlier? Say your site gets hit by an attack which knocks your site offline. If you had failover setup, your customers would still able to view your site.

Amazing right, but how does it work? Simply set up a back-up IP address for your site to failover to. Whenever your provider notices that your site is down **(Failover Monitoring)** it will first check to make sure your backup IP is up and running. Then it will automatically redirect your traffic to your backup IP instantly. It can even **Failback** your traffic back to your original IP once your site is back online.

CHAPTER 9

Your Backup Plan

There are a lot of different ways you can "backup" your domain so you can always stay online. In addition to Failover, you can set up **Secondary DNS** which basically creates a body double for your domain.

This is great for people who decide to stick with an in-house infrastructure, because now you can host your own DNS; but in the event of an outage, you'll have a backup version of your site on your Secondary DNS provider's servers. It's really easy, all you have to do is tell your name servers to redirect to your secondary provider in the event of an outage.

But wait there's more... you can actually combine a few features together to get exponentially more layers of redundancy and failsafes.

You can combine Failover with the **Global Traffic Director (GTD)**, which optimizes your traffic flow based on regional location. Basically, in the event of an outage, your site would failover to your backup IP. But what if only one region is suffering an outage? Using GTD, you can specify all other regions to redirect around the problem areas.

When used correctly, you can slash resolution times by responding to queries within the same region. That means if you have a querying client in London, the client will be responded to by a European server. Local responses mean less travel time, which means faster resolution, and potentially greater ROI!

CHAPTER 10

Everyone needs DNS

Ecommerce to advertising, DNS runs everything!

If your business or organization is dependent on the Internet for your eCommerce website, communication, or advertising... Then you are dependent on the Domain Name System.

So how do you use a third-party provider to optimize your DNS performance? We have already covered a few of the basic services that providers offer, but how do these apply to your specific organization's needs? To make your job easier, we developed a tried a true strategy for each of the top 6 industries that need DNS management.

Get Your DNS Strategy

CHAPTER 11

About Us

Since 2002 DNS Made Easy has been the world leader in providing top tier DNS services. DNS Made Easy implemented the industry's first triple independent Anycast cloud architecture for maximum DNS speed and DNS redundancy.

Over the past 14 years, DNS Made Easy's services have grown to manage hundreds of thousands of customer domains receiving more than 30 billion queries per day. Today, DNS Made Easy builds on a proud history of 99.9999% uptime and is the preferred DNS hosting choice for most major brands.

If you want to learn more about how DNS works and the benefits of DNS management, follow our blog!

Sales Engineers: +1.703.880.3095

Technical Support: +1.703.880.3095 ext. 2 and enter your support contract number.
Free 24/7 Web Support.

Phone: +1.703.935.1598

Email: sales@dnsmadeeasy.com