What is DNS?

Peter Silva, 2017-02-02

DevCentralBasics

What is the Domain Name System (DNS)?

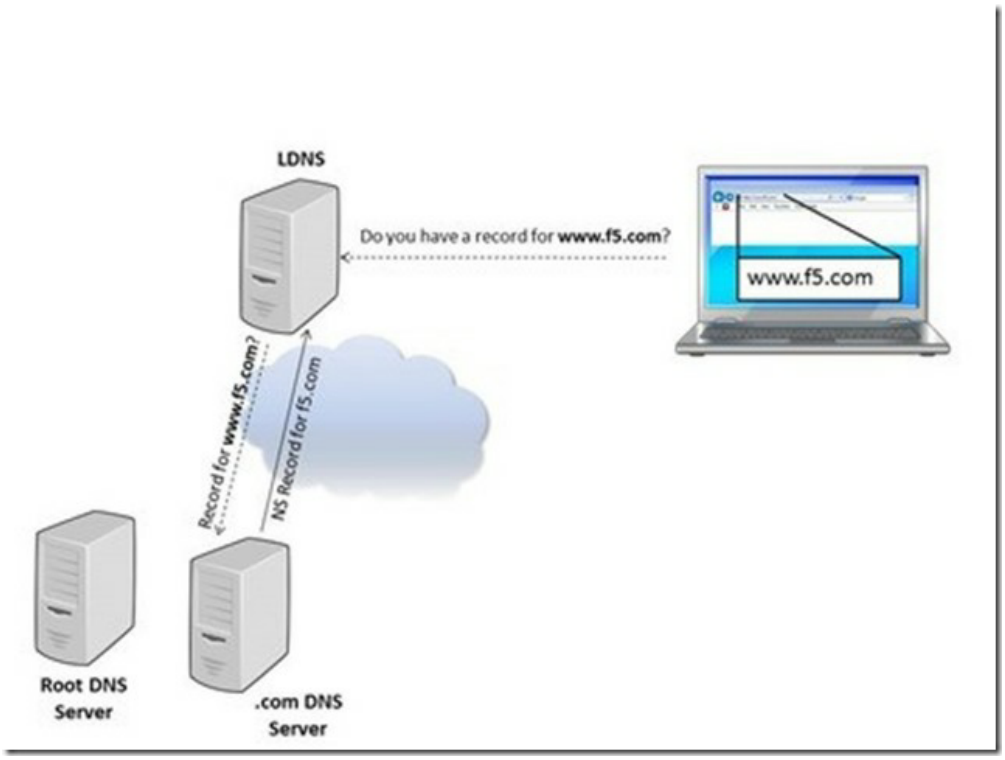
Imagine how difficult it would be to use the Internet if you had to remember dozens of number combinations to do anything. The Domain Name System (DNS) was created in 1983 to enable humans to easily identify all the computers, services, and resources connected to the Internet by name—instead of by Internet Protocol (IP) address, an increasingly difficult-to-memorize string of information. Think of all the website domain names you know off the top of your head and how hard it would be to memorize specific IP addresses for all those domain names. Think of DNS as the Internet's phone book. A DNS server translates the domain names you type into a browser, like www.f5.com, into an IP address (104.219.105.148), which allows your device to find the resource you're looking for on the Internet.

DNS is a hierarchical distributed naming system for computers, services, or other resources connected to the Internet. It associates various information with domain names that are assigned to each of the participating DNS entries.

How DNS Works

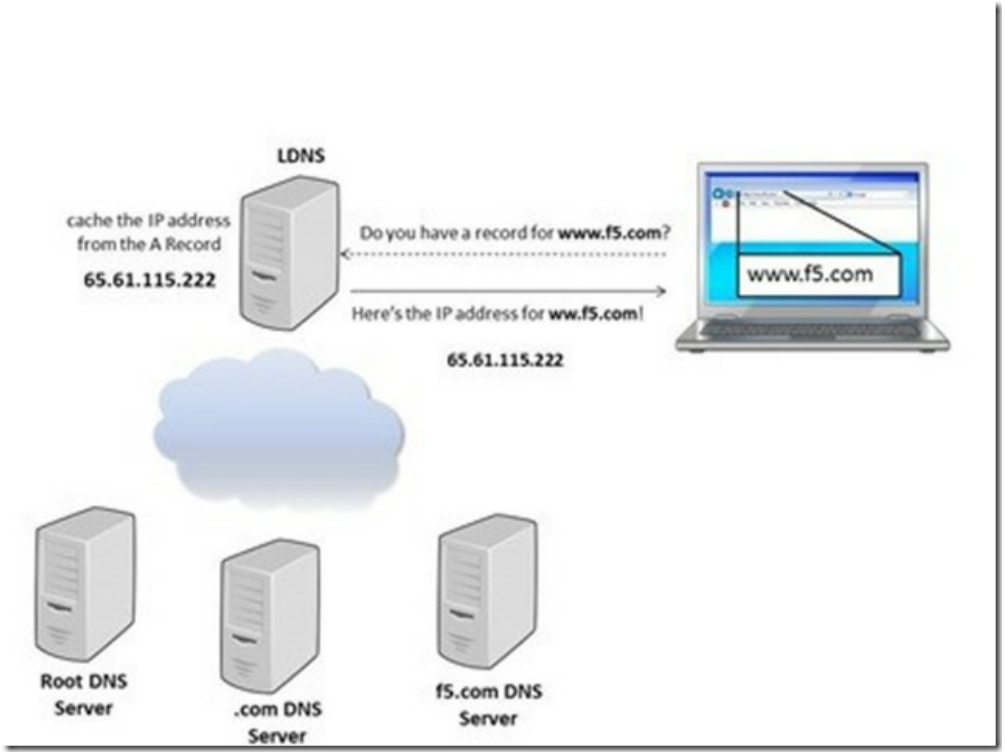
The user types the address of the site (**www.f5.com** as an example) into the web browser. The browser has no clue where **www.f5.com** is, so it sends a request to the Local DNS Server (LDNS) to ask if it has a record for **www.f5.com**. If the LDNS does not have a record for that particular site, it begins a recursive search of the Internet domains to find out who owns **www.f5.com**.

First, the LDNS contacts one of the Root DNS Servers, and the Root Server responds by telling the LDNS to contact the .com DNS Server. The LDNS then asks the .com DNS Server if it has a record for **www.f5.com**, and the .com DNS Server determines the owner of **www.f5.com** and returns a Name Server (NS) record for **f5.com**. Check out the diagram below:

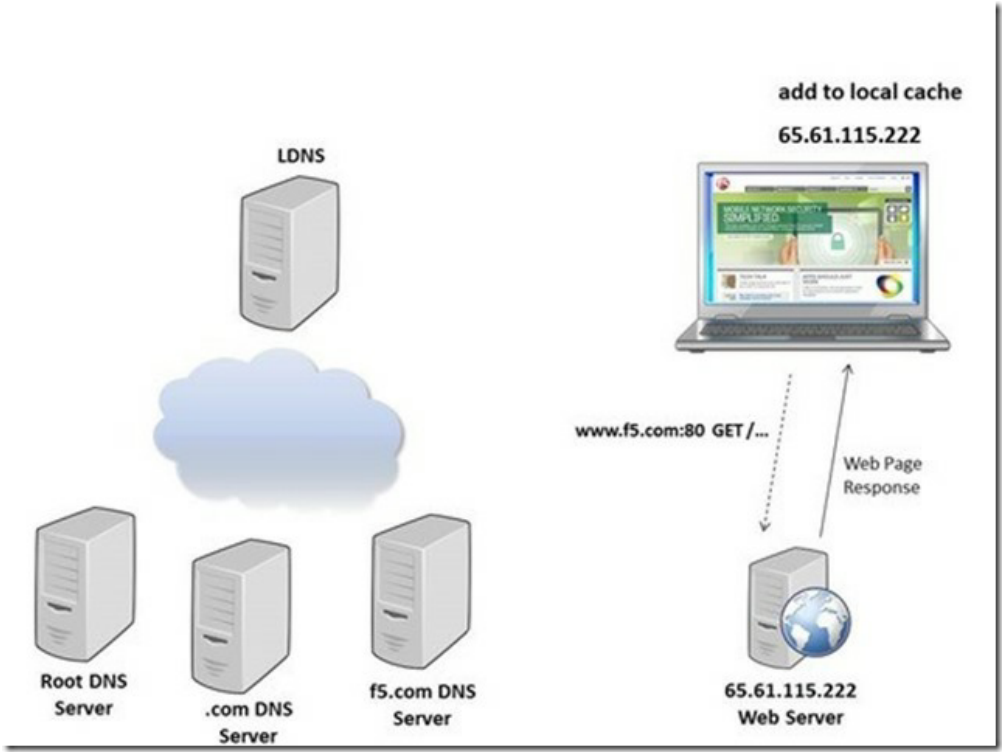


Next, the LDNS queries the f5.com DNS Server NS record. The f5.com DNS Server looks up the name: **www.f5.com**. If it finds the name, it returns an Address (A) record to the LDNS. The A record contains the name, IP address, and Time to Live (TTL). The TTL (measured in seconds) tells the LDNS how long to maintain the A record before it asks the f5.com DNS Server again.

When the LDNS receives the A record, it caches the IP address for the time specified in the TTL. Now that the LDNS had the A record for **www.f5.com**, it can answer future requests from its own cache rather than completing the entire recursive search again. LDNS returns the IP address of **www.f5.com** to the host computer, and the local browser caches the IP address on the computer for the time specified in the TTL. After all, if it can hold on to the info locally, it won't need to keep asking the LDNS.



The browser then uses the IP address to open a connection to **www.f5.com:80** and sends a **GET /...** and the web server returns the web page response.



DNS can get a lot more complicated than what this simple example shows, but this gives you an idea of how it works.

DNS Importance

As arguably the primary technology enabling the Internet, DNS is also one of the most important components in networking infrastructure. In addition to delivering content and applications, DNS also manages a distributed and redundant architecture to ensure high availability and quality user response time—so it is critical to have an available, intelligent, secure, and scalable DNS infrastructure. If DNS fails, most web applications will fail to function properly. And DNS is a prime target for attack.

The importance of a strong DNS foundation cannot be overstated. Without one, your customers may not be able to access your content and applications when they want to—and if they can't get what they want from you, they'll likely turn elsewhere.

Growing Pains

DNS is growing especially with mobile apps and IoT devices requiring name resolution. Add to that, organizations are experiencing rapid growth in terms of applications as well as the volume of traffic accessing those applications.

In the last five years, the volume of DNS queries for .com and .net addresses has more than doubled. More than 10 million domain names were added to the Internet in 2016 and future growth is expected to occur at an even faster pace as more cloud, mobile and IoT implementations are deployed.

Security Issues

If DNS is the backbone of the Internet—answering all the queries and resolving all the numbers so you can find your favorite sites—it is also one of the most vulnerable points in your network. Due to the crucial role it plays, DNS is a high-value security target. DNS DDoS attacks can flood your DNS servers to the point of failure or hijack the request and redirect requests to a malicious server. To prevent this, a distributed high-performing, secure DNS architecture and DNS offload capabilities must be integrated into the network.

Generally, DNS servers and DNS cloud services can handle varying amounts of requests per second with the costs increasing as the queries-per-second increase.

To address DNS surges and DNS DDoS attacks, companies add more DNS servers, which are not really needed during normal business operations. This costly solution also often requires manual intervention for changes. In addition, traditional DNS servers require frequent maintenance and patching, primarily for new vulnerabilities.

The Traditional Solution

When looking for DNS solutions, many organizations select BIND (Berkeley Internet Naming Daemon), the Internet's original DNS resolver. Installed on approximately 80 percent of the world's DNS servers, BIND is an open-source project maintained by Internet Systems Consortium (ISC).

Despite its popularity, BIND requires significant maintenance multiple times a year primarily due to vulnerabilities, patches, and upgrades. It can be downloaded freely, but needs servers (an additional cost, including support contracts) and an operating system. In addition, BIND typically scales to only 50,000 responses per second (RPS), making it vulnerable to both legitimate and malicious DNS surges.

ps

Next Step

If you're ready to learn more or dig deeper into DNS, check out these more advanced articles

- DNS - DevCentral Wiki
- Application Layer DNS Firewall
- Lightboard Lessons: DNS Scalability & Security
- DNS Express and Zone Transfers
- DNS Does the Job

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com