

# Easy to Understand DNS

## Easy to Understand DNS

By Paul Parisi, CTO, DNSstuff.com

When asked about the Domain Name System (DNS), most have heard about it, but in the same breath, could not tell you what it is and what it actually does.

DNS is the language of the Internet and translates human language into the language machines use. Everything on the Internet is dependent on DNS, and DNS controls the communication online. Just like conversations are dependent on clear and straight forward communication, DNS communication demands the same. When the words aren't understandable, the conversation collapses. The critical flaw in DNS discovered by Dan Kaminsky earlier this year is a perfect example of how communication must be clear. It only takes one vulnerability to take the Internet down.

## DNS and How it Works

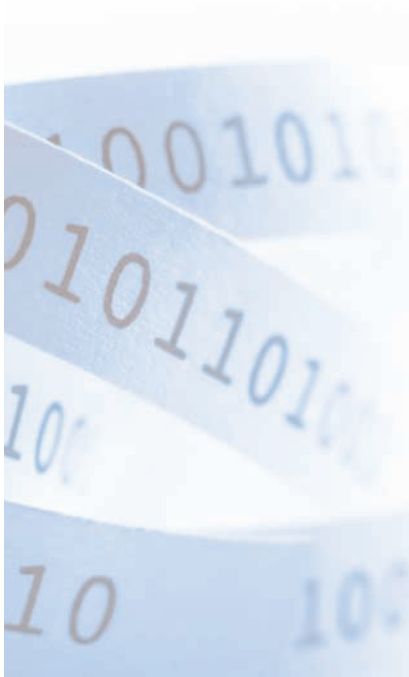
The best way to understand how DNS works is by how we give directions to another person. If you ask your friend to join you at your home for dinner, unless he knows the exact directions, he will never arrive there. The same goes for DNS. The Domain Name System is the way the Internet translates names that are read by humans, such as; [www.dnsstuff.com](http://www.dnsstuff.com), into numeric addresses for Internet destinations (IP addresses) such as; <http://72.21.210.11>.

The Internet must give detailed directions in the same way you would give detailed directions to your friend who is coming to your house for dinner. When a server needs to bring up a Web site in your browser, it must have the IP address of the server where the Web site lives. DNS is used to find the address, make a connection, and retrieve the Web site content. There are two aspects to this – DNS resolution and routing.

Resolution is being able to reach the same destination no matter what route you decide to take. The Internet houses numerous networks, with their own address spaces similar to streets and house numbers. Getting to where you need to go is dependent on the initial lookup of the destination's address. The initial lookup of the address is so important. If your friend looks up the wrong address, he will never reach your house.

Caching is the next step. Caching is how DNS keeps track of its inquiries and remembers them for a designated period of time. So, the first time you type in your inquiry, you may be referred to three servers, but the next time you provide the same inquiry, you will be given the same answer since it remembers your question.

As you can see, DNS plays the role of the phone book for the Internet. This is an important role that shouldn't be taken lightly.



# Easy to Understand DNS

## DNS Security Concerns

DNS should not be classified as one large phone book, but a series of related phone books. When your computer contacts a DNS server regarding an address, like DNSstuff.com, if that particular server doesn't know the Web site, it will ask another DNS server until you are routed to DNSstuff.com. During this process, security issues must be considered.

When people and technology coincide, DNS and the information given can be compromised. As each server is prone to breaches, those servers must constantly be monitored to mitigate malicious activity. This can be a huge challenge for IT administrators. Since there are so many DNS servers controlled by any number of people, just one human error can create critical problems that will travel through the Internet.

Innocent human error isn't the only issue that IT administrators have to worry about. There are much more sinister people at work, such as hackers and cybercriminals waiting for the perfect moment to attack your DNS. There are many ways that servers can be exploited. Hackers can hold you back from where you need to go on the Internet, and they can also make you think you have reached your destination by making the address you typed in look just like the site you thought you requested.

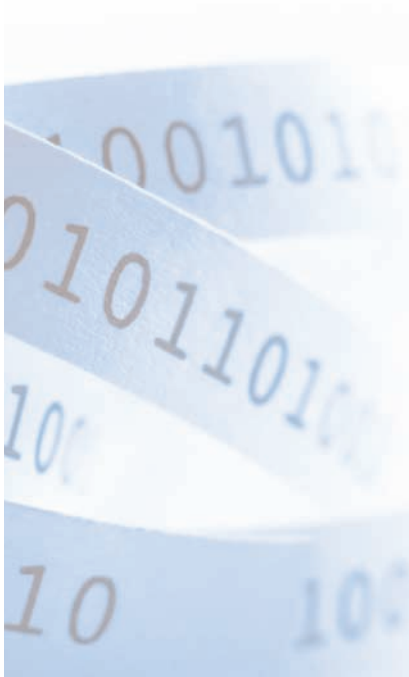
## Mitigating DNS Security Issues

Attacks cybercriminals use to exploit DNS include:

- Spoofing
- DNS Hijacking
- DNS Poisoning
- DDOS Attacks
- Fraud and Proxy Redirection – aka Man-In-The-Middle attacks

Some of these attacks are similar such as spoofing, DNS Hijacking and DNS Poisoning. Each attack tricks a DNS server into giving out the wrong address – mis-populating the server cache queried. Being redirected and connecting to the wrong IP address – especially a proxy server can cause a detrimental outcome if the record of information you transfer ends up in the wrong hands.

Distributed Denial of Service or DDOS attack is a more simplified attack than those mentioned above. A DDOS attack is comparable to having several people call one phone number repeatedly at the same time. It would be difficult to block the calls, just as it would be difficult to block many DNS queries of a server in a short period of time. This is a good example of why you should not allow your DNS servers to answer recursive queries for anyone on the Internet. Blocking outsiders from making recursive queries to DNS servers greatly reduces your risk for a DDOS attack.



# Easy to Understand DNS

## DNS Security – What You Can Do

DNS is undoubtedly one of the most important technologies an organization will ever use. At the same time, most people don't work with it on a regular basis and just assume it will always be working. As we have discussed, DNS issues can create enormous problems for businesses that rely heavily on the Internet. When an IT person has to deal with DNS issues, it is usually after a problem has occurred. As most IT administrators understand the complexity of DNS, this complexity can make even the best administrator question how they are solving an issue.

The highly distributed nature of DNS can also further complicate problem solving as there are always unknown ramifications. The DNS system is fundamentally based on trust. However, both malicious activities and human mistakes can significantly compromise the data the system holds. The question on every administrator's mind is, what can we do to mitigate compromised data and keep the DNS system secure?

You must implement a simple change control process and have a limited number of people who are allowed to make changes to the DNS. The administrator must document and communicate changes in real time and monitor and test what your DNS is doing and how it is answering. Good monitoring of your DNS will give you a more confidence in security your system – it is imperative to trust, but validate all information.

