# DNS is Like Your Mom

**Lori MacVittie, 2011-24-01**

*Both are taken for granted but provide vital services without which you and your digital presence would be lost. In the case of DNS, that should be taken literally.*


### Mom. She's always there, isn't she?

She kissed away your bumps and bruises. You treated her like Google before you had access to the web and, like Google, she came through every time you needed to write a report on butterflies or beetles or the pyramids at Giza. You asked her questions, she always had an answer. You didn't spend as much time with her as you grew older (and discovered you knew way more than she did, didn't you?) but when you needed money or life kicked you in the face, she was there for you, as always. Steady, reliable, good old mom.

You'd be lost without her, wouldn't you?

Go ahead – give her a call, shoot her an e-mail, write on her Facebook wall, order some flowers. I'll wait.

Now that we're ready, consider that there are some components of your infrastructure that are just as valuable to your organization's digital presence as your Mom is to you. Unfortunately we also tend to take them for granted.

## TAKEN FOR GRANTED

**DNS is rarely mentioned these days except when it's the target of an attack. Then we hear about it and for a few moments DNS is as it should be – a critical data center service. It's like Mother's Day, only without the dandelions posing as flowers and Hallmark cards.**

But once the excitement over the attack is over, DNS goes back into the bowels of the data center and keeps chugging along, doing what it does without complaint, patiently waiting to be appreciated once again.

Okay, okay. Enough of the guilt trip. But the truth is that DNS is often overlooked despite its importance to just about everything we do. It is the first point of contact with your customers, and it is the gatekeeper to your entire domain. Without it, customers can't find you and if they can't find you, you can't do business. It's the cornerstone, the foundation, the most critical service on the Internet. And yet it remains largely unprotected.

The reasons for that are many, but primarily it's because DNS needs to interact with the public, with the unknown. Its purpose in the architecture of the Internet is to be the authoritative source of where a given service resides. Queries to the root servers happen on the order of millions of times ***a second***. Other DNS services are similarly stressed.

There are two primary concerns for DNS:

1. Load
2. Authenticity

Load is a concern because it's possible to "take out" a DNS server simply by overloading it with requests. It's a denial of service attack on your entire organization that takes away the ability of clients to find you; making you all but invisible to the entire Internet. The second problem is one that's more recent, but just as dangerous: authenticity. This issue speaks to the ability to "hijack" your DNS or poison the cache such that customers looking for your latest gadget or service or what have you end up listening to Justin Bieber instead.

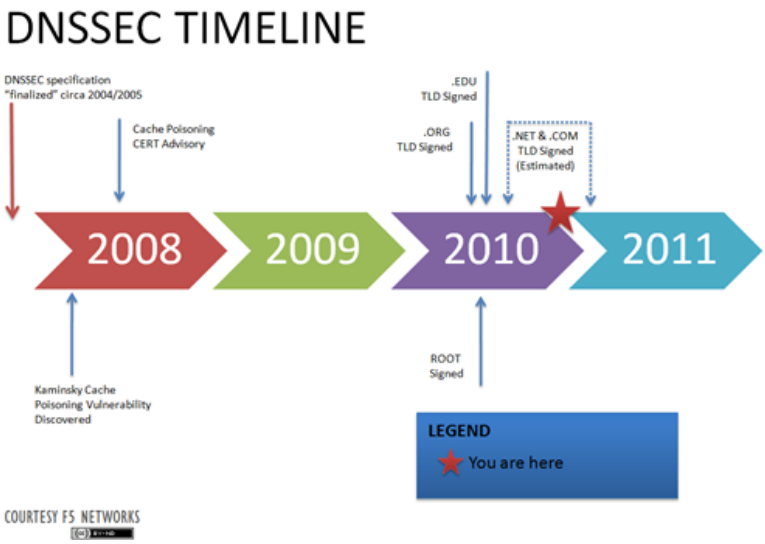
Okay, maybe that's too harsh an image. Maybe they redirect to a competitor's site, or to a porn site, or something less horrifying than Bieber. You get the picture – it's bad for you and your organization's reputation when this happens.

Point is, your DNS services can be hijacked and the result is that your sites and applications are effectively lost to the general public. Customers can't find you, remote or roaming employees can't access business critical applications, and you might find yourself associated with something with which you'd rather not have your organization tied.

## DON'T MAKE DAD ANGRY

### Your DNS infrastructure is critical. DNS itself is an aging protocol, yes, but it does what it's supposed to do and it does so in a scalable, non-disruptive way. But it does need some attention, particularly in the area of load and authenticity.


To help relieve some of the stress of increasing load and the potentially devastating impact of an overload from attack, consider the benefits of load balancing DNS. Load balancing DNS – much in the same way as load balancing web services and applications – provides a plethora of options in architecture and resource distribution that can address heavy load on DNS infrastructure. cloud computing can play a role, here, if the DNS services are virtualized in the architecture by an upstream application delivery solution. The strategy here is to scale out DNS as needed to meet demand. That's of particular importance if the upstream components (if there are any) are not capable of detecting and responding to a DNS-based DDoS attack. It'll cost you a pretty penny to scale out your DNS farm to respond, but on the scales balancing uptime of your entire digital presence with costs, well, even the business understands that trade-off.




Don't discount the impact of a dynamic data center on DNS. DNS wasn't designed to be constantly updated and yet the nature of highly virtualized and cloud computing environments requires just that – rapid changes, frequently. That will have an impact on your DNS infrastructure, and can negatively impact the costs associated with managing IP addresses. This is the core of the economy of scale problem associated with the network in relation to cloud computing and virtualization. It's why automation and orchestration – process – will become critical to the successful implementation of IT as a Service-based initiatives. Yet another facet of DNS that might have been thus far overlooked.

To address the Justin Bieber problem, i.e. hijacking or poisoning of a DNS cache, implement DNSSEC. It's one of the few "new" standards/specifications relating to DNS to hit the wires (literally) and it's a good one. DNSSEC, if you aren't familiar, leverages the foundation of a public key infrastructure to sign records such that clients can be assured of authenticity. Because miscreants aren't likely to have the proper keys and certificates with which to sign responses, hijacking your name services really can't happen in a fully DNSSEC-compliant world.

Problem is, it's not a fully DNSSEC compliant world. Yet. Movement is slow, but the root servers ***are*** being protected with DNSSEC and that means it's time for organizations everywhere to start considering how to implement a similar solution in their own infrastructure. Because it's quite possible that one day, clients will reject any non-secured response from a DNS service. And if you think your mom feels bad when you don't answer her calls (damn caller ID anyway) your DNS service will feel even badder. Or the business will, which is probably worse – cause that's like your dad getting on your case for not answer your phone when your mom calls.

## DNS CRITICAL to CLOUD-BASED STRATEGIES

**As we continue to move forward and explore how IT can leverage cloud-based compute to extend and enhance our IT strategies we find more and more that DNS is a critical component to those strategies.**

Extending the data center to include external, cloud-deployed applications requires that customers be able to find them – which means DNS. When migrating applications between locations for any reason, DNS becomes a key player in the move – ensuring new and existing connections are properly directed to the right location at the right time. DNS is one of the core technologies required to implement a cloud bursting strategy. DNS is the foundation upon which dynamic and mobile compute can be leveraged both internal and external to the data center.

DNS is key to cloud computing, whether it's public, private, or hybrid.

DNS is old, yes. It's outdated, yes. It is like just like your mom. And like your mom, it should be treated with the respect it deserves given its critical role in just about every facet of your organization's digital "life".

- It's DNSSEC Not DNSSUX
- VeriSign: We will support DNS security in 2011
- New DNS exploit now in the wild and having a blast
- The Official, Unofficial, DNS Security Extensions Blog
- The End of DNS As We Know It
- Taking Down Twitter as easy as D.N.S.
- Building a Cloudbursting Capable Infrastructure
- Cloud Balancing, Cloud Bursting, and Intercloud
- Achieving Enterprise Agility in the Cloud (Cloudbursting with VMware, BlueLock, and F5)
- DNSSEC: The Antidote to DNS Cache Poisoning and Other DNS Attacks
- DNSSEC Solutions
- DNSSEC: Compliance is Easier Than you Think

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