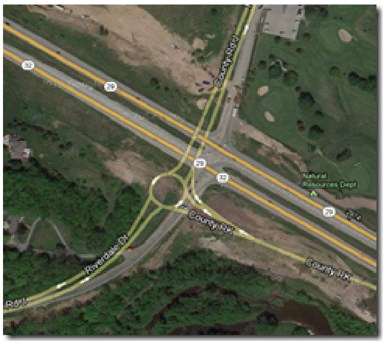
Let me tell you Where To Go.

Don MacVittie, 2012-09-08



One thing in life, whether you are using a Garmin to go to a friend's party or planning your career, you need to know where you're going. Failure to have a destination in mind makes it very difficult to get directions. Even when you know where you're going, you will have a terrible time getting there if your directions are bad. Take, for example, using a GPS to navigate between when they do major road construction and when you next update your GPS device's maps. On a road by my house, I can actually drive down the road and be told that I'm on the highway 100 feet (30 meters) distant. Because I haven't updated my device since they built this new road, it maps to the nearest one it can find going in the same direction. It is misinformed.

And, much like the accuracy of a GPS, we take DNS for granted until it goes horribly wrong. Unfortunately, with both you can be completely lost in the wild before you figure out that something is wrong.

The number of ways that DNS can go wrong is limited – it is a pretty simple system – but when it does, there is no way to get where you need to go. Just like when construction dead-ends a road. Like a road not too far from my house. Notice in the attached screenshot taken from Google Maps, how the satellite data doesn't match the road data. The roads pictured by the satellite actually intersect. The ones pictured in roadway data do not. That is because they did intersect until about eight months ago. Now the roadway data is accurate, and one road has a roundabout, while the other passes over it.

As you can plainly see, a GPS is going to tell you "go up here and turn right on road X", when in reality it is not possible to do that any more.

You don't want your DNS doing the same thing. Really don't.

There are a couple of issues that could make your DNS either fail to respond or misdirect people. I'll probably talk about them off-n-on over the next few months, because that's where my head is at the moment, but we'll discuss the two obvious ones today, just to keep this blog to blog length.

First is failure to respond – either because it is overloaded, or down, or whatever. This one is easy to resolve with redundancy and load balancing. Add in Global Load Balancing, and you can distribute traffic between datacenters, internal clouds, external clouds, whatever, assuming you have the right gear for the job. But if you're a single datacenter shop, simple redundancy is pretty straight-forward, and the only problem that might compel you to greater measures is a DDoS attack. While a risk, as a single datacenter shop, you're not likely to attract the attention of crowds that want to participate in DDoS unless you're in a very controversial market space. So make sure you have redundancy in DNS servers, and *test them*. Amazing the amount of backup/disaster recovery infrastructure that doesn't have a regular, formalized testing plan. It does you no good to have it in place if it doesn't work when you need it.

The other is misdirection. The whole point of DNS cache poisoning is to allow someone to masquerade as you. wget can copy the look-n-feel of your website, cache poisoning (or some other as-yet-unutilized DNS vector) can redirect your users to the attacker. They typed in your name, they got a page that looks like your page, but any information they enter goes to someone else. Including passwords and credit card numbers. Scary stuff. So DNS SEC is pretty much required. It protects DNS against known attacks, and against a ton of unexplored vectors, by utilizing authorization and encryption. Yeah, that's a horrible overstatement, but it works for a blog aimed at IT staff as opposed to DNS uber-specialists. So implement DNS SEC, but understand that it takes CPU cycles on DNS servers – security is never free – so if your DNS system is anywhere near capacity, it's time to upgrade that 80286 to something with a little more zing. It is a tribute to DNS that many BIND servers ***are*** running on ancient hardware, because they can, but it doesn't hurt any to refresh the hardware and get some more cycles out of DNS.

In the real world, you would not use a GPS system that might send you to the wrong place (I shut mine down when in downtown Cincinnati because it is inaccurate, for example), and you wouldn't use one that a crook could intercept the signal from and send you to a location of his choosing for a mugging rather than to your chosen destination… So don't use a DNS that both of these things are possible for. Reports indicate that there are still many, many out of date DNS systems running out there. upgrade, implement DNS SEC, and implement redundancy (if you haven't already, most DNS servers seem to be set up in pairs pretty well) or DNS load balancing. Let your customers know that you're doing it more reliable and secure – for them. And worry about one less thing while you're grilling out over the weekend. After all, while all of our systems rely on DNS, you have to admit it gets very little of our attention… Unless it breaks. Make yours more resilient, so you can continue to give it very little attention.

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113