52 hours that felt like 52 days

Wednesday was when the problem started, but it seems like I've been wrestling with this for weeks. One way to get people to sit up and take notice is to make their e-mail server and website go away and not return for 52 hours.

Between 10 and 11 Wednesday morning, an explosion and fire at a datacenter in Parsippany, New Jersey, caused the evacuation of Network Access Corporation, the company that Akashik (my website host and the host for many clients and several acquaintances) had hired to maintain its servers.

Where did the websites and e-mail go?

Within 2 hours, the fire department had allowed people back into the building, but power was off to some areas for most of the day. Many of the servers came back on line normally. The 8th floor (I presume this was the location of the explosion and fire) remained unusable for longer.

The server that my sites and my clients' site live on were back on line, but Akashik's "nameserver" machine (the "traffic cop" of the operation) would not start. Because of that, nobody could reach the web or mail servers by using a domain name.

According to Greg Moore of Akashik, the nameserver had suffered a hard disk failure and would have to be rebuilt, so he decided "to best make use of this downtime and shift accounts to another datacenter. … The result is that once the nameservers resolve, accounts will be on brand new servers sporting both twice the CPU power and RAM within a datacenter we've found to offer greater connectivity."

Move already planned

Akashik had planned to make this move soon, although under much more controlled circumstances. As I mentioned to someone earlier in this ordeal, what we had was the equivalent of a "100-year flood".

As of Friday morning at 8a.m. (Eastern), Greg reported that some domain name service (DNS) servers had started to direct traffic to the new datacenter. Roadrunner's DNS seems to always be at least 12 to 24 hours behind everyone else's DNS, so I wasn't seeing any change as late as Friday evening.

On Thursday, before I had been able to contact Greg and was uncertain what exactly was happening, I made arrangements to move some websites temporarily to a small server. I ordered DNS changes on Thursday morning. Thursday afternoon, Greg and I located each other and compared notes. It no longer made sense to use the smaller server, even temporarily, but I had already submitted the DNS changes. I submitted a second round of changes to restore the old information.

If there was irony in the fact that the explosion was the result of an uninterruptible power supply gone bad, there was further irony that in attempting to restore service faster by temporarily moving sites to an alternate server, I delayed the return of some sites – including my own.

Isn't the Internet "fail-safe"?

Yes, it is. At least it's intended to be. In fact, it is not impervious to multiple catastrophic failures or even something so blindingly simply as multiple distributed denial-of-service attacks. But the Internet is designed to protect itself. Individual machines are not. Individual datacenters are not.

Communications on the Internet are routed by intelligent devices so that the failure of a router in Columbus, for example, won't affect traffic from Cleveland to Cincinnati. The traffic may travel from Cleveland to Pittsburgh and then to Cincinnati, but it will get there. (In fact, when I connect to a client's Unix system that's no more than 2500 feet from my office, the connection is made from Columbus to Washington to New York to Chicago and back to Columbus – which is well over 2500 feet!)

Cut any individual cable and the Internet's redundancy is able to route around the cut. That's why large datacenters (such as Network Access) maintain multiple connections to the Internet. Most datacenters buy service from MCI, Sprint, Broadwing, AT&T, and others. A massive failure at any one provider won't leave them without service.

But a well-placed back-hoe cut will. All of the cables enter the building at one place. Cut there and you will have taken the datacenter off the network.

An explosion and fire will do the same thing. Believe me; I know very well.

Planning for the future

For me and for most of my clients, there is no pressing need to have a "hot" backup site ready to go at a moment's notice, but there are two things we can do to ensure that future disruptions will be resolved faster.

NOW what??

Dead Trees seemed to be a somewhat negative name for this publication. Starting with this issue, the new name is *Random Thoughts*, suggesting – if not deep analytical articles – that at least minimal thought during development of the articles. Please note that I still bear no particular animosity toward trees.

If e-mail is essential to your business, there are extra-cost options available from most hosts or from third-party vendors to back up inbound mail. When the regular server is down, the service accepts mail and holds it until your server is ready to accept it again or until you give it a different server for delivery.

For those with less critical needs, simply obtain an extra e-mail address from your Internet service provider. When all of my @blinn.com addresses were unavailable, I was still able to communicate using my Roadrunner account.

If you don't have access to a standard e-mail account from your ISP, consider a $6-per-month account from access4less.net. I have an account with this company solely for access when I'm traveling. When I'm in town, I have Roadrunner at home and a very large pipe at the office.

Yet another option would be a free e-mail account from Yahoo or one of the other providers of Web-based mail. As a last resort, use AOL.

Some computer systems absolutely must be available without fail. Airline reservation systems and, to a slightly lesser extent, their website components are in this category. At the other end of the spectrum is a website like my technology-corner.com. I'm unhappy when it's down, but it's something I provide solely to offer supplemental information for the radio show. If it's down for a week, it's an inconvenience; it's not a catastrophe.

Millions of websites exist between those extremes. Any website that's used for commerce should probably have a hot backup site. (By "hot", I mean that everything needed to run the site is there and functioning all the time. Moving to the backup site requires nothing more than a router change.) Doing this is, however, quite expensive.

My recommendation for most people is to maintain at least one full copy of your website on a local PC. If you're a client, your website is on the web server, on the web server's backup, on my local machine, and on my backup (located off-site).

Having a full copy of the working site allows you to sign up with a different service provider in the event that your primary host suffers an explosion, fire, or tornado – or has something else happen that takes them off the air.

Ol' devil DNS

Most website hosts can set up a new site in an hour or less, so making a website ready from a backup copy is quick and easy. The problem is the 24 to 72 hours that it takes for DNS information to propagate across the Internet.

Instead of depending on standard DNS propagation, this event suggests that it makes sense to buy nameserver service from an outside vendor. This means that routing will no longer depend on the combination of DNS tables from Network Solutions and the nameserver at the website host.

By maintaining your own DNS server (or hiring someone to do it) it's possible to move a website from one host to another and to have all the DNS information updated within a few hours. This can be done for probably about 1/100th of what it would cost to operate a hot backup site.

The ability to recover from a catastrophe within a few hours for a cost of less than $200 per year sounds a lot better to me than nearly instantaneous recovery for many thousands of dollars per year. ß

WinZip's latest: better

WinZip has been my favorite file compression utility since it arrived on the scene in 1991. Remember ARC? Remember PK-Zip? PKWare is still around, but the new version of the product costs nearly $100 (discounts drop that to $80.) The product is available for many operating systems, too. But if you're a Windows user, you're probably familiar with WinZip.

Version 9 is available as a free **beta** version you can download from www.winzip.com and the company will continue one of the most unusual practices in the software industry when version 9 is released: Any registered user will be able to download the new version and use it for free. This is what WinZip has done since 1991 and I don't know how they continue to do it. Any registered user of any earlier version of the product gets the new product for no additional charge.

WinZip 9 adds encryption – both 128-bit and 256-bit. Users may also create files in the original zip format or a new 64-bit zip format. The new format removes all size restrictions. The previous version was "limited" to no more than 65,535 files in a zip and no individual file could be larger than 4GB.

My favorite new feature addresses a usability problem with previous versions. The user interface is greatly improved by the addition of an Explorer-like look that lets users choose where to zip or unzip files. For the folks at WinZip – BRAVO! Again. ß

on the market by A.J. Stinnett

CORNER

"Give your people a complete job, a measure of autonomy, a client, feedback from the client, and they will move heaven and earth for you."