



## **When Networks Attack!**

*By John D. Smaling, Practice Director*

I recall not too many years ago when ATM was the solution to our network's bandwidth and redundancy woes. I also recall how complex LES/BUS and LECs were to grasp conceptually, and to actually configure and maintain. It was quite a relief when gigabit Ethernet technology became the de facto standard and shortly thereafter, routing at the core and Layer 3 at the distribution layer. Life became much, much easier. But have we taken this simplicity for granted? I believe that we have.

When something installs as easily as much of today's networking technology, it's easy to assume that it will run unchecked for years to come. As a consequence, many networks installed three or more years ago are ticking time bombs, waiting for just the right opportunity to make us pay for our casual neglect. This is particularly ironic when one considers the dollars and time invested in implementing clustered servers and highly redundant mass storage solutions to provide utility-like service to the end user community. In spite of these investments, there isn't a single network attached device, regardless of its level of redundancy that will remain accessible in the event of an enterprise-wide failure of the network.

To that end, it might be prudent to review what we at Vitalize Consulting Solutions, Inc. consider the top network issues that, left to their own devices, will eventually ruin your day(s), and make every network administrator feel like they've been parent to a latchkey child.

### **Spanning Tree Issues**

Designed for the explicit purpose of providing network failover, it's sardonically humorous that problems related to spanning tree are a common source of crippling network issues. As networks grow and expand, new additions to their distribution and/or access layers involve providing dual uplinks for redundancy purposes. Failure to enable spanning tree on these links can be a fatal mistake. The absence of spanning tree associated with redundant uplinks to the same device, or interconnected devices creates a physical network loop; a problem in every sense of the word. Furthermore, loss of identity of the spanning tree root to an oversubscribed or incapable device can cause undesirable results as well.

### **Physical Loops**

We've already discussed how physical loops can be created when redundant uplinks to the same, or interconnected devices, fail to have spanning tree enabled. However, physical network loops can occur for several reasons, not the least of which relates to a poorly documented or unstructured cable plant. How many times have you completely overhauled and documented the cable plant in your organization? Odds are the answer is a resounding "never". As a consequence, ceilings in healthcare organizations are bowing under the weight of fiber and unshielded twisted pair, or dare I say, twinax! This bowl of spaghetti, coupled with outdated or non-existent documentation virtually guarantee that, sooner or later, an engineer is going to plug in or patch a cable that creates a physical loop.

### **Port Duplexing Issues**

Today's networks support hundreds, if not thousands, of Ethernet connected devices of many shapes and sizes. Among the diversity of the connected entities, many of them differ in their speeds and duplex characteristics. Duplex or half-duplex? Ten megabits per second or 100 megabits per second? How about Auto-Detect? The latter is clearly the flavor of choice by today's network engineer. However, some devices, such as certain modalities, or older equipment, require us to explicitly match the speed and duplex settings on the hub/switch, with that of the device's Ethernet interface. Sometimes, a weary engineer makes a mistake when installing the device. Other times, furious move, add, and change activity results in hub/switch ports no longer matching the device that we just switched to that port. As more and more mismatches mount, collision and retransmission rates also multiply and eventually.....someone notices.

### **Patches & Software Release Currency**

Software updates don't apply to just applications and operating systems. Virtually every network component is managed by, or functions because of, software. Code is continually improved, bugs fixed, security holes filled, and new functionality enabled in the form of software releases. These improvements are generally

reactionary responses to the appearance of new products, functional requests, or newly discovered malicious attacks. Whatever the reason, it is generally a good idea to maintain pace with these updates. With extremely rare exception, a well managed network is never more than 2 releases behind. Is your network well managed?

## Security

Let's pretend that your network team is understaffed and overwhelmed with work requests. Now let's assume that one of those overwhelmed network engineers has to add a new switch to closet 201N. He pulls a Cisco 2960 from inventory, cracks the carton's seal, rack mounts it, plugs it into the PDU in the rack, fiber patches it to the appropriate uplink, labels it, TFTP's the latest software, and updates the closet's documentation. Good job right? Wrong! In his haste, he fails to modify the switch's enable password, and he also neglects to modify the read and write community strings on the device. Overlook either one of those steps and you're exposing holes in an otherwise carefully crafted security strategy. It's the little things that kill you, and this is a common "little thing".

These items are but a few of the more chronic kinks in your network's armor. As time progresses, these are certain to accumulate and will undoubtedly manifest themselves in an unscheduled "event". Other items that you might encounter are:

- Overloaded core components (core switches/core routers) with insufficient memory or address table limitations.
- Hop Count Issues
- Un-retired static routes or antiquated routing protocols
- Closet disorganization
- Outdated network management applications

Somewhere out there are sufficiently staffed and well organized network teams who appropriately monitor and manage their enterprise environments. These teams are rare exceptions indeed. Most of us are the beleaguered owners of limited budgets, undersized staff, and too many projects to handle thoroughly. However, these factors fall on deaf ears when you use them to justify persistently poor performance, unreliability, or worse, a protracted enterprise outage. What can you do?

Fresh eyes can do wonders to uncover issues lurking beneath the surface of your network. This doesn't always have to come from outside consultants (although this author favors that approach!). A newly hired network engineer can provide invaluable insight to the team by completing, as his first assignment, an enterprise network assessment. IT departments of different organizations often exchange information and, despite the competitive nature of their overarching businesses, there is a spirit of cooperation among competing hospitals. Given this level of collaboration, it is possible that your neighboring hospital's network team and your own team might provide assessment services to one another on a periodic basis. This is clearly not for everyone, but given the relationship among local healthcare facilities, it can be an effective strategy.

Assessments should be annual events, just like yearly health check ups make sense for you and me. However, just because we get an annual check up doesn't mean that we'll live forever. Neither will your network. Equipment wears out over time. Furthermore, network vendors generally innovate such that disruptive technological change occurs roughly every five years. As a consequence, proactive organizations will plan for a network design and some level of refresh every fifth year.

We live in challenging and hectic times. The clinical systems revolution has placed emphasis on computing resource availability like never before. Expectations of utility level reliability of information systems are absolutely warranted, but these expectations come with a price. The price manifests itself in the investments necessary to acquire and build first class infrastructure, and also the investment necessary to care and feed that very same infrastructure. Annual health checks and proactive refresh strategies are fundamental to maintaining a reliable and high performance enterprise network. I would welcome the opportunity to speak with you on this subject and other technology solutions that Vitalize Consulting Solutions, Inc. could provide. Call me at 610-444-1233 or email me at [jsmaling@getvitalized.com](mailto:jsmaling@getvitalized.com).