



Vendor Diversity is Critical in Network Deployments

The Security and Cost Benefits

He who fails to learn the lessons of history is doomed to repeat it...

If one examines the current state of the IT industry, you can quickly see that the important message conveyed by this quotation is being overlooked. Specifically, we see wide deployments of common systems, each with nearly identical software. We see common exploits or flaws being found with these “standardized systems”, and these exploits being used again and again with devastating effect. It seems as if the lessons of history have not been learned. Redundancy should apply to your vendors, not just your network.

There is also an opportunity to reduce capital expenditures on network investments by 20-35% according to Gartner's vendor influence curve research. Let's face it...nobody ever gets fired for buying the “safe choice” for networking. Yet the “safe choice” doesn't always keep you safe as the examples below will illustrate. In fact, Gartner estimates enterprises are wasting \$15 billion per year sole-sourcing their networks to the “safe choice”.

Let's go back to Monday, 13 April 1998 at around 15:00 EST. At that time, the AT&T Frame Relay network crashed with spectacular effect – 6,000 multinational customers had their Internet connections concurrently rendered useless. The effects of this were catastrophic. Not only were business-to-business communications affected, but so were ATM cash point machines for consumers and credit card transaction processing for retailers. AT&T customers lost millions due to this incident. AT&T paid penalties in excess of \$US 40 million due to service level agreement violations; and ultimately many customers switched to another WAN provider. AT&T had standardized on frame relay switches from a single vendor. All switches sourced from the same vendor meant that all switches ran the same firmware/software, which was vulnerable to the same bug. When a configuration change to a single switch triggered this latent flaw, it propagated throughout the entire AT&T network in minutes. The entire system crashed worldwide.

Now, let's fast forward to 11 August 2003. On this date the infamous ‘Blaster worm’ was released. Blaster exploited a vulnerability in a Remote Procedure Call (RPC) of the Microsoft Distributed Component Object Model (DCOM). Microsoft proactively had made a patch available on 16 July 2003; and the United States Department of Homeland Security (DHS) even took the unprecedented step of warning the public of the seriousness of this flaw. The impact was widespread – the Atlanta branch of the United States Federal Reserve Bank was forced to shut down most of its computer systems, and the CBS broadcasting corporation was disrupted by Blaster for more than two days. To this day, Blaster traffic is seen on the Internet, five years after its initial release.

Now, let's advance our calendars to 15 May 2007. Nippon Telegraph and Telephone (NTT) suffered a massive Internet outage when between 2,000 and 4,000 routers went offline for over 7 hours, impacting nearly 3 million customers across Eastern Japan. The outage was caused when experimentation caused the routing tables in these devices to overflow. Although the devices should have been able to handle the overflow gracefully, they did not and the traffic forwarding path in the routers stopped working, resulting in the outage. CIBC financial analyst Ittai Kidron asserts that this case “...at the very least highlights the need for two vendors.”

There is a common threat that exists between these seemingly unrelated events. That threat is the weakness caused by uniformity. Let's start with the AT&T frame relay outage. First, AT&T made the choice to implement its entire frame relay network with devices from the same vendor. This inherently created a serious and **common** weakness – the entire infrastructure would be vulnerable to any bug or flaw. In this case, the weakness was triggered accidentally, but we have seen many cases where flaws are exploited maliciously. Some of the responsibility for the widespread impact of this crash should also be borne by the customers themselves – one should not trust a business critical service to a single service provider! Rather, multiple service providers connected via diverse physical path and last mile connections should be considered to ensure business continuity.

The Blaster worm vulnerability is in a class all of its own, given the sheer number of installed Microsoft systems worldwide. Every single system running Windows 2000 or XP had exactly the same flaw; and given the number of systems, a worm such as Blaster can infect thousands of systems per hour. With each passing hour the number of infected systems can grow exponentially. One reason customers explained for the delay in the installation of the Microsoft patch is that larger IT departments do not deploy patches immediately, but rather test them first. Also, often the patches require a reboot – something that needs to be scheduled during maintenance windows on mission critical servers. So, even if a system is not compromised, there is still a real financial cost associated with the IT operations response and testing associated with each vulnerability discovered.

Finally, the NTT event reminds us of the weaknesses associated with deploying a homogenous infrastructure – all parts of the infrastructure will show exactly the same flaws and when stressed accidentally or maliciously will fail in exactly the same way. The experiment caused the routing tables to overflow – which is bad. The routers could not recover and failed by no longer forwarding any traffic – which is catastrophic.

We would like to introduce the concept of **Dissimilarity** – or system diversity. It is a strategy to prevent common mode failures and vulnerabilities such as those described above. Few people practice this important concept, the premise of which is that diverse systems are inherently stronger than homogeneous ones, since the probability of a common flaw is mitigated.

An example from the aerospace industry shows this concept taken to the extreme. The Boeing 777 airplane uses a fly-by-wire system for the flight control systems of the aircraft. The pilot moves a control and a computer receives this as input and actuates the control surfaces appropriately. Given the potential of software or hardware failures, this is a scary proposition. Obviously this worried Boeing too - in addition to making the flight control computer system triple redundant, Boeing introduced system diversity by:

- Specifying three completely unique computer architectures for each of the three redundant computers, including mandating the use of different microprocessors
- Specifying the use of three different software compilers from three different vendors
- Having three distinct “clean room” teams implementing the flight control software
- Locating the equipment in physically separate locations within the aircraft
- Using completely independent and physically separate power distribution sources

And the list of risk mitigation techniques goes on. What Boeing did is ensure that the vulnerability of a common bug was virtually eliminated. Let's bring the discussion back to earth. Although extreme, there is a lot that can be learned from the Boeing example.

Mission critical systems should be implemented with a diverse set of best-in-class suppliers' equipment rather than from a single source. This avoids the risk of common mode failures, and helps thwart attackers at the same time. It also helps to avoid the risk of having an entire infrastructure adversely affected by the spread of a vulnerability. Finally, when a vulnerability is found, it reduces the impact – fewer machines need to be patched, which means that the probability and pace of the patch being applied is greater.

View the network in layers. While you may choose one vendor for the network core or wide area network - you should choose another vendor for the distribution and/or edge layers. This is where a vendor's commitment to standards-based interoperability adds value through certified testing that proves interoperability for Layer 2 and Layer 3 fast path recovery and link-aggregation technologies.

Avoid procuring supposedly redundant services from the same service provider. If you have your primary Internet connection as an E1/T1 with DSL backup and they are both supplied by the same internet service provider, then the Internet connection is not truly redundant. It is necessary to procure connectivity from two providers who do not share the same physical path, last mile connection or backbone in any way.

When making network investments, buyers often select the market leader assuming it is the “safe choice”; even choosing all layers of redundancy from that single vendor. Many times the “safe choice” isn't the best choice, especially if it is the only choice. When it comes to networking technology, the “safe choice” has not always proven to be safe as a number of retailers, government agencies and other universities have found out the hard way. In addition, Gartner's vendor influence curve research estimates enterprises are wasting \$15 billion per year sole-sourcing their networks to the “safe choice”.

Every organization needs to have an alternative networking supplier. Given the opportunity to become the secondary supplier for switching, routing and wireless networking solutions, Enterasys can save an organization 20 to 35 percent on your next networking investment. Don't take our word for it – **schedule a live demonstration today** and we'll show you how we can secure any network without sacrificing performance. We leverage your existing infrastructure investments while protecting the confidentiality, integrity and availability of your information. It all adds up to a solution that is practical, achievable, and delivers rapid time to value.

It is time to exploit the strength of diversity, based on the need for multiple network suppliers.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

