

Diagnosis and treatment of stubborn, insidious, system-wide cyber infrastructure bugs.

Today's networks are pretty reliable. Simple bugs (usually involving a single vendor) are quickly and easily solved. But what happens when the bug is of a systemic nature? When the engineers are scratching their heads with blank looks on their faces? When none of the vendors are willing to admit that the problem may be on their side? When the systems are crawling instead of flying and the clients are screaming for action? What do you do??

Call Litmus Logic, of course! Read the case study to learn more.

Client – Regional Bell Operating Company (RBOC)

Bell X (fictions name for a real company) is a very large regional provider of telephone, network, wireless, and Internet services. Bell X is one of the well known 'telecommunications carriers'. It partners with many other major vendors, such as Sun, Cisco, Juniper, to deliver solutions and it employs a large number of world-class cyber infrastructure experts.

The Challenge

Bell X had entered into a contract with the state government to provide content filtering services for a large number of organizations, including public schools. This was a multi-year, multi-million dollar contract. The amount of information that the system had to filter was huge -- there were 4,000 or so Internet connections that were to be aggregated into to the filtering system. Thus, the solution was built using carrier-grade hardware purchased at carrier-grade price. The solution did not work. It couldn't handle the load. No one could figure out why -- according to the specifications, the system should not even have 'broken a sweat'. Worse yet, no one was able to duplicate the failure in the lab -- in the carrier-class equipped lab, using that same carrier-based equipment and world-class load generator to simulate the customer base. After 4 months of four different major, very well known hardware and software vendors making very little progress toward a fix, Litmus Logic was brought in to troubleshoot. By that time, Bell X was already penalized as per the non-performance clause of the contract and was paying over \$50,000 in contract penalties each month. In addition, Bell X was less than 60 days from completely defaulting on the contract -- the system failed so often that its deployment was halted after only a few hundred sites. Bell X badly needed someone to do some right things fast, which is of course what Litmus Logic is very well known for.

The Solution

Big nails require big hammers. Litmus Logic expert that came to the rescue has more than 20 years of experience in the technology and the business of cyber infrastructure and is a 10 year CCIE veteran.

The Result

Within 3 days of engagement, Litmus Logic expert identified a temporary measure that was implemented immediately. The measure increased the stability of the system to the point where Bell X no longer had to pay the penalties, and could proceed with the deployment. Everyone took a deep breath -- the contract default was no longer looming -- it has moved off. Still, the problem of capacity needed to be solved, as the temporary measure did not provide all the required functionality. Litmus Logic expert was still on the job and within 4 more days he duplicated the problem in the lab. Another few days of testing and the problem was fully understood by everyone, Bell X as well as the vendors. Two teams were assigned to come up with two new solutions trying to salvage as much of the already used equipment as possible. Bell X requested that Litmus Logic expert stay engaged and guide the process until Bell X was sure that the new solution fits the bill.