Pipeline

Knowledge Is Power

www.pipelinepub.com **Volume 4, Issue 4**

An Apple A Day...

by Tim Young

The coffee was particularly good that morning, and they had ordered just the right number of bagels. Good thing. No one likes a stale bagel. Everyone was assembled in the conference room. The prospectus packets were glossy and perfect. The morning meeting was going smashingly. All that's left is to bring in the video conference feed from the Vienna office to press a few of the finer points and these potential clients would be sold.

"Coming to us from across the pond we have Klaus Schweitzer. Are you with us, Klaus?"

Problem. Klaus is not with them. The video is pixelated and shabby. The voice feed is filled with jerks, pops, and gaps. Then static. Then silence.

While any good office can laugh off and work around a few technical difficulties, there will no doubt be hell to pay when the phone rings in the service providers' customer service office. A series of nasty scenes that may have been avoided with proper attention to the health of the network.

How can SPs avoid phone calls from frustrated subscribers (or possibly former subscribers?) like this? Through complete and forward-looking pre-deployment testing, proactive system monitoring, and real-time analysis and fault management.

Look before you leap.

One surefire way to end up in a lurch with your network is to improperly test the network prior to deployment. Basic testing to ensure that all the moving pieces are in order is clearly not enough. This must be done in conjunction with research and analysis that will show that the current network is able to handle not only today's traffic... but tomorrow's as well.

What's more, with the growth and proliferation of denial of service (DoS) attacks, the capacity of the network is an even more crucial component to avoiding downtime and maximizing customer satisfaction. While protection from DoS and DDoS (distributed DoS) attacks can be found in security software from companies like Narus, testing the effects of DoS attacks on the network in a lab environment can also be fantastically useful.

As Marc Robins of Robins Consulting said in a report appearing on the website of, and presumably commissioned by, network testing firm Spirent, prior to deployment:

> “...your company has never had access to the volume of communications you are about to introduce to it. How will you ever simulate the load these demanding applications will place on your network? You need a solution that can replicate the countless scenarios you will be introducing to your network and help you to understand the process of prioritization and load balancing. You need a holistic testing approach, or your network runs the risk of becoming as fragmented as the voice packets in your CEO's important SIP phone call – just before it gets dropped from the network entirely.”

Through effective use of such testing technology, the likelihood of such scenarios can be minimized.

Keeping an eye on things.

Still, no matter how much planning you do, stuff, to clean up a common phrase, happens. Therefore, real-time network monitoring is essential. There has been a recent push among network monitoring types to sing the praises of NetFlow, and advertise their inclusion of the open (yet still proprietary) network protocol in their solutions. So why the recognition of the Cisco brainchild now? It isn't particularly new.

It's because companies are catching on to how crucial diagnosis really is. Zeus Kerravala of Yankee Group has been quoted as saying, "More intelligent management systems can cut the mean time to identification way down, so use of NetFlow can provide more intelligence." More intelligence is good intelligence.

According to Han Hee Song of the University of Texas and Praveen Yalagandula of HP Labs, “measuring real-time end-to-end network path performance metrics is important for several emerging distributed applications such as content distribution and file sharing systems (e.g., CoDeeN, BitTorrent, and KaZaA), interactive media streaming systems (e.g., Video conference systems such as HP’s Halo and Cisco’s Telepresence), traffic engineering (e.g., for supporting IP Telephony), and overlay networks (e.g., RON and OpenDHT).” In their paper, “Real-time End-to-end Network Monitoring in Large Distributed Systems,” the stated conclusion supports a goal of promoting real-time end-to-end monitoring “while ensuring that the measurement overhead is only a small fraction of free node and network resources.” Thus, the monitoring solutions do not become so bulky as to defeat the purpose of network optimization through monitoring.

A little automation to help with the cleanup.

When the network is thoroughly monitored and any faults can be identified and isolated, there comes the need for correction of these faults in a timely manner. The traditional method for identifying and zapping the problem involved lots of grunt work and, in many cases, truck rolls that were not necessary in the long run. Fortunately, drill down capability has developed to the point where problems can be more thoroughly isolated and, as a result, more painlessly eliminated.

As with so many facets of telecom, automation is making the task of discovering, diagnosing, and repairing a fault considerably easier by removing that pesky little aspect known as "human error" or, for that matter, any sort of human interaction at all. We now have the prospect of networks that are, in effect, self-healing. For more details on the once and future prospects of that compelling and exciting area of network management, take a look at the other articles in this month's issue of Pipeline.

In the end, it all comes down to proactivity. In the quest for the proverbial ounce of prevention, you may discover that the additional costs are well worth it. After all, in an era where there are steady threats from other carriers across the entire spectrum of access technologies, one can afford as few errors as possible.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.