ENTUITY
NETWORK ANALYTICS

Network Management Misconception: Issue 2 “The Devices are up. Service will be Fine”

This paper is the second in a series where we look at common misconceptions about network management through the real-life experiences of various companies. The aim of each issue is to bring to light network risk factors, quantify those risks with examples, and—most importantly—give you the prescription to keep your network from becoming terminal to your business. In this issue, we discuss a common cause of network problems, duplex mismatch, which is potentially disastrous if not identified and corrected quickly.

The Dangers of Network Instability

Businesses today rely on bandwidth-intensive and latency-sensitive enterprise applications such as VoIP, streaming media, CRM, ERP, PDM, or a multitude of SaaS applications such as Salesforce.com. They build Internet connected trading or partner networks, where any delays in transactions can ripple work stoppages and cost overruns throughout numerous organizations. Discovering the common causes of instability, then, is paramount. Whether a network serves one building, multiple campuses, or divisions across the globe, instability usually is caused by misconfiguration or unknown change. The dynamic nature of mobility technologies and network access technologies today makes these issues less obvious and more insidious.

Duplex Mismatch Wreaks Havoc on Manufacturing Company

A surprisingly persistent and ubiquitous problem occurring in most networks is duplex mismatch between system NICs and their associated switch port. In more than 90% of the customer proof of concepts Entuity has completed, our network management solution has identified duplex mismatches that had gone unaddressed for weeks or months. The potential impact and ensuing cost is compounded since performance issues from a duplex mismatch often don’t show up under light load. When the load increases and the users are pushing the service heavily, that’s when performance will be massively impacted—just when they need it most. And with the majority of transactions being TCP based, the retry mechanisms will eventually allow the transactions to succeed, but very, very slowly.

Identifying and correcting duplex mismatches is also not a one-time, “set and forget” task. It’s an ongoing issue in the fluid, constantly evolving enterprise infrastructure of today.

Take for example a high-tech manufacturing company that was performing maintenance on their corporate application servers. Their Microsoft Exchange server needed requisite updates of security patches, so the operations team scheduled down time for 3:00 AM on a Saturday to minimize impact on the user community. Patching and updating went without a hitch, the server rebooted successfully, and everyone went home happy.

Come Monday morning however, the moods were not as light. As the wave of business users sat down at 8:00 AM with their cup of coffee to check their email, the operations call-center was flooded with the dreaded complaint, "the network is slow and Outlook says the connection to the Exchange server is lost!" Realizing that most problems come as a result of change, and that the security patches were the last change made to the server, operations staff quickly uninstalled them and rebooted (running without important security patches, which put the network at high risk). But even as the staff began to breath a sigh of relief, the calls kept coming in.

Before the day was out, five IT technicians spent half a day troubleshooting the problem while the user community waited. The final fix was to swap out the server with a spare and relegate the original server to off-hour file backup alone. That also didn't work. What was wrong? It wasn't until weeks later when they upgraded their open-source network monitoring tools for Entuity that were they able to immediately identify the true cause of this problem. Uniquely sensitive to duplex mismatch issues, Entuity alerted the network manager that the NIC reverted to halfduplex state during the server reboot, causing incompatibility with the switch. It wasn't the security patch at all.

How Entuity Identifies Duplex Mismatches

Entuity's advanced Event Management System (EMS) and comprehensive reporting capabilities allow it identify duplex mismatches in multiple ways. First, if a port duplex setting changes, Entuity raises an event that indicates the change. Second, if the port duplex setting has not changed, Entuity can identify duplex mismatches through a Port Inbound Fault "Incident," which may point to a possible duplex mismatch. (An Incident is a collection of events that help prevent event storms and add focus to situations that may impact business services.)

Finally, Entuity can identify mismatches using its embedded Report Builder. In the figure below, a tabular inventory report displays only those ports that were configured for half-duplex operation. Given that ports are usually configured for full-duplex operation, this may indicate duplex mismatches, and warrant further investigation.

Summary

For one high-tech manufacturing company, hundreds of hours of IT time uninstalling patches, swapping out the server, and finally reinstalling the patches could have been saved if they had been using Entuity. Entuity's integrated EMS and deep, actionable reporting capabilities ensure that organizations have the immediate insight they need to quickly get to the real cause of problems before disaster strikes.

About Entuity

Entuity takes the work out of network management. Our highly automated, unified enterprise-class solution puts deep network insight at your fingertips, frees IT staff to focus on strategic projects and easily integrates with major frameworks and networking environments. Entuity's support and services teams are frequently praised for their rapid response, networking expertise and involvement in special engagements. Founded in 1997 by two senior-level IT executives from the financial industry, Entuity is headquartered in London with US operations in Boston. For more information, visit entuity.com.