CASE STUDY

RESTORING CRITICAL SYSTEMS QUICKLY IN THE WAKE OF NETWORK STORMS

TRYSTAR®

THE BACKGROUND

Recently, a large data center customer experienced a massive loss of communication between the Electrical Power Monitoring System (EPMS) software and all the connected devices (power meters, PDUs, transfer switches, etc.). The power monitoring system experienced ongoing waves of communication losses followed by self-restoration, then repeated communication losses. This triggered a significant number of alarms to also drop in and out within the EPMS software. Trystar was contacted to help determine the cause of the issue.

THE CHALLENGE

The cause of the communications loss was initially unknown. With all the connected devices experiencing the same communications issue, one of the questions being asked was “Why are the Sequence of Events Recorders (SERs) responding differently than other connected devices?”. When Trystar was brought in to help troubleshoot, we looked at the event logs of the SERs and quickly realized that a network issue was likely the cause. The SER event logs also revealed the exact time the communications loss began. The timestamped event data from the SERs led to the discovery of a piece of equipment introduced to the network at that exact time. This device had created a network loop causing a network storm which resulted in the massive communications loss.

THE SOLUTION

Once the identified device was removed from the network, communications were restored between the EPMS and all downstream devices. Because of this experience, Trystar created a diagnostic tool within the SER to give it the capability of detecting if there is a network loop, then recording this in the system log. Ultimately, this capability led to the creation of new firmware which made the diagnostic tool standard on all SERs. In addition, the SERs now have the added capability of displaying an error code on the LCD screen if a network storm is detected. The firmware upgrade also issues a reboot command for the SERs to reset from any communications issue caused by the network storm.

THE RESULT

The SERs with this network diagnostic capability have become very valuable in subsequent cases where customers have experienced a network storm. Often, the customer was completely unaware that there had been an issue with the network until the SERs revealed it through its logged information. SERs are also valuable in detecting network storms that cause disruption with the EPMS because they can show the exact time the network loop began and ended. This has led other IT teams to discover and fix previously unknown issues on their networks.

15765 Acorn Trail / Faribault, MN 55021 / 507.333.3990