

Large Cable Company relies on Asentria for fail safe operation of remote sites

By installing easily-integrated SNMP traps, not even a hurricane can slow field-maintenance' response to remote site emergencies

How do you stop a tornado, ice storm, heat wave, flood, or earthquake? You can't. Yet, any telecommunications company in the business of providing telephony, Internet access, entertainment media, proprietary WAN connectivity, or any combination of the above, must maintain the integrity of its own network communications in the face of all environmental hazards or immediately risk losing customers in the wake of data loss and network downtime.

To safeguard against any untoward event, most telecom operators maintain some means to monitor critical environmental and operating conditions (such as temperature, humidity, power supply, etc.) of their vital remote sites—be they relays, booster stations, hub boxes or antenna huts. Increasingly, this important task is no longer trusted to legacy monitoring systems such as third-party alarm services or out-of network dial-up systems. Instead, the recent availability of relatively inexpensive, fully automated, alarm traps that seamlessly integrate into existing network management systems now enable the failsafe reporting of environmental threats to communications integrity.

Within the state of Florida, a large cable giant recently switched over to SNMP-trap devices that proved themselves during an April power-outage by immediately notifying network-maintenance staff so that an over-heating problem could be quickly rectified. Downtime was completely avoided as a result. On the other hand, positive results were hardly guaranteed under the old system of monitoring and notification.

Mother Nature poses a challenge

Headquartered in Philadelphia, Pennsylvania, this large cable company is principally involved in the development, management and operation of broadband cable networks and in the provision of programming content. Serving more than 21 million cable subscribers, which makes them the largest cable company in the United States.



Large Cable Company relies on Asentria for fail safe operation of remote sites

Like many other communication companies, this cable company relies on the failsafe operation of remote sites to handle traffic throughout its broad coverage area that includes 35 states and the District of Columbia. Nowhere was this reliance more critical than in Florida, where fierce weather conditions occasionally threaten communication links for all providers.

“The biggest problem with being in Florida, is that when hurricanes and tropical storms come our way there are widespread power outages, so the local alarm-monitoring companies get inundated with alarms going off,” a field engineer with this cable company for the past seven years points out. “Under such conditions, they don’t have the time to contact all their customers in time, which has been an ongoing problem.”

His domain covers a two-county area spanning approximately 100 kilometers of coastline just south of the city of Tampa. Within these bounds are 13 remote sites that contain sensitive equipment that handles both television broadcast traffic and high-speed Internet traffic to thousands of cable customers.

“All 13 hub sites are powered by 110 AC that we get from Florida Power & Light, and all of them have air conditioning because the equipment within is very sensitive to heat,” he explains. “About half of these sites are cabinets located on the side of the road, and these are backed up by on-site batteries. The rest of the sites are physical buildings, and they have their own gasoline-powered generator for back-up power.”

“In either case, it’s important for us to be notified when the power goes out,” he continues. “The backup batteries in the cabinets can only run the air conditioner and equipment a short time before they both go out. With the buildings containing generators, you don’t quickly lose power to the equipment, but the air conditioners are only hooked up to the line AC, so once they stop running, the temperature quickly rises. The key is to get out to each location and cool it back down as soon as possible.”

Yet, he routinely encountered difficulty in obtaining timely notification of power outages and other problems because there was no direct communication between the remote sites and the head-end.

“The way it seemed to fail is when we had a local security company actually monitoring our sites,” he recalls. “They would put a security panel in each site that would do simple contact closures. Once a thermostat, for example, reached a certain temperature it would trip a contact, which would then dial their central station and sound the alarm. That would initiate the manual process of having one of their dispatchers call our dispatch. Our dispatch would then page our field-maintenance staff to notify us that the temperature spiked, or a generator started, at a certain site. It was a very slow process.”

Routine monitoring of back-up battery and generator status also proved time consuming, as the engineer and his staff would have to physically drive out to each site and check the run times of generators, for instance, then manually enter the findings in a logbook. Still, the greatest threat to service was the lack of automation in the emergency-notification process.

“Our focus right now is definitely ‘customer first’ and that’s a real key point with us — we don’t want to lose customers because of the system going down,” he stresses. “With that in mind we are trying to do everything we can to maintain uptime and quality of service.”

The precipitating factor in this cable company’s quest to improve response to potential downtime proved to be a tropical storm that passed through Florida during the month of September 2002, knocking out power to a majority of the state.

“Our cabinets lost line-power, ran for the duration that the batteries would allow, and then basically shut completely off,” he recalls. “We were depending on the monitoring company to tell us that the power was out so we could get a portable generator out. But since that

notification never happened, the system went down. That was kind of the last straw. We knew we had to look somewhere to get this situation automated.”

The search for an automated solution

Many telecom companies, including this cable company, already have some type of network management software (NMS) installed at the head end. Yet, not all have a means of seamlessly integrating operating and environmental conditions at their remote sites, into the NMS.

In response, a handful of vendors have developed equipment that can send a notice—in the form of an SNMP “trap” of an event or condition at a remote site. It was from this group that he set out to identify a solution.

“I evaluated a lot of products, and I found the Asentria device to be the most applicable fit for a couple of reasons,” he states. “You can feed many devices into this box without needing any proprietary drivers. Some other companies that offer monitoring devices require you to do custom engineering or create a proprietary data pass. We also looked at some that were similar in function to the Asentria product but cost considerably more.”

Based in Seattle, Washington, Asentria has specialized in data collection devices for the telecommunications industry since 1988. The company’s site-management product line grew out of an extensive experience in network alarm management and remote equipment access, especially for SNMP systems. These devices typically monitor critical business equipment — such as phone systems, power supplies or communications/ networking components — as well as the physical conditions that impact the health of such equipment, and then provide the network interface and intelligence required to get these non-networked devices into the control of the network.

He opted for Asentria SNMP-Link Model SL81 that combines three functions in one compact package:

a legacy device monitor, an environmental monitor and a terminal server. It can monitor any device with a contact closure output such as a battery, UPS, PBX, air conditioning unit or door strike plate—as well as water-level sensors, smoke detectors, motion detectors, noise sensors — and generate an SNMP trap or other alarms and reports that can travel via Ethernet, phone line, Internet or wireless system. As many as 16 external monitoring units—including those using T-Bos protocols can be daisy-chained into separate rooms or areas from one SL81, making the unit highly scalable.

Of particular benefit to cable company’s needs in western Florida, network managers gain secure remote access to the SL81, and any RS-232 device connected to it, from their NMS without dispatching a technician to the site.

Implementing quick-response, and prevention

The installation of the SL81 units in all 13 cable sites took place in late 2003.

“The process went very well. In fact, I did it all myself,” he notes. “I really didn’t have any large problems because: the device will accept many inputs like contact closures; they have standard voltage inputs; and you can also do RS232 inputs so you can take a box that doesn’t have the ability to send an alarm and import it without doing any custom engineering.”

He set the system up so that he can either “tone” into it at the sites that have fiber connectivity, or dial in over the public switch network on the sites that do not, using the standard hyper terminal that’s built into Windows. No additional software was required.

The installation has provided the cable company with the means to keep closer watch on their remote sites, while saving third-party monitoring costs.

“Deploying our own monitoring system has allowed

Large Cable Company relies on Asentria for fail safe operation of remote sites

us to eliminate two groups, the security company and our internal dispatch process,” he points out. “Now whenever a failure occurs, the head-end techs are notified directly. It has also given our techs the ability to dial-into the monitoring equipment and check the current operating environment in real time. In addition to emergency situations, it also notifies us when our generators exercise once a week.”

“In the case of an emergency, such as when the commercial power goes out and a generator starts, it will not only tell us that it’s running but it will tell us if the fuel level or the oil pressure runs low,” he adds. “Knowing that the generator successfully started up, transferred power and ran without the need for a site visit is very helpful.”

For the remote cabinet sites that use battery backup, he explains how monitoring the batteries informs them not only of a sudden power shortage, but also when the battery voltage drops below a certain level for any reason.

“It’ll tell us automatically when the battery voltage starts to drop to a level that will require us get a generator out there to be able to keep the equipment running,” says Rutkowski. “If there is no power outage, then maybe it’s a bad battery and we just need to get out there and replace it; so this system provides us with useful preventative maintenance capabilities.”

Further preventive measures extend to protecting the equipment from even minimal rises in temperature, which can damage components over a period of time.

“These devices have given us more visibility into our sites, whereas before we never realized exactly what was going

on,” he says. “For example, the ambient temperature in one particular hub site was running very hot and we didn’t know about it in the past because the monitoring company only had a static, threshold temperature setting that had to be exceeded before an alarm would sound. But with the product we now have, I can dial into the site and look at the exact temperature in real time.”

The most recent incident to face the system occurred on April 12, 2004, when line power was momentarily lost at one remote site. Fast response was necessary, as the air conditioning shut off and the temperature would begin to rise. Within 15 seconds, the head-end staff was automatically notified. Twelve minutes later, a technician arrived at the site to start correcting the problem, as evidenced by the entry-door light flashing. No equipment was damaged.

“Customer First” service assured, well into the future

“As we deploy the boxes, we are finding other uses and points to monitor,” he says. “We hope to monitor every optical receiver in our hub sites, giving us better visibility into our fiber network to allow a pro-active response in the event of a fiber cut.”

“With our focus on customer service, we are trying to do everything we can to maintain uptime and quality of service, and monitoring our hub sites and doing preventative maintenance can definitely help us deal with future occurrences, environmental or otherwise.”

For more information go to www.asentria.com. 

