

Plugging the Holes in a Telecom Network

“Phone Company/
ISP improves uptime
and customer service
by connecting remote
legacy equipment to the
corporate network ”

Telecom operations typically have sophisticated network and systems management (NSM) software in place to monitor their servers, workstations and routers. Such systems often utilize Simple Network Management Protocol (SNMP) as a means of transmitting and receiving network monitoring information. Great if you run only modern equipment. But what about the other elements that impact the health of a network such as power sources, legacy PBXs, batteries, legacy telecom equipment that don't recognize SNMP, or environmental factors such as temperature, water and humidity. If you don't address these elements, they can exert a significant toll on downtime.

This was the case at the Matanuska Telephone Association – a phone company, cellular provider and Internet Service Provider (ISP) operating in the vicinity of Palmer, Alaska (about 45 miles north of Anchorage). Matanuska's network spans an area of 10,000 square miles. While the backbone and central office were modern, many last-mile telecom huts on the periphery contained legacy equipment and non SNMP-enabled batteries that could not be centrally monitored.

How were service issues dealt with? If seven subscribers called with a problem with their phone or Internet, the company dispatched someone to fix it. “People sometimes had to wait overnight before a bug was resolved,” said Rich Allen, traffic administrator at the Matanuska Telephone Association.

The company solved the problem using a combination of two products: SNMP-Link 81 from Asentria, Inc of Seattle, WA, and a network monitoring system known as InterMapper by Dartware, LLC of Hanover, NH. AlarmsPro Inc., worked closely with Matanuska to deploy the hardware and software at its Palmer headquarters, as well as the telecom huts throughout its territory.



Pluggin the Holes in a Telecom Network

Network Blind Spots

Log into any monitoring system today and access the network maps. You can rapidly document the infrastructure and, at a glance, view the health of the network as a whole. If a situation is apparent, you can drill down to that specific locality to isolate the bug, and even investigate interconnections between devices.

The panorama can be so dazzling, however, that it masks a multitude of blind spots. These zones don't show up on maps as they represent areas invisible to the system. This can include: legacy, non-SNMP and non-networked devices; PBX's (enterprise phone system) or Central Office switches; temperature and humidity factors; water sensors and smoke detectors; door sensors; battery (power) sensors; air conditioning (AC) units; carbon monoxide sensors; and output relays.

Equipment rooms, for example, often contain devices that lack a network interface. Though many of these are quite old, they are often smoothly running and too expensive to replace. Fortunately, tools are available that "speak" to these boxes and bridge the gap with an SNMP network at a fraction of the replacement cost.

"There are three levels of integrating legacy devices into an SNMP network," said Tim Stoner, president of Asentria. "You can read alarms issued from the device's RS-232 serial ports (the standard ports between computers and peripherals); send queries concerning the amount of free disk space remaining, the number of phone calls made, and the voltage or signal strength; and set thresholds for each device to alert IT of any potential issues."

Monitoring Temperature and Batteries

Two of the most important elements to monitor in telecom are temperature and battery voltage. All electronic equipment, after all, is sensitive to fluctuations in temperature. Many hardware specs list operating temperature in the 50 to 95 degrees Fahrenheit range – bad news if your business has to deal with the harsh winters of Alaska. That's why Matanuska Telephone

Association pays particular attention to the monitoring of temperature and battery health at its last-mile telecom equipment huts.

"Temperature and battery conditions can bring any site to its knees," said Frank Knapp, CEO of AlarmsPro. "If the temperature is too high, you can experience a thermal runaway which is very bad for the battery and can even cause explosions."

Knapp explains that the batteries at a \$100,000 battery plant will last far longer if they are buffered from extremes of temperature or voltage. His company worked with Matanuska to set up alarms if voltage levels decay. The phone company's telecom huts contain banks of batteries that supply power to the equipment in case the power goes out. Negative (-)48 Volt battery banks are used, comprised of 24 two-volt batteries. Typically, phone companies have no way of knowing when a battery goes bad, even if the overall voltage remains acceptable. Using the Asentria SNMP-Link SL81, AlarmsPro divided the batteries into two groups so they can monitor the voltage output of each half. By comparing the voltages, they can rapidly determine if a cell has gone bad – the voltage on one half of the battery set will be different with that of the other half. The battery monitoring software that comes with the SL81 sends alarms to InterMapper whenever the batteries are unbalanced. Thus Matanuska knows about a battery failure before the whole system is affected.

"If the voltage drops below a set point, we can send a technician to address the situation before it becomes critical," said Matanuska's Allen. "By keeping a close eye on temperature and voltage levels we attain a lot more battery life."

Depending on the available infrastructure at the specific telecom hut, alarms and messages can travel via Ethernet, phone line, Internet or wireless. Managers receive alarms via pagers, email, or they can view alerts on their InterMapper or Asentria software.

“Many excellent manufacturers continue to build good equipment that can’t interface with the IT infrastructure,” said Knapp. “InterMapper works with the SL81 to provide any maps you need to effectively monitor your equipment.”

As some of Matanuska’s last-mile locations don’t have Ethernet, alternative means of connection are used to keep costs low. With a large territory to cover and some sites being remote as well as sparsely populated, the phone company sometimes has to use existing dial-up lines to relay alerts.

“Whatever means of connection is employed, we have a total of 30 SL81’s operating in our territory, and they have moved us from reactive to proactive mode,” said Allen.

He says that in the past, if the grid went down, there was no way of knowing that the huts were operating on battery power. After eight hours when the batteries were spent and user complaints mounted, the company would send a technician to investigate.

“By monitoring battery power using the SL81/InterMapper solution, we now have an eight hour window to take action before the batteries run out,” said Allen. “Also, we can monitor the state of our batteries in real-time, so they are always available in the event of an outage. Without a doubt, we now offer improved service to our subscribers.”

Terminal Server

Knapp also points out that the Asentria box can act as a terminal server, and that this feature proves especially valuable with aging PBX systems. If a PBX does not have a network interface, it will at least have an RS-232 maintenance port. By connecting that port to one of the Input/Output (I/O) ports on an SL81, the PBX can be monitored using a network monitoring system, or via dialup. Alarms and trending data can be viewed graphically. This applies to all major PBX’s such as those manufactured by Nortel, Lucent and others.

The Nortel Option 11, 61 and 81, for example, produce a large number of alarms and messages. Most of these alarms, however, represent minor concerns which may require little or no proactive monitoring. It is vital, therefore, to isolate the important alarms. Knapp notes that the Asentria SL81 can easily recognize these alarms and communicate them to a technician.

Similarly, collecting alarms from a Lucent switch poses its own challenges. Lucent switches do not issue alarms out of a serial port. To manage these alarms, the SL81 searches through several menus to locate the most pertinent alarms.

Further, the Asentria SL81 device also monitors microwave, making it possible to isolate periods of signal fade, rather than waiting for the signal to vanish completely.

“You can monitor PBX’s or microwave signals and trend the results on graphs that highlight when service is diminishing or a situation may be developing,” said Knapp. “Further, the SL81 does what no one else does – it translates analog values into real-world numbers such as dBm or adjusted voltage levels so you have no need to interpret the results.”

Managing Threats

To maintain a high level of service, telecommunications providers must carefully manage threatening conditions before they cripple mission-critical equipment. By paying close attention to critical issues such as temperature and battery voltage, providers can minimize the huge costs associated with equipment damage, data loss and facility downtime.

“By monitoring and handling a variety of remote equipment, events and environmental conditions, the life cycle of legacy equipment can be greatly extended,” said Stoner. “It is possible to monitor any device with a contact closure output such as a battery, UPS, PBX, air conditioning unit or door strike plate – and alert your


Plugging the Holes in a Telecom Network

network monitoring system when an event occurs.”

The Company

Asentria develops remote site monitoring and telemanagement solutions that enable providers of critical communications infrastructure to more efficiently and reliably run their networks. Asentria’s products help ensure quality of service and lower operational costs, while making it easier to provision, maintain and support remote equipment. Our strategic solutions fit both large and small communication networks and provide high-value, cost-effective and competitive differentiators to our customers.

Asentria helps administrators cost-effectively manage their call reporting data and remote site infrastructure, while extending confidence and security to ensure availability, integrity and performance. Asentria enables administrators to avoid failures from poorly performing equipment that threaten end-user service expectations, while providing better control to predict the performance of remote infrastructure. These new levels of protection shield end-users from remote site equipment failure. Our service provider and enterprise customers trust their remote equipment sites to Asentria. The company is headquartered in Seattle, Washington.

For more information go to www.asentria.com. 



[1200 N. 96th St., Seattle, WA 98103] [Tel: 206.344.8800] [Fax: 206.344.2116]

info@Asentria.com

Asentria.com