REMOTE

SITE & EQUIPMENT MANAGEMENT

Summer 2012
A Webcom Publication

Building Networks in Pakistan's Extreme Environments Puts Remote Management to the Test

please see page 14

Addressing Cyber Security Vulnerabilities in the Power Grid Infrastructure

please see page 10

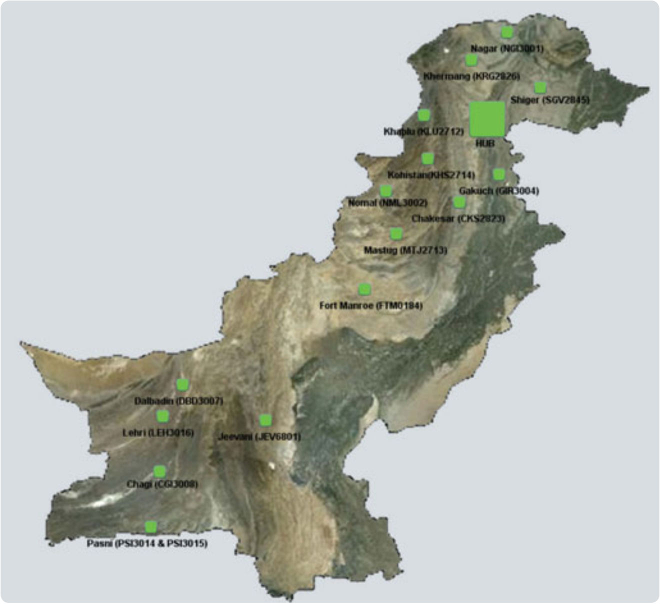
Networking - Page 20

Security - Page 22

Building Networks in Pakistan's Extreme Environments Puts Remote Management to the Test

Hamid Nawaz, Chief Operating Officer
Supernet Limited

Pakistan presents unique challenges and opportunities for the telecommunications providers in the region. The opportunity is apparent, as Pakistan has an estimated population of more than 177 million all located in an area that's about twice the size of the state of California, and a communications infrastructure that continues to struggle to keep up with the growing demand for mobile bandwidth. Network operators, however, are presented with challenges, both politically and geographically, when building out and managing networks that straddle mountainous hard-scrabble terrain and the physical issues in reaching the far flung pockets of population in the south west of Pakistan.



Compass Overview of Pakistan Remote Site

Supernet Limited is a satellite network service provider and systems integrator located in Pakistan that specializes in providing end-to-end satellite based GSM backhaul networks for the telecommunications companies in the region. They've assisted four of the major telecommunications service providers in building out their networks and are providing the management infrastructure to remotely operate these networks. Over the past few years, Supernet has installed more than 300 remote facilities in Pakistan, and has experienced and overcome many of the challenges of remotely managing telecommunications networks in extreme environments.

While some of the obstacles encountered are unique to Pakistan's climate and topography, most of the issues are common to managing any remote facility, whether it is a satellite earth station, microwave towers or a broadcast transmitter. Coupled with the diverse and demanding geographic conditions in Pakistan, there are certain other challenges such as sites not being easily accessible, power often not readily available and the high cost in both time and expense of visiting sites that can often require specialized equipment. To get to a site from a repair depot can often take most of the day and proper equipment for performing repairs is essential, as there are no locally available replacements.

Supernet's goal is to build out affordable, highly reliable networks that provide carriers high quality of service and low cost of ownership, where the numerous sites comprising their networks can be remotely managed and remotely recovered from most common problems. In the event that a site could not be remotely recovered from a failure, a remote site management solution would be used to ensure that when a technician was dispatched, they were fully prepared with the proper equipment to recover the site.

To make this a reality, an operator in the network operations center would need as much visibility into the remote site as possible. For the GSM backhaul, this consists of an interface into the satellite RF equipment (modems, converters, power amplifiers and antenna controllers) mostly via a proprietary serial protocol. Additionally, some of the devices and the network components such as routers and Ethernet switches communicate using the SNMP communications standard over the LAN at the remote site. Finally, the remote site solution would need to manage the facility alarms, which include UPS power levels, generator fuel levels, door open/close status and temperature readings, which in some instances communicate through serial or SNMP methods, but may also be via a contact closure interface.

Often times the reason why sites go down is not related to the RF equipment itself, but due to the systems supporting the facility, such as a generator not having enough fuel to sustain the site through a power outage. This makes the monitoring of those systems critical. If the operator at the Network Operations Center (NOC) is aware of the condition, they can arrange for the site to be refueled prior to losing service, or re-route the traffic to another location.

That means the software resident at the remote sites needs to be flexible enough to support a wide variety of protocols including serial and SNMP. Researching the available options indicated that many solutions could not or did not support the full breadth of data points available from the interface, only a sub-set. With equipment being remotely controlled only, operators would require full monitoring and control capabilities, allowing them to remotely recover a site, if possible, before dispatching a technician. If an onsite visit was required, they would need all the information available to determine the root cause of the failure, so as to avoid a partial or incomplete restoration of the service.

From a hardware perspective this presented the unique problem of trying to establish the physical interface into all the equipment (servers, network hubs, serial port hardware and contact closure equipment) in a confined area where space was at a premium. The remote management solution's hardware platform would need to allow communication using Ethernet to SNMP equipment, and on-board serial ports to communicate to the serial equipment, as well as contact closures for the facility and other non-SNMP or serial alarms at the site.

Technicians dispatched to the sites would need to access the remote manager for trouble shooting and analysis. Ideally, the remote unit would include a separate Ethernet port on the front panel for the technician to locally connect a laptop or PC, so they could obtain the status and alarm information and control the equipment using a browser-based GUI rather than having to navigate the equipment's front panels. Since the units were remote, entry to the system needed to be over HTTPs, a secure HTTP protocol version, with password protected log-in to prevent any unauthorized access to the remote controller.

The next obstacle to overcome was getting the data securely from the remote site to the NOC so the operators could manage the remote sites and ensure the server at the NOC was properly in synchronization with the status at the remote location. To accomplish this, TCP/IP or PPP over TCP/IP protocols were required, which would validate that the messages sent between a remote and the NOC were actually received. These communications should also be encrypted to ensure there was no unauthorized access into the system.

This often had to occur over the satellite hop between the remote site and the NOC, with its inherent delays and limited bandwidth (by design), since the bulk of the network's capacity was allocated to the GSM traffic. To ensure that the operators were updated promptly when events or a status changed at the remote locations, as well as to conserve bandwidth, the remote sites would only send data to the NOC when a change occurred. So as the remote manager polled the equipment out at the site, it would only need to send the equipment responses back to the NOC that differed from the data it had previously sent. To further refine this, the solution should be able to define how much the point had to fluctuate before it was considered changed. So if a status value change was by 0.01 of an engineering unit, but was tuned only to send data that changed by more than 0.1 engineering unit, it would not be sent.

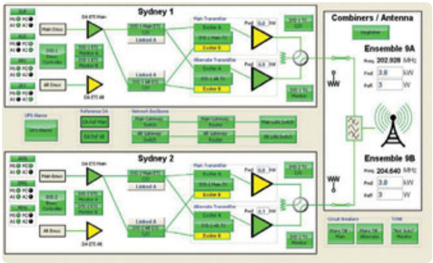
High activity periods are typically when problems most often occur, and the solution needed to provide the operator with the complete picture despite the limited bandwidth. One technique used to minimize bandwidth and ensure operational responsiveness was to conduct bulk transfers of the data, rather than send each change individually, which requires more overhead bandwidth. The system would group the changes into one message, compress it, and then send it to the NOC, greatly reducing the bandwidth required during these high activity periods.

If a problem eventually caused a termination of the communications between the remote and the NOC, the remote manager at the site had the ability to buffer the status changes, alarms and system events that were occurring during the communications failure so that once re-established the operators would be updated on the events that occurred during the blackout period.

A capability for a back-up communications link to the remote site from the NOC was also necessary, so that if a communication failure occurred over the primary satellite network, system access to the remote could be maintained via a dial-up, cellular, GSM or satellite phone (Iridium, for example), or via an Internet connection.

After much evaluation, Supernet selected the Compass and Mercury products from Newpoint Technologies. Mercury units were installed at the remote locations and run the core Compass software application for managing the equipment. The Mercury hardware has expansion bays that can be used to add serial ports, Ethernet ports or contact closures, allowing the use of a single flexible chassis for interfacing with all the disparate interfaces that are required when complete visibility into the remote sites is essential.

At the NOC, operators are provided a GUI from which they can view and manage all of the remote sites that comprise their network, and quickly identify sites that are experiencing problems. By drilling down into the site, the operator can view the actual device or parameter that is in the alarm condition, and take appropriate action to resolve the problem before the failure becomes service affecting.



Representation of a remote site using the Compass Software

The Compass software, provided with a library of more than 1,500 device interfaces, enabled Supernet to communicate with the equipment at the site, and ensured operators are kept up to date on all changes and events occurring at the remote locations.

Back at the NOC, a centralized Compass Server, allows operators to have full visibility of all activities across the network, ensuring they are immediately aware of any failures on the network and can remotely control the equipment to mitigate incidents before taking the costly action of deploying a technician to a site.

For higher availability requirements, Mercury is available with RAID hard drive arrays, hot swappable power supplies, and can even be provided with a built in UPS to allow orderly shutdown of a remote site when a complete power outage is unavoidable.

Supernet continues to roll out additional sites even today for these networks in Pakistan, helping telecommunications providers overcome the challenges of launching and expanding GSM networks, and assisting them in remotely managing their networks.

For more information please visit www.newpointtech.com.

Feature Article
Securing Remote Substations for a Smarter Grid
A New Approach to Situational Awareness and Incident Response
REMOTE
Site & Equipment Management
December 2011/January 2012
www.RemoteMagazine.com
A Webcom Publication
Satellite Technology –
The Key to Remote Communications
For Government Agencies
please see page 12
Securing Remote Substations
For a Smarter Grid
please see page 6
Editor's Choice
Page 4
Security
Page 20