DragonWave
www.dragonwaveinc.com

securityhive

Weather-Hardened Microwave Network

Erik McLaughlin

July 15, 2015

At present, new application requirements for public safety agencies are driving backhaul capacity to greater levels. To meet these requirements, the initiation of dedicated 700MHz LTE spectrum is playing a very important role. Adopting the dynamic 700MHz LTE network coverage allows public safety agencies to accommodate various data intensive applications including video surveillance, high speed internet access, video conferencing and IP voice services. All of these services help ensure that public safety agencies' can enhance their performance, security, and timing/accuracy.

There are different challenges to overcome for current outdoor-based public safety infrastructure systems. Firstly, the all-IP infrastructure provides a common base for inter-agency communication. Currently, modern IP-based radios can arrange solutions from 10 Mbps to multi-Gbps, which covers the safety network's capacity and ensures end-to-end communication for numerous critical applications.

Other components of outdoor-based public safety infrastructure systems, such as security cameras, secure Wi-Fi access points, and LTE, can be placed on non-telecom infrastructure (i.e., traffic lights, street lights, bill board stands, etc.).

This allows for lower costs because this "street furniture" already exists and also provides a means to avoid additional expenses (i.e., cabling, power etc.). The main and unique obstacles for these sorts of sites are the amount of space available for backhaul and the security of the sites. So, how does microwave address the backhaul capacity and inherent security requirements for public safety networks?

Designing for Capacity and Reliability

The adoption of LTE for public safety networks demands higher capacity, scalability and resiliency. Microwave radios address all the essential demands to support LTE on public safety networks.

Most importantly, microwave solutions range from 10Mbps to N x Gbps and incorporate modulation capability of 2048QAM, as well as advanced compression techniques and wider channels, so that capacities are now surpassing Gigabit levels on a single radio to deliver maximum scalability for public safety applications.

Achieving this level of scalability is essential because LTE for public safety networks now involves new data centric applications that coexist with voice services, such as live video feeds and other high-speed data applications. Moreover, adaptive modulation allows the radios to maintain up-time during altering weather conditions, and critical services are preserved using Ethernet's Quality of Service mechanism, ensuring continuation of high priority services.

Using integrated advanced Ethernet switching, microwave radios can also deliver resilient ring/mesh topological network connections without the use of an external switch/router. Ring/mesh-based architectures provide a distinct advantage over hub and spoke systems, in that they provide not just path redundancy, but also hardware protection to deliver a viable resilient networking solution.

Network Security

Other backhaul solutions are incapable of fulfilling a dedicated, co-located appliance that delivers end-to-end security due to the lack of available shelter space. On the other hand, all-outdoor microwave systems with integrated security capability can deliver management security in order to provide secure entry through local or remote access to the system. These systems must have:

- SSH Web GUI
    - At present days most microwave systems use a web-based GUI to configure, manage, or troubleshoot the device.

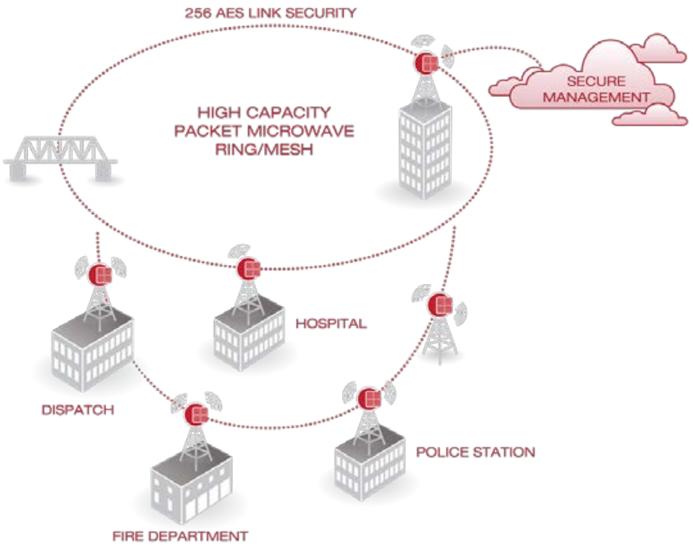
- SSL for Command Line Interface
  - It improves the security of remote Telnet sessions for operators using CLI to configure their devices.
- Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACAS+)
  - Both options provide a central authentication of users for management access into the system.
- SNMPv3 supporting Encryption
  - SNMP is a commonly used protocol to interact with higher layer Element Management Systems. Version 3 introduced a stronger security cryptographic security through strong authentication and data encryption abilities.

Although the aforementioned microwave features address management security, there are still cases where the public safety network operator is looking for additional security measures.

Even though current microwave links are intrinsically secure, through a combination of pencil-thin beam widths and radio-to-radio authentication, there are locations that may still be vulnerable to wireless snooping. To minimize this potential threat, some of today's microwave solutions provide full payload encryption, with 256AES encryption commonly seen as the de-facto method used.

The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements of cryptography modules and systems, including microwave systems. A full list of validated FIPS 140-2 systems, can be found at

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm



All-outdoor microwave backhaul solutions can deliver the pivotal elements needed for the transport layer of an outdoor-based LTE system.

Next-generation, all-outdoor microwave radios offer the essential combination of having a small form factor with high scalability for LTE and data rich applications, the resiliency to meet the SLA of mission critical services, and a FIPS certification to ensure the highest level of security. Therefore, all-outdoor microwave solutions meet all the expected requirements from operators (capacity, resiliency, and security etc.) in order to support LTE for public safety networks today and for the future.

View this Article Online

http://bit.ly/1fLSqWp