Cambium Networks™

7 things utilities should know about private wireless networks

Written by Scott Imhoff
VP of product management,
Cambium Networks

Originally featured on

energycentral.

Utilities have long used wireless communication networks as a complement to wired networks to support their operations---from land mobile radio communication systems supporting field operations, to low-frequency narrowband networks transporting supervisory control and data acquisition (SCADA) data. (Today, SCADA is frequently incorporated under the ubiquitous Industrial Internet of Things banner.)

However, a number of factors are today driving tremendous growth in private wireless networks. These include acceleration in distributed generation and renewables, grid automation, network resilience, the accelerating retirement of analog circuits by telephone companies, concerns over security, and a broad objective to comprehensively measure and monitor the grid from generation through transmission to distribution.

Today's wireless technologies offer utilities unprecedented flexibility in designing communication networks that provide the coverage, capacity, scalability, and reliability required to meet their mission critical voice and data communication needs today---and tomorrow. While every utility's wireless communication network architecture will have similar characteristics and elements, no two will be identical as they are architected to meet the specific utility's infrastructure, geography and topography, operational objectives, and customer density.

Having said that, there are seven wireless network design attributes that are reflected in every network.

CAPACITY VS. RANGE

Several factors impact the data capacity that can be delivered at a particular distance. Those factors include choice of spectrum, channel width (e.g., a 25 KHz channel vs. a 20 MHz channel), transmitter power, terrain, noise immunity, and antenna size. In general, capacity comes down the longer the distance to be covered. The longest range will be achieved using a lower frequency, narrow channel, with a high-gain antenna, while higher capacities can be achieved by selecting wider channels in higher frequency ranges, albeit at shorter ranges.

The fundamental question to ask in designing a system is "How much data capacity do I need and where do I need it?" Typical utilities will require a range of solutions capable of delivering Kilobytes to Gigabytes of data; from meters to hundreds of kilometers. With all this in mind, it's important to have a software tool that makes it easy to evaluate "what-if" scenarios to select the best combination of channel size, antenna, and radio to achieve the desired capacity with the necessary availability.

TOPOLOGIES (PTP, RINGS, MESH, PMP)

Virtually all utilities will operate multiple topographies within their network to execute their business objectives. Point-to-point (PTP) topologies are best suited for providing high-capacity links over long distances. PTP links are also great for short-range spurs connecting a single location to the wireline backbone, and using a point-to-multipoint (PMP) or 802.11 access solution at the remote end for further distribution of the capacity. PTP connections cover longer distances that are less susceptible to interference as the antenna patterns are narrower—so the energy can be focused in the direction of the transmission.

Ring topologies are excellent for resilient operations of high-capacity links covering a large area. The ability to automatically and nearly instantaneously redirect traffic (50ms switching time is a typical benchmark) from Eastbound to Westbound ensures continuous operation in the event a particular path is blocked. Resiliency in a PTP link can be enhanced with the use of redundant radios operating in concert with each other in what is referred to as 1+1 or 2+0 configurations. Mesh networks can be built using multiple PTP links or with specialized meshing protocols to enable multiple paths from point A to point B. Mesh networks have the downside of each packet traversing multiple hops, so they can lead to lower capacity and higher latency.

Point-to-multipoint (PMP) networks provide scale and capacity over a geographic area. PMP networks are typically deployed to provide connectivity for sectors or cells. The key capability to look for in PMP networks is their ability to scale both in the number of nodes per cell but also the ability to place cells next to each other without interfering. Your wireless radios should use synchronization techniques to ensure that adjacent PMP radios do not interfere with each other.

LICENSED VS. UNLICENSED

RF spectrum is a precious commodity and is available to utilities in three different formats:

1. Licensed,
2. Shared Access, or
3. Unlicensed. Licensed spectrum is typically licensed directly from the regulatory body, e.g., the United States Federal Communications Commission (FCC) or sub-leased from the license holder for a defined period of time.

Given its scarcity, licensed spectrum is relatively expensive but provides an organization exclusive access to a particular channel in a particular location. Operation in that channel should be largely free of interference from competing radios. In addition to the cost, it can take weeks to gain the approval to

operate, so licensed bands are not well suited to rapid deployments for disaster recovery or temporary installations. Licensed spectrum is typically used for high capacity microwave backhaul networks and narrowband SCADA networks.

Shared Access is a relatively recent phenomenon intended to maximize utilization of spectrum in a specific geographic area by proactively managing access to the spectrum across multiple users on a real-time basis. The FCC's Citizens Broadband Radio Service initiative includes 80MHz of spectrum at 3.5 GHz across large portions of the United States to be managed in this fashion. Shared Spectrum may be an ideal cost-effective solution for utilities, but again, each utility's circumstances will be different.

Unlicensed spectrum is generally open and available to anybody to use with no exclusive rights granted to any particular organization or individual; the only requirement being that the equipment utilized adheres to the regulatory requirements, and is installed and operated in compliance to those regulatory requirements. While this spectrum offers ubiquitous access, the lowest cost and fastest availability, the tradeoff is that competing systems may occupy the same channel at different power levels, leading to interference. Unlicensed radio manufacturers include capabilities in their radios to cope with this potential interference using advanced technologies like Dynamic Spectrum Optimization (DSO), adaptive modulation, automatic transmit power control, in-band dynamic filtering, and beamforming antennas to marginalize the impact of interference. It is highly likely that unlicensed spectrum has a valuable role to play in any wireless communication network if planned and deployed with forethought.

LINE OF SIGHT VS. NON-LINE OF SIGHT

A radio link can be described as "line of sight" (LoS) when there is an optical path between the two radios making up the link, or "non-line of sight" (NLoS) when there is some obstruction between the two radios. Near line of sight (nLoS) is simply a partial obstruction rather than a complete obstruction.

In general, lower-frequency solutions have better propagation than higher frequencies. In fact, above 6 GHz wireless solutions must operate in line of sight. From 1 GHz to 6 GHz, the capabilities will vary, and below 1 GHz the propagation becomes much better. There are several kinds of 5 GHz radios to maximize the propagation of these signals, including OFDM, multipath, ARQ and radios designed to work at very low receive sensitivities.

Considering that utility infrastructure is broadly dispersed it is certain that NLoS operation will be required – just consider foliage blocking access to sub-stations and service addresses. As such, lower frequency solutions will inevitably be part of a utilities wireless network to support substation automation and SCADA networks.

SECURITY

With ongoing cybersecurity threats, the security of wireless communications is quickly growing in importance. Historically simply encrypting the traffic with Advanced Encryption Standard (AES) checked the box on "Security". No more. Today, Information Assurance (IA) includes encrypting the traffic and control messaging, but is far more expansive including white hat hacking, securing management interfaces with HTTPS and SNMPv3, RADIUS authentication, multiple user accounts with password complexity rules, utilization of SysLog to record the details of configuration changes, and tamper evidence.

Selecting a solution with strong security features that are built into the product (rather than "bolted on" after the fact) makes it easier to comply with NERC-CIP audits. For the most security, look for solutions validated to FIPS 140-2, which is a U.S. federal government standard for security.

QUALITY OF SERVICE

Operators need to make the most efficient use of available spectrum by deploying multiple services on the same channels and also making sure the most important information is transmitted with highest priority. Solutions should have multiple Quality of Service (QoS) levels and the ability to sort traffic based on both layer 2 and layer 3 standard traffic classifiers. In this way, the source of the data can mark the class of service or priority, and the end-to-end network will ensure that the traffic is delivered with the desired level of urgency and criticality. It is also likely that the systems must support multiple VLANs to enable virtual separation of traffic – further enhancing quality of service.

NETWORK MANAGEMENT

The ability to manage a network has a direct impact on the total cost of ownership. Systems that allow centralized management of configuration, fault detection, performance and trend monitoring, and security validation minimize the effort required and also reduce the opportunities for unplanned outages. Make sure that the radios you select are compatible with local web-based interfaces or a centralized network management system that you can access remotely. (Having both of these options is the most ideal.)

Scott Imhoff

VP of product management, Cambium Networks

Cambium Networks™