Wireless that Works

Considerations for Meeting the Unique Demands of Data Centers

Overview

Packet Power provides a wireless power and environmental monitoring system that:

- Is proven to work in demanding data center environments
- Is simple to install, configure and operate across time
- Provides unmatched security
- Will work with any vendor's hardware or BMS/DCIM software

We achieve this through the use of a wireless networking protocol that we designed from the ground up to meet the specific needs of data centers. This paper describes what makes our system the best option available for wireless monitoring in mission critical facilities.

The Data Center Challenge

Data centers present a uniquely challenging wireless environment due to:

- Significant amounts of radio signal impedance from metal racks, large-floor-standing equipment, cages and other room dividers, and heavy-duty floor tiles.
- The need to monitor in variety of locations, including within racks, under the floor, in the plenum, in the general room space, across multiple rooms, etc.
- An unusually high amount of radio interference generated by the servers, switches and other devices housed in the facility
- The need to support both networks that can be very small (few monitoring points) or very large (thousands of monitoring points) at multiple locations with an enterprise.
- A tremendous focus on security
- The need to be able to isolate monitoring networks from other data networks, and even the need to isolate monitoring networks from each other
- Frequent changes in the network topology as monitoring points are added and removed in response to facility changes.

Traditional wireless networks were designed to be easy to detect, change infrequently, utilize the same protocols as corporate data networks, and work in a radio environment with limited, relatively stable interference that does not vary greatly over time. As such, they are not well-suited for use in data centers.

As an example, traditional mesh networking technologies such as Zigbee assume some degree of stability within the network, i.e. they assume if two nodes can communicate within a network they can usually establish a fairly persistent link and rely on it over time. This concept is oftentimes extended to longer, multi-hop routes that require relatively large CPU power and memory to maintain (at least in terms of the small embedded devices used for these purposes). This assumption completely breaks down in highly noisy environments like data centers, where radio interference conditions can radically change from second to second. In such a hostile environment, any system relying on a relatively static mesh model will often fail to configure itself. A system designed for data centers needs to be much more dynamic, respond rapidly to changes in the environment, and sustain even performance through widely varying levels of interference.

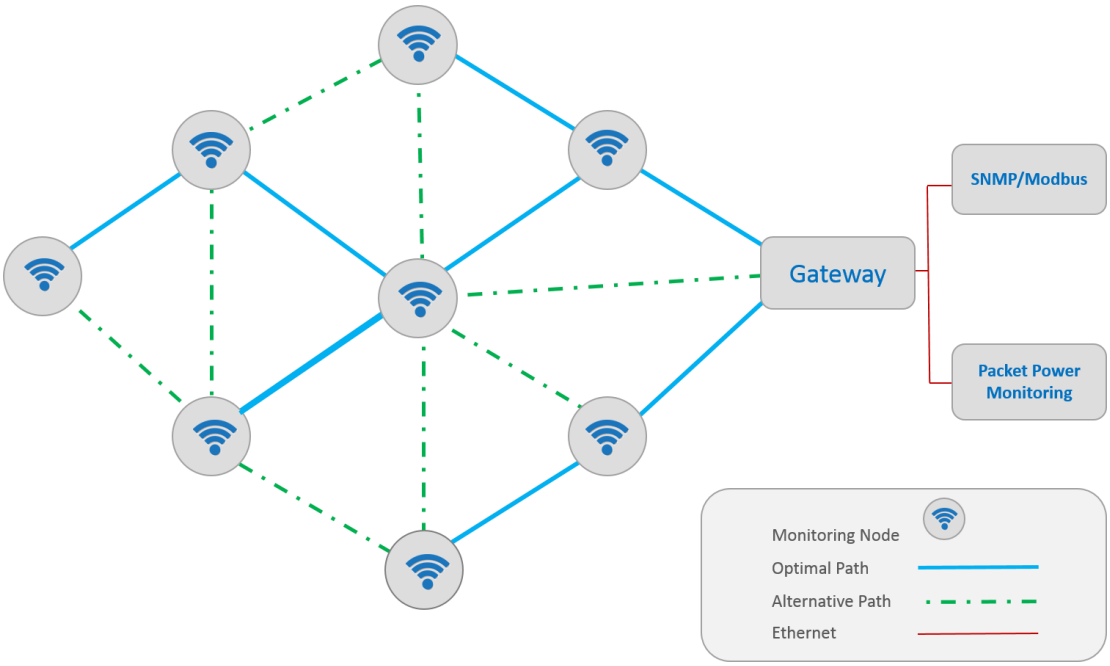
Packet Power's Approach

Our company is based on our ability to design a wireless network that can meet those challenges while being simple, robust, scalable and secure.

Basic Mesh Technology

The Packet Power system consists of wireless energy and environmental monitoring units and the Ethernet Gateway, a device that links the wireless units to a customer's Ethernet network. All devices utilize a spread-spectrum frequency-hopping **wireless mesh** radio network. This means:

- Monitoring units communicate with each other and do not have to be in direct radio communication with a gateway. This greatly increases installation flexibility, reduces the number of gateways needed, and provides for a far more resilient network.
- The radio frequency space used by the network is subdivided into multiple channels, and each time a transmission is started the unit looks for the least-utilized channel. This greatly decreases the odds of a unit creating or incurring radio interference with other devices.



The Packet Power network utilizes **dynamic routing**. Each time a device transmits, it evaluates the performance of the network paths through all the other monitoring units it can communicate with, determines the optimal network path, and makes a short data transmission.

The Packet Power network is **self-configuring**. When a device is added to the network, it automatically joins the network and begins to determine optimal communication paths. As Ethernet Gateways and other monitoring units are added or removed from the network, all units immediately adapt to the changes without any need for network management staff to oversee the change or optimize the resulting network's performance.

Packet Power devices communicate using a **purpose-built protocol**. This means the information flowing between devices is limited solely to power and environmental monitoring data and network management information. This simple protocol is possible because the network need only support monitoring devices. Contrast that to a standard protocol such as WiFi, which must have the size and complexity to handle communication for a wide range of purposes from a wide range of devices. The relative simplicity of our protocol enables easy installation, minimizes the processing resources needed in the monitoring units themselves, and provides significant security advantages.

Most Packet Power monitoring units communicate over **860-930MHz and 2.4GHz frequencies** (the actual portion of that bandwidth used varies by region around the world). The lower-frequency 860-930MHz transmissions have a longer wavelength and navigate high-interference environments better than systems that depend solely on 2.4GHz such as Zigbee or WiFi. Yet 2.4GHz can be utilized when higher speed is needed for activities such as firmware upgrades or when a particular region prohibits use of the lower frequency range.

Simple

The dynamic routing, purpose-built protocol, and self-configuring capabilities of the Packet Power wireless network provide for the simplest monitoring solution available. There is no pre-installation configuration of monitoring units, the network is self-forming, it optimizes performance with every transmission, and it adapts automatically to increases or decreases in device count and mix over time.

In addition, because the devices are wireless, there is no need to run cable drops, allocate switch ports and IP addresses, and configure the proper network settings. In retrofit situations, there is not even the need to remove the existing equipment. Not only is installation much simpler, the resulting cost savings can be hundreds of dollars per monitoring point.

Robust

The wireless mesh design, dynamic routing, purpose-built protocol, and use of a range of transmission frequencies delivers a wireless network that performs strongly in the difficult radio conditions common in data centers. Because each device has the intelligence to find an optimal path with every transmission, the network can perform and adapt without needing to rely on the emergence of a stable topology. As a result our system degrades much more gracefully and continues to operate as designed through varying levels of interference.

Our network protocol also is designed to minimize the odds of incurring or creating conflict with wireless devices that may be using the same spectrum (this could include things such as RFID units, wireless microphones, low-power short-range transmitters, or cellular phones depending on the region of the world). In over five years of operations in data centers all over the world, Packet Power devices have never been found to interfere with any other wireless system nor have other systems prevented our network from performing.

Scalable

Those same capabilities of wireless mesh design, dynamic routing, and purpose-built protocol provide for a system that easily grows from small to very large deployments without requiring specialized IT

resources to manage it. As the number of monitoring units at a site grows, simply add a Gateway to maintain consistent performance.

Performing **firmware upgrades** can be time-consuming in large networks, but it can be done easily over the wireless Packet Power network without disrupting the normal performance of the monitoring devices. Also, in large facilities, customers often wish to segregate their operations for IT or business management reasons. Packet Power's network offers full **wireless network isolation** whereby units within the same facility can be made completely invisible to each other.

Secure

Strong security is a primary requirement of any wireless network that will be used in a critical facility. There are two aspects to security: protecting the information transmitted over the wireless network, and preventing an intruder from using the monitoring network to gain access to a company's data network.

Wireless Security

The system addresses the security of data sent over the wireless network by:

- **Not transmitting sensitive data**. The best means of avoiding security issues is to not transmit data that requires protecting. Every customer that has looked closely at the nature of the information that is transmitted across our wireless network has determined that it is not of a sensitive nature and would not pose a security risk were it accessed by an unauthorized party.
- **Utilizing a non-standard protocol**. Because the network uses a non-standard protocol and an atypical radio frequency, and never broadcasts an identifier such as the SSID used by WiFi networks, the Packet Power network is a less obvious and less attractive target than monitoring networks using technologies commonly found in corporate data networks.
- **Offering encryption as an option**. All current-generation Packet Power products support AES-128 encryption of over-the-air data. Distinct encryption keys can be issued to individual customers, sites or groups of devices within a site, and separate encryption keys can be enabled for device configuration and management purposes.

IP Network Security

In addition to superior wireless data security, the system also takes steps to ensure that the Ethernet Gateway can be added to an IP network without creating security concerns.

- **Limited, purpose-built protocol**. The purpose-built protocol is limited in scope to monitoring information and network performance management, and it does not allow communication with other wireless devices.
- **Wired / wireless separation**. The processor in the Ethernet Gateway that handles wireless communication is separate from the system used for Ethernet communication.
- **Pull not push**. The Ethernet Gateway does not broadcast data over the wired network; rather, data must be pulled from the device.
- **Option for complete out of band implementation**. Customers who wish to take security even further may implement the entire monitoring system such that it is entirely out of band and isolated from the rest of their IP network.

Add these factors together and it is not possible for someone interacting with a Gateway over the wireless network to gain access to a customer's IP network. This focus on security has allowed our system to pass stringent network security tests at large financial services organizations.

Security and the Internet of Things

The rise of the "Internet of Things" (IoT) has made it possible monitor and control an incredibly wide range of devices using wireless connections. These IP-based IoT systems can be and have been used as DDoS attack platforms. Such attacks are likely to continue due to the following characteristics:

- IoT systems tend to be large targets (multiple devices)
- IoT systems tend to be powerful potential attack platforms (again, multiple devices)
- IoT systems tend to suffer from monoculture effects – they are comprised of large numbers of devices running identical software with identical, oftentimes hard or impossible to patch vulnerabilities

Packet Power's wireless architecture removes those concerns.

- **"Invisible" wireless devices**. Packet Power monitoring units are separate from and entirely invisible to the IP network and cannot be used for DDoS attacks.
- **Wired / wireless isolation**. While Packet Power's devices can feed data to the internet, they are NOT actually connected to the Internet – they are a PNoT ("Private Network of Things") rather than an IoT system. There is no IP tunneling capability between the Packet Power wireless networks used to collect the monitoring data and the IP network used to forward and process the monitoring data. Devices on the Packet Power wireless networks are not capable of directly communicating with or aware of any devices on the IP network.

For all of these reasons, after taking a close look at our system security, no customer to date has felt it necessary to enable encryption or deploy the system on an isolated network. It has been used in tightly secured data centers since 2009 without a single security incident.

Interoperability

While the Packet Power network operates independently of other wireless networks, information gathered over the wireless network can be easily shared with other monitoring systems. DCIM and BMS applications can use standard protocols such as SNMP or Modbus TCPIP to request data from the Ethernet Gateway. Custom interfaces can easily be created for either protocol. When communicating with SNMP applications that require each monitoring unit to have its own IP address, the Packet Power network can assign virtual IP addresses to each wireless monitoring unit. And when working with large networks that involve multiple Ethernet Gateways at a site, the Packet Power system makes it possible for the SNMP or Modbus application to gather information on all monitoring nodes from a single "master" Gateway.

Regulatory compliance

Packet Power devices are certified for use in most regions of the world. This includes FCC Part 15 standards; Council Directive 1999/05/EC - European Union (EU) R&TTE ETSI EN 300 220-2, Issued:2006/04/01, ETSI EN 301 489-3, Issued:2002/08/01 V1.4.1 and Council Directive 2004/108/EC

(December 15, 2004) on Electromagnetic Compatibility CENELEC EN 61326-1 Issued:2006/05/01; IEC 61326-1:2005;:1997 -; and verified against additional local requirements in Australia/New Zealand, Canada, India, South Africa and the UAE.

