Statseeker
every port. every minute. everywhere.

Wireless Reshaping IT/OT Network Best Practices

The Important Questions

Wireless has been a part of networking for more than a decade, so it isn't a new thing for network administrators to be aware of.

But which wireless?
What industry standard will be used?
And what data and format must be captured and stored?

These are the real and important questions discussed in this white paper.

Most networks have the ability to include WiFi, IEEE802.11x. That's basically old news. The benefits, and the problems, of WiFi are known, and techniques, procedures and policies are usually in place to protect the wireless portion of most modern day networks.

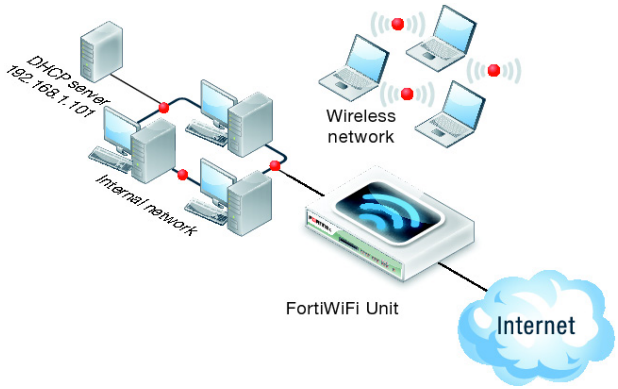
But the Internet of Things (IoT) will make significant changes in the way network architectures are designed, and nowhere will those changes be more immediate or far-reaching than in the ways wireless systems are used. Simply put; there's a lot more to this wireless issue than just WiFi.

Disruptive technologies led by the IoT technologies, challenge all aspects of current network best practices. This white paper will provide a strategic overview of how wireless technology is facilitating the connectivity-of-everything and in turn challenging and reshaping current best practices related to how networking architecture must align to drive stronger business strategies.

Let's start by looking at the IoT, and its accompanying Cloud services and Big Data analytics. Today, these technologies routinely deliver immense and unheard of amounts of data from devices and sensors that are at the edge of the network. Network architecture continues to adapt and will change dramatically to implement the data flow from these sensors. Networks will become outward focused, as the amount of data acquired from edge devices dwarfs the amount of data produced inside the network by traditional means.

Traditional WiFi Inside the Enterprise and Outside

The below graphic shows the way it used to be, with WiFi the only wireless protocol a network administrator needed to worry about. Every office had a wireless access point, and they were permanent, and mostly used for access inside the enterprise by laptop users who didn't want to plug into an Ethernet port.



It was a very small part of network design and most administrators ignored it for the most part. What was far more challenging, was the use of laptops connected to WiFi outside the enterprise - in a home, hotel or meeting room where the user was connecting via an unsecure connection or over the Internet. System administrators worked hard to ensure that this use of laptops (and eventually smart phones and tablets) was secure and could not be used as a hacking pipeline. This was mostly done using VPN technology. Once again, this use did not change the networks basic architecture.

Wireless Backhaul

Previously, network architecture for wireless used a design that had a wireless access point that was directly and quickly connected to wired Ethernet. Network backhauls were always wired. However, in more recent times, companies with sprawling multi-building campuses or manufacturing or process plants have been using wireless backhauls.

Some of these are designed using WiMAX (IEEE 802.16) as broadband microwave links. Others are designed as optical. These wireless backhauls are significantly less expensive to install, and provide secure data transmission without the need to pull cable for either copper or fiber backhauls.

Optical Data Transmission Devices

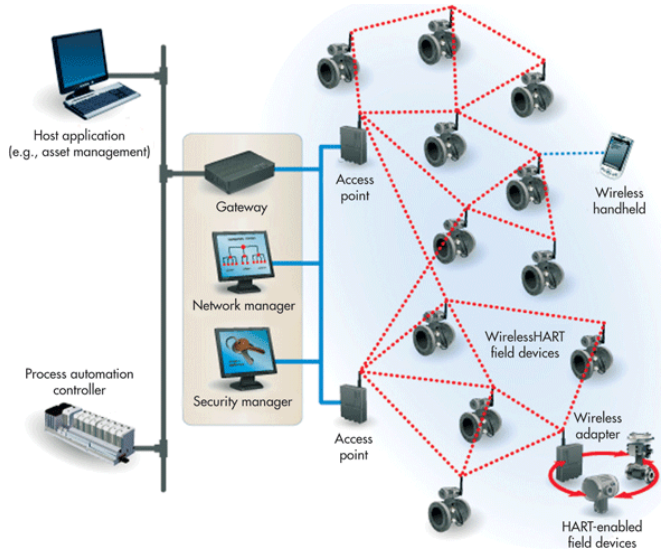
Wireless backhauls also make it easier to set up new nodes or temporary data centers, without the cost of pulling large scale fiber to the building. In building automation systems, Wireless backhauls make it possible to easily make an older building smart, without ripping the walls to install cables. In manufacturing and process plants, wireless backhauls make it possible to extend sensor and control networks everywhere in the plant, especially where there are no more cables available in marshalling cabinets, or where sensors were not included in the original design of the plant.

Wireless Sensor Networks Become the Norm

Using the Bluetooth standard and IEEE 802.15.4, among others, sensor vendors have created a plethora of sensor network protocols that will be seen increasingly by network administrators as the IoT, and its manufacturing offshoot, the Industrial Internet of Things (IIoT), become less talked about and more implemented.

Network administrators now often see Bluetooth, Low Power Bluetooth, Near Field Connection, and the assorted protocols based on IEEE 802.15.4 radios, such as ZigBee, Z-Wave, WirelessHART, and ISA100.11a-2011. ZigBee and Z-wave have been adopted primarily in building automation.

WirelessHART and ISA100 have been primarily adopted in process automation systems. Besides these there are a large number of proprietary protocols using the 900 MHz and 2 and 5 GHz MSI bands (Medical, Scientific and Instrumentation). IEEE is working on a new subchapter for the 802.11 standard, tentatively called 802.11s, which will provide a low-power mesh network version of WiFi.



Wireless Sensor Network (WirelessHART)

These sensor networks are typically low power, low data transmission rate, self organizing, and self configured mesh networks. They directly connect to the OT network using a network gateway, which moves the sensor data using Ethernet TCP/IP.

If 802.11s becomes an accepted standard, this will provide the ability to drive Ethernet IP directly to the sensor and device level, making special protocols no longer necessary. There are some efforts to use traditional 802.11x WiFi direct to sensors and devices, but they are not terribly successful because of the known bandwidth grabbing and hogging that WiFi does, and the small number of those devices that can be connected to WiFi directly.

This proliferation of wireless sensor networks will affect the design and architecture of enterprise networks. The amount of data being produced is significant. Whether it is going to enterprise servers, OT servers, or directly to the Cloud, this amount of data dwarfs what network administrators are used to seeing. While building automation sensors tend to report rather slowly, once per minute or once per five minute increments, process and factory automation sensors report much more rapidly. A process pressure transmitter might report every 250 milliseconds, while a factory automation sensor might report every 15 milliseconds. From a single sensor, that's a lot of data. Now consider how much data that is, if there are 10,000 sensors in a plant.

Is your network going to choke on that much data? Or will you clog up your pipe to the Cloud? Or will you be able to handle this avalanche of data? Good network administrators are planning for handling that much data.

Cellular Wireless Becomes More Relevant

For years, network administrators have had little to do with cellular telephony, other than to provide smart phones and tablets access to WiFi services. The IoT is changing that, too. Even in the confines of a manhole in the street, data is being collected and transmitted back to the enterprise network and the OT network, this time, using cellular modems. Does your network know how to handle this data stream? In the specific case shown in Figure A below, the cellular modem wakes up and sends the entire day's data stream in one burst. This is done to save battery life in the manhole, but it doesn't help the network's ability to handle large quantities of data.

Figure A: Wireless Cellular Modem Sends Flow Data

Now, suppose your network has over 300 of these devices in the field. Or maybe 3,000. The data from the devices in Figure A is being used in Big Data analysis of water usage to predict usage and determine where leaks are occurring. The data is sent through the network servers to Big Data analytics software. The water company eventually expects it to become enterprise critical information in the very near future.

Automatic Identification and Data Capture (AIDC) Adds More Complexity

In both the factory and in health care, bar codes, QR codes, RFID chips, and other AIDC tools have been used for years. Now they are used in many applications, from automatic tolling on highways to supply chain inventory management, to maintenance management, and Big Data applications for quality, inventory control, and statistical process control.

AIDC is used in the factory and in the process plant to help control the flow of material and parts throughout the process. AIDC technologies are the backbone of track and trace in the pharmaceuticals and fine chemicals industries, and the data they produce must be collected and distributed through the network to the various applications that use it.

Personal Monitoring Devices Drive More Connections

The latest sensor proliferation is that of personal monitoring devices. Even in IT applications, some companies want to track the position of their employees and their expensive assets. In process plants and manufacturing plants, tracking employees and assets is essential for safety. “Man down” applications, personal hazardous gas sensors, and chemical shower usage are also being implemented. The ability to track the location and condition of a plant’s firefighting apparatus may be critical in the event of an accident on the plant.

Currently, most of these sensors use either proprietary wireless protocols or one of the major 802.15.4 wireless protocols like ZigBee or WirelessHART. They access the network through wireless gateways. As IPv6 is enabled and used in the network, these devices will be able to have IP addresses and function as network devices themselves. Once again, the network is going to need to be architected to absorb this information and route it to the appropriate application for action.

Personal Wireless Oxygen Sensor

Rethinking Mobility with Wireless

We are already beginning to see the use of networked devices that are entirely mobile. Personal wearable devices like fitness bands, smart watches, smart clothing, as well as smart phones and tablets are beginning to proliferate. These devices will be networked to Cloud servers, or network servers, depending on the applications. So network administrators need to be prepared for devices entering and leaving the network at random. They will also access the network from access points outside the network. Network policies and procedures need to be developed to properly assign access and permissions depending on the location of the device and who is logged into it.

There is already an issue with BYOD (Bring Your Own Device). Some companies forbid it, some frown on it, and some have decided it is a money saving opportunity to have employees use their own smart devices. In any case, it is the network administrator who needs to cope with the rapid increase of many different smart devices, instead of one or two approved and vetted ones.

Networks used to be fixed with devices that didn’t move around. Now many networks have some portions of virtual networks, some SDN sectors, Cloud interfaces, movable sensors and devices, and network administrators have to keep track of all of it, in as near real-time as can be managed; thus the increasing reliance on network information solutions. That old saying that “you can’t manage, especially in an environment of amorphous change, what you can’t see”, becomes even more important in today’s world of ever increasing connected devices.

Security Issues

Mobile devices and the proliferation of edge devices and sensors from the IoT have created a new and different security posture. The traditional security architecture of the layered defense, like an onion, simply doesn’t work anymore.

The need is for a new security architecture that will cope with virtual servers and computer systems, bidirectional Cloud access to servers not controlled by the enterprise, edge firewalls and device level security software that uses encryption and authentication directly in the device. The new security architecture will need to act more like an immune system than a firewall. Intrusion detection and malware identification will need to be much more developed than today’s antivirus software. They will need to be like white blood cells, traversing the network and finding problematic data and software, and eliminating it.

The majority of this must be automatic. Current security responses are far too open loop, with a human response required for the majority of actions. Like the immune system of the human body, network security must do 80% of its work automatically. Only very difficult or traumatic issues should be brought up to the network administrator in person.

Envisioning the Network of the Future, Today

Today’s network administrators must be prepared for a

significantly changed network in the future. Wireless systems, both for sensors and devices, and for backhauls, will need to be introduced into the network and accounted for in planning for data throughput. The amounts of data that networks will have to deal with will increase exponentially in the next ten years. According to Gartner Group, there will be billions of devices connected to the Internet of Things by 2020. Network administrators need to be up to speed on these devices, and the wireless interconnection most of them will be using.

Summary

✓ Wireless and IoT technology demand new thinking on network architecture - are you ready?

✓ Cellular's role in aligning global networks with business strategy is accelerating; requiring a greater understanding of the technology and best practices for proper use.

✓ Wireless sensor proliferation simplifies the "Sensor-to-Boardroom" connectivity, but adds complexity to the network, demanding more upfront planning.

✓ Network security must include automatic "immune" protection, with less human interface, yet allow ubiquitous wireless access when and where data is needed as the business grows.

References:

Low-Rate Wireless Personal Area Networks, Third Edition, Guttierrez, Winkel, Callaway and Barrett, Standards Information Network IEEE Press, 2010.
Wireless Control Foundation: Continuous and Discrete Control for the Process Industry, Blevins, Chen, Nixon, Wojsznis, ISA Press 2015.
United Water Solves Big Data Problem…, https://w3.siemens.com/mcms/sensor-systems/CaseStudies/pi_00284_united_water.pdf.
Cyber Security Policy Guidebook, Bayuk, Healey, Rohmeyer, Sachs, Schmidt and Weiss, John Wiley and Sons, 2012.