HPE aruba networking

Low data rate wireless IoT monitoring

Hewlett Packard Enterprise

信尚安 XINSEC

Why HPE Aruba Networking and Xinsec

- Out-of-the-box integration with existing HPE Aruba Networking Wi-Fi infrastructure
- Eliminates the need for new PoE cabling-in areas with active infection-control barriers
- Supports LoRaWAN, 433MHz, and sub 1GHz IoT sensors
- Rich suite of IoT applications minimizes the need for custom application development to obtain insights from the IoT sensors
- Empower IT to support IoT projects requested by lines of business
- Validated interoperability

References to the Internet of Things (IoT) abound in both the business and technical press. Virtually every networking company has an IoT connectivity play, many software companies have IoT-related applications, and device vendors are pivoting to enhance IoT interoperability.

Wherever possible, customers prefer to tunnel IoT traffic over secure IT infrastructure to target applications and cloud services. Wi-Fi access points, LAN switches, and SD-WANs meet a very high bar for network security, high-speed throughput, reliability, manageability, and cost.

That said, there are applications like irrigation control and street lighting that aren't easily addressed by IT infrastructure. That's because IoT payloads must be transmitted over very long distances from battery operated IoT devices. In these use cases, low data rates are acceptable, low cost is paramount, and network security and key management don't have to meet the same standards as IT infrastructure. Wide-area, low-speed radio networks are ideal for these applications, and Long-Range radio — LoRa — is a popular option.

LoRa uses spread spectrum chirp radio communications to transmit up to 50 kilobits per second per radio channel over 15 kilometers line-of-sight (5 kilometers in cities). Communication between LoRa sensors and a LoRa gateway is handled by the LoRaWAN cloud-based medium access control layer protocol operating above the LoRa physical layer.

Data transmitted by a LoRa sensor is typically received by multiple gateways, which forward the packets to a centralized network and application servers. LoRa and LoRaWAN offer reliable wide-area IoT communications with extremely low battery consumption but have security and performance limitations that limit use in high security, high speed, and large payload applications. These limitations can be partially mitigated by locally collecting LoRa sensors data via a gateway that interfaces with a secure IT network that backhauls the data to a centralized network and application servers.

Xinsec

Xinsec is a leading supplier of medical IoT devices based in Guangzhou, China. Founded in 2006, Xinsec produces a suite of smart hospital systems for navigation, infusion pump and vital signs monitoring, bedside communication, time management system, asset tracking, and safety assistance monitoring. Among the first in China to integrate Bluetooth Low Energy (BLE) and LoRa networking into medical IoT devices, Xinsec has developed an integrated and open medical IoT platform that spans clinical and hospital facility applications.

The Xinsec GWLR 3000 Gateway communicates with Xinsec's LoRaWAN compatible sensors. The gateway can be powered over PoE or USB and may be expanded to support 433MHz and sub 1GHz IoT radios. Its roles include connecting with the network server over IP, IoT packet store-and-forward, and protocol conversion.

The ideal mounting location for the Xinsec gateway is on the ceiling. Running dedicated Ethernet cabling for a gateway is expensive because it must penetrate sterile barriers installed above the ceiling for infection control. Interfacing power and data with an already installed HPE Aruba Networking access point is far more economical and simpler to deploy.

HPE Aruba Networking has built USB ports into most of its access points since 2007. Originally intended for USB cellular modems, today the USB ports support a diverse range of IoT devices including gunshot detectors, air quality monitors, and electronic shelf tags transceivers.

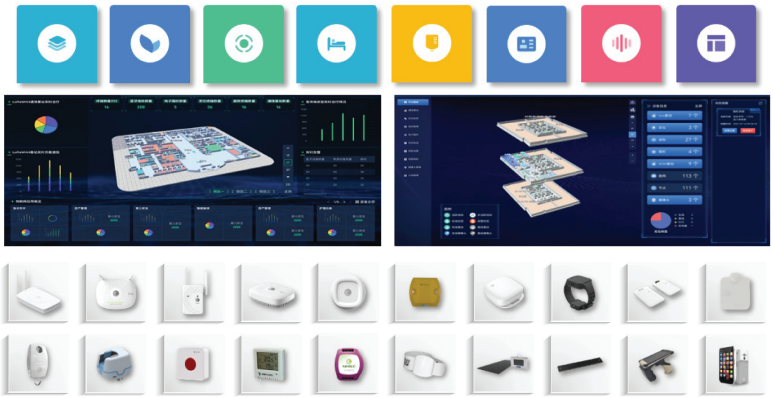

Figure 1. Xinsec IoT product family

Many HPE Aruba Networking access points also include a second Ethernet port, some with PoE pass-thru. This feature enables wired LAN access without the need for a second cable run.

Customers can leverage the USB and second Ethernet port at the time of initial deployment or use them for post-deployment services without having to rip-and-replace access points.

HPE Aruba Networking and Xinsec

HPE Aruba Networking and Xinsec have partnered to deliver healthcare IoT monitoring solutions that are inexpensive to install and benefit from IT level security mechanisms. This joint solution couples HPE Aruba Networking Wi-Fi access points (APs) with Xinsec's IoT Gateway, LoRaWAN sensors, and IoT Platform software. Sensor data are collected by the gateway, which derives power and streams data via the access point's USB or pass-thru PoE port. These data traverse a dynamically segmented secure tunnel to Xinsec's IoT Platform application running on a local or remote server.

The joint solution avoids the expense of deploying an independent IoT network, leverages low-cost battery-operated LoRaWAN sensors, and uses the customer's existing secure HPE Aruba Networking IT infrastructure for data security. The Xinsec gateway's flexible physical layers allow supplementary 433MHz or sub-1GHz sensors to be added in the future if required using the existing gateway hardware. Customers get a flat network topology with consistent device management, security roles, data policies, and application access across both the wireless IT and IoT networks.

Additionally, the joint solution avoids the risk of shadow IT to support new IoT applications. A concern of every Chief Information Security Officer (CISO), shadow IT is often the last resort of clinical teams that want to integrate new IoT services but aren't permitted on the corporate network. By tunneling IoT data to the correct target application, HPE Aruba Networking can address the CISO's security concerns while enabling clinicians to deploy or experiment with new IoT monitoring sensors. No shadow IT needed.

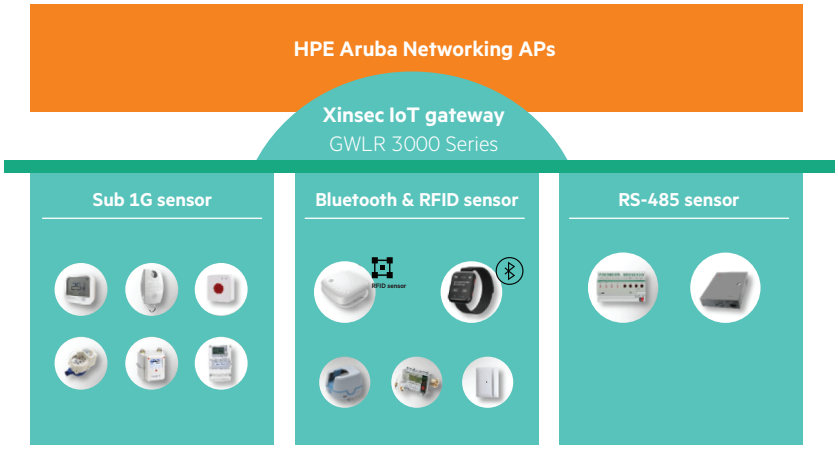

Figure 2. Xinsec IoT Network and HPE Aruba Networking APs

Unique value propositions

The joint HPE Aruba Networking-Xinsec solution brings with it many unique value propositions:

- Out-of-the-box integration with existing HPE Aruba Networking Wi-Fi infrastructure eliminates the need for new PoE cabling in areas with active infection-control barriers
- Supports LoRaWAN, 433MHz, and sub 1GHz IoT sensors
- Rich suite of IoT applications minimizes the need for custom application development to obtain insights from the IoT sensors.

Depend on Xinsec

Founded in 2006 and headquartered in Guangzhou, China, XINSEC is the world's leading provider of IOT overall solutions. The company provides complete IOT solutions and services for medium and large commercial users in China, East Asia, South Asia, West Asia and other regions.

xinsec.com.cn
Phone Number:
+86 400-902-0180
Guanghang building, 298 Lijiao Road, Haizhu District, Guangzhou, P.R.China

Certified interoperable

We've taken the guesswork out of deploying joint solutions by certifying the interoperability of Xinsec's Gateway with HPE Aruba Networking Wi-Fi access points via pass-thru PoE or USB. This allows joint deployments to be commissioned faster and simplifies maintenance of joint implementations.

Summary

Used in conjunction with HPE Aruba Networking Wi-Fi infrastructure Xinsec's healthcare IoT sensors and IoT platform allow clinics and hospital facilities to monitor critical parameters site-wide — from patient rooms to operating suites — with best-in-class security and no shadow IT.

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

All third-party marks are property of their respective owners.

PSO_hpeanwXinsec_LP_050824 a00125630ENW

Hewlett Packard Enterprise