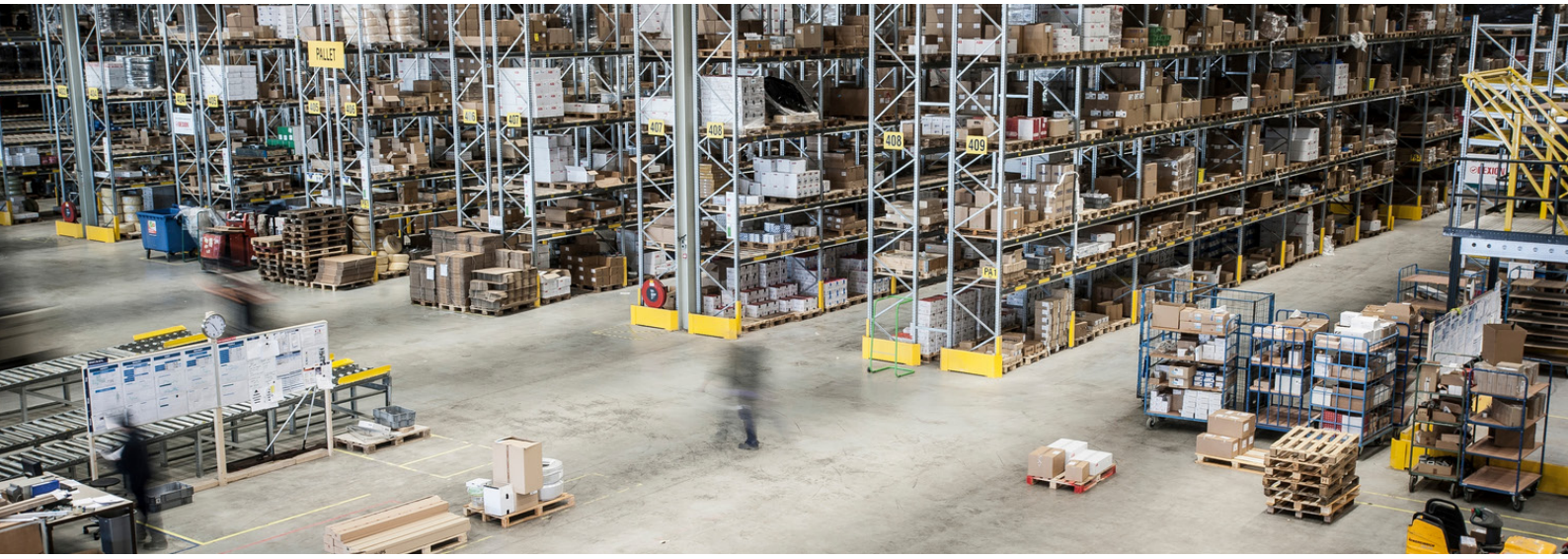
HPE aruba networking

Bridging IT and OT networks: access points as secure IoT platforms

HPE GreenLake



Benefits

- Addresses broad range of IoT applications with multiple IoT radios and USB ports.
- Eliminates the cost and complexity of gateways and IoT overlay networks.
- Enhances IoT security with tunneling, dynamic segmentation, policy management, and anomaly analytics.
- Provides ideal vantage point for IoT devices coverage and helps maximize IoT device battery life.
- Supports USB ports for additional IoT radios or powered sensors.
- Adds deployment flexibility with indoor, outdoor, and C1D2/ATEX Zone 2 APs with optional C1D1/ Zone 1 enclosures.
- Minimizes or eliminates the complexity of proprietary IoT mesh networks.

IoT devices present connectivity and security challenges

The proliferation of IoT devices at the edge creates a new set of challenges for IT. IoT devices use different connectivity types and communication protocols, often requiring vendor-specific gateways to manage devices and collect data. As a result, IoT devices are fundamentally untrustworthy and IoT gateways obscure devices on the network, causing a lack of visibility that creates greater risk. Integrating IoT data with business processes is therefore complex, requiring deep knowledge of IoT, data transport, data security, and business applications.

By combining IoT radios with a zero-trust network framework, HPE Aruba Networking access points can serve as secure IoT platforms that bolster network security, provide coverage for broad range of IoT devices, and eliminate the need for network overlays just for IoT devices.

Evolution of the access point

We are accustomed to thinking about Wi-Fi access points in the context of secure wireless network access, and for many years that was their primary function. The addition of BLE radios to HPE Aruba Networking access points (APs) opened the aperture beyond network access to include Internet of Things (IoT) devices including asset tags, mobile panic buttons, multi-axis accelerometers for monitoring rotating equipment, and a wide range of other building and factory automation sensors and actuators.

The introduction of HPE Aruba Networking's Wi-Fi 6 and Wi-Fi 6E APs heralded the advent of enhanced Wi-Fi radios with wake-up features for low-power devices, newer Bluetooth 5 and 802.15.4/Zigbee IoT radios, and expanded USB port functionality. When edge processing was required, these APs could run specialized container-based applications that locally processed IoT device data for services such a data deduplication. Taken together, these features further transformed the APs into secure, multi-purpose communication hubs that were both network access on-ramps and full-fledged Internet of Things (IoT) platforms.

HPE Aruba Networking Wi-Fi 7 access points build on the strengths of Wi-Fi 6 and 6E APs by adding additional IoT radios and USB ports and significantly expanded processing and memory for more and more sophisticated application processing at the edge. Dual USB ports can simultaneously support additional IoT radios or powered sensors like gunshot detectors or air quality monitors. Applications that run in APs are managed by HPE Aruba Networking Central and its IoT Operations capabilities. The greater memory and processing power of Wi-Fi 7 APs allow more powerful apps, downloaded from the IoT Operations App store, to perform sophisticated processing of IoT data, manage device operation, and report device status and location in real-time.

Now, all manner of low-voltage building systems — including comfort, intrusion detection, energy management, access control, personnel and asset tracking, preventive maintenance, air quality monitoring, electronic shelf label, and even gunshot monitoring — can reliably and securely communicate using nothing more than APs.

Ideal vantage

From their unique vantage as ceiling furniture, APs have an unobstructed, bird's-eye view of all nearby devices that is ideal for radio frequency (RF) and infrared (IR) communications.

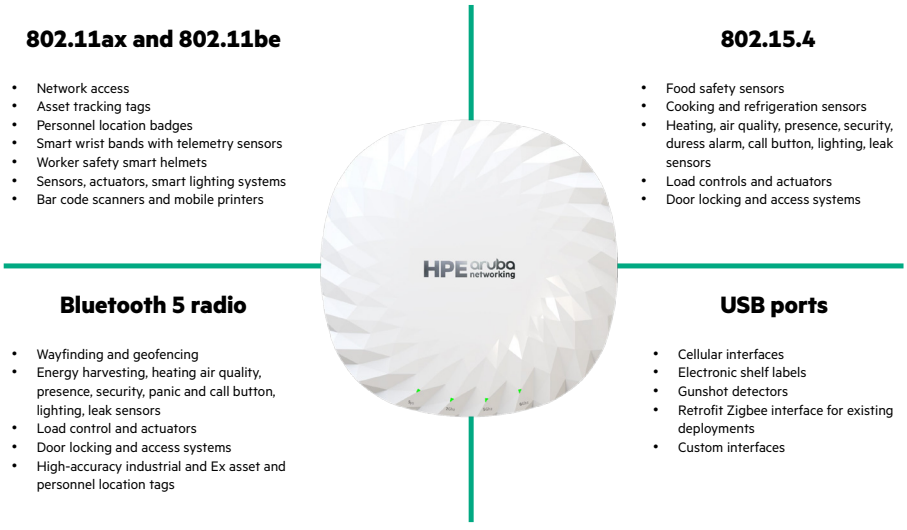


Figure 1. HPE Aruba Networking Wi-Fi 7 access points as secure IoT platforms

Bit rates fall proportionately with distance, so to deliver a high-speed user experience APs are typically spaced at 12-15 meter intervals in open areas, and often one per room. That spacing provides optimal coverage for energy-harvesting and battery-operated low power wireless IoT devices.

Many ceiling-mounted IoT devices need a local power source, ideally with battery back-up. However, mains-powered outlets are not typically found in ceiling plenums, nor are uninterruptible power supplies. HPE Aruba Networking APs provide a simple solution to the IoT power issue: USB ports provide a convenient source of power and high-speed data, without additional cable runs or equipment.

While the ceiling is an ideal location for powered detectors, it is suboptimal for temperature or humidity sensors because of wide swings caused by blowing air from HVAC systems. To detect temperature and humidity changes in the same way humans will perceive them, those sensors are almost always mounted roughly 1.1 meters from the floor, and the APs' wireless radios are ideally positioned more maximum coverage.

Hard wiring wall mounted sensors to ceiling mounted APs is never recommended because it requires piercing plenum spaces or infection control barriers in hospitals and clean rooms. The APs' wireless radios can preserve the integrity of plenums and barriers, while supporting virtually any type of in-room sensors.

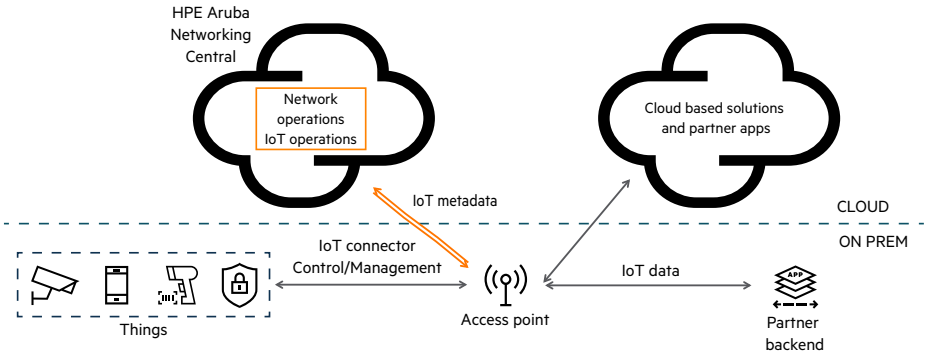


Figure 2. IoT Operations reduces the complexity associated with IoT by extending visibility to IoT applications and non-wi-fi IoT devices connected to the wireless LAN infrastructure.

Figure 3. HPE Aruba Networking HazLoc compliant APs do not require an additional enclosure for C1D2/ATEX Zone 2.

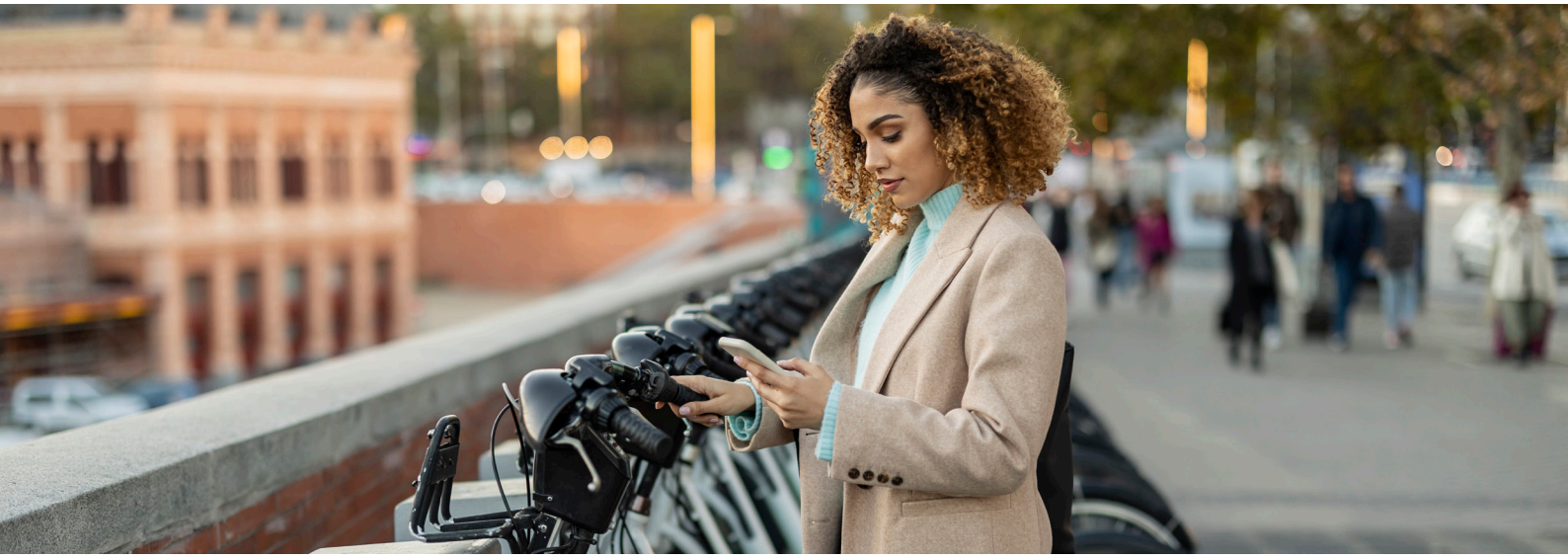
Figure 4. Optional C1D1/ATEX Zone 1 enclosure from HPE Aruba Networking Technology Partners

Less complex, more reliable

Access points eliminate the need for gateways by communicating directly with IoT devices and bidirectionally tunneling the data to target applications. Eliminating gateways reduces system complexity and cost, increases overall system reliability, and removes a typically vulnerable attack surface.

By communicating directly with IoT devices, the APs can also reduce the cluster size of IoT mesh networks, if not eliminate them altogether. Mesh backhaul multiplies the bandwidth consumed by every IoT transmission, an effect that is especially impactful in the congested 900MHz and 2.4GHz ISM bands.

Doing away with RF mesh networks, or allowing them to operate in smaller clusters, preserves bandwidth and minimizes the effect on other IoT devices operating on the same frequency. This has the added benefit of increasing the battery life of IoT devices, which don't need to retransmit backhaul packets as frequently, if at all.



HPE Aruba Networking 730 Series Campus APs key features

- Wi-Fi 7 (802.11be) supports multi-link operation (MLO) for channel aggregation and 4K QAM for higher throughput and lower latency.
- Unlocks the 6 GHz band to more than double the available capacity.
- Comprehensive tri-band coverage across 2.4 GHz, 5 GHz, and 6 GHz to deliver 9.3 Gbps maximum tri-band aggregate data rate.
- Unique Ultra Tri-Band (UTB) filtering enables 5 GHz and 6 GHz to operate without restrictions or interference.
- High availability with 5 Gbps dual Ethernets port for hitless failover of Ethernet and power.
- Built-in in GPS receiver, barometric pressure sensor, and intelligent software enable APs to self-locate and act as reference points for accurate indoor location measurements.

HPE Aruba Networking Central IoT Operations is a service available for APs running HPE Aruba Networking Wireless Operating System AOS-10 managed by HPE Aruba Networking Central, a cloud native, microservices-based platform that delivers the scalability and resiliency needed for mission-critical environments across the distributed edge. This capability eliminates the time-consuming and manual process of moving information from place to place or trying to correlate information across multiple view. It unifies visibility of IT and OT infrastructure within the network health dashboard by extending network monitoring and insights to BLE, Zigbee, and other non-IP IoT devices in the physical environment along with IP based IoT devices.

Enhanced IoT security and visibility

IoT devices are targeted for attack because they rarely have strong security built in, lack robust authentication, and store passwords in the clear due to price-constrained designs, limited compute capabilities, and design oversights. IoT devices are often located in public areas and susceptible to probing, manipulation, and network breaches. It's no wonder that vigilantly asserting trust over IoT devices and actively minimizing attack vectors are top corporate priorities.

Funneling IoT traffic through HPE Aruba Networking APs and switches allows multiple active and passive security mechanisms to protect IoT devices and their traffic. Trusted Platform Modules in the APs store credentials so probing an access point won't yield authentication, authorization, or encryption details. IoT data are securely tunneled from the APs to Aruba on-premises, virtual, and cloud with no clear text conversion in the chain.

Role-based policy decisions and access rights segment traffic from the APs to target destinations without complex and static network configurations and VLANs. HPE Aruba Networking's built-in Policy Enforcement Firewall provides deep-packet inspection of high-risk traffic. For example, a security camera can dynamically be assigned a role that restricts its traffic to a specified server, eliminating the opportunity for malicious entrance to other parts of the network.

HPE Aruba Networking's ClearPass fingerprints devices so they can automatically be assigned appropriate policies, and the HPE Aruba Networking anomaly analytics engine passively monitors activity and flags abnormal device behavior before harm can be done. If active mitigation is permitted, HPE Aruba Networking can quarantine IoT devices that violate policies, such as attempting to port scan or masquerade as another device.

IoT vendors that bypass the security funnel, say by using a LoRa network, put the enterprise at risk by routing traffic around these best-in-class protective mechanisms. Infected or compromised devices may simply go unnoticed as a result.

For additional visibility, HPE Aruba Networking Central Client Insights provides enhanced visibility of mobile and IoT devices with ML-based classification. This feature dynamically compares devices against crowdsourced fingerprints of known clients and applies MAC range classification for unknown devices. Through deep packet inspection, network devices are automatically categorized, accurate policies are enforced based on context and behavioral information. The system constantly monitors device behavior, always ensuring an up-to-date view of the network.

Battery savings

For Wi-Fi based, battery-operated devices, APs[1] support both Target Wake Time (TWT) and 20MHz channel IoT devices. TWT maximizes the sleep time of IoT devices up to several days before a check-in, extending battery life up to 10x longer than previous Wi-Fi technologies. With wake-up time negotiated between the device and AP, TWT delivers a more deterministic, power-efficient operating mode. 20MHz operation allows for lower power operation, further extending battery life. And with the ability to support 1,000 IoT devices per radio, the APs can scale to IoT deployments of any size.

The platform of choice

Many companies no longer differentiate between IT and IoT devices because of the widespread proliferation of IoT devices on IT infrastructure. Achieving more reliable and deterministic operation, with uniform security policies and visibility across both IT and IoT devices, requires a new approach to system implementation. HPE Aruba Networking's feature-rich access points are the platform of choice for that transformation.

For more information, visit https://www.arubanetworks. com/products/wireless/access-points

[1] HPE Aruba Networking Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 access points.

[2] Available services may vary by device type and AP interface.

Make the right purchase decision. Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

SO_APAsSecureIoTPlatforms_RVK_041124 a00111192ENW