aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

BRIDGING IT AND OT NETWORKS: ACCESS POINTS AS IOT PLATFORMS

EVOLUTION OF THE PLATFORM

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 Aruba access points opened the aperture beyond network access to include wayfinding, geofencing, push messaging, and asset tracking. Still the primary function was network access.

The introduction of Aruba's Wi-Fi 6 Access Points (APs) heralds the advent of enhanced Wi-Fi radios with wake-up features for low-power devices, new Bluetooth 5 and 802.15.4 IoT radios, and expanded USB port functionality. Taken together, these features transform Aruba APs into secure, multi-purpose communication hubs that are both network access on-ramps and full-fledged Internet of Things (IoT) platforms.

Now, all manner of low-voltage building systems — including comfort, intrusion detection, energy management, access control, personnel and asset tracking, man-down, call button, leak detection, and even gunshot monitoring systems — can reliably and securely communicate via Aruba's Wi-Fi 6 APs.

BENEFITS

- Multiple IoT radios and flexible USB port address broad range of IoT applications
- Ideal positioning and coverage for IoT RF and IR devices
- Maximizes battery life of IoT devices
- Indoor, Outdoor and C1D2/ATEX Zone 2 support, with multiple partners supporting Zone 1 enclosures
- Eliminates the cost of gateways and IoT overlay networks
- Minimizes or eliminates the complexity of mesh
- Tunneling, dynamic segmentation, policy management, and anomaly analytics enhance IoT security*

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 (RF) and infrared (IR) communications.

802.11ax Wi-Fi Radios

802.11ax network access
Asset tracking tags
Personnel location badges
Smart wrist bands with telemetry sensors
Worker safety smart helmets
Sensors, actuators, and smart lighting systems
Bar code scanners and mobile printers

802.15.4 ZigBee Radio

Food safety sensors
Cooking and refrigeration sensors
Heating, air quality, presence, security, duress alarm, call button, lighting, leak sensors
Load controls and actuators
Door locking and access systems

Bluetooth 5 Radio

Wayfinding and geofencing
Energy harvesting heating air quality, presence, security, panic, call, button, lighting, leak sensors
Load controls and actuators
Door locking and access systems
High-accuracy industrial and Ex asset and personnel location tags

USB Port

Cellular interfaces
Electronic shelf labels
Gunshot detectors
Retrofit Zigbee interface for existing deployments
Custom interfaces

Figure 1. Aruba Wi-Fi 6 Access Point as an IoT Platform

Bit rates fall proportionately with distance, so to deliver a high-speed user experience Wi-Fi 6 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 RF and IR IoT devices.

Many ceiling-mounted IoT devices need a local power source, ideally with battery back-up. Mains-powered outlets are not typically found in ceiling plenums, nor are UPSs.

Aruba APs provide a simple to solution to the IoT power issue: a USB port provides a convenient source of power and high-speed data, without additional cable runs or equipment.

For Wi-Fi based, battery-operated devices, Aruba's Wi-Fi 6 APs 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.

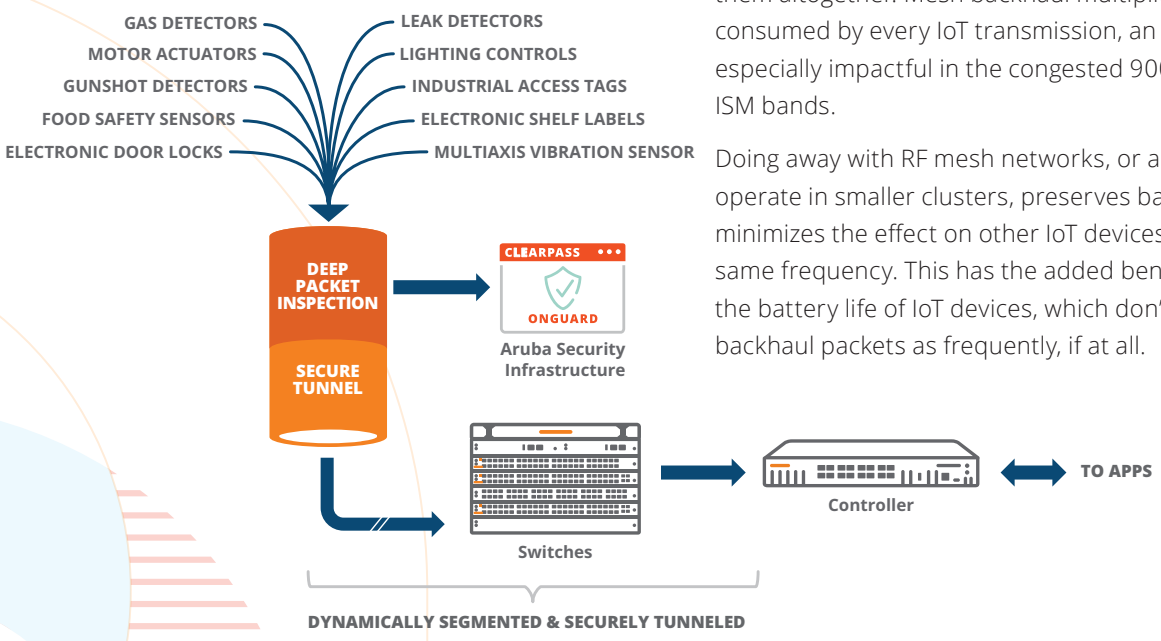

Figure 2. IoT Device Security Funnel

Figure 3. For hazardous location requirements, Aruba provides C1D2 and ATEX Zone 2 certified access points. Lightweight and ruggedly constructed, these access points support IT, IoT and operational technology devices in hazardous locations.

Figure 4. ArubaEdge Technology Partners offer C1D1 and ATEX Zone 1 enclosures for use with Aruba access points located in highly explosive environments.

LESS COMPLEX, MORE RELIABLE

Wi-Fi 6 APs 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.

ENHANCED IOT SECURITY

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 Aruba 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 controllers 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. Aruba'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.

Aruba's ClearPass fingerprints devices so they can automatically be assigned appropriate policies, and the Aruba anomaly analytics engine passively monitors activity and flags abnormal device behavior before harm can be done. If active mitigation is permitted, Aruba 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.

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. Aruba's feature-rich Wi-Fi 6 Access Points are the platform of choice for that transformation.

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

* Available services may vary by device type and AP interface, i.e., some services may be available for 802.11ax and not for Bluetooth 5.

SO_BridgingITandOTNetworks-AccessPointsAsIOTPlatforms_RVK_030321 a00111192enw