WHITE PAPER

aruba

a Hewlett Packard
Enterprise company

DESIGNING HYPER-AWARE HOSPITALITY FACILITIES

SECURE INFRASTRUCTURE AND PARTNER SOLUTIONS FOR HOTELS, RESORTS, AND CONFERENCING VENUES

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

At its core, the Internet of Things (IoT) is an amalgamation of machines in the physical world, logical representations of the physical phenomena acted upon by those machines (voltage, temperature, flow, speed), contextual data generated by networks connecting the machines (identity, location, applications in use), and business applications that analyze, mine, share, and respond to those data. In hospitality applications, the machines and applications are tailored to optimizing human activity monitoring, organizational redesign, human productivity, and health and safety. The ultimate goal of implementing IoT in hospitality is to improve efficiency, build loyalty, create unique experiences, and improve safety, which will in turn drive profits.

By securely interfacing IoT devices, and generating contextual information, Aruba's networks enable venue control, guest services, and business applications to become hyper-aware of their operating environments. Aruba's unified infrastructure, zero-trust security, and AI-powered software - used in conjunction with solutions from key technology partners – enables hospitality providers to successfully deploy and exploit IoT solutions. The richer the set of available data and context, the greater the opportunities to boost efficiency, productivity, profitability, reliability, safety, and security.

Aruba's Edge Service Platform (ESP) is the first extensible infrastructure to combine information technology (IT), operational technology (OT), and IoT into a single framework with open interfaces and APIs. Third-party devices, applications, and services can use the open interfaces and APIs to plug vertical-specific systems into ESP without having to change the underlying infrastructure. This allows ESP customers to easily support changing IT, IoT, and facilities-related operational technology (OT) requirements by plugging new systems into their existing Aruba infrastructure – no rip-and-replace needed.

ESP is built on three foundational services, and APIs provide access to technology partner devices and applications that need to access any or all of them:

- Unified infrastructure that encompasses wired and wireless networks, OT/IoT interfaces, wide area networks, and cellular networks;
- Zero trust security framework in which no user or device is granted entry or on-going access until proven trustworthy;
- Artificial intelligence for operations (AIOps) in which multiple AI and big data services are leveraged to continuously detect, monitor, isolate, and remediate issues impacting RUN excellence.

Aruba has built a broad ecosystem of hospitality technology partners whose products and services interface with ESP to address guest experiences, hospitality operations, and facilities applications.

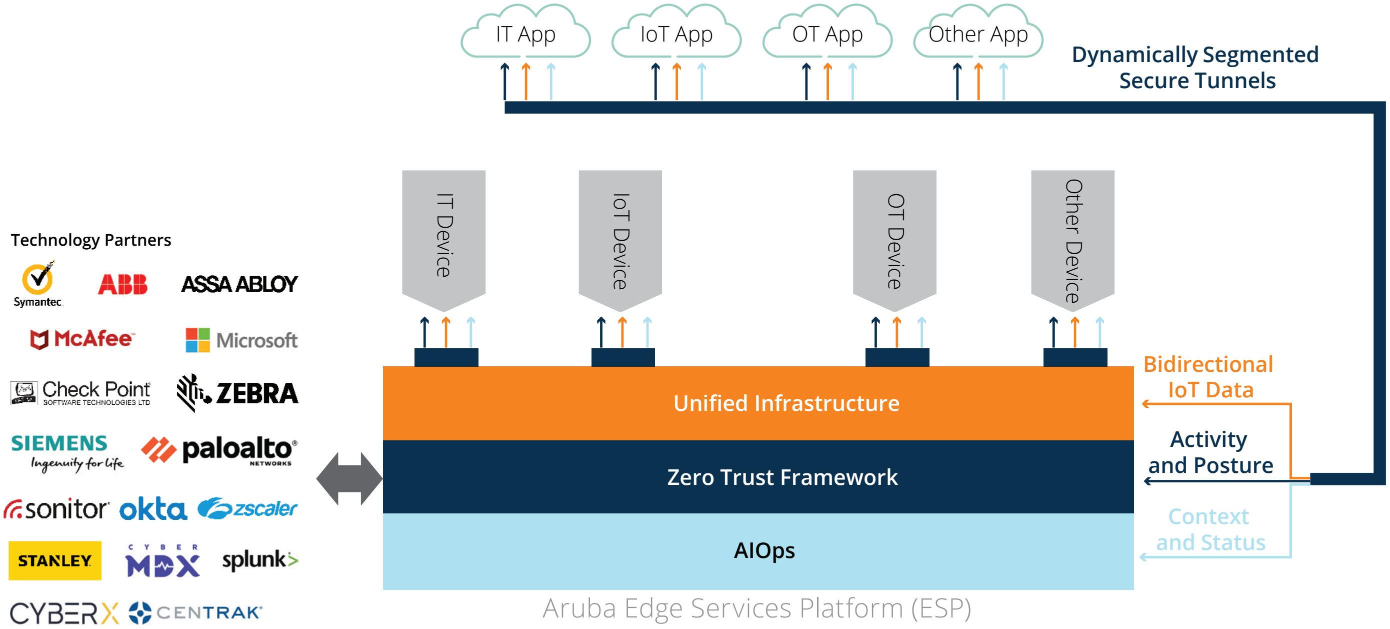


Figure 1: Aruba ESP And Technology Partner Ecosystem: The Foundation For Hyper-Aware Solutions

Solutions from Aruba and its technology partners are applicable across a broad range of hospitality markets. Use cases and partners discussed in this white paper include:

- Human Productivity – Activity Monitoring
  - Integrated Wi-Fi Services and Property Management System Integration (Eleven)
  - Real-Time Personalized Promotions to Drive Engagement (Skyfii, Zoox Smart Data)
  - Physical Distance Monitoring and Contact Tracing (AiRISTA Flow, AisleLabs, CohuHD, CXApp, Kiana, Patrocinium, Skyfii)
- Migrating from Break/Fix to Proactive Maintenance (ABB)
- Building Control and Digital Twin Enablement (EnOcean and Microsoft)
- Automating Network Access to Enhance the Efficiency of Employees, Service Personnel and Contractors (Aruba, Envoy)
- Securely Sharing Facility Wireless Networks Without Losing Control (Aruba MultiZone)
- Seamless 5G to Wi-Fi Roaming Without Distributed Antenna Systems (Aruba Air Pass)
- Redundant Intra-Site Wireless Video and Data Links (Aruba 5/60GHz Access Point)
- Reducing Mean Time to Repair with Real-Time Location Services (Aruba APs and Meridian)
- Monitoring the Switching Fabric to Detect IoT Issues (Aruba NAE Python scripting)
- Enhancing the Reliability and Quality of Mobile Staff Communications (Zebra)
- Guest, Staff and Building Security
  - Reduce Costs and Improve Guest Experiences with Electronic Door Locks (ASSA ABLOY)
  - Shipboard Real-Time Location Services (DeCurtis, Favendo)
  - Mobile Panic Button Location Solutions (TraknProtect)
  - Vaping and Air Quality Monitoring (IPVideo)
  - Gunshot Detection (AmberBox)
  - Context-Aware, Real-Time Integrated Emergency Response and Notification (Patrocinium)

INTRODUCTION

What is a hyper-aware hospitality facility, and why is the Internet of Things (IoT) relevant to it? A hyper-aware hospitality facility is an instrumented building in which applications are cognizant of the contextual status of the environment, employees, guests, energy requirements, service needs, security, and safety. IoT is collectively the eyes and ears of a hyper-aware hospitality facility, and generates logical representations of physical data, i.e., temperature, current consumption, door lock status, and occupancy, among many others. These data are supplemented with contextual information generated by the data network, i.e., identity, location, and applications in use. The combination of data and context enables hoteliers to become cognizant of, and responsive to, the occupants and their environment. The richer the set of data and context, the more adaptive the venue can become.

Before the advent of IP networks, hospitality subsystems operated autonomously from each other with independent wiring and separate applications for telephone, fire alarm, security, closed circuit television (CCTV), entertainment, power management, lighting, and heating/ventilation/air conditioning/refrigeration (HVACR) systems. The protocols, communication infrastructure, and even the means of powering each system were tailored to the specific application: single use key cards, front desk check-in and check-out, basic guest Wi-Fi, dedicated closed loop systems for HVAC, fire alarms, and service dispatch and delivery through paging and/or public address systems.

In some cases, local regulations have mandated isolation, fire alarms being a case in point. In other instances, manufacturers have wanted their devices to be isolated because it locks customers into lucrative service contracts. Regardless of the reason, many hospitality systems remain isolated and unable to share edge data.

The challenge is that cognitively-aware hospitality applications need edge data to deduce status and infer needs. For example, an automated business center room reservation system needs identity, presence, calendar, and location data to know when attendees are present so a meeting can start, and to infer when a room can be released due to non-use. Physical layer and protocol converters can address data exchange, however, expecting the property management system (PMS) to share needed context and data is highly problematic.

The 'Achilles heel' of hospitality IoT is security because IoT devices are fundamentally untrustworthy. The reason is simple. The engineers who design IoT devices are typically trained on process reliability and application-specific architectures, and their objective is to make products work reliably for as long as possible. Cybersecurity expertise sits with information technology (IT) engineers. Adhering strictly to a zero trust framework, IoT devices should not be allowed on a network unless and until trust can be asserted to the same standard as it is with IT devices.

Addressing the shortcomings of IoT device security isn't a trivial task. The diversity of installed legacy devices is vast; many have been in service for decades and predate the advent of both modern cybersecurity and the Internet. Replacing legacy devices is often technically and economically unviable, not to mention highly disruptive to on-going operations. Many new IoT devices also lack sound cybersecurity features. For this reason, many Chief Information Security Officers (CISOs) will not permit either IoT devices or gateways on their networks, a testament to the scope of the problem.

The goal should be to create a zero trust defensive framework in which no device or user is trusted until proven otherwise. The framework should leverage contextual information from a multitude of sources to scrutinize user and device security posture before and after they connect. Doing so helps overcome the limitations of fixed security perimeters tied to physical boundaries, which break down in the face of IoT devices that can connect and work from practically anywhere.

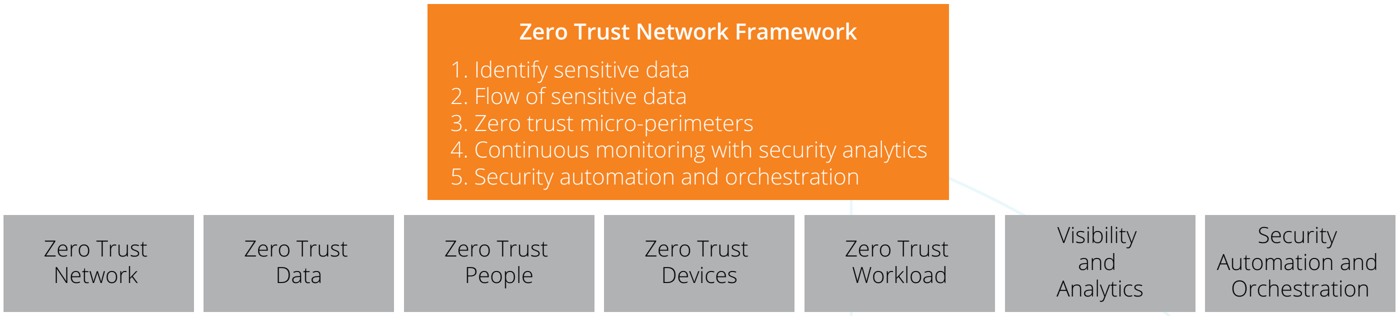

Zero Trust Network Framework
1. Identify sensitive data
2. Flow of sensitive data
3. Zero trust micro-perimeters
4. Continuous monitoring with security analytics
5. Security automation and orchestration
Zero Trust Network
Zero Trust Data
Zero Trust People
Zero Trust Devices
Zero Trust Workload
Visibility and Analytics
Security Automation and Orchestration

Figure 2: Zero Trust Framework

IoT security should include the layered protective mechanisms in accordance with a zero trust framework:

- Authenticating source/destination devices and monitoring traffic patterns;
- Encrypting data packets using commercial and, where applicable, government encryption standards;
- Micro-segmenting traffic inside secure tunnels to ensure devices communicate only with their intended applications;
- Fingerprinting IoT devices to determine if they are trusted, untrusted or unknown, and then applying appropriate roles and context-based policies that control access and network services;
- Inspecting north-south traffic with application firewalls and malware detection systems to monitor and manage behavior;
- Leveraging enterprise mobility management (EMM), mobile application management (MAM) and mobile device management (MDM) systems to monitor behavior and protect other devices in the event of a policy breach; and
- Relying on AI-based analytics to continuously look for anomalous behavior even after trust has been asserted.

Legacy IoT devices can be identified as known or unknown upon connecting to the network using their MAC address and other associated data stored in an external or internal database. The profiling data should flag if a device changes its mode of operation or masquerades as another IoT device – a common issue with MAC-based authentication - and then automatically modify the device's authorization privileges. For example, if a Windows tablet PC tries to masquerade as a hotel door lock, network access should be immediately denied.

Mitigating IoT security risks requires a blended approach that includes methods taken from mobile, cloud, automation, and physical security. The sheer breadth of IoT solutions mandates an array of embedded trust, device identity, secure credential, and real-time visibility solutions. New and unfamiliar cybersecurity risks include: IoT solutions can change the state of a digital environment, in addition to generating data, and this variability of state requires a new view of cybersecurity; IoT environments include unattended endpoints – locally and in remote sites - that can be both physically probed and logically attacked; and machine-to-machine (M2M) authentication works in newer IoT devices but not in many legacy devices, creating trust gaps between generations of devices and gateways.

The hospitality market has grown rapidly since the dawn of simple guest access Wi-Fi, and the rate of technological change has caused new challenges to brands, operators, and IT departments struggling to keep up. As a consequence, today's hyper-aware hospitality solutions require expertise outside the realm of traditional hotel services companies. Automated IT, cloud-based management, and augmented reality expertise may be needed for activity monitoring, intelligent spaces, and servicing complex systems, respectively. Cybersecurity has to underpin all intelligent hospitality systems, yet is not a core skill for most hospitality suppliers, nor are location-based services which have long been the province of IT. And finally, there's analytics, a family of highly specialized tools that help companies monetize the data they collect that is yet another province of IT.

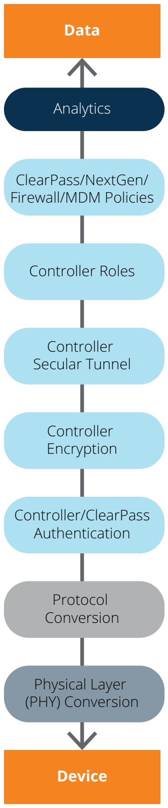

Data
Analytics
ClearPass/NextGen/ Firewall/MDM Policies
Controller Roles
Controller Secular Tunnel
Controller Encryption
Controller/ClearPass Authentication
Protocol Conversion
Physical Layer (PHY) Conversion
Device

Figure 3: IoT Protection Mechanisms

Bridging the divide between IT and IoT vendors is paramount to the successful implementation of a zero trust framework. Aruba's policy enforcement firewall and encryption, working in concert with secure tunneling and the ClearPass Policy Manager, can protect IoT systems and secure the network edge. However, policies are only as effective as the information used to build them, and that must be based on a deep understanding of automation processes and procedures underpinning hospitality operations. Applying a collaborative systems approach to the problem will help identify the IoT threat vectors and the security technologies needed for remediation.

Transforming untrusted IoT devices into trusted data will allow the strategic business goals of hyper-aware hospitality solutions to be realized without incurring unacceptable risk. Let's now examine how to align a company's strategic goals with the implementation of hyper-aware hospitality solutions.

BUSINESS TRANSFORMATION ENABLED

Some years ago the head of the Industrial Engineering Department of Yale University said, "If I had only one hour to solve a problem, I would spend up to two-thirds of that hour attempting to define what the problem is."1 In the same vein, a woodsman was once asked, "What would you do if you had just five minutes to chop down a tree?" He answered, "I would spend the first two and a half minutes sharpening my axe."2 Regardless of your industry or task, it's important to be prepared, carefully defining your objectives and selecting the tools needed to achieve them.

Sadly, this lesson is often overlooked when it comes to hospitality IoT projects. Whether it's the allure - or misunderstanding - of the IoT concept, fear of being left behind by competitors, or pressure to do something new, companies frequently rush headfirst into hospitality IoT projects without clearly defining objectives, value propositions, or the suitability of tools. The result is a high rate of failure, and disillusionment among customers.

Originally intended to describe an ecosystem of interconnected machines, the phrase "Internet of Things" has been taken literally to mean connecting all devices to the Internet. The overarching objective of IoT is not to connect every device to the Internet. IoT devices are vessels for context and data, and the objective is to tap only relevant information and devices.

How does one determine what is or is not relevant information? Relevance is established by a chain that stretches from the enterprise's strategic goals, to business objectives designed to achieve those goals, to what Gartner3 calls "business moments" – transient, customer-related opportunities that can be dynamically exploited. A business moment is the point of convergence between the owner's strategic goals and relevant IoT context and data that when properly exploited will positively change reliability, performance, and/or safety.

These business moments must be carefully orchestrated, even if they appear spontaneous to the guest or owner. Success hinges on a second chain that stretches from relevant IoT context and data thru the IoT architecture that accesses and conveys them to a target business moment. If the chain is poorly executed, say because the IoT architecture can't extract relevant information, then the business moment may pass without result, or could even trigger negative results to the detriment of the strategic goals.

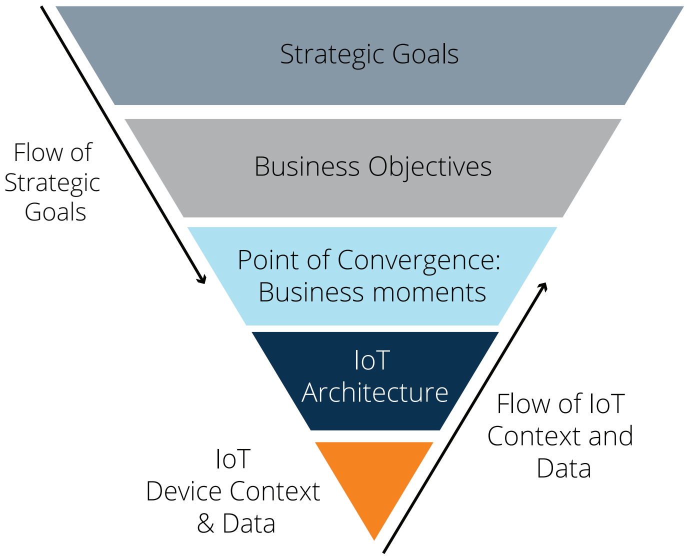

Strategic Goals
Business Objectives
Point of Convergence: Business moments
IoT Architecture
Flow of Strategic Goals
Flow of IoT Context and Data
IoT Device Context & Data

Figure 4: IoT Strategic Hierarchy

And so, we return full circle to the professor and the woodsman. The first order of business in hospitality IoT project is to identify the strategic business goals to be achieved. Those should flow down into a series of specific objectives that rely on successfully delivered business moments. The IoT architecture is the tool by which relevant IoT context and data can be extracted and exploited to reorient behavior, attitudes, and actions in favor of the strategic goals.

Business goals and objectives inform the hospitality IoT architecture and relevant devices to tap, not the other way around. IoT solutions selected for eye candy appeal or hype alone will go wanting. Aruba's goal is to help customers identify relevant IoT data and context, define and successfully deliver business moments, and, in turn, attain their business objectives and strategic goals.

Where does one start this process? The first order of business in any hospitality IoT project is to identify the customer's strategic goals and the associated business objectives that must be met. Those will inform the business moments for which the IoT architecture needs to extract relevant IoT data and context. Is the objective to reduce guest wait times by more efficiently using automated check-in or check-out? Enhance personal safety with social distancing and thermographic monitoring? Quickly locate luggage carts or dining trays? Provision location-based panic buttons to improve personal safety and well-being? Lower energy consumption? The answer(s) will impact the business moments that need to be delivered, and what constitutes relevant data and context.

Business moments inform the IoT architecture, not the other way around. One-size-fits-all hospitality solutions are doomed to fail because they won't be tailored to deliver meaningful business moments.

This document presents IoT use cases that are relevant to a broad range of hospitality applications. Most of the use cases include at least one Aruba technology partner whose solution, used in concert with Aruba infrastructure, helps address strategic business challenges.

HOSPITALITY IOT MARKET

The total economic impact of IoT applicable to hospitality in 2025 is expected to be between $260B-$777B4. Top areas impacted by IoT include automated check-in and check-out ($150B-$380B), real-time personalized promotions ($89B-$348B), human productivity and activity monitoring ($19B-$43B), and guest, staff and building security ($3B-$6B). Automated check-in and check-out is expected to result in 40-88% time reduction and 75% savings in costs, while real-time personalized promotions and activity monitoring yield 3-5% improvement in productivity. Guest, staff, and building IoT-based security should yield a 20-50% reduction in labor costs.

Commercial real estate services company Jones Lang LaSalle observed that, in general, real, estate tenants spend roughly $3 per square foot (0.092 per square meter) per year for utilities, $30 for rent, and $300 per for payroll. This "3-30-300" rule of thumb makes clear that the biggest financial benefits can be obtained by making people more productive and efficient, and the same applies to hospitality.

Historically, hospitality IoT initiatives focused on energy efficiency because this was – and remains – one of the specialties of building automation vendors. Pivoting towards human productivity requires vendors and applications that create cognitively-aware venues, and this in turn requires access to information about location, identity, applications in use, and other forms of contextual information.

Mashing up IoT data with contextual information can change the way in which machines and humans interact to make people more productive. Done well, frictionless machine-human interchanges belie the complexity of the computing, security, and communications systems needed to accomplish the task. The challenge is finding new ways to simplify human interaction with complex machine-based systems, and new ways to train integrators to install and support these systems.

The breadth of hospitality IoT initiatives mandates close attention to what a hotelier is trying to achieve. For example, is a point solution required to address a specific problem, i.e., staff panic buttons? Or is an optimized system-level solution required, i.e., migrating from a manual check-in process to an automated, identity-based solution with electronic key delivery and billing?

In all cases an extensible platform is required because hospitality IoT requirements change over time, however, by itself a platform alone is insufficient to build the full breadth of required solution. The platform needs to be supplemented with specialized technology partners to build compelling use cases. Accordingly, Aruba has curated a world-class ecosystem of infrastructure, security, and location technology partners, the solutions of which have been validated to be interoperable with Aruba infrastructure. Aruba and its technology partners have crafted a broad range of hyper-aware hospitality facility use cases, the results of which are described below.

HUMAN PRODUCTIVITY – ACTIVITY MONITORING

Large hotel brands require a simple, effective way to centrally manage guest Wi-Fi across multiple locations. With a disparate variety of legacy networks and client devices, rising bandwidth demands, and multiple service providers to manage, many hoteliers struggle to deliver a consistent, secure, and centrally-managed guest Wi-Fi experience. According to a study by Hotel Internet Services (HIS), over 90% of respondents indicated that access to guest Wi-Fi was "very important," with 58% stating that the quality of guest Wi-Fi was "highly likely" to impact future booking decisions6. Selecting the wrong wireless solution can translate into lower customer satisfaction scores and revenue opportunities.

Contextual information from Aruba infrastructure is central to the delivery of automated, efficiency-enhancing guest services. Automated check-in and check-out hinge on the ability to identify guests as they approach the property, and require reliability location and identity services to work effectively. Once rooms have been assigned, electronic keys need to be activated and linked to the property management system (PMS) to provide proper access. Location-aware infrastructure can transform traditional room service into "anywhere service" and generate new revenue streams.

INTEGRATED WI-FI SERVICES AND PROPERTY MANAGEMENT SYSTEM INTEGRATION

Eleven pioneered cloud-based guest Wi-Fi management software for the hospitality industry in 2002. Today, companies across multiple industries trust Eleven to keep more than 9 million guests connected every month. Eleven's hospitality guest Wi-Fi solutions, based on the ElevenOS platform, have been deployed by brands worldwide. The solution features PMS integration with bill-to-room capability, loyalty system integration for Wi-Fi access via program membership, and conference and event connectivity management.

Aruba and Eleven have partnered to integrate Aruba's Wi-Fi 5 and Wi-Fi 6 wireless infrastructure with ElevenOS for more reliable, scalable and easy-to-use guest Wi-Fi. When a guest enters a property, they're prompted to join the network using a customizable captive portal. The guest is centrally authenticated onto the Aruba network regardless of the service provider used. Once on the network the guest can access conference groups, request personal area networks, view promotions, or request tiered access. Authentication options include Aruba Air Pass auto authentication, and e-mail together with PMS or loyalty sign-in.

Whether it's a single property or a global chain, all locations can be managed via a Web interface that is user-friendly and designed for non-technical employees. Front desk and non-IT staff members can set up customized dashboards to create promotions, modify connectivity plans, manage conference Wi-Fi access, create personal area networks, view network usage and devices, and modify tiered access.

To configure the Aruba controller with ElevenOS, the hotelier simply creates a whitelist and sets up a RADIUS server with a server group. From there, the XML server and AAA Profile are set up and L3 authentication configured.

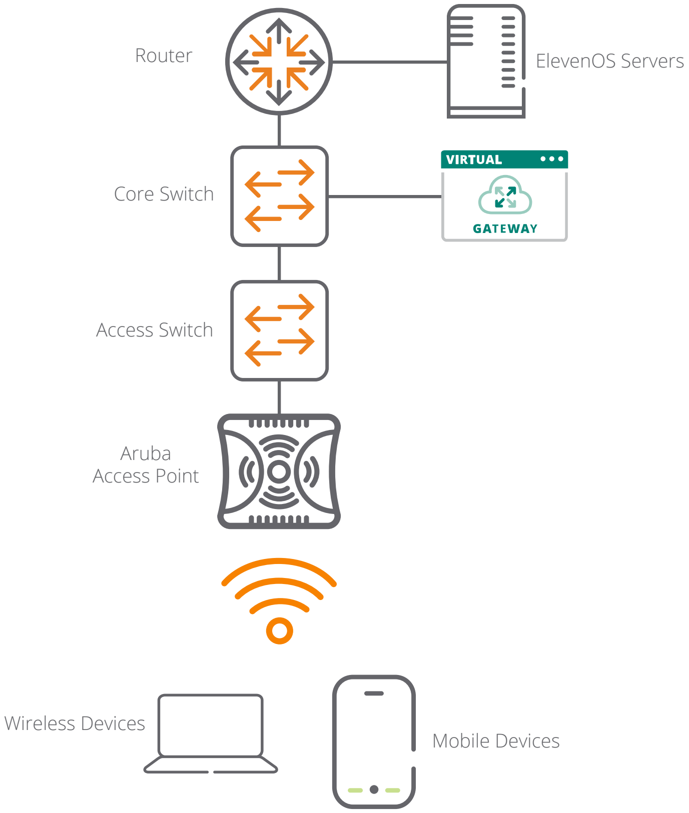


Figure 5: Aruba and Eleven Joint Solution Diagram

REAL-TIME PERSONALIZED PROMOTIONS TO DRIVE ENGAGEMENT

Marketers and operators of hotels, resorts, shopping centers, entertainment pavilions, and other physically large venues face three common challenges in their attempts to deliver better visitor experiences:

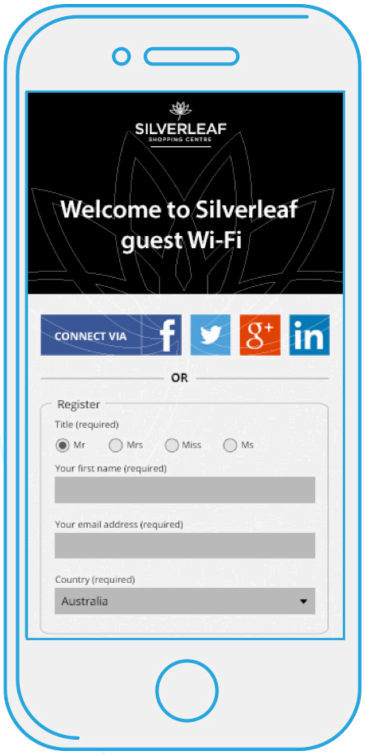
- Visitors often remain anonymous and there are few effective ways to collect information about them;
- It is challenging to understand visitor behavior within a physical space, and even harder to understand which factors influence that behavior; and
- Physical venues have few channels by which to deliver marketing messages to visitors. Generic, untailored messages rarely resonate with visitors.

Venues often use trial and error in an attempt to meaningfully engage with visitors and enhance on-site experiences, often with poor results. Yet they still try because the benefits of successful engagement are significant. It is estimated that by 2025, customer service organizations that embed AI in their multichannel customer engagement platform will elevate operational efficiency by 25%7.

To overcome these limitations, Aruba enables venues to leverage existing Wi-Fi networks to gather visitor contact information, profile details, and behavioral data. Aruba's technology partners then leverage these data to create highly specific multimedia messaging tailored to each visitor.

Skyfii's vision is to improve visitor experience by understanding user behavior thru its Skyfii IO suite of integrated visitor analytics and engagement software for physical venues. By pairing intelligent software with data science and marketing services, Skyfii can deliver tangible business outcomes through timely communication with guests and visitors with relevance to each individual's personal preferences, behaviors, and physical location.

To provide venue operators with new insights about visitor behavior, Skyfii IO uses data from a variety of network sources and aggregate it into a single system of record. A key source of this data comes from Skyfii's integration with Aruba ClearPass and Aruba Analytics and Location Engine (ALE). When guests connect to the Aruba Wi-Fi network they are greeted by a branded portal for login and thereby enriching the guest profile and adding visibility into how visitors, through their Wi-Fi devices, move about the space.


SILVERLEAF
SHOPPING CENTRE

Welcome to Silverleaf guest Wi-Fi

CONNECT VIA

OR

Register

Title (required)

● Mr ○ Mrs ○ Miss ○ Ms

Your first name (required)

Your email address (required)

Country (required)

Australia

Figure 6: Example of a Branded Portal Powered by Skyfii

With Skyfii IO Insight, venue operators can turn WLAN provided raw data into insightful and easy-to-understand reports that help them gain insights about the visitor experience. These same insights also power Skyfii IO Engage, which allow venue operators to create highly targeted visitor segments and send tailored messages based on location, behavior and profile. Since Skyfii IO is a cloud-based SaaS platform, it can be integrated with existing Aruba Wi-Fi Networks remotely without the need for additional on-site hardware.

The joint Aruba and Skyfii solution delivers five key benefits to hoteliers and venue operators:

- Automatically adds new visitors to customer relationship management applications while enriching existing records by progressively profiling all Wi-Fi guests;
- Monitors visitor flow to determine which areas are congested or overlooked, measure the impact of layout changes, and observe where staffing need to be adjusted;
- Compares how locations cross-company compare with each other based on foot traffic, visitor dwell time, facilities utilization and shopper affinity;
- Drives visitor engagement by delivering highly tailored offers to visitors, capturing exit surveys, and better understanding visitor demographics; and
- Attributing visits and purchases to campaigns and highlighting which campaigns most affect guest behavior.

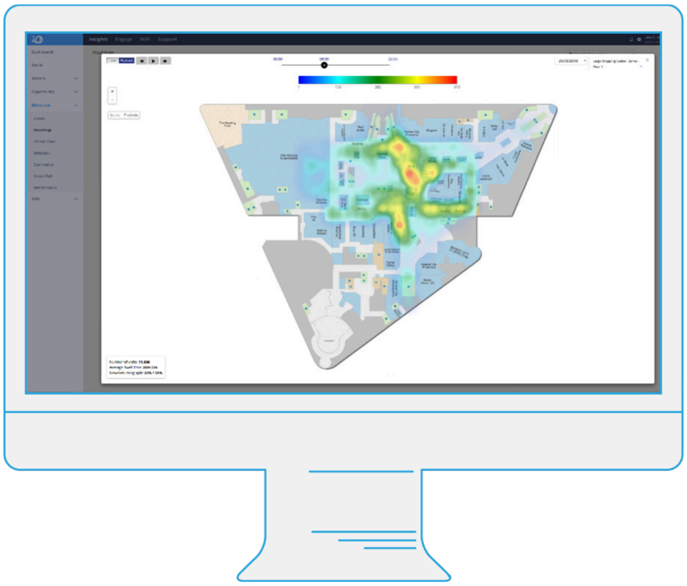


Figure 7: Contextual Data from the Aruba WLAN Enables Skyfii to Drive a Personalized Guest or Visitor Experience.

A joint Aruba and Skyfii solution helps transforms visitor experiences and can substantially impact the bottom line of hotels, conference venues, convention centers, and other large venues.

Founded in 2010, Zoox helps customers capture, process, and act upon data by delivering targeted, high-conversion advertising campaigns and direct offers to guests. The platform provides extensive reporting on viewership, interest, and conversion rates, helping hoteliers assess their return on marketing investments.

Aruba and Zoox Smart have partnered to certify the integration of Aruba's wireless and location infrastructure with the Zoox Smart platform to enable personalized marketing, loyalty, and sales campaigns. The joint solution leverages Aruba's Wi-Fi 5 and Wi-Fi 6 wireless infrastructure and ALE. When visitors enter a venue, they authenticate onto the guest Wi-Fi network using the Zoox captive portal, logging in with social media credentials. The Zoox platform automatically pulls identity and location from the Aruba infrastructure, and user data from social media platforms. Typical social data includes gender, hometown, profession, brands liked and music preferences. These data are then accessible through the Zoox Media tailored dashboards for targeted campaigns.

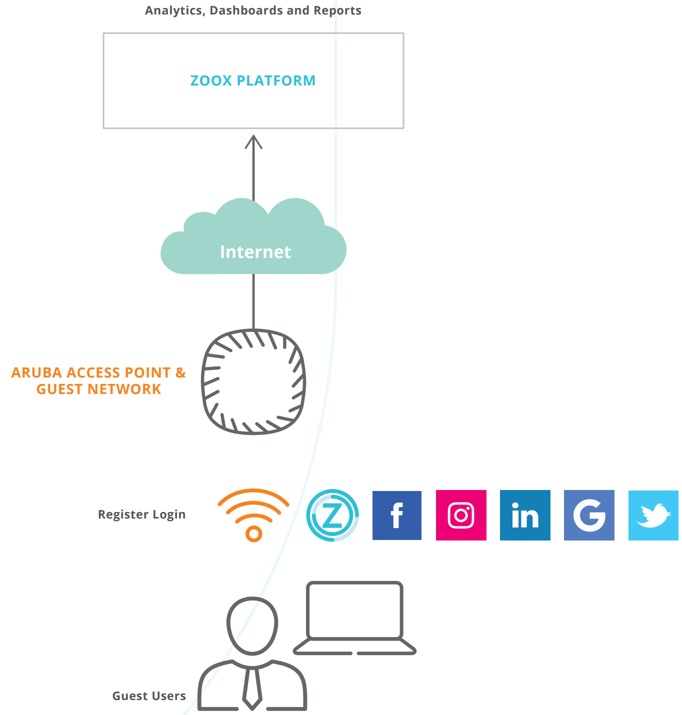
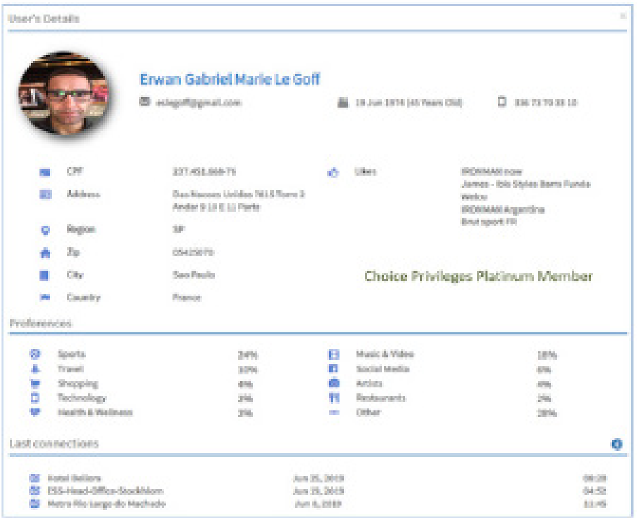

Analytics, Dashboards and Reports
ZOOX PLATFORM
Internet
ARUBA ACCESS POINT & GUEST NETWORK
Register Login
Guest Users

Figure 8: Aruba and Zoox Smart Data Joint Solution Diagram



User's Details

Erwan Gabriel Marie Le Goff

eslegoff@gmail.com | 19 Jun 1974 (45 Years Old) | 336 73 70 33 10

CPF	237.451.868-75	Likes	IRONMAN now James - Ibis Styles Barra Funda Webcv IRONMAN Argentina Brut sport FR
Address	Das Nacoes Unidas 7415 Torre 3 Andar 9 13 E 11 Parte		
Region	SP		
Zip	05425070		
City	Sao Paulo		Choice Privileges Platinum Member
Country	France		

Preferences

Sports	24%	Music & Video	18%
Travel	10%	Social Media	6%
Shopping	4%	Artists	4%
Technology	3%	Restaurants	2%
Health & Wellness	3%	Other	28%

Last connections

Hotel Bellora	Jun 25, 2019	08:28
ESS-Head-Office-Stockholm	Jun 19, 2019	04:52
Metro Rio Largo do Machado	Jun 6, 2019	11:45

Figure 9: Zooks Smart Data Guest User Profile

Available services include push notifications, location relevant advertisements, personalized promotions, satisfaction surveys, mobile concierge anywhere, captive portal engagement, location-based advertisements, and tailored personalized promotions. The result help hoteliers better understand guests' preferences, deliver better experiences, and boost revenue thru highly targeted marketing programs.

PHYSICAL DISTANCE MONITORING AND CONTACT TRACING

Hotel safety extends beyond physical and environmental hazards. Today, physical distance monitoring and contact tracing are essential for return-to-travel and stay-healthy-at-work initiatives. Whether mandated by local regulations or company policies, maintaining social distancing and infection control tracing are top of mind for hoteliers. While there is no single physical distance monitoring and contact tracing application that will work for all hospitality applications, real-time location services and identity stores have an essential role to play in virtually every infection control solution.

Aruba has teamed with multiple technology partners to deliver a broad range of return-to-work solutions. These solutions fall into four categories:

- Physical distancing enforced by wearable tags or wristbands for situations in which a personally-owned device is not suitable;
- Application-based physical distancing solutions that run on personally-owned or company issued devices;
- Presence detection systems that pick-up Wi-Fi signals from personally-owned or company issued devices, but do not require an application; and
- Thermographic and facial recognition systems that monitor the temperature of individuals' heads, and can process dozens of people simultaneously.

The AiRISTA Flow Social Distancing and Contact Tracing Solution uses a wireless tag worn by employees to help enforce guidelines for social distancing and automate contact tracing. The tags communicate with each other autonomously, without supervisory control, and trigger when they are closer than 2 meters apart. The user can be signaled with a vibration and/or sound and the devices forward the incident via Aruba access points to the AiRISTA Flow cloud-based software system.

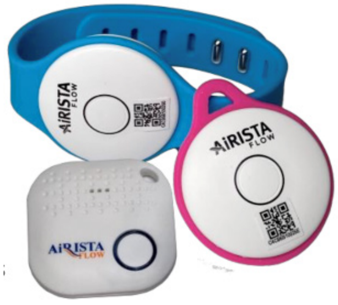


Figure 10: AiRISTA Flow BLE Proximity Tags

Aislelabs provides a real-time footfall and occupancy monitoring solution to promote social distancing in large sites without the need to download an app. The solution uses Wi-Fi enabled smart phones or tablets, together with existing Aruba Wi-Fi infrastructure, to anonymously log the movement of people and area occupancy in an auditable database. Violation alerting is triggered based on programmable thresholds.

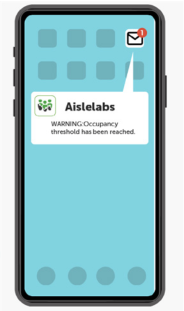


Figure 11: AisleLabs COVID-19 Social Distancing Solution

COHU | HD COSTAR

Aislelabs provides a real-time footfall and occupancy monitoring solution to promote social distancing in large sites without the need to download an app. The solution uses Wi-Fi enabled smart phones or tablets, together with existing Aruba Wi-Fi infrastructure, to anonymously log the movement of people and area occupancy in an auditable database. Violation alerting is triggered based on programmable thresholds.

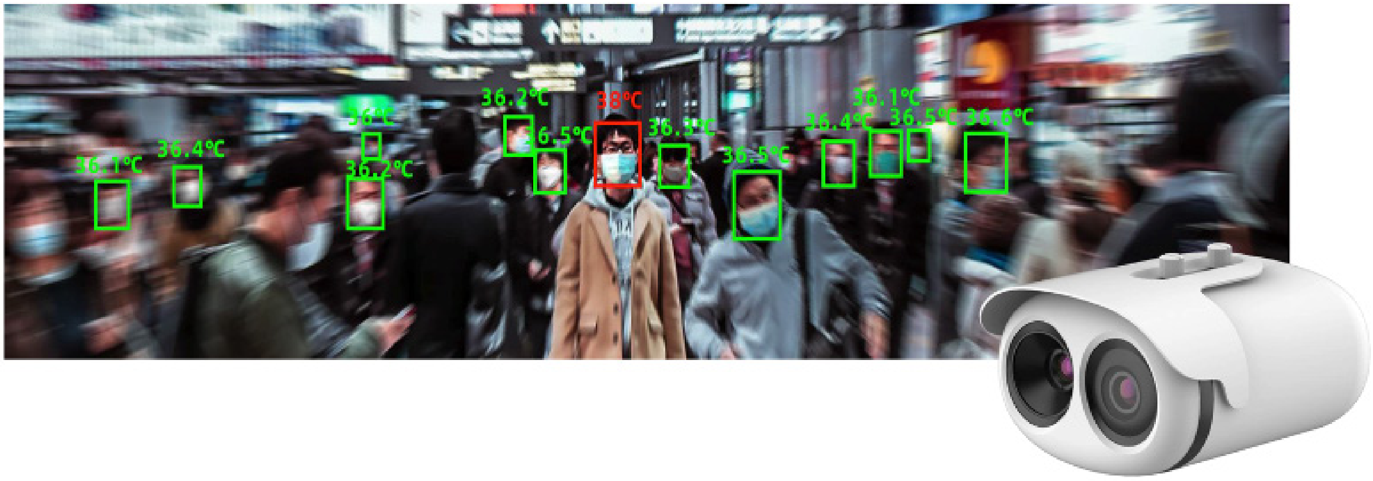


Figure 12: CohuHD Non-Contact Thermographic and Facial Recognition Camera

CX APP

The CXApp Touchless Application leverages Meridian BLE Beacons strategically placed around the workplace, and the Meridian cloud service for location data. The mobile app sends notifications based on crowded times, vacant times, and total employees per square foot, all based on real-time occupancy within the environment.

Kiana

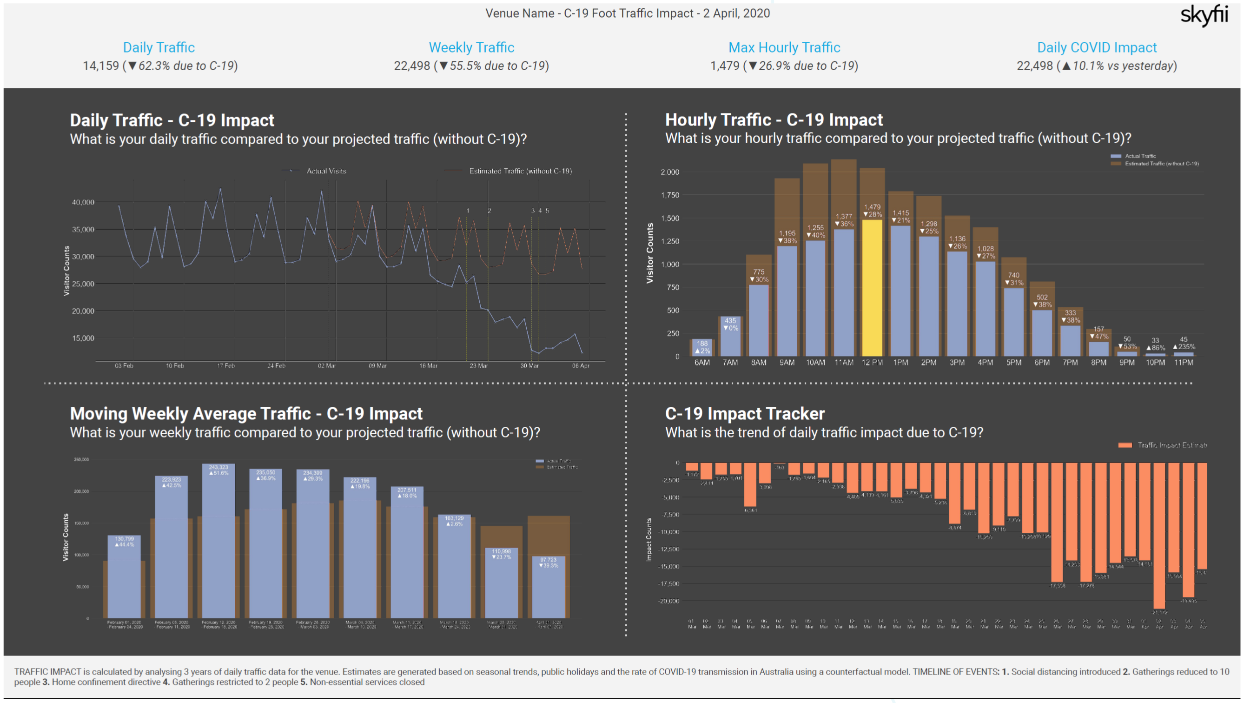
Kiana Analytics' Rapid Containment Application uses real-time location data, collected by existing Aruba access points from Wi-Fi enabled mobile phones and tablets, to identify the presence and movement of people. The application analyzes social transmission vectors, including locations and contact trees, to help mitigate spreading of communicable diseases.

Patrocinium™

The Patrocinium Safe Return Application leverages Meridian BLE Beacons, the Meridian cloud service for location data, and Patrocinium's ArcInsight analytics package. The application runs on personally-owned or corporate-issued smartphones and tablets, and automatically detects when other personnel are too close. The location and identity of the individuals are sent to the analytics application via Aruba Wi-Fi for contact tracing.

skyfii iO

OccupancyNow is an automated occupancy and social distancing management toolkit from Skyfii. The cloud-based solution uses real-time location data from existing Aruba infrastructure to maintain safe occupancy and social distancing guidelines, automatically alert staff when occupancy counts reach a set threshold, and facilitate contact tracing via Skyfii's analytics and communication tools. OccupancyNow also helps track whether routine cleaning and sanitization procedures are being performed.



Venue Name - C-19 Foot Traffic Impact - 2 April, 2020

skyfii

Daily Traffic	Weekly Traffic	Max Hourly Traffic	Daily COVID Impact
14,159 (▼*62.3% due to C-19*)	22,498 (▼*55.5% due to C-19*)	1,479 (▼*26.9% due to C-19*)	22,498 (▲*10.1% vs yesterday*)

Daily Traffic - C-19 Impact
What is your daily traffic compared to your projected traffic (without C-19)?

Hourly Traffic - C-19 Impact
What is your hourly traffic compared to your projected traffic (without C-19)?

Moving Weekly Average Traffic - C-19 Impact
What is your weekly traffic compared to your projected traffic (without C-19)?

Actual Traffic
Estimated Traffic
Visitor Counts
250,000
200,000
150,000
100,000
50,000
0
130,799 ▲44.4%
223,923 ▲42.5%
243,323 ▲51.6%
235,050 ▲36.9%
234,399 ▲29.3%
222,196 ▲19.8%
207,511 ▲18.0%
163,129 ▲2.6%
110,998 ▼23.7%
97,723 ▼39.3%
February 01, 2020 - February 04, 2020
February 05, 2020 - February 11, 2020
February 12, 2020 - February 18, 2020
February 19, 2020 - February 25, 2020
February 26, 2020 - March 03, 2020
March 04, 2020 - March 10, 2020
March 11, 2020 - March 17, 2020
March 18, 2020 - March 24, 2020
March 25, 2020 - March 31, 2020
April 01, 2020 - April 07, 2020

C-19 Impact Tracker
What is the trend of daily traffic impact due to C-19?

TRAFFIC IMPACT is calculated by analysing 3 years of daily traffic data for the venue. Estimates are generated based on seasonal trends, public holidays and the rate of COVID-19 transmission in Australia using a counterfactual model. TIMELINE OF EVENTS: **1.** Social distancing introduced **2.** Gatherings reduced to 10 people **3.** Home confinement directive **4.** Gatherings restricted to 2 people **5.** Non-essential services closed

Figure 13: Skyfii OccupancyNow Dashboard

MIGRATING FROM BREAK/FIX TO PROACTIVE MAINTENANCE

Up-time and defect-free processes are prime objectives of operations groups, whose charge is to keep heating, ventilation, air conditioning, refrigeration, water treatment, and power systems running non-stop. Addressing maintenance proactively to minimize downtime, and maximize the utilization and performance of assets, can reduce maintenance costs by up to 40%.

Proactive maintenance is an essential tool in this quest. By instrumenting equipment, monitoring for degradation, and identifying potential problems in advance of failure, proactive maintenance can provide visibility into the performance of assets, ensure high availability, and maximize the returns on often substantial capital investments.

The challenge is that identifying the source of possible failures is not always a simple task. Sensor networks and gateways have traditionally been expensive to deploy and can have vulnerable attack surfaces that keep CISOs awake at night. COOs, in turn, fret whether innovative AI proactive maintenance solutions require resources beyond the means of facilities teams.

Spending on proactive maintenance is expected to hit $12.9 billion in the next two years. Juggling the high cost asset performance management solutions, and its security risks, against the benefits of lower downtime and fewer disruptions is a challenging calculus.

An optimal solution is to leverage secure, robust IT infrastructure that is already deployed in a facility to capture machine status from IoT sensors. A dual-use IT/IoT network is more economical to deploy and can eliminate gateways and the security threat they pose.

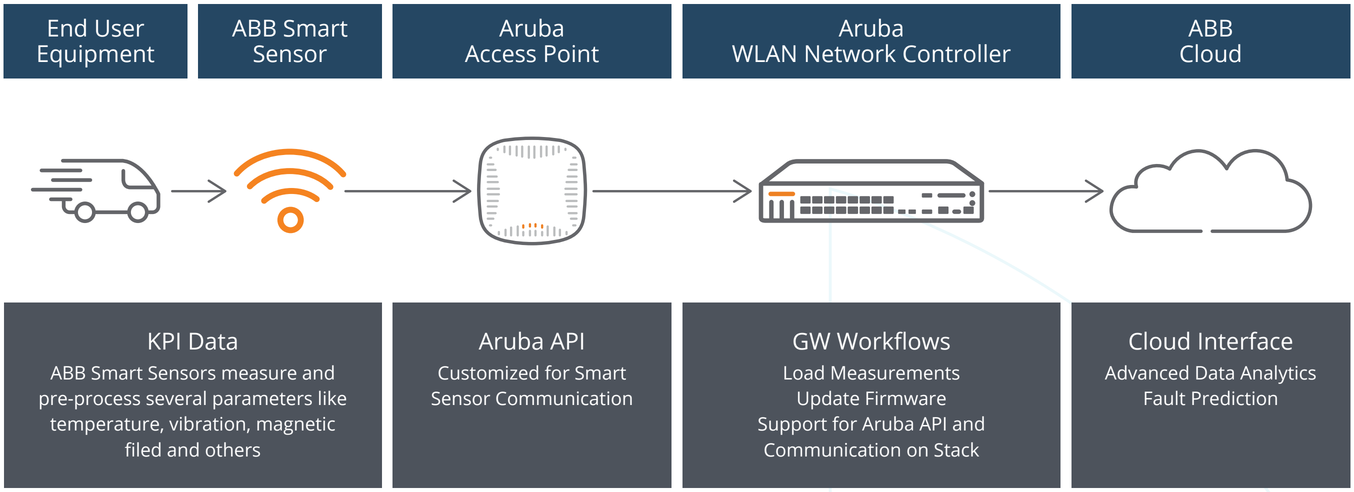
ABB

ABB is a technology leader in industrial digital transformation of electrification, automation, motion, and robotics. Through its ABB Ability™ digital platform, ABB drives improvements in productivity, reliability, and efficiency.

The ABB Ability Smart Sensor is a battery-powered, multi-sensor device that monitors rotating machinery like motor drives, chillers and pumps for abnormal behavior indicative of pending failure. Status is communicated over a secure Bluetooth link, and analyzed by ABB's advanced algorithms. Facilities engineers are automatically notified of out-of-normal conditions well before failure, allowing repairs to be performed before processes are impacted.

The Smart Sensor helps customers move from break/fix to proactive maintenance, a digital transformation that reduces downtime, enhances asset utilization, and optimizes scheduling of field engineers. All of which ultimately boost efficiency and profitability.

ABB and Aruba have partnered to enable Aruba Wi-Fi 5 and Wi-Fi 6 multi-radio access points to securely collect and forward ABB Ability™ Smart Sensor data to the ABB Ability™ Condition Monitoring application. Using Aruba zero trust infrastructure as a data collection platform provides uniform security and visibility across both IT and IoT domains. It eliminates the costs and security risks and costs associated with large fleets of gateways. Since gateways filter raw data streams that can be rich in visibility data, removing them has the added benefit of improving visibility all the way down to individual sensors.



End User Equipment

ABB Smart Sensor

Aruba Access Point

Aruba WLAN Network Controller

ABB Cloud

KPI Data
ABB Smart Sensors measure and pre-process several parameters like temperature, vibration, magnetic filed and others

Aruba API
Customized for Smart Sensor Communication

GW Workflows
Load Measurements
Update Firmware
Support for Aruba API and Communication on Stack

Cloud Interface
Advanced Data Analytics
Fault Prediction

Figure 14: Aruba and ABB Integration Overview

The Aruba-ABB solution works with brownfield and greenfield deployments of any Aruba Wi-Fi 5 and Wi-Fi 6 access points equipped with a BLE radio and AOS 8.6 or later. This means that proactive maintenance monitoring can be retrofitted to existing Aruba WLAN deployments without adding additional IT gear or gateways.

The joint ABB-Aruba solution delivers the operational visibility and robustness demanded by facilities and operations teams, without the expense of a dedicated wired sensor system. Wireless communication allows Ability Smart Sensor to be deployed anywhere without expensive conduit or enclosures. These savings extend throughout the life cycle of a deployment since adds, moves, and changes are easy and inexpensive.

The intersection between facilities and IT has historically been a point of friction, but not so with the ABB-Aruba joint solution. Both companies are respected leaders in IoT and IT, respectively, and the joint integration allows data to flow reliably and securely between systems. Visibility and robust design address the uptime concerns of COOs, while I/O-to-application security and policy management check the box for CISOs. And the cost savings will cheer CFOs.

BUILDING CONTROL AND DIGITAL TWIN ENABLEMENT

Situational awareness is essential to creating a hyper-aware hospitality facilities. IoT devices are a facility's eyes and ears, and are given voice by the secure connectivity infrastructure through which they talk with smart building applications. The better instrumented the building, the more informed the insights that can be made across time and space, including projections of future occupant and system behavior.
Energy monitoring cuts across many hotel sub-systems, encompassing a wide variety of IoT telemetry including power quality, power consumption, leak detection, air and fluid flow, enthalpy, refrigeration, lighting, temperature, and humidity.

Digital twin modeling combines IoT monitoring data with artificial intelligence, historical data, domain knowledge expertise, and graph modeling to establish and analyze relationships between and among building devices and systems. By creating real-time simulation models in the digital world that change and learn in lock-step with the building, digital twins can identify sub-optimized processes, recommend operational enhancements, assess complex systems that would be too difficult for a human to track, and monitor the trajectory of energy usage needed for proactive interventions.

The benefits of building monitoring and digital twin modeling hinge on the availability of timely access to relevant IoT data. Securely and economically interfacing IoT monitoring devices across a building can be challenging. The breadth of telemetry to be gathered, interfacing with legacy IoT devices that use non-interoperable protocols, securing the data path, and importantly the cost of deployment – initially and during adds/moves/changes – can be daunting and expensive.

Wired monitoring systems require dedicated cabling, which is expensive to deploy and labor intensive to maintain. Wireless IoT devices are more economical to deploy but the cost of battery maintenance can be prohibitive.

As hotels deploy next-generation Wi-Fi 6 wireless networks for human activity monitoring, that same secure IT infrastructure can be leveraged for guest room, public space, and operations monitoring and digital twin applications. Advanced access points that have built-in IoT radios, and support for external USB adapters, can serve as IoT data gathering platforms.

The remaining hurdle is to eliminate batteries wherever possible. Energy harvesting technology derives, captures, and stores power from external sources, e.g., kinetic, temperature, and visible light. Miniaturized energy harvesting power sources embedded inside IoT sensors solve this problem, allowing building sensors to be placed wherever needed with no wires or maintenance.

EnOcean, a venture-funded spin-off of Siemens AG, is the creator of the ISO/IEC 14543-3-10/11 energy harvesting 800/900MHz wireless standard. More than 400 EnOcean Alliance vendors build facility monitoring and control systems using this standard. Sensors require no batteries for power, and no wires to communicate, making them economical to deploy and maintenance-free. RS-232, RS-485, ModBus, LONWORKS, BACnet, KNX, and DALI control systems and devices are supported via locally powered, EnOcean-enabled gateways. These gateways extend the reach of monitoring and digital twin applications into legacy infrastructure, yielding deeper visibility and insights without incurring the cost of ripping-and-replacing installed devices.

EnOcean and Aruba have partnered to allow Aruba Wi-Fi 5 and Wi-Fi 6 access points equipped with EnOcean 800/900MHz USB adapters, and using Aruba OS version 8.7 or later, to communicate bi-directionally with ISO/IEC 14543-3-10/11 compatible devices. With literally thousands of such devices and gateways from which to choose, virtually any smart building monitoring application can be accommodated. The joint solution can be retrofitted to existing Aruba deployments, extending the value of sunk capital investments.

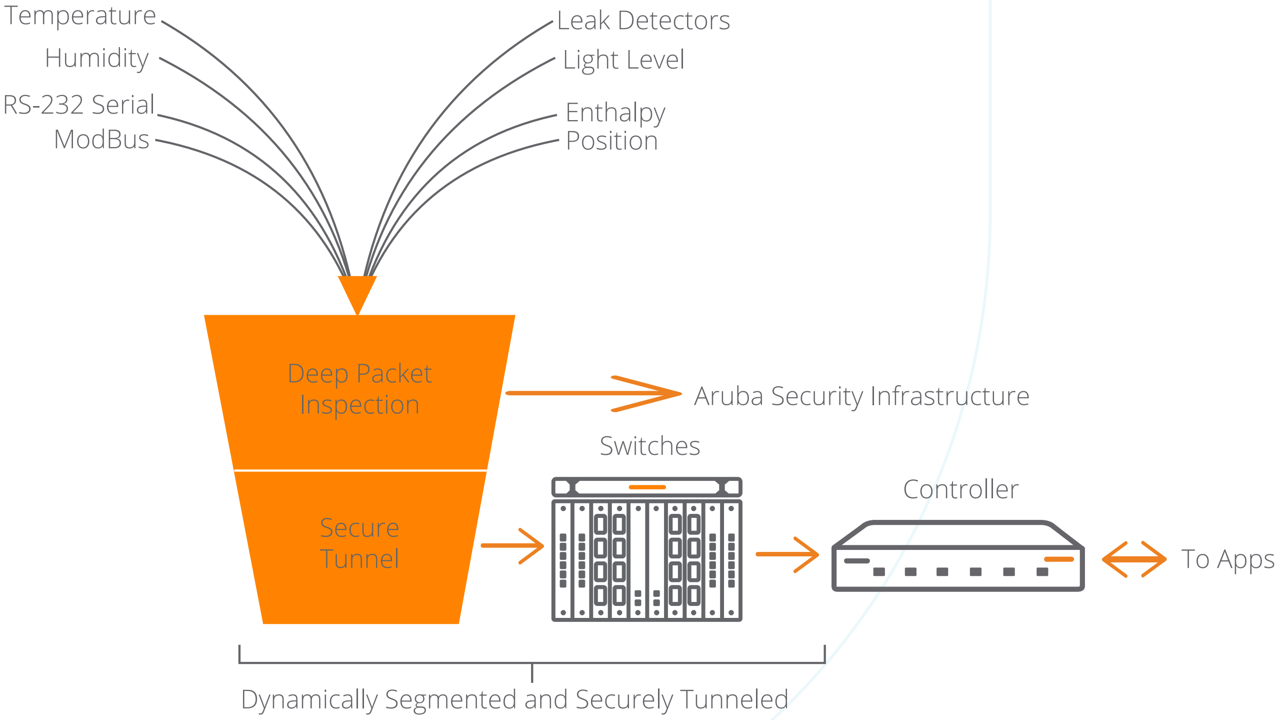


Figure 15: Aruba Access Points Are IoT Platforms For EnOcean Device Data

Aruba access points stream EnOcean telemetry data in real time via protobuf to monitoring applications over a secure Web socket connection. Applications can be on-premise, or in a public or private cloud.

The EnOcean Alliance includes software application vendors as well as device vendors, and ensures interoperability between both.

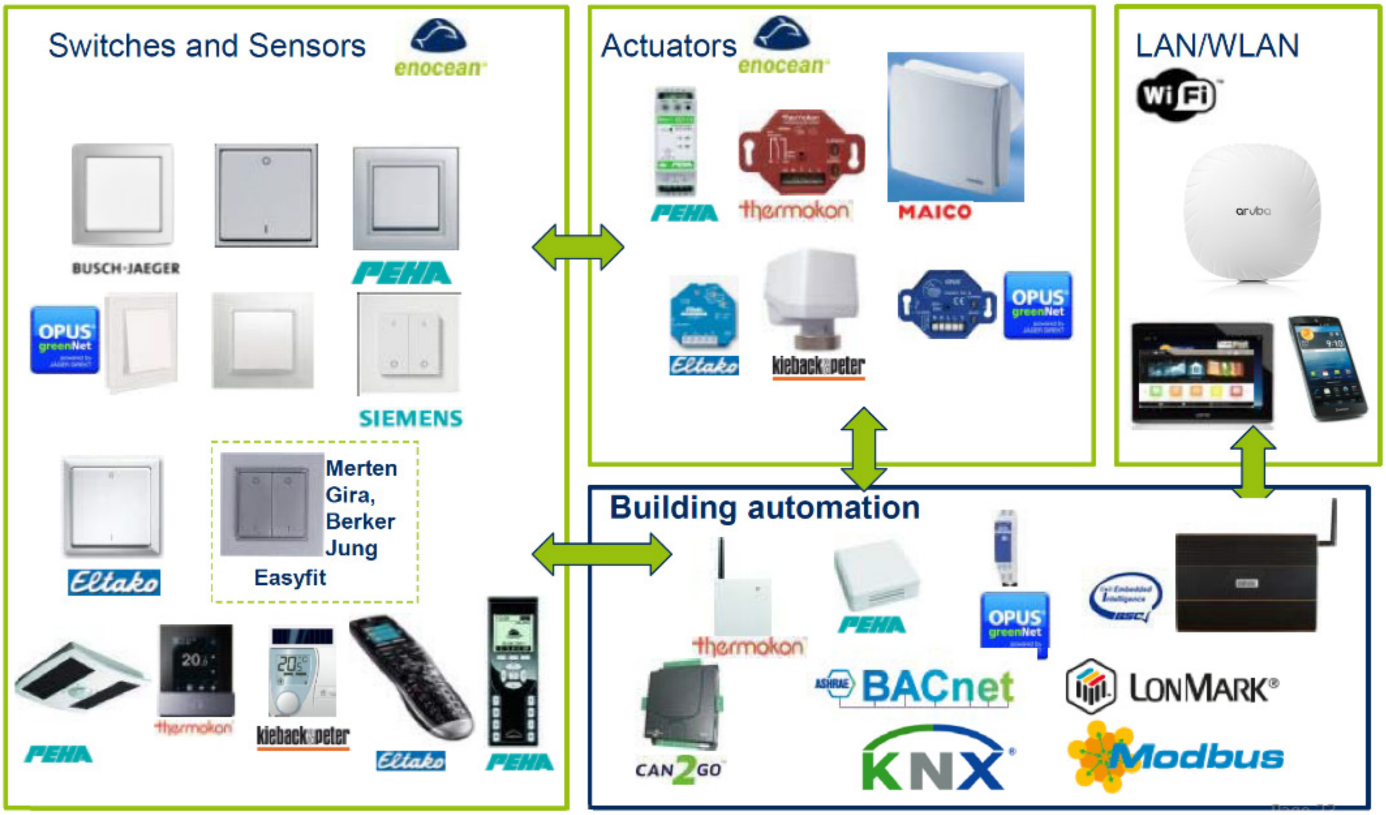


Figure 16: EnOcean Ecosystem Encompasses Room Lighting, HVAC, Energy, Intrusion, and Blind Controls

The wide range of available ISO/IEC 14543-3-10/11 compatible devices, combined with the security and extensibility of Aruba infrastructure, delivers an extraordinarily flexible and economical way to monitor room and facility devices.

Azure IoT Hub

Customers that want digital twin modeling and telemetry monitoring can point Aruba's Web socket connection to Microsoft's Azure IoT Hub – on-premise or in the Azure cloud. Azure IoT Hub will extract the telemetry data from the protobuf stream, making them available to the Azure Digital Twins IoT service.

The Azure Digital Twins service creates spatial intelligence graphs to model relationships and interactions. Thru the service users can build reusable, highly scalable, spatially-aware digital models based on their physical plants, and use them to identify optimize processes and remedy issues.

AUTOMATING NETWORK ACCESS TO ENHANCE THE EFFICIENCY OF EMPLOYEES, SERVICE PERSONNEL AND CONTRACTORS

Enhancing human productivity necessitates the availability of devices, and the creation of environments in which they operate, that are cognizant of, and automatically adaptive to, the needs of employees, service personnel, and contractors. On-boarding users onto networks has historically been challenging because of compliance requirements for secure networks on the one hand, and vulnerabilities inherent in open networks on the other. If access is too complex or unreliable then users are forced to use cellular networks that bypass IT security systems and may not function reliably without expensive distributed antenna systems. The trick is to simplify network access so it doesn't create an administrative burden, and implement security policies that protect employees, service personnel, contractors, and the property owner.

Aruba and its technology partners have a proven solution by which temporary users can be automatically badged and enrolled on the local Wi-Fi network, guided to equipment and rooms using wayfinding, and enabled to use personally-owned devices. For conferencing facilities the solution can provide visitors with secure temporary access to projection screens, entertainment systems, room controls, and other network resources in designated areas.

Key components include Aruba Wi-Fi 6 Access Points, ClearPass Guest Access, ClearPass Policy Manager, Envoy's visitor management solution, WPA3 Enhanced Open, and an Access Code captive portal. Performance of the offered services are monitored using the Aruba User Experience Insight (UXI) solution to ensure that service level agreements are satisfied and application performance meets guidelines. A comprehensive validate reference design guide for guest access is available on request.

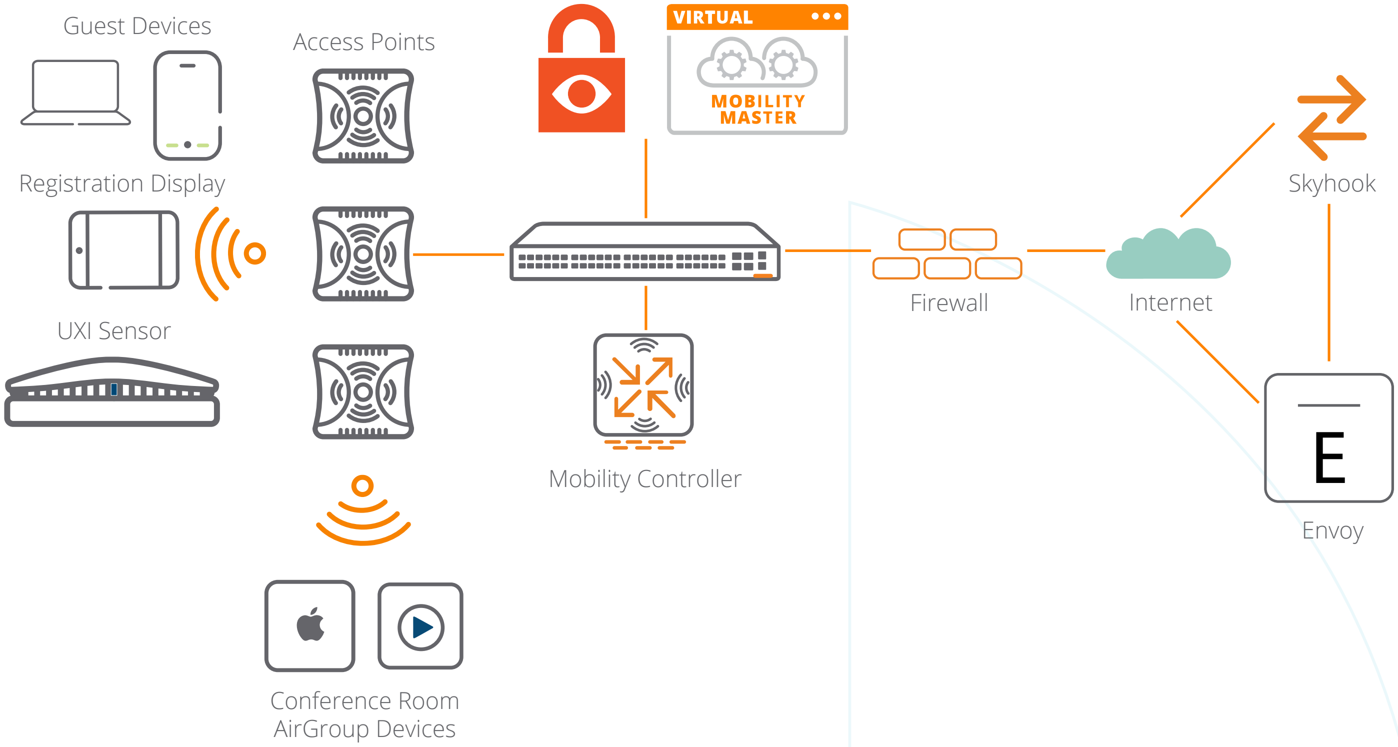


Figure 17: Automated Guest Access Solution To Enhance Staff Efficiency

Aruba 500 Series Wi-Fi 6 Access Points are recommended because of their Wi-Fi performance and integrated IoT radios for smart building sensing and control. ArubaOS 8.4 or newer code running on a Mobility Master/Mobility Controller, Aruba Instant, and/or Central are supported. A comprehensive validated reference design is available for controller-based deployments.

ClearPass 6.7.2 or later is required. ClearPass runs on hardware appliances with pre-installed software or as a Virtual Machine under VMware (ESXi 5.5, 6.0, 6.5 or higher), Microsoft Hyper-V Server (2012 R2 or 2016 R2), Hyper-V on Microsoft Windows Server (2012 R2 or 2016 R2), and KVM (CentOS 7.5).

Envoy

Envoy Visitors is a visitor management platform for a modern approach that helps streamline visiting contractor or service personnel sign-in. When temporary employees, service personnel and contractors arrive, Envoy makes it easy for them to register, presents relevant non-disclosure and health/safety forms for completion, and notifies your operation of the worker's arrival via e-mail or SMS.

Simultaneously, ClearPass dynamically provisions temporary Wi-Fi access credentials for their devices and sends an individualized security code for Wi-Fi access via e-mail or SMS.

Envoy leverages ClearPass' microservice extensions running in a container independent of the ClearPass operating system. ClearPass extensions are used to interact with external systems, including advanced two-factor authentication services and IoT firewalls.

The joint Aruba/Envoy solution automates the entire onboarding process, minimizing the need for manual assistance, and ensuring that security standards are enforced throughout the visit. Never again will hired personnel need to circumvent IT security just to obtain reliable connectivity.

SECURELY SHARING FACILITY WIRELESS NETWORKS WITHOUT LOSING CONTROL

Network access to a facility building wireless is typically tightly controlled out of concern that critical services and devices, such as Wi-Fi calling, could be negatively impacted by wireless users. However, growing demands for mobile device wireless access to enhance worker efficiency, productivity and safety increase pressure to open up wireless networks and avoid the cost and RF interference of parallel networks. Both IT and facilities groups are struggling to find a mutually acceptable solution.

Several years ago the US Department of Defense (DOD) encountered a very similar situation. There was pressure to use one common network to support secret (SIPR) and non-secret (NIPR) traffic. These distinct traffic flows were managed by different groups, each of which needed total control over access to the traffic they managed. Security was paramount, and there could be no sharing of data across groups or unauthorized network access within a group.

Aruba solved the issue by developing MultiZone, a networking solution that allows each of up to five groups to define authentication, access, operation, and management rules applicable to, and enforced within, their unique "Zone." One Aruba controller is assigned to the Primary Zone, managed by IT, which handles access points and RF settings, and directs access points to authenticate to Data Zone controllers. Separate Data Zone controllers handle authentication, access, operation, and management rules for the SIPR and NIPR groups. MultiZone supports up to five Data Zones.

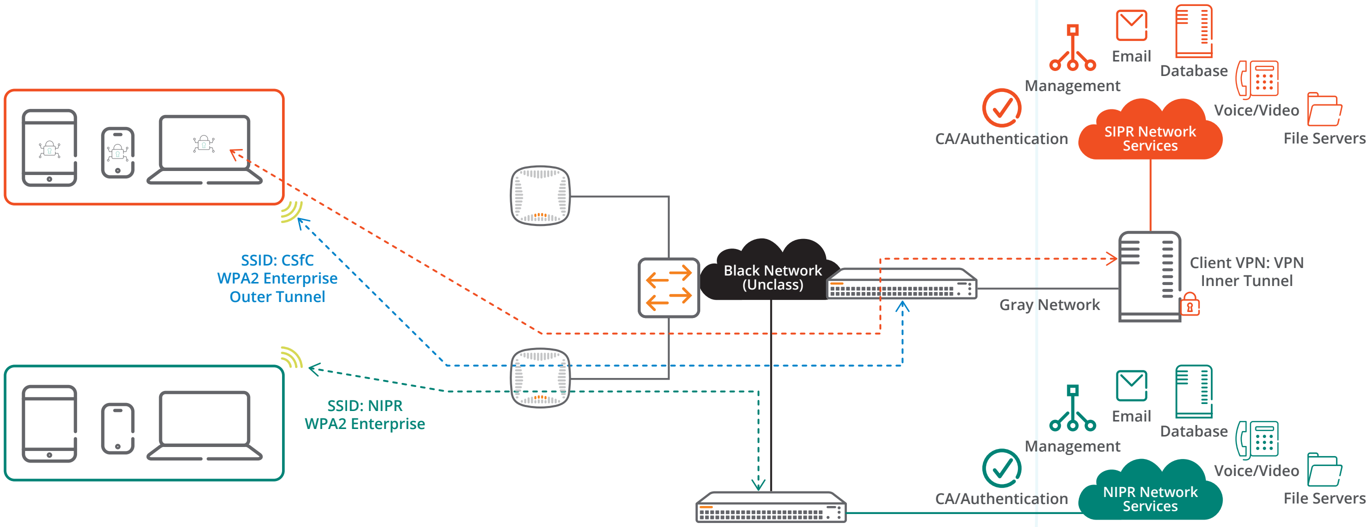


Figure 18: Aruba MultiZone Solution

The multi-tenancy design of MultiZone is ideal for hospitality applications. Separate Data Zones can be allocated to the groups managing conference centers, conventions, building controls, and contractors. Each group separately controls who and what is allowed access into their Data Zone, including Internet and VPN connectivity to remote services.

In a MultiZone system IT manages the overall infrastructure through the Primary Zone but cannot access Data Zone traffic. Uniform visibility and security can be achieved while simultaneously respecting the access control rights of Data Zone owners.

SEAMLESS 5G TO WI-FI ROAMING WITHOUT DISTRIBUTED ANTENNA SYSTEMS

If you can't connect with people and machines inside a building, then you can't extract or share information. The prevalence in hospitality facilities of low-emission glass, energy-efficient construction materials, and evolving building codes have made indoor wireless coverage from outdoor cellular networks a recurring challenge. This results in inconsistent experiences for mobile users and devices as they roam in and out of buildings. These problems are compounded with high-speed 5G, which operates at higher frequencies that do not penetrate indoors as far as 3G or 4G cellular.

For decades, indoor cellular issues have been addressed by deploying distributed antenna systems (DAS). This expensive infrastructure operates as extended antennas for one or more cellular carriers. More recently, indoor small cell (also called "femtocell") networks have been deployed by individual mobile network operators (MNOs). Unlike DAS, a separate layer of equipment is required for each MNO. Both DAS and small cells are complex, very costly, and rarely cost effective for facilities with less than 200,000 ft2 (20,000 m2) - the bulk of commercial properties worldwide.

Over 150 MNOs in nearly 50 countries have embraced Wi-Fi Calling. This service leverages the existing Wi-Fi network, which when properly designed provides pervasive coverage throughout a building. 5G includes support for Wi-Fi 6 integration as a radio access network (RAN), so building owners do not need to choose between 5G and Wi-Fi 6: Wi-Fi Calling and other services can be performed over both. For this reason, wireless LANs are the premier and most economical onramps for indoor cellular devices.

Aruba Air Pass is the industry's first seamless cellular roaming solution designed to unify enterprise and mobile network experiences. The service enables smart building 5G initiatives - including guest, employee, service personnel, contractor, and IoT device on-boarding and roaming - to be accomplished with enterprise-class security over Wi-Fi 6 without the high cost of a DAS, or issues with inconsistent cellular connectivity.

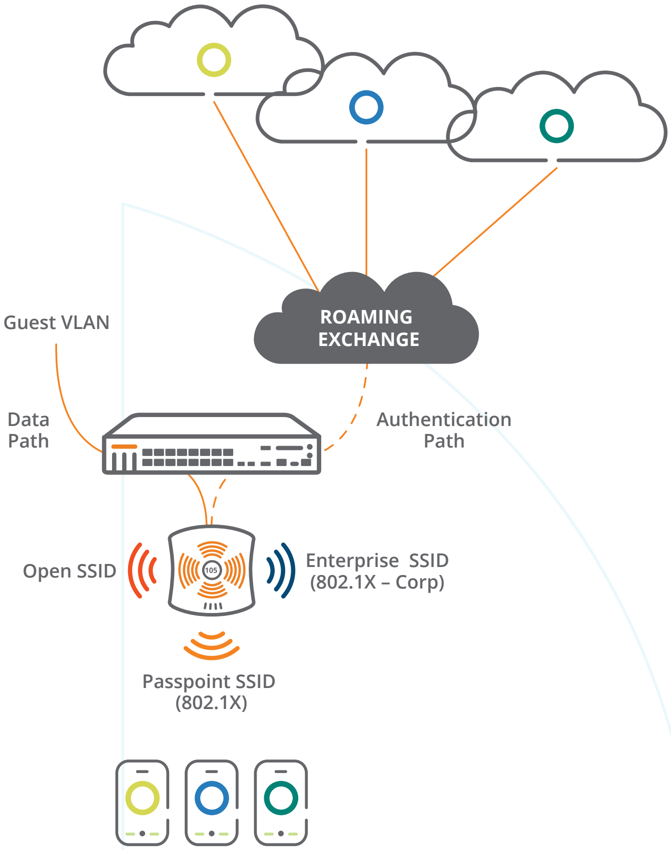


Figure 19: Aruba Air Pass System Architecture

Air Pass uses pre-negotiated agreements with MNOs that support the Wi-Fi CERTIFIED Passpoint standard to automatically gain network access using cellular SIM credentials for authentication. No captive portals, user names, or passwords are required. Aruba ClearPass provides high security network access control so that public and private resources remain secure and separate. Mobile subscribers, and Passpoint-capable IoT devices, can then roam between the cellular and Wi-Fi networks in compliance with IT security standards.

Air Pass is managed by Aruba Central, a massively-scalable cloud-based network operations, assurance, and security platform. Aruba Central simplifies the deployment, management, and orchestration of wireless, wired, and SD-WAN environments. This includes delivering 5G and Wi-Fi 6 to the network and customer edge, complete with built-in and third-party services.

Mobile users and IoT devices are increasingly accessing cloud services and other bandwidth-intensive applications like augmented and virtual reality. Air Pass leverages Air Slice for SLA-grade application assurance by dynamically allocating radio resources such as time, frequency, and spatial streams to specified users, devices, and applications.

Reliably connecting people and IoT devices inside a building is essential for great guest experiences, context-aware engagement, safety, and security. Air Pass marks an end to a dependence on expensive DAS systems. It also overcomes connectivity, security, and convenience issues associated with indoor cellular coverage gaps, insecure open wireless networks, manually hunting for Wi-Fi networks, and challenges navigating captive portals. Secure connectivity is assured regardless of where people and IoT devices work or roam.

REDUNDANT INTRA-SITE WIRELESS VIDEO AND DATA LINKS

Video surveillance and remote gate control systems at larger hotels and resorts often require outdoor data links. The choice between wired or wireless data links typically comes down to cost. If a wired network requires reaching across a parking lot or gully to surveillance cameras or an out building, it can easily take days of work to trench and repair asphalt or concrete. If there is hazardous buried material in the path, pipelines to cross, or the right of way is unavailable, the challenges continue to mount.

Wireless data links are easier to deploy than buried cables, however, the cost of a point-to-point high-speed microwave link can make it prohibitive for short-haul links under 400 meters. Less expensive links represent a single point of failure because they typically don't offer redundancy and can be impacted by nearby cellular networks. Additionally, in areas subject to high winds, even the slightest movement of the mounting brackets can throw a microwave antenna out of alignment and require a service call.

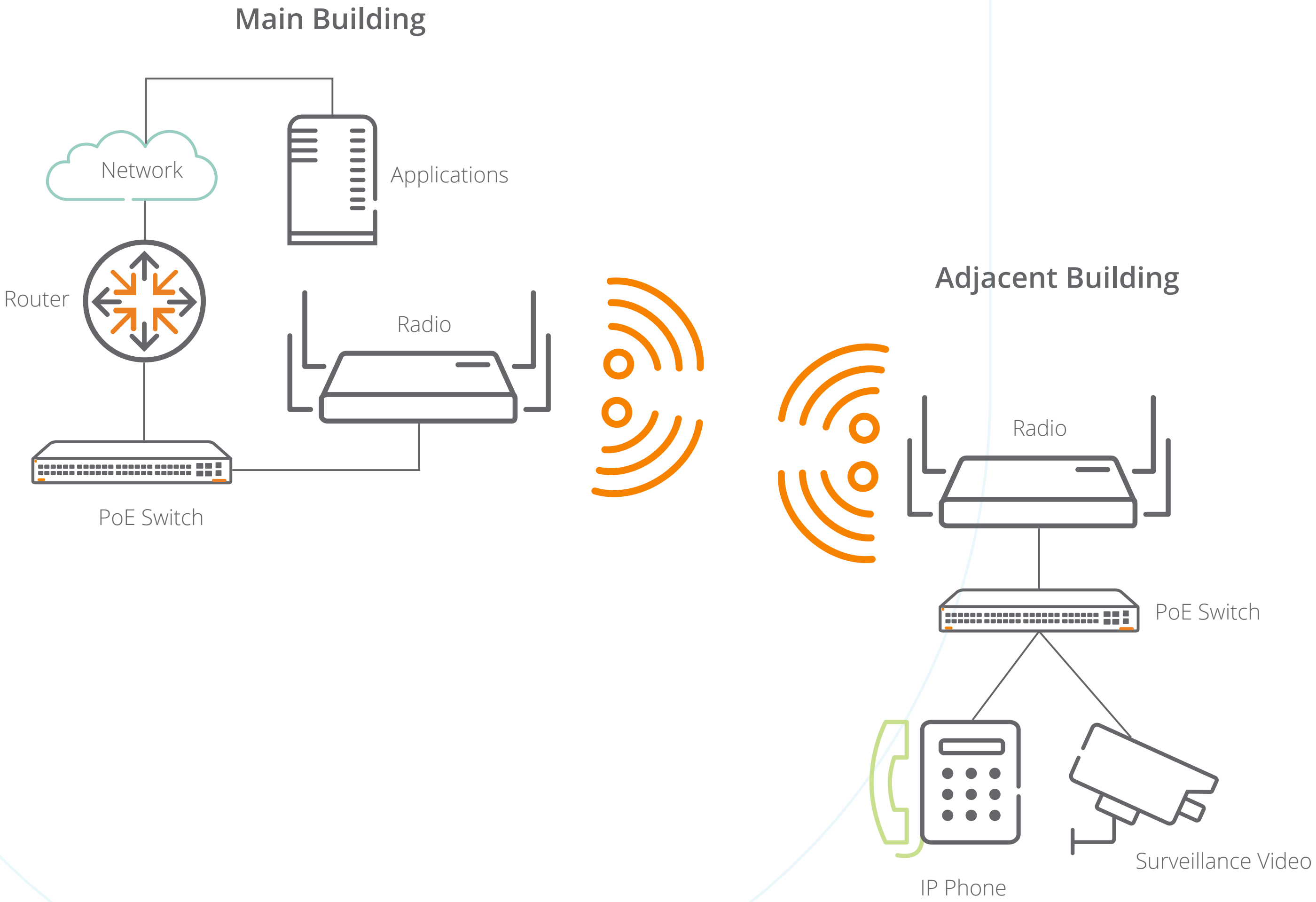


Figure 20: Point-To-Point Extension Of A Building Video Network To An Adjacent Building

Aruba's AP-387 is a high-speed, dual-radio, point-to-point link that addresses the shortcomings of today's point-to-point links. Incorporating a 60GHz millimeter wave radio with electrically steerable antenna array, the AP-387 provides automatic fallback to a 5GHz radio in the event that rain or snow attenuate the 60GHz signal. Redundant radios ensure that the link is always optimized, offering an aggregate peak rate of 3.37Gbps and a fallback rate of 867Mbps. Advanced cellular coexistence minimizes interference from cellular networks, distributed antenna systems, and commercial small cells, and femtocell equipment.

The auto-adjusting 60GHz antennas can dramatically reduce labor costs throughout the life of the site. The radios will intelligently link with alignment ±45 degrees azimuth, and ±17 degrees elevation; the 5GHz radio fixed sector antennas cover the same alignment zone. This eliminates the need for precision alignment, or high-cost skilled labor, during installation. Just point one radio in the general direction of the other, even if they are separated by as much as 20 stories of elevation, and the radios will link up.

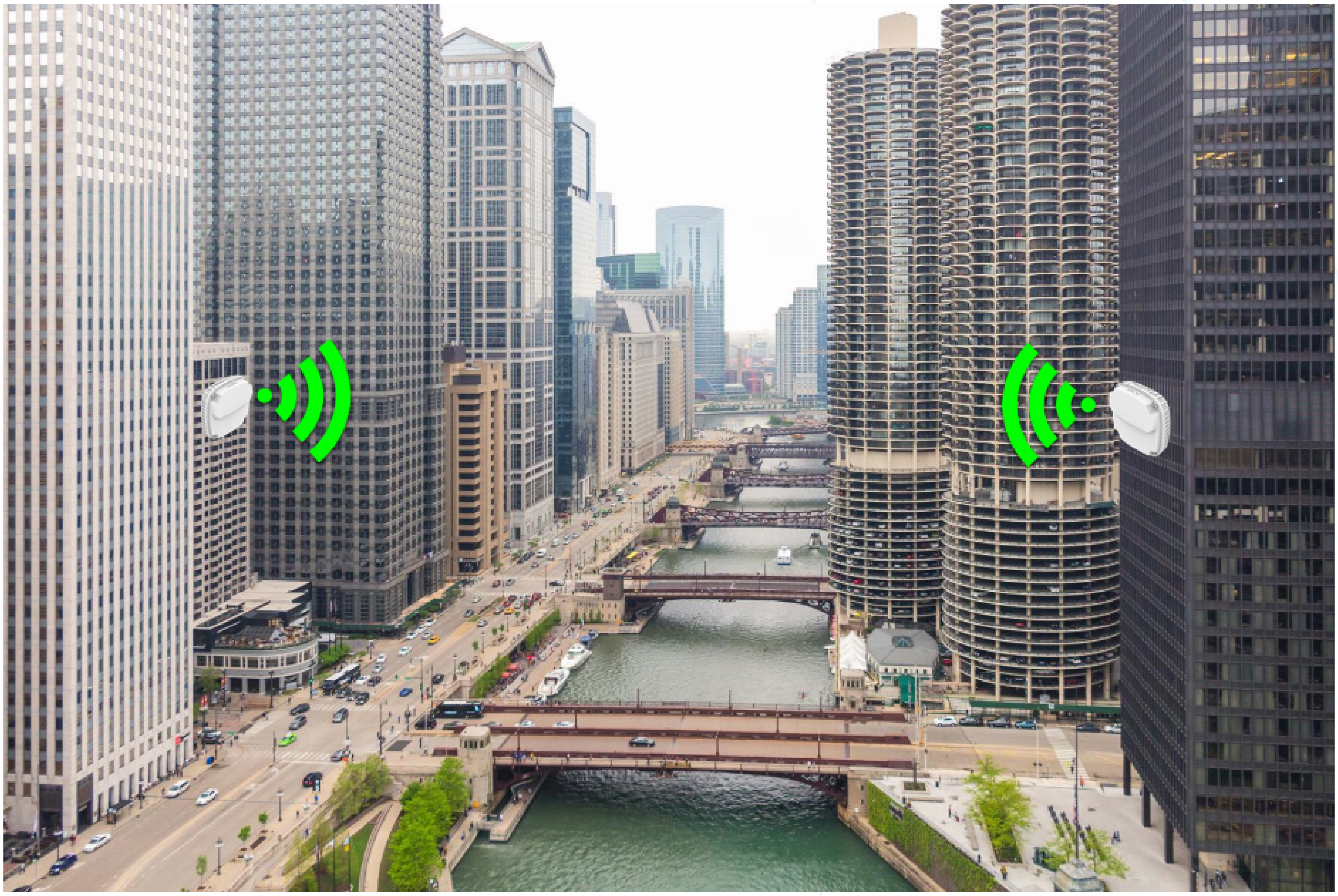


Figure 21: Aruba AP-387 High-Speed Outdoor Point-To-Point Link

Weighing just 1.2kg each, the radios can be commissioned by a single installer. The AP-387 includes an integrated BLE radio for hands-free set-up.

Extending data links to other buildings and on-site locations shouldn't compromise reliability or your budget. The AP-387 can provide a redundant, point-to-point link up to 400 meters, and with an aggregate peak rate of 3.37Gbps it can support a very broad range of IoT, telephony, streaming video, and physical security applications.

REDUCING MEAN TIME TO REPAIR WITH REAL-TIME LOCATION SERVICES

Many of the building subsystems spread throughout a hotel or resort have siloed repositories of IoT device data. Even though these data are rich with insights if properly mined, the justification for isolation is that these data are needed for facilities-owned processes which, if exposed, could be attacked or impacted by IT actions such as system updates, reboots, or maintenance.

The downside of isolating data is that it deprives applications of valuable insights that could make a facility more cognizant if mined in conjunction with other data sets, i.e., location data and proactive maintenance. Sharing contextual data – location, users, devices, and applications that originate from IoT devices and the personnel who use and manage them – can significantly enhance cognitive insights. With proper data life cycle governance these sources can be safely and securely shared, and reveal trends in guest behavior, conference room and real estate utilization, staff time and motion optimization, excessive energy consumption relative to peer facilities, and so on.

Application	Role of Location-Based Services
Human productivity optimization	Guide occupants to meetings and places of interest Improve time and motion paths Validate contractor activity
Proactive maintenance	Wayfinding to guide service personnel
Inventory optimization	Quickly find displays and high value equipment
Health and safety	Guide occupants to muster points Social distance monitoring

Figure 22: Location-Based Services By Application

From among the many types of available contextual data, location data are particularly insightful. Location data can guide us unescorted through facilities, improving our experience without encumbering others to assist us. They can help us keep track of people wherever they work or roam. And they can track capital assets so they can be quickly located and repaired.

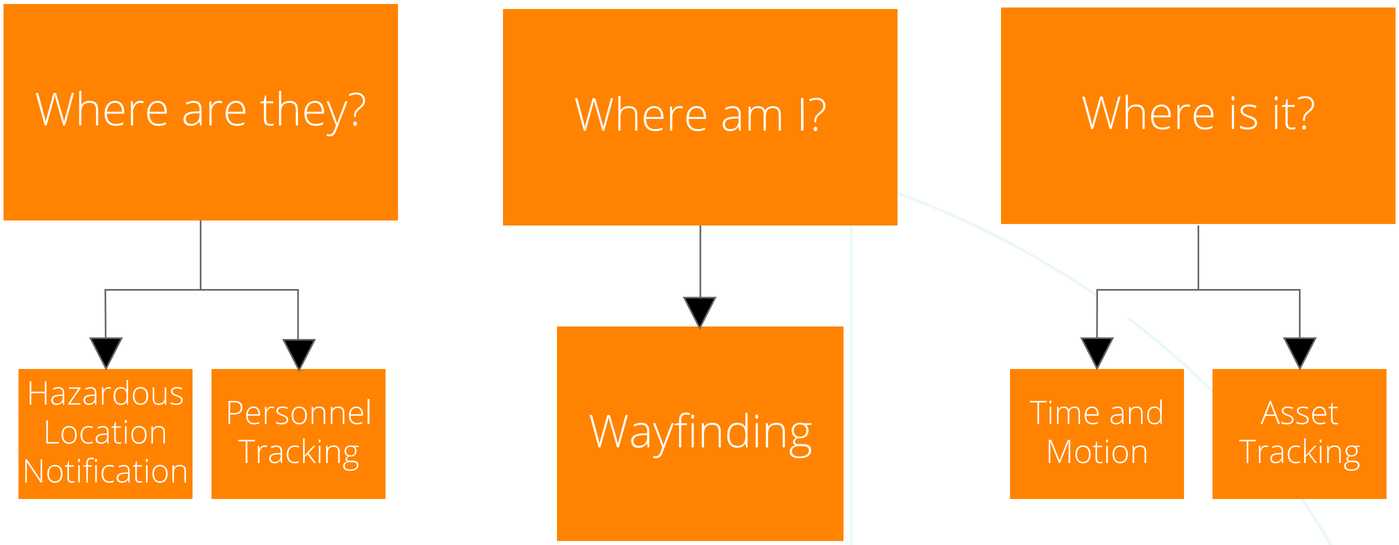


Figure 23: Aruba Location Services And Target Applications

High rise hotels and large and resorts can be difficult to navigate. If someone is delayed or lost traversing the facility the consequences can range in severity from poor guest experiences to loss of life. Engineers, contractors, and public safety officers can all benefit when a self-navigation solution – "wayfinding" – delivers them to their destinations quickly and unassisted.

Additionally, the contextual data generated along the way can be mined for business-relevant information. Examples include notification of construction zones that require safety gear, flagging occupied areas in the event of a security incident, and tracking contractor time spent on site relative to what was billed.

Aruba's Meridian platform is a mobile application platform that provides self-guided wayfinding, geofencing, and push messaging services for a broad range of IoT applications. The system consists of the following components:

- Location Beacons - standalone or integrated into Aruba access points;
- Meridian Application (App) for tablets and phones; and
- Meridian cloud service.

Beacons use Bluetooth Low Energy (BLE) to broadcast an anchor location that is picked up by the Meridian App and shared with the cloud service to assist with locationing. Beacons are built into Aruba Wi-Fi 5 and Wi-Fi 6 access points, including Class 1 Division 2/ATEX Zone 2 models qualified for HazLoc environments like fuel storage and vehicular refilling stations. Standalone battery- and USB-powered beacons are also available.

Figure 24: AP-530 Wi-Fi 6 Access Point With 802.11ax, BLE, And 802.15.4 Radios

Figure 25: AP-375EX Access Point For Hazardous Areas Like Propane Storage And Fuel Refilling

Typical wayfinding applications include:

- Guests to meeting rooms, points of interest, and muster stations;
- Navigating service personnel to machines in need to repair; and
- Providing visitors with self-service navigation around large facilities.

Self-guided wayfinding directs users to a point of interest, and offers a simple way to pinpoint their current location, search for points of interest, and access turn-by-turn directions, inside or outside. A glowing dot shows the user's location on a map, and tracks their progress along the route. Users can retrieve turn-by-turn directions from their current location without entering a starting point, an important time saver in emergencies that require mustering to safe areas.

Wayfinding also enables contractors to navigate sites without assistance, conserving operational and administrative resources from acting as guides. Upon nearing a target destination, a logical geofence can be triggered and push a contextually-relevant message or notify a relevant application, i.e., retrieve machine service records. The power of Meridian comes from the context it applies to user engagement, the precision of its geofencing, and the flexibility with which it can interact with other systems.

Reducing mean time to repair (MTTR) is a prime example of the value Meridian brings to smart building facilities applications. Imagine that the bearing on a motor drive starts to wear unevenly, and is picked up by multi-axis accelerometer in an ABB Ability Smart Sensor. The sensor relays an alert via an Aruba access point to the ABB Ability monitoring application, which dispatches an engineer preemptively before the bearing fails.

Instead of leaving it to the engineer to navigate the building on his or her own, however, the Meridian App triggers a geofence when the engineer enters the building – notifying the Finance Department when work commences - and then guides the engineer using turn-by-turn navigation to the failing motor drive.

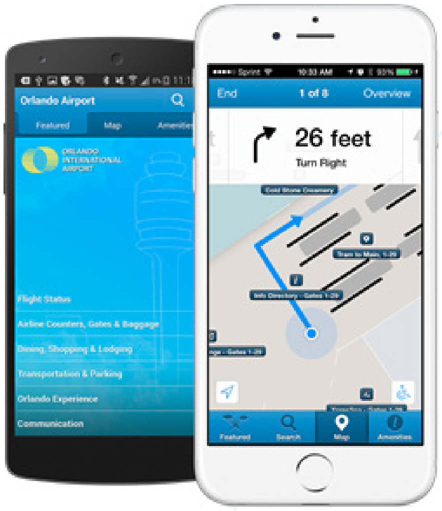


Figure 26: Meridian Turn-By-Turn Wayfinding

As the engineer approaches the machine another geofence is triggered, recalling the service record for that drive and again notifying Finance that repair work has commenced. Once the repair has been effected the engineer is guided to back to his/her truck and a third geofence notifies Finance that the work has been completed.

In large sites, wayfinding can reduce the mean time to repair by tens of minutes per incident, making engineers more efficient and reducing the risk of equipment failing while awaiting the arrival of service personnel. Equally important, the same location services can reconcile service charges and labor allocations, a complex tasks at sites with many contractors and/or service engineers.

MONITORING THE SWITCHING FABRIC TO DETECT IOT ISSUES

As facilities become more automated, the need to rapidly detect and correct IoT system errors grows in importance. Take, for example, a video surveillance system that uses networked cameras with on-board artificial intelligence to count people, perform automated facial recognition, and alert when motion detection thresholds are crossed. These tasks require streaming data from cameras to application servers. In this machine-to-machine application, if the video stream starts going astray there is no human watching in real-time to detect image degradation on a monitor.

An automated supervisory system is essential in this application for both operations optimization and preventive maintenance. Since the only common element among many machine-to-machine applications is the building's LAN that links everything together, it makes sense to look for an automated supervisory solution that runs within the switching fabric.

Figure 27: Aruba CX 8400 High-Availability Switch

Aruba's CX switch operating system uses a database-centric design and a programmatic interface to the entire database schema. All internal states, protocols, and statistics are expressed in the database, providing visibility into everything that happens on the network. With a database-driven operating system, any factor can be monitored and performance compared over time.

Aruba's Network Analytics Engine (NAE) uses Python scripts to define which switch resources to monitor and, optionally, rules for actions to take when certain conditions are true. CX is database-driven, and any factor can be monitored over time and acted upon. Python scripts typically target IIoT performance, security, and scale.

In the example above, the camera flows would be monitored with NAE scripts, and an automated notification sent to security and service personnel if degradation is detected in the data stream or switching fabric itself. Proactively addressing a video system problem prior to failure can prevent damage from undetected security breaches.

ENHANCING THE RELIABILITY AND QUAILTY OF MOBILE STAFF COMMUNICATIONS

As organizations migrate to mobile devices, network edge access shifts from wired Ethernet to Wi-Fi. Providing the quality of service (QoS), bandwidth, and management tools necessary to deliver secure, toll-quality voice and jitter-free video at scale to mobile devices over Wi-Fi requires sophisticated wireless infrastructure. Aruba's AI-based application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS - on an application-by-application, device-by-device basis - as needed to deliver highly reliable voice, video, and other multimedia services. The result is a superb user experience in which staff can roam while staying connected with each other, anywhere in the facility.

Besides high-quality voice, secure text messaging is a popular means by which staff securely communicate. Secure texts can be sent via mobile within the facility without the security risks of using standard texting applications on personal devices.

These services are delivered over the same Aruba Wi-Fi infrastructure that is used for mobile IoT telemetry, IT devices, and OT facility operations systems. Converging all services under Aruba's extensible ESP platform yields considerable cost savings, enables IT to deliver uniform security and visibility from end-to-end, and allows additional services to be added on without ripping-and-replacing infrastructure. As will be discussed elsewhere in this paper, Aruba's Air Pass technology allows cellular users to seamlessly handoff voice and data between cellular and Wi-Fi networks. In many instances this eliminates the need for expensive distributed antenna systems while offering high connection speeds, better audio quality, and fewer coverage dead spots.

Aruba has partnered with the leading mobile staff communication vendors on solutions that span a broad range of applications on wearable and handheld Wi-Fi enabled mobile devices. Properly implementing these applications and services requires a different way of architecting wired and wireless infrastructure to achieve application prioritization, QoS, and actionable monitoring and diagnostics.

Application Prioritization

Wi-Fi bandwidth is a limited and shared commodity, so it's important that business-critical applications can be prioritized over social media and lesser priority apps. Aruba's deep packet inspection engine automatically identifies thousands of different mobile applications on launch. When a business-critical application is recognized, the network will automatically establish a bandwidth contract to reserve sufficient bandwidth for proper operation. Non-critical applications are given bandwidth prioritization to deliver the best possible experience needed without compromising performance.

QoS

Hospitality productivity applications utilize end-to-end encryption to protect confidentiality and privacy. This unfortunately breaks QoS mechanisms on typical wired and wireless networks as they are unable to differentiate between non-critical and latency-sensitive traffic. Mis-tagged traffic is subject to jitter and delays.

Aruba has addressed this issue by developing a heuristics feature that can identify latency-sensitive traffic without decrypting it. The heuristics feature is a standard component of Aruba's secure mobility infrastructure that correctly tags voice and video traffic, but also retags misidentified traffic originating from non-Aruba network infrastructure.

Monitoring & Diagnostics

Cutting the cord on wired phones impacts the selection of monitoring tools. In-line tools can used to monitor wired IP phones call performance and diagnose the source of problems. Wireless phones, however, require different tools that provide end-to-end call performance visibility, and variably-sized payload and dynamic port data, to isolate the root cause and remediate issues while calls are in flight. If IT cannot correlate poor call Mean Opinion Scores (MOS) to specific network, server, client, or client peripheral issues, then root cause analysis becomes highly challenging.

To address this issue, Aruba has developed a method to pull data directly from Wi-Fi access points, switches, remote VPN links and controller that is a combination of unified communications and network infrastructure performance data – no external probes required. Monitored data include R-value, jitter, delay, packet loss, Wi-Fi access point-to-controller packet loss, caller/callee identity mapping to MAC and IP address, call status, voice/video call type, and client sessions active at the time of the call

This method allows Aruba's Central and AirWave management and operations solutions to display dropped calls, low MOS values, and performance degradation per user location and device. Aruba controllers and virtual controllers can then use these data to implement Call Admission Control (CAC) based on bandwidth and call count to boost available throughout, reduce dropped calls, minimize bandwidth oversubscription, and lower traffic congestion. The result is significantly improved user experience involving multimedia and latency-sensitive calls.

ZEBRA

Locating, harvesting, and conveying relevant, trustworthy IoT data and context is easier said than done. Data must be captured with fidelity, over networks that reach wherever IoT devices are working or roaming. And cybersecurity must be implemented and enforced from source to C-Suite, from I/O to CMO.

It is on these last points that fractures typically appear in hospitality applications. Data input is often hit or miss. Voice communications with staff are unreliable, especially when roaming. Locating inventory, service carts, and staff members is challenging. End-to-end security is aspirational but rarely achieved, especially with IoT devices and systems.

Zebra's Workforce Connect solution provides a single platform for collaboration with workflows based on contextual data. This enables staff and associates to more efficiently do their job while only needing to carry one mobile device.

Zebra and Aruba have partnered to ensure the secure and reliable operation of Zebra mobile devices, including those running Workforce Connect, over Aruba wireless networks. Aruba's deep packet inspection engine identifies and prioritizes latency sensitive Workforce Connect communications to deliver toll-quality voice to roaming devices across even the largest sites. Zebra barcode scanners are heralded for their ability to capture data reliably on the first pass, and Zebra printers and mobile computers offer unparalleled reliability and robust construction. Aruba ensures reliable service delivery to all Zebra devices when they operate and roam over Aruba Wi-Fi infrastructure, and secure dynamically-segmented communications over Aruba wired infrastructure.

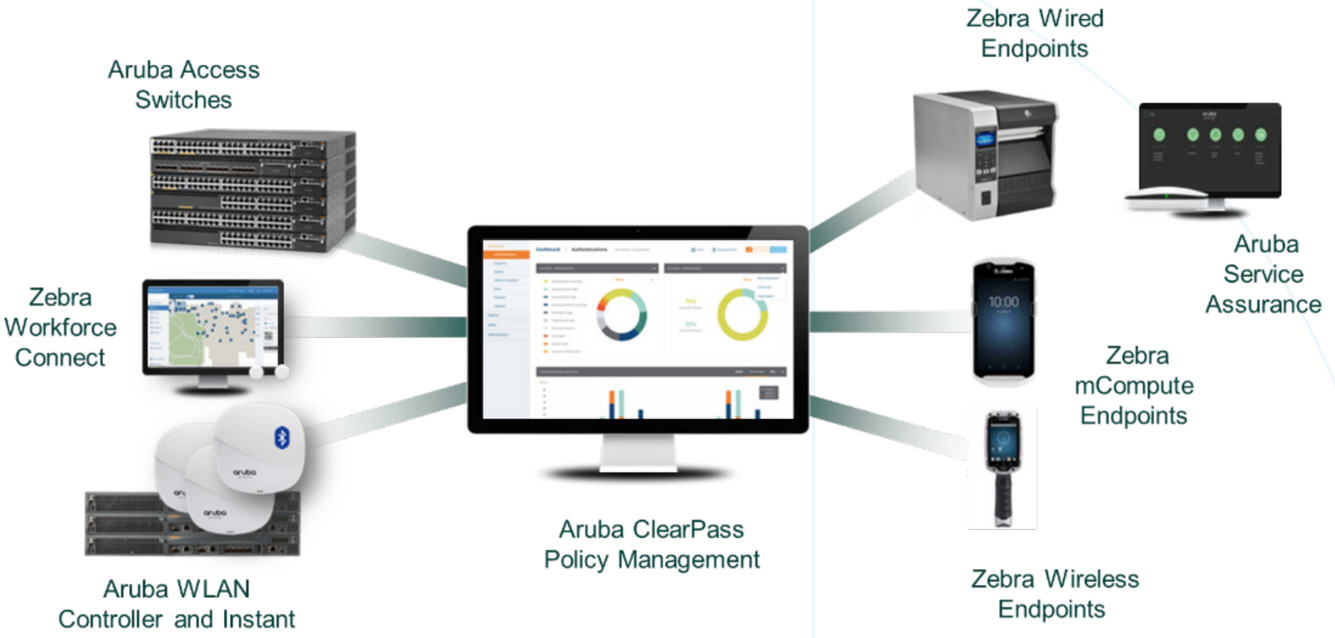


Figure 28: Aruba-Zebra Integrated Voice and Data Capture

Aruba and Zebra have taken the guesswork out of joint deployments by certifying the interoperable operation of both product sets, and by documenting reference designs across a range of hospitality applications. Joint systems go in faster and more reliably.

GUEST, STAFF, AND BUILDING SECURITY

Staff safety and efficient utilization of capital assets are top priorities for hospitality customers, and real-time location services (RTLS) have a central role in achieving these objectives. Quickly identifying the location of staff under duress can save lives and boost workforce morale. State and local legislation, hospitality unions, and major hotel brands worldwide have either committed to provide employees with employee safety devices (ESDs) or have identified the need for additional control measures. From an operations perspective, tracking the location of food trays, on-site service personnel, rollaway beds, and cribs can improve staff efficiency, reduce shrinkage, and speed guest check-ins. Underpinning all of these benefits is the need for robust, reliable RTLS.

The most cost effective and secure way to deploy RTLS is by integrating it with Wi-Fi infrastructure. This has the benefit of amortizing one capital investment across multiple services, avoids the installation cost and maintenance of a dedicated RTLS system, and enables common security policies and network visibility to extend uniformly across all services. Aruba Wi-Fi access points support a broad range of RTLS services thru integrated Wi-Fi 6, Bluetooth, and 802.15.4 radios, making them an ideal platform for monitoring ESDs.

REDUCE COSTS AND IMPROVE GUEST EXPERIENCES WITH ELECTRONIC DOOR LOCKS

Historically, hoteliers have invested in solutions that were tailored for a specific application, such as guest connectivity, door locking, heating and ventilation, room lighting, multimedia, and so on. The result has been a network of networks that don't interoperate, are expensive to deploy and maintain, have multiple management and diagnostics systems, and are unable to extract the value inherent with a unified solution. Lacking a consistent digital identity for each guest, these solutions are unable to deliver the type of highly personalized guest experience that builds loyalty and brand awareness.

Aruba ESP addresses this issue by unifying IoT, IT, and OT networks so customers can quickly integrate new systems and adapt to changing environments and user requirements. ESP is the first fully programmable platform to power more efficient decision making, and used with devices and applications from Aruba's technology partners, Aruba ESP helps customers quickly adapt to evolving business, guest, and staff demands. Virtually every subsystem - from machine inputs and outputs (I/O) in chillers to multimedia devices guestrooms, social distance monitors to gunshot detectors, HVAC monitoring to guest wayfinding - can be accommodated.

ASSA ABLOY Global Solutions

ASSA ABLOY Global Solutions is the world's largest supplier of hospitality locks and in-room safes. ZigBee-enabled VingCard® products are the most widely deployed in-room door locks for lodging applications in the hospitality, healthcare, and education markets.

ASSA ABLOY Global Solutions and Aruba have collaborated to certify Aruba access points for use with VingCard in-room locks, and securely connect them with the Visionline management software by ASSA ABLOY Global Solutions. Separate Zigbee gateways are not required, and the solution can be used in both new and existing Aruba Wi-Fi deployments.

Once deployed, the access points secure communications between the in-room locks and Visionline lock management software, while simultaneously handling guest Wi-Fi and multimedia content delivery. Aruba Wi-Fi 6 access points have an integrated 802.15.4 radio running Zigbee already built-in. Customers that have deployed Aruba Wi-Fi 5 access points can add Zigbee support by using Aruba's low-cost, plug-in ZigBee USB Adapter.

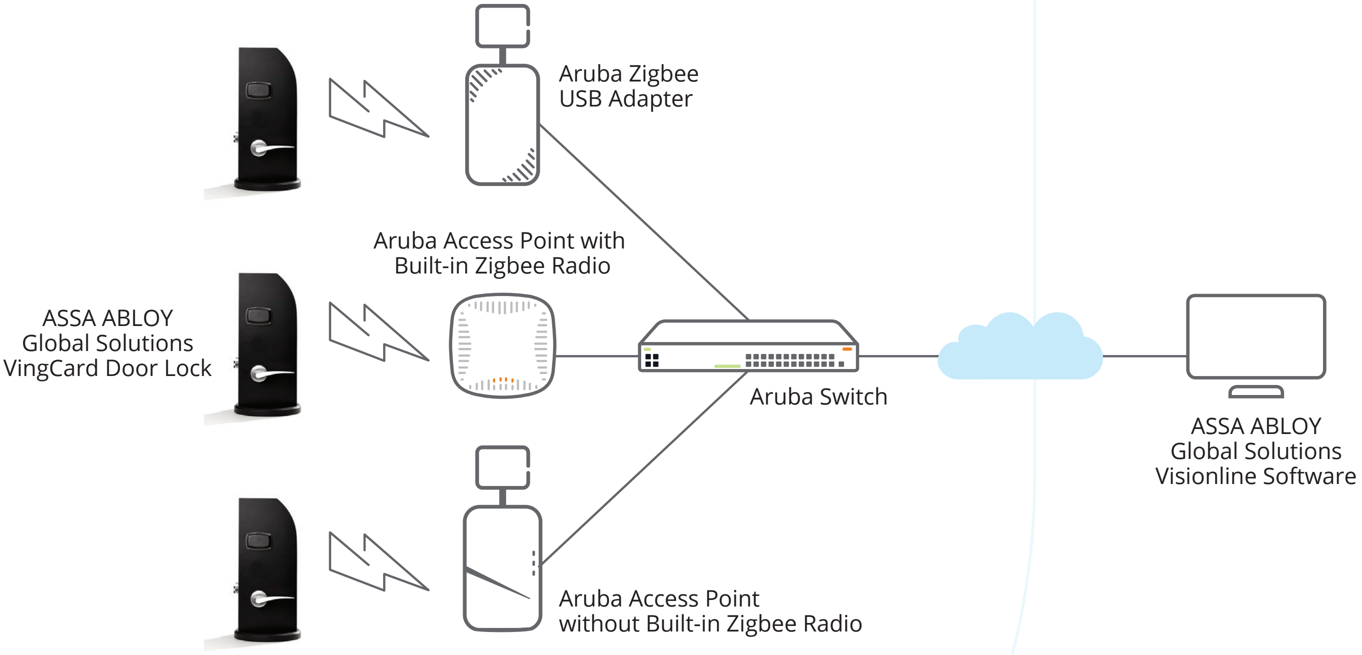

Aruba Zigbee USB Adapter
Aruba Access Point with Built-in Zigbee Radio
ASSA ABLOY Global Solutions VingCard Door Lock
Aruba Switch
ASSA ABLOY Global Solutions Visionline Software
Aruba Access Point without Built-in Zigbee Radio

Figure 29: ASSA ABLOY and Aruba Joint Solution Diagram

The joint solution allows hotel staff to remotely manage and monitor VingCard locks, eliminating needless trips by guests to the front desk and by operations staff to the rooms. Benefits include greater security and control, enhanced guest services, and more efficient front desk and engineering operations.

Guest benefits include dropped key and door ajar protection. In a traditional off-line lock, if a guest inadvertently drops a room key then whoever picks it up can go door-to-door until they find a door the key will open. With the ASSA ABLOY Global Solutions on-line system, an alert will be raised and the key invalidated after a specified number of unsuccessful unlocking attempts. If a guestroom door isn't closed properly and remains ajar, the system can automatically notify security staff to check the room.

Customer satisfaction is also positively impacted. If a guest finds his or her room unsuitable, an off-line locking system requires a trip to the front deck to rectify the situation. With the ASSA ABLOY Global Solutions on-line system, the key can be reassigned to a different room with just a call to the front desk. Guests seeking to extend their stay can also do so without needing to visit the front desk to receive an updated key.

With guests increasingly expecting instant and more personalized service, VingCard locks provide hotels with the ability keep pace with the latest trends in digital key technology. VingCard-equipped properties enable arriving guests to skip front desk lines and instead go directly to their guestrooms by using personally-owned smartphones as secure keys. The platform uses the latest in data encryption and secure channel transmission technology to ensure that only authorized users can gain room access. Hoteliers are able to instantly activate the feature whenever market or brand demands change, and without the need to replace existing hardware.

Facility operations also benefit from converging VingCard locks and Aruba wireless technology. Engineering can be notified automatically of low battery and other maintenance conditions before locks stop functioning and guests are locked out.

SHIPBOARD REAL-TIME LOCATION SERVICES

A key trend driving the demand for multi-function converged hospitality networks in the cruise industry is the desire to deliver exceptional new guest experiences over existing, commonly shared network infrastructure. The objective, driven largely by CFOs, is to build on top of sunk capital investments instead of adding new infrastructure with each new service offering. Replacing disparate and often proprietary networks with a single, commonly-shared network reduces cost and complexity…provided the network can adequately scale to handle the new services without compromising security or reliability.

Today's large cruise ships provide entertainment, dining, and passenger services throughout the ship. Easily finding a cabin room, navigating to a restaurant, or sharing location with family members all add to favorable guest experiences. Successfully delivering these experiences requires context, specifically the identity and the location of guests and their destinations. Traditional RTLS solutions that leverage cloud-based software as a service (SaaS) are unsuitable for shipboard use because at sea they require costly, latency-prone satellite connections. Instead, on-premises RTLS solutions are a must for shipboard applications.

decurtis
corporation

DeCurtis Corporation is a product-focused SaaS software solution provider offering transformational experience technology for cruise ships, restaurants, theme parks, and the extended hospitality industry.

DeCurtis has partnered with Aruba to forward BLE asset tag and wearable badge/wrist band location data via Aruba Wi-Fi 6 access points to DeCurtis' proprietary Location Solution with Privacy Engine. The DeCurtis software precisely locates the tags, badges, and wristbands in a virtual model of the ship, and provides routing information for turn-by-turn wayfinding. Location information is available to DeCurtis safety applications for mustering and emergency search purposes. The DeCurtis Location Solution includes a Privacy Engine that provides time- or location-based masking in private areas such as passenger cabins. Location information is also used for contact tracing in the event of a health incident, helping to contain outbreaks and identify exposed areas that require immediate sanitation.

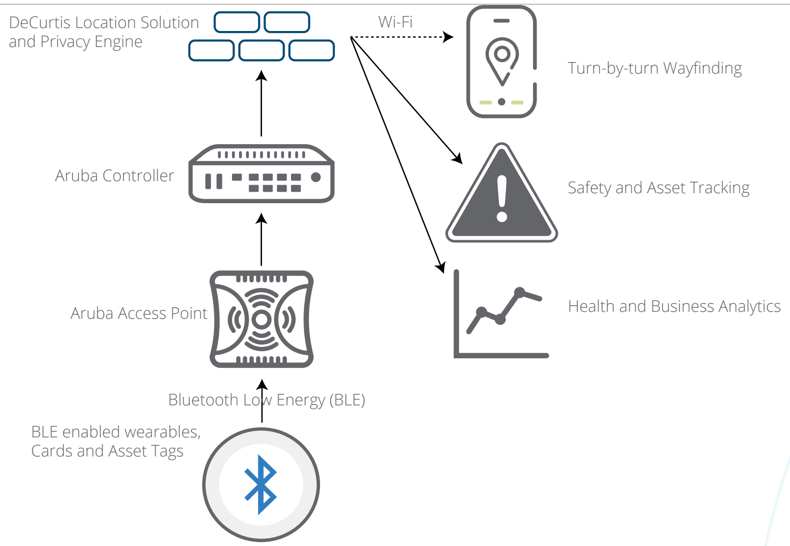


Figure 30: DeCurtis and Aruba Joint Solution Diagram

The Aruba and DeCurtis solution also enhances staff efficiency. For example, wayfinding relieves staff of the need to guide guests and new employees around the ship. Food and services can be delivered to guests wherever they are playing or roaming. And valuable assets, including food delivery carts, can be quickly located.

Favendo

Favendo is a real-time location services company, based near Nüremberg, Germany, specializing in mobile tracking and navigation solutions that meet the demanding environmental requirements of shipboard use.

Aruba and Favendo have partnered to enhance cruise ship digitalization by delivering better guest experiences and improving passenger-to-crew communications. Aruba Wi-Fi 6 access points share real-time location data with Favendo's on-premises Commander platform to deliver wayfinding, asset tracking, and proximity marketing services. Aruba's WLAN infrastructure, pervasively deployed throughout the ship, sends location data to Favendo clients without requiring battery-operated beacons. The access points also collect BLE asset tag, badge, and wristband data for tracking applications.

Using Aruba infrastructure eliminates the need for dedicated location gateways, simplifying deployments and significantly lowering installation and maintenance costs. Aruba access points securely tunnel device and location data to the Favendo Commander application, and push wayfinding data over Wi-Fi to the Favendo mobile application. This creates a single network infrastructure that serves double-duty by handling both network communication and location services.

Favendo's Commander application calculates indoor location, manages navigation, coordinates proximity marketing, and handles asset and personnel tracking. All functions are managed via an on-line dashboard, while an SDK simplifies the integration of location aware services with the cruise line's Android and iOS applications.

In addition to delivering reliable location services, Aruba Wi-Fi 6 access points also integrate with IoT devices in galleys and control rooms, and multimedia devices in dining halls and sleeping accommodations. Wi-Fi 6 offers a level of future-proofing since it's both backward compatible with older Wi-Fi devices, and interoperable with the latest high-speed mobile devices from Apple, Samsung, and others.

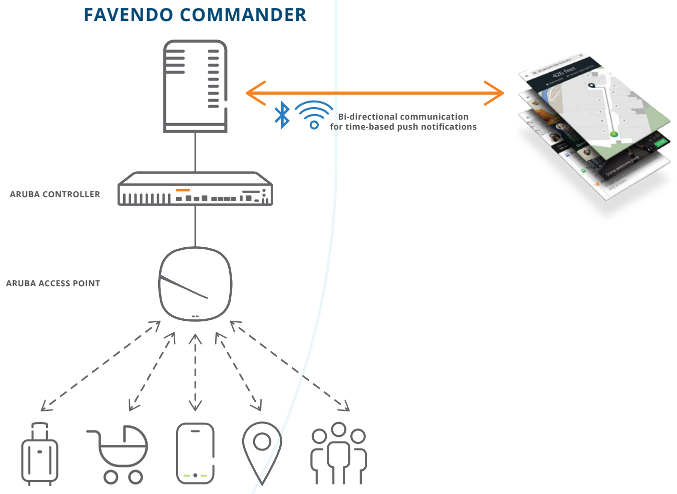

FAVENDO COMMANDER
Bi-directional communication
for time-based push notifications
ARUBA CONTROLLER
ARUBA ACCESS POINT

Figure 31: Aruba and Favendo joint solution topology

Aruba and Favendo lower life-cycle operating costs by eliminating the need for battery powered beacons, separate location gateways, and satellite-based SaaS applications. Analytics derived from the RTLS data boost revenue by enabling location-based marketing, enhance loyalty by helping the crew better serve passengers wherever they congregate, lower stress by reuniting lost passengers with their families, and increase operating efficiencies by helping to schedule services – including maintenance and cleaning – based on actual traffic patterns.

MOBILE PANIC BUTTON LOCATION SOLUTIONS

Hospitality workers are routinely exposed to job safety issues hidden from common view – abusive or threatening behavior from inebriated guests, hazardous drugs left behind in rooms, and guests' medical emergencies. These issues impact employee health, morale, and retention, and represent a serious threat to the reputation of brand owners and franchisees.

Industry associations and major hotel brands have committed to address these issues. For example, the members of the American Hotel & Lodging Association have committed to providing U.S. hotel workers with portable panic buttons by 20205, and allocating other resources to improve hotel worker safety. The UK's Health and Safety Executive and the European Agency for Safety and Health6 both identified the need for control measures to reduce the significant risk factors and harassment faced by hotel workers.

Portable panic buttons, also referred to as Employee Safety Devices (ESDs), alert security personnel in the event of dangerous or threatening situations. Used in conjunction with location-based services, ESDs can quickly raise an alert and guide safety personnel to the incident location. Besides raising assistance, the physical presence of ESDs can also serve as a visible deterrent to individuals with malicious intent.

Installing a dedicated network to support ESDs is not economically viable, and many IT departments will not permit an overlay network. Battery-operated wireless sensor networks present cybersecurity risks because they bypass standard IT security monitoring tools, and have maintenance issues associated with battery replacement.

Aruba's access points overcome these issues by incorporating Bluetooth and other ESD-compatible radios. This allows IT managed infrastructure to enhance worker safety, using Aruba security mechanisms to protect against malicious or unintentional IoT security breaches.

TraknProtect

TraknProtect is a leading supplier of BLE-based RTLS staff safety and asset tracking solutions The TraknProtect staff safety solution is comprised of Bluetooth-enabled panic buttons for employees and tags for locating vendors, inventory, beds, cribs, and food and beverage trays. These panic buttons and tags are interoperable with Aruba's Wi-Fi 5 and Wi-Fi 6 access points. Used together, a joint TraknProtect and Aruba solution eliminates the need for separate staff safety radios and makes the most of capital investments in the wireless infrastructure.

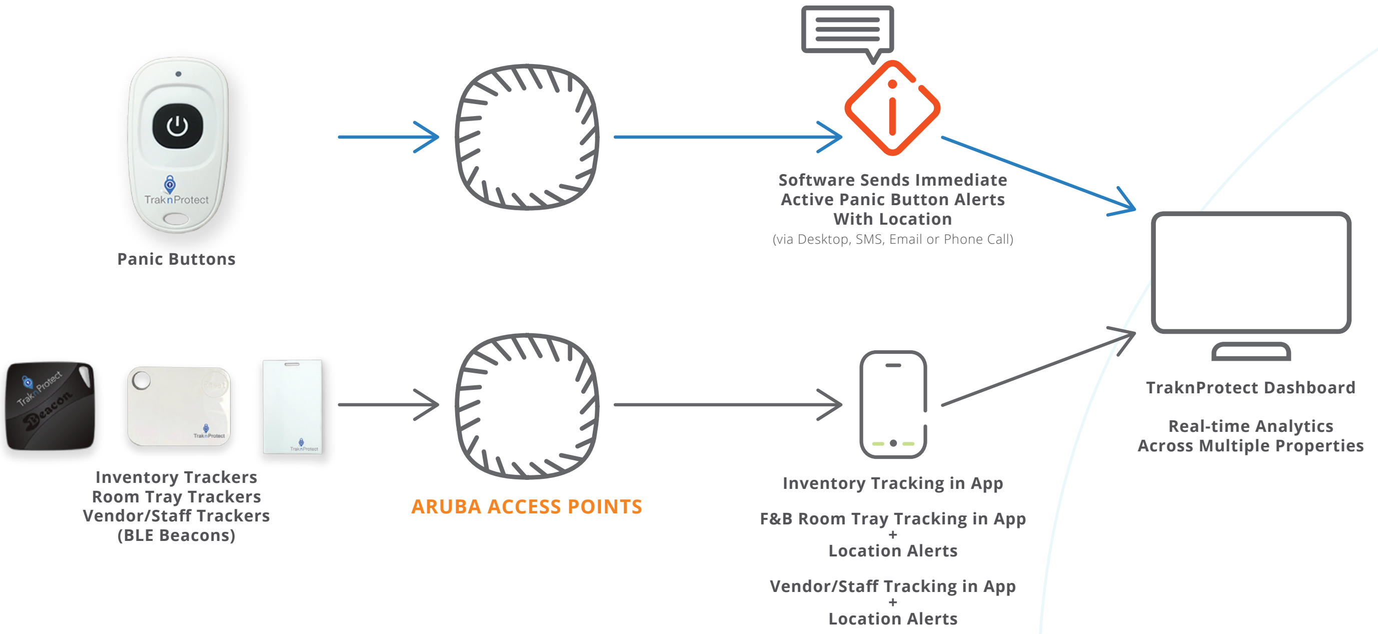

Panic Buttons
Software Sends Immediate Active Panic Button Alerts With Location
(via Desktop, SMS, Email or Phone Call)
TraknProtect Dashboard
Real-time Analytics Across Multiple Properties
Inventory Trackers
Room Tray Trackers
Vendor/Staff Trackers
(BLE Beacons)
ARUBA ACCESS POINTS
Inventory Tracking in App
F&B Room Tray Tracking in App
+
Location Alerts
Vendor/Staff Tracking in App
+
Location Alerts

Figure 32: Aruba and TraknProtect Joint Solution Diagram

When an activated ESD is detected, all access points within range report the device's presence and signal strength to the TraknProtect cloud-based platform. By correlating ESD signal strength with the location of the access points, the TraknProtect platform can accurately report the location of the activated ESD in real time, even if an employee is on the move.

Once the individual in duress has been located, the joint solution sends alerts to property management with location updates via SMS, email, and mobile app. The real-time dashboard provides context as to the exact room and floor that the button was pressed, the employee's updated location as they move, and an incident log for thorough data review.

The joint solution also offers inventory, food and beverage and vendor location tracking. Leveraging the same Bluetooth functionality in Aruba access points to scan for BLE tags, employees can quickly locate any item with a Bluetooth tag such as rollaway beds, refrigerators, cribs on the TraknProtect mobile app. The app not only identifies the item, but also which room, floor, or closet the item was last stored.

The TraknProtect mobile app also tracks tagged food and beverage trays, and where each tray was sent. Signaling which hallway needs to be maintained lets employees streamline workflows. Doing so cuts down on time to retrieve room trays, improves staff time management, and improves the overall cleanliness of the hotel.

Lastly, access points can also track Bluetooth-enabled vendor badges given to any outside vendor who enters the hotel premises. Using the dashboard, hotel management can see a heat map of where the vendors were, a timesheet of when they worked, and insights into which outside vendors provide the best service.

With the integrated Aruba and TraknProtect solution, hospitality customers no longer need a separate overlay safety network. The Aruba infrastructure that's installed for guest and staff IT services can do double-duty as a staff safety and asset tracking system.

The Aruba and TraknProtect joint solution provides peace of mind to employees, helps hotels comply with state and local legislation related to staff safety, and optimize employee productivity with vendor, inventory, and tray tracking systems.

VAPING AND AIR QUALITY MONITORING

In 2016 the U.S. Food and Drug Administration (FDA) mandated that electronic cigarettes (e-cigarette) products be regulated as tobacco products, and subsequently banned the sale of these products to minors. That same year a World Health Organization (WHO) report recommended that e-cigarettes be banned in indoor areas and wherever smoking is prohibited. Since then governments worldwide have enacted laws that prohibit e-cigarette usage (vaping) everywhere that smoking is banned. The hospitality and transportation industries, in particular, have forbidden vaping in hotel rooms, airplanes, and trains.

The challenge has been how best to enforce no-vaping rules since the vapors can be difficult to detect. E-cigarette vapor contains ammonia, and the first vaping detection sensors simply detected when a preset level of ammonia was present and triggered an alarm. The problem is that many products contain ammonia, including body sprays, resulting in a high false alarm rate.

An alternate solution is to use two different sensors to detect ammonia and other chemicals present in e-cigarette vapors. Dual-trigger sensors have a much lower false alarm rate, and raise confidence that a vaping alert is valid.

IPVideo Corporation

IPVideo is a New York-based developer of smart building physical security sensors. Their HALO IoT Smart Sensor is a multi-function security and environmental monitoring devices that hosts chemical sensors, audio detection, and a voice synthesizer.

Figure 33: HALO Smart Sensor Powered By Aruba Switches And Pass-Through PoE Access Points

IPVideo and Aruba have collaborated to enable plants to combat vaping through automated sensing and response. Powered by Aruba PoE pass-thru access points and PoE switches, HALO detects vaping and THC using dual-triggers to reduce false alarms. HALO incorporates multiple sensors so it can serve additional roles, too, i.e., detecting particulates, carbon dioxide, carbon monoxide, volatile organic compounds (VOCs), oxidizing agents, and ethanol. These features make HALO well suited to air quality monitoring applications.

Audio monitoring enables HALO to detect cries for help, while a voice synthesizer lets HALO respond to occupants with context-appropriate messages, i.e., in response to a verbal request for "help" HALO can respond that "help is on the way." Voice detection and response are processed locally, not in the cloud, to ensure that privacy is maintained.

The joint solution is ideal for enforcing no-vaping rules, and monitoring for other signs of danger.

GUNSHOT DETECTION

One of the most dangerous situations faced by first responders is a live shooter inside a building or resort. Without knowing the location of, and weapons used by, the shooter, first responders imperil themselves when they come on the scene. Situational awareness can save lives and speed apprehension of the perpetrator.

Emerging technologies for public safety sit at the cutting edge of the detection and mitigation of threatening situations, with gunshot detection being an essential element in that toolbox. Despite claims about sophisticated machine learning algorithms, older generation gunshot detection systems based on acoustic sensor arrays were notoriously prone to false alarms.

The most current generation of gunshot detection relies on multiple sensing mechanisms – muzzle flash, impulse, and pattern matching – to validate the presence, type, and even barrel length of discharged firearms. The result is fewer false alarms and more efficient routing of first responders to active shooter-involved incidents.

Installing a dedicated network to support gunshot detectors is not economically viable, and many CISOs will not permit such overlay networks. Additionally, battery-operated sensors on wireless networks, like LoRa, present cybersecurity risks by bypassing standard IT security monitoring tools. There are also maintenance issues associated with battery replacement.

Aruba's Wi-Fi access points overcome these issues by providing a USB port that supplies power and data communications for gunshot detectors. Standard Aruba security mechanisms help protect against malicious or unintentional security breaches.

AMBERBOX Gunshot Detection

AmberBox, a leading provider of next-generation gunshot detectors, and Aruba have partnered to ensure that first responders can be reliably notified when an active incident is in process. Applications include lobbies, conference centers, and publicly accessible spaces.

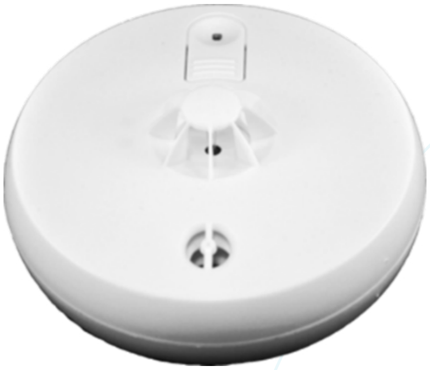


Figure 34: AmberBox Gunshot Detector

The joint solution works with Aruba Wi-Fi 5 and Wi-Fi 6naccess points already deployed on-site, avoiding the need for a separate overlay network. AmberBox sensors interface with the access points' USB ports, which provide both power and data access. Sensor spacing matches the access point spacing required for voice applications. AmberBox sensors do not interfere with the access point's ability to deliver high performance voice, video, location, and telemetry.

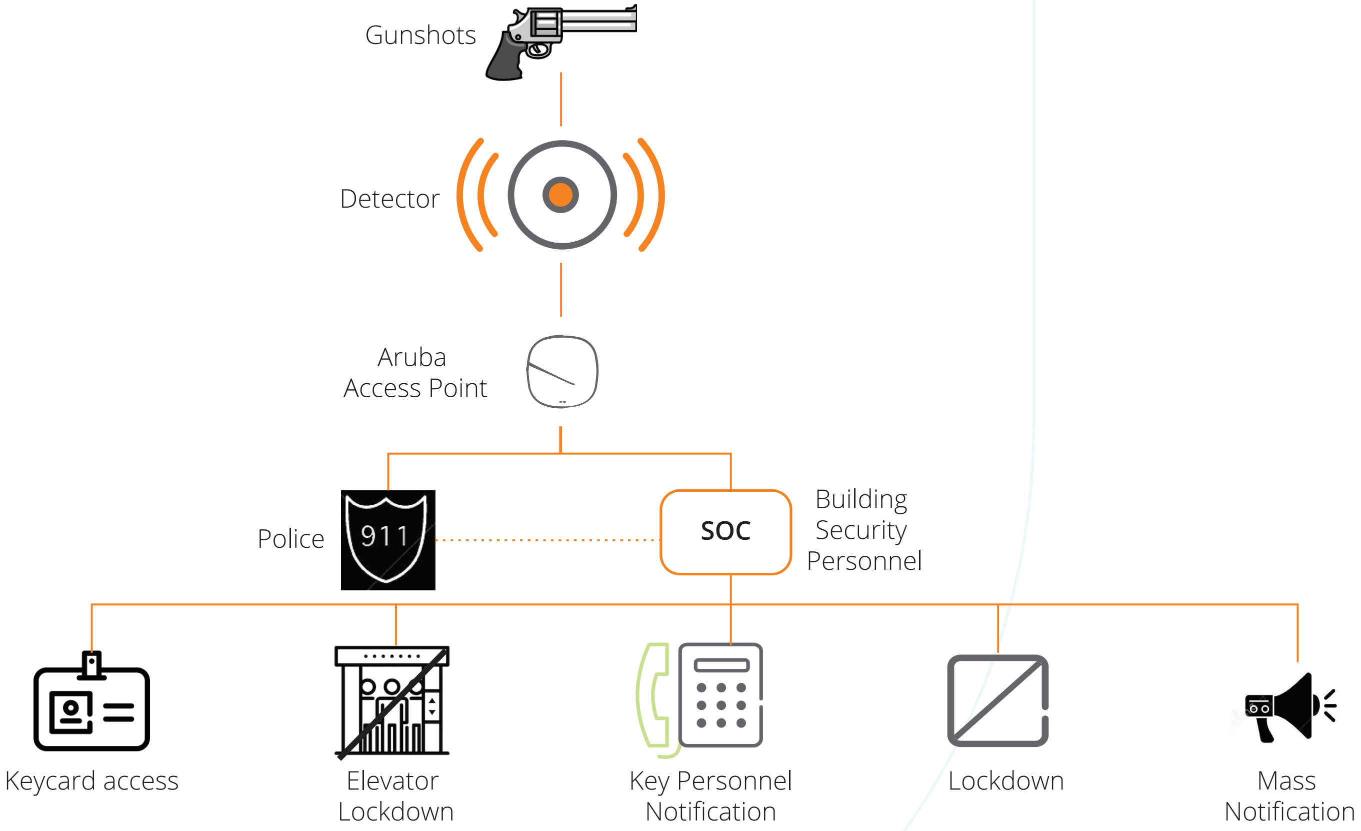


Figure 35: AmberBox Gunshot Detection And Notification System

The sensors use acoustic and infrared data to recognize when firearms are discharged. Within roughly 3.6 seconds, the sensor identifies the actual gunshot signature and relays an alert using the USB port. Access points use secure tunnels to relay data to the AmberBox monitoring application. Automatic alerts can then be sent to law enforcement via the AmberBox cloud-based e911-certified platform, with additional notifications to building security or other responding parties. A conference call line is automatically established to share information and coordinate efficiently.

AmberBox can also immediately activate facility security systems while alerting personnel with SMS, e-mail and call notification. Real-time shooter location tracking can be viewed through the Web or a mobile response platform.

Dynamic segmentation of IoT traffic is maintained throughout the Aruba infrastructure, protecting the rest of the network against compromised devices. Aruba switches automatically set-up secure connections with Aruba access points without the need for separate VLANs, regardless of the switch port into which they're connected. This feature simplifies the initial deployment of the access points, and minimizes opportunities for miswiring during adds, moves, and changes over the life of the deployment.

Key benefits of a jointly deployed solution include:

- Gunshot detectors can be placed where needed without new cabling or PoE injectors;
- No maintenance required, unlike with battery operated systems;
- Uses existing Aruba access points and leverages Aruba security mechanisms; and
- Supplements security solutions from Aruba and other partners including occupant safety monitoring, video surveillance, door locking controls, and wayfinding solutions.

Jointly deployed with AmberBox sensors, Aruba access points dramatically improve situational awareness so first responders know what they're facing on arrival.

CONTEXT-AWARE, REAL-TIME INTEGRATED EMERGENCY RESPONSE AND NOTIFICATION

Hospitality security teams have an obligation to protect the wellbeing of people who work in, visit, or travel through their facilities. Posted evacuation plans and audio/visual alarms are often considered sufficient for this purpose, but in reality they aren't. During an incident people need context-relevant information pushed to them to keep them safe under highly fluid circumstances.

Moreover, first responders need the ability to communicate in real-time with those in imminent danger, who need assistance exiting the facility, and who are in safe areas but don't know it. Active communication can often make the difference between a well-managed incident and a nightmare scenario.

Patrocinium™

Patrocinium, in partnership with Aruba, addresses integrated emergency response and notification by combining Meridian indoor location services with an innovative mobile app. The solution informs people of incidents and what actions should take based on danger in or near their specific location. Communication occurs in real time with tenants, visitors, and staff, and unique 4D graphics enables first responders to see where people are situated within buildings.

Figure 36: Meridian-Based Patrocinium Emergency Response Platform

All that is required for 4D support is a Meridian subscription and Aruba Beacons, standalone or embedded within Wi-Fi access points, throughout the facility. Patrocinium's app leverages Meridian's maps and indoor location, in addition to GPS, to provide a new level of visibility. Unlike GPS-only based location services that cannot differentiate between floors, Aruba's BLE indoor location incorporates that critical 4th dimension

Generic crisis management and emergency notification tools that use text, e-mail, social media, and audio/visual alarms to alert people of danger fall short because they can't isolate those in danger from other occupants, or provide real-time situational awareness.

Working together, the Patrocinium Platform and Meridian location services fill this critical gap. Doing away with lists and opt-in workflows, Patrocinium instead uses patented software to automatically notify occupants when they are within a danger zone geofence without first signing up for alerts. To protect user privacy, Patrocinium's geofencing technology only visualizes individuals' locations when they are in or near danger, or need assistance.

This event-triggered process generates an immediate, personalized flow of information to anyone at risk of being affected by an incident. Occupants are shown their location, relevant pushed updates, perimeters, and safe zones. If help is needed it's one button-push away. In essence, users become sensors for the security team.

Key benefits include:

- Situational awareness indoors so users can see their location relative to incidents, fire extinguishers, exits, and other safety-related data;
- Wayfinding guides users to stairwells, exits, and designated outdoor muster areas;
- A4D picture with longitude, latitude, floor number, and time gives first responders more details than they could obtain from just GPS;
- Exact location is presented when a user declares themselves safe/unsafe via the mobile app;
- Easily integrates into existing branded mobile hospitality apps - a dedicated app is not required;
- Responders can send specific information to targeted recipients; and
- Incident recording ensures that all relevant data are saved for digital auditing and reporting.

Patrocinium and Aruba have created an event-triggered process that generates an immediate, personalized flow of information to those affected by an incident. Staff and guests alike can see their location relative to an incident, send and receive updates, and see perimeters and safe zones.

SUMMARY

The machines and applications used in hospitality are tailored to optimizing human activity monitoring, organizational redesign, human productivity, and health and safety. The target business benefits - improving efficiency, building loyalty, creating unique experiences, and improving safety – can only be achieved by securely mashing up IoT and OT data with contextual information to create hyper-aware operating environments.

Aruba's unified infrastructure, zero-trust security, and AI-powered software - used in conjunction with solutions from key technology partners – enables hospitality providers to create hyper-aware hospitality facilities. By combining IT, OT, and IoT into a single open framework that can be leveraged by third-party devices, applications, and services, Aruba ESP can easily support changing IT, IoT, and facilities-related operational requirements by plugging new systems into their existing Aruba infrastructure. No rip-and-replace needed. The benefits? Higher efficiency, productivity, profitability, reliability, safety, and security.

Please contact us for information on how your properties can make the leap to hyper-awareness.

CITATIONS

[1] William H. Markle, “The Manufacturing Manager’s Skills” in The Manufacturing Man and His Job by Robert E. Finley and Henry R. Ziobro, American Management Association, Inc., New York 1966

[2] C. R. Jaccard, “Objectives and Philosophy of Public Affairs Education” in Increasing Understanding of Public Problems and Policies: A Group Study of Four Topics in the Farm Foundation, Chicago, Illinois 1956

[3] A business moment is a transient set of context-sensitive interactions between people, business, and things that yield a negotiated result as opposed to a predetermined result, i.e., a personalized, targeted offer from a retailer based on location, time, and CRM data. See Frank Buytendijk, Digital Connectivism Tenet 4: We Do Not Differentiate Between People and Things, Gartner, 1 November 2016.

[4] McKinsey Global Institute, Unlocking The Potential Of The Internet of Things, June 2015

[5] Hotel Industry Marks Significant Progress Toward 2020 Nationwide Implementation of Safety Device, October 2019, https://www.ahla.com/press-release/hotel-industry-marks-significant-progress-toward-2020-nationwide-implementation

[6] Protecting workers in hotels, restaurants and catering, 2008, https://osha.europa.eu/en/publications/report-protecting-workers-hotels-restaurants-and-catering

[7] CRM Customer Service and Support, December 2018, https://www.gartner.com/en/documents/3895585

aruba
a Hewlett Packard
Enterprise company

WP_DesigningHyper-AwareHospitalityFacilities_RVK_120420 a00100713enw

Contact Us **Share**