THE ARUBA SD-BRANCH BRANCH

As branches are the one place where your business is closest to your customers, it is important to consider how all elements of the branch – WAN, WLAN, wired, security and AI-powered operations solutions that address your IT network and service's needs. Aruba's vision for the branch are solutions that work together to provide a comprehensive edge platform, or independently within an existing branch architecture. Expected outcomes include:

- **Performance oriented wireless, wired and SD-WAN that just work**
- **The consolidation of infrastructure and management solutions for simplicity and cost-savings**
- **Security that is easy on customers and associates, while offering automated segmentation and enforcement to meet the strictest compliance demands**
- **Dynamic Segmentation that allows non-IT staff at a branch to connect devices to wired ports or Wi-Fi, which ensures proper policies, eliminates configuration errors and reduces security risks**
- **Zero-touch provisioning that lets you accelerate branch infrastructure deployments without as many costly truck rolls**

To better understand how Aruba can help your organization, the following use cases provide a practical view into how simplicity and the right technology can help transform your branch in perfect mixture of face-to-face and digital interaction.
USE CASE #1: DELIVERING A SIMPLE, HIGH PERFORMANCE WI-FI EXPERIENCE

As cloud-based applications, the increased use of IoT, and bandwidth intensive and interactive applications that require voice and video continue to find their way onto networks, ensuring a quality of service that does not impact the user experience or the business is paramount.

Problem: A legacy approach that physically requires separate infrastructure

Legacy WLAN deployments often led to multiple SSIDs within a branch for performance and security reasons with each SSID serving a unique purpose for services such as guest access, employee device access or specialized access for a particular device type. Having multiple SSID’s decreases the overall capacity and efficiency of the Wi-Fi network while also increasing network complexity, as each SSID must be translated to a network VLAN specific for its particular use.

This is only compounded by an increasing demand for high speed wireless coverage & capacity to support mobile solutions designed for associates and customers, as well as the growing need for smart building IoT. Having many SSID’s causes confusion, leads to errors and potentially opens up security holes because of devices being assigned to the wrong SSID or malicious registration of a rogue device to an SSID to exploit a pathway into the network.

Solution: Wi-Fi 6 with automated role-based enforcement

Aruba’s portfolio includes industry leading Wi-Fi 6 (802.11ax) access points (APs) capable of handling the pressures put on modern networks. These APs, together with our Network Policy and Access Control service, ClearPass, offer a new level of performance and security that meets today’s demanding network expectations while keeping the user experience as simple as possible.

Aruba’s built-in role-based access and policy enforcement firewall (PEF) simplifies how users connect and centralized policy using ClearPass creates an enforceable and auditable network regardless of if it is a guest’s mobile device, an employee laptop or a facilities-centric IoT device such as a thermostat or smart lighting.

Why this works:

- No need for separate networks or SSIDs – It’s as easy as connecting to the employee or guest SSID, and Aruba’s software takes care of the rest – how you authenticate and what you have access to
- Built-in capabilities like Aruba Air Slice, OFDMA, and MU-MIMO for Wi-Fi 6 that can handle thousands of devices simultaneously, while dramatically reducing network congestion
- No two apps are alike, so Aruba deep packet inspection lets you easily identify and prioritize a business app over some of your customers favorites, like YouTube and Netflix
- Seamless cellular to Wi-Fi handoff – Aruba’s Wi-Fi 6 performance, security and industry-wide Passpoint support offers 5G performance without the need for expensive and complex indoor cellular solutions

New ideas and the Aruba advantage

The use of social meeting areas in larger branches are being explored as a way to make the branch experience more inviting. Elderly customers won’t need to stand in long lines, and the parent with children in tow, can sit and engage with an associate in a more relaxed fashion. Aruba offers a secure, high performance connection for the associate’s device, where traffic is segmented and easily directed to the appropriate data center, regardless of the associate’s role.
USE CASE #2: SECURE IOT ADOPTION

With Aruba, it is possible to simplify the experience for IT while allowing them to securely implement IoT technologies for customer engagement and facilities use cases, all without complex overlay networks. This also eliminates manual network configuration and onboarding workflows that are prone to operator error.

Problem: IoT can introduce new devices with poor security
As IoT devices are currently about 50% wired or wireless, the need to manage independent IoT overlays through assigning specific ports to VLANs, trunks and even MPLS tags over WAN’s has become a nuisance to accommodate device connectivity (e.g. surveillance cameras and sensors), making management cumbersome and inefficient.

Solution: Utilize Aruba’s Dynamic Segmentation solution at scale
By taking further advantage of Aruba’s role-based access and Policy Enforcement Firewall, wireless and wired IoT devices can automatically be fingerprinted and assigned proper network access. Without the need to configure individual ports on Aruba Ethernet switches or create separate VLANs. The same applies to Aruba wireless solutions as separate SSIDs are not required.

Why this works:
• Automated controls make it easy for IT to define what connects to the network, what resources it can access and what users are allowed to connect to it
• Helps eliminate configuration and VLAN complexity and errors while utilizing switch ports more efficiently
• Centralized policies – the addition of Aruba ClearPass creates the ability to more accurately identify devices and automatically change the privileges of devices – even those exhibiting abnormal behavior helping to protect and identify threats

New ideas and the Aruba advantage
To better serve customers that do not feel secure using outdoor ATM machines, the use of indoor machines provides the option of introducing video-based virtual teller assistance. This is allowing banking institutions to offer traditional and newer services, while also rightsizing the number of associates needed within these branches. As these ATM machines are plugged into Aruba switches, the Aruba policy enforcement firewall is used to assigned the appropriate role and pathway through the network for the ATM’s to function.

For example, the video from these enhanced ATM machines can be automatically treated with a priority within Aruba’s network devices – connecting the customer with the virtual teller – guaranteeing a seamless and consistent experience that will make them use the service again.

USE CASE #3: SAFE CUSTOMER WI-FI ACCESS

Unsurprisingly, physical and virtual security remain high on an IT organizations to-do list. Guest or customer traffic must be kept separate from banking traffic and measures must be in place to ensure a secure experience, free of password theft.

Problem: Guest authentication and traffic are passed in the clear
More often than not, end-users who connect to public Wi-Fi are connected to an open WLAN where traffic can be potentially snooped on by malicious means in order to gain access to sensitive information. Until now, recommendations for combatting this situation have included using VPNs or to not connect at all.

Solution: Leverage new Wi-Fi encryption such as Enhanced Open
Wi-Fi 6 now includes a new protocol called Enhanced Open, where traffic is encrypted per user session and device. Customers can connect to an “open” network and now enjoy a safer experience without the added burden of doing anything extra. What’s more, WPA3 was introduced to replace WPA2 for more secure connections using advanced algorithms and simpler configuration. Both solutions are easy for IT administrators to implement and users to embrace, while enhancing the overall security posture of your networks.

Why this works:
• Your Guest, employee and device policies are consistent and universally applied regardless of location – and can be easily audited for compliance
• Aruba ClearPass allows for external captive portal authentication at scale to handle many thousands of unique user devices per day

New ideas and the Aruba advantage
In addition to offering wireless guest access, some institutions are installing convenient digital or web-based
terminals for customer use. In addition to using Aruba ClearPass to offer a branded guest portal, it’s very easy to add compliance checks such as an “acknowledgement of use” statement that customers must click prior to receiving a connection. Whether connecting via wireless or wired, the dynamic assignment of roles ensure segmentation of traffic consistently. Devices that support Enhanced Open also receive extra safeguards.

USE CASE #4: WAN MODERNIZATION
Cost savings and the opportunity to provide a better user experience, are driving IT organizations to search for alternatives to high priced WAN links such as fixed line or MPLS and look to utilize secured transit over commodity Internet circuits. As institutions are undertaking data center consolidation and using a hybrid cloud model, the need to back haul all traffic to a single location is diminishing – with services now both in a data center, a cloud provider and even through an Internet facing portal.

Problem: Route optimization and licensing per traffic volume
Changes are requiring IT organizations to see what service providers should remain involved in or handle on their own. While many SD-WAN vendors offer automation, they lack the ability to provide an end-to-end secured experience for each connection based on traffic context, such as user and device role. A majority of SD-WAN vendors also include additional licensing that limits customer’s to specific broadband speeds.

Solution: The connected SD-Branch
In addition to an innovative SD-WAN orchestration feature for the automatic setup of WAN links across a large branch deployment. Aruba does not require any bandwidth licensing. When using Aruba wireless or wired solutions, role-based access context is shared with Aruba Branch Gateways. The policy enforcement firewall and IDS/IPS capabilities let IT easily define where traffic should be sent based on user and device roles, as well as traffic type providing end-to-end consistency.

Why this works:
• While components of Aruba’s SD-Branch solution can be used independently, integration across the Aruba portfolio offer simplicity and automation that help IT quickly roll out SD-WAN, as well as needed LAN upgrades while maintaining the appropriate security posture as defined by the CISO
• All SD-WAN, wired and wireless components can be deployed using zero-touch provisioning and are cloud-managed
• IT organizations can now tailor the branch experience without lengthy service provider delays and cost for simple WAN link or optimization changes

The Aruba advantage
As the branch becomes a center for face-to-face customer engagement, Aruba’s wired, wireless and ClearPass solutions offer the ability to easily support a single SSID for multiple departments whose traffic must remain segmented for compliance and customer security purposes. Aruba ClearPass also provides the ability to authenticate users from different departments to separate domains if required. The addition of Aruba’s SD-WAN solution then enhances the security story, leverages context optimizes the use of WAN links and helps lower the bottom-line.

KEY TAKEAWAYS
Historically, the rigidity of existing network deployments and security overlays have made it difficult to widely introduce new services at scale in their branches without significantly reworking locations.

With the advancements delivered by high-performance Wi-Fi 6 infrastructure, intelligent switches and SD-WAN Gateways, as well as AI-Powered troubleshooting tools and automated security solutions, organizations now have the opportunity to accelerate digital transformation, while reducing costs. Aruba’s vision for the branch of tomorrow starts with the idea of making networking simple again.

From zero-touch provisioning to seamless in-building cellular to Wi-Fi cross-over coverage to the convergence of IoT services – all driven through a uniform policy regardless of location. The flexibility of the Aruba technology portfolio allows you to enable new business models, move faster to gain competitive advantage and enhance your customers experience through the smart use of technology, which provides both value to the bank and customer, while driving business growth.