INTRODUCTION

Providing wireless connectivity at remote sites has been a challenge for organizations with distributed locations, such as retail chains and K-12 school districts, as well as service providers looking for a wireless LAN (WLAN) solution to ease congestion on their 3G/4G networks.

These enterprises need robust WLAN functionality, including voice and video optimization, high reliability and strong security. They also need a solution that is affordable both to buy and to operate in a distributed environment, one that can be deployed rapidly and configured and managed centrally.

Continued growth in BYOD and mobile devices is adding to the need for high-performance WLANs.

In addition, hotel operators, restaurant owners, retailers, and other distributed enterprises must comply with data privacy regulations such as the Payment Card Industry (PCI) Data Security Standard and HIPAA for healthcare.

Service providers also need a cost-effective wireless solution to increase the capacity and coverage of their cellular infrastructure to ensure a positive end-user experience.

All of these organizations need a feature-rich, enterprise-grade WLAN that meets a variety of challenges:

- Offers high performance to accommodate a range of device and traffic types, including data, voice, and video.
- Eliminates deployment complexity and reduces operational overhead.
- Provides sophisticated security that protects internal assets, blocks malware, supports guest access, and isolates sensitive traffic from the rest of the networks.
- Ensures high availability, including uplink and authentication survivability.
- Scales easily, both within a given site and across sites.

Aruba Networks™ designed controllerless Aruba Instant™ WLANs to address the challenges of deploying Wi-Fi at geographically-dispersed locations that have limited or no onsite IT resources. Aruba Instant combines enterprise-grade WLAN performance, security, and scalability with industry-leading ease of use and affordability.

Aruba Instant also includes a free cloud-based activation service that eliminates the need to manually provision and configure APs. The entire deployment process is automated, including zero-touch provisioning, firmware upgrades and inventory management. This enables thousands of Aruba Instant APs to be cost-effectively deployed anywhere in the world at unprecedented speed.

NO DEDICATED CONTROLLERS

The Aruba Instant solution consists of:

- A family of high-performance controllerless 802.11n APs.
- The Aruba InstantOS™, which runs on Instant APs and RAPS to deliver enterprise-grade security, reliability, and scalability
- Aruba Activate™ for zero-touch provisioning and automatic firmware upgrades and inventory management.
- Centralized visibility, control and multisite network management with Aruba AirWave™.

Aruba Instant is easily deployed as an overlay to an existing wired LAN, eliminating the need for IT to redesign or modify the wired infrastructure.

In contrast to controller-based WLANs, controllerless Aruba Instant distributes the controller functionality – including services like authentication and configuration – to all Instant APs and Instant RAPs on the network.

At each distributed location, one dynamically-elected Instant AP performs configuration, firmware management and other management functions for the entire Instant AP cluster.
It also acts as a front end to Aruba AirWave management tools and services. If this Instant AP fails, another automatically takes over with no disruption.

IT has several options for configuring the first Instant AP at each location. One option is to power-up one Instant AP, configure it over the air, and then plug in the other APs – a process that takes about five minutes.

Alternately, customers can use the cloud-based Aruba Activate™ feature in Aruba Instant to perform zero-touch provisioning and automate firmware upgrades and inventory management, which greatly reduces deployment complexity and cost.

With Aruba Activate, Aruba Instant APs and RAPs are factory-shipped to remote deployment sites and obtain their configurations automatically when powered up. Instant APs and RAPs automatically connect to the Aruba Activate cloud, which redirects to the customer’s AirWave management server to obtain its configuration.

As a result, Aruba Activate eliminates the need for onsite technical assistance and cuts the deployment time for Aruba Instant by up to 65%.

Aruba Instant benefits from the extensive set of capabilities provided by its operating system and application engine, known as the InstantOS. It includes many capabilities, such as Aruba’s Adaptive Radio Management™ (ARM), as well as optional software modules like the Aruba Policy Enforcement Firewall™ (PEF), and RFProtect™ wireless intrusion protection and spectrum analyzer.
In addition, AirWave gives IT centralized control with a comprehensive set of management tools that include real-time monitoring, customized reporting, network infrastructure configuration, location-based services, and compliance reporting.

A multivendor wired and wireless network management system, AirWave enables management of up to 100,000 devices from a single interface. By providing IT with network-wide views of the entire RF environment, the AirWave VisualRF™ software module further simplifies management and rogue location an Aruba Instant environment.

And to ensure customers can easily implement access control, the Aruba ClearPass Access Management System™ centralizes access policies across the entire wireless, wired and VPN infrastructure.

ClearPass automates differentiated user and device access, policy management, the provisioning of devices for secure network access, and posture assessment, giving customers unparalleled simplicity when managing and securing network access.

With Aruba Instant, customers ranging from small businesses to service providers get the enterprise-grade wireless functionality they need with minimum management overhead.

**THE ARUBA INSTANT PRODUCT FAMILY**

The Aruba Instant product family consists of a wide range of APs.
- The Instant AP-134 and Instant AP-135 maximize mobile device performance in extremely high-density Wi-Fi client environments.
- The Instant AP-104 and Instant AP-105 are best suited for moderately high-density Wi-Fi client environments.
- The Instant AP-92 and Instant AP-93 feature single radios and are ideal for optimizing mobile device performance in low-density Wi-Fi client environments.
- The Instant AP-175 is designed for outdoor areas, storage yards, warehouses, container and transportation facilities, industrial production areas and other harsh environments.
- The Instant RAP-100 Series of Remote Access Points deliver secure 802.11n wireless and wired networking to SMBs and access to corporate resources from branch and home offices.
- The Instant RAP-3 Remote Access Point provides secure wired and 802.11n wireless network access for branch offices and teleworker offices.

<table>
<thead>
<tr>
<th>Aruba Instant Model</th>
<th>Spatial Streams</th>
<th>Radios</th>
<th>Antennas</th>
<th>Throughput</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant AP-135</td>
<td>3x3 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>Internal</td>
<td>450 Mbps per radio</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant AP-134</td>
<td>3x3 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>External</td>
<td>450 Mbps per radio</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant AP-105</td>
<td>2x2 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>Internal</td>
<td>300 Mbps per radio</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant AP-104</td>
<td>2x2 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>External</td>
<td>300 Mbps per radio</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant AP-93</td>
<td>2x2 MIMO</td>
<td>One (2.4 or 5 GHz)</td>
<td>Internal</td>
<td>300 Mbps</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant AP-175</td>
<td>2x2 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>External</td>
<td>300 Mbps per radio</td>
<td>Outdoor</td>
</tr>
<tr>
<td>Instant RAP-108</td>
<td>2x2 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>External</td>
<td>300 Mbps per radio</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant RAP-109</td>
<td>2x2 MIMO</td>
<td>Two (2.4 and 5 GHz)</td>
<td>Internal</td>
<td>300 Mbps per radio</td>
<td>Indoor</td>
</tr>
<tr>
<td>Instant RAP-3</td>
<td>2x2 MIMO</td>
<td>One (2.4 GHz)</td>
<td>Internal</td>
<td>300 Mbps per radio</td>
<td>Indoor</td>
</tr>
</tbody>
</table>
ARUBA INSTANTOS

InstantOS includes all the high-end network services that are found in centralized controller-managed WLANs. At each distributed location, a dynamically-elected Instant AP provides services like dynamic RADIUS proxy, DHCP services and OpenDNS support.

Dynamic RADIUS proxy

With distributed authentication, network administrators typically have to configure each authenticator as a RADIUS client. With Aruba Instant, a dynamically-elected AP acts as a RADIUS proxy, which means the network administrator only has to configure one RADIUS client per site.

DHCP services

Aruba Instant provides DHCP services for clients in one of two ways:

- Through the onboard DHCP server in a dynamically-elected Instant AP, which automatically NATs user traffic out to the Internet.
- Through an external DHCP server, the dynamically-elected Instant AP provides IP Helper/DHCP Proxy functionality.

Best-in-class RF management

InstantOS features Aruba’s signature Adaptive Radio Management technology, which optimizes Wi-Fi client behavior and automatically ensures that Aruba Instant APs stay clear of RF interference.

Without disconnecting clients or disrupting applications, ARM™ automatically adjusts channel assignments on Instant APs. ARM is the only RF management technology that is certified to operate with voice-over-wireless traffic as it dynamically adapts RF scanning in the presence of latency-sensitive applications.

ARM ensures that Wi-Fi clients associate with the best channel, frequency and Instant AP, making it the most effective RF management technology available today. By enforcing the fair distribution of bandwidth to mobile devices, ARM makes certain that data, voice and video have sufficient network resources at all times.

ARM also works in conjunction with the Aruba RFProtect Spectrum Analyzer. While ARM optimizes client behavior and ensures that APs stay clear of interference, the RFProtect Spectrum Analyzer utilizes Aruba 802.11n APs to identify and classify Wi-Fi and non-Wi-Fi sources of interference.

ARM capabilities are highlighted in the table below.

<table>
<thead>
<tr>
<th>Adaptive Channel and Power Assignment</th>
<th>Instant APs scan all channels and make cooperative decisions for channel and power assignment per radio based on co-channel, adjacent channel and other channel utilization and noise, activity on neighboring Wi-Fi networks and other real-time parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordinated Access to a Single Channel</td>
<td>Adjacent Instant APs on the same channel can share the spectrum without increasing co-channel interference. This overcomes the challenges of dense AP deployments in the 2.4-GHz band that commonly occur in lecture halls, airport lounges, and conference centers.</td>
</tr>
<tr>
<td>Band Steering</td>
<td>Band steering detects dual-band Wi-Fi clients and steers them to the 5-GHz band where there’s more room, creating more capacity for clients that are limited to 2.4 GHz. This improves Wi-Fi client performance by more than 50%.</td>
</tr>
<tr>
<td>Airtime Fairness</td>
<td>Instant APs provide equal wireless access for all clients, regardless of Wi-Fi client type, capability or operating system.</td>
</tr>
<tr>
<td>Airtime Performance Protection</td>
<td>Airtime performance protection prevents clients – especially slower ones – from monopolizing network resources. Ensuring uniform Wi-Fi performance for all clients, 802.11n users experience faster network speeds even when older 802.11a/b/g clients are present.</td>
</tr>
<tr>
<td>Automatic Coverage-Hole Correction</td>
<td>Instant APs detect RF coverage holes and communicate these event so that neighboring Instant APs can increase transmit power. This takes place in seconds and is transparent to end users.</td>
</tr>
</tbody>
</table>
# RELIABILITY AND HIGH AVAILABILITY
Controllerless Aruba Instant is engineered to be resilient to failure, ensuring that users in distributed locations are always up and running and minimizing remote support issues for IT. Aruba Instant’s high-availability features are explained in the table below.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio Failover</strong></td>
<td>If an Instant AP fails for any reason, ARM ensures that the neighboring Instant APs automatically fill in the coverage hole.</td>
</tr>
<tr>
<td><strong>Uplink Failover</strong></td>
<td>Uplink options include wired Ethernet, Wi-Fi, cellular, point-to-point protocol over Ethernet (PPPoE), and mesh. If an uplink fails, failover and failback occur with no manual intervention.</td>
</tr>
<tr>
<td><strong>Hitless Instant AP Failover</strong></td>
<td>If the first dynamically-elected Instant AP fails, another on the same Layer 2 subnet takes over based on factors such as uplink availability and Instant AP model. Configuration and user-session state are synched automatically between all Instant APs on the network with no service disruption.</td>
</tr>
<tr>
<td><strong>Management Failover</strong></td>
<td>If AirWave is unreachable for any reason, the dynamically-elected Instant AP will failover to a backup AirWave platform, ensuring no loss of monitoring configuration or other management capabilities.</td>
</tr>
<tr>
<td><strong>Authentication Server Failover</strong></td>
<td>If the RADIUS server that wireless clients authenticated against become unreachable due to a server or network failure, Aruba Instant can failover authentication to a back-up RADIUS server.</td>
</tr>
<tr>
<td><strong>Data Center Reachability</strong></td>
<td>With ClearPass Policy Manager, Aruba Instant saves a secure hashed version of each local authenticated user. If WAN connectivity is lost, users can still connect to the Aruba Instant network and access local resources.</td>
</tr>
</tbody>
</table>

# STRONG GOVERNMENT-GRADE SECURITY
Aruba Instant provides comprehensive security at all levels – device, user and data – and delivers strong government-grade protection throughout distributed enterprise networks.

**Guest authentication**
Aruba Instant provides a captive portal that can authenticate guests against an internal database or an external authentication engine. In addition, Aruba Instant eliminates the need to set up a guest VLAN by automatically creating a subnetwork to act as a DMZ that isolates the internal network from external networks and the Internet.

**BYOD authentication**
Customers need the ability to control the devices that connect to Aruba Instant WLANs. Aruba’s ClearPass Onboard feature allows users, including both guests and employees, to self-register with certificate-based authentication schemes.

![ClearPass Policy Manager](image)

ClearPass simplifies security for BYOD by centrally managing authentication, role-based access, posture checks, policy enforcement and device profiling.
Role-based access control
Aruba pioneered support for role-based access control, recognizing that users often have multiple devices, multiple applications, multiple network destinations and multiple SLAs. Role-based access allows Aruba Instant WLANs to provide a user the same experience regardless of what device and what network they use to come onboard.

Traffic separation
Aruba Instant supports up to six SSIDs per subnet, which gives enterprise organizations the flexibility to separate WLAN traffic based on user role and traffic type. For example, voice and video traffic can be assigned to a specific SSID and given high-priority handling.

Wireless intrusion protection
Aruba Instant includes a wireless intrusion detection system that safeguards the network from unauthorized or rogue APs and clients, and other devices that can potentially harm network operations.

RFProtect Wireless Intrusion Protection safeguards Aruba Instant WLANs against attacks by integrating threat protection capabilities into the network infrastructure. This integrated approach also eliminates the need for separate RF sensors and security appliances.

In addition to integrated wireless intrusion protection, RFProtect provides automatic threat mitigation, customizable security policies and automated compliance reporting to reduce the complexity and time needed to meet PCI compliance.

The addition of AirWave RAPIDS™ automatically detects and locates unauthorized clients and APs, and utilizes a set of rules to highlight the most important threats to your organization. With RAPIDS, Instant APs scan the RF environment for unauthorized devices.

RAPIDS also enables Instant APs to scan the wired network to determine if the wirelessly detected rogues are physically connected to the local network, as well as look for additional unauthorized devices in areas without wireless coverage.

```
<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Last 2 Hours</th>
<th>Last 24 Hours</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Implantation</td>
<td>0</td>
<td>19</td>
<td>88</td>
</tr>
<tr>
<td>Denial-of-Service Attack (DoS)</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Disconnect Station Attack (Station)</td>
<td>55</td>
<td>123</td>
<td>1825</td>
</tr>
<tr>
<td>Disconnect Station Attack (Station)</td>
<td>2</td>
<td>11</td>
<td>29</td>
</tr>
<tr>
<td>R0 Probe Response</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Station Associated to Rogue AP</td>
<td>71</td>
<td>1118</td>
<td>2927</td>
</tr>
<tr>
<td>Station Unassociated from Rogue AP</td>
<td>74</td>
<td>1156</td>
<td>2636</td>
</tr>
<tr>
<td>7 Attack Types</td>
<td>202</td>
<td>3114</td>
<td>7629</td>
</tr>
</tbody>
</table>

**Summary**
IDS Events for devices in folder Top and subfolders

**Rogue Data**
Device Count by RAPIDS Classification

**Working with Aruba Instant APs, AirWave RAPIDS identifies all wireless intrusion attempts and classifies rogue devices.**
RAPIDS logs information about unauthorized APs and clients, and generates reports, making Aruba Instant fully PCI compliant. Instead of manually handling each PCI requirement – a task that can involve hundreds of steps – the custom report generator has check boxes for each section of PCI. Simply check the relevant sections to produce a custom PCI compliance report.

**IPsec tunneling**

To support centralized authentication, transfer of payment card information or other datacenter applications between a remote site and a data center over a WAN, Aruba Instant can ensure end-to-end security by creating an IPsec VPN tunnel to a Mobility Controller in the data center.

**Per-user firewall**

The Aruba Instant integrated firewall monitors all data entering or leaving the network, inspects traffic from each user session, and allows or denies it according to specified role-based security policies.

The firewall blocks unauthorized data, prevents unauthorized users from accessing the enterprise network, and supports actions such as blacklisting and DSCP tagging and prioritization.

Administrators use a simple firewall policy language to define access rules, which can be applied to an SSID or WLAN, such as the guest or employee network. Users are subject to access rules defined for the SSID to which they connect.

The firewall also limits packets and controls bandwidth for different classes of users, such as students and guests.

**With integrated OpenDNS**

OpenDNS is fully integrated with controllerless Aruba Instant WLANs to ensure Internet-wide security. Simply enter your OpenDNS credentials in the Aruba Instant interface and every device that connects is protected. OpenDNS identifies all Aruba Instant APs as a cluster so there’s no need to enter IP addresses or configure network settings and Internet connection settings.

With cloud-based OpenDNS services, Aruba Instant APs deliver integrated web filtering, malware and botnet protection to every mobile device that connects to the WLAN and without requiring any software. Aruba and OpenDNS provide a wide range of content filtering capabilities:

- Filter up to 56 web categories – including adult, proxy, peer-to-peer and social networking – and custom domain lists.
- Prevent access to servers that host and distribute malware.
- Block botnet command and control points to mitigate data leaks from infected devices.
- Create bypass codes that allow select users to access blocked sites.
- Report on blocking and overall usage with optional daily emails.
- Connect to the global OpenDNS cloud-based service with zero downtime or added latency.
To boost performance, Aruba Instant APs store responses from the OpenDNS platform and search cache memory when an access request is received. When a suitable record is found, Aruba Instant APs accelerate the response by eliminating the need to contact the OpenDNS platform again.

### AAA Server Support and Survivability

Aruba Instant’s internal database supports 802.1X or MAC authentication using either an enterprise SSID or a captive-portal guest SSID. Aruba Instant supports over-the-air authentication using pre-shared keys or 802.1X, which uses WPA2 for strong security and an internal or external RADIUS server.

Each Aruba Instant AP has an instance of a free RADIUS server that maintains a distributed user database. When using internal RADIUS for 802.1X authentication, customers can load certificates and terminate EAP-PEAP, EAP-TTLS and LEAP.

Alternately, Aruba Instant can seamlessly integrate with an external RADIUS server. Leveraging the dynamic RADIUS proxy capabilities of the dynamically-elected Instant AP, an entire Instant network can be presented to the authentication back end.

If that AP fails, the Instant RADIUS proxy ensures that the RADIUS client identity remains the same, eliminating the need to modify the authentication back end. Customers can optionally configure Aruba Instant APs as RADIUS clients for distributed authentication.

### Application Optimization

Controllerless Aruba Instant features application optimizations to enhance service for all classes of applications, including a variety of real-time applications.

#### Application Fingerprinting and Voice Awareness

Aruba’s built-in application fingerprinting capability identifies encrypted traffic flows and prioritizes critical applications in real-time to ensure the highest user experience.

It also has a number of capabilities that help identify voice traffic and give it the handling it needs automatically, without user or administrator intervention. For instance, Aruba PEF™ inspects the signaling exchange and analyzes packet flows to detect, tag and prioritize important voice and video-conferencing applications.

As noted earlier, ARM recognizes when an active call is in progress and suspends any disruptive RF-layer activities or changes. In addition, Aruba’s media classification capability uses known patterns to identify, tag and prioritize VoIP over the Internet, even when the SIP exchange is encrypted. This is particularly useful for applications such as Microsoft Lync and Apple FaceTime.

Aruba Instant also includes a special setting to create a voice SSID, which automatically configures the proper SIP application-layer gateways in the firewall policy and sets the highest quality-of-service parameter.

#### Multicast Video Optimization

Multicast streaming video places a huge strain on Wi-Fi networks. With its Dynamic Multicast Optimization, Aruba Instant goes beyond tagging and forwarding video traffic to intelligently identify video requests and convert multicast traffic to unicast traffic destined to just those clients subscribed to a given feed.

Both video and non-video clients benefit from higher performance, and the network is better able to deliver different video streams to different clients.

#### Operating System Fingerprinting

Laptops, tablets and smartphones place different demands on a network. Aruba’s operating system fingerprinting capability gives customers information about the mix of devices and applications accessing the network so IT can characterize their loads accurately for better network provisioning and planning.

#### Apple Bonjour Support

Aruba’s AirGroup functionality lets network administrator limit Bonjour traffic to a per-user group of devices on the fly, without requiring any additional network configuration.

A component of Aruba ClearPass Policy Manager and InstantOS, AirGroup identifies users’ individual roles and their locations and makes network services such as Apple’s AirPrint and AirPlay available to users’ mobile devices.

With AirGroup, end users and IT administrators can self-register printers, Apple TVs, Wi-Fi projectors, Wi-Fi televisions and other consumer devices, which can then be grouped into personal, shared and location-based service groups.
EASY TO DEPLOY, CONFIGURE AND GROW
Because it is controllerless, Aruba Instant makes it easy for distributed enterprises and service providers to grow their WLAN infrastructure as business needs change. Features include:

Zero-touch provisioning
Using Aruba Activate, Instant APs can be factory-shipped to any office worldwide, plugged in, and will automatically download the appropriate configuration. In addition to zero-touch provisioning, Aruba Activate automates inventory management and firmware upgrades.

By enabling Instant APs to be configured automatically and managed centrally, Aruba Instant enables customers to deploy autonomous WLANs rapidly at numerous sites at a very low total cost of ownership – and without any tradeoff in feature richness.

Scalability
The Aruba Instant architecture does not limit the size of a network. A network administrator can expand coverage by simply adding more Instant APs to the wired Layer 2 network; combine contiguous networks by enabling Layer 3 mobility between them; even replicate a network design across multiple sites using AirWave groups and template-based configuration.

These capabilities allow Aruba Instant WLANs to grow organically with minimal changes to the underlying network infrastructure. And users can roam freely across subnet boundaries without any impact on Wi-Fi performance.

Flexible deployment options
No two customer sites are identical, which is why Aruba Instant provides a variety of deployment options – including single AP or multi-AP, desk-mount or ceiling mount, indoor or outdoor, and wired or wireless uplink – while delivering a uniform configuration and user-experience.

Effortless expansion and migration
Because Aruba Instant APs are self-organizing and auto-configure, IT can add Instant APs indoors or outdoors and easily expand an existing Wi-Fi deployment. With AirWave management, IT can centrally control Aruba Instant WLANs across dozens, even hundreds, of locations.

Customers can decide at any time to move their Instant APs to a controller-managed architecture for centralized network configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding. Instant APs easily convert to Aruba controller-managed APs in a single step.

MANAGEMENT THROUGH A SINGLE PANE OF GLASS
The lack of IT resources at remote locations creates a management challenge for many organizations looking to deploy WLANs. Aruba AirWave addresses this challenge by providing IT a single view of their entire wireless and wired infrastructure and the ability to manage it centrally, which saves money, streamlines operations and improves service quality for users.

Likewise, AirWave is a highly scalable network management system that benefits service providers, offering a single point of monitoring and configuration that enables providers to quickly and easily roll out new sites, customize alerts and triggers, and have multiple levels of users from helpdesk assistant to network architect with different levels of access.

Aruba Instant eliminates the need to configure and troubleshoot individual APs or dispatch IT personnel onsite. From a remote location, IT can centrally configure, monitor, and troubleshoot Aruba Instant WLANs, upload new software images, track devices, generate reports, and perform other vital management tasks.

Offering end-to-end visibility and centralized control, AirWave identifies users, where they access the network, the mobile devices they use, and how much bandwidth they consume.
AirWave also features an easy-to-use web interface that provides customized views of data for the entire IT team, including the service desk, network operations center and network engineering staff.

Connecting to AirWave from an Aruba Instant WLAN is easy. From the Aruba Instant user interface, a system administrator simply clicks a link and enters the required parameters, which sets up a secure connection between a dynamically-elected Instant AP and the central AirWave server.

AirWave’s centralized management and operations capabilities include:

- Device configuration and firmware distribution, including group and template-based configuration to bulk-configure devices and networks, and push the template to all deployments simultaneously. This is especially useful to service providers that deploy hundreds of locations in a short period.
- Single-point network monitoring that automatically tracks every wireless user and device.
- Customizable triggers and alerts based on user, device, network element, security, and platform events; notification options include AirWave screen alerts to email and SMS.
- Troubleshooting, including root-cause analysis and event correlation across the entire wired and wireless infrastructure.
- Centralized RF visualization with AirWave VisualRF, which helps in accurate, ongoing RF planning by enabling a network administrator to upload floor-plans, place Instant APs and observe real-time heat maps. It also pinpoints the location of rogue devices.
- Version management, whereby AirWave can host multiple versions of Aruba Instant firmware and assist in phased upgrades of the network, as well as manage WLANs in which different parts of the network are running different versions of code.
- Automated compliance reporting and auditing.
- Historical trend reporting using up to a year’s worth of data, including network and performance data, configuration changes, device inventories, rogue devices, user session histories and roaming patterns.

The VisualRF heat map shows the strength of the RF coverage in each Instant AP location.

AirWave offers granular network views, ranging from the overall health of a network down to device-level application use. Consequently, the IT staff can monitor a user’s laptop that might be experiencing connectivity issues. Similarly, IT can see the breakdown of desktop and laptop computers, smart phones, MP3 players, and other devices on an Aruba Instant WLAN.

CLEARPASS GUEST

ClearPass Guest, a key component of the Aruba ClearPass Access Management System™, is a scalable, easy-to-use visitor management solution that enables Aruba Instant WLANs to deliver secure network access to guests, employees and their mobile devices.

The intuitive user interface of ClearPass Guest greatly simplifies visitor management by streamlining workflow processes, allowing receptionists, employees and other non-IT staff to create temporary accounts for Wi-Fi access.
ClearPass Guest works with InstantOS to provide consistent access policies for guests, temporary workers or other transient employees across multiple controllerless Aruba Instant networks.

In addition, guests and employees with mobile devices can also self-register for network access. Once registered, ClearPass Guest delivers account login credentials to users via SMS text message or email. Accounts can be set to expire automatically after a specific number of hours or days. Key features of ClearPass guest include:

- Create and modify temporary user accounts; delete or set accounts to automatically expire.
- Scales to support thousands of concurrent users with minimal IT involvement.
- Unique username and password per user.
- Guests and employees can register for access through a customizable web interface.
- Deliver guest account credentials via SMS or email to simplify registration.
- Skin technology provides a customized, branded user experience.

**ENTERPRISE-CLASS WI-FI IN AN INSTANT**

Aruba Instant is the only controllerless WLAN solution to combine high-end enterprise Wi-Fi capabilities with affordability and unmatched configuration simplicity. It requires no ongoing service fees, no additional license fees, no management appliances, no virtual controllers and no physical controllers.

Through an intuitive user interface and simple over-the-air provisioning, any non-technical, non-IT person can deploy an Aruba Instant network with multiple APs in matter of minutes – without compromising security or ease of use.

Alternatively, the cloud-based Aruba Activate feature cuts Aruba Instant deployment time in half by performing zero-touch provisioning and automating firmware upgrades and inventory management. With Aruba Activate, Instant APs are factory-shipped to remote deployment sites and configure themselves when powered up.

Offering impressive scalability, Aruba Instant can be deployed at a single site or at multiple geographic locations. And as mobility requirements grow, a built-in migration path allows Aruba Instant to become part of a centralized controller-managed architecture.

Combined with AirWave, Aruba Instant makes it easy for enterprise organizations to centrally manage Aruba Instant WLANs as well as multivendor wired network infrastructures across multiple locations, while ensuring PCI compliance and support for other regulatory standards.

Controllerless Aruba Instant eliminates the tradeoffs between usability, affordability and enterprise-grade WLAN capabilities make it an ideal choice for organizations and service providers of all sizes.