ARUBA INSTANT

Combining enterprise-class Wi-Fi
with unmatched affordability
and configuration simplicity

Table of Contents

Introduction 3
Aruba Instant Overview 4
Aruba Instant APs 4
Adaptive Radio Management™ 6
Aruba Instant Security 7
Virtual Controller Technology 6
Authentication and Encryption 7
Integrated Firewall 8
Traffic Separation 8
Wireless Intrusion Protection 9
Content Filtering 9
Operating System Fingerprinting 9
Aruba Integration with Aruba Services 10
Management with AirWave™ 10
ClearPass Guest 11
VisualRF™ 12
Get Instant Wi-Fi with Aruba Instant 13
About Aruba Networks 14

Introduction

For enterprise organizations with distributed locations, such as retail chains and K-12 school districts, providing wireless connectivity at remote sites has been a challenge.

Faced with a choice between cheap, consumer-grade Wi-Fi gear and feature-rich but costly high-end wireless LAN (WLAN) equipment, many lean-running enterprises have had to tradeoff between affordability, ease of use, and functionality – or do without wireless altogether.

But continued growth in BYOD and mobile devices is driving the need for enterprise-class WLANs, and there's no stopping it. Market analysts at Forrester predict that in 2016, one billion consumers will use smartphones and 350 million of those will be used for work.

The challenge for IT organizations is to find a robust enterprise-class WLAN that is affordable in terms of the capital expense and operational overhead. And while many enterprises are staffed with savvy IT professionals at headquarters, they have limited resources and RF expertise at remote locations.

Consequently, enterprise organizations need a mobility solution that's simple to set up, highly reliable, and can be managed centrally. But they also need enterprise-grade WLAN functionality.

For example, hotel operators, restaurant owners, and retailers must comply with data privacy regulations such as the Payment Card Industry (PCI) Data Security Standard. These and other distributed organizations need a feature-rich WLAN that meets a variety of challenges:

- Provides sophisticated security that protects internal assets, blocks malware, supports guest access, and isolates sensitive traffic from the rest of the networks.
- Offers high performance to accommodate a range of device and traffic types, including data, voice, and video.
- Scales easily, both within a given site and across sites.
- Allows users to roam without logging in each time they move from one access point (AP) to another.

Aruba Instant uses innovative Virtual Controller technology to deliver enterprise-grade WLAN capabilities — including robust security, performance, and scalability.

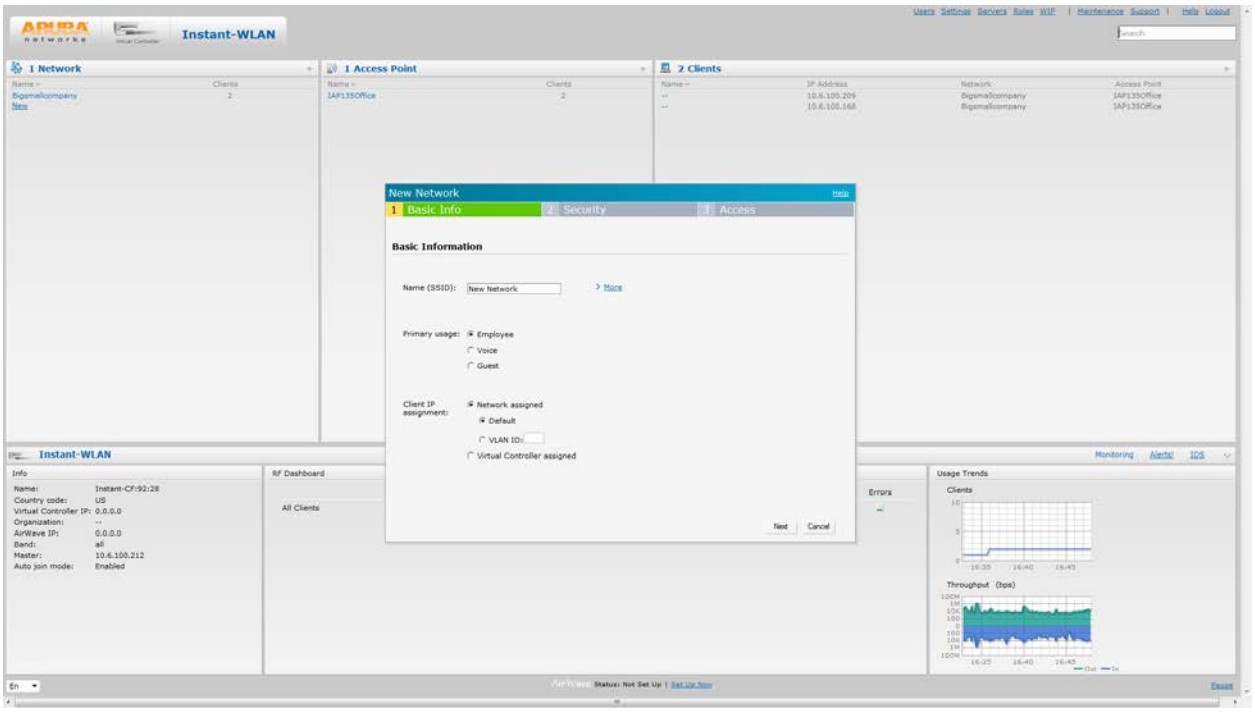
Designed for ease of use, Aruba Instant can be set up in minutes with minimal IT assistance and managed centrally through Aruba AirWave. With Aruba Instant, enterprises organizations can deploy autonomous WLANs at numerous sites without any tradeoff between feature richness, affordability and ease of use.

Aruba Instant Overview

The Aruba Instant WLAN is comprised of multiple 802.11n APs – which offer greater speed, coverage and reliability than legacy Wi-Fi – plus Virtual Controller technology. It is easily deployed as an overlay to an existing wired LAN in just a few minutes, eliminating the need for IT to redesign or modify the wired infrastructure.

Aruba Instant APs
Aruba Instant does not require IT expertise at distributed locations. All it takes to get an Aruba Instant WLAN up and running is to configure one Aruba Instant AP over the air using a simple wizard-driven process.

Offering over-the-air provisioning, there's no need to modify an IP address to configure Aruba Instant. Just power up and connect an Aruba Instant AP to the LAN, and open a PC browser to automatically access the Aruba Instant user interface login page.



The intuitive web-based setup wizard makes it easy to get Aruba Instant up and running.

From this web-based interface, the user can assign SSIDs, and select authentication mechanisms. The entire set up takes less than five minutes.

To configure additional Aruba Instant APs, simply connect and power them up. The first configured AP automatically becomes a primary Aruba Instant Virtual Controller and configures all the other APs.

Aruba Instant is a fully distributed architecture. In the event of a primary Virtual Controller failure, another Aruba Instant AP automatically takes on the role with no disruption. The primary Virtual Controller operates like any other Aruba Instant AP with full WLAN functionality.

The Aruba Instant product family consists of seven different APs – IAP-134, IAP-135, IAP-104, IAP-105, IAP-92, IAP-93 and the outdoor IAP-175.

The Aruba Instant product family.

The IAP-134 and IAP-135 maximize mobile device performance in the most extreme high-density Wi-Fi client environments, while the IAP-104 and IAP-105 are best suited for moderate high-density environments. The single-radio IAP-92 and IAP-93 are ideal for optimizing mobile device performance in low-density client environments.

The case-hardened IAP-175 is designed for outdoor high-density campuses, container and transportation facilities, and harsh industrial production areas. It features two 2x2 dual-band 2.4- and 5-GHz radios with quad antenna interfaces.

Multiple Aruba Instant APs can be configured per Layer 2 subnet, or Virtual Controller group, and enterprises can have as many subnets or Virtual Controller systems as needed on a campus or in a building.

Aruba Instant Model	Spatial Streams	Radios	Antennas	Throughput	Type
IAP-135	3x3 MIMO	Two (2.4 and 5 GHz)	Internal	450 Mbps per radio	Indoor
IAP-134	3x3 MIMO	Two (2.4 and 5 GHz)	External	450 Mbps per radio	Indoor
IAP-105	2x2 MIMO	Two (2.4 and 5 GHz)	Internal	300 Mbps per radio	Indoor
IAP-104	2x2 MIMO	Two (2.4 and 5 GHz)	External	300 Mbps per radio	Indoor
IAP-93	2x2 MIMO	One (2.4 or 5 GHz)	Internal	300 Mbps	Indoor
IAP-92	2x2 MIMO	One (2.4 or 5 GHz)	External	300 Mbps	Indoor
IAP-175	2x2 MIMO	Two (2.4 and 5 GHz)	External	300 Mbps per radio	Outdoor

Adaptive Radio Management™

Aruba's signature Adaptive Radio Management (ARM) technology automatically manages the WLAN's 2.4-GHz and 5-GHz radio bands to optimize Wi-Fi client performance and mitigate RF interference. It also ensures that each Aruba Instant AP uses the optimal channel- and transmit-power for its RF environment.

ARM™ additionally offers priority traffic handling, channel load-balancing, band steering, airtime fairness and other quality-of-service (QoS) controls to ensure that the available Wi-Fi bandwidth is fairly distributed to all mobile devices on the WLAN.

Too often, newer 5-GHz-capable devices, such as notebook PCs, connect at 2.4 GHz to a dual-band network, even though it is the most crowded, interference-prone band.

To rectify this, the ARM technology in Aruba Instant steers 5-GHz-capable clients to that band, giving them clear conditions, while clients limited to 2.4 GHz – such as bar code readers, Wi-Fi phones and older PCs – gain capacity as that band becomes less crowded.

ARM also offers automatic application-detection capabilities, which enable it to distinguish voice and video from data traffic so that appropriate QoS mechanisms can be applied to ensure that latency-sensitive applications have sufficient network resources at all times.

Virtual Controller Technology

The Aruba Instant Virtual Controller technology provides security, consistently high performance, scalability, and other enterprise-class network access services without requiring a dedicated controller.

Utilizing an adaptive, self-organizing wireless grouping, the Virtual Controller technology supports multiple Aruba Instant APs across wired LANs and over the air through the mesh, enabling the WLAN to scale effortlessly.

As with Mobility Controllers, Aruba Virtual Controller technology centralizes the functionality needed to configure and manage the Aruba Instant network. Aruba Virtual Controller technology delivers a wide range of enterprise-class WLAN capabilities required by enterprises that have multiple remote locations:

- **Reliability** – Aruba Instant is resilient to failure. If an Aruba Instant AP functioning as the primary Virtual Controller fails, another Aruba Instant AP automatically inherits the role of the primary Virtual Controller with no service disruption.
- **Mobility** – Users on Aruba Instant WLANs can roam campus-wide within the same Layer 2 domain in a Virtual Controller and across multiple Virtual Controllers. This is enabled by firewall and authentication-state synchronization across all Aruba Instant APs, as well as coordination of DHCP address allocation for NAT clients.
- **Guest access** – Aruba Instant provides automatic security classification for guests, eliminating the need to set up a guest VLAN. It automatically sets up a subnetwork to act as a DMZ that isolates the internal network from external networks and the Internet.
- **Scalability** – Offering self-organization and auto-configuration, adding Aruba Instant APs through a mesh or expanding to the outdoors is easy. At the same time, AirWave management lets IT centrally control thousands of Aruba Instant WLANs across multiple locations.
- **Cloud-based firmware server** – Aruba Instant receives firmware updates through the cloud server without the need for manual or laborious firmware updates. When a new image is available, the Aruba Instant user interface will indicate that an update is available.
- **Built-in migration path** – Aruba Instant offers a built-in migration path for organizations that want to transition to a centralized controller-based architecture. Aruba Instant APs easily convert to high-performance 802.11n campus APs that are managed by a central Aruba Mobility Controller.

Aruba Instant Security

Authentication and Encryption

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 database of up to 256 users. When using internal RADIUS for 802.1X authentication, customers can load certificates and terminate EAP-PEAP, EAP-TTLS and LEAP.

Organizations that use external RADIUS can use the Aruba Instant with a dynamic RADIUS proxy that leverages Virtual Controller technology to present the entire Aruba Instant network to the

authentication back end. Aruba Instant RADIUS proxy ensures that the RADIUS client identity remains the same if a Virtual Controller fails, eliminating the need to modify the authentication back end.

Alternately, enterprise organizations with remote sites can configure each Aruba Instant AP as a RADIUS client so they can perform distributed RADIUS authentication without going through the Virtual Controller.

For authentication on a guest network, Aruba Instant provides a captive portal, which can authenticate guests against an internal database or an external authentication engine. In addition to authentication, Aruba Instant supports standard TKIP and AES as methods of encryption for wireless traffic.

Integrated Firewall

The Aruba Instant integrated firewall inspects traffic from each user session and allows or denies that traffic before it traverses the wired and wireless network. The firewall monitors all data entering or leaving the network, blocks data that does not satisfy specified security policies, and prevents unauthorized users from accessing the enterprise network.

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.

Traffic Separation

Aruba Instant supports up to six SSIDs per Virtual Controller, which gives enterprise organizations the flexibility to separate WLAN traffic based on user role and traffic type. For example, school district employees can be assigned to one SSID, students to another, and guests to a third.

Similarly, voice and video traffic can be assigned to a specific SSID and given high-priority handling. Setting up multiple SSIDs is easy by following the wizard-driven steps in the Aruba Instant user interface.

To further simply configurations, Aruba Instant includes a special setting to create a voice SSID. This voice SSID automatically establishes the proper SIP application-layer gateways (ALGs) in the firewall policy and sets the highest QoS parameter.

In traditional wireless environments, an SSID is associated with a VLAN. However, Aruba Instant gives operators the option to associate an SSID with a user group, traffic type, or a VLAN. Specifying VLANs on the WLAN automatically enables the required trunking and tagging for the wired network.

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

The wireless intrusion protection capability also logs information about unauthorized APs and clients, and generates reports, making Aruba Instant fully PCI compliant. To prevent malicious APs from associating with network, administrators can turn on rogue AP prevention and disable the auto-join function, which ensures that only authorized Aruba Instant APs are allowed to connect.

Content Filtering
With an OpenDNS service subscription, Aruba Instant delivers integrated web filtering, malware and botnet protection to every device connected to the WLAN.

With content filtering, administrators can create Internet access policies that allow or deny user access to web sites based on categories and security ratings. Content filtering also prevents known malware hosts from accessing the WLAN, reduces bandwidth consumption and improves employee productivity by limiting access to certain web sites.

- Filter up to 55 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.

For optimum performance, Aruba Instant APs store responses from the OpenDNS servers, and search cache memory when they receive an access request. If a suitable record is found, the Aruba Instant AP responds accordingly, accelerating the response by eliminating the need to contact the DNS server again.

Operating System Fingerprinting
The OS fingerprinting feature gathers information about each client connected to an Aruba Instant WLAN to determine what OS the client is running. This information enables IT to identify rogue clients, including clients running an OS not allowed on the company network, as well as clients with an outdated OS.

OS fingerprinting also helps IT locate and patch clients with specific OS versions that have known vulnerabilities to fortify enterprise network security.

Aruba Instant Integration with Aruba Services

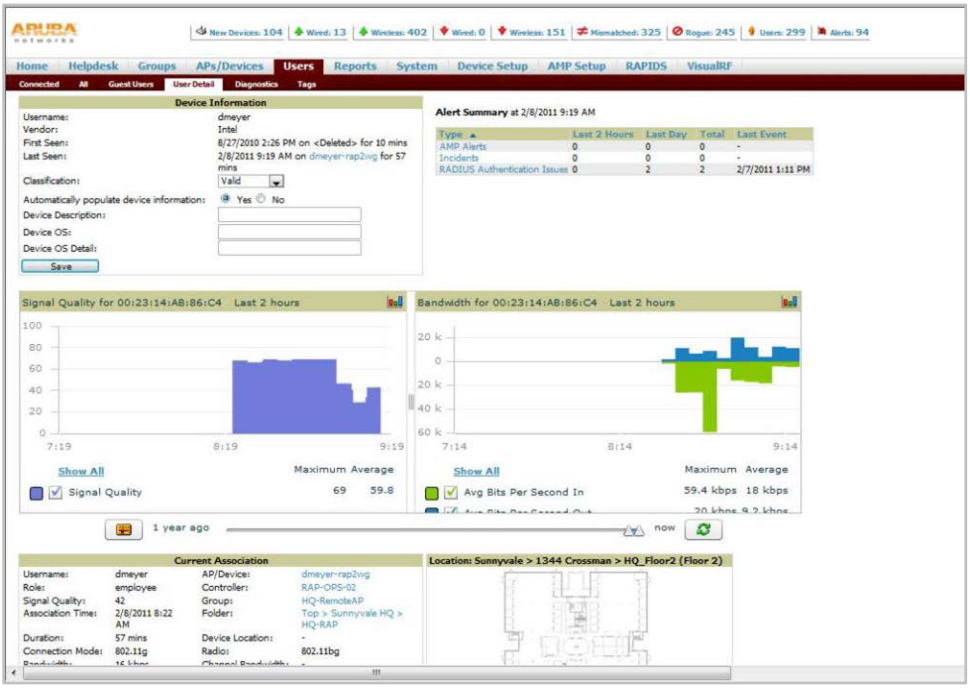
Management with AirWave™

The lack of IT resources at remote locations creates a management challenge for many organizations that wish to deploy WLANs. Aruba AirWave addresses this challenge by allowing enterprise organizations to easily manage WLANs at multiple sites from a central location.

With AirWave, enterprise organizations have a single view of their entire wireless and wired infrastructure and manage it centrally, which saves money, streamlines operations and improves service quality for users.

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 the Virtual Controller and the central AirWave server.

Unlike other WLAN management products, 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. Centralized management and operations capabilities include:

- Device configuration and firmware distribution.
- Network monitoring that automatically tracks every wireless user and device.
- Troubleshooting, including root-cause analysis and event correlation across the entire wired and wireless infrastructure.
- 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.

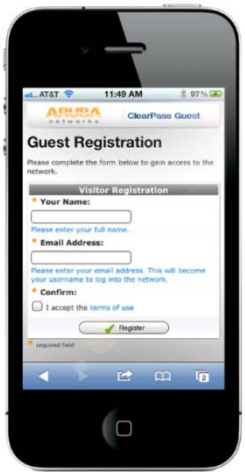
AirWave offers granular network views, ranging from the overall health of a network down to device-level application use. Consequently, the IT staff can monitor a user's laptop that might be experiencing connectivity issues. Similarly, IT can see the breakdown of desktop and laptop computers, smartphones, 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 delivers secure wireless 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 can be combined with Aruba Instant to provide consistent access policies for guests, temporary workers or other transient employees across multiple Aruba Instant Virtual Controller networks.



Guests and employees can self-register for Wi-Fi access through a customizable web interface.

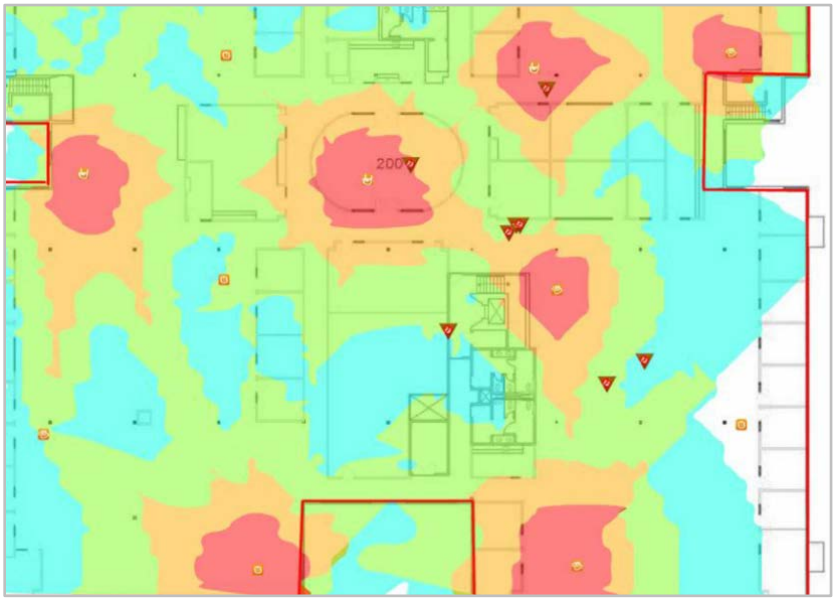
In addition, guests and employees with mobile devices can also self-register for network access. Once registered, ClearPass Guest delivers account login credentials to users via SMS text message or email. Accounts can be set to expire automatically after a specific number of hours or days. Key features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

VisualRF™

In addition, the AirWave VisualRF feature automatically generates a map of each site's RF environment and the underlying wired topology, showing in real time who is on the network, where they are and how the network is performing.

VisualRF builds this map using RF measurements gathered from active Aruba Instant APs and the primary Virtual Controller, eliminating the need for costly, separate location appliances. This comprehensive RF coverage and location data enables IT to solve problems faster, improve service quality and make well-informed planning decisions.



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

Get Instant Wi-Fi with Aruba Instant

Aruba Instant is the only wireless networking solution to combine high-end enterprise WLAN capabilities with affordability and unmatched configuration simplicity. It requires no ongoing service fees, no additional license fees, no management appliances and no external controller.

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 sacrificing strong enterprise-grade security or ease of use.

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-based 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.

Aruba Instant eliminates the tradeoffs between usability, affordability and enterprise-grade WLAN capabilities.