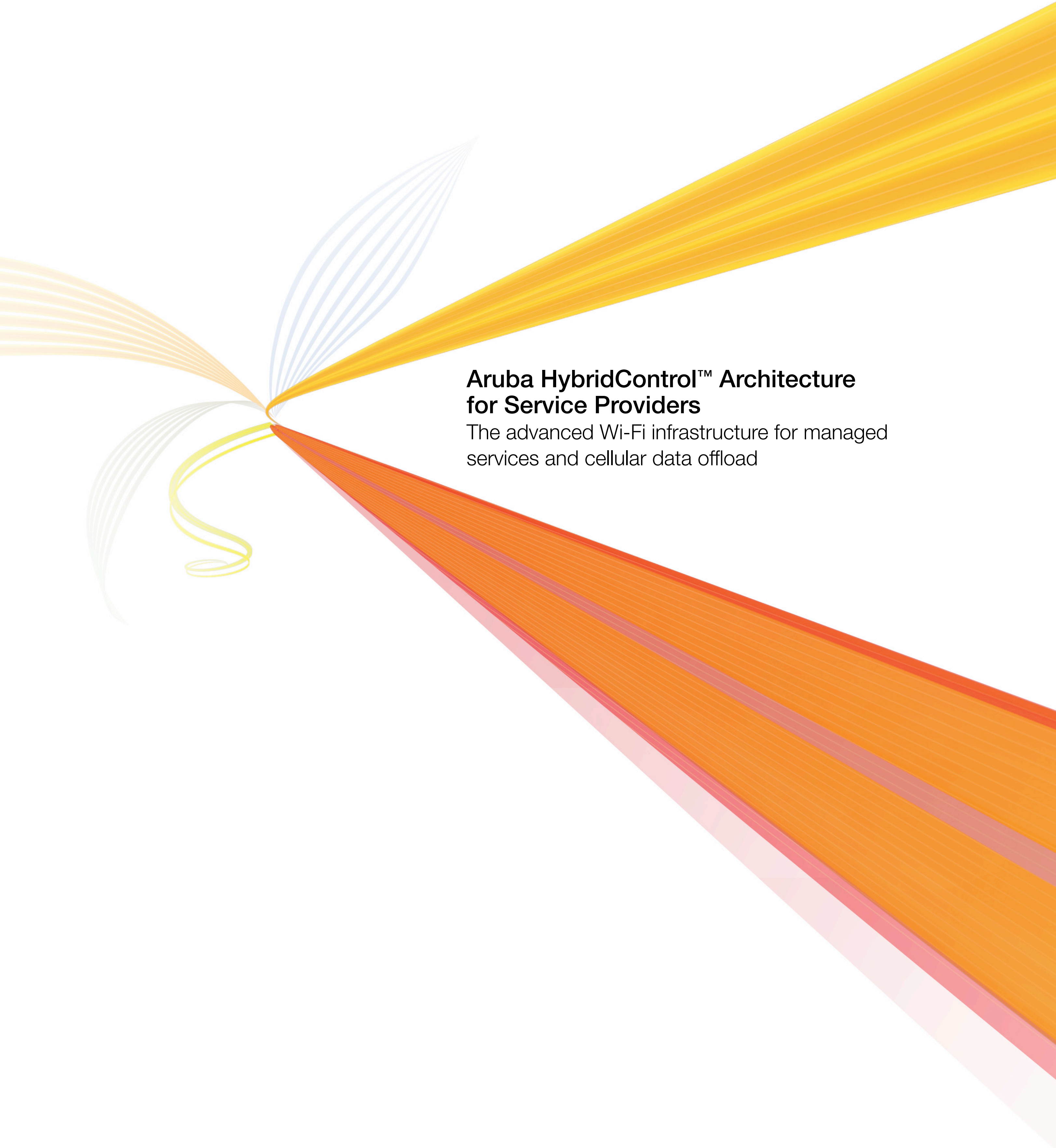


Aruba HybridControl™ Architecture for Service Providers

The advanced Wi-Fi infrastructure for managed services and cellular data offload

ARUBA networks

Table of Contents

Introduction 3

Wi-Fi requirements for cellular offload and managed services 3

Aruba HybridControl Wi-Fi architecture 4

Aruba AppRF 6

Zero-touch provisioning with Aruba Activate 7

Context aggregation and value-added services 7

Policy management and guest access 8

Wi-Fi and cellular network integration 9

Reuse of core authentication 10

Tunnel to a Wi-Fi gateway for seamless mobility 10

Summary 11

About Aruba Networks, Inc. 12

Introduction

The new public Wi-Fi infrastructure is more than just a free hotspot. Driven by bring-your-own-device (BYOD) initiatives, Wi-Fi deployments require massive scalability, intelligent hybrid offloading and managed WLAN and network access services for enterprise customers.

In addition to exceptional reliability and strong security and threat protection, this infrastructure must offer value-added services like analytics, location-based advertising and security to enable monetization by service providers.

The new Aruba HybridControl™ architecture from Aruba Networks® addresses critical cellular offload and managed services requirements for service providers – scale, security, robust RF performance, reduced operational costs, control and visibility, and integration with the core for unified policy management.

With Aruba HybridControl, massive scale is achieved and Layer 4-7 context awareness is applied to optimize the air and deliver application-centric security, visibility and control for business-critical traffic.

Wi-Fi requirements for cellular offload and managed services

The increasing use of Wi-Fi-enabled mobile devices and exponential growth in data consumption is placing an enormous strain on today's cellular networks.

As operators scramble to quickly integrate Wi-Fi to support additional capacity and deliver value-added services, there are several key WLAN infrastructure requirements:

- The Wi-Fi infrastructure must scale from thousands of small hotspots to accommodate ultra-high-density stadiums and other large public venues.
- Guarantee consistent and reliable voice, video and application performance.
- Ensure end-to-end security, including defensive and offensive mechanisms, against wireless intrusions and other threats.
- Seamlessly and intelligently transition select traffic from the cellular network to Wi-Fi.
- Securely deliver a wide range of premium content and value-added services to customers.
- Integrate and interoperate with the operator core network and policy management framework.

Large and small enterprises are considering managed services as a way to scale their Wi-Fi networks to support the influx of mobile users and devices. Key requirements for effective managed services include:

- Scale to support a large number of distributed sites, devices and users.
- Reliable voice, video and application performance.
- Differentiated access by user, device, application and location.
- Reduce deployment and management costs.
- Distribute value-added enterprise services to users across Wi-Fi networks.
- Integrate with operations and business support management systems.

Seizing the opportunity, service providers can leverage their Wi-Fi offloading investment to deliver managed services that create monetization opportunities.

There is considerable overlap between high-performance managed services networks and today's public Wi-Fi networks. Demands and expectations are the same for each and the Aruba HybridControl architecture uniquely addresses their requirements.

Aruba HybridControl Wi-Fi architecture

The Aruba HybridControl architecture lets service providers employ policies to offload data from the cellular network and rollout managed services to over 32,000 sites while offering 40-times lower capital costs, 14-times less power consumption and one-third the rack space of other solutions.

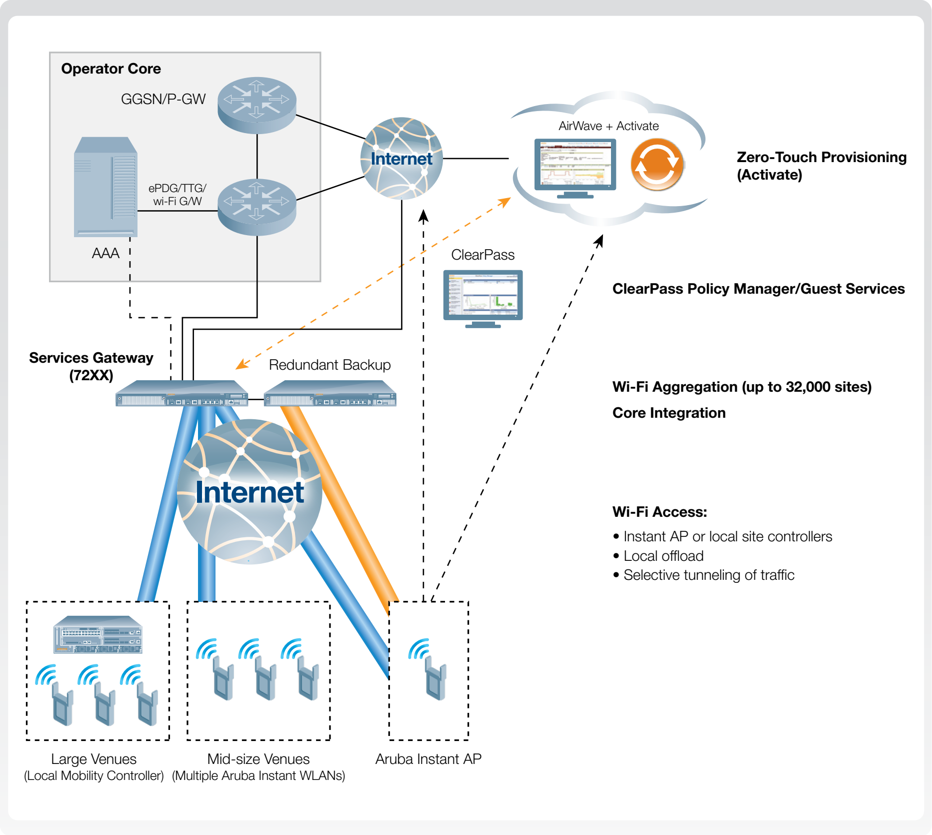


Figure 1. The Aruba HybridControl architecture is designed to provide dual-purpose Wi-Fi for policy-based cellular offload and managed WLAN services.

It combines an intelligent network edge based on controllerless Aruba Instant™ access points (APs) with powerful 7200 series Mobility Controllers that act as services gateways to deliver the scalability and resiliency required for service provider deployments.

Aruba Instant distributes WLAN functionality to APs. The data plane and control plane are distributed to allow more system-level scalability and flexibility.

Aruba Instant APs support high-end managed services-grade functionality, including Adaptive Radio Management™ for robust RF performance, per-user firewalls and role-based access control, mesh networking, quality of service, real-time spectrum analysis, AppRF technology to optimize mobile application performance, and advanced wireless intrusion detection and prevention.

Figure 2. Aruba Instant APs reduce core bandwidth needs by offloading cellular traffic locally to the Internet and intelligently tunneling select traffic, such as billing and legal intercept, through an IPsec connection to a centralized Mobility Controller.

In a cluster of Aruba Instant APs, one AP is dynamically-elected to provide all the control plane functions. If the dynamically-elected AP within a cluster goes down, another AP automatically takes over the role.

Expanding the Aruba Instant AP network in a location is as easy as plugging in additional APs, which inherit the configuration from the dynamically-elected AP.

With self-organizing Aruba Instant APs at the edge, the system is highly resilient and the impact of WAN bandwidth and latency on RF performance is completely minimized.

If an Aruba Instant AP needs to setup an IPsec VPN tunnel for select traffic, it uses a tamper-proof X.509 certificate to authenticate with an Aruba Mobility Controller that is acting as a services gateway and VPN termination point in the core. The controller validates the Instant AP request with an authentication server, responds with the authorization information, and establishes an IPsec VPN tunnel. All other traffic is bridged to the Internet.

In service provider deployments, select traffic is tunneled between Aruba Instant APs, which create secure IPsec VPN connections to an Aruba 7200 series Mobility Controller in the network core.

Figure 3. Aruba 7200 series Mobility Controllers. A single 7200 series Mobility Controller can support more than 32,000 Wi-Fi hotspots and aggregate over 100,000 APs.

Mobility Controllers also support secure authentication of Aruba Instant APs, AppRF technology to identify and optimize the performance of specific applications, and interfaces to the packet core through Wi-Fi gateways. For fast failover, Aruba Instant can have multiple VPN tunnels to different 7200 series Mobility Controllers acting as services gateways.

Key elements of the Aruba HybridControl architecture

- **Aruba Instant™ –** Intelligent, controllerless APs for local policy-based data offloading and secure tunneling of select traffic. Zero-touch provisioning makes Aruba Instant the ideal Wi-Fi solution for remote locations that have no onsite IT resources.
- **7200 series Mobility Controllers –** As a centralized services gateway, the 7200 series can scale to handle massive volumes of authentications and roaming events. It supports over 32,000 locations and performs stateful firewall policy enforcement at up to 40 Gbps.
- **AppRF technology –** To optimize mobile app performance, AppRF identifies apps, offers visibility to prioritize and block apps, provides an added layer of security for public Wi-Fi and managed application services, and scales for BYOD transaction and device density.
- **Aruba Activate –** A free, zero-touch cloud-based provisioning, inventory management and firmware upgrade service that automates the rapid rollout of large scale networks and reduces operational costs.
- **Context aggregation –** Analytics engines and other business apps can leverage contextual data about the network, users, devices, applications and location, as well as associated and unassociated client data and site-level RF data from the Aruba infrastructure.
- **ClearPass Access Management System™ –** In addition to efficient policy management, ClearPass streamlines and automates device onboarding and profiling, advanced guest Wi-Fi services, mobile device health assessments, and 802.1X provisioning.

With the distributed intelligence of Aruba Instant APs, coupled with the powerful 7200 series Mobility Controller acting as a services gateway in the core, the HybridControl architecture can scale massively. One 7200 series Mobility Controller can handle up to 32,000 Wi-Fi locations.

Additionally, multiple 7200 Mobility Controllers can be clustered in a resilient N+1 configuration to scale the deployment and provide geographic redundancy.

While Wi-Fi hotspots or branch offices can utilize cost-effective Aruba Instant APs, large and complex venues like stadiums and campuses may employ a Mobility Controller to centralize network services at the edge. The overall result is an architecture that delivers virtually limitless scalability for service provider Wi-Fi deployments.

Aruba AppRF

As more traffic traverses the Wi-Fi infrastructure, it is critical for service providers to have complete visibility and control over application traffic to preserve valuable bandwidth and deliver a secure, high-quality user experience.

Aruba AppRF technology gives managed service-providers insight into applications that are delivered to mobile devices from the mobile core and over-the-top (OTT) applications that are running on the public Internet.

Aruba application-awareness with media classification engine and application fingerprinting enables inspection of traffic flows – even when they are encrypted – to identify and prioritize important applications in real time.

Real-time unified communications applications like Microsoft Lync and Apple FaceTime, as well as cloud-based enterprise applications, can be automatically identified and visualized. Access controls and policies are then applied to specific applications, which are placed into the appropriate class of service based on service-level agreements.

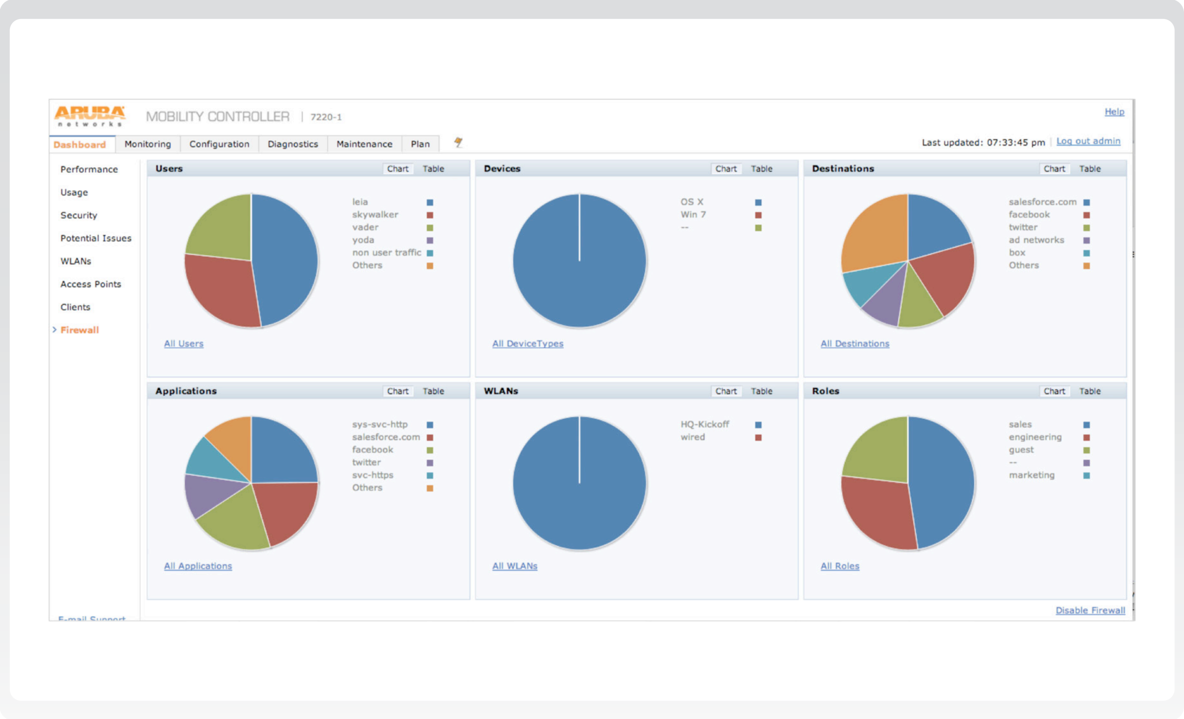


Figure 4. A graphical dashboard view of an Aruba 7200 series Mobility Controller.

AppRF additionally collects data from the network activity of authenticated users and uses this data to build lists of the most used applications, web destinations, WLANs, users, and device types.

Several tools are leveraged by AppRF to collect application information like configured Layer 4 services on the controller, application-layer gateways (ALGs), and heuristics to identify peer-to-peer traffic and analyze web traffic.

Application visibility allows appropriate action to be taken on traffic flows based on operator policy. The net effect is a vastly optimized network that gives operators better insight into traffic patterns for future performance optimization.

Zero-touch provisioning with Aruba Activate

The scale and variety of end customer deployment scenarios make service provider networks complex and challenging to install and manage. However, the Aruba AirWave™ network management system and zero-touch provisioning capabilities of Aruba Activate eliminate this complexity and reduce deployment costs by 75%.

AirWave comes with the necessary tools to manage and troubleshoot multisite wired/wireless networks, gain visibility into network and user traffic patterns, and integrate with the service provider's existing management framework.

Traditionally, the deployment of large-scale networks was very costly. The old way involved taking an AP out of the box, manually provisioning it, shipping it to the deployment site, and having an onsite technician go through the steps of installing and verifying the operation.

The free Aruba Activate service reduces deployment time through a cloud-based AP provisioning system that is also used for firmware upgrades and inventory management. Aruba Activate offers a simple, powerful way to define provisioning rules for an AP or group of APs.

With Aruba Activate, all the installer has to do is plug in the APs in factory default mode at the location and verify that the LEDs are green.

During the deployment process, the Aruba Instant AP first posts relevant identifying information to the Aruba Activate service, such as MAC address and part number.

Aruba Activate then verifies that the AP is authenticated and sends the IP address of the configuration/image server in the service provider data center and the relevant organizational information to the AP.

Next, the AP communicates with the AirWave server, finds and downloads the configuration and image from a designated folder, and begins operation.

In the operator data center, the Aruba ClearPass policy management platform can poll Aruba Activate so that new APs are automatically authorized to join the packet core network. This eliminates the need to manually configure AP whitelists on the controller, reduces operating costs and strengthens security.

In addition, Aruba Activate provides a lifecycle view of the product. By logging into the system, service providers have all relevant information about inventory and firmware levels for each Aruba Instant AP.

Context aggregation and value-added services

Contextual awareness is enabled by Aruba's integrated, stateful ICSA-certified Policy Enforcement Firewall™ (PEF) that runs on Instant APs and Mobility Controllers.

PEF™ aggregates contextual information about the state of the network, users, devices, applications, location and time of day. This allows complete fine-grained control over network access and optimizes application delivery without re-engineering the network.

Aruba also has the unique ability to capture data from unassociated clients. Contextual information, associated and unassociated client data, and relevant site-level RF data are available through an Aruba API to external applications that can leverage the information to drive more business value.

An example of this is analytics. Analytics applications mine data for business-relevant data, patterns and trends. The end result is the ability to anticipate needs and respond to customers with relevant content, products and services.

Retail analytics – including walk-by analysis, repeat visitor detection and dwell time – are highly relevant to store operations and marketing. Using analytics, retailers can compare store performance in different locations and study the effectiveness of advertising campaigns and promotions.

The results from these analytics are contingent upon the quality, quantity and timeliness of data. Context is dynamic and can include social, mobile, cloud, behavioral, situational, and environmental data about people, places, activities, preferences, and connections.

An interesting aspect of capturing information for analytics is that traffic patterns can be observed by monitoring Wi-Fi-enabled smartphones and other devices, whether or not they are associated to the network.

Unassociated Wi-Fi devices send periodic probe requests that signal presence and a trail of probe requests depicts a traffic pattern. It is estimated that 80% of Wi-Fi traffic of interest is from unassociated Wi-Fi clients and this raw traffic needs to be heavily processed to be relevant.

Aruba, with its unique ability to capture unassociated client information and other contextual data, integrates with a wide range of leading analytics engines that process data to produce highly relevant and timely business insights.

Beyond analytics, aggregated contextual information from Aruba can also be leveraged by other applications such as Wayfinding for large public venues as well as with leading advertising and promotional platforms.

Consequently, the aggregated contextual data and scalability of Aruba service provider Wi-Fi deployments can be leveraged to create more value-added services. Aruba has strong technology partnerships with leaders in analytics, mobile advertising and location-based services and can provide a complete end-to-end solution for service provider networks.

Policy management and guest access

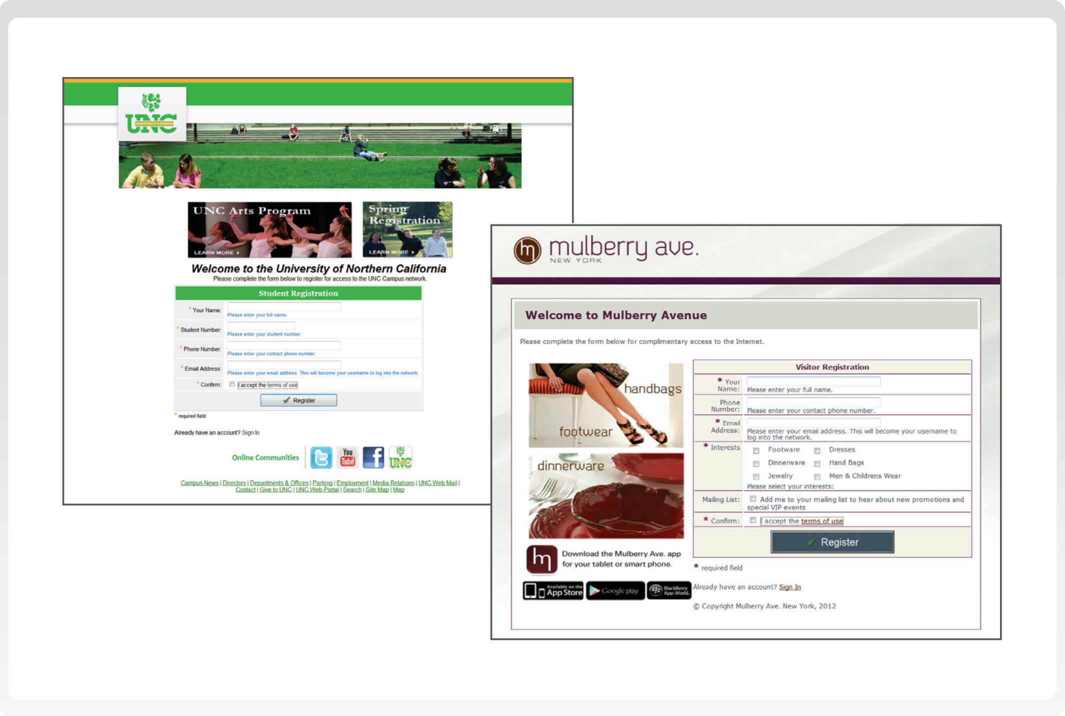
Service providers have a significant opportunity to deliver more value-added and tiered services to customers, leveraging some key industry trends including the proliferation of BYOD in the workplace and the security and management challenges they pose to enterprise IT.

In addition, many SMB and enterprise customers are looking to provide more comprehensive guest services with custom branding of splash pages or captive portals, the ability to capture more demographic information and provide targeted advertisements.

ClearPass offers unparalleled simplicity to manage, apply and enforce secure role-based network access based on context across wireless, wired and VPNs. It also provides device posture assessment, remediation and accurate device profiling.

Service providers can utilize ClearPass visitor management capabilities for advanced guest access services. It supports the creation of captive portal guest registration pages that are fully customizable so businesses can brand their services and push out targeted advertising.

In addition, ClearPass captures vital demographic data as part of the login process from public hotspots. Guest credentials can be delivered automatically via secure out-of-band SMS or via e-mail to simplify the registration process.



Welcome to the University of Northern California
Please complete the form below to register for access to the UNC Campus network.

Student Registration

* Your Name: Please enter your full name.
* Student Number: Please enter your student number.
* Phone Number: Please enter your contact phone number.
* Email Address: Please enter your email address. This will become your username to log into the network.
* Confirm: □ I accept the terms of use

* required field

Already have an account? Sign In

Campus News | Directory | Departments & Offices | Parking | Employment | Media Relations | UNC Web Mail | Contact | Give to UNC | UNC Web Portal | Search | Site Map | Map

Welcome to Mulberry Avenue

Please complete the form below for complimentary access to the Internet.

Visitor Registration

* Your Name: Please enter your full name.
Phone Number: Please enter your contact phone number.
* Email Address: Please enter your email address. This will become your username to log into the network.
* Interests □ Footware □ Dresses
□ Dinnerware □ Hand Bags
□ Jewelry □ Men & Childrens Wear
Please select your interests:
Mailing List: □ Add me to your mailing list to hear about new promotions and special VIP events
* Confirm: □ I accept the terms of use

* required field

Download the Mulberry Ave. app for your tablet or smart phone.

Already have an account? Sign In

© Copyright Mulberry Ave. New York, 2012

Figure 5. Advanced guest access capabilities in ClearPass let you create custom-branded captive portals with targeted advertising content.

ClearPass also enables the secure onboarding of mobile devices to customer enterprise networks. As BYOD continues to ramp up, it becomes cumbersome for IT departments to manually provision guest and employee-owned mobile devices with the right levels of access.

The onboarding capabilities in ClearPass make it easy for users to self-provision their Windows, Mac OS X, iOS and Android devices. Additionally, IT can create 802.1X configuration packages that users must agree to automatically provision on their devices before connecting to the network. Unique device credentials are also automatically distributed and revoked.

With ClearPass, service providers can market device onboarding, policy management, advanced guest access, endpoint posture assessments and health checks, and 802.1X provisioning as part of a comprehensive managed services offering that drives monetization opportunities.

Wi-Fi and cellular network integration

An integrated WLAN allows operators to intelligently offload traffic and provides total control and visibility into the network, user, device, and application behavior.

As a result, two cellular and Wi-Fi integration approaches have emerged:

- Basic reuse of core authentication and policy management framework.
- Tunnel traffic to services gateway for policy-based offloading and seamless mobility.

Reuse of core authentication

In this scenario, the cellular offload solution reuses credentials, such as the SIM module, to automatically authenticate subscribers to the WLAN.

This requires a services gateway with AAA/EAP-SIM authentication server functionality. It should include 3GPP interfaces to the operator's HLR/HSS subscriber databases and policy charging and recording functions (PCRF) to authenticate users and access policies. The WLAN enforces access policies.

Using a RADIUS interface, Aruba WLANs integrate with a number of services gateways and EAP-SIM/AAA servers for seamless mobile core integration.

In many cases, operators support EAP-SIM and captive portal authentication at a hotspot with separate SSIDs. While a subscriber can automatically authenticate by reusing SIM credentials, guests can be redirected to a portal or landing page and offered limited or paid access.

Tunnel to a Wi-Fi gateway for seamless mobility

The evolved packet core (EPC) supports 3GPP and non-3GPP access. It distinguishes between trusted and untrusted non-3GPP access and defines the mechanisms and interfaces for interoperability.

Within this framework, Wi-Fi can be deployed as a secure and seamless extension of the operator's network with full mobility services. Traffic is tunneled from the WLAN via Layer 2 over GRE or IPsec VPNs to a secure gateway. This gateway provides 3GPP interfaces to the packet core including GPRS tunneling protocol (GTP) to the GGSN or P-GW and diameter to the AAA system.

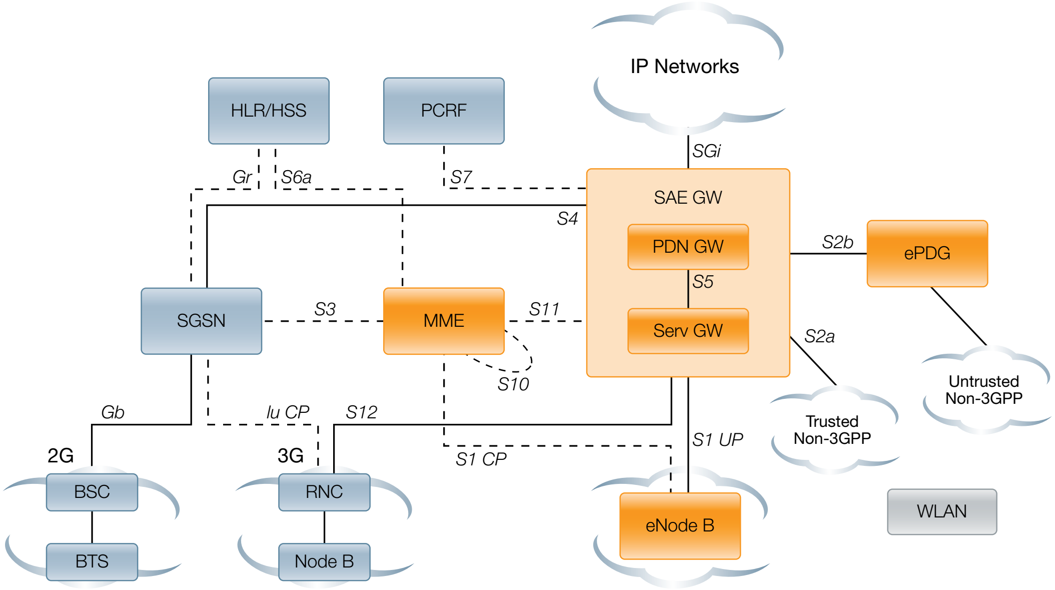


Figure 6. The evolved packet core distinguishes trusted and untrusted non-3GPP access and defines mechanisms and interfaces for interoperability.

Utilizing a trusted WLAN involves interfacing to a gateway function that provides an S2a GTP or proxy mobile IP (PMIP) interface to the GGSN or P-GW.

Untrusted WLAN access is performed via an entity called the evolved PDG (ePDG), similar to a VPN concentrator. The Mobility Controller or the AP establishes an IPsec tunnel to the ePDG, which interfaces to the P-GW via the S2b interface. This interface can be GTP or PMIP.

Aruba WLANs support trusted and untrusted non-3GPP access through secure tunnels from Mobility Controllers or Aruba Instant APs to third-party Wi-Fi gateways.

These Wi-Fi gateways provide IP address/mobility management and integrate with the packet core for operator services. They can also perform local data breakout based on policies and offload traffic from the packet core.

Mobility between the cellular network and Wi-Fi network is typically handled by network-based mobility protocols – GTP, the most commonly used, or PMIP with the P-GW acting as the user plane anchor.

The HybridControl architecture interoperates with a wide range of WLAN gateways. This gives operators total control and visibility into WLAN usage along with the ability to offer value-added, tiered, personalized and premium Wi-Fi services to customers.

These interoperable frameworks allow service providers to integrate Wi-Fi as a small cell, alternate 3G/4G RAN technology, and truly augment the broadband network and deliver vastly improved services more cost effectively.

Summary

The benefits of Wi-Fi are clear in the service provider context. It is a highly viable small-cell solution that securely offloads data traffic from the cellular network, reduces overall costs, and delivers exceptional-quality broadband services.

Recognizing the revenue potential, there is also a rapidly-growing desire among many services providers to deliver managed mobility services to a large spectrum of enterprise customers and small/medium businesses.

Whether you are considering offloading data to Wi-Fi or managed mobility services, these are the key issues to consider:

- Unprecedented WLAN system scalability to accommodate the massive influx of mobile devices and mobile applications.
- Exceptional Wi-Fi reliability under the most severe and demanding RF conditions.
- Ease of WLAN deployment and the ability to manage traffic over the air.
- Integration with the operator packet core network and the existing policy management framework.
- Advanced functionality that can be monetized into managed services that drive new revenue streams.

The Aruba HybridControl architecture for service providers supports policy-based data offloading and managed services deployments at extraordinary scale while addressing every key issue. The Aruba HybridControl architecture includes:

- **Aruba Instant™ –** Intelligent, controllerless APs for local policy-based data offloading and secure tunneling of select traffic. Zero-touch provisioning makes Aruba Instant the ideal Wi-Fi solution for remote locations that have no onsite IT resources.
- **7200 series Mobility Controllers –** As a centralized services gateway, the 7200 series can scale to handle massive volumes of authentications and roaming events. It supports Wi-Fi at over 32,000 locations and performs stateful firewall policy enforcement at up to 40 Gbps.

- **AppRF technology –** To optimize mobile app performance, AppRF identifies apps, offers visibility to prioritize or block apps, provides an added layer of security for public Wi-Fi and managed application services, and scales for BYOD transaction and device density.
- **Aruba Activate –** A free, zero-touch cloud-based provisioning, inventory management and firmware upgrade service that automates the rapid rollout of large scale networks and reduces operational costs.
- **Context aggregation –** Analytics engines and other business apps can leverage contextual data about the network, users, devices, applications and location, as well as associated and unassociated client data and site-level RF data from the Aruba infrastructure.
- **ClearPass Access Management System™ –** In addition to centralized policy management, ClearPass automates device onboarding and profiling, advanced guest Wi-Fi services, endpoint posture assessments and health checks, and 802.1X provisioning.

With the Aruba HybridControl architecture, service providers can intelligently integrate Wi-Fi at scale as part of their cellular data offload and managed services deployments and do so with lower costs and higher monetization potential.

About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

ARUBA networks

www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com