WHITE PAPER

INTEGRATING WI-FI AND CELLULAR NETWORKS

a Hewlett Packard
Enterprise company

TABLE OF CONTENTS

INTRODUCTION

Wi-Fi is ubiquitous today. The pervasiveness, performance and economics of Wi-Fi has crossed the tipping point, and we are now in a world where always-on Wi-Fi is expected. A day in the life of a consumer consists of roaming from Wi-Fi network to Wi-Fi network, with occasional breaks that are covered by a cellular data plan. Private homes, offices, businesses as well as public places like cafes, restaurants, shopping malls, stadiums, convention centers, hospitals, airplanes, trains, hotels, schools, and every other place you can think of all deploy Wi-Fi to offer Internet access.

Wi-Fi connects users in more than 450 million households worldwide and at over 47 million global public hotspots[1]. Free Wi-Fi availability is increasingly considered by consumers as a key requirement when choosing a service. In fact, Wi-Fi is considered as one of the basic amenities by millennials[2]. All consumer access devices including smartphones, tablets, e-readers, and laptops come equipped with Wi-Fi as the primary, and sometimes the only, connectivity method. An average home has more than eight devices on the Wi-Fi network and there are an estimated total of 6.8 billion Wi-Fi products in use[3]. These figures are expected to grow exponentially with the proliferation of the internet of Things (IoT).

The ever growing popularity of Wi-Fi has fueled tremendous innovation in the technology. In the last 16 years, Wi-Fi data rates have progressed from 11 Mbps with IEEE 802.11b to 3Gbps with 802.11ac Wave 2. The ubiquity of Wi-Fi access points and clients coupled with the technological advancements have already made Wi-Fi the primary means of access. Not surprisingly, Wi-Fi has been the key driving force behind the rise of the mobile Internet. Wi-Fi today carries ten times the IP data traffic as compared to the cellular networks[4].

While Wi-Fi has established itself as the chief technology to meet the global demand for data today, it is expected to maintain that lead in the foreseeable future with the continued innovation by the Wi-Fi industry to stay ahead of the growth in data traffic demand. Incorporation of OFDM, MU-MIMO, enhanced modulation and coding, and advanced interference management techniques into Wi-Fi makes it as spectrally efficient as any other technology. Moreover, the rich suite of features built over years for Wireless Local Area Networks (WLAN) make it the technology of choice for businesses and enterprises alike. In fact, public and private entities are fast getting rid of dependence on wired connections for data and voice in favor of Wi-Fi as the only mode of access within their establishments.

In today's mobile-first world, it seems natural for mobile operators to integrate Wi-Fi into their offered services so that they can manage the total connectivity experience of their subscribers. Indeed, service providers are already leveraging Wi-Fi to keep up with the data demand and offer better experience indoors and in heavily trafficked public venues. Several tier-1 mobile network operators (MNOs) have implemented Wi-Fi calling to not only leverage Wi-Fi for data, but for voice as well.

Besides leveraging Wi-Fi to enhance capacity and coverage of their network, service providers are also trying to capitalize on a fast growing market – managed Wi-Fi services. There is a significant opportunity for service providers to leverage their scale and expertise to deliver innovative mobility solutions and value-added services to enterprises and businesses.

The new public Wi-Fi network is more than just a "free hotspot". The deployments are more complex in nature and the network has to be not only highly reliable and secure but also be able to support both offload and private services required by the venue owner. Moreover, the Wi-Fi network has to be able to enable delivery of value added services such as analytics, location based advertising, and mobile engagement to enable monetization of Wi-Fi.

Aruba's Wi-Fi solutions, based on a foundation of security, scalability and RF performance, have been successfully deployed by some of world's largest and distributed enterprises including stadiums, airports, retail, restaurant chains and more. Today, Aruba's solution powers hundreds of thousands of hotspots across the world deployed and managed by leading service providers.

[1] Federal Communications Commission, "Action by the Commission April 17, 2015, by Report and Order and Further Notice of Proposed Rulemaking (FCC 15-47)," 2015.
[2] Flipkey by Tripadvisor, 2015. [Online]. Available: https://www.flipkey.com/blog/2015/06/01/what-amenities-are-millennials-really-looking-for/.
[3] Wi-FI Alliance, 2016. [Online]. Available: http://www.wi-fi.org/beacon/wi-fi-alliance/wi-fi-alliance-6-for-16-wi-fi-predictions.
[4] Wi-Fi Alliance, 2015. [Online]. Available: http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-statement-on-license-assisted-access-laa.

The foundational elements that the Aruba solution is built upon are now more critical for service provider deployments – whether for large scale Wi-Fi offload networks or for delivering managed services to a spectrum of enterprise customers. The architecture is designed to address the most critical requirements for service providers – scale, security, robust RF performance, reduced operational costs, control, visibility, and integration with the cellular core network for unified policy management.

This paper discusses the architecture for integration of Wi-Fi as alternate Radio Access Technology (RAT) into the 3GPP core network architecture to enable unified mobility services for the subscribers.

KEY CONSIDERATIONS

The increasing use of smart devices has caused a rapid increase in data consumption which in turn is placing an enormous strain on existing wireless broadband networks across many regions – especially in densely populated areas. The data congestion is leading to poor user experience and is impacting voice quality as well.

While all options need to be looked into depending on the specific circumstances, one of the most cost effective options to address data congestion is to offload traffic to Wi–Fi networks. Consumers have spoken. They prefer, seek and use Wi-Fi wherever possible. Wi-Fi offers very high bandwidth and the lowest cost per bit, and is the most widely used wireless network today.

Intelligently integrating Wi-Fi as part of the operator's network provides significant benefits in terms of enhancing both the capacity and coverage especially where people congregate the most – transportation hubs, malls, stadiums, convention centers, city centers etc. Intelligent integration implies making network selection and authentication to operator owned (or partner owned) Wi-Fi networks automatic and secure – while delivering reliable and good quality of experience. Integrated Wi-Fi networks will provide operators more control and visibility over Wi-Fi usage, ability to enforce common policies (same as in 3G/4G networks) – and even deliver walled garden services securely.

We strongly believe that Wi-Fi will play an increasingly important and strategic role as operators work to cost effectively augment network capacity to meet the ever increasing demand for data. Wi-Fi can be viewed as a small cell solution within the latest 3GPP framework (as either trusted or untrusted non-3GPP access network). Whether it is a licensed spectrum "small cell", an unlicensed spectrum "Wi-Fi small cell" or a combination thereof, operators now have the ability to easily and securely increase overall network capacity – in a cost effective manner.

As operators look to integrate Wi-Fi as an alternate Radio Access Technology (RAT) solution to add capacity and to deliver value add services, there are several key considerations for the end-to-end architecture.

- Enabling scaling from thousands of small hotspots to high density environments like stadiums – while reducing backhaul costs
- Ensuring RF reliability
- Ensuring high quality end user experience for voice and video applications
- Ensuring end-to-end security including defensive and offensive mechanisms against wireless intrusion
- Making the process of transitioning to Wi-Fi (from cellular network) automatic and secure
- Intelligently offloading traffic to Wi-Fi
- Integrating with the mobile core network policy management framework
- Delivering walled garden and other premium content over Wi-Fi networks

The innovative Aruba architecture is able to address each of these key considerations to offer differentiated services to the service provider.

CORE NETWORK INTEGRATION ARCHITECTURES

An integrated Wi-Fi solution allows operators to intelligently offload traffic while providing complete control and visibility of the user context. The cellular and Wi-Fi integration architectures can be classified into two different approaches:

A. Managed Offload: Integration with core network authentication and policy management systems

B. Integrated Offload: Integration of Wi-Fi data traffic into the core network for seamless mobility and feature parity

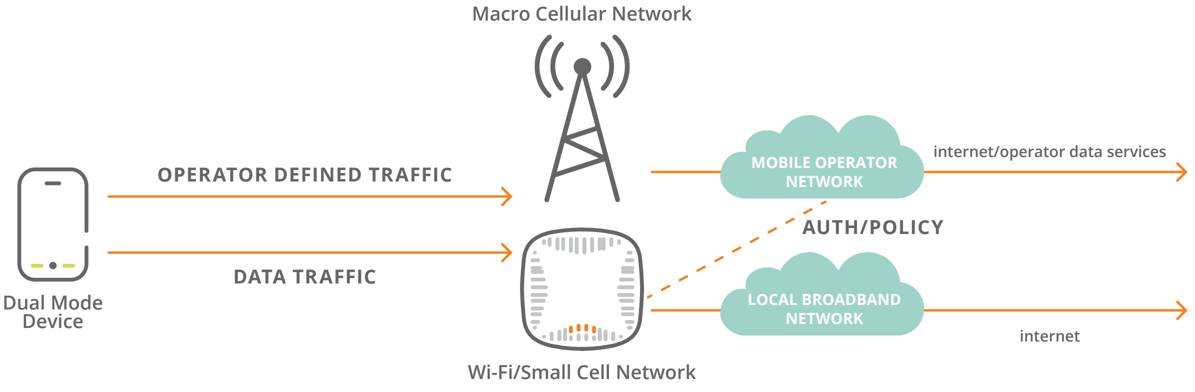

figure 1.0_051216_wificoreintegration-wpa

Figure 1: Integration with core network for common authentication and access policies.

Managed Offload with Authentication and Policy Integration

In this approach, the offload solution allows the reuse of credentials (using the SIM module for instance) to automatically authenticate to the Wi-Fi networks. This may be done using EAP-SIM/AKA methods and requires a common AAA authentication server (a services gateway) that provides 3GPP interfaces to the operator's HLR/HSS (subscriber databases) and Policy and Charging Rules Function (PCRF) to authenticate the user and enforce usage policies. The WLAN network enforces the access policies as determined by the core network.

Aruba's architecture to support this basic cellular network integration for authentication is depicted in Figure 2.

In the architecture shown in Figure 2, the Aruba WLAN integrates with the service provider's core network Authentication, Authorization and Accounting (AAA) server using the RADIUS interface. User handsets may be seamlessly authenticated using EAP-SIM/AKA based on the same credentials used to authenticate them onto the cellular network.

Both mobility controller based campus deployments as well as Instant based distributed deployments support this architecture. The mobility controller or the Instant virtual controller provides the RADIUS interface to integrate with the service provider's AAA server respectively. This RADIUS interface between Wi-Fi and the AAA server may traverse the enterprise LAN, public internet or private backhaul connection to the operator's core network.

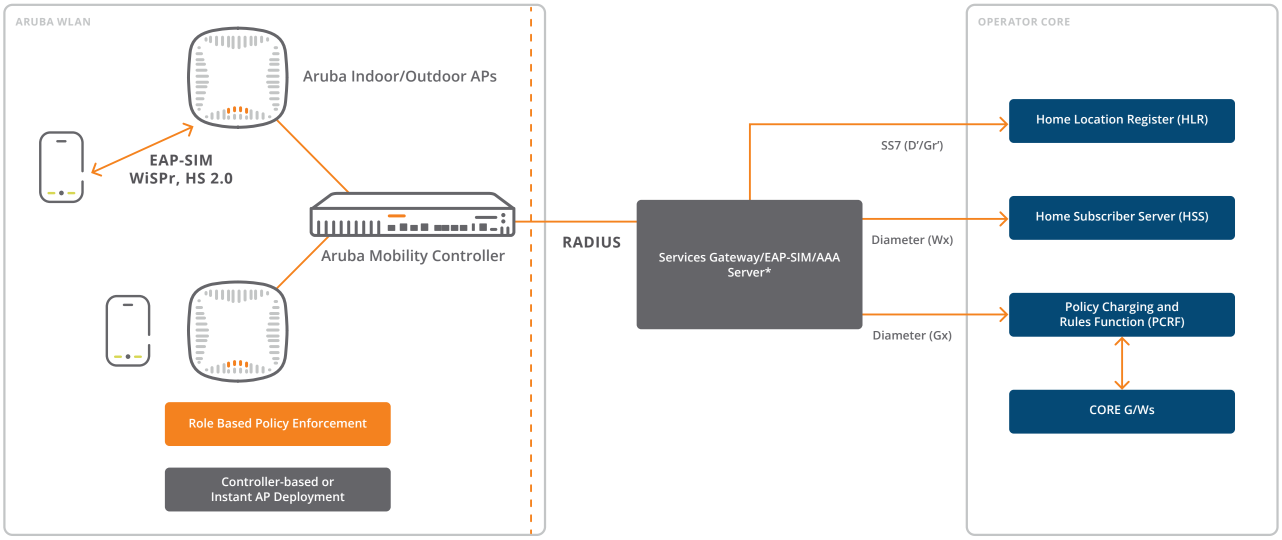
ARUBA WLAN
Aruba Indoor/Outdoor APs
EAP-SIM
WiSPr, HS 2.0
Aruba Mobility Controller
Role Based Policy Enforcement
Controller-based or Instant AP Deployment
RADIUS
Services Gateway/EAP-SIM/AAA Server*
SS7 (D'/Gr')
Diameter (Wx)
Diameter (Gx)
OPERATOR CORE
Home Location Register (HLR)
Home Subscriber Server (HSS)
Policy Charging and Rules Function (PCRF)
CORE G/Ws

figure 2.0_051216_wificoreintegration-wpa

Figure 2: Aruba architecture for core network authentication and policy integration.

On the core network side, the AAA server interfaces with the Home Subscriber Server (HSS) and the Home Location Register (HLR) databases that maintain information about the operator's subscribers. The interface to the Policy and Charging Rules Function (PCRF) enables application of specific policies defined by the service provider. The AAA server also provides interfaces with other 3GPP network functions including the PDN Gateway (P-GW).

Aruba's WLAN integrates with a number of AAA vendors including Aptilo, Accuris, Alepo, EliteCore, and Ericsson. The interface to these systems is through RADIUS and enforces all access policies.

In many cases, operators may want to support both EAP-SIM/AKA based authentication as well as captive portal based authentication at a hotspot using separate SSIDs at the hotspot. In such a scenario, while the operator's subscriber would be automatically authenticated using SIM/AKA credentials, guest users can be re-directed to a captive portal or a log-in splash page that offers them options for limited or paid access.

Integrated Offload of Wi-Fi Traffic into the Core Network

With this architecture, Wi-Fi can be deployed as a secure, seamless extension of the operator's network with full mobility and feature parity with the cellular network. This architecture involves tunneling of traffic from the WLAN network (using Layer-2 over GRE or IPSec VPN for example) to a security gateway that provides the 3GPP interfaces to the packet core including GPRS Tunneling Protocol (GTP) to the P-GW or the GGSN and Diameter to the AAA server.

With this approach, operators can seamlessly connect subscribers to Wi-Fi networks with complete control and visibility and at the same time have the ability to offer parity features as well as value-add, tiered, personalized or premium services to customers over Wi-Fi networks. While seamless mobility enhances the end-user experience, feature parity enables the service provider to offer the same services on Wi-Fi that they offer on the 3G/4G networks including voice calling, messaging, parental controls etc.

As a background, the Evolved Packet core (EPC) is designed to support both 3GPP and non-3GPP (for example WLAN) access. It distinguishes between "Trusted" and "Untrusted" non-3GPP Access. It is up to the operator to decide if a non-3GPP access network is "trusted" or "untrusted". The decision is based not just on access technology and the backhaul, but may depend on other business considerations as well.

The Evolved Packet System (EPS) architecture that supports interworking with non-3GPP systems is depicted in Figure 3.

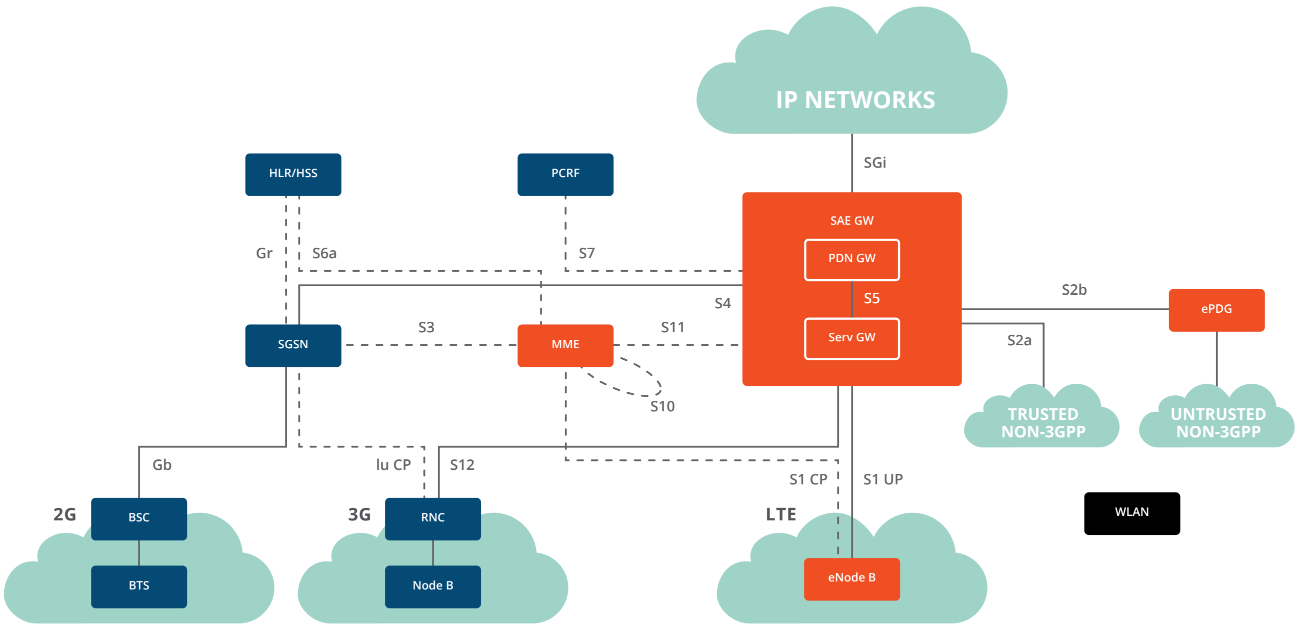

figure 3.0_051216_wificoreintegration-wpa

Figure 3: Evolved Packet System (EPS) architecture to support interworking with non-3GPP systems.

Trusted Wi-Fi or SaMOG Architecture

Interworking with a "trusted" WLAN involves interfacing with a Trusted Wi-Fi Access Gateway (TWAG) function. TWAG terminates a layer 2 (Ethernet over GRE or Ethernet over IP) interface from the WLAN and provides an S2a (GTP or Proxy Mobile IP based) interface to the P-GW or GGSN. This architecture is also sometimes referred to as the S2a Mobility over GTP (SaMOG) architecture and is shown in Figure 4.

The architecture offers the ability to tunnel only selected traffic to the operator core network (for example, based on operator specific SSID) while the other traffic (for example, open guest SSID) may be locally broken out. The TWAG is deployed by a service provider in their core network. As an option to secure the interface to the core network, particularly in cases where the service provider doesn't control the backhaul, the service provider may encapsulate the WLAN GRE tunnel within IPsec. The IPsec tunnel can be terminated by a third party Security Gateway (SeGW), to provide EoGRE/EoIP interface to the TWAG.

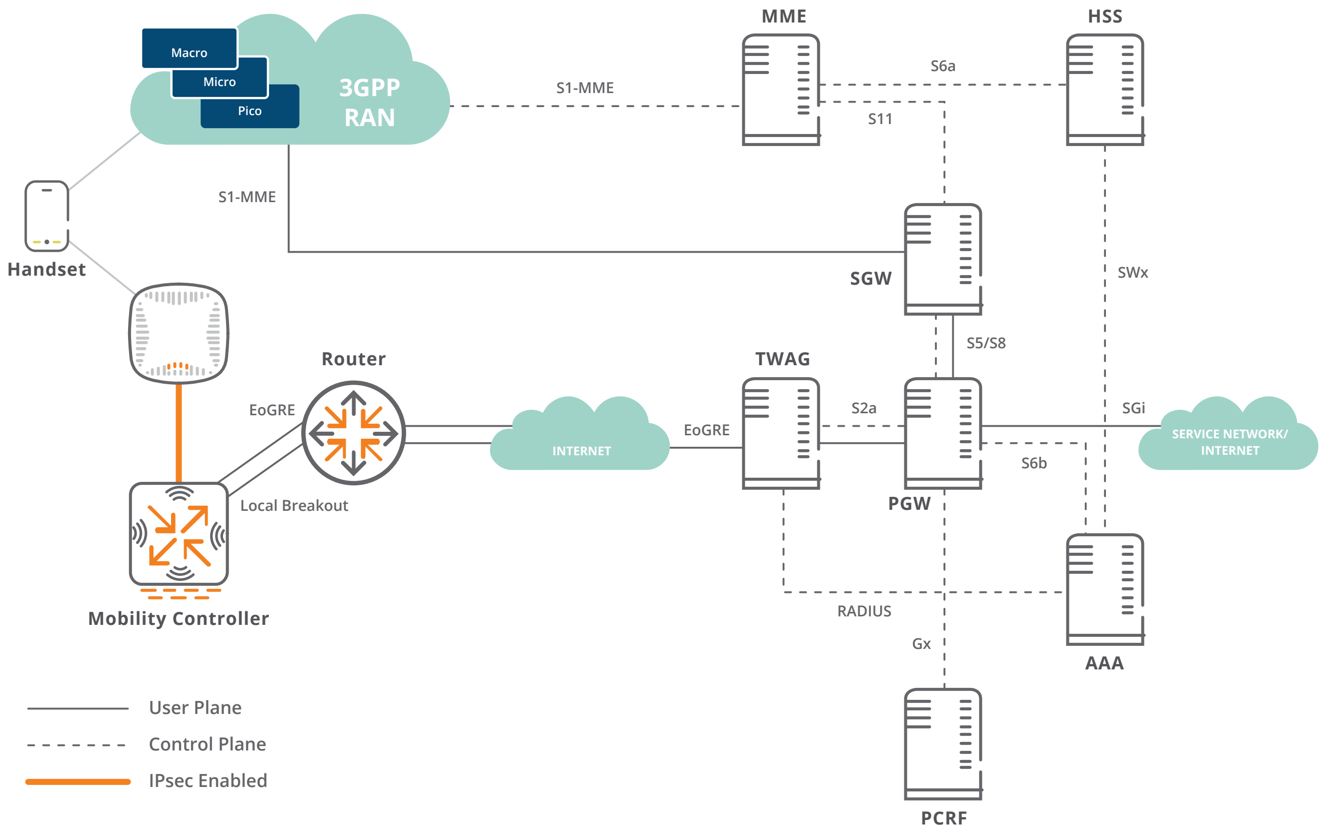

figure 4.0_051216_wificoreintegration-wpa

Figure 4: S2a Mobility over GTP (SaMOG) architecture for Trusted Wi-Fi.

Untrusted Wi-Fi Architecture

“Untrusted” WLAN access is performed via an entity called the evolved Packet Data Gateway (ePDG). ePDG is similar to a VPN concentrator that terminates the IPsec tunnels set up by the user device. The user handset uses DNS to look up the IP address of the ePDG and initiates the set up of the IPsec tunnel using IKEv2. The ePDG interfaces to the P-GW via the S2b interface (which could be GTP or Proxy Mobile IP). The untrusted Wi-Fi architecture is shown in Figure 5.

A popular use-case for untrusted Wi-Fi architecture is to enable Wi-Fi calling functionality. The user handset sets up an IPsec tunnel, one for each of the services of interest, to bring the data traffic to the ePDG and subsequently to the P-GW. The P-GW acts as a common anchor for user data traffic, both on WLAN and on the LTE network. Based on the service, P-GW routes the traffic to the IMS core or the internet. The other Wi-Fi traffic may be locally broken out at the WLAN.

The Aruba WLAN can be deployed as Trusted or Untrusted Non-3GPP Access using third party TWAG or ePDG gateways respectively. These Wi-Fi Gateways provide IP mobility management and integrate with the packet core for operator services. These gateways can also perform local data breakout based on policies and offload traffic from the packet core.

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

Aruba’s mobility controller based campus APs as well as Instant APs support integration of Wi-Fi traffic into the core network based on both trusted Wi-Fi and untrusted Wi-Fi architectures. In case of controller based deployments, the controller enables set up of the EoGRE tunnel to the TWAG. In case of Instant AP deployments, the virtual controller enables set up of the EoGRE tunnel to the TWAG. There is also an option to have each of the Instant APs set up the tunnel independently instead of going through the virtual controller.

The interface between Wi-Fi and the operator’s Wi-Fi Gateway (TWAG or ePDG) may traverse the enterprise LAN, public internet or private backhaul connection to the operator’s core network – the EoGRE tunnel in the trusted Wi-Fi case and the IPsec tunnel in the untrusted Wi-Fi case traverses any of these backhaul networks to interface with the Wi-Fi Gateway located in the operator’s core network.

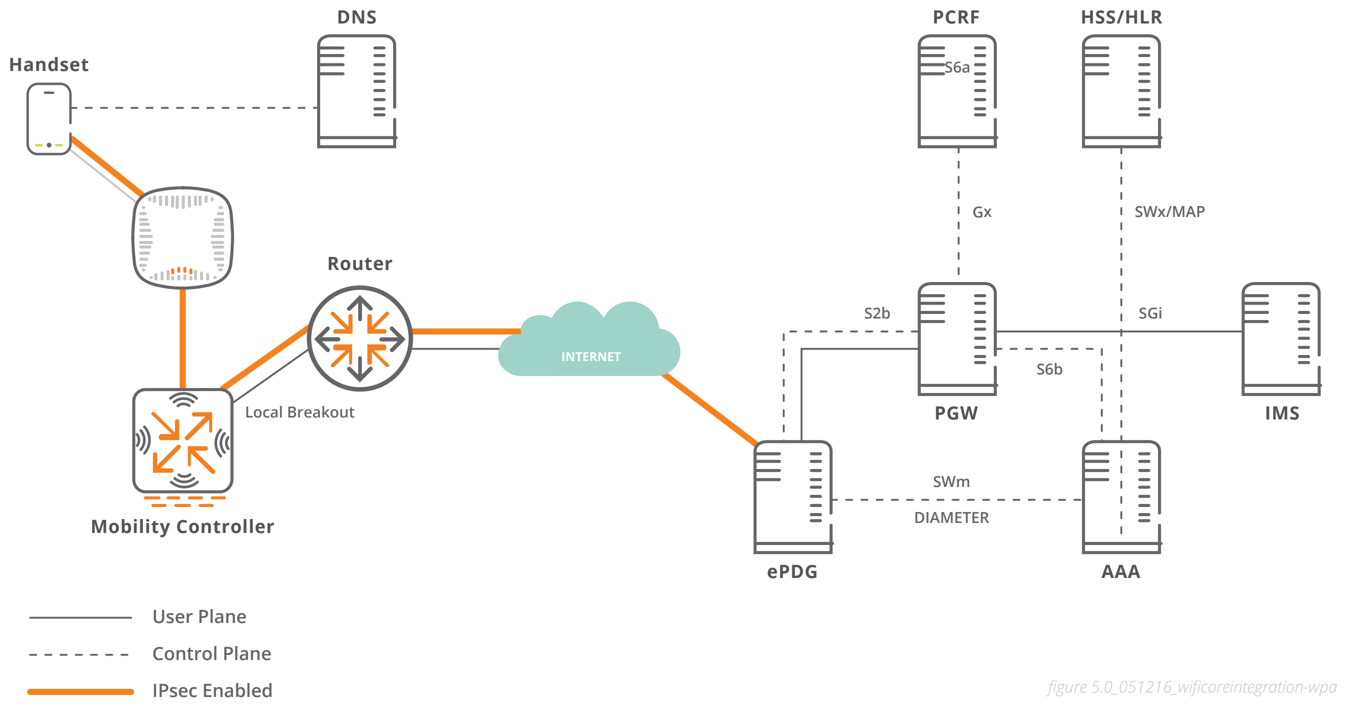

figure 5.0_051216_wificoreintegration-wpa

Figure 5: The Untrusted Wi-Fi architecture.

A simplified (conceptual) network diagram showing the unified integrated offload solution architecture from Aruba is depicted in Figure 6.

Aruba integrates with a few WLAN Gateway vendors as part of the integrated Wi-Fi solution including Alcatel-Lucent's 7750 gateway, Acme Packet/Oracle gateway and Ericsson's WMG/WIC gateways.

CONCLUSION

The integration architectures discussed allow operators to integrate Wi-Fi as an alternate radio access technology, while truly augmenting the mobile network to deliver enhanced services in a cost efficient manner. By integrating Wi-Fi into the mobile core network, service providers can enable automatic authentication, unified access policy management, seamless mobility and feature parity with cellular networks on Wi-Fi. Aruba's products provide robust performance required to support carrier-grade services and have proven interoperability with the mobile core through several third-party gateways.

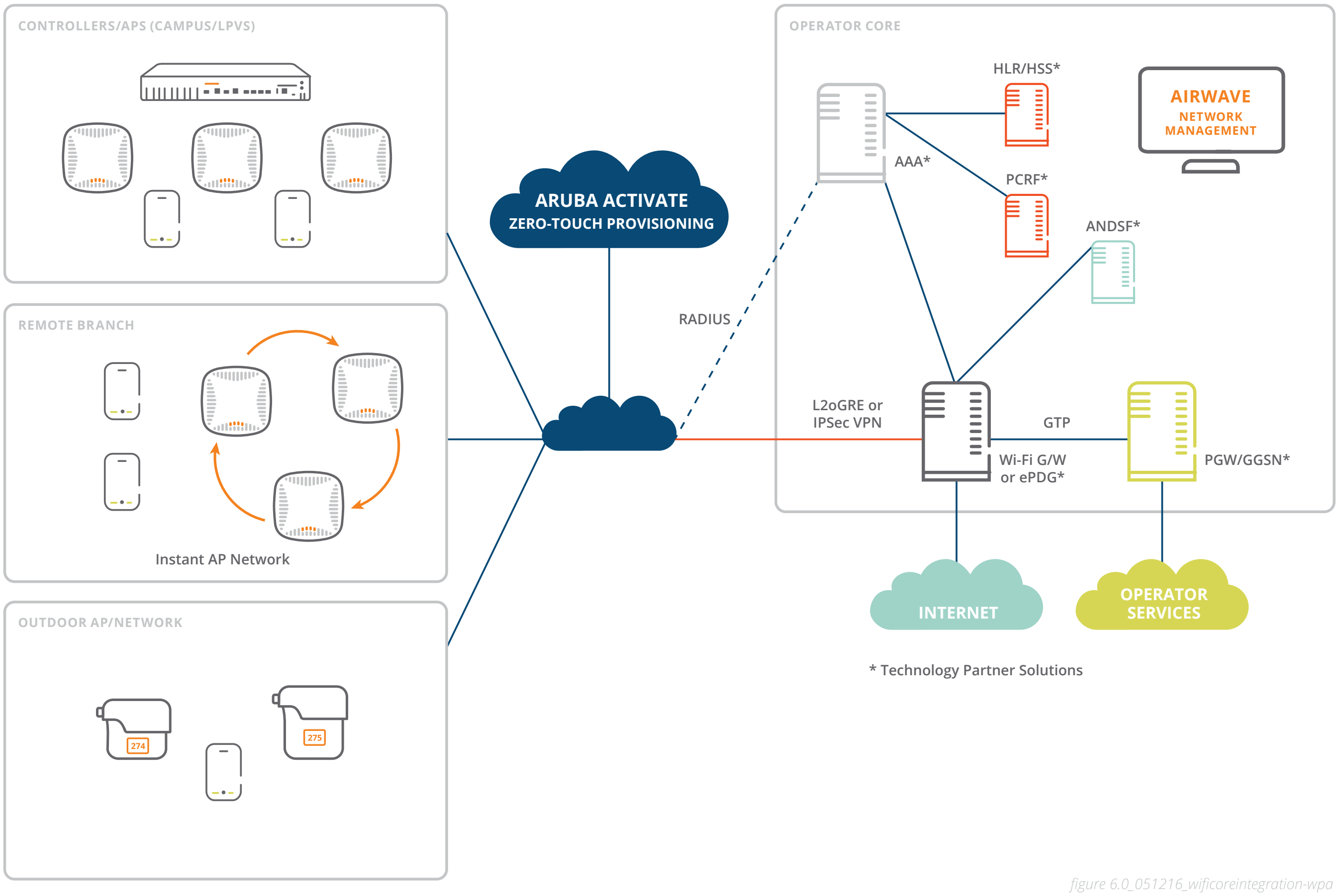

Figure 6: The integrated offload solution architecture from Aruba.

Further, Aruba's Wi-Fi mobility solutions address service providers' key requirements including reliability, scalability, visibility, security, control, reduced Opex and monetization opportunities. Aruba's controller-less Instant APs provide distributed control to support local data offload and selective tunneling of data traffic. Mobility controllers offer virtually limitless scalability in supporting tunnel aggregation. ClientMatch and Adaptive Radio Management (ARM) technologies provide robust RF management and reliability to ensure that the users get the best Wi-Fi connection possible. Support for Hotspot 2.0 enables seamless connectivity and roaming for the subscribers.

AppRF technology provides comprehensive visibility into the application and web traffic in the network. The context aware Policy Enforcement Firewall provides the service providers granular control based on user, device, application and location. Aruba Activate enables zero touch provisioning capabilities to make deploying Wi-Fi a snap, while advanced management solutions, which include cloud based Central as well as on premise Airwave options, enable ease of management, diagnostics and reporting. This in turn lowers the overall cost of delivering and operating the services.

Aruba's ClearPass enables network access control, secure device onboarding and advanced guest access solutions. The Analytics and Location Engine (ALE) provides a context aggregation function that drives third party analytics engines to offer advanced reporting. The service provider may drive additional value-added services including unified communications, mobile engagement and location based advertisements to enable further monetization of Wi-Fi deployments.

Having worked closely with several Tier-1 operators worldwide to successfully deploy carrier-grade Wi-Fi, Aruba has deep experience in fulfilling the requirements of service provider deployments. Aruba's existing carrier Wi-Fi deployments, which consists of hundreds of thousands of access points, support tens of terabytes of data traffic on a daily basis delivering immense value to the operators. Aruba understands the complexities of service provider Wi-Fi deployments and has the proven solution portfolio and best practices to help operators design effective network augmentation as well as managed services. Further, Aruba's rich suite of value-add solutions enable the service provider to further monetize Wi-Fi, enabling a strong business case to deploy Wi-Fi.

aruba
a Hewlett Packard
Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com