



---

# Introduction

Hotels, conference/convention facilities, cruise ships and other hospitality venues host an increasingly “connected” customer base. From the business traveler who requires the ability to establish VPN connections to headquarters to leisure travelers updating their online photo albums, guests demand broadband connectivity. While wired broadband technologies offer basic connectivity, they are expensive to deploy and do not enable mobility. Wi-Fi, or 802.11, offers wireless broadband connectivity and mobility within the facility. Early adopters of Wi-Fi in the hotel industry often limited their deployments of this technology to common areas (e.g. meeting rooms, lobbies, lounges), but the trend in this market is towards pervasive coverage so that guests may connect from their rooms. As the number of 802.11 APs per hotel increases, so will the complexity and cost associated with deploying and maintaining the WLAN if the appropriate solution is not implemented.

While the earliest Wi-Fi application deployed by hotels was guest “hotspot” access, limiting the WLAN to supporting this application squanders many opportunities to increase productivity, enhance services, and maintain the loyalty of customers. Internal applications such as VoWLAN and check-in “queue busting” can significantly increase productivity and customer satisfaction within the hospitality industry.

Hospitality venues have many choices available to them as they consider deploying WLAN technology. WLAN hotspot access may be fee based or offered for free to guests. The venue may choose to purchase and deploy their own WLAN or engage a service provider to manage their networks and bill guests for connectivity.

In this whitepaper, hospitality applications and associated solution requirements are examined with the intent of identifying the optimal WLAN architecture. A centralized architecture consisting of a WLAN controller and thin APs is clearly differentiated as the best implementation for WLANs in the hospitality industry.

## WLAN Hotspot Access

Business travelers demand Wi-Fi access and often have the requisite capability (i.e. 802.11 interface & VPN client) to connect. Intel’s Centrino wireless program and similar efforts by computer manufacturers have created an environment where most business class laptops are shipped with 802.11 as a standard feature. Furthermore, leisure travelers are vacationing with laptops in tow to continuously update “blogs” and digital photo albums, modify travel plans online, and remain in communication with friends and family. Hotspot access can serve as a pay for use revenue generating service or a free amenity intended to draw in lucrative business travelers.

While 802.11 equipped laptops are widely available, they vary significantly in terms of certification level. Hotels should not require more than the basic Wi-Fi certified 802.11b network interface and a WWW browser. Requiring Wi-Fi WPA or WPAv2 certifications, a best practice in enterprise WLAN deployments,

---

would deny access to a significant number of potential hotspot users. As such, the solution must be able to simultaneously support different security policies for guests and internal enterprise users. The WLAN solution should be able to support a guest SSID that is broadcast and automatically visible to users via their 802.11 client utility. When launching the browser, guests should be redirected from their default homepage to a portal (Fig. 1) where login instructions and, optionally, legal disclaimers are provided.



Fig. 1: Guest Login Portal

There are several common hotspot access scenarios:

- a) Free access: The user accepts a legal disclaimer on the guest portal that is served by the WLAN solution and is given access to the internet after supplying a login and password supplied by the front desk. At this point guests may launch their VPN client for security. Hotels should be able to customize the guest login captive portal to suit their needs. It is expected that large hotel chains may be able to derive advertising revenue by placing the banner ads of local merchants seeking to reach guests on the login portal.
- b) Fee Based Access: The hospitality venue may decide to offer fee based hotspot access. A hotspot access controller (e.g. IP3 Networks, Nomadix) is used to integrate into credit card billing facilities or the hotel "Property Management System" (PMS). Integration with PMS provides the option to bill directly to the room instead of generating a separate credit card bill for broadband access. In addition, hotels may choose to offer free, controlled access using the guest name and room number from PMS to verify the user's status as a guest.
- c) Service Provider (SP) mediated access: All the traffic from the guest hotspot SSID can be re-directed to a SP which controls access and assumes responsibility for billing.

---

Most hotels and service providers in the US charge about \$9-\$10 for 24 hours of access. In Europe the typical charge approaches €20 for 24 hours.

In all of the access scenarios above, it is critical to ensure that bandwidth can be managed at the per user/session level to ensure consistently good service. Furthermore, the system must be able to separate traffic associated with any internal use of the WLAN from hotspot data. Security policies should be configurable at the user/group level (e.g. guest, staff, security).

## **WLAN Applications for Hospitality Operations**

To deploy a WLAN entirely for hotspot access ignores compelling applications that can help improve efficiency, offer a differentiated service and grow revenues by increasing customer loyalty and attracting new guests. In this section, key hospitality applications and associated system requirements are identified.

### **Voice over WLAN (VoWLAN)**

VoWLAN is poised to become a major hotel industry application. Hospitality industry staff are constantly on the move. Cleaning crews, room service, and valets require a method of mobile communications to increase productivity and guest satisfaction. With “Voice over IP” (VoIP) infrastructure and 802.11 there is the benefit of a converged voice and data network. Alternate methods of enabling mobile voice (e.g. in-building cellular, DECT) are cost prohibitive and require a separate radio network.

VoWLAN devices may consist of handsets (e.g. Spectralink), wearable badges (e.g. Vocera), dual voice & data messaging devices (e.g. RIM BlackBerry 7270), and PDAs with “softphone” clients. More information on VoWLAN client devices & benefits to hotels can be found at:

[http://www.vocera.com/PDF/Hotel\\_case\\_study5\\_05\\_05.pdf](http://www.vocera.com/PDF/Hotel_case_study5_05_05.pdf)

<http://www.spectralink.com/files/literature/Major%20Markets%20Hospitality.pdf>

<http://www.blackberry.com/products/blackberry7200/blackberry7270.shtml>

In addition, VoWLAN introduces the concerns of ensuring Quality of Service (QoS) and secure mobility on an integrated network. The use of “soft phone” client technology and devices like the RIM BlackBerry 7270 can help maximize the utility obtained from mobile computing devices, but the QoS mechanism must be able to distinguish between voice and data streams generated by the same device. Providing an optimal environment for VoWLAN demands a system capable of maintaining good coverage (i.e. minimizing signal dead zones) by dynamically reacting to interference sources. Secure mobility demands that an 802.11i authenticated/encrypted device can undergo seamless, fast handovers between APs, even ones sitting on different subnets, without dropped calls or voice quality degradation. In addition, E911 regulations demand the ability to provide a physical location for callers.

---

## **Guest Check-in “Queue Busting”**

Guest check-in and check-out, limited to the front desk, can result in long queues and frustration for guests. With a WLAN, available staff can be conscripted into the process and check-in guests from anywhere using an 802.11 enabled device with credit card reader (e.g. Xybernaut Atigo web tablet).

This application, especially where credit card information is being handled, requires best in class security. Best practices in most hotels today demand the implementation of 802.11i authentication/encryption and the ability to detect “rogue” APs.

## **Order Taking & Point of Sale (PoS)**

Room service and wait staff can utilize 802.11 enabled devices to take orders anywhere (e.g. rooms, lounges, restaurants, pool side) and submit them to the kitchen remotely. Digitized orders can reduce the occurrence of errors as well as increase guest satisfaction by reducing the time required to deliver meals.

Untethered Point of Sale (PoS) devices can be used to reduce the amount of time wait staff must spend in transit between cash registers and guests. Wireless enabled registers can be placed outside to serve poolside guests and outdoor cafes. As with wireless check-in, this application demands the highest level of security to ensure the secure processing of credit card transactions. Shared WEP keys are simply inadequate and a WLAN solution that supports WPAv2 and wireless intrusion detection is a must.

## **Mobile Room Audit/Inspection**

Maintaining customer loyalty demands the delivery of a consistent high quality experience. WLAN capable PDAs and tablets can be used to help streamline the room inspection/quality control process and continuously update the front desk on room status. The inspector can instantly identify deficiencies for maintenance and deploy cleaning staff to rectify issues prior to the check-in of new guests.

## **802.11 Asset Tracking/Location**

The ability to track the position of critical, expensive assets (e.g. room service carts, tablet PCs, projectors for meeting rooms) can help increase productivity and prevent the loss of equipment. E911 requirements demand the ability to locate callers who are using 802.11 phones.

## **Wireless Door Lock Maintenance/Monitoring**

Guest safety and loss prevention is of paramount importance and figures greatly in hotel brand value. 802.11 interfaces in electronic door locks can be used to remotely track guest room entry and

reconfigure card key readers. Wired alternatives would be cost prohibitive and highly disruptive to hotel operations.

## Wireless Casino/Gaming

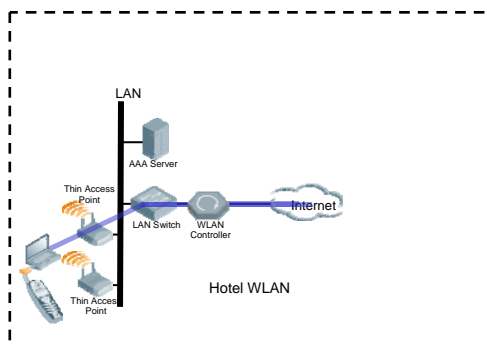
Hotel casinos may choose to offer wireless PDAs to patrons so that they may gamble throughout the premises (e.g. hotel rooms, bars, lounges, restaurants). This application has the potential to increase revenues by making gaming activities more accessible to guests. As in the case with Point of Sale (PoS) devices, gaming applications require best in class security. A WLAN solution that supports WPAv2 and wireless intrusion detection is a must.

## Current Infrastructure Limitations

Some hotels deployed legacy, “fat” individually managed APs and experienced numerous difficulties/issues:

- **High Impact to Wired Network:** The installation often required significant reconfigurations and upgrades to the wired network to introduce WLAN
- **High TCO:** “Fat” APs must be individually managed. As a hotel deployment grows this can mean hundreds of additional devices to manage resulting in high operations and maintenance costs.
- **Limited Mobility:** VoWLAN & data require fast handovers between APs and subnets. The ability to support fast handovers for 802.1x devices required proprietary key exchange mechanisms in the client device. Furthermore, intersubnet mobility required an expensive module for the wired network switch
- **Theft:** There is incentive for theft of “fat” APs located in public places as they function independently and as such can be resold illicitly.

## Benefits of a Centralized WLAN Architecture



**Fig 2: Centralized WLAN architecture for the Hospitality Services Industry**

---

The difficulties experienced by hotels with legacy AP deployments suggest that a “centralized” architecture consisting of “thin APs” and a centralized “controller” would present the optimal approach to WLANs. Centralized WLANs have numerous advantages over “fat” AP deployments:

### **Lower Deployment Cost**

A hotel/conference center deployment of “fat APs” supporting internal data, voice, and guests would require that existing wired infrastructure be upgraded or reconfigured to support multiple VLANs. The centralized architecture does not require any disruption to the installed wired infrastructure. WLAN traffic is tunneled (i.e. IPSec or GRE) from the thin APs to the central controller where traffic is aggregated.

RF site surveys constitute a significant portion of deployment costs in hotel environments. First generation “fat APs” have static RF management capability that have to be run at specific times and can not react dynamically to changing conditions. With a centralized architecture, APs can continuously monitor the RF environment and send radio measurements to the central controller which can detect coverage holes, interference, and WLAN congestion on a real time basis. If these are detected, the controller can automatically re-compute the optimum RF plan for the network and implement the new plan by automatically changing the APs’ channel assignment and transmit power levels. In the event of an AP failure, the WLAN system automatically alters adjacent AP settings to ensure no loss of signal coverage.

### **Lower TCO**

A typical large hotel deploying WLAN throughout the premises to support voice and data may require between 50-100 APs. With 1<sup>st</sup> generation “fat APs”, each AP must be configured and managed individually. Any configuration changes require that an updated configuration be pushed to each individual AP. With a centralized architecture, configuration changes are made at the controller. For example, to implement 802.1x on a hotel network of 100 “fat APs”, all 100 APs must be configured. With a centralized architecture, only the controller must be configured.

The centralized approach has the potential to reduce the upgrade costs associated with the introduction of L2 and encryption enhancements. For example, hospitality customers desiring AES will in many cases have to completely replace their 1<sup>st</sup> generation fat APs . With a centralized system encryption is implemented in the controller rather than in the AP. This means that if there are any enhancements to encryption technology, it is the controller rather than the APs that is upgraded.

### **Tighter Security**

Mobile PoS/ guest check-in applications demand that hotels implement secure WLANs. With “fat APs” the possibility of improperly configuring a subset of devices and compromising the entire

---

network is very real. Using a centralized approach to the management and control of APs, this threat is minimized. All security policies are configured and enforced at the controller.

Aside from the secure 802.11i authentication and encryption of clients, the need to protect Point of Sale(PoS)/check-in/gaming information demands the detection and prevention of various vulnerabilities and over the air attacks (e.g. rogue APs, ad-hoc networks, Man in the Middle, Denial of Service). Wireless intrusion detection capability is necessary to mitigate the risk of these attacks. IT decision makers should select a centralized WLAN where data, in addition to control traffic, is encrypted between APs and controllers.

Access to the network and security policies should be configurable at a user or group (e.g. hotel management, security, maintenance, and guests) level. This capability allows the network manager to identify any distinct roles, with associated access rules, and then to assign each individual to a role, depending on their business needs. For example, guests should not have access to the intranet but should be able to connect to the internet by supplying a login password at a captive guest portal. The centralized WLAN can ensure complete separation between internal data and guest hotspot traffic. An identity based, stateful firewall implemented in the controller ensures that security policies “follow” the user as they move throughout the network.

An additional benefit of the centralized architecture with thin APs is that it reduces the incentive for theft. Stolen thin APs, unlike “fat” APs, cannot function without a controller and hence have an insignificant black market value. Furthermore, this architecture eliminates the possibility of security keys being extracted from stolen APs.

### **Fast/Secure Mobility**

Mobility is indispensable to the delivery of superior service when and where it is desired by guests. WLAN enabled applications can help differentiate service and increase revenues.

Low latency mobility is critical for many applications (e.g. VoWLAN). Inter-AP handover of 802.11i and VPN secured devices must be handled in such a way as to minimize latency and degradation of voice quality. In 1<sup>st</sup> generation “fat AP” networks, non-standard client modifications were required to enable “fast handoff”. Implementations that require modifications to the client to enable mobility will greatly increase the cost and complexity of WLAN deployments. Inter-subnet mobility required the purchase and installation of expensive switch modules. With a centralized architecture, all traffic is tunneled back to the controller which enables fast handoff between APs and subnets.

### **QoS and the Multi-Service Network**

Hospitality WLANs must serve different classes of users (e.g. staff, guests) and applications (e.g. voice and data). It is critical that limited bandwidth resources be allocated appropriately. A centralized system that supports the end-to-end QoS required for multi-service applications, checking the legitimacy of client priority requests by following the voice signaling stream, and

---

respecting relevant L2 and L3 QoS tags is necessary to support the demands of a hotel deployment. Other desirable capabilities for voice include call admission control based on the number of active calls on an AP and bandwidth control to limit the amount of bandwidth lower priority devices (e.g. guest laptops) can use.

“Soft phones” on PDA/Tablet PCs are likely to be used for voice communications. Unlike VoWLAN handsets/badges, these devices generate both voice and data traffic. A legacy WLAN system would incorrectly classify all traffic from such devices as either data or voice. The ability for the WLAN to be able to distinguish between voice and data traffic generated by a single device is necessary to ensure that 802.11 frames are assigned the appropriate priority.

### **Location**

The WLAN should provide the capability of tracking 802.11 enabled devices/tagged assets in high density “grid” AP deployments without the need for time consuming/expensive location site surveys. For less dense deployments of APs, the WLAN solution should be able to support external location servers.

## **Critical WLAN AP Hardware Requirements**

Hotel Industry IT Managers should consider these to be the bare minimum requirements when selecting AP hardware for their centralized WLAN:

- **Flexible AP Mounting & Antenna Options:** Many hotels are concerned about aesthetics, and as such demand multiple mounting options. The ability to support above the ceiling installation while complying with local safety codes may be a requirement in some deployments. The supplier’s hardware portfolio should include both low profile/small form-factor APs with integrated antennas and APs with antenna connectors.
- **Dual 802.11g & 802.11a support:** APs should support 802.11g (which is backwards compatible with 802.11b) and 802.11a to ensure that all clients are supported.
- **Outdoor AP:** It is highly desirable to have an outdoor AP that can be used to provide coverage for the hotel grounds so that guests/staff may access the WLAN from outdoor cafes, pool areas etc.

---

## Conclusion

WLAN technology can help hospitality venues create differentiated services that reduce operational expenses, improve customer satisfaction, increase brand value and drive the growth of revenue. Business and leisure travelers now view Wi-Fi connectivity as a necessity, one that influences their choice of lodging.

WLAN systems for the hospitality industry must be capable of supporting critical internal applications (e.g. VoWLAN, check-in, room audit) and providing guests with connectivity on a single network while maintaining complete separation between internal and hotspot traffic. The sensitive nature of credit card Point of Sale/check-in transactions and gaming applications requires that IT managers institute policies that vigorously guard against the interception of data. VoWLAN demands the ability to support end-to-end QoS, Call Admission Control, and fast inter-AP/inter-subnet mobility. Deployment of the “centralized” WLAN architecture, with “thin” APs managed by a controller, is the best way to support hospitality applications while ensuring network security.

In addition to superior performance, the centralized architecture offers a compelling Total Cost of Ownership (TCO). This approach to WLAN eliminates the need for costly wired switch upgrades and minimizes the expense required for manual RF site surveys. Ongoing maintenance costs are reduced by the centralized architecture which scales down the number of distinct devices that must be individually managed. The ability to serve both hotspot and internal applications on a single network increases the Return on Investment (ROI) for WLAN.

## About Aruba Networks

Aruba securely delivers the enterprise network to users, wherever they work or roam, with usercentric networks that significantly expand the reach of traditional port-centric networks. Usercentric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable followme applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.

WP\_HOTW\_US\_071217