



Introduction

Internet access is no longer just another amenity at the hotels, it is a necessity for travelers and alike. A definite requirement for hosting business events. Hospitality establishments aiming to maximize profits are doing as such by providing 3G/4G offloading of smart phones and remote office connectivity for business men and women. In addition to providing guest with wireless internet connectivity, hotel can offload many pertinent operational aspects of the business onto the Wi-Fi network.

With Inscope Data SB3000 access solutions, hotels will need less access point per deployment due to stronger Wi-Fi signals and high performance connectivity which allows the hotel to offer high level of service by using mobile Wi-Fi devices to securely access reservation and administration tools from anywhere on the property. Wireless point of sale (POS) systems allows the hotel to offer pool side and offsite accommodation and services efficiently with onsite transactions and order taking. Wireless valet parking system, guest Wi-Fi anywhere including pool or beach side connectivity, and host of applications increase value and guest retention of the hotel property.

Wireless broadband access

Savvy business travelers demand Wi-Fi access and often have the requisite capability to connect to remote networks. 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 standard base wireless laptops are widely available, they vary significantly in terms of certification level. Hotels should not require more than the most basic Wi-Fi certified 802.11 network interface and a web browser. Requiring Wi-Fi WPA or WPA2 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 where login instructions and, optionally, legal disclaimers are provided.

Among several ways for hotspot access are:

- Wide open - 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.

- **Pay per use:** The hospitality venue may decide to offer fee based hotspot access. A hotspot access controller 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.
- **Multi-tiered Service Provider mediated access:** All the traffic from the guest hotspot SSID can be re-directed to a service provider which controls access and assumes responsibility for billing.

The typical internet usage charge in the United States is about \$8-\$15 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.

Hotel applications

To setup a wireless LAN entirely for internet 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 outlined.

- Hotel guest services, limited to the front desk, can result in long queues and frustration for guests. With a wireless LAN, available staff can be conscripted into the process and check-in guests from anywhere using an 802.11 enabled device with credit card reader. 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.
- Voice over wireless LAN is poised to become a major hotel industry application. Hospitality industry staffs 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.
- Point of sale service and order taking tasks can utilize 802.11 enabled devices to take orders anywhere 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.

- Access control via wireless like door lock maintenance, guest safety, and loss prevention is of paramount importance and figures greatly in hotel brand value. Access control, using 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.
- Hotel room inspection and periodic audit increases quality of service and provide consistent high quality experience for hotel guests. 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.
- RFID - The ability to track the position of critical, expensive assets 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 gaming keep hotel guests entertained as patrons moves throughout the premises. 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.

Hotel wireless LAN Requirements

The following are a minimum requirements when selecting wireless AP hardware for the hotel wireless network:

- Long range 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.
- Flexible deployment location: 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 band wireless AP: APs should support 2.4GHz 802.11gn and 802.11an to ensure that all clients are supported.

Conclusion

New wireless LAN 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 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. Voice over wireless LAN 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.

Inscape Data continues its tradition with the next generation wireless products to meet the high demand environment of IP video security and wireless networking industries. With equipment maintenance cost high on the list of company expenses, the AirEther™ 802.11a/b/g/n MIMO wireless systems are easy to install. When used with Inscape Data's LPS2000 or LPS series Outdoor Adjustable Voltage PoE Switch or commercial PoE injectors, PIS200, PIP100, and PES100, the AirEther 802.11a/b/g/n MIMO products provide rugged reliable wireless interconnectivity of mission critical IP video surveillance and networking functionality.