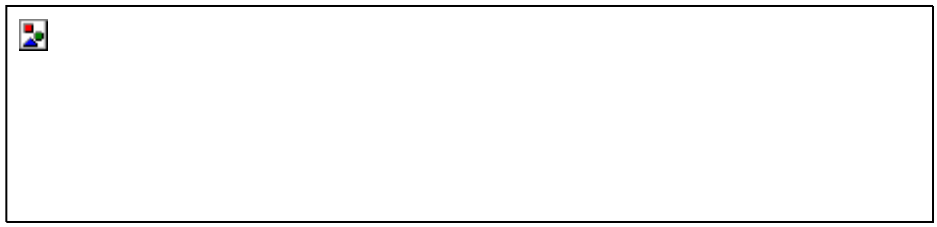


A Guide for Understanding Wireless in Hospitality
An HTNG White Paper

Hotel Technology Next Generation

August, 2013

THESE SPECIFICATIONS AND/OR SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF, OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

These specifications have not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed

A Guide for Understanding Wireless in Hospitality
An HTNG White Paper

Hotel Technology Next Generation

Edited by:
Jayne O'Neill, Management Consultants

Contributors:
Joseph Bartelo, Lorica Solutions
Randy Currie, SolutionInc
Greg Dawes, Zhone Technologies
Angela Landon, Cisco Systems
Lee McKenna, LodgeNet
Jayne O'Neill, Management Consultants
Tim Ross, Datanamics, Inc.
Dick Wagner, Marriott International
Bruce Wolf, Royal Caribbean Cruises Ltd.

Copyright © 2006 Hotel Technology Next Generation. All rights reserved. Reproduction, redistribution, or electronic storage of this material to or by persons who are not current members of (or employees or Corporate members of) Hotel Technology Next Generation, is prohibited without the express written permission of Hotel Technology Next Generation. U.S. law provides statutory penalties of up to $150,000 for each incident of copyright infringement.

Table of Contents

I. Choosing a Wireless Network

For many years hotels have offered Wireless Fidelity (Wi-Fi) to their guests, typically in common areas and only to provide high speed Internet access (HSIA). As wireless security has improved and wireless applications have become more commonplace, the hospitality industry must now grapple with the fact that guests are truly mobile workers demanding reliable, secure wireless access. Today, hoteliers can expand on their existing technology to take advantage of wireless networks and enable services that go beyond providing Internet access alone. .[1] With the proliferation of wireless handheld devices, business and vacation travelers logically expect wireless access during their stay. The increasing demand created by these guests influences how hoteliers will provide this service, what type of wireless they will deploy and whether it will be free-to-guest or revenue generating.

Hotel Technology Next Generation makes this convergence white paper available to hospitality companies interested in deploying wireless networks. In addition to answering general deployment questions, this paper will discuss various wireless technologies which exist today and those that will be available in the near future. An extensive glossary is also included to help readers better understand the terms used in this wireless world.

[1] Karin P. Koser, *Business Conveniences for Guests: All the Comforts of a Temporary Office Away From Home*, 1/26/2006

A. Wireless for a Superior Guest Experience

Real-time events demand a real-time response and providing superior customer service is the number one focus for the hospitality industry – this extends from the service provided by the staff to the quality of the product offered to the guests. In the past, many hoteliers have shied away from wireless because of overriding security concerns and the general inconsistency of the wireless service. Today, security issues have largely been alleviated through the widespread use of Virtual Private Networks (VPN) and encrypted Wi-Fi Protected Access (WPA, WPA2). Service quality can be addressed through a complete Project Plan that includes an accurate site survey and proper execution of infrastructure design and installation.

A wireless network makes it possible for hoteliers to offer curbside check-in, just-in-time maintenance and housekeeping response and more efficient restaurant, spa and resort services. It enables guests to connect to the Internet, read email, view web applications and enter private networks from any location on the hotel property. Wireless handheld and voice applications are rapidly being developed and these will offer even more services to the guests and hotel staff – all with the goal of increasing guest loyalty, improving efficiencies and generating revenue.

As discussed in the white paper *Convergence: Hotel Technology for Today and Tomorrow,* [2] the advanced communication and wireless capabilities provided by a converged network allow hotels to offer new or improved communication and entertainment services to their guests. A wireless network allows the distribution of guest information across many systems to improve and personalize guest services. This is well beyond the capabilities of today's non-converged IP Telephony, Internet and video offerings. A wireless extension of this highly intelligent and connected network allows the hotelier to offer much more than just high-speed Internet access to guests.

[2] Hotel Technology Next Generation, *Convergence: Hotel Technology for Today and Tomorrow* June 2005

1. Location Based Services

Location based wireless services facilitate instant interaction with guests by enabling hoteliers to make information available to the guest through a web-based portal by "pushing" information directly to the guest's portable device. These services are based on the ability of a wireless device to determine its exact position and then use that knowledge to perform functions or provide information based on location, either through Global Positioning Services (GPS) or by registering to a specific access point to permit well timed service delivery. Based on the guest's profile and location, hoteliers can effortlessly deliver a host of messages through location based wireless handheld devices such as providing notification of special promotions; delivery of hard to get information on entertainment and activities or advising guests of upcoming, unscheduled events. The services can include assisting guests in dining availability status; sign-in for conventions and meetings through deployment of temporary kiosks; and registration through either curbside check-in or well-placed registration desks during peak hours. Hoteliers can deliver time sensitive messages, important facts or general information in a simple manner through this wireless service.

2. Instant Access Services

One of the main benefits of wireless is that it allows instant access to the Internet and IP Telephony services from anywhere on the hotel or resort property. Properly engineered, the guest can effortlessly access the public Internet, private network, or voice mail as well as IP Telephony service from the guest room, lobby, conference center, poolside or golf course. Guests LBS enabled systems can be notified of last minute availability at the spa or of an upcoming dinner reservation while relaxing poolside; and sports enthusiasts can follow the leader board from anywhere on the course at a resort hosted golf tournament. Wireless services provide many new ways to interact with guests and staff.

3. Temporary Networks and Services

The ease of deploying wireless access allows hoteliers to offer temporary data networks to conference customers. A wireless extension of the hotel's converged network provides an easy, dynamic means to offer Internet access and the temporary data networks make set-up and tear-down quick and responsive to customer needs.

Convention services are further enhanced through wireless location based services that allow hoteliers to notify customers via Wi-Fi telephony mobile phones or personal hand held wireless devices of upcoming and timely information.

4. Workforce Mobility Services

Wireless workforce mobility services enable hotel staff and management to be more responsive to guest needs by breaking the chains that keep them bound to reservation desks, business centers and back offices. Wireless networks provide operational efficiencies and enhance many applications while providing remote access to guest profile information via wireless IP Telephony or paging systems.

Hotel staff can take advantage of this intelligent network to get secure access to timely information regardless of their location in the hotel while allowing dispatch of services such as housekeeping or maintenance to be conducted more efficiently.

5. Point-of-Sale Services

A wireless enabled hotel restaurant and bar allow for some new and exciting point-of-sale applications. With wireless order taking, waitresses can stay on the floor attending to customers while runners bring food to diners. This is especially useful in situations where the kitchen is located some distance from the guests dining - as is common in many resort properties.

New applications have also been developed to track in-room minibar sales and product expiration dates via wireless. With wireless tracking, no revenue is lost through manual errors found with the traditional honor bar system.

6. Wireless Service Summary

Wireless service delivers the agility required to respond to new or changing guest requirements. A comprehensive wireless network allows not only the expected access to the Internet, but can be used to enhance the guest experience greatly by offering a wide variety of services both free and revenue producing.

Additionally, tremendous efficiency can be realized by the hotel from a service standpoint. Necessary services such as housekeeping, maintenance, concierge, check in - check out, security operations, and many others can be streamlined to provide the guest easier access to these services and by offering the hotel a means of accomplishing them rapidly and with less labor effort.

II. The Wireless Infrastructure

For the purposes of planning and implementation, a wireless infrastructure for hospitality can be compared to a wired infrastructure. Both should be well defined in the scope of work and propose not only to meet present needs but also to remain flexible and open to improvements in technologies to accommodate future needs. The wireless infrastructure may be as basic as a standard 802.11 HSIA implementation or as complex as an integration of mobile phones, HSIA, 802.11 phones and messaging systems along with 802.11 applications support, capability for device interconnection, and support for future wireless specifications.

Wireless infrastructure discussed in this white paper focuses on service for two types of hospitality properties; a high-rise hotel consisting of a single building with twelve or more floors and a resort property that typically includes a main building with six to twelve smaller buildings distributed throughout a large area.

A. Service Requirements

A hospitality environment has unique requirements that other, more static wireless networks do not have. In addition to wireless access points, it includes a need for the network to provide user-to-user security while allowing open and easy access for guest areas. It should also provide discretionary multi-purpose application options such as HSIA, IP Telephony, VoD, and video surveillance converged over the same wireless infrastructure. Segmentation, QoS / prioritization, and security for all applications must also be included. If the network includes billable services, it should provide billing options to the room and credit card. Existing and future equipment needs should be documented and maintained along with a diagram of the existing wireless devices at the property with any planned wireless coverage areas noted.

1. Site Survey

Implementing a reliable and extensible wireless network requires a properly designed Project Plan so that its capabilities can be extended into the future. The plan should consider factors such as security, capacity, future applications and user device requirements. Since all communication will run over a converged network it's important to recognize the different types of users, their traffic and devices. Investment in the proper equipment that supports wireless service capability for all users will cost far less than the future replacement of a simple and / or inferior network. Users ranging from guests, management and staff collectively benefit from wireless networks and the plan should consider their usage when conducting the site survey.

.

The site survey engineer should simulate coverage by positioning access points and recording resulting coverage and It should be noted that high-rise buildings are often susceptible to coverage problems because of construction type and the amount of steel and concrete inside the building. Reflective glass covering and tinting may also impact signals inside buildings. An accurate property map should be created showing coverage and identifying areas that need improvement in coverage.

A variety of materials can cause interference for wireless signals and hinder the effectiveness of the implementation. The site engineer should consider this issue when conducting the site survey. The more common types are described below.

Material	2.4GHz Signal Attenuation
Window	25%
¼" Wood Veneer	40%
Sheetrock Wall	50%
Cinder Block Wall	65%
Glass Block	75%
Metal Door	75%
Ceramic Tile	75% – 90%
¾" Pressboard	90%
Granite Tabletops	95%
Mirrored Closet Doors*	95% – 100%
Silvered Mirrors	100%
Chrome or Metal Objects	100%
** Signal primarily reduced by reflection in direction of travel*	

Figure 1: Infrastructure Material and Signal Strength

III. In-Building Solutions

Once the site survey has been completed, alternative connection methods should be considered. Compliance with regulations of the FCC or other appropriate regulatory group and approval by the carrier should be well thought-out prior to installation, testing, or implementation. In building connection solutions such as Distributed Antenna System (DAS), Mobile Phone Repeater and Backhaul for wireless are described in the following sections.

A. Distributed Antenna System (DAS) Solution

The key elements of a DAS include an open wireless architecture that provides coverage for areas that typically are difficult to reach. These systems can cover an area of several floors to many floors or areas within a complex environment.

The system supports all carrier and Wi-Fi transmissions and is very useful for hospitality properties by improving cellular telephone coverage for guests. The system extends and propagates external, and in some cases internal, wireless signals to provide improved signal strength and coverage.

The application can also improve hotel staff communications when using wireless in the 900 MHz spectrums, as well as improve coverage of wireless telephony or data systems in the 2.4GHz spectrum.

Typically, wireless implementations are vendor specific and proprietary systems with little interoperability. However, by their nature, DAS supports numerous wireless standards like AMPS, TDMA, GSM, E-GSM, CDMA, WCDMA, iDEN and WLAN, and operate in standard radio frequencies in the range of 800MHz through 2500MHz.

1. Active DAS

Wireless signals are brought into a central location or "head end" from either an Off-Air or Micro-Cell signal method[3]. This head end is typically in the existing main distribution frame (MDF) located within the properties phone room.

Once the signal is received by the head end, the active DAS can then propagate it throughout the rest of the building following the process below:

- A **Radio Interface Unit** (RIU) interfaces with each of the signals acquired from each carrier.

- The **Base Unit** (BU) receives the signal from the RIU and converts the radio frequency (RF) signal to an optical signal. The BU is connected to a network controller that manages the frequencies and devices on the internal network. The carrier's optical signals are on different frequencies which allow clean transmission over a single fiber connection from the head end to remote locations and can be multiplexed and combined with other carrier's signals.

- An **Optical Backbone** uses fiber optic cable to transmit the optical signal, providing a low-loss infrastructure that transmits over long distances.

- A **Remote Hub** receives the multiplexed optical signals and converts them back to electrical RF signals. The remote hub can decode each RF signal and then re-create it for wireless transmission over antennae.

The active DAS system can not only provide signal propagation for mobile phones but can also include 802.11 (Wi-Fi) varieties over the same DAS.

.

[3] Off-Air and Micro-Cell Signal Methods are described on Page 16 of this white paper

2. Passive DAS

The Passive DAS solution works in a fashion similar to the Active DAS. With either an Off-Air or Micro-Cell signal method, both active and passive antenna solutions must have signals brought into the building for all carriers to be covered. The passive DAS process begins after the signals have been received in the head end through one of the two signal access methods. Once the signal is received, the DAS can propagate it throughout the rest of the building following the process below:

- An **Integrated Access Device** (IAC) combines the signals from all carriers' that are to be covered and transmits over a single cable.
- A **Bi-Directional Antenna** (BDA) provides signal power to a vertical coax cable that penetrates all floors. The vertical coax is a larger low-loss type cable that can go straight up through a stacked IDF system.
- A **Radiating Coax Cable** runs horizontally throughout each floor, propagating the signal. This leaky-type coax cable acts as the antenna on each floor, propagating the separate frequency of each carrier over the single cable.

The cable can also propagate 802.11 (Wi-Fi) signals. A maximum of three 802.11 wireless access points can be added to the radiating coax antenna of each floor. The radiating coax cable connects to the main vertical coax cable via a cable tap that allows the radiating antenna to receive and propagate the wireless signal.

A passive DAS In-Building Wireless System solution is shown in Figure 2 depicting the process of wireless signal transmission throughout the interior of a multi-story building.

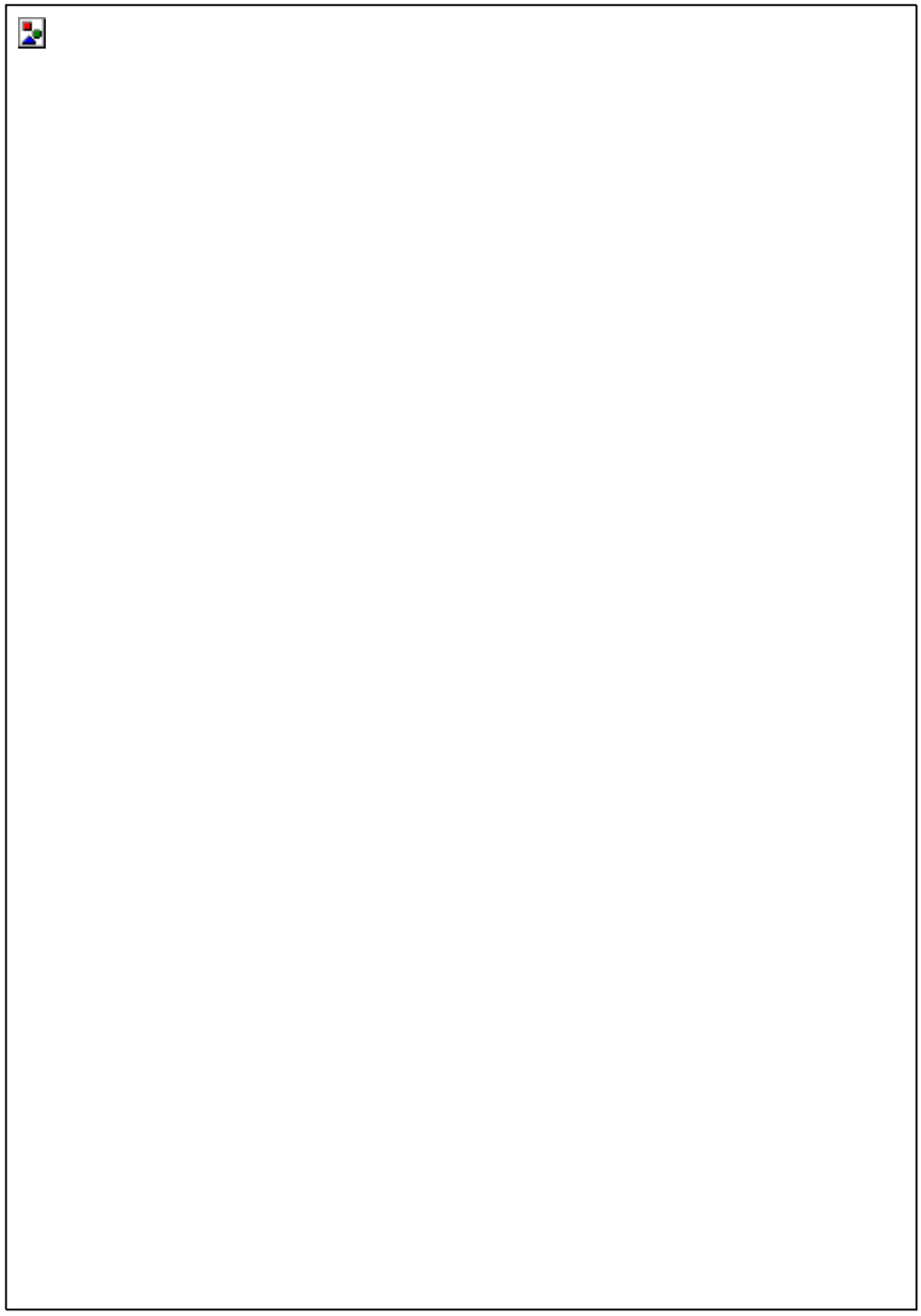


Figure 2: In-Building Wireless System

B. Mobile Phone Repeater Solution

An alternative to active and passive DAS solutions for connectivity is a Mobile Phone Repeater solution which is basically a bi-directional amplifier that uses a cable to connect to an antenna outside a building and a second cable to an area within a building.

The solution supports the use of mobile phones - therefore the need for investment in wireless service to support coverage is obvious. Mobile phones provide the core communication for today's business and vacation traveler. Most guests expect to have the ability to use their phones wherever they are, if they cannot, perception of the property is impacted. This view may not necessarily result in an early checkout, but it can affect the guest experience, resulting in a lower frequency of return stays. Considering overall customer satisfaction, the capital outlay for wireless may well be considered a worthwhile investment.

Unlike the mobile phone repeater which receives a signal and retransmits it throughout the interior of a building before sending it back outside, the DAS solution is designed to propagate signals to every area of a hotel property and may carry multiple frequencies, such as 802.11 in addition to mobile phone frequencies. A repeater solution is much less comprehensive than DAS and is designed to simply repeat an existing signal from off-air, outside a building to a specific area within.

Wireless mobile phone repeater solutions should access licensed frequency bands. Installation should be compliant with regulations of the FCC or other appropriate regulatory group and approved by the mobile phone carrier prior to installation, testing, or implementation.

The Mobile Phone Repeater solution is ideal for a hotel with sufficient coverage in all areas of guest rooms, but requires additional coverage inside certain areas such as meeting rooms. The frequency of each carrier's service must be repeated and it should be noted that in order to supply mobile phone service, the carrier's coverage must be available at the property. If a carrier's signal is not present outside the building, it cannot be brought inside the building without a hard wired connection such as a dedicated T1 to that carrier. There are some properties, particularly resorts in more remote locations with little or no mobile phone coverage available in the area. Providing service to guests in these cases can become quite costly.

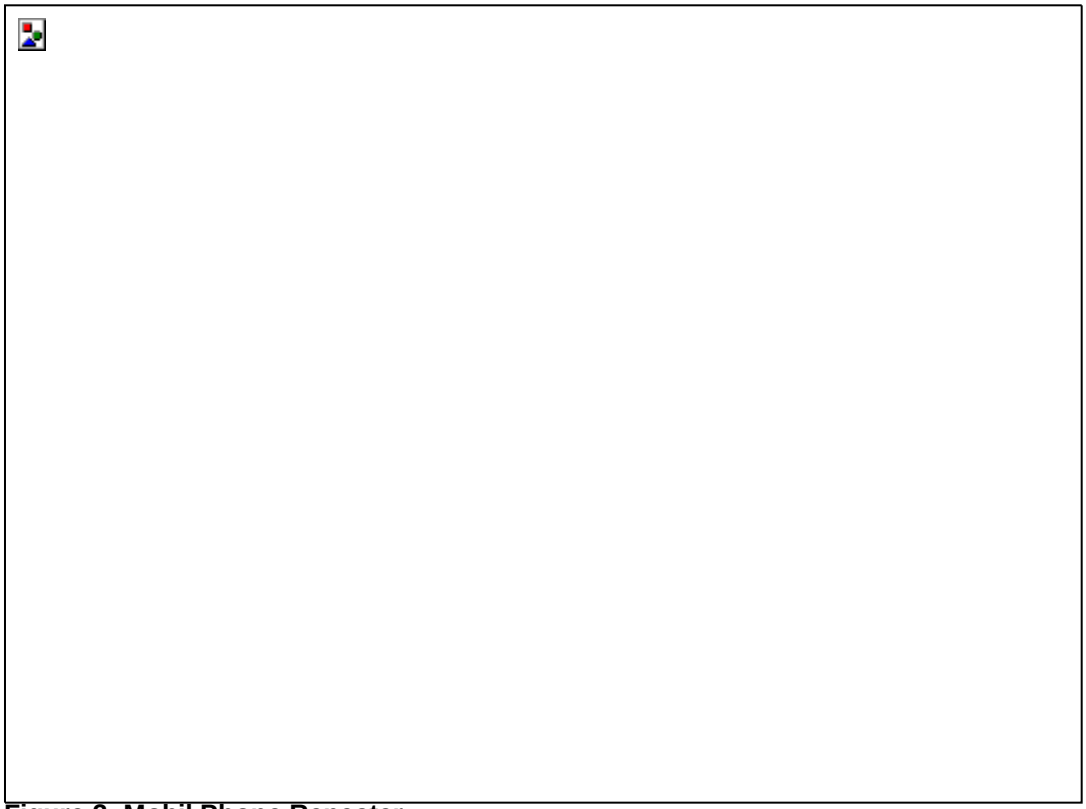


Figure 3: Mobil Phone Repeater

C. Method of Infrastructure Backhaul

Alternative connection methods called the "backhaul" are used when the in-building DAS at one site does not have a "wired" infrastructure to connect the users to the client LAN, Internet or another DAS site. The site survey should provide a property map with locations for radios and antenna to cover the hotel or resort environment. Planning should include using one of two signal methods which will get the wireless signal inside the property and distribute it effectively to the antenna. The Off-Air and Micro-Cell signal methods are described below.

1. Off-Air Method

An Off-Air method requires an antenna outside the building (donor antenna) which communicates with a carrier's existing cell tower to obtain a signal to propagate inside the property. A Yagi antenna or other directional antenna can be used for the donor antenna. Installation of an off-air solution should be compliant with regulations of the FCC or other appropriate regulatory group and approved by the mobile phone carrier prior to installation, testing, or implementation.

2. Micro-Cell Method

A Micro-Cell method requires bringing a wired circuit such as T1, or Fractional T1 into the building from each carrier and propagating the signal throughout the building. This is similar to providing a carrier's dedicated cell tower to the building, but delivers a better means of ensuring access is available. This method is usually more expensive because of the cost of providing carrier circuits to the location.

IV. 802.11 Wireless Networks

802.11 wireless networks are critical for the hospitality environment. All major branded hotels now require franchisees to provide wireless HSIA to guests. The wireless 802.11 network though, can serve many purposes and a well-planned network can provide a wide array of services that can generate revenue and provide an attractive return on investment (ROI) while greatly improving the guest experience.

A successful 802.11 site survey and implementation requires a good understanding of the scope of work prior to beginning. If flexibility and future application support are important to a successful implementation, then all resources for keeping the network scalable should be understood and utilized. If flexibility is not desired and a project's main goal is meeting the need of a single application with a budgetary constraint, all existing resources should be used to restrict the project cost. Problems can arise with "scope creep," which occurs when the implementation plan is described as single purpose, such as to provide HSIA at a low cost, and the property decides at a later date that multiple applications should be added. These higher-end technical solutions offer more diverse capability and can include: separate service set identifier (SSID) technology which enables communication between users and the access point, Virtual Local Area Network (VLAN) which provides an independent network, and higher levels of security. Any alteration in the scope of work to include these solutions can result in greater costs, therefore, accommodating future needs through added features must be considered upfront.

A. 802.11 And Wi-Fi Networking Technologies

In terms of wireless networking, 802.11 and Wi-Fi are used interchangeably to describe wireless networking technologies. In the hospitality industry, Wi-Fi networks are the standard for guest high speed Internet access. Wi-Fi devices use small radios to communicate and send information back and forth at speeds ranging from 1

Megabit per second (Mbps) to 150 Mbps with a single stream and triple that for 802.11n clients supporting MIMO

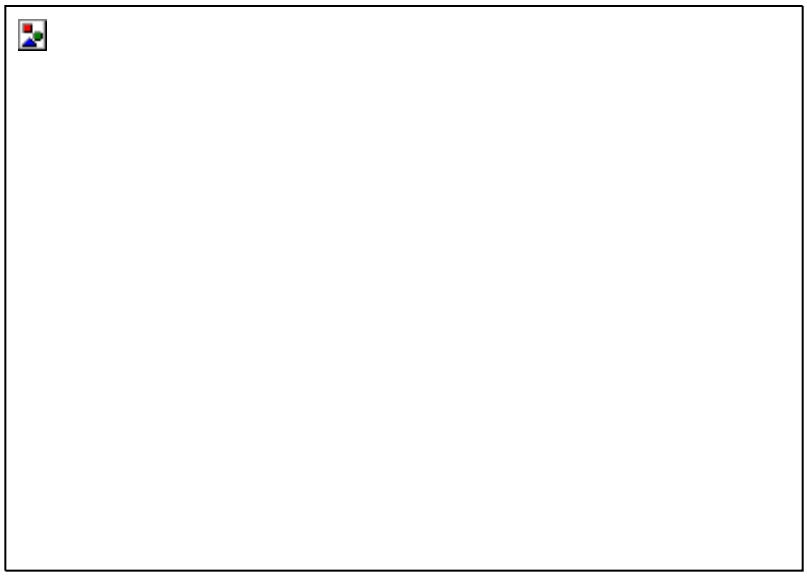


Figure 4: Signal transmission of 802.11 and Wi-Fi

802.11 wireless protocols are based on the IEEE 802.11 wireless standards adopted in 1997. The standard addresses some of the limitations of using wireless technologies for Ethernet transmissions and takes into consideration range limitations and interference from other radio signals. This specification describes the over-the-air communications interface between a wireless client and a base station or between two wireless clients.

Wireless Networking Technologies	
802.11b	The 802.11b is the first commercial release of wireless networking technology. It operates in the 2.4 GHz frequency. The system communicates at speeds up to 11 Megabits per second, but will fall back to speeds of 5.5, 2, and 1 Mbps depending on interference and the distance between devices.
802.11a	This 802.11a release of the technology operates only in 5 GHz and can transfer data across a wireless network at higher communication speeds (54 Mbps).
802.11g	The 802.11g is a mix of both 802.11b and 802.11a technologies. The 802.11g operates in the 2.4 GHz band, but can operate at the 54Mbps speed.
802.11b/g	Devices that operate using the 802.11 b/g protocols will interoperate with wireless devices that communicate using the 802.11b or 802.11g standard.
802.11n	Currently the standard in wireless networks. Supported on both 2.4GHz and 5GHz, 802.11n offers an increase of up to 6 times the speed of the 802.11g technology.
802.11ac	Next Generation of the 802.11 technology. 802.11ac will operate only in 5 GHz, support higher data rates and Multi-User MIMO.

Figure 5: Wireless Networking Technologies (802.11 series)

802.11ac Enhancements

5 GHz Only	Compels device manufacturers to adopt 5 GHz, improving performance, reliability, and overall capacity for the entire Wi-Fi ecosystem
256-QAM	When Wi-Fi signal quality is very good (very close to the AP), more efficient modulation increases data rates by 33%

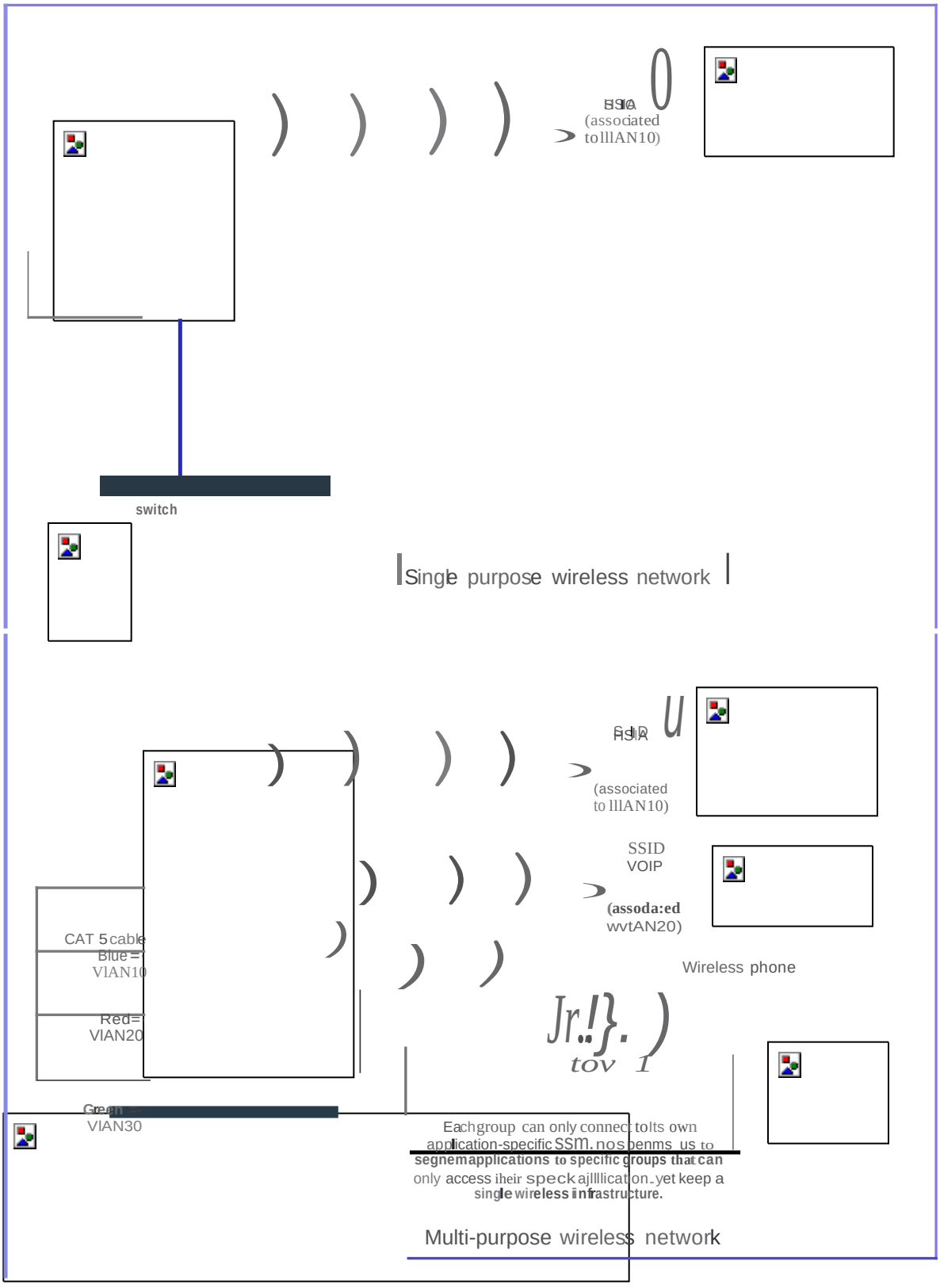
Up to 8 spatial streams	Building on 802.11n's maximum of 4 spatial streams, 11ac is prepared to support more simultaneous data streams on a channel—when this technology is viable in the future
80 and 160 MHz channels	By increasing channel bandwidth, data rates for individual stations are multiplied and their data transfer efficiency is considerably improved, though aggregate network capacity may decrease in multi-AP environments
Multi-user MIMO	MU-MIMO enables simultaneous downlink data streams to different clients at the same time, improving overall channel efficiency. MU-MIMO offloads antenna complexity to the AP and away from clients (e.g. mobile phones)
Transmit Beamforming	Building on 802.11n transmit beamforming, 11ac simplifies the implementation and creates an industry standard to improve TxBF adoption
Frame Aggregation	By packing larger data payloads in each frame, 11ac boosts overall capacity and efficiency by reducing overhead

1. IEEE Specifications and Regulation for 802.11

The Institute of Electrical and Electronic Engineers (IEEE) established the 802.11 standard and other variations, such as 802.11a, 802.11b, 802.11gand 802.11n. The IEEE is a non-profit professional association of members from approximately 150 countries. While the IEEE sets specifications and standards, it does not enforce communications regulations. That responsibility is handled by a separate governing body. In the United States the Federal Communications Commission (FCC) is tasked with enforcing regulations. Most other countries adapt regulations from the IEEE and have an enforcement agency comparable to the FCC.. 802.11 standards are based on non- licensed frequency bands so applying for permits is not required in the United States and most countries.

2. Single Purpose vs. Multi-Purpose Networks

Wireless networks with a single SSID or VLAN lack the ability to scale and cannot provide the service of many applications with special or unique requirements. Single networks such as a low-end Wireless Access Point (WAP) are limited to servicing a single application and cannot meet the needs for multiple applications. This limitation should be considered when planning a network because the shortsighted implementation of a single application can result in higher overall costs. A redesign, reimplementation, removal and replacement with multiple SSIDs, VLAN support, Quality of Service (QoS), and trunking can be quite high. The limited capability and eventual high expenditure for single purpose networks strongly suggest implementations that are planned to support multi-purpose applications - even if they will initially support a stand-alone application.



Tim Ross - Datanamics

3. Wireless Access Point (WAP)

A true converged network benefits from a multi purpose rather than single purpose wireless network implementation. With that in mind, the objectives of the 802.11 wireless site survey are to provide wireless coverage for all locations that require it, reduce coverage where it is not needed and offer the best infrastructure to afford uplinks to each wireless access point (WAP). The survey will provide information about where the WAPs will be placed, identify the best infrastructure for the WAPs, and determine how to meet the bandwidth and coverage requirements of the implementation. Many locations for WAPs may not have AC power available in the immediate area and Power over Ethernet (POE) should be implemented on all WAPs to add greater flexibility. .

4. Interference

Interference is one of the most problematic issues with 802.11 networks. Since 802.11 is a non-licensed band solution many companies add and remove 802.11 networks for different projects and events. This lack of regulation causes conflicting interference for neighboring buildings who implement 802.11 capabilities. Even with good planning, a hotel may successfully complete an implementation only to discover that a neighboring residence with an 802.11 network causes interference – and vice versa. These conflicting 802.11 networks are only one source of interference. Other intrusion comes from sources such as 2.4GHz wireless phone systems, microwave ovens, and 2.4GHz radios. Survey tools can provide a means to help find and isolate a conflicting wireless network. If the source of interference is not a conflicting 802.11 network, a spectrum analyzer may help.

B. Design Factors

1. Cell-based Coverage (indoors)

The Cell-based method uses a number of WAPs, each covering a small area. The first WAP covers an area approximately proportioned with an omni antenna. While some buildings permit wireless signals to penetrate between floors with relative ease some buildings restrict the signal to a single floor due to construction methods. Building materials, construction methods, and even placement of furniture and mirrors inside guest rooms can make a critical difference in the numbers of WAPs needed for proper coverage, as well as WAP placement. A full site survey is required to understand the impact of materials and environment on signal propagation.

Yellow = Channel 1 Blue = Channel 6 Green = Channel 11

Figure 7: Indoors cell-based coverage overlapping three (3) floors

4. Planning for Capacity vs. Coverage

In some cases an access point can cover an area that has a greater number of users than that for which it can successfully provide service due to bandwidth limitations. In these cases the design approach is to shrink cell size by using placement, attenuation and power adjustment where necessary.

- **Capacity Planning (Solution 1)**

This solution provides coverage uses twenty-four wireless access points to divide coverage into separate areas. The WAPs are placed throughout the area and surrounding spaces to minimize overlap of signal. Typically WAPs are placed low (as opposed to on ceiligns) to further reduce coverage area. RF power may be turned down on the radios and/or a directional antenna may be used to further control cell size and coverage area.

2.4GHz is limited to three non-overlapping channels and with twenty-four WAPs, channel planning will be required to minimize contention, etc. Use of overlapping channels and dynamic channel selection may be necessary. Modern channel selection technology can use channel capacity to further increase spectrum efficiency.

- **Planning for Proper Use of Channels**

  Although the 2.4GHz spectrum has eleven WiFi channels available for use, only three non-overlapping channels (1, 6, and
  11) are available.

  If channel 3 is transmitting, its transmission will reduce potential throughput on both channel 1 and channel 6.

Overlapping Channels: Yellow = Channel 1 Blue = Channel 6 Green = Channel 11

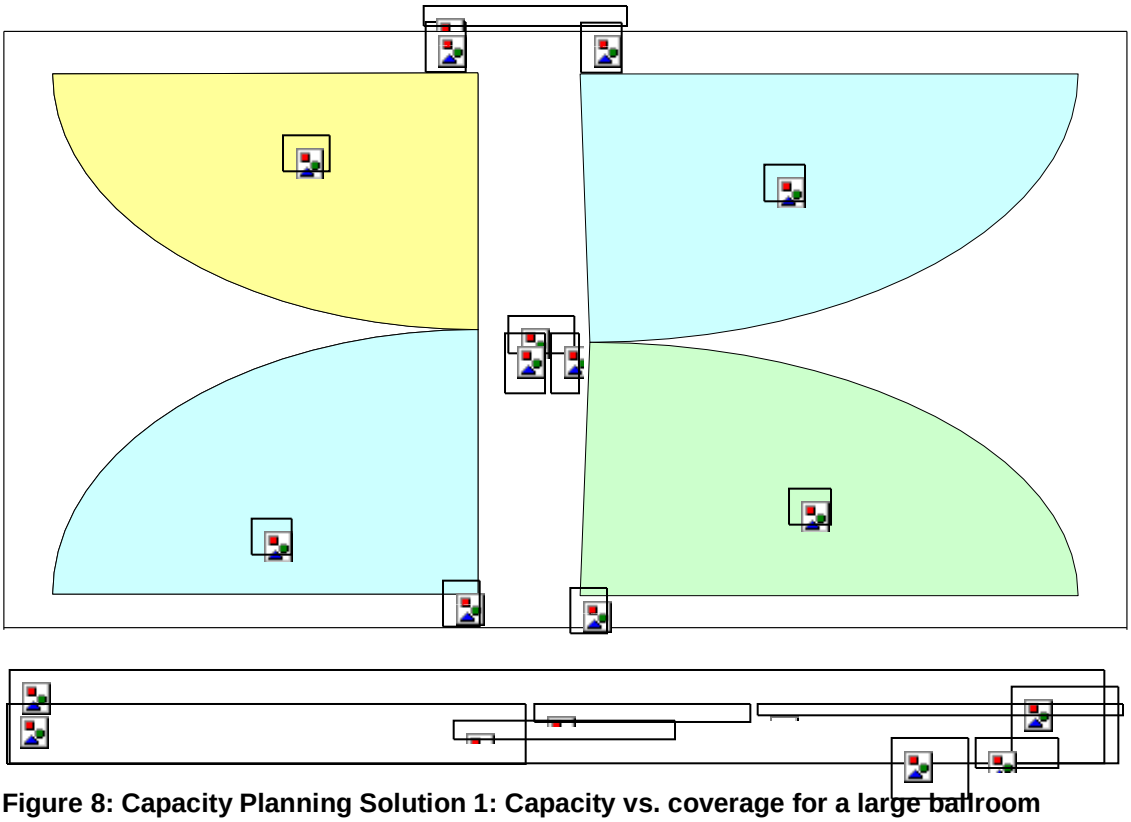


Figure 8: Capacity Planning Solution 1: Capacity vs. coverage for a large ballroom

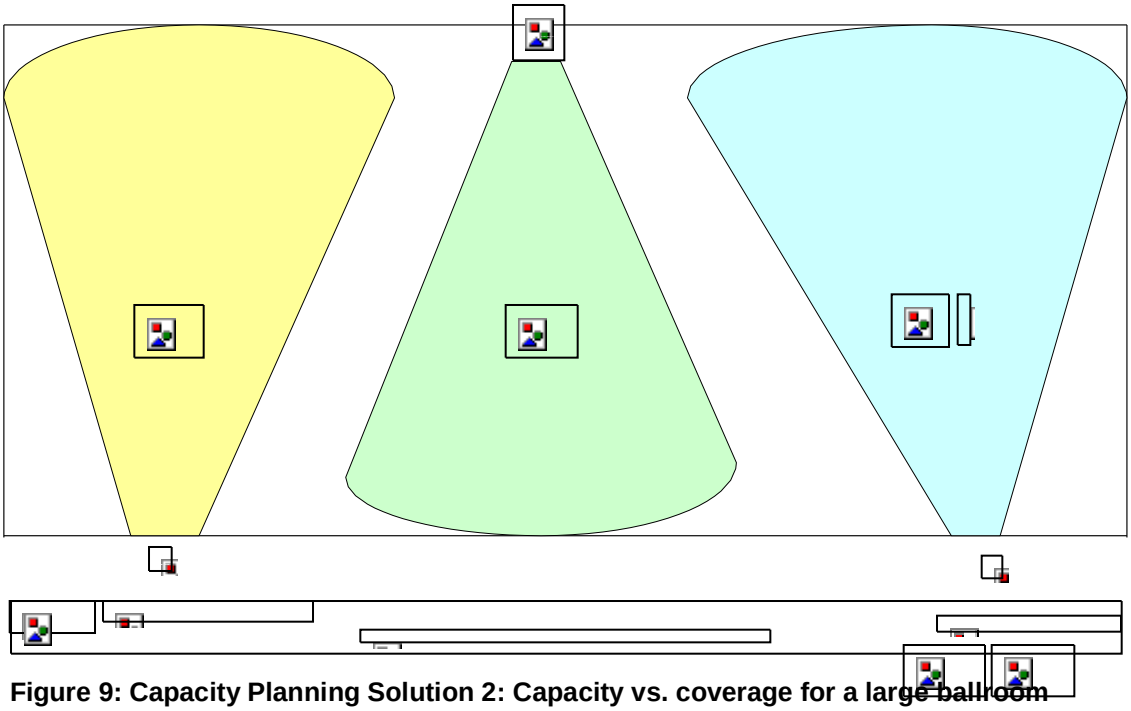


Figure 9: Capacity Planning Solution 2: Capacity vs. coverage for a large ballroom

C. Optional Mesh Networking

Mesh networking provides a wireless infrastructure for interconnecting wireless access points eliminating some of the need forcabling. This network provides an "almost" complete wireless solution requiring less cabling than older, more traditional wireless networks at the cost of reduced network throughput.

Mesh Networks are a natural evolution of combining wireless bridging and access points. Although a defined specification doesn't exist, vendors have developed several different proprietary solutions to fill the need.

Figure 10: Mesh Network Solution – High

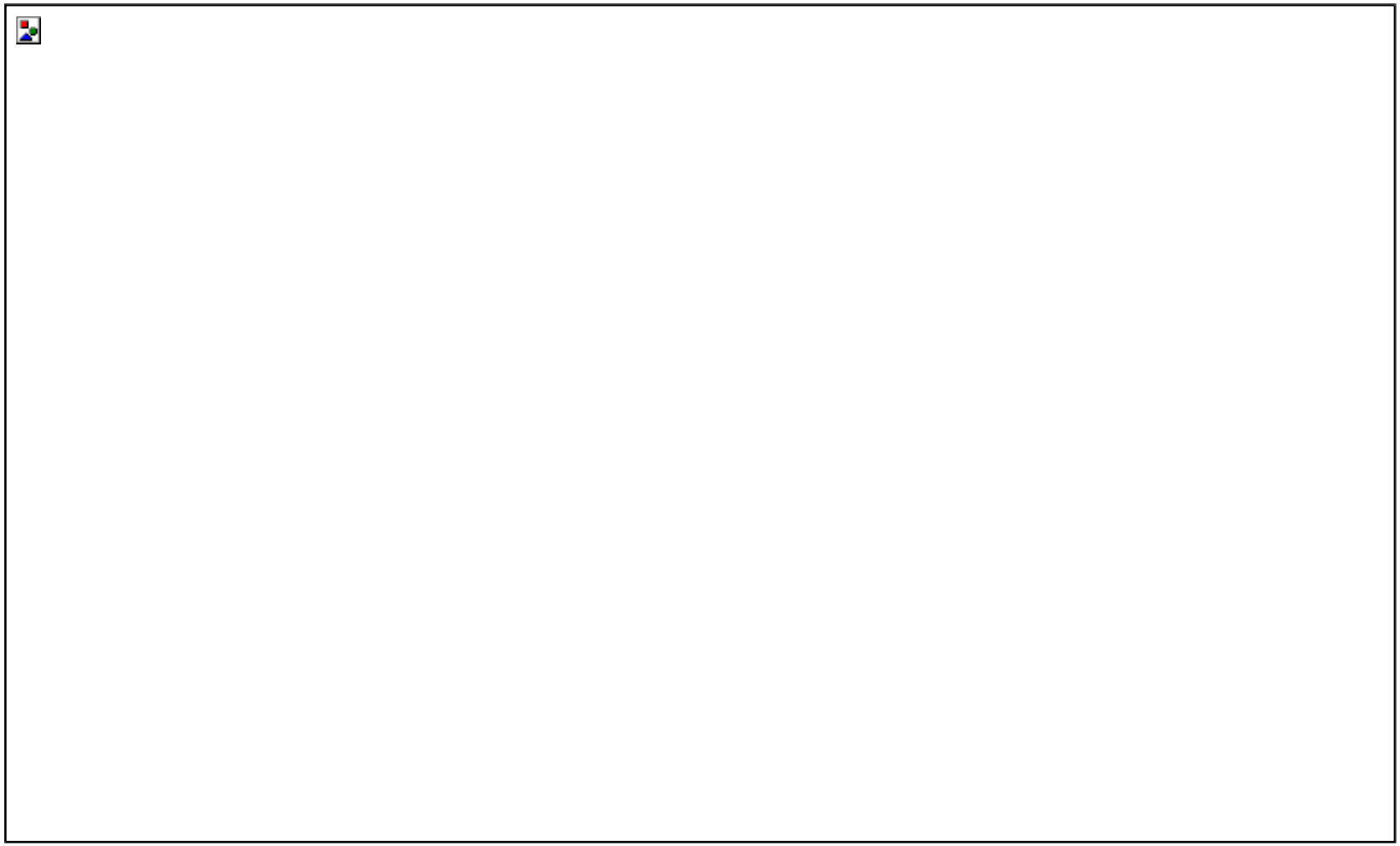
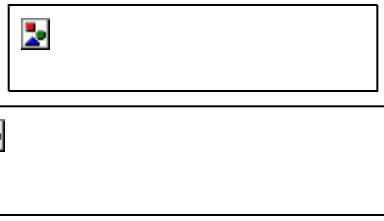


Figure 11: Mesh Network Solution – Resort Property



V. Backhaul Solutions for Wireless

To the general public, one of the most surprising costs of implementing a wireless infrastructure can often be the cost of wired cabling. The question will arise by many who ask “Why am I paying for wires when this is supposed to be a wireless network?” While the system provides a wireless service to the end user, the most effective way to provide uplinks from each wireless access point is through wired cabling, although other methods are available. In addition to Mesh Networking, backhaul solutions for providing wired uplinks for a wireless network include:

a. CAT5 Standard Ethernet Cabling

d. Fiber Optic Cabling

A. CAT5 Standard Ethernet Cabling Solution

CAT5 is the most common method of providing a backhaul system for the wireless infrastructure and provides one of the highest bandwidth systems available. CAT5 cabling is defined in EIA / TIA 568 and 569 standards and is also one of the most cost effective solutions for providing uplinks to the wireless network.

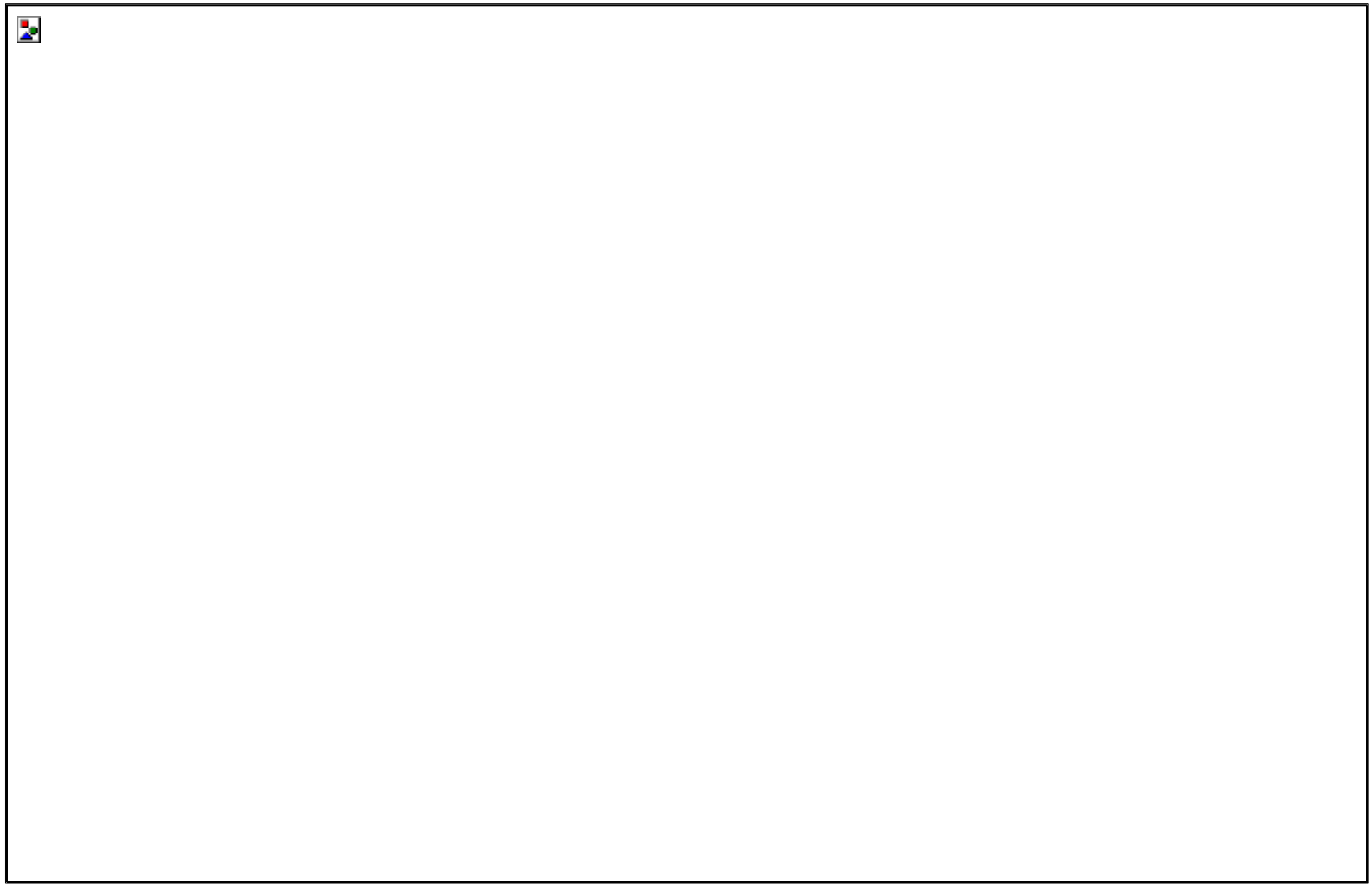


Figure 13: Cat5 Backhaul Solution High-Rise

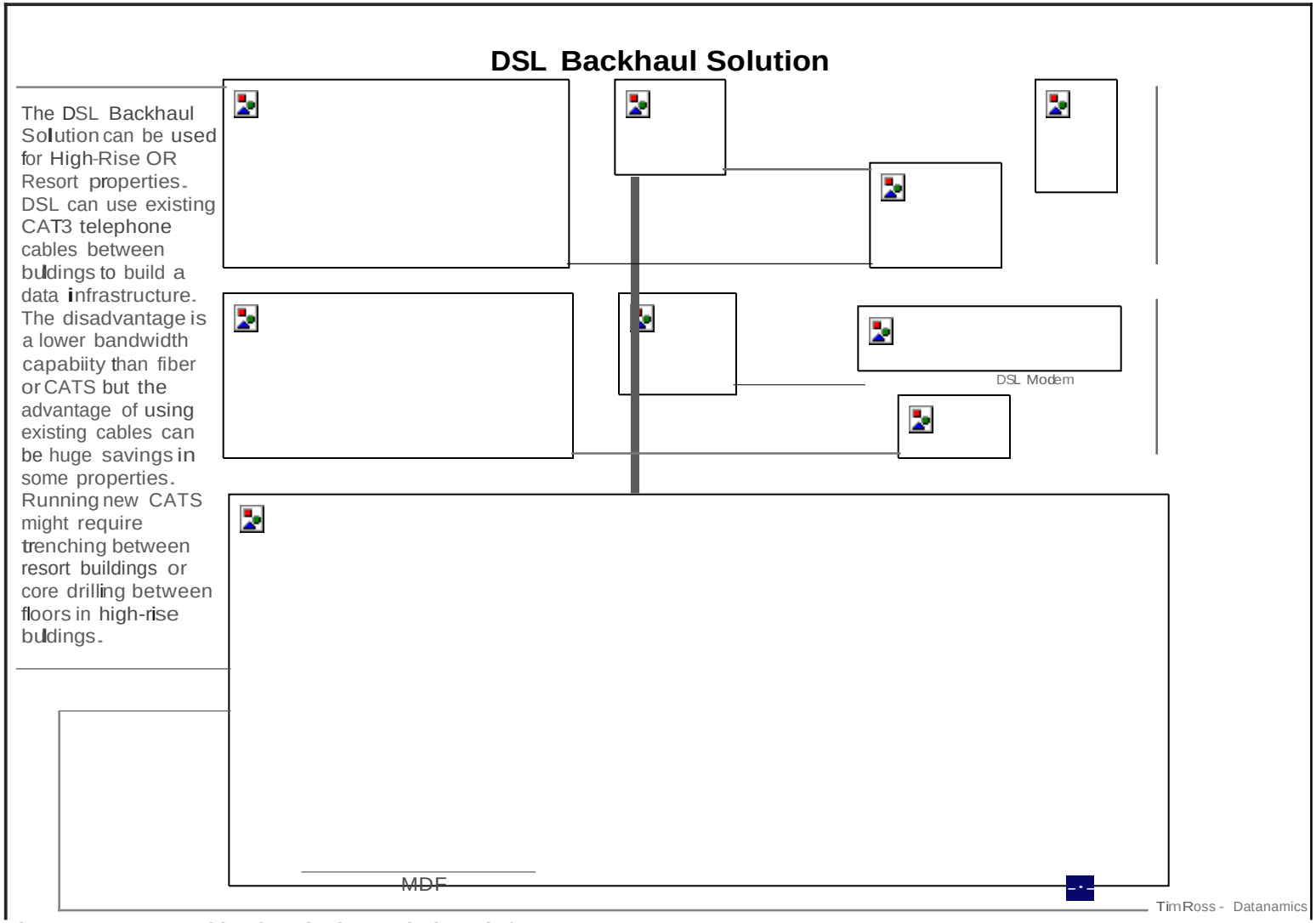


Figure 14: DSL Backhaul Solution- Wireless infrastructure

D. Fiber Optic Cabling Solution

Another backhaul method that can be used to provide uplinks to the wireless network is Fiber Optic Cabling. Fiber optic cabling is capable of the highest bandwidths available and can accommodate the longest distances between devices.

The downside to fiber optic cabling is that it is also the most expensive to implement. There are some special instances where a hotel may benefit from fiber implementations but they are not common.

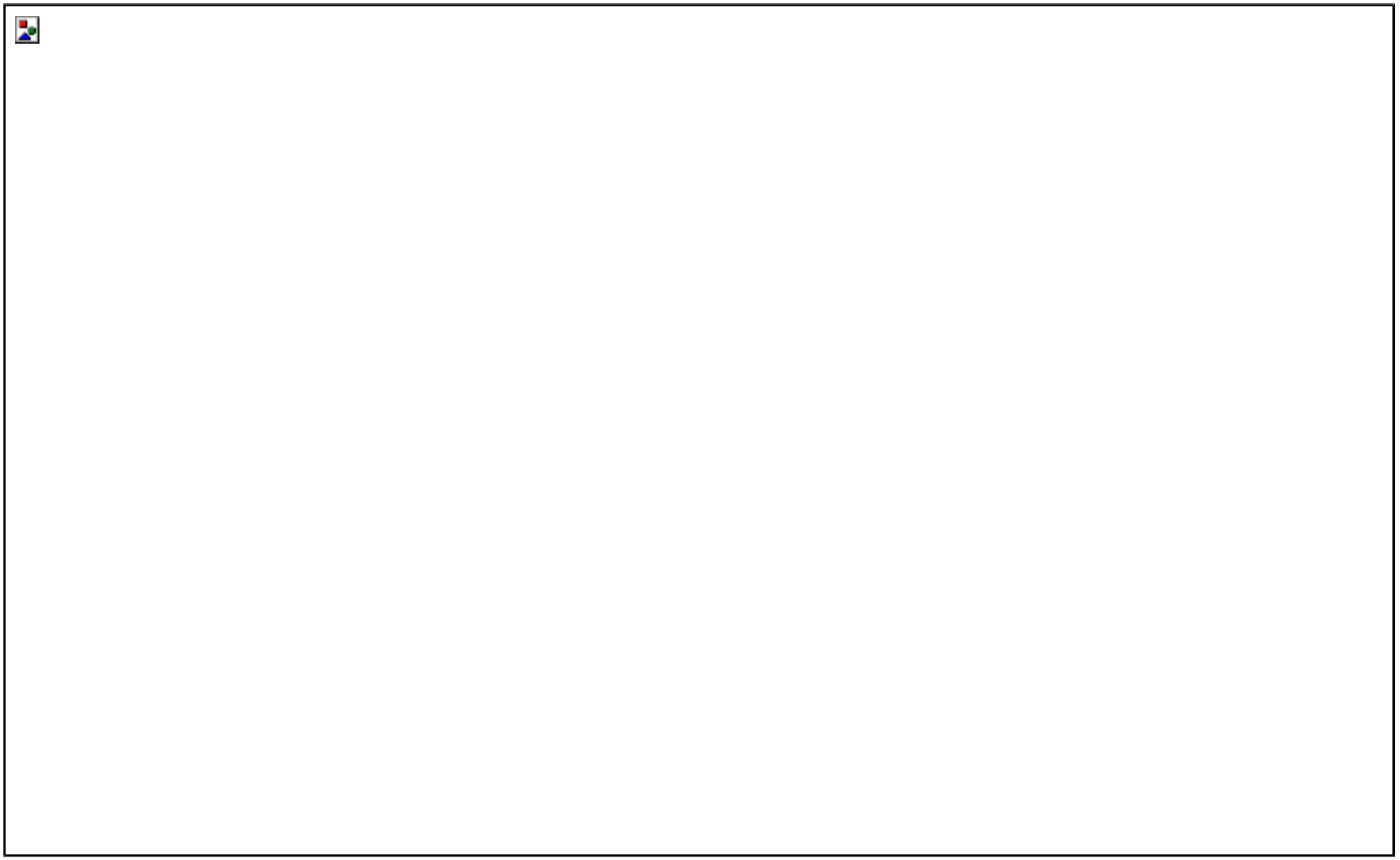


Figure 15: Fiber Backhaul Solution – High Rise

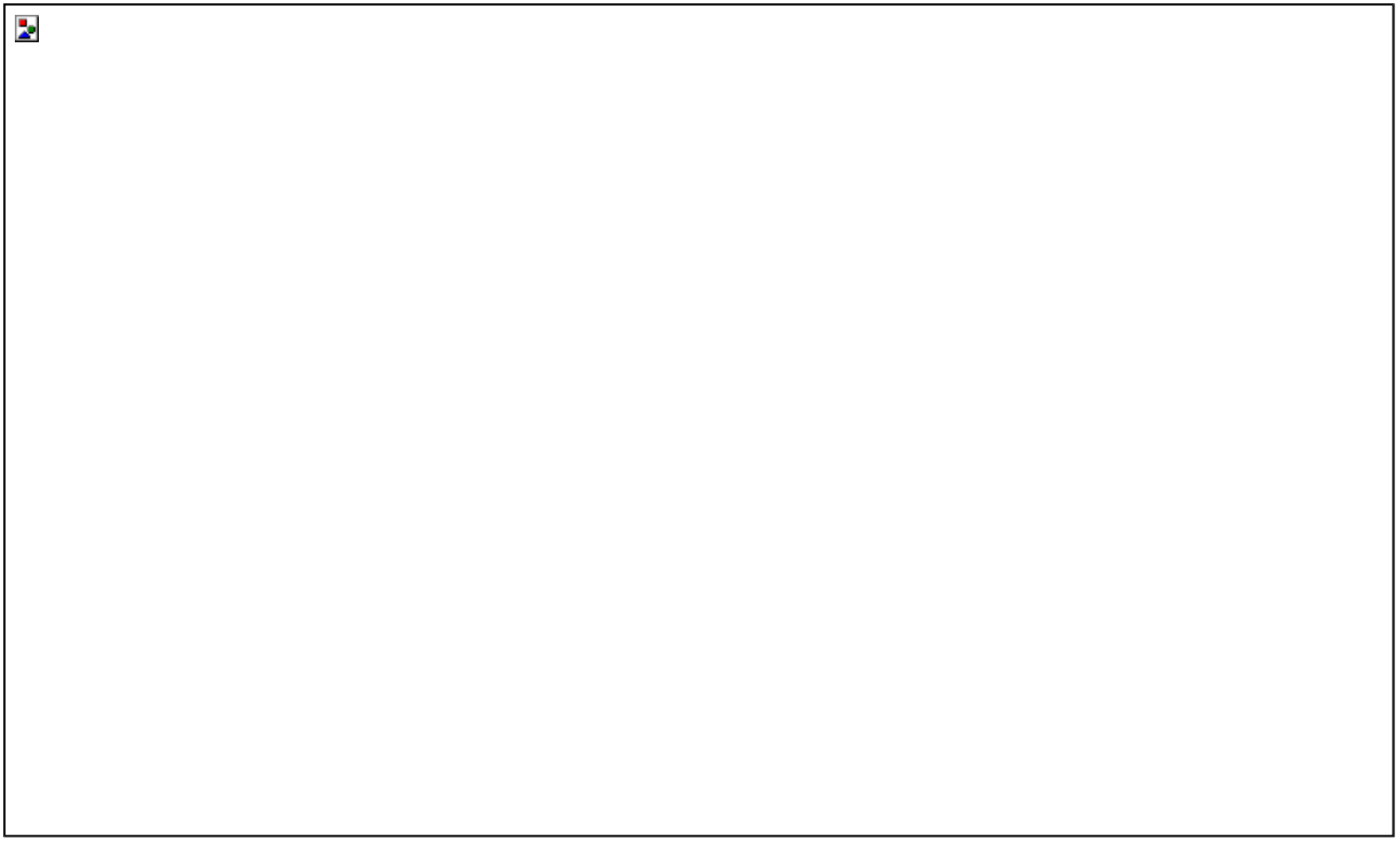


Figure 16: Fiber Network Solution – Resort Property

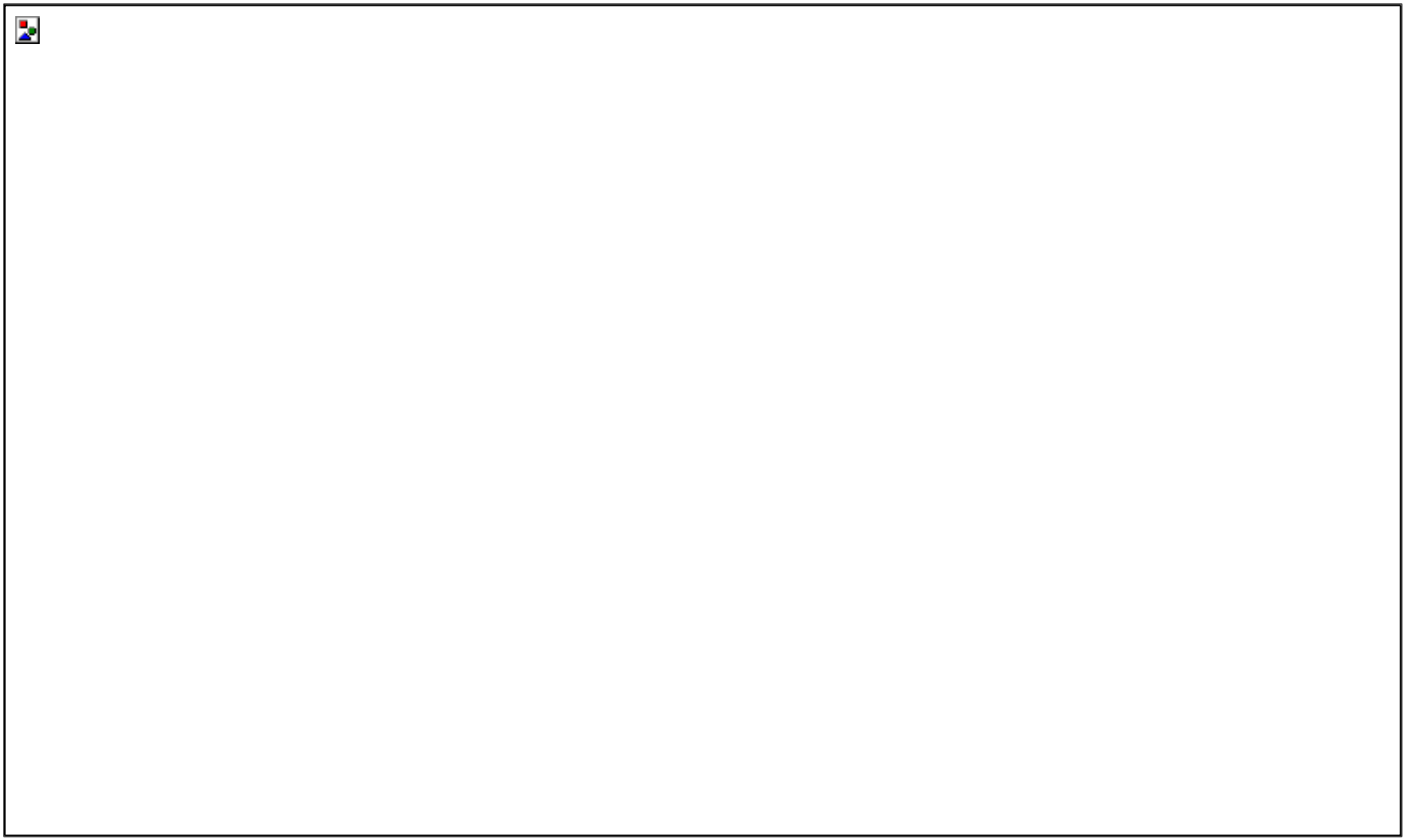


Figure 17: WDS Backhaul Solution

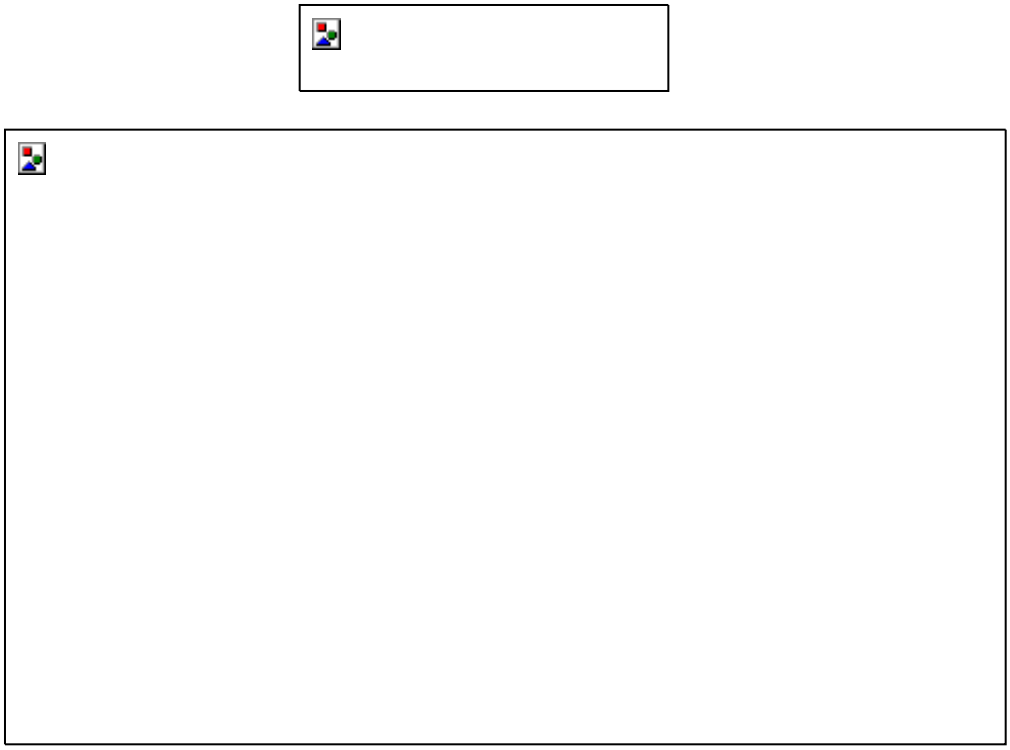


Figure 18: Global Wireless Standards

[5] To date, this is the only standard that has been certified. Certification of the portable model is still pending.

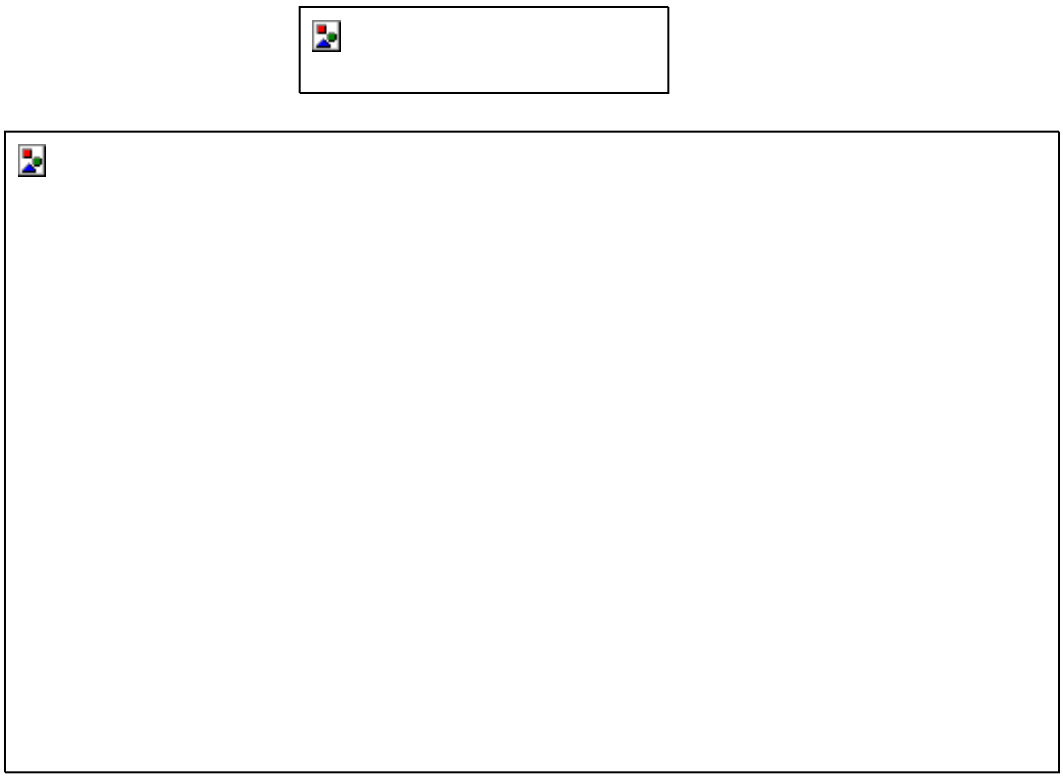


Figure 19: WiMAX Fixed Network Topology

2

VII. Specialized Wireless Technologies

In addition to the previously mentioned standards based wireless technologies, several other technologies can be applied to satisfy hotel based requirements. Furthermore, exciting new wireless technologies are emerging which can be utilized throughout the hospitality industry to solve guest related issues. This includes:

a. Wireless Bridging

b. Wireless Personal Area Networks (WPAN)

c. ZigBee™

d. Z-Wave™ Technology

e. Certified Wireless Universal Serial Bus (USB)

f. Radio Frequency Identification Device (RFID)

g. Digital Enhanced Cordless Telecommunications (DECT)

A. Wireless Bridging

Wireless Bridging is based on the 802.11 specifications. While 802.11b/g and 802.11n are more often used for end-user access, 802.11n is often used for wireless bridging. This is not a hard-standard, but often used because

802.11n can operate at 5GHz and support MIMO, while 802.11b and g operate at 2.4 GHz. Using 5GHz for bridging and 2.4GHz for access points (end- user) allows use of both spectrums.

Wireless Bridging is also used to interconnect separate buildings that do not have an existing wired infrastructure; to connect a temporary site via wireless or in those instances where it would be difficult or expensive to run cabling to other buildings.

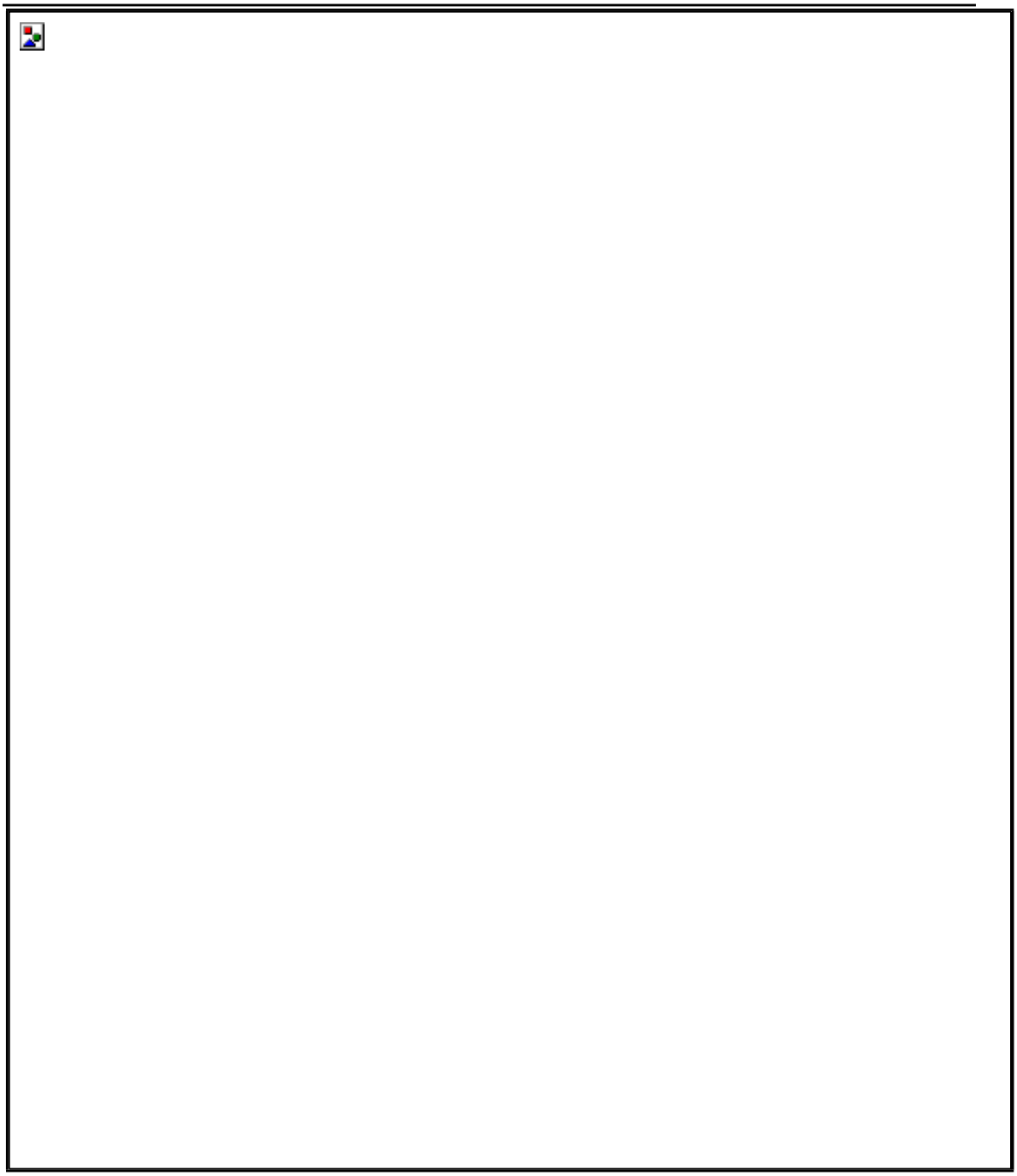


Figure 20: Wireless Bridging Solution (Inter-connect Buildings)

B. Wireless Personal Area Network (WPAN)

A personal area network (PAN) is a computer network used for communication among computer devices including telephones and personal digital assistants centered around one person. The devices may or may not belong to the person in question and may reach a distance of a few meters to as much as 10 meters. PANs can be used for intrapersonal communication among the personal devices themselves or for connecting to a higher level network and the Internet (an uplink). The PAN may be wired or wireless. A wireless personal area network (WPAN) is an ad-hoc network centered around a person or object that is stationary or in motion. A WPAN will allow a significant number of digital devices within range to communicate with each other.

1. Types of WPAN

- Bluetooth® industrial specification for wireless PANs.
- Wireless USB version of the highly deployed USB 2.0 standard.
- ZigBee™ set of high level protocols designed for low power digital radios.
- Z-Wave™ proprietary protocol for wireless home control networking.
- NanoNET proprietary set of wireless sensor protocols, designed to compete with ZigBee.
- OBEX communications protocol facilitates the exchange of binary objects between devices, is specified in the IrDA and is primarily used with infrared devices.
- RadioRa proprietary two-way RF protocol, developed for use in residential lighting control. Application is currently limited to lighting.

- TinyOS mesh network OS using the NesC language is an operating system used with an underlying wireless technology. It is geared toward manufacturing and has a typical range of 2 meters.

- Topdog proprietary protocol for wireless networking developed for use in residential and commercial lighting control.

- Wi-Fi trademark for sets of product compatibility standards for wireless local area networks. (WLAN) It is not suited for in room control.

Bluetooth® WPAN Technology

Bluetooth wireless (IEEE 802.15.1) is a short-range communications technology intended to replace the cables connecting portable and / or fixed devices while maintaining high levels of security. The specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

Key features are robustness, low power, and low cost. The technology has achieved global acceptance to the extent that any Bluetooth enabled device can connect to other Bluetooth enabled devices in proximity.

Enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets. Each device can simultaneously communicate with up to seven other devices within a single piconet. And can belong to several piconets simultaneously. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

- **Core Specification Versions**

  - Version 2.0 + Enhanced Data Rate (EDR), adopted November, 2004
  - Version 1.2, adopted November, 2003

- **Specification Make-Up**

  Unlike many other wireless standards, the Bluetooth wireless specification gives product developers both link layer and application layer definitions, which supports data and voice applications.

- **Spectrum**

  Bluetooth operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops / sec. The 2.4 GHz ISM band is available and unlicensed in most countries.

- **Interference**

  Its adaptive frequency hopping (AFH) capability was designed to reduce interference between wireless networks sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency.

  This is done by detecting other devices in the spectrum and avoiding the frequencies they are using. This adaptive hopping allows for more efficient transmission within the spectrum, providing users with greater performance even if using other technologies.

  The signal hops among 79 frequencies at 1 MHz intervals to give a high degree of interference immunity.

- **Range**

  Range of Device Applications for Bluetooth technology is available in an unprecedented range of applications from mobile phones to automobiles to medical devices for use by consumers, industrial markets, enterprises, and more. The low power consumption, small size and low cost of the chipset solution enables the technology to be used in the tiniest of devices. The operating range depends on the device class:

  - Class 3 radios: have a range of up to 1 meter or 3 feet
  - Class 2 radios: most commonly found in mobile devices and have a range of 10 meters or 30 feet
  - Class 1 radios: used primarily in industrial use cases and have a range of 100 meters or 300 feet

- **Power**

  The most commonly used radio is Class 2 and uses 2.5 mW of power and is designed to have very low power consumption. This is reinforced in the specification by allowing radios to be powered down when inactive.

- **Data Rate**

  1 Mbps for Version 1.2; Up to 3 Mbps supported for Version 2.0 + EDR

- **Technology Benefits**

  A fundamental strength of Bluetooth is the ability to simultaneously handle both data and voice transmissions. This enables users to enjoy variety of innovative solutions such as a hands-free headset for voice calls, printing and fax capabilities, and synchronizing PDA, laptop, and mobile phone applications.

The technology delivers short-range communication between devices and is a global standard. It has “profiles,” and does not need to install driver software. It also has small-form factor radio, low power, low cost, built-in security, robustness, ease-of-use, and ad hoc networking abilities.

- **Availability**

The specification is available free-of-charge to member companies around the globe. Manufacturers are busy implementing the technology to reduce the clutter of wires, create seamless connections, stream stereo audio, transfer data or carry voice communications. Bluetooth technology operates in the 2.4 GHz, one of the unlicensed industrial, scientific, medical (ISM) radio bands.

ZigBee™ Technology

The ZigBee is a published specification set of high level communication protocols designed to use small, low power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs).

The relationship between IEEE 802.15.4 and ZigBee is analogous to that existing between IEEE 802.11 and the Wi-Fi Alliance. The technology is designed to be simpler and cheaper than other WPANs such as Bluetooth.

The most capable ZigBee node type can require only about 10% of the software of a typical Bluetooth or Wireless Internet node, while the simplest nodes are about 2%. However, actual node sizes are much higher, more like 50% of Bluetooth code size. Most ZigBee solutions require an additional micro controller which can add cost.

Uses

ZigBee is aimed at applications with low data rates and low power consumption. ZigBee's current focus is to define a general-purpose, inexpensive self-organizing mesh networks that can be shared by industrial controls, medical devices, smoke and intruder alarms, building, hospitality and home automation. The network is designed to use very small amounts of power, so that individual devices might run for a year or two with a single alkaline battery.

- **Device types**

  There are three different types of devices used with this technology:

  1. ZigBee Coordinator device uses one coordinator in each network and is the most capable device. It forms the root of the network tree, is able to store information and might bridge to other networks.
  2. Full Function Device (FFD) which can act as an intermediate router, passing data from other devices.
  3. Reduced Function Device (RFD) which is just smart enough to talk to the network; it cannot relay data from other devices.

- **Radio Spectrum**

  ZigBee technology operates in the unlicensed 2.4 GHz worldwide with a typical 915 MHz in the United States and 868 MHz ISM bands across Europe.

- **Range**

  Transmission range is between 33 - 246 feet. (10 and 75 meters)

- **Power**

  The technology allows for low power consumption due to the duty cycle of battery powered nodes inside.

- **Data Rate**

  The raw, over-the-air data rate is 250 Kbps per channel in the 2.4 GHz band, 40 Kbps per channel in the 915 MHz band, and 20 Kbps per channel in the 868 MHz band.

- **Technology Benefits**

  ZigBee is a global standard for wireless connectivity and is well suited to a wide range of applications.

Z-Wave™ Technology

Z-Wave is a wireless communications standard which allows complete control of a large number of compatible devices throughout a building from a single remote control, wall panel, or Internet interface. It is designed for low-power and low-bandwidth appliances, such as home automation and sensor networks.

- **Core Specification Versions**

  In Europe, the 868MHz band has a duty cycle limitation of 1%, which means a Z-Wave unit can only transmit 1% of the time. This limitation is not present in the 908MHz band in the United States, but legislation imposes a 1mW transmission power limit compared to the 25 mW imposed throughout Europe. Z-Wave units can be in power-save mode and active only 0.1% of the time, thus reducing power consumption dramatically.

  - Bandwidth - 9600 bps
  - Modulation – GFSK
  - Range - Approx. 100 feet (30 meters indoors) and more than 300 feet (100 meters) outdoors.
  - Frequency Band - uses the 900MHz ISM frequency bands. (908.42MHz in the United States and 868.42MHz in Europe).

- **Topology and Routing**

  Z-Wave uses a mesh network topology and has no master node. A message from node A to node C can be successfully delivered even if the two nodes are not within range providing that a third node B can communicate with nodes A and C. Therefore, a Z-Wave network can span much farther than the radio range of a single unit. In order for Z-Wave units to be able to route unsolicited messages, they cannot be in sleep mode. A Z-Wave network can consist of up to 232 units with the option of bridging networks if more units are required.

- **Application Areas**

  Z-Wave is designed for low-power networks. Battery life of Z-Wave units on AA batteries is usually several years. It is not suitable for audio / video applications due to its low bandwidth but it is well suited for sensors and control units which typically transmit a few bytes at a time.

- **Interference**

  One of its greatest strengths is its ability to operate as a mesh network (i.e. with no central controller). Rather than depend solely on line-of-sight communications like other technologies, Z-Wave is able to get around obstacles by routing commands through other devices in the network. If the signal is blocked it will notify the controller that it did not complete the connection and the network will immediately seek an alternate path. It may go to a hallway light, the thermostat, or a dimmer switch before ultimately reaching the end device. It will try as many times as is necessary, or until all possibilities are exhausted. Once the operation is complete, an indication appears on the controller.

- **Technology Benefits**

  The types of devices that can go on a Z-Wave network include various hand controlled units such as on / off switches and lighting levels for interior and exterior lights, motorized exterior doors, electronic entry systems, motion controls, motorized blinds, powered skylights, home theater systems, and temperature controls for the guest room, pool or spa. The core Z-Wave technology is far less expensive to implement than other control systems. The design helps keep the prices of individual modules lower. As a result, Z-Wave solutions can be installed inexpensively.

Certified Wireless Universal Serial Bus (USB)

USB has become the de facto standard in the personal computing industry with more than 2 billion legacy wired USB connections in the world. These fast, interoperable connections will soon become available in the wireless world with the introduction of Certified Wireless USB from the USB Implementers Forum (USB-IF). This technology is the new wireless extension to USB that combines the speed and security of wired technology with the ease-of-use of wireless technology.

- **Spectrum**

  The technology will support robust high-speed wireless connectivity by utilizing the common WiMedia Ultra-wideband (UWB) radio platform.

- **Data Rate**

  Certified wireless USB performance is targeted at 480Mbps at 3 meters and 110Mbps at 10 meters.

- **Technology Benefits**

Certified wireless USB connectors are a standardized method of connectivity to a variety of devices. It is the first high-speed wireless personal interconnect technology to meet the needs of multimedia consumer electronics, PC peripherals, and mobile devices. Wireless USB will preserve the functionality of wired USB and provide enhanced support for streaming media CE devices and peripherals. The UWB technology offers a solution for high bandwidth, low cost, low power consumption, and physical size requirements of next generation consumer electronic devices.

Comparison of WPAN Technologies

The following have the most potential in the hospitality industry. The choice of technology will depend on the application and the type of devices used for in room controls such as light switches.

WPAN Protocols				
	Bluetooth 802.15.1	ZigBee 802.15.4	Z-Wave	Certified Wireless USB
Frequency	2.4 GHz	2.4 GHz Worldwide 915 MHz US 868 MHz EU	908 MHz US 868 MHz EU	7.5 GHz
Range (meters)	1-10+	1-100+	30-100	3-10
Bandwidth	720 Kbps	20-250 Kbps	9600 bps	110 - 480 Mbps
Network Size	7	Unlimited	232	127
Battery Life (days)	1-7	100-1000+	600-1000	3-5/60-90
Network Topology	Mesh	Mesh	Mesh	Hub & Spoke

Figure 21: Comparison of WPAN Technologies

C. Radio Frequency Identification Device (RFID)

RFID technology is revolutionizing how the location and movement of goods and assets are tracked. The RFID system consists of a transceiver (radio), which transfers information to a processing unit, and a “tag” (transponder), which contains the RF circuitry and information to be transmitted.

The RFID tags are microchips with antenna which come in two different configurations, passive and active. Passive tags are small “chips” that do not require any power source. The tags transmit internal data when activated by a radio signal sent by an RFID reader. Depending on the vendor and the application, the tag typically carries no more than 2KB of data. These more basic tags are sufficient when storing simple information. Active tags are more expensive and require a power source such as a battery and unlike passive tags, actively seek out a reader.

1. Interrogator (Reader)

An RFID interrogator or “reader” transmits radio frequency waves to a mini antenna attached to each tag. The radio frequency (RF) transmitter and receiver communicating with the tags are generally grouped into one of two categories, “intelligent” or “dumb readers." Intelligent RFID readers have the ability to run different protocols, filter data and run applications. A "dumb" reader is a simple device that might read only one type of tag using one frequency and one protocol.

Interrogator (reader) pricing is shown in U.S. dollars and varies depending on the features and functionality required.

Tag Type Frequency (Band)	Range	Cost
Low (125 - 134 KHz)	0 – 18 inches (12 inch average)	$100.00 - $750.00
High (13.553 – 13.567 MHz)	125 – 134 KHz (3 feet)	$200.00 - $500.00
UHF (Ultra high frequency)	400 – 1,000 MHz (10 – 20 feet)	$1,000 - $5,000

Figure 22: RFID Frequency Range

Ultra high frequency tags typically operate at 915 MHz in the United States and 868 MHz in Europe. When longer ranges are needed, such as for tracking containers, active tags use batteries to boost read ranges to 300 feet (100 meters) or more.

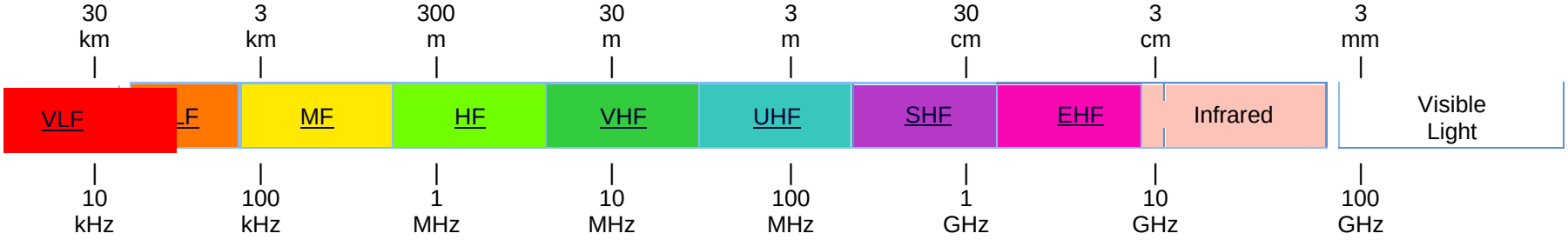


Figure 23: Frequency Allocations in the United States

2. RFID and Barcode Technology

Both RFID and barcodes capture data and send it to a destination, however, the benefits of RFID outweigh barcode technology. RFID does not require the human intervention of scanning and is more efficient and less expensive.

Barcodes must be scanned at specific orientations to establish line-of-sight and static information cannot be updated unless the user reprints the code. RFID tags need only be within radio frequency range of a reader to be scanned and can be read rapidly even when scanned in bulk.

Unlike barcodes, RFID tags are more durable and can withstand chemical and heat environments that would destroy traditional barcode labels. RFID tags can potentially contain a greater amount of data compared to barcodes, which commonly contain only static information such as the manufacturer and product identification.

RFID also have read and write capabilities and can be updated. Constraints to implementation can include the recurring cost of tags, privacy issues, capital outlay for conversion and support structure to manage the large volumes of data.

The hotel industry can utilize RFID enabled material for workflow in support of luggage handling, real-time labor force management, point of sale and supply management, guest traffic flow analysis, security and card key monitoring. The ability of RFID to record services used by guests enables management to track usage and allows them to direct effort tailored to the guest's specific needs, rather than focus on general services.

D. Digital Enhanced Cordless Telecommunication (DECT)

DECT is a digital wireless technology adopted worldwide and is designed to work with many other types of networks, such as the PSTN (conventional telephone), ISDN (new digital and data phone), GSM (mobile phones) and more. The cell radius of DECT is 25 to 100 meters, while GSM cells are 2 to 10 km. Properties include a net bit rate of 32 kbit/s and a frequency of 1900 MHz. DECT based wireless telephony can operate in the 1920-1930 MHz band, and can be used for wireless data transfers.

- **Benefits**

  DECT technology is a radio access technology and a cellular system similar to GSM and can be used for building control and security, providing intelligent systems that allow automatic control and alerting. It delivers above average voice quality to IP Telephony through broadband connections and its devices enable features such as: Mobile Presence Messenger (MPM), Instant Messaging (IM), real-time chat, image and photo communication, streaming and central address management over the net. DECT is regarded as a potential technology to solve interference issues between digital cordless phones and WLAN applications.

- **Standards**

  Generic Access Profile (GAP) applies to all DECT portable and fixed parts that support the 3.1 kHz telephony service. It defines a minimum mandatory set of technical requirements to ensure interoperability between any DECT GAP fixed part and portable part, such as handsets and base stations.

  This profile has been established by ETSI (European Telecommunications Standards Institute) as an important part of a set of DECT profiles. Every DECT device must support one or more profiles to be functional.

F. HotSpot 2.0

Hotspot 2.0 is focused on enabling a mobile device to automatically discover APs that have a roaming arrangement with other networks and then securely connect. This is very similar to the standard cellular experience that allows a phone to roam just about anywhere in the world without portal pages, etc.. Wi-Fi roaming would apply anytime a mobile device does not see an AP belonging to its home network provider. A user could roam on a Wi-Fi network that is across town or on the other side of the world. Roaming partners can include MSOs, MNOs, wireline operators, public venues, enterprises, and basically any other entity that has Wi-Fi assets. Roaming can be accomplished with dual mode devices (smartphones) or Wi-Fi-only devices like tablets and laptops.

With Hotspot 2.0, the client device is equipped by an authentication provider with one or more credentials, such as a SIM card, username/password pair, or X.509 certificate. The device can then query Hotspot 2.0 capable APs to see if it belongs to a visited network that supports roaming with the devices remote network.

Hotspot 2.0 is a program of the Wi-Fi Alliance, and is supported by the Passpoint(™) certification program which ensures APs and client devices comply with the technical specifications. Hotspot 2.0 capabilities are emerging in a series of releases. Release 1 came out in June 2012 and was focused on automating network discovery/selection, authentication, and over-the-air security. Other releases will follow in the coming years that will add additional capabilities. Mobile devices with Hotspot 2.0 support are now available in the market. While vendors may choose to introduce new models to enable Hotspot 2.0, these capabilities can be added via software updates in most cases.

VIII. Security for a Wireless Network

Hospitality has security needs that are unique to its business. A wireless network for HSIA is usually a completely open network. This means that no type of encryption or WEP (Wired Equivalent Privacy) key is required to access the network. For example, a guest might turn on their laptop, associate to the HSIA network, open Internet Explorer and be redirected to the hotel “Terms of Use” page. The user is then asked to agree to the terms and will either be asked to bill the service to the room, or be redirected to a custom splash page from which access to the Internet is made available, if the service is free. Although the user

did not enter a WEP key or require a preconfigured encryption, security is available at the user-to-user level.

A. Configuration of Wireless Security

To simplify Internet connectivity for guests, a wireless network deployed in a hotel property is generally configured to operate in a public access state. Guest computers can be set to associate with wireless access points which broadcast the SSID network name to all local network devices.

Because wireless is a radio link, other computers and / or devices can capture the network traffic. In general, most Internet sites automatically use a method called Secure Socket Layer (SSL) when information like user names, passwords, or credit card information is requested. The SSL encrypts the information between the guest's computer and the web site.

Another approach is to use VPN client software which encrypts all network traffic between the guest's computer and a VPN server housed within the hospitality property.

B. Security Filters

Guests cannot view other user activity on a shared wireless network due to "Intracell blocking," which forbids direct communication or Publicly Secure Packet Forwarding (PSPF) which denies all inter-client traffic. Regardless of what the service is called, a dynamic filter prevents any two MAC addresses that enter the same radio interface from going to a destination on the same interface. For example, when USER1 enters interface Radio1, access is allowed on any destination on FA0 / 0 (the uplink port to the Internet), but no access is given to view USER2 who is connected to Radio1 at the same time. This filter provides a level of security to any user connected to this radio. However, a user at this point could still connect to another user who happens to be on another radio (WAP). Types of security for applications on the same infrastructure are given below.

1. User-to-User Security (Port-to-Port)

The switches that provide uplinks to each WAP must also support user-to-user security to eliminate the risk of users going to the same destination. This is accomplished with port-to-port security or VLANs. Port protection provides this security as long as the WAPs are all connected to a single switch, however, if multiple switches are used, port protection often does not provide security between WAPs connected to different switches. Using a separate VLAN for each WAP is the most secure method of user-to-user security.

2. User-to-User Security (VLAN)

VLANs and multiple SSIDs can provide absolute user-to-user security. Each is in a separate "broadcast domain" which means that if a user in VLAN1 sends a layer three broadcast (such as an ARP broadcast), no user in VLAN2 will see the broadcast because each is in separate "broadcast domains." Switches and higher-end WAPs are both capable of supporting VLANs. To interconnect a switch that has multiple VLANs and a WAP that has VLANs, a "trunk" is configured to pass this information.

The 'trunk' is configured to combine traffic from multiple VLANs and pass it to and from the Internet portal while at the same time preventing VLAN traffic from being detected on any other VLAN on the network. 802.1q is an IEEE internationally accepted standard for VLANs and trunks. It is often referred to as Dot1q. Although both the WAP and the switch are aware of VLANs and VLANs can be configured on both, only the WAP can be configured with an SSID or multiple SSIDs.

3. User-to-User Security (Service Set Identifier - SSID)

An SSID is an ID assigned to an 802.11 network. If for example, an SSID "HSIA" is assigned to an 802.11 network, the SSID is allowed to "broadcast" its availability to all clients within range of the network. Let's say that same SSID "HSIA" is assigned to VLAN10 on WAP-1 able to accommodate multiple SSIDs and VLANs. A new SSID is created and called "VOIP," which is designated to accept only hotel staff wireless IP phones. The SSID "VOIP" is made a non-broadcast SSID so users are not aware of it. A WEP key is assigned so that only pre-configured devices can connect to this SSID. Even if a hacker has a RF wireless sniffer and sees the SSID, connection cannot occur because the WEP key is not available. The SSID "VOIP" is assigned to the VLAN20 for another level of security. VLAN10 and VLAN20 both provide DHCP but both receive separate subnets.

In another scenario, a SSID named "1014774" will be used for POS systems to connect. Each POS system is required to have a certificate for authentication with the certificate server. All data will be encrypted with 256 bit AES encryption and all nodes must authenticate with a certificate server prior to being allowed to transmit. This requires the highest level of security and will be assigned to VLAN30 because credit card numbers and personal information will regularly travel on the SSID. Guests can roam between WAPs throughout the hotel because each WAP shares this same configuration, with each maintaining a separate level of security.

Figure 26: Multi-Purpose Wireless Network and Application Specific SSID

A priority in the aforementioned SSID Security example is to provide for the time sensitive voice traffic in VLAN20, reserve an acceptable level of bandwidth for important financial transactions in VLAN30, before HSIA users in VLAN10 are allowed to use the remaining bandwidth.

Network congestion due to an insufficient level of bandwidth for each user-type can occur. For example, the bandwidth may not be acceptable if a group of HSIA users are downloading large files via FTP while at the same time a hotel staff member is attempting a call with an IP phone on the same WAP. The staffer might experience choppy voice quality or, if the FTP files dominated all the bandwidth, the voice call may be dropped altogether. The network design should ensure that an acceptable level of bandwidth is reserved for each user-type to allow for increased traffic.

A. Prioritization and Reservation of Bandwidth

The preceding examples provided most of the requirements for all applications to work properly with the exception of reserving enough bandwidth for each application to ensure its proper operation. The Project Plan and QoS should be designed to address those bandwidth issues and provide a solution.

IEEE's 802.1P is one of the earlier methods of reserving bandwidth and providing prioritization of traffic. Most HSIA traffic will be HTTP or FTP using TCP as the transmission protocol. TCP allows retransmission of missed packets so if these transmissions are reduced or interrupted for a few milliseconds and a packet or two are missed, each will be automatically retransmitted. To implement this plan, an access list is created for each type of traffic, or the separate VLAN subnet for each type of traffic. A security policy is managed on the WAPs to reflect how traffic should be prioritized and reserved for each group. This method provides the bandwidth and service requirements needed by each traffic group and prevents one group from starving the other of bandwidth needs.

IX. Summary

The purpose of this white paper has been to set forth a guide for understanding wireless and its potential within the hospitality industry. Wireless service can not only enhance the guest experience but can also generate a considerable level of savings and income for hoteliers. From a service perspective, savings can be attained through operational efficiencies while opportunities for revenue can deliver a quick return on investment as guest loyalty builds.

An unprecedented opportunity exists through wireless service and the various amenities it provides through next generation devices. The current provision of technology is no longer enough to ensure a return guest visit; accessible wireless services can make a repeat stay inevitable. The contemporary experience for guests necessitates the ability of access to technology that not only meets today's demands but can also adapt to tomorrow's expectations.

Sources

Koser, Karin P. *Business Conveniences for Guests: All the Comforts of a Temporary Office Away From Home*, 2006

Hotel Technology Next Generation, *Convergence: Hotel Technology for Today and Tomorrow* June 2005

Innerwireless http://ww.innerwireless.com

Bluetooth: http://www.bluetooth.com/bluetooth/

WiMedia (http://wimedia.org/en/index.asp)

Ultra Wide Band (http://uwbforum.org/)

USB: http://www.usb.org/developers/wusb/

Z-Wave Alliance: http://www.Z-Wavealliance.org/content/modules/Start/

ZigBee Alliance: http://www.zigbee.org/en/index.asp

WiMAX: www.wimaxforum.org.

NanoNET: (http://www.nanotron.com/)

OBEX Communications Protocol http://www.ravioli.pasta.cs.uit.no/open-obex/

RadioRa Protocol http://www.lutron.com/radiora/

TinyOS Mesh Network: http://www.tinyos.net/

Glossary of Terms

Active RFID tag	Battery powered RFID tag that transmits the tag information over an extended distance.
Ad Hoc Network	A temporary network typically created in a spontaneous manner. An ad hoc network requires no formal infrastructure and is limited in temporal and spatial extent. For example, mobile devices remain part of an ad-hoc network only while they are within range of the other networked devices.
Antenna	Component of an RFID tag that transmits information stored on the tag's chip and receives radio frequency energy from the reader device to activate the tag. Also, in general, a component of any radio system that transmits and / or receives RF energy.
Backhaul	Is a method used to transmit voice and data traffic from a remote site to a central site.
BDA	Bi-Directional Antenna
Bluetooth	Capability using a shared wireless platform to allow varied devices to communicate with each other and enables use of cellular telephones, camera phones and PDA's. Operates in the unlicensed ISM band at 2.4 GHz using a frequency hopping transceiver. Allows real-time AV and data communications between Bluetooth enabled hosts with link protocol based on time slots.
Bluetooth Baseband	The part of the Bluetooth system that specifies or implements the medium access and physical layer procedures to support the exchange of real-time voice, data information streams, and ad hoc networking between Bluetooth enabled devices.
CAT5	Category 5 is a standard Ethernet cabling (5th generation) used for Ethernet communications.

CDMA	Code Division Multiple Access is one of two digital cellular standards used primarily in North America.
DAS	Distributed Antenna System transport infrastructure that distributes wireless signals to remote locations from a central point.
Data Encryption	Method of encoding data to prevent others from being able to interpret the information.
DECT	Digital Enhanced (former European) Cordless Telecommunication
Device class	A method of organizing common functions and protocols for devices that serve similar functions. (Communication, audio, display etc)
DSL	Digital Subscriber Line transmits data over phone lines with out interfering with voice service.
DSLAM	Digital Subscriber Line Access Multiplexer is a network device that receives signals from multiple customer DSL connections and delivers high speed data transmission.
Ethernet	A base band LAN specification similar to the IEEE 802.3 series of standards.
EVDO	1x Evolution-Data Optimized is a wireless radio broadband data standard. The official name, defined by the Telecommunication Industry Association, is "CDMA2000, High Rate Packet Data Air Interface."
FTP	File Transfer Profile defines how folders and files on a server device can be browsed by a client device. Once a file or location is found by the client, a file can be pulled from the server to the client, or pushed from the client to the server.
GPS	Global Positioning System uses a radio navigational system involving satellites and computer networks that rely on timed events.
GSM	Global System for Mobile communications is a digital cellular system.

HID	Human Interface Device Profile defines either a specific class of device or the type of device that requires a human interface—, keyboards to remote monitoring devices. In this document, "HID" is synonymous with a device of type: human interface.
Hub	A device containing one or more ports, such as a USB. A hub is used to connect multiple devices together, but without any internal intelligence of its own. Generally, a hub is a device that serves as the center of a shared network.
IEEE 802.3	Term used for Ethernet
Interrogator / Reader	RFID reader that detects compatible RFID tags within its range and transmits an electronic field (radio waves) at a set frequency, which activates RFID tags designed to receive this frequency. When a tag activates, it transmits the information stored on its chip, to the receiving reader.
Intracell blocking	Prevents communication between subscriber units.
LAN	Local Area Network is a high-speed, low-error data network covering a small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.
LEC	Local exchange carrier. The term for a public telephone company in the United States that provides local service.
Link	Shorthand for a logical link.
Logical link	The lowest architectural level used to offer independent data transport services to clients of the Bluetooth system.
MAN	Metropolitan Area Network (MAN) is a type of network best suited to big corporations with large local area networks (LAN)
Mesh	A mesh network decreases the need for Internet gateways by enabling each network user to be a provider, dynamically forwarding data to the next node. The network routes data, voice and instructions between nodes and differs from other networks in that the component parts all connect to each other.

NAK	The value returned when a request has been sent to the device and the device is not prepared to respond.
Null	No value, or zero, depending upon context.
OBEX	Object Exchange Protocol is a transfer protocol that defines data objects and a communication protocol two devices can use to exchange those objects. OBEX enables applications to work over the Bluetooth protocol stack as well as the IrDA stack.
OFDMA	Orthogonal Frequency Division Multiple Access provides optimized use of bandwidth for the high-speed flow of data for multiple subscribers. It overcomes interference and enables bi-directional broadcast and broadband convergence.
Packet	Format of aggregated bits that are transmitted on a physical channel.
PAN	Personal Area Networking profile describes how two or more Bluetooth enabled devices can form an ad-hoc network and how the same mechanism can be used to access a remote network through a network access point. The profile roles include the network access point, group ad-hoc network and personal area network user.
Passcode	Passcode is used to authenticate incoming connections when pairing devices. It provides added assurance that a connection is directed to the expected device or person. A passcode can normally be any combination of keys (letters or numbers). Caution must be used as some devices do not map characters similarly. .
Passive RFID tag	Passive RFID tags get their power by the reader-interrogator (not a battery) which allows them to activate and respond from the electronic field (radio waves) transmitted.
PCS / PDC	Personal Communications Service is a digital mobile phone system network that typically operates at a frequency of 1900 MHz.

Piconet	A collection of devices occupying a shared physical channel where one of the devices is the Piconet master and the remaining devices are connected to it.
PIN	Personal Identification Number. A user-friendly number that can be used to authenticate connections to a device before paring has taken place.
Protocol	A report structure other than the structure defined by the report descriptor. Protocols are used by keyboards and mice to insure BIOS support.
PSPF	Publicly Secure Packet Forwarding prevents client devices associated to an access point from sharing files or communicating with other client devices associated to the access point.
Range	Area that a radio device can cover with signal. This area can be affected by many different factors.
RFID	Radio Frequency Identification Device is an automatic data capture technology that provides real time accuracy for inventory control. (Using sensor based micro-chip smart tags and receivers)
RF Site Survey	Radio Frequency site survey conducted on a mid to large sized property to gather information on the number and placement of wireless network access points needed to provide coverage throughout a facility.
Router	Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded.
SSID	Service set identifier is a name that identifies a wireless network. It is a unique identifier attached to the header of packets sent over a WLAN that acts like a password.
Switch	A network device that filters, forwards, and floods frames based on the destination address of each frame. Similar in general function to a hub, except with a high degree of internal intelligence.
Telephony	Telephone system based on the Internet protocol. (IP)

Trunking	Describes using multiple network cables or ports in parallel to increase the link speed beyond the limits of any one single cable. Also, a method of combining separate VLANs in a network to allow access of all of them to another device while maintaining the absolute security of each separate VLAN.
USB	Universal Serial Bus connectors are a standardized method of connectivity to a variety of devices.
USB Class	A USB device is organized into classifications such as HID, audio, or other-based on the device's features, supported requests, and data protocol.
UWB	Ultra Wide Band refers to a radio communications technique based on transmitting very-short-duration pulses, often of duration of nanoseconds or less, whereby the occupied bandwidth goes to very large values. This allows it to deliver data rates in excess of 100 Mbit/s, while using a small amount of power and operating in the same bands as existing communications without producing significant interference.
VLAN	Virtual Local Area Network is a network of computers that communicate as if they are connected to the same wire, even though they may be located on a number of different LAN segments. From a security standpoint, a VLAN is an isolated LAN from the rest of the overall network in which it resides.
VPN	Virtual Private Network that is constructed by using public wires to connect nodes while maintaining security of transmitted and received communications.
WAP	Wireless Application Protocol supports web based applications. Connects wireless communication devices to form a wireless network.
WDS	Wireless Distribution System enables the interconnection of access points.
WEP	Wired Equivalent Privacy is a wireless communication function and a form of encryption that provides privacy comparable to that of a traditional wired network.

Wi-Fi 802.11x	Wireless Fidelity allows interoperability and is standards based technology for any type of 802.11 network.
WiMAX	Worldwide Interoperability for Microwave Access. Standards based technology that provides high throughput broadband connection.
WiMedia Alliance	The WiMedia Alliance is a not-for-profit open industry association that promotes and enables the rapid adoption, regulation, standardization and multi-vendor interoperability of ultra wideband (UWB) worldwide.
Wireless	Telecommunication in which electromagnetic waves, such as radio, carry communication signals from one path to another.
Wireless Coverage Area	The area where two devices can exchange messages with acceptable quality and performance.
WPA	Wi-Fi Protected Access is a class of systems to secure access to wireless networks. (E.g. WPA, WPA2)
Yagi Antenna	Yagi-Uda Antenna is designed to pick up VHF and UHF transmissions and is used for its simplicity and directionality.