Spot On networks

UserSafe™ Wi-Fi Networks

multifamily | hospitality | commercial | energy management

Managed Wi-Fi Internet Services

May, 2012

55 Church Street, New Haven, CT 06510 phone 877-768-6687 fax 203-773-1947

Index

Spot On Networks Introduction……3

Introduction to Wi-Fi……..4

Bandwidth Backhaul…..……5

Benefits of Offering Managed Wi-Fi…….....……..7

Deployment Options……..9

Spot On Networks Technical Description……..……...…10

Talkback……11

Network Monitoring……..12

Equipment Monitoring……..13

Network Security……..13

Service Level Agreements……..16

Deployment Methodologies……....16

Branding……17

CALEA……19

Summary……20

Spot On Networks, LLC ("SON") Introduction

SON Networks is a Wireless Internet Service Provider (WISP) as well as a Wired Internet Service Provider (ISP) providing managed internet solutions in medium to large Multifamily properties, hotels and commercial common areas. SON provides very cost effective, secure, branded, high-speed Wireless and Wired Internet access, and managed telecommunications services to residents, guests and staff alike. Headquartered in New Haven, CT, SON manages and actively monitors its 500+ networks deployed throughout the United States.

In 2011 ubiquitous Wi-Fi coverage in residential multi-family dwelling complexes is quickly transforming from a "nice to have amenity" to a "utility". "…*they'll build wireless internet into every building, just the way they build in running water, heat and electricity today*" according to David Pogue of the New York Times. Many building owners and property developers have already realized the significant benefits from providing this service to every tenant's apartment and in all community areas.

Furthermore, Wi-Fi has the capability to offset cellular telephone and WiMax coverage issues, and SON has been engaged to develop strategies to supplement and/or assist in the reduction of cellular dead zones and the augmentation of alternative services to meet the cell system capacity needs of today's residents.

When IDC released a report recently that worldwide 100.9 million smart phones were shipped in the last three months of 2010 compared to only 92.1 million PCs. Considering that virtually every one of those phones has Wi-Fi capabilities and that 50% of phone usage is conducted in the home, users expect to be able to use their phones over a community wide Wi-Fi network. Having a wireless router in common areas is probably not going to be sufficient to satisfy residents' demands, nor is having a community wide Wi-Fi network that was designed for Laptops and not the much weaker Smartphones going to make the majority of residents happy. The recently released Kineto Smartphone survey has some really revealing information, such as:

88% of respondents are interested in a service which offers free or discounted Wi-Fi calling.

43% of Smartphone users use Wi-Fi daily while 64% use it at least 4 or more days each week.

43% primarily use it because it's faster than the cell network, while 45% use it because it's easier to access the internet.

AND FOR THE MOST TELLING STATISTIC: 78% indicated an interest in using Wi-Fi to improve indoor cellular coverage.

"Outside of the loss of data traffic, [cellular] operators have hesitated about managing their own Wi-Fi networks because they want to be sure the experience is up to par. When it's a free for all, users will get variable quality, which is a problem for operators who want to slap their brand on it", says Current Analysis analyst Peter Jarich.

There are owners that still wish to provide their residents with wired internet access. As such, SON has the capability to deploy an integrated Wired and Wireless network where the user can access either, and switch seamlessly, with their custom created User ID and Password property wide.

By deploying robust, high speed Wi-Fi Networks, building residents are able to use virtually all Wi-Fi devices. These devices include: Desktop computers, PC, Mac, IPad, PSP, PS3, Xbox, Wii, VOIP phones, Smartphones, DVR, TIVO, Chumbys, Wi-Fi Cameras, and Wi-Fi enabled GPS systems.

Wireless Fidelity (Wi-Fi) introduction

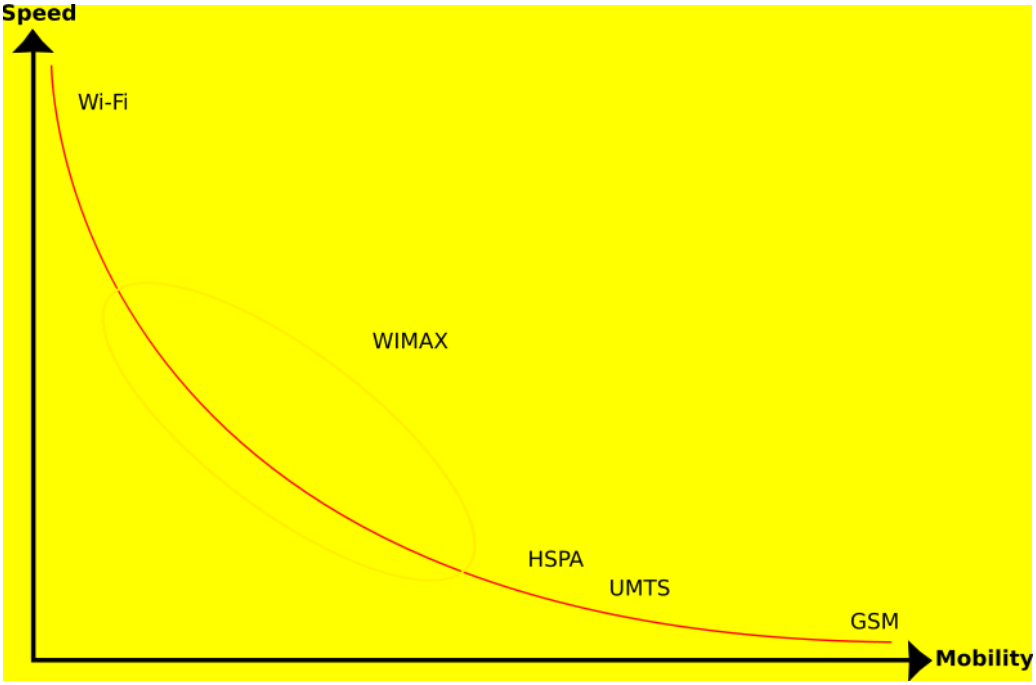
Wi-Fi is the trade name for the popular wireless technology used in home networks, enterprise environments, mobile phones, video games, and other electronic devices that require some form of wireless networking capability. In particular, it covers the various IEEE 802.11 technologies (including 802.11n, 802.11b, 802.11g, and 802.11a). “Wi-Fi” operates in the unlicensed 2.4 and 5 GHz radio frequency (RF) spectrum, also known as the Industrial, Scientific, and Medical (ISM) band.

Wi-Fi technologies are supported by nearly every modern personal computer operating system, most advanced game consoles and laptops, the majority of Smartphones, many printers, power monitoring devices and other peripherals.

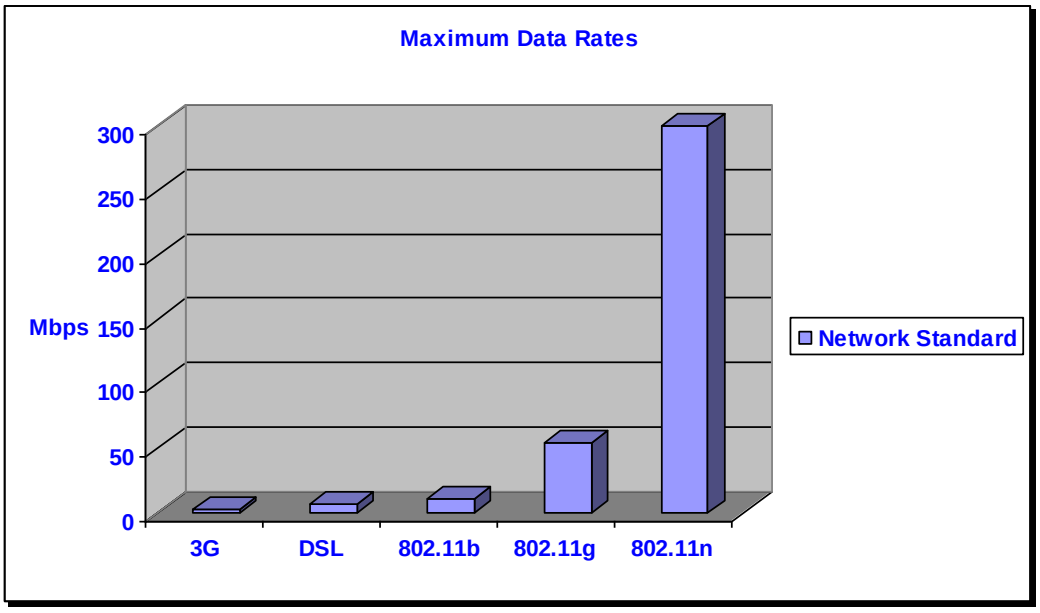
The purpose of Wi-Fi is to provide wireless, high speed, access to digital content. This content may include applications, audio and visual media, Internet connectivity, or other data. Wi-Fi generally makes access to information easier, as it can eliminate some of the physical restraints of wiring; this is especially true for mobile devices.

Managed Wi-Fi is the provisioning of Wi-Fi in multifamily and hotel properties with a network designed to avoid radio frequency interference, ensure that capacity is available for all users, proactively monitor the health of all components of the network, and respond to any issues that users may encounter.

At present, 802.11g is still the most common standardized Wi-Fi and wireless Local Area Network (LAN) technology on the market. Data transmission rates for these standards transmit at up to 54 Mbps. The new 802.11n standard, with which new devices are now being equipped, provides speeds up to 300Mbps. The 802.11ac standard, due to be ratified in late 2012, will provide speeds up to 1 Gigabit per second. In 2010 Spot On Networks started to deploy 802.11n networks (backward compatible with b,g) in both all community and common area only deployments. The chart below indicates the relationship between relative speeds and relative mobility.



With the proliferation of 802.11n, buildings are assured of being able to provide their residents or guests with enough bandwidth for the foreseeable future.



Bandwidth Backhaul

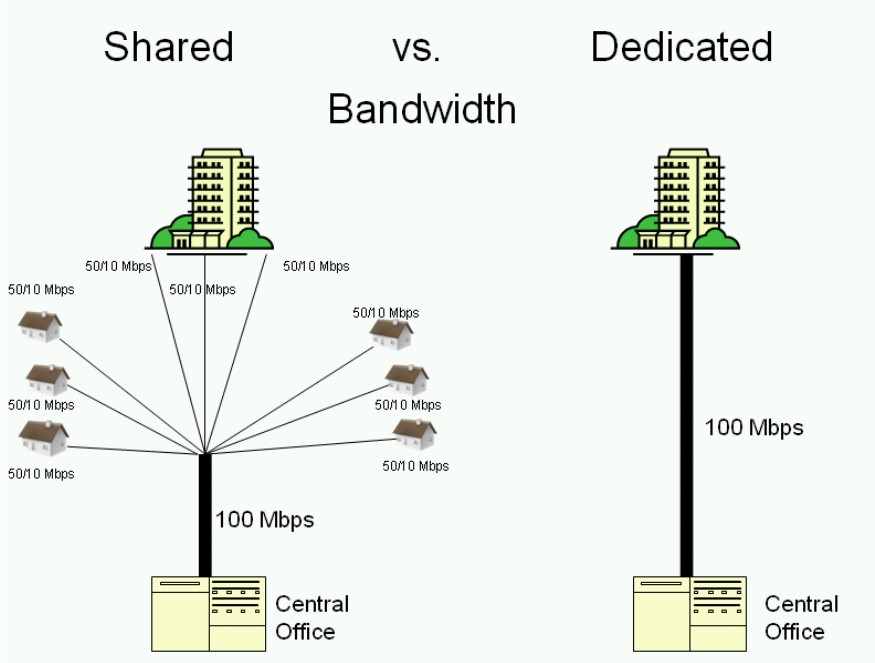
Once the design of the Wi-Fi and/or Wired Internet network has been completed, taking into account building construction, proximity of users, types of users and coverage areas, there is only one item left to consider, and it's crucial: ***Bandwidth Backhaul***. Outside of the physical

design of the network, there is nothing that can ruin a user's internet experience more than not having enough bandwidth. It would be easy to simply use a rule of thumb that states: 'For every 100 users you need to have X Mbps (megabits per second) of bandwidth available. Unfortunately bandwidth is not a black and white decision. The amount of Bandwidth needed for a high quality internet experience is dependent upon many factors such as the demographics of the residents which determine the type of internet usage, type of deployment, number of users per unit and amount of bandwidth allocated to each resident/guest. Spot On Engineers have the experience to determine necessary bandwidth for each demographic and type of deployment.

SLA (Service Level Agreement). SLAs need to be implemented no matter the demographics. Simply stated, SLAs limit the amount of bandwidth each user has access to at any given point in time. With a high enough SLAs the user is still able to download movies but at a pre determined speed, thereby ensuring that the next user has access to his/her fair share of bandwidth. SON is currently deploying networks with SLAs ranging from 3 Mbps to 50 Mbps per user.

Shared vs. Dedicated Bandwidth

Many of SON's customers are not aware that there are actually two different types of bandwidth that can be purchased; shared and dedicated. When an individual purchases an internet plan from the local telephone company or cable operator the price corresponds to the amount of bandwidth they are allocated. Typical plans range from 1.5 Mbps download and 768 Kbps upload to 50 Mbps download and 10 Mbps upload. The prices typically range from $19.99 to $200.00 per month. Conversely, when SON purchases a 100/100 Mbps dedicated internet circuit we typically pay around $3,000 per month. So why couldn't SON just buy two 50/10 Mbps circuits for $400 and get the same performance than the dedicated 100 Mbps circuit? The difference is shared vs. dedicated bandwidth. The reason the local telco or cable company can offer these plans at such low prices is because they are shared bandwidth. When one reads the fine print in the telco or cable company's contract it states that the speeds are not guaranteed but are 'Up To' speeds. That is because the bandwidth is being shared with everyone in the neighborhood.



In this rather crude example one can see that in the shared bandwidth scenario the 100 Mbps circuit brought into the neighborhood is shared by many users. The provider is promising 'up to' speeds that allow the individual user access to 'up to' the contracted amount of bandwidth. BUT, if everyone is on the internet at the same time, each user will only get a fraction of what they have contracted for. That is the reason why the cost is also a fraction of the dedicated bandwidth price. On the dedicated side, one can see no matter what time of day, the 100 Mbps is guaranteed for that building. Of course the price difference is significant. In a typical 300 unit building the per unit charge for two 50/10 Mbps circuits would only be $1.34. In that same building, a single dedicated 100/100 Mbps circuit would cost $10 per unit. As a compromise, an owner may purchase five 50/10 Mbps in order to secure a larger piece of the total bandwidth brought into the neighborhood. SON has networks utilizing either dedicated or shared bandwidth. The bottom line is that cost has to be weighed against benefit.

To summarize, bandwidth is one of the most critical factors that need to be considered when offering managed internet to residents or guests.

Benefits of offering Managed Wi-Fi

Building owners, managers and hotel operators have realized the many tangible and intangible benefits of offering managed Wireless and/or Wired internet to residents or guests. Managed Wi-Fi brings the capability of wireless high speed Internet access to all areas of a residential complex or hotel without troublesome interference from large numbers of competing consumer wireless routers. The following discussion will be broken down into two parts: benefits to residents and benefits to property owners and managers.

Spot On Networks' Managed Wi-Fi has been implemented utilizing proprietary software and standard hardware components in the Network Operations Center and the SON Monitor.

The integration of these components into the Managed Wi-Fi networks enables the monitoring of such important functions as bandwidth utilization, component operation, network health, air interface and interference. These components also provide the capability to alter network characteristics from Spot On's Network Operations Center to optimize network performance.

Benefits to residents:

1) Apartment wide coverage. Many apartments have only one hardwired Internet jack which is typically located in the living room. This allows only one device access to the Internet at a time. A parent needing to be online after work is now competing with their children who may wish to play video games with their friends across town or across the country. Wi-Fi allows all users in the apartment to use the Internet at the same time.
    a. Use the Internet in any room in the apartment.
    b. No wires to trip over or break.
    c. Mobility- No tethering.
    d. Smartphone support and support of devices with no Ethernet adapter.
2) Ubiquitous coverage throughout the entire community. Residents can now surf the Internet in their apartment, their friends apartment, the pool, or in the other community areas. Community wide Wi-Fi also provides coverage for smartphones, netbooks, IPads and portable gaming devices anywhere on the property.
3) Wi-Fi or VOIP calls can be used community wide, replacing residents' cell phone calls. Residents can now choose lower cost cell plans with fewer minutes and save money. This service may also supplement cell phone service in the event of poor in building coverage.
4) Higher speeds at lower prices.
5) Redundancy through multiple bandwidth providers assuring greater internet uptime.
6) Specially trained Spot On Networks, not outsourced, human customer service.

Benefits to property owners:

1) Increase the value of your property.
2) Attract more technologically savvy residents.
3) Increase your brand awareness and exposure.
4) Eliminate headaches for community managers and sales and leasing agents.
5) Increased rental fees.
6) Increased average lease lengths.
7) Creates a community experience.
8) Customized, branded, marketing material.
9) Dedicated personnel that have thorough knowledge of your property and its network.
10) Optional additional revenue stream.
11) A fix for poor cell phone coverage.

Deployment Options

Wi-Fi Community Area deployment

SON can deploy Wi-Fi in the community's amenity areas, such as the library, recreation room, laundry room, fitness center, business center, lounge, pool and rooftop. This will allow the property to advertise free Wi-Fi in the community areas while simultaneously driving traffic to those areas.

Optionally SON can also connect the wired computers in the business center to its network, thereby eliminating the properties legal responsibilities.

Finally, SON has an optional content filter that eliminates the possibility of residents surfing inappropriate and objectionable websites in the community areas.

Full Community deployment

The other alternative is to deploy managed Wireless and/or Wired internet throughout the entire property. This will allow users the freedom to access the internet not just in any room in their apartment but also in any other apartment and in all of the community areas. A seamless Wi-Fi network allows residents to utilize not just their laptops but also IPads, Wi-Fi equipped Cell phones, portable gaming devices, DVR, TiVo and Wi-Fi enabled radios. With today's advancement in wireless technology and the proliferation of wireless devices, there is no reason to restrict residents to one room in one apartment to utilize the internet.

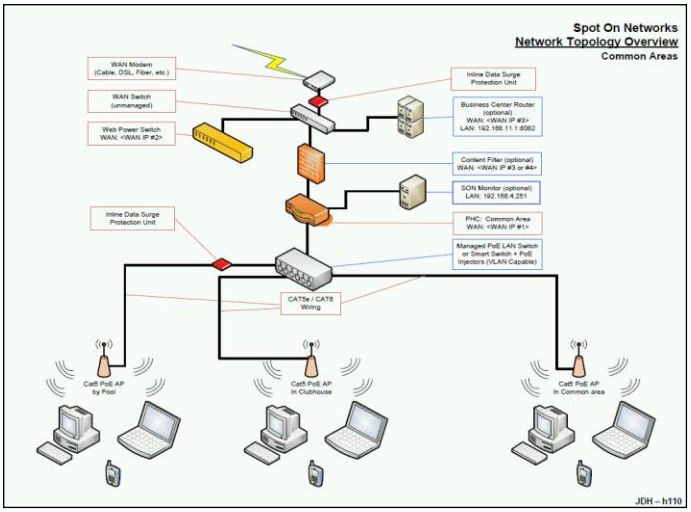
Wired and Wireless Community deployment

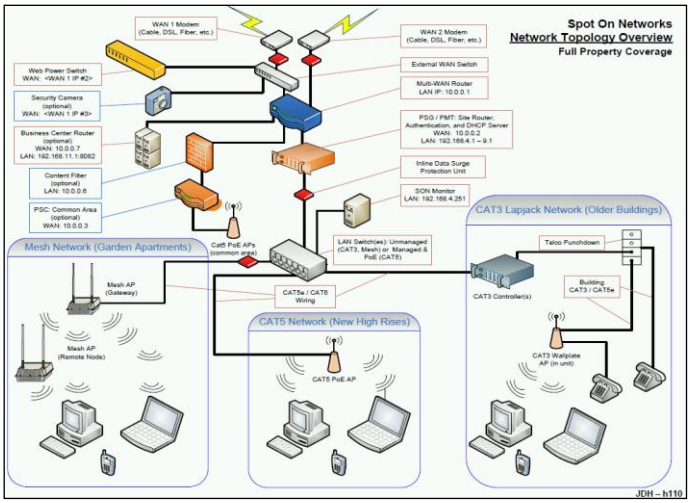
SON understands that there are still owners out there who have residents demanding community wide Wi-Fi coverage but are hesitant to not provide wired internet service as well. SON has deployed these networks where a resident or staff member can utilize their User ID and Password both on the Wi-Fi and Wired networks. The user will not experience any difference in speed between the networks. Of course there is an additional cost associated with this type of deployment since additional equipment has to be installed. One other factor to consider is whether or not to 'light up' all of the wired connections in each apartment or just one. If the owner decides to 'light up' all of the jacks in the unit, an additional switch per unit has to be deployed which adds significantly to the cost of the deployment. SON has developed an alternative solution to avoid the higher costs associated with a Wi-Fi and Wired Internet solution. SON can deploy a wireless to wired bridge which takes the Wi-Fi signal and allows users to plug in up to 5 wired internet devices into this bridge. These wireless to wired bridges can be deployed in all apartments or more often, only to those residents who wish to have a wired connection. Now owners and residents can enjoy the best of both worlds at a price that makes sense.

Spot On Networks Technical Description

As stated above, SON Networks deploys a variety of different types of Wi-Fi and Wired internet networks. On the Wi-Fi front we deploy inside the hallways or units using enterprise grade Access Points and Outside-to-In deployment using mesh type outdoor Access Points. SON has also started using a third deployment methodology which allows Access Points to be connected via existing CAT3 or regular telephone lines. The type of deployment depends upon numerous factors discussed below. Three sets of equipment are deployed by SON; in the telephone closet or demark, in the telephone closets on the floors/ buildings, in the units/hallways or outside around the property.

SON Networks Wireless Deployment





Equipment Detail:

Controller- These controllers provide for user identification, billing, service level agreements, usage reporting as well as providing CALEA compliance.
External WAN Switch- These switches allow SON to share the Internet connection between the web power switch and the Syswan.
Multi WAN Router- These routers allow SON to couple multiple broadband circuits together at a property.
Firewall- These firewalls are configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria established by SON. A firewall will only be installed in very large installations or properties with a large student population.
Power Switch These switches protect SON's equipment from power surges as well as enabling SON to remotely power cycle its equipment.
Power Over Ethernet Switches- These switches enable SON's Access Points to use power over the CAT6 cabling, thereby eliminating the need to draw power from the apartments.
Indoor Access Points (APs)- These APs will be installed either adjacent to the Apartment Distribution Frames (ADFs) in approximately every 3rd apartment or in hallways. These

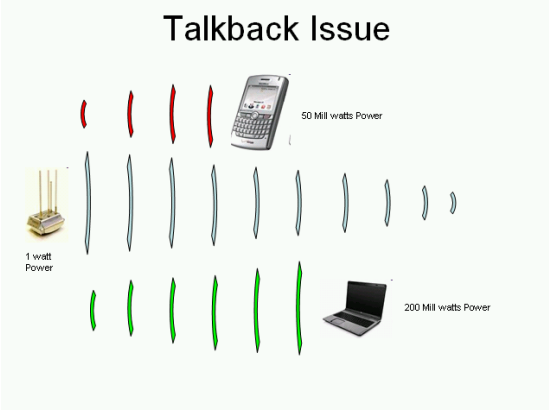
intelligent, enterprise grade APs are designed to provide the best Wireless Internet experience to a large number of users.
Mesh Access Points(APs)- These hardened, weatherproof, outdoor APs will be installed on Light posts, Garages, or eaves of buildings to provide Outside to In Wi-Fi coverage.
CAT3 Access Points(APs)- These APs will be mounted on top of an existing telephone jack in the units.
SON Monitor- This proprietary box is designed to monitor the health of the SON Wi-Fi network.
Internal Managed LAN Switch- This switch allows SON to connect its APs back to the controller.

SON Networks' equipment in demarc/ telephone closet for medium sized property or common area only deployments.

SON Network's equipment in demarc/ telephone closet for large property.

Talkback

Many Wi-Fi providers simply deploy networks that allow users to access the network with their laptop. Over the last 18 months SON has seen a huge increase in Smartphone usage on its networks. We believe that with the end of unlimited cell phone data plans, this usage is only going to grow faster. As such, a Wi-Fi network has to be build from the outset to accommodate not just powerful Wi-Fi devices such as laptops but also low power devices such as Smartphones and portable gaming devices. The reason why low power devices don't work very well on most Wi-Fi networks is called Talkback.



As one can see from the diagram, SON's most powerful Access Points emit 1 watt of power. That

allows users to see the signal from an extremely far distance. The problem is that users can see the signal, but they can't talk back to it. That is because their devices don't have the power to send their data over a long distance. This becomes even more problematic for low powered devices such as Smartphones. A good way to explain this is to imagine standing on the 50 yard line of a football stadium and speaking to the Press Announcer. When the Press Announcer speaks over his high powered sound system, the person can hear him clearly. However, if the person tries to talk back to him, there is no possibility of him being heard. To overcome the Talkback issue, it is not enough to deploy high powered Access Points, but they have to be within a certain distance of the users and intelligently deployed, in order to facilitate all Wi-Fi devices.

Network Monitoring

Spot On Networks proactively monitors its networks via the Network Operations Center (NOC), which is located in New Haven, Connecticut. The NOC monitors all aspects of each property's network with its embedded controller, SNMP queries through Nagios, and a customized Networks Operational Support System to provide 7x24x365 monitoring of site status, equipment status, user activity, and bandwidth status and usage, thereby ensuring SON's networks to be optimized for a positive user experience. Multiple dashboards have been created to ensure that all issues are constantly addressed and automatic notifications are delivered to the necessary SON personnel responsible for managing service issues.

These technologies allow the NOC to proactively work on potential problems before they become user issues. Field technicians can be dispatched to a site to take corrective measures and restore optimal service. The NOC monitors the circuits going into a property, and when circuit outages occur, they maintain the site through redundant circuits until a circuit provider dispatch is arranged to correct the problem. Up to the minute status of network issues and outages are provided by the NOC to the Customer Service Center via a common database. A customized Trouble Ticketing System has been created and is used to ensure that all user questions and issues have been responded to in a timely manner. Customer Service is therefore able to respond quickly when customers call to report a problem or concern with their SON service. SON Networks, LLC deploys its residential complex-wide Wi-Fi and/or Wired high speed internet service using distributed intelligence loosely coupled with a central intelligence apparatus. This "cloud based diagnostic system" provides an exceptionally economical, but extremely comprehensive network monitoring, control and self healing set of features and functions that provide users and building owners with a secure and easy to use service.

SON's distributed network is comprised of a Site Network, located at the property, and the before mentioned Network Operations Center ("NOC"), connected to the Site Network in real time through the "cloud". The Site Network contains a Controller, Multi Wan Router and SON Monitor that provide real time monitoring and control capability for all components of the network including Access Points, Switches and Routers. Using multiple bandwidth paths, SON is able to add capacity and provide fail over directly from its NOC.

SON's proprietary operating platforms, coupled with its automated data bases of individual network elements within the building network, not only provide detailed information about the

failed component, but establish an escalation process via a set of dashboards to keep all levels of SON personnel informed. The addition of new properties triggers a program that automatically creates configuration files for monitoring of these elements, so that our monitoring tools are always up-to-date. These configuration files are loaded into the appropriate tools to allow SON's NOC to monitor in real-time the performance of the elements, including up/down status and other Simple Network Management Program (SNMP) data.

SON has also deployed a Linux-based appliance called the SON Monitor that resides on the LAN side of each Site Network. This appliance allows network-specific optimization tools to run and allows the NOC to diagnose and repair certain issues, upgrade firmware remotely, and replicate the user experience on the network. Additional tools automate the collection of bandwidth and utilization information for review by the NOC on an exception-basis.

This infrastructure developed to monitor and control all aspects of SON's networks relieves the need to add personnel as SON adds more buildings and subscribers, reduces the cost of operations and maintenance, thus reducing overall costs to customers and partners while providing the highest level of service to SON subscribers that reduces workload for leasing staff and community personnel

SON's Customer Service, widely considered the best in the industry, is able to provide users with immediately satisfying answers and resolutions based upon the network monitoring and control, such that issues that might have escalated are eliminated as quickly as possible.

Equipment Monitoring

Spot On Networks deploys motion activated cameras in the telephone closets of its installations in order to monitor its equipment and to remotely assist on-site technicians. The camera, when transmitting, uses the SON Wi-Fi network.

Network and User Security - User**SAFE**tm

Spot On Networks designs and deploys ultra secure Wi-Fi and wired internet networks while making access to the networks as easy as possible for the end-users.

The first key aspect of network security is to ensure that only the users who are supposed to be accessing the network are allowed to log on. Every network has a "captive portal" that requires a user to log in before accessing the Internet, and logged in devices are tracked in real-time so that SON always knows who they are and how much traffic they are passing. The captive portal design is tailored to meet the needs of the different types of venues we service. Our residential networks require registration for residents to create their own user accounts using our unique "gold token" system. This allows the property management to control which users can create an account and thus access the network, and ensure that strangers cannot simply come on to the property and "steal" network access.

Once users establish accounts, they have the option to auto-authenticate their devices to the network to provide convenience by having the captive portal login process occur transparently for future access. For our hotel networks, guests receive a site-specific "security code" from the front desk when they check in. In combination with their name and room number, this code is used to ensure that only hotel guests and other authorized users can access the network. The code is unique for each hotel property and is automatically changed periodically for added security. For commercial venues, SON has developed an email-based login system where users enter their name and email address to login, allowing the commercial venue operator to collect contact information from users in their spaces and enable direct marketing applications.

User**Safe**™ is a mechanism that has been implemented in all of SON's wireless networks that prohibits devices connected to wireless access points from communicating with each other directly through the access point. By isolating each client device, SON's network creates a secure communication path to the internet without the possibility of hacking, "man in the middle" attacks or spoofing. . Virtual Private Networks, tunneled between access points and remote corporate servers, are fully supported.

All network traffic between the service controller at each property and the centralized customer registration, authentication, and database ' servers is transmitted via an https connection using SSL (Secure Sockets Layer) with 128 bit encryption. When the end user clicks "submit" on the captive portal to transmit his or her username and password to our servers, an https connection is established before the credentials are transmitted. Once logged on, the user's traffic is sent over the Internet based on the protocols required by the destination server such as http, https, ftp, POP3, etc. The SON network integrates with Chase Paymentech and Trustwave, to provide regulatory compliance with personal information security rules and secure handling of credit card payment information.

Service Level Agreements (SLA)

SON implements SLAs in order to ensure a high quality Internet experience for all users. Through demographic analysis, SON provides the optimized amount of bandwidth to each property. SON contracts with multiple bandwidth providers at its properties to ensure redundancy and maximum uptime. All residential customers have access to the same amount of bandwidth.

A good example of the reasoning behind SLAs is to think of a faucet where water flow increases as the faucet is opened. Water flow reaches a maximum when the faucet is fully open. No matter what is done, water flow will not increase further. It is analogous to the internet where the available bandwidth results in the maximum attainable speed. An estimated 5% of users use 50% of the available bandwidth. Not so with SON! Because SLAs allocate bandwidth to each user, SON can ensure that everyone has a quality, high speed internet experience. Regardless of the bandwidth brought to the property, without bandwidth controls, the same 5% of heavy users will use most of the available bandwidth. Using the water flow analogy, some users will get most of the water, while others get a few drops.

Deployment Methodologies

Wi-Fi networks cannot be deployed in a Multi-family environment without a detailed analysis of the property, which may also include a site visit to determine the many factors affecting Wi-Fi signals.

Items that negatively affect Wi-Fi:

Trees
Brick
Argon filled or Tinted Windows
Mirrors
Steel
2.4 and 5 GHz Cordless phones
Microwaves
Other Wi-Fi routers

Indoor and Common Area Access Points

Indoor Access Point 802.11 b/g/n

Outdoor AP for areas such as Pool and Rooftop

Spot On Networks deploys only intelligent, enterprise grade Access Points in all of its networks. All APs connect via CAT6 cabling to Intermediate Distribution Frames (IDFs), and from there to the demarc or telephone closet. CAT6 cabling cannot support lengths over 300 ft without external power injectors. These APs use Power over Ethernet, eliminating the need to draw power from apartments, or bringing in additional power to hallway locations.

In unit AP installation

Metal, mirrors, and brick degrade the Wi-Fi signal. A Wi-Fi user typically accesses the internet in the living room or bedrooms, which are areas typically furthest from the hallways. The network design must account for all of these obstacles and criteria. Because SON builds networks with overlapping Wi-Fi coverage, when a single AP goes off line, another one will

power itself up and take up the slack. This allows the user to have continued internet connectivity even the closest AP is temporarily off line.

Hallway installation

The hallway installation may have difficulty penetrating through the front of the apartments to the areas where users will use the service. This deployment method is still a viable alternative, providing a quality wireless internet experience but it might necessitate additional APs to be deployed. Hallway deployment will be utilized when in unit cabling is not a viable option. The benefit of this deployment is accessibility to the equipment.

Outside to In deployment

Outdoor AP up close

When the property does not have a central demarc or when CAT6 cabling cannot be installed, SON deploys a meshed outdoor solution. Signal testing is necessary at a property before the mesh solution is implemented because many factors affect the Wi-Fi signal from penetrating into apartments. Signal testing ensures better coverage for individual units and a better user experience.

These outdoor APs are hardened, weatherproof, and intelligent. The APs have many advanced capabilities that increase the user experience: they are self routing, and self healing, which allows SON to deploy a high speed, reliable community wide Wi-Fi network. SON deploys these APs on top of light posts, garages, and the eaves of buildings. There are many design considerations that need to be understood to provide adequate coverage. Spot On Design Engineers have a significant amount of experience in providing excellent coverage.

CAT3 (Telephone wire) Access Point Solution

SON has received many requests from property owners and managers to install Full Community Wi-Fi networks at existing properties where neither the Indoor CAT5/6 nor the

Outdoor mesh solutions are viable alternatives. SON has begun deploying APs in units using the existing CAT3 or telephone wiring. These APs are hard mounted over an existing telephone jack in every 3rd or 4th apartment. They draw power over the telephone lines eliminating the need to plug them into an external power source. In most instances, the user can still plug a telephone into the AP in order to make calls.

Access Point Connected to Telephone line

Branding

As with all amenities, a property must decide which one to invest in. Most times that decision is based on the Return on Investment (ROI). Sometimes the ROI is easily measureable; sometimes there are less tangible benefits. Take for instance this quote from one of our property managers:

The leasing party went great! We had everyone rushing to get their leases signed and back into us in order to get the free Wi-Fi internet. Of course, having the incentive helps because it creates a sense of urgency for the residents and allows us to secure their leases earlier. This, in effect, gives us a more accurate outlook on our long term occupancy projections. For example, instead of waiting until 30 days before their lease expires to renew it, they will renew up to 120 days earlier in order to be one of people who qualify for the free Wi-Fi internet service.

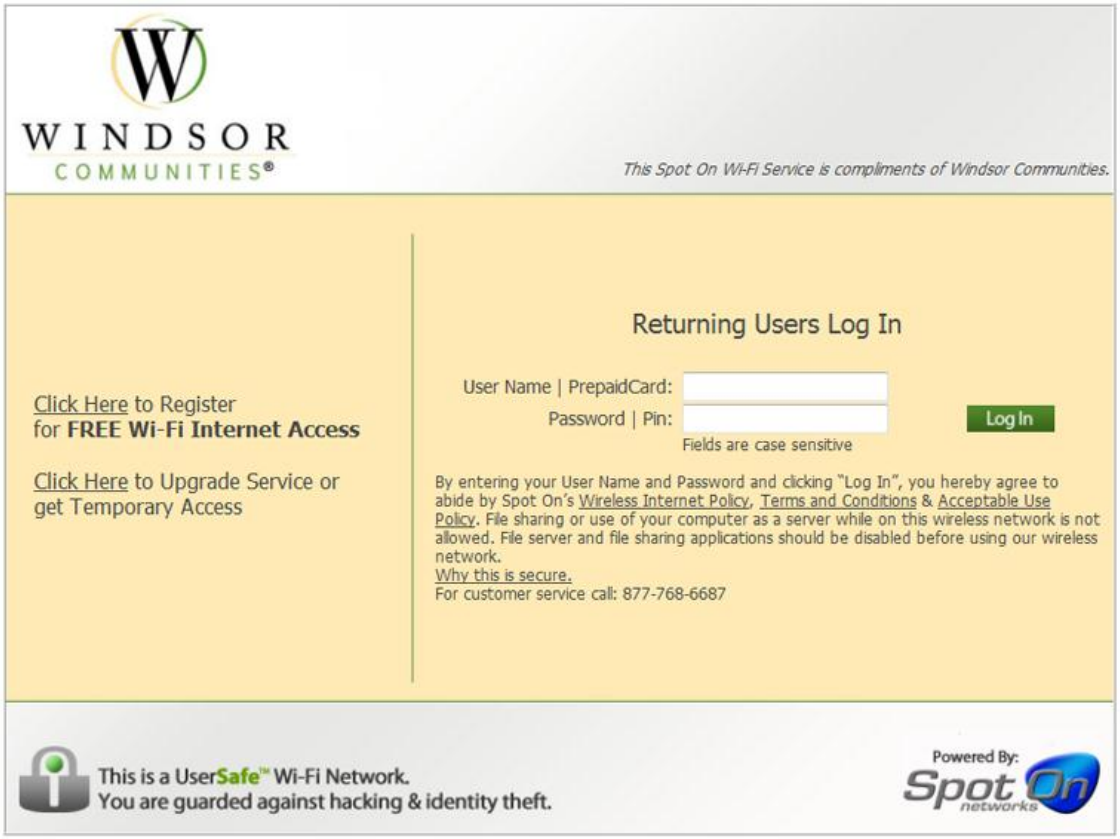
Crystal
Greenbrier Apartments

Increasing occupancy and retaining residents are two of the main reasons why our customers chose to deploy high speed wireless and wired internet. But why shouldn't the owner get the credit for offering Wi-Fi and let the provider, us, deal with all the administrative issues and customer service tasks? After all, getting exposure for your corporate brand can build resident loyalty across your entire portfolio. In order to help our customers achieve that goal, SON has developed the 'Golden Token' registration method. This consists of a branded Token that is to be handed out to existing and new residents alike.

Staff members hand out keys to the fitness center, rooftop terrace and pool; why not hand out the 'Golden Token' to the one amenity that your residents will use daily throughout your community areas and residences?

SON took branding a step further; we've also designed the log-in splash page to promote our customers' brand. How many residents used the gym today? How about the pool? But SON has learned, and can prove that virtually everyone used their internet today. That means almost all residents saw your brand today.

Internet log in page



CALEA is a 1994 statute that requires telephone companies to design their services so that they are easily tapped by law enforcement in need of "call-identifying information". In August 2005, following a request from the Dept. of Justice, the Commission moved swiftly to impose CALEA obligations on providers of broadband access services and "interconnected VoIP" services.

Communications Assistance for Law Enforcement Act (CALEA)

Overview

The Communications Assistance for Law Enforcement Act (CALEA) feature pertaining to Internet Service Providers, both wired and wireless, provides the ability to conduct lawfully authorized monitoring of a user's data traffic.

The main purpose of this feature is to lawfully monitor communications and collect information related to websites and addresses that a public broadband user visits while accessing the Internet at a location. This monitoring facility serves the purpose of capturing the URLs / IP addresses, visited by the clients during their sessions.

If an owner or manager provides Wi-Fi to their residents or guests themselves and not through a WISP that has CALEA compliant capabilities, that owner may be assessed a substantial daily fine (up to $10,000) when a legal entity issues a summons to provide the CALEA monitoring requirement. By having SON as your WISP you are completely compliant with this requirement.

Feature Implementation in brief:

The controller deployed by SON supports CALEA using its "in-session intercept" capabilities. The software embedded in the controller, coupled with the centralized operations support systems, equips law enforcement agencies with the ability to monitor the Internet packets traversing the network through the controller.

CALEA support implementation can capture either the full traffic or selected type of traffic, such as HTTP/HTTPS, TCP, or UDP. Currently, only the traffic headers are transmitted to a remote syslog server. However, the system has the capability to send all traffic from the controller on a secure tunnel (e.g. IPSec tunnel) or using a proprietary protocol as desired by the law enforcement agencies.

Monitor destination:

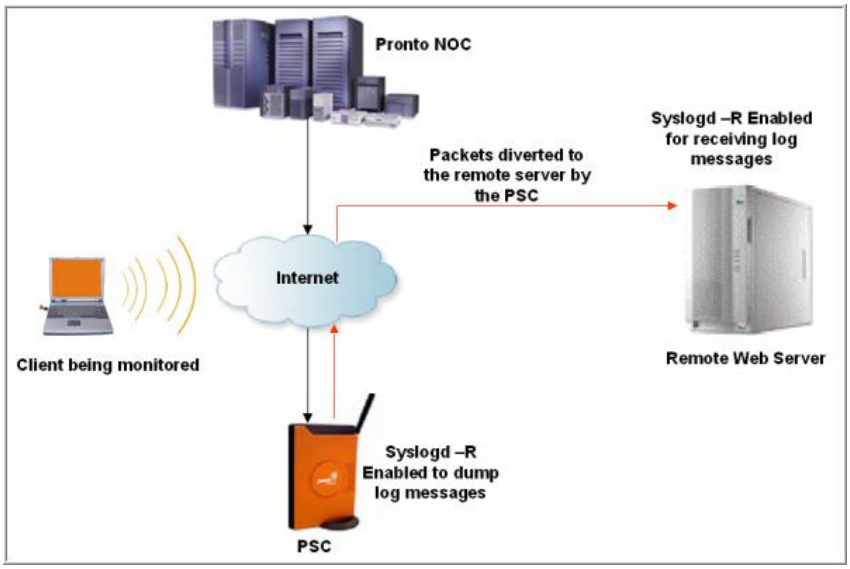
When enabling the CALEA support, a multitude of options are provided. These include:

- Monitoring specific users irrespective of the location

- Monitor specific locations for all users at that location
- On the fly monitoring for a specific user/location
- Duration of monitoring
- Traffic type, such as HTTP/HTTPS, TCP, UDP, and only headers.

The system has the capability to support any other option as desired by law enforcement agencies.

CALEA Architecture:



Summary

This White Paper was designed to give the reader a better understanding of the basics of deploying state of the art Wi-Fi and managed wired internet solutions in densely populated environments, the capabilities a WISP (Wireless Internet Service Provider) or ISP (Internet Service Provider) should have and the benefits to both residents, guests, Multi-family owners and managers and Hotel Operators. Over the last five years Spot On Networks has deployed over 400 multifamily properties and 80 hotels with Wi-Fi and managed wired internet throughout the United States. Many of the items discussed in this White Paper are a direct result from the experiences gained through these deployments.