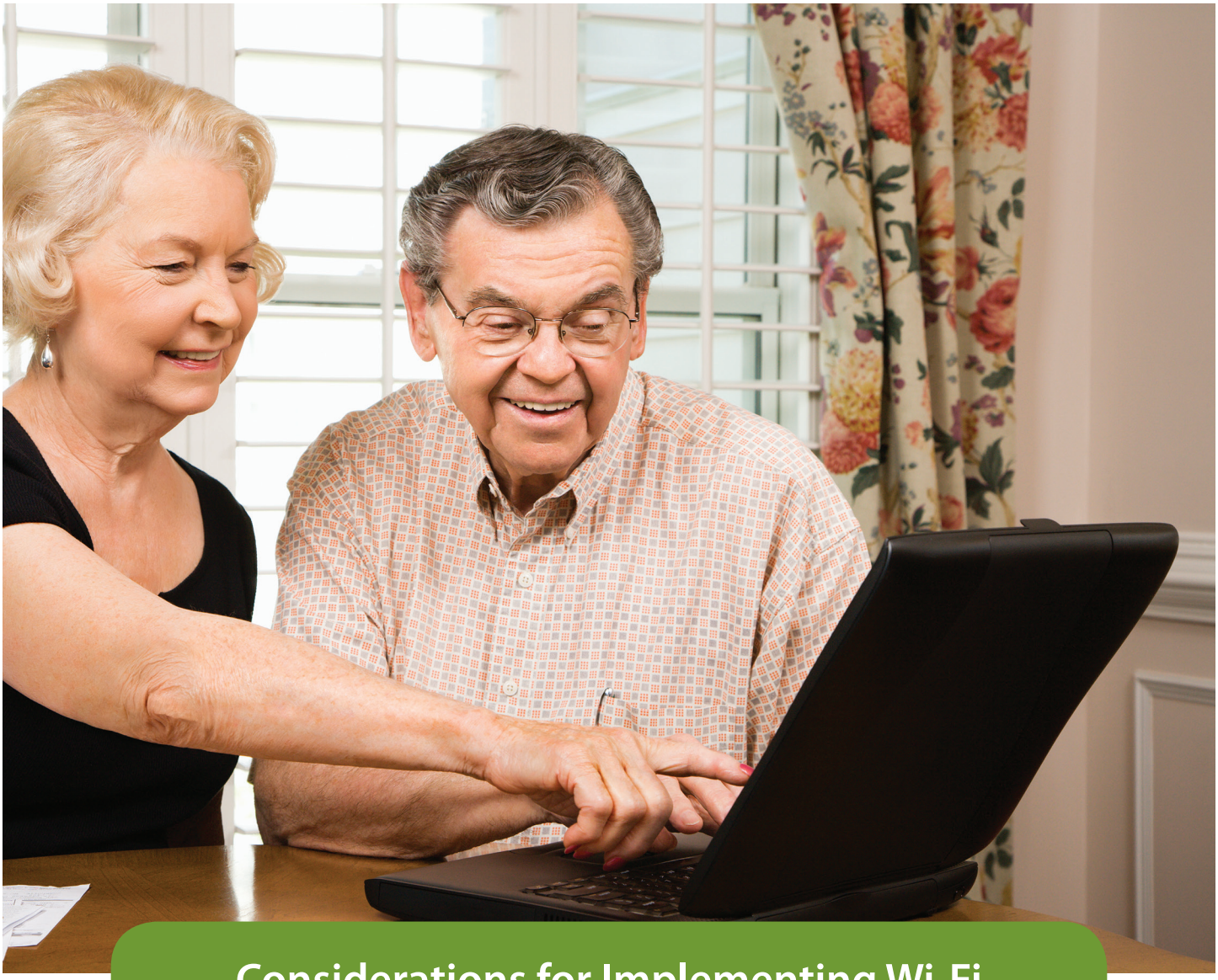

Considerations for Implementing Wi-Fi Infrastructure in Senior Living and LTC Communities

AgeTech west

Advancing a Technology-Enabled Standard of Care

White Paper

Executive Summary

In today's ultra-modern world, retirement communities must embrace the cultural reality of a new generation of Boomers and Seniors who are technology savvy. Not only this, but technological innovations weaved into the fabric of our businesses will continue to play a major role in transforming operational processes and how we care for our residents, as well as engaging our staff.

This new cultural reality translates into developing and upgrading our communities to "wired" campuses, buildings and homes that enable staff and residents to be technologically connected via Wi-Fi networks. The major challenge in this environment is the lack of communications standards that allow a myriad of technologies in various network configurations, to be effectively connected while being able to be effectively managed.

In response to senior living and long-term care providers' desire for practical, unbiased guidance on common technology deployment challenges, AgeTech West established a provider-led workgroup to do just that. This white paper aims to help information technology professionals and decision-makers successfully navigate the evolving world of Wi-Fi networks by sharing general considerations for design and implementation in senior living and long-term care communities. It also lays a foundation for developing technical best-practice standards.

There are many use cases for installation a Wi-Fi system, such as resident safety and security applications and internet hot spots. Each use case brings with it its own set of opportunities and challenges. Topics such as security and building construction, for example, can have a big impact on the overall design and implementation of a wireless system. Sample use case applications outlined in this white paper are:

- Resident and/or Public Wi-Fi – wireless internet access for residents or guests
- Wi-Fi for Business – wireless network access for business systems and software
- Wi-Fi for Emergency Responses and Wander Management Systems – PERS and wander technologies that utilize wireless devices and event reporting to central monitoring systems.

For each of the use cases we will review design and management considerations, as well as learnings and findings.

Every application is different and there is no way to capture the technical detail for each one. This document will attempt to provide a high level overview of the variables that need to be understood while rolling out a Wi-Fi network at a community. Insights will be given on the following topics:

- Wi-Fi Technology Overview
- General Considerations
- Building and Campus Infrastructures
- Regulatory Restrictions
- Support and Maintenance

Finally we will end with a "Getting Started" section that includes topics related to the establishment of project business objectives, finding a consultant, performing surveys and audits, cost drivers and operational support.

Contents

2 Executive Summary
3 Definitions
3 Background
Capacity
Demand
Interference
Structural Constraints
Infrastructure Readiness
Regulatory Restrictions
Network Management
Security
Support and Maintenance
10 Use Cases
USE CASE: Resident and/or Public Wi-Fi
Example: Hotspot for a Public Area
Example: Community-Wide Wi-Fi on Campus
USE CASE: Wi-Fi for Business
Example: Business Wi-Fi in a High-Rise Community
USE CASE: Wi-Fi for Emergency Response and Wander Management Systems
15 Appendix A: Contributing Participants
16 Appendix B: About AgeTech West

Definitions

- Wi-Fi – A wireless system that conforms to IEEE 802.11 standards (not be confused with mobile phone, bluetooth, or other proprietary radio frequency wireless systems)
- Bandwidth - Speed and capacity of network
- Wireless Access Point (WAP) – A wired or wireless device that allows other devices to wirelessly access the network
- Quality of Service (QoS) – A means for allowing higher priority traffic the right of way through a network
- Traffic Shaping/Policing – A facet of QoS and a means to limit bandwidth to devices
- VLAN (Virtual Local Area Network) –A means for allowing multiple logically separated networks on a single physical network
- SSID (Secure Set Identifier) – The name given to a Wi-Fi network
- Hotspot – A location where Wi-Fi is available
- Attenuation - The amount of radio single loss suffered through a given medium (air, trees, building materials)
- PoE (Power over Ethernet) – Allows an Ethernet cable to provide power to a device without separate power supply
- Heat Map – A wireless signal strength map depicting coverage as an overlay on a floor plan
- Floor hopping – Related to a multi-story building, where location services software identifies a wireless event on a different floor than it actually occurs
- Oversubscription – Promising more bandwidth than can be delivered all at once, with the idea that bandwidth requirements will be met a majority of the time

Background

A wireless network is a network that allows for data transmission between two or more devices without a physical connection. In recent years, wireless connections like Wi-Fi have increased bandwidth and stability to a point where they can seriously be considered as a replacement for or in place of a wired network. Although there are many varieties of wireless technology available, the 802.11 standard developed by IEEE (Institute of Electrical and Electronics Engineers) provides a family of specifications for what is now termed Wi-Fi. This includes addendums a, b, g, n and ac which provide further description of bandwidth capability.

A summary of these standards is found in the table below with rule-of-thumb values.

Table 1. Summary of 802.11 Standards

Standard	Frequency	Range	Typical Data Rate	Max Data Rate
a	5 GHz	115 ft	23 Mbps	54 Mbps
b	2.4 GHz	115 ft	4.5 Mbps	11 Mbps
g	2.4 GHz	125 ft	19 Mbps	54 Mbps
n	2.4/5 GHz	230 ft	74 Mbps	450 Mbps
ac	5 GHz	100 ft	250 Mbps	1300 Mpbs

Wi-Fi performance goals are generally driven by the area of coverage and the bandwidth desired. It is important to design to meet the aggregate performance needs of all use cases. Some use cases may have other design requirements that are a component of performance goals (for example, location services accuracy is proportional to access point density).

In order to meet a performance goal, the following design variables should be considered:

- Bandwidth capacity
- Bandwidth demand
- Structural constraints
- Electronic interference

At a high level, the following equation can be used to qualitatively describe performance:

Performance = Capacity – (Demand + Interference + Structural Constraints)

Actual performance will almost never match what a system is designed for. There are no hard numbers that can be plugged into an equation to ensure predictable results.

Capacity

Wireless bandwidth capacity is a function of the maximum bandwidth provided and the maximum number of devices connected to any given AP. These two variables dictate the access point density and layout required to meet a performance goal.

Bandwidth capacity can be limited by the ISP bandwidth, wired LAN infrastructure to which the wireless is attached and/or the limits of the wireless infrastructure itself. For example, a 100Mb wireless infrastructure will not be able provide 100Mbs of bandwidth if the ISP provided bandwidth is 50Mb. The aggregate current and future performance needs for a particular community should drive the bandwidth capacity requirements.

When designing access point layout and density, it is important to consider the number of devices that may be connected to an access point at a given time. Commercially available access points have capacity recommendations that vary by vendor and model. These recommendations provide a rule of thumb for the number of devices that can share a single AP and still provide usable bandwidth. In general, this number ranges between 20 and 50 devices.

Demand

Demand is determined by end-user application needs (browsing, streaming, etc.) and the number of end-users. In general, a Wi-Fi emergency response pendant will require less bandwidth than streaming audio on a tablet PC. It is important to note that demand is frequently dynamic, with peak usage periods that draw higher than usual bandwidth.

Table 2. Bandwidth Requirements per Application

Application by Use Case	Nominal Data Rate
Web browsing	1 Mbps
Audio Streaming	1 Mbps
Video Streaming	2-4 Mbps
Printing	1 Mbps
File Sharing	2-8 Mbps

In designing a wireless system to meet demand, the variety use cases, the number of users and the peak usage times should all be considered. This is a best guess proposition based on who many users might be concurrently using the wireless system and what the use cases may be. Often a trade-off will be made to provide enough bandwidth most of the time to meet demand rather than designing to peak demand. This is called oversubscription. Keep in mind that Often, determining the bandwidth demand is a best guess based on concurrent users and it is important to know that bandwidth demand will likely increase, potentially rapidly, over time. Monitoring bandwidth can help you determine how utilization at your site is trending and inform decisions about when a bandwidth capacity increase is necessary and by how much.

Interference

Professional installers of wireless computer networks attempt to optimize their client's Wi-Fi network by strategically choosing a subset of the 2.4 GHz band for use by their wireless network devices. The use of a spectrum analyzer will allow a professional installer to determine what is currently communicating the in the wireless range you want to use, or determine if a range is fairly clean for usage. For example, the 2.4 GHz range of 2.401 – 2.473 GHz is separated into 11, 22 MHz channels. An installer could configure the wireless access point (AP) to use channel 6, and then all data communication will occur over the range of frequencies associated with channel 6 (i.e. 2.426 GHz – 2.448 GHz). But if other wireless devices (802.11 or non-802.11) are also transmitting

over this range of frequencies then your wireless network will suffer. So, when installing a wireless network or troubleshooting a poorly performing one, it is important to choose a channel that is not subject to interference from other devices. It is important to note that 801.11 Wi-Fi uses unlicensed frequencies, which are also in use by a wide range of electronic devices, such as microwave ovens and cordless phones that can be significant sources of interference.

Another source of interference can be rogue access points. Rogue APs can create havoc on your wireless network, as they are usually do not conform to the configuration of APs that were deployed intentionally. A rogue AP can best be described as one that was plugged into the company network with no or little pre-configuration completed. In addition to introducing interference on the network, a rogue AP may allow open the network up to unwanted or malicious activity.

Structural Constraints

Building Materials: The type of construction materials used in a building can have a favorable or negative impact on the deployment of a wireless infrastructure. In general, materials with lower density will allow Wi-Fi signals to traverse the building with the least amount of resistance. The following chart shows several common building materials and the impact they have on wireless signal:

Table 3. Building Material Interference Potential

Type of Barrier	Interference Potential
Wood	Low
Plaster	Low
Synthetic Material	Low
Glass	Low
Water	Medium
Bricks	Medium
Marble	Medium
Concrete	High
Bulletproof or Low-e Glass	High
Metal	Very High

Because most wireless implementations will occur in previously constructed buildings, this table is best used to help resolve any issues you may have with interference. If it is possible to identify the various materials in the building as you design your install, an installer can plan to minimize the impact of these materials by placing the access points in areas with less dense materials.

Building Layout: Whether designing a Wi-Fi installation for a single-floor, stand-alone building or a 30 acre, multi-story campus, the architectural layout of residential, business and shared spaces can pose a variety of challenges. Floor hopping, common to multi-story buildings, and cordless phone interference, common to dense residential buildings, are two such examples. Below are a few suggestions related to typical building layouts:

- **Tower and Multi-building Campuses**
  Tower/high-rise buildings are notorious for floor hopping. Floor hopping occurs when a device associates itself with an AP on a different floor than the floor it is on. Depending on your ability and desire to manage the complexity it would create, dividing up the floors into individual SSIDs can resolve that issue. By directing client's in a particular area on a floor to a specific SSID, that client will not hop to another floor. While this resolves the floor hopping issue, it does create a roaming problem if they want their device to be mobile. To resolve this, some clients allow for prioritizing which connection they use. You can make the SSID on their floor their primary, and the building wide SSID the secondary if the first is unavailable. A similar issue can occur in multi-building campuses, whereas a client will traverse buildings in search of the optimal signal. The same concept used for the tower building can also be used in these environments.

- **Coverage Area**
  The coverage area of an access point can vary based on a number of different variables. One variable to be considered is what 802.11 protocol you are deploying, and how many access points are needed in a particular area. 802.11bg are rated at 150 ft indoors and 300 ft outdoors, and 802.11a has roughly one third the coverage of 802.11bg.

That of course does not take into account any obstructions in either environment, which is another variable to consider. Another common variable to consider is the type of AP and signal strength of the transmitter. AP's designed for home use will typically not be as strong as ones designed for business or enterprise use.

When working outdoors, there are two different strategies that could be deployed based on the environment where the access points would be installed. The first is called Sparse Side Coverage, and is used when you have limited vertical mounting options and electrical service. While this is good when you have fixed assets like camera, it is not effective for VoIP or roaming network connectivity. The other strategy that could be deployed when working outside is called Dense Side Coverage. This is the typical strategy for campus type environments, as it uses are large quantity of access points to provide overlapping coverage. It also benefits from assets like buildings, available electricity, and cabling.

➤ **Outdoor Obstructions (e.g., Trees)**
When considering potential obstructions in your wireless deployment plan, it is important to consider current and future obstructions. While there may be a clear line of sight to one location today, there may be plans to develop in that path three years from now. Additionally, the time of year may have a bearing on the layout. If there are trees on your campus, consider when the trees are in full bloom. This will give you the complete picture of the size of the obstruction.

➤ **Indoor Obstructions (e.g., Furniture)**
There are various common items in a home or business that can obstruct the radio signal from the access point. The obstructions can work to absorb, reflect, and even refract the signal, which in turn creates a low signal. Below is a list of some of the more common items:

- Cabinets or drawers
- Mirrors, Glasses
- Metal Objects
- Thick walls and ceilings
- Aquariums

Infrastructure Readiness

Infrastructure readiness is a prerequisite for smoothly integrating a Wi-Fi network into the existing environment. Considerations include:

Network Wiring and Topology: In a perfect scenario, a building would have all the cabling and power required in exactly the right place when looking to deploy a wireless infrastructure. Unfortunately, unless you are building from the ground up, that is unlikely to occur. There are some things that you can look for when researching cabling for an existing building, which can provide options when creating your design. For example, in a two or three story building, if the apartments are stacked on each other all the way down, you can use a single path through those apartments to traverse the floors. Using a common closet on each floor can hide the cabling, and provide a path for additional services. This is important as each run, to each access point, needs to return to a central switch. If the distance is too great between the AP and the switch, creating a location to place a switch within the 300 ft. maximum copper distance would be required. If the distance between each switch location exceeds 300 feet then fiber cabling would be required.

Regardless of the location of each switch within a building or campus, each will have to be connected to one another, terminating at the main head-end piece of equipment at the main point of entry. While it is possible to link each switch to one another, all the way to the main point of entry, daisy chaining them in this way is not recommended. This is primarily because a single failure in one device, takes down every other device behind it.

Hardware: Understanding the capabilities of the various hardware options can be difficult. A general understanding of cabling limitations gives you some understanding of what equipment will be needed to pair the two.

➤ **Switches**
A switch is the network device that an AP plugs into. In most cases, the switch is used to supply power to the AP, so having a switch that has Power-over-Ethernet (PoE) will provide that

connectivity. As mentioned before, as long as the copper cabling distances is never more than 300 feet, a normal switch will apply. If the distance exceeds that amount, then a switch will need to have the capability of adding fiber transceivers. These transceivers take the fiber connection and allow it to be inserting into the switch containing all your copper connections. On a campus where you could have multiple fiber connections terminating in one locations, an aggregate switch would be required to connect everything together.

- **Access Points**
  There a numerous manufacturers of wireless access points and they all have their own strengths and limitations. Since this paper is intended for general use and is not focused on particular vendors, we will cover some of the capabilities that you should look for when researching equipment.

  As previously stated, power outlets will rarely be located exactly where you need them when placing access points. For that reason, it is much easier to run a low voltage data cable to that location and then power the device from the switch. Most of the vendors today provide access points with the ability to have them powered over the ethernet cable (PoE), and thus should be one of the core requirements in your search. Other feature that you should consider would be the ability to control a few, or many, access points from one device. A wireless controller allows you to manage all the devices connected to it as if they were one, a provides a much more robust and convenient means of device management. This obviously saves time, but can also be more expensive. It is recommended that if your installation includes more than ten APs, you may want to strongly consider a controller-based solution. A deeper look at network management and wireless controllers can be found in a future section of this paper.

Temperature Control: When locating your network equipment, it is import to consider the temperature that the equipment will be exposed. A location with insufficient heating or cooling can limit the life of the equipment or cause it to function erratically during temperature swings. It is also important to remember that an interior room may seem fine when first identified, however the equipment will generate additional heat after it is placed into service. Understanding the airflow requirements based on the size and shape of the room, will help keep your equipment in good working order.

Regulatory Restrictions

Regulatory restrictions may also impact Wi-Fi network design. Your engineering/install partner may not know these 'rules', so it will be important to determine if any of these apply to your project:

- Building codes
- HIPAA
- Sarbannes-Oxley
- FCC
- OSHPD requirements in skilled nursing (California)
- Electrical Code
- Fire Code

Regulations may vary by city, county and state so be sure to check with the relevant local or regional authority to determine what impact they may have on your wireless installation.

Network Management

There are several models for managing access points and their network and access configuration. Each access point has some level of on board functional intelligence. The intelligence may be onboard the discreet access point, on a local wireless LAN Controller, or located in a Cloud based service.

On a small scale, wireless access points can be individual hot-spots with their own management system, usually including a firewall and router with WAN/LAN ports like what you use at home. If you have many access points to configure in a community, even with APs connected to the same LAN, it is very labor intensive to log into each AP

to make configuration changes and to monitor activity. To be able to efficiently manage a large number of APs, there needs to be a point of central control such as a LAN based, or cloud-based controller.

Local LAN Controllers: A hardware controller device located on the local LAN is used to manage a set of local access points. The controller manages the configuration of multiple APs making global changes easier. In many cases the controller is in the data stream meaning that all of the wireless data must traverse the controller which can be inefficient. It does allow for advanced roaming management and other features, but also requires ever-increasing controller capacity when more access points are attached. Some drawbacks to this type of deployment are that controllers can be a single point of failure and also require maintenance, such as firmware updates.

Cloud-based Controllers: A controller-less solution is another option for multiple AP management. The term controller-less, however, is a misnomer, as the controller is either in the cloud, pushed out to the AP, or a combination of both. There are vendors that use a LAN-based controller which is managed in the cloud along with the APs. Other venders are entirely cloud managed. An advantage to a cloud-based system is that APs can be pre-configured in the cloud and when they are installed and turned on, they will report into the cloud controller and download the current configuration. Having a single management console for multiple sites, accessible anywhere, is also a major advantage over local LAN controller solutions.

Security

There is a wide range of security risks, regulatory requirements, and mitigation strategies that should be considered when designing and managing Wi-Fi networks and network security while keeping approved access for authorized users simple.

It is important to keep in mind that once a device has been granted access to a Wi-Fi enabled network it could have access to all the other devices on that local area network. It could then be used to conduct illegal or inappropriate activity on the Internet for which you as the provider of that access could be held responsible. The most common abuse today involves downloading copyrighted content, for which there has been quite a bit of legal action by content owners recently.

The least secure method of providing access to Wi-Fi enabled networks is to allow open authentication with a broadcasting SSID and no password required. A more secure method of providing access is to use Protected Access - a security protocol that uses passwords and, more commonly, longer passphrases to restrict access to Wi-Fi networks. It is recommended to use WPA2 encryption, which has replaced the much less secure WEP and WPA. Within WPA2 there are several encryption key methods available based on an operators need and infrastructure. The SSID can be set to not broadcast, which means that a device looking for a network to connect to will not see it as an available network to select. This is not a very strong security measure as there are some software products that read the SSID from the network devices that are connecting to that SSID.

If you provide network access and transport for employees who use it to access Protected Health Information (PHI) then you must consider both encrypting the network access and transport as well as to limit access to devices connecting to the network. There are a variety of methods that the encryption keys can be provided to user devices. Some use passphrases that are shared by authorized users, while more secure methods can include the use of digital certificates installed on end-user devices. The more secure solutions can require secondary servers (local or cloud-based) for user authentication. There are also integrated security methods and products that can integrate username and password (something you know) with validation of digital certificate or token (something you have) in order to provide strong security with reduced user complexity.

Network proxy servers and services provide network filtering. They can limit the sites that users on a network can get to on the Internet - and these internal or web-based services can help manage access by category as well as to "white list"

(always permit) or "black list" (always deny) access by domain. These can be helpful if an operator is looking to limit exposure to toxic, inappropriate, or high bandwidth demand sites, for example.

AAA servers (Authentication, Access, and Accounting) can combine the ability to limit device and user access to the network along with what they can access and also maintain an auditing of user access. These can also restrict access by Media Access Control (MAC) address - which is fairly unique to the network client hardware, but requires that your network administrator add those addresses for every authorized device.

Administratively providing discrete user names and accounts for every employee, resident, and guest provides the best control and accountability - however this may be impractical. At a minimum from a legal risk mitigation standpoint an Acceptable Use Policy or disclaimer is effective too (and can be a document signed before a password is shared with a visitor or resident, or even one acknowledged upon initial association with your SSID).

Network segregation is a strategy and practice of separating networks for variety of reasons, some of which have already have been covered. A simple guest Wi-Fi network with a separate physical local area network and Internet Service Provider (ISP) connection with no business access on it is already physically separated from the network and internet connection used by office, clinical, etc. staff. In areas where staff, guests, and residents are present this may not be as practical as logical separation, which employs the use of a VLANs (Virtual Local Area Networks) to allow very different uses of a physical network to be digitally separate from each other while sharing the same Wi-Fi Access Points (AP), LAN, network management tools, and internet connection.

Support and Maintenance

Any wireless system installation will bring with it an ongoing need for support and maintenance. As performance demands increase and technology improves to meet it, you will need to keep the components that make up your wireless infrastructure up-to-date with current firmware versions and patches.

Each hardware device will have it own useful life, so either by failure or scheduled refresh, all components will eventually need to be replaced. It is recommended that a refresh cycle. It is recommended to plan for refresh cycles of 4-5 years, where each year 20-25% of the wireless network components are replaced and upgraded.

User support also needs consideration. If residents will be given access to your wireless system, it is important to know how they will get support, if any. You may choose to provide direct IT support to your residents, outsource support to a third party or provide no support at all. If support is offered, there will likely need to be some kind of SLA attached to it. Whatever the decision, it is crucial to communicate it clearly to residents.

Use Cases

For the purposes of illustrating the design and implementation considerations for common scenarios, we have focused on three use cases, where each are grouped according to bandwidth demand, security considerations and up-time requirements (as defined by the business). The use cases are:

- Wi-Fi for resident or public use
  - Consumer internet access
  - Wi-Fi for business use
  - Internet access
  - Business applications and services
  - VoIP
  - Building systems (door access control, cameras, environmental monitoring)
  - Resident sensors, monitoring or remote data collection
  - Asset tracking
- Wireless for emergency response and elopement

USE CASE: Resident and/or Public Wi-Fi

The resident and/or public Wi-Fi use case pertains to the delivery of wireless internet access to existing residents and/or guests. Wi-Fi may be designed to cover specific areas (such as a resident lounge) or be community-wide. There may not be a performance goal for resident and/or public Wi-Fi, as cost or other considerations may cause an organization to provide a best effort level of service. If there is a bandwidth per user target desired, then this will drive the overall performance goal for the coverage area.

Design and Management Considerations

When providing resident or public Wi-Fi access, it may be expected that there will be more concentrated demand in common areas or during special events where a group of wireless users are more likely to congregate. Using a higher density of APs in common areas may be a design consideration. Insufficient AP density can result in user devices that have associated with an AP ("five bars") but still have no access to the internet.

As streaming and other rich media become more prevalent, consideration should be given to meeting future bandwidth demands. Besides increasing bandwidth capacity, which may be cost-prohibitive, tools to meet increased bandwidth demands include traffic shaping and policing. Traffic shaping or policing can limit the amount of bandwidth provided to a single device which can ensure that individual devices do not monopolize the available bandwidth. Similarly, oversubscription may be practical to allow for enough bandwidth for most users, most of the time.

Example: Hotspot for a Public Area

Business Requirements: Offer public Wi-Fi in a free-standing, single-story building that is used as a community common area.

Background: The approximately 20,000 square foot building is a new construction project that will provide an auditorium and health facilities to residents of the community. The building is steel-frame and wood construction with ceiling access. Wi-Fi access is desired in all areas of the building.

Design: The design called for 8 access points in order to provide thorough coverage across the building. Cisco was the network equipment vendor of choice to marry easily with the existing network hardware on the rest of the campus. Since this was a new construction project, theoretical heat mapping was performed digitally based on floor plans to aid in the access point layout. Network connectivity was to be run back to the server room in a different stand-alone building, which would provide access to the existing 50Mb business-grade internet service.

Installation: Network cabling was completed during the rough-in phase of the construction project. Since the construction called for a finished, rather than drop-ceiling, access points were mounted below ceiling level to allow for easy access and visible health checks. A physical heat map was performed after installation to confirm sufficient signal strength across the building.

An SSID was configured for public use using WPA2-Personal encryption and a password. The organization chose not to implement a password

policy at the time on installation, so as not to burden residents with a password that changed periodically.

Learnings and Findings: In addition to the other common areas on the campus, resident wireless internet access demand has increased steadily. We've seen an increase in the number of mobile devices in use and an increase in the use of streaming services. The jump in demand has given us the impetus to double our ISP bandwidth to 100Mb and switch to a fiber connection.

Example: Community-Wide Wi-Fi on Campus

Business Requirements: Offer public Wi-Fi in a campus setting comprised of several two-story multi-unit buildings, single-story cottages and several single-family homes in the neighborhood,

Background: The core campus was built in the 1960's and is currently home to about 175 residents. Recently, several single-family homes across the street from the core campus were added to the CCRC. Wi-Fi resident internet access was desired in all areas of the core campus including the single-family homes.

Design: The design requirements were to cover the entire CCRC, both indoors and outside, with Wi-Fi. A 100Mb Cisco wireless infrastructure was designed. Theoretical heat mapping was performed to optimize access point placement for coverage across all indoor and outdoor spaces. Network connectivity was to be run back to the server room in the administration building, which would provide access to the existing 50Mb business-grade internet service. The existing campus conduit infrastructure was audited and found to be unsatisfactory for the cabling requirements, so the design called for new conduit and fiber to be run to each building.

Installation: New conduit was run from the server room in the administration building out to utility closets in all of the multi-unit buildings and cottage clusters above existing covered walkways. Fiber was run from the core switch out to terminating switches in the IT closets in those buildings. From there, cat5e cable was run to the individual wireless APs inside and on the exteriors of the buildings.

To cover the open space areas, outdoor APs were installed, mounted in weatherproof enclosures, on the external walls of some of the buildings. To reach the single-family dwellings across the street from the core campus, additional outdoor APs were installed on some of their exterior walls and meshed with the outdoor APs on the core campus. One or more internal APs were installed per house and meshed to the network. In total, 101 indoor and outdoor wireless APs were installed to cover the entire campus.

A physical heat map was performed after installation to verify actual signal strength across the campus.

Learnings and Findings: The project yielded several key findings. We found that bandwidth use, especially from streaming, concentrated around an individual AP could significantly affect the performance of the Wi-Fi in that area. It was clear that it was important to communicate clearly and manage residents' expectations around the wireless system performance and encourage them to retain or purchase dedicated internet service from an outside provider if their bandwidth needs were not met by the shared Wi-Fi system.

We found that it is best to setup a dedicated DHCP server to manage wireless device leases to accommodate any sizable volume, as opposed to serving up leases off the wireless LAN controller or router.

USE CASE: Wi-Fi for Business

The Wi-Fi for business use case pertains to the delivery of wireless network access for business systems. Generally, Wi-Fi for business will include several systems with varying requirements. Wi-Fi may be designed to cover specific areas (such as a skilled nursing facility) or be community-wide. Some systems will have strict minimum connectivity requirements (bandwidth and stability), whereas best effort may be adequate for other systems.

After installation, heat mapping may be performed across the coverage area to ensure

that performance requirements are met. In the case that the heat map shows gaps in coverage, additional design work and WAPs may be necessary.

Design and Management Considerations

Demand and capacity considerations for the Wi-Fi for business use case are the same as that for the resident and public Wi-Fi use case, with the exception that quality of service (QoS) may be required. Configuring QoS allows higher priority business applications the bandwidth they need to function properly. For example, QoS could be utilized to provide wireless voice the bandwidth necessary for seamless functionality at the expense of other, lower priority applications, such as general internet browsing.

As with the resident and public Wi-Fi use case, web filtering is important when business applications are considered. Web filtering provides security and bandwidth savings, but more importantly, safeguards mission critical applications.

As operators become more dependent upon Wi-Fi networks to deliver a range of systems access for residents, guests, and staff the expectation that this service will be as available and reliable as other utilities increases. In order to meet that expectation there are various methods and practices that can reduce exposure (starting from the Wi-Fi point of use).

AP layout design should consider areas of use and plan for overlapping coverage and also additional APs where there can be a higher density of devices. Think of APs as light bulbs and ensure that key areas have coverage if one goes out. APs can be routed through multiple network switches and reduce the risk if a switch fails or needs to be serviced. These switches should be connected to Uninterruptable Power Supplies (UPS) for whose battery capacity needs to be sized appropriately and backed up by a generator - to compensate for any power outages. Switches can also be routed back to the main network or cloud via multiple network copper or fiber cables. Having multiple internet service providers (ISPs) at key sites reduces the risk of internet circuit outages causing a loss of connectivity to key data and services.

Example: Business Wi-Fi in a High-Rise Community

Business Requirements: Offer community-wide Wi-Fi in a high-rise setting to support several safety, security and other business systems.

Background: The building is a 23-story tower. Business offices are found on the 2nd, 3rd and 4th floors, with a skilled nursing facility and rehab center on the 22nd and 23rd floors respectively. Wireless coverage throughout the campus is required to deliver network access to the following systems and applications:

- Activities of Daily Living (ADL) capture using tablets
- Wireless smart beds
- Wi-Fi personal emergency response (PERS) and wander management system
- Wi-Fi door access control system
- Wireless IP cameras
- Facilities work order management using mobile devices
- Mobile computing using wireless-capable laptops, smart phones and tablets

Design: The design requirements were to cover the entire high-rise from underground garages to the 23rd floor with Wi-Fi. A 100Mb Cisco wireless infrastructure was designed. Theoretical heat mapping was performed with -70db being the baseline for lowest allowable signal strength in order to meet the requirements of our PERS system. The design called for utilizing an existing fiber run that traversed each floor of the building through a utility closet on each floor and utilizing existing cat5e cable running out to residential areas for connecting access points.

Due to the fact that PERS was to be running on our wireless system, a lot of care was given to infrastructure redundancy. A final design was called out with three access points per floor. The layout allowed for overlapping coverage, providing redundancy should an AP fail.

Installation: Switches were placed in the utility closets on each floor and tied to a UPS and emergency power. Existing cat5e cables were run

from the APs back to the switches, which were all connected using the existing fiber run.

Two wireless LAN controllers were installed: one in skilled nursing on the 23rd floor and one in the server room in the garage. Both controllers were plugged into a UPS and emergency power. VLANs were created for each of the major business systems to allow for segregated traffic and network management.

A physical heat map was performed after installation to verify actual signal strength across the building.

Learnings and Findings: Several key findings were uncovered at the completion of the project. A few areas were identified that did not meet the goal of -70db and additional access points had to be installed to meet the signal strength requirements for the PERS system.

We also found that some of the wireless door access controller cards, especially in the garage areas, had a difficult time staying connected to the door access control system. This did not cause the system to be inoperable, but did cause problems pushing out configuration updates. It was determined that interference in the garage areas from other mechanical systems and lots of concrete construction caused the signal strength to wane in several areas. More powerful wireless antennas were deployed in the garages to resolve the issue.

USE CASE: Wi-Fi for Emergency Response and Wander Management Systems

Wi-Fi personal emergency response systems (PERS) and wander management utilize wireless devices that communicate switch and field incursion events back to a centralized monitoring system. The following devices are typical of a PERS:

- Push-button pendants worn or carried by an individual
- Push-button pendants or pull cord devices mounted on a wall

Typical wander management devices include:

- Pendant watches
- Field incursion sensors (exciters)

Design and Management Considerations

When designing for a Wi-Fi PERS or wander management system, location services is an important component. Location services is a feature that uses triangulation among wireless access points to determine the location of an alerting device. The accuracy of location services is largely affected by the density of access points. There is an optimal AP density to achieve the best possible accuracy of location services. This needs to be a consideration during the initial design of the wireless system. Best practice design includes ringing the building with wireless access points to optimize triangulation.

There is always a minimum signal strength requirement for a Wi-Fi PERS system. This requirement is the basis for determining the wireless performance goal. To meet the performance goal, AP density may be three times that of other use cases.

In multi-story buildings, floor hopping is almost always inevitable. Depending on the location of an alerting device and the location of nearby APs, location services may misinterpret triangulation results and identify the alerting device as being above or below the floor it is actually on. Proper AP designs can help minimize floor hopping.

After installation, heat mapping needs to be performed across the coverage area to ensure that performance requirements are met. In the case that the heat map shows gaps in coverage, additional design work and APs may be necessary.

Getting Started

This paper provides general guidelines and considerations for implementing a Wi-Fi infrastructure. But putting all the pieces together in practice may seem daunting. What follows are some tips to help you get started.

Business Objectives: It is crucial to establish your business objectives in advance of any design or installation work. If your overall end-game is too grand and/or costly to accomplish at once, think about breaking up the project into phases. In order to set your performance goals, you need to understand your audience and how they will be using the wireless system now and in the future. Some important questions to ask include:

- What is the nature of the Wi-Fi service you wish to provide? Hot spot? Resident or business use only? Both?
- What is the number of users that will be using the wireless system?
- What will their individual bandwidth demands be and will they be streaming data?
- What do you anticipate for an increase in users and bandwidth demand over time?
- Do you have specific structural to be concerned with? Outdoor coverage? Concrete or metal construction?
- Have you identified interference sources that may affect your design?

Wireless Consultant: Rarely does a wireless implementation project go off without a hitch. But to increase your chances of success, it is recommended to partner with a local wireless network design consultant. They can help you work through the design details and navigate the decision-making process when considering cost vs. benefit tradeoffs.

Infrastructure Audit: Performing a network and building infrastructure audit is critical to determine readiness for any wireless system build-out. Some of the questions that are important to ask include:

- Is the existing network environment able to scale to allow for the necessary additional wireless devices?
- If cabling is required, is there existing conduit with enough available capacity to run the necessary cable? Is the conduit in good condition? If fiber is being run, does the existing conduit utilize adequate bend angles?
- What is the construction type of the building(s) being covered? Signal penetration can vary greatly depending on the material.
- Is there adequate ceiling/floor access to run cabling and mount access points?
- If planning to use location services features, are there clean building floor plans and campus maps for importing into the wireless management system?

Wireless Survey: Performing a pre-installation wireless survey and audit is important to achieve the desired wireless performance when the project is complete. Performing a theoretical wireless heat map as part of the access point layout and design process will provide a good guess as to the wireless signal coverage. It is also good to perform a real heat map at the end of installation to verify that desired signal strength was met. Knowing what residents' appetite for having access points installed in their apartments can help guide the design process. Some residents may see it as an intrusion in their home or an eye-sore, whereas others may welcome having a hot spot (and potential strong signal) in close proximity.

Cost: Installing and maintaining a community-wide wireless infrastructure can be an expensive proposition. There are several cost drivers that determine the overall initial installation cost. The AP density is a variable that will affect the quantity and cost of AP and network switch hardware. In addition to AP density, structural constraints, such as conduit capacity and ceiling access affect amount of labor and materials to complete the necessary network and power (if not using PoE) cabling.

There may be scenarios where it is desired to control capital costs by utilizing operational dollars for wireless projects. This could be accomplished by looking to cloud-based opportunities, such as controller-less designs. There are also companies who will install and support a community-wide Wi-Fi system for a monthly fee (which includes the installation and ongoing maintenance costs.

Appendix A

AgeTech thanks the following individual Content Contributors:

Lead Author: Chris Dana, Vice President, Information Technology, Episcopal Senior Communities

Steve Eichen, Chief Information Officer, Pacific Retirement Services

Ron Mosely, Regional Vice President, Sodexo Senior Living

Joe Gerardi, Senior Vice President, Information Technology and CIO , ABHOW

Brett Ortega, Information Technology Manager, ABHOW

Charles Garcia, Vice President, Information Technology, Eskaton

Aging Service Provider Content Contributors:

American Baptist Homes of the West:
ABHOW is one of the nation's most trusted providers of senior housing and health care.

As a nonprofit, non-sectarian corporation, we are committed to providing exceptional service to older adults, their families and the wider community.

Our passion makes us pioneers. We helped create the concept of continuing care when we opened our first community in 1949. Today, we operate 43 communities in California, Arizona, Nevada and Washington, with over 2,300 team members serving more than 5,000 residents. And our passion to make a difference is stronger than ever.

Episcopal Senior Communities:
Episcopal Senior Communities (ESC) is a public benefit, nonprofit provider of housing and services to seniors. The organization's core business is in six Continuing Care Retirement Communities (CCRCs) offering a full continuum of residential care and services ranging from independent living to assisted living and memory care and have a skilled nursing facility on site. In addition, ESC owns/sponsors and operates affordable senior housing communities designed for low income seniors. In keeping with its mission and social responsibility, ESC also provides a wide variety of programs and charitable services. These programs operated with the help of volunteers and under the guidance of its Senior Resources Directors who are located in seven bay area counties offer an inventive range of low to no cost program options. These programs include resource referrals, coordination of friendly visitors as well as nutritional and other supportive services to seniors in need. The key programs in its home and Community based services are the Senior Produce Markets, Senior Center Without Walls and ElderWISE. ESC will celebrate its 50th anniversary in 2015 and is headquartered in Walnut Creek, California.

Eskaton:
Eskaton means "the dawning of a new day." We find inspiration in becoming a part of your extended family. Eskaton is a Northern California-based, nonprofit organization with over 45 years of experience. Our dedicated team members provide services and support for nearly 14,000 individuals who live in our communities or participate in our comprehensive Home Support Network. Beyond the numbers, Eskaton's positive reputation extends to our signature life-enriching programs; innovative health and wellness initiatives; professional staff training and development; and generous philanthropy. For you, your family, friends and neighbors, for society…Eskaton is transforming the aging experience.

Pacific Retirement Services:
Creating vibrant senior living communities is what Pacific Retirement Services does. PRS provides exceptional leadership to staff, residents and Board Members as an active part of each community, so that each community thrives and is responsive to the needs of its residents now and in the future. We're constantly striving for opportunities to improve the services provided to residents. PRS continuously evaluates our programs and physical plants, looking for ways to improve, expand, and keep ahead of technological advances in healthcare and industry trends. PRS-affiliated

communities are recognized for their financial strength and positioned to weather uncertain economic fluctuations or pursue opportunities that enhance resident quality of life. For over 50 years PRS has provided leadership consistent with our values. As a result, residents of 38 PRS communities have access to a retirement experience that provides an exciting lifestyle, opportunities for wellness and healthy aging, and a stable retirement experience into the future.

Appendix B

AgeTech west

Advancing a Technology-Enabled Standard of Care

AgeTech West is a collaborative founded by LeadingAge California, LeadingAge Oregon and LeadingAge Washington to advance the delivery of tech-enabled aging services toward a new standard of care. We believe that technology-enabled aging services can help older adults achieve greater "connected independence," safety and security, socialization and wellness, and management of personal health while improving care delivery, coordination and efficiencies. AgeTech acts as an educator, broker, enabler and advocate to support aging service providers as they leverage technology to better serve older adults and enhance their organizations' innovation, strategic growth and sustainability.

www.agetechwest.org