
LOUNGE
ENTRANCE HALL
FAMILY ROOM
STUB STACK
KITCHEN
BREAKFAST DINER
DINING ROOM
ELECTRIC
WATER
GARAGE
100mm UPSTAND TO DOOR FROM GARAGE SIDE
FD30/SC
SVP
16760
BOILER
STUB
5400
5,400
11,650
300

Millbrook Commons Community Technical Design

IST 220 – Section 1

Racked and Stacked

Chris Meyer
Angela Bruno
Larry Wilson
Breanna Hickok
Greg Guerrieri

Instructor: Nicklaus Giacobe

August 4th, 2013

Millbrook Commons Community

Table of Contents

III. Executive Summary

Millbrook Commons Community is being developed for singles and couples, who are aged 65 and older, most of which are self-sufficient and able to independently perform daily tasks on their own, and who are looking for a more care-free living environment. Some residents will also have impaired physical or mental capacities and need more specialized care from the staff at Millbrook Commons. This document will propose the housing plan and technical requirements needed to make Millbrook Commons a successful retirement community.

The Millbrook Commons Community is located in Centre Country, Pennsylvania and spans more than 2.5 acres. Millbrook Commons will be comprised of a mixture of apartments, condos, cottages, senior centers, and a small medical center which will support the lifestyle and medical needs of the fastest growing demographic in the United States, those over 65 years old. In this report we will show that the older generation wants to learn, and have more experience with, technology - "if only it were available" to them. Well, at Millbrook Commons, it is. Due to the complexity of the proposed Millbrook Commons Community Network, a certified staff is required to help maintain and troubleshoot any problems or errors and a network administrator, along with a small IT technician staff, will be crucial to the overall health maintenance of the network. This report will explain the proposed plan for the technology infrastructure for the entire community, as well as supporting diagrams for our proposal.

The plan we propose will explain in detail the network design for the individual residences, senior centers, and medical center. The proposal and designs will consist of considerations for the Personal Area Networks (PANs), Local Area Networks (LANs), and Metropolitan Area Networks (MANs) as well as Network Access and Security concerns for the community. Among the recommendations will be a LAN design, an initial MAN design that provides network coverage for the entire grid, media and data transport protocol, hardware needs for the network, and solutions to problems that could occur due to line-of-sight restrictions. The network access and security recommendations will cover the residents, staff, and visitors of the community. The Medical Clinic within Millbrook Commons Community will monitor all health related activities while still satisfying the privacy requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA).

Our proposal is designed to improve the quality of life for the residents of Millbrook Commons Community and we are confident that the aging demographic of Centre County, Pennsylvania will come to the conclusion that, with the living arrangements along and ease and convenience of the Medical Center, Millbrook Commons is the housing plan of choice.

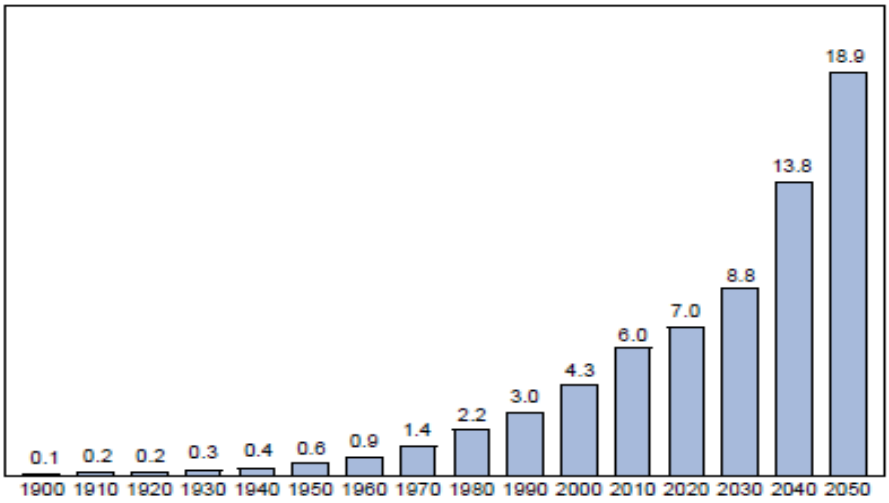
IV. Recent Trends in 65+ Age Demographic

In December 2012 the U.S. Census Bureau's Population Division released a report detailing the projections of the population by selected age groups for 2015 through 2060. Their Summary Report Table 2 indicated in the year 2015 the total population of the United States was expected to be 321,363,000, with 54,079,000 expected to be aged 65 and over. By 2060 the population is expected to grow by almost 25% to 420,268,000 of which, it is estimated, 110,910,000 will be over the age of 65. That is more than a 100% increase in the age group of 65+. It was projected by the year 2030 when the baby boomer generation will all have reached the age of 65, which is an approximate increase of 25% in the older generation. Centre County, PA's expected growth of this age group is no different. The U.S. Census reported in 2010 that Centre County, PA had a population of 153,990, of which 11.3% were over the age of 65, and by 2030 it is projected that 25% of Pennsylvania's rural population will be over the age of 65. With the expected growth of the older community the need for places like Millbrook Commons Community will increase as well.

Between the years 2010 and 2050 the growth of the 65+ generation is expected to more than double and by 2030 nearly one in five U.S. residents will be over 65. Current population reports, prepared with the combined effort of the U.S. Department of Commerce and the U.S. Department of Health and Human Services, reflect that "the age group of 85 and over is projected to be the fastest growing part of the elderly population throughout the rest of the century." (United States Census Bureau, 1996) as documented in figure 2-8 "Population 85 Years and Over: 1900-2050," below.

Figure 2-8.
Population 85 Years and Over: 1900 to 2050

(In millions)

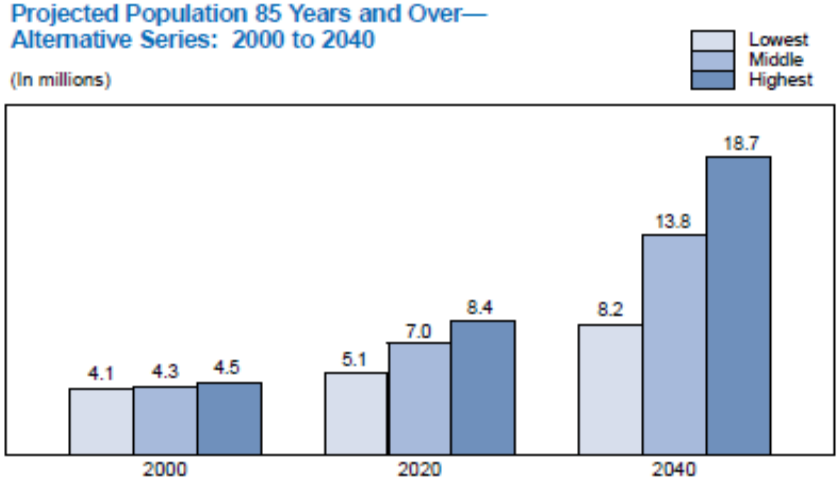


Source: U.S. Bureau of the Census, Decennial Censuses for specified years and *Population Projections of the United States by Age, Sex, Race, and Hispanic Origin: 1993 to 2050*, Current Population Reports, P25-1104, U. S. Government Printing Office, Washington, DC, 1993. Data for 1990 from *1990 Census of Population and Housing*, CPH-L-74, *Modified and Actual Age, Sex, Race, and Hispanic Origin Data*.

As the baby boomer generation continues to age, it is expected that the oldest senior citizen population will double from the projected 7 million in 2020 to almost 14 million in 2040, if using the Census Bureau's "middle series projections." By 2050 the oldest of the 65+ generation will comprise almost 5% of the total population. As illustrated in Figure 2-9 below, using the middle projections, in the year 2000 there were approximately 4.3 million Americans over the age of 85 compared to the 13.8 million projected in the year 2040; which is more than a 30% expected increase of this age group alone.

Figure 2-9.
Projected Population 85 Years and Over—Alternative Series: 2000 to 2040

(In millions)



Source: U.S. Bureau of the Census, *Population Projections of the United States, by Age, Sex, Race, and Hispanic Origin: 1993 to 2050*, Current Population Reports, P25-1104, U.S. Government Printing Office, Washington, DC, 1993.

As this generation ages, it is important to inspect the burden of their care on the working-age population and make sure there are sufficient resources to provide them with the care they need. The U.S. Census Bureau has indicated that by the year 2050 the dependency ratio between old-age dependency and youth dependency will have increased significantly since 2010, as documented in Figure 2 below. Every indicator leads to the need of more complete retirement facilities such as Millbrook Commons Community, to provide a safe place for the older generation to live with the dignity and pride they knew in their younger years.

AARP released *Connected Living for Social Aging: Designing Technology for All* in April 2011. A diagram pointed out that as older adults become more homebound due to a decline in mobility, they risk isolation from family, friends, and hobbies. At Millbrook Commons, we strive to keep the older generation engaged in society and technology in a hope to avoid the isolation that could come if the services at Millbrook Commons were not available. The connected living that is available at Millbrook Commons will allow seniors to maintain their interests and activities whether they are homebound or out and about.

A November 2011 survey by Linkage titled *Technology Survey – Age 65-100, Extending Technology Past the Boomers* revealed a lot of important information about seniors and their exposure, desire, and experience with technology. One participant from the survey said "I feel that some technology is needed for seniors. Computers help to keep their minds stimulated. A lot of technology should be available for seniors" (Linkage, 2011) while another had this to say "People are living to be older. I am 93 years old and able to do anything. They aren't thinking of real old people," (Linkage, 2011) and yet another said "I think computers are a great idea to find out and research information. You can keep in contact with your family and friends" (Linkage, 2011).

Another survey of more than 10,000 online U.S. seniors indicated, as reported by Forrester Research, more than 60% of persons 65 and older are online. Of those online:

- 91% have used e-mail
- 49% have used Facebook
- 59% have purchased products online
- 46% have shared photos with family and friends
- 44% have played online video games
- 24% have signed up for e-coupons/free products

These surveys provide a good look into what the older generation feels about expanding technology; not to mention solidifies the need for places like Millbrook Commons Community.

V. LAN/PAN/MAN Architecture Design Plan

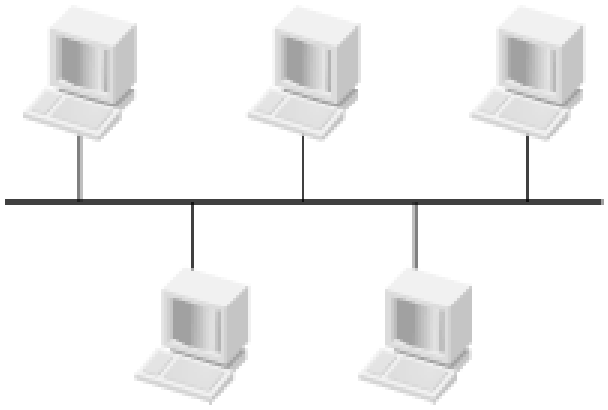
A. LAN Design Expected Recommendations

Background Material

A local-area network (LAN) is a system for linking devices and computers together in a building or a cluster of buildings. Every LAN, of whatever size, has to have an access system by which the end stations connect to the network. Two common options for LAN connections are Ethernet and Token Ring. A token ring is a sequence of bits that is passed to each node in turn in a LAN network.

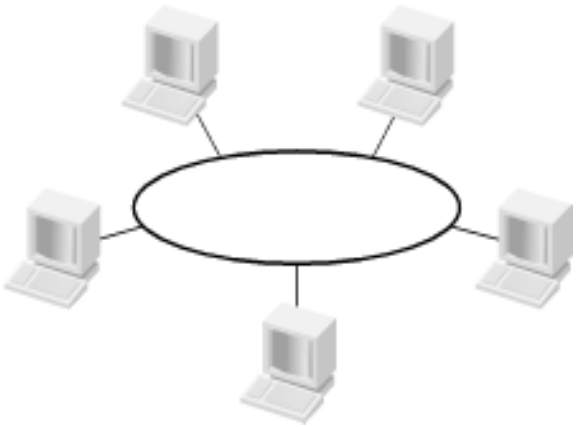
A LAN can be classified as a large building LAN, campus LAN, or small/remote LAN. Like the name describes, a large building LAN contains a major data center with high-speed access and floor communications. A campus LAN provides connectivity between buildings on a campus where redundancy is usually a requirement, and a small/remote LAN provides connectivity to remote offices with a small number of nodes. For a LAN design there are four basic topologies used to interconnect devices:

- Bus (diagram below): A single communication medium. On a bus any device can communicate with any other device and all devices can see the messages. Similarly any device can send a single signal intended for all other devices on the wire and this is called a broadcast.



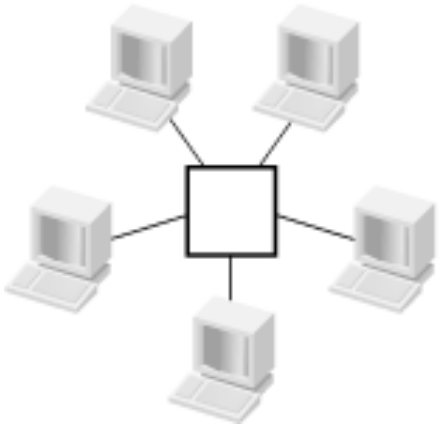
http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

- Ring (diagram below): Also known as a token ring. Each device has an upstream and a downstream neighbor. If once device wants to send a packet to another device on the same ring, it sends the packet to its downstream neighbor, which is then forwarded to its downstream neighbor and so on until it reaches its destination.



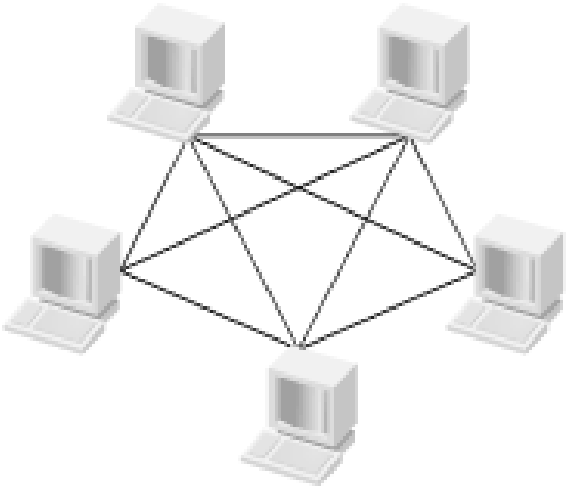
http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

- Star (diagram below): Most Ethernet and Token Ring LANs are implemented in a star topology. This implementation means that a central device connects to all of the devices with all of the devices communicating with one another by passing packets first to the central device.



http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

- Mesh (diagram below): In a mesh topology every device is connected directly to every other device with no intervening devices. Since every device is connected directly, the latency is low but inefficient because the amount of links needed is too high for the number of devices. This would only be useful for small LAN networks.



http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

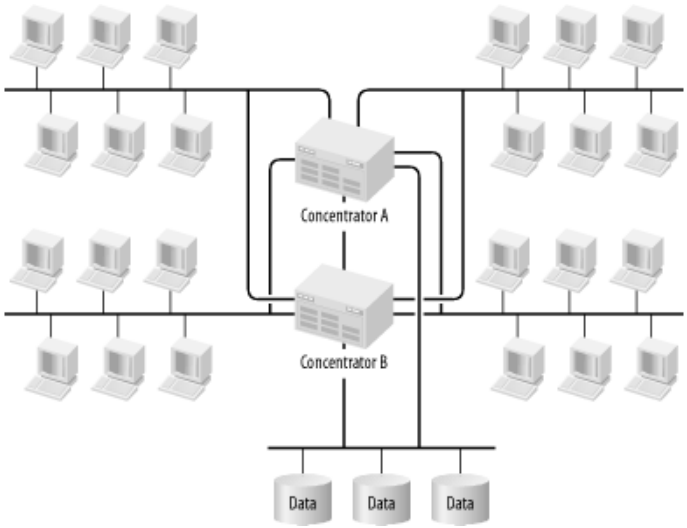
Most modern LANs are built using the star topology, regardless of their underlying technology. The reason for this is that it is easier to upgrade a network by upgrading only the device in the closet, without having to change the expensive cabling to every desk. It is also much easier to make fast switching equipment in a small self-contained box then it would be to distribute the networking technology throughout the work area. Since star topology is most common this will be used for the Millbrook Commons network.

Recommended LAN design

For the Millbrook Commons area the cottage areas will be connected using the campus LAN type to connect the different houses in the area. Whereas the condominiums, apartments, and managed care will use the large building LAN type. The living areas LAN will use the collapsed backbone design with the network backbone interconnecting various segments. The network backbone concept works well in more peer-to-peer networks where there is no central computer room, but there is communication among the various user LANs. This is good for the living areas in Millbrook Commons since the users will be in their homes and apartments.

In the collapsed backbone design a central router or switch has the long-haul connections to the various user areas. The central concentrator device is able to switch packets between its ports directly through its own high-speed backplane. One essential problem is that all network segments must share the bandwidth of the backbone for all the traffic is crossing it. The central collapse point is also the

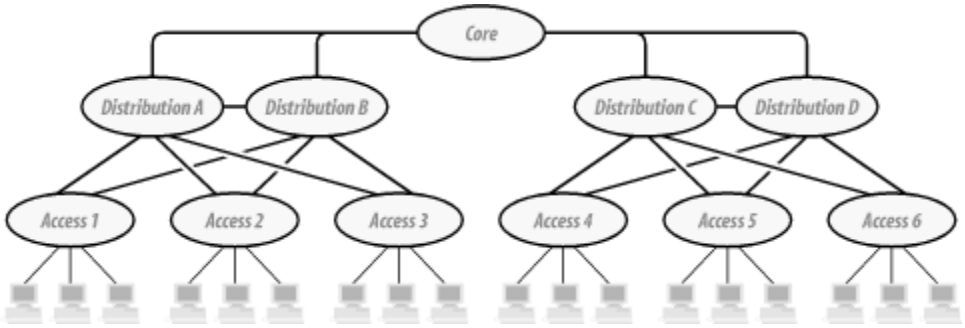
single point of failure for the entire network. A collapsed backbone with redundancy solves this problem, the diagram is shown below.



http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

One switch acts as the primary and the other ones acts as the backup. On a port-to-port basis, it is able to ensure that each user LAN segment is connected to only one of the two switched at a time. In the diagram a switch-to-switch connection is indicated in case LAN segment 1 is active on Switch A and segment 2 is active on Switch B. When this happens there needs to be a way to cross over from one switch to another.

For the computer labs, offices, and the medical clinic a hierarchical network-design model will be used.



http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

Each Access Level devices is connected to two devices at the Distribution Level. This connection immediately improves the network throughput and reliability. Doing this has effectively eliminated the Distribution Level devices as single points of failure. For example, if Distribution cloud A broke, then all three Access groups using it can switch over to Distribution cloud B transparently. This also helps with traffic patterns. Suppose an end device connected to Access cloud 1 wanted to talk to another end device in the same cloud. There is no need for the packets to even reach the Distribution Level. If that same device wants to talk to an end node connected to Access cloud 2, it does not need to use the Core. The packet can go through Distribution clouds A and B to get from Access cloud 1 to Access cloud 2. The only time packets need to cross the Core is when packets need to go further afield, to another Access cloud that is not connected to the same Distribution cloud.

Decentralized Network Management

For monitoring problems from one source there are two types of management schemes. Centralized, which means having one focus of control, and decentralized, which distributes control to many parts. A decentralized management structure is one in which decision-making authority is delegated to the lower level throughout the organization rather than limiting it to a few top people.

A probabilistic decentralized network management scheme shows how to cope with the overhead of redundant information gathering and processing, the decentralized management in dynamic and unpredictable environments, and the considerable effort required for decentralized coordination of management functions. This type of process is useful to a dynamic network because each node is not constantly processing management functions, which allows for a reduction in redundancy.

Network Management Software Protocol

A Simple Network Management Protocol (SNMP) is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP compliant devices contain a MIB which supplies the pertinent attributes of a device. A network that uses SNMP requires three key components; managed devices, agents, and network management software (NMS).

GFI max Remote Management offers 24/7 remote network monitoring and management. The Millbrook Commons Community could use this service to help deliver increased uptime to the members in the community. GFI MAX offers pre-defined and user defined checks for NAS, UPS, switches, etc. for SNMP.

Network Sensor Monitoring

Each location in the Millbrook Commons Community will be equipped with a network sensor monitor in the event that personnel or emergency services are required. For the residents that require more hands on care, their living spaces will be equipped with a hybrid wireless sensor network that will be used to monitor them. Each resident and his or her living space will be composed of a hybrid node pair, one for the member of the community (mobile) and one for his or her environment (mobile or fixed). Integrated into the network the hybrid node will be able to monitor and diagnose patients outside the medical center and will also control the home environment. This hybrid node will be connected to a wireless sensor network (WSN) and covers an administrative delimited area. This will be able to alert the Millbrook Commons medical clinic, police, and the fire department if anything goes wrong.

Wireless LAN

There are three types of Wireless LAN (WLAN); peer-to-peer, bridge, and wireless distribution system. A peer-to-peer (P2P) network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This WLAN design would be best for the implementation within the individual structures.

A WLAN bridge can be used to connect networks, typically different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN. A bridge would be best for the media centers or PCs for the residential users in Millbrook Commons. For business or other organizations environments a wireless distribution system (WDS) would be best. A WDS enables he wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them. A notable

advantage to WDS is that to preserves the MAC address of client packets across links between access points.

802.11 Equipment

802.11 is the generic name of a family of standards for wireless networking relates to Wi-Fi. The numbering system for 802.11 comes from the IEEE who uses 802 to designate many computer networking standards including Ethernet. 802.11 standards define rules for communicating on WLANs. A Network Interface Controller (NIC) is an adapter circuit board installed in a computer to provide a physical connection to a network. A repeater is used as an alternative way to extend the range of an existing WLAN instead of adding more access points. An access point is a transmitter and receiver that connect to a network through an interface such as a bus or a connector. Antennas give you more power and let you go a longer distance away from the WLAN source. Antennas also help with certain line of sight restrictions allowing you to go farther.

802.11 Protocols

There are three different types of 802.11 protocols; 802.11a, 802.11b, and 802.11g. 802.11a provides specifications for wireless ATM systems and is used in access hubs. Networks using 802.11a operate at radio frequencies between 5.72 GHz and 5.850 GHz. This specification uses a modulation scheme known as orthogonal frequency-division multiplexing that is especially well suited to use in office settings. In 802.11a data speeds as high as 54 Mbps are possible, there is less interference with 802.11a than with 802.11b because it provides more available channels and because the frequency spectrum employed by 802.11b is shared with carious household applications and medical devices.

802.11b uses the Ethernet protocol and carrier sense multiple access with collision avoidance for path sharing. The modulation used in 802.11 has historically been phase-shift keying. The modulation method selected for 802.11b s known as complementary code keying, which allows higher data speeds and is less susceptible to multipath-propagation interference.

802.11g offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps theoretical maximum with the earlier 802.11b standard. Networks employing 802.11g operate at radio frequencies between 2.400 GHz and 2.483 GHz, the same band as 802.11b. The 802.11g specification employs orthogonal frequency division multiplexing, the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps. This feature makes 802.11b and 802.11g devices compatible within a single network.

B. PAN Design Expected Recommendations

PAN Background

A Personal Area Network (PAN) is a computer network constructed to service a single user. Wired personal area networks use USB and FireWire technologies while wireless personal area networks typically use Bluetooth and ZigBee connections. These Bluetooth PANs are also referred to as piconets. PANs usually service a small area of about 30 feet and are considered to be a subset of the Local Area Network that supports one user instead of multiple users. The typical applications of these types of networks include home automation, security, and patient monitoring. PANs are designed to accommodate the low data transfer rates between remote sensor devices while operating at ultra-low energy levels and having easy and inexpensive installation. The Millbrook Commons Community Network will implement both ZigBee and Bluetooth technologies in the development of the necessary PANs throughout the facility in order to promote security, safety, and comfort for the residents.

PAN Network Topologies

There are three different types of topologies in which Personal Area Networks can be structured; star, tree, and mesh. In a star topology, there is a central node which is connected to all other devices in the network. In order for a message to be sent from device to device, it must be relayed through the central node. In a tree topology, this is a hierarchy of nodes in a tree formation with the top node and a branch/leaf structure under it. This means nodes can have a parent node above it and children nodes below it. When messages are sent they travel from the sending node up the tree until it is able to go back down the branches to the receiving node. Lastly the mesh topology uses the same structure as the tree topology except messages are able to be sent across the tree when there is a viable route to connect to.

PAN Network Components

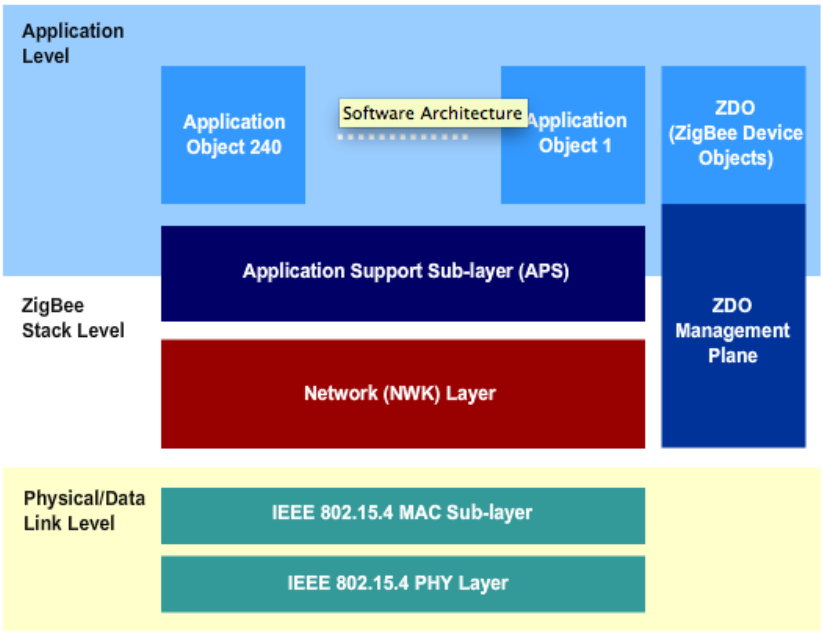
Each of these topologies consist of three different types of network components. These are the coordinator device, end device, and router. Each of these have unique roles in the network. In all ZigBee and Bluetooth networks there is only one coordinator device. It is used for system initialization in order to start the network, select the appropriate channel frequency, allow devices to connect to it, provide the routing of messages, and security management. In a star topology this is the central node and in both the tree and mesh topologies it is the top node. There are also end device components which are located at the edges of the network. These are the leaf nodes in the tree and mesh topologies and the points in the star topology. They are used to send and receive messages and are typically battery powered which go into a sleep mode, when not in use, to conserve power. Lastly there are routers which are used to relay information to end device as well as allow other nodes to connect to it. Also routers can sometimes be used as end devices if the function can be perform through their application layer. These are not needed in star topologies because the coordinator performs this function,

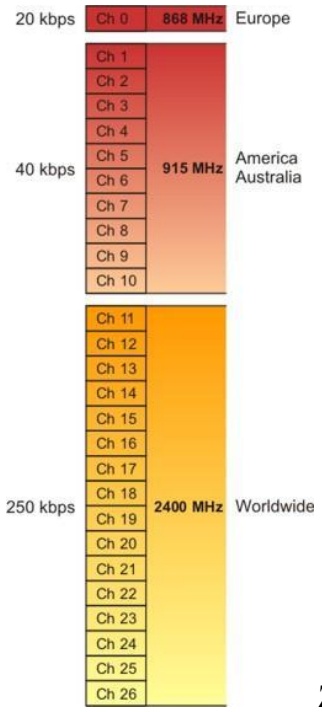
but can be used for their applications.

Legend: Dark Blue = Coordinator, Light Blue = End Device, Red = Router

ZigBee Protocol and Levels

The ZigBee protocol architecture consists of the Application level, ZigBee Stack level, and the Physical/Data Link level. The application layer contains the applications which run on and give functionality to the various connected network devices. It turns an input into digital data and takes digital data and converts it into an output. The ZigBee Stack level contains ZigBee software which provides functionality between the application level, network structure, and also routing/security including encryption, key management, and authentication. The Physical/Data Link level breaks down into the media access control (MAC) sub-layer, which handles addressing and assembly/disassembly of packets and the physical sub-layer, which uses the radio medium to transmit message and delivers data bits to the MAC sub-layer. This level is based on the wireless network standards of IEEE 802.15.4. IEEE 802.15.4 offers up to 250 kbps at the 2400 MHz universal frequency and has a total of 26 channels available to use and an additional channel 0 which contains device information. Every IEEE 802.15.4 node in the world has a unique 64 bit IEEE address which is used to identify the device. In addition, the nodes also have a 16 bit network address which is used to identify devices within a network. Any devices on the same network will need to have unique addresses.


Application Level
Application Object 240
Software Architecture
Application Object 1
ZDO (ZigBee Device Objects)
Application Support Sub-layer (APS)
ZigBee Stack Level
ZDO Management Plane
Network (NWK) Layer
Physical/Data Link Level
IEEE 802.15.4 MAC Sub-layer
IEEE 802.15.4 PHY Layer



ZigBee Pros & Cons

The advantages of using the ZigBee protocols include easy and cheap installation, ultra-low power consumption, various configuration options, and the ability to add or remove nodes from the network while it is still in service. Also ZigBee devices are able to go into an ideal state or sleep mode when not in use so they are able to save a lot of battery power. The disadvantages to ZigBee are the low data rates of only 250 kbps and the short broadcast range between devices.

Bluetooth Protocols

Bluetooth technology is made up of a wide number of protocols including telephony control protocols, cable replacement protocols, Bluetooth core protocols and some other adopted protocols. The Bluetooth core protocols include baseband, link manager protocol, logical link control and adaptation layer (L2CAP), and service discovery protocol (SDP). Baseband is what allows the radio frequency connection between devices to for a piconet. The link manager protocol deals with the specific connection of two Bluetooth devices. It is used for security purposes and provides encryption and authentication capabilities. The L2CAP layer is mostly used for multiplexing, segmentation and the reassembly of transferred packets. Finally the service discovery protocol allows devices to be discoverable between each other and must be done in order for the connection to be completed.

Bluetooth Pros & Cons

The advantages of using Bluetooth technology include low cost, license free, simple set up, anti-interference channel selection, data rates of up to 2.1 MBps and the ability to broadcast voice communications. Also Bluetooth is universally accepted with over 2,000 device manufacturers.

Implementation

The Millbrook Community Commons Network will have a few different kinds of personal area networks setup throughout the grounds. These include residential in-home PANs which will connect the device sensors for fire alarms, carbon monoxide, heat, windows, doors, motion sensors, and healthcare equipment. These will most likely use ZigBee protocols unless the data transfer rate is not sufficient, in which a Bluetooth piconet structure must be put into place. Also there will be a mesh network of ZigBee transceivers mounted outdoors throughout the community to connect all of the alarm sensors in the homes to the remote monitoring facility.

Local Network Data Collection

With some of the resident in the Millbrook Commons having to be monitored for various healthcare issues, it is very important the information being gathered from the sensors is reaching a database where it can be analyzed and stored. For example, some residents will be hooked up to ZigBee compliant healthcare monitoring systems which will measure the resident's vital signs. When the data is collected from the medical sensors it is time-stamped and sent to a gateway which will be the acting monitoring system. The device will be configured to trigger an alarm when certain parameters are met and will also send the information to an external database for future use.

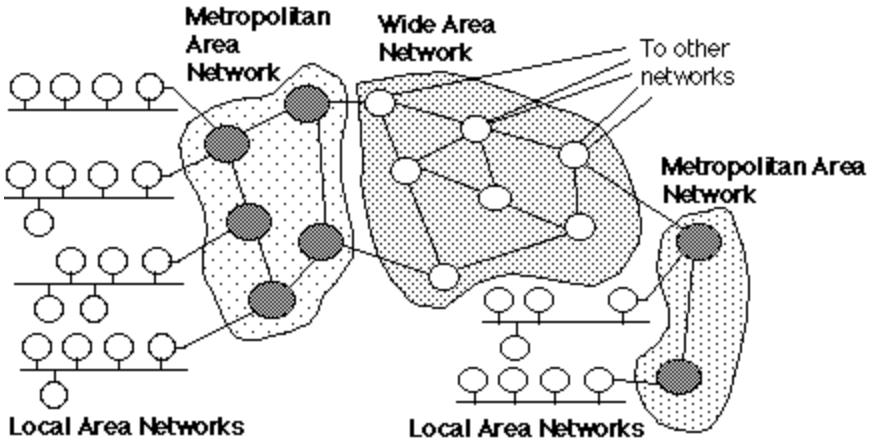
c. MAN Design Expected Recommendations

Terminology and Network Interconnections

A metropolitan area network (MAN) is another type of network like the large area network (LAN) or the wide area network (WAN), but there are noticeable differences between these networks, which distinguish one from the other. Sze (1985) lists three notable features that differentiate MANs from LANs or WANs.

1. The network size of a metropolitan area network falls between the network sizes of LANs and WANs. A MAN typically encompasses an area with a diameter between 5 and 50 km. Many MANs cover an entire city, but in some cases, MANs may be as limited in scope as a small group of buildings.
2. A MAN is usually owned by a single organization. The network resources generally are owned by a single service provider who sells their service to users. Qualities of service and performance level guarantees are negotiated with the MAN operator. WANs may share this attribute with MANs as well.
3. A MAN often performs as a high-speed network to permit sharing of regional resources. Additionally, the MAN frequently provides a shared connection to other networks via a link to a WAN.

The potential qualitative advantages of a MAN are significant and include high bandwidth, low delay, and high transmission quality. These attributes are taken advantage of in the MAN at Millbrook Commons.



Note. From "*Metropolitan Area Networks*" by Gorry Fairhurst

Requirements

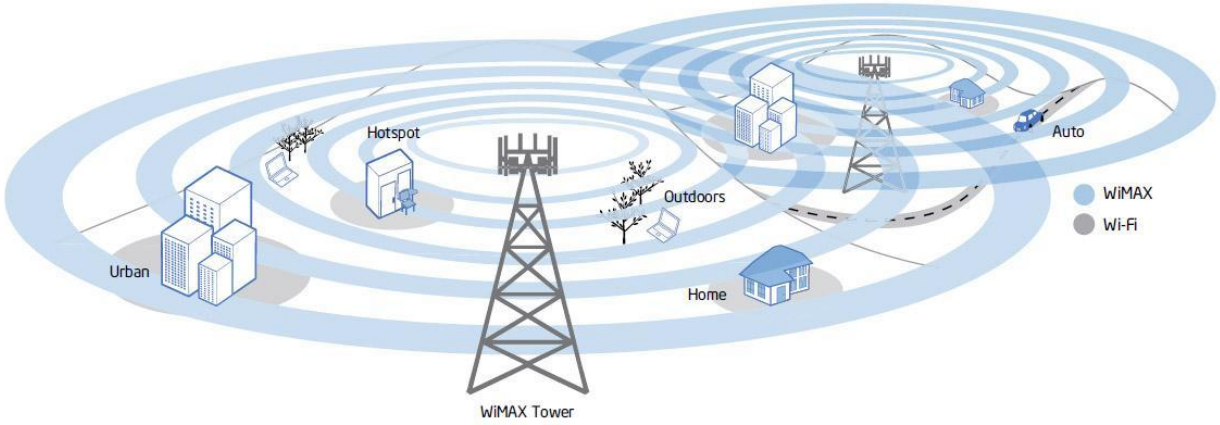
The Millbrook Commons Community consists of seniors age sixty-five or older with and without physical handicaps, and those receiving full-managed care. This demographic information dictates that this retirement community's network infrastructure provides reliable wireless services that will accommodate the way the residents will communicate with one another within Millbrook Commons, with others outside of the community, and with the Millbrook Commons staff. The proposed MAN for Millbrook commons faces multiple challenges of data usage and management from the processing requirements of voice, data, and video in a real-time environment. Users of the network will expect freedom of movement throughout Millbrook while maintaining connectivity, but not necessarily expect the same outside of the community campus. These parameters and considerations dictate that a fixed wireless solution with mesh topology is recommended as the best option.

This section proposes a metropolitan area network in a campus-like setting whose infrastructure has the capability to provide a high quality of service to meet the needs of this diverse community. As technology evolves, there will be ever-increasing stressors placed upon networks because of requirements for more storage and processing power across the network. These requirements will necessitate high-speed transfers over long distances. Goals associated with this network include equipping all buildings with a shared, secure communications infrastructure with standardized services that reduce costs as much as possible through consolidation. The MAN will do this and still deliver reliable interconnections while maintaining high-level network security.

802.16 MAN Design with Hardware/Software Recommendations

Millbrook Commons will utilize the IEEE 802.16e 2005 standards and access will be arranged similar to current cellular systems in the form of a wireless metropolitan area network. The network will use the Worldwide Interoperability for Microwave Access (WiMAX) protocol. WiMAX offers broadband-like access speed and long distance coverage comparable to a cellular network as opposed to the limited range and sparse coverage of WiFi alone.

This standard uses base stations that service users in a radius of several miles. Additional towers can be interconnected for increased throughput via a microwave link. The base station must be located in an elevated location and ideally as centralized as possible to the MAN coverage area. Potential base antenna locations include towers, tall building rooftops or other elevated structures such as a water tower. To interconnect the user to the base station, a customer premise unit, which is comparable to a satellite TV setup, is all that is necessary. Upon arrival at the customer premise unit, the signal is then routed via standard Ethernet cable directly to a single device or to multiple devices through an 802.11 hot spot or a wired Ethernet LAN. This is where the MAN and LAN networks interface occurs and will offer high-speed connections using fiber optic cable or other digital media. This single network will connect all of the access networks and provide everything from real-time services to traditional data-transfer services. The network according to (Omerovic, 2012), will also provide quality of service (QoS) and handle any kind of traffic, from constant bit-rate traffic to packet- or cell-based traffic.



Note. From "*The Future of WiMAX*" by Gaddi Blumrosen, 2009, The Future of Things.

Millbrook Commons will use the Airspan HiperMax-micro system, which is the all outdoor version of the HiperMax system and is ideal where climate controlled rooms are either not available or not preferred. MCCN will have an Airspan HiperMax antenna tower located outdoors and placed on the rooftop of the highest nearby structure just south of the Science Street and East Marilyn Avenue intersection. This positioning will ensure more than adequate coverage to the HiperMax base station unit located inside the main administration building of the community complex. Airpsan (2013) specifies that the antenna will flow data at a rate of 3.1 GB per second via fiber optic connection, but has the capability to transmit 10 GB of data per second. This excess capability will allow for future expansion of network throughput. A fiber optic cable will connect to a HiperMax base station from the tower. The HiperMax base station will connect through a fiber optic cable to its external RF unit deployed on the rooftop of the administration building ensuring maximum connectivity with

Each office building or living space on campus will have an Airspan ProST-WiFi customer premises equipment installed upon their respective rooftops for access to the 802.16 network and create mesh topology for coverage and redundancy. Additionally throughout the Millbrook Commons complex there will be ProST modules mounted atop light poles which will ensure maximum coverage and redundancy for the network. The ProST is indicated for use when a specific service level is required and MCCN requires a high level of service. A key attribute of the ProST is that it offers both line of sight (LOS) and non line of sight (NLOS) propagation capabilities. The ProST-WiFi on each building will be combined with indoor adapters called EasyWiFi designed to provide backhaul services for WiFi users. This adapter can also be upgraded to support the use as VoIP. This indoor adapter is chosen because of its versatility and because it is a simple, fast, self-install product. Residents and guests may also utilize Airspan's MiMax USB, which is compatible for use on any USB 2.0 capable device, to get WiMAX access outside or on the go around Millbrook Commons. Finally, the Airspan system will be managed by Airspan's SNMP-based network management system Netspan. The

Netspan platform operates through standard and proprietary Management Information Bases (AirSpan, 2013).

802.16 Advantages/Disadvantages

The IEEE created 802.16 standards for broadband wireless access in order to offer a protocol that delivers high-speed, high-capacity, low-cost solutions to expand fiber-optic backbone ranges. This backbone extension will provide alternative network access to homes, small businesses, and commercial buildings from conventional wired connections. This standard, as all standards do, has distinct advantages and disadvantages. According to techCYN (2010), those include:

Advantages:

1) One base station can serve hundreds of users with each user having a dedicated non-competing access point slot.

2) Faster deployment of new users compared to the slow and laborious task of installing cabling for new wired networks.

3) Speed beyond the scope of WiFi (up to 100 Mbps at 10 kilometers even in severe weather conditions).

4) Standardization (equipment of the same frequency works together).

5) WiMAX is NLOS based. (LOS not required)

Disadvantages:

1) Line of sight is needed for very distant connections.

2) Bad weather conditions may reduce network performance or interrupt the signal, especially over very long distances.

3) Other wireless equipment could cause interference.

4) WiMAX is a high energy consumption technology and requires significant electrical provisions and infrastructure.

5) High equipment and operational costs associated with a new and still emerging technology.

WiMAX will enable a large number of applications and services for the Millbrook Commons Community because of its Quality of Service, range of service, and output capabilities. WiMAX's advantages and its ability to interconnect access networks will improve facility services to residents at Millbrook. The staff will be able to provide enhanced health care, health care monitoring, and quality of life benefits. In short, WiMAX as a MAN solution is an innovative technology that allows rapid deployment with reduced costs to a retirement community located in rural Pennsylvania.

802.16 and 802.11 Interaction

Airspan's ProST-WiFi CPE provides WiMAX access along with integrated Wi-Fi capability therefore virtually anywhere on campus residents, staff, and visitors will have access and data capabilities via WiMAX or IEEE 802.11b/g WiFi.

Capacity and Overlap Requirements

The MCCN campus will largely be supported by its robust LAN infrastructure which services the administration buildings and medical buildings. The single-family apartments and condominiums are geographically separated significant distances from the LAN at Millbrook Commons which makes WiMAX a cost effective solution to provide network connectivity to residential and outlying areas of the campus. All of these locations and people associated with those locations will potentially need access to wireless services. These facilities users and human users will be utilizing bandwidth intensive applications such as streaming video for security cameras or telemedicine video conferencing. The WiMAX 802.16e standard will provide Millbrook Commons up to 75 Mb of data transfer speed which should sufficiently service Millbrook Commons' aggregate data rate for the MAN during peak hours of usage.

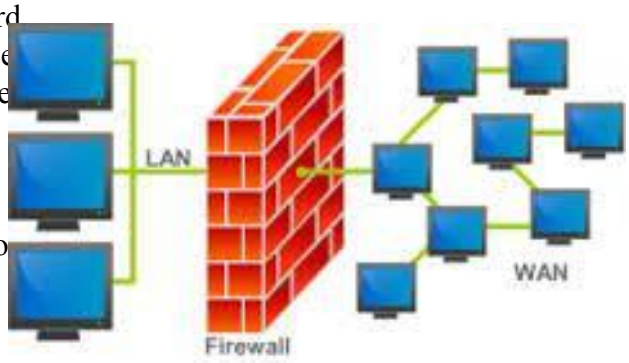
VI. Network Access and Security

Network access and security must be a top priority in order for the Millbrook Commons Community Network (MCCN) to pride itself on providing comprehensive and reliable technology services for its community. Without the development of proper security policies and procedures, MCCN is exposing all of its employees, community members, affiliates and resources to countless technology threats. With so many people relying on the network infrastructure for daily operations, it is vital to implement appropriate security measures to ensure confidentiality and network integrity. The process for accomplishing this colossal task begins with detailed planning.

As a whole, the community of MCCN will be comprised of individuals with varying degrees of IT experience. Keeping in mind that not everyone is aware of network security threats, it's important to

design a thorough security plan that encompasses the entire MCCN community, regardless of IT knowledge and proficiency.

The first step in establishing a secure network for the MCC, is to designate a strong firewall between the LAN and WAN. Ideally, the firewall should be a combination of hardware (router) and software. Network access will be restricted and only authorized traffic will be allowed to pass through the firewall. Authentication of a username and password will be required for network access. Verification will be enforced using intricate password policies and multilevel access permission. WPA2 will be required for wireless network devices. Disabling and/or filtering all unnecessary and common vulnerable ports should also minimize and discourage unauthorized access to and from the LAN.

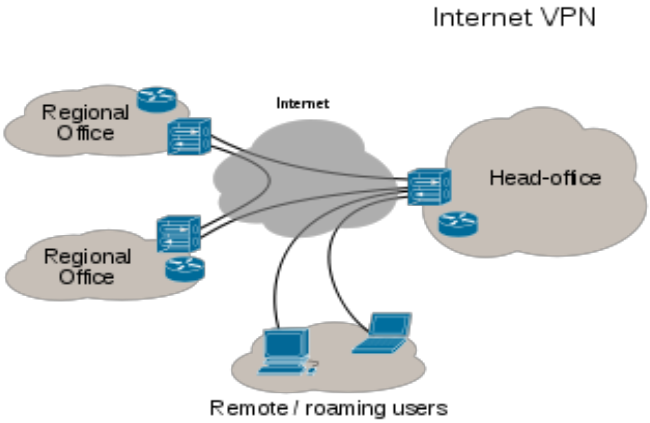


In order for the firewall to continually provide a high level of security, the number of applications that run on the firewall should be limited. Also, regular software updates are essential to ensure that the firewall is maintained for optimal protection. Although installation of the firewall will provide significant network security for the MCCN, it is not immune to information security risks. Having a properly configured and efficient firewall is merely the first layer of protection in a multilayered approach.

Installing Internet security software (antivirus software) provides the second layer of protection for the MCCN. Internet security software needs to be installed on all network computers to prevent, detect, and remove any malware that may have slipped past the firewall. While many firewalls include antivirus software, it would be best not to bog down the firewall by installing the antivirus software on a dedicated system behind the firewall. Once the antivirus server is employed, all of the network hosts should be updated with the corresponding antivirus client. The clients can then be configured from the antivirus server to establish and schedule routine tasks such as software updates and periodic scanning of all end user systems. This process simplifies the management of all MCCN devices by monitoring activities from a dedicated, central location. The combination of the firewall and Internet security software create a dedicated security perimeter around the MCCN. However, enhanced security measures need to be taken to ensure that the network cannot be breached.

Implementing an intrusion detection and prevention system (IDPS) adds another layer of security to the MCCN that constantly monitors and scans the network for malicious behavior. A distinct advantage of using an IDPS system is that it can be configured to the needs of the MCCN. The system can be set up to be passive and alert the network administrator to system or network weaknesses. Or it can be set up to be reactive and immediately respond to breaches in the system. Regardless of how it is configured, an IDPS system would further secure the MCCN by working in conjunction with the firewall and Internet security software.

Although the majority of network communication will take place primarily on-site at the Millbrook Commons Community (MCC), there may be times when authorized management and staff need secure access to the MCCN from a remote location. To securely accommodate these occasions, a virtual private network (VPN) must be established.



The benefit of creating a VPN is that it is completely scalable to efficiently accommodate the current and future needs of the MCCN. The VPN is a cost effective solution that will grant employee's access to the MCCN when necessary. It provides employees with a great deal of flexibility while still maintaining confidentiality standards through the use of encryption.

Exploring data confidentiality in greater detail, encryption is another layer of security that will be vital for protecting transmitted data across the MCCN. The MCCN will have patient medical records and private data transmitted throughout the entire network; therefore encryption is required by federal law to protect this data to a specific standard as outlined in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA clearly states that information systems housing personal health information (PHI) must be protected from intrusion. Also, when PHI is transmitted over open networks, encryption must be utilized. While HIPAA states that encryption must be employed to secure PHI data, no strict parameters are specified for what type of encryption technology must be used. A best practice approach would be to include the following principles into the MCCN to ensure that it exceeds the basic standards set forth by HIPAA. First, the MCCN needs to apply encryption to both network files and network connections. Second, the MCCN needs to always use Secure Sockets Layer (SSL) protection for web-based access to sensitive data. Third, MCCN mobile devices and media such as CD's, DVD's, USB drives, smartphones, and tablets, must also maintain HIPAA compliance standards by encrypting personal data. Finally, all MCCN inactive data needs to be encrypted as well. This includes all data stored on hard drives, servers and backup drives. Implementing and maintaining these encryption practices will provide the MCCN with a consistent, HIPAA compliant network for housing and transmitting all sensitive PHI data.

Aside from developing a standard policy for PHI data encryption, HIPAA also includes additional data security requirements that will impact the MCCN. HIPAA covers an expansive amount of security standards and technical safeguards for the protection of electronic health information. Although HIPAA is comprehensive, it is more of an outline of standard policies and procedures rather

than a specific set of technical requirements. With the MCCN storing and transferring PHI, as well as providing telemedicine for its community, it is important that these HIPAA standards are followed so that the MCCN is in compliance with federal law.

Beginning with access control standards, HIPAA states that rights or privileges to PHI should only be granted to authorized users based on a set of consistent access rules. It is also noted that authorized users should only have access to the pertinent information needed to perform their job. As previously mentioned, the MCCN needs to address this by implementing a unique user identification and password authentication process. Access should be multilevel and specifically based upon job responsibilities. Delegating character length and variety requirements will help enforce strict password criteria. It would also be beneficial to impose regular mandatory password updates.

Another area of significant focus of HIPAA is establishing and maintaining data integrity. According to HIPAA guidelines, information integrity exists when data has not been altered or destroyed in an unauthorized manner. Besides adhering to strict access control and encryption standards, the MCCN can further address this by incorporating a few additional technical safeguards. For instance, the inclusion of a process that automatically corroborates data such as a check sum or digital signature would significantly protect MCCN personal data. Another method for the MCCN to enhance integrity control for electronic communication would be to utilize a data or message authentication code (MAC). All of these electronic measures are valuable and can help fortify the MCCN with added assurance that all PHI is accurate.

While all of the aforementioned policies and procedures go a long way to ensuring network security, they cannot guarantee that the MCCN will not be compromised. Network security is a constant process that demands persistent effort. Having regular audits of all security operations including mandatory employee training and hardware/software evaluations is paramount in minimizing security threats. However, regardless of how much security threats are minimized, a worst-case scenario plan needs to be in place. It is vital that the MCCN have a thorough backup solution if the network were to be breached. Multiple backups need to be available both on and off site. They need to be stored in secure, disaster proof locations with limited access to only authorized individuals. Once in place, the backup procedures must be tested regularly to confirm they are properly working. Also, these methods must be revisited consistently to ensure that they are fulfilling the MCCN's backup needs.

VII. Network Diagrams

802.16 MAN Coverage Areas

ProST Interface
(Credit: Airspan)

This 802.16 AirSpan WiMAX network is designed to deliver high-speed broadband Internet access to Millbrook Commons by covering all the residential and outlying areas in a mesh topology. The MAN tower is connected to the HiperMax base station with fiber optic cable. The base station communicates with a ProST WiFi CPE installed in discreet and elevated locations whenever possible for maximum signal propagation. The CPEs will provide WiFi coverage inside and around these buildings by providing a wireless connection between IP-enabled devices. Devices not 802.16 compatible are recommended to use a MiMax USB device for connectivity. This system will be managed by Netspan, Airspan's SNMP-based network management system.

802.11 LAN Coverage Areas (STILL NEED)

Camera Placement Recommendations

Still need:

general PAN sensor placement recommendations, and identify all necessary hardware and proposed interconnections

VIII. References

AirSpan. (2013, July 17). *ProST and ProST WiFi*. Retrieved from Airspan Corporation Web Site: http://www.airspan.com/products/bwa/wimax-user-devices/prost-and-prost-wifi/

American Medical Association. (2010). *HIPAA Security Rule: FAQ Regarding Encryption of Personal Health Information*. Retrieved from http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf

Bluetooth Protocol (Part 2): Types, Data Exchange, Security. (). Retrieved from http://www.engineersgarage.com/articles/bluetooth-protocol-types-security

Bowers, B. (2012). *ZigBee Wireless Security: A New Age Penetration Tester's Toolkit*. Cisco. Retrieved from http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=3

Brunner, M., Dudkowski, D., & Mingardi, C. (2009). Probabilistic Decentralized Network Management. *International Symposium on Integrated Network Management,* (), . Retrieved from http://www.inf.ufpr.br/aldri/disc/artigos/2011/Apre_Trabpraticos/RO_01.pdf

Connected Living for Social Aging: Designing Technology for All. (2011, April). *AARP,* (), . Retrieved from http://www.aarp.org/content/dam/aarp/technology/innovations/2011_04/Connected-Living-for-Social-Change.pdf

Department of Health and Human Services. (2007). *HIPAA Security Series*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Dooley, K. (2002, January). Designing Large-Scale LANs. *O'Reilly Online Catalog,* (), . Retrieved from http://oreilly.com/catalog/lgscalelans/chapter/ch03.html

Fairhurst, G. *Use of MANs to provide regional networks.* University of Aberdeen, UK, Aberdeen.

Greier, J. (2004). *Extending WLAN Range with Repeaters*. Retrieved from http://www.wi-fiplanet.com/tutorials/article.php/1571601/Extending-WLAN-Range-with-Repeaters.htm

Health Insurance Portability and Accountability Act. (). Retrieved from http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

Introduction to network centralization and decentralization. (2007). Retrieved from http://searchitchannel.techtarget.com/feature/Introduction-to-network-centralization-and-decentralization

Learning Guide 802.11 protocols. (n.d.). Retrieved from http://searchnetworking.techtarget.com/tutorial/80211-protocols

Linkage. (2011). *Technology Survey Age 65 to 100*. Retrieved from http://www.ageinplacetech.com/files/aip/Linkage%20Technology%20Survey%20Final_2.pdf

Mitchell, B. (n.d.). *802.11*. Retrieved from http://compnetworking.about.com/od/wireless80211/g/bldef_80211x.htm

Network Topologies and LAN Design. (2000). Retrieved from http://networkworld.com/ns/books/ciscopress/samples/0735700745.pdf

Omerovic, S. (2012). *WiMax Overview.* Slovenia: Faculty of Electrical Engineering, University of Ljubljana, Slovenia.

Phan, T. (2011). *Encrypting Data to Meet HIPAA Compliance*. Retrieved from http://resource.onlinetech.com/encrypting-data-to-meet-hipaa-compliance/

RadioLabs Long Range WiFi Antenna. (n.d.). Retrieved from http://www.radiolabs.com/products/antennas/long-range-wifi-antenna.html

Sze, D. T. (1985). A Metropolitan Area Network. *IEEE Journal on Selected Areas in Communications*, 815-824.

techCYN. (2013, July 17). *WiMax Technology - Internet on the Go!* Retrieved from techCYN.com: http://www.techcyn.com/feature.php?id=f4

The Digital Behaviors of Older Americans. (2012). Retrieved from http://www.forrester.com/The+Digital+Behaviors+Of+Older+Americans/-/E-PRE3624

The Next Four Decades: The Older Population in the United States: 2010 to 2050. (2010). Retrieved from http://www.census.gov/prod/2010pubs/p25-1138.pdf

The Pros and Cons of Bluetooth Technology. (). Retrieved from http://www.interbluetooth.co.uk/bluetooth-pros-cons.html

U.S. Bureau of the Census. Current Population Reports, *Special Studies, P23-190, 65+ in the United States.* U.S. Government Printing Office, Washington, DC, 1996

United States Census Bureau 2012 National Population Projections: Summary Tables (Table2). (2012). Retrieved from http://www.census.gov/population/projections/data/national/2012/summarytables.html

Wireless LAN. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Wireless_LAN#Types_of_wireless_LANs

ZigBee. (2012). *ZigBee Health Care*. Retrieved from
http://www.zigbee.org/portals/0/documents/events/2012_03_26_ismict.pdf