Millbrook Community Commons Network

Part 2. Technical Design

Instructor: Elizabeth Thiry

Team 01:
Alessandra Mauser
Gary Burch
Hardik Sorayan
Leon Valery
Michael Gnankou
Nathan Zavacky
Randall Miller

December 12, 2014

TABLE OF CONTENTS

Executive Summary 1

Brief Demographic Summary 2

End-User Client Hardware Specifications 3

Definitions and Acronyms 3

Abandoned Proposals for a WiMAX Installation 5

Ethernet Backhaul Link to the Public Internet 5

Wired Ethernet IT Resources in the Community Center:

- **The Gateway Router** 6
- **Server Resources** 7
- **Other IT Resources— MCC Staff** 9
- **Other IT Resources— MCC Residents** 10

MCC Wireless LAN Network Access:

- **Residential Campus 802.11 Wireless Network Access** 10
- **Wireless 802.11 Network Access in the Main MCC Buildings** 12

Other Wired Ethernet LAN Designs:

- **Residential Independent-Living Wired Ethernet LAN (and WLAN control)** 13
- **Wired Ethernet LAN (and WLAN control) in the Medical Complex Buildings** 16
- **Campus Security LAN (and WLAN devices)** 18

Networked Audio and Video Applications at the MCC 20

Wireless Personal Area Networks:

- **The ZigBee Gateway Device** 22
- **Networkable Health Care Devices** 23
- **Smart-Home Energy Conservation, Security and Personal Convenience Devices** 24

Security Revisited 25

References 29

Executive Summary

This technical design document comprises the specification and description, at an intermediate level of detail, of a complete design of a wired and wireless IT communications network for the Millbrook Community Commons. In completing this design the team was guided by its initial understanding of the scope and goals and goals of its engagement, one that it summarized on an earlier occasion as follows:

> The team is to design a state-of-the art networking infrastructure for a retirement community just outside State College in Centre County that will: (1) provide ubiquitous mobile computing upon the campus; (2) by facilitating deployment of the latest technologies in telemedicine, smart-home design, and remote data acquisition/telemetry, improve the delivery of watchful healthcare to residents while also enhancing their security, safety, comfort and convenience; (3) accommodate the creation of more traditional wired subnets in community structures where staff and residents are concentrated, or where the need for them otherwise appears; and (4) allow for reasonably anticipated future technical innovation and population growth.
>
> To foster creation of an infrastructure that will be well adapted to the needs of its ultimate users, network design is to be preceded by study of user requirements that incorporates available demographic data, user profiles of residents/staff, and other research.
>
> Care will also be taken to ensure that the network can supply where needed the minimum QoS required to support the audio/video transmission demands of telemedicine/telenursing, as well as the residents' expected primary use of the system for live communication with family members and other residents. To offset the expected high total cost of the overall network design, economic savings from smart-home energy efficiencies and higher care-staff productivity will be encouraged to the greatest extent possible.

The results of the preliminary study that is mentioned in the second paragraph of this study were summarized in a "User Requirements" document that the team earlier submitted as the Part 1 deliverable of its engagement.

In completing the technical network design that is described within this second deliverable the team strove to be mindful of the characteristics and needs of the network's eventual endpoint users wherever they might appear to be relevant to any design choice among alternatives with which the team was immediately presented. But as the starting premises for its design of what after all is a communications infrastructure the team was unavoidably compelled to accept the physical dimensions, topography and other characteristics of the geographic area to be served— Ethernet links span a limited distance, and radio broadcast signals have usable ranges— no less than the bare numerical census of the targeted user population. For in provisioning bandwidth the adequacy of a proposed data link must initially be assessed by dividing the maximum throughput that the link can supply by the aggregate number of its anticipated downstream users.

Beyond this it is of course necessary to take heed of the kind of end-user applications that the infrastructure must support; indeed the team was to a limited extent tasked with the selection or recommendation of some few of these applications. It is in the process of imaginatively foreseeing or creating such eventual application demands that a sound appreciation of the characteristics of the network's end users can be an invaluable guide to one's otherwise unaided intuition.

In crafting its solution to the design problem that was presented by premises like these the team also strove to remain unconstrained by preconceptions about the form that the outcome of its process would take: that is, when presented with any design choice for the network the team tried to marshal and appraise, without any presuppositions, the alternatives that it found to be available, and only then to make an informed selection of the one that it judged to be "best." The end outcome of submitting to this discipline is a design that is not especially exotic or innovative, but more

resembles another instance of the familiar: peripheral Ethernet and Wi-Fi star networks connected by high-bandwidth trunks to a routing network center. But often there are just good reasons why the tried-and-true has again been adopted.

Brief Demographic Summary

Increased social wealth, improved standards of living and advances in health practices and medical care have caused average life expectancies in the industrialized world to steadily increase, as a result of which the proportion of the members of society who are elderly has likewise been steadily increasing. In some countries the disproportionate growth of the elderly segment of the population has also been exacerbated by birth-rate fluctuations like the post-WWII "baby boom" and later fertility declines experienced in the United States.

As society's elderly population grows so also do the demands that caring for their needs places upon society's limited resources, a phenomenon that has several related aspects. Because individuals are living longer, in the first place, the period of time over which care must be provided or other resources expended has simply lengthened. When individuals live longer, moreover, they also survive to an age when their physical and mental capacities are significantly lower, their health significantly poorer, and their dependency much greater. This circumstance is closely related to a second aspect of the increasing cost of caring the elderly: adequate care of the aged primarily means tending to their medical needs, and for decades the cost of providing healthcare in the United States has been increasing at a rate that far exceeds the rate of overall inflation.

Finally, the disproportionate growth of the elderly segment of the population in advanced industrialized countries means there are proportionately fewer younger members of society available to shoulder the burden of care. If this burden is not to become unsupportable innovative solutions to the many-faceted problem of providing of providing decent care to the elderly population need to be searched for and created. Today it is much hoped that creative applications of modern information technology will provide many of these solutions.

If this is to be so the elderly must be prepared to accept information technology as a major part of their lives, and to learn how to make good use of it. Research indicates that although the elderly have lagged behind the rest of the general population in their acceptance and adoption of information technology and use of the internet, there is also a pronounced trend of increasing IT use among the elderly, especially among the younger, better-educated and wealthier segment of this cohort. While Centre County for the most part exemplifies national demographic trends, the better educated and financially secure are especially well represented among its elderly.

Ways in which networking technologies have already been used as a means to create a more satisfying community life include: (1) the creation of community websites, (2) the use of networking and computing resources as instructional aids or virtual classrooms, (3) the deployment of communications applications, smart-home technologies and systems of remote data acquisition and telemetry in senior citizen centers, residences and communities, (4) the streamlining of business transactions to provide for more efficient and personalized service to customers, and (5) the increasingly widespread provision of free wireless internet access, enabling a member of the general public to connect anywhere and at any time to a website or another person. Management at the Millbrook Community Commons intends to secure its competitive position by deploying state-of-the-art information technologies wherever possible to enhance living standards, while achieving the highest standards of care.

The residents of the Millbrook Community Commons will include retirees in all three of the categories of need typically encountered in retirement communities: significantly disabled or

impaired individuals who require daily around-the-clock attention of a skilled nursing staff (45 residential units); less severely disabled individuals who require no intensive ongoing medical attention, but are still likely to need daily assistance in such personal activities as dressing themselves or bathing, and walking any farther than a short distance (55 residential units); and those residents who are fortunate enough to remain substantially capable of independent living (150 1-bedroom or 2-bedroom cottages, plus 60 apartment units). Besides its administrative, medical-nursing and caregiver staffs, MCC personnel will include an IT manager/network administrator, a security and emergency response officer, a chaplain, social worker and community activities manager, transportation manager, and maintenance and housekeeping staff.

End-User Client Hardware Specifications

Among the indicated contents of a document summarizing the team's technical design of the network was suggested a specification of end-user hardware that the team either required or recommended. In its configuration of MCC staff IT resources the team has specified generic dual-core x86 end-user hardware running 64-bit Windows 7 or later, because the near-monopoly that the Windows environment still enjoys in business desktop systems renders the assumption that staff will be familiar with the operating features of this environment a reasonable assumption to make.

Nevertheless the team opines that as a general proposition a good network design should be transparently adaptable for use by any one of the hardware or software platforms that are now commercially available and in widespread use. Its design does not pretend to adjudicate the dispute between Macintosh and Windows partisans, and can also accommodate the outlier with his Linux gaming box. A resident can and should choose to use the platform with whose use he has come to feel personally most comfortable.

The MCCN will, however, deploy a Wi-Fi technology that can deliver the latest 802.11ac Wave-1 streams from three-stream 4 x 4 MIMO antennae. To a resident who is considering the purchase of a new device the team recommends that he choose one that can take full advantage of the higher throughput and better signal quality of this new technology: in notebooks any Apple MacBook Pro or MacBook Air introduced after May 2013, or Hewlett-Packard notebook introduced after November of the same year; in tablets, a new Microsoft Surface or iPad Air 2; and in mobile phones an iPhone 6, or a new Samsung Galaxy Note 3, S4 or S5.

Definitions and Acronyms

The use that will be made in this document of a few common acronyms and their associated translations might benefit from some preliminary clarification:

WAN. Wide Area Network. When use is made of this term in this document the intended reference will ordinarily be one to the public internet. If the term is used with a qualifier, as in "enterprise WAN" or "MCC WAN," the term refers to endpoint hosts external to the MCC that are connected to internal hosts through its VPN (see below), and to the networking infrastructure that supports these connections.

MAN. Metropolitan Area Network. This is a term typically used to refer to networks that span an area as large as a larger municipality or university campus. Comprising as it does an area of only about ten square city blocks, the MCC is at the very low end of this range of reference, and the term "MAN" will not generally be used in this document; see the section on WiMAX, *infra*.

LAN. Local Area Network. When this term is used without qualification or is prefaced with a global qualifier like "MCC" it is meant to comprehend all endpoint hosts and supporting

infrastructure on the interior side of the gateway router connecting the MCC to the public internet, with the exception of those hosts like the MCC's public web, email and DNS servers that are exposed to connections with untrusted hosts though one or another of the MCC's public IPv4 addresses, and so lie within its "DMZ" or demilitarized zone.

When the term "LAN" is prefaced with some qualifier that connotes some limited geographic region or user group the term is being used loosely to refer to some subset of hosts and supporting infrastructure that is physically installed within that limited area, or may be used anywhere but just by that group. Some degree of isolation and definition is usually meant to be implied by the qualifier, but no commitment is necessarily being made about exactly how this has been accomplished in a particular case: there may or may not have created a distinct IP subnet or VLAN, access control lists may or may not have been configured, and actual lack of physical connectivity with other regions of the network may or may not exist.

The term is ordinarily meant to comprehend wireless as well as wired connectivity. When limitation is intended it is usually expressed by use of the qualified phrase "wired LAN" or "WLAN" (for wireless; see below).

WLAN. Wireless Local Area Network. This term is generally used in this document in a way that parallels the just-explained use of the term "LAN," except that its scope is limited to wireless clients, access points and controllers, and/or their logical configurations.

A more technical sense of the term "WLAN" refers to a logical entity that exists in a (nearly) one-to-one correspondence with one or more of the SSIDs (service set identifiers; up to sixteen per access point) that are reachable through a single access point or group of such access points, together with a set of associated parameters like the security policy designated for use on the WLAN. A WLAN in this limited sense is defined and associated with one or more dynamic interfaces upon a wireless controller.

It will be clear from the context which use of "WLAN" is being made.

VLAN. Virtual Local Area Network. By the use of the 802.1Q protocol a single layer-2 connected network may be partitioned into separate broadcast domains between which packet traffic can pass only through the mediation of router functionality. Cisco Catalyst switches— selected for use in the MCCN— implement a proprietary VLAN Trunking Protocol that automatically propagates the definitions of VLANs over the entire LAN, and some can be adapted to route traffic between those to which they are connected.

PAN. Personal Area Network. In contemporary use this term embraces short-range connections between endpoint user devices. So defined, the term's denotation extends to input/output devices like printers, monitors and cameras connected to desktop computers by USB, IEEE 1394 (Firewire), VGA or DVI cables and interfaces, but more commonly its use is reserved for ad-hoc wireless (WPAN) connections via protocols like 802.15.1 (Bluetooth), 802.15.4 (ZigBee) or the IrDA (infrared) group.

For security reasons the MCC may find it advisable to disable peer-to-peer wireless connections between uncertificated endpoint devices through its residential WLAN, and for that reason residents may find it more convenient to make use of Bluetooth not only for connecting devices like wireless computer keyboards and mice, but also for the impromptu connections between mobile devices like iPads and iPhones that vendors are increasingly making possible. In any case plans for MCCN need to make no special provisions to accommodate Bluetooth connections between end-user hardware devices, or between MCC-owned computers and peripheral hardware like special access devices for the vision-impaired, hearing-impaired, or otherwise disabled.

When used in this document "PAN" will refer to one of the short-range low-power ZigBee networks used to implement smart-home and similar technologies within MCC residents' homes. The range of one of these networks is often greater than the "personal" distance that typically separates master-slave infrared or Bluetooth devices, and so the term "HAN" (for "Home Area Network") is sometimes used to characterize such a network. But that latter term will not be used in this document.

Abandoned Proposals for a WiMAX Installation

Preliminary plans for the Millbrook Community Commons Network included a proposal to erect an 802.16 WiMAX base station and tower upon its site to supply metropolitan area network (MAN) wireless coverage to its campus. This proposal seems to be related to descriptions of the MCC in the project specifications that imply a site area of some seven and one-half square kilometers, or five-eighths of the total area of the Borough of State College itself.

A MAN installation might well be appropriate to a community of this geographical extent, whose resident population could be expected to exceed 5,000 seniors. Even the smaller-range 802.16e-2005 Mobile WiMAX tower base stations have cells with broadcast radii of three miles in length or greater.

But there is a marked discrepancy between the above-mentioned descriptions of the MCC in the project specifications, and their included maps that demonstrate it to be an entire order of magnitude smaller. This discrepancy has been resolved in favor of a community with the dimensions shown in the included maps (see Appendix 1), together with the information that the MCC is to be modeled upon the Quaker-run Foxdale Village retirement community on the outskirts of the Borough of State College.

Purchase of licensed broadcast frequency bands for use in a WiMAX deployment would no doubt exceed even the considerable financial means of the MCC, so it must be assumed that any base station that it erected would have to operate in the unlicensed ISM (industrial/scientific/ medical) radio frequencies. Even if the operation of a WiMAX transmitter scaled for the service of a MAN were not so inappropriate to the actual dimensions of the MCC, its operation on the outskirts of a developed university community like State College could well be expected to provoke complaints about the interference that it would certainly generate.

The team nevertheless considered designs in which the 802.11 wireless service contemplated for the MCC would be augmented by the deployment of a low-power WiMAX micro-cell station like Airspan's MicroMax model, or even pico-cell station like its Air4Gp. But the team concluded that there are simply much better ways to accomplish the purposes for which WiMAX was a suggested solution.

Ethernet Backhaul Link to the Public Internet

The internet service provider Windstream advertises 1 Gbps Ethernet internet service to local businesses.[1] At 2 Mbps per user for 500 simultaneous users— there will be approximately this number of residents (including nursing-home and assisted-living residents) in the Millbrook Community Commons— this service might be adequate, but just barely. The team recommends to its management that it negotiate with Windstream or another local ISP for a 10 Gbps Ethernet backhaul link to the public internet.

---

[1] http://www.windstreambusiness.com/products/enterprise-network-services/dedicated-internet-services/ethernet-internet

Wired Ethernet IT Resources in the Community Center

The Gateway Router

The gateway router that will be deployed in the Community Center and to which the MCC's WAN backhaul link will be connected is a Cisco Model ASR 9006 aggregation router. The aggregate processing and switching capacity of Cisco's smaller-profile ASR 9001-S are in themselves serviceable to the MCC's overall requirements, but this model lacks the slots into which can be installed the Cisco ASR 9000 Virtualized Services Module (VSM) and the Cisco ASR 9000 Integrated Services Module (ISM).

In conjunction with Cisco IOS version 5.2, the VSM will allow the Cisco 9006 to serve as one endpoint of site-to-site IPsec-secured connections over the public WAN between hosts within and outside of the MCCN. Secured sessions like this are contemplated as a means of conducting telemedical consultations between a nurse practitioner in the MCC's medical clinic and a physician on call at the offices of its chief physician's private practice, or between Dr. Lewis himself and colleagues at the local hospital of whose staff he is a long-time member; a VPN will also permit members of the MCC's administrative staff to securely access IT resources when working at home or on the road. And the Cisco 9006 with IOS v.5.2 can act as a home agent to forward (unencrypted) IP traffic to any authenticated mobile laptop from within the MCC LAN, or from the internet at large if the host bears a fixed, globally routable home IP address.

A mobile host with a public address like this will, however, be an exception to the rule, because the chief function of the Integrated Services Module that is to be installed in the Cisco 9006 router is to provide the MCCN with carrier-grade Network Address Translation (NAT). The NAT facility of the gateway router— as a result of whose deployment the private-range IP addresses of MCC hosts not within its demilitarized zone are simply unreachable by unsolicited incoming packet traffic— is the chief element of the firewall protecting the internal IT resources of Millbrook Community from malicious hosts on the untrusted public internet.

The MCCN subnets corresponding to interfaces on its gateway router will be these:

CIDR Address Range:	**Subnet Description:**	**Number of Hosts:**	
		Potential	Actual
ISP-assigned	Router interface with access line		1
172.16.0.0/16	DMZ: public WAN servers, firewall and intrusion-detection systems	65,536	<10
172.17.0.0/16	LAN server farm	65,536	<25
172.18.0.0/16	Administrative Offices subnet	65,536	<100
172.19.0.0/16	Security/Emergency Response subnet	65,536	<100
172.20.0.0/16	Community Center lifestyle services	65,536	<100
172.21.0.0/16	Medical Center complex subnet	65,536	<1,000
172.22.0.0/16	Independent-living residential subnet	65,536	<2,500

With this definition of logical address structure it should be possible in many cases to configure access control lists (ACLs) on the Cisco ASR 9006 to entirely prevent or substantially limit inappropriate access to information resources at the layer-3 network level. There should rarely if ever be ample justification, for example, for packet traffic to be permitted to travel in either direction between the Administrative Offices and independent-living residential subnets.

Server Resources

Most of the major hardware components of the Millbrook Community Commons network infrastructure will be sited within its central Community Center. A diagram schematically depicting these components and their interrelationships is included in this technical design document as its Appendix 2. In interpreting this diagram it is important to appreciate that the individuation of elements and their relative positions within the whole is logical— that is, functional— and not necessarily physical in nature. Several servers might be virtual, or running as separate instance-objects of an application class, on a single machine; by the same token a computationally intensive server process might be run as a distributed application on several server machines at once.

As was already adumbrated above, the hallmark of servers running within the MCCN's demilitarized zone is that they will maintain open transport-level sockets reachable by unsolicited incoming packet traffic from the untrusted public internet. The DMZ servers like this that the MCC will certainly deploy include an authorized DNS server as well as public web and mail servers, running open-source software like Apache on a Red Hat Enterprise Linux OS.[2] That these servers will accept incoming connections in the manner just described is the entire gravamen of their pictorial representation as being entirely unconnected to the enterprise firewall: a more likely scenario, and one actually recommended by the team, is that all incoming packet traffic be initially diverted to a server performing deep packet inspection with software like Snort within the DMZ itself. This server will log suspicious traffic matching any one of its rules to an internal network management database, even if the packets are not dropped but simply redelivered to the router.

The MCC servers that are "located in the DMZ" will actually be mounted in racks just above, below or immediately adjacent to the MCC's LAN servers in a physically-secured and closely temperature-controlled room, with a dependable backup power supply, on the lowest floor of the Community Center. The team recommends, for most enterprise applications, the high-performance Cisco UCS C220 M4 single rack-unit server, or the UCS C240 M4 double rack-unit model for storage- or I/O- intensive applications; in either case the servers will be equipped with dual Intel Xeon E5-2680 Series (version 3) 8-core 2.70-GHz processors. To assist in meeting the potentially high data-storage demands of the MCC's medical analytics, medical-records, video-surveillance and network management applications there will be connected to the database-server and file-server boxes RAID-6 arrays of Seagate 6-terabyte 3.5" 12-Gbps SAS enterprise hard drives, equipped with FIPS-level encryption and secure-erase capabilities.

Most of the MCC's LAN servers will run Red Hat Enterprise Linux (version 7 or later). This platform is required by the Cisco HealthPresence server software that is specified elsewhere in this design document for the MCC's telemedicine applications, and also supports the Oracle software that the team anticipates the MCC will want to acquire to satisfy its relational database management

[2] A secure shell (SSH) application gateway server operating in the DMZ could also allow SSH clients on opposite sides of the MCCN's enterprise NAT router to exchange encrypted telnet-style remote commands with one another. By taking advantage of SSH's "port forwarding" options VNC screen-sharing, file-transfer, X11 and other port-based application message traffic could be safely "tunneled" through the encrypted SSH connection, in an ad-hoc staff VPN.

and enterprise resource planning needs; equally important is the circumstance that the JBoss application development and server program, a leading platform for the support of the Java Enterprise Edition frameworks, is an integral component of the operating system. The team expects that programmers will use these Java EE frameworks to create the web services-based applications that ultimately will make more useful the data gathered by its residentially-based PAN sensor deployments. If programmers also want to use the AXIS Embedded SDK to develop, with AXIS' VAPIX APIs in C or C++, intelligent-surveillance applications that will realize the full potential of the MCC's planned video camera deployment (see below), an underlying GNU Linux OS is necessary too.

On the other hand the team's plan anticipates that MCC employees will for the most part operate computers running the Windows desktop operating systems with which they can be assumed to be most familiar, and to interact easily with these endpoints the MCC will want to install Microsoft server software. In the course of discussing HIPAA security requirements in its Part 1 submission, the team remarked that:

> ...MCC management must also be primarily responsible for creating, at the level of the domain server and client/server application, a thoroughgoing system of user authentication, access and accounting that grants pre-determined rights to access clearly defined data resources, upon the principle of least privilege, to authenticated users only, and logs the parameters of every resource access that is made or attempted...

For creating and enforcing a system of this kind the MCC will rely upon the services of a machine running Windows Server 2012,[3] which should also supply the network with services including internal DNS, secure X.509 certificate storage and management, ActiveDirectory and LDAP services, and RADIUS capabilities integrated with EAP methods to regulate user network access. A Microsoft Exchange server will also be running to provide complete email and related similar communications services to residents and staff.

Apart from their interactions with the Microsoft servers described in the foregoing paragraph, residents' interactions with the MCCN's LAN servers should additionally expose them only to its internal web server and proxy. As the team already described in Part 1, the Millbrook Community Commons plans to provide an accessible online community website— kept current by efforts supervised by its community activities director— that will employ techniques of interactive social media and networking to make it as easy as possible for a resident (even for a resident whose mobility is severely restricted) to establish and maintain connections with other residents in the community, while keeping abreast of community news and the scheduled events and activities on the MCC's calendar. The team envisions that the community social networking facilities that the MCC will offer to its residents will include web-hosting services sited here for those who want to create their own personal websites; it also envisions that the community website itself as well as any of these personal websites that may be created will be accessible from outside the LAN by password-protected account access to http links on the MCC's public web pages.

It was remarked by the team, elsewhere in its Part 1 document, that:

> …the elderly have long notoriously been the favored targets of door-to-door swindlers, and consequently of the special solicitude of state consumer-protection agencies; given that many of them will also be relatively unsophisticated internet patrons, their exposure to imposition will only be magnified in the digital age...

By configuring its web proxy with publicly available blacklists to filter content distributed by

[3] Since in this role Windows Server makes use of Kerberos version 5 (RFC 4120) by default, it can seamlessly regulate access to Red Hat Enterprise Linux servers.

websites known to be malicious, the MCC can mitigate the danger described in this passage. A web proxy can also somewhat alleviate the feared congestion on the MCCN's backhaul link to the internet.

On the subject of congestion a feature of the Catalyst 3650 and 6500 Series switches depicted on the diagram of the Community Center infrastructure ought also to be mentioned here in passing. The switches selected for deployment in some cases might seem to host several more ports than are necessary to support the interconnections that they are designed to service, but an otherwise unused port on a Catalyst switch can be configured by the network manager as a backup port, to supply quick recovery from a port failure on an active link. And if the device at the other end of a link that is regularly congested also supports the expedient known as link aggregation, links between that device and the switch can be multiplied with additional cables, which are then configured to act as a single higher-bandwidth connection.

Other IT Resources— MCC Staff

The administrative subnet 172.18.0.0/16 depicted on the diagram of the Community Center will service the offices of its executive officers and finance staff, its activities director, resident social worker and chaplain, the MCC's manager of resident transportation, and its housekeeping and maintenance staffs. Apart from properly configured access to central server resources, no special IT demands must be satisfied to meet the needs of users in these offices: standard-issue desktops equipped with dual-core Intel x86 CPUs and a minimum 4 GB of RAM, running a 64-bit version of Windows 7 or later, should be adequate to the needs of the users in these offices.

On the other hand the responsibilities of the MCC's Security and Emergency Response team do impose some special IT demands for which the creation of a separate subnet was thought by the team to be the first prerequisite. Depicted near the top of the diagram is a switch to which incoming connections will made by seven separate AXIS high-definition pan-tilt-zoom surveillance cameras that are described later in this technical design document. Software freely downloadable from AXIS' open application facility undoubtedly already includes applications incorporating the AXIS' Media Control ActiveX component, which enables easy viewing of Motion JPEG, MPEG-4 and H.264 streams directly in Microsoft Internet Explorer; similarly, Metis' Command Center 2.3 software provides an integrated dashboard through web-based user interfaces that will communicate with the emergency-alert devices to be located throughout the MCC campus. But a high-bandwidth link between this subnet and the MCC's central farm is needed to facilitate transmission of the video data for storage and intelligent analysis. And at least seven high-definition video monitors will need to be connected to a workstation in the department's own office to permit simultaneous panoramic viewing of the content delivered by the cameras.

The special needs entailed by the responsibilities of the MCC's IT manager and network administrator will be similar. Initial project specifications spoke at one point of designing a system that provides for decentralized system management, but as the team already noted in the summary of its Part 1 preliminary design document, the size of the MCC is sufficiently small that its entire IT department is likely to comprise this manager and a single staff assistant. What these two are most likely to require is a system that provides for highly centralized management, but with geographically distributed data acquisition and reporting and remote device control.

The Cisco servers and network switches incorporated in this design all include SNMP agents allowing for such distributed reporting and remote control, as do the AXIS cameras and most of the other endpoint hardware recommended for deployment on the network. Firewalls, intrusion detection applications and server processes also log exceptions, error conditions, accesses and other relevant data as a matter of routine. To analyze and make sense of the large volumes of data with

which these capabilities can inundate an IT administrator, good open-source applications like Zabbix and OpenNMS are freely available for installation upon the MCCN's management server, and integration with a central Oracle or Postgre database. One running instance of OpenNMS, a Java application, can collect 1.2 million data points via SNMP every five minutes, can process 125,000 syslog messages per minute, continuously, and has been shown to be capable of provisioning networks of more than 50,000 discrete devices, or networks of single devices with over 200,000 discrete interfaces, at once.

Other IT Resources— MCC Residents

In its Part 1 the team's design document acknowledged that:

> ...The MCC hopes to encourage its retirees to experience the free time suddenly on their hands as a blessing and not a curse. To this end the facility's plan not only includes sites for community gardening plots and a fully equipped gymnasium, but also a well-endowed library, woodworking shop, arts and crafts studios, and computer learning center. Staff members will be employed to guide residents in making good use of these amenities, of course, but residents will also be encouraged to pursue self-directed personal enrichment through online study, at computers available upon the premises of each...

The facilities described in this paragraph— as well as a small auditorium room equipped with a network-connected interactive theater/audio system, with full streaming capabilities— are all of them located within the confines of the MCC's Community Center, and are schematically depicted on its diagram as those collectively constituting the separate subnet 172.20.0.0/16.

The standard-issue desktops that were prescribed for general use by the MCC staff should be adequate to the needs of the residents making use of these facilities as well, although facilities should also be equipped with Apple iMacs running OS 10.9 or later for those residents who are more comfortable with this platform. In situating the desktop computers particular attention should be paid to ergonomics, setting some of them on bar-high tables for kiosk-like quick task assistance; in no case will computer monitors be firmly attached to table counters in fixed stationary positions (as is the custom in the computer laboratories deployed throughout the Penn State university system), but will instead be placed upon fully tiltable stands that can be freely moved across the surface of the supporting table top. Bluetooth assistive devices for those with impaired vision or hearing or limited manual dexterity should be readily available at every computer laboratory site, where a staffer should be trained to be able to explain the mode of their proper use.

MCC Wireless LAN Network Access

In the lower left and right-hand corners of the diagram depicting the IT infrastructure located within the MCC's Community Center are identified two Cisco Model 5508 wireless controller devices. The 802.11 access points that will be controlled by these two devices are the subject of the sections that immediately follow. Their deployment is diagrammed in Appendices 3 and 4.

Residential Campus 802.11 Wireless Network Access

At the heart of the team's plans for supplying the Millbrook Community Commons with ubiquitous outdoor 802.11 Wi-Fi connectivity in the residential campus area to the southwest of its larger main buildings is the Cisco Aironet 1570 Series outdoor access point. Cisco's latest models, the 1570 Series APs can deliver data rates of up to 1.3 Gbps under the new 801.11ac- Wave 1 standard, and up to 450 Mbps under 802.11n. They also support legacy a/b/g link protocols.

The particular model selected for the MCC network is the 1572E-AC, which requires 100-277 volts AC power at 60 Hz and must be fitted with external antennae. These latter are 4 x 4 MIMO

antennae with three spatial streams (the fourth RX and TX antennae being required for client beamforming), and can be configured as either directional or omnidirectional. The antennae can also be configured either as two 2.4 GHz and two 5 GHz ports, or as a single 2.4/5 GHz dual-band port.

Aironet 1570 Series APs have the discovery and routing capabilities associated with a wireless backhaul channel that make them capable of operating as nodes in an extended outdoor wireless mesh network. In its outdoor wireless mesh deployment guides, however, Cisco (2013a) recommends a mesh AP cell radius (for 2.4 GHz backhaul) of up to 600 feet, which equates to just 25 mesh APs per square mile. Because the site of the MCC has an area of less than 1/25 of a square mile and measures a maximum total width just over 1,200 feet, only a single "mesh" access node is required for complete outdoor coverage of its entire campus. And in fact the team has recommended the placement of a single Aironet 1572 mesh access point, equipped with omnidirectional antennae, atop a lamppost to be erected by a gazebo near the center of the campus.

Mounting of a Cisco Aironet MAP:

source: (Cisco) *Enterprise Mobility 4.1 Design Guide*, Ch. 8, "Cisco Wireless Mesh Networking", p. 8-4.

While the access points that comprise an outdoor wireless mesh network are commonly mounted in the manner depicted to the left, groups of such mesh access points (MAPs), the MAPs numbering twenty or fewer per group, are paradigmatically associated with a rooftop-mounted access point (RAP) that is connected to a controller at the edge of the wired infrastructure, and that maintains a wireless backhaul link to a node at the center of the group. The team has recommended that a second Aironet 1572E-AC be installed as a RAP like this on the roof of the MCC Community Center building, and that it be connected via fiber to a Cisco Model 6503-E Catalyst switch (and through this to a Model 5508 wireless controller) operating inside.

The primary purpose of this second outdoor access point could also be served by running a 1 Gbps link directly to the central MAP from the controller in the Community Center; if Cat-7 UTP copper is used for this purpose it could at the same time satisfy the power requirement of the central MAP via 801.3at power over Ethernet. While doing so remains an option, the team has considered that the Community Center RAP might also serve the secondary purpose of supplying outdoor wireless service to the parking-lot area in front of the main buildings (a RAP can also serve clients just like a MAP). The RAP could probably provide service to this limited region even when equipped with high-gain directional antennae aimed straight at the MAP at the center of the campus.

In its original conception the residential wireless 802.11 mesh network was intended not only to provide outdoor connectivity, but also to serve as the primary home network access for those independent-living residents who are not living on one of the three floors of the apartment building. While it appears that the Aironet 1572-based system might be capable of delivering bandwidth adequate to such a mission (3 Mbps per cottage minimum if all units are simultaneously operating with 802.11n), indoor reception would unavoidably be impaired by significant signal attenuation: although the full extent of such impairment cannot be reliably determined in the absence of an empirical site survey, factors commonly reported (3Com 2005) are 6 db or a fourfold reduction in signal strength for a 1.75" solid wooden door or 3.5" brick wall, and 7 db or a fivefold reduction for a 0.5" single-pane glass window.

Cisco outdoor wireless mesh deployments are interoperable with indoor mesh-capable access points (Cisco 2013a), and the team considered attempting to overcome the problem of signal attenuation by extending the outdoor network with Aironet 3600 Series indoor mesh-capable access

points, equipped with optional add-on radio modules to ensure that client devices would be able to make use of the 1.3 Gbps 802.11ac- Wave 1 bandwidth deliverable by the Aironet 1572. But since the team has already elsewhere found compelling reasons to incorporate the extension of wired Ethernet service to the cottages into its final recommended design— the available IP-network gateway devices for its in-home wireless ZigBee networks, for example, all seem to require such an Ethernet connection—there appeared to be no good reason to forego the considerable wireless bandwidth that can be gained by directly connecting indoor wireless access points to the MCCN's wired infrastructure with the available fiber links.

For this purpose the team has selected the Cisco Aironet 3700 Series AP, which delivers 1.3 Gbps 802.11ac- Wave 1 bandwidth out of the box, and like the 1572E can also be equipped with external 4 x 4 MIMO three-spatial-stream antennae. The hardier of the two models in this series was chosen for deployment in the cottage neighborhoods because the team proposes to suspend each installed unit above the ceiling of the cottage in which it is installed. On the wireless coverage map that is provided as an appendix, there has been depicted an AP cell size with a radius of 30 feet; this is approximately equivalent to Cisco's (2014b) rule-of-thumb guideline of 3,000 square feet per cell for deployments that aspire to a low-jitter quality of service adequate to VoIP.

Not depicted on the just-mentioned coverage map are the network links that connect the residential access points to the infrastructure. These links are identical to those schematically depicted on the diagram of residential wired Ethernet coverage that is also included as an appendix; it is expected that the underground fiber links will for the most part physically follow the pre-established paths shown by dark lines upon the MCC's map of its proposed development. Discussion of the logical addressing, security, mobility-management and other aspects of access-point configuration and control is deferred until the discussion of the wired infrastructure components that will carry these functions out.

Wireless 802.11 Network Access in the Main MCC Buildings

In the summary included in its Part 1 submission the team supplied a few of the reasons why it believes that the wired Ethernet LAN proposed to supply the connectivity needs in the apartment building, community center and medical complex (including the assisted-living and nursing-home residential units) needs to be augmented with 802.11 wireless service:

> The team also urges MCC management to reconsider its plan to provide only wired connectivity to end-system hosts within the apartment building, community center, and nursing-home/assisted-living/medical-center complex. Staff paging applications can make good use of wireless-everywhere network coverage, and in hospitals the sight of medical residents carrying laptops from room to room on their morning rounds has become a commonplace. Many nursing-home residents are effectively bedridden, too, and can make little use of a fixed-location desktop computer, while the proliferation of cables that typically encumber rooms in a nursing home is already an established nuisance...

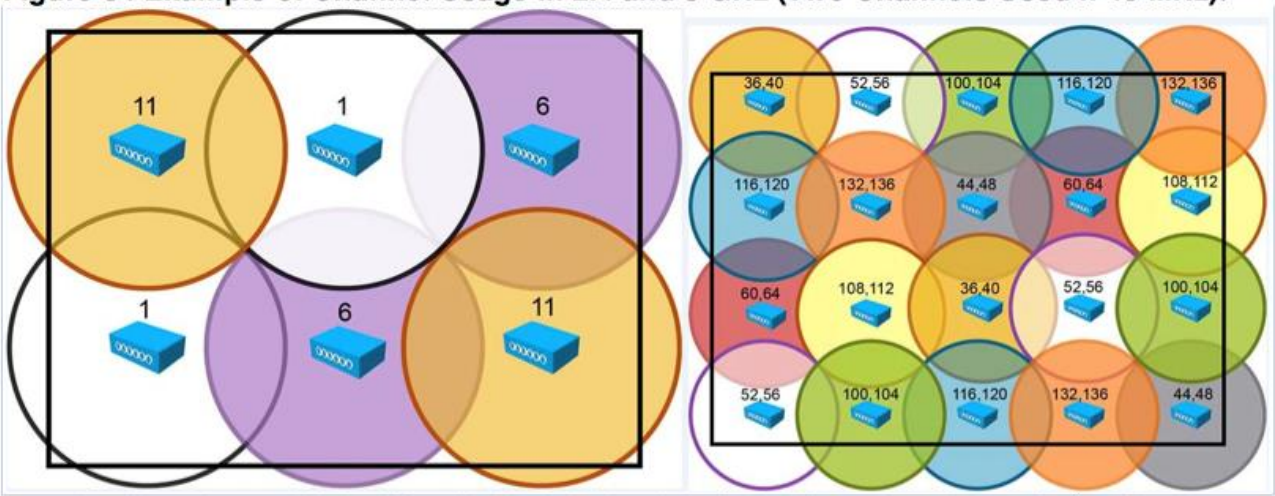
If reasons like these are not found to be sufficiently compelling, the team notes that the fall-prevention, panic-alerting and wander-management systems developed by RF Technologies and recommended in this document below for the care of nursing-home and assisted-living residents primarily rely upon Wi-Fi for sending messages to caregiver staff.

For providing Wi-Fi service in the main buildings of the MCC the team has again selected the Cisco Aironet 3700 Series, this time a 3700i model with internal antennae. In the absence of an empirical site survey and calculated link budget the team again adopts Cisco's rule-of-thumb guideline and prescribes that the access points be installed upon the ceilings of selected rooms upon every floor of every building, the units being spaced in such a manner that no interior point at which

client service is required should be farther than thirty feet from the site of the nearest access point. A diagram in which this rule of thumb has been followed, resulting in a deployment of fourteen access points per each of the three floors of the Community Center and medical complex, has been included in this document as its Appendix 4.

Configuration of channels in adjacent APs (in the campus neighborhoods as well as within the main MCC buildings) should follow familiar patterns, of which Cisco provides this example:

Figure 64 Example of Channel Usage in 2.4 and 5 GHz (Two Channels Used if 40 MHz):



source: http://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/8-0/Cisco_Aironet_3700AP.html#pgfId-76097

Like the access points in the independent-living residential units, these access points will be connected to Cisco Catalyst Model 3650 switches with 1 Gbps Cat-7 cable, through which 801.3 power can be supplied. Discussion of the logical addressing, security, mobility-management and other aspects of their configuration and control will likewise be deferred until the discussion of the wired infrastructure components that will carry these functions out.

Other Wired Ethernet LAN Designs

Residential Independent-Living Wired Ethernet LAN (and WLAN control)

The schematic design of the wired Ethernet LAN that will serve the independent-living residents in the nine cottage neighborhoods of the MCC campus and the three floors of its apartment building is depicted on another diagram that is included as Appendix 5. As has already been described above in this technical design document, the fiber links depicted in this schematic diagram will also serve as the wired backhaul to the distribution switch for the 802.11 indoor access points to be installed in these residential quarters.

The logical topology of the LAN core is a star configuration, with satellite star configurations at each of the endpoint switches. These latter in turn constitute each fiber link of the core as the logical trunk of a separate tree.

The topology that has been chosen was suggested by the spatial configuration of the MCC's component physical structures, and the simplicity that results from following this suggestion is its principal virtue. To provide failover redundancy the design might have interconnected the several endpoint switches to form a ring or partial mesh, but doing so would require Layer-2 STP or RSTP to be configured and enabled upon the switches, an added complexity that can complicate the

interactions of their connected lightweight 802.11 access points with a Cisco controller.[4] Apart from the always present possibility of human error (in this case, of a misconfiguration), the first of the only two readily imaginable causes of network failure in this topology is a hardware failure of an endpoint switch, and the most straightforward precaution against such an event— switches being relatively inexpensive devices if the functional demands made upon them are not too great— is to keep a spare preconfigured replacement on hand. And the more costly Cisco switches recommended for application on the MCCN already include redundant power supplies, control planes and/or supervisor engines as a standard or optional feature, as well as the ability to configure unused ports as backups for the more critical connections.

The second of the two easily imaginable causes of network failure in the independent-living wired LAN is a failure of one of its nine underground 10 Gbps fiber links. Although the gross statistical rate of the occurrence of such failure is in the neighborhood of only 0.25% per kilometer per year (Alcoa Fujikra 2001), an enterprise might initially consider protecting itself against such an event by installing duplicate backup fiber links and connecting them to disabled ports on the endpoint hardware devices; that enterprise would quickly abandon the notion, however, when it appreciates that over 80% of all fiber-link failures are breaks inadvertently caused during excavations.[5] The MCC will enjoy the ability to exercise complete control over any excavation that takes place upon its property, and by the simple expedient of keeping and consulting accurate maps should be able to prevent an untoward event like such a break in a fiber link.

The wired Ethernet service will be provided to residential units through inexpensive unmanaged 5-port Cisco 100 Series switches mounted upon their walls, and for security as well as esthetic purposes the Cat-6 or greater cables running from these outlets to the neighborhood's single access switch will be concealed behind the interior drywall surfaces; these access switches themselves— Cisco Catalyst 3650 Series switches with 48 ports, to accommodate as many as 22 residential units in a neighborhood plus up to a dozen Aironet 3700 802.11 access points— will be located in lockable cabinets or wiring closets accessible only with the use of a key. The dozen neighborhood access switches will each in turn be connected via 10 Gbps fiber cable to a single distribution switch, which if not located nearby to other hardware in the Community Center network center will be placed within another physically secured enclosure between the Community Center and apartment buildings. The team has selected the Cisco Model 6503-E Catalyst switch for use as the network's distribution switch.

By the use of the 802.1Q protocol a single layer-2 connected network may be partitioned into separate broadcast domains between which packet traffic can pass only through the mediation of router functionality; in the definitional introduction these were identified as virtual local area networks (VLANs). If for no other reason than to limit the circulation of ARP, DHCP and other broadcast packets among the large number of hosts that may be connected to the single 172.22.0.0/16 residential subnet, the team has decided that this large subnet should be partitioned by the creation of neighborhood VLANs.

Residents in different neighborhoods will still be able to communicate with one another without the intervention of the enterprise router, however, because a 6503-E Catalyst switch fitted with a Supervisor 720 engine and its proprietary Cisco IOS software has the ability, not only to route packet traffic between distinct VLANs by means of the 802.1Q VLAN identifier added to the header of each Ethernet frame, but also to define and associate with each routed VLAN logical

---

[4] Cisco switches also run a separate instance of STP on every VLAN created, a complication that can increase the risk of misconfiguration by another order of magnitude.

[5] *Id*. The second leading cause is chewing by rodents (5%).

layer-3 IPv4 address spaces that look and behave exactly like IPv4 subnets, allowing the creation, for example, of separate DHCP scopes for separate VLANs. (Cisco 2011). Using this capability the team has designed for implementation the IPv4 VLAN interfaces shown in the first two columns of the following table:

172.22.nn.0/20:			
172.22.0.0-172.22.15.255	Infrastructure		
172.22.16.0-172.22.31.255	Andrews	0x10-0x1E	
172.22.32.0-172.22.47.255	Bright	0x20-0x2E	
172.22.48.0-172.22.63.255	Cope	0x30-0x3E	
172.22.64.0-172.22.79.255	Dewsbury	0x40-0x4E	
172.22.80.0-172.22.95.255	Earlham	0x50-0x5E	
172.22.96.0-172.22.111.255	Fell	0x60-0x6E	
172.22.112.0-172.22.127.255	Gurney	0x70-0x7E	
172.22.128.0-172.22.143.255	Hudson	0x80-0x8E	
172.22.144.0-172.22.159.255	Ingram	0x90-0x9E	
172.22.160.0-172.22.175.255	Jones	0xA0-0xAE	
172.22.176.0-172.22.191.255	Kent	0xB0-0xBE	
172.22.192.0-172.22.207.255	Londale	0xC0-0xCE	
172.22.208.0-172.22.223.255	Campus-Security	0xD0	
172.22.224.0/19	Campus-Other	0xE0, 0xF0, 0xF8	

But to completely understand the purpose of the range of VLAN IDs shown in the third column of each neighborhood's row within this table it is first necessary to understand some of the roles that will be played on the network (Cisco 2014a) by the Cisco Model 5508 wireless controller.

At the lowest layer the Model 5508 wireless controller provides radio frequency management services, adjusting channels and redistributing traffic between nearby access points to minimize interference and balance loads. At its highest layer the controller provides also mobility services to wireless clients travelling through the coverage of successive access points, even access points being managed by a different controller in a different subnet.[6] Most pertinent to present purposes, however, is the ability of the controller to create "dynamic" wireless interfaces in a manner similar to that of the Cisco 6503-E Catalyst switch, enabling one to create, for each neighborhood, a series parallel to the one for the Andrews cottage neighborhood shown below, in which the last six 802.1Q VLAN IDs and the dynamic interfaces associated with each were created by configuration of the Model 5508 controller:

CIDR ranges:	Interface Name:	VLAN ID:
172.22.16.0/23:		
172.22.16.0-172.22.17.255	Andrews_Ethernet	0x10
172.22.18.0-172.22.19.255	Andrews_LWAPs	0x12
172.22.20.0-172.22.21.255	Andrews_Silver	0x14
172.22.22.0-172.22.23.255	Andrews_Gold	0x16
172.22.24.0-172.22.25.255	Andrews_Platinum	0x18
172.22.26.0-172.22.27.255	Andrews_HIPAA	0x1A
172.22.28.0-172.22.29.255	Andrews_Staff	0x1C
172.22.30.0-172.22.31.255	Andrews_Guest	0x1E

This exercise has a point, or rather, several points. Cisco employs a slightly technical usage of the term "WLAN" in which it refers to a logical entity that exists in a more or less one-to-one

[6] For this purpose the controller maintains a flat-file database of live client connections, which has a maximum of 1,000 simultaneous entries. If this limit is eventually pressed a larger model may be needed.

correspondence with one of the SSIDs (802.11 service set identifiers; up to sixteen that can be advertised by a given access point) that are reachable through a single access point or group of such access points, together with a set of associated parameters like the security policy designated for use on that WLAN. The nine Model 3700 lightweight access points in the Andrews neighborhood can be defined to constitute a single access-point group, in which the WLAN/SSID "Guest" is associated with the interface "Andrews_Guest," the WLAN/SSID "Silver" is associated with the interface "Andrews_Silver," and so forth. [7]

A single WLAN "HIPAA" can then exist in every neighborhood, in each of which a connection to the SSID of the same name will uniformly require EAP-TLS mutual device authentication and subsequent 128-bit AES-CCM encryption. Similarly, the terms "Silver," "Gold," and "Platinum" are terms that Cisco associates with the higher three of its four levels of differentiated QoS, any one of which can be associated with a configured WLAN, so that an association with the SSID "Guest" might always result, for example, in the client's receiving the lowest "Bronze" level of differentiated service, while a member of the emergency-response team who connects on the outdoor campus to the SSID "Staff" will enjoy a connection with the "Platinum" QoS. Meanwhile within every dynamic interface that it creates the controller will designate itself as DHCP relay at a fixed IPv4 address, and will thereafter send DHCP traffic to a virtual DHCP server instance (Ančincová et al. 2013) that assigns addresses to a scope within the dynamic interface's IP range. Addresses so assigned can later serve the enterprise router as a basis for applying traffic filtering or access control lists that appropriately discriminate among packets at the layer-3 level.

For this system to operate properly every port upon every switch must be accurately identified either as an "access" port that will carry only traditional Ethernet frames, or as a distribution or "trunk" port whose frame header will carry the additional 802.1Q tagging information; in the application that has just been described only the terminating wired Ethernet ports will actually be access ports only. The switch configuration should also first be "cleared" of all VLAN IDs other than those that are associated with packet traffic that the switch is intended to carry.

Wired Ethernet LAN (and WLAN control) in the Medical Complex Buildings

A diagram schematically depicting the configuration of network resources in the medical complex, including the clinic, assisted-living units (Darlington House) and skilled nursing care units (Anthony House), is attached as Appendix 6 to this technical design document. Along the right-hand margin of this diagram are symbolic representations of the Cisco Aironet 3700i lightweight 802.11 access points that will actually be installed on three floors of the adjoining Community Center, because these will share a Cisco Catalyst 3650 switch and Model 5508 wireless controller with the access points installed on the three floors of the medical complex. Like the Model 5508 that controls the access points in the independent-living residential sector, this latter unit is itself represented in a lower corner of the diagram of the IT resources within the Community Center (Appendix 2). The wireless controller and the larger Catalyst Model 6503-E that serves as the distribution switch for the medical complex will either be located nearby to other hardware in the Community Center network center, or within a physically secured enclosure between the Community Center and the adjoining medical complex.

In a manner similar to that just described in the preceding section, the distribution switch and controller will be used in tandem to configure 802.1Q-enabled interfaces that serve as "virtual IP

[7] The initial "CAPWAP" association of a lightweight access with its controller occurs at the layer-3 network level, for which it is not necessary that both devices be on the same subnet, but only that they both have assigned IP addresses. The _LWAP VLANs with the hexadecimal IDs ending with the digit "2" are intended only to facilitate the initial assignment of an IP to an access point for the purpose of establishing this association.

subnets," across which distinguishable groups of wireless clients may associate with one or another of several unitary WLAN/SSIDs. Distinct interfaces will thus be configured for geographically disparate regions like the medical clinic, Darlington House, Anthony House and (for its three floors of wireless access) the Community Center, but within each of the geographically single regions of Darlington House and Anthony House separate interfaces, wired as well as wireless, will need to be created for the residents and their caregivers. SSIDs advertised by the APs throughout these several regions will include a HIPAA-compliant caregiver designation, as well as "Guest" and appropriate designations for MCC residents and non-medical staff. The caregiver WLAN/SSID is the one that will be used by the fall-prevention, panic-alerting and wander-management systems recommended for the care of nursing-home and assisted-living residents to send messages to caregiver staff at nursing stations and/or upon their mobile devices. It is also the WLAN that will be used throughout the medical center for the paging of staff.

An important difference exists, it should be noted, between the functional purpose of the interfaces configured within the independent-living residential 172.22.0.0/16 subnet, and those that will be configured in the medical complex. Remember that in the former case it was in the first place important to configure routing on the Cisco 6503-E distribution switch so that hosts in different neighborhoods could easily communicate directly with one another. But the Catalyst switches selected by the team for the MCC application can also enforce access control lists (ACLs) at either the link or network layer (Cisco 2013c), and the interfaces created within the 172.21.0.0/16 medical-complex subnet will be used in combination with ACLs primarily to enforce isolation of sensitive medical data from MCC residents and others whose access to it should be prevented.

In another section of this document will be discussed at greater length the Cisco HealthPresence client/server telemedicine application, which can be used to conduct an appointment with a remote physician completely over the network wire. In the discussion of the ASR 9000 Virtual Services Module above it was explained that this module can be slotted into the MCC's ASR 9006 gateway router to enable it to protect the data exchanged during such telemedical sessions with complete IPsec encryption, but in the site-to-site tunnel mode of operation that is contemplated for the MCCN encapsulation of IP datagrams within their ESP enclosures is a process that will take place only after the datagrams have been delivered onto the router itself, just prior to their dispatch into the public WAN. And in any event traffic between the HealthPresence Connect application server on the 172.17.0.0/16 subnet and the client process running within the medical clinic will not be subject to such encryption.

There is a growing understanding that the creation of isolated "data silos" within separate functional units of an enterprise can pose problems of data consistency, integration and availability throughout larger enterprises, which have been adopting data governance policies that mandate maintenance of a "single view of the enterprise" through a unitary database serving as a backend to ERP software. The symbolic representation of file and database servers within the medical clinic region of the medical-complex IT diagram is not meant to convey an intentional departure from such a policy— Oracle RDMS software provides for the deployment of a unitary but distributed enterprise database— but only to serve as a reminder that medical staff working within the clinic, as well as the nursing stations connected to it, will routinely require HIPAA-compliant IT access to their patients' medical records. These staffers are the persons who create, update and consult them.

Access of this kind to the medical data gathered in MCC residences by remote wireless sensors and communicated to those intelligent applications that have been developed to interpret and store it will also be required by the medical clinic. In the security section of this design document below it is acknowledged that sound database design and administration will play a key role in protecting IT

resources that was perhaps insufficiently appreciated in the Part 1 document. Whatever help can be given by access restrictions enforced in layer 3 of the network will certainly not be wasted.

Campus Security LAN (and WLAN devices)

The team recommends that video surveillance of the MCC premises for security purposes be accomplished with the use of seven Axis 604X-E series Pan-Tilt-and-Zoom dome network cameras.[8] A map of the camera deployment proposed by the team— in which five cameras located on a rooftop near the junction of the community center and the apartment building provide 300°of vision, and another two cameras mounted high in the parking lot at the MCC's southwest corner provide complementary coverage of 120°— has been attached as another appendix to this document. The two cameras facing outwards towards the parking lot in front of the main buildings are the less expensive Axis model 6042-E, while the other five cameras of the design are Axis' top-of-the-line 1080-pixel high-definition model 6045-E. In clear daylight conditions this latter camera is capable at full zoom of allowing an operator to distinguish the individual digits of an automobile license plate 900 feet away, a length that just exceeds the distance from the site of the five cameras on the rooftop to the site of the other two, in the southwest-corner parking lot at the opposite end of the campus.

Axis 604X-E series cameras offer day/night functionality, enabling clear black and white video in low light conditions. The cameras not only permit an operator to remotely activate up to 240x zoom, but also allow him to command up to a full 360° pan and/or as much as 220° of tilt. The cameras are also capable of detecting motion, and can be preconfigured to move to any one of 256 available positions in response to user-selected event triggers. As the last statement implies, the cameras can generate defined event objects to be processed by intelligent video applications, and respond to the commands that are then generated by such applications: for creating them the manufacturer makes available the open APIs of its VAPIX and AXIS Camera Application platforms. The cameras are of course network-ready, and support a full panoply of networking protocols; their security capabilities include 802.1x network access control, digest authentication, TLS/SSL encryption, and user-level password protection and device access logging.

In its Part 1 design document the team expressed misgivings about the bandwidth demands that security cameras might place upon a wireless network in particular, and indeed just one of the model 6045-E cameras here being recommended, if configured to generate a motion JPEG stream of just medium image quality, would alone require instantaneous throughput of 40.8 Mbps, and could consume *3.1 Terabytes* of storage capacity in just one week of full-time operation. In the team's final design the cameras will be connected to the network by means of wired Ethernet, but the team nevertheless deems it an advantage that the Axis 604X-E series models can generate high-definition streams of good video quality while using the high-compression H.264 codec. In this mode of operation a model 6045-E camera consumes bandwidth at a rate of 8.2 Mbps, and 617 GB storage per full-time week.

The two Cat-7 Ethernet cables that the team proposes to run from a security-subnet switch in the Community Center across the full length of the MCC campus can be used to provide 801.3at power as well as connectivity to the cameras in the southwest parking lot if VDSL ethernet extenders are deployed at both ends of the links to overcome the 100-meter length limitation that would otherwise apply; Perle markets a model that allows 50 Mbps per link and can withstand harsh outdoor temperatures.[9] The team chose the routes for the UTP cables shown in the appendix to facilitate, if

[8] http://www.axis.com/en/products/q60_series/index.htm
[9] http://www.perle.com/products-10-100-1000-industrial-poe-ethernet-extender.shtml

later thought necessary or prudent, the deployment of additional surveillance cameras in strategically chosen positions, particularly those that might create more points of vantage upon the parking lots along the MCC's eastern perimeter. Layer-2 switches would have to be inserted nearby to any additional cameras later connected, but elimination of the extenders would at the same time allow for greater throughput.

The team seems to recall the original project specifications mention installation of surveillance cameras atop lampposts that line the streets within the Millbrook Community Commons. This seems of a pale with an already remarked tendency of these specifications to represent the size of the MCC as being greater than many small towns in Pennsylvania. In reality there are to be no streets within the Millbrook Community Commons campus, but only paths adapted for pedestrian, wheelchair, and perhaps limited bicycle traffic, or use by MCC staff in small motorized carts.

Nevertheless it remains beyond dispute that the one of the best deterrents to crimes like burglary is good premises lighting. This team's designs already require that street lampposts be erected near the gazebo at the center of the MCC campus and upon the southwest corner parking lot, if existing designs for the MCC do not already include them; a non-networking recommendation by the team suggests that they be erected in all other parking lots as well. There is no need to disturb the esthetics of the campus by the erection of additional, interior lampposts, on the other hand, because the illumination required for adequate security can be provided by lighting fixtures installed upon the exterior walls of cottage units, under their eaves. To prevent such exterior lighting from disturbing the sleep of the inhabitants the fixtures can be designed to be activated by cooperating exterior wall-mounted ZigBee motion sensors, in an application whose functionality is wholly contained within the confines of each residence.

The Model MS-6100:

src: http://www.metissecure.com/solution/?id=outdoor-help-station

Last but not least among the features of this team's design for a campus security LAN— apart from short-range low-power wireless applications described under another heading of this document— is a recommendation for installation of emergency help stations: the MCC may lack interior streets, but not intersections and corners, upon every one of which the team proposes that there be installed a Model MS-6100 from Metis Security Solutions. [10] In appearance this device may be as unlovely as it is instantly recognizable, but in the breadth of its functionality the MS-6100 is truly remarkable. Powered by 12-24 volt DC with a lithium-ion battery backup, this device allows a person in dire need to immediately transmit a plea for help via a push-button hands-free voice call to designated emergency first responders, to whom there is simultaneously also transmitted the caller's precise geographic location. Alerts can be automatically sent to other systems such as speaker systems, the mobile phones of personnel on patrol, and indoor communications devices. A siren, flasher and visible screen are part of an emergency system for communication of alerts that operates in the opposite direction.

The outdoor Model MS-6100 can communicate calls to the Security and Emergency Response offices within the central Community Center building by means of the 802.11 service established throughout the residential campus by the two-node Cisco "mesh" deployment. Several other modes of redundant backup communication can also be enabled upon the device, but for the purposes of the outdoor MCC deployment the relevant mode is a self-contained ZigBee wireless mesh.

[10] http://www.metissecure.com/solution/?id=outdoor-help-station

Functionality similar to that provided by the Model MS-6100 is available from the more compact and less homely indoor Model MS-5100. [11] The team is recommending installation of an MS-5100 in every residential unit outside of the medical complex (in which other alert systems, interacting with caregiver staff, will instead be deployed). The team is also recommending that the MCC make available to any resident who wishes to have it installed upon his personal smart mobile phone Metis Solutions' Panic Button[12] app, which can instantly transmit an alert that includes the device's GPS coordinates. The versatility of the entire system for Security and Emergency Response personnel can also be enhanced by the installation in their office of Metis' Command Center 2.3 software, which provides an integrated dashboard through web-based user interfaces.[13]

The Model MS-5100:

src: http://www.metissecure.com/solution/?id=indoor-help-station

Networked Audio and Video Applications at the MCC

For online audio and video chatting with family and friends, there is no reason why MCC residents should not install and make use of whichever popular application like Skype, Google Hangouts or Apple FaceTime they and their correspondents prefer. Each of these operate with buffered TCP connections, and the network infrastructure designed in this document certainly provisions enough bandwidth, upstream as well as downstream, to make possible its pleasant use. Each of them can also safely penetrate the MCCN's planned NAT barrier.

For real-time audio and video communication between residents and MCC staff, however, or between staff members among themselves, a more secure alternative— one that does not send the IP packets off the LAN in the first place to some server on the public internet— is certainly to be preferred. This is especially true in the use case of telemedicine-conferencing between MCC residents and members of the medical/caregiver staff, even if for technical reasons audio and video packet data, like medical documents transmitted by means of a fax, are excepted from the requirements of the HIPAA Security Rule.

An open-source application that seems to best meet these requirements is Jitsi,[14] which can run on the Windows, Mac OS X and Linux desktop platforms, and supports nearly all of the audio and video codecs in common use today. Jitsi uses the ZRTP protocol to authenticate its end-users and for their subsequent symmetric key exchange, and then employs SRTP to encrypt and encapsulate the underlying RTP datagrams; instant messages and any files transferred within them are transmitted during TLS-secured TCP connections.[15] Installation of the application JitsiMeet upon a server with sufficient bandwidth (high processing power is unnecessary, because component streams are separately transmitted) extends Jitsi capabilities by facilitating multiparty video-conferencing. Unfortunately non-experimental Android and iOS versions of Jitsi, for use with mobile telephones and tablets, are still unavailable.

For real-time high-definition audio and video consultation between staff in the medical center and off-premises medical professionals, the team recommends installation upon a server and

---

[11] http://www.metissecure.com/solution/?id=indoor-help-station

[12] http://www.metissecure.com/solution/?id=panic_buttons

[13] http://www.metissecure.com/solution/?id=command-center

[14] https://jitsi.org/

[15] ZRTP uses Diffey-Hellman exchange and so cannot prevent man-in-the-middle attacks. To guard against this possibility the Jitsi application uses an onscreen exchange of simple 4-character nonces.

workstation at the medical center (as well as at the off-premises location of the correspondent provider professional) the latest available version of Cisco's HealthPresence software. This software establishes an environment in which a patient and his professional attendant may conduct a virtual appointment with a remote provider, during the course of which data collected by interoperable medical devices— third-party devices that digitally communicate with the attendant's workstation through common digital interfaces like Bluetooth, USB, S-video or RCA, and are Cisco-certified as compatible with the HealthPresence application platform— are transmitted in real time, along with the audio/video context, to the remote provider's workstation. Cisco HealthPresence also allows integration with compatible workflow and productivity tools including electronic medical records systems, directory services, and medical practice applications that address items like scheduling, billing and appointment reminders. (Cisco 2012).

The software's threefold Connect Server software, comprising application server, portal and administration components, can be installed upon any Red Hat Enterprise Linux server equipped with a minimum of 16 GB of DDR3 1333 MHz RAM, two multi-threaded quad-core 2.4 GHz processors, a 4-port 10/100/1000 Mbps Ethernet NIC, and 100 GB SATA hard drive for storage as well as a DVD±R optical drive; in contrast the endpoint application can be installed even upon a laptop running Windows 7, provided only that the system is a 64-bit version (thus a nurse could visit a resident in his home with a Bluetooth-equipped laptop upon which the endpoint has been installed, and together with her patient conduct a session, informed by the output of portable medical measuring devices, with a provider physician located back at the medical complex). But in order to create the best virtual patient-physician experience that is technologically possible, a large-screen high-definition monitor should ordinarily be connected to a local attendant's workstation in the MCC medical complex.

Role-and-user-based access, with password authentication, provides security for HealthPresence at the application level. This facility is enforced by the portal component of the HealthPresence Connect Server, but for improved security generic user credentials usable by all medical attendants and providers can and should be created and enforced by the central Windows domain server. To prevent a different form of unauthorized access entire sessions must also be secured at the Layer-3 network level, by the use of tunnel-mode ESP IPsec between the conferencing endpoint gateways.

The audio and video applications described above in this section all facilitate the use of VoIP communication from a desktop computer, either as an integrated session feature or in a stand-alone "softphone" calling mode. Recent actions by the FCC have obviated, at least for service from a commercial provider interconnected with the PSTN, what otherwise would remain the most serious objection to a full-scale deployment of VoIP at a facility like the MCC, the erstwhile inability to alert first-responders to an emergency at the caller's location by dialing 911 on a VoIP phone.[16] Although potential cost savings are attractive and VoIP is clearly the wave of the future, the MCCN cannot guarantee the QoS of packet telephone service beyond the gateway to its LAN, inside of which temporary network outages will always, moreover, remain at least a possibility. If after careful study of the several trade-offs involved the MCC elects sometime in the future to pursue a full-scale deployment of VoIP, the team suggests that it then contact Windstream to explore the design of a unified communications system integrated with the existing network.

In the meantime the MCC plans to have its site wired for traditional circuit-switched telephone service. It also plans coaxial cable links, over which it will have a provider supply cable television service at no extra charge, to all residential units, and residents will have the option to purchase their own private internet service with the cable television service provider. The MCC will make

[16] The FCC summarizes the present situation at http://www.fcc.gov/guides/voip-and-911-service.

subscription virus-protection and personal-firewall security software freely available to all residents, strongly encourage them to use it— especially those who contract individually with their own personal ISP— and install or configure the software for them upon request.

Wireless Personal Area Networks

The wireless personal area networks that will exist at the Millbrook Community Commons will for the most part implement standards for short-range low-power wireless mesh 802.15.4 technology developed by the ZigBee Alliance. ZigBee networks will be created within the living quarters of residents requiring any one of the three graduated levels of care provided at the MCC, and will support applications in the fields of remote healthcare, security, energy conservation and personal convenience. At the MCC applications can also be classified according to whether or not they require communication between devices on the mesh network within a residence and IP hosts on the outside LAN or even WAN.

The ZigBee standard defines a protocol stack similar to the stack of TCP/IP. The lower link layer employs CSMA/CA with error detection and can ensure reliable communication between the endpoints of a link. The network layer provides discovery and routing and so makes possible not only device-to-device communication but also the creation and maintenance of self-healing mesh topographies. A standardized ZigBee Device Object existing on the application layer provides security services, and identifies every participating device as a simple endpoint device, a device with routing capability, or the single coordinating device that must exist upon every network. Applications operate when communicating endpoint devices exchange messages whose formats have been defined in public or private profiles, and the addressing functions of the application support sublayer maintains a database of binding tables that are used to establish these complementary pairs.

The ZigBee Device Object at the application layer provides application message encryption (based upon AES-128-CCM actually executed at the link layer) as a standard platform service. An initial 128-bit master key must be somehow be securely installed upon devices participating in the network. Afterwards the coordinating control device, operating as a trust center, maintains and distributes a single network key usable by all mesh nodes, and individual link keys derived from the master key.

The ZigBee Gateway Device

A standard developed by the ZigBee Alliance defines the generic ZigBee Gateway device (ZigBee 2012), whose crucial role is to transmit requests and responses to/from devices operating on a ZigBee mesh network across a TCP/IP network from/to the IPHAs (IP Host Applications) running on servers or workstations that make the captured data accessible to humans. The three request/response formats specified in the standard include XML/SOAP and REST, both of which are already in widespread use for creating html-GUI applications based upon the data provided by web services. The ZigBee Alliance rightfully specifies additional security requirements as a prerequisite for gateways used in smart-home and healthcare deployments, and its standard provides for the optional transmission of messages in https (TLS-secured) connections.

Unfortunately it sometimes appears that the ZigBee platform, however promising for the future, is still very much a vision awaiting practical implementation. At zigbee.org the team could find only two ZigBee-certified gateway devices, both developed by Telecom Italia, that appear to be TLS-capable; each runs on embedded Linux and implements the lightweight REST web messaging framework. And developed IPHAs that make use of the REST message/object format do not yet seem to be commercially available anywhere.

Nevertheless the Canadian firm Exegin advertises an IP Host Application Framework for developers that includes a full protocol stack (based on REST), a library of functions for the attributes in the ZigBee Cluster Library (ZCL), and an example Java example application called Tiki.[17] And the JAX-RS component of the current Java Enterprise Edition Version 7 includes functionality for accessing resources offered by RESTful web services. (Jendrock, Cervara-Navarro, Evans, Haase & Markito 2014). So the team's design includes a plan to equip every residential unit in the MCC with a generic Telecom-Italia Linux ZigBee gateway device, in the expectation that the MCC will either itself internally develop, or contract with outsider firms to develop, the IPHAs that will run on its servers or staff workstations.

The relative paucity of commercial off-the-shelf but certified standards-compliant solutions is puzzling. For several years now ZigBee Alliance member Freescale Semiconductors has made available to potential developers of complete medical and smart-home systems a full line of 802.15.4 components that includes not only circuits and silicon, but also embedded system software as well as design templates (their Home Health Hub reference platform, for example, provides programmable onsite interactive screen GUI capability with 802.11, Ethernet and GPRS gateway connectivity for the local ZigBee/Bluetooth PAN).[18] The team recommends to MCC management that it solicit contract proposals for the design, development, manufacture and deployment at the MCC of complete application solutions that will put 802.15.4 technologies already available from Freescale Semiconductor to effective use throughout its premises.

Networkable Health Care Devices

Already available ZigBee-certified remote medical monitoring devices include a pulse oximeter, blood-pressure monitor, blood glucose reader and weight scale, all developed by Brunel University in London. Freescale Semiconductor builds an accelerometer and gyroscope that can be incorporated into a wearable fall-detecting sensor, so devices of this kind should be available too; an IPHA could conversely be programmed to deliver an alert whenever the motion-detecting sensors used in security and smart-home applications do not detect any physical activity within the home for the length of a predefined extended interval that warrants concern.

The in-home panic alarm devices manufactured by Metis Security Solutions and targeted for use within the MCC have already been described elsewhere within this technical design document, where it was noted that the team recommended these systems for use in the independent-living resident units only. In the assisted-living and nursing-home residential quarters within the MCC medical complex the team instead recommends deployment of RF Technology's wireless QuickResponse Plus wearable pendants with Smart ID.[19] When a resident pushes a button on one of these wearable devices, his name and location data are immediately sent to a central nursing computer station and, optionally, to designated caregiver staff mobile devices.

The more fit of the active independent-living residents may already own wearable devices that measure and store time-series records of physical activity, heart rate and sleep patterns, and can upload the collected data to a computer or mobile device for later analysis and display via Bluetooth or USB interfaces.[20] The devices to which stored data like these are later uploaded need not be limited, of course, to those owned by the resident who is wearing the device, but can include other devices carried by members of MCC's medical/caregiving staff.

---

[17] http://www.exegin.com/software/zigbee_ipha.php

[18] http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=RDHEALTH_HUB

[19] http://www.rft.com/Quick_Response_Plus_with_Smart_ID-c1379-wp8260.htm

[20] http://www.pcmag.com/article2/0,2817,2404445,00.asp

Home prescription compliance can be monitored by a simple ZigBee-communicating pill dispenser like one developed by Brunel University. For seniors who own mobile phones or tablets and are familiar with their use, medication-taking reminder systems based upon the transmission of SMS alerts have been proven to be effective, and apps like OnTimeRx by AmeliaPlex[21] can be installed on all currently popular mobile platforms. For less technologically comfortable seniors a combined compliance and audio reminder system that includes a programmable automatic dispenser that delivers noncompliance alerts by telephone can be purchased from Philips as a subscription service whose price starts at $44 per senior per month.[22]

Within the nursing-home facility might be widely deployed ZigBee-based pressure-sensing bed and seat mats, to detect when a patient attempts to rise unaided; RF Technologies offers a recommended Sensatec System that already includes integrated and configurable delivery of alarms to designated nursing stations.[23] Finally, the team recommends for use with residents suffering from cognitive impairment the RF Technologies' CodeAlert wandering management system, which triggers locks and activates alarms whenever a patient wearing a transmitter attempts to leave a designated monitored area.[24]

Smart-Home Energy Conservation, Security and Personal Convenience Devices

There is no shortage of commercial firms offering smart-home products to promote security, energy efficiency and convenience. Here, too, unfortunately, neither the ZigBee Alliance nor anyone else has enjoyed the success that the Wi-Fi Alliance has attained in winning acceptance of open standards, and nearly all of the available products are partial proprietary solutions that are not interoperable with one another (Kastrenakes 2014).

For this reason the team was happy when its research finally disclosed the existence of the ZigBee Alliance member ubisys technologies GmbH, a German engineering firm that produces and markets worldwide a complete, standards-compliant smart-home installation. A diagram depicting some of the components of its smart-home installation, culled from the website accessible at http://www.ubisys.de/en/smarthome/solutions.html, is attached to this document as Appendix 7.

This diagram does not come close to depicting all of the features and capabilities of the ubisys system. For home security the system deploys threshold video surveillance and remote front door access control, as well as window and door sensors, motion detectors, smoke, gas and fire detectors, and pipe rupture detectors that all can actuate programmable alarms. Upon detection of a break-in, for example, all lights in the home will immediately be turned on and all window blinds opened; other scenarios that can be triggered by the occurrence of an event defined to require an alarm include the immediate transmission of a message to a remote smart phone, or a security monitoring service with which the property has been registered. These measures are of course in addition to, and complement, the Metis in-home push-button alert system that was already described above.

Capabilities offered by ubisys to enhance control of energy use include a heating regulator to which the thermoelectric actuators of an underfloor heating system can be attached to allow simultaneous thermostatic control of up to six independent heating circuits per module. The motion sensors in the home also interact with the already light-sensitive illumination dimming controls to adjust artificial lighting to ambient conditions and human presence or absence. A metering function

---

[21] http://www.ontimerx.com/

[22] http://www.managemypills.com/content/How_PMD_Works

[23] http://www.rft.com/Sensatec_Fall_Management-c1379-wp8208.htm

[24] http://www.rft.com/Code_Alert_Wandering_Management-c1379-wp8200.htm. RF Technology is a business partner of Freescale Semiconductor. All of the devices described above rely upon Wi-Fi communications, however.

allows per-appliance measurement and graphical presentation of thirteen separate energy consumption parameters, and remote power switches permit the resident to reduce device standby power consumption.

The human interfaces provided by ubisys for its smart-home installation include a programmable 7-inch wall mounted touchscreen display that allows one to simultaneously control or monitor multiple system elements, view graphically presented statistical consumption data either in the aggregate or by device, and programmatically define sets of system event-response scenarios. A ZigBee USB stick extends this interface to a nearby desktop computer, and ubisys has also created, as was intimated above, Apple iOS and Android apps to supply residents or their delegates with this interface on smart phones and tablets. Connectivity with the IP network necessary to support this latter access is supplied by a secure and standards-compliant ZigBee gateway device.

Like the Telecom-Italia Linux ZigBee gateway device specified above for medical ZigBee applications, the ubisys gateway requires an Ethernet connection, over which it can also satisfy its limited 1-watt power requirement. A second gateway may appear to be a regrettable redundancy, but in fact the small-footprint ubisys device, communicating as it does with its IPHAs through the Gateway Remote Interface Protocol (or GRIP, the most lightweight of the three protocols optionally supported on a ZigBee gateway), complements rather than duplicates the functionality of the Telecom-Italia REST portal. A ZigBee endpoint can communicate with an IPHA through either.

Before leaving the subject of the smart home the team has a last word to offer, this time on the subject of resident convenience. For decades the dream of a single device that would provide its user with unified, understandable command and control of the televisions, home theaters, DVD recorders, game consoles, cable boxes and other entertainment devices within the home has been something of a holy grail, one that expensive devices like the Harmony remote have never quite succeeded in wholly attaining. To this end the ZigBee Alliance has promulgated its new ZigBee Remote Control 2.0 standard incorporating its RF4CE technology; unhindered by the interference problems, line-of-sight requirements and other limitations of 30-year-old IrDA implementations, this standard offers the promise of an experience in which a television selects the correct input port, a surround-sound home theater system selects the proper codec, port and mode, a remote control switches to the proper control interface, window curtains close and lights in the viewing room dim, all automatically upon the insertion of a DVD into a tray.

Once again realization of this dream is being hindered by the slowness of consumer electronics manufacturers to permit the required non-proprietary control of their products' behavior. This may change, however: Comcast is now incorporating ZigBee RF4CE technology into set-top boxes. The team recommends to MCN management that when it equips residential quarters with home-entertainment products it seek to secure ZigBee compatibility whenever possible.

Security Revisited

The team finds no reason to abandon the summary of HIPAA-based network security requirements that it set forth in its earlier Part 1 document, which it reproduces here without the original footnote citations to applicable detailed NIST Special Publications:

> Information sent over every wired and wireless network segment of the Millbrook Community Commons will unavoidably include "protected health information" pertaining to identifiable community residents. The Millbrook Community Commons will furnish, bill and receive payment for health care in the normal course of its business, and in doing so will electronically transmit one or more of the "covered transactions" for which the HHS Secretary has promulgated standards at 45 C.F.R. Part 162. As such the MCC is a "covered entity" subject to the privacy and security standards

of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 29 U.S.C. §§1181 *et seq*.; 42 U.S.C. §300gg, §§1320d *et seq*., as this statute has been extended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of February 17, 2009, 42 U.S.C. §300jj *et seq*., §§17901 *et seq*., and the regulations promulgated by the Secretary of Health and Human Services thereunder.

These regulations include the Privacy Rule and, more especially pertinent for present purposes, the Security Rule, which are codified together at 45 C.F.R., Part 160 and Part 164, Subparts A, C and E. During the internal processes that preceded the drafting of this latter regulation, as well as the legally mandated period of public comment that followed the publication of the proposed version of the rule before its adoption in final form, the HHS Secretary solicited and obtained guidance from leading private-industry experts in the field of information privacy/security, as well as public agencies like the National Institute of Standards and Technology (the body responsible for developing IT standards for all federal operations other than national security). Perhaps unsurprisingly, the Security Rule for the most part formulates, in appropriately general terms meant to be adaptable to future technological evolution, a compendium of current best practices; as such its requirements ought not to be regarded as a regrettable burden specially entailed by MCC's role as a covered health care provider, but as a reliable guide to securing the integrity, privacy and security of *all* of the information assets with which the MCC will be entrusted, or will itself create. Besides residents' protected health information, these latter will also certainly at a minimum include: residents' financial and other personal information, maintained in their customer accounts; employee information maintained by MCC's human resources function; and the central database serving MCC's own enterprise resources planning applications.

Primary responsibility for the implementation of certain major provisions of the Security Rule should clearly be assigned, preferably by detailed service-level agreement, to MCC management itself. These include the responsibility for physical security, enforced by the designation of specified limited-access zones, physical systems and devices, the deployment of locks, monitors or sensors and, if necessary, security guards, and the creation of a system of staff-member identification. Closely related to this physical-security requirement is the need to establish change-management policies governing the addition of new resources to the IT platform, the retention of an NAID-certified vendor to guarantee secure destruction of data written upon retired devices, and a process for the on-disk storage encryption of the most sensitive information. MCC management must also be primarily responsible for creating, at the level of the domain server and client/server application, a thoroughgoing system of user authentication, access and accounting that grants pre-determined rights to access clearly defined data resources, upon the principle of least privilege, to authenticated users only, and logs the parameters of every resource access that is made or attempted. It is also management's role, finally, to ensure that its staff are adequately trained in the use of this system, and to employ capable auditors to verify that the system is functioning as intended, according to design.

It is evident, however, that even where MCC management will be primarily responsible for Security-Rule compliance the networking team may still have an important role to play. For example, there are security-related as well as esthetic and operational benefits to be obtained if the network design specifies that all optical and twisted-pair cabling is to be enclosed within conduit, and located where possible behind walls or ceilings; the design might also specify that optical fiber only— less vulnerable to tapping, and insensitive to interference as well— is to be used for confidential or mission-critical wired connections. The networking team must also at a minimum ensure that the infrastructure it designs will be functionally capable of supporting the servers and applications that management intends to deploy; in such matters as the selection, location and configuration of a gateway firewall and intrusion detection system, moreover, or the secure configuration of MCC's servers (which will include not only its mail, HTTP and database servers, but also the AAA domain server used to authorize access to its encrypted wireless networks), the role of the network team will probably rise from the level of consultation to the level of collaborative

> design. The same will hold true with respect to the creation of system redundancies for the purpose of data backup and disaster recovery.
>
> The design of effective systems for the encrypted transport of data over the MCC's internal network, on the other hand, is a primary responsibility of this team. If the MCC management intends to allow staff members off-premises access to its internal network over the public internet through a VPN, if off-premises transport of protected health information in its practice of telemedicine will not invariably be protected at the transport layer through TLS/SSL, or simply if MCC management elects to "go the extra mile" and routinely encrypt LAN transmissions over the wire, the team must ensure that all routers and connected hosts are IPsec-capable, and configured to work with SAs that incorporate adequate methods of symmetric encryption. To implement smart-home technologies for security and energy management and permit remote monitoring of key indicators of residents' physical safety and health, the MCC plans to create short-range wireless mesh networks that will operate within its residents' cottages and apartments; the communicating ZigBee devices that comprise these short-range mesh networks and are used for data acquisition or supervisory control already include built-in functionality that operates immediately below the ZigBee application layer and provides application message encryption (based upon AES-128-CCM at the link-layer) as a standard platform service. In the … 802.11n networks that will provide ubiquitous wireless service within the MCC's cottage campus, the network design recommended by our team will conform to all applicable NIST-mandated security standards for federal networks: mutual authentication of the wireless device and RADIUS server, and concomitant generation of a symmetric master session key, through the EAP-TLS method, making use of the CA, server and device X.509 certificates and public-private key pairs of the RSA encryption algorithm; during subsequent exchanges between the wireless device and base station (to which the RADIUS server will have securely transmitted the generated MSK) that include the four-way handshake of 802.11i …derivation from the MSK of the transient session subkeys that will be deployed to guarantee confidentiality and message integrity, while frustrating replay or other man-in-the-middle attacks; and in the actual hashing and encryption processes for which these several keys have been derived (including, most pertinently, those that will finally occur during actual transmissions of client data) making use of the CCM submethod of 128-bit AES-1, with encryption modules certifiable under FIPS 140-2.

(See generally Scholl, et al., 2008). Security-minded features of the team's technical network design that are meant to facilitate the implementation of the requirements described in these paragraphs have been given prominence in many sections of this document already. In the course of implementing its earlier vision for security by a physical hardware design the team has found occasion, moreover, to discover a few new emphases as well.

For one thing the team has come to appreciate that satisfactory compliance with HIPAA not only requires *achieving* data security and privacy, but also developing the capability to simultaneously *demonstrate* that one has achieved it, a process that in systems of disaster prevention or quality control is often called "verification" of the system. In other words the team came to understand that it would fail in a duty that it owes to the MCC management who employed it if the system that it designed could not significantly limit in advance the scope of a subsequent HIPAA audit. Without limiting the network's exposure in this way it is difficult to be confident that a later test will more likely than not be passed.[25]

The description in the team's Part 1 document of the measures that will be to be taken to provide 802.11i security in the MCC's indoor/outdoor campus wireless network, for example, envisaged application of elevated NIST-mandated HIPAA security measures to all traffic passing

[25] The data-security firm Reclamere, headquartered in nearby Tyrone, PA, provides contractual security audit services of this kind, as well as forensic damage assessments of the kind that HIPAA requires in the event of a discovered privacy breach. Reclamere is also a NAID-certified vendor of secure e-cycling services for retired IT devices, and offers assistance for enterprise backup and disaster-recovery planning as well. http://www.reclamere.com.

across a single global network. Since it would be impractical to allow guest access on a wireless network employing EAP-TLS mutual device authentication preliminary to dynamic mutual symmetric key generation, the Part 1 document asserted that such guest access would probably just be denied in the MCCN. But while it may still be good practice to require, for every wireless connection, the greatest security precautions practicable, the single global wireless network that the Part 1 document clearly envisages is one that would obviously be difficult to successfully audit to determine its level of HIPAA compliance.

In the final plan that the team developed and presents within this Part 2, by contrast, guest-level access to MCC networks is expected and explicitly provided, but in such a manner that a guest's access to information resources can be limited through network design and configuration to just those that may be available on the public internet. (Specific security measures for guest connections were not earlier described, but a WPA2 Personal method, with the PBKDF2 hashing algorithm used to generate a pre-shared CCMP encryption key from a periodically changing ASCII password, are recommended here, as well as the configuration of the ACL filters that the previous sentence already implies). The extended passage recited above clearly assigns to MCC management the primary responsibility to prevent, by the use of AAA measures at the domain server and application level, unnecessary or inappropriate access to vital informational assets. Just as clearly did the same passage underestimate the degree to which such sensitive resources, by thoughtful network design and configuration, can be protected at lower layer-2 and layer-3 levels by their isolation and disaggregation.

This better appreciation of the help that can be given by effective network design was encouraged by coming to understand some of the more generally serviceable of the myriad security enhancements that have been added to component Cisco devices. Like the detailed prescriptions that can be gleaned from a perusal of the many numbered NIST special publications, these are as diverse and manifold as the threats that they were defensively tailored to counter, and no further attempt describe or summarize them will be useful in this context. Generally every precaution that can be taken should be; every advertised OS patch must be promptly applied; one must be ever vigilant and alert, and not just reactive but proactive too.

One last observation pertaining to the subject of the security of the MCCN, however, will be made before closing. End users often experience the requirements of good security as an inconvenient nuisance, but this is not the only way in which such measures can conflict with legitimate user priorities. It was remarked in an earlier section of this document, pertaining to security arrangements for the IT resources at MCC's medical clinic, that

> …[t]here is a growing understanding that the creation of isolated "data silos" within separate functional units of an enterprise can pose problems of data consistency, integration and availability throughout larger enterprises, which have been adopting data governance policies that mandate maintenance of a "single view of the enterprise" through a unitary database serving as a backend to ERP software…

The mandate to centralize data resources is clearly at odds with a purpose to isolate data for security purposes near the point of its final use. Harmonizing the important purposes of these two conflicting tendencies will require sound database design and administration, which will play a key role in protecting IT resources that was not acknowledged in the team's earlier Part 1 deliverable.

References

3Com Corporation (2005). *3Com wireless antennas guide*. Retrieved from http://www.scribd.com/doc/32613170/3Com-Wireless-Antennas

Alcoa Fujikra Ltd. (2001). *Reliability of fiber optic cable systems: buried fiber optic cable, optical groundwire cable, all dielectric, self-supporting cable*. Retrieved from http://www.southern-telecom.com/solutions/AFL-Reliability.pdf

Ančincová, B., Hradílek, J., Silas, D., Prpič, M., Wadeley, S., Kopalová, E., Domingo, D. (2013). Configuring a Multihomed DHCP Server. In *Red Hat Enterprise Linux 6 deployment guide, edition 6* (section 14.4). Retrieved from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/index.html

AXIS Communications, Inc. (n.d.). *Technical guide to network video*. Retrieved from http://www.axis.com/products/video/about_networkvideo/index.htm

Cisco Systems, Inc. (2011). *Catalyst 6500 Series supervisor engine guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Module_Installation/Sup_Eng_Guide/supe_gd.html

Cisco Systems, Inc. (2012). *Cisco HealthPresence 2.5 Solution design guide, version 2.5*. Retrieved from http://www.cisco.com/c/en/us/support/video/healthpresence/products-implementation-design-guides-list.html

Cisco Systems, Inc. (2013a). *Cisco wireless mesh access points, design and deployment guide, release 7.4*. Retrieved from http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/7-4/design/guide/mesh74.html

Cisco Systrems, Inc. (2013b). *Enterprise mobility 7.3 design guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch13Loca.html

Cisco Systems, Inc. (2013c) *Security configuration guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* Retrieved from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3se/security/configuration_guide/b_sec_3se_3650_cg.html

Cisco Systems, Inc. (2014a) *Cisco Wireless LAN controller configuration guide, release 8.0*. Retrieved from http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.html

Cisco Systems, Inc. (2014b) *Cisco Aironet Series 1700/2700/3700 access point deployment guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/8-0/Cisco_Aironet_3700AP.html

Jendrock, E., Cervara-Navarro, R., Evans, I., Haase, K. & Markito, W. (2014). Accessing REST Resources with the JAX-RS Client API. In *Java Platform, Enterprise Edition, the Java EE*

tutorial, *release 7* (chapter 30). Retrieved from https://docs.oracle.com/javaee/7/tutorial/partcdi.htm - GJBNR

Kastrenakes, Jacob. "The dumb state of the smart home." *The Verge*, January 24, 2014. Retrieved from http://www.theverge.com/2014/1/24/5336104/smart-home-standard-are-a-mess-zigbee-z-wave

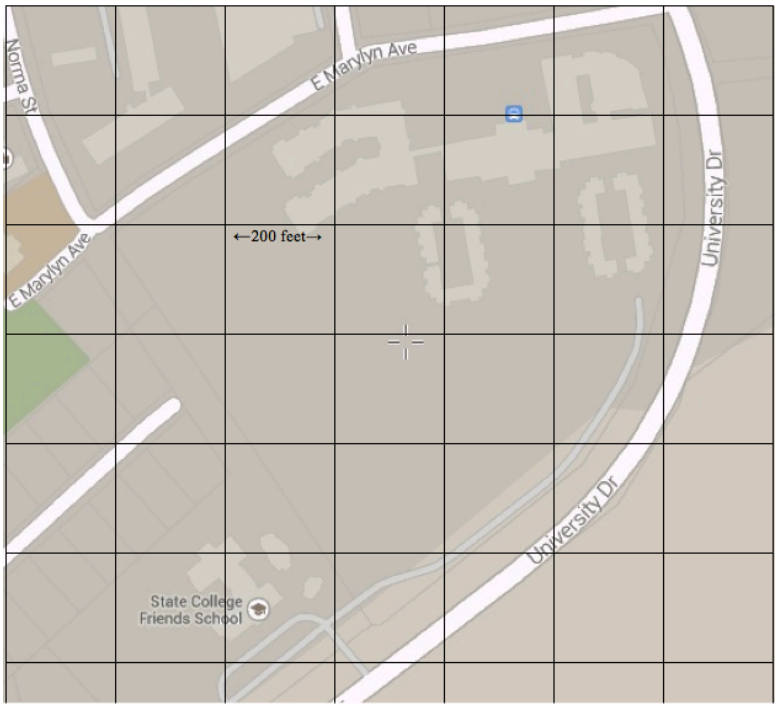
Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Dancy Smith, C., Steinberg, D. (2008). *NIST Special Publication 800-66 revision 1: An introductory resource guide for implementing the Health Insurance and Portability Act (HIPAA) Security Rule*. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

ZigBee Alliance (2010). *Understanding ZigBee Gateway: How ZigBee extends an IP network*. Retrieved from http://zigbee.org/zigbee-for-developers/zigbee-gateway/http://www.zigbee.org.

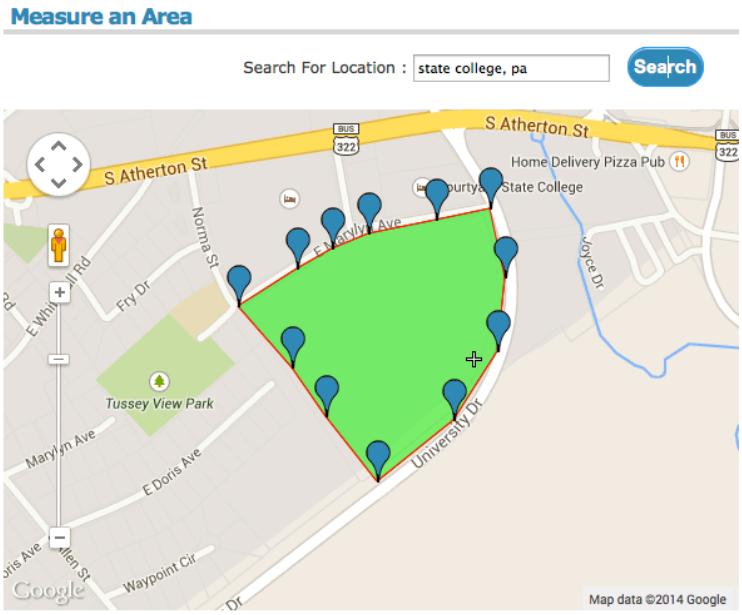
APPENDICES

Geometry ..... Appendix 1
Community Center Infrastructure Diagram ..... Appendix 2
Campus Residential WLAN Coverage Map ..... Appendix 3
Wireless Coverage in the Community Center and Medical Complex ... Appendix 4
Independent-Living Wired Ethernet LAN ..... Appendix 5
Assisted-Living Quarters, Nursing Home and Medical Clinic ..... Appendix 6
Network Camera Coverage ..... Appendix 7
Smart-Home System Overview (ubisys) ..... Appendix 8
Datasheets for Selected Network Components (available in a separate volume upon request):
- Cisco ASR Aggregation Services Routers ..... 13 pages
- Cisco ASR 9000 Series Virtualized Services Module ..... 4 pages
- Cisco ASR 9000 Series Integrated Services Module ..... 7 pages
- Cisco UCS C220 M4 Rack Server ..... 6 pages
- Cisco UCS C240 M4 Rack Server ..... 6 pages
- Seagate 6 TB SAS 12 Gbps Enterprise Hard Drive ..... 3 pages
- Cisco Aironet 1570 Series Outdoor Access Point ..... 12 pages
- Cisco Aironet 3700 Series Access Points ..... 10 pages
- Cisco Catalyst 6500-E Series Switch Chassis ..... 5 pages
- Cisco Catalyst 6900 Series 40-Gigabit Interface Module ..... 8 pages
- Cisco Catalyst 3650 Series Switches ..... 28 pages
- Cisco Catalyst 100 Series Unmanaged Switches ..... 7 pages
- Cisco 5500 Series Wireless Controllers ..... 9 pages
- AXIS Q60-E PTZ Dome Network Cameras ..... 4 pages
- Metis Secure Model MS-6100 Outdoor Help Station ..... 2 pages
- Metis Secure Model MS-5100 In-Building Help Station ..... 2 pages
- Metis Secure Panic Button Systems ..... 2 pages

Millbrook Community Commons: distances



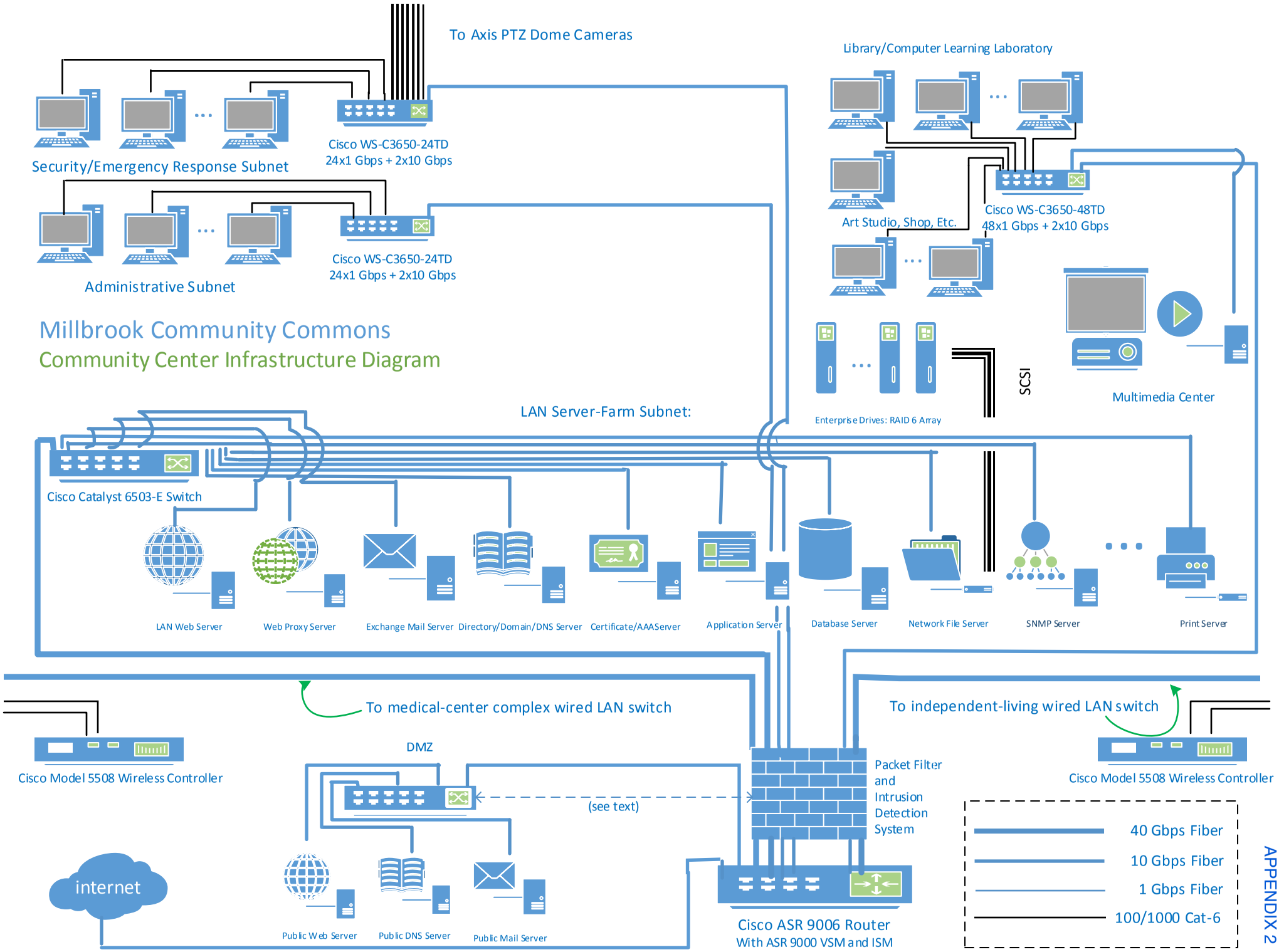
Millbrook Community Commons: area



Area Output

89192.256 m²
0.089 km²
22.040 Acres
8.919 Hectares
960057.455 Feet²

planimeter made available at www.freemaptools.com/area-calculator-htm


To Axis PTZ Dome Cameras
Library/Computer Learning Laboratory
Security/Emergency Response Subnet
Cisco WS-C3650-24TD
24x1 Gbps + 2x10 Gbps
Cisco WS-C3650-48TD
48x1 Gbps + 2x10 Gbps
Art Studio, Shop, Etc.
Administrative Subnet
Cisco WS-C3650-24TD
24x1 Gbps + 2x10 Gbps
Millbrook Community Commons
Community Center Infrastructure Diagram
SCSI
Multimedia Center
Enterprise Drives: RAID 6 Array
LAN Server-Farm Subnet:
Cisco Catalyst 6503-E Switch
LAN Web Server
Web Proxy Server
Exchange Mail Server
Directory/Domain/DNS Server
Certificate/AAAServer
Application Server
Database Server
Network File Server
SNMP Server
Print Server
To medical-center complex wired LAN switch
To independent-living wired LAN switch
Cisco Model 5508 Wireless Controller
Cisco Model 5508 Wireless Controller
DMZ
(see text)
Packet Filter
and
Intrusion
Detection
System
internet
Public Web Server
Public DNS Server
Public Mail Server
Cisco ASR 9006 Router
With ASR 9000 VSM and ISM
40 Gbps Fiber
10 Gbps Fiber
1 Gbps Fiber
100/1000 Cat-6
APPENDIX 2

Millbrook Community Commons

Campus Residential WLAN Coverage Map

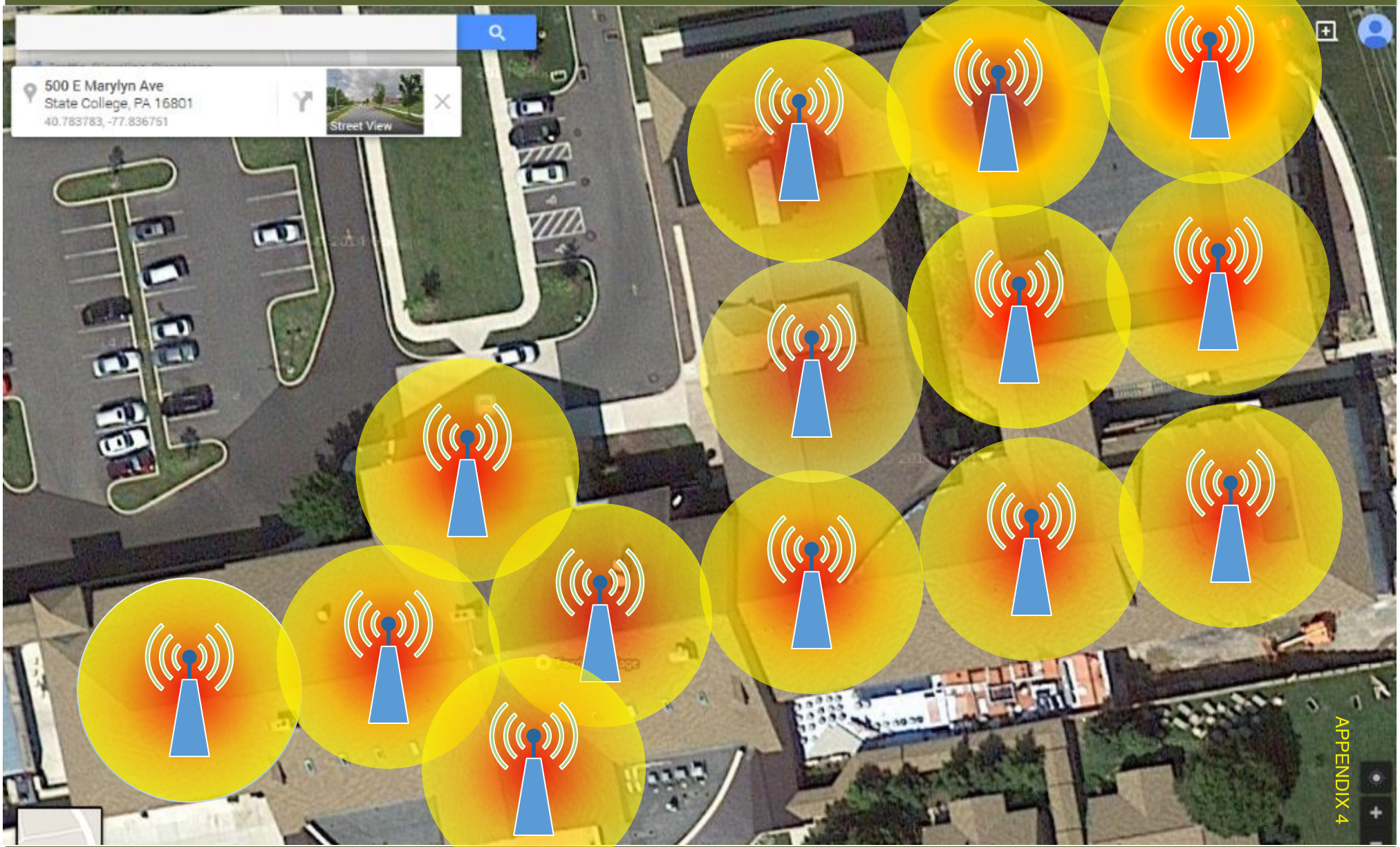
Cisco Aironet 1570 802.11ac/n Outdoor Mesh Access Point
(Community Center Rooftop AP to Central Mesh AP)

Cisco Aironet 3700 802.11ac/n Indoor Access Point
(to central wireless controller via shared 10 Gbps lines)

Cisco 5500 Series Wireless LAN Controller
(via wired Ethernet infrastructure)

Millbrook Community Commons

Wireless Coverage in the Community Center and Medical Complex



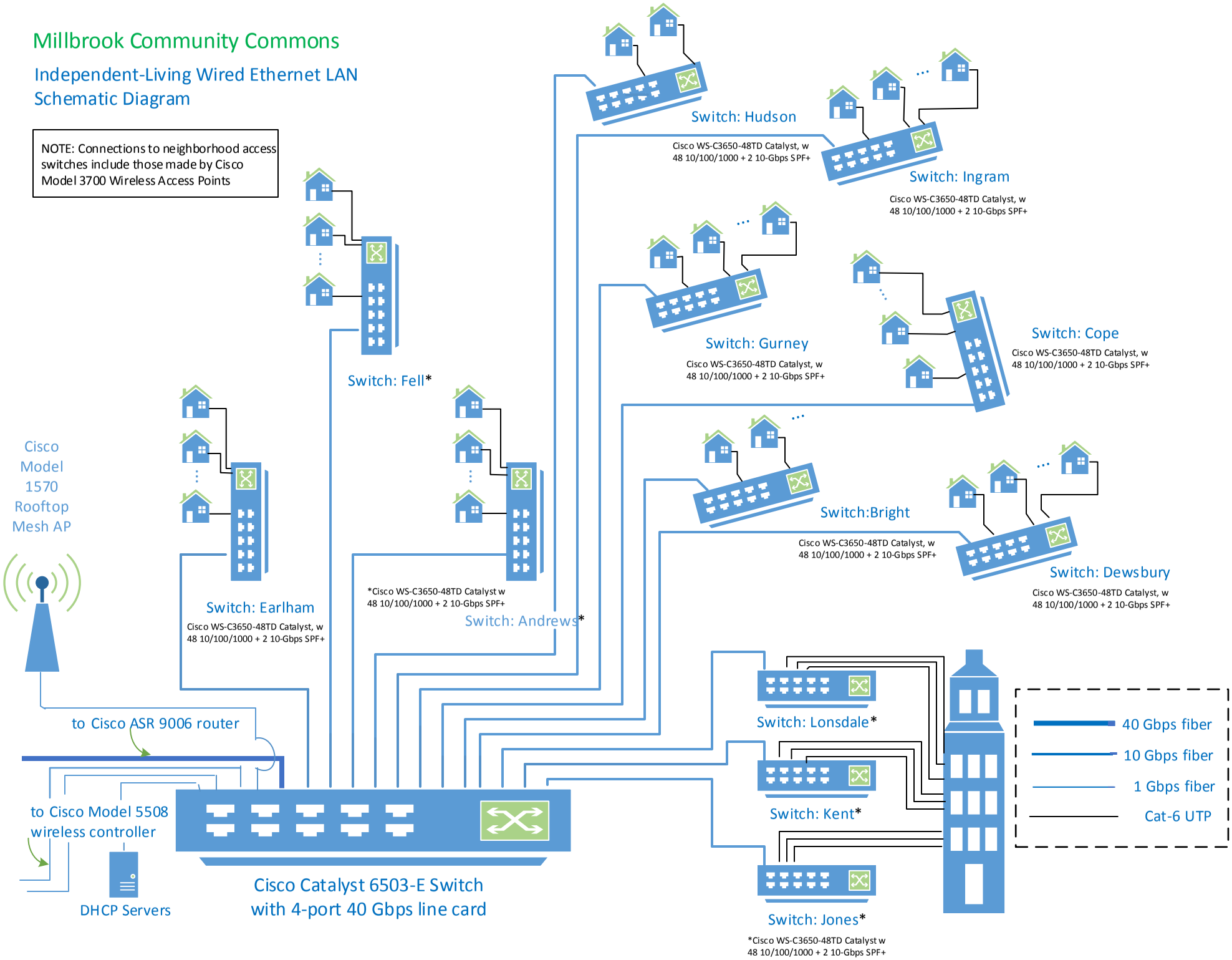
APPENDIX 4

14 Cisco Aironet Model 3700i Indoor Access Points Per Floor x 3 Floors

Millbrook Community Commons

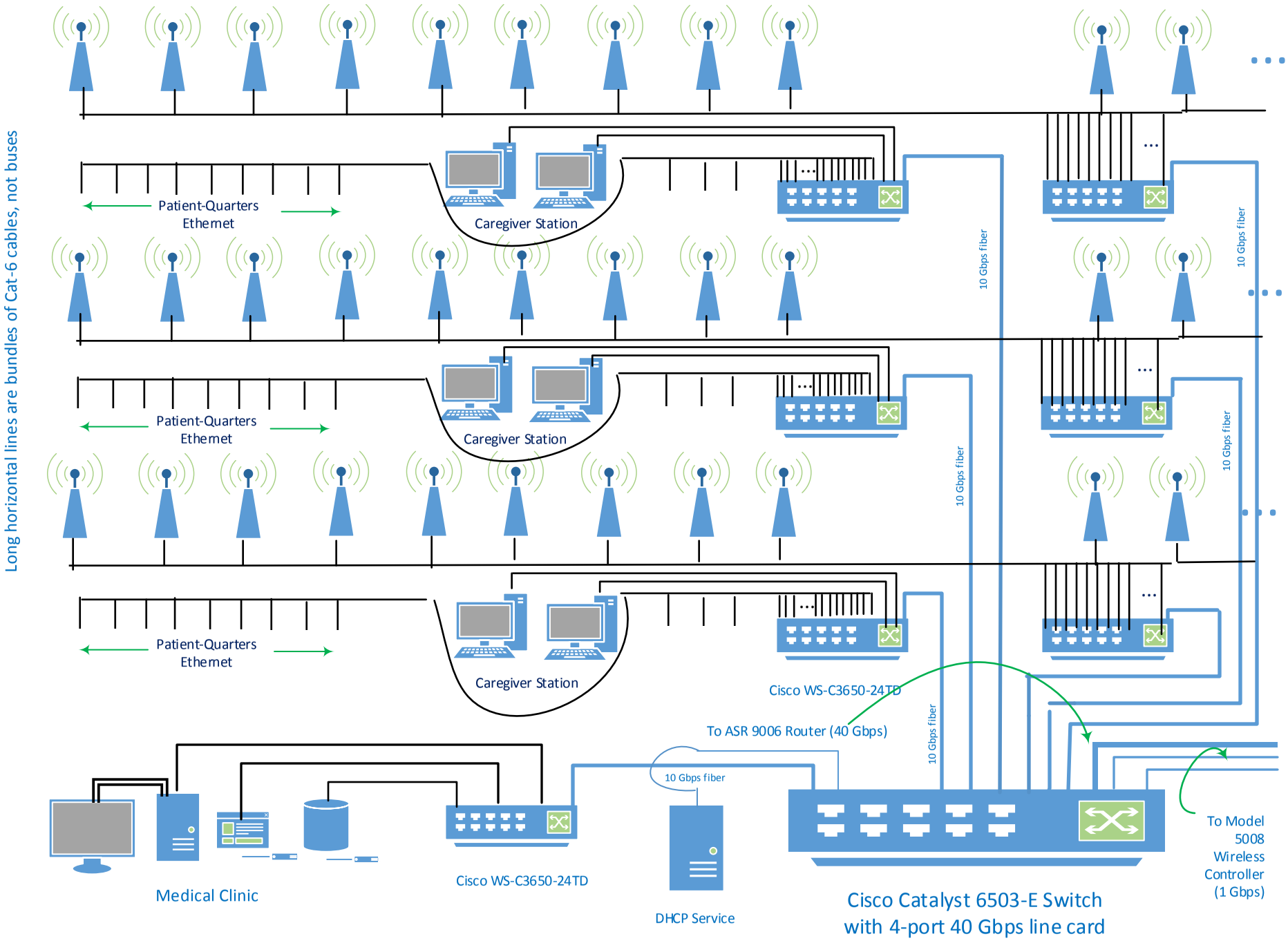
Independent-Living Wired Ethernet LAN Schematic Diagram

NOTE: Connections to neighborhood access switches include those made by Cisco Model 3700 Wireless Access Points



APPENDIX 5

Millbrook Community Commons: Assisted-Living Quarters, Nursing Home and Medical Clinic

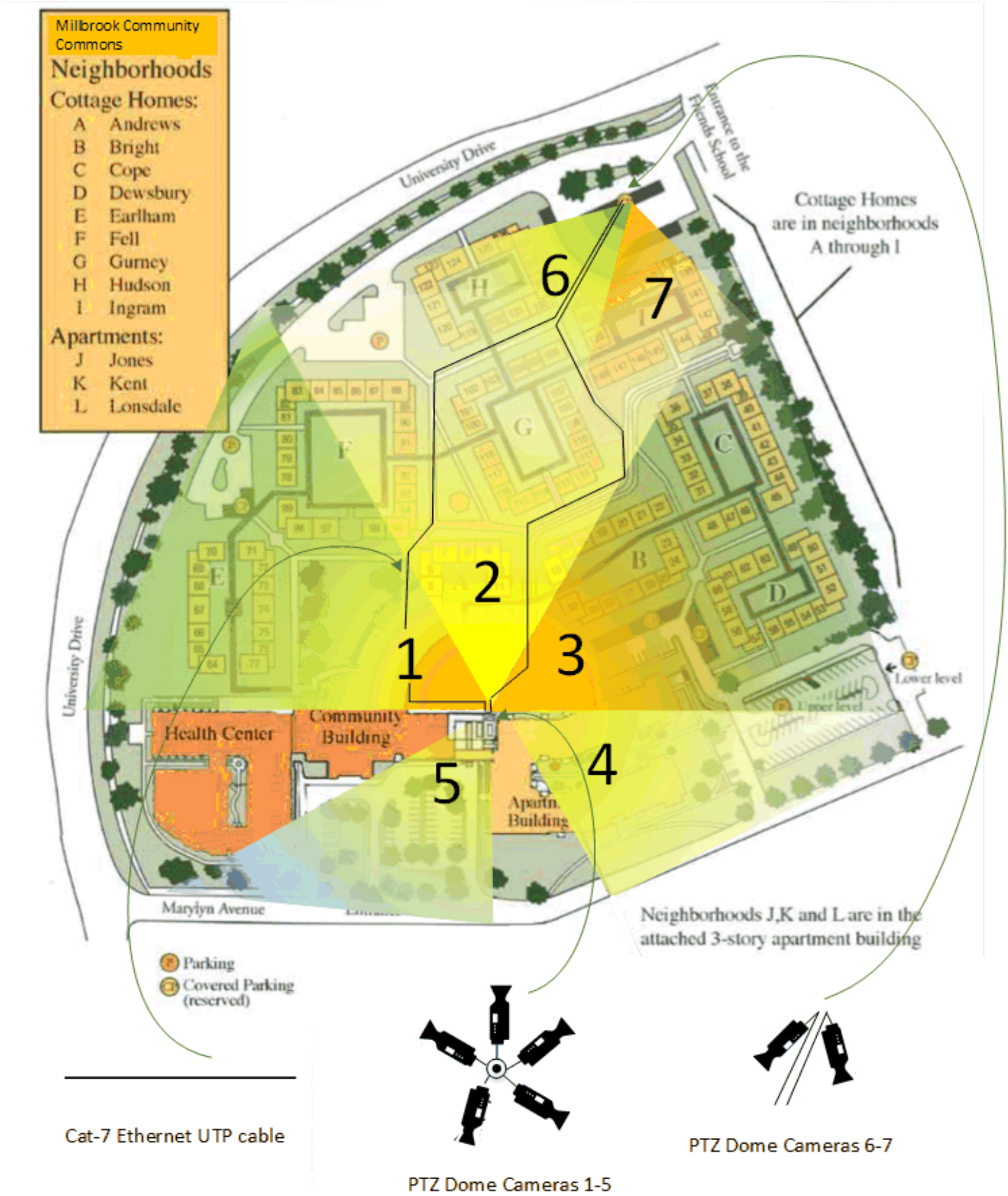


APPENDIX 6

Millbrook Community Commons

Network Camera Coverage

APPENDIX 7



Cat-7 Ethernet UTP cable

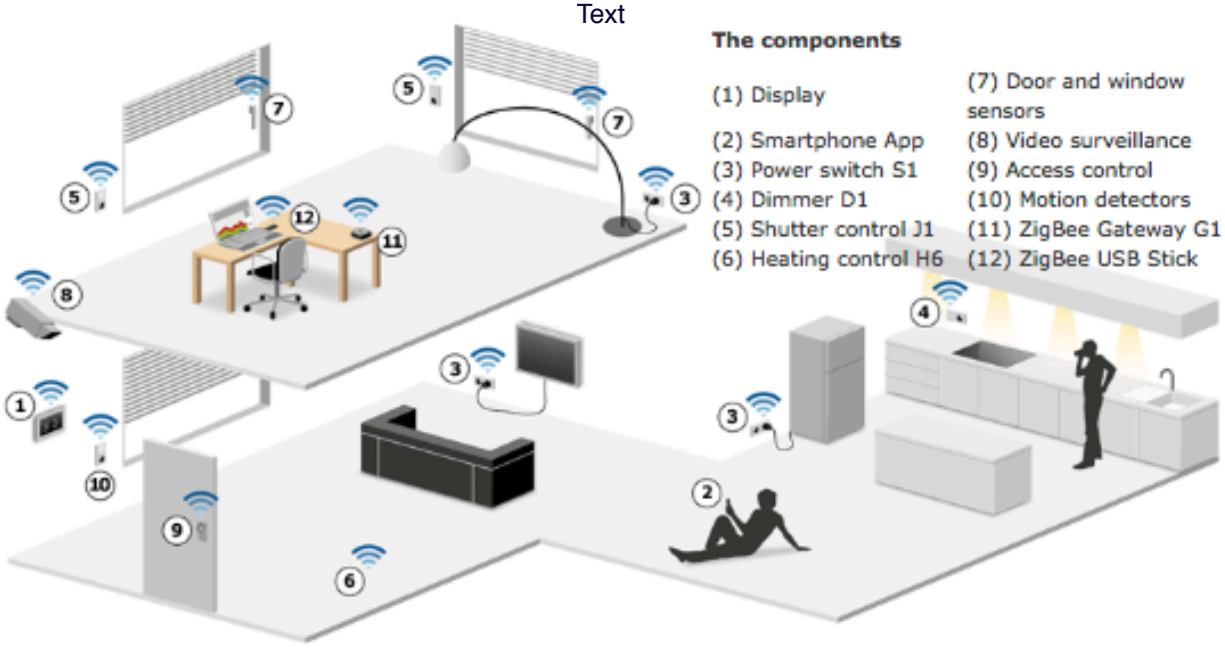
PTZ Dome Cameras 1-5

PTZ Dome Cameras 6-7

› Summary
› System overview
› Innovation
› ZigBee technology
› Technologies in comparison
› Installation
› Updates & Remote maintenance

System overview

Text



The components

(1) Display
(2) Smartphone App
(3) Power switch S1
(4) Dimmer D1
(5) Shutter control J1
(6) Heating control H6
(7) Door and window sensors
(8) Video surveillance
(9) Access control
(10) Motion detectors
(11) ZigBee Gateway G1
(12) ZigBee USB Stick

Short summary

The radio based system for intelligent building automation „Smart Home" by ubisy offers lighting control, shutter control, heating regulation, access verification as well as alarm-, security- and various comfort-functions.

The most important features

- **easy** handling
- **uncomplicated** Installation (no additional services required)
- **energy efficiency** (smart switching, dimming and consumption metering)
- **reasonably priced** when purchasing, installing, configuring, operating
- **Updatable** firmware

Advantages of the system

With our innovative, highly secure, very robust and reliable technology „Made in Germany" you can not only update your property but also by and by expand your smart home quickly and without much effort. When and how extensive is entirely up to you.

Cost reduction

- Dimming function reduces power consumption
- Motion detectors will realize nobody is in the room and automatically turn of the lights
- Heating will be regulated efficiently
- Cost control by displaying energy consumption per user

Additional benefits

- Operated by Apps, wall displays and conventional switches
- Sustainability: Your switches and sockets remain mounted
- Exceptional security (tested, international standards)
- „Smart Grid"-ready

Groups and scenarios

Combine different devices into groups to be able to turn all elements on and off together. Put together various scenarios in advance to be summoned and selected on demand and executed with a simple click on a button.

© 2006 – 2014 ubisys technologies GmbH. All rights reserved.